



## **Cisco Nexus 9000 シリーズ NX-OS セキュリティ コンフィギュレーションガイド リリース 9.3(x)**

初版：2019 年 7 月 20 日

最終更新：2021 年 4 月 28 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/>

【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/](http://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。

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

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

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.

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

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

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

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

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

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: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. 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. (1721R)

© 2019–2021 Cisco Systems, Inc. All rights reserved.



## 目次

---

はじめに :

[はじめに](#) **xxix**

[対象読者](#) **xxix**

[表記法](#) **xxix**

[Cisco Nexus 9000 シリーズ スイッチの関連資料](#) **xxx**

[マニュアルに関するフィードバック](#) **xxx**

[通信、サービス、およびその他の情報](#) **xxxi**

---

第 1 章

[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**

---

第 2 章

[概要](#) **7**

[ライセンス要件](#) **7**

[Authentication, Authorization, and Accounting \(認証、許可、およびアカウントिंग\)](#) **8**

[RADIUS および TACACS+ セキュリティ プロトコル](#) **8**

[LDAP](#) **9**

[SSH および Telnet](#) **9**

[ユーザ アカウントおよびユーザ ロール](#) **10**

[IP ACL](#) **10**

[MAC ACL](#) **10**

[VACL](#) **10**

[DHCP スヌーピング](#) **11**

[ダイナミック ARP インспекション](#) **11**

[IP ソース ガード](#) **11**

[パスワード暗号化](#) **12**

キーチェーン管理	12
コントロールプレーン ポリシング	12
レート制限	13
ソフトウェア イメージ	13
仮想デバイス コンテキスト	13

---

**第 3 章****FIPS の設定 15**

FIPS について	15
FIPS のセルフテスト	15
FIPS エラー状態	16
FIPS の前提条件	17
FIPS の注意事項と制約事項	17
FIPS のデフォルト設定	17
FIPS の設定	18
FIPS モードの有効化	18
FIPS の無効化	19
FIPS の設定の確認	20
FIPS の設定例	20
FIPS に関する追加情報	20

---

**第 4 章****AAA の設定 23**

AAA について	23
AAA セキュリティサービス	23
AAA を使用する利点	24
リモート AAA サービス	25
AAA サーバグループ	25
AAA サービス設定オプション	25
??? ??????????????????	27
AES パスワード暗号化およびプライマリ暗号キー	28
AAA の前提条件	28
AAA の注意事項と制約事項	28



AAA のデフォルト設定	29
AAA の設定	29
AAA の設定プロセス	30
コンソール ログイン認証方式の設定	30
デフォルトのログイン認証方式の設定	32
ローカル認証へのフォールバックのディセーブル化	34
AAA 認証のデフォルト ユーザ ロールのイネーブル化	36
ログイン認証失敗メッセージのイネーブル化	37
成功および失敗したログイン試行のロギング	37
CHAP 認証のイネーブル化	39
MSCHAP または MSCHAP V2 認証のイネーブル化	41
デフォルトの AAA アカウンティング方式の設定	43
Cisco NX-OS デバイスによる AAA サーバの VSA の使用	45
VSA の概要	45
VSA の形式	45
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	46
セキュア ログイン機能の設定	46
ログイン パラメータの設定	46
ユーザ ログインセッションの制限	48
パスワードの長さの制限	49
ユーザ名のパスワードプロンプトのイネーブル化	49
RADIUS または TACACS+ の共有秘密の設定	50
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	51
AAA 設定の確認	52
AAA の設定例	53
ログイン パラメータの設定例	53
パスワードプロンプト機能の設定例	54
AAA に関する追加情報	55
第 5 章	<b>RADIUS の設定</b> 57
	RADIUS について 57

RADIUS ネットワーク環境	58
RADIUS の動作	58
RADIUS ?????????? ?	59
ベンダー固有属性	59
RADIUS 認可変更について	61
セッション再認証	61
セッションの終了	62
RADIUS の前提条件	62
RADIUS の注意事項と制約事項	62
RADIUS の認可変更の注意事項と制約事項	63
RADIUS のデフォルト設定	63
RADIUS サーバの設定	63
RADIUS サーバの設定プロセス	64
RADIUS サーバホストの設定	64
グローバル RADIUS キーの設定	66
特定の RADIUS サーバ用のキーの設定	67
RADIUS サーバグループの設定	69
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	71
ログイン時にユーザによる RADIUS サーバの指定を許可	71
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	73
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	74
RADIUS サーバのアカウントिंगおよび認証属性の設定	75
RADIUS サーバのグローバルな定期モニタリングの設定	77
各 RADIUS サーバの定期モニタリングの設定	79
RADIUS デッドタイム間隔の設定	80
ワンタイムパスワードの設定	81
RADIUS サーバまたはサーバグループの手動モニタリング	82
Dynamic Author Server の有効化または無効化	83
RADIUS 認可変更の設定	83
RADIUS 設定の確認	84
RADIUS 認可変更の設定の検証	84

RADIUS サーバのモニタリング	85
RADIUS サーバ統計情報のクリア	86
RADIUS の設定例	86
RADIUS 認可変更の設定例	86
次の作業	87
RADIUS に関する追加情報	87

---

**第 6 章**

<b>TACACS+ の設定</b>	<b>89</b>
TACACS+ について	89
TACACS+ の利点	90
ユーザ ログインにおける TACACS+ の動作	90
デフォルトの TACACS+ サーバ暗号化タイプおよび秘密キー	91
TACACS+ サーバのコマンド許可サポート	91
TACACS+ ??????????	91
TACACS+ のベンダー固有属性	92
TACACS+ 用の Cisco VSA 形式	92
TACACS+ の前提条件	93
TACACS+ の注意事項と制約事項	93
TACACS+ のデフォルト設定	94
ワンタイム パスワード サポート	94
TACACS+ の設定	95
TACACS+ サーバの設定プロセス	95
TACACS+ のイネーブル化	95
TACACS+ サーバ ホストの設定	96
グローバル TACACS+ キーの設定	98
特定の TACACS+ サーバ用のキーの設定	99
TACACS+ サーバ グループの設定	100
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	102
ユーザによるログイン時の TACACS+ サーバ指定の許可	103
TACACS+ サーバのタイムアウト間隔の設定	104
TCP ポートの設定	105

TACACS+ サーバのグローバルな定期モニタリングの設定	106
各 TACACS+ サーバの定期モニタリングの設定	108
TACACS+ デッドタイム間隔の設定	110
ASCII 認証の設定	111
TACACS+ サーバでの AAA 許可の設定	112
TACACS+ サーバでのコマンド許可の設定	113
TACACS+ サーバでのコマンド許可のテスト	116
コマンド許可検証のイネーブル化とディセーブル化	116
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	117
権限ロールのユーザ コマンドの許可または拒否	120
TACACS+ サーバまたはサーバグループの手動モニタリング	121
TACACS+ のディセーブル化	122
TACACS+ サーバのモニタリング	122
TACACS+ サーバ統計情報のクリア	123
TACACS+ の設定の確認	124
TACACS+ の設定例	124
次の作業	126
TACACS+ に関する追加情報	126

## 第 7 章

**LDAP の設定 129**

LDAP について	129
LDAP 認証および許可	130
ユーザ ログインにおける LDAP の動作	130
LDAP ??????????	131
LDAP のベンダー固有属性	132
LDAP 用の Cisco VSA 形式	132
LDAP のバーチャライゼーションサポート	132
LDAP の前提条件	132
LDAP の注意事項と制約事項	132
LDAP のデフォルト設定	133
LDAP の設定	133

LDAP サーバの設定プロセス	133
LDAP のイネーブル化/ディセーブル化	134
LDAP サーバ ホストの設定	135
LDAP サーバの rootDN の設定	136
LDAP サーバ グループの設定	137
グローバルな LDAP タイムアウト間隔の設定	139
LDAP サーバのタイムアウト間隔の設定	140
TCP ポートの設定	141
LDAP 検索マップの設定	142
LDAP サーバの定期的モニタリングの設定	143
LDAP デッドタイム間隔の設定	145
LDAP サーバでの AAA 許可の設定	145
LDAP サーバのモニタリング	147
LDAP サーバ統計情報のクリア	147
LDAP 設定の確認	148
LDAP の設定例	148
次の作業	149
LDAP に関する追加情報	149

---

**第 8 章**

<b>SSH および Telnet の設定</b>	<b>151</b>
SSH および Telnet について	151
SSH サーバ	151
SSH クライアント	152
SSH サーバ キー	152
デジタル証明書を使用した SSH 認証	153
Telnet サーバ	153
SSH および Telnet の前提条件	153
SSH と Telnet の注意事項と制約事項	153
SSH および Telnet のデフォルト設定	154
SSH の設定	155
SSH サーバ キーの生成	155

ユーザアカウント用 SSH 公開キーの指定	156
IETF SECSH 形式による SSH 公開キーの指定	156
OpenSSH 形式の SSH 公開キーの指定	157
SSH ログイン試行の最大回数の設定	158
SSH セッションの開始	159
ブートモードからの SSH セッションの開始	160
SSH のパスワードが不要なファイルコピーの設定	161
SCP サーバと SFTP サーバの設定	163
X.509v3 証明書ベースの SSH 認証の設定	164
レガシー SSH アルゴリズム サポートの設定	167
サポートされるアルゴリズム : FIPモードが有効の場合	169
デフォルトの SSH サーバポートの変更	169
SSH ホストのクリア	172
SSH サーバのディセーブル化	172
SSH サーバキーの削除	173
SSH セッションのクリア	174
Telnet の設定	174
Telnet サーバのイネーブル化	174
リモートデバイスとの Telnet セッションの開始	175
Telnet セッションのクリア	175
SSH および Telnet の設定の確認	176
SSH の設定例	177
SSH のパスワードが不要なファイルコピーの設定例	178
X.509v3 証明書ベースの SSH 認証の設定例	180
SSH および Telnet に関する追加情報	180

## 第 9 章

**PKI の設定** 183

PKI の概要	183
CA とデジタル証明書	183
信頼モデル、トラストポイント、アイデンティティ CA	184
RSA のキーペアとアイデンティティ証明書	184

複数の信頼できる CA のサポート	186
PKI の登録のサポート	186
カットアンドペーストによる手動での登録	186
複数の RSA キー ペアとアイデンティティ CA のサポート	187
ピア証明書の検証	187
証明書の取消確認	187
CRL のサポート	187
NDcPP : syslog の OCSP	188
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	188
PKI の注意事項と制約事項	188
PKI のデフォルト設定	189
CA の設定とデジタル証明書	189
ホスト名と IP ドメイン名の設定	189
RSA キー ペアの生成	190
トラストポイント CA のアソシエーションの作成	192
CA の認証	193
証明書取消確認方法の設定	195
証明書要求の作成	196
アイデンティティ証明書のインストール	198
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	199
PKCS 12 形式でのアイデンティティ情報のエクスポート	200
PKCS 12 形式でのアイデンティティ情報のインポート	201
CRL の設定	202
CA の設定からの証明書の削除	203
Cisco NX-OS デバイスからの RSA キー ペアの削除	205
PKI の設定の確認	205
PKI の設定例	206
Cisco NX-OS デバイスでの証明書の設定	206
CA ??????????	209
???????????????	215
?????????	229

CRL ??????	232
CRL ??????	234
CRL のインポート	239
PKI に関する追加情報	242
PKI の関連資料	242
PKI の標準規格	242

---

**第 10 章**

<b>ユーザ アカウントおよび RBAC の設定</b>	<b>243</b>
ユーザ アカウントと RBAC について	243
ユーザ アカウント	243
強力なパスワードの特性	244
ユーザ ロール	245
ユーザ ロールのルール	246
ユーザ アカウントおよび RBAC の注意事項と制約事項	246
ユーザ アカウントおよび RBAC のデフォルト設定	247
パスワードの強度確認のイネーブル化	248
ユーザ アカウントの設定	249
??????	251
ユーザ ロールおよびルールの作成	251
機能グループの作成	254
ユーザ ロール インターフェイス ポリシーの変更	255
ユーザ ロール VLAN ポリシーの変更	257
ユーザ ロールの VRF ポリシーの変更	258
No Service Password-Recovery について	259
No Service Password-Recovery のイネーブル化	260
ユーザ アカウントおよび RBAC 設定の確認	261
ユーザ アカウントおよび RBAC の設定例	262
ユーザ アカウントおよび RBAC に関する追加情報	264

---

**第 11 章**

<b>802.1X の設定</b>	<b>265</b>
802.1X について	265



?????????	265
????????????????	266
インターフェイスのオーセンティケータ PAE ステータス	267
許可ステートおよび無許可ステートのポート	268
MAC 認証バイパス	269
MAC ベースの認証 (MAB) に基づいたダイナミック VLAN 割り当て	270
RADIUS からの VLAN 割り当て	270
シングル ホストおよびマルチ ホストのサポート	270
サポートされるトポロジ	271
DAACL について	271
DAACL の注意事項と制約事項	271
802.1X の前提条件	272
802.1X の注意事項と制約事項	272
802.1X のデフォルト設定	274
802.1X の設定	275
802.1X の設定プロセス	275
802.1X 機能のイネーブル化	276
802.1X の AAA 認証方式の設定	276
インターフェイスでの 802.1X 認証の制御	277
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	279
インターフェイスの定期再認証のイネーブル化	280
手動によるサブリカントの再認証	281
インターフェイスの 802.1X 認証タイマーの変更	282
MAC 認証バイパスのイネーブル化	284
デフォルト dot1.x 認証方式の設定 - MAB	285
ダイナミック アクセス リストの作成	286
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	288
Cisco NX-OS デバイスでの 802.1X 認証のディセーブル化	289
802.1X 機能のディセーブル化	290
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	291
インターフェイスでのオーセンティケータとサブリカント間のフレームの最大数の設定	292

802.1X 認証の RADIUS アカウンティングのイネーブル化	293
802.1X の AAA アカウンティング方式の設定	294
インターフェイスでの再認証最大リトライ回数の設定	295
802.1X 設定の確認	296
VXLAN EVPN の 802.1X サポート	296
VXLAN EVPN の 802.1X サポートに関する注意事項と制約事項	296
VXLAN EVPN の 802.1X サポートの設定	297
VXLAN EVPN の 802.1X サポートの確認	298
802.1X のモニタリング	301
802.1X の設定例	302
802.1X に関する追加情報	302

---

**第 12 章****IP ACL の設定 305**

ACL について	305
ACL のタイプと適用	306
ACL ?????	308
ルールについて	309
IP ACL および MAC ACL のプロトコル	309
送信元と宛先	310
IP ACL および MAC ACL の暗黙ルール	310
その他のフィルタリング オプション	310
シーケンス番号	312
論理演算子と論理演算ユニット	312
IPv4 ACL ロギング	313
時間範囲	313
ポリシーベース ACL	315
統計情報と ACL	316
Atomic ACL のアップデート	316
IP ACL に対する Session Manager のサポート	317
ACL TCAM リージョン	317
ACL タイプでサポートされる最大ラベル サイズ	325

IP ACL の前提条件	325
IP ACL の注意事項と制約事項	326
IP ACL のデフォルト設定	334
IP ACL の設定	334
IP ACL の作成	334
IP ACL の変更	337
VTY ACL の作成	339
IP ACL 内のシーケンス番号の変更	340
IP ACL の削除	341
ACL TCAM リージョンサイズの設定	342
テンプレートを使用した ACL TCAM リージョンサイズの設定	354
TCAM カービングの設定	356
UDF ベース ポート ACL の設定	363
ルータ ACL としての IP ACL の適用	366
ポート ACL としての IP ACL の適用	367
IP ACL の VACL としての適用	368
IPv4 ACL ロギングの設定	368
要求をリダイレクトするための HTTP メソッドによる ACL の設定	371
IPv6 拡張ヘッダーの ACL の設定	373
IP ACL の設定の確認	374
IP ACL の統計情報のモニタリングとクリア	377
IP ACL の設定例	378
システム ACL について	379
TCAM リージョンの分割	380
システム ACL の設定	380
システム ACL の設定および show コマンドの例	380
オブジェクト グループの設定	383
オブジェクト グループに対する Session Manager のサポート	383
IPv4 アドレス オブジェクト グループの作成および変更	383
IPv6 アドレス オブジェクト グループの作成および変更	384
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	385

オブジェクトグループの削除	387
オブジェクトグループの設定の確認	387
??????	388
時間範囲の Session Manager サポート	388
時間範囲の作成	388
時間範囲の変更	389
時間範囲の削除	391
時間範囲のシーケンス番号の変更	392
時間範囲設定の確認	392
IP ACL に関する追加情報	393

---

**第 13 章**

<b>MAC ACL の設定</b>	<b>395</b>
MAC ACL について	395
MAC パケット分類	395
MAC ACL の注意事項と制約事項	396
MAC ACL のデフォルト設定	397
MAC ACL の設定	397
MAC ACL の作成	397
UDF ベースの MAC ACL の設定	398
インターフェイス MAC アドレスの設定と制限	400
MAC ACL の変更	402
MAC ACL 内のシーケンス番号の変更	404
MAC ACL の削除	404
ポート ACL としての MAC ACL の適用	405
MAC ACL の VACL としての適用	406
MAC パケット分類のイネーブル化またはディセーブル化	406
MAC ACL の設定の確認	408
MAC ACL の統計情報のモニタリングとクリア	408
MAC ACL の設定例	408
MAC ACL に関する追加情報	409

---

**第 14 章****VLAN ACL の設定 411**

- VLAN ACL について 411
  - VLAN アクセス マップとエントリ 411
  - VACL とアクション 412
  - VACL の統計情報 412
  - VACL に対する Session Manager のサポート 412
- VACL の前提条件 412
- VACL の注意事項と制約事項 413
- VACL のデフォルト設定 414
- VACL の設定 414
  - VACL の作成または VACL エントリの追加 414
  - VACL または VACL エントリの削除 415
  - VACL の VLAN への適用 416
- VACL 設定の確認 417
- VACL 統計情報のモニタリングとクリア 418
- VACL の設定例 418
- VACL に関する追加情報 418

---

**第 15 章****ポートセキュリティの設定 419**

- ポートセキュリティの概要 419
  - セキュア MAC アドレスの学習 420
    - スタティック方式 420
    - ダイナミック方式 420
    - スティッキ方式 421
  - ダイナミック アドレスのエージング 421
- セキュア MAC アドレスの最大数 422
- セキュリティ違反と処理 422
- ポートセキュリティとポートタイプ 424
- 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 424
- ポートタイプの変更 426

ポートセキュリティの前提条件	427
ポートセキュリティのデフォルト設定	427
ポートセキュリティの注意事項と制約事項	427
vPC上のポートセキュリティの注意事項と制約事項	428
ポートセキュリティの設定	429
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	429
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	430
スティック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	431
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	432
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	434
スティックセキュアMACアドレスの削除	435
ダイナミックセキュアMACアドレスの削除	436
MACアドレスの最大数の設定	437
アドレスエージングのタイプと期間の設定	438
セキュリティ違反時の処理の設定	440
ポートセキュリティの設定の確認	441
セキュアMACアドレスの表示	441
ポートセキュリティの設定例	441
vPCドメインでのポートセキュリティの設定例	441
例：孤立ポートでのポートセキュリティの設定	442
例：vPCレグ上のポートセキュリティの設定	442
ポートセキュリティに関する追加情報	443

## 第 16 章

**DHCP の設定** 445

DHCP スヌーピングについて	446
信頼できる送信元と信頼できない送信元	446
DHCP スヌーピング バインディング データベース	447
vPC 環境での DHCP スヌーピング	447
DHCP スヌーピング バインディング エントリの同期	448
パケット検証	448

DHCP ??????? Option 82 ?????	448
DHCP リレー エージェントについて	450
DHCP リレー エージェント	450
DHCP ??? ??????? Option 82	450
DHCP リレー エージェントに対する VRF サポート	452
DHCP スマート リレー エージェント	453
DHCPv6 リレー エージェントについて	453
DHCPv6 リレー エージェント	453
DHCPv6 リレー エージェントに対する VRF サポート	454
DHCP クライアントについて	454
DHCP の前提条件	454
DHCP の注意事項と制約事項	454
DHCP のデフォルト設定	456
DHCP の設定	457
DHCP の最小設定	457
DHCP 機能のイネーブル化またはディセーブル化	458
DHCP スヌーピングの設定	458
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	458
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	459
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	460
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	461
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	463
インターフェイスの信頼状態の設定	464
DHCP リレー信頼ポート機能のイネーブル化またはディセーブル化	465
インターフェイスの DHCP リレー信頼または非信頼ポートとしての設定	466
すべてのインターフェイスの信頼状態の設定	468
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	469
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	470
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	471
DHCP Server Identifier オーバーライド サブオプション	472
インターフェイスへの DHCP サーバアドレスの設定	473

DHCP リレー送信元インターフェイスの設定	475
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	476
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	477
DHCP リレー サブネット選択の設定	478
DHCPv6 の設定	479
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	479
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	480
インターフェイスへの DHCPv6 サーバアドレスの設定	482
DHCPv6 オプション 79 のイネーブル化	483
DHCPv6 リレー送信元インターフェイスの設定	484
IPv6 RA ガードの設定	485
DHCP クライアントのイネーブル化	486
UDP リレーの設定	488
UDP リレーについて	488
UDP リレーの注意事項と制約事項	489
UDP リレーの設定	489
UDP リレーの設定例	491
UDP リレーの設定の確認	491
DHCP 設定の確認	492
IPv6 RA ガードの統計情報の表示	493
DHCP スヌーピング バインディングの表示	493
DHCP スヌーピング バインディング データベースのクリア	493
DHCP のモニタリング	494
DHCP スヌーピング統計情報のクリア	494
DHCP リレー統計情報のクリア	494
DHCPv6 リレー統計情報のクリア	494
DHCP の設定例	494
DHCP クライアントの設定例	495
DHCP に関する追加情報	496



## 第 17 章

<b>IPv6 ファースト ホップ セキュリティの設定</b>	<b>497</b>
ファーストホップセキュリティについて	497
IPv6 グローバル ポリシー	498
IPv6 ファーストホップセキュリティ バインディング テーブル	498
ファーストホップセキュリティの注意事項と制約事項	499
vPC ファーストホップセキュリティ設定について	499
DHCP リレー オンスタック	499
VPC レッグでの DHCP リレー	500
孤立ポートでの DHCP クライアントリレー	501
RA ガード	503
IPv6 RA ガードの概要	503
IPv6 RA ガードの注意事項と制約事項	503
DHCPv6 ガード	503
DHCPの概要 : DHCPv6 ガード	503
DHCPv6 ガードの制限事項	504
IPv6 スヌーピング	504
IGMP スヌーピングの概要	504
IPv6 スヌーピングに関する注意事項と制限事項	505
IPv6 FHS の設定方法	506
デバイスでの IPv6 RA ガード ポリシーの設定	506
インターフェイスの IPv6 RA ガードの設定	508
DHCP—DHCPv6 ガードの設定	509
IPv6 スヌーピングの設定	511
IPv6 スヌーピングの確認とトラブルシューティング	514
設定例	515
例 : IPv6 RA ガードの設定	515
例 : DHCP—DHCPv6 ガードの設定	515
例 : IPv6 ファーストホップセキュリティ バインディング テーブルの設定	515
例 : IPv6 スヌーピングの設定	516
IPv6 ファーストホップセキュリティに関する追加情報	516

---

第 18 章	<b>ダイナミック ARP インспекションの設定</b>	<b>517</b>
	DAI について	517
	『ARP』	517
	ARP ?????????	518
	DAI および ARP スプーフィング攻撃	518
	????????????????????????????????????	519
	DAI パケットのロギング	520
	DAI の前提条件	520
	DAI の注意事項と制約事項	521
	DAI のデフォルト設定	522
	DAI の設定	522
	VLAN での DAI のイネーブル化とディセーブル化	522
	レイヤ 2 インターフェイスの DAI 信頼状態の設定	523
	追加検証のイネーブル化またはディセーブル化	524
	DAI のログ バッファ サイズの設定	526
	DAI のログ フィルタリングの設定	526
	DAI の設定の確認	527
	DAI の統計情報のモニタリングとクリア	528
	DAI の設定例	528
	DAI ??????? 2 ???????	528
	デバイス A の設定	529
	デバイス B の設定	531
	DAI に関する追加情報	533
	関連資料	533
	標準	533

---

第 19 章	<b>IP ソース ガードの設定</b>	<b>535</b>
	IP ソース ガードについて	535
	IP ソース ガードの前提条件	536
	IP ソース ガードの注意事項と制約事項	536

IP ソース ガードのデフォルト設定	537
IP ソース ガードの設定	538
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	538
スタティック IP ソース エントリの追加または削除	539
トランク ポート用 IP ソース ガードの設定	539
IP ソース ガード バインディングの表示	540
IP ソース ガードの統計情報のクリア	540
IP ソース ガードの設定例	541
その他の参考資料	541
関連資料	541

---

**第 20 章**

<b>パスワード暗号化の設定</b>	<b>543</b>
AES パスワード暗号化およびプライマリ暗号キーについて	543
パスワード暗号化の注意事項と制約事項	544
パスワード暗号化のデフォルト設定	545
パスワード暗号化の設定	545
プライマリ キーの設定および AES パスワード暗号化機能の有効化	545
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	547
タイプ 6 暗号化パスワードの元の状態への変換	547
MACsec キーでのタイプ 6 暗号化のイネーブル化	548
タイプ 6 暗号化パスワードの削除	549
パスワード暗号化の設定の確認	549
パスワード暗号化の設定例	549

---

**第 21 章**

<b>キーチェーン管理の設定</b>	<b>551</b>
キーチェーン管理について	551
キーのライフタイム	551
キーチェーン管理の前提条件	552
キーチェーン管理の注意事項と制約事項	552
キーチェーン管理のデフォルト設定	553

キーチェーン管理の設定	553
キーチェーンの作成	553
キーチェーンの削除	554
プライマリ キーの設定および AES パスワード暗号化機能の有効化	555
キーのテキストの設定	556
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	558
OSPFv2 暗号化認証用のキーの設定	559
アクティブなキーのライフタイムの確認	561
キーチェーン管理の設定の確認	561
キーチェーン管理の設定例	561
次の作業	561
キーチェーン管理に関する追加情報	562

---

**第 22 章**

<b>ユニキャスト RPF の設定</b>	<b>563</b>
ユニキャスト RPF について	563
ユニキャスト RPF プロセス	564
ユニキャスト RPF の注意事項と制約事項	565
ユニキャスト RPF のデフォルト設定	568
-R ラインカードを搭載した Cisco Nexus 9500 スイッチのユニキャスト RPF の設定	568
Cisco Nexus 9300 スイッチのユニキャスト RPF の設定	569
ユニキャスト RPF の設定例	572
ユニキャスト RPF の設定の確認	573
ユニキャスト RPF に関する追加情報	573

---

**第 23 章**

<b>スイッチポート ブロッキングの設定</b>	<b>575</b>
スイッチポート ブロッキングについて	575
スイッチポート ブロッキングの注意事項および制約事項	575
スイッチポート ブロッキングのデフォルト設定	576
スイッチポート ブロッキングの設定	576
スイッチポート ブロッキング設定の確認	577
スイッチポート ブロッキングの設定例	577

## コントロールプレーン ポリシングの設定 579

## CoPP について 579

## コントロールプレーン保護 581

## コントロールプレーンのパケットタイプ 581

## CoPP の分類 582

## レート制御メカニズム 582

## ダイナミックおよびスタティック CoPP ACL 582

## デフォルトのポリシング ポリシー 583

## モジュラ QoS コマンドライン インターフェイス 596

## CoPP と管理インターフェイス 597

## CoPP の注意事項と制約事項 597

## CoPP のデフォルト設定 601

## CoPP の設定 601

## コントロールプレーン クラス マップの設定 601

## コントロールプレーン ポリシー マップの設定 603

## コントロールプレーン サービス ポリシーの設定 605

## ラインカードごとの CoPP のスケールファクタの設定 607

## デフォルトの CoPP ポリシーの変更または再適用 608

## CoPP ベストプラクティス ポリシーのコピー 609

## プロトコル ACL フィルタリング 609

## CoPP の ARP ACL フィルタリングの設定 610

## CoPP の IP ACL フィルタリングの設定 612

## CoPP の設定の確認 614

## CoPP 設定ステータスの表示 617

## CoPP のモニタリング 617

## SNMP での CoPP のモニタリング 618

## CoPP 統計情報のクリア 618

## CoPP の設定例 619

## CoPP の設定例 619

## 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 620

## CoPP に関する追加情報 621

## 第 25 章

## レート制限の設定 623

- レート制限について 623
- レート制限の注意事項と制約事項 624
- レート制限のデフォルト設定 625
- レート制限の設定 625
- レート制限のモニタリング 628
- レート制限統計情報のクリア 628
- レート制限の設定の確認 628
- レート制限の設定例 629
- レート制限に関する追加情報 629

## 第 26 章

## MACsec の設定 631

- MACsec について 631
  - キー ライフタイムおよびヒットレス キー ロールオーバー 632
  - フォールバック キー 632
- MACSec の注意事項と制約事項 632
- MACsec の有効化 636
- MACsec の無効化 637
- MACsec キーチェーンとキーの設定 638
- MACsec フォールバック キーの設定 640
- MACsec ポリシーの設定 642
- PSK のローテーション 643
- 設定可能な EAPOL の宛先とイーサネットタイプについて 644
  - EAPOL 設定の有効化 644
  - EAPOL 設定の無効化 645
- MACsec 設定の確認 646
- MACsec 統計の表示 648
- MACsec の設定例 651
- XML の例 653

MIB 661

関連資料 661







## はじめに

この前書きは、次の項で構成されています。

- [対象読者 \(xxix ページ\)](#)
- [表記法 \(xxix ページ\)](#)
- [Cisco Nexus 9000 シリーズ スイッチの関連資料 \(xxx ページ\)](#)
- [マニュアルに関するフィードバック \(xxx ページ\)](#)
- [通信、サービス、およびその他の情報 \(xxxi ページ\)](#)

## 対象読者

このマニュアルは、Cisco Nexus スイッチの設置、設定、および維持に携わるネットワーク管理者を対象としています。

## 表記法

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
<b>bold</b>	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。
<i>italic</i>	イタリック体の文字は、ユーザが値を指定する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角かっこ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、角かっこで囲み、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、波かっこで囲み、縦棒で区切って示しています。

表記法	説明
[x {y   z}]	角かっこまたは波かっこ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。角かっこ内の波かっこと縦棒は、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ないでください。引用符を使用すると、その引用符も含めて string と見なされます。

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、スクリーン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、イタリック体のスクリーン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。

## Cisco Nexus 9000 シリーズ スイッチの関連資料

Cisco Nexus 9000 シリーズ スイッチ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/ps13386/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps13386/tsd_products_support_series_home.html)

## 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。ご協力をよろしくお願いいたします。

## 通信、サービス、およびその他の情報

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

### Cisco バグ検索ツール

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





# 第 1 章

## 新機能および変更された機能に関する情報

この章では、『Cisco Nexus 9000 シリーズ NX-OS セキュリティ ガイド、リリース 9.3(x)』に記載されている、新機能および変更された機能に関するリリース固有の情報について説明します。

- [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

次の表は、『Cisco Nexus 9000 シリーズ NX-OS セキュリティ コンフィギュレーション ガイド リリース 9.3(x)』に記載されている新機能および変更機能をまとめたものです。それぞれの説明が記載されている箇所も併記されています。

表 1: 新機能および変更された機能

機能	説明	変更が行われたリリース	参照先
IP ACL	PACL/L2QOS/L2 SPAN ACLのラベルサイズを62に増やす機能が追加されました。この機能は、Nexus 9300-FX プラットフォームスイッチでのみサポートされています。	9.3(6)	<a href="#">ACLタイプでサポートされる最大ラベルサイズ (325 ページ)</a>

機能	説明	変更が行われたリリース	参照先
MAC 認証バイパスによる認証のみ	dot1q 対応ポート上のすべてのトラフィックのデフォルト認証方式として MAB を設定する機能が追加されました。  この機能は、すべての Cisco Nexus 9000 シリーズスイッチでサポートされています。	9.3(5)	<a href="#">デフォルト dot1.x 認証認証方式の設定 - MAB (285 ページ)</a>
Dynamic ACL	MAB クライアントの dot1q ブロック リストへのアクセスを制限する機能が追加されました。この機能は、Cisco Nexus 9336-FX2、Nexus 9236C、Nexus 93108TC-EX、および Nexus 93180YC-EX スイッチでサポートされています。	9.3(5)	<ul style="list-style-type: none"> <li>• <a href="#">DACL について (271 ページ)</a></li> <li>• <a href="#">ダイナミックアクセスリストの作成 (286 ページ)</a></li> </ul>
DHCPv6	Cisco Nexus 9300-GX プラットフォームスイッチの DHCPv6 リレー パケットで DHCPv6 オプション 79 (クライアントリンク層アドレス) のサポートが追加されました。	9.3(5)	<ul style="list-style-type: none"> <li>• <a href="#">DHCPv6 オプション 79 のイネーブル化 (483 ページ)</a></li> <li>• <a href="#">DHCP に関する追加情報 (496 ページ)</a></li> </ul>
IPv6 ファーストホップセキュリティ	Cisco Nexus 9300-GX プラットフォームスイッチのサポートが追加されました。	9.3(5)	<a href="#">ファーストホップセキュリティの注意事項と制約事項 (499 ページ)</a>
IPv6 出力 ACL	-R および RX ラインカードを備えた Cisco Nexus 9504 および 9508 プラットフォームスイッチでの IPv6 出力 ACL のサポートが追加されました。	9.3(5)	<a href="#">IP ACL の注意事項と制約事項 (326 ページ)</a>

機能	説明	変更が行われたリリース	参照先
IP ソース ガード (IPSG)	Cisco Nexus 9300-GX プラットフォームスイッチでのサポートが追加されました。	9.3(5)	IP ソース ガイドの注意事項と制約事項 (536 ページ)
MACsec	Cisco Nexus N9K-C93180YC-FX3S、Nexus N9K-X9732C-FX、およびNexus N9K-X9788TC-FX ラインカードでのサポートが追加されました。	9.3(5)	MACSecの注意事項と制約事項 (632 ページ)
NDcPP : syslog の OCSP	syslog サーバの OCSP サポートが追加されました。この機能は、すべての Cisco Nexus 9000 シリーズスイッチでサポートされています。	9.3(5)	<ul style="list-style-type: none"> <li>• 証明書の取消確認 (187 ページ)</li> <li>• PKI の注意事項と制約事項 (188 ページ)</li> <li>• NDcPP : syslog の OCSP (188 ページ)</li> </ul>
PACLリダイレクト	Cisco Nexus 9300-GX スイッチでの PACL リダイレクトのサポートが追加されました。	9.3(5)	IP ACL の注意事項と制約事項 (326 ページ)
MACsec キーのタイプ 6 暗号化	MACsec 事前共有キーをタイプ 6 暗号化形式で保存する機能が追加されました。  この機能は、MACsec をサポートするすべての Nexus 9000 シリーズスイッチでサポートされます。	9.3(5)	<ul style="list-style-type: none"> <li>• パスワード暗号化の注意事項と制約事項 (544 ページ)</li> <li>• MACsec キーでのタイプ 6 暗号化のイネーブル化 (548 ページ)</li> </ul>

機能	説明	変更が行われたリリース	参照先
IP ヘルパー アドレス	DHCPv4 ポート番号 67 および 68 を除くすべての UDP ポートを宛先とするリレーブロードキャストのルート設定を有効にする機能が追加されました。この機能は、-EX/FXラインカードを搭載した Nexus 9200、9300、9300-EX、Nexus 9300-FX/FX2、および Nexus 9500 スイッチでサポートされています。	9.3(5)	<a href="#">UDP リレーの設定 (488 ページ)</a>
802.1x	Cisco Nexus 9300-GX フォーム スイッチでの 802.1X のサポートが追加されました。	9.3(3)	<a href="#">802.1X の注意事項と制約事項 (272 ページ)</a>
DAI	Cisco Nexus 9300-GX スイッチでの DAI のサポートが追加されました。	9.3(3)	<a href="#">DAI の注意事項と制約事項 (521 ページ)</a>
DHCP	Cisco Nexus 9300-GX スイッチでの DHCP スヌーピングおよび DHCP リレーのサポートが追加されました。	9.3(3)	<a href="#">DHCP の注意事項と制約事項 (454 ページ)</a>
DHCP	DHCP オプション 82 パケットのサーバ識別子オーバーライドオプションを無効にする機能が追加されました。	9.3(3)	<a href="#">DHCP Server Identifier オーバーライドサブオプション (472 ページ)</a>
DHCP	インターフェイスに両方のサブネットが含まれる場合に、DHCP リレーがプライマリまたはセカンダリサブネットを選択できるようになりました。	9.3(3)	<a href="#">DHCP リレーサブネット選択の設定 (478 ページ)</a>



機能	説明	変更が行われたリリース	参照先
DHCPv6	すべての Cisco Nexus 9000 シリーズ スイッチ およびラインカードの DHCPv6 リレーパケットでの DHCPv6 オプション 79 (クライアントリンク層アドレス) のサポートが追加されました。	9.3(3)	<ul style="list-style-type: none"> <li>• <a href="#">DHCPv6 オプション 79 のイネーブル化 (483 ページ)</a></li> <li>• <a href="#">DHCP に関する追加情報 (496 ページ)</a></li> </ul>
IP ACL	-R および -RX ラインカードを使用した Cisco Nexus 9500 プラットフォームスイッチでの出力 IPv4 および IPv6 RACL のサポートが追加されました	9.3(3)	<a href="#">IP ACL の注意事項と制約事項 (326 ページ)</a>
MAC UDF	Cisco Nexus 9300-GX スイッチの UDF ベースの MAC アクセス リスト (ACL) を設定する機能。	9.3(3)	<a href="#">UDF ベースの MAC ACL の設定 (398 ページ)</a>
MACsec	Cisco Nexus 93108TC2-FX、Cisco Nexus 93180YC2-FX、Cisco Nexus 93216TC-FX2、および Cisco Nexus 93360YC-FX2 スイッチでの MACsec のサポートが追加されました。	9.3(3)	<a href="#">MACSec の注意事項と制約事項 (632 ページ)</a>
ユーザ定義の MAC アドレス	16 ～ 256 の範囲でユーザ定義の MAC アドレス制限を設定できます。	9.3(2)	<ul style="list-style-type: none"> <li>• <a href="#">MAC ACL の注意事項と制約事項 (396 ページ)</a></li> <li>• <a href="#">インターフェイス MAC アドレスの設定と制限 (400 ページ)</a></li> </ul>

機能	説明	変更が行われたリリース	参照先
MAC UDF	デバイスがユーザ定義フィールド (UDF) で照合し、マッチするパケットを MAC ACL に適用するのを可能にする機能。	9.3(2)	<a href="#">UDF ベースの MAC ACL の設定 (398 ページ)</a>
MACSec	MACsec は、Cisco Nexus N9K-C9364C、N9K-C9332C、および N9K-C9348GC-FXP プラットフォームスイッチでサポートされるようになりました。	9.3(1)	<a href="#">MACSec の注意事項と制約事項 (632 ページ)</a>
uRPF	uRPF は、モジュラ EX および FX ラインカードファミリを搭載した Cisco Nexus 9500 シリーズスイッチでサポートされるようになりました。	9.3(1)	<a href="#">ユニキャスト RPF の注意事項と制約事項 (565 ページ)</a>
MAC UDF	Cisco Nexus 9200、9300、および 9300-EX シリーズスイッチの UDF ベースの MAC アクセスリスト (ACL) を設定する機能。この機能により、デバイスはユーザ定義フィールド (UDF) で照合を行い、マッチするパケットを MAC ACL に適用できます。	9.3(1)	<a href="#">UDF ベースの MAC ACL の設定 (398 ページ)</a>



## CHAPTER 2

### 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。

- [ライセンス要件 \(7 ページ\)](#)
- [Authentication, Authorization, and Accounting \(認証、許可、およびアカウントिंग\) , on page 8](#)
- [RADIUS および TACACS+ セキュリティ プロトコル, on page 8](#)
- [LDAP, on page 9](#)
- [SSH および Telnet, on page 9](#)
- [ユーザアカウントおよびユーザ ロール, on page 10](#)
- [IP ACL, on page 10](#)
- [MAC ACL, on page 10](#)
- [VACL, on page 10](#)
- [DHCP スヌーピング, on page 11](#)
- [ダイナミック ARP インスペクション, on page 11](#)
- [IP ソース ガード, on page 11](#)
- [パスワード暗号化, on page 12](#)
- [キーチェーン管理, on page 12](#)
- [コントロールプレーン ポリシング, on page 12](#)
- [レート制限, on page 13](#)
- [ソフトウェア イメージ \(13 ページ\)](#)
- [仮想デバイス コンテキスト \(13 ページ\)](#)

### ライセンス要件

Cisco NX-OS ライセンス方式の推奨の詳細と、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。

# Authentication, Authorization, and Accounting (認証、許可、およびアカウントティング)

認証、許可、アカウントティング (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。

## アカウントティング

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。アカウント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。



**Note** 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+ を使用する場合は、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。

詳細については、[AAA の設定](#)の章を参照してください。

## 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、アカウントिंग機能が提供されます。

詳細については、[TACACS+ の設定](#)の章および[RADIUS の設定](#)の章を参照してください。

## 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。

詳細については、[LDAP の設定](#)の章を参照してください。

## 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、無償あるいは商用の SSH サーバと関係して動作します。

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。

詳細については、[SSH および Telnet の設定](#)の章を参照してください。

## ユーザアカウントおよびユーザロール

ユーザアカウントを作成して管理し、Cisco NX-OS デバイス上で行え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。

詳細については、[ユーザアカウントおよびRBACの設定](#)の章を参照してください。

## 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 ソフトウェアは、ある IP 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、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については処理を続行し、拒否されたパケットはドロップします。

詳細については、[IP ACL の設定](#)の章を参照してください。

## 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、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については処理を続行し、拒否されたパケットはドロップします。

## 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。

詳細については、[VLAN ACL の設定](#)の章を参照してください。

## 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спекション (DAI) および IP ソース ガード (IPSG) 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。

## ダイナミック ARP インспекション

ダイナミック ARP インспек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 が有効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。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。

## 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。

## 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。プライマリ暗号キーは、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。

詳細については、[パスワード暗号化の設定](#)の章を参照してください。

## 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、[キーチェーン管理の設定](#)の章を参照してください。

## コントロールプレーンポリシング

Cisco NX-OS デバイスは、DoS 攻撃によるパフォーマンスへの影響を防ぐために CoPP 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。

詳細については、[コントロールプレーンポリシングの設定](#)の章を参照してください。



## 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。

詳細については、[レート制限の設定](#)の章を参照してください。

## ソフトウェア イメージ

Cisco NX-OS ソフトウェアは、1つの NXOS ソフトウェア イメージで構成されています。このイメージは、すべての Cisco Nexus 3400 シリーズ スイッチで実行されます。

## 仮想デバイス コンテキスト

Cisco NX-OS では、仮想デバイスをエミュレートする Virtual Device Context (VDCs) に、OS およびハードウェア リソースを分割できます。Cisco Nexus 9000 シリーズ スイッチは、現在のところ、複数の VDC をサポートしていません。すべてのスイッチリソースはデフォルト VDC で管理されます。





## 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。

- [FIPS について](#)（15 ページ）
- [FIPS の前提条件](#)（17 ページ）
- [FIPS の注意事項と制約事項](#)（17 ページ）
- [FIPS のデフォルト設定](#)（17 ページ）
- [FIPS の設定](#)（18 ページ）
- [FIPS の設定の確認](#)（20 ページ）
- [FIPS の設定例](#)（20 ページ）
- [FIPS に関する追加情報](#)（20 ページ）

## FIPS について

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としています。

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。

## 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。

## 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。

- 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。
- FIPS モードがオンの場合は、Radius と TACACS を無効にします。これは、FIPS モードの OpenSSL により適用されます。

## 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 モードの有効化

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。

始める前に

デフォルト VDC にいることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>fips mode enable</b> 例： switch(config)# fips mode enable	FIPS モードをイネーブルにします。  (注) <b>fips mode enable</b> 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	<b>exit</b> 例： switch(config)# exit switch#	設定モードを終了します。
ステップ 4	(任意) <b>show fips status</b> 例： switch# show fips status FIPS mode is enabled	FIPS モードのステータスを表示します。
ステップ 5	必須: <b>copy running-config startup-config</b> 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	必須: <b>reload</b> 例 : <pre>switch# reload</pre>	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。

## FIPS の無効化

デバイスの FIPS モードをディセーブルにできます。

### 始める前に

デフォルト VDC にいることを確認します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>no fips mode enable</b> 例 : <pre>switch(config)# no fips mode enable</pre>	FIPS モードをディセーブルにします。
ステップ 3	<b>exit</b> 例 : <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 4	(任意) <b>show fips status</b> 例 : <pre>switch# show fips status FIPS mode is disabled</pre>	FIPS モードのステータスを表示します。
ステップ 5	<b>copy running-config startup-config</b> 例 : <pre>switch# copy running-config startup-config</pre>	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	<b>reload</b> 例 : switch# reload	Cisco NX-OS デバイスをリロードします。

## 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
<b>show fips status</b>	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 9000 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	『 <i>Cisco NX-OS Licensing Guide</i> 』
コマンドリファレンス	『 <i>Cisco Nexus 9000 Series NX-OS Security Command Reference</i> 』



## 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





## 第 4 章

# AAA の設定

この章では、Cisco NX-OS デバイスで認証、許可、アカウントिंग（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。

- [AAA について, on page 23](#)
- [AAA の前提条件, on page 28](#)
- [AAA の注意事項と制約事項, on page 28](#)
- [AAA のデフォルト設定, on page 29](#)
- [AAA の設定, on page 29](#)
- [ローカル AAA アカウントング ログのモニタリングとクリア , on page 51](#)
- [AAA 設定の確認, on page 52](#)
- [AAA の設定例, on page 53](#)
- [ログインパラメータの設定例（53 ページ）](#)
- [パスワードプロンプト機能の設定例（54 ページ）](#)
- [AAA に関する追加情報, on page 55](#)

## AAA について

ここでは、Cisco NX-OS デバイスの 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。

#### アカウントティング

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。

アカウントティング機能では、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。アカウントティングログは、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。



**Note** Cisco NX-OS ソフトウェアでは、認証、許可、およびアカウントティングを個別にサポートしています。たとえば、アカウント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トिंग ログを中央で管理できます。
- ファブリック内の各 Cisco NX-OS デバイスについてユーザ属性を管理する方が、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簡単です。

## AAA サーバグループ

認証、許可、アカウントिंग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、最初のグループ内のサーバからエラーを受け取った場合、次のサーバグループ内のサーバで試行します。

## 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
- ユーザ管理セッション アカウントिंग

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。

**Table 3: 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	<code>aaa authentication login default</code>

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
コンソール ログイン	<b>aaa authentication login console</b>
ユーザ セッション アカウンティング	<b>aaa accounting default</b>

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。



**Note** 「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 プールからのサーバは、Cisco NX-OS デバイス上の RADIUS サーバ グループ内で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。

**Table 4: 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
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

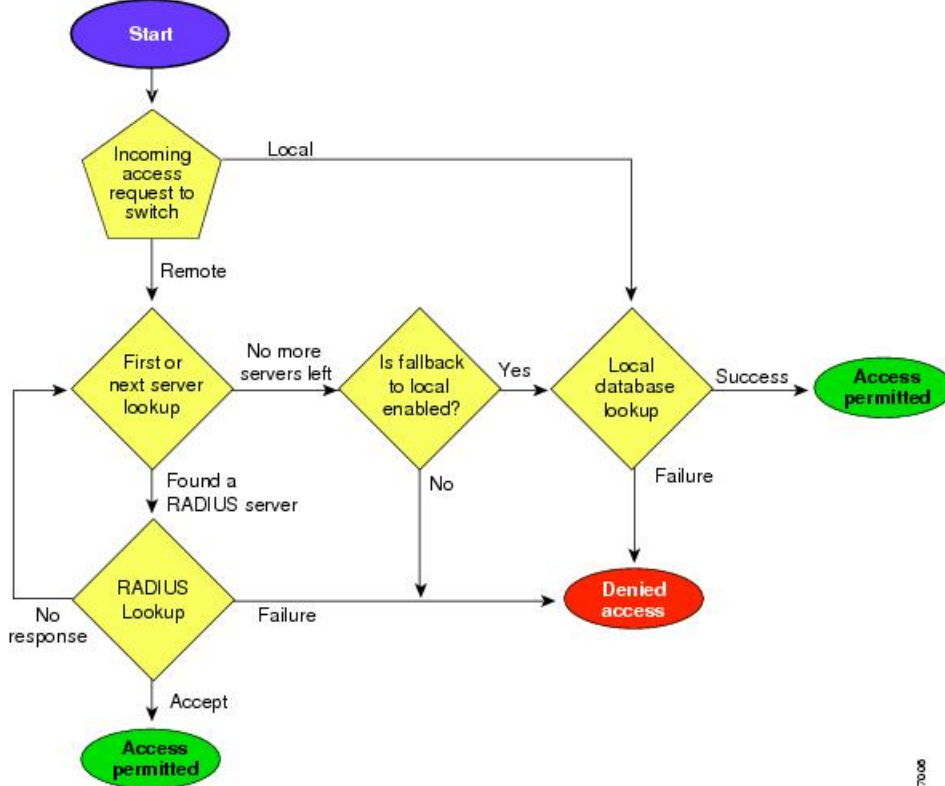


**Note** コンソール ログイン認証、ユーザ ログイン認証、およびユーザ管理セッションアカウンティングについて、Cisco NX-OS デバイスは各オプションを指定された順序で試行します。その他の設定済みオプションが失敗した場合、ローカルオプションがデフォルト方式です。コンソールまたはデフォルトログインのローカルオプションを無効にするには、**no aaa authentication login {console | default} fallback error local** コマンドを使用します。

???

Figure 1: ???

?????



157006

?????

- Cisco NX-OS Telnet/SSH
- Cisco NX-OS AAA
  - AAA RADIUS
  - AAA TACACS+
- Cisco NX-OS AAA



## Note

?????? ?????????????????? ???  
 ???

## AES パスワード暗号化およびプライマリ暗号キー

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有効にし、パスワード暗号化および復号化に使用されるプライマリ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プライマリ 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。

## 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。
- 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。
- Cisco Nexus 9000 シリーズスイッチは、TACACS + でのみ **aaa authentication login ascii-authentication** コマンドをサポートします (RADIUS ではサポートしません)。
- デフォルトのログイン認証方式を (**local** キーワードを使用せずに) 変更すると、コンソールログイン認証方式が設定によって上書きされます。コンソール認証方式を明示的に設定



するには、`aaa authentication login console {group group-list [none] | local | none}` コマンドを使用します。

- **login block-for** および **login quiet-mode** コンフィギュレーション モード コマンドは、それぞれ **system login block-for** および **system login quiet-mode** に名前が変更されました。
- **system login quiet-mode access-class QUIET\_LIST** コマンドを使用する場合は、指定したトラフィックのみをブロックするようにアクセスリストが正しく定義されていることを確認する必要があります。たとえば、信頼できないホストからのユーザログインのみをブロックする必要がある場合、アクセスリストは、それらのホストからのSSH、Telnet、およびHTTP ベースのアクセスに対応するポート22、23、80、および443を指定する必要があります。

## 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。

**Table 5: 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	ローカル
デフォルト認証方式	ローカル
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	ローカル
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 機能を設定する手順について説明します。



### Note

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りますので注意してください。



**Note** Cisco Nexus 9K シリーズ スイッチは、TACAAS+ に対してのみ CLI コマンド `aaa authentication login ascii-authentication` をサポートしますが、RADIUS に対してはサポートしません。デフォルト認証である PAP が有効になるように、`aaa authentication login ascii-authentication` スイッチが無効になっていることを確認します。そうしないと、`syslog` エラーが表示されます。

## AAA の設定プロセス

AAA 認証およびアカウントिंग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 アカウントिंग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。



**Note** `aaa authentication` コマンドの `group radius` および `groupserver-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。



**Note** 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に関する詳細情報については、『Cisco Nexus 9000 Series NX-OS Troubleshooting Guide』を参照してください。

### Before you begin

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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	コンフィギュレーションモードに入ります。
ステップ 2	<b>aaa authentication login console { group group-list [none]   local   none}</b> <b>Example:</b> <pre>switch(config)# aaa authentication login console group radius</pre>	コンソールのログイン認証方式を設定します。  <i>group-list</i> 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。  <b>radius</b> 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。  <b>named-group</b> 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。  <b>local</b> 方式は、ローカルデータベースを認証に使用します。 <b>none</b> 方式では、AAA 認証が使用されないように指定します。  デフォルトのコンソールログイン方式は <b>local</b> 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

	Command or Action	Purpose
		ローカルへのフォールバックが無効でない限り、使用されます。
ステップ 3	<b>exit</b>  <b>Example:</b> switch(config)# <b>exit</b> switch#	設定モードを終了します。
ステップ 4	(Optional) <b>show aaa authentication</b>  <b>Example:</b> switch# <b>show aaa authentication</b>	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	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> switch# <b>copy running-config startup-config</b>	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。

### Before you begin

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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> switch# <b>configure terminal</b> 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	<b>aaa authentication login default { group group-list [none]   local   none }</b>	デフォルト認証方式を設定します。

	Command or Action	Purpose
	<p><b>Example:</b></p> <pre>switch(config)# aaa authentication login default group radius</pre>	<p><i>group-list</i> 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。</p> <ul style="list-style-type: none"> <li>• <b>radiusRADIUS</b> サーバのグローバルプールを使用して認証を行います。</li> <li>• <b>named-group</b> : 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。</li> </ul> <p><b>local</b> 方式は、ローカルデータベースを認証に使用します。<b>none</b> 方式では、AAA 認証が使用されないように指定します。デフォルトのログイン方式は <b>local</b> 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。</p> <p>次のいずれかを設定できます。</p> <ul style="list-style-type: none"> <li>• AAA 認証グループ</li> <li>• 認証なしの AAA 認証グループ</li> <li>• ローカル認証</li> <li>• 認証なし</li> </ul>

	Command or Action	Purpose
		<p><b>Note</b> <b>local</b> 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、ローカル認証は、リモートサーバが到達不能の場合のデフォルトであるためです。たとえば、<b>aaa authentication login default group g1</b> を設定した場合、AAA グループ <b>g1</b> 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、<b>aaa authentication login default group g1 none</b> を設定した場合、AAA グループ <b>g1</b> 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。</p>
ステップ 3	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 4	<p>(Optional) <b>show aaa authentication</b></p> <p><b>Example:</b></p> <pre>switch# show aaa authentication</pre>	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	<p>(Optional) <b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch# copy running-config startup-config</pre>	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。

**Caution**

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。

**Before you begin**

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。

**Procedure**

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> switch# <b>configure terminal</b> 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	<b>no aaa authentication login {console   default} fallback error local</b>  <b>Example:</b> switch(config)# <b>no aaa authentication login console fallback error local</b>	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。  <div style="background-color: #f0f0f0; padding: 5px;">□ WARNING!!! Disabling fallback can lock your switch. □</div>
ステップ 3	(Optional) <b>exit</b>  <b>Example:</b> switch(config)# <b>exit</b> switch#	設定モードを終了します。
ステップ 4	(Optional) <b>show aaa authentication</b>  <b>Example:</b> switch# <b>show aaa authentication</b>	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。

	Command or Action	Purpose
ステップ 5	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> switch# <b>copy running-config startup-config</b>	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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> switch# <b>configure terminal</b> 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	<b>aaa user default-role</b>  <b>Example:</b> switch(config)# <b>aaa user default-role</b>	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 <b>no</b> 形式を使用します。
ステップ 3	<b>exit</b>  <b>Example:</b> switch(config)# <b>exit</b> switch#	設定モードを終了します。
ステップ 4	(Optional) <b>show aaa user default-role</b>  <b>Example:</b> switch# <b>show aaa user default-role</b>	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	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> switch# <b>copy running-config startup-config</b>	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.
```

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> switch# <b>configure terminal</b> 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	<b>aaa authentication login error-enable</b> <b>Example:</b> switch(config)# <b>aaa authentication login error-enable</b>	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	<b>exit</b> <b>Example:</b> switch(config)# <b>exit</b> switch#	設定モードを終了します。
ステップ 4	(Optional) <b>show aaa authentication</b> <b>Example:</b> switch# <b>show aaa authentication</b>	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	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch# <b>copy running-config startup-config</b>	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。

## 成功および失敗したログイン試行のロギング

成功および失敗したすべてのログイン試行のログを、設定済みのsyslogサーバへ記録するようにスイッチを設定できます。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 : <pre>switch# configure terminal</pre>	グローバル 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	必須: <b>[no] login on-failure log</b> 例 : <pre>switch(config)# login on-failure log</pre>	<p>ロギング レベルが 6 に設定されている場合のみ、失敗した認証に関するすべてのメッセージを設定済みの syslog サーバに記録します。この設定では、次の syslog メッセージが失敗したログインの後に表示されます。</p> <p>「AUTHPRIV-3-SYSTEM_MSG: pam_aaa:Authentication failed for user admin from 172.22.00.00」</p> <p>(注) ログ レベルで authpriv を 6 とした場合、前述のメッセージと併せて追加の Linux カーネル認証メッセージも表示されます。これらの追加メッセージを無視させたい場合は、authpriv 値を 3 に設定する必要があります。</p>
ステップ 3	必須: <b>[no] login on-success log</b> 例 : <pre>switch(config)# login on-success log switch(config)# logging level authpriv 6 switch(config)# logging level daemon 6</pre>	<p>ロギング レベルが 6 に設定されている場合のみ、成功した認証に関するすべてのメッセージを設定済みの syslog サーバに記録します。この設定では、次の syslog メッセージが成功したログインの後に表示されます。</p> <p>「AUTHPRIV-6-SYSTEM_MSG: pam_aaa:Authentication success for user admin from 172.22.00.00」</p> <p>(注) ログ レベルで authpriv を 6 とした場合、前述のメッセージと併せて追加の Linux カーネル認証メッセージも表示されます。これらの追加メッセージを無視させたい場合は、authpriv 値を 3 に設定する必要があります。</p>

	コマンドまたはアクション	目的
ステップ 4	(任意) <b>show login on-failure log</b> 例： switch(config)# <b>show login on-failure log</b>	ログイン認証失敗メッセージを syslog サーバのログに記録するよう、スイッチが設定されているかを表示します。
ステップ 5	(任意) <b>show login on-successful log</b> 例： switch(config)# <b>show login on-successful log</b>	ログイン認証成功メッセージを syslog サーバのログに記録するよう、スイッチが設定されているかを表示します。
ステップ 6	(任意) <b>copy running-config startup-config</b> 例： switch(config)# <b>copy running-config startup-config</b>	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イク認証プロトコル (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+) を通じて、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) 認証を使用します。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。



### Note

Cisco Nexus 9K シリーズ スイッチは、TACAAS+ に対してのみ CLI コマンド `aaa authentication login ascii-authentication` をサポートしますが、RADIUS に対してはサポートしません。デフォルト認証である PAP が有効になるように、`aaa authentication login ascii-authentication` スイッチが無効になっていることを確認します。そうしないと、syslog エラーが表示されます。次に例を示します。

```
2017 Jun 14 16:14:15 N9K-1 %RADIUS-2-RADIUS_NO_AUTHEN_INFO: ASCII authentication not supported
2017 Jun 14 16:14:16 N9K-1 %AUTHPRIV-3-SYSTEM_MSG: pam_aaa:Authentication failed from 192.168.12.34 - dcos_sshd[16804]
```

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

Table 6: 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。

### Before you begin

ログイン用の AAA ASCII 認証をディセーブルにします。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> switch# <b>configure terminal</b> 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	<b>no aaa authentication login ascii-authentication</b> <b>Example:</b> switch(config)# <b>no aaa authentication login ascii-authentication</b>	ASCII 認証をディセーブルにします。
ステップ 3	<b>aaa authentication login chap enable</b> <b>Example:</b> switch(config)# <b>aaa authentication login chap enable</b>	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。 <b>Note</b> 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	(Optional) <b>exit</b> <b>Example:</b> switch(config)# <b>exit</b> switch#	設定モードを終了します。

	Command or Action	Purpose
ステップ 5	(Optional) <b>show aaa authentication login chap</b>  <b>Example:</b> switch# <b>show aaa authentication login chap</b>	CHAP の設定を表示します。
ステップ 6	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> switch# <b>copy running-config startup-config</b>	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イク認証プロトコル (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 Version 2 (MSCHAP V2) にも対応しています。リモート認証サーバ (RADIUS または TACACS+) を通じて、Cisco NX-OS スイッチ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。



**Note** Cisco NX-OS ソフトウェアは、次のメッセージを表示する場合があります。

「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) 認証を使用します。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。

Table 7. 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。

### Before you begin

ログイン用の AAA ASCII 認証をディセーブルにします。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> switch# <b>configure terminal</b> 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	<b>no aaa authentication login ascii-authentication</b> <b>Example:</b> switch(config)# <b>no aaa authentication login ascii-authentication</b>	ASCII 認証をディセーブルにします。
ステップ 3	<b>aaa authentication login {mschap   mschapv2} enable</b> <b>Example:</b> switch(config)# <b>aaa authentication login mschap enable</b>	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。 <b>Note</b> 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	<b>exit</b> <b>Example:</b>	設定モードを終了します。

	Command or Action	Purpose
	switch(config)# <b>exit</b> switch#	
ステップ 5	(Optional) <b>show aaa authentication login</b> <b>{mschap   mschapv2}</b>  <b>Example:</b> switch# <b>show aaa authentication login</b> <b>mschap</b>	MSCHAP または MSCHAP V2 の設定を表示します。
ステップ 6	(Optional) <b>copy running-config</b> <b>startup-config</b>  <b>Example:</b> switch# <b>copy running-config</b> <b>startup-config</b>	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 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+ 方式と RADIUS 方式をサポートします。Cisco NX-OS デバイスは、ユーザ 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+ セキュリティ サーバまたは RADIUS セキュリティ サーバに報告します。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 レコードとして報告します。そのアカウンティング レコードは、セキュリティ サーバ上のアカウンティング ログに格納されます。

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。



#### Note

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。

### Before you begin

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

## Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	コンフィギュレーションモードに入ります。
ステップ 2	<b>aaa accounting default {group group-list   local}</b> <b>Example:</b> <pre>switch(config)# aaa accounting default group radius</pre>	デフォルトのアカウント方式を設定します。  <i>group-list</i> 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。 <ul style="list-style-type: none"> <li>• <b>radiusRADIUS</b> サーバのグローバルプールを使用してアカウントを行います。</li> <li>• <b>named-group</b> : 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トに使用されます。</li> </ul> <b>local</b> 方式はローカルデータベースを使用してアカウントを行います。  デフォルトのアカウント方式は、 <b>local</b> 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	<b>exit</b> <b>Example:</b> <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 4	(Optional) <b>show aaa accounting</b> <b>Example:</b> <pre>switch# show aaa accounting</pre>	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	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch# copy running-config startup-config</pre>	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 サーバ上での Cisco NX-OS 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 デバイスでの認証に RADIUS サーバを使用する場合は、許可情報などのユーザ属性を認証結果とともに返すように、RADIUS サーバに RADIUS プロトコルで指示します。この許可情報は、VSA で指定されます。

### VSA の形式

次の VSA プロトコル オプションが、Cisco NX-OS ソフトウェアでサポートされています。

#### 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。

#### roles

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 `network-admin` のロールに属している場合、値フィールドは `network-operator network-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 network-admin
```

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

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



**Note** VSA を、`shell:roles*"network-operator network-admin"` または `"shell:roles*\"network-operator network-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 サーバで VSA `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 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 ログイン機能の設定

### ログインパラメータの設定

ログインパラメータの設定では、サービス妨害 (DoS) 攻撃の可能性が検出された場合に、以降のログイン試行を自動的にブロックさせる、あるいは接続試行の失敗が複数検出された場合に、辞書攻撃の進行をスローダウンさせるため強制的に待機モードに入らせることができます。



(注) システムのスイッチオーバーが発生するか、または AAA プロセスが再起動した場合、この機能は再起動します。



(注) **login block-for** および **login quiet-mode** コンフィギュレーションモードコマンドは、それぞれ **system login block-for** および **system login quiet-mode** に名前が変更されました。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# <b>configure terminal</b>	グローバル 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	<b>[no] system login block-for seconds attempts tries within seconds</b> 例： switch(config)# <b>system login block-for 100 attempts 2 within 60</b>	待機モードの期間を設定します。すべての引数の範囲は 1 ~ 65535 です。  この例では、60 秒以内に 2 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しています。  このコマンドを入力すると、Telnet または SSH を経由したログイン試行は、待機モード中にすべて拒否されます。アクセス コントロール リスト (ACL) も、 <b>system</b> コマンドが入力されない限り、待機時間から除外されません。  (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入力する必要があります。
ステップ 3	(任意) <b>[no] system login quiet-mode access-class acl-name</b> 例： switch(config)# <b>system login quiet-mode access-class myacl</b>	待機モードに切り替わるときに、スイッチに適用される ACL を指定します。スイッチが待機モードにある場合、すべてのログイン要求が拒否され、使用可能な接続はコンソールを経由したものだけになります。
ステップ 4	(任意) <b>show system login [failures]</b> 例： switch(config)# <b>show system login</b>	ログイン パラメータを表示します。 <b>failures</b> オプションは、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。
ステップ 5	(任意) <b>copy running-config startup-config</b> 例：	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
	<code>switch(config)# copy running-config startup-config</code>	

## ユーザ ログインセッションの制限

ユーザあたりの同時ログインセッションの最大数を制限できます。これは複数の不要なセッションをユーザに与えることを防止し、不正ユーザによる有効な SSH または Telnet セッションへのアクセスという潜在的なセキュリティ問題を解消します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： <code>switch# configure terminal</code>	グローバル 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	<b>[no] user max-logins max-logins</b> 例： <code>switch(config)# user max-logins 1</code>	ユーザあたりの同時ログインセッションの最大数を制限します。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、ユーザあたりに割り当てられる Telnet または SSH セッションは 1 つだけになります。  (注) 設定されたログインの制限は、すべてのユーザに適用されます。個々のユーザごとに異なる制限を設定することはできません。
ステップ 3	(任意) <b>show running-config all   i max-login</b> 例： <code>switch(config)# show running-config all   i max-login</code>	ユーザごとに許可されたログインセッションの最大数を表示します。
ステップ 4	(任意) <b>copy running-config startup-config</b> 例： <code>switch(config)# copy running-config startup-config</code>	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。

## パスワードの長さの制限

ユーザパスワードの最小および最大の長さを制限できます。この機能を使用して、ユーザに強力なパスワードを入力するように強制することでシステムのセキュリティを高めることができます。

### 始める前に

**password strength-check** コマンドを使用して、パスワードの強度の確認をイネーブルにする必要があります。パスワードの長さは制限しているがパスワードの強度の確認はイネーブルにしていない場合、制限長を超えたパスワードをユーザが入力すると、エラーは表示されますが、ユーザアカウントは作成されます。パスワード長を強制的に適用させてこうしたユーザアカウントの作成を防ぐには、パスワードの強度の確認をイネーブルにしてパスワードの長さを制限する必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： <code>switch# configure terminal</code>	グローバル 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	<b>[no] userpassphrase {min-length min-length   max-length max-length}</b> 例： <code>switch(config)# userpassphrase min-length 8 max-length 80</code>	ユーザパスワードの最小または最大の長さを制限します。パスワードの最小長は 4～127 文字であり、パスワードの最大長さは 80～127 文字です。
ステップ 3	(任意) <b>show userpassphrase {length   max-length   min-length}</b> 例： <code>switch(config)# show userpassphrase length</code>	ユーザパスワードの最小および最大の長さが表示されます。
ステップ 4	(任意) <b>copy running-config startup-config</b> 例： <code>switch(config)# copy running-config startup-config</code>	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。

## ユーザ名のパスワード プロンプトのイネーブル化

ユーザによるユーザ名入力後にパスワード入力を要求するように、スイッチを設定できます。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# <b>configure terminal</b>	グローバル 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	<b>password prompt username</b> 例： switch(config)# <b>password prompt username</b> Password prompt username is enabled. After providing the required options in the username command, press enter. User will be prompted for the username password and password will be hidden. Note: Choosing password key in the same line while configuring user account, password will not be hidden.	<b>password</b> オプションを付けずに <b>username</b> コマンドまたは <b>snmp-server user</b> コマンドが入力された後に、ユーザに対してパスワード入力要求のプロンプトを表示するようスイッチを設定します。ユーザが入力したパスワードは非表示にされます。この機能をディセーブルにするには、このコマンドの <b>no</b> 形式を使用します。
ステップ 3	(任意) <b>copy running-config startup-config</b> 例： switch(config)# <b>copy running-config startup-config</b>	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 または TACACS+ の共有秘密の設定

スイッチと RADIUS または TACACS+ サーバ間のアカウントing およびリモート認証用に設定する共有秘密は、機密情報であるため隠しておく必要があります。これらの暗号化された共有秘密の生成には、**radius-server [host] key** および **tacacs-server [host] key** コマンドをそれぞれ使用します。暗号化された共有秘密の保存には SHA256 ハッシュ メソッドが使用されます。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# <b>configure terminal</b>	グローバル 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	<b>generate type7_encrypted_secret</b> 例： switch(config)# <b>generate type7_encrypted_secret</b> Type-7 (Vigenere) Encryption, Use this encrypted secret to configure radius and tacacs shared secret with key type 7. Copy complete secret with double	RADIUS または TACACS+ 共有秘密をキー タイプ 7 で設定します。共有秘密をプレーンテキストで 2 回入力するよう求められます。秘密情報は、入力時に非表示にされます。その後、暗号化されたバージョンの秘密情報が表示されま

	コマンドまたはアクション	目的
	quotes.  Enter plain text secret: Confirm plain text secret: Type 7 Encrypted secret is : "fewhg"	(注) プレーン テキストの秘密情報の暗号化バージョンを別途生成しておき、その後で暗号化された共有秘密を設定することができます。その際には、 <b>radius-server [host] key</b> および <b>tacacs-server [host] key</b> を使用します コマンドを使用します。
ステップ 3	(任意) <b>copy running-config startup-config</b>  例 :  switch(config)# <b>copy running-config startup-config</b>	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 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 アクティビティのローカル ログを保持しています。このログはモニタリングしたりクリアしたりできます。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>show accounting log</b> [ <i>size</i>   <b>last-index</b>   <b>start-seqnum</b> <i>number</i>   <b>start-time</b> <i>year month day hh:mm:ss</i> ]  <b>Example:</b>  switch# <b>show accounting log</b>	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、 <i>size</i> 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、 <b>last-index</b> キーワードを使用します。
ステップ 2	(Optional) <b>clear accounting log</b> [ <b>logflash</b> ]  <b>Example:</b>	アカウンティング ログの内容をクリアします。 <b>logflash</b> キーワードはログフ

	Command or Action	Purpose
	switch# clear aaa accounting log	ラッシュに保存されているアカウントティング 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
<b>show aaa accounting</b>	AAA アカウンティングの設定を表示します。
<b>show aaa authentication [login {ascii-authentication   chap   error-enable   mschap   mschapv2}]</b>	AAA 認証ログイン設定情報を表示します。
<b>show aaa groups</b>	AAA サーバグループの設定を表示します。
<b>show login [failures]</b>	ログインパラメータを表示します。 <b>failures</b> オプションは、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。  <b>Note</b> <b>clear login failures</b> コマンドは、現在の監視期間内のログイン失敗をクリアします。
<b>show login on-failure log</b>	ログイン認証失敗メッセージを syslog サーバのログに記録するよう、スイッチが設定されているかを表示します。
<b>show login on-successful log</b>	ログイン認証成功メッセージを syslog サーバのログに記録するよう、スイッチが設定されているかを表示します。
<b>show running-config aaa [all]</b>	実行コンフィギュレーションの AAA 設定を表示します。
<b>show running-config all   i max-login</b>	ユーザごとに許可されたログインセッションの最大数を表示します。



コマンド	目的
<b>show startup-config aaa</b>	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。
<b>show userpassphrase {length   max-length   min-length}</b>	ユーザ パスワードの最小および最大の長さが表示されます。

## 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
```

## ログインパラメータの設定例

次に、60 秒以内に 3 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。この例は、ログインの失敗を示しません。

```
switch# configure terminal
switch(config)# login block-for 100 attempts 3 within 60
switch(config)# 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 3 login failures occur in 60 seconds or less,
logins will be disabled for 100 seconds.
```

```
Switch presently in Normal-Mode.
Current Watch Window remaining time 45 seconds.
Present login failure count 0.
```

```
switch(config)# show login failures
*** No logged failed login attempts with the device.***
```

以下に、待機モード ACL の設定例を示します。待機時間中、myacl の ACL 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。この例は、ログインの失敗も示します。

```
switch# configure terminal
switch(config)# login block-for 100 attempts 3 within 60
switch(config)# login quiet-mode access-class myacl
```

```
switch(config)# show login
```

```
Switch is enabled to watch for login Attacks.
If more than 3 login failures occur in 60 seconds or less,
```

```
logins will be disabled for 100 seconds.
```

```
Switch presently in Quiet-Mode.
Will remain in Quiet-Mode for 98 seconds.
Denying logins from all sources.
```

```
switch(config)# show login failures
Information about last 20 login failure's with the device.
```

```
-----
Username          Line           SourceIPAddr    Appname         TimeStamp
-----
asd               /dev/pts/0    171.70.55.158  login          Mon Aug  3 18:18:54 2015
qweq              /dev/pts/0    171.70.55.158  login          Mon Aug  3 18:19:02 2015
qwe               /dev/pts/0    171.70.55.158  login          Mon Aug  3 18:19:08 2015
-----
```

## パスワードプロンプト機能の設定例

次の例では、**username** コマンド入力後にユーザパスワード入力要求のプロンプトを表示し、パスワードが入力されなかった場合にはエラーメッセージを表示するようスイッチを設定する方法を示します。

```
switch# configure terminal
switch(config)# password prompt username
Password prompt username is enabled.
After providing the required options in the username command, press enter.
User will be prompted for the username password and password will be hidden.
Note: Choosing password key in the same line while configuring user account, password
will not be hidden.
```

```
switch(config)# username user1
Enter password:
Confirm password:
warning: password for user:user1 not set. S/he may not be able to login
```

次の例では、**snmp-server user** コマンド入力後にユーザパスワード入力要求のプロンプトを表示し、その後、ユーザに提示するプロンプトを表示するようにスイッチを設定する方法を示します。

```
switch# configure terminal
switch(config)# password prompt username
Password prompt username is enabled.
After providing the required options in the username command, press enter.
User will be prompted for the username password and password will be hidden.
Note: Choosing password key in the same line while configuring user account, password
will not be hidden.
```

```
N9K-1(config)# snmp-server user user1
Enter auth md5 password (Press Enter to Skip):
Enter auth sha password (Press Enter to Skip):
```

## 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 のライセンス	<i>Cisco NX-OS</i> ライセンス ガイド

### 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
AAA に関連する MIB	サポートされている 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。 <a href="ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html">ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html</a>





## 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。

- [RADIUS について, on page 57](#)
- [RADIUS 認可変更について \(61 ページ\)](#)
- [RADIUS の前提条件, on page 62](#)
- [RADIUS の注意事項と制約事項 \(62 ページ\)](#)
- [RADIUS の認可変更の注意事項と制約事項 \(63 ページ\)](#)
- [RADIUS のデフォルト設定, on page 63](#)
- [RADIUS サーバの設定, on page 63](#)
- [Dynamic Author Server の有効化または無効化 \(83 ページ\)](#)
- [RADIUS 認可変更の設定 \(83 ページ\)](#)
- [RADIUS 設定の確認, on page 84](#)
- [RADIUS 認可変更の設定の検証 \(84 ページ\)](#)
- [RADIUS サーバのモニタリング, on page 85](#)
- [RADIUS サーバ統計情報のクリア, on page 86](#)
- [RADIUS の設定例, on page 86](#)
- [RADIUS 認可変更の設定例 \(86 ページ\)](#)
- [次の作業, on page 87](#)
- [RADIUS に関する追加情報, on page 87](#)

## RADIUS について

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 デバイスで稼働し、すべてのユーザ認証情報およびネットワークサービスアクセス情報が格納された中央の RADIUS サーバに認証要求およびアカウントング要求を送信します。

## 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 を使用した 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設定できます。ユーザごとのプロファイルにより、Cisco NX-OS デバイスは、既存の RADIUS ソリューションを使用してポートを容易に管理できると同時に、共有リソースを効率的に管理してさまざまなサービス レベル契約（SLA）を提供できます。

## RADIUS の動作

ユーザが RADIUS を使用して Cisco NX-OS デバイスへのログインおよび認証を試行すると、次のプロセスが実行されます。

- 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。



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 デバイスでの認証に RADIUS サーバを使用する場合は、許可情報などのユーザ属性を認証結果とともに返すように、RADIUS サーバに RADIUS プロトコルで指示します。この許可情報は、VSA で指定されます。

次の VSA プロトコル オプションが、Cisco NX-OS ソフトウェアでサポートされています。

### 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 ソフトウェアでは、次の属性がサポートされています。

### roles

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 `network-admin` のロールに属している場合、値フィールドは `network-operator network-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 network-admin
shell:roles*"network-operator network-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 network-admin\
Cisco-AVPair = shell:roles*\network-operator network-admin\
```



**Note** VSA を、`shell:roles*"network-operator network-admin"` または `"shell:roles*\network-operator network-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 認可変更について

標準 RADIUS インターフェイスは通常、ネットワークに接続しているデバイスから要求が送信され、クエリが送信されたサーバが応答するプルモデルで使用されます。Cisco NX-OS ソフトウェアは、プッシュモデルで使用される RFC 5176 で定義された RADIUS Change of Authorization (CoA) 要求をサポートしています。このモデルでは、要求は外部サーバからネットワークに接続されたデバイスへ発信され、外部の認証、認可、およびアカウンティング (AAA) またはポリシー サーバからの動的なセッション再設定が可能になります。

Dot1x が有効の場合、ネットワーク デバイスはオーセンティケータとして機能し、セッションごとのダイナミック COA を処理します。

次の要求がサポートされています。

- セッション再認証
- セッションの終了

## セッション再認証

セッション認証を開始するために、認証、許可、アカウンティング (AAA) サーバは、Cisco VSA と 1 つ以上のセッション ID 属性を含む標準 CoA 要求メッセージを送信します。Cisco VSA は、Cisco:Avpair="subscriber:command=reauthenticate" の形式です。

次のシナリオでは、現在のセッション状態によって、メッセージに対するデバイスの応答が決まります。

- セッションが現在、IEEE 802.1x によって認証されている場合、デバイスは Extensible Authentication Protocol over LAN (EAPoL) -RequestId メッセージをサーバに送信することで応答します。
- セッションが現在 MAC 認証バイパス (MAB) によって認証されている場合、デバイスはアクセス要求をサーバに送信し、最初に成功した認証で使ったのと同じ ID 属性を渡します。
- デバイスがコマンドを受信した際にセッション認証が実行中である場合は、デバイスはプロセスを終了し、認証シーケンスを再開し、最初に試行されるように設定された方式で開始します。

## セッションの終了

CoA 接続解除要求は、ホストポートをディセーブルにせずにセッションを終了します。CoA 接続解除要求終了によって、指定したホストのオーセンティケータステートマシンが再初期化されますが、ホストのネットワークへのアクセスは制限されません。

セッションが見つからない場合、デバイスは「Session Context Not Found」エラーコード属性を使用して Disconnect-NAK メッセージを返します。

セッションが見つかったが、何らかの内部エラーのためにNASがセッションを削除できなかった場合、デバイスは「Session Context Not Removable」エラーコード属性を持つ Disconnect-NAK メッセージを返します。

セッションが見つかった場合、デバイスはセッションを終了します。セッションが完全に削除されると、デバイスは Disconnect-ACK メッセージを返します。

## 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 IPv6 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。

## 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 デバイスに設定できる RADIUS サーバの最大数は 64 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。
- 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。
- N9K-X9636C-R および N9K-X9636Q-R ラインカードおよび N9K-C9508-FM-R ファブリックモジュールの場合、特殊文字を含むユーザ名の RADIUS 認証は失敗します。
- Cisco Nexus 9K シリーズスイッチは、TACAAS+ に対してのみ CLI コマンド `aaa authentication login ascii-authentication` をサポートしますが、RADIUS に対してはサポートしません。デフォルト認証である PAP が有効になるように、`aaa authentication login ascii-authentication` スイッチが無効になっていることを確認します。そうしないと、syslog エラーが表示されません。

## RADIUS の認可変更の注意事項と制約事項

RADIUS の認可変更に関する注意事項と制約事項は次のとおりです。

- RADIUS の認可変更は FEX によりサポートされています。
- RADIUS の認可変更は VXLAN EVPN によりサポートされています。

## 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。

**Table 8: 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	認証とアカウントिंग
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
アカウントिंग 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。



### Note

Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。



**Note** Cisco Nexus 9K シリーズ スイッチは、TACAAS+ に対してのみ CLI コマンド `aaa authentication login ascii-authentication` をサポートしますが、RADIUS に対してはサポートしません。デフォルト認証である PAP が有効になるように、`aaa authentication login ascii-authentication` スイッチが無効になっていることを確認します。そうしないと、`syslog` エラーが表示されます。

## RADIUS サーバの設定プロセス

1. Cisco NX-OS デバイスと RADIUS サーバとの接続を確立します。
2. RADIUS サーバの RADIUS 秘密キーを設定します。
3. 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。
4. 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
5. (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。

### Related Topics

[RADIUS サーバホストの設定](#) (64 ページ)

[グローバル RADIUS キーの設定](#) (66 ページ)

## 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。



**Note** 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。

### Before you begin

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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> switch# <b>configure terminal</b> 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	<b>radius-server host</b> { <i>ipv4-address</i>   <i>ipv6-address</i>   <i>hostname</i> } <b>Example:</b> switch(config)# <b>radius-server host</b> 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	(Optional) <b>show radius</b> { <b>pending</b>   <b>pending-diff</b> } <b>Example:</b> switch(config)# <b>show radius pending</b>	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	(Optional) <b>radius commit</b> <b>Example:</b> switch(config)# <b>radius commit</b>	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 に適用します。
ステップ 5	<b>exit</b> <b>Example:</b> switch(config)# <b>exit</b> switch#	設定モードを終了します。
ステップ 6	(Optional) <b>show radius-server</b> <b>Example:</b> switch# <b>show radius-server</b>	RADIUS サーバの設定を表示します。
ステップ 7	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch# <b>copy running-config startup-config</b>	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。

### Related Topics

[特定の RADIUS サーバ用のキーの設定](#) (67 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 キーとは、Cisco NX-OS デバイスと TACACS+ サーバ ホスト間の共有秘密テキストストリングです。

### Before you begin

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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>radius-server key [0   6   7] key-value</b> <b>Example:</b> <pre>switch(config)# radius-server key 0 QsEfThUkO</pre> <b>Example:</b> <pre>switch(config)# radius-server key 7 "fewhg"</pre>	<p>すべての RADIUS サーバ用の RADIUS キーを指定します。 <i>key-value</i> 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) 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。</p> <p>デフォルトでは、RADIUS キーは設定されません。</p> <p><b>Note</b>     <b>generate type7_encrypted_secret</b> を使用してすでに共有秘密を設定している場合 2 番目の例のように引用符で囲んで入力してください。詳細については、<a href="#">RADIUS または TACACS+ の共有秘密の設定, on page 50</a>を参照してください。</p>
ステップ 3	<b>exit</b> <b>Example:</b> <pre>switch(config)# exit switch#</pre>	設定モードを終了します。

	Command or Action	Purpose
ステップ 4	(Optional) <b>show radius-server</b>  <b>Example:</b> switch# <b>show radius-server</b>	RADIUS サーバの設定を表示します。  <b>Note</b> 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、 <b>show running-config</b> コマンドを使用します。
ステップ 5	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> switch# <b>copy running-config startup-config</b>	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。

**Related Topics**

[RADIUS サーバ グループの設定 \(69 ページ\)](#)

[AES パスワード暗号化およびプライマリ暗号キーについて \(543 ページ\)](#)

## 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。

**Before you begin**

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。

**Procedure**

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> switch# <b>configure terminal</b> 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	<b>radius-server host</b> { <i>ipv4-address</i>   <i>ipv6-address</i>   <i>hostname</i> } <b>key</b> [0   6   7] <i>key-value</i>  <b>Example:</b>	特定の RADIUS サーバ用の RADIUS キーを指定します。 <i>key-value</i> 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)

	Command or Action	Purpose
	<pre>switch(config)# radius-server host 10.10.1.1 key 0 PlIjUhYg</pre> <p><b>Example:</b></p> <pre>switch(config)# radius-server host 10.10.1.1 key 7 "fewhg"</pre>	<p>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。</p> <p>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。</p> <p><b>Note</b>     <b>generate type7_encrypted_secret</b> を使用してすでに共有秘密を設定している場合 2 番目の例のように引用符で囲んで入力してください。詳細については、<a href="#">RADIUS または TACACS+ の共有秘密の設定, on page 50</a>を参照してください。</p>
ステップ 3	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 4	<p>(Optional) <b>show radius-server</b></p> <p><b>Example:</b></p> <pre>switch# show radius-server</pre>	<p>RADIUS サーバの設定を表示します。</p> <p><b>Note</b>     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、<b>show running-config</b> コマンドを使用します。</p>
ステップ 5	<p>(Optional) <b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch# copy running-config startup-config</pre>	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。

### Related Topics

[RADIUS サーバホストの設定](#) (64 ページ)

[AES パスワード暗号化およびプライマリ暗号キーについて](#) (543 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。

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。

### Before you begin

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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>aaa group server radius group-name</b> <b>Example:</b> <pre>switch(config)# aaa group server radius RadServer switch(config-radius)#</pre>	<p>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。 <i>group-name</i> 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。</p> <p>RADIUS サーバグループを削除するには、このコマンドの <b>no</b> 形式を使用します。</p> <p><b>Note</b> デフォルトのシステム生成デフォルトグループ (RADIUS) は削除できません。</p>
ステップ 3	<b>server {ipv4-address   ipv6-address   hostname}</b> <b>Example:</b> <pre>switch(config-radius)# server 10.10.1.1</pre>	<p>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。</p> <p>指定した RADIUS サーバが見つからない場合は、<b>radius-server host</b> 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。</p>
ステップ 4	<b>(Optional) deadtime minutes</b> <b>Example:</b> <pre>switch(config-radius)# deadtime 30</pre>	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。

	Command or Action	Purpose
		<p><b>Note</b> 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。</p>
ステップ 5	<p>(Optional) <b>server</b> {<i>ipv4-address</i>   <i>ipv6-address</i>   <i>hostname</i>}</p> <p><b>Example:</b> switch(config-radius)# <b>server</b> 10.10.1.1</p>	<p>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。</p> <p><b>Tip</b> 指定した RADIUS サーバが見つからない場合は、<b>radius-server host</b> 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。</p>
ステップ 6	<p>(Optional) <b>use-vrf</b> <i>vrf-name</i></p> <p><b>Example:</b> switch(config-radius)# <b>use-vrf</b> vrf1</p>	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	<p><b>exit</b></p> <p><b>Example:</b> switch(config-radius)# <b>exit</b> switch(config)#</p>	設定モードを終了します。
ステップ 8	<p>(Optional) <b>show radius-server groups</b> [<i>group-name</i>]</p> <p><b>Example:</b> switch(config)# <b>show radius-server groups</b></p>	RADIUS サーバグループの設定を表示します。
ステップ 9	<p>(Optional) <b>copy running-config startup-config</b></p> <p><b>Example:</b> switch(config)# <b>copy running-config startup-config</b></p>	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。

### Related Topics

[RADIUS デッドタイム間隔の設定 \(80 ページ\)](#)

## 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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> switch# <b>configure terminal</b> 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	<b>ip radius source-interface interface</b> <b>Example:</b> switch(config)# <b>ip radius source-interface mgmt 0</b>	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	<b>exit</b> <b>Example:</b> switch(config)# <b>exit</b> switch#	設定モードを終了します。
ステップ 4	(Optional) <b>show radius-server</b> <b>Example:</b> switch# <b>show radius-server</b>	RADIUS サーバの設定情報を表示します。
ステップ 5	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch# <b>copy running-config startup-config</b>	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。

### Related Topics

[RADIUS サーバグループの設定 \(69 ページ\)](#)

## 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の AAA 認証方式に基づいて認証要求を転送します。VRF と認証要求送信先 RADIUS サーバをユーザが指定できるように Cisco NX-OS デバイスを設定するには、`directed-request` オプションをイネーブルにします。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。



**Note** `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。



**Note** 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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <code>switch# configure terminal</code> <code>switch(config)#</code>	グローバル 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	<b>radius-server directed-request</b> <b>Example:</b> <code>switch(config)# radius-server directed-request</code>	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	(Optional) <b>show radius {pending   pending-diff}</b> <b>Example:</b> <code>switch(config)# show radius pending</code>	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	(Optional) <b>radius commit</b> <b>Example:</b> <code>switch(config)# radius commit</code>	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ます。
ステップ 5	<b>exit</b> <b>Example:</b> <code>switch(config)# exit</code> <code>switch#</code>	設定モードを終了します。
ステップ 6	(Optional) <b>show radius-server directed-request</b> <b>Example:</b> <code>switch# show radius-server directed-request</code>	<code>directed request</code> の設定を表示します。

	Command or Action	Purpose
ステップ 7	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch# copy running-config startup-config</pre>	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 デバイスはローカル認証に戻す前に、RADIUS サーバへの送信を 1 回だけ再試行します。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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グ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	<b>radius-server retransmit count</b>  <b>Example:</b> <pre>switch(config)# radius-server retransmit 3</pre>	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	<b>radius-server timeout seconds</b>  <b>Example:</b> <pre>switch(config)# radius-server timeout 10</pre>	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	(Optional) <b>show radius {pending   pending-diff}</b>  <b>Example:</b> <pre>switch(config)# show radius pending</pre>	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	(Optional) <b>radius commit</b>  <b>Example:</b> <pre>switch(config)# radius commit</pre>	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ます。
ステップ 6	<b>exit</b>  <b>Example:</b>	設定モードを終了します。

	Command or Action	Purpose
	<code>switch(config)# exit</code> <code>switch#</code>	
ステップ 7	(Optional) <b>show radius-server</b>  <b>Example:</b> <code>switch# show radius-server</code>	RADIUS サーバの設定を表示します。
ステップ 8	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <code>switch# copy running-config startup-config</code>	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。

## 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 デバイスはローカル認証に戻す前に、RADIUS サーバへの送信を 1 回だけ再試行します。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、タイムアウトエラーを宣言する前に、RADIUS サーバからの応答を待機するタイムアウト間隔も設定できます。

### Before you begin

1 つまたは複数の RADIUS サーバホストを設定します。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> <code>switch# configure terminal</code> <code>switch(config)#</code>	グ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	<b>radius-server host</b> { <i>ipv4-address</i>   <i>ipv6-address</i>   <i>hostname</i> } <b>retransmit count</b>  <b>Example:</b> <code>switch(config)# radius-server host server1 retransmit 3</code>	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。  <b>Note</b> 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	<b>radius-server host</b> { <i>ipv4-address</i>   <i>ipv6-address</i>   <i>hostname</i> } <b>timeout seconds</b>  <b>Example:</b>	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。

	Command or Action	Purpose
	<code>switch(config)# radius-server host server1 timeout 10</code>	<b>Note</b> 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	(Optional) <code>show radius {pending   pending-diff}</code> <b>Example:</b> <code>switch(config)# show radius pending</code>	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	(Optional) <code>radius commit</code> <b>Example:</b> <code>switch(config)# radius commit</code>	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、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、RADIUS 設定を他の Cisco NX-OS デバイスに配布します。
ステップ 6	<code>exit</code> <b>Example:</b> <code>switch(config)# exit switch#</code>	設定モードを終了します。
ステップ 7	(Optional) <code>show radius-server</code> <b>Example:</b> <code>switch# show radius-server</code>	RADIUS サーバの設定を表示します。
ステップ 8	(Optional) <code>copy running-config startup-config</code> <b>Example:</b> <code>switch# copy running-config startup-config</code>	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。

**Related Topics**

[RADIUS サーバホストの設定 \(64 ページ\)](#)

## RADIUS サーバのアカウントिंगおよび認証属性の設定

RADIUS サーバをアカウントング専用、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 サーバはアカウント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 アカウント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。

**Before you begin**

1 つまたは複数の RADIUS サーバ ホストを設定します。

**Procedure**

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> switch# <b>configure terminal</b> 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	(Optional) <b>radius-server host</b> { <i>ipv4-address</i>   <i>ipv6-address</i>   <i>hostname</i> } <b>acct-port</b> <i>udp-port</i>  <b>Example:</b> switch(config)# <b>radius-server host</b> 10.10.1.1 <b>acct-port</b> 2004	RADIUS アカウントिंग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。
ステップ 3	(Optional) <b>radius-server host</b> { <i>ipv4-address</i>   <i>ipv6-address</i>   <i>hostname</i> } <b>accounting</b>  <b>Example:</b> switch(config)# <b>radius-server host</b> 10.10.1.1 <b>accounting</b>	RADIUS サーバをアカウントिंगだけに使用することを指定します。デフォルトでは、アカウントINGと認証の両方に使用されます。
ステップ 4	(Optional) <b>radius-server host</b> { <i>ipv4-address</i>   <i>ipv6-address</i>   <i>hostname</i> } <b>auth-port</b> <i>udp-port</i>  <b>Example:</b> switch(config)# <b>radius-server host</b> 10.10.2.2 <b>auth-port</b> 2005	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	(Optional) <b>radius-server host</b> { <i>ipv4-address</i>   <i>ipv6-address</i>   <i>hostname</i> } <b>authentication</b>  <b>Example:</b> switch(config)# <b>radius-server host</b> 10.10.2.2 <b>authentication</b>	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、アカウントINGと認証の両方に使用されます。
ステップ 6	(Optional) <b>show radius</b> { <b>pending</b>   <b>pending-diff</b> }  <b>Example:</b> switch(config)# <b>show radius pending</b>	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	(Optional) <b>radius commit</b>  <b>Example:</b> switch(config)# <b>radius commit</b>	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ます。



	Command or Action	Purpose
ステップ 8	<b>exit</b> <b>Example:</b> <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 9	(Optional) <b>show radius-server</b> <b>Example:</b> <pre>switch(config)# show radius-server</pre>	RADIUS サーバの設定を表示します。
ステップ 10	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch# copy running-config startup-config</pre>	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。

#### Related Topics

[RADIUS サーバホストの設定 \(64 ページ\)](#)

## 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。



**Note** 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 サーバがどのくらいの期間要求を受信しなかった場合に、Cisco NX-OS デバイスがテストパケットを送信するかを指定します。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。



**Note** 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。



**Note** 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。

**Before you begin**

RADIUS をイネーブルにします。

**Procedure**

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>radius-server test {idle-time minutes   password password [idle-time minutes]   username name [password password [idle-time minutes]]}</b> <b>Example:</b> <pre>switch(config)# radius-server test username user1 password Ur2Gd2BH idle-time 3</pre>	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。 <b>Note</b> 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	<b>radius-server deadtime minutes</b> <b>Example:</b> <pre>switch(config)# radius-server deadtime 5</pre>	Cisco NX-OS デバイスが、前回応答しなかった RADIUS サーバをチェックするまでの時間 (分) 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	<b>exit</b> <b>Example:</b> <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 5	(Optional) <b>show radius-server</b> <b>Example:</b> <pre>switch# show radius-server</pre>	RADIUS サーバの設定を表示します。
ステップ 6	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch# copy running-config startup-config</pre>	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。

## Related Topics

[各 RADIUS サーバの定期モニタリングの設定](#) (79 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 サーバがどのくらいの期間要求を受信しなかった場合に Cisco NX-OS スイッチがテストパケットを送信するかを指定します。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。



## Note

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。



## Note

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。



## Note

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

## Before you begin

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。

## Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>radius-server host</b> { <i>ipv4-address</i>   <i>ipv6-address</i>   <i>hostname</i> } <b>test</b> { <i>idle-time minutes</i>   <b>password</b> <i>password</i> [ <i>idle-time minutes</i> ]   <b>username</b> <i>name</i> [ <b>password</b> <i>password</i> [ <i>idle-time minutes</i> ]]} <b>Example:</b>	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 <b>test</b> 、デフォルトのパスワードは <b>test</b> 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。

	Command or Action	Purpose
	<pre>switch(config)# radius-server host 10.10.1.1 test username user1 password Ur2Gd2BH idle-time 3</pre>	<b>Note</b> 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	<b>radius-server deadtime minutes</b> <b>Example:</b> <pre>switch(config)# radius-server deadtime 5</pre>	Cisco NX-OS デバイスが、前回応答しなかった RADIUS サーバをチェックするまでの時間 (分) 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	<b>exit</b> <b>Example:</b> <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 5	(Optional) <b>show radius-server</b> <b>Example:</b> <pre>switch# show radius-server</pre>	RADIUS サーバの設定を表示します。
ステップ 6	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch# copy running-config startup-config</pre>	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。

#### Related Topics

[RADIUS サーバホストの設定 \(64 ページ\)](#)

[RADIUS サーバのグローバルな定期モニタリングの設定 \(77 ページ\)](#)

## 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。デッドタイム間隔には、Cisco NX-OS デバイスが、RADIUS サーバをデッド状態であると宣言した後、そのサーバがアライブ状態に戻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間隔を指定します。デフォルト値は 0 分です。



**Note** 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、デッド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。

## Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> switch# <b>configure terminal</b> 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	<b>radius-server deadtime minutes</b> <b>Example:</b> switch(config)# <b>radius-server deadtime</b> 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	(Optional) <b>show radius {pending   pending-diff}</b> <b>Example:</b> switch(config)# <b>show radius pending</b>	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	(Optional) <b>radius commit</b> <b>Example:</b> switch(config)# <b>radius commit</b>	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ます。
ステップ 5	<b>exit</b> <b>Example:</b> switch(config)# <b>exit</b> switch#	設定モードを終了します。
ステップ 6	(Optional) <b>show radius-server</b> <b>Example:</b> switch# <b>show radius-server</b>	RADIUS サーバの設定を表示します。
ステップ 7	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch# <b>copy running-config startup-config</b>	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。

## Related Topics

[RADIUS サーバ グループの設定 \(69 ページ\)](#)

## 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。



**Note** 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。

### Before you begin

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 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。

### Procedure

	Command or Action	Purpose
ステップ 1	<pre>test aaa server radius {ipv4-address   ipv6-address   hostname} [vrf vrf-name] username password</pre> <p><b>Example:</b></p> <pre>switch# test aaa server radius 10.10.1.1 user1 Ur2Gd2BH</pre>	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	<pre>test aaa group group-name username password</pre> <p><b>Example:</b></p> <pre>switch# test aaa group RadGroup user2 As3He3CI</pre>	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。

## Dynamic Author Server の有効化または無効化

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 : switch# <b>configure terminal</b> 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	<b>aaa server radius dynamic-author</b> 例 : switch(config)# <b>aaa server radius dynamic-author</b>	RADIUS dynamic author server を有効にします。このコマンドのno形式を使用すれば、RADIUS dynamic author server を無効にできます。

## RADIUS 認可変更の設定

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 : switch# <b>configure terminal</b> 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	<b>[no] aaa server radius dynamic-author</b> 例 : switch(config)# <b>aaa server radius dynamic-author</b>	スイッチを AAA サーバとして設定し、外部ポリシー サーバとの連携を促進します。このコマンドの no 形式を使用して、RADIUS ダイナミックオーサーと、関連付けられたクライアントを無効にできます。
ステップ 3	<b>[no] client {ip-address   hostname } [server-key [0   7 ] string ]</b> 例 : switch(config-locsvr-da-radius)# client 192.168.0.5 server-key cisco1	AAA サーバクライアントの IP アドレスまたはホスト名を設定します。オプションの server-key キーワードと string 引数を使用して、クライアントレベルのサーバキーを設定します。クライアントサーバを削除するには、このコマンドの no 形式を使用します。

	コマンドまたはアクション	目的
		(注) クライアント レベルでサーバキーを設定すると、グローバルレベルで設定されたサーバキーが上書きされます。
ステップ 4	<b>[no] port <i>port-number</i></b>  例： <pre>switch(config-locsvr-da-radius)# port 3799</pre>	設定された RADIUS クライアントからの RADIUS 要求をデバイスが受信するポートを指定します。ポート範囲は1～65535です。デフォルトのポートに戻すには、このコマンドの <b>no</b> 形式を使用します。  (注) パケットオブディスコネクトのデフォルトポートは1700です。
ステップ 5	<b>[no] server-key [0   7] <i>string</i></b>	RADIUS キーをデバイスと RADIUS クライアントとの間で共有されるように設定します。サーバキーを削除するには、このコマンドの <b>no</b> 形式を使用します。

## 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
<b>show radius {status   pending   pending-diff}</b>	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。
<b>show running-config radius [all]</b>	実行コンフィギュレーションの RADIUS 設定を表示します。
<b>show startup-config radius</b>	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。
<b>show radius-server [hostname   ipv4-address   ipv6-address] [directed-request   groups   sorted   statistics]</b>	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。

## RADIUS 認可変更の設定の検証

RADIUS 認可変更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
<code>show running-config dot1x</code>	実行コンフィギュレーションの dot1x 設定を表示します。
<code>show running-config aaa</code>	実行コンフィギュレーションの AAA 設定を表示します。
<code>show running-config radius</code>	実行コンフィギュレーションの RADIUS 設定を表示します。
<code>show aaa server radius statistics</code>	ローカルの RADIUS サーバ統計情報を表示します。
<code>show aaa client radius statistics {ip address   hostname }</code>	ローカルの RADIUS クライアント統計情報を表示します。
<code>clear aaa server radius statistics</code>	ローカルの RADIUS サーバ統計情報をクリアします。
<code>clear aaa client radius statistics {ip address   hostname }</code>	ローカルの RADIUS クライアント統計情報をクリアします。

## 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します。

### Before you begin

1 つまたは複数の RADIUS サーバ ホストを設定します。

### Procedure

	Command or Action	Purpose
ステップ 1	<code>show radius-server statistics {hostname   ipv4-address   ipv6-address}</code>  <b>Example:</b> <pre>switch# show radius-server statistics 10.10.1.1</pre>	RADIUS 統計情報を表示します。

### Related Topics

[RADIUS サーバ ホストの設定 \(64 ページ\)](#)

[RADIUS サーバ統計情報のクリア \(86 ページ\)](#)

## 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。

### Before you begin

Cisco NX-OS デバイスの RADIUS サーバを設定します。

### Procedure

	Command or Action	Purpose
ステップ 1	(Optional) <b>show radius-server statistics</b> <i>{hostname   ipv4-address   ipv6-address}</i>  <b>Example:</b> switch# <b>show radius-server statistics</b> 10.10.1.1	Cisco NX-OS デバイスの RADIUS サーバ統計情報を表示します。
ステップ 2	<b>clear radius-server statistics</b> <i>{hostname   ipv4-address   ipv6-address}</i>  <b>Example:</b> switch# <b>clear radius-server statistics</b> 10.10.1.1	RADIUS サーバ統計情報をクリアします。

### Related Topics

[RADIUS サーバホストの設定 \(64 ページ\)](#)

## 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
```

## RADIUS 認可変更の設定例

次に、RADIUS の認可変更を設定する方法の例を示します。

```
radius-server host 10.77.143.170 key 7 "fewhg123" authentication accounting
aaa server radius dynamic-author
client 10.77.143.170 vrf management server-key 7 "fewhg123"
```

## 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』
VRF コンフィギュレーション	『Cisco Nexus 9000 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
RADIUS に関連する MIB	サポートされている 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。 <a href="ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html">ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html</a>





## 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。

- [TACACS+ について, on page 89](#)
- [TACACS+ の前提条件, on page 93](#)
- [TACACS+ の注意事項と制約事項 \(93 ページ\)](#)
- [TACACS+ のデフォルト設定, on page 94](#)
- [ワンタイムパスワードサポート \(94 ページ\)](#)
- [TACACS+ の設定, on page 95](#)
- [TACACS+ サーバのモニタリング, on page 122](#)
- [TACACS+ サーバ統計情報のクリア, on page 123](#)
- [TACACS+ の設定の確認, on page 124](#)
- [TACACS+ の設定例, on page 124](#)
- [次の作業, on page 126](#)
- [TACACS+ に関する追加情報, on page 126](#)

## TACACS+ について

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/サーバプロトコルは、トランスポート要件に 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認証を提供します。

## 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

ユーザが TACACS+ を使用して、パスワード認証プロトコル (PAP) によるログインを Cisco NX-OS デバイスに対して試行すると、次のプロセスが実行されます。



**Note** 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 デバイスが接続を確立すると、TACACS+ デーモンにアクセスして、ユーザ名とパスワードを取得します。
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受信します。

### 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 デバイスがユーザの許可を要求している場合は、許可が開始されます。

### 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 デバイスが ERROR 応答を受信すると、Cisco NX-OS デバイスは代替方式でユーザ認証を試行します。

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。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 デバイスは再度 TACACS+ デーモンにアクセスします。デーモンはACCEPTまたはREJECT許可応答を返します。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。秘密キーとは、Cisco NX-OS デバイスと TACACS+ サーバホスト間の共有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+サーバ設定で使用されるグローバルな秘密キーを設定できます。

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上書きできます。

## 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+ ??????????

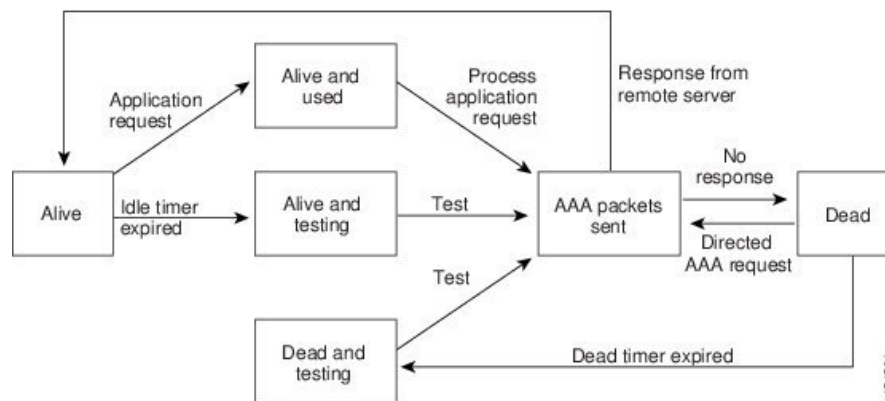
```

??????? TACACS+ ????????AAA ??????????????????????AAA ??????????????????Cisco NX-OS ??????????
TACACS+ ?????????????TACACS+ ?????????????????????????????????????Cisco NX-OS ??????????????
TACACS+ ??????????dead???????????? TACACS+ ?????? AAA ?????????????Cisco NX-OS ??????????????
TACACS+ ?????????????????????????????????????????????????????????????? AAA ?????????????TACACS+
????????????????????TACACS+ ?????????????????????????????????????????SNMP????????????Cisco
NX-OS ?????????????????????????????????????????????????????????????? ??????????????

```

Figure 3: TACACS+ ??????

????TACACS+ ??? ?????????????????????????????



**Note** ???? ?????? ?????????????????????????????????????TACACS+ ??? ????????????????????????????? TACACS+ ???????????

## 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。

次の VSA プロトコル オプションが、Cisco NX-OS ソフトウェアでサポートされています。

#### 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 ソフトウェアでは、次の属性がサポートされています。

### roles

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 network-admin のロールに属している場合、値フィールドは network-operator network-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 network-admin
```

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



**Note** VSA を shell:roles\*"network-operator network-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 デバイスに設定できる TACACS+ サーバの最大数は 64 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。
- 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。
- TACACS+ サーバでのコマンド認証は、コンソールセッションに使用できます。
- N9K-X9636C-R および N9K-X9636Q-R ラインカードおよび N9K-C9508-FM-R ファブリックモジュールの場合、特殊文字を含むユーザ名の TACACS+ 認証は失敗します。

## 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。

Table 9: 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

## ワンタイムパスワードサポート

ワンタイムパスワードサポート (OTP) は、1回のログインセッションまたはトランザクションに有効なパスワードです。OTPは、通常の (スタティック) パスワードに関連する多数の欠点を回避します。OTPは攻撃をリプレイするリスクはありません。すでにサービスへのログインまたは操作の実行に使用された OTP を侵入者が記録しようとしても、OTP は有効ではなくなっているため、悪用されません。

OTP は RADIUS や TACACS プロトコルデーモンに対してのみ適用できます。RADIUS プロトコルデーモンの場合は、ASCII 認証モードを無効にする必要があります。TACACS+ プロトコルデーモンの場合は、ASCII 認証モードを有効にする必要があります。TACACS+ サーバでパスワードの ASCII 認証を有効にするには、**aaa authentication login ascii-authentication** コマンドを使用します。

## TACACS+ の設定

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



**Note** Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

## TACACS+ サーバの設定プロセス

### Procedure

- ステップ 1** TACACS+ をイネーブルにします。
- ステップ 2** TACACS+ サーバと Cisco NX-OS デバイスとの接続を確立します。
- ステップ 3** TACACS+ サーバの秘密キーを設定します。
- ステップ 4** 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 5** (任意) TCP ポートを設定します。
- ステップ 6** (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 7** (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。

### Related Topics

[TACACS+ のイネーブル化](#) (95 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設定されています。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。

## Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> switch# <b>configure terminal</b> 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	<b>feature tacacs+</b> <b>Example:</b> switch(config)# <b>feature tacacs+</b>	TACACS+ をイネーブルにします。
ステップ 3	<b>exit</b> <b>Example:</b> switch(config)# <b>exit</b> switch#	設定モードを終了します。
ステップ 4	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch# <b>copy running-config startup-config</b>	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。



**Note** 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。

## Before you begin

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。

## Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> switch# <b>configure terminal</b> 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	<b>tacacs-server host</b> { <i>ipv4-address</i>   <i>ipv6-address</i>   <i>hostname</i> } <b>Example:</b> switch(config)# <b>tacacs-server host</b> 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。
ステップ 3	(Optional) <b>show tacacs+</b> { <b>pending</b>   <b>pending-diff</b> } <b>Example:</b> switch(config)# <b>show tacacs+ pending</b>	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	(Optional) <b>tacacs+ commit</b> <b>Example:</b> switch(config)# <b>tacacs+ commit</b>	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ます。
ステップ 5	<b>exit</b> <b>Example:</b> switch(config)# <b>exit</b> switch#	設定モードを終了します。
ステップ 6	(Optional) <b>show tacacs-server</b> <b>Example:</b> switch# <b>show tacacs-server</b>	TACACS+ サーバの設定を表示します。
ステップ 7	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch# <b>copy running-config startup-config</b>	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。

## Related Topics

[TACACS+ のイネーブル化](#) (95 ページ)

[TACACS+ サーバ グループの設定](#) (100 ページ)

## グローバル TACACS+ キーの設定

Cisco NX-OS デバイスで使用するすべてのサーバについて、グローバルレベルで秘密 TACACS+ キーを設定できます。秘密キーとは、Cisco NX-OS デバイスと TACACS+ サーバホスト間の共有秘密テキストストリングです。

### Before you begin

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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>tacacs-server key [0   6   7] key-value</b> <b>Example:</b> <pre>switch(config)# tacacs-server key 0 QsEfThUkO</pre> <b>Example:</b> <pre>switch(config)# tacacs-server key 7 "fewhg"</pre>	<p>すべての TACACS+ サーバ用の TACACS+ キーを指定します。 <i>key-value</i> 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。</p> <p>デフォルトでは、秘密キーは設定されていません。</p> <p><b>Note</b>     <b>generate type7_encrypted_secret</b> を使用してすでに共有秘密を設定している場合 2 番目の例のように引用符で囲んで入力してください。詳細については、<a href="#">RADIUS または TACACS+ の共有秘密の設定, on page 50</a>を参照してください。</p>
ステップ 3	<b>exit</b> <b>Example:</b> <pre>switch(config)# exit switch#</pre>	設定モードを終了します。

	Command or Action	Purpose
ステップ 4	(Optional) <b>show tacacs-server</b>  <b>Example:</b> switch# <b>show tacacs-server</b>	TACACS+ サーバの設定を表示します。  <b>Note</b> 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、 <b>show running-config</b> コマンドを使用します。
ステップ 5	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> switch# <b>copy running-config startup-config</b>	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。

**Related Topics**

[TACACS+ のイネーブル化](#) (95 ページ)

[AES パスワード暗号化およびプライマリ暗号キーについて](#) (543 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。秘密キーとは、Cisco NX-OS デバイスと TACACS+ サーバ ホスト間の共有秘密テキスト ストリングです。

**Before you begin**

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。

**Procedure**

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> switch# <b>configure terminal</b> 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	<b>tacacs-server host</b> { <i>ipv4-address</i>   <i>ipv6-address</i>   <i>host-name</i> } <b>key</b> [0   6   7] <i>key-value</i>  <b>Example:</b> switch(config)# <b>tacacs-server host</b> 10.10.1.1 <b>key</b> 0 P1IjUhYg  <b>Example:</b>	特定の TACACS+サーバの秘密キーを指定します。 <i>key-value</i> 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

	Command or Action	Purpose
	<pre>switch(config)# tacacs-server host 10.10.1.1 key 7 "fewhg"</pre>	<p>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。</p> <p>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。</p> <p><b>Note</b>     <b>generate type7_encrypted_secret</b> を使用してすでに共有秘密を設定している場合 2 番目の例のように引用符で囲んで入力してください。詳細については、<a href="#">RADIUS または TACACS+ の共有秘密の設定, on page 50</a>を参照してください。</p>
ステップ 3	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 4	<p>(Optional) <b>show tacacs-server</b></p> <p><b>Example:</b></p> <pre>switch# show tacacs-server</pre>	<p>TACACS+ サーバの設定を表示します。</p> <p><b>Note</b>     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、<b>show running-config</b> コマンドを使用します。</p>
ステップ 5	<p>(Optional) <b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch# copy running-config startup-config</pre>	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。

### Related Topics

[AES パスワード暗号化およびプライマリ暗号キーについて](#) (543 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。

### Before you begin

TACACS+ をイネーブルにします。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> switch# <b>configure terminal</b> 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	<b>aaa group server tacacs+ group-name</b>  <b>Example:</b> switch(config)# <b>aaa group server tacacs+ TacServer</b> 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 3	<b>server {ipv4-address   ipv6-address   hostname}</b>  <b>Example:</b> switch(config-tacacs+)# <b>server 10.10.2.2</b>	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。  指定した TACACS+サーバが見つからない場合は、 <b>tacacs-server host</b> 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	<b>exit</b>  <b>Example:</b> switch(config-tacacs+)# <b>exit</b> 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 5	(Optional) <b>show tacacs-server groups</b>  <b>Example:</b> switch(config)# <b>show tacacs-server groups</b>	TACACS+サーバグループの設定を表示します。
ステップ 6	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> switch(config)# <b>copy running-config startup-config</b>	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。

### Related Topics

[TACACS+ のイネーブル化](#) (95 ページ)

[リモート AAA サービス](#) (25 ページ)

[TACACS+ サーバホストの設定](#) (96 ページ)

[TACACS+ デッドタイム間隔の設定](#) (110 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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> switch# <b>configure terminal</b> 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	<b>ip tacacs source-interface interface</b> <b>Example:</b> switch(config)# <b>ip tacacs source-interface mgmt 0</b>	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	<b>exit</b> <b>Example:</b> switch(config)# <b>exit</b> switch#	設定モードを終了します。
ステップ 4	(Optional) <b>show tacacs-server</b> <b>Example:</b> switch# <b>show tacacs-server</b>	TACACS+サーバの設定情報を表示します。
ステップ 5	(Optional) <b>copy running-config startup config</b> <b>Example:</b> switch# <b>copy running-config startup-config</b>	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。

### Related Topics

[TACACS+ のイネーブル化](#) (95 ページ)

[TACACS+ サーバグループの設定](#) (100 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 デバイスはデフォルトの AAA 認証方式に基づいて認証要求を転送します。このオプションを有効にすると、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 で、`hostname` は設定された TACACS+ サーバの名前です。



**Note** `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。



**Note** 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。

### Before you begin

TACACS+ をイネーブルにします。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <code>switch# configure terminal</code> <code>switch(config)#</code>	グローバル 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	<b>tacacs-server directed-request</b> <b>Example:</b> <code>switch(config)# tacacs-server directed-request</code>	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。
ステップ 3	(Optional) <b>show tacacs+ {pending   pending-diff}</b> <b>Example:</b> <code>switch(config)# show tacacs+ pending</code>	保留状態になっている TACACS+ 設定を表示します。
ステップ 4	(Optional) <b>tacacs+ commit</b> <b>Example:</b> <code>switch(config)# tacacs+ commit</code>	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ます。
ステップ 5	<b>exit</b> <b>Example:</b> <code>switch(config)# exit</code> <code>switch#</code>	設定モードを終了します。

	Command or Action	Purpose
ステップ 6	(Optional) <b>show tacacs-server directed-request</b>  <b>Example:</b> switch# <b>show tacacs-server directed-request</b>	TACACS+ の directed request の設定を表示します。
ステップ 7	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> switch# <b>copy running-config startup-config</b>	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。

**Related Topics**

[TACACS+ のイネーブル化](#) (95 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、タイムアウトエラーを宣言する前に、TACACS+ サーバからの応答を待機するタイムアウト間隔を設定できます。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。

**Before you begin**

TACACS+ をイネーブルにします。

**Procedure**

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> switch# <b>configure terminal</b> 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	<b>tacacs-server host {ipv4-address   ipv6-address   hostname} timeout seconds</b>  <b>Example:</b> switch(config)# <b>tacacs-server host server1 timeout 10</b>	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。  <b>Note</b> 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。

	Command or Action	Purpose
ステップ 3	(Optional) <b>show tacacs+ {pending   pending-diff}</b>  <b>Example:</b> switch(config)# <b>show tacacs+ pending</b>	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	(Optional) <b>tacacs+ commit</b>  <b>Example:</b> switch(config)# <b>tacacs+ commit</b>	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ます。
ステップ 5	<b>exit</b>  <b>Example:</b> switch(config)# <b>exit</b> switch#	設定モードを終了します。
ステップ 6	(Optional) <b>show tacacs-server</b>  <b>Example:</b> switch# <b>show tacacs-server</b>	TACACS+ サーバの設定を表示します。
ステップ 7	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> switch# <b>copy running-config startup-config</b>	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。

**Related Topics**

[TACACS+ のイネーブル化](#) (95 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+ 要求にポート 49 を使用します。

**Before you begin**

TACACS+ をイネーブルにします。

**Procedure**

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> switch# <b>configure terminal</b> 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。

	Command or Action	Purpose
ステップ 2	<b>tacacs-server host</b> { <i>ipv4-address</i>   <i>ipv6-address</i>   <i>hostname</i> } <b>port</b> <i>tcp-port</i> <b>Example:</b> <pre>switch(config)# tacacs-server host 10.10.1.1 port 2</pre>	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	(Optional) <b>show tacacs+</b> { <i>pending</i>   <i>pending-diff</i> } <b>Example:</b> <pre>switch(config)# show tacacs+ distribution pending</pre>	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	(Optional) <b>tacacs+ commit</b> <b>Example:</b> <pre>switch(config)# tacacs+ commit</pre>	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ます。
ステップ 5	<b>exit</b> <b>Example:</b> <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 6	(Optional) <b>show tacacs-server</b> <b>Example:</b> <pre>switch# show tacacs-server</pre>	TACACS+ サーバの設定を表示します。
ステップ 7	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch# copy running-config startup-config</pre>	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。

### Related Topics

[TACACS+ のイネーブル化](#) (95 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。



**Note** 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+サーバがどのくらいの期間要求を受信しなかった場合に、Cisco NX-OS デバイスがテストパケットを送信するかを指定します。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。



**Note** テストパラメータは、すべての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。



**Note** 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。



**Note** 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。

### Before you begin

TACACS+ をイネーブルにします。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>tacacs-server test {idle-time minutes   password password [idle-time minutes]   username name [password password [idle-time minutes]]}</b> <b>Example:</b> <pre>switch(config)# tacacs-server test username user1 password Ur2Gd2BH idle-time 3</pre>	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。 <b>Note</b> 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。

	Command or Action	Purpose
ステップ 3	<b>tacacs-server dead-time</b> <i>minutes</i>  <b>Example:</b> <pre>switch(config)# tacacs-server dead-time 5</pre>	Cisco NX-OS デバイスが、前回応答しなかった TACACS+サーバをチェックするまでの時間 (分) 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	<b>exit</b>  <b>Example:</b> <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 5	(Optional) <b>show tacacs-server</b>  <b>Example:</b> <pre>switch# show tacacs-server</pre>	TACACS+サーバの設定を表示します。
ステップ 6	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch# copy running-config startup-config</pre>	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。

**Related Topics**

[各 TACACS+ サーバの定期モニタリングの設定](#) (108 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+サーバがどのくらいの期間要求を受信しなかった場合に、Cisco NX-OS デバイスがテストパケットを送信するかを指定します。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。



**Note** 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。



**Note** 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。





**Note** 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。



**Note** テストパラメータは、すべてのスイッチに配布されます。テストパラメータは、ファブリック内のスイッチには配信されません。

### Before you begin

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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>tacacs-server host</b> { <i>ipv4-address</i>   <i>ipv6-address</i>   <i>hostname</i> } <b>test</b> { <i>idle-time minutes</i>   <b>password</b> <i>password</i> [ <i>idle-time minutes</i> ]   <b>username</b> <i>name</i> [ <b>password</b> <i>password</i> [ <i>idle-time minutes</i> ]]} <b>Example:</b> <pre>switch(config)# tacacs-server host 10.10.1.1 test username user1 password Ur2Gd2BH idle-time 3</pre>	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 <code>test</code> 、デフォルトのパスワードは <code>test</code> 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。 <b>Note</b> 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	<b>tacacs-server dead-time</b> <i>minutes</i> <b>Example:</b> <pre>switch(config)# tacacs-server dead-time 5</pre>	Cisco NX-OS デバイスが、前回応答しなかった TACACS+ サーバをチェックするまでの時間 (分) 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	<b>exit</b> <b>Example:</b> <pre>switch(config)# exit switch#</pre>	設定モードを終了します。

	Command or Action	Purpose
ステップ 5	(Optional) <b>show tacacs-server</b>  <b>Example:</b> switch# <b>show tacacs-server</b>	TACACS+ サーバの設定を表示します。
ステップ 6	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> switch# <b>copy running-config startup-config</b>	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。

**Related Topics**

[TACACS+ サーバホストの設定 \(96 ページ\)](#)

[TACACS+ サーバのグローバルな定期モニタリングの設定 \(106 ページ\)](#)

## 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。デッドタイム間隔には、Cisco NX-OS デバイスが TACACS+ サーバをデッド状態であると宣言した後、そのサーバがアライブ状態に戻ったかどうかを判断するためにテスト パケットを送信するまでの間隔を指定します。



**Note** 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、デッド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。

**Before you begin**

TACACS+ をイネーブルにします。

**Procedure**

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> switch# <b>configure terminal</b> 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	<b>tacacs-server deadtime minutes</b>  <b>Example:</b> switch(config)# <b>tacacs-server deadtime</b> 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。

	Command or Action	Purpose
ステップ 3	(Optional) <b>show tacacs+ {pending   pending-diff}</b>  <b>Example:</b> switch(config)# <b>show tacacs+ pending</b>	保留状態になっている TACACS+ 設定を表示します。
ステップ 4	(Optional) <b>tacacs+ commit</b>  <b>Example:</b> switch(config)# <b>tacacs+ commit</b>	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ます。
ステップ 5	<b>exit</b>  <b>Example:</b> switch(config)# <b>exit</b> switch#	設定モードを終了します。
ステップ 6	(Optional) <b>show tacacs-server</b>  <b>Example:</b> switch# <b>show tacacs-server</b>	TACACS+ サーバの設定を表示します。
ステップ 7	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> switch# <b>copy running-config startup-config</b>	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。

## 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。

### Before you begin

TACACS+ をイネーブルにします。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> switch# <b>configure terminal</b> 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	<b>aaa authentication login ascii-authentication</b>  <b>Example:</b> switch(config)# <b>aaa authentication login ascii-authentication</b>	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。

	Command or Action	Purpose
ステップ 3	(Optional) <b>show tacacs+ {pending   pending-diff}</b>  <b>Example:</b> switch(config)# <b>show tacacs+ pending</b>	保留状態になっている TACACS+ 設定を表示します。
ステップ 4	(Optional) <b>tacacs+ commit</b>  <b>Example:</b> switch(config)# <b>tacacs+ commit</b>	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ます。
ステップ 5	<b>exit</b>  <b>Example:</b> switch(config)# <b>exit</b> switch#	設定モードを終了します。
ステップ 6	(Optional) <b>show tacacs-server</b>  <b>Example:</b> switch# <b>show tacacs-server</b>	TACACS+ サーバの設定を表示します。
ステップ 7	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> switch# <b>copy running-config startup-config</b>	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。

### Before you begin

TACACS+ をイネーブルにします。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> switch# <b>configure terminal</b> 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	<b>aaa authorization ssh-certificate default {group group-list [none]   local   none}</b>  <b>Example:</b> switch(config)# <b>aaa authorization ssh-certificate</b>	TACACS+ サーバのデフォルトの AAA 許可方式を設定します。  <b>ssh-certificate</b> キーワードは、証明書認証を使用した TACACS+ 許可またはロー

	Command or Action	Purpose
	<pre>default group TACACSServer1 TACACSServer2</pre>	<p>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。</p> <p><i>group-list</i> 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。<b>local</b> 方式では、ローカルデータベースを認証に使用します。<b>none</b> 方式では、AAA 認証が使用されないように指定します。</p>
ステップ 3	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>switch(config)# exit switch#</pre>	<p>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。</p>
ステップ 4	<p>(Optional) <b>show aaa authorization [all]</b></p> <p><b>Example:</b></p> <pre>switch# show aaa authorization</pre>	<p>AAA 許可設定を表示します。<b>all</b> キーワードを指定すると、デフォルト値が表示されます。</p>
ステップ 5	<p>(Optional) <b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch# copy running-config startup-config</pre>	<p>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。</p>

#### Related Topics

[TACACS+ のイネーブル化](#) (95 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。



#### Caution

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。



**Note** 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。認証は、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ますが、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。



**Note** 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。

### Before you begin

TACACS+ をイネーブルにします。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>aaa authorization {commands   config-commands} {console   default} {group group-list [local]   local}</b> <b>Example:</b> <pre>switch(config)# aaa authorization commands default group TacGroup Per command authorization will disable RBAC for all users. Proceed (y/n)?</pre>	<p>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。</p> <p><b>commands</b> キーワードを使用するとすべての EXEC コマンドの許可ソースを設定でき、<b>config-commands</b> キーワードを使用すると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できます。</p> <p><b>console</b> 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、<b>default</b> 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。</p> <p><b>group-list</b> 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。<b>local</b> 方</p>

	Command or Action	Purpose
		<p>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。</p> <p><b>local</b> 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なかった場合に、<b>local</b> をフォールバック方式として設定しているときにだけ使用されます。デフォルトの方式は <b>local</b> です。</p> <p>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。</p> <p>確認プロンプトで <b>Enter</b> キーを押した場合のデフォルトのアクションは <b>n</b> です。</p>
ステップ 3	(Optional) <b>show tacacs+ {pending   pending-diff}</b> <b>Example:</b> <pre>switch(config)# show tacacs+ pending</pre>	保留状態になっている TACACS+ 設定を表示します。
ステップ 4	(Optional) <b>tacacs+ commit</b> <b>Example:</b> <pre>switch(config)# tacacs+ commit</pre>	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ます。
ステップ 5	<b>exit</b> <b>Example:</b> <pre>switch(config)# exit switch#</pre>	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	(Optional) <b>show aaa authorization [all]</b> <b>Example:</b> <pre>switch(config)# show aaa authorization</pre>	AAA 許可設定を表示します。 <b>all</b> キーワードを指定すると、デフォルト値が表示されます。
ステップ 7	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	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。

### Related Topics

[TACACS+ のイネーブル化](#) (95 ページ)

[TACACS+ サーバでのコマンド許可のテスト](#) (116 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。



**Note** 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。



**Note** **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。

### Before you begin

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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>test aaa authorization command-type {commands   config-commands} user username command command-string</b>  <b>Example:</b> <pre>switch# test aaa authorization command-type commands user TestUser command reload</pre>	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。  <b>commands</b> キーワードはEXEC コマンドだけを指定し、 <b>config-commands</b> 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。  <b>Note</b> <i>command-string</i> 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。

### Related Topics

[TACACS+ のイネーブル化](#) (95 ページ)

[TACACS+ サーバでのコマンド許可の設定](#) (113 ページ)

[ユーザアカウントおよびRBACの設定](#)

## 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

	コマンドまたはアクション	目的
ステップ 1	<b>terminal verify-only [ username username ]</b> 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は Cisco NX-OS ソフトウェアによって示されます。
ステップ 2	<b>terminal no verify-only [ username username ]</b> 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、Role-Based Access Control (RBAC; ロールベース アクセス コントロール) 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。



#### Warning

**enable secret** コマンドは使用しないでください。このコマンドはサポートされておらず、廃止予定です。将来のリリースでは使用できなくなります。代わりに、RBAC ルールを使用すると、よりきめ細かいセキュリティ制御が可能になります。RBAC の詳細については、『[Cisco Nexus 9000 Series NX-OS Security Configuration Guide](#)』の「Configuring User Accounts and RBAC」を参照してください。

特権レベル	ユーザ ロール権限
15	network-admin 権限

特権レベル	ユーザ ロール権限
13 ~ 1	<ul style="list-style-type: none"> <li>• <b>feature privilege</b> の場合、スタンドアロン ロール権限 コマンドがディセーブルの場合)。</li> <li>• ロールの累積権限からなる特権レベル 0 と同じ権限 (<b>feature privilege</b> コマンドがイネーブルの場合)</li> </ul>
0	<b>show</b> コマンドや <b>exec</b> コマンド ( <b>ping</b> 、 <b>trace</b> 、 <b>ssh</b> など) を実行するための権限

**Important**

ネットワーク管理者のみがルートに権限を昇格できます。新しいセキュリティ対策により、ネットワーク オペレータ (priv-1 ユーザ) は **show tech** を収集できません。したがって、**enable** コマンドだけでは権限のエスカレーションを行えません。

**Note**

- **feature privilege** コマンドがイネーブルの場合、権限ロールは下位の権限ロールの権限を継承します。
- 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。

**Procedure**

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>[no] feature privilege</b> <b>Example:</b> <pre>switch(config)# feature privilege</pre>	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。 <b>enable</b> 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。デフォルトはディセーブルです。
ステップ 3	<b>[no] enable secret [0   5] password [priv-lvl priv-lvl   all]</b> <b>Example:</b> <pre>switch(config)# enable secret 5 def456 priv-lvl 15</pre>	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

	Command or Action	Purpose
		<p>ザに要求します。デフォルトはディセーブルです。</p> <p>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<b>0</b>を入力し、暗号化された形式を指定する場合は<b>5</b>を入力します。 <i>password</i> 引数に指定できる文字数は、最大 64 文字です。 <i>priv-lvl</i> 引数は、1 ~ 15 です。</p> <p><b>Note</b> シークレット パスワードをイネーブルにするには、<b>feature privilege</b> 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。</p>
ステップ 4	<p><b>[no] username username priv-lvl n</b></p> <p><b>Example:</b></p> <pre>switch(config)# username user2 priv-lvl 15</pre>	<p>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。デフォルトはディセーブルです。</p> <p><b>priv-lvl</b> キーワードはユーザに割り当てる特権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 (<i>priv-lvl 0</i> ~ <i>priv-lvl 15</i>) は、ユーザ ロール <i>priv-0</i> ~ <i>priv-15</i> にマッピングされます。</p>
ステップ 5	<p>(Optional) <b>show privilege</b></p> <p><b>Example:</b></p> <pre>switch(config)# show privilege</pre>	<p>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。</p>
ステップ 6	<p>(Optional) <b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch(config)# copy running-config startup-config</pre>	<p>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。</p>
ステップ 7	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>switch(config)# exit switch#</pre>	<p>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。</p>
ステップ 8	<p><b>enable level</b></p> <p><b>Example:</b></p> <pre>switch# enable 15</pre>	<p>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。 <i>level</i> 引数はユーザのアクセ</p>

	Command or Action	Purpose
		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。

### Related Topics

[権限ロールのユーザ コマンドの許可または拒否](#) (120 ページ)

[ユーザ ロールおよびルールの作成](#) (251 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なっ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**。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> 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	<b>[no] role name priv-n</b>  <b>Example:</b> 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	<b>rule number {deny   permit} command command-string</b>  <b>Example:</b> 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。ルールごとに最大 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つのルールが3つのルールを持っている場合、ルール3がルール2

	Command or Action	Purpose
		<p>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。</p> <p><i>command-string</i> 引数には、空白スペースを含めることができます。</p> <p><b>Note</b> 必要な規則の数だけこのコマンドを繰り返します。</p>
ステップ 4	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>switch(config-role)# exit switch(config)#</pre>	<p>ロール コンフィギュレーション モードを終了します。</p>
ステップ 5	<p>(Optional) <b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch(config)# copy running-config startup-config</pre>	<p>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。</p>

#### Related Topics

[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 \(117 ページ\)](#)

[ユーザ ロールおよびルールの作成 \(251 ページ\)](#)

## 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。

#### Before you begin

TACACS+ をイネーブルにします。

#### Procedure

	Command or Action	Purpose
ステップ 1	<p><b>test aaa server tacacs+</b> {<i>ipv4-address</i>   <i>ipv6-address</i>   <i>hostname</i>} [<b>vrf</b> <i>vrf-name</i>] <i>username password</i></p> <p><b>Example:</b></p> <pre>switch# test aaa server tacacs+ 10.10.1.1 user1 Ur2Gd2BH</pre>	<p>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。</p>
ステップ 2	<p><b>test aaa group</b> <i>group-name username password</i></p> <p><b>Example:</b></p>	<p>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。</p>

	Command or Action	Purpose
	switch# test aaa group TacGroup user2 As3He3CI	

### Related Topics

[TACACS+ サーバホストの設定 \(96 ページ\)](#)

[TACACS+ サーバグループの設定 \(100 ページ\)](#)

## TACACS+ のディセーブル化

TACACS+ をディセーブルにできます。



**Caution** 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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	<b>no feature tacacs+</b> <b>Example:</b> switch(config)# no feature tacacs+	TACACS+ をディセーブルにします。
ステップ 3	<b>exit</b> <b>Example:</b> switch(config)# exit switch#	設定モードを終了します。
ステップ 4	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> 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。

## 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できます。

**Before you begin**

Cisco NX-OS デバイスの TACACS+ サーバを設定します。

**Procedure**

	Command or Action	Purpose
ステップ 1	<b>show tacacs-server statistics</b> <i>{hostname   ipv4-address   ipv6-address}</i>  <b>Example:</b> <pre>switch# show tacacs-server statistics 10.10.1.1</pre>	TACACS+ 統計情報を表示します。

**Related Topics**

[TACACS+ サーバホストの設定](#) (96 ページ)

[TACACS+ サーバ統計情報のクリア](#) (123 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。

**Before you begin**

Cisco NX-OS デバイスの TACACS+ サーバを設定します。

**Procedure**

	Command or Action	Purpose
ステップ 1	(Optional) <b>show tacacs-server statistics</b> <i>{hostname   ipv4-address   ipv6-address}</i>  <b>Example:</b> <pre>switch# show tacacs-server statistics 10.10.1.1</pre>	Cisco NX-OS デバイスの TACACS+ サーバ統計情報を表示します。
ステップ 2	<b>clear tacacs-server statistics</b> <i>{hostname   ipv4-address   ipv6-address}</i>  <b>Example:</b> <pre>switch# clear tacacs-server statistics 10.10.1.1</pre>	TACACS+ サーバ統計情報をクリアします。

**Related Topics**

[TACACS+ サーバホストの設定](#) (96 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
<code>show tacacs+ { status   pending   pending-diff }</code>	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。
<code>show running-config tacacs [all]</code>	実行コンフィギュレーションの TACACS+ 設定を表示します。
<code>show startup-config tacacs</code>	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。
<code>show tacacs-server [host-name   ipv4-address   ipv6-address] [directed-request   groups   sorted   statistics]</code>	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。
<code>show privilege</code>	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。

## 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
-----
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 コマンドを入力すると、ユーザは、管理者が enable secret コマンドを使用して設定したパスワードを入力するように求められます。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 © 2013, 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 © 2013, 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が pwd コマンドを実行できるようにする例を示します。

```
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が **show running-config** コマンドを実行できないようにする例を示します。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』
VRF コンフィギュレーション	『Cisco NX-OS 9000 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**

<b>MIB</b>	<b>MIB のリンク</b>
TACACS+に関連する MIB	サポートされている 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。  <a href="ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html">ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html</a>





## 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。次の項が含まれています。

- [LDAP について \(129 ページ\)](#)
- [LDAP の前提条件 \(132 ページ\)](#)
- [LDAP の注意事項と制約事項 \(132 ページ\)](#)
- [LDAP のデフォルト設定 \(133 ページ\)](#)
- [LDAP の設定 \(133 ページ\)](#)
- [LDAP サーバのモニタリング \(147 ページ\)](#)
- [LDAP サーバ統計情報のクリア \(147 ページ\)](#)
- [LDAP 設定の確認 \(148 ページ\)](#)
- [LDAP の設定例 \(148 ページ\)](#)
- [次の作業 \(149 ページ\)](#)
- [LDAP に関する追加情報 \(149 ページ\)](#)

## LDAP について

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 台のアクセスコントロールサーバ (LDAP デーモン) で各サービス認証と認可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 (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。

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** : ユーザ認証は失敗します。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、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)



(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。

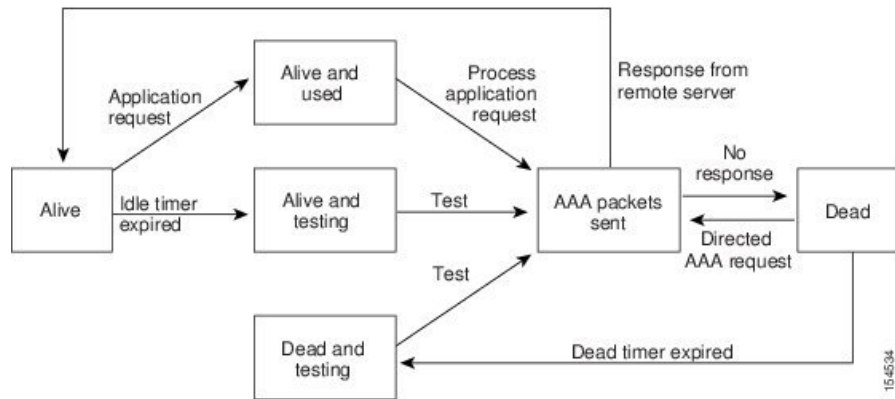


(注) LDAP では、認証の前に許可を行うことができます。

## LDAP ??????????

?????? LDAP ???????AAA ??????????????????????AAA ??????????????????LDAP ?????????????? LDAP  
 ??Cisco NX-OS ?????????????? LDAP ??????????dead????????????? LDAP  
 ?????? AAA ??????????Cisco NX-OS ?????????? LDAP ?? ???????????  
 AAA ??????????????LDAP ??????????????????????????LDAP  
 ??SNMP?????????????Cisco NX-OS  
 ?? ??????????????????????LDAP ??? ??????????????????????

図 4: LDAP ???????



(注) ??LDAP ??? ?????????????????????????????? LDAP ??????????????

## 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。

- `roles` : 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。

## LDAP のバーチャライゼーション サポート

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 9000 Series NX-OS Unicast Routing Configuration 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。

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。

### 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。

1. LDAP をイネーブルにします。

2. LDAP サーバと Cisco NX-OS デバイスの接続を確立します。
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。
4. (任意) TCP ポートを設定します。
5. (任意) LDAP サーバにデフォルト AAA 認証方式を設定します。
6. (任意) LDAP 検索マップを設定します。
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/ディセーブル化](#) (134 ページ)

[LDAP サーバホストの設定](#) (135 ページ)

[LDAP サーバの rootDN の設定](#) (136 ページ)

[LDAP サーバグループの設定](#) (137 ページ)

[TCP ポートの設定](#) (141 ページ)

[LDAP 検索マップの設定](#) (142 ページ)

[LDAP サーバの定期的モニタリングの設定](#) (143 ページ)

## LDAP のイネーブル化/ディセーブル化

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

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	必須: <b>[no] feature ldap</b> 例： switch(config)# feature ldap	LDAP をイネーブルにします。LDAP を無効にするには、このコマンドの <b>no</b> 形式を使用します。  (注) 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。
ステップ 3	(任意) <b>copy running-config startup-config</b> 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。

### 関連トピック

- [LDAP サーバの設定プロセス \(133 ページ\)](#)
- [LDAP サーバホストの設定 \(135 ページ\)](#)
- [LDAP サーバの rootDN の設定 \(136 ページ\)](#)
- [LDAP サーバグループの設定 \(137 ページ\)](#)
- [グローバルな LDAP タイムアウト間隔の設定 \(139 ページ\)](#)
- [LDAP サーバのタイムアウト間隔の設定 \(140 ページ\)](#)
- [TCP ポートの設定 \(141 ページ\)](#)
- [LDAP 検索マップの設定 \(142 ページ\)](#)
- [LDAP サーバの定期的モニタリングの設定 \(143 ページ\)](#)
- [LDAP デッドタイム間隔の設定 \(145 ページ\)](#)
- [LDAP サーバでの AAA 許可の設定 \(145 ページ\)](#)

## 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。



**Note** 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。

### Before you begin

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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>[no] ldap-server host {ipv4-address   ipv6-address   host-name} [enable-ssl]</b> <b>Example:</b>	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。

	Command or Action	Purpose
	switch(config)# ldap-server host 10.10.2.2 enable-ssl	<b>enable-ssl</b> キーワードは、LDAP クライアントに SSL セッションを確立させてからバインドまたは検索の要求を送信することにより、転送されたデータの整合性と機密保持を保証します。
ステップ 3	(Optional) <b>show ldap-server</b>  <b>Example:</b> switch(config)# show ldap-server	LDAP サーバの設定を表示します。
ステップ 4	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> 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。

#### Related Topics

- [LDAP サーバの設定プロセス \(133 ページ\)](#)
- [LDAP のイネーブル化/ディセーブル化 \(134 ページ\)](#)
- [LDAP サーバグループの設定 \(137 ページ\)](#)
- [LDAP サーバの rootDN の設定 \(136 ページ\)](#)
- [LDAP サーバグループの設定 \(137 ページ\)](#)
- [LDAP サーバの定期的モニタリングの設定 \(143 ページ\)](#)
- [LDAP サーバのモニタリング \(147 ページ\)](#)
- [LDAP サーバ統計情報のクリア \(147 ページ\)](#)

## 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。

#### 始める前に

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

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  例 :	グローバル 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
	switch# configure terminal switch(config)#	
ステップ 2	<p><b>[no] ldap-server host {ipv4-address   ipv6-address   hostname} rootDN root-name [password password [port tcp-port [timeout seconds]   timeout seconds]]</b></p> <p>例 :</p> <pre>switch(config)# ldap-server host 10.10.1.1 rootDN cn=manager,dc=acme,dc=com password Ur2Gd2BH timeout 60</pre>	<p>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。</p> <p>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）。</p>
ステップ 3	<p>（任意） <b>show ldap-server</b></p> <p>例 :</p> <pre>switch(config)# show ldap-server</pre>	LDAP サーバの設定を表示します。
ステップ 4	<p>（任意） <b>copy running-config startup-config</b></p> <p>例 :</p> <pre>switch(config)# copy running-config startup-config</pre>	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 サーバの設定プロセス](#) (133 ページ)

[LDAP のイネーブル化/ディセーブル化](#) (134 ページ)

[LDAP サーバホストの設定](#) (135 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。

#### Before you begin

LDAP をイネーブルにします。

## Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	<b>[no] aaa group server ldap group-name</b> <b>Example:</b> 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	<b>[no] server {ipv4-address   ipv6-address   host-name}</b> <b>Example:</b> 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かった場合は、 <b>ldap-server host</b> 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	(Optional) <b>[no] authentication {bind-first [append-with-baseDN DNstring]   compare [password-attribute password]}</b> <b>Example:</b> switch(config-ldap)# authentication compare password-attribute TyuL8r	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	(Optional) <b>[no] enable user-server-group</b> <b>Example:</b> switch(config-ldap)# enable user-server-group	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	(Optional) <b>[no] enable Cert-DN-match</b> <b>Example:</b> switch(config-ldap)# enable Cert-DN-match	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	(Optional) <b>no [use-vrf vrf-name]</b> <b>Example:</b> switch(config-ldap)# use-vrf vrf1	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 8	<b>exit</b> <b>Example:</b>	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。

	Command or Action	Purpose
	switch(config-ldap)# exit switch(config)#	
ステップ 9	(Optional) <b>show ldap-server groups</b>  <b>Example:</b> switch(config)# show ldap-server groups	LDAP サーバ グループの設定を表示します。
ステップ 10	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> 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。

#### Related Topics

- [LDAP サーバの設定プロセス \(133 ページ\)](#)
- [LDAP サーバ ホストの設定 \(135 ページ\)](#)
- [LDAP のイネーブル化/ディセーブル化 \(134 ページ\)](#)
- [LDAP サーバ ホストの設定 \(135 ページ\)](#)

## 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。

#### 始める前に

LDAP をイネーブルにします。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  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	<b>[no] ldap-server timeout seconds</b>  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	(任意) <b>show ldap-server</b>  例 : switch(config)# show ldap-server	LDAP 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 4	(任意) <b>copy running-config startup-config</b> 例 : <pre>switch(config)# copy running-config startup-config</pre>	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/ディセーブル化](#) (134 ページ)

[LDAP サーバのタイムアウト間隔の設定](#) (140 ページ)

[LDAP サーバのタイムアウト間隔の設定](#) (140 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。

#### 始める前に

LDAP をイネーブルにします。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>[no] ldap-server host {ipv4-address   ipv6-address   hostname} timeout seconds</b> 例 : <pre>switch(config)# ldap-server host server1 timeout 10</pre>	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	(任意) <b>show ldap-server</b> 例 : <pre>switch(config)# show ldap-server</pre>	LDAP 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 4	(任意) <b>copy running-config startup-config</b>  例 : <pre>switch(config)# copy running-config startup-config</pre>	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

[グローバルな LDAP タイムアウト間隔の設定 \(139 ページ\)](#)

[LDAP のイネーブル化/ディセーブル化 \(134 ページ\)](#)

[グローバルな LDAP タイムアウト間隔の設定 \(139 ページ\)](#)

## 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。

#### 始める前に

LDAP をイネーブルにします。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  例 : <pre>switch# configure terminal switch(config)#</pre>	グ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	<b>[no] ldap-server host {ipv4-address   ipv6-address   hostname} port tcp-port [timeout seconds]</b>  例 : <pre>switch(config)# ldap-server host 10.10.1.1 port 200 timeout 5</pre>	<p>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。</p> <p>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)。</p>

	コマンドまたはアクション	目的
		(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	(任意) <b>show ldap-server</b> 例： switch(config)# show ldap-server	LDAP サーバの設定を表示します。
ステップ 4	(任意) <b>copy running-config startup-config</b> 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。

#### 関連トピック

[LDAP サーバの設定プロセス \(133 ページ\)](#)

[LDAP のイネーブル化/ディセーブル化 \(134 ページ\)](#)

## 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。

#### 始める前に

LDAP をイネーブルにします。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>ldap search-map map-name</b> 例： switch(config)# ldap search-map map1 switch(config-ldap-search-map)#	LDAP 検索マップを設定します。

	コマンドまたはアクション	目的
ステップ 3	(任意) <code>[userprofile   trustedCert   CRLLookup   user-certdn-match   user-pubkey-match   user-switch-bind] attribute-name attribute-name search-filter filter base-DN base-DN-name</code> 例 : <pre>switch(config-ldap-search-map)# userprofile attribute-name att-name search-filter (&amp;(objectClass=inetOrgPerson)(cn=\$userid)) base-DN dc=acme,dc=com</pre>	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 <code>user-switchgroup</code> 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。  <i>attribute-name</i> 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	(任意) <code>exit</code> 例 : <pre>switch(config-ldap-search-map)# exit switch(config)#</pre>	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	(任意) <code>show ldap-search-map</code> 例 : <pre>switch(config)# show ldap-search-map</pre>	設定された LDAP 検索マップを表示します。
ステップ 6	(任意) <code>copy running-config startup-config</code> 例 : <pre>switch(config)# copy running-config startup-config</pre>	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 サーバの設定プロセス \(133 ページ\)](#)

[LDAP のイネーブル化/ディセーブル化 \(134 ページ\)](#)

## 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。

## 始める前に

LDAP をイネーブルにします。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	必須: <b>[no] ldap-server host {ipv4-address   ipv6-address   hostname} test rootDN root-name [idle-time minutes   password password [idle-time minutes]   username name [password password [idle-time minutes]]]</b> 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。
ステップ 3	<b>[no] ldap-server deadtime minutes</b> 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	(任意) <b>show ldap-server</b> 例： switch(config)# show ldap-server	LDAP サーバの設定を表示します。
ステップ 5	(任意) <b>copy running-config startup-config</b> 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。

## 関連トピック

[LDAP サーバの設定プロセス \(133 ページ\)](#)

[LDAP のイネーブル化/ディセーブル化 \(134 ページ\)](#)

[LDAP サーバホストの設定 \(135 ページ\)](#)

## 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。

### 始める前に

LDAP をイネーブルにします。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>[no] ldap-server deadtime minutes</b> 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	(任意) <b>show ldap-server</b> 例： switch(config)# show ldap-server	LDAP サーバの設定を表示します。
ステップ 4	(任意) <b>copy running-config startup-config</b> 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。

### 関連トピック

[LDAP のイネーブル化/ディセーブル化 \(134 ページ\)](#)

## 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。

始める前に

LDAP をイネーブルにします。

手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>aaa authorization {ssh-certificate   ssh-publickey} default {group group-list   local}</b> 例 : <pre>switch(config)# aaa authorization ssh-certificate default group LDAPServer1 LDAPServer2</pre>	<p>LDAP サーバのデフォルトの AAA 許可方式を設定します。</p> <p><b>ssh-certificate</b> 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、<b>ssh-publickey</b> キーワードは SSH 公開キーを使用した LDAP 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。</p> <p><i>group-list</i> 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。<b>local</b> 方式はローカルデータベースを使用して許可を行います。</p>
ステップ 3	(任意) <b>show aaa authorization [all]</b> 例 : <pre>switch(config)# show aaa authorization</pre>	AAA 許可設定を表示します。 <b>all</b> キーワードを指定すると、デフォルト値が表示されます。
ステップ 4	(任意) <b>copy running-config startup-config</b> 例 : <pre>switch(config)# copy running-config startup-config</pre>	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/ディセーブル化](#) (134 ページ)

## 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。

### 始める前に

Cisco NX-OS デバイスに LDAP サーバを設定します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>show ldap-server statistics</b> {hostname   ipv4-address   ipv6-address}  例 : <pre>switch# show ldap-server statistics 10.10.1.1</pre>	LDAP サーバの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](#) (135 ページ)

[LDAP サーバ統計情報のクリア](#) (147 ページ)

[LDAP サーバ統計情報のクリア](#) (147 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。

### 始める前に

Cisco NX-OS デバイスに LDAP サーバを設定します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	(任意) <b>show ldap-server statistics</b> {hostname   ipv4-address   ipv6-address}  例 : <pre>switch# show ldap-server statistics 10.10.1.1</pre>	LDAP サーバの統計情報を表示します。
ステップ 2	<b>clear ldap-server statistics</b> {hostname   ipv4-address   ipv6-address}	LDAP サーバ統計情報をクリアします。

	コマンドまたはアクション	目的
	例 : switch# clear ldap-server statistics 10.10.1.1	

#### 関連トピック

[LDAP サーバのモニタリング](#) (147 ページ)

[LDAP サーバ ホストの設定](#) (135 ページ)

[LDAP サーバのモニタリング](#) (147 ページ)

## LDAP 設定の確認

LDAP 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
<b>show running-config ldap [all]</b>	実行コンフィギュレーションの LDAP 設定を表示します。
<b>show startup-config ldap</b>	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。
<b>show ldap-server</b>	LDAP 設定情報を表示します。
<b>show ldap-server groups</b>	LDAP サーバ グループの設定情報を表示します。
<b>show ldap-server statistics {hostname   ipv4-address   ipv6-address}</b>	LDAP 統計情報を表示します。
<b>show ldap-search-map</b>	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。

## 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 att-name search-filter "
```



```
((&(objectClass=Person)(sAMAccountName=$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
```

次の例は、認証を検証する方法を示しています。

```
failing
test aaa group LdapServer user <user-password>
user has failed authentication

! working
test aaa group LdapServer user <user-password>
user has been authenticated
```

## 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

### 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』
VRF コンフィギュレーション	『Cisco Nexus 9000 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**

<b>MIB</b>	<b>MIB のリンク</b>
LDAPに関連する MIB	サポートされている 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。 <a href="ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html">ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html</a>



## 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。

- [SSH および Telnet について, on page 151](#)
- [SSH および Telnet の前提条件, on page 153](#)
- [SSH と Telnet の注意事項と制約事項 \(153 ページ\)](#)
- [SSH および Telnet のデフォルト設定, on page 154](#)
- [SSH の設定 , on page 155](#)
- [Telnet の設定, on page 174](#)
- [SSH および Telnet の設定の確認, on page 176](#)
- [SSH の設定例, on page 177](#)
- [SSH のパスワードが不要なファイル コピーの設定例, on page 178](#)
- [X.509v3 証明書ベースの SSH 認証の設定例 \(180 ページ\)](#)
- [SSH および Telnet に関する追加情報, on page 180](#)

## SSH および Telnet について

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。

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、無償あるいは商用の SSH サーバと連係して動作します。

## SSH サーバキー

SSH では、Cisco NX-OS とのセキュア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 Algorithm (DSA) を使用した SSH バージョン 2
- 楕円曲線デジタル署名アルゴリズム (ECDSA) 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 サービスでは、SSH バージョン 2 に対応する以下の 2 通りのキーペアを使用できます。

- **dsa** オプションでは、SSH バージョン 2 プロトコル用の DSA キーペアを作成します。
- **rsa** オプションでは、SSH バージョン 2 プロトコル用の RSA キーペアを作成します。
- **ecdsa** オプションでは、SSH バージョン 2 プロトコル用の ECDSA キーペアを作成します。

デフォルトでは、Cisco NX-OS ソフトウェアは 1024 ビットの RSA キーを生成します。

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

**Caution**

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 のいずれかで設定されており、無効にされたり期限が切れたりしていなければ、証明書の検証は成功します。

X.509 証明書を使用する SSH 認証用にデバイスを設定できます。認証に失敗した場合は、パスワードの入力が求められます。

X.509v3 証明書（RFC 6187）を使用する SSH 認証を設定できます。X.509v3 証明書ベースの SSH 認証では、スマートカードと組み合わせた証明書を使用して、シスコ デバイスへのアクセスの 2 要素認証を有効にします。SSH クライアントは、シスコパートナーの Pragma Systems によって提供されます。

## 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 サーバが 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 の前提条件

レイヤ 3 インターフェイス上で IP、mgmt 0 インターフェイス上でアウトバンド、またはイーサネット インターフェイス上でインバンドを設定していることを確認します。

## 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。
- **no feature ssh feature** コマンドを使用すると、ポート 22 はディセーブルになりません。ポート 22 は常にオープンで、すべての着信外部接続を拒否する拒否ルールがプッシュされます。
- Poodle の脆弱性により、SSLv3 はサポートされなくなりました。

- IPSG は、次のものではサポートされません。
  - Cisco Nexus 9372PX、9372TX、および 9332PQ スイッチの最後の 6 個の 40 Gb 物理ポート
  - Cisco Nexus 9396PX、9396TX、および 93128TX スイッチのすべての 40G 物理ポート
- X.509 証明書を使用する SSH 認証用にデバイスを設定できます。認証に失敗した場合は、パスワードの入力が求められます。
- 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 を使用してデバイスにアクセスできます。
- SSH パスワードレスファイルコピーを目的として AAA プロトコル (RADIUS や TACACS+ など) を介してリモート認証されたユーザアカウントにインポートされた SSH 公開キーと秘密キーは、同じ名前のローカルユーザアカウントでない限り、Nexus デバイスがリロードされると保持されません。リモートユーザアカウントは、SSH キーがインポートされる前にデバイスで設定されます。
- SSH タイムアウト期間は、tac-pac 生成時間よりも長くする必要があります。そうしないと、VSH ログに %VSHD-2-VSHD\_SYSLOG\_EOL\_ERR エラーが表示されることがあります。理想的には、tac-pac または showtech を収集する前に 0 (無限) に設定します。



(注) Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

## 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。

Table 10: 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

パラメータ	デフォルト
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。

#### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>no feature ssh</b> <b>Example:</b> <pre>switch(config)# no feature ssh</pre>	SSH をディセーブルにします。
ステップ 3	<b>ssh key {dsa [force]   rsa [bits[force]]   ecdsa [bits [ force]]}</b> <b>Example:</b> <pre>switch(config)# ssh key rsa 2048</pre>	<p>SSH サーバ キーを生成します。</p> <p><i>bits</i> 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。有効な範囲は 768 ~ 2048 です。デフォルト値は 1024 です。</p> <p>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。</p> <p>既存のキーを置き換える場合は、<b>force</b> キーワードを使用します。</p> <p><b>Note</b>    <code>ssh key dsa</code> を設定する場合は、次の追加設定を行う必要があります：<code>ssh keytypes all</code> および <code>ssh kexalgos all</code></p>

	Command or Action	Purpose
ステップ 4	<b>ssh rekey max-data max-data max-time max-time</b> <b>Example:</b> <pre>switch(config)# ssh rekey max-data 1K max-time 1M</pre>	キー再生成パラメータを設定します。
ステップ 5	<b>feature ssh</b> <b>Example:</b> <pre>switch(config)# feature ssh</pre>	SSH をイネーブルにします。
ステップ 6	<b>exit</b> <b>Example:</b> <pre>switch(config)# exit switch#</pre>	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	(Optional) <b>show ssh key [dsa   rsa   ecdsa] [md5]</b> <b>Example:</b> <pre>switch# show ssh key</pre>	SSH サーバ キーを表示します。  このコマンドは、デフォルトで SHA256 形式でフィンガープリントを表示します。SHA256 は、以前のデフォルトの MD5 形式よりも安全です。ただし、フィンガープリントを MD5 形式で表示する必要がある場合の下位互換性のために、 <b>md5</b> オプションが追加されています。
ステップ 8	<b>show run security all</b>	
ステップ 9	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch# copy running-config startup-config</pre>	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

### 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。



**Before you begin**

IETF SCHSH 形式の SSH 公開キーを作成します。

**Procedure**

	Command or Action	Purpose
ステップ 1	<b>copy server-file bootflash:filename</b> <b>Example:</b> <pre>switch# copy tftp://10.10.1.1/secsh_file.pub bootflash:secsh_file.pub</pre>	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	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>username username sshkey file bootflash:filename</b> <b>Example:</b> <pre>switch(config)# username User1 sshkey file bootflash:secsh_file.pub</pre>	IETF SECSH 形式の SSH 公開キーを設定します。
ステップ 4	<b>exit</b> <b>Example:</b> <pre>switch(config)# exit switch#</pre>	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	(Optional) <b>show user-account</b> <b>Example:</b> <pre>switch# show user-account</pre>	ユーザアカウントの設定を表示します。
ステップ 6	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch# copy running-config startup-config</pre>	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。

**Before you begin**

OpenSSH 形式の SSH 公開キーを作成します。

## Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	<b>username username sshkey ssh-key</b> <b>Example:</b> switch(config)# username User1 sshkey ssh-rsa AAAENaClYc2NwWElwAAAEPAj19FQzLl9z3fDxk3CllM7/yjzF50v7gEP K0BnsiGAKulnI7/Qhur4LNgD/6ow51b9HARFY/ChLNQY6pig30c6G XhNjnlLB7ihmp7dlddMQwOrXNshXrSiH3D/v%ziEh5S4Tpx8=	OpenSSH 形式の SSH 公開キーを設定します。
ステップ 3	<b>exit</b> <b>Example:</b> 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	<b>(Optional) show user-account</b> <b>Example:</b> switch# show user-account	ユーザアカウントの設定を表示します。
ステップ 5	<b>(Optional) copy running-config startup-config</b> <b>Example:</b> 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。

## 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。

**Note**

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。

## Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>ssh login-attempts number</b> <b>Example:</b> <pre>switch(config)# ssh login-attempts 5</pre>	<p>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。</p> <p><b>Note</b> このコマンドの <b>no</b> 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。</p>
ステップ 3	<b>(Optional) show running-config security all</b> <b>Example:</b> <pre>switch(config)# show running-config security all</pre>	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	<b>(Optional) copy running-config startup-config</b> <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	(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。

### Before you begin

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。

## Procedure

	Command or Action	Purpose
ステップ 1	<b>ssh</b> [username@]{ipv4-address   hostname} [vrf vrf-name] <b>Example:</b> 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	<b>ssh6</b> [username@]{ipv6-address   hostname} [vrf vrf-name] <b>Example:</b> 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。

## Before you begin

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。

## Procedure

	Command or Action	Purpose
ステップ 1	<b>ssh</b> [username@]hostname <b>Example:</b> 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。
ステップ 2	<b>exit</b> <b>Example:</b> switch(boot)# exit	ブートモードを終了します。
ステップ 3	<b>copy scp://[username@]hostname/filepath directory</b> <b>Example:</b> 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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>[no] username username keypair generate {rsa [bits [force]]   dsa [force]}</b> <b>Example:</b> <pre>switch(config)# username user1 keypair generate rsa 2048 force</pre>	<p>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。</p> <p><i>bits</i> 引数には、キーの生成に使用するビット数を指定します。有効な範囲は 768 ~ 2048 です。デフォルト値は 1024 です。</p> <p>既存のキーを置き換える場合は、<b>force</b> キーワードを使用します。<b>force</b> 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。</p>
ステップ 3	<b>(Optional) show username usernamekeypair</b> <b>Example:</b> <pre>switch(config)# show username user1 keypair</pre>	<p>指定したユーザの公開キーを表示します。</p> <p><b>Note</b> 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。</p>
ステップ 4	<b>Required: username username keypair export {bootflash:filename   volatile:filename} {rsa   dsa} [force]</b> <b>Example:</b> <pre>switch(config)# username user1 keypair export bootflash:key_rsa rsa</pre>	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。

	Command or Action	Purpose
		<p>既存のキーを置き換える場合は、<b>force</b> キーワードを使用します。<b>force</b> 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。</p> <p>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 <b>.pub</b> 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 (*<b>.pub</b>) をコピーできるようになります。</p> <p><b>Note</b> 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。</p>
ステップ 5	<p>Required: <b>username username keypair import {bootflash:filename   volatile:filename} {rsa   dsa} [force]</b></p> <p><b>Example:</b></p> <pre>switch(config)# username user1 keypair import bootflash:key_rsa rsa</pre>	<p>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。</p> <p>既存のキーを置き換える場合は、<b>force</b> キーワードを使用します。<b>force</b> 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。</p> <p>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 <b>.pub</b> 拡張子を付けてインポートされます。</p>

	Command or Action	Purpose
		<p><b>Note</b> 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。</p> <p><b>Note</b> 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。</p>

### What to do next

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。



**Note** 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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>[no] feature scp-server</b> <b>Example:</b> <pre>switch(config)# feature scp-server</pre>	Cisco NX-OS デバイス上で SCP サーバをイネーブルまたはディセーブルにします。

	Command or Action	Purpose
ステップ 3	Required: <b>[no] feature sftp-server</b> <b>Example:</b> switch(config)# feature sftp-server	Cisco NX-OS デバイス上で 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	Required: <b>exit</b> <b>Example:</b> 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	(Optional) <b>show running-config security</b> <b>Example:</b> switch# show running-config security	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	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> 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。

## X.509v3 証明書ベースの SSH 認証の設定

X.509v3 証明書を使用する SSH 認証を設定できます。

始める前に

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

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  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	<b>username user-id [password [0   5] password]</b>  例： switch(config)# username jsmith password 4Ty18Rnt	ユーザ アカウントを設定します。 <i>user-id</i> 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



	コマンドまたはアクション	目的
		<p>きますが、ローカルユーザ名では使用できません。</p> <p>ユーザ名の先頭は英数字で始まる必要があります。</p> <p>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 <b>0</b> は、パスワードがクリアテキストであり、<b>5</b> 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 <b>0</b> (クリアテキスト) です。</p> <p>(注) パスワードを指定しなかった場合、ユーザは Cisco NX-OS デバイスにログインできません。</p> <p>(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。</p>
ステップ 3	<p><b>username</b> <i>user-id</i> <b>ssh-cert-dn</b> <i>dn-name</i> <b>{dsa   rsa}</b></p> <p>例 :</p> <pre>switch(config)# username jsmith ssh-cert-dn "/O = ABCcompany, OU = ABC1, emailAddress = jsmith@ABCcompany.com, L = Metropolis, ST = New York, C = US, CN = jsmith" rsa</pre>	<p>既存のユーザアカウント認証に使用する SSH X.509 証明書の識別名と DSA アルゴリズムを指定します。識別名は最大 512 文字で、例に示す形式に従う必要があります。電子メールアドレスと状態がそれぞれ <b>emailAddress</b> と <b>ST</b> に設定されていることを確認します。</p>
ステップ 4	<p><b>[no] crypto ca trustpoint</b> <i>trustpoint</i></p> <p>例 :</p> <pre>switch(config)# crypto ca trustpoint winca switch(config-trustpoint)#</pre>	<p>トラストポイントを設定します。</p> <p>(注) このコマンドの <b>no</b> 形式を使用してトラストポイントを削除する前に、まず <b>delete crl</b> および <b>delete ca-certificate</b> コマンドを使用して、CRL および CA 証明書を削除する必要があります。</p>
ステップ 5	<p><b>crypto ca authenticate</b> <i>trustpoint</i></p> <p>例 :</p>	<p>トラストポイントの CA 証明書を設定します。</p>

	コマンドまたはアクション	目的
	<pre>switch(config-trustpoint)# crypto ca authenticate winca</pre>	<p>(注) CA 証明書を削除するには、トラストポイント コンフィギュレーション モードで <b>delete ca-certificate</b> コマンドを入力します。</p>
ステップ 6	<p>(任意) <b>crypto ca crl request trustpoint bootflash:static-crl.crl</b></p> <p>例 :</p> <pre>switch(config-trustpoint)# crypto ca crl request winca bootflash:crllist.crl</pre>	<p>この項はオプションですが、強く推奨されます。トラストポイントの証明書失効リスト (CRL) を設定します。CRL ファイルは、トラストポイントによって失効した証明書のリストのスナップショットです。このスタティック CRL リストは、認証局 (CA) からデバイスに手動でコピーされます。</p> <p>(注) スタティック CRL は、サポートされている唯一の失効チェック方式です。</p> <p>(注) CRL を削除するには、<b>delete crl</b> コマンドを入力します。</p>
ステップ 7	<p>(任意) <b>show crypto ca certificates</b></p> <p>例 :</p> <pre>switch(config-trustpoint)# show crypto ca certificates</pre>	<p>設定されている証明書またはチェーンと、関連付けられているトラストポイントを表示します。</p>
ステップ 8	<p>(任意) <b>show crypto ca crl trustpoint</b></p> <p>例 :</p> <pre>switch(config-trustpoint)# show crypto ca crl winca</pre>	<p>指定したトラストポイントの CRL リストの内容を表示します。</p>
ステップ 9	<p>(任意) <b>show user-account</b></p> <p>例 :</p> <pre>switch(config-trustpoint)# show user-account</pre>	<p>設定されたユーザアカウントの詳細を表示します。</p>
ステップ 10	<p>(任意) <b>show users</b></p> <p>例 :</p> <pre>switch(config-trustpoint)# show users</pre>	<p>デバイスにログオンしているユーザが表示されます。</p>
ステップ 11	<p>(任意) <b>copy running-config startup-config</b></p> <p>例 :</p>	<p>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。</p>

	コマンドまたはアクション	目的
	switch(config-trustpoint)# copy running-config startup-config	

## レガシー SSH アルゴリズム サポートの設定

レガシー SSH セキュリティ アルゴリズム、メッセージ認証コード (MAC)、キータイプ、および暗号のサポートを設定できます。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 : <pre>switch# configure terminal switch(config)#?</pre>	グローバル 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	(任意) <b>ssh kexalgos [all]</b> 例 : <pre>switch(config)# ssh kexalgos all</pre>	<p>接続ごとのキーの生成に使用されるキー交換方式である、サポートされているすべての <b>KexAlgorithms</b> を有効にするには、<b>all</b> キーワードを使用します。</p> <p>サポートされる KexAlgorithms は次のとおりです。</p> <ul style="list-style-type: none"> <li>• curve25519-sha256</li> <li>• diffie-hellman-group-exchange-sha256</li> <li>• diffie-hellman-group1-sha1</li> </ul> <p>(注) このアルゴリズムは、Cisco NX-OS リリース 9.3(5) 以降ではサポートされていません。SSH クライアントをアップグレードします。</p> <ul style="list-style-type: none"> <li>• diffie-hellman-group14-sha1</li> <li>• diffie-hellman-group1-sha1</li> <li>• ecdh-sha2-nistp256</li> <li>• ecdh-sha2-nistp384</li> <li>• ecdh-sha2-nistp521</li> </ul>

	コマンドまたはアクション	目的
ステップ 3	(任意) <b>ssh macs all</b> 例 : <pre>switch(config)# ssh macs all</pre>	<p>トラフィック変更の検出に使用されるメッセージ認証コードである、サポートされているすべての MAC を有効にします。</p> <p>サポートされる MAC は次のとおりです。</p> <ul style="list-style-type: none"> <li>• hmac-sha1</li> <li>• hmac-sha2-256</li> <li>• hmac-sha2-512</li> </ul>
ステップ 4	(任意) <b>ssh ciphers [ all ]</b> 例 : <pre>switch(config)# ssh ciphers all</pre>	<p>サポートされているすべての暗号を有効にして接続を暗号化するには、<b>all</b> キーワードを使用します。</p> <p>サポート対象の暗号方式 :</p> <ul style="list-style-type: none"> <li>• aes128-cbc</li> <li>• aes192-cbc</li> <li>• aes256-cbc</li> <li>• aes128-ctr</li> <li>• aes192-ctr</li> <li>• aes256-ctr</li> <li>• aes256-gcm@openssh.com</li> <li>• aes128-gcm@openssh.com</li> </ul>
ステップ 5	(任意) <b>ssh keytypes all</b> 例 : <pre>switch(config)# ssh keytypes all</pre>	<p>サーバがクライアントに対して自身を認証するために使用できる公開キー アルゴリズムである、サポートされているすべての PubkeyAcceptedKeyType を有効にします。</p> <p>サポートされるキー タイプは次のとおりです。</p> <ul style="list-style-type: none"> <li>• ecdsa-sha2-nistp256</li> <li>• ecdsa-sha2-nistp384</li> <li>• ecdsa-sha2-nistp521</li> <li>• ssh-dss</li> <li>• ssh-rsa</li> </ul>

## サポートされるアルゴリズム : FIPモードが有効の場合

FIP モードが有効な場合にサポートされるアルゴリズムのリストは次のとおりです。

表 11: サポートされるアルゴリズム : FIPモードが有効の場合

アルゴリズム	サポートあり	Unsupported
ciphers	<ul style="list-style-type: none"> <li>• aes128-ctr</li> <li>• aes256-ctr</li> <li>• aes256-gcm@openssh.com</li> <li>• aes128-gcm@openssh.com</li> </ul>	<ul style="list-style-type: none"> <li>• aes192-ctr</li> <li>• aes128-cbc</li> <li>• aes192-cbc</li> <li>• aes256-cbc</li> </ul>
hmac	<ul style="list-style-type: none"> <li>• hmac-sha2-256</li> <li>• hmac-sha2-512</li> <li>• hmac-sha1</li> </ul>	<ul style="list-style-type: none"> <li>• hmac-sha2-256-ctm@openssh.com</li> <li>• hmac-sha2-512-ctm@openssh.com</li> <li>• hmac-sha1-ctm@openssh.com</li> </ul>
kexalgo	<ul style="list-style-type: none"> <li>• ecdh-sha2-nistp256</li> <li>• ecdh-sha2-nistp384</li> <li>• ecdh-sha2-nistp521</li> <li>• diffie-hellman-group16-sha512</li> <li>• diffie-hellman-group14-sha1</li> <li>• diffie-hellman-group14-sha256</li> </ul>	<ul style="list-style-type: none"> <li>• curve25519-sha256</li> <li>• curve25519-sha256@libssh.org</li> </ul>
keytypes	<ul style="list-style-type: none"> <li>• rsa-sha2-256</li> <li>• ecdsa-sha2-nistp256</li> <li>• ecdsa-sha2-nistp384</li> <li>• ecdsa-sha2-nistp521</li> </ul>	ssh-rsa

## デフォルトの SSH サーバポートの変更

Cisco NX-OS Cisco リリース 9.2(1) 以降では、SSHv2 のポート番号をデフォルトのポート番号 22 から変更できます。デフォルトの SSH ポートの変更時に使用される暗号化により、より強力なプライバシーとセッション整合性をサポートする接続が実現します。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>no feature ssh</b> 例 : <pre>switch(config)# no feature ssh</pre>	SSH をディセーブルにします。
ステップ 3	<b>show sockets local-port-range</b> 例 : <pre>switch(config)# show sockets local port range (15001 - 58000) switch(config)# local port range (58001 - 63535) and nat port range (63536 - 65535)  switch# show sockets local-port-range  Kstack local port range (15001 - 22002) Netstack local port range (22003 - 65535)</pre>	使用可能なポート範囲を表示します。
ステップ 4	<b>ssh port local-port</b> 例 :	ポートを設定します。

	コマンドまたはアクション	目的
	<code>switch(config)# ssh port 58003</code>	<p>(注) 以前のリリースからリリース 9.3(1)以降のリリースにアップグレードする場合は、ユーザ定義の SSH ポートを使用する機能が次の範囲内にあることを確認してください。</p> <ul style="list-style-type: none"> <li>リリース 9.3(1) およびリリース 9.3(2) の場合： Kstack ローカルポートの範囲は 15001 ～ 58000、netstack ローカルポートの範囲は 58001 ～ 63535、nat ポートの範囲は 63536 ～ 65535</li> <li>リリース 9.3(3) 以降： Kstack ローカルポートの範囲は 15001 ～ 58000、netstack ローカルポートの範囲は 58001 ～ 60535、nat ポートの範囲は 60536 ～ 65535</li> </ul>
ステップ 5	<p><b>feature ssh</b></p> <p>例： <code>switch(config)# feature ssh</code></p>	SSH をイネーブルにします。
ステップ 6	<p><b>exit</b></p> <p>例： <code>switch(config)# exit</code> <code>switch#</code></p>	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	<p>(任意) <b>show running-config security all</b></p> <p>例： <code>switch# ssh port 58003</code></p>	セキュリティの設定を表示します。
ステップ 8	<p>(任意) <b>copy running-config startup-config</b></p> <p>例： <code>switch# copy running-config startup-config</code></p>	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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>clear ssh hosts</b> <b>Example:</b> 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

Cisco NX-OS では、デフォルトで SSH サーバが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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	<b>no feature ssh</b> <b>Example:</b> switch(config)# no feature ssh	SSH をディセーブルにします。
ステップ 3	<b>exit</b> <b>Example:</b> 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	(Optional) <b>show ssh server</b> <b>Example:</b> switch# show ssh server	SSH サーバの設定を表示します。
ステップ 5	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> 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。



## 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。



**Note** 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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	<b>no feature ssh</b> <b>Example:</b> switch(config)# no feature ssh	SSH をディセーブルにします。
ステップ 3	<b>no ssh key[dsa  rsa  ecdsa]</b> <b>Example:</b> 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	<b>exit</b> <b>Example:</b> 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	(Optional) <b>show ssh key</b> <b>Example:</b> switch# show ssh key	SSH サーバ キーの設定を表示します。
ステップ 6	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> 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。

### Related Topics

[SSH サーバ キーの生成](#) (155 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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>show users</b> <b>Example:</b> switch# show users	ユーザセッション情報を表示します。
ステップ 2	<b>clear line vty-line</b> <b>Example:</b> 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 サーバのイネーブル化

Cisco NX-OS デバイス上で Telnet サーバを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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	<b>feature telnet</b> <b>Example:</b> 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	<b>exit</b> <b>Example:</b> 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	(Optional) <b>show telnet server</b> <b>Example:</b> switch# show telnet server	Telnet サーバの設定を表示します。

	Command or Action	Purpose
ステップ 5	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch# copy running-config startup-config</pre>	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。

### Before you begin

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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>telnet</b> { <i>ipv4-address</i>   <i>host-name</i> } [ <i>port-number</i> ] [ <b>vrf</b> <i>vrf-name</i> ]  <b>Example:</b> <pre>switch# telnet 10.10.1.1</pre>	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	<b>telnet6</b> { <i>ipv6-address</i>   <i>host-name</i> } [ <i>port-number</i> ] [ <b>vrf</b> <i>vrf-name</i> ]  <b>Example:</b> <pre>switch# telnet6 2001:0DB8::ABCD:1 vrf management</pre>	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。

### Related Topics

[Telnet サーバのイネーブル化](#) (174 ページ)

## Telnet セッションのクリア

Cisco NX-OS デバイスから Telnet セッションをクリアできます。

### Before you begin

Cisco NX-OS デバイス上で Telnet サーバをイネーブルにします。

## Procedure

	Command or Action	Purpose
ステップ 1	<b>show users</b> <b>Example:</b> switch# show users	ユーザ セッション情報を表示します。
ステップ 2	<b>clear line vty-line</b> <b>Example:</b> 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
<b>show ssh key [dsa   rsa] [md5]</b>	SSH サーバ キーを表示します。  Cisco NX-OS リリース 7.0(3)I4(6) および 7.0(3)I6(1) 以降のリリースでは、このコマンドはデフォルトで SHA256 形式でフィンガープリントを表示します。SHA256 は、以前のデフォルトの MD5 形式よりも安全です。ただし、フィンガープリントを MD5 形式で表示する必要がある場合の下位互換性のために、 <b>md5</b> オプションが追加されています。
<b>show running-config security [all]</b>	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。 <b>all</b> キーワードを指定すると、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。
<b>show ssh server</b>	SSH サーバの設定を表示します。
<b>show telnet server</b>	Telnet サーバの設定を表示します。
<b>show username usernamekeypair</b>	指定したユーザの公開キーを表示します。
<b>show user-account</b>	設定されたユーザ アカウントの詳細を表示します。
<b>show users</b>	デバイスにログオンしているユーザが表示されます。
<b>show crypto ca certificates</b>	X.509v3 証明書ベースの SSH 認証に設定された CA 証明書および関連するトラストポイントを表示します。
<b>show crypto ca crl trustpoint</b>	指定したトラストポイントの CRL リストの内容を表示します。

# 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。

## Procedure

**ステップ 1** SSH サーバをディセーブルにします。

### Example:

```
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。

### Example:

```
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。

### Example:

```
switch(config)# feature ssh
```

**ステップ 4** SSH サーバ キーを表示します。

### Example:

```
switch(config)# show ssh key
could not retrieve dsa key information
*****
rsa Keys generated:Tue Mar 14 13:13:47 2017

ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDh4+DZboQJbJt10nJhgKBYL5l0lhsFM2oZRi9+JqEU
GA44I9ej+E5NIRZ1x8ohIt6Vx9Et5cs07Pw72rjUwR3UPmuAm79k7I/SyLGEP3WUL7sqbLvNF5GqKXph
oqMT075WUdbGWphorA2g0tTObRrFIQBjVQ0SSBh3oEaaALqYUQ==

bitcount:1024
fingerprint:
SHA256:V6KAeLAIKRRUPBZmlYq3rl6JW7Eo7vhLi6CXYxD/+Y
*****
*****
```

**ステップ 5** OpenSSH 形式の SSH 公開キーを指定します。

### Example:

```
switch(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAEAy19oF6QaZ19G+3f1XswK3OiW4H7YyUyuA50r
v7gsEPjhOBYmsi6PAVKuilnIf/DQhum+1JNqJP/eLowb7ubO+1VKRXYF/G+1JNlIQ
W3g9igG30c6k6+XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmSiH3UD/vKyziEh5
```

```
4Tplx8=
```

**ステップ 6** 設定を保存します。

**Example:**

```
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。

**Procedure**

**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。

**Example:**

```
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。

**Example:**

```
switch(config)# show username admin keypair

*****

rsa Keys generated: Thu Jul  9 11:10:29 2013

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAxWmjJT+oQhIcvnrMbx2BmD0P8boZE1TfJ
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。

**Example:**

```
switch(config)# username admin keypair export bootflash:key_rsa rsa
Enter Passphrase:
switch(config)# dir
.
.
.
          951      Jul 09 11:13:59 2013  key_rsa
          221      Jul 09 11:14:00 2013  key_rsa.pub
.
.
```

**ステップ 4** これら 2 つのファイルを他の Cisco NX-OS デバイスへコピーした後、**copy scp** または **copy sftp** コマンドを使用して、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。

**Example:**

```
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 2013

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAxWmjJT+oQhIcVnrMbx2BmD0P8boZE1TfJ
Fx9fexWp6rOiztlwODtehnjadWc6A+DE2DvYNvqsrU9TByyYDPQkR/+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。

**Example:**

```
$ 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** (Optional) DSA キーについてこの手順を繰り返します。

## X.509v3 証明書ベースの SSH 認証の設定例

次の例は、X.509v3 証明書を使用する SSH 認証の設定方法を示しています。

```
configure terminal
username jsmith password 4Ty18Rnt
username jsmith ssh-cert-dn "/O = ABCcompany, OU = ABC1,
emailAddress = jsmith@ABCcompany.com, L = Metropolis, ST = New York, C = US, CN = jsmith"
  rsa
crypto ca trustpoint tp1
crypto ca authenticate tp1
crypto ca crl request tp1 bootflash:crl1.crl

show crypto ca certificates
Trustpoint: tp1
CA certificate 0:
subject= /CN=SecDevCA
issuer= /CN=SecDevCA
serial=01AB02CD03EF04GH05IJ06KL07MN
notBefore=Jun 29 12:36:26 2016 GMT
notAfter=Jun 29 12:46:23 2021 GMT
SHA1 Fingerprint=47:29:E3:00:C1:C1:47:F2:56:8B:AC:B2:1C:64:48:FC:F4:8D:53:AF
purposes: sslserver sslclient

show crypto ca crl tp1
Trustpoint: tp1 CRL: Certificate Revocation List (CRL):
  Version 2 (0x1)
  Signature Algorithm: sha1WithRSAEncryption
  Issuer: /CN=SecDevCA
  Last Update: Aug 8 20:03:15 2016 GMT
  Next Update: Aug 16 08:23:15 2016 GMT
  CRL extensions:
    X509v3 Authority Key Identifier:
      keyid:30:43:AA:80:10:FE:72:00:DE:2F:A2:17:E4:61:61:44:CE:78:FF:2A

show user-account
user:user1
  this user account has no expiry date
  roles:network-operator
  ssh cert DN : /C = US, ST = New York, L = Metropolis, O = cisco , OU = csg, CN
= user1; Algo: x509v3-sign-rsa

show users
NAME      LINE      TIME          IDLE          PID          COMMENT
user1     pts/1     Jul 27 18:43  00:03         18796        (10.10.10.1)  session=ssh
```

## 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 ライセンス ガイド



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 9000 Series NX-OS Unicast Routing Configuration Guide』

**RFC**

RFC	タイトル
<a href="#">RFC 6187</a>	『X.509v3 Certificates for Secure Shell Authentication』

**MIB**

MIB	MIB のリンク
SSH および Telnet に関連する MIB	サポートされている 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。 <a href="ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html">ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html</a>





## 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。

- [PKI の概要, on page 183](#)
- [PKI の注意事項と制約事項 \(188 ページ\)](#)
- [PKI のデフォルト設定, on page 189](#)
- [CA の設定とデジタル証明書, on page 189](#)
- [PKI の設定の確認, on page 205](#)
- [PKI の設定例, on page 206](#)
- [PKI に関する追加情報, on page 242](#)

## 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 の公開キーを認識する必要があります。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 デバイスでは、デバイス上に多くのトラストポイントを置くことができ、デバイス上のすべてのアプリケーションは、任意のトラストポイント CA によって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。



**Note** 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 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。CRL、NDcPP:OCSP for Syslog、なし、またはこれらの方式の組み合わせを指定できます。

## 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。

## NDcPP : syslog の OCSP

ピアが失効情報を取得し、この情報を検証して証明書失効のステータスを確認する場合、Online Certificate Status Protocol (OCSP) は証明書失効を確認するための方式になります。この方式では、証明書失効のステータスは、クラウドを介して OCSP 応答者に到達するピアの能力、または証明書失効情報を検索する際の証明書送信者の能力によって制限されます。

リモート syslog サーバが OCSP レスポンダ URL を持つ証明書を共有すると、クライアントはサーバ証明書を外部 OCSP レスポンダ (CA) サーバに送信します。CA サーバはこの証明書を検証し、有効な証明書か失効した証明書かを確認します。この場合、クライアントは失効した証明書リストをローカルに保持する必要はありません。

## 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 リリース 9.3 (5) 以降では、Cisco NX-OS ソフトウェアは NDcPP: OCSP for Syslog をサポートしています。



(注) Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

## 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。

Table 12: 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
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

## 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。

**Caution**

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。

**Procedure**

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	<b>hostname hostname</b> <b>Example:</b> switch(config)# hostname DeviceA	デバイスのホスト名を設定します。
ステップ 3	<b>ip domain-name name [use-vrf vrf-name]</b> <b>Example:</b> 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	<b>exit</b> <b>Example:</b> switch(config)# exit switch#	設定モードを終了します。
ステップ 5	(Optional) <b>show hosts</b> <b>Example:</b> switch# show hosts	IP ドメイン名を表示します。
ステップ 6	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> 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。

## 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。

Cisco NX-OS リリース 9.3(3) 以降では、Cisco NX-OS デバイスをトラストポイント CA に関連付ける前に、明示的に RSA キーペアを生成する必要があります。Cisco NX-OS リリース 9.3(3) よりも前では、使用できない場合、RSA キーペアは自動生成されます。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>crypto key generate rsa [label label-string] [exportable] [modulus size]</b> <b>Example:</b> <pre>switch(config)# crypto key generate rsa exportable</pre>	<p>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。</p> <p>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。</p> <p>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。</p> <p><b>Note</b> 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。</p> <p>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。</p> <p><b>Caution</b> キー ペアのエクスポートの可否は変更できません。</p>
ステップ 3	<b>exit</b> <b>Example:</b> <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 4	(Optional) <b>show crypto key mypubkey rsa</b> <b>Example:</b>	作成したキーを表示します。

	Command or Action	Purpose
	<code>switch# show crypto key mypubkey rsa</code>	
ステップ 5	<p>(Optional) <b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch# copy running-config startup-config</pre>	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。

### Before you begin

RSA キーペアを作成します。

### Procedure

	Command or Action	Purpose
ステップ 1	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>switch# configure terminal switch(config)#</pre>	グ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	<p><b>crypto ca trustpoint name</b></p> <p><b>Example:</b></p> <pre>switch(config)# crypto ca trustpoint admin-ca switch(config-trustpoint)#</pre>	<p>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。</p> <p><b>Note</b> 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。</p>
ステップ 3	<p><b>enrollment terminal</b></p> <p><b>Example:</b></p> <pre>switch(config-trustpoint)# enrollment terminal</pre>	<p>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せん。</p> <p><b>Note</b> 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。</p>

	Command or Action	Purpose
ステップ 4	<b>rsa keypair label</b> <b>Example:</b> <pre>switch(config-trustpoint)# rsa keypair SwitchA</pre>	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。 <b>Note</b> 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	<b>exit</b> <b>Example:</b> <pre>switch(config-trustpoint)# exit switch(config)#</pre>	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	<b>(Optional) show crypto ca trustpoints</b> <b>Example:</b> <pre>switch(config)# show crypto ca trustpoints</pre>	トラストポイントの情報を表示します。
ステップ 7	<b>(Optional) copy running-config startup-config</b> <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	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。

### Related Topics

[RSA キー ペアの生成](#) (190 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力し、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。



### Note

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。

**Before you begin**

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。

**Procedure**

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>crypto ca authenticate name</b> <b>Example:</b> <pre>switch(config)# crypto ca authenticate admin-ca input (cut &amp; paste) CA certificate (chain) in PEM format; end the input with a line containing only END OF INPUT : -----BEGIN CERTIFICATE----- MIIChQCoygWIFgICWDSiazCZPESRLjkOzejABjckkicwOPQLEAOB KEDjB4CCSGSib3UEFARFwLhrRzUbjxNjy5j20CzABjMEFAPKID MRtEAYDQDEWILXUxRa2EjAQBNMFACTUhrndhGyZIKMAGALIE CMFQ2Iz28EzABjMFAStGfchNO3Hz2LHEjABjNEMICLWAXLISED QIpe%0NtAImMjQmcbFw0wZAIMMjUIMtchMTCQSAhgkKzIhxdN AQERhVfZGhQQnc2MmNk3EIMWGALEBMSU4EjAQBNMFACTUth cnfndCFYIESMFALEBmQrRzZFS3JIMQ4LDAYDQDEWDAxjzEIMBEG AILECMRtVc3RcnfZIESMFALEBmQDEhrndhENBRwDQkKzIhxdN AQEBQAD3AASAEFwW7b3HXIEPNSIHZLhNcM5YpzcrcNXOMeRXXI CzEAgjXIZAFSLQQLiMhRc/4ljfRwXKysCvEFAcBzCBALBjMHQ8E FMAc6iDMDRUPQH/BULjwEB/zcBjNMQERGLUjyJdMbrQMR20jRQ GjvIHEvawDF0BQQWjAucYgfoCa#R0DovL3NZS0wC9DXORW5j2s I0FwXUUSjMNHnNjDawo0GjLYqnlSzi0vLxcc3NIIA4ENLcrFbnV h3cQ8hrmfhJLhQEh3UMFAGCSGQjBjCAGQDgFAMAGCSGSib3QjEB EQIAP0EAH6Qd8E399TwwFqGQgNLJqHhARCI0eyt/WGpZksf9Ea 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</pre>	<p>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。</p> <p>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。</p> <p><b>Note</b> 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。</p>
ステップ 3	<b>exit</b> <b>Example:</b> <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 4	<b>(Optional) show crypto ca trustpoints</b> <b>Example:</b> <pre>switch# show crypto ca trustpoints</pre>	トラストポイント CA の情報を表示します。

	Command or Action	Purpose
ステップ 5	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch# copy running-config startup-config</pre>	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。

### Related Topics

[トラストポイント CA のアソシエーションの作成](#) (192 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。

### Before you begin

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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>crypto ca trustpoint name</b>  <b>Example:</b> <pre>switch(config)# crypto ca trustpoint admin-ca switch(config-trustpoint)#</pre>	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	<b>revocation-check {crl [none]   none}</b>  <b>Example:</b> <pre>switch(config-trustpoint)# revocation-check none</pre>	証明書取消確認方法を設定します。デフォルトの方式は <b>crl</b> 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。

	Command or Action	Purpose
ステップ 4	<b>exit</b> <b>Example:</b> <pre>switch(config-trustpoint)# exit switch(config)#</pre>	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	(Optional) <b>show crypto ca trustpoints</b> <b>Example:</b> <pre>switch(config)# show crypto ca trustpoints</pre>	トラストポイント CA の情報を表示します。
ステップ 6	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	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。

#### Related Topics

[CA の認証](#) (193 ページ)

[CRL の設定](#) (202 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。

#### Before you begin

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。

#### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グ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	<b>crypto ca enroll name</b> <b>Example:</b>	認証した CA に対する証明書要求を作成します。



	Command or Action	Purpose
	<pre>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----- MIIBzCCARQAwIEEgCAIEAwRMA4GA1UEAww5ajc2b2wzDjEj KzIhcnVpQHEBQDgOMIGPocGALBY1UA2NC7jU1D6MqNlgZt8r14IK 0U0AnN4qs8VAMZSIL74JjZw6kIDTysrjuCXgjoWj0Ehw/5IT9y E2NU8omcShvEzG7ysVPMKczh5pj+argzHGG9IXtq4WMSK2w8S VgHD8AgBAGjtzABgqjkiC9ABQxCBQomZMTzMDCCSgSib3QET DjgMcwQDRCRQH/BswGTRVMA4GA1UEAww5ajc2b2wzDjEjKzIh KzIhcnVpQHEBQDgOMIGPocGALBY1UA2NC7jU1D6MqNlgZt8r14IK PftaWUE/pwGhayQ2T3ccqvel2L5L33EE2kEXiI6U88nDjgIMjja8 8a23NDp8v6kWA9WwL8NUZEFKqjfrgENIZacU88zqKMetKytU0- -----END CERTIFICATE REQUEST-----</pre>	<p><b>Note</b> 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。</p>
ステップ 3	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>switch(config-trustpoint)# exit switch(config)#</pre>	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	<p>(Optional) <b>show crypto ca certificates</b></p> <p><b>Example:</b></p> <pre>switch(config)# show crypto ca certificates</pre>	CA 証明書を表示します。
ステップ 5	<p>(Optional) <b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch(config)# copy running-config startup-config</pre>	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。

### Related Topics

[トラストポイント CA のアソシエーションの作成 \(192 ページ\)](#)

## 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。

### Before you begin

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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>crypto ca import name certificate</b> <b>Example:</b> <pre>switch(config)# crypto ca import admin-ca certificate input (cut &amp; paste) certificate in PEM format: -----BEGIN CERTIFICATE----- MIIEADCCAgwGByqGKj00QAAAAADABjchkiG9wCgQEAAD0B4DjYB4G C3gS1b3DQEPRFRWlhrRZLBJaXjy5j20kCAEgNEMVAKIOMREFAAD VQIBLILYXUjAa2EjEjAQBjMFAcIUUhrdHbG9ZIEOMAGALUChMQZ1z Y28zABEgNEMVAsIhZlbnN3ZmVjAQBjMFAcIUUhrdHbG9ZIEOMAGALU NIEBMTwzANBaw0wNjEwMTwzANBawGjAVBjNEMVEMZlZ2FzLUEU Y21z28i29hMIGMA0GCSqGSIb3DQEBAQAAQDkiQBgQC/GNAQzjQ4IC dQlWkjSjSICpLk5eJhNQCjQpauKsZEPjE2LuiyeCEBylrdwYGE8a77 qlxr42/si9IRIb/8uLU/cj9jSSB456ca7wVA8ndE6jMChIM4lva/cp4Qb x7RifdJ06FqfZEjsl7/Elad9LxwIDQAB4ICEaCAg8wQDdFQFqH/EBSv GjTRwMhMwM55jaXjy5j20kZHEwH6ImHQDdFQOHEHEKLi+2sqwBEfjR hWmVyc9jrgMIMBjNHSBjQjgcCpFCc8eAD6wJIEBvjSkUBlFhxwGw plGIMICQSwHgKfZlhxvNQCBEHhVVRZGzIQjpc2NinNtEIMAKALU EhMCSUjEjAQBjMFAcIUUhrdHbG9ZIEEMFAALUEBwMQhrZ2R3sJIMQ4w DADQQBwDANjzEIMBEGALUECMh0Vc3RvcmFhZIESMFAALUEBwMQBEh cmhTEBjAFNkHjQZIE9EiMRLA6GALUHWRM5wLqscCqFGHdFA6 Iy8z2UMDgQ2VydUcm8stC9BGFjbnEIMjE0S5jcmwMFAUCjGhrqj3U6 Iy8xHNEZS0wCEBEXORv5jb2s8SERWXXUSUMENInjDDBigZlhwWBBQH AQEFjBMDsGCCGQUBzAhi9odRwOi8vc3NlITp4L0NlcjRbnjkb3wcc3Nl LlP4XOfwXXUSUMENInjdA9BgrBjEgEQwAolzhnlSzlBzLkcc3NlLlP4 XENlcjRbnjkb3wcc3NlITp4XOfwXXUSUMENInjdABjchkiG9wCgQEAQ AAEAD0B4G8he7Nl9eCtMBhr24K6ZSjDQrOZLUlqprllkPyejtsyflw E36cI2u4WsExREqxibTk8ycx7V5o= -----END CERTIFICATE-----</pre>	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。
ステップ 3	<b>exit</b> <b>Example:</b> <pre>switch(config)# exit switch#</pre>	設定モードを終了します。

	Command or Action	Purpose
ステップ 4	(Optional) <b>show crypto ca certificates</b>  <b>Example:</b> switch# show crypto ca certificates	CA 証明書を表示します。
ステップ 5	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> 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。

**Related Topics**

[トラストポイント CA のアソシエーションの作成 \(192 ページ\)](#)

## 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。

**Note**

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せん。

**Related Topics**

[PKCS 12 形式でのアイデンティティ情報のエクスポート \(200 ページ\)](#)

## 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。



**Note** 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。

### Before you begin

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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>crypto ca export name pkcs12 bootflash:filename password</b> <b>Example:</b> <pre>switch(config)# crypto ca export admin-ca pkcs12 bootflash:adminid.p12 nbv123</pre>	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	<b>exit</b> <b>Example:</b> <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 4	<b>copy bootflash:filename scheme://server/ [url /]filename</b> <b>Example:</b> <pre>switch# copy bootflash:adminid.p12 tftp:adminid.p12</pre>	PKCS#12 形式のファイルをリモートサーバにコピーします。  <i>scheme</i> 引数に対しては、 <b>tftp:</b> 、 <b>ftp:</b> 、 <b>scp:</b> 、または <b>sftp:</b> を入力できます。 <i>server</i> 引数は、リモートサーバのアドレスまたは名前であり、 <i>url</i> 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。

	Command or Action	Purpose
		<i>server</i> 、 <i>url</i> 、および <i>filename</i> の各引数は、大文字小文字を区別して入力します。

#### Related Topics

[RSA キー ペアの生成](#) (190 ページ)

[CA の認証](#) (193 ページ)

[アイデンティティ証明書のインストール](#) (198 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。



**Note** インポートの URL を指定するときには使用できるのは、`bootflash:filename` という形式だけです。

#### Before you begin

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 がい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。

#### Procedure

	Command or Action	Purpose
ステップ 1	<b>copy <i>scheme</i>:// <i>server</i>[<i>url</i> /]<i>filename</i></b> <b>bootflash:<i>filename</i></b>  <b>Example:</b> <pre>switch# copy tftp:adminid.p12 bootflash:adminid.p12</pre>	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。  <i>scheme</i> 引数に対しては、 <b>tftp:</b> 、 <b>ftp:</b> 、 <b>scp:</b> 、または <b>sftp:</b> を入力できます。 <i>server</i> 引数は、リモートサーバのアドレスまたは名前であり、 <i>url</i> 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。  <i>server</i> 、 <i>url</i> 、および <i>filename</i> 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	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーションモードを開始します。

	Command or Action	Purpose
ステップ 3	<b>crypto ca import name pkcs12</b> <b>bootflash:filename</b>  <b>Example:</b> <pre>switch(config)# crypto ca import admin-ca pkcs12 bootflash:adminid.p12 nbv123</pre>	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	<b>exit</b>  <b>Example:</b> <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 5	(Optional) <b>show crypto ca certificates</b>  <b>Example:</b> <pre>switch# show crypto ca certificates</pre>	CA 証明書を表示します。
ステップ 6	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch# copy running-config startup-config</pre>	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。

### Before you begin

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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>copy scheme:[//server/[url /]]filename</b> <b>bootflash:filename</b>  <b>Example:</b> <pre>switch# copy tftp:adminca.crl bootflash:adminca.crl</pre>	リモートサーバから CRL をダウンロードします。  <i>scheme</i> 引数に対しては、 <b>tftp:</b> 、 <b>ftp:</b> 、 <b>scp:</b> 、または <b>sftp:</b> を入力できます。 <i>server</i> 引数は、リモートサーバのアドレスまたは名前であり、 <i>url</i> 引数はリモー

	Command or Action	Purpose
		トサーバにあるソース ファイルへのパスです。  <i>server</i> 、 <i>url</i> 、および <i>filename</i> 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	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>crypto ca crl request name bootflash:filename</b>  <b>Example:</b> <pre>switch(config)# crypto ca crl request admin-ca bootflash:adminca.crl</pre>	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	<b>exit</b>  <b>Example:</b> <pre>switch(config)# exit switch#</pre>	設定モードを終了します。
ステップ 5	(Optional) <b>show crypto ca crl name</b>  <b>Example:</b> <pre>switch# show crypto ca crl admin-ca</pre>	CA の CRL 情報を表示します。
ステップ 6	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch# copy running-config startup-config</pre>	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。

## Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>crypto ca trustpoint name</b> <b>Example:</b> <pre>switch(config)# crypto ca trustpoint admin-ca switch(config-trustpoint)#</pre>	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	<b>delete ca-certificate</b> <b>Example:</b> <pre>switch(config-trustpoint)# delete ca-certificate</pre>	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	<b>delete certificate [force]</b> <b>Example:</b> <pre>switch(config-trustpoint)# delete certificate</pre>	<p>アイデンティティ証明書を削除します。</p> <p>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、<b>force</b> 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。</p>
ステップ 5	<b>exit</b> <b>Example:</b> <pre>switch(config-trustpoint)# exit switch(config)#</pre>	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	(Optional) <b>show crypto ca certificates [name]</b> <b>Example:</b> <pre>switch(config)# show crypto ca certificates admin-ca</pre>	CA の証明書情報を表示します。
ステップ 7	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	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、現在は使用されてい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。



**Note** 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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	<b>crypto key zeroize rsa label</b> <b>Example:</b> switch(config)# crypto key zeroize rsa MyKey	RSA キー ペアを削除します。
ステップ 3	<b>exit</b> <b>Example:</b> switch(config)# exit switch#	設定モードを終了します。
ステップ 4	(Optional) <b>show crypto key mypubkey rsa</b> <b>Example:</b> switch# show crypto key mypubkey rsa	RSA キー ペアの設定を表示します。
ステップ 5	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> 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。

### Related Topics

[証明書要求の作成](#) (196 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
<code>show crypto key mypubkey rsa</code>	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。
<code>show crypto ca certificates</code>	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。
<code>show crypto ca crl</code>	CA の CRL についての情報を表示します。
<code>show crypto ca trustpoints</code>	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。



**Note** 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。

### Procedure

**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-----
MIIC4jCCAoygAwIBAgIQBWDsiay0GzRPSRI1jK0ZejanBgkqhkiG9w0BAQUFADCB
kDEgMB4GCSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAk1O
MRIwEAYDVQQIEw1LYXJuYXRha2ExEjAQBGNVBAcTCUJhbmdbhG9yZTEOMAwGA1UE
ChMFQ21zY28xEzARBGNVBAStCm5ldHN0b3JhZ2UxEjAQBGNVBAMTCUFWYXJuYSBD
QTAEFw0wNTA1MDMyMjQ2MzdaFw0wNzA1MDMyMjU1MTdaMTGQMSAwHgYJKoZIhvcN
AQkBFhFhbWVfuZGt1QGNpc2NvLmNvbTELMakGA1UEBhMCSU4xEjAQBGNVBAgTCUth
cm5hdGFrYTESMBAGA1UEBxMJQmFuZ2Fsb3JlMQ4wDAYDVQQKEwVdaXNjbzETMBEG
A1UECmMKbmV0c3RvcnFnZTESMBAGA1UEAxMjQXBhcm5hIENBMFwwDQYJKoZIhvcN
AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHzluNccNM87ypyzwuoSNZXOMpeRXXI
OzyBAgiXT2ASFuUOwQ1iDM8rO/41jf8RxxvYKvysCAwEAooBvzCBvDALBgNVHQ8E
BAMCAYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyJyRoMbrCNMRU2OyRhQ
GgsWBHEwawYDVR0fBGQwYjAuoCygKoYoaHR0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJuYYSUyMENBLmNybdAwOC6gLIYqZmlsZTovL1xccc3NlLTA4XEN1cnRFbnJv
bGxcQXBhcm5hJTIwQ0EuY3JsMBAGCSsGAQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEB
BQUAA0EAAHv6UQ+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-----
MIIBqzCCARQCAQAwHDEaMBGGA1UEAxMRVnYXNjby5jb20wgZ8wDQYJ
KoZlIhvcNAQEBBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVA5mQNIgJ2kt8r14lKY
0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnJuCXGvjb+wj0hEhv/y51T9y
P2NJ8orngShrvFZgC7ysN/PyMwKcgzhbVpp+rargZvHtGJ91XTq4WoVksCzXv8S
VqyH0vEvAgMBAAAGTzAVBgkqhkiG9w0BCQcxCBMGBmJ2MTIzMDYGCsGGSIB3DQeJ
DjEpmCcwJQYDVR0RAQH/BBswGYIRVnYXNjby5jb22HBKwWH6IwDQYJ
KoZlIhvcNAQEBBQADgYEAkt60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99G1FWgt
PfrNcWUE/pw6HayfQ12T3ecgNwe12d15133YBF2bktExiI6U188nTOjg1XMjja8
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-----
MIIEADCCA6qgAwIBAgIKCj00oQAAAAAdDANBgkqhkiG9w0BAQUFADCBBkDEgMB4G
CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xZAJBGNVBAYTAKlOMRIWEAYD
VQQIEW1lYXNjby5jb20wgZ8wDQYJ
KoZlIhvcNAQEBBQADgY0AMIGJAoGBAL8Y1UAJ2NC7jUJ1DVA5mQNIgJ2kt8r14lKY
0JC6ManNy4qxk8VeMXZSiLJ4JgTzKWdxbLDkTTysnJuCXGvjb+wj0hEhv/y51T9y
P2NJ8orngShrvFZgC7ysN/PyMwKcgzhbVpp+rargZvHtGJ91XTq4WoVksCzXv8S
VqyH0vEvAgMBAAAGTzAVBgkqhkiG9w0BCQcxCBMGBmJ2MTIzMDYGCsGGSIB3DQeJ
DjEpmCcwJQYDVR0RAQH/BBswGYIRVnYXNjby5jb22HBKwWH6IwDQYJ
KoZlIhvcNAQEBBQADgYEAkt60KER6Qo8nj0sDXZVHSfJZh6K6JtDz3Gkd99G1FWgt
PfrNcWUE/pw6HayfQ12T3ecgNwe12d15133YBF2bktExiI6U188nTOjg1XMjja8
8a23bNDpNsM8rklwA6hWkrVL8NUZEFJxqbjfngPNTZacJCUS6ZqKCMetbKytUx0=
-----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。

---

#### Related Topics

[CA ??????????](#) (209 ページ)

[??????????????](#) (215 ページ)

## CA ??????????

Microsoft Certificate Service ? Web ?????????? CA ??????????????????????????????

## Procedure

---

- ステップ 1 Microsoft Certificate Services ? Web ??????????[Retrieve the CA certificate or certificate revocation task] ??????[Next] ?????????

*Microsoft* Certificate Services -- Apama CA

### Welcome

---

You use this web site to request a certificate for your web browser, e-mail client, or other software. You will be able to securely identify yourself to other people over the web, sign your e-mail messages, and encrypt data 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
-

ステップ 2 ?????????????????? CA ??????????????[Base 64 encoded] ??????[Download CA certificate] ??????????

Microsoft Certificate Services -- Aparna CA

### Retrieve The CA Certificate Or Certificate Revocation List

[Install this CA certification path](#) to allow your computer to trust certificates issued from t

It is not necessary to manually install the CA certification path if you request and install a  
CA certification path will be installed for you automatically.

#### Choose file to download:

CA Certificate:

DER encoded or  Base 64 encoded

[Download CA certificate](#)

[Download CA certification path](#)

[Download latest certificate revocation list](#)

## ステップ 3 [File Download] ?????????? [Open] ??????????

**Microsoft** Certificate Services -- Aparna CA

### Retrieve The CA Certificate Or Certificate Revocation List

[Install this CA certification path](#) to allow your computer to trust certificates issued from this

It is not necessary to manually install the CA. The CA certification path will be installed for you.

**Choose file to download:**  
 CA Certificate:


DER encoded or  Base64 encoded

[Download CA certificate](#)  
[Download CA certification path](#)  
[Download latest certificate revocation list](#)

**File Download**

Some files can harm your computer. If the file information looks suspicious, or you do not fully trust the source, save this file.

File name: certnew.cer  
 File type: Security Certificate  
 From: 10.76.45.108

 This type of file could harm your computer if it contains malicious code.

Would you like to open the file or save it to your computer?

Always ask before opening this type of file.



ステップ 4 [Certificate] ???????????? [Copy to File] ???????[OK] ??????????

The screenshot shows the Microsoft Certificate Services console for 'Aparna CA'. The main page is titled 'Retrieve The CA Certificate Or Certificate Revocation List'. It includes instructions on installing the CA certification path and a section for choosing a file to download. The 'Choose file to download' section shows 'Current [Aparna CA]' selected. Below this are three download links: 'Download CA certificate', 'Download CA certificate', and 'Download latest certificate'. On the right, a 'Certificate' dialog box is open, showing the 'Certification Path' tab. The dialog displays a table of certificate fields and their values.

Field	Value
Version	V3
Serial number	0560 D289 ACB4 1994 4F4
Signature algorithm	sha1RSA
Issuer	Aparna CA, netstorage, C
Valid from	04 Mei 2005 4:16:37
Valid to	04 Mei 2007 4:25:17
Subject	Aparna CA, netstorage, C
Public key	RSA (512 Bits)

ステップ 5 [Certificate Export Wizard] ?????????? [Base-64 encoded X.509 (.CER)] ??????[Next] ??????????

The screenshot displays the Microsoft Certificate Services console for 'Aparna CA'. The main window shows the 'Retrieve The CA Certificate Or Certificate Revocation List' page. A 'Certificate Export Wizard' dialog box is overlaid on top. The wizard has three tabs: 'General', 'Details', and 'Certification Path'. The 'Export File Format' section is active, showing options for exporting certificates. The 'Base-64 encoded X.509 (.CER)' option is selected. Other options include 'DER encoded binary X.509 (.CER)', 'Cryptographic Message Syntax S...', and 'Personal Information Exchange -'. There are checkboxes for 'Include all certificates in the c...', 'Enable strong protection (req...', and 'Delete the private key if the e...'. The background page has a 'Choose file to download:' section with a dropdown menu showing 'Current [Aparna CA]' and several download links.

ステップ 6 [Certificate Export Wizard] ?????????? [File name:] ??? ??????????????????????[Next] ??????????

ステップ 7 [Certificate Export Wizard] ??????????[Finish] ??????????

ステップ 8 Microsoft Windows ? type ??????????Base-64?PEM???????????? CA ??????????

```

C:\WINNT\system32\cmd.exe
D:\testcerts>type aparnaCA.cer
-----BEGIN CERTIFICATE-----
MIIC4jCCAoYgAwIBAgIQBWD5iaY0GZRPSRI1jK0ZeJANBgkqhkiG9w0BAQUFADCB
kDEgMB4GCSqGSIb3DQEJARYRYW1hbMRRZUBjaXNjb3Y5jb20xCzAIBgNVBAYTAk10
MRIwEAYDUQIEdwLLYXJ1eXRha2EwEjAQBgNVBAcTCUJhbmdhG9yZTEOMAEGA1UE
ChMFQ21zY28xEzARBgNVBAstCm5ldHN0b3JhZ2UxEjAQBgNVBAMTCUFWYXJuYSBD
QTAEFw0wNTA1MDMyMjQzMzdaFw0wNzA1MDMyMjU1MTdaMIGQMSAwHgYJKoZIhvcN
AQkBFHhFhbWwZGt1QGNpc2NvLmNvbTElMAkGA1UEBhMCSU4xEjAQBgNVBAgTCUth
cm5hdGFrYTESMBAGA1UEBjxMjQmFuZ2FsY3JlMQ4wDAYDUQKKEwJDAKNjBzETMBEG
A1UECXMkQmU0c3RvcnFnZTESMBAGA1UEAxMjQXBhcm5hIENBMFwwDQYJKoZIhvcN
AQEBBQADSwAwSAJBAMW/7b3+DXJPANBsIHHZluNccNM87yppyzwuoSNZXOMpeRXXI
OzyBAgiXT2ASFuU0wQ1iDM8rO/41jf8RxxvYKvysCAwEAAaOBvzCBvDALBgNVHQ8E
BAMCAcYwDwYDUR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJyJyRoMbrCNMRU2OyRhQ
GgsWbHEwawYDUR0fBGQwYjAuOCygKoYoahr0cDovL3NzZS0wOC9DZXJ0RW5yb2xs
L0FwYXJuYSUyMENBLmNybDAwOC6gLIYqZmlsZTouL1xc3NlITA4XENlcnRFbnJu
bGxcQXBhcm5hJT1wQ0EuY3JsMBAAGCSsGAQQBgjcVAQQAQgEAMAA0GCSqGSIb3DQEB
BQUAA0EAHv6UQ+8nE399Tww+KaGr0g0NIJaNgLh0AFcT0rEyuyt/WYGPzksF9Ea
NBG7E0oN66zex0EOEfG1Us6mXp1//w==
-----END CERTIFICATE-----
D:\testcerts>

```

??????????????

PKCS#12 ???????CSR????? Microsoft Certificate ???

## Procedure

ステップ 1 Microsoft Certificate Services ? Web ??????????[Request a certificate] ??????[Next] ?????????

*Microsoft* Certificate Services -- Apama CA

### Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other software. You will be able to securely identify yourself to other people over the web, sign your e-mail messages, and encrypt data 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

ステップ 2 [Advanced request] ??????[Next] ??????

**Microsoft** Certificate Services -- Aparna CA

### Choose Request Type

Please select the type of request you would like to make:

User certificate request:

Web Browser Certificate

E-Mail Protection Certificate

Advanced request

??????????????

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] ??????[Next] ????????

Microsoft Certificate Services -- Aparna CA

### Advanced Certificate Requests

You can request a certificate for yourself, another user, or a computer using one of the following methods. Your certification authority (CA) will determine the certificates that you can obtain.

- Submit a certificate request to this CA using a form.
- Submit a certificate request using a base64 encoded PKCS #10 file or a renewal request using a base64 encoded PKCS #7 file.
- Request a certificate for a smart card on behalf of another user using the Smart Card Enrollment Wizard. *You must have an enrollment agent certificate to submit a request for another user.*

ステップ 4 [Saved Request] ???? ??????base64 ? PKCS#10 ??????????????[Next] ????????????????? Cisco NX-OS  
????????????????????

Microsoft Certificate Services -- Aparna CA

---

### Submit A Saved Request

Paste a base64 encoded PKCS #10 certificate request or PKCS #7 renewal request (server) into the request field to submit the request to the certification authority (CA).

**Saved Request:**

Base64 Encoded Certificate Request (PKCS #10 or #7):

```
VqyHOvEvAgMBAAGgTzAVBgkqhkiG9w0BCQexCBMG
DjEpMCcwJQYDVRORAQH/BBswGYIRVmVnYXMtMS5j
KoZIHvcNAQEEBQADgYEAKT6OKER6Qo8nj0sDXZVH
PftrNcWUE/pw6HayfQ12T3ecgNwe12d15133YBF2
8a23bNDpNsM8rk1wA6hWkrVL8NUZEFJxqbjfngPN
-----END CERTIFICATE REQUEST-----
```

[Browse](#) for a file to insert.

**Additional Attributes:**

Attributes:

## ステップ 5 CA ?????????????????????????????? 1 ? 2 ???????

Microsoft Certificate Services -- Apama CA

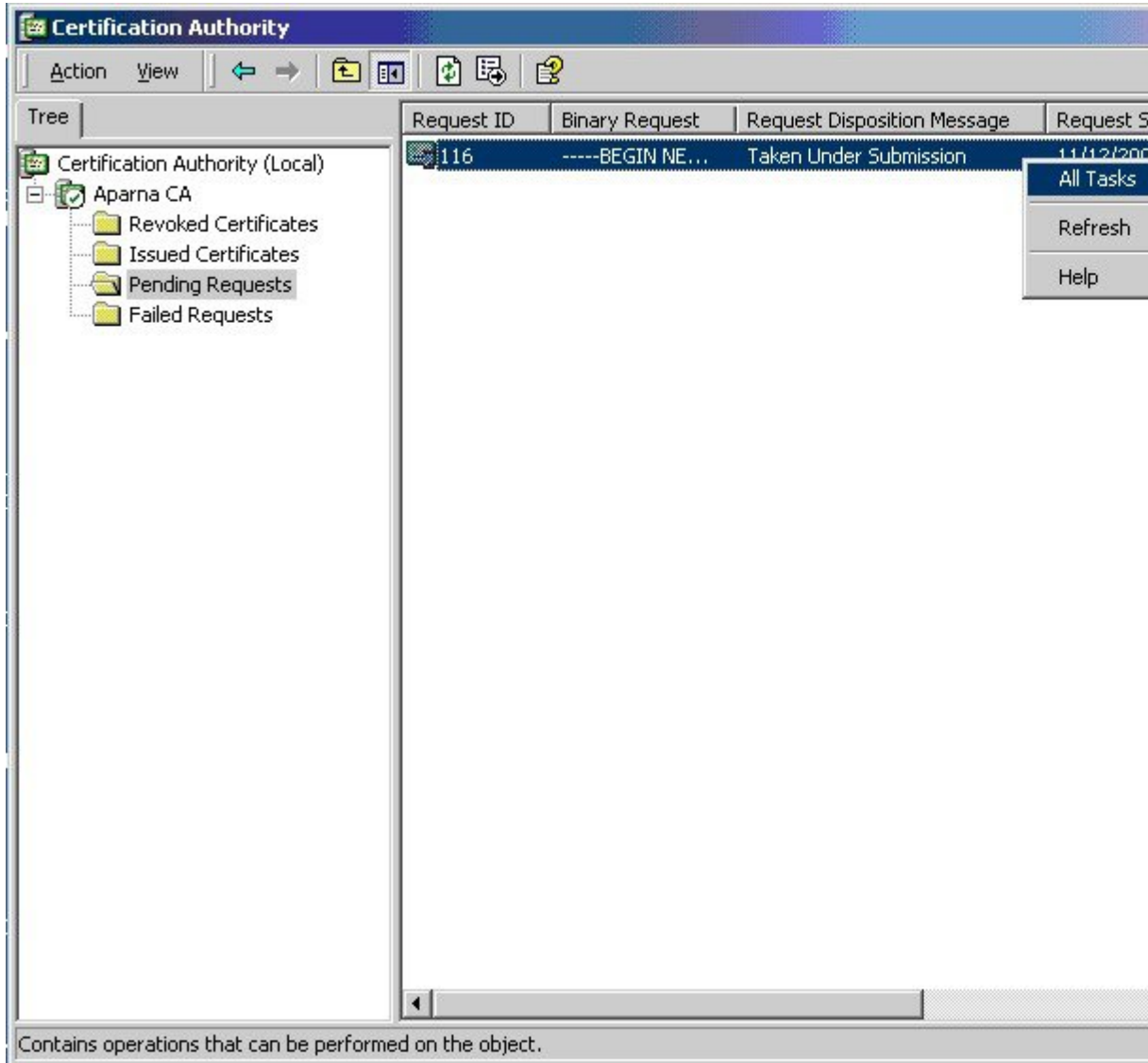
### Certificate Pending

Your certificate request has been received. However, you must wait for an administrator to approve your request. Please return to this web site in a day or two to retrieve your certificate.

**Note:** You must return with **this** web browser within 10 days to retrieve your certificate



ステップ 6 CA ???



ステップ 7 Microsoft Certificate Services ? Web ??????????[Check on a pending certificate] ??????[Next] ?????????

*Microsoft* Certificate Services -- Apama CA

## Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other software. You will be able to securely identify yourself to other people over the web, sign your e-mail messages, and encrypt data, 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

ステップ 8 ??????????????????[Next] ??????????

**Microsoft** Certificate Services -- Aparna CA

### Check On A Pending Certificate Request

Please select the certificate request you want to check:

Saved-Request Certificate (12 Nopember 2005 20:30:22)

ステップ 9 [Base 64 encoded] ???????[Download CA certificate] ????????

**Microsoft** Certificate Services -- Aparna CA

### Certificate Issued

The certificate you requested was issued to you.

DER encoded or  Base 64 encoded



[Download CA certificate](#)

[Download CA certification path](#)

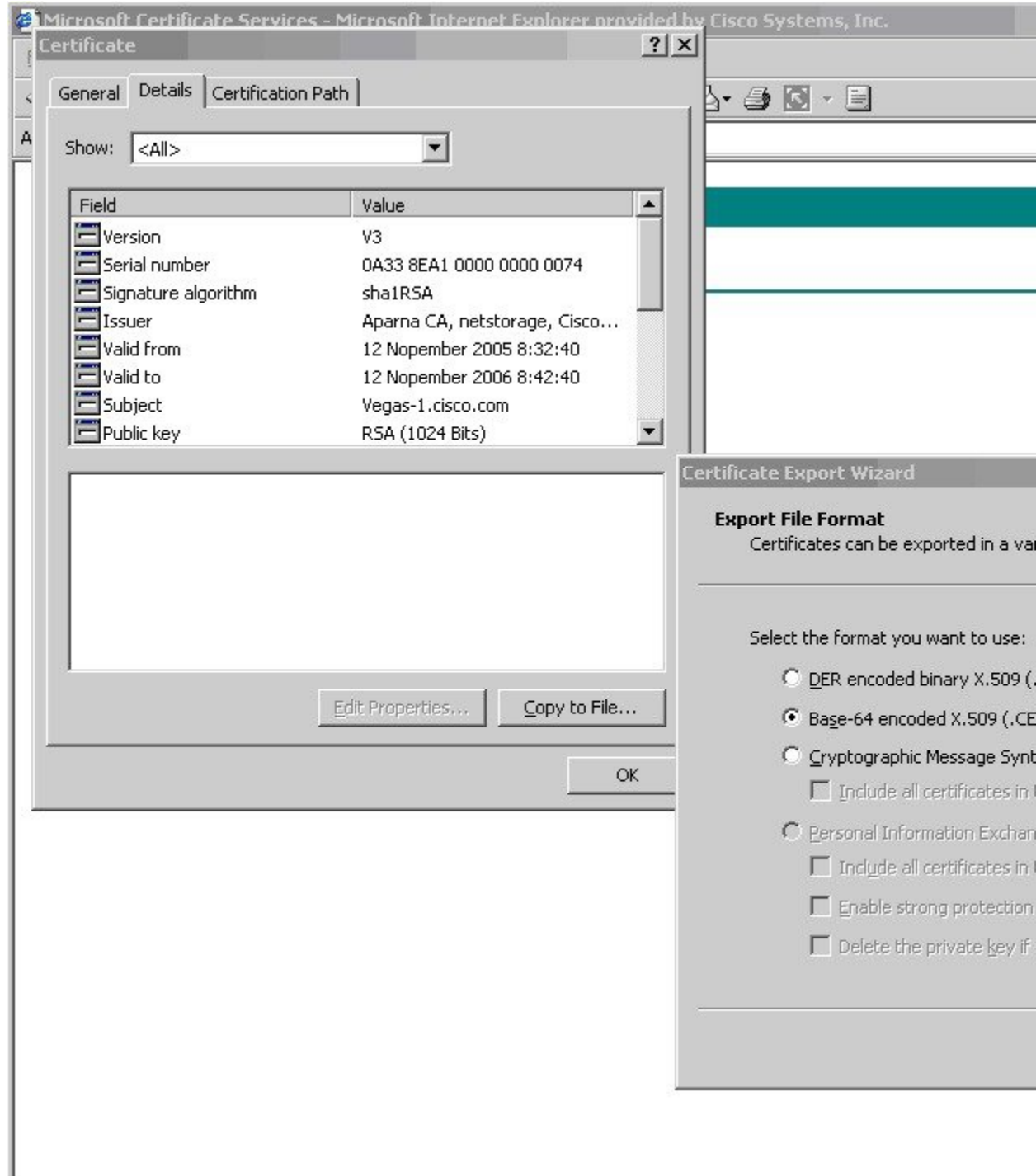
ステップ 10 [File Download] ???????????[Open] ???????????

The screenshot shows a web browser window with the title bar "Microsoft Certificate Services -- Aparna CA". The main content area displays "Certificate Issued" and the message "The certificate you requested was issued to you." Below this, there are two radio buttons: "DER encoded" (unselected) and "Base 64" (selected). To the left of the radio buttons is a small icon of a certificate. Below the radio buttons are two blue links: "Download CA certificate" and "Download CA certification path".

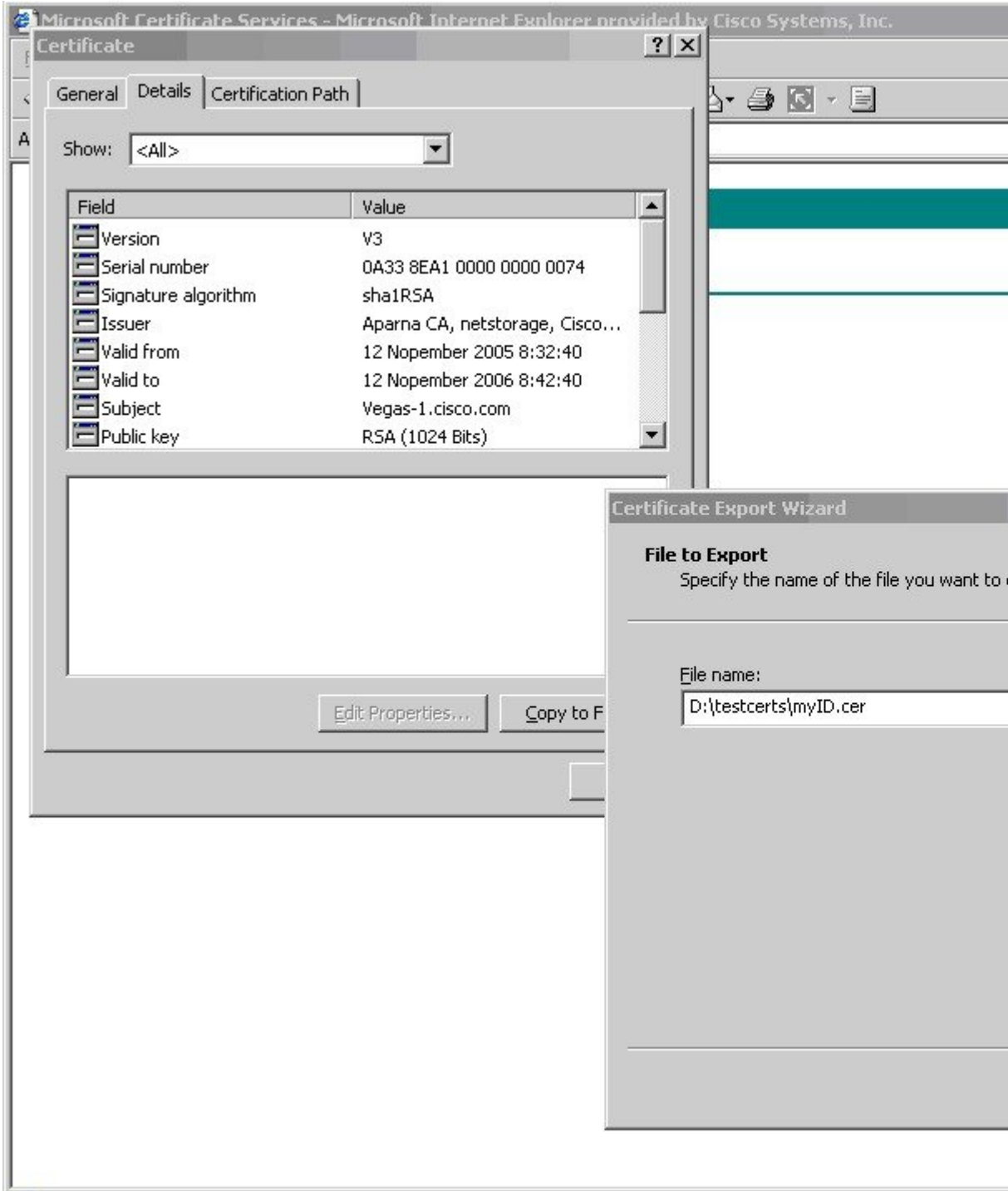
Overlaid on the right side of the browser window is a "File Download" dialog box. The dialog box has a question mark icon and the text: "Some files can harm your computer. If the file information looks suspicious, or you do not fully trust the source, save this file." Below this text, the following information is displayed: "File name: certnew.cer", "File type: Security Certificate", and "From: 10.76.45.108". A yellow warning triangle icon is followed by the text: "This type of file could harm your computer if it contains malicious code." At the bottom of the dialog box, there are three buttons: "Open", "Save", and "Cancel". Below the buttons is a checked checkbox with the text: "Always ask before opening this type of file".

??????????????

ステップ 11 [Certificate] ?????[Details] ??????[Copy to File...] ??????[Certificate Export Wizard] ??????[Base-64 encoded X.509 (.CER)] ??????[Next] ??????

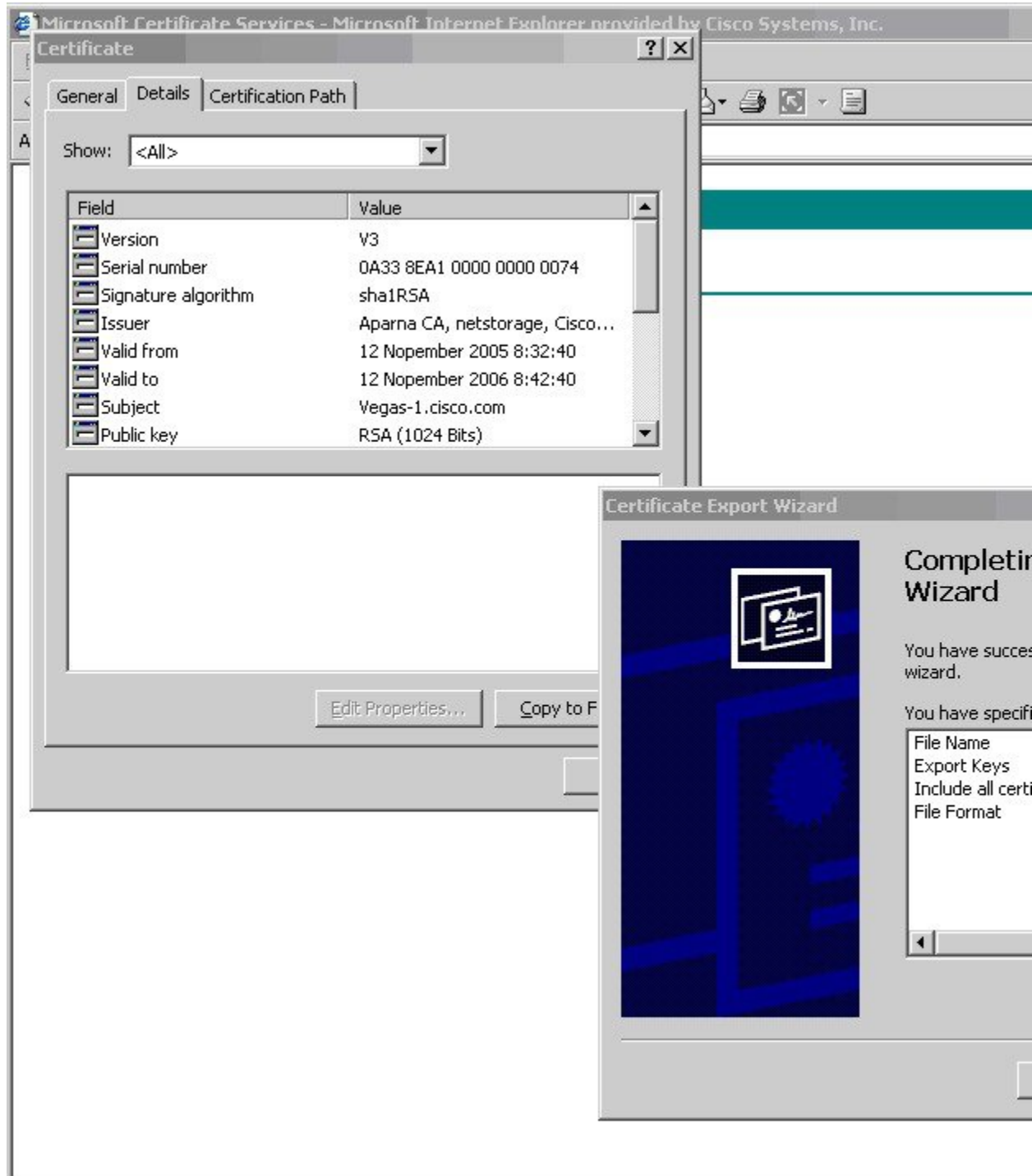


ステップ 12 [Certificate Export Wizard] ?????????? [File name:] ??? ????[Next] ????????



??????????????

## ステップ 13 [Finish] ??????????





ステップ 14 Microsoft Windows ? type ?????????????????????? Base-64 ??????????????????????

```

C:\WINNT\system32\cmd.exe
D:\testcerts>type myID.cer
-----BEGIN CERTIFICATE-----
MIIEADCCA6ggAwIBAgIKCj00oQAAAAAAAAdDANBgkqhkiG9w0BAQUFADCBkDEgMB4G
CSqGSIb3DQEJARYRYW1hbmRrZUBjaXNjby5jb20xCzAJBgNVBAYTAk1OMRIwEAYD
UQqIEwLLYXJuYXRha2ExEjAQBGNVBAcTUJhbmdbG9yZTEOMAwGA1UEChMFQ2Iz
Y28xEzARBGNVBAcTUc5LdHN0b3JhZ2UxEjAQBGNVBAMTUFwYXJuYSBDQTAeFw0w
NTEyMTIwMzA5NDBaFw0wNjExMTIwMzE5NDBaMBwxCjAyaYBgNVBAMTEUZZL2FzLT
EuY2IzY28uY29tMIgMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC/GNUACd.jQu41C
dQ1WkjkjSICdpLfK5eJSmNCQujGpzcukS ZPFxjF2Uo iyeCYE8ylnCwYw5E08rJ47
gLxr42/sI9IRIb/8udU/cj9jSSfKK56koa7xWYAu8rDfz8jMCnIM4W1aY/q2q4Gb
x7RifdV06uFqFZEgs17/Elash9LxLwIDAQABo4ICEzCCAg8wJQYDUR0RAQH/BBsw
GYIRUUnYXMTMS5.jaXNjby5jb22HbKwWH6IwHQYDUR00BBYEFKCLi+2sspWEfgrR
bhWmLUyo9jngMIHMBGnVHSMEGcQwgcGAFCCo8kaDG6wjTEUNjskYUBoLFmxcoYGW
pIGTMIQMSAwHgYJKoZl hvCNAQkBFhFhbWfuZGtLQGNpc2NvLmNvbTlELMakGA1UE
BhMCSU4xEjAQBGNVBAcTUthcm5hdGFrYTESMBA GA1UEBxMJQmFuZ2Fsb3JlMQ4w
DAYDUQQKEwUDaXNjbzETMBEGA1UECXMkQmV0c3RvcmlhZDZESMBA GA1UEAxMJQXBh
cm5hIENBghAFYnKJRlQZLE9JEiWMrR16MGsGA1UdHwRkMGIwLQAsoCqGKgh0dHA6
Ly9zc2UtMDgvQ2VudEUC9sbC9BcGFybmELMjBDRS5jcmwwMKAuoCygKkZpbGU6
Ly9cXHNzZS0wOFxkZXJ0RW5yb2xsXEFwYXJuYXUyMENDLmNyYDCCBgYIKwYBBQUH
AQEEfjB8MDsGCCsGAQUFBzAChi9odHRwOi8vc3NLLTA4L0NlcnRFbnJvbGwvc3NL
LTA4X0FwYXJuYXUyMENDLmNyYDCCBgYIKwYBBQUH AQEEfjB8MDsGCCsGAQUFBzAChi
9odHRwOi8vc3NLLTA4X0FwYXJuYXUyMENDLmNyYDCCBgYIKwYBBQUH AQEEfjB8MDs
GAQUFBzAChi9odHRwOi8vc3NLLTA4X0FwYXJuYXUyMENDLmNyYDCCBgYIKwYBBQUH
AANBADbGBGsbe7GNLh9xeOTWBNbm24U69ZSUDDc0cUZUUTgrpnTqVpPyejtsyfLw
E36cI Zu4WsExREgxbTk8ycx7V5o=
-----END CERTIFICATE-----

D:\testcerts>

```

Related Topics

- [証明書要求の作成 \(196 ページ\)](#)
- [Cisco NX-OS デバイスでの証明書の設定 \(206 ページ\)](#)

????????

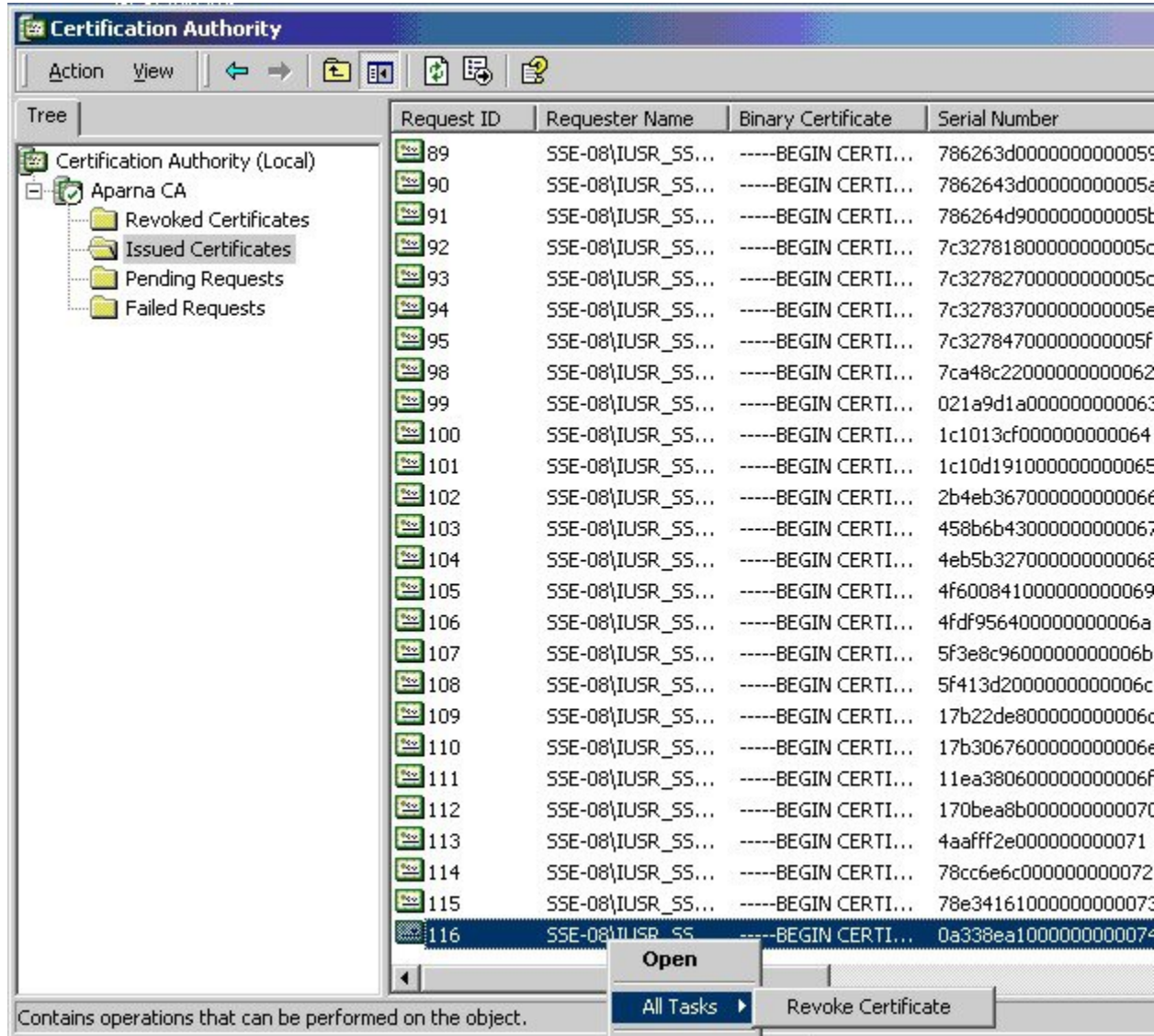
Microsoft CA ??????????????????????

Procedure

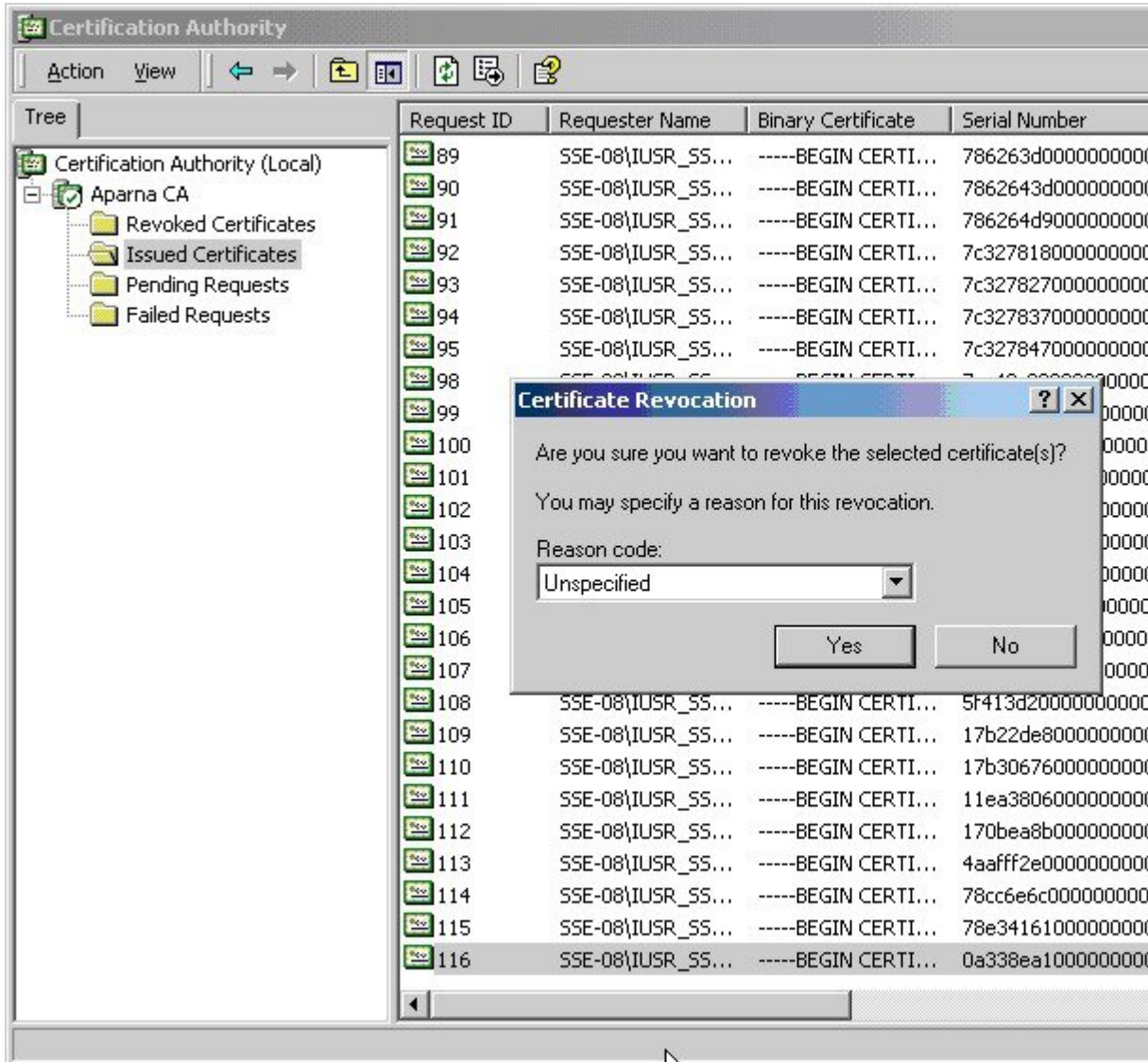
ステップ 1 [Certification Authority] ??????[Issued Certificates] ??????????????????????

????????

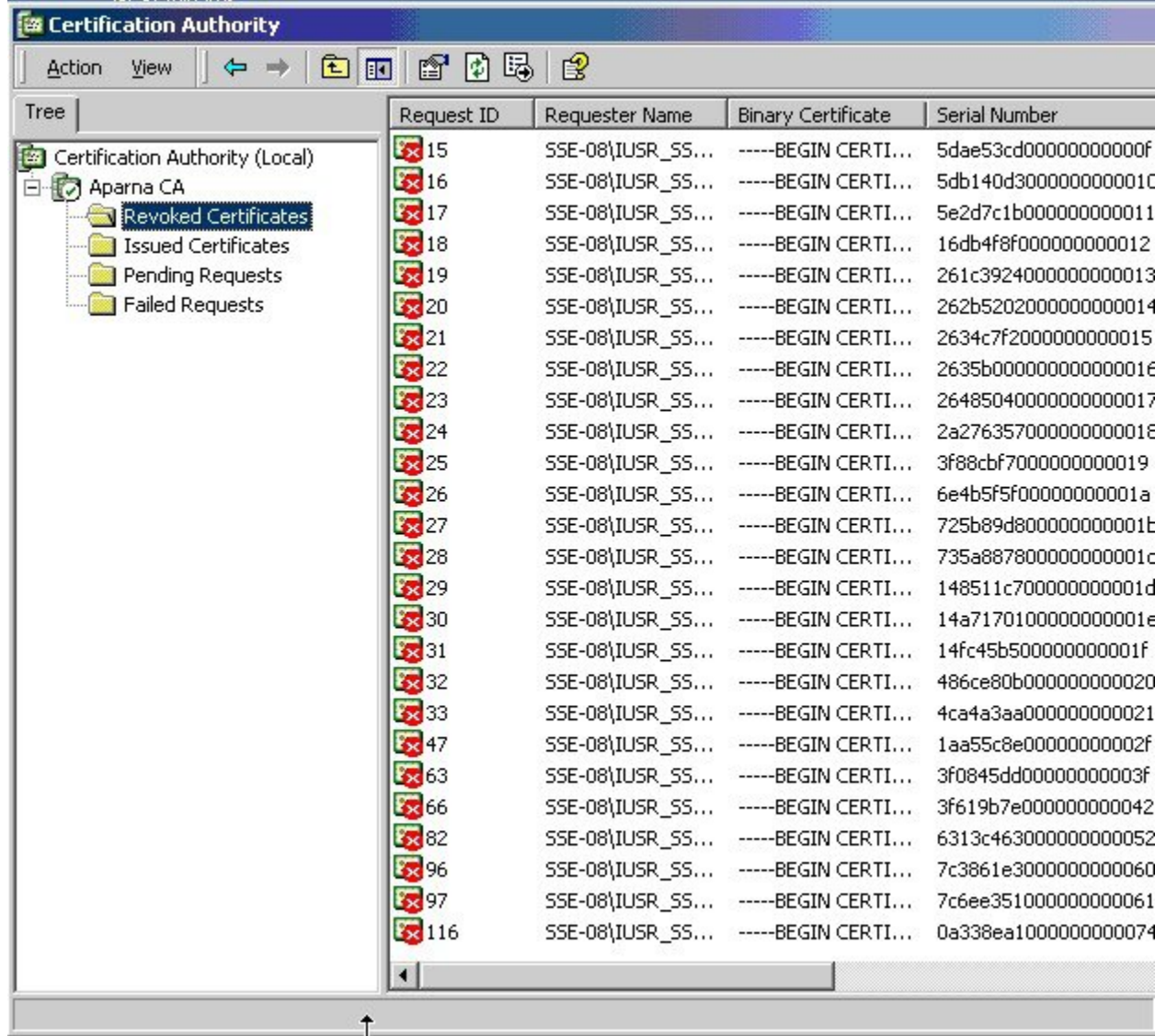
ステップ 2 [All Tasks] &gt; [Revoke Certificate] ??????????



ステップ 3 [Reason code] ?????? ?????????????????[Yes] ?????????



ステップ 4 [Revoked Certificates] ???



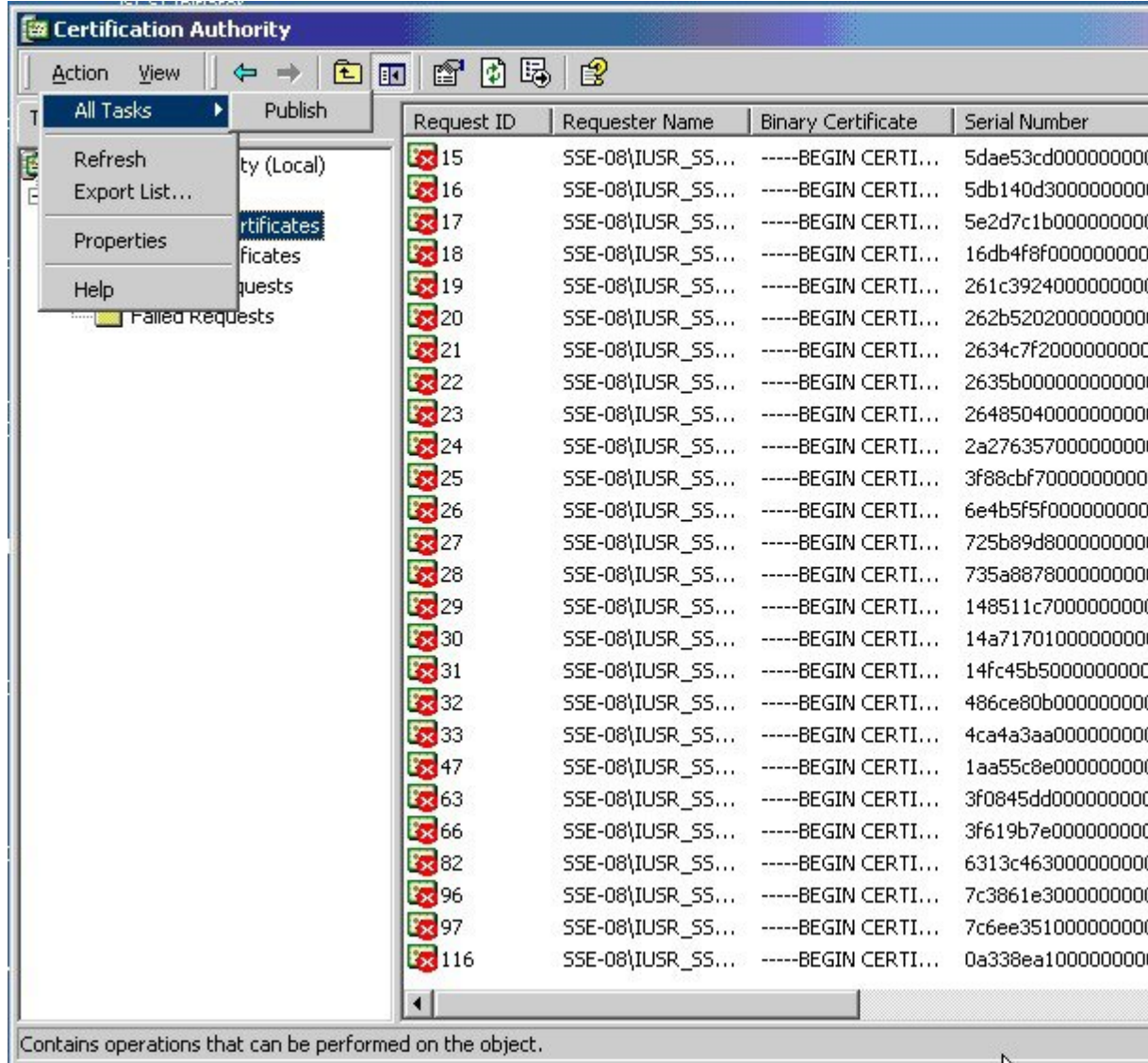
CRL ??????

Microsoft CA ???????????? CRL ?????????????????????????????

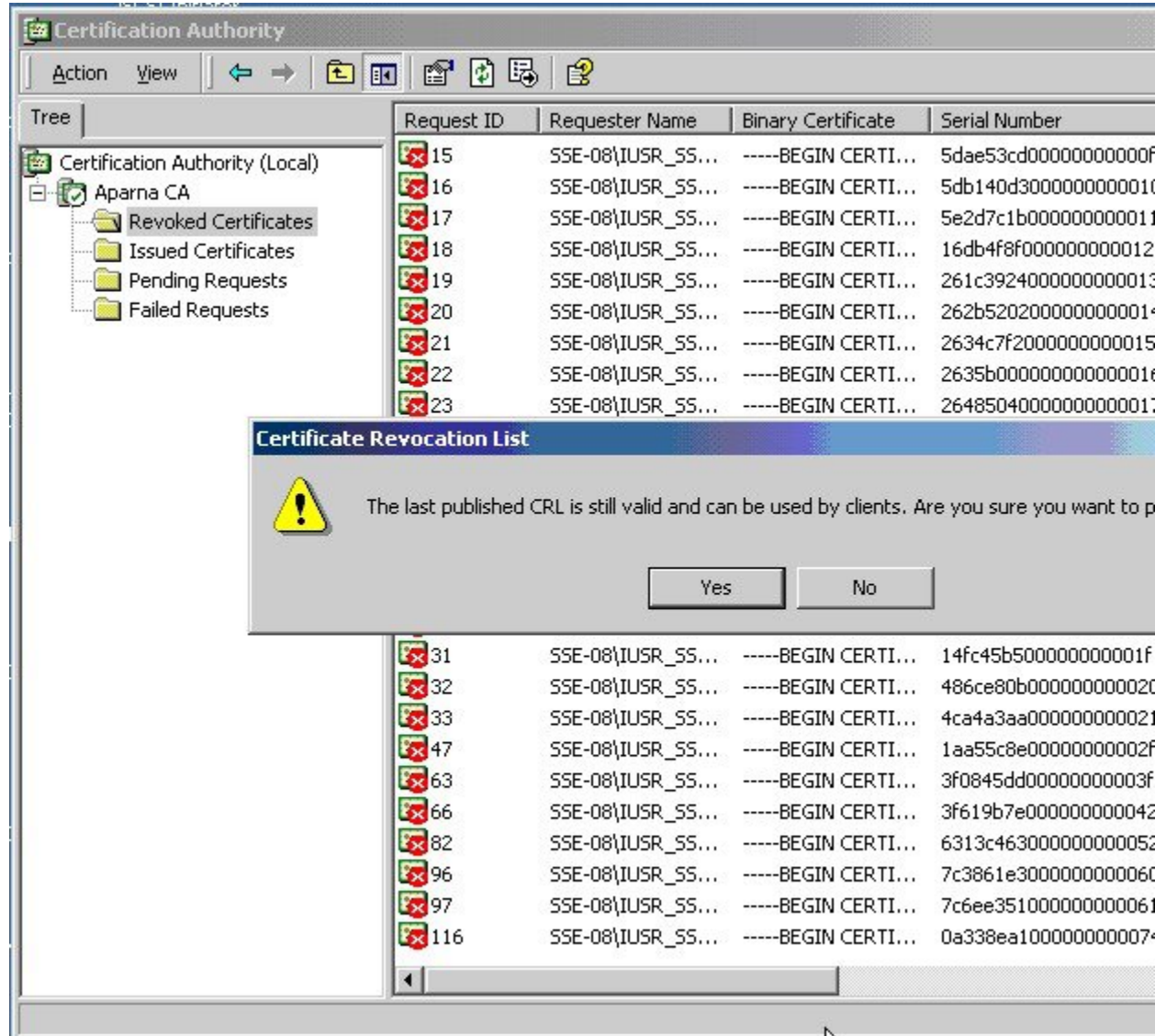


## Procedure

ステップ 1 [Certification Authority] ??????[Action] > [All Tasks] > [Publish] ??????????



ステップ 2 [Certificate Revocation List] ??????????[Yes] ?????????? CRL ???????



## CRL ???????

Microsoft ?? CA ? Web ????? CRL ?????????????????????????????????

## Procedure

- ステップ 1 Microsoft Certificate Services ? Web ?????????? [Retrieve the CA certificate or certificate revocation list] ??????? [Next] ??????????

*Microsoft* Certificate Services -- Aparna CA

### Welcome

You use this web site to request a certificate for your web browser, e-mail client, or other application. You will be able to securely identify yourself to other people over the web, sign your e-mail messages, and encrypt data 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

## ステップ 2 [Download latest certificate revocation list] ?????????

Microsoft Certificate Services -- Aparna CA

### Retrieve The CA Certificate Or Certificate Revocation List

[Install this CA certification path](#) to allow your computer to trust certificates issued from this

It is not necessary to manually install the CA certification path if you request and install a c  
CA certification path will be installed for you automatically.

#### Choose file to download:

CA Certificate:

DER encoded or  Base 64 encoded

[Download CA certificate](#)

[Download CA certification path](#)

[Download latest certificate revocation list](#)



## ステップ 3 [File Download] ??????????[Save] ??????????

The screenshot shows a web browser window titled "Microsoft Certificate Services -- Aparna CA". The main heading is "Retrieve The CA Certificate Or Certificate Revocation List". Below this, there is a link: "Install this CA certification path to allow your computer to trust certificates issued from t".

Text on the page: "It is not necessary to manually install the CA. The CA certification path will be installed for you."

**Choose file to download:**  
CA Certificate:

DER encoded or  Base64 encoded

[Download CA certificate](#)  
[Download CA certification path](#)  
[Download latest certificate](#)

Overlaid on the right is a "File Download" dialog box with a warning icon and the text: "Some files can harm your computer. If the file information looks suspicious, or you do not fully trust the source, save this file." The dialog shows the following details:

- File name: certcr1.crl
- File type: Certificate Revocation List
- From: 10.76.45.108

At the bottom of the dialog, it asks: "Would you like to open the file or save it to your computer?" with buttons for "Open", "Save", and "Cancel". There is a checked checkbox for "Always ask before opening this type of file".





```
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: 5349AD46000000000000A
      Revocation Date: Jun 27 23:47:22 2005 GMT
      CRL entry extensions:
        X509v3 CRL Reason Code:
          CA Compromise
    Serial Number: 53BD173C000000000000B
      Revocation Date: Jul 4 18:04:01 2005 GMT
      CRL entry extensions:
        X509v3 CRL Reason Code:
          Certificate Hold
    Serial Number: 591E7ACE000000000000C
      Revocation Date: Aug 16 21:53:15 2005 GMT
    Serial Number: 5D3FD52E000000000000D
      Revocation Date: Jun 29 22:07:25 2005 GMT
      CRL entry extensions:
        X509v3 CRL Reason Code:
          Key Compromise
    Serial Number: 5DAB7713000000000000E
      Revocation Date: Jul 14 00:33:56 2005 GMT
    Serial Number: 5DAE53CD000000000000F
```

```
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
```

**Note** 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 のライセンス	<i>Cisco NX-OS</i> ライセンス ガイド
VRF コンフィギュレーション	『 <i>Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide</i> 』

### 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。	—



## 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。

- [ユーザアカウントと RBAC について, on page 243](#)
- [ユーザアカウントおよび RBAC の注意事項と制約事項 \(246 ページ\)](#)
- [ユーザアカウントおよび RBAC のデフォルト設定, on page 247](#)
- [パスワードの強度確認のイネーブル化, on page 248](#)
- [ユーザアカウントの設定, on page 249](#)
- [?????, on page 251](#)
- [No Service Password-Recovery について \(259 ページ\)](#)
- [No Service Password-Recovery のイネーブル化 \(260 ページ\)](#)
- [ユーザアカウントおよび RBAC 設定の確認, on page 261](#)
- [ユーザアカウントおよび RBAC の設定例, on page 262](#)
- [ユーザアカウントおよび RBAC に関する追加情報, on page 264](#)

## ユーザアカウントと RBAC について

ユーザアカウントを作成して管理し、Cisco NX-OS で行え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が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。

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、mtuser、ftuser、man、および sys。



---

**Note** 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。

---



**Caution** ユーザ名は、先頭が英数字で始まる必要があり、その他に使用できる特殊文字は(+ = . \_ \ -)。#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。



---

**Note** Cisco Nexus デバイスのパスワードには、ドル記号 (\$) やパーセント記号 (%) などの特殊文字を使用できます。

---

- 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



---

**Note** クリアテキストのパスワードでは、パスワードの先頭に引用符 (" または ')、縦棒 (|)、大なり記号 (>) などの特殊文字を含めることはできません。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。パスワードでは大文字と小文字が区別されます。

---





**Note** 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。

### Related Topics

[パスワードの強度確認のイネーブル化](#) (248 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、特定の仮想ルーティング/転送 (VRF) インスタンス、VLAN、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、次のユーザロールが用意されています。

- `network-admin` : Cisco NX-OS デバイス全体への完全な読み取り/書き込みアクセス権
- `network-operator` または `vdc-operator` : Cisco NX-OS デバイス全体への完全な読み取りアクセス権



### Note

- Cisco Nexus 9000 シリーズスイッチは、複数の VDC をサポートしていません。ただし、`the vdc-operator` ロールが利用可能で、これには `network-operator` ロールと同じ権限と制約事項が付随します。
- Cisco Nexus 9000 シリーズスイッチは、VDC 管理者がネットワーク管理者と同じ権限と制限を持つような、単一の VDC をサポートします。



**Note** ユーザロールは変更できません。



**Note** 一部の `show` コマンドは、`network-operator` ユーザには表示されないようにすることができます。加えて、一部の `show` 以外のコマンド (`telnet` など) を、このユーザロールで使用できるようにすることができます。

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では `show`、`exit`、`end`、および `configure terminal` コマンドにしかアクセスできません。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。



**Note** 複数のルールに属するユーザは、そのル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ルール A を持っていたとします。しかし、同じユーザが ルール B も持ち、このル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。

## 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コマンドです。次の制御パラメータは機能です。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、機能グループです。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。

SNMP OID は RBAC でサポートされています。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できます。

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つのルールが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 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。

- ユーザ ロールには最大 256 個の規則を追加できます。
- デフォルトの機能グループである L3 に加えて、最大 64 のユーザ定義機能グループを追加できます。

- 最大 256 人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` ロールでは、`show running-config` および `show startup-config` コマンドを実行できません。
- Cisco Nexus 9000 シリーズスイッチは、VDC 管理者がネットワーク管理者と同じ権限と制限を持つ単一の VDC をサポートします。
- AAA ポリシーに従って、ロールがユーザに最後のロールとして関連付けられている場合、そのロールは、そのユーザから関連付けが解除されるまで削除できません。



(注) Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

## 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。

Table 13: 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
ユーザアカウントロール	作成ユーザが <code>network-admin</code> ロールを持つ場合は <code>network-operator</code>
デフォルトユーザロール	<code>network-operator</code>
インターフェイスポリシー	すべてのインターフェイスにアクセス可能
VLANポリシー	すべてのVLANにアクセス可能

パラメータ	デフォルト
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。



**Note** 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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	<b>password strength-check</b> <b>Example:</b> 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 <b>no</b> 形式を使用します。
ステップ 3	<b>exit</b> <b>Example:</b> 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	(Optional) <b>show password strength-check</b> <b>Example:</b> switch# show password strength-check	パスワードの強度確認の設定を表示します。
ステップ 5	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> 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。

**Related Topics**[強力なパスワードの特性](#) (244 ページ)

# ユーザアカウントの設定

1 つの Cisco NX-OS デバイスに最大 256 個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 (Username) ]
- 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 パスワードは、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。

SHA256 は、パスワードの暗号化に使用されるハッシュアルゴリズムです。暗号化の一環として、64 ビット SALT の 5000 回の反復がパスワードに追加されます。

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。

**Note**

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。

**Procedure**

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	(Optional) <b>show role</b> <b>Example:</b> switch(config)# show role	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。

	Command or Action	Purpose
ステップ 3	<p><b>username</b> <i>user-id</i> [<b>password</b> [0   5] <i>password</i>] [<b>expire date</b>] [<b>role</b> <i>role-name</i>]</p> <p><b>Example:</b></p> <pre>switch(config)# username NewUser password 4Ty18Rnt</pre>	<p>ユーザアカウントを設定します。 <i>user-id</i> 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。</p> <p>ユーザ名の先頭は英数字で始まる必要があります。</p> <p>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 <b>0</b> は、パスワードがクリアテキストであり、<b>5</b> 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 <b>0</b> (クリアテキスト) です。</p> <p><b>Note</b> パスワードを指定しなかった場合、ユーザは Cisco NX-OS デバイスにログインできません。</p> <p><b>Note</b> 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。</p> <p><b>expire date</b> オプションのフォーマットは YYYY-MM-DD です。デフォルトでは、失効日はありません。</p> <p>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。</p>
ステップ 4	<p><b>username</b> <i>user-id</i> <b>ssh-cert-dn</b> <i>dn-name</i> {<b>dsa</b>   <b>rsa</b>}</p> <p><b>Example:</b></p> <pre>switch(config)# username NewUser ssh-cert-dn "/CN = NewUser, OU = Cisco Demo, O = Cisco, C = US" rsa</pre> <p><b>Example:</b></p>	<p>既存のユーザアカウント認証に使用する SSH X.509 証明書の識別名と DSA アルゴリズムを指定します。識別名は最大 512 文字で、例に示す形式に従う必要があります。電子メールアドレスと状態がそれぞれ <b>emailAddress</b> と <b>ST</b> に設定されていることを確認します。</p>

	Command or Action	Purpose
	<pre>switch(config)# username jsmith ssh-cert-dn "/O = ABCcompany, OU = ABC1, emailAddress = jsmith@ABCcompany.com, L = Metropolis, ST = New York, C = US, CN = jsmith" rsa</pre>	
ステップ 5	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>switch(config)# exit switch#</pre>	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	<p>(Optional) <b>show user-account</b></p> <p><b>Example:</b></p> <pre>switch# show user-account</pre>	ロール設定を表示します。
ステップ 7	<p>(Optional) <b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch# copy running-config startup-config</pre>	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。

**Related Topics**

[?????? \(251 ページ\)](#)

[ユーザ ロールおよびルールの作成 \(251 ページ\)](#)

# ??????

???????? ???????????????????

## ユーザ ロールおよびルールの作成

最大 64 個のユーザ 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 つのルールが 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。



**Note**

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 ロールでのみ実行できます。

**Before you begin**

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。

**Procedure**

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	<b>role name role-name</b> <b>Example:</b> 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。 <i>role-name</i> 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	<b>rule number {deny   permit} command command-string</b> <b>Example:</b> switch(config-role)# rule 1 deny command clear users	コマンド規則を設定します。  <i>command-string</i> 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、 <b>interface ethernet</b> 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	<b>rule number {deny   permit} {read   read-write}</b> <b>Example:</b> 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。
ステップ 5	<b>rule number {deny   permit} {read   read-write} feature feature-name</b> <b>Example:</b> 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。  <b>show role feature</b> 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	<b>rule number {deny   permit} {read   read-write} feature-group group-name</b> <b>Example:</b>	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。



	Command or Action	Purpose
	<pre>switch(config-role)# rule 4 deny read-write feature-group L3</pre>	<p><b>show role feature-group</b> 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。</p> <p>必要な規則の数だけこのコマンドを繰り返します。</p>
ステップ 7	<p><b>rule number {deny   permit} {read   read-write} oid snmp_oid_name</b></p> <p><b>Example:</b></p> <pre>switch(config-role)# rule 5 deny read-write oid 1.3.6.1.2.1.1.9</pre>	<p>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、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。</p> <p><b>Note</b> 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。</p> <p>必要な規則の数だけこのコマンドを繰り返します。</p>
ステップ 8	<p>(Optional) <b>description text</b></p> <p><b>Example:</b></p> <pre>switch(config-role)# description This role does not allow users to use clear commands</pre>	<p>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。</p>
ステップ 9	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>switch(config-role)# exit switch(config)#</pre>	<p>ロールコンフィギュレーションモードを終了します。</p>
ステップ 10	<p>(Optional) <b>show role</b></p> <p><b>Example:</b></p> <pre>switch(config)# show role</pre>	<p>ユーザロールの設定を表示します。</p>
ステップ 11	<p>(Optional) <b>show role {pending   pending-diff}</b></p> <p><b>Example:</b></p> <pre>switch(config)# show role pending</pre>	<p>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。</p>

	Command or Action	Purpose
ステップ 12	(Optional) <b>role commit</b>  <b>Example:</b> switch(config)# role commit	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ます。
ステップ 13	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> 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。

## 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。最大 64 個の機能グループを作成できます。



**Note** 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。

### Before you begin

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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> 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	<b>role feature-group name group-name</b>  <b>Example:</b> 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。  <i>group-name</i> 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	<b>feature feature-name</b>  <b>Example:</b> switch(config-role-featuregrp)# feature radius	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。

	Command or Action	Purpose
		<b>Note</b> 機能の一覧を表示する場合は、 <b>show role component</b> コマンドを使用します。
ステップ 4	<b>exit</b> <b>Example:</b> 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	(Optional) <b>show role feature-group</b> <b>Example:</b> switch(config)# show role feature-group	ロール機能グループ設定を表示します。
ステップ 6	(Optional) <b>show role {pending   pending-diff}</b> <b>Example:</b> switch(config)# show role pending	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	(Optional) <b>role commit</b> <b>Example:</b> switch(config)# role commit	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ます。
ステップ 8	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> 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。

## 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 ロールによってすべてのインターフェイスへのアクセスが許可されます。

### Before you begin

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。

## Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	<b>role name role-name</b> <b>Example:</b> 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	<b>interface policy deny</b> <b>Example:</b> 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	<b>permit interface interface_list</b> <b>Example:</b> 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	<b>exit</b> <b>Example:</b> 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	(Optional) <b>show role</b> <b>Example:</b> switch(config-role)# show role	ロール設定を表示します。
ステップ 7	(Optional) <b>show role {pending   pending-diff}</b> <b>Example:</b> switch(config-role)# show role pending	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	(Optional) <b>role commit</b> <b>Example:</b> switch(config-role)# role commit	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ます。
ステップ 9	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch(config-role)# 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。

**Related Topics**

[ユーザロールおよびルールの作成](#) (251 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、ユーザロールによってすべてのVLANへのアクセスが許可されます。

**Before you begin**

1つまたは複数のユーザロールを作成します。

**Procedure**

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> 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	<b>role name role-name</b>  <b>Example:</b> 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	<b>vlan policy deny</b>  <b>Example:</b> 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。
ステップ 4	<b>permit vlan vlan-list</b>  <b>Example:</b> 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	<b>exit</b>  <b>Example:</b> 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	(Optional) <b>show role</b>  <b>Example:</b> switch(config)# show role	ロール設定を表示します。
ステップ 7	(Optional) <b>show role {pending   pending-diff}</b>  <b>Example:</b>	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。

	Command or Action	Purpose
	<code>switch(config-role)# show role pending</code>	
ステップ 8	(Optional) <b>role commit</b> <b>Example:</b> <code>switch(config-role)# role commit</code>	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ます。
ステップ 9	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <code>switch(config-role)# copy running-config startup-config</code>	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。

**Related Topics**

[ユーザロールおよびルールの作成](#) (251 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、ユーザロールによってすべてのVRFへのアクセスが許可されます。

**Before you begin**

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。

**Procedure**

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <code>switch# configure terminal</code> <code>switch(config)#</code>	グ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	<b>role name</b> <i>role-name</i> <b>Example:</b> <code>switch(config)# role name UserA</code> <code>switch(config-role)#</code>	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	<b>vrf policy deny</b> <b>Example:</b> <code>switch(config-role)# vrf policy deny</code> <code>switch(config-role-vrf)#</code>	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。

	Command or Action	Purpose
ステップ 4	<b>permit vrf vrf-name</b>  <b>Example:</b> <pre>switch(config-role-vrf)# permit vrf vrf1</pre>	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	<b>exit</b>  <b>Example:</b> <pre>switch(config-role-vrf)# exit switch(config-role)#</pre>	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。
ステップ 6	(Optional) <b>show role</b>  <b>Example:</b> <pre>switch(config-role)# show role</pre>	ロール設定を表示します。
ステップ 7	(Optional) <b>show role {pending   pending-diff}</b>  <b>Example:</b> <pre>switch(config-role)# show role pending</pre>	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	(Optional) <b>role commit</b>  <b>Example:</b> <pre>switch(config-role)# role commit</pre>	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ます。
ステップ 9	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch(config-role)# copy running-config startup-config</pre>	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。

**Related Topics**

[ユーザ ロールおよびルールの作成 \(251 ページ\)](#)

## No Service Password-Recovery について

No Service Password-Recovery 機能により、コンソールへのアクセスを持つ誰もがルータおよびルータのネットワークにアクセスする機能を与えられることになります。No Service Password-Recovery 機能を使用すると、『[Cisco Nexus 9000 Series NX-OS Troubleshooting Guide](#)』に記載されている標準的な手順でパスワードを回復できなくなります。

# No Service Password-Recovery のイネーブル化

No Service Password-Recovery 機能が有効になっている場合、ネットワーク権限を持つ管理者以外は管理者パスワードを変更できません。

## 始める前に

no service password-recovery コマンドを開始する場合、シスコでは、デバイスから離れた場所にシステム コンフィギュレーション ファイルのコピーを保存することを推奨しています。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>no service password-recovery</b> 例： <pre>switch(config)# no service password-recovery WARNING: Executing this command will disable the password recovery mechanism. Do not execute this command without another plan for password recovery. Are you sure you want to continue? (y/n) : [y] y switch(config)# copy run start [#####] 100% Copy complete, now saving to disk (please wait)... Copy complete.</pre>	パスワード回復メカニズムを無効にします。
ステップ 3	(任意) <b>copy running-config startup-config</b> 例： <pre>switch# copy running-config startup-config</pre>	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	<b>Reload</b> 例： <pre>switch(config)# Reload This command will reboot the system. (y/n)? [n] y 2018 Jun 26 16:23:19 BAR %\$ VDC-1 %\$ %PLATFORM-2-PFM_SYSTEM_RESET: Manual system restart from Command Line Interface</pre>	



	コマンドまたはアクション	目的
	<pre>CISCO SWITCH Ver 8.34 CISCO SWITCH Ver 8.34 Manual system restart from Command Line Interface writing reset reason 9, .. ..  switch(boot)# config t Enter configuration commands, one per line. End with CNTL/Z. switch(boot) (config)# admin-password Abcd!123\$ ERROR: service password-recovery disabled. Cannot change password! switch(boot) (config)#</pre>	
ステップ 5	<p><b>exit</b></p> <p>例 :</p> <pre>switch(config)# exit switch#</pre>	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	<p>(任意) <b>show user-account</b></p> <p>例 :</p> <pre>switch# show user-account</pre>	ロール設定を表示します。
ステップ 7	<p>(任意) <b>copy running-config startup-config</b></p> <p>例 :</p> <pre>switch# copy running-config startup-config</pre>	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
<b>show cli syntax roles network-admin</b>	network-admin ロールが使用できるが、コマンドの構文を表示します。
<b>show cli syntax roles network-operator</b>	network-operator ロールで使用できるコマンドの構文を表示します。

コマンド	目的
<b>show role</b>	ユーザ ロールの設定を表示します。
<b>show role feature</b>	機能リストを表示します。
<b>show role feature-group</b>	機能グループの設定を表示します。
<b>show startup-config security</b>	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。
<b>show running-config security [all]</b>	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。 <b>all</b> 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。
<b>show user-account</b>	ユーザアカウント情報を表示します。

## 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 2 permit read-write feature bgp
  rule 1 deny command clear *
```

次に、BGP をイネーブルにして表示し、EIGRP 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 *; bgp *
  rule 2 permit read-write feature bgp
  rule 3 permit read feature eigrp
```

上の例で、ルール 1 はインターフェイス上で BGP を設定することを可能にし、ルール 2 は **config bgp** コマンドを設定して実行レベルの **show** コマンドと **debug** コマンドを BGP に対してイネーブルにすることを有効にし、ルール 3 は実行レベルの **show** コマンドと **debug eigrp** コマンドをイネーブルにすることを可能にしています。

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 aaa
  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 のライセンス	Cisco NX-OS ライセンス ガイド
VRF コンフィギュレーション	『Cisco Nexus 9000 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
ユーザアカウントおよび RBAC に関連する MIB	サポートされている 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。 <a href="ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html">ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html</a>



# 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。

- [802.1X について, on page 265](#)
- [DACL について \(271 ページ\)](#)
- [802.1X の前提条件, on page 272](#)
- [802.1X の注意事項と制約事項 \(272 ページ\)](#)
- [802.1X のデフォルト設定, on page 274](#)
- [802.1X の設定, on page 275](#)
- [802.1X 設定の確認, on page 296](#)
- [VXLAN EVPN の 802.1X サポート \(296 ページ\)](#)
- [802.1X のモニタリング, on page 301](#)
- [802.1X の設定例, on page 302](#)
- [802.1X に関する追加情報, on page 302](#)

## 802.1X について

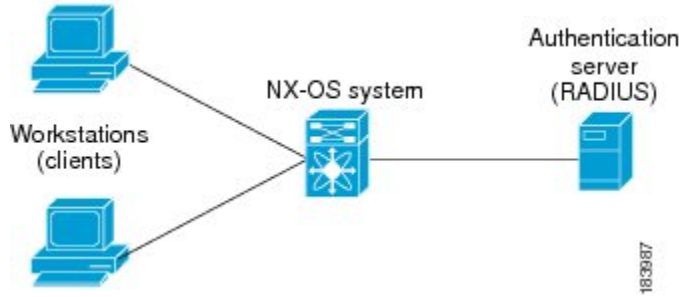
802.1X では、クライアント サーバベースのアクセス コントロールと認証プロトコルを定義し、許可されていないクライアントが公にアクセス可能なポートを経由して LAN に接続するのを規制します。認証サーバは、Cisco NX-OS デバイスのポートに接続されるクライアントを個々に認証します。

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。

????????

802.1X ??? ???

Figure 5: 802.1X ????????



????????????

??????

LAN ??? Cisco NX-OS ??? ?????????????Cisco NX-OS ??????????????????  
 ??????????????????Microsoft Windows XP ??????????????????802.1X ??????????  
 ?????????????????????

??????

??LAN ??? Cisco NX-OS  
 ??? Cisco NX-OS ?????????????Cisco NX-OS  
 ???EAP????????? Remote  
 Authentication Dial-In User Service?RADIUS????????? ?????????????????????????????Cisco Secure  
 Access Control Server ?????? 3.0 ?????????RADIUS ?????????? ???? ?????????RADIUS ????? 1 ???????  
 RADIUS ??????????????????????????????

??????????

??EAP  
 ?????????????/????????????????????????????????????RADIUS ??????????????????

???????????? EAPOL ??? EAP ?????? RADIUS  
 ????????????????????????????????????? EAP ??? EAP  
 ??? EAP  
 ???



**Note** Cisco NX-OS ?????????????802.1X ??????????????????

????????????????

????????????Cisco NX-OS ???  
 ??? EAP-Request/Identity  
 ??? 1 ????????????????????? Identity/Request  
 ???EAP-Response/Identity ??????????????  
 ????????????????????????????????????? EAP-Request/Identity ????????????????????? EAPOL  
 ???



Note

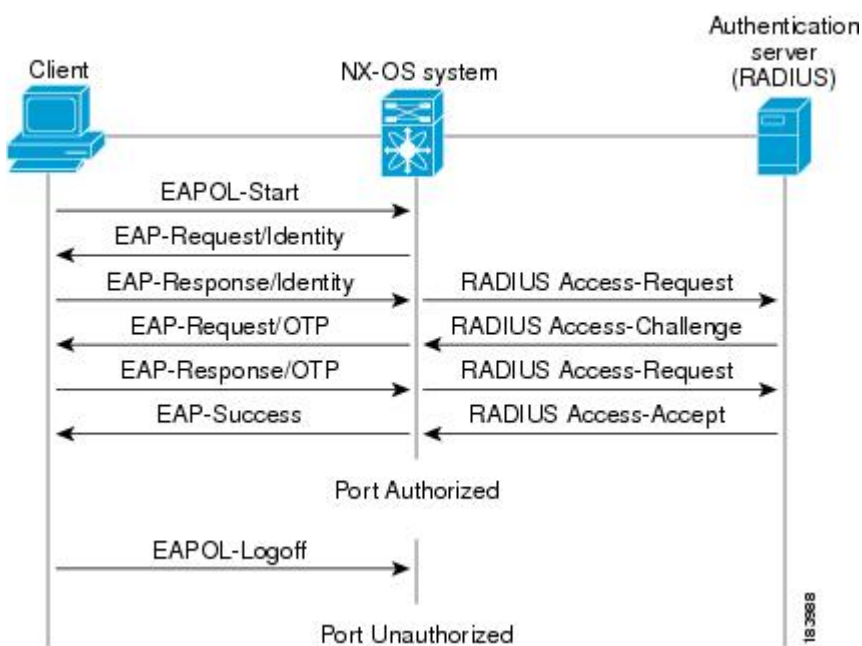
????? ???? ???? 802.1X ?????????????????????????????????Cisco NX-OS ?????????????? EAPOL  
?? 3 ????? EAP-Request/Identity  
??

?? EAP  
??

??????? EAP ?????????????????????????????

Figure 6: ???????

????????????? RADIUS ?????????? ??????OTP????????????????????????????????OTP ???????????????  
??



????????????? ???

## 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。

## 許可状態および無許可状態のポート

サブ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状態で決まります。ポートは、無許可状態で開始します。この状態にあるポートは、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。サブリカントの認証に成功すると、ポートは許可状態に移行し、サブ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状態の 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状態となり、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状態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状態があります。

### 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状態に移行します。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。この許可状態はデフォルトです。

### Force unauthorized

ポートが無許可状態のままになり、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。

### Auto

802.1X ポートベースの認証をイネーブルにします。ポートは無許可状態で開始し、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 ステータスがダウンからアップに移行したとき、またはサブリカントから 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ブリカントの 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ブリカントを一意に識別します。

サブ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）、ポートが許可状態に変わり、認証されたサブ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、ポートは無許可状態のままですが、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、サブリカントのネットワーク アクセスは認可されません。

サブ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状態に移行します。

ポートのリンク ステータス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、ポートは無許可状態に戻ります。



## MAC 認証バイパス

MAC 認証バイパス機能を使用して、サブリカントの MAC アドレスに基づいてサブ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。

サブリカントからの 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 アドレスをサブリカント 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ブリカントの 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。

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 対応サブ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 サブ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、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。

## MAC ベースの認証 (MAB) に基づいたダイナミック VLAN 割り当て

Cisco Nexus 9000 シリーズ スイッチはダイナミック VLAN 割り当てをサポートします。802.1x 認証または MAB の完了後、ポートの起動前に、認証の結果として、特定の VLAN ベースに配置するピア/ホストを (認証の一部として) 許可することもできます。RADIUS サーバは、一般的に、Access-Accept メッセージ内にトンネル属性を含めることによって目的の VLAN を示します。VLAN を取得してポートにバインディングするこの手順は、ダイナミック VLAN 割り当てを構成します。

## RADIUS からの VLAN 割り当て

dot1x または MAB によって認証が完了すると、RADIUS サーバからの応答にダイナミック VLAN 情報を含むことができるようになり、これをポートに割り当てることができます。この情報は、トンネル属性の形式の受け入れアクセス メッセージの RADIUS サーバからの応答に存在します。VLAN 割り当てのために、次のトンネル属性が送信されます。

- Tunnel-type=VLAN(13)
- Tunnel-Medium-Type=802
- Tunnel-Private-Group-ID=VLANID

アクセス VLAN の設定のために、3 つのパラメータをすべて受け取る必要があります。

## 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。

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、ポイントツーポイントトポロジをサポートします。

この設定では、802.1X 対応のオーセンティケータ（Cisco NX-OS デバイス）ポートにサブリカント（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ブリカントを検出します。サブリカントがログオフしたとき、または別のサブ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。

## DACL について

ダイナミック ACL（DACL）は、ユーザおよびグループがアクセスできる権限を含む単一の ACL です。dot1q MAB クライアントへのアクセスを制限します。DACL ポリシーが Cisco ISE サーバからプッシュされ、MAC アドレスがブラックリストに登録されます。これにより、ブラックリストに登録された MAC に ACL が適用され、MAB へのアクセスが制限されます。単一の DACL は、すべてのブラックリスト MAB クライアントをサポートします。

Cisco NX-OS Release 9.3(5) では、DACL は Cisco Nexus スイッチで事前設定されています。

## DACL の注意事項と制約事項

DACL には、次の注意事項と制約事項があります。

- Cisco NX-OS リリース 9.3(5) では、DACL は Cisco Nexus 9336-FX2、Nexus 9236C、Nexus 93108TC-EX、および Nexus 93180YC-EX スイッチでサポートされています。
- DACL は、MAC 認証バイパスによる認証のみをサポートします。EAPOL はサポートされていません。
- DACL は、単一のアクセス VLAN がサポートされているレイヤ2アクセスポートでサポートされます。
- ブラックリストに登録されたすべてのクライアントで、DACL はスイッチ上で単一のグローバル ACL をサポートします。
- 集中型 ISE サーバから受信した ACL 名は、スイッチで事前設定された ACL 名と一致する必要があります。
- ブラックリストに登録されたクライアントトラフィックは、DNS、DHCP、および BOOTPC プロトコルに適用される固定 ACL ルールに基づいてフィルタリングされます。

- `acl-rules` が変更されると、既存の `dot1x` セッションは以前の `acl-rules` を引き続き使用します。`acl-rules` の変更後に `clear dot1x all` コマンドを実行する必要があります。

## 802.1X の前提条件

- Cisco Nexus リリース 7.0(3)I7(1) ソフトウェア。

## 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 リリース 9.3(3) 以降、Dot1x は Cisco Nexus 9300-GX プラットフォームスイッチでサポートされます。
- (中断あり/中断なしの) インサーブिस ソフトウェアアップグレード (ISSU) を使用して Cisco Nexus シリーズスイッチを Cisco NX-OS リリース 9.2(1) にアップグレードする場合は、まず `no feature dot1x` コマンドを使用して 802.1x を無効にします。機能を有効にするには、`feature dot1x` コマンドを使用してマルチ認証を機能させます。
- Cisco NX-OS リリース 9.2(1) 以降では、802.1X ポートでマルチ認証モードが有効になります。VLAN の割り当ては、最初の認証済みホストに対し行われます。ユーザクレデンシャルに基づいてその後に許可されたデータホストは、正しく認証されたと見なされます。ただし、まだ VLAN が割り当てられていないか、ポートで最初に正しく認証されたホストと一致する VLAN 割り当てがなされていることを条件とします。これにより、ポートで正常に認証されたすべてのホストは、確実に同じ VLAN メンバになります。VLAN 割り当ての柔軟性は、最初に認証されたホストだけで生じます。
- Cisco NX-OS リリース 9.2(3) 以降、802.1X ポートベース認証は FEX-ST およびホストインターフェイス (HIF) ポートでサポートされます。IEEE 802.1X ポートベース認証のサポートは、ストレートおよびデュアルホーム FEX の両方に適用されます。
- Cisco Nexus 9000 シリーズスイッチは、以下のものについては、802.1X をサポートしていません。
  - トランジット トポロジの設定
  - vPC ポート
  - PVLAN ポート
  - L3 (ルーテッド) ポート
  - ポートセキュリティ
  - CTS および MACsec が有効になっているポート。
  - LACP ポートチャネルを使用した Dot1x。



---

(注) Dot1x は、スタティック ポートチャネルをサポートします。

---



---

(注) vPC ポートおよびサポートされていないすべての機能では、802.1X は無効になります。

---

- Cisco NX-OS ソフトウェアが 802.1X 認証をサポートするのは、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 チャネルのメンバー 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。
- メンバーが 802.1X 用に設定されている場合、Cisco NX-OS ソフトウェアは、ポート チャネルメンバーでのシングルホスト モードの設定をサポートしません。メンバー 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。
- 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せん。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、すべてのメンバー ポートで 802.1X 設定を同一にする必要があります。
- 802.1X 認証を有効にした場合、サブ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 のすべての機能が有効になります。
- 802.1X 対応ポートでは、認証が成功した後にのみ STP BPDU が許可されます。STP の競合を回避するために、STP エッジポートでのみ 802.1X 機能をイネーブルにすることを推奨します。
- 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、CTS または MACsec 機能については動作しません。グローバルな「mac-learn disable」と dot1x 機能は相互に排他的であり、同時に設定することはできません。
- Dot1x は IP ソースガードおよび uRPF 機能とは相互に排他的であり、同時に設定することはできません。Cisco Nexus シリーズ スイッチを Cisco NX-OS リリース 9.2(3) にアップグレードする場合は、これらの機能のいずれかを無効にする必要があります。
- 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ー 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、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。ポートチャネルでサポートされるモードは、マルチホストモードだけです。

- Cisco NX-OS リリース9.2(1) では、MAC 認証バイパスは N3K-C3164Q-40GE スイッチではサポートされていません。
- 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。
- スイッチのリロード中、Dot1x は RADIUS アカウンティングの停止を生成しません。
- 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
  - ゲスト VLAN
- 非アクティブなセッションの再認証を防ぐには、`authentication timer inactivity` コマンドを使用して、非アクティブタイマーを、`authentication timer reauthenticate` コマンドで設定された再認証間隔よりも短い間隔に設定します。
- N9K-M12PQ アップリンク モジュール ポートでの `dot1x` の選択的な有効化または無効化は、Cisco Nexus 9300 プラットフォーム スイッチではサポートされていません。
- インターフェイスで `dot1x` が有効になっている異なる VLAN で、同じ MAC が学習されると、セキュリティ違反が発生します。
- DME 対応プラットフォームで `dot1x` を有効にした状態で MAC の学習を無効に設定しても、エラーメッセージは表示されません。
- Cisco Nexus リリース9.2(1) では、VLAN がインターフェイスで設定されていなくても、タグ付き EAPOL フレームは処理され、クライアントのインターフェイスで認証は成功します。
- 孤立ポートで学習されたセキュア MAC は、vPCピアで同期されません。

## 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。

Table 14: 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	設定なし

パラメータ	デフォルト
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 ( <b>force-authorized</b> ) <b>Note</b> ポートはサブリカントとの 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 デバイスがサブ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ブ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
サブリカント タイムアウト時間	30 秒 (認証サーバからの要求をサブリカントにリレーするとき、Cisco NX-OS デバイスがサブリカントに要求を再送信するまでに、サブ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 (サブ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。

### 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。

#### Procedure

- 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

サブ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。

### Procedure

	Command or Action	Purpose
ステップ1	<b>configure terminal</b> <b>Example:</b> switch# <b>configure terminal</b> 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	<b>feature dot1x</b> <b>Example:</b> switch(config)# <b>feature dot1x</b>	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	<b>exit</b> <b>Example:</b> switch(config)# <b>exit</b> switch#	設定モードを終了します。
ステップ4	(Optional) <b>show dot1x</b> <b>Example:</b> switch# <b>show dot1x</b>	802.1X 機能のステータスを表示します。
ステップ5	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch# <b>copy running-config startup-config</b>	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。

### Before you begin

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。



## Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	<b>aaa authentication dot1x default group group-list</b> <b>Example:</b> 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。  <i>group-list</i> 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。  <ul style="list-style-type: none"> <li>• <b>radius</b>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。</li> <li>• <b>named-group</b> : 認証に RADIUS サーバのグローバル プールを使用します。</li> </ul>
ステップ 3	<b>exit</b> <b>Example:</b> switch(config)# exit switch#	設定モードを終了します。
ステップ 4	(Optional) <b>show radius-server</b> <b>Example:</b> switch# show radius-server	RADIUS サーバの設定を表示します。
ステップ 5	(Optional) <b>show radius-server group [group-name]</b> <b>Example:</b> switch# show radius-server group rad2	RADIUS サーバ グループの設定を表示します。
ステップ 6	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> 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。

## 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 認証ステータスは、次のとおりです。

**Auto**

インターフェイス上で、802.1X 認証をイネーブルにします。

**Force-authorized**

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。

**Before you begin**

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

**Procedure**

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	<b>interface ethernet slot / port</b> <b>Example:</b> 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	<b>dot1x port-control {auto   force-authorized   forced-unauthorized}</b> <b>Example:</b> 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	<b>exit</b> <b>Example:</b> switch(config)# exit switch#	設定モードを終了します。
ステップ 5	(Optional) <b>show dot1x all</b> <b>Example:</b> switch# show dot1x all	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	(Optional) <b>show dot1x interface ethernet slot / port</b> <b>Example:</b> switch# show dot1x interface ethernet 2/1	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。

	Command or Action	Purpose
ステップ 7	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> 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。

## 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。

### 始める前に

802.1X 機能をイネーブルにします。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  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	(任意) <b>show dot1x interface ethernet slot/port</b>  例 : switch# show dot1x interface ethernet 2/1	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	<b>interface ethernet slot/port</b>  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	<b>[no] dot1x pae authenticator</b>  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、 <b>no</b> 形式を使用します。

	コマンドまたはアクション	目的
		(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、 <b>dot1x pae authentication</b> 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	(任意) <b>copy running-config startup-config</b>  例： <pre>switch(config)# copy running-config startup-config</pre>	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。



**Note** 再認証プロセス中、すでに認証されているサブリカントのステータスは影響を受けません。

### Before you begin

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>interface ethernet slot/port</b>  <b>Example:</b> <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	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	<b>dot1x re-authentication</b>  <b>Example:</b> <pre>switch(config-if)# dot1x re-authentication</pre>	インターフェイスに接続されているサブ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。

	Command or Action	Purpose
ステップ 4	(Optional) <b>dot1x timeout re-authperiod</b> <i>seconds</i>  <b>Example:</b> <pre>switch(config-if)# dot1x timeout re-authperiod 3300</pre>	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。  <b>Note</b> 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	<b>exit</b>  <b>Example:</b> <pre>switch(config-if)# exit switch(config)#</pre>	設定モードを終了します。
ステップ 6	(Optional) <b>show dot1x all</b>  <b>Example:</b> <pre>switch(config)# show dot1x all</pre>	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	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	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。

## 手動によるサブリカントの再認証

Cisco NX-OS デバイス全体のサブリカントまたはインターフェイスのサブリカントを手動で再認証できます。



**Note** 再認証プロセス中、すでに認証されているサブリカントのステータスは影響を受けません。

### Before you begin

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

## Procedure

	Command or Action	Purpose
ステップ 1	<b>dot1x re-authenticate [interface slot/port]</b>  <b>Example:</b> <pre>switch# dot1x re-authenticate interface 2/1</pre>	Cisco NX-OS デバイスまたはインターフェイス上のサブリカントを再認証します。

## 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 デバイスがサブ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、サブ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、サブ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、認証に成功したサブリカントからの 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ブリカント間の再送信タイマー

サブリカントは、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ブリカント間の再送信タイマー

サブリカントは、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。

### Inactive period timeout

Cisco NX-OS デバイスが設定された期間にわたって非アクティブのままである場合、`timeout inactivity-period` 値は、非アクティブ期間を決定します。最小推奨値は 1800 秒です。値が再認証時間の値よりも小さいことを確認する必要があります。



**Note** このデフォルト値は、リンクの信頼性が低下した場合や、特定のサブ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。

### Before you begin

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	<b>interface ethernet slot/port</b> <b>Example:</b> 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	(Optional) <b>dot1x timeout quiet-period seconds</b> <b>Example:</b> switch(config-if)# dot1x timeout quiet-period 25	オーセンティケータが EAP-Request/Identity フレームに対するサブ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	(Optional) <b>dot1x timeout ratelimit-period seconds</b> <b>Example:</b> switch(config-if)# dot1x timeout ratelimit-period 10	認証に成功したサブリカントからの 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	(Optional) <b>dot1x timeout server-timeout seconds</b> <b>Example:</b> switch(config-if)# dot1x timeout server-timeout 60	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。
ステップ 6	(Optional) <b>dot1x timeout supp-timeout seconds</b> <b>Example:</b>	Cisco NX-OS デバイスが EAP 要求フレームを再送信する前に、サブリカントが EAP 要求フレームに応答してくる

	Command or Action	Purpose
	<code>switch(config-if)# dot1x timeout supp-timeout 20</code>	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	(Optional) <b>dot1x timeout tx-period</b> <i>seconds</i>  <b>Example:</b> <code>switch(config-if)# dot1x timeout tx-period 40</code>	サブリカントから 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	(Optional) <b>dot1x timeout inactivity-period</b> <i>seconds</i>  <b>Example:</b> <code>switch(config-if)# dot1x timeout inactivity-period 1800</code>	スイッチが非アクティブ状態を維持できる秒数を設定します。最小推奨値は 1800 秒です。
ステップ 9	<b>exit</b>  <b>Example:</b> <code>switch(config)# exit</code> switch#	設定モードを終了します。
ステップ 10	(Optional) <b>show dot1x all</b>  <b>Example:</b> <code>switch# show dot1x all</code>	802.1X の設定を表示します。
ステップ 11	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <code>switch# copy running-config startup-config</code>	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

サブ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。

始める前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。



## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>interface ethernet slot/port</b> 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	<b>dot1x mac-auth-bypass [eap]</b> 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。 <b>eap</b> 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	<b>exit</b> 例： switch(config-if)# exit switch(config)#	設定モードを終了します。
ステップ 5	(任意) <b>show dot1x all</b> 例： switch# show dot1x all	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	(任意) <b>copy running-config startup-config</b> 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。

## デフォルト dot1.x 認証認証方式の設定 - MAB

Cisco NX-OS リリース 9.3(5) 以降では、dot1x 対応ポートで受信されるすべてのトラフィックは、MAC 認証バイパス (MAB) によってのみ認証できます。Cisco NX-OS リリース 9.3(5) よりも前では、すべてのトラフィックは最初に EAPOL によって認証され、MAB による認証は EAPOL 認証セッションがタイムアウトした後にのみ行われました。

## 始める前に

Cisco NX-OS デバイスで MAB 機能をイネーブルにします。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>interface ethernet slot/port</b> 例： switch(config)# interface ethernet 2/1 switch(config-if)	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	<b>dot1x mac-auth-bypass</b> 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。
ステップ 4	<b>[no] dot1x authentication order mab</b> 例： switch(config-if)# dot1x authentication order mab	RADIUS サーバでデータ トラフィックの認証に対して MABをイネーブルにします。このコマンドの <b>no</b> 形式を使用すると、デフォルトの認証方式を EAPOL に変更します。
ステップ 5	<b>exit</b> 例： switch(config-if)# exit switch(config)#	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	(任意) <b>show dot1x all</b> 例： switch# show dot1x all	802.1X 機能のすべてのステータスおよびコンフィギュレーション情報を表示します。
ステップ 7	(任意) <b>copy running-config startup-config</b> 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。

## ダイナミック アクセス リストの作成

始める前に

次の状態を確認してください。

- dot1x MAB クライアントの特定のトラフィッククラスを許可またはブロックするように、すべての ACE で ACL 名 (acl-name) を事前にプログラムします。デバイスに設定されている ACL 名 (acl-name) は、ISE サーバから受信する acl-name と一致する必要があります。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>hardware access-list tcam region ing-dacl tcam size</b> 例 : switch(config)# hardware access-list tcam region ing-dacl 256 switch(config)#	TCAM サイズを指定します。指定できる範囲は 0 ~ 2147483647 です。
ステップ 3	<b>ip access-list blacklist</b> 例 : switch(config)# ip access-list creative_blacklist	定義済みのブラックリストを設定し、設定された TCAM サイズに基づいて適用します。
ステップ 4	(任意) <b>show ip access-list</b> 例 : switch(config)# ip access-list creative_blacklist1	設定済みの IP アクセス リストを表示します。
ステップ 5	(任意) <b>show ip access-list dynamic</b> 例 : switch(config)# ip access-list creative_blacklist1_new_Ethernet1/1 statistics per-entry 10 permit udp 0000.1b40.ff13 0000.0000.0000 any range bootps bootpc vlan 100 [match=123] 20 permit udp 0000.1b40.ff13 0000.0000.0000 any eq domain vlan 100 [match=456] 30 deny 0000.1b40.ff13 0000.0000.0000 any [match=789]	設定済みの IP アクセス リストを表示します。
ステップ 6	(任意) <b>copy running-config startup-config</b> 例 :	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
	<code>switch(config)# copy running-config startup-config</code>	

## 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。

### Before you begin

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <code>switch# configure terminal</code> <code>switch(config)#</code>	グローバル 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	<b>interface ethernet <i>slot/port</i></b> <b>Example:</b> <code>switch(config)# interface ethernet 2/1</code> <code>switch(config-if)</code>	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	<b>dot1x host-mode {multi-host   single-host}</b> <b>Example:</b> <code>switch(config-if)# dot1x host-mode multi-host</code>	ホスト モードを設定します。デフォルトは、single-host です。 <b>Note</b> 指定したインターフェイスで <b>dot1x port-control</b> インターフェイス設定コマンドが <b>auto</b> に設定されていることを確認してください。
ステップ 4	<b>dot1x host-mode multi-auth</b> <b>Example:</b> <code>switch(config-if)# dot1x host-mode multi-auth</code>	複数認証モードを設定します。ポートは、EAPまたはMABのいずれか、または両方の組み合わせが正常に認証された場合にのみ許可されます。認証に失敗すると、ネットワーク アクセスが制限されます。 EAP または MAB の認証
ステップ 5	<b>exit</b> <b>Example:</b>	設定モードを終了します。

	Command or Action	Purpose
	<code>switch(config-if)# exit</code> <code>switch(config)#</code>	
ステップ 6	(Optional) <b>show dot1x all</b>  <b>Example:</b> <code>switch# show dot1x all</code>	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	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <code>switch(config)# copy running-config startup-config</code>	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。



**Note** 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。

### Before you begin

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> <code>switch# configure terminal</code> <code>switch(config)#</code>	グ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	<b>no dot1x system-auth-control</b>  <b>Example:</b> <code>switch(config)# no dot1x system-auth-control</code>	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。

	Command or Action	Purpose
		<b>Note</b> Cisco NX-OS デバイス上の 802.1X 認証をイネーブルにするには、 <b>dot1x system-auth-control</b> コマンドを使用します。
ステップ 3	<b>exit</b> <b>Example:</b> switch(config)# exit switch#	設定モードを終了します。
ステップ 4	(Optional) <b>show dot1x</b> <b>Example:</b> switch# show dot1x	802.1X 機能のステータスを表示します。
ステップ 5	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> 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。

## 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。

### Before you begin

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> switch# <b>configure terminal</b> 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	<b>no feature dot1x</b> <b>Example:</b>	802.1X 機能をディセーブルにします。

	Command or Action	Purpose
	<code>switch(config)# no feature dot1x</code>	<b>Caution</b> 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	<b>exit</b> <b>Example:</b> <code>switch(config)# exit</code> <code>switch#</code>	設定モードを終了します。
ステップ 4	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <code>switch# copy running-config startup-config</code>	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。

### Before you begin

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <code>switch# configure terminal</code> <code>switch(config)#</code>	グローバル 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	<b>interface ethernet slot/port</b> <b>Example:</b> <code>switch(config)# interface ethernet 2/1</code> <code>switch(config-if)</code>	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	<b>dot1x default</b> <b>Example:</b> <code>switch(config-if)# dot1x default</code>	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	<b>exit</b> <b>Example:</b> <code>switch(config-if)# exit</code> <code>switch(config)#</code>	設定モードを終了します。

	Command or Action	Purpose
ステップ 5	(Optional) <b>show dot1x all</b>  <b>Example:</b> switch(config)# show dot1x all	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	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> 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。

## インターフェイスでのオーセンティケータとサブリカント間のフレームの最大数の設定

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ブ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。

### Before you begin

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> 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	<b>interface ethernet slot/port</b>  <b>Example:</b> 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	<b>dot1x max-req count</b>  <b>Example:</b> 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。  <b>Note</b> 指定したインターフェイスで <b>dot1x port-control</b> インターフェイス設定コマンドが <b>auto</b> に設定されていることを確認してください。



	Command or Action	Purpose
ステップ 4	<b>exit</b> <b>Example:</b> 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	(Optional) <b>show dot1x all</b> <b>Example:</b> switch# show dot1x all	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	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> 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。

## 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。

### Before you begin

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	<b>dot1x radius-accounting</b> <b>Example:</b> 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	<b>exit</b> <b>Example:</b> switch(config)# exit switch#	設定モードを終了します。
ステップ 4	(Optional) <b>show dot1x</b> <b>Example:</b> switch# show dot1x	802.1X の設定を表示します。

	Command or Action	Purpose
ステップ 5	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch# copy running-config startup-config</pre>	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。

### Before you begin

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>	グローバル 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	<b>aaa accounting dot1x default group group-list</b>	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。  <i>group-list</i> 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。  <ul style="list-style-type: none"> <li>• <b>radius</b> : 設定済みのすべての RADIUS サーバ</li> <li>• <b>named-group</b> : 設定済みの任意の RADIUS サーバグループ名</li> </ul>
ステップ 3	<b>exit</b>	設定モードを終了します。
ステップ 4	(Optional) <b>show aaa accounting</b>	AAA アカウンティングの設定を表示します。
ステップ 5	(Optional) <b>copy running-config startup-config</b>	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。

**Example**

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ブ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。

**Before you begin**

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

**Procedure**

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	<b>interface ethernet slot/port</b> <b>Example:</b> 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	<b>dot1x max-reauth-req retry-count</b> <b>Example:</b> 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	<b>exit</b> <b>Example:</b> 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	(Optional) <b>show dot1x all</b> <b>Example:</b> switch# show dot1x all	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。

	Command or Action	Purpose
ステップ 6	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	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
<b>show dot1x</b>	802.1X 機能のステータスを表示します。
<b>show dot1x all</b> [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。
<b>show dot1x interface ethernet slot/port</b> [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。
<b>show running-config dot1x</b> [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。
<b>show startup-config dot1x</b>	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。

## VXLAN EVPN の 802.1X サポート

ここでは、VXLAN EVPN の 802.1X 機能の設定方法について説明します。

### VXLAN EVPN の 802.1X サポートに関する注意事項と制約事項

VXLAN EVPN の 802.1X サポートに関する注意事項と制約事項を次に示します。

- 
- ポートチャネルインターフェイスまたはポートチャネルのメンバーポートはサポートされません。
- vPC ポートはサポートされません。

- この機能の現在のサポートでは、802.1X セキュア MAC 更新のために BGP-EVPN コントロールプレーンで定期的および動的な EVPN 更新を使用します。そのため、グローバルポリシーが「dot1x mac-move deny」であっても、EVPN をまたいで移動することはできません。
- 「dot1x mac-move」ポリシーがファブリック全体で同じに設定されていることを確認します。ノード間で設定の検証は行われなため、設定ポリシーが同期していない場合は予期しない動作が発生する可能性があります。
- 拒否モードと許可モードのローカルからリモートへの MAC 移動動作は許可されます。したがって、拒否モードが有効になっていても、MAC 移動は許可されます。
- dot1x とポートセキュリティ ポートが異なる VLAN を使用していることを確認します。同じ VLAN を両方のポートに割り当てることはできません。
- Dot1x は VLAN に対応していないため、2 つの異なる VLAN で同じ MAC を使用することはできません。選択された MAC 移動モードに応じて、MAC は新しい VLAN に移動されるか、拒否されます。
- スタティック MAC とセキュア MAC を同時に設定することはできません。
- -R ライン カードを搭載した Cisco Nexus 9504 および Cisco Nexus 9508 プラットフォームスイッチは、VXLAN でのマルチ認証およびマルチ認証をサポートしていません。
- RADIUS の認可変更は VXLAN EVPN によりサポートされています。
- スケール設定の推奨再認証時間間隔はデフォルト値で、3600 秒です。

## VXLAN EVPN の 802.1X サポートの設定

この手順では、VXLAN EVPN の 802.1X を設定します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# <b>configure terminal</b>	グローバル 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	<b>feature dot1x</b> 例： switch(config)# <b>feature dot1x</b>	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	<b>dot1x mac-move {permit   deny}</b> 例： switch(config)# <b>dot1x mac-move permit</b>	<b>deny</b> パラメータは MAC 移動を拒否します。 <b>permit</b> パラメータは MAC 移動を許可します。

	コマンドまたはアクション	目的
ステップ 4	<p>(任意) <b>show running-config dot1x all</b></p> <p>例 :</p> <pre>switch(config)# show running-config dot1x all  !Command: show running-config dot1x all !No configuration change since last restart !Time: Thu Sep 20 10:22:58 2018  version 9.2(2) Bios:version 07.64 feature dot1x  dot1x system-auth-control dot1x mac-move deny  interface Ethernet1/1  dot1x host-mode multi-auth  dot1x pae authenticator  dot1x port-control auto  no dot1x re-authentication  dot1x max-req 1  dot1x max-reauth-req 2  dot1x timeout quiet-period 60  dot1x timeout re-authperiod 3600  dot1x timeout tx-period 1  dot1x timeout server-timeout 30  dot1x timeout ratelimit-period 0  dot1x timeout supp-timeout 30  dot1x timeout inactivity-period 0  dot1x mac-auth-bypass  interface Ethernet1/33  dot1x host-mode multi-auth  dot1x pae authenticator  dot1x port-control auto  no dot1x re-authentication  dot1x max-req 1  dot1x max-reauth-req 2  dot1x timeout quiet-period 60  dot1x timeout re-authperiod 3600  dot1x timeout tx-period 1  dot1x timeout server-timeout 30  dot1x timeout ratelimit-period 0  dot1x timeout supp-timeout 30  dot1x timeout inactivity-period 0  dot1x mac-auth-bypass</pre>	802.1X の設定を表示します。

## VXLAN EVPN の 802.1X サポートの確認

VXLAN の設定情報での 802.1X サポートを表示するには、次のいずれかのコマンドを入力します。

コマンド	目的
<b>show running-config dot1x all</b>	dot1x 実行設定を表示します。
<b>show dot1x all summary</b>	インターフェイスのステータスを表示します。
<b>show dot1x</b>	デフォルト設定を表示します。
<b>show dot1x all</b>	インターフェイスの詳細を表示します。

### show running-config dot1x all コマンドの例

```
switch# show running-config dot1x all
!Command: show running-config dot1x all
!No configuration change since last restart
!Time: Thu Sep 20 10:22:58 2018
```

```
version 9.2(2) Bios:version 07.64
feature dot1x
```

```
dot1x system-auth-control
dot1x mac-move deny
```

```
interface Ethernet1/1
 dot1x host-mode multi-auth
 dot1x pae authenticator
 dot1x port-control auto
 no dot1x re-authentication
 dot1x max-req 1
 dot1x max-reauth-req 2
 dot1x timeout quiet-period 60
 dot1x timeout re-authperiod 3600
 dot1x timeout tx-period 1
 dot1x timeout server-timeout 30
 dot1x timeout ratelimit-period 0
 dot1x timeout supp-timeout 30
 dot1x timeout inactivity-period 0
 dot1x mac-auth-bypass
```

```
interface Ethernet1/33
 dot1x host-mode multi-auth
 dot1x pae authenticator
 dot1x port-control auto
 no dot1x re-authentication
 dot1x max-req 1
 dot1x max-reauth-req 2
 dot1x timeout quiet-period 60
 dot1x timeout re-authperiod 3600
 dot1x timeout tx-period 1
 dot1x timeout server-timeout 30
 dot1x timeout ratelimit-period 0
 dot1x timeout supp-timeout 30
 dot1x timeout inactivity-period 0
 dot1x mac-auth-bypass
```

### show dot1x all summary コマンドの例

```
switch# show dot1x all summary
```

```

      Interface    PAE          Client      Status
-----
      Ethernet1/1  AUTH         none        UNAUTHORIZED

      Interface    PAE          Client      Status
-----
      Ethernet1/33 AUTH         00:16:5A:4C:00:07 AUTHORIZED
                        00:16:5A:4C:00:06 AUTHORIZED
                        00:16:5A:4C:00:05 AUTHORIZED
                        00:16:5A:4C:00:04 AUTHORIZED

```

switch#

switch# **show mac address-table vlan 10**

Legend:

\* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC  
age - seconds since last seen,+ - primary entry using vPC Peer-Link,  
(T) - True, (F) - False, C - ControlPlane MAC, ~ - vsan

VLAN	MAC Address	Type	age	Secure	NTFY	Ports
* 10	0016.5a4c.0004	secure	-	T	F	Eth1/33
* 10	0016.5a4c.0005	secure	-	T	F	Eth1/33
* 10	0016.5a4c.0006	secure	-	T	F	Eth1/33
* 10	0016.5a4c.0007	secure	-	T	F	Eth1/33

switch#

switch# **show mac address-table vlan 10 (VPC-PEER)**

Legend:

\* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC  
age - seconds since last seen,+ - primary entry using vPC Peer-Link,  
(T) - True, (F) - False, C - ControlPlane MAC, ~ - vsan

VLAN	MAC Address	Type	age	Secure	NTFY	Ports
* 10	0016.5a4c.0004	secure	-	T	F	vPC Peer-Link
* 10	0016.5a4c.0005	secure	-	T	F	vPC Peer-Link
* 10	0016.5a4c.0006	secure	-	T	F	vPC Peer-Link
* 10	0016.5a4c.0007	secure	-	T	F	vPC Peer-Link

switch#

switch# **show mac address-table vlan 10 (RVTEP)**

Legend:

\* - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC  
age - seconds since last seen,+ - primary entry using vPC Peer-Link,  
(T) - True, (F) - False, C - ControlPlane MAC, ~ - vsan

VLAN	MAC Address	Type	age	Secure	NTFY	Ports
C 10	0016.5a4c.0004	dynamic	0	F	F	nvel(67.67.67.67)
C 10	0016.5a4c.0005	dynamic	0	F	F	nvel(67.67.67.67)
C 10	0016.5a4c.0006	dynamic	0	F	F	nvel(67.67.67.67)
C 10	0016.5a4c.0007	dynamic	0	F	F	nvel(67.67.67.67)

### show dot1x コマンドの例

switch# **show dot1x**

```

      Sysauthcontrol Enabled
      Dot1x Protocol Version 2
      Mac-Move Deny

```

### show dot1x all コマンドの例

switch# **show dot1x all**

```

      Sysauthcontrol Enabled
      Dot1x Protocol Version 2
      Mac-Move Deny

```



```

Dot1x Info for Ethernet1/1
-----
          PAE = AUTHENTICATOR
          PortControl = AUTO
          HostMode = MULTI AUTH
          ReAuthentication = Disabled
          QuietPeriod = 60
          ServerTimeout = 30
          SuppTimeout = 30
          ReAuthPeriod = 3600 (Locally configured)
          ReAuthMax = 2
          MaxReq = 1
          TxPeriod = 1
          RateLimitPeriod = 0
          InactivityPeriod = 0
          Mac-Auth-Bypass = Enabled

Dot1x Info for Ethernet1/33
-----
          PAE = AUTHENTICATOR
          PortControl = AUTO
          HostMode = MULTI AUTH
          ReAuthentication = Disabled
          QuietPeriod = 60
          ServerTimeout = 30
          SuppTimeout = 30
          ReAuthPeriod = 3600 (Locally configured)
          ReAuthMax = 2
          MaxReq = 1
          TxPeriod = 1
          RateLimitPeriod = 0
          InactivityPeriod = 0
          Mac-Auth-Bypass = Enabled

```

## 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。

### Before you begin

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>show dot1x {all   interface ethernet slot/port} statistics</b>  <b>Example:</b> switch# <b>show dot1x all statistics</b>	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
```



**Note** 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	
VRF コンフィギュレーション	

### 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)』

標準	タイトル
RFC 3580	『IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines』





## 第 12 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。

この章は、次の項で構成されています。

- [ACL について, on page 305](#)
- [IP ACL の前提条件, on page 325](#)
- [IP ACL の注意事項と制約事項 \(326 ページ\)](#)
- [IP ACL のデフォルト設定, on page 334](#)
- [IP ACL の設定, on page 334](#)
- [IP ACL の設定の確認, on page 374](#)
- [IP ACL の統計情報のモニタリングとクリア \(377 ページ\)](#)
- [IP ACL の設定例, on page 378](#)
- [システム ACL について \(379 ページ\)](#)
- [オブジェクト グループの設定, on page 383](#)
- [オブジェクト グループの設定の確認, on page 387](#)
- [???????, on page 388](#)
- [時間範囲設定の確認, on page 392](#)
- [IP ACL に関する追加情報, on page 393](#)

## ACL について

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。

### 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

MAC ACL は非 IP トラフィックにだけ適用されます。

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

### UDF ベースの一致による MAC ACL

UDF ベースのマッチングで MAC ACL をフィルタリングします。

### 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

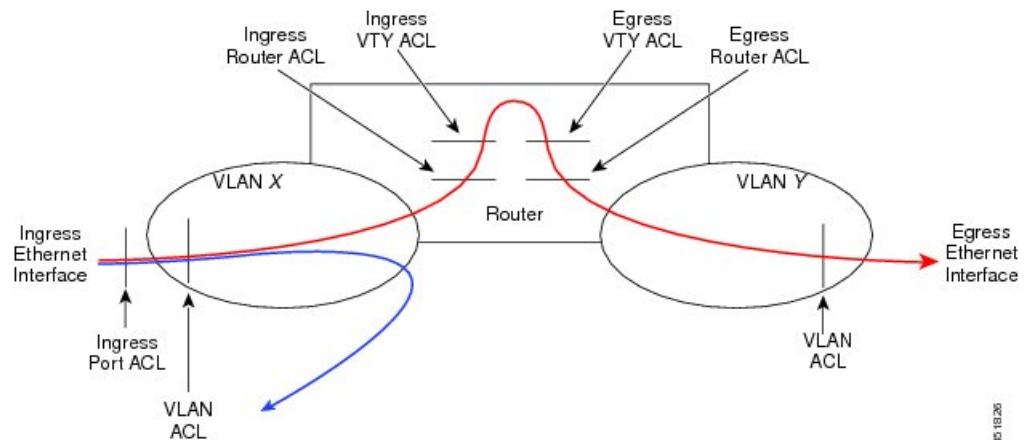
次の表に、セキュリティ ACL の適用例の概要を示します。

Table 15: セキュリティ ACL の適用

適用	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	<ul style="list-style-type: none"> <li>レイヤ 2 インターフェイス</li> <li>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</li> </ul> <p>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。</p>	<ul style="list-style-type: none"> <li>IPv4 ACL</li> <li>Cisco Nexus 9200、9300、および 9300-EX シリーズ スイッチの UDF ベースのマッチングで IPv4 ACL をサポートします。</li> <li>IPv6 ACL</li> <li>9300-EX シリーズ スイッチの UDF ベースのマッチングで IPv6 ACL をサポートします。</li> <li>MAC ACL</li> <li>UDF ベースのマッチングを行う MAC ACL。</li> </ul>
ルータ ACL	<ul style="list-style-type: none"> <li>VLAN インターフェイス</li> <li>物理層 3 インターフェイス</li> <li>レイヤ 3 イーサネット サブインターフェイス</li> <li>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</li> <li>管理インターフェイス</li> </ul> <p><b>Note</b> 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。</p>	<ul style="list-style-type: none"> <li>IPv4 ACL</li> <li>IPv6 ACL</li> </ul> <p><b>Note</b> 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。</p> <p><b>Note</b> 出力ルータ ACL は、サブインターフェイスおよび Cisco Nexus 9300 シリーズ スイッチのアップリンク ポートではサポートされていません。</p>
VLAN ACL	<ul style="list-style-type: none"> <li>VLAN</li> </ul>	<ul style="list-style-type: none"> <li>IPv4 ACL</li> <li>IPv6 ACL</li> <li>MAC ACL</li> </ul>
VTY ACL	<ul style="list-style-type: none"> <li>VTY</li> </ul>	<ul style="list-style-type: none"> <li>IPv4 ACL</li> <li>IPv6 ACL</li> </ul>







## 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増えることがあります。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。

アクセスリストコンフィギュレーションモードでルールを作成するには、**permit**または**deny**コマンドを使用します。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。

## IP ACL および MAC 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の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。

## 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 ACL、IPv6 ACL、MAC ACL のどの ACL を設定するのかによって異なります。

## 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、次の暗黙のルールがあります。

```
deny ipv6 any any
```

この暗黙ルールによって、デバイスは不一致 IPv6 トラフィックを確実に拒否します。



**Note** IPv6 の nd-na、nd-ns、router-advertisement、router-solicitation パケットは、IPv6 ACL の暗黙の許可ルールとしては使用できません。明示的に許可するには、次の規則を追加する必要があります。

- **permit icmp any any nd-na**
- **permit icmp any any nd-ns**
- **permit icmp any any router-advertisement**
- **permit icmp any any router-solicitation**

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
  - 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
  - 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
  - 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 (Ethertype)
  - VLAN ID
  - サービス クラス (CoS)
  
- Cisco NX-OS リリース 9.2(4) 以降、N9K-X96136YC-R、N9K-X9636C-R、および N9K-X9636C-RX ラインカードと N9K-C9504-FM-R を搭載した Cisco Nexus 9500 プラットフォーム スイッチの IPv4 ACL および IPv6 ファブリック モジュールは、次の追加のフィルタリング オプションをサポートしています。
  - 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

## 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。

### 既存のルールの中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。

また、Cisco NX-OS では、ACL 内ルールのシーケンス番号を再割り当てできます。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、それらのルールの上に 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。Cisco NX-OS では、入力方向でのみ論理演算子をサポートします。

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。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 LOU を使用します。
- lt**  
1 LOU を使用します。
- neq**  
1 LOU を使用します。
- range**  
1 LOU を使用します。

## IPv4 ACL ロギング

IPv4 ACL ロギング機能は、IPv4 ACL のフローをモニタし、統計情報をログに記録します。

フローは、送信元インターフェイス、プロトコル、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、宛先ポート値によって定義されます。フローの統計情報には、転送されたパケット（ACL エントリの許可条件に一致する各フロー）およびドロップされたパケット（ACL エントリの拒否条件に一致する各フロー）の数が含まれます。

## 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、時間範囲を名前ですべて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。



**Note** 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、ポリシーベース ルーティング (PBR)、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。



#### Note

ポリシーベース ルーティング (PBR) ACL は、アクセス コントロール エントリ (ACE) の拒否または **deny** コマンドによるルール設定をサポートしません。

## 統計情報と ACL

このデバイスは IPv4、IPv6、および MAC の 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。



**Note** 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트는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。

### Related Topics

[IP ACL の統計情報のモニタリングとクリア](#) (377 ページ)

[IP ACL および MAC ACL の暗黙ルール](#) (310 ページ)

## Atomic ACL のアップデート

デフォルトでは、Cisco Nexus 9000 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はありません。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。

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
```

## 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。

## ACL TCAM リージョン

ハードウェアの ACL Ternary Content Addressable Memory (TCAM) リージョンのサイズを変更できます。

Cisco Nexus 9300 と 9500 シリーズ スイッチおよび、Cisco Nexus 3164Q、31128PQ、3232C、および 3264Q スイッチの場合、出力 TCAM のサイズは 1K で、4 つの 256 エントリに分割されています。Cisco Nexus NFE2 対応デバイス (Cisco Nexus 3232C や 3264Q スイッチなど) の場合、入力 TCAM のサイズは 6K で、12 の 512 スライスに分割されています。3 つのスライスが 1 つのグループにされます。他の Cisco Nexus 9300 と 9500 シリーズ スイッチおよび 3164Q と 31128PQ の場合、入力 TCAM のサイズは 4K で、8 つの 256 スライスと 4 つの 512 スライスに分割されています。各スライスが、割り当てユニットになります。1 つのスライスを割り当てることができるのは 1 つのリージョンだけです。たとえば、1 つのサイズ 512 のスライスを使用してサイズ 256 の機能を 2 つ設定することはできません。同様に、1 つのサイズ 256 のスライスを使用してサイズ 128 の機能を 2 つ設定することはできません。IPv4 TCAM リージョンはシングル幅です。IPv6、QoS、MAC、CoPP およびシステム TCAM リージョンはダブル幅であり、物理 TCAM エントリの 2 倍を消費します。たとえば、サイズ 256 の論理リージョン エントリが実際に消費する物理 TCAM エントリは 512 です。

IPv6、ポート ACL、VLAN ACL、およびルータ ACL を作成して、QoS の IPv6 および MAC アドレスを照合できます。ただし、Cisco NX-OS ではすべてを同時にサポートすることはできません。IPv6、MAC、その他の所要の TCAM リージョンをイネーブルにするには、既存の TCAM リージョン (TCAM カービング) を削除するか、サイズを減らす必要があります。個々の TCAM リージョンのコンフィギュレーション コマンドでは、新しい変更結果が TCAM に適合するかが、システムにより評価されます。適合しない場合は、エラーがレポートされ、コマンドは拒否されます。新しい要件に適した領域を確保するには、既存の TCAM リージョンを削除するか、サイズを減らす必要があります。

Cisco Nexus 9200 シリーズ スイッチの場合、出力 TCAM のサイズは 2K で、入力 TCAM のサイズは 4K です。TCAM スライスおよび、シングル幅とダブル幅の概念は、これらのスイッチには適用されません。たとえば、ing-ifacl リージョンは、IPv4、IPv6、または MAC タイプのエントリをホストできます。IPv4 および MAC タイプが 1 つの TCAM エントリを占めるのに対して、IPv6 タイプは 2 つの TCAM エントリを占めます。

N9K-X9636C-RX では、PACL が外部 TCAM リージョンを使用する場合、内部 TCAM は ifacl に 2K を使用する必要があります、入力 RAACL-IPv4 は最大 2044 を使用できます。出力 PACL 外部 TCAM リージョンを使用する場合は、追加の 4 つのエントリが必要です。

ACL TCAM リージョン サイズには、次の注意事項と制約事項があります。

- 既存の TCAM リージョンで RAACL または PACL をイネーブル化するには、12,288 を超える TCAM リージョンを分割する必要があります。
- Cisco Nexus 9300 シリーズ スイッチの場合、X9536PQ、X9564PX、および X9564TX ラインカードを使用して、40G ポートでの QoS 分類ポリシーの適用が強制されます。ここでは、256 エントリの粒度でのカービングに使用できる 768 の TCAM エントリが利用可能です。これらのリージョン名にはプレフィックス「ns-」が付けられます。
- X9536PQ、X9564PX、および X9564TX ラインカードの場合、IPv6 TCAM リージョンだけがダブル幅のエントリを消費します。他の TCAM リージョンは、シングル幅のエントリを消費します。
- VACL リージョンを設定する場合、入力と出力の両方向で同じサイズが設定されます。リージョン サイズがいずれかの方向に対応できない設定は拒否されます。
- Cisco Nexus 9200 シリーズ スイッチの場合、ing-sup リージョンは 512 エントリの最小サイズを占め、egr-sup リージョンは 256 エントリの最小サイズを占めます。これらのリージョンをより小さい値に設定することはできません。リージョンサイズのカービングは 256 エントリの倍数でのみ行えます（スパンリージョンは例外で、512 エントリの倍数でのカービングのみが可能です）。
- RAACL v6、CoPP、およびマルチキャストの TCAM サイズはデフォルト値です。以下の Cisco Nexus 9504 および Cisco Nexus 9508 ラインカードでは、リロード中にラインカード障害が発生しないように、これらの TCAM サイズをゼロ以外にする必要があります。
  - N9K-X96136YC-R
  - N9K-X9636C-RX
  - N9K-X9636Q-R
  - N9K-X9636C-R
- 出力 RAACL が 4K を超える場合、TCAM カービング設定では、入力 RAACL (RAACL) + 出力 RAACL (e-racl) の合計を 20480 にする必要があります。次の TCAM カービングの例を参照してください。

```
hardware access-list tcam region ifacl 0
hardware access-list tcam region ipv6-ifacl 0
hardware access-list tcam region mac-ifacl 0
hardware access-list tcam region racl 0
```

```
hardware access-list tcam region ipv6-racl 0
hardware access-list tcam region span 0
hardware access-list tcam region redirect_v4 0
hardware access-list tcam region redirect_v6 0
hardware access-list tcam region e-racl 20480
```

- IPv6 RACL は IPv6 IFCAL で部分的に使用できます。これは、N9K-X96136YC-R、N9K-X9636C-R、N9K-X9636Q-R、および N9K-X9636C-RX ラインカードを搭載した Cisco Nexus N9K-C9508 および N9K-C9504 に適用されます。
- N9K-X9636C-R および N9K-X9636Q-R ラインカードは、最大 12K の TCAM リージョン サイズをサポートします。より大きな数を設定しても、TCAM リージョンは 12K に設定されます。
- N9K-X96136YC-R および N9K-X9636C-R ラインカードは、2K の出力 RACL をサポートします。
- N9K-X9636C-RX ラインカードは、12K を超える TCAM リージョン サイズをサポートします。RACL IPv4 TCAM リージョンを 100K に設定したときの TCAM リージョンのサイズは、N9K-X9636C-R および N9K-X9636Q-R ラインカードの場合は 12K に、N9K-X9636C-RX ラインカードの場合は 100K に設定されます（他のすべての TCAM リージョンは設定されており、N9K-X9636C-R および N9K-X9636Q-R ラインカード用に 12K に対応するだけのスペースがあることを条件とします）。
- N9K-X9636C-RX ラインカードでは、内部 TCAM に加えて、128K の外部 TCAM を使用できます。

次の表に、特定機能を動作させるために設定が必要なリージョンを示します。リージョンのサイズは、各機能のスケール要件に基づいて選択する必要があります。

表 16: ACL TCAM リージョンごとの機能

機能名	リージョン名
ポート ACL	<p>ifacl : IPv4 ポート ACL 用</p> <p>ifacl-udf : IPv4ポート ACL の UDF 用 (Cisco Nexus 3232C および 3264Q スイッチのみ)</p> <p>ing-ifacl : 入力 IPv4、IPv6、および MAC ポート ACL 用 (Cisco Nexus 9200、9300、および 9300-EX シリーズ スイッチのみ)</p> <p>ing-ifacl : 入力 IPv4、IPv6、MAC ポート ACL、および MAC ポート ACL の UDF 用 (Cisco Nexus 9200、9300、および 9300-EX シリーズ スイッチのみ)</p> <p>ipv6-ifacl : IPv6 ポート ACL 用</p> <p>mac-ifacl : MAC ポート ACL 用</p>
ポート QoS (レイヤ 2 ポートまたはポート チャンネルに適用される QoS 分類ポリシー)	<p>qos、qos-lite、rp-qos、rp-qos-lite、ns-qos、e-qos、または e-qos-lite : IPv4 パケット分類用</p> <p>ing-l2-qos : 入力レイヤ 2 パケット分類用 (Cisco Nexus 9200 シリーズ スイッチのみ)</p> <p>ipv6-qos、rp-ipv6-qos、ns-ipv6-qos、または e-ipv6-qos : IPv6 パケット分類用</p> <p>mac-qos、rp-mac-qos、ns-mac-qos、または e-mac-qos : 非 IP パケット分類用</p> <p>(注) Cisco Nexus 9300 シリーズ スイッチの 40G ポートで分類する必要があるトラフィックの場合、qos リージョンおよび対応する ns-*qos 領域をカービングする必要があります。</p>

機能名	リージョン名
VACL	vacl : IPv4 パケット用 ipv6-vacl : IPv6 パケット用 mac-vacl : 非 IP パケット用
VLAN QoS (VLAN に適用される QoS 分類ポリシー)	vqos または ns-vqos : IPv4 パケット分類用 ipv6-vqos または ns-ipv6-vqos : IPv6 パケット分類用 ing-l3-vlan-qos : 入力レイヤ 3、VLAN、および SVI QoS パケット分類用 (Cisco Nexus 9200 シリーズスイッチのみ) mac-vqos または ns-mac-vqos : 非 IP パケット分類用 (注) Cisco Nexus 9300 シリーズスイッチの 40G ポートで分類する必要があるトラフィックの場合、qos リージョンおよび対応する ns-*qos 領域をカービングする必要があります。
RACL	egr-racl : 出力 IPv4 および IPv6 RACL 用 (Cisco Nexus 9200 シリーズスイッチのみ) e-racl : 出力 IPv4 RACL 用 e-ipv6-racl : 出力 IPv6 RACL 用 ing-racl : 入力 IPv4 および IPv6 RACL 用 (Cisco Nexus 9200 シリーズスイッチのみ) racl : IPv4 RACL 用 racl-lite : IPv4 RACL 用 (Cisco Nexus 3232C および 3264Q スイッチのみ) racl-udf : IPv4 RACL 上の UDF 用 (Cisco Nexus 3232C および 3264Q スイッチのみ) ipv6-racl : IPv6 RACL 用

機能名	リージョン名
レイヤ 3 QoS (レイヤ 3 ポートまたはポート チャンネルに適用される QoS 分類ポリシー)	l3qos、l3qos-lite、または ns-l3qos : IPv4 パケット分類用  ipv6-l3qos または ns-ipv6-l3qos : IPv6 パケット分類用  (注) Cisco Nexus 9300 シリーズスイッチの 40G ポートで分類する必要があるトラフィックの場合、qos リージョンおよび対応する ns-*qos 領域をカービングする必要があります。
VLAN 送信元または VLAN フィルタ SPAN (Cisco Nexus 9500 または 9300 シリーズ スイッチ)  40G ポートの Rx SPAN (Cisco Nexus 9300 シリーズ スイッチのみ)	span

機能名	リージョン名
SPAN フィルタ	<p><b>ifacl</b> : レイヤ2 (スイッチポート) 送信元インターフェイスでの IPv4 トラフィック フィルタリング用。</p> <p><b>ifacl-udf</b> : IPv4ポート ACL の UDF 用 (Cisco Nexus 3232C および 3264Q スイッチのみ)</p> <p><b>ipv6-ifacl</b> : レイヤ2 (スイッチポート) 送信元インターフェイスでの IPv6 トラフィック フィルタリング用。</p> <p><b>mac-ifacl</b> : レイヤ2 (スイッチポート) 送信元インターフェイスでの レイヤ2 トラフィック フィルタリング用。</p> <p><b>racl-udf</b> : IPv4 RACL 上の UDF 用 (Cisco Nexus 3232C および 3264Q スイッチのみ)</p> <p><b>vacl</b> : VLAN 送信元での IPv4 トラフィック フィルタリング用。</p> <p><b>ipv6-vacl</b> : VLAN 送信元での IPv6 トラフィック フィルタリング用。</p> <p><b>mac-vacl</b> : VLAN 送信元での レイヤ2 トラフィック フィルタリング用。</p> <p><b>racl</b> : レイヤ3 インターフェイスでの IPv4 トラフィック フィルタリング用。</p> <p><b>ipv6-racl</b> : レイヤ3 インターフェイスでの IPv6 トラフィック フィルタリング用。</p> <p><b>ing-l2-span-filter</b> : 入力レイヤ2 SPAN トラフィックのフィルタリング用 (Cisco Nexus 9200 シリーズ および 9300-EX シリーズ スイッチのみ)</p> <p><b>ing-l3-span-filter</b> : 入力レイヤ3 および VLAN SPAN トラフィックのフィルタリング用 (Cisco Nexus 9200 および 9300-EX シリーズ スイッチのみ)</p>

機能名	リージョン名
SVI カウンタ  (注) このリージョンは、レイヤ3 SVI インターフェイスの packets カウンタをイネーブルにします。	svi
BFD、DHCP リレー、または DHCPv6 リレー	redirect  (注) Cisco Nexus 9200 シリーズスイッチの場合、BFD が使用するのは ing-sup リージョンですが、DHCPv4 リレー、DHCPv4 スヌーピング、および DHCPv4 クライアントが使用するのは ing-redirect リージョンです。
CoPP	copp  (注) リージョンサイズは 0 にできません。
システム管理型 ACL	system  (注) リージョンサイズは変更できません。
vPC コンバージェンス  (注) このリージョンは、vPC リンクがダウンしてトラフィックのピアリンクへのリダイレクトが必要となった場合に、コンバージェンス時間をブーストします。	vpc-convergence  (注) このリージョンサイズを 0 に設定すると、vPC リンク障害時のコンバージェンス時間に影響を与える可能性があります。
ファブリック エクステンダ (FEX)	fex-ifacl、fex-ipv6-ifacl、 fex-ipv6-qos、fex-mac-ifacl、 fex-mac-qos、fex-qos、fex-qos-lite
ダイナミック ARP インспекション (DAI)	arp-ether
IP ソース ガード (IPSG)	ipsg
マルチキャスト PIM Bidir	mcast_bidir (Broadcom ベースの Cisco Nexus 9000 シリーズスイッチのみ)
スタティック MPLS	mpls



機能名	リージョン名
ネットワーク アドレス変換 (NAT)	nat
NetFlow	ing-netflow
OpenFlow	OpenFlow
sFlow	sflow
スーパーバイザ モジュール	egr-sup : 出力スーパーバイザ (Cisco Nexus 9200 シリーズ スイッチのみ) ing-sup : 入力スーパーバイザ (Cisco Nexus 9200 シリーズ スイッチのみ)

#### 関連トピック

[ACL TCAM リージョン サイズの設定 \(342 ページ\)](#)

[TCAM カービングの設定 \(356 ページ\)](#)

## ACL タイプでサポートされる最大ラベル サイズ

Cisco NX-OS スイッチは、対応する ACL タイプに対して次のラベル サイズをサポートします。

表 17: ACL タイプと最大ラベル サイズ

ACL タイプ	方向 (Direction)	Label	ラベルタイプ
RACL/PBR/VACL/L3-VLAN QoS/L3-VLAN SPAN ACL	受信側	62	BD
PACL/L2 QoS/L2 SPAN ACL	受信側	62 <sup>1</sup>	IF
RACL/VACL/L3-VLAN QoS	送信側	254	BD
L2 QoS	送信側	31	IF

<sup>1</sup> `hardware access-list tcam label ing-ifacl 6` コマンドを入力してスイッチをリロードすると、ラベル サイズを 62 に増やすことができます。Cisco NX-OS リリース 9.3 (6) 以降では、`hardware access-list tcam label ing-ifacl 6` コマンドが導入され、Cisco Nexus 9300-FX プラットフォーム スイッチにのみ適用されます。

## 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。

- 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、1,000 以上のルールが含まれている ACL に対して特に推奨されます。**Session Manager** の詳細については、『*Cisco Nexus 9000 Series NX-OS System Management Configuration Guide*』を参照してください。
- 12K ～ 64K の範囲の IPv4 PAACL の設定は、-RX ラインカードを搭載した Cisco Nexus 9500 シリーズ スイッチでサポートされます。
- 異なるシーケンス番号を持つ重複した ACL エントリは、設定で許可されます。ただし、これらの重複エントリはハードウェア アクセス リストにプログラムされません。
- 最大 62 の一意の ACL を設定できます。各 ACL は、1 つのラベルを持ちます。同じ ACL が複数のインターフェイスで設定される場合、同じラベルが共有されます。ただし、各 ACL が一意のエントリを持つ場合、ACL のラベルは共有されず、そのラベルの上限は 62 です。これは、Cisco Nexus 9500 シリーズ スイッチおよび Cisco Nexus 3636C-R スイッチには適用されません。
- 通常、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（他の 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。
- 時間範囲を使用する ACL を適用すると、デバイスは、その ACL エントリで参照される時間範囲の開始時または終了時に ACL エントリを更新します。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。時間範囲によつ

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 9000 Series NX-OS Interfaces Configuration Guide』を参照してください。
- 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。
- 出力 VTY ACL (アウトバウンド方向の VTY 回線に適用される IP ACL) は、ファイル転送プロトコル (TFTP、FTP、SCP、SFTP など) が出力 VTY ACL 内で明示的に許可されていない限り、スイッチがファイル転送プロトコルによってファイルをコピーするのを禁止します。
- 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。
- IP トンネルでは、ACL または QoS ポリシーがサポートされません。
- VXLAN の ACL には、次のガイドラインが適用されます。
  - アクセスからネットワーク方向 (レイヤ 2 からレイヤ 3 のカプセル化パス) のトラフィックに対してレイヤ 2 ポートに適用される入力ポート ACL は、内部ペイロードでサポートされます。
  - ポート ACL をアクセス側で使用して、オーバーレイ ネットワークに進入するトラフィックをフィルタ処理して除外することを推奨します。
  - ネットワークからアクセス方向 (レイヤ 3 からレイヤ 2 のカプセル化解除パス) の内部または外部ペイロードで照合されるアップリンクレイヤ 3 インターフェイスに適用される入力ルータ ACL はサポートされません。
  - アクセスからネットワーク方向 (カプセル化パス) の内部または外部ペイロードで照合されるアップリンクレイヤ 3 インターフェイスに適用される出力ルータ ACL はサポートされません。
- Cisco Nexus 9300 および 9500 シリーズスイッチ、および Cisco Nexus 9200 および 9300-EX シリーズスイッチには、VXLAN トラフィックで使用できる ACL オプションに関する次の制限があります。
  - ネットワークからアクセス方向 (カプセル化解除パス) のトラフィックに対する、レイヤ 2 ポートに適用される出力ポート ACL はサポートされません。
  - アクセスからネットワーク方向 (カプセル化パス) のトラフィックに対する、VLAN に適用される入力 VACL はサポートします。
  - ネットワークからアクセス方向 (カプセル化解除パス) のトラフィックに対する、VLAN に適用される出力 VACL はサポートします。

- アクセスからネットワーク方向（カプセル化パス）のトラフィックに対する、SVIに面するテナントまたはサーバに適用される入力 RACL はサポートします。
- ネットワークのアクセス方向（カプセル化解除パス）へのトラフィック用に、テナントまたはサーバに適用される出力 RACL はサポートします。
- IPv6 ACL のロギングはサポートされません。
- 出力方向の IPv4 ACL ロギングはサポートされません。
- VACL の ACL ロギングはサポートされません。
- ACL ロギングは、**ip port access-group** コマンドによって設定されたポート ACL と、**ip access-group** コマンドによって設定されたルータ ACL にのみ適用されます。
- IPv4 ACL フローの総数は、DoS 攻撃を避けるためにユーザ定義の最大値に限定されます。この制限に到達すると、新しいログは既存のフローが終了するまで作成されません。
- IPv4 ACL ロギングによって生成される syslog エントリ数は、ACL ロギングプロセスで設定されたログレベルによって制限されています。syslog エントリの数がこの制限を超えると、ロギング機能が一部のロギングメッセージをドロップする場合があります。したがって、IPv4 ACL ロギングは課金ツールや ACL との一致数を正確に把握するための情報源として使用しないでください。
- 出力ルータ ACL は、サブインターフェイスおよび Cisco Nexus 9300 シリーズ スイッチのアップリンク ポートではサポートされていません。
- Cisco NX-OS リリース 9.2(1) では、N9K-X9636C-R、N9K-X9636C-RX、および N9K-X9636Q-R ライン カードを搭載した Cisco Nexus 9508 スイッチでの出力 ACL はサポートされていません。
- レイヤ 3 の物理または論理インターフェイスに適用されるルータ ACL がマルチキャストトラフィックとマッチしません。マルチキャストトラフィックをブロックする必要がある場合は、代わりに PAACL を使用します。この動作は、Cisco Nexus 9000、9300、9300-EX と 9500 シリーズ スイッチ、および Cisco Nexus 3164Q、31128PQ、3232C、および 3264Q スイッチに適用されます。
- ネットワーク フォワーディング エンジン（NFE）対応スイッチの場合、トンネルインターフェイスの外部ヘッダーで照合される入力 RACL はサポートされません。
- 複数のインターフェイスに同じ QoS ポリシーと ACL が適用された場合、ラベルが共有されるのは、QoS ポリシーが **no-stats** オプションで適用されたときだけです。
- スイッチ ハードウェアは、出力 TCAM でのレンジチェック（レイヤ 4 オペレーション）をサポートしません。したがって、レイヤ 4 オペレーションベースの分類をする ACL および QoS ポリシーは、出力 TCAM での複数エントリに拡張する必要があります。この制限は、出力 TCAM スペースの計画で考慮するようにしてください。
- N9K-X96136YC-R、N9K-X9636C-RX、N9K-X9636C-RX、N9K-X9636Q-R の場合は、**hardware profile acl-eg-ext module all** コマンドを、**eg-racl-v6** を EoR スイッチの SVI またはポートオブジェクトに適用する前に実行します。

- TCAM リソースは次のシナリオで共有されます。
  - ルーテッド ACL を複数のスイッチ仮想インターフェイス (SVI) に入力方向で適用する場合。
  - ルーテッド ACL を複数の物理レイヤ 3 インターフェイスに入力または出力方向で適用する場合。
- TCAM リソースは次のシナリオでは共有されません。
  - VACL (VLAN ACL) が複数の VLAN に適用される場合。
  - ルーテッド ACL を出力方向の複数の SVI に適用する場合。
- HTTP 方式に基づくアクセスリストは、Cisco Nexus 9200、9300-EX、9300-FX、9300-FX2、9300-FXP、および 9300-GX プラットフォームスイッチと、N9K-X9700-EX および N9K-X9700-FX ラインカードではサポートされません。これらすべてのスイッチでは、UDF ベースの ACL を使用する必要があります。
- HTTP メソッドは FEX ポートではサポートされません。
- **mode tap aggregation** コマンドは、MPLS ストリッピングで使用する場合を除き、TAP アグリゲーションで必要とされません。ただし HTTP メソッドは、MPLS パケットのストリップ後はサポートされません。
- 次の注意事項と制約事項は、Cisco Nexus 9200 および 9200-EX シリーズ スイッチに適用されます。
  - 出力 MAC ACL はサポートされません。
  - トンネルがトラフィックの発信元となっているデバイスでのトンネルインターフェイスの外部ヘッダーでパケットが照合される場合、出力 RACL はインターフェイスでサポートされません。
  - トンネル インターフェイスの外部ヘッダーで照合される入力 RACL はサポートされません。
  - IP 長ベースの照合はサポートされません。
  - すべての ACL ベースの機能を同時に有効にすることはできません。
  - 16 のレイヤ 4 オペレーションがサポートされます。
  - レイヤ 4 オペレーションは、出力 TCAM リージョンではサポートされません。
  - MAC 圧縮テーブルのサイズは 4096 + 512 オーバーフロー TCAM です。
  - MAC アドレスと MAC マスクのオーバーラップは拒否されます。
  - ACL ログ レート リミッタには、送信またはドロップされたパケットに関するハードウェア カウンタはありません。

- ACL ログ レート リミッタの実装は各 TCAM エントリ レベルで行われ（集約されたレート制限を使用するのではなく）、デフォルトは 1 pps です。
- ネットワーク アドレス変換 (NAT) の例外カウンタはゼロです。
- TAP アグリゲーションでは PAACL リダイレクトだけがサポートされます。VAACL リダイレクトはサポートされていません。
- DHCPv4 スヌーピングまたはリレー、DHCPv6 リレー、ARP スヌーピング、VXLAN の 4 つの機能のうち、同時にサポートできるのは 3 つだけです。適用されるのは最初に設定された 3 つの機能であり、3 つのブリッジドメイン ラベル ビットがすべて使用中になるため、4 番目は失敗します。
- RAACL は、マルチキャスト MAC 宛先アドレスを持つパケットでは照合できません。
- 次の注意事項と制約事項は、Cisco Nexus 9364C-GX、Cisco Nexus 9316D-GX、および Cisco Nexus 93600CD-GX シリーズ スイッチに適用されます。
  - MAC 圧縮テーブルのサイズは 4096 + 512 オーバーフロー TCAM です。
  - MAC アドレスと MAC マスクのオーバーラップは拒否されます。
- -R ラインカードを備えた Cisco Nexus 9504 および 9508 プラットフォーム スイッチでは、次の TCAM はサポートされません。
  - すべての FEX 関連 TCAM
  - すべての xxx-lite 関連の TCAM リージョン
  - レンジャー関連の TCAM
  - すべての FCoE 関連の TCAM
- ing-netflow リージョンの TCAM カービング設定は、-FX ラインカードでは実行できます。-EX ラインカードでは、デフォルトの ing-netflow リージョン TCAM カービングが 1024 であり、それ以外の場合は設定できません。-EX および -FX ラインカードのポートの場合、ing-netflow リージョンの推奨最大値は 1024 です。
- Cisco Nexus 9200 および 9300-EX シリーズスイッチでは、sup-redirect ACL の方が SUP 宛てのトラフィックに対してより高いプライオリティを持っているため、ACL ログオプションを使用したルータ ACL は有効になりません。
- FHRP VIP 宛てのトラフィックで、トラフィックを許可するように設計された ACL ログが有効な ACE と一致する FHRP スタンバイで入力されるトラフィックの場合、Cisco Nexus 9000 シリーズスイッチはこのパケットをドロップします。
- Cisco Nexus 3048、3172PQ、3172TQ、3132Q-X、3172PQ-XL、3172TQ-XL、31108PC-V、31108TC-V、3132Q-V、3132C-Z、3232C、3264Q、3264C-E、36180YC-R および 3636C-R スイッチでは、同じ VLAN タグに一致する SVI およびサブインターフェイスがある場合、その SVI でアクセスリストが設定されていると、サブインターフェイスを介してルーティ

ングされるトラフィックはドロップされます。これはASICの制限によるもので、L3サブインターフェイスの出力ルータ ACLはこの制限によりサポートされません。

- Cisco NX-OS リリース 9.2(2) では、N9K-X96136YC-R、N9K-X9636C-R、N9K-X9636Q-R、および N9K-X9636C-RX ラインカードを搭載したCisco Nexus 9508 および 9504 プラットフォームスイッチの、出力ルータ ACL での次の機能は、サポートされていません。
  - ICMP Type Match をサポートするUDF。
  - ACL ログオン出力
  - 追加のフィルタオプション tcp/udp ポートと lt/gt を指定した出力 IPv4 ルータ ACL
  - 追加のフィルタオプション tcp/udp ポートと neq を含む出力 IPv4 ルータ ACL
  - 範囲付きの追加のフィルタオプション tcp/udp ポートを含む出力 IPv4 ルータ ACL
  - フラグ付き出力 IPv4 ルータ ACL
  - 外部 TCAM の出力ルータ ACL
  - 出力 PACL のサポート
  - 統計のサポート
  - ラベル共有
- Cisco NX-OS リリース9.2(3) では、-R および -RX ラインカードを備えた Cisco Nexus 9500 プラットフォーム スイッチは、ACL で次をサポートします。
  - 統計のサポート
  - ラベル共有
- Cisco NX-OS リリース9.2(3) では、-R および -RX ラインカードを備えた Cisco Nexus 9500 プラットフォーム スイッチには、次の注意事項があります。
  - アトミック ACL 更新は、マルチホップ BFD および CoPP 機能を除くすべての入力 ACL 機能でサポートされます。
  - アトミック ACL 更新は、出力 ACL 機能ではサポートされません。
  - ラベル共有は、同じ ASIC 内の異なるインターフェイス上の同じポリシーでのみサポートされます。
  - Cisco NX-OS リリース 9.2(3) では、次の ACL 統計情報がサポートされています。
    - PACL : IPv4 (内部、外部両方の TCAM を含む)
    - ルータ ACL : IPv4 (入力 RAACL-IPv4 と出力 RAACL-IPv4 の両方の内部 TCAM)
    - 出力では 2K カウンタのみがサポートされます。
  - Cisco NX-OS リリース 9.2(3) では、次のACL統計情報はサポートされていません。

- BFD
  - DHCP : IPv4およびIPv6
  - PACL : MAC
  - PACL : IPv6
  - PBR : IPv4 および IPv6
  - RAACL : Pv6
  - 外部 TCAM を使用する場合は RAACL : IPv4
- 
- `hardware profile acl-stats module xx` コマンドを使用して ACL TCAM エントリのカウンタをイネーブルにすると、`show interface` の `input discard` フィールドは常にゼロになります。この制限は、-R および -RX ラインカードを備えた Cisco Nexus 9500 プラットフォームスイッチにのみ適用されます。
  - Cisco NX-OS リリース 9.3(3) では、-R および -RX ラインカードを備えた Cisco Nexus 9500 プラットフォームスイッチは、以下をサポートしません。
    - 出力のアトミック アップデート
    - 外部 TCAM の出力ルータ ACL
    - UDF を伴う出力ルータ ACL
    - 出力と入力の両方のルータ ACL v6 カウンタ
    - 14 ops による出力および出力ルータ ACL IPv6
    - サブインターフェイスの出力ルータ ACL
    - IPv6 ICMP タイプおよびコードによる出力および入力ルータ ACL
    - tcp-flag を使用した IPv6 入力ルータ ACL
    - 追加オプション付きの IPv4 ルータ ACL
  - Cisco NX-OS リリース 9.3(3) では、出力 IPv6 RAACL は、-R および -RX ラインカードを備えた Cisco Nexus 9500 プラットフォーム スイッチで次をサポートします。
    - レイヤ 4 プロトコル
    - TCP フラグ
    - フラグメント
    - ACL ログ
  - Cisco NX-OS リリース 9.3(3) では、出力 IPv4 RAACL は、-R および -RX ラインカードを備えた Cisco Nexus 9504 および 9508 プラットフォーム スイッチで次をサポートします。
    - TCP フラグ



- ICMP のタイプとコード
- ACL ログ
- Cisco NX-OS リリース 9.3(5) では、IPv6 出力 ACL は、-R および -RX ラインカードを備えた Cisco Nexus 9504 および 9508 プラットフォーム スイッチで次をサポートします。
  - レイヤ 4 プロトコル
  - TCP フラグ
  - フラグメント
  - IPv4 の ACL ログ
  - IPv6 ヘッダーのフィールド

IPv6 出力 ACL には、次の制限が適用されます。

- ポートグループおよびレイヤ 4 操作はサポートされていません。範囲は `eg-racl-ipv6` の複数の ACE エントリに拡張されます。
- アドレス グループで定義されたホストはサポートされていません。
- カウンタはサポートされていません。
- 出力 IPv6 RACL は、サブインターフェイスおよび外部 TCAM ではサポートされません。
- アトミック更新はサポートされていません。
- `acl-eg-ext` が有効になっている場合、VXLAN はサポートされません。
- IPv6 アドレスを使用した IPv6 出力 ACL ログはサポートされていません。
- Cisco NX-OS リリース 9.3(5) 以降、PACL リダイレクトは Cisco Nexus 9300-GX スイッチでサポートされます。次の制限が適用されます。
  - PACL リダイレクトをサポートするには、入力タップインターフェイスで `mode tap-agg` コマンドを実行する必要があります。
  - MPLS ストリップ機能をサポートするには、`mpls strip` および `hardware acl tap-aug` コマンドを設定し、スイッチをリロードする必要があります。
  - ダブルタグ VLAN の場合、2 番目の VLAN の範囲は 2 ~ 510 です。
  - dot1q VLAN を使用した MPLS ストリップはサポートされていません。
  - リダイレクトポートがアクセスポートとして設定されている場合でも、着信パケットがタグ付けされている場合、リダイレクトポートはタグを伝送します。
  - 拒否 ACE では、TapAgg リダイレクトはサポートされていません。

- 出力 ACL は、VLAN 間ルーティングフローの 2 番目の VLAN の IP アドレスを宛先とするトラフィックをサポートしません。
- Cisco Nexus 9300-EX/FX/FX2/FX3/GXプラットフォーム スイッチおよび Cisco Nexus N9K-93180YC-FX スイッチでは、レイヤ 3 インターフェイスのマルチキャスト MAC 宛先アドレスを持つパケットで RACL を照合できません。ルーティング可能な修飾子を削除するように ACL を設定する場合は、**ignore routable** コマンドを使用します。ただし、**ignore-routable** を RACL に追加して SVI に適用すると、RACL はブリッジされたパケットともマッチします。

## 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。

Table 18: 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。
IP ACL エントリ	1024
ACL ルール	すべての ACL に暗黙のルールが適用されます。
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。

### Related Topics

[IP ACL および MAC ACL の暗黙ルール](#) (310 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。

#### Before you begin

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。

## Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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。 <ul style="list-style-type: none"> <li>• <b>ip access-list name</b></li> <li>• <b>ipv6 access-list name</b></li> </ul> <b>Example:</b> <pre>switch(config)# ip access-list acl-01 switch(config-acl)#</pre>	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。 <i>name</i> 引数は 64 文字以内で指定します。
ステップ 3	(Optional) <b>fragments {permit-all   deny-all}</b> <b>Example:</b> <pre>switch(config-acl)# fragments permit-all</pre>	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。 <b>fragments</b> コマンドが含まれている ACL がデバイスによってトラフィックに適用される場合、 <b>fragments</b> コマンドは初期状態でないフラグメント（このフラグメントは、ACL 内のどの明示的な <b>permit</b> コマンドまたは <b>deny</b> コマンドとも一致しません）のみと一致します。
ステップ 4	<b>[sequence-number] {permit   deny}</b> <b>protocol {source-ip-prefix   source-ip-mask}</b> <b>{destination-ip-prefix   destination-ip-mask}</b> <b>Example:</b> <pre>switch(config-acl)# 10 permit ipv6 1::1 2::2 3::3 4::4</pre>	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。 <i>sequence-number</i> 引数には、1 ~ 4294967295 の整数を指定します。 <b>permit</b> コマンドと <b>deny</b> 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。 IPv4 および IPv6 アクセス リストの場合、送信元と宛先の IPv4 または IPv6 プレフィックスを指定できます。これは、最初の連続するビットでのみ一致します。または、アドレスのいずれかのビットに一致する送信元と宛先の IPv4 または IPv6 ワイルドカードマスクを指定できます。IPv6 ワイルドカードマスクは、Cisco Nexus 9200、9300-EX、および 9300-FX/FX2/FXP スイッチと Cisco Nexus 9364C スイッチでサポートされます。

	Command or Action	Purpose
ステップ 5	(Optional) <b>statistics per-entry</b> <b>Example:</b> <pre>switch(config-acl)# statistics per-entry</pre>	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。  <b>Note</b> Cisco NX-OS リリース 9.2(3) 以降では、-R ラインカードを備えた Cisco Nexus 9500 スイッチのサポートが追加されています。Cisco Nexus 9500 プラットフォームスイッチを使用している場合、これは必須の手順です。
ステップ 6	<b>hardware profile acl-stats module xx</b> <b>Example:</b> <pre>switch(config-acl)# hardware profile acl-stats module 10</pre>	内部 TCAM と外部 TCAM の両方で ACL TCAM エントリのカウンタを有効にします。  <b>Note</b> このコマンドは、-R および -RX ラインカードと Cisco Nexus 3636C-R および 36180YC-R スイッチを備えた Cisco Nexus 9500 プラットフォームスイッチにのみ適用されます。カウンタを有効にすると、VLAN と SVI の統計情報は失われます。
ステップ 7	<b>reload module xx</b> <b>Example:</b> <pre>switch(config)# reload module 10</pre>	スイッチをリロードします。  <b>Note</b> Cisco Nexus 9500 プラットフォームスイッチの場合、このコマンドはオプションであり、 <b>hardware profile ac-stats</b> が適用されているモジュールのみをリロードする必要があります。
ステップ 8	<b>ignore routeable</b> <b>Example:</b> <pre>switch(config)# ignore routeable</pre>	Cisco Nexus 9300-EX および 9300-FX プラットフォームスイッチでマルチキャストトラフィックのフィルタリングを有効にします。
ステップ 9	(Optional) 次のいずれかのコマンドを入力します。 <ul style="list-style-type: none"> <li>• <b>show ip access-lists name</b></li> <li>• <b>show ipv6 access-lists name</b></li> </ul>	IP ACL の設定を表示します。

	Command or Action	Purpose
	<b>Example:</b> <pre>switch(config-acl)# show ip access-lists acl-01</pre>	
ステップ 10	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch(config-acl)# copy running-config startup-config</pre>	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。

### Before you begin

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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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。 <ul style="list-style-type: none"> <li>• <b>ip access-list name</b></li> <li>• <b>ipv6 access-list name</b></li> </ul> <b>Example:</b> <pre>switch(config)# ip access-list acl-01 switch(config-acl)#</pre>	名前指定した 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	(Optional) [ <i>sequence-number</i> ] { <b>permit</b>   <b>deny</b> } <i>protocol source destination</i>  <b>Example:</b>	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

	Command or Action	Purpose
	<pre>switch(config-acl)# 100 permit ip 192.168.2.0/24 any</pre>	<p>番号を指定しないと、ルールは ACL の末尾に追加されます。 <i>sequence-number</i> 引数には、1 ~ 4294967295 の整数を指定します。</p> <p>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。</p>
ステップ 4	<p>(Optional) [no] <b>fragments</b> {<b>permit-all</b>   <b>deny-all</b>}</p> <p><b>Example:</b></p> <pre>switch(config-acl)# fragments permit-all</pre>	<p>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。 <b>fragments</b> コマンドが含まれている ACL がデバイスによってトラフィックに適用される場合、<b>fragments</b> コマンドは初期状態でないフラグメント（このフラグメントは、ACL 内のどの明示的な <b>permit</b> コマンドまたは <b>deny</b> コマンドとも一致しません）のみと一致します。</p> <p><b>no</b> 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。</p>
ステップ 5	<p>(Optional) <b>no</b> {<i>sequence-number</i>   {<b>permit</b>   <b>deny</b>} <i>protocol source destination</i>}</p> <p><b>Example:</b></p> <pre>switch(config-acl)# no 80</pre>	<p>指定したルールを IP ACL から削除します。</p> <p>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。</p>
ステップ 6	<p>(Optional) [no] <b>statistics per-entry</b></p> <p><b>Example:</b></p> <pre>switch(config-acl)# statistics per-entry</pre>	<p>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。</p> <p><b>no</b> 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。</p>
ステップ 7	<p>(Optional) 次のいずれかのコマンドを入力します。</p> <ul style="list-style-type: none"> <li>• <b>show ip access-lists</b> <i>name</i></li> <li>• <b>show ipv6 access-lists</b> <i>name</i></li> </ul> <p><b>Example:</b></p> <pre>switch(config-acl)# show ip access-lists acl-01</pre>	<p>IP ACL の設定を表示します。</p>

	Command or Action	Purpose
ステップ 8	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch(config-acl)# copy running-config startup-config</pre>	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。

**Related Topics**

[IP ACL 内のシーケンス番号の変更 \(340 ページ\)](#)

## 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。

**Before you begin**

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。

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。

**Procedure**

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>{ip   ipv6} access-list name</b>  <b>Example:</b> <pre>switch(config)# ip access-list vtyacl</pre>	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	<b>{permit   deny}</b> プロトコル 送信元 接続先 [log] [time-range 時間]  <b>Example:</b> <pre>switch(config-ip-acl)# permit tcp any any</pre>	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	<b>exit</b>  <b>Example:</b>	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。

	Command or Action	Purpose
	<pre>switch(config-ip-acl)# exit switch(config)#</pre>	
ステップ 5	<b>line vty</b> <b>Example:</b> <pre>switch(config)# line vty switch(config-line)#</pre>	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	<b>{ip   ipv6} access-class 名前 {in   out}</b> <b>Example:</b> <pre>switch(config-line)# ip access-class vtyacl out</pre>	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。
ステップ 7	(Optional) <b>show {ip   ipv6} access-lists</b> <b>Example:</b> <pre>switch# show ip access-lists</pre>	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	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch# copy running-config startup-config</pre>	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。

### Before you begin

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、その設定に必要な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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>resequence {ip   ipv6} access-list name starting-sequence-number increment</b> <b>Example:</b>	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



	Command or Action	Purpose
	switch(config)# resequence access-list ip acl-01 100 10	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。 <i>starting-sequence-number</i> 引数と <i>increment</i> 引数は、1 ~ 4294967295 の整数で指定します。
ステップ 3	(Optional) <b>show ip access-lists name</b>  <b>Example:</b> switch(config)# show ip access-lists acl-01	IP ACL の設定を表示します。
ステップ 4	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> 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。

## IP ACL の削除

IP ACL をデバイスから削除できます。

### Before you begin

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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> 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。  <ul style="list-style-type: none"> <li>• <b>no ip access-list name</b></li> <li>• <b>no ipv6 access-list name</b></li> </ul> <b>Example:</b> switch(config)# no ip access-list acl-01	名前指定した IP ACL を実行コンフィギュレーションから削除します。

	Command or Action	Purpose
ステップ 3	(Optional) 次のいずれかのコマンドを入力します。 <ul style="list-style-type: none"> <li>• <b>show ip access-lists name summary</b></li> <li>• <b>show ipv6 access-lists name summary</b></li> </ul> <b>Example:</b> <pre>switch(config)# show ip access-lists acl-01 summary</pre>	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	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	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。

## ACL TCAM リージョン サイズの設定

ハードウェアの ACL Ternary Content Addressable Memory (TCAM) リージョンのサイズを変更できます。TCAM カービング後には、設定を保存してスイッチをリロードする必要があります。スイッチに障害のあるモジュールがある場合は、設定の保存に時間がかかります。

ここでの例は、Cisco Nexus 9200、9300、および 9500 シリーズ スイッチおよび、Cisco Nexus 3164Q、31128PQ、3232C、および 3264Q スイッチのすべてで使用できますが、TCAM テンプレートを使用して ACL TCAM リージョン サイズを設定する必要がある NFE2 対応デバイス (X9432C-S 100G ラインカードや C9508-FM-S ファブリック モジュールなど) には適用できません。TCAM テンプレートの使用方法の詳細については、「テンプレートを使用した ACL TCAM リージョン サイズの設定」を参照してください。



- (注)
- テンプレートを適用すると（「[テンプレートを使用した ACL TCAM リージョン サイズの設定 \(354 ページ\)](#)」を使用）、ここで説明した **hardware access-list tcam region** コマンドは機能しません。このコマンドを使用するには、テンプレートのコミットを解除する必要があります。
  - マルチキャスト PIM Bidir 機能の **hardware access-list tcam region** コマンドは、Broadcom ベースの Cisco Nexus 9000 シリーズ スイッチにのみ適用されます。
  - QoS TCAM カービングの設定については、『*Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide*』を参照してください。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>[no] hardware access-list tcam region region tcam-size</b> 例 : <pre>switch(config)# hardware access-list tcam region mpls 256</pre>	ACL TCAM リージョン サイズを変更します。使用可能なリージョンは次のとおりです。 <ul style="list-style-type: none"> <li>• <b>n9k-arp-acl</b> : CPUに向かう途中でインターフェイスに入るARPパケットのレート制限を設定します。arp パケットが設定されたレートに準拠するように、インターフェイスごとにこのレート制限を設定する必要があります。</li> <li>• <b>arp-ether</b> : ARP/レイヤ 2 Ethertype TCAM リージョン サイズを設定します。</li> <li>• <b>copp</b> : CoPP TCAM リージョン サイズを設定します。</li> <li>• <b>e-flow</b> : 出力フロー カウンタの TCAM リージョン サイズを設定します。</li> <li>• <b>copp</b> : CoPP TCAM リージョン サイズを設定します。</li> <li>• <b>egr-racl</b> : 出力 IPv4 または IPv6 ルータ ACL (RACL) TCAM リージョン サイズを設定します (Cisco Nexus 9200 スイッチのみ)。</li> <li>• <b>egr-sup</b> : 出力スーパーバイザ TCAM リージョン サイズを設定します (Cisco Nexus 9200 スイッチのみ)。</li> <li>• <b>e-ipv6-qos</b> : IPv6 出力 QoS TCAM リージョン サイズを設定します。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <b>e-ipv6-racl</b> : IPv6 出力ルータ ACL (ERACL) TCAM リージョン サイズを設定します。</li> <li>• <b>e-mac-qos</b> : 出力 MAC QoS TCAM リージョン サイズを設定します。</li> <li>• <b>e-qos</b> : IPv4 出力 QoS TCAM リージョン サイズを設定します。</li> <li>• <b>e-qos-lite</b> : IPv4 出力 QoS Lite TCAM リージョン サイズを設定します。</li> <li>• <b>e-racl</b> : IPv4 出力ルータ ACL (ERACL) TCAM リージョン サイズを設定します。</li> <li>• <b>fex-ifacl</b> : FEX IPv4 ポート ACL TCAM リージョン サイズを設定します。</li> <li>• <b>fex-ipv6-ifacl</b> : FEX IPv6 ポート ACL TCAM リージョン サイズを設定します。</li> <li>• <b>fex-ipv6-qos</b> : FEX IPv6 ポート QoS TCAM リージョン サイズを設定します。</li> <li>• <b>fex-mac-ifacl</b> : FEX MAC ポート ACL TCAM リージョン サイズを設定します。</li> <li>• <b>fex-mac-qos</b> : FEX MAC ポート QoS TCAM リージョン サイズを設定します。</li> <li>• <b>fex-qos</b> : FEX IPv4 ポート QoS TCAM リージョン サイズを設定します。</li> <li>• <b>fex-qos-lite</b> : FEX IPv4 ポート QoS Lite TCAM リージョン サイズを設定します。</li> <li>• <b>fhs</b> : fhs TCAM リージョンのサイズを設定します。Cisco Nexus 9300 および 9500 シリーズ スイッチの fhs</li> </ul>

	コマンドまたはアクション	目的
		<p>リージョンに TCAM を設定できません。</p> <ul style="list-style-type: none"> <li>• <b>flow</b> : 入力フロー カウンタ TCAM リージョン サイズを設定します。</li> <li>• <b>ifacl</b> : IPv4 ポート ACL TCAM リージョン サイズを設定します。</li> <li>• <b>ifacl-udf</b> : IPv4 ポート ACL ユーザ定義フィールド (UDF) TCAM リージョンのサイズを設定します (Cisco Nexus 3232C および 3264Q スイッチのみ)。</li> <li>• <b>ing-ifacl</b> : 入力 IPv4、IPv6、または MAC ポート ACL TCAM リージョンサイズを設定します (Cisco Nexus 9200、9300、9300-EX スイッチのみ)。</li> </ul> <p>(注) ユーザ定義フィールド (UDF) を <b>ing-ifacl</b> TCAM リージョンに付加して、UDF ベースの IPv4 または IPv6 ポート ACL を設定できます。UDF ベースの IPv6 ポート ACL は、Cisco Nexus 9300-EX スイッチでのみサポートされます。詳細な情報および設定の手順については、「<a href="#">UDF ベース ポート ACL の設定 (363 ページ)</a>」を参照してください。</p> <ul style="list-style-type: none"> <li>• <b>ing-l2qos</b> : 入力レイヤ 2 QoS TCAM リージョン サイズを設定します (Cisco Nexus 9200 スイッチのみ)。</li> <li>• <b>ing-l2-span-filter</b> : 入力レイヤ 2 SPAN フィルタ TCAM リージョン サイズを設定します (Cisco Nexus</li> </ul>

	コマンドまたはアクション	目的
		<p>9200 および 9300-EX スイッチのみ)。</p> <ul style="list-style-type: none"> <li>• <b>ing-l3-span-filter</b> : 入力レイヤ 3 および VLAN SPAN フィルタ TCAM リージョン サイズを設定します (Cisco Nexus 9200 および 9300-EX スイッチのみ)。</li> <li>• <b>ing-l3-vlan-qos</b> : 入力レイヤ 3、VLAN、および SVI QoS TCAM リージョン サイズを設定します (Cisco Nexus 9200 スイッチのみ)。</li> <li>• <b>ing-netflow</b> : NetFlow TCAM リージョン サイズを設定します。</li> <li>• <b>ing-racl</b> : IPv4 または IPv6 入力ルータ ACL (RACL) TCAM リージョン サイズを設定します (Cisco Nexus 9200 シリーズ スイッチのみ)。</li> <li>• <b>ing-redirect</b> : DHCPv4 リレー、DHCPv4 スヌーピング、および DHCPv4 クライアントのリダイレクト TCAM リージョン サイズを設定します (Cisco Nexus 9200 スイッチのみ)。</li> <li>• <b>ing-sup</b> : 入力スーパーバイザ TCAM リージョン サイズを設定します (Cisco Nexus 9200 シリーズ スイッチのみ)。</li> <li>• <b>ipsg</b> : IP ソース ガード SMAC-IP バインディング TCAM リージョン サイズを設定します。</li> <li>• <b>ipv6-ifacl</b> : IPv6 ポート ACL TCAM リージョン サイズを設定します。</li> <li>• <b>ipv6-l3qos</b> : IPv6 レイヤ 3 QoS TCAM リージョン サイズを設定します。</li> <li>• <b>ipv6-qos</b> : IPv6 ポート QoS TCAM リージョン サイズを設定します。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <b>ipv6-racl</b> : IPv6 RACL TCAM リージョン サイズを設定します。</li> <li>• <b>ipv6-vacl</b> : IPv6 VACL TCAM リージョン サイズを設定します。</li> <li>• <b>ipv6-vqos</b> : IPv6 VLAN QoS TCAM リージョン サイズを設定します。</li> <li>• <b>l3qos</b> : IPv4 レイヤ 3 QoS TCAM リージョン サイズを設定します。</li> <li>• <b>l3qos-lite</b> : IPv4 レイヤ 3 QoS Lite TCAM リージョン サイズを設定します。</li> <li>• <b>mac-ifacl</b> : MAC ポート ACL TCAM リージョン サイズを設定します。</li> <li>• <b>mac-l3qos</b> : MAC レイヤ 3 QoS TCAM リージョン サイズを設定します。</li> <li>• <b>mac-qos</b> : MAC ポート QoS TCAM リージョン サイズを設定します。</li> <li>• <b>mac-vacl</b> : MAC VACL TCAM リージョン サイズを設定します。</li> <li>• <b>mac-vqos</b>—Configures the size of the MAC VLAN QoS TCAM region.</li> <li>• <b>mcast_bidir</b> : マルチキャスト PIM Bidir TCAM リージョン サイズを設定します。</li> <li>• <b>mpls</b> : スタティック MPLS TCAM リージョン サイズを設定します。</li> <li>• <b>nat</b> : ネットワーク アドレス変換 (NAT) TCAM リージョン サイズを設定します。</li> <li>• <b>ns-ipv6-l3qos</b> : X9536PQ、X9564PX、X9564TX ラインカード、および M12PQ 汎用拡張モジュール (GEM) の IPv6 レイヤ 3 QoS TCAM リージョン サイズを設定します。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <b>ns-ipv6-qos</b> : X9536PQ、X9564PX、X9564TX ラインカード、および M12PQ 汎用拡張モジュール (GEM) の IPv6 ポート QoS TCAM リージョン サイズを設定します。</li> <li>• <b>ns-ipv6-vqos</b> : X9536PQ、X9564PX、X9564TX ラインカード、および M12PQ 汎用拡張モジュール (GEM) の IPv6 VLAN QoS TCAM リージョン サイズを設定します。</li> <li>• <b>ns-l3qos</b> : X9536PQ、X9564PX、X9564TX ラインカード、および M12PQ 汎用拡張モジュール (GEM) の IPv4 レイヤ 3 QoS TCAM リージョン サイズを設定します。</li> <li>• <b>ns-mac-l3qos</b> : X9536PQ、X9564PX、X9564TX ラインカード、および M12PQ 汎用拡張モジュール (GEM) の MAC レイヤ 3 QoS TCAM リージョン サイズを設定します。</li> <li>• <b>ns-mac-qos</b> : X9536PQ、X9564PX、X9564TX ラインカード、および M12PQ 汎用拡張モジュール (GEM) の MAC ポート QoS TCAM リージョン サイズを設定します。</li> <li>• <b>ns-mac-vqos</b> : X9536PQ、X9564PX、X9564TX ラインカード、および M12PQ 汎用拡張モジュール (GEM) の MAC VLAN QoS TCAM リージョン サイズを設定します。</li> <li>• <b>ns-qos</b> : X9536PQ、X9564PX、X9564TX ラインカード、および M12PQ 汎用拡張モジュール (GEM) の IPv4 ポート QoS TCAM リージョン サイズを設定します。</li> <li>• <b>ns-vqos</b> : X9536PQ、X9564PX、X9564TX ラインカード、および</li> </ul>



	コマンドまたはアクション	目的
		<p>M12PQ 汎用拡張モジュール (GEM) の IPv4 VLAN QoS TCAM リージョン サイズを設定します。</p> <ul style="list-style-type: none"> <li>• <b>openflow</b> : オープンフロー TCAM リージョン サイズを設定します。</li> <li>• <b>qos</b> : IPv4 ポート QoS TCAM リージョン サイズを設定します。</li> <li>• <b>qos-lite</b> : IPv4 ポート QoS Lite TCAM リージョン サイズを設定します。</li> <li>• <b>racl</b> : IPv4 ルータ ACL (RACL) TCAM リージョン サイズを設定します。</li> <li>• <b>racl-lite</b> : IPv4 ルータ ACL (RACL) Lite TCAM リージョン (Cisco Nexus 3232C および 3264Q スイッチ) のサイズを設定します。</li> <li>• <b>racl-udf</b> : IPv4 ルータ ACL (RACL) ユーザ定義フィールド (UDF) TCAM リージョン (Cisco Nexus 3232C および 3264Q スイッチ) のサイズを設定します。</li> <li>• <b>redirect</b> : リダイレクト TCAM リージョンのサイズを設定します。</li> <li>• <b>redirect-tunnel</b> : VXLAN を介した BFD に使用されるリダイレクトトンネル TCAM リージョンのサイズを設定します。</li> </ul> <p>(注) このコマンドは、TP_SERVICES_PKG ライセンスがインストールされている場合にのみサポートされます。</p> <ul style="list-style-type: none"> <li>• <b>rp-ipv6-qos</b> : 100G 9408PC ラインカードおよび 100G M4PC 汎用拡張モジュール (GEM) の IPv6 ポート QoS TCAM リージョン サイズを設定します。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <b>rp-mac-qos</b> : 100G 9408PC ラインカードおよび 100G M4PC 汎用拡張モジュール (GEM) の MAC ポート QoS TCAM リージョン サイズを設定します。</li> <li>• <b>rp-qos</b> : 100G 9408PC ラインカードおよび 100G M4PC 汎用拡張モジュール (GEM) の IPv4 ポート QoS TCAM リージョン サイズを設定します。</li> <li>• <b>rp-qos-lite</b> : 100G 9408PC ラインカードおよび 100G M4PC 汎用拡張モジュール (GEM) の IPv4 ポート QoS Lite TCAM リージョン サイズを設定します。</li> <li>• <b>sflow</b> : Cisco Nexus 9332PQ、9372PX、9372TX、93120TX スイッチ、および N9K-M6PQ または N9K-M12PQ 汎用拡張モジュール (GEM) 搭載の Cisco Nexus 9396PX、9396TX、93128TX スイッチの sFlow TCAM リージョン サイズを設定します。</li> <li>• <b>span</b> : SPAN TCAM リージョン サイズを設定します。</li> <li>• <b>svi</b> : 入力 SVI カウンタの TCAM リージョン サイズを設定します。</li> <li>• <b>vacl</b> : IPv4 VAACL TCAM リージョン サイズを設定します。</li> <li>• <b>vpc-convergence</b> : vPC コンバージェンス TCAM リージョン サイズを設定します。</li> <li>• <b>vqos</b> : IPv4 VLAN QoS TCAM リージョン サイズを設定します。</li> <li>• <b>vqos-lite</b> : IPv4 VLAN QoS Lite TCAM リージョン サイズを設定します。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <i>tcam-size</i> : TCAM サイズ。サイズは 256 の倍数です。サイズが 256 より大きい場合は、512 の倍数でなければなりません。FHS の場合、範囲は 0~4096 です。</li> </ul> <p>デフォルトの TCAM リージョン サイズに戻すには、このコマンドの <b>no</b> 形式を使用します。</p> <p>(注) <b>hardware access-list tcam region {racl   ifacl   vacl} qualify udf udf-names</b> コマンドを使用して IPv4 ユーザ定義フィールド (UDF) を racl、ifacl、および vacl TCAM リージョンにアタッチして、IPv4 UDF ベースの ERSPAN を設定します。</p> <p><b>hardware access-list tcam region {ing-ifacl   ing-l2-span-filter   ing-l3-span-filter} qualify v6udf v6udf-names</b> コマンドを使用して、IPv6 UDF を ing-l2-span-filter and ing-l3-span-filter TCAM にアタッチして、IPv6 UDF ベースの ERSPAN を設定します。詳細および設定手順については、最新の『Cisco Nexus 9000 Series NX-OS System Management Configuration Guide』を参照してください。</p>
ステップ 3	<b>copy running-config startup-config</b> 例 : <pre>switch(config)# copy running-config startup-config</pre>	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	(任意) <b>show hardware access-list tcam region</b> 例 : <pre>switch(config)# show hardware access-list tcam region</pre>	デバイスで次のリロード時に適用される TCAM サイズを表示します。

	コマンドまたはアクション	目的
ステップ 5	<b>reload</b>  例 : <pre>switch(config)# reload</pre>	デバイスがリロードされます。  (注) 新しいサイズの値は、 <b>copy running-config startup-config + reload</b> を入力するか、すべてのラインカードモジュールをリロードした後にのみ有効になります。

### 例

次に、Cisco Nexus NFE 対応スイッチで RACL TCAM リージョンのサイズを変更する例を示します。

```
switch(config)#hardware access-list tcam region n9k-arp-acl 256switch(config)#copy r s
switch(config)# reload
Configuring storm-control-cpu:
switch (config)# interface ethernet 1/10switch
switch (config-if)# storm-control-cpu arp rate 150
switch (config)# show access-list storm-control-cpu arp-stats interface ethernet 1/10

slot 1
```

次に、Cisco Nexus 9500 シリーズ スイッチで RACL TCAM リージョンのサイズを変更する例を示します。

```
switch(config)# hardware access-list tcam region racl 256
[SUCCESS] New tcam size will be applicable only at boot time.
You need to 'copy run start' and 'reload'
switch(config)# copy running-config startup-config
switch(config)# reload
WARNING: This command will reboot the system
Do you want to continue? (y/n) [n] y
```

次に、変更を確認するために、TCAM リージョンのサイズを表示する例を示します。

```
switch(config)# show hardware access-list tcam region
TCAM Region Sizes:

          IPV4 PACL [ifacl] size = 512
          IPV6 PACL [ipv6-ifacl] size = 0
          MAC PACL [mac-ifacl] size = 0
          IPV4 Port QoS [qos] size = 256
          IPV6 Port QoS [ipv6-qos] size = 0
          MAC Port QoS [mac-qos] size = 0
          FEX IPV4 PACL [fex-ifacl] size = 0
          FEX IPV6 PACL [fex-ipv6-ifacl] size = 0
          FEX MAC PACL [fex-mac-ifacl] size = 0
          FEX IPV4 Port QoS [fex-qos] size = 0
          FEX IPV6 Port QoS [fex-ipv6-qos] size = 0
          FEX MAC Port QoS [fex-mac-qos] size = 0
          IPV4 VACL [vacl] size = 512
          IPV6 VACL [ipv6-vacl] size = 0
          MAC VACL [mac-vacl] size = 0
          IPV4 VLAN QoS [vqos] size = 0
```

```

IPV6 VLAN QoS [ipv6-vqos] size = 0
MAC VLAN QoS [mac-vqos] size = 0
IPV4 RACL [racl] size = 512
IPV6 RACL [ipv6-racl] size = 0
IPV4 Port QoS Lite [qos-lite] size = 0
FEX IPV4 Port QoS Lite [fex-qos-lite] size = 0
IPV4 VLAN QoS Lite [vqos-lite] size = 0
IPV4 L3 QoS Lite [l3qos-lite] size = 0
Egress IPv4 QoS [e-qos] size = 0
Egress IPv6 QoS [e-ipv6-qos] size = 0
Egress MAC QoS [e-mac-qos] size = 0
Egress IPv4 VACL [vacl] size = 512
Egress IPv6 VACL [ipv6-vacl] size = 0
Egress MAC VACL [mac-vacl] size = 0
Egress IPv4 RACL [e-racl] size = 256
Egress IPv6 RACL [e-ipv6-racl] size = 0
Egress IPv4 QoS Lite [e-qos-lite] size = 0
IPV4 L3 QoS [l3qos] size = 0
IPV6 L3 QoS [ipv6-l3qos] size = 0
MAC L3 QoS [mac-l3qos] size = 0
Ingress System size = 256
Egress System size = 256
SPAN [span] size = 256
Ingress COPP [copp] size = 256
Ingress Flow Counters [flow] size = 0
Egress Flow Counters [e-flow] size = 0
Ingress SVI Counters [svi] size = 0
Redirect [redirect] size = 512
NS IPv4 Port QoS [ns-qos] size = 256
NS IPv6 Port QoS [ns-ipv6-qos] size = 0
NS MAC Port QoS [ns-mac-qos] size = 0
NS IPv4 VLAN QoS [ns-vqos] size = 256
NS IPv6 VLAN QoS [ns-ipv6-vqos] size = 0
NS MAC VLAN QoS [ns-mac-vqos] size = 0
NS IPv4 L3 QoS [ns-l3qos] size = 256
NS IPv6 L3 QoS [ns-ipv6-l3qos] size = 0
NS MAC L3 QoS [ns-mac-l3qos] size = 0
VPC Convergence [vpc-convergence] size = 256
IPSG SMAC-IP bind table [ipsg] size = 0
Ingress ARP-Ether ACL [arp-ether] size = 0
ranger+ IPv4 QoS Lite [rp-qos-lite] size = 0
ranger+ IPv4 QoS [rp-qos] size = 256
ranger+ IPv6 QoS [rp-ipv6-qos] size = 256
ranger+ MAC QoS [rp-mac-qos] size = 256
NAT ACL[nat] size = 0
Mpls ACL size = 0
Ingress IPv4 N3K QoS size = 0
Ingress IPv6 N3K QoS size = 0
MOD RSVD size = 0
sFlow ACL [sflow] size = 0
mcast bidir ACL size = 0
Openflow size = 0

```

次に、デフォルトの RACL TCAM リージョン サイズに戻す例を示します。

```

switch(config)# no hardware profile tcam region racl 512
[SUCCESS] New tcam size will be applicable only at boot time.
You need to 'copy run start' and 'reload'
switch(config)# copy running-config startup-config
switch(config)# reload
WARNING: This command will reboot the system
Do you want to continue? (y/n) [n] y

```

## テンプレートを使用した ACL TCAM リージョンサイズの設定

カスタムテンプレートを使用、作成、および適用することで、ACL TCAM リージョンサイズを設定できます。

Cisco Nexus 9200、9300、および9500シリーズスイッチおよび、Cisco Nexus 3164Q、31128PQ、3232C、および3264Qスイッチについては、いずれもこの手順または「[ACL TCAM リージョンサイズの設定](#)」の手順を使用してACL TCAM リージョンサイズを設定できます。ただし、NFE2 対応デバイス（X9432C-S 100G ラインカードやC9508-FM-S ファブリック モジュールなど）では **hardware access-list tcam region** コマンドがサポートされていないので、テンプレートを使用してACL TCAM リージョンサイズを設定する必要があります。



- (注)
- TCAM テンプレートを適用すると、**hardware access-list tcam region** コマンドは機能しません。このコマンドを使用するには、テンプレートのコミットを解除する必要があります。
  - QoS TCAM カービングの設定については、『*Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide*』を参照してください。
  - TCAM プロファイルテンプレートは、C9508-FM-S ファブリック モジュールではサポートされません。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>[no] hardware profile tcam resource template <i>template-name</i> ref-template {nfe   nfe2   {12-13   13}}</b> 例 : <pre>switch(config)# hardware profile tcam resource template SR_MPLS_CARVE ref-template nfe2 switch(config-tcam-temp)#</pre>	ACL TCAM リージョンのサイズを設定するためのテンプレートを作成します。 <b>nfe</b> : ネットワークフォワーディングエンジン (NFE) 対応の Cisco Nexus 9300 および 9500 シリーズ、3164Q、および 31128PQ デバイスでのデフォルト TCAM テンプレート。 <b>nfe2</b> : NFE2 対応の Cisco Nexus 9500 シリーズ、3232C、および 3264Q デバイスのデフォルト TCAM テンプレート。 <b>12-13</b> : Cisco Nexus 9200 シリーズスイッチでのレイヤ 2 およびレイヤ 3 設定のデフォルト TCAM テンプレート。

	コマンドまたはアクション	目的
		<b>I3</b> : Cisco Nexus 9200 シリーズ スイッチでのレイヤ 3 設定のデフォルト TCAM テンプレート。レイヤ 3 TCAM テンプレートは、Cisco Nexus 9200 シリーズ スイッチのデフォルトテンプレートです。
ステップ 3	(任意) <code>region tcam-size</code> 例 : <code>switch(config-tcam-temp)# mpls 256</code>	所要の TCAM リージョンおよびそのサイズをテンプレートに追加します。テンプレートに追加する各リージョンで、このコマンドを入力します。使用可能なリージョンの一覧については、「 <a href="#">ACL TCAM リージョン サイズの設定</a> 」を参照してください。
ステップ 4	<b>exit</b> 例 : <code>switch(config-tcam-temp)# exit</code> <code>switch(config#)</code>	TCAM テンプレート 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	<b>[no] hardware profile tcam resource service-template template-name</b> 例 : <code>switch(config)# hardware profile tcam resource service-template SR_MPLS_CARVE</code>	カスタムテンプレートを、すべてのラインカードおよびファブリック モジュールに適用します。
ステップ 6	(任意) <b>show hardware access-list tcam template {all   nfe   nfe2   I2-I3   I3   template-name}</b> 例 : <code>switch(config)# show hardware access-list tcam template SR_MPLS_CARVE</code>	すべての TCAM テンプレートまたは特定のテンプレートの設定を表示します。
ステップ 7	(任意) <b>copy running-config startup-config</b> 例 : <code>switch(config)# copy running-config startup-config</code>	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 8	<b>reload</b> 例 : <code>switch(config)# reload</code>	デバイスがリロードされます。  (注) 設定は、 <b>copy running-config startup-config + reload</b> を入力した後にのみ有効になります。

## TCAM カービングの設定

デフォルト TCAM リージョン設定はプラットフォームごとに異なり、すべての TCAM リージョンには対応しません。所要のリージョンをイネーブルにするには、1 つのリージョンの TCAM サイズを減らしてから、所要のリージョンの TCAM サイズを増やす必要があります。



(注) QoS TCAM カービングの設定については、『*Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide*』を参照してください。

次の表に、各種プラットフォームでの入出力 TCAM リージョンのデフォルト サイズを示します。

表 19: デフォルト TCAM リージョン設定 (入力) : Cisco Nexus 9500 シリーズ スイッチ用

リージョン名	サイズ	幅	合計サイズ
IPv4 RACL	1536	1	1536
IPv4 レイヤ 3 QoS	256	2	512
SPAN	256	1	256
CoPP	256	2	512
システム	256	2	512
リダイレクト	256	1	256
vPC コンバージェンス	512	1	512
			4 K

表 20: デフォルト TCAM リージョン設定 (出力) : Cisco Nexus 9500 シリーズ スイッチ用

リージョン名	サイズ	幅	合計サイズ
IPv4 RACL	768	1	768
システム	256	1	256
			1 K

表 21: デフォルトの TCAM サイズ : Cisco Nexus 9504 および 9508 プラットフォーム スイッチ

地域	サイズ
MAC PACL [mac-ifacl]	1952
IPV6 ポート QoS [ipv6-qos]	256
PV6 L3 QoS [ipv6-l3qos]	256
SPAN [span]	96



地域	サイズ
Ingress CoPP [copp]	128
リダイレクト IPv4	2048
リダイレクト IPv6	2048

表 22: デフォルト TCAM リージョン設定 (入力) : Cisco Nexus 9300-FX シリーズ スイッチ用

リージョン名	サイズ	幅	合計サイズ
IPv4 RAACL	2304	1	2304
レイヤ 2 QoS	256	1	256
レイヤ 3/VLAN QoS	512	1	512
システム	512	1	512
レイヤ 2 SPAN フィルタ	256	1	256
レイヤ 3 SPAN フィルタ	256	1	256
SPAN	512	1	512
NetFlow/Analytics フィルタ	512	1	512
			5K

表 23: デフォルト TCAM リージョン設定 (出力) : Cisco Nexus 9300-FX シリーズ スイッチ用

リージョン名	サイズ	幅	合計サイズ
IPv4 RAACL	1792	1	1792
システム	256	1	256
			2 K

表 24: デフォルト TCAM リージョン設定 (入力) : Cisco Nexus 9300-EX シリーズ スイッチ用

リージョン名	サイズ	幅	合計サイズ
IPv4 RAACL	1792	1	1792
レイヤ 2 QoS	256	1	256
レイヤ 3/VLAN QoS	512	1	512
システム	512	1	512
レイヤ 2 SPAN ACL	256	1	256

リージョン名	サイズ	幅	合計サイズ
レイヤ 3/VLAN SPAN ACL	256	1	256
SPAN	512	1	512
			4 K

表 25: デフォルト TCAM リージョン設定 (出力) : Cisco Nexus 9300-EX シリーズ スイッチ用

リージョン名	サイズ	幅	合計サイズ
IPv4 RACL	1792	1	1792
システム	256	1	256
			2 K

表 26: デフォルト TCAM リージョン設定 (入力) : Cisco Nexus 9300 シリーズ スイッチ用

リージョン名	サイズ	幅	合計サイズ
IPv4 ポート ACL	512	1	512
IPv4 ポート QoS	256	2	512
IPv4 VACL	512	1	512
IPv4 RACL	512	1	512
SPAN	256	1	256
CoPP	256	2	512
ACI リーフ ライン カード用 IPv4 ポート QoS	256	1	256
ACI リーフ ライン カード用 IPv4 VLAN QoS	256	1	256
ACI リーフ ライン カード用 IPv4 レイヤ 3 QoS	256	1	256
システム	256	2	512
リダイレクト	512	1	512
vPC コンバージェンス	256	1	256
			4 K

表 27: デフォルト TCAM リージョン設定 (出力) : Cisco Nexus 9300 シリーズ スイッチ用

リージョン名	サイズ	幅	合計サイズ
IPv4 VACL	512	1	512
IPv4 RACL	256	1	256
システム	256	1	256
			1 K

表 28: デフォルト TCAM リージョン設定 (入力) : Cisco Nexus 9200 シリーズ スイッチでのレイヤ 2 からレイヤ 3 設定用

リージョン名	サイズ	幅	合計サイズ
入力 NAT	0	1	0
入力ポート ACL	256	1	256
入力 VACL	256	1	256
入力 RACL	1536	1	1536
入力レイヤ 2 QoS	256	1	256
入力レイヤ 3 VLAN QoS	256	1	256
入力スーパーバイザ	512	1	512
入力レイヤ 2 ACL SPAN	256	1	256
入力レイヤ 3 ACL SPAN	256	1	256
ポートベース SPAN	512	1	512
			4096

表 29: デフォルト TCAM リージョン設定 (出力) : Cisco Nexus 9200 シリーズ スイッチでのレイヤ 2 からレイヤ 3 設定用

リージョン名	サイズ	幅	合計サイズ
出力 VACL	256	1	256
出力 RACL	1536	1	1536
出力スーパーバイザ	256	1	256
			2048

表 30: デフォルト TCAM リージョン設定 (入力) : Cisco Nexus 9200 シリーズ スイッチでのレイヤ 3 設定用

リージョン名	サイズ	幅	合計サイズ
入力 NAT	0	1	0
入力ポート ACL	0	1	0
入力 VACL	0	1	0
入力 RAACL	1792	1	1792
入力レイヤ 2 QoS	256	1	256
入力レイヤ 3 VLAN QoS	512	1	512
入力スーパーバイザ	512	1	512
入力レイヤ 2 ACL SPAN	256	1	256
入力レイヤ 3 ACL SPAN	256	1	256
ポートベース SPAN	512	1	512
			4096

表 31: デフォルト TCAM リージョン設定 (出力) : Cisco Nexus 9200 シリーズ スイッチでのレイヤ 3 設定用

リージョン名	サイズ	幅	合計サイズ
出力 VACL	0	1	0
出力 RAACL	1792	1	1792
出力スーパーバイザ	256	1	256
			2048

次の例では、Cisco Nexus 9500 シリーズ スイッチでの IPv6 RAACL TCAM サイズを 256 に設定します。サイズが 256 の IPv6 RAACL は、IPv6 がダブル幅であるため、512 エントリを使用します。



- (注) 異なるリージョン用に TCAM の設定を変更したり、異なるデバイス用に TCAM の設定を変更するには、同様の手順に従ってください。

Cisco Nexus 9500 シリーズ スイッチで入力 IPv6 RAACL TCAM リージョンのサイズを設定するには、2 つのオプションのいずれか 1 つを実行します。

#### オプション #1

入力 IPv4 RACL を 1024 エントリ減らし (1536 - 1024 = 512)、入力 IPv6 RACL を 512 エントリ増やします。このオプションが優先されます。

```
switch(config)# hardware access-list tcam region racl 512
Warning: Please reload the linecard for the configuration to take effect
switch(config)# hardware access-list tcam region ipv6-racl 256
Warning: Please reload the linecard for the configuration to take effect
```

表 32: IPv4 RACL (入力) を減らした後の更新された TCAM リージョン設定

リージョン名	サイズ	幅	合計サイズ
IPv4 RACL	1024	1	1024
IPv6 RACL	256	2	256 個のエントリ スライスが使用できないため、1024 個の <sup>2</sup>
IPv4 レイヤ 3 QoS	256	2	512
SPAN	256	1	256
CoPP	256	2	512
システム	256	2	512
リダイレクト	256	1	256
vPC コンバージェンス	512	1	512
			4 K

<sup>2</sup> 2 x 512 エントリ スライスが割り当てられます。

## オプション #2

IPv4 レイヤ 3 QoS のサイズを 0 に減らして削除し、入力 IPv6 RACL を追加します。このオプションは、IPv4 レイヤ 3 QoS を使用していない場合に使用できます。

```
switch(config)# hardware access-list tcam region l3qos 0
Warning: Please reload the linecard for the configuration to take effect
switch(config)# hardware access-list tcam region ipv6-racl 256
Warning: Please reload the linecard for the configuration to take effect
```

表 33: レイヤ 3 QoS (入力) を削除した後の更新された TCAM リージョン設定

リージョン名	サイズ	幅	合計サイズ
IPv4 RACL	1536	1	1536
IPv6 RACL	256	2	512
IPv4 レイヤ 3 QoS	0	2	0
SPAN	256	1	256
CoPP	256	2	512
システム	256	2	512

リージョン名	サイズ	幅	合計サイズ
リダイレクト	256	1	256
vPC コンバージェンス	512	1	512
			4 K

サイズ 256 の出力 IPv6 RACL をイネーブルにするには、出力 IPv4 RACL を 256 に減らし、出力 IPv6 RACL を追加します。

```
switch(config)# hardware access-list tcam region e-racl 256
Warning: Please reload the linecard for the configuration to take effect
switch(config)# hardware access-list tcam region e-ipv6-racl 256
Warning: Please reload the linecard for the configuration to take effect
```

表 34: IPv4 RACL (出力) を減らした後のデフォルト TCAM リージョン設定

リージョン名	サイズ	幅	合計サイズ
IPv4 RACL	256	1	256
IPv6 RACL	256	2	512
システム	256	1	256
			1 K

TCAM リージョンのサイズを調整した後、**show hardware access-list tcam region** コマンドを入力して、デバイスの次回リロード時に適用可能な TCAM サイズを表示します。



**注目** すべてのモジュールの同期を維持するには、すべてのラインカードモジュールをリロードするか、**copy running-config startup-config + reload** を入力してデバイスをリロードする必要があります。TCAM リージョン設定が複数であっても、リロードする必要があるのは1回だけです。TCAM リージョン設定がすべて完了するのを待ってから、デバイスをリロードできます。

設定によっては、TCAM サイズが超過したり、スライスが不足する場合があります。

TCAM リージョンの設定時に、すべての TCAM リージョンの 4K 入力制限を超えると、次のメッセージが表示されます。

```
ERROR: Aggregate TCAM region configuration exceeded the available Ingress TCAM space.
Please re-configure.
```

スライス数が超えると、次のメッセージが表示されます。

```
ERROR: Aggregate TCAM region configuration exceeded the available Ingress TCAM slices.
Please re-configure.
```

TCAM リージョンの設定時に、すべての TCAM リージョンの 1K 出力制限を超えると、次のメッセージが表示されます。

```
ERROR: Aggregate TCAM region configuration exceeded the available Egress TCAM space.
Please re-configure.
```

特定の機能の TCAM が設定されていない状態で TCAM カービングを必要とする機能を適用しようとする、次のメッセージが表示されます。

```
ERROR: Module x returned status: TCAM region is not configured. Please configure TCAM region and retry the command.
```



(注) 256 というデフォルトのリダイレクト TCAM リージョンサイズは、多数の BFD または DHCP リレーセッションを実行している場合は十分でない可能性があります。より多くの BFD または DHCP リレーセッションに対応するために、TCAM サイズを 512 に増やす必要がある場合があります。

#### 関連トピック

[ACL TCAM リージョンサイズの設定 \(342 ページ\)](#)

## UDF ベース ポート ACL の設定

UDF ベースのポート ACL は、Cisco Nexus 9200、9300、および 9300-EX シリーズスイッチに対して設定できます。この機能により、デバイスはユーザ定義フィールド (UDF) でのマッチングを行い、マッチしたパケットを IPv4 ポート ACL に適用できます。

UDF ベースのポート IPv6 ACL は、Cisco Nexus 9300-EX スイッチに対して設定できます。この機能により、デバイスは新しい UDF でマッチングを行い、マッチしたパケットを IPv6 ポート ACL に適用できます。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>udf udf-name offset-base offset length</b> 例 : <pre>switch(config)# udf pktoff10 packet-start 10 2</pre> 例 : <pre>switch(config)# udf pktoff10 header outer 13 20 2</pre>	次のように UDF を定義します。 <ul style="list-style-type: none"> <li>• <b>udf-name</b> : UDF の名前を指定します。名前には最大 16 文字の英数字を入力できます。</li> <li>• <b>offset-base</b> : UDF オフセットベースを以下のように指定します。ここで <b>header</b> は、オフセットを考慮したパケットヘッダーです。 <b>{packet-start   header {outer   inner {13   14}}}</b>.</li> <li>• <b>offset</b> : オフセットベースからオフセットさせるバイト数を指定しま</li> </ul>

	コマンドまたはアクション	目的
		<p>す。オフセットベース（レイヤ3/レイヤ4ヘッダー）からの先頭バイトに一致させるには、オフセットを0に設定します。</p> <ul style="list-style-type: none"> <li>• <i>length</i> : オフセットからのバイト数を指定します。1バイトまたは2バイトだけがサポートされます。追加のバイト数に一致させるには、複数のUDFの定義が必要です。</li> </ul> <p>複数のUDFを定義できますが、必要なUDFのみを定義することを推奨します。</p>
ステップ 3	<p><b>hardware access-list tcam region ing-ifac1 qualify {udf udf-name   v6udf v6udf-name}</b></p> <p>例 :</p> <pre>switch(config)# hardware access-list tcam region ing-ifac1 qualify udf pktoff10</pre>	<p>IPv4 または IPv6 ポート ACL に適用する ing-ifac1 TCAM リージョンに UDF をアタッチします。</p> <p>TCAM リージョンに接続できる UDF の数は、プラットフォームによって異なります。Cisco Nexus 9200 スイッチの場合は最大2つのUDF、Cisco Nexus 9300 スイッチの場合は最大8つのUDF、Cisco Nexus 9300-EX スイッチの場合はIPv4ポートACLに対して最大18のUDF、またはIPv6ポートACLに対して7つのUDFを接続できます。</p> <p>(注) UDF 修飾子が追加されると、TCAM リージョンはシングル幅からダブル幅になります。十分な空き領域があることを確認してください。そうでない場合、このコマンドは拒否されます。必要であれば、未使用リージョンでのTCAMスペースを削減してから、このコマンドを再入力することもできます。詳細については、「<a href="#">ACL TCAM リージョン サイズの設定</a>」を参照してください。</p>



	コマンドまたはアクション	目的
		(注) このコマンドの <b>no</b> 形式を使用すると、UDF の TCAM リージョンへの付加は解除され、リージョンはシングル幅に戻ります。
ステップ 4	必須: <b>copy running-config startup-config</b> 例 : <pre>switch(config)# copy running-config startup-config</pre>	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。
ステップ 5	必須: <b>reload</b> 例 : <pre>switch(config)# reload</pre>	デバイスがリロードされます。 (注) UDF 設定は、 <b>copy running-config startup-config + reload</b> を入力した後のみ有効になります。
ステップ 6	<b>ip access-list udf-acl</b> 例 : <pre>switch(config)# ip access-list udfacl switch(config-acl)#</pre>	IPv4 アクセス コントロール リスト (ACL) を作成し、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。
ステップ 7	次のいずれかのコマンドを入力します。 <ul style="list-style-type: none"> <li>• <b>permit udf udf-name value mask</b></li> <li>• <b>permit ip source destination udf udf-name value mask</b></li> </ul> 例 : <pre>switch(config-acl)# permit udf pkttoff10 0x1234 0xffff</pre> 例 : <pre>switch(config-acl)# permit ip any any udf pkttoff10 0x1234 0xffff</pre>	ACL を UDF でのみ一致させるか (例 1)、あるいは外部パケットフィールドについて現在のアクセス コントロール エントリ (ACE) と併せて UDF で一致させるように設定します (例 2)。値とマスクの引数の範囲は 0x0 ~ 0xFFFF です。 1 つの ACL には、UDF の有無にかかわらず、同時に複数の ACE を持たせることができます。各 ACE ごとに異なる UDF フィールドで一致させることもできれば、すべての ACE で同じリストの UDF で一致させることもできます。
ステップ 8	(任意) <b>copy running-config startup-config</b> 例 : <pre>switch(config)# copy running-config startup-config</pre>	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
- VLAN インターフェイス
- 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。



**Note** 出力ルータ ACL は、サブインターフェイスおよび Cisco Nexus 9300 シリーズ スイッチのアップリンク ポートではサポートされていません。

### Before you begin

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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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。 <ul style="list-style-type: none"> <li>• <b>interface ethernet</b> <i>slot/port</i> [ . <i>number</i> ]</li> <li>• <b>interface port-channel</b> <i>channel-number</i></li> <li>• <b>interface vlan</b> <i>vlan-id</i></li> <li>• <b>interface mgmt</b> <i>port</i></li> </ul> <b>Example:</b> <pre>switch(config)# interface ethernet 2/3 switch(config-if)#</pre>	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。 <ul style="list-style-type: none"> <li>• <b>ip access-group</b> <i>access-list</i> { <b>in</b>   <b>out</b> }</li> <li>• <b>ipv6 traffic-filter</b> <i>access-list</i> { <b>in</b>   <b>out</b> }</li> </ul> <b>Example:</b> <pre>switch(config-if)# ip access-group acl1 in</pre>	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。

	Command or Action	Purpose
ステップ 4	(Optional) <b>show running-config aclmgr</b>  <b>Example:</b> switch(config-if)# show running-config aclmgr	ACL の設定を表示します。
ステップ 5	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> switch(config-if)# 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。

**Related Topics**[IP ACL の作成](#) (334 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ンネル）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。

**Note**

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。

**Before you begin**

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。

**Procedure**

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> 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。  <ul style="list-style-type: none"> <li>• <b>interface ethernet slot/port</b></li> <li>• <b>interface port-channel channel-number</b></li> </ul> <b>Example:</b>	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。

	Command or Action	Purpose
	switch(config)# interface ethernet 2/3 switch(config-if)#	
ステップ 3	次のいずれかのコマンドを入力します。  <ul style="list-style-type: none"> <li>• <b>ip port access-group access-list in</b></li> <li>• <b>ipv6 port traffic-filter access-list in</b></li> </ul> <b>Example:</b> switch(config-if)# ip port access-group acl-12-marketing-group 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、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	(Optional) <b>show running-config aclmgr</b>  <b>Example:</b> switch(config-if)# show running-config aclmgr	ACL の設定を表示します。
ステップ 5	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> switch(config-if)# 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。

**Related Topics**[IP ACL の作成](#) (334 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](#) (406 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。

**Related Topics**[VACL の設定](#) (414 ページ)

## IPv4 ACL ロギングの設定

IPv4 ACL ロギングプロセスを設定するには、まずアクセスリストを作成し、指定された ACL を使用してインターフェイスで IPv4 トラフィックのフィルタリングをイネーブルにし、最後に ACL ロギングプロセスパラメータを設定します。

**手順**

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  例 :	グローバル 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
	switch# configure terminal switch(config)#	
ステップ 2	<b>ip access-list name</b>  例 : switch(config)# ip access-list logging-test switch(config-acl)#	IPv4 ACL を作成し、IP ACL コンフィギュレーションモードを開始します。 <i>name</i> 引数は 64 文字以内で指定します。
ステップ 3	<b>{permit   deny} ip source-address destination-address log</b>  例 : switch(config-acl)# permit ip any 10.30.30.0/24 log	条件に一致する IPv4 トラフィックを許可または拒否する、ACL のルールを作成します。ルールに一致する各パケットについての情報ロギングメッセージの生成をイネーブルにするには、 <b>log</b> キーワードを含める必要があります。  <i>source-address</i> および <i>destination-address</i> 引数には、IP アドレスとネットワークワイルドカード、IP アドレスと可変長サブネットマスク、ホストアドレス、または任意のアドレスを指定する <b>any</b> などがあります。
ステップ 4	<b>exit</b>  例 : switch(config-acl)# exit switch(config)#	設定を更新し、IP ACL 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	<b>interface ethernet slot/port</b>  例 : switch(config)# 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。
ステップ 6	<b>ip access-group name in</b>  例 : switch(config-if)# ip access-group logging-test in	指定された ACL を使用して、インターフェイス上で IPv4 トラフィックのフィルタリングをイネーブルにします。着信トラフィックに ACL を適用できます。
ステップ 7	<b>exit</b>  例 : switch(config-if)# exit switch(config)#	設定を更新して、インターフェイスコンフィギュレーションモードを終了します。

	コマンドまたはアクション	目的
ステップ 8	<b>logging ip access-list cache interval</b> <i>interval</i> 例 : <pre>switch(config)# logging ip access-list cache interval 490</pre>	ACL ロギングプロセスのログ更新間隔を秒数で設定します。デフォルト値は 300 秒です。指定できる範囲は 5 ~ 86400 秒です。
ステップ 9	<b>logging ip access-list cache entries</b> <i>number-of-flows</i> 例 : <pre>switch(config)# logging ip access-list cache entries 8001</pre>	ACL ロギングプロセスによってモニタリングするフローの最大数を指定します。デフォルト値は 8000 です。指定できる値の範囲は、0 ~ 1048576 です。
ステップ 10	<b>logging ip access-list cache threshold</b> <i>threshold</i> 例 : <pre>switch(config)# logging ip access-list cache threshold 490</pre>	アラート間隔の期限が満了する前に規定の packets 数がログ記録されると、システムは <b>syslog</b> メッセージを生成します。
ステップ 11	<b>logging ip access-list detailed</b> 例 : <pre>switch(config)# logging ip access-list detailed</pre>	<b>show logging ip access-list cache</b> コマンドの出力で、アクセスコントロールエントリ (ACE) のシーケンス番号、ACE のアクション、ACL の名前、ACL の方向、ACL のフィルタタイプ、および ACL の適用インターフェイスの情報表示をイネーブルにします。
ステップ 12	<b>hardware rate-limiter access-list-log</b> <i>packets</i> 例 : <pre>switch(config)# hardware rate-limiter access-list-log 200</pre>	ACL 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 <b>pps</b> で設定します。範囲は 0 ~ 30000 です。
ステップ 13	<b>aclog match-log-level</b> <i>severity-level</i> 例 : <pre>switch(config)# aclog match-log-level 5</pre>	ACL 一致をログ記録する最小の重大度を指定します。デフォルト値は 6 (情報) です。0 (緊急) ~ 7 (デバッグ) までの範囲があります。
ステップ 14	(任意) <b>show logging ip access-list cache [detail]</b> 例 : <pre>switch(config)# show logging ip access-list cache</pre>	送信元 IP と宛先 IP アドレス、送信元ポートと宛先ポートの情報、送信元インターフェイスなどの、アクティブログフロー情報を表示します。 <b>logging ip access-list detailed</b> コマンドを入力すると、出力には、アクセスコントロールエントリ (ACE) のシーケンス番号、ACE のアクション、ACL の名前、ACL の方向、ACL のフィルタタイプ、およ

	コマンドまたはアクション	目的
		IPv4 ACL の適用インターフェイスの情報も含まれます。

## 要求をリダイレクトするための HTTP メソッドによる ACL の設定

特定の HTTP メソッドを代行受信し、特定のポートに接続されたサーバにリダイレクトするよう ACL を設定できます。

次の HTTP メソッドをリダイレクトできます。

- connect
- delete
- get
- head
- post
- put
- trace

### 始める前に

コマンドの **hardware access-list team region ifacl 512 double-wide** を使用して、IFACL リージョンに関してダブル幅の TCAM をイネーブルにします。このコマンドは、グローバル コンフィギュレーションに適用されます。この設定を有効にするには、スイッチをリロードします。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>ip access-list name</b> 例： <pre>switch(config)# ip access-list acl-01 switch(config-acl)#</pre>	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。 <i>name</i> 引数は 64 文字以内で指定します。
ステップ 3	<b>[sequence-number] permit protocol source destination http-method method [tcp-option-length length] [redirect interface]</b> 例：	特定の HTTP メソッドをサーバにリダイレクトするように ACL を設定します。 次の HTTP メソッドがサポートされています。

	コマンドまたはアクション	目的
	<pre>switch(config-acl)# permit tcp 1.1.1.1/32 any http-method get</pre>	<ul style="list-style-type: none"> <li>• <b>connect</b> : HTTP パケットを CONNECT メソッドで照合 [0x434f4e4e]</li> <li>• <b>delete</b> : HTTP パケットを DELETE メソッドで照合 [0x44454c45]</li> <li>• <b>get</b> : HTTP パケットを GET メソッドで照合 [0x47455420]</li> <li>• <b>head</b> : HTTP パケットを HEAD メソッドで照合 [0x48454144]</li> <li>• <b>post</b> : HTTP パケットを POST メソッドで照合 [0x504f5354]</li> <li>• <b>put</b> : HTTP パケットを PUT メソッドで照合 [0x50555420]</li> <li>• <b>trace</b> : HTTP パケットを TRACE メソッドで照合 [0x54524143]</li> </ul> <p><b>tcp-option-length</b> オプションは、パケット中の TCP オプションヘッダーの長さを指定します。アクセスコントロールエントリ (ACE) 中には、最大 4 つの TCP オプション長を設定できます (4 バイトの倍数)。length の範囲は 0 ~ 40 です。このオプションを設定しないと、長さは 0 に指定され、TCP ヘッダー オプションのないパケットのみが ACE で照合可能になります。このオプションにより HTTP メソッドは、可変長 TCP オプションヘッダーを持つパケットであっても照合可能になります。</p> <p><b>redirect</b> オプションは、HTTP メソッドを特定のポートに接続されたサーバにリダイレクトさせます。HTTP リダイレクト機能は、レイヤ 3 ポートでは動作しません。</p>
ステップ 4	<p>(任意) <b>show ip access-lists name</b></p> <p>例 :</p> <pre>switch(config-acl)# show ip access-lists acl-01</pre>	IP ACL 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	(任意) <b>show run interface interface slot/port</b> 例 : <pre>switch(config-acl)# show run interface ethernet 2/2</pre>	インターフェイスの設定を表示します。

### 例

次の例は、パケット中の TCP ヘッダー オプションの長さを指定し、ポート チャネル 4001 に接続されたサーバにポスト HTTP メソッドをリダイレクトさせます。

```
switch(config)# ip access-list http-redirect-acl
switch(config-acl)# 10 permit tcp any any http-method get tcp-option-length 4 redirect port-channel4001
switch(config-acl)# 20 permit tcp any any http-method post redirect port-channel4001
switch(config-acl)# statistics per-entry
switch(config)# interface Ethernet 1/33
switch(config-if)# ip port access-group http-redirect-acl in
```

## IPv6 拡張ヘッダーの ACL の設定

この手順は、次のデバイスにのみ適用されます。

- Cisco Nexus 9504 および 9508 モジュラ シャーシ (N9K-X9636C-R、N9K-X9636Q-R、N9K-X9636C-RX、および N9K-X96136YC-R)
- Cisco Nexus 3600 プラットフォーム スイッチ (N3K-C36180YC-R および N3K-C3636C-R)

Cisco NX-OS リリース 9.3(7) 以降では、ここにリストされているデバイスで IPv6 ACL を設定する場合、拡張ヘッダーを含む IPv6 パケットの処理に関する新しいルールを含める必要があります。IPv6 拡張ヘッダーの詳細については、『Cisco Nexus 9000 シリーズ NX-OS ユニキャストルーティング設定ガイド』の NX-OS リリース 9.3(x) 以降の「簡素化した IPv6 パケットヘッダー」を参照してください。



- (注) この手順で選択した許可ルールまたは拒否ルールは、パケットの他のフィールドに一致する他の ACL ルールに関係なく、少なくとも 1 つの拡張ヘッダーを持つ IPv6 パケットに適用されます。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>ipv6 access-list name</b> 例： switch(config)# ipv6 access-list acl-01 switch(config-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	<b>extension-header {permit-all   deny-all}</b> 例： switch(config-acl)# extension-header permit-all switch(config-acl)#	一致したパケットに必要なアクションを選択します。  <ul style="list-style-type: none"> <li>• <b>permit-all</b> : 少なくとも 1 つの拡張ヘッダーを持つ IPv6 パケットが許可されます。</li> <li>• <b>deny-all</b> : 少なくとも 1 つの拡張ヘッダーを持つ IPv6 パケットがドロップされます。</li> </ul>

## 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。

コマンド	目的
<b>show hardware access-list tcam region</b>	デバイスで次のリロード時に適用される TCAM サイズを表示します。

コマンド	目的
<b>show hardware access-list tcam template</b> {all   nfe   nfe2   I2-I3   I3   <i>template-name</i> }	<p>すべての TCAM テンプレートまたは特定のテンプレートの設定を表示します。</p> <p><b>nfe</b> : ネットワーク フォワードイング エンジン (NFE) 対応の Cisco Nexus 9300 および 9500 シリーズ、3164Q、および 31128PQ デバイスでのデフォルト TCAM テンプレート。</p> <p><b>nfe2</b> : NFE2 対応の Cisco Nexus 9500、3232C、および 3264Q デバイスのデフォルト TCAM テンプレート。</p> <p><b>I2-I3</b> : Cisco Nexus 9200 シリーズ スイッチでのレイヤ 2 およびレイヤ 3 設定のデフォルト TCAM テンプレート。</p> <p><b>I3</b> : Cisco Nexus 9200 シリーズ スイッチでのレイヤ 3 設定のデフォルト TCAM テンプレート。</p>
<b>show ip access-lists</b>	IPv4 ACL の設定を表示します。
<b>show ipv6 access-lists</b>	IPv6 ACL の設定を表示します。

コマンド	目的
<b>show logging ip access-list cache [detail]</b>	送信元 IP と宛先 IP アドレス、送信元ポートと宛先ポートの情報、および送信元インターフェイスなどの、アクティブログフロー情報を表示します。 <b>logging ip access-list detailed</b> コマンドを入力すると、出力には、アクセスコントロールエントリ (ACE) のシーケンス番号、ACE のアクション、ACL の名前、ACL の方向、ACL のフィルタタイプ、および ACL の適用インターフェイスの情報も含まれます。
<b>show logging ip access-list status</b>	拒否フローの最大数、現在の有効なログ間隔と現在の有効なしきい値を表示します。
<b>show running-config acllog</b>	ACL ログの実行コンフィギュレーションを表示します。
<b>show running-config aclmgr [all]</b>	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。  <b>Note</b> このコマンドは、実行コンフィギュレーションのユーザ設定 ACL を表示します。 <b>all</b> 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。
<b>show startup-config acllog</b>	ACL ログ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。

コマンド	目的
<code>show startup-config aclmgr [all]</code>	<p>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。</p> <p><b>Note</b> 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設定 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。</p>

## 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。

コマンド	目的
<code>show ip access-lists</code>	IPv4 ACL の設定を表示します。IPv4 ACL に <b>statistics per-entry</b> コマンドが含まれている場合は、 <b>show ip access-lists</b> 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。
<code>show ipv6 access-lists</code>	IPv6 ACL の設定を表示します。IPv6 ACL に <b>statistics per-entry</b> コマンドが含まれている場合は、 <b>show ipv6 access-lists</b> 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。
<code>clear ip access-list counters</code>	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。
<code>clear ipv6 access-list counters</code>	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 回線上的の入力 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
```

次の例では、IPv4 ACL ロギングを設定する方法を示します。

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ip access-list logging-test
switch(config-acl)# permit ip any 2001:DB8:1::1/64 log
switch(config-acl)# exit
switch(config)# interface ethernet 1/1
switch(config-if)# ip access-group logging-test in
switch(config-if)# exit
switch(config)# logging ip access-list cache interval 400
switch(config)# logging ip access-list cache entries 100
switch(config)# logging ip access-list cache threshold 900
switch(config)# hardware rate-limiter access-list-log 200
switch(config)# acllog match-log-level 5
```

以下に、UDF ベース ポート ACL の設定例を示します。

```
switch# configure terminal
switch(config)# hardware access-list tcam region ing-ifacl 256
switch(config)# udf pktoff10 packet-start 10 2
switch(config)# udf pktoff20 packet-start 10 1
switch(config)# hardware access-list tcam region ing-ifacl qualify udf pktoff10 pktoff20
```

```
switch# configure terminal
switch(config)# ip access-list udfacl
switch(config-acl)# statistics per-entry
switch(config-acl)# 10 permit ip any any udf pkttoff10 0x1234 0xffff

switch# configure terminal
switch(config)# interface Ethernet1/1
switch(config-if)# ip port access-group udfacl in
switch(config-if)# switchport
switch(config-if)# no shutdown
```

## システム ACL について

Cisco Nexus 9500 シリーズ スイッチでは、-R および -RX ライン カードを使用してシステム ACL を設定できます。システム ACL を使用すると、スイッチ内の同じアクセスリストを持つすべてのポートにレイヤ 2 ポート ACL (PACL) を設定できます。システム ACL を設定すると、TCAM の使用率が低下し、ポリシーの適用または変更中に時間とメモリの使用率が低下します。

システム ACL の設定については、次の注意事項と制限事項を参照してください。

- システム PACL は、レイヤ 2 インターフェイスでのみサポートされます。
- -R ライン カードを備えた Cisco Nexus 9500 シリーズ スイッチでスイッチが起動するために、他のすべての基本機能で最大 10K の ACE がサポートされます。-RX ライン カードを搭載した Cisco Nexus 9500 シリーズ スイッチのハードウェア容量は 64K ACE です。
- N3K-C3636C-R および N3K-C36180YC-R ライン カードを搭載した Cisco Nexus 3600 プラットフォーム スイッチでシステム ACL を設定することもできます。
- IPv4 PACL TCAM リージョン (ifacl) を -R ライン カードの合計物理 TCAM 容量 (12k) よりも多く設定すると、-R ライン カードのみの電源が切断されます。
- ACE 統計情報は、システム ACL ではまだサポートされていません。
- IPv6 は、システム ACL ではまだサポートされていません。
- システム ACL は、ブレイクアウト ポートではサポートされません。
- -R シリーズ ライン カードを搭載した Cisco Nexus シリーズ スイッチでの Quality of Service、ACL、または TCAM カービング設定については、『[Cisco Nexus 3600 NX-OS Quality of Service 設定ガイド、リリース 7.x](#)』を参照してください。
- 非アトミック更新は、すべてのトラフィックをドロップまたは許可します。デフォルトで、ACL の更新が完了するまで非アトミック更新はすべてのトラフィックをドロップします。非アトミック ACL 更新動作は、**hardware access-list update default-result permit** CLI コマンドを使用して制御できます。この CLI は物理ポートでのみ動作します。次の例を参照してください。

```
hardware access-list update default-result permit => #Allows all the traffic
during ACL updates. There may be < 10secs traffic drop.
```

```
no hardware access-list update default-result permit => #This is the default
behavior. It denies all the traffic during ACL updates.
```

- Cisco NX-OS リリース 9.2(2) 以前のリリースでは、アトミック ACL 更新は Cisco Nexus -R シリーズ ライン カードではサポートされていませんが、非アトミック更新 **hardware access-list update default-result** が Cisco Nexus -R シリーズ ライン カードでサポートされません。

## TCAM リージョンの分割

システム ACL を設定する前に、まず TCAM リージョンを分割します。1k 未満の ACL を設定する場合は、TCAM リージョンを分割する必要がないことに注意してください。詳細については、[ACL TCAM リージョン サイズの設定 \(342 ページ\)](#) を参照してください。



- (注) Cisco NX-OS リリース 7.0(3)F3(4) 以降では、PACL IPv4、RACL IPv4、および RACL IPv6 を 12k を超えて設定できます。

## システム ACL の設定

IPv4 ACL を作成したら、システム ACL を設定します。

### 始める前に

デバイスで IPv4 ACL を作成します。詳細については、「[IP ACL の作成 \(334 ページ\)](#)」を参照してください。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>config t</b>	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	<b>system acl</b>	システム ACL を設定します。
ステップ 3	<b>ip port access-group &lt;pacl name&gt; in</b>	インターフェイスにレイヤ 2 PACL を適用します。ポート ACL では、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。

## システム ACL の設定および show コマンドの例

システム ACL の show コマンドについては、次の設定例を参照してください。



## 1K スケールのシステム PACL の設定（デフォルト TCAM を使用）

1K スケールのシステム PACL の設定については、次の例を参照してください（デフォルト TCAM を使用）。

ステップ 1 : PACL を作成します。

```
config t
ip access-list PACL-DNA
  10 permit ip 1.1.1.1/32 any
  20 permit tcp 3.0.0.0/8 255.0.0.0 eq 1500
  25 deny udp any any eq 500
  26 deny tcp any eq 490 any
  ....
  1000 deny any any
```

ステップ 2 : PACL をシステム レベルに適用します。

```
configuration terminal
system acl
  ip port access-group PACL-DNA in
```

スイッチに設定されているシステム ACLを検証するには、**sh run aclmgr | sec system** コマンドを使用します。

```
switch# sh run aclmgr | sec system
system acl
  ip port access-group test in
switch#
```

スイッチに設定されている PACL を検証するには、**sh ip access-lists <name> [summary]** コマンドを使用します。

```
switch# sh ip access-lists test

IP access list test
  10 deny udp any any eq 27
  20 permit ip 1.1.1.1/32 100.100.100.100/32
  30 permit ip 1.2.1.1/32 100.100.100.100/32
  40 permit ip 1.3.1.1/32 100.100.100.100/32
  50 permit ip 1.4.1.1/32 100.100.100.100/32
  60 permit ip 1.5.1.1/32 100.100.100.100/32
  70 permit ip 1.6.1.1/32 100.100.100.100/32
  80 permit ip 1.7.1.1/32 100.100.100.100/32
  90 permit ip 1.8.1.1/32 100.100.100.100/32

switch# sh ip access-lists test summary
IPV4 ACL test
Total ACEs Configured: 12279
Configured on interfaces:
Active on interfaces:
  - ingress
  - ingress

switch#
```

PACL IPv4 (ifacl) TCAMリージョンサイズを検証するには、**show hardware access-list tcam region** コマンドを使用します。

```
switch# show hardware access-list tcam region
*****WARNING*****
*****The output shows NFE tcam region info*****
***Please refer to 'show hardware access-list tcam template' for NFE2***
*****
          IPV4 PAACL [ifacl] size = 12280
          IPV6 PAACL [ipv6-ifacl] size = 0
          MAC PAACL [mac-ifacl] size = 0
          IPV4 Port QoS [qos] size = 640
          IPV6 Port QoS [ipv6-qos] size = 256
          MAC Port QoS [mac-qos] size = 0
          FEX IPV4 PAACL [fex-ifacl] size = 0
          FEX IPV6 PAACL [fex-ipv6-ifacl] size = 0
          FEX MAC PAACL [fex-mac-ifacl] size = 0
          FEX IPV4 Port QoS [fex-qos] size = 0
          FEX IPV6 Port QoS [fex-ipv6-qos] size = 0
          FEX MAC Port QoS [fex-mac-qos] size = 0
          IPV4 VACL [vacl] size = 0
          IPV6 VACL [ipv6-vacl] size = 0
          MAC VACL [mac-vacl] size = 0
          IPV4 VLAN QoS [vqos] size = 0
          IPV6 VLAN QoS [ipv6-vqos] size = 0
          MAC VLAN QoS [mac-vqos] size = 0
          IPV4 RACL [racl] size = 0
          IPV6 RACL [ipv6-racl] size = 128
          IPV4 Port QoS Lite [qos-lite] size = 0
          FEX IPV4 Port QoS Lite [fex-qos-lite] size = 0
          IPV4 VLAN QoS Lite [vqos-lite] size = 0
          IPV4 L3 QoS Lite [l3qos-lite] size = 0
          Egress IPV4 QoS [e-qos] size = 0
          Egress IPV6 QoS [e-ipv6-qos] size = 0
          Egress MAC QoS [e-mac-qos] size = 0
          Egress IPV4 VACL [vacl] size = 0
          Egress IPV6 VACL [ipv6-vacl] size = 0
          Egress MAC VACL [mac-vacl] size = 0
          Egress IPV4 RACL [e-racl] size = 0
          Egress IPV6 RACL [e-ipv6-racl] size = 0
          Egress IPV4 QoS Lite [e-qos-lite] size = 0
          IPV4 L3 QoS [l3qos] size = 640
          IPV6 L3 QoS [ipv6-l3qos] size = 256
          MAC L3 QoS [mac-l3qos] size = 0
          Ingress System size = 0
          Egress System size = 0
          SPAN [span] size = 96
          Ingress COPP [copp] size = 128
          Ingress Flow Counters [flow] size = 0

switch#
```

ACL 関連のテクニカル サポート情報を表示するには、**show tech-support aclmgr** および **show tech-support aclqos** コマンドを使用します。

```
show tech-support aclmgr
show tech-support aclqos
```

# 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 9000 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。



### Note

Cisco Nexus リリース 7.0(3)I5(2) 以降では、**no host IPv4-address** コマンドはサポートされていません。DME サポートでは、**no sequence** コマンドを使用しない削除はサポートされていません。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> 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	<b>object-group ip address name</b>  <b>Example:</b> 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。  <ul style="list-style-type: none"> <li>• [sequence-number] <b>host IPv4-address</b></li> <li>• [sequence-number] IPv4-address/prefix-len</li> <li>• [sequence-number] IPv4-address network-wildcard</li> </ul> <b>Example:</b>	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、 <b>host</b> コマンドを使用して単一のホストを指定するか、または <b>host</b> 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。  IPv4 オブジェクトグループのプレフィックス長を指定できます。これは、最初の

	Command or Action	Purpose
	switch(config-ipaddr-ogroup)# host 10.99.32.6	連続ビットでのみ一致します。または、アドレスの任意のビットで一致するワイルドカードマスクを指定できます。
ステップ 4	次のいずれかのコマンドを入力します。  <ul style="list-style-type: none"> <li>• no [sequence-number]</li> <li>• no host IPv4-address</li> <li>• no IPv4-address/prefix-len</li> <li>• no IPv4-address network-wildcard</li> </ul> <b>Example:</b> 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	(Optional) <b>show object-group name</b>  <b>Example:</b> switch(config-ipaddr-ogroup)# show object-group ipv4-addr-group-13	オブジェクト グループの設定を表示します。
ステップ 6	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> switch(config-ipaddr-ogroup)# 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。

## 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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> 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	<b>object-group ipv6 address name</b>  <b>Example:</b> 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。  <ul style="list-style-type: none"> <li>• [sequence-number] host IPv6-address</li> </ul>	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、 <b>host</b> コマンドを使用して単一のホストを

	Command or Action	Purpose
	<ul style="list-style-type: none"> <li>• <i>[sequence-number]</i> <i>IPv6-address/prefix-len</i></li> <li>• <i>[sequence-number]</i> <i>IPv6-address network-wildcard</i></li> </ul> <p><b>Example:</b></p> <pre>switch(config-ipv6addr-ogroup)# host 2001:db8:0:3ab0::1</pre> <p><b>Example:</b></p> <pre>switch(config-ipv6addr-ogroup)# 10 1::1 2::2</pre>	<p>指定するか、または <b>host</b> 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。</p> <p>IPv6 オブジェクトグループのプレフィックス長を指定できます。これは、最初の連続ビットでのみ一致します。または、アドレスの任意のビットと一致するワイルドカードを指定できます。IPv6 ワイルドカードマスクは、Cisco Nexus 9200、9300-EX、および 9300-FX/FX2/FXP スイッチと Cisco Nexus 9364C スイッチでサポートされます。</p>
ステップ 4	<p>次のいずれかのコマンドを入力します。</p> <ul style="list-style-type: none"> <li>• <b>no</b> <i>sequence-number</i></li> <li>• <b>no</b> <i>host IPv6-address</i></li> <li>• <b>no</b> <i>IPv6-address/prefix-len</i></li> <li>• <b>no</b> <i>IPv6-address network-wildcard</i></li> </ul> <p><b>Example:</b></p> <pre>switch(config-ipv6addr-ogroup)# no host 2001:db8:0:3ab0::1</pre>	<p>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、<b>no</b> 形式の <b>host</b> コマンドを使用します。</p>
ステップ 5	<p>(Optional) <b>show object-group name</b></p> <p><b>Example:</b></p> <pre>switch(config-ipv6addr-ogroup)# show object-group ipv6-addr-group-A7</pre>	<p>オブジェクトグループの設定を表示します。</p>
ステップ 6	<p>(Optional) <b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch(config-ipv6addr-ogroup)# copy running-config startup-config</pre>	<p>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。</p>

## 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。

### Procedure

	Command or Action	Purpose
ステップ 1	<p><b>configure terminal</b></p> <p><b>Example:</b></p>	<p>グローバルコンフィギュレーションモードを開始します。</p>

	Command or Action	Purpose
	switch# configure terminal switch(config)#	
ステップ 2	<b>object-group ip port name</b>  <b>Example:</b> 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	<i>[sequence-number] operator port-number</i> <i>[port-number]</i>  <b>Example:</b> 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。 <ul style="list-style-type: none"> <li>• <b>eq</b> : 指定したポート番号だけに一致します。</li> <li>• <b>gt</b> : 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。</li> <li>• <b>lt</b> : 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。</li> <li>• <b>neq</b> : 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。</li> <li>• <b>range</b> : 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。</li> </ul> <p><b>Note</b>     <b>range</b> コマンドだけは、2 つの <i>port-number</i> 引数を必要とします。</p>
ステップ 4	<b>no</b> { <i>sequence-number</i>   <i>operator port-number</i> <i>[port-number]</i> }  <b>Example:</b> 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 <b>no</b> 形式で使用します。
ステップ 5	(Optional) <b>show object-group name</b>  <b>Example:</b> switch(config-port-ogroup)# show object-group NYC-datacenter-ports	オブジェクト グループの設定を表示します。

	Command or Action	Purpose
ステップ 6	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> switch(config-port-ogroup)# 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。

## 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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> 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	<b>no object-group {ip address   ipv6 address   ip port} name</b>  <b>Example:</b> switch(config)# no object-group ip address ipv4-addr-group-A7	指定のオブジェクト グループを削除します。
ステップ 3	(Optional) <b>show object-group</b>  <b>Example:</b> switch(config)# show object-group	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	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> 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。

## 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、次のいずれかのコマンドを入力します。

コマンド	目的
<b>show object-group</b>	オブジェクト グループの設定を表示します。

コマンド	目的
<code>show {ip   ipv6} access-lists name [expanded]</code>	ACL 設定の拡張された統計情報を表示します。
<code>show running-config aclmgr</code>	オブジェクトグループを含めて、ACL の設定を表示します。

??????

## 時間範囲の Session Manager 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 9000 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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> <code>switch# configure terminal</code> <code>switch(config)#</code>	グローバル 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	<b>time-range name</b>  <b>Example:</b> <code>switch(config)# time-range</code> <code>workday-daytime</code> <code>switch(config-time-range)#</code>	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	(Optional) <b>[sequence-number] periodic weekday time to [weekday] time</b>  <b>Example:</b> <code>switch(config-time-range)# periodic</code> <code>monday 00:00:00 to friday 23:59:59</code>	指定開始日時と終了日時の間（両端を含める）の 1 日以上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	(Optional) <b>[sequence-number] periodic list-of-weekdays time to time</b>  <b>Example:</b>	<code>list-of-weekdays</code> 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



	Command or Action	Purpose
	<pre>switch(config-time-range)# periodic weekdays 06:00:00 to 20:00:00</pre>	<p>ルを作成します。<i>list-of-weekdays</i> 引数の値には次のキーワードも使用できます。</p> <ul style="list-style-type: none"> <li>• <b>daily</b> : 1 週間のすべての曜日</li> <li>• <b>weekdays</b> : 月曜日から金曜日まで</li> <li>• <b>weekend</b> : 土曜日から日曜日まで</li> </ul>
ステップ 5	<p>(Optional) [<i>sequence-number</i>] <b>absolute start</b> <i>time date</i> [<b>end</b> <i>time date</i>]</p> <p><b>Example:</b></p> <pre>switch(config-time-range)# absolute start 1:00 15 march 2013</pre>	<p><b>start</b> キーワードの後ろに指定した日時から有効になる絶対基準でのルールを作成します。<b>end</b> キーワードを省略した場合、そのルールは開始日時を過ぎると常に有効になります。</p>
ステップ 6	<p>(Optional) [<i>sequence-number</i>] <b>absolute</b> [<b>start</b> <i>time date</i>] <b>end</b> <i>time date</i></p> <p><b>Example:</b></p> <pre>switch(config-time-range)# absolute end 23:59:59 31 may 2013</pre>	<p><b>end</b> キーワードの後ろに指定した日時まで有効になる絶対基準でのルールを作成します。<b>start</b> 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ずっと有効です。</p>
ステップ 7	<p>(Optional) <b>show time-range</b> <i>name</i></p> <p><b>Example:</b></p> <pre>switch(config-time-range)# show time-range workday-daytime</pre>	<p>時間範囲の設定を表示します。</p>
ステップ 8	<p>(Optional) <b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch(config-time-range)# copy running-config startup-config</pre>	<p>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。</p>

## 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。

既存のルールの中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。

### Procedure

	Command or Action	Purpose
ステップ 1	<p><b>configure terminal</b></p> <p><b>Example:</b></p>	<p>グローバル コンフィギュレーション モードを開始します。</p>

	Command or Action	Purpose
	switch# configure terminal switch(config)#	
ステップ 2	<b>time-range name</b>  <b>Example:</b> 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	(Optional) [ <i>sequence-number</i> ] <b>periodic weekday time to [weekday] time</b>  <b>Example:</b> switch(config-time-range)# periodic monday 00:00:00 to friday 23:59:59	指定開始日時と終了日時の間（両端を含める）の 1 日以上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	(Optional) [ <i>sequence-number</i> ] <b>periodic list-of-weekdays time to time</b>  <b>Example:</b> switch(config-time-range)# 100 periodic weekdays 05:00:00 to 22:00:00	<i>list-of-weekdays</i> 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。 <i>list-of-weekdays</i> 引数の値には次のキーワードも使用できます。  <ul style="list-style-type: none"> <li>• <b>daily</b> : 1 週間のすべての曜日</li> <li>• <b>weekdays</b> : 月曜日から金曜日まで</li> <li>• <b>weekend</b> : 土曜日から日曜日まで</li> </ul>
ステップ 5	(Optional) [ <i>sequence-number</i> ] <b>absolute start time date [end time date]</b>  <b>Example:</b> switch(config-time-range)# absolute start 1:00 15 march 2013	<b>start</b> キーワードの後ろに指定した日時から有効になる絶対基準でのルールを作成します。 <b>end</b> 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	(Optional) [ <i>sequence-number</i> ] <b>absolute [start time date] end time date</b>  <b>Example:</b> switch(config-time-range)# absolute end 23:59:59 31 may 2013	<b>end</b> キーワードの後ろに指定した日時まで有効になる絶対基準でのルールを作成します。 <b>start</b> 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ずっと有効です。
ステップ 7	(Optional) <b>no {<i>sequence-number</i>   periodic arguments . . .   absolute arguments . . . }</b>  <b>Example:</b> switch(config-time-range)# no 80	時間範囲から特定のルールを削除します。
ステップ 8	(Optional) <b>show time-range name</b>  <b>Example:</b> switch(config-time-range)# show time-range workday-daytime	時間範囲の設定を表示します。

	Command or Action	Purpose
ステップ 9	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch(config-time-range)# copy running-config startup-config</pre>	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。

**Related Topics**

[時間範囲のシーケンス番号の変更](#) (392 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。

**Before you begin**

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。

**Procedure**

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>no time-range name</b>  <b>Example:</b> <pre>switch(config)# no time-range daily-workhours</pre>	名前を指定した時間範囲を削除します。
ステップ 3	(Optional) <b>show time-range</b>  <b>Example:</b> <pre>switch(config-time-range)# show time-range</pre>	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	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch# copy running-config startup-config</pre>	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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>resequence time-range name starting-sequence-number increment</b> <b>Example:</b> <pre>switch(config)# resequence time-range daily-workhours 100 10 switch(config)#</pre>	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	(Optional) <b>show time-range name</b> <b>Example:</b> <pre>switch(config)# show time-range daily-workhours</pre>	時間範囲の設定を表示します。
ステップ 4	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	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。

コマンド	目的
<b>show time-range</b>	時間範囲の設定を表示します。
<b>show running-config aclmgr</b>	すべての時間範囲を含めて、ACL の設定を表示します。

## 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
TAP アグリゲーション	<a href="#">『Configuring TAP Aggregation and MPLS Stripping』</a>





## 第 13 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。

この章は、次の項で構成されています。

- [MAC ACL について, on page 395](#)
- [MAC ACL の注意事項と制約事項 \(396 ページ\)](#)
- [MAC ACL のデフォルト設定, on page 397](#)
- [MAC ACL の設定, on page 397](#)
- [MAC ACL の設定の確認, on page 408](#)
- [MAC ACL の統計情報のモニタリングとクリア, on page 408](#)
- [MAC ACL の設定例, on page 408](#)
- [MAC ACL に関する追加情報, on page 409](#)

## MAC ACL について

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。

## 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。



(注) MAC パケット分類は、Cisco NX-OS リリース 9.3(3) ではサポートされていません。

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	<ul style="list-style-type: none"> <li>• 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。</li> <li>• IP ポート ACL をインターフェイスで適用できません。</li> </ul>
ディセーブル	<ul style="list-style-type: none"> <li>• 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。</li> <li>• IP ポート ACL をインターフェイスで適用できます。</li> </ul>

## 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。
- 適用する ACL エントリが多すぎると、設定が拒否される可能性があります。
- MAC パケット分類は、MAC ACL が VACL の一部として適用されている場合、サポートされません。
- MAC パケット分類は、Cisco Nexus 9300 シリーズ スイッチの 40G アップリンク ポートでの QoS ポリシーの一致基準として MAC ACL が使用されている場合、サポートされません。
- EX/FX 以外の Cisco Nexus 9000 シリーズ スイッチで MAC ACL を定義する場合は、トラフィックが適切に照合されるように `ethertype` を定義する必要があります。
- Cisco Nexus 9300-EX プラットフォーム スイッチでは、Mac パケット分類が部分的にサポートされています。パケットを L2 パケットとしてマーキングするための直接のフィールドがない場合、スイッチは、キーフィールド内に特定のフィールド (`src_mac`、`dst_mac`、`vlan` など) があるすべてのパケットのマッチングを行います。ただし、`eth_type` フィールドではマッチングを行いません。したがって、MAC プロトコル番号フィールドを除いて同一のフィールドを持つ 2 つのルールをインストールすると、マッチング条件はハードウェアで同一のままになります。したがって、ルールシーケンスの最初のエントリは、すべてのプロトコル番号のすべてのパケットに対してヒットしますが、`mac-packet` 分類が設定されている場合の MAC プロトコル番号は `no-op` になります。
- `mac address-table limit <16-256> user-defined` コマンドを使用してユーザ定義の MAC 制限を設定すると、FHRP グループ制限が自動的に調整され、ユーザ定義の MAC 制限と FHRP 制限の合計は 490 になります。たとえば、ユーザ定義の MAC 制限を 100 に設定すると、FHRP 制限は 390 に減少します。
- Cisco NX-OS Release 9.3(2) 以降では、ユーザ定義の MAC アドレス制限を 16 ～ 256 の範囲で設定できます。



- Cisco Nexus 93600CD-GX スイッチは、ポート 1/1-24 でのブレイクアウトをサポートしていません。

## 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。

Table 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。

#### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> 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	<b>mac access-list name</b>  <b>Example:</b> 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	<b>{permit   deny} source destination-protocol</b>  <b>Example:</b> switch(config-mac-acl)# 100 permit mac 00c0.4f00.0000 0000.00ff.ffff any 0x0806	MAC ACL 内にルールを作成します。  <b>permit</b> コマンドと <b>deny</b> 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。

	Command or Action	Purpose
ステップ 4	(Optional) <b>statistics per-entry</b> <b>Example:</b> switch(config-mac-acl)# statistics per-entry	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 5	(Optional) <b>show mac access-lists name</b> <b>Example:</b> switch(config-mac-acl)# show mac access-lists acl-mac-01	MAC ACL の設定を表示します。
ステップ 6	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch(config-mac-acl)# 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。

## UDF ベースの MAC ACL の設定

Cisco Nexus 9200、9300、および 9300-EX シリーズ スイッチの UDF ベースの MAC アクセスリスト (ACL) を設定できます。この機能により、デバイスはユーザ定義フィールド (UDF) で照合し、一致するパケットを MAC ACL に適用できます。

Cisco NX-OS リリース 9.3(3) 以降、Cisco Nexus 9364C-GX、Cisco Nexus 9316D-GX、および Cisco Nexus 93600CD-GX スイッチで UDF ベース MAC アクセスリスト (ACL) を設定できます。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> <b>例:</b> 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	<b>udf udf-name offset-base offset length</b> <b>例:</b> switch(config)# udf pkttoff10 packet-start 10 2	次のように UDF を定義します。 <ul style="list-style-type: none"> <li>• <b>udf-name</b> : UDF の名前を指定します。名前には最大 16 文字の英数字を入力できます。</li> <li>• <b>offset-base</b> : UDF オフセットベースを <b>{packet-start}</b> のように指定します。</li> <li>• <b>offset</b> : オフセットベースからオフセットさせるバイト数を指定します。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <i>length</i> : オフセットからのバイト数を指定します。1 バイトまたは 2 バイトだけがサポートされます。追加のバイト数に一致させるには、複数の UDF の定義が必要です。</li> </ul> <p>複数の UDF を定義できますが、必要な UDF のみを定義することを推奨します。</p>
ステップ 3	<p><b>hardware access-list tcam region ing-ifacl qualify {udf udf-name }</b></p> <p>例 :</p> <pre>switch(config)# hardware access-list tcam region ing-ifacl qualify udf pktoff10</pre>	<p>IPv4 または IPv6 ポート ACL に適用する ing-ifacl TCAM リージョンに UDF をアタッチします。</p> <p>最大 18 個の UDF がサポートされます。</p> <p>(注) UDF 修飾子が追加されると、TCAM リージョンはシングル幅からダブル幅になります。十分な空き領域があることを確認してください。そうでない場合、このコマンドは拒否されます。必要であれば、未使用リージョンでの TCAM スペースを削減してから、このコマンドを再入力することもできます。詳細については、「<a href="#">ACL TCAM リージョンサイズの設定</a>」を参照してください。</p> <p>(注) このコマンドの <b>no</b> 形式を使用すると、UDF の TCAM リージョンへの付加は解除され、リージョンはシングル幅に戻ります。</p>
ステップ 4	<p>必須: <b>copy running-config startup-config</b></p> <p>例 :</p> <pre>switch(config)# copy running-config startup-config</pre>	<p>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。</p>
ステップ 5	<p>必須: <b>reload</b></p>	<p>デバイスがリロードされます。</p>

	コマンドまたはアクション	目的
	例： switch(config)# reload	(注) UDF 設定は、 <b>copy running-config startup-config + reload</b> を入力した後にのみ有効になります。
ステップ 6	<b>mac access-list udf-acl</b> 例： switch(config)# mac access-list udfacl switch(config-acl)#	MAC アクセス コントロール リスト (ACL) を作成して、MAC 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 7	<b>permit mac source destination udf udf-name value mask</b> 例： switch(config-acl)# permit mac any any udf pkttoff10 0x1234 0xffff	MAC ACL を設定して、外部パケットフィールドについて現在のアクセスコントロールエントリ (ACE) と併せて UDF で一致させるように設定します (例 2)。値とマスクの引数の範囲は 0x0~0xFFFF です。  1つの ACL には、UDF の有無にかかわらず、同時に複数の ACE を持たせることができます。各 ACE ごとに異なる UDF フィールドで一致させることもできれば、すべての ACE で同じリストの UDF で一致させることもできます。
ステップ 8	<b>interface port-channel channel-number</b> 例： switch(config)# interface port-channel 5 switch(config-if)#	レイヤ 2 のポート チャンネル 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 9	<b>mac port access-group udf-access-list</b> 例： switch(config-if)# mac port access-group udf-acl-01	UDF ベース MAC ACL をインターフェイスに適用します。
ステップ 10	(任意) <b>copy running-config startup-config</b> 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。

## インターフェイス MAC アドレスの設定と制限

静的 MAC アドレスは、SVI、レイヤ 3 インターフェイス、ポート チャンネル、レイヤ 3 サブインターフェイス、およびトンネルインターフェイスで設定できます。また、ポートおよびポー

トチャンネルの範囲で静的MACアドレスを設定することもできます。ただし、すべてのポートはレイヤ3にある必要があります。ポートの範囲内の1つのポートがレイヤ2にある場合でも、コマンドは拒否され、エラーメッセージが表示されます。

デフォルトでは、スイッチに設定できるMACアドレスの最大数は16です。ただし、この制限を変更して、MACアドレス数の範囲を16–256に設定することができます。

vPC対応スイッチでの設定制限には、ローカルに設定されたユーザ定義のMACアドレスと、vPCピアから同期されたユーザ定義のMACアドレスの両方が含まれます。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>interface ethernet slot/port</b> 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	<b>[no] mac-address static router MAC address</b> 例： switch(config-if)# mac-address 0019.D2D0.00AE	<p>インターフェイスMACアドレスを設定します。設定を削除するには、このコマンドの <b>no</b> 形式を使用します。次の4つのサポートされる形式のいずれでもMACアドレスを入力できます。</p> <ul style="list-style-type: none"> <li>• E.E.E</li> <li>• EE-EE-EE-EE-EE-EE</li> <li>• EE:EE:EE:EE:EE:EE</li> <li>• EEEE.EEEE.EEEE</li> </ul> <p>(注) 次の無効なMACアドレスを入力しないでください。</p> <ul style="list-style-type: none"> <li>• nul MAC アドレス： 0000.0000.0000</li> <li>• ブロードキャスト MAC アドレス： FFFF.FFFF.FFFF</li> <li>• マルチキャスト MAC アドレス： 0100.DAAA.ADDD</li> </ul>

	コマンドまたはアクション	目的
ステップ 4	(任意) <b>show interface ethernet slot/port</b>  例： switch(config-if)# show interface ethernet 2/1 switch(config)#	インターフェイスのすべての情報を表示します。
ステップ 5	<b>mac address-table limit 16-256 user-defined</b>  例： switch(config)# mac address-table limit 200 user-defined switch(config)#	スイッチに設定できる MAC アドレスの最大数を設定します。
ステップ 6	(任意) <b>show mac address-table limit user-defined</b>  例： switch(config)# show mac address-table limit user-defined	スイッチに設定できる MAC アドレスの最大数を表示します。

## 例

次に、インターフェイス MAC アドレスを設定する方法の例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 3/3
switch(config-if)# mac-address aaaa.bbbb.dddd
switch(config-if)# show interface ethernet 3/3
switch(config-if)#
switch(config)# mac address-table limit 100 user-defined
Warning: Configure the same User-Defined Mac Limit on the peer.
Warning: New Fhrp max group limit is 390
switch# show mac address-table limit user-defined
User Defined Mac Limit: 100
FHRP Mac Limit: 390
=====
```

## MAC ACL の変更

MAC ACL をデバイスから削除できます。

### Before you begin

MAC ACL が設定されているインターフェイスを探すには、**show mac access-lists** コマンドを、**summary** キーワードを指定して実行します。

## Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	<b>mac access-list name</b> <b>Example:</b> switch(config)# mac access-list acl-mac-01 switch(config-mac-acl)#	名前指定した 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	(Optional) [ <i>sequence-number</i> ] { <b>permit</b>   <b>deny</b> } <i>source destination-protocol</i> <b>Example:</b> switch(config-mac-acl)# 100 permit mac 00c0.4f00.0000 0000.00ff.ffff any 0x0806	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。 <b>permit</b> コマンドと <b>deny</b> 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。
ステップ 4	(Optional) <b>no</b> { <i>sequence-number</i>   { <b>permit</b>   <b>deny</b> } <i>source destination-protocol</i> } <b>Example:</b> switch(config-mac-acl)# no 80	指定したルールを MAC ACL から削除します。 <b>permit</b> コマンドと <b>deny</b> 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。
ステップ 5	(Optional) [ <b>no</b> ] <b>statistics per-entry</b> <b>Example:</b> switch(config-mac-acl)# statistics per-entry	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。 <b>no</b> 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	(Optional) <b>show mac access-lists name</b> <b>Example:</b> switch(config-mac-acl)# show mac access-lists acl-mac-01	MAC ACL の設定を表示します。
ステップ 7	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch(config-mac-acl)# 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。

## 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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	<b>resequence mac access-list name starting-sequence-number increment</b> <b>Example:</b> 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	(Optional) <b>show mac access-lists name</b> <b>Example:</b> switch(config)# show mac access-lists acl-mac-01	MAC ACL の設定を表示します。
ステップ 4	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> 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。

## MAC ACL の削除

MAC ACL をデバイスから削除できます。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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。



	Command or Action	Purpose
ステップ 2	<b>no mac access-list <i>name</i></b> <b>Example:</b> <pre>switch(config)# no mac access-list acl-mac-01 switch(config)#</pre>	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	(Optional) <b>show mac access-lists <i>name</i> summary</b> <b>Example:</b> <pre>switch(config)# show mac access-lists acl-mac-01 summary</pre>	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	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	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 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

### Before you begin

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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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。 <ul style="list-style-type: none"> <li><b>interface ethernet <i>slot/port</i></b></li> <li><b>interface port-channel <i>channel-number</i></b></li> </ul> <b>Example:</b>	<ul style="list-style-type: none"> <li>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。</li> <li>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</li> </ul>

	Command or Action	Purpose
	<pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre> <p><b>Example:</b></p> <pre>switch(config)# interface port-channel 5 switch(config-if)#</pre>	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	<p><b>mac port access-group <i>access-list</i></b></p> <p><b>Example:</b></p> <pre>switch(config-if)# mac port access-group acl-01</pre>	MAC ACL をインターフェイスに適用します。
ステップ 4	<p>(Optional) <b>show running-config aclmgr</b></p> <p><b>Example:</b></p> <pre>switch(config-if)# show running-config aclmgr</pre>	ACL の設定を表示します。
ステップ 5	<p>(Optional) <b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch(config-if)# copy running-config startup-config</pre>	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。

## 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。

始める前に

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

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル 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。 <ul style="list-style-type: none"> <li>• <b>interface ethernet slot/port</b></li> <li>• <b>interface port-channel channel-number</b></li> </ul> 例 : <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre> 例 : <pre>switch(config)# interface port-channel 5 switch(config-if)#</pre>	<ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> </ul>
ステップ 3	<b>[no] mac packet-classify</b> 例 : <pre>switch(config-if)# mac packet-classify</pre>	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。 <b>no</b> 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	(任意) 次のいずれかのコマンドを入力します。 <ul style="list-style-type: none"> <li>• <b>show running-config interface ethernet slot/port</b></li> <li>• <b>show running-config interface port-channel channel-number</b></li> </ul> 例 : <pre>switch(config-if)# show running-config interface ethernet 2/1</pre> 例 : <pre>switch(config-if)# show running-config interface port-channel 5</pre>	<ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> </ul>
ステップ 5	(任意) <b>copy running-config startup-config</b> 例 : <pre>switch(config-if)# copy running-config startup-config</pre>	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 の設定の確認

MAC ACL 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。

コマンド	目的
<code>show mac access-lists</code>	MAC ACL の設定を表示します。
<code>show running-config aclmgr [all]</code>	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。 <b>Note</b> このコマンドは、実行コンフィギュレーションのユーザ設定 ACL を表示します。 <b>all</b> 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。
<code>show startup-config aclmgr [all]</code>	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。 <b>Note</b> 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設定 ACL を表示します。 <b>all</b> 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 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。

コマンド	目的
<code>show mac access-lists</code>	MAC ACL の設定を表示します。MAC ACL に <b>statistics per-entry</b> コマンドが含まれている場合は、 <b>show mac access-lists</b> 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。
<code>clear mac access-list counters</code>	MAC ACL の統計情報をクリアします。

## 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 0x0806
```

```
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
TAP アグリゲーション	<a href="#">『Configuring TAP Aggregation and MPLS Stripping』</a>





## 第 14 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。

- [VLAN ACL について, on page 411](#)
- [VACL の前提条件, on page 412](#)
- [VACL の注意事項と制約事項 \(413 ページ\)](#)
- [VACL のデフォルト設定, on page 414](#)
- [VACL の設定, on page 414](#)
- [VACL 設定の確認, on page 417](#)
- [VACL 統計情報のモニタリングとクリア, on page 418](#)
- [VACL の設定例, on page 418](#)
- [VACL に関する追加情報, on page 418](#)

## VLAN ACL について

VLAN ACL (VACL) は、MAC ACL または IP 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。

## 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 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。

### Forward

デバイス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。

### Redirect

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。

### Drop

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。

## 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。Session Manager の詳細については、『*Cisco Nexus 9000 Series NX-OS System Management Configuration 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は、セッションマネージャを使用して設定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。Session Managerの詳細については、『Cisco Nexus 9000 Series NX-OS System Management Configuration Guide』を参照してください。
- 適用する ACL エントリが多すぎると、設定が拒否される可能性があります。
- 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。
- VACL のロギングはサポートされません。
- TCAM リソースは、VACL を複数の VLAN で適用する場合、共有されません。
- Cisco Nexus 9200 および 9300-EX シリーズスイッチは、VACL リダイレクトオプションをサポートしています。1つの物理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へのリダイレクトが許可されます。
- VACL は、N9K-X9636C-R、N9K-X9636C-RX、および N9K-X9636Q-R ラインカードを搭載した Cisco Nexus 9500 Series スイッチではサポートされていません。
- VACL では deny 文はサポートされていません。その代わりに、permit 文と「drop」アクションを組み合わせると、同様の結果を得ることができます。
- VACL を「redirect」オプションを使用して設定する場合、リダイレクトインターフェイスとして定義するインターフェイスは、この VACL の適用先である VLAN のメンバーとして設定する必要があります。リダイレクションを機能させるには、この VLAN がこのインターフェイス上でフォワーディング状態になっている必要があります。これらの条件が満たされない場合、スイッチは VACL とマッチしたパケットをドロップします。
- VACL カウンタをクリアするには、アクティブな VLAN フィルタが設定されていることを確認する必要があります。

VXLAN の VACL には、次のガイドラインが適用されます。

- アクセスからネットワーク方向（レイヤ 2 からレイヤ 3 のカプセル化パス）の VXLAN VLAN に適用される VACL は、内部ペイロードでサポートされます。
- VACL をアクセス側で使用して、オーバーレイ ネットワークに進入するトラフィックをフィルタ処理して除外することを推奨します。
- カプセル化解除された VXLAN トラフィックでの出力 VACL は、サポートされません。

## 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。

Table 36: 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。

## 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。

#### Before you begin

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。

#### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>vlan access-map map-name [sequence-number]</b> <b>Example:</b> <pre>switch(config)# vlan access-map acl-mac-map switch(config-access-map)#</pre>	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。

	Command or Action	Purpose
ステップ 3	次のいずれかのコマンドを入力します。 <ul style="list-style-type: none"> <li>• <b>match</b> {ip   ipv6} address <i>ip-access-list</i></li> <li>• <b>match mac</b> address <i>mac-access-list</i></li> </ul> <b>Example:</b> <pre>switch(config-access-map)# match mac address acl-ip-lab</pre> <b>Example:</b> <pre>switch(config-access-map)# match mac address acl-mac-01</pre>	アクセスマップエントリに ACL を指定します。
ステップ 4	<b>action</b> {drop   forward   redirect} <b>Example:</b> <pre>switch(config-access-map)# action forward</pre> <b>Example:</b> <pre>switch(config-access-map)# vlan access-map vacl1 switch(config-access-map)# action redirect e1/1 switch(config-access-map)# action redirect po100</pre>	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。  <b>action</b> コマンドは、 <b>drop</b> 、 <b>forward</b> 、および <b>redirect</b> オプションをサポートします。
ステップ 5	(Optional) <b>[no] statistics per-entry</b> <b>Example:</b> <pre>switch(config-access-map)# statistics per-entry</pre>	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。  <b>no</b> 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	(Optional) <b>show running-config aclmgr</b> <b>Example:</b> <pre>switch(config-access-map)# show running-config aclmgr</pre>	ACL の設定を表示します。
ステップ 7	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch(config-access-map)# copy running-config startup-config</pre>	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。

**Before you begin**

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。

**Procedure**

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> 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	<b>no vlan access-map</b> <i>map-name</i> [ <i>sequence-number</i> ]  <b>Example:</b> 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。 <i>sequence-number</i> 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	(Optional) <b>show running-config aclmgr</b>  <b>Example:</b> switch(config)# show running-config aclmgr	ACL の設定を表示します。
ステップ 4	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> 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。

**VACL の VLAN への適用**

VACL を VLAN に適用できます。

**Before you begin**

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。

**Procedure**

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b>	グローバル コンフィギュレーション モードを開始します。

	Command or Action	Purpose
	switch# configure terminal switch(config)#	
ステップ 2	<b>[no] vlan filter map-name vlan-list list</b>  <b>Example:</b> 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。 <b>no</b> を使用すると、VACL の適用が解除されます。
ステップ 3	(Optional) <b>show running-config aclmgr</b>  <b>Example:</b> switch(config)# show running-config aclmgr	ACL の設定を表示します。
ステップ 4	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> 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。

## VACL 設定の確認

VACL 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。

コマンド	目的
<b>show running-config aclmgr [all]</b>	VACL-related の設定も含めて、ACL の設定を表示します。  <b>Note</b> このコマンドは、実行コンフィギュレーションのユーザ設定 ACL を表示します。 <b>all</b> 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。
<b>show startup-config aclmgr [all]</b>	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。  <b>Note</b> 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設定 ACL を表示します。 <b>all</b> 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。
<b>show vlan filter</b>	VLAN に適用されている VACL の情報を表示します。
<b>show vlan access-map</b>	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。

コマンド	目的
<b>show vlan access-list</b>	VACL の設定を表示します。VLAN アクセス マップに <b>statistics per-entry</b> コマンドが含まれている場合は、 <b>show vlan access-list</b> 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。
<b>clear vlan access-list counters</b>	VACL の統計情報をクリアします。

## 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
QoS の設定	『Cisco Nexus 9000 Series NX-OS Quality of Service Configuration Guide』



## 第 15 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。

- [ポート セキュリティの概要, on page 419](#)
- [ポート セキュリティの前提条件, on page 427](#)
- [ポート セキュリティのデフォルト設定, on page 427](#)
- [ポート セキュリティの注意事項と制約事項, on page 427](#)
- [vPC 上のポート セキュリティの注意事項と制約事項 \(428 ページ\)](#)
- [ポート セキュリティの設定, on page 429](#)
- [ポート セキュリティの設定の確認, on page 441](#)
- [セキュア MAC アドレスの表示, on page 441](#)
- [ポート セキュリティの設定例, on page 441](#)
- [vPC ドメインでのポート セキュリティの設定例 \(441 ページ\)](#)
- [ポート セキュリティに関する追加情報, on page 443](#)

## 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 セットからの入力トラフィックだけを許可するようなレイヤ 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。



### Note

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有効に設定されたインターフェイスごとに、スタティックまたはダイナミック方式で、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。

### 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。

### 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



## スティック方式

スティック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、スティック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。スティックセキュア 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ク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ク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、代わりにスティック学習を実行します。スティック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

## 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。



**Note** この機能は Cisco Nexus 9200 および 9300-EX シリーズ スイッチでサポートされています。

### 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。



**Note** 絶対エージングタイムを設定すると、送信元 MAC からのトラフィックが流れていても、MAC エージングが発生します。ただし、MAC エージングおよび再学習中に、一時的なトラフィック ドロップが発生する可能性があります。

## 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、スタティックまたはダイナミックに学習された MAC アドレスにも適用されます。



**Tip** 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。

## 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。

### MAC 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過してしまう場合

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。

- デバイスが 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 番目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。

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

セキュア MAC アドレス以外のアドレスからの入力トラフィックをドロップします。

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。

### 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

レイヤ 2 転送モジュール (L2FM) のロギング レベルが 4 または 5 に増加した場合のみ、MAC 移動通知が表示されます。

MAC 移動違反が発生すると、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を増分し、設定された違反モードに関係なく、インターフェイスはエラーディセーブルになります。違反モードが[制限 (Restrict)]または[保護 (Protect)]に設定されている場合、違反はシステム ログに記録されます。

MAC移動違反は、設定された違反モードに関係なく、インターフェイスがエラーディセーブルになるため、**errdisable** コマンドを使用して自動 **errdisable** リカバリをイネーブルにすることを推奨します。

## 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ンネル

レイヤ2イーサネットポートチャン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。



---

**Note** VXLAN インターフェイスではポートセキュリティを設定できません。

---



---

**Note** ポートセキュリティは、Cisco Nexus 9300-EX/FX/FX2/FX3 シリーズ スイッチ上の非 vPC 展開でのみ FEX インターフェイスに対してサポートされます。Cisco NX-OS リリース 9.3(5) 以降、Cisco Nexus 9300-FX3 シリーズ スイッチがサポートされます。

---

## ポートセキュリティとポートチャンネルインターフェイス

ポートセキュリティは、レイヤ2ポートチャンネルインターフェイスでサポートされます。ポートチャン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。

## 一般的なガイドライン

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ク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。

#### ポートからトランクポートへのアクセス

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。

### スイッチポートからルートポート

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。

### ルートポートからスイッチポート

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。

## 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。

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	Dynamic
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、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。
- ポートセキュリティは、VXLAN インターフェイスではサポートされていません。

- ポートセキュリティは、Cisco Nexus 9300-EX シリーズスイッチの非 vPC 展開でのみ FEX インターフェイスに対してサポートされます。
- Cisco Nexus 9000 シリーズスイッチの USB ポートを無効にする方法はサポートされていません。
- プライマリ VLAN とセカンダリ VLAN 間のアソシエーションの設定後、このアソシエーションを削除すると、プライマリ VLAN 上に作成されたすべてのスタティック MAC アドレスは、プライマリ VLAN 上に限り存続します。



**Note** 一部の状況では、エラーメッセージが表示されずに設定が受け入れられますが、コマンドには効果がありません。

プライマリ VLAN とセカンダリ VLAN 間の関連付けを設定した後、次の手順を実行します。

- セカンダリ VLAN のスタティック MAC アドレスは作成できません。
- セカンダリ VLAN を学習したダイナミック MAC アドレスは期限切れになります。

## vPC 上の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に関する注意事項および制限事項とは別に、vPC のポートセキュリティに関する次の注意事項および制限事項を満たしていることを確認します。

- ポートセキュリティは、vPC 展開の FEX インターフェイスではサポートされません。
- vPC ドメイン内の両方の vPC ピアで、ポートセキュリティをグローバルに有効にする必要があります。
- 両方の vPC ピアの vPC 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する必要があります。
- プライマリ vPC ピアでスタティックセキュア MAC アドレスを設定する必要があります。スタティック MAC アドレスは、セカンダリ vPC ピアと同期されます。セカンダリピアでスタティックセキュア MAC アドレスも設定できます。第二スタティック MAC アドレスはセカンダリ vPC 設定に表示されますが、有効にはなりません。
- プライマリ vPC ポートとセカンダリ vPC ポートの両方で、最大 MAC カウント値が同じであることを確認する必要があります。
- セカンダリ vPC ポートでは、スタティック MAC の制限チェックは行われません。シスコは、最大 MAC カウントで定義されているように、セカンダリ vPC ポートで同じ数のスタティック MAC を設定することを推奨します。
- 学習したすべての MAC アドレスは vPC ピア間で同期されます。



- 両方の vPC ピアは、ダイナミックまたはスタティック MAC アドレスの学習方式で設定できます。シスコは、同じ方法を使用して両方の vPC ピアを設定することを推奨します。これは、vPC ロールの変更など、特定の場合にポートのシャットダウン (errDisabled 状態) を防ぐのに役立ちます。
- ダイナミック MAC アドレスは、両方の vPC ピアでエージング期限に達した後のみドロップされます。
- セキュア MAC アドレスの最大数は、プライマリ vPC スイッチ上で設定します。プライマリ vPC スイッチは数の検証を行い、セカンダリ スイッチで最大数設定を無視します。
- 違反時の処理は、プライマリ vPC 上で設定します。セキュリティ違反がトリガーされると、プライマリ vPC スイッチに定義されたセキュリティ処理が常に実行されます。
- 両方の vPC ピアで設定が正しいことを確認するには、**show vpc consistency-parameters id** コマンドを使用できます。
- スイッチでインサーブिसソフトウェアアップグレード (ISSU) が実行されている間、ポートセキュリティの動作はそのピア スイッチ上で停止されます。ピア スイッチはどの新しい MAC アドレスも学習せず、この動作中に発生した MAC の移動は無視されます。ISSU が完了すると、ピア スイッチに通知され、通常のポートセキュリティ機能が再開します。
- 上位バージョンへの ISSU がサポートされていますが、下位バージョンへの ISSU はサポートされていません。

## 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。

#### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します。

	Command or Action	Purpose
ステップ 2	<b>[no] feature port-security</b> <b>Example:</b> 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。 <b>no</b> 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	(Optional) <b>show port-security</b> <b>Example:</b> 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	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> 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。

## 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。

### Before you begin

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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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。

	Command or Action	Purpose
ステップ 2	次のいずれかのコマンドを入力します。  <ul style="list-style-type: none"> <li>• <b>interface ethernet slot/port</b></li> <li>• <b>interface port-channel channel-number</b></li> </ul> <b>Example:</b> <pre>switch(config)# interface ethernet 2/1 switch(config-if) #</pre>	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	<b>switchport</b>  <b>Example:</b> <pre>switch(config-if) # switchport</pre>	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	<b>[no] switchport port-security</b>  <b>Example:</b> <pre>switch(config-if) # switchport port-security</pre>	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。 <b>no</b> 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	(Optional) <b>show running-config port-security</b>  <b>Example:</b> <pre>switch(config-if) # show running-config port-security</pre>	ポートセキュリティの設定を表示します。
ステップ 6	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch(config-if) # copy running-config startup-config</pre>	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。

## スティック 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ク 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。スティック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、スティック MAC アドレス ラーニングはディセーブルです。

### Before you begin

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。

## Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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。  • <b>interface ethernet slot/port</b> • <b>interface port-channel channel-number</b>  <b>Example:</b> switch(config)# interface ethernet 2/1 switch(config-if)#	スティック 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	<b>switchport</b> <b>Example:</b> 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	<b>[no] switchport port-security mac-address sticky</b> <b>Example:</b> switch(config-if)# switchport port-security mac-address sticky	そのインターフェイスのスティック MAC アドレス ラーニングをイネーブルにします。 <b>no</b> オプションを使用するとスティック 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	(Optional) <b>show running-config port-security</b> <b>Example:</b> 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	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch(config-if)# 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。

## 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。



**Note** 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。

### Before you begin

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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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。  • <b>interface ethernet slot/port</b> • <b>interface port-channel channel-number</b> <b>Example:</b> 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	<b>[no] switchport port-security mac-address address [vlan vlan-ID]</b> <b>Example:</b> 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、 <b>vlan</b> キーワードを使用します。
ステップ 4	(Optional) <b>show running-config port-security</b> <b>Example:</b> 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。

	Command or Action	Purpose
ステップ 5	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch(config-if)# copy running-config startup-config</pre>	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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グ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。  <ul style="list-style-type: none"> <li>• <b>interface ethernet slot/port</b></li> <li>• <b>interface port-channel channel-number</b></li> </ul> <b>Example:</b> <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	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	<b>no switchport port-security mac-address address</b>  <b>Example:</b> <pre>switch(config-if)# no switchport port-security mac-address 0019.D2D0.00AE</pre>	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	(Optional) <b>show running-config port-security</b>  <b>Example:</b> <pre>switch(config-if)# show running-config port-security</pre>	ポートセキュリティの設定を表示します。
ステップ 5	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch(config-if)# copy running-config startup-config</pre>	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。

### 始める前に

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

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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。  • <b>interface ethernet slot/port</b> • <b>interface port-channel channel-number</b>  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	<b>no switchport port-security mac-address sticky</b>  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。
ステップ 4	<b>clear port-security dynamic address address</b>  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	(任意) <b>show port-security address interface {ethernet slot/port   port-channel channel-number}</b>  例： switch(config)# show port-security address interface ethernet 2/1	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。

	コマンドまたはアクション	目的
ステップ 6	(任意) <b>switchport port-security mac-address sticky</b>  例 : <pre>switch(config-if)# switchport port-security mac-address sticky</pre>	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。

### Before you begin

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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>clear port-security dynamic {interface ethernet slot/port   address address} [vlan vlan-ID]</b>  <b>Example:</b> <pre>switch(config)# clear port-security dynamic interface ethernet 2/1</pre>	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。  <b>interface</b> 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。  <b>address</b> 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、 <b>vlan</b> キーワードを使用します。
ステップ 3	(Optional) <b>show port-security address</b>  <b>Example:</b> <pre>switch(config)# show port-security address</pre>	セキュア MAC アドレスを表示します。



	Command or Action	Purpose
ステップ 4	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch(config-if)# copy running-config startup-config</pre>	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。



### Note

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。

### Before you begin

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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グ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。  <ul style="list-style-type: none"> <li>• <b>interface ethernet slot/port</b></li> <li>• <b>interface port-channel channel-number</b></li> </ul> <b>Example:</b> <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	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。

	Command or Action	Purpose
ステップ 3	<p>[no] <b>switchport port-security maximum number</b> [vlan <i>vlan-ID</i>]</p> <p><b>Example:</b></p> <pre>switch(config-if)# switchport port-security maximum 425</pre>	<p>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。有効な <i>number</i> の最高値は 1025 です。 <b>no</b> 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。</p> <p>最大数を適用する VLAN を指定する場合は、 <b>vlan</b> キーワードを使用します。</p>
ステップ 4	<p>(Optional) <b>show running-config port-security</b></p> <p><b>Example:</b></p> <pre>switch(config-if)# show running-config port-security</pre>	<p>ポートセキュリティの設定を表示します。</p>
ステップ 5	<p>(Optional) <b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch(config-if)# copy running-config startup-config</pre>	<p>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。</p>

## 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。

### Before you begin

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。

### Procedure

	Command or Action	Purpose
ステップ 1	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>switch# configure terminal switch(config)#</pre>	<p>グローバルコンフィギュレーションモードを開始します。</p>

	Command or Action	Purpose
ステップ 2	次のいずれかのコマンドを入力します。  <ul style="list-style-type: none"> <li>• <b>interface ethernet slot/port</b></li> <li>• <b>interface port-channel channel-number</b></li> </ul> <b>Example:</b> <pre>switch(config)# interface ethernet 2/1 switch(config-if) #</pre>	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	<b>[no] switchport port-security aging type {absolute   inactivity}</b>  <b>Example:</b> <pre>switch(config-if) # switchport port-security aging type inactivity</pre>	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。 <b>no</b> 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	<b>[no] switchport port-security aging time minutes</b>  <b>Example:</b> <pre>switch(config-if) # switchport port-security aging time 120</pre>	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。 <i>minutes</i> の最大値は 1440 です。 <b>no</b> 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。  <b>Note</b> Cisco Nexus 9200 および 9300-EX シリーズ スイッチの場合、設定されたエージング タイムに最大 2 分が追加されることがあります。たとえば、エージングタイムを 10 分に設定すると、エージアウトはトラフィックが停止してから 10 ~ 12 分後に発生します。
ステップ 5	(Optional) <b>show running-config port-security</b>  <b>Example:</b> <pre>switch(config-if) # show running-config port-security</pre>	ポートセキュリティの設定を表示します。
ステップ 6	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch(config-if) # copy running-config startup-config</pre>	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。

### Before you begin

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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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。 <ul style="list-style-type: none"> <li>• <b>interface ethernet</b> <i>slot/port</i></li> <li>• <b>interface port-channel</b> <i>channel-number</i></li> </ul> <b>Example:</b> <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	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	<b>[no] switchport port-security violation {protect   restrict   shutdown}</b> <b>Example:</b> <pre>switch(config-if)# switchport port-security violation restrict</pre>	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。 <b>no</b> 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	(Optional) <b>show running-config port-security</b> <b>Example:</b> <pre>switch(config-if)# show running-config port-security</pre>	ポートセキュリティの設定を表示します。
ステップ 5	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch(config-if)# copy running-config startup-config</pre>	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。

コマンド	目的
<code>show running-config port-security</code>	ポートセキュリティの設定を表示します。
<code>show port-security</code>	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。
<code>show port-security interface</code>	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。
<code>show port-security address</code>	セキュア MAC アドレスを表示します。
<code>show vpc consistency-parameters vpc id</code>	両方の vPC ピアの設定を確認します。

## 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。

## 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
```

## vPC ドメインでのポートセキュリティの設定例

次に、vPC ドメインで vPC ピア上のポートセキュリティをイネーブルにして設定する例を示します。最初のスイッチがプライマリ vPC ピアであり、2 番目のスイッチがセカンダリ vPC ピアです。スイッチでポートセキュリティを設定する前に、vPC ドメインを作成し、vPC ピアリンク隣接関係が確立されていることを確認します。

## 例：孤立ポートでのポートセキュリティの設定

```

primary_switch(config)# feature port-security
primary_switch(config-if)# int e1/1
primary_switch(config-if)# switchport port-security
primary_switch(config-if)# switchport port-security max 1025
primary_switch(config-if)# switchport port-security violation restrict
primary_switch(config-if)# switchport port-security aging time 4
primary_switch(config-if)# switchport port-security aging type absolute
primary_switch(config-if)# switchport port-security mac sticky
primary_switch(config-if)# switchport port-security mac-address 0.0.1 vlan 101
primary_switch(config-if)# switchport port-security mac-address 0.0.2 vlan 101
primary_switch(config-if)# copy running-config startup-config

secondary_switch(config)# feature port-security
secondary_switch(config)# int e3/1
secondary_switch(config-if)# switchport port-security
secondary_switch(config-if)# switchport port-security max 1025
secondary_switch(config-if)# switchport port-security violation restrict
secondary_switch(config-if)# switchport port-security aging time 4
secondary_switch(config-if)# switchport port-security aging type absolute
secondary_switch(config-if)# switchport port-security mac sticky
secondary_switch(config-if)# switchport port-security mac-address 0.0.1 vlan 101
secondary_switch(config-if)# switchport port-security mac-address 0.0.2 vlan 101
secondary_switch(config-if)# copy running-config startup-config

```

## 例：vPC レッグ上のポートセキュリティの設定

```

primary_switch(config)# feature port-security
primary_switch(config-if)# int po10
primary_switch(config-if)# switchport port-security
primary_switch(config-if)# switchport port-security max 1025
primary_switch(config-if)# switchport port-security violation restrict
primary_switch(config-if)# switchport port-security aging time 4
primary_switch(config-if)# switchport port-security aging type absolute
primary_switch(config-if)# switchport port-security mac sticky
primary_switch(config-if)# switchport port-security mac-address 0.0.1 vlan 101
primary_switch(config-if)# switchport port-security mac-address 0.0.2 vlan 101
primary_switch(config-if)# vpc 10
primary_switch(config-if)# copy running-config startup-config

secondary_switch(config)# feature port-security
secondary_switch(config)# int po10
secondary_switch(config-if)# switchport port-security
secondary_switch(config-if)# switchport port-security max 1025
secondary_switch(config-if)# switchport port-security violation restrict
secondary_switch(config-if)# switchport port-security aging time 4
secondary_switch(config-if)# switchport port-security aging type absolute
secondary_switch(config-if)# switchport port-security mac sticky
secondary_switch(config-if)# switchport port-security mac-address 0.0.1 vlan 101
secondary_switch(config-if)# switchport port-security mac-address 0.0.2 vlan 101
secondary_switch(config-if)# vpc 10
secondary_switch(config-if)# copy running-config startup-config

```

## 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 9000 Series NX-OS Layer 2 Switching Configuration Guide』

### 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
<ul style="list-style-type: none"><li>• CISCO-PORT-SECURITY-MIB</li></ul> <p><b>Note</b>    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。</p>	<p>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。</p> <p><a href="http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml">http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml</a> [英語]</p>







## 第 16 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。

- [DHCP スヌーピングについて, on page 446](#)
- [DHCP リレー エージェントについて \(450 ページ\)](#)
- [DHCPv6 リレー エージェントについて \(453 ページ\)](#)
- [DHCP クライアントについて \(454 ページ\)](#)
- [DHCP の前提条件, on page 454](#)
- [DHCP の注意事項と制約事項 \(454 ページ\)](#)
- [DHCP のデフォルト設定, on page 456](#)
- [DHCP の設定, on page 457](#)
- [DHCPv6 の設定 \(479 ページ\)](#)
- [DHCP クライアントのイネーブル化 \(486 ページ\)](#)
- [UDP リレーの設定 \(488 ページ\)](#)
- [DHCP 設定の確認, on page 492](#)
- [IPv6 RA ガードの統計情報の表示 \(493 ページ\)](#)
- [DHCP スヌーピング バインディングの表示, on page 493](#)
- [DHCP スヌーピング バインディング データベースのクリア \(493 ページ\)](#)
- [DHCP のモニタリング \(494 ページ\)](#)
- [DHCP スヌーピング統計情報のクリア \(494 ページ\)](#)
- [DHCP リレー統計情報のクリア \(494 ページ\)](#)
- [DHCPv6 リレー統計情報のクリア \(494 ページ\)](#)
- [DHCP の設定例, on page 494](#)
- [DHCP クライアントの設定例 \(495 ページ\)](#)
- [DHCP に関する追加情報, on page 496](#)

## DHCP スヌーピングについて

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。



**Note** 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。

**Note**

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。

## 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ク 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。この問題は Cisco Fabric Service over Ethernet (CFS over Ethernet) 分散を使用して、すべての DHCP パケット (要求および応答) が両方のスイッチに確実に認識されるようにすることで対処されます。これにより、vPC リンクの背後に存在するすべてのクライアントについて、両方のスイッチで同じバインディング エントリが作成および管理されるようになります。

CFS over Ethernet 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 DHCP OFFER 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。**ip dhcp packet strict-validation** コマンドを使用して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。

## DHCP Option 82

DHCP Option 82 is used to convey information about the DHCP client's location in the network. The information is contained in the DHCP Option 82 field, which is a list of IP addresses and MAC addresses. The information is used by the DHCP server to determine the IP address to assign to the client.

Cisco NX-OS DHCP Option 82 configuration

1. DHCP Option 82 configuration
2. Cisco NX-OS DHCP Option 82 configuration Option 82 MAC ID ? vlan-ifindex? vPC vlan-vpcid?vPC ID ?



Note

vPC ID vPC MAC MAC vPC ID Option 82 DHCP vPC ID

- 3. Option 82 DHCP DHCP
- 4. DHCP Option 82 ID ID IP DHCP Option 82
- 5. DHCP Cisco NX-OS Cisco NX-OS ID ID Option 82 Cisco NX-OS Option 82 DHCP DHCP

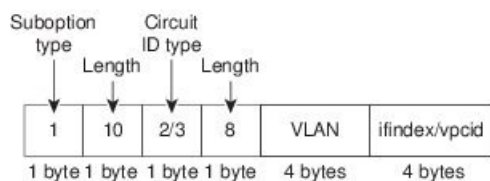
Option 82

- ID
- 
- 
- ID
- ID
- ID
- 
- 
- ID
- ID

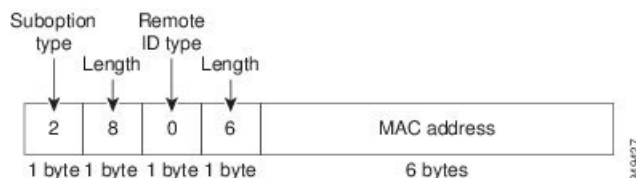
ID ID Cisco NX-OS DHCP Option 82 ID

Figure 9: ??????????????

## Circuit ID Suboption Frame Format



## Remote ID Suboption Frame Format



## DHCP リレー エージェントについて

## 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。



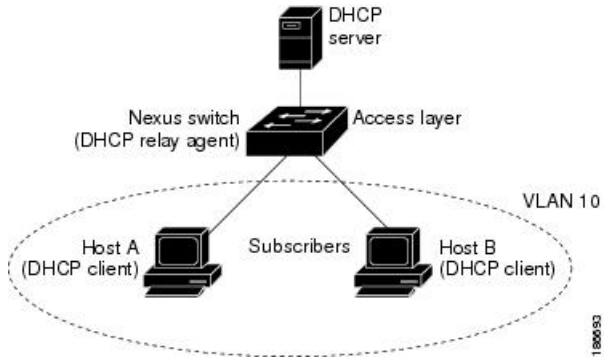
**Note** デバイスは、Option 82 情報がすでに含まれている DHCP 要求を中継するときには、Option 82 情報を変更せずに元のままの状態ですべての要求と一緒に転送します。

## DHCP ??? ??????? Option 82

??? ?????????????? DHCP ??????? Option 82 ??

Figure 10: ?????? ?????? ?????????? DHCP ??? ??????

?????????? ?????? ?????????????? ??????????????????????DHCP ??? IP ?????????????????? DHCP  
????????????????????? DHCP ?????????? IP ??????????????????????DHCP ??? ???????????  
?????????????????????DHCP ??????????????



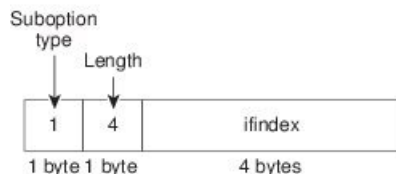
Cisco NX-OS ?????? DHCP ??? ?????? Option 82 ?????????????????????????????????

1. ???DHCP ?????? DHCP ?????????????????????????????????
2. Cisco NX-OS ?????? DHCP ?????????????????? Option 82 ??????????Option 82 ?????????? MAC  
????????? ID ?????????????? ID ? ifindex?? VXLAN VLAN ?????? vn-segment-id-mod-port?VXLAN  
VLAN ?????????????????????????????????? ID ??????????DHCP ?????????? ID ??DHCP ???????????  
SVI ?????? 3 ?????????? ifindex ??????????
3. ?????DHCP ????????? ?????????? IP ??????????????
4. ?????Option 82 ?????????? DHCP ??? DHCP ??????????????
5. DHCP ??????????????????Option 82 ?????????????????????????? ID??? ID?????????????????IP  
??? ID ?????? ID ?????????????? IP ??????????????????????DHCP  
?????DHCP ???? Option 82 ??????????????????
6. Cisco NX-OS ??????????????????????DHCP ?????? NX-OS ??????????????????????Cisco NX-OS  
?????????????ID ??????????????????????ID ?????????????????????? Option 82  
???Cisco NX-OS ?????? Option 82 ??????????????????DHCP ??????? DHCP  
???

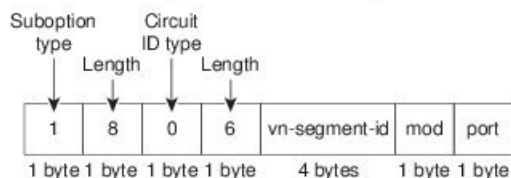
????????? ID ?????????????????? ID ??????????????????????????????

Figure 11: ??????????????

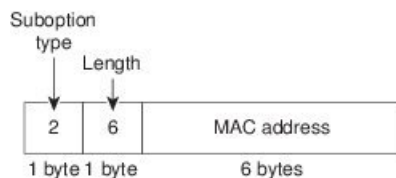
## Circuit ID Suboption Frame Format (for non-VXLAN VLANs)



## Circuit ID Suboption Frame Format (for VXLAN VLANs)



## Remote ID Suboption Frame Format



9-63426

## 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 9000 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。

## 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。

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。

## DHCPv6 リレー エージェントについて

### 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 9000 Series NX-OS Unicast Routing Configuration Guide』を参照してください。

## DHCP クライアントについて

DHCP クライアント機能によって、インターフェイスに IPv4 または IPv6 アドレスを設定できます。インターフェイスには、ルーテッドポート、管理ポート、スイッチ仮想インターフェイス (SVI) が含まれます。

## 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。

- POAP の安全性を確保するために、DHCP スヌーピングが有効であることを確認し、ファイアウォールルールを設定して意図しない、または悪意のある DHCP サーバをブロックしてください。
- Cisco Nexus 9000 シリーズスイッチは、bootp パケットのリレーをサポートしていません。ただし、スイッチはレイヤ 2 スイッチの bootp パケットをサポートします。
- DHCP サブネット ブロードキャストはサポートされていません。
- 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。
- 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。

- ネットワークで DHCP スヌーピングの後に DHCP リレーが続くことはできません (DHCP スヌーピングは、同じ Nexus デバイスで DHCP リレーが設定されている場合機能しません)。
- **ip dhcp snooping** コマンドは、N9K-X9636C-R、N9K-X9636C-RX、および N9K-X9636Q-R ラインカードおよび Cisco Nexus 34180YC スイッチを搭載した Cisco Nexus 9500 プラットフォーム スイッチではサポートされません。
- DHCP スヌーピングは VXLAN VLAN ではサポートされません。
- DHCP スヌーピングは、同じ MAC アドレスと VLAN をスタティック バインディング エントリに持つ複数の IP アドレスをサポートします。
- デフォルト VRF を使用して DHCP サーバが到達可能である場合、VXLAN は DHCP リレーをサポートします。
- 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 クライアントおよびサーバが異なる VRF 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。
- 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 リンク内のスイッチ間で 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。
- DHCP スマート リレーは、イネーブルであるインターフェイスの IP アドレスのうち、最初の 100 個に制限されます。
- DHCP スマート リレーを使用するには、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。
- 番号が付けられないインターフェイスで DHCP リレーを使用する場合は、オプション 82 を挿入するようにスイッチを設定する必要があります。
- DHCP クライアント機能には、次の注意事項と制約事項が適用されます。

- SVIは複数の設定が可能ですが、各インターフェイス VLAN は異なるサブネットにある必要があります。DHCP クライアント機能では、同一デバイスの異なるインターフェイス VLAN にある同じサブネットを使った異なる IP アドレスの設定はできません。
- DHCP クライアントおよび DHCP リレーは、同一のスイッチ上ではサポートされません。
- DHCP クライアントはレイヤ 3 のサブインターフェイスではサポートされません。
- Cisco Nexus 9300 シリーズ スイッチおよび Cisco Nexus 9500 シリーズ スイッチでは、DHCP クライアントがサポートされています。
- DHCP クライアントは、N9K-X9636C-R、N9K-X9636C-RX、N9K-X9636Q-R、および N9K-X96136YC-R ラインカードを搭載した Cisco Nexus 9500 プラットフォームスイッチではサポートされません。
- Cisco NX-OS リリース 9.3(3) 以降、DHCP スヌーピングおよび DHCP リレーは Cisco Nexus 9364C-GX、Cisco Nexus 9316D-GX、および Cisco Nexus 93600CD-GX スイッチでサポートされています。



(注) DHCP 設定制限については、『Cisco Nexus 9000 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。

Table 37: 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

パラメータ	デフォルト
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
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
リレー エージェントの DHCP Option 82	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

#### Procedure

**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** (Optional) DHCP リレー エージェントをイネーブルにします。

**ステップ 6** (Optional) DHCP サーバとクライアントが異なる VRF 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 7 (Optional) 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。

## 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の場合、DHCP リレー エージェント、DHCP スヌーピング、および DHCP に依存するすべての機能は設定できません。また、すべての DHCP 設定がデバイスから削除されます。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	<b>[no] feature dhcp</b> <b>Example:</b> 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。
ステップ 3	(Optional) <b>show running-config dhcp</b> <b>Example:</b> switch(config)# show running-config dhcp	DHCP 設定を表示します。
ステップ 4	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> 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。

## DHCP スヌーピングの設定

### 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。

**Before you begin**

DHCP 機能がイネーブルになっていることを確認します。

**Procedure**

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	<b>[no] ip dhcp snooping</b> <b>Example:</b> 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。このコマンドの <b>no</b> 形式を使用すると、DHCP スヌーピングがディセーブルになります。
ステップ 3	(Optional) <b>show running-config dhcp</b> <b>Example:</b> switch(config)# show running-config dhcp	DHCP 設定を表示します。
ステップ 4	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> 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。

**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。

**Before you begin**

DHCP 機能がイネーブルにされていることを確認します。

**Note**

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。

## Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	<b>[no] ip dhcp snooping vlan <i>vlan-list</i></b> <b>Example:</b> switch(config)# ip dhcp snooping vlan 100,200,250-252	<i>vlan-list</i> で指定する VLAN の DHCP スヌーピングをイネーブルにします。このコマンドの <b>no</b> 形式を使用すると、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	(Optional) <b>show running-config dhcp</b> <b>Example:</b> switch(config)# show running-config dhcp	DHCP 設定を表示します。
ステップ 4	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> 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。

## 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。

## Before you begin

DHCP 機能がイネーブルにされていることを確認します。

## Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	<b>[no] ip dhcp snooping verify mac-address</b> <b>Example:</b>	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。このコマンド



	Command or Action	Purpose
	<code>switch(config)# ip dhcp snooping verify mac-address</code>	の <b>no</b> 形式を使用すると、MAC アドレス検証がディセーブルになります。
ステップ 3	(Optional) <b>show running-config dhcp</b>  <b>Example:</b> <code>switch(config)# show running-config dhcp</code>	DHCP 設定を表示します。
ステップ 4	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <code>switch(config)# copy running-config startup-config</code>	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。

## 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。



**Note** 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。



**Note** 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。



**Note** Option82 はコマンドコンフィギュレーションのフォーマット文字列で指定されているように追加する必要があります。

- Option82 文字列の長さは、フォーマット文字列の長さに応じて長くなります。
- 回線 ID には、フォーマット文字列の ASCII 値を含める必要があります。

### Before you begin

DHCP 機能がイネーブルにされていることを確認します。

## Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>[no] ip dhcp snooping information option</b> <b>Example:</b> <pre>switch(config)# ip dhcp snooping information option</pre>	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。このコマンドの <b>no</b> 形式を使用すると、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	<b>(Optional) [no] ip dhcp option82 sub-option circuit-id format_type string format</b> <b>Example:</b> <pre>switch(config)# ip dhcp snooping sub-option circuit-id format-type string format</pre> <b>Example:</b> <pre>switch(config)# ip dhcp snooping sub-option circuit-id format-type string format? WORD Format string (Max Size 64)</pre>	<p>Option 82 を次のように設定します。</p> <ul style="list-style-type: none"> <li>• <i>format-type</i> を指定しない場合には、<i>circuit-id</i> には入力ポートが表示されます。たとえば <i>ethernet1/1</i> のようになります。</li> <li>• フォーマットで <i>&lt;word&gt;</i> を指定すると、<i>circuit-id</i> には指定した単語が表示されます。</li> <li>• <i>%h</i> を (<i>&lt;word&gt;</i> の代わりに) 指定すると、<i>circuit-id</i> にはホスト名が表示されます。</li> <li>• <i>%p</i> を (<i>&lt;word&gt;</i> の代わりに) 指定すると、<i>circuit-id</i> にはポート名が表示されます。</li> <li>• <i>%h:%p</i> を (<i>&lt;word&gt;</i> の代わりに) 指定すると、<i>circuit-id</i> にはホストとポート両方の名前が表示されます。</li> </ul> <p><b>Note</b> <i>no</i> 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。</p>
ステップ 4	<b>interface interface slot/port</b> <b>Example:</b> <pre>switch(config)# interface ethernet 2/2 switch(config-if)#</pre>	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、スヌーピング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。

	Command or Action	Purpose
ステップ 5	<p>(Optional) <b>ip dhcp option82 sub-option circuit-id</b></p> <p><b>Example:</b></p> <pre>switch(config-if)# ip dhcp option82 sub-option circuit-id? WORD Format string (Max Size 64)</pre> <p><b>Example:</b></p> <pre>switch(config-if)# ip dhcp option82 sub-option circuit-id test switch(config-if)#</pre>	<p>インターフェイスでオプション 82 を設定します。</p> <p><b>Note</b> <i>no</i> 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。</p>
ステップ 6	<p><b>exit</b></p> <p><b>Example:</b></p> <pre>switch(config-if)# exit switch(config)#</pre>	<p>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。</p>
ステップ 7	<p>(Optional) <b>show ip dhcp option82 info interface intf_name</b></p>	<p>DHCP 設定を表示します。そのインターフェイスで <b>option82</b> が有効か無効か、および <b>option82</b> が有効になっているインターフェイスの送信パケットが表示されます。</p>
ステップ 8	<p>(Optional) <b>show running-config dhcp</b></p> <p><b>Example:</b></p> <pre>switch(config)# show running-config dhcp</pre>	<p>DHCP 設定を表示します。</p>
ステップ 9	<p>(Optional) <b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch(config)# copy running-config startup-config</pre>	<p>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。</p>

## 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。

### Procedure

	Command or Action	Purpose
ステップ 1	<p><b>configure terminal</b></p> <p><b>Example:</b></p> <pre>switch# configure terminal switch(config)#</pre>	<p>グローバル コンフィギュレーションモードを開始します。</p>

	Command or Action	Purpose
ステップ 2	<b>[no] ip dhcp packet strict-validation</b> <b>Example:</b> 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。このコマンドの <b>no</b> 形式を使用すると、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	(Optional) <b>show running-config dhcp</b> <b>Example:</b> switch(config)# show running-config dhcp	DHCP 設定を表示します。
ステップ 4	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> 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。

## 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

### Before you begin

DHCP 機能がイネーブルにされ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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	次のいずれかのオプションを使用します。  <ul style="list-style-type: none"> <li>• <b>interface ethernet slot/port</b></li> <li>• <b>interface port-channel channel-number</b></li> </ul> <b>Example:</b>	<ul style="list-style-type: none"> <li>• 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。 <i>slot/port</i> は、DHCP スヌーピングで <b>trusted</b> または <b>untrusted</b> 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。</li> </ul>

	Command or Action	Purpose
	<pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	<ul style="list-style-type: none"> <li>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。 <i>slot/port</i> は、DHCP スヌーピングで <b>trusted</b> または <b>untrusted</b> 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。</li> </ul>
ステップ3	<p><b>[no] ip dhcp snooping trust</b></p> <p><b>Example:</b></p> <pre>switch(config-if)# ip dhcp snooping trust</pre>	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。このコマンドの <b>no</b> 形式を使用すると、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	<p>(Optional) <b>show running-config dhcp</b></p> <p><b>Example:</b></p> <pre>switch(config-if)# show running-config dhcp</pre>	DHCP 設定を表示します。
ステップ5	<p>(Optional) <b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch(config-if)# copy running-config startup-config</pre>	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 リレー信頼ポート機能のイネーブル化またはディセーブル化

DHCP リレー信頼ポート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** コマンドをグローバルに設定すると、ゲートウェイアドレスがすべてゼロに設定された場合、DHCP リレー エージェントはパケットを廃棄します。

### 始める前に

DHCP 機能がイネーブルにされていることを確認します。

### 手順

	コマンドまたはアクション	目的
ステップ1	<p><b>configure terminal</b></p> <p>例 :</p> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>[no] ip dhcp relay information option trust</b> 例： switch(config)# ip dhcp relay information option trust	DHCP リレー信頼ポートの機能を有効にします。このコマンドの <b>no</b> 形式を使用すると、この機能がディセーブルになります。
ステップ 3	(任意) <b>show ip dhcp relay</b> 例： switch(config)# show ip dhcp relay	DHCP リレーの設定を表示します。
ステップ 4	(任意) <b>show ip dhcp relay information trusted-sources</b> 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 5	(任意) <b>show running-config dhcp</b> 例： switch(config)# show running-config dhcp	DHCP 設定を表示します。
ステップ 6	(任意) <b>copy running-config startup-config</b> 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。

## インターフェイスの DHCP リレー信頼または非信頼ポートとしての設定

レイヤ 3 インターフェイスは、DHCP リレー信頼または非信頼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に設定できます。

- 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 チャンネル インターフェイス

### 始める前に

DHCP 機能がイネーブルにされていることを確認します。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>interface [ethernet slot/port[.number]   port-channel channel-number]</b> 例 : <pre>switch(config)# interface ethernet 2/1 switch(config-if)#</pre>	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。ここでは <i>slot/port</i> に <b>trusted</b> または <b>untrusted</b> に設定するレイヤ 3 イーサネット インターフェイスを指定するか、あるいは <i>channel-number</i> に <b>trusted</b> または <b>untrusted</b> に設定するレイヤ 3 ポート チャネル インターフェイスを指定できます。
ステップ 3	<b>[no] ip dhcp relay information trusted</b> 例 : <pre>switch(config-if)# ip dhcp relay information trusted</pre>	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。このコマンドの <b>no</b> 形式を使用すると、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。  (注) どのレイヤ 3 インターフェイスも、グローバル コマンドまたはインターフェイス レベルのコマンドを使用して信頼できるインターフェイスとして設定した場合、そのインターフェイスは信頼できるインターフェイスと見なされません。そのため、ポートを信頼させるコマンドをグローバル レベルでイネーブルにした場合、インターフェイス レベルの設定に関係なく、どのレイヤ 3 インターフェイスも非信頼とは見なされなくなります。
ステップ 4	(任意) <b>show ip dhcp relay information trusted-sources</b> 例 : <pre>switch(config-if)# show ip dhcp relay information trusted-sources</pre>	DHCP リレー信頼ポート設定を表示します。

	コマンドまたはアクション	目的
ステップ 5	(任意) <b>show running-config dhcp</b> 例： switch(config-if)# show running-config dhcp	DHCP 設定を表示します。
ステップ 6	(任意) <b>copy running-config startup-config</b> 例： switch(config-if)# 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。

## 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インターフェイスは、DHCP リレー信頼または非信頼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に設定できます。

- 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

**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の設定に関係なく、どのレイヤ3インターフェイスも非信頼とは見なされなくなります。

### 始める前に

DHCP 機能がイネーブルにされていることを確認します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>[no] ip dhcp relay information trust-all</b> 例： switch(config)# ip dhcp relay information trust-all	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。このコマンドの <b>no</b> 形式を使用すると、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	(任意) <b>show ip dhcp relay information trusted-sources</b> 例：	DHCP リレー信頼ポート設定を表示します。



	コマンドまたはアクション	目的
	<code>switch(config)# show ip dhcp relay information trusted-sources</code>	
ステップ 4	(任意) <b>show running-config dhcp</b> 例： <code>switch(config)# show running-config dhcp</code>	DHCP 設定を表示します。
ステップ 5	(任意) <b>copy running-config startup-config</b> 例： <code>switch(config)# copy running-config startup-config</code>	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。

### Before you begin

DHCP 機能がイネーブルになっていることを確認します。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <code>switch# configure terminal</code> <code>switch(config)#</code>	グローバル 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	<b>[no] ip dhcp relay</b> <b>Example:</b> <code>switch(config)# ip dhcp relay</code>	DHCP リレー エージェントをイネーブルにします。 <b>no</b> オプションを使用すると、DHCP 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	(Optional) <b>show ip dhcp relay</b> <b>Example:</b> <code>switch(config)# show ip dhcp relay</code>	DHCP リレーの設定を表示します。
ステップ 4	(Optional) <b>show running-config dhcp</b> <b>Example:</b> <code>switch(config)# show running-config dhcp</code>	DHCP 設定を表示します。

	Command or Action	Purpose
ステップ 5	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	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。

### Before you begin

DHCP 機能がイネーブルになっていることを確認します。

### Procedure

	Command or Action	Purpose
ステップ 1	switch# <b>configure terminal</b>	グローバル 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)# <b>[no] ip dhcp relay information option</b>	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。 <b>no</b> 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	(Optional) switch(config)# <b>[no] ip dhcp relay sub-option circuit-id customized</b>	VLAN+スロット+ポート形式で Option 82 をプログラムします。このコマンドは、SVIにのみ適用されます。 <b>no</b> 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	(Optional) switch(config)# <b>[no] ip dhcp relay sub-option circuit-id format-type string</b>	デフォルトの ifIndex バイナリ形式の代わりに、符号化されたストリング形式を使用するよう Option 82 を設定します。 <b>no</b> 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。

	Command or Action	Purpose
		<p>VLAN および SVI の場合 :</p> <ul style="list-style-type: none"> <li>• このコマンドと <b>ip dhcp relay sub-option circuit-id</b> カスタマイズコマンドの両方を設定すると、<b>ip dhcp relay sub-option circuit-id format-type string</b> コマンドがプログラムされます。</li> <li>• <b>ip dhcp relay sub-option circuit-id format-type string</b> コマンドを削除すると、<b>ip dhcp relay sub-option circuit-id</b> カスタマイズコマンドがプログラムされます。</li> <li>• 両方のコマンドが削除されると、<b>ifindex</b> がプログラムされます。</li> </ul> <p>他のインターフェイスでは、<b>ip dhcp relay sub-option circuit-id format-type string</b> コマンドが設定されている場合は、それが使用されます。それ以外の場合は、デフォルトの <b>ifindex</b> がプログラムされます。</p>
ステップ 5	(Optional) switch(config)# <b>show ip dhcp relay</b>	DHCP リレーの設定を表示します。
ステップ 6	(Optional) switch(config)# <b>show running-config dhcp</b>	DHCP 設定を表示します。
ステップ 7	(Optional) switch(config)# <b>copy running-config startup-config</b>	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 の DHCP 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。

### 始める前に

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

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>[no] ip dhcp relay information option vpn</b> 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。 <b>no</b> 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	<b>[no] ip dhcp relay sub-option type cisco</b> 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。 <b>no</b> 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	(任意) <b>show ip dhcp relay</b> 例： switch(config)# show ip dhcp relay	DHCP リレーの設定を表示します。
ステップ 5	(任意) <b>show running-config dhcp</b> 例： switch(config)# show running-config dhcp	DHCP 設定を表示します。
ステップ 6	(任意) <b>copy running-config startup-config</b> 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。

## DHCP Server Identifier オーバーライド サブオプション

Cisco NX-OS リリース 9.3(3) 以降では、サーバ ID オーバーライド オプションを無効にできません。このオプションは、DHCP リレー VPN 設定または送信元インターフェイス設定の DHCP オプション 82 パケットにはデフォルトで追加されます。

**始める前に**

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**

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 : switch# <b>configure terminal</b>	グローバル 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	<b>[no] ip dhcp relay information option server-id-override-disable</b> 例 : switch(config)# <b>ip dhcp relay information option server-id-override-disable</b>	DHCP オプション 82 パケットのサーバ ID オーバーライド オプションを無効にします。  (注) このコマンドの <b>no</b> 形式を使用すれば、サーバ ID オーバーライド オプションを再度有効にできます。

## 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。

**Before you begin**

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 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。

**Note**

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。

## Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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。 <ul style="list-style-type: none"> <li>• <b>interface ethernet slot/port[.number]</b></li> <li>• <b>interface vlan vlan-id</b></li> <li>• <b>interface port-channel channel-id[.subchannel-id]</b></li> </ul> <b>Example:</b> <pre>switch(config)# interface ethernet 2/3 switch(config-if)#</pre>	<ul style="list-style-type: none"> <li>• 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。 <i>slot/port</i> 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、<i>number</i> 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。</li> <li><b>Note</b> ポートチャネルのサブインターフェイスは Cisco NX-OS リリース 6.1(2)I3(3) および 6.1(2)I3(3a) でのみサポートされます。Cisco NX-OS リリース 9.2(1) ではサポートされていません。</li> <li>• 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。 <i>vlan-id</i> は、DHCP サーバ IP アドレスを設定する VLAN の ID です。</li> <li>• 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。 <i>channel-id</i> 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、<i>subchannel-id</i> 引数を使用してサブチャネル ID を指定します。</li> </ul>
ステップ 3	<b>ip dhcp relay address IP-address [use-vrf vrf-name]</b> <b>Example:</b> <pre>switch(config-if)# ip dhcp relay address 10.132.7.120 use-vrf red</pre>	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。

	Command or Action	Purpose
		複数の IP アドレスを設定するには、アドレスごとに <b>ip dhcp relay address</b> コマンドを使用します。
ステップ 4	(Optional) <b>show ip dhcp relay address</b>  <b>Example:</b> switch(config-if)# show ip dhcp relay address	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	(Optional) <b>show running-config dhcp</b>  <b>Example:</b> switch(config-if)# show running-config dhcp	DHCP 設定を表示します。
ステップ 6	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> switch(config-if)# 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。

## DHCP リレー送信元インターフェイスの設定

DHCP 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、DHCP 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。

### 始める前に

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

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  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	<b>[no] ip dhcp relay source-interface interface</b>  例：	DHCP 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。

	コマンドまたはアクション	目的
	<code>switch(config)# ip dhcp relay source-interface loopback 2</code>	(注) DHCP 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	(任意) <code>show ip dhcp relay [ interface interface]</code> 例： <code>switch(config)# show ip dhcp relay</code>	DHCP リレーの設定を表示します。
ステップ 4	(任意) <code>show running-config dhcp</code> 例： <code>switch(config)# show running-config dhcp</code>	DHCP 設定を表示します。
ステップ 5	(任意) <code>copy running-config startup-config</code> 例： <code>switch(config)# copy running-config startup-config</code>	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 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。

### Before you begin

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。



## Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	<b>[no] ip dhcp smart-relay global</b> <b>Example:</b> 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。このコマンドの <b>no</b> 形式を使用すると、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	(Optional) <b>show ip dhcp relay</b> <b>Example:</b> switch(config)# show ip dhcp relay	DHCP スマート リレー設定を表示します。
ステップ 4	(Optional) <b>show running-config dhcp</b> <b>Example:</b> switch(config)# show running-config dhcp	DHCP 設定を表示します。
ステップ 5	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> 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。

## 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。

### Before you begin

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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b>	グローバル コンフィギュレーション モードを開始します。

	Command or Action	Purpose
	switch# configure terminal switch(config)#	
ステップ 2	<b>interface</b> <i>interface slot/port</i>  <b>Example:</b> 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。 <i>slot/port</i> 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	<b>[no] ip dhcp smart-relay</b>  <b>Example:</b> 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。このコマンドの <b>no</b> 形式を使用すると、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	<b>exit</b>  <b>Example:</b> 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	<b>exit</b>  <b>Example:</b> 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	(Optional) <b>show ip dhcp relay</b>  <b>Example:</b> switch# show ip dhcp relay	DHCP スマートリレー設定を表示します。
ステップ 7	(Optional) <b>show running-config dhcp</b>  <b>Example:</b> switch# show running-config dhcp	DHCP 設定を表示します。
ステップ 8	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> 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。

## DHCP リレー サブネット選択の設定

インターフェイスにプライマリ IP アドレスとセカンダリ IP アドレスの両方が含まれている場合、デフォルトでは、DHCP リレーはプライマリサブネットに基づいてサーバに IP アドレスの割り当てを要求します。DHCP リレーでセカンダリ IP アドレスを使用する場合は、DHCP スマートリレーを有効にする必要があります。スマートリレーを有効にすると、DHCP リレーは最初にプライマリサブネットの IP アドレスを要求します。プライマリサブネットの IP アド

レスを取得できない場合、セカンダリサブネットの IP アドレスを要求します。セカンダリサブネットの IP アドレスは、デフォルトでは選択されません。

DHCP リレーサブネット選択機能の導入により、要件に基づいてプライマリまたはセカンダリサブネットの IP アドレスを選択するオプションを利用できるようになりました。DHCP リレーサブネット選択を設定すると、DHCP リレーパケットには、送信元およびリレーエージェントのサブネット選択で使用されるサブネットの情報が含まれるようになります。VPN または送信元インターフェイスオプションがある場合、オプション 82 のリンク選択は、設定されたサブネットに基づいて更新されます。

DHCP スマートリレーとサブネット選択の設定は、インターフェイスレベルでは相互に排他的です。DHCP スマートリレーがグローバルに有効になっており、サブネット選択がインターフェイスレベルで設定されている場合は、インターフェイス設定が優先されます。

DHCP VPN または送信元インターフェイスオプションでは、DHCP サーバはオプション 82 のリンク選択を使用して IP アドレスを割り当てる必要があります。

### 始める前に

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

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： <pre>switch# configure terminal switch(config)#</pre>	グ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	<b>interface vlan <i>vlan-id</i></b> 例： <pre>switch(config)#interface vlan 3 switch(config-if)#</pre>	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	<b>ip dhcp relay subnet-selection <i>ip address</i></b> 例： <pre>switch(config-if)#ip dhcp relay subnet-selection 20.20.21.1</pre>	指定された IP アドレスの DHCP リレーサブネット選択を設定します。

## 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。

## 始める前に

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

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>[no] ipv6 dhcp relay</b> 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。 <b>no</b> 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	(任意) <b>show ipv6 dhcp relay [ interface interface]</b> 例： switch(config)# show ipv6 dhcp relay	DHCPv6 リレーの設定を表示します。
ステップ 4	(任意) <b>show running-config dhcp</b> 例： switch(config)# show running-config dhcp	DHCP 設定を表示します。
ステップ 5	(任意) <b>copy running-config startup-config</b> 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。

## 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。

## 始める前に

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

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>[no] ipv6 dhcp relay option vpn</b> 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。 <b>no</b> 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	<b>[no] ipv6 dhcp relay option type cisco</b> 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。 <b>no</b> 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	(任意) <b>show ipv6 dhcp relay [ interface interface]</b> 例 : switch(config)# show ipv6 dhcp relay	DHCPv6 リレーの設定を表示します。
ステップ 5	(任意) <b>show running-config dhcp</b> 例 : switch(config)# show running-config dhcp	DHCP 設定を表示します。
ステップ 6	(任意) <b>copy running-config startup-config</b> 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。

## 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 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 DHCPv6 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。

### 始める前に

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

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	次のいずれかのオプションを使用します。  • <b>interface ethernet slot/port</b> • <b>interface port-channel channel-id</b> 例： switch(config)# interface ethernet 2/3 switch(config-if)#	<ul style="list-style-type: none"> <li>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。 <i>slot/port</i> 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。</li> <li>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。 <i>channel-id</i> 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。</li> </ul>
ステップ 3	<b>[no] ipv6 dhcp relay address IPv6-address [use-vrf vrf-name] [interface interface]</b> 例：	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

	コマンドまたはアクション	目的
	<pre>switch(config-if)# ipv6 dhcp relay address FF02:1::FF0E:8C6C use-vrf red</pre>	<p>トを転送する DHCPv6 サーバの IP アドレスを設定します。</p> <p>サーバが異なる VRF 上にあり、もう 1 つの <b>interface</b> 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、<b>use-vrf</b> オプションを使用してサーバの VRF 名を指定します。</p> <p>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は、<b>interface</b> オプションは必須です。</p> <p>11-10-2016 07:36 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。</p> <p>複数の IP アドレスを設定するには、アドレスごとに <b>ipv6 dhcp relay address</b> コマンドを使用します。</p>
ステップ 4	<p>(任意) <b>show running-config dhcp</b></p> <p>例 :</p> <pre>switch(config-if)# show running-config dhcp</pre>	DHCPv6 設定を表示します。
ステップ 5	<p>(任意) <b>copy running-config startup-config</b></p> <p>例 :</p> <pre>switch(config-if)# copy running-config startup-config</pre>	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 オプション 79 のイネーブル化

Cisco NX-OS Release 9.3(3) 以降では、オプション 79 を使用して、DHCPv6 クライアントのリンク層アドレスの使用をイネーブル化できます。この機能をイネーブルにすると、スイッチはリレー転送パケットにオプション 79 を追加し、IPv6 クライアントのリンク層アドレスが、DHCPv6 パケットのオプションフィールドに挿入されます。

この機能は、通常の DHCPv6 と VXLAN を使用する DHCPv6 の両方でサポートされます。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# <b>configure terminal</b>	グローバル 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	<b>ipv6 dhcp relay option79</b> 例： switch(config)# <b>ipv6 dhcp relay option79</b>	DHCPv6 ホストのリンク層アドレスを伝送するために、リレーサーバから DHCP サーバに送信される DHCP リレー転送パケットをイネーブルにします。  このコマンドは、送信されるリレー転送パケットにのみ影響します。

## 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。

## 始める前に

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

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： switch# <b>configure terminal</b> 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	<b>[no] ipv6 dhcp relay source-interface interface</b> 例：	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。



	コマンドまたはアクション	目的
	<pre>switch(config)# ipv6 dhcp relay source-interface loopback 2</pre>	(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	(任意) <b>show ipv6 dhcp relay [ interface interface]</b> 例： <pre>switch(config)# show ipv6 dhcp relay</pre>	DHCPv6 リレーの設定を表示します。
ステップ 4	(任意) <b>show running-config dhcp show running-config dhcp</b> 例： <pre>switch(config)# show running-config dhcp</pre>	DHCP 設定を表示します。
ステップ 5	(任意) <b>copy running-config startup-config</b> 例： <pre>switch(config)# copy running-config startup-config</pre>	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 RA ガードの設定

Cisco Nexus 9200、9300、および 9300-EX シリーズ スイッチ および N9K-X9732C-EX ラインカードの IPv6 ルータ アドバタイズメント (RA) ガード機能を設定できます。この機能は、レイヤ 2 インターフェイス上のすべての着信 IPv6 RA パケットをドロップするために使用されます。

### 始める前に

DHCP を有効にする必要があります (**feature dhcp** コマンドを使用)。

インターフェイスで DHCP リレーを有効にするには、DHCP (ダイナミック IP アドレッシング) を使用して IPv4 または IPv6 アドレスが割り当てられているインターフェイスで DHCP を無効にする必要があります。

PTP (機能 **ptp**) と NV オーバーレイ (機能 **nv オーバーレイ**) の両方が設定されていないことを確認します。これらの機能が設定されると、ダイナミック ifacl ラベルが予約されます。た

だし、使用可能なダイナミック ifacl ラベル ビットは2つだけです。これらの機能の両方がすでに設定されている場合、IPv6 RA ガードにダイナミック ifacl ラベルを使用できず、機能を有効にできません。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>interface interface slot/port</b> 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。
ステップ 3	<b>[no] ipv6 nd raguard</b> 例： switch(config-if)# ipv6 nd raguard	指定したインターフェイスに IPv6 RA ガード機能を適用します。
ステップ 4	(任意) <b>copy running-config startup-config</b> 例： switch(config-if)# 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。

## DHCP クライアントのイネーブル化

DHCP クライアント機能を使用して、インターフェイスでの IPv4 または IPv6 アドレス設定をイネーブルにできます。インターフェイスには、ルーテッドポート、管理ポート、スイッチ仮想インターフェイス (SVI) が含まれます。レイヤ 3 サブインターフェイスはサポートされません。



(注) DHCP クライアントは DHCP リレーおよび DHCP スヌーピング プロセスに依存しないため、**feature dhcp** コマンドをイネーブルにする必要はありません。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 : <pre>switch# configure terminal switch(config)#</pre>	グローバル 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。 <ul style="list-style-type: none"> <li>• <b>interface ethernet slot/port</b></li> <li>• <b>interface mgmt 0</b></li> <li>• <b>interface vlan vlan-id</b></li> </ul> 例 : <pre>switch(config)# interface vlan 3 switch(config-if)#</pre>	<ul style="list-style-type: none"> <li>• 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。 <i>slot/port</i> は、DHCP クライアント機能をイネーブルにする物理イーサネット インターフェイスです。</li> <li>• インターフェイスコンフィギュレーション モードを開始して、DHCP クライアント機能をイネーブルにするインターフェイスとして管理インターフェイスを指定します。</li> <li>• 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。 <i>vlan-id</i> は、DHCP クライアント機能をイネーブルにする VLAN の ID です。</li> </ul>
ステップ 3	<b>ipv6 address use-link-local-only</b> 例 : <pre>switch(config-if)# ipv6 address use-link-local-only</pre>	このコマンドは、次の手順でインターフェイスに IPv6 アドレスを割り当てる前に入力する必要があります。インターフェイスに IPv4 アドレスを割り当てる場合、このコマンドは必要はありません。
ステップ 4	<b>[no] {ip   ipv6} address dhcp</b> 例 : <pre>switch(config-if)# ip address dhcp</pre>	このインターフェイスに IPv4 または IPv6 アドレスを割り当てます。 このコマンドの <b>no</b> 形式を使用すると、IP アドレスが解放されます。
ステップ 5	(任意) 次のいずれかのオプションを使用します。 <ul style="list-style-type: none"> <li>• <b>show running-config interface ethernet slot/port</b></li> <li>• <b>show running-config interface mgmt 0</b></li> <li>• <b>show running-config interface vlan vlan-id</b></li> </ul> 例 :	実行コンフィギュレーションにおいて、インターフェイスに割り当てられた IPv4 または IPv6 アドレスを表示します。

	コマンドまたはアクション	目的
	<pre>switch(config-if)# show running-config interface vlan 3</pre>	
ステップ 6	<p>(任意) <b>copy running-config startup-config</b></p> <p>例 :</p> <pre>switch(config-if)# copy running-config startup-config</pre>	<p>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。</p> <p><b>{ip   ipv6} address dhcp</b> コマンドだけが保存されます。割り当てられた IP アドレスは、実行コンフィギュレーションに表示されていても、保存されません。</p>

## UDP リレーの設定

### UDP リレーについて

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。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。

UDP リレー機能を有効にするには、**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。

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 チャンネル
- L3 サブインターフェイス

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 udpudp-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 リレーには、次の注意事項と制約事項があります。

- Cisco NX-OS リリース 9.3(5) 以降では、UDP リレーが N9K-X9736C-FX でサポートされています。
- UDP ポートは 1 ～ 65565 の範囲である必要があります。
- 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 UDP ポートをサポートします。
- おぶじえくとグループ名には最大 64 文字までの英数字を指定できます。
- DHCP と UDP リレーは共存できません。
- サブネットブロードキャストはサポートされていません。

## UDP リレーの設定

始める前に

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

---

### 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 forward-protocol udp**

例：

```
switch(config)# ip forward-protocol udp
```

UDP リレー機能をイネーブルにします。デフォルトでは、UDP 機能はディセーブルになっています。ただし、UDP ポートの定義済みセットではイネーブルになっています。

### ステップ 3 (任意) **[no] ip forward-protocol udp** *udp-port-number*

例：

```
switch(config)# ip forward-protocol udp 1
```

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。

(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 **[no] object-group udp relay ip address** *object-group-name*

例：

```
switch(config)# ip forward-protocol udp relay ip address relay1
```

パケットの転送先となる宛先 IP アドレスを設定します。

(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 5 **[no] {host host-addr| network-addr network-mask| network-addr/mask-length}**

例：

```
switch(config)# host 2.1.2.2 30.1.1.1 255.255.255.0 10.1.1.1./24
```

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。

(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 **exit**

例：

```
switch(config-udp-group)# exit
```

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 7 **interface ethernet** *slot/port*

例：

```
switch(config)# interface ethernet 1/1
```

オブジェクト **froup** をレイヤ 3 インターフェイスに対応付けます。

(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 **ip udp relay addrgroup** *object-group-name*

例：

```
switch(config-if)# ip udp relay addrgroup group1
```

オブジェクト `group` をインターフェイスに関連付けます。

#### ステップ 9 ip udp relay subnet-broadcast

例：

```
switch(config-if)# ip udp relay subnet-broadcast
```

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。

#### ステップ 10 exit

例：

```
switch(config-if)# exit
```

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。

## UDP リレーの設定例

この例では、実行中の設定を表示し、UDP リレーを設定します。

### 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。

```
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
```

## UDP リレーの設定の確認

UDP リレーの設定情報を表示するには、次のいずれかの操作を行います。

コマンド	目的
<b>show ip udp relay</b>	UDP リブレイ 設定を表示します。
<b>show ip udp relay interface</b> [{ <i>interface-type</i>   <i>interface-range</i> }]	インターフェイス レベル属性を表示します。

コマンド	目的
<code>show ip udp relay object-group</code>	設定済みのすべての UDP リレー オブジェクトグループ、および関連する IP アドレスを表示します。
<code>show ip udp relay object-group object-group-name</code>	オブジェクトグループ、および関連する IP アドレスを表示します。

## 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。

コマンド	目的
<code>show ip dhcp relay</code>	DHCP リレーの設定を表示します。
<code>show ipv6 dhcp relay [interface interface]</code>	DHCPv6 リレーのグローバル設定またはインターフェースレベルの設定を表示します。
<code>show ip dhcp relay address</code>	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。
<code>show ip dhcp snooping</code>	DHCP スヌーピングに関する一般的な情報を表示します。
<code>show running-config dhcp [all]</code>	実行コンフィギュレーション内の DHCP 設定を表示します。 <b>Note</b> <code>show running-config dhcp</code> コマンドは、 <code>ip dhcp relay</code> コマンドと <code>ipv6 dhcp relay</code> コマンドを表示しますが、これらはデフォルトで設定されています。
<code>show running-config interface {ethernet slot/port   mgmt 0   vlan vlan-id}</code>	DHCP クライアントがイネーブルの場合、インターフェースに割り当てられた IPv4 または IPv6 アドレスを表示します。
<code>show startup-config dhcp [all]</code>	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。



## IPv6 RA ガードの統計情報の表示

IPv6 RA ガード統計情報を表示または消去するには、次のいずれかの作業を実行します。

コマンド	目的
<code>show ipv6 raguard statistics</code>	IPv6 関連 RA ガードの統計情報を表示します。

次に、サンプルの統計情報例を示します。

```
switch# show ipv6 raguard statistics
-----
Interface      Rx          Drops
-----
Ethernet1/53   4561102    4561102
```

## DHCP スヌーピング バインディングの表示

`show ip dhcp snooping binding [ip-address | mac-address | dynamic | static | vlan vlan-id | interface interface-type interface-number]` を使用します コマンドを使用します。

```
MacAddress      IpAddress LeaseSec Type   VLAN Interface
-----
0f:00:60:b3:23:33 10.3.2.2  infinite static  13  Ethernet2/46
0f:00:60:b3:23:35 10.2.2.2  infinite static  100 Ethernet2/10
```

## 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 データベースからすべてのエントリをクリアするには、`clear ip dhcp snooping binding` コマンドを使用します。

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付けられたエントリをクリアするには、`clear ip dhcp snooping binding interface ethernet slot/port` コマンドを使用します。

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付けられたエントリをクリアするには、`clear ip dhcp snooping binding interface port-channel channel-number` コマンドを使用します。

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 VLAN エントリに関連付けられたエントリを 1 つだけクリアするには、`clear ip dhcp snooping binding vlan vlan-id [mac mac-address ip ip-address interface {ethernet slot /port | port-channel channel-number}]` 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。

DHCP リレーの統計情報をグローバルまたはインターフェイスレベルでモニタするには、**show ip dhcp relay statistics [interface interface]** コマンドを使用します。

DHCPv6 リレーの統計情報をグローバルまたはインターフェイスレベルでモニタするには、**show ipv6 dhcp relay statistics [interface interface]** コマンドを使用します。

## DHCP スヌーピング統計情報のクリア

**clear ip dhcp snooping statistics [vlan vlan-id]** コマンドを使用します。

## 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に関する DHCPv6 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。

**clear ip dhcp global statistics** を使用 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に関する 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 information 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 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 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
```

## DHCP クライアントの設定例

次に、DHCP クライアント機能を使用して VLAN インターフェイスに IPv4 アドレスを割り当てる例を示します。

```
switch# configure terminal
switch(config)# interface vlan 7
switch(config-if)# no shutdown
switch(config-if)# ip address dhcp
switch(config-if)# show running-config interface vlan 7
interface Vlan7
no shutdown
ip address dhcp
```

## 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
ダイナミック ARP インспекション (DAI)	『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』
IP ソース ガード	『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』
vPC	『Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide』
VRF およびレイヤ 3 のバーチャライゼーション	『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』

### 標準

標準	タイトル
RFC 2131	『Dynamic Host Configuration Protocol』 ( <a href="http://tools.ietf.org/html/rfc2131">http://tools.ietf.org/html/rfc2131</a> )
RFC 3046	『DHCP Relay Agent Information Option』 ( <a href="http://tools.ietf.org/html/rfc3046">http://tools.ietf.org/html/rfc3046</a> )
RFC 6607	『Virtual Subnet Selection Options for DHCPv4 and DHCPv6』 ( <a href="http://tools.ietf.org/html/rfc6607">http://tools.ietf.org/html/rfc6607</a> )
RFC 6939	DHCPv6 のクライアント リンク層アドレス オプション ( <a href="https://tools.ietf.org/html/rfc6939">https://tools.ietf.org/html/rfc6939</a> )



## 第 17 章

# IPv6 ファースト ホップ セキュリティの設 定

この章では、Cisco NX-OS デバイスで First Hop Security (FHS) 機能を設定する方法を説明します。

この章は、次の項で構成されています。

- [ファーストホップセキュリティについて \(497 ページ\)](#)
- [ファーストホップセキュリティの注意事項と制約事項 \(499 ページ\)](#)
- [vPC ファーストホップセキュリティ設定について, on page 499](#)
- [RA ガード \(503 ページ\)](#)
- [DHCPv6 ガード \(503 ページ\)](#)
- [IPv6 スヌーピング \(504 ページ\)](#)
- [IPv6 FHS の設定方法 \(506 ページ\)](#)
- [設定例 \(515 ページ\)](#)
- [IPv6 ファーストホップセキュリティに関する追加情報, on page 516](#)

## ファーストホップセキュリティについて

レイヤ2およびレイヤ3スイッチは、サーバ仮想化、オーバーレイトランスポート仮想化 (OTV)、レイヤ2モビリティなどのテクノロジーを使用して、レイヤ2ドメインで動作します。これらのデバイスは、特にエンドノードに面している場合に、「ファーストホップ」と呼ばれることがあります。ファーストホップセキュリティ機能は、エンドノードを保護し、IPv6 またはデュアルスタック ネットワークでのリンク操作を最適化します。

ファーストホップセキュリティ (FHS) は、IPv6 リンクの動作を最適化し、大規模な L2 ドメインの拡張に役立つ一連の機能です。これらの機能は、さまざまな不正ユーザや設定ミスのユーザから保護します。拡張 FHS 機能は、さまざまな展開シナリオまたは攻撃ベクトルに使用できます。

次の FHS 機能がサポートされています。

- IPv6 RA ガード

- DHCPv6 ガード
- IPv6 スヌーピング



(注) この機能のイネーブル化の詳細については、[ファーストホップセキュリティの注意事項と制約事項 \(499 ページ\)](#) を参照してください。



(注) FHS 機能をイネーブルにするには、**feature dhcp** コマンドを使用します。

## IPv6 グローバル ポリシー

IPv6 グローバル ポリシーは、ストレージおよびアクセス ポリシー データベースのサービスを提供します。IPv6 スヌーピング、DHCPv6 ガード、および IPv6 RA ガードは、IPv6 グローバル ポリシーの機能です。IPv6 スヌーピング、DHCPv6 ガード、および IPv6 RA ガードをグローバルに設定するたびに、ポリシーの属性が、ソフトウェア ポリシー データベースに保存されます。その後ポリシーはインターフェイスに適用され、ポリシーが適用されたこのインターフェイスを含めるためにソフトウェア ポリシー データベース エントリが更新されます。

すべてのポート レベルの FHS ポリシーは ifacl リージョンでプログラミングされますが、VLAN レベルのポリシーは FHS リージョンでプログラミングされます。ハードウェア プロファイルを設定するには、**tcam regionfhs tcam\_size** コマンドを使用します。TCAM サイズの範囲は 0 ~ 4096 です。

- Cisco Nexus 9200、9300-EX、および 9300-FX/FX2 プラットフォーム スイッチでは、FHS パケットはソフトウェア処理のために **copp-s-dhcpreq** キューを使用します。
- Cisco Nexus 9300、9500 プラットフォーム スイッチ、Cisco Nexus 3164Q スイッチ、N9K-X9432C-S ライン カード、および Cisco Nexus 3232C および 3264Q スイッチは、クラス デフォルトを使用します。



(注) In-Service Software Upgrades (ISSU) を使用して Cisco Nexus シリーズ スイッチを Cisco NX-OS Release 7.0(3)I7(1) にアップグレードする場合は、ポート レベルの FHS ポリシーを設定する前に Cisco NX-OS ボックスをリロードする必要があります。

## IPv6 ファーストホップ セキュリティ バインディング テーブル

デバイスに接続されている IPv6 ネイバーのデータベース テーブルは、IPv6 スヌーピングなどの情報源から作成されます。このデータベース (またはバインディング) テーブルは、スプーフィングやリダイレクト攻撃を防止するために、リンク層アドレス (LLA)、IPv6 アドレス、

およびネイバーのプレフィックス バインディングを検証するためにさまざまな IPv6 ガード機能によって使用されます。

## ファーストホップセキュリティの注意事項と制約事項

ファーストホップセキュリティの一般的な注意事項と制限事項は次のとおりです。

- インターフェイスで FHS を有効にする前に、Cisco Nexus 9300 および 9500 プラットフォーム スイッチで TCAM リージョンをカービングすることを推奨します。FHS を正しく有効にするには、次の手順を実行します。
  - インターフェイスでは、**ifacl** TCAM リージョンをカービングする必要があります。
  - VLAN では、必要なリダイレクト TCAM リージョンをカービングする必要があります。
  - FEX インターフェイスでは、**fex-ipv6-ifacl** TCAM リージョンをカービングする必要があります。
- Cisco Nexus 9200、9300-EX、および 9300-FX/FX2 プラットフォーム スイッチでは、FHS を有効にする前に、**ing-redirect** TCAM リージョンをカービングすることを推奨します。
- Cisco NX-OS リリース 9.3(5) 以降、FHS は Cisco Nexus 9300-GX スイッチでサポートされます。

## vPC ファーストホップセキュリティ設定について

IPv6 ファーストホップセキュリティ vPC はさまざまな方法で導入できます。次のベストプラクティス展開シナリオを推奨します。

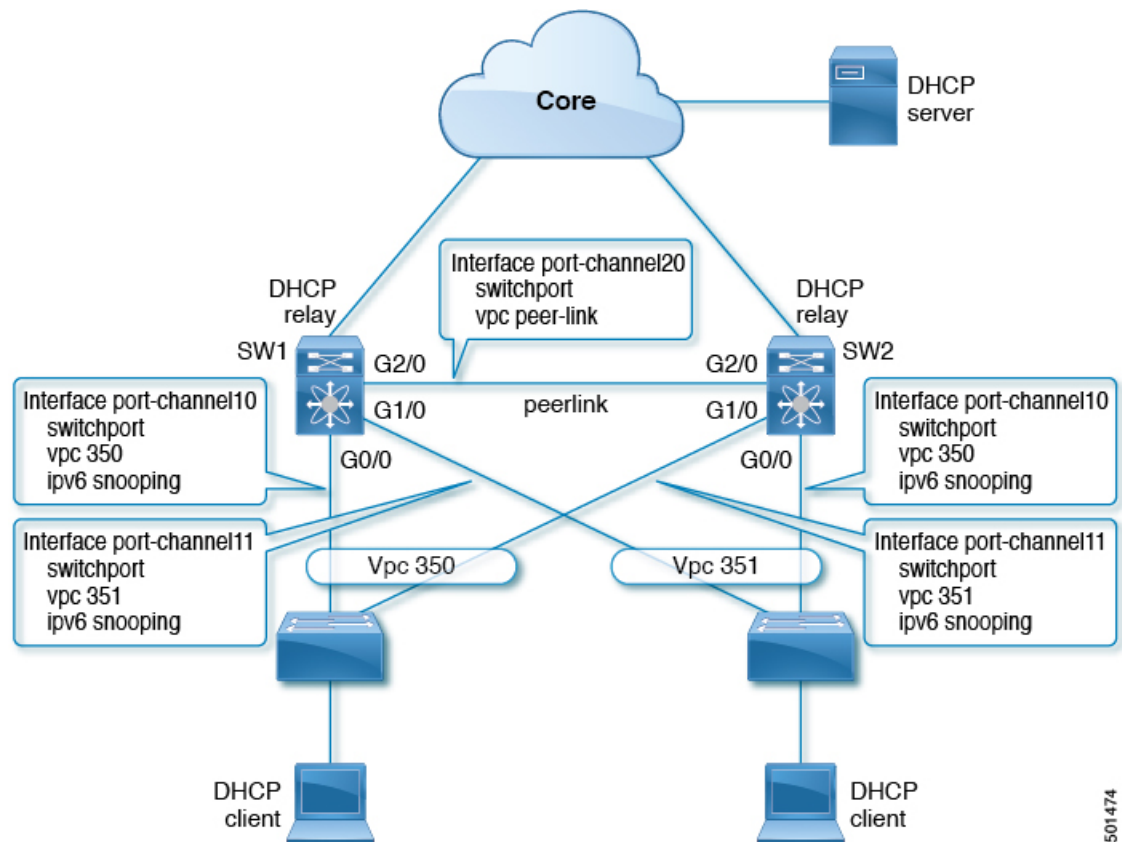
- DHCP リレー オンスタック
- vPC レッグの DHCP リレー
- 孤立ポートの DHCP クライアントとリレー

## DHCP リレー オンスタック

この導入シナリオでは、vPC リンクの背後にあるクライアント、または Nexus スイッチで実行されている DHCP リレーを使用する中間スイッチの背後にあるクライアントを、直接接続できます。Nexus スイッチで実行されている DHCP リレーを使用する中間スイッチの背後にあるクライアントに接続することは、理想的な手段です。VLAN レベルではなく、vPC インターフェイス リンク上の IPv6 スヌーピング機能を直接設定できるからです。インターフェイス レベルでの設定は、次の理由で効率的です。

- 制御トラフィック（DHCP/ND）は、ピアリンクを経由する場合、CPUにリダイレクトされて両方の vPC ピアで処理されることはありません。
- ピアリンク経由でスイッチングされたパケットに、2 回目の処理は行われません。

Figure 12: DHCP リレー オンスタックでの FHS



図では、スヌーピングポリシーは両方の vPC リンクで有効になっています。このシナリオでは、2 つの vPC ピアが vPC リンクの背後にあるすべてのホスト IP/MAC バインディングを学習し、それらを相互に同期します。2 つの vPC ピアは、IPv6 ND と IPv6 DHCP 制御プロトコルの両方を使用してバインディングを学習します。

## VPC レッグでの DHCP リレー

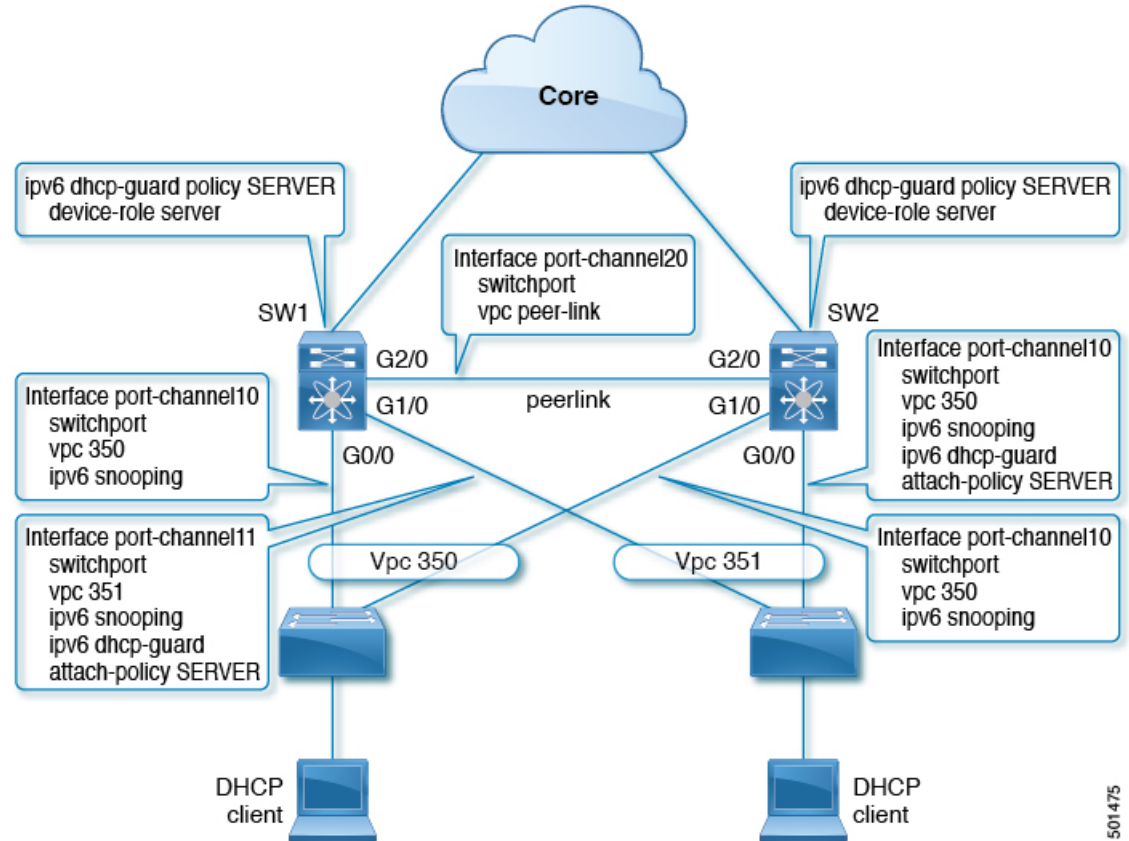
この設定では、リレーエージェントは vPC ピアで実行されません。代わりに、DHCP リレーエージェント（または DHCP サーバ）が vPC リンクの背後で実行されます（アクセスできる場所に置くことも、さらにはコアのどこかに配置することもできます）。このような導入シナリオでは、IPv6 スヌーピング機能は DHCP サーバメッセージを暗黙的に信頼せず、デフォルトで DHCP サーバメッセージをドロップします。IPv6 ポリシーをカスタマイズして、次を実装できます。

- セキュリティレベルに関する補足情報。



- デバイスロール サーバを使用した IPv6 DHCP ガード ポリシー。この設定では、IPv6 スヌーピングは vPC リンクに接続された DHCP サーバ メッセージを信頼します。

Figure 13: 外部 DHCP リレーを使用した FHS 設定



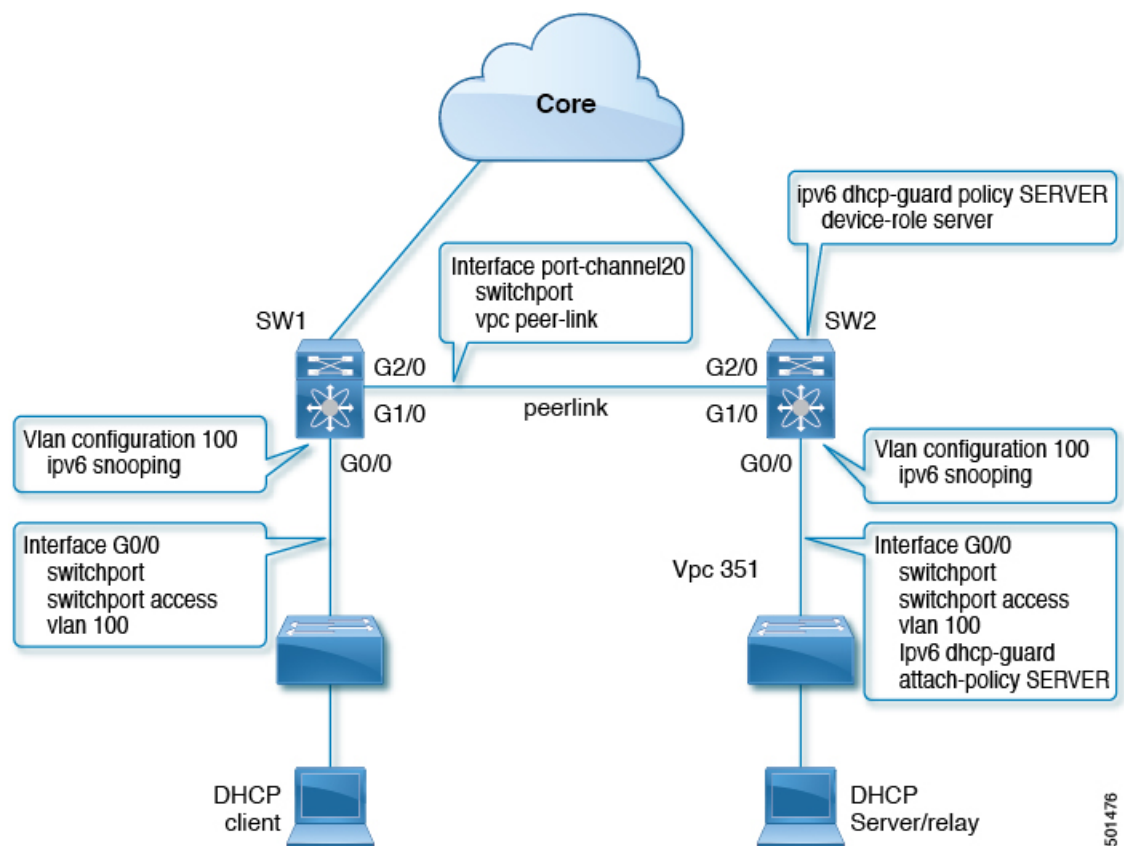
図では、クライアントはデフォルトの IPv6 スヌーピング ポリシーを持つ vPC リンクの背後に配置されています。DHCP サーバトラフィックが到達するリンクに、ipv6 スヌーピングと、ipv6 dhcp-guard attach-policy SERVER ポリシーの両方をアタッチできます。DHCP 制御トラフィックを介してクライアントバインディングエントリを作成するには、サーバまたはリレー側とクライアント側の両方の IPv6 スヌーピング ポリシーが必要です。これは、IPv6 スヌーピングがバインディングを作成するためにはクライアントとサーバの両方のパケットを確認する必要があるためです。また、IPv6 DHCP ガード ポリシーを設定して、IPv6 スヌーピング ポリシーによる DHCP サーバトラフィックを許可する必要があります。vPC ピアは vPC ポートで学習されたすべての新しく学習されたクライアントエントリを同期するため、両方のピアに同じ設定が必要です。

## 孤立ポートでの DHCP クライアントリレー

この設定では、孤立ポートを介してクライアントを接続できます。IPv6 スヌーピング機能は、vPC ポートのクライアントバインディングのみを同期します。孤立ポートは両方の vPC ピアに直接接続されていないため、同期されません。このような設定では、IPv6 スヌーピング機能は両方のスイッチで独立して実行されます。この図は、次のことを示しています。

- 最初のスイッチで、クライアント側インターフェイスに IPv6 スヌーピング ポリシーをアタッチする必要があります。ただし、vPC ピアの背後にある孤立ポート上のサーバからの DHCP サーバパケットに対応するには、VLAN レベルでポリシーを付加する必要があります。このような場合、VLAN に適用されるポリシーは、クライアントトラフィック インターフェイスと DHCP サーバトラフィックの両方を検査します。インターフェイスごとに個別の IPv6 スヌーピングポリシーは必要ありません。vPC ピア経由で着信する DHCP トラフィックも暗黙的に信頼され、ポリシーが必要な場合は、vPC ピアによって自動的にドロップされます。
- また、2 番目のスイッチで VLAN レベルで IPv6 を設定する必要があります。また、孤立ポートに面するサーバで「デバイス ロールサーバ」を使用して IPv6 DHCP ガードポリシーを設定する必要があります。これにより、IPv6 スヌーピング機能による DHCP サーバパケットのドロップが防止されます。両方のスイッチはクライアントバインディング エントリを個別に学習し、クライアントが vPC リンク上にないため、それらを同期しません。

Figure 14: 孤立ポート上のクライアントおよび DHCP リレーによる FHS 設定



501476

# RA ガード

## IPv6 RA ガードの概要

IPv6 RA ガード機能は、ネットワーク デバイス プラットフォームに到着した不要または不正な RA ガードメッセージを、ネットワーク管理者がブロックまたは拒否できるようにするためのサポートを提供します。RA は、リンクで自身をアナウンスするためにデバイスによって使用されます。IPv6 RA ガード機能は、それらの RA を分析して、承認されていないデバイスから送信された RA を除外します。ホスト モードでは、ポート上の RA とルータ リダイレクトメッセージはすべて許可されません。RA ガード機能は、レイヤ 2 (L2) デバイスの設定情報を、受信した RA フレームで検出された情報と比較します。L2 デバイスは、RA フレームとルータ リダイレクトフレームの内容を設定と照らし合わせて検証した後で、RA をユニキャストまたはマルチキャストの宛先に転送します。RA フレームの内容が検証されない場合は、RA はドロップされます。

## IPv6 RA ガードの注意事項と制約事項

IPv6 RA ガードの注意事項と制約事項は次のとおりです。

- IPv6 RA ガード機能は、IPv6 トラフィックがトンネリングされる環境では保護を行いません。
- この機能は、TCAM (Ternary Content Addressable Memory) がプログラムされているハードウェアでのみサポートされています。
- この機能は、入力方向のスイッチ ポート インターフェイスで設定できます。
- この機能は、ホスト モードとルータ モードをサポートしています。
- この機能は、入力方向だけでサポートされます。出力方向ではサポートされません。
- この機能は、補助 VLAN およびプライベート VLAN (PVLAN) でサポートされています。PVLAN の場合、プライマリ VLAN の機能が継承され、ポート機能とマージされます。
- IPv6 RA ガード機能によってドロップされたパケットはスパニングできます。

# DHCPv6 ガード

## DHCP の概要 : DHCPv6 ガード

DHCPv6 ガード機能は、サーバからクライアントに DHCP パケットを転送する、承認されていない DHCP サーバとリレー エージェントから発信される DHCP 応答やアドバタイズメントメッセージをブロックします。リレーエージェントによってクライアントからサーバに送信さ

れるクライアント メッセージはブロックされません。フィルタリングの判断は、受信側のスイッチ ポート、トランク、または VLAN に割り当てられているデバイスのロールによって決まります。この機能により、トラフィックリダイレクションやサービス妨害 (DoS) を防ぐことができます。

パケットは3つの DHCP メッセージタイプのいずれかに分類されます。すべてのクライアントメッセージは、デバイスのロールに関係なく、常にスイッチングされます。DHCPサーバのメッセージは、デバイスのロールがサーバに設定されている場合のみさらに処理されます。DHCP サーバアドバタイズメントの追加処理は、サーバプリファレンス チェックのために行われます。

デバイスが DHCPサーバとして設定されている場合、デバイスのロールの設定に関係なく、すべてのメッセージをスイッチングする必要があります。

## DHCPv6 ガードの制限事項

DHCPv6 ガードの注意事項と制約事項は次のとおりです。

- DHCPサーバから到着するパケットがリレー転送またはリレー応答である場合、デバイスロールのみがチェックされます。さらに、IPv6 DHCPガードは、スイッチで実行されているローカルリレーエージェントによって送信されたパケットにポリシーを適用しません。

## IPv6 スヌーピング

### IGMP スヌーピングの概要

IPv6 の「スヌーピング」機能は、レイヤ 2 IPv6 のファーストホップ機能をいくつか組み合わせたもので、レイヤ 2 (またはレイヤ 2 とレイヤ 3 の間) で動作し、IPv6 の機能にセキュリティと拡張性を提供します。この機能によって、Duplicate Address Detection (DAD)、アドレス解決、デバイス検出やネイバーキャッシュに対する攻撃といった、ネイバー探索メカニズムに固有のいくつかの脆弱性が軽減されます。

IPv6 スヌーピングは、レイヤ 2 ネイバー テーブルのステートレス自動設定アドレスのバインディングを学習して保護し、信頼できるバインディングテーブルを構築するためにスヌーピングメッセージを分析します。有効なバインディングのない IPv6 スヌーピングメッセージはドロップされます。IPv6 スヌーピングメッセージは、その IPv6 から MAC へのマッピングが検証可能な場合に信頼できると見なされます。

ターゲット (プラットフォームのターゲット サポートによって異なり、デバイス ポート、スイッチ ポート、レイヤ 2 インターフェイス、レイヤ 3 インターフェイス、および VLAN が含まれることがある) に IPv6 スヌーピングが設定されている場合、IPv6 トラフィックのスヌーピング プロトコルと Dynamic Host Configuration Protocol (DHCP) をルーティング デバイスのスイッチ統合セキュリティ機能 (SISF) インフラストラクチャにリダイレクトするためのキャプチャ命令がハードウェアにダウンロードされます。スヌーピング トラフィックの場合、Neighbor Discovery Protocol (NDP) メッセージは SISF に送信されます。DHCPv6の場合、

dhcwp6\_client および dhcwp\_server ポートから送信された UDP メッセージがリダイレクトされます。

IPv6 スヌーピングはその「キャプチャ ルール」を分類子に登録します。分類子では、特定のターゲットにあるすべての機能のルールがすべて集約され、対応する ACL がプラットフォーム依存モジュールにインストールされます。分類子は、リダイレクトされたトラフィックを受信すると、（トラフィックを受信しているターゲットに対して）登録されているすべての機能からすべてのエントリ ポイント（IPv6 スヌーピングのエントリ ポイントを含む）を呼び出します。IPv6 スヌーピングのエントリ ポイントは最後に呼び出されるため、他の機能によって行われた決定が IPv6 スヌーピングの決定よりも優先されます。

IPv6 スヌーピングは、IPv6 ホストが非表示になったときにネイバー テーブルを即時に更新できるように、IPv6 ホストの活性トラッキングを提供します。

加えて、IPv6 スヌーピングは、正確なバインディング テーブルに依存するその他多くの IPv6 の機能の基盤です。この機能は、アドレス収集のためにリンク上のスヌーピングおよび DHCP メッセージを検査した後に、それらのアドレスをバインディング テーブルに入力します。また、この機能は、アドレスの所有権を強制し、特定のノードが要求可能なアドレスの数を制限します。

## IPv6 スヌーピングに関する注意事項と制限事項

IPv6 スヌーピングの注意事項と制限事項は次のとおりです。

- 両方の vPC ピアで同じ設定を実行する必要があります。IPv6 スヌーピングの自動整合性チェッカはサポートされていません。
- IPv6 スヌーピング機能は、TCAM (Ternary Content Addressable Memory) がプログラムされているハードウェアでのみサポートされています。
- この機能は、入力方向のスイッチ ポート インターフェイスまたは VLAN のみで設定できます。
- IPv6 スヌーピングが DHCP バインディングを学習するには、サーバとクライアントの両方の応答を確認する必要があります。IPv6 スヌーピング ポリシーは、インターフェイス（または VLAN）に面したクライアントと、インターフェイス（または VLAN）に面した DHCP サーバの両方にアタッチする必要があります。DHCP リレーの場合、サーバの応答を確認するために、IPv6 スヌーピングポリシーを VLAN レベルでアタッチする必要があります。

# IPv6 FHS の設定方法

## デバイスでの IPv6 RA ガード ポリシーの設定



(注) **ipv6 nd rguard** コマンドがポートで設定されている場合、ルータ送信要求メッセージはこれらのポートに複製されません。ルータ要請メッセージを複製するには、ルータ側のすべてのポートをルータ ロールに設定する必要があります。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例：  Device# <code>configure terminal</code>	グローバル 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	<b>ipv6 nd rguard policy <i>policy-name</i></b> 例：  Device(config)# <code>ipv6 nd rguard policy policy1</code>	RA ガード ポリシー名を定義して、RA ガード 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 3	<b>device-role {host   router   monitor   switch}</b> 例：  Device(config-ra-guard)# <code>device-role router</code>	<p>ポートに接続されているデバイスの役割を指定します。</p> <ul style="list-style-type: none"> <li>• <b>device-role host</b> : 通常のノードまたはホストを接続するインターフェイスまたはVLAN。これは、IPV6 RA ガード ポリシーを適用します。 <b>device-role</b> ホストは、着信 RS パケットを許可し、着信 RA または RR パケットをブロックします。別のインターフェイスで受信された RS パケットは、デバイスロールホストにリダイレクトされません。 RA および RR パケット（許可されている）のみがデバイスロールホストにリダイレクトされます。</li> <li>• <b>device-role switch</b> : <b>device-role</b> スイッチは <b>device-role</b> ホストと同様に動作</li> </ul>

	コマンドまたはアクション	目的
		<p>します。たとえば、トランク ポートのラベルとして使用できます。</p> <ul style="list-style-type: none"> <li>• <b>device-role monitor</b> : このデバイスはネットワークトラフィックをモニタします。これは、RS パケットもこのインターフェイスに送信されることを除き、device-role ホストと同様に動作します。これは、トラフィックのキャプチャに役立ちます。</li> <li>• <b>device-role router</b> : ルータに接続するインターフェイス。このインターフェイスは、着信RS、RA、またはRR パケットを許可します。</li> </ul>
ステップ 4	<b>hop-limit {maximum   minimum limit}</b> 例 : <pre>Device(config-ra-guard)# hop-limit minimum 3</pre>	<p>(任意) アドバタイズされたホップ カウント制限の検証をイネーブルにします。</p> <ul style="list-style-type: none"> <li>• 設定されていない場合、このチェックは回避されます。</li> </ul>
ステップ 5	<b>managed-config-flag {on   off}</b> 例 : <pre>Device(config-ra-guard)# managed-config-flag on</pre>	<p>(任意) アドバタイズされた管理アドレスの設定フラグが on であることの検証をイネーブルにします。</p> <ul style="list-style-type: none"> <li>• 設定されていない場合、このチェックは回避されます。</li> </ul>
ステップ 6	<b>other-config-flag {on   off}</b> 例 : <pre>Device(config-ra-guard)# other-config-flag on</pre>	<p>(任意) アドバタイズされた [Other] 設定パラメータの検証をイネーブルにします。</p>
ステップ 7	<b>router-preference maximum {high   low   medium}</b> 例 : <pre>Device(config-ra-guard)# router-preference maximum high</pre>	<p>(任意) アドバタイズされたデフォルトルータの設定パラメータの値が指定された制限値以下であることの検証をイネーブルにします。</p>
ステップ 8	<b>trusted-port</b> 例 : <pre>Device(config-ra-guard)# trusted-port</pre>	<p>(任意) このポリシーが信頼できるポートに適用されることを指定します。</p> <ul style="list-style-type: none"> <li>• すべての RA ガード ポリシングが無効になります。</li> </ul>

	コマンドまたはアクション	目的
ステップ 9	<b>exit</b> 例： Device(config-ra-guard)# exit	RA ガード ポリシー コンフィギュレーション モードを終了してグローバル コンフィギュレーション モードに戻ります。

## インターフェイスの IPv6 RA ガードの設定

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： Device# 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	<b>interface type number</b> 例： Device(config)# interface ethernet 1/1 例： Device(config)# vlan configuration 10	インターフェイスのタイプと番号を指定し、デバイスをインターフェイス モードにするか、VLAN 設定モードにします。
ステップ 3	<b>ipv6 nd rguard attach-policy [policy-name]</b> 例： Device(config-if)# ipv6 nd rguard attach-policy	指定したインターフェイスに IPv6 RA ガード機能を適用します。
ステップ 4	<b>exit</b> 例： Device(config-if)# exit	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	<b>show ipv6 nd rguard policy [policy-name]</b> 例： switch# show ipv6 nd rguard policy host Policy host configuration: device-role host  Policy applied on the following interfaces:	RA ガードを使用して設定されているすべてのインターフェイスで RA ガード ポリシーを表示します。



	コマンドまたはアクション	目的
	Et0/0           vlan all Et1/0           vlan all	
ステップ 6	<b>debug ipv6 snooping raguard</b> [ <i>filter</i>   <i>interface</i>   <i>vlanid</i> ]  例 :  Device# debug ipv6 snooping raguard	IPv6 RA ガード スヌーピング情報のデバッグをイネーブルにします。

## DHCP—DHCPv6 ガードの設定

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b>  例 :  Device# 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	<b>ipv6 dhcp guard policy</b> <i>policy-name</i>  例 :  Device(config)# ipv6 dhcp guard policy poll	DHCPv6 ガード ポリシー名を定義して、DHCP ガード 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	<b>device-role</b> { <i>client</i>   <i>server</i> }  例 :  Device(config-dhcp-guard)# device-role server	ターゲット（インターフェイスまたは VLAN）に接続されているデバイスのデバイス ロールを指定します。  <ul style="list-style-type: none"> <li>• <b>device-role client</b> : 通常の DHCPv6 クライアントが接続されているインターフェイス。着信サーバパケットをブロックします。</li> <li>• <b>device-role server</b> : 通常の DHCPv6 サーバが接続されているインターフェイス。このインターフェイスから発信されるすべての DHCPv6 パケットを許可します。</li> </ul>
ステップ 4	<b>preference min</b> <i>limit</i>  例 :  Device(config-dhcp-guard)# preference min 0	(任意) アドバイズされた設定 ([ <i>preference</i> ] オプション内) が指定された制限を超過しているかどうかの検証をイネーブルにします。設定されて

	コマンドまたはアクション	目的
		いない場合、このチェックは回避されます。
ステップ 5	<b>preference max limit</b> 例 : <pre>Device(config-dhcp-guard)# preference max 255</pre>	(任意) アドバタイズされた設定 ([preference] オプション内) が指定された制限未満であるかどうかの検証をイネーブルにします。設定されていない場合、このチェックは回避されます。
ステップ 6	<b>trusted-port</b> 例 : <pre>Device(config-dhcp-guard)# trusted-port</pre>	(任意) このポリシーが信頼できるポートに適用されることを指定します。すべての DHCP ガードポリシーが無効になります。
ステップ 7	<b>exit</b> 例 : <pre>Device(config-dhcp-guard)# exit</pre>	DHCP ガード コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードに戻ります。
ステップ 8	<b>interface type number</b> 例 : <pre>Device(config)# interface GigabitEthernet 0/2/0</pre>	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 9	<b>switchport</b> 例 : <pre>Device(config-if)# switchport</pre>	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 モードにします。
ステップ 10	<b>ipv6 dhcp guard [attach-policy policy-name]</b> 例 : <pre>Device(config-if)# ipv6 dhcp guard attach-policy poll</pre>	インターフェイスに DHCPv6 ガードポリシーを対応付けます。
ステップ 11	<b>exit</b> 例 : <pre>Device(config-if)# exit</pre>	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、グローバルコンフィギュレーションモードに戻ります。
ステップ 12	<b>vlan configuration vlan-id</b> 例 :	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。

	コマンドまたはアクション	目的
	Device(config)# vlan configuration 1	
ステップ 13	<b>ipv6 dhcp guard [attach-policy policy-name]</b> 例 : Device(config-vlan-config)# ipv6 dhcp guard attach-policy pol1	VLAN に DHCPv6 ガード ポリシーを対応付けます。
ステップ 14	<b>exit</b> 例 : Device(config-vlan-config)# exit	VLAN コンフィギュレーションモードを終了し、グローバル コンフィギュレーションモードに戻ります。
ステップ 15	<b>exit</b> 例 : Device(config)# exit	グローバル コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。
ステップ 16	<b>show ipv6 dhcp guard policy [policy-name]</b> 例 : Device# show ipv6 dhcp policy guard pol1	(任意) ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。

## IPv6 スヌーピングの設定

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 : Device# 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	<b>ipv6 snooping policy policy-name</b> 例 : Device(config)# ipv6 snooping policy policy1	IPv6 スヌーピングポリシーを設定し、IPv6 スヌーピング 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	<b>device-role { node   switch }</b> 例 : <pre>Device(config-snoop-policy)# device-node switch</pre>	ターゲット（インターフェイスまたは VLAN）に接続されているデバイスの ロールを指定します。 <ul style="list-style-type: none"> <li>• <b>node</b> - がデフォルトです。バインディングが作成され、エントリがプローブされます。</li> <li>• <b>スイッチ</b> : エントリはプローブされず、信頼できるポートが有効になっている場合、バインディングは作成されません。</li> </ul>
ステップ 4	<b>[no] limit address-count</b> 例 : <pre>Device(config-snoop-policy)# limit address-count 500</pre>	バインディングエントリの数を制限します。 <b>no limit address-count</b> は制限なしを意味します。
ステップ 5	<b>[no] protocol dhcp   ndp</b> 例 : <pre>Device(config-snoop-policy)# protocol dhcp  Device(config-snoop-policy)# protocol ndp</pre>	DHCP または NDP グリーニングのいずれかをオンまたはオフにします。
ステップ 6	<b>trusted-port</b> 例 : <pre>Device(config-snoop-policy)# trusted-port</pre>	ポリシーを信頼できるポートに適用することを指定します。エントリが信頼できるポートである場合、そのトラフィックはブロックまたはドロップされません。
ステップ 7	<b>security-level glean   guard   inspect</b> 例 : <pre>Device(config-snoop-policy)# security-level guard</pre>	ポリシーに適用するセキュリティのタイプ（グリーニング、ガード、または検査）を指定します。各セキュリティレベルの意味は次のとおりです。 <ul style="list-style-type: none"> <li>• <b>glean</b> : バインディングを学習しますが、パケットはドロップしません。</li> <li>• <b>inspect</b> : アドレス盗難などの問題を検出した場合に、バインディングを学習し、パケットをドロップします。</li> <li>• <b>guard</b> : <b>inspect</b> と同様に機能しますが、さらに脅威の場合に IPv6、</li> </ul>

	コマンドまたはアクション	目的
		ND、RA、および IPv6 DHCP サーバ パケットをドロップします。
ステップ 8	<b>tracking</b> 例： Device(config-snoop-policy)# tracking enable	トラッキングをイネーブルにします。
ステップ 9	<b>exit</b> 例： Device(config-snoop-policy)# exit	IPv6 スヌーピング コンフィギュレーションモードを終了し、グローバルコンフィギュレーションモードに戻ります。
ステップ 10	<b>interface type-number</b> 例： Device(config-if)# interface ethernet 1/25	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 11	<b>[no] switchport</b> 例： Device(config-if)# switchport	レイヤ 2 モードとレイヤ 3 モードを切り替えます。
ステップ 12	<b>ipv6 snooping attach-policy policy-name</b> 例： Device(config-if)# ipv6 snooping attach-policy policyl	インターフェイスに IPv6 スヌーピング ポリシーを適用します。
ステップ 13	<b>exit</b> 例： Device(config-if)# exit	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、グローバルコンフィギュレーションモードに戻ります。
ステップ 14	<b>vlan configuration vlan-id</b> 例： Device(config)# vlan configuration 333	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 15	<b>ipv6 snooping attach-policy policy-name</b> 例： Device(config-vlan-config)# ipv6 snooping attach-policy policyl	IPv6 スヌーピング ポリシーを VLAN に適用します。
ステップ 16	<b>exit</b> 例： Device(config-vlan-config)# exit	VLAN コンフィギュレーションモードを終了し、グローバル コンフィギュレーションモードに戻ります。

	コマンドまたはアクション	目的
ステップ 17	<b>exit</b> 例： Device(config)# exit	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 18	<b>show ipv6 snooping policy <i>policy-name</i></b> 例： Device(config)# show ipv6 snooping policy policy1	ポリシー設定と、そのポリシーが適用されるインターフェイスを表示します。

## IPv6 スヌーピングの確認とトラブルシューティング

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>show ipv6 snooping capture-policy [interface <i>type number</i>]</b> 例： Device# show ipv6 snooping capture-policy interface ethernet 0/0	スヌーピング ND メッセージ キャプチャ ポリシーを表示します。
ステップ 2	<b>show ipv6 snooping counter [interface <i>type number</i>]</b> 例： Device# show ipv6 snooping counter interface FastEthernet 4/12	インターフェイス カウンタによってカウントされたパケットに関する情報を表示します。
ステップ 3	<b>show ipv6 snooping features</b> 例： Device# show ipv6 snooping features	デバイスに設定されているスヌーピング機能に関する情報を表示します。
ステップ 4	<b>show ipv6 snooping policies [interface <i>type number</i>]</b> 例： Device# show ipv6 snooping policies	設定されているポリシーと、ポリシーが接続されているインターフェイスに関する情報を表示します。
ステップ 5	<b>debug ipv6 snooping</b> 例： Device# debug ipv6 snooping	IPv6 でスヌーピング情報のデバッグをイネーブルにします。

## 設定例

### 例：IPv6 RA ガードの設定

```
Device(config)# interface ethernet 1/1

Device(config-if)# ipv6 nd rguard attach-policy

Device# show running-config interface ethernet 1/1

Building configuration...
Current configuration : 129 bytes
!
interface ethernet1/1
 switchport
 switchport access vlan 222
 switchport mode access
 access-group mode prefer port
 ipv6 nd rguard
end
```

### 例：DHCP—DHCPv6 ガードの設定

次の例は、DHCPv6 ガードの設定例を示しています。

```
configure terminal
ipv6 dhcp guard policy poll
 device-role server
 preference min 0
 preference max 255
 trusted-port
interface GigabitEthernet 0/2/0
 switchport
 ipv6 dhcp guard attach-policy poll
 vlan configuration 1
   ipv6 dhcp guard attach-policy poll
show ipv6 dhcp guard policy poll
```

### 例：IPv6 ファーストホップセキュリティ バインディング テーブルの設定

```
config terminal
ipv6 neighbor binding vlan 100 2001:db8::1 interface ethernet3/0
ipv6 neighbor binding max-entries 100
ipv6 neighbor binding logging
ipv6 neighbor binding retry-interval 8
exit
show ipv6 neighbor binding
```

## 例 : IPv6 スヌーピングの設定

```

switch (config)# ipv6 snooping policy policy1
switch(config-ipv6-snooping)# ipv6 snooping attach-policy policy1
switch(config-ipv6-snooping)# exit
.
.
.
Device# show ipv6 snooping policies policy1
Policy policy1 configuration:
  trusted-port
  device-role node
Policy applied on the following interfaces:
  Et0/0      vlan all
  Et1/0      vlan all
Policy applied on the following vlans:
  vlan 1-100,200,300-400

```

## IPv6 ファーストホップセキュリティに関する追加情報

ここでは、IPv6 ファーストホップセキュリティ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』





## 第 18 章

# ダイナミック ARP インспек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。

- [DAI について, on page 517](#)
- [DAI の前提条件, on page 520](#)
- [DAI の注意事項と制約事項（521 ページ）](#)
- [DAI のデフォルト設定, on page 522](#)
- [DAI の設定, on page 522](#)
- [DAI の設定の確認, on page 527](#)
- [DAI の統計情報のモニタリングとクリア, on page 528](#)
- [DAI の設定例, on page 528](#)
- [DAI に関する追加情報, on page 533](#)

## DAI について

### 『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。





```
VLAN 100 DAI 100.100.100.100 100.100.100.100 DAI 100.100.100.100 100.100.100.100
100.100.100.100
100.100.100.100 DAI 100.100.100.100 100.100.100.100
100.100.100.100
DAI 100.100.100.100 100.100.100.100
DAI 100.100.100.100 100.100.100.100 DAI 100.100.100.100 DAI 100.100.100.100 3 100.100.100.100
```



**Note** 100.100.100.100 VLAN 100.100.100 ARP 100.100.100.100

## 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ログに記録します。

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。



**Note** 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。

## 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。 [DHCP の設定, on page 445](#) を参照してください。
- DAI をイネーブルにする VLAN を設定する必要があります。『Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide』を参照してください。
- **hardware access-list tcam region arp-ether** コマンドを使用して、DAI 用の ACL TCAM のリージョン サイズを設定する必要があります。arp-ether リージョンが有効でない限り、DAI 設定は受け入れられません。「[ACL TCAM リージョン サイズの設定, on page 342](#)」を参照してください。

## 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。
- `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。
- DAI は、アクセスポート、トランクポート、およびポートチャンネルポートでサポートされます。
- ポートチャンネルに対する DAI の信頼設定によって、そのポートチャン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ン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。
- ポートチャン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ンネルの DAI 信頼状態の設定を保持しません。
- ポートチャンネルの信頼状態を変更すると、デバイスはそのチャン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、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。
- ARP ACL はサポートされていません。
- Cisco NX-OS リリース 9.3(3) 以降、DAI は Cisco Nexus 9364C-GX、Cisco Nexus 9316D-GX、および Cisco Nexus 93600CD-GX スイッチでサポートされています。

## 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。

Table 38: 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 <code>untrusted</code> 。
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。 ログング レート インターバルは 1 秒です。
VLAN 単位のログング	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。

#### 始める前に

DHCP 機能がイネーブルにされていることを確認します。

DAI をイネーブルにする VLAN が設定されていることを確認します。

DAI (`arp-ether`) の ACL TCAM リージョン サイズが設定されていることを確認します。

#### 手順

	コマンドまたはアクション	目的
ステップ 1	<code>configure terminal</code> 例 :	グローバル 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
	switch# configure terminal switch(config)#	
ステップ 2	<b>[no] ip arp inspection vlan <i>vlan-list</i></b>  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。 <b>no</b> 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	(任意) <b>show ip arp inspection vlan <i>vlan-id</i></b>  例： switch(config)# show ip arp inspection vlan 13	特定の VLAN の DAI 設定を表示します。
ステップ 4	(任意) <b>copy running-config startup-config</b>  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。

## 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。

### Before you begin

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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  Example: 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。

	Command or Action	Purpose
ステップ 2	<b>interface</b> <i>type port/slot</i> <b>Example:</b> 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	<b>[no] ip arp inspection trust</b> <b>Example:</b> 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。 <b>no</b> 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	(Optional) <b>show ip arp inspection interface</b> <i>type port/slot</i> <b>Example:</b> switch(config-if)# show ip arp inspection interface ethernet 2/1	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	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch(config-if)# 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。

## 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。

#### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	<code>[ ] { [ ] [ ] }</code> <b>no ip arp inspection validatesrc-macdstdst-macip</b> <b>Example:</b> 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。このコマンドの <b>no</b> 形式を使用すると、追加の DAI 検証がディセーブルになります。
ステップ 3	(Optional) <b>show running-config dhcp</b> <b>Example:</b> switch(config)# show running-config dhcp	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	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> 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。

## 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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	<b>[no] ip arp inspection log-buffer entries number</b> <b>Example:</b> 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。 <b>no</b> 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	(Optional) <b>show running-config dhcp</b> <b>Example:</b> switch(config)# show running-config dhcp	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	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> 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。

## 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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	<b>[no] ip arp inspection vlan <i>vlan-list</i> logging dhcp-bindings {all   none   permit}</b> <b>Example:</b>	次のようにして、DAI ログ フィルタリングを設定します。このコマンドの <b>no</b>

	Command or Action	Purpose
	switch(config)# ip arp inspection vlan 100 dhcp-bindings permit	形式を使用すると、DAI ログ フィルタリングは削除されます。  <ul style="list-style-type: none"> <li>• <b>all</b> : 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。</li> <li>• <b>none</b> : DHCP バインディングに一致するパケットを記録しません。</li> <li>• <b>permit</b> : 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。</li> </ul>
ステップ 3	(Optional) <b>show running-config dhcp</b>  <b>Example:</b> switch(config)# show running-config dhcp	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	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> 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。

## 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。

コマンド	目的
<b>show ip arp inspection</b>	DAI のステータスを表示します。
<b>show ip arp inspection interfaces</b> [ethernet slot/port   port-channel number]	特定のインターフェイスまたはポートチャネルの信頼状態および ARP パケット レートを表示します。
<b>show ip arp inspection log</b>	DAI のログ設定を表示します。
<b>show ip arp inspection vlan</b> vlan-id	特定の VLAN の DAI 設定を表示します。
<b>show running-config dhcp</b> [all]	DAI の設定を表示します。

# 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。

コマンド	目的
<code>show ip arp inspection statistics [vlan vlan-id]</code>	DAI の統計情報を表示します。
<code>clear ip arp inspection statistics vlan vlan-id</code>	DAI 統計情報をクリアします。
<code>clear ip arp inspection log</code>	DAI ログを消去します。

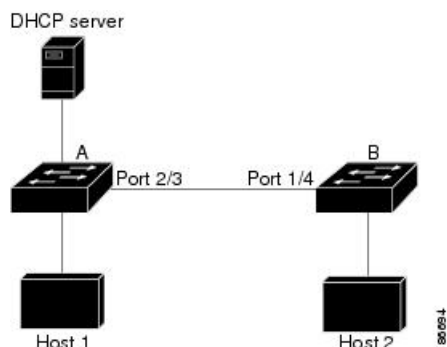
## DAI の設定例

### DAI 2

2 DAI DAI

Figure 17: DAI 2

1 A 2 B VLAN 1  
 ? DAI DHCP A DHCP IP A 1  
 2 B 2 A 2/3 B  
 1/4



DAI ARP ARP IP MAC DHCP  
 IP ARP DHCP

- DHCP A
- A 2/3 B 1/4

## 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。

### Procedure

**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# configure terminal
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、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 Jan 23 2015])

```

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。

### Procedure

**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# configure terminal
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、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 Jan 23 2015])

```

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#

```



## 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
ACL TCAM リージョン	<a href="#">IP ACL の設定</a>
『DHCP and DHCP snooping』	<a href="#">DHCP の設定 (445 ページ)</a>

### 標準

標準	タイトル
RFC-826	『An Ethernet Address Resolution Protocol』 ( <a href="http://tools.ietf.org/html/rfc826">http://tools.ietf.org/html/rfc826</a> )





## 第 19 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。

- [IP ソース ガードについて, on page 535](#)
- [IP ソース ガードの前提条件, on page 536](#)
- [IP ソース ガードの注意事項と制約事項 \(536 ページ\)](#)
- [IP ソース ガードのデフォルト設定, on page 537](#)
- [IP ソース ガードの設定, on page 538](#)
- [IP ソース ガード バインディングの表示, on page 540](#)
- [IP ソース ガードの統計情報のクリア \(540 ページ\)](#)
- [IP ソース ガードの設定例, on page 541](#)
- [その他の参考資料, on page 541](#)

## IP ソース ガードについて

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** コマンドによって表示されたバインディング テーブル エントリが次のとおりであるとしています。

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 ガードの前提条件

IP ソース ガードの前提条件は次のとおりです。

- IP ソース ガードを設定するには、その前に DHCP 機能および DHCP スヌーピングをイネーブルにする必要があります。 [DHCP の設定, on page 445](#) を参照してください。
- **hardware access-list tcam region ipsg** コマンドを使用して、IP ソース ガード用の ACL TCAM のリージョン サイズを設定する必要があります。 [ACL TCAM リージョン サイズの設定, on page 342](#) を参照してください。



### Note

デフォルトでは、ipsg のリージョン サイズはゼロです。SMAC-IP バインディングの保存と適用をするには、このリージョンに十分なエントリを割り当てる必要があります。

## 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 ガードは、Fabric Extender (FEX) および汎用拡張モジュール (GEM) ポートではサポートされていません。
- 次の注意事項と制約事項は、Cisco Nexus 9200 シリーズ スイッチに適用されます。
  - 着信インターフェイスで IPSG がイネーブルであると IPv6 の隣接関係は形成されません。
  - IPSG は HSRP スタンバイで ARP パケットを廃棄します。
  - DHCP スヌーピングおよび IPSG がイネーブルにされている場合、ホストのバインディング エントリが存在すると、ARP がなくてもトラフィックはホストに転送されます。
- Cisco NX-OS リリース 9.3(5) 以降、IP Source Guard は Cisco Nexus 9364C-GX、Cisco Nexus 9316D-GX、および Cisco Nexus 93600CD-GX スイッチでサポートされています。

## 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。

**Table 39:** 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。

### Before you begin

DHCP 機能および DHCP スヌーピングがイネーブルにされていることを確認します。

IPSG (ipsg) の ACL TCAM リージョン サイズが設定されていることを確認します。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	<b>interface ethernet slot/port</b> <b>Example:</b> switch(config)# interface ethernet 2/3 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	<b>[no] ip verify source dhcp-snooping-vlan</b> <b>Example:</b> 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。このコマンドの <b>no</b> 形式を使用すると、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	(Optional) <b>show running-config dhcp</b> <b>Example:</b> switch(config-if)# show running-config dhcp	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	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> switch(config-if)# 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、固定 IP ソース エントリは作成されません。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> 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	<b>[no] ip source binding ip-address mac-address vlan vlan-id interface interface-type slot/port</b>  <b>Example:</b> 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。このコマンドの <b>no</b> 形式を使用すると、スタティック IP ソース エントリが削除されます。
ステップ 3	(Optional) <b>show ip dhcp snooping binding [interface interface-type slot/port]</b>  <b>Example:</b> switch(config)# show ip dhcp snooping binding interface ethernet 2/3	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	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> 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。

## トランク ポート用 IP ソース ガードの設定

あるポートに IP ソース ガードが設定されている場合、それを TCAM 内で許可する DHCP スヌーピング エントリがない限り、そのポートに着信するトラフィックはドロップされます。ただし、IP ソース ガードがトランク ポートに設定されていて特定の VLAN で着信するトラフィックではこのチェックを行いたくない場合（それらで DHCP スヌーピングがイネーブルにされていない場合であっても）、除外したい VLAN のリストを指定できます。

### 始める前に

DHCP 機能および DHCP スヌーピングがイネーブルにされていることを確認します。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>[no] ip dhcp snooping ipsg-excluded vlan vlan-list</b> 例： switch(config)# ip dhcp snooping ipsg-excluded vlan 1001-1256,3097	トランク ポートの IP ソース ガードで DHCP スヌーピングのチェックから除外したい VLAN のリストを指定します。
ステップ 3	(任意) <b>show ip ver source [ethernet slot/port   port-channel channel-number]</b> 例： switch(config)# show ip ver source	どの VLAN が除外されるかを表示します。
ステップ 4	(任意) <b>copy running-config startup-config</b> 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。

## IP ソース ガード バインディングの表示

**show ip ver source [ethernet slot/port | port-channel channel-number]** を使用します コマンドを使用して、IP-MAC アドレスのバインディングを表示します。

## IP ソース ガードの統計情報のクリア

IP ソース ガードの統計情報のクリアを行うには、次の表に示すコマンドを使用します。

コマンド	目的
<b>clear access-list ipsg stats [instance number   module number]</b>	IP ソース ガードの統計情報をクリアします。



## 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
  show ip ver source
```

```
IP source guard excluded vlans:
```

```
-----
None
```

```
-----
IP source guard is enabled on the following interfaces:
```

```
-----
ethernet2/3
```

## その他の参考資料

### 関連資料

関連項目	マニュアル タイトル
ACL TCAM リージョン	<a href="#">IP ACL の設定</a>
『DHCP and DHCP snooping』	<a href="#">DHCP の設定 (445 ページ)</a>





## 第 20 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。

- [AES パスワード暗号化およびプライマリ暗号キーについて \(543 ページ\)](#)
- [パスワード暗号化の注意事項と制約事項 \(544 ページ\)](#)
- [パスワード暗号化のデフォルト設定 \(545 ページ\)](#)
- [パスワード暗号化の設定 \(545 ページ\)](#)
- [パスワード暗号化の設定の確認 \(549 ページ\)](#)
- [パスワード暗号化の設定例 \(549 ページ\)](#)

## AES パスワード暗号化およびプライマリ暗号キーについて

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有効にし、パスワード暗号化および復号化に使用されるプライマリ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プライマリ 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

- [プライマリ キーの設定および AES パスワード暗号化機能の有効化 \(545 ページ\)](#)
- [グローバル RADIUS キーの設定 \(66 ページ\)](#)
- [特定の RADIUS サーバ用のキーの設定 \(67 ページ\)](#)
- [グローバル TACACS+ キーの設定 \(98 ページ\)](#)
- [特定の TACACS+ サーバ用のキーの設定 \(99 ページ\)](#)

[プライマリ キーの設定および AES パスワード暗号化機能の有効化](#) (545 ページ)

## 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、およびプライマリ キーを設定できるのは、管理者権限 (`network-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、ロールバックに準拠していません。
- プライマリ キーがなくても AES パスワード暗号化機能を有効にできますが、プライマリ 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。
- TACACS+ の場合、AES パスワード暗号化機能をイネーブルにし、プライマリキーを設定した後、**encryption re-encrypt obfuscated** コマンドを実行して、パスワードをタイプ 6 暗号化パスワードに変換する必要があります。
- プライマリ キーを削除するとタイプ 6 暗号化が停止され、同じプライマリ 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。
- 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プライマリ キーを設定します。
- タイプ 6 暗号化は、MACsec キーチェーンでのみサポートされます。レガシー RPM または cloudsec キーではサポートされません。
- Cisco NX-OS リリース 9.3(6) 以降、タイプ 6 暗号化パスワードを元の状態に戻すことは、MACsec キーチェーンではサポートされていません。
- タイプ 6 暗号化は、AES パスワード暗号化機能が有効で、プライマリ キーが設定されている場合にのみ設定できます。
- プライマリ キーが設定され、AES パスワード暗号化機能がスイッチでイネーブルになっている場合、キーチェーン `infra` の下の各 MACsec キー ストリング設定は、タイプ 6 暗号化で自動的に暗号化されます。
- プライマリ キーの設定は、スイッチに対してローカルです。あるスイッチからタイプ 6 に設定された実行データを取得し、別のプライマリ キーが設定されている別のスイッチに適用すると、新しいスイッチでの復号化は失敗します。
- タイプ 6 暗号化の後にスタートアップ コンフィギュレーションを消去し、コンフィギュレーション置換機能を使用すると、プライマリ キーが PSS に保存されないため、コンフィギュレーションの置換は失敗します。したがって、MACsec タイプ 6 暗号化キー文字列の設定が失われます。

- タイプ 6 のキーを設定すると、SKSD が提供する復号コマンドを適用しないと、既存のタイプ 6 の暗号化キー文字列をタイプ 7 の暗号化キー文字列に変更できません。
- タイプ 6 暗号化がサポートされていない古いイメージでコールドリブートによってシステムをダウングレードする場合は、コールドリブートを続行する前に設定を削除する必要があります。これを行わないと、設定が失われます。
- システムをダウングレードすると、タイプ 6 の設定は失われます。
- ISSD によってシステムをダウングレードすると、機能確認チェックが呼び出され、ダウングレードに進む前に設定を削除するように通知されます。**encryption crypto** コマンドを使用して、タイプ 6 暗号化キーをタイプ 7 暗号化キーに変換してから、ダウングレードを続行できます。
- ISSU のアップグレード中に、タイプ 7 暗号化キーを含む古いイメージからタイプ 6 暗号化をサポートする新しいイメージに移行する場合、再暗号化が強制されるまで、rpm は既存のキーをタイプ 6 暗号化キーに変換しません。再暗号化を適用するには、**encryption re-encrypt obfuscated** コマンドを使用します。
- タイプ 6 暗号化の後にプライマリ キーを変更すると、既存のタイプ 6 暗号化キー文字列に対する復号コマンドは失敗します。既存のタイプ 6 キースtring を削除し、新しいキースtring を設定する必要があります。

## 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 40: 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
プライマリ キー	設定なし

## 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。

### プライマリ キーの設定および AES パスワード暗号化機能の有効化

タイプ 6 暗号化用のプライマリ 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有効にすることができます。

## Procedure

	Command or Action	Purpose
ステップ 1	<b>[no] key config-key ascii</b> <b>Example:</b> <pre>switch# key config-key ascii New Master Key: Retype Master Key:</pre>	<p>プライマリ キーを、AES パスワード暗号化機能で使用するよう設定します。プライマリ 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 <b>no</b> 形式を使用すると、いつでもプライマリ キーを削除できます。</p> <p>プライマリ キーを設定する前に AES パスワード暗号化機能を有効にすると、プライマリ 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。プライマリ キーがすでに設定されている場合は、新しいプライマリ キーを入力する前に現在のプライマリ キーを入力するように求められます。</p>
ステップ 2	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>[no] feature password encryption aes</b> <b>Example:</b> <pre>switch(config)# feature password encryption aes</pre>	AES パスワード暗号化機能をイネーブまたはディセーブルにします。
ステップ 4	<b>encryption re-encrypt obfuscated</b> <b>Example:</b> <pre>switch(config)# encryption re-encrypt obfuscated</pre>	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。
ステップ 5	<b>(Optional) show encryption service stat</b> <b>Example:</b> <pre>switch(config)# show encryption service stat</pre>	AES パスワード暗号化機能とプライマリ キーの設定ステータスを表示します。
ステップ 6	<b>copy running-config startup-config</b> <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	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。

	Command or Action	Purpose
		<b>Note</b> 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プライマリキーを同期するために必要です。

**Related Topics**

[AES パスワード暗号化およびプライマリ暗号キーについて](#) (543 ページ)

[AES パスワード暗号化およびプライマリ暗号キーについて](#) (543 ページ)

[キーのテキストの設定](#) (556 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](#) (558 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。

**Before you begin**

AES パスワード暗号化機能を有効にし、プライマリキーを設定したことを確認します。

**Procedure**

	Command or Action	Purpose
ステップ1	<b>encryption re-encrypt obfuscated</b>  <b>Example:</b> 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。この機能は、macsec キーチェーンではサポートされていません。

**Before you begin**

プライマリキーを設定したことを確認します。

**Procedure**

	Command or Action	Purpose
ステップ1	<b>encryption decrypt type6</b>  <b>Example:</b>	タイプ6暗号化パスワードを元の状態に変換します。

	Command or Action	Purpose
	switch# encryption decrypt type6 Please enter current Master Key:	

## MACsec キーでのタイプ 6 暗号化のイネーブル化

Advanced Encryption Standard (AES) パスワード暗号化機能とも呼ばれるタイプ 6 暗号化機能を使用すると、タイプ 6 暗号化形式で MACsec キーを安全に保存できます。

Cisco NX-OS リリース 9.3(5) 以降では、MACsec 機能をサポートするすべての Cisco Nexus 9000 シリーズ スイッチに、タイプ 6 暗号化形式で MACsec キーを保存できます。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>[no] key config-key ascii</b> 例： switch(config)# key config-key ascii switch(config)# New Master Key: Switch(config)# Retype Master Key:	スイッチのマスターキーを設定します。
ステップ 3	<b>[no] feature password encryption aes</b> 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	<b>key chain name macsec</b> 例： switch(config)# key chain 1 macsec switch(config-macseckeychain)#	MACSec キーチェーンを作成して MACSec キーのセットを保持し、MACSec キーチェーン設定モードを開始します。
ステップ 5	<b>key key-id</b> 例： switch(config-macseckeychain)# key 1000 switch(config-macseckeychain-macseckey)#	MAC secキーを作成し、MACsec キー設定モードを開始します。範囲は 1 ~ 32 オクテットで、最大サイズは 64 です。AES_128 は 32 ビットで使用され、AES_256 は 64 ビットで使用されます。
ステップ 6	<b>key-octet-string octet-string cryptographic-algorithm {AES_128_CMAC   AES_256_CMAC}</b> 例：	そのキーの octet スtring を設定します。octet-string 引数には、最大 64 文字の 16 進数文字を含めることができます。オクテット キーは内部でエンコードされるため、 <b>show running-config</b>



	コマンドまたはアクション	目的
	<pre>switch(config-macseckeychain-macseckey) # key-octet-string abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789 cryptographic-algorithm AES_256_CMAC</pre>	<p><b>macsec</b> コマンドの出力にクリア テキストのキーが現れることはありません。</p> <p>キーオクテット文字列には、次のものが含まれます。</p> <ul style="list-style-type: none"> <li>• 0 暗号化タイプ - 暗号化なし (デフォルト)</li> <li>• 6 Encryption Type-Proprietary (Type-6 encrypted)</li> <li>• 7 暗号化タイプ - 最大 64 文字の、独自仕様 WORD キー オクテット文字列</li> </ul>

## 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。

### Procedure

	Command or Action	Purpose
ステップ 1	<p><b>encryption delete type6</b></p> <p><b>Example:</b></p> <pre>switch# encryption delete type6</pre>	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
<b>show encryption service stat</b>	AES パスワード暗号化機能とプライマリ キーの設定ステータスを表示します。

## パスワード暗号化の設定例

次に、プライマリ 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=="
```



## 第 21 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。

- キーチェーン管理について, [on page 551](#)
- キーチェーン管理の前提条件, [on page 552](#)
- キーチェーン管理の注意事項と制約事項 (552 ページ)
- キーチェーン管理のデフォルト設定, [on page 553](#)
- キーチェーン管理の設定, [on page 553](#)
- アクティブなキーのライフタイムの確認, [on page 561](#)
- キーチェーン管理の設定の確認, [on page 561](#)
- キーチェーン管理の設定例, [on page 561](#)
- 次の作業, [on page 561](#)
- キーチェーン管理に関する追加情報, [on page 562](#)

## キーチェーン管理について

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 9000 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。

**Table 41:** 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tring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。

#### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	<b>key chain name</b> <b>Example:</b> switch(config)# key chain bgp-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	(Optional) <b>show key chain name</b> <b>Example:</b> switch(config-keychain)# show key chain bgp-keys	キーチェーンの設定を表示します。

	Command or Action	Purpose
ステップ 4	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> switch(config-keychain)# 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。

## 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。



**Note** 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。

### Before you begin

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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b>  <b>Example:</b> 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	<b>no key chain name</b>  <b>Example:</b> switch(config)# no key chain bgp-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	(Optional) <b>show key chain name</b>  <b>Example:</b> switch(config-keychain)# show key chain bgp-keys	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	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> switch(config-keychain)# 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。

## プライマリ キーの設定および AES パスワード暗号化機能の有効化

タイプ6暗号化用のプライマリ 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有効にすることができます。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>[no] key config-key ascii</b> <b>Example:</b> <pre>switch# key config-key ascii New Master Key: Retype Master Key:</pre>	<p>プライマリ キーを、AES パスワード暗号化機能で使用するよう設定します。プライマリ 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 <b>no</b> 形式を使用すると、いつでもプライマリ キーを削除できます。</p> <p>プライマリ キーを設定する前に AES パスワード暗号化機能を有効にすると、プライマリ 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。プライマリ キーがすでに設定されている場合は、新しいプライマリ キーを入力する前に現在のプライマリ キーを入力するように求められます。</p>
ステップ 2	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>[no] feature password encryption aes</b> <b>Example:</b> <pre>switch(config)# feature password encryption aes</pre>	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	<b>encryption re-encrypt obfuscated</b> <b>Example:</b> <pre>switch(config)# encryption re-encrypt obfuscated</pre>	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。
ステップ 5	<b>(Optional) show encryption service stat</b> <b>Example:</b> <pre>switch(config)# show encryption service stat</pre>	AES パスワード暗号化機能とプライマリ キーの設定ステータスを表示します。

	Command or Action	Purpose
ステップ 6	<b>copy running-config startup-config</b> <b>Example:</b> <pre>switch(config)# copy running-config startup-config</pre>	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。 <b>Note</b> 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プライマリ キーを同期するために必要です。

### Related Topics

- [AES パスワード暗号化およびプライマリ暗号キーについて \(543 ページ\)](#)
- [AES パスワード暗号化およびプライマリ暗号キーについて \(543 ページ\)](#)
- [キーのテキストの設定 \(556 ページ\)](#)
- [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 \(558 ページ\)](#)

## 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。

### Before you begin

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の方が便利です。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル コンフィギュレーション モードを開始します。



	Command or Action	Purpose
ステップ 2	<b>key chain name</b> <b>Example:</b> <pre>switch(config)# key chain bgp-keys switch(config-keychain)#</pre>	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	<b>key key-ID</b> <b>Example:</b> <pre>switch(config-keychain)# key 13 switch(config-keychain-key)#</pre>	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。 <i>key-ID</i> 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	<b>key-string [encryption-type] text-string</b> <b>Example:</b> <pre>switch(config-keychain-key)# key-string 0 AS3cureString</pre>	<p>そのキーのテキスト スtring を設定します。 <i>key-ID</i> 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。</p> <p><i>encryption-type</i> 引数に、次のいずれかの値を指定します。</p> <ul style="list-style-type: none"> <li>• 0 : 入力する <i>text-string</i> 引数は暗号化されていないテキストです。これがデフォルトです。</li> <li>• 7 : 入力する <i>text-string</i> 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 デバイス上で実行した <b>show key chain</b> コマンドの暗号化出力に基づいて、テキスト文字列を入力する場合に役立ちます。</li> </ul>
ステップ 5	(Optional) <b>show key chain name [mode decrypt]</b> <b>Example:</b> <pre>switch(config-keychain-key)# show key chain bgp-keys</pre>	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 <b>mode decrypt</b> 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	(Optional) <b>copy running-config startup-config</b> <b>Example:</b> <pre>switch(config-keychain-key)# copy running-config startup-config</pre>	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。

### Related Topics

[プライマリ キーの設定および AES パスワード暗号化機能の有効化](#) (545 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。



**Note** 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。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> <pre>switch# configure terminal switch(config)#</pre>	グローバル 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	<b>key chain name</b> <b>Example:</b> <pre>switch(config)# key chain bgp-keys switch(config-keychain)#</pre>	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	<b>key key-ID</b> <b>Example:</b> <pre>switch(config-keychain)# key 13 switch(config-keychain-key)#</pre>	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	<b>accept-lifetime [local] start-time duration duration-value   infinite   end-time]</b> <b>Example:</b> <pre>switch(config-keychain-key)# accept-lifetime 00:00:00 Jun 13 2013 23:59:59 Sep 12 2013</pre>	<p>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 <i>start-time</i> および <i>end-time</i> 引数を UTC として扱います。 <b>local</b> 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。</p> <p><i>start-time</i> 引数は、キーがアクティブになる日時です。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• <b>duration duration-value</b> : ライフタイムの長さ (秒)。最大値は 2147483646 秒 (約 68 年) です。</li> <li>• <b>infinite</b> : キーの受け入れライフタイムは期限切れになりません。</li> </ul>

	Command or Action	Purpose
		<ul style="list-style-type: none"> <li>• <i>end-time</i> : The <i>end-time</i> 引数はキーがアクティブでなくなる日時です。</li> </ul>
ステップ 5	<b>send-lifetime</b> [ <b>local</b> ] <i>start-time</i> <b>duration</b> <i>duration-value</i>   <b>infinite</b>   <i>end-time</i>  <b>Example:</b> <pre>switch(config-keychain-key) # send-lifetime 00:00:00 Jun 13 2013 23:59:59 Aug 12 2013</pre>	<p>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 <i>start-time</i> および <i>end-time</i> 引数を UTC として扱います。 <b>local</b> 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。</p> <p><i>start-time</i> 引数は、キーがアクティブになる日時です。</p> <p>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。</p> <ul style="list-style-type: none"> <li>• <b>duration</b> <i>duration-value</i> : ライフタイムの長さ (秒)。最大値は 2147483646 秒 (約 68 年) です。</li> <li>• <b>infinite</b> : キーの送信ライフタイムは期限切れになりません。</li> <li>• <i>end-time</i> : The <i>end-time</i> 引数はキーがアクティブでなくなる日時です。</li> </ul>
ステップ 6	(Optional) <b>show key chain name</b> [ <b>mode decrypt</b> ]  <b>Example:</b> <pre>switch(config-keychain-key) # show key chain bgp-keys</pre>	<p>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 <b>mode decrypt</b> 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。</p>
ステップ 7	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b> <pre>switch(config-keychain-key) # copy running-config startup-config</pre>	<p>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。</p>

**Related Topics**

[プライマリ キーの設定および AES パスワード暗号化機能の有効化](#) (545 ページ)

## OSPFv2 暗号化認証用のキーの設定

OSPFv2 については、Message Digest 5 (MD5) またはハッシュベースの Message Authentication Code Secure Hash Algorithm (HMAC-SHA) 認証を設定できます。

## 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>key chain name</b> 例： switch(config)# key chain bgp-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	<b>key key-ID</b> 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。 <i>key-ID</i> 引数は、0～65535 の整数で指定する必要があります。  (注) OSPFv2 の場合、key key-id コマンドのキー ID の値は 0～255 です。
ステップ 4	<b>[no] cryptographic-algorithm {HMAC-SHA-1   HMAC-SHA-256   HMAC-SHA-384   HMAC-SHA-512   MD5}</b> 例： switch(config-keychain-key)# cryptographic-algorithm HMAC-SHA-1	指定したキーに使用する OSPFv2 暗号化 アルゴリズムを設定します。1つのキーに設定できる暗号化アルゴリズムは1つだけです。
ステップ 5	(任意) <b>show key chain name</b> 例： switch(config-keychain-key)# show key chain bgp-keys	キーチェーン コンフィギュレーション を表示します。
ステップ 6	(任意) <b>copy running-config startup-config</b> 例： switch(config-keychain-key)# 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。

## 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。

コマンド	目的
<b>show key chain</b>	デバイスで設定された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。

コマンド	目的
<b>show key chain name</b>	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

bgp 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 bgp-keys
  key 0
    key-string 7 zqdest
    accept-lifetime 00:00:00 Jun 01 2013 23:59:59 Sep 12 2013
    send-lifetime 00:00:00 Jun 01 2013 23:59:59 Aug 12 2013
  key 1
    key-string 7 uaegdyto
    accept-lifetime 00:00:00 Aug 12 2013 23:59:59 May 12 2013
    send-lifetime 00:00:00 Sep 12 2013 23:59:59 Aug 12 2013
  key 2
    key-string 7 eekgsdyd
    accept-lifetime 00:00:00 Nov 12 2013 23:59:59 Mar 12 2013
    send-lifetime 00:00:00 Dec 12 2013 23:59:59 Feb 12 2013
```

## 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 9000 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
ボーダーゲートウェイプロトコル	『Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide』
OSPFv2	『Cisco Nexus 9000 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。	—



## 第 22 章

# ユニキャスト RPF の設定

この章では、Cisco NX-OS デバイスで unicast reverse path forwarding (uRPF) を設定する方法を説明します。

この章は、次の項で構成されています。

- [ユニキャスト RPF について, on page 563](#)
- [ユニキャスト RPF の注意事項と制約事項 \(565 ページ\)](#)
- [ユニキャスト RPF のデフォルト設定, on page 568](#)
- [-R ラインカードを搭載した Cisco Nexus 9500 スイッチのユニキャスト RPF の設定, on page 568](#)
- [Cisco Nexus 9300 スイッチのユニキャスト RPF の設定 \(569 ページ\)](#)
- [ユニキャスト RPF の設定例, on page 572](#)
- [ユニキャスト RPF の設定の確認, on page 573](#)
- [ユニキャスト RPF に関する追加情報, on page 573](#)

## ユニキャスト RPF について

ユニキャスト 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 IPv4 または IPv6 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 IPv4 または IPv6 パケット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 を有効にすると、スイッチ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。



**Note** 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 エンドにあるスイッチ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、スイッチ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（リターンルート）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。



**Note** 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) バリエーションが使用されていて、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。



**Caution** 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ため、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。

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 RPF 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。

## ユニキャスト RPF の注意事項と制約事項

ユニキャスト RPF (uRPF) に関する注意事項と制約事項は次のとおりです。

- uRPF は、次のプラットフォームでサポートされています。
  - N9K-X9636C-R と N9K-X9636Q-R ラインカード搭載の Cisco Nexus 9500 シリーズ スイッチ
  - N9K-X9636C-RX ラインカード搭載の Cisco Nexus 9500 シリーズ スイッチ
  - Cisco Nexus 9300 プラットフォーム スイッチ (9300-FXP スイッチを除く)
- Cisco NX-OS リリース 9.2(1) 以降、uRPF は次でサポートされます。
  - Cisco Nexus 9300-EX シリーズ スイッチ (IPv4 のみ)
  - Cisco Nexus 9300-FX/FX2 シリーズ スイッチ (IPv4 および IPv6)
- Cisco NX-OS リリース 9.3(5) 以降、uRPF は Cisco Nexus 9300-FX3 プラットフォーム スイッチ (IPv4 および IPv6) でサポートされます。
- Cisco Nexus リリース 9.3(1) 以降、uRPF はモジュラ EX/FX ラインカードファミリの Cisco Nexus 9500 シリーズ スイッチでサポートされています (『[Cisco Nexus 9500 Cloud-Scale Line Cards and Fabric Modules Data Sheet](#)』を参照)。



(注) モジュラ EX/FX ラインカードの uRPF は、DUAL STACK MCAST ルーティングモードでのみサポートされます。uRPF をイネーブルにする前に、`system routing template-dual-stack-mcast` の設定を指定します。DUAL STACK MCAST ルーティング モードの設定方法については、『[Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide](#)』を参照してください。

- uRPF 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 uRPF 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 uRPF 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 uRPF 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にわたって uRPF を展開するエンティティ数が増えるほど、インターネットコミュニティ全体の大規模なネットワークの中断を軽減できる可能性と、攻撃元を追跡できる可能性が高くなります。
- uRPF 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 uRPF 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 uRPF を設定する必要があります。
- uRPF 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。
- uRPF は、ネットワーク内部のインターフェイスに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あります。uRPF 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。
- uRPF 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。
- Cisco NX-OS リリース 9.2(1) 以降、N9K-X9636C-R および N9K-X96136YC-R スイッチでは、使用可能な IPv4 および IPv6 ユニキャスト RPF コマンドのバージョンは 1 つだけです。ただし、これにより、IPv4 と IPv6 の両方でユニキャスト RPF が有効になります。
- 次のガイドラインと制限は、N9K-X9636C-R、N9K-X9636C-RX、または N9K-X9636Q-R ラインカードを搭載した Cisco Nexus 9500 シリーズ スイッチにのみ適用されます。
  - 厳密な uRPF を機能させるには、入力インターフェイスと送信元 IP アドレスが学習されたインターフェイスで有効にします。
  - スイッチ ハードウェアは、設定されたルーティング インターフェイスごとに厳密な uRPF を実装しません。
  - 厳密な uRPF は、厳密な uRPF 対応インターフェイスの学習ルートごとに実装されません。

- ルートが ECMP として解決されると、strict uRPF はルーズモードにフォールバックします。
- トラップ解決に関するハードウェアの制限により、uRPF はインバンド経由でスーパーバイザ宛パケットに適用されない場合があります。
- IP トラフィックの場合は、IPv4 と IPv6 の設定を同時に有効にします。
- ハードウェアの制限により、N9K-X9636C-R、N9K-X9636C-RX、および N9K-X9636Q-R ラインカードは次の組み合わせのみをサポートします。

uRPF の設定		送信元 IP アドレスのトラフィックチェックの適用			
IPv4	IPv6	IP Unipath	IP ECMP	MPLS Encap/VPN/ECMP	N9K-X9636C-RX ラインカードの Unipath MPLS VPN
無効	無効	許可 (Allow)	許可 (Allow)	許可 (Allow)	許可 (Allow)
Loose	Loose	uRPF loose	uRPF loose	uRPF loose	uRPF strict
strict	strict	uRPF strict	uRPF loose	uRPF loose	uRPF strict

- Strict uRPF は、宛先インターフェイスが次の Cisco NX-OS デバイスの ICMPv6 NA パケットを受信した場合でも、ICMPv6 NA パケットを廃棄します。
  - ラインカード : N9K-X9564PX、N9K-X9564TX、N9K-X9536PQ、X9408PC-CFP2、X9464TX、X9464TX2
  - アップリンク モジュール : N9K-M12PQ
  - スイッチ : 93128TX、9396PX、9396TX、9372PX、9372PX-E、3164Q、31128PQ
- Strict uRPF は、次のプラットフォームの VxLAN 経由でインターフェイスに送信される ICMP トラフィックをブロックします。
  - Cisco Nexus 9200 プラットフォーム スイッチ
  - Cisco Nexus 9300--EX/FX/GX プラットフォーム スイッチ
  - N9K-X9700-EX および N9K-X9700-FX ラインカードを搭載した Nexus 9500 スイッチ

## 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。

Table 42: 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
ユニキャスト RPF	ディセーブル

## -R ラインカードを搭載した Cisco Nexus 9500 スイッチのユニキャスト RPF の設定

-R ラインカードを使用して Cisco Nexus 9500 シリーズ スイッチの入力インターフェイスにユニキャスト RPF を設定できます。

### Procedure

	Command or Action	Purpose
ステップ 1	<b>configure terminal</b> <b>Example:</b> 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	<b>interface ethernet slot/port</b> <b>Example:</b> 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。
ステップ 3	<b>{ip   ipv6} address ip-address/length</b> <b>Example:</b> switch(config-if)# ip address 172.23.231.240/23	インターフェイスの IPv4 または IPv6 アドレスを指定します。
ステップ 4	<b>{ip   ipv6} verify unicast source reachable-via any</b> <b>Example:</b> switch(config-if)# ip verify unicast source reachable-via any	IPv4 と IPv6 の両方に対するインターフェイスでユニキャスト RPF を設定します。

	Command or Action	Purpose
		<b>Note</b> IPv4 または IPv6 の uRPF をイネーブルにすると ( <b>ip</b> または <b>ipv6</b> キーワードを使用)、uRPF は IPv4 と IPv6 の両方でイネーブルになります。
ステップ 5	(Optional) <b>show ip interface ethernet slot/port</b>  <b>Example:</b>  switch(config)# show ip interface ethernet 2/3	インターフェイスの IP 情報を表示します。
ステップ 6	(Optional) <b>show running-config interface ethernet slot/port</b>  <b>Example:</b>  switch(config)# show running-config interface ethernet 2/3	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 7	(Optional) <b>copy running-config startup-config</b>  <b>Example:</b>  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。

## Cisco Nexus 9300 スイッチのユニキャスト RPF の設定

Cisco NX-OS リリース 9.2(1) 以降を実行する Cisco Nexus 9300 プラットフォーム スイッチ (9300-FXP スイッチを除く) の入力インターフェイスで、次のいずれかのユニキャスト RPF モードを設定できます。

### 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

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>[no] system urpf disable</b> 例： switch(config)# no system urpf disable	スイッチでユニキャスト RPF をイネーブルにします。  (注) ユニキャスト RPF 設定を適用するには、Cisco NX-OS ボックスをリロードする必要があります。
ステップ 3	<b>interface ethernet slot/port</b> 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 4	<b>{ip   ipv6} address ip-address/length</b> 例： switch(config-if)# ip address 172.23.231.240/23	インターフェイスの IPv4 または IPv6 アドレスを指定します。
ステップ 5	<b>{ip   ipv6} verify unicast source reachable-via {any [allow-default]   rx}</b> 例： switch(config-if)# ip verify unicast source reachable-via any	IPv4 および IPv6 用インターフェイスにユニキャスト RPF を設定します。  Cisco Nexus 9300-EX シリーズ スイッチ (IPv4 用) と Cisco Nexus 9300-FX/FX2 シリーズ スイッチでは、IPv4 および IPv6 uRPF を個別に有効にできます。

	コマンドまたはアクション	目的
		<p>(注) IPv4 または IPv6 のユニキャスト RPF をイネーブルにすると (<b>ip</b> または <b>ipv6</b> キーワードを使用)、ユニキャスト RPF は IPv4 と IPv6 の両方でイネーブルになります。</p> <p>インターフェイスで使用できる IPv4 および IPv6 ユニキャスト RPF コマンドのバージョンは1つだけです。1つのバージョンを設定する場合、すべてのモード変更はこのバージョンで行う必要があります、他のすべてのバージョンはそのインターフェイスによってブロックされます。</p> <ul style="list-style-type: none"> <li>• <b>any</b> キーワードは緩和モードのユニキャスト RPF を指定します。</li> <li>• <b>allow-default</b> 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であり、これを検証に使用できます。</li> </ul> <p>(注) <b>allow-default</b> キーワードは、ALPM ルーティングモードでは適用されません。</p> <p>(注) <b>allow-default</b> キーワードを指定しない場合、送信元アドレス ルックアップ (ルーズなユニキャスト RPF チェックの場合) はデフォルト ルートと一致しません。</p> <ul style="list-style-type: none"> <li>• <b>rx</b> 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。</li> </ul>
ステップ 6	<b>exit</b> 例 :	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
	switch(config-if)# exit switch(config)#	
ステップ 7	(任意) <b>show ip interface ethernet slot/port</b>  例： switch(config)# show ip interface ethernet 1/54   grep -i "unicast reverse path forwarding" IP unicast reverse path forwarding: none	インターフェイスの IP 情報を表示し、ユニキャスト RPF がイネーブルかどうかを確認します。
ステップ 8	(任意) <b>show running-config interface ethernet slot/port</b>  例： switch(config)# show running-config interface ethernet 2/3	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 9	(任意) <b>copy running-config startup-config</b>  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。

## ユニキャスト RPF の設定例

次に、-R ラインカードを搭載した Cisco Nexus 9500 シリーズスイッチで IPv4 パケットの loose ユニキャスト RPF を設定する例を示します。

```
interface Ethernet2/3
 ip address 172.23.231.240/23
 ip verify unicast source reachable-via any
```

次に、-R ラインカードを搭載した Cisco Nexus 9500 シリーズスイッチで IPv6 パケットの loose ユニキャスト RPF を設定する例を示します。

```
interface Ethernet2/1
 ipv6 address 2001:0DB8:c18:1::3/64
 ipv6 verify unicast source reachable-via any
```

次に、Cisco Nexus 9300 プラットフォームスイッチで IPv4 パケットの loose ユニキャスト RPF を設定する例を示します。

```
no system urpf disable
interface Ethernet2/3
 ip address 172.23.231.240/23
 ip verify unicast source reachable-via any
```



次に、Cisco Nexus 9300 プラットフォーム スイッチで IPv6 パケットの loose ユニキャスト RPF を設定する例を示します。

```
no system urpf disable
interface Ethernet2/1
  ipv6 address 2001:0DB8:c18:1::3/64
  ipv6 verify unicast source reachable-via any
```

次に、Cisco Nexus 9300 プラットフォーム スイッチで IPv4 パケットの strict ユニキャスト RPF を設定する例を示します。

```
no system urpf disable
interface Ethernet2/2
  ip address 172.23.231.240/23
  ip verify unicast source reachable-via rx
```

次に、Cisco Nexus 9300 プラットフォーム スイッチで IPv6 パケットの strict ユニキャスト RPF を設定する例を示します。

```
no system urpf disable
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、次のいずれかの操作を行います。

コマンド	目的
<code>show running-config interface ethernet slot/port</code>	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。
<code>show running-config ip [all]</code>	実行コンフィギュレーション内の IPv4 設定を表示します。
<code>show running-config ipv6 [all]</code>	実行コンフィギュレーション内の IPv6 設定を表示します。
<code>show startup-config interface ethernet slot/port</code>	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。
<code>show startup-config ip</code>	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。

## 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
データ管理エンジン (DME) コマンド	<a href="#">Cisco Nexus 3000 and 9000 Series NX-API REST SDK User Guide and API Reference</a> (Cisco Nexus 3000 および 9000 シリーズ NX-API REST SDK ユーザ ガイドと API リファレンス)
MPLS VPN	<a href="#">Cisco Nexus 9000 シリーズ NX-OS レイヤ 2 スイッチング コンフィギュレーション ガイド</a> (Cisco Nexus 9000 Series NX-OS Layer 2 Switching Configuration Guide)



## 第 23 章

# スイッチポート ブロッキングの設定

この章では、Cisco NX-OS デバイス上でスイッチポートブロッキング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。

- [スイッチポートブロッキングについて \(575 ページ\)](#)
- [スイッチポートブロッキングの注意事項および制約事項 \(575 ページ\)](#)
- [スイッチポートブロッキングのデフォルト設定 \(576 ページ\)](#)
- [スイッチポートブロッキングの設定 \(576 ページ\)](#)
- [スイッチポートブロッキング設定の確認 \(577 ページ\)](#)
- [スイッチポートブロッキングの設定例 \(577 ページ\)](#)

## スイッチポート ブロッキングについて

MAC アドレスが期限切れになるか、スイッチによって学習されなかったために、不明のマルチキャストまたはユニキャストトラフィックがスイッチポートにフラッドिंगすることがあります。不明なマルチキャストおよびユニキャストトラフィックがスイッチポートに転送されると、セキュリティ問題が発生する可能性があります。スイッチポートブロッキングをイネーブルにすると、マルチキャストまたはユニキャストトラフィックのポートへのフラッドिंगを防止できます。

## スイッチポートブロッキングの注意事項および制約事項

スイッチポートブロッキング設定時の注意事項および制約事項は次のとおりです。

- トラフィックストーム制御が適用されるのは入力ポートだけであるのに対して、スイッチポートブロッキングが適用されるのは出力ポートだけです。
- スwitchポートブロッキングは、すべてのスイッチドポート（PVLANポートを含む）でサポートされ、ポートが転送するすべての VLAN に適用されます。
- スwitchポートブロッキングは FEX ポートではサポートされません。

- ポート チャネルの不明のマルチキャストまたはユニキャストトラフィックをブロックすると、ポート チャネル グループのすべてのポートでブロックされます。
- スイッチポートブロッキングには制御のレベルは用意されていません。指定されたポートにおける未知の出力マルチキャストまたはユニキャストパケットのフラッディングをすべて防止します。
- スイッチポートブロッキングは、Cisco Nexus 9500 シリーズ スイッチの CPU を発信元とする制御パケットをドロップします。Cisco Nexus 9300 シリーズ スイッチのパケットはドロップしません。

## スイッチポート ブロッキングのデフォルト設定

次の表に、スイッチポートブロッキングパラメータのデフォルト設定を示します。

表 43: スイッチポートブロッキングパラメータのデフォルト値

パラメータ	デフォルト
スイッチポートブロッキング	ディセーブル

## スイッチポート ブロッキングの設定

デフォルトでは、スイッチは不明の宛先 MAC アドレスを持つパケットをすべてのポートにフラッディングします。このようなトラフィックの転送を防ぐために、不明のマルチキャストまたはユニキャストパケットをブロックするようにポートを設定できます。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 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	<b>interface {ethernet slot/port   port-channel number}</b> 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。
ステップ 3	<b>[no] switchport block {multicast   unicast}</b> 例：	指定されたインターフェイスにおける未知のマルチキャストまたはユニキャスト

	コマンドまたはアクション	目的
	<code>switch(config-if)# switchport block unicast</code>	パケットのフラッディングを防止します。 このコマンドの <b>no</b> 形式を使用すると、ポートでの通常の転送が再開されます。
ステップ 4	(任意) <b>show interface [ethernet slot/port   port-channel number] switchport</b> 例： <code>switch(config-if)# show interface ethernet 1/1 switchport</code>	スイッチポートブロッキング コンフィギュレーションを表示します。
ステップ 5	(任意) <b>copy running-config startup-config</b> 例： <code>switch(config-if)# copy running-config startup-config</code>	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。

## スイッチポート ブロッキング設定の確認

スイッチポートブロッキング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
<b>show interface switchport</b>	すべてのインターフェイスのスイッチポートブロッキングの設定を表示します。
<b>show interface {ethernet slot/port   port-channel number} switchport</b>	指定されたインターフェイスのスイッチポートブロッキングの設定を表示します。
<b>show running-config interface [ethernet slot/port   port-channel number]</b>	実行コンフィギュレーションのスイッチポートブロッキング設定を表示します。

## スイッチポート ブロッキングの設定例

次に、イーサネットインターフェイス 1/2 上でマルチキャストおよびユニキャストフラッディングをブロックし、設定を確認する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/2
switch(config-if)# switchport block multicast
```

```
switch(config-if)# switchport block unicast
switch(config-if)# show running-config interface ethernet 1/2
!Command: show running-config interface Ethernet1/2
!Time: Wed Apr 15 16:25:48 2015

version 79.2(1)

interface Ethernet1/2
switchport
switchport block multicast
switchport block unicast
```



## 第 24 章

# コントロールプレーンポリシングの設定

この章は、次の項で構成されています。

- [CoPP について, on page 579](#)
- [CoPP の注意事項と制約事項 \(597 ページ\)](#)
- [CoPP のデフォルト設定, on page 601](#)
- [CoPP の設定, on page 601](#)
- [プロトコル ACL フィルタリング \(609 ページ\)](#)
- [CoPP の設定の確認, on page 614](#)
- [CoPP 設定ステータスの表示, on page 617](#)
- [CoPP のモニタリング, on page 617](#)
- [SNMP での CoPP のモニタリング \(618 ページ\)](#)
- [CoPP 統計情報のクリア, on page 618](#)
- [CoPP の設定例, on page 619](#)
- [CoPP に関する追加情報, on page 621](#)

## CoPP について

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 ポリシーに似ており、非管理ポートからスイッチに入る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妨害 (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。Cisco 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。

### コントロールプレーン

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、Cisco 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、管理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、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。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。

DoS 攻撃の例は次のとおりです。

- 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



**Caution**

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、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。

次の例外は、ラインカードからのみ発生する可能性があります。

- match exception ip option
- match exception ipv6 option
- match exception ttl-failure

次の例外は、ファブリック モジュールからのみ発生する可能性があります。

- match exception ipv6 icmp unreachable
- match exception ip icmp unreachable

次の例外は、ラインカードとファブリック モジュールから発生する可能性があります。

- match exception mtu-failure

### 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。

### 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、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。クラスマップとポリシーマップを使用して、パケットの分類およびレート制御ポリシーを設定します。

## 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、または違反する場合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。

### 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。

さらに、一致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 9000 Series NX-OS Quality of Service Configuration Guide』を参照してください。

## ダイナミックおよびスタティック CoPP ACL

CoPP アクセスコントロールリスト (ACL) は、ダイナミックまたはスタティックのいずれかに分類されます。Cisco Nexus 9300 と 9500 シリーズおよび、3164Q、31128PQ、3232C、および 3264Q スイッチでは、ダイナミック CoPP ACL のみ使用します。Cisco Nexus 9200 シリーズ スイッチでは、ダイナミックおよびスタティックの両方の CoPP ACL を使用します。

ダイナミック CoPP ACL は Forwarding Information Base (FIB; 転送情報ベース) ベースのスーパーバイザリダイレクトパケットに対してのみ機能し、スタティック CoPP ACL は ACL ベースのスーパーバイザリダイレクトパケットに対して機能します。ダイナミック CoPP ACL が

サポートされるのは myIP およびリンクローカル マルチキャスト トラフィックであり、スタティック CoPP ACL がサポートされるのは、その他すべてのタイプのトラフィックです。

スタティック CoPP ACL の識別はサブストリングで行われます。こうしたいずれかのサブストリングを持つ ACL は、すべてスタティック CoPP ACL に分類されます。

- MAC ベースのスタティック CoPP ACL サブストリング：
  - acl-mac-cdp-udld-vtp
  - acl-mac-cfsoe
  - acl-mac-dot1x
  - acl-mac-l2-tunnel
  - acl-mac-l3-isis
  - acl-mac-lacp
  - acl-mac-lldp
  - acl-mac-sdp-srp
  - acl-mac-stp
  - acl-mac-undesirable
  
- プロトコル ベースのスタティック CoPP ACL のサブストリング：
  - acl-dhcp
  - acl-dhcp-relay-response
  - acl-dhcp6
  - acl-dhcp6-relay-response
  - acl-ptp
  
- マルチキャスト ベースのスタティック CoPP ACL サブストリング：
  - acl-igmp

スタティック CoPP ACL の詳細については、「[CoPP の注意事項と制約事項 \(597 ページ\)](#)」を参照してください。

## デフォルトのポリシー

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 カラーです。

- **Moderate** : このポリシーは1レート、2カラーです。重要クラスのバーストサイズは **strict** ポリシーより大きく、**lenient** ポリシーより小さくなります。
- **Lenient** : このポリシーは1レート、2カラーです。重要クラスのバーストサイズは **moderate** ポリシーより大きく、**dense** ポリシーより小さくなります。
- **Dense** : このポリシーは1レート、2カラーです。ポリサーの CIR 値は、**strict** ポリシーよりも低くなります。
- **Skip** : コントロールプレーン ポリシーは適用されません（ネットワークのコントロールプレーンに影響するため、**Skip** オプションの使用は推奨されません）。

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。



**Note** POAPを使用する場合、デフォルトでは厳格なポリシングは適用されないため、CoPPポリシーを設定する必要があります。

**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、ソフトウェアをアップグレードしても変更されません。



**Caution** **skip** オプションを選択し、その後に CoPP 保護を設定していない場合、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。

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か、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。

#### Related Topics

[デフォルトの CoPP ポリシーの変更または再適用](#) (608 ページ)

## デフォルトクラス マップ

**copp-system-class-critical** 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-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-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-ospf6
  match access-group name copp-system-p-acl-eigrp6
  match access-group name copp-system-p-acl-auto-rp
```

```
match access-group name copp-system-p-acl-mac-l3-isis
```

**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-exception-diag** 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-diag
  match exception ttl-failure
  match exception mtu-failure
```

**copp-system-class-important** 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-important
  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-hsrp6
  match access-group name copp-system-p-acl-vrrp6
  match access-group name copp-system-p-acl-mac-lldp
```

**copp-system-class-l2-default** 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-l2-default
  match access-group name copp-system-p-acl-mac-undesirable
```

**copp-system-class-l2-unpoliced** 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-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
```

**copp-system-class-l3mc-data** 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-l3mc-data
  match exception multicast rpf-failure
  match exception multicast dest-miss
```

**copp-system-class-l3uc-data** 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-l3uc-data
  match exception glean
```

**copp-system-class-management** 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-management
  match access-group name copp-system-p-acl-ftp
  match access-group name copp-system-p-acl-ntp
  match access-group name copp-system-p-acl-ssh
  match access-group name copp-system-p-acl-http
  match access-group name copp-system-p-acl-ntp6
```

```

match access-group name copp-system-p-acl-sftp
match access-group name copp-system-p-acl-snmp
match access-group name copp-system-p-acl-ssh6
match access-group name copp-system-p-acl-tftp
match access-group name copp-system-p-acl-https
match access-group name copp-system-p-acl-snm6
match access-group name copp-system-p-acl-tftp6
match access-group name copp-system-p-acl-radius
match access-group name copp-system-p-acl-tacacs
match access-group name copp-system-p-acl-telnet
match access-group name copp-system-p-acl-radius6
match access-group name copp-system-p-acl-tacacs6
match access-group name copp-system-p-acl-telnet6

```

**copp-system-class-monitoring** 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-monitoring
  match access-group name copp-system-p-acl-icmp
  match access-group name copp-system-p-acl-icmp6
  match access-group name copp-system-p-acl-traceroute

```

**copp-system-class-multicast-host** 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-multicast-host
  match access-group name copp-system-p-acl-ml6

```

**copp-system-class-multicast-router** 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-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

```

**copp-system-class-nat-flow** 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-nat-flow
  match exception nat-flow

```

**copp-system-class-ndp** 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-ndp
  match access-group name copp-system-p-acl-ndp

```

**copp-system-class-normal** 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-normal
  match access-group name copp-system-p-acl-mac-dot1x
  match protocol arp

```

**copp-system-class-normal-dhcp** 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-normal-dhcp
  match access-group name copp-system-p-acl-dhcp
  match access-group name copp-system-p-acl-dhcp6

```

**copp-system-class-normal-dhcp-relay-response** 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-normal-dhcp-relay-response
  match access-group name copp-system-p-acl-dhcp-relay-response
  match access-group name copp-system-p-acl-dhcp6-relay-response
```

**copp-system-class-normal-igmp** 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-normal-igmp
  match access-group name copp-system-p-acl-igmp
```

**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 access-group name copp-system-p-acl-ntp
```

**copp-system-class-undesirable** 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-undesirable
  match access-group name copp-system-p-acl-undesirable
  match exception multicast sg-rpf-failure
```

**copp-system-class-fcoe** 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-fcoe
  match access-group name copp-system-p-acl-mac-fcoe
```



---

(注) **copp-system-class-fcoe** クラスは Cisco Nexus 9200 シリーズ スイッチではサポートされていません。

---

## strict デフォルト CoPP ポリシー

Cisco Nexus 9200 シリーズ スイッチの場合、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-l3uc-data
    set cos 1
    police cir 800 kbps bc 32000 bytes conform transmit violate drop
  class copp-system-p-class-critical
    set cos 7
    police cir 36000 kbps bc 1280000 bytes conform transmit violate drop
  class copp-system-p-class-important
    set cos 6
    police cir 2500 kbps bc 1280000 bytes conform transmit violate drop
  class copp-system-p-class-multicast-router
    set cos 6
    police cir 2600 kbps bc 128000 bytes conform transmit violate drop
  class copp-system-p-class-management
    set cos 2
    police cir 10000 kbps bc 32000 bytes conform transmit violate drop
  class copp-system-p-class-multicast-host
    set cos 1
    police cir 1000 kbps bc 128000 bytes conform transmit violate drop
  class copp-system-p-class-l3mc-data
    set cos 1
    police cir 2400 kbps bc 32000 bytes conform transmit violate drop
  class copp-system-p-class-normal
    set cos 1
```

```

    police cir 1400 kbps bc 32000 bytes conform transmit violate drop
class copp-system-p-class-ndp
  set cos 6
  police cir 1400 kbps bc 32000 bytes conform transmit violate drop
class copp-system-p-class-normal-dhcp
  set cos 1
  police cir 1300 kbps bc 32000 bytes conform transmit violate drop
class copp-system-p-class-normal-dhcp-relay-response
  set cos 1
  police cir 1500 kbps bc 64000 bytes conform transmit violate drop
class copp-system-p-class-normal-igmp
  set cos 3
  police cir 3000 kbps bc 64000 bytes conform transmit violate drop
class copp-system-p-class-redirect
  set cos 1
  police cir 280 kbps bc 32000 bytes conform transmit violate drop
class copp-system-p-class-exception
  set cos 1
  police cir 150 kbps bc 32000 bytes conform transmit violate drop
class copp-system-p-class-exception-diag
  set cos 1
  police cir 150 kbps bc 32000 bytes conform transmit violate drop
class copp-system-p-class-monitoring
  set cos 1
  police cir 150 kbps bc 128000 bytes conform transmit violate drop
class copp-system-p-class-l2-unpoliced
  set cos 7
  police cir 50 mbps bc 8192000 bytes conform transmit violate drop
class copp-system-p-class-undesirable
  set cos 0
  police cir 200 kbps bc 32000 bytes conform transmit violate drop
class copp-system-p-class-nat-flow
  set cos 7
  police cir 800 kbps bc 64000 bytes conform transmit violate drop
class copp-system-p-class-l2-default
  set cos 0
  police cir 400 kbps bc 32000 bytes conform transmit violate drop
class class-default
  set cos 0
  police cir 400 kbps bc 32000 bytes conform transmit violate drop

```

Cisco Nexus 9300 と 9500 シリーズおよび、3164Q、31128PQ、3232C、および 3264Q スイッチの場合、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-l3uc-data
    set cos 1
    police cir 250 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-critical
    set cos 7
    police cir 19000 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-important
    set cos 6
    police cir 3000 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-multicast-router
    set cos 6
    police cir 3000 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-management
    set cos 2
    police cir 3000 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-multicast-host
    set cos 1
    police cir 2000 pps bc 128 packets conform transmit violate drop

```



```

class copp-system-p-class-l3mc-data
  set cos 1
  police cir 3000 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-normal
  set cos 1
  police cir 1500 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-ndp
  set cos 6
  police cir 1500 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-normal-dhcp
  set cos 1
  police cir 300 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-normal-dhcp-relay-response
  set cos 1
  police cir 400 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-normal-igmp
  set cos 3
  police cir 6000 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-redirect
  set cos 1
  police cir 1500 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-exception
  set cos 1
  police cir 50 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-exception-diag
  set cos 1
  police cir 50 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-monitoring
  set cos 1
  police cir 300 pps bc 128 packets conform transmit violate drop
class copp-system-p-class-l2-unpoliced
  set cos 7
  police cir 20000 pps bc 8192 packets conform transmit violate drop
class copp-system-p-class-undesirable
  set cos 0
  police cir 15 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-fcoe
  set cos 6
  police cir 1500 pps bc 128 packets conform transmit violate drop
class copp-system-p-class-nat-flow
  set cos 7
  police cir 100 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-l2-default
  set cos 0
  police cir 50 pps bc 32 packets conform transmit violate drop
class class-default
  set cos 0
  police cir 50 pps bc 32 packets conform transmit violate drop

```

## moderate デフォルト CoPP ポリシー

Cisco Nexus 9200 シリーズ スイッチの場合、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-l3uc-data
    set cos 1
    police cir 800 kbps bc 32000 bytes conform transmit violate drop
  class copp-system-p-class-critical
    set cos 7
    police cir 36000 kbps bc 1920000 bytes conform transmit violate drop
  class copp-system-p-class-important
    set cos 6
    police cir 2500 kbps bc 1920000 bytes conform transmit violate drop

```

```

class copp-system-p-class-multicast-router
  set cos 6
  police cir 2600 kbps bc 192000 bytes conform transmit violate drop
class copp-system-p-class-management
  set cos 2
  police cir 10000 kbps bc 48000 bytes conform transmit violate drop
class copp-system-p-class-multicast-host
  set cos 1
  police cir 1000 kbps bc 192000 bytes conform transmit violate drop
class copp-system-p-class-l3mc-data
  set cos 1
  police cir 2400 kbps bc 32000 bytes conform transmit violate drop
class copp-system-p-class-normal
  set cos 1
  police cir 1400 kbps bc 48000 bytes conform transmit violate drop
class copp-system-p-class-ndp
  set cos 6
  police cir 1400 kbps bc 48000 bytes conform transmit violate drop
class copp-system-p-class-normal-dhcp
  set cos 1
  police cir 1300 kbps bc 48000 bytes conform transmit violate drop
class copp-system-p-class-normal-dhcp-relay-response
  set cos 1
  police cir 1500 kbps bc 96000 bytes conform transmit violate drop
class copp-system-p-class-normal-igmp
  set cos 3
  police cir 3000 kbps bc 64000 bytes conform transmit violate drop
class copp-system-p-class-redirect
  set cos 1
  police cir 280 kbps bc 48000 bytes conform transmit violate drop
class copp-system-p-class-exception
  set cos 1
  police cir 150 kbps bc 48000 bytes conform transmit violate drop
class copp-system-p-class-exception-diag
  set cos 1
  police cir 150 kbps bc 48000 bytes conform transmit violate drop
class copp-system-p-class-monitoring
  set cos 1
  police cir 150 kbps bc 192000 bytes conform transmit violate drop
class copp-system-p-class-l2-unpoliced
  set cos 7
  police cir 50 mbps bc 8192000 bytes conform transmit violate drop
class copp-system-p-class-undesirable
  set cos 0
  police cir 200 kbps bc 48000 bytes conform transmit violate drop
class copp-system-p-class-nat-flow
  set cos 7
  police cir 800 kbps bc 64000 bytes conform transmit violate drop
class copp-system-p-class-l2-default
  set cos 0
  police cir 400 kbps bc 48000 bytes conform transmit violate drop
class class-default
  set cos 0
  police cir 400 kbps bc 48000 bytes conform transmit violate drop

```

Cisco Nexus 9300 と 9500 シリーズおよび、3164Q、31128PQ、3232C、および 3264Q スイッチの場合、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-l3uc-data
    set cos 1
    police cir 250 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-critical

```

```
set cos 7
police cir 19000 pps bc 192 packets conform transmit violate drop
class copp-system-p-class-important
set cos 6
police cir 3000 pps bc 192 packets conform transmit violate drop
class copp-system-p-class-multicast-router
set cos 6
police cir 3000 pps bc 192 packets conform transmit violate drop
class copp-system-p-class-management
set cos 2
police cir 3000 pps bc 48 packets conform transmit violate drop
class copp-system-p-class-multicast-host
set cos 1
police cir 2000 pps bc 192 packets conform transmit violate drop
class copp-system-p-class-l3mc-data
set cos 1
police cir 3000 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-normal
set cos 1
police cir 1500 pps bc 48 packets conform transmit violate drop
class copp-system-p-class-ndp
set cos 6
police cir 1500 pps bc 48 packets conform transmit violate drop
class copp-system-p-class-normal-dhcp
set cos 1
police cir 300 pps bc 48 packets conform transmit violate drop
class copp-system-p-class-normal-dhcp-relay-response
set cos 1
police cir 400 pps bc 96 packets conform transmit violate drop
class copp-system-p-class-normal-igmp
set cos 3
police cir 6000 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-redirect
set cos 1
police cir 1500 pps bc 48 packets conform transmit violate drop
class copp-system-p-class-exception
set cos 1
police cir 50 pps bc 48 packets conform transmit violate drop
class copp-system-p-class-exception-diag
set cos 1
police cir 50 pps bc 48 packets conform transmit violate drop
class copp-system-p-class-monitoring
set cos 1
police cir 300 pps bc 192 packets conform transmit violate drop
class copp-system-p-class-l2-unpoliced
set cos 7
police cir 20000 pps bc 8192 packets conform transmit violate drop
class copp-system-p-class-undesirable
set cos 0
police cir 15 pps bc 48 packets conform transmit violate drop
class copp-system-p-class-fcoe
set cos 6
police cir 1500 pps bc 192 packets conform transmit violate drop
class copp-system-p-class-nat-flow
set cos 7
police cir 100 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-l2-default
set cos 0
police cir 50 pps bc 48 packets conform transmit violate drop
class class-default
set cos 0
police cir 50 pps bc 48 packets conform transmit violate drop
```

## lenient デフォルト CoPP ポリシー

Cisco Nexus 9200 シリーズ スイッチの場合、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-l3uc-data
    set cos 1
    police cir 800 kbps bc 32000 bytes conform transmit violate drop
  class copp-system-p-class-critical
    set cos 7
    police cir 36000 kbps bc 2560000 bytes conform transmit violate drop
  class copp-system-p-class-important
    set cos 6
    police cir 2500 kbps bc 2560000 bytes conform transmit violate drop
  class copp-system-p-class-multicast-router
    set cos 6
    police cir 2600 kbps bc 256000 bytes conform transmit violate drop
  class copp-system-p-class-management
    set cos 2
    police cir 10000 kbps bc 64000 bytes conform transmit violate drop
  class copp-system-p-class-multicast-host
    set cos 1
    police cir 1000 kbps bc 256000 bytes conform transmit violate drop
  class copp-system-p-class-l3mc-data
    set cos 1
    police cir 2400 kbps bc 32000 bytes conform transmit violate drop
  class copp-system-p-class-normal
    set cos 1
    police cir 1400 kbps bc 64000 bytes conform transmit violate drop
  class copp-system-p-class-ndp
    set cos 6
    police cir 1400 kbps bc 64000 bytes conform transmit violate drop
  class copp-system-p-class-normal-dhcp
    set cos 1
    police cir 1300 kbps bc 64000 bytes conform transmit violate drop
  class copp-system-p-class-normal-dhcp-relay-response
    set cos 1
    police cir 1500 kbps bc 128000 bytes conform transmit violate drop
  class copp-system-p-class-normal-igmp
    set cos 3
    police cir 3000 kbps bc 64000 bytes conform transmit violate drop
  class copp-system-p-class-redirect
    set cos 1
    police cir 280 kbps bc 64000 bytes conform transmit violate drop
  class copp-system-p-class-exception
    set cos 1
    police cir 150 kbps bc 64000 bytes conform transmit violate drop
  class copp-system-p-class-exception-diag
    set cos 1
    police cir 150 kbps bc 64000 bytes conform transmit violate drop
  class copp-system-p-class-monitoring
    set cos 1
    police cir 150 kbps bc 256000 bytes conform transmit violate drop
  class copp-system-p-class-l2-unpoliced
    set cos 7
    police cir 50 mbps bc 8192000 bytes conform transmit violate drop
  class copp-system-p-class-undesirable
    set cos 0
    police cir 200 kbps bc 64000 bytes conform transmit violate drop
  class copp-system-p-class-nat-flow
    set cos 7
    police cir 800 kbps bc 64000 bytes conform transmit violate drop
  class copp-system-p-class-l2-default
    set cos 0

```

```
police cir 400 kbps bc 64000 bytes conform transmit violate drop
class class-default
set cos 0
police cir 400 kbps bc 64000 bytes conform transmit violate drop
```

Cisco Nexus 9300 と 9500 シリーズおよび、3164Q、31128PQ、3232C、および 3264Q スイッチの場合、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-l3uc-data
set cos 1
police cir 250 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-critical
set cos 7
police cir 19000 pps bc 256 packets conform transmit violate drop
class copp-system-p-class-important
set cos 6
police cir 3000 pps bc 256 packets conform transmit violate drop
class copp-system-p-class-multicast-router
set cos 6
police cir 3000 pps bc 256 packets conform transmit violate drop
class copp-system-p-class-management
set cos 2
police cir 3000 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-multicast-host
set cos 1
police cir 2000 pps bc 256 packets conform transmit violate drop
class copp-system-p-class-l3mc-data
set cos 1
police cir 3000 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-normal
set cos 1
police cir 1500 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-ndp
set cos 6
police cir 1500 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-normal-dhcp
set cos 1
police cir 300 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-normal-dhcp-relay-response
set cos 1
police cir 400 pps bc 128 packets conform transmit violate drop
class copp-system-p-class-normal-igmp
set cos 3
police cir 6000 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-redirect
set cos 1
police cir 1500 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-exception
set cos 1
police cir 50 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-exception-diag
set cos 1
police cir 50 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-monitoring
set cos 1
police cir 300 pps bc 256 packets conform transmit violate drop
class copp-system-p-class-l2-unpoliced
set cos 7
police cir 20000 pps bc 8192 packets conform transmit violate drop
class copp-system-p-class-undesirable
set cos 0
police cir 15 pps bc 64 packets conform transmit violate drop
```

```

class copp-system-p-class-fcoe
  set cos 6
  police cir 1500 pps bc 256 packets conform transmit violate drop
class copp-system-p-class-nat-flow
  set cos 7
  police cir 100 pps bc 64 packets conform transmit violate drop
class copp-system-p-class-l2-default
  set cos 0
  police cir 50 pps bc 64 packets conform transmit violate drop
class class-default
  set cos 0
  police cir 50 pps bc 64 packets conform transmit violate drop

```

## デンス デフォルト CoPP ポリシー

Cisco Nexus 9200 シリーズ スイッチの場合、dense 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-l3uc-data
  set cos 1
  police cir 800 kbps bc 32000 bytes conform transmit violate drop
class copp-system-p-class-critical
  set cos 7
  police cir 4500 kbps bc 1280000 bytes conform transmit violate drop
class copp-system-p-class-important
  set cos 6
  police cir 2500 kbps bc 1280000 bytes conform transmit violate drop
class copp-system-p-class-multicast-router
  set cos 6
  police cir 370 kbps bc 128000 bytes conform transmit violate drop
class copp-system-p-class-management
  set cos 2
  police cir 2500 kbps bc 128000 bytes conform transmit violate drop
class copp-system-p-class-multicast-host
  set cos 2
  police cir 300 kbps bc 128000 bytes conform transmit violate drop
class copp-system-p-class-l3mc-data
  set cos 1
  police cir 600 kbps bc 32000 bytes conform transmit violate drop
class copp-system-p-class-normal
  set cos 1
  police cir 1400 kbps bc 128000 bytes conform transmit violate drop
class copp-system-p-class-ndp
  set cos 1
  police cir 350 kbps bc 32000 bytes conform transmit violate drop
class copp-system-p-class-normal-dhcp
  set cos 1
  police cir 750 kbps bc 128000 bytes conform transmit violate drop
class copp-system-p-class-normal-dhcp-relay-response
  set cos 1
  police cir 750 kbps bc 128000 bytes conform transmit violate drop
class copp-system-p-class-normal-igmp
  set cos 3
  police cir 1400 kbps bc 128000 bytes conform transmit violate drop
class copp-system-p-class-redirect
  set cos 1
  police cir 200 kbps bc 32000 bytes conform transmit violate drop
class copp-system-p-class-exception
  set cos 1
  police cir 200 kbps bc 32000 bytes conform transmit violate drop
class copp-system-p-class-exception-diag
  set cos 1
  police cir 200 kbps bc 32000 bytes conform transmit violate drop

```

```
class copp-system-p-class-monitoring
  set cos 1
  police cir 150 kbps bc 128000 bytes conform transmit violate drop
class copp-system-p-class-l2-unpoliced
  set cos 7
  police cir 50 mbps bc 8192000 bytes conform transmit violate drop
class copp-system-p-class-undesirable
  set cos 0
  police cir 100 kbps bc 32000 bytes conform transmit violate drop
class copp-system-p-class-l2-default
  set cos 0
  police cir 200 kbps bc 32000 bytes conform transmit violate drop
class class-default
  set cos 0
  police cir 200 kbps bc 32000 bytes conform transmit violate drop
```

Cisco Nexus 9300 と 9500 シリーズおよび、3164Q、31128PQ、3232C、および 3264Q スイッチの場合、dense 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-l3uc-data
    set cos 1
    police cir 250 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-critical
    set cos 7
    police cir 2500 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-important
    set cos 6
    police cir 1200 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-multicast-router
    set cos 6
    police cir 1200 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-management
    set cos 2
    police cir 1200 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-multicast-host
    set cos 2
    police cir 1000 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-l3mc-data
    set cos 1
    police cir 1200 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-normal
    set cos 1
    police cir 750 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-ndp
    set cos 1
    police cir 750 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-normal-dhcp
    set cos 1
    police cir 150 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-normal-dhcp-relay-response
    set cos 1
    police cir 200 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-normal-igmp
    set cos 3
    police cir 2500 pps bc 128 packets conform transmit violate drop
  class copp-system-p-class-redirect
    set cos 1
    police cir 1500 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-exception
    set cos 1
    police cir 50 pps bc 32 packets conform transmit violate drop
  class copp-system-p-class-exception-diag
```

```

set cos 1
  police cir 50 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-monitoring
  set cos 1
  police cir 50 pps bc 128 packets conform transmit violate drop
class copp-system-p-class-l2-unpoliced
  set cos 7
  police cir 20000 pps bc 8192 packets conform transmit violate drop
class copp-system-p-class-undesirable
  set cos 0
  police cir 15 pps bc 32 packets conform transmit violate drop
class copp-system-p-class-fcoe
  set cos 6
  police cir 750 pps bc 128 packets conform transmit violate drop
class copp-system-p-class-l2-default
  set cos 0
  police cir 25 pps bc 32 packets conform transmit violate drop
class class-default
  set cos 0
  police cir 25 pps bc 32 packets conform transmit violate drop

```

## 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。

### Procedure

- 
- 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
```

**Note** `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。

### Related Topics

[IP ACL の設定](#)

[MAC ACL の設定](#)

## 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。
- 第1世代の Cisco Nexus 9000 シリーズ スイッチ (非 EX/FX/FX2) は、送信元ベースの CoPP をサポートしていません。この制限は、クラウドスケールの ASIC ベースの Cisco Nexus スイッチには存在しません。
- 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のみならず、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反応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性を評価します。
- 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なな

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 に送信しなければならない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。
- 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に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。
- 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。
- CoPP 機能をサポートする Cisco NX-OS リリースから、新しいプロトコルのその他のクラスを含む CoPP 機能をサポートする Cisco NX-OS リリースにアップグレードする場合は、CoPP の新しいクラスを使用可能にするためにセットアップユーティリティを **setup** コマンドで実行するか **copp profile** コマンドを実行する必要があります。
- コントロールプレーンポリシング (CoPP) 機能をサポートしている Cisco NX-OS リリースから CoPP 機能をサポートしていない以前の Cisco NX-OS リリースへのダウングレードを実行する前に、**show incompatibility nxos bootflash:filename** コマンドを使用して互換性を確認しておく必要があります。非互換な部分が存在する場合は、ソフトウェアをダウングレードする前に、ダウングレードイメージと互換性がない機能をすべて無効化してください。

- CoPP をディセーブルにすることはできません。これを無効にしようとする、パケットには毎秒 50 パケットのレート制限が課されます。
- スキップ CoPP ポリシー オプションは、ネットワークのコントロールプレーンに影響を与える可能性があるため、Cisco NX-OS 初期設定ユーティリティから削除されました。
- Cisco Nexus 9200 シリーズ スイッチでサポートされる CoPP ポリサー レートは、10 kbps の倍数のみです。10 kbps の倍数でないレートが設定されると、レートは丸められます。たとえば、55 Kbps のレートを設定しても、スイッチは 50 kbps を使用します。( **show policy-map type control-plane** コマンドで表示されるのはユーザ設定のレートです。詳細については、[CoPP の設定の確認 \(614 ページ\)](#) を参照してください)。
- Cisco Nexus 9200 シリーズ スイッチでは、ip icmp redirect、IPv6 icmp redirect、ip ICMP unreachable、ipv6 icmp unreachable、および mtu-failure は同じ TCAM エントリを使用し、これらがすべて分類されるクラスマップではポリシー中に最初の例外が存在します。CoPP strict プロファイルでこれらは class-exception クラス マップに分類されます。異なる CoPP のポリシーでは、最初の例外が異なるクラス マップ (たとえば class-exception-diag) に存在する場合、残りの例外は同じクラス マップに分類されます。
- copp-system-class-fcoe クラスは Cisco Nexus 9200 シリーズ スイッチではサポートされていません。
- スタティック CoPP ACL には、次のガイドラインと制限事項が適用されます。
  - Cisco Nexus 9200 シリーズ スイッチでは、スタティック CoPP ACL のみを使用します。
  - スタティック CoPP ACL は、異なる CoPP クラスに再マッピングできます。
  - アクセス コントロール エントリ (ACE) を変更したり削除してスタティック CoPP ACL にすることはできません。
  - CoPP ACL にスタティック ACL のサブストリングがある場合、このタイプのトラフィックに対してマッピングされます。たとえば、ACL に acl-mac-stp サブストリングが含まれている場合、STP トラフィックはこの ACL のクラス マップに分類されます。
  - スタティック CoPP ACL はダイナミック CoPP ACL よりも優先され、この優先度は CoPP ポリシー中での位置、設定の順序、および **show policy-map type control-plane** コマンドでの表示順には関係しません。
  - スタティック CoPP ACL は CoPP ポリシーに含めておく必要があります。これを行わないと、CoPP ポリシーは拒否されます。
- Cisco Nexus リリース 9.2(2) 以降、Cisco Nexus 9300-EX、Cisco Nexus 9300-FX シリーズ スイッチ、および Cisco Nexus 9500 プラットフォーム スイッチは、プロトコル ACL フィルタリングをサポートしています。このリリースでは、IPv6 ACL はサポートされていません。
- Cisco NX-OS リリース 9.2(3) 以降では、Cisco Nexus 9300-EX、Cisco Nexus 9300-FX シリーズ スイッチ、および Cisco Nexus 9500 プラットフォーム スイッチのダイナミック CoPP で IPv6 ACL がサポートされています。

- プロトコル ACL フィルタリング機能には、次の制限があります。
  - ダイナミック CoPP ACL を定義すると、既存のルールを追加または削除できなくなります。これは、ダイナミック CoPP ACL に付加されたすべてのクラスマップとポリシーマップに適用されます。
  - 既存のダイナミック CoPP を新しいポリシーで上書きすることはできません。新しいポリシーを追加する前に、既存のダイナミック CoPP を削除する必要があります。
  - 拒否アクションは適用されません。
  - すべてのエントリーは TCAM でプログラムされ、同じエントリーを持つ2つの MAC または IP ACL が作成され、同じまたは異なるクラスマップにバインドされている場合、異なる TCAM スペースを使用します。
  - 出力 CoPP でサポートされる最大 TCAM カービングは 128 エントリーで、128 MAC エントリーまたは 128 IPv4 エントリーのいずれかです。256 エントリーの TCAM を作成すると、デバイスは出力 CoPP に 128 エントリーを自動的に適用します。
  - ポリサーアクションはサポートされていません。
  - SNMP MIB サポートは必要ありません。
  - IPv6 ACL はダイナミック CoPP ではサポートされません。
- パケットが複数の例外条件を満たしている場合、CoPP は CoPP ACL が設定されている順序に基づいてパケットを照合し、単一のクラスに対してのみ照合します。これは予期された CoPP 動作です。

Cisco NX-OS リリース 9.3 (4) 以降では、UC FIB MISS 例外は CoPP クラス (copp-system-p-class-exception) に対してカウントされます。したがって、パケットに TTL (accounted user class copp-system-p-class-exception-diag) と UC FIB MISS 例外の両方がある場合、UC FIB MISS 例外と見なされます。この動作は、copp-system-p-class-exception クラスの順序が copp-system-p-class-exception-diag クラスよりも高い CoPP クラスの順位のために発生します。NX-OS リリース 9.3(4) より前の NX-OS リリースでは、UC FIB MISS 例外は CoPP ルールによって明示的に処理されませんでした。

- CoPP 処理は 2 つの段階で構成されます。最初の段階では、各クラスポリシーで実際のパケットサイズが再利用されますが、パケットが 2 番目の段階に入ると、44 バイトの内部ヘッダーが追加されます。これにより、すべての CoPP クラスの適合ポリシーまたは違反ポリシーが変更されます。この制限は、Cisco Nexus 9300-FX、Nexus 9300-FX2、Nexus 9364C、Nexus 9332C、および 9300-GX プラットフォームスイッチに適用されます。

# 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。

**Table 44: 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<br><br><b>Note</b> 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。

#### Before you begin

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。

#### Procedure

|        | Command or Action                                                                                 | Purpose                      |
|--------|---------------------------------------------------------------------------------------------------|------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br><b>Example:</b><br>switch# configure terminal<br>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。 |

|        | Command or Action                                                                                                                                                                               | Purpose                                                                                                                                                                                         |
|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 2 | <p><b>class-map type control-plane [match-all   match-any] class-map-name</b></p> <p><b>Example:</b></p> <pre>switch(config)# class-map type control-plane ClassMapA switch(config-cmap)#</pre> | <p>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 <b>match-any</b> 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。</p> <p><b>Note</b> 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。</p> |
| ステップ 3 | <p>(Optional) <b>match access-group name access-list-name</b></p> <p><b>Example:</b></p> <pre>switch(config-cmap)# match access-group name MyAccessList</pre>                                   | <p>IP ACL のマッチングを指定します。</p> <p><b>Note</b> 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。</p>                                                                                                   |
| ステップ 4 | <p>(Optional) <b>match exception {ip   ipv6} icmp redirect</b></p> <p><b>Example:</b></p> <pre>switch(config-cmap)# match exception ip icmp redirect</pre>                                      | <p>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。</p>                                                                                                                                             |
| ステップ 5 | <p>(Optional) <b>match exception {ip   ipv6} icmp unreachable</b></p> <p><b>Example:</b></p> <pre>switch(config-cmap)# match exception ip icmp unreachable</pre>                                | <p>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。</p>                                                                                                                                               |
| ステップ 6 | <p>(Optional) <b>match exception {ip   ipv6} option</b></p> <p><b>Example:</b></p> <pre>switch(config-cmap)# match exception ip option</pre>                                                    | <p>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。</p>                                                                                                                                              |
| ステップ 7 | <p><b>match protocol arp</b></p> <p><b>Example:</b></p> <pre>switch(config-cmap)# match protocol arp</pre>                                                                                      | <p>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。</p>                                                                                                                            |
| ステップ 8 | <p><b>exit</b></p> <p><b>Example:</b></p> <pre>switch(config-cmap)# exit switch(config)#</pre>                                                                                                  | <p>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。</p>                                                                                                                                                              |

|         | Command or Action                                                                                                                                         | Purpose                                   |
|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| ステップ 9  | (Optional) <b>show class-map type control-plane</b> [ <i>class-map-name</i> ]<br><br><b>Example:</b><br>switch(config)# show class-map type control-plane | 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 10 | (Optional) <b>copy running-config startup-config</b><br><br><b>Example:</b><br>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。 |

## 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ー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、次のデフォルトが設定されます。

- 毎秒 50 パケット (PPS) で、バーストは 32 パケット (Cisco Nexus 9300 と 9500 シリーズ および、3164Q、31128PQ、3232C、および 3264Q スイッチ)
- 毎秒 150 キロビット (kbps) で、バーストは 32,000 バイト (Cisco Nexus 9200 シリーズ スイッチ)

### Before you begin

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。

### Procedure

|        | Command or Action                                                                                                                                                     | Purpose                                                                              |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br><b>Example:</b><br>switch# configure terminal<br>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 | <b>policy-map type control-plane</b> <i>policy-map-name</i><br><br><b>Example:</b><br>switch(config)# policy-map type control-plane ClassMapA<br>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。 |
| ステップ 3 | <b>class</b> { <i>class-map-name</i> [ <b>insert-before</b> <i>class-map-name2</i> ]   <b>class-default</b> }                                                         | 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。                  |

|               | Command or Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|               | <pre>switch(config-pmap)# class ClassMapA switch(config-pmap-c)#</pre>                                                                                                                                                                                                                                                                                                                                                                                                                       | <p>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。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <p>ステップ 4</p> | <p>次のいずれかのコマンドを入力します。</p> <ul style="list-style-type: none"> <li>• <b>police [cir] {cir-rate [rate-type]}</b></li> <li>• <b>police [cir] {cir-rate [rate-type]} [bc] burst-size [burst-size-type]</b></li> <li>• <b>police [cir] {cir-rate [rate-type]} conform transmit [violate drop]</b></li> </ul> <p><b>Example:</b></p> <pre>switch(config-pmap-c)# police cir 52000 bc 1000 packets</pre> <p><b>Example:</b></p> <pre>switch(config-pmap-c)# police cir 3400 kbps bc 200 kbytes</pre> | <p>認定情報レート (CIR) を指定します。有効なレート範囲は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 0 ~ 268435456 pps (Cisco Nexus 9300 と 9500 シリーズおよび、3164Q、31128PQ、3232C、および 3264Q スイッチ)</li> <li>• 0 ~ 80000000000 bps/gbps/kbps/mbps (Cisco Nexus 9200 シリーズ スイッチ)</li> </ul> <p><b>Note</b> CIR レートの範囲は 0 から始まります。それ以前のリリースでは、CIR のレート範囲は 1 から始まります。この値を 0 とするとパケットをドロップします。</p> <p>認定バースト (BC) の範囲は次のとおりです。</p> <ul style="list-style-type: none"> <li>• 1 ~ 1073741 パケット (Cisco Nexus 9300 と 9500 シリーズおよび、3164Q、31128PQ、3232C、および 3264Q スイッチ)</li> <li>• 1 ~ 512000000 bytes/kbytes/mbytes (Cisco Nexus 9200 シリーズ スイッチ)</li> </ul> <p><b>conform transmit</b> アクションは、パケットを送信します。</p> <p><b>Note</b> 同じ CIR に BC と一致 (conform) アクションを指定できます。</p> |
| <p>ステップ 5</p> | <p>(Optional) <b>logging drop threshold [drop-count [level syslog-level]]</b></p> <p><b>Example:</b></p> <pre>switch(config-pmap-c)# logging drop threshold 100</pre>                                                                                                                                                                                                                                                                                                                        | <p>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 ~ 8000000000 バイトです。syslog-level 引</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |



|         | Command or Action                                                                                                                                                   | Purpose                                        |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------|
|         |                                                                                                                                                                     | 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 6  | (Optional) <b>set cos <i>cos-value</i></b><br><b>Example:</b><br>switch(config-pmap-c)# set cos 1                                                                   | 802.1Q CoS 値を指定します。有効な範囲は 0～7 です。デフォルト値は 0 です。 |
| ステップ 7  | <b>exit</b><br><b>Example:</b><br>switch(config-pmap-c)# exit<br>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 8  | <b>exit</b><br><b>Example:</b><br>switch(config-pmap)# exit<br>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。                   |
| ステップ 9  | (Optional) <b>show policy-map type control-plane [expand] [name <i>class-map-name</i>]</b><br><b>Example:</b><br>switch(config)# show policy-map type control-plane | 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 10 | (Optional) <b>copy running-config startup-config</b><br><b>Example:</b><br>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。      |

**Related Topics**

[コントロールプレーンクラスマップの設定 \(601 ページ\)](#)

## 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。



**Note** CoPP ポリシーを変更し CoPP のカスタム ポリシーを適用しようとした場合、ハードウェア内では非アトミックとして設定され、次のメッセージが表示されます。

```
This operation can cause disruption of control traffic. Proceed (y/n)? [no] y
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT24-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
update done for CoPP
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT23-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
update done for CoPP
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT21-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
update done for CoPP
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT25-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
update done for CoPP
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT26-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
update done for CoPP
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT22-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
update done for CoPP
2013 Nov 13 23:16:46 switch %ACLQOS-SLOT4-5-ACLQOS_NON_ATOMIC: Non atomic ACL/QoS policy
update done for CoPP
```

### Before you begin

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。

### Procedure

|        | Command or Action                                                                                                                       | Purpose                                                                                                                                        |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br><b>Example:</b><br>switch# configure terminal<br>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 | <b>control-plane</b><br><br><b>Example:</b><br>switch(config)# control-plane<br>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 | <b>[no] service-policy input <i>policy-map-name</i></b><br><br><b>Example:</b><br>switch(config-cp)# service-policy input<br>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。<br><br>CoPP をディセーブルにすることはできません。このコマンドを <b>no</b> 形式で入力すると、パケットには毎秒 50 パケットのレート制限が課されます。 |
| ステップ 4 | <b>exit</b><br><br><b>Example:</b><br>switch(config-cp)# exit<br>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。                                                                                                              |

|        | Command or Action                                                                                                                    | Purpose                                    |
|--------|--------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------|
| ステップ 5 | (Optional) <b>show running-config copp [all]</b><br><br><b>Example:</b><br>switch(config)# show running-config<br>copp               | CoPP 設定を表示します。                             |
| ステップ 6 | (Optional) <b>copy running-config startup-config</b><br><br><b>Example:</b><br>switch(config)# copy running-config<br>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。 |

**Related Topics**

[コントロールプレーン ポリシー マップの設定 \(603 ページ\)](#)

## 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 レートのスケール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。

**Procedure**

|        | Command or Action                                                                                                                   | Purpose                                                                                                                              |
|--------|-------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br><b>Example:</b><br>switch# configure terminal<br>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 | <b>control-plane</b><br><br><b>Example:</b><br>switch(config)# control-plane<br>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 | <b>scale-factor value module multiple-module-range</b><br><br><b>Example:</b><br>switch(config-cp)# scale-factor 1.10<br>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。 |

|        | Command or Action                                                                                                                              | Purpose                                                                                                                                                                                           |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        |                                                                                                                                                | デフォルトのスケールファクタ値 1.00 に戻すには、 <b>no scale-factor value module multiple-module-range</b> コマンドを使用するか、 <b>scale-factor 1 module multiple-module-range</b> 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である値 1.00 に設定します。 |
| ステップ 4 | (Optional) <b>show policy-map interface control-plane</b><br><br><b>Example:</b><br>switch(config-cp)# show policy-map interface control-plane | 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 5 | (Optional) <b>copy running-config startup-config</b><br><br><b>Example:</b><br>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。                                                                                                                                                         |

## 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。

### Procedure

|        | Command or Action                                                                                                    | Purpose                                                                                                           |
|--------|----------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>no copp profile strict moderate lenient dense</b><br><br><b>Example:</b><br>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。<br><br>CoPP をディセーブルにすることはできません。このコマンドを <b>no</b> 形式で入力すると、パケットには毎秒 50 パケットのレート制限が課されます。 |
| ステップ 2 | (Optional) <b>show copp status</b><br><br><b>Example:</b><br>switch(config)# show copp status                        | 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 | (Optional) <b>show running-config copp</b><br><br><b>Example:</b>                                                    | 実行コンフィギュレーション内の CoPP 設定を表示します。                                                                                    |

|  | Command or Action                           | Purpose |
|--|---------------------------------------------|---------|
|  | switch(config)# show running-config<br>copp |         |

**Related Topics**

[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](#) (620 ページ)

## CoPP ベスト プラクティス ポリシーのコピー

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。

**Procedure**

|        | Command or Action                                                                                                                                                    | Purpose                                                                                             |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>copp copy profile</b> {strict   moderate   lenient   dense} {prefix   suffix} <i>string</i><br><br><b>Example:</b><br>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。<br><br>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 | (Optional) <b>show copp status</b><br><br><b>Example:</b><br>switch# show copp status                                                                                | 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 | (Optional) <b>show running-config copp</b><br><br><b>Example:</b><br>switch# show running-config copp                                                                | 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。                                                      |

## プロトコル ACL フィルタリング

プロトコル ACL フィルタリングにより、NX-OS スイッチは、ホスト MAC アドレスに基づいてコントロールプレーンへのすべてのトラフィックをフィルタリングできます。プロトコル ACL フィルタリングは、MAC ACL および IP ACL でサポートされますが、IPv6 ACL ではサポートされません。

Cisco NX-OS リリース 9.2(2)以降、この機能のサポートが次の NX-OS プラットフォームスイッチに追加されました。

- Cisco Nexus 9300-EX
- Cisco Nexus 9300-EX
- Cisco Nexus 9500

## CoPP の ARP ACL フィルタリングの設定

CoPP で MAC ACL フィルタリングを設定できます。

### Before you begin

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。

### Procedure

|        | Command or Action                                                                                                                              | Purpose                                                                                                                               |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><b>Example:</b><br>switch# configure terminal<br>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 | <b>[no] hardware access-list tcam region erg-copp size</b><br><b>Example:</b><br>switch(config)# hardware access-list tcam region erg-copp 256 | CoPP TCAM リージョン サイズを設定します。                                                                                                            |
| ステップ 3 | <b>copy running-config startup-config</b><br><b>Example:</b><br>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。                                                                                             |
| ステップ 4 | <b>reload</b><br><b>Example:</b><br>switch(config)# reload                                                                                     | デバイスがリロードされます。<br><b>Note</b> 新しいサイズの値は、 <b>copy running-config startup-config + reload</b> を入力するか、すべてのラインカードモジュールをリロードした後にのみ有効になります。 |
| ステップ 5 | <b>configure terminal</b><br><b>Example:</b><br>switch# configure terminal<br>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 6 | <b>mac access-list mac-foo-1</b><br><b>Example:</b>                                                                                            |                                                                                                                                       |

|         | Command or Action                                                                                                                                                                                                                                                                                                                                                                    | Purpose                                                                                                                               |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
|         | switch# mac access-list mac-foo-1<br>switch(config-mac-acl)#                                                                                                                                                                                                                                                                                                                         |                                                                                                                                       |
| ステップ 7  | <b>class-map type control-plane [match-all   match-any] class-map-name</b><br><br><b>Example:</b><br>switch(config)# class-map type control-plane match-any c-map2<br>switch(config-cmap)#                                                                                                                                                                                           | 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 <b>match-any</b> 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。                         |
| ステップ 8  | (Optional) <b>match access-group name access-list-name</b><br><br><b>Example:</b><br>switch(config-cmap)# match access-group name IP-foo-1                                                                                                                                                                                                                                           |                                                                                                                                       |
| ステップ 9  | <b>policy-map type control-plane policy-map-name</b><br><br><b>Example:</b><br>switch(config)# policy-map type control-plane ClassMapA<br>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。                                                  |
| ステップ 10 | <b>class {class-map-name [insert-before class-map-name2]   class-default}</b><br><br><b>Example:</b><br>switch(config-pmap)# class ClassMap2<br>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。<br><br><b>class-default</b> 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 11 | 次のいずれかのコマンドを入力します。<br><br><ul style="list-style-type: none"> <li>• <b>police [cir] {cir-rate [rate-type]}</b></li> <li>• <b>police [cir] {cir-rate [rate-type]} [bc] burst-size [burst-size-type]</b></li> <li>• <b>police [cir] {cir-rate [rate-type]} conform transmit [violate drop]</b></li> </ul><br><b>Example:</b><br>switch(config-pmap-c)# police cir 52000 bc 1000 packets | 認定情報レート (CIR) を指定します。有効なレート範囲は次のとおりです。<br><br>認定バースト (BC) の範囲は次のとおりです。                                                                |
| ステップ 12 | <b>control-plane Dynamic mode</b><br><br><b>Example:</b><br>switch(config)# control-plane dynamic mode<br>switch(config-cp-dyn)#                                                                                                                                                                                                                                                     | 制御プレーン動的コンフィギュレーションモードに入ります。                                                                                                          |

|         | Command or Action                                                                                                                                            | Purpose                |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|
| ステップ 13 | <b>service-policy-dynamic input</b><br><i>policy-map-name</i><br><br><b>Example:</b><br>switch(config-cp-dyn)#<br>service-policy-dynamic input<br>PolicyMap1 | 入トラフィックのポリシーマップを指定します。 |

## CoPP の IP ACL フィルタリングの設定

出力 CoPP で IP ACL フィルタリングを設定できます。

始める前に

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

|        | コマンドまたはアクション                                                                                                                             | 目的                                                                                                                                |
|--------|------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br><br>例：<br>switch# configure terminal<br>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 | <b>[no] hardware access-list tcam region erg-copp size</b><br><br>例：<br>switch(config)# hardware access-list<br>tcam region erg-copp 256 | CoPP TCAM リージョンの出力サイズを設定します。                                                                                                      |
| ステップ 3 | <b>copy running-config startup-config</b><br><br>例：<br>switch(config)# copy running-config<br>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 4 | <b>reload</b><br><br>例：<br>switch(config)# reload                                                                                        | デバイスがリロードされます。<br><br>(注) 新しいサイズの値は、 <b>copy running-config startup-config + reload</b> を入力するか、すべてのラインカードモジュールをリロードした後にのみ有効になります。 |
| ステップ 5 | <b>configure terminal</b><br><br>例：                                                                                                      | グローバル 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                                                                                                                                         |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
|         | switch# configure terminal<br>switch(config)#                                                                                                                                    |                                                                                                                                            |
| ステップ 6  | <b>ip access-list IP-foo-1</b><br><br>例：<br>switch# ip access-list mac-foo-1<br>switch(config-acl)#                                                                              |                                                                                                                                            |
| ステップ 7  | <b>permit tcp access-list IP-foo-1 eq bgp</b><br><br>例：<br>switch(config-acl)# 10 permit tcp<br>10.1.1.1/32 10.1.1.2/32 eq bgp                                                   |                                                                                                                                            |
| ステップ 8  | <b>class-map type control-plane [match-all   match-any] class-map-name</b><br><br>例：<br>switch(config)# class-map type<br>control-plane match-any c-map2<br>switch(config-cmap)# | 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 <b>match-any</b> 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。                            |
| ステップ 9  | (任意) <b>match access-group name access-list-name</b><br><br>例：<br>switch(config-cmap)# match<br>access-group name IP-foo-1                                                       |                                                                                                                                            |
| ステップ 10 | <b>policy-map type control-plane policy-map-name</b><br><br>例：<br>switch(config)# policy-map type<br>control-plane ClassMapA<br>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。                                                    |
| ステップ 11 | <b>class {class-map-name [insert-before class-map-name2]   class-default}</b><br><br>例：<br>switch(config-pmap)# class ClassMap2<br>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。<br><br><b>class-default</b> 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 12 | 次のいずれかのコマンドを入力します。<br><br>• <b>police [cir] {cir-rate [rate-type]}</b><br>• <b>police [cir] {cir-rate [rate-type]} [bc] burst-size [burst-size-type]</b>                         | 認定情報レート (CIR) を指定します。有効なレート範囲は次のとおりです。<br><br>認定バースト (BC) の範囲は次のとおりです。                                                                     |

|         | コマンドまたはアクション                                                                                                                                                                                                                                                                                            | 目的                           |
|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------|
|         | <ul style="list-style-type: none"> <li>• <b>police [cir] {cir-rate [rate-type]}</b><br/><b>conform transmit [violate drop]</b></li> </ul> <p>例 :</p> <pre>switch(config-pmap-c)# police cir 52000 bc 1000 packets</pre> <p>例 :</p> <pre>switch(config-pmap-c)# police cir 3400 kbps bc 200 kbytes</pre> |                              |
| ステップ 13 | <p><b>control-plane Dynamic mode</b></p> <p>例 :</p> <pre>switch(config)# control-plane dynamic mode switch(config-cp-dyn)#</pre>                                                                                                                                                                        | 制御プレーン動的コンフィギュレーションモードに入ります。 |
| ステップ 14 | <p><b>service-policy-dynamic input</b><br/><i>policy-map-name</i></p> <p>例 :</p> <pre>switch(config-cp-dyn)# service-policy-dynamic input PolicyMap1</pre>                                                                                                                                              | 入トラフィックのポリシーマップを指定します。終了     |

## 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                                                  |
|----------------------------------------------------------------------------------------------|-----------------------------------------------------|
| <p><b>show policy-map type control-plane [expand] [ name</b><br/><i>policy-map-name]</i></p> | 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                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>show policy-map interface control-plane</b></p>                   | <p>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。</p> <p><b>Note</b>      スケールファクタは、CIR と BC の値を各モジュールで内部的に変更しますが、ディスプレイに表示されるのは、設定された CIR と BC の値のみです。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。</p> |
| <p><b>show class-map type control-plane</b> [<i>class-map-name</i>]</p> | <p>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。</p>                                                                                                                                                                                                                   |

| コマンド                                                                                                                                                     | 目的                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>show copp diff profile {strict   moderate   lenient   dense} [prior-ver] profile {strict   moderate   lenient   dense} show copp diff profile</pre> | <p>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。</p> <p><b>prior-ver</b> 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。</p> <p><b>prior-ver</b> 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）。</p> |
| <pre>show copp profile {strict   moderate   lenient   dense}</pre>                                                                                       | <p>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。</p>                                                                                                                                                                                                                                                                                         |
| <pre>show running-config aclmgr [all]</pre>                                                                                                              | <p>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。<b>all</b> 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。</p>                                                                                                                                                                                                       |
| <pre>show running-config copp [all]</pre>                                                                                                                | <p>実行コンフィギュレーション内の CoPP 設定を表示します。</p>                                                                                                                                                                                                                                                                                                        |

| コマンド                                          | 目的                                                                                                                                   |
|-----------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <code>show startup-config aclmgr [all]</code> | 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。 |

## CoPP 設定ステータスの表示

### Procedure

|        | Command or Action                     | Purpose                |
|--------|---------------------------------------|------------------------|
| ステップ 1 | <code>switch# show copp status</code> | CoPP 機能の設定ステータスを表示します。 |

### Example

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

### Procedure

|        | Command or Action                                            | Purpose                                                                                                                                                |
|--------|--------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <code>switch# show policy-map interface control-plane</code> | 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。<br><br>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。 |

### Example

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-p-policy-strict

class-map copp-system-p-class-critical (match-any)
  set cos 7
  police cir 19000 pps , bc 128 packets
  module 4 :
    transmitted 373977 packets;
    dropped 0 packets;
```

## SNMP での CoPP のモニタリング

Cisco Nexus リリース 9.2(3)以降、CoPP は Cisco クラスベース QoS MIB (cbQoS MIB) 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 cbQoS MIB テーブルがサポートされます。

- ccbQosServicePolicy
- cbQosInterfacePolicy
- cbQosObjects
- cbQosPolicyMapCfg
- cbQosClassMapCfg
- cbQosMatchStmtCfg
- cbQosPoliceCfg
- cbQosSetCfg

## CoPP 統計情報のクリア

### Procedure

|        | Command or Action                                                 | Purpose                                 |
|--------|-------------------------------------------------------------------|-----------------------------------------|
| ステップ 1 | (Optional) switch# <b>show policy-map interface control-plane</b> | 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。 |

|        | Command or Action                    | Purpose           |
|--------|--------------------------------------|-------------------|
| ステップ 2 | switch# <b>clear copp statistics</b> | CoPP 統計情報をクリアします。 |

### Example

次に、インターフェイス環境で、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 の設定例

次に、IP ACL と MAC ACL を使用する CoPP を設定する例を示します。

```
configure terminal
ip access-list copp-system-p-acl-igmp
permit igmp any 10.0.0.0/24

ip access-list copp-system-p-acl-msdp
permit tcp any any eq 639

mac access-list copp-system-p-acl-arp
permit any any 0x0806

ip access-list copp-system-p-acl-tacas
permit udp any any eq 49

ip access-list copp-system-p-acl-ntp
permit udp any 10.0.1.1/23 eq 123

ip access-list copp-system-p-acl-icmp
permit icmp any any

class-map type control-plane match-any copp-system-p-class-critical
match access-group name copp-system-p-acl-igmp
match access-group name copp-system-p-acl-msdp

class-map type control-plane match-any copp-system-p-class-normal
match access-group name copp-system-p-acl-icmp
match exception ip icmp redirect
match exception ip icmp unreachable
match exception ip option

policy-map type control-plane copp-system-p-policy

class copp-system-p-class-critical
police cir 19000 pps bc 128 packets conform transmit violate drop

class copp-system-p-class-important
```

```

police cir 500 pps bc 128 packets conform transmit violate drop

class copp-system-p-class-normal
police cir 300 pps bc 32 packets conform transmit violate drop

class class-default
police cir 50 pps bc 32 packets conform transmit violate drop

control-plane
service-policy input copp-system-p-policy

```

CoPP クラスを作成し、ACL を関連付けるには、次のようにします。

```

class-map type control-plane copp-arp-class
match access-group name copp-arp-acl

```

CoPP ポリシーにクラスを追加するには、次のようにします。

```

policy-map type control-plane copp-system-policy
class copp-arp-class
police pps 500

```

## 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。

```

switch# setup

----- Basic System Configuration Dialog -----

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

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 | <i>Cisco NX-OS</i> ライセンスガイド |

### 標準

| 標準       | タイトル                            |
|----------|---------------------------------|
| RFC 2698 | 『A Two Rate Three Color Marker』 |





## 第 25 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。

- [レート制限について, on page 623](#)
- [レート制限の注意事項と制約事項 \(624 ページ\)](#)
- [レート制限のデフォルト設定, on page 625](#)
- [レート制限の設定, on page 625](#)
- [レート制限のモニタリング, on page 628](#)
- [レート制限統計情報のクリア, on page 628](#)
- [レート制限の設定の確認, on page 628](#)
- [レート制限の設定例, on page 629](#)
- [レート制限に関する追加情報, on page 629](#)

## レート制限について

レート制限を行うことで、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。

次のタイプのリダイレクトパケットに対して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
- 双方向フォワーディング検出 (BFD) パケット
- catch-all 例外トラフィック
- ファブリック エクステンダ (FEX) トラフィック
- レイヤ 3 収集パケット
- レイヤ 3 マルチキャスト データ パケット
- SPAN 出力トラフィック

Cisco Nexus 9200、9332C、9364C、9300-EX、9300-FX/FXP/FX2/FX3、9300-GX プラットフォームスイッチ、および -EX/FX ラインカードを備えた Cisco Nexus 9500 プラットフォームスイッチの場合、CoPP ポリサー レートはキロビット/秒です。他の Cisco Nexus 9000 シリーズスイッチの場合、CoPP ポリサー レートはパケット/秒です。ただし、SPAN 出力トラフィックではキロビット/秒です。

## レート制限の注意事項と制約事項

レート制限に関する注意事項と制約事項は次のとおりです。

- 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。

- ハードウェア レートリミッタを設定して、SPAN 出力ポートの発信トラフィックの統計情報を表示できます。レート リミッタは、すべての Cisco Nexus 9000、9300 と 9500 シリーズスイッチおよび Cisco Nexus 3164Q、31128PQ、3232C、および 3264Q スイッチでサポートされます。
- 出力ポートのレート リミッタは、Cisco Nexus 9300 および 9500 シリーズスイッチではパイプごとに制限されます。Cisco Nexus 3164Q、31128PQ、Cisco Nexus 3232C および 3264Q スイッチです。出力ポートのレートリミッタは、Cisco Nexus 9200 および 9300-EX シリーズスイッチのスライスごとに制限されます。
- Cisco Nexus 9300 および 9500 シリーズスイッチ、Cisco Nexus 3164Q、Cisco Nexus 31128PQ、Cisco Nexus 3232C、および Cisco Nexus 3264Q スイッチは、ローカルと ERSPAN の両方をサポートします。ただし、レート リミッタは ERSPAN にのみ適用されます。これらのスイッチでレートリミッタを有効にするには、e-racl ACL TCAM リージョンを設定する必要があります。詳細については、Cisco Nexus 9000 シリーズ NX-OS セキュリティ設定ガイドの「[ACL TCAM リージョン](#)」セクションを参照してください。
- Cisco Nexus 9200 および 9300-EX シリーズスイッチ、N9K-X9736C-EX、N9K-97160YC-EX、N9K-X9732C-EX、N9K-X9732C-EXM ラインカードの場合、SPAN 出力レートリミッタは ERSPAN とローカル SPAN の両方に適用されます。これらのデバイスでレートリミッタを使用するために特別な TCAM カービングは必要ありません。

- Cisco Nexus 92160YC-X、92304QC、9.272Q、9232C、92300YC、9348GC-FXP、93108TC-FX シリーズ スイッチ、Cisco Nexus 3232C および Cisco Nexus 3264Q スイッチの場合、sFlow と ERSPAN の両方を設定しないでください。



(注) Cisco IOS の CLI に慣れている場合、この機能の Cisco NX-OS コマンドは従来の Cisco IOS コマンドと異なる点があるため注意が必要です。

## 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。

**Table 45:** 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   |
| BFD パケットのレート制限               | 10000 pps |
| 例外パケットのレート制限                 | 50 pps    |
| FEX パケットのレート制限               | 1000 pps  |
| レイヤ 3 収集パケットのレート制限           | 100 pps   |
| レイヤ 3 マルチキャスト データ パケットのレート制限 | 3000 pps  |
| SPAN 出力レート制限                 | 制限なし      |

## 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。

### Procedure

|        | Command or Action                                                                                     | Purpose                      |
|--------|-------------------------------------------------------------------------------------------------------|------------------------------|
| ステップ 1 | <b>configure terminal</b><br><b>Example:</b><br><pre>switch# configure terminal switch(config)#</pre> | グローバル コンフィギュレーション モードを開始します。 |

|        | Command or Action                                                                                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                            |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 2 | <b>hardware rate-limiter access-list-log</b><br><i>{packets   disable} [module module [port start end]]</i><br><br><b>Example:</b><br><pre>switch(config)# hardware rate-limiter access-list-log 200</pre> | 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設定します。範囲は 0 ~ 10,000 です。                                                                                                                                                                                                                              |
| ステップ 3 | <b>hardware rate-limiter bfd packets</b><br><i>[module module [port start end]]</i><br><br><b>Example:</b><br><pre>switch(config)# hardware rate-limiter bfd 500</pre>                                     | 双方向フォワーディング検出 (BFD) パケットのレート制限を設定します。範囲は 0 ~ 10,000 です。                                                                                                                                                                                                                                            |
| ステップ 4 | <b>hardware rate-limiter exception packets</b><br><i>[module module [port start end]]</i><br><br><b>Example:</b><br><pre>switch(config)# hardware rate-limiter exception 500</pre>                         | コントロールプレーン ポリシング (CoPP) ポリシーで分類されないシステムのすべての例外トラフィックのレート制限を設定します。範囲は 0 ~ 10,000 です。                                                                                                                                                                                                                |
| ステップ 5 | <b>hardware rate-limiter fex packets</b> <i>[module module [port start end]]</i><br><br><b>Example:</b><br><pre>switch(config)# hardware rate-limiter fex 500</pre>                                        | スーパーバイザ宛 FEX トラフィックのレート制限を設定します。範囲は 0 ~ 10,000 です。                                                                                                                                                                                                                                                 |
| ステップ 6 | <b>hardware rate-limiter layer-3 glean packets</b> <i>[module module [port start end]]</i><br><br><b>Example:</b><br><pre>switch(config)# hardware rate-limiter layer-3 glean 500</pre>                    | レイヤ 3 収集パケットのレート制限を設定します。範囲は 0 ~ 10,000 です。<br><br>特定の宛先のトラフィックを受信するノードは、書き換えられた情報や宛先までの間にある物理レイヤインターフェイスを認識できず、トラフィックを転送できないことがあります。こうした期間中、そのような宛先へのデータパスには収集エントリのインストールが可能です。これはグローバルなパント隣接関係へのポインタではない可能性があるため、このようなパケットのスーパーバイザへのパントには予約されたモジュールやポート値が使用されます。この収集レートの制御は、特定のレートリミッタを使用して行えます。 |

|         | Command or Action                                                                                                                                                                                                                                                                    | Purpose                                                                                                                                                                                                                        |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|         |                                                                                                                                                                                                                                                                                      | <p><b>Note</b> CoPP ポリシーは、グローバルポイント隣接のヒットにより CPU に転送される収集パケットのレートを制御します。レイヤ 3 収集ハードウェアレートリミッタは、<code>sup-redirect access-list</code> によって CPU にリダイレクトされる収集パケットの数を制限します。これは、パケットが不明な VTEP から受信される VXLAN 環境などの特殊なケースで使用されます。</p> |
| ステップ 7  | <p><b>hardware rate-limiter layer-3 multicast local-groups packets</b> [<b>module module</b> [<b>port start end</b>]]</p> <p><b>Example:</b></p> <pre>switch(config)# hardware rate-limiter layer-3 multicast local-groups 300</pre>                                                 | <p>最短パスツリー (SPT) の参加開始用にバントされたレイヤ 3 マルチキャストデータパケットのレート制限を設定します。0 ~ 10,000 です。</p>                                                                                                                                              |
| ステップ 8  | <p><b>hardware rate-limiter span-egress rate</b> [<b>module module</b>]</p> <p><b>Example:</b></p> <pre>switch(config)# hardware rate-limiter span-egress 123</pre>                                                                                                                  | <p>出力トラフィックの SPAN のレート制限を設定します。範囲は 0~100000000 です。</p> <p><b>Note</b> sFlow と SPAN 出力レートリミッタの両方を設定しないでください。</p>                                                                                                                |
| ステップ 9  | <p>(Optional) <b>show hardware rate-limiter</b> [<b>access-list-log</b>   <b>bfd</b>   <b>exception</b>   <b>fex</b>   <b>layer-3 glean</b>   <b>layer-3 multicast local-groups</b>   <b>module module</b>]</p> <p><b>Example:</b></p> <pre>switch# show hardware rate-limiter</pre> | <p>レート制限の設定を表示します。モジュールの範囲は 1~30 です。</p>                                                                                                                                                                                       |
| ステップ 10 | <p>(Optional) <b>copy running-config startup-config</b></p> <p><b>Example:</b></p> <pre>switch# copy running-config startup-config</pre>                                                                                                                                             | <p>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。</p>                                                                                                                                                                               |

## 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。

### Procedure

|        | Command or Action                                                                                                                                                                                                                                                                                            | Purpose          |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| ステップ 1 | <b>show hardware rate-limiter</b> [ <b>access-list-log</b>   <b>bfd</b>   <b>exception</b>   <b>fex</b>   <b>layer-3 glean</b>   <b>layer-3 multicast local-groups</b>   <b>span-egress</b>   <b>module module</b> ]<br><br><b>Example:</b><br><pre>switch# show hardware rate-limiter access-list-log</pre> | 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。

### Procedure

|        | Command or Action                                                                                                                                                                                                                                                                                                            | Purpose           |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------|
| ステップ 1 | <b>clear hardware rate-limiter</b> { <b>all</b>   <b>access-list-log</b>   <b>bfd</b>   <b>exception</b>   <b>fex</b>   <b>layer-3 glean</b>   <b>layer-3 multicast local-groups</b>   <b>span-egress</b> [ <b>module module</b> ]}<br><br><b>Example:</b><br><pre>switch# clear hardware rate-limiter access-list-log</pre> | 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              |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|
| <b>show hardware rate-limiter</b> [ <b>access-list-log</b>   <b>bfd</b>   <b>exception</b>   <b>fex</b>   <b>layer-3 glean</b>   <b>layer-3 multicast local-groups</b>   <b>span-egress</b>   <b>module module</b> ]<br> | レート制限の設定を表示します。 |



## レート制限の設定例

次に、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設定する例を示します。

```
switch(config)# hardware rate-limiter access-list-log
switch(config)# show hardware rate-limiter access-list-log
Units for Config: kilo bits per second
Allowed, Dropped & Total: aggregated since last clear counters
```

```
Module: 4
R-L Class          Config          Allowed          Dropped          Total
+-----+-----+-----+-----+-----+
+
access-list-log    100             0                 0                 0

Port group with configuration same as default configuration
Eth4/1-36
```

```
Module: 22
R-L Class          Config          Allowed          Dropped          Total
+-----+-----+-----+-----+-----+
+
access-list-log    100             0                 0                 0

Port group with configuration same as default configuration
Eth22/1-0
```

次に、SPAN 出力レート リミッタが sFlow と競合する例を示します。

```
switch(config)# hardware rate-limiter span-egress 123
Warning: This span-egress rate-limiter might affect functionality of sFlow
switch(config)# show hardware rate-limiter span-egress
Units for Config: kilo bits per second
Allowed, Dropped & Total: aggregated since Module: 1
```

```
R-L Class          Config          Allowed          Dropped          Total
+-----+-----+-----+-----+-----+
L3 glean           100             0                 0                 0
L3 mcast loc-grp   3000            0                 0                 0
access-list-log    100             0                 0                 0
bfd                10000           0                 0                 0
exception          50              0                 0                 0
fex                3000            0                 0                 0
span               50              0                 0                 0
dpss               6400            0                 0                 0
span-egress        123             0                 0                 0
<<configured
```

## 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 のライセンス | <i>Cisco NX-OS</i> ライセンス ガイド |



## 第 26 章

# MACsec の設定

この章では、Cisco NX-OS デバイスに MACsec を設定する手順について説明します。

- [MACsec について \(631 ページ\)](#)
- [MACsec の注意事項と制約事項 \(632 ページ\)](#)
- [MACsec の有効化 \(636 ページ\)](#)
- [MACsec の無効化 \(637 ページ\)](#)
- [MACsec キーチェーンとキーの設定 \(638 ページ\)](#)
- [MACsec フォールバック キーの設定 \(640 ページ\)](#)
- [MACsec ポリシーの設定 \(642 ページ\)](#)
- [PSK のローテーション \(643 ページ\)](#)
- [設定可能な EAPOL の宛先とイーサネット タイプについて \(644 ページ\)](#)
- [MACsec 設定の確認 \(646 ページ\)](#)
- [MACsec 統計の表示 \(648 ページ\)](#)
- [MACsec の設定例 \(651 ページ\)](#)
- [XML の例 \(653 ページ\)](#)
- [MIB \(661 ページ\)](#)
- [関連資料 \(661 ページ\)](#)

## MACsec について

Media Access Control Security (MACsec) である IEEE 802.1AE と MACsec Key Agreement (MKA) プロトコルは、イーサネットリンク上でセキュアな通信を提供します。次の機能があります。

- ライン レート暗号化機能を提供します。
- レイヤ 2 で強力な暗号化を提供することで、データの機密性を確保します。
- 整合性チェックを行い、転送中にデータを変更できないことを保証します。
- 中央集中型ポリシーを使用して選択的に有効にでき、MACsec 非対応コンポーネントがネットワークにアクセスできるようにしながら、必要に応じて適用することができます。

- レイヤ 2 ではホップバイホップ ベースでパケットを暗号化します。これにより、ネットワークは、既存のポリシーに従って、トラフィックを検査、モニタ、マーク、転送できません（エンドツーエンドレイヤ 3 暗号化技術とは異なり、パケットの内容をネットワーク デバイスから非表示にします）

## キー ライフタイムおよびヒットレス キー ロールオーバー

MACsec キー チェーンには、キー ID とオプションのライフタイムが設定された複数の事前共有キー（PSK）を含めることができます。キーのライフタイムでは、キーがいつ有効になり、いつ期限切れになるかが指定されます。ライフタイム設定が存在しない場合は、無期限のデフォルトライフタイムが使用されます。ライフタイムが設定されていて、ライフタイムの期限が切れると、MKA はキー チェーン内で次に設定された事前共有キーにロールオーバーします。キーのタイムゾーンは、ローカルまたは UTC を指定できます。デフォルトの時間帯は UTC です。

MACsec キーチェーンを設定するには、[MACsec キーチェーンとキーの設定（638 ページ）](#)を参照してください。

（キーチェーン内で）2 番目のキーを設定し、最初のキーのライフタイムを設定することで、そのキーチェーン内の 2 番目のキーにロールオーバーできます。最初のキーのライフタイムが期限切れになると、リスト内の次のキーに自動的にロールオーバーします。同一のキーがリンクの両側で同時に設定されていた場合、キーのロールオーバーはヒットレスになります。つまり、キーはトラフィックを中断せずにロールオーバーされます。

## フォールバック キー

MACsec セッションは、キー/キー名（CKN）のミスマッチで、またはスイッチとピア間のキーの期限が切れて、失敗する可能性があります。MACsec セッションが失敗した場合、フォールバック キーが設定されていれば、フォールバック セッションが引き継ぐことができます。フォールバック セッションは、プライマリ セッションの障害によるダウンタイムを防止し、ユーザが障害の原因となっている主要な問題を修正できるようにします。フォールバック キーは、プライマリ セッションの開始に失敗した場合のバックアップ セッションも提供します。この機能はオプションです。

MACsec フォールバックキーを設定するには、[MACsec フォールバック キーの設定（640 ページ）](#)を参照してください。

## MACSec の注意事項と制約事項

MACsec に関する注意事項と制約事項は次のとおりです。

- MACsec は、次のインターフェイス タイプでサポートされます。
  - レイヤ 2 スイッチポート（アクセスとトランク） access and trunk)
  - レイヤ 3 ルーテッドインターフェイス（サブインターフェイスなし）



(注) レイヤ 3 ルーテッドインターフェイスで MACsec を有効にすると、そのインターフェイスで定義されているすべてのサブインターフェイスでも暗号化が有効になります。ただし、同じレイヤ 3 ルーテッドインターフェイスのサブインターフェイスのサブセットで MACsec を選択的に有効にすることはサポートされていません。

- レイヤ 2 およびレイヤ 3 ポート チャネル (サブインターフェイスなし)
- Secure Channel Identified (SCI) エンコーディングは、Cisco Nexus 9000 シリーズ スイッチでは無効にできません。
- Cisco Nexus ToR スイッチを Cisco NX-OS リリース 7.x から Cisco NX-OS リリース 9.x にダウングレードする場合、MACsec はサポートされません。
- スイッチオーバーの直後に MACsec 機能を無効にすると、一部のセッションは保留状態のままになり、一部のピアはセキュア状態になります。
- MKA は、MACsec でサポートされている唯一のキー交換プロトコルです。Security Association Protocol (SAP) はサポートされていません。
- リンクレベルフロー制御 (LLFC) およびプライオリティフロー制御 (PFC) は、MACsec ではサポートされません。
- 同じインターフェイスに対する複数の MACsec ピア (異なる SCI 値) はサポートされません。
- **macsec shutdown** コマンドを使用して MACsec を無効にすると、MACsec 設定を保持できません。
- MACsec セッションは、最新の Rx および最新の Tx フラグが Tx SA のインストール後に最初に廃止されたキーサーバからのパケットを受け入れるのに寛容です。MACsec セッションは、セキュアな状態に収束します。
- Cisco NX-OS リリース 9.2(1) 以降では、次の設定が可能です。
  - ポリシーがインターフェイスによって参照されている間に、MACsec ポリシーを変更できるようにします。
  - ブレークアウト ポートの異なるレーン間で異なる MACsec ポリシーを許可します。
- Cisco Nexus リリース 9.2(1) 以降、MACsec は Cisco Nexus 93180YC-FX および Cisco Nexus 3264C-E スイッチでサポートされます。
- Cisco Nexus リリース 9.3(1) 以降、MACsec は Cisco Nexus N9K-C9364C、N9K-C9332C、および N9K-C9348GC-FXP プラットフォーム スイッチでサポートされます。これらのスイッチで MACsec を使用する場合は、次の制限が適用されます。

- N9K-C9364C : MACsec は N9K-C9364C の次の 16 ポートでサポートされ、緑色でマークされます (ポート 49 ~ 64)。
- N9K-C9332C : MACsec は N9K-C9332C の次の 8 ポートでサポートされ、緑色でマークされます (ポート 25 ~ 32)。
- N9K-C9348GC-FXP : MACsec は、N9K-C9348GC-FXP の次の 6 ポート (ポート 49 ~ 54) でサポートされます。



(注) Cisco N9K-C9364C および N9K-9332C プラットフォーム スイッチでは、MACsec がポートで設定または未設定の場合、MACsec セキュリティポリシータイプに関係なく、ポートフラップが発生します。

- Cisco Nexus リリース 9.3(1) 以降では、ポートチャネル インターフェイスに MACsec 設定を直接適用することはできません。ただし、MACsec 設定をポートチャネルメンバーポートに直接適用できます。
- Cisco NX-OS リリース 9.3(1) では、Cisco Nexus 9332C および 9364C シリーズ スイッチでは EAPOL 設定はサポートされていません。
- Cisco Nexus リリース 9.3(3) 以降、MACsec は Cisco Nexus 93216TC-FX2、Cisco Nexus 93360YC-FX2 でサポートされています。
- Cisco NX-OS リリース 9.3(5) 以降では、MACsec は次でサポートされます。
  - Cisco Nexus N9K-C93180YC-FX3S スイッチ。MACsec は、すべてのポートでサポートされています。
  - Cisco N9K-X9732C-FX および Cisco N9K-X9788TC-FX ラインカード
- MACsec は、Cisco Nexus N9K-C93240YC-FX2、N9K-C93336C-FX2、N9K-C93108TC-FX、N9K-C93180YC-FX プラットフォーム スイッチ、および N9K-X9736C-FX および N9K-X9732C-EXM ラインカードでサポートされています。
- Cisco Nexus 9000 シリーズ スイッチは、QSA が使用されている場合、MACsec 対応ポートで MACsec をサポートしません。

キーチェーンの制限 :

- MACsec キーのオクテット文字列は上書きできません。代わりに、新しいキーまたは新しいキーチェーンを作成する必要があります。
- **end** または **exit** を入力すると、キーチェーンの新しいキーが設定されます。エディタモードのデフォルトのタイムアウト値は 6 秒です。キーがキー オクテット文字列または 6 秒間の送信ライフタイムで設定されていない場合、MACsec セッションを起動するために不完全な情報が使用され、セッションが承認保留状態のままになる可能性があります。設

定の完了後に MACsec セッションがコンバージされない場合は、ポートをシャットダウン/非シャットダウンすることをお勧めします。

- 指定したキーチェーンでは、キーの有効期間を重複させて、有効なキーの不在期間を避ける必要があります。キーがアクティブ化されない期間が発生すると、セッション ネゴシエーションが失敗し、トラフィックがドロップされる可能性があります。MACsec キーロールオーバーでは、現在アクティブなキーの中で最も遅い開始時刻のキーが優先されます。

フォールバックの制限：

- MACsec セッションが古いプライマリキーで保護されている場合、最新のアクティブなプライマリキーが一致しない場合、フォールバックセッションには進みません。そのため、セッションは古いプライマリキーで保護されたままになり、ステータスが古い CA のキー再生成として表示されます。プライマリ PSK の新しいキーの MACsec セッションは init 状態になります。
- フォールバック キーチェーンでは、無期限のキーを 1 つだけ使用します。複数のキーはサポートされていません。
- フォールバック キーチェーンで使用されるキー ID (CKN) は、プライマリ キーチェーンで使用されるキー ID (CKN) のいずれとも一致しないようにしてください。
- 一度設定すると、インターフェイスのすべての MACsec 設定が削除されない限り、インターフェイスのフォールバック設定は削除できません。

MACsec ポリシーの制限：

- MACsec セッションがセキュアになる前に、BPDU パケットを送信できます。

レイヤ 2 トンネリング プロトコル (L2TP) の制約事項：

- MACsec は、dot1q トンネリングまたは L2TP 用に設定されたポートではサポートされません。
- 非ネイティブ VLAN のトランクポートで STP が有効になっている場合、L2TP は機能しません。

統計情報の制限：

- MACsec モードと非 MACsec モード (通常のポート シャットダウン/非シャットダウン) の間の移行中に発生する CRC エラーはほとんどありません。
- Secy 統計情報は累積され、30 秒ごとにポーリングされます。
- IEEE8021-SECY-MIB OID `secyRxSASStatsOKPkts`、`secyTxSASStatsProtectedPkts`、および `secyTxSASStatsEncryptedPkts` は最大 32 ビットのカウンタ値しか伝送できませんが、トラフィックは 32 ビットを超える可能性があります。

相互運用性の制限：

- N9K-X9732C-EXM と他のピア スイッチ（他のシスコおよびシスコ以外のスイッチ）の相互運用性は、XPN 暗号スイートでのみサポートされます。
- MACsec ピアは、AES\_128\_CMAC 暗号化アルゴリズムを使用するために同じ Cisco NX-OS リリースを実行する必要があります。以前のリリースと Cisco NX-OS リリース 9.2(1) の間の相互運用性のために、AES\_256\_CMAC 暗号化アルゴリズムでキーを使用する必要があります。
- 以前のリリースと Cisco NX-OS リリース 9.2(1) の間の相互運用性を確保するために、MACsec キーが 32 オクテット未満の場合は、MACsec キーにゼロを付加します。
- Cisco NX-OS ボックスでは、すべてのインターフェイスで代替 MAC アドレスとイーサネット タイプの一意の組み合わせを 1 つだけ設定できます。
- 転送エンジンの同じスライス内では、EAPOL ethertype と dot1q ethertype に同じ値を指定することはできません。
- EAPOL 設定を有効にするには、0 ～ 0x599 の範囲のイーサネット タイプの範囲が無効です。
- EAPOL パケットの設定中は、次の組み合わせを使用しないでください。
  - MAC アドレス 0100.0ccd.cdd0 と ethertype
  - MAC アドレスと ethertype : 0xffff、0x800、0x86dd
  - デフォルトの宛先 MAC アドレス 0180.c200.0003 とデフォルトのイーサネット タイプ 0x888e
- N9K-X9736C-FX、N9K-C9348GC-FXP、N9K-C93180YC-FX、N9K-C93108TC-FX、N9K-X9732C-FX、および N9K-X9788TC-FX プラットフォーム スイッチは、1G ポートで MACsec をサポートしていません。MACsec は 1G ポートを有する mac ブロックのポートではサポートされません。
- ポートチャネルメンバーごとの MACsec 設定サポートなしで Cisco NX-OS リリース 9.3(1) から Cisco NX-OS リリースにダウングレードしようとした場合、同じポートチャネルインターフェイスのメンバーに異なる MACsec 設定がある場合その他の場合は、次のエラーメッセージが表示されることがあります。

```

00000000 00000000 macsec 0000000000000000 macsec 0000000000000000 ISSU
0000000000

```

## MACsec の有効化

MACsec および MKA コマンドにアクセスする前に、MACsec 機能を有効にする必要があります。



## 手順

|        | コマンドまたはアクション                                                                                               | 目的                                         |
|--------|------------------------------------------------------------------------------------------------------------|--------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br>例：<br>switch# configure terminal<br>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 | <b>feature macsec</b><br>例：<br>switch(config)# feature macsec                                              | デバイスで MACsec および MKA を有効にします。              |
| ステップ 3 | (任意) <b>copy running-config startup-config</b><br>例：<br>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。 |

## MACsec の無効化

Cisco NX-OS リリース 9.2(1) 以降では、MACsec 機能を無効にしても、この機能が非アクティブ化されるだけで、関連する MACsec 設定は削除されません。

MACsec の無効化には、次の条件があります。

- MACsec shutdown はグローバルコマンドであり、インターフェイス レベルでは使用できません。
- macsec shutdown、show macsec mka session/summary、show macsec mka session detail、および show macsec mka/secy statistics コマンドは、「Macsec is shutdown」メッセージを表示します。ただし、show macsec policy および show key chain コマンドは出力を表示します。
- 連続する MACsec ステータスが macsec shutdown から no macsec shutdown に変更された場合、またはその逆の場合は、ステータス変更の間に 30 秒の間隔が必要です。

## 手順

|        | コマンドまたはアクション                                                                     | 目的                           |
|--------|----------------------------------------------------------------------------------|------------------------------|
| ステップ 1 | <b>configure terminal</b><br>例：<br>switch# configure terminal<br>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 | <b>macsec shutdown</b><br>例：<br>switch(config)# macsec shutdown                                            | デバイスの MACsec 設定を無効にします。 <b>no</b> オプションは、MACsec 機能を復元します。                                   |
| ステップ 3 | (任意) <b>copy running-config startup-config</b><br>例：<br>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。この手順は、スイッチのリロード後に MACsec をシャットダウン状態に維持する場合にのみ必要です。 |

## MACsec キーチェーンとキーの設定

デバイスに MACsec キーチェーンとキーを作成できます。



(注) MACsec キーチェーンのみが MKA セッションをコンバージします。

### 始める前に

MACsec が有効であることを確認します。

### 手順

|        | コマンドまたはアクション                                                                                        | 目的                                                                                                                                                                                                                              |
|--------|-----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br>例：<br>switch# configure terminal<br>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 | (任意) <b>[no] key-chain macsec-psk no-show</b><br>例：<br>switch(config)# key-chain macsec-psk no-show | <b>show running-config</b> および <b>show startup-config</b> コマンドの出力で、暗号化されたキーオクテット文字列をワイルドカード文字に置き換えて非表示にします。デフォルトでは、PSK キーは暗号化形式で表示され、簡単に復号化できません。このコマンドは、MACsec キーチェーンにのみ適用されます。<br><br>(注) オクテット文字列は、設定をファイルに保存するときにも非表示になります。 |

|        | コマンドまたはアクション                                                                                                                                                                                                                                                                           | 目的                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 3 | <b>key chain name macsec</b><br>例 :<br><pre>switch(config)# key chain 1 macsec switch(config-macseckeychain)#</pre>                                                                                                                                                                    | MACSec キーチェーンを作成して MACSec キーのセットを保持し、MACSec キーチェーン設定モードを開始します。                                                                                                                                                                                                                                                                                                                                                                                          |
| ステップ 4 | <b>key key-id</b><br>例 :<br><pre>switch(config-macseckeychain)# key 1000 switch(config-macseckeychain-macseckey)#</pre>                                                                                                                                                                | MAC sec キーを作成し、MACsec キー設定モードを開始します。範囲は 1-32 オクテットで、最大サイズは 64 です。<br>(注) キーの文字数は偶数でなければなりません。                                                                                                                                                                                                                                                                                                                                                           |
| ステップ 5 | <b>key-octet-string <i>octet-string</i> cryptographic-algorithm {AES_128_CMAC   AES_256_CMAC}</b><br>例 :<br><pre>switch(config-macseckeychain-macseckey)# key-octet-string abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789 cryptographic-algorithm AES_256_CMAC</pre> | そのキーの octet スtring を設定します。 <i>octet-string</i> 引数には、最大 64 文字の 16 進数文字を含めることができます。オクテットキーは内部でエンコードされるため、 <b>show running-config macsec</b> コマンドの出力にクリアテキストのキーが現れることはありません。<br>キーオクテット文字列には、次のものが含まれます。 <ul style="list-style-type: none"> <li>• 0 暗号化タイプ - 暗号化なし (デフォルト)</li> <li>• 6 暗号化タイプ - 独自仕様 (タイプ 6 暗号化)。詳細については、<a href="#">MACsec キーでのタイプ 6 暗号化のイネーブル化 (548 ページ)</a> を参照してください。</li> <li>• 7 暗号化タイプ - 最大 64 文字の、独自仕様 WORD キーオクテット文字列</li> </ul> |

|        | コマンドまたはアクション                                                                                                                                                   | 目的                                                                                                                                                                                 |
|--------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|        |                                                                                                                                                                | (注) AES_128_CMAC 暗号化アルゴリズムを使用するためには、MACsec ピアは同じ Cisco NX-OS リリースを実行する必要があります。以前のリリースと、Cisco NX-OS リリース 7.0(3)I7(2)以降のリリース間で相互運用できるようにするには、キーを AES_256_CMAC 暗号化アルゴリズムで使用する必要があります。 |
| ステップ 6 | <b>send-lifetime</b> 開始時間 <b>duration</b> 長さ<br>例 :<br><pre>switch(config-macseckeychain-macseckey) # send-lifetime 00:00:00 Oct 04 2016 duration 100000</pre> | キーの送信ライフタイムを設定します。デフォルトでは、デバイスは開始時間を UTC として扱います。<br><br><i>start-time</i> 引数は、キーがアクティブになる日時です。 <i>duration</i> 引数はライフタイムの長さ (秒) です。最大値は 2147483646 秒 (約 68 年) です。                 |
| ステップ 7 | (任意) <b>show key chain name</b><br>例 :<br><pre>switch(config-macseckeychain-macseckey) # show key chain 1</pre>                                                | キーチェーンの設定を表示します。                                                                                                                                                                   |
| ステップ 8 | (任意) <b>copy running-config startup-config</b><br>例 :<br><pre>switch(config-macseckeychain-macseckey) # copy running-config startup-config</pre>               | 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。                                                                                                                                          |

## MACsec フォールバック キーの設定

Cisco NX-OS リリース 9.2(1)以降では、プライマリセッションがスイッチとピア間のキー/キー名 (CKN) のミスマッチまたはキーの有効期限の結果として失敗した場合にバックアップセッションを開始するようにデバイスのフォールバック キーを設定できます。

### 始める前に

MACsec が有効になっており、プライマリおよびフォールバック キーチェーンとキー ID が設定されていることを確認します。「[MACsec キーチェーンとキーの設定](#)」を参照してください。

## 手順

|        | コマンドまたはアクション                                                                                                                                                                            | 目的                                                                                                                                                                                                                                                                                                                                                                                     |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br>例 :<br><pre>switch# configure terminal switch(config)#</pre>                                                                                               | グローバル 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 | <b>interface name</b><br>例 :<br><pre>switch(config)# interface ethernet 1/1 switch(config-if)#</pre>                                                                                    | 設定するインターフェイスを指定します。インターフェイスタイプと ID を指定できます。イーサネット ポートの場合は、 <b>ethernet slot/port</b> を使用します                                                                                                                                                                                                                                                                                            |
| ステップ 3 | <b>macsec keychain keychain-name policy policy-name fallback-keychain keychain-name</b><br>例 :<br><pre>switch(config-if)# macsec keychain kc2 policy abc fallback-keychain fb_kc2</pre> | <p>キー/キー ID のミスマッチまたはキーの期限切れによる MACsec セッションの失敗後に使用するフォールバック キーチェーンを指定します。フォールバック キー ID は、プライマリ キーチェーンのキー ID と一致してはなりません。</p> <p>フォールバック キーチェーン名を変更して同じコマンドを再発行することで、MACsec 設定を削除せずに、各インターフェイスのフォールバック キーチェーン設定を対応するインターフェイスで変更できます。</p> <p>(注) コマンドは、フォールバック キーチェーン名を除き、インターフェイスの既存のコンフィギュレーション コマンドとまったく同じように入力する必要があります。</p> <p>「<a href="#">MACsec キーチェーンとキーの設定</a>」を参照してください。</p> |
| ステップ 4 | (任意) <b>copy running-config startup-config</b><br>例 :<br><pre>switch(config-if)# copy running-config startup-config</pre>                                                               | 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。                                                                                                                                                                                                                                                                                                                                             |

## MACsec ポリシーの設定

異なるパラメータを使用して複数の MACsec ポリシーを作成できます。しかし、1つのインターフェイスでアクティブにできるポリシーは1つのみです。

始める前に

MACsec が有効であることを確認します。

手順

|        | コマンドまたはアクション                                                                                          | 目的                                                                                                                                                                                                                               |
|--------|-------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br>例：<br>switch# configure terminal<br>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 | <b>macsec policy name</b><br>例：<br>switch(config)# macsec policy abc<br>switch(config-macsec-policy)# | MACsec ポリシーを作成します。                                                                                                                                                                                                               |
| ステップ 3 | <b>cipher-suite name</b><br>例：<br>switch(config-macsec-policy)# cipher-suite GCM-AES-256              | GCM-AES-128、GCM-AES-256、GCM-AES-XPB-128、または GCM-AES-XPB-256 のいずれかを設定します。                                                                                                                                                         |
| ステップ 4 | <b>key-server-priority number</b><br>例：<br>switch(config-macsec-policy)# key-server-priority 0        | キー交換中はピア間の接続が解除されるように、キー サーバのプライオリティを設定します。範囲は0（最高）〜255（最低）で、デフォルト値は16です。                                                                                                                                                        |
| ステップ 5 | <b>security-policy name</b><br>例：<br>switch(config-macsec-policy)# security-policy should-secure      | 次のいずれかのセキュリティポリシーを設定して、データおよび制御パケットの処理を定義します。 <ul style="list-style-type: none"> <li>• <b>must-secure</b> : MACsec をヘッダー持たないパケットはドロップされます。</li> <li>• <b>should-secure</b> : MACsec ヘッダーを持たないパケットも許可されます。これはデフォルト値です。</li> </ul> |

|         | コマンドまたはアクション                                                                                                                | 目的                                                                                                                                                                  |
|---------|-----------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ステップ 6  | <b>window-size number</b><br>例：<br>switch(config-macsec-policy)#<br>window-size 512                                         | インターフェイスが、設定されたウィンドウサイズ未満の packets を受け入れないように、再生保護ウィンドウを設定します。範囲は 0 ~ 596000000 です。                                                                                 |
| ステップ 7  | <b>sak-expiry-time time</b><br>例：<br>switch(config-macsec-policy)#<br>sak-expiry-time 100                                   | SAK キー再生成を強制する時間を秒単位で設定します。このコマンドを使用して、セッションキーを予測可能な時間間隔に変更できます。デフォルトは 0 です。                                                                                        |
| ステップ 8  | <b>conf-offset name</b><br>例：<br>switch(config-macsec-policy)#<br>conf-offset CONF-OFFSET-0                                 | 暗号化を開始するレイヤ 2 フレームの機密性オフセットの 1 つとして、CONF-OFFSET-0、CONF-OFFSET-30、または CONF-OFFSET-50 のいずれかを設定します。このコマンドは、中間スイッチがパケットヘッダー {dmac、smac、etype} を MPLS タグのように使用するために必要です。 |
| ステップ 9  | (任意) <b>show macsec policy</b><br>例：<br>switch(config-macsec-policy)# show<br>macsec policy                                 | MACSec ポリシー設定を表示します。                                                                                                                                                |
| ステップ 10 | (任意) <b>copy running-config startup-config</b><br>例：<br>switch(config-macsec-policy)# copy<br>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。                                                                                                                           |

## PSK のローテーション

SAK の有効期限が MACsec ポリシーで 60 秒に設定されている場合は、次の手順に従って PSK を切り替えます。

### 手順

- ステップ 1 MACsec ポリシーから SAK 期限切れタイマーを削除するには、**no sak-expiry-time** コマンドを使用します。

(注) 設定内のポリシーの数だけ、SAKの有効期限タイマーを削除する必要があります。インターフェイスごとに削除する必要はありません。ポリシーを1つだけ定義してすべてのインターフェイスに適用した場合は、このポリシーからのみ SAK の有効期限タイマーを削除する必要があります。

ステップ2 2分間待機します。

ステップ3 **key key-id** コマンドを使用して、キーチェーンの下に新しいキーをプログラムします。

ステップ4 新しいキーとのセッションが保護されたら、**no key key-id** コマンドを使用して古いキーを削除します。

ステップ5 2分間待機します。

ステップ6 SAK キー再生成タイマーを MACsec ポリシーに追加するには、**sak-expiry-timer 60** コマンドを使用します。

## 設定可能な EAPOL の宛先とイーサネットタイプについて

Cisco NX-OS リリース 9.2(2) 以降では、WAN MACsec を使用するネットワークで、Extensible Authentication Protocol (EAP) over LAN (EAPOL) プロトコルの宛先アドレスとイーサネットタイプの値を非標準値に変更できます。

設定可能な EAPOL MAC およびイーサネットタイプでは、標準 MKA パケットを消費するイーサネットネットワーク上で CE デバイスが MKA セッションを形成できるように、MKA パケットの MAC アドレスとイーサネットタイプを変更できます。

EAPOL 宛先イーサネットタイプは、デフォルトのイーサネットタイプ 0x888E から代替値に変更できます。または、EAPOL 宛先 MAC アドレスは、デフォルト DMAC の 01:80:C2:00:00:03 から代替値に変更できます。プロバイダーブリッジによって消費されないようにします。

この機能はインターフェイスレベルで使用でき、代替 EAPOL 設定は、次のように任意のインターフェイスでいつでも変更できます。

- MACsec がインターフェイスですでに設定されている場合、セッションは新しい代替 EAPOL 設定で起動します。
- MACsec がインターフェイスで設定されていない場合、EAPOL 設定はインターフェイスに適用され、MACsec がそのインターフェイスで設定されている場合に有効になります。

## EAPOL 設定の有効化

EAPOL 設定は、使用可能な任意のインターフェイスでイネーブルにできます。

始める前に

MACsec が有効であることを確認します。



## 手順

|        | コマンドまたはアクション                                                                                                                            | 目的                                                                                                                        |
|--------|-----------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| ステップ 1 | <b>configure terminal</b><br>例 :<br>switch# configure terminal<br>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 | <b>interface name</b><br>例 :<br>switch(config)# interface ethernet 1/1<br>switch(config-if)#                                            | 設定するインターフェイスを指定します。インターフェイスタイプと ID を指定できます。イーサネット ポートの場合は、 <b>ethernet slot/port</b> を使用します                               |
| ステップ 3 | <b>eapol mac-address mac_address [ethertype eth_type]</b>                                                                               | 指定されたインターフェイス タイプおよび ID で EAPOL 設定をイネーブルにします。<br><br>(注) イーサネットタイプが指定されていない場合、MKA パケットのデフォルトイーサネットタイプ (0x888e) であると見なします。 |
| ステップ 4 | <b>eapol mac-address broadcast-address [ethertype eth_type]</b>                                                                         | ブロードキャストアドレスを代替 MAC アドレスとしてイネーブルにします。                                                                                     |
| ステップ 5 | (任意) <b>copy running-config startup-config</b><br>例 :<br>switch(config-macseckeychain-macseckey)#<br>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 | <b>show macsec mka session detail</b>                                                                                                   | EAPOL 設定を表示します。                                                                                                           |

## EAPOL 設定の無効化

使用可能なインターフェイスで EAPOL 設定を無効にできます。

## 手順

|        | コマンドまたはアクション                                                                      | 目的                           |
|--------|-----------------------------------------------------------------------------------|------------------------------|
| ステップ 1 | <b>configure terminal</b><br>例 :<br>switch# configure terminal<br>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 | <b>interface name</b><br>例：<br>switch(config)# interface ethernet 1/1<br>switch(config-if)#                                            | 設定するインターフェイスを指定します。インターフェイスタイプと ID を指定できます。イーサネットポートの場合は、 <b>ethernet slot/port</b> を使用します |
| ステップ 3 | <b>[no] eapol mac-address mac_address</b><br><b>[ethertype eth_type]</b>                                                               | 指定されたインターフェイスタイプおよび ID で EAPOL 設定を無効にします。                                                  |
| ステップ 4 | (任意) <b>copy running-config startup-config</b><br>例：<br>switch(config-macseckeychain-macseckey)#<br>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。                                                  |

## MACsec 設定の確認

MACsec 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。

| コマンド                                                                                   | 目的                                                                   |
|----------------------------------------------------------------------------------------|----------------------------------------------------------------------|
| <b>show key chain name</b>                                                             | キーチェーンの設定を表示します。                                                     |
| <b>show macsec mka session</b><br><b>[interface type slot/port]</b><br><b>[detail]</b> | 特定のインターフェイスまたはすべてのインターフェイスの MACsec MKA セッションに関する情報を表示します。            |
| <b>show macsec mka session details</b>                                                 | すべての EAPOL パケットのインターフェイスで現在使用されている MAC アドレスおよびイーサネットタイプに関する情報を表示します。 |
| <b>show macsec mka summary</b>                                                         | MACsec MKA 設定を表示します。                                                 |
| <b>show macsec policy</b><br><b>[policy-name]</b>                                      | 特定の MACsec ポリシーまたはすべての MACsec ポリシーの設定を表示します。                         |
| <b>show running-config macsec</b>                                                      | MACsec の実行コンフィギュレーション情報を表示します。                                       |

次に、すべてのインターフェイスの MACsec MKA セッションに関する情報を表示する例を示します。

```
switch# show macsec mka session
Interface          Local-TxSCI          #Peers    Status
  Key-Server      Auth Mode
-----
Ethernet2/2       2c33.11b8.7d14/0001    1          Secured
  Yes             PRIMARY-PSK
Ethernet2/3       2c33.11b8.7d18/0001    1          Secured
```

```

Yes PRIMARY-PSK
-----
-----

```

```

Total Number of Sessions : 2
      Secured Sessions : 2
      Pending Sessions : 0

```

次に、特定のインターフェイスの MACsec MKA セッションに関する情報を表示する例を示します。前の例で説明したテーブルの一般的な要素に加えて、現在の MACsec セッションタイプを定義する認証モードも示します。

```
switch# show macsec mka session interface ethernet 1/1
```

| Interface   | Local-TxSCI         | # Peers | Status  | Key-Server | Auth Mode    |
|-------------|---------------------|---------|---------|------------|--------------|
| Ethernet1/1 | 70df.2fdc.baf4/0001 | 0       | Pending | Yes        | PRIMARY-PSK  |
| Ethernet1/1 | 70df.2fdc.baf4/0001 | 1       | Secured | No         | FALLBACK-PSK |

次に、特定のイーサネットインターフェイスの MACsec MKA セッションに関する詳細情報を表示する例を示します。

```

Interface Name      : Ethernet2/2
  Session Status    : SECURED - Secured MKA Session with MACsec
  Local Tx-SCI      : 2c33.11b8.7d14/0001
  Local Tx-SSCI     : 2
  MKA Port Identifier : 2
  CAK Name (CKN)    : 12
  CA Authentication Mode : PRIMARY-PSK
  Member Identifier (MI) : B54263EF7949A561E25CE617
  Message Number (MN) : 523
  MKA Policy Name    : tests2
  Key Server Priority : 16
  Key Server         : Yes
  Include ICV        : No
  SAK Cipher Suite   : GCM-AES-XPB-256
  SAK Cipher Suite (Operational) : GCM-AES-XPB-256
  Replay Window Size : 148809600
  Confidentiality Offset : CONF-OFFSET-0
  Confidentiality Offset (Operational) : CONF-OFFSET-0
  Latest SAK Status  : Rx & TX
  Latest SAK AN      : 0
  Latest SAK KI      : B54263EF7949A561E25CE61700000001
  Latest SAK KN      : 1
  Last SAK key time  : 12:59:38 PST Tue Mar 19 2019
  CA Peer Count      : 1
  Eapol dest mac     : 0180.c200.0003
  Ether-type         : 0x888e
Peer Status:
  Peer MI            : 2C2C090E62A96F4D6E018210
  RxSCI              : 2c33.11b8.8b88/0001
  Peer CAK           : Match
  Latest Rx MKPDU    : 13:16:54 PST Tue Mar 19 2019

```

次に、MACsec MKA 設定を表示する例を示します。

```

switch# show macsec mka summary
Interface      MACSEC-policy      Keychain
-----
Ethernet2/13   1                    1/10000000000000000000
Ethernet2/14   1                    1/10000000000000000000

```

次に、すべての MACsec ポリシーの設定を表示する例を示します。

```
switch# show macsec policy
MACSec Policy                               Cipher          Pri Window      Offset Security
      SAK Rekey time ICV Indicator
-----
system-default-macsec-policy                GCM-AES-XPN-256 16  148809600    0      should-secure
  pn-rollover FALSE
tests1                                       GCM-AES-XPN-256 16  148809600    0      should-secure
  pn-rollover FALSE
tests2                                       GCM-AES-XPN-256 16  148809600    0      should-secure
  pn-rollover FALSE
tests3                                       GCM-AES-256     16  148809600    0      should-secure
  pn-rollover FALSE
```

次の例では、**show running-config** および **show startup-config** コマンドの出力にキー オクテット文字列が表示されることを示しています。ただし、**key-chain macsec-psk no-show** コマンドが設定されている場合を除きます。

```
key chain KC256-1 macsec
  key 2000
    key-octet-string 7
    075e701e1c5a4a5143475e5a527d7c7c706a6c724306170103555a5c57510b051e47080
    a05000101005e0e50510f005c4b5f5d0b5b070e234e4d0a1d0112175b5e cryptographic-algorithm
    AES_256_CMAC
```

次の例では、**show running-config** および **show startup-config** コマンドの出力にキー オクテット文字列が表示されることを示しています。こちらは、**key-chain macsec-psk no-show** コマンドが設定されている場合です。

```
key chain KC256-1 macsec
  key 2000
    key-octet-string 7 ***** cryptographic-algorithm AES_256_CMAC
```

## MACsec 統計の表示

次のコマンドを使用して、MACsec 統計情報を表示できます。

| コマンド                                                                   | 説明                       |
|------------------------------------------------------------------------|--------------------------|
| <b>show macsec mka statistics</b> [ <i>interface type slot/port</i> ]  | MACsec MKA 統計情報を表示します。   |
| <b>show macsec secy statistics</b> [ <i>interface type slot/port</i> ] | MACsec セキュリティ統計情報を表示します。 |

次に、特定のイーサネット インターフェイスの MACsec MKA 統計情報の例を示します。

```
switch# show macsec mka statistics interface ethernet 2/2

Per-CA MKA Statistics for Session on interface (Ethernet2/2) with CKN 0x10
=====
CA Statistics
  Pairwise CAK Rekeys..... 0
```

```

SA Statistics
  SAKs Generated..... 0
  SAKs Rekeyed..... 0
  SAKs Received..... 0
  SAK Responses Received.. 0

MKPDU Statistics
  MKPDUs Transmitted..... 1096
    "Distributed SAK".. 0

  MKPDUs Validated & Rx... 0
    "Distributed SAK".. 0

MKA Statistics for Session on interface (Ethernet2/2)
=====
CA Statistics
  Pairwise CAK Rekeys..... 0

SA Statistics
  SAKs Generated..... 0
  SAKs Rekeyed..... 0
  SAKs Received..... 0
  SAK Responses Received.. 0

MKPDU Statistics
  MKPDUs Transmitted..... 1096
    "Distributed SAK".. 0
  MKPDUs Validated & Rx... 0
    "Distributed SAK".. 0
  MKPDUs Tx Success..... 1096
  MKPDUs Tx Fail..... 0
  MKPDU Tx Pkt build fail... 0
  MKPDU No Tx on intf down.. 0
  MKPDU No Rx on intf down.. 0
  MKPDUs Rx CA Not found..... 0
  MKPDUs Rx Error..... 0
  MKPDUs Rx Success..... 0

MKPDU Failures
  MKPDU Rx Validation ..... 0
  MKPDU Rx Bad Peer MN..... 0
  MKPDU Rx Non-recent Peerlist MN..... 0
  MKPDU Rx Drop SAKUSE, KN mismatch..... 0
  MKPDU Rx Drop SAKUSE, Rx Not Set..... 0
  MKPDU Rx Drop SAKUSE, Key MI mismatch.... 0
  MKPDU Rx Drop SAKUSE, AN Not in Use..... 0
  MKPDU Rx Drop SAKUSE, KS Rx/Tx Not Set... 0
  MKPDU Rx Drop Packet, Ethertype Mismatch. 0

SAK Failures
  SAK Generation..... 0
  Hash Key Generation..... 0
  SAK Encryption/Wrap..... 0
  SAK Decryption/Unwrap..... 0

CA Failures
  ICK Derivation..... 0
  KEK Derivation..... 0
  Invalid Peer MACsec Capability... 0

MACsec Failures
  Rx SA Installation..... 0

```

```
Tx SA Installation..... 0
```

次に、特定のイーサネットインターフェイスの MACsec セキュリティ統計情報を表示する例を示します。



(注) Rx および Tx 統計情報の非制御パケットと制御パケットには、次の違いがあります。

- Rx 統計
  - 非制御=暗号化および非暗号化
  - 制御 = 非暗号化
- TX 統計情報 :
  - 非制御 = 非暗号化
  - 制御 = 暗号化
  - 共通 = 暗号化および非暗号化

```
switch(config)# show macsec secy statistics interface e2/28/1

Interface Ethernet2/28/1 MACSEC SecY Statistics:
-----
Interface Rx Statistics:
  Unicast Uncontrolled Pkts: 14987
  Multicast Uncontrolled Pkts: 1190444
  Broadcast Uncontrolled Pkts: 4
  Uncontrolled Pkts - Rx Drop: 0
  Uncontrolled Pkts - Rx Error: 0
  Unicast Controlled Pkts: N/A (N9K-X9736C-FX not supported)
  Multicast Controlled Pkts: N/A (N9K-X9736C-FX not supported)
  Broadcast Controlled Pkts: N/A (N9K-X9736C-FX not supported)
  Controlled Pkts: 247583
  Controlled Pkts - Rx Drop: N/A (N9K-X9736C-FX not supported)
  Controlled Pkts - Rx Error: N/A (N9K-X9736C-FX not supported)
  In-Octets Uncontrolled: 169853963 bytes
  In-Octets Controlled: 55027017 bytes
  Input rate for Uncontrolled Pkts: N/A (N9K-X9736C-FX not supported)
  Input rate for Uncontrolled Pkts: N/A (N9K-X9736C-FX not supported)
  Input rate for Controlled Pkts: N/A (N9K-X9736C-FX not supported)
  Input rate for Controlled Pkts: N/A (N9K-X9736C-FX not supported)

Interface Tx Statistics:
  Unicast Uncontrolled Pkts: N/A (N9K-X9736C-FX not supported)
  Multicast Uncontrolled Pkts: N/A (N9K-X9736C-FX not supported)
  Broadcast Uncontrolled Pkts: N/A (N9K-X9736C-FX not supported)
  Uncontrolled Pkts - Rx Drop: N/A (N9K-X9736C-FX not supported)
  Uncontrolled Pkts - Rx Error: N/A (N9K-X9736C-FX not supported)
  Unicast Controlled Pkts: N/A (N9K-X9736C-FX not supported)
  Multicast Controlled Pkts: N/A (N9K-X9736C-FX not supported)
  Broadcast Controlled Pkts: N/A (N9K-X9736C-FX not supported)
  Controlled Pkts: 205429
  Controlled Pkts - Rx Drop: N/A (N9K-X9736C-FX not supported)
  Controlled Pkts - Rx Error: N/A (N9K-X9736C-FX not supported)
  Out-Octets Uncontrolled: N/A (N9K-X9736C-FX not supported)
```

```

Out-Octets Controlled: 20612648 bytes
Out-Octets Common: 151787484 bytes
Output rate for Uncontrolled Pkts: N/A (N9K-X9736C-FX not supported)
Output rate for Uncontrolled Pkts: N/A (N9K-X9736C-FX not supported)
Output rate for Controlled Pkts: N/A (N9K-X9736C-FX not supported)
Output rate for Controlled Pkts: N/A (N9K-X9736C-FX not supported)

SECY Rx Statistics:
Transform Error Pkts: N/A (N9K-X9736C-FX not supported)
Control Pkts: 952284
Untagged Pkts: N/A (N9K-X9736C-FX not supported)
No Tag Pkts: 0
Bad Tag Pkts: 0
No SCI Pkts: 0
Unknown SCI Pkts: 0
Tagged Control Pkts: N/A (N9K-X9736C-FX not supported)

SECY Tx Statistics:
Transform Error Pkts: N/A (N9K-X9736C-FX not supported)
Control Pkts: 967904
Untagged Pkts: N/A (N9K-X9736C-FX not supported)

SAK Rx Statistics for AN [3]:
Unchecked Pkts: 0
Delayed Pkts: 0
Late Pkts: 0
OK Pkts: 1
Invalid Pkts: 0
Not Valid Pkts: 0
Not-Using-SA Pkts: 0
Unused-SA Pkts: 0
Decrypted In-Octets: 235 bytes
Validated In-Octets: 0 bytes

SAK Tx Statistics for AN [3]:
Encrypted Protected Pkts: 2
Too Long Pkts: N/A (N9K-X9736C-FX not supported)
SA-not-in-use Pkts: N/A (N9K-X9736C-FX not supported)
Encrypted Protected Out-Octets: 334 bytes
switch(config)#

```

## MACsec の設定例

次に、ユーザ定義の MACsec ポリシーを設定し、そのポリシーをインターフェイスに適用する例を示します。

```

switch(config)# macsec policy 1
switch(config-macsec-policy)# cipher-suite GCM-AES-256
switch(config-macsec-policy)# window-size 512
switch(config-macsec-policy)# key-server-priority 0
switch(config-macsec-policy)# conf-offset CONF-OFFSET-0
switch(config-macsec-policy)# security-policy should-secure
switch(config-macsec-policy)# exit

```

```

switch(config)# int e2/13-14
switch(config-if-range)# macsec keychain 1 policy 1
switch(config-if-range)# exit
switch(config)# show macsec mka summary

```

| Interface    | MACSEC-policy | Keychain             |
|--------------|---------------|----------------------|
| Ethernet2/13 | 1             | 1/100000000000000000 |

```
Ethernet2/14      1                               1/100000000000000000
```

```
switch(config)# show macsec mka session
Interface      Local-TxSCI      # Peers   Status   Key-Server
-----
Ethernet2/13   006b.flbe.d31c/0001  1         Secured  Yes
Ethernet2/14   006b.flbe.d320/0001  1         Secured  No
```

```
switch(config)# show running-config macsec
!Command: show running-config macsec
!Time: Mon Dec  5 04:53:40 2016
```

```
version 9.2(1)feature macsec
macsec policy 1
  cipher-suite GCM-AES-256
  key-server-priority 0
  window-size 512
  conf-offset CONF-OFFSET-0
  security-policy should-secure
```

```
interface Ethernet2/13
  macsec keychain 1 policy 1
```

```
interface Ethernet2/14
  macsec keychain 1 policy 1
```

次に、MACsec キーチェーンを設定し、インターフェイスにシステムデフォルトの MACsec ポリシーを追加する例を示します。

```
switch(config)# key chain 1 macsec
switch(config-macseckeychain)# key 1000
switch(config-macseckeychain-macseckey)# key-octet-string
abcdef0123456789abcdef0123456789abcdef0123456789abcdef0123456789 cryptographic-algorithm
aes_256_CMAC
switch(config-macseckeychain-macseckey)# exit
```

```
switch(config)# int e2/13-14
switch(config-if-range)# macsec keychain 1
switch(config-if-range)# exit
switch(config)#
```

```
switch(config)# show running-config macsec
!Command: show running-config macsec
!Time: Mon Dec  5 04:50:16 2016
version 7.0(3)I4(5)
feature macsec
interface Ethernet2/13
  macsec keychain 1 policy system-default-macsec-policy
interface Ethernet2/14
  macsec keychain 1 policy system-default-macsec-policy
```

```
switch(config)# show macsec mka session
Interface      Local-TxSCI      # Peers   Status
Key-Server     Auth Mode
-----
Ethernet2/2    2c33.11b8.7d14/0001  1         Secured
  Yes          PRIMARY-PSK
Ethernet2/3    2c33.11b8.7d18/0001  1         Secured
  Yes          PRIMARY-PSK
-----
Total Number of Sessions : 2
```



```

Secured Sessions : 2
Pending Sessions : 0

switch(config)# show macsec mka summary
Interface          Status  Cipher (Operational)  Key-Server  MACSEC-policy  Keychain
  Fallback-keychain
-----
-----
Ethernet2/1        down    -                      -            tests1         keych1
  no keychain
Ethernet2/2        Secured GCM-AES-XPB-256      Yes          tests2         keych2
  no keychain
Ethernet2/3        Secured GCM-AES-256      Yes          tests3         keyc3
  no keychain

```

## XML の例

MACsec は、`|xml` を使用したスクリプト用に次の `show` コマンドの XML 出力をサポートします。

- `show key chain name |xml`
- `show macsec mka session interface interface slot/port details |xml`
- `show macsec mka statistics interface interface slot/port |xml`
- `show macsec mka summary |xml`
- `show macsec policy name |xml`
- `show macsec secy statistics interface interface slot/port |xml`
- `show running-config macsec |xml`

次に、上記の各 `show` コマンドの出力例を示します。

例 1：キーチェーンの設定を表示します

```

switch# show key chain "Kc2" |xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="http://www.cisco.com/nxos:1.0:rpm">
  <nf:data>
    <show>
      <key>
        <chain>
          <__XML__OPT_Cmd_rpm_show_keychain_cmd_keychain>
            <keychain>Kc2</keychain>
          </__XML__OPT_Cmd_rpm_show_keychain_cmd_keychain>
        </chain>
      </key>
    </show>
  </nf:data>
</nf:rpc-reply>
]]>]]>

```

例 2：特定のインターフェイスの MACsec MKA セッションに関する情報を表示します。



```

<show>
<macsec>
  <mka>
    <statistics>
      <__XML__OPT_Cmd_some_macsec_mka_statistics_interface>
        <interface>
          <__XML__INTF_ifname>
            <__XML__PARAM_value>
              <__XML__INTF_output>Ethernet4/31</__XML__INTF_output>
              <__XML__INTF_output>Ethernet4/31</__XML__INTF_output>
            </__XML__PARAM_value>
          </__XML__INTF_ifname>
        </interface>
        <__XML__OPT_Cmd_some_macsec_mka_statistics__readonly__>
          <__readonly__>
            <TABLE_mka_intf_stats>
              <ROW_mka_intf_stats>
                <TABLE_ca_stats>
                  <ROW_ca_stats>
                    <ca_stat_ckn>0x2</ca_stat_ckn>
                    <ca_stat_pairwise_cak_rekey>0</ca_stat_pairwise_cak_rekey>
                    <sa_stat_sak_generated>0</sa_stat_sak_generated>
                    <sa_stat_sak_rekey>0</sa_stat_sak_rekey>
                    <sa_stat_sak_received>91</sa_stat_sak_received>
                    <sa_stat_sak_response_rx>0</sa_stat_sak_response_rx>
                    <mkpdu_stat_mkpdu_tx>2808</mkpdu_stat_mkpdu_tx>
                    <mkpdu_stat_mkpdu_tx_distsak>0</mkpdu_stat_mkpdu_tx_distsak>
                    <mkpdu_stat_mkpdu_rx>2714</mkpdu_stat_mkpdu_rx>
                    <mkpdu_stat_mkpdu_rx_distsak>91</mkpdu_stat_mkpdu_rx_distsak>
                  </ROW_ca_stats>
                </TABLE_ca_stats>
              </ROW_mka_intf_stats>
            </TABLE_mka_intf_stats>
          </__readonly__>
        </__XML__OPT_Cmd_some_macsec_mka_statistics__readonly__>
        <interface>
          <__XML__INTF_ifname>
            <__XML__PARAM_value>
              <__XML__INTF_output>Ethernet4/31</__XML__INTF_output>
            </__XML__PARAM_value>
          </__XML__INTF_ifname>
        </interface>
        <__XML__OPT_Cmd_some_macsec_mka_statistics__readonly__>
          <__readonly__>
            <TABLE_mka_intf_stats>
              <ROW_mka_intf_stats>
                <TABLE_idb_stats>
                  <ROW_idb_stats>
                    <ca_stat_pairwise_cak_rekey>0</ca_stat_pairwise_cak_rekey>
                    <sa_stat_sak_generated>0</sa_stat_sak_generated>
                    <sa_stat_sak_rekey>0</sa_stat_sak_rekey>
                    <sa_stat_sak_received>91</sa_stat_sak_received>
                    <sa_stat_sak_response_rx>0</sa_stat_sak_response_rx>
                    <mkpdu_stat_mkpdu_tx>2808</mkpdu_stat_mkpdu_tx>
                    <mkpdu_stat_mkpdu_tx_distsak>0</mkpdu_stat_mkpdu_tx_distsak>
                    <mkpdu_stat_mkpdu_rx>2714</mkpdu_stat_mkpdu_rx>
                    <mkpdu_stat_mkpdu_rx_distsak>91</mkpdu_stat_mkpdu_rx_distsak>
                    <idb_stat_mkpdu_tx_success>2808</idb_stat_mkpdu_tx_success>
                    <idb_stat_mkpdu_tx_fail>0</idb_stat_mkpdu_tx_fail>
                    <idb_stat_mkpdu_tx_pkt_build_fail>0</idb_stat_mkpdu_tx_pkt_build_fail>
                    <idb_stat_mkpdu_no_tx_on_intf_down>0</idb_stat_mkpdu_no_tx_on_intf_down>
                    <idb_stat_mkpdu_no_rx_on_intf_down>0</idb_stat_mkpdu_no_rx_on_intf_down>
                    <idb_stat_mkpdu_rx_ca_notfound>0</idb_stat_mkpdu_rx_ca_notfound>
                    <idb_stat_mkpdu_rx_error>0</idb_stat_mkpdu_rx_error>
                  </ROW_idb_stats>
                </TABLE_idb_stats>
              </ROW_mka_intf_stats>
            </TABLE_mka_intf_stats>
          </__readonly__>
        </__XML__OPT_Cmd_some_macsec_mka_statistics__readonly__>
      </__XML__OPT_Cmd_some_macsec_mka_statistics__readonly__>
    </statistics>
  </mka>
</macsec>
</show>

```

```

        <idb_stat_mkpdu_rx_success>2714</idb_stat_mkpdu_rx_success>
        <idb_stat_mkpdu_failure_rx_integrity_check_error>0</idb_stat_mkpdu_
failure_rx_integrity_check_error>
        <idb_stat_mkpdu_failure_invalid_peer_mn_error>0</idb_stat_mkpdu_fai
lure_invalid_peer_mn_error>
        <idb_stat_mkpdu_failure_nonrecent_peerlist_mn_error>1</idb_stat_mkp
du_failure_nonrecent_peerlist_mn_error>
        <idb_stat_mkpdu_failure_sakuse_kn_mismatch_error>0</idb_stat_mkpdu_
failure_sakuse_kn_mismatch_error>
<idb_stat_mkpdu_failure_sakuse_rx_not_set_error>0</idb_stat_mkpdu_f
ailure_sakuse_rx_not_set_error>
        <idb_stat_mkpdu_failure_sakuse_key_mi_mismatch_error>0</idb_stat_mk
pdu_failure_sakuse_key_mi_mismatch_error>
        <idb_stat_mkpdu_failure_sakuse_sakuse_an_not_in_use_error>0</idb_stat_mkpdu
failure_sakuse_an_not_in_use_error>
        <idb_stat_mkpdu_failure_sakuse_ks_rx_tx_not_set_error>0</idb_stat_m
kpdu_failure_sakuse_ks_rx_tx_not_set_error>
        <idb_stat_mkpdu_failure_sakuse_eapol_ethertype_mismatch_error>0</id
b_stat_mkpdu_failure_sakuse_eapol_ethertype_mismatch_error>
        <idb_stat_sak_failure_sak_generate_error>0</idb_stat_sak_failure_sa
k_generate_error>
        <idb_stat_sak_failure_hash_generate_error>0</idb_stat_sak_failure_h
ash_generate_error>
        <idb_stat_sak_failure_sak_encryption_error>0</idb_stat_sak_failure_
sak_encryption_error>
        <idb_stat_sak_failure_sak_decryption_error>0</idb_stat_sak_failure_
sak_decryption_error>
        <idb_stat_sak_failure_ick_derivation_error>0</idb_stat_sak_failure_
ick_derivation_error>
        <idb_stat_sak_failure_kek_derivation_error>0</idb_stat_sak_failure_
kek_derivation_error>
        <idb_stat_sak_failure_invalid_macsec_capability_error>0</idb_stat_s
ak_failure_invalid_macsec_capability_error>
        <idb_stat_macsec_failure_rx_sa_create_error>0</idb_stat_macsec_fail
ure_rx_sa_create_error>
        <idb_stat_macsec_failure_tx_sa_create_error>0</idb_stat_macsec_fail
ure_tx_sa_create_error>
    </ROW_idb_stats>
</TABLE_idb_stats>
</ROW_mka_intf_stats>
</TABLE_mka_intf_stats>
</__readonly__>
</__XML__OPT_Cmd_some_macsec_mka_statistics__readonly__>
</__XML__OPT_Cmd_some_macsec_mka_statistics_interface>
</statistics>
</mka>
</macsec>
</show>
</nf:data>
</nf:rpc-reply>
]]>]]>

```

例 4 : MACsec MKA 設定を表示します。

```

switch# show macsec mka summary | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="http://ww
ww.cisco.com/nxos:1.0">
  <nf:data>
    <show>
      <macsec>
        <mka>
          <__XML__OPT_Cmd_some_macsec_summary>
            <__XML__OPT_Cmd_some_macsec__readonly__>

```



```

</show>
</nf:data>
</nf:rpc-reply>
]]>]]>

```

例 6 : MACsec セキュリティ統計情報を表示します。

```

switch# show macsec secy statistics interface ethernet 4/31 | xml
<?xml version="1.0" encoding="ISO-8859-1"?>
<nf:rpc-reply xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="http://www.cisco.com/nxos:1.0">
  <nf:data>
    <show>
      <macsec>
        <secy>
          <statistics>
            <interface>
              <_XML_INTF_ifname>
                <_XML_PARAM_value>
                  <_XML_INTF_output>Ethernet4/31</_XML_INTF_output>
                </_XML_PARAM_value>
              <_XML_OPT_Cmd_some_macsec_secy_statistics__readonly__>
                <_readonly__>
                  <TABLE_statistics>
                    <ROW_statistics>
                      <in_pkts_unicast_uncontrolled>0</in_pkts_unicast_uncontrolled>
                      <in_pkts_multicast_uncontrolled>42</in_pkts_multicast_uncontrolled>
                      <in_pkts_broadcast_uncontrolled>0</in_pkts_broadcast_uncontrolled>
                      <in_rx_drop_pkts_uncontrolled>0</in_rx_drop_pkts_uncontrolled>
                      <in_rx_err_pkts_uncontrolled>0</in_rx_err_pkts_uncontrolled>
                      <in_pkts_unicast_controlled>0</in_pkts_unicast_controlled>
                      <in_pkts_multicast_controlled>2</in_pkts_multicast_controlled>
                      <in_pkts_broadcast_controlled>0</in_pkts_broadcast_controlled>
                      <in_rx_drop_pkts_controlled>0</in_rx_drop_pkts_controlled>
                      <in_rx_err_pkts_controlled>0</in_rx_err_pkts_controlled>
                      <in_octets_uncontrolled>7230</in_octets_uncontrolled>
                      <in_octets_controlled>470</in_octets_controlled>
                      <input_rate_uncontrolled_pps>0</input_rate_uncontrolled_pps>
                      <input_rate_uncontrolled_bps>9</input_rate_uncontrolled_bps>
                      <input_rate_controlled_pps>0</input_rate_controlled_pps>
                      <input_rate_controlled_bps>23</input_rate_controlled_bps>
                      <out_pkts_unicast_uncontrolled>0</out_pkts_unicast_uncontrolled>
                      <out_pkts_multicast_uncontrolled>41</out_pkts_multicast_uncontrolled>
                      <out_pkts_broadcast_uncontrolled>0</out_pkts_broadcast_uncontrolled>
                      <out_rx_drop_pkts_uncontrolled>0</out_rx_drop_pkts_uncontrolled>
                      <out_rx_err_pkts_uncontrolled>0</out_rx_err_pkts_uncontrolled>
                      <out_pkts_unicast_controlled>0</out_pkts_unicast_controlled>
                      <out_pkts_multicast_controlled>2</out_pkts_multicast_controlled>
                      <out_pkts_broadcast_controlled>0</out_pkts_broadcast_controlled>
                      <out_rx_drop_pkts_controlled>0</out_rx_drop_pkts_controlled>
                      <out_rx_err_pkts_controlled>0</out_rx_err_pkts_controlled>
                      <out_octets_uncontrolled>6806</out_octets_uncontrolled>
                      <out_octets_controlled>470</out_octets_controlled>
                      <out_octets_common>7340</out_octets_common>
                      <output_rate_uncontrolled_pps>2598190092</output_rate_uncontrolled_pps>
                      <output_rate_uncontrolled_bps>2598190076</output_rate_uncontrolled_bps>
                      <output_rate_controlled_pps>0</output_rate_controlled_pps>
                      <output_rate_controlled_bps>23</output_rate_controlled_bps>
                      <in_pkts_transform_error>0</in_pkts_transform_error>
                      <in_pkts_control>40</in_pkts_control>
                      <in_pkts_untagged>0</in_pkts_untagged>
                      <in_pkts_no_tag>0</in_pkts_no_tag>
                      <in_pkts_badtag>0</in_pkts_badtag>
                      <in_pkts_no_sci>0</in_pkts_no_sci>
                    </ROW_statistics>
                  </TABLE_statistics>
                </_readonly__>
              </_XML_OPT_Cmd_some_macsec_secy_statistics__readonly__>
            </interface>
          </statistics>
        </secy>
      </macsec>
    </show>
  </nf:data>
</nf:rpc-reply>

```

```

<in_pkts_unknown_sci>0</in_pkts_unknown_sci>
<in_pkts_tagged_ctrl>0</in_pkts_tagged_ctrl>
<out_pkts_transform_error>0</out_pkts_transform_error>
<out_pkts_control>41</out_pkts_control>
<out_pkts_untagged>0</out_pkts_untagged>
<rx_sa_an>1</rx_sa_an>
<in_pkts_unchecked>0</in_pkts_unchecked>
<in_pkts_delayed>0</in_pkts_delayed>
<in_pkts_late>0</in_pkts_late>
<in_pkts_ok>1</in_pkts_ok>
<in_pkts_invalid>0</in_pkts_invalid>
<in_pkts_not_valid>0</in_pkts_not_valid>
<in_pkts_not_using_sa>0</in_pkts_not_using_sa>
<in_pkts_unused_sa>0</in_pkts_unused_sa>
<in_octets_decrypted>223</in_octets_decrypted>
<in_octets_validated>0</in_octets_validated>
<tx_sa_an>1</tx_sa_an>
<out_pkts_encrypted_protected>1</out_pkts_encrypted_protected>
<out_pkts_too_long>0</out_pkts_too_long>
<out_pkts_sa_not_inuse>0</out_pkts_sa_not_inuse>
<out_octets_encrypted_protected>223</out_octets_encrypted_protected>
</ROW_statistics>
</TABLE_statistics>
</__readonly__>
</__XML__OPT_Cmd_some_macsec_secy_statistics__readonly__>
</__XML__INTF_ifname>
</interface>
</statistics>
</secy>
</macsec>
</show>
</nf:data>
</nf:rpc-reply>
]]>]]>

```

例 7 : MACsec の実行コンフィギュレーション情報を表示します。

```

switch# show running-config macsec | xml

!Command: show running-config macsec
!Time: Fri Jan 20 07:12:34 2017

version 7.0(3)I4(6)
*****
This may take time. Please be patient.
*****
<?xml version="1.0"?>
<nf:rpc xmlns:nf="urn:ietf:params:xml:ns:netconf:base:1.0" xmlns="http://www.cis
co.com/nxos:7.0.3.I4.6.:configure_" xmlns:m="http://www.cisco.com/nxos:7.0.3.I4.6.:_exec"
xmlns:m1="http://www.cisco.com/nxos:7.0.3.I4.6.:configure__macsec__policy"
xmlns:m2="http://www.cisco.com/nxos:7.0.3.I4.6.:configure__if-eth-non-member_"
message-id="1">
  <nf:get-config>
    <nf:source>
      <nf:running/>
    </nf:source>
    <nf:filter>
      <m:configure>
        <m:terminal>
          <feature>
            <macsec/>
          </feature>
          <macsec>
            <policy>

```

```

    <__XML_PARAM_policy_name>
      <__XML_value>am2</__XML_value>
      <ml:cipher-suite>
        <ml:__XML_PARAM_suite>
          <ml:__XML_value>GCM-AES-XPB-256</ml:__XML_value>
        </ml:__XML_PARAM_suite>
      </ml:cipher-suite>
      <ml:key-server-priority>
        <ml:__XML_PARAM_pri>
          <ml:__XML_value>0</ml:__XML_value>
        </ml:__XML_PARAM_pri>
      </ml:key-server-priority>
    </ml:window-size>
  <ml:__XML_PARAM_size>
    <ml:__XML_value>512</ml:__XML_value>
  </ml:__XML_PARAM_size>
</ml:window-size>
<ml:conf-offset>
  <ml:__XML_PARAM_offset>
    <ml:__XML_value>CONF-OFFSET-0</ml:__XML_value>
  </ml:__XML_PARAM_offset>
</ml:conf-offset>
<ml:security-policy>
  <ml:__XML_PARAM_policy>
    <ml:__XML_value>must-secure</ml:__XML_value>
  </ml:__XML_PARAM_policy>
</ml:security-policy>
<ml:sak-expiry-time>
  <ml:__XML_PARAM_ts>
    <ml:__XML_value>60</ml:__XML_value>
  </ml:__XML_PARAM_ts>
</ml:sak-expiry-time>
</__XML_PARAM_policy_name>
</policy>
</macsec>
<interface>
  <__XML_PARAM_interface>
    <__XML_value>Ethernet2/1</__XML_value>
  <m2:macsec>
    <m2:keychain>
      <m2:__XML_PARAM_keychain_name>
        <m2:__XML_value>kc2</m2:__XML_value>
      <m2:policy>
        <m2:__XML_PARAM_policy_name>
          <m2:__XML_value>am2</m2:__XML_value>
        </m2:__XML_PARAM_policy_name>
      </m2:policy>
    </m2:__XML_PARAM_keychain_name>
  </m2:keychain>
</m2:macsec>
</__XML_PARAM_interface>
</interface>

```

[TRUNCATED FOR READABILITY]

```

<interface>
  <__XML_PARAM_interface>
    <__XML_value>Ethernet4/31</__XML_value>
  <m2:macsec>
    <m2:keychain>
      <m2:__XML_PARAM_keychain_name>
        <m2:__XML_value>kc2</m2:__XML_value>
      <m2:policy>
        <m2:__XML_PARAM_policy_name>

```



```

        <m2:XML_value>am2</m2:XML_value>
      </m2:XML_PARAM_policy_name>
    </m2:policy>
    <m2:XML_PARAM_keychain_name>
  </m2:keychain>
</m2:macsec>
</XML_PARAM_interface>
</interface>
</m:terminal>
</m:configure>
</nf:filter>
</nf:get-config>
</nf:rpc>
]]>]]>

```

## MIB

MACsec は次の MIB をサポートします。

- IEEE8021-SECY-MIB
- CISCO-SECY-EXT-MIB

サポートされている MIB を検索してダウンロードするには、

<ftp://ftp.cisco.com/pub/mibs/supportlists/nexus9000/Nexus9000MIBSupportList.html> にアクセスします。

## 関連資料

| 関連項目       | マニュアルタイトル                                                                    |
|------------|------------------------------------------------------------------------------|
| キーチェーン管理   | <a href="#">『Cisco Nexus 9000 Series NX-OS Security Configuration Guide』</a> |
| システム メッセージ | <a href="#">Cisco Nexus 9000 シリーズ NX-OS システム メッセージ リファレンス</a>                |





## 索引

### 記号

- ?? [266](#)
- 802.1X [266](#)
- ???
- ????? [229](#)
- ??????? [265](#)
- 802.1X ??? [265](#)

### 数字

- 802.1X [265, 267, 269, 270, 271, 272, 274, 275, 276, 296, 302](#)
- MAC 認証バイパス [269](#)
- オーセンティケータ PAE [267](#)
- 機能のイネーブル化 [276](#)
- サポートされるトポロジ [271](#)
- シングル ホストのサポート [270](#)
- 制限事項 [272](#)
- 設定 [275](#)
- 設定の確認 [296](#)
- 設定例 [302](#)
- 説明 [265](#)
- 前提条件 [272](#)
- ガイドラインに準拠 [272](#)
- デフォルト設定 [274](#)
- マルチ ホストのサポート [270](#)
- 802.1X ?? [266](#)
- ?? [266](#)
- 802.1X 再認証 [295](#)
- インターフェイスでの最大再試行回数の設定 [295](#)
- 802.1X サブリカント [281](#)
- 手動による再認証 [281](#)
- 802.1X 認証 [268, 293](#)
- RADIUS アカウンティングのイネーブル化 [293](#)
- ポートの許可ステート [268](#)

### A

- aaa accounting dot1x default group [294](#)
- aaa authentication dot1x default group [277](#)
- aaa authentication login error-enable [37](#)
- aaa accounting default [26](#)

- aaa accounting default group [44](#)
- aaa accounting default local [44](#)
- aaa authentication login {mschap | mschapv2} enable [42](#)
- aaa authentication login ascii-authentication [111](#)
- aaa authentication login chap enable [40](#)
- aaa authentication login console [26, 31, 32](#)
- aaa authentication login console group [31, 32](#)
- aaa authentication login console local [31, 32](#)
- aaa authentication login console none [31, 32](#)
- aaa authentication login default [25](#)
- aaa authorization {commands | config-commands} {console | default} {group} [114](#)
- aaa authorization {group | local} [146](#)
- aaa authorization {ssh-certificate | ssh-publickey} [146](#)
- aaa authorization default [146](#)
- aaa authorization ssh-certificate default [112](#)
- aaa group server ldap [138](#)
- aaa group server radius [69](#)
- aaa group server tacacs+ [101](#)
- aaa user default-role [36](#)
- absolute end [390](#)
- absolute start [390](#)
- accept-lifetime [558](#)
- aclog match-log-level [370](#)
- action {drop | forward | redirect} [415](#)
- authentication (bind-first | compare) [138](#)

### B

- BGP [564](#)
- ユニキャスト RPF との使用 [564](#)

### C

- CA [183, 184, 186, 187, 189, 193, 196, 198, 203, 205, 206, 209](#)
- ????????????? [209](#)
- identity [184](#)
- アイデンティティ証明書のインストール [198](#)
- アイデンティティ証明書要求の作成 [196](#)
- カットアンドペーストによる登録 [186](#)
- 証明書の削除 [203](#)
- 設定 [189](#)
- 設定の表示 [205](#)
- 設定例 [206](#)

## CA (続き)

- 説明 183
- 認証 193
- ピア証明書 187
- 複数 187
- 複数のトラスト ポイント 186
- 目的 183

## CA トラスト ポイント 192

- PKI のアソシエーションの作成 192

## chgrp 154

## chown 154

## cipher-suite 642

## class-map 596

## class-map type control-plane {match-all | match-any} 602, 611, 613

## class class-default 603

## class insert-before 603

## clear hardware rate-limiter {all | access-list-log | bfd | exception | fex | layer-3 glean | layer-3 multicast local-groups | span-egress} 628

## clear port-security dynamic address 435

## clear port-security dynamic 436

## clear access-list ipsg stats 540

## clear accounting log 51

## clear copp statistics 619

## clear hardware rate-limiter module 628

## clear ip access-list counters 377

## clear ip arp inspection log 528

## clear ip arp inspection statistics 528

## clear ip dhcp global statistics 494

## clear ip dhcp relay statistics interface 494

## clear ip dhcp snooping binding interface ethernet 493

## clear ip dhcp snooping binding interface port-channel 493

## clear ip dhcp snooping binding vlan 493

## clear ip dhcp snooping statistics 494

## clear ip dhcp snooping statistics vlan 494

## clear ipv6 access-list counters 377

## clear ipv6 dhcp relay statistics interface 494

## clear ldap-server statistics 147

## clear line 174, 176

## clear mac access-list counters 408

## clear radius-server statistics 86

## clear ssh hosts 172

## clear tacacs-server statistics 123

## conf-offset 643

## control-plane 596, 606, 607

## copp copy profile {strict | moderate | lenient | dense} 609

## copp copy profile prefix | suffix} 609

## copp profile 608

## copp profile dense 608

## copp profile lenient 608

## copp profile moderate 608

## copp profile strict 608

## copy scp 179

## copy scp: 160

## copy sftp 179

## CRL 187, 202, 232, 234, 239

## ?? 232

## ?????? 232, 234

## インポートの例 239

## 設定 202

## 説明 187

## crypto ca auticate 165

## crypto ca crl request 166

## crypto ca trustpoint 165

## cryptographic-algorithm {HMAC-SHA-1 | HMAC-SHA-256 | HMAC-SHA-384 | HMAC-SHA-512 | MD5} 560

## D

## DHCP リレー オンスタック 499

## 説明 499

## DoS 攻撃 565

## ユニキャスト RPF、配置 565

## dot1x default 291

## dot1x host-mode {multi-host | single-host} 288

## dot1x max-req 292

## dot1x port-control {auto | force-authorized | forced-unauthorized} 278

## dot1x re-authentication 280

## dot1x timeout quiet-period 283

## dot1x timeout ratelimit-period 283

## dot1x timeout re-authperiod 281

## dot1x timeout server-timeout 283

## dot1x timeout supp-timeout 283

## dot1x timeout tx-period 284

## E

## enable Cert-DN-match 138

## enable user-server-group 138

## encryption decrypt type6 547

## encryption delete type6 549

## encryption re-encrypt obfuscated 546, 547, 555

## F

## feature dot1x 276

## feature macsec 637, 638

## feature port-security 430

## feature dhcp 458

## feature ldap 134

## feature password encryption aes 546, 555

## feature privilege 118

## feature scp-server 163

## feature sftp-server 164

## feature ssh 156, 171

## feature tacacs+ 96

## feature telnet 174

## FIPS 15, 18, 19, 20

## 有効化 18

## FIPS (続き)

- 設定例 20
- セルフテスト 15
- 無効化 19

fragments {permit-all | deny-all} 335, 338

## G

generate type7\_encrypted\_secret 50, 66, 68, 98, 100

## H

- hardware access-list tcam region ing-ifacl qualify udf 364, 399
- hardware rate-limiter span-egress 627
- hardware access-list tcam region 343, 612
- hardware profile tcam resource service-template 355
- hardware profile tcam resource template 354
- hardware rate-limiter access-list-log 370, 626
- hardware rate-limiter bfd 626
- hardware rate-limiter exception 626
- hardware rate-limiter fex 626
- hardware rate-limiter layer-3 glean 626
- hardware rate-limiter layer-3 multicast local-groups 627

## I

ID 証明書 196, 198, 203

- PKI の削除 203
- インストール 198
- 要求の作成 196

interface policy dent 256

- ip dhcp relay information option server-id-override-disable 473
- ip dhcp relay sub-option circuit-id customized 470
- ip dhcp relay sub-option circuit-id format-type string 470
- ip verify unicast source reachable-via any 568
- ip verify unicast source reachable-via 570
- ip access-class 340
- ip access-group 366, 369
- ip access-list 335, 337, 339, 365, 371
- ip arp inspection log-buffer entries 526
- ip arp inspection trust 524
- ip arp inspection validate 525
- ip arp inspection validate dst-mac 525
- ip arp inspection validate ip 525
- ip arp inspection validate src-mac 525
- ip arp inspection vlan 523, 526
- ip dhcp packet strict-validation 448, 464
- ip dhcp relay 469, 472
- ip dhcp relay address 474, 475
- ip dhcp relay address use-vrf 474
- ip dhcp relay information option 470
- ip dhcp relay information option trust 466
- ip dhcp relay information option vpn 472
- ip dhcp relay information trust-all 468

- ip dhcp relay information trusted 467
- ipdhcprelaysource-interface 475
- ip dhcp relay sub-option type cisco 472
- ip dhcp smart-relay 478
- ip dhcp smart-relay global 477
- ip dhcp snooping information option 462
- ip dhcp snooping ipsg-excluded vlan 540
- ip dhcp snooping trust 465
- ip dhcp snooping verify mac-address 460
- ip dhcp snooping vlan 460
- ip port access group 368
- ip radius source-interface 71
- ip source binding 539
- ip tacacs source-interface 102
- ipv6 address use-link-local-only 487
- ipv6 traffic-filter 366
- ipv6 verify unicast source reachable-via any 568
- ipv6 verify unicast source reachable-via 570
- ipv6 access-class 340
- ipv6 access-list 335, 337, 339
- ipv6 dhcp relay 480
- ipv6 dhcp relay address 482
- ipv6 dhcp relay option type cisco 481
- ipv6 dhcp relay option vpn 481
- ipv6 dhcp relay source-interface 484
- ipv6 port traffic-filter 368
- ip verify source dhcp-snooping-vlan 538
- IP ドメイン名 189
  - PKI の設定 189

## K

- key-chain macsec-psk no-show 638
- key-octet-string 639
- key-server-priority 642
- key-string 557
- キーチェーン 553, 557, 558, 560, 639
- key config-key ascii 546, 555

## L

- ldap-server deadtime 144, 145
- ldap-server host 135, 140, 141, 144
- ldap-server host idle-time 144
- ldap-server host password 137, 144
- ldap-server host port 137, 141
- ldap-server host rootDN 137
- ldap-server host test rootDN 144
- ldap-server host timeout 137, 141
- ldap-server host username 144
- ldap-server timeout 139
- ldap search-map 142
- line vty 340
- logging drop threshold 604
- logging ip access-list cache entries 370

logging ip access-list cache interval [370](#)  
 logging ip access-list cache threshold [370](#)  
 logging ip access-list detailed [370](#)  
 login block-for [47](#)  
 login block-for attempts [47](#)  
 login on-failure log [38](#)  
 login on-success log [38](#)  
 login quiet-mode access-class [47](#)

## M

mac access-list [397, 400, 403](#)  
 mac packet-classify [407](#)  
 mac port access-group [400, 406](#)  
 macsec policy [642](#)  
 MAC アドレス [420](#)  
   ラーニング [420](#)  
 MAC 認証 [269](#)  
   802.1X のバイパス [269](#)  
 match {ip | ipv6} address [415](#)  
 match access-group name [602, 611, 613](#)  
 match exception {ip | ipv6} icmp redirect [602](#)  
 match exception {ip | ipv6} icmp unreachable [602](#)  
 match exception {ip | ipv6} option [602](#)  
 match mac address [415](#)  
 match protocol arp [602](#)

## N

no dot1x system-auth-control [289](#)  
 no feature dot1x [290](#)  
 no {periodic | absolute} [390](#)  
 no aaa authentication login {console | default | fallback error local [26,](#)  
   [35](#)  
 no aaa authentication login ascii-authentication [40, 42](#)  
 no feature ssh [155, 170, 172, 173](#)  
 no feature tacacs+ [122](#)  
 no host [384, 385](#)  
 no ip access-list [341](#)  
 no ipv6 access-list [341](#)  
 no key chain [554](#)  
 no mac access-list [405](#)  
 no object-group {ip address | ipv6 address | ip port} [387](#)  
 no ssh key dsa [173](#)  
 no ssh key rsa [173](#)  
 no time-range [391](#)  
 no vlan access-map [416](#)

## O

object-group ip address [383](#)  
 object-group ip port [386](#)  
 object-group ipv6 address [384](#)

## P

password prompt username [50](#)  
 password strength-check [248](#)  
 permit [335, 337, 338, 339](#)  
 permit mac [400](#)  
 permit | deny [397](#)  
 permit http-method [371](#)  
 permit interface [256](#)  
 permit ip [365](#)  
 permit udf [365](#)  
 permit vlan [257](#)  
 permit vrf [259](#)  
 PKI [183, 186, 187, 188, 189, 190, 205, 206](#)  
   IP ドメイン名の設定 [189](#)  
   RSA キーペアの作成 [190](#)  
   証明書失効確認 [187](#)  
   制限事項 [188](#)  
   設定の表示 [205](#)  
   設定例 [206](#)  
   説明 [183](#)  
   ガイドラインに準拠 [188](#)  
   デフォルト設定 [189](#)  
   登録のサポート [186](#)  
   ホスト名の設定 [189](#)  
 police cir [604, 611, 613](#)  
 policy-map [596](#)  
 policy-map type control-plane [603](#)

## R

radius-server deadtime [78, 80, 81](#)  
 radius-server directed-request [72](#)  
 radius-server host [51, 65, 67, 69, 74, 76, 79](#)  
 radius-server host accounting [76](#)  
 radius-server host acct-port [76](#)  
 radius-server host auth-port [76](#)  
 radius-server host authentication [76](#)  
 radius-server host idle-time [79](#)  
 radius-server host password [79](#)  
 radius-server host retransmit [74](#)  
 radius-server host test [79](#)  
 radius-server host timeout [74](#)  
 radius-server host username [79](#)  
 radius-server key [51, 66](#)  
 radius-server retransmit [73](#)  
 radius-server test {idle-time} [78](#)  
 radius-server test {password} [78](#)  
 radius-server test {username} [78](#)  
 radius-server timeout [73](#)  
 radius commit [65, 72, 73, 76, 81](#)  
 RADIUS アカウンティング [293](#)  
   802.1X 認証のイネーブル化 [293](#)  
 resequence {ip | ipv6} access-list [340](#)

resequence mac access-list [404](#)  
 resequence time-range [392](#)  
 role commit [254, 255, 256, 258, 259](#)  
 role feature-group name [254](#)  
 role name [252, 256, 257, 258](#)  
 role name priv [120](#)  
 RSA キー ペア [184, 187, 188, 190, 200, 201, 205](#)  
   Cisco NX-OS デバイスからの削除 [205](#)  
   PKI の作成 [190](#)  
   インポート [188, 201](#)  
   エクスポート [188, 200](#)  
   設定の表示 [205](#)  
   説明 [184](#)  
   複数 [187](#)  
 rule {deny|permit} command [252](#)  
 rule {deny | permit} {read | read-write} [252](#)  
 rule {deny | permit} {read | read-write} feature [252](#)  
 rule {deny | permit} {read | read-write} feature-group [252](#)  
 rule {deny | permit} {read | read-write} oid [253](#)  
 rule {deny | permit} command [120](#)

## S

sak-expiry-time [643](#)  
 scale-factor [607](#)  
 security-policy [642](#)  
 send-lifetime [559, 640](#)  
 service-policy [596](#)  
 service-policy input [606](#)  
 set cos [605](#)  
 show crypto ca certificates [166, 176](#)  
 show crypto ca crt [166, 176](#)  
 show dot1x {all | interface ethernet} [301](#)  
 show dot1x all [278, 281, 284, 289, 292, 293](#)  
 show dot1x interface ethernet [278](#)  
 show dot1x [276, 290](#)  
 show hardware rate-limiter span-egress [628](#)  
 show ip interface [569](#)  
 show macsec mka session [646](#)  
 show macsec mka statistics [648](#)  
 show macsec mka summary [646](#)  
 show macsec policy [643, 646](#)  
 show macsec secy statistics [648](#)  
 show port-security address interface [435](#)  
 show port-security address [436, 441](#)  
 show port-security interface [441](#)  
 show port-security [430, 441](#)  
 show running-config interface ethernet [407, 487, 573, 577](#)  
 show running-config interface port-channel [407, 577](#)  
 show running-config interface vlan [487](#)  
 show running-config ip [573](#)  
 show running-config ipv6 [573](#)  
 show running-config macsec [646](#)  
 show running-config port-security [431, 432, 433, 434, 438, 439, 441](#)  
 show ssh key md5 [176](#)

show startup-config interface ethernet [573](#)  
 show startup-config ip [573](#)  
 show system login [47](#)  
 show system login failures [47](#)  
 show username [161](#)  
 show vlan filter [417](#)  
 show {ip | ipv6 | access-lists} [388](#)  
 show aaa accounting [44, 294](#)  
 show aaa authentication [32, 34, 35, 37, 52](#)  
 show aaa authentication login {ascii-authentication | chap | error-enable  
   | mschap | mschapv2} [52](#)  
 show aaa authentication login {mschap | mschapv2} [43](#)  
 show aaa authentication login chap [41](#)  
 show aaa authorization [113, 115, 146](#)  
 show aaa authorization all [113](#)  
 show aa accounting [52](#)  
 show aaa groups [52](#)  
 show aaa user default-role [36](#)  
 show accounting log [51](#)  
 show class-map type control-plane [603, 615](#)  
 show cli syntax roles network-admin [261](#)  
 show cli syntax roles network-operator [261](#)  
 show copp profile [616](#)  
 show copp status [608, 609, 617](#)  
 show encryption service stat [546, 555](#)  
 show hardware access-list team region [351, 374](#)  
 show hardware access-list team template [355, 375](#)  
 show hardware rate-limiter [627, 628](#)  
 show hardware rate-limiter access-list-log [627, 628](#)  
 show hardware rate-limiter bfd [627, 628](#)  
 show hardware rate-limiter exception [627, 628](#)  
 show hardware rate-limiter fex [627, 628](#)  
 show hardware rate-limiter layer-3 glean [627, 628](#)  
 show hardware rate-limiter layer-3 multicast local-groups [627, 628](#)  
 show hardware rate-limiter module [627, 628](#)  
 show incompatibility nxos bootflash: [598](#)  
 show interface switchport [577](#)  
 show ip access-lists [336, 338, 340, 341, 372, 375, 377](#)  
 show ip access-lists summary [342](#)  
 show ip arp inspection [527](#)  
 show ip arp inspection interface [524](#)  
 show ip arp inspection interfaces [527](#)  
 show ip arp inspection log [527](#)  
 show ip arp inspection statistics [528](#)  
 show ip arp inspection vlan [523, 527](#)  
 show ip dhcp relay [466, 469, 471, 476, 477, 478, 492](#)  
 show ip dhcp relay address [492](#)  
 show ip dhcp relay information trusted-sources [466, 467, 468](#)  
 show ip dhcp relay statistics [494](#)  
 show ip dhcp snooping binding [493, 539](#)  
 show ipv6 access-lists [336, 338, 340, 375, 377](#)  
 show ipv6 access-lists summary [342](#)  
 show ipv6 dhcp relay [480, 481, 485, 492](#)  
 show ipv6 dhcp relay interface [481](#)  
 show ipv6 dhcp relay statistics [494](#)  
 show ip ver source [540](#)

- show ip ver source ethernet **540**  
 show ip ver source port-channel **540**  
 show key chain **553, 554, 557, 559, 560, 561, 640**  
 show key chain mode decrypt **557, 559**  
 show ldap-search-map **143, 148**  
 show ldap-server **136, 137, 139, 140, 142, 144, 145, 148**  
 show ldap-server groups **139, 148**  
 show ldap-server statistics **147, 148**  
 show logging ip access-list cache **370, 376**  
 show logging ip access-list status **376**  
 show login **47, 52**  
 show login failures **47**  
 show login on-failure log **39**  
 show login on-successful log **39**  
 show mac access-lists **398, 403, 404, 405, 408**  
 show object-group **384, 385, 386, 387**  
 show password strength-check **248**  
 show policy-map interface control-plane **608, 615, 617, 618**  
 show policy-map type control-plane **605, 614**  
 show policy-map type control-plane expand **605**  
 show policy-map type control-plane name **605**  
 show privilege **119, 124**  
 show radius-server **65, 67, 68, 71, 74, 75, 77, 78, 80, 81, 84, 277**  
 show radius-server directed-request **72**  
 show radius-server groups **70, 277**  
 show radius-server statistics **85, 86**  
 show radius {pending | pending-diff} **65, 72, 73, 75, 76, 81**  
 show radius {status | pending | pending-diff} **84**  
 show role **249, 253, 256, 257, 259, 262**  
 show role {pending | pending-diff} **253, 255, 256, 257, 259**  
 show role feature **262**  
 show role feature-group **255, 262**  
 show run interface **373**  
 show running-config aaa **52**  
 show running-config acllog **376**  
 show running-config aclmgr **367, 368, 376, 388, 406, 408, 415, 416, 417, 616**  
 show running-config aclmgr all **376, 408**  
 show running-config all | i max-login **48, 52**  
 show running-config copp **607, 608, 609, 616**  
 show running-config copp all **607**  
 show running-config dhcp **458, 460, 461, 463, 464, 465, 466, 468, 469, 471, 472, 475, 476, 477, 478, 480, 481, 483, 525, 526, 527, 538**  
 show running-config interface **492, 577**  
 show running-config interface mgmt 0 **487**  
 show running-config ldap **148**  
 show running-config radius **84**  
 show running-config security **164, 176, 262**  
 show running-config security all **159, 176, 262**  
 show running-config tacacs **124**  
 show running-config tacacs all **124**  
 show ssh key **156, 173, 176**  
 show ssh key dsa **176**  
 show ssh key rsa **176**  
 show ssh server **172, 176**  
 show startup-config aaa **53**  
 show startup-config acllog **376**  
 show startup-config aclmgr **377, 408, 417, 617**  
 show startup-config aclmgr all **377, 408, 417**  
 show startup-config dhcp **492**  
 show startup-config dhcp all **492**  
 show startup-config ldap **148**  
 show startup-config radius **84**  
 show startup-config security **262**  
 show startup-config tacacs **124**  
 show tacacs-server **97, 99, 100, 102, 105, 106, 108, 110, 111, 112, 124**  
 show tacacs-server directed-request **104, 124**  
 show tacacs-server groups **101, 124**  
 show tacacs-server sorted **124**  
 show tacacs-server statistics **123, 124**  
 show tacacs+ {pending | pending-diff} **97, 103, 105, 106, 111, 112, 115**  
 show tacacs+ {status | pending | pending-diff} **124**  
 show telnet server **174, 176**  
 show time-range **390, 391, 392**  
 show user-account **157, 158, 166, 176, 251, 261, 262**  
 show username keypair **176**  
 show userpassphrase {length | max-length | min-length} **49, 53**  
 show users **166, 174, 176**  
 show vlan access-map **417**  
 ssh **160**  
 ssh6 **160**  
 ssh6 vrf **160**  
 ssh key **155**  
 ssh key force **155**  
 ssh key rsa **155**  
 ssh login-attempts **159**  
 ssh vrf **160**  
 statistics per-entry **336, 338, 398, 403, 415**  
 switchport **431, 432**  
 switchport port-security **431**  
 switchport port-security aging time **439**  
 switchport port-security aging type **439**  
 switchport port-security mac-address sticky **432, 435, 436**  
 switchport port-security mac-address **433, 434**  
 switchport port-security maximum **438**  
 switchport port-security violation **440**  
 switchport block {multicast | unicast} **576**  
 switchport block ethernet switchport **577**  
 switchport block port-channel switchport **577**  
 system login block-for **47**  
 system login block-for attempts **47**  
 system login block-for within **47**  
 system login quiet-mode access-class **47**
- ## T
- tacacs-server deadtime **110**  
 tacacs-server dead-time **108, 109**  
 tacacs-server directed-request **103**  
 tacacs-server host **51, 97, 99, 101, 104, 106, 109**  
 tacacs-server host port **106**



tacacs-server host timeout **104**  
 tacacs-server key **51, 98**  
 tacacs-server test **107**  
 tacacs-server test idle-time **107**  
 tacacs-server test username **107**  
 tacacs+ commit **97, 103, 105, 106, 111, 112, 115**  
 Telnet **175**  
 telnet6 **175**  
 telnet6 vrf **175**  
 telnet vrf **175**  
 terminal no verify-only **117**  
 terminal no verify-only username **117**  
 terminal verify-only **117**  
 terminal verify-only username **117**  
 test aaa authorization command-type {commands | config-commands}  
     user command **116**  
 test aaa group **82, 121**  
 test aaa server radius **82**  
 test aaa server radius vrf **82**  
 test aaa server tacacs+ **121**  
 time-range **390**

## U

udf **363, 398**  
 use-vrf **70, 138**  
 user max-logins **48**  
 username keypair export **161**  
 username keypair export {rsa | dsa} **161**  
 username keypair generate **161**  
 username keypair import **162**  
 username keypair import (rsa | dsa) **162**  
 username password **164, 250**  
 username sshkey **158**  
 username sshkey file bootflash **157**  
 userpassphrase min-length **49**  
 userpassphrase max-length **49**

## V

vlan access-map **414**  
 vlan filter **417**  
 vlan policy deny **257**  
 vPC ファーストホップ セキュリティ設定 **499**  
     説明 **499**  
 VPC レッグでの DHCP リレー **500**  
     説明 **500**  
 vrf policy deny **258**

## W

window-size **643**

## い

enable secret **118**

## お

オーセンティケーター PAE **267, 279**  
     インターフェイスからの削除 **279**  
     インターフェイスの作成 **279**  
     説明 **267**

## き

キー **548, 557, 558, 560, 639**  
 feature **254**  
 deny **335, 337, 338, 339**

## く

class **603**

## こ

孤立ポートの DHCP クライアントリレー **501**  
     説明 **501**

## さ

サーバ **69, 70, 101, 138**  
 サービス拒絶攻撃 **565**  
     IP アドレス スプーフィング、軽減 **565**

## し

証明機関。参照先：CA  
 証明書失効確認 **195**  
     方法の設定 **195**  
 証明書失効リスト。参照先：CRL

## せ

制限事項 **427**  
     ポートセキュリティ **427**  
 セキュア MAC アドレス **420**  
     ラーニング **420**  
 セキュリティ **420**  
     ポート **420**  
         MAC アドレス ラーニング **420**  
 説明 **253**

## た

ダイナミック モード [611, 614](#)

## ち

ガイドラインに準拠 [427](#)  
ポート セキュリティ [427](#)

## て

定期 [390](#)  
デジタル証明書 [183, 187, 188, 189](#)  
インポート [188](#)  
エクスポート [188](#)  
設定 [189](#)  
説明 [183, 188](#)  
peers [187](#)  
目的 [183](#)  
deadtime [69](#)  
デフォルト設定 [189, 274, 427](#)  
802.1X [274](#)  
PKI [189](#)  
ポート セキュリティ [427](#)

## と

トラスト ポイント [184, 186, 199](#)  
説明 [184](#)  
複数 [186](#)  
リブート後の設定の保存 [199](#)

## ほ

ポート [268](#)  
802.1X の許可ステート [268](#)

ポート セキュリティ [419, 420, 422, 427](#)  
MAC アドレス ラーニング [420](#)  
MAC 移動 [422](#)  
違反 [422](#)  
制限事項 [427](#)  
説明 [419](#)  
ガイドラインに準拠 [427](#)  
デフォルト設定 [427](#)  
ホスト [383, 384](#)  
hostnames [189](#)  
PKI の設定 [189](#)  
police [604, 611, 613](#)

## ゆ

username [119, 157](#)  
ユニキャスト RPF [563, 564, 565, 568, 572, 573](#)  
BGP 属性 [564](#)  
BOOTP [565](#)  
DHCP [565](#)  
FIB [563](#)  
実装 [564](#)  
制限事項 [565](#)  
設定の確認 [573](#)  
設定例 [572](#)  
説明 [563](#)  
ガイドラインに準拠 [565](#)  
デフォルト設定 [568](#)  
導入 [565](#)  
トンネリング [565](#)

## り

reload [352, 355, 365, 399, 610, 612](#)