Cisco Nexus 7000 Series NX-OS セキュリティ コンフィギュレーション ガイド

初版：2012 年 07 月 27 日

最終更新：2016 年 05 月 11 日

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

Text Part Number: OL-25776-03-J

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

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

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

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries.To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks.Third-party trademarks mentioned are the property of their respective owners.The use of the word partner does not imply a partnership relationship between Cisco and any other company.(1110R)

© 2017 Cisco Systems, Inc. All rights reserved.

目 次

はじめに xxxv

対象読者 xxxv

表記法 xxxv

Cisco Nexus 7000 シリーズ NX-OS ソフトウェアの関連資料 xxxvii

マニュアルに関するフィードバック xxxix

マニュアルの入手方法およびテクニカル サポート xxxix

新機能および変更された機能に関する情報 1

新機能および変更された機能に関する情報 1

概要 13

Authentication, Authorization, and Accounting（認証、許可、およびアカウンティング） 14

RADIUS および TACACS+ セキュリティ プロトコル 15

LDAP 15

SSH および Telnet 15

PKI 16

ユーザ アカウントおよびユーザ ロール 16

802.1X 16

NAC 17

Cisco TrustSec 17

IP ACL 17

MAC ACL 18

VACL 18

ポート セキュリティ 18

DHCP スヌーピング 19

ダイナミック ARP インスペクション 19

IP ソース ガード 20

パスワード暗号化 20

キーチェーン管理 20
Unicast RPF 21
トラフィック ストーム制御 21
コントロール プレーン ポリシング 21
レート制限 22
FIPS の設定 23
機能情報の確認 23
FIPS の概要 24
FIPS のセルフテスト 24
FIPS エラー状態 25
RADIUS キーラップ 25
FIPS の仮想化サポート 26
FIPS のライセンス要件 26
FIPS の前提条件 26
FIPS の注意事項と制約事項 27
FIPS のデフォルト設定 27
FIPS の設定 27
FIPS モードのイネーブル化 28
FIPS モードのディセーブル化 29
FIPS の設定の確認 30
FIPS の設定例 30
FIPS に関する追加情報 31
FIPS の機能の履歴 31
AAA の設定 33
機能情報の確認 33
AAA の概要 34
AAA セキュリティ サービス 34
AAA を使用する利点 35
リモート AAA サービス 35
AAA サーバ グループ 35
AAA サービス設定オプション 36
ユーザ ログインの認証および許可プロセス 38

AES パスワード暗号化およびマスター暗号キー 39
AAA のバーチャライゼーション サポート 40
AAA のライセンス要件 40
AAA の前提条件 40
AAA の注意事項と制約事項 41
AAA のデフォルト設定 41
AAA の設定 41
AAA の設定プロセス 42
コンソール ログイン認証方式の設定 42
デフォルトのログイン認証方式の設定 44
ローカル認証へのフォールバックのディセーブル化 46
AAA 認証のデフォルト ユーザ ロールのイネーブル化 48
ログイン認証失敗メッセージのイネーブル化 49
CHAP 認証のイネーブル化 50
MSCHAP または MSCHAP V2 認証のイネーブル化 52
マスター キーの設定および AES パスワード暗号化機能のイネーブル化 55
既存のパスワードのタイプ 6 暗号化パスワードへの変換 56
タイプ 6 暗号化パスワードの元の状態への変換 56
タイプ 6 暗号化パスワードの削除 57
デフォルトの AAA アカウンティング方式の設定 57
Cisco NX-OS デバイスによる AAA サーバの VSA の使用 59
VSA の概要 59
VSA の形式 60
AAA サーバ上での Cisco NX-OS のユーザ ロールおよび SNMPv3 パラメータの指定 61
セキュア ログインの拡張機能 61
ログイン パラメータの設定 61
ログイン パラメータの設定例 63
ユーザごとのログイン ブロックの設定 63
ユーザごとのログイン ブロックの設定例 65
ユーザ 1 人あたりのセッション数の制限（ユーザ 1 人あたり、ログイン 1 回あたり） 65

パスフレーズの設定とユーザ アカウントのロック 66
ユーザ名のパスワード プロンプトのイネーブル化 68
OS の整合性を確認するための SHA-256 アルゴリズムのサポート 69
RADIUS/TACACS+ を使用するための共有キー値の設定 69
ローカル AAA アカウンティング ログのモニタリングとクリア 70
AAA 設定の確認 71
AAA の設定例 72
AAA に関する追加情報 72
AAA の機能の履歴 73
RADIUS の設定 75
機能情報の確認 75
RADIUS の概要 76
RADIUS ネットワーク環境 76
RADIUS の動作 76
RADIUS サーバのモニタリング 77
RADIUS 設定の配布 78
ベンダー固有属性 79
RADIUS のバーチャライゼーション サポート 80
RADIUS のライセンス要件 80
RADIUS の前提条件 81
RADIUS の注意事項と制約事項 81
RADIUS のデフォルト設定 81
RADIUS サーバの設定 82
RADIUS サーバの設定プロセス 82
RADIUS 設定の配布のイネーブル化 83
RADIUS サーバ ホストの設定 84
グローバル RADIUS キーの設定 86
特定の RADIUS サーバ用のキーの設定 87
RADIUS サーバ グループの設定 89
RADIUS サーバ グループのためのグローバル発信元インターフェイスの設定 91
ログイン時にユーザによる RADIUS サーバの指定を許可 92
グローバルな RADIUS 送信リトライ回数とタイムアウト間隔の設定 93

サーバに対する RADIUS 送信リトライ回数とタイムアウト間隔の設定 95
RADIUS サーバのアカウンティングおよび認証属性の設定 97
RADIUS サーバのグローバルな定期モニタリングの設定 99
各 RADIUS サーバの定期モニタリングの設定 101
RADIUS デッド タイム間隔の設定 103
ワンタイム パスワードの設定 104
RADIUS 情報の配布のコミット 105
RADIUS の配布セッションの廃棄 106
RADIUS の配布セッションのクリア 107
RADIUS サーバまたはサーバ グループの手動モニタリング 108
RADIUS 設定の確認 108
RADIUS サーバのモニタリング 109
RADIUS サーバ統計情報のクリア 109
RADIUS の設定例 110
次の作業 110
RADIUS に関する追加情報 110
RADIUS の機能の履歴 111
TACACS+ の設定 113
機能情報の確認 113
TACACS+ の概要 114
TACACS+ の利点 114
ユーザ ログインにおける TACACS+ の動作 114
デフォルトの TACACS+ サーバ暗号化タイプおよび秘密キー 115
TACACS+ サーバのコマンド許可サポート 116
TACACS+ サーバのモニタリング 116
TACACS+ 設定の配布 117
TACACS+ のベンダー固有属性 117
TACACS+ 用の Cisco VSA 形式 118
TACACS+ のライセンス要件 119
TACACS+ の前提条件 119
TACACS+ の注意事項と制約事項 119
TACACS+ のデフォルト設定 120

TACACS+ の設定 120
TACACS+ サーバの設定プロセス 121
TACACS+ のイネーブル化 121
TACACS+ サーバ ホストの設定 122
グローバル TACACS+ キーの設定 124
特定の TACACS+ サーバ用のキーの設定 126
TACACS+ サーバ グループの設定 127
TACACS+ サーバ グループのためのグローバル発信元インターフェイスの設定 129
ユーザによるログイン時の TACACS+ サーバ指定の許可 131
グローバルな TACACS+ タイムアウト間隔の設定 132
TACACS+ サーバのタイムアウト間隔の設定 133
TCP ポートの設定 135
TACACS+ サーバのグローバルな定期モニタリングの設定 136
各 TACACS+ サーバの定期モニタリングの設定 138
TACACS+ デッド タイム間隔の設定 141
ASCII 認証の設定 142
TACACS+ サーバでの AAA 許可の設定 144
TACACS+ サーバでのコマンド許可の設定 145
TACACS+ サーバでのコマンド許可のテスト 148
コマンド許可検証のイネーブル化とディセーブル化 149
TACACS+ サーバでの許可に使用する特権レベルのサポートの設定 149
権限ロールのユーザ コマンドの許可または拒否 152
TACACS+ 設定の配布のイネーブル化 154
TACACS+ 設定の配布のコミット 155
TACACS+ の配布セッションの廃棄 156
TACACS+ の配布セッションのクリア 157
TACACS+ サーバまたはサーバ グループの手動モニタリング 158
TACACS+ のディセーブル化 159
TACACS+ サーバのモニタリング 160
TACACS+ サーバ統計情報のクリア 160
TACACS+ の設定の確認 161
TACACS+ の設定例 162

次の作業 163
TACACS+ に関する追加情報 163
TACACS+ の機能の履歴 164
LDAP の設定 167
機能情報の確認 167
LDAP の概要 168
LDAP 認証および許可 168
ユーザ ログインにおける LDAP の動作 169
LDAP サーバのモニタリング 170
LDAP のベンダー固有属性 170
LDAP 用の Cisco VSA 形式 171
LDAP のバーチャライゼーション サポート 171
LDAP のライセンス要件 172
LDAP の前提条件 172
LDAP の注意事項と制約事項 172
LDAP のデフォルト設定 173
LDAP の設定 173
LDAP サーバの設定プロセス 174
LDAP のイネーブル化 174
LDAP サーバ ホストの設定 175
LDAP サーバの rootDN の設定 177
LDAP サーバ グループの設定 178
グローバルな LDAP タイムアウト間隔の設定 180
LDAP サーバのタイムアウト間隔の設定 181
グローバル LDAP サーバ ポートの設定 183
TCP ポートの設定 184
LDAP 検索マップの設定 185
LDAP サーバの定期的モニタリングの設定 187
LDAP デッド タイム間隔の設定 188
LDAP サーバでの AAA 許可の設定 189
LDAP のディセーブル化 191
LDAP サーバのモニタリング 192

LDAP サーバ統計情報のクリア 192
LDAP 設定の確認 193
LDAP の設定例 194
次の作業 194
LDAP に関する追加情報 194
LDAP の機能の履歴 195
SSH および Telnet の設定 197
機能情報の確認 197
SSH および Telnet の概要 198
SSH サーバ 198
SSH クライアント 198
SSH サーバ キー 198
デジタル証明書を使用した SSH 認証 199
Telnet サーバ 199
SSH および Telnet のバーチャライゼーション サポート 199
SSH および Telnet のライセンス要件 200
SSH および Telnet の前提条件 200
SSH と Telnet の注意事項と制約事項 200
SSH および Telnet のデフォルト設定 201
SSH の設定 201
SSH サーバ キーの生成 201
ユーザ アカウント用 SSH 公開キーの指定 203
IETF SECSH 形式による SSH 公開キーの指定 203
OpenSSH 形式の SSH 公開キーの指定 204
SSH ログイン試行の最大回数の設定 206
SSH 接続のログイン猶予時間の設定 207
SSH セッションの開始 208
ブート モードからの SSH セッションの開始 209
SSH のパスワードが不要なファイル コピーの設定 210
SCP サーバと SFTP サーバの設定 212
SSH ホストのクリア 213
SSH サーバのディセーブル化 214

SSH サーバ キーの削除 215
SSH セッションのクリア 216
Telnet の設定 216
Telnet サーバのディセーブル化 217
リモート デバイスとの Telnet セッションの開始 218
Telnet セッションのクリア 218
SSH および Telnet の設定の確認 219
SSH の設定例 220
SSH のパスワードが不要なファイル コピーの設定例 221
SSH および Telnet に関する追加情報 222
SSH および Telnet の機能の履歴 223
PKI の設定 225
機能情報の確認 225
PKI の概要 226
CA とデジタル証明書 226
信頼モデル、トラストポイント、アイデンティティ CA 226
RSA のキー ペアとアイデンティティ証明書 227
複数の信頼できる CA のサポート 228
PKI の登録のサポート 228
カットアンドペーストによる手動での登録 228
複数の RSA キー ペアとアイデンティティ CA のサポート 229
ピア証明書の検証 229
証明書の取消確認 230
CRL のサポート 230
証明書と対応するキー ペアのインポートとエクスポート 230
PKI のバーチャライゼーション サポート 230
PKI のライセンス要件 230
PKI の注意事項と制約事項 231
PKI のデフォルト設定 231
CA の設定とデジタル証明書 232
ホスト名と IP ドメイン名の設定 232
RSA キー ペアの生成 233

トラストポイント CA のアソシエーションの作成 235
証明書認証の cert-store の設定 236
証明書マッピングのフィルタの設定 238
CA の認証 240
証明書取消確認方法の設定 242
証明書要求の作成 244
アイデンティティ証明書のインストール 246
トラストポイントの設定がリブート後も維持されていることの確認 247
PKCS 12 形式でのアイデンティティ情報のエクスポート 248
PKCS 12 形式でのアイデンティティ情報のインポート 249
CRL の設定 251
CA の設定からの証明書の削除 252
Cisco NX-OS デバイスからの RSA キー ペアの削除 254
PKI の設定の確認 255
PKI の設定例 255
Cisco NX-OS デバイスでの証明書の設定 256
cert-store および証明書マッピングのフィルタの設定 259
CA 証明書のダウンロード 260
アイデンティティ証明書の要求 264
証明書の取り消し 272
CRL の作成と公開 274
CRL のダウンロード 275
CRL のインポート 278
PKI に関する追加情報 280
PKI の関連資料 280
PKI の標準規格 281
PKI の機能の履歴 281
ユーザ アカウントおよび RBAC の設定 283
機能情報の確認 283
ユーザ アカウントおよび RBAC の概要 284
ユーザ アカウント 284
強力なパスワードの特性 284

ユーザ ロール 285
ユーザ ロールのルール 286
ユーザ ロールの設定の配布 287
RBAC のバーチャライゼーション サポート 288
ユーザ アカウントおよび RBAC のライセンス要件 288
ユーザ アカウントおよび RBAC の注意事項と制約事項 289
ユーザ アカウントおよび RBAC のデフォルト設定 289
パスワードの強度確認のイネーブル化 290
ユーザ アカウントの設定 292
ロールの設定 294
ユーザ ロール設定の配布のイネーブル化 294
ユーザ ロールおよびルールの作成 295
機能グループの作成 298
ユーザ ロール インターフェイス ポリシーの変更 300
ユーザ ロール VLAN ポリシーの変更 302
ユーザ ロールの VRF ポリシーの変更 303
ユーザ ロール設定の配布へのコミット 305
ユーザ ロールの配布セッションの廃棄 307
ユーザ ロールの配布セッションのクリア 308
ユーザ アカウントおよび RBAC 設定の確認 308
ユーザ アカウントおよび RBAC の設定例 309
ユーザ アカウントおよび RBAC に関する追加情報 311
ユーザ アカウントおよび RBAC の関連資料 312
ユーザ アカウントおよび RBAC の標準規格 312
ユーザ アカウントと RBAC の MIB 312
ユーザ アカウントおよび RBAC の機能の履歴 312
802.1X の設定 315
機能情報の確認 315
802.1X の概要 316
デバイスのロール 316
認証の開始およびメッセージ交換 317
インターフェイスのオーセンティケータ PAE ステータス 318

許可ステートおよび無許可ステートのポート 319
MAC 認証バイパス 320
802.1X とポート セキュリティ 321
シングル ホストおよびマルチ ホストのサポート 322
サポートされるトポロジ 323
802.1X のバーチャライゼーション サポート 323
802.1X のライセンス要件 323
802.1X の前提条件 324
802.1X の注意事項と制約事項 324
802.1X のデフォルト設定 325
802.1X の設定 327
802.1X の設定プロセス 327
802.1X 機能のイネーブル化 327
802.1X の AAA 認証方式の設定 328
インターフェイスでの 802.1X 認証の制御 330
メンバ ポートでの 802.1X 認証の設定 331
インターフェイスでのオーセンティケータ PAE の作成または削除 334
グローバル定期再認証のイネーブル化 335
インターフェイスの定期再認証のイネーブル化 337
手動によるサプリカントの再認証 338
手動による 802.1X 認証の初期化 339
802.1X グローバル認証タイマーの変更 339
インターフェイスの 802.1X 認証タイマーの変更 341
シングル ホスト モードまたはマルチ ホスト モードのイネーブル化 344
MAC 認証バイパスのイネーブル化 346
Cisco NX-OS デバイスでの 802.1X 認証のディセーブル化 347
802.1X 機能のディセーブル化 348
802.1X グローバル設定のデフォルト値へのリセット 349
802.1X インターフェイス設定のデフォルト値へのリセット 350
オーセンティケータとサプリカント間のフレーム再送信最大リトライ回数のグローバル設定 351

インターフェイスでのオーセンティケータとサプリカント間のフレーム再送信最大リトライ回数の設定 353
802.1X 認証の RADIUS アカウンティングのイネーブル化 354
802.1X の AAA アカウンティング方式の設定 355
インターフェイスでの再認証最大リトライ回数の設定 356
802.1X 設定の確認 357
802.1X のモニタリング 358
802.1X の設定例 358
802.1X に関する追加情報 359
802.1X の機能の履歴 360
NAC の設定 361
機能情報の確認 361
NAC の概要 362
NAC デバイスのロール 362
NAC のポスチャ検証 365
IP デバイス トラッキング 367
NAC LPIP 368
ポスチャ検証 369
ポスチャ検証のトリガー 369
ポスチャ検証の方法 369
例外リスト 369
EAPoUDP 370
ACL を使用したポリシーの適用 370
監査サーバおよび非応答ホスト 371
NAC タイマー 372
ホールド タイマー 372
AAA タイマー 373
再送信タイマー 373
再検証タイマー 373
ステータス クエリー タイマー 374
NAC ポスチャ検証および冗長スーパーバイザ モジュール 374
LPIP 検証および他のセキュリティ機能 374
802.1X 374

ポート セキュリティ 374
DHCP スヌーピング 375
ダイナミック ARP インスペクション 375
IP ソース ガード 375
ポスチャのホスト固有 ACE 376
アクティブ PACL 376
VACL 376
NAC のバーチャライゼーション サポート 376
NAC のライセンス要件 376
NAC の前提条件 377
NAC の注意事項と制約事項 377
LPIP の制約事項 377
NAC のデフォルト設定 378
NAC の設定 378
NAC の設定プロセス 379
EAPoUDP のイネーブル化 379
EAPoUDP のデフォルト AAA 認証方式のイネーブル化 380
インターフェイスへの PACL の適用 382
インターフェイスでの NAC のイネーブル化 383
アイデンティティ ポリシーおよびアイデンティティ プロファイル エントリの設定 384
クライアントレス エンドポイント装置の検証 387
EAPoUDP のロギングのイネーブル化 388
EAPoUDP のグローバル最大リトライ回数の変更 389
個別インターフェイスの EAPoUDP 最大リトライ回数の変更 390
EAPoUDP の UDP ポートの変更 392
EAPoUDP ポスチャ検証の同時セッション数に関するレート制限の設定 393
グローバル自動ポスチャ再検証の設定 394
個別インターフェイスでの自動ポスチャ再検証の設定 395
EAPoUDP グローバル タイマーの変更 397
個別インターフェイスでの EAPoUDP タイマーの変更 399
EAPoUPD グローバル設定のデフォルト値へのリセット 402

EAPoUPD インターフェイス設定のデフォルト値へのリセット 403
IP デバイス トラッキングの設定 404
IP デバイス トラッキングのクリア 407
手動による EAPoUDP セッションの初期化 408
手動による EAPoUDP セッションの再検証 409
EAPoUDP セッションのクリア 411
EAPoUDP 機能のディセーブル化 412
NAC の設定の確認 413
NAC の設定例 414
NAC に関する追加情報 414
NAC の機能の履歴 414
Cisco TrustSec の設定 417
機能情報の確認 417
Cisco TrustSec の概要 418
Cisco TrustSec のアーキテクチャ 418
認証 421
Cisco TrustSec と認証 421
EAP-FAST への Cisco TrustSec の機能拡張 422
802.1X ロールの選択 423
Cisco TrustSec 認証の概要 423
デバイス ID 424
デバイスのクレデンシャル 424
ユーザ クレデンシャル 424
トランク ポートおよび FabricPath ポートでのネイティブ VLAN タギング 425
SGACL と SGT 426
送信元セキュリティ グループの判断 428
宛先セキュリティ グループの判断 428
SGACL ロギング 429
SGACL モニタ モード 429
SXP によるレガシー アクセス ネットワークへの SGT の伝播 429
SXPv3 を使用した Cisco TrustSec 431
SXPv3 サブネットの展開 431

SXP バージョン ネゴシエーション 432
デフォルト ルートの SGT バインディングの SXP サポート 433
Cisco TrustSec サブネットと SGT のマッピング 433
許可とポリシーの取得 434
許可の変更 434
環境データのダウンロード 435
RADIUS リレー機能 435
仮想ポート チャネル（vPC）の SGT サポート 435
バインディング送信元プライオリティ 436
仮想化のサポート 437
Cisco TrustSec のライセンス要件 437
Cisco TrustSec の前提条件 437
Cisco TrustSec の注意事項と制約事項 438
Cisco TrustSec パラメータのデフォルト設定 440
Cisco TrustSec の設定 440
Cisco TrustSec SGT 機能のイネーブル化 441
Cisco TrustSec デバイスのクレデンシャルの設定 442
ネイティブ VLAN タギングの設定 444
ネイティブ VLAN タギングのグローバル設定 444
インターフェイスでのネイティブ VLAN タギングの設定 444
Cisco TrustSec の AAA の設定 445
Cisco TrustSec シード Cisco NX-OS デバイスでの AAA の設定 446
Cisco TrustSec 非シード NX-OS デバイスでの AAA の設定 448
Cisco TrustSec の認証、許可、SAP、およびデータ パス セキュリティの設定 450
Cisco TrustSec の認証および許可の設定プロセス 450
Cisco TrustSec 認証のイネーブル化 450
インターフェイスおよびポート プロファイルに対する Cisco TrustSec データ パス リプレイ保護の設定 453
インターフェイスおよびポート プロファイルに対する Cisco TrustSec SAP 動作モードの設定 455
インターフェイスおよびポート プロファイルに対する Cisco TrustSec SGT 伝播の設定 457

インターフェイスの SAP キーの再生成 459
手動での Cisco TrustSec 認証の設定 460
インターフェイスでの Cisco TrustSec のポーズ フレームの暗号化または復号化の設定 464
SGACL ポリシーの設定 466
SGACL ポリシーの設定プロセス 467
SGACL バッチ プログラミングのイネーブル化 467
VLAN に対する SGACL ポリシーの強制のイネーブル化 468
VRF インスタンスでの SGACL ポリシーの強制のイネーブル化 469
SGACL ロギングの設定 471
SGACL モニタ モードの設定 474
Cisco TrustSec SGT の手動設定 476
VLAN に対する IPv4 アドレスと SGACL SGT のマッピングの手動設定 477
VRF インスタンスに対する IPv4 アドレスと SGACL SGT のマッピングの手動設定 478
VLAN と SGT のマッピングの設定 480
SGACL ポリシーの手動設定 481
ダウンロードされた SGACL ポリシーの表示 484
ダウンロードされた SGACL ポリシーのリフレッシュ 484
環境データの更新 485
RBACL の統計情報のイネーブル化 486
Cisco TrustSec の SGACL ポリシーのクリア 488
SXP の手動設定 488
Cisco TrustSec SXP の設定プロセス 488
Cisco TrustSec SXP のイネーブル化 489
Cisco TrustSec SXP のピア接続の設定 490
デフォルトの SXP パスワードの設定 492
デフォルトの SXP 送信元 IPv4 アドレスの設定 493
SXP 復帰期間の変更 495
SXP リトライ期間の変更 496
SXPv3 の設定 497
SGT バインディングのデフォルト ルートの設定 498

サブネットと SGT のマッピングの設定 499
ポート チャネル メンバでの Cisco TrustSec サポート 500
設定モデル 500
Cisco NX-OS Release 7.2(0)D1(1) のユーザ インターフェイスの更新 501
インサービス ソフトウェア アップグレード 501
Cisco TrustSec の設定の確認 501
Cisco TrustSec の設定例 504
Cisco TrustSec のイネーブル化 504
シード Cisco NX-OS デバイスへの Cisco TrustSec AAA の設定 504
インターフェイスに対する Cisco TrustSec 認証のイネーブル化 504
手動での Cisco TrustSec 認証の設定 504
デフォルト VRF インスタンスに対する Cisco TrustSec ロールベース ポリシー強制の設定 505
デフォルト以外の VRF に対する Cisco TrustSec ロールベース ポリシー強制の設定 505
VLAN に対する Cisco TrustSec ロールベース ポリシー強制の設定 505
デフォルト VRF インスタンスに対する IPv4 アドレスと SGACL SGT のマッピングの設定 506
デフォルト以外の VRF インスタンスに対する IPv4 アドレスと SGACL SGT のマッピングの設定 506
VLAN に対する IPv4 アドレスと SGACL SGT のマッピングの設定 506
Cisco TrustSec SGACL の手動設定 506
SXP ピア接続の手動設定 507
Cisco TrustSec に関する追加情報 508
Cisco TrustSec の機能の履歴 508
Cisco TrustSec MACSec の設定 513
機能情報の確認 513
Cisco TrustSec MACSec の前提条件 514
Cisco TrustSec MACSec の注意事項と制約事項 514
Cisco TrustSec MACSec について 515
Cisco TrustSec のアーキテクチャ 515
認証 518

Cisco TrustSec と認証 518
EAP-FAST への Cisco TrustSec の機能拡張 519
802.1X ロールの選択 520
Cisco TrustSec 認証の概要 520
デバイス ID 521
デバイスのクレデンシャル 521
ユーザ クレデンシャル 521
トランク ポートおよび FabricPath ポートでのネイティブ VLAN タギング 522
MACSec 523
CTS MACSEC GCM 256 ビットと拡張パケット シーケンス番号のサポート 523
Cisco TrustSec MACSec のライセンス要件 524
Cisco TrustSec パラメータのデフォルト設定 525
Cisco TrustSec MACSec の設定 526
Cisco TrustSec MACSec 機能のイネーブル化 526
Cisco TrustSec デバイスのクレデンシャルの設定 527
ネイティブ VLAN タギングの設定 529
ネイティブ VLAN タギングのグローバル設定 529
インターフェイスでのネイティブ VLAN タギングの設定 529
Cisco TrustSec の認証、許可、SAP、およびデータ パス セキュリティの設定 530
Cisco TrustSec の認証および許可の設定プロセス 530
Cisco TrustSec 認証のイネーブル化 531
インターフェイスおよびポート プロファイルに対する Cisco TrustSec データパス リプレイ保護の設定 533
インターフェイスおよびポート プロファイルに対する Cisco TrustSec SAP 動作モードの設定 535
インターフェイスの SAP キーの再生成 537
手動での Cisco TrustSec 認証の設定 538
Dot1x モードでの Cisco TrustSec 認証の設定 542
ポート チャネル メンバでの Cisco TrustSec サポート 544
設定モデル 544
Cisco NX-OS Release 7.2(0)D1(1) のユーザ インターフェイスの更新 545
インサービス ソフトウェア アップグレード 545

Cisco TrustSec MACSec の設定の確認 546
Cisco TrustSec MACSec に関する追加情報 546
Cisco TrustSec MACSec の機能の履歴 547
IP ACL の設定 549
機能情報の確認 550
ACL の概要 550
ACL のタイプと適用 550
ACL の適用順序 553
ルールについて 554
IP ACL のプロトコル 555
送信元と宛先 555
IP ACL および MAC ACL の暗黙ルール 555
その他のフィルタリング オプション 556
シーケンス番号 557
論理演算子と論理演算ユニット 558
ロギング 559
ACL キャプチャ 559
時間範囲 560
ポリシーベース ACL 562
統計情報と ACL 562
Atomic ACL のアップデート 563
Atomic ACL アップデートの計画 564
ACL TCAM バンク マッピング 565
フレキシブル ACL TCAM バンク チェーニング 565
フレキシブル ACL TCAM バンク チェーニング モード 566
IP ACL に対する Session Manager のサポート 568
IP ACL のバーチャライゼーション サポート 568
IP ACL のライセンス要件 568
IP ACL の前提条件 568
IP ACL の注意事項と制約事項 569
IP ACL のデフォルト設定 574
IP ACL の設定 575

IP ACL の作成 575
IP ACL の変更 577
VTY ACL の作成 579
IP ACL 内のシーケンス番号の変更 581
IP ACL の削除 582
ルータ ACL としての IP ACL の適用 584
ポート ACL としての IP ACL の適用 585
IP ACL の VACL としての適用 587
ACL TCAM バンク マッピングの設定 587
フレキシブル ACL TCAM バンク チェーニングの設定 589
ACL キャプチャのイネーブル化またはディセーブル化 590
ACL キャプチャ セッションの設定 591
キャプチャ セッション ACE を使用した ACL のインターフェイスへの適用 593
すべての ACL キャプチャ セッションのインターフェイスへの適用 595
IP ACL の設定の確認 596
IP ACL の統計情報のモニタリングとクリア 598
IP ACL の設定例 599
オブジェクト グループの設定 600
オブジェクト グループに対する Session Manager のサポート 600
IPv4 アドレス オブジェクト グループの作成および変更 600
IPv6 アドレス オブジェクト グループの作成および変更 602
プロトコル ポート オブジェクト グループの作成および変更 604
オブジェクト グループの削除 606
オブジェクト グループの設定の確認 606
時間範囲の設定 607
時間範囲に対する Session Manager のサポート 607
時間範囲の作成 607
時間範囲の変更 609
時間範囲の削除 611
時間範囲のシーケンス番号の変更 612
時間範囲設定の確認 613
フレキシブル ACL TCAM バンク チェーニングのトラブルシューティング 613

IP ACL に関する追加情報 614
IP ACL の機能の履歴 615
MAC ACL の設定 617
機能情報の確認 617
MAC ACL の概要 618
MAC パケット分類 618
MAC ACL のライセンス要件 618
MAC ACL の前提条件 619
MAC ACL の注意事項と制約事項 619
MAC ACL のデフォルト設定 619
MAC ACL の設定 620
MAC ACL の作成 620
MAC ACL の変更 621
MAC ACL 内のシーケンス番号の変更 623
MAC ACL の削除 623
ポート ACL としての MAC ACL の適用 624
MAC ACL の VACL としての適用 626
MAC パケット分類のイネーブル化またはディセーブル化 626
MAC ACL の設定の確認 628
MAC ACL の統計情報のモニタリングとクリア 628
MAC ACL の設定例 629
MAC ACL に関する追加情報 629
MAC ACL の機能の履歴 630
VLAN ACL の設定 631
機能情報の確認 631
VLAN ACL の概要 632
VLAN アクセス マップとエントリ 632
VACL とアクション 632
VACL の統計情報 632
VACL に対する Session Manager のサポート 633
VACL のバーチャライゼーション サポート 633
VACL のライセンス要件 633

VACL の前提条件 634
VACL の注意事項と制約事項 634
VACL のデフォルト設定 635
VACL の設定 635
VACL の作成または VACL エントリの追加 635
VACL または VACL エントリの削除 637
VACL の VLAN への適用 638
拒否 ACE サポートの設定 639
VACL 設定の確認 640
VACL 統計情報のモニタリングとクリア 641
VACL の設定例 642
VACL に関する追加情報 642
VLAN ACL の機能の履歴 643
ポート セキュリティの設定 645
機能情報の確認 645
ポート セキュリティの概要 646
セキュア MAC アドレスの学習 646
スタティック方式 646
ダイナミック方式 647
スティッキ方式 647
ダイナミック アドレスのエージング 648
セキュア MAC アドレスの最大数 648
セキュリティ違反と処理 649
ポート セキュリティとポート タイプ 651
ポート セキュリティとポート チャネル インターフェイス 652
ポート タイプの変更 654
802.1X とポート セキュリティ 655
ポート セキュリティのバーチャライゼーション サポート 656
ポート セキュリティのライセンス要件 656
ポート セキュリティの前提条件 657
ポート セキュリティのデフォルト設定 657
ポート セキュリティの注意事項と制約事項 658

ポート セキュリティの設定 658
ポート セキュリティのグローバルなイネーブル化またはディセーブル化 658
レイヤ 2 インターフェイスに対するポート セキュリティのイネーブル化またはディセーブル化 659
スティッキ MAC アドレス ラーニングのイネーブル化またはディセーブル化 661
インターフェイスのスタティック セキュア MAC アドレスの追加 663
インターフェイスのスタティック セキュア MAC アドレスの削除 664
スティッキ セキュア MAC アドレスの削除 666
ダイナミック セキュア MAC アドレスの削除 667
MAC アドレスの最大数の設定 668
アドレス エージングのタイプと期間の設定 670
セキュリティ違反時の処理の設定 671
ポート セキュリティの設定の確認 673
セキュア MAC アドレスの表示 673
ポート セキュリティの設定例 673
ポート セキュリティに関する追加情報 674
ポート セキュリティの機能の履歴 674
DHCP の設定 677
機能情報の確認 678
DHCP スヌーピングの概要 678
信頼できる送信元と信頼できない送信元 678
DHCP スヌーピング バインディング データベース 679
vPC 環境での DHCP スヌーピング 680
DHCP スヌーピング バインディング エントリの同期 680
パケット検証 680
DHCP スヌーピングの Option 82 データ挿入 681
DHCP リレー エージェントの概要 684
DHCP リレー エージェント 684
DHCP リレー エージェントの Option 82 684
DHCP リレー エージェントに対する VRF サポート 686
DHCP スマート リレー エージェント 687
DHCPv6 リレー エージェントの概要 687

DHCPv6 リレー エージェント 687
DHCPv6 リレー エージェントに対する VRF サポート 687
Lightweight DHCPv6 リレー エージェントについて 688
Lightweight DHCPv6 リレー エージェント 688
VLAN およびインターフェイスでの LDRA 688
Lightweight DHCPv6 リレー エージェントの注意事項と制約事項 689
UDP リレーについて 689
UDP リレー 689
UDP リレーのイネーブル化 689
UDP のサブネット ブロードキャスト 690
UDP リレーの注意事項と制約事項 691
DHCP の仮想化サポート 691
DHCP のライセンス要件 692
DHCP の前提条件 692
DHCP の注意事項と制約事項 692
DHCP のデフォルト設定 694
DHCP の設定 695
DHCP の最小設定 695
DHCP 機能のイネーブル化またはディセーブル化 696
DHCP スヌーピングのグローバルなイネーブル化またはディセーブル化 697
VLAN に対する DHCP スヌーピングのイネーブル化またはディセーブル化 698
DHCP スヌーピングの MAC アドレス検証のイネーブル化またはディセーブル化 699
Option 82 データの挿入および削除のイネーブル化またはディセーブル化 700
DHCP パケットの厳密な検証のイネーブル化またはディセーブル化 702
インターフェイスの信頼状態の設定 703
DHCP リレー信頼ポート設定機能のイネーブル化およびディセーブル化 704
インターフェイスを DHCP リレーの信頼できるポートまたは信頼できないポートとして設定する 705
すべてのインターフェイスの信頼状態の設定 707
DHCP リレー エージェントのイネーブル化またはディセーブル化 709
DHCP リレー エージェントに対する Option 82 のイネーブル化またはディセーブル化 710

DHCP リレーエージェントに対する VRF サポートのイネーブル化またはディセーブル化 711
レイヤ 3 インターフェイスの DHCP リレー エージェントに対するサブネット ブロードキャスト サポートのイネーブル化またはディセーブル化 712
インターフェイスへの DHCP サーバ アドレスの設定 714
DHCP スマート リレーのグローバルなイネーブル化またはディセーブル化 716
レイヤ 3 インターフェイスでの DHCP スマート リレーのイネーブル化またはディセーブル化 717
DHCPv6 の設定 719
DHCPv6 リレー エージェントのイネーブル化またはディセーブル化 719
DHCPv6 リレー エージェントに対する VRF サポートのイネーブル化またはディセーブル化 720
インターフェイスへの DHCPv6 サーバ アドレスの設定 721
DHCPv6 リレー送信元インターフェイスの設定 723
Lightweight DHCPv6 リレー エージェントの設定 725
インターフェイスの Lightweight DHCPv6 リレー エージェントの設定 725
VLAN の Lightweight DHCPv6 リレー エージェントの設定 726
UDP リレーの設定 727
DHCP 設定の確認 729
DHCP バインディングの表示 729
LDRA 情報の表示とクリア 729
UDP リレー情報の表示 730
DHCP スヌーピング バインディング データベースのクリア 733
DHCP リレー統計情報のクリア 734
DHCPv6 リレー統計情報のクリア 734
DHCP のモニタリング 734
DHCP の設定例 735
LDRA の設定例 736
DHCP に関する追加情報 736
DHCP の機能の履歴 737
ダイナミック ARP インスペクションの設定 739
機能情報の確認 739

DAI の概要 740
ARP 740
ARP スプーフィング攻撃 740
DAI および ARP スプーフィング攻撃 741
インターフェイスの信頼状態とネットワーク セキュリティ 742
ARP ACL および DHCP スヌーピング エントリのプライオリティ 744
DAI パケットのロギング 744
DAI のバーチャライゼーション サポート 745
DAI のライセンス要件 745
DAI の前提条件 745
DAI の注意事項と制約事項 745
DAI のデフォルト設定 746
DAI の設定 747
VLAN での DAI のイネーブル化とディセーブル化 747
レイヤ 2 インターフェイスの DAI 信頼状態の設定 748
DAI フィルタリングを目的とした ARP ACL の VLAN への適用 750
追加検証のイネーブル化またはディセーブル化 751
DAI のログ バッファ サイズの設定 752
DAI のログ フィルタリングの設定 753
DAI の設定の確認 754
DAI の統計情報のモニタリングとクリア 755
DAI の設定例 755
例 1：2 つのデバイスが DAI をサポートする場合 755
デバイス A の設定 756
デバイス B の設定 758
例 2：1 つのデバイスが DAI をサポートする場合 760
ARP ACL の設定 762
ARP ACL に対する Session Manager のサポート 762
ARP ACL の作成 763
ARP ACL の変更 764
ARP ACL の削除 766
ARP ACL のシーケンス番号の変更 767

ARP ACL の設定の確認 767
DAI に関する追加情報 768
DAI の機能の履歴 768
IP ソース ガードの設定 771
機能情報の確認 771
IP ソース ガードの概要 772
IP ソース ガードのバーチャライゼーション サポート 772
IP ソース ガードのライセンス要件 773
IP ソース ガードの前提条件 773
IP ソース ガイドの注意事項と制約事項 773
IP ソース ガードのデフォルト設定 774
IP ソース ガードの設定 774
レイヤ 2 インターフェイスに対する IP ソース ガードのイネーブル化またはディセーブル化 774
スタティック IP ソース エントリの追加または削除 775
IP ソース ガード バインディングの表示 776
IP ソース ガードの設定例 776
IP ソース ガードに関する追加情報 777
IP ソース ガードの機能の履歴 777
パスワード暗号化の設定 779
機能情報の確認 779
パスワード暗号化の概要 780
AES パスワード暗号化およびマスター暗号キー 780
パスワード暗号化の仮想化サポート 780
パスワード暗号化のライセンス要件 780
パスワード暗号化の注意事項と制約事項 781
パスワード暗号化のデフォルト設定 781
パスワード暗号化の設定 782
マスター キーの設定および AES パスワード暗号化機能のイネーブル化 782
既存のパスワードのタイプ 6 暗号化パスワードへの変換 783
タイプ 6 暗号化パスワードの元の状態への変換 784
タイプ 6 暗号化パスワードの削除 784

パスワード暗号化の設定の確認 785
パスワード暗号化の設定例 785
パスワード暗号化に関する追加情報 786
パスワード暗号化の機能の履歴 786
キーチェーン管理の設定 787
機能情報の確認 787
キーチェーン管理の概要 788
キーチェーンおよびキーチェーン管理 788
キーのライフタイム 788
キーチェーン管理のバーチャライゼーション サポート 789
Licensing Requirements for Keychain Management 789
キーチェーン管理の前提条件 789
キーチェーン管理の注意事項と制約事項 790
キーチェーン管理のデフォルト設定 790
キーチェーン管理の設定 790
キーチェーンの作成 790
キーチェーンの削除 791
マスター キーの設定および AES パスワード暗号化機能のイネーブル化 792
キーのテキストの設定 794
キーの受け入れライフタイムおよび送信ライフタイムの設定 795
アクティブなキーのライフタイムの確認 797
キーチェーン管理の設定の確認 798
キーチェーン管理の設定例 798
次の作業 798
キーチェーン管理に関する追加情報 799
キーチェーン管理の機能の履歴 799
トラフィック ストーム制御の設定 801
機能情報の確認 801
トラフィック ストーム制御の概要 802
トラフィック ストーム制御のバーチャライゼーション サポート 803
トラフィック ストーム制御のライセンス要件 803
トラフィック ストーム制御の注意事項と制約事項 804

トラフィック ストーム制御のデフォルト設定 804
トラフィック ストーム制御の設定 805
トラフィック ストーム制御の設定の確認 806
トラフィック ストーム制御カウンタのモニタリング 807
トラフィック ストーム制御の設定例 807
トラフィック ストーム制御に関する追加情報 807
トラフィック ストーム制御の機能履歴 808
ユニキャスト RPF の設定 809
機能情報の確認 809
ユニキャスト RPF の概要 810
ユニキャスト RPF プロセス 810
グローバル統計 811
ユニキャスト RPF のバーチャライゼーション サポート 812
ユニキャスト RPF のライセンス要件 812
ユニキャスト RPF の注意事項と制約事項 812
ユニキャスト RPF のデフォルト設定 813
ユニキャスト RPF の設定 813
ユニキャスト RPF の設定例 816
ユニキャスト RPF の設定の確認 816
ユニキャスト RPF に関する追加情報 817
ユニキャスト RPF の機能の履歴 817
コントロール プレーン ポリシングの設定 819
機能情報の確認 819
CoPP の概要 820
コントロール プレーン保護 821
コントロール プレーンのパケット タイプ 821
CoPP の分類 822
レート制御メカニズム 822
デフォルトのポリシング ポリシー 823
デフォルト クラス マップ 824
strict デフォルト CoPP ポリシー 831
moderate デフォルト CoPP ポリシー 833

lenient デフォルト CoPP ポリシー 834
デンス デフォルト CoPP ポリシー 835
1 秒間あたりのパケットのクレジット制限 836
モジュラ QoS コマンドライン インターフェイス 836
CoPP と管理インターフェイス 837
CoPP のバーチャライゼーション サポート 837
CoPP のライセンス要件 837
CoPP の注意事項と制約事項 837
CoPP のデフォルト設定 840
CoPP の設定 841
コントロール プレーン クラス マップの設定 841
コントロール プレーン ポリシー マップの設定 843
コントロール プレーン サービス ポリシーの設定 847
ラインカードごとの CoPP のスケール ファクタの設定 848
デフォルトの CoPP ポリシーの変更または再適用 851
CoPP ベスト プラクティス ポリシーのコピー 851
CoPP の設定の確認 852
CoPP 設定ステータスの表示 855
CoPP のモニタリング 856
SNMP での CoPP のモニタリング 857
CoPP 統計情報のクリア 857
CoPP の設定例 858
CoPP Configuration Example 858
ICMP ping と ARP 要求の分割による CoPP のオーバーフローの防止 859
セットアップ ユーティリティによるデフォルト CoPP ポリシーの変更または再適用 861
CoPP に関する追加情報 862
CoPP の機能の履歴 863
レート制限の設定 867
機能情報の確認 867
レート制限の概要 868
レート制限のバーチャライゼーション サポート 869
レート制限のライセンス要件 869

レート制限の注意事項と制約事項 **869**

レート制限のデフォルト設定 **870**

レート制限の設定 **871**

スーパーバイザに到達するパケットのレート制限の設定 **876**

レート制限のモニタリング **877**

レート制限統計情報のクリア **877**

レート制限の設定の確認 **878**

レート制限の設定例 **879**

レート制限に関する追加情報 **879**

レート制限の機能の履歴 **879**

はじめに

ここでは、次の項について説明します。

- 対象読者，xxxv ページ
- 表記法，xxxv ページ
- Cisco Nexus 7000 シリーズ NX-OS ソフトウェアの関連資料，xxxvii ページ
- マニュアルに関するフィードバック，xxxix ページ
- マニュアルの入手方法およびテクニカル サポート，xxxix ページ

対象読者

このマニュアルは、Cisco Nexus デバイスのコンフィギュレーションおよびメンテナンスを担当するネットワーク管理者を対象としています。

表記法

（注） お客様のニーズを満たすためにドキュメントを更新するという継続的な取り組みの一環として、シスコでは設定タスクの文書化方法を変更しました。そのため、本ドキュメントには、従来とは異なるスタイルでの設定タスクが説明されている部分もあります。ドキュメントに新たに組み込まれるようになったセクションには、以下のセクションが含まれます。

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。

表記法	説明
italic	イタリック体の文字は、ユーザが値を入力する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角カッコで囲んで示しています。
[x | y]	いずれか 1 つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。
{x | y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	角カッコまたは波カッコが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
`variable`	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。

例では、次の表記法を使用しています。

表記法	説明
`screen フォント`	スイッチが表示する端末セッションおよび情報は、screen フォントで示しています。
`太字の screen フォント`	ユーザが入力しなければならない情報は、太字の screen フォントで示しています。
イタリック体の *screen* フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコ（< >）で囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

このマニュアルでは、次の表記法を使用しています。

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

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

Cisco Nexus 7000 シリーズ NX-OS ソフトウェアの関連資料

Cisco Nexus 7000 シリーズ NX-OS 全体のマニュアル セットは、次の URL にあります。
http://www.cisco.com/en/us/products/ps9402/tsd_products_support_series_home.html

リリース ノート

リリース ノートは、次の URL から入手できます。
http://www.cisco.com/en/US/products/ps9402/prod_release_notes_list.html

コンフィギュレーション ガイド

これらのマニュアルは、次の URL から入手できます。
http://www.cisco.com/en/US/products/ps9402/products_installation_and_configuration_guides_list.html
このカテゴリのマニュアルには、次が含まれます。

- 『*Cisco Nexus 7000 Series NX-OS Configuration Examples*』
- 『*Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Fundamentals Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS IP SLAs Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS LISP Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS MPLS Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Multicast Routing Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS OTV Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide*』

- 『*Cisco Nexus 7000 Series NX-OS SAN Switching Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Security Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Verified Scalability Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Quick Start*』
- 『*Cisco Nexus 7000 Series NX-OS OTV Quick Start Guide*』
- 『*Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500*』
- 『*Cisco Nexus 2000 Series Fabric Extender Software Configuration Guide*』

コマンド リファレンス

これらのマニュアルは、次の URL から入手できます。

http://www.cisco.com/en/US/products/ps9402/prod_command_reference_list.html

このカテゴリのマニュアルには、次が含まれます。

- 『*Cisco Nexus 7000 Series NX-OS Command Reference Master Index*』
- 『*Cisco Nexus 7000 Series NX-OS FabricPath Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS Fundamentals Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS High Availability Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS Interfaces Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS LISP Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS MPLS Configuration Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Multicast Routing Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS OTV Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS Quality of Service Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS SAN Switching Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS System Management Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS Unicast Routing Command Reference*』
- 『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Command Reference*』

- 『*Cisco NX-OS FCoE Command Reference for Cisco Nexus 7000 and Cisco MDS 9500*』

その他のソフトウェアのマニュアル

これらのマニュアルは、以下のランディング ページから検索できます。

http://www.cisco.com/en/us/products/ps9402/tsd_products_support_series_home.html

- 『*Cisco Nexus 7000 Series NX-OS MIB Quick Reference*』
- 『*Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide*』
- 『*Cisco Nexus 7000 Series NX-OS Troubleshooting Guide*』
- 『*Cisco NX-OS Licensing Guide*』
- 『*Cisco NX-OS System Messages Reference*』
- 『*Cisco NX-OS XML Interface User Guide*』

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、HTML ドキュメント内のフィードバック フォームよりご連絡ください。ciscodfa-docfeedback@cisco.com。

ご協力をよろしくお願いいたします。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手、Cisco Bug Search Tool（BST）の使用、サービス要求の送信、追加情報の収集の詳細については、『What's New in Cisco Product Documentation』を参照してください。

新しく作成された、または改訂されたシスコのテクニカル コンテンツをお手元に直接送信するには、『What's New in Cisco Product Documentation』RSS フィードをご購読ください。RSS フィードは無料のサービスです。

第 1 章

新機能および変更された機能に関する情報

- 新機能および変更された機能に関する情報，1 ページ

新機能および変更された機能に関する情報

次の表に、このマニュアルの新機能および変更された機能を要約し、各機能がサポートされているリリースを示します。ご使用のソフトウェア リリースで、本書で説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。

表 *1*：新規および変更されたセキュリティ機能

機能	説明	変更されたリリース	参照先
M3 モジュールでの IP ACL の設定	M3 モジュールのサポートが導入されました。	7.3(0)DX(1)	IP ACL の設定，（549 ページ）
ユーザごとのログイン ブロック	ユーザごとのログイン ブロックのサポートが追加されました。	7.3(0)D1(1)	AAA の設定，（33 ページ）
SGACL ACLLOG	SGACL ロギングをイネーブルにする機能が追加されました。	7.3(0)D1(1)	Cisco TrustSec の設定
SGACL モニタリング	SGACL のモニタリングをイネーブルにする機能が追加されました。	7.3(0)D1(1)	Cisco TrustSec の設定
SXPv3	SGT 交換プロトコル バージョン 3 のサポートが追加されました。	7.3(0)D1(1)	Cisco TrustSec の設定

新機能および変更された機能に関する情報

機能	説明	変更されたリリース	参照先
Cisco TrustSec サブネットと SGT のマッピング	Cisco TrustSec サブネットと SGT のマッピングのサポートが追加されました。	7.3(0)D1(1)	Cisco TrustSec の設定
Lightweight DHCPv6 リレーエージェント	Lightweight DHCPv6 リレー エージェントのサポートが追加されました。	7.3(0)D1(1)	DHCP の設定，（677 ページ）
UDP リレー	UDP リレー機能のサポートが追加されました。	7.3(0)D1(1)	DHCP の設定，（677 ページ）
フレキシブル ACL TCAM バンク チェーニング	フレキシブル ACL TCAM バンク チェーニング機能のサポートが追加されました。	7.3(0)D1(1)	IP ACL の設定，（549 ページ）
F3 の FabricPath での Cisco TrustSec MACsec	F3 シリーズ モジュールの FabricPath での Cisco TrustSec MACsec のサポートが追加されました。	7.2(1)D1(1)	Cisco TrustSec の設定
SSH 接続のログイン猶予時間の設定	SSH 接続のログイン猶予時間を設定する機能が追加されました。	7.2(0)D1(1)	SSH および Telnet の設定，（197 ページ）
Cisco TrustSec	次の機能のサポートが追加されました。 • ポート チャネル メンバでの Cisco TrustSec サポート • 2,00,000 IP-SGT マップ • 『Change of Authorization』 • FabricPath での SGT は、F2E および F3 ライン カードでサポートされます。 • 従来のイーサネット モードの F3 ライン カードでの MACSec 機能 • ポートプロファイルによる SGT 分類 • 仮想ポート チャネル（vPC）および vPC+ への SGT サポート	7.2(0)D1(1)	Cisco TrustSec の設定
コントロールプレーン ポリシング	IP ユニキャスト RPF 障害パケットを分類およびレート制限する機能が追加されました。	6.2(10)	コントロールプレーン ポリシングの設定，（819 ページ）

機能	説明	変更されたリリース	参照先
ACL TCAM バンクマッピング	バンク マッピング マトリクスを表示するコマンドが追加されました。	6.2(10)	IP ACL の設定, （549 ページ）
Cisco TrustSec	F3 シリーズ モジュールに対して SGT サポートが追加されました。	6.2(10)	#unique_16
DHCP リレーの trusted インターフェイス	次のコマンドのサポートが追加されました • **ip dhcp relay information option trust** • **ip dhcp relay information trusted** • **ip dhcp relay information trust-all**	6.2(8)	DHCP の設定, （677 ページ）
Cisco TrustSec	MACSec が F2e モジュールを サポートできるようになりました。 SGACL プログラミング タスクをバッチするサポートが追加されました。	6.2(6)	Cisco TrustSec の設定
Cisco TrustSec	VLAN を SGT にマップする機能が追加されました。	6.2(2)	Cisco TrustSec の設定
Cisco TrustSec	SAP PMK を暗号化し、実行コンフィギュレーションに暗号化された形式で PMK を表示する機能が追加されました。	6.2(2)	Cisco TrustSec の設定
Cisco TrustSec	設定された PMK の 16 進値を表示するための **show cts sap pmk** コマンドが追加されました。	6.2(2)	Cisco TrustSec の設定
Cisco TrustSec	インターフェイスの Cisco TrustSec 機能を表示するための **show cts capability interface** コマンドが追加されました。	6.2(2)	Cisco TrustSec の設定
Cisco TrustSec	10 進値を受け入れるための、**cts sgt**、**policy static sgt**、および **clear cts policy sqt** コマンドがイネーブルになりました。	6.2(2)	Cisco TrustSec の設定
Cisco TrustSec	ISE から sgname テーブルをダウンロードし、環境データ タイマーが切れると環境データを手動で更新する機能が追加されました。	6.2(2)	Cisco TrustSec の設定

新機能および変更された機能に関する情報

機能	説明	変更されたリリース	参照先
Cisco TrustSec	特定の SXP ピア、VLAN、または VRF に対する SGT マッピングまたは SGT マップ設定のサマリーを表示するためのオプションのキーワードが **show cts role-based sgt-map** コマンドに追加されました。	6.2(2)	Cisco TrustSec の設定
Cisco TrustSec	すべての CTS 対応インターフェイスに関する概要を表示するための **brief** キーワードが **show cts interface** コマンドに追加されました。	6.2(2)	Cisco TrustSec の設定
Cisco TrustSec	F2e および F2 シリーズ モジュールに対する SGT サポートが追加されました。	6.2(2)	Cisco TrustSec の設定
CoPP	各モジュールの各ポリシーに関する 5 分間移動平均と一致および違反したバイトカウントのピーク値を表示するための **show policy-map interface control-plane** コマンドの出力が更新されました。	6.2(2)	Cisco TrustSec の設定
CoPP	VRRP IPv6 トラフィックをポリシングするための VRRP6 ACL サポートが追加されました。HSRP ACL は制御パケットの正しい宛先アドレスを反映するよう変更されます。	6.2(2)	コントロールプレーン ポリシングの設定, （819 ページ）
CoPP	マルチキャスト トラフィックの動作が、異なるクラスにおいて異なるレートでポリシングされることから、3 つのクラス（マルチキャスト ホスト、マルチキャスト ルータ、標準）にグループ化され、一定のレートでポリシングされるように変更されました。	6.2(2)	コントロールプレーン ポリシングの設定, （819 ページ）
CoPP	SNMP で CoPP をモニタする機能が追加されました。	6.2(2)	コントロールプレーン ポリシングの設定, （819 ページ）
DHCP	DHCPv6 リレー エージェントのサポートが追加されました。	6.2(2)	DHCP の設定, （677 ページ）

機能	説明	変更されたリリース	参照先
IP ACL	ACL TCAM バンク マッピングのサポートが追加されました。	6.2(2)	IP ACL の設定, （549 ページ）
IP ACL	ACL TCAM バンク マッピングのサポートが追加されました。	6.2(2)	IP ACL の設定, （549 ページ）
レート制限	レイヤ 3 収集高速パス パケットに対するサポートが追加されました。	6.2(2)	レート制限の設定, （867 ページ）
VLAN ACL	シーケンス中の拒否 ACE に対するサポートが追加されました。	6.1(3)	VLAN ACL の設定, （631 ページ）
Cisco TrustSec	Advanced Services ライセンスの要件を削除しました。	6.1(1)	Cisco TrustSec の設定
Cisco TrustSec	40G および 100G M2 シリーズ モジュールの MACsec のサポートが追加されました。	6.1(1)	Cisco TrustSec の設定
CoPP	FCoE に対する新しいクラスが追加されました。LISP、LISP6 および MAC レイヤ 3 IS-IS ACL が重要なクラスに追加されました。fcoe-fib-miss 一致例外が好ましくないクラスに追加されました。MAC レイヤ 2 トンネル ACL がレイヤ 2 非ポリシー クラスに追加されました。「permit icmp any any 143」ルールが acl-icmp6-msgs ACL に追加されました。	6.1(1)	コントロールプレーン ポリシングの設定, （819 ページ）
FIPS	スーパーバイザ2モジュールを含むスイッチのデジタルイメージ署名に対するサポートが追加されました。	6.1(1)	FIPS の設定, （23 ページ）
FIPS	M2 シリーズ モジュールに関する FIPS の注意事項が更新されました。	6.1(1)	FIPS の設定, （23 ページ）
IP ACL および MAC ACL	M2 シリーズ モジュールが更新されました。	6.1(1)	IP ACL の設定, （549 ページ） および MAC ACL の設定, （617 ページ）
Cisco TrustSec	F2 シリーズ モジュールが更新されました。	6.0(1)	Cisco TrustSec の設定

新機能および変更された機能に関する情報

機能	説明	変更されたリリース	参照先
CoPP	デンス デフォルト CoPP ポリシーが追加されました。	6.0(1)	コントロールプレーン ポリシングの設定, （819 ページ）
CoPP	ラインカードごとに CoPP のスケール ファクタを設定する機能が追加されました。	6.0(1)	コントロールプレーン ポリシングの設定, （819 ページ）
FIPS	F2 シリーズ モジュールに関する FIPS の注意事項が更新されました。	6.0(1)	FIPS の設定, （23 ページ）
IP ACL、MAC ACL、および VACL	F2 シリーズ モジュールが更新されました。	6.0(1)	IP ACL の設定, （549 ページ）、MAC ACL の設定, （617 ページ）、および VLAN ACL の設定, （631 ページ）
レート制限	F2 シリーズ モジュールのサポートが追加されました。	6.0(1)	レート制限の設定, （867 ページ）
RBAC	F2 シリーズ モジュールのサポートが追加されました。	6.0(1)	ユーザアカウントおよび RBAC の設定, （283 ページ）
TACACS+	コンソール セッションのコマンド許可を設定する機能が追加されました。	6.0(1)	TACACS+ の設定, （113 ページ）
ユーザアカウントおよび RBAC	SNMP OID に読み取り専用ルールまたは読み取り/書き込みルールを設定する機能が追加されました。	6.0(1)	ユーザアカウントおよび RBAC の設定, （283 ページ）
ACL と CoPP	実行コンフィギュレーションとスタートアップ コンフィギュレーションでユーザ設定 ACL だけを表示する（およびデフォルトの CoPP 設定 ACL を表示しない）ように、**show running-config aclmgr** コマンドと **show startup-config aclmgr** コマンドが変更されました。	5.2(1)	IP ACL の設定, （549 ページ）、MAC ACL の設定, （617 ページ）、VLAN ACL の設定, （631 ページ）、およびコントロールプレーン ポリシングの設定, （819 ページ）

機能	説明	変更されたリリース	参照先
Cisco TrustSec	インターフェイスでのポーズ フレームの暗号化と復号化のサポートが追加されました。	5.2(1)	Cisco TrustSec の設定
CoPP	設定ユーティリティを再度実行しないでデフォルト CoPP ポリシーを変更または再適用する機能が追加されました。	5.2(1)	コントロールプレーン ポリシングの設定, （819 ページ）
CoPP	CoPP ベスト プラクティス ポリシーを読み取り専用に変更し、ポリシーを修正するためにコピーする機能が追加されました。	5.2(1)	コントロールプレーン ポリシングの設定, （819 ページ）
CoPP	CoPP ベスト プラクティス ポリシーの詳細を表示する **show copp profile** コマンドと、ポリシー間の違いを表示する **show copp diff profile** コマンドが追加されました。	5.2(1)	コントロールプレーン ポリシングの設定, （819 ページ）
CoPP	**show copp status** コマンドが変更され、CoPP ベスト プラクティス ポリシーのどの部分がコントロール プレーンにアタッチされているかを表示するようになりました。	5.2(1)	コントロールプレーン ポリシングの設定, （819 ページ）
CoPP	セットアップ ユーティリティで、ベスト プラクティス CoPP プロファイルの **none** オプションの名前が **skip** に変更されました。	5.2(1)	コントロールプレーン ポリシングの設定, （819 ページ）
CoPP	デフォルトのクラス マップが更新され、MPLS LDP、MPLS OAM、MPLS RSVP、DHCP リレー、および OTV-AS のサポートが含まれました。	5.2(1)	コントロールプレーン ポリシングの設定, （819 ページ）
DHCP	DHCP リレー エージェントに対するサブネットのブロードキャストのサポートと、DHCP スマート リレーのサポートが追加されました。	5.2(1)	DHCP の設定, （677 ページ）
FCoE ACL	F1 シリーズ モジュールに FCoE ACL のサポートが追加されました。	5.2(1)	IP ACL の設定, （549 ページ）

新機能および変更された機能に関する情報

機能	説明	変更されたリリース	参照先
IP ACL	M1 シリーズモジュールに ACL キャプチャのサポートが追加されました。	5.2(1)	IP ACL の設定，（549 ページ）
LDAP	**ldap-server port** コマンドが非推奨になりました。	5.2(1)	LDAP の設定，（167 ページ）
パスワードの暗号化	AES パスワード暗号化と設定可能なマスター暗号キーのサポートが追加されました。	5.2(1)	パスワード暗号化の設定，（779 ページ）
RADIUS	RADIUS サーバ キーのタイプ 6 暗号化のサポートが追加されました。	5.2(1)	RADIUS の設定，（75 ページ）
TACACS+	TACACS+ サーバ キーのタイプ 6 暗号化のサポートが追加されました。	5.2(1)	TACACS+ の設定，（113 ページ）
コントロールプレーン ポリシー マップ	ドロップされるパケットのしきい値を指定し、設定したしきい値をドロップ数が超えた場合に syslog を生成する機能が追加されました。	5.1(1)	コントロールプレーン ポリシングの設定，（819 ページ）
CoPP	デフォルトのポリシーが更新され、802.1Q サービス クラス（cos）の値が含まれました。	5.1(1)	コントロールプレーン ポリシングの設定，（819 ページ）
CoPP	非 IP トラフィック クラスのサポートが追加されました。	5.1(1)	コントロールプレーン ポリシングの設定，（819 ページ）
DHCP スヌーピング	vPC 環境で動作する最適化 DHCP スヌーピング。	5.1(1)	DHCP の設定，（677 ページ）
FIPS	連邦情報処理標準（FIPS）モードを設定する機能が追加されました。	5.1(1)	FIPS の設定，（23 ページ）
レート制限	F1 シリーズモジュールパケットのサポートが追加されました。	5.1(1)	レート制限の設定，（867 ページ）
レート制限	スーパーバイザ モジュールに到達するパケットのレート制限を設定し、レート制限を超えた場合にシステム メッセージを記録する機能が追加されました。	5.1(1)	レート制限の設定，（867 ページ）

機能	説明	変更されたリリース	参照先
レート制限	レート制限をディセーブルにしたり、特定のモジュールおよびポート範囲のレート制限を設定したりするためのオプションが追加されました。	5.1(1)	レート制限の設定, （867 ページ）
SCP および SFTP サーバ	リモート デバイスとの間でのファイルのコピーをサポートするために、Cisco NX-OS デバイスで SCP サーバおよび SFTP サーバを設定する機能が追加されました。	5.1(1)	SSH および Telnet の設定, （197 ページ）
ユーザ ロール	network-admin ロールおよび network-operator ロールが使用できるコマンドの構文を表示する機能が追加されました。	5.1(1)	ユーザアカウントおよび RBAC の設定, （283 ページ）
VTY ACL	VTY 回線で受信したトラフィックに対するアクセス コントロールのサポートが追加されました。	5.1(1)	IP ACL の設定, （549 ページ）
802.1X	ポート チャネルのメンバ ポートで 802.1X の設定をサポートします。	5.0(2)	802.1X の設定, （315 ページ）
AAA 許可	TACACS+ サーバ用のデフォルトの AAA 許可方法の設定をサポートします。	5.0(2)	TACACS+ の設定, （113 ページ）
CHAP 認証	CHAP認証のイネーブル化またはディセーブル化を許可します。	5.0(2)	AAA の設定, （33 ページ）
CoPP	デフォルトのポリシーが更新され、ACL HSRP6 のサポートが含まれました。	5.0(2)	コントロールプレーン ポリシングの設定, （819 ページ）
DHCP	DHCP リレー エージェントの VRF へのサポートを許可します。また、**ip dhcp relay information option vpn** コマンドが追加され、**ip dhcp relay address** コマンドが変更されました。	5.0(2)	DHCP の設定, （677 ページ）

新機能および変更された機能に関する情報

機能	説明	変更されたリリース	参照先
DHCP	リンク選択、サーバ ID オーバーライド、および VRF 名/VPN ID リレー エージェントの Option 82 サブオプション用のシスコ独自の番号である 150、152、および 151 の DHCP での使用をサポートします。	5.0(2)	DHCP の設定, （677 ページ）
IP ACL、MAC ACL、および VACL	スケーラブルなサービス ライセンスがインストールされており、XL ラインカードを使用している場合、最大 128K の ACL エントリを許可します。	5.0(2)	IP ACL の設定, （549 ページ）、MAC ACL の設定, （617 ページ）、および VLAN ACL の設定, （631 ページ）
LDAP	Lightweight Directory Access Protocol（LDAP）の設定をサポートします。	5.0(2)	LDAP の設定, （167 ページ）
ローカル認証	リモート認証が失敗したときに、ローカル認証へのフォールバックをイネーブルにします。	5.0(2)	AAA の設定, （33 ページ）
ローカル認証	ローカル認証へのフォールバックのディセーブル化を許可します。	5.0(2)	AAA の設定, （33 ページ）
OTP	ワンタイムパスワードをサポートします。	5.0(2)	RADIUS の設定, （75 ページ）
定期サーバモニタリング	グローバルな RADIUS サーバと TACACS+ サーバの定期モニタリングをサポートします。	5.0(2)	RADIUS の設定, （75 ページ） および TACACS+ の設定, （113 ページ）
PKI	リモートの cert-store と証明書マッピングのフィルタをサポートします。	5.0(2)	PKI の設定, （225 ページ）
権限ロール	権限ロールのユーザ コマンドを許可または拒否できます。	5.0(2)	TACACS+ の設定, （113 ページ）
レート制限	レイヤ 2 トンネル プロトコル（L2TP）パケットをサポートします。	5.0(2)	レート制限の設定, （867 ページ）
SGACL ポリシー	RBACL ロギングのイネーブル化またはディセーブル化を許可します。	5.0(2)	Cisco TrustSec の設定

機能	説明	変更されたリリース	参照先
SGACL ポリシー	RBACL 統計情報のイネーブル化、ディセーブル化、モニタリング、およびクリアを許可します。	5.0(2)	Cisco TrustSec の設定
SSH	SSH ログインの最大試行回数の設定をサポートします。	5.0(2)	SSH および Telnet の設定, （197 ページ）
SSH	リモート デバイスに接続するために、Cisco NX-OS デバイスのブート モードからの SSH セッションの開始をサポートします。	5.0(2)	SSH および Telnet の設定, （197 ページ）
SSH	パスワードなしで Cisco NX-OS デバイスから SCP サーバまたは SFTP サーバへのファイルのコピーをサポートします。	5.0(2)	SSH および Telnet の設定, （197 ページ）
TACACS+ の特権レベルの許可	Cisco NX-OS デバイスでローカルに設定されたユーザ ロールに対して、TACACS+ サーバでユーザ用に設定された特権レベルをマッピングできます。	5.0(2)	TACACS+ の設定, （113 ページ）

新機能および変更された機能に関する情報

第 2 章

概要

Cisco NX-OS ソフトウェアがサポートするセキュリティ機能を利用すると、ネットワークをパフォーマンスの劣化や障害から保護するだけでなく、故意に行われる攻撃や、善意のネットワーク ユーザの意図しない危険な間違いにより生ずるデータの紛失または毀損に対しても保護できます。

この章は、次の項で構成されています。

- Authentication, Authorization, and Accounting（認証、許可、およびアカウンティング）, 14 ページ
- RADIUS および TACACS+ セキュリティ プロトコル, 15 ページ
- LDAP, 15 ページ
- SSH および Telnet, 15 ページ
- PKI, 16 ページ
- ユーザ アカウントおよびユーザ ロール, 16 ページ
- 802.1X, 16 ページ
- NAC, 17 ページ
- Cisco TrustSec, 17 ページ
- IP ACL, 17 ページ
- MAC ACL, 18 ページ
- VACL, 18 ページ
- ポート セキュリティ, 18 ページ
- DHCP スヌーピング, 19 ページ
- ダイナミック ARP インスペクション, 19 ページ
- IP ソース ガード, 20 ページ
- パスワード暗号化, 20 ページ

- キーチェーン管理，20 ページ
- Unicast RPF，21 ページ
- トラフィック ストーム制御，21 ページ
- コントロール プレーン ポリシング，21 ページ
- レート制限，22 ページ

Authentication,Authorization,andAccounting（認証、許可、およびアカウンティング）

認証、許可、アカウンティング（AAA）は、3 つの独立したセキュリティ機能をまとめて一貫性のあるモジュラ形式で設定するためのアーキテクチャ フレームワークです。

認証

ログイン/パスワードダイアログ、チャレンジ/レスポンス、メッセージング サポート、および暗号化（選択したセキュリティ プロトコルに基づく）などによるユーザの識別方法を提供します。認証は、ユーザに対してネットワークとネットワーク サービスへのアクセスを許可する前に、ユーザの識別を行う方法です。AAA 認証を設定するには、まず認証方式の名前付きリストを定義し、そのリストを各種インターフェイスに適用します。

許可

ワンタイム許可またはサービスごとの許可、ユーザ単位のアカウント リストとプロファイル、ユーザ グループ サポート、および IP、IPX、ARA、Telnet のサポートなど、リモート アクセスの制御方法を提供します。
RADIUS や TACACS+ などのリモート セキュリティ サーバは、適切なユーザで該当する権利を定義した属性値（AV）のペアをアソシエートすることによって、ユーザに特定の権限を付与します。AAA 許可は、ユーザが何を実行する権限を与えられるかを表す一連の属性を組み立てることで機能します。これらの属性とデータベースに格納されているユーザの情報とが比較され、その結果が AAA に返されてユーザの実際の権限と制限事項が決定されます。

Accounting

ユーザ ID、開始時刻と終了時刻、実行コマンド（PPP など）、パケット数、バイト数といった、課金、監査、およびレポートに使用するセキュリティ サーバ情報の収集と送信を行う手段を提供します。アカウンティングを使用することで、ユーザがアクセスしているサービスや、ユーザが消費しているネットワーク リソース量を追跡できます。

（注） 認証は AAA と別個に設定することができます。ただし RADIUS または TACACS+ を使用する場合や、バックアップの認証方式を設定する場合は、AAA を設定する必要があります。

関連トピック

AAA の設定，（33 ページ）

RADIUS および TACACS+ セキュリティ プロトコル

AAA は、セキュリティ機能の管理にセキュリティ プロトコルを使用します。ルータまたはアクセス サーバがネットワーク アクセス サーバとして動作している場合は、ネットワーク アクセス サーバと RADIUS または TACACS+ セキュリティ サーバとの間の通信を確立する手段に、AAA が使用されます。

このマニュアルでは、次のセキュリティ サーバ プロトコルを設定する手順を説明します。

RADIUS

不正アクセスからネットワークを保護する分散型クライアント/サーバシステムです。RADIUS は AAA を使用して実装されます。シスコの実装では RADIUS クライアントは Cisco ルータ上で稼働します。認証要求は、すべてのユーザ認証情報とネットワーク サービス アクセス情報が格納されている中央の RADIUS サーバに送信されます。

TACACS+

ルータまたはネットワーク アクセス サーバにアクセスしようとするユーザの検証を集中的に行うセキュリティ アプリケーションです。TACACS+ は AAA を使用して実装されます。TACACS+ サービスは、通常 UNIX または Windows NT ワークステーション上で動作する TACACS+ デーモンのデータベースで管理されます。TACACS+ では、独立したモジュラ型の認証、許可、アカウンティング機能が提供されます。

関連トピック

RADIUS の設定，（75 ページ）
TACACS+ の設定，（113 ページ）

LDAP

Lightweight Directory Access Protocol（LDAP）は、Cisco NX-OS デバイスにアクセスしようとするユーザの検証を集中的に行います。LDAP では、1 台のアクセス コントロール サーバ（LDAP デーモン）で認証と認可を個別に提供できます。

関連トピック

LDAP の設定，（167 ページ）

SSH および Telnet

セキュア シェル（SSH）サーバを使用すると、SSH クライアントは Cisco NX-OS デバイスとの間でセキュアな暗号化された接続を確立できます。SSH は強化暗号化を使用して認証を行います。

Cisco NX-OS ソフトウェアの SSH サーバは、市販の一般的な SSH クライアントと相互運用ができます。

Cisco NX-OS ソフトウェアの SSH クライアントは、市販の一般的な SSH クライアントと相互運用ができます。

Telnet プロトコルは、ホストとの TCP/IP 接続を確立します。Telnet を使用すると、あるサイトのユーザが別のサイトのログインサーバと TCP 接続を確立し、キーストロークをデバイス間でやり取りできます。Telnet は、リモートデバイス アドレスとして IP アドレスまたはドメイン名のいずれかを受け入れます。

関連トピック

SSH および Telnet の設定, （197 ページ）

PKI

公開キー インフラストラクチャ（PKI）を使用すると、ネットワーク上で通信を安全に行うためのデジタル証明書をデバイスが入手して使用できるようになり、デジタル証明書に対応した SSH などのアプリケーションの管理性と拡張性も向上します。

関連トピック

PKI の設定, （225 ページ）

ユーザ アカウントおよびユーザ ロール

ユーザ アカウントの作成および管理を行い、Cisco NX-OS デバイス上で実行できる操作を制限するロールを割り当てることができます。ロールベース アクセス コントロール（RBAC）を使用すると、割り当てたロールにルールを定義して、ユーザが行える管理操作の権限を制限できます。

関連トピック

ユーザ アカウントおよび RBAC の設定, （283 ページ）

802.1X

802.1X では、クライアント サーバ ベースのアクセス コントロールと認証プロトコルを定義し、許可されていないクライアントが公にアクセス可能なポートを経由して LAN に接続するのを規制します。認証サーバは、Cisco NX-OS デバイスのポートに接続されるクライアントを個々に認証します。

802.1X アクセス コントロールでは、クライアントが認証されるまで、そのクライアントが接続しているポート経由では Extensible Authentication Protocol over LAN（EAPOL）トラフィックしか許可されません。認証に成功すると、通常のトラフィックはポートを通過できるようになります。

関連トピック

802.1X の設定, （315 ページ）

NAC

Network Admission Control（NAC）を使用すると、エンドポイント装置にネットワーク アクセスを許可する前に、エンドポイント装置のセキュリティ適合性と脆弱性をチェックできます。このセキュリティ適合性のチェックのことを、ポスチャ検証といいます。ポスチャ検証により、ワーム、ウイルス、およびその他の不正アプリケーションがネットワーク全体に拡散することを防止できます。

NACは、エンドポイント装置がネットワークの保護された領域にアクセス可能になる前に、エンドポイント装置のポスチャ（状態）がセキュリティ ポリシーに適合しているかどうかを検証します。セキュリティ ポリシーに適合する場合は、ネットワークの保護されたサービスにアクセスすることが許可されます。セキュリティ ポリシーに適合しない場合は、修復専用のネットワークにアクセスが制限されます。修復ネットワークではデバイスのポスチャが再度チェックされます。

関連トピック

NAC の設定, （361 ページ）

Cisco TrustSec

The Cisco TrustSec security architecture builds secure networks by establishing clouds of trusted network devices. Each device in the cloud is authenticated by its neighbors. Communication on the links between devices in the cloud is secured with a combination of encryption, message integrity checks, and replay protection mechanisms. Cisco TrustSec also uses the device and user identification information acquired during authentication for classifying, or coloring, the packets as they enter the network. This packet classification is maintained by tagging packets on ingress to the Cisco TrustSec network so that they can be properly identified for the purpose of applying security and other policy criteria along the data path. The tag, also called the security group tag (SGT), allows the network to enforce the access control policy by enabling the endpoint device to act upon the SGT to filter traffic. Cisco TrustSec uses ingress tagging and egress filtering to enforce access control policy in as a conversation.

関連トピック

Cisco TrustSec の設定

IP ACL

IP ACL は、トラフィックをパケットのレイヤ 3 ヘッダーの IPv4 情報に基づいてフィルタリングするために使用できるルールの順序セットです。各ルールには、パケットがルールに一致するために満たさなければならない条件のセットが規定されています。Cisco NX-OS ソフトウェアがパケットにIP ACL を適用することを判定するときは、すべてのルールの条件に照らしてパケットを調べます。最初の一致によってパケットを許可するか拒否するか判定します。一致するものがな

い場合は、Cisco NX-OS ソフトウェアは適切なデフォルト ルールを適用します。Cisco NX-OS ソフトウェアは、許可されたパケットの処理を継続し、拒否されたパケットをドロップします。

関連トピック

IP ACL の設定, （549 ページ）

MAC ACL

MAC ACL は各パケットのレイヤ 2 ヘッダーの情報を使用してトラフィックをフィルタリングする ACL です。各ルールには、パケットがルールに一致するために満たさなければならない条件のセットが規定されています。Cisco NX-OS ソフトウェアがパケットに MAC ACL を適用することを判定するときは、すべてのルールの条件に照らしてパケットを調べます。最初の一致によってパケットを許可するか拒否するか判定します。一致するものがない場合は、NX-OS ソフトウェアは適切なデフォルト ルールを適用します。Cisco NX-OS ソフトウェアは、許可されたパケットの処理を継続し、拒否されたパケットをドロップします。

関連トピック

MAC ACL の設定, （617 ページ）

VACL

VLAN ACL（VACL）は、IP ACL または MAC ACL の適用例の 1 つです。VACL を設定し、VLAN との間でルーティングされるかまたは VLAN 内でブリッジングされるすべてのパケットに適用できます。VACL は、セキュリティ パケット フィルタリングおよび特定の物理インターフェイスへのトラフィックのリダイレクトだけを目的としたものです。VACL は方向（入力または出力）で定義されることはありません。

関連トピック

VLAN ACL の設定, （631 ページ）

ポート セキュリティ

ポート セキュリティを使用すると、限定された MAC アドレス セットからのインバウンド トラフィックだけを許可するようなレイヤ 2 インターフェイスを設定できます。この限定セットの MAC アドレスをセキュア MAC アドレスといいます。さらに、デバイスは、同じ VLAN 内の別のインターフェイスでは、これらの MAC アドレスからのトラフィックを許可しません。セキュア MAC アドレスの数は、インターフェイス単位で設定します。

関連トピック

ポート セキュリティの設定, （645 ページ）

DHCP スヌーピング

DHCP スヌーピングは、信頼できないホストと信頼できる DHCP サーバとの間でファイアウォールのような機能を果たします。DHCP スヌーピングでは次のアクティビティを実行します。

- 信頼できない送信元からの DHCP メッセージを検証し、無効なメッセージをフィルタ処理して除外します。
- DHCP スヌーピング バインディング データベースを構築し、管理します。このデータベースには、リース IP アドレスがある信頼できないホストに関する情報が保存されています。
- DHCP スヌーピング バインディング データベースを使用して、信頼できないホストからの以降の要求を検証します。

ダイナミック ARP インスペクション（DAI）および IP ソース ガードも、DHCP スヌーピング バインディング データベースに格納された情報を使用します。

関連トピック

DHCP の設定，（677 ページ）

ダイナミック ARP インスペクション

ダイナミック ARP インスペクション（DAI）を使用することで、有効な ARP 要求と応答だけが中継されることを保証できます。DAI がイネーブルになり適切に設定されている場合、Cisco NX-OS デバイスは次のアクティビティを実行します。

- 信頼できないポートを経由したすべての ARP 要求および ARP 応答を代行受信します。
- 代行受信した各パケットが、IP アドレスと MAC アドレスの有効なバインディングを持つことを確認してから、ローカル ARP キャッシュを更新するか、または適切な宛先にパケットを転送します。
- 無効な ARP パケットはドロップします。

DAI は DHCP スヌーピング バインディング データベースに保存された有効な IP アドレスと MAC アドレスのバインディングに基づき、ARP パケットの有効性を判断できます。このデータベースは、VLAN とデバイス上で DHCP スヌーピングがイネーブルにされている場合に、DHCP スヌーピングによって構築されます。ARP パケットを信頼できるインターフェイス上で受信した場合は、デバイスはこのパケットを検査せずに転送します。信頼できないインターフェイス上では、デバイスは有効性を確認できたパケットだけを転送します。

関連トピック

ダイナミック ARP インスペクションの設定，（739 ページ）

IP ソース ガード

IP ソース ガードは、インターフェイス単位のトラフィック フィルタです。各パケットの IP アドレスと MAC アドレスが、IP と MAC のアドレス バインディングのうち、次に示す 2 つの送信元のどちらかと一致する場合だけ、IP トラフィックを許可します。

- DHCP スヌーピング バインディング テーブル内のエントリ
- 設定したスタティック IP ソース エントリ

信頼できる IP と MAC アドレス バインディングに基づいてフィルタリングするので、有効なホストの IP アドレスのスプーフィングを使用した攻撃の防止に役立ちます。IP ソース ガードを妨ぐためには、攻撃者は有効なホストの IP アドレスと MAC アドレスを両方スプーフィングする必要があります。

関連トピック

IP ソース ガードの設定，（771 ページ）

パスワード暗号化

高度暗号化規格（AES）パスワード暗号化機能では、サポートするアプリケーション（現在は RADIUS および TACACS+）のすべての既存および新規に作成されたクリア テキスト パスワードを、堅牢でリバーシブルのタイプ 6 暗号化形式で保存します。マスター暗号キーは、パスワードを暗号化および復号化するために使用されます。また、この機能を使用して、暗号化が脆弱な既存のすべてのパスワードをタイプ 6 暗号化パスワードに変換することもできます。

関連トピック

パスワード暗号化の設定，（779 ページ）

キーチェーン管理

キーチェーン管理を使用すると、キーチェーンの作成と管理を行えます。キーチェーンはキーのシーケンスを意味します（共有秘密ともいいます）。キーチェーンは、他のデバイスとの通信をキーベース認証を使用して保護する機能と合わせて使用できます。デバイスでは複数のキーチェーンを設定できます。

キーベース認証をサポートするルーティング プロトコルの中には、キーチェーンを使用してヒットレス キー ロールオーバーによる認証を実装できるものがあります。

関連トピック

キーチェーン管理の設定，（787 ページ）

Unicast RPF

ユニキャスト Reverse Path Forwarding（RPF）機能を使用すると、ネットワークに変形または偽造（スプーフィング）されたIPソースアドレスが注入されて引き起こされる問題を、裏付けのない IP ソース アドレスを廃棄する方法により緩和します。たとえば、Smurf や Tribal Flood Network（TFN）など、いくつかの一般的なサービス拒絶（DoS）攻撃では、偽造の送信元 IP アドレスやすぐに変更される送信元IPアドレスを利用して、攻撃を突き止めたりフィルタリングしたりする手段を防ぎます。ユニキャスト RPF では、送信元アドレスが有効で IP ルーティング テーブルと一致するパケットだけを転送することにより、攻撃を回避します。

関連トピック

ユニキャスト RPF の設定，（809 ページ）

トラフィック ストーム制御

トラフィック ストーム制御（トラフィック抑制ともいいます）を使用すると、着信トラフィックのレベルを 1 秒より大きなインターバルでモニタできます。この間、トラフィック レベル（ポートの使用可能合計帯域幅に対するパーセンテージ）が、設定したトラフィック ストーム制御レベルと比較されます。入力トラフィックが、ポートに設定したトラフィック ストーム制御レベルに到達すると、トラフィック ストーム制御機能によってそのインターバルが終了するまでトラフィックがドロップされます。

関連トピック

トラフィック ストーム制御の設定，（801 ページ）

コントロール プレーン ポリシング

Cisco NX-OS デバイスは、サービス拒絶（DoS）攻撃によるパフォーマンスへの影響を防ぐために、コントロール プレーン ポリシングを備えています。Cisco NX-OS デバイスのスーパーバイザ モジュールには、マネージメント プレーンとコントロール プレーンの両方が搭載され、ネットワークの運用にクリティカルなモジュールです。スーパーバイザ モジュールの動作が途絶するような場合には、重大なネットワークの停止につながります。スーパーバイザに過剰なトラフィックが加わると、スーパーバイザ モジュールが過負荷になり、Cisco NX-OS デバイス全体のパフォーマンスが低下する可能性があります。スーパーバイザ モジュールへの攻撃には、DoS 攻撃のようにコントロール プレーンを流れる IP トラフィック ストリームが非常に高いレートで発生するものなど、さまざまな種類があります。攻撃によってコントロール プレーンはこれらのパケットの処理に大量の時間を費やしてしまい、本来のトラフィック処理が不可能になります。

関連トピック

コントロール プレーン ポリシングの設定，（819 ページ）

レート制限

レート制限を行うことで、出力例外のリダイレクト パケットにより Cisco NX-OS デバイス上のスーパーバイザ モジュールに過剰な負荷がかかるのを回避できます。

関連トピック

レート制限の設定, （867 ページ）

第 3 章

FIPS の設定

この章では、Cisco NX-OS デバイスで連邦情報処理標準（FIPS）モードを設定する方法について説明します。

この章は、次の項で構成されています。

- 機能情報の確認，23 ページ
- FIPS の概要，24 ページ
- FIPS のライセンス要件，26 ページ
- FIPS の前提条件，26 ページ
- FIPS の注意事項と制約事項，27 ページ
- FIPS のデフォルト設定，27 ページ
- FIPS の設定，27 ページ
- FIPS の設定の確認，30 ページ
- FIPS の設定例，30 ページ
- FIPS に関する追加情報，31 ページ
- FIPS の機能の履歴，31 ページ

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

FIPS の概要

FIPS 140-2 の刊行物『*Security Requirements for Cryptographic Modules*』には、暗号モジュールに対する米国政府の要件が詳細に記載されています。FIPS 140-2 では、暗号モジュールがハードウェア、ソフトウェア、ファームウェア、または何らかの組み合わせのセットで、暗号機能またはプロセスを実装し、暗号化アルゴリズムおよび任意のキー生成機能を含み、明確に定義された暗号境界の内部に位置しなければならないと定義しています。

FIPS は特定の暗号化アルゴリズムがセキュアであることを条件とするほか、ある暗号モジュールが FIPS 準拠であると称する場合は、どのアルゴリズムを使用すべきかを指定しています。

FIPS のセルフテスト

暗号モジュールは、自身の正常な動作を保証するために、電源投入時セルフテストと条件付きセルフテストを実行する必要があります。

電源投入時セルフテストは、デバイスの電源が投入された後に自動的に実行されます。デバイスがFIPSモードになるのは、すべてのセルフテストが正常に完了した後だけです。いずれかのセルフテストが失敗すると、デバイスはシステム メッセージをログに記録し、エラー状態に移行します。

デバイスは、既知解テスト（KAT）という暗号化アルゴリズムを使用して、デバイス上に実装されている FIPS 140-2 で承認された暗号機能（暗号化、復号化、認証、および乱数生成）ごとに FIPS モードをテストします。デバイスは、このアルゴリズムを、すでに正しい出力がわかっているデータに対して適用します。次に、計算された出力を、以前に生成された出力と比較します。計算された出力が既知解に等しくない場合は、KAT が失敗します。

適用可能なセキュリティ機能または操作が呼び出された場合は、条件付きセルフテストが自動的に実行されます。電源投入時セルフテストとは異なって、条件付きセルフテストはそれぞれに関連する機能がアクセスされるたびに実行されます。

条件付きセルフテストでは次を含むテストが行われます。

ペアワイズ一貫性テスト

このテストは、公開キーまたは秘密キーのペアが生成されたときに実行されます。

連続乱数ジェネレータ テスト

このテストは、乱数が生成されたときに実行されます。

また、Cisco TrustSec マネージャは、暗号化されたテキストが決してプレーン テキストとして送信されないようにするためにバイパス テストを実行します。

（注） CTS に対応したポート上でバイパス テストが失敗すると、それらの対応するポートのみがシャットダウンされます。バイパス テストは、データ パスの輻輳によって発生したパケットドロップのために失敗することがあります。このような場合は、そのポートを再び立ち上げてみることを推奨します。

FIPS エラー状態

システムがFIPSモードで起動されると、スーパーバイザおよびラインカードモジュール上でFIPS電源投入時セルフテストが実行されます。これらの起動テストのいずれかが失敗すると、システム全体が FIPS エラー状態に移行されます。この状態では、FIPS の要件に従って、すべての暗号キーが削除され、すべてのラインカードがシャットダウンされます。このモードは、デバッグのみを目的にしています。

スイッチがFIPSエラー状態になった後、ラインカードをリロードすると常に、そのラインカードが障害状態に移行されます。スイッチをFIPSモードに戻すには、再起動する必要があります。ただし、スイッチがFIPSモードになった後、ラインカードのそれ以降のリロードまたは挿入で電源投入時セルフテストが失敗すると常に、そのラインカードにのみ影響を与え、対応するラインカードのみが障害状態に移行されます。

RADIUS キーラップ

RADIUS キーラップのサポートは RADIUS プロトコルの拡張機能です。RADIUS メッセージを認証し、セッション キーを配布する Cisco Access Control Server（ACS）のための FIPS 認定機能が用意されています。

RADIUS キーラップでは、キーを転送するための Advanced Encryption Standard（AES）キーラップアルゴリズムを使用して RADIUS プロトコルのセキュリティを向上させます。またパケットの完全性を保護するために HMAC-SHA1 アルゴリズムを使用しています。ここでは、Key Encryption Key（KEK）とハッシュ キーは互いに異なる必要があり、パスワードに基づいてはならず、応答のオーセンティケータの計算で使用する RADIUS 共有秘密から暗号について無関係である必要があると指定されています。

（注） プロキシおよびメッセージのオーセンティケータは、RADIUSキーラップではサポートされていません。

FIPS モードをイネーブルにすると、RADIUS キーラップは自動的にイネーブルになります。その結果、キーラップ属性が EAP 属性を含む RADIUS 要求に追加されますが、これは Protected Access Credential（PAC）のプロビジョニングのためではありません。属性は Cisco ACS に送信され、ここで EAP-TLS セッション キーが IEEE 802.1X EAP オーセンティケータに配信されます。セッション キーは AES を使用して暗号化され、RADIUS メッセージは HMAC-SHA-1 を使用して認証されます。

（注） Cisco ACS Release 5.2 では、RADIUS キーラップ機能をサポートしています。

関連トピック

RADIUS の設定, （75 ページ）

FIPS の仮想化サポート

FIPS モードの設定と、FIPS のセルフテストの実行は、デフォルトの仮想デバイス コンテキスト（VDC）でのみ行えます。VDC の詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

FIPS のライセンス要件

次の表に、FIPS のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	FIPS にはライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

FIPS の前提条件

FIPS には、次の前提条件があります。

- Telnet をディセーブルにします。ユーザのログインはセキュア シェル（SSH）だけで行ってください。
- SNMP v1 および v2 をディセーブルにしてください。SNMP v3 に対して設定された、デバイス上の既存ユーザ アカウントのいずれについても、認証およびプライバシー用 AES/3DES は SHA で設定されていなければなりません。
- SSH サーバの RSA1 キー ペアすべてを削除してください。
- Cisco TrustSec セキュリティ アソシエーション プロトコル（SAP）ネゴシエーション中に使用する HMAC-SHA1 メッセージ整合性チェック（MIC）をイネーブルにします。そのためには、cts-manual または cts-dot1x モードで **sap hash-algorithm HMAC-SHA-1** コマンドを入力し

ます。このコマンドはF1シリーズまたはF2シリーズモジュールではサポートされていないことに注意してください。

FIPS の注意事項と制約事項

FIPS 設定時の注意事項と制約事項は次のとおりです。

- RADIUS の keywrap 機能は、Cisco ACS Release 5.2 以降のリリースでのみ動作します。
- SSH でサポートされているユーザ認証メカニズムは、ユーザ名とパスワード、公開キー、および X.509 証明書です。
- パスワードは、最小 8 文字の英数字である必要があります。
- F1 シリーズおよび F2 シリーズ モジュールでは、FIPS モードはサポートされません。ただし、FIPS モードで動作している Cisco NX-OS デバイス内に F1 シリーズまたは F2 シリーズ モジュールを導入できます。
- F1 シリーズおよび F2 シリーズ モジュールでは、cts-dot1x モードまたは cts-manual モードはサポートされません。
- デジタル イメージ署名はスーパーバイザ 2 モジュールを含む Cisco Nexus 7000 シリーズ スイッチでサポートされます。
- M2 シリーズ モジュールは FIPS モードをサポートしません。ただし、FIPS モードで動作している Cisco NX-OS デバイス内に M2 シリーズ モジュールを導入できます。

FIPS のデフォルト設定

次の表に、FIPS パラメータのデフォルト設定を示します。

表 *2* : **デフォルトの *FIPS* パラメータ**

パラメータ	デフォルト
FIPS モード	ディセーブル

FIPS の設定

ここでは、Cisco NX-OS デバイスで FIPS モードを設定する方法について説明します。

FIPS モードのイネーブル化

Cisco NX-OS Release 5.1 以降では、デバイスの FIPS モードをイネーブルにできます。

はじめる前に

デフォルト VDC にいることを確認します。

手順の概要

1. **configure terminal**
2. **fips mode enable**
3. **exit**
4. （任意） **show fips status**
5. **copy running-config startup-config**
6. **reload**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**fips mode enable** 例： `switch(config)# fips mode enable`	FIPS モードをイネーブルにします。 （注） **fips mode enable** はすべての LC がオンラインのときにのみ入力できます。LC がオンラインでないときに入力すると、LC で障害が発生します。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show fips status**
	
	例：
	`switch# show fips status`
	`FIPS mode is enabled`
		（任意）
		FIPS モードのステータスを表示します。

ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

	コマンドまたはアクション	目的
ステップ 6	**reload** 例： `switch# reload`	Cisco NX-OS デバイスをリロードします。 （注） FIPS をイネーブルにすると、システムが FIPS モードで動作するためにリブートが必要です。

関連トピック

FIPS モードのディセーブル化, （29 ページ）

FIPS モードのディセーブル化

デバイスの FIPS モードをディセーブルにできます。

はじめる前に

デフォルト VDC にいることを確認します。

手順の概要

1. **configure terminal**
2. **no fips mode enable**
3. **exit**
4. （任意） **show fips status**
5. **copy running-config startup-config**
6. **reload**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**no fips mode enable** 例： `switch(config)# no fips mode enable`	FIPS モードをディセーブルにします。

	コマンドまたはアクション	目的

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show fips status**
	
	例：
	`switch# show fips status`
	`FIPS mode is disabled`
		（任意）
		FIPS モードのステータスを表示します。

ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。
ステップ 6	**reload** 例： `switch# reload`	Cisco NX-OS デバイスをリロードします。

関連トピック

FIPS モードのイネーブル化, （28 ページ）

FIPS の設定の確認

FIPS 設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show fips status	FIPS 機能のステータスを表示します。

このコマンドの出力フィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

FIPS の設定例

FIPS モードをイネーブルにする例を示します。

```
config terminal
fips mode enable
show fips status
```

```
exit
copy running-config startup-config
reload
```

FIPS に関する追加情報

ここでは、FIPS の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS のライセンス	『*Cisco NX-OS Licensing Guide*』
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』
VDC コンフィギュレーション	『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』

標準

標準	タイトル
FIPS 140-2	暗号モジュールのセキュリティ要件

FIPS の機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 *3* : *FIPS* の機能の履歴

機能名	リリース	機能情報
FIPS	6.1(1)	スーパーバイザ2モジュールを含むスイッチのデジタル イメージ署名に対するサポートが追加されました。
FIPS	6.1(1)	M2 シリーズモジュールに関する FIPS の注意事項が更新されました。

機能名	リリース	機能情報
FIPS	6.0(1)	F2 シリーズ モジュールに関する FIPS の注意事項が更新されました。
FIPS	5.1(1)	この機能が導入されました。

第 4 章

AAA の設定

この章では、Cisco NX-OS デバイスで認証、許可、アカウンティング（AAA）を設定する手順について説明します。

この章は、次の項で構成されています。

- 機能情報の確認，33 ページ
- AAA の概要，34 ページ
- AAA のライセンス要件，40 ページ
- AAA の前提条件，40 ページ
- AAA の注意事項と制約事項，41 ページ
- AAA のデフォルト設定，41 ページ
- AAA の設定，41 ページ
- ローカル AAA アカウンティング ログのモニタリングとクリア，70 ページ
- AAA 設定の確認，71 ページ
- AAA の設定例，72 ページ
- AAA に関する追加情報，72 ページ
- AAA の機能の履歴，73 ページ

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

AAA の概要

ここでは、Cisco NX-OS デバイスでの AAA について説明します。

AAA セキュリティ サービス

AAA 機能を使用すると、Cisco NX-OS デバイスを管理するユーザの ID を確認し、ユーザにアクセスを許可し、ユーザの実行するアクションを追跡できます。Cisco NX-OS デバイスは、Remote Access Dial-In User Service（RADIUS）プロトコルまたは Terminal Access Controller Access Control System Plus（TACACS+）プロトコルをサポートします。

Cisco NX-OS は入力されたユーザ ID およびパスワードの組み合わせに基づいて、ローカル データベースによるローカル認証または許可、あるいは 1 つまたは複数の AAA サーバによるリモート認証または許可を実行します。Cisco NX-OS デバイスと AAA サーバの間の通信は、事前共有秘密キーによって保護されます。すべての AAA サーバ用または特定の AAA サーバ専用に共通秘密キーを設定できます。

AAA セキュリティは、次のサービスを実行します。

認証

ログインとパスワードのダイアログ、チャレンジとレスポンス、メッセージング サポート、および選択したセキュリティ プロトコルに応じた暗号化などを使用してユーザを識別します。

認証は、デバイスにアクセスする人物またはデバイスの ID を確認するプロセスです。この ID の確認は、Cisco NX-OS デバイスにアクセスするエンティティから提供されるユーザ ID とパスワードの組み合わせに基づいて行われます。Cisco NX-OS デバイスでは、ローカル認証（ローカル ルックアップ データベースを使用）またはリモート認証（1 台または複数の RADIUS サーバまたは TACACS+ サーバを使用）を実行できます。

許可

アクセス コントロールを提供します。AAA 許可は、ユーザが何を実行する権限を与えられるかを表す一連の属性を組み立てるプロセスです。Cisco NX-OS ソフトウェアでは、AAA サーバからダウンロードされる属性を使用して権限付与が行われます。RADIUS や TACACS+ などのリモート セキュリティ サーバは、適切なユーザで該当する権利を定義した属性値（AV）のペアをアソシエートすることによって、ユーザに特定の権限を付与します。

Accounting

情報を収集する、情報をローカルのログに記録する、情報を AAA サーバに送信して課金、監査、レポート作成などを行う方法を提供します。

アカウンティング機能では、Cisco NX-OS デバイスへのアクセスに使用されるすべての管理セッションを追跡し、ログに記録して管理します。この情報を使用して、トラブルシューティングや監査のためのレポートを生成できます。アカウンティング ログは、ローカルに保存することもできれば、リモート AAA サーバに送信することもできます。

（注） Cisco NX-OS ソフトウェアでは、認証、許可、およびアカウンティングを個別にサポートしています。たとえば、アカウンティングは設定せずに、認証と許可を設定したりできます。

AAA を使用する利点

AAA は、次のような利点を提供します。

- アクセス設定の柔軟性と制御性の向上
- 拡張性
- 標準化された認証方式（RADIUS、TACACS+ など）
- 複数のバックアップ デバイス

リモート AAA サービス

RADIUS プロトコルおよび TACACS+ プロトコルを介して提供されるリモート AAA サービスには、ローカル AAA サービスと比べて次のような利点があります。

- ファブリック内の各 Cisco NX-OS デバイスのユーザ パスワード リストの管理が容易になります。
- AAA サーバはすでに企業内に幅広く導入されており、簡単に AAA サービスに使用できます。
- ファブリック内のすべての Cisco NX-OS デバイスのアカウンティング ログを中央で管理できます。
- ファブリック内の各 Cisco NX-OS デバイスのユーザ属性の管理が、Cisco NX-OS デバイスのローカル データベースを使用するよりも容易になります。

AAA サーバ グループ

認証、許可、アカウンティングのためのリモート AAA サーバは、サーバ グループを使用して指定できます。サーバ グループとは、同じ AAA プロトコルを実装した一連のリモート AAA サーバです。サーバ グループの目的は、リモート AAA サーバが応答できなくなったときにフェールオーバー サーバを提供することです。グループ内の最初のリモート サーバが応答しなかった場合、いずれかのサーバが応答を送信するまで、グループ内の次のリモート サーバで試行が行われます。サーバ グループ内のすべての AAA サーバが応答しなかった場合、そのサーバ グループ オプションは障害が発生しているものと見なされます。必要に応じて、複数のサーバ グループを指定できます。Cisco NX-OS デバイスは、最初のサーバ グループのすべてのサーバからエラーを受信した場合に、次のサーバ グループのサーバを試行します。

AAA サービス設定オプション

Cisco NX-OS デバイスの AAA 設定は、サービス ベースです。次のサービスごとに異なった AAA 設定を作成できます。

- User Telnet または Secure Shell（SSH）ログイン認証
- コンソール ログイン認証
- Cisco TrustSec 認証
- 802.1X 認証
- Network Admission Control（NAC）の Extensible Authentication Protocol over User Datagram Protocol（EAPoUDP）認証
- ユーザ管理セッション アカウンティング
- 802.1X アカウンティング

次の表に、AAA サービス設定オプションごとに CLI（コマンドライン インターフェイス）の関連コマンドを示します。

表 *4* : *AAA* サービス コンフィギュレーション コマンド

AAA サービス コンフィギュレーション オプション	関連コマンド
Telnet または SSH ログイン	**aaa authentication login default**
コンソール ログイン	**aaa authentication login console**
Cisco TrustSec 認証	**aaa authentication cts default**
802.1X 認証	**aaa authentication dot1x default**
EAPoUDP 認証	**aaa authentication eou default**
ユーザ セッション アカウンティング	**aaa accounting default**
802.1X アカウンティング	**aaa accounting dot1x default**

AAA サービスには、次の認証方式を指定できます。

すべての RADIUS サーバ

RADIUS サーバのグローバル プールを使用して認証を行います。

指定サーバ グループ

設定した特定の RADIUS、TACACS+、または LDAP サーバ グループを使用して認証を行います。

ローカル

ローカルのユーザ名またはパスワード データベースを使用して認証を行います。

なし

AAA 認証が使用されないように指定します。

（注） 「指定サーバ グループ」方式でなく、「すべての RADIUS サーバ」方式を指定した場合、Cisco NX-OS デバイスは、設定された RADIUS サーバのグローバル プールから設定の順に RADIUS サーバを選択します。このグローバル プールから選択されるサーバは、Cisco NX-OS デバイス上で RADIUS サーバ グループに選択的に設定できるサーバです。

次の表に、AAA サービスに対応して設定できる AAA 認証方式を示します。

表 *5*：*AAA* サービスの *AAA* 認証方式

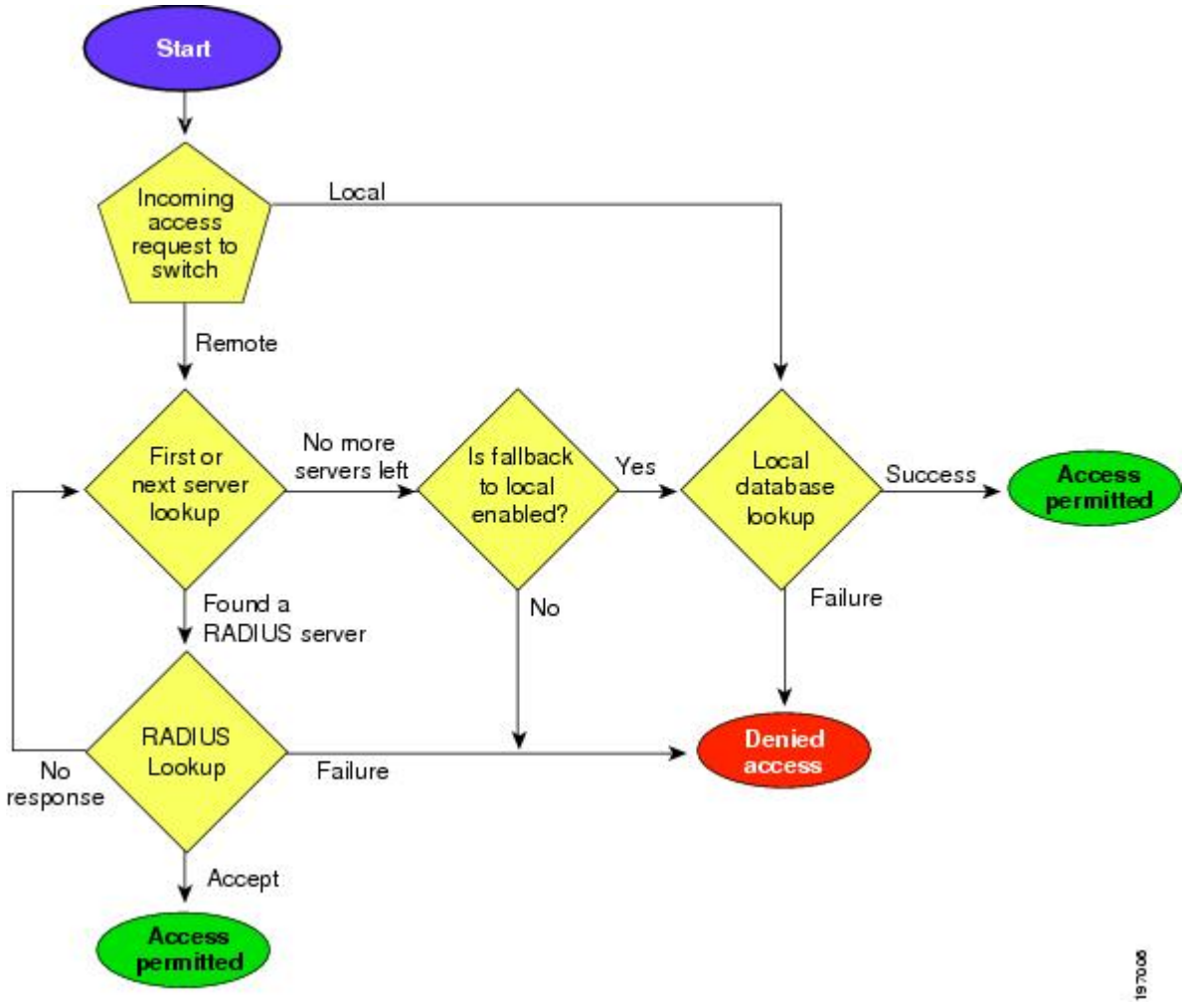
AAA サービス	AAA の方式
コンソール ログイン認証	サーバ グループ、ローカル、なし
ユーザ ログイン認証	サーバ グループ、ローカル、なし
Cisco TrustSec 認証	サーバ グループのみ
802.1X 認証	サーバ グループのみ
EAPoUDP 認証	サーバ グループのみ
ユーザ管理セッション アカウンティング	サーバ グループ、ローカル
802.1X アカウンティング	サーバ グループ、ローカル

（注） コンソール ログイン認証、ユーザ ログイン認証、およびユーザ管理セッション アカウンティングの場合は、Cisco NX-OS デバイスが、指定された順序で各オプションを試行します。その他の設定済みオプションが失敗した場合、ローカル オプションがデフォルト方式です。**no aaa authentication login** {**console** | **default**} **fallback error local** コマンドを使用すると、コンソール ログインまたはデフォルト ログインの local オプションをディセーブルにできます。

ユーザ ログインの認証および許可プロセス

次の図に、ユーザ ログインの認証および許可プロセスのフローチャートを示します。

図 *1*：ユーザ ログインの認証および許可フロー



（注） この図は、ユーザ名とパスワードによる SSH 認証にのみ該当します。公開キー SSH 認証には適用されません。ユーザ名とパスワードによる SSH 認証は、常に AAA を介して行われます。

次に、このプロセスについて順番に説明します。

- Cisco NX-OS デバイスにログインする場合、Telnet、SSH、またはコンソール ログインのオプションが使用できます。

- サーバ グループ認証方式を使用して AAA サーバ グループを設定した場合は、Cisco NX-OS デバイスが、次のように認証要求をグループ内の最初の AAA サーバに送信します。
  - 特定の AAA サーバが応答しなかった場合は、その次の AAA サーバ、さらにその次へと、各サーバが順に試行されます。この処理は、リモート サーバが認証要求に応答するまで続けられます。
  - サーバ グループのすべての AAA サーバが応答しなかった場合、その次のサーバ グループのサーバが試行されます。
  - コンソール ログインでローカルへのフォールバックがディセーブルでないかぎり、設定されている認証方式がすべて失敗した場合、ローカル データベースを使用して認証が実行されます。
- Cisco NX-OS デバイスがリモート AAA サーバでユーザの認証に成功した場合は、次のいずれかが適用されます。
  - AAA サーバ プロトコルが RADIUS の場合、cisco-av-pair 属性で指定されているユーザ ロールが認証応答とともにダウンロードされます。
  - AAA サーバ プロトコルが TACACS+ の場合、シェルのカスタム属性として指定されているユーザ ロールを取得するために、もう 1 つの要求が同じサーバに送信されます。
  - リモート AAA サーバからのユーザ ロールの取得に成功しない場合、ユーザに vdc-operator ロールが割り当てられます。
- ローカルでユーザ名とパスワードの認証が成功した場合は、ログインが許可され、ローカル データベースに設定されているロールが割り当てられます。

（注） 「残りのサーバ グループなし」とは、すべてのサーバ グループのいずれのサーバからも応答がないということです。「残りのサーバなし」とは、現在のサーバ グループ内のいずれのサーバからも応答がないということです。

AES パスワード暗号化およびマスター暗号キー

強力で、反転可能な 128 ビットの高度暗号化規格（AES）パスワード暗号化（タイプ 6 暗号化ともいう）をイネーブルにすることができます。タイプ 6 暗号化の使用を開始するには、AES パスワード暗号化機能をイネーブルにし、パスワード暗号化および復号化に使用されるマスター暗号キーを設定する必要があります。

AES パスワード暗号化をイネーブルにしてマスター キーを設定すると、タイプ 6 パスワード暗号化をディセーブルにしない限り、サポートされているアプリケーション（現在は RADIUS と TACACS+）の既存および新規作成されたクリア テキスト パスワードがすべて、タイプ 6 暗号化の形式で保存されます。また、既存の弱いすべての暗号化パスワードをタイプ 6 暗号化パスワードに変換するように Cisco NX-OS を設定することもできます。

関連トピック

マスター キーの設定および AES パスワード暗号化機能のイネーブル化，（55 ページ）
グローバル RADIUS キーの設定，（86 ページ）
特定の RADIUS サーバ用のキーの設定，（87 ページ）
グローバル TACACS+ キーの設定，（124 ページ）
特定の TACACS+ サーバ用のキーの設定，（126 ページ）

AAA のバーチャライゼーション サポート

デフォルトのコンソール方式と AAA アカウンティング ログを除き、すべての AAA 設定と操作は仮想デバイス コンテキスト（VDC）に対してローカルです。コンソール ログインの AAA 認証方式の設定と操作は、デフォルト VDC に対してだけ適用されます。AAA アカウンティング ログは、デフォルト VDC だけに存在します。任意の VDC から内容を表示できますが、内容のクリアはデフォルト VDC で行う必要があります。

VDC の詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

AAA のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	AAA にはライセンスは必要ありません。ライセンスパッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。 Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

AAA の前提条件

リモート AAA サーバには、次の前提条件があります。

- 少なくとも 1 台の RADIUS サーバ、TACACS+ サーバ、または LDAP サーバが IP を使用して到達可能であることを確認します。
- Cisco NX-OS デバイスが AAA サーバのクライアントとして設定されていることを確認します。

- 秘密キーが Cisco NX-OS デバイスおよびリモート AAA サーバに設定されていることを確認します。
- リモート サーバが Cisco NX-OS デバイスからの AAA 要求に応答することを確認します。

AAA の注意事項と制約事項

AAA に関する注意事項と制約事項は次のとおりです。

- ローカルの Cisco NX-OS デバイス上に設定されているユーザ アカウントが、AAA サーバ上のリモート ユーザ アカウントと同じ名前の場合、Cisco NX-OS ソフトウェアは、AAA サーバ上に設定されているユーザ ロールではなく、ローカル ユーザ アカウントのユーザ ロールをリモート ユーザに適用します。

AAA のデフォルト設定

次の表に、AAA パラメータのデフォルト設定を示します。

表 *6*：*AAA* パラメータのデフォルト設定

パラメータ	デフォルト
コンソール認証方式	local
デフォルト認証方式	local
ログイン認証失敗メッセージ	ディセーブル
CHAP 認証	ディセーブル
MSCHAP 認証	ディセーブル
デフォルト アカウンティング方式	local
アカウンティング ログの表示サイズ	250 KB

AAA の設定

ここでは、Cisco NX-OS デバイスで AAA を設定する手順について説明します。

（注） Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

AAA の設定プロセス

AAA 認証およびアカウンティングを設定するには、次の作業を行います。

1. 認証にリモート RADIUS、TACACS+、または LDAP サーバを使用する場合は、Cisco NX-OS デバイス上でホストを設定します。
2. コンソール ログイン認証方式を設定します。
3. ユーザ ログインのためのデフォルトのログイン認証方式を設定します。
4. デフォルト AAA アカウンティングのデフォルト方式を設定します。

コンソール ログイン認証方式の設定

ここでは、コンソール ログインの認証方式を設定する方法を説明します。

認証方式には、次のものがあります。

- RADIUS サーバのグローバル プール
- RADIUS、TACACS+、または LDAP サーバの指定サブセット
- Cisco NX-OS デバイスのローカル データベース
- ユーザ名だけ（none）

デフォルトの方式はローカルですが、ディセーブルにするオプションがあります。

（注） コンソール ログインの AAA の設定と操作は、デフォルト VDC に対してだけ適用されます。

（注） **aaa authentication** コマンドの **group radius** および **group***server-name* 形式は、以前に定義された RADIUS サーバのセットを参照します。ホスト サーバを設定するには、**radius server-host** コマンドを使用します。サーバの名前付きグループを作成するには、**aaa group server radius** コマンドを使用します。

（注） リモート認証がイネーブルになっているときにパスワード回復を実行すると、パスワード回復の実行後すぐにコンソール ログインのローカル認証がイネーブルになります。そのため、新しいパスワードを使用してコンソール ポート経由で Cisco NX-OS デバイスにログインできます。ログイン後は、引き続きローカル認証を使用するか、または AAA サーバで設定された管理者パスワードのリセット後にリモート認証をイネーブルにすることができます。パスワード回復プロセスの詳細については、『*Cisco NX-OS* のパスワード回復手順』を参照してください。

はじめる前に

デフォルト VDC にいることを確認します。

必要に応じて RADIUS、TACACS+、または LDAP サーバ グループを設定します。

手順の概要

1. **configure terminal**
2. **aaa authentication login console** {**group***group-list* [**none**] | **local** | **none**}
3. **exit**
4. （任意） **show aaa authentication**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**aaa authentication login console** {**group***group-list* [**none**]	**local**	**none**} 例： `switch(config)# aaa authentication login console group radius`	コンソールのログイン認証方式を設定します。 *group-list* 引数には、グループ名をスペースで区切ったリストを指定します。グループ名は、次のように指定します。 **radius** RADIUS サーバのグローバル プールを使用して認証を行います。 ***named-group*** RADIUS、TACACS+、または LDAP サーバの指定サブセットを使用して認証を行います。 **local** 方式を指定すると、認証にローカル データベースが使用されます。**none** 方式を指定すると、AAA 許可が使用されなくなります。

	コマンドまたはアクション	目的
		デフォルトのコンソール ログイン方式は **local** です。これは、方式が何も設定されていない場合、または設定された認証方式すべてについて応答が得られない場合に、コンソール ログインに対してローカルへのフォールバックがディセーブルでない限り、使用されます。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show aaa authentication** 例： `switch# show aaa authentication`	（任意） コンソール ログイン認証方式の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

デフォルトのログイン認証方式の設定

認証方式には、次のものがあります。

- RADIUS サーバのグローバル プール
- RADIUS、TACACS+、または LDAP サーバの指定サブセット
- Cisco NX-OS デバイスのローカル データベース
- ユーザ名だけ

デフォルトの方式はローカルですが、ディセーブルにするオプションがあります。

はじめる前に

必要に応じて RADIUS、TACACS+、または LDAP サーバ グループを設定します。

手順の概要

1. **configure terminal**
2. **aaa authentication login default** {**group***group-list* [**none**] | **local** | **none**}
3. **exit**
4. （任意） **show aaa authentication**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**aaa authentication login default** {**group***group-list* [**none**]	**local**	**none**} 例： `switch(config)# aaa authentication login default group radius`	デフォルト認証方式を設定します。 *group-list* 引数には、グループ名をスペースで区切ったリストを指定します。グループ名は、次のように指定します。 • **radius** を指定すると、RADIUS サーバのグローバル プールが認証に使用されます。 • *named-group*：認証に RADIUS、TACACS+ または LDAP サーバの名前付きサブセットを使用します。 **local** 方式を指定すると、認証にローカルデータベースが使用されます。**none** 方式を指定すると、AAA 許可が使用されなくなります。デフォルトのログイン方式は **local** です。これは、方式が何も設定されていない場合、または設定された認証方式すべてについて応答が得られない場合に、コンソール ログインに対してローカルへのフォール バックがディセーブルでない限り、使用されます。 次のいずれかを設定できます。 • AAA 認証グループ • 認証なしの AAA 認証グループ • ローカル認証 • 認証なし

	コマンドまたはアクション	目的
		（注） **local** キーワードは、AAA 認証グループを設定するときはサポートされません（必須ではありません）。これは、リモートサーバが到達不能の場合のデフォルトがローカル認証であるためです。たとえば、**aaa authentication login default group g1** を設定した場合、AAA グループ g1 を使用して認証を行うことができなければ、ローカル認証が試行されます。これに対し、**aaa authentication login default group g1 none** を設定した場合は、AAA グループ g1 を使用して認証を行うことができなければ、認証は実行されません。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show aaa authentication** 例： `switch# show aaa authentication`	（任意） デフォルトのログイン認証方式の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ローカル認証へのフォールバックのディセーブル化

デフォルトでは、コンソール ログインまたはデフォルト ログインのリモート認証が設定されている場合、どの AAA サーバにも到達不能なときに（認証エラーになります）、ユーザが Cisco NX-OS デバイスからロックアウトされないように、ローカル認証にフォールバックされます。ただし、セキュリティを向上させるために、ローカル認証へのフォールバックをディセーブルにできます。

⚠

注意 ローカル認証へのフォールバックをディセーブルにすると、Cisco NX-OS デバイスがロックされ、パスワード回復を実行しないとアクセスできなくなることがあります。デバイスからロックアウトされないようにするために、ローカル認証へのフォールバックをディセーブルにする対象は、デフォルト ログインとコンソール ログインの両方ではなく、いずれかだけにすることを推奨します。

（注） コンソール ログインの AAA の設定と操作は、デフォルト VDC に対してだけ適用されます。

はじめる前に

コンソール ログインのリモート認証を設定する場合は、事前にデフォルト VDC にいることを確認します。デフォルト ログインのリモート認証は、VDC 単位で設定できます。

コンソール ログインまたはデフォルト ログインのリモート認証を設定します。

手順の概要

1. **configure terminal**
2. **no aaa authentication login {console | default} fallback error local**
3. （任意） **exit**
4. （任意） **show aaa authentication**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**no aaa authentication login {console | default} fallback error local** 例： `switch(config)# no aaa authentication login console fallback error local`	コンソールログインまたはデフォルトログインについて、リモート認証が設定されている場合にどの AAA サーバにも到達不能なときに実行されるローカル認証へのフォールバックをディセーブルにします。 ローカル認証へのフォールバックをディセーブルにすると、次のメッセージが表示されます。 "WARNING!!! Disabling fallback can lock your switch."

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		（任意）
		設定モードを終了します。

ステップ 4	**show aaa authentication** 例： `switch# show aaa authentication`	（任意） コンソール ログインおよびデフォルト ログイン認証方式の設定を表示します。

	コマンドまたはアクション	目的
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

AAA 認証のデフォルト ユーザ ロールのイネーブル化

ユーザ ロールを持たないリモート ユーザに、デフォルトのユーザ ロールを使用して、RADIUS または TACACS+ リモート認証による Cisco NX-OS デバイスへのログインを許可できます。AAA のデフォルトのユーザ ロール機能をディセーブルにすると、ユーザ ロールを持たないリモート ユーザはデバイスにログインできなくなります。

この機能は必要に応じて VDC に対してイネーブルまたはディセーブルにできます。デフォルトの VDC では、デフォルトのユーザ ロールは network-operator です。デフォルト以外の VDC では、デフォルトの VDC は vdc-operator です。

はじめる前に

正しい VDC 内にいることを確認します。VDC を切り替えるには、**switchto vdc** コマンドを使用します。

手順の概要

1. **configure terminal**
2. **aaa user default-role**
3. **exit**
4. （任意） **show aaa user default-role**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

	コマンドまたはアクション	目的
ステップ 2	**aaa user default-role** 例： `switch(config)# aaa user default-role`	AAA 認証のためのデフォルト ユーザ ロールをイネーブルにします。デフォルトではイネーブルになっています。 デフォルト ユーザ ロールの機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show aaa user default-role** 例： `switch# show aaa user default-role`	（任意） AAA デフォルト ユーザ ロールの設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ログイン認証失敗メッセージのイネーブル化

ログイン時にリモート AAA サーバが応答しない場合、そのログインは、ローカル ユーザ データベースにロール オーバーして処理されます。このような場合に、ログイン失敗メッセージがイネーブルになっていると、次のメッセージがユーザの端末に表示されます。

```
Remote AAA servers unreachable; local authentication done.
Remote AAA servers unreachable; local authentication failed.
```

はじめる前に

正しい VDC 内にいることを確認します。VDC を切り替えるには、**switchto vdc** コマンドを使用します。

手順の概要

1. **configure terminal**
2. **aaa authentication login error-enable**
3. **exit**
4. （任意） **show aaa authentication**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**aaa authentication login error-enable** 例： `switch(config)# aaa authentication login error-enable`	ログイン認証失敗メッセージをイネーブルにします。デフォルトではディセーブルになっています。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show aaa authentication** 例： `switch# show aaa authentication`	（任意） ログイン失敗メッセージの設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

CHAP 認証のイネーブル化

Cisco NX-OS ソフトウェアは、チャレンジ ハンドシェーク認証プロトコル（CHAP）をサポートしています。このプロトコルは、業界標準の Message Digest（MD5）ハッシュ方式を使用して応答を暗号化する、チャレンジレスポンス認証方式のプロトコルです。リモート認証サーバ（RADIUS または TACACS+）を介した Cisco NX-OS デバイスへのユーザ ログインに、CHAP を使用できます。

デフォルトでは、Cisco NX-OS デバイスとリモート サーバの間でパスワード認証プロトコル（PAP）認証が使用されます。CHAP がイネーブルの場合は、CHAP ベンダー固有属性（VSA）を認識するように RADIUS サーバまたは TACACS+ サーバを設定する必要があります。

次の表に、CHAP に必要な RADIUS および TACACS+ VSA を示します。

表 *7* : ***CHAP RADIUS*** および ***TACACS+ VSA***

ベンダー ID 番号	ベンダー タイプ番号	VSA	説明
311	11	CHAP-Challenge	AAA サーバから CHAP ユーザに送信されるチャレンジを保持します。これは、Access-Request パケットと Access-Challenge パケットの両方で使用できます。
211	11	CHAP-Response	チャレンジに対する応答として CHAP ユーザが入力した値を保持します。Access-Request パケットだけで使用します。

はじめる前に

ログイン用の AAA ASCII 認証をディセーブルにします。

手順の概要

1. **configure terminal**
2. **no aaa authentication login ascii-authentication**
3. **aaa authentication login chap enable**
4. （任意） **exit**
5. （任意） **show aaa authentication login chap**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例 :
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

	コマンドまたはアクション	目的
ステップ 2	**no aaa authentication login ascii-authentication** 例： `switch(config)# no aaa authentication login ascii-authentication`	ASCII 認証をディセーブルにします。
ステップ 3	**aaa authentication login chap enable** 例： `switch(config)# aaa authentication login chap enable`	CHAP 認証をイネーブルにします。デフォルトではディセーブルになっています。 （注） Cisco NX-OS デバイスで CHAP と MSCHAP（または MSCHAP V2）の両方をイネーブルにすることはできません。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		（任意）
		設定モードを終了します。

ステップ 5	**show aaa authentication login chap** 例： `switch# show aaa authentication login chap`	（任意） CHAP の設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

MSCHAP または MSCHAP V2 認証のイネーブル化

マイクロソフト チャレンジ ハンドシェーク認証プロトコル（MSCHAP）は、マイクロソフト版の CHAP です。Cisco NX-OS ソフトウェアは、MSCHAP バージョン 2（MSCHAP V2）もサポートしています。リモート認証サーバ（RADIUS または TACACS+）を介した Cisco NX-OS デバイスへのユーザ ログインに、MSCHAP を使用できます。MSCHAP V2 では、リモート認証 RADIUS サーバを介した Cisco NX-OS デバイスへのユーザ ログインだけがサポートされます。MSCHAP V2 の場合に TACACS+ グループを設定すると、デフォルトの AAA ログイン認証では、次に設定されている方式が使用されます。他のサーバ グループが設定されていない場合は、ローカル方式が使用されます。

（注） Cisco NX-OS ソフトウェアで、次のメッセージが表示される場合があります。

「Warning: MSCHAP V2 is supported only with Radius.」

この警告メッセージは単なる情報メッセージであり、RADIUS での MSCHAP V2 の動作には影響しません。

デフォルトでは、Cisco NX-OS デバイスとリモート サーバの間でパスワード認証プロトコル（PAP）認証が使用されます。MSCHAP または MSCHAP V2 をイネーブルにする場合は、MSCHAP および MSCHAP V2 ベンダー固有属性（VSA）を認識するように RADIUS サーバを設定する必要があります。

次の表に、MSCHAP に必要な RADIUS VSA を示します。

表 *8*：*MSCHAP* および *MSCHAP V2 RADIUS VSA*

ベンダー ID 番号	ベンダー タイプ番号	VSA	説明
311	11	MSCHAP-Challenge	AAA サーバから MSCHAP または MSCHAP V2 ユーザに送信されるチャレンジを保持します。これは、Access-Request パケットと Access-Challenge パケットの両方で使用できます。
211	11	MSCHAP-Response	チャレンジに対する応答として MSCHAP または MSCHAP V2 ユーザが入力した値を保持します。Access-Request パケットでしか使用されません。

はじめる前に

ログイン用の AAA ASCII 認証をディセーブルにします。

手順の概要

1. **configure terminal**
2. **no aaa authentication login ascii-authentication**
3. **aaa authentication login** {**mschap** | **mschapv2**} **enable**
4. **exit**
5. （任意） **show aaa authentication login** {**mschap** | **mschapv2**}
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**no aaa authentication login ascii-authentication** 例： `switch(config)# no aaa authentication login ascii-authentication`	ASCII 認証をディセーブルにします。
ステップ 3	**aaa authentication login** {**mschap**	**mschapv2**} **enable** 例： `switch(config)# aaa authentication login mschap enable`	MSCHAP または MSCHAP V2 認証をイネーブルにします。デフォルトではディセーブルになっています。 （注） Cisco NX-OS デバイスで MSCHAP と MSCHAP V2 の両方をイネーブルにすることはできません。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 5	**show aaa authentication login** {**mschap**	**mschapv2**} 例： `switch# show aaa authentication login mschap`	（任意） MSCHAP または MSCHAP V2 の設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

マスターキーの設定およびAESパスワード暗号化機能のイネーブル化

タイプ 6 暗号化用のマスター キーを設定し、高度暗号化規格（AES）パスワード暗号化機能をイネーブルにすることができます。

手順の概要

1. **[no] key config-key ascii**
2. **configure terminal**
3. **[no] feature password encryption aes**
4. （任意） **show encryption service stat**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**[no] key config-key ascii**
	
	例：
	`switch# key config-key ascii`
	`New Master Key:`
	`Retype Master Key:`
		マスター キーを、AES パスワード暗号化機能で使用するように設定します。マスター キーは、16 ～ 32 文字の英数字を使用できます。このコマンドの **no** 形式を使用すると、いつでもマスター キーを削除できます。
		
		マスター キーを設定する前に AES パスワード暗号化機能をイネーブルにすると、マスター キーが設定されていない限りパスワード暗号化が実行されないことを示すメッセージが表示されます。マスター キーがすでに設定されている場合、新しいマスター キーを入力する前に現在のマスター キーを入力するように求められます。

ステップ 2	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 3	**[no] feature password encryption aes** 例： `switch(config)# feature password encryption aes`	AES パスワード暗号化機能をイネーブルまたはディセーブルにします。
ステップ 4	**show encryption service stat** 例： `switch(config)# show encryption service stat`	（任意） AES パスワード暗号化機能とマスター キーの設定ステータスを表示します。

	コマンドまたはアクション	目的
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。 （注） このコマンドは、実行コンフィギュレーションとスタートアップコンフィギュレーションのマスターキーを同期するために必要です。

関連トピック

AES パスワード暗号化およびマスター暗号キー，（39 ページ）
キーのテキストの設定，（794 ページ）
キーの受け入れライフタイムおよび送信ライフタイムの設定，（795 ページ）

既存のパスワードのタイプ 6 暗号化パスワードへの変換

既存の単純で脆弱な暗号化パスワードをタイプ 6 暗号化パスワードに変換できます。

はじめる前に

AES パスワード暗号化機能をイネーブルにし、マスター キーを設定したことを確認します。

手順の概要

1. **encryption re-encrypt obfuscated**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**encryption re-encrypt obfuscated** 例： `switch# encryption re-encrypt obfuscated`	既存の単純で脆弱な暗号化パスワードをタイプ 6 暗号化パスワードに変換します。

タイプ 6 暗号化パスワードの元の状態への変換

タイプ 6 暗号化パスワードを元の状態に変換できます。

はじめる前に

マスター キーを設定したことを確認します。

手順の概要

1. **encryption decrypt type6**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**encryption decrypt type6**
	
	例：
	`switch# encryption decrypt type6`
	`Please enter current Master Key:`
		タイプ 6 暗号化パスワードを元の状態に変換します。

タイプ 6 暗号化パスワードの削除

Cisco NX-OS デバイスからすべてのタイプ 6 暗号化パスワードを削除できます。

手順の概要

1. **encryption delete type6**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**encryption delete type6** 例： `switch# encryption delete type6`	すべてのタイプ 6 暗号化パスワードを削除します。

デフォルトの AAA アカウンティング方式の設定

Cisco NX-OS ソフトウェアは、アカウンティングに TACACS+ および RADIUS 方式をサポートします。Cisco NX-OS デバイスは、ユーザのアクティビティを、アカウンティング レコードの形式で TACACS+ または RADIUS セキュリティ サーバにレポートします。各アカウンティング レコードに、アカウンティング属性値（AV）のペアが入っており、それが AAA サーバに格納されます。

AAA アカウンティングをアクティブにすると、Cisco NX-OS デバイスは、これらの属性をアカウンティング レコードとしてレポートします。アカウンティング レコードはその後セキュリティ サーバのアカウンティング ログに保存されます。

特定のアカウンティング方式を定義するデフォルト方式リストを作成できます。次の方式を含めることができます。

RADIUS サーバ グループ

RADIUS サーバのグローバル プールを使用してアカウンティングを行います。

指定されたサーバ グループ

指定された RADIUS または TACACS+ サーバ グループを使用してアカウンティングを行います。

ローカル

ローカルのユーザ名またはパスワード データベースを使用してアカウンティングを行います。

（注） サーバ グループが設定されていて、そのサーバ グループが応答しない場合、デフォルトではローカル データベースが認証に使用されます。

はじめる前に

必要に応じて RADIUS または TACACS+ サーバ グループを設定します。

手順の概要

1. **configure terminal**
2. **aaa accounting default** {**group***group-list* | **local**}
3. **exit**
4. （任意） **show aaa accounting**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		コンフィギュレーション モードに入ります。

ステップ 2	**aaa accounting default** {**group***group-list* | **local**}	デフォルトのアカウンティング方式を設定します。

	コマンドまたはアクション	目的
	例： `switch(config)# aaa accounting default group radius`	*group-list* 引数には、グループ名をスペースで区切ったリストを指定します。グループ名は、次のように指定します。 • **radius** を指定すると、RADIUS サーバのグローバル プールがアカウンティングに使用されます。 • *named-group*：TACACS+ サーバまたは RADIUS サーバの名前付きサブセットがアカウンティングに使用されます。 **local** 方式では、アカウンティングにローカル データベースが使用されます。 デフォルトのアカウンティング方式は、**local** です。これはサーバ グループが何も設定されていない場合、または設定されたすべてのサーバ グループから応答が得られなかった場合に使用されます。

ステップ 3	**exit**
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show aaa accounting** 例： `switch# show aaa accounting`	（任意） デフォルトの AAA アカウンティング方式の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Cisco NX-OS デバイスによる AAA サーバの VSA の使用

ベンダー固有属性（VSA）を使用して、AAA サーバ上で Cisco NX-OS のユーザ ロールおよび SNMPv3 パラメータを指定できます。

VSA の概要

インターネット技術特別調査委員会（IETF）が、ネットワーク アクセス サーバと RADIUS サーバの間での VSA の通信のための方式を規定する標準を作成しています。IETF は属性 26 を使用します。ベンダーは VSA を使用して、一般的な用途には適さない独自の拡張属性をサポートできます。シスコの RADIUS 実装は、この仕様で推奨される形式を使用して、1 つのベンダー固有オプ

ションをサポートしています。シスコのベンダー ID は 9、サポートされるオプションのベンダータイプは 1（名前付き cisco-av-pair）です。値は次の形式のストリングです。

```
protocol : attribute separator value *
```

protocol は、特定の許可タイプを表すシスコの属性です。separator は、必須属性の場合は =（等号）、オプションの属性の場合は *（アスタリスク）です。

Cisco NX-OS デバイス上の認証に RADIUS サーバを使用した場合、RADIUS プロトコルでは RADIUS サーバに対して、認証結果とともに権限付与情報などのユーザ属性を返すように指示します。この許可情報は、VSA で指定されます。

VSA の形式

Cisco NX-OS ソフトウェアでは次の VSA プロトコル オプションをサポートしています。

Shell

ユーザ プロファイル情報を提供する access-accept パケットで使用されるプロトコル。

Accounting

accounting-request パケットで使用されるプロトコル。値にスペースが含まれている場合は、二重引用符で囲んでください。

次の属性が Cisco NX-OS ソフトウェアでサポートされています。

ロール

ユーザに割り当てられたすべてのロールの一覧です。値フィールドは、グループ名を空白で区切ったリストの入ったストリングです。たとえば、ユーザが network-operator および vdc-admin のロールに属している場合、値フィールドは network-operator vdc-admin となります。このサブ属性は Access-Accept フレームの VSA 部分に格納され、RADIUS サーバから送信されます。この属性は shell プロトコル値とだけ併用できます。次に、ロール属性を使用する例を示します。

```
shell:roles=network-operator vdc-admin
```

```
shell:roles*network-operator vdc-admin
```

次に、FreeRADIUS でサポートされるロール属性の例を示します。

```
Cisco-AVPair = shell:roles=\network-operator vdc-admin\
```

```
Cisco-AVPair = shell:roles*\network-operator vdc-admin\
```

（注） VSA を shell:roles*"network-operator vdc-admin" または "shell:roles*\"network-operator vdc-admin\"" として指定した場合、この VSA はオプション属性としてフラグ設定され、他のシスコ デバイスはこの属性を無視します。

accountinginfo

標準の RADIUS アカウンティング プロトコルに含まれる属性とともにアカウンティング情報を格納します。この属性が送信されるのは、スイッチ上の RADIUS クライアントからの Account-Request フレームの VSA 部分内だけです。この属性は、アカウンティング プロトコル関連の PDU でしか使用できません。

AAA サーバ上での Cisco NX-OS のユーザ ロールおよび SNMPv3 パラメータの指定

AAA サーバ上で VSA に cisco-av-pair を使用して、次の形式で Cisco NX-OS デバイスのユーザ ロールのマッピングを指定できます。

```
shell:roles="roleA roleB …"
```

cisco-av-pair 属性にロール オプションを指定しなかった場合のデフォルトのユーザ ロールは、network-operator です。

次のように SNMPv3 認証とプライバシー プロトコル属性を指定することもできます。

```
shell:roles="roleA roleB..." snmpv3:auth=SHA priv=AES-128
```

SNMPv3 認証プロトコルに指定できるオプションは、SHA と MD5 です。プライバシー プロトコルに指定できるオプションは、AES-128 と DES です。cisco-av-pair 属性にこれらのオプションを指定しなかった場合のデフォルトの認証プロトコルは、MD5 と DES です。

セキュア ログインの拡張機能

次のセキュア ログインの拡張機能は、Cisco NX-OS でサポートされます。

ログイン パラメータの設定

Cisco NX-OS デバイスへの DoS 攻撃の疑いを検出し、辞書攻撃による影響の緩和に役立つログイン パラメータを設定するには、ここに示す手順を実行します。

すべてのログイン パラメータは、デフォルトではディセーブルです。他のログイン コマンドを使用する前に **loginblock-for** コマンドを入力してデフォルトのログイン機能をイネーブルにする必要があります。**loginblock-for** コマンドをイネーブルにすると、次のデフォルトが強制されます。

- Telnet または SSH を通じて行われるすべてのログイン試行は、待機時間中拒否されます。つまり、**loginquiet-modeaccess-class** コマンドが入力されるまで、ACL はログイン時間から除外されません。

手順の概要

1. **configureterminal**
2. **[no] loginblock-for***seconds***attempts***tries***within***seconds*
3. **[no] loginquiet-modeaccess-class** {*acl-name* | *acl-number*}
4. **exit**
5. **showloginfailures**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**[no] loginblock-for***seconds***attempts***tries***within***seconds* 例： `Switch(config)# login block-for 100 attempts 2 within 100`	Cisco NX-OS デバイスで DoS の検出に役立つログイン パラメータを設定します。 （注） このコマンドは、その他のログイン コマンドを使用する前に発行する必要があります。
ステップ 3	**[no] loginquiet-modeaccess-class** {*acl-name*	*acl-number*} 例： `Switch(config)# login quiet-mode access-class myacl`	（任意）このコマンドはオプションですが、このコマンドを使用してデバイスが待機モードに切り替わったときに適用する ACL を指定することを推奨します。デバイスが待機モードになっている間は、すべてのログイン要求が拒否され、使用できる接続はコンソール経由の接続のみになります。
ステップ 4	**exit** 例： `Switch(config)# exit`	特権 EXEC モードに戻ります。
ステップ 5	**showloginfailures** 例： `Switch# show login`	ログイン パラメータを表示します。 • **failures**：失敗したログイン試行に関連する情報のみを表示します。

ログイン パラメータの設定例

ログイン パラメータの設定例

次に、100 秒以内に 15 回ログイン要求が失敗した場合に 100 秒の待機モードに入るようにスイッチを設定する例を示します。待機時間中、ACL「myacl」からのホスト以外、すべてのログイン要求が拒否されます。

```
Switch(config)# login block-for 100 attempts 15 within 100
Switch(config)# login quiet-mode access-class myacl
```

ログイン パラメータの表示例

show login コマンドからの次のサンプル出力は、ログイン パラメータが指定されていないことを確認します。

```
Switch# show login

No Quiet-Mode access list has been configured, default ACL will be applied.

Switch is enabled to watch for login Attacks.
If more than 2 login failures occur in 45 seconds or less,  logins will be disabled for 70
 seconds.

Switch presently in Normal-Mode.
Current Watch Window remaining time 10 seconds.
Present login failure count 0.
```

show login failures コマンドからの次のサンプル出力は、スイッチ上で失敗したすべてのログイン試行を表示します。

```
Switch# show login failures

Information about last 20 login failures with the device.
--------------------------------------------------------------------------------
Username                                Line    Source                Appname
TimeStamp
--------------------------------------------------------------------------------
admin                                    pts/0   bgl-ads-728.cisco.com   login
        Wed Jun 10 04:56:16 2015
admin                                    pts/0   bgl-ads-728.cisco.com   login
        Wed Jun 10 04:56:19 2015
--------------------------------------------------------------------------------
```

show login failures コマンドからの次のサンプル出力は、現在記録されている情報がないことを確認します。

```
Switch# show login failures
*** No logged failed login attempts with the device.***
```

ユーザごとのログイン ブロックの設定

ユーザごとのログイン ブロック機能を使用すると、Denial of Service（DoS）攻撃の疑いを検出して、辞書攻撃の影響を緩和することができます。この機能はローカル ユーザのみに適用されます。ログインに失敗したユーザをブロックするようにログイン パラメータを設定するには、ここに示す手順を実行します。

手順の概要

1. **configureterminal**
2. **aaa authenticationrejected***attempts***in***seconds***ban***seconds*
3. **exit**
4. **showrunningconfig**
5. **showaaalocal userblocked**
6. **clearaaalocal userblocked**{**username***user* | **all**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**aaa authenticationrejected***attempts***in***seconds***ban***seconds* 例： `switch(config)# aaa authentication rejected 3 in 20 ban 300`	ユーザをブロックするようにログイン パラメータを設定します。 （注） デフォルトのログイン パラメータに戻すには **no aaa authenticationrejected** コマンドを使用します。
ステップ 3	**exit** 例： `switch(config)# exit`	特権 EXEC モードに戻ります。
ステップ 4	**showrunningconfig** 例： `switch# show running config`	（任意）ログイン パラメータを表示します。
ステップ 5	**showaaalocal userblocked** 例： `switch# show aaa local user blocked`	（任意）ブロックされたローカルユーザを表示します。
ステップ 6	**clearaaalocal userblocked**{**username***user*	**all**} 例： `switch# clear aaa local user blocked username testuser`	（任意）ブロックされたローカルユーザをクリアします。 • **all**：ブロックされたすべてのローカル ユーザをクリアします。

	コマンドまたはアクション	目的

ユーザごとのログイン ブロックの設定例

ユーザごとのログイン ブロックの設定パラメータ

次に、60 秒の間に 5 回のログイン試行が失敗した場合に、300 秒間ユーザをブロックするログイン パラメータを設定する例を示します。

```
switch(config)# aaa authentication rejected 5 in 60 ban 300
```

ログイン パラメータの表示

次に、スイッチで設定されているログイン パラメータを表示する例を示します。

```
switch# show run | i rejected
aaa authentication rejected 5 in 60 ban 300
```

ブロック済みローカル ユーザの表示

次に、ブロック済みローカル ユーザを表示する例を示します。

```
switch# show aaa local user blocked
Local-user                  State

testuser                    Watched (till 11:34:42 IST Feb 5 2015)
```

ブロック済みローカル ユーザのクリア

次に、ブロック済みローカル ユーザ testuser をクリアする例を示します。

```
switch# clear aaa local user blocked username testuser
```

ユーザ1人あたりのセッション数の制限（ユーザ1人あたり、ログイン1回あたり）

ユーザ 1 人あたりの最大セッション数を制限するには、ここに示す手順を実行します。

手順の概要

1. **configureterminal**
2. **[no] user max-logins***max-logins*
3. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**[no] user max-logins***max-logins* 例： `Switch(config)# user max-logins 1`	ユーザ 1 人あたりの最大セッション数を制限します。指定できる範囲は 1 ～ 7 です。最大ログイン制限を 1 に設定すると、ユーザ 1 人あたりのセッション数（telnet/SSH）が 1 つに制限されます。
ステップ 3	**exit** 例： `Switch(config)# exit`	特権 EXEC モードに戻ります。

パスフレーズの設定とユーザ アカウントのロック

パスフレーズの長さ、有効期間、およびユーザアカウントロック機能を設定するには、ここに示す手順を実行します。

手順の概要

1. **userpassphrase** { **min-length** | **max-length** }
2. **userpassphrase** { **min-length** & **max-length** }
3. **show userpassphrase** {**min-length**| **max-length**|**length**}
4. **no userpassphrase** {**min-length** | **max-length** | **length** }
5. **show userpassphrase all**
6. **userpassphrase** { **default-lifetime** | **default-warntime** | **default-gracetime** }
7. **username**<*username*> **passphrase** { **lifetime**| **warntime** | **gracetime**}
8. **no username** <*username*> **passphrase** { **lifetime** | **warntime** | **gracetime** | **timevalues** }
9. **show username**<*username*> **passphrase timevalues**
10. **username** <*username*> **lock-user-account**
11. **username** <*username*> **expire-userpassphrase**
12. **show locked-users**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**userpassphrase** { **min-length** | **max-length** } 例： `Switch(config)# userpassphrase {  min-length <8 ? 127> | max-length <80 ? 127> }`	（管理者のみ）パスフレーズの最小長または最大長のいずれかを設定できます
ステップ 2	**userpassphrase** { **min-length** & **max-length** } 例： `Switch(config)# userpassphrase {  min-length <8 ? 127> & max-length <80 ? 127> }`	（管理者のみ）パスフレーズの最小長と最大長の両方を設定できます
ステップ 3	**show userpassphrase** {**min-length**| **max-length**|**length**} 例： `Switch(config)# show userpassphrase {min-length | max-length | length }`	min-length または max-length オプションを使用すると、パスフレーズの最小長または最大長を表示できます。length オプションを使用すると、パスフレーズの長さの設定をすべて表示できます。
ステップ 4	**no userpassphrase** {**min-length** | **max-length** | **length** } 例： `Switch(config)# userpassphrase {min-length | max-length | length }`	パスフレーズの長さの設定がデフォルト値にリセットされます
ステップ 5	**show userpassphrase all** 例： `Switch(config)# show userpassphrase all`	userpassphrase で設定されたすべてのパラメータ値が一覧表示されます
ステップ 6	**userpassphrase** { **default-lifetime** | **default-warntime** | **default-gracetime** } 例： `Switch(config)# userpassphrase { default-lifetime  | default-warntime | default-gracetime }`	（管理者のみ）デフォルト設定を更新できます
ステップ 7	**username**<*username*> **passphrase** { **lifetime**| **warntime** | **gracetime**} 例： `Switch(config)# username  <user1> passphrase { lifetime | warntime | gracetime }`	（管理者のみ）任意のユーザに対してパスフレーズの有効期間を設定できます
ステップ 8	**no username** <*username*> **passphrase** { **lifetime** | **warntime** | **gracetime** | **timevalues** } 例： `Switch(config)# username <user1> passphrase { lifetime | warntime | gracetime | timevalues }`	（管理者のみ）任意のユーザのパスフレーズ有効期間をデフォルト値にリセットできます

	コマンドまたはアクション	目的
ステップ 9	**show username**<*username*> **passphrase timevalues** 例： `Switch(config)# show username <user1> passphrase timevalues`	ユーザは自身のパスフレーズ有効期間を表示でき、管理者は任意のユーザのパスフレーズ有効期間を表示できます
ステップ 10	**username** <*username*> **lock-user-account** 例： `Switch(config)# username <user1> lock-user-account`	（管理者のみ）任意のユーザ アカウントをロックできます
ステップ 11	**username** <*username*> **expire-userpassphrase** 例： `Switch(config)# username <user1> expire-userpassphrase`	（管理者のみ）任意のユーザ パスフレーズをただちに有効期限切れにすることができます
ステップ 12	**show locked-users** 例： `Switch(config)# show locked-users`	（管理者のみ）ロックされたすべてのユーザを表示し、ロックを解除することができます

ユーザ名のパスワード プロンプトのイネーブル化

手順の概要

1. **configureterminal**
2. **[no] password prompt username**
3. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**[no] password prompt username** 例： `Switch(config)# password prompt username`	ログイン パスワード入力要求をイネーブルにします。このコマンドをイネーブルになっている場合、ユーザが **username** コマンドを入力すると、パスワードを入力するよう求められます。パスワードの入力には隠し文字を使用できます。ログイン パスワード入力要求をディセーブルにするには、このコマンドの **no** 形式を使用します。
ステップ 3	**exit** 例： `Switch(config)# exit`	特権 EXEC モードに戻ります。

OS の整合性を確認するための SHA-256 アルゴリズムのサポート

show file bootflash:/ sha256sum コマンドを使用して、ファイルの sha256sum を表示します。このコマンドのサンプル出力を次に示します。

```
Switch# show file bootflash:/ sha256sum
abd9d40020538acc363df3d1bae7d1df16841e4903fca2c07c7898bf4f549ef5
```

RADIUS/TACACS+ を使用するための共有キー値の設定

リモート認証およびアカウンティング用に設定する共有秘密は非表示にする必要があります。**radius-server key** および **tacacs-server key** コマンドでは、別のコマンドを使用して暗号化された共有秘密を使用できます。

手順の概要

1. **configureterminal**
2. **generate type7_encrypted_secret**
3. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configureterminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**generate type7_encrypted_secret** 例： `Switch(config)# generate type7_encrypted_secret`	キー タイプ 7 で RADIUS および TACACS の共有秘密を設定します。暗号化された共有秘密を生成する間はユーザ入力が非表示になります。 （注） プレーンテキストから暗号化された文字列を別個に生成して、暗号化された共有秘密を後から設定することもできます。
ステップ 3	**exit** 例： `Switch(config)# exit`	特権 EXEC モードに戻ります。

ローカル AAA アカウンティング ログのモニタリングとクリア

Cisco NX-OS デバイスは、AAA アカウンティングのアクティビティに関するローカル ログを維持しています。このログはモニタリングしたりクリアしたりできます。

（注） AAA アカウンティング ログは、デフォルト VDC に対してローカルです。任意の VDC から内容をモニタリングできますが、内容のクリアはデフォルト VDC で行う必要があります。

手順の概要

1. **show accounting log** [*size* | **last-index** | **start-seqnum** *number* | **start-time***year month day hh*:*mm*:*ss*]
2. （任意） **clear accounting log**[**logflash**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show accounting log** [*size* | **last-index** | **start-seqnum** *number* | **start-time***year month day hh*:*mm*:*ss*] 例： `switch# show accounting log`	アカウンティング ログを表示します。このコマンド出力には、デフォルトで最大 250,000 バイトのアカウンティング ログが表示されます。コマンドの出力を制限する場合は、*size* 引数を使用します。指定できる範囲は 0 ～ 250000 バイトです。また、ログ出力の開始シーケンス番号または開始時間を指定できます。開始インデックスの範囲は、1 ～ 1000000 です。アカウンティング ログ ファイルにある最後のインデックス番号の値を表示するには、**last-index** キーワードを使用します。
ステップ 2	**clear accounting log**[**logflash**] 例： `switch# clear aaa accounting log`	（任意） アカウンティング ログの内容をクリアします。**logflash** キーワードは現在の VDC のログ フラッシュに保存されているアカウンティング ログをクリアします。

AAA 設定の確認

AAA の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show aaa accounting	AAA アカウンティングの設定を表示します。
show aaa authentication [**login** {**ascii-authentication** | **chap** | **error-enable** | **mschap** | **mschapv2**}]	AAA 認証ログイン設定情報を表示します。
show aaa groups	AAA サーバ グループの設定を表示します。
show running-config aaa [**all**]	実行コンフィギュレーションの AAA 設定を表示します。
show startup-config aaa	スタートアップ コンフィギュレーションの AAA 設定を表示します。

これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

AAA の設定例

次に、AAA を設定する例を示します。

```
aaa authentication login default group radius
aaa authentication login console group radius
aaa accounting default group radius
```

AAA に関する追加情報

ここでは、AAA の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS ライセンス設定	『*Cisco NX-OS Licensing Guide*』
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』
SNMP	『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
• CISCO-AAA-SERVER-MIB • CISCO-AAA-SERVER-EXT-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

AAA の機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 *9*：*AAA* の機能の履歴

機能名	リリース	機能情報
ユーザごとのログイン ブロック	7.3(0)D1(1)	ユーザごとのログイン ブロックのサポートが追加されました。「セキュア ログインの拡張機能」の項を参照してください。
セキュア ログインの拡張機能	7.2(0)D1(1)	セキュア ログインの拡張機能が追加されました。「セキュア ログインの拡張機能」の項を参照してください。
AAA	6.0(1)	Release 5.2 以降、変更はありません。
AAA	5.2(1)	Cisco Nexus 3000 シリーズ スイッチのサポートが追加されました。
AAA	5.2(1)	Release 5.1 以降、変更はありません。
AAA	5.1(1)	Release 5.0 以降、変更はありません。
AAA 認証	5.0(2)	ユーザ ログインに対する AAA 認証のイネーブル化またはディセーブル化のサポートが追加されました。
AAA 認証	5.0(2)	ユーザ ロールを持たないリモート ユーザに、デフォルトのユーザ ロールを使用して、RADIUS または TACACS+ リモート認証によって Cisco NX-OS デバイスにログインすることがサポートされるようになりました。

機能名	リリース	機能情報
ログイン認証	5.0(2)	ログイン認証失敗メッセージのイネーブル化またはディセーブル化のサポートが追加されました。
CHAP 認証	5.0(2)	CHAP 認証のイネーブル化またはディセーブル化のサポートが追加されました。
ローカル認証	5.0(2)	リモート認証が失敗したときに、ローカル認証へのフォールバックをイネーブルにすることがサポートされるようになりました。
ローカル認証	5.0(2)	ローカル認証へのフォールバックをディセーブルにすることがサポートされるようになりました。
MSCHAP V2 認証	4.2(1)	MSCHAP V2 認証のイネーブル化またはディセーブル化のサポートが追加されました。
AAA	4.2(1)	リリース 4.1 からの変更はありません。

第 5 章

RADIUS の設定

この章では、Cisco NX-OS デバイスで Remote Access Dial-In User Service（RADIUS）プロトコルを設定する手順について説明します。

この章は、次の項で構成されています。

- 機能情報の確認，75 ページ
- RADIUS の概要，76 ページ
- RADIUS のライセンス要件，80 ページ
- RADIUS の前提条件，81 ページ
- RADIUS の注意事項と制約事項，81 ページ
- RADIUS のデフォルト設定，81 ページ
- RADIUS サーバの設定，82 ページ
- RADIUS 設定の確認，108 ページ
- RADIUS サーバのモニタリング，109 ページ
- RADIUS サーバ統計情報のクリア，109 ページ
- RADIUS の設定例，110 ページ
- 次の作業，110 ページ
- RADIUS に関する追加情報，110 ページ
- RADIUS の機能の履歴，111 ページ

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。こ

のモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

RADIUS の概要

RADIUS 分散クライアント/ サーバ システムを使用すると、不正アクセスからネットワークを保護できます。シスコの実装では、RADIUS クライアントは Cisco NX-OS デバイス上で稼働します。認証要求とアカウンティング要求は、すべてのユーザ認証情報とネットワーク サービスアクセス情報が格納されている中央の RADIUS サーバに送信されます。

RADIUS ネットワーク環境

RADIUS は、高度なセキュリティを必要とし、同時にリモート ユーザのネットワーク アクセスを維持する必要があるさまざまなネットワーク環境に実装できます。

RADIUS は、アクセス セキュリティを必要とする次のネットワーク環境で使用します。

- RADIUS をサポートしている複数ベンダーのネットワーク デバイスを使用したネットワーク
たとえば、複数ベンダーのネットワーク デバイスで、単一の RADIUS サーバ ベースのセキュリティ データベースを使用できます。
- すでに RADIUS を使用中のネットワーク。RADIUS 機能を持つ Cisco NX-OS デバイスをネットワークに追加できます。この作業は、AAA サーバに移行するときの最初の手順になります。
- リソース アカウンティングが必要なネットワーク。RADIUS アカウンティングは、RADIUS 認証または RADIUS 認可とは個別に使用できます。RADIUS アカウンティング機能を使用すると、サービスの開始および終了時に、セッション中に使用したリソース（時間、パケット、バイトなど）の量を示すデータを送信できます。インターネット サービス プロバイダー（ISP）は、RADIUS アクセス コントロールおよびアカウンティング用ソフトウェアのフリーウェア版を使用して、特殊なセキュリティおよび課金ニーズに対応しています。
- 認証プロファイルをサポートするネットワークネットワークで RADIUS サーバを使用すると、AAA 認証を設定し、ユーザごとのプロファイルをセットアップできます。ユーザ単位のプロファイルにより、既存の RADIUS ソリューションを使用するポートの管理性が向上し、共有リソースを効率的に管理して、各種のサービスレベル契約を提供できるようになります。

RADIUS の動作

RADIUS を使用する Cisco NX-OS デバイスに、ユーザがログインおよび認証を試みると、次の処理が行われます。

- ユーザが、ユーザ名とパスワードの入力を求められ、入力します。

- ユーザ名および暗号化されたパスワードが、ネットワーク経由でRADIUSサーバに送信されます。
- ユーザは、RADIUS サーバから次のいずれかの応答を受信します。

ACCEPT

ユーザが認証されました。

REJECT

ユーザは認証されず、ユーザ名とパスワードの再入力を求められるか、アクセスを拒否されます。

CHALLENGE

RADIUS サーバによってチャレンジが発行されます。チャレンジは、ユーザから追加データを収集します。

CHANGE PASSWORD

RADIUSサーバからユーザに、新しいパスワードを選択するよう要求が発行されます。

ACCEPT応答またはREJECT応答には、EXEC許可またはネットワーク許可に使用される追加データが含まれています。RADIUS 認可を使用するには、まず RADIUS 認証を完了する必要があります。ACCEPT または REJECT パケットに含まれる追加データの内容は次のとおりです。

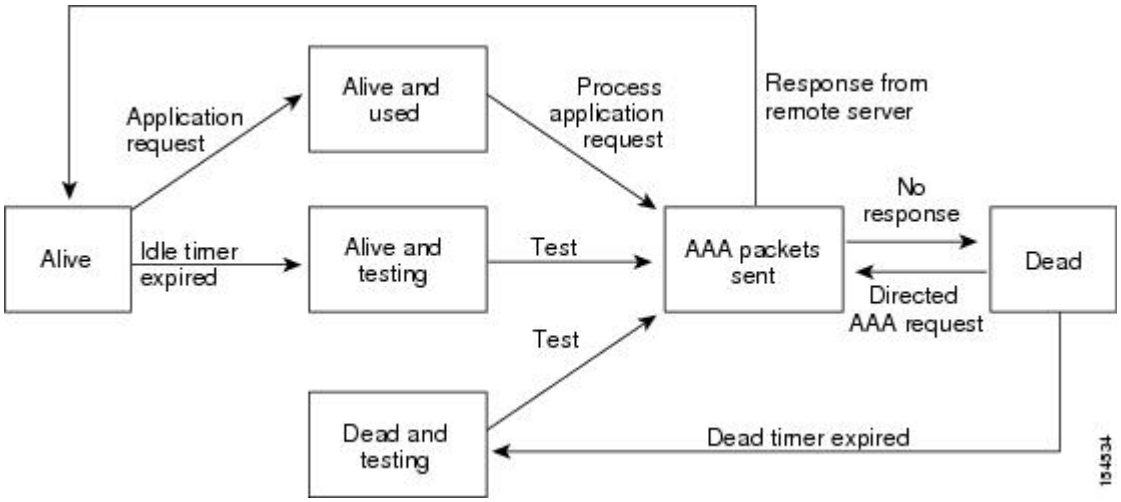
- ユーザがアクセス可能なサービス（Telnet、rlogin、またはローカルエリア トランスポート（LAT）接続、ポイントツーポイントプロトコル（PPP）、シリアル ライン インターネット プロトコル（SLIP）、EXEC サービスなど）
- 接続パラメータ（ホストまたはクライアントの IPv4 または IPv6 アドレス、アクセス リスト、ユーザ タイムアウト）

RADIUS サーバのモニタリング

応答しない RADIUS サーバがあると、AAA 要求の処理が遅れることがあります。AAA 要求の処理時間を短縮するために、定期的にRADIUS サーバをモニタしてRADIUS サーバが応答している（アライブ）かどうかを調べるように、CiscoNX-OS を設定できます。CiscoNX-OSデバイスは、応答の遅い RADIUS サーバをデッド（dead）としてマークし、デッド RADIUS サーバには AAA 要求を送信しません。Cisco NX-OS デバイスは、デッド RADIUS サーバを定期的にモニタし、応答があればアライブ状態に戻します。このモニタリング プロセスでは、実際の AAA 要求が送信される前に、RADIUS サーバが稼働状態であることを確認します。RADIUS サーバがデッドまたはアライブの状態に変わると簡易ネットワーク管理プロトコル（SNMP）トラップが生成され、Cisco NX-OS デバイスは障害が発生していることをエラー メッセージで表示します。

次の図に、RADIUS サーバ モニタリングの状態を示します。

図 *2*：*RADIUS* サーバの状態



（注） アライブ サーバとデッド サーバのモニタリング間隔は異なります。これらはユーザが設定できます。RADIUS サーバ モニタリングを実行するには、テスト認証要求を RADIUS サーバに送信します。

RADIUS 設定の配布

Cisco Fabric Services（CFS）を使用すると、Cisco NX-OS デバイスからネットワーク上の他の Cisco NX-OS デバイスに RADIUS 設定を配布できます。使用しているデバイスにおいて、ある機能に対して CFS 配布をイネーブルにすると、そのデバイスは CFS 領域に属します。この CFS 領域には、その機能に対して CFS 配布をイネーブルにしているネットワーク上の他のデバイスが含まれます。RADIUS に対する CFS 配布はデフォルトではディセーブルになっています。

（注） 設定変更を配布する場合は、RADIUS に対する CFS を各デバイスで明示的にイネーブルにする必要があります。

使用している Cisco NX-OS デバイスで RADIUS に対する CFS 配布をイネーブルにした後、最初に入力した RADIUS コンフィギュレーション コマンドによって、Cisco NX-OS ソフトウェアで次の処理が行われます。

- Cisco NX-OS デバイスで CFS セッションを作成します。
- RADIUS に対する CFS がイネーブルにされている CFS 領域で、すべての Cisco NX-OS デバイスの RADIUS 設定をロックします。
- RADIUS の設定変更を Cisco NX-OS デバイスの一時バッファに保存します。

この変更は、CFS 領域にあるデバイスに対して配布するよう明示的にコミットするまで、Cisco NX-OS デバイスの一時バッファに存在します。変更をコミットすると、Cisco NX-OS ソフトウェアが次の処理を実行します。

- Cisco NX-OS デバイスの実行コンフィギュレーションに変更を適用します。
- 更新された RADIUS 設定を CFS 領域内にある他の Cisco NX-OS デバイスに配布します。
- CFS 領域内にある他のデバイスの RADIUS 設定のロックを解除します。
- CFS セッションを終了します。

CFS では RADIUS サーバ グループの設定またはサーバ キーとグローバル キーは配布しません。キーは Cisco NX-OS デバイスに対して一意であり、他の Cisco NX-OS デバイスと共有できません。

CFS の詳細については、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*』を参照してください。

ベンダー固有属性

インターネット技術特別調査委員会（IETF）が、ネットワーク アクセス サーバと RADIUS サーバの間での VSA の通信のための方式を規定する標準を作成しています。IETF は属性 26 を使用します。ベンダーは VSA を使用して、一般的な用途には適さない独自の拡張属性をサポートできます。シスコの RADIUS 実装は、この仕様で推奨される形式を使用して、1 つのベンダー固有オプションをサポートしています。シスコのベンダー ID は 9、サポートされるオプションのベンダータイプは 1（名前付き cisco-av-pair）です。値は次の形式のストリングです。

```
protocol : attribute separator value *
```

protocol は、特定の許可タイプを表すシスコの属性です。separator は、必須属性の場合は =（等号）、オプションの属性の場合は *（アスタリスク）です。

Cisco NX-OS デバイス上の認証に RADIUS サーバを使用した場合、RADIUS プロトコルでは RADIUS サーバに対して、認証結果とともに権限付与情報などのユーザ属性を返すように指示します。この許可情報は、VSA で指定されます。

Cisco NX-OS ソフトウェアでは次の VSA プロトコル オプションをサポートしています。

Shell

ユーザ プロファイル情報を提供する access-accept パケットで使用されるプロトコル。

Accounting

accounting-request パケットで使用されるプロトコル。値にスペースが含まれている場合は、二重引用符で囲む必要があります。

Cisco NX-OS ソフトウェアは、次の属性をサポートしています。

ロール

ユーザが属するすべてのロールの一覧です。値フィールドは、スペースで区切られたロール名を一覧表示したストリングです。たとえば、ユーザが network-operator および vdc-admin のロールに属している場合、値フィールドは network-operator vdc-admin となります。このサブ属性は Access-Accept フレームの VSA 部分に格納され、RADIUS サーバから送信されます。この属性はシェル プロトコル値とだけ併用できます。次に、Cisco Access Control Server（ACS）でサポートされるロール属性の例を示します。

```
shell:roles=network-operator vdc-admin
```

```
shell:roles*"network-operator vdc-admin
```

次に、FreeRADIUS でサポートされるロール属性の例を示します。

```
Cisco-AVPair = shell:roles=\network-operator vdc-admin\
```

```
Cisco-AVPair = shell:roles*\network-operator vdc-admin\
```

（注） VSA を shell:roles*"network-operator vdc-admin" または "shell:roles*\"network-operator vdc-admin\"" として指定した場合、この VSA はオプション属性としてフラグ設定され、他のシスコ デバイスはこの属性を無視します。

accountinginfo

標準の RADIUS アカウンティング プロトコルに含まれる属性とともにアカウンティング情報を格納します。この属性は、スイッチ上の RADIUS クライアントからの Account-Request フレームの VSA 部分だけに送信されます。この属性と共に使用できるのは、アカウンティングのプロトコル データ ユニット（PDU）だけです。

RADIUS のバーチャライゼーション サポート

RADIUS の設定と操作は、仮想デバイス コンテキスト（VDC）に対してローカルです。VDC の詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

Cisco NX-OS デバイスは、仮想ルーティング/転送（VRF）インスタンスを使用して RADIUS サーバにアクセスします。VRF の詳細情報については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

RADIUS のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	RADIUS にはライセンスは必要ありません。ライセンスパッケージに含まれていない機能はすべて Cisco NX-OS システムイメージにバンドルされており、追加費用は一切発生しません。 Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

RADIUS の前提条件

RADIUS には、次の前提条件があります。

- RADIUS サーバの IPv4 または IPv6IP アドレスまたはホスト名を取得していること。
- RADIUS サーバからキーを取得すること。
- Cisco NX-OS デバイスが AAA サーバの RADIUS クライアントとして設定されていることを確認します。

RADIUS の注意事項と制約事項

RADIUS に関する注意事項と制約事項は次のとおりです。

- Cisco NX-OS デバイス上には最大 64 の RADIUS サーバを設定できます。
- ローカルの Cisco NX-OS デバイス上に設定されているユーザ アカウントが、AAA サーバ上のリモート ユーザ アカウントと同じ名前の場合、Cisco NX-OS ソフトウェアは、AAA サーバ上に設定されているユーザ ロールではなく、ローカル ユーザ アカウントのユーザ ロールをリモート ユーザに適用します。
- ワンタイム パスワードをサポートするのは RADIUS プロトコルだけです。

RADIUS のデフォルト設定

次の表に、RADIUS パラメータのデフォルト設定を示します。

表 *10*：*RADIUS* パラメータのデフォルト設定

パラメータ	デフォルト
サーバの役割	認証とアカウンティング

パラメータ	デフォルト
デッド タイマー間隔	0 分
再送信回数	1
再送信タイマー間隔	5 秒
認証ポート	1812
アカウンティング ポート	1813
アイドル タイマー間隔	0 分
サーバの定期的モニタリングのユーザ名	test
サーバの定期的モニタリングのパスワード	test

RADIUS サーバの設定

ここでは、Cisco NX-OS デバイスで RADIUS サーバを設定する手順を説明します。

（注） Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

RADIUS サーバの設定プロセス

1. 必要に応じて、RADIUS のための CFS 配布機能をイネーブルにします。
2. RADIUS サーバと Cisco NX-OS デバイスの接続を確立します。
3. RADIUS サーバの RADIUS 秘密キーを設定します。
4. 必要に応じて、AAA 認証方式用に、RADIUS サーバのサブセットを使用して RADIUS サーバ グループを設定します。
5. 必要に応じて、次のオプションのパラメータを設定します。
   - デッドタイム間隔
   - ユーザ ログイン時の RADIUS サーバの指定の許可
   - タイムアウト間隔
   - TCP ポート

6 （任意）RADIUS設定の配布がイネーブルになっている場合は、ファブリックに対してRADIUS設定をコミットします。

関連トピック

RADIUS サーバ ホストの設定，（84 ページ）
グローバル RADIUS キーの設定，（86 ページ）

RADIUS 設定の配布のイネーブル化

RADIUS 設定の配布がイネーブルになっている Cisco NX-OS デバイスだけが、CFS 領域内での RADIUS 設定変更の配布に参加できます。

はじめる前に

CFS 配布がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **radius distribute**
3. **exit**
4. （任意） **show radius status**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**radius distribute** 例： `switch(config)# radius distribute`	RADIUS設定の配布をイネーブルにします。デフォルトではディセーブルになっています。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

	コマンドまたはアクション	目的
ステップ 4	**show radius status** 例： `switch(config)# show radius status`	（任意） RADIUS CFS 配布の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

RADIUS サーバ ホストの設定

リモートの RADIUS サーバにアクセスするには、RADIUS サーバの IP アドレスまたはホスト名を設定する必要があります。最大 64 の RADIUS サーバを設定できます。

（注） RADIUS サーバの IP アドレスまたはホスト名を Cisco NX-OS デバイスに設定するとき、デフォルトでは RADIUS サーバはデフォルトの RADIUS サーバ グループに追加されます。RADIUS サーバを別の RADIUS サーバ グループに追加することもできます。

はじめる前に

サーバがすでにサーバ グループのメンバーとして設定されていることを確認します。

サーバが RADIUS トラフィックを認証するよう設定されていることを確認します。

Cisco NX-OS デバイスが AAA サーバの RADIUS クライアントとして設定されていることを確認します。

手順の概要

1. **configure terminal**
2. **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*}
3. （任意） **show radius** {**pending** | **pending-diff**}
4. （任意） **radius commit**
5. **exit**
6. （任意） **show radius-server**
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} 例： `switch(config)# radius-server host 10.10.1.1`	認証に使用する RADIUS サーバの IPv4 または IPv6 アドレスまたはホスト名を指定します。
ステップ 3	**show radius** {**pending** | **pending-diff**} 例： `switch(config)# show radius pending`	（任意） 配布するために保留状態になっている RADIUS 設定を表示します。
ステップ 4	**radius commit** 例： `switch(config)# radius commit`	（任意） CFS によるユーザ ロール設定の配布機能をイネーブルにしている場合は、一時データベース内にある RADIUS の設定変更を実行コンフィギュレーションに適用して、RADIUS 設定を他の Cisco NX-OS デバイスに配布します。

ステップ 5	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 6	**show radius-server** 例： `switch# show radius-server`	（任意） RADIUS サーバの設定を表示します。
ステップ 7	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

特定の RADIUS サーバ用のキーの設定，（87 ページ）

グローバル RADIUS キーの設定

Cisco NX-OS デバイスで使用するすべてのサーバの RADIUS キーを設定できます。RADIUS キーは、Cisco NX-OS デバイスと RADIUS サーバ ホストの間の共有秘密テキスト ストリングです。

（注） CFS では RADIUS キーは配布しません。

はじめる前に

リモート RADIUS サーバの RADIUS キーの値を取得します。

リモート RADIUS サーバに RADIUS キーを設定します。

手順の概要

1. **configure terminal**
2. **radius-server key** [**0** | **6** | **7**] *key-value*
3. **exit**
4. （任意） **show radius-server**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**radius-server key** [**0**	**6**	**7**] *key-value* 例： `switch(config)# radius-server key 0 QsEfThUkO`	すべての RADIUS サーバ用の RADIUS キーを指定します。*key-value* がクリアテキスト形式（**0**）か、タイプ 6 暗号化形式（**6**）か、タイプ 7 暗号化形式（**7**）かを指定できます。Cisco NX-OS ソフトウェアでは、実行コンフィギュレーションに保存する前にクリアテキストのキーを暗号化します。デフォルトの形式はクリア テキストです。最大で 63 文字です。 デフォルトでは、RADIUS キーは設定されません。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

	コマンドまたはアクション	目的
ステップ 4	**show radius-server** 例： `switch# show radius-server`	（任意） RADIUS サーバの設定を表示します。 （注） RADIUS キーは実行コンフィギュレーションに暗号化された形式で保存されます。暗号化された RADIUS キーを表示するには、**show running-config** コマンドを使用します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

RADIUS サーバ グループの設定，（89 ページ）
RADIUS 設定の配布，（78 ページ）
AES パスワード暗号化およびマスター暗号キー，（39 ページ）

特定の RADIUS サーバ用のキーの設定

Cisco NX-OS デバイスで特定の RADIUS サーバ用のキーを設定できます。RADIUS キーは、Cisco NX-OS デバイスと特定の RADIUS サーバとの間で共有する秘密テキスト ストリングです。

はじめる前に

1 つまたは複数の RADIUS サーバ ホストを設定します。

リモート RADIUS サーバのキーの値を取得します。

RADIUS サーバにキーを設定します。

手順の概要

1. **configure terminal**
2. **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **key** [**0** | **6** | **7**] *key-value*
3. **exit**
4. （任意） **show radius-server**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **key** [**0** | **6** | **7**] *key-value* 例： `switch(config)# radius-server host 10.10.1.1 key 0 PlIjUhYg`	特定の RADIUS サーバ用の RADIUS キーを指定します。*key-value* がクリアテキスト形式（**0**）か、タイプ 6 暗号化形式（**6**）か、タイプ 7 暗号化形式（**7**）かを指定できます。Cisco NX-OS ソフトウェアでは、実行コンフィギュレーションに保存する前にクリア テキストのキーを暗号化します。デフォルトの形式はクリア テキストです。最大で 63 文字です。 この RADIUS キーが グローバル RADIUS キーの代わりに使用されます。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show radius-server** 例： `switch# show radius-server`	（任意） RADIUS サーバの設定を表示します。 （注） RADIUS キーは実行コンフィギュレーションに暗号化された形式で保存されます。暗号化された RADIUS キーを表示するには、**show running-config** コマンドを使用します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

RADIUS サーバ ホストの設定, （84 ページ）
AES パスワード暗号化およびマスター暗号キー, （39 ページ）

RADIUS サーバ グループの設定

サーバ グループを使用して、1 台または複数台のリモート AAA サーバによる認証を指定できます。グループのメンバーはすべて、RADIUS プロトコルに属している必要があります。設定した順序に従ってサーバが試行されます。VDC には最大 100 のサーバ グループを設定できます。

これらのサーバ グループはいつでも設定できますが、設定したグループを有効にするには、AAA サービスに適用する必要があります。

（注） CFS では RADIUS サーバ グループの設定は配布しません。

はじめる前に

グループ内のすべてのサーバが RADIUS サーバであることを確認します。

手順の概要

1. **configure terminal**
2. **aaa group server radius***group-name*
3. **server** {*ipv4-address* | *ipv6-address* | *host-name*}
4. （任意） **deadtime***minutes*
5. （任意） **server** {*ipv4-address* | *ipv6-address* | *host-name*}
6. （任意） **use-vrf***vrf-name*
7. **exit**
8. （任意） **show radius-server groups** [*group-name*]
9. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**aaa group server radius***group-name*
	
	例：
	`switch(config)# aaa group server radius RadServer`
	`switch(config-radius)#`
		RADIUS サーバ グループを作成し、そのグループの RADIUS サーバ グループ コンフィギュレーション サブモードを開始します。*group-name* 引数は、最大 127 文字の長さの英数字のストリングで、大文字小文字が区別されます。

	コマンドまたはアクション	目的
ステップ 3	**server** {*ipv4-address* | *ipv6-address* | *host-name*} 例： `switch(config-radius)# server 10.10.1.1`	RADIUS サーバを、RADIUS サーバ グループのメンバーとして設定します。 指定した RADIUS サーバが見つからない場合は、**radius-server host** コマンドを使用してサーバを設定し、このコマンドをもう一度実行します。
ステップ 4	**deadtime***minutes* 例： `switch(config-radius)# deadtime 30`	（任意） モニタリング デッド タイムを設定します。デフォルト値は 0 分です。指定できる範囲は 1 ～ 1440 です。 （注） RADIUS サーバ グループのデッド タイム間隔が 0 より大きい場合は、この値がグローバルなデッド タイム値より優先されます。
ステップ 5	**server** {*ipv4-address* | *ipv6-address* | *host-name*} 例： `switch(config-radius)# server 10.10.1.1`	（任意） RADIUS サーバを、RADIUS サーバ グループのメンバーとして設定します。 ヒント 指定した RADIUS サーバが見つからない場合は、**radius-server host** コマンドを使用してサーバを設定し、このコマンドをもう一度実行します。
ステップ 6	**use-vrf***vrf-name* 例： `switch(config-radius)# use-vrf vrf1`	（任意） サーバ グループ内のサーバとの接続に使用する VRF を指定します。

ステップ 7	**exit**
	
	例：
	`switch(config-radius)# exit`
	`switch(config)#`
		設定モードを終了します。

ステップ 8	**show radius-server groups** [*group-name*] 例： `switch(config)# show radius-server groups`	（任意） RADIUS サーバ グループの設定を表示します。
ステップ 9	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

RADIUS デッド タイム間隔の設定, （103 ページ）

RADIUS サーバ グループのためのグローバル発信元インターフェイスの設定

RADIUS サーバ グループにアクセスする際に使用する、RADIUS サーバ グループ用のグローバル発信元インターフェイスを設定できます。また、特定の RADIUS サーバ グループ用に異なる発信元インターフェイスを設定することもできます。デフォルトでは、Cisco NX-OS ソフトウェアは使用可能なあらゆるインターフェイスを使用します。

手順の概要

1. **configure terminal**
2. **ip radius source-interface** *interface*
3. **exit**
4. （任意） **show radius-server**
5. （任意） **copy running-config startup config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**ip radius source-interface** *interface* 例： `switch(config)# ip radius source-interface mgmt 0`	このデバイスで設定されているすべての RADIUS サーバグループ用のグローバル発信元インターフェイスを設定します。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show radius-server** 例： `switch# show radius-server`	（任意） RADIUS サーバの設定情報を表示します。
ステップ 5	**copy running-config startup config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

RADIUS サーバ グループの設定, （89 ページ）

ログイン時にユーザによる RADIUS サーバの指定を許可

デフォルトでは、Cisco NX-OS デバイスはデフォルト AAA 認証方式に基づいて認証要求を転送します。Cisco NX-OS デバイス上で directed-request（誘導要求）オプションをイネーブルにすることにより、認証要求の送信先の VRF および RADIUS サーバをユーザが指定できるようになります。このオプションをイネーブルにした場合、ユーザは *username@vrfname:hostname* としてログインできます。ここで、*vrfname* は使用する VRF、**hostname** は設定された RADIUS サーバの名前です。

（注） directed-request オプションをイネーブルにすると、Cisco NX-OS デバイスでは認証に RADIUS 方式だけを使用し、デフォルトのローカル方式は使用しないようになります。

（注） ユーザ指定のログインは Telnet セッションに限りサポートされます。

手順の概要

1. **configure terminal**
2. **radius-server directed-request**
3. （任意） **show radius {pending | pending-diff}**
4. （任意） **radius commit**
5. **exit**
6. （任意） **show radius-server directed-request**
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**radius-server directed-request** 例： `switch(config)# radius-server directed-request`	ログイン時にユーザが認証要求の送信先となる RADIUS サーバを指定できるようにします。デフォルトでは無効になっています。
ステップ 3	**show radius {pending | pending-diff}** 例： `switch(config)# show radius pending`	（任意） 配布するために保留状態になっている RADIUS 設定を表示します。
ステップ 4	**radius commit** 例： `switch(config)# radius commit`	（任意） CFS によるユーザ ロール設定の配布機能をイネーブルにしている場合は、一時データベース内にある RADIUS の設定変更を実行コンフィギュレーションに適用して、RADIUS 設定を他の Cisco NX-OS デバイスに配布します。

ステップ 5	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 6	**show radius-server directed-request** 例： `switch# show radius-server directed-request`	（任意） directed request の設定を表示します。
ステップ 7	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

RADIUS 設定の配布，（78 ページ）

グローバルな RADIUS 送信リトライ回数とタイムアウト間隔の設定

すべての RADIUS サーバに対するグローバルな再送信リトライ回数とタイムアウト間隔を設定できます。デフォルトでは、Cisco NX-OS デバイスは RADIUS サーバに 1 回だけ送信を再試行してから、ローカル認証に切り換えます。このリトライの回数は、サーバごとに最大 5 回まで増やすことができます。タイムアウト間隔には、Cisco NX-OS デバイスが RADIUS サーバからの応答を待つ時間を指定します。これを過ぎるとタイムアウト エラーになります。

手順の概要

1. **configure terminal**
2. **radius-server retransmit***count*
3. **radius-server timeout***seconds*
4. （任意） **show radius** {**pending** | **pending-diff**}
5. （任意） **radius commit**
6. **exit**
7. （任意） **show radius-server**
8. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**radius-server retransmit***count* 例： `switch(config)# radius-server retransmit 3`	すべての RADIUS サーバの再送信回数を指定します。デフォルトの再送信回数は 1 で、範囲は 0 ～ 5 です。
ステップ 3	**radius-server timeout***seconds* 例： `switch(config)# radius-server timeout 10`	RADIUS サーバの送信タイムアウト間隔を指定します。デフォルトのタイムアウト間隔は 5 秒で、範囲は 1 ～ 60 秒です。
ステップ 4	**show radius** {**pending**	**pending-diff**} 例： `switch(config)# show radius pending`	（任意） 配布するために保留状態になっている RADIUS 設定を表示します。
ステップ 5	**radius commit** 例： `switch(config)# radius commit`	（任意） CFS によるユーザ ロール設定の配布機能をイネーブルにしている場合は、一時データベース内にある RADIUS の設定変更を実行コンフィギュレーションに適用して、RADIUS 設定を他の Cisco NX-OS デバイスに配布します。

ステップ 6	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

	コマンドまたはアクション	目的
ステップ 7	**show radius-server** 例： `switch# show radius-server`	（任意） RADIUS サーバの設定を表示します。
ステップ 8	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

RADIUS 設定の配布，（78 ページ）

サーバに対する RADIUS 送信リトライ回数とタイムアウト間隔の設定

デフォルトでは、Cisco NX-OS デバイスは RADIUS サーバに 1 回だけ送信を再試行してから、ローカル認証に切り換えます。このリトライの回数は、サーバごとに最大 5 回まで増やすことができます。Cisco NX-OS デバイスが RADIUS サーバからの応答を待つタイムアウト間隔も設定できます。これを過ぎるとタイムアウト エラーになります。

はじめる前に

1 つまたは複数の RADIUS サーバ ホストを設定します。

手順の概要

1. **configure terminal**
2. **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **retransmit***count*
3. **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **timeout***seconds*
4. （任意） **show radius** {**pending** | **pending-diff**}
5. （任意） **radius commit**
6. **exit**
7. （任意） **show radius-server**
8. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **retransmit***count* 例： `switch(config)# radius-server host server1 retransmit 3`	特定のサーバに対する再送信回数を指定します。デフォルトはグローバル値です。 （注） 特定の RADIUS サーバに指定した再送信回数は、すべての RADIUS サーバに指定した再送信回数より優先されます。
ステップ 3	**radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **timeout***seconds* 例： `switch(config)# radius-server host server1 timeout 10`	特定のサーバの送信タイムアウト間隔を指定します。デフォルトはグローバル値です。 （注） 特定の RADIUS サーバに指定したタイムアウト間隔は、すべての RADIUS サーバに指定したタイムアウト間隔より優先されます。
ステップ 4	**show radius** {**pending** | **pending-diff**} 例： `switch(config)# show radius pending`	（任意） 配布するために保留状態になっている RADIUS 設定を表示します。
ステップ 5	**radius commit** 例： `switch(config)# radius commit`	（任意） CFS によるユーザ ロール設定の配布機能をイネーブルにしている場合は、一時データベース内にある RADIUS の設定変更を実行コンフィギュレーションに適用して、RADIUS 設定を他の Cisco NX-OS デバイスに配布します。

ステップ 6	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 7	**show radius-server** 例： `switch# show radius-server`	（任意） RADIUS サーバの設定を表示します。
ステップ 8	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

関連トピック

RADIUS サーバ ホストの設定，（84 ページ）
RADIUS 設定の配布，（78 ページ）

RADIUS サーバのアカウンティングおよび認証属性の設定

RADIUS サーバをアカウンティング専用、または認証専用に使用するかを指定できます。デフォルトでは、RADIUS サーバはアカウンティングと認証の両方に使用されます。また、デフォルトのポートとの競合が発生する場合は、RADIUS アカウンティング メッセージと認証メッセージの送信先である宛先 UDP ポート番号を指定することもできます。

はじめる前に

1 つまたは複数の RADIUS サーバ ホストを設定します。

手順の概要

1. **configure terminal**
2. （任意） **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **acct-port***udp-port*
3. （任意） **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **accounting**
4. （任意） **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **auth-port** *udp-port*
5. （任意） **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **authentication**
6. （任意） **show radius** {**pending** | **pending-diff**}
7. （任意） **radius commit**
8. **exit**
9. （任意） **show radius-server**
10. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **acct-port***udp-port* 例： `switch(config)# radius-server host 10.10.1.1 acct-port 2004`	（任意） RADIUS アカウンティングのメッセージに使用する UDP ポートを指定します。デフォルトの UDP ポートは 1813 です。範囲は 0 ～ 65535 です。

	コマンドまたはアクション	目的
ステップ 3	**radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **accounting** 例： `switch(config)# radius-server host 10.10.1.1 accounting`	（任意） RADIUS サーバをアカウンティングだけに使用することを指定します。デフォルトでは、アカウンティングと認証の両方に使用されます。
ステップ 4	**radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **auth-port** *udp-port* 例： `switch(config)# radius-server host 10.10.2.2 auth-port 2005`	（任意） RADIUS 認証メッセージ用の UDP ポートを指定します。デフォルトの UDP ポートは 1812 です。範囲は 0 ～ 65535 です。
ステップ 5	**radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **authentication** 例： `switch(config)# radius-server host 10.10.2.2 authentication`	（任意） RADIUS サーバを認証だけに使用することを指定します。デフォルトでは、アカウンティングと認証の両方に使用されます。
ステップ 6	**show radius** {**pending** | **pending-diff**} 例： `switch(config)# show radius pending`	（任意） 配布するために保留状態になっている RADIUS 設定を表示します。
ステップ 7	**radius commit** 例： `switch(config)# radius commit`	（任意） CFS によるユーザ ロール設定の配布機能をイネーブルにしている場合は、一時データベース内にある RADIUS の設定変更を実行コンフィギュレーションに適用して、RADIUS 設定を他の Cisco NX-OS デバイスに配布します。

ステップ 8	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 9	**show radius-server** 例： `switch(config)# show radius-server`	（任意） RADIUS サーバの設定を表示します。
ステップ 10	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

RADIUS サーバ ホストの設定，（84 ページ）
RADIUS 設定の配布，（78 ページ）

RADIUS サーバのグローバルな定期モニタリングの設定

各サーバに個別にテスト パラメータを設定しなくても、すべての RADIUS サーバの可用性をモニタリングできます。テスト パラメータが設定されていないサーバは、グローバル レベルのパラメータを使用してモニタリングされます。

（注） 各サーバ用に設定されたテスト パラメータは、グローバルのテスト パラメータより優先されます。

グローバル コンフィギュレーション パラメータには、サーバで使用するユーザ名とパスワード、およびアイドル タイマーなどがあります。アイドル タイマーには、RADIUS サーバで何の要求も受信されない状態の時間を指定します。これを過ぎると Cisco NX-OS デバイスはテスト パケットを送信します。このオプションを設定して定期的にサーバをテストしたり、1 回だけテストを実行したりできます。

（注） CFS ではグローバル RADIUS サーバ グループの設定は配布しません。

（注） ネットワークのセキュリティを保護するために、RADIUS データベースの既存のユーザ名と同じものを使用しないことを推奨します。

（注） デフォルトのアイドル タイマー値は 0 分です。アイドル タイム インターバルが 0 分の場合、RADIUS サーバの定期的なモニタリングは実行されません。

はじめる前に

RADIUS をイネーブルにします。

手順の概要

1. **configure terminal**
2. **radius-server test** {**idle-time***minutes* | **password***password* [**idle-time***minutes*] | **username***name* [**password***password* [**idle-time***minutes*]]}
3. **radius-server deadtime***minutes*
4. **exit**
5. （任意） **show radius-server**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**radius-server test** {**idle-time***minutes*	**password***password* [**idle-time***minutes*]	**username***name* [**password***password* [**idle-time***minutes*]]} 例： `switch(config)# radius-server test username user1 password Ur2Gd2BH idle-time 3`	グローバルなサーバモニタリング用のパラメータを指定します。デフォルトのユーザ名は test、デフォルトのパスワードは test です。アイドル タイマーのデフォルト値は 0 分です。有効な範囲は 0 ～ 1440 分です。 （注） RADIUS サーバの定期的なモニタリングを行うには、アイドル タイマーに 0 より大きな値を設定する必要があります。
ステップ 3	**radius-server deadtime***minutes* 例： `switch(config)# radius-server deadtime 5`	以前に応答の遅かった RADIUS サーバを Cisco NX-OS デバイスがチェックを始めるまでの分数を指定します。デフォルト値は 0 分です。有効な範囲は 0 ～ 1440 分です。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 5	**show radius-server** 例： `switch# show radius-server`	（任意） RADIUS サーバの設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

各 RADIUS サーバの定期モニタリングの設定, （101 ページ）

各 RADIUS サーバの定期モニタリングの設定

各 RADIUS サーバの可用性をモニタリングできます。コンフィギュレーション パラメータには、サーバで使用するユーザ名とパスワード、およびアイドル タイマーなどがあります。アイドル タイマーには、RADIUS サーバで何の要求も受信されない状態の時間を指定します。これを過ぎると Cisco NX-OS デバイスはテスト パケットを送信します。このオプションを設定して定期的にサーバをテストしたり、1 回だけテストを実行したりできます。

（注） 各サーバ用に設定されたテスト パラメータは、グローバルのテスト パラメータより優先されます。

（注） セキュリティ上の理由から、RADIUS データベース内の既存のユーザ名と同じテスト ユーザ名を設定しないことを推奨します。

（注） デフォルトのアイドル タイマー値は 0 分です。アイドル時間の間隔が 0 分の場合、Cisco NX-OS デバイスは RADIUS サーバの定期モニタリングを実行しません。

はじめる前に

RADIUS をイネーブルにします。

1 つまたは複数の RADIUS サーバ ホストを追加します。

手順の概要

1. **configure terminal**
2. **radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **test** {**idle-time***minutes* | **password***password* [**idle-time***minutes*] | **username***name* [**password***password* [**idle-time***minutes*]]}
3. **radius-server deadtime***minutes*
4. **exit**
5. （任意） **show radius-server**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**radius-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **test** {**idle-time***minutes* | **password***password* [**idle-time***minutes*] | **username***name* [**password***password* [**idle-time***minutes*]]} 例： `switch(config)# radius-server host 10.10.1.1 test username user1 password Ur2Gd2BH idle-time 3`	サーバ モニタリング用のパラメータを個別に指定します。デフォルトのユーザ名は test、デフォルトのパスワードは test です。アイドル タイマーのデフォルト値は 0 分です。有効な範囲は 0 ～ 1440 分です。 （注） RADIUS サーバの定期的なモニタリングを行うには、アイドル タイマーに 0 より大きな値を設定する必要があります。
ステップ 3	**radius-server deadtime***minutes* 例： `switch(config)# radius-server deadtime 5`	以前に応答の遅かった RADIUS サーバを Cisco NX-OS デバイスがチェックを始めるまでの分数を指定します。デフォルト値は 0 分です。有効な範囲は 1 ～ 1440 分です。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 5	**show radius-server** 例： `switch# show radius-server`	（任意） RADIUS サーバの設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

RADIUS サーバ ホストの設定, （84 ページ）
RADIUS サーバのグローバルな定期モニタリングの設定, （99 ページ）

RADIUS デッド タイム間隔の設定

すべての RADIUS サーバのデッド タイム間隔を設定できます。デッド タイム間隔では、Cisco NX-OS デバイスが RADIUS サーバをデッドであると宣言した後、そのサーバがアライブになったかどうかを確認するためにテスト パケットを送信するまでの時間を指定します。デフォルト値は 0 分です。

（注） デッド タイム間隔が 0 分の場合、RADIUS サーバは、応答を返さない場合でも、デットとしてマークされません。RADIUS サーバ グループに対するデッド タイム間隔を設定できます。

手順の概要

1. **configure terminal**
2. **radius-server dead-time** *minutes*
3. （任意） **show radius** {**pending** | **pending-diff**}
4. （任意） **radius commit**
5. **exit**
6. （任意） **show radius-server**
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**radius-server dead-time** *minutes* 例： `switch(config)# radius-server deadtime 5`	デッド タイム間隔を設定します。デフォルト値は 0 分です。有効な範囲は 1 ～ 1440 分です。
ステップ 3	**show radius** {**pending**	**pending-diff**} 例： `switch(config)# show radius pending`	（任意） 配布するために保留状態になっている RADIUS 設定を表示します。
ステップ 4	**radius commit** 例： `switch(config)# radius commit`	（任意） CFS によるユーザ ロール設定の配布機能をイネーブルにしている場合は、一時データベース内にある RADIUS の設定変更を実行コンフィギュレーションに適用して、

	コマンドまたはアクション	目的
		RADIUS 設定を他の Cisco NX-OS デバイスに配布します。

ステップ 5	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 6	**show radius-server** 例： `switch# show radius-server`	（任意） RADIUS サーバの設定を表示します。
ステップ 7	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

RADIUS サーバ グループの設定，（89 ページ）
RADIUS 設定の配布，（78 ページ）

ワンタイム パスワードの設定

RSA SecurID トークン サーバを使用することで、Cisco NX-OS デバイスでワンタイム パスワード（OTP）をサポートできます。この機能を使用すると、ユーザは、暗証番号（ワンタイムパスワード）とその時点で RSA SecurID トークンに表示されるトークン コードの両方を入力することで、Cisco NX-OS デバイスに対する認証を実行できます。

（注） Cisco NX-OS デバイスにログインするために使用されるトークン コードは、60 秒ごとに変更されます。デバイス検出に関する問題を防ぐために、Cisco Secure ACS 内部データベースに存在する異なるユーザ名を使用することを推奨します。

はじめる前に

Cisco NX-OS デバイスで、RADIUS サーバ ホストとデフォルトのリモート ログイン認証を設定します。

次のものがインストールされていることを確認します。

- Cisco Secure Access Control Server（ACS）Version 4.2

- RSA Authentication Manager Version 7.1（RSA SecurID トークン サーバ）
- RSA ACE Agent/Client

ワンタイム パスワードをサポートするために、Cisco NX-OS デバイスで（RADIUS サーバ ホストとリモート認証以外の）設定を行う必要はありません。ただし、Cisco Secure ACS を次のように設定する必要があります。

1. RSA SecurID トークン サーバ認証をイネーブルにします。
2. RSA SecurID トークン サーバを不明ユーザ ポリシー データベースに追加します。

RADIUS 情報の配布のコミット

一時バッファに保存されている RADIUS のグローバル設定およびサーバ特有の設定を、ファブリック内のすべてのデバイス（元のデバイスを含む）の実行コンフィギュレーションに適用します。

手順の概要

1. **configure terminal**
2. （任意） **show radius** {**pending** | **pending-diff**}
3. **radius commit**
4. **exit**
5. （任意） **show role session status**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**show radius** {**pending**	**pending-diff**} 例： `switch(config)# show radius pending`	（任意） 配布するために保留状態になっている RADIUS 設定を表示します。
ステップ 3	**radius commit** 例： `switch(config)# radius commit`	CFS によるユーザ ロール設定の配布機能をイネーブルにしている場合は、一時データベース内にある RADIUS の設定変更を実行コンフィギュレーションに適用して、RADIUS 設定を他の Cisco NX-OS デバイスに配布します。

	コマンドまたはアクション	目的

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 5	**show role session status** 例： `switch# show role session status`	（任意） ユーザ ロールについての CSF セッションのステータスを表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションに適用します。

RADIUS の配布セッションの廃棄

RADIUS の設定変更の一時データベースを廃棄して、CFS 配布セッションを終了します。

手順の概要

1. **configure terminal**
2. （任意） **show radius** {**pending** | **pending-diff**}
3. **radius abort**
4. **exit**
5. （任意） **show radius session status**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**show radius** {**pending**	**pending-diff**} 例： `switch(config)# show radius pending`	（任意） 配布するために保留状態になっている RADIUS 設定を表示します。

	コマンドまたはアクション	目的
ステップ 3	**radius abort** 例： `switch(config)# radius abort`	一時ストレージにある RADIUS 設定を廃棄して、セッションを終了します。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 5	**show radius session status** 例： `switch# show radius session status`	（任意） RADIUS CFS セッションのステータスを表示します。

RADIUS の配布セッションのクリア

実行中の Cisco Fabric Services の配布セッション（存在する場合）をクリアして、RADIUS 機能のためのファブリックのロックを解除します。

手順の概要

1. **clear radius session**
2. （任意） **show radius session status**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**clear radius session** 例： `switch# clear radius session`	セッションをクリアして、ファブリックのロックを解除します。
ステップ 2	**show radius session status** 例： `switch# show radius session status`	（任意） RADIUS CFS セッションのステータスを表示します。

RADIUS サーバまたはサーバ グループの手動モニタリング

RADIUS サーバまたはサーバ グループに対し手動でテスト メッセージを送信できます。

手順の概要

1. **test aaa server radius** {*ipv4-address* | *ipv6-address* | *host-name*} [**vrf** *vrf-name*] *username password*
2. **test aaa group***group-name username password*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**test aaa server radius** {*ipv4-address* | *ipv6-address* | *host-name*} [**vrf** *vrf-name*] *username password* 例： `switch# test aaa server radius 10.10.1.1 user1 Ur2Gd2BH`	RADIUS サーバにテスト メッセージを送信して可用性を確認します。
ステップ 2	**test aaa group***group-name username password* 例： `switch# test aaa group RadGroup user2 As3He3CI`	RADIUS サーバ グループにテスト メッセージを送信して可用性を確認します。

RADIUS 設定の確認

RADIUS の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show radius {**status** | **pending** | **pending-diff**}	Cisco Fabric Services の RADIUS 設定の配布状況と他の詳細事項を表示します。
show running-config radius [**all**]	実行コンフィギュレーションの RADIUS 設定を表示します。
show startup-config radius	スタートアップ コンフィギュレーションの RADIUS 設定を表示します。
show radius-server [*host-name* | *ipv4-address* | *ipv6-address*] [**directed-request** | **groups** | **sorted** | **statistics**]	設定済みのすべての RADIUS サーバのパラメータを表示します。

このコマンドの出力フィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

RADIUS サーバのモニタリング

Cisco NX-OS デバイスが保持している RADIUS サーバのアクティビティに関する統計情報をモニタリングできます。

はじめる前に

1 つまたは複数の RADIUS サーバ ホストを設定します。

手順の概要

1. **show radius-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show radius-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*} 例： `switch# show radius-server statistics 10.10.1.1`	RADIUS 統計情報を表示します。

関連トピック

RADIUS サーバ ホストの設定，（84 ページ）
RADIUS サーバ統計情報のクリア，（109 ページ）

RADIUS サーバ統計情報のクリア

Cisco NX-OS デバイスが保持している RADIUS サーバのアクティビティに関する統計情報を表示します。

はじめる前に

Cisco NX-OS デバイスに RADIUS サーバを設定します。

手順の概要

1. （任意） **show radius-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*}
2. **clear radius-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show radius-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*} 例： `switch# show radius-server statistics 10.10.1.1`	（任意） Cisco NX-OS デバイスでの RADIUS サーバ統計情報を表示します。
ステップ 2	**clear radius-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*} 例： `switch# clear radius-server statistics 10.10.1.1`	RADIUS サーバ統計情報をクリアします。

関連トピック

RADIUS サーバ ホストの設定, （84 ページ）

RADIUS の設定例

次に、RADIUS を設定する例を示します。

```
radius-server key 7 "ToIkLhPpG"
radius-server host 10.10.1.1 key 7 "ShMoMhTl" authentication accounting
aaa group server radius RadServer
    server 10.10.1.1
```

次の作業

これで、サーバ グループも含めて AAA 認証方式を設定できるようになります。

RADIUS に関する追加情報

ここでは、RADIUS の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS ライセンス設定	『*Cisco NX-OS Licensing Guide*』
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』

関連項目	マニュアル タイトル
VRF コンフィギュレーション	『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
• CISCO-AAA-SERVER-MIB • CISCO-AAA-SERVER-EXT-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

RADIUS の機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 *11*：*RADIUS* の機能の履歴

機能名	リリース	機能情報
RADIUS	6.0(1)	Release 5.2 以降、変更はありません。
RADIUS	5.2(1)	Cisco Nexus 3000 シリーズ スイッチのサポートが追加されました。
RADIUS	5.2(1)	RADIUS サーバ キーのタイプ 6 暗号化が追加されました。
RADIUS	5.1(1)	Release 5.0 以降、変更はありません。

機能名	リリース	機能情報
RADIUS サーバ グループ	5.0(2)	すべての RADIUS サーバ グループ用のグローバル発信元インターフェイスの設定のサポートが追加されました。
RADIUS サーバ グループ	5.0(2)	特定の RADIUS サーバ グループ用の発信元インターフェイスの設定のサポートが追加されました。
定期サーバ モニタリング	5.0(2)	RADIUS サーバのグローバルな定期モニタリングのサポートが追加されました。
OTP	5.0(2)	ワンタイムパスワードのサポートが追加されました。
RADIUS 統計情報	4.2(1)	RADIUS サーバ ホストの統計情報のクリアのサポートが追加されました。
RADIUS	4.2(1)	リリース 4.1 からの変更はありません。

第 6 章

TACACS+ の設定

この章では、Cisco NX-OS デバイス上で Terminal Access Controller Access Control System Plus（TACACS+）プロトコルを設定する手順について説明します。

この章は、次の項で構成されています。

- 機能情報の確認，113 ページ
- TACACS+ の概要，114 ページ
- TACACS+ のライセンス要件，119 ページ
- TACACS+ の前提条件，119 ページ
- TACACS+ の注意事項と制約事項，119 ページ
- TACACS+ のデフォルト設定，120 ページ
- TACACS+ の設定，120 ページ
- TACACS+ サーバのモニタリング，160 ページ
- TACACS+ サーバ統計情報のクリア，160 ページ
- TACACS+ の設定の確認，161 ページ
- TACACS+ の設定例，162 ページ
- 次の作業，163 ページ
- TACACS+ に関する追加情報，163 ページ
- TACACS+ の機能の履歴，164 ページ

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。こ

のモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

TACACS+ の概要

TACACS+ は、Cisco NX-OS デバイスにアクセスしようとするユーザの検証を集中的に行うセキュリティ プロトコルです。TACACS+ サービスは、通常 UNIX または Windows NT ワークステーション上で動作する TACACS+ デーモンのデータベースで管理されます。Cisco NX-OS デバイスに設定した TACACS+ 機能を使用可能にするには、TACACS+ サーバにアクセスして TACACS+ サーバを設定しておく必要があります。

TACACS+ では、認証、許可、アカウンティングの各ファシリティを個別に提供します。TACACS+ では、単一のアクセス コントロール サーバ（TACACS+ デーモン）が各サービス（認証、許可、およびアカウンティング）を別個に提供します。各サービスを固有のデータベースに結合し、デーモンの機能に応じてそのサーバまたはネットワークで使用できる他のサービスを使用できます。

TACACS+ クライアント/サーバ プロトコルでは、トランスポート要件を満たすため TCP（TCP ポート 49）を使用します。Cisco NX-OS デバイスは、TACACS+ プロトコルを使用して集中型の認証を行います。

TACACS+ の利点

TACACS+ には、RADIUS 認証にはない次の利点があります。

- 独立した AAA ファシリティを提供する。たとえば Cisco NX-OS デバイスは、認証を行わずにアクセスを許可できます。
- AAA クライアントとサーバ間のデータ送信に TCP トランスポート プロトコルを使用しているため、コネクション型プロトコルによる確実な転送を実行します。
- スイッチと AAA サーバ間でプロトコル ペイロード全体を暗号化して、高度なデータ機密性を実現します。RADIUS プロトコルはパスワードだけを暗号化します。

ユーザ ログインにおける TACACS+ の動作

TACACS+ を使用する Cisco NX-OS デバイスに対して、ユーザがパスワード認証プロトコル（PAP）ログインを試みると、次の処理が行われます。

（注） TACACS+ では、デーモンがユーザを認証するために十分な情報を得られるまで、デーモンとユーザとの自由な対話を許可します。通常、デーモンはユーザ名とパスワードを入力するよう求めますが、ユーザの母親の旧姓などの追加項目を求めることもできます。

1 Cisco NX-OS デバイスは接続が確立されると、ユーザ名とパスワードを取得するために TACACS+ デーモンに接続します。

2 Cisco NX-OS デバイスは、最終的に TACACS+ デーモンから次のいずれかの応答を得ます。

ACCEPT

ユーザの認証に成功したので、サービスを開始します。Cisco NX-OS デバイスがユーザ許可を必要とする場合は、許可処理が始まります。

REJECT

ユーザの認証に失敗しました。TACACS+ デーモンは、ユーザに対してそれ以上のアクセスを拒否するか、ログイン シーケンスを再試行するよう要求します。

ERROR

デーモンによる認証サービスの途中でエラーが発生したか、またはデーモンと Cisco NX-OS デバイスの間のネットワーク接続でエラーが発生しました。Cisco NX-OS デバイスは ERROR 応答を受信した場合、別の方法でユーザの認証を試行します。

認証が終了し、NX-OS デバイスで許可がイネーブルになっていれば、続いてユーザの許可フェーズに入ります。ユーザは TACACS+ 許可に進む前に、まず TACACS+ 認証を正常に完了する必要があります。

3 TACACS+ 許可が必要な場合、Cisco NX-OS デバイスは再び TACACS+ デーモンに接続します。デーモンから ACCEPT または REJECT 応答が返されます。ACCEPT 応答には、ユーザに対する EXEC または NETWORK セッションの送信に使用される属性が含まれます。また ACCEPT 応答により、ユーザがアクセス可能なサービスが決まります。

この場合のサービスは次のとおりです。

- Telnet、rlogin、ポイントツーポイント プロトコル（PPP）、シリアル ライン インターネット プロトコル（SLIP）、EXEC サービス
- 接続パラメータ（ホストまたはクライアントの IP アドレス（IPv4 または IPv6）、アクセス リスト、ユーザ タイムアウト）

デフォルトの TACACS+ サーバ暗号化タイプおよび秘密キー

スイッチを TACACS+ サーバに対して認証するには、TACACS+ 秘密キーを設定する必要があります。秘密キーは、Cisco NX-OS デバイスと TACACS+ サーバ ホストの間で共有される秘密テキスト ストリングです。キーの長さは 63 文字で、出力可能な任意の ASCII 文字を含めることができます（スペースは使用できません）。Cisco NX-OS デバイス上のすべての TACACS+ サーバの設定には、グローバル事前共有キーを使用できます。

グローバルな秘密キーの設定は、個々の TACACS+ サーバの設定時に明示的に **key** オプションを使用することによって無効にできます。

TACACS+ サーバのコマンド許可サポート

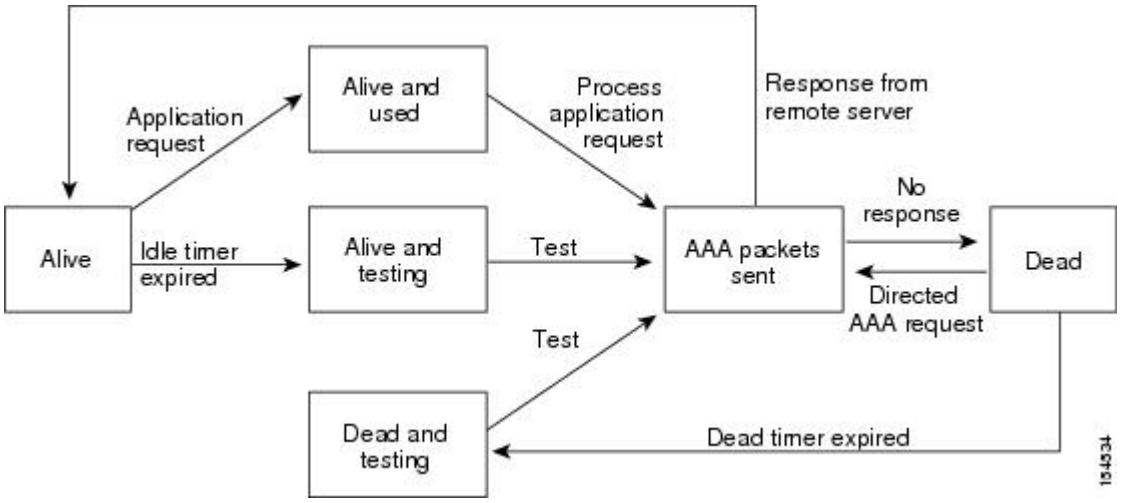
デフォルトでは、認証されたユーザがコマンドライン インターフェイス（CLI）でコマンドを入力したときに、Cisco NX-OS ソフトウェアのローカル データベースに対してコマンド許可が行われます。また、TACACS+ を使用して、認証されたユーザに対して許可されたコマンドを確認することもできます。

TACACS+ サーバのモニタリング

応答を返さない TACACS+ サーバがあると、AAA 要求の処理に遅延が発生する可能性があります。AAA 要求の処理時間を短縮するために、TACACS+ サーバを定期的にモニタして TACACS+ サーバが応答している（アライブ）かどうかを調べることができます。Cisco NX-OS デバイスは、応答の遅い TACACS+ サーバをデッド（dead）としてマークし、デッド TACACS+ サーバには AAA 要求を送信しません。Cisco NX-OS デバイスはデッド TACACS+ サーバを定期的にモニタし、応答があればアライブ状態に戻します。このモニタリング プロセスでは、実際の AAA 要求が送信される前に、TACACS+ サーバが稼働状態であることを確認します。TACACS+ サーバがデッドまたはアライブの状態に変わると簡易ネットワーク管理プロトコル（SNMP）トラップが生成され、Cisco NX-OS デバイスはパフォーマンスに影響が出る前に、障害が発生していることをエラー メッセージで表示します。

次の図に、TACACS+ サーバ モニタリングのサーバの状態を示します。

図 *3*：*TACACS+* サーバの状態



（注） アライブ サーバとデッド サーバのモニタリング間隔は異なります。これらはユーザが設定できます。TACACS+ サーバ モニタリングを実行するには、テスト認証要求を TACACS+ サーバに送信します。

TACACS+ 設定の配布

Cisco Fabric Services（CFS）を使用すると、Cisco NX-OS デバイスからネットワーク上の他の Cisco NX-OS デバイスに TACACS+ 設定および権限ロールを配布できます。使用しているデバイスにおいて、ある機能に対して CFS 配布をイネーブルにすると、そのデバイスは CFS 領域に属します。この CFS 領域には、その機能に対して CFS 配布をイネーブルにしているネットワーク上の他のデバイスが含まれます。TACACS+ に対する CFS 配布はデフォルトではディセーブルになっています。

（注） 設定変更を配布する場合は、TACACS+ に対する CFS を各デバイスで明示的にイネーブルにする必要があります。

使用している Cisco NX-OS デバイスで TACACS+ に対する CFS 配布をイネーブルにした後、最初に入力した TACACS+ コンフィギュレーション コマンドによって、Cisco NX-OS ソフトウェアで次の処理が行われます。

- Cisco NX-OS デバイスで CFS セッションを作成します。
- TACACS+ に対する CFS がイネーブルにされている CFS 領域で、すべての Cisco NX-OS デバイスの TACACS+ 設定をロックします。
- TACACS+ の設定変更を Cisco NX-OS デバイスの一時バッファに保存します。

この変更は、CFS 領域にあるデバイスに対して配布するよう明示的にコミットするまで、Cisco NX-OS デバイスの一時バッファに存在します。変更をコミットすると、Cisco NX-OS ソフトウェアが次の処理を実行します。

- Cisco NX-OS デバイスの実行コンフィギュレーションに変更を適用します。
- 更新された TACACS+ 設定を CFS 領域内にある他の Cisco NX-OS デバイスに配布します。
- CFS 領域内にある他のデバイスの TACACS+ 設定のロックを解除します。
- CFS セッションを終了します。

CFS では TACACS+ サーバ グループの設定、定期的な TACACS+ サーバのテスト設定、およびサーバ キーとグローバル キーは配布しません。キーは Cisco NX-OS デバイスに対して一意であり、他の Cisco NX-OS デバイスと共有できません。

CFS の詳細については、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*』を参照してください。

TACACS+ のベンダー固有属性

インターネット技術特別調査委員会（IETF）ドラフト標準には、ネットワーク アクセス サーバと TACACS+ サーバの間でベンダー固有属性（VSA）を伝達する方法が規定されています。IETF は

属性 26 を使用します。ベンダーは VSA を使用して、一般的な用途には適さない独自の拡張属性をサポートできます。

TACACS+ 用の Cisco VSA 形式

シスコの TACACS+ 実装では、IETF 仕様で推奨される形式を使用したベンダー固有のオプションを 1 つサポートしています。シスコのベンダー ID は 9、サポートされるオプションのベンダー タイプは 1（名前付き cisco-av-pair）です。値は次の形式のストリングです。

```
protocol : attribute separator value *
```

protocol は、特定の許可タイプを表すシスコの属性です。separator は、必須属性の場合は =（等号）、オプションの属性の場合は *（アスタリスク）です。

Cisco NX-OS デバイスでの認証に TACACS+ サーバを使用した場合、TACACS+ プロトコルは TACACS+ サーバに対し、認証結果とともに権限付与情報などのユーザ属性を返すように指示します。この許可情報は、VSA で指定されます。

Cisco NX-OS ソフトウェアでは次の VSA プロトコル オプションをサポートしています。

Shell

ユーザ プロファイル情報を提供する access-accept パケットで使用されるプロトコル。

Accounting

accounting-request パケットで使用されるプロトコル。値にスペースが含まれている場合は、二重引用符で囲む必要があります。

Cisco NX-OS ソフトウェアは、次の属性をサポートしています。

ロール

ユーザが属するすべてのロールの一覧です。値フィールドは、スペースで区切られたロール名を一覧表示したストリングです。たとえば、ユーザが network-operator および vdc-admin のロールに属している場合、値フィールドは network-operator vdc-admin となります。このサブ属性は Access-Accept フレームの VSA 部分に格納され、TACACS+ サーバから送信されます。この属性はシェルプロトコル値とだけ併用できます。次に、Cisco ACS でサポートされるロール属性の例を示します。

```
shell:roles=network-operator vdc-admin
```

```
shell:roles*network-operator vdc-admin
```

（注） VSA を shell:roles*"network-operator vdc-admin" として指定した場合、この VSA はオプション属性としてフラグ設定され、他のシスコ デバイスはこの属性を無視します。

accountinginfo

標準の TACACS+ アカウンティング プロトコルに含まれる属性とともにアカウンティング情報を格納します。この属性は、スイッチ上の TACACS+ クライアントから、Account-Request フレームの VSA 部分にだけ格納されて送信されます。この属性と共に使用できるのは、アカウンティングのプロトコル データ ユニット（PDU）だけです。

TACACS+ のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	TACACS+ にはライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。 Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

TACACS+ の前提条件

TACACS+ には、次の前提条件があります。

- TACACS+ サーバの IPv4 または IPv6 アドレスまたはホスト名を取得すること。
- TACACS+ サーバから秘密キーを取得すること（ある場合）。
- Cisco NX-OS デバイスが AAA サーバの TACACS+ クライアントとして設定されていること。

TACACS+ の注意事項と制約事項

TACACS+ に関する注意事項と制約事項は次のとおりです。

- Cisco NX-OS デバイス上には最大 64 の TACACS+ サーバを設定できます。
- ローカルの Cisco NX-OS デバイス上に設定されているユーザ アカウントが、AAA サーバ上のリモート ユーザ アカウントと同じ名前の場合、Cisco NX-OS ソフトウェアは、AAA サーバ上に設定されているユーザ ロールではなく、ローカル ユーザ アカウントのユーザ ロールをリモート ユーザに適用します。
- グループ内に 6 台以上のサーバが設定されている場合は、デッドタイム間隔を設定することを推奨します。6 台以上のサーバを設定する必要がある場合は、デッド タイム間隔を 0 より

大きな値に設定し、テスト ユーザ名とテスト パスワードを設定することで、デッド サーバのモニタリングを有効にしてください。

- Cisco NX-OS Release 4.x および 5.x の場合、TACACS+ サーバ上のコマンド許可は、コンソール以外のセッションでのみ使用可能です。コンソールを使用してサーバにログインすると、コマンド認可はディセーブルになります。Cisco NX-OS Release 6.0 から、TACACS+ サーバ上のコマンド許可は、コンソールセッションとコンソール以外のセッションの両方で使用可能になりました。

TACACS+ のデフォルト設定

次の表に、TACACS+ パラメータのデフォルト設定値を示します。

表 *12* : *TACACS+* パラメータのデフォルト設定

パラメータ	デフォルト
TACACS+	ディセーブル
デッド タイマー間隔	0 分
タイムアウト間隔	5 秒
アイドル タイマー間隔	0 分
サーバの定期的モニタリングのユーザ名	test
サーバの定期的モニタリングのパスワード	test
TACACS+ 許可の特権レベル サポート	ディセーブル

TACACS+ の設定

ここでは、Cisco NX-OS デバイスで TACACS+ を設定する手順を説明します。

（注） Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

TACACS+ サーバの設定プロセス

ステップ 1 TACACS+ をイネーブルにします。
ステップ 2 必要であれば、TACACS+ のための CFS 配布機能をイネーブルにします。
ステップ 3 TACACS+ サーバと Cisco NX-OS デバイスの接続を確立します。
ステップ 4 TACACS+ サーバの秘密キーを設定します。
ステップ 5 必要に応じて、AAA 認証方式用に、TACACS+ サーバのサブセットを使用して TACACS+ サーバ グループを設定します。
ステップ 6 （任意）TCP ポートを設定します。
ステップ 7 （任意）必要に応じて、TACACS+ サーバの定期モニタリングを設定します。
ステップ 8 （任意）TACACS+ の配布がイネーブルになっている場合は、ファブリックに対して TACACS+ 設定をコミットします。

関連トピック

TACACS+ のイネーブル化，（121 ページ）

TACACS+ のイネーブル化

デフォルトでは、Cisco NX-OS デバイスの TACACS+ 機能はディセーブルになっています。認証に関するコンフィギュレーション コマンドと検証コマンドを使用するには、TACACS+ 機能を明示的にイネーブルにする必要があります。

手順の概要

1. **configure terminal**
2. **feature tacacs+**
3. **exit**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**feature tacacs+** 例： `switch(config)# feature tacacs+`	TACACS+ をイネーブルにします。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

TACACS+ サーバ ホストの設定

リモートの TACACS+ サーバにアクセスするには、Cisco NX-OS デバイス上でその TACACS+ サーバの IP アドレスかホスト名を設定する必要があります。最大 64 の TACACS+ サーバを設定できます。

（注） TACACS+ サーバの IP アドレスまたはホスト名を Cisco NX-OS デバイスに設定するとき、デフォルトでは TACACS+ サーバはデフォルトの TACACS+ サーバ グループに追加されます。TACACS+ サーバは別の TACACS+ サーバ グループに追加することもできます。

はじめる前に

TACACS+ をイネーブルにします。

リモート TACACS+ サーバの IP アドレス（IPv4 または IPv6）またはホスト名を取得していること。

手順の概要

1. **configure terminal**
2. **tacacs-server host** {*host-name* | *ipv4-address* | *ipv6-address*} [**key** [**0** | **6** | **7**] *shared-secret*] [**port** *port-number*] [**timeout** *seconds*] [**single-connection**]
3. （任意） **show tacacs+** {**pending** | **pending-diff**}
4. （任意） **tacacs+ commit**
5. **exit**
6. （任意） **show tacacs-server**
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**tacacs-server host** {*host-name* | *ipv4-address* | *ipv6-address*} [**key** [**0** | **6** | **7**] *shared-secret*] [**port** *port-number*] [**timeout** *seconds*] [**single-connection**] 例： `switch(config)# tacacs-server host 10.10.2.2`	TACACS+ サーバの IP アドレス（IPv4 または IPv6）、またはホスト名を指定します。 単一の TACACS+ 接続を設定することでパフォーマンスを改善するには、**single-connection** オプションを使用します。通信が必要になるたびに、デバイスを開き、デーモンへの TCP 接続を閉じるのではなく、このオプションによって、デバイスとデーモン間の単一のオープンな接続を保守します。
ステップ 3	**show tacacs+** {**pending** | **pending-diff**} 例： `switch(config)# show tacacs+ pending`	（任意） 配布するために保留状態になっている TACACS+ 設定を表示します。
ステップ 4	**tacacs+ commit** 例： `switch(config)# tacacs+ commit`	（任意） CFS によるユーザ ロール設定の配布機能をイネーブルにしている場合は、一時データベース内にある TACACS+ の設定変更を実行コンフィギュレーションに適用して、TACACS+ 設定を他の NX-OS デバイスに配布します。

ステップ 5	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

	コマンドまたはアクション	目的
ステップ 6	**show tacacs-server** 例： `switch# show tacacs-server`	（任意） TACACS+ サーバの設定を表示します。
ステップ 7	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

TACACS+ のイネーブル化，（121 ページ）
TACACS+ 設定の配布のイネーブル化，（154 ページ）
TACACS+ サーバ グループの設定，（127 ページ）

グローバル TACACS+ キーの設定

Cisco NX-OS デバイスで使用されるすべてのサーバ用の秘密 TACACS+ キーをグローバル レベルで設定できます。秘密キーは、Cisco NX-OS デバイスと TACACS+ サーバ ホストのと間の共有秘密テキスト ストリングです。

（注） CFS ではグローバル TACACS+ キーを配布しません。キーは Cisco NX-OS デバイスに対して一意であり、他の Cisco NX-OS デバイスと共有できません。

はじめる前に

TACACS+ をイネーブルにします。

リモート TACACS+ サーバの秘密キーの値を取得します。

手順の概要

1. **configure terminal**
2. **tacacs-server key** [**0** | **6** | **7**] *key-value*
3. **exit**
4. （任意） **show tacacs-server**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**tacacs-server key** [**0** | **6** | **7**] *key-value* 例： `switch(config)# tacacs-server key 0 QsEfThUkO`	すべての TACACS+ サーバ用の TACACS+ キーを指定します。*key-value* がクリアテキスト形式（**0**）か、タイプ 6 暗号化形式（**6**）か、タイプ 7 暗号化形式（**7**）かを指定できます。Cisco NX-OS ソフトウェアでは、実行コンフィギュレーションに保存する前にクリアテキストのキーを暗号化します。デフォルトの形式はクリア テキストです。最大で 63 文字です。 デフォルトでは、秘密キーは設定されていません。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show tacacs-server** 例： `switch# show tacacs-server`	（任意） TACACS+ サーバの設定を表示します。 （注）　秘密キーは実行コンフィギュレーションに暗号化された形式で保存されます。暗号化された秘密キーを表示するには、**show running-config** コマンドを使用します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

TACACS+ のイネーブル化，（121 ページ）
TACACS+ 設定の配布のイネーブル化，（154 ページ）
AES パスワード暗号化およびマスター暗号キー，（39 ページ）

特定の TACACS+ サーバ用のキーの設定

TACACS+ サーバの秘密キーを設定できます。秘密キーは、Cisco NX-OS デバイスと TACACS+ サーバ ホストとの間の共有秘密テキスト ストリングです。

（注） CFS では TACACS+ サーバのキーを配布しません。キーは Cisco NX-OS デバイスに対して一意であり、他の Cisco NX-OS デバイスと共有できません。

はじめる前に

TACACS+ をイネーブルにします。

リモート TACACS+ サーバの秘密キーの値を取得します。

手順の概要

1. **configure terminal**
2. **tacacs-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **key** [**0** | **6** | **7**] *key-value*
3. **exit**
4. （任意） **show tacacs-server**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**tacacs-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **key** [**0** | **6** | **7**] *key-value* 例： `switch(config)# tacacs-server host 10.10.1.1 key 0 PlIjUhYg`	特定の TACACS+ サーバの秘密キーを指定します。**key** オプションを使用すると、秘密キーの形式を指定できます。 • *key-value* をクリア テキスト形式で入力する場合は、**key 0** を指定します • *key-value* をタイプ 6 暗号化形式で入力する場合は、**key 6** を指定します • *key-value* をタイプ 7 暗号化形式で入力する場合は、**key 7** を指定します key が指定されていない場合、*key-value* はクリア テキストと見なされ、実行コンフィギュレーションに保存される前にタイプ 7 暗号化を使用して暗号化されます。*key-value* の最大長は 63 文字です

	コマンドまたはアクション	目的
		グローバル秘密キーではなく、この秘密キーが使用されます。 （注） タイプ 6 暗号化では、AES 暗号とユーザ定義のマスター キーが使用されます。このマスタ キーがない場合、タイプ 6 のキーは使用できません。マスター キーはユーザにより定義され、設定には表示されません。タイプ 6 パスワードを使用すると安全性がより高くなります。 タイプ 7 暗号化では、脆弱な暗号と OS に組み込まれた暗号化キーが使用されます。暗号化と復号のキーが OS に組み込まれているため、特定のデバイスで設定されたタイプ 7 パスワードは他のデバイスでも復号することができます。

ステップ 3	**exit**
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show tacacs-server** 例： `switch# show tacacs-server`	（任意） TACACS+ サーバの設定を表示します。 （注） 秘密キーは実行コンフィギュレーションに暗号化された形式で保存されます。暗号化された秘密キーを表示するには、**show running-config** コマンドを使用します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

AES パスワード暗号化およびマスター暗号キー，（39 ページ）

TACACS+ サーバ グループの設定

サーバ グループを使用して、1 台または複数台のリモート AAA サーバによるユーザ認証を指定することができます。グループのメンバーはすべて、TACACS+ プロトコルに属している必要があります。設定した順序に従ってサーバが試行されます。

これらのサーバ グループはいつでも設定できますが、設定したグループを有効にするには、AAA サービスに適用する必要があります。

（注） CFS では TACACS+ サーバ グループの設定は配布しません。

はじめる前に

TACACS+ をイネーブルにします。

手順の概要

1. **configure terminal**
2. **tacacs-server host** {*host-name* | *ipv4-address* | *ipv6-address*} [**key** [**0** | **6** | **7**] *shared-secret*] [**port** *port-number*] [**timeout** *seconds*] [**single-connection**]
3. **aaa group server tacacs+***group-name*
4. **server** {*ipv4-address* | *ipv6-address* | *host-name*}
5. **exit**
6. （任意） **show tacacs-server groups**
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**tacacs-server host** {*host-name* | *ipv4-address* | *ipv6-address*} [**key** [**0** | **6** | **7**] *shared-secret*] [**port** *port-number*] [**timeout** *seconds*] [**single-connection**]
	
	例：
	`switch(config)# tacacs-server host 10.10.2.2`
	`switch(config-tacacs+)#`
		TACACS+ サーバの IP アドレス（IPv4 または IPv6）、またはホスト名を指定します。
		単一の TACACS+ 接続を設定することでパフォーマンスを改善するには、**single-connection** オプションを使用します。通信が必要になるたびに、デバイスを開き、デーモンへの TCP 接続を閉じるのではなく、このオプションによって、デバイスとデーモン間の単一のオープンな接続を保守します。

ステップ 3	**aaa group server tacacs+***group-name*
	
	例：
	`switch(config)# aaa group server tacacs+ TacServer`
	`switch(config-tacacs+)#`
		TACACS+ サーバ グループを作成し、そのグループの TACACS+ サーバ グループ コンフィギュレーション モードを開始します。

ステップ 4	**server** {*ipv4-address* | *ipv6-address* | *host-name*} 例： `switch(config-tacacs+)# server 10.10.2.2`	TACACS+ サーバを、TACACS+ サーバ グループのメンバーとして設定します。

	コマンドまたはアクション	目的
		指定した TACACS+ サーバが見つからない場合は、**tacacs-server host** コマンドを使用してサーバを設定し、このコマンドをもう一度実行します。

ステップ 5	**exit**
	
	例：
	`switch(config-tacacs+)# exit`
	`switch(config)#`
		TACACS+ サーバ グループ コンフィギュレーション モードを終了します。

ステップ 6	**show tacacs-server groups** 例： `switch(config)# show tacacs-server groups`	（任意） TACACS+ サーバ グループの設定を表示します。
ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

TACACS+ のイネーブル化，（121 ページ）
リモート AAA サービス，（35 ページ）
TACACS+ サーバ ホストの設定，（122 ページ）
TACACS+ デッド タイム間隔の設定，（141 ページ）

TACACS+サーバグループのためのグローバル発信元インターフェイスの設定

TACACS+ サーバ グループにアクセスする際に使用する、TACACS+ サーバ グループ用のグローバル発信元インターフェイスを設定できます。また、特定の TACACS+ サーバ グループ用に異なる発信元インターフェイスを設定することもできます。デフォルトでは、Cisco NX-OS ソフトウェアは使用可能なあらゆるインターフェイスを使用します。

手順の概要

1. **configure terminal**
2. **ip tacacs source-interface** *interface*
3. **exit**
4. （任意） **show tacacs-server**
5. （任意） **copy running-config startup config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**ip tacacs source-interface** *interface* 例： `switch(config)# ip tacacs source-interface mgmt 0`	このデバイスで設定されているすべての TACACS+ サーバ グループ用のグローバル発信元インターフェイスを設定します。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show tacacs-server** 例： `switch# show tacacs-server`	（任意） TACACS+ サーバの設定情報を表示します。
ステップ 5	**copy running-config startup config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

TACACS+ のイネーブル化，（121 ページ）
TACACS+ サーバ グループの設定，（127 ページ）

ユーザによるログイン時の TACACS+ サーバ指定の許可

スイッチ上で directed-request（誘導要求）オプションをイネーブルにすることにより、認証要求の送信先の TACACS+ サーバをユーザが指定できるようになります。デフォルトでは、Cisco NX-OS デバイスは認証要求を、デフォルト AAA 認証方式に基づいて転送します。このオプションをイネーブルにすると、ユーザは *username@vrfname:hostname* としてログインできます。*vrfname* は使用する VRF、*hostname* は設定する TACACS+ サーバの名前です。

（注） directed-request オプションをイネーブルにすると、Cisco NX-OS デバイスでは認証に TACACS+ 方式だけを使用し、デフォルトのローカル方式は使用しないようになります。

（注） ユーザ指定のログインは Telnet セッションに限りサポートされます。

はじめる前に

TACACS+ をイネーブルにします。

手順の概要

1. **configure terminal**
2. **tacacs-server directed-request**
3. （任意） **show tacacs+ {pending | pending-diff}**
4. （任意） **tacacs+ commit**
5. **exit**
6. （任意） **show tacacs-server directed-request**
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**tacacs-server directed-request** 例： `switch(config)# tacacs-server directed-request`	ログイン時にユーザが認証要求の送信先となる TACACS+ サーバを指定できるようにします。デフォルトでは無効になっています。

	コマンドまたはアクション	目的
ステップ 3	**show tacacs+ {pending | pending-diff}** 例： `switch(config)# show tacacs+ pending`	（任意） 保留状態になっている TACACS+ 設定を表示します。
ステップ 4	**tacacs+ commit** 例： `switch(config)# tacacs+ commit`	（任意） CFS によるユーザ ロール設定の配布機能をイネーブルにしている場合は、一時データベース内にある TACACS+ の設定変更を実行コンフィギュレーションに適用して、TACACS+ 設定を他の NX-OS デバイスに配布します。

ステップ 5	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 6	**show tacacs-server directed-request** 例： `switch# show tacacs-server directed-request`	（任意） TACACS+ の directed request の設定を表示します。
ステップ 7	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

TACACS+ のイネーブル化，（121 ページ）
TACACS+ 設定の配布のイネーブル化，（154 ページ）

グローバルな TACACS+ タイムアウト間隔の設定

デバイスがすべての TACACS+ サーバからの応答を待つグローバルなタイムアウト間隔を設定できます。これを過ぎるとタイムアウト エラーになります。タイムアウト間隔には、デバイスが TACACS+ サーバからの応答を待つ時間を指定します。これを過ぎるとタイムアウト エラーになります。

はじめる前に

TACACS+ をイネーブルにします。

手順の概要

1. [Feature Selector] ペインで、[Security] > [AAA] > [Server Groups] を選択します。
2. [Summary] ペインで、デバイスをダブルクリックしてサーバ グループを表示します。
3. [Default TACACS Server Group] をクリックします。
4. [Details] ペインで、[Global Settings] タブをクリックします。
5. [Time out(secs)] フィールドに、タイムアウト間隔の秒数を入力します。
6. メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。

手順の詳細

ステップ 1 [Feature Selector] ペインで、[Security] > [AAA] > [Server Groups] を選択します。

ステップ 2 [Summary] ペインで、デバイスをダブルクリックしてサーバ グループを表示します。

ステップ 3 [Default TACACS Server Group] をクリックします。

ステップ 4 [Details] ペインで、[Global Settings] タブをクリックします。

ステップ 5 [Time out(secs)] フィールドに、タイムアウト間隔の秒数を入力します。
デフォルトは 5 秒です。

ステップ 6 メニュー バーで [File] > [Deploy] を選択して変更をデバイスに適用します。

関連トピック

TACACS+ のイネーブル化，（121 ページ）
TACACS+ 設定の配布のイネーブル化，（154 ページ）

TACACS+ サーバのタイムアウト間隔の設定

Cisco NX-OS デバイスが TACACS+ サーバからの応答を待つタイムアウト間隔を設定できます。これを過ぎるとタイムアウト エラーになります。タイムアウト間隔には、Cisco NX-OS デバイスが TACACS+ サーバからの応答を待つ時間を指定します。これを過ぎるとタイムアウト エラーになります。

はじめる前に

TACACS+ をイネーブルにします。

手順の概要

1. **configure terminal**
2. **tacacs-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **timeout***seconds*
3. （任意） **show tacacs+** {**pending** | **pending-diff**}
4. （任意） **tacacs+ commit**
5. **exit**
6. （任意） **show tacacs-server**
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**tacacs-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **timeout***seconds* 例： `switch(config)# tacacs-server host server1 timeout 10`	特定のサーバのタイムアウト間隔を指定します。デフォルトはグローバル値です。 （注） 特定の TACACS+ サーバに指定したタイムアウト間隔は、すべての TACACS+ サーバに指定したタイムアウト間隔より優先されます。
ステップ 3	**show tacacs+** {**pending** | **pending-diff**} 例： `switch(config)# show tacacs+ pending`	（任意） 配布するために保留状態になっている TACACS+ 設定を表示します。
ステップ 4	**tacacs+ commit** 例： `switch(config)# tacacs+ commit`	（任意） CFS によるユーザ ロール設定の配布機能をイネーブルにしている場合は、一時データベース内にある TACACS+ の設定変更を実行コンフィギュレーションに適用して、TACACS+ 設定を他の Cisco NX-OS デバイスに配布します。

ステップ 5	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 6	**show tacacs-server** 例： `switch# show tacacs-server`	（任意） TACACS+ サーバの設定を表示します。

	コマンドまたはアクション	目的
ステップ 7	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

TACACS+ のイネーブル化，（121 ページ）
TACACS+ 設定の配布のイネーブル化，（154 ページ）

TCP ポートの設定

別のアプリケーションとポート番号が競合している場合は、TACACS+ サーバ用に別の TCP ポートを設定できます。デフォルトでは、Cisco NX-OS デバイスはすべての TACACS+ 要求に対しポート 49 を使用します。

はじめる前に

TACACS+ をイネーブルにします。

手順の概要

1. **configure terminal**
2. **tacacs-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **port** *tcp-port*
3. （任意） **show tacacs+** {**pending** | **pending-diff**}
4. （任意） **tacacs+ commit**
5. **exit**
6. （任意） **show tacacs-server**
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**tacacs-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **port** *tcp-port* 例： `switch(config)# tacacs-server host 10.10.1.1 port 2`	サーバに送る TACACS+ メッセージに使用する TCP ポートを指定します。デフォルトの TCP ポートは 49 です。有効な範囲は 1 ～ 65535 です。
ステップ 3	**show tacacs+** {**pending** | **pending-diff**} 例： `switch(config)# show tacacs+ distribution pending`	（任意） 配布するために保留状態になっている TACACS+ 設定を表示します。
ステップ 4	**tacacs+ commit** 例： `switch(config)# tacacs+ commit`	（任意） CFS によるユーザ ロール設定の配布機能をイネーブルにしている場合は、一時データベース内にある TACACS+ の設定変更を実行コンフィギュレーションに適用して、TACACS+ 設定を他の NX-OS デバイスに配布します。

ステップ 5	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 6	**show tacacs-server** 例： `switch# show tacacs-server`	（任意） TACACS+ サーバの設定を表示します。
ステップ 7	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

TACACS+ のイネーブル化，（121 ページ）
TACACS+ 設定の配布のイネーブル化，（154 ページ）

TACACS+ サーバのグローバルな定期モニタリングの設定

各サーバに個別にテスト パラメータを設定しなくても、すべての TACACS+ サーバの可用性をモニタリングできます。テストパラメータが設定されていないサーバは、グローバル レベルのパラメータを使用してモニタリングされます。

（注） 各サーバ用に設定されたテスト パラメータは、グローバルのテスト パラメータより優先されます。

グローバル コンフィギュレーション パラメータには、サーバで使用するユーザ名とパスワード、およびアイドル タイマーなどがあります。アイドル タイマーには、TACACS+ サーバで何の要求も受信されない状態の時間を指定します。これを過ぎると Cisco NX-OS デバイスはテスト パケットを送信します。このオプションを設定して定期的にサーバをテストしたり、1 回だけテストを実行したりできます。

（注） テスト パラメータは、Cisco NX-OS Release 5.x 以降が稼動しているスイッチに配布されます。ファブリック内に旧リリースが稼働しているスイッチが1つでもある場合は、ファブリック内のすべてのスイッチにテスト パラメータが配布されなくなります。

（注） ネットワークのセキュリティ保護のため、TACACS+ データベース内の既存のユーザ名と同じユーザ名を使用しないことを推奨します。

（注） デフォルトのアイドル タイマー値は 0 分です。アイドル タイム間隔が 0 分の場合、TACACS+ サーバの定期的なモニタリングは実行されません。

はじめる前に

TACACS+ をイネーブルにします。

手順の概要

1. **configure terminal**
2. **tacacs-server test** {**idle-time***minutes* | **password***password* [**idle-time***minutes*] | **username***name* [**password***password* [**idle-time***minutes*]]}
3. **tacacs-server dead-time***minutes*
4. **exit**
5. （任意） **show tacacs-server**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**tacacs-server test** {**idle-time***minutes* | **password***password* [**idle-time***minutes*] | **username***name* [**password***password* [**idle-time***minutes*]]} 例： `switch(config)# tacacs-server test username user1 password Ur2Gd2BH idle-time 3`	グローバルなサーバモニタリング用のパラメータを指定します。デフォルトのユーザ名は test、デフォルトのパスワードは test です。アイドル タイマーのデフォルト値は 0 分です。有効な範囲は 0 ～ 1440 分です。 （注） TACACS+ サーバの定期的なモニタリングを行うには、アイドル タイマーに 0 より大きな値を設定する必要があります。
ステップ 3	**tacacs-server dead-time***minutes* 例： `switch(config)# tacacs-server dead-time 5`	以前に応答の遅かった TACACS+ サーバを Cisco NX-OS デバイスがチェックを始めるまでの分数を指定します。デフォルト値は 0 分です。有効な範囲は 0 ～ 1440 分です。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 5	**show tacacs-server** 例： `switch# show tacacs-server`	（任意） TACACS+ サーバの設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

各 TACACS+ サーバの定期モニタリングの設定, （138 ページ）

各 TACACS+ サーバの定期モニタリングの設定

各 TACACS+ サーバの可用性をモニタリングできます。コンフィギュレーション パラメータには、サーバで使用するユーザ名とパスワード、およびアイドル タイマーなどがあります。アイド

ル タイマーには、TACACS+ サーバで何の要求も受信されない状態の時間を指定します。これを過ぎると Cisco NX-OS デバイスはテスト パケットを送信します。このオプションを設定して定期的にサーバをテストしたり、1 回だけテストを実行したりできます。

（注） 各サーバ用に設定されたテスト パラメータは、グローバルのテスト パラメータより優先されます。

（注） ネットワークのセキュリティ保護のため、TACACS+ データベース内の既存のユーザ名と同じユーザ名を使用しないことを推奨します。

（注） デフォルトのアイドル タイマー値は 0 分です。アイドル タイム間隔が 0 分の場合、TACACS+ サーバの定期的なモニタリングは実行されません。

（注） テスト パラメータは、Cisco NX-OS Release 5.x が稼働しているスイッチに配布されます。ファブリック内に旧リリースが稼働しているスイッチが1つでもある場合は、ファブリック内のすべてのスイッチにテスト パラメータが配布されなくなります。

はじめる前に

TACACS+ をイネーブルにします。

1 つまたは複数の TACACS+ サーバ ホストを追加します。

手順の概要

1. **configure terminal**
2. **tacacs-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **test** {**idle-time***minutes* | **password***password* [**idle-time***minutes*] | **username***name* [**password***password* [**idle-time***minutes*]]}
3. **tacacs-server dead-time***minutes*
4. **exit**
5. （任意） **show tacacs-server**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**tacacs-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **test** {**idle-time***minutes* | **password***password* [**idle-time***minutes*] | **username***name* [**password***password* [**idle-time***minutes*]]} 例： `switch(config)# tacacs-server host 10.10.1.1 test username user1 password Ur2Gd2BH idle-time 3`	サーバ モニタリング用のパラメータを個別に指定します。デフォルトのユーザ名は test、デフォルトのパスワードは test です。アイドル タイマーのデフォルト値は 0 分です。有効な範囲は 0 ～ 1440 分です。 （注） TACACS+ サーバの定期的なモニタリングを行うには、アイドル タイマーに 0 より大きな値を設定する必要があります。
ステップ 3	**tacacs-server dead-time***minutes* 例： `switch(config)# tacacs-server dead-time 5`	以前に応答の遅かった TACACS+ サーバを Cisco NX-OS デバイスがチェックを始めるまでの分数を指定します。デフォルト値は 0 分です。有効な範囲は 0 ～ 1440 分です。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 5	**show tacacs-server** 例： `switch# show tacacs-server`	（任意） TACACS+ サーバの設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

TACACS+ サーバ ホストの設定, （122 ページ）
TACACS+ サーバのグローバルな定期モニタリングの設定, （136 ページ）
TACACS+ 設定の配布のイネーブル化, （154 ページ）

TACACS+ デッド タイム間隔の設定

すべての TACACS+ サーバのデッド タイム間隔を設定できます。デッド タイム間隔では、Cisco NX-OS デバイスが TACACS+ サーバをデッドであると宣言した後、そのサーバがアライブになったかどうかを確認するためにテスト パケットを送信するまでの時間を指定します。

（注） デッド タイム間隔が 0 分の場合、TACACS+ サーバは、応答を返さない場合でも、デットとしてマークされません。デッド タイマーはグループ単位で設定できます。

はじめる前に

TACACS+ をイネーブルにします。

手順の概要

1. **configure terminal**
2. **tacacs-server deadtime** *minutes*
3. （任意） **show tacacs+** {**pending** | **pending-diff**}
4. （任意） **tacacs+ commit**
5. **exit**
6. （任意） **show tacacs-server**
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**tacacs-server deadtime** *minutes* 例： `switch(config)# tacacs-server deadtime 5`	グローバルなデッド タイム間隔を設定します。デフォルト値は 0 分です。有効な範囲は 1 ～ 1440 分です。
ステップ 3	**show tacacs+** {**pending**	**pending-diff**} 例： `switch(config)# show tacacs+ pending`	（任意） 保留状態になっている TACACS+ 設定を表示します。

	コマンドまたはアクション	目的
ステップ 4	**tacacs+ commit** 例： `switch(config)# tacacs+ commit`	（任意） CFS によるユーザ ロール設定の配布機能をイネーブルにしている場合は、一時データベース内にある TACACS+ の設定変更を実行コンフィギュレーションに適用して、TACACS+ 設定を他の NX-OS デバイスに配布します。

ステップ 5	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 6	**show tacacs-server** 例： `switch# show tacacs-server`	（任意） TACACS+ サーバの設定を表示します。
ステップ 7	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

TACACS+ 設定の配布のイネーブル化, （154 ページ）

ASCII 認証の設定

TACACS+ サーバで ASCII 認証をイネーブルにできます。

はじめる前に

TACACS+ をイネーブルにします。

手順の概要

1. **configure terminal**
2. **aaa authentication login ascii-authentication**
3. （任意） **show tacacs+ {pending | pending-diff}**
4. （任意） **tacacs+ commit**
5. **exit**
6. （任意） **show tacacs-server**
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**aaa authentication login ascii-authentication** 例： `switch(config)# aaa authentication login ascii-authentication`	ASCII認証をイネーブルにします。デフォルトではディセーブルになっています。
ステップ 3	**show tacacs+ {pending | pending-diff}** 例： `switch(config)# show tacacs+ pending`	（任意） 保留状態になっている TACACS+ 設定を表示します。
ステップ 4	**tacacs+ commit** 例： `switch(config)# tacacs+ commit`	（任意） CFS によるユーザ ロール設定の配布機能をイネーブルにしている場合は、一時データベース内にある TACACS+ の設定変更を実行コンフィギュレーションに適用して、TACACS+ 設定を他の Cisco NX-OS デバイスに配布します。

ステップ 5	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 6	**show tacacs-server** 例： `switch# show tacacs-server`	（任意） TACACS+ サーバの設定を表示します。

	コマンドまたはアクション	目的
ステップ 7	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

TACACS+ サーバでの AAA 許可の設定

TACACS+ サーバのデフォルトの AAA 許可方式を設定できます。

はじめる前に

TACACS+ をイネーブルにします。

手順の概要

1. **configure terminal**
2. **aaa authorization ssh-certificate default** {**group***group-list* [**none**] | **local** | **none**}
3. **exit**
4. （任意） **show aaa authorization** [**all**]
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**aaa authorization ssh-certificate default** {**group***group-list* [**none**]	**local**	**none**}
			
			例：
			`switch(config)# aaa authorization ssh-certificate`
			`default group TACACSServer1 TACACSServer2`
				TACACS+ サーバのデフォルトの AAA 許可方式を設定します。
				ssh-certificate キーワードは、証明書認証を使用した TACACS+ 許可またはローカル許可を設定します。デフォルトの許可は、ユーザに割り当てたロールに対して許可されたコマンドのリストであるローカル許可です。
				group-list 引数には、TACACS+ サーバ グループの名前をスペースで区切ったリストを指定します。このグループに属するサーバに対して、AAA 許可のためのアクセスが行われます。**local**

	コマンドまたはアクション	目的
		方式では、ローカル データベースを認証に使用します。**none** 方式では、AAA 許可が使用されないように指定します。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 4	**show aaa authorization** [**all**] 例： `switch# show aaa authorization`	（任意） AAA 認可設定を表示します。**all** キーワードは、デフォルト値を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

TACACS+ のイネーブル化，（121 ページ）

TACACS+ サーバでのコマンド許可の設定

TACACS+ サーバでコマンド許可を設定できます。

注意 コマンド許可では、デフォルト ロールを含むユーザのロールベース許可コントロール（RBAC）がディセーブルになります。

（注） Cisco NX-OS Release 4.x および 5.x の場合、コマンド許可は、非コンソール セッションだけに使用できます。コンソールを使用してサーバにログインすると、コマンド認可はディセーブルになります。Cisco NX-OS Release 6.0 以降では、コマンド許可は、非コンソール セッションとコンソール セッションの両方に使用できます。デフォルトでは、コマンド許可はデフォルト（非コンソール）セッション用に設定されていても、コンソールセッションに対してディセーブルです。コンソールセッションでコマンド許可をイネーブルにするには、コンソールの AAA グループを明示的に設定する必要があります。

（注） デフォルトでは、状況依存ヘルプおよびコマンドのタブ補完に表示されるのは、割り当てられたロールでユーザに対するサポートが定義されているコマンドだけです。コマンド許可をイネーブルにすると、Cisco NX-OS ソフトウェアでは、ユーザに割り当てられているロールに関係なく、状況依存ヘルプおよびタブ補完にすべてのコマンドが表示されるようになります。

はじめる前に

TACACS+ をイネーブルにします。

手順の概要

1. **configure terminal**
2. **aaa authorization** {**commands** | **config-commands**} {**console** | **default**}
3. （任意） **show tacacs+**{**pending**| **pending-diff**}
4. （任意） **tacacs+ commit**
5. **exit**
6. （任意） **show aaa authorization** [**all**]
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**aaa authorization** {**commands**	**config-commands**} {**console**	**default**}
			
			例：
			`switch(config)# aaa authorization commands`
			`default group TacGroup`
			`Per command authorization will disable RBAC for all users. Proceed (y/n)?`
				TACACS+ サーバの特定の役割にコマンド許可方式を設定します。
				commands キーワードは、すべての EXEC コマンドの許可ソースを設定し、**config-commands** キーワードは、すべてのコンフィギュレーション コマンドの許可ソースを設定します。
				console キーワードは、コンソール セッションのコマンド許可を設定し、**default** キーワードは、非コンソール セッションのコマンド許可を設定します。
				group-list 引数には、TACACS+ サーバ グループの名前をスペースで区切ったリストを指定します。このグループに属しているサーバに対して、コマンド許可のためのアクセスが行われます。**local** 方式では、許可にローカル ロールベース データベースが使用されます。

	コマンドまたはアクション	目的
		local 方式は、設定されたすべてのサーバ グループから応答が得られず、フォールバック方式として **local** が設定されている場合にのみ使用されます。デフォルトの方式は **local** です。 TACACS+ サーバ グループの方式のあとにフォールバック方式を設定していないと、すべてのサーバ グループから応答が得られなかった場合は許可に失敗します。 確認プロンプトで Enter キーを押した場合のデフォルトのアクションは n です。
ステップ 3	**show tacacs+** {**pending**| **pending-diff**} 例： `switch(config)# show tacacs+ pending`	（任意） 保留状態になっている TACACS+ 設定を表示します。
ステップ 4	**tacacs+ commit** 例： `switch(config)# tacacs+ commit`	（任意） CFS によるユーザ ロール設定の配布機能をイネーブルにしている場合は、一時データベース内にある TACACS+ の設定変更を実行コンフィギュレーションに適用して、TACACS+ 設定を他の Cisco NX-OS デバイスに配布します。

ステップ 5	**exit**
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 6	**show aaa authorization** [**all**] 例： `switch(config)# show aaa authorization`	（任意） AAA 認可設定を表示します。**all** キーワードは、デフォルト値を表示します。
ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

TACACS+ のイネーブル化，（121 ページ）
TACACS+ サーバでのコマンド許可のテスト，（148 ページ）

TACACS+ サーバでのコマンド許可のテスト

TACACS+ サーバで、ユーザに対するコマンド許可をテストできます。

（注） 許可の正しいコマンドを送信しないと、結果の信頼性が低くなります。

（注） **test** コマンドでは許可に、コンソール方式ではなくデフォルト（非コンソール）方式を使用します。

はじめる前に

TACACS+ をイネーブルにします。

TACACS+ サーバにコマンド許可が設定されていることを確認します。

手順の概要

1. **test aaa authorization command-type** {**commands** | **config-commands**} **user***username***command***command-string*

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**test aaa authorization command-type** {**commands** | **config-commands**} **user***username***command***command-string*
	
	例：
	`switch# test aaa authorization command-type commands`
	`user TestUser command reload`
		TACACS+ サーバで、コマンドに対するユーザの許可をテストします。
		commands キーワードは、EXEC コマンドだけを指定し、**config-commands** キーワードはコンフィギュレーション コマンドだけを指定します。
		（注） *command-string* 引数にスペースが含まれる場合は、二重引用符（"）で囲みます。

関連トピック

TACACS+ のイネーブル化，（121 ページ）
TACACS+ サーバでのコマンド許可の設定，（145 ページ）
ユーザ アカウントおよび RBAC の設定，（283 ページ）

コマンド許可検証のイネーブル化とディセーブル化

デフォルトのユーザセッションまたは別のユーザ名に対して、コマンドラインインターフェイス（CLI）でコマンド許可検証をイネーブルにしたり、ディセーブルにしたりできます。

（注） 許可検証をイネーブルにした場合は、コマンドは実行されません。

手順の概要

1. **terminal verify-only** [**username***username*]
2. **terminal no verify-only** [**username***username*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**terminal verify-only** [**username***username*] 例： `switch# terminal verify-only`	コマンド許可検証をイネーブルにします。このコマンドを入力すると、入力したコマンドが許可されているかどうかが Cisco NX-OS ソフトウェアによって示されます。
ステップ 2	**terminal no verify-only** [**username***username*] 例： `switch# terminal no verify-only`	コマンド許可検証をディセーブルにします。

TACACS+ サーバでの許可に使用する特権レベルのサポートの設定

TACACS+ サーバでの許可に使用する特権レベルのサポートを設定できます。

許可の決定に特権レベルを使用する Cisco IOS デバイスとは異なり、Cisco NX-OS デバイスでは、ロールベース アクセス コントロール（RBAC）を使用します。両方のタイプのデバイスを同じ TACACS+ サーバで管理できるようにするには、TACACS+ サーバで設定した特権レベルを、Cisco NX-OS デバイスで設定したユーザ ロールにマッピングします。

TACACS+ サーバでのユーザの認証時には、特権レベルが取得され、それを使用して「priv-*n*」という形式（*n* が特権レベル）のローカル ユーザ ロール名が生成されます。このローカル ロールの権限がユーザに割り当てられます。特権レベルは 16 あり、対応するユーザ ロールに直接マッピングされます。次の表に、各特権レベルに対応するユーザ ロール権限を示します。

Privilege Level	ユーザ ロール権限
15	network-admin 権限
14	vdc-admin 権限
13 ～ 1	• スタンドアロン ロール権限（**feature privilege** コマンドがディセーブルの場合）。 • ロールの累積権限からなる特権レベル 0 と同じ権限（**feature privilege** コマンドがイネーブルの場合）。
0	**show** コマンドや **exec** コマンド（**ping**、**trace**、**ssh** など）を実行するための権限。

（注） **feature privilege** コマンドをイネーブルにすると、権限ロールは低いレベルの権限ロールの権限を継承します。

（注） Cisco Secure Access Control Server（ACS）にも、Cisco NX-OS デバイスの特権レベルを設定する必要があります。次の URL から入手できるマニュアルを参照してください。

http://www.cisco.com/en/US/products/sw/secursw/ps5338/products_installation_and_configuration_guides_list.html

手順の概要

1. **configure terminal**
2. [**no**] **feature privilege**
3. [**no**] **enable secret** [**0** | **5**] *password* [**priv-lvl** *priv-lvl* | **all**]
4. [**no**] **username** *username***priv-lvl** *n*
5. （任意） **show privilege**
6. （任意） **copy running-config startup-config**
7. **exit**
8. **enable** *level*

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **feature privilege** 例： `switch(config)# feature privilege`	ロールの累積権限をイネーブルまたはディセーブルにします。**enable** コマンドは、この機能をイネーブルにした場合しか表示されません。デフォルトではディセーブルになっています。
ステップ 3	[**no**] **enable secret** [**0** | **5**] *password* [**priv-lvl** *priv-lvl* | **all**] 例： `switch(config)# enable secret 5 def456 priv-lvl 15`	特定の特権レベルのシークレット パスワードをイネーブルまたはディセーブルにします。特権レベルが上がるたびに、正しいパスワードを入力するようにユーザに要求します。デフォルトではディセーブルになっています。 パスワードの形式としてクリア テキストを指定する場合は **0** を入力し、暗号化された形式を指定する場合は**5**を入力します。*password* 引数に指定できる文字数は、最大 64 文字です。*priv-lvl* 引数は、1 ～ 15 です。 （注） シークレットパスワードをイネーブルにするには、**feature privilege** コマンドを入力してロールの累積権限をイネーブルにする必要があります。
ステップ 4	[**no**] **username** *username***priv-lvl** *n* 例： `switch(config)# username user2 priv-lvl 15`	ユーザの許可に対する特権レベルの使用をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。 **priv-lvl** キーワードはユーザに割り当てる権限レベルを指定します。デフォルトの特権レベルはありません。特権レベル 0 ～ 15（priv-lvl 0 ～ priv-lvl 15）は、ユーザ ロール priv-0 ～ priv-15 にマッピングされます。
ステップ 5	**show privilege** 例： `switch(config)# show privilege`	（任意） ユーザ名、現在の特権レベル、および累積権限のサポートのステータスを表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

	コマンドまたはアクション	目的

ステップ 7	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 8	**enable** *level* 例： `switch# enable 15`	上位の特権レベルへのユーザの昇格をイネーブルにします。このコマンドの実行時にはシークレット パスワードが要求されます。*level* 引数はユーザのアクセスを許可する特権レベルを指定します。指定できるレベルは 15 だけです。

関連トピック

権限ロールのユーザ コマンドの許可または拒否, （152 ページ）
ユーザ ロールおよびルールの作成, （295 ページ）

権限ロールのユーザ コマンドの許可または拒否

ネットワーク管理者は、権限ロールを変更して、ユーザが特定のコマンドを実行できるようにしたり実行できなくしたりすることができます。

権限ロールのルールを変更する場合は、次の注意事項に従う必要があります。

- priv-14 ロールと priv-15 ロールは変更できません。
- 拒否ルールは priv-0 ロールにだけ追加できます。
- priv-0 ロールでは以下のコマンドは常に許可されます。**configure**、**copy**、**dir**、**enable**、**ping**、**show**、**ssh**、**telnet**、**terminal**、**traceroute**、**end**、**exit**。

手順の概要

1. **configure terminal**
2. [**no**] **role name priv-***n*
3. **rule** *number* {**deny** | **permit**} **command** *command-string*
4. **exit**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **role name priv-***n*
	
	例：
	`switch(config)# role name priv-5`
	`switch(config-role)#`
		権限ロールをイネーブルまたはディセーブルにして、ロール コンフィギュレーション モードを開始します。*n* 引数には、特権レベルを 0 ～ 13 の数値で指定します。

ステップ 3	**rule** *number* {**deny** | **permit**} **command** *command-string* 例： `switch(config-role)# rule 2 permit command pwd`	権限ロールのユーザ コマンド ルールを設定します。これらのルールで、ユーザによる特定のコマンドの実行を許可または拒否します。ロールごとに最大256のルールを設定できます。ルール番号によって、ルールが適用される順序が決まります。ルールは降順で適用されます。たとえば、1つのロールが3つのルールを持っている場合、ルール3がルール2よりも前に適用され、ルール 2 はルール 1 よりも前に適用されます。 *command-string* 引数には、空白スペースを含めることができます。 （注） 必要な規則の数だけこのコマンドを繰り返します。

ステップ 4	**exit**
	
	例：
	`switch(config-role)# exit`
	`switch(config)#`
		ロール コンフィギュレーション モードを終了します。

ステップ 5	**copy running-config startup-config**
	
	例：
	`switch(config)# copy running-config`
	
	`startup-config`
		（任意）
		実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

TACACS+ サーバでの許可に使用する特権レベルのサポートの設定，（149 ページ）
ユーザ ロールおよびルールの作成，（295 ページ）

TACACS+ 設定の配布のイネーブル化

設定の配布がイネーブルになっている Cisco NX-OS デバイスだけが、CFS 領域内での TACACS+ 設定配布の変更に参加できます。

はじめる前に

CFS 配布がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **tacacs+ distribute**
3. **exit**
4. （任意） **show tacacs+ status**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**tacacs+ distribute** 例： `switch(config)# tacacs+ distribute`	TACACS+ 設定の配布をイネーブルにします。デフォルトではディセーブルになっています。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show tacacs+ status** 例： `switch(config)# show tacacs+ status`	（任意） TACACS+ の CFS による配布の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

TACACS+ のイネーブル化，（121 ページ）
TACACS+ サーバ ホストの設定，（122 ページ）
TACACS+ サーバの設定プロセス，（121 ページ）
TACACS+ サーバ グループの設定，（127 ページ）

TACACS+ 設定の配布のコミット

一時バッファに保存されている TACACS+ のグローバル設定およびサーバ設定を、ファブリック内のすべての Cisco NX-OS デバイス（元のデバイスを含む）の実行コンフィギュレーションに適用します。

はじめる前に

TACACS+ をイネーブルにします。

手順の概要

1. **configure terminal**
2. （任意） **show tacacs+ {pending | pending-diff}**
3. **tacacs+ commit**
4. **exit**
5. （任意） **show tacacs+ distribution status**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**show tacacs+ {pending | pending-diff}** 例： `switch(config)# show tacacs+ pending`	（任意） 配布するために保留状態になっている TACACS+ 設定を表示します。
ステップ 3	**tacacs+ commit** 例： `switch(config)# tacacs+ commit`	CFS によるユーザ ロール設定の配布機能をイネーブルにしている場合は、一時データベース内にある TACACS+ の設定変更を実行コンフィギュレーションに適用して、TACACS+ 設定を他の Cisco NX-OS デバイスに配布します。

	コマンドまたはアクション	目的

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 5	**show tacacs+ distribution status** 例： `switch(config)# show tacacs+ distribution status`	（任意） TACACS+ の配布の設定とステータスを表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションに適用します。

関連トピック

TACACS+ 設定の配布のイネーブル化, （154 ページ）

TACACS+ の配布セッションの廃棄

TACACS+ の設定変更の一時データベースを廃棄して、CFS 配布セッションを終了します。

はじめる前に

TACACS+ をイネーブルにします。

手順の概要

1. **configure terminal**
2. （任意） **show tacacs+ {pending | pending-diff}**
3. **tacacs+ abort**
4. **exit**
5. （任意） **show tacacs+ distribution status**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**show tacacs+ {pending | pending-diff}** 例： `switch(config)# show tacacs+ pending`	（任意） 配布するために保留状態になっている TACACS+ 設定を表示します。
ステップ 3	**tacacs+ abort** 例： `switch(config)# tacacs+ abort`	一時ストレージにある TACACS+ 設定を廃棄して、セッションを終了します。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 5	**show tacacs+ distribution status** 例： `switch(config)# show tacacs+ distribution status`	（任意） TACACS+ の配布の設定とステータスを表示します。

関連トピック

TACACS+ 設定の配布のイネーブル化, （154 ページ）

TACACS+ の配布セッションのクリア

アクティブな CFS 配布セッションをクリアして、ネットワーク内の TACACS+ 設定のロックを解除します。

はじめる前に

TACACS+ をイネーブルにします。

手順の概要

1. **clear tacacs+ session**
2. （任意） **show tacacs+ distribution status**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**clear tacacs+ session** 例： `switch# clear tacacs+ session`	TACACS+ のための CFS セッションをクリアして、ファブリックのロックを解除します。
ステップ 2	**show tacacs+ distribution status** 例： `switch(config)# show tacacs+ distribution status`	（任意） TACACS+ の配布の設定とステータスを表示します。

関連トピック

TACACS+ 設定の配布のイネーブル化，（154 ページ）

TACACS+ サーバまたはサーバ グループの手動モニタリング

TACACS+ サーバまたはサーバ グループに、手動でテスト メッセージを送信できます。

はじめる前に

TACACS+ をイネーブルにします。

手順の概要

1. **test aaa server tacacs+** {*ipv4-address* | *ipv6-address* | *host-name*} [**vrf***vrf-name*] *username password*
2. **test aaa group***group-name username password*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**test aaa server tacacs+** {*ipv4-address* | *ipv6-address* | *host-name*} [**vrf***vrf-name*] *username password* 例： `switch# test aaa server tacacs+ 10.10.1.1 user1 Ur2Gd2BH`	TACACS+ サーバにテスト メッセージを送信して可用性を確認します。
ステップ 2	**test aaa group***group-name username password* 例： `switch# test aaa group TacGroup user2 As3He3CI`	TACACS+ サーバ グループにテスト メッセージを送信して可用性を確認します。

関連トピック

TACACS+ サーバ ホストの設定, （122 ページ）
TACACS+ サーバ グループの設定, （127 ページ）

TACACS+ のディセーブル化

TACACS+ をディセーブルにできます。

注意 TACACS+ をディセーブルにすると、関連するすべての設定が自動的に廃棄されます。

手順の概要

1. **configure terminal**
2. **no feature tacacs+**
3. **exit**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**no feature tacacs+** 例： `switch(config)# no feature tacacs+`	TACACS+ をディセーブルにします。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

TACACS+ サーバのモニタリング

Cisco NX-OS デバイスが保持している TACACS+ サーバのアクティビティに関する統計情報をモニタリングできます。

はじめる前に

Cisco NX-OS デバイスに TACACS+ サーバを設定します。

手順の概要

1. **show tacacs-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show tacacs-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*} 例： `switch# show tacacs-server statistics 10.10.1.1`	TACACS+ 統計情報を表示します。

関連トピック

TACACS+ サーバ ホストの設定，（122 ページ）
TACACS+ サーバ統計情報のクリア，（160 ページ）

TACACS+ サーバ統計情報のクリア

Cisco NX-OS デバイスが保持している TACACS+ サーバのアクティビティに関する統計情報を表示します。

はじめる前に

Cisco NX-OS デバイスに TACACS+ サーバを設定します。

手順の概要

1. （任意） **show tacacs-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*}
2. **clear tacacs-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show tacacs-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*} 例： `switch# show tacacs-server statistics 10.10.1.1`	（任意） Cisco NX-OS デバイスでの TACACS+ サーバ統計情報を表示します。
ステップ 2	**clear tacacs-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*} 例： `switch# clear tacacs-server statistics 10.10.1.1`	TACACS+ サーバ統計情報をクリアします。

関連トピック

TACACS+ サーバ ホストの設定, （122 ページ）

TACACS+ の設定の確認

TACACS+ の設定を表示するには、次のいずれかの作業を行います。

コマンド	目的
show tacacs+ {**status** | **pending** | **pending-diff**}	Cisco Fabric Services の TACACS+ 設定の配布状況と他の詳細事項を表示します。
show running-config tacacs+ [**all**]	実行コンフィギュレーションの TACACS+ 設定を表示します。
show startup-config tacacs	スタートアップ コンフィギュレーションの TACACS+ 設定を表示します。
show tacacs-server [*host-name* | *ipv4-address* | *ipv6-address*] [**directed-request** | **groups** | **sorted** | **statistics**]	設定済みのすべての TACACS+ サーバのパラメータを表示します。
show privilege	現在の特権レベル、ユーザ名、および累積権限サポートのステータスを表示します。

このコマンドの出力フィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

TACACS+ の設定例

次に、TACACS+ サーバ ホストおよびサーバ グループを設定する例を示します。

```
feature tacacs+
tacacs-server key 7 "ToIkLhPpG"
tacacs-server host 10.10.2.2 key 7 "ShMoMhTl"
aaa group server tacacs+ TacServer
    server 10.10.2.2
```

次に、コマンド許可検証を設定して使用する例を示します。

```
switch# terminal verify-only
switch# show interface ethernet 7/2 brief
%Success
switch# terminal no verify-only
switch# show interface ethernet 7/2 brief

--------------------------------------------------------------------------------
Ethernet      VLAN   Type Mode   Status  Reason                   Speed     Port
Interface                                                                   Ch #
--------------------------------------------------------------------------------
Eth7/2        1      eth  access down    SFP not inserted           auto(D) --
```

次に、ロールの累積権限をイネーブルにし、特権レベル 2 のシークレット パスワードを設定し、特権レベル 2 の許可用に user3 を設定する例を示します。

```
switch# configure terminal
switch(config)# feature privilege
switch(config)# enable secret def456 priv-lvl 2
switch(config)# username user3 priv-lvl 2
switch(config)# show privilege
User name: user3
Current privilege level: -2
Feature privilege: Enabled
switch(config)# copy running-config startup-config
switch(config)# exit
```

次に、user3 を priv-2 ロールから priv-15 ロールに変更する例を示します。**enable 15** コマンドを入力した後、ユーザは、**enable secret** コマンドを使用して管理者によって設定されたパスワードを入力するよう求められます。特権レベルを 15 に設定すると、このユーザには、イネーブル モードにおける network-admin 権限が付与されます。

```
User Access Verification
login: user3
Password: ******
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright ©) 2002-2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
switch#
switch# enable 15
Password: def456
```

```
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright ©) 2002-2009, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
switch-enable#
```

次に、priv-5 以上のロールを持つすべてのユーザによる **pwd** コマンドの実行を許可する例を示します。

```
switch# configure terminal
switch(config)# role name priv-5
switch(config-role)# rule 1 permit command pwd
```

次に、priv-5 未満のロールを持つすべてのユーザによる **show running-config** コマンドを拒否する例を示します。まず、このコマンドを実行する権限を priv-0 ロールから削除する必要があります。次に、ロール priv-5 でこのコマンドを許可し、priv-5 以上のロールを持つユーザにこのコマンドを実行する権限が付与されるようにする必要があります。

```
switch# configure terminal
switch(config)# role name priv-0
switch(config-role)# rule 2 deny command show running-config
switch(config-role)# exit
switch(config)# role name priv-5
switch(config-role)# rule 3 permit command show running-config
switch(config-role)# exit
```

次の作業

これで、サーバ グループも含めて AAA 認証方式を設定できるようになります。

TACACS+ に関する追加情報

ここでは、TACACS+ の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS のライセンス	『*Cisco NX-OS Licensing Guide*』
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』

関連項目	マニュアル タイトル
VRF コンフィギュレーション	『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
• CISCO-AAA-SERVER-MIB • CISCO-AAA-SERVER-EXT-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

TACACS+ の機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 *13* : *TACACS+* の機能の履歴

機能名	リリース	機能情報
TACACS+	6.2(2)	単一の TACACS+ 接続のサポートが追加されました。
TACACS+	6.0(1)	コンソール セッションのコマンド許可を設定する機能が追加されました。
TACACS+	5.2(1)	TACACS+ サーバ キーのタイプ 6 暗号化が追加されました。

機能名	リリース	機能情報
TACACS+	5.1(1)	Release 5.0 以降、変更はありません。
TACACS+ の特権レベルの許可	5.0(2)	Cisco NX-OS デバイスでローカルに設定されたユーザ ロールに対して、TACACS+ サーバでユーザ用に設定された特権レベルのマッピングをサポートするようになりました。
権限ロール	5.0(2)	権限ロールのユーザ コマンドの許可または拒否のサポートが追加されました。
定期サーバ モニタリング	5.0(2)	TACACS+ サーバのグローバルな定期モニタリングのサポートが追加されました。
AAA 許可	5.0(2)	TACACS+ サーバのデフォルトの AAA 許可方式の設定のサポートが追加されました。

第 7 章

LDAP の設定

この章では、Cisco NX-OS デバイス上で Lightweight Directory Access Protocol（LDAP）を設定する方法について説明します。

この章は、次の項で構成されています。

- 機能情報の確認，167 ページ
- LDAP の概要，168 ページ
- LDAP のライセンス要件，172 ページ
- LDAP の前提条件，172 ページ
- LDAP の注意事項と制約事項，172 ページ
- LDAP のデフォルト設定，173 ページ
- LDAP の設定，173 ページ
- LDAP サーバのモニタリング，192 ページ
- LDAP サーバ統計情報のクリア，192 ページ
- LDAP 設定の確認，193 ページ
- LDAP の設定例，194 ページ
- 次の作業，194 ページ
- LDAP に関する追加情報，194 ページ
- LDAP の機能の履歴，195 ページ

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。こ

のモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

LDAP の概要

Lightweight Directory Access Protocol（LDAP）は、Cisco NX-OS デバイスにアクセスしようとするユーザの検証を集中的に行います。LDAP サービスは、通常 UNIX または Windows NT ワークステーション上で稼働する LDAP デーモンのデータベースで管理されます。Cisco NX-OS デバイスに設定した LDAP 機能を使用可能にするには、LDAP サーバにアクセスして設定しておく必要があります。

LDAP では、認証と認可のファシリティが別々に提供されます。LDAP では、1 つのアクセス コントロール サーバ（LDAP デーモン）が認証と認可の各サービスを個別に提供できます。各サービスを固有のデータベースに結合し、デーモンの機能に応じてそのサーバまたはネットワークで使用できる他のサービスを使用できます。

LDAP クライアント/サーバ プロトコルでは、トランスポート要件を満たすために、TCP（TCP ポート 389）を使用します。Cisco NX-OS デバイスは、LDAP プロトコルを使用して集中型の認証を行います。

LDAP 認証および許可

クライアントは、簡易バインド（ユーザ名とパスワード）を使用して LDAP サーバとの TCP 接続および認証セッションを確立します。許可プロセスの一環として、LDAP サーバはそのデータベースを検索し、ユーザ プロファイルやその他の情報を取得します。

バインドしてから検索する（認証を行ってから許可する）か、または検索してからバインドするように、バインド操作を設定できます。デフォルトでは、検索してからバインドする方式が使用されます。

検索してからバインドする方式の利点は、baseDN の前にユーザ名（cn 属性）を追加することで認定者名（DN）を形成するのではなく、検索結果で受け取った DN をバインディング時にユーザ DN として使用できることです。この方式は、ユーザ DN がユーザ名と baseDN の組み合わせとは異なる場合に特に役立ちます。ユーザ バインドのために、bindDN が baseDN + append-with-baseDN として構成されます。ここで、append-with-baseDN は cn=$userid のデフォルト値です。

（注） バインド方式の代わりに、比較方式を使用して LDAP 認証を確立することもできます。比較方式では、サーバでユーザ入力の属性値を比較します。たとえば、ユーザ パスワード属性を比較して認証を行うことができます。デフォルトのパスワード属性タイプは userPassword です。

ユーザ ログインにおける LDAP の動作

LDAP を使用する Cisco NX-OS デバイスに対して、ユーザがパスワード認証プロトコル（PAP）ログインを試みると、次の処理が行われます。

（注） LDAP では、デーモンがユーザを認証するために十分な情報を得られるまで、デーモンとユーザとの自由な対話を許可します。通常、デーモンはユーザ名とパスワードの組み合わせを入力するよう求めますが、他の項目を求めることもできます。

（注） LDAP では、認証の前に許可を行うことができます。

1. Cisco NX-OS デバイスは接続が確立されると、ユーザ名とパスワードを取得するために LDAP デーモンに接続します。
2. Cisco NX-OS デバイスは、最終的に LDAP デーモンから次のいずれかの応答を得ます。

   ACCEPT

   ユーザの認証に成功したので、サービスを開始します。Cisco NX-OS デバイスがユーザ許可を必要とする場合は、許可処理が始まります。

   REJECT

   ユーザの認証が失敗します。LDAP デーモンは、ユーザに対してそれ以上のアクセスを拒否するか、ログイン操作を再試行するように要求します。

   ERROR

   デーモンによる認証サービスの途中でエラーが発生したか、またはデーモンと Cisco NX-OS デバイスの間のネットワーク接続でエラーが発生しました。Cisco NX-OS デバイスは ERROR 応答を受信した場合、別の方法でユーザの認証を試行します。

   認証が終了し、Cisco NX-OS デバイスで許可がイネーブルになっていれば、続いてユーザの許可フェーズに入ります。LDAP 許可に進むには、まず LDAP 認証を正常に終了する必要があります。
3. LDAP 許可が必要な場合、Cisco NX-OS デバイスは再び LDAP デーモンに接続します。デーモンから ACCEPT または REJECT 応答が返されます。ACCEPT 応答には、ユーザに対する EXEC または NETWORK セッションの送信に使用される属性が含まれます。また ACCEPT 応答により、ユーザがアクセス可能なサービスが決まります。

   この場合のサービスは次のとおりです。

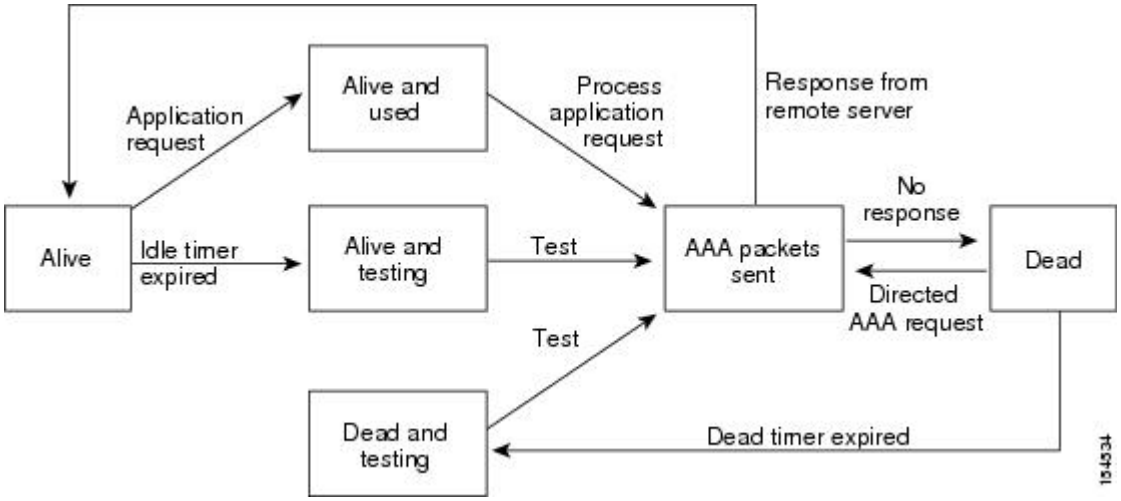
   - Telnet、rlogin、ポイントツーポイント プロトコル（PPP）、シリアル ライン インターネット プロトコル（SLIP）、EXEC サービス
   - 接続パラメータ（ホストまたはクライアントの IP アドレス（IPv4 または IPv6）、アクセス リスト、ユーザ タイムアウト）

LDAP サーバのモニタリング

応答を返さないLDAPサーバがあると、AAA要求の処理に遅延が発生することがあります。AAA要求の処理時間を短縮するために、LDAP サーバを定期的にモニタしてLDAP サーバが応答している（アライブ）かどうかを調べることができます。Cisco NX-OSデバイスは、応答の遅いLDAPサーバをデッド（dead）としてマークし、デッドLDAP サーバには AAA 要求を送信しません。Cisco NX-OS デバイスはデッドLDAP サーバを定期的にモニタし、応答があればアライブ状態に戻します。このモニタリング プロセスでは、実際の AAA 要求が送信される前に、LDAP サーバが稼働状態であることを確認します。LDAP サーバがデッドまたはアライブの状態に変わると簡易ネットワーク管理プロトコル（SNMP）トラップが生成され、Cisco NX-OSデバイスはパフォーマンスに影響が出る前に、障害が発生していることをエラー メッセージで表示します。

次の図に、LDAP サーバ モニタリングのサーバの状態を示します。

図 *4*：*LDAP* サーバの状態



（注） アライブ サーバとデッド サーバのモニタリング間隔は異なります。これらはユーザが設定できます。LDAP サーバ モニタリングを実行するには、テスト認証要求を LDAP サーバに送信します。

LDAP のベンダー固有属性

Internet Engineering Task Force（IETF; インターネット技術特別調査委員会）ドラフト標準には、ネットワーク アクセス サーバと LDAP サーバ間での Vendor-Specific Attribute（VSA; ベンダー固有属性）の通信方法が規定されています。IETF は属性 26 を使用します。ベンダーは VSA を使用して、一般的な用途には適さない独自の拡張属性をサポートできます。

LDAP 用の Cisco VSA 形式

シスコの LDAP 実装では、IETF 仕様で推奨される形式を使用したベンダー固有オプションを 1 つサポートしています。シスコのベンダー ID は 9、サポートされるオプションのベンダー タイプは 1（名前付き cisco-av-pair）です。値は次の形式のストリングです。

```
protocol : attribute separator value *
```

protocol は、特定の許可タイプを表すシスコの属性です。separator は、必須属性の場合は =（等号）、オプションの属性の場合は *（アスタリスク）です。

Cisco NX-OS デバイス上の認証に LDAP サーバを使用した場合、LDAP では LDAP サーバに対して、認証結果とともに権限付与情報などのユーザ属性を返すように指示します。この許可情報は、VSA で指定されます。

Cisco NX-OS ソフトウェアでは次の VSA プロトコル オプションをサポートしています。

Shell

ユーザ プロファイル情報を提供する access-accept パケットで使用されるプロトコル。

Cisco NX-OS ソフトウェアは、次の属性をサポートしています。

ロール

ユーザが属するすべてのロールの一覧です。値フィールドは、スペースで区切られたロール名を一覧表示したストリングです。たとえば、ユーザが network-operator および vdc-admin のロールに属している場合、値フィールドは network-operator vdc-admin となります。このサブ属性は Access-Accept フレームの VSA 部分に格納され、LDAP サーバから送信されます。この属性はシェル プロトコル値とだけ併用できます。次に、Cisco ACS でサポートされるロール属性の例を示します。

```
shell:roles=network-operator vdc-admin
```

```
shell:roles*network-operator vdc-admin
```

（注） VSA を shell:roles*"network-operator vdc-admin" として指定した場合、この VSA はオプション属性としてフラグ設定され、他のシスコ デバイスはこの属性を無視します。

LDAP のバーチャライゼーション サポート

LDAP の設定と操作は、仮想デバイス コンテキスト（VDC）に対してローカルです。VDC の詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

Cisco NX-OS デバイスは、仮想ルーティング/転送（VRF）インスタンスを使用して LDAP サーバにアクセスします。VRF の詳細情報については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

LDAP のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	LDAP にはライセンスは必要ありません。ライセンスパッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

LDAP の前提条件

LDAP の前提条件は次のとおりです。

- LDAP サーバの IPv4 または IPv6 アドレスまたはホスト名を取得すること
- Cisco NX-OS デバイスが AAA サーバの LDAP クライアントとして設定されていること

LDAP の注意事項と制約事項

LDAP に関する注意事項と制約事項は次のとおりです。

- Cisco NX-OS デバイス上には最大 64 の LDAP サーバを設定できます。
- Cisco NX-OS は LDAP バージョン 3 だけをサポートします。
- Cisco NX-OS は次の LDAP サーバだけをサポートします。
  - OpenLDAP
  - Microsoft Active Directory
- Secure Sockets Layer（SSL）上の LDAP は、SSL バージョン 3 および Transport Layer Security（TLS）バージョン 1 だけをサポートします。
- ローカルの Cisco NX-OS デバイス上に設定されているユーザ アカウントが、AAA サーバ上のリモート ユーザ アカウントと同じ名前の場合、Cisco NX-OS ソフトウェアは、AAA サーバ上に設定されているユーザ ロールではなく、ローカル ユーザ アカウントのユーザ ロールをリモート ユーザに適用します。

LDAP のデフォルト設定

次の表に、LDAP パラメータのデフォルト設定を示します。

表 *14* : *LDAP* パラメータのデフォルト設定

パラメータ	デフォルト
LDAP	ディセーブル
LDAP 認証方式	検索してからバインド
LDAP 認証メカニズム	プレーン
デッドタイム間隔	0 分
タイムアウト間隔	5 秒
アイドル タイマー間隔	60 分
サーバの定期的モニタリングのユーザ名	test
サーバの定期的モニタリングのパスワード	Cisco

LDAP の設定

ここでは、Cisco NX-OS デバイスで LDAP を設定する手順を説明します。

（注） Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

LDAP サーバの設定プロセス

次の設定プロセスに従って、LDAP サーバを設定できます。

ステップ 1 LDAP をイネーブルにします。
ステップ 2 LDAP サーバと Cisco NX-OS デバイスの接続を確立します。
ステップ 3 必要に応じて、AAA 認証方式用に、LDAP サーバのサブセットを使用して LDAP サーバ グループを設定します。
ステップ 4 （任意）TCP ポートを設定します。
ステップ 5 （任意）LDAP サーバにデフォルト AAA 認証方式を設定します。
ステップ 6 （任意）LDAP 検索マップを設定します。
ステップ 7 （任意）必要に応じて、LDAP サーバの定期モニタリングを設定します。

関連トピック

LDAP のイネーブル化, （174 ページ）
LDAP サーバ ホストの設定, （175 ページ）
LDAP サーバの rootDN の設定, （177 ページ）
LDAP サーバ グループの設定, （178 ページ）
TCP ポートの設定, （184 ページ）
LDAP 検索マップの設定, （185 ページ）
LDAP サーバの定期的モニタリングの設定, （187 ページ）

LDAP のイネーブル化

デフォルトでは、Cisco NX-OS デバイスの LDAP 機能はディセーブルになっています。認証に関するコンフィギュレーション コマンドと検証コマンドを使用するには、LDAP 機能を明示的にイネーブルにする必要があります。

手順の概要

1. **configure terminal**
2. **feature ldap**
3. **exit**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**feature ldap** 例： `switch(config)# feature ldap`	LDAP をイネーブルにします。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

LDAP サーバ ホストの設定

リモートの LDAP サーバにアクセスするには、Cisco NX-OS デバイス上でその LDAP サーバの IP アドレスまたはホスト名を設定する必要があります。最大 64 の LDAP サーバを設定できます。

（注） デフォルトでは、LDAP サーバの IP アドレスまたはホスト名を Cisco NX-OS デバイスで設定すると、LDAP サーバがデフォルトの LDAP サーバ グループに追加されます。LDAP サーバを別の LDAP サーバ グループに追加することもできます。

はじめる前に

LDAP をイネーブルにします。

リモートの LDAP サーバの IPv4 または IPv6 アドレスまたはホスト名を取得します。

Secure Sockets Layer（SSL）プロトコルをイネーブルにする予定の場合は、Cisco NX-OS デバイスで LDAP サーバ証明書を手動で設定します。

手順の概要

1. **configure terminal**
2. [**no**] **ldap-server host** {*ipv4-address* | *ipv6-address* | *host-name*} [**enable-ssl**]
3. **exit**
4. （任意） **show ldap-server**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **ldap-server host** {*ipv4-address* | *ipv6-address* | *host-name*} [**enable-ssl**] 例： `switch(config)# ldap-server host 10.10.2.2 enable-ssl`	LDAP サーバの IPv4 または IPv6 アドレス、あるいはホスト名を指定します。 **enable-ssl** キーワードは、バインドまたは検索の要求を送信する前に LDAP クライアントに Secure Sockets Layer（SSL）セッションを確立させることにより、転送されたデータの整合性と機密性を確保します。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show ldap-server** 例： `switch# show ldap-server`	（任意） LDAP サーバの設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

LDAP のイネーブル化，（174 ページ）
LDAP サーバ グループの設定，（178 ページ）

LDAP サーバの rootDN の設定

LDAP サーバ データベースのルート指定名（DN）を設定できます。rootDN は、LDAP サーバにバインドしてそのサーバの状態を確認するために使用します。

はじめる前に

LDAP をイネーブルにします。

リモートの LDAP サーバの IPv4 または IPv6 アドレスまたはホスト名を取得します。

手順の概要

1. **configure terminal**
2. [**no**] **ldap-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **rootDN***root-name* [**password***password*] [**port***tcp-port* [**timeout***seconds*] | [**timeout***seconds*]]
3. **exit**
4. （任意） **show ldap-server**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **ldap-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **rootDN***root-name* [**password***password*] [**port***tcp-port* [**timeout***seconds*] | [**timeout***seconds*]] 例： `switch(config)# ldap-server host 10.10.1.1 rootDN cn=manager,dc=acme,dc=com password Ur2Gd2BH timeout 60`	LDAP サーバデータベースの rootDN を指定し、ルートのパスワードをバインドします。 任意で、サーバに送る LDAP メッセージに使用する TCP ポートを指定します。有効な範囲は 1 ～ 65535 です。デフォルトの TCP ポートはグローバル値です（グローバル値が設定されていない場合は 389）。また、サーバのタイムアウト間隔も指定します。値の範囲は 1 ～ 60 秒です。デフォルトのタイムアウト値はグローバル値です（グローバル値が設定されていない場合は 5 秒）。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

	コマンドまたはアクション	目的
ステップ 4	**show ldap-server** 例： `switch# show ldap-server`	（任意） LDAP サーバの設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

LDAP のイネーブル化，（174 ページ）
LDAP サーバ ホストの設定，（175 ページ）

LDAP サーバ グループの設定

サーバ グループを使用して、1 台または複数台のリモート AAA サーバによるユーザ認証を指定することができます。グループのメンバはすべて、LDAP を使用するように設定する必要があります。設定した順序に従ってサーバが試行されます。

これらのサーバ グループはいつでも設定できますが、設定したグループを有効にするには、AAA サービスに適用する必要があります。

はじめる前に

LDAP をイネーブルにします。

手順の概要

1. **configure terminal**
2. [**no**] **aaa group server ldap***group-name*
3. [**no**] **server** {*ipv4-address* | *ipv6-address* | *host-name*}
4. （任意） [**no**] **authentication** {**bind-first** [**append-with-baseDN** *DNstring*] | **compare** [**password-attribute** *password*]}
5. （任意） [**no**] **enable user-server-group**
6. （任意） [**no**] **enable Cert-DN-match**
7. （任意） [**no**] **use-vrf** *vrf-name*
8. **exit**
9. （任意） **show ldap-server groups**
10. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **aaa group server ldap***group-name*
	
	例：
	`switch(config)# aaa group server ldap LDAPServer1`
	`switch(config-ldap)#`
		LDAP サーバ グループを作成し、そのグループの LDAP サーバ グループ コンフィギュレーション モードを開始します。

ステップ 3	[**no**] **server** {*ipv4-address* | *ipv6-address* | *host-name*} 例： `switch(config-ldap)# server 10.10.2.2`	LDAP サーバを、LDAP サーバ グループのメンバとして設定します。 指定した LDAP サーバが見つからない場合は、**ldap-server host** コマンドを使用してサーバを設定し、このコマンドをもう一度実行します。
ステップ 4	[**no**] **authentication** {**bind-first** [**append-with-baseDN** *DNstring*] | **compare** [**password-attribute** *password*]} 例： `switch(config-ldap)# authentication compare password-attribute TyuL8r`	（任意） バインド方式または比較方式を使用して LDAP 認証を実行します。デフォルトの LDAP 認証方式は、検索してからバインドするバインド方式です。
ステップ 5	[**no**] **enable user-server-group** 例： `switch(config-ldap)# enable user-server-group`	（任意） グループ検証をイネーブルにします。LDAP サーバでグループ名を設定する必要があります。ユーザは、ユーザ名が LDAP サーバで設定されたこのグループのメンバとして示されている場合にだけ、公開キー認証を通じてログインできます。
ステップ 6	[**no**] **enable Cert-DN-match** 例： `switch(config-ldap)# enable Cert-DN-match`	（任意） ユーザ プロファイルでユーザ証明書のサブジェクト DN がログイン可能と示されている場合にだけユーザがログインできるようにします。
ステップ 7	[**no**] **use-vrf** *vrf-name* 例： `switch(config-ldap)# use-vrf vrf1`	（任意） サーバ グループ内のサーバとの接続に使用する VRF を指定します。 （注） このコマンドは、Cisco Nexus 7000 シリーズ スイッチでだけサポートされています。

	コマンドまたはアクション	目的

ステップ 8	**exit**
	
	例：
	`switch(config-ldap)# exit`
	`switch(config)#`
		LDAP サーバ グループ コンフィギュレーション モードを終了します。

ステップ 9	**show ldap-server groups** 例： `switch(config)# show ldap-server groups`	（任意） LDAP サーバ グループの設定を表示します。
ステップ 10	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

LDAP のイネーブル化，（174 ページ）
LDAP サーバ ホストの設定，（175 ページ）

グローバルな LDAP タイムアウト間隔の設定

Cisco NX-OS デバイスがすべての LDAP サーバからの応答を待つ時間を決定するグローバル タイムアウト間隔を設定できます。これを過ぎるとタイムアウト エラーになります。

はじめる前に

LDAP をイネーブルにします。

手順の概要

1. **configure terminal**
2. **[no] ldap-server timeout***seconds*
3. **exit**
4. （任意） **show ldap-server**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **ldap-server timeout***seconds* 例： `switch(config)# ldap-server timeout 10`	LDAP サーバのタイムアウト間隔を指定します。デフォルトのタイムアウト間隔は 5 秒です。有効な範囲は 1 ～ 60 秒です。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show ldap-server** 例： `switch# show ldap-server`	（任意） LDAP サーバの設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

LDAP のイネーブル化，（174 ページ）
LDAP サーバのタイムアウト間隔の設定，（181 ページ）

LDAP サーバのタイムアウト間隔の設定

Cisco NX-OS デバイスが LDAP サーバからの応答を待つ時間を決定するタイムアウト間隔を設定できます。これを過ぎるとタイムアウト エラーになります。

はじめる前に

LDAP をイネーブルにします。

手順の概要

1. **configure terminal**
2. [**no**] **ldap-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **timeout***seconds*
3. **exit**
4. （任意） **show ldap-server**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **ldap-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **timeout***seconds* 例： `switch(config)# ldap-server host server1 timeout 10`	特定のサーバのタイムアウト間隔を指定します。デフォルトはグローバル値です。 （注） 特定の LDAP サーバに指定したタイムアウト間隔は、すべての LDAP サーバで使用されるグローバルなタイムアウト間隔を上書きします。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show ldap-server** 例： `switch# show ldap-server`	（任意） LDAP サーバの設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

LDAP のイネーブル化, （174 ページ）
グローバルな LDAP タイムアウト間隔の設定, （180 ページ）

グローバル LDAP サーバ ポートの設定

クライアントが TCP 接続を開始するグローバル LDAP サーバ ポートを設定できます。デフォルトでは、Cisco NX-OS デバイスはすべての LDAP 要求に対しポート 389 を使用します。

はじめる前に

LDAP をイネーブルにします。

手順の概要

1. **configure terminal**
2. [**no**] **ldap-server port***tcp-port*
3. **exit**
4. （任意） **show ldap-server**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **ldap-server port***tcp-port* 例： `switch(config)# ldap-server port 2`	サーバへの LDAP メッセージに使用するグローバル TCP ポートを指定します。デフォルトの TCP ポートは 389 です。有効な範囲は 1 ～ 65535 です。 （注） このコマンドは、Cisco NX-OS Release 5.2 以降では推奨されません。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show ldap-server** 例： `switch# show ldap-server`	（任意） LDAP サーバの設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

LDAP のイネーブル化, （174 ページ）
TCP ポートの設定, （184 ページ）

TCP ポートの設定

別のアプリケーションとポート番号が競合している場合は、LDAP サーバ用に別の TCP ポートを設定できます。デフォルトでは、Cisco NX-OS デバイスはすべての LDAP 要求に対しポート 389 を使用します。

はじめる前に

LDAP をイネーブルにします。

手順の概要

1. **configure terminal**
2. [**no**] **ldap-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **port** *tcp-port* [**timeout** *seconds*]
3. **exit**
4. （任意） **show ldap-server**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **ldap-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **port** *tcp-port* [**timeout** *seconds*] 例： `switch(config)# ldap-server host 10.10.1.1 port 200 timeout 5`	サーバに送る LDAP メッセージに使用する TCP ポートを指定します。デフォルトの TCP ポートは 389 です。有効な範囲は 1 ～ 65535 です。任意でサーバのタイムアウト間隔を指定します。値の範囲は 1 ～ 60 秒です。デフォルトのタイムアウト値はグローバル値です（グローバル値が設定されていない場合は 5 秒）。 （注） 特定の LDAP サーバに指定したタイムアウト間隔は、すべての LDAP サーバで使用されるグローバルなタイムアウト間隔を上書きします。

	コマンドまたはアクション	目的

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show ldap-server** 例： `switch# show ldap-server`	（任意） LDAP サーバの設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

LDAP のイネーブル化，（174 ページ）
グローバル LDAP サーバ ポートの設定，（183 ページ）

LDAP 検索マップの設定

検索クエリーを LDAP サーバに送信するように LDAP 検索マップを設定できます。サーバはそのデータベースで、検索マップで指定された基準を満たすデータを検索します。

はじめる前に

LDAP をイネーブルにします。

手順の概要

1. **configure terminal**
2. **ldap search-map***map-name*
3. （任意） [**userprofile** | **trustedCert** | **CRLLookup** | **user-certdn-match** | **user-pubkey-match** | **user-switch-bind**] **attribute-name** *attribute-name* **search-filter** *filter* **base-DN** *base-DN-name*
4. **exit**
5. （任意） **show ldap-search-map**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**ldap search-map***map-name*
	
	例：
	`switch(config)# ldap search-map map1`
	`switch(config-ldap-search-map)#`
		LDAP 検索マップを設定します。

ステップ 3	[**userprofile** | **trustedCert** | **CRLLookup** | **user-certdn-match** | **user-pubkey-match** | **user-switch-bind**] **attribute-name** *attribute-name* **search-filter** *filter* **base-DN** *base-DN-name* 例： `switch(config-ldap-search-map)# userprofile attribute-name att-name search-filter (&(objectClass=inetOrgPerson)(cn=$userid)) base-DN dc=acme,dc=com`	（任意） ユーザ プロファイル、信頼できる証明書、CRL、証明書 DN 一致、公開キー一致、または user-switchgroup ルックアップ検索操作の属性名、検索フィルタ、およびベース DN を設定します。これらの値は、検索クエリーを LDAP サーバに送信するために使用されます。 *attribute-name* 引数は Nexus ロール定義を含む LDAP サーバ属性の名前です。

ステップ 4	**exit**
	
	例：
	`switch(config-ldap-search-map)# exit`
	`switch(config)#`
		LDAP 検索マップ コンフィギュレーション モードを終了します。

ステップ 5	**show ldap-search-map** 例： `switch(config)# show ldap-search-map`	（任意） 設定された LDAP 検索マップを表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

LDAP のイネーブル化, （174 ページ）

LDAP サーバの定期的モニタリングの設定

LDAP サーバの可用性をモニタリングできます。設定パラメータには、サーバに対して使用するユーザ名とパスワード、サーバにバインドして状態を確認するための rootDN、およびアイドル タイマーがあります。アイドル タイマーには、LDAP サーバで何の要求も受信されない状態の時間を指定します。これを過ぎると Cisco NX-OS デバイスはテスト パケットを送信します。このオプションを設定して定期的にサーバをテストしたり、1 回だけテストを実行したりできます。

（注） ネットワークのセキュリティを保護するために、LDAP データベースの既存のユーザ名と同じものを使用しないことを推奨します。

はじめる前に

LDAP をイネーブルにします。

手順の概要

1. **configure terminal**
2. [**no**] **ldap-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **test rootDN** *root-name* [**idle-time***minutes* | **password***password* [**idle-time***minutes*] | **username***name* [**password***password* [**idle-time***minutes*]]]
3. [**no**] **ldap-server deadtime***minutes*
4. **exit**
5. （任意） **show ldap-server**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **ldap-server host** {*ipv4-address* | *ipv6-address* | *host-name*} **test rootDN** *root-name* [**idle-time***minutes* | **password***password* [**idle-time***minutes*] | **username***name* [**password***password* [**idle-time***minutes*]]] 例： `switch(config)# ldap-server host 10.10.1.1 test rootDN root1 username user1 password Ur2Gd2BH idle-time 3`	サーバ モニタリング用のパラメータを指定します。デフォルトのユーザ名は test、デフォルトのパスワードは Cisco です。アイドル タイマーのデフォルト値は 60 分です。有効な範囲は 1 ～ 1,440 分です。 （注） LDAP サーバ データベースの既存のユーザでないユーザを指定することを推奨します。

	コマンドまたはアクション	目的
ステップ 3	[no] **ldap-server deadtime***minutes* 例： `switch(config)# ldap-server deadtime 5`	以前に応答の遅かった LDAP サーバを Cisco NX-OS デバイスがチェックを始めるまでの分数を指定します。デフォルト値は 0 分です。有効な範囲は 0 ～ 60 分です。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 5	**show ldap-server** 例： `switch# show ldap-server`	（任意） LDAP サーバの設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

LDAP のイネーブル化，（174 ページ）
LDAP サーバ ホストの設定，（175 ページ）

LDAP デッド タイム間隔の設定

すべての LDAP サーバのデッドタイム間隔を設定できます。デッドタイム間隔では、Cisco NX-OS デバイスが LDAP サーバをデッドであると宣言した後、そのサーバがアライブになったかどうかを確認するためにテスト パケットを送信するまでの時間を指定します。

（注） デッドタイム間隔に 0 分を設定すると、LDAP サーバは、応答を返さない場合でも、デッドとしてマークされません。デッド タイム間隔はグループ単位で設定できます。

はじめる前に

LDAP をイネーブルにします。

手順の概要

1. **configure terminal**
2. [**no**] **ldap-server deadtime** *minutes*
3. **exit**
4. （任意） **show ldap-server**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **ldap-server deadtime** *minutes* 例： `switch(config)# ldap-server deadtime 5`	グローバルなデッド タイム間隔を設定します。デフォルト値は 0 分です。範囲は 1 ～ 60 分です。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show ldap-server** 例： `switch# show ldap-server`	（任意） LDAP サーバの設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

LDAP のイネーブル化, （174 ページ）

LDAP サーバでの AAA 許可の設定

LDAP サーバのデフォルトの AAA 許可方式を設定できます。

はじめる前に

LDAP をイネーブルにします。

手順の概要

1. **configure terminal**
2. **aaa authorization** {**ssh-certificate** | **ssh-publickey**} **default** {**group***group-list* | **local**}
3. **exit**
4. （任意） **show aaa authorization** [**all**]
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**aaa authorization** {**ssh-certificate** | **ssh-publickey**} **default** {**group***group-list* | **local**}
	
	例：
	`switch(config)# aaa authorization ssh-certificate`
	`default group LDAPServer1 LDAPServer2`
		LDAP サーバのデフォルトの AAA 許可方式を設定します。
		ssh-certificate キーワードは、証明書認証を使用した LDAP 許可またはローカル許可を設定し、**ssh-publickey** キーワードは、SSH 公開キーを使用した LDAP 認可またはローカル認可を設定します。デフォルトの許可は、ユーザに割り当てたロールに対して許可されたコマンドのリストであるローカル許可です。
		group-list 引数には、LDAP サーバ グループ名をスペースで区切ったリストを指定します。このグループに属するサーバに対して、AAA 許可のためのアクセスが行われます。**local** 方式では、許可にローカル データベースが使用されます。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 4	**show aaa authorization** [**all**] 例： `switch(config)# show aaa authorization`	（任意） AAA 認可設定を表示します。**all** キーワードは、デフォルト値を表示します。

	コマンドまたはアクション	目的
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

関連トピック

LDAP のイネーブル化, （174 ページ）

LDAP のディセーブル化

LDAP をディセーブルにできます。

注意 LDAP をディセーブルにすると、関連するすべての設定が自動的に廃棄されます。

手順の概要

1. **configure terminal**
2. **no feature ldap**
3. **exit**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**no feature ldap** 例： `switch(config)# no feature ldap`	LDAP をディセーブルにします。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

	コマンドまたはアクション	目的
ステップ 4	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

LDAP サーバのモニタリング

Cisco NX-OS デバイスが保持している LDAP サーバのアクティビティに関する統計情報をモニタリングできます。

はじめる前に

Cisco NX-OS デバイスに LDAP サーバを設定します。

手順の概要

1. **show ldap-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show ldap-server statistics** {*hostname*	*ipv4-address*	*ipv6-address*} 例： `switch# show ldap-server statistics 10.10.1.1`	LDAP 統計情報を表示します。

関連トピック

LDAP サーバ ホストの設定，（175 ページ）
LDAP サーバ統計情報のクリア，（192 ページ）

LDAP サーバ統計情報のクリア

Cisco NX-OS デバイスが保持している LDAP サーバのアクティビティに関する統計情報を表示します。

はじめる前に

Cisco NX-OS デバイスに LDAP サーバを設定します。

手順の概要

1. （任意） **show ldap-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*}
2. **clear ldap-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show ldap-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*} 例： `switch# show ldap-server statistics 10.10.1.1`	（任意） Cisco NX-OS デバイスでの LDAP サーバ統計情報を表示します。
ステップ 2	**clear ldap-server statistics** {*hostname* | *ipv4-address* | *ipv6-address*} 例： `switch# clear ldap-server statistics 10.10.1.1`	LDAP サーバ統計情報をクリアします。

関連トピック

LDAP サーバ ホストの設定，（175 ページ）
LDAP サーバのモニタリング，（192 ページ）

LDAP 設定の確認

LDAP 設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show running-config ldap [**all**]	実行コンフィギュレーションの LDAP 設定を表示します。
show startup-config ldap	スタートアップ コンフィギュレーションの LDAP 設定を表示します。
show ldap-server	LDAP 設定情報を表示します。
show ldap-server groups	LDAP サーバ グループの設定情報を表示します。

コマンド	目的
show ldap-server statistics {*host-name* | *ipv4-address* | *ipv6-address*}	LDAP 統計情報を表示します。
show ldap-search-map	設定されている LDAP 属性マップに関する情報を表示します。

このコマンドの出力フィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

LDAP の設定例

次に、LDAP サーバ ホストおよびサーバ グループを設定する例を示します。

```
feature ldap
ldap-server host 10.10.2.2 enable-ssl
aaa group server ldap LdapServer
    server 10.10.2.2
exit
show ldap-server
show ldap-server groups
```

次に、LDAP 検索マップを設定する例を示します。

```
ldap search-map s0
userprofile attribute-name description search-filter
(&(objectClass=inetOrgPerson)(cn=$userid)) base-DN dc=acme,dc=com
exit
show ldap-search-map
```

次に、LDAP サーバに対する証明書認証を使用して AAA 許可を設定する例を示します。

```
aaa authorization ssh-certificate default group LDAPServer1 LDAPServer2
exit
show aaa authorization
```

次の作業

これで、サーバ グループも含めて AAA 認証方式を設定できるようになります。

LDAP に関する追加情報

ここでは、LDAP の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS のライセンス	『*Cisco NX-OS Licensing Guide*』
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』
VRF コンフィギュレーション	『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
• CISCO-AAA-SERVER-MIB • CISCO-AAA-SERVER-EXT-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

LDAP の機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 *15*： *LDAP* の機能の履歴

機能名	リリース	機能情報
LDAP	6.0(1)	Release 5.2 以降、変更はありません。
LDAP	5.2(1)	**ldap-server port** コマンドが非推奨になりました。

機能名	リリース	機能情報
LDAP	5.1(1)	Release 5.0 以降、変更はありません。
LDAP	5.0(2)	この機能が導入されました。

第 8 章

SSH および Telnet の設定

この章では、Cisco NX-OS デバイス上でセキュア シェル（SSH）プロトコルおよび Telnet を設定する手順について説明します。

この章は、次の項で構成されています。

- 機能情報の確認，197 ページ
- SSH および Telnet の概要，198 ページ
- SSH および Telnet のライセンス要件，200 ページ
- SSH および Telnet の前提条件，200 ページ
- SSH と Telnet の注意事項と制約事項，200 ページ
- SSH および Telnet のデフォルト設定，201 ページ
- SSH の設定，201 ページ
- Telnet の設定，216 ページ
- SSH および Telnet の設定の確認，219 ページ
- SSH の設定例，220 ページ
- SSH のパスワードが不要なファイル コピーの設定例，221 ページ
- SSH および Telnet に関する追加情報，222 ページ
- SSH および Telnet の機能の履歴，223 ページ

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリス

トについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

SSH および Telnet の概要

ここでは、SSH および Telnet について説明します。

SSH サーバ

SSH サーバを使用すると、SSH クライアントは Cisco NX-OS デバイスとの間で暗号化された安全な接続を確立できます。SSH は強化暗号化を使用して認証を行います。Cisco NX-OS ソフトウェアの SSH サーバは、市販の一般的な SSH クライアントと相互運用ができます。

SSH がサポートするユーザ認証メカニズムには、Remote Authentication Dial-In User Service（RADIUS）、TACACS+、LDAP、およびローカルに格納されたユーザ名とパスワードを使用した認証があります。

SSH クライアント

SSH クライアントは、SSH プロトコルで稼働しデバイス認証および暗号化を提供するアプリケーションです。Cisco NX-OS デバイスは、SSH クライアントを使用して、別の Cisco NX-OS デバイスまたは SSH サーバの稼働する他のデバイスとの間で暗号化された安全な接続を確立できます。この接続は、暗号化されたアウトバウンド接続を実現します。認証と暗号化により、SSH クライアントは、セキュリティ保護されていないネットワーク上でもセキュアな通信を実現できます。

Cisco NX-OS ソフトウェアの SSH クライアントは、市販の一般的な SSH クライアントと相互運用ができます。

SSH サーバ キー

SSH では、Cisco NX-OS デバイスと安全な通信を行うためにサーバ キーが必要です。SSH サーバ キーは、次の SSH オプションに使用できます。

- Rivest, Shamir, and Adelman（RSA）公開キー暗号化を使用した SSH バージョン 2
- Digital System Algrorithm（DSA）を使用した SSH バージョン 2

SSH サービスをイネーブルにする前に、適切なバージョンの SSH サーバ キー ペアを取得してください。使用中の SSH クライアント バージョンに応じて、SSH サーバ キー ペアを生成します。SSH サービスは、SSH バージョン 2 で使用する次の 2 種類のキー ペアを受け入れます。

- **dsa** オプションを使用すると、SSH バージョン 2 プロトコルに対応する DSA キーペアが生成されます。

- **rsa** オプションを使用すると、SSH バージョン 2 プロトコルに対応する RSA キーペアが生成されます。

デフォルトでは、Cisco NX-OS ソフトウェアは 1024 ビットの RSA キーを作成します。

SSH は、次の公開キー形式をサポートします。

- OpenSSH
- IETF SSH（SECSH）
- Privacy-Enhanced Mail（PEM）の公開キー証明書

注意 SSH キーをすべて削除すると、SSH サービスを開始できません。

デジタル証明書を使用した SSH 認証

Cisco NX-OS デバイスでの SSH 認証では、ホスト認証用に X.509 デジタル証明書をサポートしています。X.509 デジタル証明書は、メッセージの出所と整合性を保証するデータ項目です。これには安全な通信のための暗号化されたキーが含まれています。また、発信者のアイデンティティを証明するために信頼できる認証局（CA）によって署名されています。X.509 デジタル証明書のサポートにより、認証に DSA と RSA のいずれかのアルゴリズムを使用します。

証明書のインフラストラクチャでは、Secure Socket Layer（SSL）に対応し、セキュリティ インフラストラクチャによってクエリーまたは通知を通じて最初に返される証明書が使用されます。証明書が信頼できる CA のいずれかから発行されたものであれば、証明書の検証は成功です。

デバイスは、X.509 証明書を使用する SSH 認証用か、公開キー証明書を使用する SSH 認証用のいずれかに設定できますが、両方は不可能です。これらのいずれかが設定されているときに認証に失敗すると、パスワードの入力が求められます。

Telnet サーバ

Telnet プロトコルは、ホストとの TCP/IP 接続を確立します。Telnet を使用すると、あるサイトのユーザが別のサイトのログイン サーバと TCP 接続を確立し、キーストロークをデバイス間でやり取りできます。Telnet は、リモート デバイス アドレスとして IP アドレスまたはドメイン名のいずれかを受け入れます。

デフォルトでは、Telnet サーバは Cisco NX-OS デバイス上でディセーブルになっています。

SSH および Telnet のバーチャライゼーション サポート

SSH および Telnet の設定と操作は、仮想デバイス コンテキスト（VDC）に対してローカルです。VDC の詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

SSH および Telnet のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	SSH および Telnet にはライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

SSH および Telnet の前提条件

SSH および Telnet の前提条件は次のとおりです。

- レイヤ 3 インターフェイス上に IP、mgmt 0 インターフェイス上にアウトバンド、またはイーサネット インターフェイス上にインバンドを設定していること

SSH と Telnet の注意事項と制約事項

SSH および Telnet に関する注意事項と制約事項は次のとおりです。

- Cisco NX-OS ソフトウェアは、SSH バージョン 2（SSHv2）だけをサポートしています。
- デバイスには、X.509 証明書を使用した SSH 認証か、または公開キー証明書を使用した SSH 認証のどちらかを設定できますが、その両方は設定できません。これらのいずれかが設定されているときに認証に失敗すると、パスワードの入力が求められます。
- Cisco NX-OS Release 5.1 から、SSH は FIPS モードで実行されます。
- SFTP サーバ機能では、通常の SFTP の **chown** および **chgrp** コマンドはサポートされません。
- SFTP サーバがイネーブルになっている場合は、admin ユーザだけが SFTP を使用してスイッチにアクセスできます。

（注） Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

関連トピック

FIPS の設定, （23 ページ）

SSH および Telnet のデフォルト設定

次の表に、SSH および Telnet パラメータのデフォルト設定を示します。

表 *16*：デフォルトの *SSH* および *Telnet* パラメータ

パラメータ	デフォルト
SSH サーバ	イネーブル
SSH サーバ キー	1024 ビットで生成された RSA キー
RSA キー生成ビット数	1024
Telnet サーバ	ディセーブル
Telnet ポート番号	23
SSH ログインの最大試行回数	3
SCP サーバ	ディセーブル
SFTP サーバ	ディセーブル

SSH の設定

ここでは、SSH の設定方法について説明します。

SSH サーバ キーの生成

セキュリティ要件に基づいて SSH サーバ キーを生成できます。デフォルトの SSH サーバ キーは、1024 ビットで生成される RSA キーです。

手順の概要

1. **configure terminal**
2. **no feature ssh**
3. **ssh key** {**dsa** [**force**] | **rsa** [*bits* [**force**]]}
4. **feature ssh**
5. **exit**
6. （任意） **show ssh key**
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**no feature ssh** 例： `switch(config)# no feature ssh`	SSH をディセーブルにします。
ステップ 3	**ssh key** {**dsa** [**force**]	**rsa** [*bits* [**force**]]} 例： `switch(config)# ssh key rsa 2048`	SSH サーバ キーを生成します。 *bits* 引数には、RSA キーの生成に使用するビット数を指定します。Cisco NX-OS Release 5.1 以降では、範囲は 1024 ～ 2048 です。Cisco NX-OS Release 5.0 で、範囲は 768 ～ 2048 です。デフォルト値は 1024 です。 DSA キーのサイズを指定できません。これは常に 1024 ビットに設定されます。 既存のキーを置き換える場合は、キーワード **force** を使用します。
ステップ 4	**feature ssh** 例： `switch(config)# feature ssh`	SSH をイネーブルにします。

ステップ 5	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 6	**show ssh key** 例： `switch# show ssh key`	（任意） SSH サーバ キーを表示します。
ステップ 7	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ユーザ アカウント用 SSH 公開キーの指定

SSH 公開キーを設定すると、パスワードを要求されることなく、SSH クライアントを使用してログインできます。SSH 公開キーは、次のいずれかの形式で指定できます。

- OpenSSH 形式
- Internet Engineering Task Force（IETF）SECSH 形式
- Privacy Enhanced Mail（PEM）形式の公開キー証明書

IETF SECSH 形式による SSH 公開キーの指定

ユーザ アカウント用に IETF SECSH 形式で SSH 公開キーを指定できます。

はじめる前に

IETF SCHSH 形式の SSH 公開キーを作成します。

手順の概要

1. **copy***server-file***bootflash:***filename*
2. **configure terminal**
3. **username***username***sshkey file bootflash:***filename*
4. **exit**
5. （任意） **show user-account**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**copy***server-file***bootflash:***filename* 例： `switch# copy tftp://10.10.1.1/secsh_file.pub bootflash:secsh_file.pub`	サーバから IETF SECSH 形式の SSH キーを含むファイルをダウンロードします。サーバは FTP、Secure Copy（SCP）、Secure FTP（SFTP）、または TFTP のいずれかを使用できます。
ステップ 2	**configure terminal** 例： `switch# configure terminal switch(config)#`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**username***username***sshkey file bootflash:***filename* 例： `switch(config)# username User1 sshkey file bootflash:secsh_file.pub`	IETF SECSH 形式の SSH 公開キーを設定します。
ステップ 4	**exit** 例： `switch(config)# exit switch#`	グローバル コンフィギュレーション モードを終了します。
ステップ 5	**show user-account** 例： `switch# show user-account`	（任意） ユーザ アカウントの設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

OpenSSH 形式の SSH 公開キーの指定

ユーザ アカウントに OpenSSH 形式の SSH 公開キーを指定できます。

はじめる前に

OpenSSH 形式の SSH 公開キーを作成します。

手順の概要

1. **configure terminal**
2. **username** *username* **sshkey** *ssh-key*
3. **exit**
4. （任意） **show user-account**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**username** *username* **sshkey** *ssh-key* 例： `switch(config)# username User1 sshkey ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZl9G+3f1XswK3OiW4H7YyUyuA50rv7gsEPjhOBYmsi6PAVKui1nIf/DQhum+lJNqJP/eLowb7ubO+lVKRXFY/G+lJNIQW3g9igG30c6k6+XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmSiH3UD/vKyziEh5S4Tplx8=`	OpenSSH 形式の SSH 公開キーを設定します。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 4	**show user-account** 例： `switch# show user-account`	（任意） ユーザ アカウントの設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

SSH ログイン試行の最大回数の設定

SSH ログイン試行の最大回数を設定できます。許可される試行の最大回数を超えると、セッションが切断されます。

（注） ログイン試行の合計回数には、公開キー認証、証明書ベースの認証、およびパスワードベースの認証を使用した試行が含まれます。イネーブルにされている場合は、公開キー認証が優先されます。証明書ベースとパスワード ベースの認証だけがイネーブルにされている場合は、証明書ベースの認証が優先されます。これらすべての方法で、ログイン試行の設定された数を超えると、認証失敗回数を超過したことを示すメッセージが表示されます。

手順の概要

1. **configure terminal**
2. **ssh login-attempts***number*
3. （任意） **show running-config security all**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**ssh login-attempts***number* 例： `switch(config)# ssh login-attempts 5`	ユーザが SSH セッションへのログインを試行できる最大回数を設定します。ログイン試行のデフォルトの最大回数は 3 です。値の範囲は 1 ～ 10 です。 （注） このコマンドの **no** 形式を使用すると、以前のログイン試行の値が削除され、ログイン試行の最大回数がデフォルト値の 3 に設定されます。
ステップ 3	**show running-config security all** 例： `switch(config)# show running-config security all`	（任意） SSH ログイン試行の設定された最大回数を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） （任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

SSH 接続のログイン猶予時間の設定

リモート デバイスから Cisco NX-OS デバイスへの SSH 接続に対しては、ログイン猶予時間を設定できます。この設定では、クライアントが認証を完了するまでの猶予時間を指定します。SSH セッションにログインするまでの時間が指定した猶予時間を超えるとセッションが切断され、再度ログインを試みる必要があります。

（注） リモート デバイスの SSH サーバをイネーブルにします。

手順の概要

1. **configure terminal**
2. **feature ssh**
3. **ssh login-gracetime***number*
4. （任意） **exit**
5. （任意） **show running-config security**
6. （任意） **show running-config security all**
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**feature ssh**
	
	例：
	`switch# feature ssh`
	`switch(config)#`
		SSH をイネーブルにします。

ステップ 3	**ssh login-gracetime***number* 例： `switch(config)# ssh login-gracetime 120`	リモート デバイスから Cisco NX-OS デバイスへの SSH 接続のログイン猶予時間を秒単位で設定します。デフォルトのログイン猶予時間は 120 秒です。範囲は、1 ～ 2147483647 です。 （注） このコマンドの **no** 形式を使用すると設定したログイン猶予時間が削除され、デフォルト値の 120 秒にリセットされます。

	コマンドまたはアクション	目的
ステップ 4	**exit** 例： `switch(config)# exit`	（任意） グローバル コンフィギュレーション モードを終了します。
ステップ 5	**show running-config security** 例： `switch(config)# show running-config security`	（任意） 設定した SSH ログイン猶予時間が表示されます。
ステップ 6	**show running-config security all** 例： `switch(config)# show running-config security all`	（任意） デフォルトまたは設定した SSH ログイン猶予時間が表示されます。
ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） （任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。

SSH セッションの開始

Cisco NX-OS デバイスから IPv4 または IPv6 を使用して SSH セッションを開始し、リモート デバイスと接続します。

はじめる前に

リモートデバイスのホスト名を取得し、必要なら、リモートデバイスのユーザ名も取得します。

リモート デバイスの SSH サーバをイネーブルにします。

手順の概要

1. **ssh** [*username@*]{*ipv4-address* | *hostname*} [**vrf***vrf-name*]
2. **ssh6** [*username@*]{*ipv6-address* | *hostname*} [**vrf** *vrf-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ssh** [*username@*]{*ipv4-address* | *hostname*} [**vrf***vrf-name*] 例： `switch# ssh 10.10.1.1`	IPv4 を使用してリモート デバイスとの SSH IPv4 セッションを作成します。デフォルトの VRF はデフォルト VRF です。
ステップ 2	**ssh6** [*username@*]{*ipv6-address* | *hostname*} [**vrf** *vrf-name*] 例： `switch# ssh6 HostA`	IPv6 を使用してリモート デバイスとの SSH IPv6 セッションを作成します。

ブート モードからの SSH セッションの開始

SSH セッションは、リモート デバイスに接続する Cisco NX-OS デバイスのブート モードから開始できます。

はじめる前に

リモートデバイスのホスト名を取得し、必要なら、リモートデバイスのユーザ名も取得します。

リモート デバイスの SSH サーバをイネーブルにします。

Cisco NX-OS デバイスがキックスタート イメージのみを使用してロードされていることを確認します。

手順の概要

1. **ssh** [*username@*]*hostname*
2. **exit**
3. **copy scp:**//[*username@*]*hostname*/*filepath directory*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ssh** [*username@*]*hostname* 例： `switch(boot)# ssh user1@10.10.1.1`	リモート デバイスへの SSH セッションを、Cisco NX-OS デバイスのブート モードから作成します。デフォルト VRF が常に使用されます。

	コマンドまたはアクション	目的
ステップ 2	**exit** 例： `switch(boot)# exit`	ブート モードを終了します。
ステップ 3	**copy scp:**//[*username@*]*hostname*/*filepath directory* 例： `switch# copy scp://user1@10.10.1.1/users abc`	セキュア コピー プロトコル（SCP）を使用して、ファイルを Cisco NX-OS デバイスからリモート デバイスへコピーします。デフォルト VRF が常に使用されます。

SSH のパスワードが不要なファイル コピーの設定

Cisco NX-OS デバイスから Secure Copy（SCP）サーバまたは Secure FTP（SFTP）サーバに、パスワードなしでファイルをコピーすることができます。これを行うには、SSH による認証用の公開キーと秘密キーで構成される RSA または DSA のアイデンティティを作成する必要があります。

手順の概要

1. **configure terminal**
2. [**no**] **username** *username* **keypair generate** {**rsa** [*bits* [**force**]] | **dsa** [**force**]}
3. （任意） **show username** *username* **keypair**
4. **username** *username* **keypair export** {**bootflash:***filename* | **volatile:***filename*} {**rsa** | **dsa**} [**force**]
5. **username** *username* **keypair import** {**bootflash:***filename* | **volatile:***filename*} {**rsa** | **dsa**} [**force**]

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **username** *username* **keypair generate** {**rsa** [*bits* [**force**]]	**dsa** [**force**]} 例： `switch(config)# username user1 keypair generate rsa 2048 force`	SSH の公開キーと秘密キーを生成し、指定したユーザの Cisco NX-OS デバイスのホームディレクトリ（$HOME/.ssh）に格納します。Cisco NX-OS デバイスでは、これらのキーを使用してリモート マシンの SSH サーバと通信します。

	コマンドまたはアクション	目的
		bits 引数には、キーの生成に使用するビット数を指定します。Cisco NX-OS Release 5.1 以降では、範囲は 1024 ～ 2048 です。Cisco NX-OS Release 5.0 で、範囲は 768 ～ 2048 です。デフォルト値は 1024 です。 既存のキーを置き換える場合は、キーワード **force** を使用します。**force** キーワードを省略した場合、SSH キーがすでに存在していれば、SSH キーは生成されません。
ステップ 3	**show username** *username* **keypair** 例： `switch(config)# show username user1 keypair`	（任意） 指定したユーザの公開キーを表示します。 （注） セキュリティ上の理由から、このコマンドで秘密キーは表示されません。
ステップ 4	**username** *username* **keypair export** {**bootflash:***filename* | **volatile:***filename*} {**rsa** | **dsa**} [**force**] 例： `switch(config)# username user1 keypair export bootflash:key_rsa rsa`	Cisco NX-OS デバイスのホーム ディレクトリから、指定したブートフラッシュ ディレクトリまたは一時ディレクトリに、公開キーと秘密キーをエクスポートします。 既存のキーを置き換える場合は、キーワード **force** を使用します。**force** キーワードを省略した場合、SSH キーがすでに存在していれば、SSH キーはエクスポートされません。 生成したキー ペアをエクスポートするとき、秘密キーを暗号化するパスフレーズを入力するように求められます。秘密キーは、指定したファイルとしてエクスポートされ、公開キーは、同じファイル名に .pub 拡張子を付けてエクスポートされます。これで、このキー ペアを任意の Cisco NX-OS デバイスにコピーし、SCP または SFTP を使用してサーバのホーム ディレクトリに公開キー ファイル（*.pub）をコピーできるようになります。 （注） セキュリティ上の理由から、このコマンドはグローバル コンフィギュレーション モードでしか実行できません。
ステップ 5	**username** *username* **keypair import** {**bootflash:***filename* | **volatile:***filename*} {**rsa** | **dsa**} [**force**] 例： `switch(config)# username user1 keypair import bootflash:key_rsa rsa`	指定したブートフラッシュ ディレクトリまたは一時ディレクトリから、Cisco NX-OS デバイスのホーム ディレクトリに、エクスポートした公開キーと秘密キーをインポートします。 既存のキーを置き換える場合は、キーワード **force** を使用します。**force** キーワードを省略した場合、SSH キーがすでに存在していれば、SSH キーはインポートされません。 生成したキー ペアをインポートするとき、秘密キーを復号化するパスフレーズを入力するように求められます。秘密キーは指定したファイルとしてインポートされ、公開キーは同じファイル名に .pub 拡張子を付けてインポートされます。 （注） セキュリティ上の理由から、このコマンドはグローバル コンフィギュレーション モードでしか実行できません。

	コマンドまたはアクション	目的
		（注） パスワードなしでサーバにアクセスできるのは、サーバでキーが設定されているユーザのみです。

次の作業

SCP サーバまたは SFTP サーバで、次のコマンドを使用して、*.pub ファイル（たとえば、key_rsa.pub）に格納された公開キーを authorized_keys ファイルに追加します。

$ cat key_rsa.pub >> $HOME/.ssh/ authorized_keys

これで、標準の SSH コマンドおよび SCP コマンドを使用してパスワードを指定しなくても、Cisco NX-OS デバイスからサーバにファイルをコピーできます。

SCP サーバと SFTP サーバの設定

リモート デバイスとの間でファイルをコピーできるように、Cisco NX-OS デバイスで SCP サーバまたは SFTP サーバを設定できます。SCP サーバまたは SFTP サーバをイネーブルにした後、Cisco NX-OS デバイスとの間でファイルをコピーするために、リモート デバイスで SCP または SFTP コマンドを実行できます。

（注） arcfour および blowfish cipher オプションは SCP サーバではサポートされません。

手順の概要

1. **configure terminal**
2. [**no**] **feature scp-server**
3. [**no**] **feature sftp-server**
4. **exit**
5. （任意） **show running-config security**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	[no] feature scp-server 例： switch(config)# feature scp-server	Cisco NX-OS デバイスで SCP サーバをイネーブルまたはディセーブルにします。
ステップ 3	[no] feature sftp-server 例： switch(config)# feature sftp-server	Cisco NX-OS デバイスで SFTP サーバをイネーブルまたはディセーブルにします。
ステップ 4	exit 例： switch(config)# exit switch#	グローバル コンフィギュレーション モードを終了します。
ステップ 5	show running-config security 例： switch# show running-config security	（任意） SCP サーバと SFTP サーバの設定ステータスを表示します。
ステップ 6	copy running-config startup-config 例： switch# copy running-config startup-config	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

SSH ホストのクリア

サーバから SCP または SFTP を使用してファイルをダウンロードする場合、またはこのデバイスからリモート ホストに SSH セッションを開始する場合には、そのサーバと信頼できる SSH 関係が確立されます。ユーザアカウントの、信頼できる SSH サーバのリストはクリアすることができます。

手順の概要

1. **clear ssh hosts**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	clear ssh hosts 例： switch# clear ssh hosts	SSH ホスト セッションおよび既知のホスト ファイルをクリアします。

SSH サーバのディセーブル化

デフォルトでは、SSH サーバは Cisco NX-OS デバイス上でイネーブルになっています。SSH サーバをディセーブルにすると、SSH でスイッチにアクセスすることを防止できます。

手順の概要

1. **configure terminal**
2. **no feature ssh**
3. **exit**
4. （任意） **show ssh server**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**no feature ssh** 例： `switch(config)# no feature ssh`	SSH をディセーブルにします。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 4	**show ssh server** 例： `switch# show ssh server`	（任意） SSH サーバの設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

SSH サーバ キーの削除

SSH サーバをディセーブルにした後、Cisco NX-OS デバイス上の SSH サーバ キーを削除できます。

（注） SSH を再度イネーブルにするには、まず、SSH サーバ キーを生成する必要があります。

手順の概要

1. **configure terminal**
2. **no feature ssh**
3. **no ssh key** [**dsa** | **rsa**]
4. **exit**
5. （任意） **show ssh key**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**no feature ssh** 例： `switch(config)# no feature ssh`	SSH をディセーブルにします。
ステップ 3	**no ssh key** [**dsa**	**rsa**] 例： `switch(config)# no ssh key rsa`	SSH サーバ キーを削除します。 デフォルトでは、すべての SSH キーが削除されます。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 5	**show ssh key** 例： `switch# show ssh key`	（任意） SSH サーバ キーの設定を表示します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

SSH サーバ キーの生成, （201 ページ）

SSH セッションのクリア

Cisco NX-OS デバイスから SSH セッションを クリアできます。

手順の概要

1. **show users**
2. **clear line***vty-line*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show users** 例： `switch# show users`	ユーザ セッション情報を表示します。
ステップ 2	**clear line***vty-line* 例： `switch(config)# clear line pts/12`	ユーザ SSH セッションをクリアします。

Telnet の設定

ここでは、Cisco NX-OS デバイスで Telnet を設定する手順を説明します。

Telnet サーバのディセーブル化

Telnet サーバを Cisco NX-OS デバイス上でイネーブルにできます。デフォルトでは、Telnet はディセーブルです。

手順の概要

1. **configure terminal**
2. **feature telnet**
3. **exit**
4. （任意） **show telnet server**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**feature telnet** 例： `switch(config)# feature telnet`	Telnet サーバをイネーブルにします。デフォルトではディセーブルになっています。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 4	**show telnet server** 例： `switch# show telnet server`	（任意） Telnet サーバの設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

リモート デバイスとの Telnet セッションの開始

Cisco NX-OS デバイスから SSH セッションを開始して、リモート デバイスと接続できます。IPv4 または IPv6 のいずれかを使用して Telnet セッションを開始できます。

はじめる前に

リモート デバイスのホスト名または IP アドレスと、必要な場合はリモート デバイスのユーザ名を取得します。

Cisco NX-OS デバイス上で Telnet サーバをイネーブルにします。

リモート デバイス上で Telnet サーバをイネーブルにします。

手順の概要

1. **telnet** {*ipv4-address* | *host-name*} [*port-number*] [**vrf***vrf-name*]
2. **telnet6** {*ipv6-address* | *host-name*} [*port-number*] [**vrf***vrf-name*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**telnet** {*ipv4-address* | *host-name*} [*port-number*] [**vrf***vrf-name*] 例： `switch# telnet 10.10.1.1`	IPv4 を使用してリモート デバイスとの Telnet セッションを開始します。デフォルトのポート番号は 23 です。有効な範囲は 1 ～ 65535 です。デフォルトの VRF はデフォルト VRF です。
ステップ 2	**telnet6** {*ipv6-address* | *host-name*} [*port-number*] [**vrf***vrf-name*] 例： `switch# telnet6 2001:0DB8::ABCD:1 vrf management`	IPv6 を使用してリモート デバイスとの Telnet セッションを開始します。デフォルトのポート番号は 23 です。有効な範囲は 1 ～ 65535 です。デフォルトの VRF はデフォルト VRF です。

関連トピック

Telnet サーバのディセーブル化, （217 ページ）

Telnet セッションのクリア

Telnet セッションを Cisco NX-OS デバイスからクリアできます。

はじめる前に

Cisco NX-OS デバイス上で Telnet サーバをイネーブルにします。

手順の概要

1. **show users**
2. **clear line***vty-line*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show users** 例： `switch# show users`	ユーザ セッション情報を表示します。
ステップ 2	**clear line***vty-line* 例： `switch(config)# clear line pts/12`	ユーザ Telnet セッションをクリアします。

SSH および Telnet の設定の確認

SSH および Telnet の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show ssh key [**dsa** | **rsa**]	SSH サーバ キー ペアの情報を表示します。
show running-config security [**all**]	実行コンフィギュレーション内の SSH とユーザ アカウントの設定を表示します。キーワード **all** を指定すると、SSH およびユーザ アカウントのデフォルト値が表示されます。
show ssh server	SSH サーバの設定を表示します。
show telnet server	Telnet サーバの設定を表示します。
show username *username* **keypair**	指定したユーザの公開キーを表示します。

これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

SSH の設定例

次の例は、OpenSSH キーを使用して SSH を設定する方法を示しています。

ステップ 1 SSH サーバをディセーブルにします。

例：
```
switch# configure terminal
switch(config)# no feature ssh
```

ステップ 2 SSH サーバ キーを生成します。

例：

```
switch(config)# ssh key rsa
generating rsa key(1024 bits)......
generated rsa key
```

ステップ 3 SSH サーバをイネーブルにします。

例：
```
switch(config)# feature ssh
```

ステップ 4 SSH サーバ キーを表示します。

例：
```
switch(config)# show ssh key
rsa Keys generated:Sat Sep 29 00:10:39 2007

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAvWhEBsF55oaPHNDBnpXOTw6+/OdHoLJZKr
+MZm99n2U0ChzZG4svRWmHuJY4PeDWl0e5yE3g3EO3pjDDmt923siNiv5aSga60K36lr39
HmXL6VgpRVn1XQFiBwn4na+H1d3Q0hDt+uWEA0tka2uOtXlDhliEmn4HVXOjGhFhoNE=

bitcount:1024
fingerprint:
51:6d:de:1c:c3:29:50:88:df:cc:95:f0:15:5d:9a:df
************************************
could not retrieve dsa key information
************************************
```

ステップ 5 OpenSSH 形式の SSH 公開キーを指定します。

例：
```
switch(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZl9G+3f1XswK3OiW4H7YyUyuA50r
v7gsEPjhOBYmsi6PAVKui1nIf/DQhum+lJNqJP/eLowb7ubO+lVKRXFY/G+lJNIQ
W3g9igG30c6k6+XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmSiH3UD/vKyziEh5
4Tplx8=
```

ステップ 6 設定を保存します。

例：
```
switch(config)# copy running-config startup-config
```

SSH のパスワードが不要なファイル コピーの設定例

次に、Cisco NX-OS デバイスから Secure Copy（SCP）サーバまたは Secure FTP（SFTP）サーバに、パスワードなしでファイルをコピーする例を示します。

ステップ 1 SSH の公開キーと秘密キーを生成し、指定したユーザの Cisco NX-OS デバイスのホーム ディレクトリに格納します。

例：
```
switch# configure terminal
switch(config)# username admin keypair generate rsa
generating rsa key(1024 bits)......
generated rsa key
```

ステップ 2 指定したユーザの公開キーを表示します。

例：
```
switch(config)# show username admin keypair

**************************************

rsa Keys generated: Thu Jul  9 11:10:29 2009

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAxWmjJT+oQhIcvnrMbx2BmD0P8boZElTfJ
Fx9fexWp6rOiztlwODtehnjadWc6A+DE2DvYNvqsrU9TBypYDPQkR/+Y6cKubyFW
VxSBG/NHztQc3+QC1zdkIxGNJbEHyFoajzNEO8LLOVFIMCZ2Td7gxUGRZc+fbq
S33GZsCAX6v0=

bitcount:262144
fingerprint:
8d:44:ee:6c:ca:0b:44:95:36:d0:7d:f2:b5:78:74:7d
**************************************

could not retrieve dsa key information
**************************************
```

ステップ 3 Cisco NX-OS デバイスのホームディレクトリから、指定したブートフラッシュディレクトリに、公開キーと秘密キーをエクスポートします。

例：
```
switch(config)# username admin keypair export bootflash:key_rsa rsa
Enter Passphrase:
switch(config)# dir
.
```

```
.
.
        951     Jul 09 11:13:59 2009  key_rsa
        221     Jul 09 11:14:00 2009  key_rsa.pub
.
.
```

ステップ 4 **copy scp** または **copy sftp** コマンドを使用して、別の Cisco NX-OS デバイスにこれら 2 つのファイルをコピーした後、Cisco NX-OS デバイスのホーム ディレクトリにインポートします。

例：

```
switch(config)# username admin keypair import bootflash:key_rsa rsa
Enter Passphrase:
switch(config)# show username admin keypair
**************************************

rsa Keys generated: Thu Jul  9 11:10:29 2009

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAxWmjJT+oQhIcvnrMbx2BmD0P8boZElTfJ
Fx9fexWp6rOiztlwODtehnjadWc6A+DE2DvYNvqsrU9TBypYDPQkR/+Y6cKubyFW
VxSBG/NHztQc3+QC1zdkIxGNJbEHyFoajzNEO8LLOVFIMCZ2Td7gxUGRZc+fbq
S33GZsCAX6v0=

bitcount:262144
fingerprint:
8d:44:ee:6c:ca:0b:44:95:36:d0:7d:f2:b5:78:74:7d
**************************************

could not retrieve dsa key information
**************************************
switch(config)#
```

ステップ 5 SCP サーバまたは SFTP サーバで、key_rsa.pub に格納されている公開キーを authorized_keys ファイルに追加します。

例：

```
$ cat key_rsa.pub >> $HOME/.ssh/ authorized_keys
```

これで、標準の SSH コマンドおよび SCP コマンドを使用してパスワードを指定しなくても、Cisco NX-OS デバイスからサーバにファイルをコピーできます。

ステップ 6 （任意） DSA キーについてこの手順を繰り返します。

SSH および Telnet に関する追加情報

ここでは、SSH および Telnet の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS のライセンス	『*Cisco NX-OS Licensing Guide*』
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』
VRF コンフィギュレーション	『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
• CISCO-SECURE-SHELL-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

SSH および Telnet の機能の履歴

次の表に、これらの機能のリリースの履歴を示します。

表 *17* : *SSH* および *Telnet* の機能の履歴

機能名	リリース	機能情報
SSH および Telnet	7.2(0)D1(1)	SSH ログインの最大試行回数の設定のサポートを追加しました。

機能名	リリース	機能情報
SSH および Telnet	6.0(1)	Release 5.2 以降、変更はありません。
SSH および Telnet	5.2(1)	Release 5.1 以降、変更はありません。
SCP および SFTP サーバ	5.1(1)	リモート デバイスとの間でのファイルのコピーをサポートするために、Cisco NX-OS デバイスで SCP サーバおよび SFTP サーバを設定する機能が追加されました。
SSH	5.1(1)	SSH は FIPS モードで実行されます。
SSH	5.1(1)	最小の RSA キー サイズが 768 ビットから 1024 ビットに変更されました。
SSH	5.0(2)	SSH ログインの最大試行回数の設定のサポートを追加しました。
SSH	5.0(2)	リモート デバイスに接続するために、Cisco NX-OS デバイスのブート モードから SSH セッションを開始する機能が追加されました。
SSH	5.0(2)	パスワードなしで Cisco NX-OS デバイスから SCP または SFTP サーバにファイルをコピーする機能が追加されました。
PKI	5.0(2)	リモートの cert-store のサポートを追加しました。

第 9 章

PKI の設定

この章では、Cisco NX-OS での公開キー インフラストラクチャ（PKI）のサポートについて説明します。PKI を使用すると、ネットワーク上で通信を安全に行うためのデジタル証明書をデバイスが入手して使用できるようになり、セキュア シェル（SSH）の管理性と拡張性も向上します。

この章は、次の項で構成されています。

- 機能情報の確認，225 ページ
- PKI の概要，226 ページ
- PKI のライセンス要件，230 ページ
- PKI の注意事項と制約事項，231 ページ
- PKI のデフォルト設定，231 ページ
- CA の設定とデジタル証明書，232 ページ
- PKI の設定の確認，255 ページ
- PKI の設定例，255 ページ
- PKI に関する追加情報，280 ページ
- PKI の機能の履歴，281 ページ

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

PKI の概要

ここでは、PKI について説明します。

CA とデジタル証明書

証明機関（CA）は証明書要求を管理して、ホスト、ネットワーク デバイス、ユーザなどの参加エンティティに証明書を発行します。CA は参加エンティティに対して集中型のキー管理を行います。

デジタル署名は、公開キー暗号法に基づいて、デバイスや個々のユーザをデジタル的に認証します。RSA 暗号化システムなどの公開キー暗号法では、各デバイスやユーザはキーペアを持ち、これには秘密キーと公開キーが含まれています。秘密キーは秘密裡に保管し、これを知っているのは所有するデバイスまたはユーザだけです。一方、公開キーは誰もが知っているものです。これらのキーの一方で暗号化されたものは、他方のキーで復号化できます。署名は、送信者の秘密キーを使用してデータを暗号化したときに作成されます。受信側は、送信側の公開キーを使用してメッセージを復号化することで、シグニチャを検証します。このプロセスは、受信者が送信者の公開キーのコピーを持っていて、これが本当に送信者のものであり、送信者を騙る他人のものではないことを高い確実性を持って知っていることを基盤としています。

デジタル証明書は、デジタル署名と送信者を結び付けるものです。デジタル証明書には、名前、シリアル番号、企業、部署または IP アドレスなど、ユーザまたはデバイスを特定する情報を含んでいます。また、エンティティの公開キーのコピーも含んでいます。証明書に署名する CA は、受信者が明示的に信頼する第三者機関であり、アイデンティティの正当性を立証し、デジタル証明書を作成します。

CA のシグニチャを検証するには、受信者は、CA の公開キーを認識している必要があります。一般的にはこのプロセスはアウトオブバンドか、インストール時に行われる操作によって処理されます。たとえば、通常の Web ブラウザでは、デフォルトで、複数の CA の公開キーが設定されています。

信頼モデル、トラストポイント、アイデンティティ CA

PKI の信頼モデルは、設定変更が可能な複数の信頼できる CA によって階層化されています。信頼できる CA のリストを使用して各参加デバイスを設定して、セキュリティ プロトコルの交換の際に入手したピアの証明書がローカルに信頼できる CA のいずれかで発行されていた場合には、これを認証できるようにすることができます。Cisco NX-OS ソフトウェアでは、信頼できる CA の自己署名ルート証明書（または下位 CA の証明書チェーン）をローカルに保存しています。信頼できる CA のルート証明書（または下位 CA の場合には全体のチェーン）を安全に入手するプロセスを、*CA* 認証と呼びます。

信頼できる CA について設定された情報をトラストポイントと呼び、CA 自体もトラストポイント *CA* と呼びます。この情報は、CA 証明書（下位 CA の場合は証明書チェーン）と証明書取消確認情報で構成されています。

Cisco NX-OS デバイスは、トラストポイントに登録して、アイデンティティ証明書を入手し、キーペアと関連付けることができます。このトラストポイントをアイデンティティ *CA* と呼びます。

RSA のキー ペアとアイデンティティ証明書

アイデンティティ証明書を入手するには、1 つまたは複数の RSA キーペアを作成し、各 RSA キーペアと Cisco NX-OS デバイスが登録しようとしているトラストポイント CA を関連付けます。Cisco NX-OS デバイスは、CA ごとにアイデンティティを 1 つだけ必要とします。これは CA ごとに 1 つのキー ペアと 1 つのアイデンティティ証明書で構成されています。

Cisco NX-OS ソフトウェアでは、設定変更が可能なキーのサイズ（またはモジュラス）で RSA キーペアを作成できます。デフォルトのキーのサイズは 512 です。また、RSA キー ペアのラベルも設定できます。デフォルトのキー ラベルは、デバイスの完全修飾ドメイン名（FQDN）です。

トラストポイント、RSA キーペア、およびアイデンティティ証明書の関係を要約したものを次に示します。

- トラストポイントとは、Cisco NX-OS デバイスが、あらゆるアプリケーション（SSH など）のピア証明書用に信頼する特定の CA です。
- Cisco NX-OS デバイスは多数のトラストポイントを持つことができ、デバイス上のすべてのアプリケーションがあらゆるトラストポイント CA で発行されたピア証明書を信頼できます。
- トラストポイントは特定のアプリケーション用に限定されません。
- Cisco NX-OS デバイスは、トラストポイントに対応する CA に登録して、アイデンティティ証明書を入手します。デバイスは複数のトラストポイントに登録できます。これは、各トラストポイントから異なるアイデンティティ証明書を入手できることを意味します。アイデンティティ証明書は、発行する CA によって証明書に指定されている目的に応じてアプリケーションで使用します。証明書の目的は、証明書の拡張機能として証明書に保存されます。
- トラストポイントに登録するときには、証明を受ける RSA キー ペアを指定する必要があります。このキーペアは、登録要求を作成する前に作成されていて、トラストポイントに関連付けられている必要があります。トラストポイント、キーペア、およびアイデンティティ証明書との間のアソシエーション（関連付け）は、証明書、キーペア、またはトラストポイントが削除されて明示的になくなるまで有効です。
- アイデンティティ証明書のサブジェクト名は、Cisco NX-OS デバイスの完全修飾ドメイン名です。
- デバイス上には 1 つまたは複数の RSA キー ペアを作成でき、それぞれを 1 つまたは複数のトラストポイントに関連付けることができます。しかし、1 つのトラストポイントに関連付けられるキー ペアは 1 だけです。これは 1 つの CA からは 1 つのアイデンティティ証明書しか入手できないことを意味します。
- Cisco NX-OS デバイスが複数のアイデンティティ証明書を（それぞれ別の CA から）入手する場合は、アプリケーションがピアとのセキュリティ プロトコルの交換で使用する証明書は、アプリケーション固有のものになります。

- 1つのアプリケーションに1つまたは複数のトラストポイントを指定する必要はありません。証明書の目的がアプリケーションの要件を満たしていれば、どのアプリケーションもあらゆるトラストポイントで発行されたあらゆる証明書を使用できます。
- あるトラストポイントから複数のアイデンティティ証明書を入手したり、あるトラストポイントに複数のキー ペアを関連付ける必要はありません。ある CA はあるアイデンティティ（または名前）を 1 回だけ証明し、同じ名前で複数の証明書を発行することはありません。ある CA から複数のアイデンティティ証明書を入手する必要があり、またその CA が同じ名前で複数の証明書の発行を許可している場合は、同じ CA 用の別のトラストポイントを定義して、別のキー ペアを関連付け、証明を受ける必要があります。

複数の信頼できる CA のサポート

Cisco NX-OS デバイスは、複数のトラストポイントを設定して、それぞれを別の CA に関連付けることにより、複数の CA を信頼できるようになります。信頼できる CA が複数あると、ピアに証明書を発行した特定の CA にデバイスを登録する必要がなくなります。代わりに、ピアが信頼する複数の信頼できる CA をデバイスに設定できます。すると、Cisco NX-OS デバイスは設定されている信頼できる CA を使用して、ピアから受信した証明書で、ピア デバイスの ID で定義されている CA から発行されたものではないものを検証できるようになります。

PKI の登録のサポート

登録とは、SSH などのアプリケーションに使用するデバイス用のアイデンティティ証明書を入手するプロセスです。これは、証明書を要求するデバイスと、認証局の間で生じます。

Cisco NX-OS デバイスでは、PKI 登録プロセスを実行する際に、次の手順を取ります。

- デバイスで RSA の秘密キーと公開キーのペアを作成します。
- 標準の形式で証明書要求を作成し、CA に送ります。

（注） 要求が CA で受信されたとき、CA サーバでは CA アドミニストレータが登録要求を手動で承認しなくてはならない場合があります。

- 発行された証明書を CA から受け取ります。これは CA の秘密キーで署名されています。
- デバイスの不揮発性のストレージ領域（ブートフラッシュ）に証明書を書き込みます。

カットアンドペーストによる手動での登録

Cisco NX-OS ソフトウェアでは、手動でのカットアンドペーストによる証明書の取得と登録をサポートしています。カットアンドペーストによる登録とは、証明書要求をカットアンドペーストして、デバイスと CA 間で認証を行うことを意味します。

手動による登録プロセスでカットアンドペーストを使用するには、次の手順を実行する必要があります。

- 証明書登録要求を作成します。これはCisco NX-OSデバイスでbase64でエンコードされたテキスト形式として表示されます。
- エンコードされた証明書要求のテキストをEメールまたはWebフォームにカットアンドペーストし、CA に送ります。
- 発行された証明書（base64 でエンコードされたテキスト形式）を CA から E メールまたは Web ブラウザによるダウンロードで受け取ります。
- 証明書のインポート機能を使用して、発行された証明書をデバイスにカットアンドペーストします。

複数の RSA キー ペアとアイデンティティ CA のサポート

複数のアイデンティティ CA を使用すると、デバイスが複数のトラストポイントに登録できるようになり、その結果、別々の CA から複数のアイデンティティ証明書が発行されます。この機能によって、Cisco NX-OS デバイスは複数のピアを持つ SSH およびアプリケーションに、これらのピアに対応する CA から発行された証明書を使用して参加できるようになります。

また複数の RSA キー ペアの機能を使用すると、登録している各 CA ごとの別々のキー ペアをデバイスで持てるようになります。これは、他の CA で指定されているキーの長さなどの要件と競合することなく、各 CA のポリシー要件に適合させることができます。デバイスでは複数の RSA キーペアを作成して、各キーペアを別々のトラストポイントに関連付けることができます。したがって、トラストポイントに登録するときには、関連付けられたキー ペアを証明書要求の作成に使用します。

ピア証明書の検証

PKI では、Cisco NX-OS デバイスでのピア証明書の検証機能をサポートしています。Cisco NX-OS ソフトウェアでは、SSH などのアプリケーションのためのセキュリティ交換の際にピアから受け取った証明書を検証します。アプリケーションはピア証明書の正当性を検証します。Cisco NX-OS ソフトウェアでは、ピア証明書の検証の際に次の手順を実行します。

- ピア証明書がローカルの信頼できる CA のいずれかから発行されていることを確認します。
- ピア証明書が現在時刻において有効であること（期限切れでない）ことを確認します。
- ピア証明書が、発行した CA によって取り消されていないことを確認します。

取消確認については、Cisco NX-OS ソフトウェアでは証明書失効リスト（CRL）をサポートしています。トラストポイント CA ではこの方法を使用して、ピア証明書が取り消されていないことを確認できます。

証明書の取消確認

Cisco NX-OS ソフトウェアでは、CA 証明書の取消のステータスを確認できます。アプリケーションでは、指定した順序に従って取消確認メカニズムを使用できます。選択肢には、CRL、none、これらの方式の組み合わせがあります。

CRL のサポート

CA では証明書失効リスト（CRL）を管理して、有効期限前に取り消された証明書についての情報を提供します。CA では CRL をリポジトリで公開して、発行したすべての証明書の中にダウンロード用の公開 URL 情報を記載しています。ピア証明書を検証するクライアントは、発行した CA から最新の CRL を入手して、これを使用して証明書が取り消されていないかどうかを確認できます。クライアントは、自身の信頼できる CA のすべてまたは一部の CRL をローカルにキャッシュして、その CRL が期限切れになるまで必要に応じて使用することができます。

Cisco NX-OS ソフトウェアでは、先にダウンロードしたトラストポイントについての CRL を手動で設定して、これをデバイスのブートフラッシュ（cert-store）にキャッシュすることができます。ピア証明書の検証の際、Cisco NX-OS ソフトウェアは、CRL がすでにローカルにキャッシュされていて、取消確認でこの CRL を使用するよう設定されている場合にだけ、発行した CA からの CRL をチェックします。それ以外の場合、Cisco NX-OS ソフトウェアでは CRL チェックを実行せず、他の取消確認方式が設定されている場合を除き、証明書は取り消されていないと見なします。

証明書と対応するキー ペアのインポートとエクスポート

CA 認証と登録のプロセスの一環として、下位 CA 証明書（または証明書チェーン）とアイデンティティ証明書を標準の PEM（base64）形式でインポートできます。

トラストポイントでのアイデンティティ情報全体を、パスワードで保護される PKCS#12 標準形式でファイルにエクスポートできます。このファイルは、後で同じデバイス（システム クラッシュの後など）や交換したデバイスににインポートすることができます。PKCS#12 ファイル内の情報は、RSA キー ペア、アイデンティティ証明書、および CA 証明書（またはチェーン）で構成されています。

PKI のバーチャライゼーション サポート

PKI 機能の設定と操作は、仮想デバイス コンテキスト（VDC）に対してローカルです。VDC の詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

PKI のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	PKI 機能にはライセンスは必要ありません。ライセンスパッケージに含まれていない機能はすべて Cisco NX-OS システムイメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

PKI の注意事項と制約事項

PKI に関する注意事項と制約事項は次のとおりです。

- Cisco NX-OS デバイスに設定できるキー ペアの最大数は 16 です。
- Cisco NX-OS デバイスで宣言できるトラストポイントの最大数は 16 です。
- Cisco NX-OS デバイスに設定できるアイデンティティ証明書の最大数は 16 です。
- CA 証明書チェーン内の証明書の最大数は 10 です。
- ある CA に対して認証できるトラストポイントの最大数は 10 です。
- 設定のロールバックでは PKI の設定はサポートしていません。
- Cisco NX-OS ソフトウェアでは、OSCP をサポートしていません。

（注） Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

PKI のデフォルト設定

次の表に、PKI パラメータのデフォルト設定を示します。

表 *18* : *PKI* パラメータのデフォルト値

パラメータ	デフォルト
トラスト ポイント	なし
RSA キー ペア	なし

パラメータ	デフォルト
RSA キー ペアのラベル	デバイスの FQDN
RSA キー ペアのモジュール	512
RSA キー ペアのエクスポートの可否	イネーブル
取消確認方式	CRL
証明書認証の cert-store	local

CA の設定とデジタル証明書

ここでは、Cisco NX-OS デバイス上で CA とデジタル証明書が相互に連携して動作するようにするために、実行が必要な作業について説明します。

ホスト名と IP ドメイン名の設定

デバイスのホスト名または IP ドメイン名をまだ設定していない場合は、設定する必要があります。これは、Cisco NX-OS ソフトウェアでは、アイデンティティ証明書のサブジェクトとして完全修飾ドメイン名（FQDN）を使用するためです。また、Cisco NX-OS ソフトウェアでは、キーの作成の際にラベルが指定されていないと、デバイスの FQDN をデフォルトのキー ラベルとして使用します。たとえば、DeviceA.example.com という名前の証明書は、DeviceA というデバイスのホスト名と example.com というデバイスの IP ドメイン名に基づいています。

注意 証明書を作成した後にホスト名または IP ドメイン名を変更すると、証明書が無効になります。

手順の概要

1. **configure terminal**
2. **hostname***hostname*
3. **ip domain-name***name* [**use-vrf***vrf-name*]
4. **exit**
5. （任意） **show hosts**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**hostname***hostname* 例： `switch(config)# hostname DeviceA`	デバイスのホスト名を設定します。
ステップ 3	**ip domain-name***name* [**use-vrf***vrf-name*] 例： `DeviceA(config)# ip domain-name example.com`	デバイスの IP ドメイン名を設定します。VRF 名が指定されていないと、このコマンドではデフォルトの VRF を使用します。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 5	**show hosts** 例： `switch# show hosts`	（任意） IP ドメイン名を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

RSA キー ペアの生成

RSA キー ペアは、アプリケーション向けのセキュリティ プロトコルの交換時に、セキュリティ ペイロードの署名、暗号化、および復号化のために作成します。デバイスのための証明書を取得する前に、RSA キー ペアを作成する必要があります。

手順の概要

1. **configure terminal**
2. **crypto key generate rsa** [**label***label-string*] [**exportable**] [**modulus***size*]
3. **exit**
4. （任意） **show crypto key mypubkey rsa**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**crypto key generate rsa** [**label***label-string*] [**exportable**] [**modulus***size*] 例： `switch(config)# crypto key generate rsa exportable`	RSA キーペアを生成します。デバイスに設定できるキーペアの最大数は 16 です。 ラベル文字列には、大文字と小文字を区別して、最大 64 文字の英数字で値を指定します。デフォルトのラベル文字列は、ピリオド文字（.）で区切ったホスト名と FQDN です。 有効なモジュラスの値は 512、768、1024、1536、および 2048 です。デフォルトのモジュラスのサイズは 512 です。 （注） 適切なキーのモジュラスを決定する際には、Cisco NX-OS デバイスと CA（登録を計画している対象）のセキュリティ ポリシーを考慮する必要があります。 デフォルトでは、キー ペアはエクスポートできません。エクスポート可能なキー ペアだけ、PKCS#12 形式でエクスポートできます。 **注意** キー ペアのエクスポートの可否は変更できません。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show crypto key mypubkey rsa** 例： `switch# show crypto key mypubkey rsa`	（任意） 作成したキーを表示します。

	コマンドまたはアクション	目的
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

トラストポイント CA のアソシエーションの作成

Cisco NX-OS デバイスとトラストポイント CA を関連付ける必要があります。

はじめる前に

RSA キー ペアを作成します。

手順の概要

1. **configure terminal**
2. **crypto ca trustpoint***name*
3. **enrollment terminal**
4. **rsakeypair***label*
5. **exit**
6. （任意） **show crypto ca trustpoints**
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**crypto ca trustpoint***name*
	
	例：
	`switch(config)# crypto ca trustpoint admin-ca`
	`switch(config-trustpoint)#`
		デバイスが信頼するトラストポイント CA を宣言し、トラストポイント コンフィギュレーション モードを開始します。
		（注） デバイスに設定できるトラストポイントの最大数は 16 です。

	コマンドまたはアクション	目的
ステップ 3	**enrollment terminal** 例： `switch(config-trustpoint)# enrollment terminal`	手動でのカットアンドペーストによる証明書の登録をイネーブルにします。デフォルトではイネーブルになっています。 （注） Cisco NX-OS ソフトウェアでは、手動でのカットアンドペースト方式による証明書の登録だけをサポートしています。
ステップ 4	**rsakeypair***label* 例： `switch(config-trustpoint)# rsakeypair SwitchA`	RSA キー ペアのラベルを指定して、このトラストポイントを登録用に関連付けます。 （注） CA ごとに 1 つの RSA キー ペアだけを指定できます。

ステップ 5	**exit**
	
	例：
	`switch(config-trustpoint)# exit`
	`switch(config)#`
		トラストポイント コンフィギュレーション モードを終了します。

ステップ 6	**show crypto ca trustpoints** 例： `switch(config)# show crypto ca trustpoints`	（任意） トラストポイントの情報を表示します。
ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

RSA キー ペアの生成，（233 ページ）

証明書認証の cert-store の設定

証明書認証の cert-store を指定することができます。デフォルトでは、アプリケーション証明書は、ローカルの cert-store（Cisco NX-OS デバイス）に保管された CA 証明書を使用して認証されます。CA 証明書を別の場所に保管する必要があるアプリケーションの場合は、Lightweight Directory Access Protocol（LDAP）サーバをリモートの cert-store として設定できます。

はじめる前に

リモートの cert-store を設定する場合は、リモート デバイスで LDAP サーバを設定し、認証に使用される CA 証明書が Active Directory にロードされていることを確認します。

手順の概要

1. **configure terminal**
2. **crypto ca lookup** {**local** | **remote** | **both**}
3. （任意） **show crypto ca certstore**
4. （任意） **crypto ca remote ldap server-group** *group-name*
5. （任意） **crypto ca remote ldap crl-refresh-time** *hours*
6. （任意） **show crypto ca remote-certstore**
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**crypto ca lookup** {**local**	**remote**	**both**} 例： `switch(config)# crypto ca lookup remote`	ローカルまたはリモートの cert-store に保管された CA 証明書を使用して、アプリケーション証明書を認証します。デフォルトは local です。both を選択すると、アプリケーション証明書はローカルの cert-store を使用して認証されますが、認証に失敗した場合やCA証明書が見つからなかった場合に、リモートの cert-store が使用されます。 （注） **crypto ca lookup** コマンドはアドオン方式のコマンドではありません。コマンドを実行するたびに既存のコマンドが上書きされます。
ステップ 3	**show crypto ca certstore** 例： `switch(config)# show crypto ca certstore`	（任意） cert-store の設定を表示します。
ステップ 4	**crypto ca remote ldap server-group** *group-name* 例： `switch(config)# crypto ca remote ldap server-group group1`	（任意） リモートの cert-store を設定した場合に、LDAP との通信に使用する LDAP サーバ グループを設定します。サーバ グループ名を最大 64 文字の英数字で入力できます。
ステップ 5	**crypto ca remote ldap crl-refresh-time** *hours* 例： `switch(config)# crypto ca remote ldap crl-refresh-time 10`	（任意） リモートの cert-store と LDAP サーバ グループを設定した場合に、リモートの cert-store の情報で証明書失効リスト（CRL）を更新するリフレッシュ タイムを設定します。CRL は、取り消されて無効になっているCA証明書のリストです。リフレッ

	コマンドまたはアクション	目的
		シュ タイムは、0 ～ 744 時間の範囲で指定します。0 を入力すると、リフレッシュ ルーチンが 1 回実行されます。
ステップ 6	**show crypto ca remote-certstore** 例： `switch(config)# show crypto ca remote-certstore`	（任意） リモートの cert-store の設定を表示します。
ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

証明書マッピングのフィルタの設定, （238 ページ）

証明書マッピングのフィルタの設定

認証に使用される CA 証明書を検証するためのマッピングのフィルタを設定できます。マッピングのフィルタは、CA 証明書をユーザ名と照合するために使用されます。

Cisco NX-OS は次の証明書マッピングのフィルタをサポートします。

- %username%：ユーザのログイン名が代入されます。
- %username-without-domain%：ドメインを除くユーザのログイン名が代入されます（Windows のみ）。
- %hostname%：ピアのホスト名が代入されます。
- *：ワイルド文字に対応します。

はじめる前に

証明書認証の cert-store を設定します。

手順の概要

1. **configure terminal**
2. **crypto certificatemap mapname** *map-name*
3. **filter** [**subject-name** *subject-name* | **altname-email** *e-mail-ID* | **altname-upn** *user-principal-name*]
4. **exit**
5. （任意） **crypto cert ssh-authorize** [**default** | *issuer-CAname*] [**map** *map-name1* [*map-name2*]]
6. （任意） **show crypto certificatemap**
7. （任意） **show crypto ssh-auth-map**
8. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**crypto certificatemap mapname** *map-name* 例： `switch(config)# crypto certificatemap mapname filtermap1`	新しいフィルタ マップを作成します。

ステップ 3	**filter** [**subject-name** *subject-name*	**altname-email** *e-mail-ID*	**altname-upn** *user-principal-name*]
			
			例：
			`switch(config-certmap-filter)# filter altname-email jsmith@acme.com`
				フィルタ マップ内で証明書マッピングのフィルタを 1 つまたは複数設定します。フィルタでは、次の証明書フィールド属性がサポートされます。
				• subject-name：必要なサブジェクト名です。LDAP の認定者名（DN）文字列の形式で指定します。次に例を示します。
				`filter subject-name cn=%username%,ou=PKI,o=Acme,c=US`
				• altname-email：サブジェクト名の代わりに証明書に含まれている必要がある E メール アドレスです。次に例を示します。
				`filter altname-email %username%@*`
				• altname-upn：サブジェクト名の代わりに証明書に含まれている必要があるプリンシパル名です。次に例を示します。
				`filter altname-upn %username-without-domain%@%hostname%`
				
				証明書は、マップで設定されたすべてのフィルタを通過した場合に検証にパスします。

	コマンドまたはアクション	目的

ステップ 4	**exit**
	
	例：
	`switch(config-certmap-filter)# exit`
	`switch(config)#`
		証明書マッピングのフィルタ コンフィギュレーション モードを終了します。

ステップ 5	**crypto cert ssh-authorize** [**default** | *issuer-CAname*] [**map** *map-name1* [*map-name2*]] 例： `switch(config)# crypto cert ssh-authorize default map filtermap1`	（任意） セキュア シェル（SSH）プロトコル用の証明書マッピングのフィルタを設定します。SSH 認証用のデフォルトのフィルタ マップを使用するか、CA 証明書の発行元を指定できます。デフォルトのマップを使用しない場合は、認証用のフィルタ マップを 1 つまたは 2 つ指定できます。 CA 証明書の発行元を指定した場合、ユーザ アカウントにバインドされた証明書が検証され、設定されたマップのいずれかを通過すると検証にパスします。
ステップ 6	**show crypto certificatemap** 例： `switch(config)# show crypto certificatemap`	（任意） 証明書マッピングのフィルタを表示します。
ステップ 7	**show crypto ssh-auth-map** 例： `switch(config)# show crypto ssh-auth-map`	（任意） SSH認証用に設定されたマッピングのフィルタを表示します。
ステップ 8	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

証明書認証の cert-store の設定, （236 ページ）

CA の認証

CA が Cisco NX-OS デバイスに対して認証されると、CA を信頼するプロセスの設定が完了します。まず、PEM 形式の CA の自己署名証明書を入手し、Cisco NX-OS デバイスを CA に対して認証する必要があります。この証明書には、CA の公開キーが含まれています。この CA の証明書は自己署名（CA が自身の証明書に署名したもの）であるため、CA の公開キーは、CA アドミニストレータに連絡し、CA 証明書のフィンガープリントを比較して手動で認証する必要があります。

（注） 認証する CA が他の CA の下位 CA である場合、認証する CA は自己署名 CA ではありません。その上位の CA がさらに別の CA の下位である場合もあります。最終的には自己署名 CA に到達します。このタイプの CA 証明書を、認証する CA の *CA* 証明書チェーンと呼びます。この場合は、CA 認証の際に、証明書チェーン内のすべての CA の CA 証明書の完全なリストを入力する必要があります。CA 証明書チェーン内の証明書の最大数は 10 です。

はじめる前に

CA とのアソシエーションを作成します。

CA 証明書または CA 証明書チェーンを入手します。

手順の概要

1. **configure terminal**
2. **crypto ca authenticate***name*
3. **exit**
4. （任意） **show crypto ca trustpoints**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**crypto ca authenticate***name*
	
	例：
	`switch(config)# crypto ca authenticate admin-ca`
	`input (cut & paste) CA certificate (chain) in PEM format;`
	`end the input with a line containing only END OF INPUT :`
	`-----BEGIN CERTIFICATE-----`
	`MIIC4jCCAoygAwIBAgIQBWDSiay0GZRPSRIljK0ZejANBgkqhkiG9w0BAQUFADCB`
	`kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklO`
	`MRIwEAYDVQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UE`
		CA の証明書をカットアンドペーストするようプロンプトが表示されます。CA を宣言したときに使用した名前と同じ名前を使用します。
		
		ある CA に対して認証できるトラストポイントの最大数は 10 です。
		
		（注） 下位 CA の認証の場合、Cisco NX-OS ソフトウェアでは、自己署名 CA に到達する CA 証明書の完全なチェーンが必要になります。これは証明書の検証や PKCS#12 形式でのエクスポートに CA チェーンが必要になるためです。

	コマンドまたはアクション	目的
	ChMFQ2lzY28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBD QTAeFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN AQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UEBhMCSU4xEjAQBgNVBAgTCUth cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVDaXNjbzETMBEG A1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHzluNccNM87ypyzwuoSNZXOMpeRXXI OzyBAgiXT2ASFuUOwQ1iDM8rO/41jf8RxvYKvysCAwEAAaOBvzCBvDALBgNVHQ8E BAMCAcYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyjyRoMbrCNMRU2OyRhQ GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs L0FwYXJuYSUyMENBLmNybDAwoC6gLIYqZmlsZTovL1xcc3NlLTA4XENlcnRFbnJv bGxcQXBhcm5hJTIwQ0EuY3JsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEB BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaqNgLh0AFcT0rEyuyt/WYGPzksF9Ea NBG7E0oN66zex0EOEfG1Vs6mXp1//w== -----END CERTIFICATE----- END OF INPUT Fingerprint(s): MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12 Do you accept this certificate? [yes/no]: yes	
ステップ 3	**exit** 例： switch(config)# exit switch#	設定モードを終了します。
ステップ 4	**show crypto ca trustpoints** 例： switch# show crypto ca trustpoints	（任意） トラストポイント CA の情報を表示します。
ステップ 5	**copy running-config startup-config** 例： switch# copy running-config startup-config	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

トラストポイント CA のアソシエーションの作成，（235 ページ）

証明書取消確認方法の設定

クライアント（SSH ユーザなど）とのセキュリティ交換の際に、Cisco NX-OS デバイスは、クライアントから送られたピア証明書の検証を実行します。検証プロセスには、証明書の取消状況の確認が含まれます。

CA からダウンロードした CRL を確認するよう、デバイスに設定できます。CRL のダウンロードとローカルでの確認では、ネットワーク上にトラフィックは発生しません。しかし、証明書がダウンロードとダウンロードの中間で取り消され、デバイス側ではその取り消しに気付かない場合も考えられます。

はじめる前に

CA を認証します。

CRL チェックを使用する場合は、CRL が設定済みであることを確認します。

手順の概要

1. **configure terminal**
2. **crypto ca trustpoint***name*
3. **revocation-check** {**crl** [**none**] | **none**}
4. **exit**
5. （任意） **show crypto ca trustpoints**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**crypto ca trustpoint***name*
	
	例：
	`switch(config)# crypto ca trustpoint admin-ca`
	`switch(config-trustpoint)#`
		トラストポイント CA を指定し、トラストポイント コンフィギュレーション モードを開始します。

ステップ 3	**revocation-check** {**crl** [**none**]	**none**} 例： `switch(config-trustpoint)# revocation-check none`	証明書取消確認方法を設定します。デフォルト方式は **crl** です。 Cisco NX-OS ソフトウェアでは、指定した順序に従って証明書取消方式を使用します。

ステップ 4	**exit**
	
	例：
	`switch(config-trustpoint)# exit`
	`switch(config)#`
		トラストポイント コンフィギュレーション モードを終了します。

ステップ 5	**show crypto ca trustpoints** 例： `switch(config)# show crypto ca trustpoints`	（任意） トラストポイント CA の情報を表示します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

CA の認証，（240 ページ）
CRL の設定，（251 ページ）

証明書要求の作成

使用する各デバイスの RSA キー ペア用に、対応するトラストポイント CA からアイデンティティ証明書を入手するために、要求を作成する必要があります。その後、表示された要求を CA 宛の E メールまたは Web サイトのフォームにカットアンドペーストします。

はじめる前に

CA とのアソシエーションを作成します。

CA 証明書または CA 証明書チェーンを入手します。

手順の概要

1. **configure terminal**
2. **crypto ca enroll** *name*
3. **exit**
4. （任意） **show crypto ca certificates**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 2	**crypto ca enroll** *name*
	
	例：
	`switch(config)# crypto ca enroll admin-ca`
	`Create the certificate request ..`
	` Create a challenge password. You will need to verbally provide this`
	`  password to the CA Administrator in order to revoke your certificate.`
	`  For security reasons your password will not be saved in the configuration.`
	`  Please make a note of it.`
	`  Password:nbv123`
	` The subject name in the certificate will be: DeviceA.cisco.com`
	` Include the switch serial number in the subject name? [yes/no]: no`
	` Include an IP address in the subject name [yes/no]: yes`
	`ip address:172.22.31.162`
	` The certificate request will be displayed...`
	`-----BEGIN CERTIFICATE REQUEST-----`
	`MIIBqzCCARQCAQAwHDEaMBgGA1UEAxMRVmVnYXMtMS5jaXNjby5jb20wgZ8wDQYJ`
	`KoZIhvcNAQEBBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8rl4lKY`
	`0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y`
	`P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVkSCzXv8S`
	`VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCSqGSIb3DQEJ`
	`DjEpMCcwJQYDVR0RAQH/BBswGYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwDQYJ`
	`KoZIhvcNAQEEBQADgYEAkT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99GlFWgt`
	`PftrNcWUE/pw6HayfQl2T3ecgNwel2d15133YBF2bktExiI6Ul88nTOjglXMjja8`
	`8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0=`
	`-----END CERTIFICATE REQUEST-----`
		認証した CA に対する証明書要求を作成します。
		
		（注） チャレンジ パスワードを記憶しておいてください。このパスワードは設定と一緒に保存されません。証明書を取り消す必要がある場合には、このパスワードを入力する必要があります。

ステップ 3	**exit**
	
	例：
	`switch(config-trustpoint)# exit`
	`switch(config)#`
		トラストポイント コンフィギュレーション モードを終了します。

ステップ 4	**show crypto ca certificates** 例： `switch(config)# show crypto ca certificates`	（任意） CA 証明書を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

トラストポイント CA のアソシエーションの作成, （235 ページ）

アイデンティティ証明書のインストール

アイデンティティ証明書は、CA から E メールまたは Web ブラウザ経由で base64 でエンコードされたテキスト形式で受信できます。CAから入手したアイデンティティ証明書を、エンコードされたテキストをカットアンドペーストしてインストールする必要があります。

はじめる前に

CA とのアソシエーションを作成します。

CA 証明書または CA 証明書チェーンを入手します。

手順の概要

1. **configure terminal**
2. **crypto ca import***name***certificate**
3. **exit**
4. （任意） **show crypto ca certificates**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**crypto ca import***name***certificate**
	
	例：
	`switch(config)# crypto ca import admin-ca certificate`
	`input (cut & paste) certificate in PEM format:`
	`-----BEGIN CERTIFICATE-----`
	`MIIEADCCA6qgAwIBAgIKCjOOoQAAAAAAdDANBgkqhkiG9w0BAQUFADCBkDEgMB4G`
	`CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklOMRIwEAYD`
	`VQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ2lz`
	`Y28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBDQTAeFw0w`
	`NTExMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBwxGjAYBgNVBAMTEVZlZ2FzLTEu`
	`Y2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C`
	`dQ1WkjKjSICdpLfK5eJSmNCQujGpzcuKsZPFXjF2UoiyeCYE8ylncWyw5E08rJ47`
	`glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMCnIM4W1aY/q2q4Gb`
	`x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDVR0RAQH/BBsw`
	`GYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwHQYDVR0OBBYEFKCLi+2sspWEfgrR`
	`bhWmlVyo9jngMIHMBgNVHSMEgcQwgcGAFCco8kaDG6wjTEVNjskYUBoLFmxxoYGW`
	`pIGTMIGQMSAwHgYJKoZIhvcNAQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UE`
	`BhMCSU4xEjAQBgNVBAgTCUthcm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4w`
	`DAYDVQQKEwVDaXNjbzETMBEGA1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBh`
	`cm5hIENBghAFYNKJrLQZlE9JEiWMrRl6MGsGA1UdHwRkMGIwLqAsoCqGKGh0dHA6`
	`Ly9zc2UtMDgvQ2VydEVucm9sbC9BcGFybmElMjBDQS5jcmwwMKAuoCyGKmZpbGU6`
	`Ly9cXHNzZS0wOFxDZXJ0RW5yb2xsXEFwYXJuYSUyMENBLmNybDCBigYIKwYBBQUH`
	`AQEEfjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3NlLTA4L0NlcnRfbnJvbGwvc3Nl`
	`LTA4X0FwYXJuYSUyMENBLmNydDA9BggrBgEFBQcwAoYxZmlsZTovL1xcc3NlLTA4`
		admin-ca という名前の CA に対するアイデンティティ証明書をカットアンドペーストするよう、プロンプトが表示されます。
		
		デバイスに設定できるアイデンティティ証明書の最大数は 16 です。

	コマンドまたはアクション	目的
	XENlcnRFbnJvbGxcc3NlLTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF AANBADbGBGsbe7GNLh9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyejtsyflw E36cIZu4WsExREqxbTk8ycx7V5o= -----END CERTIFICATE-----	
ステップ 3	**exit** 例： switch(config)# exit switch#	設定モードを終了します。
ステップ 4	**show crypto ca certificates** 例： switch# show crypto ca certificates	（任意） CA 証明書を表示します。
ステップ 5	**copy running-config startup-config** 例： switch# copy running-config startup-config	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

トラストポイント CA のアソシエーションの作成, （235 ページ）

トラストポイントの設定がリブート後も維持されていることの確認

トラストポイントの設定が、Cisco NX-OS デバイスのリブート後も維持されていることを確認できます。

トラストポイントの設定は、通常の Cisco NX-OS デバイスの設定であり、スタートアップ コンフィギュレーションに確実にコピーした場合にだけ、システムのリブート後も維持されます。トラスト ポイント設定をスタートアップ コンフィギュレーションにコピーしておけば、トラストポイントに関連する証明書、キー ペア、および CRL が自動的に保持されます。逆に、トラストポイントがスタートアップ コンフィギュレーションにコピーされていないと、証明書、キー ペア、および関連CRL は保持されません。リブート後に、対応するトラスト ポイント設定が必要になるからです。設定した証明書、キーペア、およびCRL を確実に保持するために、必ず、実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーしてください。また、証明書またはキー ペアを削除した後は実行コンフィギュレーションを保存して、削除が永続的に反映されるようにしてください。

トラストポイントに関連付けられた証明書と CRL は、そのトラストポイントがすでにスタートアップ コンフィギュレーションに保存されていれば、インポートした時点で（つまりスタートアップ コンフィギュレーションにコピーしなくても）維持されるようになります。

パスワードで保護したアイデンティティ証明書のバックアップを作成して、これを外部のサーバに保存することを推奨します。

（注） コンフィギュレーションを外部サーバにコピーすると、証明書およびキー ペアも保存されます。

関連トピック

PKCS 12 形式でのアイデンティティ情報のエクスポート，（248 ページ）

PKCS 12 形式でのアイデンティティ情報のエクスポート

アイデンティティ証明書を、トラストポイントの RSA キー ペアや CA 証明書（または下位 CA の場合はチェーン全体）と一緒に PKCS#12 ファイルにバックアップ目的でエクスポートすることができます。デバイスのシステム クラッシュからの復元の際や、スーパーバイザ モジュールの交換の際には、証明書や RSA キー ペアをインポートすることができます。

（注） エクスポートの URL を指定するときに使用できるのは、bootflash:*filename* という形式だけです。

はじめる前に

CA を認証します。

アイデンティティ証明書をインストールします。

手順の概要

1. **configure terminal**
2. **crypto ca export***name* **pkcs12 bootflash:***filenamepassword*
3. **exit**
4. **copy booflash:***filenamescheme***://***server/* [*url/*]*filename*

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**crypto ca export***name* **pkcs12 bootflash:***filenamepassword* 例： `switch(config)# crypto ca export admin-ca pkcs12 bootflash:adminid.p12 nbv123`	アイデンティティ証明書と、トラストポイント CA の対応するキーペアと CA 証明書をエクスポートします。パスワードには、大文字と小文字を区別して、最大 128 文字の英数字で値を指定します。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**copy bootflash:***filenamescheme***://***server/*[*url/*]*filename* 例： `switch# copy bootflash:adminid.p12 tftp:adminid.p12`	PKCS#12 形式のファイルをリモート サーバにコピーします。 *scheme* 引数として、**tftp:**、**ftp:**、**scp:**、または **sftp:** を指定できます。*server* 引数は、リモート サーバのアドレスまたは名前であり、*url* 引数はリモート サーバにあるソース ファイルへのパスです。 *server*、*url*、および *filename* の各引数は、大文字小文字を区別して入力します。

関連トピック

RSA キー ペアの生成, （233 ページ）
CA の認証, （240 ページ）
アイデンティティ証明書のインストール, （246 ページ）

PKCS 12 形式でのアイデンティティ情報のインポート

デバイスのシステム クラッシュからの復元の際や、スーパーバイザモジュールの交換の際には、証明書や RSA キー ペアをインポートすることができます。

（注） インポートの URL を指定するときに使用できるのは、bootflash:*filename* という形式だけです。

はじめる前に

CA 認証によってトラストポイントに関連付けられている RSA キー ペアがないこと、およびトラストポイントに関連付けられている CA がないことを確認して、トラストポイントが空であるようにします。

手順の概要

1. **copy***scheme***://***server***/**[*url*/]*filename***bootflash:***filename*
2. **configure terminal**
3. **crypto ca import***name***pksc12 bootflash:***filename*
4. **exit**
5. （任意） **show crypto ca certificates**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**copy***scheme***://***server***/**[*url*/]*filename***bootflash:***filename* 例： `switch# copy tftp:adminid.p12 bootflash:adminid.p12`	PKCS#12 形式のファイルをリモート サーバからコピーします。 *scheme* 引数として、**tftp:**、**ftp:**、**scp:**、または **sftp:** を指定できます。*server* 引数は、リモート サーバのアドレスまたは名前であり、*url* 引数はリモート サーバにあるソース ファイルへのパスです。 *server*、*url*、および *filename* の各引数は、大文字小文字を区別して入力します。
ステップ 2	**configure terminal** 例： `switch# configure terminal switch(config)#`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**crypto ca import***name***pksc12 bootflash:***filename* 例： `switch(config)# crypto ca import admin-ca pkcs12 bootflash:adminid.p12 nbv123`	アイデンティティ証明書と、トラストポイント CA の対応するキーペアと CA 証明書をインポートします。
ステップ 4	**exit** 例： `switch(config)# exit switch#`	設定モードを終了します。
ステップ 5	**show crypto ca certificates** 例： `switch# show crypto ca certificates`	（任意） CA 証明書を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

CRL の設定

トラストポイントからダウンロードした CRL を手動で設定することができます。Cisco NX-OS ソフトウェアでは、CRL をデバイスのブートフラッシュ（cert-store）にキャッシュします。ピア証明書の検証の際、Cisco NX-OS ソフトウェアが発行した CA からの CRL をチェックするのは、CRL をデバイスにダウンロードしていて、この CRL を使用する証明書取消確認を設定している場合だけです。

はじめる前に

証明書取消確認がイネーブルになっていることを確認します。

手順の概要

1. **copy***scheme*:[*//server/*[*url/*]]*filename***bootflash:***filename*
2. **configure terminal**
3. **crypto ca crl request***name***bootflash:***filename*
4. **exit**
5. （任意） **show crypto ca crl***name*
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**copy***scheme*:[*//server/*[*url/*]]*filename***bootflash:***filename* 例： `switch# copy tftp:adminca.crl bootflash:adminca.crl`	リモート サーバから CRL をダウンロードします。 *scheme* 引数として、**tftp:**、**ftp:**、**scp:**、または **sftp:** を指定できます。*server* 引数は、リモート サーバのアドレスまたは名前であり、*url* 引数はリモート サーバにあるソース ファイルへのパスです。 *server*、*url*、および *filename* の各引数は、大文字小文字を区別して入力します。
ステップ 2	**configure terminal** 例： `switch# configure terminal switch(config)#`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**crypto ca crl request***name***bootflash:***filename* 例： `switch(config)# crypto ca crl request admin-ca bootflash:adminca.crl`	ファイルで指定されている CRL を設定するか、現在の CRL と置き換えます。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 5	**show crypto ca crl***name* 例： `switch# show crypto ca crl admin-ca`	（任意） CA の CRL 情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

CA の設定からの証明書の削除

トラスト ポイントに設定されているアイデンティティ証明書や CA 証明書を削除できます。最初にアイデンティティ証明書を削除し、その後で CA 証明書を削除します。アイデンティティ証明書を削除した後で、RSA キーペアとトラストポイントの関連付けを解除できます。証明書の削除は、期限切れになった証明書や取り消された証明書、破損した（あるいは破損したと思われる）キー ペア、現在は信頼されていない CA を削除するために必要です。

手順の概要

1. **configure terminal**
2. **crypto ca trustpoint***name*
3. **delete ca-certificate**
4. **delete certificate** [**force**]
5. **exit**
6. （任意） **show crypto ca certificates** [*name*]
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**crypto ca trustpoint***name*
	
	例：
	`switch(config)# crypto ca trustpoint admin-ca`
	`switch(config-trustpoint)#`
		トラストポイント CA を指定し、トラストポイント コンフィギュレーション モードを開始します。

ステップ 3	**delete ca-certificate** 例： `switch(config-trustpoint)# delete ca-certificate`	CA 証明書または証明書チェーンを削除します。
ステップ 4	**delete certificate** [**force**] 例： `switch(config-trustpoint)# delete certificate`	アイデンティティ証明書を削除します。 削除しようとしているアイデンティティ証明書が証明書チェーン内の最後の証明書である場合や、デバイス内の唯一のアイデンティティ証明書である場合は、**force** オプションを使用する必要があります。この要件は、証明書チェーン内の最後の証明書や唯一のアイデンティティ証明書を誤って削除してしまい、アプリケーション（SSH など）で使用する証明書がなくなってしまうことを防ぐために設けられています。

ステップ 5	**exit**
	
	例：
	`switch(config-trustpoint)# exit`
	`switch(config)#`
		トラストポイント コンフィギュレーション モードを終了します。

ステップ 6	**show crypto ca certificates** [*name*] 例： `switch(config)# show crypto ca certificates admin-ca`	（任意） CA の証明書情報を表示します。
ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Cisco NX-OS デバイスからの RSA キー ペアの削除

RSA キー ペアが何らかの理由で破損し、現在は使用されてないと見られるときには、その RSA キー ペアを Cisco NX-OS デバイスから削除することができます。

（注） デバイスから RSA キー ペアを削除した後、CA アドミニストレータに、その CA にあるこのデバイスの証明書を取り消すよう依頼します。その証明書を最初に要求したときに作成したチャレンジ パスワードを入力する必要があります。

手順の概要

1. **configure terminal**
2. **crypto key zeroize rsa***label*
3. **exit**
4. （任意） **show crypto key mypubkey rsa**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**crypto key zeroize rsa***label* 例： `switch(config)# crypto key zeroize rsa MyKey`	RSA キー ペアを削除します。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show crypto key mypubkey rsa** 例： `switch# show crypto key mypubkey rsa`	（任意） RSA キー ペアの設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

証明書要求の作成，（244 ページ）

PKI の設定の確認

PKI 設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show crypto key mypubkey rsa	Cisco NX-OS デバイスで作成された RSA 公開キーの情報を表示します。
show crypto ca certificates	CA とアイデンティティ証明書についての情報を表示します。
show crypto ca crl	CA の CRL についての情報を表示します。
show crypto ca certstore	cert-store の設定を表示します。
show crypto ca remote-certstore	リモートの cert-store の設定を表示します。
show crypto certificatemap	証明書マッピングのフィルタを表示します。
show crypto ssh-auth-map	SSH認可用に設定されたマッピングのフィルタを表示します。
show crypto ca trustpoints	CA トラストポイントについての情報を表示します。

PKI の設定例

ここでは、Microsoft Windows Certificate サーバを使用して Cisco NX-OS デバイスで証明書と CRL を設定する作業の例について説明します。

（注） デジタル証明書の作成には、どのようなタイプのサーバでも使用できます。Microsoft Windows Certificate サーバに限られることはありません。

Cisco NX-OS デバイスでの証明書の設定

Cisco NX-OS デバイスで証明書を設定するには、次の手順に従ってください。

ステップ 1 デバイスの FQDN を設定します。

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# hostname Device-1
Device-1(config)#
```

ステップ 2 デバイスの DNS ドメイン名を設定します。

```
Device-1(config)# ip domain-name cisco.com
```

ステップ 3 トラストポイントを作成します。

```
Device-1(config)# crypto ca trustpoint myCA
Device-1(config-trustpoint)# exit
Device-1(config)# show crypto ca trustpoints
trustpoint: myCA; key:
revokation methods:  crl
```

ステップ 4 このデバイス用の RSA キー ペアを作成します。

```
Device-1(config)# crypto key generate rsa label myKey exportable modulus 1024
Device-1(config)# show crypto key mypubkey rsa
key label: myKey
key size: 1024
exportable: yes
```

ステップ 5 RSA キー ペアとトラストポイントを関連付けます。

```
Device-1(config)# crypto ca trustpoint myCA
Device-1(config-trustpoint)# rsakeypair myKey
Device-1(config-trustpoint)# exit
Device-1(config)# show crypto ca trustpoints
trustpoint: myCA; key: myKey
revokation methods:  crl
```

ステップ 6 Microsoft Certificate Service の Web インターフェイスから CA をダウンロードします。

ステップ 7 トラストポイントに登録する CA を認証します。

```
Device-1(config)# crypto ca authenticate myCA
input (cut & paste) CA certificate (chain) in PEM format;
end the input with a line containing only END OF INPUT :
-----BEGIN CERTIFICATE-----
```

```
MIIC4jCCAoygAwIBAgIQBWDSiay0GZRPSRIljK0ZejANBgkqhkiG9w0BAQUFADCB
kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklO
MRIwEAYDVQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UE
ChMFQ2lzY28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBD
QTAeFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN
AQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UEBhMCSU4xEjAQBgNVBAgTCUth
cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVDaXNjbzETMBEG
A1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBhcm5hIENBMFwwDQYJKoZIhvcN
AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHzluNccNM87ypyzwuoSNZXOMpeRXXI
OzyBAgiXT2ASFuUOwQ1iDM8rO/41jf8RxvYKvysCAwEAAaOBvzCBvDALBgNVHQ8E
BAMCAcYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyjyRoMbrCNMRU2OyRhQ
GgsWbHEwawYDVR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJuYSUyMENBLmNybDAwoC6gLIYqZmlsZTovL1xcc3NlLTA4XENlcnRFbnJv
bGxcQXBhcm5hJTIwQ0EuY3JsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEB
BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaqNgLh0AFcT0rEyuyt/WYGPzksF9Ea
NBG7E0oN66zex0EOEfG1Vs6mXp1//w==
-----END CERTIFICATE-----
END OF INPUT
Fingerprint(s): MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12
Do you accept this certificate? [yes/no]:y

Device-1(config)# show crypto ca certificates
Trustpoint: myCA
CA certificate 0:
subject= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/
L=Bangalore/O=Yourcompany/OU=netstorage/CN=Aparna CA
issuer= /emailAddress=admin@yourcompany.com/C=IN/ST=Karnataka/
L=Bangalore/O=Yourcompany/OU=netstorage/CN=Aparna CA
serial=0560D289ACB419944F4912258CAD197A
notBefore=May  3 22:46:37 2005 GMT
notAfter=May  3 22:55:17 2007 GMT
MD5 Fingerprint=65:84:9A:27:D5:71:03:33:9C:12:23:92:38:6F:78:12
purposes: sslserver sslclient ike
```

ステップ 8 トラストポイントに登録するために使用する証明書要求を作成します。

```
Device-1(config)# crypto ca enroll myCA
 Create the certificate request ..
 Create a challenge password. You will need to verbally provide this
  password to the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the configuration.
  Please make a note of it.
  Password: nbv123
 The subject name in the certificate will be: Device-1.cisco.com
 Include the switch serial number in the subject name? [yes/no]: no
 Include an IP address in the subject name [yes/no]: yes
ip address: 10.10.1.1
 The certificate request will be displayed...
-----BEGIN CERTIFICATE REQUEST-----
MIIBqzCCARQCAQAwHDEaMBgGA1UEAxMRVmVnYXMtMS5jaXNjby5jb20wgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVaSMqNIgJ2kt8rl4lKY
0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnjuCXGvjb+wj0hEhv/y51T9y
P2NJJ8ornqShrvFZgC7ysN/PyMwKcgzhbVpj+rargZvHtGJ91XTq4WoVkSCzXv8S
VqyH0vEvAgMBAAGgTzAVBgkqhkiG9w0BCQcxCBMGbmJ2MTIzMDYGCSqGSIb3DQEJ
```

```
DjEpMCcwJQYDVR0RAQH/BBswGYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwDQYJ
KoZIhvcNAQEEBQADgYEAkT60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99GlFWgt
PftrNcWUE/pw6HayfQl2T3ecgNwel2d15133YBF2bktExiI6Ul88nTOjglXMjja8
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0=
-----END CERTIFICATE REQUEST-----
```

ステップ 9 Microsoft Certificate Service の Web インターフェイスからアイデンティティ証明書を要求します。

ステップ 10 アイデンティティ証明書をインポートします。

```
Device-1(config)# crypto ca import myCA certificate
input (cut & paste) certificate in PEM format:
-----BEGIN CERTIFICATE-----
MIIEADCCA6qgAwIBAgIKCjOOoQAAAAAAdDANBgkqhkiG9w0BAQUFADCBkDEgMB4G
CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAklOMRIwEAYD
VQQIEwlLYXJuYXRha2ExEjAQBgNVBAcTCUJhbmdhbG9yZTEOMAwGA1UEChMFQ2lz
Y28xEzARBgNVBAsTCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFwYXJuYSBDQTAeFw0w
NTExMTIwMzAyNDBaFw0wNjExMTIwMzEyNDBaMBwxGjAYBgNVBAMTEVZlZ2FzLTEu
Y2lzY28uY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNVACdjQu41C
dQ1WkjKjSICdpLfK5eJSmNCQujGpzcuKsZPFXjF2UoiyeCYE8ylncWyw5E08rJ47
glxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMCnIM4W1aY/q2q4Gb
x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDVR0RAQH/BBsw
GYIRVmVnYXMtMS5jaXNjby5jb22HBKwWH6IwHQYDVR0OBBYEFKCLi+2sspWEfgrR
bhWmlVyo9jngMIHMBgNVHSMEgcQwgcGAFCco8kaDG6wjTEVNjskYUBoLFmxxoYGW
pIGTMIGQMSAwHgYJKoZIhvcNAQkBFhFhbWFuZGtlQGNpc2NvLmNvbTELMAkGA1UE
BhMCSU4xEjAQBgNVBAgTCUthcm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4w
DAYDVQQKEwVDaXNjbzETMBEGA1UECxMKbmV0c3RvcmFnZTESMBAGA1UEAxMJQXBh
cm5hIENBghAFYNKJrLQZlE9JEiWMrRl6MGsGA1UdHwRkMGIwLqAsoCqGKGh0dHA6
Ly9zc2UtMDgvQ2VydEVucm9sbC9BcGFybmElMjBDQS5jcmwwMKAuoCyGKmZpbGU6
Ly9cXHNzZS0wOFxDZXJ0RW5yb2xsXEFwYXJuYSUyMENBLmNybDCBigYIKwYBBQUH
AQEEfjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3NlLTA4L0NlcnRfbnJvbGwvc3Nl
LTA4X0FwYXJuYSUyMENBLmNydDA9BggrBgEFBQcwAoYxZmlsZTovL1xcc3NlLTA4
XENlcnRfbnJvbGxcc3NlLTA4X0FwYXJuYSUyMENBLmNydDANBgkqhkiG9w0BAQUF
AANBADbGBGsbe7GNLh9xeOTWBNbm24U69ZSuDDcOcUZUUTgrpnTqVpPyejtsyflw
E36cIZu4WsExREqxbTk8ycx7V5o=
-----END CERTIFICATE-----
Device-1(config)# exit
Device-1#
```

ステップ 11 証明書の設定を確認します。

ステップ 12 証明書の設定をスタートアップ コンフィギュレーションに保存します。

関連トピック

CA 証明書のダウンロード, （260 ページ）
アイデンティティ証明書の要求, （264 ページ）

cert-store および証明書マッピングのフィルタの設定

証明書認証用のリモートの cert-store を設定し、証明書マッピングのフィルタを設定するには、次の手順を実行します。

手順の概要

1. 証明書認証用のリモートの cert-store を指定します。
2. cert-store の設定を表示します。
3. LDAP との通信時に使用する LDAP サーバ グループを設定します。
4. リモートの cert-store の証明書失効リスト（CRL）を更新するリフレッシュ タイムを設定します。
5. リモートの cert-store の設定を表示します。
6. 新しいフィルタ マップを作成します。
7. フィルタ マップ内の証明書マッピングのフィルタを設定します。
8. SSH の証明書マッピングのフィルタを設定します。
9. 証明書マッピングのフィルタを表示します。
10. 証明書の設定をスタートアップ コンフィギュレーションに保存します。

手順の詳細

ステップ 1 証明書認証用のリモートの cert-store を指定します。

```
switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# crypto ca lookup remote
switch(config)#
```

ステップ 2 cert-store の設定を表示します。

```
switch(config)# show crypto ca certstore
```

ステップ 3 LDAP との通信時に使用する LDAP サーバ グループを設定します。

```
switch(config)# crypto ca remote ldap server-group group1
```

ステップ 4 リモートの cert-store の証明書失効リスト（CRL）を更新するリフレッシュ タイムを設定します。

```
switch(config)# crypto ca remote ldap crl-refresh-time 10
```

ステップ 5 リモートの cert-store の設定を表示します。

```
switch(config)# show crypto ca remote-certstore
```

ステップ 6 新しいフィルタ マップを作成します。

```
switch(config)# crypto certificatemap mapname filtermap1
```

ステップ 7 フィルタ マップ内の証明書マッピングのフィルタを設定します。

```
switch(config-certmap-filter)# filter subject-name cn=jsmith,ou=PKI,o=Acme,c=US
switch(config-certmap-filter)# filter altname-email jsmith@acme.com
switch(config-certmap-filter)# exit
switch(config)#
```

ステップ 8 SSH の証明書マッピングのフィルタを設定します。

```
switch(config)# crypto cert ssh-authorize default map filtermap1
```

ステップ 9 証明書マッピングのフィルタを表示します。

```
switch(config)# show crypto certificatemap
switch(config)# show crypto ssh-auth-map
```

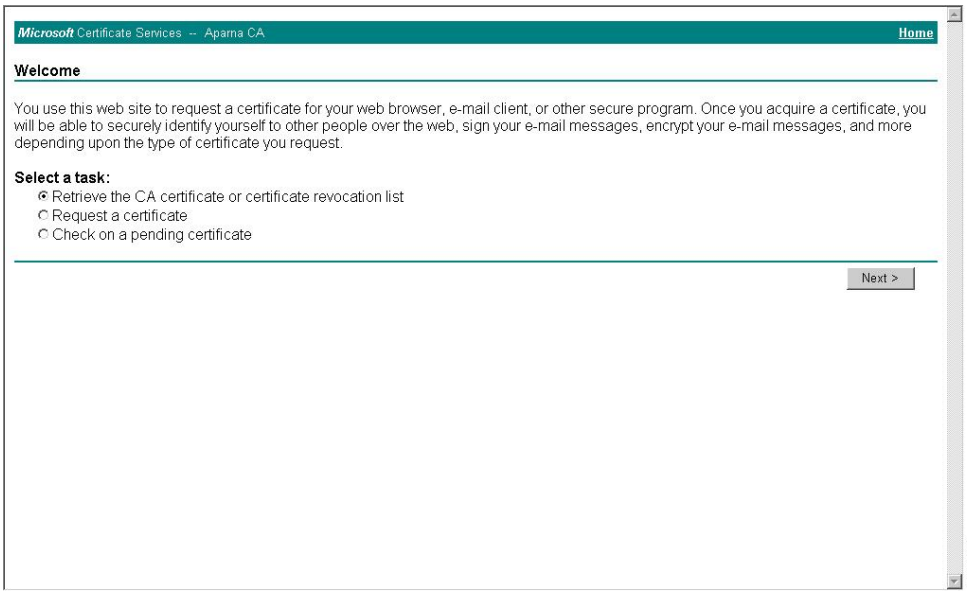
ステップ 10 証明書の設定をスタートアップ コンフィギュレーションに保存します。

```
switch(config)# copy running-config startup-config
```

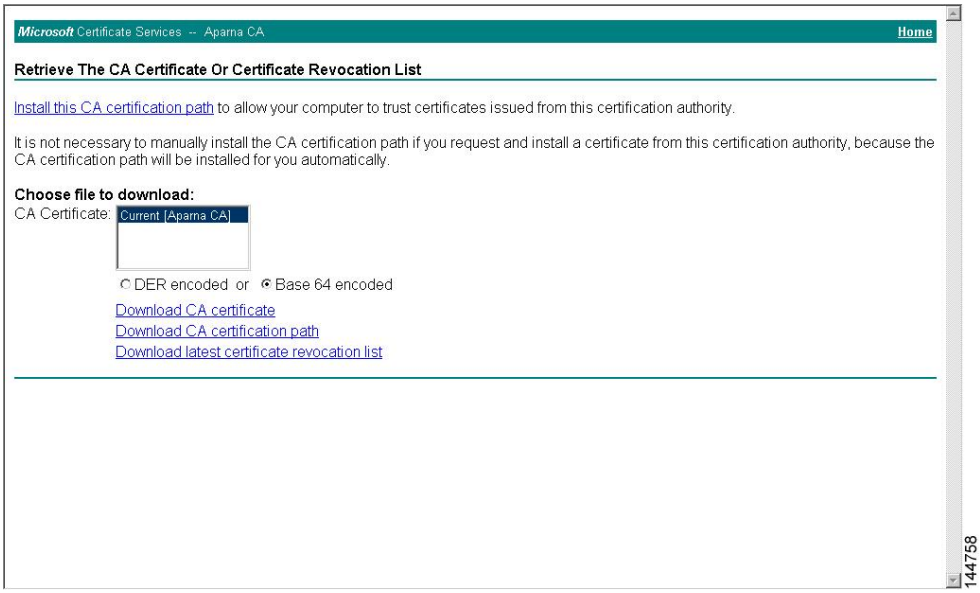
CA 証明書のダウンロード

Microsoft Certificate Service の Web インターフェイスから CA 証明書をダウンロードする手順は、次のとおりです。

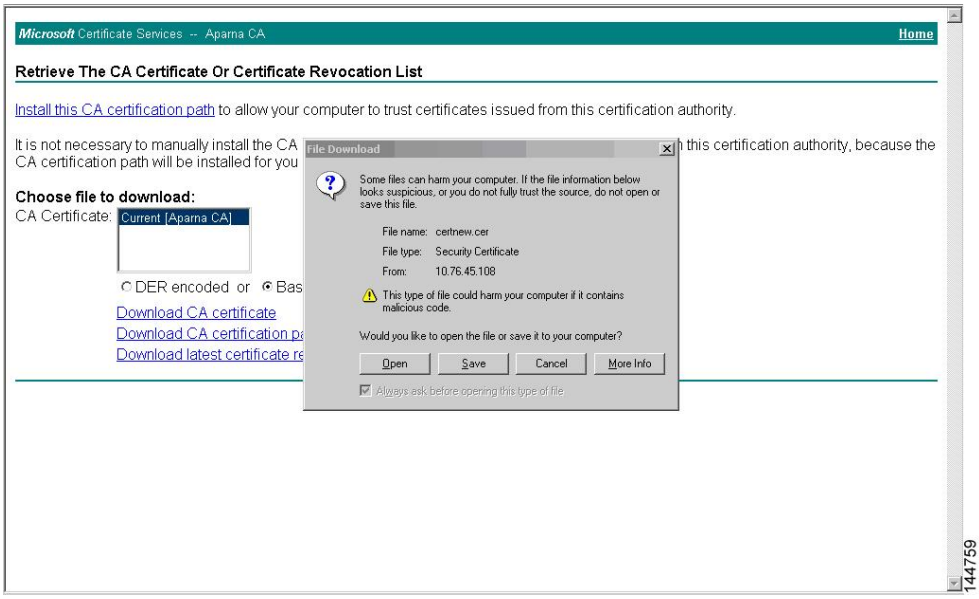
ステップ 1 Microsoft Certificate Services の Web インターフェイスから、[Retrieve the CA certificate or certificate revocation task] をクリックし、[Next] をクリックします。



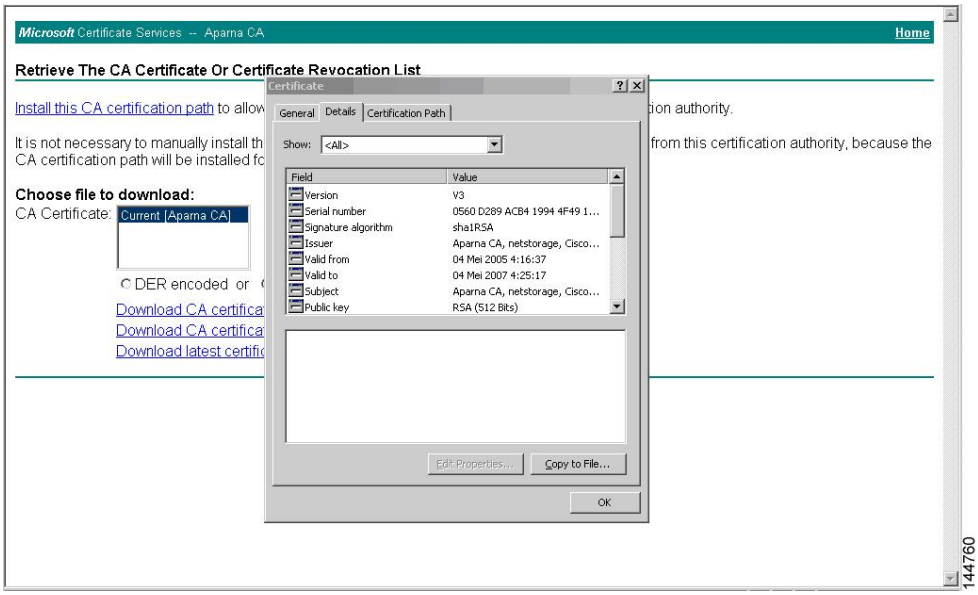
ステップ 2 表示されたリストから、ダウンロードする CA 証明書ファイルを選択します。[Base 64 encoded] をクリックし、[Download CA certificate] をクリックします。



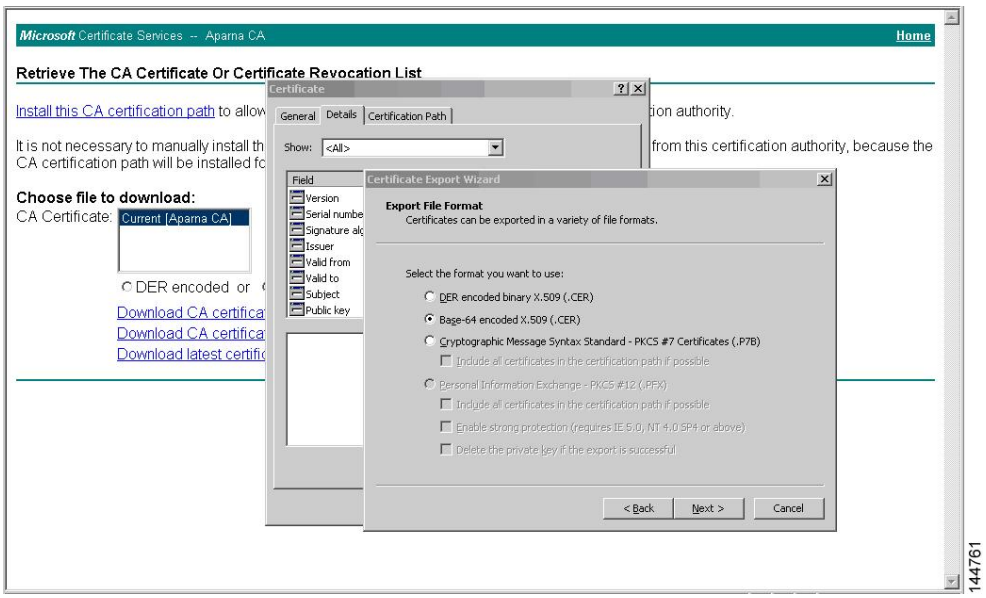
ステップ 3 [File Download] ダイアログボックスにある [Open] をクリックします。



ステップ 4 [Certificate] ダイアログボックスにある [Copy to File] をクリックし、[OK] をクリックします。



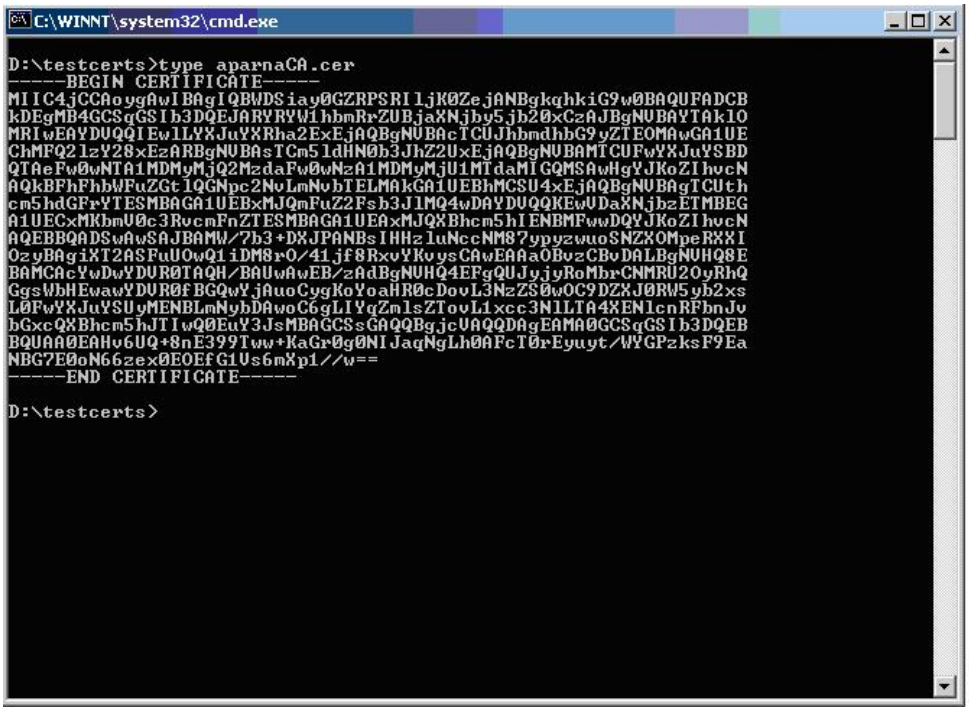
ステップ 5 [Certificate Export Wizard] ダイアログボックスから [Base-64 encoded X.509 (CER)] を選択し、[Next] をクリックします。



ステップ 6 [Certificate Export Wizard] ダイアログボックスにある [File name:] テキスト ボックスに保存するファイル名を入力し、[Next] をクリックします。

ステップ 7 [Certificate Export Wizard] ダイアログボックスで、[Finish] をクリックします。

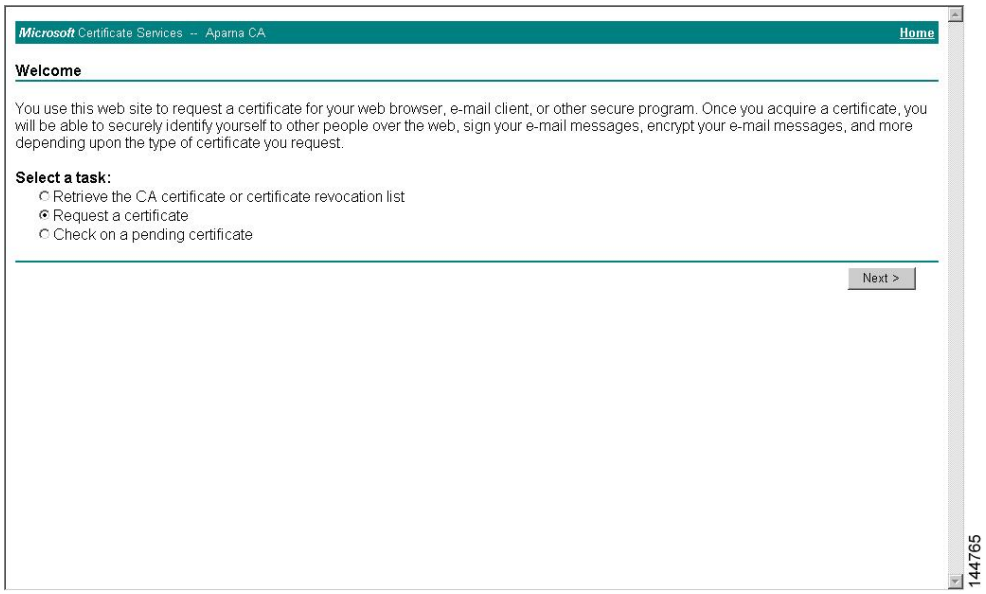
ステップ 8 Microsoft Windows の **type** コマンドを入力して、Base-64（PEM）形式で保存されている CA 証明書を表示します。



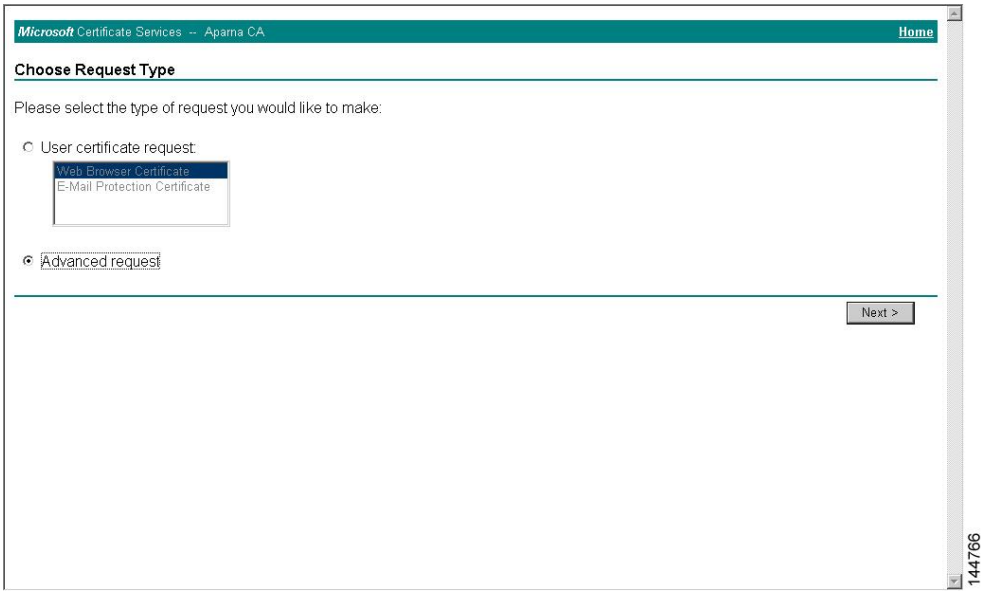
アイデンティティ証明書の要求

PKCS#12 証明書署名要求（CSR）を使用して Microsoft Certificate サーバにアイデンティティ証明書を要求するには、次の手順に従ってください。

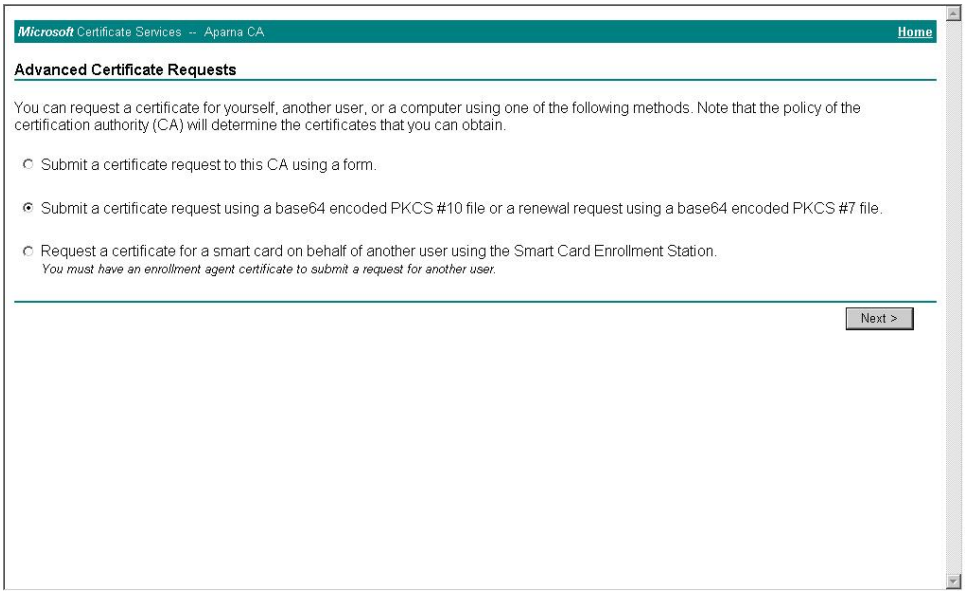
ステップ 1 Microsoft Certificate Services の Web インターフェイスから、[Request a certificate] をクリックし、[Next] をクリックします。



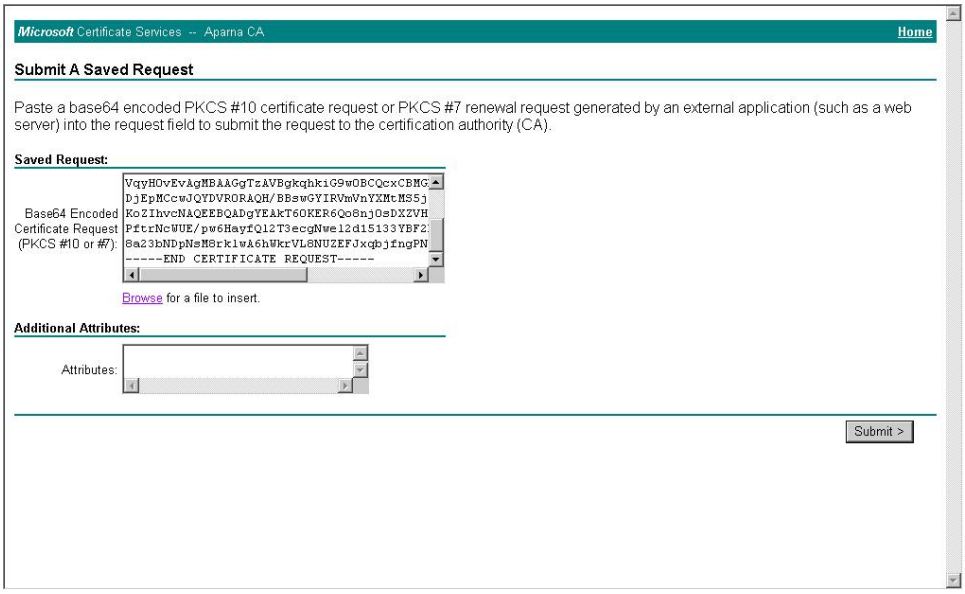
ステップ 2 [Advanced request] をクリックし、[Next] をクリックします。



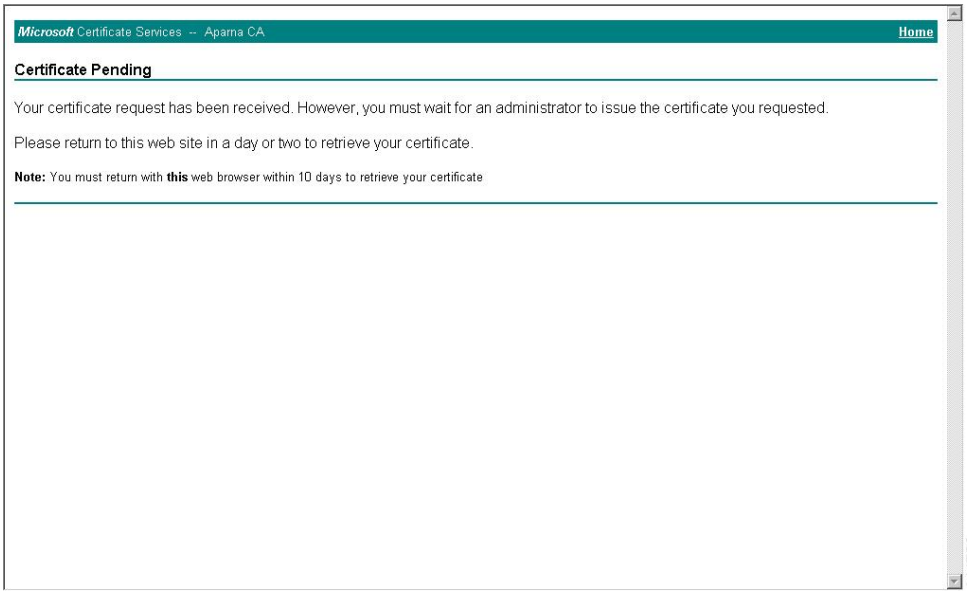
ステップ 3 [Submit a certificate request using a base64 encoded PKCS#10 file or a renewal request using a base64 encoded PKCS#7 file] をクリックし、[Next] をクリックします。



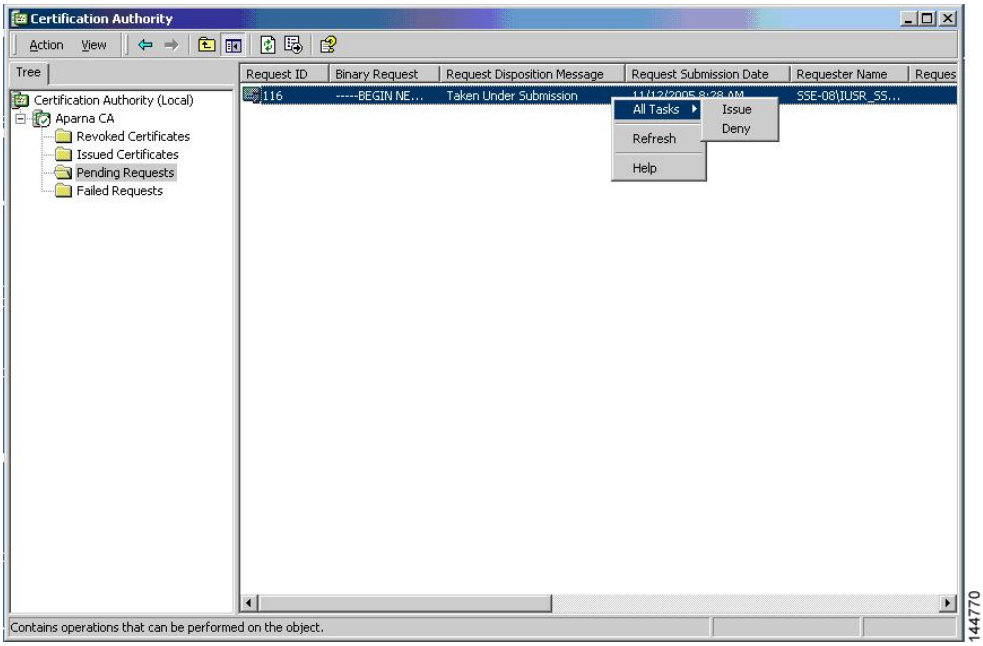
ステップ 4 [Saved Request] テキスト ボックスに、base64 の PKCS#10 証明書要求をペーストし、[Next] をクリックします。証明書要求が Cisco NX-OS デバイスのコンソールからコピーされます。



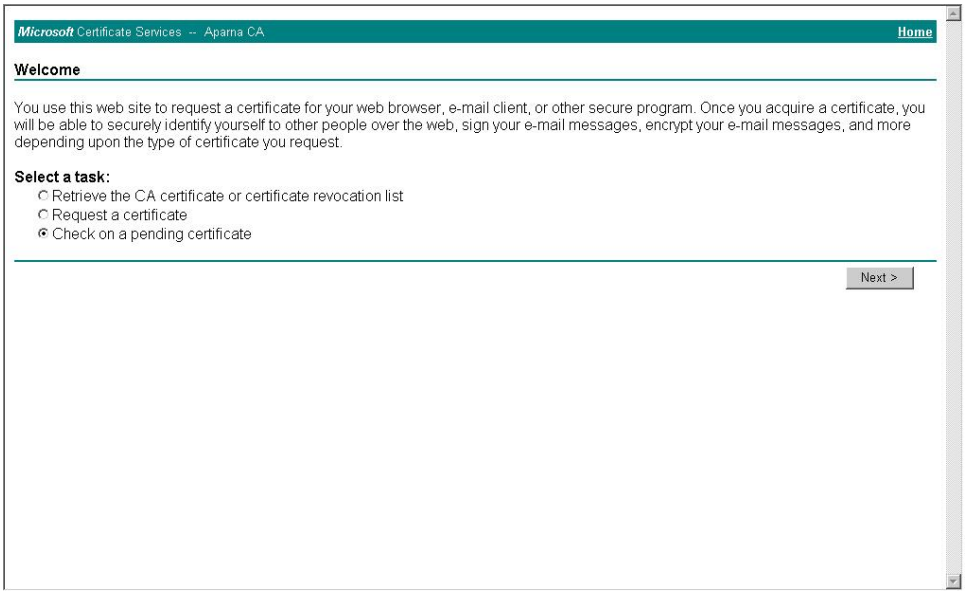
ステップ 5 CA アドミニストレータから証明書が発行されるまで、1 ～ 2 日間待ちます。



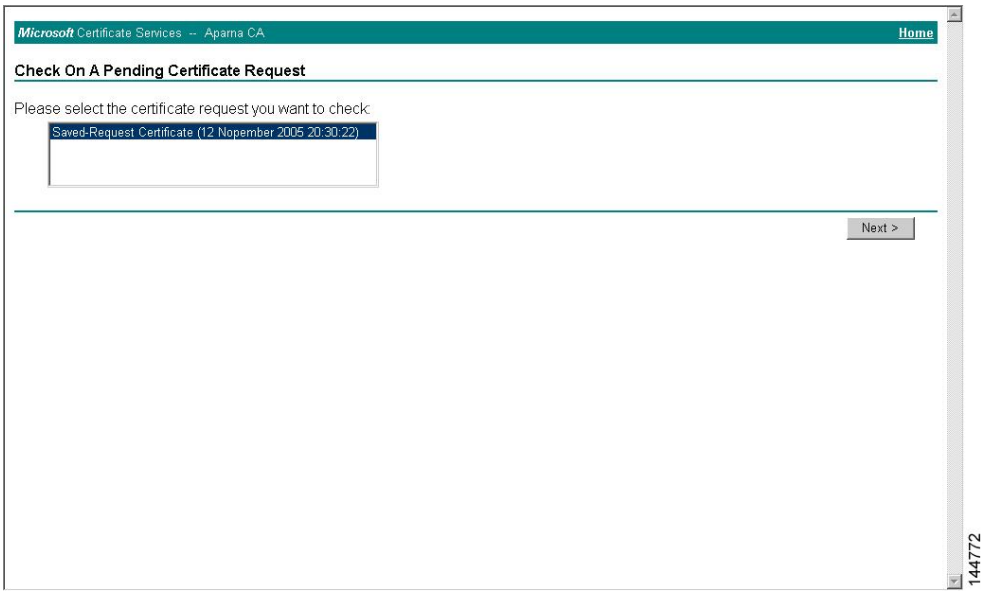
ステップ 6 CA アドミニストレータが証明書要求を承認するのを確認します。



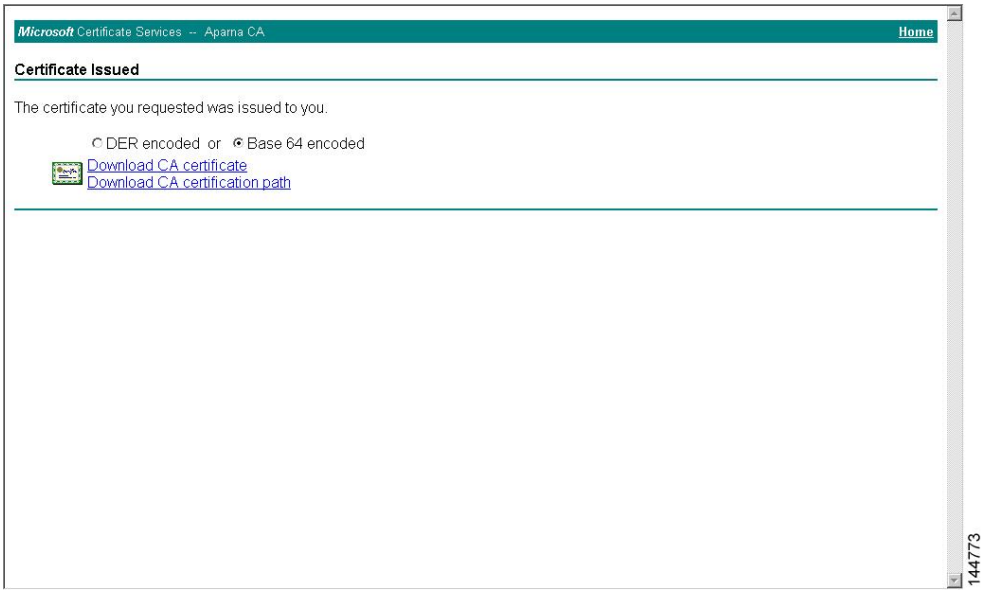
ステップ 7 Microsoft Certificate Services の Web インターフェイスから、[Check on a pending certificate] をクリックし、[Next] をクリックします。


Microsoft Certificate Services -- Aparna CA
Home
Welcome
You use this web site to request a certificate for your web browser, e-mail client, or other secure program. Once you acquire a certificate, you will be able to securely identify yourself to other people over the web, sign your e-mail messages, encrypt your e-mail messages, and more depending upon the type of certificate you request.
Select a task:
Retrieve the CA certificate or certificate revocation list
Request a certificate
Check on a pending certificate
Next >
144771

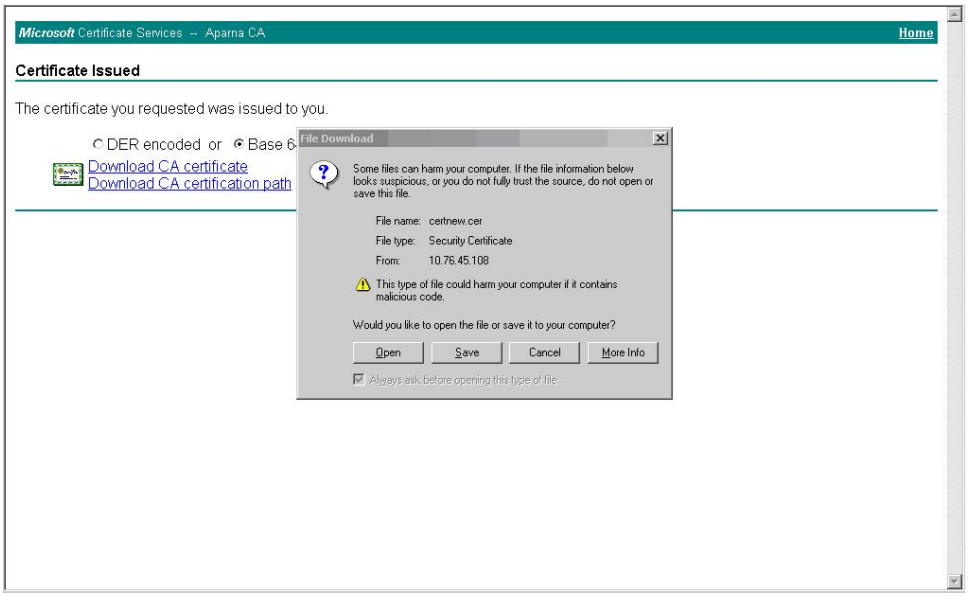
ステップ 8 チェックする証明書要求を選択して、[Next] をクリックします。



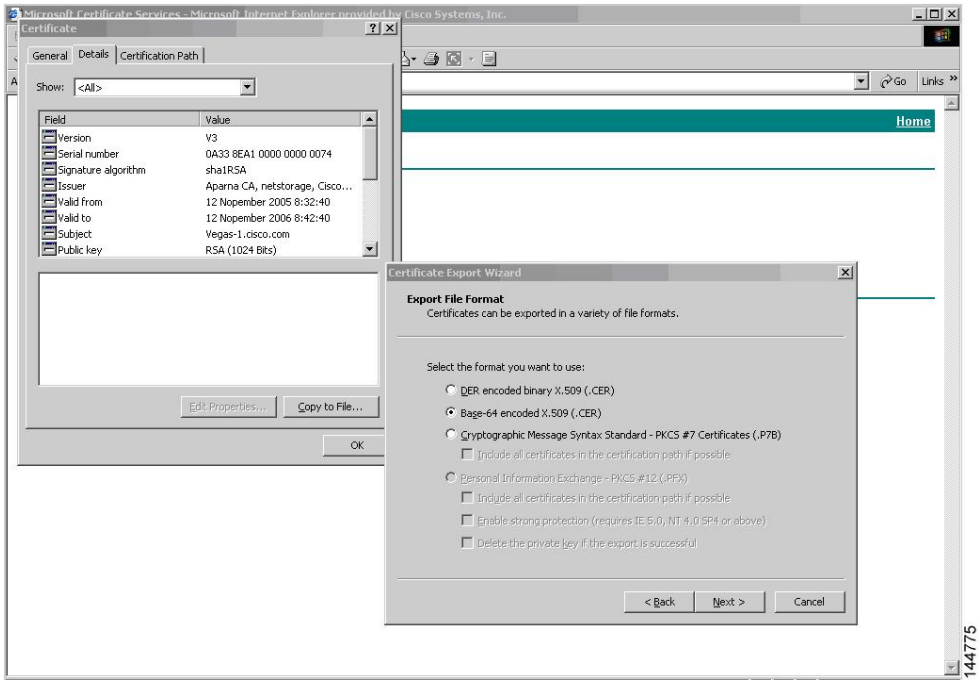
ステップ 9 [Base 64 encoded] をクリックして、[Download CA certificate] をクリックします。



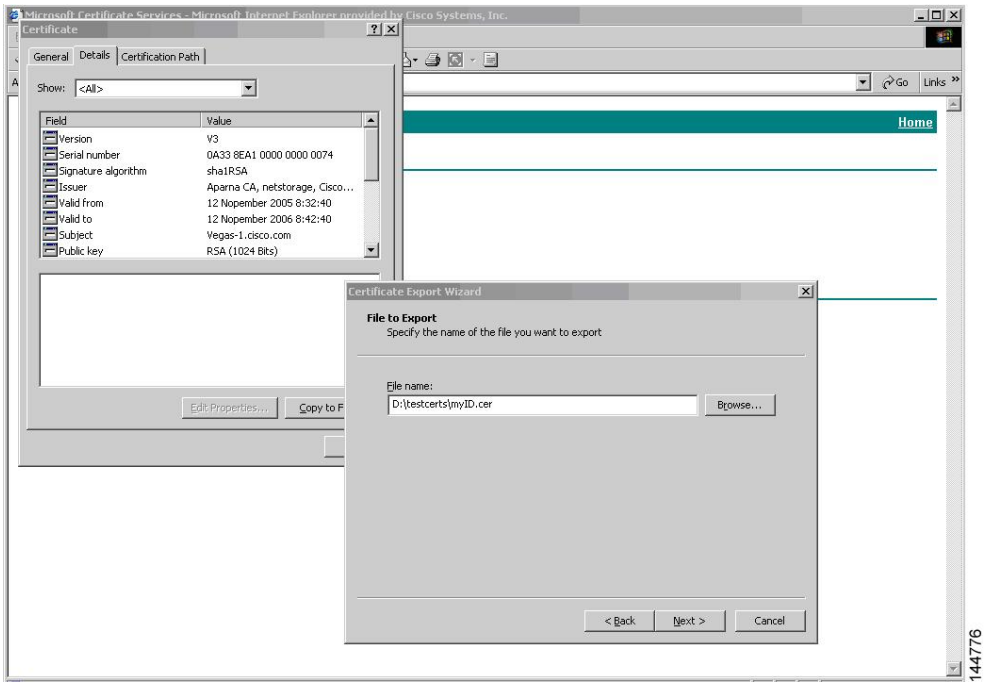
ステップ 10 [File Download] ダイアログボックスで、[Open] をクリックします。



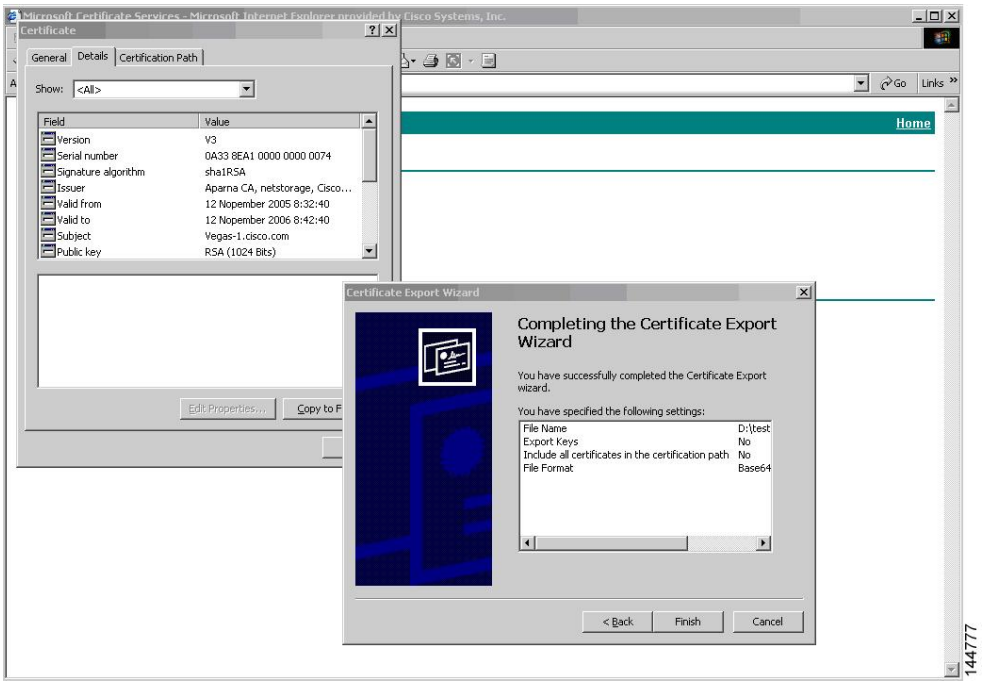
ステップ 11 [Certificate] ボックスで、[Details] タブをクリックし、[Copy to File...] をクリックします。[Certificate Export Wizard] ダイアログボックスで、[Base-64 encoded X.509 (.CER)] をクリックし、[Next] をクリックします。



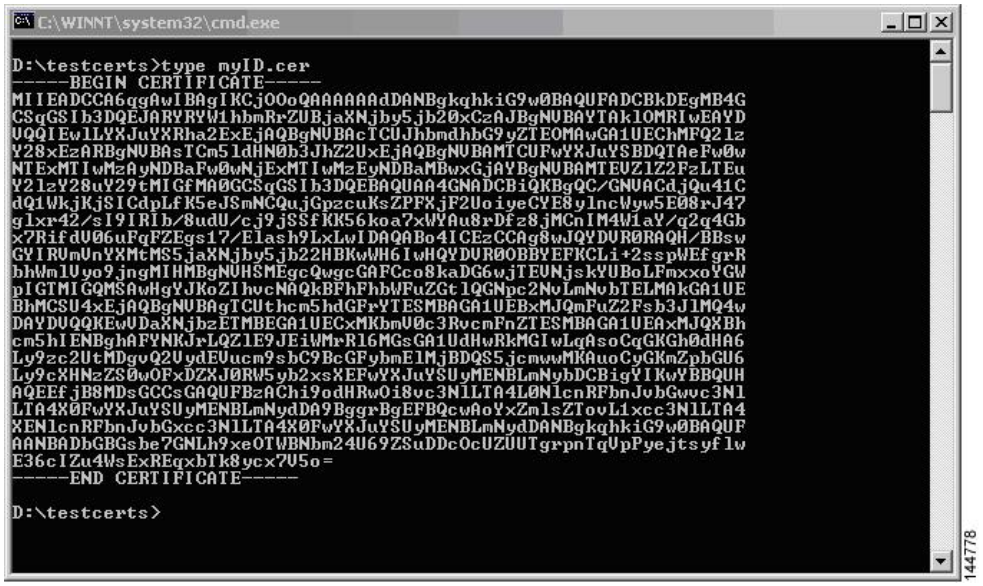
ステップ 12 [Certificate Export Wizard] ダイアログボックスにある [File name:] テキスト ボックスに保存するファイル名を入力し、[Next] をクリックします。



ステップ 13 [Finish] をクリックします。



ステップ 14 Microsoft Windows の type コマンドを入力して、アイデンティティ証明書を Base-64 でエンコードされた形式で表示します。



関連トピック

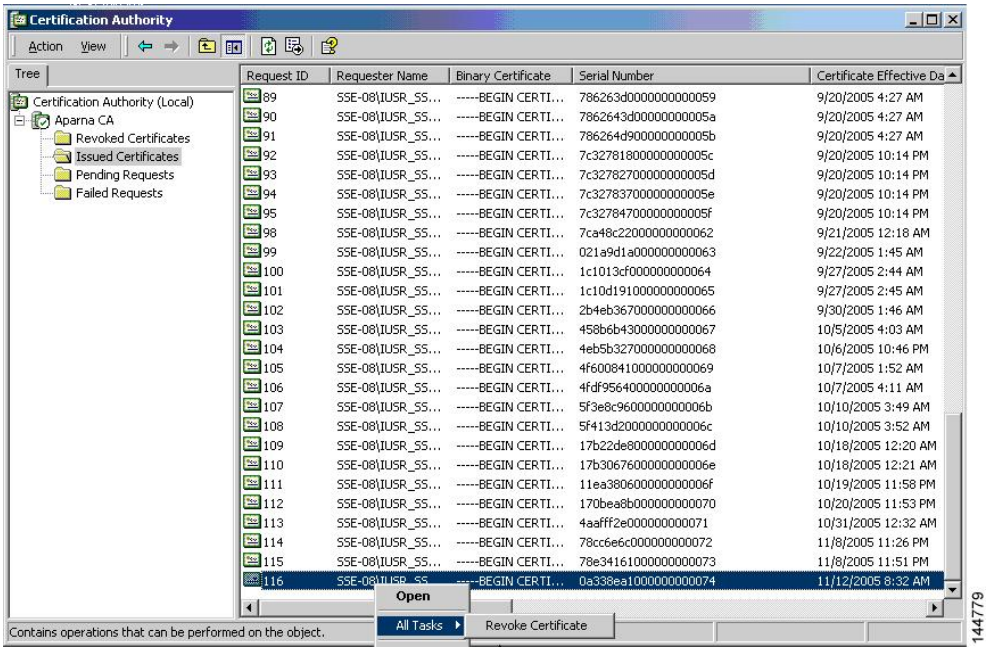
証明書要求の作成, （244 ページ）
Cisco NX-OS デバイスでの証明書の設定, （256 ページ）

証明書の取り消し

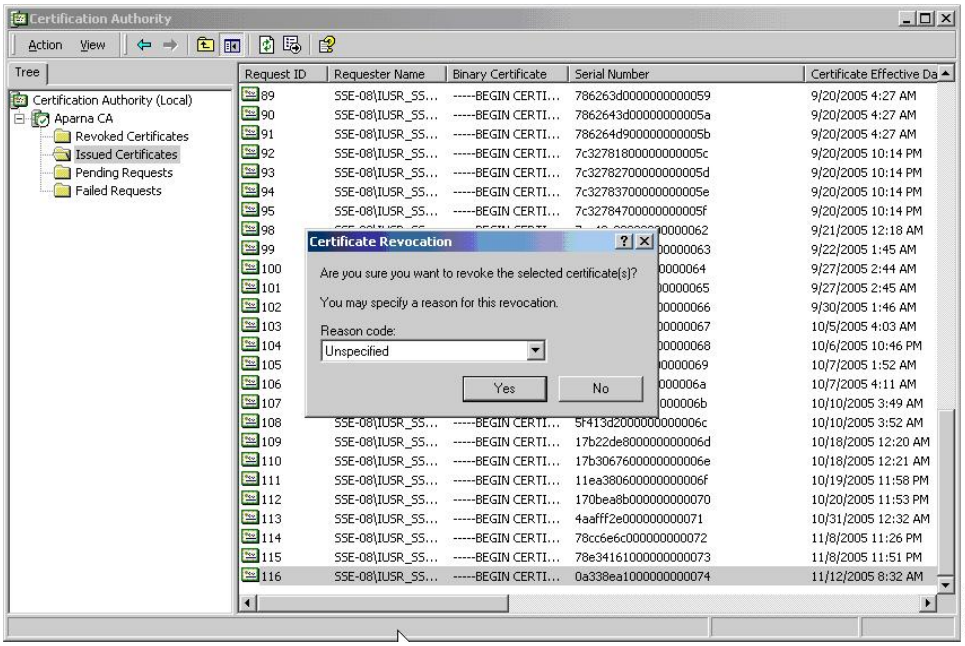
Microsoft CA 管理者プログラムを使用して証明書を取り消す手順は、次のとおりです。

ステップ 1 [Certification Authority] ツリーから、[Issued Certificates] フォルダをクリックします。リストから、取り消す証明書を右クリックします。

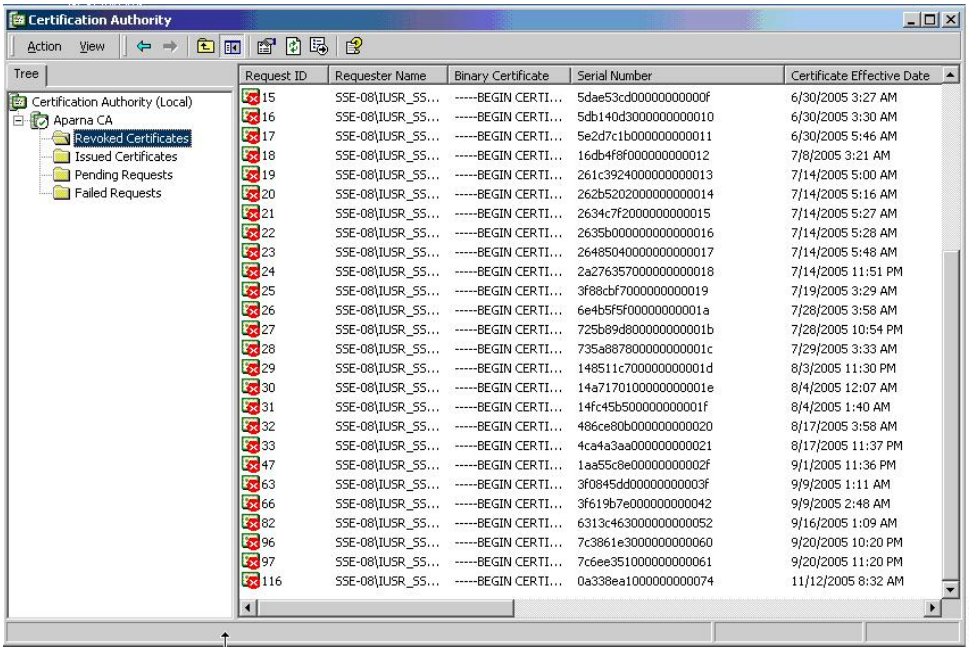
ステップ 2 [All Tasks] > [Revoke Certificate] の順に選択します。



ステップ 3 [Reason code] ドロップダウン リストから取り消しの理由を選択し、[Yes] をクリックします。



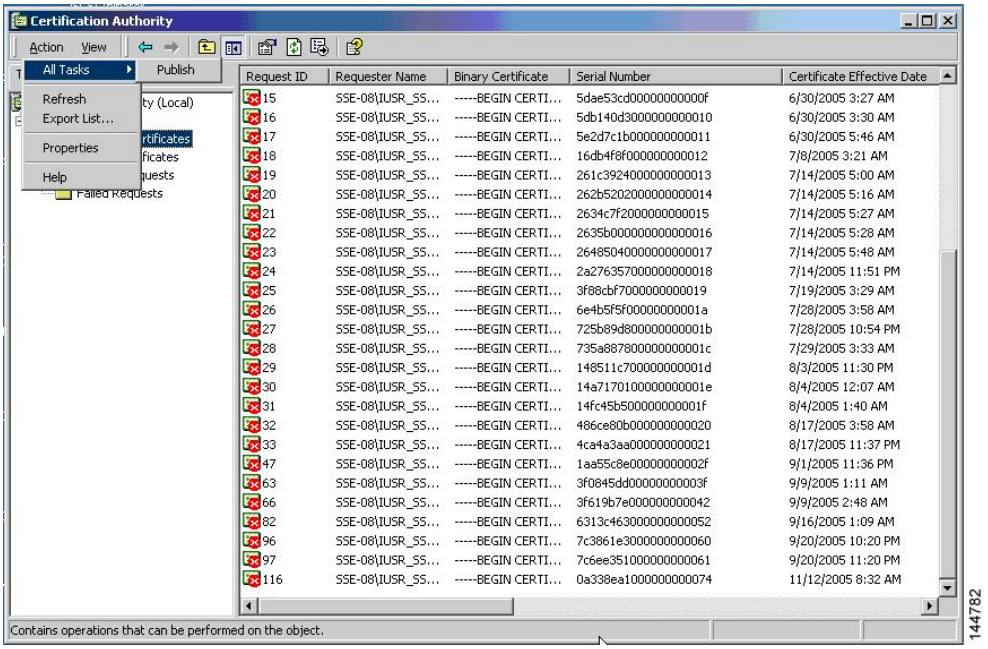
ステップ 4 [Revoked Certificates] フォルダをクリックして、証明書の取り消しを表示および確認します。



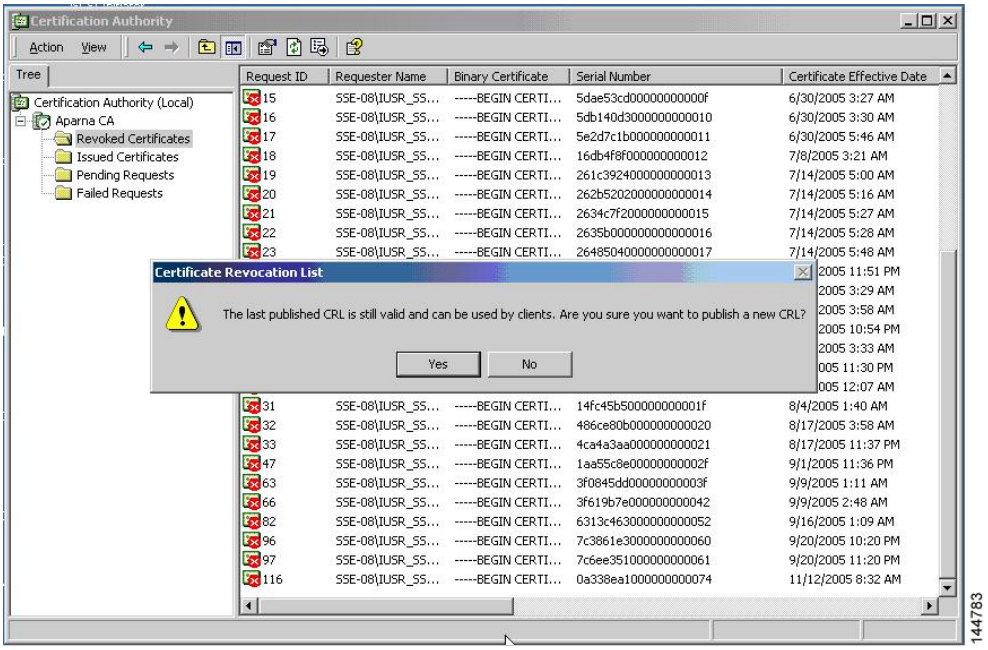
CRL の作成と公開

Microsoft CA 管理者プログラムを使用して CRL を作成および公開する手順は、次のとおりです。

ステップ 1 [Certification Authority] の画面から、[Action] > [All Tasks] > [Publish] の順に選択します。



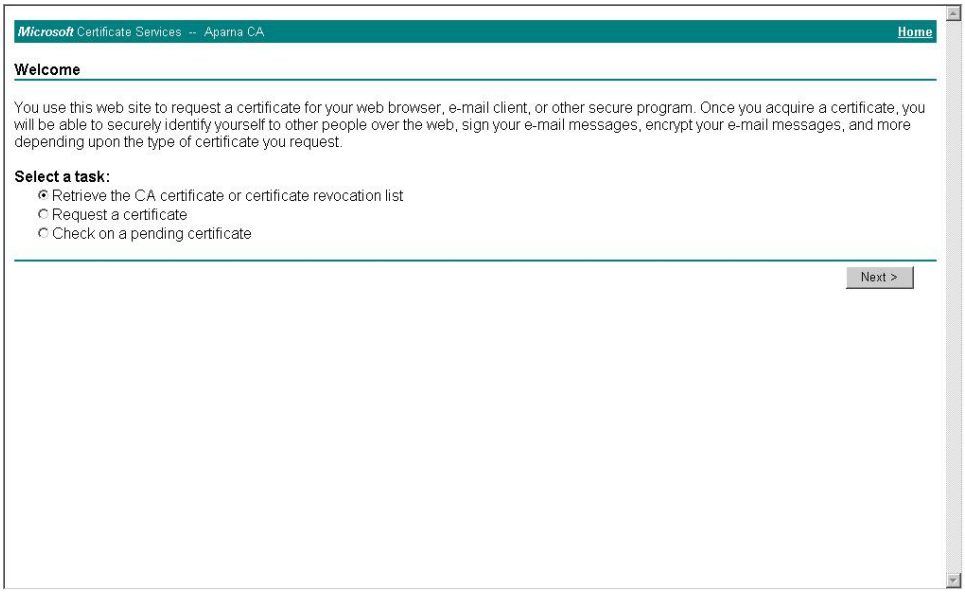
ステップ 2 [Certificate Revocation List] ダイアログボックスで、[Yes] をクリックして最新の CRL を公開します。



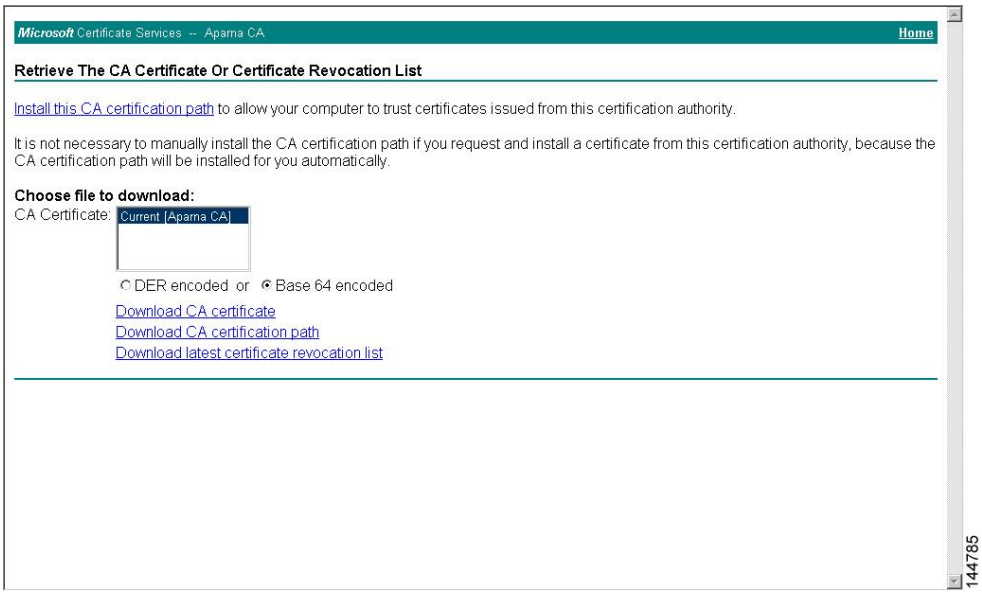
CRL のダウンロード

Microsoft 社の CA の Web サイトから CRL をダウンロードする手順は、次のとおりです。

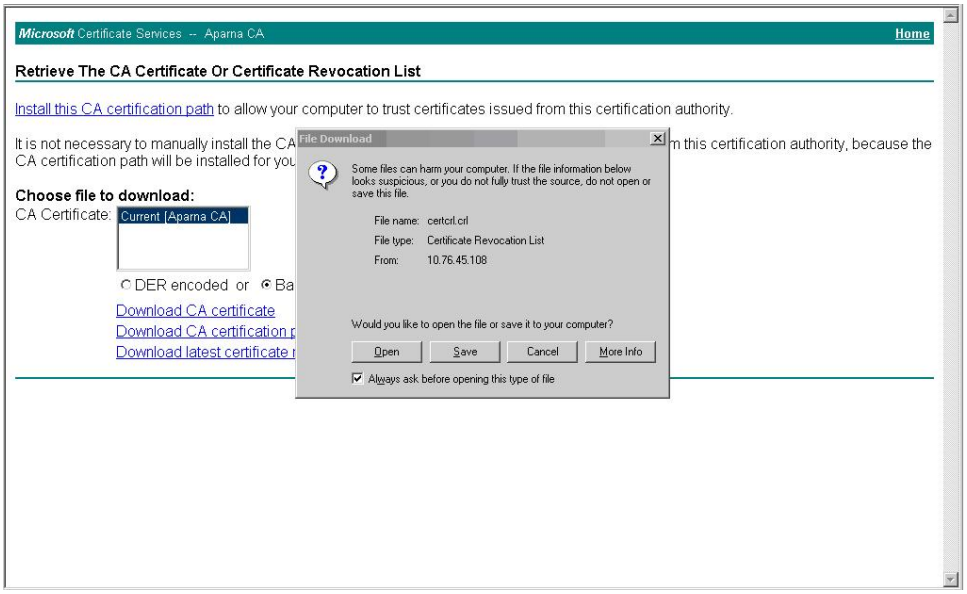
ステップ 1 Microsoft Certificate Services の Web インターフェイスから、[Retrieve the CA certificate or certificate revocation list] をクリックし、[Next] をクリックします。



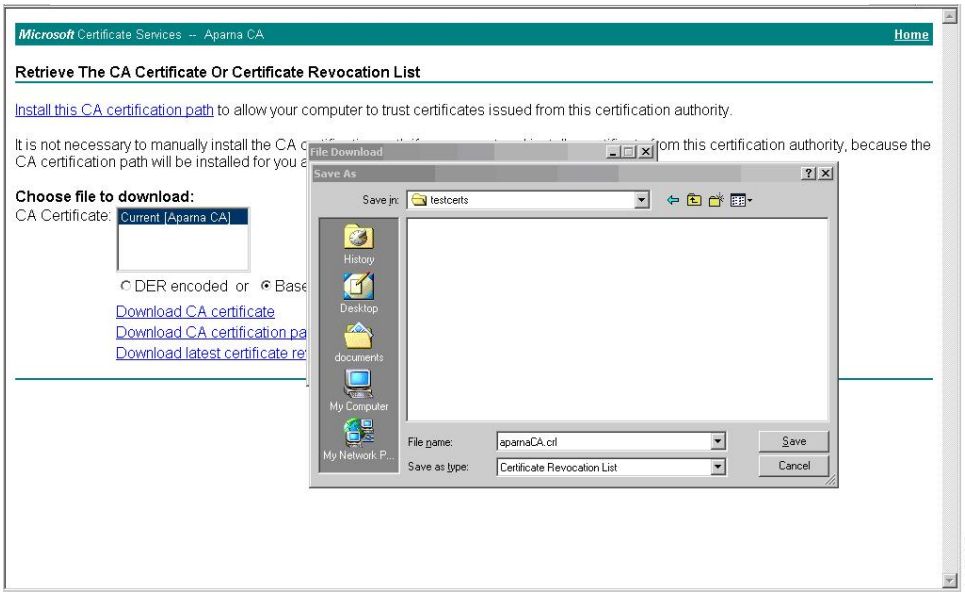
ステップ 2 [Download latest certificate revocation list] をクリックします。



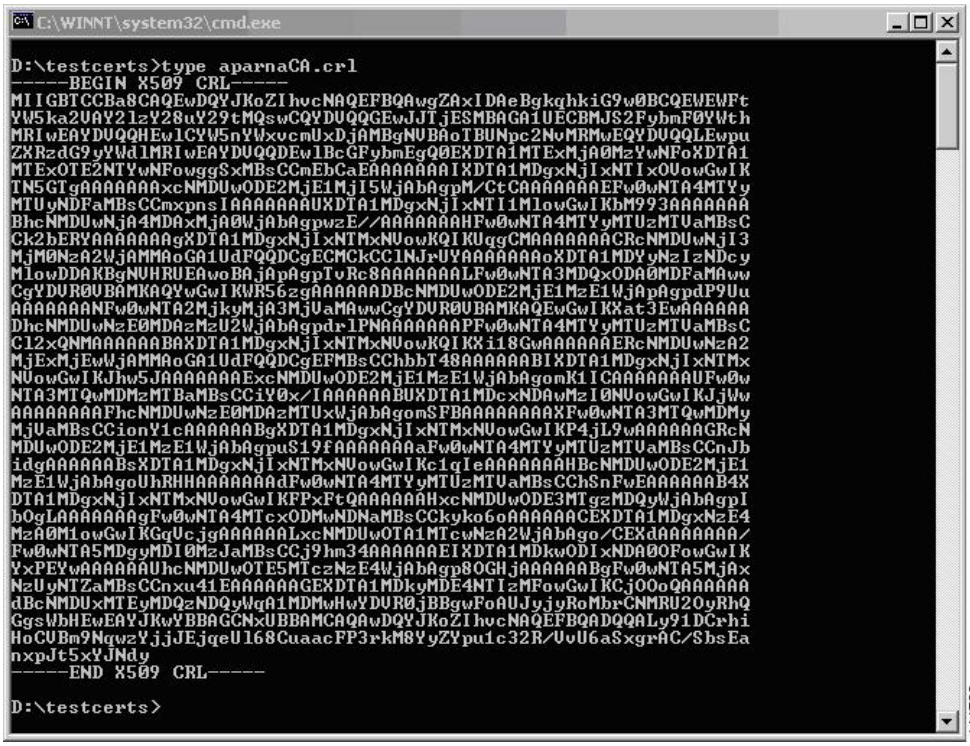
ステップ 3 [File Download] ダイアログボックスで、[Save] をクリックします。



ステップ 4 [Save As] ダイアログボックスで、保存するファイル名を入力して、[Save] をクリックします。



ステップ 5 Microsoft Windows の **type** コマンドを入力して、CRL を表示します。



関連トピック

証明書取消確認方法の設定, （242 ページ）

CRL のインポート

CRL を CA に対応するトラストポイントにインポートする手順は、次のとおりです。

ステップ 1 CRL ファイルを Cisco NX-OS デバイスのブートフラッシュにコピーします。

```
Device-1# copy tftp:apranaCA.crl bootflash:aparnaCA.crl
```

ステップ 2 CRL を設定します。

```
Device-1# configure terminal
Device-1(config)# crypto ca crl request myCA bootflash:aparnaCA.crl
Device-1(config)#
```

ステップ 3 CRL の内容を表示します。

```
Device-1(config)# show crypto ca crl myCA
Trustpoint: myCA
CRL:
Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: /emailAddress=admin@yourcompany.com/C=IN/ST=Karnatak
Yourcompany/OU=netstorage/CN=Aparna CA
        Last Update: Nov 12 04:36:04 2005 GMT
        Next Update: Nov 19 16:56:04 2005 GMT
        CRL extensions:
            X509v3 Authority Key Identifier:
            keyid:27:28:F2:46:83:1B:AC:23:4C:45:4D:8E:C9:18:50:1
            1.3.6.1.4.1.311.21.1:
                ...
Revoked Certificates:
    Serial Number: 611B09A1000000000002
        Revocation Date: Aug 16 21:52:19 2005 GMT
Serial Number: 4CDE464E000000000003
        Revocation Date: Aug 16 21:52:29 2005 GMT
    Serial Number: 4CFC2B42000000000004
        Revocation Date: Aug 16 21:52:41 2005 GMT
    Serial Number: 6C699EC2000000000005
        Revocation Date: Aug 16 21:52:52 2005 GMT
    Serial Number: 6CCF7DDC000000000006
        Revocation Date: Jun  8 00:12:04 2005 GMT
    Serial Number: 70CC4FFF000000000007
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 4D9B1116000000000008
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 52A80230000000000009
        Revocation Date: Jun 27 23:47:06 2005 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
            CA Compromise
```

```
Serial Number: 5349AD4600000000000A
        Revocation Date: Jun 27 23:47:22 2005 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
            CA Compromise
Serial Number: 53BD173C00000000000B
        Revocation Date: Jul  4 18:04:01 2005 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
            Certificate Hold
Serial Number: 591E7ACE00000000000C
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 5D3FD52E00000000000D
        Revocation Date: Jun 29 22:07:25 2005 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
            Key Compromise
Serial Number: 5DAB771300000000000E
        Revocation Date: Jul 14 00:33:56 2005 GMT
    Serial Number: 5DAE53CD00000000000F
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 5DB140D3000000000010
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 5E2D7C1B000000000011
        Revocation Date: Jul  6 21:12:10 2005 GMT
        CRL entry extensions:
            X509v3 CRL Reason Code:
            Cessation Of Operation
Serial Number: 16DB4F8F000000000012
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 261C3924000000000013
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 262B5202000000000014
        Revocation Date: Jul 14 00:33:10 2005 GMT
    Serial Number: 2634C7F2000000000015
        Revocation Date: Jul 14 00:32:45 2005 GMT
    Serial Number: 2635B000000000000016
        Revocation Date: Jul 14 00:31:51 2005 GMT
    Serial Number: 26485040000000000017
        Revocation Date: Jul 14 00:32:25 2005 GMT
    Serial Number: 2A276357000000000018
Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 3F88CBF7000000000019
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 6E4B5F5F00000000001A
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 725B89D800000000001B
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 735A887800000000001C
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 148511C700000000001D
        Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 14A7170100000000001E
        Revocation Date: Aug 16 21:53:15 2005 GMT
```

```
Serial Number: 14FC45B500000000001F
    Revocation Date: Aug 17 18:30:42 2005 GMT
Serial Number: 486CE80B000000000020
    Revocation Date: Aug 17 18:30:43 2005 GMT
Serial Number: 4CA4A3AA000000000021
    Revocation Date: Aug 17 18:30:43 2005 GMT
Serial Number: 1AA55C8E00000000002F
    Revocation Date: Sep  5 17:07:06 2005 GMT
Serial Number: 3F0845DD00000000003F
    Revocation Date: Sep  8 20:24:32 2005 GMT
Serial Number: 3F619B7E000000000042
    Revocation Date: Sep  8 21:40:48 2005 GMT
Serial Number: 6313C463000000000052
    Revocation Date: Sep 19 17:37:18 2005 GMT
Serial Number: 7C3861E3000000000060
    Revocation Date: Sep 20 17:52:56 2005 GMT
Serial Number: 7C6EE351000000000061
    Revocation Date: Sep 20 18:52:30 2005 GMT
Serial Number: 0A338EA1000000000074   <-- Revoked identity certificate
    Revocation Date: Nov 12 04:34:42 2005 GMT
Signature Algorithm: sha1WithRSAEncryption
    0b:cb:dd:43:0a:b8:62:1e:80:95:06:6f:4d:ab:0c:d8:8e:32:
    44:8e:a7:94:97:af:02:b9:a6:9c:14:fd:eb:90:cf:18:c9:96:
    29:bb:57:37:d9:1f:d5:bd:4e:9a:4b:18:2b:00:2f:d2:6e:c1:
    1a:9f:1a:49:b7:9c:58:24:d7:72
```

（注） 取り消されたデバイスのアイデンティティ証明書（シリアル番号は0A338EA1000000000074）が最後に表示されています。

PKI に関する追加情報

ここでは、PKI の実装に関する追加情報について説明します。

PKI の関連資料

関連項目	マニュアル タイトル
Cisco NX-OS ライセンス設定	『*Cisco NX-OS Licensing Guide*』
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』
VRF コンフィギュレーション	『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』

PKI の標準規格

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

PKI の機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 *19* : *PKI* の機能の履歴

機能名	リリース	機能情報
PKI	6.0(1)	Release 5.2 以降、変更はありません。
PKI	5.2(1)	Release 5.1 以降、変更はありません。
PKI	5.1(1)	Release 5.0 以降、変更はありません。
PKI	5.0(2)	リモートの cert-store および証明書マッピングのフィルタがサポートされるようになりました。

第 10 章

ユーザ アカウントおよび RBAC の設定

この章では、Cisco NX-OS デバイス上でユーザ アカウントおよびロールベース アクセス コントロール（RBAC）を設定する手順について説明します。

この章は、次の項で構成されています。

- 機能情報の確認，283 ページ
- ユーザ アカウントおよび RBAC の概要，284 ページ
- ユーザ アカウントおよび RBAC のライセンス要件，288 ページ
- ユーザ アカウントおよび RBAC の注意事項と制約事項，289 ページ
- ユーザ アカウントおよび RBAC のデフォルト設定，289 ページ
- パスワードの強度確認のイネーブル化，290 ページ
- ユーザ アカウントの設定，292 ページ
- ロールの設定，294 ページ
- ユーザ アカウントおよび RBAC 設定の確認，308 ページ
- ユーザ アカウントおよび RBAC の設定例，309 ページ
- ユーザ アカウントおよび RBAC に関する追加情報，311 ページ
- ユーザ アカウントおよび RBAC の機能の履歴，312 ページ

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

ユーザ アカウントおよび RBAC の概要

ユーザ アカウントの作成および管理を行い、Cisco NX-OS デバイス上で実行できる操作を制限するロールを割り当てることができます。RBAC は、ユーザが実行する必要のある管理操作の許可を制限するロールの割り当てのルールを定義することを可能にします。

ユーザ アカウント

最大 256 のユーザ アカウントを作成できます。デフォルトでは、明示的に期限を指定しないかぎり、ユーザ アカウントは無期限に有効です。expire オプションを使用すると、ユーザ アカウントをディセーブルにする日付を設定できます。

ユーザは、ユーザ アカウントを複数の VDC 上に所有できます。これらのユーザは、最初に 1 つの VDC に接続してから複数の VDC 間を移動できます。

次の語は予約済みであり、ユーザ設定に使用できません。bin、daemon、adm、lp、sync、shutdown、halt、mail、news、uucp、operator、games、gopher、ftp、nobody、nscd、mailnull、root、rpc、rpcuser、xfs、gdm、mtsuser、ftpuser、man、および sys。

（注） ユーザのパスワードは、設定ファイルでは表示されません。

注意 ユーザ名の先頭は英数字とする必要があります。ユーザ名には特殊文字 (+=._\-) のみを含めることができます。# 記号と ! 記号はサポートされていません。ユーザ名に許可されていない文字が含まれている場合、指定したユーザはログインできません。

強力なパスワードの特性

強力なパスワードは、次の特性を持ちます。

- 長さが 8 文字以上である
- 複数の連続する文字（「abcd」など）を含んでいない
- 複数の同じ文字の繰返し（「aaabbb」など）を含んでいない
- 辞書に載っている単語を含んでいない
- 正しい名前を含んでいない
- 大文字および小文字の両方が含まれている
- 数字が含まれている

強力なパスワードの例を次に示します。

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

（注） 出力可能なすべての ASCII 文字は、引用符で囲めば、パスワード文字列でサポートされます。

（注） Cisco NX-OS Release 7.1 以降では、NXOS の PSB 5.0 要件がサポートされます。SEC-PWD-DEFMIN：デフォルトの最小パスフレーズ長はゼロ以外、少なくとも 8 文字にする必要があります。ユーザ インターフェイスでは、パスワードでなくパスフレーズを表す PASSPHRASES という語が使用されている場合があります。

パスワードの強度確認をイネーブルにすると、パスワードが単純である場合（短く、簡単に解読されるパスワードなど）に、Cisco NX-OS ソフトウェアによってパスワード設定が拒否されます。サンプル設定のように、強力なパスワードを設定してください。パスワードは大文字と小文字が区別されます。

関連トピック

パスワードの強度確認のイネーブル化，（290 ページ）

ユーザ ロール

ユーザ ロールには、そのロールを割り当てられたユーザが実行できる操作を定義するルールが含まれています。各ユーザ ロールに複数のルールを含めることができ、各ユーザが複数のロールを持つことができます。たとえば、ロール 1 では設定操作の実行だけが許可されており、ロール 2 ではデバッグ操作の実行だけが許可されている場合、ロール 1 とロール 2 の両方に属するユーザは、設定操作とデバッグ操作を実行できます。また、特定の VLAN、仮想ルーティング/転送（VRF）インスタンス、およびインターフェイスへのアクセスも制限できます。

Cisco NX-OS ソフトウェアには、デフォルトで次の 4 つのユーザ ロールが用意されています。

- network-admin：NX-OS デバイス全体に対する読み取り/書き込みアクセスを実行できます（デフォルト DVC でだけ使用可能）。
- network-operator：NX-OS デバイス全体に対する読み取りアクセスを実行できます（デフォルト DVC でだけ使用可能）。
- vdc-admin：VDC に限定した読み取り/書き込みアクセス。
- vdc-operator：VDC に限定した読み取りアクセス。

（注） デフォルトのユーザ ロールは変更できません。

（注） network-operator ユーザおよび vdc-operator ユーザには、一部の **show** コマンドが表示されない場合があります。また、**show** コマンド以外のコマンドの中には（**telnet** など）、これらのユーザ ロールでも使用できるコマンドがあります。

VDC 内でカスタム ロールを作成できます。デフォルトでは、管理者のロールがないユーザ アカウントは、**show**、**exit**、**end**、および **configure terminal** を行うことができます。ルールを追加して、ユーザが機能を設定できるようにすることが可能です。
同じ物理デバイス上の VDC は、ユーザ ロールを共有しません。各 VDC には、独立したユーザ ロール データベースがあります。ロールは、VDC 内でルールと属性を割り当てることで設定します。

（注） 複数のロールに属するユーザは、そのロールで許可されるすべてのコマンドの組み合わせを実行できます。コマンドへのアクセス権は、コマンドへのアクセス拒否よりも優先されます。たとえば、ユーザが、コンフィギュレーション コマンドへのアクセスが拒否されたロール A を持っていたとします。しかし、同じユーザが RoleB も持ち、このロールではコンフィギュレーション コマンドにアクセスできるとします。この場合、このユーザはコンフィギュレーション コマンドにアクセスできます。

（注） network-admin ユーザのみ、チェックポイントやロールバックを RBAC ロールで実行できます。他のユーザは、そのロールの permit ルールにこれらのコマンドがあるにはありますが、それらのコマンドを実行しようとするとユーザ アクセスが拒否されます

ユーザ ロールのルール

ルールは、ロールの基本要素です。ルールは、そのロールがユーザにどの操作の実行を許可するかを定義します。ルールは次のパラメータで適用できます。

コマンド

正規表現で定義されたコマンドまたはコマンド グループ

機能

正規表現で定義されたコマンドまたはコマンド グループ

機能グループ

機能のデフォルト グループまたはユーザ定義グループ

OID

SNMP オブジェクト ID（OID）。

command、feature、および feature group の各パラメータにより、階層的な関係が作成されます。最も基本的な制御パラメータは command です。次の制御パラメータは feature です。これは、その機能にアソシエートされているすべてのコマンドを表します。最後の制御パラメータが、feature group です。機能グループは、関連する機能を組み合わせたものです。機能グループによりルールを簡単に管理できます。また、Cisco NX-OS ソフトウェアには、使用可能な機能グループ L3 があらかじめ定義されています。

ロールごとに最大 256 のルールを設定できます。ルールが適用される順序は、ユーザ指定のルール番号で決まります。ルールは降順で適用されます。たとえば、1 つのロールが 3 つのルールを持っている場合、ルール 3 がルール 2 よりも前に適用され、ルール 2 はルール 1 よりも前に適用されます。

ユーザ ロールの設定の配布

Cisco Fabric Services（CFS）を使用すると、Cisco NX-OS デバイスからネットワーク上の他の Cisco NX-OS デバイスにユーザ ロールの設定を配布できます。使用しているデバイスにおいて、ある機能に対して CFS 配布をイネーブルにすると、そのデバイスは CFS 領域に属します。この CFS 領域には、その機能に対して CFS 配布をイネーブルにしているネットワーク上の他のデバイスが含まれます。ユーザ ロール機能に対する CFS 配布はデフォルトではディセーブルになっています。

（注） 設定変更を配布する場合は、ユーザ ロールに対する CFS を各デバイスで明示的にイネーブルにする必要があります。

使用している Cisco NX-OS デバイスでユーザ ロールに対する CFS 配布をイネーブルにした後、最初に入力したユーザ ロール コンフィギュレーション コマンドによって、Cisco NX-OS ソフトウェアで次の処理が行われます。

- Cisco NX-OS デバイスで CFS セッションを作成します。
- ユーザ ロールに対する CFS がイネーブルにされている CFS 領域で、すべての Cisco NX-OS デバイスのユーザ ロール設定をロックします。
- ユーザ ロールの設定変更を Cisco NX-OS デバイスの一時バッファに保存します。

この変更は、CFS 領域にあるデバイスに対して配布するよう明示的にコミットするまで、Cisco NX-OS デバイスの一時バッファに存在します。変更をコミットすると、Cisco NX-OS ソフトウェアが次の処理を実行します。

- Cisco NX-OS デバイスの実行コンフィギュレーションに変更を適用します。
- 更新されたユーザ ロール設定を CFS 領域内にある他の Cisco NX-OS デバイスに配布します。
- CFS 領域内にある他のデバイスのユーザ ロール設定のロックを解除します。
- CFS セッションを終了します。

CFS の詳細については、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*』を参照してください。

RBAC のバーチャライゼーション サポート

network-admin および network-operator のロールを持つユーザは、デフォルト VDC からログインすると、すべての仮想デバイス コンテキスト（VDC）での操作ができ、**switchto vdc** コマンドを使用して、他の VDC にアクセスできます。他のすべてのユーザ ロールは、VDC にローカルです。ロールは VDC 間で共有されません。各 VDC には、独立したユーザ ロール データベースがあります。

次の注意事項と制約事項は、**switchto vdc** コマンドに適用されます。

- network-admin または network-operator のロールを持つユーザのみが **switchto vdc** コマンドを使用できます。他のユーザは使用することができません。
- ユーザは、別のロールに **switchto vdc** コマンドを使用する権限を付与できません。
- network-admin が **switchto vdc** コマンドを使用すると、このユーザは新規 VDC に対する vdc-admin になります。同様に network-operator が **switchto vdc** コマンドを使用すると、このユーザは新規 VDC に対する vdc-operator になります。**switchto vdc** コマンドを入力した後は、ユーザに関連付けられている他のロールはすべて無効になります。
- network-admin または network-operator が switchto vdc コマンドを使用した後は、このユーザはこのコマンドを使用して別の VDC に切り替えることはできません。唯一のオプションとして、元の VDC に戻るための **switchback** コマンドを使用できます。

Cisco NX-OS Release 5.2 以降では、ストレージ VDC の RBAC を設定できます。ストレージ VDC の RBAC は Cisco Nexus 7000 シリーズ スイッチ用の RBAC であり、Cisco MDS 9500 シリーズ スイッチのものとは異なることに注意してください。

（注） VDC の詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

ユーザ アカウントおよび RBAC のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	ユーザ アカウントおよび RBAC にはライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

ユーザ アカウントおよび RBAC の注意事項と制約事項

ユーザ アカウントおよび RBAC に関する注意事項と制約事項は次のとおりです。

- 1 つの VDC には最大 64 のユーザ定義のユーザ ロールを作成できるほか、デフォルト VDC には 4 つのデフォルトのユーザ ロール、デフォルト以外の VDC には 2 つのデフォルトのユーザ ロールを作成できます。
- ユーザ ロールには最大 256 個の規則を追加できます。
- 1 つの VDC には最大 64 のユーザ定義の機能グループを追加できるほか、デフォルトの機能グループ L3 を追加できます。
- 1 つの VDC には最大 256 のユーザを設定できます。
- 1 つのユーザ アカウントに最大 64 個のユーザ ロールを割り当てられます。
- ローカルの Cisco NX-OS デバイス上に設定されているユーザ アカウントが、AAA サーバ上のリモート ユーザ アカウントと同じ名前の場合、Cisco NX-OS ソフトウェアは、AAA サーバ上に設定されているユーザ ロールではなく、ローカル ユーザ アカウントのユーザ ロールをリモート ユーザに適用します。
- デフォルトの admin と SNMP ユーザ アカウントは削除できません。
- デフォルトのユーザ ロールを、デフォルトの admin ユーザ アカウントから削除することはできません。
- network-operator および vdc-operator ロールは、**show running-config** および **show startup-config** コマンドを実行できません。
- RBAC は、同じ VLAN 内の F1 シリーズ モジュール ポートと M1 シリーズ モジュール ポートの間のトラフィックではサポートされていません。
- Cisco NX-OS リリース 6.0 以降では、RBAC は F2 シリーズ モジュールでサポートされます。

（注） Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

ユーザ アカウントおよび RBAC のデフォルト設定

次の表に、ユーザ アカウントおよび RBAC パラメータのデフォルト設定を示します。

表 *20*：デフォルトのユーザ アカウントおよび *RBAC* パラメータ

パラメータ	デフォルト
ユーザ アカウント パスワード	未定義
ユーザ アカウントの有効期限	なし。
デフォルト VDC のユーザ アカウント ロール	作成ユーザが network-admin のロールを持つ場合は network-operator、または vdc-admin のロールを持つ場合は vdc-operator
VDC 以外のユーザ アカウント ロール	作成ユーザが vdc-admin を持つ場合は vdc-operator
デフォルト VDC のデフォルト ユーザ ロール	network-operator
デフォルト以外の VDC のデフォルト ユーザ ロール	vdc-operator
インターフェイス ポリシー	すべてのインターフェイスがアクセス可能
VLAN ポリシー	すべての VLAN がアクセス可能
VRF ポリシー	すべての VRF にアクセス可能
機能グループ	L3

パスワードの強度確認のイネーブル化

ユーザ アカウントに対して弱いパスワードを設定しないように、パスワードの強度確認機能をイネーブルにすることができます。

（注） パスワード強度確認をイネーブルにしても、Cisco NX-OS ソフトウェアでは、既存パスワードの強度確認は行われません。

手順の概要

1. **configure terminal**
2. **password strength-check**
3. **exit**
4. （任意） **show password strength-check**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**password strength-check** 例： `switch(config)# password strength-check`	パスワードの強度確認をイネーブルにします。デフォルトではイネーブルになっています。 パスワードの強度確認をディセーブルにするには、このコマンドの **no** 形式を使用します。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 4	**show password strength-check** 例： `switch# show password strength-check`	（任意） パスワードの強度確認の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

強力なパスワードの特性，（284 ページ）

ユーザ アカウントの設定

Cisco NX-OS デバイス上には最大 256 のユーザ アカウントを作成できます。ユーザ アカウントは、次の属性を持ちます。

- ユーザ名
- パスワード
- 失効日
- ユーザ ロール

パスワードはクリア テキストか暗号化された形式で入力できます。Cisco NX-OS では、実行コンフィギュレーションに保存する前にクリア テキストのパスワードを暗号化します。暗号化された形式のパスワードは、これ以上の暗号化を行わずに実行コンフィギュレーションに保存されます。

ユーザ アカウントは、最大 64 個のユーザ ロールを持つことができます。コマンドライン インターフェイス（CLI）の状況依存ヘルプ ユーティリティを使用して、利用できるコマンドを確認できます。

（注） ユーザ アカウントの属性に加えられた変更は、そのユーザがログインして新しいセッションを作成するまで有効になりません。

手順の概要

1. **configure terminal**
2. （任意） **show role**
3. **username***user-id* [**password** [**0** | **5**] *password*] [**expire***date*] [**role***role-name*]
4. **exit**
5. （任意） **show user-account**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**show role** 例： `switch(config)# show role`	（任意） 使用可能なユーザ ロールを表示します。必要に応じて、他のユーザ ロールを設定できます。
ステップ 3	**username***user-id* [**password** [**0** | **5**] *password*] [**expire***date*] [**role***role-name*] 例： `switch(config)# username NewUser password 4Ty18Rnt`	ユーザ アカウントを設定します。*user-id* 引数は、最大 28 文字の英数字で、大文字と小文字が区別されます。指定できる文字は、A ～ Z の英大文字、a ～ z の英小文字、0 ～ 9 の数字、ハイフン（-）、ピリオド（.）、アンダースコア（_）、プラス符号（+）、および等号（=）です。アット マーク（@）はリモート ユーザ名では使用できますが、ローカル ユーザ名では使用できません。 デフォルト パスワードは定義されていません。オプションの **0** は、パスワードがクリア テキストであることを、**5** は、パスワードが暗号化されていることを意味します。デフォルトは **0**（クリア テキスト）です。 （注） パスワードを指定しないと、ユーザは Cisco NX-OS デバイスにログインできない場合があります。 （注） 暗号化パスワード オプションを使用してユーザ アカウントを作成する場合、対応する SNMP ユーザは作成されません。 **expire***date* オプションの形式は、YYYY-MM-DD です。デフォルトでは、失効日はありません。 ユーザ アカウントは、最大 64 個のユーザ ロールを持つことができます。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 5	**show user-account** 例： `switch# show user-account`	（任意） ロール設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

ロールの設定，（294 ページ）

ユーザ ロールおよびルールの作成, （295 ページ）

ロールの設定

ここでは、ユーザ ロールの設定方法について説明します。

ユーザ ロール設定の配布のイネーブル化

ユーザ ロールの設定をネットワーク上の他の Cisco NX-OS デバイスに配布するには、最初にユーザ ロールについての CFS の配布をイネーブルにする必要があります。

手順の概要

1. **configure terminal**
2. **role distribute**
3. **exit**
4. （任意） **show role session status**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**role distribute** 例： `switch(config)# role distribute`	ユーザ ロール設定の配布をイネーブルにします。デフォルトではディセーブルになっています。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show role session status** 例： `switch# show role session status`	（任意） ユーザ ロールの配布のステータス情報を表示します。

	コマンドまたはアクション	目的
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ユーザ ロールおよびルールの作成

VDC には最大 64 のユーザ ロールを設定できます。各ユーザ ロールが、最大 256 個のルールを持つことができます。ユーザ ロールを複数のユーザ アカウントに割り当てることができます。

指定したルール番号は、ルールが適用される順番を決定します。ルールは降順で適用されます。たとえば、1 つのロールが 3 つのルールを持っている場合、ルール 3 がルール 2 よりも前に適用され、ルール 2 はルール 1 よりも前に適用されます。

（注） ユーザ ロールに設定された読み取り/書き込みルールに関係なく、一部のコマンドは、あらかじめ定義された network-admin および vdc-admin のロールだけを通じて実行できます。ユーザ ロールの詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

（注） ユーザ アカウントのユーザ ロールまたは権限を変更した場合、変更後のロールは次回のログイン以降で有効になります。

はじめる前に

ユーザ ロール設定を配布する場合は、設定を配布する対象のすべての Cisco NX-OS デバイスでユーザ ロール設定の配布をイネーブルにします。

手順の概要

1. **configure terminal**
2. **role name***role-name*
3. **rule***number* {**deny** | **permit**} **command***command-string*
4. **rule***number* {**deny** | **permit**} {**read** | **read-write**}
5. **rule***number* {**deny** | **permit**} {**read** | **read-write**} **feature***feature-name*
6. **rule***number* {**deny** | **permit**} {**read** | **read-write**} **feature-group***group-name*
7. **rule***number* {**deny** | **permit**} {**read** | **read-write**} **oid***snmp_oid_name*
8. （任意） **description***text*
9. **exit**
10. （任意） **show role**
11. （任意） **show role**{**pending**| **pending-diff**}
12. （任意） **role commit**
13. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**role name***role-name*
	
	例：
	`switch(config)# role name UserA`
	`switch(config-role)#`
		ユーザ ロールを指定し、ロール コンフィギュレーション モードを開始します。*role-name* 引数は、最大 16 文字の長さの英数字のストリングで、大文字小文字が区別されます。

ステップ 3	**rule***number* {**deny**	**permit**} **command***command-string* 例： `switch(config-role)# rule 1 deny command clear users`	コマンド規則を設定します。 *command-string* には、スペースおよび正規表現を含めることができます。たとえば、interface ethernet にはすべてのイーサネット インターフェイスが含まれます。 必要な規則の数だけこのコマンドを繰り返します。
ステップ 4	**rule***number* {**deny**	**permit**} {**read**	**read-write**} 例： `switch(config-role)# rule 2 deny read-write`	すべての操作の読み取り専用ルールまたは読み取り/書き込みルールを設定します。

	コマンドまたはアクション	目的
ステップ 5	**rule***number* {**deny** | **permit**} {**read** | **read-write**} **feature***feature-name* 例： `switch(config-role)# rule 3 permit read feature router-bgp`	機能に対して、読み取り専用規則か読み取りと書き込みの規則かを設定します。 **show role feature** コマンドを使用すれば、機能のリストが表示されます。 必要な規則の数だけこのコマンドを繰り返します。
ステップ 6	**rule***number* {**deny** | **permit**} {**read** | **read-write**} **feature-group***group-name* 例： `switch(config-role)# rule 4 deny read-write feature-group L3`	機能グループに対して、読み取り専用規則か読み取りと書き込みの規則かを設定します。 **show role feature-group** コマンドを使用すれば、機能グループのリストが表示されます。 必要な規則の数だけこのコマンドを繰り返します。
ステップ 7	**rule***number* {**deny** | **permit**} {**read** | **read-write**} **oid***snmp_oid_name* 例： `switch(config-role)# rule 5 deny read-write oid 1.3.6.1.2.1.1.9`	SNMP オブジェクト ID（OID）の読み取り専用または読み書きルールを設定します。OID には最大 32 の要素を入力することができます。このコマンドは、SNMP ベースのパフォーマンス モニタリング ツールがデバイスをポーリングするために使用できますが、IP ルーティング テーブル、ARP キャッシュ、MAC アドレス テーブル、特定の MIB などのシステムの集中的な拠点へのアクセスは制限されます。 （注） 一番深層の OID はスカラ レベルまたはテーブル ルート レベルにすることができます。 必要な規則の数だけこのコマンドを繰り返します。
ステップ 8	**description***text* 例： `switch(config-role)# description This role does not allow users to use clear commands`	（任意） ロールの説明を設定します。説明にはスペースも含めることができます。

ステップ 9	**exit**
	
	例：
	`switch(config-role)# exit`
	`switch(config)#`
		ロール コンフィギュレーション モードを終了します。

ステップ 10	**show role** 例： `switch(config)# show role`	（任意） ユーザ ロールの設定を表示します。
ステップ 11	**show role**{**pending**| **pending-diff**} 例： `switch(config)# show role pending`	（任意） 配布するために保留状態になっているユーザ ロール設定を表示します。

	コマンドまたはアクション	目的
ステップ 12	**role commit** 例： `switch(config)# role commit`	（任意） CFS によるユーザ ロール設定の配布機能をイネーブルにしている場合は、一時データベース内にあるユーザ ロールの設定変更を実行コンフィギュレーションに適用して、ユーザ ロール設定を他の Cisco NX-OS デバイスに配布します。
ステップ 13	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

ユーザ ロール設定の配布へのコミット，（305 ページ）

機能グループの作成

カスタム機能グループを作成して、Cisco NX-OS ソフトウェアが提供するデフォルトの機能リストに追加できます。これらの機能グループは 1 つまたは複数の機能を含んでいます。VDC には最大 64 の機能グループを設定できます。

（注） デフォルト機能グループ L3 を変更することはできません。

はじめる前に

ユーザ ロール設定を配布する場合は、設定を配布する対象のすべての Cisco NX-OS デバイスでユーザ ロール設定の配布をイネーブルにします。

手順の概要

1. **configure terminal**
2. **role feature-group name***group-name*
3. **feature***feature-name*
4. **exit**
5. （任意） **show role feature-group**
6. （任意） **show role {pending | pending-diff}**
7. （任意） **role commit**
8. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**role feature-group name***group-name*
	
	例：
	`switch(config)# role feature-group name GroupA`
	`switch(config-role-featuregrp)#`
		ユーザ ロール機能グループを指定して、ロール機能グループ コンフィギュレーション モードを開始します。
		
		group-name 引数は、最大 32 文字の長さの英数字のストリングで、大文字小文字が区別されます。

ステップ 3	**feature***feature-name* 例： `switch(config-role-featuregrp)# feature vdc`	機能グループの機能を指定します。 必要な機能の数だけこのコマンドを繰り返します。 （注） 機能の一覧を表示する場合は、**show role component** コマンドを使用します。

ステップ 4	**exit**
	
	例：
	`switch(config-role-featuregrp)# exit`
	`switch(config)#`
		ロール機能グループ コンフィギュレーション モードを終了します。

ステップ 5	**show role feature-group** 例： `switch(config)# show role feature-group`	（任意） ロール機能グループ設定を表示します。
ステップ 6	**show role** {**pending** | **pending-diff**} 例： `switch(config)# show role pending`	（任意） 配布するために保留状態になっているユーザ ロール設定を表示します。
ステップ 7	**role commit** 例： `switch(config)# role commit`	（任意） CFS によるユーザ ロール設定の配布機能をイネーブルにしている場合は、一時データベース内にあるユーザ ロールの設定変更を実行コンフィギュレーションに適用して、ユーザ ロール設定を他の Cisco NX-OS デバイスに配布します。
ステップ 8	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

ユーザ ロール設定の配布へのコミット，（305 ページ）

ユーザ ロール インターフェイス ポリシーの変更

ユーザ ロール インターフェイス ポリシーを変更することで、ユーザがアクセスできるインターフェイスを制限できます。デフォルトでは、ユーザ ロールは VDC のすべてのインターフェイスにアクセスできます。

はじめる前に

1 つまたは複数のユーザ ロールを作成します。

ユーザ ロール設定を配布する場合は、設定を配布する対象のすべての Cisco NX-OS デバイスでユーザ ロール設定の配布をイネーブルにします。

手順の概要

1. **configure terminal**
2. **role name** *role-name*
3. **interface policy deny**
4. **permit interface***interface-list*
5. **exit**
6. （任意） **show role**
7. （任意） **show role** {**pending** | **pending-diff**}
8. （任意） **role commit**
9. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**role name** *role-name*
	
	例：
	`switch(config)# role name UserA`
	`switch(config-role)#`
		ユーザ ロールを指定し、ロール コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 3	**interface policy deny**
	
	例：
	`switch(config-role)# interface policy deny`
	`switch(config-role-interface)#`
		ロール インターフェイス ポリシー コンフィギュレーション モードを開始します。

ステップ 4	**permit interface***interface-list* 例： `switch(config-role-interface)# permit interface ethernet 2/1-4`	ロールがアクセスできるインターフェイスのリストを指定します。 必要なインターフェイスの数だけこのコマンドを繰り返します。

ステップ 5	**exit**
	
	例：
	`switch(config-role-interface)# exit`
	`switch(config-role)#`
		ロール インターフェイス ポリシー コンフィギュレーション モードを終了します。

ステップ 6	**show role** 例： `switch(config-role)# show role`	（任意） ロール設定を表示します。
ステップ 7	**show role {pending | pending-diff}** 例： `switch(config-role)# show role pending`	（任意） 配布するために保留状態になっているユーザ ロール設定を表示します。
ステップ 8	**role commit** 例： `switch(config-role)# role commit`	（任意） CFS によるユーザ ロール設定の配布機能をイネーブルにしている場合は、一時データベース内にあるユーザ ロールの設定変更を実行コンフィギュレーションに適用して、ユーザ ロール設定を他の Cisco NX-OS デバイスに配布します。
ステップ 9	**copy running-config startup-config** 例： `switch(config-role)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

ユーザ ロールおよびルールの作成，（295 ページ）
ユーザ ロール設定の配布へのコミット，（305 ページ）

ユーザ ロール VLAN ポリシーの変更

ユーザ ロール VLAN ポリシーを変更することで、ユーザがアクセスできる VLAN を制限できます。デフォルトでは、ユーザ ロールは VDC のすべての VLAN にアクセスできます。

はじめる前に

1 つまたは複数のユーザ ロールを作成します。

ユーザ ロール設定を配布する場合は、設定を配布する対象のすべての Cisco NX-OS デバイスでユーザ ロール設定の配布をイネーブルにします。

手順の概要

1. **configure terminal**
2. **role name***role-name*
3. **vlan policy deny**
4. **permit vlan***vlan-list*
5. **exit**
6. （任意） **show role**
7. （任意） **show role** {**pending** | **pending-diff**}
8. （任意） **role commit**
9. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**role name***role-name*
	
	例：
	`switch(config)# role name UserA`
	`switch(config-role)#`
		ユーザ ロールを指定し、ロール コンフィギュレーション モードを開始します。

ステップ 3	**vlan policy deny**
	
	例：
	`switch(config-role)# vlan policy deny`
	`switch(config-role-vlan)#`
		ロール VLAN ポリシー コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**permit vlan***vlan-list* 例： `switch(config-role-vlan)# permit vlan 1-4`	ロールがアクセスできる VLAN の範囲を指定します。 必要な VLAN の数だけこのコマンドを繰り返します。

ステップ 5	**exit**
	
	例：
	`switch(config-role-vlan)# exit`
	`switch(config-role)#`
		ロール VLAN ポリシー コンフィギュレーション モードを終了します。

ステップ 6	**show role** 例： `switch(config)# show role`	（任意） ロール設定を表示します。
ステップ 7	**show role {pending | pending-diff}** 例： `switch(config-role)# show role pending`	（任意） 配布するために保留状態になっているユーザ ロール設定を表示します。
ステップ 8	**role commit** 例： `switch(config-role)# role commit`	（任意） CFS によるユーザ ロール設定の配布機能をイネーブルにしている場合は、一時データベース内にあるユーザ ロールの設定変更を実行コンフィギュレーションに適用して、ユーザ ロール設定を他の Cisco NX-OS デバイスに配布します。
ステップ 9	**copy running-config startup-config** 例： `switch(config-role)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

ユーザ ロールおよびルールの作成，（295 ページ）
ユーザ ロール設定の配布へのコミット，（305 ページ）

ユーザ ロールの VRF ポリシーの変更

ユーザ ロールの VRF ポリシーを変更して、ユーザがアクセスできる VRF を制限できます。デフォルトでは、ユーザ ロールは VDC のすべての VRF にアクセスできます。

はじめる前に

1 つまたは複数のユーザ ロールを作成します。

ユーザ ロール設定を配布する場合は、設定を配布する対象のすべての Cisco NX-OS デバイスでユーザ ロール設定の配布をイネーブルにします。

手順の概要

1. **configure terminal**
2. **role name** *role-name*
3. **vrf policy deny**
4. **permit vrf***vrf-name*
5. **exit**
6. （任意） **show role**
7. （任意） **show role** {**pending** | **pending-diff**}
8. （任意） **role commit**
9. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**role name** *role-name*
	
	例：
	`switch(config)# role name UserA`
	`switch(config-role)#`
		ユーザ ロールを指定し、ロール コンフィギュレーション モードを開始します。

ステップ 3	**vrf policy deny**
	
	例：
	`switch(config-role)# vrf policy deny`
	`switch(config-role-vrf)#`
		ロール VRF ポリシー コンフィギュレーション モードを開始します。

ステップ 4	**permit vrf***vrf-name* 例： `switch(config-role-vrf)# permit vrf vrf1`	ロールがアクセスできる VRF を指定します。 必要な VRF の数だけこのコマンドを繰り返します。

ステップ 5	**exit**
	
	例：
	`switch(config-role-vrf)# exit`
	`switch(config-role)#`
		ロール VRF ポリシー コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 6	**show role** 例： `switch(config-role)# show role`	（任意） ロール設定を表示します。
ステップ 7	**show role** {**pending** | **pending-diff**} 例： `switch(config-role)# show role pending`	（任意） 配布するために保留状態になっているユーザ ロール設定を表示します。
ステップ 8	**role commit** 例： `switch(config-role)# role commit`	（任意） CFS によるユーザ ロール設定の配布機能をイネーブルにしている場合は、一時データベース内にあるユーザ ロールの設定変更を実行コンフィギュレーションに適用して、ユーザ ロール設定を他の Cisco NX-OS デバイスに配布します。
ステップ 9	**copy running-config startup-config** 例： `switch(config-role)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

ユーザ ロールおよびルールの作成，（295 ページ）
ユーザ ロール設定の配布へのコミット，（305 ページ）

ユーザ ロール設定の配布へのコミット

一時バッファに保存されているユーザ ロールのグローバル設定やサーバ設定を、ファブリック内のすべてのスイッチ（元のスイッチを含む）の実行コンフィギュレーションに適用できます。

はじめる前に

Cisco NX-OS デバイス上でユーザ ロール設定の配布をイネーブルにします。

手順の概要

1. **configure terminal**
2. （任意） **show role** {**pending** | **pending-diff**}
3. （任意） **role commit**
4. **exit**
5. （任意） **show role session status**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**show role** {**pending**	**pending-diff**} 例： `switch(config)# show role pending`	（任意） 配布するために保留状態になっているユーザ ロール設定を表示します。
ステップ 3	**role commit** 例： `switch(config)# role commit`	（任意） CFS によるユーザ ロール設定の配布機能をイネーブルにしている場合は、一時データベース内にあるユーザ ロールの設定変更を実行コンフィギュレーションに適用して、ユーザ ロール設定を他の Cisco NX-OS デバイスに配布します。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 5	**show role session status** 例： `switch# show role session status`	（任意） ユーザ ロールについての CSF セッションのステータスを表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） CFS がイネーブルになっているネットワーク内のすべての Cisco NX-OS デバイスのスタートアップ コンフィギュレーションに実行コンフィギュレーションを適用します。

関連トピック

ユーザ ロールの設定の配布，（287 ページ）

ユーザ ロールの配布セッションの廃棄

ユーザ ロールの変更の一時データベースを廃棄して、CFS 配布セッションを終了します。

はじめる前に

Cisco NX-OS デバイス上でユーザ ロール設定の配布をイネーブルにします。

手順の概要

1. **configure terminal**
2. （任意） **show role {pending | pending-diff}**
3. **role abort**
4. **exit**
5. （任意） **show role session status**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**show role {pending | pending-diff}** 例： `switch(config)# show role pending`	（任意） 配布するために保留状態になっているユーザ ロール設定を表示します。
ステップ 3	**role abort** 例： `switch(config)# role abort`	一時ストレージにあるユーザ ロール設定を廃棄して、セッションを終了します。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 5	**show role session status** 例： `switch# show role session status`	（任意） ユーザ ロールについての CSF セッションのステータスを表示します。

関連トピック

ユーザ ロール設定の配布へのコミット，（305 ページ）
ユーザ ロールの設定の配布，（287 ページ）

ユーザ ロールの配布セッションのクリア

実行中の Cisco Fabric Services の配布セッション（存在する場合）をクリアして、ユーザ ロール機能のためのファブリックのロックを解除します。

Cisco NX-OS デバイス上でユーザ ロール設定の配布をイネーブルにします。

手順の概要

1. **clear role session**
2. （任意） **show role session status**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**clear role session** 例： `switch# clear role session`	セッションをクリアして、ファブリックのロックを解除します。
ステップ 2	**show role session status** 例： `switch# show role session status`	（任意） ユーザ ロールについての CSF セッションのステータスを表示します。

関連トピック

ユーザ ロール設定の配布へのコミット，（305 ページ）
ユーザ ロールの設定の配布，（287 ページ）

ユーザ アカウントおよび RBAC 設定の確認

ユーザ アカウントおよび RBAC 設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show cli syntax roles network-admin	network-admin ロールが使用できて vdc-admin ロールが使用できないコマンドの構文を表示します。
show cli syntax roles network-operator	network-operator ロールが使用できて vdc-operator ロールが使用できないコマンドの構文を表示します。
show role	ユーザ ロールの設定を表示します。
show role feature	機能リストを表示します。
show role feature-group	機能グループの設定を表示します。
show startup-config security	スタートアップ コンフィギュレーションのユーザ アカウント設定を表示します。
show running-config security [**all**]	実行コンフィギュレーションのユーザ アカウント設定を表示します。**all** キーワードを指定すると、ユーザ アカウントのデフォルト値が表示されます。
show user-account	ユーザ アカウント情報を表示します。

これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

ユーザ アカウントおよび RBAC の設定例

次に、ユーザ ロールを設定する例を示します。

```
role name User-role-A
  rule 3 permit read-write feature l2nac
  rule 2 permit read-write feature dot1x
  rule 1 deny command clear *
```

次に、HSRP をイネーブルにして表示し、GLBP を表示するようにインターフェイスを設定できるユーザ ロールを作成する例を示します。

```
role name iftest
   rule 1 permit command config t; interface *; hsrp *
   rule 2 permit read-write feature hsrp
   rule 3 permit read feature glbp
```

上の例では、ルール 1 はインターフェイス上の HSRP の設定を許可し、ルール 2 は **config hsrp** コマンドの設定と HSRP に対する EXEC レベルの **show** および **debug** コマンドのイネーブル化を許可し、さらにルール 3 は EXEC レベルの **show** および **debug glbp** コマンドのイネーブル化を許可します。

次に、特定のインターフェイスだけを設定できるユーザ ロールを設定する例を示します。

```
role name Int_Eth2-3_only
  rule 1 permit command configure terminal; interface *
  interface policy deny
    permit interface Ethernet2/3
```

次に、ユーザ ロール機能グループを設定する例を示します。

```
role feature-group name Security-features
  feature radius
  feature tacacs
  feature dot1x
  feature aaa
  feature l2nac
  feature acl
  feature access-list
```

次に、ユーザ アカウントを設定する例を示します。

```
username user1 password A1s2D4f5 role User-role-A
```

次に、アクセスを OID サブツリーの一部に制限するための OID ルールを追加する例を示します。

```
role name User1
  rule 1 permit read feature snmp
  rule 2 deny read oid 1.3.6.1.2.1.1.9
show role name User1

Role: User1
  Description: new role
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ----------------------------------------------------------------------
  2       deny    read        oid                 1.3.6.1.2.1.1.9
  1       permit  read        feature             snmp
```

次に、指定された OID サブツリーへの書き込み権限を許可する例を示します。

```
role name User1
rule 3 permit read-write oid 1.3.6.1.2.1.1.5
show role name User1

Role: User1
  Description: new role
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
```

```
-------------------------------------------------------------------
3       permit  read-write  oid                 1.3.6.1.2.1.1.5
2       deny    read        oid                 1.3.6.1.2.1.1.9
1       permit  read        feature             snmp
```

ユーザ アカウントおよび RBAC に関する追加情報

ここでは、ユーザ アカウントおよび RBAC の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS ライセンス設定	『*Cisco NX-OS Licensing Guide*』
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』
VRF コンフィギュレーション	『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

MIB	MIB のリンク
• CISCO-COMMON-MGMT-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

ユーザ アカウントおよび RBAC の関連資料

関連項目	マニュアル タイトル
Cisco NX-OS ライセンス設定	『*Cisco NX-OS Licensing Guide*』
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』
VRF コンフィギュレーション	『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』

ユーザ アカウントおよび RBAC の標準規格

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

ユーザ アカウントと RBAC の MIB

MIB	MIB のリンク
• CISCO-COMMON-MGMT-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

ユーザ アカウントおよび RBAC の機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 *21*：ユーザ アカウントおよび *RBAC* の機能の履歴

機能名	リリース	機能情報
RBAC	6.0(1)	F2 シリーズ モジュールのサポートが追加されました。
ユーザアカウントおよびRBAC	6.0(1)	SNMP OID に読み取り専用ルールまたは読み取り/書き込みルールを設定する機能が追加されました。
ユーザアカウントおよびRBAC	5.2(1)	Release 5.1 以降、変更はありません。
ユーザアカウントおよびRBAC	5.2(1)	Cisco Nexus 3000 シリーズ スイッチのサポートが追加されました。
ユーザ ロール	5.1(1)	network-admin ロールおよび network-operator ロールが使用できるコマンドの構文を表示する機能が追加されました。
ユーザアカウントおよびRBAC	5.1(1)	Release 5.0 以降、変更はありません。
ユーザアカウントおよびRBAC	5.0(2)	リモートユーザ名でアットマーク記号（@）をサポートする機能が追加されました。
ユーザアカウントおよびRBAC	5.0(2)	Release 4.2 以降、変更はありません。
ユーザ名	4.2(1)	ユーザ名に指定できる文字は、a ～ z の英小文字、A ～ Z の英大文字、0 ～ 9 の数字、プラス符号（+）、ハイフン（-）、等号（=）、アンダースコア（_）、およびピリオド（.）に制限されています。

第 11 章

802.1X の設定

この章では、Cisco NX-OS デバイス上で IEEE 802.1X ポートベースの認証を設定する手順について説明します。

この章は、次の項で構成されています。

- 機能情報の確認，315 ページ
- 802.1X の概要，316 ページ
- 802.1X のライセンス要件，323 ページ
- 802.1X の前提条件，324 ページ
- 802.1X の注意事項と制約事項，324 ページ
- 802.1X のデフォルト設定，325 ページ
- 802.1X の設定，327 ページ
- 802.1X 設定の確認，357 ページ
- 802.1X のモニタリング，358 ページ
- 802.1X の設定例，358 ページ
- 802.1X に関する追加情報，359 ページ
- 802.1X の機能の履歴，360 ページ

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

802.1X の概要

802.1X では、クライアント サーバ ベースのアクセス コントロールと認証プロトコルを定義し、許可されていないクライアントが公にアクセス可能なポートを経由してLANに接続するのを規制します。認証サーバは、Cisco NX-OS デバイスのポートに接続されるクライアントを個々に認証します。

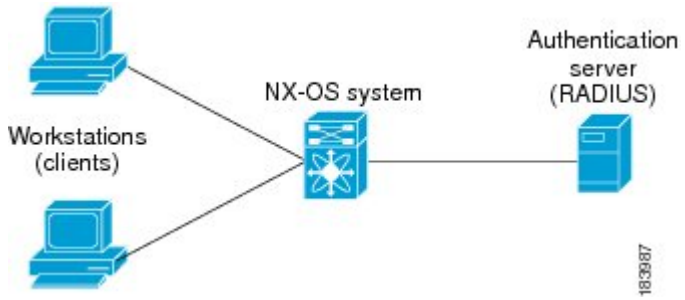
802.1Xアクセス コントロールでは、クライアントが認証されるまで、そのクライアントが接続しているポート経由では Extensible Authentication Protocol over LAN（EAPOL）トラフィックしか許可されません。認証に成功すると、通常のトラフィックはポートを通過できるようになります。

デバイスのロール

802.1X ポート ベースの認証では、ネットワーク上のデバイスにそれぞれ特定のロールがあります。

次の図は、802.1X のデバイスのロールを示しています。

図 *5*：*802.1X* デバイスのロール



特定のロールは次のとおりです。

サプリカント

LAN および Cisco NX-OS デバイス サービスへのアクセスを要求し、Cisco NX-OS デバイスからの要求に応答するクライアント デバイスです。ワークステーションでは、Microsoft Windows XP が動作するデバイスで提供されるような、802.1X 準拠のクライアント ソフトウェアが稼働している必要があります。

（注） Windows XP のネットワーク接続および Cisco 802.1X ポートベース認証の問題に関しては、次の URL にある Microsoft サポート技術情報の記事を参照してください。http://support.microsoft.com/support/kb/articles/Q303/5/97.ASP

認証サーバ

サプリカントの実際の認証を行います。認証サーバはサプリカントの識別情報を確認し、LAN および Cisco NX-OS デバイスのサービスへのアクセスをサプリカントに許可すべきかどうかを Cisco NX-OS デバイスに通知します。Cisco NX-OS デバイスはプロキシとして動作するので、認証サービスはサプリカントに対しては透過的に行われます。認証サーバとして、拡張認証プロトコル（EAP）拡張機能を備えた Remote Authentication Dial-In User Service（RADIUS）セキュリティデバイスだけがサポートされています。この認証サーバは、Cisco Secure Access Control Server バージョン 3.0 で使用可能です。RADIUS はサプリカント サーバ モデルを使用し、RADIUS サーバと 1 つまたは複数の RADIUS クライアントとの間でセキュア認証情報を交換します。

オーセンティケータ

サプリカントの認証ステータスに基づいて、ネットワークへの物理アクセスを制御します。オーセンティケータは、サプリカントと認証サーバとの仲介デバイス（プロキシ）として動作し、サプリカントから識別情報を要求し、得られた識別情報を認証サーバに確認し、サプリカントに応答をリレーします。オーセンティケータには、EAP フレームのカプセル化/カプセル化解除、および認証サーバとの対話を処理する、RADIUS クライアントが含まれています。

オーセンティケータが EAPOL フレームを受信して認証サーバにリレーする際は、イーサネット ヘッダーを取り除き、残りの EAP フレームを RADIUS 形式にカプセル化します。このカプセル化のプロセスでは EAP フレームの変更または確認が行われないため、認証サーバはネイティブ フレーム フォーマットの EAP をサポートする必要があります。オーセンティケータは認証サーバからフレームを受信すると、サーバのフレーム ヘッダーを削除し、残りの EAP フレームをイーサネット用にカプセル化してサプリカントに送信します。

（注） Cisco NX-OS デバイスがなれるのは、802.1X オーセンティケータだけです。

認証の開始およびメッセージ交換

オーセンティケータ（Cisco NX-OS デバイス）とサプリカント（クライアント）のどちらも認証を開始できます。ポート上で認証をイネーブルにした場合、オーセンティケータはポートのリンク ステートがダウンからアップに移行した時点で、認証を開始する必要があります。続いて、オーセンティケータは EAP-Request/Identity フレームをサプリカントに送信して識別情報を要求します（通常、オーセンティケータは 1 つまたは複数の識別情報の要求のあとに、最初の Identity/Request フレームを送信します）。サプリカントはフレームを受信すると、EAP-Response/Identity フレームで応答します。

サプリカントがブートアップ時にオーセンティケータから EAP-Request/Identity フレームを受信しなかった場合、サプリカントは EAPOL 開始フレームを送信することにより認証を開始することができます。この開始フレームにより、オーセンティケータはサプリカントの識別情報を要求します。

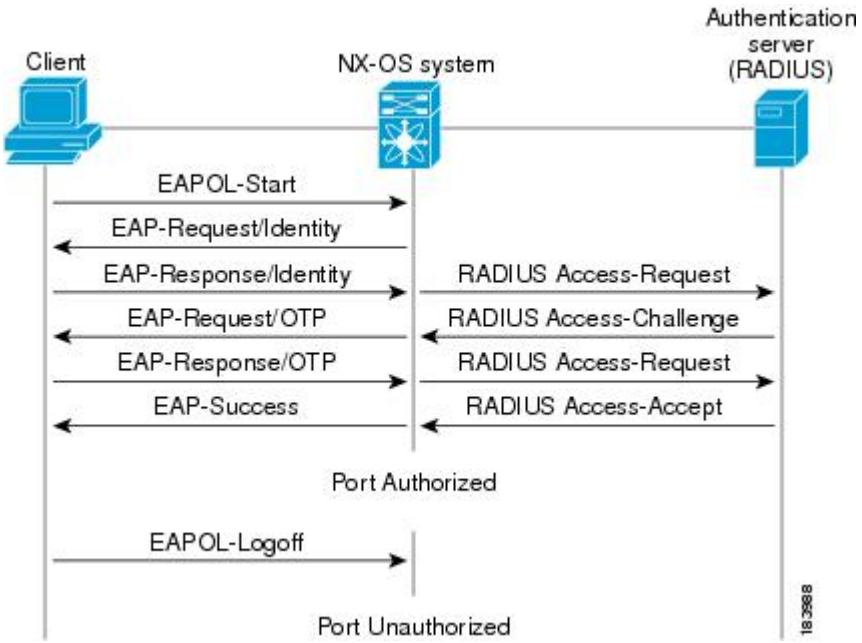
（注） ネットワーク アクセス デバイスで 802.1X がイネーブルになっていない場合、またはサポートされていない場合、Cisco NX-OS デバイスはサプリカントからの EAPOL フレームをすべてドロップします。サプリカントが、認証の開始を 3 回試みても EAP-Request/Identity フレームを受信しなかった場合、サプリカントはポートが許可ステートにあるものとしてデータを送信します。ポートが許可ステートになっている場合は、サプリカントの認証が成功したことを意味します。

サプリカントが自己の識別情報を提示すると、オーセンティケータは仲介装置としてのロールを開始し、認証が成功または失敗するまで、サプリカントと認証サーバの間で EAP フレームを送受信します。認証が成功すると、オーセンティケータのポートは許可ステートになります。

実際に行われる EAP フレーム交換は、使用する認証方式によって異なります。

次の図に、サプリカントが RADIUS サーバにワンタイム パスワード（OTP）認証方式を使用して開始するメッセージ交換を示します。OTP 認証デバイスは、シークレット パスフレーズを使用して、一連のワンタイム（使い捨て）パスワードを生成します。

図 *6*：メッセージ交換



ユーザのシークレット パスフレーズは、認証時やパスフレーズの変更時などにネットワークを通過することはありません。

インターフェイスのオーセンティケータ PAE ステータス

インターフェイスで 802.1X をイネーブルにすると、Cisco NX-OS ソフトウェアにより、オーセンティケータ Port Access Entity（PAE）インスタンスが作成されます。オーセンティケータ PAE は、

インターフェイスでの認証をサポートするプロトコル エンティティです。インターフェイスで802.1Xをディセーブルにしても、オーセンティケータ PAEインスタンスは自動的にクリアされません。必要に応じ、オーセンティケータ PAE をインターフェイスから明示的に削除し、再度適用することができます。

許可ステートおよび無許可ステートのポート

サプリカントのネットワークへのアクセスが許可されるかどうかは、オーセンティケータのポート ステートで決まります。ポートは、無許可ステートで開始します。このステートにあるポートは、802.1Xプロトコルパケットを除いたすべての入トラフィックおよび出トラフィックを禁止します。サプリカントの認証に成功すると、ポートは許可ステートに移行し、サプリカントのすべてのトラフィック送受信を通常どおりに許可します。

802.1X 認証をサポートしていないクライアントが無許可ステートの 802.1X ポートに接続した場合、オーセンティケータはクライアントの識別情報を要求します。この状況では、クライアントは要求に応答せず、ポートは引き続き無許可ステートとなり、クライアントはネットワーク アクセスを許可されません。

反対に、802.1x対応のクライアントが、802.1xプロトコルの稼働していないポートに接続すると、クライアントは EAPOL 開始フレームを送信して認証プロセスを開始します。応答がなければ、クライアントは同じ要求を所定の回数だけ送信します。応答がないので、クライアントはポートが許可ステートであるものとしてフレーム送信を開始します。

ポートには次の許可ステートがあります。

Force authorized

802.1X ポートベースの認証をディセーブルにし、認証情報の交換を必要としないで許可ステートに移行します。ポートはクライアントとの 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。この許可ステートはデフォルトです。

Force unauthorized

ポートが無許可ステートのままになり、クライアントからの認証の試みをすべて無視します。オーセンティケータは、インターフェイスを経由してクライアントに認証サービスを提供することができません。

自動

802.1Xポートベースの認証をイネーブルにします。ポートは無許可ステートで開始し、ポート経由で送受信できるのはEAPOLフレームだけです。ポートのリンク ステートがダウンからアップに移行したとき、またはサプリカントから EAPOL 開始フレームを受信したときに、認証プロセスが開始します。オーセンティケータは、クライアントの識別情報を要求し、クライアントと認証サーバとの間で認証メッセージのリレーを開始します。オーセンティケータはサプリカントのMACアドレスを使用して、ネットワークアクセスを試みる各サプリカントを一意に識別します。

サプリカントの認証に成功すると（認証サーバから Accept フレームを受信すると）、ポートが許可ステートに変わり、認証されたサプリカントからの全フレームがポート経由での送受信を許可されます。認証が失敗すると、ポートは無許可ステートのままですが、認証を再試行することは

できます。認証サーバに到達できない場合、オーセンティケータは要求を再送信できます。所定の回数だけ試行してもサーバから応答が得られない場合には、認証が失敗し、サプリカントのネットワーク アクセスは認可されません。

サプリカントはログオフするとき、EAPOL ログオフ メッセージを送信します。このメッセージによって、オーセンティケータのポートは無許可ステートに移行します。

ポートのリンク ステートがアップからダウンに移行した場合、または EAPOL ログオフ フレームを受信した場合、ポートは無許可ステートに戻ります。

MAC 認証バイパス

MAC 認証バイパス機能を使用して、サプリカントの MAC アドレスに基づいてサプリカントを認証するように、Cisco NX-OS デバイスを設定できます。たとえば、プリンタなどのデバイスに接続されている 802.1X 機能を設定したインターフェイスで、この機能をイネーブルにすることができます。

サプリカントからの EAPOL 応答を待機している間に 802.1X 認証がタイムアウトした場合は、MAC 認証バイパスを使用して Cisco NX-OS デバイスはクライアントの許可を試みます。

インターフェイスで MAC 認証バイパス機能をイネーブルにすると、Cisco NX-OS デバイスは MAC アドレスをサプリカント ID として使用します。認証サーバには、ネットワーク アクセスが許可されたサプリカントの MAC アドレスのデータベースがあります。Cisco NX-OS デバイスは、インターフェイスでクライアントを検出した後、クライアントからのイーサネット パケットを待ちます。Cisco NX-OS デバイスは、MAC アドレスに基づいてユーザ名とパスワードを含んだ RADIUS アクセス/要求フレームを認証サーバに送信します。許可に成功した場合、Cisco NX-OS デバイスはクライアントにネットワークへのアクセスを許可します。許可に失敗した場合、ゲスト VLAN が設定されていれば、ポートにゲスト VLAN を割り当てます。

リンクのライフタイム中に EAPOL パケットがインターフェイスで検出される場合、このインターフェイスに接続されているデバイスが 802.1X 対応サプリカントであることを Cisco NX-OS デバイスが判別し、（MAC 認証バイパスではなく）802.1X 認証を使用してインターフェイスを許可します。インターフェイスのリンク ステータスがダウンした場合、EAPOL 履歴はクリアされます。

Cisco NX-OS デバイスがすでに MAC 認証バイパスを使用してインターフェイスを許可していて、802.1X サプリカントを検出した場合、Cisco NX-OS デバイスはインターフェイスに接続されているクライアントを無許可にしません。再認証を実行する際に、Termination-Auction RADIUS 属性値が DEFAULT であるために前のセッションが終了した場合、Cisco NX-OS デバイスは 802.1X 認証を優先再認証プロセスとして使用します。

MAC 認証バイパスで許可されたクライアントを再認証することができます。再認証プロセスは、802.1X で認証されたクライアントと同様です。再認証中に、ポートは前に割り当てられた VLAN に残ります。再認証に成功した場合、スイッチはポートを同じ VLAN 内に保持します。再認証に失敗した場合、ゲスト VLAN が設定されていればポートにゲスト VLAN を割り当てます。

再認証が Session-Timeout RADIUS 属性（Attribute [27]）と Termination-Action RADIUS 属性（Attribute [29]）に基づいていて、Termination-Action RADIUS 属性（Attribute [29]）アクションが初期化の場合、（属性値は DEFAULT）、MAC 認証バイパス セッションが終了して、再認証中に接続が失われます。MAC 認証バイパスがイネーブルで 802.1X 認証がタイムアウトした場合、スイッチは

MAC 認証バイパス機能を使用して再許可を開始します。これらの AV ペアの詳細については、RFC 3580『*IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines*』を参照してください。

MAC 認証バイパスは、次の機能と相互作用します。

- 802.1X 認証：802.1X 認証がポートでイネーブルの場合にだけ、MAC 認証バイパスをイネーブルにできます。
- ポート セキュリティ：同じレイヤ 2 ポート上で 802.1X 認証とポート セキュリティを設定できます。
- Network Admission Control（NAC）レイヤ 2 IP 検証：例外リスト内のホストを含む 802.1X ポートが MAC 認証バイパスで認証されたあとに、この機能が有効になります。

802.1X とポート セキュリティ

ポート セキュリティと 802.1X は同じインターフェイス上に設定できます。ポート セキュリティによって、802.1X 認証の MAC アドレスを保護できます。802.1X はポート セキュリティよりも前にパケットを処理するので、1 つのインターフェイスで両方をイネーブルにすると、802.1X が、そのインターフェイスで、未知の MAC アドレスからのインバウンド トラフィックを妨げます。

同じインターフェイス上で 802.1X とポート セキュリティをイネーブルにしても、ポート セキュリティは設定どおりにスティッキ方式またはダイナミック方式で MAC アドレスの学習を続行します。また、シングル ホスト モードとマルチ ホスト モードのどちらで 802.1X をイネーブルにするかによって、次のいずれかが発生します。

シングル ホスト モード

ポート セキュリティは認証済みのホストの MAC アドレスを学習します。

マルチ ホスト モード

ポートセキュリティは、このインターフェイスでダイナミックに学習された MAC アドレスをドロップし、802.1X で認証された最初のホストの MAC アドレスを学習します。

802.1X がポート セキュリティに渡した MAC アドレスによってセキュア MAC アドレスの適用可能な最大数を違反することになる場合、デバイスはホストに認証エラー メッセージを送信します。

802.1X によって認証された MAC アドレスは、たとえそのアドレスがポート セキュリティによってスティッキ方式またはスタティック方式で学習されていたとしても、ダイナミック方式で学習されたアドレスと同様に扱われます。802.1X で認証されたセキュア MAC アドレスを削除しようとしても、そのアドレスはセキュア アドレスのまま保持されます。

認証済みのホストの MAC アドレスがスティッキ方式またはスタティック方式でセキュア アドレスになった場合、デバイスはそのアドレスをダイナミック方式で学習されたものとして扱うので、その MAC アドレスを手動で削除することはできません。

認証済みのホストのセキュアMACアドレスがポートセキュリティのエージング期限に達すると、ポート セキュリティは 802.1X と連動して、そのホストを再認証します。デバイスは、エージングのタイプに応じて、次のように異なる動作をします。

Absolute

ポート セキュリティは 802.1X に通知し、デバイスはホストの再認証を試行します。そのアドレスが引き続きセキュアアドレスになるかどうかは、再認証の結果によって決まります。再認証が成功すれば、デバイスはそのセキュア アドレスのエージング タイマーを再起動します。再認証に失敗した場合、デバイスはそのインターフェイスのセキュア アドレス リストからそのアドレスをドロップします。

Inactivity

ポート セキュリティは、そのインターフェイスのセキュア アドレス リストからそのセキュアアドレスをドロップし、802.1X に通知します。デバイスはホストの再認証を試行します。再認証が成功すれば、ポート セキュリティは再度そのアドレスをセキュア アドレスにします。

シングル ホストおよびマルチ ホストのサポート

802.1X機能では、1つのポートのトラフィックを1台のエンドポイント装置に限定することも（シングル ホスト モード）、1 つのポートのトラフィックを複数のエンドポイント装置に許可することも（マルチ ホスト モード）できます。

シングル ホスト モードでは、802.1X ポートで 1 台のエンドポイント装置のみからのトラフィックが許可されます。エンドポイント装置が認証されると、Cisco NX-OS デバイスはポートを許可ステートにします。エンドポイント装置がログオフすると、Cisco NX-OS デバイスはポートを無許可ステートに戻します。802.1X のセキュリティ違反とは、認証に成功して許可された単一の MAC アドレスとは異なる MAC アドレスをソースとするフレームが検出された場合をいいます。このような場合、このセキュリティ アソシエーション（SA）違反（他の MAC アドレスからの EAPOL フレーム）が検出されたインターフェイスはディセーブルにされます。シングル ホスト モードは、ホストツースイッチ型トポロジで1台のホストがCisco NX-OSデバイスのレイヤ2ポート（イーサネット アクセス ポート）またはレイヤ 3 ポート（ルーテッド ポート）に接続されている場合にだけ適用できます。

マルチ ホスト モードに設定されている 802.1X ポートで、認証が必要になるのは最初のホストだけです。最初のホストの許可に成功すると、ポートは許可ステートに移行します。ポートが許可ステートになると、後続のホストがネットワーク アクセスの許可を受ける必要はありません。再認証に失敗したり、または EAPOL ログオフ メッセージを受信して、ポートが無許可ステートになった場合には、接続しているすべてのクライアントはネットワーク アクセスを拒否されます。マルチ ホスト モードでは、SA 違反の発生時にインターフェイスをシャットダウンする機能がディセーブルになります。マルチ ホスト モードは、スイッチツースイッチ型トポロジおよびホストツースイッチ型トポロジの両方に適用できます。

サポートされるトポロジ

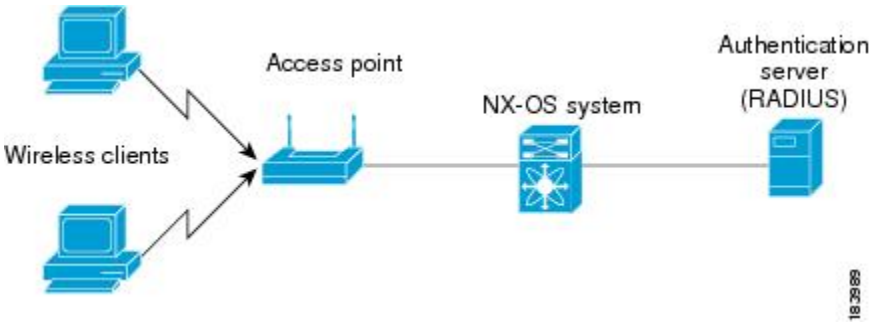
802.1X ポートベースの認証は、次の 2 つのトポロジでサポートされます。

- ポイントツーポイント
- Wireless LAN（ワイヤレス LAN）

ポイントツーポイント構成では、802.1X 対応のオーセンティケータ（Cisco NX-OS デバイス）ポートにサプリカント（クライアント）を 1 台だけ接続することができます。オーセンティケータは、ポートのリンク ステートがアップ ステートに移行したときにサプリカントを検出します。サプリカントがログオフしたとき、または別のサプリカントに代わったときには、オーセンティケータはポートのリンク ステートをダウンに変更し、ポートは無許可ステートに戻ります。

次の図に、ワイヤレス LAN 上での 802.1X ポートベースの認証を示します。802.1X ポートはマルチ ホスト ポートとして設定され、1 台のサプリカントが認証されるとすぐにポートが許可されます。

図 *7*：ワイヤレス *LAN* の例



ポートが許可されると、ポートに間接的に接続された他のすべてのホストに対して、ネットワーク アクセスが許可されます。ポートが無許可ステートになった場合（再認証が失敗した場合、または EAPOL ログオフ メッセージを受信した場合）、Cisco NX-OS デバイスは接続しているすべてのサプリカントのネットワーク アクセスを禁止します。

802.1X のバーチャライゼーション サポート

802.1X の設定と操作は、仮想デバイス コンテキスト（VDC）に対してローカルです。VDC の詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

802.1X のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	802.1Xにライセンスは必要ありません。ライセンスパッケージに含まれていない機能はすべてCisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

802.1X の前提条件

802.1X には次の前提条件があります。

- ネットワーク内の 1 つまたは複数の RADIUS サーバがアクセス可能であること。
- MACアドレス認証バイパス機能をイネーブルにする場合を除き、802.1Xサプリカントがポートに接続されていること。

802.1X の注意事項と制約事項

802.1X ポートベースの認証には、次の設定に関する注意事項と制約事項があります。

- Cisco NX-OS ソフトウェアが 802.1X 認証をサポートするのは、物理ポート上だけです。
- Cisco NX-OS ソフトウェアは、ポート チャネルまたはサブインターフェイスでは 802.1X 認証をサポートしません。
- Cisco NX-OS ソフトウェアは、ポート チャネルのメンバ ポートでは 802.1X 認証をサポートしますが、ポート チャネル自体ではサポートしません。
- Cisco NX-OS ソフトウェアは、ポート チャネル メンバが 802.1X 用に設定されている場合、そのメンバでは次の 802.1X 設定をサポートしません。
  - シングル ホスト モードではホスト モードを設定できません。メンバ ポートではマルチホスト モードだけがサポートされます。
  - メンバ ポートでは MAC 認証バイパスをイネーブルにできません。
  - ポート チャネルではポート セキュリティを設定できません。
- 802.1X設定を含むメンバポートと含まないメンバポートはポートチャネルで共存できます。ただし、チャネリングと 802.1X が連携して動作するためには、すべてのメンバ ポートで 802.1X 設定を同一にする必要があります。

- 802.1X 認証をイネーブルにした場合、サプリカントが認証されてから、イーサネット インターフェイス上のレイヤ 2 またはレイヤ 3 のすべての機能がイネーブルになります。
- Cisco NX-OS ソフトウェアが 802.1X 認証をサポートするのは、ポート チャネル、トランク、またはアクセス ポート内のイーサネット インターフェイス上だけです。
- Cisco NX-OS ソフトウェアは、ポート チャネル内のトランク インターフェイスまたはメンバ インターフェイス上ではシングル ホスト モードをサポートしません。
- Cisco NX-OS ソフトウェアは、トランク インターフェイス上では MAC アドレス認証バイパス機能をサポートしません。
- Cisco NX-OS ソフトウェアは、ポート チャネル上では MAC アドレス認証バイパス機能をサポートしません。
- Cisco NX-OS ソフトウェアは、vPC ポートでの Dot1X および MCT をサポートしません。
- Cisco NX-OS ソフトウェアは、次の 802.1X プロトコル拡張機能をサポートしません。
  - 論理 VLAN 名から ID への 1 対多のマッピング
  - Web 許可
  - ダイナミック ドメイン ブリッジ割り当て
  - IP テレフォニー
- 次に、ダイナミック VLAN 割り当ての制約事項を示します。
  - ダイナミック VLAN 割り当ては、ストレート スルー接続でのみ、HIF ポート（FEX ポート）でサポートされます。
  - この機能は、Switchport アクセス ポート上でのみサポートされます。
  - RADIUS により割り当てられる VLAN は、スイッチですでに設定されている必要があります。
  - この機能は、VPC ポート、ポート チャネル、トランク ポート、および L3 ポートではサポートされません。
  - RADIUS により VLAN が割り当てられた後、別のアクセス VLAN でそれを上書きすることはできません。

802.1X のデフォルト設定

次の表に、802.1X パラメータのデフォルト設定を示します。

表 *22* : *802.1X* のデフォルト パラメータ

パラメータ	デフォルト
802.1X 機能	ディセーブル
AAA 802.1X 認証方式	未設定
インターフェイス単位の 802.1x プロトコル イネーブル ステート	ディセーブル（**force-authorized**） （注） ポートはサプリカントとの 802.1X ベース認証を行わずに、通常のトラフィックを送受信します。
定期的な再認証	ディセーブル
再認証の間隔（秒）	3600 秒
待機タイムアウト時間	60 秒（Cisco NX-OS デバイスがサプリカントとの認証情報の交換に失敗した後、待機状態を続ける秒数）
再送信タイムアウト時間	30 秒（Cisco NX-OS デバイスが EAP-Request/Identity フレームに対するサプリカントからの応答を待ち、要求を再送信するまでの秒数）
最大再送信回数	2 回（Cisco NX-OS デバイスが認証プロセスを再開するまでに、EAP-Request/Identity フレームを送信する回数）
ホスト モード	シングル ホスト
サプリカント タイムアウト時間	30秒（認証サーバからの要求をサプリカントにリレーするとき、Cisco NX-OS デバイスがサプリカントに要求を再送信するまでに、サプリカントの応答を待つ時間）
認証サーバ タイムアウト時間	30秒（サプリカントからの応答を認証サーバにリレーするとき、Cisco NX-OS デバイスがサーバに応答を再送信するまでに、サーバからの応答を待つ時間）

802.1X の設定

ここでは、802.1X 機能の設定方法について説明します。

（注） Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

802.1X の設定プロセス

ここでは、802.1X を設定するプロセスについて説明します。

手順の概要

1. 802.1X 機能をイネーブルにします。
2. リモート RADIUS サーバへの接続を設定します。
3. イーサネット インターフェイスで 802.1X 機能をイネーブルにします。

手順の詳細

ステップ 1 802.1X 機能をイネーブルにします。
ステップ 2 リモート RADIUS サーバへの接続を設定します。
ステップ 3 イーサネット インターフェイスで 802.1X 機能をイネーブルにします。

802.1X 機能のイネーブル化

サプリカント デバイスを認証する前に、Cisco NX-OS デバイス上で 802.1X 機能をイネーブルにする必要があります。

手順の概要

1. **configure terminal**
2. **feature dot1x**
3. **exit**
4. （任意） **show dot1x**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**feature dot1x** 例： `switch(config)# feature dot1x`	802.1X機能をイネーブルにします。デフォルトではディセーブルになっています。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show dot1x** 例： `switch# show dot1x`	（任意） 802.1X 機能のステータスを表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

802.1X の AAA 認証方式の設定

802.1X 認証にリモート RADIUS サーバを使用できます。RADIUS サーバおよび RADIUS サーバ グループを設定し、デフォルト AAA 認証方式を指定したあとに、Cisco NX-OS デバイスは 802.1X 認証を実行します。

はじめる前に

リモート RADIUS サーバ グループの名前またはアドレスを取得します。

手順の概要

1. **configure terminal**
2. **aaa authentication dot1x default group***group-list*
3. **exit**
4. （任意） **show radius-server**
5. （任意） **show radius-server group** [*group-name*]
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**aaa authentication dot1x default group***group-list* 例： `switch(config)# aaa authentication dot1x default group rad2`	802.1X 認証に使用する RADIUS サーバ グループを指定します。 *group-list* 引数には、グループ名をスペースで区切ったリストを指定します。グループ名は、次のように指定します。 • **radius** を指定すると、RADIUS サーバのグローバル プールが認証に使用されます。 • *named-group*：認証に RADIUS サーバのグローバル プールを使用します。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show radius-server** 例： `switch# show radius-server`	（任意） RADIUS サーバの設定を表示します。
ステップ 5	**show radius-server group** [*group-name*] 例： `switch# show radius-server group rad2`	（任意） RADIUS サーバ グループの設定を表示します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスでの 802.1X 認証の制御

インターフェイス上で実行される 802.1X 認証を制御できます。インターフェイスの 802.1X 認証ステートは、次のとおりです。

自動

インターフェイス上で、802.1X 認証をイネーブルにします。

強制認証

インターフェイス上の 802.1X 認証をディセーブルにし、認証を行わずにインターフェイス上のすべてのトラフィックを許可します。このステートがデフォルトです。

Force-unauthorized

インターフェイス上のすべてのトラフィックを禁止します。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface ethernet** *slot* / *port*
3. **dot1x port-control** {**auto** | **force-authorized** | **forced-unauthorized**}
4. **exit**
5. （任意） **show dot1x all**
6. （任意） **show dot1x interface ethernet***slot*/*port*
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet** *slot* / *port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**dot1x port-control** {**auto** | **force-authorized** | **forced-unauthorized**} 例： `switch(config-if)# dot1x port-control auto`	インターフェイスの 802.1X 認証ステートを変更します。デフォルトの設定は force-authorized です。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 5	**show dot1x all** 例： `switch# show dot1x all`	（任意） 802.1X 機能のすべてのステータスおよび設定情報を表示します。
ステップ 6	**show dot1x interface ethernet***slot*/*port* 例： `switch# show dot1x interface ethernet 2/1`	（任意） インターフェイスの 802.1X 機能のステータスおよび設定情報を表示します。
ステップ 7	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

メンバ ポートでの 802.1X 認証の設定

ポート チャネルのメンバで 802.1X 認証を設定できます。

（注） ポート チャネル自体では 802.1X 認証を設定できません。

メンバ ポートで 802.1X 認証を設定する方法は 2 つあります。メンバ ポートで 802.1X を設定してからそのポートをポート チャネルに追加する方法と、ポート チャネルを作成し、そのポート チャネルにポートを追加してからそのポートで 802.1X を設定する方法です。ここで示す手順は、1 つめの方法の手順です。2 つめの方法で 802.1X を設定するには、次のコマンドを使用します。

- **interface port-channel** *channel-number*
- **interface ethernet** *slot*/*port*
- **channel-group** *channel-number* [**force**] [**mode** {**on** | **active** | **passive**}]
- **dot1x port-control auto**

（注） 上記のコマンドの詳細については、ご使用のプラットフォームの『*Cisco NX-OS Interfaces Command Reference*』を参照してください。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port*
3. **dot1x port-control auto**
4. [**no**] **switchport**
5. **dot1x host-mode multi-host**
6. **channel-group** *channel-number* [**force**] [**mode** {**on** | **active** | **passive**}]
7. **exit**
8. **exit**
9. （任意） **show dot1x all**
10. （任意） **show dot1x interface ethernet***slot*/*port*
11. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 2	**interface ethernet***slot*/*port*
	
	例：
	`switch(config)# interface ethernet 7/1`
	`switch(config-if)#`
		設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**dot1x port-control auto** 例： `switch(config-if)# dot1x port-control auto`	インターフェイスの 802.1X 認証ステートを変更します。
ステップ 4	[**no**] **switchport** 例： `switch(config-if)# switchport`	インターフェイスをレイヤ 2 ポートとして設定します。**no** キーワードを使用する場合は、レイヤ 3 ポートとして設定します。
ステップ 5	**dot1x host-mode multi-host** 例： `switch(config-if)# dot1x host-mode multi-host`	インターフェイスのマルチ ホスト モードをイネーブルにします。このコマンドはポート チャネルにポートを追加する際に必要です。
ステップ 6	**channel-group** *channel-number* [**force**] [**mode** {**on** | **active** | **passive**}] 例： `switch(config-if)# channel-group 5 force`	チャネル グループ内にポートを設定し、モードを設定します。チャネル番号の有効範囲は 1 ～ 4096 です。ポート チャネルがない場合は、Cisco NX-OS ソフトウェアによって、このチャネル グループに関連付けられたポート チャネルが作成されます。 オプションの **force** キーワードを使用すると、互換性のない設定を持つインターフェイスを強制的にチャネルに追加できます。強制されるインターフェイスは、チャネル グループと同じ速度、デュプレックス、およびフロー制御設定を持っている必要があります。 （注） ポート チャネルから 802.1X 対応ポートを削除するには、**no channel-group** *channel-number* コマンドを使用します。

ステップ 7	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 8	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 9	**show dot1x all** 例： `switch# show dot1x all`	（任意） 802.1X機能のすべてのステータスおよび設定情報を表示します。
ステップ 10	**show dot1x interface ethernet***slot*/*port* 例： `switch# show dot1x interface ethernet 7/1`	（任意） インターフェイスの 802.1X 機能のステータスおよび設定情報を表示します。
ステップ 11	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスでのオーセンティケータ PAE の作成または削除

インターフェイスで 802.1X オーセンティケータ Port Access Entity（PAE）インスタンスを作成または削除できます。

（注） デフォルトでは、インターフェイスで 802.1X をイネーブルにしたときに、Cisco NX-OS ソフトウェアによってインターフェイスでオーセンティケータ PAE インスタンスが作成されます。

はじめる前に

802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. （任意） **show dot1x interface ethernet***slot*/*port*
3. **interface ethernet***slot*/*port*
4. [**no**] **dot1x pae authenticator**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**show dot1x interface ethernet***slot*/*port* 例： `switch# show do1x interface ethernet 2/1`	（任意） インターフェイス上の 802.1X の設定を表示します。

ステップ 3	**interface ethernet***slot*/*port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 4	[**no**] **dot1x pae authenticator** 例： `switch(config-if)# dot1x pae authenticator`	インターフェイスでオーセンティケータ PAE インスタンスを作成します。インターフェイスから PAE インスタンスを削除するには、**no** 形式を使用します。 （注） オーセンティケータ PAE がインターフェイスにすでに存在している場合は、**dot1x pae authentication** コマンドを実行してもインターフェイス上の設定は変更されません。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

グローバル定期再認証のイネーブル化

802.1X グローバル定期再認証をイネーブルにし、再認証を実行する頻度を指定します。期間を指定しないで再認証をイネーブルにした場合、再認証を行う間隔は 3600 秒（1 時間）です。

（注） 再認証プロセス中、すでに認証されているサプリカントのステータスは影響を受けません。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **dot1x re-authentication**
3. **dot1x timeout re-authperiod** *seconds*
4. （任意） **exit**
5. （任意） **show dot1x all**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**dot1x re-authentication** 例： `switch(config)# dot1x re-authentication`	Cisco NX-OS デバイス上ですべてのサプリカントの定期再認証をイネーブルにします。デフォルトでは、定期再認証はディセーブルです。
ステップ 3	**dot1x timeout re-authperiod** *seconds* 例： `switch(config)# dot1x timeout re-authperiod 3000`	再認証の間隔（秒）を設定します。 デフォルトは 3600 秒です。有効な範囲は 1 ～ 65535 です。 （注） 定期再認証をイネーブルにする場合だけ、このコマンドは Cisco NX-OS デバイスの動作に影響します。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		（任意）
		設定モードを終了します。

ステップ 5	**show dot1x all** 例： `switch# show dot1x all`	（任意） 802.1X 機能のすべてのステータスおよび設定情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスの定期再認証のイネーブル化

インターフェイスの802.1X定期再認証をイネーブルにし、再認証を実行する頻度を指定します。期間を指定しないで再認証をイネーブルにした場合、再認証を行う間隔はグローバル値にデフォルト設定されます。

（注） 再認証プロセス中、すでに認証されているサプリカントのステータスは影響を受けません。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port*
3. **dot1x re-authentication**
4. （任意） **dot1x timeout re-authperiod***seconds*
5. **exit**
6. （任意） **show dot1x all**
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet***slot*/*port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**dot1x re-authentication** 例： `switch(config-if)# dot1x re-authentication`	インターフェイスに接続されているサプリカントの定期再認証をイネーブルにします。デフォルトでは、定期再認証はディセーブルです。

	コマンドまたはアクション	目的
ステップ 4	**dot1x timeout re-authperiod***seconds* 例： `switch(config-if)# dot1x timeout re-authperiod 3300`	（任意） 再認証の間隔（秒）を設定します。デフォルトは 3600 秒です。有効な範囲は 1 ～ 65535 です。 （注） インターフェイス上の定期再認証をイネーブルにする場合だけ、このコマンドは Cisco NX-OS デバイスの動作に影響します。

ステップ 5	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		設定モードを終了します。

ステップ 6	**show dot1x all** 例： `switch(config)# show dot1x all`	（任意） 802.1X機能のすべてのステータスおよび設定情報を表示します。
ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

手動によるサプリカントの再認証

Cisco NX-OS デバイス全体のサプリカントまたはインターフェイスのサプリカントを手動で再認証できます。

（注） 再認証プロセス中、すでに認証されているサプリカントのステータスは影響を受けません。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **dot1x re-authenticate** [**interface***slot*/*port*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**dot1x re-authenticate** [**interface***slot*/*port*] 例： `switch# dot1x re-authenticate interface 2/1`	Cisco NX-OS デバイスまたはインターフェイス上のサプリカントを再認証します。

手動による 802.1X 認証の初期化

Cisco NX-OS デバイスまたは特定のインターフェイスですべてのサプリカントの認証を、手動で初期化することができます。

（注） 認証を初期化すると、クライアントの認証プロセスを開始する前に既存のすべての認証ステータスがクリアされます。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **dot1x initialize** [**interface ethernet** *slot*/*port*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**dot1x initialize** [**interface ethernet** *slot*/*port*] 例： `switch# dot1x initialize interface ethernet 2/1`	Cisco NX-OS デバイスまたは指定のインターフェイス上の 802.1X 認証を初期化します。

802.1X グローバル認証タイマーの変更

Cisco NX-OS デバイスでは、次の 802.1X グローバル認証タイマーをサポートしています。

待機時間タイマー

デバイスがサプリカントを認証できない場合、デバイスは所定の時間アイドル状態になり、その後再試行します。待機時間タイマーの値でアイドルの時間が決まります。認証が失敗する原因には、サプリカントが無効なパスワードを提供した場合があります。デフォルトよりも小さい値を入力することによって、ユーザへの応答時間を短縮できます。デフォルトは 60 秒です。有効な範囲は 1 ～ 65535 です。

スイッチとサプリカント間の再送信時間タイマー

クライアントは、デバイスの EAP-Request/Identity フレームに対し、EAP-Response/Identity フレームで応答します。デバイスがこの応答を受信できなかった場合、所定の時間（再送信時間）だけ待機した後、フレームを再送信します。デフォルトは 30 です。範囲は 1 ～ 65535 秒です。

（注） また、待機時間タイマーおよびスイッチとサプリカント間の送信時間タイマーをインターフェイス レベルでも設定できます。

（注） このデフォルト値は、リンクの信頼性が低下した場合や、特定のサプリカントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う場合にだけ変更してください。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. （任意） **dot1x timeout quiet-period** *seconds*
3. （任意） **dot1x timeout tx-period** *seconds*
4. **exit**
5. （任意） **show dot1x all**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**dot1x timeout quiet-period** *seconds* 例： `switch(config)# dot1x timeout quiet-period 30`	（任意） Cisco NX-OS デバイスがサプリカントとの認証情報の交換に失敗した後、待機状態を続ける時間を秒数で設定します。デフォルトは 60 秒です。範囲は 1 ～ 65535 秒です。
ステップ 3	**dot1x timeout tx-period** *seconds* 例： `switch(config)# dot1x timeout tx-period 20`	（任意） Cisco NX-OS デバイスが、EAP-Request/Identity フレームに対するサプリカントからの応答を待ち、要求を再送信するまでの時間を秒数で設定します。デフォルトは 30 秒です。範囲は 1 ～ 65535 秒です。

ステップ 4	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		設定モードを終了します。

ステップ 5	**show dot1x all** 例： `switch(config)# show dot1x all`	（任意） 802.1X の設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスの 802.1X 認証タイマーの変更

Cisco NX-OS デバイスのインターフェイス上で変更できる 802.1X 認証タイマーは、次のとおりです。

待機時間タイマー

Cisco NX-OS デバイスがサプリカントを認証できない場合、スイッチは所定の時間アイドル状態になり、その後再試行します。待機時間タイマーの値でアイドルの時間が決まります。認証が失敗する原因には、サプリカントが無効なパスワードを提供した場合があります。デフォルトよりも小さい値を入力することによって、ユーザへの応答時間を短縮できます。デフォルトは、グローバル待機時間タイマーの値です。範囲は 1 ～ 65535 秒です。

レート制限タイマー

レート制限時間中、サプリカントから過剰に送信されている EAPOL-Start パケットを抑制します。オーセンティケータはレート制限時間中、認証に成功したサプリカントからの EAPOL-Start パケットを無視します。デフォルト値は 0 秒で、オーセンティケータはすべての EAPOL-Start パケットを処理します。範囲は 1 ～ 65535 秒です。

レイヤ 4 パケットに対するスイッチと認証サーバ間の再送信タイマー

認証サーバは、レイヤ 4 パケットを受信するたびにスイッチに通知します。スイッチがパケット送信後に通知を受信できない場合、Cisco NX-OS デバイスは所定の時間だけ待機した後、パケットを再送信します。デフォルトは 30 秒です。範囲は 1 ～ 65535 秒です。

EAP 応答フレームに対するスイッチとサプリカント間の再送信タイマー

サプリカントは、Cisco NX-OS デバイスの EAP-Request/Identity フレームに対し、EAP-Response/Identity フレームで応答します。Cisco NX-OS デバイスがこの応答を受信できなかった場合、所定の時間（再送信時間）だけ待機した後、フレームを再送信します。デフォルトは 30 秒です。範囲は 1 ～ 65535 秒です。

EAP 要求フレームに対するスイッチとサプリカント間の再送信タイマー

サプリカントは、EAP 要求フレームを受信したことを Cisco NX-OS デバイスに通知します。オーセンティケータがこの通知を受信できなかった場合、オーセンティケータは所定の時間だけ待機した後、フレームを再送信します。デフォルトは、グローバル再送信時間タイマーの値です。範囲は 1 ～ 65535 秒です。

（注） このデフォルト値は、リンクの信頼性が低下した場合や、特定のサプリカントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う場合にだけ変更してください。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port*
3. （任意） **dot1x timeout quiet-period***seconds*
4. （任意） **dot1x timeout ratelimit-period***seconds*
5. （任意） **dot1x timeout server-timeout***seconds*
6. （任意） **dot1x timeout supp-timeout***seconds*
7. （任意） **dot1x timeout tx-period***seconds*
8. **exit**
9. （任意） **show dot1x all**
10. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet***slot*/*port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)`
		設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**dot1x timeout quiet-period***seconds* 例： `switch(config-if)# dot1x timeout quiet-period 25`	（任意） オーセンティケータが EAP-Request/Identity フレームに対するサプリカントからの応答を待ち、要求を再送信するまでの時間を秒数で設定します。デフォルトはすべてのインターフェイスに設定されるグローバル秒数です。範囲は 1 ～ 65535 秒です。
ステップ 4	**dot1x timeout ratelimit-period***seconds* 例： `switch(config-if)# dot1x timeout ratelimit-period 10`	（任意） 認証に成功したサプリカントからの EAPOL-Start パケットを無視する時間を秒数で設定します。デフォルト値は 0 秒です。範囲は 1 ～ 65535 秒です。
ステップ 5	**dot1x timeout server-timeout***seconds* 例： `switch(config-if)# dot1x timeout server-timeout 60`	（任意） Cisco NX-OS デバイスが認証サーバにパケットを送信する前に待機する時間を秒数で設定します。デフォルトは 30 秒です。範囲は 1 ～ 65535 秒です。

	コマンドまたはアクション	目的
ステップ 6	**dot1x timeout supp-timeout***seconds* 例： `switch(config-if)# dot1x timeout supp-timeout 20`	（任意） Cisco NX-OS デバイスが EAP 要求フレームを再送信する前に、サプリカントが EAP 要求フレームに応答してくるのを待機する時間を秒数で設定します。デフォルトは 30 秒です。範囲は 1 ～ 65535 秒です。
ステップ 7	**dot1x timeout tx-period***seconds* 例： `switch(config-if)# dot1x timeout tx-period 40`	（任意） サプリカントから EAP 要求フレームを受信した通知が送信されない場合に、EAP 要求フレームを再送信する間隔を秒数で設定します。デフォルトはすべてのインターフェイスに設定されるグローバル秒数です。範囲は 1 ～ 65535 秒です。

ステップ 8	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 9	**show dot1x all** 例： `switch# show dot1x all`	（任意） 802.1X の設定を表示します。
ステップ 10	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

シングル ホスト モードまたはマルチ ホスト モードのイネーブル化

インターフェイス上でシングル ホスト モードまたはマルチ ホスト モードをイネーブルにすることができます。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port*
3. **dot1x host-mode** {**multi-host** | **single-host**}
4. **exit**
5. （任意） **show dot1x all**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet***slot*/*port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)`
		設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**dot1x host-mode** {**multi-host**	**single-host**} 例： `switch(config-if)# dot1x host-mode multi-host`	ホスト モードを設定します。デフォルトは、single-host です。 （注） 指定したインターフェイスで **dot1x port-control** インターフェイス コンフィギュレーション コマンドが **auto** に設定されていることを確認してください。

ステップ 4	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		設定モードを終了します。

ステップ 5	**show dot1x all** 例： `switch# show dot1x all`	（任意） 802.1X 機能のすべてのステータスおよび設定情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

MAC 認証バイパスのイネーブル化

サプリカントの接続されていないインターフェイス上で、MAC認証バイパスをイネーブルにすることができます。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port*
3. **dot1x mac-auth-bypass** [**eap**]
4. **exit**
5. （任意） **show dot1x all**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet***slot*/*port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)`
		設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**dot1x mac-auth-bypass** [**eap**] 例： `switch(config-if)# dot1x mac-auth-bypass`	MAC認証バイパスをイネーブルにします。デフォルトはバイパスのディセーブルです。**eap** キーワードを使用して、許可に EAP を使用するように Cisco NX-OS デバイスを設定します。

ステップ 4	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		設定モードを終了します。

ステップ 5	**show dot1x all** 例： `switch# show dot1x all`	（任意） 802.1X 機能のすべてのステータスおよび設定情報を表示します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Cisco NX-OS デバイスでの 802.1X 認証のディセーブル化

Cisco NX-OS デバイス上の 802.1X 認証をディセーブルにできます。デフォルトでは、802.1X 機能をイネーブルにすると、Cisco NX-OS ソフトウェアが 802.1X 認証をイネーブルにします。ただし、802.1X 機能をディセーブルにした場合、設定は Cisco NX-OS デバイスから削除されます。Cisco NX-OS ソフトウェアでは、802.1X の設定を失わずに 802.1X 認証をディセーブルにできます。

（注） 802.1X 認証をディセーブルにすると、設定されているポート モードに関係なく、すべてのインターフェイスのポート モードがデフォルトの force-authorized になります。802.1X 認証を再びイネーブルにすると、Cisco NX-OS ソフトウェアはインターフェイス上に設定したポート モードを復元します。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **no dot1x system-auth-control**
3. **exit**
4. （任意） **show dot1x**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**no dot1x system-auth-control** 例： `switch(config)# no dot1x system-auth-control`	Cisco NX-OS デバイス上の 802.1X 認証をディセーブルにします。デフォルトではイネーブルになっています。 （注） Cisco NX-OS デバイス上の 802.1X 認証をイネーブルにするには、**dot1x system-auth-control** コマンドを使用します。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show dot1x** 例： `switch# show dot1x`	（任意） 802.1X 機能のステータスを表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

802.1X 機能のディセーブル化

Cisco NX-OS デバイス上の 802.1X 機能をディセーブルにできます。

802.1X をディセーブルにすると、関連するすべての設定が自動的に廃棄されます。Cisco NX-OS ソフトウェアは、802.1X を再度イネーブルにして設定を回復する場合に使用できる自動チェックポイントを作成します。詳細については、ご使用のプラットフォームの『*Cisco NX-OS System Management Configuration Guide*』を参照してください。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **no feature dot1x**
3. **exit**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**no feature dot1x** 例： `switch(config)# no feature dot1x`	802.1X 機能をディセーブルにします。 **注意** 802.1X機能をディセーブルにすると、802.1X のすべての設定が削除されます。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

802.1X グローバル設定のデフォルト値へのリセット

802.1X グローバル設定をデフォルト値に設定できます。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **dot1x default**
3. **exit**
4. （任意） **show dot1x all**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**dot1x default** 例： `switch(config)# dot1x default`	802.1X グローバル設定をデフォルト値に戻します。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show dot1x all** 例： `switch# show dot1x all`	（任意） 802.1X 機能のすべてのステータスおよび設定情報を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

802.1X インターフェイス設定のデフォルト値へのリセット

インターフェイスの 802.1X 設定をデフォルト値にリセットすることができます。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port*
3. **dot1x default**
4. **exit**
5. （任意） **show dot1x all**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet***slot*/*port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)`
		設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**dot1x default** 例： `switch(config-if)# dot1x default`	インターフェイスの 802.1X 設定をデフォルト値に戻します。

ステップ 4	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		設定モードを終了します。

ステップ 5	**show dot1x all** 例： `switch(config)# show dot1x all`	（任意） 802.1X機能のすべてのステータスおよび設定情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

オーセンティケータとサプリカント間のフレーム再送信最大リトライ回数のグローバル設定

オーセンティケータとサプリカント間の再送信時間を変更できるだけでなく、（サプリカントから応答がなかった場合に）Cisco NX-OS デバイスが認証プロセスを再開するまでに、サプリカントに EAP-Request/Identity フレームを送信する回数を設定することができます。

（注） このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のサプリカントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う場合にだけ変更してください。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **dot1x max-req***retry-count*
3. **exit**
4. （任意） **show dot1x all**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**dot1x max-req***retry-count* 例： `switch(config)# dot1x max-req 3`	802.1X認証プロセスを再開するまでの、最大要求リトライ回数を変更します。デフォルトは2回です。有効な範囲は 1 ～ 10 回です。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show dot1x all** 例： `switch(config)# show dot1x all`	（任意） 802.1X機能のすべてのステータスおよび設定情報を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスでのオーセンティケータとサプリカント間のフレーム再送信最大リトライ回数の設定

セッションがタイムアウトするまでに、Cisco NX-OS デバイスがインターフェイス上でサプリカントに認証要求を再送信する最大回数を設定できます。デフォルトは 2 回です。有効な範囲は 1 ～ 10 回です。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface ethernet** *slot/port*
3. **dot1x max-req** *count*
4. **exit**
5. （任意） **show dot1x all**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet** *slot/port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**dot1x max-req** *count* 例： `switch(config-if)# dot1x max-req 3`	最大認証要求リトライ回数を変更します。デフォルトは 2 回です。有効な範囲は 1 ～ 10 回です。 （注） 指定したインターフェイスで **dot1x port-control** インターフェイス コンフィギュレーション コマンドが **auto** に設定されていることを確認してください。

	コマンドまたはアクション	目的

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 5	**show dot1x all** 例： `switch# show dot1x all`	（任意） 802.1X 機能のすべてのステータスおよび設定情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

802.1X 認証の RADIUS アカウンティングのイネーブル化

802.1X 認証のアクティビティに対する RADIUS アカウンティングをイネーブルにできます。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **dot1x radius-accounting**
3. **exit**
4. （任意） **show dot1x**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**dot1x radius-accounting** 例： `switch(config)# dot1x radius-accounting`	802.1X に対する RADIUS アカウンティングをイネーブルにします。デフォルトではディセーブルになっています。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show dot1x** 例： `switch# show dot1x`	（任意） 802.1X の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

802.1X の AAA アカウンティング方式の設定

802.1X 機能に対する AAA アカウンティング方式をイネーブルにできます。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **aaa accounting dot1x default group***group-list*
3. **exit**
4. （任意） **show aaa accounting**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal**	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**aaa accounting dot1x default group***group-list*	802.1X に対する AAA アカウンティングをイネーブルにします。デフォルトではディセーブルになっています。 *group-list* 引数には、グループ名をスペースで区切ったリストを指定します。グループ名は、次のように指定します。 • **radius**：設定済みのすべての RADIUS サーバ • *named-group*：設定済みの任意の RADIUS サーバ グループ名
ステップ 3	**exit**	設定モードを終了します。
ステップ 4	**show aaa accounting**	（任意） AAA アカウンティングの設定を表示します。
ステップ 5	**copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

次に、802.1X 機能をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# aaa accounting dot1x default group radius
switch(config)# exit
switch# show aaa accounting
switch# copy running-config startup-config
```

インターフェイスでの再認証最大リトライ回数の設定

セッションがタイムアウトするまでに、Cisco NX-OS デバイスがインターフェイス上でサプリカントに再認証要求を再送信する最大回数を設定できます。デフォルトは 2 回です。有効な範囲は 1 ～ 10 回です。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port*
3. **dot1x max-reauth-req***retry-count*
4. **exit**
5. （任意） **show dot1x all**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet***slot*/*port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		設定するインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**dot1x max-reauth-req***retry-count* 例： `switch(config-if)# dot1x max-reauth-req 3`	最大再認証要求リトライ回数を変更します。デフォルトは 2 回です。有効な範囲は 1 ～ 10 回です。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 5	**show dot1x all** 例： `switch# show dot1x all`	（任意） 802.1X 機能のすべてのステータスおよび設定情報を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

802.1X 設定の確認

802.1X 情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show dot1x	802.1X 機能のステータスを表示します。
show dot1x all [**details** | **statistics** | **summary**]	802.1X機能のすべてのステータスおよび設定情報を表示します。

コマンド	目的
show dot1x interface ethernet*slot*/*port* [**details** | **statistics** | **summary**]	イーサネット インターフェイスの 802.1X 機能のステータスおよび設定情報を表示します。
show running-config dot1x [**all**]	実行コンフィギュレーション内の 802.1X 機能の設定を表示します。
show startup-config dot1x	スタートアップ コンフィギュレーション内の 802.1X 機能の設定を表示します。

これらのコマンドの出力フィールドの詳細については、ご使用のプラットフォームの『*Cisco NX-OS Security Command Reference*』を参照してください。

802.1X のモニタリング

Cisco NX-OS デバイスが保持している 802.1X のアクティビティに関する統計情報を表示できます。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **show dot1x** {**all** | **interface ethernet***slot*/*port*} **statistics**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show dot1x** {**all** | **interface ethernet***slot*/*port*} **statistics** 例： `switch# show dot1x all statistics`	802.1X 統計情報を表示します。

802.1X の設定例

次に、アクセス ポートに 802.1X を設定する例を示します。

```
feature dot1x
aaa authentication dot1x default group rad2
interface Ethernet2/1
dot1x pae-authenticator
```

```
dot1x port-control auto
```

次に、トランク ポートに 802.1X を設定する例を示します。

```
feature dot1x
aaa authentication dot1x default group rad2
interface Ethernet2/1
dot1x pae-authenticator
dot1x port-control auto
dot1x host-mode multi-host
```

（注） 802.1X 認証が必要なすべてのインターフェイスに対して、**dot1x pae authenticator** コマンドおよび **dot1x port-control auto** コマンドを繰り返してください。

802.1X に関する追加情報

ここでは、802.1X の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS ライセンス設定	『*Cisco NX-OS Licensing Guide*』
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』
VRF コンフィギュレーション	『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』

標準

標準	タイトル
IEEE Std 802.1X- 2004（IEEE Std 802.1X-2001 の改訂版）	『*802.1X IEEE Standard for Local and Metropolitan Area Networks Port-Based Network Access Control*』
RFC 2284	『*PPP Extensible Authentication Protocol (EAP)*』
RFC 3580	『*IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines*』

MIB

MIB	MIB のリンク
• IEEE8021-PAE-MIB	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

802.1X の機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 *23* : *802.1X* の機能の履歴

機能名	リリース	機能情報
802.1X	6.0(1)	Release 5.2 以降、変更はありません。
802.1X	5.2(1)	Release 5.1 以降、変更はありません。
802.1X	5.1(1)	Release 5.0 以降、変更はありません。

第 12 章

NAC の設定

この章では、Cisco NX-OS デバイス上で Network Admission Control（NAC）を設定する手順を説明します。

この章は、次の項で構成されています。

- 機能情報の確認，361 ページ
- NAC の概要，362 ページ
- NAC のライセンス要件，376 ページ
- NAC の前提条件，377 ページ
- NAC の注意事項と制約事項，377 ページ
- NAC のデフォルト設定，378 ページ
- NAC の設定，378 ページ
- NAC の設定の確認，413 ページ
- NAC の設定例，414 ページ
- NAC に関する追加情報，414 ページ
- NAC の機能の履歴，414 ページ

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

NAC の概要

NACを使用すると、エンドポイント装置のネットワーク アクセスを許可する前に、エンドポイント装置のセキュリティ適合性と脆弱性をチェックできます。このセキュリティ適合性のチェックのことを、ポスチャ検証といいます。ポスチャ検証により、ワーム、ウイルス、およびその他の不正アプリケーションがネットワーク全体に拡散することを防止できます。

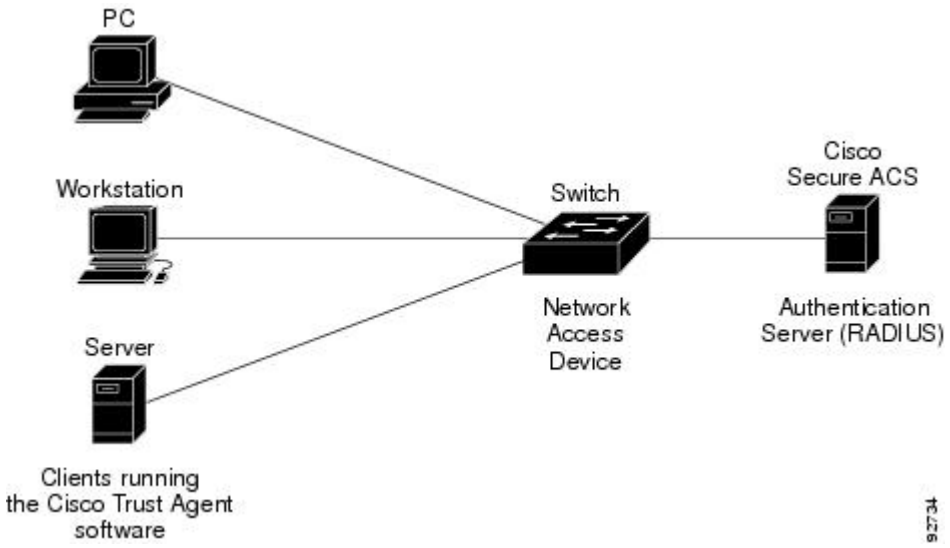
NACは、エンドポイント装置がネットワークの保護された領域にアクセス可能になる前に、エンドポイント装置のポスチャ（状態）がセキュリティ ポリシーに適合しているかどうかを検証します。セキュリティ ポリシーに適合する場合は、ネットワークの保護されたサービスにアクセスすることが許可されます。デバイスがセキュリティ ポリシーに適合しない場合は、修復専用のネットワークにアクセスが許可されます。修復ネットワークではデバイスのポスチャが再度チェックされます。

NAC デバイスのロール

NAC は、ネットワーク上の各デバイスにロールを割り当てます。

次の図に、NAC デバイスのロールを設定したネットワークの例を示します。

図 *8*：ポスチャ検証デバイス



NAC は、次のネットワーク デバイスのロールをサポートしています。

エンドポイント装置

Cisco NX-OS デバイスのアクセス ポートに直接接続される PC、ワークステーション、またはサーバなどのネットワークのシステムまたはクライアントです。エンドポイント装置では Cisco Trust Agent（CTA）ソフトウェアが稼働し、LAN およびスイッチのサービスへのアクセスを要求し、スイッチからの要求に応答します。エンドポイント装置はウイルスの感染源である可能性があり、NAC はエンドポイント装置にネットワーク アクセスを許可する前に、アンチウイルス ステータスを検証する必要があります。

（注） Cisco Trust Agent ソフトウェアは、ポスチャ エージェントまたはアンチウイルス クライアントとも呼ばれます。Cisco Trust Agent ソフトウェアの詳細については、次の URL にアクセスしてください。

http://www.cisco.com/en/US/products/sw/secursw/ps5057/index.html

ネットワーク アクセス デバイス（NAD）

ネットワーク エッジで検証サービスの提供およびとポリシーの適用、クライアントのアクセス ポリシーに基づいてネットワークへの物理アクセスを制御する Cisco NX-OS デバイスです。NAD は、エンドポイントと認証サーバの間で拡張認証プロトコル（EAP）メッセージをリレーします。
NAD は、ネットワークに対する新しい接続を検出すると、ポスチャ クレデンシャルを照会します。エンドポイント装置にポスチャ エージェント（PA）がインストールされている場合は、インバンド ポスチャ検証を実行します。NAD は、エンドポイント装置と AAA サーバとの間で、ポスチャ検証情報の交換に関するすべてのメッセージのリレー エージェントとして動作します。PA が見つからない場合は、監査サーバを介してアウトオブバンド ポスチャ検証を実行します。

NAD は、ネットワークに対する新しい接続を検出すると、ポスチャ クレデンシャルを照会します。エンドポイント装置にポスチャ エージェント（PA）がインストールされている場合は、インバンド ポスチャ検証を実行します。NAD は、エンドポイント装置と AAA サーバとの間で、ポスチャ検証情報の交換に関するすべてのメッセージのリレー エージェントとして動作します。PA が見つからない場合は、監査サーバを介してアウトオブバンド ポスチャ検証を実行します。

（インバンドかアウトバンドかにかかわらず）ポスチャ検証情報の交換が完了すると、NAD はどのホストが NAD デバイスを経由してネットワークの宛先にアクセスできるかを、AAA サーバから受信したネットワーク アクセス プロファイルに基づいて制御します。ネットワーク アクセス プロファイルは、次のいずれかの形式をとります。

- VLAN またはプライベート VLAN。
- アクセス コントロール リスト（ACL）は、NAC プロセスとは無関係にすべてのホストに付与されるデフォルト アクセス（DHCP サーバ、修復サーバ、監査サーバなどへのアクセス）に加えて、このホストが到達可能な宛先とそのトラフィック タイプを指定します。

NAD は、次のタイミングでポスチャ検証プロセスをトリガーします。

- 新しいセッションの開始
- 再検証タイマーの期限切れ
- システム管理者コマンドの入力
- PA によるポスチャの変更の通知（PA を備えるエンドポイント装置のみ対象）

Cisco NX-OS デバイスの場合、EAP メッセージのカプセル化の情報はユーザ データグラム プロトコル（UDP）に基づいています。UDP は、EAP over UDP（EAPoUDP または EoU）フレームの形で使用されます。

認証サーバ

実際のクライアント認証を行うサーバのことです。認証サーバはクライアントのアンチウイルス ステータスを検証し、アクセス ポリシーを確定し、LAN および NAD サービスへのアクセスをクライアントに許可するかどうかを NAD に通知します。NAD はプロキシとして動作するため、NAD と認証サーバの間の EAP メッセージ交換は、NAD に対しては透過的に行われます。

Cisco NX-OS デバイスは、RADIUS、認証、許可、アカウンティング（AAA）、および EAP 拡張機能を備えた Cisco Secure Access Control Server（ACS）Version 4.0 以降をサポートします。

ポスチャ検証サーバ

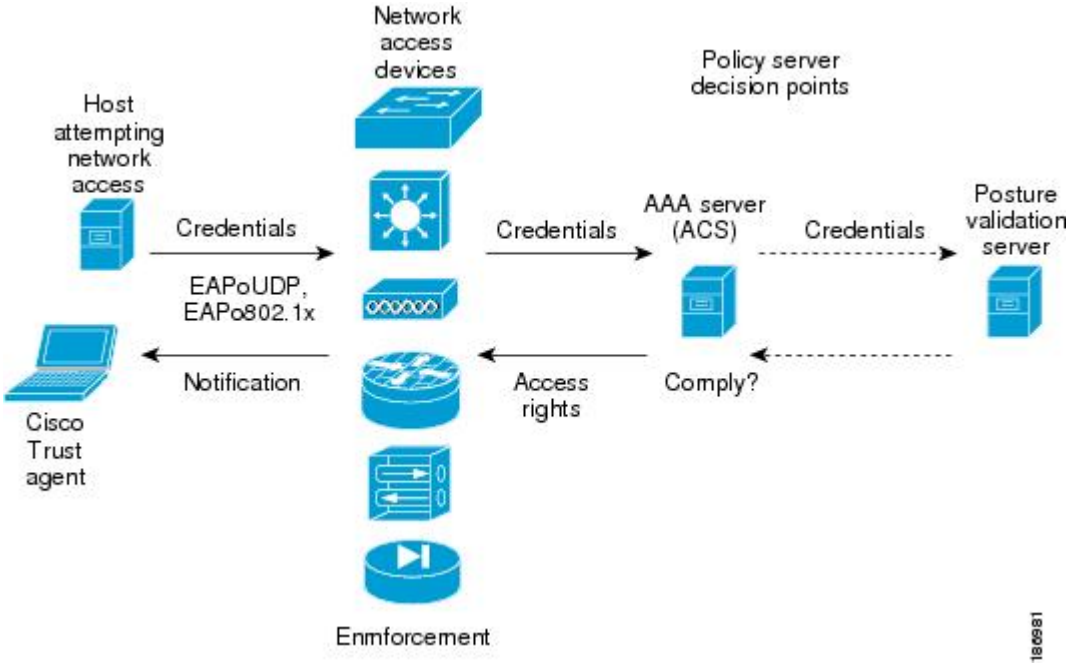
ポスチャ クレデンシャル セットをポリシー ルール セットに照らして許可する際に、NAC においてアプリケーション固有のポリシー デシジョン ポイントとして動作するサードパーティ製のサーバです。ポスチャ検証サーバは、認証サーバから要求を受信します。

NAC のポスチャ検証

ポスチャ検証は、ネットワーク リソースへの接続または使用を試みるエンドポイント装置を NAC 対応の NAD が検出したときに行われます。新しいエンドポイント装置を検出すると、NAD はエンドポイント装置のネットワーク アクセス プロファイルを AAA サーバ（Cisco Secure ACS など）に要求します。

次の図に、NAC によるエンドポイント装置のポスチャ検証プロセスを示します。

図 *9*：*NAC* によるエンドポイント装置のポスチャ検証



AAA サーバは、エンドポイント装置にポスチャ エージェントがインストールされているかどうかを確認します。エンドポイント装置にポスチャ エージェント（Cisco Trust Agent など）が存在すれば、AAA サーバは NAD を経由してエンドポイント装置にポスチャ情報を要求します。エンドポイント装置は、AAA サーバにポスチャ クレデンシャル セットを使用して応答します。AAA サーバは、このポスチャ情報をローカルで検証するか、あるいは 1 つまたは複数の外部ポスチャ検証サーバにポスチャ検証処理を任せます。

エンドポイント装置にポスチャ エージェントが存在しなければ、AAA サーバは監査サーバに別な手段（フィンガープリントやポート スキャンなど）でポスチャ情報を収集するように要求できます。また、AAA サーバは監査サーバに、収集した情報を検証しポスチャ検証結果を返すように要求することもできます。

AAA サーバは、これらのソースからのポスチャ検証結果を集約し、エンドポイント装置がネットワーク ポリシーに準拠しているかどうかを基に許可の判定を行います。AAA サーバは、エンドポイント装置のネットワーク アクセス プロファイルを確定すると、そのプロファイルを NAD に送信してエンドポイント装置の許可を適用できるようにします。

AAA サーバによるエンドポイント装置のクレデンシャルの検査では、1 つまたは複数のアプリケーション ポスチャ トークン（APT）が作成されます。APT は、ベンダー アプリケーションの適合性チェックを表しています。AAA サーバは、各ポスチャ検証サーバからすべての APT を集約し 1 つのシステム ポスチャ トークン（SPT）にまとめます。この SPT は、エンドポイント装置の総合適合性を表しています。SPT の値は、APT セットの中の最も不良な APT に基づいています。APT および SPT は、どちらも次の既定のトークンを使用して表されます。

Healthy

エンドポイント装置はポスチャ ポリシーに適合しており、この装置に課せられる規制はありません。

Checkup

エンドポイント装置はポリシーの範囲内にありますが、最新のソフトウェアが使用されていないため、アップデートを推奨します。

Transition

エンドポイント装置はポスチャの検証を受けている途中であり、その検証結果が出るまで暫定的にアクセスが許可されています。transitionは、ホストがブート中のため完全なポスチャ情報を入手できない、または完全な監査結果が得られない場合の状態です。

Quarantine

エンドポイント装置はポリシーに適合していません。この装置を検疫ネットワークに規制して修復する必要があります。他のエンドポイント装置にただちに脅威となるわけではありませんが、この装置は攻撃やウイルス感染に脆弱であり、できるだけ早急にアップデートする必要があります。

Infected

エンドポイント装置は他のエンドポイント装置に実際の脅威となっています。ネットワーク アクセスを厳格に規制し、この装置に修復処置を施すか、この装置へのすべてのネットワーク アクセスを禁止する必要があります。

Unknown

AAA サーバは、エンドポイント装置のポスチャ クレデンシャルを確認できません。適切なポスチャ クレデンシャルを取得しネットワーク アクセス許可の評価ができるように、エンドポイント装置の完全性を確認する必要があります。

IP デバイス トラッキング

IP デバイス トラッキングを使用すると、AAA サーバが使用できない場合でも、エンドポイント装置を引き続いてネットワークに接続できます。NAC の一般的な導入では、Cisco Secure ACS を使用してクライアントの状態（ポスチャ）が検証され、ポリシーが NAD に返されます。

IP デバイス トラッキングには、次の利点があります。

- AAAが使用できない間、エンドポイント装置は制限があるにしても、ネットワークへの接続は維持されます。
- AAA サーバが再び使用可能になると、ユーザは再検証を受けることができ、ACS からユーザのポリシーをダウンロードできます。

（注） AAA サーバの停止時は、ホストに既存のポリシーが関連付けられていない場合にだけ、NAD は IP デバイス トラッキング ポリシーを適用します。通常、再検証中に AAA サーバが停止した場合は、NAD はエンドポイント装置に使用されている現行のポリシーを保持します。

NAC LPIP

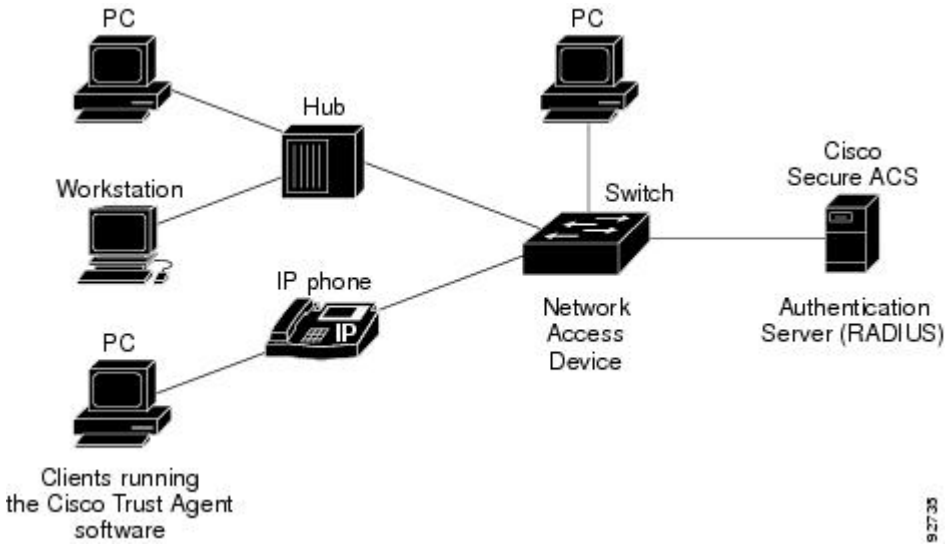
NAC LAN Port IP（LPIP）検証では、レイヤ 3 トランスポート EAPoUDP を使用してポスチャ検証情報が伝送されます。LPIP 検証には、次の特徴があります。

- レイヤ 2 ポート上でだけ動作し、レイヤ 3 ポート上では動作できません。
- ポート上で IP トラフィックを送信するすべてのホストがポスチャ検証の対象になります。

LPIP 検証では、DHCP メッセージまたはアドレス解決プロトコル（ARP）メッセージのスヌーピングによりアドミッション コントロールをトリガーします。データ パスでの IP パケットの代行受信は使用されません。LPIP 検証ではアクセス コントロール リスト（ACL）を使用してポリシーを適用します。

次の図に、NAD ポートに接続されたシングル ホスト、または同一 NAD ポートに接続されたマルチ ホストの LPIP 検証プロセスを示します。

図 *10*：*LPIP* 検証を使用するネットワーク



LPIP 検証をイネーブルにすると、EAPoUDP は IPv4 トラフィックだけをサポートします。NAD はエンドポイント装置またはクライアントのアンチウイルス ステータスをチェックして、アクセス コントロール ポリシーを適用します。

ポスチャ検証

1 つまたは複数のエンドポイント装置が接続されるポートで LPIP 検証をイネーブルにすると、Cisco NX-OS デバイスは DHCP スヌーピングおよび ARP スヌーピングを使用して、接続されたホストを識別します。Cisco NX-OS デバイスは、ARP パケットを受信した後、または DHCP スヌーピングのバインディング エントリを作成した後にポスチャ検証を開始します。デフォルトでは、接続されたホストの検出には ARP スヌーピングが使用されます。DHCP スヌーピング バインディング エントリが作成されたときに NAD にホストを検出させるには、DHCP スヌーピングをイネーブルにする必要があります。

ポスチャ検証のトリガー

LPIP 検証では、ARP スヌーピングを使用して、ダイナミックに取得した IP アドレスを持つホストまたはスタティックに設定された IP アドレスを持つホストを検出します。NAD が未知のホストからの ARP 要求を受信すると、ポスチャ検証をトリガーします。インターフェイスで DHCP スヌーピングがイネーブルになっている場合には、NAD に DHCP バインディング エントリが作成されるとポスチャ検証がトリガーされます。DHCP パケットは ARP 要求が送信される前に交換されるので、DHCP スヌーピングのほうがわずかに早く応答します。ARP スヌーピングと DHCP スヌーピングの両方が、同じホストのポスチャ検証をトリガーすることがあります。その場合、DHCP スヌーピング バインディングの作成によって起動されたトリガーが、ARP スヌーピングに優先します。

（注） DHCP スヌーピングと ARP スヌーピングを使用してホストの存在を検出する場合、悪意あるホストがスタティック ARP テーブルを設定してポスチャ検証をバイパスする可能性があります。この種の脅威から保護するために、ポートで IP ソース ガードをイネーブルにします。IP ソース ガードを使用すると、未認証のホストによるネットワークへのアクセスを防ぐことができます。

ポスチャ検証の方法

ホストのポスチャ検証がトリガーされると、次のいずれかの方法を使用してホストに適用するポリシーを指定できます。

- 例外リスト
- EAPoUDP

例外リスト

例外リストには、ローカル プロファイルとポリシー設定が含まれます。IP アドレスまたは MAC アドレスに基づいてデバイスをスタティックに許可または検証する場合は、アイデンティティ プロファイルを使用します。アイデンティティ プロファイルはローカル ポリシーに関連付けし、ローカル ポリシーにアクセス コントロール属性を指定できます。

例外リストを使用すると、特定のエンドポイント装置のポスチャ検証をバイパスして、スタティックに設定したポリシーを適用できます。ポスチャ検証がトリガーされると、NADは例外リストのホスト情報をチェックします。例外リストと一致した場合、NADはそのエンドポイント装置用に設定されたポリシーを適用します。

EAPoUDP

エンドポイント装置が例外リストと一致しなかった場合、NAD は EAPoUDP パケットを送信してポスチャ検証を開始します。ポスチャ検証の実行中、NADはデフォルトのアクセスポリシーを適用します。NAD が EAPoUDP メッセージをホストに送信し、ホストがこのアンチウイルス状態要求メッセージに応答すると、NAD は受信した EAPoUDP 応答を Cisco Secure ACS に転送します。NADが所定の回数試行してもホストから応答が得られない場合、このホストを非応答として分類します。ACS がクレデンシャルを検証すると、認証サーバが Access-Accept または Access-Reject メッセージを NAD に返します。NAD は EAPoUDP セッション テーブルを更新し、アクセス制限事項を適用します。これにより不適切なポスチャのエンドポイント装置は、隔離され検疫されるか、ネットワーク アクセスを拒否されます。

（注） Access-Reject メッセージは、EAPoUDP 情報の交換が失敗したことを意味します。これは、エンドポイント装置のポスチャが不適切であるという意味ではありません。

Access-Accept メッセージの場合は、NAD は Policy-based ACL（PACL）名を含むポリシーを適用し、EAP 再検証タイマーとステータス クエリー タイマーを開始します。

Access-Preject メッセージの場合は、NADはホストの適用ポリシーをすべて削除し、エンドポイント装置を既定の時間（ホールドタイマー）、Held ステートにします。ホールドタイマーの期限が切れると、エンドポイント装置は再検証されます。

（注） エンドポイント装置の DHCP スヌーピング バインディング エントリを削除すると、NAD はセッション テーブルからこのクライアントのエントリを削除します。これ以降、このクライアントは認証されません。

関連トピック

ACL を使用したポリシーの適用, （370 ページ）

ACL を使用したポリシーの適用

LPIP 検証では、ポリシーの適用に PACL を使用します。

NAD は、ポリシー検証に失敗（AAA サーバが Accept-Reject メッセージを送信）すると PACL を適用します。デフォルト ポリシーでは、ポートに適用されるアクティブな MAC ACL が使用されます（Port ACL（PACL）とも呼ばれます）。アクティブ MAC ACL には、スタティックに設定された PACL、または 802.1X 認証に基づいた AAA サーバ指定の PACL を使用できます。

PACL には、エンドポイント装置の IP アドレスのリストに展開されるグループを定義します。通常、PACL にはエンドポイント装置の IP アドレスを含みます。NAD は特定のグループを使用してエンドポイント装置を分類すると、そのエンドポイント装置に対応する IP アドレスを該当するグループに追加します。これにより、ポリシーがエンドポイント装置に適用されます。

NAD ポートの LPIP 検証を定義する場合は、その NAD ポートにデフォルトの PACL も定義する必要があります。また、そのデフォルト ACL を、ポスチャ検証が未完了のホストの IP トラフィックに適用するようにしてください。

NAD にデフォルト ACL が設定されていて、Cisco Secure ACS がホストのアクセス ポリシーを NAD に送信した場合、NAD は NAD ポートに接続されているそのホストからのトラフィックにこのポリシーを適用します。ポリシーがトラフィックに適用される場合、NAD はそのトラフィックを転送します。ポリシーが適用されない場合、NAD はデフォルトの ACL を適用します。ただし、NAD が Cisco Secure ACS からエンドポイント装置のアクセス ポリシーを取得しても、デフォルト ACL が設定されていないと、LPIP 検証の設定は有効になりません。

（注） DHCP スヌーピングと ARP スヌーピングは、どちらも VLAN 単位でイネーブルになります。ただし、NAC レイヤ 2 ポスチャ検証によりダウンロードされるセキュリティ ACL は、ポート単位で適用されます。その結果、これらの機能がいずれかの VLAN でイネーブルになると、DHCP パケットと ARP パケットはすべて代行受信されます。

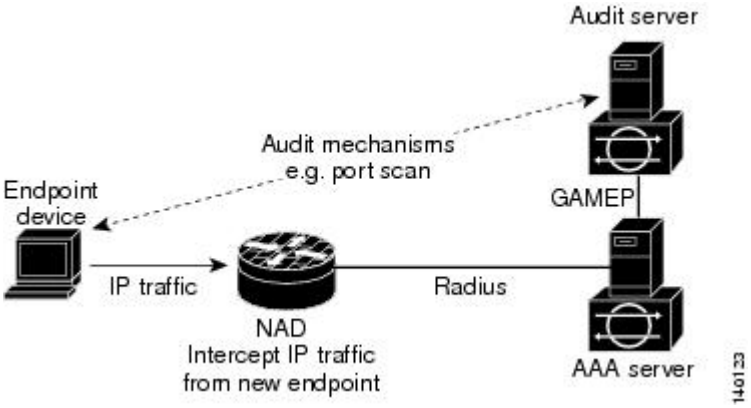
監査サーバおよび非応答ホスト

ポスチャ エージェント（Cisco Trust Agent）が稼働していないエンドポイント装置は、NAD から要求されてもクレデンシャルを提供できません。このようなデバイスを、エージェントレスまたは非応答と表現します。

NAC アーキテクチャは監査サーバをサポートしており、これを使用してエージェントレス エンドポイント装置を検証します。監査サーバは、エンドポイント装置にポスチャ エージェントがない場合でもそのセキュリティ適合性を調査、スキャン、および判別できるサードパーティ製サーバです。監査サーバの検査結果をアクセス サーバに反映させることができるので、エンドポイント装置固有のネットワーク アクセス ポリシーの適用が可能になり、すべての非応答エンドポイント装置に共通の制限ポリシーを適用する必要がありません。任意のサードパーティ製監査処理を NAC アーキテクチャに統合することで、より堅牢なホスト監査および検査機能を構築できます。

次の図に、一般的なトポロジに監査サーバを組み込む方法を示します。

図 *11*：*NAC* デバイスのロール



NACは、監査サーバが到達可能になっていて、エンドポイント装置が監査サーバと通信できることを前提としています。ポスチャ検証が設定されたNADを経由してエンドポイント装置がネットワーク アクセスを行うと、NAD は AAA サーバ（Cisco Secure ACS）に、このホストに適用するアクセスポリシーを要求します。AAAサーバは、外部の監査サーバによるホストのスキャンをトリガーするように設定できます。監査サーバによるスキャンは非同期に行われ、完了までに数秒かかります。スキャンの実行中、AAAサーバは、適用を行う最小限の制限セキュリティポリシーと短時間のポーリング タイマー（セッション タイムアウト）を NAD に伝送します。監査サーバから結果が返されるまで、NADは所定の時間間隔でAAAサーバをポーリングします。AAAサーバは監査結果を受け取ると、監査結果に基づいてアクセスポリシーを計算し、NADからの次の要求で、適用に必要なこのポリシーを NAD に送信します。

NAC タイマー

ここでは、NAC タイマーについて説明します。

ホールド タイマー

ホールド タイマーは、EAPoUDP セッションの失敗を検証する試みのあとに、次の新規セッションがすぐに開始されないように抑制します。NAC はこのタイマーを、Cisco Secure ACS が Accept-Reject メッセージを NAD に送信した場合にだけ使用します。ホールド タイマーのデフォルト値は 180 秒（3 分）です。

EAPoUDPセッションの検証が失敗するのは、ホストのポスチャ検証が失敗した場合、セッションタイマーの期限が切れた場合、NAD または Cisco Secure ACS が無効なメッセージを受信した場合などです。NADまたは認証サーバが無効なメッセージを連続して受信する場合は、悪意あるユーザが DoS 攻撃（サービス拒絶攻撃）を仕掛けようとしている可能性もあります。

AAA タイマー

AAA タイマーは、ポスチャ検証の実行中、NAD が要求を再送信する前に AAA サーバからの応答を待機する時間を制御します。再送信タイマーのデフォルト値は 60 秒です。

（注） このタイマーの設定値が低すぎると、不必要な再送信が行われる可能性があり、設定値が高すぎると、応答時間が長くなる可能性があります。

再送信タイマー

再送信タイマーは、ポスチャ検証の実行中、NAD が要求を再送信する前にクライアントからの応答を待機する時間を制御します。再送信タイマーのデフォルト値は 3 秒です。

（注） このタイマーの設定値が低すぎると、不必要な再送信が行われる可能性があり、設定値が高すぎると、応答時間が長くなる可能性があります。

再検証タイマー

再検証タイマーは、ポスチャ検証の実行中に EAPoUDP メッセージを使用していたエンドポイント装置に対し、NAD が NAC ポリシーを適用する期間を制御します。このタイマーは、最初のポスチャ検証が完了した時点で開始されます。ホストが再検証されると、このタイマーはリセットされます。再検証タイマーのデフォルト値は 36000 秒（10 時間）です。

Cisco NX-OS ソフトウェアの再検証タイマーは、AAA サーバ（Cisco Secure ACS）からの Access-Accept メッセージに含まれる Session-Timeout RADIUS 属性（Attribute [27]）、および Termination-Action RADIUS-REQUEST 属性（Attribute [29]）に基づいて動作します。NAD が Session-Timeout 値を受信した場合、この値は NAD の再検証タイマー値に優先します。

再検証タイマーが満了した場合の NAD のアクションは、次の Termination-Action 属性の値に応じて異なります。

- Termination-Action RADIUS 属性の値がデフォルト値の場合は、セッションは終了します。
- NAD が受信した Termination-Action 属性の値がデフォルト以外の場合は、ポスチャ検証の実行中、EAPoUDP セッションおよび現在のアクセス ポリシーは有効な状態を維持します。
- Termination-Action 属性の値が RADIUS の場合は、NAD はクライアントを再検証します。
- サーバからのパケットに Termination-Action 属性が含まれない場合は、EAPoUDP セッションは終了します。

ステータス クエリー タイマー

ステータスクエリータイマーは、以前検証したクライアントが存在し、そのポスチャが変更されていないことを確認するまでの、NAD の待機時間を制御します。EAPoUDP メッセージによって認証されたクライアントだけが、このタイマーを使用します。このタイマーは、クライアントの最初の検証が完了した時点で開始されます。ステータス クエリー タイマーのデフォルト値は 300 秒（5 分）です。

ホストが再認証されると、このタイマーはリセットされます。このタイマーが満了すると、NAD はホストに Status-Query メッセージを送信して、ホストのポスチャ検証の状態を確認します。ポスチャが変更されたことを示すメッセージをホストが NAD に送信すると、NAD はホストのポスチャを再検証します。

NAC ポスチャ検証および冗長スーパーバイザ モジュール

スイッチオーバーが発生した場合、Cisco NX-OS デバイスはエンドポイント装置と現在の PACL アプリケーションに関する情報を保持しますが、各 EAPoUDP セッションの現在のステートは失われます。Cisco NX-OS デバイスは、現在の PACL アプリケーションを削除し、ポスチャ検証を再開します。

LPIP 検証および他のセキュリティ機能

ここでは、LPIP 検証と Cisco NX-OS デバイス上の他のセキュリティ機能との相互作用について説明します。

802.1X

ポートに 802.1X と LPIP の両方を設定した場合、802.1X 認証によるソース MAC チェックに合格しないトラフィックは、ポスチャ検証をトリガーしません。ポートに 802.1X を設定した場合、接続されているホストが 802.1X により認証されるまでは、ポートはトラフィック（EAP over LAN（EAPOL）を除く）の送信および受信ができません。このメカニズムにより、ホストが認証されるまでは、ホストからの IP トラフィックがポスチャ検証をトリガーしないようになっています。

ポート セキュリティ

NAD は、ソース MAC アドレスをポート セキュリティの MAC アドレスと照合し、照合されなかった場合はそのエンドポイント装置をドロップします。NAD は、ポート セキュリティで検証された MAC アドレスにだけポスチャ検証を許可します。ポート セキュリティ違反が発生し、ポートがシャットダウンした場合は、Cisco NX-OS ソフトウェアはそのポートの LPIP ステートを削除します。

DHCP スヌーピング

DHCP によってバインディング エントリが作成されるまでは、ポスチャ検証は実行されません。DHCP スヌーピングと LPIP をイネーブルにした場合、DHCP を使用して IP アドレスを取得するホストのバインディング エントリを DHCP が作成したときに、Cisco NX-OS ソフトウェアがそのホストのポスチャ検証をトリガーします。

ダイナミック ARP インスペクション

インターフェイス上で LPIP 検証をイネーブルにすると、パケットがダイナミック ARP インスペクション（DAI）に合格した場合だけ、ポスチャ検証がトリガーされます。DAI をイネーブルにしないと、すべての ARP パケット（有効な MAC/IP ペアの場合）でポスチャ検証がトリガーされます。

（注） ARP スヌーピングは、ホストの検出に使用されるデフォルトのメカニズムです。ただし、ARP スヌーピングと DAI は同じものではありません。LPIP 検証をイネーブルにすると、Cisco NX-OS ソフトウェアは ARP パケットを LPIP 検証に渡します。DAI をイネーブルにすると、Cisco NX-OS ソフトウェアは ARP パケットを DAI に渡します。

（注） DHCP スヌーピングがイネーブルになっている場合、Cisco NX-OS ソフトウェアは DAI をバイパスします。

IP ソース ガード

IP ソース ガードは、インターフェイス単位のトラフィック フィルタです。各パケットの IP アドレスと MAC アドレスが、IP と MAC のアドレス バインディングのうち、次に示す 2 つの送信元のどちらかと一致する場合だけ、IP トラフィックを許可します。

- DHCP スヌーピング バインディング テーブル内のエントリ
- 設定したスタティック IP ソース エントリ

信頼できる IP と MAC アドレス バインディングに基づいてフィルタリングするので、有効なホストの IP アドレスのスプーフィングを使用した攻撃の防止に役立ちます。IP ソース ガードを妨ぐためには、攻撃者は有効なホストの IP アドレスと MAC アドレスを両方スプーフィングする必要があります。

関連トピック

IP ソース ガードの設定, （771 ページ）

ポスチャのホスト固有 ACE

Cisco NX-OS ソフトウェアは、パケットが拒否条件と一致する場合はパケットをドロップし、パケットが許可条件と一致する場合はアクティブ PACL をスキップします。ACE の最後まで明示的な拒否がなく、一致もなかった場合、Cisco NX-OS ソフトウェアはパケットをアクティブ PACL と照合します。

（注） DHCP スヌーピングまたは DAI をイネーブルにすると、NAD はポスチャのホスト固有 ACE を処理しません。

アクティブ PACL

アクティブ PACL は、スタティックに設定された PACL の場合と、802.1X 認証に基づいた AAA サーバ指定の PACL の場合があります。パケットは、いずれかの拒否条件に一致するとドロップされ、許可条件に一致すると次のステップに進みます。

（注） DHCP スヌーピングまたは DAI がイネーブルになっている場合、NAD はアクティブ PACL を処理しません。

VACL

Cisco NX-OS ソフトウェアは、拒否条件と一致するパケットをすべてドロップします。

（注） DHCP スヌーピングまたは DAI がイネーブルになっている場合、NAD は VACL をバイパスします。

NAC のバーチャライゼーション サポート

NAC の設定と操作は、仮想デバイス コンテキスト（VDC）に対してローカルです。

VDC の詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

NAC のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	NACにはライセンスは必要ありません。ライセンスパッケージに含まれていない機能はすべてCisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

NAC の前提条件

NAC の前提条件は次のとおりです。

- NAD と各エンドポイント装置との間にレイヤ 3 ルートが存在していること

NAC の注意事項と制約事項

NAC に関する注意事項と制約事項は次のとおりです。

- EAPoUDP バイパスと AAA ダウン ポリシーはサポートされません。
- NAC は、認証に RADIUS だけを使用します。

LPIP の制約事項

LPIP 検証に関する制約事項は次のとおりです。

- LPIP 検証が許可されるのは、アクセス ポートだけです。
- LPIP 検証をトランク ポートまたはポート チャネル上でイネーブルできません。
- LPIP 検証は、スパンの終点であるポート上では許可されません。
- LPIP 検証は、プライベート VLAN に属するポート上では許可されません。
- LPIP 検証は、IPv6 をサポートしていません。
- LPIP 検証が許可されるのは、NAD に直接接続されたエンドポイント装置上だけです。
- NAD とエンドポイント装置との間にレイヤ 3 ルートがないと LPIP 検証を使用できません。

NAC のデフォルト設定

次の表に、NAC パラメータのデフォルト設定を示します。

表 *24* : *NAC* パラメータのデフォルト設定

パラメータ	デフォルト
EAPoUDP	ディセーブル
EAP UDP ポート番号	21862（0x5566）
クライアントレス ホストの使用	ディセーブル
定期的な自動再検証	イネーブル
再検証タイムアウト間隔	36000 秒（10 時間）
再送信タイムアウト間隔	3 秒
ステータス クエリー タイムアウト間隔	300 秒（5 分）
ホールド タイムアウト間隔	180 秒（3 分）
AAA タイムアウト間隔	60 秒（1 分）
最大リトライ回数	3.
EAPoUDP レート制限最大数	20 同時セッション
EAPoUDP ロギング	ディセーブル
IP デバイス トラッキング	イネーブル

NAC の設定

ここでは、NAC の設定方法について説明します。

（注） Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

NAC の設定プロセス

NAC の設定には、次の作業を行います。

手順の概要

1. EAPoUDP をイネーブルにします。
2. AAA サーバへの接続を設定します。
3. エンドポイント装置と接続するインターフェイスに PACL を適用します。
4. エンドポイント装置と接続するインターフェイス上で NAC をイネーブルにします。

手順の詳細

ステップ 1 EAPoUDP をイネーブルにします。
ステップ 2 AAA サーバへの接続を設定します。
ステップ 3 エンドポイント装置と接続するインターフェイスに PACL を適用します。
ステップ 4 エンドポイント装置と接続するインターフェイス上で NAC をイネーブルにします。

関連トピック

EAPoUDP のイネーブル化, （379 ページ）
EAPoUDP のデフォルト AAA 認証方式のイネーブル化, （380 ページ）
インターフェイスへの PACL の適用, （382 ページ）
インターフェイスでの NAC のイネーブル化, （383 ページ）

EAPoUDP のイネーブル化

Cisco NX-OS デバイスは、エンドポイントと認証サーバの間で拡張認証プロトコル（EAP）メッセージをリレーします。NAC を設定する前に、Cisco NX-OS デバイス上で EAP over UDP（EAPoUDP）をイネーブルにする必要があります。

手順の概要

1. **configure terminal**
2. **feature eou**
3. **exit**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**feature eou** 例： `switch(config)# feature eou`	EAPoUDP をイネーブルにします。デフォルトではディセーブルになっています。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 4	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

EAPoUDP のデフォルト AAA 認証方式のイネーブル化

EAPoUDP のデフォルト AAA 認証方式をイネーブルにする必要があります。

（注） LPIP は認証に RADIUS だけを使用できます。

はじめる前に

EAPoUDP をイネーブルにします。

必要に応じて RADIUS または TACACS+ サーバ グループを設定します。

手順の概要

1. **configure terminal**
2. **aaa authentication eou default group***group-list*
3. **exit**
4. （任意） **show aaa authentication**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**aaa authentication eou default group***group-list* 例： `switch(config)# aaa authentication eou default group RadServer`	EAPoUDP のデフォルト AAA 認証方式として、1 つまたは複数の RADIUS サーバ グループのリストを設定します。*group-list* 引数には、グループをスペースで区切ったリストを指定します。グループ名は次のとおりです。 • **radius** を指定すると、RADIUS サーバのグローバル プールが認証に使用されます。 • *named-group*：RADIUS サーバの名前付きサブセットを認証に使用します。 デフォルトでは、認証方式は設定されていません。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 4	**show aaa authentication** 例： `switch# show aaa authentication`	（任意） デフォルトの AAA 認証方式を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

EAPoUDP のイネーブル化，（379 ページ）
AAA の設定，（33 ページ）
RADIUS の設定，（75 ページ）

インターフェイスへの PACL の適用

AAA サーバから PACL を入手できない場合は、NAD 上の LPIP ポスチャ検証を実行するアクセス インターフェイスに PACL を適用する必要があります。

はじめる前に

MAC ACL を作成します。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port*
3. **mac access-group***access-list*
4. **exit**
5. （任意） **show running-config interface**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet***slot*/*port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		イーサネット インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**mac access-group***access-list* 例： `switch(config-if)# mac access-group acl-01`	指定の方向に流れるトラフィックを対象に、PACL をインターフェイスに適用します。 （注） インターフェイスは、PACL を 1 つだけ保有できます。インターフェイス上の PACL を交換する場合は、新しい PACL 名でこのコマンドを再度入力します。

ステップ 4	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		グローバル コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 5	**show running-config interface** 例： `switch(config)# show running-config interface`	（任意） インターフェイスの PACL 設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスでの NAC のイネーブル化

ポスチャ検証を行うには、インターフェイス上で NAC をイネーブルにする必要があります。

はじめる前に

EAPoUDP をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port*
3. **switchport**
4. **switchport mode access**
5. **nac enalbe**
6. **exit**
7. （任意） **show running-config interface**
8. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 2	**interface ethernet***slot/port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		イーサネット インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**switchport** 例： `switch(config-if)# switchport`	インターフェイスをレイヤ 2 スイッチング インターフェイスとして設定します。デフォルトでは、すべてのポートがレイヤ 3 ポートです。
ステップ 4	**switchport mode access** 例： `switch(config-if)# switchport mode access`	ポート モードをアクセスとして設定します。
ステップ 5	**nac enalbe** 例： `switch(config-if)# nac enable`	インターフェイスで NAC をイネーブルにします。

ステップ 6	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 7	**show running-config interface** 例： `switch(config)# show running-config interface`	（任意） インターフェイスの PACL 設定を表示します。
ステップ 8	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

EAPoUDP のイネーブル化, （379 ページ）

アイデンティティ ポリシーおよびアイデンティティ プロファイル エントリの設定

アイデンティティ プロファイルを使用して LPIP ポスチャ検証の例外を設定できます。アイデンティティ プロファイルには、LPIP 検証の際に対象外とするエンドポイント装置のエントリも含め

ます。オプションとして、アイデンティティプロファイルごとにアイデンティティポリシーを設定し、そのポリシーにNX-OSデバイスがエンドポイント装置に適用するPACLを指定することができます。デフォルトのアイデンティティ ポリシーは、インターフェイスのPACLです。

はじめる前に

EAPoUDP をイネーブルにします。

手順の概要

1. **configure terminal**
2. **identity policy***policy-name*
3. **object-group***access-list*
4. （任意） **description "***text***"**
5. **exit**
6. （任意） **show identity policy**
7. **identity profile eapoudp**
8. **device** {**authenticate** | **not-authenticate**} {**ip-address***ipv4-address* [*ipv4-subnet-mask*] | **mac-address***mac-address* [*mac-subnet-mask*]} **policy***name*
9. **exit**
10. （任意） **show identity profile eapoudp**
11. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**identity policy***policy-name*
	
	例：
	`switch(config)# identity policy AccType1`
	`switch(config-id-policy)#`
		アイデンティティ ポリシー名を指定し、アイデンティティ ポリシー コンフィギュレーション モードを開始します。最大 1024 のアイデンティティ ポリシーを作成できます。名前の最大長は 100 文字です。

ステップ 3	**object-group***access-list* 例： `switch(config-id-policy)# object-group maxaclx`	ポリシーの IP ACP または MAC ACL を指定します。

	コマンドまたはアクション	目的
ステップ 4	**description "***text***"** 例： `switch(config-id-policy)# description "This policy prevents endpoint device without a PA"`	（任意） アイデンティティ ポリシーの説明を記します。最大長は 100 文字です。

ステップ 5	**exit**
	
	例：
	`switch(config-id-policy)# exit`
	`switch(config)#`
		アイデンティティ ポリシー コンフィギュレーション モードを終了します。

ステップ 6	**show identity policy** 例： `switch(config)# show identity policy`	（任意） アイデンティティ ポリシーの設定を表示します。

ステップ 7	**identity profile eapoudp**
	
	例：
	`switch(config)# identity profile eapoudp`
	`switch(config-id-prof)#`
		EAPoUDP のアイデンティティ プロファイル コンフィギュレーション モードを開始します。

ステップ 8	**device** {**authenticate** | **not-authenticate**} {**ip-address***ipv4-address* [*ipv4-subnet-mask*] | **mac-address***mac-address* [*mac-subnet-mask*]} **policy***name* 例： `switch(config-id-prof)# device authenticate ip-address 10.10.2.2 policy AccType1`	例外エントリを指定します。エントリの最大数は 5000 です。

ステップ 9	**exit**
	
	例：
	`switch(config-id-prof)# exit`
	`switch(config)#`
		アイデンティティ プロファイル コンフィギュレーション モードを終了します。

ステップ 10	**show identity profile eapoudp** 例： `switch(config)# show identity profile eapoudp`	（任意） アイデンティティ プロファイルの設定を表示します。
ステップ 11	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

EAPoUDP のイネーブル化, （379 ページ）

クライアントレス エンドポイント装置の検証

ネットワーク内の PA 未搭載（クライアントレス）のエンドポイント装置に対してポスチャ検証を実行できます。このポスチャ検証は、エンドポイント装置にアクセスできる監査サーバが実行します。

はじめる前に

EAPoUDP をイネーブルにします。

AAA サーバとクライアントレス エンドポイント装置が監査サーバにアクセスできることを確認します。

手順の概要

1. **configure terminal**
2. **eou allow clientless**
3. **exit**
4. （任意） **show eou**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**eou allow clientless** 例： `switch(config)# eou allow clientless`	クライアントレス エンドポイント装置のポスチャ検証を可能にします。デフォルトではディセーブルになっています。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 4	**show eou** 例： `switch# show eou`	（任意） EAPoUDP の設定を表示します。

	コマンドまたはアクション	目的
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

EAPoUDP のイネーブル化, （379 ページ）

EAPoUDP のロギングのイネーブル化

EAPoUDPイベント メッセージのロギングをイネーブルにできます。EAPoUDPイベントには、エラーやステータスの変化などが含まれます。これらのイベント メッセージは、設定されている syslog に送られます。

はじめる前に

EAPoUDP をイネーブルにします。

手順の概要

1. **configure terminal**
2. **eou logging**
3. **exit**
4. （任意） **show eou**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**eou logging** 例： `switch(config)# eou logging`	EAPoUDP ロギングをイネーブルにします。デフォルトではディセーブルになっています。

	コマンドまたはアクション	目的

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 4	**show eou** 例： `switch)# show eou`	（任意） EAPoUDP の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

EAPoUDP のイネーブル化, （379 ページ）

EAPoUDP のグローバル最大リトライ回数の変更

EAPoUDP のグローバル最大リトライ回数を変更できます。デフォルト値は 3 です。

はじめる前に

EAPoUDP をイネーブルにします。

手順の概要

1. **configure terminal**
2. **eou max-retry***count*
3. **exit**
4. （任意） **show eou**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**eou max-retry***count* 例： `switch(config)# eou max-retry 2`	EAPoUDP の最大リトライ回数を変更します。デフォルトは 3 です。有効な範囲は 1 ～ 3 です。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 4	**show eou** 例： `switch# show eou`	（任意） EAPoUDP の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

EAPoUDP のイネーブル化，（379 ページ）
個別インターフェイスの EAPoUDP 最大リトライ回数の変更，（390 ページ）

個別インターフェイスの EAPoUDP 最大リトライ回数の変更

個別インターフェイスの EAPoUDP 最大リトライ回数を変更できます。デフォルト値は 3 です。

はじめる前に

EAPoUDP をイネーブルにします。

インターフェイスで NAC をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port*
3. **eou max-retry***count*
4. **exit**
5. （任意） **show eou**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet***slot*/*port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		イーサネット インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**eou max-retry***count* 例： `switch(config-if)# eou max-retry 2`	EAPoUDP の最大リトライ回数を変更します。デフォルトは 3 です。有効な範囲は 1 ～ 3 です。

ステップ 4	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 5	**show eou** 例： `switch(config)# show eou`	（任意） EAPoUDP の設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

EAPoUDP のイネーブル化，（379 ページ）

EAPoUDP のグローバル最大リトライ回数の変更，（389 ページ）
インターフェイスでの NAC のイネーブル化，（383 ページ）

EAPoUDP の UDP ポートの変更

EAPoUDP で使用される UDP ポートを変更できます。デフォルト ポートは 21862 です。

はじめる前に

EAPoUDP をイネーブルにします。

手順の概要

1. **configure terminal**
2. **eou port***udp-port*
3. **exit**
4. （任意） **show eou**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**eou port***udp-port* 例： `switch(config)# eou port 27180`	EAPoUDP で使用される UDP ポートを変更します。デフォルトは 21862 です。有効な範囲は 1 ～ 65535 です。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 4	**show eou** 例： `switch# show eou`	（任意） EAPoUDP の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

EAPoUDP のイネーブル化, （379 ページ）

EAPoUDPポスチャ検証の同時セッション数に関するレート制限の設定

EAPoUDP ポスチャ検証の同時セッション数を制御するレート制限を設定できます。EAPoUDP ポスチャ検証の最大同時セッション数を制御するレート制限値を変更できます。デフォルト値は 20 です。ゼロ（0）に設定すると、レート制限はディセーブルになります。

はじめる前に

EAPoUDP をイネーブルにします。

手順の概要

1. **configure terminal**
2. **eou ratelimit***number-of-sessions*
3. **exit**
4. （任意） **show eou**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**eou ratelimit***number-of-sessions* 例： `switch(config)# eou ratelimit 15`	EAPoUDP ポスチャ検証の同時セッション数を設定します。デフォルトは 20 です。範囲は 0 ～ 200 です。 （注） ゼロ（0）に設定すると、レート制限はディセーブルになります。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 4	**show eou** 例： `switch# show eou`	（任意） EAPoUDP の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

EAPoUDP のイネーブル化, （379 ページ）

グローバル自動ポスチャ再検証の設定

Cisco NX-OS ソフトウェアは、設定された間隔で Cisco NX-OS デバイスのエンドポイント装置のポスチャを自動的に再検証します。デフォルトの間隔は 36,000 秒（10 時間）です。再検証をディセーブルにしたり、再検証の間隔を変更することができます。

はじめる前に

EAPoUDP をイネーブルにします。

手順の概要

1. **configure terminal**
2. （任意） **eou revalidate**
3. （任意） **eou timeout revalidation***seconds*
4. **exit**
5. （任意） **show eou**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**eou revalidate** 例： `switch(config)# eou revalidate`	（任意） 自動ポスチャ検証をイネーブルにします。デフォルトではイネーブルになっています。
ステップ 3	**eou timeout revalidation***seconds* 例： `switch(config)# eou timeout revalidation 30000`	（任意） 再検証タイマーの間隔を変更します。デフォルト値は 36000 です。指定できる範囲は 5 ～ 86400 秒です。 自動ポスチャ検証をディセーブルにするには、**no eou revalidate** コマンドを使用します。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 5	**show eou** 例： `switch# show eou`	（任意） EAPoUDP の設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

EAPoUDP のイネーブル化, （379 ページ）
個別インターフェイスでの自動ポスチャ再検証の設定, （395 ページ）

個別インターフェイスでの自動ポスチャ再検証の設定

Cisco NX-OS ソフトウェアは、設定された間隔で Cisco NX-OS デバイスのエンドポイント装置のポスチャを自動的に再検証します。デフォルトの間隔は 36,000 秒（10 時間）です。再検証をディセーブルにしたり、再検証の間隔を変更することができます。

はじめる前に

EAPoUDP をイネーブルにします。

インターフェイスで NAC をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface ethernet** *slot/port*
3. （任意） **eou revalidate**
4. （任意） **eou timeout revalidation***seconds*
5. **exit**
6. （任意） **show eou**
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet** *slot/port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		イーサネットインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**eou revalidate** 例： `switch(config-if)# eou revalidate`	（任意） 自動ポスチャ検証をイネーブルにします。デフォルトではイネーブルになっています。 自動ポスチャ検証をディセーブルにするには、**no eou revalidate** コマンドを使用します。
ステップ 4	**eou timeout revalidation***seconds* 例： `switch(config-if)# eou timeout revalidation 30000`	（任意） 再検証タイマーの間隔を変更します。デフォルト値は 36000 です。指定できる範囲は 5 ～ 86400 秒です。

ステップ 5	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 6	**show eou** 例： `switch(config)# show eou`	（任意） EAPoUDP の設定を表示します。

	コマンドまたはアクション	目的
ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

EAPoUDP のイネーブル化，（379 ページ）
グローバル自動ポスチャ再検証の設定，（394 ページ）
インターフェイスでの NAC のイネーブル化，（383 ページ）

EAPoUDP グローバル タイマーの変更

Cisco NX-OS ソフトウェアは、EAPoUDP の次のグローバル タイマーをサポートしています。

AAA

ポスチャ検証の実行中に、NAD が要求を再送信する前に AAA サーバからの応答を待機する時間を制御します。

ホールド時間

EAPoUDP セッションの失敗を検証する試みのあとに、すぐに次の新規セッションが開始されないように抑制します。NAC はこのタイマーを、Cisco Secure ACS が Accept-Reject メッセージを NAD に送信した場合にだけ使用します。

再送信

ポスチャ検証の実行中に、NAD が要求を再送信する前にクライアントからの応答を待機する時間を制御します。

再検証

ポスチャ検証の実行中に EAPoUDP メッセージを使用していたエンドポイント装置に対し、NAD が NAC ポリシーを適用する期間を制御します。このタイマーは、最初のポスチャ検証が完了した時点で開始されます。

ステータス クエリー

以前検証したクライアントが存在し、そのポスチャが変更されていないことを確認するまでの、NAD の待機時間を制御します。EAPoUDP メッセージによって認証されたクライアントだけが、このタイマーを使用します。このタイマーは、クライアントの最初の検証が完了した時点で開始されます。

はじめる前に

EAPoUDP をイネーブルにします。

手順の概要

1. **configure terminal**
2. （任意） **eou timeout aaa***seconds*
3. （任意） **eou timeout hold-period***seconds*
4. （任意） **eou timeout retransmit***seconds*
5. （任意） **eou timeout revalidation***seconds*
6. （任意） **eou timeout status-query***seconds*
7. **exit**
8. （任意） **show eou**
9. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**eou timeout aaa***seconds* 例： `switch(config)# eou timeout aaa 30`	（任意） AAA タイムアウト間隔を変更します。デフォルト値は 60 秒（1 分）です。有効な範囲は 0 ～ 60 秒です。
ステップ 3	**eou timeout hold-period***seconds* 例： `switch(config)# eou timeout hold-period 300`	（任意） ホールド時間タイムアウト間隔を変更します。デフォルト値は 180 秒（3 分）です。範囲は 60 ～ 86400 秒です。
ステップ 4	**eou timeout retransmit***seconds* 例： `switch(config)# eou timeout retransmit 10`	（任意） 再送信タイムアウト間隔を変更します。デフォルトは 3 秒です。有効な範囲は 1 ～ 60 秒です。
ステップ 5	**eou timeout revalidation***seconds* 例： `switch(config)# eou timeout revalidation 30000`	（任意） 再検証タイマーの間隔を変更します。デフォルト値は 36000 です。指定できる範囲は 5 ～ 86400 秒です。

	コマンドまたはアクション	目的
ステップ 6	**eou timeout status-query***seconds* 例： `switch(config)# eou timeout status-query 360`	（任意） ステータス クエリー タイムアウト間隔を変更します。デフォルトは 300 秒（5 分）です。有効な範囲は 10 ～ 1800 秒です。

ステップ 7	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 8	**show eou** 例： `switch# show eou`	（任意） EAPoUDP の設定を表示します。
ステップ 9	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

EAPoUDP のイネーブル化，（379 ページ）
個別インターフェイスでの EAPoUDP タイマーの変更，（399 ページ）
NAC タイマー，（372 ページ）

個別インターフェイスでの EAPoUDP タイマーの変更

Cisco NX-OS ソフトウェアは、NAC がイネーブルになっている各インターフェイスで、EAPoUDP に関する次のタイマーをサポートしています。

AAA

ポスチャ検証の実行中に、NAD が要求を再送信する前に AAA サーバからの応答を待機する時間を制御します。

ホールド時間

EAPoUDP セッションの失敗を検証する試みのあとに、すぐに次の新規セッションが開始されないように抑制します。NAC はこのタイマーを、Cisco Secure ACS が Accept-Reject メッセージを NAD に送信した場合にだけ使用します。

再送信

ポスチャ検証の実行中に、NAD が要求を再送信する前にクライアントからの応答を待機する時間を制御します。

再検証

ポスチャ検証の実行中にEAPoUDPメッセージを使用していたエンドポイント装置に対し、NADがNACポリシーを適用する期間を制御します。このタイマーは、最初のポスチャ検証が完了した時点で開始されます。

ステータス クエリー

以前検証したクライアントが存在し、そのポスチャが変更されていないことを確認するまでの、NADの待機時間を制御します。EAPoUDPメッセージによって認証されたクライアントだけが、このタイマーを使用します。このタイマーは、クライアントの最初の検証が完了した時点で開始されます。

はじめる前に

EAPoUDP をイネーブルにします。

インターフェイスで NAC をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port*
3. （任意） **eou timeout aaa***seconds*
4. （任意） **eou timeout hold-period***seconds*
5. （任意） **eou timeout retransmit***seconds*
6. （任意） **eou timeout revalidation***seconds*
7. （任意） **eou timeout status-query***seconds*
8. **exit**
9. （任意） **show eou**
10. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 2	**interface ethernet***slot/port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		イーサネットインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**eou timeout aaa***seconds* 例： `switch(config-if)# eou timeout aaa 50`	（任意） AAA タイムアウト間隔を変更します。デフォルト値は 60 秒（1 分）です。有効な範囲は 0 ～ 60 秒です。
ステップ 4	**eou timeout hold-period***seconds* 例： `switch(config-if)# eou timeout hold-period 300`	（任意） ホールド時間タイムアウト間隔を変更します。デフォルト値は 180 秒（3 分）です。範囲は 60 ～ 86400 秒です。
ステップ 5	**eou timeout retransmit***seconds* 例： `switch(config-if)# eou timeout retransmit 10`	（任意） 再送信タイムアウト間隔を変更します。デフォルトは 3 秒です。有効な範囲は 1 ～ 60 秒です。
ステップ 6	**eou timeout revalidation***seconds* 例： `switch(config-if)# eou timeout revalidation 30000`	（任意） 再検証タイマーの間隔を変更します。デフォルト値は 36000 です。指定できる範囲は 5 ～ 86400 秒です。
ステップ 7	**eou timeout status-query***seconds* 例： `switch(config-if)# eou timeout status-query 360`	（任意） ステータス クエリー タイムアウト間隔を変更します。デフォルトは 300 秒（5 分）です。有効な範囲は 10 ～ 1800 秒です。

ステップ 8	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 9	**show eou** 例： `switch(config)# show eou`	（任意） EAPoUDP の設定を表示します。
ステップ 10	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

EAPoUDP のイネーブル化, （379 ページ）
EAPoUDP グローバル タイマーの変更, （397 ページ）
NAC タイマー, （372 ページ）
インターフェイスでの NAC のイネーブル化, （383 ページ）

EAPoUPD グローバル設定のデフォルト値へのリセット

EAPoUDP グローバル設定をデフォルト値にリセットできます。

はじめる前に

EAPoUDP をイネーブルにします。

手順の概要

1. **configure terminal**
2. **eou default**
3. **exit**
4. （任意） **show eou**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**eou default** 例： `switch(config)# eou default`	EAPoUDP 設定をデフォルト値にリセットします。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 4	**show eou** 例： `switch# show eou`	（任意） EAPoUDP の設定を表示します。

	コマンドまたはアクション	目的
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

EAPoUDP のイネーブル化，（379 ページ）
EAPoUPD インターフェイス設定のデフォルト値へのリセット，（403 ページ）

EAPoUPD インターフェイス設定のデフォルト値へのリセット

インターフェイスの EAPoUDP 設定をデフォルト値にリセットできます。

はじめる前に

EAPoUDP をイネーブルにします。

インターフェイスで NAC をイネーブルにします。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port*
3. **eou default**
4. **exit**
5. （任意） **show eou interface ethernet** *slot*/*port*
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 2	**interface ethernet***slot/port*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		イーサネットインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**eou default** 例： `switch(config-if)# eou default`	インターフェイスの EAPoUDP 設定をデフォルト値にリセットします。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 5	**show eou interface ethernet** *slot/port* 例： `switch(config)# show eou interface ethernet 2/1`	（任意） EAPoUDP の設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

EAPoUDP のイネーブル化，（379 ページ）
EAPoUPD グローバル設定のデフォルト値へのリセット，（402 ページ）
インターフェイスでの NAC のイネーブル化，（383 ページ）

IP デバイス トラッキングの設定

IP デバイス トラッキングを設定できます。AAA サーバに対する IP デバイス トラッキングの処理は、次のようになります。

- Cisco NX-OS デバイスが新しいセッションを検出します。
- ポスチャ検証のトリガー前に AAA サーバが到達不能であれば、Cisco NX-OS デバイスは IP デバイス トラッキング ポリシーを適用し、セッションのステートを AAA DOWN にします。
- AAA サーバが再度使用可能になると、ホストの再検証が実行されます。

（注） AAA サーバの停止時は、エンドポイント装置に他の既存のポリシーが関連付けられていない場合だけ、Cisco NX-OS デバイスが IP トラッキング ポリシーを適用します。再検証中に AAA サーバが停止した場合は、Cisco NX-OS デバイスはエンドポイント装置に使用されているポリシーを保持します。

手順の概要

1. **configure terminal**
2. **ip device tracking enable**
3. （任意） **ip device tracking probe** {**count***count* | **interval***seconds*}
4. （任意） **radius-server host** {*hostname* | *ip-address*} **test** [**username***username* [**password***password*]] [**idle-time***minutes*]
5. **exit**
6. （任意） **show ip device tracking all**
7. （任意） **show radius-server** {*hostname* | *ip-address*}
8. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**ip device tracking enable** 例： `switch(config)# ip device tracking enable`	IP デバイス トラッキングをイネーブルにします。デフォルトの状態はイネーブルです。
ステップ 3	**ip device tracking probe** {**count***count* | **interval***seconds*} 例： `switch(config)# ip device tracking probe count 4`	（任意） IP デバイス トラッキング テーブルに対し、次のパラメータを設定します。 **count** Cisco NX-OS デバイスが ARP プローブを送信する回数を設定します。指定できる範囲は 1 ～ 5 です。デフォルトは 3 です。

	コマンドまたはアクション	目的
		interval Cisco NX-OS デバイスが ARP プローブを再送する前に、応答を待機する秒数を設定します。有効な範囲は 1 ～ 302300 秒です。デフォルトは 30 秒です。
ステップ 4	**radius-server host** {*hostname* | *ip-address*} **test** [**username***username* [**password***password*]] [**idle-time***minutes*] 例： `switch(config)# radius-server host 10.10.1.1 test username User2 password G1r2D37&k idle-time 5`	（任意） RADIUS サーバのテスト パケットのパラメータを設定します。デフォルトのユーザ名は test、デフォルトのパスワードは test です。 **idle-time** パラメータには、サーバの動作ステータスを確認するために行うサーバテストの実行頻度を設定します。RADIUS サーバへのトラフィックがない場合は、NAD はこのアイドル タイマーの値に基づき、RADIUS サーバにダミーのパケットを送信します。アイドル タイマーのデフォルト値は 0 分です（ディセーブル）。 複数の RADIUS サーバがある場合は、このコマンドを再度入力します。
ステップ 5	**exit** 例： `switch(config)# exit switch#`	グローバル コンフィギュレーション モードを終了します。
ステップ 6	**show ip device tracking all** 例： `switch# show ip device tracking all`	（任意） IP デバイス トラッキングの情報を表示します。
ステップ 7	**show radius-server** {*hostname* | *ip-address*} 例： `switch# show radius-server 10.10.1.1`	（任意） RADIUS サーバ情報を表示します。
ステップ 8	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

EAPoUDP のイネーブル化, （379 ページ）

IP デバイス トラッキングのクリア

AAA サーバの IP トラッキング情報をクリアできます。

手順の概要

1. （任意） **clear ip device tracking all**
2. （任意） **clear ip device tracking interface ethernet***slot*/*port*
3. （任意） **clear ip device tracking ip-address***ipv4-address*
4. （任意） **clear ip device tracking mac-address***mac-address*
5. （任意） **show ip device tracking all**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**clear ip device tracking all** 例： `switch# clear ip device tracking all`	（任意） すべてのEAPoUDPセッションをクリアします。
ステップ 2	**clear ip device tracking interface ethernet***slot*/*port* 例： `switch# clear ip device tracking interface ethernet 2/1`	（任意） 指定のインターフェイス上のEAPoUDPセッションをクリアします。
ステップ 3	**clear ip device tracking ip-address***ipv4-address* 例： `switch# clear ip device tracking ip-address 10.10.1.1`	（任意） 指定の IPv4 アドレス（A.B.C.D 形式）の EAPoUDP セッションをクリアします。
ステップ 4	**clear ip device tracking mac-address***mac-address* 例： `switch# clear ip device tracking mac-address 000c.30da.86f4`	（任意） 指定の MAC アドレス（XXXX.XXXX.XXXX 形式）の EAPoUDP セッションをクリアします。
ステップ 5	**show ip device tracking all** 例： `switch# show ip device tracking all`	（任意） IP デバイス トラッキングの情報を表示します。

手動による EAPoUDP セッションの初期化

手動で EAPoUDP セッションを初期化できます。

はじめる前に

EAPoUDP をイネーブルにします。

手順の概要

1. （任意） **eou initialize all**
2. （任意） **eou initialize authentication** {**clientless** | **eap** | **static**}
3. （任意） **eou initialize interface ethernet***slot*/*port*
4. （任意） **eou initialize ip-address***ipv4-address*
5. （任意） **eou initialize mac-address***mac-address*
6. （任意） **eou initialize posturetoken***name*
7. （任意） **show eou all**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**eou initialize all** 例： `switch# eou initialize all`	（任意） すべての EAPoUDP セッションを初期化します。
ステップ 2	**eou initialize authentication** {**clientless** | **eap** | **static**} 例： `switch# eou initialize authentication static`	（任意） 指定の認証タイプの EAPoUDP セッションを初期化します。
ステップ 3	**eou initialize interface ethernet***slot*/*port* 例： `switch# eou initialize interface ethernet 2/1`	（任意） 指定のインターフェイス上の EAPoUDP セッションを初期化します。
ステップ 4	**eou initialize ip-address***ipv4-address* 例： `switch# eou initialize ip-address 10.10.1.1`	（任意） 指定の IPv4 アドレス（A.B.C.D 形式）の EAPoUDP セッションを初期化します。

	コマンドまたはアクション	目的
ステップ 5	**eou initialize mac-address***mac-address* 例： `switch# eou initialize mac-address 000c.30da.86f4`	（任意） 指定の MAC アドレス（XXXX.XXXX.XXXX 形式）の EAPoUDP セッションを初期化します。
ステップ 6	**eou initialize posturetoken***name* 例： `switch# eou initialize posturetoken Healthy`	（任意） 指定のポスチャ トークン名の EAPoUDP セッションを初期化します。 （注） トークン名を表示する場合は、**show eou all** コマンドを使用します。
ステップ 7	**show eou all** 例： `switch# show eou all`	（任意） EAPoUDP セッションの設定を表示します。

関連トピック

EAPoUDP のイネーブル化, （379 ページ）

手動による EAPoUDP セッションの再検証

手動で EAPoUDP セッションを再検証できます。

はじめる前に

EAPoUDP をイネーブルにします。

手順の概要

1. （任意） **eou revalidate all**
2. （任意） **eou revalidate authentication** {**clientless** | **eap** | **static**}
3. （任意） **eou revalidate interface ethernet***slot*/*port*
4. （任意） **eou revalidate ip-address***ipv4-address*
5. （任意） **eou revalidate mac-address***mac-address*
6. （任意） **eou revalidate posturetoken***name*
7. （任意） **show eou all**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**eou revalidate all** 例： `switch# eou revalidate all`	（任意） すべての EAPoUDP セッションを再検証します。
ステップ 2	**eou revalidate authentication** {**clientless** | **eap** | **static**} 例： `switch# eou revalidate authentication static`	（任意） 指定の認証タイプの EAPoUDP セッションを再検証します。
ステップ 3	**eou revalidate interface ethernet***slot/port* 例： `switch# eou revalidate interface ethernet 2/1`	（任意） 指定のインターフェイス上の EAPoUDP セッションを再検証します。
ステップ 4	**eou revalidate ip-address***ipv4-address* 例： `switch# eou revalidate ip-address 10.10.1.1`	（任意） 指定の IPv4 アドレスの EAPoUDP セッションを再検証します。
ステップ 5	**eou revalidate mac-address***mac-address* 例： `switch# eou revalidate mac-address 000c.30da.86f4`	（任意） 指定の MAC アドレスの EAPoUDP セッションを再検証します。
ステップ 6	**eou revalidate posturetoken***name* 例： `switch# eou revalidate posturetoken Healthy`	（任意） 指定のポスチャ トークン名の EAPoUDP セッションを再検証します。 （注）　トークン名を表示する場合は、**show eou all** コマンドを使用します。
ステップ 7	**show eou all** 例： `switch# show eou all`	（任意） EAPoUDP セッションの設定を表示します。

関連トピック

EAPoUDP のイネーブル化, （379 ページ）

EAPoUDP セッションのクリア

EAPoUDP セッションを Cisco NX-OS デバイスからクリアできます。

はじめる前に

EAPoUDP をイネーブルにします。

手順の概要

1. （任意） **clear eou all**
2. （任意） **clear eou authentication** {**clientless** | **eap** | **static**}
3. （任意） **clear eou interface ethernet***slot*/*port*
4. （任意） **clear eou ip-address***ipv4-address*
5. （任意） **clear eou mac-address***mac-address*
6. （任意） **clear eou posturetoken***name*
7. （任意） **show eou all**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**clear eou all** 例： `switch# clear eou all`	（任意） すべての EAPoUDP セッションをクリアします。
ステップ 2	**clear eou authentication** {**clientless** | **eap** | **static**} 例： `switch# clear eou authentication static`	（任意） 指定の認証タイプの EAPoUDP セッションをクリアします。
ステップ 3	**clear eou interface ethernet***slot*/*port* 例： `switch# clear eou interface ethernet 2/1`	（任意） 指定のインターフェイス上の EAPoUDP セッションをクリアします。
ステップ 4	**clear eou ip-address***ipv4-address* 例： `switch# clear eou ip-address 10.10.1.1`	（任意） 指定の IPv4 アドレスの EAPoUDP セッションをクリアします。
ステップ 5	**clear eou mac-address***mac-address* 例： `switch# clear eou mac-address 000c.30da.86f4`	（任意） 指定の MAC アドレスの EAPoUDP セッションをクリアします。

	コマンドまたはアクション	目的
ステップ 6	**clear eou posturetoken***name* 例： `switch# clear eou posturetoken Healthy`	（任意） 指定のポスチャ トークン名の EAPoUDP セッションをクリアします。 （注） トークン名を表示する場合は、**show eou all** コマンドを使用します。
ステップ 7	**show eou all** 例： `switch# show eou all`	（任意） EAPoUDP セッションの設定を表示します。

関連トピック

EAPoUDP のイネーブル化, （379 ページ）

EAPoUDP 機能のディセーブル化

Cisco NX-OS デバイス上の EAPoUDP 機能をディセーブルにできます。

注意 EAPoUDP をディセーブルにすると、Cisco NX-OS デバイスからすべての EAPoUDP 設定が削除されます。

はじめる前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順の概要

1. **configure terminal**
2. **no feature eou**
3. **exit**
4. （任意） **show feature**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**no feature eou** 例： `switch(config)# no feature eou`	EAPoUDP をディセーブルにします。 **注意** EAPoUDP 機能をディセーブルにすると、すべての EAPoUDP 設定が削除されます。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	**show feature** 例： `switch# show feature`	（任意） Cisco NX-OS 機能のイネーブルまたはディセーブル ステータスを表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

NAC の設定の確認

NAC の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show eou [**all** | **authentication** {**clientless** | **eap** | **static**} | **interface ethernet***slot*/*port* | **ip-address***ipv4-address* | **mac-address***mac-address* | **posturetoken***name*]	EAPoUDP の設定を表示します。
show ip device tracking [**all** | **interface ethernet***slot*/*port* | **ip-address***ipv4-address* | **mac-address***mac-address*]	IP デバイス トラッキングの情報を表示します。
show running-config eou [**all**]	実行コンフィギュレーション内の EAPoUDP 設定を表示します。

コマンド	目的
show startup-config eou	スタートアップ コンフィギュレーション内の EAPoUDP 設定を表示します。

このコマンドの出力フィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

NAC の設定例

次に、NAC を設定する例を示します。

```
feature eou
aaa authentication eou default group radius
mac access-list macacl-01
  10 permit any any 0x100
interface Ethernet8/1
  mac access-group macacl-01
```

NAC に関する追加情報

ここでは、NAC に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS のライセンス	『*Cisco NX-OS Licensing Guide*』
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』

NAC の機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 *25*：*NAC* の機能の履歴

機能名	リリース	機能情報
NAC	6.0(1)	Release 5.2 以降、変更はありません。

機能名	リリース	機能情報
NAC	5.2(1)	Release 5.1 以降、変更はありません。
NAC	5.1(1)	Release 5.0 以降、変更はありません。
NAC	5.0(2)	Release 4.2 以降、変更はありません。

第 13 章

Cisco TrustSec の設定

この章では、Cisco NX-OS デバイスに Cisco TrustSec を設定する手順について説明します。

この章は、次の項で構成されています。

- 機能情報の確認，417 ページ
- Cisco TrustSec の概要，418 ページ
- Cisco TrustSec のライセンス要件，437 ページ
- Cisco TrustSec の前提条件，437 ページ
- Cisco TrustSec の注意事項と制約事項，438 ページ
- Cisco TrustSec パラメータのデフォルト設定，440 ページ
- Cisco TrustSec の設定，440 ページ
- サブネットと SGT のマッピングの設定，499 ページ
- ポート チャネル メンバでの Cisco TrustSec サポート，500 ページ
- Cisco TrustSec の設定の確認，501 ページ
- Cisco TrustSec の設定例，504 ページ
- Cisco TrustSec に関する追加情報，508 ページ
- Cisco TrustSec の機能の履歴，508 ページ

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリス

トについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

Cisco TrustSec の概要

ここでは、Cisco TrustSec について説明します。

Cisco TrustSec のアーキテクチャ

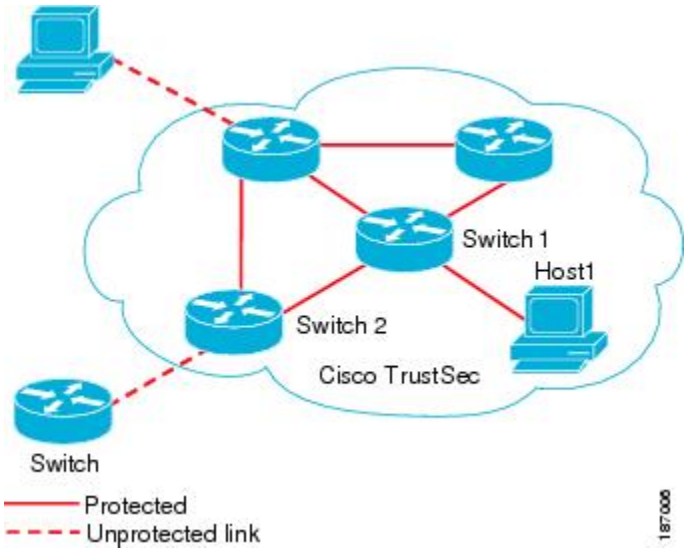
Cisco TrusSec のセキュリティ アーキテクチャは、信頼できるネットワーク デバイスのクラウドを確立することによってセキュア ネットワークを構築します。クラウド内の各デバイスは、そのネイバーによって認証されます。クラウド内のデバイス間リンクでの通信は、暗号化、メッセージ整合性検査、データパス リプレイ防止メカニズムを組み合わせたセキュリティで保護されます。また Cisco TrustSec は、認証時に取得されたデバイスおよびユーザの識別情報を、ネットワークに入る際のパケットの分類またはカラリングに使用します。このパケット分類は、Cisco TrustSec ネットワークへの入力時にパケットにタグ付けされることにより維持されます。タグによってパケットはデータ パス全体を通じて正しく識別され、セキュリティおよびその他のポリシー基準が適用されます。このタグは、セキュリティ グループ タグ（SGT）と呼ばれることもあります。エンドポイント装置が SGT に応じてトラフィックをフィルタリングできるようにすることにより、アクセス コントロール ポリシーをネットワークに強制できます。

（注） 入力とは、宛先へのパス上のパケットが最初の Cisco TrustSec 対応デバイスに入ることです。出力とは、パス上の最後の Cisco TrustSec 対応デバイスを出ることです。

次の図に、Cisco TrustSec クラウドの例を示します。この例では、Cisco TrustSec クラウド内に、ネットワーク接続されたデバイスが数台とエンドポイント装置が 1 台あります。エンドポイント

装置 1 台とネットワーク接続デバイス 1 台がクラウドの外部にあるのは、これらが Cisco TrustSec 対応デバイスでないか、またはアクセスを拒否されたからです。

図 *12* : ***Cisco TrustSec*** ネットワーク クラウドの例



Cisco TrustSec アーキテクチャは、主に次のコンポーネントで構成されています。

認証

Cisco TrustSec ネットワークにデバイスを加入させる前に、各デバイスの識別情報を検証します。

許可

認証されたデバイスの識別情報に基づいて、Cisco TrustSec ネットワークのリソースに対するデバイスのアクセス権のレベルを決定します。

アクセス コントロール

各パケットのソース タグを使用して、パケット単位でアクセス ポリシーを適用します。

セキュアな通信

Cisco TrustSec ネットワークの各リンク上のパケットに、暗号化、整合性検査、およびデータパス リプレイ防止を提供します。

Cisco TrustSec ネットワークには、次のエンティティがあります。

サプリカント

Cisco TrustSec ネットワークへの加入を試行するデバイス

オーセンティケータ（AT）

すでに Cisco TrustSec ネットワークに含まれているデバイス

許可サーバ

認証情報、許可情報、またはその両方を提供できるサーバ

サプリカントと AT の間のリンクの初回の確立時には、次の一連のイベントが発生します。

認証（802.1X）

認証サーバがサプリカントの認証を実行します。または、これらのデバイスが無条件に相互認証するように設定している場合は認証がそのまま完了します。

許可

リンクの両側が、そのリンクに適用する SGT および ACL などのポリシーを取得します。サプリカントは、認証サーバへの他のレイヤ 3 ルートがない場合には、AT をリレーとして使用する必要があります。

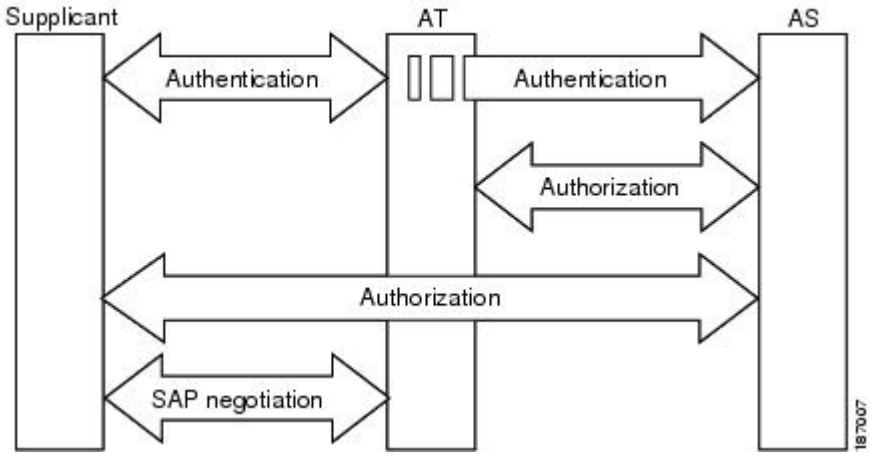
セキュリティ アソシエーション プロトコル（SAP）ネゴシエーション

サプリカントと AT の間で、EAPOL-Key が交換され、暗号スイートのネゴシエーション、セキュリティ パラメータ インデックス（SPI）の交換、およびキーの管理が実行されます。これら 3 つの作業が正常に完了すると、セキュリティ アソシエーション（SA）が確立します。

SAP ネゴシエーションが完了するまで、ポートは無許可ステート（ブロッキング ステート）です。

次の図に、SAP ネゴシエーションを示します。この図では、SAP ネゴシエーションが完了するまで、ポートが無許可ステートであることも示しています。

図 *13*：*SAP* ネゴシエーション



SAP ネゴシエーションには、次のいずれかの動作モードを使用します。

- Galois/Counter Mode（GCM）暗号化
- GCM 認証（GMAC）

- カプセル化なし（クリア テキスト）
- 暗号化も認証もなしのカプセル化

Cisco TrustSec は、IEEE 802.1AE 規格に基づいて、ESP-128 GCM および GMAC を使用します。

認証

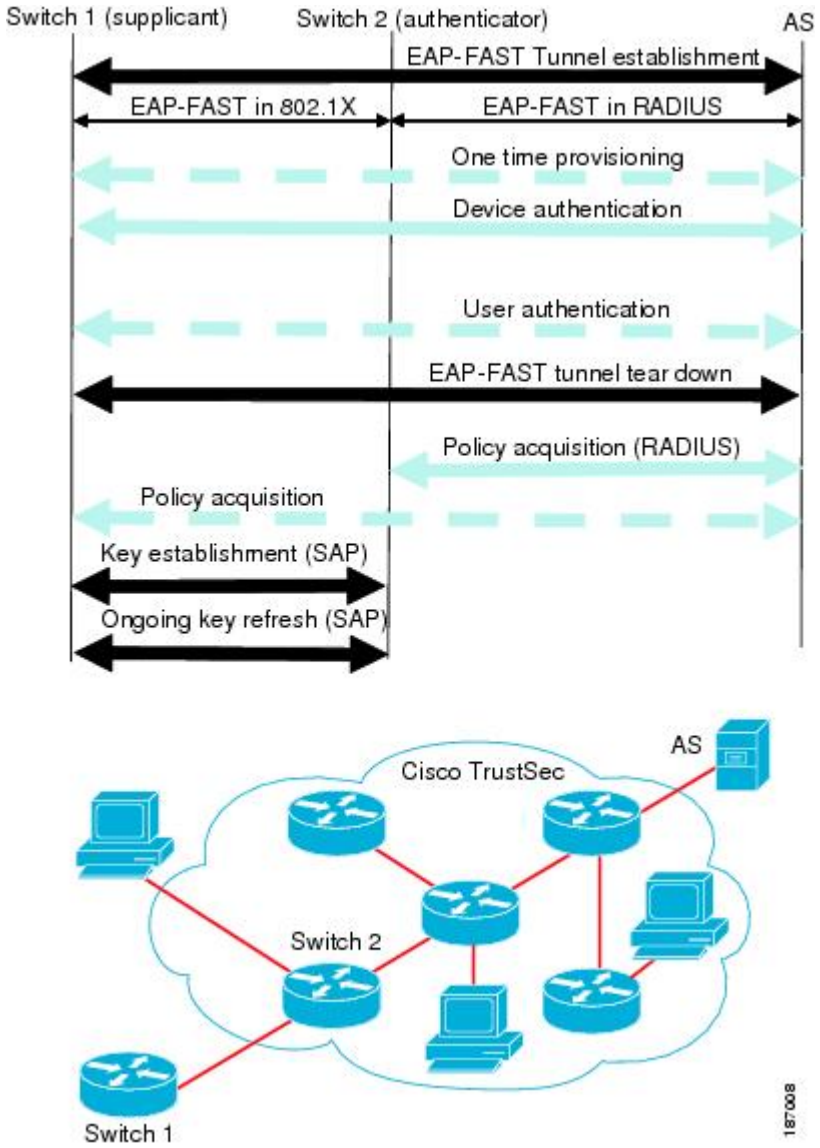
Cisco TrustSec は、デバイスのネットワーク加入を許可する前にデバイスを認証します。Cisco TrustSec は、拡張認証プロトコル（EAP）方式としての Extensible Authentication Protocol Flexible Authentication via Secure Tunnel（EAP-FAST）とともに、802.1X 認証を使用して、認証を実行します。

Cisco TrustSec と認証

Cisco TrustSec は認証に EAP-FAST を使用します。EAP-FAST カンバセーションによって、チェーンを使用した EAP-FAST トンネル内で他の EAP 方式の交換が可能になります。これにより、管理者は Microsoft Challenge Handshake Authentication Protocol Version 2（MSCHAPv2）のような従来型のユーザ認証方式を使用しながら、EAP-FAST トンネルが提供するセキュリティも利用できます。

次の図に、EAP-FAST トンネルおよび Cisco TrustSec で使用する内部方式を示します。

図 *14*：*Cisco TrustSec* の認証



EAP-FAST への Cisco TrustSec の機能拡張

Cisco TrustSec に EAP-FAST を実装することにより、次の機能拡張が実現しました。

オーセンティケータの認証

AT と認証サーバの間の共有秘密を得るために Protected Access Credential（PAC）を使用するように AT に求めることにより、AT のアイデンティティをセキュアに判断します。また、この機能により、AT が使用できるすべての IP アドレスに関して認証サーバに RADIUS 共有秘密を設定する手間が省けます。

ネイバーの ID を各ピアに通知

認証交換の完了までに、認証サーバはサプリカントと AT の両方を識別します。認証サーバは、保護された EAP-FAST 終端で追加の type-length-value（TLV）パラメータを使用して、AT のアイデンティティと、その AT が Cisco TrustSec に対応しているかどうかをサプリカントに伝えます。認証サーバはさらに、Access- Accept メッセージの RADIUS 属性を使用して、サプリカントのアイデンティティおよびそのサプリカントが Cisco TrustSec に対応しているかどうかを AT に伝えます。各ピアは、ネイバーのアイデンティティを認識しているため、認証サーバに追加の RADIUS Access-Requests を送信し、リンクに適用されるポリシーを取得できます。

AT ポスチャ評価

AT は、サプリカントの代わりに認証サーバと認証交換を開始すると、そのポスチャ情報を認証サーバに提供します。

802.1X ロールの選択

802.1X では、AT に認証サーバとの IP 接続が必要です。AT は RADIUS over UDP/IP を使用してサプリカントと AT の認証交換をリレーする必要があるためです。PC などのエンドポイント装置はネットワークへの接続時にサプリカントとして動作することになります。ただし、2 つのネットワーク デバイス間の Cisco TrustSec 接続の場合、各ネットワーク デバイスの 802.1X ロールが他方のネットワーク デバイスに即座に認識されない場合もあります。

NX-OS デバイスに AT とサプリカントのロールを手動で設定する代わりに、Cisco TrustSec はロール選択アルゴリズムを実行し、AT として動作する Cisco NX-OS デバイスとサプリカントとして動作するデバイスを自動的に判断します。ロール選択アルゴリズムは、RADIUS サーバに IP で到達可能なデバイスに AT ロールを割り当てます。どちらのデバイスも AT とサプリカントの両方のステート マシンを起動します。ある Cisco NX-OS デバイスが、ピアに RADIUS サーバへのアクセス権があることを検出すると、そのデバイスは自身の AT ステート マシンを終了し、サプリカントのロールを引き受けます。両方の Cisco NX デバイスに RADIUS サーバへのアクセス権がある場合、アルゴリズムは EAP over LAN（EAPOL）パケット送信の送信元として使用される MAC アドレスを比較します。MAC アドレスの値が大きい方の Cisco NX-OS デバイスが AT になり、もう一方の Cisco NX-OS デバイスがサプリカントになります。

Cisco TrustSec 認証の概要

Cisco TrustSec 認証プロセスが完了するまでに、認証サーバは次の処理を行います。

- サプリカントと AT のアイデンティティの検証
- サプリカントがエンドポイント装置の場合はユーザの認証

Cisco TrustSec 認証プロセスの完了時には、AT およびサプリカントの両方が次の情報を取得しています。

- ピアのデバイス ID
- ピアの Cisco TrustSec 機能についての情報

- SAP に使用されるキー

デバイス ID

Cisco TrustSec はデバイスの ID として IP アドレスも MAC アドレスも使用しません。その代わり、各 Cisco TrustSec 対応 Cisco NX-OS デバイスに、Cisco TrustSec ネットワークで一意に識別できる名前（デバイス ID）を手動で割り当てる必要があります。このデバイス ID は次の操作に使用されます。

- 認証ポリシーの検索
- 認証時におけるデータベース内のパスワードの検索

デバイスのクレデンシャル

Cisco TrustSec はパスワードベースのクレデンシャルをサポートしています。認証サーバは、代わりに自己署名式の証明書を使用する場合もあります。Cisco TrustSec はパスワードでサプリカントを認証し、MSCHAPv2 を使用することにより、たとえ認証サーバの証明書を検証できなくても、相互認証が可能です。

認証サーバはこれらのクレデンシャルを EAP-FAST フェーズ 0（プロビジョニング）の交換（サプリカントで PAC がプロビジョニングされる）中にサプリカントの相互認証に使用します。Cisco TrustSec は PAC の期限が切れるまで、EAP-FAST フェーズ 0 の交換は再実行しません。その後のリンク起動時には、EAP-FAST フェーズ 1 とフェーズ 2 の交換だけを実行します。EAP-FAST フェーズ 1 交換では、認証サーバとサプリカントの相互認証に PAC を使用します。Cisco TrustSec がデバイスのクレデンシャルを使用するのは、PAC プロビジョニング（または再プロビジョニング）段階だけです。

認証サーバは、Cisco TrustSec ネットワークにサプリカントが最初に加入する際に、一時的に設定されたパスワードをそのサプリカントの認証に使用します。サプリカントが最初に Cisco TrustSec ネットワークに加入する際に、認証サーバは証明書を作成してサプリカントを認証し、強力なパスワードを生成して、これを PAC でサプリカントに送信します。認証サーバはさらに、データベースに新しいパスワードを保存します。認証サーバとサプリカントは、その後の EAP-FAST フェーズ 0 交換の相互認証にこのパスワードを使用します。

ユーザ クレデンシャル

Cisco TrustSec には、エンドポイント装置の特定タイプのユーザ クレデンシャルは必要ありません。ユーザに対して任意のタイプの認証方式（MSCHAPv2、LEAP、Generic Token Card（GTC）、または OTP など）を選択し、対応するクレデンシャルを使用できます。Cisco TrustSec は、EAP-FAST フェーズ 2 交換の一部として EAP-FAST トンネル内でユーザ認証を実行します。

トランク ポートおよび FabricPath ポートでのネイティブ VLAN タギング

MACSec は、トランク ポートおよび FabricPath ポートでのネイティブ VLAN タギング機能により、FabricPath でサポートされます。ネイティブ VLAN タギングは、グローバルに、または制御パケットとデータ パケットのインターフェイスで設定できます。ネイティブ VLAN タギングをグローバルにイネーブルにするには、次のコマンドを使用します。

- **vlan dot1q tag native exclude control**
- **vlan dot1q tag native fabricpath**
- **vlan dot1q tag native fabricpath exclude control**

ネイティブ VLAN タギングを FabricPath ポートでイネーブルにするには、次のコマンドを使用します。

- **switchport trunk native vlan tag exclude control**
- **switchport fabricpath native vlan tag**
- **switchport fabricpath native vlan tag exclude control**

ネイティブ VLAN タギングにより、パケットの送受信時のタグ付きおよびタグなしモードへのサポートが提供されます。次の表では、上記のコマンドのグローバル設定またはポート設定でのパケットのモードを示します。

タギングの設定	TX 制御	TX データ（ネイティブ VLAN）	RX 制御	RX データ
グローバル トランク ポート タギング	タグなし	タグ付き	タグなしおよびタグ付き	タグ付き
グローバル FabricPath タギング	タグなし	タグなし	タグなしおよびタグ付き	タグなしおよびタグ付き
データ パケットへのグローバル FabricPath タギング	タグなし	タグ付き	タグなしおよびタグ付き	タグ付き
ポート レベルのトランク ポート タギング	タグなし	タグ付き	タグなしおよびタグ付き	タグ付き

タギングの設定	TX 制御	TX データ（ネイティブ VLAN）	RX 制御	RX データ
ポート レベルの Fabricpath タギング	タグなし	タグなし	タグなしおよびタグ付き	タグなしおよびタグ付き
データ パケットへのポート レベルの FabricPath タギング	タグなし	タグ付き	タグなしおよびタグ付き	タグ付き

SGACL と SGT

セキュリティ グループ アクセス リスト（SGACL）を使用すると、割り当てられたセキュリティ グループに基づいてユーザが実行できる操作を制御できます。許可をロールにまとめることにより、セキュリティ ポリシーの管理が容易になります。Cisco NX-OS デバイスにユーザを追加する際に、1 つ以上のセキュリティ グループを割り当てれば、ユーザは適切な許可を即座に受信できます。セキュリティ グループを変更することにより、新しい許可を追加したり、現在の許可を制限することもできます。

Cisco TrustSec はセキュリティ グループに、セキュリティ グループ タグ（SGT）という 16 ビットの固有のタグを割り当てます。Cisco NX-OS デバイス内の SGT の数は認証済みのネットワーク エンティティの数に制限されます。SGT は全社内の送信元の許可を示す単一ラベルです。範囲は Cisco TrustSec ネットワーク内でグローバルです。

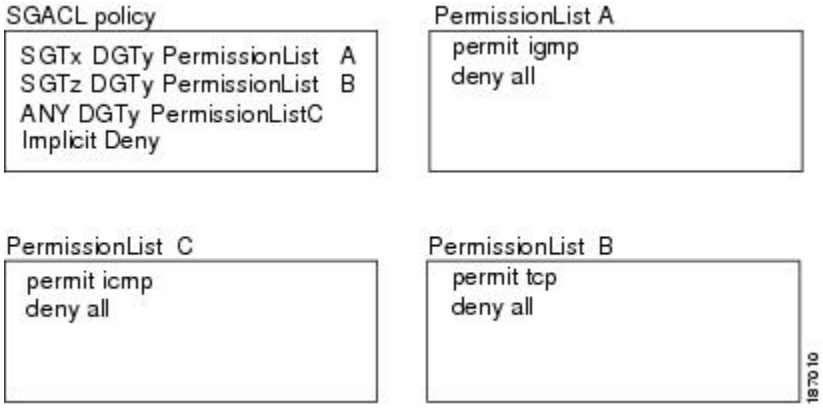
管理サーバは、セキュリティ ポリシーの設定に基づいて SGT を引き出します。これらを手動で設定する必要はありません。

いったん認証されると、Cisco TrustSec はデバイスを送信元とするすべてのパケットに、そのデバイスが割り当てられているセキュリティ グループを表す SGT を付けます。タグ付けされたパケットはネットワークを通じて Cisco TrustSec ヘッダーで SGT を運びます。このタグは、送信元のグループを表しているので、送信元の SGT として参照されます。Cisco TrustSec は、ネットワークの出口で、パケットの宛先デバイスに割り当てられているグループを判断し、アクセス コントロール ポリシーを適用します。

Cisco TrustSec はセキュリティ グループ間のアクセス コントロール ポリシーを定義します。Cisco TrustSec は、ネットワーク内のデバイスをセキュリティ グループに割り当て、セキュリティ グループ間およびセキュリティ グループ内でアクセス コントロールを適用することにより、ネットワーク内での原則的なアクセス コントロールを行います。

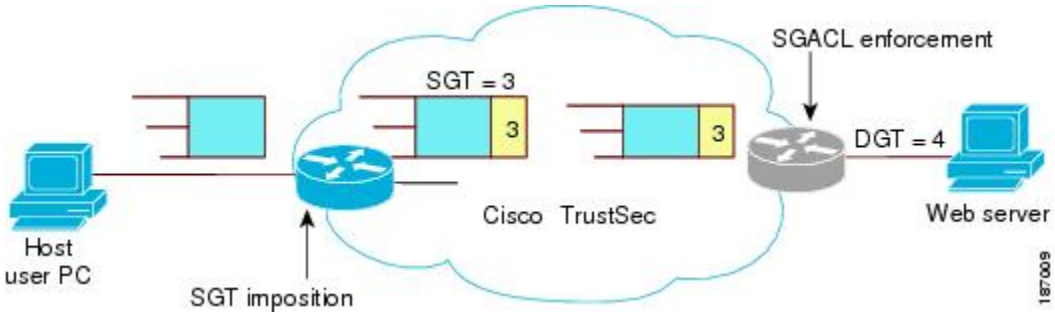
次の図に SGACL ポリシーの例を示します。

図 *15*：*SGACL* ポリシーの例



Cisco TrustSec ネットワークでは、次の図のように SGT の割り当てと SGACL の強制が実行されます。

図 *16*：*Cisco TrustSec* ネットワークでの *SGT* と *SGACL*



Cisco NX-OS デバイスは、従来の ACL の IP アドレスではなく、デバイス グループに Cisco TrustSec アクセス コントロール ポリシーを定義します。このような組み合わせの解除によって、ネットワーク全体でネットワーク デバイスを自由に移動し、IP アドレスを変更できます。ネットワークトポロジ全体を変更することが可能です。ロールと許可が同じであれば、ネットワークが変更されてもセキュリティ ポリシーには影響しません。この機能によって、ACL のサイズが大幅に節約され、保守作業も簡単になります。

従来の IP ネットワークでは、設定されているアクセス コントロール エントリ（ACE）の数は次のようにして決まります。

ACE の数=（指定されている送信元の数）X（指定されている宛先の数）X（指定されている許可の数）

Cisco TrustSec では、次の式を使用します。

ACE の数 = 指定されている許可の数

送信元セキュリティ グループの判断

Cisco TrustSec クラウドの入口のネットワーク デバイスは、Cisco TrustSec クラウドにパケットを転送する際に、パケットに SGT をタグ付けできるように、Cisco TrustSec クラウドに入るパケットの SGT を判断する必要があります。出口のネットワーク デバイスは、SGACL を適用できるように、パケットの SGT を判断する必要があります。

ネットワーク デバイスは、次のいずれかの方法でパケットの SGT を判断できます。

- ポリシー取得時に送信元の SGT を取得する：Cisco TrustSec 認証フェーズ後、ネットワーク デバイスは認証サーバからポリシーを取得します。認証サーバは、ピア デバイスが信頼できるかどうかを伝えます。ピア デバイスが信頼できない場合、認証サーバはそのピア デバイスから着信するすべてのパケットに適用する SGT も提供します。
- Cisco TrustSec ヘッダーの送信元 SGT フィールドを取得する：信頼できるピア デバイスからパケットが着信した場合、そのパケットにとってネットワーク デバイスが Cisco TrustSec クラウド内の最初のネットワーク デバイスではない場合に、Cisco TrustSec ヘッダーの SGT フィールドで正しい値が伝送されます。
- 送信元 IP アドレスに基づいて送信元 SGT を検索する：場合によっては、送信元 IP アドレスに基づいてパケットの SGT を判断するようにパケットを手動で設定できます。SGT Exchange Protocol（SXP）も、IP-address-to-SGT マッピング テーブルに値を格納できます。

宛先セキュリティ グループの判断

Cisco TrustSec クラウドの出口のネットワーク デバイスは、SGACL を適用する宛先グループを判断します。場合によっては、入口のデバイスまたは出口以外のその他のデバイスが、使用できる宛先グループの情報を持っていることもあります。このような場合、SGACL は出口のデバイスではなくこれらのデバイスに適用されます。

Cisco TrustSec は、パケットの宛先グループを決定します。以下のとおりに設定します。

- ポリシー取得時に出力ポートの宛先 SGT を取得する。
- 宛先 IP アドレスに基づいて宛先 SGT を検索する。

宛先 SGT を設定して、ファブリック エクステンダ（FEX）または vEthernet ポート上の出力ブロードキャスト、マルチキャスト、および不明なユニキャスト トラフィックに対して Cisco TrustSec を強制することはしません。代わりに、DST をゼロ（不明）に設定します。次に、正しい設定の例を示します。

```
cts role-based access-list acl-on-fex-egress
     deny udp
     deny ip
cts role-based sgt 9 dst 0 access-list acl-on-fex-egress
```

SGACL ロギング

Cisco NX-OS Release 7.3(0)D1(1) 以降では、SGACL ロギング機能を使用して、SGACL ポリシーを出力ポイントに適用した後にその効果を観察できます。次の内容を確認できます。

- フローが許可されるか、拒否されるか。
- フローが SGACL によりモニタされているか、または適用されているか。

（注） デフォルトで、SGACL 機能はディセーブルになっています。

（注） SGACL モニタ モードは、詳細な SGACL ロギングのイネーブル化を要件とします。詳細な SGACL ロギングをディセーブルにすると、SGACL モニタ モードがディセーブルになります。

（注） 詳細な SGACL ロギングは Cisco Nexus M シリーズ モジュールではサポートされません。

SGACL モニタ モード

Cisco TrustSec の事前導入段階で、管理者は、モニタ モードを使用して、ポリシーが当初意図したとおりであることを確認するために、セキュリティ ポリシーを適用しない状態でテストします。セキュリティポリシーになんらかの問題があった場合には、モニタ モードが、その問題を識別するための便利なメカニズムと、SGACL の適用をイネーブルにする前にポリシーを修正する機会を提供します。これにより、管理者は、ポリシーを適用する前にポリシー アクションの結果をより可視的に確認でき、対象のポリシーがセキュリティ要件を満たしている（ユーザが認証されなければリソースへのアクセスは拒否される）ことを確認できます。

モニタリング機能は、SGT-DGT ペア レベルで提供されます。デフォルトで、SGACL モニタ モードはディセーブルになっています。SGACL モニタ モード機能を有効にすると、拒否アクションがライン カード上の ACL 許可として実装されます。これにより、SGACL カウンタおよびロギングでは、接続が SGACL ポリシーによりどう処理されているかを表示できます。ここでは、すべてのモニタ対象トラフィックが許可されるため、SGACL モニタ モードでは、SGACL によるサービスの中断はありません。

SXP によるレガシー アクセス ネットワークへの SGT の伝播

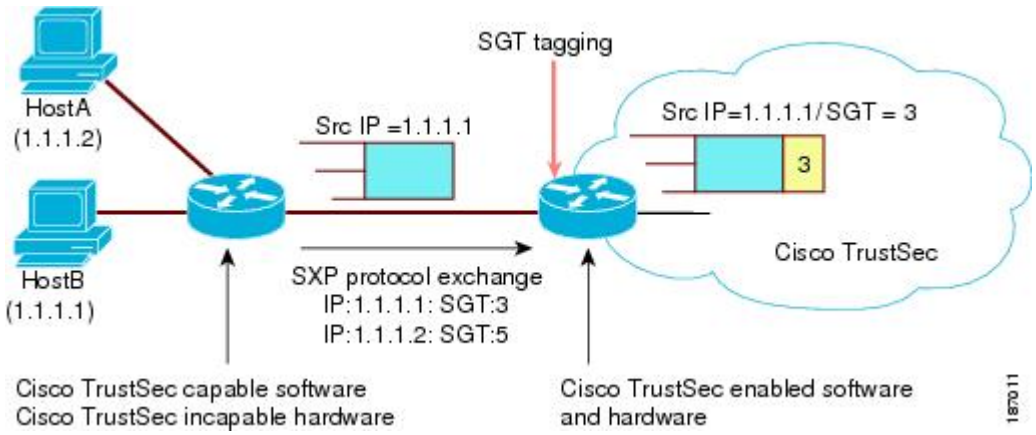
アクセス レイヤの Cisco NX-OS デバイス ハードウェアは Cisco TrustSec をサポートしています。Cisco TrustSec ハードウェアがないと、Cisco TrustSec ソフトウェアはパケットに SGT をタグ付け

できません。SXP を使用すると、Cisco TrustSec のハードウェア サポートがないネットワーク デバイスに SGT を伝播できます。

SXP はアクセス レイヤ デバイスと宛先レイヤ デバイスの間で動作します。アクセス レイヤ デバイスは SXP を使用して、SGT とともに Cisco TrustSec 認証デバイスの IP アドレスをディストリビューション スイッチに渡します。Cisco TrustSec 対応のソフトウェアとハードウェアを両方備えたディストリビューションデバイスはこの情報を使用して、パケットに適切にタグを付け、SGACL ポリシーを強制します。

次の図に、SXP を使用して、従来のネットワークで SGT 情報を伝播する方法を示します。

図 *17*：*SXP* を使用した *SGT* 情報の伝播



パケットへの SGT のタグ付けには、ハードウェアによるサポートが必要です。ネットワーク内に、パケットに SGT のタグ付けを行えないデバイスが含まれている可能性もあります。これらのデバイスから Cisco TrustSec 対応のハードウェアを搭載しているデバイスに IP アドレスと SGT のマッピングを送信できるようにするには、SXP 接続を手動で設定する必要があります。SXP 接続の手動での設定には、次のことが必要です。

- SXP データの整合性と認証が必要になる場合は、ピア デバイスの両方に同じ SXP パスワードを設定する必要があります。SXP パスワードは各ピア接続に対して明示的に指定することも、デバイスに対してグローバルに設定することもできます。SXP パスワードは必須ではありません。
- 各ピアを SXP 接続に SXP スピーカーまたは SXP リスナーとして設定する必要があります。スピーカー デバイスはリスナー デバイスに SXP 情報を渡します。
- 送信元 IP アドレスを指定して各ピアの関係付けに使用したり、特定の送信元 IP アドレスを設定していないピア接続に対してデフォルトの送信元 IP アドレスを設定したりすることができます。

SXPv3 を使用した Cisco TrustSec

セキュリティ グループ タグ（SGT）交換プロトコル（SXP）は、ネットワーク デバイス間で IP アドレスと SGT のバインディング情報を伝播する制御プロトコルです。Cisco NX-OS Release 7.3(0)D1(1) 以降、SXP バージョン 3（SXPv3）機能により、SGT バインディングへの IPv4 サブネットのトランスポートがサポートされます。

サブネットと SGT のバインディングを使用して、マッピングを保存するのに必要な転送情報ベース（FIB）エントリを最小化でき、これにより顧客は TrustSec 導入の規模を拡大できます。多くのシナリオで、L3 インターフェイスと SGT の代わりに、サブネットと SGT のバインディングを使用できます。

（注） Cisco NX-OS Release 7.3(0)D1(1) では、SXPv2 はサポートされません。

（注） SXPv3 は IPv6 をサポートしません。

SXPv3 サブネットの展開

SXPv3 プロトコルにより、サブネット バインディングの展開の制限を設定できます。バージョン 3 以前のピアで接続がセットアップされている場合、SXP は、サブネット バインディングをホスト アドレス バインディングに展開します。SXP によるバインディングの展開は、IPv4 サブネット バインディングにのみ適用されます。

サブネット展開の特性は次のとおりです。

- SGT 値が異なる重複した IP アドレスへのバインディングを展開すると、プレフィックス長が最も長い IP アドレスからマッピングが取得されます。
- サブネット展開が設定された制限に達すると、展開できないサブネットに対してシステム ログが生成されます。
- バインディングの展開により、サブネット内のブロードキャスト IP アドレスが展開されることはありません。また、SXP によってホストの IP アドレスがサブネット バインディングにサマライズされることもありません。SXP 伝搬経路では、サブネット バインディングを認識しないノードがある場合、たとえサブネット バインディングを認識するノードがあっても、バインディングは展開され、ホスト IP バインディングとして残りの伝播経路経由で伝播されます。
- 展開のデフォルトの制限はゼロ（0）で、許可される最大展開制限は 65535 です。ネットワーク内に SXP の下位バージョンをサポートするデバイスがない場合は、展開の制限を 0 に設定できます。

cts sxp mapping network-map [*num_bindings*] コマンドを使用して、ネットワーク制限を展開できます。*num_bindings* パラメータには、0 から 65535 までを使用できます。ゼロ（0）は展開できないことを意味し、65535 では、最大展開制限が許可されます。デフォルト値は 0 です。

展開制限が 67 に設定され、サブネットが /24 である例を検討します。Cisco NX-OS は、CTS に認識された最初のサブネット SGT の最初の 67 個の IP アドレスを展開します。サブネット /24 はより多くのホストを含むため、十分な展開が行われず、syslog が生成されます。

（注） 最大展開制限が 65535 に設定されている場合、Cisco NX-OS は、サブネット /16 内のすべての IP のマッピングをサポートします。ただし、展開制限を最大の制限値に設定する場合は、それによるハードウェアやソフトウェアへの影響を考慮する必要があります。

SXP バージョン ネゴシエーション

SXP セッションは、スピーカーデバイスとリスナーデバイス間で確立されます。デフォルトで、CTS デバイスは、サポートされる最も高い SXP バージョンをアドバタイズします。ネゴシエーションは、スピーカーデバイスとリスナーデバイスによりサポートされる最も高い共通バージョンに基づいて行われます。スタンドアロン CTS によりサポートされるデバイスは、ピアデバイスの SXP バージョンに依存して、そのピア デバイスと異なるバージョンの SXP セッションを確立できます。

次の表に、さまざまなシナリオでの、相互運用性のためのバージョン ネゴシエーションに関する情報を示します。

表 *26* : *SXP* バージョン ネゴシエーションのケース

ケース番号	Speaker	Listener	SXP セッションのステータス
1	SXPv1	SXPv1	SXPv1 セッションが確立されます。
2	SXPv1	SXPv2	SXPv1 セッションが確立されます。
3	SXPv1	SXPv3	SXPv1 セッションが確立されます。
4	SXPv2	SXPv1	SXPv1 セッションが確立されます。
5	SXPv2	SXPv2	Cisco Nexus 7000 デバイスは SXPv2 をサポートしないため、確立できません。
6	SXPv2	SXPv3	SXPv3 を持つ Cisco Nexus 7000 デバイスが SXPv2 を持つ別の Cisco SXP デバイスと相互運用している場合、Cisco Nexus 7000 デバイスは SXPv1 として接続を確立します。
7	SXPv3	SXPv1	SXPv1 セッションが確立されます。

ケース番号	Speaker	Listener	SXP セッションのステータス
8	SXPv3	SXPv2	SXPv3 を持つ Cisco Nexus 7000 デバイスが SXPv2 を持つ別の Cisco SXP デバイスと相互運用している場合、Cisco Nexus 7000 デバイスは SXPv1 として接続を確立します。
9	SXPv3	SXPv3	SXPv3 セッションが確立されます。

デフォルト ルートの SGT バインディングの SXP サポート

送信元 IP アドレスまたは宛先 IP アドレスの IP-SGT が設定されていない場合、SGT バインディングのデフォルト ルートを指定できます。このシナリオでは、SGT はデフォルト ルート エントリから導出されます。デフォルトルートは、SXPv3 を持つリスナーデバイスにのみ使用できることに注意してください。デフォルトでは、SXP の使用によるデフォルト ルート経由の SGT バインディングのトランスポートはディセーブルになっています。**cts sxp allow default-route-sgt** コマンドを使用して、デフォルトルート経由の SGT バインディングのトランスポートをイネーブルにできます。SGT バインディングのデフォルトルートをディセーブルにするには、このコマンドの **no** 形式を使用します。

Cisco TrustSec サブネットと SGT のマッピング

サブネットと SGT のマッピングは、指定したサブネット内のすべてのホスト アドレスに SGT をバインドします。このマッピングが実行されると、Cisco TrustSec により、指定のサブネットに属する送信元 IP アドレスを持つ着信パケットに SGT が課せられます。これにより、データセンターホストを流れるトラフィックに CTS ポリシーを適用することができます。VRF インスタンスで IPv4 サブネットと SGT のバインディングを設定できます。

IPv4 ネットワークでは、SXPv3 以降のバージョンは SXPv3 ピアからサブネットのネットワーク アドレスまたはプレフィックス文字列を受信し、解析できます。

たとえば、IPv4 サブネット 198.1.1.0/29 は次のように拡張されます（ホスト アドレスの 3 ビットのみ）。

- ホスト アドレス 198.1.1.1 から 198.1.1.7 はタグ付けされて SXP ピアに伝播します。
- ネットワーク、およびブロードキャスト アドレス 198.1.1.0 および 198.1.1.8 は、タグ付けされず、伝播しません。

（注） SXPv1 ピアにエクスポートされるサブネット バインディングの数の増大を制限するには、**cts sxp mapping network-map** グローバル設定コマンドを使用します。

サブネット バインディングは静的です。つまり、アクティブなホストは学習されません。これらは SGT インポジションおよび SGACL の強制にローカルで使用できます。サブネットと SGT の

マッピングによってタグ付けされたパケットは、レイヤ 2 またはレイヤ 3 TrustSec リンクに伝播できます。また、**cts sxp allow default-route-sgt** コマンドを使用して、デフォルト ルート（不明な IP アドレス 0.0.0.0）による SGT バインディングをトランスポートできます。

許可とポリシーの取得

認証が終了すると、サプリカントと AT はいずれも認証サーバからセキュリティ ポリシーを取得します。サプリカントと AT はお互いに対してポリシーを強制します。サプリカントと AT はいずれも、認証後に受信したピア デバイス ID を提供します。ピア デバイス ID を使用できない場合、Cisco TrustSec は手動で設定されたピア デバイス ID を使用できます。

認証サーバは次の属性を返します。

Cisco TrustSec の信頼状態

パケットに SGT を付けるにあたり、ネイバー デバイスが信用できるかどうかを示します。

ピア SGT

ピアが属しているセキュリティ グループを示します。ピアが信頼されない場合は、ピアから受信したすべてのパケットは、入力インターフェイスで設定された SGT でタグ付けされます。このインターフェイスで強制がイネーブルである場合、ピア SGT に関連付けられた SGACL がダウンロードされます。SGACL がピアの SGT に関連付けられているかどうかデバイスが認識できないと、そのデバイスは SGACL を取得するために追加要求を送信する場合もあります。

許可の有効期限

ポリシーの期限が切れるまでの秒数を示します。シスコ独自の AV のペアは、許可または Cisco TrustSec デバイスへのポリシー応答の期限を表します。Cisco TrustSec デバイスはポリシーと許可を期限が切れる前にリフレッシュする必要があります。

ヒント　Cisco TrustSec デバイスは、認証サーバからピアの適切なポリシーを取得できない場合に備えて、最小限のデフォルト アクセス ポリシーをサポートする必要があります。

許可の変更

管理者がサーバ上で AAA プロファイルを更新すると、Cisco TrustSec は RADIUS 許可の変更機能を使用して、Cisco Identity Services Engine（ISE）からスイッチにポリシーを自動的にダウンロードします。

（注）　この機能は、Cisco ISE でのみ動作し、Cisco Secure Access Control Server（ACS）では動作しません。

環境データのダウンロード

Cisco TrustSec 環境データは、Cisco TrustSec ノードとしてのデバイスの機能を支援するひとまとまりの情報またはポリシーです。デバイスは、Cisco TrustSec クラウドに最初に加入する際に、認証サーバから環境データを取得しますが、一部のデータをデバイスに手動で設定することもできます。たとえば、Cisco TrustSec のシードデバイスには認証サーバの情報を設定する必要がありますが、この情報は、デバイスが認証サーバから取得するサーバ リストを使用して、後から追加することができます。

デバイスは、期限前に Cisco TrustSec 環境データをリフレッシュする必要があります。また、このデータの有効期限が切れていなければ、データをキャッシュし、リブート後に再利用することもできます。

デバイスは RADIUS を使用して、認証サーバから次の環境データを取得します。

サーバ リスト

クライアントがその後の RADIUS 要求に使用できるサーバのリスト（認証および許可の両方）

Device SGT

そのデバイス自体が属しているセキュリティ グループ

有効期間

Cisco TrustSec デバイスが環境データをリフレッシュする頻度を左右する期間

RADIUS リレー機能

802.1X 認証プロセスで Cisco TrustSec AT のロールを引き受ける Cisco NX-OS デバイスは、認証サーバへの IP 接続を通じて、UDP/IP での RADIUS メッセージの交換により、認証サーバからポリシーと許可を取得します。サプリカントデバイスは認証サーバとの IP 接続がなくてもかまいません。サプリカントに 認証サーバとの IP 接続 がない場合、Cisco TrustSec は AT をサプリカントの RADIUS リレーとして機能させることができます。

サプリカントは、RADIUS サーバの IP アドレスと UDP ポートを持つ Cisco TrustSec AT に特別な EAP over LAN（EAPOL）メッセージを送信し、RADIUS 要求を完了します。Cisco TrustSec AT は受信した EAPOL メッセージから RADIUS 要求を抽出し、これを UDP/IP を通じて認証サーバに送信します。認証サーバから RADIUS 応答が返ると、Cisco TrustSec AT はメッセージを EAPOL フレームにカプセル化して、サプリカントに転送します。

仮想ポート チャネル（vPC）の SGT サポート

Cisco NX-OS Release 7.2(0)D1(1) 以降では、CTS は、仮想ポート チャネル（vPC）および vPC+ でサポートされます。次の Cisco TrustSec 設定は、vPC と vPC+ の両ピアで一致している必要があります。

1. vPC のすべてのインターフェイス上のポート - SGT 設定（SGT および trust モード）
2. IP - SGT 設定
3. VLAN-SGT 設定
4. SXP ピア接続設定
5. SGT キャッシング設定
6. AAA/RADIUS 設定
7. SGACL ポリシー設定
8. VLAN および VRF 設定への SGACL 適用

（注）
- 設定が一致していなくても警告は生成されず、互換性チェックも行われません。
- Cisco TrustSec の手動設定モード（**cts manual** コマンドを実行）で、**propagate-sgt** および **policy static sgt** コマンドを使用して、SGT 伝播をイネーブルにした状態で、vPC ピア リンクを trusted モードで設定する必要があります。
- IP-SGT 学習は FabricPath ポートではサポートされませんが、インライン SGT タギングは FabricPath リンクでサポートされます。CTS が FabricPath ポートでイネーブルの場合、そのポートで、**propagate-sgt** および **policy static sgt** コマンドがイネーブルである必要があります。

バインディング送信元プライオリティ

TrustSec は完全優先方式で IP-SGT バインディング ソース間の競合を解決します。たとえば、SGT は **policy** {**dynamic identity***peer-name*|**static sgt***tag*} CTS 手動インターフェイス モード コマンド（アイデンティティ ポート マッピング）を使用してインターフェイスに適用されます。現在の優先順位の適用順序は、最も小さい（1）から最高（7）まで、次のとおりです。

1. Cisco Fabric Services（CFS）：vPC ピアに関して学習された、CTS の IP-SGT バインディング。これは、vPC ピア デバイスにのみ適用できます。
2. VLAN-SGT：VLAN-SGT マッピングにより設定されている VLAN 上のスヌーピングされた ARP または DHCP パケットから学習されたバインディング。
3. SGT-caching：SGT-caching が設定されている VLAN または VRF で学習された IP-SGT バインディング。
4. SXP：SXP ピアから学習されたバインディング。
5. Learnt on interface：EPM とデバイス トラッキングによって学習された認証済みホストのバインディング。このタイプのバインディングには、L2 [I]PM が設定されたポートの ARP スヌーピングによって学習された個々のホストも含まれます。

6 CLI：**cts role-based sgt-map** グローバル コンフィギュレーション コマンドの IP-SGT 形式を使用して設定されたアドレス バインディング。

7 Port ASIC：CTS の信頼状態の設定に基づいて、インラインで、またはポートから直接生成された SGT バインディング。

仮想化のサポート

Cisco TrustSec の設定と操作は、仮想デバイス コンテキスト（VDC）に対してローカルです。VDC の詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

Cisco TrustSec のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	Cisco NX-OS Release 6.1 以降では、Cisco TrustSec にはライセンスは不要です。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。 Cisco NX-OS Release 6.1 よりも前の場合は、Cisco TrustSec には Advanced Services ライセンスが必要です。Cisco TrustSec ライセンスには猶予期間はありません。Cisco TrustSec を使用するためには、事前に Advanced Services ライセンスを取得しインストールする必要があります。 （注） Cisco NX-OS ライセンス方式の詳細と、ライセンスの取得および適用の方法については、『*Cisco NX-OS Licensing Guide*』を参照してください。

Cisco TrustSec の前提条件

Cisco TrustSec の前提条件は次のとおりです。

- デバイスが 6.1 よりも前の Cisco NX-OS リリースを実行している場合は、Advanced Services ライセンスをインストールする必要があります。

- 802.1X 機能をイネーブルにする必要があります。
- Cisco TrustSec 機能をイネーブルにする前に、802.1X 機能をイネーブルにする必要があります。802.1X インターフェイス レベルの機能が使用できませんが、デバイスが RADIUS で認証するためには 802.1X が必要です。
- Cisco TrustSec 機能をイネーブルにする必要があります。

Cisco TrustSec の注意事項と制約事項

Cisco TrustSec に関する注意事項と制約事項は次のとおりです。

- Cisco TrustSec MACSec：SP により提供される擬似回線接続に MACSec を導入する際には、次の一連の要件を使用する必要があります。これらの要件は、SP から適切なサービス、品質、または特性を引き出すのに役立ちます。

  Nexus 7000 は、DWDM を使用するものなど、ポイントツーポイント リンク上の MACSec、および次の条件を満たす EoMPLS などの非 PTP リンク上の MACSec をサポートします。

  - MACSec リンク上のパケットは、順序変更やバッファリングができません。
  - MACSec リンクに追加のフレームを挿入することはできません。
  - エンドツーエンドのリンク イベント通知が必要です（サービスが中断されたときに顧客がリンク障害を知ることができるよう、エッジデバイスやどこかの中間デバイスでリンクが切れた場合は通知が送信される必要があります）。

- 40G 以上で同じ帯域幅がある MACsec リンクでは、複数のセキュリティ アソシエーション（SCI/AN ペア）は、セキュリティアソシエーションプロトコル（SAP）交換で設定します。
- Cisco TrustSec SGT は IPv4 アドレスのみをサポートします。
- Cisco TrustSec SGT のインライン タギングは、OTV、VXLAN、FCoE、またはプログラマブル ファブリックでサポートされません。
- SXP は管理（mgmt 0）インターフェイスを使用できません。
- 半二重モードのインターフェイスでは、Cisco TrustSec をイネーブルにできません。
- SVI を通じてルーティングされるパケットに SGACL を適用する場合、すべての VLAN および関連する VRF インスタンスで SGACL をイネーブルにする必要があります。
- 1 つのインターフェイスに、Cisco TrustSec と 802.1X の両方は設定できません。設定できるのはこれらのどちらか一方です。ただし、Cisco TrustSec で EAP-FAST 認証を使用するには、802.1X 機能をイネーブルにする必要があります。
- Cisco TrustSec の AAA 認証および許可は、Cisco Secure Access Control Server（ACS）と Cisco Identity Services Engine（ISE）でのみサポートされます。
- sgname テーブルをダウンロードしたり、環境データをリフレッシュするには、Cisco Identity Services Engine（ISE）リリース 1.0 以降のリリースを使用する必要があります。Cisco Secure Access Control Server（ACS）は、これらの機能をサポートしません。

- Cisco TrustSec は 200,000 IP-SGT マップをサポートします。これは、各モジュールの FIB TCAM のスペース可用性によって決まります。100,000 を超える IP-SGT マッピングを手動で設定すると、CLI ロールバックがサポートされないことに注意してください。詳細については、『*Cisco Nexus 7000 Series NX-OS Verified Scalability Guide*』を参照してください。
- CISCO-TRUSTSEC-SXP-MIB はインスタンス番号を提供しません。*ctsxSxpConnInstance* オブジェクトは、CTS SXP 接続のインスタンス番号を提供しません。この番号は現在維持されないため、表示することができません。
- 非デフォルト VDC で CTS 設定をリロードすると、syslog メッセージがトリガーされます。Cisco Trusted Security（CTS）の適用が VLAN でイネーブルの場合に、VDC のリロードが発生すると、CTS は VLAN での適用のディセーブル化を 2 回試みます。2 回目の試行時に、次の syslog メッセージが表示されます。
  `CTS-2-RBACL_ENFORCEMENT_FAILED:Failed to disable RBACL enf on vdc reload`
  VLAN はリロード時に削除され、それらの VLAN 上の適用の設定も CTS により削除されるため、VDC リロードに関するこの syslog メッセージは無視できます。
- CTS コンフィギュレーション コマンドは使用できません。**no cts dev-id pswd dev-pswd** コマンドは、現在、NX-OS ソフトウェアでサポートされません。**cts dev-id pass** コマンドが設定されている場合、同じコマンドを使用してコマンド設定の置き換えはできますが、削除はできません。
- CTS MACSec ポート モードを Cache Engine（CE）モードから FabricPath モードに変更すると、ネイティブ VLAN タギングを FabricPath コア ポートでディセーブルにするまで、CTS MACSec リンクに CRC エラーが表示されます。CTS ポートで発生するこのような設定変更は、フラッピングされる必要があります。ただし、これによりトラフィックの中断が引き起こされる可能性があります。このような状況では、CRC エラーの表示とトラフィックの中断を避けるために、次のステップを実行します。
  1. CTS MACsec がイネーブルの間は、キャッシュ エンジン ポートをディセーブルにする。
  2. ポート モードを FabricPath モードに変更する。
  3. FabricPath コア ポートのネイティブ VLAN タギングをディセーブルにする。
  4. ポートをイネーブルにします。
- サブネットと SGT のバインディングはデフォルトで拡張されません。拡張可能にするには、**cts sxp mapping network-map** コマンドをゼロ以外の値に設定する必要があります。
- 対応する SGT バインディングが存在する場合でも、より長いプレフィックスに関連付けられた SGT が常に選択されます。たとえば、サブネット - SGT バインディング 10 を含むホスト 12.1.0.0/16 と、IP - SGT バインディング 20 を含むホスト 12.1.1.1 を検討します。親プレフィックス SGT が 10 であっても、ホスト 12.1.1.1 の SGT 20 が選択されます。同様に、VLAN 121 がサブネット 12.1.0.0/16 に宛てられ、VLAN - SGT バインディング 30 とともに設定されている場合、サブネット - SGT バインディングは VLAN - SGT マッピングより長いと判断されるため、ホスト 12.1.1.1 は SGT 値 20 を、ホスト 12.1.1.2 は SGT 値 10 を保持し続けます。
- モニタ モードをイネーブルにするには、**cts role-based detailed-logging** コマンドをイネーブルにします。現在行われているように、ACE レベルでロギングをイネーブルまたはディセーブルにできます。

- RBACL レベルまたは ACE レベルでのモニタリングはサポートされません。
- ログ出力カウントはレート制限されますが、カウンタ統計情報はハードウェアから直接取得されるため、モニタ モードのカウンタ統計情報とログ出力が一致しない場合があります。
- CLI、ISE、または両方を使用して **monitor all** をイネーブルにすると、すべての SGT-DGT ペアのモニタリングが、ペアごとの設定とは無関係に、オンになります。
- モニタ モード機能をディセーブルにすると、スイッチはデフォルトの動作に戻ります。ISE によりモニタされた SGACL はインストールされません。CLI によりインストールされたすべての SGACL は、設定されたとおりのポリシーの適用または拒否を開始します。

Cisco TrustSec パラメータのデフォルト設定

次の表に、Cisco TrustSec パラメータのデフォルト設定を示します。

表 *27*：*Cisco TrustSec* パラメータのデフォルト設定

パラメータ	デフォルト
Cisco TrustSec	ディセーブル
すべてのインターフェイスのポーズフレームの暗号化および復号化	ポーズフレームの暗号化および復号化をサポートするラインカードでイネーブル
SXP	ディセーブル
SXP デフォルト パスワード	なし
SXP 復帰期間	120 秒（2 分）
SXP リトライ期間	60 秒（1 分）
キャッシング	ディセーブル
RBACL ロギング	ディセーブル
RBACL 統計情報	ディセーブル

Cisco TrustSec の設定

ここでは、Cisco TrustSec の設定作業について説明します。

Cisco TrustSec SGT 機能のイネーブル化

Cisco TrustSec を設定する前に、Cisco NX-OS デバイス上の 802.1X 機能および Cisco TrustSec の機能をイネーブルにする必要があります。

（注） Cisco TrustSec 機能をイネーブルにすると、その後に 802.1X 機能をディセーブルにすることはできません。

はじめる前に

デバイスが 6.1 よりも前の Cisco NX-OS リリースを実行している場合は、Advanced Services ライセンスをインストールしていることを確認します。

手順の概要

1. **configure terminal**
2. **feature dot1x**
3. **feature cts**
4. **exit**
5. （任意） **show cts**
6. （任意） **show feature**
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**feature dot1x** 例： `switch(config)# feature dot1x`	802.1X 機能をイネーブルにします。
ステップ 3	**feature cts** 例： `switch(config)# feature cts`	Cisco TrustSec 機能をイネーブルにします。

	コマンドまたはアクション	目的

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 5	**show cts** 例： `switch# show cts`	（任意） Cisco TrustSec の設定を表示します。
ステップ 6	**show feature** 例： `switch# show feature`	（任意） 機能がイネーブルになったステータスを表示します。
ステップ 7	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Cisco TrustSec デバイスのクレデンシャルの設定

ネットワーク内の Cisco TrustSec 対応 Cisco NX-OS デバイス各々に、固有の Cisco TrustSec クレデンシャルを設定する必要があります。Cisco TrustSec はクレデンシャルのパスワードをデバイスの認証に使用します。

（注） Cisco Secure ACS にも Cisco NX-OS デバイスの Cisco TrustSec クレデンシャルを設定する必要があります（次の URL のマニュアルを参照してください。

http://www.cisco.com/en/US/products/sw/secursw/ps5338/products_installation_and_configuration_guides_list.html）。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **cts device-id***name***password***password*
3. **exit**
4. （任意） **show cts**
5. （任意） **show cts environment**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**cts device-id***name***password***password* 例： `switch(config)# cts device-id MyDevice1 password CiscO321`	固有のデバイス ID およびパスワードを設定します。*name* 引数は、最大 32 文字で大文字と小文字を区別します。 （注） デバイスの ID とパスワードの設定を削除するには、このコマンドの **no** 形式を使用します。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 4	**show cts** 例： `switch# show cts`	（任意） Cisco TrustSec の設定を表示します。
ステップ 5	**show cts environment** 例： `switch# show cts environment`	（任意） Cisco TrustSec 環境データを表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ネイティブ VLAN タギングの設定

ネイティブ VLAN タギングのグローバル設定

ネイティブ VLAN タギングをグローバルに設定するには、ここに示す手順を実行します。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **vlan dot1q tag native** {**fabricpath**} **exclude control**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan dot1q tag native** {**fabricpath**} **exclude control** 例： `switch(config)# vlan do1q tag native exclude control`	必要に応じて制御パケットとデータ パケットにタグを追加します。 • データ パケットのみにタグを追加するには **exclude control** キーワードを使用します。 • FabricPath ポートで制御パケットとデータ パケットにタグを追加するには **fabricpath** キーワードを使用します。

インターフェイスでのネイティブ VLAN タギングの設定

ネイティブ VLAN タギングをグローバルに設定するには、ここに示す手順を実行します。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **interface***typeslot*/*port*
3. **vlan dot1q tag native** {**fabricpath**} **exclude control**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***typeslot*/*port* 例： `switch(config)# interface ethernet 1/4`	チャネル グループに追加するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**vlan dot1q tag native** {**fabricpath**} **exclude control** 例： `switch(config-if)# vlan do1q tag native exclude control`	必要に応じて制御パケットとデータ パケットにタグを追加します。 • データ パケットのみにタグを追加するには **exclude control** キーワードを使用します。 • FabricPath ポートで制御パケットとデータ パケットにタグを追加するには **fabricpath** キーワードを使用します。

Cisco TrustSec の AAA の設定

Cisco TrustSec の認証に Cisco Secure ACS を使用できます。ネットワーク クラウド内の Cisco TrustSec 対応 Cisco NX-OS デバイスの 1 つに、RADIUS サーバ グループを設定し、デフォルトの AAA 認証および許可を指定する必要があります。Cisco TrustSec は RADIUS リレーをサポートしているため、AAA を設定するのは、Cisco Secure ACS に直接接続されている Cisco NX-OS シード デバイスだけです。Cisco TrustSec がイネーブルのすべての Cisco NX-OS デバイスに対して、Cisco TrustSec は自動的にプライベート AAA サーバ グループ aaa-private-sg を提供します。シード Cisco NX-OS デバイスは、Cisco Secure ACS との通信に管理仮想ルーティングおよび転送（VRF）インスタンスを使用します。

（注） Cisco TrustSec をサポートしているのは、Cisco Secure ACS だけです。

Cisco TrustSec シード Cisco NX-OS デバイスでの AAA の設定

ここでは、Cisco TrustSec ネットワーク クラウド内のシード Cisco NX-OS デバイスで AAA を設定する手順を説明します。

（注） シード Cisco NX-OS デバイスの AAA RADIUS サーバ グループを設定する際には、VRF インスタンスを指定する必要があります。管理 VRF インスタンスを使用する場合、ネットワーク クラウド内の非シード デバイスにそれ以上の設定を行う必要はありません。異なる VRF インスタンスを使用する場合は、非シードデバイスにVRFインスタンスを設定する必要があります。

はじめる前に

Cisco Secure ACS の IPv4 または IPv6 のアドレスまたはホスト名を取得します。

Cisco TrustSec がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **key** [**0** | **7**] *key* **pac**
3. （任意） **show radius-server**
4. **aaa group server radius** *group-name*
5. **server** {*ipv4-address* | *ipv6-address* | *hostname*}
6. **use-vrf***vrf-name*
7. **exit**
8. **aaa authentication dot1x default group***group-name*
9. **aaa authorization cts default group***group-name*
10. **exit**
11. （任意） **show radius-server groups** [*group-name*]
12. （任意） **show aaa authentication**
13. （任意） **show aaa authorization**
14. （任意） **show cts pacs**
15. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**radius-server host** {*ipv4-address* | *ipv6-address* | *hostname*} **key** [**0** | **7**] *key* **pac** 例： `switch(config)# radius-server host 10.10.1.1 key L1a0K2s9 pac`	キーと PAC を使用して RADIUS サーバ ホストを設定します。*hostname* 引数は、256 文字以内の英数字で指定します。大文字と小文字が区別されます。*key* 引数は、63 文字以内の英数字で指定します。大文字と小文字が区別されます。**0** オプションは、キーがクリア テキストであることを示します。**7** オプションは、キーが暗号化されていることを示します。デフォルトはクリア テキストです。
ステップ 3	**show radius-server** 例： `switch# show radius-server`	（任意） RADIUS サーバの設定を表示します。

ステップ 4	**aaa group server radius** *group-name*
	
	例：
	`switch(config)# aaa group server radius Rad1`
	`switch(config-radius)#`
		RADIUS サーバ グループを指定し、RADIUS サーバ グループ コンフィギュレーション モードを開始します。

ステップ 5	**server** {*ipv4-address* | *ipv6-address* | *hostname*} 例： `switch(config-radius)# server 10.10.1.1`	RADIUS サーバ ホストのアドレスを指定します。
ステップ 6	**use-vrf***vrf-name* 例： `switch(config-radius)# use-vrf management`	AAA サーバ グループの管理 VRF インスタンスを指定します。 （注） 管理 VRF インスタンスを使用する場合、ネットワーク クラウド内の非シード デバイスにそれ以上の設定を行う必要はありません。異なる VRF インスタンスを使用する場合は、非シード デバイスに VRF インスタンスを設定する必要があります。

ステップ 7	**exit**
	
	例：
	`switch(config-radius)# exit`
	`switch(config)#`
		RADIUS サーバ グループ コンフィギュレーション モードを終了します。

ステップ 8	**aaa authentication dot1x default group***group-name* 例： `switch(config)# aaa authentication dot1x default group Rad1`	802.1X 認証に使用する RADIUS サーバ グループを指定します。

	コマンドまたはアクション	目的
ステップ 9	**aaa authorization cts default group***group-name* 例： `switch(config)# aaa authentication cts default group Rad1`	Cisco TrustSec 認証に使用する RADIUS サーバ グループを指定します。

ステップ 10	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 11	**show radius-server groups** [*group-name*] 例： `switch# show radius-server group rad1`	（任意） RADIUS サーバ グループの設定を表示します。
ステップ 12	**show aaa authentication** 例： `switch# show aaa authentication`	（任意） AAA 認証の設定を表示します。
ステップ 13	**show aaa authorization** 例： `switch# show aaa authorization`	（任意） AAA 認可設定を表示します。
ステップ 14	**show cts pacs** 例： `switch# show cts pacs`	（任意） Cisco TrustSec PAC 情報を表示します。
ステップ 15	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Cisco TrustSec 非シード NX-OS デバイスでの AAA の設定

Cisco TrustSec はネットワーク クラウド内の非シード Cisco NX-OS デバイスに aaa-private-sg という名前の AAA サーバ グループを設定します。デフォルトでは、aaa-private-sg サーバ グループは Cisco Secure ACS との通信に管理 VRF インスタンスを使用します。非シード Cisco NX-OS デバイスに対するそれ以上の設定は必要ありません。ただし、異なる VRF インスタンスの使用を選択した場合は、正しい VRF インスタンスを使用するように、非シード Cisco NX-OS デバイスの aaa-private-sg を変更する必要があります。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

ネットワーク内のシード Cisco NX-OS デバイスが設定されていることを確認します。

手順の概要

1. **configure terminal**
2. **aaa group server radius aaa-private-sg**
3. **use-vrf***vrf-name*
4. **exit**
5. （任意） **show radius-server groups aaa-private-sg**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**aaa group server radius aaa-private-sg**
	
	例：
	`switch(config)# aaa group server radius aaa-private-sg`
	`switch(config-radius)#`
		RADIUS サーバ グループ aaa-private-sg を指定し、RADIUS サーバ グループ コンフィギュレーション モードを開始します。

ステップ 3	**use-vrf***vrf-name* 例： `switch(config-radius)# use-vrf MyVRF`	AAA サーバ グループの管理 VRF インスタンスを指定します。

ステップ 4	**exit**
	
	例：
	`switch(config-radius)# exit`
	`switch(config)#`
		RADIUS サーバ グループ コンフィギュレーション モードを終了します。

ステップ 5	**show radius-server groups aaa-private-sg** 例： `switch(config)# show radius-server groups aaa-private-sg`	（任意） デフォルト サーバ グループ用の RADIUS サーバ グループの設定を表示します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Cisco TrustSec の認証、許可、SAP、およびデータ パス セキュリティの設定

ここでは、Cisco TrustSec の認証、許可、SAP、およびデータ パス セキュリティの設定作業について説明します。

Cisco TrustSec の認証および許可の設定プロセス

Cisco TrustSec の認証および許可を設定するには、次の手順を行います。

手順の概要

1. Cisco TrustSec 機能をイネーブルにします。
2. Cisco TrustSec 認証をイネーブルにします。
3. インターフェイスに対して Cisco TrustSec の 802.1X 認証をイネーブルにします。

手順の詳細

ステップ 1 Cisco TrustSec 機能をイネーブルにします。

ステップ 2 Cisco TrustSec 認証をイネーブルにします。

ステップ 3 インターフェイスに対して Cisco TrustSec の 802.1X 認証をイネーブルにします。

Cisco TrustSec 認証のイネーブル化

インターフェイスに対して Cisco TrustSec 認証をイネーブルにする必要があります。デフォルトでは、データパス リプレイ保護機能がイネーブルになり、SAP 動作モードは GCM-encrypt です。

注意 Cisco TrustSec 認証の設定を有効にするには、インターフェイスのイネーブル化とディセーブル化を行う必要があり、インターフェイス上のトラフィックが中断されます。

（注） Cisco TrustSec の 802.1X モードをイネーブルにすると、そのインターフェイス上の許可と SAP がイネーブルになります。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port* [-*port2*]
3. **cts dot1x**
4. （任意） **no replay-protection**
5. （任意） **sap modelist** {**gcm-encrypt** | **gmac** | **no-encap** | **null**}
6. **exit**
7. **shutdown**
8. **no shutdown**
9. **exit**
10. （任意） **show cts interface** {**all** | **brief** | **ethernet***slot*/*port*}
11. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet***slot*/*port* [-*port2*]
	
	例：
	`switch(config)# interface ethernet 2/2`
	`switch(config-if)#`
		単一ポートまたはポート範囲を指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**cts dot1x**
	
	例：
	`switch(config-if)# cts dot1x`
	`switch(config-if-cts-dot1x)#`
		Cisco TrustSec の 802.1X 認証をイネーブルにして、Cisco TrustSec 802.1X コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	**no replay-protection** 例： `switch(config-if-cts-dot1x)# no replay-protection`	（任意） リプレイ保護をディセーブルにします。デフォルトではイネーブルになっています。
ステップ 5	**sap modelist** {**gcm-encrypt** | **gmac** | **no-encap** | **null**} 例： `switch(config-if-cts-dot1x)# sap modelist gcm-encrypt`	（任意） インターフェイスに SAP 動作モードを設定します。 GCM 暗号化の場合は **gcm-encrypt** キーワードを使用します。このオプションがデフォルトです。 GCM 認証のみの場合は **gmac** キーワードを使用します。 SAP をカプセル化せず、SGT の挿入も行わない場合は、**no-encap** キーワードを使用します。 認証および暗号化を行わずにカプセル化のみを行うには、**null** キーワードを使用します。

ステップ 6	**exit**
	
	例：
	`switch(config-if-cts-dot1x)# exit`
	`switch(config-if)#`
		Cisco TrustSec 802.1X コンフィギュレーション モードを終了します。

ステップ 7	**shutdown** 例： `switch(config-if)# shutdown`	インターフェイスをディセーブルにします。
ステップ 8	**no shutdown** 例： `switch(config-if)# no shutdown`	インターフェイスをイネーブルにして、インターフェイスの Cisco TrustSec 認証をイネーブルにします。

ステップ 9	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 10	**show cts interface** {**all** | **brief** | **ethernet***slot*/*port*} 例： `switch(config)# show cts interface all`	（任意） インターフェイスに対する Cisco TrustSec の設定を表示します。
ステップ 11	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスおよびポート プロファイルに対する Cisco TrustSec データパス リプレイ保護の設定

デフォルトでは、Cisco NX-OS ソフトウェアによってデータパス リプレイ保護機能をイネーブルにします。接続デバイスが SAP をサポートしていない場合は、レイヤ 2 Cisco TrustSec のインターフェイスでデータパス リプレイ保護をディセーブルにできます。

ポートプロファイルに対してこの作業を行うと、グループに参加するすべてのポートプロファイルに設定が継承されます。

注意 データパス リプレイ保護の設定を有効にするには、インターフェイスのイネーブル化とディセーブル化を行う必要があり、インターフェイス上のトラフィックが中断されます。

はじめる前に

インターフェイスの Cisco TrustSec 認証がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port* [-*port2*]
3. **cts dot1x**
4. **no replay-protection**
5. **exit**
6. **shutdown**
7. **no shutdown**
8. **exit**
9. （任意） **show cts interface** {**all** | **brief** | **ethernet***slot*/*port*}
10. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 2	**interface ethernet***slot*/*port* [*-port2*]
	
	例：
	`switch(config)# interface ethernet 2/2`
	`switch(config-if)#`
		単一ポートまたはポート範囲を指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**cts dot1x**
	
	例：
	`switch(config-if)# cts dot1x`
	`switch(config-if-cts-dot1x)#`
		Cisco TrustSec の 802.1X 認証をイネーブルにして、Cisco TrustSec 802.1X コンフィギュレーション モードを開始します。

ステップ 4	**no replay-protection** 例： `switch(config-if-cts-dot1x)# no replay-protection`	データパス リプレイ保護をディセーブルにします。デフォルトではイネーブルになっています。 インターフェイスでデータパス リプレイ保護をイネーブルにするには、**replay-protection** コマンドを使用します。

ステップ 5	**exit**
	
	例：
	`switch(config-if-cts-dot1x)# exit`
	`switch(config-if)#`
		Cisco TrustSec 802.1X コンフィギュレーション モードを終了します。

ステップ 6	**shutdown** 例： `switch(config-if)# shutdown`	インターフェイスをディセーブルにします。
ステップ 7	**no shutdown** 例： `switch(config-if)# no shutdown`	インターフェイスをイネーブルにして、インターフェイスのデータパス リプレイ保護機能をディセーブルにします。

ステップ 8	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 9	**show cts interface** {**all** | **brief** | **ethernet***slot*/*port*} 例： `switch(config)# show cts interface all`	（任意） インターフェイスに対する Cisco TrustSec の設定を表示します。
ステップ 10	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスおよびポート プロファイルに対する Cisco TrustSec SAP 動作モードの設定

レイヤ 2 Cisco TrustSec のインターフェイスに SAP 動作モードを設定できます。デフォルトの SAP 動作モードは GCM-encrypt です。

ポートプロファイルに対してこの作業を行うと、グループに参加するすべてのポートプロファイルに設定が継承されます。

注意 SAP動作モードの設定を有効にするには、インターフェイスのイネーブル化とディセーブル化を行う必要があり、インターフェイス上のトラフィックが中断されます。

はじめる前に

インターフェイスの Cisco TrustSec 認証がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port* [**-***port2*]
3. **cts dot1x**
4. **sap modelist** [**gcm-encrypt** | **gmac** | **no-encap** | **null**]
5. **exit**
6. **shutdown**
7. **no shutdown**
8. **exit**
9. （任意） **show cts interface** {**all** | **brief** | **ethernet***slot*/*port*}
10. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 2	**interface ethernet***slot/port* [*-port2*]
	
	例：
	`switch(config)# interface ethernet 2/2`
	`switch(config-if)#`
		単一のインターフェイスまたはインターフェイス範囲を指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**cts dot1x**
	
	例：
	`switch(config-if)# cts dot1x`
	`switch(config-if-cts-dot1x)#`
		Cisco TrustSec の 802.1X 認証をイネーブルにして、Cisco TrustSec 802.1X コンフィギュレーション モードを開始します。

ステップ 4	**sap modelist** [**gcm-encrypt** | **gmac** | **no-encap** | **null**] 例： `switch(config-if-cts-dot1x)# sap modelist gmac`	インターフェイスに SAP 認証モードを設定します。 GCM 暗号化の場合は **gcm-encrypt** キーワードを使用します。このオプションがデフォルトです。 GCM 認証のみの場合は **gmac** キーワードを使用します。 インターフェースで SAP をカプセル化せず、SGT の挿入も行わない場合は、**no-encap** キーワードを使用します。 認証およびインターフェースでの SAP 暗号化を行わずにカプセル化のみを行うには、**null** キーワードを使用します。カプセル化されるのは SGT だけです。

ステップ 5	**exit**
	
	例：
	`switch(config-if-cts-dot1x)# exit`
	`switch(config-if)#`
		Cisco TrustSec 802.1X コンフィギュレーション モードを終了します。

ステップ 6	**shutdown** 例： `switch(config-if)# shutdown`	インターフェイスをディセーブルにします。
ステップ 7	**no shutdown** 例： `switch(config-if)# no shutdown`	インターフェイスをイネーブルにして、そのインターフェイスの SAP 動作モードをイネーブルにします。

ステップ 8	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 9	**show cts interface** {**all** | **brief** | **ethernet***slot*/*port*} 例： `switch(config)# show cts interface all`	（任意） インターフェイスに対する Cisco TrustSec の設定を表示します。
ステップ 10	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスおよびポート プロファイルに対する Cisco TrustSec SGT 伝播の設定

レイヤ 2 インターフェイスでの SGT の伝播機能は、デフォルトでイネーブルになっています。インターフェイスに接続しているピア デバイスで SGT がタグ付けされた Cisco TrustSec パケットを制御できない場合は、そのインターフェイスで SGT 伝播機能をディセーブルにすることができます。

ポートプロファイルに対してこの作業を行うと、グループに参加するすべてのポートプロファイルに設定が継承されます。

注意 SGT の伝播の設定を有効にするには、インターフェイスのイネーブル化とディセーブル化を行う必要があり、インターフェイス上のトラフィックが中断されます。

はじめる前に

インターフェイスの Cisco TrustSec 認証がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port* [-*port2*]
3. **cts dot1x**
4. **no propagate-sgt**
5. **exit**
6. **shutdown**
7. **no shutdown**
8. **exit**
9. （任意） **show cts interface** {**all** | **brief** | **ethernet***slot*/*port*}
10. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet***slot*/*port* [-*port2*]
	
	例：
	`switch(config)# interface ethernet 2/2`
	`switch(config-if)#`
		単一ポートまたはポート範囲を指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**cts dot1x**
	
	例：
	`switch(config-if)# cts dot1x`
	`switch(config-if-cts-dot1x)#`
		Cisco TrustSec の 802.1X 認証をイネーブルにして、Cisco TrustSec 802.1X コンフィギュレーション モードを開始します。

ステップ 4	**no propagate-sgt** 例： `switch(config-if-cts-dot1x)# no propagate-sgt`	SGT 伝播をディセーブルにします。デフォルトではイネーブルになっています。 インターフェイスで SGT 伝播をイネーブルにするには、**propagate-sgt** コマンドを使用します。

ステップ 5	**exit**
	
	例：
	`switch(config-if-cts-dot1x)# exit`
	`switch(config-if)#`
		Cisco TrustSec 802.1X コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 6	**shutdown** 例： `switch(config-if)# shutdown`	インターフェイスをディセーブルにします。
ステップ 7	**no shutdown** 例： `switch(config-if)# no shutdown`	インターフェイスをイネーブルにして、インターフェイスのデータパス リプレイ保護機能をディセーブルにします。

ステップ 8	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 9	**show cts interface** {**all** | **brief** | **ethernet***slot*/*port*} 例： `switch(config)# show cts interface all`	（任意） インターフェイスに対する Cisco TrustSec の設定を表示します。
ステップ 10	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスの SAP キーの再生成

SAP交換をトリガーして、新しいキーセットを生成し、インターフェイス上のデータ トラフィックを保護できます。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

手順の概要

1. **cts rekey ethernet***slot*/*port*
2. （任意） **show cts interface** {**all** | **brief** | **ethernet** *slot*/*port*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**cts rekey ethernet***slot*/*port* 例： `switch# cts rekey ethernet 2/3`	インターフェイスの SAP キーを生成します。
ステップ 2	**show cts interface** {**all** | **brief** | **ethernet** *slot*/*port*} 例： `switch# show cts interface all`	（任意） インターフェイスに対する Cisco TrustSec の設定を表示します。

手動での Cisco TrustSec 認証の設定

Cisco NX-OS デバイスに Cisco Secure ACS へのアクセス権がない場合や、MAC アドレス認証バイパス機能がイネーブルになっていて認証が必要でない場合には、インターフェイスに手動で Cisco TrustSec を設定することも可能です。接続の両側のインターフェイスに手動で設定する必要があります。

（注） 半二重モードのインターフェイスでは、Cisco TrustSec をイネーブルにできません。インターフェイスが半二重モードに設定されているかどうかを調べるには、**show interface** コマンドを使用します。

注意 手動モードでの Cisco TrustSec の設定を有効にするには、インターフェイスのイネーブル化とディセーブル化を行う必要があり、インターフェイス上のトラフィックが中断されます。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **interface***interfaceslot*/*port*
3. **cts manual**
4. **sap pmk** {*key*[**left-zero-padded**] [**display encrypt**] | **encrypted***encrypted_pmk* | **use-dot1x**} [**modelist** {**gcm-encrypt** |**gcm-encrypt-256** | **gmac** | **no-encap** | **null**}]
5. （任意） **policy dynamic identity***peer-name*
6. （任意） **policy static sgt***tag* [**trusted**]
7. **exit**
8. **shutdown**
9. **no shutdown**
10. **exit**
11. （任意） **show cts interface** {**all** | **brief** | **ethernet***slot*/*port*}
12. （任意） **show cts sap pmk** {**all** | **interface ethernet***slot*/*port*}
13. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface***interfaceslot*/*port*
	
	例：
	`switch(config)# interface ethernet 2/2`
	`switch(config-if)#`
		インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**cts manual**
	
	例：
	`switch(config-if)# cts manual`
	`switch(config-if-cts-manual)#`
		Cisco TrustSec 手動コンフィギュレーション モードを開始します。
		（注） 半二重モードのインターフェイスでは、Cisco TrustSec をイネーブルにできません。

ステップ 4	**sap pmk** {*key*[**left-zero-padded**] [**display encrypt**]	**encrypted***encrypted_pmk*	**use-dot1x**} [**modelist** {**gcm-encrypt** |**gcm-encrypt-256**	**gmac**	**no-encap**	**null**}]	SAP の Pairwise Master Key（PMK）と動作モードを設定します。Cisco TrustSec の手動モードでは、SAP はデフォルトでディセーブルになっています。 *key* 引数は、最大 32 文字の偶数文字数の 16 進値です。 PMK の長さが 32 バイト未満の場合に、入力された文字列の左側をゼロで埋めるには、**left-zero-padded** キーワードを使用します。

	コマンドまたはアクション	目的
	例： `switch(config-if-cts-manual)# sap pmk fedbaa modelist gmac`	設定された PMK が実行コンフィギュレーションの AES 暗号化形式で表示されるように指定するには、**display encrypt** キーワードを使用します。 暗号化された 64 バイトの PMK 文字列（16 進数で 128 文字）を指定するには、**encrypted***encrypted_pmk* キーワードを使用します。 ピア デバイスが Cisco TrustSec 802.1X 認証または許可をサポートせず、SAP データ パス暗号化と認証をサポートしている場合は、**use-dot1x** キーワードを使用します。 モードのリストには、次に示すデータ パス暗号化と認証の暗号モードを指定します。 GCM 暗号化の場合は **gcm-encrypt** キーワードを使用します。このオプションがデフォルトです。 GCM 暗号化の場合は **gcm-encrypt-256** キーワードを使用します。 GCM 認証の場合は **gmac** キーワードを使用します。 カプセル化と SGT 挿入を行わない場合は、**no-encap** キーワードを使用します。 認証または暗号化なしで SGT のカプセル化を行うには、**null** キーワードを使用します。
ステップ 5	**policy dynamic identity***peer-name* 例： `switch(config-if-cts-manual)# policy dynamic identity MyDevice2`	（任意） ダイナミック許可ポリシーのダウンロードを設定します。*peer-name* 引数は、ピア デバイスの Cisco TrustSec デバイス ID です。ピア名では、大文字と小文字が区別されます。 （注） Cisco TrustSec クレデンシャルが設定されていることおよび Cisco TrustSec の AAA が設定されていることを確認します。 （注） **policy dynamic** コマンドと **policy static** コマンドは同時に使用できません。一度に 1 つしか適用できません。交互に変更するには、他のコマンドを設定する前に、このコマンドの **no** 形式を使用して設定を削除する必要があります。
ステップ 6	**policy static sgt***tag* [**trusted**] 例： `switch(config-if-cts-manual)# policy static sgt 0x2`	（任意） スタティック許可ポリシーを設定します。*tag* 引数は、10 進値または **0x***hhhh* 形式の 16 進値です。10 進数の範囲は 2 ～ 65519 で、16 進数の範囲は 0x2 ～ 0xffef です。**trusted** キーワードを指定すると、SGT 付きでインターフェイスにトラフィックが着信した場合、そのタグは上書きされません。

	コマンドまたはアクション	目的
		（注） **policy dynamic** コマンドと **policy static** コマンドは同時に使用できません。一度に 1 つしか適用できません。交互に変更するには、他のコマンドを設定する前に、このコマンドの **no** 形式を使用して設定を削除する必要があります。

ステップ 7	**exit**
	
	例：
	`switch(config-if-cts-manual)# exit`
	`switch(config-if)#`
		Cisco TrustSec 手動コンフィギュレーション モードを終了します。

ステップ 8	**shutdown** 例： `switch(config-if)# shutdown`	インターフェイスをディセーブルにします。
ステップ 9	**no shutdown** 例： `switch(config-if)# no shutdown`	インターフェイスをイネーブルにして、インターフェイスの Cisco TrustSec 認証をイネーブルにします。

ステップ 10	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 11	**show cts interface** {**all** | **brief** | **ethernet***slot*/*port*} 例： `switch# show cts interface all`	（任意） インターフェイスの Cisco TrustSec 設定を表示します。
ステップ 12	**show cts sap pmk** {**all** | **interface ethernet***slot*/*port*} 例： `switch# show cts sap pmk all`	（任意） すべてのインターフェイスまたは特定のイーサネットインターフェイスに対し設定された PMK の 16 進値を表示します。
ステップ 13	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスでの Cisco TrustSec のポーズ フレームの暗号化または復号化の設定

ポーズ フレームは、イーサネット フロー制御に使用される MAC 制御フレームです。一部のラインカードのポートは、ポーズ フレームの暗号化と復号化を実行します。一方、他のラインカードのポートにはこの機能がありません。このような不一致により相互運用性の問題が発生し、ポートはポーズ フレームを廃棄するか、無視します。

ポーズ フレームを暗号化するか、または個々のインターフェイス上でクリアするかを決定できます。接続の両側のインターフェイスを設定する必要があります。dot1x または手動モードのいずれかを使用して実行できます。2 つのポートが CTS リンクを実現するように接続され、一方がクリア Pause Capable、他方がセキュア（暗号化または復号化）Pause Capable である場合、ポーズ フレームは、正しく送受信するために、クリア テキストでリンク間に送信する必要があります。

（注） Cisco NX-OS Release 6.2.2 以降では、すべての F シリーズおよび M1 シリーズ モジュールにおいてセキュア（暗号化および復号）フレームとクリア ポーズ フレームの両方がサポートされています。以前のリリースでは、F1 シリーズ モジュール、F2 シリーズ モジュール、F2e シリーズ モジュール、および N7K-M132XP-12(L) モジュールは クリア ポーズ フレームのみサポートしています。

（注） 半二重モードのインターフェイスでは、Cisco TrustSec をイネーブルにできません。インターフェイスが半二重モードに設定されているかどうかを調べるには、**show interface** コマンドを使用します。

注意 ポーズ フレームの暗号化または復号化の設定を有効にするには、インターフェイスのイネーブル化とディセーブル化を行う必要があり、インターフェイス上のトラフィックが中断されます。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

flowcontrol {**send** | **receive**} コマンドを使用して、インターフェイスでフロー制御がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port*
3. **cts dot1x** or **cts manual**
4. [**no**] **encrypt pause-frame**
5. **exit**
6. **shutdown**
7. **no shutdown**
8. **exit**
9. （任意） **show cts interface** {**all** | **brief** | **ethernet***slot*/*port*}
10. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet***slot*/*port*
	
	例：
	`switch(config)# interface ethernet 2/2`
	`switch(config-if)#`
		インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**cts dot1x** or **cts manual**
	
	例：
	`switch(config-if)# cts dot1x`
	`switch(config-if-cts-dot1x)#`
		Cisco TrustSec dot1x または手動コンフィギュレーション モードを開始します。
		（注） 半二重モードのインターフェイスでは、Cisco TrustSec をイネーブルにできません。

ステップ 4	[**no**] **encrypt pause-frame** 例： `switch(config-if-cts-dot1x)# no encrypt pause-frame`	インターフェイスの Cisco TrustSec のポーズ フレームの暗号化または復号化を設定します。**no encrypt pause-frame** が設定されている場合、ポーズ フレームは暗号化されずに送信されます。**encrypt pause-frame** が設定されている場合、ポーズ フレームは CTS リンク上で暗号化されて送信されます。

ステップ 5	**exit**
	
	例：
	`switch(config-if-cts-dot1x)# exit`
	`switch(config-if)#`
		Cisco TrustSec dot1x または手動コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 6	**shutdown** 例： `switch(config-if)# shutdown`	インターフェイスをディセーブルにします。
ステップ 7	**no shutdown** 例： `switch(config-if)# no shutdown`	インターフェイスをイネーブルにしたり、インターフェイス上で Cisco TrustSec のポーズ フレームの暗号化または復号化をイネーブルにしたりします。

ステップ 8	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 9	**show cts interface** {**all** | **brief** | **ethernet***slot*/*port*} 例： `switch# show cts interface all`	（任意） インターフェイスの Cisco TrustSec 設定を表示します。
ステップ 10	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

SGACL ポリシーの設定

ここでは、SGACL ポリシーの設定作業について説明します。

SGACL ポリシーの設定プロセス

Cisco TrustSec の SGACL ポリシーを設定するには、次の手順を行います。

ステップ 1 パフォーマンスを向上させるためには、全体的に SGACL バッチ プログラミングをイネーブルにします。

ステップ 2 レイヤ 2 インターフェイスの場合は、Cisco TrustSec がイネーブルになっているインターフェイスがある VLAN に対して、SGACL ポリシーの強制をイネーブルにします。

ステップ 3 レイヤ 3 インターフェイスの場合は、Cisco TrustSec がイネーブルになっているインターフェイスがある VRF インスタンスに対して、SGACL ポリシーの強制をイネーブルにします。

ステップ 4 SGACL ポリシーの設定のダウンロードに Cisco Secure ACS 上の AAA を使用しない場合は、SGACL のマッピングとポリシーを手動で設定します。

SGACL バッチ プログラミングのイネーブル化

セキュリティ グループ アクセス コントロール リスト（SGACL）のプログラミングのバッチ処理をイネーブルにするには、次のタスクを実行します。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# [**no**] **cts role-based policy batched-programming enable**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# [**no**] **cts role-based policy batched-programming enable**	SGACL プログラミング関連タスクのバッチ処理をイネーブルにします。 この機能を明示的にイネーブルにした後に SGACL バッチ プログラミングをディセーブルにするには、このコマンドの **no** 形式を使用します。

VLAN に対する SGACL ポリシーの強制のイネーブル化

SGACL を使用する場合、Cisco TrustSec がイネーブルになっているレイヤ 2 インターフェイスがある VLAN 内で、 SGACL ポリシーの強制をイネーブルにする必要があります。

（注） この操作は、FCoE VLAN では実行できません。

はじめる前に

- Cisco TrustSec がイネーブルになっていることを確認します。
- SGACL バッチ プログラミングがイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **vlan***vlan-id*
3. **cts role-based enforcement**
4. **exit**
5. （任意） **show cts role-based enable**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**vlan***vlan-id*
	
	例：
	`switch(config)# vlan 10`
	`switch(config-vlan)#`
		VLAN を指定し、VLAN コンフィギュレーション モードを開始します。

ステップ 3	**cts role-based enforcement** 例： `switch(config-vlan)# cts role-based enforcement`	VLAN に対する Cisco TrustSec SGACL ポリシーの強制をイネーブルにします。

	コマンドまたはアクション	目的
		（注） VLAN で cts role-based enforcement をイネーブルにし、ポートでその他の設定をイネーブルにしないように設定すると、それらのポートを通過するトラフィックには (0,0) SGACL が適用されます。この SGACL はスタティックに設定することができ、Cisco ISE からダウンロードすることもできます。

ステップ 4	**exit**
	
	例：
	`switch(config-vlan)# exit`
	`switch(config)#`
		VLAN 設定を保存し、VLAN コンフィギュレーション モードを終了します。

ステップ 5	**show cts role-based enable** 例： `switch(config)# show cts role-based enable`	（任意） Cisco TrustSec SGACL 強制の設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

VRF インスタンスでの SGACL ポリシーの強制のイネーブル化

SGACL を使用する場合、Cisco TrustSec がイネーブルになっているレイヤ 3 インターフェイスがある VRF インスタンス内で、SGACL ポリシーの強制をイネーブルにする必要があります。

（注） 管理 VRF インスタンスの場合は、SGACL ポリシーの強制をイネーブルにできません。

はじめる前に

- Cisco TrustSec がイネーブルになっていることを確認します。
- SGACL バッチ プログラミングがイネーブルになっていることを確認します。
- ダイナミック アドレス解決プロトコル（ARP）インスペクションまたは Dynamic Host Configuration Protocol（DHCP）スヌーピングがイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **vrf context***vrf-name*
3. **cts role-based enforcement**
4. **exit**
5. （任意） **show cts role-based enable**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**vrf context***vrf-name*
	
	例：
	`switch(config)# vrf context MyVrf`
	`switch(config-vrf)#`
		VRF インスタンスを指定し、VRF コンフィギュレーション モードを開始します。

ステップ 3	**cts role-based enforcement** 例： `switch(config-vrf)# cts role-based enforcement`	VRF インスタンスに対する Cisco TrustSec SGACL ポリシーの強制をイネーブルにします。

ステップ 4	**exit**
	
	例：
	`switch(config-vrf)# exit`
	`switch(config)#`
		VRF コンフィギュレーション モードを終了します。

ステップ 5	**show cts role-based enable** 例： `switch(config)# show cts role-based enable`	（任意） Cisco TrustSec SGACL 強制の設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

SGACL ロギングの設定

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

ステップ 1 グローバル コンフィギュレーション モードを開始します。
switch# **configure terminal**

ステップ 2 SGACL の詳細ロギングをイネーブルにします。
switch(config)# **cts role-based detailed-logging**

ステップ 3 IP アクセス リストの詳細ロギングをイネーブルにします。
switch(config)# **[no] logging ip access-list detailed**

ステップ 4 （任意） 端末モニタで ACLLOG SYSLOG が表示されるようにロギング レベルのデフォルト値を変更します。
switch(config)# **logging level acllog 6**

ステップ 5 （任意） キャッシュの出力を最近の接続のみに制限するために、15秒ごとにキャッシュをクリアします。
switch(config)# **logging ip access-list cache interval 15**

ステップ 6 グローバル コンフィギュレーション モードを終了します。
switch(config)# **exit**

ステップ 7 詳細ロギングの IP アクセス リストと ACE アクションに関する情報を表示します。
switch# **show logging ip access-list cache detail**

ステップ 8 （任意） Cisco TrustSec の実行コンフィギュレーションを表示します。
switch# **show run cts**

SGACL ロギングの設定

この例では、実行コンフィギュレーションに続き、詳細ロギングのIPアクセスリストを表示する検証コマンドを示します。出力内で強調されている部分はモニタ モードと ACE アクションのステータスです。プレースホルダは実際の設定に応じた値に置き換えてください。

```
configure terminal
 cts role-based detailed-logging
 logging ip access-list detailed
 logging level acllog 6
 logging ip access-list cache interval 15
.
.
.
switch(config)# sh logging ip access-list cache detail
SGT     Src IP         Dst IP      S-Port    D-Port    Src Intf       Protocol  Monitor
 ACL-Name  ACE-Number ACE-Action      ACL-Direction    ACL-Filter-Type    ACL Applied Intf
    Hits
-------------------------------------------------------------------------------------------
40      4.1.1.2      3.1.1.1     0       0         Ethernet4/11 (1)ICMP     (1 )ON     ----
```

```
    -----       Deny           -----            -----             -----            0
   ---------------------------------------------------------------------------------
10      1.1.1.1      2.1.1.2     0       0         Ethernet4/46 (1)ICMP    (1 )ON    ----
    -----       Permit         -----            -----             -----            8

-------------------------------------------------------------------------------
20      2.1.1.2      1.1.1.1     0       0         Ethernet4/34 (1)ICMP    (0 )OFF    ----
    -----       Deny           -----            -----             -----            3

-------------------------------------------------------------------------------
30      3.1.1.1      4.1.1.2     0       0         Ethernet8/48 (1)ICMP    (0 )OFF    ----
    -----       Permit         -----            -----             -----            0

-------------------------------------------------------------------------------

Number of cache entries: 4
```

次の例では、**monitor all** をイネーブルにしたときの詳細ロギングを示します。

```
switch(config)# show logging ip access-list  cache detail
SGT     Src IP        Dst IP     S-Port    D-Port    Src Intf      Protocol          Monitor
    ACL-Name  ACE-Number    ACE-Action    ACL-Direction    ACL-Filter-Type    ACL Applied
Intf    Hits
-------------------------------------------------------------------------------------------
26      172.16.2.6       10.1.1.1           0       0         Ethernet6/14 (1)ICMP   (1 )ON
     ----     -----          Deny          -----            -----              -----
         20
-------------------------------------------------------------------------------

Number of cache entries: 1
```

（注） この出力では、ログに Deny と表示されていますが、Monitor (1) ON と表示されている場合はトラフィックは拒否されません。

次の例は、システム ログを示しています。

```
2016 Jan 22 10:48:47 xbow-vdc4 %$ VDC-4 %$ %ACLLOG-6-ACLLOG_FLOW_INTERVAL: Src IP: 172.16.2.6,
 Dst IP: 10.1.1.1, Src Port: 0, Dst Port: 0, Src Intf: Ethernet6/14, Protocol: "ICMP"(1),
Monitor: (1)"ON" , ACL Name: ---, ACE Action: Deny, Appl Intf: ---, Hit-count: 20
```

次の例は、CTS ポリシーを示しています。

```
switch# show cts  role-based  policy

sgt:26
dgt:101 rbacl:test(monitored)
        deny ip log

switch# show running-config  cts

!Command: show running-config cts
!Time: Fri Jan 22 11:01:54 2016

version 7.3(0)D1(1)
feature cts
cts role-based counters enable
cts role-based detailed-logging
cts role-based monitor enable
cts role-based monitor all
cts role-based sgt-map 10.1.1.1 101
cts role-based sgt-map 172.16.2.6 26
cts role-based access-list permit
  permit ip log
cts role-based access-list test
  deny ip log
cts role-based sgt 26 dgt 101 access-list test
```

```
cts role-based enforcement

logging level cts 6

switch(config)# show cts role-based counters

RBACL policy counters enabled
Counters last cleared: 01/22/2016 at 10:58:27 AM

sgt:26 dgt:101  [20]
rbacl:test(monitored)
        deny ip log     [20]

switch(config)# show system internal access-list output entries detail  module 6

Flags: F - Fragment entry  E - Port Expansion
       D - DSCP Expansion  M - ACL Expansion
       T - Cross Feature Merge Expansion

                VDC-4 VRF table 1 :
                ====================

INSTANCE 0x0
---------------

  Tcam 0 resource usage:
  ----------------------
  Label_a = 0x200
   Bank 0
   ------
     IPv4 Class
       Policies: Rbacl()
       Netflow profile: 0
       Netflow deny profile: 0
       Entries:
         [Index] Entry [Stats]
         ---------------------
  [0014:000a:000a] prec 3 permit ip 0.0.0.26/32 0.0.0.101/32  log  [0]
  [0015:000b:000b] prec 3 permit ip 0.0.0.0/0 0.0.0.0/0  log  [0]
  [0016:000c:000c] prec 3 permit ip 0.0.0.0/0 0.0.0.0/0   [0]


  L4 protocol cam entries usage: none

  No mac protocol cam entries are in use


INSTANCE 0x1
---------------

  Tcam 0 resource usage:
  ----------------------
  Label_a = 0x200
   Bank 0
   ------
     IPv4 Class
       Policies: Rbacl()
       Netflow profile: 0
       Netflow deny profile: 0
       Entries:
         [Index] Entry [Stats]
         ---------------------
  [0014:000a:000a] prec 3 permit ip 0.0.0.26/32 0.0.0.101/32  log  [20]

  [0015:000b:000b] prec 3 permit ip 0.0.0.0/0 0.0.0.0/0  log  [0]
  [0016:000c:000c] prec 3 permit ip 0.0.0.0/0 0.0.0.0/0   [0]
```

SGACL モニタ モードの設定

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

カウンタがイネーブルになっていることを確認します。

ステップ 1 グローバル コンフィギュレーション モードを開始します。
switch# **configure terminal**

ステップ 2 SGACL の詳細ロギングをイネーブルにします。
switch(config)# **cts role-based detailed-logging**

ステップ 3 必要に応じて、次のいずれかを実行します。

- すべての SGACL に対してモニタリング モードをイネーブルにします。

  switch(config)# **[no] cts role-based monitor all**

- SGT-DGT ペアごとにモニタリングをイネーブルにします。

  switch(config)# **[no] cts role-based monitor permissions from** {*sgt*|**unknown**} **to** {*dgt*|**unknown**} [**ipv4**| **ipv6**]

  IPv4 ロールベース アクセス コントロール リスト（RBACLs）のモニタリングはデフォルトでイネーブルになっています。現在、IPv6 オプションはサポートされていません。

ステップ 4 Cisco TrustSec SGACL ポリシーとペアごとのモニタ モード機能に関する詳細を表示します。
switch(config)# **show cts role-based policy**

ステップ 5 RBACL 統計情報のモニタリング ステータスを表示し、すべての RBACL ポリシーの統計情報を一覧表示します。
switch(config)# **show cts role-based counters**

（注） 他の **show** コマンドを使用して SGACL syslog を表示することもできます。

ステップ 6 （任意） Cisco TrustSec の実行コンフィギュレーションを表示します。
switch(config)# **show run cts**

SGACL モニタ モードの設定

この例では、SGT 20 から DGT 30 までの SGACL モニタ モードを設定する際の実行コンフィギュレーションを示します。プレースホルダは実際の設定に応じた値に置き換えてください。

```
configure terminal
 cts role-based detailed-logging
 cts role-based monitor permissions from <20> to <30>
 exit
```

SGACL モニタ モード情報の表示

次の例では、Cisco TrustSec SGACL ポリシーと、SGT-DGT ペアごとのモニタ モード機能の詳細を示します。

```
switch(config)# sh cts role-based policy

sgt:unknown
dgt:unknown     rbacl:rbacl1
        permit ip log

sgt:10
dgt:20  rbacl:rbacl1(monitored)
        permit ip log

sgt:20
dgt:10  rbacl:rbacl2
        deny ip log

sgt:30
dgt:40  rbacl:rbacl1
        permit ip

sgt:40
dgt:30  rbacl:rbacl2(monitored)
        deny ip

sgt:any
dgt:any rbacl:rbacl1
        permit ip log
```

次の例では、RBACL 統計情報のモニタリング ステータスと、すべての RBACL ポリシーの統計情報を示します。

```
switch(config)# sh cts role-based counters

RBACL policy counters enabled
Counters last cleared: 12/23/2015 at 01:41:46 AM

sgt:unknown dgt:unknown [0]
rbacl:rbacl1
        permit ip log   [0]

sgt:10 dgt:20   [5]
rbacl:rbacl1(monitored)
        permit ip log   [5]

sgt:20 dgt:10   [5]
rbacl:rbacl2
        deny ip log     [5]

sgt:30 dgt:40   [0]
rbacl:rbacl1
        permit ip   [0]

sgt:40 dgt:30   [0]
rbacl:rbacl2(monitored)
        deny ip     [0]

sgt:any dgt:any [0]
rbacl:rbacl1
        permit ip log   [0]
```

次の例では、Cisco TrustSec の実行コンフィギュレーションを示します。

```
switch(config)# show run cts

!Command: show running-config cts
!Time: Wed Dec 23 02:01:43 2015

version 7.3(0)D1(1)
```

```
feature cts
cts role-based counters enable
cts role-based detailed-logging
cts role-based monitor enable
cts role-based sgt-map 1.1.1.1 10
cts role-based sgt-map 2.1.1.2 20
cts role-based sgt-map 3.1.1.1 30
cts role-based sgt-map 4.1.1.2 40
cts role-based access-list rbacl1
  permit ip log
cts role-based access-list rbacl2
  deny ip log
cts role-based sgt 0 dgt 0 access-list rbacl1
cts role-based sgt 10 dgt 20 access-list rbacl1
cts role-based sgt 20 dgt 10 access-list rbacl2
cts role-based sgt 30 dgt 40 access-list rbacl1
cts role-based sgt 40 dgt 30 access-list rbacl2
cts role-based sgt any dgt any access-list rbacl1
cts role-based monitor permissions from 10 to 20
cts role-based monitor permissions from 40 to 30
cts role-based enforcement
```

次の例では、SGACL ロギングを含まない Cisco TrustSec の実行コンフィギュレーションを示します。

```
switch(config)# show run cts

!Command: show running-config cts
!Time: Wed Dec 23 02:01:43 2015

version 7.3(0)D1(1)
feature cts
cts role-based counters enable
cts role-based detailed-logging
cts role-based monitor enable
cts role-based sgt-map 1.1.1.1 10
cts role-based sgt-map 2.1.1.2 20
cts role-based sgt-map 3.1.1.1 30
cts role-based sgt-map 4.1.1.2 40
cts role-based access-list rbacl1
  permit ip log
cts role-based access-list rbacl2
  deny ip log
cts role-based access-list rbacl1_no_log
  permit ip
cts role-based access-list rbacl2_no_log
  deny ip
cts role-based sgt 0 dgt 0 access-list rbacl1
cts role-based sgt 10 dgt 20 access-list rbacl1
cts role-based sgt 20 dgt 10 access-list rbacl2
cts role-based sgt 30 dgt 40 access-list rbacl1_no_log
cts role-based sgt 40 dgt 30 access-list rbacl2_no_log
cts role-based sgt any dgt any access-list rbacl1
cts role-based monitor permissions from 10 to 20
cts role-based monitor permissions from 40 to 30
cts role-based enforcement
```

Cisco TrustSec SGT の手動設定

このデバイスから発信されるパケットに、固有の Cisco TrustSec Security Group Tag（SGT）を手動で設定できます。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

ステップ 1 グローバル コンフィギュレーション モードを開始します。
switch# **configure terminal**

ステップ 2 デバイスから送信されるパケットの SGT を設定します。
switch(config)# **cts sgt***tag*

（注） *tag* 引数は、10 進値または **0x***hhhh* 形式の 16 進値です。10 進数の範囲は 2 ～ 65519 で、16 進数の範囲は 0x2 ～ 0xffef です。

ステップ 3 グローバル コンフィギュレーション モードを終了します。
switch(config)# **exit**

ステップ 4 （任意） Cisco TrustSec の環境データ情報を表示します。
switch# **show cts environment-data**

ステップ 5 （任意） 実行中のコンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。
switch# **copy running-config startup-config**

VLAN に対する IPv4 アドレスと SGACL SGT のマッピングの手動設定

Cisco NX-OS デバイスに使用可能な Cisco Secure ACS、ダイナミック ARP インスペクション、または DHCP スヌーピングが搭載されていない場合は、IPv4 アドレスを VLAN の SGACL SGT マッピングに手動で設定することもできます。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

VLAN の SGACL ポリシーの強制がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **vlan***vlan-id*
3. **cts role-based sgt-map***ipv4-address tag*
4. **exit**
5. （任意） **show cts role-based sgt-map**[**summary** | **sxp peer** *peer-ipv4-addr* | **vlan** *vlan-id* | **vrf** *vrf-name*]
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**vlan***vlan-id*
	
	例：
	`switch(config)# vlan 10`
	`switch(config-vlan)#`
		VLAN を指定し、VLAN コンフィギュレーション モードを開始します。

ステップ 3	**cts role-based sgt-map***ipv4-address tag* 例： `switch(config-vlan)# cts role-based sgt-map 10.10.1.1 100`	VLAN に対する SGACL ポリシーの SGT マッピングを設定します。

ステップ 4	**exit**
	
	例：
	`switch(config-vlan)# exit`
	`switch(config)#`
		VLAN 設定を保存し、VLAN コンフィギュレーション モードを終了します。

ステップ 5	**show cts role-based sgt-map**[**summary** | **sxp peer** *peer-ipv4-addr* | **vlan** *vlan-id* | **vrf** *vrf-name*] 例： `switch(config)# show cts role-based sgt-map`	（任意） Cisco TrustSec SGACL SGT のマッピング設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

VRF インスタンスに対する IPv4 アドレスと SGACL SGT のマッピングの手動設定

SGACL ポリシー設定のダウンロードに Cisco Secure ACS を使用できない場合は、IPv4 アドレスと SGACL SGT のマッピングを VRF インスタンスに手動で設定できます。Cisco NX-OS デバイスで、Cisco Secure ACS、ダイナミック ARP インスペクション、DHCP スヌーピングを使用できない場合は、この機能を使用できます。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

VRF インスタンスの SGACL ポリシーの強制がイネーブルになっていることを確認します。

レイヤ 3 モジュールがイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **vrf context** *vrf-name*
3. **cts role-based sgt-map***ipv4-address tag*
4. **exit**
5. （任意） **show cts role-based sgt-map** [**summary** | **sxp peer** *peer-ipv4-addr* | **vlan** *vlan-id* | **vrf** *vrf-name*]
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**vrf context** *vrf-name*
	
	例：
	`switch(config)# vrf context accounting`
	`switch(config-vrf)#`
		VRF インスタンスを指定し、VRF コンフィギュレーション モードを開始します。

ステップ 3	**cts role-based sgt-map***ipv4-address tag* 例： `switch(config-vrf)# cts role-based sgt-map 10.10.1.1 100`	VLAN に対する SGACL ポリシーの SGT マッピングを設定します。

ステップ 4	**exit**
	
	例：
	`switch(config-vrf)# exit`
	`switch(config)#`
		VRF コンフィギュレーション モードを終了します。

ステップ 5	**show cts role-based sgt-map** [**summary** | **sxp peer** *peer-ipv4-addr* | **vlan** *vlan-id* | **vrf** *vrf-name*] 例： `switch(config)# show cts role-based sgt-map`	（任意） Cisco TrustSec SGACL SGT のマッピング設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

VLAN と SGT のマッピングの設定

VLAN を SGT にマッピングできます。この手順は、VLAN には対応しているが SGT には非対応のデバイスに対して CTS を配置するのに役立ちます。ホストまたはサーバに割り当てられている VLAN に基づき、そのホストまたはサーバに SGT を割り当てることができます。この VLAN からのトラフィックには、所定の SGT のマークが付けられます。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **vlan***vlan-id*
3. **cts role-based sgt***sgt-value*
4. **exit**
5. （任意） **show cts role-based sgt vlan** {**all** | *vlan-id*}
6. （任意） **show cts role-based sgt-map** [**summary** | **sxp peer** *peer-ipv4-addr* | **vlan** *vlan-id* | **vrf** *vrf-name*]
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**vlan***vlan-id*
	
	例：
	`switch(config)# vlan 10`
	`switch(config-vlan)#`
		VLAN を指定し、VLAN コンフィギュレーション モードを開始します。

ステップ 3	**cts role-based sgt***sgt-value* 例： `switch(config-vlan)# cts role-based sgt 3`	SGT に VLAN をマッピングします。*sgt-value* 引数の範囲は 1 ～ 65519 です。

ステップ 4	**exit**
	
	例：
	`switch(config-vlan)# exit`
	`switch(config)#`
		VLAN 設定を保存し、VLAN コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 5	**show cts role-based sgt vlan** {**all** | *vlan-id*} 例： `switch(config)# show cts role-based sgt vlan all`	（任意） 指定した VLAN に対し設定された SGT を表示します。
ステップ 6	**show cts role-based sgt-map** [**summary** | **sxp peer** *peer-ipv4-addr* | **vlan** *vlan-id* | **vrf** *vrf-name*] 例： `switch(config)# show cts role-based sgt-map summary`	（任意） SGT のマッピングを表示します。
ステップ 7	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

SGACL ポリシーの手動設定

SGACL ポリシー設定のダウンロードに Cisco Secure ACS を使用しない場合は、Cisco NX-OS デバイスに手動で SGACL ポリシーを設定できます。ロールベース アクセス コントロール リスト（RBACL）ロギングをイネーブルにすることもできます。これにより、ユーザは、Cisco NX-OS デバイスに着信する特定タイプのパケットをモニタできるようになります。

（注） システムで ACLLOG と RBACL の syslog が生成される前に、記録されたパケットがレート制限され、フローがキャッシュされます。**show logging ip access-list cache detail** コマンドを使用すると、記録されたパケットの Source Group Tag（SGT）を表示できます。このコマンドの詳細については、『*Cisco Nexus 7000 Series NX-OS System Management Command Reference*』を参照してください。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

Cisco TrustSec ロギングを機能させるには、Cisco TrustSec カウンタまたは統計情報をイネーブルにする必要があります。

VLAN および VRF インスタンスに対する SGACL ポリシーの強制がイネーブルになっていることを確認します。

RBACL ロギングをイネーブルにする場合は、VLAN および VRF インスタンスに対する RBACL ポリシーの強制がイネーブルになっていることを確認します。

RBACL ロギングをイネーブルにする場合は、ACLLOG syslog のログレベルが 6 に、CTS マネージャ syslog のログレベルが 5 に設定されていることを確認します。

RBACL ロギングをイネーブルにする場合は、CTS マネージャ syslog のログ レベルが 6 以下に設定されていることを確認します。

手順の概要

1. **configure terminal**
2. **cts role-based access-list** *list-name*
3. （任意） {**deny** | **permit**} **all** [**log**]
4. （任意） {**deny** | **permit**} **icmp** [**log**]
5. （任意） {**deny** | **permit**} **igmp** [**log**]
6. （任意） {**deny** | **permit**} **ip** [**log**]
7. （任意） {**deny** | **permit**} **tcp** [{**dst** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number* | **range***port-number1 port-number2*}] [**log**]
8. {**deny** | **permit**} **udp** [{**dst** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number* | **range***port-number1 port-number2*}] [**log**]
9. **exit**
10. **cts role-based sgt** {*sgt-value* | **any** | **unknown**} **dgt** {*dgt-value* | **any** | **unknown**} **access-list***list-name*
11. （任意） **show cts role-based access-list**
12. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**cts role-based access-list** *list-name*
	
	例：
	`switch(config)# cts role-based access-list MySGACL`
	`switch(config-rbacl)#`
		SGACL を指定し、ロールベース アクセス リスト コンフィギュレーション モードを開始します。*list-name* 引数には、大文字と小文字を区別して、最大 32 文字の英数字で値を指定します。

ステップ 3	{**deny**	**permit**} **all** [**log**] 例： `switch(config-rbacl)# deny all log`	（任意） すべてのトラフィックを拒否または許可します。必要に応じて **log** キーワードを使用して、この設定と一致するパケットが記録されるように指定することができます。

	コマンドまたはアクション	目的
ステップ 4	{**deny** | **permit**} **icmp** [**log**] 例： `switch(config-rbacl)# permit icmp`	（任意） インターネット制御メッセージ プロトコル（ICMP）トラフィックを拒否または許可します。必要に応じて**log**キーワードを使用して、この設定と一致するパケットが記録されるように指定することができます。
ステップ 5	{**deny** | **permit**} **igmp** [**log**] 例： `switch(config-rbacl)# deny igmp`	（任意） インターネット グループ管理プロトコル（IGMP）トラフィックを拒否または許可します。必要に応じて **log** キーワードを使用して、この設定と一致するパケットが記録されるように指定することができます。
ステップ 6	{**deny** | **permit**} **ip** [**log**] 例： `switch(config-rbacl)# permit ip`	（任意） IP トラフィックを拒否または許可します。必要に応じて **log** キーワードを使用して、この設定と一致するパケットが記録されるように指定することができます。
ステップ 7	{**deny** | **permit**} **tcp** [{**dst** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number* | **range***port-number1 port-number2*}] [**log**] 例： `switch(config-rbacl)# deny tcp dst eq 100`	（任意） TCP トラフィックを拒否または許可します。デフォルトではすべての TCP トラフィックが許可されます。*port-number*、*port-number1*、port-number2 の引数の範囲は 0 ～ 65535 です。必要に応じて **log** キーワードを使用して、この設定と一致するパケットが記録されるように指定することができます。
ステップ 8	{**deny** | **permit**} **udp** [{**dst** | **src**} {{**eq** | **gt** | **lt** | **neq**} *port-number* | **range***port-number1 port-number2*}] [**log**] 例： `switch(config-rbacl)# permit udp src eq 1312`	UDP トラフィックを拒否または許可します。デフォルトではすべての UDP トラフィックが許可されます。*port-number*、*port-number1*、port-number2 の引数の範囲は 0 ～ 65535 です。必要に応じて **log** キーワードを使用して、この設定と一致するパケットが記録されるように指定することができます。

ステップ 9	**exit**
	
	例：
	`switch(config-rbacl)# exit`
	`switch(config)#`
		ロールベース アクセス リスト コンフィギュレーション モードを終了します。

ステップ 10	**cts role-based sgt** {*sgt-value* | **any** | **unknown**} **dgt** {*dgt-value* | **any** | **unknown**} **access-list***list-name* 例： `switch(config)# cts role-based sgt 3 dgt 10 access-list MySGACL`	SGT 値と SGACL をマッピングします。*sgt-value* 引数と *dgt-value* 引数の範囲は、0 ～ 65520 です。 （注） SGT と SGACL をマッピングするには、あらかじめ SGACL を作成しておく必要があります。

	コマンドまたはアクション	目的
ステップ 11	**show cts role-based access-list** 例： `switch(config)# show cts role-based access-list`	（任意） Cisco TrustSec SGACL の設定を表示します。
ステップ 12	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ダウンロードされた SGACL ポリシーの表示

Cisco TrustSec のデバイス クレデンシャルと AAA の設定後、Cisco Secure ACS からダウンロードされた Cisco TrustSec SGACL ポリシーを検証できます。Cisco NX-OS ソフトウェアは、インターフェイスに対する認証および許可、SXP、または IPv4 アドレスおよび SGACL SGT の手動マッピングによって新しい SGT を学習すると、SGACL ポリシーをダウンロードします。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

手順の概要

1. **show cts role-based access-list**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show cts role-based access-list** 例： `switch# show cts role-based access-list`	Cisco TrustSec SGACL を表示します（Cisco Secure ACS からダウンロードされたものと Cisco NX-OS デバイスに手動で設定されたものの両方）。

ダウンロードされた SGACL ポリシーのリフレッシュ

Cisco Secure ACS によって Cisco NX-OS デバイスにダウンロードされた SGACL ポリシーをリフレッシュできます。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

手順の概要

1. **cts refresh role-based-policysgt** {*sgt-value* | **any** | **unknown**}
2. （任意） **show cts role-based policy**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**cts refresh role-based-policysgt** {*sgt-value* | **any** | **unknown**}
	
	例：
	`switch# cts refresh role-based-policy`
	
	例：
	`switch# cts refresh role-based-policy sgt any`
		Cisco Secure ACS からの Cisco TrustSec SGACL をリフレッシュします。
		• **sgt**：SGT の出力ポリシーが更新されます。
		• *sgt-value*：指定した SGT の出力ポリシーが更新されます。
		• **any**：すべての SGT の出力ポリシーが更新されます。
		• **unknown**：不明な SGT の出力ポリシーが更新されます。

ステップ 2	**show cts role-based policy** 例： `switch# show cts role-based policy`	（任意） Cisco TrustSec SGACL ポリシーを表示します。

環境データの更新

AAA サーバから環境データのダウンロードを更新できます。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

Cisco Identity Services Engine（ISE）リリース 1.0 以降を使用していることを確認します。

手順の概要

1. **cts refresh environment-data**
2. **show cts environment-data**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**cts refresh environment-data** 例： `switch# cts refresh environment-data`	AAA サーバから環境データをリフレッシュします。
ステップ 2	**show cts environment-data** 例： `switch# show cts environment-data`	ローカル デバイスに関するダウンロードされた環境データを表示します。 （注） SGT 名テーブル エントリは ISE からダウンロードできます。

RBACL の統計情報のイネーブル化

ロールベース アクセス コントロール リスト（RBACL）ポリシーと一致するパケット数のカウントを要求できます。この統計情報は、 Source Group Tag（SGT）と Destination Group Tag（DGT）ごとに収集されます。

（注） RBACL ポリシーを変更するとき、割り当て済みのアクセス コントロール エントリ（ACE）の統計情報が表示され、新しく割り当てられた ACE 統計情報が 0 に初期化されます。

（注） RBACL 統計情報は、Cisco NX-OS デバイスのリロード時または統計情報を故意にクリアしたときにだけ失われます。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

RBACL 統計情報をイネーブルにする場合は、VLAN および VRF インスタンスに対する RBACL ポリシーの強制がイネーブルになっていることを確認します。

RBACL 統計情報をイネーブルにするには、ハードウェアのエントリが各ポリシーに 1 つずつ必要です。ハードウェアに十分な領域が残っていない場合は、エラー メッセージが表示され、統計情報をイネーブルにできません。

手順の概要

1. **configure terminal**
2. **[no] cts role-based counters enable**
3. （任意） **copy running-config startup-config**
4. **exit**
5. （任意） **show cts role-based counters [sgt** {*sgt-value* | **any** | **unknown**}] [**dgt** {*dgt-value* | **any** | **unknown**}]
6. （任意） **clear cts role-based counters**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**[no] cts role-based counters enable** 例： `switch(config)# cts role-based counters enable`	RBACL 統計情報をイネーブルまたはディセーブルにします。デフォルトではディセーブルになっています。
ステップ 3	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 5	**show cts role-based counters [sgt** {*sgt-value* | **any** | **unknown**}] [**dgt** {*dgt-value* | **any** | **unknown**}] 例： `switch# show cts role-based counters sgt 10 dgt 20`	（任意） RBACL 統計情報の設定ステータスを表示し、すべての RBACL ポリシーの統計情報を一覧表示します。必要に応じて、特定の Source Group Tag（SGT）または Destination Group Tag（DGT）の RBACL ポリシーと一致するパケットの合計数を表示します。*sgt-value* 引数と *dgt-value* 引数の範囲は、0 ～ 65519 です。
ステップ 6	**clear cts role-based counters** 例： `switch# clear cts role-based counters`	（任意） すべてのカウンタが 0 にリセットされるように、RBACL 統計情報をクリアします。

Cisco TrustSec の SGACL ポリシーのクリア

Cisco TrustSec の SGACL ポリシーをクリアできます。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

手順の概要

1. （任意） **show cts role-based policy**
2. **clearcts policy** {**all** | **peer***device-name* | **sgt***sgt-value*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show cts role-based policy** 例： `switch# clear cts policy all`	（任意） Cisco TrustSec RBACL ポリシーの設定を表示します。
ステップ 2	**clearcts policy** {**all**	**peer***device-name*	**sgt***sgt-value*} 例： `switch# clear cts policy all`	Cisco TrustSec 接続情報のポリシーをクリアします。

SXP の手動設定

SGT Exchange Protocol（SXP）を使用すると、Cisco TrustSec のハードウェア サポートがないネットワーク デバイスに SGT を伝播できます。ここでは、ネットワーク内の Cisco NX-OS デバイスに Cisco TrustSec SXP を設定する手順について説明します。

Cisco TrustSec SXP の設定プロセス

Cisco TrustSec SXP の手動による設定手順は次のとおりです。

手順の概要

1. Cisco TrustSec 機能をイネーブルにします。
2. VRF インスタンスに対する SGACL ポリシーの強制をイネーブルにします。
3. Cisco TrustSec SXP をイネーブルにします。
4. SXP ピア接続を設定します。

手順の詳細

ステップ 1 Cisco TrustSec 機能をイネーブルにします。

ステップ 2 VRF インスタンスに対する SGACL ポリシーの強制をイネーブルにします。

ステップ 3 Cisco TrustSec SXP をイネーブルにします。

ステップ 4 SXP ピア接続を設定します。

（注） SXP には管理（mgmt 0）接続は使用できません。

Cisco TrustSec SXP のイネーブル化

ピアの接続を設定する前に、Cisco TrustSec SXP をイネーブルにする必要があります。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **cts sxp enable**
3. **exit**
4. （任意） **show cts sxp**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**cts sxp enable** 例： `switch(config)# cts sxp enable`	Cisco TrustSec の SXP をイネーブルにします。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 4	**show cts sxp** 例： `switch# show cts sxp`	（任意） SXP の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Cisco TrustSec SXP のピア接続の設定

スピーカーおよびリスナーの両方のデバイスで SXP ピア接続を設定する必要があります。パスワード保護を使用している場合は、必ず両エンドに同じパスワードを使用してください。

（注） デフォルトの SXP 送信元 IP アドレスが設定されていない場合に、接続の SXP 送信元アドレスを指定しないと、Cisco NX-OS ソフトウェアは既存のローカル IP アドレスから SXP 送信元 IP アドレスを抽出します。その Cisco NX-OS デバイスから開始される各 TCP 接続で SXP 送信元アドレスが異なる可能性があります。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

SXP がイネーブルになっていることを確認します。

VRF インスタンスの RBACL ポリシーの強制がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **cts sxp connection peer***peer-ipv4-addr*[**source***src-ipv4-addr*] **password** {**default** | **none** | **required***password*} **mode**{**speaker** |**listener**| **local** | **peer** | **speaker**}} [**vrf***vrf-name*]
3. **exit**
4. （任意） **show cts sxp connections**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**cts sxp connection peer***peer-ipv4-addr*[**source***src-ipv4-addr*] **password** {**default** | **none** | **required***password*} **mode**{**speaker** |**listener**| **local** | **peer** | **speaker**}} [**vrf***vrf-name*] 例： `switch(config)# cts sxp connection peer 10.10.1.1 source 20.20.1.1 password default mode listener`	SXP アドレス接続を設定します。 **source** キーワードには発信元デバイスの IPv4 アドレスを指定します。デフォルトの発信元は、**cts sxp default source-ip** コマンドを使用して設定した IPv4 アドレスです。 **password** キーワードには、SXP で接続に使用するパスワードを指定します。次のオプションがあります。 • **cts sxp default password** コマンドを使用して設定したデフォルトの SXP パスワードを使用するには、**default** オプションを使用します。 • パスワードを使用しないようにするには **none** オプションを使用します。 • コマンドで指定したパスワードを使用するには、**required** オプションを使用します。 • リスナーをスピーカーとして使用し、スピーカーをリスナーとして使用するには、**local** キーワードを使用します • ピア デバイスを SXP リスナーとして使用するには、**peer** キーワードを使用します。 **speaker** および **listener** キーワードは、リモート ピア デバイスのロールを指定します。 **vrf** キーワードでは、ピアに対する VRF インスタンスを指定します。デフォルトはデフォルト VRF インスタンスです。

	コマンドまたはアクション	目的
		（注） SXP には管理（mgmt 0）インターフェイスを使用できません。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 4	**show cts sxp connections** 例： `switch# show cts sxp connections`	（任意） SXP 接続とステータスを表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

デフォルトの SXP パスワードの設定

デフォルトでは、SXP は接続のセットアップ時にパスワードを使用しません。Cisco NX-OS デバイスにデフォルトの SXP パスワードを設定できます。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

SXP がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **cts sxp default password***password*
3. **exit**
4. （任意） **show cts sxp**
5. （任意） **show running-config cts**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**cts sxp default password***password* 例： `switch(config)# cts sxp default password A2Q3d4F5`	SXP のデフォルト パスワードを設定します。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 4	**show cts sxp** 例： `switch# show cts sxp`	（任意） SXP の設定を表示します。
ステップ 5	**show running-config cts** 例： `switch# show running-config cts`	（任意） 実行コンフィギュレーションの SXP 設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

デフォルトの SXP 送信元 IPv4 アドレスの設定

Cisco NX-OS ソフトウェアは、送信元 IPv4 アドレスが指定されないと、新規の TCP 接続すべてにデフォルトの送信元 IPv4 アドレスを使用します。デフォルトの送信元 IP アドレスが変更されると既存の SXP 接続がリセットされ、SXP を通じて学習された IP-SGT バインディングがクリアされます。送信元 IP アドレスが設定されている SXP 接続では、復帰する際に同じ IP アドレスが使用されます。

送信元 IP アドレスが設定されていない SXP 接続では、デフォルトの IP アドレスが送信元 IP アドレスとして使用されます。このような接続が正常に動作するためには、正しい宛先 IP アドレスがピアで設定されていて、デフォルトの送信元 IP アドレスに到達可能であることが必要条件となります。デバイスにデフォルトの送信元 IP アドレスを設定する前に、動作中の既存の接続がこれらの条件を満たしているかどうかを確認することを推奨します。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

SXP がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **cts sxp default source-ip***src-ip-addr*
3. **exit**
4. （任意） **show cts sxp**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**cts sxp default source-ip***src-ip-addr* 例： `switch(config)# cts sxp default source-ip 10.10.3.3`	SXP のデフォルトの送信元 IPv4 アドレスを設定します。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 4	**show cts sxp** 例： `switch# show cts sxp`	（任意） SXP の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

SXP 復帰期間の変更

ピアがSXP接続を終了すると、内部ホールドダウンタイマーが開始されます。内部ホールドダウンタイマーが終了する前にピアが再接続すると、SXP復帰期間タイマーが開始されます。SXP復帰期間タイマーがアクティブな間、Cisco NX-OS ソフトウェアは前回の接続で学習した SGT マッピング エントリを保持し、無効なエントリを削除します。デフォルト値は 120 秒（2 分）です。SXP 復帰期間を 0 秒に設定すると、タイマーがディセーブルになり、前回の接続のすべてのエントリが削除されます。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

SXP がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **cts sxp reconcile-period***seconds*
3. **exit**
4. （任意） **show cts sxp**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**cts sxp reconcile-period***seconds* 例： `switch(config)# cts sxp reconcile-period 180`	SXP復帰タイマー期間を変更します。デフォルト値は 120 秒（2 分）です。範囲は 0 ～ 64000 です。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 4	**show cts sxp** 例： `switch# show cts sxp`	（任意） SXP の設定を表示します。

	コマンドまたはアクション	目的
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

SXP リトライ期間の変更

SXP リトライ期間によって、Cisco NX-OS ソフトウェアが SXP 接続を再試行する頻度が決まります。SXP 接続が正常に確立されなかった場合、Cisco NX-OS ソフトウェアは SXP リトライ期間タイマーの終了後に、新たな接続の確立を試行します。デフォルト値は 60 秒（1 分）です。SXP 再試行期間を 0 秒に設定するとタイマーは無効になり、接続は再試行されません。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

SXP がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **cts sxp retry-period***seconds*
3. **exit**
4. （任意） **show cts sxp**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**cts sxp retry-period***seconds* 例： `switch(config)# cts sxp retry-period 120`	SXP リトライ タイマー期間を変更します。デフォルト値は 60 秒（1 分）です。範囲は 0 ～ 64000 です。

	コマンドまたはアクション	目的

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 4	**show cts sxp** 例： `switch# show cts sxp`	（任意） SXP の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

SXPv3 の設定

はじめる前に

- Cisco TrustSec がイネーブルになっていることを確認します。
- SXP がイネーブルになっていることを確認します。
- Cisco TrustSec SXP ピア接続が設定されていることを確認します。

ステップ 1 グローバル コンフィギュレーション モードを開始します。
switch# **configure terminal**

ステップ 2 （任意） ネットワーク制限を拡大します。
switch(config)# **[no] cts sxp mapping network-map** [*num_bindings*]

（注） *num_bindings* パラメータでは 0 ～ 65535 の値を指定できます。ゼロ（0）は展開できないことを意味し、65535 では、最大展開制限が許可されます。デフォルト値は 0 です。

ステップ 3 サブネットと SGT のバインディングを設定します。
switch(config)# **cts role-based sgt-map** {*A.B.C.D/<0-32>*} *sgt-number*

ステップ 4 Cisco TrustSec SXP 設定の詳細を表示します。
switch (config)# **show cts sxp**

ステップ 5 サポートされる SXP バージョンを表示します。
switch(config)# **show cts sxp connection**

SXPv3 の設定

この例では、実行コンフィギュレーションに続き、Cisco TrustSec SXP 設定の詳細とサポートされる SXP バージョンを表示する検証コマンドを示します。プレースホルダは実際の設定に応じた値に置き換えてください。

```
configure terminal
 cts sxp enable
 cts sxp mapping network-map <64>
 cts role-based sgt-map <10.10.10.10/29> <1032>
.
.
.
switch(config)# show cts sxp
CTS SXP Configuration:
SXP enabled
SXP retry timeout:60
SXP reconcile timeout:120
Highest supported SXP version: 3
SXP network-map limit: 64
SXP default-route-SGT transport: Enabled
Unsupported SXP version(s): 2

switch(config)# show cts sxp connection
PEER_IP_ADDR    VRF             PEER_SXP_MODE   SELF_SXP_MODE   CONNECTION STATE    VERSION
30.1.1.3        default          listener        speaker          connected           3
```

SGT バインディングのデフォルト ルートの設定

はじめる前に

- Cisco TrustSec がイネーブルになっていることを確認します。
- SXP がイネーブルになっていることを確認します。
- Cisco TrustSec SXP ピア接続が設定されていることを確認します。

ステップ 1 グローバル コンフィギュレーション モードを開始します。
switch# **configure terminal**

ステップ 2 SGT バインディングのデフォルト ルートをイネーブルにします。
switch(config)# **[no] cts sxp allow default-route-sgt**

ステップ 3 スピーカーの SGT バインディングのデフォルト ルートを指定します。
switch(config)# **cts role-based sgt-map** {*0.0.0.0/0*} *sgt-number*

ステップ 4 Cisco TrustSec SXP 設定の詳細を表示します。
switch(config)# **show cts sxp**

SGT バインディングのデフォルト ルートの設定

この例では、実行コンフィギュレーションに続き、Cisco TrustSec SXP 設定の詳細を表示する検証コマンドを示します。プレースホルダは実際の設定に応じた値に置き換えてください。

```
configure terminal
 cts sxp enable
 cts sxp allow default-route-sgt
 cts role-based sgt-map <0.0.0.0/0> <200>
.
.
.
switch(config)# show cts sxp
CTS SXP Configuration:
SXP enabled
SXP retry timeout:60
SXP reconcile timeout:120
Highest supported SXP version:3
Network Map expansion limit:0
Default Route SGT Propagation: Enabled
Unsupported SXP version(s):2
```

サブネットと SGT のマッピングの設定

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

ステップ 1 グローバル コンフィギュレーション モードを開始します。
switch# **configure terminal**

ステップ 2 サブネットと SGT のマッピングを設定します。
switch(config)# **cts role-based sgt-map** {*ip-addr*|*prefix length*} *sgt*

（注） *sgt number* キーワード ペアでは、指定したサブネットの各ホスト アドレスにバインドする SGT 番号を指定します。

ステップ 3 すべての SGT バインディングを表示します。
switch(config)# **show cts role-based sgt-map**

ステップ 4 グローバル コンフィギュレーション モードを終了します。
switch(config)# **exit**

サブネットと SGT のマッピングの設定

この例では、実行コンフィギュレーションに続き、すべての SGT バインディングを表示する検証コマンドを示します。プレースホルダは実際の設定に応じた値に置き換えてください。

```
configure terminal
 cts role-based sgt-map <10.10.10.8/29> <6>
.
```

```
.
.
switch(config)# show cts role-based sgt-map
IP ADDRESS                              SGT     VRF/VLAN    SGT CONFIGURATION
10.10.10.8/29                           6        vrf:1      CLI Configured
12.1.0.0/16                             10       vrf:1      CLI Configured
12.1.1.1                                20       vrf:1      CLI Configured
12.1.1.2                                30       vlan:121   CLI Configured
```

ポート チャネル メンバでの Cisco TrustSec サポート

Cisco NX-OS Release 7.2(0)D1(1) 以前では、TrustSec 設定に関して、ポート チャネル メンバ インターフェイスで互換性が適用されませんでした。また、Cisco TrustSec 設定は、ポート チャネル インターフェイスで許可されませんでした。

Cisco NX-OS Release 7.2(0)D1(1) 以降では、ポート チャネル メンバで TrustSec 設定の互換性が適用され、ポート チャネル インターフェイスでの TrustSec 設定も許可されます。次のセクションでさらに詳しく説明します。

設定モデル

設定モデルを次に示します。

- ポート チャネル インターフェイスでの Cisco TrustSec 設定：

  ポート チャネル インターフェイスで設定された Cisco TrustSec 設定はすべて、その全メンバ インターフェイスに継承されます。

- ポート チャネル メンバ インターフェイスでの Cisco TrustSec 設定：

  ポート チャネル互換性パラメータは、ポート チャネル メンバ インターフェイスで設定できません。

  非互換性を生じない他の Cisco TrustSec 設定（MACSec 設定など）は、ポート チャネル メンバ インターフェイスで設定できます。

- ポート チャネルへの新しいメンバの追加：

  - **channel-group** コマンドの使用：

    ポート チャネルでの設定とすべてのメンバでの設定に互換性があれば、新しいメンバの追加は許可されます。そうでない場合、追加は拒否されます。

    （注） Cisco TrustSec がポート チャネルで設定されておらず、追加するメンバ上の Cisco TrustSec 設定が互換性がある場合、追加は許可され、ポート チャネルはメンバ インターフェイスから互換性パラメータを継承します。

  - **channel-group force** コマンドの使用：

    追加するインターフェイスがポート チャネル設定をサポートしている場合、ポート チャネルから互換性パラメータを継承し、追加は許可されます。ただし、追加されるイン

ターフェイスの一部がポート チャネル設定をサポートしない場合、追加は拒否されます。

Cisco NX-OS Release 7.2(0)D1(1) のユーザ インターフェイスの更新

次に、Cisco NX-OS Release 7.2(0)D1(1) のユーザ インターフェイスの更新を示します。

- Cisco TrustSec の設定になんらかの非互換性がある場合に **channel group** または **channel-group force** コマンドを発行すると、互換性のない設定を指摘するエラー メッセージがユーザに表示されます。
- **show run** および **show start** コマンドは、ポート チャネル インターフェイス上、および物理イーサネット インターフェイス上の Cisco TrustSec 設定を表示します。
- **show cts role-based sgt-map** コマンドは、ポート チャネル インターフェイス上で学習されたポートと SGT の学習されたマッピングを、必要に応じて表示します。

インサービス ソフトウェア アップグレード

この機能をサポートしない下位バージョンからインサービス ソフトウェアアップグレード（ISSU）が実行されると、ISSUが完了するとすぐに、すべてのポートチャネルが、最初に設定されたメンバ インターフェイスから互換性パラメータを継承します。設定の非互換性が検出されたポートチャネルについて、警告レベルの syslog が生成されます。

Cisco TrustSec の設定の確認

Cisco TrustSec の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show cts	Cisco TrustSec の情報を表示します。
show cts capability interface {**all** | **ethernet***slot*/*port*}	すべてのインターフェイスまたは特定のイーサネットインターフェイスの Cisco TrustSec 機能を表示します。

コマンド	目的
show cts authorization entries [**interfaceethernet***slot*/*port*.*subinterface*]	すべてのインターフェイスまたは特定のイーサネットインターフェイスに、Cisco TrustSec 許可の一部としてダウンロードされ保存されているピア ポリシー データが表示されます。
show cts credentials	EAP-FAST の Cisco TrustSec クレデンシャルを表示します。
show cts environment-data	Cisco TrustSec の環境データを表示します。
show cts interface{**all** | **brief** | **ethernet***slot*/*port*}	インターフェイスの Cisco TrustSec 設定を表示します。
show cts pacs	デバイス キー ストア内の Cisco TrustSec 許可情報と PAC を表示します。
show cts role-based access-list	Cisco TrustSec の SGACL 情報を表示します。
show cts role-based counters[**sgt***sgt-value*] [**dgt***dgt-value*]	RBACL 統計情報の設定ステータスを表示し、すべての RBACL ポリシーの統計情報を一覧表示します。必要に応じて、特定の Source Group Tag（SGT）または Destination Group Tag（DGT）の RBACL ポリシーと一致するパケットの合計数を表示します。
show cts role-based enable	Cisco TrustSec の SGACL 強制の状態を表示します。
show cts role-based policy [[**dgt** | **sgt**]{*value* | **any** | **unknown**}]	すべての宛先セキュリティ グループ タグ（DGT）と送信元セキュリティ グループ タグ（SGT）のペア、または指定した DGT または SGT の Cisco TrustSec SGACL ポリシー情報を表示します。

コマンド	目的
show cts role-based sgt-map[**summary** | **sxp peer***peer-ipv4-addr* | **vlan***vlan-id* | **vrf***vrf-name* | **cached** | **synched**]	Cisco TrustSec SGACL SGT のマップ設定を表示します。 • **summary**：SGT マッピングの概要を表示します。 • **sxp peer**：指定した SXP ピアの SGT マップ設定を表示します。 • **vlan**：指定した VLAN の SGT マップ設定を表示します。 • **vrf**：指定した VRF の SGT マップ設定を表示します。 • **cached**：キャッシュにより学習された SGT マップを表示します。 • **synched**：Cisco Fabric Services の同期により学習された SGT を表示します。
show cts role-based sgt vlan {**all** | *vlan-id*}	すべての VLAN または特定の VLAN に対する設定済み SGT を表示します。
show cts server-list	Cisco TrustSec シードおよびの非シード デバイスに使用可能な RADIUS サーバの保存されたリストのみを表示します。
show cts sxp[**connection** | **sgt-map**] [**vrf***vrf-name*]	Cisco TrustSec SXP の情報を表示します。
show running-config cts	実行コンフィギュレーションの Cisco TrustSec 情報を表示します。

Cisco TrustSec の設定例

ここでは、Cisco TrustSec の設定例を示します。

Cisco TrustSec のイネーブル化

Cisco TrustSec をイネーブルにする例を示します。

```
feature dot1x
feature cts
cts device-id device1 password Cisco321
```

シード Cisco NX-OS デバイスへの Cisco TrustSec AAA の設定

次の例では、シード Cisco NX-OS デバイスに Cisco TrustSec の AAA を設定します。

```
radius-server host 10.10.1.1 key Cisco123 pac
aaa group server radius Rad1
  server 10.10.1.1
  use-vrf management
aaa authentication dot1x default group Rad1
aaa authorization cts default group Rad1
```

インターフェイスに対する Cisco TrustSec 認証のイネーブル化

次の例では、インターフェイスに対して、クリア テキスト パスワードを使用する Cisco TrustSec 認証をイネーブルにします。

```
interface ethernet 2/1
  cts dot1x
  shutdown
  no shutdown
```

手動での Cisco TrustSec 認証の設定

次の例では、インターフェイスに手動スタティック ポリシーで Cisco TrustSec 認証を設定します。

```
interface ethernet 2/1
  cts manual
    sap pmk abcdef modelist gmac
    policy static sgt 0x20
```

次の例では、インターフェイスに手動ダイナミック ポリシーで Cisco TrustSec 認証を設定します。

```
interface ethernet 2/2
  cts manual
```

```
    policy dynamic identity device2
```

次の例では、設定された PMK が実行コンフィギュレーションの AES 暗号化形式で表示されるよう指定する方法を示します。

```
 interface ethernet 2/2
   cts manual
     sap pmk fedbaa display encrypt

show cts sap pmk interface ethernet 2/2
show running-config
```

デフォルト VRF インスタンスに対する Cisco TrustSec ロールベース ポリシー強制の設定

次の例では、デフォルト VRF インスタンスに対して Cisco TrustSec のロールベース ポリシー強制をイネーブルにします。

```
cts role-based enforcement
```

デフォルト以外の VRF に対する Cisco TrustSec ロールベース ポリシー強制の設定

次の例では、デフォルト以外の VRF に対して Cisco TrustSec のロールベース ポリシー強制をイネーブルにします。

```
vrf context test
  cts role-based enforcement
```

VLAN に対する Cisco TrustSec ロールベース ポリシー強制の設定

次の例では、VLAN に対して Cisco TrustSec のロールベース ポリシー強制をイネーブルにします。

```
vlan 10
  cts role-based enforcement
```

デフォルト VRF インスタンスに対する IPv4 アドレスと SGACL SGT のマッピングの設定

次の例では、デフォルト VRF インスタンスに対して Cisco TrustSec ロールベース ポリシーの IPv4 アドレス対 SGACL SGT マッピングを手動で設定します。

```
cts role-based sgt-map 10.1.1.1 20
```

デフォルト以外の VRF インスタンスに対する IPv4 アドレスと SGACL SGT のマッピングの設定

次の例では、デフォルト以外の VRF インスタンスに対して Cisco TrustSec ロールベース ポリシーの IPv4 アドレス対 SGACL SGT マッピングを手動で設定します。

```
vrf context test
  cts role-based sgt-map 30.1.1.1 30
```

VLAN に対する IPv4 アドレスと SGACL SGT のマッピングの設定

次の例では、VLAN に対して Cisco TrustSec ロールベース ポリシーの IPv4 アドレス対 SGACL SGT マッピングを手動で設定します。

```
vlan 10
  cts role-based sgt-map 20.1.1.1 20
```

Cisco TrustSec SGACL の手動設定

次に、Cisco TrustSec SGACL を手動で設定する例を示します。

```
cts role-based access-list abcd
  permit icmp
cts role-based sgt 10 dgt 20 access-list abcd
```

次に、RBACL ロギングをイネーブルにする例を示します。

```
cts role-based access-list RBACL1
  deny tcp src eq 1111 dest eq 2222 log
cts role-based sgt 10 dgt 20 access-list RBACL1
cts role-based sgt-map 1.1.1.1 10
cts role-based sgt-map 1.1.1.2 20
```

この設定では、次の ACLLOG syslog が生成されます。

```
%ACLLOG-6-ACLLOG_FLOW_INTERVAL: SGT: 10, Source IP: 1.1.1.1, Destination IP: 1.1.1.2, Source
```

```
Port: 1111, Destination Port: 2222, Source Interface: Ethernet4/1, Protocol: tcp, Hit-count
= 2
```

（注） ACLLOG syslog には、一致した RBACL ポリシーの Destination Group Tag（DGT）情報が含まれていません。この情報を検索するには、ログ メッセージで宛先 IP アドレスの IP-SGT マッピングを参照し、**show cts role-based sgt-map** コマンドを入力します。

次に、RBACL 統計情報をイネーブルおよび表示する例を示します。

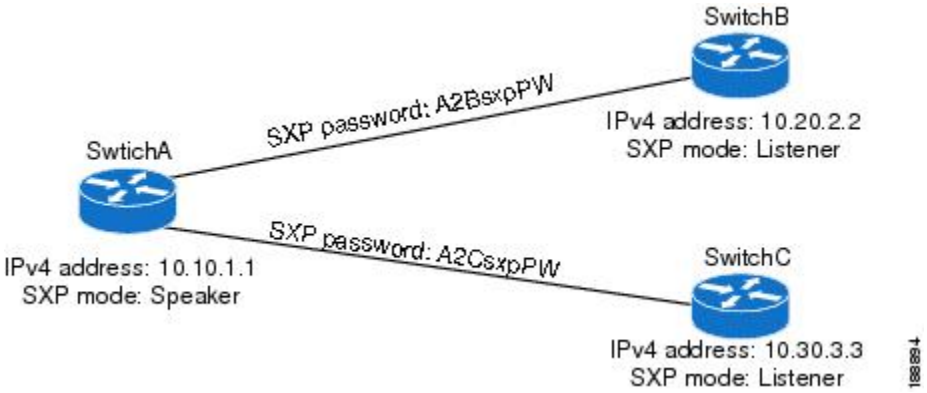
```
cts role-based counters enable
show cts role-based counters sgt 10 dgt 20


RBACL policy counters enabled
sgt: 10 dgt: 20 [180]
rbacl test1:
deny tcp src eq 1111 dest eq 2222   [75]
deny tcp src eq 2222 dest eq 3333   [25]
rbacl test2:
deny udp src eq 1111 dest eq 2222   [30]
deny udp src eq 2222 dest eq 3333   [50]
```

SXP ピア接続の手動設定

次の図に、デフォルト VRF インスタンスでの SXP ピア接続の例を示します。

図 *18*： *SXP* ピア接続の例



次に、SwitchA に SXP ピア接続を設定する例を示します。

```
feature cts
cts role-based enforcement
cts sxp enable
cts sxp connection peer 10.20.2.2 password required A2BsxpPW mode listener
cts sxp connection peer 10.30.3.3 password required A2CsxpPW mode listener
```

次に、SwitchB に SXP ピア接続を設定する例を示します。

```
feature cts
cts role-based enforcement
```

```
cts sxp enable
cts sxp connection peer 10.10.1.1 password required A2BsxpPW mode speaker
```

次に、SwitchC に SXP ピア接続を設定する例を示します。

```
feature cts
cts role-based enforcement
cts sxp enable
cts sxp connection peer 10.10.1.1 password required A2CsxpPW mode speaker
```

Cisco TrustSec に関する追加情報

ここでは、Cisco TrustSec の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS のライセンス	『*Cisco NX-OS Licensing Guide*』
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』

Cisco TrustSec の機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 *28*：*Cisco TrustSec* の機能の履歴

機能名	リリース	機能情報
SGACL ACLLOG	7.3(0)D1(1)	SGACL ロギングをイネーブルにする機能が追加されました。
SGACL モニタリング	7.3(0)D1(1)	SGACL のモニタリングをイネーブルにする機能が追加されました。
SXPv3	7.3(0)D1(1)	SGT 交換プロトコル バージョン3のサポートが追加されました。

機能名	リリース	機能情報
Cisco TrustSec サブネットと SGT のマッピング	7.3(0)D1(1)	Cisco TrustSec サブネットと SGT のマッピングのサポートが追加されました。
F3 の FabricPath での Cisco TrustSec MACsec	7.2(1)D1(1)	F3 シリーズ モジュールの FabricPath での Cisco TrustSec MACsec のサポートが追加されました。
ポート チャネル メンバでの Cisco TrustSec サポート	7.2(0)D1(1)	ポート チャネル メンバに Cisco TrustSec のサポートが追加されました。
Cisco TrustSec	6.2(10)	F3 シリーズ モジュールに対して SGT サポートが追加されました。
Cisco TrustSec	6.2(2)	VLAN を SGT にマップする機能が追加されました。
Cisco TrustSec	6.2(2)	SAP PMK を暗号化し、実行コンフィギュレーションに暗号化された形式で PMK を表示する機能が追加されました。
Cisco TrustSec	6.2(2)	設定された PMK の 16 進値を表示するための **show cts sap pmk** コマンドが追加されました。
Cisco TrustSec	6.2(2)	インターフェイスの Cisco TrustSec 機能を表示するための **show cts capability interface** コマンドが追加されました。
Cisco TrustSec	6.2(2)	10 進値を受け入れるための、**cts sgt**、**policy static sgt**、および **clear cts policy sqt** コマンドがイネーブルになりました。

機能名	リリース	機能情報
Cisco TrustSec	6.2(2)	ISE から sgname テーブルをダウンロードし、環境データ タイマーが切れると環境データを手動で更新する機能が追加されました。
Cisco TrustSec	6.2(2)	特定の SXP ピア、VLAN、または VRF に対する SGT マッピングまたは SGT マップ設定のサマリーを表示するためのオプションのキーワードが **show cts role-based sgt-map** コマンドに追加されました。
Cisco TrustSec	6.2(2)	すべての CTS 対応インターフェイスに関する概要を表示するための **brief** キーワードが **show cts interface** コマンドに追加されました。
Cisco TrustSec	6.2(2)	F2e および F2 シリーズ モジュールに対する SGT サポートが追加されました。
Cisco TrustSec	6.1(1)	Advanced Services ライセンスの要件を削除しました。
Cisco TrustSec	6.1(1)	40G および 100G M2 シリーズ モジュールの MACsec のサポートが追加されました。
Cisco TrustSec	6.0(1)	F2 シリーズ モジュールが更新されました。
Cisco TrustSec	5.2(1)	インターフェイス上のポーズ フレームの暗号化と復号化をサポートします。

機能名	リリース	機能情報
SGACL ポリシー	5.0(2)	RBACL ロギングのイネーブル化またはディセーブル化をサポートします。
SGACL ポリシー	5.0(2)	RBACL 統計情報のイネーブル化、ディセーブル化、モニタリング、およびクリアをサポートします。
Cisco TrustSec	4.2(1)	リリース 4.1 からの変更はありません。

第 14 章

Cisco TrustSec MACSec の設定

この章では、Cisco NX-OS デバイスに Cisco TrustSec MACSec を設定する手順について説明します。

この章は、次の項で構成されています。

- 機能情報の確認，513 ページ
- Cisco TrustSec MACSec の前提条件，514 ページ
- Cisco TrustSec MACSec の注意事項と制約事項，514 ページ
- Cisco TrustSec MACSec について，515 ページ
- Cisco TrustSec MACSec のライセンス要件，524 ページ
- Cisco TrustSec パラメータのデフォルト設定，525 ページ
- Cisco TrustSec MACSec の設定，526 ページ
- ポート チャネル メンバでの Cisco TrustSec サポート，544 ページ
- Cisco TrustSec MACSec の設定の確認，546 ページ
- Cisco TrustSec MACSec に関する追加情報，546 ページ
- Cisco TrustSec MACSec の機能の履歴，547 ページ

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

Cisco TrustSec MACSec の前提条件

Cisco TrustSec の前提条件は次のとおりです。

- デバイスが 6.1 よりも前の Cisco NX-OS リリースを実行している場合は、Advanced Services ライセンスをインストールする必要があります。
- 802.1X 機能をイネーブルにする必要があります。
- Cisco TrustSec 機能をイネーブルにする前に、802.1X 機能をイネーブルにする必要があります。802.1X インターフェイス レベルの機能が使用できませんが、デバイスが RADIUS で認証するためには 802.1X が必要です。
- Cisco TrustSec 機能をイネーブルにする必要があります。

Cisco TrustSec MACSec の注意事項と制約事項

Cisco TrustSec MACSec（802.1ae）のハードウェア サポートについては、Cisco Nexus 7000 I/O Module Comparison Matrix を参照してください。

Cisco TrustSec に関する注意事項と制約事項は次のとおりです。

Cisco TrustSec MACSec：SP により提供される擬似回線接続に MACSec を導入する際には、次の一連の要件を使用する必要があります。これらの要件は、SP から適切なサービス、品質、または特性を引き出すのに役立ちます。

Nexus 7000 は、DWDM を使用するものなど、ポイントツーポイント リンク上の MACSec、および次の条件を満たす EoMPLS などの非 PTP リンク上の MACSec をサポートします。

- MACSec リンク上のパケットは、順序変更やバッファリングができません。
- MACSec リンクに追加のフレームを挿入することはできません。
- エンドツーエンドのリンク イベント通知が必要です（サービスが中断されたときに顧客がリンク障害を知ることができるよう、エッジデバイスやどこかの中間デバイスでリンクが切れた場合は通知が送信される必要があります）。

40G以上で同じ帯域幅がある MACsec リンクでは、複数のセキュリティ アソシエーション（SCI/AN ペア）は、セキュリティ アソシエーション プロトコル（SAP）交換で設定します。

CTS MACSec ポート モードを Cache Engine（CE）モードから FabricPath モードに変更すると、ネイティブ VLAN タギングを FabricPath コア ポートでディセーブルにするまで、CTS MACSec リンクに CRC エラーが表示されます。CTS ポートで発生するこのような設定変更は、フラッピングされる必要があります。ただし、これによりトラフィックの中断が引き起こされる可能性があります。このような状況では、CRC エラーの表示とトラフィックの中断を避けるために、次のステップを実行します。

- CTS MACsec がイネーブルの間は、キャッシュ エンジン ポートをディセーブルにする。
- ポート モードを FabricPath モードに変更する。

- FabricPath コア ポートのネイティブ VLAN タギングをディセーブルにする。
- ポートをイネーブルにします。

M3 ライン カードと古いライン カードとを相互運用する場合、リンクを有効にするには、ユーザは M3 ライン カードのレガシー モードのみを設定する必要があります。両方のピアで設定が一致している必要があります。古いライン カードでは、GCM-256 ビット オプションは機能を利用できないため使用できません。

Cisco TrustSec MACSec について

ここでは、Cisco TrustSec MACSec について説明します。

Cisco TrustSec のアーキテクチャ

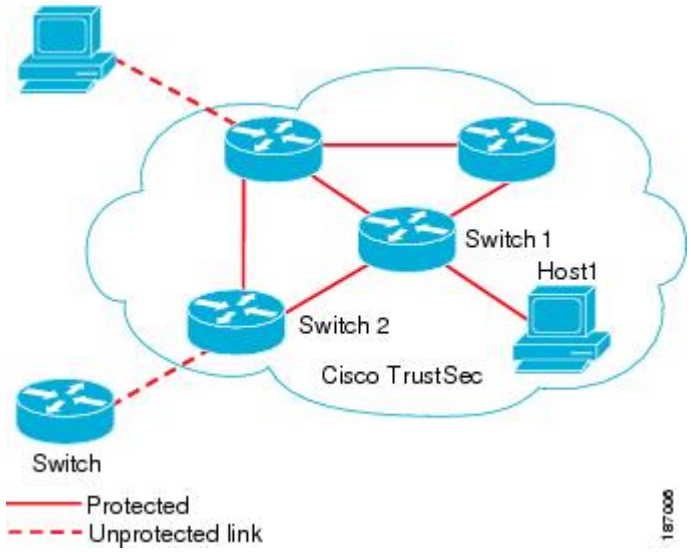
Cisco TrusSec のセキュリティ アーキテクチャは、信頼できるネットワーク デバイスのクラウドを確立することによってセキュア ネットワークを構築します。クラウド内の各デバイスは、そのネイバーによって認証されます。クラウド内のデバイス間リンクでの通信は、暗号化、メッセージ整合性検査、データパス リプレイ防止メカニズムを組み合わせたセキュリティで保護されます。また Cisco TrustSec は、認証時に取得されたデバイスおよびユーザの識別情報を、ネットワークに入る際のパケットの分類またはカラリングに使用します。このパケット分類は、Cisco TrustSec ネットワークへの入力時にパケットにタグ付けされることにより維持されます。タグによってパケットはデータ パス全体を通じて正しく識別され、セキュリティおよびその他のポリシー基準が適用されます。このタグは、セキュリティ グループ タグ（SGT）と呼ばれることもあります。エンドポイント装置が SGT に応じてトラフィックをフィルタリングできるようにすることにより、アクセス コントロール ポリシーをネットワークに強制できます。

（注） 入力とは、宛先へのパス上のパケットが最初の Cisco TrustSec 対応デバイスに入ることです。出力とは、パス上の最後の Cisco TrustSec 対応デバイスを出ることです。

次の図に、Cisco TrustSec クラウドの例を示します。この例では、Cisco TrustSec クラウド内に、ネットワーク接続されたデバイスが数台とエンドポイント装置が 1 台あります。エンドポイント

装置 1 台とネットワーク接続デバイス 1 台がクラウドの外部にあるのは、これらが Cisco TrustSec 対応デバイスでないか、またはアクセスを拒否されたからです。

図 *19*：*Cisco TrustSec* ネットワーク クラウドの例



Cisco TrustSec アーキテクチャは、主に次のコンポーネントで構成されています。

認証

Cisco TrustSec ネットワークにデバイスを加入させる前に、各デバイスの識別情報を検証します。

許可

認証されたデバイスの識別情報に基づいて、Cisco TrustSec ネットワークのリソースに対するデバイスのアクセス権のレベルを決定します。

アクセス コントロール

各パケットのソース タグを使用して、パケット単位でアクセス ポリシーを適用します。

セキュアな通信

Cisco TrustSec ネットワークの各リンク上のパケットに、暗号化、整合性検査、およびデータパス リプレイ防止を提供します。

Cisco TrustSec ネットワークには、次のエンティティがあります。

サプリカント

Cisco TrustSec ネットワークへの加入を試行するデバイス

オーセンティケータ（AT）

すでに Cisco TrustSec ネットワークに含まれているデバイス

許可サーバ

認証情報、許可情報、またはその両方を提供できるサーバ

サプリカントと AT の間のリンクの初回の確立時には、次の一連のイベントが発生します。

認証（802.1X）

認証サーバがサプリカントの認証を実行します。または、これらのデバイスが無条件に相互認証するように設定している場合は認証がそのまま完了します。

許可

リンクの両側が、そのリンクに適用する SGT および ACL などのポリシーを取得します。サプリカントは、認証サーバへの他のレイヤ 3 ルートがない場合には、AT をリレーとして使用する必要があります。

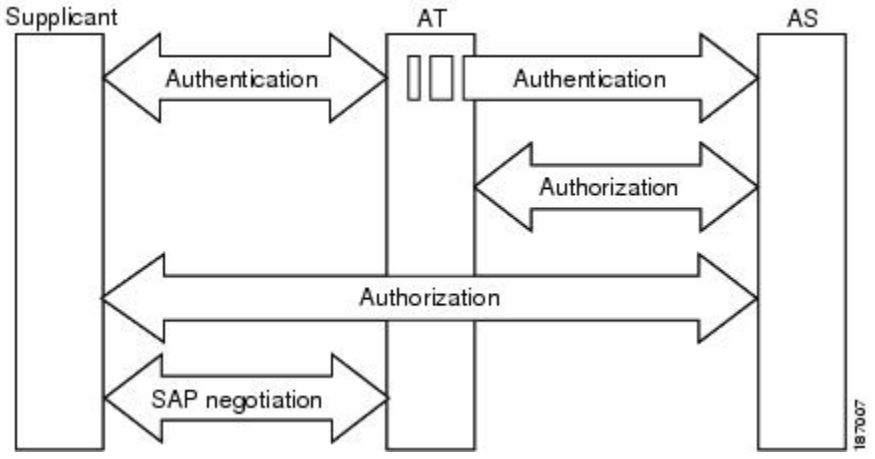
セキュリティ アソシエーション プロトコル（SAP）ネゴシエーション

サプリカントと AT の間で、EAPOL-Key が交換され、暗号スイートのネゴシエーション、セキュリティ パラメータ インデックス（SPI）の交換、およびキーの管理が実行されます。これら 3 つの作業が正常に完了すると、セキュリティ アソシエーション（SA）が確立します。

SAP ネゴシエーションが完了するまで、ポートは無許可ステート（ブロッキング ステート）です。

次の図に、SAP ネゴシエーションを示します。この図では、SAP ネゴシエーションが完了するまで、ポートが無許可ステートであることも示しています。

図 *20*：*SAP* ネゴシエーション



SAP ネゴシエーションには、次のいずれかの動作モードを使用します。

- Galois/Counter Mode（GCM）暗号化
- GCM 認証（GMAC）

- カプセル化なし（クリア テキスト）
- 暗号化も認証もなしのカプセル化

Cisco TrustSec は、IEEE 802.1AE 規格に基づいて、ESP-128 GCM および GMAC を使用します。

認証

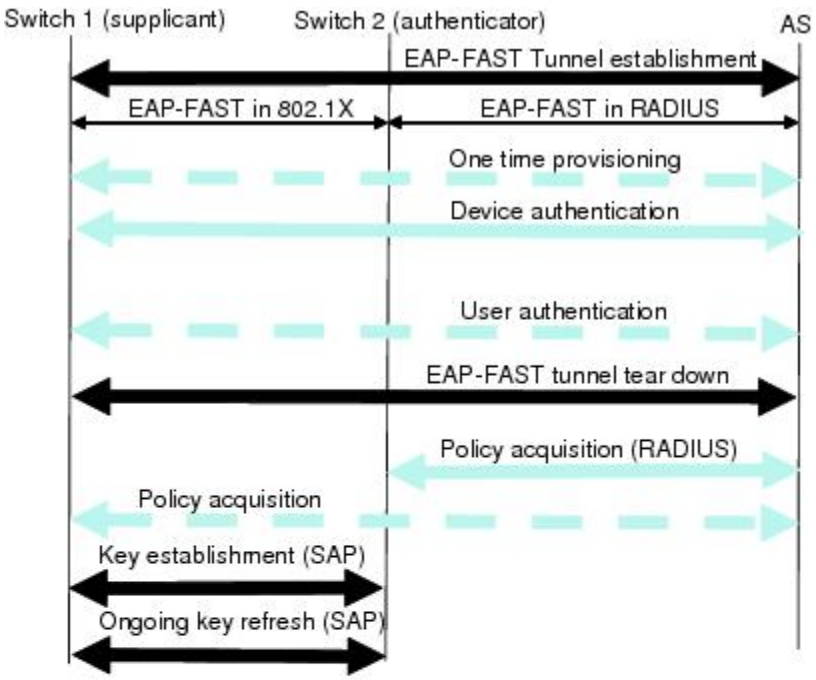
Cisco TrustSec は、デバイスのネットワーク加入を許可する前にデバイスを認証します。Cisco TrustSec は、拡張認証プロトコル（EAP）方式としての Extensible Authentication Protocol Flexible Authentication via Secure Tunnel（EAP-FAST）とともに、802.1X 認証を使用して、認証を実行します。

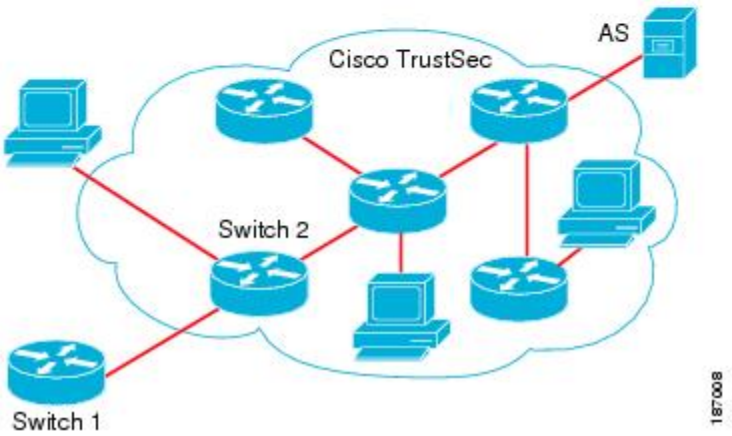
Cisco TrustSec と認証

Cisco TrustSec は認証に EAP-FAST を使用します。EAP-FAST カンバセーションによって、チェーンを使用した EAP-FAST トンネル内で他の EAP 方式の交換が可能になります。これにより、管理者は Microsoft Challenge Handshake Authentication Protocol Version 2（MSCHAPv2）のような従来型のユーザ認証方式を使用しながら、EAP-FAST トンネルが提供するセキュリティも利用できます。

次の図に、EAP-FAST トンネルおよび Cisco TrustSec で使用する内部方式を示します。

図 *21*：*Cisco TrustSec* の認証





EAP-FAST への Cisco TrustSec の機能拡張

Cisco TrustSec に EAP-FAST を実装することにより、次の機能拡張が実現しました。

オーセンティケータの認証

AT と認証サーバの間の共有秘密を得るために Protected Access Credential（PAC）を使用するように AT に求めることにより、AT のアイデンティティをセキュアに判断します。また、この機能により、AT が使用できるすべての IP アドレスに関して認証サーバに RADIUS 共有秘密を設定する手間が省けます。

ネイバーの ID を各ピアに通知

認証交換の完了までに、認証サーバはサプリカントと AT の両方を識別します。認証サーバは、保護された EAP-FAST 終端で追加の type-length-value（TLV）パラメータを使用して、AT のアイデンティティと、その AT が Cisco TrustSec に対応しているかどうかをサプリカントに伝えます。認証サーバはさらに、Access- Accept メッセージの RADIUS 属性を使用して、サプリカントのアイデンティティおよびそのサプリカントが Cisco TrustSec に対応しているかどうかを AT に伝えます。各ピアは、ネイバーのアイデンティティを認識しているため、認証サーバに追加の RADIUS Access-Requests を送信し、リンクに適用されるポリシーを取得できます。

AT ポスチャ評価

AT は、サプリカントの代わりに認証サーバと認証交換を開始すると、そのポスチャ情報を認証サーバに提供します。

802.1X ロールの選択

802.1X では、AT に認証サーバとの IP 接続が必要です。AT は RADIUS over UDP/IP を使用してサプリカントと AT の認証交換をリレーする必要があるためです。PC などのエンドポイント装置はネットワークへの接続時にサプリカントとして動作することになります。ただし、2 つのネットワーク デバイス間の Cisco TrustSec 接続の場合、各ネットワーク デバイスの 802.1X ロールが他方のネットワーク デバイスに即座に認識されない場合もあります。

NX-OS デバイスに AT とサプリカントのロールを手動で設定する代わりに、Cisco TrustSec はロール選択アルゴリズムを実行し、AT として動作する Cisco NX-OS デバイスとサプリカントとして動作するデバイスを自動的に判断します。ロール選択アルゴリズムは、RADIUS サーバに IP で到達可能なデバイスに AT ロールを割り当てます。どちらのデバイスも AT とサプリカントの両方のステート マシンを起動します。ある Cisco NX-OS デバイスが、ピアに RADIUS サーバへのアクセス権があることを検出すると、そのデバイスは自身の AT ステート マシンを終了し、サプリカントのロールを引き受けます。両方の Cisco NX デバイスに RADIUS サーバへのアクセス権がある場合、アルゴリズムは EAP over LAN（EAPOL）パケット送信の送信元として使用される MAC アドレスを比較します。MAC アドレスの値が大きい方の Cisco NX-OS デバイスが AT になり、もう一方の Cisco NX-OS デバイスがサプリカントになります。

Cisco TrustSec 認証の概要

Cisco TrustSec 認証プロセスが完了するまでに、認証サーバは次の処理を行います。

- サプリカントと AT のアイデンティティの検証
- サプリカントがエンドポイント装置の場合はユーザの認証

Cisco TrustSec 認証プロセスの完了時には、AT およびサプリカントの両方が次の情報を取得しています。

- ピアのデバイス ID
- ピアの Cisco TrustSec 機能についての情報

- SAP に使用されるキー

デバイス ID

Cisco TrustSec はデバイスの ID として IP アドレスも MAC アドレスも使用しません。その代わり、各 Cisco TrustSec 対応 Cisco NX-OS デバイスに、Cisco TrustSec ネットワークで一意に識別できる名前（デバイス ID）を手動で割り当てる必要があります。このデバイス ID は次の操作に使用されます。

- 認証ポリシーの検索
- 認証時におけるデータベース内のパスワードの検索

デバイスのクレデンシャル

Cisco TrustSec はパスワードベースのクレデンシャルをサポートしています。認証サーバは、代わりに自己署名式の証明書を使用する場合もあります。Cisco TrustSec はパスワードでサプリカントを認証し、MSCHAPv2 を使用することにより、たとえ認証サーバの証明書を検証できなくても、相互認証が可能です。

認証サーバはこれらのクレデンシャルを EAP-FAST フェーズ 0（プロビジョニング）の交換（サプリカントで PAC がプロビジョニングされる）中にサプリカントの相互認証に使用します。Cisco TrustSec は PAC の期限が切れるまで、EAP-FAST フェーズ 0 の交換は再実行しません。その後のリンク起動時には、EAP-FAST フェーズ 1 とフェーズ 2 の交換だけを実行します。EAP-FAST フェーズ 1 交換では、認証サーバとサプリカントの相互認証に PAC を使用します。Cisco TrustSec がデバイスのクレデンシャルを使用するのは、PAC プロビジョニング（または再プロビジョニング）段階だけです。

認証サーバは、Cisco TrustSec ネットワークにサプリカントが最初に加入する際に、一時的に設定されたパスワードをそのサプリカントの認証に使用します。サプリカントが最初に Cisco TrustSec ネットワークに加入する際に、認証サーバは証明書を作成してサプリカントを認証し、強力なパスワードを生成して、これを PAC でサプリカントに送信します。認証サーバはさらに、データベースに新しいパスワードを保存します。認証サーバとサプリカントは、その後の EAP-FAST フェーズ 0 交換の相互認証にこのパスワードを使用します。

ユーザ クレデンシャル

Cisco TrustSec には、エンドポイント装置の特定タイプのユーザ クレデンシャルは必要ありません。ユーザに対して任意のタイプの認証方式（MSCHAPv2、LEAP、Generic Token Card（GTC）、または OTP など）を選択し、対応するクレデンシャルを使用できます。Cisco TrustSec は、EAP-FAST フェーズ 2 交換の一部として EAP-FAST トンネル内でユーザ認証を実行します。

トランク ポートおよび FabricPath ポートでのネイティブ VLAN タギング

MACSec は、トランク ポートおよび FabricPath ポートでのネイティブ VLAN タギング機能により、FabricPath でサポートされます。ネイティブ VLAN タギングは、グローバルに、または制御パケットとデータ パケットのインターフェイスで設定できます。ネイティブ VLAN タギングをグローバルにイネーブルにするには、次のコマンドを使用します。

- **vlan dot1q tag native exclude control**
- **vlan dot1q tag native fabricpath**
- **vlan dot1q tag native fabricpath exclude control**

ネイティブ VLAN タギングを FabricPath ポートでイネーブルにするには、次のコマンドを使用します。

- **switchport trunk native vlan tag exclude control**
- **switchport fabricpath native vlan tag**
- **switchport fabricpath native vlan tag exclude control**

ネイティブ VLAN タギングにより、パケットの送受信時のタグ付きおよびタグなしモードへのサポートが提供されます。次の表では、上記のコマンドのグローバル設定またはポート設定でのパケットのモードを示します。

タギングの設定	TX 制御	TX データ（ネイティブ VLAN）	RX 制御	RX データ
グローバル トランク ポート タギング	タグなし	タグ付き	タグなしおよびタグ付き	タグ付き
グローバル FabricPath タギング	タグなし	タグなし	タグなしおよびタグ付き	タグなしおよびタグ付き
データ パケットへのグローバル FabricPath タギング	タグなし	タグ付き	タグなしおよびタグ付き	タグ付き
ポート レベルのトランク ポート タギング	タグなし	タグ付き	タグなしおよびタグ付き	タグ付き

タギングの設定	TX 制御	TX データ（ネイティブ VLAN）	RX 制御	RX データ
ポート レベルの Fabricpath タギング	タグなし	タグなし	タグなしおよびタグ付き	タグなしおよびタグ付き
データ パケットへのポート レベルの FabricPath タギング	タグなし	タグ付き	タグなしおよびタグ付き	タグ付き

MACSec

MACsec は、IEEE 802.1AE 規格ベースのレイヤ 2 ホップバイホップ暗号化であり、これにより、メディア アクセス非依存プロトコルに対してデータの機密性と完全性を確保できます。

MACsec は、暗号化キーにアウトオブバンド方式を使用して、有線ネットワーク上で MAC レイヤの暗号化を提供します。MACsec Key Agreement（MKA）プロトコルでは、必要なセッション キーを提供し、必要な暗号化キーを管理します。ホスト側のリンク（ネットワーク アクセス デバイスと、PC や IP フォンなどのエンドポイント デバイス間のリンク）だけが MACsec を使用して保護できます。

MACsec Key Agreement（MKA）による 802.1AE 暗号化は、ルータまたはスイッチとホスト デバイス間の暗号化用に、ダウンリンク ポートでサポートされます。

MACsec は、イーサネット パケットの送信元および宛先 MAC アドレスを除くすべてのデータを暗号化します。

WAN またはメトロ イーサネット上に MACsec サービスを提供するために、サービス プロバイダーは、Ethernet over Multiprotocol Label Switching（EoMPLS）および L2TPv3 などのさまざまなトランスポート レイヤ プロトコルを使用して、E-Line や E-LAN などのレイヤ 2 透過サービスを提供しています。

EAP-over-LAN（EAPOL）プロトコル データ ユニット（PDU）のパケット本体は、MACsec Key Agreement PDU（MKPDU）と呼ばれます。3 ハートビート（1 ハートビートは 2 秒）後に MKPDU が受信されない場合、ライブ ピアのリストからピアが削除されます。たとえば、クライアントが切断さると、最後の MKPDU が クライアントにより受信されてから 3 ハートビートが経過するまで、スイッチ上の参加者は MKA を操作し続けます。

CTS MACSEC GCM 256 ビットと拡張パケット シーケンス番号のサポート

Cisco Nexus Release 7.3(0)DX(1) 以前のリリースで使用可能な SAP GCM 暗号スイートは、データの暗号化および復号化に使用する 128 ビット AES キー生成をサポートします。Cisco Nexus Release

7.3(0)DX(1) でサポートが導入された M3 ライン カードで、64 ビット シーケンス番号の 256 ビット AES キーを含むデータを暗号化または復号化できます。

Cisco Nexus Release 7.3(0)DX(1) で導入され、SAP GCM 暗号化スイートの拡張である CTS MACsec GCM 256 ビット機能では、ハードウェアの 256 ビット AES キー機能が利用されています。

（注） CTS MACsec GCM 256 ビット機能は、M3 ライン カードでのみサポートされます。GCM 256 ビット暗号化モードは、Cisco Nexus Release 7.3(0)DX(1) 以降のリリースでサポートされます。

M3 ライン カードでは、拡張パケット シーケンス番号（XPN）である、64 ビット シーケンス番号がサポートされます。GCM-256 暗号化モードがイネーブルの場合、CTS-Manager により、ドライバがハードウェア内で XPN ビットをプログラミングするようになります。XPN 規格に従い、暗号化の入力ベクトルには次の 2 つのフィールドが必要です。

- 32 ビット Short Secure Channel Identifier（SSCI）
- 96 ビット salt

これらのフィールドは SAP プロトコルの定数値であり、CTS Manager によりドライバに送信されて、ドライバがハードウェア内でプログラミングするのを可能にします。

（注） Cisco Nexus Release 7.3(0)DX(1) より以前のリリースでは、ISSU を実行して永続ストレージ サービス（PSS）から SAP セッション構造を復元する際、CTS Manager により、既存の 128 ビット AES キー対応インターフェイスは影響されないよう保証されます。

（注） 新しく導入された GCM 暗号化モードは、Cisco Nexus Release 7.3(0)DX(1) 以前のリリースではサポートされません。したがって、**gcm-encrypt-256** キーワードが Cisco Nexus Release 7.3(0)DX(1) に保存されている場合に、ユーザが Cisco Nexus Release 7.3(0)DX(1) から以前のリリースに copy running-config startup-config コマンドを使用して保存済みの設定とともに移行する場合、以前のリリースに移行する前に、保存されていない設定を削除するよう求められる必要があります。

Cisco TrustSec MACSec のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	Cisco NX-OS Release 6.1 以降では、Cisco TrustSec にはライセンスは不要です。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。 Cisco NX-OS Release 6.1 よりも前の場合は、Cisco TrustSec には Advanced Services ライセンスが必要です。Cisco TrustSec ライセンスには猶予期間はありません。Cisco TrustSec を使用するためには、事前に Advanced Services ライセンスを取得しインストールする必要があります。 （注） Cisco NX-OS ライセンス方式の詳細と、ライセンスの取得および適用の方法については、『*Cisco NX-OS Licensing Guide*』を参照してください。

Cisco TrustSec パラメータのデフォルト設定

次の表に、Cisco TrustSec パラメータのデフォルト設定を示します。

表 *29*：*Cisco TrustSec* パラメータのデフォルト設定

パラメータ	デフォルト
Cisco TrustSec	ディセーブル
すべてのインターフェイスのポーズフレームの暗号化および復号化	ポーズフレームの暗号化および復号化をサポートするラインカードでイネーブル
SXP	ディセーブル
SXP デフォルト パスワード	なし
SXP 復帰期間	120 秒（2 分）
SXP リトライ期間	60 秒（1 分）
キャッシング	ディセーブル
RBACL ロギング	ディセーブル

パラメータ	デフォルト
RBACL 統計情報	ディセーブル

Cisco TrustSec MACSec の設定

ここでは、Cisco TrustSec MACSec の設定作業について説明します。

Cisco TrustSec MACSec 機能のイネーブル化

Cisco TrustSec MACSec 機能を設定する前に、Cisco NX-OS デバイス上の 802.1X 機能および Cisco TrustSec 機能をイネーブルにする必要があります。

（注） Cisco TrustSec MACSec 機能をイネーブルにすると、その後に 802.1X 機能をディセーブルにすることはできません。

手順の概要

1. **configure terminal**
2. **feature dot1x**
3. **feature cts**
4. **exit**
5. （任意） **show cts**
6. （任意） **show feature**
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**feature dot1x** 例： `switch(config)# feature dot1x`	802.1X 機能をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 3	**feature cts** 例： `switch(config)# feature cts`	Cisco TrustSec 機能をイネーブルにします。

ステップ 4	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 5	**show cts** 例： `switch# show cts`	（任意） Cisco TrustSec の設定を表示します。
ステップ 6	**show feature** 例： `switch# show feature`	（任意） 機能がイネーブルになったステータスを表示します。
ステップ 7	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Cisco TrustSec デバイスのクレデンシャルの設定

ネットワーク内の Cisco TrustSec 対応 Cisco NX-OS デバイス各々に、固有の Cisco TrustSec クレデンシャルを設定する必要があります。Cisco TrustSec はクレデンシャルのパスワードをデバイスの認証に使用します。

（注） Cisco Secure ACS にも Cisco NX-OS デバイスの Cisco TrustSec クレデンシャルを設定する必要があります（次の URL のマニュアルを参照してください。

http://www.cisco.com/en/US/products/sw/secursw/ps5338/products_installation_and_configuration_guides_list.html）。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **cts device-id***name***password***password*
3. **exit**
4. （任意） **show cts**
5. （任意） **show cts environment**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**cts device-id***name***password***password* 例： `switch(config)# cts device-id MyDevice1 password CiscO321`	固有のデバイス ID およびパスワードを設定します。*name* 引数は、最大 32 文字で大文字と小文字を区別します。 （注） デバイスの ID とパスワードの設定を削除するには、このコマンドの **no** 形式を使用します。

ステップ 3	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 4	**show cts** 例： `switch# show cts`	（任意） Cisco TrustSec の設定を表示します。
ステップ 5	**show cts environment** 例： `switch# show cts environment`	（任意） Cisco TrustSec 環境データを表示します。
ステップ 6	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ネイティブ VLAN タギングの設定

ネイティブ VLAN タギングのグローバル設定

ネイティブ VLAN タギングをグローバルに設定するには、ここに示す手順を実行します。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **vlan dot1q tag native** {**fabricpath**} **exclude control**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan dot1q tag native** {**fabricpath**} **exclude control** 例： `switch(config)# vlan do1q tag native exclude control`	必要に応じて制御パケットとデータ パケットにタグを追加します。 • データ パケットのみにタグを追加するには **exclude control** キーワードを使用します。 • FabricPath ポートで制御パケットとデータ パケットにタグを追加するには **fabricpath** キーワードを使用します。

インターフェイスでのネイティブ VLAN タギングの設定

ネイティブ VLAN タギングをグローバルに設定するには、ここに示す手順を実行します。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **interface***typeslot/port*
3. **vlan dot1q tag native** {**fabricpath**} **exclude control**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface***typeslot/port* 例： `switch(config)# interface ethernet 1/4`	チャネル グループに追加するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**vlan dot1q tag native** {**fabricpath**} **exclude control** 例： `switch(config-if)# vlan do1q tag native exclude control`	必要に応じて制御パケットとデータ パケットにタグを追加します。 • データ パケットのみにタグを追加するには **exclude control** キーワードを使用します。 • FabricPath ポートで制御パケットとデータ パケットにタグを追加するには **fabricpath** キーワードを使用します。

Cisco TrustSec の認証、許可、SAP、およびデータ パス セキュリティの設定

ここでは、Cisco TrustSec の認証、許可、SAP、およびデータ パス セキュリティの設定作業について説明します。

Cisco TrustSec の認証および許可の設定プロセス

Cisco TrustSec の認証および許可を設定するには、次の手順を行います。

手順の概要

1. Cisco TrustSec 機能をイネーブルにします。
2. Cisco TrustSec 認証をイネーブルにします。
3. インターフェイスに対して Cisco TrustSec の 802.1X 認証をイネーブルにします。

手順の詳細

ステップ 1 Cisco TrustSec 機能をイネーブルにします。

ステップ 2 Cisco TrustSec 認証をイネーブルにします。

ステップ 3 インターフェイスに対して Cisco TrustSec の 802.1X 認証をイネーブルにします。

Cisco TrustSec 認証のイネーブル化

インターフェイスに対して Cisco TrustSec 認証をイネーブルにする必要があります。デフォルトでは、データパス リプレイ保護機能がイネーブルになり、SAP 動作モードは GCM-encrypt です。

注意 Cisco TrustSec 認証の設定を有効にするには、インターフェイスのイネーブル化とディセーブル化を行う必要があり、インターフェイス上のトラフィックが中断されます。

（注） Cisco TrustSec の 802.1X モードをイネーブルにすると、そのインターフェイス上の許可と SAP がイネーブルになります。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port* [**-***port2*]
3. **cts dot1x**
4. （任意） **no replay-protection**
5. （任意） **sap modelist** {**gcm-encrypt** | **gmac** | **no-encap** | **null**}
6. **exit**
7. **shutdown**
8. **no shutdown**
9. **exit**
10. （任意） **show cts interface** {**all** | **brief** | **ethernet***slot*/*port*}
11. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet***slot*/*port* [-*port2*]
	
	例：
	`switch(config)# interface ethernet 2/2`
	`switch(config-if)#`
		単一ポートまたはポート範囲を指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**cts dot1x**
	
	例：
	`switch(config-if)# cts dot1x`
	`switch(config-if-cts-dot1x)#`
		Cisco TrustSec の 802.1X 認証をイネーブルにして、Cisco TrustSec 802.1X コンフィギュレーション モードを開始します。

ステップ 4	**no replay-protection** 例： `switch(config-if-cts-dot1x)# no replay-protection`	（任意） リプレイ保護をディセーブルにします。デフォルトではイネーブルになっています。
ステップ 5	**sap modelist** {**gcm-encrypt** | **gmac** | **no-encap** | **null**} 例： `switch(config-if-cts-dot1x)# sap modelist gcm-encrypt`	（任意） インターフェイスに SAP 動作モードを設定します。 GCM 暗号化の場合は **gcm-encrypt** キーワードを使用します。このオプションがデフォルトです。 GCM 認証のみの場合は **gmac** キーワードを使用します。 SAP をカプセル化せず、SGT の挿入も行わない場合は、**no-encap** キーワードを使用します。 認証および暗号化を行わずにカプセル化のみを行うには、**null** キーワードを使用します。

ステップ 6	**exit**
	
	例：
	`switch(config-if-cts-dot1x)# exit`
	`switch(config-if)#`
		Cisco TrustSec 802.1X コンフィギュレーション モードを終了します。

ステップ 7	**shutdown** 例： `switch(config-if)# shutdown`	インターフェイスをディセーブルにします。

	コマンドまたはアクション	目的
ステップ 8	**no shutdown** 例： `switch(config-if)# no shutdown`	インターフェイスをイネーブルにして、インターフェイスの Cisco TrustSec 認証をイネーブルにします。

ステップ 9	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 10	**show cts interface** {**all** | **brief** | **ethernet***slot*/*port*} 例： `switch(config)# show cts interface all`	（任意） インターフェイスに対する Cisco TrustSec の設定を表示します。
ステップ 11	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

インターフェイスおよびポート プロファイルに対する Cisco TrustSec データパス リプレイ保護の設定

デフォルトでは、Cisco NX-OS ソフトウェアによってデータパス リプレイ保護機能をイネーブルにします。接続デバイスが SAP をサポートしていない場合は、レイヤ 2 Cisco TrustSec のインターフェイスでデータパス リプレイ保護をディセーブルにできます。

ポートプロファイルに対してこの作業を行うと、グループに参加するすべてのポートプロファイルに設定が継承されます。

注意 データパス リプレイ保護の設定を有効にするには、インターフェイスのイネーブル化とディセーブル化を行う必要があり、インターフェイス上のトラフィックが中断されます。

はじめる前に

インターフェイスの Cisco TrustSec 認証がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port* [-*port2*]
3. **cts dot1x**
4. **no replay-protection**
5. **exit**
6. **shutdown**
7. **no shutdown**
8. **exit**
9. （任意） **show cts interface** {**all** | **brief** | **ethernet***slot*/*port*}
10. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet***slot*/*port* [-*port2*]
	
	例：
	`switch(config)# interface ethernet 2/2`
	`switch(config-if)#`
		単一ポートまたはポート範囲を指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**cts dot1x**
	
	例：
	`switch(config-if)# cts dot1x`
	`switch(config-if-cts-dot1x)#`
		Cisco TrustSec の 802.1X 認証をイネーブルにして、Cisco TrustSec 802.1X コンフィギュレーション モードを開始します。

ステップ 4	**no replay-protection** 例： `switch(config-if-cts-dot1x)# no replay-protection`	データパス リプレイ保護をディセーブルにします。デフォルトではイネーブルになっています。 インターフェイスでデータパス リプレイ保護をイネーブルにするには、**replay-protection** コマンドを使用します。

ステップ 5	**exit**
	
	例：
	`switch(config-if-cts-dot1x)# exit`
	`switch(config-if)#`
		Cisco TrustSec 802.1X コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 6	**shutdown** 例： `switch(config-if)# shutdown`	インターフェイスをディセーブルにします。
ステップ 7	**no shutdown** 例： `switch(config-if)# no shutdown`	インターフェイスをイネーブルにして、インターフェイスのデータパス リプレイ保護機能をディセーブルにします。

ステップ 8	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 9	**show cts interface** {**all** | **brief** | **ethernet***slot*/*port*} 例： `switch(config)# show cts interface all`	（任意） インターフェイスに対する Cisco TrustSec の設定を表示します。
ステップ 10	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスおよびポート プロファイルに対する Cisco TrustSec SAP 動作モードの設定

レイヤ 2 Cisco TrustSec のインターフェイスに SAP 動作モードを設定できます。デフォルトの SAP 動作モードは GCM-encrypt です。

ポートプロファイルに対してこの作業を行うと、グループに参加するすべてのポートプロファイルに設定が継承されます。

⚠

注意 SAP動作モードの設定を有効にするには、インターフェイスのイネーブル化とディセーブル化を行う必要があり、インターフェイス上のトラフィックが中断されます。

はじめる前に

インターフェイスの Cisco TrustSec 認証がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port* [**-***port2*]
3. **cts dot1x**
4. **sap modelist** [**gcm-encrypt** | **gmac** | **no-encap** | **null**]
5. **exit**
6. **shutdown**
7. **no shutdown**
8. **exit**
9. （任意） **show cts interface** {**all** | **brief** | **ethernet***slot*/*port*}
10. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet***slot*/*port* [**-***port2*]
	
	例：
	`switch(config)# interface ethernet 2/2`
	`switch(config-if)#`
		単一のインターフェイスまたはインターフェイス範囲を指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**cts dot1x**
	
	例：
	`switch(config-if)# cts dot1x`
	`switch(config-if-cts-dot1x)#`
		Cisco TrustSec の 802.1X 認証をイネーブルにして、Cisco TrustSec 802.1X コンフィギュレーション モードを開始します。

ステップ 4	**sap modelist** [**gcm-encrypt**	**gmac**	**no-encap**	**null**] 例： `switch(config-if-cts-dot1x)# sap modelist gmac`	インターフェイスに SAP 認証モードを設定します。 GCM 暗号化の場合は **gcm-encrypt** キーワードを使用します。このオプションがデフォルトです。 GCM 認証のみの場合は **gmac** キーワードを使用します。 インターフェースで SAP をカプセル化せず、SGT の挿入も行わない場合は、**no-encap** キーワードを使用します。 認証およびインターフェースでの SAP 暗号化を行わずにカプセル化のみを行うには、**null** キーワードを使用します。カプセル化されるのは SGT だけです。

	コマンドまたはアクション	目的

ステップ 5	**exit**
	
	例：
	`switch(config-if-cts-dot1x)# exit`
	`switch(config-if)#`
		Cisco TrustSec 802.1X コンフィギュレーション モードを終了します。

ステップ 6	**shutdown** 例： `switch(config-if)# shutdown`	インターフェイスをディセーブルにします。
ステップ 7	**no shutdown** 例： `switch(config-if)# no shutdown`	インターフェイスをイネーブルにして、そのインターフェイスの SAP 動作モードをイネーブルにします。

ステップ 8	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 9	**show cts interface** {**all** | **brief** | **ethernet***slot*/*port*} 例： `switch(config)# show cts interface all`	（任意） インターフェイスに対する Cisco TrustSec の設定を表示します。
ステップ 10	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスの SAP キーの再生成

SAP交換をトリガーして、新しいキーセットを生成し、インターフェイス上のデータ トラフィックを保護できます。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

手順の概要

1. **cts rekey ethernet***slot*/*port*
2. （任意） **show cts interface** {**all** | **brief** | **ethernet** *slot*/*port*}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**cts rekey ethernet***slot*/*port* 例： `switch# cts rekey ethernet 2/3`	インターフェイスの SAP キーを生成します。
ステップ 2	**show cts interface** {**all** | **brief** | **ethernet** *slot*/*port*} 例： `switch# show cts interface all`	（任意） インターフェイスに対する Cisco TrustSec の設定を表示します。

手動での Cisco TrustSec 認証の設定

Cisco NX-OS デバイスに Cisco Secure ACS へのアクセス権がない場合や、MAC アドレス認証バイパス機能がイネーブルになっていて認証が必要でない場合には、インターフェイスに手動で Cisco TrustSec を設定することも可能です。接続の両側のインターフェイスに手動で設定する必要があります。

（注） 半二重モードのインターフェイスでは、Cisco TrustSec をイネーブルにできません。インターフェイスが半二重モードに設定されているかどうかを調べるには、**show interface** コマンドを使用します。

注意 手動モードでの Cisco TrustSec の設定を有効にするには、インターフェイスのイネーブル化とディセーブル化を行う必要があり、インターフェイス上のトラフィックが中断されます。

はじめる前に

Cisco TrustSec がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **interface***interfaceslot*/*port*
3. **cts manual**
4. **sap pmk** {*key*[**left-zero-padded**] [**display encrypt**] | **encrypted***encrypted_pmk* | **use-dot1x**} [**modelist** {**gcm-encrypt** |**gcm-encrypt-256** | **gmac** | **no-encap** | **null**}]
5. （任意） **policy dynamic identity***peer-name*
6. （任意） **policy static sgt***tag* [**trusted**]
7. **exit**
8. **shutdown**
9. **no shutdown**
10. **exit**
11. （任意） **show cts interface** {**all** | **brief** | **ethernet***slot*/*port*}
12. （任意） **show cts sap pmk** {**all** | **interface ethernet***slot*/*port*}
13. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface***interfaceslot*/*port*
	
	例：
	`switch(config)# interface ethernet 2/2`
	`switch(config-if)#`
		インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**cts manual**
	
	例：
	`switch(config-if)# cts manual`
	`switch(config-if-cts-manual)#`
		Cisco TrustSec 手動コンフィギュレーション モードを開始します。
		（注） 半二重モードのインターフェイスでは、Cisco TrustSec をイネーブルにできません。

ステップ 4	**sap pmk** {*key*[**left-zero-padded**] [**display encrypt**]	**encrypted***encrypted_pmk*	**use-dot1x**} [**modelist** {**gcm-encrypt** |**gcm-encrypt-256**	**gmac**	**no-encap**	**null**}]	SAP の Pairwise Master Key（PMK）と動作モードを設定します。Cisco TrustSec の手動モードでは、SAP はデフォルトでディセーブルになっています。 *key* 引数は、最大 32 文字の偶数文字数の 16 進値です。 PMK の長さが 32 バイト未満の場合に、入力された文字列の左側をゼロで埋めるには、**left-zero-padded** キーワードを使用します。

	コマンドまたはアクション	目的
	例： `switch(config-if-cts-manual)# sap pmk fedbaa modelist gmac`	設定された PMK が実行コンフィギュレーションの AES 暗号化形式で表示されるように指定するには、**display encrypt** キーワードを使用します。 暗号化された 64 バイトの PMK 文字列（16 進数で 128 文字）を指定するには、**encrypted***encrypted_pmk* キーワードを使用します。 ピア デバイスが Cisco TrustSec 802.1X 認証または許可をサポートせず、SAP データ パス暗号化と認証をサポートしている場合は、**use-dot1x** キーワードを使用します。 モードのリストには、次に示すデータ パス暗号化と認証の暗号モードを指定します。 GCM 暗号化の場合は **gcm-encrypt** キーワードを使用します。このオプションがデフォルトです。 GCM 暗号化の場合は **gcm-encrypt-256** キーワードを使用します。 GCM 認証の場合は **gmac** キーワードを使用します。 カプセル化と SGT 挿入を行わない場合は、**no-encap** キーワードを使用します。 認証または暗号化なしで SGT のカプセル化を行うには、**null** キーワードを使用します。
ステップ 5	**policy dynamic identity***peer-name* 例： `switch(config-if-cts-manual)# policy dynamic identity MyDevice2`	（任意） ダイナミック許可ポリシーのダウンロードを設定します。*peer-name* 引数は、ピア デバイスの Cisco TrustSec デバイス ID です。ピア名では、大文字と小文字が区別されます。 （注） Cisco TrustSec クレデンシャルが設定されていることおよび Cisco TrustSec の AAA が設定されていることを確認します。 （注） **policy dynamic** コマンドと **policy static** コマンドは同時に使用できません。一度に 1 つしか適用できません。交互に変更するには、他のコマンドを設定する前に、このコマンドの **no** 形式を使用して設定を削除する必要があります。
ステップ 6	**policy static sgt***tag* [**trusted**] 例： `switch(config-if-cts-manual)# policy static sgt 0x2`	（任意） スタティック許可ポリシーを設定します。*tag* 引数は、10 進値または **0x***hhhh* 形式の 16 進値です。10 進数の範囲は 2 ～ 65519 で、16 進数の範囲は 0x2 ～ 0xffef です。**trusted** キーワードを指定すると、SGT 付きでインターフェイスにトラフィックが着信した場合、そのタグは上書きされません。

	コマンドまたはアクション	目的
		（注） **policy dynamic** コマンドと **policy static** コマンドは同時に使用できません。一度に 1 つしか適用できません。交互に変更するには、他のコマンドを設定する前に、このコマンドの **no** 形式を使用して設定を削除する必要があります。

ステップ 7	**exit**
	
	例：
	`switch(config-if-cts-manual)# exit`
	`switch(config-if)#`
		Cisco TrustSec 手動コンフィギュレーション モードを終了します。

ステップ 8	**shutdown** 例： `switch(config-if)# shutdown`	インターフェイスをディセーブルにします。
ステップ 9	**no shutdown** 例： `switch(config-if)# no shutdown`	インターフェイスをイネーブルにして、インターフェイスの Cisco TrustSec 認証をイネーブルにします。

ステップ 10	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 11	**show cts interface** {**all** | **brief** | **ethernet***slot*/*port*} 例： `switch# show cts interface all`	（任意） インターフェイスの Cisco TrustSec 設定を表示します。
ステップ 12	**show cts sap pmk** {**all** | **interface ethernet***slot*/*port*} 例： `switch# show cts sap pmk all`	（任意） すべてのインターフェイスまたは特定のイーサネットインターフェイスに対し設定された PMK の 16 進値を表示します。
ステップ 13	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Dot1x モードでの Cisco TrustSec 認証の設定

はじめる前に

手順の概要

1. **configure terminal**
2. **interface***interfaceslot*/*port*
3. **cts manual**
4. **sap pmk** {*key*[**left-zero-padded**] [**display encrypt**] | **encrypted***encrypted_pmk* | **use-dot1x**} [**modelist** {**gcm-encrypt** | **gmac** | **no-encap** | **null**}]
5. **exit**
6. **shutdown**
7. **no shutdown**
8. **exit**
9. （任意） **show cts interface** {**all** | **brief** | **ethernet***slot*/*port*}
10. （任意） **show cts sap pmk** {**all** | **interface ethernet***slot*/*port*}
11. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface***interfaceslot*/*port*
	
	例：
	`switch(config)# interface ethernet 2/29-30`
	`switch(config-if-range)#`
		インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**cts manual**
	
	例：
	`switch(config-if-range)# cts dot1x`
	`switch(config-if-cts-dot1x)#`
		Cisco TrustSec Dot1x コンフィギュレーション モードを開始します。

ステップ 4	**sap pmk** {*key*[**left-zero-padded**] [**display encrypt**]	**encrypted***encrypted_pmk*	**use-dot1x**} [**modelist** {**gcm-encrypt**	**gmac**	**no-encap**	**null**}]	SAP の Pairwise Master Key（PMK）と動作モードを設定します。Cisco TrustSec の手動モードでは、SAP はデフォルトでディセーブルになっています。 *key* 引数は、最大 32 文字の偶数文字数の 16 進値です。

	コマンドまたはアクション	目的
	例： `switch(config-if-cts-dot1x)# sap modelist gcm-encrypt-256`	PMK の長さが 32 バイト未満の場合に、入力された文字列の左側をゼロで埋めるには、**left-zero-padded** キーワードを使用します。 設定された PMK が実行コンフィギュレーションの AES 暗号化形式で表示されるように指定するには、**display encrypt** キーワードを使用します。 暗号化された 64 バイトの PMK 文字列（16 進数で 128 文字）を指定するには、**encrypted***encrypted_pmk* キーワードを使用します。 ピア デバイスが Cisco TrustSec 802.1X 認証または許可をサポートせず、SAP データ パス暗号化と認証をサポートしている場合は、**use-dot1x** キーワードを使用します。 モードのリストには、次に示すデータ パス暗号化と認証の暗号モードを指定します。 GCM 暗号化の場合は **gcm-encrypt** キーワードを使用します。このオプションがデフォルトです。 256 ビットの GCM 暗号化の場合は **gcm-encrypt-256** キーワードを使用します。 GCM 認証の場合は **gmac** キーワードを使用します。 カプセル化と SGT 挿入を行わない場合は、**no-encap** キーワードを使用します。 認証または暗号化なしで SGT のカプセル化を行うには、**null** キーワードを使用します。

ステップ 5	**exit**
	例：
	`switch(config-if-cts-dot1x)# exit`
	`switch(config-if)#`
		Cisco TrustSec Dot1x コンフィギュレーション モードを終了します。

ステップ 6	**shutdown** 例： `switch(config-if)# shutdown`	インターフェイスをディセーブルにします。
ステップ 7	**no shutdown** 例： `switch(config-if)# no shutdown`	インターフェイスをイネーブルにして、インターフェイスの Cisco TrustSec 認証をイネーブルにします。

	コマンドまたはアクション	目的

ステップ 8	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 9	**show cts interface** {**all** | **brief** | **ethernet***slot*/*port*} 例： `switch# show cts interface all`	（任意） インターフェイスの Cisco TrustSec 設定を表示します。
ステップ 10	**show cts sap pmk** {**all** | **interface ethernet***slot*/*port*} 例： `switch# show cts sap pmk all`	（任意） すべてのインターフェイスまたは特定のイーサネット インターフェイスに対し設定された PMK の 16 進値を表示します。
ステップ 11	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ポート チャネル メンバでの Cisco TrustSec サポート

Cisco NX-OS Release 7.2(0)D1(1) 以前では、TrustSec 設定に関して、ポート チャネル メンバ インターフェイスで互換性が適用されませんでした。また、Cisco TrustSec 設定は、ポート チャネル インターフェイスで許可されませんでした。

Cisco NX-OS Release 7.2(0)D1(1) 以降では、ポート チャネル メンバで TrustSec 設定の互換性が適用され、ポート チャネル インターフェイスでの TrustSec 設定も許可されます。次のセクションでさらに詳しく説明します。

設定モデル

設定モデルを次に示します。

- ポート チャネル インターフェイスでの Cisco TrustSec 設定：

  ポート チャネル インターフェイスで設定された Cisco TrustSec 設定はすべて、その全メンバ インターフェイスに継承されます。

- ポート チャネル メンバ インターフェイスでの Cisco TrustSec 設定：

ポート チャネル互換性パラメータは、ポート チャネル メンバ インターフェイスで設定できません。

非互換性を生じない他の Cisco TrustSec 設定（MACSec 設定など）は、ポート チャネル メンバ インターフェイスで設定できます。

- ポート チャネルへの新しいメンバの追加：
  - **channel-group** コマンドの使用：

    ポートチャネルでの設定とすべてのメンバでの設定に互換性があれば、新しいメンバの追加は許可されます。そうでない場合、追加は拒否されます。

    （注） Cisco TrustSec がポート チャネルで設定されておらず、追加するメンバ上の Cisco TrustSec 設定が互換性がある場合、追加は許可され、ポート チャネルはメンバ インターフェイスから互換性パラメータを継承します。

  - **channel-group force** コマンドの使用：

    追加するインターフェイスがポートチャネル設定をサポートしている場合、ポートチャネルから互換性パラメータを継承し、追加は許可されます。ただし、追加されるインターフェイスの一部がポート チャネル設定をサポートしない場合、追加は拒否されます。

Cisco NX-OS Release 7.2(0)D1(1) のユーザ インターフェイスの更新

次に、Cisco NX-OS Release 7.2(0)D1(1) のユーザ インターフェイスの更新を示します。

- Cisco TrustSec の設定になんらかの非互換性がある場合に **channel group** または **channel-group force** コマンドを発行すると、互換性のない設定を指摘するエラー メッセージがユーザに表示されます。
- **show run** および **show start** コマンドは、ポート チャネル インターフェイス上、および物理イーサネット インターフェイス上の Cisco TrustSec 設定を表示します。
- **show cts role-based sgt-map** コマンドは、ポート チャネル インターフェイス上で学習されたポートと SGT の学習されたマッピングを、必要に応じて表示します。

インサービス ソフトウェア アップグレード

この機能をサポートしない下位バージョンからインサービス ソフトウェア アップグレード（ISSU）が実行されると、ISSU が完了するとすぐに、すべてのポート チャネルが、最初に設定されたメンバ インターフェイスから互換性パラメータを継承します。設定の非互換性が検出されたポート チャネルについて、警告レベルの syslog が生成されます。

Cisco TrustSec MACSec の設定の確認

Cisco TrustSec MACSec の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show cts	Cisco TrustSec の情報を表示します。
show cts capability interface {**all** | **ethernet***slot*/*port*}	すべてのインターフェイスまたは特定のイーサネット インターフェイスの Cisco TrustSec 機能を表示します。
show cts credentials	EAP-FAST の Cisco TrustSec クレデンシャルを表示します。
show cts environment-data	Cisco TrustSec の環境データを表示します。
show cts interface{**all** | **brief** | **ethernet***slot*/*port*}	インターフェイスの Cisco TrustSec 設定を表示します。
show cts pacs	デバイス キー ストア内の Cisco TrustSec 許可情報と PAC を表示します。
show running-config cts	実行コンフィギュレーションの Cisco TrustSec 情報を表示します。

Cisco TrustSec MACSec に関する追加情報

ここでは、Cisco TrustSec の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS のライセンス	『*Cisco NX-OS Licensing Guide*』
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』

Cisco TrustSec MACSec の機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 *30*：*Cisco TrustSec MACSec* の機能の履歴

機能名	リリース	機能情報
CTS MACSEC GCM 256 ビットと拡張パケット シーケンス番号のサポート	7.3(0)DX(1)	次の機能のサポートが追加されました。
F3 の FabricPath での Cisco TrustSec MACsec	7.2(1)D1(1)	F3 シリーズ モジュールの FabricPath での Cisco TrustSec MACsec のサポートが追加されました。
ポート チャネル メンバでの Cisco TrustSec サポート	7.2(0)D1(1)	ポート チャネル メンバに Cisco TrustSec のサポートが追加されました。
Cisco TrustSec	6.2(2)	SAP PMK を暗号化し、実行コンフィギュレーションに暗号化された形式で PMK を表示する機能が追加されました。
Cisco TrustSec	6.2(2)	設定された PMK の 16 進値を表示するための **show cts sap pmk** コマンドが追加されました。
Cisco TrustSec	6.2(2)	インターフェイスの Cisco TrustSec 機能を表示するための **show cts capability interface** コマンドが追加されました。
Cisco TrustSec	6.2(2)	すべての CTS 対応インターフェイスに関する概要を表示するための **brief** キーワードが **show cts interface** コマンドに追加されました。

機能名	リリース	機能情報
Cisco TrustSec	6.1(1)	40G および 100G M2 シリーズ モジュールの MACsec のサポートが追加されました。
Cisco TrustSec	4.2(1)	リリース 4.1 からの変更はありません。

第 15 章

IP ACL の設定

この章では、Cisco NX-OS デバイスの IP アクセス コントロール リスト（ACL）を設定する方法について説明します。

特に指定がなければ、IP ACL は IPv4 および IPv6 の ACL を意味します。

（注） 管理対象デバイス上で実行されている Cisco NX-OS リリースでは、説明するすべての機能または設定がサポートされない場合があります。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースのマニュアルとリリース ノートを参照してください。

この章は、次の項で構成されています。

- 機能情報の確認，550 ページ
- ACL の概要，550 ページ
- IP ACL のライセンス要件，568 ページ
- IP ACL の前提条件，568 ページ
- IP ACL の注意事項と制約事項，569 ページ
- IP ACL のデフォルト設定，574 ページ
- IP ACL の設定，575 ページ
- IP ACL の設定の確認，596 ページ
- IP ACL の統計情報のモニタリングとクリア，598 ページ
- IP ACL の設定例，599 ページ
- オブジェクト グループの設定，600 ページ
- オブジェクト グループの設定の確認，606 ページ
- 時間範囲の設定，607 ページ

- 時間範囲設定の確認，613 ページ
- フレキシブル ACL TCAM バンク チェーニングのトラブルシューティング，613 ページ
- IP ACL に関する追加情報，614 ページ
- IP ACL の機能の履歴，615 ページ

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

ACL の概要

ACL とは、トラフィックのフィルタリングに使用する順序付きのルール セットのことです。各ルールには、パケットがルールに一致するために満たさなければならない条件のセットが規定されています。デバイスは、ある ACL がパケットに適用されると判断すると、そのすべてのルールの条件にパケットを照合し、テストします。最初に一致したルールで、そのパケットが許可されるか拒否されるかが決定されます。一致するものがなければ、デバイスは適用可能な暗黙のルールを適用します。デバイスは、許可されたパケットの処理を続行し、拒否されたパケットはドロップします。

ACL を使用すると、ネットワークおよび特定のホストを、不要なトラフィックや望ましくないトラフィックから保護できます。たとえば、ACL を使用して、厳重にセキュリティ保護されたネットワークからインターネットにハイパー テキスト トランスファ プロトコル（HTTP）トラフィックが流入するのを禁止できます。また、特定のサイトへの HTTP トラフィックだけを許可することもできます。その場合は、サイトの IP アドレスが、IP ACL に指定されているかどうかによって判定します。

ACL のタイプと適用

セキュリティ トラフィック フィルタリングには次のタイプの ACL を使用できます。

FCoE ACL

Fibre Channel over Ethernet（FCoE）ACL は、ファイバ チャネル トラフィックだけに適用されます。FCoE の詳細については、『*Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500*』を参照してください。

IPv4 ACL

IPv4 トラフィックだけに適用されます。

IPv6 ACL

IPv6 トラフィックだけに適用されます。

MAC ACL

デフォルトでは、IP 以外のトラフィックだけに適用されます。ただし、すべてのトラフィックに MAC ACL を提供するようにレイヤ 2 インターフェイスを設定できます。

セキュリティ グループ ACL（SGACL）

Cisco TrustSec によってタグ付けされたトラフィックに適用されます。

IP ACL および MAC ACL には次のタイプの適用例があります。

ポート ACL

レイヤ 2 トラフィックのフィルタリング

ルータ ACL

レイヤ 3 トラフィックのフィルタリング

VLAN ACL

VLAN トラフィックのフィルタリング

VTY ACL

仮想テレタイプ（VTY）トラフィックのフィルタリング

次の表に、セキュリティ ACL の適用例の概要を示します。

表 *31*：セキュリティ *ACL* の適用

アプリケーション	サポートするインターフェイス	サポートする ACL のタイプ
ポート ACL	• レイヤ 2 インターフェイス • レイヤ 2 イーサネット ポート チャネル インターフェイス ポート ACL をトランク ポートに適用すると、その ACL は、当該トランク ポート上のすべての VLAN 上のトラフィックをフィルタリングします。	• IPv4 ACL • IPv6 ACL • MAC ACL

アプリケーション	サポートするインターフェイス	サポートする ACL のタイプ
ルータ ACL	• VLAN インターフェイス • 物理層 3 インターフェイス • レイヤ 3 イーサネット サブインターフェイス • レイヤ 3 イーサネット ポート チャネル インターフェイス • レイヤ 3 イーサネット ポート チャネル サブインターフェイス • トンネル • 管理インターフェイス （注） VLAN インターフェイスを設定するには、先に VLAN インターフェイスをグローバルにイネーブルにする必要があります。詳細については、『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide*』を参照してください。	• IPv4 ACL • IPv6 ACL （注） MAC ACL は、MAC パケット分類をイネーブルにする場合だけ、レイヤ 3 インターフェイスでサポートされます。
VLAN ACL	• VLANs	• IPv4 ACL • IPv6 ACL • MAC ACL
VTY ACL	• VTY	• IPv4 ACL • IPv6 ACL

関連トピック

MAC ACL の概要，（618 ページ）

VLAN ACL の概要, （632 ページ）
MAC ACL の概要, （618 ページ）
SGACL と SGT , （426 ページ）

ACL の適用順序

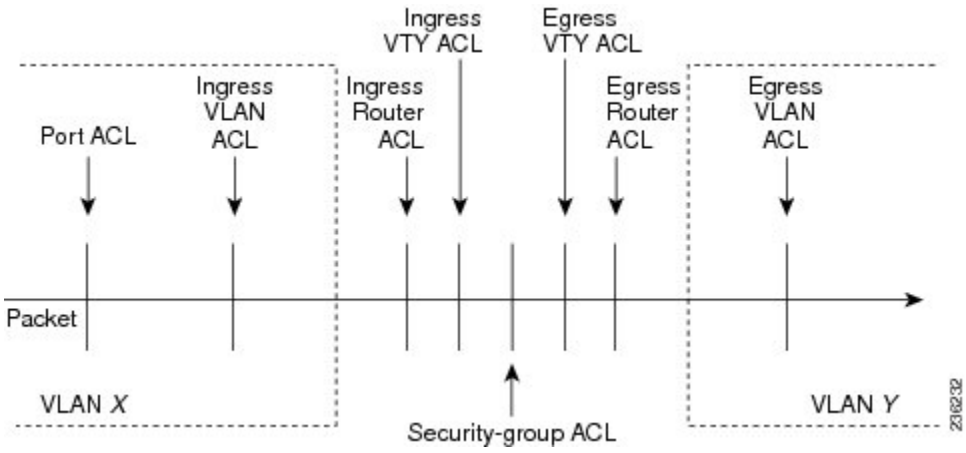
デバイスは、パケットを処理する際に、そのパケットの転送パスを決定します。デバイスがトラフィックに適用する ACL はパスによって決まります。デバイスは、次の順序で ACL を適用します。

1. ポート ACL
2. 入力 VACL
3. 入力ルータ ACL
4. 入力 VTY ACL
5. SGACL
6. 出力 VTY ACL
7. 出力ルータ ACL
8. 出力 VACL

パケットが入力 VLAN 内でブリッジされる場合、ルータ ACL は適用されません。

次の図に、デバイスが ACL を適用する順序を示します。

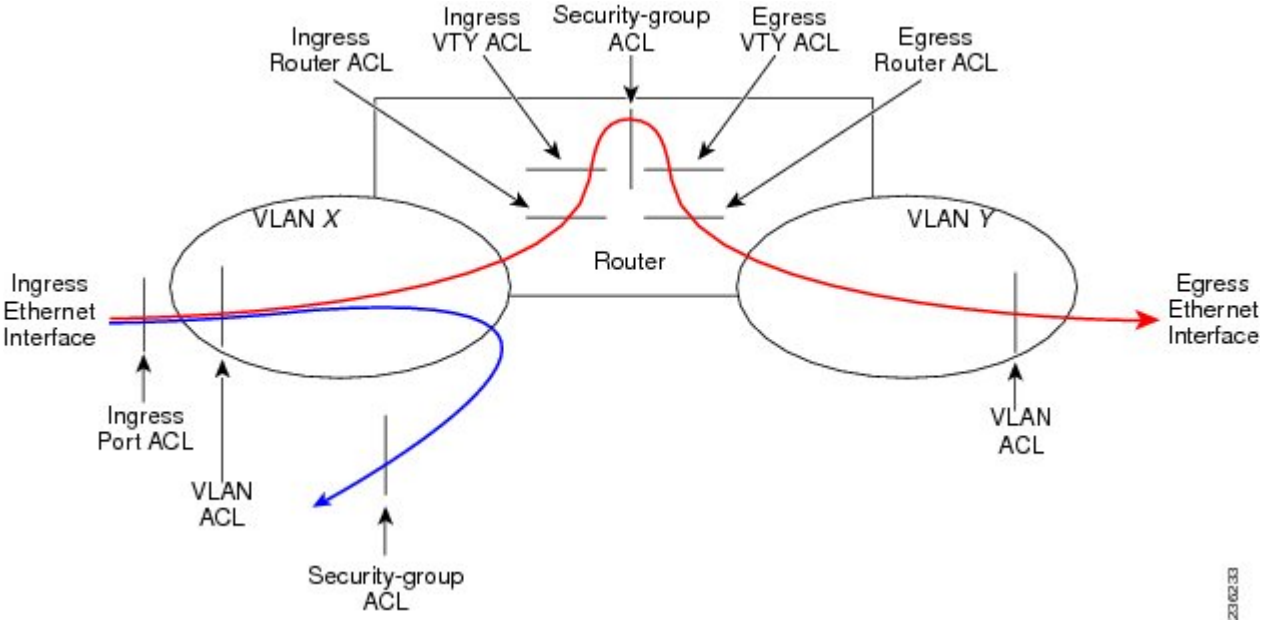
図 *22*：*ACL* の適用順序



次の図に、ACL のタイプに応じた ACL の適用場所を示します。赤いパスは送信元とは異なるインターフェイス上の宛先に送信されるパケットを表しています。青いパスは同じ VLAN 内でブリッジされるパケットを表しています。

デバイスは適用可能な ACL だけを適用します。たとえば、入力ポートがレイヤ 2 ポートの場合、VLAN インターフェイスである VLAN 上のトラフィックには、ポート ACL とルータ ACL が両方とも適用される可能性があります。さらに、その VLAN に VACL が適用される場合、デバイスはその VACL も適用します。

図 *23* : *ACL* とパケット フロー



関連トピック

SGACL と SGT , （426 ページ）

ルールについて

ACLによるネットワーク トラフィックのフィルタリング方法を設定する際に、何を作成、変更、削除するかを決めるのがルールです。ルールは実行コンフィギュレーション内に表示されます。ACL をインターフェイスに適用するか、またはインターフェイスにすでに適用されている ACL 内のルールを変更すると、スーパーバイザ モジュールは実行コンフィギュレーション内のルールから ACL のエントリを作成し、それらの ACL エントリを適用可能な I/O モジュールに送信します。ACL の設定によっては、ルールよりも ACL エントリの方が数が多くなることがあります。特に、ルールを設定するときにオブジェクト グループを使用してポリシーベース ACL を実装する場合などです。

ルールは、**permit** または **deny** コマンドを使用してアクセス リスト コンフィギュレーション モードで作成できます。これにより、デバイスは許可ルール内の基準と一致するトラフィックを許可し、拒否ルール内の基準と一致するトラフィックをブロックします。ルールに一致するためにトラフィックが満たさなければならない基準を設定するためのオプションが多数用意されています。

ここでは、ルールを設定する際に使用できるオプションをいくつか紹介します。すべてのオプションの説明については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』の該当する **permit** および **deny** コマンドを参照してください。

IP ACL のプロトコル

IPv4、IPv6、および MAC の ACL では、トラフィックをプロトコルで識別できます。指定の際の手間を省くために、一部のプロトコルは名前で指定できます。たとえば、IPv4 または IPv6 ACL では、ICMP を名前で指定できます。

プロトコルはすべて番号で指定できます。MAC ACL では、プロトコルをそのプロトコルの EtherType 番号（16 進数）で指定できます。たとえば、MAC ACL ルールの IP トラフィックの指定に 0x0800 を使用できます。

IPv4 および IPv6 ACL では、インターネット プロトコル番号を表す整数でプロトコルを指定できます。たとえば、レイヤ 2 トンネリング プロトコル（L2TP）を指定するには、115 を使用します。

ACL の各タイプが名前でサポートするプロトコルのリストについては、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』『』の該当する **permit** コマンドおよび **deny** コマンドを参照してください。

送信元と宛先

各ルールには、ルールに一致するトラフィックの送信元と宛先を指定します。指定する送信元および宛先には、特定のホスト、ホストのネットワークまたはグループ、あるいは任意のホストを使用できます。送信元と宛先の指定方法は、IPv4、IPv6、または MAC のどの ACL を設定するのかによって異なります。送信元と宛先の指定方法については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』の該当する **permit** および **deny** コマンドを参照してください。

IP ACL および MAC ACL の暗黙ルール

IP ACL および MAC ACL には暗黙ルールがあります。暗黙ルールは、実行コンフィギュレーションには設定されていませんが、ACL 内の他のルールと一致しない場合にデバイスがトラフィックに適用するルールです。ACL のルール単位の統計情報を維持するようにデバイスを設定した場合、暗黙ルールの統計情報はデバイスに維持されません。

すべての IPv4 ACL には、次の暗黙のルールがあります。

```
deny ip any any
```

この暗黙ルールによって、デバイスは不一致 IP トラフィックを確実に拒否します。

すべての IPv6 ACL には、次の暗黙ルールがあります。

```
permit icmp any any nd-na
permit icmp any any nd-ns
permit icmp any any router-advertisement
permit icmp any any router-solicitation
deny ipv6 any any
```

ICMPv6 のネイバー探索メッセージを拒否するルールを持つ IPv6 ACL を設定した場合を除き、最初の 4 つのルールによって、デバイスはネイバー探索アドバタイズメント メッセージと請求メッセージを許可するようになります。5 つめのルールにより、デバイスは不一致の IPv6 トラフィックを拒否します。

（注） IPv6 の ACL に **deny ipv6 any any** というルールを明示的に設定すると、暗黙の permit ルールでトラフィックをまったく許可できなくなります。**deny ipv6 any any** というルールを明示的に設定するものの、ICMPv6 ネイバー探索メッセージは許可したい場合は、5 つの暗黙の IPv6 ACL ルールをすべて明示的に設定します。

すべての MAC ACL には、次の暗黙のルールがあります。

```
deny any any protocol
```

この暗黙ルールによって、デバイスは、トラフィックのレイヤ 2 ヘッダーに指定されているプロトコルに関係なく、不一致トラフィックを確実に拒否します。

その他のフィルタリング オプション

追加のオプションを使用してトラフィックを識別できます。これらのオプションは、ACL のタイプによって異なります。次のリストには、ほとんどの追加フィルタリング オプションが含まれていますが、すべてを網羅しているわけではありません。

- IPv4 ACL には、次の追加フィルタリング オプションが用意されています。
  - レイヤ 4 プロトコル
  - 認証ヘッダー プロトコル
  - Enhanced Interior Gateway Routing Protocol（EIGRP）
  - カプセル化セキュリティ ペイロード
  - 総称ルーティング カプセル化（GRE）
  - KA9Q NOS 互換 IP over IP トンネリング
  - Open Shortest Path First（OSPF）
  - ペイロード圧縮プロトコル
  - プロトコル独立型マルチキャスト（PIM）
  - TCP/UDP ポート
  - ICMP タイプおよびコード
  - IGMP タイプ
  - 優先レベル
  - DiffServ コード ポイント（DSCP）値

- ACK、FIN、PSH、RST、SYN、または URG ビットがセットされた TCP パケット
- 確立済み TCP 接続
- パケット長

- IPv6 ACL では、次のフィルタリング オプションが追加されています。
  - レイヤ 4 プロトコル
  - 認証ヘッダー プロトコル
  - カプセル化セキュリティ ペイロード
  - ペイロード圧縮プロトコル
  - Stream Control Transmission Protocol（SCTP）
  - SCTP、TCP、および UDP の各ポート
  - ICMP タイプおよびコード
  - IGMP タイプ
  - フロー ラベル
  - DSCP の値
  - ACK、FIN、PSH、RST、SYN、または URG ビットがセットされた TCP パケット
  - 確立済み TCP 接続
  - パケット長

- MAC ACL は、次の追加フィルタリング オプションをサポートしています。
  - レイヤ 3 プロトコル
  - VLAN ID
  - サービス クラス（CoS）

ルールに適用できるすべてのフィルタリング オプションについては、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』の該当する **permit** および **deny** コマンドを参照してください。

シーケンス番号

デバイスはルールのシーケンス番号をサポートしています。入力するすべてのルールにシーケンス番号が割り当てられます（ユーザによる割り当てまたはデバイスによる自動割り当て）。シーケンス番号によって、次の ACL 設定作業が容易になります。

既存のルールの間に新しいルールを追加

シーケンス番号を指定することによって、ACL内での新規ルールの挿入場所を指定します。たとえば、ルール番号100と110の間に新しいルールを挿入する必要がある場合は、シーケンス番号105を新しいルールに割り当てます。

ルールの削除

シーケンス番号を使用しない場合は、ルールを削除するために、次のようにルール全体を入力する必要があります。

```
switch(config-acl)# no permit tcp 10.0.0.0/8 any
```

このルールに101番のシーケンス番号が付いていれば、次コマンドだけでルールを削除できます。

```
switch(config-acl)# no 101
```

ルールの移動

シーケンス番号を使用すれば、同じACL内の異なる場所にルールを移動する必要がある場合に、そのルールのコピーをシーケンス番号で正しい位置に挿入してから、元のルールを削除できます。この方法により、トラフィックを中断せずにルールを移動できます。

シーケンス番号を使用せずにルールを入力すると、デバイスはそのルールをACLの最後に追加し、そのルールの直前のルールのシーケンス番号よりも10大きい番号を割り当てます。たとえば、ACL内の最後のルールのシーケンス番号が225で、シーケンス番号を指定せずにルールを追加した場合、デバイスはその新しいルールにシーケンス番号235を割り当てます。

さらに、Cisco NX-OSではACL内のルールにシーケンス番号を再割り当てすることも可能です。シーケンス番号の再割り当ては、ACL内に、100、101のように連続するシーケンス番号のルールがある場合、それらのルールの間に1つ以上のルールを挿入する必要があるときに便利です。

論理演算子と論理演算ユニット

TCPおよびUDPトラフィックのIP ACLルールでは、論理演算子を使用して、ポート番号に基づきトラフィックをフィルタリングできます。このデバイスは、論理演算ユニット（LOU）というレジスタに、演算子とオペランドの組み合わせを格納します。Cisco Nexus 7000シリーズデバイスは104のLOUをサポートしています。

各タイプの演算子は、次のようにLOUを使用します。

eq

LOUには格納されません。

gt

1/2 LOUを使用します。

lt

1/2 LOUを使用します。

neq

1/2 LOU を使用します。

range

1 LOU を使用します。

デバイスは、次の場合に演算子とオペランドの組み合わせを LOU に格納します。

- 演算子またはオペランドが、他のルールで使用されている演算子とオペランドの組み合わせと異なる場合、この組み合わせは LOU に格納されます。

  たとえば、演算子とオペランドの組み合わせ「gt 10」と「gt 11」は、別々に LOU の半分に格納されます。「gt 10」と「lt 10」も別々に格納されます。

- 演算子とオペランドの組み合わせがルール内の送信元ポートと宛先ポートのうちどちらに適用されるかは、LOU の使用方法に影響を与えます。同じ組み合わせの一方が送信元ポートに、他方が宛先ポートに別々に適用される場合は、2 つの同じ組み合わせが別々に格納されます。

  たとえば、あるルールによって、演算子とオペランドの組み合わせ「gt 10」が送信元ポートに、別のルールによって同じ組み合わせ「gt 10」が宛先ポートに適用される場合、両方の組み合わせが LOU の半分に格納され、結果として 1 つの LOU 全体が使用されることになります。このため、「gt 10」を使用するルールが追加されても、これ以上 LOU は使用されません。

ロギング

ルールに一致するパケットに関する情報ログ メッセージの作成をイネーブルにできます。ログ メッセージには、パケットについての次の情報が含まれます。

- プロトコル
- TCP、UDP、またはICMPのいずれのパケットか、あるいは、番号が付けられただけのパケットか
- 送信元と宛先のアドレス
- 送信元と宛先のポート番号（該当する場合）

ACL キャプチャ

インターフェイスまたはVLAN上のトラフィックを選択的にモニタするために、ACLキャプチャを設定できます。

ACLルールのキャプチャ オプションをイネーブルにすると、このルールに一致したパケットは、指定された **permit** または **deny** アクションに基づいて転送またはドロップされます。また、さらに分析するために代替の宛先ポートにコピーされる場合もあります。

キャプチャ オプションでの ACL ルールは、次のように適用できます。

- VLAN 上で
- すべてのインターフェイス上の入力方向に
- すべてのレイヤ 3 インターフェイス上の出力方向に

ACL キャプチャは、さまざまなシナリオで使用できます。たとえば、ACL キャプチャで ACL ルールを使用してトンネルに属するパケットを識別したり、トンネル パケットのコピー（またはキャプチャ）を特定の宛先に送信したりできます。また、ACL キャプチャを使用すると、特定の VLAN 上のすべての HTTP トラフィックをモニタすることもできます。

最後に、キャプチャ セッションを ACL ルールごとに設定するのではなく、ACL 全体に対して設定することも可能です。この設定により、キャプチャ セッションがすべての ACL ルールに適用されます。

関連トピック

ACL キャプチャのイネーブル化またはディセーブル化, （590 ページ）
ACL キャプチャ セッションの設定, （591 ページ）
キャプチャ セッション ACE を使用した ACL のインターフェイスへの適用, （593 ページ）
すべての ACL キャプチャ セッションのインターフェイスへの適用, （595 ページ）

時間範囲

時間範囲を使用して、ACL ルールが有効になる時期を制御できます。たとえば、インターフェイスに着信するトラフィックに特定の ACL を適用するとデバイスが判断し、その ACL のあるルールの時間範囲が有効になっていない場合、デバイスは、トラフィックをそのルールと照合しません。デバイスは、そのデバイスのクロックに基づいて時間範囲を評価します。

時間範囲を使用する ACL を適用すると、デバイスはその ACL で参照される時間範囲の開始時または終了時に影響する I/O モジュールをアップデートします。時間範囲によって開始されるアップデートはベストエフォート型のプライオリティで実行されます。時間範囲によってアップデートが生じたときにデバイスの処理負荷が非常に高い場合、デバイスはアップデートを最大数秒間遅らせることがあります。

IPv4、IPv6、および MAC の各 ACL は時間範囲をサポートしています。デバイスがトラフィックに ACL を適用する場合、有効なルールは次のとおりです。

- 時間範囲が指定されていないすべてのルール
- デバイスがその ACL をトラフィックに適用した時点（秒）が時間範囲に含まれているルール

名前が付けられた時間範囲は再利用できます。多くの ACL ルールを設定する場合は、時間範囲を名前で一度設定すれば済みます。時間範囲の名前は最大 64 の英文字で指定します。

時間範囲には、1 つまたは複数のルールで構成されます。これらのルールは次の 2 種類に分類できます。

絶対

特定の開始日時、終了日時、その両方を持つルール、またはそのどちらも持たないルール。絶対時間範囲のルールがアクティブかどうかは、開始日時または終了日時の有無によって、次のように決まります。

- 開始日時と終了日時が両方指定されている：この時間範囲ルールは、現在の時刻が開始日時よりも後で終了日時よりも前の場合にアクティブになります。
- 開始日時が指定され、終了日時は指定されていない：この時間範囲ルールは、現在の時刻が開始日時よりも後である場合にアクティブになります。
- 開始日時は指定されず、終了日時が指定されている：この時間範囲ルールは、現在の時刻が終了日時よりも前である場合にアクティブになります。
- 開始日時も終了日時も指定されていない：この時間範囲ルールは常にアクティブです。

たとえば、新しいサブネットへのアクセスを許可するようにネットワークを設定する場合、そのサブネットをオンラインにする予定日の真夜中からアクセスを許可するような時間範囲を指定し、この時間範囲をそのサブネットに適用する ACL ルールに使用します。デバイスはこのルールを含む ACL を適用する場合、開始日時が過ぎると、この時間範囲を使用するルールの適用を自動的に開始します。

定期

毎週 1 回以上アクティブになるルール。たとえば、定期時間範囲を使用すると、平日の営業時間中だけ、研究室のサブネットにアクセスできるようにすることができます。デバイスは、そのルールを含む ACL が適用されていて、時間範囲がアクティブな場合にだけ、この時間範囲を使用する ACL ルールを自動的に適用します。

（注） デバイスは、時間範囲内のルールの順序に関係なく、時間範囲がアクティブかどうかを判断します。Cisco NX-OS は、時間範囲を編集できるように時間範囲内にシーケンス番号を入れます。

時間範囲には備考を含めることもできます。備考を使用すると、時間範囲にコメントを挿入できます。備考は、最大 100 文字の英数字で指定します。

デバイスは次の方法で時間範囲がアクティブかどうかを判断します。

- 時間範囲に絶対ルールが 1 つまたは複数含まれている：現在の時刻が 1 つまたは複数の絶対ルールの範囲内であれば、その時間範囲はアクティブです。
- 時間範囲に定期ルールが 1 つまたは複数含まれている：現在の時刻が 1 つまたは複数の定期ルールの範囲内であれば、その時間範囲はアクティブです。
- 時間範囲に絶対ルールと定期ルールが両方含まれている：現在の時刻が 1 つまたは複数の絶対ルールと 1 つ以上の定期ルールの範囲内にある場合に、その時間範囲はアクティブです。

時間範囲に絶対ルールと定期ルールが両方含まれている場合、定期ルールがアクティブになるのは、最低 1 つの絶対ルールがアクティブな場合だけです。

ポリシーベース ACL

デバイスはポリシーベース ACL（PBACL）をサポートしています。PBACL を使用すると、オブジェクト グループ全体にアクセス コントロール ポリシーを適用できます。オブジェクト グループは、IP アドレスのグループまたは TCP ポートもしくは UDP ポートのグループです。ルール作成時に、IP アドレスやポートを指定するのではなく、オブジェクト グループを指定できます。

IPv4 または IPv6 の ACL の設定にオブジェクト グループを使用すると、ルールの送信元または宛先に対してアドレスまたはポートの追加や削除を行う場合に、ACL を簡単にアップデートできます。たとえば、3 つのルールが同じ IP アドレス グループ オブジェクトを参照している場合は、3 つのすべてのルールを変更しなくても、オブジェクトに IP アドレスを追加すれば済みます。

PBACL を使用しても、インターフェイスに ACL を適用する際にその ACL が必要とするリソースは減りません。PBACL の適用時、またはすでに適用されている PBACL のアップデート時には、デバイスはオブジェクト グループを参照する各ルールを展開し、グループ内の各オブジェクトと ACL エントリが 1 対 1 になるようにします。あるルールに、送信元と宛先が両方ともオブジェクト グループとして指定されている場合、この PBACL を適用する際に I/O モジュールに作成される ACL エントリの数は、送信元グループ内のオブジェクト数に宛先グループ内のオブジェクト数をかけた値になります。

ポート、ルータ、 VLAN の ACL には、次のオブジェクト グループ タイプが適用されます。

IPv4 アドレス オブジェクト グループ

IPv4 ACL ルールで送信元または宛先アドレスの指定に使用できます。**permit** コマンドまたは **deny** コマンドを使用してルールを設定する際に、**addrgroup** キーワードを使用すると、送信元または宛先のオブジェクト グループを指定できます。

IPv6 アドレス オブジェクト グループ

IPv6 ACL ルールで送信元または宛先アドレスの指定に使用できます。**permit** コマンドまたは **deny** コマンドを使用してルールを設定する際に、**addrgroup** キーワードを使用すると、送信元または宛先のオブジェクト グループを指定できます。

プロトコル ポート オブジェクト グループ

IPv4 および IPv6 の TCP および UDP ルールで送信元または宛先のポートの指定に使用できます。**permit** コマンドまたは **deny** コマンドを使用してルールを設定する際に、**portgroup** キーワードを使用すると、送信元または宛先のオブジェクト グループを指定できます。

統計情報と ACL

このデバイスは IPv4 ACL、IPv6 ACL、および MAC ACL に設定した各ルールのグローバル統計を保持できます。1 つの ACL が複数のインターフェイスに適用される場合、ルール統計には、その

ACL が適用されるすべてのインターフェイスと一致する（ヒットする）パケットの合計数が維持されます。

（注） インターフェイスレベルの ACL 統計はサポートされていません。

設定する ACL ごとに、その ACL の統計情報をデバイスが維持するかどうかを指定できます。これにより、ACL によるトラフィック フィルタリングが必要かどうかに応じて ACL 統計のオン、オフを指定できます。また、ACL 設定のトラブルシューティングにも役立ちます。

デバイスには ACL の暗黙ルールの統計情報は維持されません。たとえば、すべての IPv4 ACL の末尾にある暗黙の **deny ip any any** ルールと一致するパケットのカウントはデバイスに維持されません。暗黙ルールの統計情報を維持する場合は、暗黙ルールと同じルールを指定した ACL を明示的に設定する必要があります。

関連トピック

IP ACL の統計情報のモニタリングとクリア，（598 ページ）
IP ACL および MAC ACL の暗黙ルール，（555 ページ）

Atomic ACL のアップデート

Atomic ACL のアップデートは、既存の ACL とアップデートした ACL の両方が TCAM メモリにプログラミングされたハードウェア操作です。これが操作のデフォルト モードです。このアップデート法の利点は、ACL の変更がサービスに影響しないということです。ACL を変更するとき、現在の ACL が TCAM にすでにプログラミングされています。そして Cisco Nexus 7000 シリーズのデバイスは、現在の ACL を取得して、それを変更分とマージして ACL プライムを生成します。ACL プライムもまた、TCAM にプログラムされます。その後 Cisco Nexus 7000 シリーズのデバイスは、ポインタを変更して ACL プライムをインターフェイスに関連付けられるようにします。最後の手順として、TCAM から古い ACL を削除します。これは機能的には、Atomic ACL のアップデートを使用する場合、ACL TCAM リソースの 50 パーセントを超えることができないということを意味します。Atomic ACL のアップデートがアクティブなときに ACL リソースの 50 パーセントを超えると、「ERROR: Tcam will be over used, please turn off atomic update」というメッセージを受信し、新しい ACL の変更は適用されません。

Nonatomic ACL のアップデートは、50 パーセント超の ACL TCAM を使用している場合に必要です。このモードがアクティブな場合、Cisco Nexus 7000 シリーズのデバイスは、早急に TCAM から古い ACL を削除して、それを ACL プライムに置き換えます。これにより、最大 100 パーセントの ACL TCAM を使用できますが、マイナス面としてサービスの一時中断が起きる場合があります。それは、古い ACL によって許可されたパケットが ACL プライムが ACL TCAM に正常にプログラムされるまでドロップされるためです。

デフォルトでは、Cisco Nexus 7000 シリーズのデバイスのスーパーバイザ モジュールで、ACL の変更を I/O モジュールにアップデートする際には、Atomic ACL のアップデートを実行します。Atomic アップデートでは、アップデートされる ACL が適用されるトラフィックを中断させることがありません。しかし、Atomic アップデートでは、ACL のアップデートを受け取る I/O モジュールに、関係する ACL の既存のすべてのエントリに加えて、アップデートされた ACL エントリを

保存するのに十分なリソースがあることが必要です。アップデートが行われた後、アップデートに使用されたリソースは開放されます。I/O モジュールに十分なリソースがない場合は、デバイスからエラー メッセージが出力され、この I/O モジュールに対する ACL のアップデートは失敗します。

I/O モジュールに Atomic アップデートに必要なリソースがない場合は、**no hardware access-list update atomic** コマンドを使用して Atomic アップデートをディセーブルにすることができますが、デバイスで既存の ACL を削除して、アップデートされた ACL を適用するには、多少の時間がかかります。ACL が適用されるトラフィックは、デフォルトでドロップされます。

ACL が適用されるすべてのトラフィックを許可し、同時に非 Atomic アップデートを受信するようにするには、**hardware access-list update default-result permit** コマンドを使用してください。

（注） **hardware access-list update** コマンドはデフォルトの VDC でだけ使用できます。ただし、すべての VDC に適用されます。

次の例では、ACL に対する Atomic アップデートをディセーブルにする方法を示します。

```
switch# config t
switch(config)# no hardware access-list update atomic
```

次の例では、非 Atomic ACL アップデートの際に、関連するトラフィックを許可する方法を示します。

```
switch# config t
switch(config)# hardware access-list update default-result permit
```

次の例では、Atomic アップデート方式に戻る方法を示します。

```
switch# config t
switch(config)# no hardware access-list update default-result permit
switch(config)# hardware access-list update atomic
```

Atomic ACL アップデートの計画

各モジュールのすべての ACL で使用している ACE（Access Control Element）の数を認識するために必要な Atomic ACL アップデートを適切に計画します。また、TCAM がサポートできる ACE の数を把握する必要があります。**show hardware access-list resource utilization mod***module-number* コマンドを使用して現在の使用状況を確認できます。

```
show hardware access-list resource
utilization mod 3
 INSTANCE 0x0
 -------------
 ACL Hardware Resource Utilization (Mod 3)
 ------------------------------------------
                Used  Free  Percent
                            Utilization
 ------------------------------------------------------
 Tcam 0, Bank 0  1   16383  0.01
 Tcam 0, Bank 1  2   16382  0.01
 Tcam 1, Bank 0  7   16377  0.04
 Tcam 1, Bank 1  138 16246  0.84
```

M シリーズ モジュールの場合、ACL TCAM は 4 バンクに分散されます。非 XL モジュールの場合、各バンクに合計 64K エントリーに対し 16,000 エントリがあります。XL モジュールの場合、

各バンクに合計 128,000 エントリーに対し 32,000 エントリがあります。通常、単一の ACL は単一の TCAM バンクのリソースのみを使用します。単一の ACL が、すべてのバンクからのリソースを使用することをイネーブルにするには、**hardware access-list resource pooling module***mod-numbe*r コマンドを使用してバンク プーリングを有効にする必要があります。

バンク プーリングがイネーブルにされたことを **show hardware access-list resource pooling** コマンドで確認できます。

ACL TCAM バンク マッピング

ACL Ternary Control Address Memory（TCAM）バンク マッピングにより、TCAM バンクがより予測可能な方法でより多くの機能の組み合わせに対応できるようになります。機能は、機能グループにあらかじめ分類され、TCAM バンクとの共存が許可される機能に応じてさらに機能クラスに事前定義されます。たとえば、1 つのポート ACL（ポート ACL）機能と 1 つのレイヤ 2 NetFlow 機能は、1 つの機能クラスとして定義されます。これらのクラスは、特定のバンクに割り当てられます。特定の TCAM バンクでサポートされない機能クラスをイネーブルまたはディセーブルにするとエラー メッセージが表示されます。

ACL TCAM バンク マッピングにより、一連の機能を同時に設定したり、共存できない機能の組み合わせが同じ TCAM バンクに設定された場合に蓄積する複数の結果を削減することができます。この機能を使用すると、領域を最適化し、TCAM バンクの使用率を最大化できます。

Cisco NX-OS Release 6.2(10) 以降では、**show hardware access-list** {**input** | **output**} {**interface** | **vlan**} **feature-combo***features* コマンドを発行して、バンク マッピングのマトリックスを表示できます。

フレキシブル ACL TCAM バンク チェーニング

Cisco NX-OS Release 7.3(0)D1(1) 以前のリリースでは、ACL による Ternary Control Address Memory バンクの使用は、次のとおりでした。

- 単一の ACL が、単一の TCAM バンクのリソースを使用。
- 単一の ACL が、バンク チェーニング モードがイネーブルであるすべての TCAM バンクのリソースを使用。

バンク チェーニング モードでは、すべてのバンクに対応できるほど ACL が大きくない場合でも、1 つの宛先に対して 1 つの ACL 結果タイプのみ設定できます。ただし、フレキシブル バンク チェーニング機能はこの制限を克服し、2 つの TCAM バンクをチェーニングして、方向ごとに、1 パケットに 2 つの結果を含む 2 つの ACL を設定できます。これにより、複数の TCAM バンクにまたがるより大きな ACL を使用できます。

（注） フレキシブル ACL TCAM バンク チェーニング機能は、F3 シリーズ モジュールでのみサポートされます。

次に、F3 モジュールを使用したシナリオを検討します。モジュールには 16 K のエントリ、各バンクには 4 K のエントリが含まれています。

- シナリオ 1：1 つの PACL が設定されており、16 K のエントリが含まれます。

  ソリューション：このシナリオでは、PACL に対応するために、4 つのすべての TCAM バンクを使用する完全バンク チェーニング モードをイネーブルにする必要があります。

- シナリオ 2：1 つの PACL が L2 ポートに設定され、1 つの RACL が VLAN に設定されています。L2 ポートが VLAN の一部であることに注意してください。各 ACL には 8 K 未満のエントリが含まれます。

  ソリューション：完全バンク チェーニング モードでは、PACL と RACL の組み合わせはサポートされません。ただし、この組み合わせは、フレキシブル TCAM バンク チェーニング機能ではサポートされます。PACL は第 1 の TCAM の 2 つのバンクに対応し、RACL は第 2 の TCAM の 2 つのバンクに対応します。

（注） フレキシブル ACL TCAM バンク チェーニング機能は、admin VDC 内で、モジュール レベルでイネーブル化されます。

フレキシブル ACL TCAM バンク チェーニング モード

フレキシブル ACL TCAM バンク チェーニング機能は、次のモードをサポートします。

- VLAN-VLAN モード：方向ごとに、1 つの宛先に 2 つの VLAN 機能を設定する場合、このモードを使用します。たとえば、1 つの VLAN に QoS 機能と RACL 機能がある場合、TCAM 上で ACL に対応するには VLAN-VLAN モードを使用します。
- PORT-VLAN モード：方向ごとに、1 つの宛先にポート機能と VLAN 機能を設定する場合、このモードを使用します。たとえば、ポート上に NetFlow 機能、VLAN 上に BFD がある場合、TCAM 上でこれらの機能に対応するには PORT-VLAN モードを使用します。詳細な例については、シナリオ 2 を参照してください。

VLAN-VLAN モードおよび PORT-VLAN モードで TCAM バンクに割り当てられた機能は、バンク マッピング テーブルで確認できます。TCAM バンク マッピング テーブルを表示するには、次のコマンドを使用します。

 # show system internal access-list feature bank-chain mapvlan-vlan|port-vlan {egress | ingress} [module*module-number***]**

出力としてマッピング テーブルが表示されます。TCAM バンク マッピング内で同じ TCAM 下で、機能の結果タイプが重複するかどうかを確認できます。1 つの機能の結果タイプが重複しても、設定は失敗します。詳細については、「フレキシブル *ACL TCAM* バンク チェーニングのトラブルシューティング」を参照してください。

この機能が TCAM バンクで共存できるかどうかもチェックします。たとえば、1 つの RACL 機能と 1 つのレイヤ 2 NetFlow 機能は、1 つの機能クラスとして定義されます。これらのクラスは、特定のバンクに割り当てられます。特定の TCAM バンクでサポートされない機能クラスをイネーブルまたはディセーブルにするとエラー メッセージが表示されます。詳細は、「*ACL TCAM* バンク マッピング」を参照してください。

TCAM バンク マッピングの表示

次の例は、VLAN-VLAN TCAM バンク チェーニング モードのマッピング出力を示しています。

```
switch# show system internal access-list feature bank-chain map vlan-vlan ingress module 3
```

Feature	Rslt Type	T0B0	T0B1	T1B0	T1B1
QoS	Qos	X	X		
RACL	Acl			X	X
PBR	Acl			X	X
VACL	Acl			X	X
DHCP	Acl			X	X
ARP	Acl			X	X
Netflow	Acl			X	X
Netflow (SVI)	Acl			X	X
Netflow Sampler	Acc	X	X		
Netflow Sampler (SVI)	Acc	X	X		
SPM WCCP	Acl			X	X
BFD	Acl			X	X
SPM OTV	Acl			X	X
ACLMGR ERSPAN (source)	Acl			X	X
SPM_VINCI_PROXY	Acl			X	X
SPM_VINCI_ANYCAST	Acl			X	X
SPM_VINCI_FABRIC_VLAN	Acl			X	X
SPM ITD	Acl			X	X
SPM EVPN ARP	Acl			X	X

同じTCAMバンクに表示されていても、結果タイプが異なる場合、同時に設定することはできません。出力は、次の機能が TCAM0 と組み合わせて設定できないことを示しています。

- QoS および NetFlow サンプラ
- QoS および NetFlow サンプラ（SVI）

TCAM1については、QoS、NetFlowサンプラ、NetFlowサンプラ（SVI）を含まない任意の機能組み合わせを設定できます。

次の例は、PORT-VLAN TCAM バンク チェーニング モードのマッピング出力を示しています。

```
switch# show system internal access-list feature bank-chain map port-vlan ingress
```

Feature	Rslt Type	T0B0	T0B1	T1B0	T1B1
PACL	Acl	X	X		
RACL	Acl			X	X
DHCP	Acl			X	X
QoS	Qos	X	X		
PBR	Acl			X	X
VACL	Acl			X	X
Netflow	Acl			X	X
Netflow Sampler	Acc	X	X		
SPM WCCP	Acl			X	X
BFD	Acl			X	X
SPM OTV	Acl	X	X		
FEX	Acl	X	X		
SPM CBTS	Acl	X	X		
SPM LISP INST	Acl	X	X		
Openflow	Acl			X	X
SPM ITD	Acl			X	X

入力方向で QoS 機能を設定する場合のシナリオを検討します。ただし、QoS 機能が TCAM0 に対応していてる場合、PACL、Netflow Sampler、SPM OTV、FEX、SPM CBTS、および SPM LISP INST 機能は設定できません。また、PACL 機能は入力にのみ適用できることに注意してください。

IP ACL に対する Session Manager のサポート

Session Manager は IP ACL および MAC ACL の設定をサポートしています。この機能を使用すると、ACL の設定を調べて、その設定に必要とされるリソースが利用可能であるかどうかを、リソースを実行コンフィギュレーションにコミットする前に確認できます。

IP ACL のバーチャライゼーション サポート

仮想デバイス コンテキスト（VDC）で使用される IP ACL および MAC ACL には、次の事項が適用されます。

- ACL は各 VDC に固有です。ある VDC に作成した ACL は別の VDC に使用できません。
- ACL が複数の VDC に共有されることはないので、ACL 名は他の VDC に再利用できます。
- デバイスは、ACL やルールを VDC 単位では制限しません。
- アトミック ACL 更新の設定は、デフォルト VDC で実行する必要がありますが、すべての VDC に適用されます。

IP ACL のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	IP ACL を使用するためにライセンスは必要ありません。ただし、XL ラインカードを使用して最大 128K の ACL エントリをサポートするには、スケーラブルなサービス ライセンスをインストールする必要があります。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

IP ACL の前提条件

IP ACL の前提条件は次のとおりです。

- IP ACL を設定するためには、IP アドレッシングおよびプロトコルに関する知識が必要です。

- ACL を設定するインターフェイス タイプについての知識が必要です。

IP ACL の注意事項と制約事項

IP ACL の設定に関する注意事項と制約事項は次のとおりです。

- アクセス コントロール リスト（ACL）は、元のパケットの入力に適用されると、実際の出力ポートの宛先インデックスを取得します。その時点では、Encapsulated Remote Switched Port Analyzer（ERSPAN）セッションの出力のポイントは認識されません。パケットは、書き換え後に ACL エンジンを通過しないため、ERSPAN パケットに一致させることができません。
- ACL の設定には Session Manager を使用することを推奨します。この機能を使用すると、ACL の設定を調べて、その設定に必要とされるリソースが利用可能であるかどうかを、リソースを実行コンフィギュレーションにコミットする前に確認できます。この機能は、約 1,000 以上のルールが含まれている ACL に対して特に有効です。Session Manager の詳細については、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*』を参照してください。
- ほとんどの場合、IP パケットに対する ACL 処理は I/O モジュール上で実行されます。これには、ACL 処理を加速化するハードウェアを使用します。場合によっては、スーパーバイザ モジュールで処理が実行されることもあります。この場合、特に非常に多数のルールが設定されている ACL を処理する際には、処理速度が遅くなることがあります。管理インターフェイス トラフィックは、常にスーパーバイザ モジュールで処理されます。次のカテゴリのいずれかに属する IP パケットがレイヤ 3 インターフェイスから出る場合、これらのパケットはスーパーバイザ モジュールに送られて処理されます。
  - レイヤ 3 最大伝送単位チェックに失敗し、そのためにフラグメント化を要求しているパケット
  - IP オプションがある IPv4 パケット（追加された IP パケット ヘッダーのフィールドは、宛先アドレス フィールドの後）
  - 拡張 IPv6 ヘッダー フィールドがある IPv6 パケット

  レート制限を行うことで、リダイレクト パケットによってスーパーバイザ モジュールに過剰な負荷がかかるのを回避します。

（注） Cisco NX-OS Release 4.2(3) よりも前のリリースでは、ACL ロギングは、スーパーバイザ モジュールで生じる ACL 処理には対応していません。

- 時間範囲を使用する ACL を適用すると、デバイスはその ACL で参照される時間範囲の開始時または終了時に、影響する I/O モジュールに対する ACL エントリをアップデートします。時間範囲によって開始されるアップデートはベストエフォート型のプライオリティで実行されます。時間範囲によってアップデートが生じたときにデバイスの処理負荷が非常に高い場合、デバイスはアップデートを最大数秒間遅らせることがあります。

- IP ACL を VLAN インターフェイスに適用するためには、VLAN インターフェイスをグローバルにイネーブル化する必要があります。VLANインターフェイスの詳細については、『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide*』を参照してください。
- サポートされる IP ACL エントリの最大数は、XL ライン カードを使用しないデバイスで 64,000、XL ライン カードを使用するデバイスで 128,000 です。
- XL 以外のラインカードに適用する ACL エントリが多すぎると、設定が拒否されます。

  VTY ACL 機能はすべての VTY 回線のすべてのトラフィックを制限します。異なる VTY 回線に異なるトラフィックの制限を指定できません。

  どのルータの ACL も VTY ACL として設定できます。
- VTY に設定された ACL は、mgmt0 インターフェイスには適用されません。Mgmt0 ACL は特にインターフェイスに適用する必要があります。
- Cisco Nexus 2000 シリーズ Fabric Extender は、親の Cisco Nexus 7000 シリーズ デバイスで使用可能な入力 ACL をフルレンジでサポートしています。Fabric Extender に関する詳細については、『*Configuring the Cisco Nexus 2000 Series Fabric Extender*』を参照してください。
- ACL ポリシーは Fabric Extender ファブリック ポート チャネルではサポートされません。
- ACL キャプチャはハードウェアベース機能で、管理インターフェイスまたはスーパーバイザで発信される制御パケットではサポートされません。さらに、SNMP コミュニティ ACL および VTY ACL などのソフトウェア ACL でもサポートされません。
- ACL キャプチャをイネーブルにすると、すべての VDC の ACL ロギングと ACL ロギングのレート制限がディセーブルになります。
- ポートチャネル インターフェイス、およびスーパーバイザ インバンド ポートは ACL キャプチャの宛先としてサポートされません。
- ACL キャプチャ セッションの宛先インターフェイスは、入力転送と入力の MAC の学習をサポートしません。宛先インターフェイスでこれらオプションが設定されている場合、モニタが ACL のキャプチャ セッションをダウン状態にし続けます。入力転送および MAC の学習がイネーブルになっているかどうかを確認するには、**show monitor session all** コマンドを使用します。

  （注） インターフェイスで入力転送および MAC 学習をディセーブルにするには、**switchport monitor** コマンドを使用できます。
- パケットの送信元ポートと ACL キャプチャの宛先ポートは、同じパケット複製 ASIC の一部であってはなりません。両方のポートが同じ ASIC に属する場合、パケットはキャプチャされません。**show monitor session** コマンドにより、ACL キャプチャの宛先ポートとして同じ ASIC に接続するすべてのポートが表示されます。
- すべての VDC につき、システムで同時にアクティブにできる ACL キャプチャ セッションは 1 つだけです。

- **hardware access-list capture** コマンドを設定する前に ACL キャプチャ モニタ セッションを設定する場合は、モニタ セッションをシャット ダウンし、バックアップをしてセッションを開始する必要があります。
- 未定義の ACL をインターフェイスに適用すると、システムは空の ACL と見なし、すべてのトラフィックを許可します。
- IPv6 ポリシーの Atomic アップデートは中断を伴う場合があります。IPv6 送信元アドレスまたは宛先アドレスの追加、削除、変更がある場合は、更新により中断が発生する場合があります。
  - IPv6 ACE のレイヤ 4 フィールドを変更すると、中断は発生しません。
  - IPv6 アドレスの追加は常に中断を伴うわけではありませんが、中断が発生することがあります。
  - 既存のエントリのプレフィックス長を変更したり、新しいプレフィックス長のエントリを追加/削除した場合、中断が発生する場合があります。

  （注） F3 および M3 シリーズ モジュールでは、IPv6 ポリシーの Atomic アップデートは中断を伴いません。
- リソース プーリングと ACL TCAM バンク マッピングを同時にイネーブルにすることはできません。
- 共有インターフェイス上では、**mac packet-classify** コマンドを設定できません。
- M1 シリーズ モジュール
  - M1 シリーズ モジュールのサポート ACL キャプチャ。
  - FCoE ACL は M1 シリーズ モジュールではサポートされません。
  - M1 シリーズ モジュールでは、**mac packet-classify** コマンドによってポートおよび VLAN ポリシーの MAC ACL がイネーブルになります
  - M1 シリーズ モジュールは WCCP をサポートします。
- M2 シリーズ モジュール
  - M2 シリーズ モジュールのサポート ACL キャプチャ。
  - FCoE ACL は M2 シリーズ モジュールではサポートされません。
  - M2 シリーズ モジュールでは、**mac packet-classify** コマンドによってポートおよび VLAN ポリシーの MAC ACL がイネーブルになります
  - M2 シリーズ モジュールは WCCP をサポートします。
- Cisco NX-OS Release 7.3(0)DX(1) 以降では、M3 シリーズ モジュールがサポートされます。注意事項と制限事項は次のとおりです。

- M3 シリーズ モジュールは、ACL キャプチャをサポートします。
- FCoE ACL は M3 シリーズ モジュールではサポートされません。
- M3 シリーズ モジュールでは、**mac packet-classify** コマンドによってポートおよび VLAN ポリシーの MAC ACL がイネーブルになります
- M3 シリーズ モジュールは WCCP をサポートします。

• F1 シリーズ モジュール

- F1 シリーズ モジュールの各転送エンジンは 1000 の入力 ACL エントリをサポートします。また、984 のエントリがユーザ設定に使用できます。F1 シリーズ モジュール用の IP ACL エントリの総数は 1000 ～ 16,000 です。転送エンジンに応じてポリシーが適用されます。
- F1 シリーズ モジュールの 16 の転送エンジンごとに、複数の ACL で最大 250 の IPv6 アドレスをサポートします。
- 各ポート ACL は、F1 シリーズ モジュールの異なるレイヤ 4 演算を最大 4 つサポートできます。
- F1 シリーズ モジュールはルータ ACL をサポートしていません。
- F1 シリーズ モジュールには、ACL ロギングをサポートしていません。
- F1 シリーズ モジュールはバンク チェーニングをサポートしていません。
- F1 シリーズ モジュールは ACL キャプチャをサポートしていません。
- FCoE ACL は、F1 シリーズ モジュールでのみサポートされます。
- F1 シリーズ モジュールでは、WCCP はサポートされません。
- F1 シリーズ モジュールでは、ACL TCAM バンク マッピングはサポートされません。
- F1 シリーズ モジュール プロキシ転送トラフィックの場合、ACL 分類は次の表に示すレイヤ 3 プロトコルと照合されます。

表 *32*：プロトコル番号と関連付けられているレイヤ *3* プロトコル

プロトコル番号	レイヤ 3 プロトコル
1	ICMP
2	IGMP
4	IPv4 カプセル化
6	TCP
17	UDP

（注） 表に記載されていないレイヤ 3 プロトコルは、プロトコル番号 4（IPv4 カプセル化）に分類されます。

- F2 シリーズ モジュール
  - F2 シリーズ モジュールの 12 の転送エンジンごとに、総数 16,000 の TCAM エントリが 2 つのバンクに対して均等に分割されます。デフォルトの 168 エントリが予約されます。各転送エンジンは、512 の IPv6 圧縮 TCAM エントリを持ちます。
  - F2 シリーズ モジュールは ACL キャプチャをサポートしていません。
  - F2 シリーズ モジュールの場合、出力 ACL の **log** オプションはマルチキャスト パケットではサポートされません。
  - F2 シリーズ モジュールが異なる VDC 間で共有されている場合、1 つの VDC で設定された出力 ACL は別の VDC へと押し出されます。
  - F2 シリーズ モジュールは SVI の出力 WCCP をサポートしていません。
  - F2 シリーズ モジュールの場合、**mac packet-classify** コマンドにより、VLAN ポリシーの IPv4 ACL または IPv6 ACL ではなく、ポート ポリシーの MAC ACL をイネーブルにします。
- 2 つのバンクを同じ TCAM 内でチェーニングできます。ただし、複数の TCAM 間でバンクをチェーニングすることはできません。
- バンク チェーニング機能とバンク マッピング機能は共存できません。
- フレキシブル ACL TCAM バンク チェーニング機能の設定のために VLAN-VLAN モードをイネーブルにしているときは、PACL、L2 QoS、および L2 NetFlow などの ACL 機能は設定できません。
- フレキシブル ACL TCAM バンク チェーニング機能は、F3 シリーズ モジュールでのみサポートされます。
- すべてのモジュールでのフレキシブル ACL TCAM バンク チェーニング機能のイネーブル化はサポートされません。
- F3 シリーズ モジュール
  - F3 シリーズ モジュール転送エンジンでは、総数 16,000 の TCAM エントリが 2 つのバンクに対して均等に分割されます。
  - F3 シリーズ モジュールは、ACL キャプチャをサポートします。
  - F3 シリーズ モジュールは、FCoE ACL をサポートします。
  - F3 シリーズ モジュールの場合、出力 ACL の log オプションはマルチキャスト パケットではサポートされません。

- F3 シリーズ モジュールが異なる VDC 間で共有されている場合、1 つの VDC で設定された出力 ACL は別の VDC へと押し出されます。
- F3 シリーズ モジュールの場合、**mac packet-classify** コマンドにより、VLAN ポリシーの IPv4 ACL または IPv6 ACL ではなく、ポート ポリシーの MAC ACL をイネーブルにします。
- 2 つのバンクを同じ TCAM 内でチェーニングできます。ただし、複数の TCAM 間でバンクをチェーニングすることはできません。
- バンク チェーニング機能とバンク マッピング機能は共存できません。
- フレキシブル ACL TCAM バンク チェーニング機能の設定のために VLAN-VLAN モードをイネーブルにしているときは、PACL、L2 QoS、および L2 NetFlow などの ACL 機能は設定できません。
- フレキシブル ACL TCAM バンク チェーニング機能は、F3 シリーズ モジュールでのみサポートされます。
- すべてのモジュールでのフレキシブル ACL TCAM バンク チェーニング機能のイネーブル化はサポートされません。

IP ACL のデフォルト設定

次の表に、IP ACL パラメータのデフォルト設定を示します。

表 *33*：*IP ACL* パラメータのデフォルト値

パラメータ	デフォルト
IP ACL	デフォルトでは IP ACL は存在しません。
ACL ルール	すべての ACL に暗黙のルールが適用されます。
ACL キャプチャ	ディセーブル
オブジェクト グループ	デフォルトではオブジェクト グループは存在しません。
時間範囲	デフォルトでは時間範囲は存在しません。
ACL TCAM バンク マッピング	ディセーブル

関連トピック

IP ACL および MAC ACL の暗黙ルール，（555 ページ）

IP ACL の設定

IP ACL の作成

デバイスに IPv4 ACL または IPv6 ACL を作成し、これにルールを追加できます。

はじめる前に

ACL の設定には Session Manager を使用することを推奨します。この機能によって、ACL の設定を確認し、設定を実行コンフィギュレーションにコミットする前に、その設定が必要とするリソースが利用可能かどうかを確認できます。この機能は、約 1,000 以上のルールが含まれている ACL に対して特に有効です。Session Manager の詳細については、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*』を参照してください。

手順の概要

1. **configure terminal**
2. 次のいずれかのコマンドを入力します。
   - **ipaccess-list***name*
   - **ipv6access-list***name*
3. （任意） **fragments** {**permit-all** | **deny-all**}
4. [*sequence-number*] {**permit** | **deny**}*protocolsourcedestination*
5. （任意） **statistics per-entry**
6. （任意） 次のいずれかのコマンドを入力します。
   - **show ip access-lists***name*
   - **show ipv6 access-lists***name*
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 2	次のいずれかのコマンドを入力します。
	• **ipaccess-list***name*
	• **ipv6access-list***name*
	
	例：
	`switch(config)# ip access-list acl-01`
	`switch(config-acl)#`
		IP ACL を作成して、IP ACL コンフィギュレーション モードを開始します。*name* 引数は 64 文字以内で指定します。

ステップ 3	**fragments** {**permit-all** | **deny-all**} 例： `switch(config-acl)# fragments permit-all`	（任意） 初期状態でないフラグメントのフラグメント処理を最適化します。デバイスで、**fragments** コマンドが含まれる ACL がトラフィックに適用される場合、**fragments** コマンドは、ACL での明示的な **permit** コマンドまたは **deny** コマンドに一致しない非初期フラグメントだけに一致します。
ステップ 4	[*sequence-number*] {**permit** | **deny**}*protocolsourcedestination* 例： `switch(config-acl)# permit ip 192.168.2.0/24 any`	IP ACL 内にルールを作成します。多数のルールを作成できます。*sequence-number* 引数には、1 ～ 4294967295 の整数を指定します。 **permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。
ステップ 5	**statistics per-entry** 例： `switch(config-acl)# statistics per-entry`	（任意） その ACL のルールと一致するパケットのグローバル統計をデバイスが維持するように設定します。
ステップ 6	次のいずれかのコマンドを入力します。 • **show ip access-lists***name* • **show ipv6 access-lists***name* 例： `switch(config-acl)# show ip access-lists acl-01`	（任意） IP ACL の設定を表示します。
ステップ 7	**copy running-config startup-config** 例： `switch(config-acl)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

IP ACL の変更

既存の IPv4 ACL または IPv6 ACL のルールの追加と削除は実行できますが、既存のルールを変更することはできません。ルールを変更するには、そのルールを削除してから、変更を加えたルールを再作成します。

既存のルールの間に新しいルールを挿入する必要がある場合で、現在のシーケンス番号の空き状況ではすべてを挿入できないときは、**resequence** コマンドを使用してシーケンス番号を再割り当てします。

はじめる前に

ACL の設定には Session Manager を使用することを推奨します。この機能を使用すると、ACL の設定を調べて、その設定に必要とされるリソースが利用可能であるかどうかを、リソースを実行コンフィギュレーションにコミットする前に確認できます。この機能は、約 1,000 以上のルールが含まれている ACL に対して特に有効です。Session Manager の詳細については、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*』を参照してください。

手順の概要

1. **configure terminal**
2. 次のいずれかのコマンドを入力します。
   - **ipaccess-list***name*
   - **ipv6access-list***name*
3. （任意） [*sequence-number*] {**permit** | **deny**}*protocolsourcedestination*
4. （任意） [**no**] **fragments** {**permit-all** | **deny-all**}
5. （任意） **no** {*sequence-number* | {**permit** | **deny**}*protocolsourcedestination*}
6. （任意） [**no**] **statistics per-entry**
7. （任意） 次のいずれかのコマンドを入力します。
   - **show ip access-lists***name*
   - **show ipv6 access-lists***name*
8. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	次のいずれかのコマンドを入力します。
	• **ipaccess-list***name*
	• **ipv6access-list***name*
	
	例：
	`switch(config)# ip access-list acl-01`
	`switch(config-acl)#`
		名前で指定した ACL の IP ACL コンフィギュレーション モードを開始します。

ステップ 3	[*sequence-number*] {**permit** | **deny**}*protocolsourcedestination* 例： `switch(config-acl)# 100 permit ip 192.168.2.0/24 any`	（任意） IP ACL 内にルールを作成します。シーケンス番号を指定すると、ACL 内のルール挿入位置を指定できます。シーケンス番号を指定しないと、ルールは ACL の末尾に追加されます。*sequence-number* 引数には、1 ～ 4294967295 の整数を指定します。 **permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。詳細については、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*』を参照してください。
ステップ 4	[**no**] **fragments** {**permit-all** | **deny-all**} 例： `switch(config-acl)# fragments permit-all`	（任意） 初期状態でないフラグメントのフラグメント処理を最適化します。デバイスで、**fragments** コマンドが含まれる ACL がトラフィックに適用される場合、**fragments** コマンドは、ACL での明示的な **permit** コマンドまたは **deny** コマンドに一致しない非初期フラグメントだけに一致します。 **no** オプションを使用すると、フラグメント処理の最適化が削除されます。
ステップ 5	**no** {*sequence-number* | {**permit** | **deny**}*protocolsourcedestination*} 例： `switch(config-acl)# no 80`	（任意） 指定したルールを IP ACL から削除します。 **permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

	コマンドまたはアクション	目的
ステップ 6	[no] **statistics per-entry** 例： `switch(config-acl)# statistics per-entry`	（任意） そのACLのルールと一致するパケットのグローバル統計をデバイスが維持するように設定します。 **no** オプションを使用すると、デバイスはその ACL のグローバル統計の維持を停止します。
ステップ 7	次のいずれかのコマンドを入力します。 • **show ip access-lists***name* • **show ipv6 access-lists***name* 例： `switch(config-acl)# show ip access-lists acl-01`	（任意） IP ACL の設定を表示します。
ステップ 8	**copy running-config startup-config** 例： `switch(config-acl)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

IP ACL 内のシーケンス番号の変更，（581 ページ）

VTY ACL の作成

入力方向または出力方向の全 VTY 回線で、すべての IPv4 または IPv6 トラフィックへのアクセスを制御することにより、VTY ACL を設定できます。

はじめる前に

すべての仮想端末回線にユーザが接続できるため、すべての仮想端末回線に同じ制約を設定する必要があります。

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

ACL の設定には Session Manager を使用することを推奨します。この機能を使用すると、ACL の設定を調べて、その設定に必要とされるリソースが利用可能であるかどうかを、リソースを実行コンフィギュレーションにコミットする前に確認でき、特に約 1000 以上のルールを含む ACL に役立ちます。Session Manager の詳細については、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*』を参照してください。

手順の概要

1. **configure terminal**
2. {**ip** | **ipv6**} **access-list***name*
3. {**permit** | **deny**} *protocol source destination* [**log**] [**time-range** *time*]
4. **exit**
5. **line vty**
6. {**ip** | **ipv6**} **access-class***name* {**in** | **out**}
7. （任意） **show** {**ip** | **ipv6**} **access-lists**
8. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	{**ip** | **ipv6**} **access-list***name* 例： `switch(config)# ip access-list vtyacl`	ACL を作成し、その ACL の IP アクセス リスト コンフィギュレーション モードを開始します。*name* 引数の最大長は 64 文字です。
ステップ 3	{**permit** | **deny**} *protocol source destination* [**log**] [**time-range** *time*] 例： `switch(config-ip-acl)# permit tcp any any`	ACL ルールを作成し、指定した送信元とのすべての TCP トラフィックを許可します。

ステップ 4	**exit**
	
	例：
	`switch(config-ip-acl)# exit`
	`switch(config)#`
		IP アクセス リスト コンフィギュレーション モードを終了します。

ステップ 5	**line vty**
	
	例：
	`switch(config)# line vty`
	`switch(config-line)#`
		仮想端末を指定し、ライン コンフィギュレーション モードを開始します。

ステップ 6	{**ip** | **ipv6**} **access-class***name* {**in** | **out**} 例： `switch(config-line)# ip access-class vtyacl out`	指定された ACL を使用してすべての VTY 回線に対する着信および発信接続を制限します。*name* 引数の最大長は 64 文字です。

	コマンドまたはアクション	目的
ステップ 7	**show** {**ip** | **ipv6**} **access-lists** 例： `switch# show ip access-lists`	（任意） 任意の VTY ACL を含め、設定された ACL を表示します。
ステップ 8	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

IP ACL 内のシーケンス番号の変更

IP ACL 内のルールに付けられたすべてのシーケンス番号を変更できます。

はじめる前に

ACL の設定には Session Manager を使用することを推奨します。この機能を使用すると、ACL の設定を調べて、その設定に必要とされるリソースが利用可能であるかどうかを、リソースを実行コンフィギュレーションにコミットする前に確認できます。この機能は、約 1,000 以上のルールが含まれている ACL に対して特に有効です。Session Manager の詳細については、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*』を参照してください。

手順の概要

1. **configure terminal**
2. **resequence** {**ip** | **ipv6**} **access-list** *name starting-sequence-numberincrement*
3. （任意） **show ip access-lists** *name*
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**resequence** {**ip** | **ipv6**} **access-list** *name starting-sequence-numberincrement* 例： `switch(config)# resequence access-list ip acl-01 100 10`	ACL 内に記述されているルールにシーケンス番号を付けます。指定した開始シーケンス番号が最初のルールに付けられます。後続の各ルールには、直前のルールよりも大きい番号が付けられます。番号の間隔は、指定した増分によって決まります。*starting-sequence-number* 引数と *increment* 引数は、1 ～ 4294967295 の整数で指定します。
ステップ 3	**show ip access-lists** *name* 例： `switch(config)# show ip access-lists acl-01`	（任意） IP ACL の設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

IP ACL の削除

IP ACL をデバイスから削除できます。

はじめる前に

そのACLがインターフェイスに適用されているかどうかを確認します。削除できるのは、現在適用されている ACL です。ACL を削除しても、その ACL が適用されていたインターフェイスの設定は影響を受けません。デバイスは削除された ACL を空であると見なします。IP ACL が設定されているインターフェイスを探すには、**show ip access-lists** コマンドまたは **show ipv6 access-lists** コマンドと一緒に summary キーワードを使用します。

手順の概要

1. **configure terminal**
2. 次のいずれかのコマンドを入力します。
   - **noip access-list***name*
   - **noipv6 access-list***name*
3. （任意） 次のいずれかのコマンドを入力します。
   - **show ip access-lists***name* **summary**
   - **show ipv6 access-lists***name* **summary**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	次のいずれかのコマンドを入力します。 • **noip access-list***name* • **noipv6 access-list***name* 例： `switch(config)# no ip access-list acl-01`	名前で指定した IP ACL を実行コンフィギュレーションから削除します。
ステップ 3	次のいずれかのコマンドを入力します。 • **show ip access-lists***name* **summary** • **show ipv6 access-lists***name* **summary** 例： `switch(config)# show ip access-lists acl-01 summary`	（任意） IP ACL の設定を表示します。ACL がインターフェイスに引き続き適用されている場合は、インターフェイスが表示されます。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ルータ ACL としての IP ACL の適用

IPv4 または IPv6 ACL は、次のタイプのインターフェイスに適用できます。

- 物理層 3 インターフェイスおよびサブインターフェイス
- レイヤ 3 イーサネット ポート チャネル インターフェイスおよびサブインターフェイス
- VLAN インターフェイス
- トンネル
- 管理インターフェイス

これらのインターフェイス タイプに適用された ACL はルータ ACL と見なされます。

はじめる前に

適用する ACL が存在し、目的に応じたトラフィック フィルタリングが設定されていることを確認します。

手順の概要

1. switch# **configure terminal**
2. 次のいずれかのコマンドを入力します。
   - switch(config)# **interfaceethernet***slot*/*port*[**.***number*]
   - switch(config)# **interfaceport-channel***channel-number*[**.***number*]
   - switch(config)# **interfacetunnel***tunnel-number*
   - switch(config)# **interfacevlan***vlan-ID*
   - switch(config)# **interfacemgmt***port*
3. 次のいずれかのコマンドを入力します。
   - switch(config-if)# **ipaccess-group** *access-list* {**in** | **out**}
   - switch(config-if)# **ipv6 traffic-filter** *access-list* {**in** | **out**}
4. （任意） switch(config-if)# **show running-config aclmgr**
5. （任意） switch(config-if)# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	次のいずれかのコマンドを入力します。 • switch(config)# **interfaceethernet***slot*/*port*[**.***number*] • switch(config)# **interfaceport-channel***channel-number*[**.***number*] • switch(config)# **interfacetunnel***tunnel-number* • switch(config)# **interfacevlan***vlan-ID* • switch(config)# **interfacemgmt***port*	指定したインターフェイス タイプのコンフィギュレーション モードを開始します。
ステップ 3	次のいずれかのコマンドを入力します。 • switch(config-if)# **ipaccess-group** *access-list* {**in** | **out**} • switch(config-if)# **ipv6 traffic-filter** *access-list* {**in** | **out**}	IPv4 ACL または IPv6 ACL を、指定方向のトラフィックのレイヤ 3 インターフェイスに適用します。各方向にルータ ACL を 1 つ適用できます。
ステップ 4	switch(config-if)# **show running-config aclmgr**	（任意） ACL の設定を表示します。
ステップ 5	switch(config-if)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

IP ACL の作成, （575 ページ）

ポート ACL としての IP ACL の適用

IPv4 または IPv6 ACL は、レイヤ 2 インターフェイス（物理ポートまたはポート チャネル）に適用できます。これらのインターフェイス タイプに適用された ACL は、ポート ACL と見なされます。

はじめる前に

適用する ACL が存在し、目的に応じたトラフィック フィルタリングが設定されていることを確認します。

（注） インターフェイスを **mac packet-classify** で設定する場合は、**mac packet-classify** コマンドをインターフェイス設定から削除するまで、IP ポート ACL をインターフェイスに適用できません。

手順の概要

1. **configure terminal**
2. 次のいずれかのコマンドを入力します。
   - **interfaceethernet***slot*/*port*
   - **interfaceport-channel***channel-number*
3. 次のいずれかのコマンドを入力します。
   - **ipportaccess-group***access-list***in**
   - **ipv6 port traffic-filter***access-list***in**
4. （任意） **show running-config aclmgr**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	次のいずれかのコマンドを入力します。
	• **interfaceethernet***slot*/*port*
	• **interfaceport-channel***channel-number*
	
	例：
	`switch(config)# interface ethernet 2/3`
	`switch(config-if)#`
		指定したインターフェイス タイプのコンフィギュレーション モードを開始します。

ステップ 3	次のいずれかのコマンドを入力します。 • **ipportaccess-group***access-list***in**	IPv4 または IPv6 ACL をインターフェイスまたはポートチャネルに適用します。ポート ACL では、

	コマンドまたはアクション	目的
	• **ipv6 port traffic-filter***access-list***in** 例： `switch(config-if)# ip port access-group acl-l2-marketing-group in`	インバウンドフィルタリングだけがサポートされています。1 つのインターフェイスに 1 つのポート ACL を適用できます。
ステップ 4	**show running-config aclmgr** 例： `switch(config-if)# show running-config aclmgr`	（任意） ACL の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

関連トピック

IP ACL の作成，（575 ページ）
MAC パケット分類のイネーブル化またはディセーブル化，（626 ページ）

IP ACL の VACL としての適用

IP ACL は VACL として適用できます。

関連トピック

VACL の設定，（635 ページ）

ACL TCAM バンク マッピングの設定

ACL TCAM バンクのマッピングを許可するように、デバイスを設定できます。この機能により、TCAM バンクがより予測可能な方法で機能の組み合わせに対応できるようになります。

はじめる前に

デフォルトの VDC に属することを確認します（または **switchto** コマンドを使用します）。

手順の概要

1. **configure terminal**
2. [**no**] **hardware access-list resource feature bank-mapping**
3. **show hardware access-list** {**input** | **output**} {**interface** | **vlan** } **feature-combo***features*
4. （任意） **show system internal access-list feature bank-class map** {**ingress** | **egress**} [**module***module*]
5. **copy running-config startup-config**

手順の詳細

ステップ 1 configure terminal

例：
```
switch# configure terminal
switch(config)#
```
グローバル コンフィギュレーション モードを開始します。

ステップ 2 [no] hardware access-list resource feature bank-mapping

例：
```
switch(config)# hardware access-list resource feature bank-mapping
```
機能グループまたは機能クラスに対する ACL TCAM バンクのマッピングをイネーブルにします。

（注） このコマンドはデフォルトの VDC でのみ使用できますが、すべての VDC に適用されます。

ステップ 3 show hardware access-list {input | output} {interface | vlan } feature-combo*features*

例：
```
switch# show hardware access-list input vlan feature-combo pacl

_____________________________________________________________________________
Feature                      Rslt Type      T0B0      T0B1      T1B0      T1B1
_____________________________________________________________________________
PACL                            Acl          X
QoS                             Qos                    X
```
バンク マッピング マトリックスが表示されます。

ステップ 4 （任意） show system internal access-list feature bank-class map {ingress | egress} [module*module*]

例：
```
switch(config)# show system internal access-list feature bank-class map ingress module 4

Feature Class Definition:
0. CLASS_QOS :
QoS,
1. CLASS_INBAND :
Tunnel Decap, SPM LISP, SPM ERSPAN (termination),
2. CLASS_PACL :
PACL, Netflow,
3. CLASS_DHCP :
DHCP, Netflow, ARP, VACL,
4. CLASS_RACL :
RACL, RACL_STAT, Netflow (SVI), ARP,
```

```
5. CLASS_VACL :
VACL, VACL_STAT, ARP, FEX, Netflow,
6. CLASS_RV_ACL :
RACL, PBR, BFD, ARP, SPM WCCP, VACL, SPM OTV, FEX, CTS implicit Tunnel
```

機能グループとクラスの組み合わせの表を表示します。

ステップ 5 **copy running-config startup-config**

例：

```
switch# copy running-config startup-config
```

実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

フレキシブル ACL TCAM バンク チェーニングの設定

フレキシブル ACL TCAM バンク チェーニング機能を設定するには、ここに示す手順を実行します。

ステップ 1 グローバル コンフィギュレーション モードを開始します。
switch# **configure terminal**

ステップ 2 フレキシブル TCAM バンク チェーニング機能をイネーブルにします。
switch(config)# **hardware access-list resource pooling {vlan-vlan|port-vlan} module***module-number*

ステップ 3 グローバル コンフィギュレーション モードを終了します。
switch(config)# **exit**

ステップ 4 フレキシブル TCAM バンク チェーニング モードを表示します。
switch# **show system internal access-list globals**

ステップ 5 （任意） フレキシブル TCAM バンク マッピング テーブルを表示します。
switch# **show system internal access-list feature bank-chain map {vlan-vlan|port-vlan} {egress | ingress}** [**module***module-number*]

フレキシブル ACL TCAM バンク チェーニングの設定

次の実行コンフィギュレーションでは、モジュール 3 に対して VLAN-VLAN モードでフレキシブル ACL TCAM バンク チェーニング機能を設定する方法を示します。プレースホルダは実際の設定に応じた値に置き換えてください。

```
configure terminal
  hardware access-list resource pooling <vlan-vlan> module <3>
 exit
```

次の例では、TCAM バンク チェーニング モードを確認する方法を示します。

```
switch# show system internal access-list globals
```

```
slot  3
=======
  Atomic Update : ENABLED
  Default ACL   : DENY
  Bank Chaining : VLAN-VLAN
  Seq Feat Model : NO_DENY_ACE_SUPPORT
  This pltfm supports seq feat model
  Bank Class Model : DISABLED
  This pltfm supports bank class model
  Fabric path DNL : DISABLED
  Seq Feat Model : NO_DENY_ACE_SUPPORT
  This pltfm supports seq feat model

  L4 proto CAM extend : DISABLED
  This pltfm supports L4 proto CAM extend
  MPLS Topmost As Pipe Mode : DISABLED
  This pltfm supports mpls topmost as pipe mode
  LOU Threshold Value : 5
```

次の例では、VLAN-VLAN モードのマッピング出力を示します。

```
switch# show system internal access-list feature bank-chain map vlan-vlan egress
_____________________________________________________________________________
Feature                 Rslt Type      T0B0      T0B1      T1B0      T1B1
_____________________________________________________________________________
QoS                         Qos         X         X
RACL                        Acl                             X         X
VACL                        Acl                             X         X
Tunnel Decap                Acl         X         X
Netflow                     Acl                             X         X
Netflow Sampler             Acc         X         X
Rbacl                       Acl         X         X
CTS implicit Tunnel         Acl         X         X
SPM WCCP                    Acl                             X         X
SPM OTV                     Acl         X         X
SPM LISP                    Acl         X         X
SPM ERSPAN (termination)    Acl         X         X
OTV25 DECAP                 Acl         X         X
SPM NVE                     Acl                             X         X
SPM NVE RDT                 Acl                             X         X
SPM ITD                     Acl                             X         X
```

ACL キャプチャのイネーブル化またはディセーブル化

Cisco NX-OS Release 5.2 以降では、デフォルト VDC の ACL キャプチャをイネーブルまたはディセーブルにできます。

はじめる前に

デフォルト VDC にいることを確認します。

手順の概要

1. **configure terminal**
2. **[no] hardware access-list capture**
3. （任意） **show hardware access-list status module***slot*
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**[no] hardware access-list capture** 例： `switch(config)# hardware access-list capture`	すべての VDC の ACL キャプチャをイネーブルまたはディセーブルにします。 （注） ACL キャプチャをイネーブルにすると、警告メッセージが表示され、ACL ロギングが全 VDC に対して無効になっていることを通知します。ACL キャプチャをディセーブルにすると、ACL ロギングはイネーブルになります。
ステップ 3	**show hardware access-list status module***slot* 例： `switch(config)# show hardware access-list status module 2`	（任意） ACL キャプチャの設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

ACL キャプチャ，（559 ページ）
ACL キャプチャ セッションの設定，（591 ページ）
キャプチャ セッション ACE を使用した ACL のインターフェイスへの適用，（593 ページ）
すべての ACL キャプチャ セッションのインターフェイスへの適用，（595 ページ）

ACL キャプチャ セッションの設定

Cisco NX-OS Release 5.2 以降では、ACL キャプチャ セッションを設定できます。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

手順の概要

1. **configure terminal**
2. **monitor session***session***type acl-capture**
3. **destination interface***interface slot*/*port*
4. **no shut**
5. **exit**
6. （任意） **show ip access-lists capture session** *session*
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**monitor session***session***type acl-capture**
	
	例：
	`switch(config)# monitor session 2 type acl-capture`
	`switch(config-acl-capture)#`
		ACL キャプチャ セッションを設定します。*session* 引数の範囲は 1 ～ 48 です。

ステップ 3	**destination interface***interface slot*/*port*
	
	例：
	`switch(config-acl-capture)# destination interface ethernet 2/2`
	`switch#`
		ACL キャプチャ パケットの宛先を設定します。
		（注） 物理インターフェイスだけが宛先に使用できます。ポートチャネルインターフェイス、およびスーパーバイザ インバンド ポートはサポートされません。
		（注） このコマンドを複数回入力して、複数の宛先を追加することができます。

ステップ 4	**no shut** 例： `switch(config-acl-capture)# no shut`	ACL キャプチャ セッションを管理的にアップします。 （注） セッションは、ACL キャプチャがデフォルト VDC でイネーブルになったことをモニタが確認した後にのみ、アップ状態になります。

ステップ 5	**exit**
	
	例：
	`switch(config-acl-capture)# exit`
	`switch(config)#`
		モニタ設定を更新し、ACL キャプチャ コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 6	**show ip access-lists capture session** *session* 例： `switch(config)# show ip access-lists capture session 2`	（任意） ACL のキャプチャ セッションの設定を表示します。
ステップ 7	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

キャプチャ セッション ACE を使用した ACL のインターフェイスへの適用

ACL のアクセス コントロール エントリ（ACE）のキャプチャ セッションをイネーブルにし、インターフェイスに ACL を適用できます。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

手順の概要

1. **configure terminal**
2. **ip access-list***name*
3. **permit***protocol source destination* **capture session** *session*
4. **exit**
5. **interface***interface slot*/*port*
6. **ip access-group***name* **in**
7. **no shut**
8. （任意） **show running-config aclmgr**
9. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**ip access-list***name*
	
	例：
	`switch(config)# ip access-list acl1`
	`switch(config-acl)#`
		アクセス リストを作成します。

ステップ 3	**permit***protocol source destination* **capture session** *session* 例： `switch(config-acl)# permit tcp any any capture session 2`	ACL の ACE に対するキャプチャ セッションをイネーブルにします。*session* 引数の範囲は 1 ～ 16 です。

ステップ 4	**exit**
	
	例：
	`switch(config-acl)# exit`
	`switch(config)#`
		アクセスリストコンフィギュレーションモードを終了します。

ステップ 5	**interface***interface slot*/*port*
	
	例：
	`switch(config)# interface ethernet 7/1`
	`switch(config-if)#`
		ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 6	**ip access-group***name* **in** 例： `switch(config-if)# ip access-group acl1 in`	インターフェイスにキャプチャセッションACEを使用した ACL を適用します。
ステップ 7	**no shut** 例： `switch(config-if)# no shut`	インターフェイスを管理的にアップします。
ステップ 8	**show running-config aclmgr** 例： `switch(config-if)# show running-config aclmgr`	（任意） ACLの設定およびACLが適用されたインターフェイスを表示します。

	コマンドまたはアクション	目的
ステップ 9	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

すべての ACL キャプチャ セッションのインターフェイスへの適用

全 ACL のキャプチャ セッションをイネーブルにし、インターフェイスに ACL を適用できます。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。

手順の概要

1. **configure terminal**
2. **ip access-list***name*
3. **capture session***session*
4. **exit**
5. **interface***interface slot*/*port*
6. **ip access-group***name* **in**
7. **no shut**
8. （任意） **show running-config aclmgr**
9. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**ip access-list***name*
	
	例：
	`switch(config)# ip access-list acl1`
	`switch(config-acl)#`
		アクセス リストを作成します。

	コマンドまたはアクション	目的
ステップ 3	**capture session***session* 例： `switch(config-acl)# capture session 2`	全 ACL のキャプチャ セッションをイネーブルにします。*session* 引数の範囲は 1 ～ 16 です。

ステップ 4	**exit**
	
	例：
	`switch(config-acl)# exit`
	`switch(config)#`
		アクセス リスト コンフィギュレーション モードを終了します。

ステップ 5	**interface***interface slot*/*port*
	
	例：
	`switch(config)# interface ethernet 7/1`
	`switch(config-if)#`
		ポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 6	**ip access-group***name* **in** 例： `switch(config-if)# ip access-group acl1 in`	インターフェイスにキャプチャ セッション設定を使用した ACL を適用します。
ステップ 7	**no shut** 例： `switch(config-if)# no shut`	インターフェイスを管理的にアップします。
ステップ 8	**show running-config aclmgr** 例： `switch(config-if)# show running-config aclmgr`	（任意） ACL の設定および ACL が適用されたインターフェイスを表示します。
ステップ 9	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

IP ACL の設定の確認

IP ACL の設定情報を表示するには、次のいずれかの作業を行います。これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

コマンド	目的
show hardware access-list status module *slot*	ACL キャプチャの設定を表示します。
show ip access-lists[**capture session** *session*]	IPv4 ACL の設定を表示します。
show ipv6 access-lists[**capture session** *session*]	IPv6 ACL の設定を表示します。
show system internal access-list feature bank-class map {**ingress** | **egress**} [**module** *module*]	機能グループとクラスの組み合わせの表を表示します。
show running-config aclmgr [**all**]	IP ACL の設定および IP ACL が適用されるインターフェイスを含めて、ACL の実行コンフィギュレーションを表示します。 （注） Cisco NX-OS Release 5.2 以降では、このコマンドは、実行コンフィギュレーションのユーザ定義 ACL を表示します。**all** オプションを使用すると、実行コンフィギュレーションのデフォルト（CoPP 設定）とユーザ定義による ACL の両方が表示されます。

コマンド	目的
show startup-config aclmgr [**all**]	ACL のスタートアップ コンフィギュレーションを表示します。 （注） Cisco NX-OS Release 5.2 以降では、このコマンドは、スタートアップ コンフィギュレーションのユーザ定義 ACL を表示します。**all** オプションを使用すると、スタートアップ コンフィギュレーションのデフォルト（CoPP 設定）とユーザ定義による ACL の両方が表示されます。

IP ACL の統計情報のモニタリングとクリア

IP ACL の統計情報のモニタまたはクリアを行うには、次の表に示すコマンドのいずれかを使用します。これらのコマンドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

コマンド	目的
show ip access-lists	IPv4 ACL の設定を表示します。IPv4 ACL に **statistics per-entry** コマンドが含まれている場合は、**show ip access-lists** コマンドの出力に、各ルールと一致したパケットの数が含まれます。
show ipv6 access-lists	IPv6 ACL の設定を表示します。IPv6 ACL に **statistics per-entry** コマンドが含まれている場合は、**show ipv6 access-lists** コマンドの出力に、各ルールと一致したパケットの数が含められます。
clear ip access-list counters	すべての IPv4 ACL または特定の IPv4 ACL の統計情報をクリアします。
clear ipv6 access-list counters	すべての IPv6 ACL または特定の IPv6 ACL の統計情報をクリアします。

IP ACL の設定例

acl-01 という名前の IPv4 ACL を作成し、これをポート ACL としてイーサネット インターフェイス 2/1（レイヤ 2 インターフェイス）に適用する例を示します。

```
ip access-list acl-01
  permit ip 192.168.2.0/24 any
interface ethernet 2/1
  ip port access-group acl-01 in
```

acl-120 という名前の IPv6 ACL を作成し、これをルータ ACL としてイーサネット インターフェイス 2/3（レイヤ 3 インターフェイス）に適用する例を示します。

```
ipv6 access-list acl-120
  permit tcp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
  permit udp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
  permit tcp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
  permit udp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
interface ethernet 2/3
  ipv6 traffic-filter acl-120 in
```

次に、single-source という名前の VTY ACL を作成し、それを VTY 回線上の入力 IP トラフィックに対して適用する例を示します。この ACL は、通過するすべての TCP トラフィックを許可し、その他のすべての IP トラフィックをドロップします。

```
ip access-list single-source
  permit tcp 192.168.7.5/24 any
  exit
  line vty
  ip access-class single-source in
  show ip access-lists
```

次に、デフォルト VDC で ACL キャプチャをイネーブルにして、ACL キャプチャ パケットの宛先を設定する例を示します。

```
hardware access-list capture
  monitor session 1 type acl-capture
  destination interface ethernet 2/1
  no shut
  exit
  show ip access-lists capture session 1
```

次に、ACL のアクセス コントロール エントリ（ACE）のキャプチャ セッションをイネーブルにしてから、その ACL をインターフェイスに適用する例を示します。

```
ip access-list acl1
  permit tcp any any capture session 1
  exit
  interface ethernet 1/11
  ip access-group acl1 in
  no shut
  show running-config aclmgr
```

次に、キャプチャ セッションのアクセス コントロール エントリ（ACE）を含む ACL を VLAN に適用する例を示します。

```
vlan access-map acl-vlan-first
  match ip address acl-ipv4-first
  match mac address acl-mac-first
  action foward
  statistics per-entry
```

```
  vlan filter acl-vlan-first vlan-list 1
  show running-config vlan 1
```

次に、ACL 全体のキャプチャ セッションをイネーブルにしてから、その ACL をインターフェイスに適用する例を示します。

```
ip access-list acl2
  capture session 2
  exit
  interface ethernet 7/1
  ip access-group acl1 in
  no shut
  show running-config aclmgr
```

オブジェクト グループの設定

IPv4 ACL および IPv6 ACL のルールに送信元と宛先のアドレスおよびプロトコル ポートを指定する際に、オブジェクト グループを使用できます。

オブジェクト グループに対する Session Manager のサポート

Session Manager はオブジェクト グループの設定をサポートしています。この機能を使用すると、設定セッションを作成し、オブジェクト グループの設定変更を実行コンフィギュレーションにコミットする前に確認できます。Session Manager の詳細については、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*』を参照してください。

IPv4 アドレス オブジェクト グループの作成および変更

IPv4 アドレス グループ オブジェクトの作成および変更を実行できます。

手順の概要

1. **configure terminal**
2. **object-group ip address** *name*
3. 次のいずれかのコマンドを入力します。
   - [*sequence-number*] **host***IPv4-address*
   - [*sequence-number*] *IPv4-addressnetwork-wildcard*
   - [*sequence-number*] *IPv4-address*/*prefix-len*
4. 次のいずれかのコマンドを入力します。
   - **no** [*sequence-number*]
   - **no host***IPv4-address*
   - **no** *IPv4-addressnetwork-wildcard*
   - **no** *IPv4-address*/*prefix-len*
5. （任意） **show object-group***name*
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**object-group ip address** *name*
	
	例：
	`switch(config)# object-group ip address ipv4-addr-group-13`
	`switch(config-ipaddr-ogroup)#`
		IPv4 アドレス オブジェクト グループを作成し、IPv4 アドレス オブジェクト グループ コンフィギュレーション モードを開始します。

ステップ 3	次のいずれかのコマンドを入力します。 • [*sequence-number*] **host***IPv4-address* • [*sequence-number*] *IPv4-addressnetwork-wildcard* • [*sequence-number*] *IPv4-address*/*prefix-len* 例： `switch(config-ipaddr-ogroup)# host 10.99.32.6`	オブジェクト グループのエントリを作成します。作成するエントリごとに、**host** コマンドを使用して単一のホストを指定するか、または**host** コマンドを省略してホストのネットワークを指定します。

	コマンドまたはアクション	目的
ステップ 4	次のいずれかのコマンドを入力します。 • **no** [*sequence-number*] • **no** **host***IPv4-address* • **no** *IPv4-addressnetwork-wildcard* • **no** *IPv4-address*/*prefix-len* 例： `switch(config-ipaddr-ogroup)# no host 10.99.32.6`	オブジェクト グループのエントリを削除します。オブジェクト グループから削除するエントリごとに、**no** 形式の **host** コマンドを使用します。
ステップ 5	**show object-group***name* 例： `switch(config-ipaddr-ogroup)# show object-group ipv4-addr-group-13`	（任意） オブジェクト グループの設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config-ipaddr-ogroup)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

IPv6 アドレス オブジェクト グループの作成および変更

IPv6 アドレス グループ オブジェクトの作成および変更を実行できます。

手順の概要

1. **config t**
2. **object-group ipv6 address***name*
3. 次のいずれかのコマンドを入力します。
   - [*sequence-number*] **host***IPv6-address*
   - [*sequence-number*] *IPv6-address*/*prefix-len*
4. 次のいずれかのコマンドを入力します。
   - **no** *sequence-number*
   - **no host***IPv6-address*
   - **no** *IPv6-address*/*prefix-len*
5. （任意） **show object-group***name*
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**object-group ipv6 address***name*
	
	例：
	`switch(config)# object-group ipv6 address ipv6-addr-group-A7`
	`switch(config-ipv6addr-ogroup)#`
		IPv6 アドレス オブジェクト グループを作成し、IPv6 アドレス オブジェクト グループ コンフィギュレーション モードを開始します。

ステップ 3	次のいずれかのコマンドを入力します。 • [*sequence-number*] **host***IPv6-address* • [*sequence-number*] *IPv6-address*/*prefix-len* 例： `switch(config-ipv6addr-ogroup)# host 2001:db8:0:3ab0::1`	オブジェクト グループのエントリを作成します。作成するエントリごとに、**host** コマンドを使用して単一のホストを指定するか、または**host** コマンドを省略してホストのネットワークを指定します。
ステップ 4	次のいずれかのコマンドを入力します。 • **no** *sequence-number* • **no host***IPv6-address*	オブジェクト グループからエントリを削除します。オブジェクト グループから削除するエントリごとに、**no** 形式の **host** コマンドを使用します。

	コマンドまたはアクション	目的
	• **no** *IPv6-address/prefix-len* 例： `switch(config-ipv6addr-ogroup)# no host 2001:db8:0:3ab0::1`	
ステップ 5	**show object-group***name* 例： `switch(config-ipv6addr-ogroup)# show object-group ipv6-addr-group-A7`	（任意） オブジェクト グループの設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config-ipv6addr-ogroup)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

プロトコル ポート オブジェクト グループの作成および変更

プロトコル ポート オブジェクト グループの作成および変更を実行できます。

手順の概要

1. **configure terminal**
2. **object-group ip port** *name*
3. [*sequence-number*] *operatorport-number* [*port-number*]
4. **no** {*sequence-number* | *operatorport-number* [*port-number*]}
5. （任意） **show object-group***name*
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal switch(config)#`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 2	**object-group ip port** *name*
	
	例：
	`switch(config)# object-group ip port NYC-datacenter-ports`
	`switch(config-port-ogroup)#`
		プロトコル ポート オブジェクト グループを作成し、ポート オブジェクト グループ コンフィギュレーション モードを開始します。

ステップ 3	[*sequence-number*] *operatorport-number* [*port-number*] 例： `switch(config-port-ogroup)# eq 80`	オブジェクト グループのエントリを作成します。作成するエントリごとに、次の演算子コマンドを 1 つ使用します。 • **eq**：指定したポート番号だけに一致します。 • **gt**：指定したポート番号より大きい（等しいものは含まない）ポート番号に一致します。 • **lt**：指定したポート番号より小さい（等しいものは含まない）ポート番号に一致します。 • **neq**：指定したポート番号以外のすべてのポート番号に一致します。 • **range**：指定した 2 つのポート番号と、その間の範囲のポート番号に一致します。 （注） **range** コマンドだけは、2 つの *port-number* 引数を必要とします。
ステップ 4	**no** {*sequence-number* | *operatorport-number* [*port-number*]} 例： `switch(config-port-ogroup)# no eq 80`	オブジェクト グループからエントリを削除します。削除するエントリごとに、該当する演算子コマンドを **no** 形式で使用します。
ステップ 5	**show object-group***name* 例： `switch(config-port-ogroup)# show object-group NYC-datacenter-ports`	（任意） オブジェクト グループの設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config-port-ogroup)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

オブジェクト グループの削除

IPv4 アドレス オブジェクト グループ、IPv6 アドレス オブジェクト グループ、またはプロトコル ポート オブジェクト グループを削除できます。

手順の概要

1. **configure terminal**
2. **no object-group** {**ip address** | **ipv6 address** | **ip port**} *name*
3. （任意） **show object-group**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**no object-group** {**ip address** | **ipv6 address** | **ip port**} *name* 例： `switch(config)# no object-group ip address ipv4-addr-group-A7`	指定したオブジェクト グループを削除します。
ステップ 3	**show object-group** 例： `switch(config)# show object-group`	（任意） すべてのオブジェクト グループを表示します。削除されたオブジェクト グループは表示されません。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

オブジェクト グループの設定の確認

オブジェクト グループの設定情報を表示するには、次の作業のいずれかを行います。

コマンド	目的
show object-group	オブジェクト グループの設定を表示します。
show running-config aclmgr	オブジェクト グループを含めて、ACL の設定を表示します。

これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

時間範囲の設定

時間範囲に対する Session Manager のサポート

Session Manager は時間範囲の設定をサポートしています。この機能を使用すると、設定セッションを作成し、時間範囲の設定変更を実行コンフィギュレーションにコミットする前に確認できます。Session Manager の詳細については、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*』を参照してください。

時間範囲の作成

デバイス上で時間範囲を作成し、これにルールを追加できます。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。異なる VDC では ACL 名を再使用できるので、作業をしている VDC を確認することを推奨します。

手順の概要

1. **configure terminal**
2. **time-range***name*
3. （任意） [*sequence-number*] **periodic***weekdaytime***to** [*weekday*] *time*
4. （任意） [*sequence-number*] **periodic***list-of-weekdaystime***to***time*
5. （任意） [*sequence-number*] **absolute start***timedate* [**end** *time date*]
6. （任意） [*sequence-number*] **absolute** [start *timedate*] **end** *time date*
7. （任意） **show time-range** *name*
8. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**time-range***name*
	
	例：
	`switch(config)# time-range workday-daytime`
	`switch(config-time-range)#`
		時間範囲を作成し、時間範囲コンフィギュレーション モードを開始します。

ステップ 3	[*sequence-number*] **periodic***weekdaytime***to** [*weekday*] *time* 例： `switch(config-time-range)# periodic monday 00:00:00 to friday 23:59:59`	（任意） 指定開始日時と終了日時の間（両端を含める）の 1 日以上の連続した曜日だけ有効になるような定期ルールを作成します。
ステップ 4	[*sequence-number*] **periodic***list-of-weekdaystime***to***time* 例： `switch(config-time-range)# periodic weekdays 06:00:00 to 20:00:00`	（任意） *list-of-weekdays* 引数で指定された曜日の指定開始時刻と終了時刻の間（両端を含む）だけ有効になるような定期ルールを作成します。*list-of-weekdays* 引数の値には次のキーワードも使用できます。 • **daily**：すべての曜日 • **weekdays**：月曜から金曜まで（Monday ～ Friday） • **weekend**：土曜と日曜（Saturday ～ Sunday）
ステップ 5	[*sequence-number*] **absolute start***timedate* [**end** *time date*] 例： `switch(config-time-range)# absolute start 1:00 15 march 2008`	（任意） **start** キーワードの後ろに指定した日時から有効になる絶対ルールを作成します。**end** キーワードを省略すると、そのルールは開始日時を過ぎると常に有効になります。
ステップ 6	[*sequence-number*] **absolute** [start *timedate*] **end** *time date* 例： `switch(config-time-range)# absolute end 23:59:59 31 december 2008`	（任意） **end** キーワードの後ろに指定した日時まで有効になる絶対ルールを作成します。**start** キーワードを省略すると、そのルールは終了日時を過ぎるまで常に有効です。
ステップ 7	**show time-range** *name* 例： `switch(config-time-range)# show time-range workday-daytime`	（任意） 時間範囲の設定を表示します。

	コマンドまたはアクション	目的
ステップ 8	**copy running-config startup-config** 例： `switch(config-time-range)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

時間範囲の変更

既存の時間範囲のルールの追加および削除を実行できます。既存のルールは変更できません。ルールを変更するには、そのルールを削除してから、変更を加えたルールを再作成します。

既存のルールの間に新しいルールを挿入する必要がある場合で、現在のシーケンス番号の空き状況ではすべてを挿入できないときは、**resequence** コマンドを使用してシーケンス番号を再割り当てします。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。異なる VDC では ACL 名を再使用できるので、作業をしている VDC を確認することを推奨します。

手順の概要

1. **configure terminal**
2. **time-range***name*
3. （任意） [*sequence-number*] **periodic***weekdaytime***to** [*weekday*] *time*
4. （任意） [*sequence-number*] **periodic***list-of-weekdaystime***to***time*
5. （任意） [*sequence-number*] **absolutestart***timedate* [**end** *time date*]
6. （任意） [*sequence-number*] **absolute** [**start***timedate*] **end** *time date*
7. （任意） **no** {*sequence-number* | **periodic***arguments ...*| **absolute***arguments...*}
8. （任意） **show time-range** *name*
9. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 2	**time-range***name*
	
	例：
	`switch(config)# time-range workday-daytime`
	`switch(config-time-range)#`
		特定の時間範囲の時間範囲コンフィギュレーションモードを開始します。

ステップ 3	[*sequence-number*] **periodic***weekdaytime***to** [*weekday*] *time* 例： `switch(config-time-range)# periodic monday 00:00:00 to friday 23:59:59`	（任意） 指定開始日時と終了日時の間（両端を含める）の 1 日以上の連続した曜日だけ有効になるような定期ルールを作成します。
ステップ 4	[*sequence-number*] **periodic***list-of-weekdaystime***to***time* 例： `switch(config-time-range)# 100 periodic weekdays 05:00:00 to 22:00:00`	（任意） *list-of-weekdays* 引数で指定された曜日の指定開始時刻と終了時刻の間（両端を含む）だけ有効になるような定期ルールを作成します。*list-of-weekdays* 引数の値には次のキーワードも使用できます。 • **daily**：すべての曜日 • **weekdays**：月曜から金曜まで（Monday ～ Friday） • **weekend**：土曜と日曜（Saturday ～ Sunday）
ステップ 5	[*sequence-number*] **absolutestart***timedate* [**end** *time date*] 例： `switch(config-time-range)# absolute start 1:00 15 march 2008`	（任意） **start** キーワードの後ろに指定した日時から有効になる絶対ルールを作成します。**end** キーワードを省略すると、そのルールは開始日時を過ぎると常に有効になります。
ステップ 6	[*sequence-number*] **absolute** [**start***timedate*] **end** *time date* 例： `switch(config-time-range)# absolute end 23:59:59 31 december 2008`	（任意） **end** キーワードの後ろに指定した日時まで有効になる絶対ルールを作成します。**start** キーワードを省略すると、そのルールは終了日時を過ぎるまで常に有効です。
ステップ 7	**no** {*sequence-number* | **periodic***arguments* ...| **absolute***arguments...*} 例： `switch(config-time-range)# no 80`	（任意） 時間範囲から特定のルールを削除します。
ステップ 8	**show time-range** *name* 例： `switch(config-time-range)# show time-range workday-daytime`	（任意） 時間範囲の設定を表示します。

	コマンドまたはアクション	目的
ステップ 9	**copy running-config startup-config** 例： `switch(config-time-range)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

時間範囲のシーケンス番号の変更，（612 ページ）

時間範囲の削除

デバイスから時間範囲を削除できます。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。異なる VDC では ACL 名を再使用できるので、作業をしている VDC を確認することを推奨します。

その時間範囲が ACL ルールのいずれかに使用されているかどうかを確認します。削除できるのは、ACL ルールに使用されている時間範囲です。ACL ルールに使用されている時間範囲を削除しても、その ACL が適用されているインターフェイスの設定には影響しません。デバイスは削除された時間範囲を使用する ACL ルールを空であると見なします。

手順の概要

1. **configure terminal**
2. **notime-range***name*
3. （任意） **show time-range**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**notime-range***name* 例： `switch(config)# no time-range daily-workhours`	名前を指定した時間範囲を削除します。
ステップ 3	**show time-range** 例： `switch(config-time-range)# show time-range`	（任意） すべての時間範囲の設定を表示します。削除された時間範囲は表示されません。
ステップ 4	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

時間範囲のシーケンス番号の変更

時間範囲のルールに割り当てられているすべてのシーケンス番号を変更できます。

はじめる前に

正しい VDC を使用していることを確認します（または **switchto vdc** コマンドを使用します）。異なる VDC では ACL 名を再使用できるので、作業をしている VDC を確認することを推奨します。

手順の概要

1. **configure terminal**
2. **resequencetime-range** *name starting-sequence-numberincrement*
3. （任意） **show time-range***name*
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 2	**resequencetime-range** *name starting-sequence-numberincrement*
	
	例：
	`switch(config)# resequence time-range daily-workhours 100 10`
	`switch(config)#`
		時間範囲のルールにシーケンス番号を割り当てます。指定した開始シーケンス番号は最初のルールに割り当てられます。後続の各ルールには、直前のルールよりも大きい番号が付けられます。番号の間隔は、指定した増分によって決まります。

ステップ 3	**show time-range***name* 例： `switch(config)# show time-range daily-workhours`	（任意） 時間範囲の設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

時間範囲設定の確認

時間範囲の設定情報を表示するには、次のいずれかの作業を行います。これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

コマンド	目的
show time-range	時間範囲の設定を表示します。
show running-config aclmgr	すべての時間範囲を含めて、ACL の設定を表示します。

フレキシブル ACL TCAM バンク チェーニングのトラブルシューティング

問題：VLAN またはポートで機能の設定が失敗する。

シナリオ：モジュール 2 で、VLAN-VLAN モードで、フレキシブル ACL TCAM バンク チェーニング機能を設定します。宛先 VLAN の QoS 機能を設定します。さらに、ロールベース アクセス コントロール リスト（RBACL）を同じ VLAN で設定する必要があります。この場合に、RBACL 機能の設定が失敗します。

ソリューション：次のように、TCAM バンク マッピング テーブルで、機能の結果タイプが同じ TCAM で重複しているかどうかを確認します。

```
switch# show system internal access-list feature bank-chain map vlan-vlan egress module 2
_____________________________________________________________________________
Feature                 Rslt Type       T0B0       T0B1       T1B0       T1B1
_____________________________________________________________________________
QoS                          Qos          X          X
RACL                         Acl                                X          X
VACL                         Acl                                X          X
Tunnel Decap                 Acl          X          X
Netflow                      Acl                                X          X
Netflow Sampler              Acc          X          X
Rbacl                        Acl          X          X
CTS implicit Tunnel          Acl          X          X
SPM WCCP                     Acl                                X          X
SPM OTV                      Acl          X          X
SPM LISP                     Acl          X          X
SPM ERSPAN (termination)     Acl          X          X
OTV25 DECAP                  Acl          X          X
SPM NVE                      Acl                                X          X
SPM NVE RDT                  Acl                                X          X
SPM ITD                      Acl                                X          X
```

異なる結果タイプを持つ機能が同じ TCAM で重複しているかどうかを確認します。このシナリオでは、QoS 機能と RBACL 機能の異なる結果タイプが同じ TCAM（T0B0 と T0B1）に表示されています。同じ TCAM バンクに表示されていても、結果タイプが異なる場合、同時に設定することはできません。

IP ACL に関する追加情報

関連資料

関連項目	マニュアル タイトル
IP ACL コマンド：完全なコマンド構文、コマンドモード、コマンド履歴、デフォルト値、使用上の注意、例	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』
オブジェクト グループのコマンド：完全なコマンド構文、コマンドモード、コマンド履歴、デフォルト値、使用上の注意、例	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』
時間範囲のコマンド：完全なコマンド構文、コマンドモード、コマンド履歴、デフォルト値、使用上の注意、例	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』
SNMP	『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

IP ACL の機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 *34*： *IP ACL* の機能の履歴

機能名	リリース	機能情報
M3 モジュールでの ACL の設定	7.3(0)DX(1)	M3 モジュールのサポートが導入されました。
フレキシブル ACL TCAM バンク チェーニング	7.3(0)D1(1)	フレキシブル ACL TCAM バンク チェーニング機能のサポートが追加されました。
ACL TCAM バンク マッピング	6.2(10)	バンク マッピング マトリクスを表示するコマンドが追加されました。
IP ACL	6.2(2)	ACL TCAM バンク マッピングのサポートが追加されました。
IP ACL	6.1(1)	M2 シリーズ モジュールが更新されました。
IP ACL	6.0(1)	F2 シリーズ モジュールが更新されました。
FCoE ACL	5.2(1)	F1 シリーズ モジュールに FCoE ACL のサポートが追加されました。
IP ACL	5.2(1)	M1 シリーズ モジュールに ACL キャプチャのサポートが追加されました。

機能名	リリース	機能情報
IP ACL	5.2(1)	実行コンフィギュレーションとスタートアップ コンフィギュレーションでユーザ設定 ACL だけを表示する（およびデフォルトの CoPP 設定 ACL を表示しない）ように、**show running-config aclmgr** コマンドと **show startup-config aclmgr** コマンドが変更されました。
VTY ACL	5.1(1)	VTY 回線で受信したトラフィックに対するアクセス コントロールのサポートが追加されました。
IP ACL	5.0(2)	スケーラブルなサービス ライセンスがインストールされており、XL ラインカードを使用している場合、最大 128K の ACL エントリがサポートされるようになりました。
ACL のロギング	4.2(3)	ACL 処理用にスーパーバイザ モジュールに送信されたパケットのロギングのサポートが追加されました。
IP ACL	4.2(1)	レイヤ 2 インターフェイスでの MAC パケット分類のサポートが追加されました。

第 16 章

MAC ACL の設定

この章では、Cisco NX-OS デバイスの MAC アクセス コントロール リスト（ACL）を設定する手順について説明します。

この章の内容は、次のとおりです。

- 機能情報の確認，617 ページ
- MAC ACL の概要，618 ページ
- MAC ACL のライセンス要件，618 ページ
- MAC ACL の前提条件，619 ページ
- MAC ACL の注意事項と制約事項，619 ページ
- MAC ACL のデフォルト設定，619 ページ
- MAC ACL の設定，620 ページ
- MAC ACL の設定の確認，628 ページ
- MAC ACL の統計情報のモニタリングとクリア，628 ページ
- MAC ACL の設定例，629 ページ
- MAC ACL に関する追加情報，629 ページ
- MAC ACL の機能の履歴，630 ページ

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

MAC ACL の概要

MAC ACL は、パケットのレイヤ 2 ヘッダーを使用してトラフィックをフィルタリングする ACL です。バーチャライゼーションのサポートなど、MAC ACL の基本的な機能の多くは IP ACL と共通です。

関連トピック

ACL の概要, （550 ページ）

MAC パケット分類

MAC パケット分類により、レイヤ 2 インターフェイス上の MAC ACL を、IP トラフィックなどインターフェイスに入るすべてのトラフィックに適用するか、非 IP トラフィックだけに適用するかを制御できます。

MAC パケット分類の状態	インターフェイスでの効果
イネーブル	• インターフェイス上の MAC ACL は、IP トラフィックなどインターフェイスに入るすべてのトラフィックに適用されます。 • IP ポート ACL をインターフェイスで適用できません。
ディセーブル	• インターフェイス上の MAC ACL は、インターフェイスに入る非 IP トラフィックだけに適用されます。 • インターフェイスで IP ポート ACL を適用することができます。

関連トピック

MAC パケット分類のイネーブル化またはディセーブル化, （626 ページ）

MAC ACL のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	MAC ACL にはライセンスは必要ありません。ただし、XL ラインカードを使用して最大 128K の ACL エントリをサポートするには、スケーラブルなサービス ライセンスをインストールする必要があります。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

MAC ACL の前提条件

MAC ACL を設定するための前提条件はありません。

MAC ACL の注意事項と制約事項

MAC ACL の設定に関する注意事項と制約事項は次のとおりです。

- MAC ACL は入トラフィックだけに適用されます。
- DHCP スヌーピング機能がイネーブルのときには、ACL の統計情報はサポートされません。

MAC ACL のデフォルト設定

次の表に、MAC ACL パラメータのデフォルト設定を示します。

表 *35*：*MAC ACL* のデフォルト パラメータ

パラメータ	デフォルト
MAC ACL	デフォルトでは MAC ACL は存在しません。
ACL ルール	すべての ACL に暗黙のルールが適用されます。

MAC ACL の設定

MAC ACL の作成

MAC ACL を作成し、これにルールを追加できます。

手順の概要

1. **configure terminal**
2. **macaccess-list***name*
3. {**permit** | **deny**} *sourcedestination protocol*
4. （任意） **statistics per-entry**
5. （任意） **show mac access-lists***name*
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**macaccess-list***name*
	
	例：
	`switch(config)# mac access-list acl-mac-01`
	`switch(config-mac-acl)#`
		MAC ACL を作成して、ACL コンフィギュレーション モードを開始します。

ステップ 3	{**permit**	**deny**} *sourcedestination protocol* 例： `switch(config-mac-acl)# permit 00c0.4f00.0000 0000.00ff.ffff any`	MAC ACL 内にルールを作成します。 **permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。
ステップ 4	**statistics per-entry** 例： `switch(config-mac-acl)# statistics per-entry`	（任意） その ACL のルールと一致するパケットのグローバル統計をデバイスが維持するように設定します。

	コマンドまたはアクション	目的
ステップ 5	**show mac access-lists***name* 例： `switch(config-mac-acl)# show mac access-lists acl-mac-01`	（任意） MAC ACL の設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config-mac-acl)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

MAC ACL の変更

MAC ACL をデバイスから削除できます。

はじめる前に

MAC ACL が設定されているインターフェイスを探すには、summary キーワードを指定して **show mac access-lists** コマンドを使用します。

手順の概要

1. **configure terminal**
2. **macaccess-list***name*
3. （任意） [*sequence-number*] {**permit** | **deny**} *sourcedestination protocol*
4. （任意） **no** {*sequence-number* | {**permit** | **deny**} *sourcedestination protocol*}
5. （任意） [**no**] **statistics per-entry**
6. （任意） **show mac access-lists***name*
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 2	**macaccess-list***name*
	
	例：
	`switch(config)# mac access-list acl-mac-01`
	`switch(config-mac-acl)#`
		名前で指定した ACL の ACL コンフィギュレーション モードを開始します。

ステップ 3	[*sequence-number*] {**permit** | **deny**} *sourcedestination protocol* 例： `switch(config-mac-acl)# 100 permit mac 00c0.4f00.00 0000.00ff.ffff any`	（任意） MAC ACL 内にルールを作成します。シーケンス番号を指定すると、ACL 内のルール挿入位置を指定できます。シーケンス番号を指定しないと、ルールは ACL の末尾に追加されます。 **permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。
ステップ 4	**no** {*sequence-number* | {**permit** | **deny**} *sourcedestination protocol*} 例： `switch(config-mac-acl)# no 80`	（任意） 指定したルールを MAC ACL から削除します。 **permit** コマンドと **deny** コマンドには、トラフィックを識別するための多くの方法が用意されています。詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。
ステップ 5	[**no**] **statistics per-entry** 例： `switch(config-mac-acl)# statistics per-entry`	（任意） その ACL のルールと一致するパケットのグローバル統計をデバイスが維持するように設定します。 **no** オプションを使用すると、デバイスはその ACL のグローバル統計の維持を停止します。
ステップ 6	**show mac access-lists***name* 例： `switch(config-mac-acl)# show mac access-lists acl-mac-01`	（任意） MAC ACL の設定を表示します。
ステップ 7	**copy running-config startup-config** 例： `switch(config-mac-acl)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

MAC ACL 内のシーケンス番号の変更

MAC ACL 内のルールに付けられたすべてのシーケンス番号を変更できます。ACL にルールを挿入する必要がある場合で、シーケンス番号が不足しているときは、再割り当てすると便利です。

手順の概要

1. **configure terminal**
2. **resequence mac access-list** *name starting-sequence-numberincrement*
3. （任意） **show mac access-lists***name*
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**resequence mac access-list** *name starting-sequence-numberincrement* 例： `switch(config)# resequence mac access-list acl-mac-01 100 10`	ACL 内に記述されているルールにシーケンス番号を付けます。starting-sequence number に指定したシーケンス番号が最初のルールに付けられます。後続の各ルールには、直前のルールよりも大きい番号が付けられます。番号の間隔は、指定した増分によって決まります。
ステップ 3	**show mac access-lists***name* 例： `switch(config)# show mac access-lists acl-mac-01`	（任意） MAC ACL の設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

MAC ACL の削除

MAC ACL をデバイスから削除できます。

手順の概要

1. **configure terminal**
2. **nomacaccess-list***name*
3. （任意） **show mac access-lists** *name* **summary**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**nomacaccess-list***name*
	
	例：
	`switch(config)# no mac access-list acl-mac-01`
	`switch(config)#`
		名前で指定した MAC ACL を実行コンフィギュレーションから削除します。

ステップ 3	**show mac access-lists** *name* **summary** 例： `switch(config)# show mac access-lists acl-mac-01 summary`	（任意） MAC ACL の設定を表示します。ACL がインターフェイスに引き続き適用されている場合は、インターフェイスが表示されます。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ポート ACL としての MAC ACL の適用

MAC ACL をポート ACL として、次のいずれかのインターフェイス タイプに適用できます。

- レイヤ 2 またはレイヤ 3 のイーサネット インターフェイス
- レイヤ 2 またはレイヤ 3 のポート チャネル インターフェイス

はじめる前に

適用する ACL が存在し、必要な方法でトラフィックをフィルタリングするように設定されていることを確認します。

手順の概要

1. **configure terminal**
2. 次のいずれかのコマンドを入力します。
   - **interfaceethernet***slot*/*port*
   - **interfaceport-channel***channel-number*
3. **mac port access-group***access-list*
4. （任意） **show running-config aclmgr**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	次のいずれかのコマンドを入力します。
	• **interfaceethernet***slot*/*port*
	• **interfaceport-channel***channel-number*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
	
	例：
	`switch(config)# interface port-channel 5`
	`switch(config-if)#`
		• レイヤ 2 またはレイヤ 3 のインターフェイス コンフィギュレーション モードを開始します。
		• レイヤ 2 またはレイヤ 3 のポート チャネル インターフェイスのインターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**mac port access-group***access-list* 例： `switch(config-if)# mac port access-group acl-01`	MAC ACL をインターフェイスに適用します。
ステップ 4	**show running-config aclmgr** 例： `switch(config-if)# show running-config aclmgr`	（任意） ACL の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

MAC ACL の VACL としての適用

MAC ACL を VACL として適用できます。

関連トピック

VACL の設定, （635 ページ）

MAC パケット分類のイネーブル化またはディセーブル化

レイヤ 2 インターフェイスに対して MAC パケット分類をイネーブルまたはディセーブルに設定できます。

はじめる前に

インターフェイスを、レイヤ 2 インターフェイスとして設定する必要があります。

（注） インターフェイスが **ip port access-group** コマンドまたは **ipv6 port traffic-filter** コマンドを使用して設定されている場合は、インターフェイス コンフィギュレーションから **ip port access-group** コマンドおよび **ipv6 port traffic-filter** コマンドを削除しない限り、MAC パケット分類をイネーブルにできません。

手順の概要

1. **configure terminal**
2. 次のいずれかのコマンドを入力します。
   - **interfaceethernet***slot*/*port*
   - **interfaceport-channel***channel-number*
3. **[no] mac packet-classify**
4. （任意） 次のいずれかのコマンドを入力します。
   - **show running-config interface ethernet***slot*/*port*
   - **show running-config interfaceport-channel***channel-number*
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	次のいずれかのコマンドを入力します。
	• **interfaceethernet***slot*/*port*
	• **interfaceport-channel***channel-number*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
	
	例：
	`switch(config)# interface port-channel 5`
	`switch(config-if)#`
		• イーサネット インターフェイスのインターフェイス コンフィギュレーション モードを開始します。
		• ポート チャネル インターフェイスのインターフェイス コンフィギュレーション モードを開始します。

ステップ 3	[**no**] **mac packet-classify** 例： `switch(config-if)# mac packet-classify`	インターフェイスのMACパケット分類をイネーブルにします。**no** オプションを使用すると、インターフェイスのMACパケット分類がディセーブルになります。

ステップ 4	次のいずれかのコマンドを入力します。
	• **show running-config interface ethernet***slot*/*port*
	• **show running-config interfaceport-channel***channel-number*
	
	例：
	`switch(config-if)# show running-config interface ethernet 2/1`
	
	例：
	`switch(config-if)# show running-config interface port-channel 5`
		（任意）
		• イーサネット インターフェイスの実行コンフィギュレーションを表示します。
		• ポート チャネル インターフェイスの実行コンフィギュレーションを表示します。

ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

MAC パケット分類, （618 ページ）

MAC ACL の設定の確認

MAC ACL の設定情報を表示するには、次のいずれかの作業を実行します。これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

コマンド	目的
show mac access-lists	MAC ACL の設定を表示します。
show running-config aclmgr[**all**]	MAC ACL および MAC ACL が適用されるインターフェイスを含めて、ACL の設定を表示します。 （注） Cisco NX-OS Release 5.2 以降では、このコマンドは、実行コンフィギュレーションのユーザ定義 ACL を表示します。**all** オプションを使用すると、実行コンフィギュレーションのデフォルト（CoPP 設定）とユーザ定義による ACL の両方が表示されます。
show startup-config aclmgr [**all**]	ACL のスタートアップ コンフィギュレーションを表示します。 （注） Cisco NX-OS Release 5.2 以降では、このコマンドは、スタートアップ コンフィギュレーションのユーザ定義ACL を表示します。**all** オプションを使用すると、スタートアップコンフィギュレーションのデフォルト（CoPP 設定）とユーザ定義による ACL の両方が表示されます。

MAC ACL の統計情報のモニタリングとクリア

MAC ACL に関する統計情報（各ルールに一致したパケットの数など）をモニタするには、**show mac access-lists** コマンドを使用します。

MAC ACL の統計情報のモニタまたはクリアを行うには、次の表に示すコマンドのいずれかを使用します。これらのコマンドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

コマンド	目的
show mac access-lists	MAC ACL の設定を表示します。MAC ACL に statistics per-entry コマンドが含まれている場合は、**show mac access-lists** コマンドの出力に、各ルールと一致したパケットの数が含まれます。
clear mac access-list counters	すべての MAC ACL、または特定の MAC ACL の統計情報を消去します。

MAC ACL の設定例

次に、acl-mac-01 という名前の MAC ACL を作成し、これをイーサネット インターフェイス 2/1（レイヤ 2 インターフェイス）に適用する例を示します。

```
mac access-list acl-mac-01
  permit 00c0.4f00.0000 0000.00ff.ffff any
interface ethernet 2/1
  mac port access-group acl-mac-01
```

MAC ACL に関する追加情報

関連資料

関連項目	マニュアル タイトル
MAC ACL コマンド：完全なコマンド構文、コマンドモード、コマンド履歴、デフォルト値、使用上の注意、例	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MAC ACL の機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 *36*：*MAC ACL* の機能の履歴

機能名	リリース	機能情報
MAC ACL	6.1(1)	M2 シリーズ モジュールが更新されました。
MAC ACL	6.0(1)	F2 シリーズ モジュールが更新されました。
MAC ACL	5.2(1)	実行コンフィギュレーションとスタートアップ コンフィギュレーションでユーザ設定 ACL だけを表示する（およびデフォルトの CoPP 設定 ACL を表示しない）ように、**show running-config aclmgr** コマンドと **show startup-config aclmgr** コマンドが変更されました。
MAC ACL	5.0(2)	スケーラブルなサービス ライセンスがインストールされており、XL ライン カードを使用している場合、最大 128,000 の ACL エントリがサポートされるようになりました。
MAC ACL	4.2(1)	MAC パケット分類がサポートされるようになりました。

第 17 章

VLAN ACL の設定

この章では、Cisco NX-OS デバイスの VLAN ACL（アクセス リスト）の設定方法を説明します。この章は、次の項で構成されています。

- 機能情報の確認，631 ページ
- VLAN ACL の概要，632 ページ
- VACL のライセンス要件，633 ページ
- VACL の前提条件，634 ページ
- VACL の注意事項と制約事項，634 ページ
- VACL のデフォルト設定，635 ページ
- VACL の設定，635 ページ
- VACL 設定の確認，640 ページ
- VACL 統計情報のモニタリングとクリア，641 ページ
- VACL の設定例，642 ページ
- VACL に関する追加情報，642 ページ
- VLAN ACL の機能の履歴，643 ページ

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

VLAN ACL の概要

VLAN ACL（VACL）は、IP ACL または MAC ACL の適用例の 1 つです。VACL を設定し、VLAN との間でルーティングされるかまたは VLAN 内でブリッジングされるすべてのパケットに適用できます。VACL は、セキュリティ パケット フィルタリングおよび特定の物理インターフェイスへのトラフィックのリダイレクトだけを目的としたものです。VACL は方向（入力または出力）で定義されることはありません。

関連トピック

ACL の概要，（550 ページ）

VLAN アクセス マップとエントリ

VACL は、アクセス マップを使用して、1 つまたは複数のマップ エントリを順序化したリストを収容します。各マップ エントリは、IP ACL または MAC ACL を処理に関連付けます。各エントリにはシーケンス番号が付き、これに基づいてエントリの優先度を管理できます。

デバイスがパケットに VACL を適用する際、パケットを許可する ACL を含む最初のアクセスマップ エントリで設定されている処理を適用します。

VACL とアクション

アクセス マップ コンフィギュレーション モードでは、**action** コマンドを使用して、次のいずれかのアクションを指定します。

フォワード

スイッチの通常の動作によって決定された宛先にトラフィックを送信します。

リダイレクト

1 つまたは複数の指定インターフェイスにトラフィックをリダイレクトします。

ドロップ

トラフィックをドロップします。ドロップを処理として指定する場合、ドロップされたパケットのログをデバイスが記録するよう指定することもできます。

VACL の統計情報

VACL の各ルールのグローバル統計が維持されます。VACL を複数の VLAN に適用した場合、保持されるルール統計情報は、その VACL が適用されている各インターフェイス上で一致（ヒット）したパケットの総数になります。

（注） インターフェイスレベルの VACL 統計はサポートされていません。

設定する VLAN アクセス マップごとに、その VACL の統計情報を維持するかどうかを指定できます。この機能を使用すると、VACL によってフィルタリングされたトラフィックのモニタが必要かどうかに応じて、あるいは VLAN アクセスマップの設定のトラブルシューティングが必要かどうかに応じて、VACL 統計をオンまたはオフにできます。

関連トピック

VACL 統計情報のモニタリングとクリア, （641 ページ）

VACL に対する Session Manager のサポート

Session Manager は VACL の設定をサポートしています。この機能を使用すると、ACL の設定を調べて、その設定に必要とされるリソースが利用可能であるかどうかを、リソースを実行コンフィギュレーションにコミットする前に確認できます。Session Manager の詳細については、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*』を参照してください。

VACL のバーチャライゼーション サポート

仮想デバイス コンテキスト（VDC）で使用される VACL には、次の事項が適用されます。

- ACL は各 VDC に固有です。ある VDC に作成した ACL は別の VDC に使用できません。
- ACL が複数の VDC に共有されることはないので、ACL 名は他の VDC に再利用できます。
- デバイスは、ACL やルールを VDC 単位では制限しません。

VACL のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	VACL にはライセンスは必要ありません。ただし、XL ラインカードを使用して最大 128,000 の ACL エントリをサポートするには、スケーラブルなサービス ライセンスをインストールする必要があります。 ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

VACL の前提条件

VACL の前提条件は次のとおりです。

- VACL に使用する IP ACL または MAC ACL が存在し、必要な方法でトラフィックをフィルタリングするように設定されていることを確認します。

VACL の注意事項と制約事項

VACL の設定に関する注意事項は次のとおりです。

- ACL の設定には Session Manager を使用することを推奨します。この機能を使用すると、ACL の設定を調べて、その設定に必要とされるリソースが利用可能であるかどうかを、リソースを実行コンフィギュレーションにコミットする前に確認できます。Session Manager の詳細については、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*』を参照してください。
- DHCP スヌーピング機能がイネーブルのときには、ACL の統計情報はサポートされません。
- サポートされる VACL エントリの最大数は、XL ラインカードを使用しないデバイスで 64,000、XL ラインカードを使用するデバイスで 128,000 です。
- XL 以外のラインカードに適用する ACL エントリが多すぎると、設定が拒否されます。
- F1 シリーズ モジュールの各転送エンジンは 1000 の入力 ACL エントリをサポートします。また、984 のエントリがユーザ設定に使用できます。F1 シリーズ モジュール用の VACL エントリの総数は 1000 ～ 16,000 です。転送エンジンに応じてポリシーが適用されます。
- F1 シリーズ モジュール内の 16 の各転送エンジンは、複数の ACL にわたる最大 250 の IPv6 アドレスをサポートしています。
- F1 シリーズ モジュールには、ACL ロギングをサポートしていません。

- F1 シリーズ モジュールはバンク チェーニングをサポートしていません。
- 各 VACL は、F1 シリーズ モジュールでの最大 6 つの異なるレイヤ 4 動作をサポートできます。
- F1 シリーズ モジュールの同じポートの複数の VLAN（たとえば、VLAN 10、20）上で同じ ACL が適用される場合は、複数回（この場合は、VLAN 10 上と VLAN 20 上で）プログラミングされます。
- F2 シリーズ モジュールの 12 の転送エンジンごとに、総数 16,000 の TCAM エントリが 2 つのバンクに対して均等に分割されます。デフォルトの 168 エントリが予約されます。各転送エンジンは、512 の IPv6 圧縮 TCAM エントリを持ちます。
- SPAN 宛先ポートへの VACL リダイレクトはサポートされません。
- F2 シリーズ、M1 シリーズ、および M2 シリーズ モジュールのみがシーケンス中の拒否 ACE をサポートします。
- 拒否 ACE サポートの統計は、次のシーケンス ベース機能の終了シーケンスでのみサポートされます：VACL、ポリシーベース ルーティング（PBR）、および Quality Of Service（QoS）。

VACL のデフォルト設定

次の表に、VACL パラメータのデフォルト設定値を示します。

表 *37*：*VACL* のデフォルト パラメータ

パラメータ	デフォルト
VACL	デフォルトでは IP ACL は存在しません。
ACL ルール	すべての ACL に暗黙のルールが適用されます。
拒否 ACE サポート	ディセーブル

VACL の設定

VACL の作成または VACL エントリの追加

VACL エントリを新規作成したり、既存の VACL にエントリを追加できます。どちらの場合も、作成した VACL エントリが、1 つまたは複数の ACL を一致トラフィックに適用される処理と関連付ける VLAN アクセス マップ エントリとなります。

はじめる前に

VACL に使用する ACL が存在し、目的に応じたトラフィック フィルタリングが設定されていることを確認します。

手順の概要

1. **configure terminal**
2. **vlan access-map** *map-name* [*sequence-number*]
3. 次のいずれかのコマンドを入力します。
   - **match** {**ip** | **ipv6**} **address***ip-access-list*
   - **matchmacaddress***mac-access-list*
4. **action** {**drop** | **forward** | **redirect**}
5. （任意） **[no] statistics per-entry**
6. （任意） **show running-config aclmgr**
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**vlan access-map** *map-name* [*sequence-number*]
	
	例：
	`switch(config)# vlan access-map acl-mac-map`
	`switch(config-access-map)#`
		指定した VLAN アクセス マップの VLAN アクセス マップ コンフィギュレーション モードを開始します。VLAN アクセス マップが存在しない場合は、デバイスによって作成されます。
		シーケンス番号を指定しなかった場合、デバイスによって新しいエントリが作成され、このシーケンス番号はアクセスマップの最後のシーケンス番号よりも 10 大きい番号となります。

ステップ 3	次のいずれかのコマンドを入力します。 • **match** {**ip**	**ipv6**} **address***ip-access-list* • **matchmacaddress***mac-access-list* 例： `switch(config-access-map)# match mac address acl-ip-lab`	アクセス マップ エントリに ACL を指定します。

	コマンドまたはアクション	目的
	例： `switch(config-access-map)# match mac address acl-mac-01`	
ステップ 4	**action** {**drop** | **forward** | **redirect**} 例： `switch(config-access-map)# action forward`	ACL に一致したトラフィックにデバイスが適用する処理を指定します。 **action** コマンドはさまざまなオプションをサポートしています。詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。
ステップ 5	[**no**] **statistics per-entry** 例： `switch(config-access-map)# statistics per-entry`	（任意） その VACL のルールと一致するパケットのグローバル統計をデバイスが維持するように設定します。 **no** オプションを使用すると、デバイスはその VACL のグローバル統計の維持を停止します。
ステップ 6	**show running-config aclmgr** 例： `switch(config-access-map)# show running-config aclmgr`	（任意） ACL の設定を表示します。
ステップ 7	**copy running-config startup-config** 例： `switch(config-access-map)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

VACL または VACL エントリの削除

VACL を削除できます。これにより、VLAN アクセス マップも削除されます。

また、VACL から単一の VLAN アクセス マップ エントリを削除することもできます。

はじめる前に

その VACL が VLAN に適用されているかどうかを確認します。削除できるのは、現在適用されている VACL です。VACL を削除しても、その VACL が適用されていた VLAN の設定は影響を受けません。デバイスは削除された VACL を空であると見なします。

手順の概要

1. **configure terminal**
2. **no vlan access-map** *map-name* [*sequence-number*]
3. （任意） **show running-config aclmgr**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**no vlan access-map** *map-name* [*sequence-number*] 例： `switch(config)# no vlan access-map acl-mac-map 10`	指定したアクセス マップの VLAN アクセス マップの設定を削除します。*sequence-number* 引数を指定して、VACL に複数のエントリが含まれる場合、このコマンドにより指定したエントリだけが削除されます。
ステップ 3	**show running-config aclmgr** 例： `switch(config)# show running-config aclmgr`	（任意） ACL の設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

VACL の VLAN への適用

VACL を VLAN に適用できます。

はじめる前に

VACL を適用する際には、その VACL が存在し、目的に応じたトラフィック フィルタリングが設定されていることを確認します。

手順の概要

1. **configure terminal**
2. [**no**] **vlan filter** *map-name* **vlan-list** *list*
3. （任意） **show running-config aclmgr**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **vlan filter** *map-name* **vlan-list** *list*
	
	例：
	`switch(config)# vlan filter acl-mac-map vlan-list 1-20,26-30`
	`switch(config)#`
		指定したリストによって、VACL を VLAN に適用します。**no** を使用すると、VACL の適用が解除されます。

ステップ 3	**show running-config aclmgr** 例： `switch(config)# show running-config aclmgr`	（任意） ACL の設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

拒否 ACE サポートの設定

シーケンス ベースの機能である VACL、ポリシー ベース ルーティング（PBR）、および QoS について、シーケンス内の拒否アクセス コントロール エントリ（ACE）をサポートするようにデバイスを設定できます。拒否 ACE がイネーブルの場合、class-map-acl 内の **deny** ACE（deny キーワードをともなった ACL ルール）に一致するトラフィックは、permit ACE にヒットするまで、後に続く class-map-acl と再帰的に照合されます。

はじめる前に

デフォルトまたは管理者 VDC にいることを確認します。

手順の概要

1. **configure terminal**
2. [**no**] **hardware access-list allow deny ace**
3. （任意） **show running-config aclmgr**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **hardware access-list allow deny ace** 例： `switch(config)# hardware access-list allow deny ace`	シーケンス中の拒否 ACE サポートをイネーブルにします。
ステップ 3	**show running-config aclmgr** 例： `switch(config)# show running-config aclmgr`	（任意） ACL の設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

VACL 設定の確認

VACL 設定情報を表示するには、次の作業のいずれかを行います。これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

コマンド	目的
show running-config aclmgr[**all**]	VACL-related の設定も含めて、ACL の設定を表示します。 （注） Cisco NX-OS Release 5.2 以降では、このコマンドは、実行コンフィギュレーションのユーザ定義 ACL を表示します。**all** オプションを使用すると、実行コンフィギュレーションのデフォルト（CoPP 設定）とユーザ定義による ACL の両方が表示されます。
show startup-config aclmgr [**all**]	ACL のスタートアップ コンフィギュレーションを表示します。 （注） Cisco NX-OS Release 5.2 以降では、このコマンドは、スタートアップ コンフィギュレーションのユーザ定義ACLを表示します。**all** オプションを使用すると、スタートアップコンフィギュレーションのデフォルト（CoPP 設定）とユーザ定義による ACL の両方が表示されます。
show vlan filter	VLAN に適用されている VACL の情報を表示します。
show vlan access-map	VLANアクセスマップに関する情報を表示します。

VACL 統計情報のモニタリングとクリア

VACL の統計情報をモニタまたはクリアを行うには、次の表に示すコマンドのいずれかを使用します。これらのコマンドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

コマンド	目的
show vlan access-list	VACL の設定を表示します。VLAN アクセスマップに **statistics per-entry** コマンドが含まれている場合は、**show vlan access-list** コマンドの出力に、各ルールと一致したパケットの数が含まれます。

コマンド	目的
clear vlan access-list counters	すべての VACL、または特定の VACL の統計情報を消去します。

VACL の設定例

次の例では、acl-mac-01 という名前の MAC ACL で許可されたトラフィックを転送する VACL を設定し、その VACL を VLAN 50 ～ 82 に適用します。

```
conf t
vlan access-map acl-mac-map
  match mac address acl-mac-01
  action forward
vlan filter acl-mac-map vlan-list 50-82
```

VACL に関する追加情報

関連資料

関連項目	マニュアル タイトル
VACL のコマンド：完全なコマンド構文、コマンドモード、コマンド履歴、デフォルト値、使用上の注意、例	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』
ポリシー ベース ルーティング (PBR) 設定	『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』
QoS の設定	『*Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

VLAN ACL の機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 *38*：*VLAN ACL* の機能の履歴

機能名	リリース	機能情報
VLAN ACL	6.1(3)	シーケンス中の拒否 ACE に対するサポートが追加されました。
VLAN ACL	6.0(1)	F2 シリーズ モジュールが更新されました。
VLAN ACL	5.2(1)	実行コンフィギュレーションとスタートアップ コンフィギュレーションでユーザ設定 ACL だけを表示する（およびデフォルトの CoPP 設定 ACL を表示しない）ように、**show running-config aclmgr** コマンドと **show startup-config aclmgr** コマンドが変更されました。
VLAN ACL	5.1(1)	Release 5.0 以降、変更はありません。
VLAN ACL	5.0(2)	スケーラブルなサービス ライセンスがインストールされており、XL ライン カードを使用している場合、最大 128,000 の ACL エントリがサポートされるようになりました。
VLAN アクセス マップ	4.2(1)	リリース 4.1 からの変更はありません。

第 18 章

ポート セキュリティの設定

この章では、Cisco NX-OS デバイスにポート セキュリティを設定する手順について説明します。この章は、次の項で構成されています。

- 機能情報の確認，645 ページ
- ポート セキュリティの概要，646 ページ
- ポート セキュリティのライセンス要件，656 ページ
- ポート セキュリティの前提条件，657 ページ
- ポート セキュリティのデフォルト設定，657 ページ
- ポート セキュリティの注意事項と制約事項，658 ページ
- ポート セキュリティの設定，658 ページ
- ポート セキュリティの設定の確認，673 ページ
- セキュア MAC アドレスの表示，673 ページ
- ポート セキュリティの設定例，673 ページ
- ポート セキュリティに関する追加情報，674 ページ
- ポート セキュリティの機能の履歴，674 ページ

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

ポート セキュリティの概要

ポート セキュリティを使用すると、限定された MAC アドレス セットからの着信トラフィックだけを許可するようにレイヤ 2 物理インターフェイスおよびレイヤ 2 ポート チャネル インターフェイスを設定できます。この限定セットの MAC アドレスをセキュア MAC アドレスといいます。さらに、デバイスは、同じ VLAN 内の別のインターフェイスでは、これらの MAC アドレスからのトラフィックを許可しません。セキュア MAC アドレスの数は、インターフェイス単位で設定します。

（注） 特に指定がなければ、インターフェイスは物理インターフェイスとポートチャネル インターフェイスの両方物理インターフェイス、ポートチャネル インターフェイス、および vPC を意味します。同様に、レイヤ *2* インターフェイスはレイヤ 2 物理インターフェイスとレイヤ 2 ポート チャネル インターフェイスの両方を意味します。

セキュア MAC アドレスの学習

MAC アドレスは学習というプロセスによってセキュア アドレスになります。MAC アドレスは、1 つのインターフェイスだけでセキュア MAC アドレスになることができます。デバイスは、ポート セキュリティがイネーブルに設定されたインターフェイスごとに、スタティック、ダイナミック、またはスティッキの方式で、限られた数の MAC アドレスを学習できます。デバイスがセキュア MAC アドレスを格納する方法は、デバイスがセキュア MAC アドレスを学習した方法によって異なります。

関連トピック

セキュア MAC アドレスの最大数, （648 ページ）

スタティック方式

スタティック学習方式では、ユーザが手動でインターフェイスの実行コンフィギュレーションにセキュア MAC アドレスを追加したり、設定から削除したりできます。実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーすると、デバイスを再起動してもスタティック セキュア MAC アドレスには影響がありません。

スタティック セキュア MAC アドレスのエントリは、次のいずれかのイベントが発生するまで、インターフェイスの設定内に維持されます。

- ユーザが明示的に設定からアドレスを削除した場合。
- ユーザがそのインターフェイスをレイヤ 3 インターフェイスとして設定した場合。

スタティック方式では、ダイナミック方式またはスティッキ方式のアドレス学習がイネーブルになっているかどうかに関係なく、セキュア アドレスを追加できます。

関連トピック

インターフェイスのスタティック セキュア MAC アドレスの削除, （664 ページ）
ポート タイプの変更, （654 ページ）

ダイナミック方式

デフォルトでは、インターフェイスのポート セキュリティをイネーブルにすると、ダイナミック学習方式がイネーブルになります。この方式では、デバイスは、入力トラフィックがインターフェイスを通過するときに MAC アドレスをセキュア アドレスにします。このようなアドレスがまだセキュア アドレスではなく、デバイスのアドレス数が適用可能な最大数に達していなければ、デバイスはそのアドレスをセキュア アドレスにして、トラフィックを許可します。

デバイスは、ダイナミック セキュア MAC アドレスをメモリに保存します。ダイナミック セキュア MAC アドレスのエントリは、次のいずれかのイベントが発生するまで、インターフェイスの設定内に維持されます。

- デバイスが再起動した場合。
- インターフェイスが再起動した場合。
- アドレスが、ユーザによって設定されたインターフェイスのエージング期限に達した場合。
- ユーザがアドレスを明示的に削除した場合。
- ユーザがそのインターフェイスをレイヤ 3 インターフェイスとして設定した場合。

関連トピック

ダイナミック アドレスのエージング, （648 ページ）
ダイナミック セキュア MAC アドレスの削除, （667 ページ）

スティッキ方式

スティッキ方式をイネーブルにすると、デバイスは、ダイナミック アドレス学習と同じ方法で MAC アドレスをセキュア アドレスにしますが、この方法で学習されたアドレスは NVRAM に保存されます。そのため、スティッキ方式で学習されたアドレスは、デバイスの再起動後も維持されます。スティッキ セキュア MAC アドレスは、インターフェイスの実行コンフィギュレーション内にはありません。

ダイナミックとスティッキのアドレス学習は両方同時にイネーブルにできません。あるインターフェイスのスティッキ学習をイネーブルにした場合、デバイスはダイナミック学習を停止して、代わりにスティッキ学習を実行します。スティッキ学習をディセーブルにすると、デバイスはダイナミック学習を再開します。

スティッキ セキュア MAC アドレスのエントリは、次のいずれかのイベントが発生するまで、インターフェイスの設定内に維持されます。

- ユーザがアドレスを明示的に削除した場合。

- ユーザがそのインターフェイスをレイヤ 3 インターフェイスとして設定した場合。

関連トピック

スティッキ セキュア MAC アドレスの削除, （666 ページ）

ダイナミック アドレスのエージング

デバイスは、ダイナミック方式で学習された MAC アドレスのエージングを行い、エージングの期限に達すると、アドレスをドロップします。エージングの期限は、インターフェイスごとに設定できます。有効な範囲は 0 ～ 1440 分です。0 を設定すると、エージングはディセーブルになります。

MACアドレスのエージングを判断するためにデバイスが使用する方法も設定できます。アドレスエージングの判断には、次に示す 2 つの方法が使用されます。

Inactivity

適用可能なインターフェイス上のアドレスからデバイスが最後にパケットを受信して以降の経過時間。

Absolute

デバイスがアドレスを学習して以降の経過時間。これがデフォルトのエージング方法ですが、デフォルトのエージング時間は 0 分（エージングはディセーブル）です。

（注） MAC アドレスをエージング アウトするのに absolute 法が使用されている場合、トラフィック レートによっては、MAC アドレスがエージング アウトされて再学習されるたびに、いくつかのパケットがドロップする可能性があります。これを回避するには、非アクティブ タイムアウトを使用します。

セキュア MAC アドレスの最大数

デフォルトでは、各インターフェイスのセキュアMACアドレスは1つだけです。各インターフェイス、またはインターフェイス上の各VLANに許容可能な最大MACアドレス数を設定できます。最大数は、ダイナミック、スティッキ、スタティックのいずれの方式で学習された MAC アドレスにも適用されます。

（注） vPC ドメインでは、プライマリ vPC 上の設定が有効になります。

ヒント　アドレスの最大数を 1 に設定し、接続されたデバイスの MAC アドレスを設定すると、そのデバイスにはポートの全帯域幅が保証されます。

各インターフェイスに許容されるセキュア MAC アドレスの数は、次の 3 つの制限によって決定されます。

デバイスの最大数

デバイスが許容できるセキュア MAC アドレスの最大数は 8192 です。この値は変更できません。新しいアドレスを学習するとデバイスの最大数を超過してしまう場合、たとえインターフェイスや VLAN の最大数に達していなくても、デバイスは新しいアドレスの学習を許可しません。

インターフェイスの最大数

ポートセキュリティで保護されるインターフェイスごとに、セキュア MAC アドレスの最大数 1025 を設定できます。デフォルトでは、インターフェイスの最大アドレス数は 1 です。インターフェイスの最大数を、デバイスの最大数より大きくすることはできません。

VLAN の最大数

ポート セキュリティで保護される各インターフェイスについて、VLAN あたりのセキュア MAC アドレスの最大数を設定できます。VLAN の最大数は、インターフェイスに設定されている最大数より大きくできません。VLAN 最大数の設定が適しているのは、トランク ポートの場合だけです。VLAN の最大数には、デフォルト値はありません。

インターフェイスあたりの、VLAN とインターフェイスの最大数は必要に応じて設定できます。ただし、新しい制限値が、適用可能なセキュア アドレス数よりも少ない場合は、まず、セキュア MAC アドレスの数を減らす必要があります。

関連トピック

セキュリティ違反と処理, （649 ページ）
ダイナミック セキュア MAC アドレスの削除, （667 ページ）
スティッキ セキュア MAC アドレスの削除, （666 ページ）
インターフェイスのスタティック セキュア MAC アドレスの削除, （664 ページ）

セキュリティ違反と処理

次の 2 つのイベントのいずれかが発生すると、ポート セキュリティ機能によってセキュリティ違反がトリガーされます。

最大数違反

あるインターフェイスにセキュアMACアドレス以外のアドレスから入力トラフィックが着信し、そのアドレスを学習するとセキュアMACアドレスの適用可能な最大数を超えてしまう場合

あるインターフェイスにVLANとインターフェイスの両方の最大数が設定されている場合は、どちらかの最大数を超えると、違反が発生します。たとえば、ポート セキュリティが設定されている単一のインターフェイスについて、次のように想定します。

- VLAN 1 の最大アドレス数は 5 です。
- このインターフェイスの最大アドレス数は 10 です。

デバイスは、次のいずれかが発生すると違反を検出します。

- VLAN 1 のアドレスをすでに 5 つ学習していて、6 つめのアドレスからのインバウンド トラフィックが VLAN 1 のインターフェイスに着信した場合
- このインターフェイス上のアドレスをすでに10個学習していて、11番めのアドレスからのインバウンド トラフィックがこのインターフェイスに着信した場合

MAC 移動違反

あるインターフェイスのセキュアMACアドレスになっているアドレスからの入力トラフィックが、そのインターフェイスと同じ VLAN 内の別のインターフェイスに着信した場合

セキュリティ違反が発生すると、デバイスは、インターフェイスのセキュリティ違反カウンタの値を増加させ、インターフェイスのポート セキュリティ設定に指定されている処理を実行します。セキュア MAC アドレスからの入力トラフィックが、そのアドレスをセキュア アドレスにしたインターフェイスとは異なるインターフェイスに着信したことにより違反が発生した場合、デバイスはトラフィックを受信したインターフェイスに対して処理を実行します。

デバイスが実行できる処理は次のとおりです。

シャットダウン

違反をトリガーしたパケットの受信インターフェイスをシャットダウンします。このインターフェイスはエラー ディセーブル状態になります。これがデフォルトの処理です。インターフェイスの再起動後も、セキュアMACアドレスを含めて、ポートセキュリティの設定は維持されます。

シャットダウン後にデバイスが自動的にインターフェイスを再起動するように設定するには、**errdisable** グローバル コンフィギュレーション コマンドを使用します。あるいは、**shutdown** および **no shut down** のインターフェイス コンフィギュレーション コマンドを入力することにより、手動でインターフェイスを再起動することもできます。

制限

非セキュア MAC アドレスからの入力トラフィックをすべてドロップします。

デバイスはドロップされたパケット数を保持しますが、これをセキュリティ違反回数と呼びます。インターフェイスで発生するセキュリティ違反が最大数に到達するまでアドレス学習を継続します。最初のセキュリティ違反のあとに学習されたアドレスからのトラフィックはドロップされます。

保護

これ以上の違反の発生を防止します。セキュリティ違反をトリガーしたアドレスは学習されますが、そのアドレスからのトラフィックはドロップされます。それ以降、アドレス学習は実行されなくなります。

関連トピック

ポート セキュリティに関する追加情報, （674 ページ）

ポート セキュリティとポート タイプ

ポート セキュリティを設定できるのは、レイヤ 2 インターフェイスだけです。各種のインターフェイスまたはポートとポート セキュリティについて次に詳しく説明します。

アクセス ポート

レイヤ 2 アクセス ポートとして設定したインターフェイスにポート セキュリティを設定できます。アクセス ポートでポート セキュリティが適用されるのは、アクセス VLAN だけです。アクセス ポートには、VLAN 最大数を設定しても効果はありません。

トランク ポート

レイヤ 2 トランク ポートとして設定したインターフェイスにポート セキュリティを設定できます。デバイスが VLAN 最大数を適用するのは、トランク ポートに関連付けられた VLAN だけです。

SPAN ポート

SPAN 送信元ポートにはポート セキュリティを設定できますが、SPAN 宛先ポートには設定できません。

イーサネット ポート チャネル

レイヤ 2 イーサネット ポート チャネル インターフェイスのポート セキュリティはアクセス モードまたはトランク モードで設定できます。

ファブリック エクステンダ（FEX）ポート

ポート セキュリティは GEM ポートおよび FEX ポートでサポートされています。

プライベート VLAN 対応ポート

ポート セキュリティは、プライベート VLAN ポートとしてイネーブルにされたポートでサポートされています。

PVLAN Host（物理インターフェイスのみ）

プライベートVLAN（PVLAN）を設定して、レイヤ2 レベルでのトラフィック分離とセキュリティを実現できます。PVLAN は 1 つのプライマリ VLAN と 1 つのセカンダリ VLAN を 1 つまたは複数組み合わせたもので、プライマリ VLAN はすべて同じです。

PVLAN Promiscuous（物理インターフェイスのみ）

PVLAN 無差別ポートにレイヤ 2 VLAN ネットワーク インターフェイスやスイッチ仮想インターフェイス（SVI）を設定し、プライマリ PVLAN にルーティング機能を持たせることもできます。これは、物理インターフェイスだけでサポートされます。

PVLAN トランク セカンダリ/無差別

Switchport モードで、PVLAN トランク セカンダリ/無差別を設定できます。これは、物理インターフェイスとポートチャネルの両方でサポートされます。

ポート セキュリティとポート チャネル インターフェイス

ポート セキュリティは、レイヤ 2 ポート チャネル インターフェイスでサポートされます。ポートチャネルインターフェイス上で動作するポートセキュリティは、ここで説明する内容以外は、物理インターフェイスの場合と同じです。

全般的な注意事項

ポートチャネルインターフェイスのポートセキュリティは、アクセス モードまたはトランク モードのいずれかで動作します。トランク モードでは、ポート セキュリティで適用される MAC アドレスの制限が、VLAN 単位ですべてのメンバ ポートに適用されます。

ポート チャネル インターフェイスのポート セキュリティをイネーブルにしても、ポート チャネルのロード バランシングには影響しません。

ポートセキュリティは、ポートチャネルインターフェイスを通過するポートチャネル制御トラフィックには適用されません。ポート セキュリティを使用すると、セキュリティ違反にならないようにして、ポート チャネル制御パケットを通過させることができます。ポート チャネル制御トラフィックには、次のプロトコルが含まれます。

- ポート集約プロトコル（PAgP）
- リンク集約制御プロトコル（LACP）
- スイッチ間リンク（ISL）
- IEEE 802.1Q

セキュア メンバ ポートの設定

ポート チャネル インターフェイスのポート セキュリティ設定は、メンバ ポートのポート セキュリティ設定には影響しません。

メンバ ポートの追加

セキュア インターフェイスをポート チャネル インターフェイスのメンバ ポートとして追加した場合、デバイスはメンバ ポートで学習されたダイナミック セキュア アドレスをすべて廃棄しますが、メンバ ポートのその他のポート セキュリティ設定はすべて実行コンフィギュレーションに保持します。セキュア メンバ ポートで学習されたスティッキ方式とスタティック方式のセキュア MAC アドレスも、NVRAM ではなく実行コンフィギュレーションに保存されます。

ポート セキュリティがメンバ ポートではイネーブルになっていて、ポート チャネル インターフェイスではイネーブルになっていない場合、メンバ ポートをポート チャネル インターフェイスに追加しようとすると警告されます。セキュア メンバ ポートを非セキュア ポート チャネル インターフェイスに強制的に追加するには、**force** キーワードを指定して **channel-group** コマンドを使用します。

ポートがポート チャネル インターフェイスのメンバである間は、メンバ ポートのポート セキュリティを設定できません。これを行うには、まずメンバ ポートをポート チャネル インターフェイスから削除する必要があります。

メンバ ポートの削除

メンバ ポートをポート チャネル インターフェイスから削除すると、メンバ ポートのポート セキュリティ設定が復元されます。ポート チャネル インターフェイスに追加する前にそのポートで学習されたスタティック方式とスティッキ方式のセキュア MAC アドレスは、NVRAM に復元され、実行コンフィギュレーションからは削除されます。

（注） ポート チャネル インターフェイスを削除したあとで、すべてのポートのセキュリティを必要に応じて確保するためには、すべてのメンバ ポートのポート セキュリティ設定を詳細に検査することを推奨します。

ポート チャネル インターフェイスの削除

セキュア ポート チャネル インターフェイスを削除すると、次の処理が行われます。

- ポート チャネル インターフェイスの学習されたセキュア MAC アドレスがすべて廃棄されます。これには、ポート チャネル インターフェイスで学習されたスタティック方式とスティッキ方式のセキュア MAC アドレスが含まれます。
- 各メンバ ポートのポート セキュリティ設定が復元されます。ポート チャネル インターフェイスに追加する前にそれらのメンバ ポートで学習されたスタティック方式とスティッキ方式のセキュア MAC アドレスは、NVRAM に復元され、実行コンフィギュレーションからは削除されます。ポート チャネル インターフェイスへの参加前にメンバ ポートでポート セキュリティがイネーブルになっていなかった場合、そのメンバ ポートでは、ポート チャネル インターフェイスの削除後もポート セキュリティがイネーブルになりません。

（注） ポート チャネル インターフェイスを削除したあとで、すべてのポートのセキュリティを必要に応じて確保するためには、すべてのメンバ ポートのポート セキュリティ設定を詳細に検査することを推奨します。

ポート セキュリティのディセーブル化

いずれかのメンバ ポートでポート セキュリティがイネーブルになっている場合、ポート チャネル インターフェイスのポート セキュリティをディセーブルにできません。これを行うには、まずすべてのセキュア メンバ ポートをポート チャネル インターフェイスから削除します。メンバ ポートのポート セキュリティをディセーブルにしたあと、必要に応じて、ポート チャネル インターフェイスに再度追加できます。

ポート タイプの変更

レイヤ 2 インターフェイスにポート セキュリティを設定し、そのインターフェイスのポート タイプを変更した場合、デバイスは次のように動作します。

アクセス ポートからトランク ポート

レイヤ 2 インターフェイスをアクセス ポートからトランク ポートに変更すると、デバイスはダイナミック方式で学習されたすべてのセキュア アドレスをドロップします。デバイスは、スタティック方式で学習したアドレスをネイティブ トランク VLAN に移行します。VLAN がすでに存在する場合、スティッキ MAC は同じ VLAN に維持され、そうでない場合、トランク ポートのネイティブ VLAN に移動します。

トランク ポートからアクセス ポート

レイヤ 2 インターフェイスをトランク ポートからアクセス ポートに変更すると、デバイスはダイナミック方式で学習されたすべてのセキュア アドレスをドロップします。ネイティブ トランク VLAN でスティッキ方式で学習されたアドレスはすべて、アクセス VLAN に移行されます。ネイティブ トランク VLAN でない場合、スティッキ方式で学習されたセキュア アドレスはドロップされます。

スイッチド ポートからルーテッド ポート

インターフェイスをレイヤ 2 インターフェイスからレイヤ 3 インターフェイスに変更すると、デバイスはそのインターフェイスのポート セキュリティをディセーブルにし、そのインターフェイスのすべてのポート セキュリティ設定を廃棄します。デバイスは、学習方式に関係なく、そのインターフェイスのセキュア MAC アドレスもすべて廃棄します。

ルーテッド ポートからスイッチド ポート

インターフェイスをレイヤ 3 インターフェイスからレイヤ 2 インターフェイスに変更すると、デバイス上のそのインターフェイスのポート セキュリティ設定はなくなります。

802.1X とポート セキュリティ

ポート セキュリティと 802.1X は同じインターフェイス上に設定できます。ポート セキュリティによって、802.1X 認証の MAC アドレスを保護できます。802.1X はポート セキュリティよりも前にパケットを処理するので、1 つのインターフェイスで両方をイネーブルにすると、802.1X が、そのインターフェイスで、未知の MAC アドレスからのインバウンド トラフィックを妨げます。

同じインターフェイス上で 802.1X とポート セキュリティをイネーブルにしても、ポート セキュリティは設定どおりにスティッキ方式またはダイナミック方式で MAC アドレスの学習を続行します。また、シングル ホスト モードとマルチ ホスト モードのどちらで 802.1X をイネーブルにするかによって、次のいずれかが発生します。

シングル ホスト モード

ポート セキュリティは認証済みのホストの MAC アドレスを学習します。

マルチ ホスト モード

ポートセキュリティは、このインターフェイスでダイナミックに学習された MAC アドレスをドロップし、802.1X で認証された最初のホストの MAC アドレスを学習します。

802.1X がポート セキュリティに渡した MAC アドレスによってセキュア MAC アドレスの適用可能な最大数を違反することになる場合、デバイスはホストに認証エラー メッセージを送信します。

802.1X によって認証された MAC アドレスは、たとえそのアドレスがポート セキュリティによってスティッキ方式またはスタティック方式で学習されていたとしても、ダイナミック方式で学習

されたアドレスと同様に扱われます。802.1X で認証されたセキュア MAC アドレスを削除しようとしても、そのアドレスはセキュア アドレスのまま保持されます。

認証済みのホストの MAC アドレスがスティッキ方式またはスタティック方式でセキュア アドレスになった場合、デバイスはそのアドレスをダイナミック方式で学習されたものとして扱うので、その MAC アドレスを手動で削除することはできません。

認証済みのホストのセキュアMACアドレスがポートセキュリティのエージング期限に達すると、ポート セキュリティは 802.1X と連動して、そのホストを再認証します。デバイスは、エージングのタイプに応じて、次のように異なる動作をします。

Absolute

ポート セキュリティは 802.1X に通知し、デバイスはホストの再認証を試行します。そのアドレスが引き続きセキュアアドレスになるかどうかは、再認証の結果によって決まります。再認証が成功すれば、デバイスはそのセキュア アドレスのエージング タイマーを再起動します。再認証に失敗した場合、デバイスはそのインターフェイスのセキュア アドレス リストからそのアドレスをドロップします。

Inactivity

ポート セキュリティは、そのインターフェイスのセキュア アドレス リストからそのセキュアアドレスをドロップし、802.1X に通知します。デバイスはホストの再認証を試行します。再認証が成功すれば、ポート セキュリティは再度そのアドレスをセキュア アドレスにします。

ポート セキュリティのバーチャライゼーション サポート

ポート セキュリティは次のように VDC をサポートします。

- ポート セキュリティは各 VDC に設定されます。ポート セキュリティは VDC 単位でイネーブルにし設定できます。
- セキュア MAC アドレスは VDC ごとに個別に維持されます。
- ある VDC のセキュア MAC アドレスが別の VDC の保護インターフェイス上にあっても、セキュリティ違反にはなりません。

ポート セキュリティのライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	ポートセキュリティにはライセンスは必要ありません。ライセンスパッケージに含まれていない機能は、Cisco NX-OS デバイス イメージにバンドルされており、追加料金なしで利用できます。Cisco NX-OS ライセンス方式の詳細については、*License and Copyright Information for Cisco NX-OS Software*（http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/license_agreement/nx-ossw_lisns.html）を参照してください。

ポート セキュリティの前提条件

ポート セキュリティの前提条件は次のとおりです。

- ポート セキュリティで保護するデバイスのポート セキュリティをグローバルにイネーブル化すること。

ポート セキュリティのデフォルト設定

次の表に、ポート セキュリティ パラメータのデフォルト設定を示します。

表 *39*：ポート セキュリティ パラメータのデフォルト値

パラメータ	デフォルト
ポートセキュリティがグローバルにイネーブルかどうか	ディセーブル
インターフェイス単位でポートセキュリティがイネーブルかどうか	ディセーブル
MAC アドレス ラーニング方式	ダイナミック
セキュア MAC アドレスのインターフェイス最大数	1
セキュリティ違反時の処理	シャットダウン

ポート セキュリティの注意事項と制約事項

ポート セキュリティを設定する場合、次の注意事項に従ってください。

- ポート セキュリティは PVLAN ポートでサポートされています。
- ポート セキュリティは、スイッチド ポート アナライザ（SPAN）の宛先ポートをサポートしません。
- ポート セキュリティは他の機能に依存しません。
- チャネル グループ内のポートを設定する前に、ポート セキュリティをディセーブルにする必要があります。
- ポート セキュリティは vPC ポートではサポートされていません。
- ポート セキュリティは、レイヤ 2 イーサネット インターフェイス上で 802.1X とともに動作します。

関連トピック

802.1X とポート セキュリティ，（321 ページ）

ポート セキュリティの設定

ポートセキュリティのグローバルなイネーブル化またはディセーブル化

デバイスに対してポート セキュリティ機能のグローバルなイネーブル化またはディセーブル化が可能です。デフォルトで、ポート セキュリティはグローバルにディセーブルになっています。

ポートセキュリティをディセーブルにすると、インターフェイスのすべてのポートセキュリティ設定が無効になります。ポート セキュリティをグローバルにディセーブル化すると、すべてのポート セキュリティ設定が失われます。

手順の概要

1. **configure terminal**
2. **[no] feature port-security**
3. **show port-security**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **feature port-security** 例： `switch(config)# feature port-security`	ポート セキュリティをグローバルにイネーブル化します。**no** オプションを使用すると ポート セキュリティはグローバルにディセーブル化されます。
ステップ 3	**show port-security** 例： `switch(config)# show port-security`	ポート セキュリティのステータスを表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

レイヤ 2 インターフェイスに対するポート セキュリティのイネーブル化またはディセーブル化

レイヤ 2 インターフェイスに対してポート セキュリティ機能のイネーブル化またはディセーブル化が可能です。デフォルトでは、ポート セキュリティはすべてのインターフェイスでディセーブルです。

インターフェイスのポート セキュリティをディセーブルにすると、そのインターフェイスのすべてのスイッチポートのポート セキュリティ設定が失われます。

次の方法でポート チャネルのポート セキュリティをイネーブルにすることができます。

- channel-group コマンドを使用してメンバー リンクを 1 つのポート チャネルとしてバンドルした後、ポート チャネルのポート セキュリティをイネーブルにする。
- ポート チャネルを作成し、ポート セキュリティを設定する。メンバー リンクのポート セキュリティを設定した後、channel-group コマンドを使用してメンバー リンクを 1 つのポート チャネルとしてバンドルする。

はじめる前に

ポート セキュリティがグローバルにイネーブル化されている必要があります。

レイヤ 2 イーサネット インターフェイスがポート チャネル インターフェイスのメンバである場合、レイヤ 2 イーサネット インターフェイスに対するポート セキュリティはイネーブルまたはディセーブルにできません。

セキュア レイヤ 2 ポート チャネル インターフェイスのメンバのいずれかのポート セキュリティがイネーブルになっている場合、先にポート チャネル インターフェイスからセキュア メンバ ポートをすべて削除しない限り、そのポート チャネル インターフェイスのポート セキュリティをディセーブルにできません。

手順の概要

1. **configure terminal**
2. 次のいずれかのコマンドを入力します。
   - **interfaceethernet***slot*/*port*
   - **interfaceport-channel***channel-number*
3. **switchport**
4. **[no] switchport port-security**
5. **show running-config port-security**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	次のいずれかのコマンドを入力します。
	• **interfaceethernet***slot*/*port*
	• **interfaceport-channel***channel-number*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		ポートセキュリティを設定するイーサネットインターフェイスまたはポート チャネル インターフェイスのインターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**switchport** 例： `switch(config-if)# switchport`	そのインターフェイスを、レイヤ2インターフェイスとして設定します。

	コマンドまたはアクション	目的
ステップ 4	**[no] switchport port-security** 例： `switch(config-if)# switchport port-security`	インターフェイス上でポート セキュリティをイネーブルにします。**no** オプションを使用すると、そのインターフェイスのポート セキュリティがディセーブルになります。
ステップ 5	**show running-config port-security** 例： `switch(config-if)# show running-config port-security`	ポート セキュリティの設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

セキュア MAC アドレスの学習，（646 ページ）
スティッキ MAC アドレス ラーニングのイネーブル化またはディセーブル化，（661 ページ）

スティッキ MAC アドレス ラーニングのイネーブル化またはディセーブル化

インターフェイスのスティッキ MAC アドレス ラーニングをディセーブルまたはイネーブルに設定できます。スティッキ学習をディセーブルにすると、そのインターフェイスはダイナミック MAC アドレス ラーニング（デフォルトの学習方式）に戻ります。

デフォルトでは、スティッキ MAC アドレス ラーニングはディセーブルです。

はじめる前に

ポート セキュリティがグローバルにイネーブル化されている必要があります。

手順の概要

1. **configure terminal**
2. 次のいずれかのコマンドを入力します。
   - **interfaceethernet***slot*/*port*
   - **interfaceport-channel***channel-number*
3. **switchport**
4. [**no**] **switchport port-security mac-address sticky**
5. **show running-config port-security**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	次のいずれかのコマンドを入力します。
	• **interfaceethernet***slot*/*port*
	• **interfaceport-channel***channel-number*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		スティッキ MAC アドレス ラーニングを設定するインターフェイスのインターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**switchport** 例： `switch(config-if)# switchport`	そのインターフェイスを、レイヤ 2 インターフェイスとして設定します。
ステップ 4	[**no**] **switchport port-security mac-address sticky** 例： `switch(config-if)# switchport port-security mac-address sticky`	そのインターフェイスのスティッキ MAC アドレス ラーニングをイネーブルにします。**no** オプションを使用すると スティッキ MAC アドレス ラーニングがディセーブルになります。
ステップ 5	**show running-config port-security** 例： `switch(config-if)# show running-config port-security`	ポート セキュリティの設定を表示します。

	コマンドまたはアクション	目的
ステップ 6	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスのスタティック セキュア MAC アドレスの追加

レイヤ 2 インターフェイスにスタティック セキュア MAC アドレスを追加できます。

（注） MAC アドレスが任意のインターフェイスでセキュア MAC アドレスである場合、その MAC アドレスがすでにセキュア MAC アドレスとなっているインターフェイスからその MAC アドレスを削除するまで、その MAC アドレスをスタティック セキュア MAC アドレスとして別のインターフェイスに追加することはできません。

デフォルトでは、インターフェイスにスタティック セキュア MAC アドレスは設定されません。

はじめる前に

ポート セキュリティがグローバルにイネーブル化されている必要があります。

インターフェイスのセキュア MAC アドレス最大数に達していないことを確認します。必要に応じて、セキュア MAC アドレスを削除するか、インターフェイスの最大アドレス数を変更できます。

手順の概要

1. **configure terminal**
2. 次のいずれかのコマンドを入力します。
   - **interfaceethernet***slot*/*port*
   - **interfaceport-channel***channel-number*
3. [**no**] **switchport port-security mac-address** *address* [**vlan***vlan-ID*]
4. **show running-config port-security**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	次のいずれかのコマンドを入力します。
	• **interfaceethernet***slot*/*port*
	• **interfaceport-channel***channel-number*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		指定したインターフェイスのインターフェイス コンフィギュレーション モードを開始します。

ステップ 3	[**no**] **switchport port-security mac-address** *address* [**vlan***vlan-ID*] 例： `switch(config-if)# switchport port-security mac-address 0019.D2D0.00AE`	現在のインターフェイスのポート セキュリティにスタティック MAC アドレスを設定します。そのアドレスからのトラフィックを許可する VLAN を指定する場合は、**vlan** キーワードを使用します。
ステップ 4	**show running-config port-security** 例： `switch(config-if)# show running-config port-security`	ポート セキュリティの設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

ポート セキュリティの設定の確認, （673 ページ）
MAC アドレスの最大数の設定, （668 ページ）
ダイナミック セキュア MAC アドレスの削除, （667 ページ）
インターフェイスのスタティック セキュア MAC アドレスの削除, （664 ページ）

インターフェイスのスタティック セキュア MAC アドレスの削除

レイヤ 2 インターフェイスのスタティック セキュア MAC アドレスを削除できます。

手順の概要

1. **configure terminal**
2. 次のいずれかのコマンドを入力します。
   - **interfaceethernet***slot*/*port*
   - **interfaceport-channel***channel-number*
3. **noswitchport port-security mac-address** *address*
4. **show running-config port-security**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	次のいずれかのコマンドを入力します。
	• **interfaceethernet***slot*/*port*
	• **interfaceport-channel***channel-number*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		スタティック セキュア MAC アドレスを削除するインターフェイスのインターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**noswitchport port-security mac-address** *address* 例： `switch(config-if)# no switchport port-security mac-address 0019.D2D0.00AE`	現在のインターフェイスのポート セキュリティからスタティック セキュア MAC アドレスを削除します。
ステップ 4	**show running-config port-security** 例： `switch(config-if)# show running-config port-security`	ポート セキュリティの設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

スティッキ セキュア MAC アドレスの削除

スティッキ セキュア MAC アドレスを削除できます。この際、削除するアドレスが設定されているインターフェイスで、スティッキ方式のアドレス学習を一時的にディセーブルにする必要があります。

はじめる前に

ポート セキュリティがグローバルにイネーブル化されている必要があります。

手順の概要

1. **configure terminal**
2. 次のいずれかのコマンドを入力します。
   - **interfaceethernet***slot*/*port*
   - **interfaceport-channel***channel-number*
3. **no switchport port-security mac-address sticky**
4. **clear port-security dynamic address***address*
5. （任意） **show port-security address interface** {**ethernet** *slot*/*port* | **port-channel** *channel-number*}
6. （任意） **switchport port-security mac-address sticky**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	次のいずれかのコマンドを入力します。
	• **interfaceethernet***slot*/*port*
	• **interfaceport-channel***channel-number*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		スティッキ セキュア MAC アドレスを削除するインターフェイスのインターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**no switchport port-security mac-address sticky** 例： `switch(config-if)# no switchport port-security mac-address sticky`	インターフェイスのスティッキ MAC アドレス ラーニングをディセーブルにします。これにより、インターフェイスのスティッキ セキュア MAC アドレスが、ダイナミック セキュア MAC アドレスに変換されます。

	コマンドまたはアクション	目的
ステップ 4	**clear port-security dynamic address***address* 例： `switch(config-if)# clear port-security dynamic address 0019.D2D0.02GD`	指定したダイナミック セキュア MAC アドレスを削除します。
ステップ 5	**show port-security address interface** {**ethernet** *slot*/*port* | **port-channel** *channel-number*} 例： `switch(config)# show port-security address`	（任意） セキュア MAC アドレスを表示します。削除したアドレスは表示されません。
ステップ 6	**switchport port-security mac-address sticky** 例： `switch(config-if)# switchport port-security mac-address sticky`	（任意） そのインターフェイスのスティッキ MAC アドレス ラーニングを再度イネーブルにします。

ダイナミック セキュア MAC アドレスの削除

ダイナミックに学習されたセキュア MAC アドレスを削除できます。

はじめる前に

ポート セキュリティがグローバルにイネーブル化されている必要があります。

手順の概要

1. **configure terminal**
2. **clear port-security dynamic** {**interface ethernet***slot*/*port* | **address***address*} [**vlan***vlan-ID*]
3. **show port-security address**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**clear port-security dynamic** {**interface ethernet***slot*/*port* | **address***address*} [**vlan***vlan-ID*] 例： `switch(config)# clear port-security dynamic interface ethernet 2/1`	ダイナミックに学習されたセキュア MAC アドレスを削除します。次の方法で指定できます。 **interface** キーワードを使用すると、指定したインターフェイスでダイナミックに学習されたアドレスがすべて削除されます。 **address** キーワードを使用すると、指定した単一のダイナミック学習アドレスが削除されます。 特定の VLAN のアドレスを削除するようにコマンドに制限を加えるには、**vlan** キーワードを使用します。
ステップ 3	**show port-security address** 例： `switch(config)# show port-security address`	セキュア MAC アドレスを表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

MAC アドレスの最大数の設定

レイヤ 2 インターフェイスで学習可能な MAC アドレスまたはスタティックに設定可能な MAC アドレスの最大数を設定できます。レイヤ 2 インターフェイス上の VLAN 単位でも MAC アドレスの最大数を設定できます。インターフェイスに設定できる最大アドレス数は 1025 です。システムの最大アドレス数は 8192 です。

デフォルトでは、各インターフェイスのセキュア MAC アドレスの最大数は 1 です。VLAN には、セキュア MAC アドレス数のデフォルトの最大値はありません。

（注） インターフェイスですでに学習されているアドレス数またはインターフェイスにスタティックに設定されたアドレス数よりも小さい数を最大数に指定すると、デバイスはこのコマンドを拒否します。ダイナミック方式で学習されたアドレスをすべて削除するには、**shutdown** および **no shutdown** のコマンドを使用して、インターフェイスを再起動します。

はじめる前に

ポート セキュリティがグローバルにイネーブル化されている必要があります。

手順の概要

1. **configure terminal**
2. 次のいずれかのコマンドを入力します。
   - **interfaceethernet***slot*/*port*
   - **interfaceport-channel***channel-number*
3. [**no**] **switchport port-security maximum** *number* [**vlan***vlan-ID*]
4. **show running-config port-security**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	次のいずれかのコマンドを入力します。
	• **interfaceethernet***slot*/*port*
	• **interfaceport-channel***channel-number*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。*slot* は、MAC アドレスの最大数を設定するインターフェイスです。

ステップ 3	[**no**] **switchport port-security maximum** *number* [**vlan***vlan-ID*] 例： `switch(config-if)# switchport port-security maximum 425`	現在のインターフェイスで学習可能なMACアドレスまたはスタティックに設定可能なMACアドレスの最大数を設定します。*number* の最大値は 1025 です。**no** オプションを使用すると、MACアドレスの最大数がデフォルト値（1）にリセットされます。 最大数を適用する VLAN を指定する場合は、**vlan** キーワードを使用します。
ステップ 4	**show running-config port-security** 例： `switch(config-if)# show running-config port-security`	ポート セキュリティの設定を表示します。

	コマンドまたはアクション	目的
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

ダイナミック セキュア MAC アドレスの削除, （667 ページ）
インターフェイスのスタティック セキュア MAC アドレスの削除, （664 ページ）

アドレス エージングのタイプと期間の設定

MAC アドレス エージングのタイプと期間を設定できます。デバイスは、ダイナミック方式で学習された MAC アドレスがエージング期限に到達する時期を判断するためにこれらの設定を使用します。

デフォルトのエージング タイプは絶対エージングです。

デフォルトのエージング タイムは 0 分（エージングはディセーブル）です。

はじめる前に

ポート セキュリティがグローバルにイネーブル化されている必要があります。

手順の概要

1. **configure terminal**
2. 次のいずれかのコマンドを入力します。
   - **interfaceethernet***slot*/*port*
   - **interfaceport-channel***channel-number*
3. **[no] switchport port-security aging type {absolute | inactivity}**
4. **[no] switchport port-security aging time** *minutes*
5. **show running-config port-security**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	次のいずれかのコマンドを入力します。
	• **interfaceethernet***slot*/*port*
	• **interfaceport-channel***channel-number*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		MAC エージングのタイプと期間を設定するインターフェイスのインターフェイス コンフィギュレーション モードを開始します。

ステップ 3	[**no**] **switchport port-security aging type** {**absolute** | **inactivity**} 例： `switch(config-if)# switchport port-security aging type inactivity`	ダイナミックに学習されたMACアドレスにデバイスが適用するエージング タイプを設定します。**no** オプションを使用すると、エージングタイプがデフォルト値（絶対エージング）にリセットされます。
ステップ 4	[**no**] **switchport port-security aging time** *minutes* 例： `switch(config-if)# switchport port-security aging time 120`	ダイナミックに学習されたMACアドレスがドロップされるまでのエージング タイムを分単位で設定します。*minutes* の最大値は 1440 です。**no** オプションを使用すると、エージング タイムがデフォルト値である 0（エージングはディセーブル）にリセットされます。
ステップ 5	**show running-config port-security** 例： `switch(config-if)# show running-config port-security`	ポート セキュリティの設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

セキュリティ違反時の処理の設定

セキュリティ違反が発生した場合にデバイスが実行する処理を設定できます。違反時の処理は、ポート セキュリティをイネーブルにしたインターフェイスごとに設定できます。

デフォルトのセキュリティ処理では、セキュリティ違反が発生したポートがシャットダウンされます。

はじめる前に

ポート セキュリティがグローバルにイネーブル化されている必要があります。

手順の概要

1. **configure terminal**
2. 次のいずれかのコマンドを入力します。
   - **interfaceethernet***slot*/*port*
   - **interfaceport-channel***channel-number*
3. [**no**] **switchport port-security violation** {**protect** | **restrict** | **shutdown**}
4. **show running-config port-security**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	次のいずれかのコマンドを入力します。
	• **interfaceethernet***slot*/*port*
	• **interfaceport-channel***channel-number*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		セキュリティ違反時の処理を設定するインターフェイスのインターフェイス コンフィギュレーション モードを開始します。

ステップ 3	[**no**] **switchport port-security violation** {**protect** | **restrict** | **shutdown**} 例： `switch(config-if)# switchport port-security violation restrict`	現在のインターフェイスのポートセキュリティにセキュリティ違反時の処理を設定します。**no** オプションを使用すると、違反時の処理がデフォルト値（インターフェイスのシャットダウン）にリセットされます。
ステップ 4	**show running-config port-security** 例： `switch(config-if)# show running-config port-security`	ポート セキュリティの設定を表示します。

	コマンドまたはアクション	目的
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ポート セキュリティの設定の確認

ポート セキュリティの設定情報を表示するには、次のいずれかの作業を行います。このコマンドの出力フィールドについての詳細は、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

コマンド	目的
show running-config port-security	ポート セキュリティの設定を表示します。
show port-security	デバイスのポートセキュリティのステータスを表示します。
show port-security interface	特定のインターフェイスのポートセキュリティのステータスを表示します。
show port-security address	セキュア MAC アドレスを表示します。

セキュア MAC アドレスの表示

セキュア MAC アドレスを表示するには、**show port-security address** コマンドを使用します。このコマンドの出力フィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

ポート セキュリティの設定例

次に示す例は、VLAN とインターフェイスのセキュア アドレス最大数が指定されているイーサネット 2/1 インターフェイスのポート セキュリティ設定です。この例のインターフェイスはトランク ポートです。違反時の処理は Restrict（制限）に設定されています。

```
feature port-security
interface Ethernet 2/1
  switchport
  switchport port-security
```

```
switchport port-security maximum 10
switchport port-security maximum 7 vlan 10
switchport port-security maximum 3 vlan 20
switchport port-security violation restrict
```

ポート セキュリティに関する追加情報

関連資料

関連項目	マニュアル タイトル
レイヤ 2 スイッチング	『*Cisco Nexus 7000 Series NX-OS Layer 2 Switching Configuration Guide*』
ポート セキュリティ コマンド：完全なコマンド構文、コマンド モード、コマンド履歴、デフォルト値、使用上の注意、例	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

MIB

Cisco NX-OS はポート セキュリティに関して読み取り専用の SNMP をサポートしています。

MIB	MIB のリンク
• CISCO-PORT-SECURITY-MIB （注） トラップは、セキュア MAC アドレスの違反の通知についてサポートされています。	MIB を検索およびダウンロードするには、次の URL にアクセスしてください。 http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

ポート セキュリティの機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 *40* : ポート セキュリティの機能の履歴

機能名	リリース	機能情報	
ポート セキュリティ	6.0(1)	Release 5.2 以降、変更はありません。	
ポート セキュリティ	5.2(1)	Release 5.1 以降、変更はありません。	
ポート セキュリティ	5.1(1)	Release 5.0 以降、変更はありません。	
ポート セキュリティ	5.0(2)	Release 4.2 以降、変更はありません。	
ポート セキュリティ	4.2(1)	レイヤ 2 ポート チャネル インターフェイスがサポートされるようになりました。	

第 19 章

DHCP の設定

この章では、Cisco NX-OS デバイスで Dynamic Host Configuration Protocol（DHCP）を設定する手順について説明します。

この章は、次の項で構成されています。

- 機能情報の確認，678 ページ
- DHCP スヌーピングの概要，678 ページ
- DHCP リレー エージェントの概要，684 ページ
- DHCPv6 リレー エージェントの概要，687 ページ
- Lightweight DHCPv6 リレー エージェントについて，688 ページ
- UDP リレーについて，689 ページ
- DHCP の仮想化サポート，691 ページ
- DHCP のライセンス要件，692 ページ
- DHCP の前提条件，692 ページ
- DHCP の注意事項と制約事項，692 ページ
- DHCP のデフォルト設定，694 ページ
- DHCP の設定，695 ページ
- DHCPv6 の設定，719 ページ
- Lightweight DHCPv6 リレー エージェントの設定，725 ページ
- UDP リレーの設定，727 ページ
- DHCP 設定の確認，729 ページ
- DHCP バインディングの表示，729 ページ
- LDRA 情報の表示とクリア，729 ページ
- UDP リレー情報の表示，730 ページ

- DHCP スヌーピング バインディング データベースのクリア，733 ページ
- DHCP リレー統計情報のクリア，734 ページ
- DHCPv6 リレー統計情報のクリア，734 ページ
- DHCP のモニタリング，734 ページ
- DHCP の設定例，735 ページ
- LDRA の設定例，736 ページ
- DHCP に関する追加情報，736 ページ
- DHCP の機能の履歴，737 ページ

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

DHCP スヌーピングの概要

DHCP スヌーピングは、信頼できないホストと信頼できる DHCP サーバとの間でファイアウォールのような機能を果たします。DHCP スヌーピングでは次のアクティビティを実行します。

- 信頼できない送信元からの DHCP メッセージを検証し、無効なメッセージをフィルタ処理して除外します。
- DHCP スヌーピング バインディング データベースを構築し、管理します。このデータベースには、リース IP アドレスがある信頼できないホストに関する情報が保存されています。
- DHCP スヌーピング バインディング データベースを使用して、信頼できないホストからの以降の要求を検証します。

DHCP スヌーピングは、グローバルおよび VLAN 単位でイネーブルにできます。デフォルトでは、この機能はグローバルおよびすべての VLAN でディセーブルです。この機能は、1 つの VLAN または特定の VLAN 範囲でイネーブルにできます。

信頼できる送信元と信頼できない送信元

DHCP スヌーピングがトラフィックの送信元を信頼するかどうかを設定できます。信頼できない送信元の場合、トラフィック攻撃やその他の敵対的アクションが開始される可能性があります。

こうした攻撃を防ぐため、DHCP スヌーピングは信頼できない送信元からのメッセージをフィルタリングします。

企業ネットワークでは、信頼できる送信元はその企業の管理制御下にあるデバイスです。これらのデバイスには、ネットワーク内のスイッチ、ルータ、およびサーバが含まれます。ファイアウォールを越えるデバイスやネットワーク外のデバイスは信頼できない送信元です。一般的に、ホスト ポートは信頼できない送信元として扱われます。

サービス プロバイダーの環境では、サービス プロバイダー ネットワークにないデバイスは、信頼できない送信元です（カスタマー スイッチなど）。ホスト ポートは、信頼できない送信元です。

Cisco NX-OS デバイスでは、接続インターフェイスの信頼状態を設定することにより、送信元を信頼できるものとして扱うことができます。

すべてのインターフェイスのデフォルトの信頼状態は、信頼できない状態になります。DHCP サーバ インターフェイスは、信頼できるインターフェイスとして設定する必要があります。ユーザのネットワーク内でデバイス（スイッチまたはルータ）に接続されている場合、他のインターフェイスも信頼できるインターフェイスとして設定できます。ホストポートインターフェイスは、通常、信頼できるインターフェイスとしては設定しません。

（注） DHCP スヌーピングを適切に機能させるためには、すべての DHCP サーバが信頼できるインターフェイスを介してデバイスと接続される必要があります。

DHCP スヌーピング バインディング データベース

DHCP スヌーピングは、代行受信した DHCP メッセージから抽出した情報を使用し、ダイナミックにデータベースを構築し維持します。DHCP スヌーピングがイネーブルにされた VLAN に、ホストが関連付けられている場合、データベースには、リース IP アドレスがある信頼できない各ホストのエントリが保存されています。データベースには、信頼できるインターフェイスを介して接続するホストに関するエントリは保存されません。

（注） DHCP スヌーピング バインディング データベースは DHCP スヌーピング バインディング テーブルとも呼ばれます。

デバイスが特定の DHCP メッセージを受信すると、DHCP スヌーピングはデータベースをアップデートします。たとえば、デバイスが DHCPACK メッセージをサーバから受信すると、この機能によってデータベースにエントリが追加されます。IP アドレスのリース期限が過ぎたり、デバイスがホストから DHCPRELEASE メッセージを受信すると、この機能によってデータベース内のエントリが削除されます。

DHCP スヌーピング バインディング データベースの各エントリには、ホストの MAC アドレス、リース IP アドレス、リース期間、バインディング タイプ、VLAN 番号、およびホストに関連するインターフェイス情報が保存されます。

ダイナミック ARP インスペクション（DAI）および IP ソース ガードも、DHCP スヌーピング バインディング データベースに格納された情報を使用します。

clear ip dhcp snooping binding コマンドを使用すると、バインディング データベースからエントリ削除できます。

関連トピック

DHCP スヌーピング バインディング データベースのクリア，（733 ページ）

vPC 環境での DHCP スヌーピング

仮想ポート チャネル（vPC）では、2 台の Cisco NX-OS スイッチを 3 番目のデバイスに 1 つの論理ポート チャネルとして認識させることができます。第 3 のデバイスは、スイッチ、サーバ、ポートチャネルをサポートするその他の任意のネットワーキングデバイスのいずれでもかまいません。

標準的な vPC 環境では、DHCP 要求は一方の vPC ピア スイッチに到達でき、応答は他方の vPC ピア スイッチに到達できるため、一方のスイッチには部分的な DHCP（IP-MAC）バインディング エントリが生成され、他方のスイッチにはバインディング エントリが生成されません。その結果、DHCP スヌーピング、およびダイナミック ARP インスペクション（DAI）や IP ソース ガードなどのそれに関連する機能は中断されます。Cisco NX-OS Release 5.1 以降では、Cisco Fabric Service over Ethernet（CFSoE）配布を使用して、すべての DHCP パケット（要求と応答）を、両方のスイッチで表示されるようにすることで、この問題を解決しました。これは、vPC リンクの背後にあるすべてのクライアントの両方のスイッチで同じバインディング エントリを作成および維持するのに役立ちます。

CFSoE 分散ではまた、vPC リンク上の DHCP 要求および応答を 1 台のスイッチのみが転送するようにもできます。vPC 以外の環境では、両方のスイッチが DHCP パケットを転送します。

DHCP スヌーピング バインディング エントリの同期

ダイナミック DHCP バインディング エントリは、次のシナリオで同期される必要があります。

- リモート vPC がオンラインになったとき、その vPC リンクのすべてのバインディング エントリがピアと同期する必要があります。
- DHCP スヌーピングがピア スイッチでイネーブルになっている場合、すべての vPC リンクのダイナミック バインディング エントリがピアと同期する必要があります。

パケット検証

デバイスは、DHCP スヌーピングがイネーブルの VLAN にある信頼できないインターフェイスで受信された DHCP パケットを検証します。デバイスは、次のいずれかの条件が発生しないかぎり、DHCP パケットを転送します（これらの条件が発生した場合、パケットはドロップされます）。

- 信頼できないインターフェイスで DHCP 応答パケット（DHCPACK、DHCPNAK、または DHCPOFFER などのパケット）を受信した場合。
- 信頼できないインターフェイスからパケットを受信し、この送信元 MAC アドレスと DHCP クライアント ハードウェア アドレスが一致しない場合。このチェックは、DHCP スヌーピングの MAC アドレス検証オプションがオンの場合だけ、実行されます。
- DHCP スヌーピング バインディング テーブル内にエントリを持つ信頼できないホストから DHCPRELEASE または DHCPDECLINE メッセージを受信したが、バインディング テーブル内のインターフェイス情報が、このメッセージを受信したインターフェイスと一致しない場合。

さらに、DHCP パケットの厳密な検証をイネーブルにすることもできます。これにより、DHCP パケットのオプション フィールドが確認されます。これには、オプション フィールドの最初の 4 バイト内の「マジック クッキー」値も含まれます。デフォルトでは、厳密な検証はディセーブルになっています。これを **ip dhcp packet strict-validation** コマンドによりイネーブルにすると、DHCP スヌーピングで無効なオプション フィールドを含むパケットを処理した場合に、パケットがドロップされます。

関連トピック

DHCP パケットの厳密な検証のイネーブル化またはディセーブル化, （702 ページ）

DHCP スヌーピングの Option 82 データ挿入

DHCP では、多数の加入者に対する IP アドレスの割り当てを一元管理できます。Option 82 をイネーブルにすると、デバイスはネットワークに接続する加入者デバイス（およびその MAC アドレス）を識別します。加入者 LAN 上のマルチ ホストをアクセス デバイスの同一ポートに接続でき、これらは一意に識別されます。

Cisco NX-OS デバイスで Option 82 をイネーブルにすると、次のイベントが順番に発生します。

1. ホスト（DHCP クライアント）は DHCP 要求を生成し、これをネットワーク上にブロードキャストします。
2. Cisco NX-OS デバイスはこの DHCP 要求を受信すると、パケット内に Option 82 情報を追加します。Option 82 情報には、デバイスの MAC アドレス（リモート ID サブオプション）、およびパケットを受信したポートの識別子である vlan-mod-port（回線 ID サブオプション）が含まれます。ポート チャネルの背後にあるホストの場合、回線 ID にはポート チャネルの if_index が入力されます。

（注） vPC ピア スイッチの場合、リモート ID サブオプションには vPC スイッチの MAC アドレスが入ります。これは両方のスイッチにおいて一意です。この MAC アドレスは vPC ドメイン ID とともに計算されます。Option 82 情報は、DHCP 要求が他の vPC ピア スイッチに転送される前に最初に受信したスイッチで挿入されます。

3. デバイスは、Option 82 フィールドを含む DHCP 要求を DHCP サーバに転送します。

4 DHCPサーバはこのパケットを受信します。Option82に対応しているサーバであれば、このリモート ID、回線 ID、またはその両方を使用して、IP アドレスの割り当てやポリシーの適用を行うことができます。たとえば、単一のリモート ID または回線 ID に割り当てることのできる IP アドレスの数を制限するポリシーなどです。DHCP サーバは、DHCP 応答内に Option 82 フィールドをエコーします。

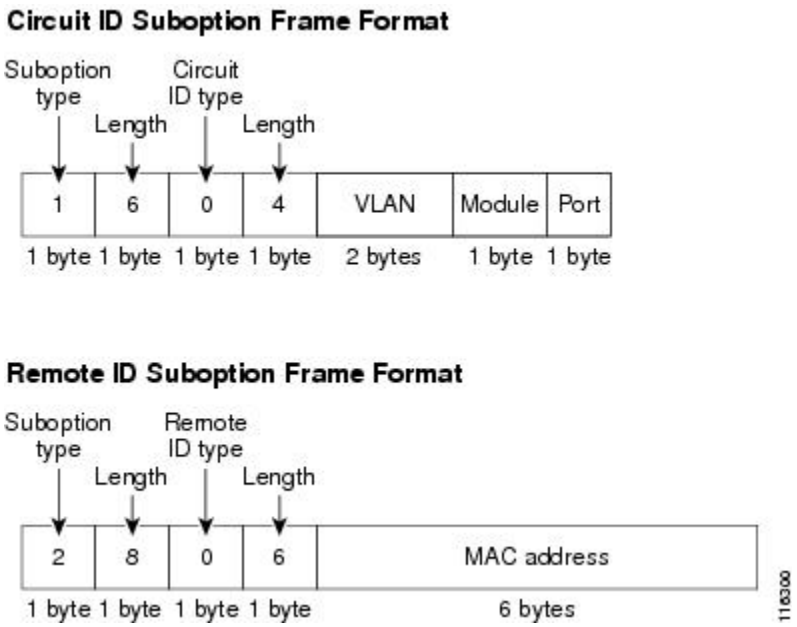
5 DHCP サーバは Cisco NX-OS デバイスに応答を送信します。Cisco NX-OS デバイスは、リモート ID フィールド、および場合によっては回線 ID フィールドを検査することで、最初に Option 82 データを挿入したのがこのデバイス自身であることを確認します。Cisco NX-OS デバイスは Option 82 フィールドを削除してから、DHCP 要求を送信した DHCP クライアントと接続しているインターフェイスにパケットを転送します。

上記の一連のイベントが発生した場合、次の値は変更されません。

- 回線 ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - 回線 ID タイプ
  - 回線 ID タイプの長さ
- リモート ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - リモート ID タイプ
  - 回線 ID タイプの長さ

次の図は、リモート ID サブオプションおよび回線 ID サブオプションのパケット形式を示しています。Cisco NX-OS デバイスがこのパケット形式を使用するのは、DHCP スヌーピングがグローバルにイネーブル化され、Option 82 データの挿入と削除がイネーブルに設定された場合です。回線 ID サブオプションの場合、モジュール フィールドはモジュールのスロット番号となります。

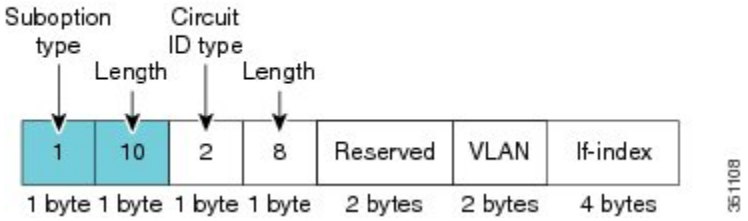
図 *24* : サブオプションのパケット形式

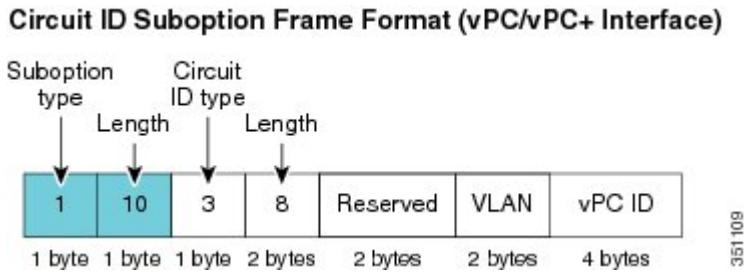


Cisco NX-OS Release 6.2(2) から開始され、Option 82 が DHCP スヌーピングでイネーブルにされたときに新しい回線 ID 形式が使用されます。新しい回線 ID 形式はデフォルトで使用されていて、ディセーブルにできません。しかし、新しい回線 ID 形式が IP アドレス割り当てに以前の Option 82 形式を使用している場合、これに対して DHCP サーバを設定する必要がある可能性があります。次の図は、Option 82 が DHCP スヌーピングに対してイネーブルなったときにレギュラ インターフェイスおよび vPC インターフェイスに対して使用される新しいデフォルト回線 ID 形式を示しています。

拡張 Option 82 形式は、DHCP パケットの処理を改善します。vPC および vPC+ インターフェイスに対して、別のポート チャネル番号で設定されたインターフェイスがあった場合のために、この新しい形式によって vPC ピアに一意の回線 ID が割り当てられます。

図 *25* : レギュラおよび *vPC* インターフェイスの回線 *ID* サブオプション フレーム形式





DHCP リレー エージェントの概要

DHCP リレー エージェント

DHCP リレー エージェントを実行するようにデバイスを設定できます。DHCP リレー エージェントは、クライアントとサーバの間で DHCP パケットを転送します。これは、クライアントとサーバが同じ物理サブネット上にない場合に便利な機能です。リレー エージェントは DHCP メッセージを受信すると、新規の DHCP メッセージを生成して別のインターフェイスに送信します。リレー エージェントはゲートウェイ アドレスを設定し（DHCP パケットの giaddr フィールド）、パケットにリレー エージェント情報のオプション（Option 82）を追加して（設定されている場合）、DHCP サーバに転送します。サーバからの応答は、Option 82 を削除してからクライアントに転送されます。

Option 82 をイネーブルにすると、デバイスはデフォルトでバイナリの ifindex 形式を使用します。必要に応じて Option 82 設定を変更して、代わりに符号化ストリング形式を使用できます。

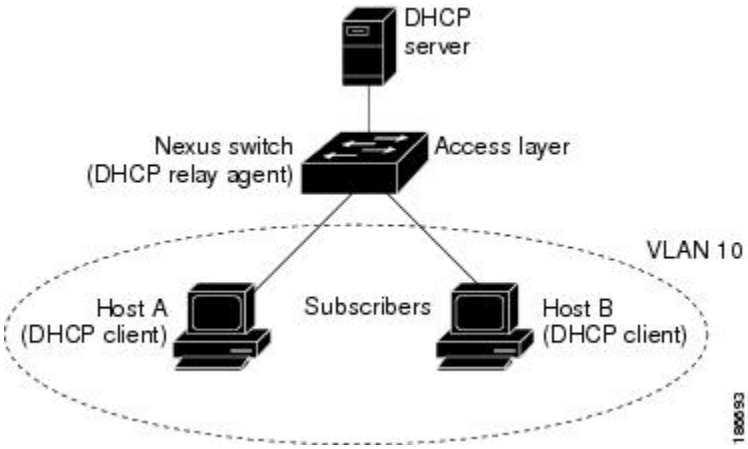
（注） デバイスは、Option 82 情報がすでに含まれている DHCP 要求を中継するときには、Option 82 情報を変更せずに元のままの状態で要求と一緒に転送します。

DHCP リレー エージェントの Option 82

リレー エージェントによって転送された DHCP パケットに関する Option 82 情報のデバイスでの挿入および削除をイネーブルにすることができます。

次の図のメトロポリタン イーサネット ネットワークでは、アクセス レイヤのデバイスに接続されている加入者に、DHCP サーバが IP アドレスを一元的に割り当てます。各 DHCP クライアントと、これらに関連付けられた DHCP サーバは、同一の IP ネットワークまたはサブネット内に存在しません。したがって、DHCP リレー エージェントをヘルパー アドレスによって設定することで、ブロードキャスト転送をイネーブルにし、クライアントとサーバ間で DHCP メッセージを転送します。

図 *26* : メトロポリタン イーサネット ネットワークにおける *DHCP* リレー エージェント



Cisco NX-OS デバイス上で DHCP リレー エージェントの Option 82 をイネーブルにすると、次の一連のイベントが発生します。

1 ホスト（DHCP クライアント）は DHCP 要求を生成し、これをネットワーク上にブロードキャストします。

2 Cisco NX-OS デバイスはこの DHCP 要求を受信すると、パケット内に Option 82 情報を追加します。Option 82 情報には、デバイスの MAC アドレス（リモート ID サブオプション）、およびパケットを受信したポートの識別子である vlan-mod-port（回線 ID サブオプション）が含まれます。DHCP リレーでは、回線 ID には、DHCP リレーが設定されている SVI またはレイヤ 3 インターフェイスの if_index が入力されます。

（注） vPC ピア デバイスの場合、リモート ID サブオプションには、両方のデバイスで一意である vPC デバイス MAC アドレスが含まれます。この MAC アドレスは vPC ドメイン ID とともに計算されます。Option 82 情報は、DHCP 要求が最初に受信されたデバイスで挿入された後、他の vPC ピア デバイスに転送されます。

3 デバイスは、DHCP パケットにリレー エージェントの IP アドレスを追加します。

4 デバイスは、Option 82 フィールドを含む DHCP 要求を DHCP サーバに転送します。

5 DHCP サーバはこのパケットを受信します。Option 82 に対応しているサーバであれば、このリモート ID、回線 ID、またはその両方を使用して、IP アドレスの割り当てやポリシーの適用を行うことができます。たとえば、単一のリモート ID または回線 ID に割り当てることのできる IP アドレスの数を制限するポリシーなどです。DHCP サーバは、DHCP 応答内に Option 82 フィールドをエコーします。

6 Cisco NX-OS デバイスがサーバへの要求を中継した場合、DHCP サーバはその NX-OS デバイスに応答をユニキャストします。Cisco NX-OS デバイスは、リモート ID フィールド、および場合によっては回線 ID フィールドを検査することで、最初に Option 82 データを挿入したのがこのデバイス自身であることを確認します。Cisco NX-OS デバイスは Option 82 フィールドを

削除してから、DHCP 要求を送信した DHCP クライアントと接続しているインターフェイスにパケットを転送します。

DHCP リレー エージェントに対する VRF サポート

DHCP ブロードキャスト メッセージを Virtual Routing and Forwarding（VRF; 仮想ルーティング/転送）インスタンスのクライアントから別の VRF の DHCP サーバに転送するように、DHCP リレー エージェントを設定できます。単一の DHCP サーバを使用して複数の VRF のクライアントの DHCP をサポートできるため、IP アドレス プールを VRF ごとではなく 1 つにまとめることにより、IP アドレスを節約できます。VRF の一般的な情報については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

DHCP リレー エージェントに対する VRF サポートをイネーブルにするには、DHCP リレー エージェントに対する Option 82 をイネーブルにする必要があります。

DHCP リレー アドレスと VRF 情報を設定したインターフェイスに DHCP 要求が着信した場合、DHCP サーバのアドレスが、別の VRF のメンバであるインターフェイスのネットワークに属するものであれば、デバイスは要求に Option 82 情報を挿入し、サーバの VRF の DHCP サーバにそれが転送されます。Option 82 情報は次のとおりです。

VPN 識別子

DHCP 要求を受信するインターフェイスが属する VRF の名前。

リンクの選択

DHCP 要求を受信するインターフェイスのサブネット アドレス。DHCP スマート リレーがイネーブルの場合、リンクの選択にはアクティブな giaddr のサブネットが指定されます。

サーバ識別子オーバーライド

DHCP 要求を受信するインターフェイスの IP アドレス。DHCP スマート リレーがイネーブルの場合、サーバの識別子にはアクティブな giaddr が指定されます。

（注） DHCP サーバは、VPN 識別子、リンクの選択、サーバ識別子オーバーライドの各オプションをサポートする必要があります。

デバイスは DHCP 応答メッセージを受信すると、Option 82 情報を取り除き、クライアントの VRF の DHCP クライアントに応答を転送します。

関連トピック

DHCP リレー エージェントに対する VRF サポートのイネーブル化またはディセーブル化, （711 ページ）

DHCP スマート リレー エージェント

DHCP リレー エージェントは、ホストからブロードキャスト DHCP 要求パケットを受信すると、インバウンド インターフェイスのプライマリ アドレスに giaddr を設定し、それらのパケットをサーバに転送します。サーバは、プールが使い果たされるまで giaddr サブネット プールから IP アドレスを割り当て、それ以降の要求を無視します。

Cisco NX-OS Release 5.2 から、最初のサブネット プールが使い果たされるか、またはサーバがそれ以降の要求を無視した場合は、セカンダリ IP アドレス サブネット プールから IP アドレスを割り当てるように DHCP スマート リレー エージェントを設定できます。この機能拡張は、ホストの数がプール内の IP アドレスの数を超えている場合や、セカンダリ アドレスを使用してインターフェイス上に複数のサブネットが設定されている場合に有効です。

関連トピック

DHCP スマート リレーのグローバルなイネーブル化またはディセーブル化, （716 ページ）
レイヤ 3 インターフェイスでの DHCP スマート リレーのイネーブル化またはディセーブル化, （717 ページ）

DHCPv6 リレー エージェントの概要

DHCPv6 リレー エージェント

DHCPv6 リレー エージェントを実行するようにデバイスを設定できます。DHCPv6 リレー エージェントは、クライアントとサーバの間で DHCP パケットを転送します。これは、クライアントとサーバが同じ物理サブネット上にない場合に便利な機能です。リレー エージェントは DHCPv6 メッセージを受信すると、新規の DHCPv6 メッセージを生成して別のインターフェイスに送信します。リレー エージェントはゲートウェイ アドレス（DHCPv6 パケットの giaddr フィールド）をセットし、DHCPv6 サーバに転送します。

DHCPv6 リレー エージェントに対する VRF サポート

DHCPv6 ブロードキャスト メッセージを仮想ルーティング/転送（VRF）インスタンスのクライアントから別の VRF の DHCPv6 サーバに転送するように、DHCPv6 リレー エージェントを設定できます。単一の DHCPv6 サーバを使用して複数の VRF のクライアントの DHCP をサポートできるため、IP アドレス プールを VRF ごとではなく 1 つにまとめることにより、IP アドレスを節約できます。VRF の一般的な情報については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

Lightweight DHCPv6 リレー エージェントについて

関連トピック

Lightweight DHCPv6 リレー エージェント, （688 ページ）
VLAN およびインターフェイスでの LDRA, （688 ページ）
Lightweight DHCPv6 リレー エージェントの注意事項と制約事項, （689 ページ）

Lightweight DHCPv6 リレー エージェント

1 つ以上のルータへの IPv6 ノードのアグリゲーションについては、さまざまなリンク レイヤ ネットワーク トポロジが存在します。単一リンク上に多数のノードを含むレイヤ 2 アグリゲーション ネットワーク（IEEE 802.1D ブリッジングまたは類似したもの）では、通常、DHCP バージョン 6（DHCPv6）サーバまたは DHCP リレー エージェントは、DHCP クライアントがネットワークに接続されている方式を認識していません。Cisco NX-OS Release 7.3(0)D1(1) 以降では、クライアントとサーバ間で DHCPv6 メッセージを転送する Lightweight DHCPv6 リレー エージェント（LDRA）を実行するようデバイスのインターフェイスを設定できます。

LDRA 機能は、主にクライアント向けインターフェイスを特定するため、DHCPv6 メッセージ交換にリレー エージェント オプションを挿入するために使用されます。LDRA は、クライアントおよび DHCPv6 リレー エージェントまたはサーバと同じ IPv6 リンク内に常駐します。

VLAN およびインターフェイスでの LDRA

LDRA は、VLAN およびインターフェイスで設定できます。LDRA はデフォルトではイネーブルになっていません。LDRA をイネーブルにする場合、グローバルおよびインターフェイス レベルでイネーブルにする必要があります。インターフェイスは、クライアント向け trusted、クライアント向け untrusted、またはサーバ向けとして設定する必要があります。クライアント向けインターフェイスはすべて、trusted または untrusted として設定する必要があります。デフォルトでは、LDRA 内のすべてのクライアント向けインターフェイスは、untrusted として設定されています。クライアント向けインターフェイスが untrusted とみなされると、LDRA はクライアント向けインターフェイスで受信された RELAY-FORWARD タイプのメッセージを破棄します。

VLAN では、LDRA 設定は、クライアント向け trusted、またはクライアント向け untrusted として設定する必要があります。VLAN で LDRA 機能を設定すると、この機能は VLAN 内のすべてのポートまたはインターフェイスで設定されます。ただし、VLAN 内のインターフェイスをクライアント向け untrusted として設定し、VLAN をクライアント向け trusted として設定すると、インターフェイスの設定が VLAN の設定に優先されます。VLAN 内の少なくとも 1 つのインターフェイスは、サーバ向けインターフェイスとして設定する必要があります。

Lightweight DHCPv6 リレー エージェントの注意事項と制約事項

- LDRA を実装しているアクセス ノードは、IPv6 制御またはルーティングをサポートしません。
- インターフェイスまたはポートを、同時にクライアント向けとサーバ向けの両方に設定することはできません。
- 仮想ポート チャネルをサポートするには、LDRA 設定は vPC ピア上で対称である必要があります。
- LDRA と DHCP スヌーピングの併用は、同じ VLAN ではサポートされません。
- LDRA は Cisco Fabricpath をサポートします。

UDP リレーについて

UDP リレー

デフォルトでは、ルータはブロードキャスト パケットを転送しません。ブロードキャスト パケットを転送するには、ルータの設定が必要です。Cisco NX-OS Release 7.3(0)D1(1) 以降では、UDP リレー機能を使用して、DHCPv4 ポート 67 および 68 を除く UDP ポート宛てのブロードキャストをリレーできます。UDP リレー機能は、IP ヘルパー機能とも呼ばれます。

（注） DHCP 要求の転送については、DHCP の設定, （677 ページ）を参照してください。

UDP リレーのイネーブル化

UDP リレー機能をイネーブルにするには、**ip forward-protocol udp** コマンドを使用します。デフォルトでは、UDP 機能はディセーブルになっています。次の UDP ポートは、**ip forward-protocol udp** コマンドを実行するとデフォルトでイネーブルになります。

- 簡易ファイル転送プロトコル（TFTP）（ポート 69）
- タイム サービス（ポート 37）
- NetBIOS ネーム サーバ（ポート 137）
- NetBIOS データグラム サーバ（ポート 138）
- TACACS サービス（ポート 49）
- IEN-116 ネーム サービス（ポート 42）

- Domain Naming System（ポート 53）

DHCPv4 UDP ポート 67 および 68 を除く、1 ～ 65535 の範囲内にある他の UDP ポートでも、UDP リレー機能をイネーブルまたはディセーブルにできます。

（注） UDP リレー機能をイネーブルにする前に、DHCP 機能をイネーブルにする必要があります。

パケットを転送するには、転送先の IP アドレスまたはネットワーク アドレスを使用して IP アドレス オブジェクト グループを設定し、その後、IP アドレス オブジェクト グループと L3 インターフェイスを関連付けます。サブネット ブロードキャストは、各レイヤ 3 インターフェイスでも設定できます。

UDP リレー機能は、次のタイプのレイヤ 3 インターフェイスでサポートされます。

- 物理ポート
- VLAN インターフェイス（SVI）
- L3 ポート チャネル
- L3 サブインターフェイス
- M1 および M2 FEX インターフェイス

DHCP リレーとは異なり、UDP ブロードキャスト パケットはラインカードでのみで使用されます。

UDP のサブネット ブロードキャスト

デフォルトでは、宛先のブロードキャスト パケットの UDP 転送はインターフェイスでイネーブルになっていません。**ip udp relay subnet-broadcast** コマンドを使用して、L3 またはスイッチ仮想インターフェイス（SVI）上で UDP リレー機能をイネーブルにすることができます。サブネット ブロードキャストをイネーブルにすると、次の条件を満たすすべての UDP パケットが転送されます。

- パケットは、IP レベルの宛先ブロードキャスト、つまり、インターフェイスのプライマリ サブネット ブロードキャストまたはいずれかのセカンダリ サブネット ブロードキャストである必要があります。
- パケットの宛先 UDP ポート番号は、デフォルト UDP ポートのいずれか、または **ip forward-protocol udp***udp-port-num* 設定コマンドを使用して指定されている他の UDP ポートのいずれかである必要があります。

サブネット ブロードキャストをイネーブルにしている場合は、ポリシーをそれぞれの L3 または SVI インターフェイスに対応して更新する必要があります。

UDP リレーの注意事項と制約事項

- UDP リレー機能は、M シリーズ ラインカードでのみサポートされます。
- 1 つのオブジェクト グループに許可される UDP 宛先アドレスの最大数は 300 です。
- 任意の L3 または SVI インターフェイスを最大 1 つのオブジェクト グループに関連付けることができます。したがって、任意のインターフェイスを最大 300 の UDP リレーの IP アドレスに関連付けることができます。
- UDP リレー機能は、7 つのデフォルト ポートを含む最大 200 の UDP ポートをサポートします。
- サブネットブロードキャストは、インターフェイスの最大2つのセカンダリ IPアドレス（プライマリ アドレス以外）に対してサポートされます。インターフェイスのセカンダリ IP アドレスはいくつでも設定できますが、UDP リレー ACL は、以下に対してのみプログラムされます。
  - ブロードキャスト アドレス（255.255.255.255）
  - インターフェイスのプライマリ アドレス
  - インターフェイスの 2 つのセカンダリ アドレス
- 宛先ごとの統計情報の表示はサポートされません。**internal** コマンドを使用して、ポリシーの ACL TCAM 統計情報を確認できます。
- 様々なインターフェイスでの個々の UDP リレー ポリシーの設定は次に依存します。
  - ラインカード
  - イネーブル化されているポートの UDP リレー機能
  - L3 または SVI インターフェイスでイネーブル化されているサブネット ブロードキャスト

DHCP の仮想化サポート

仮想デバイス コンテキスト（VDC）で使用される DHCP には、次の事項が該当します。

- DHCP スヌーピング バインディング データベースは各 VDC に固有です。ある VDC のバインディングが他の VDC の DHCP スヌーピングに影響することはありません。
- バインディング データベースのサイズは VDC 単位では制限されません。
- DHCP のスマート リレー エージェントは、デフォルトとデフォルト以外の VDC で個別に設定できます。

DHCP のライセンス要件

次の表に、DHCP のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	DHCP にはライセンスは不要です。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

DHCP の前提条件

DHCP の前提条件は、次のとおりです。

- DHCP スヌーピングまたは DHCP リレー エージェントを設定するためには、DHCP についての知識が必要です。

DHCP の注意事項と制約事項

DHCP 設定時の注意事項と制約事項は次のとおりです。

- クライアント vPC VLAN でのユニキャスト Reverse Packeting Forwarding（uRFP）ストリクト モードと、DHCP リレー機能による First-Hop Redundancy Protocol（FHRP）の両方を使用している場合、デフォルトで、DHCP 要求は（FHRP VIP ではなく）物理出力 IP アドレス インターフェイスから送信されます。その結果、DHCP サーバが直接接続されたサブネット上になく、vPC ペアに戻る複数の ECMP ルーティングがある場合、一部のパケットが、元のスイッチでなく隣接スイッチに到着し、RFP によってドロップされる場合があります。これは予想された動作です。このシナリオを回避するには、次のいずれかの回避策を実行します。
  - uRFP ストリクト モードの代わりに、uRFP ルーズ モードを使用する。
  - 影響を受ける FHRP インターフェイスのインターフェイスアドレスに対し、スタティック ルートを設定し、IGP にスタティック ルートを再配信する。
- Cisco NX-OS リリース 6.2 以降のリリースでは、最大の DHCP スヌーピングの規模をサポートするために、DHCP パケットに関する Option 82 情報の挿入をイネーブルにする必要があります。

- システム スイッチオーバー後、DHCP グローバル統計情報には不正な値が表示されます。それらの値は PSS に保存されておらず、消去されないためです。パケット パスの間に PSS で統計情報を更新すると、スケール に影響します。
- DHCP クライアントおよびサーバが異なる VRF インスタンスに存在する状況で DHCP リレーを使用する場合、VRF 内で 1 つの DHCP サーバだけを使用します。
- デバイス上で グローバルに DHCP スヌーピングをイネーブル化するには、DHCP サーバおよびDHCP リレーエージェントとして機能するデバイスを、事前に設定しイネーブルにしておく必要があります。
- ネットワーク内で、DHCP スヌーピングの後に DHCP リレーを配置しないでください。
- DHCP スヌーピングを使用して設定を行っている VLAN で VLAN ACL（VACL）が設定されている場合、その VACL で DHCP サーバと DHCP ホストの間の DHCP トラフィックが許可されていることを確認します。VLAN およびその VLAN の SVI 上で DHCP スヌーピングと DHCP リレーの両方がイネーブルになっていると、DHCP リレーが優先されます。
- DHCP サーバ アドレスを使用して設定を行っているレイヤ 3 インターフェイスで入力ルータ ACL が設定されている場合、そのルータ ACL で DHCP サーバと DHCP ホストの間の DHCP トラフィックが許可されていることを確認します。
- DHCP スヌーピング機能がイネーブルのときには、アクセス コントロール リスト（ACL）の統計情報はサポートされません。
- vPC リンク内のデバイス間で DHCP 設定が同期されていることを確認します。同期されていないと、ランタイム エラーが発生し、パケットがドロップされる場合があります。
- Cisco NX-OS Release 5.1 から、FabricPath で DHCP スヌーピングがサポートされます。FabricPath ネットワーク内で DHCP スヌーピングをイネーブルにする場合は、次の注意事項に従ってください。
  - DHCP スヌーピングは、CE-FabricPath 境界デバイス上でイネーブルにする必要があります。
  - アクセス レイヤ自体でネットワークを保護するために、DHCP スヌーピングはすべてのアクセス レイヤ デバイス上でイネーブルになっています。
  - ユーザがすべてのアクセス レイヤ デバイス上で DHCP スヌーピングをイネーブルにしているため、DHCP は、FabricPath モードではポート上のどのバインディング エントリも学習しません。その結果、DAI がイネーブルになっている場合、FabricPath ポート上で受信された ARP パケットは許可されます。
  - FabricPath モードでは、ポート上で IPSG をイネーブルにすることはできません。

（注） FabricPath の詳細については、『*Cisco Nexus 7000 Series NX-OS FabricPath Configuration Guide*』を参照してください。

- DHCP スマート リレーと DHCP サブネット ブロードキャストのサポートは、それがイネーブルにされているインターフェイスの最初の 100 個の IP アドレスに制限されます。
- DHCP スマート リレーと DHCP サブネット ブロードキャストのサポートを使用するには、インターフェイスでヘルパー アドレスを設定する必要があります。
- DHCP スマート リレーがイネーブルになっている vPC 環境では、インターフェイスのプライマリおよびセカンダリ アドレスのサブネットは、両方の Cisco NX-OS デバイスで同じである必要があります。
- インターフェイスで DHCPv6 サーバアドレスを設定する場合は、宛先インターフェイスをグローバル IPv6 アドレスで使用することはできません。

（注） DHCP 設定制限については、『*Cisco Nexus 7000 Series NX-OS Verified Scalability Guide*』を参照してください。

DHCP のデフォルト設定

次の表に、DHCP パラメータのデフォルト設定を示します。

表 *41*：デフォルトの *DHCP* パラメータ

パラメータ	デフォルト
DHCP 機能	ディセーブル
DHCP スヌーピング	ディセーブル
VLAN 上で DHCP スヌーピング	ディセーブル
DHCP スヌーピングの MAC アドレス検証	イネーブル
DHCP スヌーピングの Option 82 サポート	ディセーブル
DHCP スヌーピング信頼状態	信頼できない
DHCP リレー エージェント	イネーブル
DHCPv6 リレー エージェント	イネーブル
Lightweight DHCPv6 リレー エージェント	ディセーブル
UDP リレー機能	ディセーブル

パラメータ	デフォルト
DHCP リレーエージェントに対する VRF サポート	ディセーブル
DHCPv6 リレー エージェントに対する VRF サポート	ディセーブル
DHCP relay sub-option type cisco	ディセーブル
DHCPv6 relay option type cisco	ディセーブル
リレー エージェントの DHCP Option 82	ディセーブル
DHCP リレーエージェントに対するサブネット ブロードキャスト サポート	ディセーブル
DHCP スマート リレー エージェント	ディセーブル
DHCP サーバの IP アドレス	なし

DHCP の設定

DHCP の最小設定

ステップ 1 DHCP 機能をイネーブルにします。
DHCP 機能がディセーブルになっていると、DHCP スヌーピングを設定できません。

ステップ 2 DHCP スヌーピングをグローバルにイネーブルにします。

ステップ 3 少なくとも 1 つの VLAN で、DHCP スヌーピングをイネーブルにします。
デフォルトでは、DHCP スヌーピングはすべての VLAN でディセーブルになります。

ステップ 4 DHCP サーバとデバイスが、信頼できるインターフェイスを使用して接続されていることを確認します。

ステップ 5 （任意） DHCP サーバとクライアントが異なる VRF インスタンスに存在する場合は、次の手順に従います。

a) DHCP リレー エージェントの Option 82 をイネーブルにします。

b) DHCP リレー エージェントに対して VRF サポートをイネーブルにします。

ステップ 6 （任意） インターフェイスに DHCP サーバの IP アドレスを設定します。

関連トピック

DHCP 機能のイネーブル化またはディセーブル化, （696 ページ）
DHCP スヌーピングのグローバルなイネーブル化またはディセーブル化, （697 ページ）
VLAN に対する DHCP スヌーピングのイネーブル化またはディセーブル化, （698 ページ）
インターフェイスの信頼状態の設定, （703 ページ）
DHCP リレー エージェントのイネーブル化またはディセーブル化, （709 ページ）
DHCP リレー エージェントに対する Option 82 のイネーブル化またはディセーブル化, （710 ページ）
DHCP リレー エージェントに対する VRF サポートのイネーブル化またはディセーブル化, （711 ページ）
インターフェイスへの DHCP サーバ アドレスの設定, （714 ページ）

DHCP 機能のイネーブル化またはディセーブル化

デバイスのDHCP機能をイネーブルまたはディセーブルに設定できます。デフォルトでは、DHCPはディセーブルです。

DHCP 機能がディセーブルになっていると、DHCP スヌーピングや DHCP リレー エージェント、またはダイナミック ARP インスペクションおよび IP ソース ガードなどの DHCP に依存する機能の設定ができません。また、DHCP、ダイナミック ARP インスペクション、および IP ソース ガードの設定はすべてデバイスから削除されます。

手順の概要

1. **config t**
2. **[no] feature dhcp**
3. （任意） **showrunning-config dhcp**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**[no] feature dhcp** 例： `switch(config)# feature dhcp`	DHCP 機能をイネーブルにします。**no** オプションを使用すると、DHCP機能がディセーブルになり、DHCP設定が消去されます。

	コマンドまたはアクション	目的
ステップ 3	**showrunning-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

DHCP スヌーピングのグローバルなイネーブル化またはディセーブル化, （697 ページ）

DHCP スヌーピングのグローバルなイネーブル化またはディセーブル化

デバイスに対して DHCP スヌーピング機能のグローバルなイネーブル化またはディセーブル化が可能です。

はじめる前に

DHCP 機能がイネーブルになっていることを確認します。

手順の概要

1. **config t**
2. **[no] ip dhcp snooping**
3. （任意） **showrunning-config dhcp**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**[no] ip dhcp snooping** 例： `switch(config)# ip dhcp snooping`	DHCP スヌーピングをグローバルにイネーブル化します。**no** オプションを使用すると DHCP スヌーピングがディセーブルになります。
ステップ 3	**showrunning-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

DHCP 機能のイネーブル化またはディセーブル化, （696 ページ）

VLAN に対する DHCP スヌーピングのイネーブル化またはディセーブル化

1 つまたは複数の VLAN に対して DHCP スヌーピングをイネーブルまたはディセーブルに設定できます。デフォルトでは、DHCP スヌーピングはすべての VLAN でディセーブルになります。

はじめる前に

DHCP 機能がイネーブルになっていることを確認します。

（注） DHCP スヌーピングを使用して設定を行っている VLAN で VACL が設定されている場合、その VACL で DHCP サーバと DHCP ホストの間の DHCP トラフィックが許可されていることを確認します。

手順の概要

1. **config t**
2. **[no] ipdhcp snooping vlan** *vlan-list*
3. （任意） **showrunning-config dhcp**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **ipdhcp snooping vlan** *vlan-list* 例： `switch(config)# ip dhcp snooping vlan 100,200,250-252`	*vlan-list* で指定する VLAN の DHCP スヌーピングをイネーブルにします。**no** オプションを使用すると、指定した VLAN の DHCP スヌーピングがディセーブルになります。
ステップ 3	**showrunning-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

DHCP 機能のイネーブル化またはディセーブル化, （696 ページ）

DHCP スヌーピングの MAC アドレス検証のイネーブル化またはディセーブル化

DHCP スヌーピングの MAC アドレス検証をイネーブルまたはディセーブルにします。信頼できないインターフェイスからパケットを受信し、この送信元 MAC アドレスと DHCP クライアント ハードウェア アドレスが一致しない場合、アドレス検証によってデバイスはパケットをドロップします。MAC アドレス検証はデフォルトでイネーブルになります。

はじめる前に

DHCP 機能がイネーブルになっていることを確認します。

手順の概要

1. **config t**
2. **[no] ipdhcp snooping verify mac-address**
3. （任意） **showrunning-config dhcp**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**[no] ipdhcp snooping verify mac-address** 例： `switch(config)# ip dhcp snooping verify mac-address`	DHCP スヌーピングの MAC アドレス検証をイネーブルにします。**no** オプションを使用すると MAC アドレス検証がディセーブルになります。
ステップ 3	**showrunning-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

DHCP 機能のイネーブル化またはディセーブル化, （696 ページ）

Option 82 データの挿入および削除のイネーブル化またはディセーブル化

DHCP リレー エージェントを使用せずに転送された DHCP パケットへの Option 82 情報の挿入および削除をイネーブルまたはディセーブルにできます。デフォルトでは、デバイスはDHCPパケットに Option 82 情報を挿入しません。

（注） Option 82 に対する DHCP リレー エージェントのサポートは、個別に設定されます。

（注） より大きい DHCP pps の規模をサポートするには、DHCP パケットへの Option 82 情報の挿入をイネーブルにします。

はじめる前に

DHCP 機能がイネーブルになっていることを確認します。

手順の概要

1. **config t**
2. **[no] ip dhcp snooping information option**
3. （任意） **showrunning-config dhcp**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**[no] ip dhcp snooping information option** 例： `switch(config)# ip dhcp snooping information option`	DHCP パケットの Option 82 情報の挿入および削除をイネーブルにします。**no** オプションを使用すると、Option 82 情報の挿入および削除がディセーブルになります。
ステップ 3	**showrunning-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

DHCP 機能のイネーブル化またはディセーブル化, （696 ページ）
DHCP リレー エージェントに対する Option 82 のイネーブル化またはディセーブル化, （710 ページ）

DHCP パケットの厳密な検証のイネーブル化またはディセーブル化

DHCP パケットの厳密な検証をイネーブルまたはディセーブルにできます。デフォルトでは、DHCP パケットの厳密な検証はディセーブルになっています。

手順の概要

1. **config t**
2. **[no] ip dhcp packet strict-validation**
3. （任意） **showrunning-config dhcp**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**[no] ip dhcp packet strict-validation** 例： `switch(config)# ip dhcp packet strict-validation`	DHCP パケットの厳密な検証をイネーブルにします。**no** オプションを使用すると、DHCP パケットの厳密な検証がディセーブルになります。
ステップ 3	**showrunning-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスの信頼状態の設定

各インターフェイスが DHCP メッセージの送信元として信頼できるかどうかを設定できます。デフォルトでは、すべてのインターフェイスは信頼できません。DHCP の信頼状態は、次のタイプのインターフェイスに設定できます。

- レイヤ 2 イーサネット インターフェイス
- レイヤ 2 ポート チャネル インターフェイス

はじめる前に

DHCP 機能がイネーブルになっていることを確認します。

インターフェイスがレイヤ 2 インターフェイスとして設定されていることを確認します。

手順の概要

1. **config t**
2. 次のいずれかのオプションを使用します。
   - **interfaceethernet***slot*/*port*
   - **interfaceport-channel***channel-number*
3. [**no**] **ip dhcp snooping trust**
4. （任意） **showrunning-config dhcp**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	次のいずれかのオプションを使用します。
	• **interfaceethernet***slot*/*port*
	• **interfaceport-channel***channel-number*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		• インターフェイス コンフィギュレーション モードを開始します。*slot*/*port* は、DHCP スヌーピングで trusted または untrusted に設定するレイヤ 2 イーサネット インターフェイスです。
		• インターフェイス コンフィギュレーション モードを開始します。*slot*/*port* は、DHCP スヌーピングで trusted または untrusted に設定するレイヤ 2 ポート チャネル インターフェイスです。

	コマンドまたはアクション	目的
ステップ 3	**[no] ip dhcp snooping trust** 例： `switch(config-if)# ip dhcp snooping trust`	DHCP スヌーピングに関してインターフェイスを信頼できるインターフェイスとして設定します。**no** オプションを使用すると、ポートは信頼できないインターフェイスとして設定されます。
ステップ 4	**showrunning-config dhcp** 例： `switch(config-if)# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

DHCP 機能のイネーブル化またはディセーブル化, （696 ページ）

DHCP リレー信頼ポート設定機能のイネーブル化およびディセーブル化

DHCP リレー信頼ポート設定機能をイネーブルまたはディセーブルに設定できます。デフォルトでは、DHCP パケット内のゲートウェイ アドレスがすべてゼロに設定され、リレー情報オプションがすでにパケット内に存在する場合、DHCP リレー エージェントはパケットを廃棄しません。**ip dhcp relay information option trust** コマンドがグローバルに設定されていて、ゲートウェイ アドレスがすべてゼロに設定されている場合、DHCP リレーエージェントはパケットを廃棄します。

はじめる前に

DHCP 機能がイネーブルになっていることを確認します。

手順の概要

1. **config t**
2. **[no] ip dhcp relay information option trust**
3. （任意） **show ip dhcp relay**
4. （任意） **show ip dhcp relay information trusted-sources**
5. （任意） **showrunning-config dhcp**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **ip dhcp relay information option trust** 例： `switch(config)# ip dhcp relay information option trust`	DHCP リレー信頼ポート設定機能をイネーブルにします。**no** オプションを使用すると、この機能がディセーブルになります。
ステップ 3	**show ip dhcp relay** 例： `switch(config)# show ip dhcp relay`	（任意） DHCP リレーの設定を表示します。
ステップ 4	**show ip dhcp relay information trusted-sources** 例： `switch(config)# show ip dhcp relay information trusted-sources`	（任意） DHCP リレー信頼ポート設定を表示します。
ステップ 5	**showrunning-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスを DHCP リレーの信頼できるポートまたは信頼できないポートとして設定する

特定のレイヤ 3 インターフェイスを DHCP リレーにおいて信頼できるインターフェイスまたは信頼できないインターフェイスとして設定できます。デフォルトでは、すべてのインターフェイスは信頼できません。DHCP リレーの信頼状態は、次のタイプのインターフェイスで設定できます。

- レイヤ 3 イーサネット インターフェイスおよびサブインターフェイス
- レイヤ 3 ポート チャネル インターフェイス
- インターフェイス VLAN

はじめる前に

DHCP 機能がイネーブルになっていることを確認します。

手順の概要

1. **config t**
2. 次のいずれかのオプションを使用します。
   - **interfaceethernet***slot*/*port*.[*number*]
   - **interfaceport-channel***channel-number*.[*subchannel-id*]
   - **interfacevlan***vlan-id*
3. [**no**] **ip dhcp relay information trusted**
4. **show ip dhcp relay information trusted-sources**
5. （任意） **showrunning-config dhcp**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	次のいずれかのオプションを使用します。
	• **interfaceethernet***slot*/*port*.[*number*]
	• **interfaceport-channel***channel-number*.[*subchannel-id*]
	• **interfacevlan***vlan-id*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		• インターフェイス コンフィギュレーション モードを開始します。*slot*/*port* は、trusted または untrusted に設定するレイヤ 3 イーサネット インターフェイスです。
		• インターフェイス コンフィギュレーション モードを開始します。*channel-number* は、trusted または untrusted に設定するレイヤ 3 ポート チャネル インターフェイスです。
		• インターフェイス コンフィギュレーション モードを開始します。*vlan-id* は、trusted または untrusted に設定する VLAN インターフェイスです。

ステップ 3	[**no**] **ip dhcp relay information trusted** 例： `switch(config-if)# ip dhcp relay information trusted`	DHCP リレー エージェント情報に関して、インターフェイスを信頼できるインターフェイスとして設定します。**no** オプションを使用すると、ポートは信頼できないインターフェイスとして設定されます。

	コマンドまたはアクション	目的
		（注） L3 インターフェイスの場合、trusted に設定されたインターフェイスは、グローバル コマンドで設定されたかインターフェイス レベル コマンドで設定されたかに関係なく、信頼できるインターフェイスと見なされます。したがって、グローバル レベルで trusted-port コマンドをイネーブルにすると、インターフェイス レベルでの設定に関係なく、どの L3 インターフェイスも untrusted とは見なされなくなります。
ステップ 4	**show ip dhcp relay information trusted-sources** 例： `switch(config-if)# show ip dhcp relay information trusted-sources`	DHCP リレー信頼ポート設定を表示します。
ステップ 5	**showrunning-config dhcp** 例： `switch(config-if)# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

すべてのインターフェイスの信頼状態の設定

すべてのレイヤ 3 インターフェイスを DHCP リレーにおいて信頼できるインターフェイスまたは信頼できないインターフェイスとして設定することができます。デフォルトでは、すべてのインターフェイスは信頼できません。DHCP リレーの信頼状態は、次のタイプのインターフェイスで設定できます。

- レイヤ 3 イーサネット インターフェイスおよびサブインターフェイス
- レイヤ 3 ポート チャネル インターフェイス
- インターフェイス VLAN

ip dhcp relay information trust-all コマンドをイネーブルにすると、インターフェイス レベルでの設定に関係なく、すべてのレイヤ 3 インターフェイスが信頼できるものと見なされます。

はじめる前に

DHCP 機能がイネーブルになっていることを確認します。

手順の概要

1. **config t**
2. [**no**] **ip dhcp relay information trust-all**
3. **show ip dhcp relay information trusted-sources**
4. （任意） **showrunning-config dhcp**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **ip dhcp relay information trust-all** 例： `switch(config)# ip dhcp relay information trust-all`	指定したインターフェイスを DHCP メッセージの信頼できる送信元として設定します。**no** オプションを使用すると、ポートは信頼できないインターフェイスとして設定されます。
ステップ 3	**show ip dhcp relay information trusted-sources** 例： `switch(config)# show ip dhcp relay information trusted-sources`	DHCP リレー信頼ポート設定を表示します。
ステップ 4	**showrunning-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DHCP リレー エージェントのイネーブル化またはディセーブル化

DHCP リレー エージェントをイネーブルまたはディセーブルに設定できます。デフォルトでは、DHCP リレー エージェントはイネーブルです。

はじめる前に

DHCP 機能がイネーブルになっていることを確認します。

手順の概要

1. **config t**
2. **[no] ip dhcp relay**
3. （任意） **show ip dhcp relay**
4. （任意） **showrunning-config dhcp**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**[no] ip dhcp relay** 例： `switch(config)# ip dhcp relay`	DHCP リレー エージェントをイネーブルにします。**no** オプションを使用すると、リレーエージェントがディセーブルになります。
ステップ 3	**show ip dhcp relay** 例： `switch(config)# show ip dhcp relay`	（任意） DHCP リレーの設定を表示します。
ステップ 4	**showrunning-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

DHCP 機能のイネーブル化またはディセーブル化, （696 ページ）

DHCP リレー エージェントに対する Option 82 のイネーブル化またはディセーブル化

デバイスに対し、リレー エージェントによって転送された DHCP パケットへの Option 82 情報の挿入と削除をイネーブルまたはディセーブルにできます。

デフォルトでは、DHCP リレー エージェントは DHCP パケットに Option 82 情報を挿入しません。

手順の概要

1. **configure terminal**
2. **[no] ip dhcp relay**
3. **[no] ip dhcp relay information option**
4. （任意） **show ip dhcp relay**
5. （任意） **show running-config dhcp**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**[no] ip dhcp relay** 例： `switch(config)# ip dhcp relay`	DHCP リレー機能をイネーブルにします。**no** オプションを使用すると、この動作がディセーブルになります。
ステップ 3	**[no] ip dhcp relay information option** 例： `switch(config)# ip dhcp relay information option`	DHCP リレー エージェントによって転送されるパケットに対する Option 82 情報の挿入および削除をイネーブルにします。Option 82 情報は、デフォルトでバイナリ ifIndex 形式です。**no** オプションを使用すると、この動作がディセーブルになります。
ステップ 4	**show ip dhcp relay** 例： `switch(config)# show ip dhcp relay`	（任意） DHCP リレーの設定を表示します。

	コマンドまたはアクション	目的
ステップ 5	**show running-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） リブートおよびリスタート時に実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーして、変更を継続的に保存します。

DHCP リレー エージェントに対する VRF サポートのイネーブル化またはディセーブル化

ある VRF のインターフェイスで受信した DHCP 要求を、別の VRF インスタンスの DHCP サーバにリレーできるよう、デバイスを設定することができます。

はじめる前に

DHCP リレー エージェントの Option 82 をイネーブルにする必要があります。

手順の概要

1. **config t**
2. **[no] ip dhcp relay information option vpn**
3. **[no] ip dhcp relay sub-option type cisco**
4. （任意） **show ip dhcp relay**
5. （任意） **showrunning-config dhcp**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**[no] ip dhcp relay information option vpn** 例： `switch(config)# ip dhcp relay information option vpn`	DHCP リレーエージェントに対して VRF サポートをイネーブルにします。**no** オプションを使用すると、この動作がディセーブルになります。
ステップ 3	**[no] ip dhcp relay sub-option type cisco** 例： `switch(config)# ip dhcp relay sub-option type cisco`	リンク選択、サーバ ID オーバーライド、および VRF 名/VPN ID リレー エージェント Option 82 サブオプションを設定する場合は、DHCP をイネーブルにして、シスコ独自の番号である 150、152、および 151 を使用します。**no** オプションを使用すると、DHCP では、リンク選択、サーバ ID オーバーライド、および VRF 名/VPN ID サブオプションに対して、RFC 番号 5、11、151 が使用されるようになります。
ステップ 4	**show ip dhcp relay** 例： `switch(config)# show ip dhcp relay`	（任意） DHCP リレーの設定を表示します。
ステップ 5	**showrunning-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

DHCP リレー エージェントに対する VRF サポート，（686 ページ）
DHCP リレー エージェントに対する Option 82 のイネーブル化またはディセーブル化，（710 ページ）

レイヤ 3 インターフェイスの DHCP リレー エージェントに対するサブネット ブロードキャスト サポートのイネーブル化またはディセーブル化

クライアントからのサブネットのブロードキャスト IP アドレスに DHCP パケットのリレーをサポートするように、デバイスを設定できます。この機能がイネーブルの場合、VLAN ACL（VACL）

は、IP ブロードキャスト パケット、すべてのサブネット ブロードキャスト（プライマリ サブネット ブロードキャストおよびセカンダリ サブネット ブロードキャスト）パケットを許容します。

はじめる前に

DHCP 機能がイネーブルになっていることを確認します。

DHCP リレー エージェントがイネーブルであることを確認します。

手順の概要

1. **config t**
2. **interface** *interface slot*/*port*
3. [**no**] **ip dhcp relay subnet-broadcast**
4. **exit**
5. **exit**
6. （任意） **showip dhcp relay**
7. （任意） **showrunning-config dhcp**
8. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface** *interface slot*/*port*
	
	例：
	`switch(config)# interface ethernet 2/2`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。*slot*/*port* は、DHCP リレー エージェントに対するサブネット ブロードキャスト サポートをイネーブルまたはディセーブルにするインターフェイスです。

ステップ 3	[**no**] **ip dhcp relay subnet-broadcast** 例： `switch(config-if)# ip dhcp relay subnet-broadcast`	DHCP リレー エージェントに対するサブネット ブロードキャスト サポートをイネーブルにします。**no** オプションを使用すると、この動作がディセーブルになります。

ステップ 4	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的

ステップ 5	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 6	**showip dhcp relay** 例： `switch# show ip dhcp relay`	（任意） DHCP リレーの設定を表示します。
ステップ 7	**showrunning-config dhcp** 例： `switch# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 8	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスへの DHCP サーバ アドレスの設定

1 つのインターフェイスに複数の DHCP サーバ IP アドレスを設定できます。インバウンド DHCP BOOTREQUEST パケットがインターフェイスに着信すると、リレー エージェントはそのパケットを指定されたすべての DHCP サーバ IP アドレスに転送します。リレー エージェントは、すべての DHCP サーバからの応答を、要求を送信したホストへ転送します。

はじめる前に

DHCP 機能がイネーブルになっていることを確認します。

DHCP サーバが正しく設定されていることを確認します。

インターフェイスに設定する、各 DHCP サーバの IP アドレスを決定します。

DHCP サーバがインターフェイスとは異なる VRF インスタンスに含まれている場合、VRF サポートがイネーブルになっていることを確認します。

（注） DHCP サーバ アドレスを設定しているインターフェイスで入力ルータ ACL が設定されている場合、そのルータ ACL で DHCP サーバと DHCP ホストの間の DHCP トラフィックが許可されていることを確認します。

手順の概要

1. **config t**
2. 次のいずれかのオプションを使用します。
   - **interfaceethernet***slot*/*port*[**.***number*]
   - **interfacevlan***vlan-id*
   - **interfaceport-channel***channel-id*[*.subchannel-id*]
3. **ip dhcp relay address** *IP-address* [**use-vrf** *vrf-name*]
4. （任意） **showip dhcp relay address**
5. （任意） **showrunning-config dhcp**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	次のいずれかのオプションを使用します。
	• **interfaceethernet***slot*/*port*[**.***number*]
	• **interfacevlan***vlan-id*
	• **interfaceport-channel***channel-id*[*.subchannel-id*]
	
	例：
	`switch(config)# interface ethernet 2/3`
	`switch(config-if)#`
		• インターフェイス コンフィギュレーション モードを開始します。*slot*/*port* は、DHCP サーバ IP アドレスを設定する物理イーサネット インターフェイスです。サブインターフェイスを設定する場合は、*number* 引数を使用してサブインターフェイス番号を指定します。
		• インターフェイス コンフィギュレーション モードを開始します。*vlan-id* は、DHCP サーバ IP アドレスを設定する VLAN の ID です。
		• インターフェイス コンフィギュレーション モードを開始します。*channel-id* は、DHCP サーバ IP アドレスを設定するポート チャネルの ID です。サブチャネルを設定する場合は、*subchannel-id* 引数を使用してサブチャネル ID を指定します。

ステップ 3	**ip dhcp relay address** *IP-address* [**use-vrf** *vrf-name*] 例： `switch(config-if)# ip dhcp relay address 10.132.7.120 use-vrf red`	リレー エージェントがこのインターフェイスで受信した BOOTREQUEST パケットを転送する DHCP サーバの IP アドレスを設定します。

	コマンドまたはアクション	目的
		複数の IP アドレスを設定するには、アドレスごとに **ip dhcp relay address** コマンドを使用します。
ステップ 4	**showip dhcp relay address** 例： `switch(config-if)# show ip dhcp relay address`	（任意） 設定済みのすべての DHCP サーバアドレスを表示します。
ステップ 5	**showrunning-config dhcp** 例： `switch(config-if)# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

DHCP 機能のイネーブル化またはディセーブル化, （696 ページ）

DHCP スマート リレーのグローバルなイネーブル化またはディセーブル化

デバイスの DHCP スマート リレーをグローバルにイネーブルまたはディセーブルに設定できます。

はじめる前に

DHCP 機能がイネーブルになっていることを確認します。

DHCP リレー エージェントがイネーブルであることを確認します。

手順の概要

1. **config t**
2. **[no] ip dhcp smart-relay global**
3. （任意） **showip dhcp relay**
4. （任意） **showrunning-config dhcp**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **ip dhcp smart-relay global** 例： `switch(config)# ip dhcp smart-relay global`	DHCP スマート リレーをグローバルにイネーブルにします。**no**オプションを使用すると DHCP スマート リレーがディセーブルになります。
ステップ 3	**showip dhcp relay** 例： `switch(config)# show ip dhcp relay`	（任意） DHCP スマート リレー設定を表示します。
ステップ 4	**showrunning-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

レイヤ 3 インターフェイスでの DHCP スマート リレーのイネーブル化またはディセーブル化

レイヤ 3 インターフェイスで DHCP スマート リレーをイネーブルまたはディセーブルに設定できます。

はじめる前に

DHCP 機能がイネーブルになっていることを確認します。

DHCP リレー エージェントがイネーブルであることを確認します。

手順の概要

1. **config t**
2. **interface***interfaceslot*/*port*
3. [**no**] **ip dhcp smart-relay**
4. **exit**
5. **exit**
6. （任意） **showip dhcp relay**
7. （任意） **showrunning-config dhcp**
8. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface***interfaceslot*/*port*
	
	例：
	`switch(config)# interface ethernet 2/3`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。*slot*/*port* は、DHCP スマート リレーをイネーブルまたはディセーブルにするインターフェイスです。

ステップ 3	[**no**] **ip dhcp smart-relay** 例： `switch(config-if)# ip dhcp smart-relay`	インターフェイスで DHCP スマート リレーをイネーブルにします。**no** オプションを使用すると、インターフェイスの DHCP スマート リレーがディセーブルになります。

ステップ 4	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 5	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 6	**showip dhcp relay** 例： `switch# show ip dhcp relay`	（任意） DHCP スマート リレー設定を表示します。

	コマンドまたはアクション	目的
ステップ 7	**showrunning-config dhcp** 例： `switch# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 8	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DHCPv6 の設定

DHCPv6 リレー エージェントのイネーブル化またはディセーブル化

DHCPv6 リレーエージェントをイネーブルまたはディセーブルに設定できます。デフォルトでは、DHCPv6 リレー エージェントはイネーブルです。

はじめる前に

DHCP 機能がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. [**no**] **ipv6 dhcp relay**
3. （任意） **show ipv6 dhcp relay** [**interface** *interface*]
4. （任意） **showrunning-config dhcp**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	[**no**] **ipv6 dhcp relay** 例： `switch(config)# ipv6 dhcp relay`	DHCPv6 リレー エージェントをイネーブルにします。**no** オプションを使用すると、リレー エージェントがディセーブルになります。
ステップ 3	**show ipv6 dhcp relay** [**interface** *interface*] 例： `switch(config)# show ipv6 dhcp relay`	（任意） DHCPv6 リレーの設定を表示します。
ステップ 4	**showrunning-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DHCPv6 リレー エージェントに対する VRF サポートのイネーブル化またはディセーブル化

ある VRF のインターフェイスで受信した DHCPv6 要求を、別の VRF の DHCPv6 サーバにリレーする機能をサポートするように、デバイスを設定できます。

はじめる前に

DHCP 機能がイネーブルになっていることを確認します。

DHCPv6 リレー エージェントがイネーブルであることを確認します。

手順の概要

1. **configure terminal**
2. [**no**] **ipv6 dhcp relay option vpn**
3. [**no**] **ipv6 dhcp relay option type cisco**
4. （任意） **show ipv6 dhcp relay** [**interface** *interface*]
5. （任意） **showrunning-config dhcp**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **ipv6 dhcp relay option vpn** 例： `switch(config)# ipv6 dhcp relay option vpn`	DHCPv6 リレー エージェントに対して VRF サポートをイネーブルにします。**no** オプションを使用すると、この動作がディセーブルになります。
ステップ 3	[**no**] **ipv6 dhcp relay option type cisco** 例： `switch(config)# ipv6 dhcp relay option type cisco`	これにより、DHCPv6 リレー エージェントが、ベンダー固有オプションの一部として仮想サブネット選択（VSS）の詳細情報を挿入します。**no** オプションを使用すると、DHCPv6 リレー エージェントが VSS 詳細情報を、VSS オプションの一部として（68）挿入します。これは、RFC-6607 で定義された動作です。このコマンドは、RFC-6607 に対応していないものの、クライアント VRF 名に基づいた IPv6 アドレスを割り当てる DHCPv6 サーバを使用する場合に役立ちます。
ステップ 4	**show ipv6 dhcp relay** [**interface** *interface*] 例： `switch(config)# show ipv6 dhcp relay`	（任意） DHCPv6 リレーの設定を表示します。
ステップ 5	**showrunning-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスへの DHCPv6 サーバ アドレスの設定

1 つのインターフェイスに複数の DHCPv6 サーバ IP アドレスを設定できます。インバウンド DHCPv6 BOOTREQUEST パケットがインターフェイスに着信すると、リレー エージェントはそのパケットを指定されたすべての DHCP サーバ IP アドレスに転送します。リレー エージェントは、すべての DHCPv6 サーバからの応答を、要求を送信したホストへ転送します。

はじめる前に

DHCP 機能がイネーブルになっていることを確認します。

DHCPv6 サーバが正しく設定されていることを確認します。

インターフェイスに設定する、各 DHCPv6 サーバの IP アドレスを決定します。

DHCPv6 サーバがインターフェイスとは異なる VRF に含まれている場合、VRF サポートがイネーブルになっていることを確認します。

（注） DHCPv6 サーバ アドレスを設定しているインターフェイスで入力ルータ ACL が設定されている場合、そのルータ ACL で DHCP サーバと DHCPv6 ホストの間の DHCP トラフィックが許可されていることを確認します。

手順の概要

1. **config t**
2. 次のいずれかのオプションを使用します。
   - **interfaceethernet***slot*/*port*[**.***number*]
   - **interfaceport-channel***channel-id*[*.subchannel-id*]
3. [**no**] **ipv6 dhcp relay address***IPv6-address* [**use-vrf** *vrf-name*] [**interface** *interface*]
4. （任意） **show running-config dhcp**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**config t**
	
	例：
	`switch# config t`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	次のいずれかのオプションを使用します。
	• **interfaceethernet***slot*/*port*[**.***number*]
	• **interfaceport-channel***channel-id*[*.subchannel-id*]
	
	例：
	`switch(config)# interface ethernet 2/3`
	`switch(config-if)#`
		• インターフェイス コンフィギュレーション モードを開始します。*slot*/*port* は、DHCPv6 サーバ IP アドレスを設定する物理イーサネット インターフェイスです。サブインターフェイスを設定する場合は、*number* 引数を使用してサブインターフェイス番号を指定します。
		• インターフェイス コンフィギュレーション モードを開始します。*channel-id* は、DHCPv6 サーバ IP アドレスを設定するポート チャネルの ID です。サブチャネルを設

	コマンドまたはアクション	目的
		定する場合は、*subchannel-id* 引数を使用してサブチャネル ID を指定します。
ステップ 3	[**no**] **ipv6 dhcp relay address***IPv6-address* [**use-vrf** *vrf-name*] [**interface** *interface*] 例： `switch(config-if)# ipv6 dhcp relay address FF02:1::FF0E:8C6C use-vrf red`	リレー エージェントがこのインターフェイスで受信した BOOTREQUEST パケットを転送する DHCPv6 サーバの IP アドレスを設定します。 サーバが異なる VRF 上にあり、もう 1 つの interface 引数を使用して宛先の出力インターフェイスを指定する場合は、**use-vrf** オプションを使用してサーバの VRF 名を指定します。 サーバ アドレスには、リンクスコープのユニキャストまたはマルチキャスト アドレス、またはグローバルまたはサイトローカルのユニキャストまたはマルチキャスト アドレスを使用できます。リンクスコープのサーバ アドレスおよびマルチキャストアドレスを指定する場合、**interface** オプションは必須です。グローバルまたはサイトスコープのサーバ アドレスには許可されていません。 複数の IP アドレスを設定するには、アドレスごとに **ipv6 dhcp relay address** コマンドを使用します。
ステップ 4	**show running-config dhcp** 例： `switch(config-if)# show running-config dhcp`	（任意） DHCPv6 設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DHCPv6 リレー送信元インターフェイスの設定

DHCPv6 リレーエージェントの送信元インターフェイスを設定できます。デフォルトでは、DHCPv6 リレー エージェントは発信パケットの送信元アドレスとしてリレー エージェント アドレスを使用します。送信元インターフェイスを設定すると、リレーされたメッセージの送信元アドレスとして、より安定したアドレス（ループバック インターフェイス アドレスなど）を使用することができます。

はじめる前に

DHCP 機能がイネーブルになっていることを確認します。

DHCPv6 リレー エージェントがイネーブルであることを確認します。

手順の概要

1. **configure terminal**
2. [**no**] **ipv6 dhcp relay source-interface***interface*
3. （任意） **show ipv6 dhcp relay** [**interface** *interface*]
4. （任意） **showrunning-config dhcp**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **ipv6 dhcp relay source-interface***interface* 例： `switch(config)# ipv6 dhcp relay source-interface loopback 2`	DHCPv6 リレーエージェントの送信元インターフェイスを設定します。 （注） DHCPv6 リレー送信元インターフェイスは、グローバルに、インターフェイスごとに、またはその両方に設定できます。グローバルおよびインターフェイス レベルの両方が設定されている場合は、インターフェイス レベルの設定がグローバル設定を上書きします。
ステップ 3	**show ipv6 dhcp relay** [**interface** *interface*] 例： `switch(config)# show ipv6 dhcp relay`	（任意） DHCPv6 リレーの設定を表示します。
ステップ 4	**showrunning-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DHCP 設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Lightweight DHCPv6 リレー エージェントの設定

インターフェイスの Lightweight DHCPv6 リレー エージェントの設定

インターフェイスの Lightweight DHCPv6 リレー エージェント（LDRA）を設定するには、ここに示す手順を実行します。

手順の概要

1. **configure terminal**
2. **[no] ipv6 dhcp-ldra**
3. **interface***slot*/*port*
4. **switchport**
5. **[no] ipv6 dhcp-ldra{client-facing-trusted | client-facing-untrusted | client-facing-disable | server-facing}**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**[no] ipv6 dhcp-ldra** 例： `switch(config)# ipv6 dhcp-ldra`	LDRA 機能をグローバルにイネーブルにします。
ステップ 3	**interface***slot*/*port* 例： `switch(config)# interface ethernet 0/0`	インターフェイスのタイプおよび番号を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**switchport** 例： `switch(config-if)# switchport`	レイヤ 3 モードになっているインターフェイスを、レイヤ 2 設定用にレイヤ 2 モードに切り替えます。

	コマンドまたはアクション	目的
ステップ 5	**[no] ipv6 dhcp-ldra{client-facing-trusted | client-facing-untrusted | client-facing-disable | server-facing}** 例： `switch(config-if)# ipv6 dhcp-ldra server-facing`	指定したインターフェイスまたはポートの LDRA 機能をイネーブルにします。**no** オプションを指定すると、LDRA 機能がディセーブルになります。 （注） **client-facing-trusted** を使用すると、クライアント側のインターフェイスまたはポートが信頼できるポートとして設定されます。信頼できるポートでは DHCPv6 パケットの通過が許可され、LDRA オプションに基いてカプセル化されます。**client-facing-untrusted** を使用すると、クライアント側のインターフェイスまたはポートが信頼できないポートとして設定されます。信頼できないポートでは LDRA 機能が実行されますが、破棄されるのは LDRA に着信したリレー転送パケットのみです。**client-facing-disable** キーワードを使用すると、インターフェイスまたはポートの LDRA 機能がディセーブルになります。ディセーブルになったポートでは DHCPv6 パケットのレイヤ 2 転送が行われます。**server-facing** キーワードを使用すると、インターフェイスまたはポートがサーバ側ポートとして設定されます。サーバ側ポートではサーバからの応答パケットの通過が許可されます。

VLAN の Lightweight DHCPv6 リレー エージェントの設定

VLAN の DHCPv6 リレーエージェント（LDRA）を設定するには、ここに示す手順を実行します。

はじめる前に

VLAN に IP アドレスが割り当てられていないことを確認します。

手順の概要

1. **configure terminal**
2. **[no] ipv6 dhcp-ldra**
3. **[no] ipv6 dhcp-ldra attach–policyvlan***vlan-id***{client-facing-trusted | client-facing-untrusted}**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**[no] ipv6 dhcp-ldra** 例： `switch(config)# ipv6 dhcp-ldra`	LDRA 機能をグローバルにイネーブルにします。
ステップ 3	**[no] ipv6 dhcp-ldra attach–policyvlan***vlan-id***{client-facing-trusted | client-facing-untrusted}** 例： `switch(config)# ipv6 dhcp-ldra attach-policy vlan 25 client-facing-trusted`	指定した VLAN で LDRA 機能をイネーブルにします。**no** オプションを指定すると、LDRA 機能がディセーブルになります。 （注） **client-facing-trusted** キーワードを使用すると、VLANに関連付けられたすべてのポートまたはインターフェイスが、信頼できるクライアント側ポートとして設定されます。**client-facing-untrusted** キーワードを使用すると、VLANに関連付けられたすべてのポートまたはインターフェイスが、信頼できないクライアント側ポートとして設定されます。

UDP リレーの設定

はじめる前に

DHCP 機能がイネーブルになっていることを確認します。

ステップ 1 グローバル コンフィギュレーション モードを開始します。
switch# **configure terminal**

ステップ 2 UDP リレー機能をイネーブルにします。
switch(config)# **[no] ip forward-protocol udp**

（注） デフォルトでは、事前に定義された一連の UDP ポートで UDP リレー機能がイネーブルになっています。

ステップ 3 （任意） デフォルト以外の UDP ポートで UDP リレー機能をイネーブルにします。

switch(config)# **[no] ip forward-protocol udp***port-number*

（注） DHCP ポートを除く 1 ～ 65565 の範囲の任意の UDP ポートで UDP 転送をイネーブルまたはディセーブルにすることができます。

ステップ 4 パケットの転送先となる宛先 IP アドレスを設定します。
switch(config)# **[no] object-group udp relay ip addres***object-group-name*

ステップ 5 パケットの転送先となる宛先 IP アドレスで構成されるオブジェクト グループを設定します。
switch(config-udp-ogroup)# **[no]** {**host***host-addr*| *network-addr network-mask*| *network-addr/mask-length*}

（注） 作成するエントリごとに、**host** コマンドを使用して単一のホストを指定するか、または **host** コマンドを省略してホストのネットワークを指定します。

ステップ 6 オブジェクト グループのコンフィギュレーション モードを終了します。
switch(config-udp-ogroup)# **exit**

ステップ 7 L3 インターフェイスにオブジェクト グループを関連付けます。
switch(config)# **interface ethernet***slot/port*

switch(config-if)# **[no] ip udp relay addrgroup***object-group name*

（注） L3 インターフェイスは、物理ポート、インターフェイス VLAN（SVI）、L3 ポート チャネル、L3 サブインターフェイスのいずれでも構いません。

ステップ 8 インターフェイスに対してサブネット ブロードキャストを設定します。
switch(config-if)# **ip udp relay subnet-broadcast**

ステップ 9 インターフェイス コンフィギュレーション モードを終了します。
switch(config-if)# **exit**

UDP リレーの設定

この例では、UDP リレー機能を設定する際の実行コンフィギュレーションを示します。プレースホルダは実際の設定に応じた値に置き換えてください。

```
configure terminal
 feature dhcp
 ip forward-protocol udp
 object-group udp relay ip address <udprelay1>
   host <20.1.2.2>
   <30.1.1.1> <255.255.255.0>
   <10.1.1.1/24>
   exit
 interface ethernet <e1/1>
  ip udp relay addrgroup <udprelay1>
  ip udp relay subnet-broadcast
  exit
```

DHCP 設定の確認

DHCP の設定情報を表示するには、次のいずれかの作業を行います。これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

コマンド	目的
show running-config dhcp[**all**]	実行コンフィギュレーション内の DHCP 設定を表示します。
show ip dhcp relay	DHCP リレーの設定を表示します。
show ipv6 dhcp relay [**interface** *interface*]	DHCPv6 リレーのグローバル設定またはインターフェイス レベルの設定を表示します。
show ip dhcp relay address	デバイスに設定されているすべての DHCP サーバ アドレスを表示します。
show ip dhcp snooping	DHCP スヌーピングに関する一般的な情報を表示します。
show startup-config dhcp [**all**]	スタートアップ コンフィギュレーションの DHCP 設定を表示します。

DHCP バインディングの表示

DHCP バインディング テーブルを表示するには、**show ip dhcp snooping binding** コマンドを使用します。このコマンドの出力フィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

LDRA 情報の表示とクリア

Lightweight DHCPv6 リレー エージェント（LDRA）情報を表示するには、次の表に示すコマンドのいずれかを使用します。これらのコマンドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

コマンド	目的
show ipv6 dhcp-ldra	LDRA 設定の詳細を表示します。
show ipv6 dhcp-ldra statistics	DHCP セッションを開始する前と後の LDRA 設定の統計情報を表示します。

DHCPv6 LDRA 固有の統計情報をクリアするには、**clear ipv6 dhcp-ldra statistics** コマンドを使用します。

LDRA 統計情報の表示

次の例は、スイッチの LDRA 統計情報を表示します。

```
switch(config)# show ipv6 dhcp-ldra statistics
                DHCPv6 LDRA client facing statistics.
Messages received               2
Messages sent                   2
Messages discarded              0


Messages                        Received
SOLICIT                         1
REQUEST                         1

Messages                        Sent
RELAY-FORWARD                   2
                DHCPv6 LDRA server facing statistics.
Messages received               2
Messages sent                   2
Messages discarded              0


Messages                        Received
RELAY-REPLY                     2

Messages                        Sent
ADVERTISE                       1
REPLY                           1
```

UDP リレー情報の表示

UDP リレー情報を表示するには、次の表に示すコマンドのいずれかを使用します。これらのコマンドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

コマンド	目的
show ip udp relay	UDP リレー属性を表示します。
show ip udp relay interface [{*interface-type* | *interface-name* | *interface-range*}]	UDP リレー インターフェイス属性を表示します。

コマンド	目的
show ip udp relay object-group [*object-group-name*]	設定済みの UDP リレー オブジェクト グループと関連する IP アドレスまたはネットワーク アドレスを表示します。
show system internal udp-relay database	UDP リレーの詳細を表示します。

UDP リレー属性の表示

次の例は、UDP リレー属性を表示します。

```
switch# show ip udp relay
UDP relay service is enabled

UDP relay on default UDP ports:

  Default UDP Ports                        Status
 ---------------------------                  -------------
Time service                     (port 37 )      enabled
IEN-116 Name Service             (port 42 )      enabled
TACACS service                   (port 49 )      enabled
Domain Naming System             (port 53 )      enabled
Trivial File Transfer Protocol   (port 69 )      enabled
NetBIOS Name Server             (port 137)      enabled
NetBIOS Datagram Server          (port 138)      enabled

UDP relay is enabled on the following non-default UDP ports:
-----------------------------------------------------------------

Object-group and Subnet-broadcast configurations:
Interface   Subnet-broadcast  Object-group
----------  ----------------  ------------
Vlan700     disabled          Smart
Vlan800     enabled           Hello
```

UDP リレー インターフェイス属性の表示

次の例は、すべてのインターフェイスでの UDP リレー情報を表示します。

```
switch# show ip udp relay interface
UDP Relay is configured on the following interfaces:

Interface     Subnet-broadcast  Object-group
----------    ------------------ ------------
Vlan700        disabled           Smart
Vlan800        enabled            Hello
```

次の例は、指定したインターフェイス vlan800 での UDP リレー情報を表示します。

```
switch# show ip udp relay interface vlan 800
Interface     Subnet-broadcast  Object-group
----------    ----------------  -------------
Vlan 800        disabled          Smart
```

UDP リレー オブジェクト グループの表示

次の例は、すべての UDP リレー オブジェクト グループと関連する IP アドレスまたはネットワーク アドレスを表示します。

```
switch# show ip udp relay object-group
UDP Relay IPv4 address object-group NorthServer
```

```
        host 7.4.9.6
        10.20.30.40/24

UDP Relay IPv4 address object-group SouthServer
        host 3.4.5.6
        5.6.7.8/16
```

次の例は、指定した UDP リレー オブジェクト グループと関連する IP アドレスまたはネットワーク アドレスを表示します。

```
switch# show ip udp relay object-group galaxy
IPv4 address object-group galaxy
        host 3.4.5.6
        5.6.7.8/16
```

UDP リレー情報の表示

次の例は、UDP リレー詳細を表示します。

```
switch# show system internal udp-relay database

 UDP Relay enabled : Yes

 Relay enabled on the following UDP Ports:
 ------------------------------------------------------------------

 Sr No.    UDP-Port          Default Port?
 ------    ---------------   ----------------------
   1.        37                  Yes
   2.        42                  Yes
   3.        49                  Yes
   4.        53                  Yes
   5.        69                  Yes
   6.       137                 Yes
   7.       138                 Yes
  ----------------------------------------

 Object Groups information:
 ------------------------------------------

 ------------------------------------------------------------
 Object-Group Name      :  Hello
 No. of Relay Addresses :  3
    1 . IP-Addr : 2.6.8.12        Netmask : 255.255.255.255
    2 . IP-Addr : 9.8.7.6         Netmask : 255.255.255.255
    3 . IP-Addr : 2.4.6.8         Netmask : 255.255.0.0

 Associated Interfaces:
 ------------------------------------
    Vlan800             Subnet-broadcast enabled
 ------------------------------------------------------------------
 Object-Group Name      :  Smart
 No. of Relay Addresses :  1
    1 . IP-Addr : 4.5.6.7         Netmask : 255.255.0.0

 Associated Interfaces:
 ------------------------------------
    Vlan700             Subnet-broadcast disabled
```

DHCP スヌーピング バインディング データベースのクリア

DHCP スヌーピング バインディング データベースからエントリを削除できます。1 つのエントリ、インターフェイスに関連するすべてのエントリ、データベース内のすべてのエントリなどを削除することが可能です。

はじめる前に

DHCP 機能がイネーブルになっていることを確認します。

手順の概要

1. （任意） **clear ip dhcp snooping binding**
2. （任意） **clear ip dhcp snooping binding interface ethernet** *slot*/*port*[.*subinterface-number*]
3. （任意） **clear ip dhcp snooping binding interface port-channel** *channel-number*[.*subchannel-number*]
4. （任意） **clear ip dhcp snooping binding vlan** *vlan-id* **mac** *mac-address* **ip** *ip-address* **interface** {**ethernet** *slot*/*port*[.*subinterface-number* | **port-channel** *channel-number*[.*subchannel-number*] }
5. （任意） **show ip dhcp snooping binding**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**clear ip dhcp snooping binding** 例： `switch# clear ip dhcp snooping binding`	（任意） DHCP スヌーピング バインディング データベースからすべてのエントリをクリアします。
ステップ 2	**clear ip dhcp snooping binding interface ethernet** *slot*/*port*[.*subinterface-number*] 例： `switch# clear ip dhcp snooping binding interface ethernet 1/4`	（任意） DHCP スヌーピング バインディング データベースから、特定のイーサネット インターフェイスに関連するエントリをクリアします。
ステップ 3	**clear ip dhcp snooping binding interface port-channel** *channel-number*[.*subchannel-number*] 例： `switch# clear ip dhcp snooping binding interface port-channel 72`	（任意） DHCP スヌーピング バインディング データベースから、特定のポート チャネル インターフェイスに関連するエントリをクリアします。
ステップ 4	**clear ip dhcp snooping binding vlan** *vlan-id* **mac** *mac-address* **ip** *ip-address* **interface** {**ethernet** *slot*/*port*[.*subinterface-number* | **port-channel** *channel-number*[.*subchannel-number*] }	（任意） DHCP スヌーピング バインディング データベースから、特定のエントリをクリアします。

	コマンドまたはアクション	目的
	例： `switch# clear ip dhcp snooping binding vlan 23 mac 0060.3aeb.54f0 ip 10.34.54.9 interface ethernet 2/11`	
ステップ 5	**show ip dhcp snooping binding** 例： `switch# show ip dhcp snooping binding`	（任意） DHCP スヌーピング バインディング データベースを表示します。

関連トピック

DHCP 機能のイネーブル化またはディセーブル化, （696 ページ）

DHCP リレー統計情報のクリア

グローバル DHCP リレーの統計情報をクリアするには、**clear ip dhcp relay statistics** コマンドを使用します。

特定のインターフェイスの DHCP リレーの統計情報をクリアするには、**clear ip dhcp relay statistics interface** *interface* コマンドを使用します。

DHCPv6 リレー統計情報のクリア

グローバル DHCPv6 リレーの統計情報をクリアするには、**clear ipv6 dhcp relay statistics** コマンドを使用します。

特定のインターフェイスの DHCPv6 リレーの統計情報をクリアするには、**clear ipv6 dhcp relay statistics interface***interface* コマンドを使用します。

DHCP のモニタリング

DHCP スヌーピングをモニタするには、**show ip dhcp snooping statistics** コマンドを使用します。

show ip dhcp relay statistics[**interface***interface*] コマンドを使用して、グローバルまたはインターフェイス レベルでの DHCP リレー統計情報をモニタします。

show ip dhcp snooping statisticsvlan [*vlan-id*] **interface**[**ethernet**|*port-channel*][*id*] コマンド（オプション）を使用して、VLAN より下位のインターフェイス別のスヌーピング統計情報に関する正確な統計情報を確認します。

show ipv6 dhcp relay statistics[**interface***interface*] コマンドを使用して、グローバルまたはインターフェイス レベルでの DHCPv6 リレー統計情報をモニタします。

（注） これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

DHCP の設定例

次の例では、2 つの VLAN で DHCP スヌーピングをイネーブルにし、Option 82 のサポートをイネーブルにして、イーサネット インターフェイス 2/5 を trusted に設定して、DHCP サーバがこのインターフェイスに接続できるようにします。

```
feature dhcp
ip dhcp snooping
ip dhcp snooping info option

interface Ethernet 2/5
  ip dhcp snooping trust
ip dhcp snooping vlan 1
ip dhcp snooping vlan 50
```

次の例では、DHCP リレー エージェントをイネーブルにして、イーサネット インターフェイス 2/3 に DHCP サーバ IP アドレス（10.132.7.120）を設定します。DHCP サーバは red という名前の VRF インスタンス内にあります。

```
feature dhcp
ip dhcp snooping
ip dhcp relay
ip dhcp relay information option
ip dhcp relay information option vpn

interface Ethernet 2/3
  ip dhcp relay address 10.132.7.120 use-vrf red
```

次に、DHCP スマート リレー エージェントをイネーブルにして使用する例を示します。この例では、デバイスはイーサネット インターフェイス 2/2 上で受信された DHCP ブロードキャスト パケットを DHCP サーバ（10.55.11.3）に転送し、giaddr フィールド内に 192.168.100.1 を挿入します。DHCP サーバに 192.168.100.0/24 ネットワークのためのプールが設定されている場合、その DHCP サーバは応答します。サーバが応答しない場合、デバイスは giaddr フィールド内の 192.168.100.1 を使用して、さらに 2 つの要求を送信します。それでもデバイスが応答を受信しない場合は、代わりに giaddr フィールド内で 172.16.31.254 を使用し始めます。

```
feature dhcp
ip dhcp snooping
ip dhcp relay
ip dhcp smart-relay global

interface Ethernet 2/2
  ip address 192.168.100.1/24
  ip address 172.16.31.254/24 secondary
  ip dhcp relay address 10.55.11.3
```

LDRA の設定例

インターフェイスの LDRA の設定

次に、LDRA をイネーブル化し、イーサネット 1/1 インターフェイスをクライアント向け trusted として設定する例を示します。

```
switch# configure terminal
switch(config)# ipv6 dhcp-ldra
switch(config)# interface ethernet 1/1
switch(config-if)# switchport
switch(config-if)# ipv6 dhcp-ldra client-facing-trusted
```

VLAN 用 LDRA の設定

次に、LDRA をイネーブル化し、VLAN ID 25 の VLAN をクライアント向け trusted として設定する例を示します。

DHCP に関する追加情報

関連資料

関連項目	マニュアル タイトル
DHCP コマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト、使用上の注意事項、および例	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』
VRF およびレイヤ 3 のバーチャライゼーション	『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』
vPC	『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide*』

標準

標準	タイトル
RFC-2131	『Dynamic Host Configuration Protocol』（http://tools.ietf.org/html/rfc2131）
RFC-3046	『DHCP Relay Agent Information Option』（http://tools.ietf.org/html/rfc3046）

標準	タイトル
RFC-6607	Virtual Subnet Selection Options for DHCPv4 and DHCPv6 http://tools.ietf.org/html/rfc6607

DHCP の機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 *42*： *DHCP* の機能の履歴

機能名	リリース	機能情報
UDP リレー	7.3(0)D1(1)	UDP リレー機能のサポートが追加されました。
DHCP	7.3(0)D1(1)	Lightweight DHCPv6 リレーエージェント（LDRA）のサポートが追加されました。
DHCP	6.2(2)	DHCPv6 リレー エージェントのサポートが追加されました。
DHCP	6.2(2)	Option 82 が DHCP スヌーピングに対しイネーブルである場合に使用される、新しいデフォルトの回線 ID 形式が追加されました。
DHCP	6.0(1)	Release 5.2 以降、変更はありません。
DHCP	5.2(1)	DHCP スマート リレーのサポートが追加されました。
DHCP	5.2(1)	DHCP リレー エージェントのサブネット ブロードキャスト サポートが追加されました。

機能名	リリース	機能情報
DHCP	5.1(1)	vPC環境で動作する最適化 DHCP スヌーピング。
DHCP	5.0(2)	DHCP リレー エージェントが VRF をサポートするように変更されました。**ip dhcp relay information option vpn** コマンドが追加されました。**ip dhcp relay address** コマンドが変更され、**use-vrf***vrf-name* オプションが追加されました。
DHCP	5.0(2)	DHCP をイネーブルにして、リンク選択、サーバ ID オーバーライド、および VRF 名/VPN ID リレーエージェントの Option 82 サブオプションにシスコ独自の番号 150、152、および151 を使用できるようにするために、**ip dhcp relay sub-option type cisco** コマンドが追加されました。
DHCP	4.2(1)	**service dhcp** コマンドが廃止され、**ip dhcp relay** コマンドに置き換えられました。

第 20 章

ダイナミック ARP インスペクションの設定

この章では、Cisco NX-OS デバイスでダイナミック アドレス解決プロトコル（ARP）インスペクション（DAI）を設定する方法について説明します。

この章は、次の項で構成されています。

- 機能情報の確認，739 ページ
- DAI の概要，740 ページ
- DAI のライセンス要件，745 ページ
- DAI の前提条件，745 ページ
- DAI の注意事項と制約事項，745 ページ
- DAI のデフォルト設定，746 ページ
- DAI の設定，747 ページ
- DAI の設定の確認，754 ページ
- DAI の統計情報のモニタリングとクリア，755 ページ
- DAI の設定例，755 ページ
- ARP ACL の設定，762 ページ
- ARP ACL の設定の確認，767 ページ
- DAI に関する追加情報，768 ページ
- DAI の機能の履歴，768 ページ

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。こ

のモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

DAI の概要

ARP

ARP では、IP アドレスを MAC アドレスにマッピングすることで、レイヤ 2 ブロードキャスト ドメイン内の IP 通信を実現します。たとえば、ホスト B がホスト A に情報を送信しようとして、ホスト B の ARP キャッシュにホスト A の MAC アドレスがないという場合、ARP の用語では、ホスト B が送信者、ホスト A はターゲットになります。

ホスト B は、ホスト A の IP アドレスと関連付けられた MAC アドレスを取得するために、このブロードキャスト ドメインにあるホストすべてに対してブロードキャスト メッセージを生成します。このブロードキャスト ドメイン内のホストはすべて ARP 要求を受信し、ホスト A は MAC アドレスで応答します。

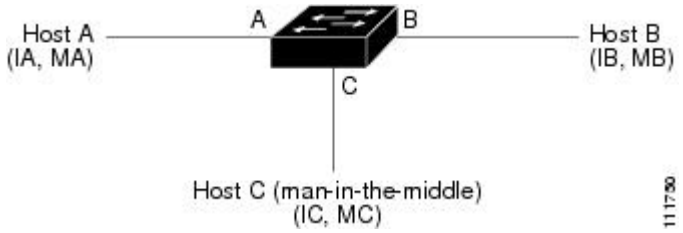
ARP スプーフィング攻撃

ARP では、たとえ ARP 要求を受信していなくても、ホストからの応答が可能なので、ARP スプーフィング攻撃と ARP キャッシュ ポイズニングが発生する可能性があります。攻撃が開始されると、攻撃を受けたデバイスからのすべてのトラフィックは、攻撃者のコンピュータを経由してルータ、スイッチ、またはホストに送信されるようになります。

ARP スプーフィング攻撃は、サブネットに接続されているデバイスの ARP キャッシュに偽りの情報を送信することにより、レイヤ 2 ネットワークに接続されているホスト、スイッチ、ルータに影響を及ぼす可能性があります。ARP キャッシュに偽りの情報を送信することを ARP キャッシュ ポイズニングといいます。スプーフ攻撃では、サブネット上の他のホストに対するトラフィックの代行受信も可能です。

次の図に、ARP キャッシュ ポイズニングの例を示します。

図 *27* : *ARP* キャッシュ ポイズニング



ホスト A、B、C は、それぞれインターフェイス A、B、C を介してデバイスに接続されています。これらのインターフェイスは同一サブネットに属します。カッコ内は、各ホストの IP および MAC

アドレスを示します。たとえば、ホスト A は IP アドレス IA、および MAC アドレス MA を使用します。ホスト A がホスト B に IP データを送信する必要がある場合、ホスト A は IP アドレス IB に関連付けられた MAC アドレスを求める ARP 要求をブロードキャストします。デバイスとホスト B はこの ARP 要求を受信すると、IP アドレス IA および MAC アドレス MA を持つホストの ARP バインディングを、それぞれの ARP キャッシュ内に書き込みます。たとえば、IP アドレス IA は MAC アドレス MA にバインドされます。ホスト B が応答すると、デバイスとホスト A は、IP アドレス IB および MAC アドレス MB を持つホストのバインディングを、それぞれの ARP キャッシュ内に書き込みます。

ホスト C は、バインディングを伴う 2 つの偽造 ARP 応答をブロードキャストすることにより、デバイス、ホスト A、ホスト B の ARP キャッシュをポイズニングできます。偽造 ARP 応答の 1 つは、IP アドレス IA と MAC アドレス MC を持つホストの応答、もう 1 つは IP アドレス IB と MAC アドレス MC を持つホストの応答です。これにより、ホスト B とデバイスは、IA を宛先とするトラフィックの宛先 MAC アドレスとして、MAC アドレス MC を使用します。つまり、ホスト C がこのトラフィックを代行受信することになります。同様に、ホスト A とデバイスは、IB を宛先とするトラフィックの宛先 MAC アドレスとして MAC アドレス MC を使用します。

ホスト C は IA および IB に関連付けられた本物の MAC アドレスを知っているため、正しい MAC アドレスを宛先として使用することで、代行受信したトラフィックをこれらのホストに転送できます。このトポロジでは、ホスト C は、ホスト A からホスト B へのトラフィック ストリーム内に自身を割り込ませています。これは、*man-in-the-middle* 攻撃の典型的な例です。

DAI および ARP スプーフィング攻撃

DAI を使用することで、有効な ARP 要求および応答だけがリレーされるようになります。DAI がイネーブルになり適切に設定されている場合、Cisco Nexus デバイスは次のアクティビティを実行します。

- 信頼できないポートを経由したすべての ARP 要求および ARP 応答を代行受信します。
- 代行受信した各パケットが、IP アドレスと MAC アドレスの有効なバインディングを持つことを確認してから、ローカル ARP キャッシュを更新するか、または適切な宛先にパケットを転送します。
- 無効な ARP パケットはドロップします。

DAI は DHCP スヌーピング バインディング データベースに保存された有効な IP アドレスと MAC アドレスのバインディングに基づいて、ARP パケットの有効性を判断します。このデータベースは、VLAN とデバイス上で DHCP スヌーピングがイネーブルにされている場合に、DHCP スヌーピングによって構築されます。また、このデータベースにはユーザが作成するスタティック エントリも保存できます。ARP パケットを信頼できるインターフェイス上で受信した場合は、デバイスはこのパケットを検査せずに転送します。信頼できないインターフェイス上では、デバイスは有効性を確認できたパケットだけを転送します。

DAI では、スタティックに設定した IP アドレスを持つホストに対し、ユーザ定義の ARP アクセス コントロール リスト（ACL）と照合することで ARP パケットを検証できます。ドロップしたパケットはログに記録されます。

DAI では、パケット内の IP アドレスが無効な場合に ARP パケットをドロップするのか、または ARP パケット本体の MAC アドレスがイーサネット ヘッダーに指定されたアドレスと一致しない場合に ARP パケットをドロップするのかを設定できます。

関連トピック

DAI フィルタリングを目的とした ARP ACL の VLAN への適用, （750 ページ）
DAI パケットのロギング, （744 ページ）
追加検証のイネーブル化またはディセーブル化, （751 ページ）

インターフェイスの信頼状態とネットワーク セキュリティ

DAI は、デバイスの各インターフェイスに信頼状態を関連付けます。信頼できるインターフェイス上で受信されたパケットは、DAI のすべての有効性検査をバイパスしますが、信頼できないインターフェイス上で受信されたパケットには、DAI の有効性検査が行われます。

一般的なネットワーク構成では、次のガイドラインに従ってインターフェイスの信頼状態を設定します。

Untrusted

ホストに接続されているインターフェイス

Trusted

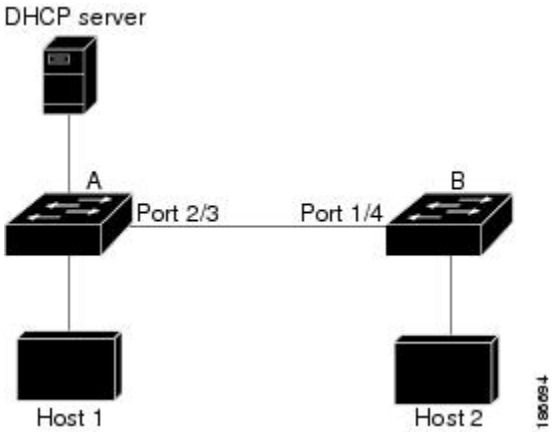
デバイスに接続されているインターフェイス

この設定では、デバイスからネットワークに送信される ARP パケットはすべて、セキュリティ検査をバイパスします。VLAN 内、またはネットワーク内のその他の場所では、他の検査を実行する必要はありません。

注意 信頼状態の設定は、慎重に行ってください。信頼すべきインターフェイスを信頼できないインターフェイスとして設定すると、接続が失われる場合があります。

次の図では、デバイス A およびデバイス B の両方が、ホスト 1 およびホスト 2 を収容する VLAN 上で DAI を実行していると仮定します。ホスト 1 およびホスト 2 が、デバイス A に接続されている DHCP サーバから IP アドレスを取得すると、デバイス A だけがホスト 1 の IP/MAC アドレスをバインドします。デバイス A とデバイス B 間のインターフェイスが信頼できない場合は、ホスト 1 からの ARP パケットはデバイス B ではドロップされ、ホスト 1 およびホスト 2 の間の接続は切断されます。

図 *28* : ***DAI*** をイネーブルにした ***VLAN*** での ***ARP*** パケット検証



信頼できないインターフェイスを信頼できるインターフェイスとして設定すると、ネットワークにセキュリティ ホールが生じる可能性があります。デバイス A が DAI を実行していなければ、ホスト 1 はデバイス B の ARP キャッシュを簡単にポイズニングできます（デバイス間のリンクが信頼できるものとして設定されている場合はホスト 2 も同様）。この状況は、デバイス B が DAI を実行している場合でも起こりえます。

DAI は、DAI が稼働するデバイスに接続されているホスト（信頼できないインターフェイス上）がネットワーク内の他のホストの ARP キャッシュをポイズニングしないように保証します。ただし、DAI が稼働するデバイスに接続されているホストのキャッシュがネットワークの他の部分のホストによってポイズニングされるのを防ぐことはできません。

VLAN 内の一部のデバイスで DAI が稼働し、他のデバイスでは稼働していない場合は、DAI が稼働しているデバイス上のインターフェイスの信頼状態を次のガイドラインに従って設定します。

Untrusted

ホスト、または DAI を実行していないデバイスに接続されているインターフェイス

Trusted

DAI が稼働しているデバイスに接続されているインターフェイス

DAI が稼働していないデバイスからのパケットのバインディングを検証するには、DAI が稼働しているデバイスに ARP ACL を設定します。バインディングの有効性を判断できない場合は、DAI が稼働しているデバイスを DAI が稼働していないデバイスからレイヤ 3 で隔離します。

（注） ネットワークの設定によっては、VLAN 内の一部のデバイスで ARP パケットを検証できない場合もあります。

関連トピック

レイヤ 2 インターフェイスの DAI 信頼状態の設定, （748 ページ）
例 2：1 つのデバイスが DAI をサポートする場合, （760 ページ）

ARP ACL および DHCP スヌーピング エントリのプライオリティ

デフォルトでは、DAI は DAI パケットを、DHCP スヌーピング データベース内の IP-MAC アドレス バインディングと照合することにより、DAI トラフィックをフィルタリングします。

ARP ACL をトラフィックに適用すると、その ARP ACL はデフォルトのフィルタリング動作よりも優先されます。デバイスはまず、ARP パケットを、ユーザが設定した ARP ACL と照合します。ARP ACL が ARP パケットを拒否した場合、DHCP スヌーピング データベースに有効な IP-MAC バインディングがあるかどうかに関係なく、デバイスはそのパケットを拒否します。

（注） VLAN ACL（VACL）は、ARP ACL と DHCP スヌーピング エントリのどちらよりも優先されます。たとえば、VACL と ARP ACL を VLAN に適用し、VACL が ARP トラフィックに作用するように設定した場合、デバイスは、ARP ACL や DHCP スヌーピングのエントリではなく、VACL に基づいて ARP トラフィックの許可または拒否を判断します。

関連トピック

ARP ACL の設定, （762 ページ）
DAI フィルタリングを目的とした ARP ACL の VLAN への適用, （750 ページ）

DAI パケットのロギング

Cisco NX-OS は処理された DAI パケットについてのログ エントリのバッファを維持しています。各ログエントリには、受信側の VLAN、ポート番号、送信元 IP アドレスおよび宛先 IP アドレス、送信元 MAC アドレスおよび宛先 MAC アドレスといったフロー情報が記録されます。

ログに記録するパケットのタイプを指定することもできます。デフォルトでは、Cisco Nexus デバイスは DAI がドロップしたパケットだけを記録します。

ログ バッファがあふれると、デバイスは最も古い DAI ログ エントリを新しいエントリで上書きします。バッファ内の最大エントリ数を設定できます。

（注） Cisco NX-OS は、ログに記録される DAI パケットに関するシステム メッセージを生成しません。

関連トピック

DAI のログ バッファ サイズの設定, （752 ページ）
DAI のログ フィルタリングの設定, （753 ページ）

DAI のバーチャライゼーション サポート

仮想デバイス コンテキスト（VDC）で使用される DAI には、次の事項が適用されます。

- IP-MAC アドレス バインディングは各 VDC に固有です。
- ARP ACL は各 VDC に固有です。ある VDC に作成した ACL は別の VDC に使用できません。
- ACL が複数の VDC に共有されることはないので、ACL 名は他の VDC に再利用できます。
- システムは、ARP ACL や ルールを VDC 単位では制限しません。

DAI のライセンス要件

次の表に、DAI のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	DAI にはライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

DAI の前提条件

- DHCP を設定するには、その前に DAI 機能をイネーブルにする必要があります。

DAI の注意事項と制約事項

DAI に関する注意事項と制約事項は次のとおりです。

- DAI は入力セキュリティ機能であり、出力検査は行いません。
- DAI は、DAI をサポートしないデバイス、またはこの機能がイネーブルにされていないデバイスに接続されているホストに対しては、効果がありません。man-in-the-middle 攻撃は 1 つのレイヤ 2 ブロードキャスト ドメインに限定されるため、DAI が有効なドメインを、DAI が実行されないドメインから切り離す必要があります。これにより、DAI が有効なドメイン内のホストの ARP キャッシュをセキュリティ保護できます。

- DAI では、着信 ARP 要求および ARP 応答内の IP アドレスと MAC アドレスとのバインディングを、DHCP スヌーピング バインディング データベース内のエントリに基づいて検証します。DAI が ARP パケットの有効性を判断するのにスタティック IP-MAC アドレス バインディングを使用するように設定する場合、DHCP スヌーピングの設定はイネーブルにするだけで済みます。DAI が ARP パケットの有効性を判断するのにダイナミック IP-MAC アドレス バインディングを使用するように設定する場合は、DAI を設定した VLAN と同じ VLAN に DHCP スヌーピングを設定する必要があります。
- **feature dhcp** コマンドを使用して DHCP 機能をイネーブルにすると、I/O モジュールが DHCP を受信する前、または DAI の設定前に約 30 秒の遅延が発生します。この遅延は、DHCP 機能がディセーブルになった設定から、DHCP 機能がイネーブルになった設定に変更するために使用する方式には関係なく発生します。たとえば、ロールバック機能を使用して、DHCP 機能をイネーブルにする設定に戻した場合、ロールバックを完了してから約 30 秒後に I/O モジュールが DHCP と DAI 設定を受信します。
- DHCP スヌーピングをディセーブルにしている場合、または DHCP 以外の環境では、ARP ACL を使用してパケットの許可および拒否を行う必要があります。
- DAI は、アクセス ポート、トランク ポート、ポート チャネル ポート、およびプライベート VLAN ポートでサポートされます。
- ポート チャネルに対する DAI の信頼設定によって、そのポート チャネルに割り当てたすべての物理ポートの信頼状態が決まります。たとえば、ある物理ポートを信頼できるインターフェイスとして設定し、信頼できないインターフェイスであるポート チャネルにその物理ポートを追加した場合、その物理ポートは信頼できない状態になります。
- ポート チャネルから物理ポートを削除した場合、その物理ポートはポート チャネルの DAI 信頼状態の設定を保持しません。
- ポート チャネルの信頼状態を変更すると、デバイスはそのチャネルを構成するすべての物理ポートに対し、新しい信頼状態を設定します。
- ARP パケットが有効かどうかを判定するために DAI でスタティック IP-MAC アドレス バインディングを使用するように設定する場合は、DHCP スヌーピングがイネーブルになっていること、およびスタティック IP-MAC アドレス バインディングを設定していることを確認します。
- ARP パケットが有効かどうかを判定するために DAI でダイナミック IP-MAC アドレス バインディングを使用するように設定する場合は、DHCP スヌーピングがイネーブルになっていることを確認します。

DAI のデフォルト設定

次の表に、DAI パラメータのデフォルト設定を示します。

表 *43* : デフォルトの *DAI* パラメータ

パラメータ	デフォルト
DAI	すべての VLAN でディセーブル。
インターフェイスの信頼状態	すべてのインターフェイスは untrusted。
非 DHCP 環境に対する ARP ACL	ARP ACL は定義されません。
有効性検査	検査は実行されません。
ログ バッファ	DAI をイネーブルにした場合は、拒否または廃棄されたすべての ARP パケットが記録されます。 ログ内のエントリ数は 32 です。 システム メッセージ数は、毎秒 5 つに制限されます。 ロギング レート インターバルは 1 秒です。
VLAN 単位のロギング	拒否または廃棄されたすべての ARP パケットが記録されます。

DAI の設定

VLAN での DAI のイネーブル化とディセーブル化

VLAN に対して DAI をイネーブルまたはディセーブルにすることができます。デフォルトでは、DAI はすべての VLAN でディセーブルです。

はじめる前に

DAI をイネーブルにする場合は、次の点を確認してください。

- DHCP 機能がイネーブルになっていることを確認します。
- DAI をイネーブルにする VLAN が設定されている。

手順の概要

1. **configure terminal**
2. [**no**] **ip arp inspection vlan***list*
3. （任意） **showip arp inspection vlan***list*
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **ip arp inspection vlan***list* 例： `switch(config)# ip arp inspection vlan 13`	VLAN の特定のリストに対して DAI をイネーブルにします。**no** オプションを使用すると、指定した VLAN の DAI がディセーブルになります。
ステップ 3	**showip arp inspection vlan***list* 例： `switch(config)# show ip arp inspection vlan 13`	（任意） VLAN の特定リストの DAI ステータスを表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

レイヤ 2 インターフェイスの DAI 信頼状態の設定

レイヤ 2 インターフェイスの DAI インターフェイス信頼状態を設定できます。デフォルトでは、すべてのインターフェイスは信頼できません。

デバイスは、信頼できるレイヤ 2 インターフェイス上で受信した ARP パケットを転送しますが、検査は行いません。

信頼できないインターフェイス上では、デバイスはすべての ARP 要求および ARP 応答を代行受信します。デバイスは、ローカル キャッシュをアップデートして、代行受信したパケットを適切な宛先に転送する前に、そのパケットの IP-MAC アドレス バインディングが有効かどうかを検証します。そのパケットのバインディングが無効であると判断すると、デバイスはそのパケットをドロップし、ロギングの設定に従ってログに記録します。

はじめる前に

DAI をイネーブルにする場合は、DHCP 機能がイネーブルであることを確認します。

手順の概要

1. **configure terminal**
2. **interface***typenumber/slot*
3. [**no**] **ip arp inspection trust**
4. （任意） **show ip arp inspection interface** *type number/slot*
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface***typenumber/slot*
	
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	[**no**] **ip arp inspection trust** 例： `switch(config-if)# ip arp inspection trust`	インターフェイスを、信頼できる ARP インターフェイスとして設定します。**no** オプションを使用すると、そのインターフェイスは信頼できない ARP インターフェイスとして設定されます。
ステップ 4	**show ip arp inspection interface** *type number/slot* 例： `switch(config-if)# show ip arp inspection interface ethernet 2/1`	（任意） 特定のインターフェイスの信頼状態および ARP パケット レートを表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

インターフェイスの信頼状態とネットワーク セキュリティ，（742 ページ）
DAI のログ フィルタリングの設定，（753 ページ）

DAI フィルタリングを目的とした ARP ACL の VLAN への適用

1 つまたは複数の VLAN に ARP ACL を適用できます。デバイスがパケットを許可するのは、ACL がそのパケットを許可する場合だけです。デフォルトでは、どの VLAN にも ARP ACL は適用されません。

はじめる前に

適用する ARP ACL が正しく設定されていることを確認します。

手順の概要

1. **configure terminal**
2. [**no**] **ip arp inspection filter** *acl-name* **vlan** *list*
3. （任意） **showip arp inspection vlan***list*
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **ip arp inspection filter** *acl-name* **vlan** *list* 例： `switch(config)# ip arp inspection filter arp-acl-01 vlan 100`	ARP ACL を VLAN のリストに適用します。あるいは、**no** オプションを使用している場合は、ARP ACL を VLAN のリストから削除します。
ステップ 3	**showip arp inspection vlan***list* 例： `switch(config)# show ip arp inspection vlan 100`	（任意） 特定の VLAN リストの DAI ステータスを表示します（ARP ACL が適用されているかどうかも含む）。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

ARP ACL の設定, （762 ページ）

追加検証のイネーブル化またはディセーブル化

ARP パケットの追加検証をイネーブルまたはディセーブルにできます。デフォルトでは、ARP パケットの追加検証はイネーブルになりません。追加検証が設定されていない場合、送信元 MAC アドレス、ARP パケットの IP/MAC バインディング エントリと照合する送信元 IP アドレスのチェックは、イーサネット送信元MACアドレス（ARP送信者のMACアドレスではない）と ARP 送信者の IP アドレスを使用して実行されます。

DAI は、IP アドレスと MAC アドレスとの無効なバインディングを持つ ARP パケットを代行受信、記録、および廃棄します。宛先MACアドレス、送信元および宛先IPアドレス、送信元MACアドレスに対し、追加検証をイネーブルにすることができます。

追加検証を実装するには、**ip arp inspection validate** コマンドで次のキーワードを使用します。

dst-mac

ARP 応答のイーサネット ヘッダー内の宛先 MAC アドレスを、ARP 本体のターゲット MAC アドレスと比較して検査します。イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、廃棄されます。

ip

ARP 本文をチェックして、無効な IP アドレスや予期しない IP アドレスがないかを確認します。アドレスには 0.0.0.0、255.255.255.255、およびすべての IP マルチキャスト アドレスが含まれます。送信元 IP アドレスはすべての ARP 要求および ARP 応答内で検査され、宛先 IP アドレスは ARP 応答内だけで検査されます。

src-mac

ARP 要求と応答のイーサネット ヘッダー内の送信元 MAC アドレスを、ARP 本体の送信者 MAC アドレスと比較して検査します。イネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、廃棄されます。

追加検証をイネーブルにする場合は、次の点に注意してください。

- 少なくとも 1 つのキーワードを指定する必要があります。指定するキーワードは、1 つでも、2 つでも、3 つすべてでもかまいません。
- 各 **ip arp inspection validate** コマンドにより、それまでに指定したコマンドの設定が置き換えられます。**ip arp inspection validate** コマンドによって src -mac および dst-mac 検証をイネーブルにし、2 つめの **ip arp inspection validate** コマンドで IP 検証をイネーブルにした場合は、2 つめのコマンドを入力した時点で src-mac と dst-mac の検証がディセーブルになります。

手順の概要

1. **configure terminal**
2. [**no**] **ip arp inspection validate** {[**src-mac**] [**dst-mac**] [**ip**]}
3. （任意） **show running-config dhcp**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **ip arp inspection validate** {[**src-mac**] [**dst-mac**] [**ip**]} 例： `switch(config)# ip arp inspection validate src-mac dst-mac ip`	追加の DAI 検証をイネーブルにします。あるいは、**no** オプションを使用して、追加の DAI 検証をディセーブルにします。
ステップ 3	**show running-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DAI の設定も含めて、DHCP スヌーピング設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DAI のログ バッファ サイズの設定

DAI のログ バッファ サイズを設定できます。デフォルトのバッファ サイズは 32 メッセージです。

手順の概要

1. **configure terminal**
2. [**no**] **ip arp inspection log-buffer entries***number*
3. （任意） **show running-config dhcp**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **ip arp inspection log-buffer entries***number* 例： `switch(config)# ip arp inspection log-buffer entries 64`	DAI のログ バッファ サイズを設定します。**no** オプションを使用すると、デフォルトのバッファ サイズ（32 メッセージ）に戻ります。設定できるバッファ サイズは、1 ～ 1024 メッセージです。
ステップ 3	**show running-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DAI の設定も含めて、DHCP スヌーピング設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DAI のログ フィルタリングの設定

DAI パケットを記録するかどうかをデバイスが判断する方法を設定できます。デフォルトでは、デバイスはドロップされる DAI パケットをログに記録します。

手順の概要

1. **configure terminal**
2. 次のいずれかのコマンドを入力します。
   - **ip arp inspection vlan***vlan-list***loggingdhcp-bindings all**
   - **ip arp inspection vlan***vlan-list***loggingdhcp-bindings none**
   - **ip arp inspection vlan***vlan-list***loggingdhcp-bindingspermit**
   - **no ip arp inspection vlan***vlan-list***loggingdhcp-bindings** {**all** | **none** | **permit**}
3. （任意） **show running-config dhcp**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	次のいずれかのコマンドを入力します。 • **ip arp inspection vlan***vlan-list***loggingdhcp-bindings all** • **ip arp inspection vlan***vlan-list***loggingdhcp-bindings none** • **ip arp inspection vlan***vlan-list***loggingdhcp-bindingspermit** • **no ip arp inspection vlan***vlan-list***loggingdhcp-bindings** {**all** | **none** | **permit**} 例： `switch(config)# ip arp inspection vlan 100 dhcp-bindings permit`	次のようにして、DAI ログ フィルタリングを設定します。**no** オプションを使用すると、DAI ログ フィルタリングが削除されます。 • DHCP バインディングに一致するすべてのパケットを記録します。 • DHCP バインディングに一致するパケットを記録しません。 • DHCP バインディングによって許可されるパケットを記録します。 • DAI ログ フィルタリングを削除します。
ステップ 3	**show running-config dhcp** 例： `switch(config)# show running-config dhcp`	（任意） DAI の設定も含めて、DHCP スヌーピング設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

DAI の設定の確認

DAI の設定情報を表示するには、次のいずれかの作業を行います。これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

コマンド	目的
show ip arp inspection	DAI のステータスを表示します。

コマンド	目的
show ip arp inspection interface ethernet	信頼状態を表示します。
show ip arp inspection vlan	特定の VLAN の DAI 設定を表示します。
show arp access-lists	ARP ACL を表示します。
show ip arp inspection log	DAI のログ設定を表示します。

DAI の統計情報のモニタリングとクリア

DAI の統計情報のモニタまたはクリアを行うには、次の表に示すコマンドを使用します。これらのコマンドの詳細については、Cisco Nexus デバイスの『*Security Command Reference*』を参照してください。

コマンド	目的
show ip arp inspection statistics	DAI の統計情報を表示します。
clear ip arp inspection statistics vlan <id>	DAI 統計情報をクリアします。

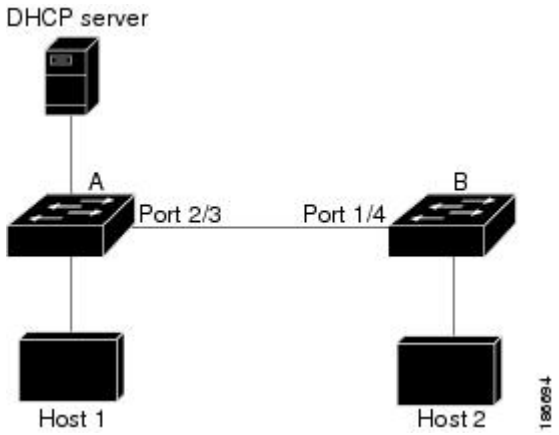
DAI の設定例

例 1：2 つのデバイスが DAI をサポートする場合

2 つのデバイスが DAI をサポートする場合の DAI の設定手順を次に示します。

次の図に、この例のネットワーク構成を示します。ホスト 1 はデバイス A に、ホスト 2 はデバイス B にそれぞれ接続されています。デバイスは両方とも、ホストが配置されている VLAN 1 で DAI を実行しています。DHCP サーバはデバイス A に接続されています。両方のホストは、同一の DHCP サーバから IP アドレスを取得します。デバイス A はホスト 1 およびホスト 2 のバインディングを持ち、デバイス B はホスト 2 のバインディングを持ちます。デバイス A のイーサネット インターフェイス 2/3 は、デバイス B のイーサネット インターフェイス 1/4 に接続されています。

図 *29*：*DAI* をサポートする *2* つのデバイス



DAI では、着信 ARP 要求および ARP 応答内の IP アドレスと MAC アドレスとのバインディングを、DHCP スヌーピング バインディング データベース内のエントリに基づいて検証します。IP アドレスを動的に割り当てられた ARP パケットを許可するには、DHCP スヌーピングをイネーブルにする必要があります。

- この構成は、DHCP サーバがデバイス A から別の場所に移動されると機能しません。
- この構成によってセキュリティが損なわれないようにするには、デバイス A のイーサネット インターフェイス 2/3、およびデバイス B のイーサネット インターフェイス 1/4 を、信頼できるインターフェイスとして設定します。

デバイス A の設定

デバイス A で DAI をイネーブルにし、イーサネット インターフェイス 2/3 を信頼できるインターフェイスとして設定するには、次の作業を行います。

ステップ 1 デバイス A にログインして、デバイス A とデバイス B の間の接続を確認します。

```
switchA# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute
Device ID              Local Intrfce   Hldtme  Capability  Platform      Port ID
switchB                Ethernet2/3     177     R S I    WS-C2960-24TC Ethernet1/4
switchA#
```

ステップ 2 VLAN 1 で DAI をイネーブルにし、設定を確認します。

```
switchA# config t
switchA(config)# ip arp inspection vlan 1
switchA(config)# show ip arp inspection vlan 1
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
```

```
IP Address Validation      : Disabled
Vlan : 1
-----------
Configuration   : Enabled
Operation State : Active
switchA(config)#
```

ステップ 3 イーサネット インターフェイス 2/3 を、信頼できるインターフェイスとして設定します。

```
switchA(config)# interface ethernet 2/3
switchA(config-if)# ip arp inspection trust
switchA(config-if)# exit
switchA(config)# exit
switchA# show ip arp inspection interface ethernet 2/3
 Interface        Trust State    Rate (pps)    Burst Interval
 -------------    -----------    ----------    --------------
 Ethernet2/3      Trusted           15             5
```

ステップ 4 バインディングを確認します。

```
switchA# show ip dhcp snooping binding
MacAddress          IpAddress        LeaseSec  Type           VLAN  Interface
------------------  ---------------  --------  -------------  ----  -------------
00:60:0b:00:12:89  10.0.0.1         0         dhcp-snooping  1     Ethernet2/3
switchA#
```

ステップ 5 DAI がパケットを処理する前、およびあとの統計情報を調べます。

```
switchA# show ip arp inspection statistics vlan 1
Vlan : 1
-----------
ARP Req Forwarded  = 0
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 0
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchA#
```

ホスト 1 が IP アドレス 10.0.0.1 および MAC アドレス 0002.0002.0002 を持つ 2 つの ARP 要求を送信すると、両方の要求が許可されます。これは、次の統計情報で確認できます。

```
switchA# show ip arp inspection statistics vlan 1
Vlan : 1
-----------
ARP Req Forwarded  = 2
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 2
```

```
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
```

ホスト 1 が、IP アドレス 10.0.0.3 を持つ ARP 要求を送信しようとすると、このパケットはドロップされ、エラー メッセージがログに記録されます。

```
00:12:08: %SW_DAI-4-DHCP_SNOOPING_DENY: 2 Invalid ARPs (Req) on Ethernet2/3, vlan
1.([0002.0002.0002/10.0.0.3/0000.0000.0000/0.0.0.0/02:42:35 UTC Fri Jul 13 2008])
```

この場合に表示される統計情報は次のようになります。

```
switchA# show ip arp inspection statistics vlan 1
switchA#
Vlan : 1
-----------
ARP Req Forwarded  = 2
ARP Res Forwarded  = 0
ARP Req Dropped    = 2
ARP Res Dropped    = 0
DHCP Drops         = 2
DHCP Permits       = 2
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchA#
```

デバイス B の設定

デバイス B で DAI をイネーブルにし、イーサネット インターフェイス 1/4 を信頼できるインターフェイスとして設定するには、次の作業を行います。

ステップ 1 デバイス B にログインして、デバイス B とデバイス A の間の接続を確認します。

```
switchB# show cdp neighbors
Capability Codes: R - Router, T - Trans-Bridge, B - Source-Route-Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater,
                  V - VoIP-Phone, D - Remotely-Managed-Device,
                  s - Supports-STP-Dispute
Device ID              Local Intrfce   Hldtme  Capability  Platform      Port ID
switchA                Ethernet1/4     120     R S I    WS-C2960-24TC Ethernet2/3
switchB#
```

ステップ 2 VLAN 1 で DAI をイネーブルにし、設定を確認します。

```
switchB# config t
switchB(config)# ip arp inspection vlan 1
switchB(config)# show ip arp inspection vlan 1
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
Vlan : 1
-----------
Configuration   : Enabled
Operation State : Active
switchB(config)#
```

ステップ 3 イーサネット インターフェイス 1/4 を、信頼できるインターフェイスとして設定します。

```
switchB(config)# interface ethernet 1/4
switchB(config-if)# ip arp inspection trust
switchB(config-if)# exit
switchB(config)# exit
switchB# show ip arp inspection interface ethernet 1/4
 Interface        Trust State    Rate (pps)    Burst Interval
 -------------    -----------    ----------    --------------
 Ethernet1/4      Trusted           15             5
switchB#
```

ステップ 4 DHCP スヌーピング バインディングのリストを確認します。

```
switchB# show ip dhcp snooping binding
MacAddress          IpAddress        LeaseSec  Type           VLAN  Interface
------------------  ---------------  --------  -------------  ----  -------------
00:01:00:01:00:01  10.0.0.2         4995      dhcp-snooping  1     Ethernet1/4
switchB#
```

ステップ 5 DAI がパケットを処理する前、およびあとの統計情報を調べます。

```
switchB# show ip arp inspection statistics vlan 1
Vlan : 1
-----------
ARP Req Forwarded  = 0
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 0
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchB#
```

ホスト 2 が、IP アドレス 10.0.0.2 および MAC アドレス 0001.0001.0001 を持つ ARP 要求を送信すると、このパケットは転送され、統計情報が更新されます。

```
switchB# show ip arp inspection statistics vlan 1
Vlan : 1
-----------
ARP Req Forwarded  = 1
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 1
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchB#
```

ホスト 2 が IP アドレス 10.0.0.1 を持つ ARP 要求を送信しようとすると、この要求はドロップされ、システム メッセージがログに記録されます。

```
00:18:08: %SW_DAI-4-DHCP_SNOOPING_DENY: 1 Invalid ARPs (Req) on Ethernet1/4, vlan
1.([0001.0001.0001/10.0.0.1/0000.0000.0000/0.0.0.0/01:53:21 UTC Fri Jun 13 2008])
```

この場合に表示される統計情報は次のようになります。

```
switchB# show ip arp inspection statistics vlan 1
Vlan : 1
-----------
ARP Req Forwarded  = 1
ARP Res Forwarded  = 0
ARP Req Dropped    = 1
ARP Res Dropped    = 0
DHCP Drops         = 1
DHCP Permits       = 1
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchB#
```

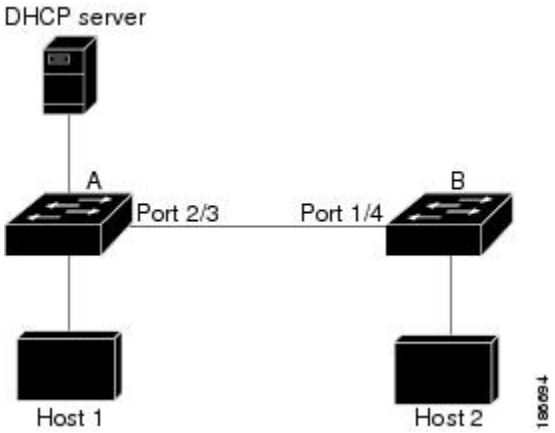
例 2：1 つのデバイスが DAI をサポートする場合

この手順では、ネットワーク設定に含まれる第 2 のデバイスが DAI または DHCP スヌーピングをサポートしない場合に、DAI を設定する方法を示します。

次の図に示されているデバイス B は、DAI または DHCP スヌーピングをサポートしていません。そのため、デバイス A のイーサネット インターフェイス 2/3 を信頼できるインターフェイスとして設定すると、セキュリティ ホールが生じます。これは、デバイス A およびホスト 1 が、デバイス B またはホスト 2 によって攻撃される可能性があるためです。

この可能性を排除するには、デバイス A のイーサネット インターフェイス 2/3 を信頼できないインターフェイスとして設定する必要があります。ホスト 2 からの ARP パケットを許可するには、ARP ACL をセットアップして、これを VLAN 1 に適用する必要があります。ホスト 2 の IP アドレスがスタティックではない場合は、デバイス A に ARP ACL 設定を正確に適用できなくなるため、レイヤ 3 でデバイス B からデバイス A を切り離す必要があります。これらのスイッチ間では、ルータを使用してパケットをルーティングします。

図 *30*：*DAI* をサポートする *1* つのデバイス



ステップ 1 IP アドレス 10.0.0.1 および MAC アドレス 0001.0001.0001 を許可するアクセス リストを設定して、設定内容を確認します。

```
switchA# config t
switchA(config)# arp access-list H2
switchA(config-arp-acl)# permit ip host 10.0.0.1 mac host 0001.0001.0001
switchA(config-arp-acl)# exit
switchA(config)# show arp access-lists H2
ARP access list H2
10 permit ip host 1.1.1.1 mac host 0001.0001.0001
switchA(config)#
```

ステップ 2 VLAN 1 に ACL を適用して、設定を確認します。

```
switchA(config)# ip arp inspection filter H2 vlan 1
switchA(config)# show ip arp inspection vlan 1
Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
Vlan : 200
-----------
Configuration    : Enabled
Operation State  : Active
```

```
ACL Match/Static : H2 / No
```

ステップ 3 イーサネット インターフェイス 2/3 を信頼できないインターフェイスとして設定し、設定内容を確認します。

（注） デフォルトでは、インターフェイスは信頼できない状態（untrusted）になります。

```
switchA(config)# interface ethernet 2/3
switchA(config-if)# no ip arp inspection trust
switchA(config-if)# exit
switchA# show ip arp inspection interface ethernet 2/3
switchA#
```

このインターフェイスはデフォルトの設定であり、信頼できない状態になっているので、**show ip arp inspection interface** コマンドでは出力は表示されません。

ホスト 2 がデバイス A のイーサネット インターフェイス 2/3 から 5 つの ARP 要求を送信し、1 つの get 要求がデバイス A によって許可された場合、統計情報は次のように更新されます。

```
switchA# show ip arp inspection statistics vlan 1
Vlan : 1
-----------
ARP Req Forwarded  = 5
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 0
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switchA#
```

ARP ACL の設定

ARP ACL に対する Session Manager のサポート

Session Manager は ARP ACL の設定をサポートしています。この機能を使用すると、設定セッションを作成し、ARP ACL の設定変更を実行コンフィギュレーションにコミットする前に確認できます。Session Manager の詳細については、『*Cisco Nexus 7000 Series NX-OS System Management Configuration Guide*』を参照してください。

ARP ACL の作成

デバイスに ARP ACL を作成し、これにルールを追加できます。

手順の概要

1. **configure terminal**
2. **arpaccess-list***name*
3. [*sequence-number*] {**permit** | **deny**} **ip** {**any** | **host***sender-IP* | *sender-IPsender-IP-mask*} **mac** {**any** | **host***sender-MAC* | *sender-MAC sender-MAC-mask*} [**log**]
4. [*sequence-number*] {**permit** | **deny**} **requestip** {**any** | **host***sender-IP* | *sender-IP sender-IP-mask*} **mac** {**any** | **host***sender-MAC*|*sender-MACsender-MAC-mask*} [**log**]
5. [*sequence-number*] {**permit** | **deny**} **responseip** {**any** | **host***sender-IP* | *sender-IP sender-IP-mask*} [**any** | **host***target-IP*|*target-IP target-IP-mask*]] **mac** {**any** | **host***sender-MAC* | *sender-MACsender-MAC-mask*} [**any** | **host***target-MAC* | *target-MAC target-MAC-mask*] [**log**]
6. （任意） **show arp access-lists***acl-name*
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**arpaccess-list***name*
	
	例：
	`switch(config)# arp access-list arp-acl-01`
	`switch(config-arp-acl)#`
		ARP ACL を作成し、ARP ACL コンフィギュレーション モードを開始します。

ステップ 3	[*sequence-number*] {**permit** | **deny**} **ip** {**any** | **host***sender-IP* | *sender-IPsender-IP-mask*} **mac** {**any** | **host***sender-MAC* | *sender-MAC sender-MAC-mask*} [**log**] 例： `switch(config-arp-acl)# permit ip 192.168.2.0 255.2555.255.0 mac 00C0.4F00.0000 ffff.ff00.0000`	メッセージ送信者の IP アドレスおよび MAC アドレスに基づいて、ARP メッセージを許可または拒否するルールを作成します。シーケンス番号を指定すると、ACL 内のルール挿入位置を指定できます。シーケンス番号を指定しないと、ルールは ACL の末尾に追加されます。
ステップ 4	[*sequence-number*] {**permit** | **deny**} **requestip** {**any** | **host***sender-IP* | *sender-IP sender-IP-mask*} **mac** {**any** | **host***sender-MAC*|*sender-MACsender-MAC-mask*} [**log**]	メッセージ送信者の IP アドレスおよび MAC アドレスに基づいて、ARP 要求メッセージを許可または拒否するルールを作成します。シーケンス番号を指定すると、ACL内のルール挿入位置を指定できます。シー

	コマンドまたはアクション	目的
	例： `switch(config-arp-acl)# permit request ip 192.168.102.0 0.0.0.255 mac any`	ケンス番号を指定しないと、ルールは ACL の末尾に追加されます。
ステップ 5	[*sequence-number*] {**permit** | **deny**} **responseip** {**any** | **host***sender-IP* | *sender-IP sender-IP-mask*} [**any** | **host***target-IP*|*target-IP target-IP-mask*]] **mac** {**any** | **host***sender-MAC* | *sender-MACsender-MAC-mask*} [**any** | **host***target-MAC* | *target-MAC target-MAC-mask*] [**log**] 例： `switch(config-arp-acl)# permit response ip host 192.168.202.32 any mac host 00C0.4FA9.BCF3 any`	メッセージの送信者およびターゲットの IPv4 アドレスおよび MAC アドレスに基づいて、ARP 応答メッセージを許可または拒否するルールを作成します。シーケンス番号を指定すると、ACL 内のルール挿入位置を指定できます。シーケンス番号を指定しないと、ルールは ACL の末尾に追加されます。
ステップ 6	**show arp access-lists***acl-name* 例： `switch(config-arp-acl)# show arp access-lists arp-acl-01`	（任意） ARP ACL の設定を表示します。
ステップ 7	**copy running-config startup-config** 例： `switch(config-arp-acl)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ARP ACL の変更

既存の ARP ACL のルールの変更および削除を実行できます。既存のルールは変更できません。ルールを変更するには、そのルールを削除してから、変更を加えたルールを再作成します。

既存のルールの間に新しいルールを挿入する必要がある場合で、現在のシーケンス番号の空き状況ではすべてを挿入できないときは、**resequence** コマンドを使用してシーケンス番号を再割り当てします。

手順の概要

1. **configure terminal**
2. **arpaccess-list***name*
3. （任意） [*sequence-number*] {**permit** | **deny**} [**request** | **response**] **ip***IP-data***mac***MAC-data*
4. （任意） **no** {*sequence-number* | {**permit** | **deny**}[**request** | **response**] **ip***IP-data***mac***MAC-data*
5. **showarpaccess-lists**
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**arpaccess-list***name*
	
	例：
	`switch(config)# arp access-list arp-acl-01`
	`switch(config-acl)#`
		名前を指定する ACL の ARP ACL コンフィギュレーション モードを開始します。

ステップ 3	[*sequence-number*] {**permit** | **deny**} [**request** | **response**] **ip***IP-data***mac***MAC-data* 例： `switch(config-arp-acl)# 100 permit request ip 192.168.132.0 255.2555.255.0 mac any`	（任意） ルールを作成します。 シーケンス番号を指定すると、ACL内のルール挿入位置を指定できます。シーケンス番号を指定しないと、ルールは ACL の末尾に追加されます。
ステップ 4	**no** {*sequence-number* | {**permit** | **deny**}[**request** | **response**] **ip***IP-data***mac***MAC-data* 例： `switch(config-arp-acl)# no 80`	（任意） 指定したルールを ARP ACL から削除します。
ステップ 5	**showarpaccess-lists** 例： `switch(config-arp-acl)# show arp access-lists`	ARP ACL の設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config-arp-acl)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

ARP ACL の作成, （763 ページ）
ARP ACL のシーケンス番号の変更, （767 ページ）

ARP ACL の削除

ARP ACL をデバイスから削除できます。

はじめる前に

その ACL が VLAN に適用されているかどうかを確認します。削除できるのは、現在適用されている ACL です。ACL を削除しても、その ACL が適用されている VLAN の設定には影響しません。デバイスは削除された ACL を空であると見なします。

手順の概要

1. **configure terminal**
2. **noarpaccess-list***name*
3. **showarpaccess-lists**
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**noarpaccess-list***name* 例： `switch(config)# no arp access-list arp-acl-01`	名前を指定した ARP ACL を実行コンフィギュレーションから削除します。
ステップ 3	**showarpaccess-lists** 例： `switch(config)# show arp access-lists`	ARP ACL の設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ARP ACL のシーケンス番号の変更

ARP ACL 内のルールに割り当てられているすべてのシーケンス番号を変更できます。

手順の概要

1. **configure terminal**
2. **resequencearp access-list** *name starting-sequence-numberincrement*
3. **showarpaccess-lists** *name*
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**resequencearp access-list** *name starting-sequence-numberincrement*
	
	例：
	`switch(config)# resequence arp access-list arp-acl-01 100 10`
	`switch(config)#`
		ACL 内に記述されているルールにシーケンス番号を付けます。指定した開始シーケンス番号が最初のルールに付けられます。後続の各ルールには、直前のルールよりも大きい番号が付けられます。番号の間隔は、指定した増分によって決まります。

ステップ 3	**showarpaccess-lists** *name* 例： `switch(config)# show arp access-lists arp-acl-01`	*name* 引数で指定した ACL の ARP ACL 設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ARP ACL の設定の確認

ARP ACL の設定情報を表示するには、次の表に示すコマンドを使用します。これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

コマンド	目的
show arp access-lists	ARP ACL の設定を表示します。
show running-config aclmgr	実行コンフィギュレーション内の ACL を表示します。

DAI に関する追加情報

関連資料

関連項目	マニュアル タイトル
DAI コマンド：完全なコマンド構文、コマンド モード、コマンド履歴、デフォルト値、使用上の注意、例	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』
DHCP スヌーピングのコマンド：完全なコマンド構文、コマンド モード、コマンド履歴、デフォルト値、使用上の注意、例	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』

標準

標準	タイトル
RFC-826	『An Ethernet Address Resolution Protocol』（http://tools.ietf.org/html/rfc826）

DAI の機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 *44*：*DAI* の機能の履歴

機能名	リリース	機能情報
ダイナミック ARP インスペクション	6.0(1)	Release 5.2 以降、変更はありません。

機能名	リリース	機能情報
ダイナミック ARP インスペクション	5.2(1)	Release 5.1 以降、変更はありません。
ダイナミック ARP インスペクション	5.1(1)	Release 5.0 以降、変更はありません。
ダイナミック ARP インスペクション	5.0(2)	Release 4.2 以降、変更はありません。
ダイナミック ARP インスペクション	4.2(1)	リリース 4.1 からの変更はありません。

第 21 章

IP ソース ガードの設定

この章では、Cisco NX-OS デバイスで IP ソース ガードを設定する手順について説明します。

この章は、次の項で構成されています。

- 機能情報の確認，771 ページ
- IP ソース ガードの概要，772 ページ
- IP ソース ガードのライセンス要件，773 ページ
- IP ソース ガードの前提条件，773 ページ
- IP ソース ガイドの注意事項と制約事項，773 ページ
- IP ソース ガードのデフォルト設定，774 ページ
- IP ソース ガードの設定，774 ページ
- IP ソース ガード バインディングの表示，776 ページ
- IP ソース ガードの設定例，776 ページ
- IP ソース ガードに関する追加情報，777 ページ
- IP ソース ガードの機能の履歴，777 ページ

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

IP ソース ガードの概要

IP ソース ガードは、インターフェイス単位のトラフィック フィルタです。各パケットの IP アドレスと MAC アドレスが、IP と MAC のアドレス バインディングのうち、次に示す 2 つの送信元のどちらかと一致する場合だけ、IP トラフィックを許可します。

- Dynamic Host Configuration Protocol（DHCP）スヌーピング バインディング テーブル内のエントリ
- 設定したスタティック IP ソース エントリ

信頼できる IP および MAC のアドレス バインディングのフィルタリングは、スプーフィング攻撃（有効なホストの IP アドレスを使用して不正なネットワーク アクセス権を取得する攻撃）の防止に役立ちます。IP ソース ガードを妨ぐためには、攻撃者は有効なホストの IP アドレスと MAC アドレスを両方スプーフィングする必要があります。

DHCP スヌーピングで信頼状態になっていないレイヤ 2 インターフェイスの IP ソース ガードをイネーブルにできます。IP ソース ガードは、アクセス モードとトランク モードで動作するように設定されているインターフェイスをサポートしています。IP ソース ガードを最初にイネーブルにすると、次のトラフィックを除いて、そのインターフェイス上のインバウンド IP トラフィックがすべてブロックされます。

- DHCP パケット。DHCP パケットは、DHCP スヌーピングによって検査が実行され、その結果に応じて転送またはドロップされます。
- Cisco NX-OS デバイスに設定したスタティック IP ソース エントリからの IP トラフィック。

デバイスが IP トラフィックを許可するのは、DHCP スヌーピングによって IP パケットの IP アドレスと MAC アドレスのバインディング テーブル エントリが追加された場合、またはユーザがスタティック IP ソース エントリを設定した場合です。

パケットの IP アドレスと MAC アドレスがバインディング テーブル エントリにも、スタティック IP ソース エントリにもない場合、その IP パケットはドロップされます。たとえば、**show ip dhcp snooping binding** コマンドによって、次のようなバインディング テーブル エントリが表示されるとします。

```
MacAddress          IpAddress    LeaseSec   Type         VLAN      Interface
------------------  -----------  ---------  -------      -------    ----------
00:02:B3:3F:3B:99   10.5.5.2       6943     dhcp-snooping  10      Ethernet2/3
```

IP アドレスが 10.5.5.2 の IP パケットをデバイスが受信した場合、IP ソース ガードによってこのパケットが転送されるのは、このパケットの MAC アドレスが 00:02:B3:3F:3B:99 のときだけです。

IP ソース ガードのバーチャライゼーション サポート

仮想デバイス コンテキスト（VDC）で使用される IP ソース ガードには、次の事項が適用されます。

- IP-MAC アドレス バインディングは各 VDC に固有です。ある VDC 内のバインディングが他の VDC の IP ソース ガードに影響を及ぼすことはありません。
- Cisco NX-OS は、バインディング データベースのサイズを VDC 単位では制限しません。

IP ソース ガードのライセンス要件

次の表に、IP ソース ガードのライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	IP ソース ガードにはライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

IP ソース ガードの前提条件

IP ソース ガードの前提条件は次のとおりです。

- DHCP 機能をイネーブルにする必要があります。

IP ソース ガイドの注意事項と制約事項

IP ソース ガードに関する注意事項と制約事項は次のとおりです。

- IP ソース ガードは、インターフェイス上の IP トラフィックを、IP-MAC アドレス バインディング テーブル エントリまたはスタティック IP ソース エントリに送信元が含まれているトラフィックだけに制限します。インターフェイス上の IP ソース ガードを初めてイネーブルにする際には、そのインターフェイス上のホストが DHCP サーバから新しい IP アドレスを受信するまで、IP トラフィックが中断されることがあります。
- IP ソース ガードの機能は、DHCP スヌーピング（IP-MAC アドレス バインディング テーブルの構築および維持に関して）、またはスタティック IP ソース エントリの手動での維持に依存しています。

IP ソース ガードのデフォルト設定

次の表に、IP ソース ガードのパラメータのデフォルト設定を示します。

表 *45* : *IP* ソース ガードのパラメータのデフォルト値

パラメータ	デフォルト
IP ソース ガード	各インターフェイスでディセーブル
IP ソース エントリ	なし。デフォルトではスタティック IP ソース エントリはありません。デフォルトの IP ソース エントリもありません。

IP ソース ガードの設定

レイヤ2インターフェイスに対するIP ソース ガードのイネーブル化またはディセーブル化

レイヤ2インターフェイスに対してIP ソース ガードをイネーブルまたはディセーブルに設定できます。デフォルトでは、すべてのインターフェイスに対して IP ソース ガードはディセーブルになっています。

はじめる前に

DHCP 機能がイネーブルになっていることを確認します。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port*
3. **[no] ip verify source dhcp-snooping-vlan**
4. （任意） **show running-config dhcp**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet***slot*/*port*
	
	例：
	`switch(config)# interface ethernet 2/3`
	`switch(config-if)#`
		指定したインターフェイスに対してインターフェイス コンフィギュレーション モードを開始します。

ステップ 3	[**no**] **ip verify source dhcp-snooping-vlan** 例： `switch(config-if)# ip verify source dhcp-snooping vlan`	インターフェイスの IP ソース ガードをイネーブルにします。**no** オプションを使用すると、そのインターフェイスの IP ソース ガードがディセーブルになります。
ステップ 4	**show running-config dhcp** 例： `switch(config-if)# show running-config dhcp`	（任意） IP ソース ガードの設定も含めて、DHCP スヌーピングの実行コンフィギュレーションを表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config-if)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

スタティック IP ソース エントリの追加または削除, （775 ページ）

スタティック IP ソース エントリの追加または削除

デバイス上のスタティック IP ソース エントリの追加または削除を実行できます。デフォルトでは、デバイスにはスタティック IP ソース エントリは設定されていません。

手順の概要

1. **configure terminal**
2. [**no**] **ip source binding** *IP-address MAC-address* **vlan** *vlan-ID* **interface ethernet** *slot*/*port*
3. （任意） **show ip dhcp snooping binding** [**interface ethernet***slot*/*port*]
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	[**no**] **ip source binding** *IP-address MAC-address* **vlan** *vlan-ID* **interface ethernet** *slot*/*port* 例： `switch(config)# ip source binding 10.5.22.17 001f.28bd.0013 vlan 100 interface ethernet 2/3`	現在のインターフェイスのスタティック IP ソース エントリを作成します。スタティック IP ソース エントリを削除する場合は、**no** オプションを使用します。
ステップ 3	**show ip dhcp snooping binding** [**interface ethernet***slot*/*port*] 例： `switch(config)# show ip dhcp snooping binding interface ethernet 2/3`	（任意） スタティック IP ソース エントリを含めて、指定したインターフェイスの IP-MAC アドレス バインディングを表示します。スタティック エントリは、Type カラムの表示で示されます。
ステップ 4	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

レイヤ 2 インターフェイスに対する IP ソース ガードのイネーブル化またはディセーブル化, （774 ページ）
IP ソース ガード バインディングの表示, （776 ページ）

IP ソース ガード バインディングの表示

IP-MAC アドレス バインディングを表示するには、**show ip verify source** コマンドを使用します。

IP ソース ガードの設定例

スタティック IP ソース エントリを作成し、インターフェイスの IP ソース ガードをイネーブルにする例を示します。

```
ip source binding 10.5.22.17 001f.28bd.0013 vlan 100 interface ethernet 2/3
interface ethernet 2/3
```

```
no shutdown
ip verify source dhcp-snooping-vlan
```

IP ソース ガードに関する追加情報

関連資料

関連項目	マニュアル タイトル
IP ソース ガード コマンド：完全なコマンド構文、コマンドモード、コマンド履歴、デフォルト値、使用上の注意、例	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

IP ソース ガードの機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 *46*：*IP* ソース ガードの機能の履歴

機能名	リリース	機能情報
IP ソース ガード	6.0(1)	Release 5.2 以降、変更はありません。
IP ソース ガード	5.2(1)	Release 5.1 以降、変更はありません。
IP ソース ガード	5.1(1)	Release 5.0 以降、変更はありません。
IP ソース ガード	5.0(2)	Release 4.2 以降、変更はありません。

機能名	リリース	機能情報
IP ソース ガード	4.2(1)	リリース 4.1 からの変更はありません。

第 22 章

パスワード暗号化の設定

この章では、Cisco NX-OS デバイスにパスワード暗号化を設定する手順について説明します。

この章は、次の項で構成されています。

- 機能情報の確認，779 ページ
- パスワード暗号化の概要，780 ページ
- パスワード暗号化のライセンス要件，780 ページ
- パスワード暗号化の注意事項と制約事項，781 ページ
- パスワード暗号化のデフォルト設定，781 ページ
- パスワード暗号化の設定，782 ページ
- パスワード暗号化の設定の確認，785 ページ
- パスワード暗号化の設定例，785 ページ
- パスワード暗号化に関する追加情報，786 ページ
- パスワード暗号化の機能の履歴，786 ページ

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

パスワード暗号化の概要

ここでは、Cisco NX-OS デバイスでのパスワード暗号化について説明します。

AES パスワード暗号化およびマスター暗号キー

強力で、反転可能な 128 ビットの高度暗号化規格（AES）パスワード暗号化（タイプ 6 暗号化ともいう）をイネーブルにすることができます。タイプ 6 暗号化の使用を開始するには、AES パスワード暗号化機能をイネーブルにし、パスワード暗号化および復号化に使用されるマスター暗号キーを設定する必要があります。

AES パスワード暗号化をイネーブルにしてマスター キーを設定すると、タイプ 6 パスワード暗号化をディセーブルにしない限り、サポートされているアプリケーション（現在は RADIUS と TACACS+）の既存および新規作成されたクリア テキスト パスワードがすべて、タイプ 6 暗号化の形式で保存されます。また、既存の弱いすべての暗号化パスワードをタイプ 6 暗号化パスワードに変換するように Cisco NX-OS を設定することもできます。

関連トピック

マスター キーの設定および AES パスワード暗号化機能のイネーブル化，（55 ページ）
グローバル RADIUS キーの設定，（86 ページ）
特定の RADIUS サーバ用のキーの設定，（87 ページ）
グローバル TACACS+ キーの設定，（124 ページ）
特定の TACACS+ サーバ用のキーの設定，（126 ページ）

パスワード暗号化の仮想化サポート

AES パスワード暗号化機能で使用するマスター キーは VDC ごとに一意です。

（注） VDC の詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

パスワード暗号化のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	パスワード暗号化にはライセンスは必要ありません。ライセンスパッケージに含まれていない機能はすべてCisco NX-OSシステムイメージにバンドルされており、追加費用は一切発生しません。 Cisco NX-OSライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

パスワード暗号化の注意事項と制約事項

パスワード暗号化設定時の注意事項と制約事項は次のとおりです。

- AES パスワード暗号化機能、関連付けられた暗号化と復号化のコマンド、およびマスターキーを設定できるのは、管理者権限（network-admin または vdc-admin）を持つユーザだけです。
- AES パスワード暗号化機能を使用できるアプリケーションは RADIUS と TACACS+ だけです。
- タイプ 6 暗号化パスワードを含む設定は、ロールバックに従いません。
- マスター キーがなくても AES パスワード暗号化機能をイネーブルにできますが、マスターキーがシステムに存在する場合だけ暗号化が開始されます。
- マスター キーを削除するとタイプ 6 暗号化が停止され、同じマスター キーが再構成されない限り、既存のすべてのタイプ 6 暗号化パスワードが使用できなくなります。
- Cisco NX-OS Release 5.2 から以前のリリースにダウングレードする前に、すべてのタイプ 6 パスワードを復号化し、AESパスワード暗号化機能をディセーブルにして、マスターキーを削除してください。
- デバイス設定を別のデバイスに移行するには、他のデバイスに移植する前に設定を復号化するか、または設定が適用されるデバイス上に同じマスター キーを設定します。

パスワード暗号化のデフォルト設定

次の表に、パスワード暗号化パラメータのデフォルト設定を示します。

表 *47* : パスワード暗号化パラメータのデフォルト設定

パラメータ	デフォルト
AES パスワード暗号化機能	ディセーブル
マスター キー	未設定

パスワード暗号化の設定

ここでは、Cisco NX-OS デバイスでパスワード暗号化を設定する手順について説明します。

（注） Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

マスターキーの設定および**AES**パスワード暗号化機能のイネーブル化

タイプ 6 暗号化用のマスター キーを設定し、高度暗号化規格（AES）パスワード暗号化機能をイネーブルにすることができます。

手順の概要

1. **[no] key config-key ascii**
2. **configure terminal**
3. **[no] feature password encryption aes**
4. （任意） **show encryption service stat**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ **1**	**[no] key config-key ascii**
	
	例：
	`switch# key config-key ascii`
	`New Master Key:`
	`Retype Master Key:`
		マスター キーを、AES パスワード暗号化機能で使用するように設定します。マスター キーは、16 ～ 32 文字の英数字を使用できます。このコマンドの **no** 形式を使用すると、いつでもマスター キーを削除できます。
		
		マスター キーを設定する前に AES パスワード暗号化機能をイネーブルにすると、マスター キーが設定されていない限りパスワード暗号化が実行されないことを示すメッセージが表示されます。マスター キーがすでに設定されている場合、新しいマス

	コマンドまたはアクション	目的
		ター キーを入力する前に現在のマスター キーを入力するように求められます。

ステップ 2	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 3	**[no] feature password encryption aes** 例： `switch(config)# feature password encryption aes`	AES パスワード暗号化機能をイネーブルまたはディセーブルにします。
ステップ 4	**show encryption service stat** 例： `switch(config)# show encryption service stat`	（任意） AES パスワード暗号化機能とマスター キーの設定ステータスを表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。 （注） このコマンドは、実行コンフィギュレーションとスタートアップ コンフィギュレーションのマスター キーを同期するために必要です。

関連トピック

AES パスワード暗号化およびマスター暗号キー，（39 ページ）
キーのテキストの設定，（794 ページ）
キーの受け入れライフタイムおよび送信ライフタイムの設定，（795 ページ）

既存のパスワードのタイプ 6 暗号化パスワードへの変換

既存の単純で脆弱な暗号化パスワードをタイプ 6 暗号化パスワードに変換できます。

はじめる前に

AES パスワード暗号化機能をイネーブルにし、マスター キーを設定したことを確認します。

手順の概要

1. **encryption re-encrypt obfuscated**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**encryption re-encrypt obfuscated** 例： `switch# encryption re-encrypt obfuscated`	既存の単純で脆弱な暗号化パスワードをタイプ 6 暗号化パスワードに変換します。

タイプ 6 暗号化パスワードの元の状態への変換

タイプ 6 暗号化パスワードを元の状態に変換できます。

はじめる前に

マスター キーを設定したことを確認します。

手順の概要

1. **encryption decrypt type6**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**encryption decrypt type6**
	
	例：
	`switch# encryption decrypt type6`
	`Please enter current Master Key:`
		タイプ 6 暗号化パスワードを元の状態に変換します。

タイプ 6 暗号化パスワードの削除

Cisco NX-OS デバイスからすべてのタイプ 6 暗号化パスワードを削除できます。

手順の概要

1. **encryption delete type6**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**encryption delete type6** 例： `switch# encryption delete type6`	すべてのタイプ 6 暗号化パスワードを削除します。

パスワード暗号化の設定の確認

パスワード暗号化の設定情報を表示するには、次の作業を行います。

コマンド	目的
show encryption service stat	AES パスワード暗号化機能とマスター キーの設定ステータスを表示します。

これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

パスワード暗号化の設定例

次に、マスター キーを作成し、AES パスワード暗号化機能をイネーブルにして、TACACS+ アプリケーションのためのタイプ 6 暗号化パスワードを設定する例を示します。

```
key config-key ascii
  New Master Key:
  Retype Master Key:
configure terminal
feature password encryption aes
show encryption service stat
  Encryption service is enabled.
  Master Encryption Key is configured.
  Type-6 encryption is being used.
feature tacacs+
tacacs-server key Cisco123
show running-config tacacs+
  feature tacacs+
  logging level tacacs 5
  tacacs-server key 6
"JDYkqyIFWeBvzpljSfWmRZrmRSRE8syxKlOSjP9RCCkFinZbJI3GD5c6rckJR/Qju2PKLmOewbheAA=="
```

パスワード暗号化に関する追加情報

ここでは、パスワード暗号化の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS ライセンス設定	『*Cisco NX-OS Licensing Guide*』
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

パスワード暗号化の機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 *48*：パスワード暗号化の機能の履歴

機能名	リリース	機能情報
パスワードの暗号化	6.0(1)	Release 5.2 以降、変更はありません。
パスワードの暗号化	5.2(1)	この機能が導入されました。

第 23 章

キーチェーン管理の設定

この章では、Cisco NX-OS デバイスでキーチェーン管理を設定する手順について説明します。

この章は、次の項で構成されています。

- 機能情報の確認，787 ページ
- キーチェーン管理の概要，788 ページ
- Licensing Requirements for Keychain Management，789 ページ
- キーチェーン管理の前提条件，789 ページ
- キーチェーン管理の注意事項と制約事項，790 ページ
- キーチェーン管理のデフォルト設定，790 ページ
- キーチェーン管理の設定，790 ページ
- アクティブなキーのライフタイムの確認，797 ページ
- キーチェーン管理の設定の確認，798 ページ
- キーチェーン管理の設定例，798 ページ
- 次の作業，798 ページ
- キーチェーン管理に関する追加情報，799 ページ
- キーチェーン管理の機能の履歴，799 ページ

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリス

トについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

キーチェーン管理の概要

キーチェーンおよびキーチェーン管理

キーチェーン管理を使用すると、キーチェーンの作成と管理を行えます。キーチェーンはキーのシーケンスを意味します（共有秘密ともいいます）。キーチェーンは、他のデバイスとの通信をキーベース認証を使用して保護する機能と合わせて使用できます。デバイスでは複数のキーチェーンを設定できます。

キーベース認証をサポートするルーティング プロトコルの中には、キーチェーンを使用してヒットレス キー ロールオーバーによる認証を実装できるものがあります。詳細については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

キーのライフタイム

安定した通信を維持するためには、キーベース認証で保護されるプロトコルを使用する各デバイスに、1 つの機能に対して同時に複数のキーを保存し使用できる必要があります。キーチェーン管理は、キーの送信および受け入れライフタイムに基づいて、キー ロールオーバーを処理するセキュアなメカニズムを提供します。デバイスはキーのライフタイムを使用して、キーチェーン内のアクティブなキーを判断します。

キーチェーンの各キーには次に示す 2 つのライフタイムがあります。

受け入れライフタイム

別のデバイスとのキー交換時にデバイスがそのキーを受け入れる期間。

送信ライフタイム

別のデバイスとのキー交換時にデバイスがそのキーを送信する期間。

キーの送信ライフタイムおよび受け入れライフタイムは、次のパラメータを使用して定義します。

Start-time

ライフタイムが開始する絶対時間。

End-time

次のいずれかの方法で定義できる終了時。

- ライフタイムが終了する絶対時間
- 開始時からライフタイムが終了するまでの経過秒数
- 無限のライフタイム（終了時なし）

キーの送信ライフタイム中、デバイスはルーティングアップデートパケットをキーとともに送信します。送信されたキーがデバイス上のキーの受け入れライフタイム期間内でない場合、そのデバイスはキーを送信したデバイスからの通信を受け入れません。

どのキーチェーンも、キーのライフタイムが重なるように設定することを推奨します。このようにすると、アクティブなキーがないことによるネイバー認証の失敗を避けることができます。

キーチェーン管理のバーチャライゼーション サポート

仮想デバイス コンテキスト（VDC）で使用されるキーチェーンには、次の事項が適用されます。

- キーチェーンは各 VDC に固有です。ある VDC で作成した キーチェーン は別の VDC に使用できません。
- キーチェーンが複数の VDC に共有されることはないので、キーチェーン名は他の VDC に再利用できます。
- デバイスは、キーチェーンを VDC 単位では制限しません。

Licensing Requirements for Keychain Management

This table shows the licensing requirements for keychain management.

Product	License Requirement
Cisco NX-OS	Keychain management requires no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For an explanation of the Cisco NX-OS licensing scheme, see the *Cisco NX-OS Licensing Guide*.

キーチェーン管理の前提条件

キーチェーン管理には前提条件はありません。

キーチェーン管理の注意事項と制約事項

キーチェーン管理に関する注意事項と制約事項は次のとおりです。

- システム クロックを変更すると、キーがアクティブになる時期に影響が生じます。

キーチェーン管理のデフォルト設定

次の表に、Cisco NX-OS キーチェーン管理パラメータのデフォルト設定を示します。

表 *49*：キーチェーン管理パラメータのデフォルト値

パラメータ	デフォルト
キー チェーン	デフォルトではキーチェーンはありません。
キー	デフォルトでは新しいキーチェーンの作成時にキーは作成されません。
受け入れライフタイム	常に有効です。
送信ライフタイム	常に有効です。
キーストリング入力の暗号化	暗号化されません。

キーチェーン管理の設定

キーチェーンの作成

デバイスにキーチェーンを作成できます。新しいキーチェーンには、キーは含まれていません。

手順の概要

1. **configure terminal**
2. **keychain***name*
3. （任意） **show key chain***name*
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**keychain***name*
	
	例：
	`switch(config)# key chain glbp-keys`
	`switch(config-keychain)#`
		キーチェーンを作成し、キーチェーン コンフィギュレーション モードを開始します。

ステップ 3	**show key chain***name* 例： `switch(config-keychain)# show key chain glbp-keys`	（任意） キーチェーンの設定を表示します。
ステップ 4	**copy running-config startup-config** 例： `switch(config-keychain)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

マスター キーの設定および AES パスワード暗号化機能のイネーブル化，（55 ページ）

キーチェーンの削除

デバイスのキーチェーンを削除できます。

（注） キーチェーンを削除すると、キーチェーン内のキーはどれも削除されます。

はじめる前に

キーチェーンを削除する場合は、そのキーチェーンを使用している機能がないことを確認してください。削除するキーチェーンを使用するように設定されている機能がある場合、その機能は他のデバイスとの通信に失敗する可能性が高くなります。

手順の概要

1. **configure terminal**
2. **no keychain***name*
3. （任意） **show key chain** *name*
4. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**no keychain***name* 例： `switch(config)# no key chain glbp-keys`	キーチェーンおよびそのキーチェーンに含まれているすべてのキーを削除します。
ステップ 3	**show key chain** *name* 例： `switch(config-keychain)# show key chain glbp-keys`	（任意） そのキーチェーンが実行コンフィギュレーション内にないことを確認します。
ステップ 4	**copy running-config startup-config** 例： `switch(config-keychain)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

キーチェーンの作成, （790 ページ）

マスターキーの設定およびAESパスワード暗号化機能のイネーブル化

タイプ 6 暗号化用のマスター キーを設定し、高度暗号化規格（AES）パスワード暗号化機能をイネーブルにすることができます。

手順の概要

1. **[no] key config-key ascii**
2. **configure terminal**
3. **[no] feature password encryption aes**
4. （任意） **show encryption service stat**
5. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**[no] key config-key ascii**
	
	例：
	`switch# key config-key ascii`
	`New Master Key:`
	`Retype Master Key:`
		マスター キーを、AES パスワード暗号化機能で使用するように設定します。マスター キーは、16 ～ 32 文字の英数字を使用できます。このコマンドの **no** 形式を使用すると、いつでもマスター キーを削除できます。
		
		マスター キーを設定する前に AES パスワード暗号化機能をイネーブルにすると、マスター キーが設定されていない限りパスワード暗号化が実行されないことを示すメッセージが表示されます。マスター キーがすでに設定されている場合、新しいマスター キーを入力する前に現在のマスター キーを入力するように求められます。

ステップ 2	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 3	**[no] feature password encryption aes** 例： `switch(config)# feature password encryption aes`	AES パスワード暗号化機能をイネーブルまたはディセーブルにします。
ステップ 4	**show encryption service stat** 例： `switch(config)# show encryption service stat`	（任意） AES パスワード暗号化機能とマスター キーの設定ステータスを表示します。
ステップ 5	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。 （注） このコマンドは、実行コンフィギュレーションとスタートアップ コンフィギュレーションのマスター キーを同期するために必要です。

関連トピック

AES パスワード暗号化およびマスター暗号キー，（39 ページ）
キーのテキストの設定，（794 ページ）
キーの受け入れライフタイムおよび送信ライフタイムの設定，（795 ページ）

キーのテキストの設定

キーのテキストを設定できます。テキストは共有秘密です。デバイスはこのテキストをセキュアな形式で保存します。

デフォルトでは、受け入れライフタイムおよび送信ライフタイムは無限になり、キーは常に有効です。キーにテキストを設定してから、そのキーの受け入れライフタイムと送信ライフタイムを設定します。

はじめる前に

そのキーのテキストを決めます。テキストは、暗号化されていないテキストとして入力できます。また、**show key chain** コマンド使用時に Cisco NX-OS がキー テキストの表示に使用する暗号形式で入力することもできます。特に、別のデバイスから **show key chain** コマンドを実行し、その出力に表示されるキーと同じキー テキストを作成する場合には、暗号化形式での入力が便利です。

手順の概要

1. **configure terminal**
2. **keychain***name*
3. **key***key-ID*
4. **key-string** [*encryption-type*] *text-string*
5. （任意） **show key chain** *name* [**mode decrypt**]
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**keychain***name*
	
	例：
	`switch(config)# key chain glbp-keys`
	`switch(config-keychain)#`
		指定したキーチェーンのキーチェーン コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 3	**key***key-ID*
	
	例：
	`switch(config-keychain)# key 13`
	`switch(config-keychain-key)#`
		指定したキーのキー コンフィギュレーション モードを開始します。*key-ID* 引数は、0 ～ 65535 の整数で指定する必要があります。

ステップ 4	**key-string** [*encryption-type*] *text-string*
	
	例：
	`switch(config-keychain-key)#`
	`key-string 0 AS3cureStr1ng`
		そのキーのテキスト ストリングを設定します。*text-string* 引数は、大文字と小文字を区別して、英数字で指定します。特殊文字も使用できます。
		encryption-type 引数に、次のいずれかの値を指定します。
		• 0：入力する *text-string* 引数は暗号化されていないテキストです。これはデフォルトです。
		• 7：入力する *text-string* 引数は暗号化されています。シスコ固有の暗号方式で暗号化されます。このオプションは、別の Cisco NX-OS デバイスで **show key chain** コマンドを実行し、表示された暗号化出力に基づいてテキスト ストリングを入力する場合に便利です。

ステップ 5	**show key chain** *name* [**mode decrypt**]
	
	例：
	`switch(config-keychain-key)# show`
	`key chain glbp-keys`
		（任意）
		キーテキストの設定も含めて、キーチェーンの設定を表示します。デバイス管理者だけが使用できる mode decrypt オプションを使用すると、キーはクリアテキストで表示されます。

ステップ 6	**copy running-config startup-config**
	
	例：
	`switch(config-keychain-key)# copy`
	`running-config startup-config`
		（任意）
		実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

キーの受け入れライフタイムおよび送信ライフタイムの設定, （795 ページ）

キーの受け入れライフタイムおよび送信ライフタイムの設定

キーの受け入れライフタイムおよび送信ライフタイムを設定できます。デフォルトでは、受け入れライフタイムおよび送信ライフタイムは無限になり、キーは常に有効です。

（注） キーチェーン内のキーのライフタイムが重複するように設定することを推奨します。このようにすると、アクティブなキーがないために、キーによるセキュア通信の切断を避けることができます。

手順の概要

1. **configure terminal**
2. **keychain***name*
3. **key***key-ID*
4. **accept-lifetime** [**local**] *start-time***duration***duration-value* | **infinite** | *end-time*]
5. **send-lifetime** [**local**] *start-time***duration***duration-value* | **infinite** | *end-time*]
6. （任意） **show key chain** *name* [**mode decrypt**]
7. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**keychain***name*
	
	例：
	`switch(config)# key chain glbp-keys`
	`switch(config-keychain)#`
		指定したキーチェーンのキーチェーン コンフィギュレーション モードを開始します。

ステップ 3	**key***key-ID*
	
	例：
	`switch(config-keychain)# key 13`
	`switch(config-keychain-key)#`
		指定したキーのキー コンフィギュレーション モードを開始します。

ステップ 4	**accept-lifetime** [**local**] *start-time***duration***duration-value*	**infinite**	*end-time*]
			
			例：
			`switch(config-keychain-key)#`
			`accept-lifetime 00:00:00 Jun 13 2008`
			`23:59:59 Sep 12 2008`
				キーの受け入れライフタイムを設定します。デフォルトでは、デバイスは *start-time* および *end-time* 引数を UTC として扱います。**local** キーワードを指定すると、デバイスはこれらの時間を現地時間として扱います。
				
				start-time 引数は、キーがアクティブになる日時です。
				
				ライフタイムの終了時は次のいずれかのオプションで指定できます。
				
				• **duration** *duration-value*：ライフタイムの長さ（秒）。最大値は 2147483646 秒（約 68 年）です。

	コマンドまたはアクション	目的
		• **infinite**：キーの受け入れライフタイムは期限切れになりません。 • *end-time*：The *end-time* 引数はキーがアクティブでなくなる日時です。
ステップ 5	**send-lifetime** [**local**] *start-time***duration***duration-value* | **infinite** | *end-time*] 例： `switch(config-keychain-key)# send-lifetime 00:00:00 Jun 13 2008 23:59:59 Aug 12 2008`	キーの送信ライフタイムを設定します。デフォルトでは、デバイスは *start-time* および *end-time* 引数を UTC として扱います。**local** キーワードを指定すると、デバイスはこれらの時間を現地時間として扱います。 *start-time* 引数は、キーがアクティブになる日時です。 送信ライフタイムの終了時は次のいずれかのオプションで指定できます。 • **duration** *duration-value*：ライフタイムの長さ（秒）。最大値は 2147483646 秒（約 68 年）です。 • **infinite**：キーの送信ライフタイムは期限切れになりません。 • *end-time*：The *end-time* 引数はキーがアクティブでなくなる日時です。
ステップ 6	**show key chain** *name* [**mode decrypt**] 例： `switch(config-keychain-key)# show key chain glbp-keys`	（任意） キー テキストの設定も含めて、キーチェーンの設定を表示します。デバイス管理者だけが使用できる mode decrypt オプションを使用すると、キーはクリアテキストで表示されます。
ステップ 7	**copy running-config startup-config** 例： `switch(config-keychain-key)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

関連トピック

キーのライフタイム，（788 ページ）

アクティブなキーのライフタイムの確認

キーチェーン内のキーのうち、受け入れライフタイムまたは送信ライフタイムがアクティブなキーを確認するには、次の表のコマンドを使用します。このコマンドの出力フィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

コマンド	目的
show key chain	デバイスに設定されているキーチェーンを表示します。

キーチェーン管理の設定の確認

キーチェーン管理の設定情報を表示するには、次の作業を行います。このコマンドの出力フィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

コマンド	目的
show key chain	デバイスに設定されているキーチェーンを表示します。

キーチェーン管理の設定例

glbp keys という名前のキーチェーンを設定する例を示します。各キーテキスト ストリングは暗号化されています。各キーの受け入れライフタイムは送信ライフタイムよりも長くなっています。これは、誤ってアクティブ キーのない時間を設定してもなるべく通信が失われないようにするためです。

```
key chain glbp-keys
  key 0
    key-string 7 zqdest
    accept-lifetime 00:00:00 Jun 01 2008 23:59:59 Sep 12 2008
    send-lifetime 00:00:00 Jun 01 2008 23:59:59 Aug 12 2008
  key 1
    key-string 7 uaeqdyito
    accept-lifetime 00:00:00 Aug 12 2008 23:59:59 Dec 12 2008
    send-lifetime 00:00:00 Sep 12 2008 23:59:59 Nov 12 2008
  key 2
    key-string 7 eekgsdyd
    accept-lifetime 00:00:00 Nov 12 2008 23:59:59 Mar 12 2009
    send-lifetime 00:00:00 Dec 12 2008 23:59:59 Feb 12 2009
```

次の作業

キーチェーンを使用するルーティング機能については、『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』を参照してください。

キーチェーン管理に関する追加情報

関連資料

関連項目	マニュアル タイトル
Gateway Load Balancing Protocol	『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』
ボーダー ゲートウェイ プロトコル	『*Cisco Nexus 7000 Series NX-OS Unicast Routing Configuration Guide*』
キーチェーン管理のコマンド：コマンド構文の詳細、コマンドモード、コマンド履歴、デフォルト設定、使用上のガイドライン、および例	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	—

キーチェーン管理の機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 *50*：キーチェーン管理の機能の履歴

機能名	リリース	機能情報
キーチェーン管理	6.0(1)	Release 5.2 以降、変更はありません。
キーチェーン管理	5.2(1)	Release 5.1 以降、変更はありません。
キーチェーン管理	5.1(1)	Release 5.0 以降、変更はありません。

機能名	リリース	機能情報
キーチェーン管理	5.0(2)	Release 4.2 以降、変更はありません。
キーチェーン管理	4.2(1)	リリース 4.1 からの変更はありません。

第 24 章

トラフィック ストーム制御の設定

この章では、Cisco NX-OS デバイスに、トラフィック ストーム制御機能を設定する手順について説明します。

この章は、次の項で構成されています。

- 機能情報の確認，801 ページ
- トラフィック ストーム制御の概要，802 ページ
- トラフィック ストーム制御のバーチャライゼーション サポート，803 ページ
- トラフィック ストーム制御のライセンス要件，803 ページ
- トラフィック ストーム制御の注意事項と制約事項，804 ページ
- トラフィック ストーム制御のデフォルト設定，804 ページ
- トラフィック ストーム制御の設定，805 ページ
- トラフィック ストーム制御の設定の確認，806 ページ
- トラフィック ストーム制御カウンタのモニタリング，807 ページ
- トラフィック ストーム制御の設定例，807 ページ
- トラフィック ストーム制御に関する追加情報，807 ページ
- トラフィック ストーム制御の機能履歴，808 ページ

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

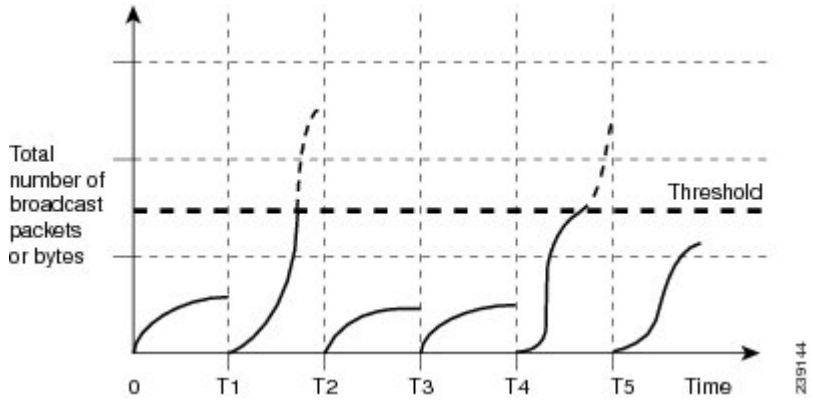
トラフィック ストーム制御の概要

トラフィック ストームは、パケットが LAN でフラッディングする場合に発生するもので、過剰なトラフィックを生成し、ネットワークのパフォーマンスを低下させます。トラフィック ストーム制御機能を使用すると、物理インターフェイス上におけるブロードキャスト、マルチキャスト、または未知のユニキャスト トラフィック ストームによって、レイヤ 2 ポート経由の通信が妨害されるのを防げます。

トラフィック ストーム制御（トラフィック抑制ともいう）では、ブロードキャスト、マルチキャスト、ユニキャストの着信トラフィックのレベルを 10 ミリ秒間隔でモニタできます。この間、トラフィック レベル（ポートの使用可能合計帯域幅に対するパーセンテージ）が、設定したトラフィック ストーム制御レベルと比較されます。入力トラフィックが、ポートに設定したトラフィック ストーム制御レベルに到達すると、トラフィック ストーム制御機能によってそのインターバルが終了するまでトラフィックがドロップされます。

次の表に、指定したインターバルでのレイヤ 2 インターフェイス上のブロードキャスト トラフィック パターンを示します。この例では、トラフィック ストーム制御が T1 と T2 時間の間、および T4 と T5 時間の間で発生します。これらの間隔中に、ブロードキャスト トラフィックの量が設定済みのしきい値を超過したためです。

図 *31*：ブロードキャストの抑制



トラフィック ストーム制御しきい値の数値と期間の組み合わせにより、トラフィック ストーム制御アルゴリズムがさまざまな粒度で機能します。しきい値が高いほど、通過できるパケット数が多くなります。

Cisco NX-OS デバイスのトラフィック ストーム制御はハードウェアに実装されています。トラフィック ストーム制御は、レイヤ 2 インターフェイスからスイッチング バスに渡されるパケットを巡回モニタします。また、パケットの宛先アドレスに設定されている Individual/Group ビットを使用して、パケットがユニキャストかブロードキャストかを判断し、10 ミリ秒以内の間隔で現在のパケット数を追跡します。パケット数がしきい値に到達したら、後続のパケットをすべて破棄します。

トラフィック ストーム制御では、トラフィック量の計測に帯域幅方式を使用します。制御対象のトラフィックが使用できる、利用可能な合計帯域幅に対するパーセンテージを設定します。パケッ

トは一定間隔で着信するわけではないので、10ミリ秒の間隔はトラフィック ストーム制御の動作に影響を及ぼす可能性があります。

次に、トラフィック ストーム制御動作の例を示します。

- ブロードキャスト トラフィック ストーム制御をイネーブルにした場合、ブロードキャスト トラフィックが 10 ミリ秒のインターバル中に制御レベルを超えると、インターバルが終了するまですべてのブロードキャスト トラフィックがドロップされます。
- ブロードキャストとマルチキャストのトラフィック ストーム制御をイネーブルにした場合、ブロードキャストとマルチキャストの混合トラフィックが 10 ミリ秒のインターバル中に制御レベルを超えると、インターバルが終了するまでブロードキャストとマルチキャストのすべてのトラフィックがドロップされます。
- ブロードキャストとマルチキャストのトラフィック ストーム制御をイネーブルにした場合、ブロードキャスト トラフィックが 10 ミリ秒のインターバル中に制御レベルを超えると、インターバルが終了するまでブロードキャストとマルチキャストのすべてのトラフィックがドロップされます。
- ブロードキャストとマルチキャストのトラフィック ストーム制御をイネーブルにした場合、マルチキャスト トラフィックが 10 ミリ秒のインターバル中に制御レベルを超えると、インターバルが終了するまでブロードキャストとマルチキャストのすべてのトラフィックがドロップされます。

デフォルトでは、トラフィックが設定レベルを超えても、Cisco NX-OS ソフトウェアは是正のための処理を実行しません。ただし、組み込みイベントマネージャ（EEM）によって、トラフィックが一定期間内に収まらない（しきい値未満にならない）場合にインターフェイスをエラー ディセーブル状態にするように設定できます。EEM の設定の詳細については、『*Cisco Nexus 7000 Series NX-OS System Management Command Reference*』を参照してください。

トラフィックストーム制御のバーチャライゼーションサポート

トラフィック ストーム制御の設定と操作は、仮想デバイス コンテキスト（VDC）に対してローカルです。

VDC の詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

トラフィック ストーム制御のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	トラフィック ストーム制御にはライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

トラフィック ストーム制御の注意事項と制約事項

トラフィック ストーム制御レベルを設定する際の注意事項と制約事項は次のとおりです。

- ポート チャネル インターフェイス上にトラフィック ストーム制御を設定できます。
- ポート チャネル インターフェイスのメンバであるインターフェイスには、トラフィック ストーム制御を設定しないでください。ポート チャネルのメンバとして設定されているインターフェイスにトラフィック ストーム制御を設定すると、そのポートは中断状態になります。
- レベルをインターフェイスの帯域幅全体に対する割合として指定します。
  - レベルの指定範囲は 0 ～ 100 です。
  - 任意で、レベルの小数部を 0 ～ 99 の範囲で指定できます。
  - 100% は、トラフィック ストーム制御がないことを意味します。
  - 0.0% は、すべてのトラフィックを抑制します。

ハードウェアの制限およびサイズの異なるパケットがカウントされる方式のため、レベルの割合は概数になります。着信トラフィックを構成するフレームのサイズに応じて、実際に適用されるパーセンテージ レベルと設定したパーセンテージ レベルの間には、数パーセントの誤差がある可能性があります。

（注） Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

トラフィック ストーム制御のデフォルト設定

次の表に、トラフィック ストーム制御パラメータのデフォルト設定値を示します。

トラフィック ストーム制御の設定

表 *51*：デフォルトのトラフィック ストーム制御パラメータ

パラメータ	デフォルト
トラフィック ストーム制御	ディセーブル
しきい値パーセンテージ	100

トラフィック ストーム制御の設定

制御対象のトラフィックが使用できる、利用可能な合計帯域幅に対するパーセンテージを設定できます。

（注） トラフィック ストーム制御機能では、トラフィック ストーム制御の動作を 10 ミリ秒間隔で変更できます。

手順の概要

1. **configure terminal**
2. **interface** {**ethernet***slot*/*port* | **port-channel***number*}
3. **storm-control** {**broadcast** | **multicast** | **unicast**} **level***percentage*[**.***fraction*]
4. **exit**
5. （任意） **show running-config interface** {**ethernet***slot*/*port* | **port-channel***number*}
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface** {**ethernet***slot*/*port*	**port-channel***number*}
		
		例：
		`switch# interface ethernet 1/1`
		`switch(config-if)#`
			インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**storm-control** {**broadcast** | **multicast** | **unicast**} **level***percentage*[**.***fraction*] 例： `switch(config-if)# storm-control unicast level 40`	インターフェイスを通過するトラフィックのトラフィック ストーム制御を設定します。デフォルトのステートはディセーブルです。 （注） **storm-control unicast** コマンドはすべてユニキャストパケットに対するトラフィック ストーム制御を設定します。

ステップ 4	**exit**
	
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 5	**show running-config interface** {**ethernet***slot*/*port* | **port-channel***number*} 例： `switch(config)# show running-config interface ethernet 1/1`	（任意） トラフィック ストーム制御の設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

トラフィック ストーム制御の設定の確認

トラフィック ストーム制御の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show interface [**ethernet***slot*/*port* | **port-channel***number*] **counters storm-control**	特定のインターフェイスについて、トラフィック ストーム制御の設定を表示します。
show running-config interface	トラフィック ストーム制御の設定を表示します。

これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

トラフィック ストーム制御カウンタのモニタリング

トラフィック ストーム制御動作に関して Cisco NX-OS デバイスが維持するカウンタをモニタリングできます。

手順の概要

1. **show interface** [**ethernet***slot*/*port* | **port-channel***number*] **counters storm-control**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show interface** [**ethernet***slot*/*port*	**port-channel***number*] **counters storm-control** 例： `switch# show interface counters storm-control`	トラフィック ストーム制御カウンタを表示します。

トラフィック ストーム制御の設定例

次に、トラフィック ストーム制御の設定例を示します。

```
interface Ethernet1/1
  storm-control broadcast level 40
  storm-control multicast level 40
  storm-control unicast level 40
```

トラフィック ストーム制御に関する追加情報

ここでは、トラフィック ストーム制御の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS ライセンス設定	『*Cisco NX-OS Licensing Guide*』
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』

トラフィック ストーム制御の機能履歴

次の表に、この機能のリリースの履歴を示します。

表 *52*：トラフィック ストーム制御の機能履歴

機能名	リリース	機能情報	
トラフィック ストーム制御	6.0(1)	Release 5.2 以降、変更はありません。	
トラフィック ストーム制御	5.2(1)	Release 5.1 以降、変更はありません。	
トラフィック ストーム制御	5.1(1)	Release 5.0 以降、変更はありません。	
トラフィック ストーム制御	5.0(2)	Release 4.2 以降、変更はありません。	
トラフィック ストーム制御	4.2(1)	リリース 4.1 からの変更はありません。	

第 25 章

ユニキャスト RPF の設定

この章では、Cisco NX-OS デバイス上で出力トラフィックのレート制限を設定する手順について説明します。

この章は、次の項で構成されています。

- 機能情報の確認，809 ページ
- ユニキャスト RPF の概要，810 ページ
- ユニキャスト RPF のバーチャライゼーション サポート，812 ページ
- ユニキャスト RPF のライセンス要件，812 ページ
- ユニキャスト RPF の注意事項と制約事項，812 ページ
- ユニキャスト RPF のデフォルト設定，813 ページ
- ユニキャスト RPF の設定，813 ページ
- ユニキャスト RPF の設定例，816 ページ
- ユニキャスト RPF の設定の確認，816 ページ
- ユニキャスト RPF に関する追加情報，817 ページ
- ユニキャスト RPF の機能の履歴，817 ページ

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。このモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

ユニキャスト RPF の概要

ユニキャスト RPF 機能では、変形または偽造（スプーフィング）された IPv4 または IPv6 ソース アドレスがネットワークに注入されて引き起こされる問題を、裏付けのない IPv4 または IPv6 パケットを廃棄することによって緩和します。たとえば、Smurf や Tribal Flood Network（TFN）など、いくつかの一般的なサービス拒絶（DoS）攻撃は、偽造の送信元 IPv4 または IPv6 アドレスやすぐに変更される送信元 IPv4 または IPv6 アドレスを利用して、攻撃を突き止めたりフィルタリングしたりする手段を妨ぐことができます。ユニキャスト RPF では、送信元アドレスが有効で IP ルーティング テーブルと一致するパケットだけを転送することにより、攻撃を回避します。

インターフェイス上でユニキャスト RPF をイネーブルにすると、デバイスはそのインターフェイス上で受信されたすべての入力パケットを検証することにより、送信元アドレスと発信元インターフェイスがルーティング テーブル内に現れ、しかもパケット受信場所のインターフェイスと一致することを確認します。この送信元アドレス検査は転送情報ベース（FIB）に依存しています。

（注） ユニキャスト RPF は入力機能であり、接続のアップストリーム エンドにあるデバイス の入力インターフェイスにのみ適用されます。

ユニキャスト RPF は、FIB のリバース ルックアップを実行することにより、デバイス インターフェイスでの受信パケットがそのパケットの送信元への最良リターン パスで着信していることを確認します。パケットが最適なリバースパスルートのいずれかから受信された場合、パケットは通常どおりに転送されます。パケットを受信したインターフェイス上にリバースパスルートがない場合、攻撃者によって送信元アドレスが変更される可能性があります。ユニキャスト RPF がそのパケットのリバース パスを見つけられない場合は、パケットはドロップされます。

（注） ユニキャスト RPF では、コストが等しいすべての「最良」リターン パスが有効と見なされます。つまり、複数のリターン パスが存在していても、各パスのルーティング コスト（ホップ カウントや重みなど）が他のパスと等しく、そのルートが FIB 内にある限り、ユニキャスト RPF は機能します。ユニキャスト RPF は、Enhanced Interior Gateway Routing Protocol（EIGRP）バリアントが使用されていて、送信元 IP アドレスに戻る同等でない候補パスが存在する場合にも機能します。

ユニキャスト RPF プロセス

ユニキャスト RPF には、キーの実装原則がいくつかあります。

- パケットは、パケットの送信元に対する最適なリターン パス（ルート）があるインターフェイスで受信する必要があります（このプロセスは対照ルーティングと呼ばれます）。FIB に受信インターフェイスへのルートと一致するルートが存在する必要があります。スタティック ルート、ネットワーク文、ダイナミック ルーティングによって FIB にルートが追加されます。

- 受信側インターフェイスでの IP 送信元アドレスは、そのインターフェイスのルーティング エントリと一致する必要があります。
- ユニキャスト RPF は入力機能であり、接続のアップストリーム エンドのデバイスの入力インターフェイスだけに適用されます。

ダウンストリーム ネットワークにインターネットへの他の接続があっても、ダウンストリーム ネットワークにユニキャスト RPF を使用できます。

注意 攻撃者が送信元アドレスへの最良パスを変更する可能性があるので、加重やローカルプリファレンスなどのオプションのBGP属性を使用する際には、十分に注意してください。変更によって、ユニキャスト RPF の操作に影響が出ます。

ユニキャスト RPF と ACL を設定したインターフェイスでパケットが受信されると、Cisco NX-OS ソフトウェアは次の動作を行います。

手順の概要

1. インバウンド インターフェイスで入力 ACL をチェックします。
2. ユニキャストRFPを使用し、FIBテーブル内のリバースルックアップを実行することにより、そのパケットが送信元への最良リターン パスで着信したことを確認します。
3. パケットの転送を目的として FIB ルックアップを実行します。
4. アウトバウンド インターフェイスで出力 ACL をチェックします。
5. パケットを転送します。

手順の詳細

ステップ 1 インバウンド インターフェイスで入力 ACL をチェックします。

ステップ 2 ユニキャストRFPを使用し、FIBテーブル内のリバースルックアップを実行することにより、そのパケットが送信元への最良リターン パスで着信したことを確認します。

ステップ 3 パケットの転送を目的として FIB ルックアップを実行します。

ステップ 4 アウトバウンド インターフェイスで出力 ACL をチェックします。

ステップ 5 パケットを転送します。

グローバル統計

Cisco NX-OS デバイスがユニキャスト RPF チェックの失敗によりインターフェイスでパケットをドロップするたびに、その情報が転送エンジン（FE）単位でデバイスにおいてグローバルにカウントされます。ドロップされたパケットのグローバル統計からは、ネットワーク上での攻撃の可能性に関する情報を得ることができますが、攻撃の送信元となるインターフェイスは特定されま

せん。ユニキャスト RPF チェックの失敗によりドロップされたパケットのインターフェイス単位の統計情報は利用できません。

ユニキャスト RPF のバーチャライゼーション サポート

ユニキャスト RPF の設定と操作は、仮想デバイス コンテキスト（VDC）に対してローカルです。VDC の詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

ユニキャスト RPF のライセンス要件

製品	ライセンス要件
Cisco NX-OS	ユニキャスト RPF にはライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

ユニキャスト RPF の注意事項と制約事項

ユニキャスト RPF に関する注意事項と制約事項は次のとおりです。

- ユニキャスト RPF は、ネットワーク内のより大きな部分からのダウンストリームのインターフェイスで適用する必要があります（ネットワークのエッジに適用するのが望ましい）。
- なるべくダウンストリームでユニキャスト RPF を適用する方が、アドレス スプーフィングの軽減やスプーフされたアドレスの送信元の特定の精度が高くなります。たとえば、集約デバイスでユニキャスト RPF を適用すると、多くのダウンストリーム ネットワークまたはクライアントからの攻撃を軽減できるとともに、管理が簡単になりますが、攻撃の送信元は特定できません。ネットワーク アクセス サーバにユニキャスト RPF を適用すると、攻撃の範囲を絞り、攻撃元を追跡しやすくなります。ただし、多数のサイトにユニキャスト RPF を展開すると、ネットワーク運用の管理コストが増加します。
- インターネット、イントラネット、およびエクストラネットのリソース全体でユニキャスト RPF を配布するエンティティが多いほど、インターネット コミュニティを通じた大規模なネットワークの中断が軽減される可能性が高くなり、攻撃の送信元をトレースできる可能性も高くなります。
- ユニキャスト RPF は、総称ルーティング カプセル化（GRE）トンネルのようなトンネルでカプセル化された IP パケットは検査しません。トンネリングとカプセル化のレイヤがパケッ

トから除かれてからユニキャストRPFがネットワーク トラフィックを処理するように、ホーム ゲートウェイにユニキャスト RPF を設定する必要があります。

- ユニキャスト RPF は、ネットワークからのアクセス ポイントが 1 つだけ、またはアップストリーム接続が 1 つだけの「単一ホーム」環境で使用できます。アクセス ポイントが 1 つのネットワークは対称ルーティングを提供します。これはつまり、パケットがネットワークに入るインターフェイスはその IP パケットの送信元への最良のリターン パスでもあるということです。
- ネットワーク内部のインターフェイスにはユニキャストRPFを使用しないでください。内部インターフェイスは、ルーティングを非対称にする可能性が高く、パケットの送信元へのルートが複数存在する場合が多いからです。ユニキャストRPFを設定するのは、元々対称であるか、対称に設定されている場合だけにしてください。ストリクト ユニキャスト RPF を設定しないでください。
- ユニキャスト RPF を使用すると、送信元が 0.0.0.0 で宛先が 255.255.255.255 のパケットを通過させて、ブートストラップ プロトコル（BOOTP）と Dynamic Host Configuration Protocol（DHCP）を正しく動作させることができます。

（注） Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

ユニキャスト RPF のデフォルト設定

次の表に、ユニキャスト RPF パラメータのデフォルト設定を示します。

表 *53* : ユニキャスト *RPF* パラメータのデフォルト設定

パラメータ	デフォルト
Unicast RPF	ディセーブル

ユニキャスト RPF の設定

入力インターフェイスに次のいずれかのユニキャスト RPF モードを設定できます。

ユニキャスト RPF の設定

ストリクト ユニキャスト RPF モード

厳格モードでは、ユニキャストRPFがFIBで一致するパケット送信元アドレスを見つけて、パケットを受信した入力インターフェイスが FIB 内のユニキャスト RPF インターフェイスのいずれかと一致した場合に、チェックに合格します。チェックに合格しないと、パケットは廃棄されます。このタイプのユニキャスト RPF チェックは、パケット フローが対称であると予想される場合に使用できます。

ルーズ ユニキャスト RPF モード

緩和モードでは、FIB でのパケット送信元アドレスのルックアップで一致が戻り、FIB の結果からその送信元が少なくとも1つの実インターフェイスで到達可能であることが示された場合に、チェックに合格します。パケットを受信した入力インターフェイスがFIB内のインターフェイスのいずれかと一致する必要はありません。

手順の概要

1. **configure terminal**
2. **interface ethernet***slot*/*port*
3. **ip verify unicast source reachable-via** {**any** [**allow-default**] | **rx**}
4. **ipv6 verify unicast source reachable-via** {**any** [**allow-default**] | **rx**}
5. **exit**
6. （任意） **show ip interface ethernet***slot*/*port*
7. （任意） **show running-config interface ethernet***slot*/*port*
8. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**interface ethernet***slot*/*port*
	
	例：
	`switch(config)# interface ethernet 2/3`
	`switch(config-if)#`
		イーサネット インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。

ステップ 3	**ip verify unicast source reachable-via** {**any** [**allow-default**]	**rx**} 例： `switch(config-if)# ip verify unicast source reachable-via any`	IPv4 用インターフェイスにユニキャスト RPF を設定します。 **any** キーワードはルーズ モードのユニキャスト RPF を指定します。

	コマンドまたはアクション	目的
		allow-default キーワードを指定すると、送信元アドレスのルックアップでデフォルトルートと一致させることが可能になり、それを検証に使用できます。 **rx** キーワードは厳格モードのユニキャスト RPF を指定します。

ステップ 4	**ipv6 verify unicast source reachable-via** {**any** [**allow-default**] | **rx**}
	例：
	`Example:`
	`switch(config-if)# ipv6 verify unicast source reachable-via any`
		IPv6 用インターフェイスにユニキャスト RPF を設定します。
		any キーワードはルーズ モードのユニキャスト RPF を指定します。
		allow-default キーワードを指定すると、送信元アドレスのルックアップでデフォルトルートと一致させることが可能になり、それを検証に使用できます。
		rx キーワードは厳格モードのユニキャスト RPF を指定します。

ステップ 5	**exit**
	例：
	`switch(config-cmap)# exit`
	`switch(config)#`
		クラスマップ コンフィギュレーション モードを終了します。

ステップ 6	**show ip interface ethernet***slot*/*port* 例： `switch(config)# show ip interface ethernet 2/3`	（任意） インターフェイスの IP 情報を表示します。
ステップ 7	**show running-config interface ethernet***slot*/*port* 例： `switch(config)# show running-config interface ethernet 2/3`	（任意） 実行コンフィギュレーション内のインターフェイスの情報を表示します。
ステップ 8	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ユニキャスト RPF の設定例

緩和モードの IPv4 パケット用ユニキャスト RPF の設定例を示します。

```
interface Ethernet2/3
  ip address 172.23.231.240/23
  ip verify unicast source reachable-via any
```

厳格モードの IPv4 パケット用ユニキャスト RPF の設定例を示します。

```
interface Ethernet2/2
  ip address 172.23.231.240/23
  ip verify unicast source reachable-via rx
```

緩和モードの IPv6 パケット用ユニキャスト RPF の設定例を示します。

```
interface Ethernet2/1
  ipv6 address 2001:0DB8:c18:1::3/64
  ipv6 verify unicast source reachable-via any
```

厳格モードの IPv6 パケット用ユニキャスト RPF の設定例を示します。

```
interface Ethernet2/4
  ipv6 address 2001:0DB8:c18:1::3/64
  ipv6 verify unicast source reachable-via rx
```

ユニキャスト RPF の設定の確認

ユニキャスト RPF の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show running-config interface ethernet*slot*/*port*	実行コンフィギュレーション内のインターフェイスの設定を表示します。
show running-config ip [**all**]	実行コンフィギュレーション内の IPv4 設定を表示します。
show running-config ipv6 [**all**]	実行コンフィギュレーション内の IPv6 設定を表示します。
show startup-config interface ethernet*slot*/*port*	スタートアップ コンフィギュレーション内のインターフェイスの設定を表示します。
show startup-config ip	スタートアップ コンフィギュレーション内の IP 設定を表示します。

これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

ユニキャスト RPF に関する追加情報

ここでは、ユニキャスト RPF の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS ライセンス設定	『*Cisco NX-OS Licensing Guide*』
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』

ユニキャスト RPF の機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 *54* : ユニキャスト *RPF* の機能の履歴

機能名	リリース	機能情報
Unicast RPF	6.0(1)	Release 5.2 以降、変更はありません。
Unicast RPF	5.2(1)	Release 5.1 以降、変更はありません。
Unicast RPF	5.1(1)	Release 5.0 以降、変更はありません。
Unicast RPF	5.0(2)	Release 4.2 以降、変更はありません。
Unicast RPF	4.2(1)	リリース 4.1 からの変更はありません。

第 26 章

コントロール プレーン ポリシングの設定

この章の内容は、次のとおりです。

- 機能情報の確認，819 ページ
- CoPP の概要，820 ページ
- CoPP のライセンス要件，837 ページ
- CoPP の注意事項と制約事項，837 ページ
- CoPP のデフォルト設定，840 ページ
- CoPP の設定，841 ページ
- CoPP の設定の確認，852 ページ
- CoPP 設定ステータスの表示，855 ページ
- CoPP のモニタリング，856 ページ
- SNMP での CoPP のモニタリング，857 ページ
- CoPP 統計情報のクリア，857 ページ
- CoPP の設定例，858 ページ
- セットアップユーティリティによるデフォルト CoPP ポリシーの変更または再適用，861 ページ
- CoPP に関する追加情報，862 ページ
- CoPP の機能の履歴，863 ページ

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。こ

のモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

CoPP の概要

コントロール プレーン ポリシング（CoPP）はコントロール プレーンを保護し、それをデータ プレーンから分離することによって、ネットワークの安定性、到達可能性、およびパケット配信を保証します。

この機能により、コントロールプレーンにポリシーマップを適用できるようになります。このポリシー マップは通常の QoS ポリシーのように見え、ルータまたはレイヤ 3 スイッチの任意の IP アドレスに宛てられたすべてのトラフィックに適用されます。ネットワーク デバイスへの一般的な攻撃ベクトルは、過剰なトラフィックがデバイス インターフェイスに転送されるサービス拒絶（DoS）攻撃です。

Cisco NX-OS デバイスは、DoS 攻撃がパフォーマンスに影響しないようにするために CoPP を提供します。このような攻撃は誤って、または悪意を持って実行される場合があり、通常は、スーパーバイザ モジュールまたは CPU 自体に宛てられた大量のトラフィックが含まれます。

スーパーバイザ モジュールは、管理対象のトラフィックを次の 3 つの機能コンポーネント（プレーン）に分類します。

データ プレーン

すべてのデータ トラフィックを処理します。NX-OS デバイスの基本的な機能は、インターフェイス間でパケットを転送することです。スイッチ自身に向けられたものでないパケットは、中継パケットと呼ばれます。データ プレーンで処理されるのはこれらのパケットです。

制御プレーン

ルーティング プロトコルのすべての制御トラフィックを処理します。ボーダー ゲートウェイ プロトコル（BGP）や Open Shortest Path First（OSPF）プロトコルなどのルーティング プロトコルは、デバイス間で制御パケットを送信します。これらのパケットはルータのアドレスを宛先とし、コントロール プレーン パケットと呼ばれます。

管理プレーン

コマンドライン インターフェイス（CLI）や簡易ネットワーク管理プロトコル（SNMP）など、NX-OS デバイスを管理する目的のコンポーネントを実行します。

スーパーバイザ モジュールには、マネージメント プレーンとコントロール プレーンの両方が搭載され、ネットワークの運用にクリティカルなモジュールです。スーパーバイザ モジュールの動作が途絶したり、スーパーバイザ モジュールが攻撃されたりすると、重大なネットワークの停止につながります。たとえばスーパーバイザに過剰なトラフィックが加わると、スーパーバイザ モジュールが過負荷になり、NX-OS デバイス全体のパフォーマンスが低下する可能性があります。またたとえば、スーパーバイザ モジュールに対する DoS 攻撃は、コントロール プレーンに対して非常に高速に IP トラフィック ストリームを生成することがあります。これにより、コントロー

ル プレーンは、これらのパケットを処理するために大量の時間を費やしてしまい、本来のトラフィックを処理できなくなります。

次に、DoS 攻撃の例を示します。

- インターネット制御メッセージ プロトコル（ICMP）エコー要求
- IP フラグメント
- TCP SYN フラッディング

これらの攻撃によりデバイスのパフォーマンスが影響を受け、次のようなマイナスの結果をもたらします。

- サービス品質の低下（音声、ビデオ、または重要なアプリケーション トラフィックの低下など）
- ルート プロセッサまたはスイッチ プロセッサの高い CPU 使用率
- ルーティング プロトコルのアップデートまたはキープアライブの消失によるルート フラップ
- 不安定なレイヤ 2 トポロジ
- CLI との低速な、または応答を返さない対話型セッション
- メモリやバッファなどのプロセッサ リソースの枯渇
- 着信パケットの無差別のドロップ

注意 コントロール プレーンの保護策を講じることで、スーパーバイザ モジュールを偶発的な攻撃や悪意ある攻撃から確実に保護することが重要です。

コントロール プレーン保護

コントロール プレーンを保護するために、Cisco NX-OS デバイスはコントロール プレーンに向かうさまざまなパケットを異なるクラスに分離します。クラスの識別が終わると、Cisco NX-OS デバイスはパケットをポリシングします。これにより、スーパーバイザ モジュールに過剰な負担がかからないようになります。

コントロール プレーンのパケット タイプ

コントロール プレーンには、次のような異なるタイプのパケットが到達します。

受信パケット

ルータの宛先アドレスを持つパケット。宛先アドレスには、レイヤ2アドレス（ルータ MAC アドレスなど）やレイヤ 3 アドレス（ルータ インターフェイスの IP アドレスなど）があります。これらのパケットには、ルータ アップデートとキープアライブ メッセージも含まれます。ルータが使用するマルチキャスト アドレス宛てに送信されるマルチキャスト パケットも、このカテゴリに入ります。

例外パケット

スーパーバイザ モジュールによる特殊な処理を必要とするパケット。たとえば、宛先アドレスが Forwarding Information Base（FIB; 転送情報ベース）に存在せず、結果としてミスとなった場合は、スーパーバイザ モジュールが送信側に到達不能パケットを返します。他には、IP オプションがセットされたパケットもあります。

リダイレクト パケット

スーパーバイザ モジュールにリダイレクトされるパケット。ダイナミック ホスト コンフィギュレーション プロトコル（DHCP）スヌーピングやダイナミック アドレス解決プロトコル（ARP）インスペクションなどの機能は、パケットをスーパーバイザ モジュールにリダイレクトします。

収集パケット

宛先 IP アドレスのレイヤ 2 MAC アドレスが FIB に存在していない場合は、スーパーバイザ モジュールがパケットを受信し、ARP 要求をそのホストに送信します。

これらのさまざまなパケットはすべて、コントロール プレーンへの悪意ある攻撃に利用され、Cisco NX-OS デバイスに過剰な負荷をかける可能性があります。CoPP は、これらのパケットを異なるクラスに分類し、これらのパケットをスーパーバイザが受信する速度を個別に制御するメカニズムを提供します。

CoPP の分類

効果的に保護するために、Cisco NX-OS デバイスはスーパーバイザ モジュールに到達するパケットを分類して、パケット タイプに基づいた異なるレート制御ポリシーを適用できるようにします。たとえば、Hello メッセージなどのプロトコル パケットには厳格さを緩め、IP オプションがセットされているためにスーパーバイザ モジュールに送信されるパケットには厳格さを強めることが考えられます。

レート制御メカニズム

パケットの分類が終わると、Cisco NX-OS デバイスにはスーパーバイザ モジュールに到達するパケットのレートを制御するメカニズムがあります。スーパーバイザ モジュールへのトラフィックのレート制御には 2 つのメカニズムを使用します。1 つはポリシング、もう 1 つはレート制限と呼ばれるものです。

ハードウェア ポリサーを使用すると、トラフィックが所定の条件に一致する場合、超過する場合、または違反する場合のそれぞれについて異なるアクションを定義できます。このアクションには、パケットの送信、パケットのマーク付け、およびパケットのドロップがあります。

ポリシングには、次のパラメータを設定できます。

認定情報レート（CIR）

望ましい帯域幅を、ビット レート、またはリンク レートの割合として指定します。

最大情報レート（PIR）

望ましい帯域幅を、ビット レート、またはリンク レートの割合として指定します。

認定バースト（BC）

指定した時間枠内に CIR を超過する可能性があるが、スケジューリングには影響を与えないトラフィック バーストのサイズ。

拡張バースト（BE）

すべてのトラフィックが PIR に達する前に到達する可能性のあるトラフィック バーストのサイズ。

さらに、一致トラフィック、超過トラフィック、および違反トラフィックに対して、送信またはドロップなどの異なるアクションを設定できます。

ポリシング パラメータの詳細については、『*Cisco Nexus 7000 Series NX-OS Quality of Service Configuration Guide*』を参照してください。

デフォルトのポリシング ポリシー

Cisco NX-OS デバイスの初回起動時に、DoS 攻撃からスーパーバイザ モジュールを保護するためのデフォルトの copp-system-p-policy-strict ポリシーが Cisco NX-OS ソフトウェアによりインストールされます。最初のセットアップ ユーティリティで、次のいずれかの CoPP ポリシー オプションを選択することにより、保護レベルを設定できます。

- Strict：このポリシーは、1 レート 2 カラーで BC 値が 250 ms です（ただし、この値が 1000 ms の重要なクラスは除きます）。
- Moderate：このポリシーは、1 レート 2 カラーで BC 値が 310 ms です（ただし、この値が 1250 ms の重要なクラスは除きます）。これらの値は、strict ポリシーより 25% 高く設定されています。
- Lenient：このポリシーは、1 レート 2 カラーで BC 値が 375 ms です（ただし、この値が 1500 ms の重要なクラスは除きます）。これらの値は、strict ポリシーより 50% 高く設定されています。
- Dense：このポリシーは 1 レート、2 カラーです。critical、normal、redirect、exception、undesirable、l2-default および default クラスの BC 値は 250 ms です。important、management、normal-dhcp、normal-dhcp-relay-response、および monitoring クラスの BC 値は 1000 ms です。l2-unpoliced クラスの BC 値は 5 MB です。

（注） シャーシが F2 シリーズ モジュールを満載している場合や、他の I/O モジュールよりも多くの F2 シリーズ モジュールを搭載している場合は、このデフォルト ポリシーを推奨します。

- Skip：コントロール プレーン ポリシーは適用されません。Cisco NX-OS の 5.2 以前のリリースでは、このオプション名は none です。

オプションを選択しなかった場合や、セットアップ ユーティリティを実行しなかった場合には、strict ポリシングが適用されます。strict ポリシーから開始し、必要に応じて、CoPP ポリシーを変更することを推奨します。

copp-system-p-policy ポリシーには、基本的なデバイス操作に最も適した値が設定されています。使用する DoS に対する保護要件に適合するよう、特定のクラスやアクセス コントロール リスト（ACL）を追加する必要があります。デフォルト CoPP ポリシーは Cisco NX-OS ソフトウェアをアップグレードしても変更されません。

注意 **skip** オプションを選択し、続いて CoPP 保護も設定しない場合、Cisco NX-OS デバイスは DoS 攻撃に対して脆弱な状態になります。

Cisco NX-OS リリース 5.2 以降のリリースでは、CLI プロンプトから **setup** コマンドを実行して再度セットアップ ユーティリティを起動する、または**copp profile** コマンドを使用して、CoPP のデフォルト ポリシーを再割り当てできます。

デフォルト クラス マップ

（注） ここで提供されるクラス マップは Cisco NX-OS リリース 6.2(2) 向けです。値の一部は、以前のリリースによって異なる場合があります。

copp-system-class-exception クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-exception
    match exception ip option
    match exception ip icmp unreachable
    match exception ipv6 option
    match exception ipv6 icmp unreachable
```

copp-system-class-critical クラスの設定は次のとおりです。

```
ip access-list copp-system-p-acl-igmp
    permit igmp any 224.0.0.0/3

ip access-list copp-system-p-acl-lisp
    permit udp any any eq 4342

ip access-list copp-system-p-acl-msdp
    permit tcp any gt 1024 any eq 639
    permit tcp any eq 639 any gt 1024
```

```
ip access-list copp-system-p-acl-bgp
    permit tcp any gt 1024 any eq bgp
    permit tcp any eq bgp any gt 1024

ip access-list copp-system-p-acl-eigrp
    permit eigrp any any

ip access-list copp-system-p-acl-lisp6
    permit udp any any eq 4342

ip access-list copp-system-p-acl-rip
    permit udp any 224.0.0.0/24 eq rip

ip access-list copp-system-p-acl-ospf
    permit ospf any any

ip access-list copp-system-p-acl-pim
    permit pim any 224.0.0.0/24


    permit udp any any eq 496
    permit ip any 224.0.0.13/32

ipv6 access-list copp-system-p-acl-bgp6
    permit tcp any gt 1024 any eq bgp
    permit tcp any eq bgp any gt 1024

ipv6 access-list copp-system-p-acl-ospf6
    permit 89 any any

ipv6 access-list copp-system-p-acl-pim6
    permit 103 any FF02::D/128
    permit udp any any eq pim-auto-rp

ipv6 access-list copp-system-p-acl-rip6
    permit udp any ff02::9/64 eq 521

ip access-list copp-system-p-acl-vpc
    permit udp any any eq 3200

ip access-list copp-system-p-acl-mpls-ldp
    permit udp any eq 646 any eq 646
    permit tcp any any eq 646
    permit tcp any eq 646 any

ip access-list copp-system-p-acl-mpls-oam
    permit udp any eq 3503 any

ip access-list copp-system-p-acl-mpls-rsvp
    permit 46 any any

ip access-list copp-system-p-acl-otv-as
    permit udp any any eq 8472

mac access-list copp-system-p-acl-mac-l2pt
  permit any 0100.0ccd.cdd0 0000.0000.0000

mac access-list copp-system-p-acl-mac-otv-isis
  permit any 0100.0cdf.dfdf 0000.0000.0000

mac access-list copp-system-p-acl-mac-fabricpath-isis
  permit any 0180.c200.0041 0000.0000.0000

mac access-list copp-system-p-acl-mac-l3-isis
    permit any 0180.c200.0015 0000.0000.0000
    permit any 0180.c200.0014.0000.0000.0000

class-map type control-plane match-any copp-system-p-class-critical
    match access-group name copp-system-p-acl-bgp
    match access-group name copp-system-p-acl-rip
    match access-group name copp-system-p-acl-vpc
    match access-group name copp-system-p-acl-bgp6
    match access-group name copp-system-p-acl-lisp
```

```
    match access-group name copp-system-p-acl-ospf
    match access-group name copp-system-p-acl-rip6
    match access-group name copp-system-p-acl-eigrp
    match access-group name copp-system-p-acl-lisp6
    match access-group name copp-system-p-acl-ospf6
    match access-group name copp-system-p-acl-eigrp6
    match access-group name copp-system-p-acl-otv-as
    match access-group name copp-system-p-acl-mac-l2pt
    match access-group name copp-system-p-acl-mpls-ldp
    match access-group name copp-system-p-acl-mpls-oam
    match access-group name copp-system-p-acl-mpls-rsvp
    match access-group name copp-system-p-acl-mac-l3-isis
    match access-group name copp-system-p-acl-mac-otv-isis
    match access-group name copp-system-p-acl-mac-fabricpath-isis
    match protocol mpls router-alert
    match protocol mpls exp 6
```

（注） LISP、LISP6 および MAC レイヤ 3 IS-IS ACL が、Cisco NX-OS リリース 6.1 で追加されました。

copp-system-class-important クラスの設定は次のとおりです。

```
ip access-list copp-system-p-acl-hsrp
    permit udp any 224.0.0.2/32 eq 1985
    permit udp any 224.0.0.102/32 eq 1985
```

（注） Cisco NX-OS リリース 6.2(2) 以降では、HSRP 制御パケットは、前述のように、既定の宛先アドレスを使用します。6.2(2) 以前の Cisco NX-OS リリースでは、ホットスタンバイ ルータ プロトコル（HSRP）ACL には、次の設定に示すように、最後のオクテットが無視された lenient エントリがあります。

```
ip access-list copp-system-p-acl-hsrp
    permit udp any 224.0.0.0/24 eq 1985
```

```
ipv6 access-list copp-system-p-acl-hsrp6
    permit udp any ff02::66/128 eq 2029

ip access-list copp-system-p-acl-vrrp

    permit ip any 224.0.0.18/32

ip access-list copp-system-p-acl-glbp
    permit udp any eq 3222 224.0.0.0/24 eq 3222

ip access-list copp-system-p-acl-pim-reg
    permit pim any any

ipv6 access-list copp-system-p-acl-icmp6-msgs
    permit icmp any any router-advertisement
    permit icmp any any router-solicitation
    permit icmp any any nd-na
    permit icmp any any nd-ns
    permit icmp any any mld-query
    permit icmp any any mld-report
    permit icmp any any mld-reduction
    permit icmp any any 143

ip access-list copp-system-p-acl-cts
    permit tcp any any eq 64999
    permit tcp any eq 64999 any

ip access-list copp-system-p-acl-pim-mdt-join
    permit udp any 224.0.0.13/32

ipv6 access-list copp-system-p-acl-vrrp6
```

```
    permit ipv6 any ff02::12/128

ip access-list copp-system-p-acl-wccp

    permit udp any eq 2048 any eq 2048

mac access-list copp-system-p-acl-mac-lldp
  permit any 0180.c200.000c 0000.0000.0000 0x88cc

mac access-list copp-system-p-acl-mac-flow-control
  permit any 0180.c200.0001 0000.0000.0000 0x8808

class-map type control-plane match-any copp-system-p-class-important
    match access-group name copp-system-p-acl-cts
    match access-group name copp-system-p-acl-glbp
    match access-group name copp-system-p-acl-hsrp
    match access-group name copp-system-p-acl-vrrp
    match access-group name copp-system-p-acl-wccp
    match access-group name copp-system-p-acl-hsrp6
    match access-group name copp-system-p-acl-vrrp6
    match access-group name copp-system-p-acl-mac-lldp
    match access-group name copp-system-p-acl-mac-flow-control
```

（注） 「permit icmp any any 143」ルールが Cisco NX-OS リリース 6.1 の MLDv2 レポートをサポートするために acl-icmp6-msgs ACL に追加されました。

（注） VRRP6 ACL が Cisco NX-OS リリース 6.2(2) で追加されました。

（注） Cisco NX-OS リリース 6.2(2) 以降では、マルチキャスト トラフィックの動作が、異なるクラスにおいて異なるレートでポリシングされることから、次のようにマルチキャスト トラフィックのタイプによって 3 つのクラス（マルチキャスト ホスト、マルチキャスト ルータ、標準）にグループ化され、一定のレートでポリシングされるように変更されました。

```
ip access-list copp-system-p-acl-igmp
  permit igmp any 224.0.0.0/3
ipv6 access-list copp-system-p-acl-mld
  permit icmp any any mld-query
  permit icmp any any mld-report
  permit icmp any any mld-reduction
  permit icmp any any 143
ip access-list copp-system-p-acl-msdp
  permit tcp any gt 1024 any eq 639
  permit tcp any eq 639 any gt 1024
ipv6 access-list copp-system-p-acl-ndp
  permit icmp any any router-solicitation
  permit icmp any any router-advertisement
  permit icmp any any 137
  permit icmp any any nd-ns
  permit icmp any any nd-na
ip access-list copp-system-p-acl-pim
  permit pim any 224.0.0.0/24
  permit udp any any eq 496
  permit ip any 224.0.0.13/32
ip access-list copp-system-p-acl-pim-mdt-join
  permit udp any 224.0.0.13/32
ip access-list copp-system-p-acl-pim-reg
  permit pim any any
ipv6 access-list copp-system-p-acl-pim6
  permit pim any ff02::d/128
```

```
  permit udp any any eq 496
ipv6 access-list copp-system-p-acl-pim6-reg
  permit pim any any
mac access-list copp-system-p-acl-mac-dot1x
  permit any 0180.c200.0003 0000.0000.0000 0x888e
class-map type control-plane match-any copp-system-p-class-multicast-host
  match access-group name copp-system-p-acl-mld
  match access-group name copp-system-p-acl-igmp
class-map type control-plane match-any copp-system-p-class-multicast-router
  match access-group name copp-system-p-acl-pim
  match access-group name copp-system-p-acl-msdp
  match access-group name copp-system-p-acl-pim6
  match access-group name copp-system-p-acl-pim-reg
  match access-group name copp-system-p-acl-pim6-reg
  match access-group name copp-system-p-acl-pim-mdt-join
class-map type control-plane match-any copp-system-p-class-ndp
  match access-group name copp-system-p-acl-ndp
```

copp-system-class-management クラスの設定は次のとおりです。

```
ip access-list copp-system-p-acl-tacacs
    permit tcp any any eq tacacs
    permit tcp any eq tacacs any

ip access-list copp-system-p-acl-radius
    permit udp any any eq 1812
    permit udp any any eq 1813
    permit udp any any eq 1645
    permit udp any any eq 1646
    permit udp any eq 1812 any
    permit udp any eq 1813 any
    permit udp any eq 1645 any
    permit udp any eq 1646 any

ip access-list copp-system-p-acl-ntp
    permit udp any any eq ntp

ip access-list copp-system-p-acl-ftp
    permit tcp any any eq ftp-data
    permit tcp any any eq ftp
    permit tcp any eq ftp-data any
    permit tcp any eq ftp any

ip access-list copp-system-p-acl-tftp
    permit udp any any eq tftp
    permit udp any any eq 1758
    permit udp any eq tftp any
    permit udp any eq 1758 any

ip access-list copp-system-p-acl-sftp
    permit tcp any any eq 115
    permit tcp any eq 115 any

ip access-list copp-system-p-acl-ssh
    permit tcp any any eq 22
    permit tcp any eq 22 any

ip access-list copp-system-p-acl-snmp
    permit udp any any eq snmp
    permit udp any any eq snmptrap

ip access-list copp-system-p-acl-telnet
    permit tcp any any eq telnet
    permit tcp any any eq 107
    permit tcp any eq telnet any
    permit tcp any eq 107 any

ipv6 access-list copp-system-p-acl-tacacs6
    permit tcp any any eq tacacs
    permit tcp any eq tacacs any

ipv6 access-list copp-system-p-acl-radius6
```

```
    permit udp any any eq 1812
    permit udp any any eq 1813
    permit udp any any eq 1645
    permit udp any any eq 1646
    permit udp any eq 1812 any
    permit udp any eq 1813 any
    permit udp any eq 1645 any
    permit udp any eq 1646 any

ipv6 access-list copp-system-p-acl-ntp6
    permit udp any any eq ntp
    permit udp any eq ntp any

ipv6 access-list copp-system-p-acl-tftp6
    permit udp any any eq tftp
    permit udp any any eq 1758
    permit udp any eq tftp any
    permit udp any eq 1758 any

ipv6 access-list copp-system-p-acl-ssh6
    permit tcp any any eq 22
    permit tcp any eq 22 any

ipv6 access-list copp-system-p-acl-telnet6
    permit tcp any any eq telnet
    permit tcp any any eq 107
    permit tcp any eq telnet any
    permit tcp any eq 107 any

class-map type control-plane match-any copp-system-p-class-management
    match access-group name copp-system-p-acl-tacacs
    match access-group name copp-system-p-acl-radius
    match access-group name copp-system-p-acl-ntp
    match access-group name copp-system-p-acl-ftp
    match access-group name copp-system-p-acl-tftp
    match access-group name copp-system-p-acl-sftp
    match access-group name copp-system-p-acl-ssh
    match access-group name copp-system-p-acl-snmp
    match access-group name copp-system-p-acl-telnet
    match access-group name copp-system-p-acl-tacacs6
    match access-group name copp-system-p-acl-radius6
    match access-group name copp-system-p-acl-ntp6
    match access-group name copp-system-p-acl-tftp6
    match access-group name copp-system-p-acl-ssh6
    match access-group name copp-system-p-acl-telnet6
```

copp-system-class-normal クラスの設定は次のとおりです。

```
ip access-list copp-system-p-acl-dhcp
  permit udp any neq bootps any eq bootps
  permit udp any eq bootpc any

ip access-list copp-system-p-acl-dhcp-relay-response
  permit udp any eq bootps any
  permit udp any any eq bootpc

mac access-list copp-system-p-acl-mac-dot1x
  permit any 0180.c200.0003 0000.0000.0000 0x888e

class-map type control-plane match-any copp-system-p-class-normal
   match access-group name copp-system-p-acl-mac-dot1x
   match exception multicast directly-connected-sources
   match protocol arp

class-map type control-plane match-any copp-system-p-class-normal-dhcp
  match redirect dhcp-snoop
  match access-group name copp-system-p-acl-dhcp

class-map type control-plane match-any copp-system-p-class-normal-dhcp-relay-response
  match access-group name copp-system-p-acl-dhcp-relay-response
```

copp-system-class-redirect クラスの設定は次のとおりです。

```
class-map type control-plane match-any copp-system-p-class-redirect
    match redirect arp-inspect
```

copp-system-class-monitoring クラスの設定は次のとおりです。

```
ip access-list copp-system-p-acl-icmp
    permit icmp any any echo
    permit icmp any any echo-reply

ip access-list copp-system-p-acl-traceroute
    permit icmp any any ttl-exceeded
    permit icmp any any port-unreachable
    permit udp any any range 33434 33534

ipv6 access-list copp-system-p-acl-icmp6
    permit icmp any any echo-request
    permit icmp any any echo-reply

class-map type control-plane match-any copp-system-p-class-monitoring
    match access-group name copp-system-p-acl-icmp
    match access-group name copp-system-p-acl-traceroute
    match access-group name copp-system-p-acl-icmp6
```

copp-system-class-l2-unpoliced クラスの設定は次のとおりです。

```
mac access-list copp-system-p-acl-mac-cdp-udld-vtp
    permit any 0100.0ccc.cccc 0000.0000.0000

mac access-list copp-system-p-acl-mac-stp
    permit any 0100.0ccc.cccd 0000.0000.0000
    permit any 0180.c200.0000 0000.0000.0000

mac access-list copp-system-p-acl-mac-lacp
    permit any 0180.c200.0002 0000.0000.0000 0x8809

mac access-list copp-system-p-acl-mac-cfsoe
    permit any 0180.C200.000E 0000.0000.0000 0x8843

mac access-list copp-system-p-acl-mac-gold
    permit any any 0x3737

mac access-list copp-system-p-acl-mac-l2-tunnel
    permit any any 0x8840

class-map type control-plane copp-system-p-class-l2-unpoliced
    match access-group name copp-system-p-acl-mac-stp
    match access-group name copp-system-p-acl-mac-lacp
    match access-group name copp-system-p-acl-mac-cfsoe
    match access-group name copp-system-p-acl-mac-sdp-srp
    match access-group name copp-system-p-acl-mac-l2-tunnel
    match access-group name copp-system-p-acl-mac-cdp-udld-vtp
    match access-group name copp-system-p-acl-mac-gold
```

（注） MAC レイヤ 2 トンネル ACL が、Cisco NX-OS リリース 6.1 で追加されました。

copp-system-class-l2-default クラスの設定は次のとおりです。

```
mac access-list copp-system-p-acl-mac-undesirable
    permit any any

class-map type control-plane copp-system-p-class-l2-default
```

```
    match access-group name copp-system-p-acl-mac-undesirable
    match protocol mpls
```

copp-system-class-fcoe クラスの設定は次のとおりです。

```
mac access-list copp-system-p-acl-mac-fcoe
    permit any any 0x8906
    permit any any 0x8914

class-map type control-plane match-any copp-system-p-class-fcoe
    match access-group name copp-system-p-acl-mac-fcoe
```

（注） copp-system-class-fcoe クラスが、Cisco NX-OS リリース 6.1 で追加されました。

copp-system-class-undesirable クラスの設定は次のとおりです。

```
ip access-list copp-system-p-acl-undesirable
    permit udp any any eq 1434

class-map type control-plane match-any copp-system-p-class-undesirable
    match access-group name copp-system-p-acl-undesirable
    match exception fcoe-fib-miss
```

（注） fcoe-fib-miss 一致例外が、Cisco NX-OS リリース 6.1 で追加されました。

```
mac access-list copp-system-acl-mac-cdp-udld-vtp
  permit any 0100.0ccc.cccc 0000.0000.0000
mac access-list copp-system-acl-mac-cfsoe
  permit any 0180.c200.000e 0000.0000.0000 0x8843
mac access-list copp-system-acl-mac-dot1x
  permit any 0180.c200.0003 0000.0000.0000 0x888e
mac access-list copp-system-acl-mac-flow-control
  permit any 0180.c200.0001 0000.0000.0000 0x8808
mac access-list copp-system-acl-mac-gold
  permit any any 0x3737
mac access-list copp-system-acl-mac-l2mp-isis
  permit any 0180.c200.0015 0000.0000.0000
  permit any 0180.c200.0014 0000.0000.0000
mac access-list copp-system-acl-mac-l2pt
  permit any 0100.0ccd.cdd0 0000.0000.0000
mac access-list copp-system-acl-mac-lacp
  permit any 0180.c200.0002 0000.0000.0000 0x8809
mac access-list copp-system-acl-mac-lldp
  permit any 0180.c200.000e 0000.0000.0000 0x88c
mac access-list copp-system-acl-mac-stp
  permit any 0100.0ccc.cccd 0000.0000.0000
  permit any 0180.c200.0000 0000.0000.0000
mac access-list copp-system-acl-mac-undesirable
  permit any any
```

strict デフォルト CoPP ポリシー

Cisco NX-OS リリース 6.2(2) での strict CoPP ポリシーの設定は次のとおりです。

```
policy-map type control-plane copp-system-p-policy-strict

    class copp-system-p-class-critical
        set cos 7
```

```
    police cir 36000 kbps bc 250 ms conform transmit violate drop

class copp-system-p-class-important
    set cos 6
    police cir 1400 kbps bc 1500 ms conform transmit violate drop

class copp-system-p-class-multicast-router
    set cos 6
    police cir 2600 kbps bc 1000 ms conform transmit violate drop

class copp-system-p-class-management
    set cos 2
    police cir 10000 kbps bc 250 ms conform transmit violate drop

class copp-system-p-class-multicast-host
    set cos 1
    police cir 1000 kbps bc 1000 ms conform transmit violate drop

class copp-system-p-class-normal
    set cos 1
    police cir 680 kbps bc 250 ms conform transmit violate drop

class copp-system-p-class-ndp
    set cos 6
    police cir 680 kbps bc 250 ms conform transmit violate drop

class copp-system-p-class-normal-dhcp
    set cos 1
    police cir 1500 kbps bc 250 ms conform transmit violate drop

class copp-system-p-class-normal-dhcp-relay-response
    set cos 1
    police cir 1800 kbps bc 500 ms conform transmit violate drop

class copp-system-p-class-redirect
    set cos 1
    police cir 280 kbps bc 250 ms conform transmit violate drop

class copp-system-p-class-exception
    set cos 1
    police cir 360 kbps bc 250 ms conform transmit violate drop

class copp-system-p-class-monitoring
    set cos 1
    police cir 130 kbps bc 1000 ms conform transmit violate drop

class copp-system-p-class-l2-unpoliced
    police cir 8 gbps bc 5 mbytes conform transmit violate transmit

class copp-system-p-class-undesirable
    set cos 0
    police cir 32 kbps bc 250 ms conform drop violate drop

class copp-system-p-class-fcoe
    set cos 6
    police cir 1060 kbps bc 1000 ms conform transmit violate drop

class copp-system-p-class-l2-default
    police cir 10 kbps bc 250 ms conform transmit violate drop

class class-default
    set cos 0
    police cir 10 kbps bc 250 ms conform transmit violate drop
```

（注） copp-system-p-class-fcoe クラスが、Cisco NX-OS リリース 6.1 で追加されました。copp-system-p-class-multicast-router および copp-system-p-class-multicast-host クラスが、Cisco NX-OS リリース 6.2(2) で追加されました。

moderate デフォルト CoPP ポリシー

Cisco NX-OS リリース 6.2(2) での moderate CoPP ポリシーの設定は次のとおりです。

```
policy-map type control-plane copp-system-p-policy-moderate

    class copp-system-p-class-critical
        set cos 7
        police cir 36000 kbps bc 310 ms conform transmit violate drop

    class copp-system-p-class-important
        set cos 6
        police cir 1400 kbps bc 1250 ms conform transmit violate drop

    class copp-system-p-class-multicast-router
        set cos 6
        police cir 2600 kbps bc 1000 ms conform transmit violate drop

    class copp-system-p-class-management
        set cos 2
        police cir 10000 kbps bc 310 ms conform transmit violate drop

    class copp-system-p-class-multicast-host
        set cos 1
        police cir 1000 kbps bc 1000 ms conform transmit violate drop

    class copp-system-p-class-normal
        set cos 1
        police cir 680 kbps bc 310 ms conform transmit violate drop

    class copp-system-p-class-ndp
        set cos 6
        police cir 680 kbps bc 310 ms conform transmit violate drop

    class copp-system-p-class-normal-dhcp
        set cos 1
        police cir 1500 kbps bc 310 ms conform transmit violate drop

    class copp-system-p-class-normal-dhcp-relay-response
        set cos 1
        police cir 1800 kbps bc  620  ms conform transmit violate drop

    class copp-system-p-class-redirect
        set cos 1
        police cir 280 kbps bc 310 ms conform transmit violate drop

    class copp-system-p-class-exception
        set cos 1
        police cir 360 kbps bc 310 ms conform transmit violate drop

    class copp-system-p-class-monitoring
        set cos 1
        police cir 130 kbps bc 1250 ms conform transmit violate drop

    class copp-system-p-class-l2-unpoliced
        police cir 8 gbps bc 5 mbytes conform transmit violate transmit

    class copp-system-p-class-undesirable
        set cos 0
        police cir 32 kbps bc 310 ms conform drop violate drop

    class copp-system-p-class-fcoe
        set cos 6
        police cir 1060 kbps bc 1250 ms conform transmit violate drop

    class copp-system-p-class-l2-default
        police cir 10 kbps bc 310 ms conform transmit violate drop

    class class-default
        set cos 0
```

```
        police cir 10 kbps bc 250 ms conform transmit violate drop
```

（注） copp-system-p-class-fcoe クラスが、Cisco NX-OS リリース 6.1 で追加されました。copp-system-p-class-multicast-router および copp-system-p-class-multicast-host クラスが、Cisco NX-OS リリース 6.2(2) で追加されました。

lenient デフォルト CoPP ポリシー

Cisco NX-OS リリース 6.2(2) での lenient CoPP ポリシーの設定は次のとおりです。

```
policy-map type control-plane copp-system-p-policy-lenient

    class copp-system-p-class-critical
        set cos 7
        police cir 36000 kbps bc 375 ms conform transmit violate drop

    class copp-system-p-class-important
        set cos 6
        police cir 1400 kbps bc 1500 ms conform transmit violate drop

    class copp-system-p-class-multicast-router
        set cos 6
        police cir 2600 kbps bc 1000 ms conform transmit violate drop

    class copp-system-p-class-management
        set cos 2
        police cir 10000 kbps bc 375 ms conform transmit violate drop

    class copp-system-p-class-multicast-host
        set cos 1
        police cir 1000 kbps bc 1000 ms conform transmit violate drop

    class copp-system-p-class-normal
        set cos 1
        police cir 680 kbps bc 375 ms conform transmit violate drop

    class copp-system-p-class-ndp
        set cos 6
        police cir 680 kbps bc 375 ms conform transmit violate drop

    class copp-system-p-class-normal-dhcp
        set cos 1
        police cir 1500 kbps bc 375 ms conform transmit violate drop

    class copp-system-p-class-normal-dhcp-relay-response
        set cos 1
        police cir 1800 kbps bc 750 ms conform transmit violate drop

    class copp-system-p-class-redirect
        set cos 1
        police cir 280 kbps bc 375 ms conform transmit violate drop

    class copp-system-p-class-exception
        set cos 1
        police cir 360 kbps bc 375 ms conform transmit violate drop

    class copp-system-p-class-monitoring
        set cos 1
        police cir 130 kbps bc 1500 ms conform transmit violate drop

    class copp-system-p-class-l2-unpoliced
        police cir 8 gbps bc 5 mbytes conform transmit violate transmit

    class copp-system-p-class-undesirable
```

```
        set cos 0
        police cir 32 kbps bc 375 ms conform drop violate drop

    class copp-system-p-class-fcoe
        set cos 6
        police cir 1060 kbps bc 1500 ms conform transmit violate drop

    class copp-system-p-class-l2-default
        police cir 10 kbps bc 375 ms conform transmit violate drop

    class class-default
        set cos 0
        police cir 10 kbps bc 250 ms conform transmit violate drop
```

（注） copp-system-p-class-fcoe クラスが、Cisco NX-OS リリース 6.1 で追加されました。copp-system-p-class-multicast-router および copp-system-p-class-multicast-host クラスが、Cisco NX-OS リリース 6.2(2) で追加されました。

デンス デフォルト CoPP ポリシー

Cisco NX-OS リリース 6.2(2) でのデンス CoPP ポリシーの設定は次のとおりです。

```
policy-map type control-plane copp-system-p-policy-dense
  class copp-system-p-class-critical
    set cos 7
    police cir 4500 kbps bc 250 ms conform transmit violate drop
  class copp-system-p-class-important
    set cos 6
    police cir 1400 kbps bc 1500 ms conform transmit violate drop
  class copp-system-p-class-multicast-router
    set cos 6
    police cir 370 kbps bc 1000 ms conform transmit violate drop
  class copp-system-p-class-management
    set cos 2
    police cir 2500 kbps bc 1000 ms conform transmit violate drop
  class copp-system-p-class-multicast-host
    set cos 1
    police cir 190 kbps bc 1000 ms conform transmit violate drop
  class copp-system-p-class-normal
    set cos 1
    police cir 300 kbps bc 250 ms conform transmit violate drop
  class copp-system-p-class-ndp
    set cos 6
    police cir 300 kbps bc 250 ms conform transmit violate drop
  class copp-system-p-class-normal-dhcp
    set cos 1
    police cir 660 kbps bc 1000 ms conform transmit violate drop
  class copp-system-p-class-normal-dhcp-relay-response
    set cos 1
    police cir 800 kbps bc 1000 ms conform transmit violate drop
  class copp-system-p-class-redirect
    set cos 1
    police cir 200 kbps bc 250 ms conform transmit violate drop
  class copp-system-p-class-exception
    set cos 1
    police cir 200 kbps bc 250 ms conform transmit violate drop
  class copp-system-p-class-monitoring
    set cos 1
    police cir 130 kbps bc 1000 ms conform transmit violate drop
  class copp-system-p-class-l2-unpoliced
    police cir 8 gbps bc 5 mbytes conform transmit violate transmit
  class copp-system-p-class-undesirable
    set cos 0
    police cir 32 kbps bc 250 ms conform drop violate drop
```

```
class copp-system-p-class-fcoe
  set cos 6
  police cir 600 kbps bc 1000 ms conform transmit violate drop
class copp-system-p-class-l2-default
  police cir 10 kbps bc 250 ms conform transmit violate drop
class class-default
  set cos 0
  police cir 10 kbps bc 250 ms conform transmit violate drop
```

（注） copp-system-p-class-fcoe クラスが、Cisco NX-OS リリース 6.1 で追加されました。copp-system-p-class-multicast-router および copp-system-p-class-multicast-host クラスが、Cisco NX-OS リリース 6.2(2) で追加されました。

1 秒間あたりのパケットのクレジット制限

特定のポリシーの 1 秒間あたりのパケット（PPS）の合計（ポリシーの各クラス部分の PPS の合計）の上限は、PPS のクレジット制限（PCL）の上限になります。特定のクラスの PPS が増加して PCL 超過すると、設定が拒否されます。目的の PPS を増やすには、PCL を超える PPS の分を他のクラスから減少させる必要があります。

モジュラ QoS コマンドライン インターフェイス

CoPP は、モジュラ QoS コマンドライン インターフェイス（MQC）を使用します。MQC は CLI の構造を持っています。MQC を使用すると、トラフィック クラスの定義、トラフィック ポリシー（ポリシーマップ）の作成、およびインターフェイスへのトラフィック ポリシーの適用が可能になります。トラフィック ポリシーには、トラフィック クラスに適用する CoPP 機能を含めます。

手順の概要

1. **class-map** コマンドを使用して、トラフィック クラスを定義します。トラフィック クラスは、トラフィックの分類に使用します。
2. **policy-map** コマンドを使用して、トラフィック ポリシーを定義します。トラフィック ポリシー（ポリシー マップ）には、トラフィック クラスと、トラフィック クラスに適用する 1 つまたは複数の CoPP 機能を含めます。トラフィック ポリシー内の CoPP の機能で、分類されたトラフィックの処理方法が決まります。
3. **control-plane** コマンドおよび **service-policy** コマンドを使用して、トラフィック ポリシー（ポリシー マップ）をコントロール プレーンに適用します。

手順の詳細

ステップ 1 **class-map** コマンドを使用して、トラフィック クラスを定義します。トラフィック クラスは、トラフィックの分類に使用します。

次に、copp-sample-class と呼ばれる新しいマップを作成する例を示します。

```
class-map type control-plane copp-sample-class
```

ステップ 2 **policy-map** コマンドを使用して、トラフィック ポリシーを定義します。トラフィック ポリシー（ポリシー マップ）には、トラフィック クラスと、トラフィック クラスに適用する 1 つまたは複数の CoPP 機能を含めます。トラフィック ポリシー内の CoPP の機能で、分類されたトラフィックの処理方法が決まります。

ステップ 3 **control-plane** コマンドおよび **service-policy** コマンドを使用して、トラフィック ポリシー（ポリシー マップ）をコントロール プレーンに適用します。
次に、コントロール プレーンにポリシー マップを適用する例を示します。

```
control-plane
service-policy input copp-system-policy
```

（注） copp-system-policy は常に設定され、適用されます。このコマンドを明示的に使用する必要はありません。

CoPP と管理インターフェイス

Cisco NX-OS デバイスは、管理インターフェイス（mgmt0）をサポートしないハードウェア ベースの CoPP だけをサポートします。アウトオブバンド mgmt0 インターフェイスは CPU に直接接続するため、CoPP が実装されているインバンド トラフィック ハードウェアは通過しません。

mgmt0 インターフェイスで、ACL を設定して、特定タイプのトラフィックへのアクセスを許可または拒否することができます。

CoPP のバーチャライゼーション サポート

CoPP はデフォルト仮想デバイス コンテキスト（VDC）または管理者 VDC のみで設定できますが、その CoPP 設定は Cisco NX-OS デバイス上のすべての VDC に適用されます。VDC の詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

CoPP のライセンス要件

この機能には、ライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべて Cisco NX-OS システム イメージにバンドルされており、追加費用は一切発生しません。NX-OS ライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

CoPP の注意事項と制約事項

CoPP に関する注意事項と制約事項は次のとおりです。

- 最初に strict デフォルト CoPP ポリシーを使用し、後で、データセンターおよびアプリケーションの要件に基づいて CoPP ポリシーを変更することを推奨します。

- シャーシが F2 または F2e シリーズ モジュールを満載している場合や、他のタイプの I/O モジュールよりも多くの F2 または F2e シリーズ モジュールを搭載している場合は、デフォルトのデンス ポリシーを適用することを推奨します。
- シャーシが F2 または F2e と M シリーズの両方のモジュールを搭載している場合は、スケール ファクタを設定し、デフォルトのデンス ポリシーを適用することを推奨します。
- CoPP のカスタマイズは継続的なプロセスです。CoPP を設定するときには、特定の環境で使用されるプロトコルや機能に加えて、サーバ環境に必要なスーパーバイザ機能を考慮する必要があります。これらのプロトコルや機能が変更されたら、CoPP を変更する必要があります。
- CoPP を継続的にモニタすることを推奨します。ドロップが発生した場合は、CoPP がトラフィックを誤ってドロップしたのか、または誤動作や攻撃に応答してドロップしたのかを判定してください。いずれの場合も、状況を分析し、CoPP ポリシーを変更する必要を評価します。
- 他のクラスマップで指定しないトラフィックはすべて、最後のクラス（デフォルト クラス）に配置されます。このクラス内のドロップをモニタし、これらのドロップが必要のないトラフィックに基づいているのか、または設定されていないために追加が必要な機能の結果であるかどうかを調査します。
- アクセス コントロール リスト（ACL）を通してルータ プロセッサにリダイレクトする必要のあるパケット（たとえば、ARP および DHCP）を判定するために、すべてのブロードキャスト トラフィックが CoPP ロジックを通して送信されます。リダイレクトする必要のないブロードキャスト トラフィックは CoPP ロジックに対して照合され、準拠したパケットと違反したパケットの両方がハードウェア内でカウントされますが、CPU には送信されません。CPU に送信する必要のあるブロードキャスト トラフィックと、CPU に送信する必要のないブロードキャスト トラフィックを異なるクラスに分離する必要があります。
- **set cos** 設定を削除する場合、M1 シリーズ モジュールと SVI とトランク ポートがある F2/F2e シリーズ モジュール間の動作に違いがあります。M1 シリーズ モジュールでは、DSCP と UserPriority（UP）両方によって（VLAN ヘッダーで）レイヤ 3 制御パケットを受信すると、キューイングは DSCP を使用して実行されます。F2/F2e シリーズ モジュールでは、キューイングは UP を使用して実行されます。
- 5.2 より前の Cisco NX-OS リリースでは、デフォルトの copp-system-policy ポリシーを変更または再適用するにはセットアップ ユーティリティを使用する必要があります。セットアップ ユーティリティにアクセスするには、CLI で **setup** コマンドを使用します。
- CoPP を設定した後、古いクラス マップや未使用のルーティング プロトコルなど、使用されていないものはすべて削除してください。
- CoPP ポリシーによって、ルーティング プロトコルなどのクリティカルなトラフィック、またはデバイスへのインタラクティブなアクセスがフィルタリングされないように注意してください。このトラフィックをフィルタリングすると、Cisco NX-OS デバイスへのリモート アクセスが禁止され、コンソール接続が必要となる場合があります。

- Cisco NX-OS ソフトウェアは、出力 CoPP とサイレント モードをサポートしません。CoPP は、入力でのみサポートされます（コントロール プレーン インターフェイスに対して **service-policy output copp** コマンドは使用できません）。
- ハードウェアのアクセス コントロール エントリ（ACE）ヒット カウンタは、ACL 論理だけで使用できます。CPU のトラフィックを評価するには、ソフトウェアの ACE ヒット カウンタと **show access-lists** および **show policy-map type control-plane** コマンドを使用します。
- Cisco NX-OS デバイスのハードウェアは、フォワーディング エンジン単位で CoPP を実行します。CoPP は分散ポリシーをサポートしていません。したがって、レートを選択する場合は、集約トラフィックでスーパーバイザ モジュールに過剰な負荷をかけることのない値にしてください。
- スーパーバイザに到達し、CoPP によってドロップされる可能性のあるトラフィックのよりきめ細かなビューを取得するには、SVI で NetFlow 機能を使用できます。それには、ACL ヒット カウントを NetFlow テーブルに示されている値と比較します。
- F1 シリーズ モジュールでは、CoPP はサポートされません。
- Cisco NX-OS Release 5.0 では、CoPP は非 IP トラフィックの分類をサポートしていません。代わりに、ACL を使用して、スーパーバイザ モジュールに到達する非 IP トラフィックをドロップまたは制限できます。
- Cisco NX-OS Release 5.1 から、次のルールが適用されます。
  - CoPP では、非 IP および IP トラフィック クラスがサポートされます。
  - L2PT、OTV-ISIS、および FabricPath-ISIS パケットは、copp-system-class-critical ポリシーの下に分類されます。
  - LLDP およびフロー制御パケットは、copp-system-class-important ポリシーの下に分類されます。
  - Dot1x パケットは、copp-system-class-normal のポリシーの下に分類されます。
  - STP、CDP、UDLD、VTP、LACP、GOLD、および CFSoE パケットは、copp-system-class-l2-unpoliced ポリシーの下に分類されます。これらのパケットは分類されるだけで、ポリシングはされません。対応するポリサーによって、統計情報が簡単に表示されます。これらのパケットは、常にスーパーバイザに転送されます。
  - 非 IP トラフィックの残りは、copp-system-class-l2-default ポリシーの下に分類されます。
  - どの copp クラスにも一致しない IP トラフィックは、class-default ポリシーの下に分類されます。
- CoPP MAC ポリシーは、Cisco NX-OS Release 5.1 からサポートされます。
- インサービス ソフトウェア グレード（ISSU）を使用して Cisco NX-OS Release 5.1 にアップグレードする場合は、FabricPath、OTV、L2PT、LLDP、DHCP、および DOT1X の機能のデフォルト CoPP ポリシーを手動で設定する必要があります。

- Cisco NX-OS Release 5.2 から、CoPP のベスト プラクティス ポリシーは読み取り専用です。その設定を変更する場合は、それをコピーする必要があります。コピーされたポリシーは、ユーザの設定として扱われます。
- ISSU を使用して Cisco NX-OS Release 5.2 にアップグレードする場合は、コントロール プレーンにアタッチされたポリシーがユーザ設定のポリシーとして扱われます。**show copp profile** コマンドを使用して CoPP プロファイルを確認し、必要な変更を加えます。
- インサービス ソフトウェア ダウングレード（ISSD）を使用して Cisco NX-OS Release 5.2 からダウングレードする場合は、CoPP によって互換性のない設定が報告され、CoPP プロファイルをコピーするよう指示されます。それ以前のバージョンでは、すべての設定がユーザ コンフィギュレーション モードに復元されます。
- ISSD を使用せずに Cisco NX-OS Release 5.2 からダウングレードする場合、CoPP 設定は失われ、CoPP ポリシーがコントロール プレーンにアタッチされなくなります。
- ISSU を使用して新しい Cisco NX-OS リリースにアップグレードする場合、新しいリリースのデフォルト CoPP ポリシーは適用されません。独自に設定された CoPP ポリシーがあって、それを使用し続けたい可能性があるため、以前のリリースのポリシーが引き続き適用されます。ただし、以前のバージョンでデフォルトの CoPP ポリシーを変更していない場合は、Cisco NX-OS リリース 5.2 以降のリリースをインストールするときに、**copp profile** [**strict** | **moderate** | **lenient**] コマンドを使用してそのバージョンの最新のデフォルトの CoPP ポリシーを適用することを推奨します。このアクションにより、前のポリシーが削除され新しいポリシーが適用されます。
- Cisco NX-OS リリース 5.2 以降では、デフォルトの CoPP ポリシーは読み取り専用です。修正を行うには、**copp copy profile** {**strict** | **moderate** | **lenient**} {**prefix** | **suffix**} *string* を使用してデフォルトのプロファイルをコピーして、変更を行い、**service-policy input***policy-map-name* コマンドを使用してコントロール プレーンにそのポリシーを適用します。
- 複数のフローが同じクラスにマッピングされる場合、個々のフローの統計情報は使用できません。
- SNMP による CoPP のモニタリングのサポートは、リストされた cbQoSMIB テーブルとコントロール プレーンにアタッチされた要素に限定されます。

（注） Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

CoPP のデフォルト設定

次の表に、CoPP パラメータのデフォルト設定を示します。

表 *55* : *CoPP* パラメータのデフォルト設定

パラメータ	デフォルト
デフォルト ポリシー	strict
デフォルト ポリシー	9 ポリシー エントリ （注） 関連するクラス マップでサポートされるポリシーの最大数は 128 です。
スケール ファクタ値	1.00

CoPP の設定

ここでは、CoPP の設定方法について説明します。

コントロール プレーン クラス マップの設定

コントロール プレーン ポリシーのコントロール プレーン クラス マップを設定する必要があります。

トラフィックを分類するには、既存の ACL に基づいてパケットを照合します。ACL キーワードの permit および deny は、照合時には無視されます。

IP バージョン 4（IPv4）および IP バージョン 6（IPv6）のパケットに対してポリシーを設定できます。

はじめる前に

デフォルト VDC にいることを確認します。

クラス マップ内で ACE ヒット カウンタを使用する場合は、IP ACL が設定してあることを確認します。

手順の概要

1. switch# **configure terminal**
2. switch(config)# **class-map type control-plane** [**match-all** | **match-any**] *class-map-name*
3. （任意） switch(config-cmap)# **match access-group name***access-list-name*
4. （任意） switch(config-cmap)# **match exception** {**ip** | **ipv6**} **icmp redirect**
5. （任意） switch(config-cmap)# **match exception** {**ip** | **ipv6**} **icmp unreachable**
6. （任意） switch(config-cmap)# **match exception** {**ip** | **ipv6**} **option**
7. （任意） switch(config-cmap)# **match exception** {**ip** | **ipv6**} **unicast rpf-failure**
8. switch(config-cmap)# **match protocol arp**
9. （任意） switch(config-cmap)# **match redirect arp-inspect**
10. （任意） switch(config-cmap)# **match redirect dhcp-snoop**
11. switch(config-cmap)# **exit**
12. （任意） switch(config)# **show class-map type control-plane** [*class-map-name*]
13. （任意） switch(config)# **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	switch(config)# **class-map type control-plane** [**match-all** | **match-any**] *class-map-name*	コントロールプレーン クラスマップを指定し、クラスマップ コンフィギュレーション モードを開始します。デフォルトのクラス一致は match-any です。名前は最大 64 文字で、大文字と小文字は区別されます。 （注） class-default、match-all、または match-any をクラス マップ名に使用できません。
ステップ 3	switch(config-cmap)# **match access-group name***access-list-name*	（任意） IP ACL のマッチングを指定します。 （注） ACL キーワードの permit および deny は、CoPP 照合時には無視されます。
ステップ 4	switch(config-cmap)# **match exception** {**ip** | **ipv6**} **icmp redirect**	（任意） IPv4 または IPv6 ICMP リダイレクト例外パケットのマッチングを指定します。
ステップ 5	switch(config-cmap)# **match exception** {**ip** | **ipv6**} **icmp unreachable**	（任意） IPv4 または IPv6 ICMP 到達不能例外パケットのマッチングを指定します。

	コマンドまたはアクション	目的
ステップ 6	switch(config-cmap)# **match exception** {**ip** | **ipv6**} **option**	（任意） IPv4 または IPv6 ICMP オプション例外パケットのマッチングを指定します。
ステップ 7	switch(config-cmap)# **match exception** {**ip** | **ipv6**} **unicast rpf-failure**	（任意） IPv4 または IPv6 のユニキャスト Reverse Path Forwarding（ユニキャスト RPF）例外パケットのマッチングを指定します。任意の CoPP クラス マップで、クラス マップのレート制限設定に従い、IPv4 または IPv6 の URPF 例外パケットをレート制限できます。
ステップ 8	switch(config-cmap)# **match protocol arp**	IP アドレス解決プロトコル（ARP）および逆アドレス解決プロトコル（RARP）パケットのマッチングを指定します。
ステップ 9	switch(config-cmap)# **match redirect arp-inspect**	（任意） ARP インスペクション リダイレクト パケットのマッチングを指定します。
ステップ 10	switch(config-cmap)# **match redirect dhcp-snoop**	（任意） DHCP スヌーピング リダイレクト パケットのマッチングを指定します。
ステップ 11	switch(config-cmap)# **exit**	クラスマップ コンフィギュレーション モードを終了します。
ステップ 12	switch(config)# **show class-map type control-plane** [*class-map-name*]	（任意） コントロールプレーン クラスマップの設定を表示します。
ステップ 13	switch(config)# **copy running-config startup-config**	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

コントロール プレーン ポリシー マップの設定

CoPP のポリシー マップを設定する必要があります。ポリシー マップにはポリシング パラメータを含めます。クラスのポリサーを設定しなかった場合、デフォルトのポリサー一致アクションは、ドロップです。Cisco NX-OS ソフトウェアは、クラスが 0 の 1 レート 2 カラー ポリシングと 2 レート 3 カラー ポリシング。

はじめる前に

デフォルト VDC にいることを確認します。

コントロール プレーン クラス マップが設定してあることを確認します。

手順の概要

1. **configure terminal**
2. **policy-map type control-plane***policy-map-name*
3. **class** {*class-map-name* [**insert-before***class-map-name2*] | **class-default**}
4. **police** [**cir**] {*cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]}
5. **police** [**cir**] {cir-rate [**bps** | **gbps** | **kbps** | **mbps** | **pps**]} [**bc**] *burst-size* [**bytes** | **kbytes** | **mbytes** | **ms** | **packets** | **us**]
6. **police** [**cir**] {*cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]} **conform** {**drop** | **set-cos-transmit***cos-value* | **set-dscp-transmit***dscp-value* | **set-prec-transmit***prec-value* | **transmit**} [**exceed** {**drop** | **set dscp dscp table cir-markdown-map** | **transmit**}] [**violate** {**drop** | **set dscp dscp table pir-markdown-map** | **transmit**}]
7. **police** [**cir**] {*cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]} **pir***pir-rate* [**bps** | **gbps** | **kbps** | **mbps**] [[**be**] *burst-size* [**bytes** | **kbytes** | **mbytes** | **ms** | **packets** | **us**]]
8. （任意） **logging drop threshold** [*drop-count* [**level** *syslog-level*]]
9. （任意） **setcos** [**inner**] *cos-value*
10. （任意） **setdscp** [**tunnel**] {*dscp-value* | **af11** | **af12** | **af13** | **af21** | **af22** | **af23** | **af31** | **af32** | **af33** | **af41** | **af42** | **af43** | **cs1** | **cs2** | **cs3** | **cs4** | **cs5** | **cs6** | **cs7** | **ef** | **default**}
11. （任意） **set precedence** [**tunnel**] {*prec-value* | **critical** | **flash** | **flash-override** | **immediate** | **internet** | **network** | **priority** | **routine**}
12. **exit**
13. **exit**
14. （任意） **show policy-map type control-plane** [**expand**] [**name***class-map-name*]
15. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**policy-map type control-plane***policy-map-name*
	
	例：
	`switch(config)# policy-map type control-plane ClassMapA`
	`switch(config-pmap)#`
		コントロールプレーンポリシーマップを指定し、ポリシーマップ コンフィギュレーション モードを開始します。ポリシーマップ名は最大64文字で、大文字と小文字は区別されます。

	コマンドまたはアクション	目的

ステップ 3	**class** {*class-map-name* [**insert-before***class-map-name2*] | **class-default**}
	
	例：
	`switch(config-pmap)# class ClassMapA`
	`switch(config-pmap-c)#`
		コントロールプレーン クラスマップ名またはクラスデフォルトを指定し、コントロールプレーン クラス コンフィギュレーション モードを開始します。
		class-default クラス マップは、必ずポリシー マップのクラス マップ リストの末尾に位置します。

ステップ 4	**police** [**cir**] {*cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]} 例： `switch(config-pmap-c)# police cir 52000`	認定情報レート（CIR）を指定します。レートの有効な範囲は、0 ～ 80000000000 です。CIR のデフォルト単位は bps です。
ステップ 5	**police** [**cir**] {cir-rate [**bps** | **gbps** | **kbps** | **mbps** | **pps**]} [**bc**] *burst-size* [**bytes** | **kbytes** | **mbytes** | **ms** | **packets** | **us**] 例： `switch(config-pmap-c)# police cir 52000 bc 1000`	CIR と Committed 認定バースト（BC）を指定します。CIR の有効な範囲は 0 ～ 80000000000 で、BC の有効な範囲は 0 ～ 512000000 です。CIR のデフォルト単位は bps で、BC サイズのデフォルト単位は **bytes** です。
ステップ 6	**police** [**cir**] {*cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]} **conform** {**drop** | **set-cos-transmit***cos-value* | **set-dscp-transmit***dscp-value* | **set-prec-transmit***prec-value* | **transmit**} [**exceed** {**drop** | **set dscp dscp table cir-markdown-map** | **transmit**}] [**violate** {**drop** | **set dscp dscp table pir-markdown-map** | **transmit**}] 例： `switch(config-pmap-c)# police cir 52000 conform transmit exceed drop`	CIR と一致アクションを指定します。CIR の有効な範囲は、0 ～ 80000000000 です。レートのデフォルト単位は bps です。*cos-value* と *prec-value* 引数の範囲は 0 ～ 7 です。*dscp-value* 引数の範囲は 0 ～ 63 です。 オプションは次のとおりです。 • **drop**：パケットをドロップします。 • **set-cos-transmit**：サービス クラス（CoS）値を設定します。 • **set-dscp-transmit**：DiffServ コードポイント値を設定します。 • **set-prec-transmit**：優先順位値を設定します。 • **transmit**：パケットを送信します。 • **set dscp dscp table cir-markdown-map**：超過（exceed）アクションを CIR マークダウン マップに設定します。 • **set dscp dscp table pir-markdown-map**：違反（violate）アクションを PIR マークダウン マップに設定します。 （注） 同じ CIR に BC と一致（conform）アクションを指定できます。

	コマンドまたはアクション	目的
ステップ 7	**police** [**cir**] {*cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]} **pir***pir-rate* [**bps** | **gbps** | **kbps** | **mbps**] [[**be**] *burst-size* [**bytes** | **kbytes** | **mbytes** | **ms** | **packets** | **us**]] 例： `switch(config-pmap-c)# police cir 52000 pir 78000 be 2000`	CIR と最大情報レート（PIR）を指定します。CIR の有効な範囲は 0 ～ 80000000000 で、PIR の有効な範囲は 1 ～ 80000000000 です。任意で Extended 拡張バースト（BE）サイズを設定できます。BE の有効な範囲は、1 ～ 512000000 です。CIR のデフォルト単位は **bps**、PIR のデフォルト単位は bps、および BE サイズのデフォルト単位は **bytes** です。 （注） 同じ CIR に BC、一致（conform）アクション、および PIR を指定できます。
ステップ 8	**logging drop threshold** [*drop-count* [**level** *syslog-level*]] 例： `switch(config-pmap-c)# logging drop threshold 100`	（任意） ドロップされたパケットのしきい値を指定し、ドロップ数が設定したしきい値を超えた場合、Syslog を生成します。*drop-count* 引数の範囲は 1 ～ 80000000000 バイトです。*syslog-level* 引数の範囲は 1 ～ 7 であり、デフォルト レベルは 4 です。
ステップ 9	**setcos** [**inner**] *cos-value* 例： `switch(config-pmap-c)# set cos 1`	（任意） 802.1Q CoS 値を指定します。Q-in-Q 環境には **inner** キーワードを使用します。有効な範囲は 0 ～ 7 です。デフォルト値は 0 です。
ステップ 10	**setdscp** [**tunnel**] {*dscp-value* | **af11** | **af12** | **af13** | **af21** | **af22** | **af23** | **af31** | **af32** | **af33** | **af41** | **af42** | **af43** | **cs1** | **cs2** | **cs3** | **cs4** | **cs5** | **cs6** | **cs7** | **ef** | **default**} 例： `switch(config-pmap-c)# set dscp 10`	（任意） IPv4 と IPv6 のパケットの DiffServ コード ポイント値を指定します。トンネル カプセル化を設定する場合は、**tunnel** キーワードを使用します。範囲は 0 ～ 63 です。デフォルト値は 0 です。
ステップ 11	**set precedence** [**tunnel**] {*prec-value* | **critical** | **flash** | **flash-override** | **immediate** | **internet** | **network** | **priority** | **routine**} 例： `switch(config-pmap-c)# set precedence 2`	（任意） IPv4 と IPv6 のパケットの優先順位値を指定します。トンネル カプセル化を設定する場合は、**tunnel** キーワードを使用します。有効な範囲は 0 ～ 7 です。デフォルト値は 0 です。

ステップ 12	**exit**
	
	例：
	`switch(config-pmap-c)# exit`
	`switch(config-pmap)#`
		ポリシー マップ クラス コンフィギュレーション モードを終了します。

ステップ 13	**exit**
	
	例：
	`switch(config-pmap)# exit`
	`switch(config)#`
		ポリシーマップ コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 14	**show policy-map type control-plane** [**expand**] [**name***class-map-name*] 例： `switch(config)# show policy-map type control-plane`	（任意） コントロール プレーン ポリシー マップの設定を表示します。
ステップ 15	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

コントロール プレーン サービス ポリシーの設定

CoPP サービス ポリシーに対して 1 つまたは複数のポリシー マップを設定できます。

はじめる前に

デフォルト VDC にいることを確認します。

コントロール プレーン ポリシー マップが設定してあることを確認します。

手順の概要

1. **configure terminal**
2. **control-plane**
3. **service-policy input** *policy-map-name*
4. **exit**
5. （任意） **show running-config copp** [**all**]
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的

ステップ 2	**control-plane**
	
	例：
	`switch(config)# control-plane`
	`switch(config-cp)#`
		コントロール プレーン コンフィギュレーション モードを開始します。

ステップ 3	**service-policy input** *policy-map-name* 例： `switch(config-cp)# service-policy input PolicyMapA`	入トラフィックのポリシーマップを指定します。ポリシーマップが複数ある場合は、このステップを繰り返します。 **no service-policy input** *policy-map-name* コマンドを使用して、コントロールプレーンからポリシーを削除します。

ステップ 4	**exit**
	
	例：
	`switch(config-cp)# exit`
	`switch(config)#`
		コントロール プレーン コンフィギュレーション モードを終了します。

ステップ 5	**show running-config copp** [**all**] 例： `switch(config)# show running-config copp`	（任意） CoPP 設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ラインカードごとの CoPP のスケール ファクタの設定

ラインカードごとの CoPP のスケール ファクタを設定できます。

スケール ファクタの設定は、特定のラインカードに適用された CoPP のポリシーのポリサー レートのスケーリングに使用されます。受け入れ値は 0.10 ～ 2.00 です。特定のラインカードに対して現在の CoPP ポリシーを変更せずに、ポリサー レートを増加または削減できます。変更はすぐに有効となるため、CoPP ポリシーを再適用する必要はありません。

（注） CoPP のプログラミングが各 I/O モジュールの転送エンジンで実行されます。Cisco Nexus 7000 M シリーズ I/O モジュールには 1 つまたは 2 つの転送エンジンを含むことができ、Cisco Nexus7000 F シリーズ モジュールにはモジュールに応じて 6 ~ 12 の転送エンジンを含むことができます。

M シリーズ モジュールで使用される同一の CoPP ポリシー プロファイル（ストリクト）が F シリーズ モジュールで適用される場合、F シリーズ モジュールからスーパーバイザに来るトラフィックの回数を、M シリーズ モジュールから来るトラフィックよりも多くすることができます。スーパーバイザに過剰な負荷がかかるのを回避するために、F シリーズ モジュールと、F シリーズ モジュールおよび M シリーズ モジュールの特定の組み合わせに対しデンス CoPP プロファイルを設定できます。

インストールされた I/O モジュールに基づいて、I/O モジュールごとにスケール ファクタを設定し、適切な CoPP ポリシープロファイルを適用するには、これらのガイドラインに従ってください。

- シャーシが F シリーズ モジュールを満載している場合は、スケール ファクタの設定なしでデンス プロファイルを適用することを推奨します。
- シャーシが M シリーズ モジュールを満載している場合は、スケール ファクタの設定なしでストリクト プロファイルを適用することを推奨します。
- シャーシが M シリーズ ライン カードよりも多くの F シリーズ ライン カードを搭載している場合は、M シリーズ ライン カードにのみデンス プロファイルを適用し、スケール ファクタ値 2 を設定することを推奨します。
- シャーシが F シリーズ ライン カードよりも多くの M シリーズ ライン カードを搭載している場合は、F シリーズ ライン カードにのみストリクト プロファイルを適用し、スケール ファクタ値 0.4 を設定することを推奨します。

はじめる前に

デフォルト VDC にいることを確認します。

手順の概要

1. **configure terminal**
2. **control-plane**
3. **scale-factor***value* **module***multiple-module-range*
4. （任意） **show running-config copp** [**all**]
5. （任意） **show policy-map interface control-plane** [**class***class-map* | **module***slot*]
6. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**control-plane**
	
	例：
	`switch(config)# control-plane`
	`switch(config-cp)#`
		コントロールプレーン コンフィギュレーション モードを開始します。

ステップ 3	**scale-factor***value* **module***multiple-module-range* 例： `switch(config-cp)# scale-factor 1.10 module 1-2`	ラインカードごとにポリサー レートを設定します。許可されたスケール ファクタ値は 0.10 ～ 2.00 です。スケール ファクタ値が設定されている場合、ポリシング値にはモジュールの対応するスケール ファクタ値が乗算され、特定のモジュールにプログラミングされます。 スケール ファクタ値をデフォルトの 1.00 に戻すには、**no scale-factor***value* **module***multiple-module-range* コマンドを使用するか、**scale-factor 1 module***multiple-module-range* コマンドを使用して明示的にデフォルトのスケール ファクタ値を 1.00 に設定します。
ステップ 4	**show running-config copp** [**all**] 例： `switch(config-cp)# show running-config copp`	（任意） 実行コンフィギュレーション内の CoPP 設定を表示します。
ステップ 5	**show policy-map interface control-plane** [**class***class-map* | **module***slot*] 例： `switch(config-cp)# show policy-map interface control-plane`	（任意） CoPP ポリシーが適用される場合に適用されるスケール ファクタ値を表示します。
ステップ 6	**copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

デフォルトの CoPP ポリシーの変更または再適用

別のデフォルト CoPP ポリシーに変更したり、同じデフォルト CoPP ポリシーを再適用したりすることができます。

（注） 5.2 よりも前の Cisco NX-OS リリースでデフォルト CoPP ポリシーを変更または再適用するには、設定ユーティリティを使用する必要があります。設定ユーティリティにアクセスするには **setup** コマンドを使用します。

手順の概要

1. [**no**] **copp profile** [**strict** | **moderate** | **lenient** | **dense**]
2. （任意） **show copp status**
3. （任意） **show running-config copp**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	[**no**] **copp profile** [**strict** | **moderate** | **lenient** | **dense**] 例： `switch(config)# copp profile moderate`	CoPP ベスト プラクティス ポリシーを適用します。
ステップ 2	**show copp status** 例： `switch(config)# show copp status`	（任意） 最後の設定動作およびそのステータスなど、CoPP のステータスを表示します。このコマンドを実行すると、CoPP ベスト プラクティス ポリシーがコントロール プレーンにアタッチされていることを確認することもできます。
ステップ 3	**show running-config copp** 例： `switch(config)# show running-config copp`	（任意） 実行コンフィギュレーション内の CoPP 設定を表示します。

CoPP ベスト プラクティス ポリシーのコピー

Cisco NX-OS Release 5.2 以降では、CoPP ベスト プラクティス ポリシーは、読み取り専用です。その設定を変更する場合は、それをコピーする必要があります。

手順の概要

1. **copp copy profile** {**strict** | **moderate** | **lenient** | **dense**} {**prefix** | **suffix**} *string*
2. （任意） **show copp status**
3. （任意） **show running-config copp**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**copp copy profile** {**strict**	**moderate**	**lenient**	**dense**} {**prefix**	**suffix**} *string* 例： `switch# copp copy profile strict prefix abc`	CoPP ベスト プラクティス ポリシーのコピーを作成します。 CoPP は、指定したプレフィックスまたはサフィックスのすべてのクラス マップおよびポリシー マップの名前を変更します。
ステップ 2	**show copp status** 例： `switch# show copp status`	（任意） 最後の設定動作およびそのステータスなど、CoPP のステータスを表示します。このコマンドを実行すると、コピーされたポリシーがコントロール プレーンにアタッチされていないことを確認することもできます。
ステップ 3	**show running-config copp** 例： `switch# show running-config copp`	（任意） コピーされたポリシー設定を含む、実行コンフィギュレーション内の CoPP 設定を表示します。

CoPP の設定の確認

CoPP の設定情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show policy-map type control-plane [**expand**] [**name** *policy-map-name*]	コントロール プレーン ポリシー マップと関連するクラス マップ、および CIR と BC の値を表示します。

コマンド	目的
show policy-map interface control-plane [**class** *class-map* | **module** *slot*]	ポリシーの値と関連するクラスマップ、およびポリシーごとまたはクラスマップごとのドロップが表示されます。また、CoPP ポリシーが適用されている場合は、スケール ファクタ値も表示されます。スケール ファクタ値がデフォルト（1.00）の場合は表示されません。 （注） スケール ファクタは各モジュールでCIR、BC、PIR、BE の値を内部的に変更しますが、その表示では設定された CIR、BC、PIR、BE の値だけが表示されます。モジュールに実際に適用される値は、スケール ファクタに設定値を掛けた値です。
show class-map type control-plane [*class-map-name*]	このクラス マップにバインドされている ACL を含め、コントロール プレーン クラス マップの設定を表示します。

コマンド	目的
show copp diff profile {**strict** | **moderate** | **lenient** | **dense**} [**prior-ver**] **profile** {**strict** | **moderate** | **lenient** | **dense**}	2 つの CoPP ベスト プラクティス ポリシーの違いを表示します。 **prior-ver** オプションを指定しない場合、このコマンドは、現在適用されている 2 つのデフォルトの CoPP のベスト プラクティス ポリシー（現在適用されている厳密なポリシーと現在適用されている中程度のポリシーなど）の差異を表示します。 **prior-ver** オプションを指定した場合、このコマンドは、現在適用されているデフォルトの CoPP ベストプラクティスポリシーと以前に適用したデフォルトの CoPP ベストプラクティスポリシーの違いを表示します（現在適用されている厳密なポリシーと以前適用した緩いポリシーなど）。
show copp profile {**strict** | **moderate** | **lenient** | **dense**}	クラスおよびポリサー値とともに、CoPP ベスト プラクティス ポリシーの詳細を表示します。
show ip access-lists [*acl-name*]	ACL を含むアクセス リストを表示します。**statistics per-entry** コマンドが使用されている場合は、特定のエントリのヒット カウントが表示されます。
show running-config aclmgr [**all**]	実行コンフィギュレーションのユーザ設定によるアクセス コントロール リスト（ACL）を表示します。**all** オプションを使用すると、実行コンフィギュレーションのデフォルト（CoPP 設定）とユーザ定義による ACL の両方が表示されます。

コマンド	目的
show running-config copp [**all**]	実行コンフィギュレーション内の CoPP 設定を表示します。
show startup-config aclmgr [**all**]	スタートアップ コンフィギュレーションのユーザ設定によるアクセス コントロール リスト（ACL）を表示します。**all** オプションを使用すると、スタートアップコンフィギュレーションのデフォルト（CoPP 設定）とユーザ定義による ACL の両方が表示されます。

これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

CoPP 設定ステータスの表示

はじめる前に

デフォルト VDC にいることを確認します。

手順の概要

1. switch# **show copp status**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **show copp status**	CoPP 機能の設定ステータスを表示します。

次に、CoPP 設定ステータスを表示する例を示します。

```
switch# show copp status
```

CoPP のモニタリング

はじめる前に

デフォルト VDC にいることを確認します。

手順の概要

1. switch# **show policy-map interface control-plane** [**class***class-map* | **module***slot*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **show policy-map interface control-plane** [**class***class-map* | **module***slot*]	適用された CoPP ポリシーの一部であるすべてのクラスに関して、パケットレベルの統計情報を表示します。 統計情報は、OutPackets（コントロールプレーンに対して許可されたパケット）と DropPackets（レート制限によってドロップされたパケット）に関して指定します。 （注） スーパーバイザ 3 または F2e シリーズ モジュールを使用すると、このコマンドの出力でバイト数の表示にレイヤ 3 パケット長が使用されます。M1、M2、または F2 シリーズ モジュールを使用すると、コマンドの出力ではバイト数にレイヤ 2 パケット長が使用されます。

次に、CoPP をモニタする例を示します。

```
switch# show policy-map interface control-plane
Control Plane

service-policy input: copp-system-policy-default

class-map copp-system-class-igmp (match-any)
match protocol igmp
police cir 1024 kbps , bc 65535 bytes
conformed 0 bytes; action: transmit
violated 0 bytes;
class-map copp-system-class-pim-hello (match-any)
match protocol pim
police cir 1024 kbps , bc 4800000 bytes
conformed 0 bytes; action: transmit
violated 0 bytes;
....
```

この例では、一致および違反したバイト数の 5 分間の移動平均およびピーク値が **show policy-map interface control-plane** コマンドの出力に表示されます。この例では、5 分間の提起レートは一致および違反したバイト数の 5 分間の移動平均、5 分間の違反レートは違反バイト数の 5 分間の移

動平均です。さらにピーク レートは、起動以降またはカウンタのリセット以降の最高値で、その発生時がタイムスタンプで示されます。

```
module 9:
    conformed 0 bytes,
        5-min offered rate 10 bytes/sec
        peak rate 12 bytes/sec at 12:29:38.654 UTC Sun Jun 30 2013
    violated 0 bytes,
        5-min violate rate 20 bytes/sec
        peak rate 22 bytes/sec at 12:26:22.652 UTC Sun Jun 30 2013
```

SNMP での CoPP のモニタリング

Cisco NX-OS Release 6.2(2) 以降、CoPP はシスコ クラスベースの QoS MIB（cbQoSMIB）をサポートします。CoPP 要素はすべて、SNMP を使用してモニタできるようになりました（ただし変更は不可）。この機能は、コントロール プレーンにアタッチされたポリシーとサブ要素（クラス、一致ルール、セットアクションなど）にのみ適用されます。コントロールプレーンで使用されていないポリシーの要素は、SNMP では見えません。

次の cbQoSMIB テーブルがサポートされます。

- ccbQosServicePolicy
- cbQosInterfacePolicy
- cbQosObjects
- cbQosPolicyMapCfg
- cbQosClassMapCfg
- cbQosMatchStmtCfg
- cbQosPoliceCfg
- cbQosSetCfg

cbQoSMIB テーブルと要素の詳細情報は、次の URL で入手可能です：

- http://tools.cisco.com/Support/SNMP/do/BrowseOID.do?local=en&translate=Translate&objectInput=1.3.6.1.4.1.9.9.166
- http://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus6000/sw/system_management/7x/b_6k_System_Mgmt_Config_7x/b_6k_System_Mgmt_Config_7x_chapter_010110.html

CoPP 統計情報のクリア

はじめる前に

デフォルト VDC にいることを確認します。

手順の概要

1. （任意） switch# **show policy-map interface control-plane** [**class** *class-map* | **module** *slot*]
2. switch# **clear copp statistics**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	switch# **show policy-map interface control-plane** [**class** *class-map* | **module** *slot*]	（任意） 現在適用されている CoPP ポリシーおよびクラスごとの統計情報を表示します。
ステップ 2	switch# **clear copp statistics**	CoPP 統計情報をクリアします。

次に、インターフェース環境で、CoPP 統計情報をクリアする例を示します。

```
switch# show policy-map interface control-plane
switch# clear copp statistics
```

CoPP の設定例

ここでは、CoPP の設定例を示します。

CoPP Configuration Example

The following example shows how to configure CoPP using IP ACLs and MAC ACLs:

```
configure terminal
ip access-list copp-system-acl-igmp
permit igmp any 10.0.0.0/24

ip access-list copp-system-acl-msdp
permit tcp any any eq 639

mac access-list copp-system-acl-arp
permit any any 0x0806

ip access-list copp-system-acl-tacas
permit udp any any eq 49

ip access-list copp-system-acl-gre
permit 47 any any

ip access-list copp-system-acl-ntp
permit udp any 10.0.1.1/23 eq 123

ip access-list copp-system-acl-icmp
permit icmp any any

class-map type control-plane match-any copp-system-class-critical
match access-group name copp-system-acl-igmp
```

```
match access-group name copp-system-acl-msdp

class-map type control-plane match-any copp-system-class-important
match access-group name copp-system-acl-gre

class-map type control-plane match-any copp-system-class-normal
match access-group name copp-system-acl-icmp
match exception ip icmp redirect
match exception ip icmp unreachable
match exception ip option
match redirect arp-inspect
match redirect dhcp-snoop

policy-map type control-plane copp-system-policy

class copp-system-class-critical
police cir 2000 kbps bc 1500 bytes pir 3000 kbps be 1500 bytes conform
    transmit exceed transmit violate drop

class copp-system-class-important
police cir 1000 kbps bc 1500 bytes pir 1500 kbps be 1500 bytes conform
    transmit exceed transmit violate drop

class copp-system-class-normal
police cir 400 kbps bc 1500 bytes pir 600 kbps be 1500 bytes conform
    transmit exceed transmit violate drop

class class-default
police cir 200 kbps bc 1500 bytes pir 300 kbps be 1500 bytes conform
    transmit exceed transmit violate drop

control-plane
service-policy input copp-system-policy
```

The following example shows how to create the CoPP class and associate an ACL:

```
class-map type control-plane copp-arp-class
match access-group name copp-arp-acl
```

The following example shows how to add the class to the CoPP policy:

```
policy-map type control-plane copp-system-policy
class copp-arp-class
police pps 500
```

ICMP ping と ARP 要求の分割による CoPP のオーバーフローの防止

一部のサーバでは、アクティブな NIC が集約スイッチにアクセスできることを確認するために、デフォルト ゲートウェイに対する ICMP ping と ARP 要求を使用しています。その結果として CoPP 値が超過すると、CoPP はすべてのネットワークに対してトラフィックのドロップを開始します。正しく機能していないサーバが大量の ICMP ping および ARP 要求を送信すると、ある集約ブロック内にあるすべてのサーバでアクティブな NIC が失われ、NIC の切り替えが開始されます。

使用しているサーバがこのように設定されている場合は、サブネットのサブネットまたはグループに基づいて ICMP ping と ARP 要求を分割することにより、CoPP のオーバーフローを最小限に抑えることができます。その後、サーバで障害が発生して CoPP がオーバーフローした場合でも、スーパーバイザが一部のサブネットワークでのみ ICMP ping と ARP 要求に応答します。

クラスマップまたはポリシーマップの最後のエントリは、指定されていないネットワークでのすべての ICMP ping および ARP 要求を特定する必要があります。これらのカウンタが増えることは、ICMP と ARP の既存の ACL で指定されていない新しいネットワークが追加されたことを意味します。この場合は、ICMP と ARP に関連する ACL を更新する必要があります。

（注） デフォルト CoPP ごとに、ICMP ping は copp-system-p-class-monitoring に、ARP 要求は copp-system-p-class-normal に分類します。

次に、ICMP と ARP 要求を分割して、CoPP のオーバーフローを回避する例を示します。

最初に、アプリケーションの調査の結果に基づいてグループ化するネットワークを識別する新しい ACL を追加します。

```
arp access-list copp-arp-1
statistics per-entry
10 permit ip 10.1.1.0 255.255.255.0 mac any
20 permit ip 10.1.2.0 255.255.255.0 mac any
30 permit ip 10.1.3.0 255.255.255.0 mac any
arp access-list copp-arp-2
statistics per-entry
10 permit ip 10.2.1.0 255.255.255.0 mac any
20 permit ip 10.2.2.0 255.255.255.0 mac any
30 permit ip 10.2.3.0 255.255.255.0 mac any
arp access-list copp-arp-3
statistics per-entry
10 permit ip 10.3.1.0 255.255.255.0 mac any
20 permit ip 10.3.2.0 255.255.255.0 mac any
30 permit ip 10.3.3.0 255.255.255.0 mac any
...
arp access-list copp-arp-10
10 permit ip any any mac any

ip access-list copp-icmp-1
statistics per-entry
10 permit icmp 10.2.1.0 255.255.255.0 any
20 permit icmp 10.2.2.0 255.255.255.0 any
30 permit icmp 10.2.3.0 255.255.255.0 any
ip access-list copp-icmp-2
statistics per-entry
10 permit icmp 10.3.1.0 255.255.255.0 any
10 permit icmp 10.3.2.0 255.255.255.0 any
10 permit icmp 10.3.3.0 255.255.255.0 any
ip access-list copp-icmp-3
statistics per-entry
10 permit icmp 10.4.1.0 255.255.255.0 any
10 permit icmp 10.4.2.0 255.255.255.0 any
10 permit icmp 10.4.3.0 255.255.255.0 any
...
ip access-list copp-icmp-10
10 permit icmp any any
```

CoPP の新しいクラス マップにこれらの ACL を追加します。

```
class-map type control-plane match-any copp-cm-arp-1
 match access-group name copp-arp-1
class-map type control-plane match-any copp-cm-arp-2
 match access-group name copp-arp-2
class-map type control-plane match-any copp-cm-arp-3
 match access-group name copp-arp-3
...
class-map type control-plane match-any copp-cm-arp-10
 match access-group name copp-arp-10# class-map type control-plane match-any copp-cm-icmp-1

 match access-group name copp-icmp-1
class-map type control-plane match-any copp-cm-icmp-2
 match access-group name copp-icmp-2
class-map type control-plane match-any copp-cm-icmp-3
 match access-group name copp-icmp-3
...
class-map type control-plane match-any copp-cm-icmp-10
 match access-group name copp-icmp-10
```

新しいポリシーと先に作成したクラス マップを追加して、CoPP ポリシー マップを変更します。

```
policy-map type control-plane copp-system-p-policy
class copp-cm-icmp-1
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-icmp-2
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-icmp-3
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-icmp-4
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-icmp-10
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-arp-1
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-arp-2
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-arp-3
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-arp-4
      police cir X kbps bc X ms conform transmit violate drop
class copp-cm-arp-10
      police cir X kbps bc X ms conform transmit violate drop
```

既存のクラス マップから ICMP と ARP を削除します。

```
class-map type control-plane match-any copp-system-p-class-normal
no match protocol arp

class-map type control-plane match-any copp-system-p-class-monitoring
no match access-grp name copp-system-p-acl-icmp
```

セットアップ ユーティリティによるデフォルト CoPP ポリシーの変更または再適用

セットアップ ユーティリティを使用して CoPP のデフォルト ポリシーを再適用する例を次に示します。

（注） Cisco NX-OS Release 5.2 以降では、**copp profile** コマンドを使用して、デフォルト CoPP ポリシーを変更または再適用できます。

```
switch# setup

         ---- Basic System Configuration Dialog VDC: 1 ----

This setup utility will guide you through the basic configuration of
the system. Setup configures only enough connectivity for management
of the system.


*Note: setup is mainly used for configuring the system initially,
when no configuration is present. So setup always assumes system
defaults and not the current system configuration values.


Press Enter at anytime to skip a dialog. Use ctrl-c at anytime
to skip the remaining dialogs.

Would you like to enter the basic configuration dialog (yes/no): yes
```

```
Do you want to enforce secure password standard (yes/no)[y]: <CR>

  Create another login account (yes/no) [n]: n

  Configure read-only SNMP community string (yes/no) [n]: n

  Configure read-write SNMP community string (yes/no) [n]: n

  Enter the switch name : <CR>

  Enable license grace period? (yes/no) [n]: n

  Continue with Out-of-band (mgmt0) management configuration? (yes/no) [y]: n

  Configure the default gateway? (yes/no) [y]: n

  Configure advanced IP options? (yes/no) [n]: <CR>

  Enable the telnet service? (yes/no) [n]: y

  Enable the ssh service? (yes/no) [y]: <CR>

    Type of ssh key you would like to generate (dsa/rsa) : <CR>

  Configure the ntp server? (yes/no) [n]: n

  Configure default interface layer (L3/L2) [L3]: <CR>

  Configure default switchport interface state (shut/noshut) [shut]: <CR>

  Configure best practices CoPP profile (strict/moderate/lenient/dense/skip) [strict]:
strict

  Configure CMP processor on current sup (slot 6)? (yes/no) [y]: n

  Configure CMP processor on redundant sup (slot 5)? (yes/no) [y]: n

The following configuration will be applied:
  password strength-check
  no license grace-period
  no telnet server enable
  no system default switchport
  system default switchport shutdown
  policy-map type control-plane copp-system-p-policy

Would you like to edit the configuration? (yes/no) [n]: <CR>

Use this configuration and save it? (yes/no) [y]: y

switch#
```

CoPP に関する追加情報

ここでは、CoPP の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
ライセンス	『*Cisco NX-OS Licensing Guide*』
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』

標準

標準	タイトル
RFC 2698	『A Two Rate Three Color Marker』

CoPP の機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 *56* : *CoPP* の機能の履歴

機能名	リリース	機能情報
CoPP	6.2(2)	各モジュールの各ポリシーに関する5分間移動平均と一致および違反したバイトカウントのピーク値を表示するための **show policy-map interface control-plane** コマンドの出力が更新されました。
CoPP	6.2(2)	VRRP IPv6 トラフィックをポリシングするための VRRP6 ACL サポートが追加されました。HSRP ACL は制御パケットの正しい宛先アドレスを反映するよう変更されます。
CoPP	6.2(2)	マルチキャスト トラフィックの動作が、異なるクラスにおいて異なるレートでポリシングされることから、3つのクラス（マルチキャスト ホスト、マルチキャスト ルータ、標準）にグループ化され、一定のレートでポリシングされるように変更されました。

機能名	リリース	機能情報
CoPP	6.2(2)	SNMP で CoPP をモニタする機能が追加されました。
CoPP	6.1(1)	FCoE に対する新しいクラスが追加されました。LISP、LISP6 および MAC レイヤ 3 IS-IS ACL が重要なクラスに追加されました。fcoe-fib-miss 一致例外が好ましくないクラスに追加されました。MAC レイヤ 2 トンネル ACL がレイヤ 2 非ポリシー クラスに追加されました。「permit icmp any any 143」ルールが acl-icmp6-msgs ACL に追加されました。
CoPP	6.0(1)	デンス デフォルト CoPP ポリシーが追加されました。
CoPP	6.0(1)	ラインカードごとに CoPP のスケール ファクタを設定する機能が追加されました。
CoPP	5.2(1)	設定ユーティリティを再度実行しないでデフォルト CoPP ポリシーを変更または再適用する機能が追加されました。
CoPP	5.2(1)	CoPP ベスト プラクティス ポリシーを読み取り専用に変更し、ポリシーを修正するためにコピーする機能が追加されました。

機能名	リリース	機能情報
CoPP	5.2(1)	CoPP ベスト プラクティス ポリシーの詳細を表示する **show copp profile** コマンドと、ポリシー間の違いを表示する **show copp diff profile** コマンドが追加されました。
CoPP	5.2(1)	実行コンフィギュレーションとスタートアップ コンフィギュレーションでユーザ設定 ACL だけを表示する（およびデフォルトの CoPP 設定 ACL を表示しない）ように、**show running-config aclmgr** コマンドと **show startup-config aclmgr** コマンドが変更されました。
CoPP	5.2(1)	**show copp status** コマンドが変更され、CoPP ベスト プラクティス ポリシーのどの部分がコントロール プレーンにアタッチされているかを表示するようになりました。
CoPP	5.2(1)	セットアップ ユーティリティで、ベスト プラクティス CoPP プロファイルの **none** オプションの名前が **skip** に変更されました。
CoPP	5.2(1)	デフォルトのクラス マップが更新され、MPLS LDP、MPLS OAM、MPLS RSVP、DHCP リレー、および OTV-AS のサポートが含まれました。

機能名	リリース	機能情報
コントロール プレーン ポリシー マップ	5.1(1)	ドロップされるパケットのしきい値を指定し、設定したしきい値をドロップ数が超えた場合に syslog を生成する機能が追加されました。
CoPP	5.1(1)	デフォルトのポリシーが更新され、802.1Q サービス クラス（cos）の値が含まれました。
CoPP	5.1(1)	非 IP トラフィック クラスのサポートが追加されました。
CoPP	5.0(2)	デフォルトのポリシーが更新され、ACL HSRP6 のサポートが含まれました。
CoPP	4.2(3)	デフォルトのポリシーが更新され、ACL DHCP のサポートが含まれました。
CoPP	4.2(1)	デフォルトのポリシーが更新され、WCCP および Cisco TrustSec のサポートが含まれました。

第 27 章

レート制限の設定

この章では、Cisco NX-OS デバイスでスーパーバイザ宛のトラフィックのレート制限を設定する手順について説明します。

この章は、次の項で構成されています。

- 機能情報の確認，867 ページ
- レート制限の概要，868 ページ
- レート制限のバーチャライゼーション サポート，869 ページ
- レート制限のライセンス要件，869 ページ
- レート制限の注意事項と制約事項，869 ページ
- レート制限のデフォルト設定，870 ページ
- レート制限の設定，871 ページ
- スーパーバイザに到達するパケットのレート制限の設定，876 ページ
- レート制限のモニタリング，877 ページ
- レート制限統計情報のクリア，877 ページ
- レート制限の設定の確認，878 ページ
- レート制限の設定例，879 ページ
- レート制限に関する追加情報，879 ページ
- レート制限の機能の履歴，879 ページ

機能情報の確認

ご使用のソフトウェア リリースで、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、https://tools.cisco.com/bugsearch/ の Bug Search Tool およびご使用のソフトウェア リリースのリリース ノートを参照してください。こ

のモジュールに記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「新機能および変更された機能に関する情報」の章または以下の「機能の履歴」表を参照してください。

レート制限の概要

レート制限を行うことにより、例外のためにリダイレクトされたパケットによって Cisco NX-OS デバイス上のスーパーバイザ モジュールに過剰な負荷がかかるのを回避できます。次のタイプのリダイレクト パケットに対して pps（パケット/秒）単位でレート制限を設定できます。

- アクセス リスト ログ パケット
- スーパーバイザ モジュールにコピーされるデータ パケットおよび制御パケット
- F1 シリーズ モジュール パケット
  - rl-1 STP および Fabricpath-ISIS
  - rl-2 L3-ISIS および OTV-ISIS
  - rl-3 UDLD、LACP、CDP、および LLDP
  - rl-4 Q-in-Q および ARP 要求
  - rl-5 IGMP、NTP、DHCP スヌープ、ポート セキュリティ、および Mgmt トラフィック
- レイヤ 2 トンネリング プロトコル（L2TP）パケット
- レイヤ 2 マルチキャストスヌーピング パケット
- レイヤ 2 ポート セキュリティ パケット
- レイヤ 2 ストーム制御パケット
- レイヤ 2 仮想ポート チャネル（vPC）低パケット
- レイヤ 3 制御パケット
- レイヤ 3 収集パケット
- レイヤ 3 収集高速パス パケット
- レイヤ 3 最大伝送単位（MTU）チェック エラー パケット
- レイヤ 3 マルチキャスト データ パケット
- レイヤ 3 存続可能時間（TTL）チェック エラー パケット
- 受信パケット

Cisco NX-OS Release 5.1 から、スーパーバイザ モジュールに到達するパケットのレート制限も設定できます。

レート制限のバーチャライゼーション サポート

レート制限はデフォルト仮想デバイス コンテキスト（VDC）だけで設定できますが、そのレート制限の設定はCisco NX-OSデバイス上のすべてのVDCに適用されます。VDCの詳細については、『*Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide*』を参照してください。

レート制限のライセンス要件

次の表に、この機能のライセンス要件を示します。

製品	ライセンス要件
Cisco NX-OS	レート制限にはライセンスは必要ありません。ライセンス パッケージに含まれていない機能はすべてCisco NX-OSシステム イメージにバンドルされており、追加費用は一切発生しません。Cisco NX-OSライセンス方式の詳細については、『*Cisco NX-OS Licensing Guide*』を参照してください。

レート制限の注意事項と制約事項

レート制限機能には、次の設定に関する注意事項と制限事項があります。

- スーパーバイザ宛の例外トラフィックおよびリダイレクトされたトラフィックに対してレート制限を設定できます。スーパーバイザ宛の他のタイプのトラフィックには、コントロール プレーン ポリシング（CoPP）を使用します。

（注） ハードウェア レート制限は、スーパーバイザのCPUを過剰な入力トラフィックから保護します。ハードウェア レート制限によって許容されるトラフィック レートは、グローバルに設定され、個々のI/Oモジュールのそれぞれに適用されます。結果的に許容されるレートは、システム内のI/Oモジュールの数によって異なります。CoPPでは、Modular Quality-of-Service CLI（MQC）を利用して、スーパーバイザのCPUをさらに細かく保護することができます。

- F1シリーズ モジュールはスーパーバイザ モジュールに送信されるすべての制御トラフィックで共有される最大5個のレート リミッタをサポートします。

（注） F2 シリーズ モジュールでは、F1 シリーズ モジュールの 5 個のレート リミッタはサポートされません。

- F2、M1 および M2 シリーズ モジュールでは、IP リダイレクトは設定されたレイヤ 3 存続可能時間（TTL）のレート制限に従ってレート限定されます。

（注） Cisco IOS の CLI に慣れている場合、この機能に対応する Cisco NX-OS コマンドは通常使用する Cisco IOS コマンドと異なる場合があるので注意してください。

複数のモジュールにハードウェア レート リミッタを設定すると、モジュール レベルのレート リミッタがシステム レベルよりも優先されます。

関連トピック

コントロール プレーン ポリシングの設定, （819 ページ）

レート制限のデフォルト設定

次の表に、レート制限パラメータのデフォルト設定を示します。

表 *57*：レート制限パラメータのデフォルト設定

パラメータ	デフォルト
アクセス リスト ロギング パケットのレート制限	100 pps
コピー パケットのレート制限	30,000 pps
F1 シリーズ モジュールのレート制限	RL-1：4,500 pps RL-2：1,000 pps RL-3：1,000 pps RL-4：100 pps RL-5：1,500 pps （注） これらの F1 シリーズ モジュールのレート制限は、F2 シリーズ モジュールには適用されません。
レイヤ 2 L2TP パケットのレート制限	4,096 pps

パラメータ	デフォルト
レイヤ2マルチキャストスヌーピングパケットのレート制限	10,000 pps
レイヤ 2 ポート セキュリティ パケットのレート制限	ディセーブル
レイヤ 2 ストーム制御パケットのレート制限	ディセーブル
レイヤ 2 VPC 低パケットのレート制限	4,000 pps
レイヤ 3 制御パケットのレート制限	10,000 pps
レイヤ 3 収集パケットのレート制限	100 pps
レイヤ 3 収集高速パスのレート制限	100 pps
レイヤ 3 MTU パケットのレート制限	500 pps
レイヤ 3 存続可能時間（TTL）パケットのレート制限	500 pps
受信パケットのレート制限	30,000 pps
スーパーバイザ パケットのレート制限	10,000 pps

レート制限の設定

スーパーバイザ宛トラフィックにレート制限を設定できます。

手順の概要

1. **configure terminal**
2. **hardware rate-limiter access-list-log** {*packets* | **disable**} [**module***module* [**port***startend*]]
3. **hardware rate-limiter copy** {*packets* | **disable**} [**module***module* [**port***startend*]]
4. **hardware rate-limiter f1** {**rl-1** | **rl-2** | **rl-3** | **rl-4** | **rl-5** {*packets* | **disable**}} [**module***module* [**port***startend*]]
5. **hardware rate-limiter layer-2 l2pt** {*packets* | **disable**} [**module***module* [**port***startend*]]
6. **hardware rate-limiter layer-2 mcast-snooping** {*packets* | **disable**} [**module***module* [**port***startend*]]
7. **hardware rate-limiter layer-2 port-security** {*packets* | **disable**} [**module***module* [**port***startend*]]
8. **hardware rate-limiter layer-2 storm-control** {*packets* | **disable**} [**module***module* [**port***startend*]]
9. **hardware rate-limiter layer-2 vpc-low** {*packets* | **disable**} [**module***module* [**port***startend*]]
10. **hardware rate-limiter layer-3 control** {*packets* | **disable**} [**module***module* [**port***startend*]]
11. **hardware rate-limiter layer-3 glean** {*packets* | **disable**} [**module***module* [**port***startend*]]
12. **hardware rate-limiter layer-3 glean-fast** {*packets* | **disable**} [**module***module* [**port***startend*]]
13. **hardware rate-limiter layer-3 mtu** {*packets* | **disable**} [**module***module* [**port***startend*]]
14. **hardware rate-limiter layer-3 multicast** {*packets* | **disable**} [**module***module* [**port***startend*]]
15. **hardware rate-limiter layer-3 ttl** {*packets* | **disable**} [**module***module* [**port***startend*]]
16. **hardware rate-limiter receive** {*packets* | **disable**} [**module***module* [**port***startend*]]
17. **exit**
18. （任意） **show hardware rate-limiter** [**access-list-log** | **copy** | **f1** {**rl-1** | **rl-2** | **rl-3** | **rl-4** | **rl-5**} |**layer-2** {**l2pt** |**mcast-snooping** | **port-security** | **storm-control** | **vpc-low**} | **layer-3** {**control** | **glean** | **glean-fast** |**mtu** | **multicast** | **ttl**} | **module***module* | **receive**]
19. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**hardware rate-limiter access-list-log** {*packets*	**disable**} [**module***module* [**port***startend*]] 例： `switch(config)# hardware rate-limiter access-list-log 200`	アクセス リスト ロギングのためにスーパーバイザ モジュールにコピーされるパケットのレート制限を pps で設定します。範囲は 0 ～ 30000 です。

	コマンドまたはアクション	目的
ステップ 3	**hardware rate-limiter copy**{*packets* | **disable**} [**module***module* [**port***startend*]] 例： `switch(config)# hardware rate-limiter copy 30000`	スーパーバイザ モジュールにコピーされるデータ パケットおよび制御パケットのレート制限を pps で設定します。範囲は 0 ～ 30000 です。 （注） レイヤ 3 制御、マルチキャスト直接接続、およびARP 要求のパケットは、レイヤ 2 コピー レート リミッタによって制御されます。最初の 2 つのタイプのパケットはレイヤ 3 レート リミッタによっても制御され、最後の 2 つのタイプはコントロール プレーン ポリシング（CoPP）によっても制御されます。
ステップ 4	**hardware rate-limiter f1** {**rl-1** | **rl-2** | **rl-3** | **rl-4** | **rl-5** {*packets* | **disable**}} [**module***module* [**port***startend*]] 例： `switch(config)# hardware rate-limiter f1 rl-1 1000`	F1 シリーズ モジュール パケットのレート制限を pps で設定します。範囲は 0 ～ 30000 です。 （注） **f1** {**rl-1** | **rl-2** | **rl-3** | **rl-4** | **rl-5**} レート リミッタのみが F1 シリーズ モジュールでサポートされます。他のレート リミッタは、F2 シリーズおよびM1 シリーズ モジュールにだけ適用できます。
ステップ 5	**hardware rate-limiter layer-2 l2pt**{*packets* | **disable**} [**module***module* [**port***startend*]] 例： `switch(config)# hardware rate-limiter layer-2 l2pt 30000`	レイヤ 2 トンネル プロトコル パケットのレート制限を pps で設定します。範囲は 0 ～ 30000 です。
ステップ 6	**hardware rate-limiter layer-2 mcast-snooping**{*packets* | **disable**} [**module***module* [**port***startend*]] 例： `switch(config)# hardware rate-limiter layer-2 mcast-snooping 20000`	レイヤ 2 マルチキャスト スヌーピング パケットのレート制限を pps で設定します。範囲は 0 ～ 30000 です。
ステップ 7	**hardware rate-limiter layer-2 port-security**{*packets* | **disable**} [**module***module* [**port***startend*]] 例： `switch(config)# hardware rate-limiter layer-2 port-security 100000`	ポート セキュリティ パケットのレート制限を pps で設定します。範囲は 0 ～ 30000 です。

	コマンドまたはアクション	目的
ステップ 8	**hardware rate-limiter layer-2 storm-control**{*packets* | **disable**} [**module***module* [**port***startend*]] 例： `switch(config)# hardware rate-limiter layer-2 storm-control 10000`	ブロードキャスト、マルチキャスト、および不明なユニキャスト ストーム制御のトラフィックのレート制限を pps で設定します。範囲は 0 ～ 30000 です。
ステップ 9	**hardware rate-limiter layer-2 vpc-low**{*packets* | **disable**} [**module***module* [**port***startend*]] 例： `switch(config)# hardware rate-limiter layer-2 vpc-low 10000`	VPC low キュー上でのレイヤ 2 制御パケットのレート制限を pps で設定します。範囲は 0 ～ 30000 です。
ステップ 10	**hardware rate-limiter layer-3 control**{*packets* | **disable**} [**module***module* [**port***startend*]] 例： `switch(config)# hardware rate-limiter layer-3 control 20000`	レイヤ 3 制御パケットのレート制限を pps で設定します。範囲は 0 ～ 30000 です。
ステップ 11	**hardware rate-limiter layer-3 glean**{*packets* | **disable**} [**module***module* [**port***startend*]] 例： `switch(config)# hardware rate-limiter layer-3 glean 200`	レイヤ 3 収集パケットのレート制限を pps で設定します。範囲は 0 ～ 30000 です。
ステップ 12	**hardware rate-limiter layer-3 glean-fast**{*packets* | **disable**} [**module***module* [**port***startend*]] 例： `switch(config)# hardware rate-limiter layer-3 glean-fast 500`	レイヤ 3 収集高速パス パケットのレート制限を pps で設定します。このコマンドは、F2e、M1、または M2 シリーズ モジュールからスーパーバイザにパケットを送信します。範囲は 0 ～ 30000 です。 収集高速パスは、スーパーバイザによる収集パケットの処理を最適化します。具体的には、ライン カードによりパケット内の ARP をトリガーするために必要な情報が提供され、スーパーバイザがこの情報を調べる手間が省けます。収集高速パスを使用してスーパーバイザに送信されたパケットはレート制限されます。 （注） 収集高速パスはデフォルトでイネーブルになっています。収集高速パスのプログラミングが隣接のリソース枯渇が原因で発生しない場合は、システムが通常の収集プログラミングに戻ります。

	コマンドまたはアクション	目的
ステップ 13	**hardware rate-limiter layer-3 mtu**{*packets* | **disable**} [**module***module* [**port***startend*]] 例： `switch(config)# hardware rate-limiter layer-3 mtu 1000`	レイヤ 3 MTU エラー リダイレクト パケットのレート制限を pps で設定します。範囲は 0 ～ 30000 です。
ステップ 14	**hardware rate-limiter layer-3 multicast**{*packets* | **disable**} [**module***module* [**port***startend*]] 例： `switch(config)# hardware rate-limiter layer-3 multicast 20000`	レイヤ 3 マルチキャスト パケットのレート制限を pps で設定します。範囲は 0 ～ 30000 です。
ステップ 15	**hardware rate-limiter layer-3 ttl**{*packets* | **disable**} [**module***module* [**port***startend*]] 例： `switch(config)# hardware rate-limiter layer-3 ttl 1000`	レイヤ 3 TTL エラー リダイレクト パケットのレート制限を pps で設定します。範囲は 0 ～ 30000 です。
ステップ 16	**hardware rate-limiter receive**{*packets* | **disable**} [**module***module* [**port***startend*]] 例： `switch(config)# hardware rate-limiter receive 40000`	スーパーバイザモジュールにリダイレクトされるパケットのレート制限を pps で設定します。範囲は 0 ～ 30000 です。

ステップ 17	**exit**
	
	例：
	`switch(config)# exit`
	`switch#`
		グローバル コンフィギュレーション モードを終了します。

ステップ 18	**show hardware rate-limiter** [**access-list-log** | **copy** | **f1** {**rl-1** | **rl-2** | **rl-3** | **rl-4** | **rl-5**} |**layer-2** {**l2pt** |**mcast-snooping** | **port-security** | **storm-control** | **vpc-low**} | **layer-3** {**control** | **glean** | **glean-fast** |**mtu** | **multicast** | **ttl**} | **module***module* | **receive**] 例： `switch# show hardware rate-limiter`	（任意） レート制限の設定を表示します。
ステップ 19	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

スーパーバイザに到達するパケットのレート制限の設定

Cisco NX-OS Release 5.1 以降では、スーパーバイザ モジュールに到達するパケットのレート制限をデバイスでグローバルに設定できます。着信または発信パケットのレートが設定済みレート制限を超過した場合、デバイスはシステム メッセージを記録しますが、パケットをドロップしません。

（注） 特定のインターフェイスのスーパーバイザ モジュールに到達するパケットのレート制限も設定できます。詳細については、『*Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide*』を参照してください。

手順の概要

1. **configure terminal**
2. **[no] rate-limit cpu direction {input | output | both} pps** *packets***action log**
3. （任意） **exit**
4. （任意） **show system internal pktmgr internal control sw-rate-limit**
5. （任意） **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	
	例：
	`switch# configure terminal`
	`switch(config)#`
		グローバル コンフィギュレーション モードを開始します。

ステップ 2	**[no] rate-limit cpu direction {input | output | both} pps** *packets***action log** 例： `switch(config)# rate-limit cpu direction both pps 100 action log`	スーパーバイザ モジュールに到達するパケットのレート制限を pps で設定し、着信パケットまたは発信パケットのレートがレート制限を超えた場合、システム メッセージを記録します。範囲は 1 ～ 100000 です。デフォルト レートは 10000 です。
ステップ 3	**exit** 例： `switch(config)# exit`	（任意） グローバル コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 4	**show system internal pktmgr internal control sw-rate-limit** 例： `switch# show system internal pktmgr internal control sw-rate-limit`	（任意） スーパーバイザモジュールに到達するパケットのインバンドおよびアウトバンドのグローバル レート制限の設定を表示します。
ステップ 5	**copy running-config startup-config** 例： `switch# copy running-config startup-config`	（任意） 実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

レート制限のモニタリング

レート制限をモニタリングできます。

手順の概要

1. **show hardware rate-limiter** [**access-list-log** | **copy** | **f1** {**rl-1** | **rl-2** | **rl-3** | **rl-4** | **rl-5**} | **layer-2** {**l2pt** | **mcast-snooping** | **port-security** | **storm-control** | **vpc-low**} | **layer-3** {**control** | **glean** | **glean-fast** | **mtu** | **multicast** | **ttl**} | **module** *module* | **receive**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show hardware rate-limiter** [**access-list-log**	**copy**	**f1** {**rl-1**	**rl-2**	**rl-3**	**rl-4**	**rl-5**}	**layer-2** {**l2pt**	**mcast-snooping**	**port-security**	**storm-control**	**vpc-low**}	**layer-3** {**control**	**glean**	**glean-fast**	**mtu**	**multicast**	**ttl**}	**module** *module*	**receive**] 例： `switch# show hardware rate-limiter layer-3 glean`	レート制限統計情報を表示します。

レート制限統計情報のクリア

レート制限統計情報をクリアできます。

手順の概要

1. **clear hardware rate-limiter** {**all** | **access-list-log** | **copy** | **f1** {**rl-1** | **rl-2** | **rl-3** | **rl-4** | **rl-5**} | **layer-2** {**l2pt** | **mcast-snooping** | **port-security** | **storm-control** | **vpc-low**} | **layer-3** {**control** | **glean** | **glean-fast** | **mtu** | **multicast** | **ttl**} | **receive**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**clear hardware rate-limiter** {**all**	**access-list-log**	**copy**	**f1** {**rl-1**	**rl-2**	**rl-3**	**rl-4**	**rl-5**}	**layer-2** {**l2pt**	**mcast-snooping**	**port-security**	**storm-control**	**vpc-low**}	**layer-3** {**control**	**glean**	**glean-fast**	**mtu**	**multicast**	**ttl**}	**receive**} 例： `switch# clear hardware rate-limiter`	レート制限統計情報をクリアします。

レート制限の設定の確認

レート制限の設定情報を表示するには、次の作業を行います。

コマンド	目的
show hardware rate-limiter [**access-list-log**	**copy**	**f1** {**rl-1**	**rl-2**	**rl-3**	**rl-4**	**rl-5**}	**layer-2** {**l2pt**	**mcast-snooping**	**port-security**	**storm-control**	**vpc-low**}	**layer-3** {**control**	**glean**	**glean-fast**	**mtu**	**multicast**	**ttl**}	**module** *module*	**receive**]	レート制限の設定を表示します。
show system internal pktmgr interface ethernet *slot*/*port*	特定のインターフェイスのスーパーバイザ モジュールに到達するパケットのインバンドおよびアウトバンドのレート制限の設定を表示します。
show system internal pktmgr internal control sw-rate-limit	スーパーバイザ モジュールに到達するパケットのインバンドおよびアウトバンドのグローバル レート制限の設定を表示します。

これらのコマンド出力のフィールドの詳細については、『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』を参照してください。

レート制限の設定例

次に、レート制限を設定する例を示します。

```
switch(config)# hardware rate-limiter layer-3 control 20000
switch(config)# hardware rate-limiter copy 30000
```

次に、スーパーバイザ モジュールに到達するパケットのデバイスのレート制限をグローバルに設定する例を示します。

```
switch(config)# rate-limit cpu direction both pps 1000 action log
switch(config)# show system internal pktmgr internal control sw-rate-limit inband pps global threshold
 1000  outband pps global threshold 1000
```

レート制限に関する追加情報

ここでは、レート制限の実装に関する追加情報について説明します。

関連資料

関連項目	マニュアル タイトル
Cisco NX-OS ライセンス設定	『*Cisco NX-OS Licensing Guide*』
コマンド リファレンス	『*Cisco Nexus 7000 Series NX-OS Security Command Reference*』

レート制限の機能の履歴

次の表に、この機能のリリースの履歴を示します。

表 *58*：レート制限の機能の履歴

機能名	リリース	機能情報
レート制限	6.2(2)	レイヤ 3 収集高速パス パケットに対するサポートが追加されました。
レート制限	6.0(1)	F2 シリーズ モジュールのサポートが追加されました。

機能名	リリース	機能情報
レート制限	5.2(1)	Release 5.1 以降、変更はありません。
レート制限	5.1(1)	F1 シリーズ モジュール パケットのサポートが追加されました。
レート制限	5.1(1)	スーパーバイザ モジュールに到達するパケットのレート制限を設定し、レート制限を超えた場合にシステム メッセージを記録する機能が追加されました。
レート制限	5.1(1)	レート制限をディセーブルにしたり、特定のモジュールおよびポート範囲のレート制限を設定したりするためのオプションが追加されました。
レート制限	5.0(2)	レイヤ 2 トンネル プロトコル（L2TP）パケットがサポートされるようになりました。
レート制限	4.2(1)	リリース 4.1 からの変更はありません。