



## Cisco IOS XE Fuji 16.9.x (Catalyst 9300 スイッチ) セキュリティ コンフィギュレーションガイド

初版：2018年7月18日

最終更新：2020年1月30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/>





## 目次

---

第 1 章	<b>不正アクセスの防止</b> 1
	機能情報の確認 1
	不正アクセスの防止 1
	不正アクセスの防止のための機能情報 2

---

第 2 章	<b>パスワードおよび権限レベルによるスイッチ アクセスの制御</b> 3
	パスワードおよび権限によるスイッチ アクセスの制御の制約事項 3
	パスワードおよび権限レベルに関する情報 4
	デフォルトのパスワードおよび権限レベル設定 4
	追加のパスワードセキュリティ 4
	パスワードの回復 5
	端末回線の Telnet 設定 5
	ユーザ名とパスワードのペア 5
	権限レベル 5
	パスワードおよび権限レベルでスイッチ アクセスを制御する方法 6
	スタティック 有効 パスワードの設定または変更 6
	暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護 8
	パスワード回復のディセーブル化 10
	端末回線に対する Telnet パスワードの設定 11
	ユーザ名とパスワードのペアの設定 13
	コマンドの特権レベルの設定 15
	回線のデフォルト特権レベルの変更 16
	権限レベルへのログインおよび終了 18
	スイッチ アクセスのモニタリング 18

パスワードおよび権限レベルの設定例	19
例：スタティック イネーブルパスワードの設定または変更	19
例：暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護	19
例：端末回線に対する Telnet パスワードの設定	19
例：コマンドの権限レベルの設定	19
その他の参考資料	20
パスワードおよび権限によるスイッチアクセスの制御の機能履歴	20

## 第 3 章

## 認証の設定 23

認証の設定の前提条件	23
認証の設定に関する制約事項	23
認証の設定に関する情報	24
認証の名前付き方式リスト	24
方式リストとサーバグループ	24
方式リストの例	25
RADIUS 認可変更について	27
CoA 要求	28
CoA 要求応答コード	29
CoA 要求コマンド	30
ドメインストリッピング	32
AAA 認証方式を設定する方法	33
AAA を使用したログイン認証の設定	33
イネーブルパスワードによるログイン認証	35
Kerberos によるログイン認証	35
ラインパスワードによるログイン認証	36
ローカルパスワードによるログイン認証	36
group RADIUS によるログイン認証	36
アクセス要求での RADIUS 属性 8 の設定	36
group TACACS によるログイン認証	37
group group-name によるログイン認証	37
AAA を使用した PPP 認証の設定	37

Kerberos による PPP 認証	39
ローカルパスワードによる PPP 認証	40
group RADIUS による PPP 認証	40
アクセス要求での RADIUS 属性 44 の設定	40
group TACACS による PPP 認証	40
group group-name による PPP 認証	41
PPP 要求に対する AAA スケーラビリティの設定	41
AAA を使用した ARAP 認証の設定	42
認可済みゲスト ログインを許可する ARAP 認証	44
ゲスト ログインを許可する ARAP 認証	44
ラインパスワードによる ARAP 認証	45
ローカルパスワードによる ARAP 認証	45
group RADIUS による ARAP 認証	45
group TACACS による ARAP 認証	45
group group-name による ARAP 認証	46
AAA を使用した NASI 認証の設定	46
イネーブルパスワードによる NASI 認証	48
ラインパスワードによる NASI 認証	48
ローカルパスワードによる NASI 認証	48
group RADIUS による NASI 認証	49
group TACACS による NASI 認証	49
group group-name による NASI 認証	49
ログイン入力にかける時間の指定	50
特権レベルでのパスワード保護のイネーブル化	50
パスワードプロンプトに表示するテキストの変更	51
ユーザー名が空のアクセス要求が RADIUS サーバーに送信されないようにする	52
AAA 認証のメッセージバナーの設定	53
ログインバナーの設定	53
Failed-Login バナーの設定	53
AAA パケット オブ ディスコネクトの設定	54
二重認証のイネーブル化	55

二重認証の機能	55
二重認証の設定	57
二重認証後のユーザー プロファイルへのアクセス	58
自動二重認証のイネーブル化	58
自動二重認証の設定	60
自動二重認証のトラブルシューティング	61
RADIUS CoA 用の動的認可サービスの設定	61
bounce および disable RADIUS CoA 要求を無視するためのデバイスの設定	63
サーバー グループ レベルでのドメイン ストリッピングの設定	64
非 AAA 認証方式	65
ラインパスワード保護の設定	65
ユーザー名認証の確立	66
CHAP 認証または PAP 認証の有効化	68
MS-CHAP の使用	73
MS-CHAP を使用した PPP 認証の定義	74
認証の例	75
例：RADIUS 認証	75
例：TACACS 認証	76
例：Kerberos 認証	78
例：AAA スケーラビリティ	78
例：AAA 認証のログイン バナーおよび Failed-Login バナーの設定	79
例：AAA パケット オブ ディスコネクト サーバー キー	80
例：二重認証	80
例：自動二重認証	86
認証設定の機能履歴	87

---

**第 4 章****認可の設定 89**

AAA 認可の前提条件	89
認可の設定の概要	90
認可の名前付き方式リスト	90
AAA 認可方式	91

認可方式	91
方式リストとサーバグループ	92
AAA 認可タイプ	93
承認タイプ	93
認可の属性値ペア	94
認可の設定方法	94
名前付き方式リストによる AAA 認可の設定	94
グローバル コンフィギュレーション コマンドの認可のディセーブル化	95
リバース Telnet の認可の設定	96
認可設定の例	97
例：TACACS 認可	97
例：RADIUS 許可	97
例：リバース Telnet 許可	98
認可の設定に関する追加情報	100
許可設定の機能履歴	100

## 第 5 章

アカウントिंगの設定	103
アカウントिंगを設定するための前提条件	103
アカウントिंगの設定の制約事項	104
トピック 2.1	104
アカウントिंगの設定に関する情報	104
アカウントिंगの名前付き方式リスト	104
方式リストとサーバグループ	105
AAA アカウントिंग方式	106
AAA アカウントिंगタイプ	108
ネットワーク アカウントिंग	108
EXEC アカウントिंग	111
コマンドアカウントिंग	112
接続アカウントिंग	113
システムアカウントिंग	115
リソースアカウントिंग	115

AAA アカウンティングの強化	117
AAA ブロードキャスト アカウンティング	117
AAA セッション MIB	118
アカウンティング属性と値のペア	119
AAA アカウンティングの設定方法	119
名前付き方式リストによる AAA アカウンティングの設定	119
ヌルユーザ名セッション時のアカウンティング レコード生成の抑制	121
中間アカウンティング レコードの生成	121
定期的アカウンティング レコードを有効化する代替手段の設定	122
中間サービス アカウンティング レコードの生成	123
失敗したログインまたはセッションに対するアカウンティング レコードの生成	124
EXEC-Stop レコードよりも前のアカウンティング NETWORK-Stop レコードの指定	124
スイッチオーバー上のシステム アカウンティング レコードの抑制	125
AAA リソース失敗終了アカウンティングの設定	125
開始 - 終了レコードの AAA リソース アカウンティングの設定	125
AAA ブロードキャスト アカウンティング	126
DNIS による AAA ブロードキャスト アカウンティングの設定	126
AAA セッション MIB	127
AAA サーバが到達不能な場合のルータとのセッションの確立	128
アカウンティングのモニタリング	129
アカウンティングのトラブルシューティング	129
AAA アカウンティングの設定例	129
例：名前付き方式リストの設定	129
例：AAA リソース アカウンティングの設定	132
例：AAA ブロードキャスト アカウンティングの設定	132
例：DNIS による AAA ブロードキャスト アカウンティングの設定	133
例：AAA セッション MIB	133
アカウンティングの設定に関するその他の参考資料	133
アカウンティングの設定の機能履歴	134



ローカル認証および許可の設定方法	137
スイッチのローカル認証および許可の設定	137
ローカル認証および許可のモニタリング	139
ローカル認証および許可の機能履歴	140

---

**第 7 章**
**TACACS+ の設定 141**

TACACS+ の前提条件	141
TACACS+ によるスイッチ アクセスの制御について	142
TACACS+ およびスイッチ アクセス	142
TACACS+ の概要	142
TACACS+ の動作	144
方式リスト	144
TACACS+ 設定オプション	145
TACACS+ ログイン認証	145
特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可	146
TACACS+ Accounting	146
TACACS+ のデフォルト設定	146
TACACS+ とスイッチ アクセスを設定する方法	146
TACACS+ サーバホストの指定および認証キーの設定	146
TACACS+ ログイン認証の設定	148
特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定	151
TACACS+ アカウンティングの起動	153
AAA サーバが到達不能な場合のルータとのセッションの確立	154
TACACS+ のモニタリング	154
TACACS+ によるスイッチ アクセスの制御に関するその他の参考資料	155
TACACS+ の機能の履歴	155

---

**第 8 章**
**RADIUS の設定 157**

RADIUS を設定するための前提条件	157
RADIUS の設定に関する制約事項	158
RADIUS に関する情報	158

RADIUS およびスイッチ アクセス	158
RADIUS の概要	159
RADIUS の動作	160
RADIUS 許可の変更	161
Change-of-Authorization 要求	162
CoA 要求応答コード	164
CoA 要求コマンド	165
セッション強制終了のスタック構成ガイドライン	168
RADIUS のデフォルト設定	169
RADIUS サーバ ホスト	169
RADIUS ログイン認証	170
AAA サーバグループ	170
AAA 許可	171
RADIUS アカウンティング	171
ベンダー固有の RADIUS 属性	171
ベンダー独自仕様の RADIUS サーバ通信	186
RADIUS の設定方法	187
RADIUS サーバ ホストの識別	187
RADIUS ログイン認証の設定	189
AAA サーバグループの定義	192
ユーザイネーブルアクセスおよびネットワーク サービスに関する RADIUS 許可の設定	194
RADIUS アカウンティングの起動	196
すべての RADIUS サーバの設定	197
ベンダー固有の RADIUS 属性を使用するデバイス設定	199
ベンダー独自の RADIUS サーバとの通信に関するデバイスの設定	200
次の上での CoA の設定 デバイス	202
CoA 機能のモニタリング	205
RADIUS の機能の履歴	205

---

第 9 章	<b>RadSec の設定</b>	207
-------	-------------------	-----

RadSec の設定に関する制限事項	207
RadSec に関する情報	207
RadSec の設定方法	207
RadSec over TLS の設定	208
TLS CoA の動的認可の設定	209
RadSec over DTLS の設定	210
DTLS CoA の動的認可の設定	211
RadSec のモニタリング	213
RadSec の設定例	213
例：RadSec over TLS の設定	213
例：TLS CoA の動的認可の設定	213
例：RadSec over DTLS の設定	214
例：DTLS CoA の動的認可の設定	214
RadSec 設定の機能履歴	214

---

**第 10 章**

<b>Kerberos の設定</b>	<b>215</b>
Kerberos によるスイッチ アクセスの制御の前提条件	215
Kerberos に関する情報	215
Kerberos とスイッチ アクセス	216
Kerberos の概要	216
Kerberos の動作	218
境界スイッチに対する認証の取得	219
KDC からの TGT の取得	219
ネットワーク サービスに対する認証の取得	219
Kerberos を設定する方法	220
Kerberos 設定の監視	220
Kerberos の機能履歴	220

---

**第 11 章**

<b>MACsec の暗号化</b>	<b>221</b>
MACsec 暗号化の前提条件	221
MACsec 暗号化の制約事項	221

MACsec 暗号化の概要	222
MACsec 暗号化の推奨事項	223
Media Access Control Security と MACsec Key Agreement	224
MKA ポリシー	224
ポリシーマップアクションの定義	225
仮想ポート	225
MKA 統計情報	226
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	226
リプレイ保護ウィンドウ サイズ	226
MACsec、MKA、および 802.1x ホストモード	227
証明書ベースの MACsec 暗号化	228
MACsec 暗号化の前提条件	228
スイッチ間 MKA MACsec マストセキュアポリシー	228
MACsec Extended Packet Numbering (XPN)	229
ポートチャネルの MKA/MACsec	230
MACsec 暗号アナウンスメント	230
MACsec 暗号アナウンスメントに関する制約事項	231
MACsec 暗号化の設定方法	231
MKA および MACsec の設定	231
MKA ポリシーの設定	231
スイッチからホストへの MACsec の暗号化設定	233
PSK を使用した MKA MACsec の設定	236
PSK を使用した MACsec MKA の設定	236
PSK を使用した、インターフェイスでの MACsec MKA の設定	237
証明書ベース MACsec 暗号化の設定	239
キー ペアの生成	239
SCEP による登録の設定	240
登録の手動設定	242
スイッチ間の MACsec の暗号化設定	244
MACsec XPN の設定	246
XPN の MKA ポリシーの設定	246

XPN MKA ポリシーをインターフェイスに適用する	247
ポートチャンネル用の MKA/MACsec の設定	248
PSK を使用したポートチャンネルの MKA/MACsec の設定	248
レイヤ 2 EtherChannel のポートチャンネル論理インターフェイスの設定	250
レイヤ 3 EtherChannel のポートチャンネル論理インターフェイスの設定	251
MACsec 暗号アナウンスメントの設定	252
セキュアアナウンスメントの MKA ポリシーの設定	252
セキュアアナウンスメントのグローバル設定	254
インターフェイスでの EAPOL アナウンスメントの設定	255
Cisco TrustSec MACsec の設定	256
手動モードでの Cisco TrustSec スイッチ間リンク セキュリティの設定	256
MACsec 暗号化の設定例	258
例：MKA および MACsec の設定	258
例：PSK を使用した MACsec MKA の設定	258
例：証明書ベース MACsec 暗号化を使用した MACsec MKA の設定	260
例：MACsec XPN の設定	260
例：PSK を使用したポートチャンネルの MACsec MKA の設定	262
例：MACsec 暗号アナウンスメントの設定	269
例：Cisco TrustSec スイッチ間リンクセキュリティ	273
例：MKA 情報の表示	273
MACsec 暗号化の機能情報	280

---

 第 12 章

セキュア シェル (SSH) の設定	281
セキュア シェルを設定するための前提条件	281
セキュア シェルの設定に関する制約事項	282
セキュア シェルの設定について	282
SSH およびスイッチ アクセス	282
SSH サーバ、統合クライアント、およびサポートされているバージョン	283
SSH 設定時の注意事項	283
Secure Copy Protocol の概要	284
Secure Copy Protocol	284

セキュア シェルの設定方法	285
SSH を実行するためのデバイスのセットアップ	285
SSH サーバの設定	286
SSH の設定およびステータスのモニタリング	289
セキュア シェルの機能情報	289

## 第 13 章

**SSH 認証の X.509v3 証明書 291**

SSH 認証の X.509v3 証明書	291
SSH 認証の X.509v3 証明書の前提条件	291
SSH 認証の X.509v3 証明書の制約事項	291
SSH 認証用の X.509v3 証明書に関する情報	292
デジタル証明書	292
X.509v3 を使用したサーバーおよびユーザー認証	292
SSH 認証用の X.509v3 証明書の設定方法	292
サーバー認証にデジタル証明書を使用するための IOS SSH サーバーの設定	293
ユーザ認証用のユーザのデジタル証明書を確認するための IOS SSH サーバの設定	294
デジタル証明書を使用したサーバーおよびユーザー認証の設定の確認	296
SSH 認証用の X.509v3 証明書の設定例	296
例：サーバー認証にデジタル証明書を使用するための IOS SSH サーバーの設定	296
例：ユーザ認証用のユーザのデジタル証明書を確認するための IOS SSH サーバの設定	297
SSH 認証用の X.509v3 証明書の機能履歴	297

## 第 14 章

**コモン クライテリア認定用の SSH アルゴリズム 299**

コモン クライテリア認定用の SSH アルゴリズムに関する情報	299
コモン クライテリア認定用の SSH アルゴリズム	299
Cisco IOS SSH サーバー アルゴリズム	299
Cisco IOS SSH クライアント アルゴリズム	300
コモン クライテリア認定用の SSH アルゴリズムの設定方法	301
Cisco IOS SSH サーバーおよびクライアントの暗号キー アルゴリズムの設定	301
トラブルシューティングのヒント	302
Cisco IOS SSH サーバーおよびクライアントの MAC アルゴリズムの設定	303

トラブルシューティングのヒント	304
Cisco IOS SSH サーバーのホスト キー アルゴリズムの設定	304
トラブルシューティングのヒント	305
コモンクライテリア認定用の SSH アルゴリズムの設定例	305
例：Cisco IOS SSH サーバーの暗号キー アルゴリズムの設定	306
例：Cisco IOS SSH クライアントの暗号キー アルゴリズムの設定	306
例：Cisco IOS SSH サーバーの MAC アルゴリズムの設定	306
例：Cisco IOS SSH サーバーのホスト キー アルゴリズムの設定	306
コモンクライテリア認定用の SSH アルゴリズムの確認	306
コモンクライテリア認定用のセキュアシェルアルゴリズムの機能情報	307

---

**第 15 章**
**Secure Socket Layer HTTP の設定 309**

Secure Socket Layer HTTP について	309
セキュア HTTP サーバおよびクライアントの概要	309
CA のトラストポイント	310
CipherSuite	311
SSL のデフォルト設定	312
SSL の設定時の注意事項	313
Secure Socket Layer HTTP の設定方法	313
CA のトラストポイントの設定	313
セキュア HTTP サーバの設定	315
セキュア HTTP クライアントの設定	319
セキュア HTTP サーバおよびクライアントのステータスのモニタリング	321
Secure Socket Layer HTTP に関するその他の参考資料	321
Secure Socket Layer HTTP の機能履歴	322

---

**第 16 章**
**IPv4 ACL 323**

ACL によるネットワーク セキュリティに関する情報	323
IPv4 アクセスコントロールリストの制約事項	324
ACL を使用したネットワーク セキュリティについて理解する	325
ACL の概要	325

アクセス コントロール エントリ	326
ACL でサポートされるタイプ	326
サポートされる ACL	326
ACL 優先順位	327
ポート ACL	327
ルータ ACL	329
VLAN マップ	329
ACE およびフラグメント化されたトラフィックとフラグメント化されていないトラフィック	330
ACE およびフラグメント化されたトラフィックとフラグメント化されていないトラフィックの例	330
ACL とスイッチ スタック	331
アクティブ スイッチおよび ACL の機能	332
スタック メンバおよび ACL の機能	332
アクティブ スイッチの障害および ACL	332
標準 IPv4 ACL および拡張 IPv4 ACL	332
IPv4 ACL スイッチでサポートされていない機能	333
アクセス リスト番号	333
番号付き標準 IPv4 ACL	334
番号付き拡張 IPv4 ACL	334
名前付き IPv4 ACL	335
ACL ロギング	336
ハードウェアおよびソフトウェアによる IP ACL の処理	336
VLAN マップの設定時の注意事項	337
VLAN マップとルータ ACL	338
VLAN マップとルータ ACL の設定時の注意事項	338
ACL の時間範囲	339
IPv4 ACL のインターフェイスに関する注意事項	340
ACL によるネットワーク セキュリティに関する情報	340
ACL の設定方法	340
IPv4 ACL の設定	340



番号付き標準 ACL の作成	341
番号付き拡張 ACL の作成	342
名前付き標準 ACL の作成	347
名前付き拡張 ACL の作成	348
ACL の時間範囲の設定	350
端末回線への IPv4 ACL の適用	352
インターフェイスへの IPv4 ACL の適用	353
名前付き MAC 拡張 ACL の作成	355
レイヤ 2 インターフェイスへの MAC ACL の適用	357
VLAN マップの設定	358
VLAN マップの作成	360
VLAN への VLAN マップの適用	362
IPv4 ACL のモニタリング	363
ACL の設定例	364
例：ACL での時間範囲を使用	364
例：ACL へのコメントの挿入	365
IPv4 ACL の設定例	365
小規模ネットワークが構築されたオフィス用の ACL	365
例：小規模ネットワークが構築されたオフィスの ACL	366
例：番号付き ACL	367
例：拡張 ACL	367
例：名前付き ACL	368
例：IP ACL に適用される時間範囲	369
例：コメント付き IP ACL エントリの設定	369
例：ACL ロギング	370
ACL および VLAN マップの設定例	372
例：パケットを拒否する ACL および VLAN マップの作成	372
例：パケットを許可する ACL および VLAN マップの作成	372
例：IP パケットのドロップおよび MAC パケットの転送のデフォルトアクション	372
例：MAC パケットのドロップおよび IP パケットの転送のデフォルトアクション	373
例：すべてのパケットをドロップするデフォルトアクション	373

ネットワークでの VLAN マップの使用方法の設定例	374
例：ワイヤリング クローゼットの設定	374
例：別の VLAN にあるサーバーへのアクセスの制限	375
例：別の VLAN にあるサーバーへのアクセスの拒否	376
ACL の設定例	377
IPv4 アクセスコントロールリストの機能履歴	377

---

**第 17 章****IPv6 ACL 379**

IPv6 ACL の概要	379
スイッチ スタックおよび IPv6 ACL	380
ACL 優先順位	380
VLAN マップ	381
他の機能およびスイッチとの相互作用	381
IPv6 ACL の制限	382
IPv6 ACL のデフォルト設定	383
IPv6 ACL の設定	383
インターフェイスへの IPv6 ACL の付加	388
VLAN マップの設定	389
VLAN への VLAN マップの適用	391
IPv6 ACL のモニタリング	392
IPv6 ACL の機能履歴	393

---

**第 18 章****DHCP の設定 395**

DHCP の設定に関する制限	395
DHCP に関する情報	395
DHCP サーバ	395
DHCP リレー エージェント	395
DHCP スヌーピング	396
オプション 82 データ挿入	397
Cisco IOS DHCP サーバ データベース	401
DHCP スヌーピング バインディング データベース	401

DHCP スヌーピングおよびスイッチ スタック	403
DHCP 機能の設定方法	403
DHCP スヌーピングのデフォルト設定	403
DHCP スヌーピング設定時の注意事項	404
DHCP サーバの設定	405
DHCP サーバーとスイッチ スタック	405
DHCP リレー エージェントの設定	405
パケット転送アドレスの指定	406
DHCP スヌーピングおよびオプション 82 を設定するための前提条件	409
Cisco IOS DHCP サーバデータベースのイネーブル化	410
DHCP スヌーピング情報のモニタリング	410
DHCP サーバー ポートベースのアドレス割り当ての設定	411
DHCP サーバー ポートベースのアドレス割り当ての	411
ポートベースのアドレス テーブルのデフォルト設定	411
ポートベースのアドレス割り当て設定時の注意事項	412
DHCP スヌーピング バインディング データベース エージェントのイネーブル化	412
DHCP サーバ ポートベースのアドレス割り当てのイネーブル化	414
DHCP サーバ ポートベースのアドレス割り当てのモニタリング	416
DHCP の機能情報	416
<hr/>	
第 19 章	<b>DHCPv6 オプションのサポート</b> 419
DHCPv6 オプションのサポートに関する情報	419
CAPWAP アクセスコントローラ DHCPv6 オプション	419
DNS 検索リストのオプション	420
DHCPv6 クライアントのリンク層アドレスオプション	421
DHCPv6 リレー エージェント	421
DHCPv6 オプションサポートの設定方法	421
CAPWAP アクセスポイントの設定	421
IPv6 ルータ アドバタイズメント オプションを使用した DNS 検索リストの設定	422
DHCPv6 オプションサポートの設定例	424
例 : CAPWAP アクセスポイントの設定	424

DHCPv6 オプションサポートの確認	424
DHCPv6 オプションサポートの機能情報	426

---

**第 20 章**

<b>IP ソース ガードの設定</b>	<b>427</b>
IP ソース ガードの概要	427
IP ソース ガード	427
スタティック ホスト用 IP ソース ガード	428
IP ソース ガードの設定時の注意事項	429
IP ソース ガードの設定方法	430
IP ソース ガードのイネーブル化	430
レイヤ 2 アクセス ポートでのスタティック ホスト用 IP ソース ガードの設定	431
IP ソース ガードのモニタリング	433
IP ソース ガードの機能の履歴	434

---

**第 21 章**

<b>ダイナミック ARP インспекションの設定</b>	<b>435</b>
ダイナミック ARP インспекションの制約事項	435
ダイナミック ARP インспекションの概要	437
インターフェイスの信頼状態とネットワーク セキュリティ	439
ARP パケットのレート制限	440
ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ	440
廃棄パケットのロギング	441
ダイナミック ARP インспекションのデフォルト設定	441
ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ	442
非 DHCP 環境での ARP ACL の設定	442
DHCP 環境でのダイナミック ARP インспекションの設定	445
着信 ARP パケットのレート制限	448
ダイナミック ARP インспекション検証チェックの実行	451
DAI のモニタリング	453
DAI の設定の確認	453
ダイナミック ARP インспекションの機能方法	454

## 第 22 章

<b>IPv6 ファースト ホップ セキュリティの設定</b>	<b>455</b>
IPv6 でのファースト ホップ セキュリティの前提条件	455
IPv6 でのファースト ホップ セキュリティの制約事項	455
IPv6 でのファースト ホップ セキュリティに関する情報	456
IPv6 スヌーピング ポリシーの設定方法	458
IPv6 スヌーピング ポリシーをインターフェイスにアタッチする方法	460
IPv6 スヌーピング ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法	462
IPv6 スヌーピング ポリシーを VLAN にグローバルにアタッチする方法	463
IPv6 バインディング テーブルの内容を設定する方法	464
IPv6 ネイバー探索検査ポリシーの設定方法	465
IPv6 ネイバー探索検査ポリシーをインターフェイスにアタッチする方法	467
IPv6 ネイバー探索検査ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法	468
IPv6 ネイバー探索検査ポリシーを全体的に VLAN にアタッチする方法	469
IPv6 ルータ アドバタイズメント ガード ポリシーの設定方法	470
IPv6 ルータ アドバタイズメント ガード ポリシーをインターフェイスにアタッチする方法	473
IPv6 ルータ アドバタイズメント ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法	474
IPv6 ルータ アドバタイズメント ガード ポリシーを VLAN にグローバルにアタッチする方法	476
IPv6 DHCP ガード ポリシーの設定方法	476
IPv6 DHCP ガード ポリシーをインターフェイスまたはインターフェイス上の VLAN にアタッチする方法	479
IPv6 DHCP ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法	480
IPv6 DHCP ガード ポリシーを全体的に VLAN にアタッチする方法	481
IPv6 ソース ガードの設定方法	482
IPv6 ソース ガード ポリシーをインターフェイスにアタッチする方法	483
IPv6 ソース ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法	484

IPv6 プレフィックス ガードの設定方法	485
IPv6 プレフィックス ガード ポリシーをインターフェイスにアタッチする方法	486
IPv6 プレフィックス ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法	487
IPv6 ファースト ホップ セキュリティの設定例	488
例：IPv6 ソース ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法	488
例：IPv6 プレフィックス ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法	489
IPv6 ファースト ホップ セキュリティの機能履歴	489
<hr/>	
第 23 章	<b>SISF ベースのデバイストラッキングの設定</b>
SISF ベースのデバイストラッキングに関する情報	491
SISF ベースのデバイストラッキングの概要	491
SISF ベースのデバイストラッキングを有効にするオプション	492
レガシー IPDT と IPv6 スヌーピングから SISF ベースのデバイストラッキングへの移行	493
SISF ベースのデバイストラッキングの設定方法	495
SISF ベースのデバイストラッキングの手動による有効化	495
ターゲットへのデフォルト デバイス トラッキング ポリシーの適用	495
カスタム設定を使用したカスタム デバイス トラッキング ポリシーの作成	496
デバイス トラッキング ポリシーのインターフェイスへの適用	500
デバイス トラッキング ポリシーの VLAN への適用	501
Cisco IOS XE Fuji 16.9.x 以降のリリースでの SISF ベースのデバイストラッキングのプログラムによる有効化	502
トランクポートからのバインディングエントリの作成を停止するためのマルチスイッチネットワークの設定	503
SISF ベースのデバイストラッキングの設定例	505
例：Cisco IOS XE Everest 16.9.x 以降のリリースでの SISF ベースのデバイストラッキングのプログラムによる有効化	505
例：ターゲットでの IPv6 デバイストラッキングの無効化	507
例：VLAN 上の SVI に対する IPv6 の有効化（重複アドレスの問題を軽減するため）	508
例：IPv4 重複アドレスの問題の緩和	508

例：短いデバイストラッキング バインディング到達可能時間の回避	510
SISF の機能履歴	510

## 第 24 章

<b>IEEE 802.1x ポートベースの認証の設定</b>	<b>513</b>
IEEE 802.1x ポートベース認証の制約事項	513
802.1x ポートベース認証について	514
ポートベース認証プロセス	514
ポートベース認証の開始およびメッセージ交換	517
ポートベース認証の認証マネージャ	519
ポートベース認証方法	519
ユーザー単位 ACL および Filter-Id	520
ポートベース認証マネージャ CLI コマンド	520
許可ステートおよび無許可ステートのポート	522
ポートベース認証とスイッチ スタック	523
802.1X のホスト モード	524
802.1x マルチ認証モード	524
ユーザーごとのマルチ認証 VLAN 割り当て	525
MAC 移動	527
MAC 置換	527
802.1x アカウンティング	528
802.1x アカウンティング属性値ペア	528
802.1x 準備状態チェック	529
スイッチと RADIUS サーバー間の通信	530
VLAN 割り当てを使用した 802.1x 認証	530
ユーザー単位 ACL を使用した 802.1x 認証	532
ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証	533
VLAN ID ベース MAC 認証	533
ゲスト VLAN を使用した 802.1x 認証	534
制限付き VLAN を使用した 802.1x 認証	535
アクセス不能認証バイパスを使用した 802.1x 認証	536
複数認証ポートのアクセス不能認証バイパスのサポート	536

アクセス不能認証バイパスの認証結果	537
アクセス不能認証バイパス機能の相互作用	537
802.1x クリティカル音声 VLAN	538
802.1x ユーザ ディストリビューション	539
802.1x ユーザ ディストリビューションの設定時の注意事項	539
音声 VLAN ポートを使用した IEEE 802.1x 認証	539
VoL 機能を使用した IEEE 802.1x 認証	540
MAC 認証バイパスを使用した IEEE 802.1x 認証	541
Network Admission Control レイヤ 2 IEEE 802.1x 検証	542
柔軟な認証の順序設定	543
Open1x 認証	543
マルチドメイン認証	544
Network Edge Access Topology (NEAT) を使用した 802.1x サプリカントおよびオーセン ティケーター	546
音声認識 802.1x セキュリティ	548
コモンセッション ID	548
802.1x ポートベース認証の設定方法	549
802.1x 認証のデフォルト設定	549
802.1x 認証設定時の注意事項	550
802.1X 認証	550
VLAN 割り当て、ゲスト VLAN、制限付き VLAN、アクセス不能認証バイパス	551
MAC 認証バイパス	552
ポートあたりのデバイスの最大数	553
802.1x 準備状態チェックの設定	553
音声認識 802.1x セキュリティの設定	555
802.1x 違反モードの設定	557
802.1X 認証の設定	559
802.1x ポートベース認証の設定	560
スイッチ/RADIUS サーバー間通信の設定	563
ホスト モードの設定	564
定期的な再認証の設定	566



待機時間の変更	567
スイッチからクライアントへの再送信時間の変更	569
スイッチからクライアントへのフレーム再送信回数の設定	570
再認証回数の設定	571
MAC 移動のイネーブル化	572
MAC 置換のイネーブル化	573
802.1x アカウンティングの設定	575
ゲスト VLAN の設定	577
制限付き VLAN の設定	578
制限付き VLAN の認証試行回数の設定	580
クリティカル音声 VLAN を使用した 802.1x アクセス不能認証バイパスの設定	581
アクセス不能認証バイパスの設定例	585
WoL を使用した 802.1x 認証の設定	585
MAC 認証バイパスの設定	586
802.1x ユーザー ディストリビューションの設定	587
VLAN グループの設定例	588
NAC レイヤ 2 802.1x 検証の設定	589
NEAT を使用したオーセンティケータ スイッチの設定	591
NEAT を使用したサブリカント スイッチの設定	593
ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証の設定	596
ダウンロード可能な ACL の設定	596
ダウンロード ポリシーの設定	598
VLAN ID ベース MAC 認証の設定	600
柔軟な認証順序の設定	601
Open1x の設定	602
ポート上での 802.1x 認証のディセーブル化	604
802.1x 認証設定のデフォルト値へのリセット	605
802.1x の統計情報およびステータスのモニターリング	606
IEEE 802.1x ポートベースの認証の機能履歴	607

Web ベース認証の概要	609
デバイスのロール	610
ホストの検出	611
セッションの作成	611
認証プロセス	612
ローカル Web 認証バナー	613
Web 認証カスタマイズ可能な Web ページ	616
ガイドライン	616
認証プロキシ Web ページの注意事項	617
成功ログインに対するリダイレクト URL の注意事項	618
その他の機能と Web ベース認証の相互作用	619
ポートセキュリティ	619
LAN ポート IP	619
ゲートウェイ IP	619
ACL	619
コンテキストベース アクセス コントロール	619
EtherChannel	620
Web ベース認証の設定方法	620
デフォルトの Web ベース認証の設定	620
Web ベース認証の設定に関する注意事項と制約事項	620
認証ルールとインターフェイスの設定	622
AAA 認証の設定	624
スイッチ/RADIUS サーバー間通信の設定	626
HTTP サーバーの設定	628
認証プロキシ Web ページのカスタマイズ	629
成功ログインに対するリダイレクション URL の指定	631
Web ベース認証パラメータの設定	632
Web ベースの認証ローカル バナーの設定	633
Web ベース認証キャッシュ エントリの削除	634
Web ベース認証ステータスの監視	635

## 第 26 章

<b>ポート単位のトラフィック制御の設定</b>	<b>637</b>
ポートベースのトラフィック制御の概要	637
ストーム制御に関する情報	637
ストーム制御	637
トラフィック アクティビティの測定方法	638
トラフィック パターン	638
ストーム制御の設定方法	639
ストーム制御およびしきい値レベルの設定	639
保護ポートに関する情報	642
保護ポート	642
保護ポートのデフォルト設定	643
保護ポートのガイドライン	643
保護ポートの設定方法	643
保護ポートの設定	643
保護ポートの監視	645
ポートブロッキングに関する情報	645
ポートブロッキング	645
ポートブロッキングの設定方法	645
インターフェイスでのフラッディング トラフィックのブロッキング	645
ポートブロッキングの監視	647
ポートベースのトラフィック制御に関するその他の関連資料	647
ポートベースのトラフィック制御の機能履歴	648

## 第 27 章

<b>ポート セキュリティ</b>	<b>649</b>
ポートセキュリティの前提条件	649
ポートセキュリティの制約事項	649
ポートセキュリティの概要	650
ポートセキュリティ	650
セキュア MAC アドレスのタイプ	650
スティッキ セキュア MAC アドレス	650

セキュリティ違反	651
ポートセキュリティ エージング	652
ポートセキュリティとスイッチ スタック	652
デフォルトのポートセキュリティ設定	653
ポートセキュリティの設定時の注意事項	653
ポートセキュリティの設定方法	655
ポートセキュリティのイネーブル化および設定	655
ポートセキュリティ エージングのイネーブル化および設定	661
ポートセキュリティの設定例	663

## 第 28 章

## コントロールプレーン ポリシングの設定 665

CoPP の制約事項	665
CoPP の概要	666
CoPP の概要	666
システム定義の CoPP の特徴	667
ユーザー設定可能な CoPP の特徴	675
ソフトウェアバージョンのアップグレードまたはダウングレード	676
ソフトウェアバージョンのアップグレードと CoPP	676
ソフトウェアバージョンのダウングレードと CoPP	677
CoPP の設定方法	678
CPU キューの有効化またはポリサー レートの変更	678
CPU キューの無効化	679
すべての CPU キューに対するデフォルトのポリサー レートの設定	681
CoPP の設定例	682
例：CPU キューの有効化または CPU キューのポリサー レートの変更	682
例：CPU キューの無効化	683
例：すべての CPU キューに対するデフォルトのポリサー レートの設定	684
CoPP のモニタリング	686
CoPP の機能履歴	686

## 第 29 章

## PKI での証明書の許可および失効の設定 691

PKI での証明書の許可および失効の設定	691
証明書の許可および失効に関する前提条件	691
証明書の許可および失効に関する制約事項	692
証明書の許可および失効に関する情報	692
PKI の許可	692
証明書ステータスのための PKI と AAA サーバーの統合	692
CRL または OCSP サーバー：証明書失効メカニズムの選択	695
許可または失効用に証明書ベースの ACL を使用する場合	697
PKI 証明書チェーンの検証	699
PKI に対して証明書の許可および失効を設定する方法	700
AAA サーバーとの PKI 統合の設定	700
PKI 証明書ステータス チェックの失効メカニズムの設定	705
証明書の許可および失効の設定	708
証明書チェーンの設定	717
証明書の許可および失効の設定例	718
PKI AAA 許可の設定および確認の例	718
例：失効メカニズムの設定	722
例：証明書失効チェック用に中央サイトでハブルータを構成する	723
例：証明書の許可および失効の設定	727
例：証明書チェーン検証の設定	730
PKI での証明書の許可および失効の追加リファレンス	731
PKI での証明書の許可および失効の機能履歴	731





# 第 1 章

## 不正アクセスの防止

- [機能情報の確認 \(1 ページ\)](#)
- [不正アクセスの防止 \(1 ページ\)](#)
- [不正アクセスの防止のための機能情報 \(2 ページ\)](#)

### 機能情報の確認

ご使用のソフトウェアリリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの **Bug Search Tool** およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、**Cisco Feature Navigator** を使用します。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> からアクセスします。Cisco.com のアカウントは必要ありません。

### 不正アクセスの防止

不正ユーザーによる、スイッチの再設定や設定情報の閲覧を防止できます。一般的には、ネットワーク管理者からスイッチへのアクセスを許可する一方、非同期ポートを用いてネットワーク外からダイヤルアップ接続するユーザーや、シリアルポートを通じてネットワーク外から接続するユーザー、またはローカルネットワーク内の端末またはワークステーションから接続するユーザーによるアクセスを制限します。

スイッチへの不正アクセスを防止するには、次のセキュリティ機能を1つまたは複数設定します。

- 最低限のセキュリティとして、各スイッチポートでパスワードおよび権限を設定します。このパスワードは、スイッチにローカルに保存されます。ユーザーがポートまたは回線を通じてスイッチにアクセスしようとするとき、ポートまたは回線に指定されたパスワードを入力してからでなければ、スイッチにアクセスできません。

- 追加のセキュリティレイヤとして、ユーザー名とパスワードをペアで設定できます。このペアはスイッチでローカルに保存されます。このペアは回線またはポートに割り当てられ、各ユーザを認証します。ユーザは認証後、スイッチにアクセスできます。権限レベルを定義している場合は、ユーザ名とパスワードの各ペアに特定の権限レベルを、対応する権利および権限とともに割り当てすることもできます。
- ユーザ名とパスワードのペアを使用したいが、そのペアをローカルではなく中央のサーバに保存したい場合は、セキュリティサーバ上のデータベースに保存できます。これにより、複数のネットワークングデバイスが同じデータベースを使用してユーザ認証情報を（必要に応じて許可情報も）得ることができます。
- また、失敗したログイン試行をログに記録するログイン拡張機能もイネーブルにすることもできます。ログイン拡張は、設定した回数のログインが失敗したあとに、それ以降のログイン試行をブロックするために設定することもできます。詳細については、『Cisco IOS Login Enhancements』マニュアルを参照してください。

## 不正アクセスの防止のための機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、[www.cisco.com/go/cfn](http://www.cisco.com/go/cfn) に移動します。Cisco.com のアカウントは必要ありません。

表 1: 不正アクセスの防止のための機能情報

機能名	リリース	機能情報
不正アクセスの防止	Cisco IOS XE Everest 16.5.1a	不正ユーザーによる、スイッチの再設定や設定情報の閲覧を防止できます。





## 第 2 章

# パスワードおよび権限レベルによるスイッチ アクセスの制御

- [パスワードおよび権限によるスイッチ アクセスの制御の制約事項 \(3 ページ\)](#)
- [パスワードおよび権限レベルに関する情報 \(4 ページ\)](#)
- [パスワードおよび権限レベルでスイッチ アクセスを制御する方法 \(6 ページ\)](#)
- [スイッチ アクセスのモニタリング \(18 ページ\)](#)
- [パスワードおよび権限レベルの設定例 \(19 ページ\)](#)
- [その他の参考資料 \(20 ページ\)](#)
- [パスワードおよび権限によるスイッチ アクセスの制御の機能履歴 \(20 ページ\)](#)

## パスワードおよび権限によるスイッチ アクセスの制御の制約事項

パスワードおよび権限によるスイッチ アクセスの制御の制約事項は、次のとおりです。

- **boot manual** グローバルコンフィギュレーション コマンドを使用して、スイッチを手動で起動するように設定している場合は、パスワード回復をディセーブルにできません。このコマンドは、スイッチの電源の再投入後、ブートローダプロンプト (*switch:*) を表示させます。
- パスワードタイプ 0 およびタイプ 7 は廃止されました。したがって、コンソール、Telnet、SSH、webUI、NETCONF への管理者ログインに使用されるパスワードタイプ 0 およびタイプ 7 は、パスワードタイプ 8 またはタイプ 9 に移行する必要があります。
- ISG および Dot1x の CHAP、EAP などのローカル認証でユーザー名とパスワードがタイプ 0 およびタイプ 7 の場合、アクションは不要です。
- イネーブルパスワードタイプ 0 およびタイプ 7 は、パスワードタイプ 8 またはタイプ 9 に移行する必要があります。
- パスワードタイプ 5 は廃止されました。パスワードタイプ 5 は、より強力なパスワードタイプ 8 またはタイプ 9 に移行する必要があります。

# パスワードおよび権限レベルに関する情報

## デフォルトのパスワードおよび権限レベル設定

ネットワークで端末のアクセスコントロールを行う簡単な方法は、パスワードを使用して権限レベルを割り当てることです。パスワード保護によって、ネットワークまたはネットワークデバイスへのアクセスが制限されます。権限レベルによって、ネットワークデバイスにログイン後、ユーザがどのようなコマンドを使用できるかが定義されます。

次の表に、デフォルトのパスワードおよび権限レベル設定を示します。

表 2: デフォルトのパスワードおよび権限レベル設定

機能	デフォルト設定
イネーブルパスワードおよび権限レベル	パスワードは定義されていません。デフォルトはレベル 15 です (特権 EXEC レベル)。パスワードは、コンフィギュレーションファイル内では暗号化されていない状態です。
イネーブルシークレットパスワードおよび権限レベル	パスワードは定義されていません。デフォルトはレベル 15 です (特権 EXEC レベル)。パスワードは、暗号化されたからコンフィギュレーションファイルに書き込まれます。
回線パスワード	パスワードは定義されていません。

## 追加のパスワードセキュリティ

セキュリティレベルを強化するために、特にネットワークを超えるパスワードや Trivial File Transfer Protocol (TFTP; 簡易ファイル転送プロトコル) サーバーに保存されたパスワードについて、グローバルコンフィギュレーションコマンド **enable password** または **enable secret** を使用できます。コマンドの作用はどちらも同じです。このコマンドにより、暗号化されたパスワードを設定できます。特権 EXEC モード (デフォルト設定) または特定の権限レベルにアクセスするユーザは、このパスワードを入力する必要があります。

より高度な暗号化アルゴリズムが使用されるので、**enable secret** コマンドを使用することを推奨します。

**enable secret** コマンドを設定した場合、このコマンドは **enable password** コマンドよりも優先されます。同時に 2 つのコマンドを有効にはできません。

パスワードの暗号化をイネーブルにすると、ユーザー名パスワード、認証キーパスワード、イネーブルコマンドパスワード、コンソールおよび仮想端末回線パスワードなど、すべてのパスワードに適用されます。

## パスワードの回復

スイッチに物理的にアクセスできるエンドユーザは、デフォルトで、スイッチの電源投入時にブートプロセスに割り込み、新しいパスワードを入力することによって、失われたパスワードを回復できます。

パスワード回復ディセーブル化機能では、この機能の一部をディセーブルにすることによりスイッチのパスワードへのアクセスを保護できます。この機能がイネーブルの場合、エンドユーザは、システムをデフォルト設定に戻すことに同意した場合に限り、ブートプロセスに割り込むことができます。パスワード回復をディセーブルにしても、ブートプロセスに割り込んでパスワードを変更できますが、コンフィギュレーションファイル (config.text) および VLAN データベース ファイル (vlan.dat) は削除されます。

パスワード回復をディセーブルにする場合は、エンドユーザがブートプロセスに割り込んでシステムをデフォルトの状態に戻すような場合に備え、セキュア サーバにコンフィギュレーションファイルのバックアップ コピーを保存しておくことを推奨します。スイッチ上でコンフィギュレーションファイルのバックアップ コピーを保存しないでください。VTP (VLAN トランッキング プロトコル) トランスペアレント モードでスイッチが動作している場合は、VLAN データベース ファイルのバックアップ コピーも同様にセキュア サーバに保存してください。スイッチがシステムのデフォルト設定に戻ったときに、XMODEM プロトコルを使用し、保存したファイルをスイッチにダウンロードできます。

## 端末回線の Telnet 設定

初めてスイッチに電源を投入すると、自動セットアッププログラムが起動して IP 情報を割り当て、この後続けて使用できるようにデフォルト設定を作成します。さらに、セットアッププログラムは、パスワードによる Telnet アクセス用にスイッチを設定することを要求します。セットアッププログラムの実行中にこのパスワードを設定しなかった場合は、端末回線に対する Telnet パスワードを設定するときに設定できます。

## ユーザ名とパスワードのペア

ユーザ名とパスワードのペアを設定できます。このペアはスイッチ上でローカルに保存されません。このペアは回線またはポートに割り当てられ、各ユーザを認証します。ユーザは認証後、スイッチにアクセスできます。権限レベルを定義している場合は、ユーザ名とパスワードの各ペアに特定の権限レベルを、対応する権利および権限とともに割り当てることもできます。

## 権限レベル

シスコデバイスでは、権限レベルを使用して、スイッチ動作の異なるレベルに対してパスワードセキュリティを提供します。デフォルトでは、Cisco IOS ソフトウェアは、パスワードセキュリティの 2 つのモード (権限レベル) で動作します。ユーザ EXEC (レベル 1) および特権 EXEC (レベル 15) です。各モードに、最大 16 個の階層レベルからなるコマンドを設定できます。複数のパスワードを設定することにより、ユーザグループ別に特定のコマンドへのアクセスを許可することができます。

### 回線の権限レベル

ユーザーは、回線にログインし、別の権限レベルを有効に設定することにより、**privilege level** ラインコンフィギュレーションコマンドを使用して設定された権限レベルを上書きできます。また、**disable** コマンドを使用することにより、権限レベルを引き下げることができます。上位の権限レベルのパスワードがわかっている場合、ユーザーはそのパスワードを使用して上位の権限レベルをイネーブルにできます。回線の使用を制限するには、コンソール回線に高いレベルまたは権限レベルを指定してください。

たとえば、多くのユーザに **clear line** コマンドへのアクセスを許可する場合、レベル2のセキュリティを割り当て、レベル2のパスワードを広範囲のユーザに配布できます。また、**configure** コマンドへのアクセス制限を強化する場合は、レベル3のセキュリティを割り当て、そのパスワードを限られたユーザグループに配布することもできます。

### コマンド権限レベル

コマンドをある権限レベルに設定すると、構文がそのコマンドのサブセットであるコマンドはすべて、そのレベルに設定されます。たとえば、**show ip traffic** コマンドをレベル15に設定すると、**show** コマンドと **show ip** コマンドは、異なるレベルに個別に設定しない限り、権限レベルは自動的に15に設定されます。

## パスワードおよび権限レベルでスイッチ アクセスを制御する方法

### スタティック 有効パスワードの設定または変更

イネーブルパスワードは、特権 EXEC モードへのアクセスを制御します。スタティック イネーブルパスワードを設定または変更するには、次の手順を実行します。

#### 手順の概要

1. **enable**
2. **configure terminal**
3. **enable password *password***
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

#### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 :	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。

	コマンドまたはアクション	目的
	デバイス> <code>enable</code>	
ステップ 2	<b>configure terminal</b> 例 : デバイス# <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 3	<b>enable password <i>password</i></b> 例 : デバイス (config)# <code>enable password secret321</code>	<p>特権 EXEC モードにアクセスするための新しいパスワードを定義するか、既存のパスワードを変更します。</p> <p>デフォルトでは、パスワードは定義されません。</p> <p><i>password</i> には、1～25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。疑問符 (?) は、パスワードを作成する場合に、疑問符の前に Ctrl+v を入力すれば使用できます。たとえば、パスワード <code>abc?123</code> を作成するときは、次のようになります。</p> <ol style="list-style-type: none"> <li>1. <code>abc</code> を入力します。</li> <li>2. Ctrl+v を入力します。</li> <li>3. <code>?123</code> を入力します。</li> </ol> <p>システムからイネーブルパスワードを入力するように求められた場合、疑問符の前に Ctrl+v を入力する必要はなく、パスワードのプロンプトにそのまま <code>abc?123</code> と入力できます。</p>
ステップ 4	<b>end</b> 例 : デバイス (config)# <code>end</code>	特権 EXEC モードに戻ります。
ステップ 5	<b>show running-config</b> 例 : デバイス# <code>show running-config</code>	入力を確認します。

	コマンドまたはアクション	目的
ステップ 6	<b>copy running-config startup-config</b> 例：  デバイス# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## 暗号化によるイネーブルおよびイネーブル シークレット パスワードの保護

特権 EXEC モード (デフォルト) または指定された特権レベルにアクセスするためにユーザーが入力する必要がある暗号化パスワードを確立するには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. 次のいずれかを使用します。
  - `enable password [level level] {password encryption-type encrypted-password}`
  - `enable secret [level level] {password encryption-type encrypted-password}`
4. **service password-encryption**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  デバイス> <b>enable</b>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>• パスワードを入力します (要求された場合)。</li> </ul>
ステップ 2	<b>configure terminal</b> 例：  デバイス# <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。

	コマンドまたはアクション	目的
ステップ 3	<p>次のいずれかを使用します。</p> <ul style="list-style-type: none"> <li>• <code>enable password [level level] {password encryption-type encrypted-password}</code></li> <li>• <code>enable secret [level level] {password encryption-type encrypted-password}</code></li> </ul> <p>例 :</p> <pre>デバイス(config)# enable password example102</pre> <p>または</p> <pre>デバイス(config)# enable secret level 1 password secret123sample</pre>	<ul style="list-style-type: none"> <li>• 特権 EXEC モードにアクセスするための新しいパスワードを定義するか、既存のパスワードを変更します。</li> <li>• シークレットパスワードを定義します。これは非可逆的な暗号化方式を使用して保存されます。 <ul style="list-style-type: none"> <li>• (任意) <i>level</i> に指定できる範囲は 0 ~ 15 です。レベル 1 が通常のユーザ EXEC モード権限です。デフォルト レベルは 15 です (特権 EXEC モード権限)。</li> <li>• <i>password</i> には、1 ~ 25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されません。</li> <li>• (任意) <i>encryption-type</i> には、シスコ独自の暗号化アルゴリズムであるタイプ 5 しか使用できません。暗号化タイプを指定する場合は、暗号化されたパスワードを使用する必要があります。この暗号化パスワードは、別のスイッチの設定からコピーします。</li> </ul> </li> </ul> <p>(注) 暗号化タイプを指定してクリア テキストパスワードを入力した場合は、再び特権 EXEC モードを開始することはできません。暗号化されたパスワードが失われた場合は、どのような方法でも回復することはできません。</p>
ステップ 4	<p><code>service password-encryption</code></p> <p>例 :</p> <pre>デバイス(config)# service password-encryption</pre>	<p>(任意) パスワードの定義時または設定の書き込み時に、パスワードを暗号化します。</p> <p>暗号化を行うと、コンフィギュレーションファイル内でパスワードが読み取り可能な形式になるのを防止できます。</p>
ステップ 5	<p><code>end</code></p> <p>例 :</p>	<p>特権 EXEC モードに戻ります。</p>

	コマンドまたはアクション	目的
	デバイス(config)# end	
ステップ 6	<b>show running-config</b> 例： デバイス# show running-config	入力を確認します。
ステップ 7	<b>copy running-config startup-config</b> 例： デバイス# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

## パスワード回復のディセーブル化

パスワードの回復をディセーブルにしてスイッチのセキュリティを保護するには、次の手順を実行します。

### 始める前に

パスワード回復をディセーブルにする場合は、エンドユーザがブートプロセスに割り込んでシステムをデフォルトの状態に戻すような場合に備え、セキュア サーバにコンフィギュレーションファイルのバックアップ コピーを保存しておくことを推奨します。スイッチ上でコンフィギュレーションファイルのバックアップ コピーを保存しないでください。VTP (VLAN トランッキング プロトコル) トランスペアレント モードでスイッチが動作している場合は、VLAN データベース ファイルのバックアップ コピーも同様にセキュア サーバに保存してください。スイッチがシステムのデフォルト設定に戻ったときに、XMODEM プロトコルを使用して、保存したファイルをスイッチにダウンロードできます。

### 手順の概要

1. enable
2. configure terminal
3. system disable password recovery switch {all | <1-9>}
4. end

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：	特権 EXEC モードを有効にします。  • パスワードを入力します (要求された場合)。



	コマンドまたはアクション	目的
	デバイス> <code>enable</code>	
ステップ 2	<b>configure terminal</b> 例： デバイス# <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 3	<b>system disable password recovery switch {all   &lt;1-9&gt;}</b> 例： デバイス(config)# <code>system disable password recovery switch all</code>	パスワード回復をディセーブルにします。  <ul style="list-style-type: none"> <li>• <code>all</code> : スタック内のスイッチで設定を行います。</li> <li>• <code>&lt;1-9&gt;</code> : 選択したスイッチ番号で設定を行います。</li> </ul> <p>この設定は、フラッシュメモリの中で、ブートローダおよび Cisco IOS イメージがアクセスできる領域に保存されますが、ファイルシステムには含まれません。また、ユーザーがアクセスすることはできません。</p>
ステップ 4	<b>end</b> 例： デバイス(config)# <code>end</code>	特権 EXEC モードに戻ります。

#### 次のタスク

`disable password recovery` を削除するには、`no system disable password recovery switch all` 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。

## 端末回線に対する Telnet パスワードの設定

接続された端末回線に対する Telnet パスワードを設定するには、ユーザー EXEC モードで次の手順を実行します。

#### 始める前に

- エミュレーション ソフトウェアを備えた PC またはワークステーションをスイッチ コンソール ポートに接続するか、または PC をイーサネット管理ポートに接続します。
- コンソールポートのデフォルトのデータ特性は、9600 ボー、8 データ ビット、1 ストップ ビット、パリティなしです。コマンドラインプロンプトが表示されるまで、Return キーを何回か押す必要があります。

## 手順の概要

1. **enable**
2. **configure terminal**
3. **line vty 0 15**
4. **password *password***
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  デバイス> <b>enable</b>	(注) パスワードが特権 EXEC モードへのアクセスに必要な場合は、その入力が必要です。  特権 EXEC モードを開始します。
ステップ 2	<b>configure terminal</b> 例：  デバイス# <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 3	<b>line vty 0 15</b> 例：  デバイス(config)# <b>line vty 0 15</b>	Telnet セッション (回線) の数を設定し、ライン コンフィギュレーション モードを開始します。  コマンド対応デバイスでは、最大 16 のセッションが可能です。0 および 15 を指定すると、使用できる 16 の Telnet セッションすべてを設定することになります。
ステップ 4	<b>password <i>password</i></b> 例：  デバイス(config-line)# <b>password abcxyz543</b>	1 つまたは複数の回線に対応する Telnet パスワードを設定します。  <i>password</i> には、1～25 文字の英数字の文字列を指定します。文字列を数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されません。
ステップ 5	<b>end</b> 例：  デバイス(config-line)# <b>end</b>	特権 EXEC 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 6	<b>show running-config</b> 例：  デバイス# <code>show running-config</code>	入力を確認します。
ステップ 7	<b>copy running-config startup-config</b> 例：  デバイス# <code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

## ユーザ名とパスワードのペアの設定

ユーザー名とパスワードのペアを設定するには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **username name [ privilege level] { password encryption-type password}**
4. 次のいずれかを使用します。
  - **line console 0**
  - **line vty 0 15**
5. **login local**
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  デバイス> <code>enable</code>	特権 EXEC モードを有効にします。  • パスワードを入力します (要求された場合)。
ステップ 2	<b>configure terminal</b> 例：  デバイス# <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。

	コマンドまたはアクション	目的
ステップ 3	<p><b>username name [ privilege level ] { password encryption-type password }</b></p> <p>例 :</p> <pre>デバイス(config)# username adamsample privilege 1 password secret456</pre> <pre>デバイス(config)# username 111111111111 mac attribute</pre>	<p>各ユーザのユーザ名、権限レベル、パスワードを設定します。</p> <ul style="list-style-type: none"> <li>• <i>name</i> には、ユーザー ID を 1 ワードで指定するか、または MAC アドレスを指定します。スペースと引用符は使用できません。</li> <li>• ユーザ名と MAC フィルタの両方に対し、最大 12000 のクライアントを個別に設定できます。</li> <li>• (任意) <i>level</i> には、アクセス権を得たユーザーに設定する権限レベルを指定します。指定できる範囲は 0 ~ 15 です。レベル 15 では特権 EXEC モードでのアクセスが可能です。レベル 1 では、ユーザ EXEC モードでのアクセスとなります。</li> <li>• <i>encryption-type</i> には、暗号化されていないパスワードが後ろに続く場合は 0 を入力します。暗号化されたパスワードが後ろに続く場合は 7 を指定します。</li> <li>• <i>password</i> には、デバイスへアクセスするためにユーザーが入力しなければならないパスワードを指定します。パスワードは 1 ~ 25 文字で、埋め込みスペースを使用でき、<b>username</b> コマンドの最後のオプションとして指定します。</li> </ul>
ステップ 4	<p>次のいずれかを使用します。</p> <ul style="list-style-type: none"> <li>• <b>line console 0</b></li> <li>• <b>line vty 0 15</b></li> </ul> <p>例 :</p> <pre>デバイス(config)# line console 0</pre> <p>または</p> <pre>デバイス(config)# line vty 15</pre>	<p>ライン コンフィギュレーション モードを開始し、コンソール ポート (回線 0) または VTY 回線 (回線 0 ~ 15) を設定します。</p>
ステップ 5	<p><b>login local</b></p> <p>例 :</p> <pre>デバイス(config-line)# login local</pre>	<p>ログイン時のローカルパスワードチェックをイネーブルにします。認証は、ステップ 3 で指定されたユーザ名に基づきます。</p>
ステップ 6	<p><b>end</b></p> <p>例 :</p>	<p>特権 EXEC モードに戻ります。</p>

	コマンドまたはアクション	目的
	デバイス (config) # <b>end</b>	
ステップ 7	<b>show running-config</b> 例 : デバイス # <b>show running-config</b>	入力を確認します。
ステップ 8	<b>copy running-config startup-config</b> 例 : デバイス # <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## コマンドの特権レベルの設定

コマンドの権限レベルを設定するには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **privilege mode level level command**
4. **enable password level level password**
5. **end**
6. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : デバイス > <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します (要求された場合)。
ステップ 2	<b>configure terminal</b> 例 : デバイス # <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。

	コマンドまたはアクション	目的
ステップ 3	<p><b>privilege mode level level command</b></p> <p>例 :</p> <pre>デバイス(config)# <b>privilege exec level 14 configure</b></pre>	<p>コマンドの特権レベルを設定します。</p> <ul style="list-style-type: none"> <li>• <i>mode</i> には、グローバル コンフィギュレーション モードの場合は <b>configure</b> を、EXEC モードの場合は <b>exec</b> を、インターフェイス コンフィギュレーション モードの場合は <b>interface</b> を、ライン コンフィギュレーション モードの場合は <b>line</b> をそれぞれ入力します。</li> <li>• <i>level</i> の範囲は 0 ~ 15 です。レベル 1 が通常のユーザー EXEC モード権限です。レベル 15 は、<b>enable</b> パスワードによって許可されるアクセスレベルです。</li> <li>• <i>command</i> には、アクセスを制限したいコマンドを指定します。</li> </ul>
ステップ 4	<p><b>enable password level level password</b></p> <p>例 :</p> <pre>デバイス(config)# <b>enable password level 14 SecretPswd14</b></pre>	<p>権限レベルをイネーブルにするためのパスワードを指定します。</p> <ul style="list-style-type: none"> <li>• <i>level</i> の範囲は 0 ~ 15 です。レベル 1 が通常のユーザー EXEC モード権限です。</li> <li>• <i>password</i> には、1 ~ 25 文字の英数字のストリングを指定します。ストリングを数字で始めることはできません。大文字と小文字を区別し、スペースを使用できますが、先行スペースは無視されます。デフォルトでは、パスワードは定義されません。</li> </ul>
ステップ 5	<p><b>end</b></p> <p>例 :</p> <pre>デバイス(config)# <b>end</b></pre>	<p>特権 EXEC モードに戻ります。</p>
ステップ 6	<p><b>copy running-config startup-config</b></p> <p>例 :</p> <pre>デバイス# <b>copy running-config startup-config</b></pre>	<p>(任意) コンフィギュレーションファイルに設定を保存します。</p>

## 回線のデフォルト特権レベルの変更

指定した回線のデフォルトの権限レベルを変更するには、次の手順を実行します。

## 手順の概要

1. **enable**
2. **configure terminal**
3. **line vty *line***
4. **privilege level *level***
5. **end**
6. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  デバイス> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  デバイス# <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 3	<b>line vty <i>line</i></b> 例：  デバイス(config)# <b>line vty 10</b>	アクセスを制限する仮想端末回線を選択します。
ステップ 4	<b>privilege level <i>level</i></b> 例：  デバイス(config)# <b>privilege level 15</b>	回線のデフォルト特権レベルを変更します。  <i>level</i> の範囲は 0 ~ 15 です。レベル 1 が通常のユーザー EXEC モード権限です。レベル 15 は、 <b>enable</b> パスワードによって許可されるアクセス レベルです。
ステップ 5	<b>end</b> 例：  デバイス(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 6	<b>copy running-config startup-config</b> 例：  デバイス# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

### 次のタスク

ユーザーは、回線にログインし、別の権限レベルを有効に設定することにより、**privilege level** ラインコンフィギュレーションコマンドを使用して設定された権限レベルを上書きできます。また、**disable** コマンドを使用することにより、権限レベルを引き下げることができます。上位の権限レベルのパスワードがわかっている場合、ユーザーはそのパスワードを使用して上位の権限レベルをイネーブルにできます。回線の使用を制限するには、コンソール回線に高いレベルまたは権限レベルを指定してください。

## 権限レベルへのログインおよび終了

指定した権限レベルにログインする、または指定した権限レベルを終了するには、ユーザー EXEC モードで次の手順を実行します。

### 手順の概要

1. **enable level**
2. **disable level**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable level</b> 例： デバイス> <b>enable 15</b>	指定された特権レベルにログインします。 この例で、レベル 15 は特権 EXEC モードです。 <i>level</i> に指定できる範囲は 0 ~ 15 です。
ステップ 2	<b>disable level</b> 例： デバイス# <b>disable 1</b>	指定した特権レベルを終了します。 この例で、レベル 1 はユーザ EXEC モードです。 <i>level</i> に指定できる範囲は 0 ~ 15 です。

## スイッチ アクセスのモニタリング

表 3: DHCP 情報を表示するためのコマンド

<b>show privilege</b>	権限レベルの設定を表示します。
-----------------------	-----------------



## パスワードおよび権限レベルの設定例

### 例：スタティック イネーブルパスワードの設定または変更

次に、イネーブルパスワードを *11u2c3k4y5* に変更する例を示します。パスワードは暗号化されず、レベル 15 のアクセスが与えられます（従来の特権 EXEC モードアクセス）。

```
デバイス(config)# enable password 11u2c3k4y5
```

### 例：暗号化によるイネーブルおよびイネーブルシークレットパスワードの保護

次に、権限レベル 2 に対して暗号化パスワード *\$1\$FaD0\$Xyti5Rkls3LoyxzS8* を設定する例を示します。

```
デバイス(config)# enable secret level 2 5 $1$FaD0$Xyti5Rkls3LoyxzS8
```

### 例：端末回線に対する Telnet パスワードの設定

次に、Telnet パスワードを *let45me67in89* に設定する例を示します。

```
デバイス(config)# line vty 10
デバイス(config-line)# password let45me67in89
```

### 例：コマンドの権限レベルの設定

ここで、**configure** コマンドを権限レベル 14 に設定する方法、レベル 14 のコマンドを使用する場合にユーザーが入力するパスワードとして *SecretPswd14* を定義する方法を示します。

```
デバイス(config)# privilege exec level 14 configure
デバイス(config)# enable password level 14 SecretPswd14
```

## その他の参考資料

### エラー メッセージ デコーダ

説明	リンク
このリリースのシステムエラーメッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	<a href="https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi">https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi</a>

### MIB

MB	MIB のリンク
	<p>選択したプラットフォーム、Cisco IOS リリース、およびフィーチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

### シスコのテクニカル サポート

説明	リンク
<p>シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。</p> <p>お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service (Field Notice からアクセス)、Cisco Technical Services Newsletter、Really Simple Syndication (RSS) フィードなどの各種サービスに加入できます。</p> <p>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。</p>	<a href="http://www.cisco.com/support">http://www.cisco.com/support</a>

## パスワードおよび権限によるスイッチアクセスの制御の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	パスワードおよび権限によるスイッチ アクセスの制御	パスワード保護によって、ネットワークまたはネットワークデバイスへのアクセスが制限されます。権限レベルによって、ネットワークデバイスにログイン後、ユーザがどのようなコマンドを使用できるかが定義されます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。





## 第 3 章

# 認証の設定

認証は、選択したセキュリティプロトコルに応じてログイン/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、および暗号化などのユーザーの識別方法を提供します。認証は、ユーザー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、ユーザーの識別を行う方法です。

- [認証の設定の前提条件 \(23 ページ\)](#)
- [認証の設定に関する制約事項 \(23 ページ\)](#)
- [認証の設定に関する情報 \(24 ページ\)](#)
- [AAA 認証方式を設定する方法 \(33 ページ\)](#)
- [認証設定の機能履歴 \(87 ページ\)](#)

## 認証の設定の前提条件

シスコソフトウェアによる認証の実装は、認証、許可、およびアカウンティング (AAA) 認証と非認証方式に分かれています。シスコでは、可能であれば AAA セキュリティ サービスを試用して認証を実装することを推奨します。

## 認証の設定に関する制約事項

- 設定できる AAA 方式リストの数は 250 です。
- **acct-port** キーワードを使用してアカウンティング要求と異なる UDP 宛先ポートに、および非標準オプションの有無に関係なく **auth-port** キーワードを使用して認証要求の UDP 宛先ポートに同じ RADIUS サーバーの IP アドレスを設定した場合、RADIUS サーバーは非標準オプションを受け入れません。

# 認証の設定に関する情報

## 認証の名前付き方式リスト

まず認証方式の名前付きリストを定義して AAA 認証を設定し、その名前付きリストを各種インターフェイスに適用します。この方式リストは、認証のタイプと実行順序を定義したものです。定義されたいずれかの認証方式を実行するには、この方式リストを特定のインターフェイスに適用する必要があります。唯一の例外は、デフォルトの方式リスト（「default」という名前）です。デフォルトの方式リストは、明示的に定義された名前付きの方式リストを持つインターフェイスを除くすべてのインターフェイスに自動的に適用されます。定義済みの方式リストは、デフォルトの方式リストに優先します。

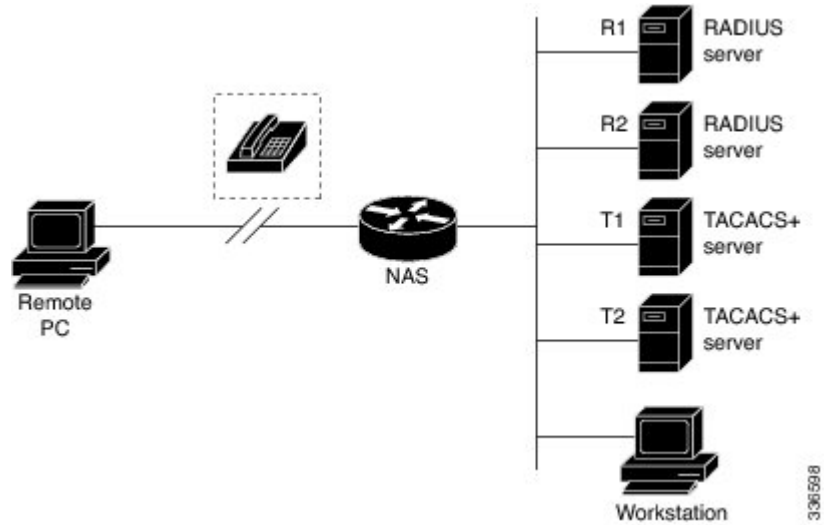
方式リストとは、ユーザー認証のために照会される認証方式を記述したシーケンシャルリストです。方式リストを使用すると、認証に使用するセキュリティプロトコルを1つまたは複数指定できるため、最初の方式が失敗した場合に備えて認証のバックアップシステムを確保できます。シスコソフトウェアは、ユーザーを認証するため、リストに記載されている最初の方式が使用されます。その方式で応答に失敗した場合、シスコソフトウェアは、方式リストに記載されている次の認証方式を選択します。このプロセスは、方式リストのいずれかの認証方式と通信に成功するか、定義されているすべての方式が試行されるまで継続されます。

このシスコソフトウェアでは、前の方式からの応答がない場合にだけ、リストの次の認証方式で認証が試行される、という点に注意してください。このサイクルのいずれかの時点で認証に失敗した場合、つまりセキュリティサーバーまたはローカルユーザー名データベースからユーザーアクセスを拒否する応答があった場合には、許可プロセスが停止し、それ以上の認証方式は試行されません。

## 方式リストとサーバグループ

サーバグループは、方式リストに使用する既存の RADIUS または TACACS+ サーバ ホストをグループ化する方法の1つです。次の図に、4台のセキュリティサーバー（R1 と R2 は RADIUS サーバ、T1 と T2 は TACACS+ サーバ）が設置された一般的な AAA ネットワーク設定を示します。R1 と R2 で RADIUS サーバのグループを構成します。T1 と T2 で TACACS+ サーバのグループを構成します。

図 1: 一般的な AAA ネットワーク設定



サーバー グループを使用して、設定したサーバー ホストのサブセットを指定し、特定のサービスに使用します。たとえば、サーバー グループを使用すると、R1 および R2 を 1 つのサーバー グループとして定義し、T1 および T2 を別のサーバー グループとして定義できます。また、認証ログインの方式リストに R1 および T1 を指定し、PPP 認証の方式リストに R2 および T2 を指定することもできます。

サーバグループには、1 台のサーバに対して複数のホストエントリを含めることができます。エントリごとに固有の識別情報を設定します。固有の識別情報は、IP アドレスと UDP ポート番号の組み合わせで構成されます。これにより、RADIUS ホストとして定義されているさまざまなポートが、固有の AAA サービスを提供できるようになります。つまり、この固有識別情報を使用して、ある IP アドレスに位置する 1 台のサーバ上に複数の UDP ポートが存在する場合、それぞれの UDP ポートに対して RADIUS 要求を送信できます。1 台の RADIUS サーバ上にある異なる 2 つのホストエントリが 1 つのサービス（認証など）に設定されている場合、設定されている 2 番目のホスト エントリは最初のホスト エントリのフェールオーバー バックアップとして動作します。この例の場合、最初のホスト エントリがアカウントिंगサービスの提供に失敗すると、同じデバイスに設定されている 2 番目のホストエントリを使用してアカウントिंगサービスを提供するように、ネットワークアクセスサーバが試行します（試行される RADIUS ホストエントリの順番は、設定されている順序に従います）。

サーバグループの設定および着信番号識別サービス（DNIS）番号に基づくサーバグループの設定の詳細については、「Configuring RADIUS」または「Configuring TACACS+」の章を参照してください。

## 方式リストの例

たとえば、システム管理者が、すべてのインターフェイスに同じ認証方式を使用して PPP 接続を認証する、というセキュリティ ソリューションを決定したとします。RADIUS グループでは、まず認証情報のために R1 に接続し、応答がない場合、R2 に接続します。R2 が応答しない場合、TACACS+ グループの T1 に接続し、T1 が応答しない場合、T2 に接続します。すべての指定したサーバが応答しなかった場合、認証はアクセスサーバ自体のローカルユーザー

名データベースで行われます。このソリューションを実装するには、システム管理者が次のコマンドを入力してデフォルトの方式リストを作成します。

```
aaa authentication ppp default group radius group tacacs+ local
```

この例では、「default」が方式リストの名前です。この方式リストにプロトコルを含める場合、名前の後に、照会される順で指定します。デフォルトのリストは、すべてのインターフェイスに自動的に適用されます。

リモートユーザーがネットワークにダイヤルインしようとする、ネットワークアクセスサーバーは、まず R1 に認証情報を照会します。ユーザーが R1 から認証されると、R1 からネットワーク アクセス サーバーに対して PASS 応答が発行され、ユーザーはネットワークにアクセスできるようになります。R1 から FAIL 応答が返されると、ユーザーはアクセスを拒否され、セッションは終了します。R1 が応答しない場合、ネットワークアクセスサーバーでは ERROR として処理され、認証情報について R2 に照会されます。このパターンは、ユーザーが認証または拒否されるか、セッションが終了するまで、残りの指定した方式について続行されます。

FAIL 応答は ERROR とまったく異なる点に注意してください。FAIL とは、適用可能な認証データベースに含まれる、認証の成功に必要な基準をユーザーが満たしていないことを示します。認証は FAIL 応答で終了します。ERROR とは、認証の照会に対してサーバーが応答しなかったことを示します。そのため、認証は試行されません。ERROR が検出された場合にだけ、認証方式リストに定義されている次の認証方式が AAA によって選択されます。

たとえば、システム管理者が、1つのインターフェイス、または一部のインターフェイスにだけ方式リストを適用するとします。この場合、システム管理者は名前付き方式リストを作成し、その名前付きリストを対象のインターフェイスに適用します。次に、システム管理者が、インターフェイス 3 にだけ適用する認証方式を実装する場合の例を示します。

```
aaa authentication ppp default group radius group tacacs+ local
aaa authentication ppp apple group radius group tacacs+ local none
interface async 3
 ppp authentication chap apple
```

この例では、「apple」が方式リストの名前です。また、この方式リストに含まれるプロトコルは、名前の後に、実行する順で指定されています。方式リストを作成すると、該当するインターフェイスに適用されます。AAA および PPP 認証コマンド両方の方式リスト名 (apple) は一致する必要があります。

次の例では、システム管理者がサーバー グループを使用し、PPP 認証の場合は R2 および T2 だけが有効であることを指定します。この場合、管理者は、メンバがそれぞれ R2 (172.16.2.7) と T2 (172.16.2.77) であるサーバーグループを定義する必要があります。この例では、RADIUS サーバーグループ「rad2only」は **aaa group server** コマンドを使用して次のように定義されます。

```
aaa group server radius rad2only
 server 172.16.2.7
```

TACACS+ サーバーグループ「tac2only」は、**aaa group server** コマンドを使用して次のように定義されます。



```
aaa group server tacacs+ tac2only
server 172.16.2.77
```

次に、管理者はサーバー グループを使用して PPP 認証を適用します。この例では、PPP 認証用のデフォルト方式リストは **group rad2only**、**group tac2only**、**local** の順序に従います。

```
aaa authentication ppp default group rad2only group tac2only local
```

VTY 回線で方式リストを設定する場合、対応する方式リストを AAA に追加する必要があります。次の例は、VTY 回線の下に方式リストを設定する方法を示しています。

```
Device# configure terminal
Device(config)# line vty 0 4
Device(config)# authorization commands 15 auth1
```

次の例は、AAA で方式リストを設定する方法を示しています。

```
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authorization commands 15 auth1 group tacacs+
```

VTY 回線で方式リストを設定しない場合、デフォルトの方式リストを AAA に追加する必要があります。次の例は、方式リストを使用しない VTY 設定を示しています。

```
Device# configure terminal
Device(config)# line vty 0 4
```

次の例は、デフォルトの方式リストを設定する方法を示しています。

```
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authorization commands 15 default group tacacs+
```

## 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、クエリー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。シスコのソフトウェアは、プッシュ モデルで使用される RFC 5176 で定義された RADIUS 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、許可、アカウントिंग (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。

次のセッション単位の CoA 要求を使用します。

- セッション再認証
- セッションの終了
- ポート シャットダウンでのセッション終了
- ポート バウンスでのセッション終了
- セキュリティとパスワード

- アカウンティング

## CoA 要求

CoA 要求は、RFC 5176 に記載されているように、プッシュ モデルで使用するによって、セッション識別、ホスト再認証、およびセッション終了を行うことができます。モデルは、次のように、1 つの要求 (CoA-Request) と 2 つの考えられる応答コードで構成されます。

- CoA acknowledgment (ACK) [CoA-ACK]
- CoA non-acknowledgment (NAK) [CoA-NAK]

要求は CoA クライアント (通常は RADIUS またはポリシー サーバ) から開始されて、リッスナーとして動作するデバイスに転送されます。

## RFC 5176 規定

Disconnect Request メッセージは Packet of Disconnect (POD) とも呼ばれますが、セッション終了に対してデバイスでサポートされています。

次の表に、RADIUS 認可変更 (CoA) 機能でサポートされている IETF 属性を示します。

表 4: サポートされている IETF 属性

属性番号	属性名
24	状態
31	Calling-Station-ID
44	Acct-Session-ID
80	Message-Authenticator
101	Error-Cause

次の表に、Error-Cause 属性で取ることができる値を示します。

表 5: Error-Cause の値

値	説明
201	削除された残留セッション コンテキスト
202	無効な EAP パケット (無視)
401	サポートされていない属性
402	見つからない属性
403	NAS 識別情報のミスマッチ

値	説明
404	無効な要求
405	サポートされていないサービス
406	サポートされていない拡張機能
407	無効な属性値
501	管理上の禁止
502	ルート不可能な要求 (プロキシ)
503	セッション コンテキストが検出されない
504	セッション コンテキストが削除できない
505	その他のプロキシ処理エラー
506	リソースが使用不可能
507	要求が発信された
508	マルチセッションの選択がサポートされていない

## CoA 要求応答コード

CoA 要求の応答コードは、デバイスへコマンドを発行するために使用されます。サポートされているコマンドを「CoA 要求コマンド」に示します。

RFC 5176 で定義されている CoA 要求応答コードのパケットの形式は、コード、ID、長さ、オーセンティケータ、およびタイプ、長さ、値 (TLV) 形式の属性から構成されます。

属性フィールドは、Cisco ベンダー固有属性 (VSA) を送信するために使用します。

### セッションの識別

特定のセッションに対する接続解除および CoA 要求の場合、デバイスは次の 1 つまたは複数の属性に基づいてセッションを検出します。

- Acct-Session-Id (IETF 属性 #44)
- Audit-Session-Id (シスコのベンダー固有属性 (VSA) )
- Calling-Station-Id (ホスト MAC アドレスを含む IETF 属性 #31)

CoA メッセージに含まれるすべてのセッション ID 属性がそのセッションと一致しない限り、デバイスは「Invalid Attribute Value」エラーコード属性を含む Disconnect-NAK または CoA-NAK を返します。



(注) CoA NAK メッセージは、キーの不一致があるすべての CoA 要求に送信されるわけではありません。メッセージは、クライアントの最初の 3 つの要求にのみ送信されます。その後、そのクライアントからのすべてのパケットがドロップされます。キーの不一致が見つかり、CoA NAK メッセージで送信される応答オーセンティケータはダミーのキー値から計算されます。

### CoA ACK 応答コード

許可ステートの変更に成功した場合は、肯定確認応答 (ACK) が送信されます。CoA ACK 内で返される属性は CoA 要求によって異なります。

### CoA NAK 応答コード

否定応答 (NAK) は許可ステートの変更に失敗したことを示し、エラーの理由を示す属性を含めることができます。

### CoA 要求コマンド

デバイスでサポートされているコマンドを次の表に示します。すべての CoA コマンドには、デバイスと CoA クライアント間のセッション ID が含まれている必要があります。

表 6: デバイスでサポートされる CoA 要求コマンド

コマンド	シスコの VSA
Bounce host port	Cisco:Avpair="subscriber:command=bounce-host-port"
Disable host port	Cisco:Avpair="subscriber:command=disable-host-port"
Reauthenticate host	Cisco:Avpair="subscriber:command=reauthenticate"
Terminate session	VSA を必要としない標準の接続解除要求です

### 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、アカウントिंग (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用したのと同じ 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。

ホストのネットワークへのアクセスを制限するには、

Cisco:Avpair="subscriber:command=disable-host-port" VSA を含む CoA 要求を使用します。このコマンドは、ホストがネットワーク上で問題を起きていることを把握し、ホストのネットワークアクセスを即座にブロックする必要がある場合に便利です。ポートのネットワークアクセスを復元する場合は、非 RADIUS メカニズムを使用して再びイネーブルにします。

### CoA 要求の disable host port

RADIUS サーバーの CoA disable port コマンドを実行すると、セッションをホストしている認証ポートが管理的にシャットダウンされます。その結果、セッションは終了します。このコマンドは、ホストがネットワーク上で問題を起きていることを把握し、ホストのネットワークアクセスを即座にブロックする必要がある場合に便利です。ポートのネットワークアクセスを復元する場合は、非 RADIUS メカニズムを使用して再びイネーブルにします。このコマンドは、次の VSA を含む標準の CoA-Request メッセージで伝達されます。

```
Cisco:Avpair="subscriber:command=disable-host-port"
```

このコマンドはセッション指向であるため、「セッション ID」セクションに示されている 1 つ以上のセッション ID 属性とともに使用する必要があります。セッションを検出できない場合、デバイスは「Session Context Not Found」エラーコード属性を含む CoA-NAK メッセージを返します。デバイスは、セッションを検出すると、ホスティングポートを無効にし、CoA-ACK メッセージを返します。

デバイスが CoA-ACK をクライアントに返す前にデバイスに障害が発生した場合、クライアントから要求が再送信されると、新しいアクティブデバイス上でそのプロセスが繰り返されます。デバイスが CoA-ACK メッセージをクライアントに返した後でデバイスに障害が発生したが、操作が完了していない場合、その操作は新しいアクティブデバイスで再開されます。

RADIUS サーバの CoA disable port コマンドを無視するには、「bounce および disable RADIUS CoA 要求を無視するためのデバイスの設定」を参照してください。

### CoA 要求の bounce port

RADIUS サーバーの CoA bounce port が RADIUS サーバーから送信されると、認証ポートでリンクのフラップが発生します。その結果、このポートに接続している 1 つまたは複数のホストから、DHCP の再ネゴシエーションが開始されます。この状況は、VLAN の変更があり、この認証ポートに関する変化を検出するメカニズムがないデバイス（プリンタなど）がエンドポイ

ントの場合に発生する可能性があります。CoA bounce port は、次の新しい VSA を含む標準の CoA-Request メッセージで伝達されます。

```
Cisco:Avpair="subscriber:command=bounce-host-port"
```

このコマンドはセッション指向であるため、「セッションID」に示されている1つ以上のセッションID属性とともに使用する必要があります。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 CoA-NAK メッセージを返します。このセッションがある場合は、デバイスはホストポートを10秒間ディセーブルし、再びイネーブルにし（ポートバウンス）、CoA-ACKを返します。

RADIUS サーバの CoA bounce port を無視するには、「bounce および disable RADIUS CoA 要求を無視するためのデバイスの設定」を参照してください。

## ドメインストリッピング

AAA ブロードキャスト アカウンティング機能を有効にすると、アカウンティング情報を複数の AAA サーバーに同時に送信できます。つまり、アカウンティング情報を1つまた複数の AAA サーバーに同時にブロードキャストすることが可能です。この機能を使用すると、プライベートおよびパブリック AAA サーバーにアカウント情報を送信できます。この機能では、音声アプリケーションによる課金情報も提供されます。

ドメインストリッピング機能を使用すると、ドメインストリッピングをサーバーグループレベルで設定できます。

サーバー単位のグループ コンフィギュレーションはグローバル コンフィギュレーションを上書きします。ドメインストリッピングが、グローバルではイネーブルではないがサーバーグループでイネーブルになっている場合、そのサーバーグループに対してのみイネーブルになります。また、Virtual Routing and Forwarding (VRF) 固有のドメインストリッピングがグローバルで設定されていて、別の VRF のドメインストリッピングがサーバーグループで設定されている場合、ドメインストリッピングは両方の VRF でイネーブルになります。VRF の設定は、サーバーグループ コンフィギュレーション モードから取得されます。サーバーグループ コンフィギュレーションがグローバル コンフィギュレーション モードでディセーブルになっているが、サーバーグループ コンフィギュレーション モードで使用可能である場合、サーバーグループ コンフィギュレーション モードでのすべての設定が適用可能です。

ドメインストリッピングおよびブロードキャスト アカウンティングを設定した後で、設定ごとに別個のアカウント記録を作成できます。

**domain-stripping** コマンドと **directed-request** コマンドの両方が有効になっている場合、ドメインストリッピングが優先され、ダイレクトリクエスト機能は動作しません。

# AAA 認証方式を設定する方法

## AAA を使用したログイン認証の設定

AAA セキュリティ サービスにより、さまざまなログイン認証方式を容易に実行できるようになります。 **aaa authentication login** コマンドを使用すると、サポートされているログイン認証方式のいずれを使用するかに関係なく、AAA 認証が有効になります。 **aaa authentication login** コマンドを使用すると、ログイン時に試行する認証方式リストを 1 つまたは複数作成できます。これらのリストは、**login authentication** ライン コンフィギュレーション コマンドによって適用されます。

AAA を使用してログイン認証を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

### 手順の概要

1. Router(config)# **aaa new-model**
2. Router(config)# **aaa authentication login**{default | list-name} method1[method2...]
3. Router(config)# **line** [aux | console | tty | vty] line-number [ending-line-number]
4. Router(config-line)# **login authentication**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router(config)# <b>aaa new-model</b>	AAA をグローバルに有効にします。
ステップ 2	Router(config)# <b>aaa authentication login</b> {default   list-name} method1[method2...]	ローカルな認証リストを作成します。
ステップ 3	Router(config)# <b>line</b> [aux   console   tty   vty] line-number [ending-line-number]	認証リストを適用する回線について、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 4	Router(config-line)# <b>login authentication</b>  例 :  {default   list-name}	1 つの回線または複数回線に認証リストを適用します。

### 次のタスク

*list-name* は、作成するリストを指定するときに使用される名前です。文字列を使用できます。method 引数は、認証アルゴリズムが試行する実際の方式を指します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。すべての方式でエラーが返されても引き続き認証を行うように指定するには、コマンドラインの最後の方式として **none** を指定します。

たとえば、（この例では）TACACS+ サーバーでエラーが返されても引き続き認証を行うように指定するには、次のコマンドを入力します。

```
aaa authentication login default group tacacs+ none
```



(注) **none** キーワードを指定すると、すべてのユーザーがログイン認証に成功するため、認証のバックアップ方式としてだけ使用してください。

**login authentication** コマンドにリストが指定されていない場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状態で使用される方式を指定します。デフォルト認証方式リストは、自動的にすべてのインターフェイスに適用されます。

たとえば、ログイン時のユーザー認証のデフォルト方式としてRADIUSを指定するには、次のコマンドを入力します。

```
aaa authentication login default group radius
```

次の表に、サポートされるログイン認証方式を示します。

表 7: AAA 認証ログイン方式

キーワード	Description
<b>enable</b>	認証に有効化パスワードを使用します。
<b>krb5</b>	Kerberos 5 を認証に使用します。
<b>krb5-telnet</b>	ルータへの接続に Telnet を使用する場合、Kerberos 5 Telnet 認証プロトコルを使用します。このキーワードを選択する場合、方式リストの最初の方式としてこのキーワードを指定する必要があります。
<b>line</b>	認証にラインパスワードを使用します。
<b>local</b>	認証にローカルなユーザ名データベースを使用します。
<b>local-case</b>	認証に大文字と小文字が区別されるローカルなユーザ名を使用します。
<b>none</b>	認証を使用しません。
<b>group radius</b>	認証にすべての RADIUS サーバのリストを使用します。
<b>group tacacs+</b>	認証にすべての TACACS+ サーバのリストを使用します。
<b>group</b> <i>group-name</i>	<b>aaa group server radius</b> または <b>aaa group server tacacs+</b> コマンドで定義されているように、認証に RADIUS または TACACS+ サーバのサブセットを使用します。





- (注) **login** コマンドによって変更されるのはユーザー名および特権レベルだけであり、シェルは実行されません。したがって、**autocommand** は実行されません。この状況で **autocommand** を実行するには、Telnet セッションをルータに復帰（ループバック）させる必要があります。この方法で **autocommand** 機能を実装する場合は、ルータがセキュアな Telnet セッションを使用するように設定されていることを確認してください。

## イネーブルパスワードによるログイン認証

認証方式としてイネーブルパスワードを指定するには、**enable** 方式キーワードを指定して **aaa authentication login** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザー認証方式としてイネーブルパスワードを指定するには、次のコマンドを入力します。

```
aaa authentication login default enable
```

ログイン認証方式としてイネーブルパスワードを使用するには、イネーブルパスワードを定義しておく必要があります。イネーブルパスワードの定義の詳細については、「Configuring Passwords and Privileges」を参照してください。

## Kerberos によるログイン認証

Kerberos による認証は、他のほとんどの認証方式とは異なり、ユーザーのパスワードはリモート アクセス サーバーに送信されません。ネットワークにログインするリモート ユーザーは、ユーザー名の指定を求められます。ユーザのエントリがキー発行局（KDC）に存在する場合は、そのユーザのパスワードを含む暗号化されたチケット認可チケット（TGT）が作成され、ルータに送信されます。次に、ユーザにパスワードの入力が求められ、ルータではそのパスワードを含む TGT の復号化が試行されます。復号化に成功すると、ユーザは認証され、ルータ上にあるユーザのクレデンシャル キャッシュに TGT が保存されます。

krb5 は KINIT プログラムを使用しませんが、ルータに対して認証するために、ユーザが KINIT プログラムを実行して TGT を取得する必要はありません。これは、Cisco IOS XE の Kerberos 実装のログイン手順に KINIT が統合されているためです。

ログイン認証方式として Kerberos を指定するには、**krb5** 方式 キーワードを指定して **aaa authentication login** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザー認証方式として Kerberos を指定するには、次のコマンドを入力します。

```
aaa authentication login default krb5
```

ログイン認証方式として Kerberos を使用するには、Kerberos セキュリティ サーバーとの通信をイネーブルにしておく必要があります。Kerberos サーバーとの通信を確立する方法の詳細については、「Kerberos の設定」の章を参照してください。

## ラインパスワードによるログイン認証

ログイン認証方式としてラインパスワードを指定するには、**line** 方式キーワードを指定して **aaa authentication login** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザー認証方式としてラインパスワードを指定するには、次のコマンドを入力します。

```
aaa authentication login default line
```

ログイン認証方式としてラインパスワードを使用するには、ラインパスワードを定義しておく必要があります。ラインパスワードの定義の詳細については、「ラインパスワード保護の設定」を参照してください。

## ローカルパスワードによるログイン認証

Cisco ルータまたはアクセスサーバーが認証にローカルユーザー名データベースを使用するように指定するには、**local** 方式キーワードを指定して **aaa authentication login** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザー認証方式としてローカルユーザー名データベースを指定するには、次のコマンドを入力します。

```
aaa authentication login default local
```

ローカルユーザー名データベースにユーザを追加する方法については、「ユーザー名認証の確立」を参照してください。

## group RADIUS によるログイン認証

ログイン認証方式として RADIUS を指定するには、**group radius** 方式を指定して **aaa authentication login** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザー認証方式として RADIUS を指定するには、次のコマンドを入力します。

```
aaa authentication login default group radius
```

ログイン認証方式として RADIUS を使用するには、RADIUS セキュリティ サーバーとの通信をイネーブルにしておく必要があります。RADIUS サーバーとの通信を確立する方法の詳細については、「RADIUS の設定」の章を参照してください。

## アクセス要求での RADIUS 属性 8 の設定

**aaa authentication login** コマンドを使用して RADIUS を指定し、NAS から IP アドレスを要求するようにログインホストを設定すると、グローバル コンフィギュレーション モードで **radius-server attribute 8 include-in-access-req** コマンドを使用して、**access-request** パケットで属性 8 (Framed-IP-Address) を送信できます。このコマンドによって、ユーザー認証の前に、NAS から RADIUS サーバーに対してユーザー IP アドレスのヒントを提供できます。属性 8 の詳細については、巻末の付録「RADIUS 属性」を参照してください。

## group TACACS によるログイン認証

ログイン認証方式として TACACS+ を指定するには、**group tacacs+** 方式を指定して、**aaa authentication login** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザー認証方式として TACACS+ を指定するには、次のコマンドを入力します。

```
aaa authentication login default group tacacs+
```

ログイン認証方式として TACACS+ を使用するには、TACACS+ セキュリティ サーバーとの通信をイネーブルにしておく必要があります。TACACS+ サーバーとの通信を確立する方法の詳細については、「TACACS+ の設定」の章を参照してください。

## group group-name によるログイン認証

ログイン認証方式として使用する RADIUS または TACACS+ サーバーのサブセットを指定するには、**group group-name** 方式を指定して **aaa authentication login** コマンドを使用します。グループ名とそのグループのメンバを指定して定義するには、**aaa group server** コマンドを使用します。たとえば、**aaa group server** コマンドを使用して、**group loginrad** のメンバを最初に定義します。

```
aaa group server radius loginrad
server 172.16.2.3
server 172.16.2.17
server 172.16.2.32
```

このコマンドにより、172.16.2.3、172.16.2.17、172.16.2.32 の RADIUS サーバーがグループ **loginrad** のメンバとして指定されます。

他の方式リストが定義されていない場合にログイン時のユーザー認証方式として **group loginrad** を指定するには、次のコマンドを入力します。

```
aaa authentication login default group loginrad
```

ログイン認証方式としてグループ名を使用するには、RADIUS または TACACS+ セキュリティ サーバーとの通信をイネーブルにしておく必要があります。RADIUS サーバーとの通信を確立する方法の詳細については、「RADIUS の設定」の章を参照してください。TACACS+ サーバーとの通信を確立する方法の詳細については、「TACACS+ の設定」の章を参照してください。

## AAA を使用した PPP 認証の設定

多くのユーザは、**async** または ISDN を介したダイヤルアップでネットワーク アクセス サーバにアクセスします。**async** または ISDN を介したダイヤルアップは、CLI を完全にバイパスします。その代わりに、接続が確立するとすぐにネットワーク プロトコル (PPP や ARA など) が開始されます。

AAA セキュリティ サービスにより、PPP を実行するシリアルインターフェイスに使用できるさまざまな認証方式の実行が容易になります。**aaa authentication ppp** コマンドを使用すると、

サポートされている PPP 認証方式のいずれを使用するかに関係なく、AAA 認証が有効になります。

PPP を使用してシリアル回線に AAA 認証方式を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

手順の概要

1. Router(config)# **aaa new-model**
2. Router(config)# **aaa authentication ppp** {default | list-name} method1[method2... ]
3. Router(config)# **interface** interface-type interface-number
4. Router(config-if)# **ppp authentication** {protocol1 [protocol2... ]} [if-needed] {default | list-name} [callin] [one-time][optional]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Router(config)# <b>aaa new-model</b>	AAA をグローバルに有効にします。
ステップ 2	Router(config)# <b>aaa authentication ppp</b> {default   list-name} method1[method2... ]	ローカルな認証リストを作成します。
ステップ 3	Router(config)# <b>interface</b> interface-type interface-number	認証リストを適用するインターフェイスについて、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	Router(config-if)# <b>ppp authentication</b> {protocol1 [protocol2... ]} [if-needed] {default   list-name} [callin] [one-time][optional]	1 つの回線または複数回線に認証リストを適用します。このコマンドの protocol1 と protocol2 は、CHAP、MS-CHAP、および PAP のプロトコルを示します。PPP 認証は、まず protocol1 に指定された最初の認証方式を使用して試行されます。認証に protocol1 を使用できない場合は、次に設定されているプロトコルを使用して認証のネゴシエーションを行います。

次のタスク

**aaa authentication ppp** コマンドを使用して、PPP を介して認証を試行するときに使用する認証方式のリストを 1 つまたは複数作成します。これらのリストは、**ppp authentication** ライン コンフィギュレーション コマンドによって適用されます。

名前付きリストが **ppp authentication** コマンドに指定されていない場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用される方式を指定します。

たとえば、ユーザー認証のデフォルト方式としてローカルユーザー名データベースを指定するには、次のコマンドを入力します。

```
aaa authentication ppp default local
```

*list-name* は、作成するリストを指定するときに使用される名前です。任意の文字列を使用できます。*method* 引数は、認証アルゴリズムが試行する実際の方式を指します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。すべての方式でエラーが返されても引き続き認証を行うように指定するには、コマンドラインの最後の方式として **none** を指定します。

たとえば、（この例では）TACACS+ サーバーでエラーが返されても引き続き認証を行うように指定するには、次のコマンドを入力します。

```
aaa authentication ppp default group tacacs+ none
```



(注) **none** を指定するとすべてのユーザーが認証に成功してログインできるようになるため、認証のバックアップ方式として使用する必要があります。

次の表に、サポートされるログイン認証方式を示します。

表 8: AAA 認証 PPP 方式

キーワード	Description
<b>if-needed</b>	ユーザが TTY 回線で認証済みの場合、認証しません。
<b>krb5</b>	認証に Kerberos 5 を使用します（PAP 認証にだけ使用できます）。
<b>local</b>	認証にローカルなユーザ名データベースを使用します。
<b>local-case</b>	認証に大文字と小文字が区別されるローカルなユーザ名を使用します。
<b>none</b>	認証を使用しません。
<b>group radius</b>	認証にすべての RADIUS サーバのリストを使用します。
<b>group tacacs+</b>	認証にすべての TACACS+ サーバのリストを使用します。
<b>group group-name</b>	<b>aaa group server radius</b> または <b>aaa group server tacacs+</b> コマンドで定義されているように、認証に RADIUS または TACACS+ サーバのサブセットを使用します。

## Kerberos による PPP 認証

PPP を実行するインターフェイスで使用する認証方式として Kerberos を指定するには、**krb5** 方式キーワードを指定して **aaa authentication ppp** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にユーザー認証方式として Kerberos を指定するには、次のコマンドを入力します。

```
aaa authentication ppp default krb5
```

PPP 認証方式として Kerberos を使用するには、Kerberos セキュリティ サーバーとの通信をイネーブルにしておく必要があります。Kerberos サーバーとの通信を確立する方法の詳細については、「Kerberos の設定」の章を参照してください。



(注) Kerberos ログイン認証は、PPP PAP 認証とだけ連携します。

## ローカルパスワードによる PPP 認証

Cisco ルータまたはアクセスサーバーが認証にローカルユーザー名データベースを使用するには、方式キーワード **local** を指定して **aaa authentication ppp** コマンドを使用します。たとえば、他の方式リストが定義されていない場合に、PPP を実行する回線に使用するユーザ認証方式としてローカルユーザー名データベースを指定するには、次のコマンドを入力します。

```
aaa authentication ppp default local
```

ローカルユーザー名データベースにユーザを追加する方法については、「ユーザ名認証の確立」を参照してください。

## group RADIUS による PPP 認証

ログイン認証方式として RADIUS を指定するには、**group radius** 方式を指定して **aaa authentication ppp** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザー認証方式として RADIUS を指定するには、次のコマンドを入力します。

```
aaa authentication ppp default group radius
```

PPP 認証方式として RADIUS を使用するには、RADIUS セキュリティ サーバーとの通信をイネーブルにしておく必要があります。RADIUS サーバーとの通信を確立する方法の詳細については、「RADIUS の設定」の章を参照してください。

## アクセス要求での RADIUS 属性 44 の設定

**group radius** 方式で **aaa authentication ppp** コマンドを使用して、ログイン認証方式として RADIUS を指定した後、グローバル コンフィギュレーション モードで **radius-server attribute 44 include-in-access-req** コマンドを使用して、アクセス要求パケットで属性 44 (Acct-Session-ID) を送信するようにデバイスを設定できます。このコマンドによって、RADIUS デーモンはコールを開始から終了まで追跡できます。

## group TACACS による PPP 認証

ログイン認証方式として TACACS+ を指定するには、**group tacacs+** 方式を指定して、**aaa authentication ppp** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザー認証方式として TACACS+ を指定するには、次のコマンドを入力します。

```
aaa authentication ppp default group tacacs+
```

PPP 認証方式として TACACS+ を使用するには、TACACS+ セキュリティ サーバーとの通信をイネーブルにしておく必要があります。TACACS+ サーバーとの通信を確立する方法の詳細については、「TACACS+ の設定」の章を参照してください。

## group group-name による PPP 認証

ログイン認証方式として使用する RADIUS または TACACS+ サーバーのサブセットを指定するには、**group group-name** 方式を指定して **aaa authentication ppp** コマンドを使用します。グループ名とそのグループのメンバを指定して定義するには、**aaa group server** コマンドを使用します。たとえば、**aaa group server** コマンドを使用して、**group ppprad** のメンバを最初に定義します。

```
aaa group server radius ppprad
server 172.16.2.3
server 172.16.2.17
server 172.16.2.32
```

このコマンドにより、172.16.2.3、172.16.2.17、172.16.2.32 の RADIUS サーバーがグループ **ppprad** のメンバとして指定されます。

他の方式リストが定義されていない場合にログイン時のユーザー認証方式として **group ppprad** を指定するには、次のコマンドを入力します。

```
aaa authentication ppp default group ppprad
```

PPP 認証方式としてグループ名を使用するには、RADIUS または TACACS+ セキュリティ サーバーとの通信をイネーブルにしておく必要があります。RADIUS サーバーとの通信を確立する方法の詳細については、「RADIUS の設定」の章を参照してください。TACACS+ サーバーとの通信を確立する方法の詳細については、「TACACS+ の設定」の章を参照してください。

## PPP 要求に対する AAA スケーラビリティの設定

ネットワークアクセスサーバー (NAS) の PPP マネージャによって割り当てられた複数のバックグラウンドプロセスを設定およびモニターして、AAA 認証要求と認可要求に対応できます。AAA スケーラビリティ機能によって、PPP に対する AAA 要求を処理するために使用される複数のプロセスを設定できるようになります。つまり、同時に認証または認可できるユーザー数が増えます。

PPP に対する AAA 要求を処理するために、特定の数のバックグラウンドプロセスを割り当てるには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router (config) # <b>aaa processes</b> <i>number</i>	PPP に対する AAA 認証要求および認可要求を処理するために、特定の数のバックグラウンドプロセスを割り当てます。

引数 *number* には、PPP に対する AAA 認証要求と認可要求を処理するために確保するバックグラウンドプロセス数を定義します。また、1 ~ 2147483647 の任意の値を設定できます。PPP マネージャが PPP に対する要求を処理する方法のため、この引数には、同時に認証できる新規ユーザーの数も定義します。この引数は、いつでも増減できます。



(注) 追加バックグラウンドプロセスの割り当ては、コストが高くなる可能性があります。PPP に対する AAA 要求を処理できるバックグラウンドプロセスの最小数を設定してください。

## AAA を使用した ARAP 認証の設定

**aaa authentication arap** コマンドを使用して、AppleTalk Remote Access Protocol (ARAP) ユーザーがデバイスにログインを試行するときに使用する認証方式のリストを1つまたは複数作成できます。これらのリストは、**arap authentication** ラインコンフィギュレーションコマンドで使用されます。

グローバル コンフィギュレーション モードで次のコマンドを使用します。

### 手順の概要

1. Device(config)# **aaa new-model**
2. Device(config)# **aaa authentication arap**
3. Device(config)# **line number**
4. Device(config-line)# **autoselect arap**
5. Device(config-line)# **autoselect during-login**
6. Device(config-line)# **arap authentication list-name**
7. Device(config-line)# **end**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Device(config)# <b>aaa new-model</b>	AAA をグローバルに有効にします。
ステップ 2	Device(config)# <b>aaa authentication arap</b> 例： ARAP ユーザーに対する認証をイネーブルにします。	
ステップ 3	Device(config)# <b>line number</b>	(任意) ライン コンフィギュレーション モードに変更します。
ステップ 4	Device(config-line)# <b>autoselect arap</b>	(任意) ARAP の自動選択をイネーブルにします。
ステップ 5	Device(config-line)# <b>autoselect during-login</b>	(任意) ユーザー ログイン時に ARAP セッションを自動的に開始します。



	コマンドまたはアクション	目的
ステップ 6	Device(config-line)# <b>arap authentication</b> <i>list-name</i>	(任意 : <b>default</b> が <b>aaa authentication arap</b> コマンドに使用されている場合は不要) 回線上の ARAP に対する TACACS+ 認証を有効にします。
ステップ 7	Device(config-line)# <b>end</b>	特権 EXEC モードに戻ります。

### 次のタスク

*list-name* は、作成するリストを指定するときに使用される名前です。任意の文字列を使用できます。*method* 引数は、認証アルゴリズムが試行する方式の実際のリストを指します。試行は入力されている順序で行われます。

名前付きリストが **arap authentication** コマンドに指定されていない場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用される方式を指定します。

追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。すべての方式でエラーが返されても引き続き認証を行うように指定するには、コマンドラインの最後の方式として **none** を指定します。



(注) **none** を指定するとすべてのユーザーのログインが認証されるようになるため、認証のバックアップ方式として使用する必要があります。

次の表に、サポートされるログイン認証方式を示します。

表 9: AAA 認証 ARAP 方式

キーワード	Description
<b>auth-guest</b>	ユーザが EXEC モードにログイン済みの場合にだけ、ゲストログインを許可します。
<b>guest</b>	ゲストログインを許可します。
<b>line</b>	認証にラインパスワードを使用します。
<b>local</b>	認証にローカルなユーザ名データベースを使用します。
<b>local-case</b>	認証に大文字と小文字が区別されるローカルなユーザ名を使用します。
<b>group radius</b>	認証にすべての RADIUS サーバのリストを使用します。
<b>group tacacs+</b>	認証にすべての TACACS+ サーバのリストを使用します。

キーワード	Description
<b>group</b> <i>group-name</i>	<b>aaa group server radius</b> または <b>aaa group server tacacs+</b> コマンドで定義されているように、認証に RADIUS または TACACS+ サーバーのサブセットを使用します。

たとえば、ARAP とともに使用するデフォルトの AAA 認証方式リストを作成するには、次のコマンドを使用します。

```
aaa authentication arap default if-needed none
```

ARAP に同じ認証方式リストを作成し、リストに *MIS-access* と名前を付けるには、次のコマンドを入力します。

```
aaa authentication arap MIS-access if-needed none
```

ここでは、次の内容について説明します。

## 認可済みゲスト ログインを許可する ARAP 認証

ユーザーが EXEC に正常にログイン済みの場合にだけ、ゲストログインを許可するには、**auth-guest** キーワードを指定して **aaa authentication arap** コマンドを使用します。この方式は ARAP 認証方式リストの先頭に指定する必要がありますが、この方式が成功しなかった場合は引き続き他の方式を試行できます。たとえば、認証のデフォルト方式として、すべての認可済みゲストログイン（つまり、EXEC にログイン済みのユーザーによるログイン）を許可し、その方式が失敗した場合にだけ RADIUS を使用するには、次のコマンドを入力します。

```
aaa authentication arap default auth-guest group radius
```



- (注) AAA を初期化すると、デフォルトで ARAP によるゲストログインはディセーブルになります。ゲストログインを許可するには、**guest** キーワードまたは **auth-guest** キーワードを指定して **aaa authentication arap** コマンドを使用する必要があります。

## ゲスト ログインを許可する ARAP 認証

ゲストログインを許可するには、**guest** キーワードを指定して **aaa authentication arap** コマンドを使用します。この方式は ARAP 認証方式リストの先頭に指定する必要がありますが、この方式が成功しなかった場合は引き続き他の方式を試行できます。たとえば、認証のデフォルト方式としてすべてのゲストログインを許可し、その方式が失敗した場合にだけ RADIUS を使用するには、次のコマンドを入力します。

```
aaa authentication arap default guest group radius
```

## ラインパスワードによる ARAP 認証

認証方式としてラインパスワードを指定するには、方式キーワード **line** を指定して **aaa authentication arap** コマンドを使用します。たとえば、他の方式リストが定義されていない場合に、ARAP ユーザー認証方式としてラインパスワードを指定するには、次のコマンドを入力します。

```
aaa authentication arap default line
```

ARAP 認証方式としてラインパスワードを使用するには、ラインパスワードを定義しておく必要があります。ラインパスワードの定義の詳細については、この章の「ラインパスワード保護の設定」を参照してください。

## ローカルパスワードによる ARAP 認証

Cisco ルータまたはアクセスサーバーが認証にローカルユーザー名データベースを使用するように指定するには、方式キーワード **local** を指定して **aaa authentication arap** コマンドを使用します。たとえば、他の方式リストが定義されていない場合に、ARAP ユーザー認証方式としてローカルユーザー名データベースを指定するには、次のコマンドを入力します。

```
aaa authentication arap default local
```

ローカルユーザー名データベースにユーザを追加する方法については、「ユーザ名認証の確立」を参照してください。

## group RADIUS による ARAP 認証

NAS 認証方式として RADIUS を指定するには、**group radius** 方式を指定して **aaa authentication arap** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザー認証方式として RADIUS を指定するには、次のコマンドを入力します。

```
aaa authentication arap default group radius
```

ARAP 認証方式として RADIUS を使用する前に、RADIUS セキュリティ サーバーとの通信をイネーブルにしておく必要があります。RADIUS サーバーとの通信を確立する方法の詳細については、「RADIUS の設定」の章を参照してください。

## group TACACS による ARAP 認証

ARAP 認証方式として TACACS+ を指定するには、**group tacacs+** 方式を指定して、**aaa authentication arap** コマンドを使用します。たとえば、他の方式リストが定義されていない場合にログイン時のユーザー認証方式として TACACS+ を指定するには、次のコマンドを入力します。

```
aaa authentication arap default group tacacs+
```

ARAP 認証方式として TACACS+ を使用するには、TACACS+ セキュリティ サーバーとの通信をイネーブルにしておく必要があります。TACACS+ サーバーとの通信を確立する方法の詳細については、「TACACS+ の設定」の章を参照してください。

## group group-name による ARAP 認証

ARAP 認証方式として使用する RADIUS または TACACS+ サーバーのサブセットを指定するには、**group group-name** 方式を指定して **aaa authentication arap** コマンドを使用します。グループ名とそのグループのメンバを指定して定義するには、**aaa group server** コマンドを使用します。たとえば、**aaa group server** コマンドを使用して、**group araprad** のメンバを最初に定義します。

```
aaa group server radius araprad
server 172.16.2.3
server 172.16.2.17
server 172.16.2.32
```

このコマンドにより、172.16.2.3、172.16.2.17、172.16.2.32 の RADIUS サーバーがグループ **araprad** のメンバとして指定されます。

他の方式リストが定義されていない場合にログイン時のユーザー認証方式として **group araprad** を指定するには、次のコマンドを入力します。

```
aaa authentication arap default group araprad
```

ARAP 認証方式としてグループ名を使用するには、RADIUS または TACACS+ セキュリティサーバーとの通信をイネーブルにしておく必要があります。RADIUS サーバーとの通信を確立する方法の詳細については、「RADIUS の設定」の章を参照してください。TACACS+ サーバーとの通信を確立する方法の詳細については、「TACACS+ の設定」の章を参照してください。

## AAA を使用した NASI 認証の設定

**aaa authentication nasi** コマンドを使用して、NetWare Asynchronous Services Interface (NASI) ユーザーがデバイスにログインを試行するときに使用する認証方式のリストを1つまたは複数作成できます。これらのリストは、**nasi authentication line** コンフィギュレーション コマンドで使用されます。

AAA を使用して NASI 認証を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

### 手順の概要

1. Device(config)# **aaa new-model**
2. Device(config)# **aaa authentication nasi**
3. Device(config)# **line number**
4. Device(config-line)# **nasi authentication list-name**
5. Device(config-line)# **end**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Device(config)# <b>aaa new-model</b>	AAA をグローバルに有効にします。

	コマンドまたはアクション	目的
ステップ 2	Device(config)# <b>aaa authentication nasi</b> 例 :	NASI ユーザーに対する認証をイネーブルにします。
ステップ 3	Device(config)# <i>line number</i>	(任意 : <b>default</b> が <b>aaa authentication nasi</b> コマンドに使用されている場合は不要) 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 4	Device(config-line)# <b>nasi authentication list-name</b>	(任意 : <b>default</b> が <b>aaa authentication nasi</b> コマンドに使用されている場合は不要) 回線上の NASI に対する TACACS+ 認証を有効にします。
ステップ 5	Device(config-line)# <b>end</b>	特権 EXEC モードに戻ります。

### 次のタスク

*list-name* は、作成するリストを指定するときに使用される名前です。任意の文字列を使用できます。*method* 引数は、認証アルゴリズムが試行する方式の実際のリストを指します。試行は入力されている順序で行われます。

**aaa authentication nasi** コマンドに名前付きリストが指定されていない場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用される方式を指定します。

追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。すべての方式でエラーが返されても引き続き認証を行うように指定するには、コマンドラインの最後の方式として **none** を指定します。



- (注) **none** を指定するとすべてのユーザーのログインが認証されるようになるため、認証のバックアップ方式として使用する必要があります。

次の表に、サポートされる NASI 認証方式を示します。

表 10: AAA 認証 NASI 方式

キーワード	Description
<b>enable</b>	認証にイネーブルパスワードを使用します。
<b>line</b>	認証にラインパスワードを使用します。
<b>local</b>	認証にローカルなユーザ名データベースを使用します。
<b>local-case</b>	認証に大文字と小文字が区別されるローカルなユーザ名を使用します。
<b>none</b>	認証を使用しません。

キーワード	Description
<b>group radius</b>	認証にすべての RADIUS サーバのリストを使用します。
<b>group tacacs+</b>	認証にすべての TACACS+ サーバのリストを使用します。
<b>group</b> <i>group-name</i>	<b>aaa group server radius</b> または <b>aaa group server tacacs+</b> コマンドで定義されているように、認証に RADIUS または TACACS+ サーバのサブセットを使用します。

## イネーブルパスワードによる NASI 認証

認証方式としてイネーブルパスワードを指定するには、キーワード **enable** を指定して **aaa authentication nasi** コマンドを使用します。たとえば、他の方式リストが定義されていない場合に、NASI ユーザー認証方式としてイネーブルパスワードを指定するには、次のコマンドを使用します。

```
aaa authentication nasi default enable
```

認証方式としてイネーブルパスワードを使用するには、イネーブルパスワードを定義しておく必要があります。イネーブルパスワードの定義の詳細については、「Configuring Passwords and Privileges」を参照してください。

## ラインパスワードによる NASI 認証

認証方式としてラインパスワードを指定するには、方式キーワード **line** を指定して **aaa authentication nasi** コマンドを使用します。たとえば、他の方式リストが定義されていない場合に、NASI ユーザー認証方式としてラインパスワードを指定するには、次のコマンドを入力します。

```
aaa authentication nasi default line
```

NASI 認証方式としてラインパスワードを使用するには、ラインパスワードを定義しておく必要があります。ラインパスワードの定義の詳細については、「ラインパスワード保護の設定」を参照してください。

## ローカルパスワードによる NASI 認証

Cisco ルータまたはアクセスサーバが認証情報にローカルユーザー名データベースを使用するように指定するには、方式キーワード **local** を指定して **aaa authentication nasi** コマンドを使用します。たとえば、他の方式リストが定義されていない場合に、NASI ユーザー認証方式としてローカルユーザー名データベースを指定するには、次のコマンドを入力します。

```
aaa authentication nasi default local
```

ローカルユーザー名データベースにユーザを追加する方法については、「ユーザ名認証の確立」を参照してください。

## group RADIUS による NASI 認証

NASI 認証方式として RADIUS を指定するには **group radius** 方式を指定して **aaa authentication nasi** コマンドを使用します。たとえば、他の方式リストが定義されていない場合に、NASI ユーザー認証方式として RADIUS を指定するには、次のコマンドを入力します。

```
aaa authentication nasi default group radius
```

NASI 認証方式として RADIUS を使用するには、RADIUS セキュリティ サーバーとの通信をイネーブルにしておく必要があります。RADIUS サーバーとの通信を確立する方法の詳細については、「RADIUS の設定」の章を参照してください。

## group TACACS による NASI 認証

NASI 認証方式として TACACS+ を指定するには、**group tacacs+** 方式キーワードを指定して **aaa authentication nasi** コマンドを使用します。たとえば、他の方式リストが定義されていない場合に、NASI ユーザー認証方式として TACACS+ を指定するには、次のコマンドを入力します。

```
aaa authentication nasi default group tacacs+
```

認証方式として TACACS+ を使用するには、TACACS+ セキュリティ サーバーとの通信をイネーブルにしておく必要があります。TACACS+ サーバーとの通信を確立する方法の詳細については、「TACACS+ の設定」の章を参照してください。

## group group-name による NASI 認証

NASI 認証方式として使用する RADIUS または TACACS+ サーバーのサブセットを指定するには、**group group-name** 方式を指定して **aaa authentication nasi** コマンドを使用します。グループ名とそのグループのメンバを指定して定義するには、**aaa group server** コマンドを使用します。たとえば、**aaa group server** コマンドを使用して、**group nasirad** のメンバを最初に定義します。

```
aaa group server radius nasirad
server 172.16.2.3
server 172.16.2.17
server 172.16.2.32
```

このコマンドにより、172.16.2.3、172.16.2.17、172.16.2.32 の RADIUS サーバーがグループ **nasirad** のメンバとして指定されます。

他の方式リストが定義されていない場合にログイン時のユーザー認証方式として **group nasirad** を指定するには、次のコマンドを入力します。

```
aaa authentication nasi default group nasirad
```

NASI 認証方式としてグループ名を使用するには、RADIUS または TACACS+ セキュリティ サーバーとの通信をイネーブルにしておく必要があります。RADIUS サーバーとの通信を確立する方法の詳細については、「RADIUS の設定」の章を参照してください。TACACS+ サーバーとの通信を確立する方法の詳細については、「TACACS+ の設定」の章を参照してください。

## ログイン入力にかかる時間の指定

**timeout login response** コマンドを使用すると、ログイン入力（ユーザー名やパスワードなど）がタイムアウトするまでの待機時間を指定できます。デフォルトのログイン値は 30 秒です。  
**timeout login response** コマンドを使用して、1 ~ 300 秒のタイムアウト値を指定できます。30 秒というデフォルトのログインタイムアウト値を変更するには、ラインコンフィギュレーションモードで次のコマンドを使用します。

コマンド	目的
Router(config-line)# <b>timeout login response</b> seconds	タイムアウトまでログイン情報を待機する時間を指定します。

## 特権レベルでのパスワード保護のイネーブル化

ユーザーが特権 EXEC コマンドレベルにアクセスできるかどうかを判断するときに使用する一連の認証方式を作成するには、**aaa authentication enable default** コマンドを使用します。最大 4 つの認証方式を指定できます。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。すべての方式でエラーが返されても引き続き認証を行うように指定するには、コマンドラインの最後の方式として **none** を指定します。

グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router(config)# <b>aaa authentication enable default</b> method1 [method2...]	特権 EXEC レベルを要求するユーザに対して、ユーザ ID とパスワードのチェックをイネーブルにします。  (注) ルータから RADIUS サーバーに送信されたすべての <b>aaa authentication enable default</b> 要求には、ユーザー名「\$enab15\$」が含まれます。TACACS+ サーバに送信された要求にはログイン認証用に入力されたユーザ名が含まれます。

メソッド引数は、認証アルゴリズムが試行した方式の実際のリストを入力された順に参照します。次の表は、サポートされているイネーブル認証方式を示します。

表 11: AAA 認証イネーブル デフォルト方式

キーワード	Description
<b>enable</b>	認証にイネーブルパスワードを使用します。
<b>line</b>	認証にラインパスワードを使用します。
<b>none</b>	認証を使用しません。



キーワード	Description
<b>group radius</b>	認証にすべての RADIUS ホストのリストを使用します。 (注) RADIUS 方式は、ユーザ名別では機能しません。
<b>group tacacs+</b>	認証にすべての TACACS+ ホストのリストを使用します。
<b>group</b> <i>group-name</i>	<b>aaa group server radius</b> または <b>aaa group server tacacs+</b> コマンドで定義されているように、認証に RADIUS または TACACS+ サーバーのサブセットを使用します。

## パスワードプロンプトに表示するテキストの変更

Cisco IOS XE ソフトウェアからユーザーに対してパスワードの入力を求めるときに表示されるデフォルトテキストを変更するには、**aaa authentication password-prompt** コマンドを使用します。このコマンドによって、イネーブルパスワードと、リモートセキュリティサーバーから提供されていないログインパスワードのパスワードプロンプトが変更されます。このコマンドの **no** 形式を使用すると、パスワードプロンプトが次のデフォルト値に戻ります。

Password:

**aaa authentication password-prompt** コマンドでは、リモートの TACACS+ サーバーまたは RADIUS サーバーから提供されるダイアログは変更されません。

**aaa authentication password-prompt** コマンドは、RADIUS をログイン方式として使用するときには機能します。RADIUS サーバに到達不能の場合でも、コマンドで定義されたパスワードプロンプトが表示されます。**aaa authentication password-prompt** コマンドは、TACACS+ と併用できません。TACACS+ は、NAS に対して、ユーザに表示するパスワードプロンプトを提供します。TACACS+ サーバが到達可能な場合、NAS はそのサーバからパスワードプロンプトを受け取り、**aaa authentication password-prompt** コマンドで定義したプロンプトではなく、受け取ったプロンプトを使用します。TACACS+ サーバが到達不能の場合、**aaa authentication password-prompt** コマンドで定義したパスワードプロンプトが使用される可能性があります。

グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Router (config) # <b>aaa authentication password-prompt</b> <i>text-string</i>	ユーザにパスワードの入力を求めるときに表示するデフォルトテキストを変更します。

■ ユーザー名が空のアクセス要求が RADIUS サーバーに送信されないようにする

## ユーザー名が空のアクセス要求が RADIUS サーバーに送信されないようにする

次の設定手順では、ユーザー名が空のアクセス要求が RADIUS サーバーに送信されないようにする方法について説明します。この機能により、RADIUS サーバーとの不要なやりとりを回避でき、RADIUS ログの量を少なくすることができます。



(注) **aaa authentication suppress null-username** コマンドを開始できるのは、Cisco IOS XE Release 2.4 です。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication suppress null-username**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	<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 3	<b>aaa new-model</b> 例： Device(config)# configure terminal	AAA をグローバルに有効にします。
ステップ 4	<b>aaa authentication suppress null-username</b> 例： Device(config)# aaa authentication suppress null-username	ユーザー名が空のアクセス要求が RADIUS サーバーに送信されないようにします。

## AAA 認証のメッセージ バナーの設定

AAA は、設定可能でパーソナライズされたログインおよび failed-login バナーの使用をサポートします。ユーザーが AAA を使用して認証を受けるシステムにログインする場合、および何らかの理由で認証が失敗した場合に表示されるメッセージ バナーを設定できます。

### ログイン バナーの設定

ユーザーがログインするときに表示されるメッセージを設定する（デフォルトのログインメッセージを置き換える）には、次のタスクを実行します。

#### 始める前に

ログイン バナーを作成するには、デリミタを設定する必要があります。設定することで、続くテキスト文字列をバナーとして表示する必要があることがシステムに通知されます。次に、テキスト文字列自体を設定する必要があります。デリミタは、バナーの末尾を示すために、テキスト スtring の末尾で繰り返されます。デリミタには、拡張 ASCII 文字セットの任意の 1 文字を使用できます。ただし、デリミタとして定義した文字は、バナー用のテキスト文字列には使用できません。

#### 手順の概要

1. **aaa new-model** Device(config)# **aaa new-model**
2. Device(config)# **aaa authentication banner** *delimiter string delimiter*
3. Device(config)# **end**

#### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>aaa new-model</b> Device(config)# <b>aaa new-model</b>	AAA をイネーブルにします。
ステップ 2	Device(config)# <b>aaa authentication banner</b> <i>delimiter string delimiter</i>	パーソナライズされたログイン バナーを作成します。
ステップ 3	Device(config)# <b>end</b>	特権 EXEC モードに戻ります。

#### 次のタスク

ログイン バナーの設定後、まだ実行していない場合は、AAA を使用した認証の基本設定を完了する必要があります。さまざまな、使用可能な AAA 認証の詳細については、『認証、許可、アカウントिंग コンフィギュレーション ガイド』の「認証の設定」を参照してください。

### Failed-Login バナーの設定

ユーザーログインが失敗したときに表示されるメッセージを設定する（デフォルトの failed-login メッセージを置き換える）には、次のタスクを実行します。

### 始める前に

failed-login バナーを作成するには、デリミタを設定する必要があります。設定することで、続くテキスト文字列をバナーとして表示する必要があることがシステムに通知されます。次に、テキスト文字列自体を設定する必要があります。デリミタは、failed-login バナーの末尾を示すために、テキストストリングの末尾で繰り返されます。デリミタには、拡張 ASCII 文字セットの任意の 1 文字を使用できます。ただし、デリミタとして定義した文字は、バナーを構成するテキストストリングには使用できません。

### 手順の概要

1. Device(config)# **aaa new-model**
2. Device(config)# **aaa authentication fail-message delimiter string delimiter**
3. Device(config)# **end**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Device(config)# <b>aaa new-model</b>	AAA をイネーブルにします。
ステップ 2	Device(config)# <b>aaa authentication fail-message delimiter string delimiter</b>	ユーザーログインが失敗したときに表示されるメッセージを作成します。
ステップ 3	Device(config)# <b>end</b>	特権 EXEC モードに戻ります。

### 次のタスク

failed-login バナーの設定後、まだ実行していない場合は、AAA を使用した認証の基本設定を完了する必要があります。さまざまな、使用可能な AAA 認証の詳細については、『認証、許可、アカウントिंग コンフィギュレーションガイド』の「認証の設定」を参照してください。

## AAA パケットオブディスコネクトの設定

特定のセッション属性が指定された場合、パケットオブディスコネクト (POD) によってネットワークアクセスサーバー (NAS) の接続が終了されます。UNIX ワークステーション上にある POD クライアントでは、AAA から取得したセッション情報を使用して、ネットワークアクセスサーバーで実行されている POD サーバーに接続解除パケットを送信します。NAS では、1 つまたは複数の一致するキー属性を含む任意の着信ユーザーセッションを終了します。必要なフィールドがない場合、または完全一致が見つからない場合、要求は拒否されます。

POD を設定するには、グローバルコンフィギュレーションモードで次のタスクを実行します。

### 手順の概要

1. Device(config)# **aaa accounting network default**
2. Device(config)# **aaa accounting delay-start**

3. Device(config)# **aaa pod server server-keystring**
4. Device(config)# **radius-server host IP addressnon-standard**

#### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Device(config)# <b>aaa accounting network default</b>  例 :  <b>start-stop radius</b>	AAA アカウンティング レコードをイネーブルにします。
ステップ 2	Device(config)# <b>aaa accounting delay-start</b>	(任意) POD パケットで使用できるように、Framed-IP-Address が割り当てられるまで、開始アカウンティング レコードの生成を遅延します。
ステップ 3	Device(config)# <b>aaa pod server server-keystring</b>	POD の受信イネーブルにします。
ステップ 4	Device(config)# <b>radius-server host IP addressnon-standard</b>	RADIUS のベンダー固有バージョンを使用する RADIUS ホストを宣言します。

## 二重認証のイネーブル化

シスコのリリースによっては、PPP セッションの認証には、PAP または CHAP のどちらか 1 つの認証方法しか使用できないことがあります。二重認証方式の場合、ネットワークアクセス権を得るには、リモートユーザーが (CHAP または PAP 認証後に) 認証の第 2 段階に合格する必要があります。

この第 2 段階 (「二重」) の認証には、ユーザーがパスワードを知っている必要がありますが、ユーザーのリモートホストにパスワードは保存されません。そのため、第 2 段階の認証は、ホストではなくユーザーに固有です。その結果、リモートホストから情報が盗まれた場合でも有効な、追加のセキュリティレベルが実現します。さらに、ユーザー別にネットワーク特権をカスタマイズできるため、柔軟性も高くなります。

第 2 段階の認証には、CHAP ではサポートされないトークンカードなど、ワンタイムパスワードを使用できます。ワンタイムパスワードを使用している場合、ユーザーパスワードが盗まれても盗用者の役に立ちません。

### 二重認証の機能

二重認証を使用する場合、2 つの認証/認可段階があります。この 2 つの段階は、リモートユーザーがダイヤルインした後、および PPP セッションが開始された後に発生します。

第 1 段階では、ユーザーがリモートホスト名を使用してログインして CHAP (または PAP) がリモートホストを認証し、次に PPP が AAA とネゴシエートしてリモートホストを認可しま

す。このプロセスで、リモート ホストに関連付けられたネットワーク アクセス特権は、そのユーザーに関連付けられます。



(注) ローカル ホストに対して Telnet 接続だけを許可するように、この第 1 段階ではネットワーク管理者が認可を制限することを推奨します。

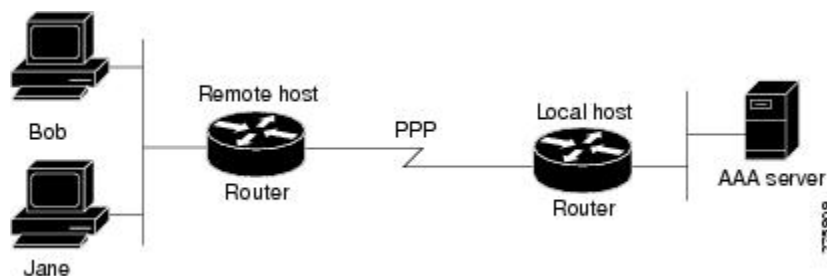
第 2 段階では、リモート ユーザーが、認証を受けるネットワーク アクセス サーバーに対して Telnet を送信する必要があります。リモート ユーザーがログインする場合、AAA ログイン認証を使用してユーザーを認証する必要があります。次に、AAA を使用して再度許可を受けるために、**access-profile** コマンドを入力する必要があります。この認可が完了すると、ユーザーは二重に認証され、ユーザー別のネットワーク特権に従ってネットワークにアクセスできるようになります。

システム管理者は、セキュリティサーバーで適切なパラメータを設定することで、各認証段階の後にリモート ユーザーが保持するネットワーク特権を決定します。二重認証を使用するには、**access-profile** コマンドを発行してアクティブ化する必要があります。



**注意** 複数のホストがネットワーク アクセス サーバーに対して PPP 接続を共有する場合、二重認証によって望ましくない状況が発生することがあります (次の図を参照)。まず、ユーザー Bob が PPP セッションを開始し、ネットワーク アクセス サーバーで二重認証をアクティブにした場合 (次の図を参照)、Bob の PPP セッションが期限切れになるまで、他のすべてのユーザーは Bob と同じネットワーク特権を持つこととなります。この問題が発生するのは、PPP セッション時に Bob の認可プロファイルがネットワーク アクセス サーバーのインターフェイスに適用され、他のユーザーからの PPP トラフィックに Bob が確立した PPP セッションが使用されるためです。第 2 に、Bob が PPP セッションを開始して二重認証をアクティブにし、(Bob の PPP セッションが期限切れになる前に) 別のユーザー Jane が **access-profile** コマンドを実行する場合 (または、Jane がネットワーク アクセス サーバーに Telnet を送信し、**autocommand access-profile** が実行された場合)、再度許可が発生し、Jane の許可プロファイルがインターフェイスに適用され、Bob のプロファイルは置換されます。その結果、Bob の PPP トラフィックの不通や中止が発生することや、Bob が本来は持っていないレベルの特権が Bob に付与されることがあります。

図 2: 危険性を伴うトポロジ : 複数のホストがネットワーク アクセス サーバーに対する PPP 接続を共有



## 二重認証の設定

二重認証を設定するには、次の手順を実行します。

1. **aaa-new model** グローバル コンフィギュレーション コマンドを使用して、AAA を有効にします。AAA をイネーブルにする方法の詳細については、「AAA Overview」を参照してください。
2. **aaa authentication** コマンドを使用して、ログインおよびPPP 認証方式リストを使用するようにネットワークアクセスサーバーを設定します。次に、これらの方式リストを適切な回線やインターフェイスに適用します。
3. **aaa authorization** コマンドを使用して、ログイン時の AAA ネットワーク許可を設定します。ネットワーク認可の設定の詳細については、「認可の設定」の章を参照してください。
4. セキュリティプロトコルパラメータ（たとえば、RADIUS または TACACS+）を設定します。RADIUS の詳細については、「Configuring RADIUS」の章を参照してください。TACACS+ の詳細については、「Configuring TACACS+」の章を参照してください。
5. セキュリティサーバーで、ユーザーがローカルホストに接続できるアクセスコントロールリストの AV ペアを使用するには、Telnet 接続を確立する必要があります。
6. （任意）autocommand として **access-profile** コマンドを設定します。autocommand を設定すると、リモートユーザーは、個人のユーザープロファイルに関連付けられた許可済み権限にアクセスするために、手動で **access-profile** コマンドを入力する必要はなくなります。



- (注) **access-profile** コマンドが autocommand として設定されている場合でも、二重認証を完了するには、ユーザーがローカルホストに Telnet を送信し、ログインする必要があります。

ユーザー固有の許可ステートメントを作成する場合、次の規則に従います（これらの規則は、**access-profile** コマンドのデフォルトの動作に関連します）。

- セキュリティサーバーでアクセスコントロールリストの AV ペアを設定する場合、有効な AV ペアを使用します。
- リモートユーザーがインターフェイスの既存の認可（第2段階の認証/認可の前に存在する認可）を使用し、異なるアクセスコントロールリスト（ACL）を持つようにするには、ユーザー固有の認可定義で ACL AV ペアだけを指定します。この方法は、デフォルトの認可プロファイルを設定してリモートホストに適用し、ACL はユーザー別に適用する場合などに有効です。
- これらのユーザー固有の許可ステートメントを後でインターフェイスに適用すると、ユーザーの許可に使用する **access-profile** コマンドの実行形式によって、既存のインターフェイス設定に追加することや、既存のインターフェイス設定を置き換えることができます。許可ステートメントを設定する前に、**access-profile** コマンドの機能について理解する必要があります。

- ISDN または Multilink PPP を使用する予定がある場合、ローカルホストで仮想テンプレートも設定する必要があります。

二重認証に関する問題を解決するには、**debug aaa per-user** デバッグコマンドを使用します。このコマンドの詳細については、『Cisco IOS Debug Command Reference』を参照してください。

## 二重認証後のユーザー プロファイルへのアクセス

二重認証で、リモートユーザーがローカルホスト名を使用してローカルホストに対する PPP リンクを確立すると、リモートホストは CHAP (または PAP) 認証されます。CHAP (または PAP) 認証後、PPP は AAA とネゴシエートして、リモートホストに関連付けられたネットワークアクセス特権をユーザーに割り当てます (この段階の特権では、ユーザーがローカルホストに接続するには Telnet 接続を必須にするという制限を付けることを推奨します)。

ユーザーが二重認証の第 2 段階を開始する必要があり、ローカルホストに対して Telnet 接続を確立する場合、ユーザーは個人のユーザー名とパスワード (CHAP または PAP のユーザー名とパスワードとは異なります) を入力します。この処理の結果、個人のユーザー名/パスワードに従って AAA 認証が発生します。ただし、ローカルホストに関連付けられた初期の権限が有効です。ローカルホストに関連付けられた権限は、**access-profile** コマンドを使用して、ユーザープロファイルのユーザー用に定義されている権限で置き換えられるか、結合されます。

二重認証後にユーザープロファイルにアクセスするには、EXEC コンフィギュレーションモードで次のコマンドを使用します。

コマンド	目的
Router> <b>access-profile [merge   replace] [ignore-sanity-checks]</b>	二重認証後に、ユーザに関連付けられた権限にアクセスします。

autocommand として実行するように **access-profile** コマンドを設定した場合、リモートユーザーのログイン後に自動的に実行されます。

## 自動二重認証のイネーブル化

自動二重認証を実装することで、ユーザーにとって二重認証プロセスが容易になります。自動二重認証は、二重認証が持つセキュリティ上の利点をすべて備えています。リモートユーザーにとってよりシンプルでユーザーフレンドリなインターフェイスです。二重認証の場合、ユーザー認証の第 2 レベルは、ユーザーがネットワークアクセスサーバーまたはルータに Telnet に送信し、ユーザー名とパスワードを入力したときに完了します。自動二重認証の場合、ユーザーがネットワークアクセスサーバーに Telnet を送信する必要はありません。その代わりに、ユーザー名とパスワードまたは Personal Identification Number (PIN) の入力を求めるダイアログボックスが表示されます。自動二重認証機能を使用するには、対応するクライアントアプリケーションがリモートユーザーホストで実行されている必要があります。





- (注) 自動二重認証は、既存の二重認証機能と同様に、Multilink PPP ISDN 接続専用です。自動二重認証は、X.25 や SLIP など他のプロトコルとは併用できません。

自動二重認証は、既存の二重認証機能の強化です。自動二重認証を設定するには、まず次の手順を実行して二重認証を設定する必要があります。

1. **aaa-new model** グローバル コンフィギュレーション コマンドを使用して、AAA を有効にします。
2. **aaa authentication** コマンドを使用して、ログインおよび PPP 認証方式リストを使用するようにネットワークアクセスサーバーを設定します。次に、これらの方式リストを適切な回線やインターフェイスに適用します。
3. **aaa authorization** コマンドを使用して、ログイン時の AAA ネットワーク許可を設定します。ネットワーク認可の設定の詳細については、「認可の設定」の章を参照してください。
4. セキュリティプロトコルパラメータ（たとえば、RADIUS または TACACS+）を設定します。RADIUS の詳細については、「Configuring RADIUS」の章を参照してください。TACACS+ の詳細については、「Configuring TACACS+」の章を参照してください。
5. セキュリティサーバーで、ユーザーがローカルホストに接続できるアクセスコントロールリストの AV ペアを使用するには、Telnet 接続を確立する必要があります。
6. autocommand として **access-profile** コマンドを設定します。autocommand を設定すると、リモートユーザーは、個人のユーザープロファイルに関連付けられた許可済み権限にアクセスするために、手動で **access-profile** コマンドを入力する必要はなくなります。autocommand の設定方法については、『Cisco IOS Dial Technologies Command Reference, Release 12.2.』の **autocommand** コマンドを参照してください。



- (注) **access-profile** コマンドが autocommand として設定されている場合でも、二重認証を完了するには、ユーザーがローカルホストに Telnet を送信し、ログインする必要があります。

ユーザー固有の許可ステートメントを作成する場合、次の規則に従います（これらの規則は、**access-profile** コマンドのデフォルトの動作に関連します）。

- セキュリティサーバーでアクセスコントロールリストの AV ペアを設定する場合、有効な AV ペアを使用します。
- リモートユーザーがインターフェイスの既存の認可（第2段階の認証/認可の前に存在する認可）を使用し、異なるアクセスコントロールリスト（ACL）を持つようにするには、ユーザー固有の認可定義で ACL AV ペアだけを指定します。この方法は、デフォルトの認可プロファイルを設定してリモートホストに適用し、ACL はユーザー別に適用する場合などに有効です。

- これらのユーザー固有の許可ステートメントを後でインターフェイスに適用すると、ユーザーの許可に使用する **access-profile** コマンドの実行方法によって、既存のインターフェイス設定に追加することや、既存のインターフェイス設定を置き換えることができます。許可ステートメントを設定する前に、**access-profile** コマンドの機能について理解する必要があります。
- ISDN または Multilink PPP を使用する予定がある場合、ローカルホストで仮想テンプレートも設定する必要があります。

二重認証に関する問題を解決するには、**debug aaa per-user** デバッグコマンドを使用します。このコマンドの詳細については、『*Cisco IOS Debug Command Reference*』を参照してください。

二重認証を設定したら、自動機能を追加できます。

## 自動二重認証の設定

自動ダブル認証を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

### 手順の概要

1. Device(config)# **ip trigger-authentication**
2. 次のいずれかを実行します。
  - Device(config)# **interface bri number**
  - 
  - 
  - Device(config)# **interface serial number :23**
3. Device(config-if)# **ip trigger-authentication**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Device(config)# <b>ip trigger-authentication</b> 例 :  [ <b>timeout seconds</b> ] [ <b>port number</b> ]	二重認証の自動化をイネーブルにします。
ステップ 2	次のいずれかを実行します。  • Device(config)# <b>interface bri number</b> • • • Device(config)# <b>interface serial number :23</b>	ISDN BRI インターフェイスまたは ISDN PRI 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	Device(config-if)# <b>ip trigger-authentication</b>	自動二重認証をインターフェイスに適用します。

## 自動二重認証のトラブルシューティング

自動二重認証の問題を解決するには、特権 EXEC モードで次のコマンドを使用します。

### 手順の概要

1. Device# **show ip trigger-authentication**
2. Device# **clear ip trigger-authentication**
3. Device# **debug ip trigger-authentication**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Device# <b>show ip trigger-authentication</b>	自動二重認証が試行され、成功または失敗したりリモートホストのリストが表示されます。
ステップ 2	Device# <b>clear ip trigger-authentication</b>	自動二重認証が試行されたリモートホストのリストをクリアします（これは、 <b>show ip trigger-authentication</b> コマンドで表示されるテーブルをクリアします）。
ステップ 3	Device# <b>debug ip trigger-authentication</b>	自動二重認証に関する <b>debug</b> の出力が表示されません。

## RADIUS CoA 用の動的認可サービスの設定

次の手順を使用して、動的認可サービスの認証、許可、アカウントिंग（AAA）サーバとしてのルータが、入力方向と出力方向でポリシーマップをプッシュする CoA 機能をサポートできるようにします。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa server radius dynamic-author**
5. **client** {ip\_addr | hostname} [server-key [0 | 7] string]
6. **domain** {delimiter character | stripping [right-to-left]}
7. **port** {port-num}

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 :	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	Router> enable	
ステップ 2	<b>configure terminal</b> 例： Router# 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 3	<b>aaa new-model</b> 例： Router(config)# aaa new-model	AAA をイネーブルにします。
ステップ 4	<b>aaa server radius dynamic-author</b> 例： Router(config)# aaa server radius dynamic-author	ローカル AAA サーバを動的認可サービス用にセットアップして、動的認可ローカル サーバ コンフィギュレーション モードに入ります。このサービスは、ポリシー マップを入力方向と出力方向にプッシュする CoA 機能をサポートするように有効にする必要があります。このモードでは、RADIUS アプリケーション コマンドが設定されます。
ステップ 5	<b>client {ip_addr   hostname} [server-key [0   7] string]</b> 例： Router(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 <b>server-key</b> キーワードと <i>string</i> 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。  (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 6	<b>domain {delimiter character   stripping [right-to-left]}</b> 例： Router(config-locsvr-da-radius)# domain stripping right-to-left 例： Router(config-locsvr-da-radius)# domain delimiter @	(任意) RADIUS アプリケーションについてユーザ名のドメイン オプションを設定します。  • <b>delimiter</b> キーワードで、ドメインデリミタを指定します。次のいずれかのオプションを文字引数に指定できます：@、/、\$、%、\、# または -  • <b>stripping</b> キーワードは、着信のユーザー名と、@ ドメインデリミタの左側にある名前を比較します。  • The <b>right-to-left</b> キーワードは、右から左方向に見て最初のデリミタで文字列を終了します。
ステップ 7	<b>port {port-num}</b> 例：	CoA 要求に UDP ポート 3799 を設定します。

	コマンドまたはアクション	目的
	Router(config-locsvr-da-radius)# port 3799	

## bounce および disable RADIUS CoA 要求を無視するためのデバイスの設定

複数のホストを使用して認証ポートを認証していて、このポートで1つのホストに対してフラップする認可変更 (CoA) 要求があるか、このポートで終了するホストセッションがある場合、このポート上のその他のホストにも影響があります。したがって、複数のホストを使用して認証されたポートは、フラップの場合に1つまたは複数のホストから DHCP の再ネゴシエーションをトリガーします。または、1つまたは複数のホストについて、セッションをホストする認証ポートを管理的にシャットダウンします。

次の手順を使用して、`bounce port` コマンドまたは `disable port` コマンドの形式で RADIUS サーバの認可変更 (CoA) 要求を無視するようにデバイスを設定します。

### 手順の概要

1. `enable`
2. `configure terminal`
3. `aaa new-model`
4. `authentication command bounce-port ignore`
5. `authentication command disable-port ignore`
6. `end`

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device> enable	特権 EXEC モードを有効にします。  • パスワードを入力します (要求された場合)。
ステップ 2	<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 3	<b>aaa new-model</b> 例 : Device(config)# aaa new-model	認証、認可、アカウントिंग (AAA) をグローバルに有効化します。

	コマンドまたはアクション	目的
ステップ 4	<b>authentication command bounce-port ignore</b> 例 : <pre>Device(config)# authentication command bounce-port ignore</pre>	(任意) RADIUS サーバの bounce port コマンドを無視するようにデバイスを設定します。無視しない場合、認証ポート上でホストがフラップをリンクし、結果として、そのポートに接続する 1 つまたは複数のホストから DHCP 再ネゴシエーションが発生します。
ステップ 5	<b>authentication command disable-port ignore</b> 例 : <pre>Device(config)# authentication command disable-port ignore</pre>	(任意) RADIUS サーバの CoA disable port コマンドを無視するようにデバイスを設定します。無視しない場合、1 または複数のホストセッションをホストする認証ポートが管理的にシャットダウンされません。 <ul style="list-style-type: none"> <li>• ポートがシャットダウンされると、セッションも終了します。</li> </ul>
ステップ 6	<b>end</b> 例 : <pre>Device(config)# end</pre>	特権 EXEC モードに戻ります。

## サーバー グループ レベルでのドメインストリッピングの設定

### 手順の概要

1. **enable**
2. **configure terminal**
3. **aaa group server radius server-name**
4. **domain-stripping [strip-suffix word] [right-to-left] [prefix-delimiter word] [delimiter word]**
5. **end**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : <pre>Device&gt; enable</pre>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>• パスワードを入力します (要求された場合)。</li> </ul>
ステップ 2	<b>configure terminal</b> 例 : <pre>Device# 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。

	コマンドまたはアクション	目的
ステップ 3	<b>aaa group server radius <i>server-name</i></b> 例： Device(config)# aaa group server radius rad1	RADIUS サーバを追加し、サーバグループ RADIUS コンフィギュレーション モードを開始します。 • <i>server-name</i> 引数には、RADIUS サーバグループ名を指定します。
ステップ 4	<b>domain-stripping [strip-suffix <i>word</i>] [right-to-left] [prefix-delimiter <i>word</i>] [delimiter <i>word</i>]</b> 例： Device(config-sg-radius)# domain-stripping delimiter username@example.com	サーバグループ レベルでドメイン ストリッピングを設定します。
ステップ 5	<b>end</b> 例： Device(config-sg-radius)# end	サーバグループ RADIUS 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。

## 非 AAA 認証方式

### ラインパスワード保護の設定

このタスクは、パスワードを入力し、パスワードチェック処理を確立することで、端末回線にアクセス コントロールを提供するために使用します。



- (注) ラインパスワード保護を設定し、TACACS または拡張 TACACS を設定する場合、TACACS のユーザー名とパスワードの方が、ラインパスワードよりも優先されます。まだセキュリティポリシーを実装していない場合、AAA を使用することを推奨します。

#### 手順の概要

1. **enable**
2. **configure terminal**
3. **line [aux | console | tty | vty] *line-number* [*ending-line-number*]**
4. **password *password***
5. **login**

#### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	Device> enable	
ステップ 2	<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 3	<b>line [aux   console   tty   vty] line-number [ending-line-number]</b> 例： Device(config)# line console 0	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 4	<b>password password</b> 例： Device(config-line)# secret word	回線上の端末または他のデバイスにパスワードを割り当てます。パスワードチェッカでは大文字と小文字が区別され、スペースを使用できます。たとえば、パスワード「Secret」とパスワード「secret」は異なるパスワードです。また、「two words」は有効なパスワードです。
ステップ 5	<b>login</b> 例： Device(config-line)# login	ログイン時のパスワードチェックをイネーブルにします。  このコマンドの <b>no</b> 形式を使用してパスワードチェックを無効にすると、ラインパスワード検証を無効にできます。  (注) <b>login</b> コマンドによって変更されるのはユーザー名および特権レベルだけであり、シェルは実行されません。したがって、 <b>autocommand</b> は実行されません。この状況で <b>autocommand</b> を実行するには、Telnet セッションをルータに復帰 (ループバック) させる必要があります。この方法で <b>autocommand</b> 機能を実装する場合は、ルータがセキュアな Telnet セッションを使用するように設定されていることを確認してください。

## ユーザー名認証の確立

ユーザー名ベースの認証システムを作成できます。これは、次のような場合に役立ちます。

- TACACS をサポートしないネットワークに、TACACS のようなユーザー名と暗号化されたパスワード認証システムを提供する場合



- 特殊なケース（たとえば、アクセスリストの確認、パスワードの確認なし、ログイン時の `autocommand` の実行、「エスケープなし」の状況など）に備えたログインを提供する場合

ユーザ名の認証を確立するには、システム設定の必要に応じて、グローバルコンフィギュレーションモードで次のコマンドを使用します。

### 手順の概要

1. 次のいずれかを実行します。
  - Device(config)# **username** *name* [**nopassword** | **password** *password* | **password** *encryption-type encrypted password*]
  - 
  - Device(config)# **username** *name* [**access-class** *number*]
2. Device(config)# **username** *name* [**privilege** *level*]
3. Device(config)# **username** *name* [**autocommand** *command*]
4. Device(config)# **username** *name* [**noescape**] [**nohangup**]

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	次のいずれかを実行します。 <ul style="list-style-type: none"> <li>• Device(config)# <b>username</b> <i>name</i> [<b>nopassword</b>   <b>password</b> <i>password</i>   <b>password</b> <i>encryption-type encrypted password</i>]</li> <li>•</li> <li>• Device(config)# <b>username</b> <i>name</i> [<b>access-class</b> <i>number</i>]</li> </ul>	暗号化されたパスワードを使用してユーザー名認証を確立します。 または (任意) アクセスリストによるユーザー名認証を確立します。
ステップ 2	Device(config)# <b>username</b> <i>name</i> [ <b>privilege</b> <i>level</i> ]	(任意) ユーザの特権レベルを設定します。
ステップ 3	Device(config)# <b>username</b> <i>name</i> [ <b>autocommand</b> <i>command</i> ]	(任意) 自動実行されるコマンドを指定します。
ステップ 4	Device(config)# <b>username</b> <i>name</i> [ <b>noescape</b> ] [ <b>nohangup</b> ]	(任意) 「エスケープなし」のログイン環境を設定します。

### 次のタスク

キーワード **noescape** を指定すると、ユーザーは接続先のホストでエスケープ文字を使用できなくなります。**nohangup** 機能を使用すると、`autocommand` の使用後に接続が解除されません。



**注意** **service password-encryption** コマンドを有効にしない限り、設定のパスワードはクリアテキストで表示されます。**service password-encryption** コマンドに関する詳細情報については、『*Cisco IOS Security Command Reference*』を参照してください。

## CHAP 認証または PAP 認証の有効化

インターネットサービスプロバイダー (ISP) のダイヤルソリューションに使用されている最も一般的なトランスポートプロトコルの1つは、ポイントツーポイントプロトコル (PPP) です。従来、リモートユーザーはアクセスサーバーにダイヤルインして、PPPセッションを開始していました。PPPのネゴシエート後は、リモートユーザーはISPネットワークに接続され、そしてインターネットに接続されます。

ISPはアクセスサーバーへの接続を顧客に限定したいため、リモートユーザーはアクセスサーバーに対して認証を受けてから、PPPセッションを開始する必要があります。通常、リモートユーザーは、アクセスサーバーからのプロンプトに応じてユーザー名とパスワードを入力して、認証を受けます。これは実行可能なソリューションですが、管理が困難で、リモートユーザーにとっても面倒です。

よりよいソリューションは、PPPに組み込まれた認証プロトコルを使用することです。この場合、リモートユーザーはアクセスサーバーにダイヤルインし、アクセスサーバーとPPPの最小サブセットを開始します。この操作で、ISPのネットワークに対するアクセス権はリモートユーザーに付与されません。単に、アクセスサーバーがリモートデバイスと通話できるだけです。

現在、PPPは2つの認証プロトコルをサポートします。パスワード認証プロトコル (PAP) およびチャレンジハンドシェイク認証プロトコル (CHAP) の2つです。いずれもRFC 1334で規定され、同期インターフェイスと非同期インターフェイスでサポートされます。PAPまたはCHAPを介する認証は、サーバーからのプロンプトを受けてユーザー名とパスワードを入力する方法と同等です。CHAPの場合、接続の間にリモートユーザーのパスワードは送信されないため、より安全性が高いと考えられます。

(PAP認証またはCHAP認証の有無に関係なく) PPPはダイヤルアウトソリューションでもサポートされます。アクセスサーバーがダイヤルアウト機能を使用するのは、アクセスサーバーからリモートデバイスに対してコールを開始し、PPPなどのトランスポートプロトコルを起動しようとするときです。

CHAPとPAPに関する詳細については、『*Cisco IOS XE Dial Technologies Configuration Guide, Release 2*』を参照してください。



(注) CHAPまたはPAPを使用するには、PPPカプセル化を実行する必要があります。

インターフェイスでCHAPをイネーブルにし、リモートデバイスがそのインターフェイスに接続しようとする、アクセスサーバーからリモートデバイスにCHAPパケットが送信されます。CHAPパケットは、リモートデバイスに応答するように要求または「チャレンジ」しま

す。チャレンジ パケットは、ローカル ルータの ID、ランダム 番号、および ホスト 名から構成 されます。

リモート デバイスは、チャレンジ パケットを受信すると、ID、リモート デバイスのパスワ ード、およびランダム 番号を連結し、リモート デバイスのパスワードを使用してすべてを暗号化 します。リモート デバイスは、その結果を、暗号化プロセスで使用されたパスワードに関連付 けられた名前とともにアクセス サーバーに返信します。

アクセス サーバーがその応答を受信すると、受信した名前を使用して、ユーザー データベ ースに保存されているパスワードを取得します。取得したパスワードは、暗号化プロセスで使用 されたリモート デバイスと同じパスワードです。アクセス サーバーは、新しく取得したパス ワードを使用して、連結された情報を暗号化します。その結果が応答パケットで送信された結 果と一致する場合、認証は成功です。

CHAP 認証を使用する利点は、リモート デバイスのパスワードがクリア テキストで送信され ないことです。結果として、他のデバイスによるパスワード盗用や、ISP のネットワークに対 する不正アクセスの取得を回避できます。

CHAP トランザクションが発生するのは、リンクが確立したときだけです。アクセス サーバ ーは、以降のコール中にパスワードを要求しません（ただし、ローカル デバイスは、コール中に 他のデバイスからこのような要求があった場合、応答する可能性があります）。

PAP をイネーブルにすると、アクセス サーバに接続しようとするリモート ルータは、認証要 求を送信する必要があります。認証要求に指定されているユーザー名とパスワードが受け入れ られた場合、Cisco IOS XE ソフトウェアから認証の確認応答が送信されます。

CHAP または PAP をイネーブルにすると、アクセス サーバーは、ダイヤルインするリモート デバイスからの認証を必須にするようになります。イネーブルにしたプロトコルをリモート デ バイスがサポートしていない場合、コールはドロップされます。

CHAP または PAP を使用するには、次のタスクを実行する必要があります。

1. PPP カプセル化をイネーブルにします。
2. インターフェイスで CHAP または PAP をイネーブルにします。
3. CHAP の場合、認証が必須の各リモート システムについて、ホスト名の認証および秘密 (パスワード) を設定します。

## PPP カプセル化の有効化

PPP カプセル化をイネーブルにするには、インターフェイス コンフィギュレーション モード で次のコマンドを使用します。

コマンド	目的
Device (config-if) # <b>encapsulation ppp</b>	インターフェイスで PPP をイネーブルにします。

## PAP または CHAP のイネーブル化

PPP カプセル化として設定されているインターフェイスで、CHAP 認証または PAP 認証をイネーブルにするには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
<pre>Device(config-if)# PPP authentication {protocol1 [protocol2...]} [if-needed] {default   list-name} [callin] [one-time]</pre>	<p>サポートされる認証プロトコルと、使用順序を定義します。このコマンドの <i>protocol1</i> と <i>protocol2</i> は、CHAP、MS-CHAP、および PAP のプロトコルを示します。PPP 認証は、まず <i>protocol1</i> に指定された最初の認証方式を使用して試行されます。認証に <i>protocol1</i> を使用できない場合は、次に設定されているプロトコルを使用して認証のネゴシエーションを行います。</p>

インターフェイスで **ppp authentication chap** を設定する場合、そのインターフェイスで PPP 接続を開始するすべての受信コールは、CHAP を使用して認証される必要があります。同様に、**ppp authentication pap** を設定する場合、PPP 接続を開始するすべての受信コールは、PAP を使用して認証される必要があります。**ppp authentication chap pap** を設定する場合、アクセスサーバーは、CHAP を使用して PPP セッションを開始するすべての受信コールを認証しようとします。リモートデバイスが CHAP をサポートしない場合、アクセスサーバーは PAP を使用してコールを認証しようとします。リモートデバイスが CHAP も PAP もサポートしない場合、認証は失敗し、コールはドロップされます。**ppp authentication pap chap** を設定する場合、アクセスサーバーは、PAP を使用して PPP セッションを開始するすべての受信コールを認証しようとします。リモートデバイスが PAP をサポートしない場合、アクセスサーバーは CHAP を使用してコールを認証しようとします。リモートデバイスがいずれのプロトコルもサポートしない場合、認証は失敗し、コールはドロップされます。**callin** キーワードを指定して **ppp authentication** コマンドを設定すると、アクセスサーバーは、リモートデバイスがコールを開始した場合にだけ、リモートデバイスの認証を行います。

認証方式リストと **one-time** キーワードを使用できるのは、AAA を有効にした場合だけです。TACACS または拡張 TACACS を有効にしている場合は、使用できません。**ppp authentication** コマンドを使用して認証方式リストの名前を指定すると、PPP は、指定した方式リストに定義されている方式を使用して、接続を認証しようとします。AAA をイネーブルにし、名前で定義されている方式リストがない場合、PPP は、デフォルトに定義されている方式を使用して接続を認証しようとします。**one-time** キーワードを指定して **ppp authentication** コマンドを使用すると、認証中にワンタイムパスワードをサポートできます。

**if-needed** キーワードを使用できるのは、TACACS または拡張 TACACS を使用している場合だけです。**if-needed** キーワードを指定して **ppp authentication** コマンドを使用することは、現在のコール期間中にリモートデバイスがまだ認証されていない場合にだけ、PPP が PAP または CHAP を介してリモートデバイスを認証することを示します。リモートデバイスが、標準のログイン手順で認証を受け、EXEC プロンプトから PPP を開始した場合、**ppp authentication chap if-needed** がインターフェイスで設定されていれば、PPP は CHAP を介して認証しません。



**注意** **aaa authentication ppp** コマンドを使用して設定されていない *list-name* を使用する場合、その回線での PPP は無効になります。

ローカルルータまたはアクセスサーバーが認証を必須とする各リモートシステムについて、**username** エントリを追加する方法については、「[ユーザー名認証の確立 \(66 ページ\)](#)」を参照してください。

## 着信認証と発信認証

PPP は双方向の認証をサポートしています。通常、リモートデバイスがアクセスサーバーにダイヤルインするときは、それが許可されているアクセスであることをリモートデバイスが証明するように、アクセスサーバーから要求されます。これは着信認証と呼ばれます。同時に、リモートデバイスは、身元を証明するようにアクセスサーバーに要求することもできます。これは発信認証と呼ばれます。また、アクセスサーバーは、リモートデバイスに対してコールを開始するときにも、発信認証を実行します。

### 発信 PAP 認証のイネーブル化

発信 PAP 認証をイネーブルにするには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Device(config-if)# <b>ppp pap sent-username</b> <i>username password password</i>	発信 PAP 認証をイネーブルにします。

アクセスサーバーからリモートデバイスに対してコールを開始する場合は常に、またはアウトバウンド認証のためにリモートデバイスの要求に応答する必要がある場合は、**ppp pap sent-username** コマンドで指定されたユーザー名とパスワードを使用して自身を認証します。

### PAP 認証要求の拒否

ピアからの PAP 認証要求を拒否するには（つまり、すべてのコールで PAP 認証をディセーブルにするには）、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Device(config-if)# <b>ppp pap refuse</b>	PAP 認証を要求するピアからの PAP 認証を拒否します。

**refuse** キーワードが使用されない場合、ルータはピアから受信した PAP 認証チャレンジを拒否しません。

## 共通 CHAP パスワードの作成

リモート CHAP 認証だけの場合、不明なピアからのチャレンジに対して使用する共通 CHAP シークレットパスワードを作成するように、ルータを設定できます。たとえば、ルータが、新しい（つまり不明な）ルータが追加された、ルータのロータリー（別ベンダー製のルータ、または古いバージョンの Cisco IOS ソフトウェアを実行するルータ）に発信する場合などです。**ppp chap password** コマンドを使用すると、任意のダイヤラインターフェイスまたは非同期グループインターフェイスで、複数のユーザー名およびパスワード コンフィギュレーション コマンドをこのコマンドの単一のコピーで置換できます。

ルータのコレクションに発信するルータが、共通の CHAP シークレットパスワードを設定できるようにするには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Device(config-if)# <b>ppp chap password</b> secret	ルータのコレクションに発信するルータが、共通の CHAP シークレットパスワードを設定できるようにします。

## CHAP 認証要求の拒否

ピアからの CHAP 認証要求を拒否するには（つまり、すべてのコールで CHAP 認証をディセーブルにするには）、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Device(config-if)# <b>ppp chap refuse</b> [callin]	CHAP 認証を要求するピアからの CHAP 認証を拒否します。

**callin** キーワードが使用されると、ルータは、ピアから受信した CHAP 認証チャレンジへの応答を拒否します。ただし、ルータが送信する CHAP チャレンジに対しては、ピアが応答することを必須とします。

（**ppp pap sent-username** コマンドを使用して）発信 PAP がイネーブルの場合、拒否パケットの認証方式として、PAP が提案されます。

## ピアが認証されるまで CHAP 認証を遅延する

ピアがルータから認証を受けるまで、CHAP 認証を要求するピアに対してルータを認証しないように指定するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Device(config-if)# <b>ppp chap wait</b> secret	ピアがルータから認証を受けるまで、CHAP 認証を遅延するようにルータを設定します。

このコマンド（デフォルト）により、CHAP 認証を要求するピアがルータの認証を受けてから、ルータがピアの認証を受けるように指定します。no ppp chap wait コマンドにより、ルータが認証チャレンジに即座に応答するように指定されます。

## MS-CHAP の使用

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（MS-CHAP）は、Microsoft バージョンの CHAP であり、RFC 1994 の拡張です。標準バージョンの CHAP と同様に、MS-CHAP は PPP 認証に使用されます。この場合、Microsoft Windows NT または Microsoft Windows 95 を使用する PC と、ネットワーク アクセス サーバーとして動作する Cisco デバイスまたはアクセス サーバーとの間に認証が発生します。

MS-CHAP と標準の CHAP の違いは次のとおりです。

- MS-CHAP をイネーブルにするには、LCP オプション 3 の Authentication Protocol で、CHAP Algorithm 0x80 をネゴシエートします。
- MS-CHAP 応答パケットは、Microsoft Windows NT 3.5 および 3.51、Microsoft Windows 95、および Microsoft LAN Manager 2.x と互換性を持つように設計されたフォーマットです。このフォーマットを使用する場合、オーセンティケータは、クリアパスワードまたは可逆的に暗号化されたパスワードを保存する必要はありません。
- MS-CHAP には、オーセンティケータが制御する認証リトライ メカニズムがあります。
- MS-CHAP には、オーセンティケータが制御するチャレンジパスワードメカニズムがあります。
- MS-CHAP には、Failure パケット メッセージフィールドで返される「reason-for failure」コードセットが定義されています。

実装したセキュリティ プロトコルに応じて、AAA セキュリティ サービスの有無にかかわらず、MS-CHAP による PPP 認証を使用できます。AAA をイネーブルにしている場合、MS-CHAP を使用する PPP 認証は、TACACS+ および RADIUS の両方と併用できます。次の表に、RADIUS が MS-CHAP をサポートできるベンダー固有 RADIUS 属性（IETF Attribute 26）を示します。

表 12: MS-CHAP 用のベンダー固有 RADIUS 属性

ベンダー ID 番号	ベンダータイプ番号	ベンダー固有属性	説明
311	11	MSCHAP-Challenge	ネットワーク アクセスサーバが MS-CHAP ユーザに送信するチャレンジが含まれます。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。

ベンダー ID 番号	ベンダータイ プ 番号	ベンダー固有属性	説明
211	11	MSCHAP-Response	PPP MS-CHAP ユーザがチャレンジに対する応答で提供するレスポンス値が含まれます。 Access-Request パケットでしか使用されません。 この属性は、PPP CHAP ID と同じです

## MS-CHAP を使用した PPP 認証の定義

MS-CHAP を使用して PPP 認証を定義するには、インターフェイス コンフィギュレーション モードで次のコマンドを使用します。

### 手順の概要

1. Device(config-if)# **encapsulation ppp**
2. Device(config-if)# **ppp authentication ms-chap [if-needed] [list-name | default] [callin] [one-time]**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Device(config-if)# <b>encapsulation ppp</b>	PPP カプセル化をイネーブルにします。
ステップ 2	Device(config-if)# <b>ppp authentication ms-chap [if-needed] [list-name   default] [callin] [one-time]</b>	MS-CHAP を使用して PPP 認証を定義します。

### 次のタスク

あるインターフェイスで **ppp authentication ms-chap** を設定する場合、PPP 接続を開始するそのインターフェイスに着信するすべてのコールは、MS-CHAP を使用して認証する必要があります。 **callin** キーワードを指定して **ppp authentication** コマンドを設定すると、アクセスサーバーは、リモートデバイスがコールを開始した場合にだけ、リモートデバイスの認証を行います。

認証方式リストと **one-time** キーワードを使用できるのは、AAA を有効にした場合だけです。TACACS または拡張 TACACS を有効にしている場合は、使用できません。 **ppp authentication** コマンドを使用して認証方式リストの名前を指定すると、PPP は、指定した方式リストに定義されている方式を使用して、接続を認証しようとします。AAA をイネーブルにし、名前で定義されている方式リストがない場合、PPP は、デフォルトに定義されている方式を使用して接続を認証しようとします。 **one-time** キーワードを指定して **ppp authentication** コマンドを使用すると、認証中にワンタイムパスワードをサポートできます。

**if-needed** キーワードを使用できるのは、TACACS または拡張 TACACS を使用している場合だけです。 **if-needed** キーワードを指定して **ppp authentication** コマンドを使用することは、現在のコール期間中にリモートデバイスがまだ認証されていない場合にだけ、PPP が MS-CHAP を介してリモートデバイスを認証することを示します。リモートデバイスが、標準のログイン手



順で認証を受け、EXECプロンプトからPPPを開始した場合、**ppp authentication chap if-needed**が設定されていれば、PPPはMS-CHAPを介して認証しません。



- (注) MS-CHAPを使用するPPP認証と、ユーザー名認証を併用する場合、ローカルユーザー名/パスワードデータベースにMS-CHAPシークレットを含める必要があります。ユーザー名認証の詳細については、「ユーザー名認証の確立」の項を参照してください。

## 認証の例

### 例：RADIUS 認証

ここでは、RADIUSを使用する2つの設定例を紹介します。

次に、RADIUSを使用して認証および認可を行うようにルータを設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# aaa authentication login radius-login group radius local
Device(config)# aaa authentication ppp radius-ppp if-needed group radius
Device(config)# aaa authorization exec default group radius if-authenticated
Device(config)# aaa authorization network default group radius
Device(config)# line 3
Device(config-line)# login authentication radius-login
Device(config-line)# exit
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# ppp authentication radius-ppp
Device(config-if)# end
```

このRADIUS認証および認可設定のサンプル行は、次のように定義されます。

- **aaa authentication login radius-login group radius local** コマンドを実行すると、ルータは、ログインプロンプトで認証にRADIUSを使用するように設定されます。RADIUSがエラーを返すと、ユーザーはローカルデータベースを使用して認証されます。
- **aaa authentication ppp radius-ppp if-needed group radius** コマンドを実行すると、ユーザーがまだログインしていない場合、Cisco IOS XEソフトウェアはCHAPまたはPAPによるPPP認証を使用するように設定されます。EXEC施設がユーザーを認証すると、PPP認証は実行されません。
- **aaa authorization exec default group radius if-authenticated** コマンドを実行すると、autocommandや特権レベルなど、EXEC認可時に使用される情報について、RADIUSデータベースに照会されます。ただし、ユーザーの認証が成功した場合にだけ、権限が付与されます。
- **aaa authorization network default group radius** コマンドを実行すると、ネットワーク認可、アドレス割り当て、および他のアクセスリストについてRADIUSに照会されます。
- **login authentication radius-login** コマンドを使用すると、ライン3についてradius-login方式リストが有効になります。

- **ppp authentication radius-ppp** コマンドを使用すると、シリアルインターフェイス 0 について radius-ppp 方式リストが有効になります。

次に、ユーザー名とパスワードの入力を求め、その内容を確認し、ユーザーの EXEC レベルを認可し、特権レベル 2 の認可方式として指定するように、ルータを設定する例を示します。この例では、ユーザー名プロンプトにローカルユーザー名を入力すると、そのユーザー名が認証に使用されます。

ローカルデータベースを使用してユーザーが認証されると、RADIUS 認証からのデータは保存されないため、RADIUS を使用する EXEC 認可は失敗します。また、この方式リストではローカルデータベースを使用して autocommand を検索します。autocommand がない場合、ユーザーは EXEC ユーザーになります。次に、ユーザーが特権レベル 2 に設定されているコマンドを発行しようとする、TACACS+ を使用してコマンドの認可が試行されます。

```
Device> enable
Device# configure terminal
Device(config)# aaa authentication login default group radius local
Device(config)# aaa authorization exec default group radius local
Device(config)# aaa authorization command 2 default group tacacs+ if-authenticated
Device(config)# radius server radserver
Device(config-sg-radius)# address ipv4 10.2.3.1
Device(config-sg-radius)# exit
Device(config)# radius-server attribute 44 include-in-access-req
Device(config)# radius-server attribute 8 include-in-access-req
Device(config)# end
```

この RADIUS 認証および認可設定のサンプル行は、次のように定義されます。

- **aaa authentication login default group radius local** コマンドにより、RADIUS (RADIUS が応答しない場合はルータのローカル ユーザー データベース) がユーザー名およびパスワードを確認するように指定します。
- **aaa authorization exec default group radius local** コマンドにより、RADIUS を使用してユーザーが認証される場合、ユーザーの EXEC レベルの設定に RADIUS 認証情報を使用するように指定します。RADIUS 情報が使用されない場合、このコマンドにより、EXEC 認可にローカル ユーザー データベースが使用されるように指定します。
- **aaa authorization command 2 default group tacacs+ if-authenticated** コマンドにより、すでにユーザーの認証が成功している場合、特権レベル 2 に設定されているコマンドに TACACS+ 認可を指定します。
- **radius-server attribute 44 include-in-access-req** コマンドにより、access-request パケットで RADIUS 属性 44 (Acct-Session-ID) を送信します。
- **radius-server attribute 8 include-in-access-req** コマンドにより、access-request パケットで RADIUS 属性 8 (Framed-IP-Address) を送信します。

## 例：TACACS 認証

次に、PPP 認証に使用するセキュリティ プロトコルとして TACACS+ を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication ppp test group tacacs+ local
Device(config)# interface gigabitethernet 1/1/2
Device(config-if)# ppp authentication chap pap test
Device(config-if)# exit
Device(config)# tacacs server server1
Device(config-server-tacacs)# address ipv4 192.0.2.3
Device(config-server-tacacs)# key key1
Device(config-server-tacacs)# end
```

この TACACS+ 認証設定のサンプル行は、次のように定義されます。

- **aaa new-model** コマンドは、AAA セキュリティ サービスをイネーブルにします。
- **aaa authentication** コマンドにより、PPP を実行するシリアルインターフェイスに使用する方式リスト「test」を定義します。キーワード **group tacacs+** は、TACACS+ を介して認証を実行することを示します。認証中に TACACS+ から何らかのエラーが返される場合、キーワード **local** は、ネットワーク アクセス サーバー上のローカルデータベースを使用して認証が試行されることを示します。
- **interface** コマンドにより、回線を選択します。
- **ppp authentication** コマンドにより、この回線に test 方式リストを適用します。
- **address ipv4** コマンドにより、TACACS+ デーモンが 192.0.2.3 という IP アドレスを持っていると指定します。
- **key** コマンドにより、共有暗号キーが「key1」になるように定義します。

次に、PPP に AAA 認証を設定する例を示します。

```
Device(config)# aaa authentication ppp default if-needed group tacacs+ local
```

この例のキーワード **default** は、デフォルトですべてのインターフェイスに PPP 認証が適用されることを示します。**if-needed** キーワードは、ユーザーが ASCII ログイン手順を介してすでに認証済みの場合、PPP は不要なので、スキップできることを示します。認証が必要な場合、**group tacacs+** キーワードは、TACACS+ を介して認証が実行されることを示します。認証中に TACACS+ から何らかのエラーが返される場合、キーワード **local** は、ネットワーク アクセス サーバー上のローカルデータベースを使用して認証が試行されることを示します。

次に、PAP に同じ認証アルゴリズムを作成し、「default」ではなく「MIS-access」の方式リストを呼び出す例を示します。

```
Device> enable
Device# configure terminal
Device(config)# aaa authentication ppp MIS-access if-needed group tacacs+ local
Device(config)# interface gigabitethernet 1/1/2
Device(config)# ppp authentication pap MIS-access
Device(config)# end
```

この例では、リストはどのインターフェイスにも適用されないため（自動的にすべてのインターフェイスに適用されるデフォルトリストとは異なります）、管理者は **interface** コマンドを使用して、この認証スキームを適用するインターフェイスを選択する必要があります。次

に、管理者は **ppp authentication** コマンドを使用して、選択したインターフェイスにこの方式リストを適用する必要があります。

## 例 : Kerberos 認証

ログイン認証方式として **Kerberos** を指定するには、次のコマンドを使用します。

```
aaa authentication login default krb5
```

PPP に **Kerberos** 認証を指定するには、次のコマンドを使用します。

```
aaa authentication ppp default krb5
```

## 例 : AAA スケーラビリティ

次に、セキュリティプロトコルとして **RADIUS** による **AAA** を使用する一般的なセキュリティ設定例を示します。この例では、ネットワーク アクセス サーバーは、16 バックアッププロセスを割り当てて **PPP** に対する **AAA** 要求を処理するように設定されています。

```
aaa new-model
radius-server host alcatraz
radius-server key myRaDiUSpassWoRd
radius-server configure-nas
username root password ALongPassword
aaa authentication ppp dialins group radius local
aaa authentication login admins local
aaa authorization network default group radius local
aaa accounting network default start-stop group radius
aaa processes 16
line 1 16
  autoselect ppp
  autoselect during-login
  login authentication admins
  modem dialin
interface group-async 1
  group-range 1 16
  encapsulation ppp
  ppp authentication pap dialins
```

この **RADIUS AAA** 設定のサンプル行は、次のように定義されます。

- **aaa new-model** コマンドは、AAA ネットワーク セキュリティ サービスをイネーブルにします。
- **radius-server host** コマンドは **RADIUS** サーバー ホストの名前を定義します。
- **radius-server key** コマンドは、ネットワーク アクセス サーバーと **RADIUS** サーバー ホストの間の共有秘密テキスト文字列を定義します。
- **radius-server configure-nas** コマンドは、デバイスが最初に起動したときに、シスコルータまたはアクセスサーバーがスタティックルートと IP プール定義について **RADIUS** サーバーに照会するように定義します。
- **username** コマンドはユーザー名とパスワードを定義します。これらの情報は、PPP パスワード認証プロトコル (**PAP**) の発信元身元確認に使用されます。

- **aaa authentication ppp dialins group radius local** コマンドで、まず RADIUS 認証を指定する認証方式リスト「dialins」を定義します。次に、(RADIUS サーバーが応答しない場合) PPP を使用するシリアル回線でローカル認証が使用されます。
- **aaa authentication login admins local** コマンドは、ログイン認証に別の方式リスト「admins」を定義します。
- **aaa authorization network default group radius local** コマンドは、アドレスと他のネットワーク パラメータを RADIUS ユーザーに割り当てるために使用されます。
- **aaa accounting network default start-stop group radius** コマンドは、PPP の使用状況を追跡します。
- **aaa processes** コマンドにより、PPP に対する AAA 要求を処理するために 16 個のバックグラウンドプロセスを割り当てます。
- **line** コマンドはコンフィギュレーション モードをグローバル コンフィギュレーションからライン コンフィギュレーションに切り替え、設定対象の回線を指定します。
- **autoselect ppp** コマンドは、選択した回線上で PPP セッションを自動的に開始できるようにします。
- **autoselect during-login** コマンドを使用すると、Return キーを押さずにユーザ名およびパスワードのプロンプトが表示されます。ユーザがログインすると、autoselect 機能 (この場合は PPP) が開始します。
- **login authentication admins** コマンドは、ログイン認証に「admins」方式リストを適用します。
- **modem dialin** コマンドは、選択した回線に接続されているモデムを設定し、着信コールだけを受け入れるようにします。
- **interface group-async** コマンドは、非同期インターフェイス グループを選択して定義します。
- **group-range** コマンドは、インターフェイス グループ内のメンバー非同期インターフェイスを定義します。
- **encapsulation ppp** コマンドは、指定のインターフェイスに使用されるカプセル化方式として PPP を設定します。
- **ppp authentication pap dialins** コマンドは「dialins」方式リストを指定したインターフェイスに適用します。

## 例：AAA 認証のログインバナーおよび Failed-Login バナーの設定

次に、ユーザーがシステムにログインするときに表示されるログインバナー (この場合、「Unauthorized Access Prohibited」というフレーズ) を設定する例を示します。アスタリスク (\*) はデリミタとして使用されます。RADIUS はデフォルト ログイン認証方式として指定されます。

## 例：AAA パケットオブディスコネクト サーバー キー

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication banner *Unauthorized Access Prohibited*
Device(config)# aaa authentication login default group radius
```

この設定によって、次のログイン バナーが表示されます。

```
Unauthorized Access Prohibited
Username:
```

次の例では、ユーザーがシステムにログインしようとして失敗すると表示される Failed-Login バナー（この場合、「Failed login. Try again」というフレーズ）を設定する方法を示します。アスタリスク（\*）はデリミタとして使用されます。RADIUS はデフォルト ログイン認証方式として指定されます。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication banner *Unauthorized Access Prohibited*
Device(config)# aaa authentication fail-message *Failed login. Try again.*
Device(config)# aaa authentication login default group radius
```

この設定によって、次のログイン バナーおよび Failed-Login バナーが表示されます。

```
Unauthorized Access Prohibited
Username:
Password:
Failed login. Try again.
```

## 例：AAA パケットオブディスコネクト サーバー キー

次に、パケットオブディスコネクト（POD）を設定する例を示します。その結果、特定のセッション属性が指定されると、ネットワーク アクセス サーバー（NAS）の接続が終了します。

```
aaa new-model
aaa authentication ppp default radius
aaa accounting network default start-stop radius
aaa accounting delay-start
aaa pod server server-key xyz123
radius-server host 192.0.2.3 non-standard
radius-server key rad123
```

## 例：二重認証

ここでは、二重認証に使用できる設定例を示します。実際のネットワークおよびセキュリティ要件によっては、この例とは大幅に異なる可能性があります。



(注) 設定例には、特定の IP アドレスと他の特定の情報が含まれます。この情報は説明のための例であり、実際の設定には異なる IP アドレス、異なるユーザー名とパスワード、異なる認可ステートメントを使用します。

### 例：二重認証による AAA のローカルホストの設定

次の 2 つの例では、PPP とログイン認証、およびネットワークと EXEC 認可に AAA を使用するようにローカルホストを設定する方法を示します。例はそれぞれ RADIUS の例と TACACS+ の例です。

いずれの例でも、先頭の 3 行で AAA を設定し、特定のサーバーを AAA サーバーとして設定しています。続く 2 行で PPP およびログイン認証に AAA を設定し、最後の 2 行でネットワークおよび EXEC 認可を設定します。最後の行が必要なのは、**access-profile** コマンドを autocommand として実行する場合だけです。

次に、RADIUS AAA サーバーを使用するデバイス設定の例を示します。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# radius server radserver
Device(config-sg-radius)# address ipv4 secureserver
Device(config-sg-radius)# key myradiuskey
Device(config-sg-radius)# exit
Device(config)# aaa authentication ppp default group radius
Device(config)# aaa authentication login default group radius
Device(config)# aaa authorization network default group radius
Device(config)# aaa authorization exec default group radius
Device(config)# end
```

次に、TACACS+ サーバーを使用するデバイス設定の例を示します。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# tacacs server server1
Device(config-server-tacacs)# address ipv4 192.0.2.3
Device(config-server-tacacs)# key mytacacskey
Device(config-server-tacacs)# exit
Device(config)# aaa authentication ppp default group tacacs+
Device(config)# aaa authentication login default group tacacs+
Device(config)# aaa authorization network default group tacacs+
Device(config)# aaa authorization exec default group tacacs+
Device(config)# end
```

### 例：第 1 段階の PPP 認証と許可に関する AAA サーバーの設定

次に、AAA サーバーでの設定例を示します。また、RADIUS 用の AAA 設定例の一部を示します。

TACACS+ サーバーも同様に設定できます（「TACACS による設定完了の例」を参照してください）。

この例では、二重認証の第 1 段階で CHAP によって認証される「hostx」というリモートホストに関する認証/認可を定義します。ACLAV ペアは、リモートホストによる Telnet 接続をローカルホストに制限しています。ローカルホストの IP アドレスは 10.0.0.2 です。

次に、RADIUS 用の AAA サーバーの設定例を一部示します。

```
hostx Password = "welcome"
      User-Service-Type = Framed-User,
      Framed-Protocol = PPP,
```

## 例：第2段階の Per-User 認証と許可に関する AAA サーバーの設定

```

cisco-avpair = "lcp:interface-config=ip unnumbered fastethernet 0",
cisco-avpair = "ip:inacl#3=permit tcp any 172.21.114.0 0.0.0.255 eq telnet",
cisco-avpair = "ip:inacl#4=deny icmp any any",
cisco-avpair = "ip:route#5=10.0.0.0 255.0.0.0",
cisco-avpair = "ip:route#6=10.10.0.0 255.0.0.0",
cisco-avpair = "ipx:inacl#3=deny any"

```

## 例：第2段階の Per-User 認証と許可に関する AAA サーバーの設定

ここでは、RADIUS サーバーでの AAA 設定例の一部を示します。これらの設定では、ユーザ名が「patuser」のユーザ (Pat) の認証と認可を定義します。このユーザは、二重認証の第2段階でユーザ認証されます。

TACACS+ サーバーも同様に設定できます（「TACACS による設定完了の例」を参照してください）。

3つの例は、**access-profile** コマンドの3つの各形式で使用できる RADIUS AAA 設定の例を示します。

最初の例は、**access-profile** コマンドのデフォルトの形式（キーワードなし）で機能する AAA 設定例の一部を示します。1つの ACL AV ペアのみが定義されます。また、この例では **autocommand** として **access-profile** コマンドも設定します。

```

patuser Password = "welcome"
User-Service-Type = Shell-User,
cisco-avpair = "shell:autocmd=access-profile"
User-Service-Type = Framed-User,
Framed-Protocol = PPP,
cisco-avpair = "ip:inacl#3=permit tcp any host 10.0.0.2 eq telnet",
cisco-avpair = "ip:inacl#4=deny icmp any any"

```

2番目の例は、**access-profile** コマンドの **access-profile merge** 形式で機能する AAA 設定例の一部を示します。また、この例では **autocommand** として **access-profile merge** コマンドも設定します。

```

patuser Password = "welcome"
User-Service-Type = Shell-User,
cisco-avpair = "shell:autocmd=access-profile merge"
User-Service-Type = Framed-User,
Framed-Protocol = PPP,
cisco-avpair = "ip:inacl#3=permit tcp any any"
cisco-avpair = "ip:route=10.0.0.0 255.255.0.0",
cisco-avpair = "ip:route=10.1.0.0 255.255.0.0",
cisco-avpair = "ip:route=10.2.0.0 255.255.0.0"

```

3番目の例は、**access-profile** コマンドの **access-profile replace** 形式で機能する AAA 設定例の一部を示します。また、この例では **autocommand** として **access-profile replace** コマンドも設定します。

```

patuser Password = "welcome"
User-Service-Type = Shell-User,
cisco-avpair = "shell:autocmd=access-profile replace"
User-Service-Type = Framed-User,
Framed-Protocol = PPP,
cisco-avpair = "ip:inacl#3=permit tcp any any",
cisco-avpair = "ip:inacl#4=permit icmp any any",
cisco-avpair = "ip:route=10.10.0.0 255.255.0.0",

```



```
cisco-avpair = "ip:route=10.11.0.0 255.255.0.0",
cisco-avpair = "ip:route=10.12.0.0 255.255.0.0"
```

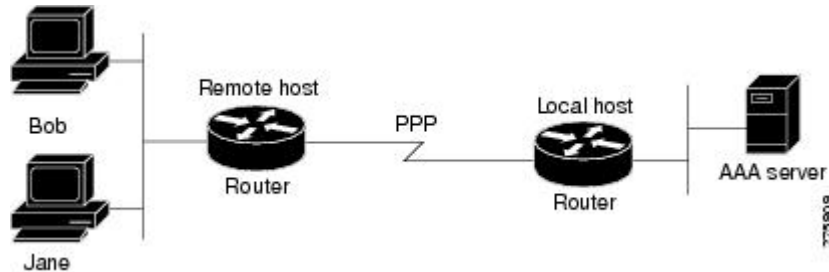
### 例：TACACS による設定完了

この例では、リモートホスト（二重認証の第1段階で使用）および特定のユーザー（二重認証の第2段階で使用）の両方向けの、TACACS+ 認可プロファイルの設定を示します。このTACACS+ の例には、前のRADIUS の例とほぼ同じ設定情報が使用されます。

この設定例は、リモートホスト「hostx」および3 ユーザ（ユーザ名が「pat\_default」、 「pat\_merge」、および「pat\_replace」）のTACACS+サーバ上にある認証/認可プロファイルを示します。これら3つのユーザー名の設定は、**access-profile** コマンドの3種類のフォームに対応する異なる設定を示しています。また、3つのユーザー設定は、**access-profile** コマンドの各形式について **autocommand** の設定方法も示しています。

次の図に、トポロジを示します。図の後に、TACACS+ 設定ファイルの例を示します。

図 3: 二重認証のトポロジ例



この設定例は、リモートホスト「hostx」および3 ユーザ（ユーザ名が「pat\_default」、 「pat\_merge」、および「pat\_replace」）のTACACS+サーバ上にある認証/認可プロファイルを示します。

```
key = "mytacacskey"
default authorization = permit
#-----Remote Host (BRI)-----
#
# This allows the remote host to be authenticated by the local host
# during fist-stage authentication, and provides the remote host
# authorization profile.
#-----
user = hostx
{
  login = cleartext "welcome"
  chap = cleartext "welcome"
  service = ppp protocol = lcp {
    interface-config="ip unnumbered fastethernet 0"
  }
  service = ppp protocol = ip {
    # It is important to have the hash sign and some string after
    # it. This indicates to the NAS that you have a per-user
    # config.
    inacl#3="permit tcp any 172.21.114.0 0.0.0.255 eq telnet"
    inacl#4="deny icmp any any"
    route#5="10.0.0.0 255.0.0.0"
    route#6="10.10.0.0 255.0.0.0"
```

```

    }
    service = ppp protocol = ipx {
        # see previous comment about the hash sign and string, in protocol = ip
        inacl#3="deny any"
    }
}
#----- "access-profile" default user "only acfs" -----
#
# Without arguments, access-profile removes any access-lists it can find
# in the old configuration (both per-user and per-interface), and makes sure
# that the new profile contains ONLY access-list definitions.
#
#-----
user = pat_default
{
    login = cleartext "welcome"
    chap = cleartext "welcome"
    service = exec
    {
        # This is the autocommand that executes when pat_default logs in.
        autocmd = "access-profile"
    }
    service = ppp protocol = ip {
        # Put whatever access-lists, static routes, whatever
        # here.
        # If you leave this blank, the user will have NO IP
        # access-lists (not even the ones installed prior to
        # this)!
        inacl#3="permit tcp any host 10.0.0.2 eq telnet"
        inacl#4="deny icmp any any"
    }
    service = ppp protocol = ipx {
        # Put whatever access-lists, static routes, whatever
        # here.
        # If you leave this blank, the user will have NO IPX
        # access-lists (not even the ones installed prior to
        # this)!
    }
}
#----- "access-profile merge" user -----
#
# With the 'merge' option, first all old access-lists are removed (as before),
# but then (almost) all AV pairs are uploaded and installed. This will allow
# for uploading any custom static routes, sap-filters, and so on, that the user
# may need in his or her profile. This needs to be used with care, as it leaves
# open the possibility of conflicting configurations.
#
#-----
user = pat_merge
{
    login = cleartext "welcome"
    chap = cleartext "welcome"
    service = exec
    {
        # This is the autocommand that executes when pat_merge logs in.
        autocmd = "access-profile merge"
    }
    service = ppp protocol = ip
    {
        # Put whatever access-lists, static routes, whatever
        # here.
        # If you leave this blank, the user will have NO IP
        # access-lists (not even the ones installed prior to
        # this)!
    }
}

```

```

        inacl#3="permit tcp any any"
        route#2="10.0.0.0 255.255.0.0"
        route#3="10.1.0.0 255.255.0.0"
        route#4="10.2.0.0 255.255.0.0"
    }
    service = ppp protocol = ipx
    {
        # Put whatever access-lists, static routes, whatever
        # here.
        # If you leave this blank, the user will have NO IPX
        # access-lists (not even the ones installed prior to
        # this)!
    }
}
#----- "access-profile replace" user -----
#
# With the 'replace' option, ALL old configuration is removed and ALL new
# configuration is installed.
#
# One caveat: access-profile checks the new configuration for address-pool and
# address AV pairs. As addresses cannot be renegotiated at this point, the
# command will fail (and complain) when it encounters such an AV pair.
# Such AV pairs are considered to be "invalid" for this context.
#-----
user = pat_replace
{
    login = cleartext
t
"
welcome
"

    chap = cleartext "welcome"
    service = exec
    {
        # This is the autocommand that executes when pat_replace logs in.
        autocmd = "access-profile replace"
    }
    service = ppp protocol = ip
    {
        # Put whatever access-lists, static routes, whatever
        # here.
        # If you leave this blank, the user will have NO IP
        # access-lists (not even the ones installed prior to
        # this)!
        inacl#3="permit tcp any any"
        inacl#4="permit icmp any any"
        route#2="10.10.0.0 255.255.0.0"
        route#3="10.11.0.0 255.255.0.0"
        route#4="10.12.0.0 255.255.0.0"
    }
    service = ppp protocol = ipx
    {
        # put whatever access-lists, static routes, whatever
        # here.
        # If you leave this blank, the user will have NO IPX
        # access-lists (not even the ones installed prior to
        # this)!
    }
}

```

## 例：自動二重認証

次に、自動二重認証が設定された設定ファイル全体の例を示します。自動二重認証に適用されるコンフィギュレーションコマンドは、2つのアスタリスク（\*\*）を使用した記述よりも優先されます。

```
Current configuration:
!
version 16.10
no service password-encryption
!
hostname myrouter
!
!
! **The following AAA commands are used to configure double authentication:
!
! **The following command enables AAA:
aaa new-model
! **The following command enables user authentication via the RADIUS AAA server:
!
aaa authentication login default none
aaa authentication ppp default group radius
! **The following command causes the remote user's authorization profile to be
! downloaded from the AAA server to the router when required:
!
aaa authorization network default group radius
!
enable password mypassword
!
ip host blue 172.21.127.226
ip host green 172.21.127.218
ip host red 172.21.127.114
ip domain-name example.com
ip name-server 172.16.2.75
!
!
interface GigabitEthernet0/0/0
 ip address 172.21.127.186 255.255.255.248
 no ip route-cache
 no ip mroute-cache
 no keepalive
 ntp disable
 no cdp enable
!
interface Virtual-Template1
 ip unnumbered loopback0
 no ip route-cache
 no ip mroute-cache
!
! **The following command specifies that device authentication occurs via PPP CHAP:
 ppp authentication chap
!
router eigrp 109
 network 172.21.0.0
 no auto-summary
!
ip default-gateway 172.21.127.185
no ip classless
ip route 172.21.127.114 255.255.255.255 172.21.127.113
! **Virtual profiles are required for double authentication to work:
virtual-profile virtual-template 1
```

```

dialer-list 1 protocol ip permit
no cdp run
! **The following command defines where the TACACS+ AAA server is:
tacacs server server1
address ipv4 172.16.57.35
! **The following command defines the key to use with TACACS+ traffic (required):
key mytacacskey
snmp-server community public RO
!
line con 0
  exec-timeout 0 0
  login authentication console
line aux 0
  transport input all
line vty 0 4
  exec-timeout 0 0
  password lab
!
end

```

## 認証設定の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	AAA Authentication	認証は、選択したセキュリティプロトコルに応じてログイン/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、および暗号化などのユーザーの識別方法を提供します。認証は、ユーザー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、ユーザーの識別を行う方法です。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。





## 第 4 章

# 認可の設定

AAA 認可を使用すると、ユーザーが利用できるサービスを制限できます。AAA 認可をイネーブルにすると、ネットワーク アクセス サーバーはユーザーのプロファイルから取得した情報を使用して、ユーザーの設定を設定します。このプロファイルは、ローカル ユーザー データベースまたはセキュリティ サーバーにあります。認可が完了すると、ユーザー プロファイルの情報で許可されているサービスであれば、ユーザーは要求したサービスに対するアクセス権を付与されます。

- [AAA 認可の前提条件 \(89 ページ\)](#)
- [認可の設定の概要 \(90 ページ\)](#)
- [認可の設定方法 \(94 ページ\)](#)
- [認可設定の例 \(97 ページ\)](#)
- [認可の設定に関する追加情報 \(100 ページ\)](#)
- [許可設定の機能履歴 \(100 ページ\)](#)

## AAA 認可の前提条件

名前付き方式リストを使用して認証を設定する前に、まず、次のタスクを実行する必要があります。

- ネットワーク アクセス サーバで AAA をイネーブルにします。
- AAA 認証を設定します。一般的に、認可は認証後に実行し、認証が適切に動作することに依存します。AAA 認証の設定方法については、「[認証の設定](#)」モジュールを参照してください。
- RADIUS または TACACS+ 認可を発行している場合、RADIUS または TACACS+ セキュリティ サーバーの特性を定義します。シスコのネットワーク アクセス サーバーを設定して RADIUS セキュリティサーバーと通信する方法の詳細については、「[RADIUS の設定](#)」の章を参照してください。シスコのネットワーク アクセス サーバーを設定して TACACS+ セキュリティサーバーと通信する方法の詳細については、「[TACACS+ の設定](#)」モジュールを参照してください。

- ローカル認可を発行している場合、**username** コマンドを使用して、特定のユーザーに関連付けられている権限を定義します。**username** コマンドに関する詳細情報については、『Cisco IOS Security Command Reference』を参照してください。

## 認可の設定の概要

### 認可の名前付き方式リスト

許可方式リストによって、許可の実行方法とこれらの方式の実行順序が定義されます。方式リストは、順に照会する認可方式（RADIUS または TACACS+ など）を記述した指定リストです。方式リストを使用すると、許可に使用するセキュリティプロトコルを1つ以上指定できるため、最初の方式が失敗した場合のバックアップシステムを確保できます。Cisco IOS XE ソフトウェアでは、特定のネットワークサービスについてユーザーを許可するために最初の方式が使用されます。その方式が応答しない場合、リストの次の方式が選択されます。このプロセスは、リストのいずれかの認可方式と通信に成功するか、定義されているすべての方式が試行されるまで継続されます。



- (注) Cisco IOS XE ソフトウェアでは、前の方式からの応答がない場合にのみ、リストの次の許可方式が試行されます。このサイクルの任意の時点で許可が失敗した場合（つまり、セキュリティサーバーまたはローカルユーザー名データベースからユーザーサービスの拒否応答が返される場合）、許可プロセスは停止し、その他の許可方式は試行されません。

方式リストは、要求した認可タイプに固有です。

- Commands** : ユーザが実行する EXEC モード コマンドに適用されます。コマンドの認可は、特定の特権レベルに関連付けられた、グローバル コンフィギュレーション コマンドなどのすべての EXEC モード コマンドについて、認可を試行します。
- EXEC** : ユーザ EXEC ターミナルセッションに関連付けられた属性に適用されます。
- Network** : ネットワーク接続に適用されます。これには、PPP、SLIP、または ARAP 接続が含まれます。
- Reverse Access** : リバース Telnet セッションに適用されます。

方式の指定リストを作成すると、指定した許可タイプに対して特定の許可方式リストが定義されます。

定義されると、方式リストを特定の回線またはインターフェイスに適用してから、定義済み方式のいずれかを実行する必要があります。唯一の例外は、デフォルトの方式リスト（「default」という名前）です。名前付き方式リストを指定せずに、特定の許可タイプ用の **aaa authorization** コマンドが発行されると、名前付き方式リストが明示的に定義されている場合を除いて、すべてのインターフェイスまたは回線にデフォルトの方式リストが自動的に適用されます。（定義



済みの方式リストは、デフォルトの方式リストに優先します)。デフォルトの方式リストが定義されていない場合、デフォルトでローカル認可が実行されます。

## AAA 認可方式

AAA は 5 種類の認可方式をサポートしています。

- **TACACS+** : ネットワーク アクセス サーバは、TACACS+ セキュリティ デーモンと認可情報を交換します。TACACS+ 認可は、属性値ペアを関連付けることでユーザに特定の権限を定義します。属性ペアは適切なユーザとともに TACACS+ セキュリティ サーバのデータベースに保存されます。
- **If-Authenticated** : ユーザが認証に成功した場合、ユーザは要求した機能にアクセスできます。
- **None** : ネットワーク アクセス サーバは、認可情報を要求しません。認可は、この回線/インターフェイスで実行されません。
- **Local** : ルータまたはアクセスサーバは、**username** コマンドの定義に従って、ローカルデータベースに問い合わせ、たとえばユーザーに固有の権限を許可します。ローカルデータベースを介して制御できるのは、一部の機能だけです。
- **RADIUS** : ネットワーク アクセス サーバは RADIUS セキュリティ サーバからの認可情報を要求します。RADIUS 認可では、属性を関連付けることでユーザーに固有の権限を定義します。属性は適切なユーザーとともに RADIUS サーバ上のデータベースに保存されます。



(注) CSCuc32663 では、パスワードおよび認可ログは、TACACS+、LDAP、または RADIUS セキュリティ サーバへ送信される前にマスクされます。マスクされていない情報を TACACS+、LDAP または RADIUS セキュリティサーバに送信するには、**aaa authorization commands visible-keys** コマンドを使用します。

## 認可方式

ネットワークアクセスサーバから TACACS+ セキュリティサーバを介して認可情報を要求するには、**group tacacs+ method** キーワードを指定して **aaa authorization** コマンドを使用します。TACACS+ セキュリティサーバを使用して認可を設定する詳細な方法については、「TACACS+ の設定」の章を参照してください。TACACS+ サーバが、PPP や ARA などのネットワークサービスの使用を認可できるようにする例については、「TACACS 認可の例」を参照してください。

ユーザーが認証済みであれば、要求した機能へのアクセスを許可するには、**if-authenticated method** キーワードを指定して **aaa authorization** コマンドを使用します。この方式を選択する場合、すべての要求した機能は、認証済みユーザーに自動的に許可されます。

特定のインターフェイスまたは回線から認可を実行したくない場合があります。指定した回線またはインターフェイスで許可動作を停止するには、**none method** キーワードを使用します。この方式を選択すると、すべてのアクションについて認可はディセーブルになります。

ローカル許可を選択するには（つまり、ルータまたはアクセスサーバがローカルユーザーデータベースに問い合わせ、ユーザーが使用可能な機能を決定する場合）、**local method** キーワードを指定して **aaa authorization** コマンドを使用します。ローカル許可に関連する機能は、**username** グローバル コンフィギュレーション コマンドを使用して定義します。許可されている機能のリストについては、「認証の設定」の章を参照してください。

ネットワークアクセスサーバから RADIUS セキュリティサーバを介して許可を要求するには、**radius method** キーワードを使用します。RADIUS セキュリティサーバを使用して認可を設定する詳細な方法については、「RADIUS の設定」の章を参照してください。

ネットワークアクセスサーバから RADIUS セキュリティサーバを介して許可を要求するには、**group radius method** キーワードを指定して **aaa authorization** コマンドを使用します。RADIUS セキュリティサーバを使用して認可を設定する詳細な方法については、「RADIUS の設定」の章を参照してください。RADIUS サーバがサービスを認可できるようにする例については、「RADIUS 認可の例」を参照してください。



- (注) SLIP の認可方式リストは、関連インターフェイスで PPP に設定されているすべての方式に従います。特定のインターフェイスに定義および適用されるリストがない場合（または PPP 設定が指定されていない場合）、認可のデフォルト設定が適用されます。

## 方式リストとサーバグループ

サーバグループは、方式リストに使用する既存の RADIUS または TACACS+ サーバ ホストをグループ化する方法の 1 つです。次の図に、4 台のセキュリティサーバ（R1 と R2 は RADIUS サーバ、T1 と T2 は TACACS+ サーバ）が設置された一般的な AAA ネットワーク設定を示します。R1 と R2 で RADIUS サーバのグループを構成します。T1 と T2 で TACACS+ サーバのグループを構成します。

サーバグループを使用して、設定したサーバホストのサブセットを指定し、特定のサービスに使用します。たとえば、サーバグループを使用すると、R1 および R2 を別のサーバグループとして定義し、T1 および T2 を別のサーバグループとして定義できます。つまり、R1 と T1 を方式リストに指定できるか、または R2 と T2 を方式リストに指定できます。そのため、RADIUS および TACACS+ のリソースを割り当てる場合の柔軟性が高くなります。

サーバグループには、1 台のサーバに対して複数のホストエントリを含めることができます。エントリごとに固有の識別情報を設定します。固有の識別情報は、IP アドレスと UDP ポート番号の組み合わせで構成されます。これにより、RADIUS ホストとして定義されているさまざまなポートが、固有の AAA サービスを提供できるようになります。つまり、この固有識別情報を使用して、ある IP アドレスに位置する 1 台のサーバ上に複数の UDP ポートが存在する場合、それぞれの UDP ポートに対して RADIUS 要求を送信できます。1 台の RADIUS サーバ上にある異なる 2 つのホストエントリが 1 つのサービス（認可など）に設定されている場合、設定されている 2 番目のホストエントリは最初のホストエントリのフェールオーバー バック

アップとして動作します。この例の場合、最初のホスト エントリがアカウントिंग サービスの提供に失敗すると、同じデバイスに設定されている2番目のホスト エントリを使用してアカウントング サービスを提供するように、ネットワーク アクセス サーバーが試行します（試行される RADIUS ホスト エントリの順番は、設定されている順序に従います）。

サーバー グループの設定および DNIS 番号に基づくサーバー グループの設定の詳細については、「RADIUS の設定」または「TACACS+ の設定」の章を参照してください。

## AAA 認可タイプ

Cisco IOS XE ソフトウェアは、5 種類の認可をサポートしています。

- **Commands** : ユーザが実行する EXEC モード コマンドに適用されます。コマンドの認可は、特定の特権レベルに関連付けられた、グローバル コンフィギュレーション コマンドなどのすべての EXEC モード コマンドについて、認可を試行します。
- **EXEC** : ユーザ EXEC ターミナルセッションに関連付けられた属性に適用されます。
- **Network** : ネットワーク接続に適用されます。これには、PPP、SLIP、または ARAP 接続が含まれます。
- **Reverse Access** : リバース Telnet セッションに適用されます。
- **Configuration** : AAA サーバからのコンフィギュレーションのダウンロードに適用されません。
- **IP Mobile** : IP モバイル サービスの認可に適用されます。

## 承認タイプ

名前付き認可方式リストは、指定される認可の種類によって変わります。

ユーザー別に固有のセキュリティポリシーを適用する認可をイネーブルにする方式リストを作成するには、**auth-proxy** キーワードを使用します。認証プロキシ機能の詳細については、このガイドの「Traffic Filtering and Firewalls」の部の「Configuring Authentication Proxy」を参照してください。

すべてのネットワーク関連サービス要求（SLIP、PPP、PPP NCP、ARAP など）について認可を有効にする方式リストを作成するには、**network** キーワードを使用します。

ユーザーが EXEC シェルを実行できるかどうかを認可で決定できるように方式リストを作成するには、**exec** キーワードを使用します。

特定の特権レベルに関連付けられた個々の EXEC コマンドについて認可を有効にする方式リストを作成するには、**commands** キーワードを使用します。これにより、指定されたコマンドレベル（0～15）に関連付けられているすべてのコマンドを認可できます。

リバース Telnet 機能について認可を有効にする方式リストを作成するには、**reverse-access** キーワードを使用します。

Cisco IOS XE ソフトウェアでサポートされている認可のタイプの詳細については、「AAA 認可タイプ」を参照してください。

## 認可の属性値ペア

RADIUS および TACACS+ の認可はいずれも、セキュリティサーバーのデータベースに保存されている属性を処理することで、ユーザーに固有の権限を定義します。RADIUS と TACACS+ のいずれも、属性はセキュリティサーバーに定義され、ユーザーに関連付けられ、ユーザーの接続に適用されるネットワーク アクセス サーバーに送信されます。

サポートされる RADIUS 属性のリストについては、「RADIUS 属性の概要および RADIUS IETF 属性」の章を参照してください。サポートされる TACACS+ の AV ペアのリストについては、「TACACS+ の設定」の章を参照してください。

## 認可の設定方法

### 名前付き方式リストによる AAA 認可の設定

名前付き方式リストを使用して AAA 認可を設定するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

#### 手順の概要

1. Device(config)# **aaa authorization** {**auth-proxy** | **network** | **exec** | **commands level** | **reverse-access** | **configuration** | **ipmobile**} {**default** | *list-name*} [*method1* [*method2...*]]
2. 次のいずれかを実行します。
  - Device(config)# **line** [**aux** | **console** | **tty** | **vty**] *line-number* [*ending-line-number*]
  - Device(config)# **interface** *interface-type* *interface-number*
3. 次のいずれかを実行します。
  - Device(config-line)# **authorization** {**arap** | **commands level** | **exec** | **reverse-access**} {**default** | *list-name*}
  - Device(config-line)# **ppp authorization** {**default** | *list-name*}

#### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	Device(config)# <b>aaa authorization</b> { <b>auth-proxy</b>   <b>network</b>   <b>exec</b>   <b>commands level</b>   <b>reverse-access</b>   <b>configuration</b>   <b>ipmobile</b> } { <b>default</b>   <i>list-name</i> } [ <i>method1</i> [ <i>method2...</i> ]]	特定の認可タイプの認可方式リストを作成し、認可をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 2	次のいずれかを実行します。 <ul style="list-style-type: none"> <li>• Device(config)# <b>line</b> [aux   console   tty   vty] <i>line-number</i> [<i>ending-line-number</i>]</li> <li>• Device(config)# <b>interface</b> <i>interface-type</i> <i>interface-number</i></li> </ul>	認可方式リストを適用する回線について、ライン コンフィギュレーション モードを開始します。 または、認可方式リストを適用するインターフェイスについて、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかを実行します。 <ul style="list-style-type: none"> <li>• Device(config-line)# <b>authorization</b> {arap   <b>commands</b> <i>level</i>   <b>exec</b>   <b>reverse-access</b>} {<b>default</b>   <i>list-name</i>}</li> <li>• Device(config-line)# <b>ppp authorization</b> {<b>default</b>   <i>list-name</i>}</li> </ul>	1つの回線または複数回線に認可リストを適用します。 または、1つのインターフェイスまたは複数インターフェイスに認可リストを適用します。

## グローバル コンフィギュレーション コマンドの認可のディセーブル化

**commands** キーワードを指定して **aaa authorization** コマンドを使用すると、その特権レベルに関連付けられているすべての EXEC モードコマンド（グローバル コンフィギュレーション コマンドを含む）に対して許可が試行されます。一部の EXEC レベル コマンドと同じコンフィギュレーション コマンドもあるため、認可プロセスが混乱する可能性があります。**no aaa authorization config-commands** を使用すると、ネットワーク アクセス サーバーがコンフィギュレーション コマンド認可の試行を停止します。

すべてのグローバル コンフィギュレーション コマンドについて AAA 認可をディセーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Device (config) # <b>no aaa authorization config-commands</b>	すべてのグローバル コンフィギュレーション コマンドについて認可をディセーブルにします。

コンソール上で AAA 認可をディセーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。



- (注) デフォルトでコンソールの AAA 認可はディセーブルです。コンソールで AAA 許可が有効になっている場合は、AAA の設定段階で **no aaa authorization console** コマンドを設定して無効にします。ユーザー認証用のコンソールでは AAA をディセーブルにする必要があります。

コマンド	目的
Device (config) # <b>no aaa authorization console</b>	コンソールでの認証を無効にします。

## リバース Telnet の認可の設定

Telnet は、リモート ターミナル接続に使用される標準ターミナルエミュレーションプロトコルです。通常、ネットワーク アクセス サーバーに（主にダイヤルアップ接続経由で）ログインし、Telnet を使用してそのネットワーク アクセス サーバーから他のネットワーク デバイスにアクセスします。ただし、場合によっては、リバース Telnet セッションを確立する必要があります。リバース Telnet セッションでは、反対方向の Telnet 接続（つまり、ネットワーク 内部から、ネットワーク 周辺にあるネットワーク アクセス サーバーに対する接続）が確立されます。その接続によって、ネットワーク アクセス サーバーに接続しているモデムや他のデバイスへのアクセスを取得します。リバース Telnet は、ユーザーがネットワーク アクセス サーバーに接続されているモデム ポートに Telnet を送信できるようにすることで、ユーザーにダイヤルアウト機能を提供します。

リバース Telnet を介してアクセスできるポートのアクセス権を制御することが重要です。適切に制御しないと、たとえば、不正ユーザーがモデムに自由にアクセスし、着信コールをトラップして迂回させたり、不正な宛先にコールを送信したりする可能性があります。

リバース Telnet 時の認証は、Telnet 用の標準の AAA ログイン手順を介して実行されます。通常、Telnet またはリバース Telnet セッションを確立するには、ユーザーはユーザー名とパスワードを指定する必要があります。リバース Telnet 認可は、認証に加えて認可を必須にすることで、追加（任意）レベルのセキュリティを提供します。リバース Telnet 認可をイネーブルにすることで、標準の Telnet ログイン手順を介してユーザー認証を完了した後に、RADIUS または TACACS+ を使用して、そのユーザーが非同期ポートにリバース Telnet アクセスを実行できるかどうかを認可できます。

リバース Telnet 認可には次の利点があります。

- リバース Telnet アクティビティを実行しているユーザーに、リバース Telnet を使用して特定の非同期ポートにアクセスする権限を付与することで、追加レベルの保護を実現しています。
- リバース Telnet 認可を管理できる（アクセス リスト以外の）代替方式があります。

ネットワーク アクセス サーバーが TACACS+ または RADIUS サーバーからの認可情報を要求するように設定してから、ユーザーによるリバース Telnet セッションの確立を許可するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
Device(config)# <b>aaa authorization reverse-access</b> method1 [method2 ...]	ネットワーク アクセス サーバーが認可情報を要求するように設定してから、ユーザーによるリバース Telnet セッションの確立を許可します。

この機能によって、ネットワーク アクセス サーバーは、セキュリティ サーバー（RADIUS または TACACS+）からリバース Telnet 認可情報を要求できます。セキュリティ サーバー上のユーザーに固有のリバース Telnet 特権を設定する必要があります。

## 認可設定の例

### 例：TACACS 認可

次に、TACACS+ サーバーを使用して、PPP や ARA などのネットワーク サービスの使用を認可する例を示します。TACACS+ サーバーが使用不能の場合、または認可プロセス中にエラーが発生した場合、フォールバック方式 (none) はすべての認可要求を許可することです。

```
aaa authorization network default group tacacs+ none
```

次に、TACACS+ を使用してネットワークの認可を許可する例を示します。

```
aaa authorization network default group tacacs+
```

次に、同じ認可を提供し、「mci」と「att」というアドレス プールも作成する例を示します。

```
aaa authorization network default group tacacs+
ip address-pool local
ip local-pool mci 172.16.0.1 172.16.0.255
ip local-pool att 172.17.0.1 172.17.0.255
```

これらのアドレス プールは、TACACS デーモンによって選択できます。デーモンの設定例を次に示します。

```
user = mci_customer1 {
  login = cleartext "some password"
  service = ppp protocol = ip {
    addr-pool=mci
  }
}
user = att_customer1 {
  login = cleartext "some other password"
  service = ppp protocol = ip {
    addr-pool=att
  }
}
```

### 例：RADIUS 許可

次に、RADIUS を使用して認可を行うようにルータを設定する方法の例を示します。

```
aaa new-model
aaa authorization exec default group radius if-authenticated
aaa authorization network default group radius
radius-server host ip
radius-server key
```

この RADIUS 認可設定のサンプル行は、次のように定義されます。

- **aaa authorization exec default group radius if-authenticated** コマンドで、ネットワークアクセスサーバーが RADIUS サーバーに接続して、ユーザーのログイン時にユーザーが EXEC シェルを起動する権限があるかどうかを決定するように設定します。ネットワークアクセ

スルーターが RADIUS サーバーに接続するときにエラーが発生した場合、フォールバック方式は、ユーザーが適切に認証されていると CLI の起動を許可します。

返される RADIUS 情報を使用して、その接続に適用される autocommand または接続アクセスリストを指定できます。

- **aaa authorization network default group radius** コマンドにより、RADIUS を介するネットワーク許可を設定します。この操作は、アドレス割り当ての管理、アクセスリストのアプリケーション、および他の多様なユーザー別の数量に使用できます。



(注) この例ではフォールバック方式を指定していないため、何らかの理由で認可に失敗すると、RADIUS サーバーからの応答はありません。

## 例：リバース Telnet 許可

次に、ネットワーク アクセス サーバーが TACACS+ セキュリティ サーバーから認可情報を要求してから、ユーザーによるリバース Telnet セッションの確立を許可する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication login default group tacacs+
Device(config)# aaa authorization reverse-access default group tacacs+
Device(config)# tacacs server server1
Device(config-server-tacacs)# address ipv4 172.31.255.0
Device(config-server-tacacs)# timeout 90
Device(config-server-tacacs)# key sharedkey
Device(config-server-tacacs)# end
```

この TACACS+ リバース Telnet 認可設定のサンプル行は、次のように定義されます。

- **aaa new-model** コマンドは AAA を有効にします。
- **aaa authentication login default group tacacs+** コマンドで、ログイン時のユーザー認証のデフォルト方式として TACACS+ を指定します。
- リバース Telnet セッションを確立しようとしているときに、**aaa authorization reverse-access default group tacacs+** コマンドで、ユーザー認可の方式として TACACS+ を指定します。
- **tacacs server** コマンドで、TACACS+ サーバーを識別します。
- **timeout** コマンドで、ネットワーク アクセス サーバーが TACACS+ サーバーの応答を待機する期間を設定します。
- **key** コマンドで、ネットワーク アクセス サーバーと TACACS+ デーモン間のすべての TACACS+ 通信に使用される暗号キーを定義します。

次に、ネットワーク アクセス サーバー「maple」上のポート tty2、およびネットワーク アクセス サーバー「oak」上のポート tty5 に対するリバース Telnet アクセス権をユーザー pat に付与する汎用の TACACS+ サーバーを設定する例を示します。



```

user = pat
  login = cleartext lab
  service = raccess {
    port#1 = maple/tty2
    port#2 = oak/tty5
  }

```



- (注) この例では、「maple」と「oak」には、DNS 名またはエイリアスではなく、ネットワーク アクセス サーバーのホスト名が設定されています。

次に、TACACS+ サーバー (CiscoSecure) を設定して、ユーザー pat にリバース Telnet アクセス権を付与する例を示します。

```

user = pat
  profile_id = 90
  profile_cycle = 1
  member = Tacacs_Users
  service=shell {
    default cmd=permit
  }
  service=raccess {
    allow "c2511e0" "tty1" ".*"
    refuse ".*" ".*" ".*"
    password = clear "goaway"
  }

```



- (注) CiscoSecure は、バージョン 2.1(x)～バージョン 2.2(1) のコマンドライン インターフェイスを使用して、リバース Telnet だけをサポートしています。

空の「service=raccess {}」句は、リバース Telnet のネットワーク アクセス サーバー ポートに対して無条件のアクセス権をユーザーに許可しています。「service=raccess」句が存在しない場合、ユーザーはリバース Telnet のすべてのポートに対してアクセスを拒否されます。

TACACS+ の設定の詳細については、「TACACS+ の設定」の章を参照してください。CiscoSecure の設定の詳細については、『CiscoSecure Access Control Server User Guide』の version 2.1(2) 以降を参照してください。

次に、ネットワーク アクセス サーバーが RADIUS セキュリティ サーバーから認可を要求してから、ユーザーによるリバース Telnet セッションの確立を許可する例を示します。

```

Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication login default group radius
Device(config)# aaa authorization reverse-access default group radius
Device(config)# radius server ip
Device(config-radius-server)# key sharedkey
Device(config-radius-server)# address ipv4 172.31.255.0 auth-port 1645 acct-port 1646
Device(config-radius-server)# end

```

この RADIUS リバース Telnet 認可設定のサンプル行は、次のように定義されます。

- **aaa new-model** コマンドは AAA を有効にします。

- **aaa authentication login default group radius** コマンドで、ログイン時のユーザー認証のデフォルト方式として RADIUS を指定します。
- リバース Telnet セッションを確立しようとしているときに、**aaa authorization reverse-access default group radius** コマンドで、ユーザー認可の方式として RADIUS を指定します。
- **radius** コマンドで、RADIUS サーバーを指定します。
- **key** コマンドで、ネットワークアクセスサーバーと RADIUS デーモン間のすべての RADIUS 通信に使用される暗号キーを定義します。

次に、ネットワークアクセスサーバー「maple」上のポート tty2 で、ユーザー「pat」にリバース Telnet アクセス権を付与する RADIUS サーバーに要求を送信する例を示します。

```
Username = "pat"
Password = "goaway"
User-Service-Type = Shell-User
cisco-avpair = "raccess:port#1=maple/tty2"
```

構文「raccess:port=any/any」で、リバース Telnet のネットワーク アクセス サーバー ポートに対して無条件のアクセス権をユーザーに許可します。「raccess:port={nasname }/{tty number }」句がユーザー プロファイルにない場合、ユーザーはすべてのポートでリバース Telnet へのアクセスを拒否されます。

RADIUS の設定の詳細については、「RADIUS の設定」の章を参照してください。

## 認可の設定に関する追加情報

### シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## 許可設定の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	AAA 許可	AAA 認可を使用すると、ユーザーが利用できるサービスを制限できます。AAA 認可をイネーブルにすると、ネットワーク アクセス サーバーはユーザーのプロファイルから取得した情報を使用して、ユーザーの設定を設定します。このプロファイルは、ローカルユーザー データベースまたはセキュリティ サーバーにあります。認可が完了すると、ユーザー プロファイルの情報で許可されているサービスであれば、ユーザーは要求したサービスに対するアクセス権を付与されます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。





## 第 5 章

# アカウントティングの設定

AAA アカウントティング機能を使用すると、ユーザーがアクセスするサービス、およびユーザーが消費するネットワーク リソース量を追跡できます。AAA アカウントティングをイネーブルにすると、ネットワーク アクセス サーバーから TACACS+ または RADIUS セキュリティ サーバー（実装しているセキュリティ手法によって異なります）に対して、アカウントティング レコードの形式でユーザー アクティビティがレポートされます。各アカウントティング レコードにはアカウントティングの Attribute-Value (AV) ペアが含まれ、レコードはセキュリティ サーバーに格納されます。このデータを分析して、ネットワーク管理、クライアント課金、および監査に利用できます。

- [アカウントティングを設定するための前提条件](#)（103 ページ）
- [アカウントティングの設定の制約事項](#)（104 ページ）
- [アカウントティングの設定に関する情報](#)（104 ページ）
- [AAA アカウントティングの設定方法](#)（119 ページ）
- [AAA アカウントティングの設定例](#)（129 ページ）
- [アカウントティングの設定に関するその他の参考資料](#)（133 ページ）
- [アカウントティングの設定の機能履歴](#)（134 ページ）

## アカウントティングを設定するための前提条件

次のタスクを実行してから、名前付き方式リストを使用してアカウントティングを設定します。

- ネットワークアクセスサーバで AAA を有効にするには、グローバル コンフィギュレーション モードで **aaa new-model** コマンドを使用します。
- RADIUS または TACACS+ 認可が発行されている場合、RADIUS または TACACS+ セキュリティ サーバの特性を定義します。Cisco ネットワーク アクセス サーバを設定して RADIUS セキュリティ サーバと通信する方法の詳細については、「RADIUS の設定」モジュールを参照してください。Cisco ネットワーク アクセス サーバを設定して TACACS+ セキュリティ サーバと通信する方法の詳細については、「TACACS+ の設定」モジュールを参照してください。

## アカウントティングの設定の制約事項

- アカウントティング情報は、最大 4 台の AAA サーバにのみ同時送信できます。
- Service Selection Gateway (SSG) システムの場合、**aaa accounting network broadcast** コマンドを実行すると、**start-stop** アカウントティングレコードのみがブロードキャストされます。**ssg accounting interval** コマンドを使用して中間アカウントティングレコードを設定する場合、中間アカウントティングレコードは、設定したデフォルト RADIUS サーバーにのみ送信されます。

### トピック 2.1

## アカウントティングの設定に関する情報

### アカウントティングの名前付き方式リスト

認証および認可方式リストと同様に、アカウントティングの方式リストには、アカウントティングの実行方法とその方式を実行するシーケンスが定義されています。

アカウントティングの名前付き方式リストには、特定のセキュリティプロトコルを指定し、アカウントティングサービスの特定の行またはインターフェイスに使用できます。唯一の例外は、デフォルトの方式リスト（「default」という名前）です。デフォルトの方式リストは、明示的に定義された名前付きの方式リストを持つインターフェイスを除くすべてのインターフェイスに自動的に適用されます。定義済みの方式リストは、デフォルトの方式リストに優先します。

方式リストは、シーケンスで照会されるアカウントティング方式（RADIUS、TACACS+ など）を説明する単なる名前付きリストです。方式リストでは、アカウントティングに1つまたは複数のセキュリティプロトコルを指定できます。そのため、最初の方式が失敗した場合に備えてアカウントティングのバックアップシステムを確保できます。Cisco IOS ソフトウェアでは、リストされている最初の方式を使用して、アカウントティングをサポートします。その方式が応答しない場合、リストされている次のアカウントティング方式が選択されます。このプロセスは、リストのいずれかのアカウントティング方式と通信に成功するか、定義されているすべての方式が試行されるまで継続されます。



- (注) Cisco IOS ソフトウェアでは、前の方式で応答が得られない場合にのみ、リストされている次のアカウントティング方式でアカウントティングが試行されます。このサイクルの任意の時点でアカウントティングが失敗した場合（つまり、セキュリティサーバーからユーザーアクセスの拒否応答が返される場合）、アカウントティングプロセスは停止し、その他のアカウントティング方式は試行されません。

アカウントティング方式リストは、要求されるアカウントティングの種類によって変わります。AAA は、次の 7 種類のアカウントティングをサポートしています。

- **Network** : パケットやバイトカウントなど、すべての PPP、SLIP、または ARAP セッションに関する情報を提供します。
- **EXEC** : ネットワーク アクセス サーバーのユーザー EXEC ターミナルセッションに関する情報を提供します。
- **Commands** : ユーザーが発行する EXEC モード コマンドに関する情報を提供します。コマンドアカウントティングは、特定の特権レベルに関連付けられた、グローバル コンフィギュレーション コマンドなどのすべての EXEC モード コマンドについて、アカウントティング レコードを生成します。
- **Connection** : Telnet、ローカルエリア トランスポート (LAT)、TN3270、パケット アセンブラ/ディスクアセンブラ (PAD)、rlogin などのネットワーク アクセス サーバーから行われたすべてのアウトバンド接続に関する情報を出力します。
- **System** : システムレベルのイベントに関する情報を提供します。
- **Resource** : ユーザー認証に成功したコールの「開始」および「終了」レコードを提供します。また、認証に失敗したコールの「終了」レコードを提供します。
- **VRRS** : Virtual Router Redundancy Service (VRRS) に関する情報を提供します。



- (注) システム アカウントティングは、名前付きアカウントティング リストを使用しません。システム アカウントティングのデフォルト リストだけを定義できます。

この場合も、名前付き方式リストが作成されると、指定したアカウントティングタイプのアカウ  
ンティング方式のリストが定義されます。

アカウントティング方式リストを特定の回線またはインターフェイスに適用してから、定義済み  
方式のいずれかを実行する必要があります。唯一の例外は、デフォルトの方式リスト (「default」  
という名前) です。名前付き方式リストを指定せずに、特定のアカウントティングタイプに対し  
て **aaa accounting** コマンドを発行すると、明示的に名前付き方式リストが定義されている場合  
を除き、すべてのインターフェイスまたは回線にデフォルトの方式リストが自動的に適用され  
ます (定義した方式リストは、デフォルトの方式リストよりも優先されます)。デフォルトの  
方式リストが定義されていない場合、アカウントティングは実行されません。

ここでは、次の内容について説明します。

## 方式リストとサーバグループ

サーバ グループは、方式リストに使用する既存の RADIUS または TACACS+ サーバ ホス  
トをグループ化する方法の 1 つです。次の図に、4 台のセキュリティ サーバ (R1 と R2 は  
RADIUS サーバ、T1 と T2 は TACACS+ サーバ) が設置された一般的な AAA ネットワーク 設  
定を示します。R1 と R2 は RADIUS サーバのグループから構成されます。T1 と T2 は  
TACACS+ サーバのグループから構成されます。

Cisco IOS ソフトウェア、RADIUS サーバ、および TACACS+ サーバの設定はグローバルです。サーバー グループを使用して、設定済みのサーバー ホストのサブセットを指定できます。このようなサーバー グループは、特定のサービスに使用できます。たとえば、サーバー グループを使用すると、R1 と R2 を個別のサーバー グループ (SG1 と SG2) として定義し、T1 と T2 を個別のサーバー グループ (SG3 と SG4) として定義できます。つまり、R1 と T1 (SG1 と SG3) または R2 と T2 (SG2 と SG4) を方式リストに指定することができます。そのため、RADIUS および TACACS+ のリソースを割り当てる場合の柔軟性が高くなります。

サーバーグループには、1 台のサーバに対して複数のホストエントリを含めることができます。エントリごとに固有の識別情報を設定します。固有の識別情報は、IP アドレスと UDP ポート番号の組み合わせで構成されます。これにより、RADIUS ホストとして定義されているさまざまなポートが、固有の AAA サービスを提供できるようになります。つまり、この固有識別情報を使用して、1 台のサーバー上に複数の UDP ポートが存在する場合、同じ IP アドレスからそれぞれの UDP ポートに対して RADIUS 要求を送信できます。1 台の RADIUS サーバ上にある異なる 2 つのホストエントリが 1 つのサービス (アカウントングなど) に設定されている場合、設定されている 2 番目のホスト エントリは最初のホストエントリのフェールオーバーバックアップとして動作します。この例を使用して、最初のホストエントリがアカウントングサービスの提供に失敗した場合、ネットワーク アクセス サーバーは、同じデバイスに設定されている 2 番目のホストエントリに対してアカウントングサービスを試行します (RADIUS ホストエントリは、設定順に試行されます)。

サーバーグループの設定、および着信番号識別サービス (DNIS) 番号に基づくサーバーグループの設定の詳細については、『Cisco IOS Security Configuration Guide: Securing User Services』の「Configuring RADIUS」または「Configuring TACACS+」モジュールを参照してください。

## AAA アカウンティング方式

Cisco IOS ソフトウェアはアカウントングについて次の 2 つの方式をサポートします。

- TACACS+ : ネットワーク アクセス サーバーは、アカウントング レコードの形式で TACACS+ セキュリティ サーバーに対してユーザー アクティビティを報告します。各アカウントング レコードは、アカウントング AV ペアが含まれ、セキュリティ サーバー上で保管されます。
- RADIUS : ネットワーク アクセス サーバーは、アカウントング レコードの形式で RADIUS セキュリティ サーバーに対してユーザー アクティビティを報告します。各アカウントング レコードは、アカウントング AV ペアが含まれ、セキュリティ サーバー上で保管されます。



(注) CSCuc32663 では、パスワードおよびアカウントング ログは、TACACS+ または RADIUS セキュリティ サーバーへ送信される前にマスクされます。マスクされていない情報を TACACS+ または RADIUS セキュリティ サーバーに送信するには、**aaa accounting commands visible-keys** コマンドを使用します。



## アカウントティングレコードの種類

最小限のアカウントティングの場合、**stop-only** キーワードを使用します。このキーワードによって、要求されたユーザープロセスの終了時に、終了レコードアカウントティング通知を送信するよう、指定した方式（**RADIUS** または **TACACS+**）に指示します。詳細なアカウントティング情報が必要な場合、**start-stop** キーワードを使用して、要求されたイベントの開始時には開始アカウントティング通知、そのイベントの終了時には修理用アカウントティング通知を送信します。この回線またはインターフェイスですべてのアカウントティング アクティビティを終了するには、**none** キーワードを使用します。

## アカウントティング方式

次の表に、サポートされるアカウントティング方式を示します。

表 13: AAA アカウントティング方式

キーワード	Description
<b>group radius</b>	アカウントティングにすべての RADIUS サーバーのリストを使用します。
<b>group tacacs+</b>	アカウントティングにすべての TACACS+ サーバーのリストを使用します。
<b>group</b> <i>group-name</i>	<i>group-name</i> サーバー グループで定義したように、アカウントティングのための RADIUS サーバーまたは TACACS+ サーバーのサブセットを使用します。

method 引数は、認証アルゴリズムが試行する実際の方式を指します。追加の認証方式は、直前の方式で（失敗した場合ではなく）エラーが返された場合にのみ使用されます。他のすべての方式がエラーを返しても、認証に成功したことを指定するには、コマンドで追加の方式を指定します。たとえば、TACACS+ 認証がエラーを返す場合に認証のバックアップ方式として RADIUS を指定する `acct_tac1` という方式リストを作成するには、次のコマンドを入力します。

```
aaa accounting network acct_tac1 stop-only group tacacs+ group radius
```

名前付きリストが `aaa accounting` コマンドに指定されていない場合に使用するデフォルトのリストを作成するには、**default** キーワードの後ろにデフォルト状況で使用される方式を指定します。デフォルト認証方式リストは、自動的にすべてのインターフェイスに適用されます。

たとえば、ログイン時のユーザー認証のデフォルト方式として RADIUS を指定するには、次のコマンドを入力します。

```
aaa accounting network default stop-only group radius
```

AAA アカウントティングは、次の方式をサポートします。

- **group tacacs** : ネットワーク アクセス サーバーからアカウントティング情報を TACACS+ セキュリティサーバーに送信するようにするには、**group tacacs+** 方式キーワードを使用します。

- **group radius** : ネットワーク アクセス サーバーからアカウントティング情報を RADIUS セキュリティサーバーに送信するようにするには、**group radius** 方式キーワードを使用します。



(注) SLIP のアカウントティング方式リストは、関連インターフェイスで PPP に設定されているすべての方式に従います。特定のインターフェイスに定義および適用されるリストがない場合（または PPP 設定が指定されていない場合）、アカウントティングのデフォルト設定が適用されます。

- **group group-name** : RADIUS または TACACS+ サーバーのサブセットを指定して、アカウントティング方式として使用するには、**group group-name** 方式を指定して **aaa accounting** コマンドを使用します。グループ名とそのグループのメンバを指定して定義するには、**aaa group server** コマンドを使用します。たとえば、**aaa group server** コマンドを使用して、**group loginrad** のメンバを最初に定義します。

```
aaa group server radius loginrad
server 172.16.2.3
server 172.16.2.17
server 172.16.2.32
```

このコマンドにより、172.16.2.3、172.16.2.17、172.16.2.32 の RADIUS サーバーが **group loginrad** のメンバとして指定されます。

他の方式リストが定義されていない場合、ネットワークアカウントティングの方式として **group loginrad** を指定するには、次のコマンドを入力します。

```
aaa accounting network default start-stop group loginrad
```

アカウントティング方式としてグループ名を使用するには、事前に RADIUS または TACACS+ セキュリティ サーバーとの通信をイネーブルにする必要があります。

## AAA アカウンティング タイプ

### ネットワーク アカウンティング

ネットワーク アカウンティングは、パケットやバイト カウントなど、すべての PPP、SLIP、または ARAP セッションに関する情報を提供します。

次に、EXEC セッションを介して着信する PPP ユーザの RADIUS ネットワーク アカウンティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:44:45 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 5
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "562"
Acct-Status-Type = Start
```

```

Acct-Authentic = RADIUS
Service-Type = Exec-User
Acct-Session-Id = "0000000D"
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identififier = "172.16.25.15"

Wed Jun 27 04:45:00 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 5
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "562"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
Service-Type = Framed
Acct-Session-Id = "0000000E"
Framed-IP-Address = "10.1.1.2"
Framed-Protocol = PPP
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identififier = "172.16.25.15"

Wed Jun 27 04:47:46 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 5
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "562"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Framed
Acct-Session-Id = "0000000E"
Framed-IP-Address = "10.1.1.2"
Framed-Protocol = PPP
Acct-Input-Octets = 3075
Acct-Output-Octets = 167
Acct-Input-Packets = 39
Acct-Output-Packets = 9
Acct-Session-Time = 171
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identififier = "172.16.25.15"

Wed Jun 27 04:48:45 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 5
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "408"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Exec-User
Acct-Session-Id = "0000000D"
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identififier = "172.16.25.15"

```

次に、最初にEXECセッションを開始したPPPユーザのTACACS+ネットワークアカウントティングレコードに含まれる情報の例を示します。

```

Wed Jun 27 04:00:35 2001 172.16.25.15  username1  tty4  562/4327528
starttask_id=28      service=shell
Wed Jun 27 04:00:46 2001 172.16.25.15  username1  tty4  562/4327528  starttask_id=30
addr=10.1.1.1      service=ppp

```

```

Wed Jun 27 04:00:49 2001 172.16.25.15  username1  tty4  408/4327528  update
      task_id=30      addr=10.1.1.1  service=ppp  protocol=ip  addr=10.1.1.1
Wed Jun 27 04:01:31 2001 172.16.25.15  username1  tty4  562/4327528  stoptask_id=30
      addr=10.1.1.1  service=ppp  protocol=ip  addr=10.1.1.1  bytes_in=2844
      bytes_out=1682  paks_in=36  paks_out=24  elapsed_time=51
Wed Jun 27 04:01:32 2001 172.16.25.15  username1  tty4  562/4327528  stoptask_id=28
      service=shell  elapsed_time=57

```



(注) アカウンティング パケット レコードの正確なフォーマットは、セキュリティ サーバデーモンに応じて変わります。

次に、`autoselect` を介して着信する PPP ユーザの RADIUS ネットワーク アカウンティング レコードに含まれる情報の例を示します。

```

Wed Jun 27 04:30:52 2001
  NAS-IP-Address = "172.16.25.15"
  NAS-Port = 3
  User-Name = "username1"
  Client-Port-DNIS = "4327528"
  Caller-ID = "562"
  Acct-Status-Type = Start
  Acct-Authentic = RADIUS
  Service-Type = Framed
  Acct-Session-Id = "0000000B"
  Framed-Protocol = PPP
  Acct-Delay-Time = 0
  User-Id = "username1"
  NAS-Identifier = "172.16.25.15"

```

```

Wed Jun 27 04:36:49 2001
  NAS-IP-Address = "172.16.25.15"
  NAS-Port = 3
  User-Name = "username1"
  Client-Port-DNIS = "4327528"
  Caller-ID = "562"
  Acct-Status-Type = Stop
  Acct-Authentic = RADIUS
  Service-Type = Framed
  Acct-Session-Id = "0000000B"
  Framed-Protocol = PPP
  Framed-IP-Address = "10.1.1.1"
  Acct-Input-Octets = 8630
  Acct-Output-Octets = 5722
  Acct-Input-Packets = 94
  Acct-Output-Packets = 64
  Acct-Session-Time = 357
  Acct-Delay-Time = 0
  User-Id = "username1"
  NAS-Identifier = "172.16.25.15"

```

次に、`autoselect` を介して着信する PPP ユーザの TACACS+ ネットワーク アカウンティング レコードに含まれる情報の例を示します。

```

Wed Jun 27 04:02:19 2001 172.16.25.15  username1  Async5  562/4327528
starttask_id=35      service=ppp
Wed Jun 27 04:02:25 2001 172.16.25.15  username1  Async5  562/4327528  update
      task_id=35      service=ppp  protocol=ip  addr=10.1.1.2
Wed Jun 27 04:05:03 2001 172.16.25.15  username1  Async5  562/4327528  stoptask_id=35

```

```

service=ppp      protocol=ip      addr=10.1.1.2   bytes_in=3366   bytes_out=2149
paks_in=42      paks_out=28      elapsed_time=164

```

## EXEC アカウンティング

EXEC アカウンティングは、ネットワーク アクセス サーバ上にあるユーザ EXEC ターミナルセッション（ユーザシェル）に関する情報を提供します。たとえば、ユーザ名、日付、開始時刻と終了時刻、アクセス サーバの IP アドレス、および（ダイヤルインユーザの場合）発信元の電話番号などです。

次に、ダイヤルインユーザの RADIUS EXEC アカウンティング レコードに含まれる情報の例を示します。

```

Wed Jun 27 04:26:23 2001
  NAS-IP-Address = "172.16.25.15"
  NAS-Port = 1
  User-Name = "username1"
  Client-Port-DNIS = "4327528"
  Caller-ID = "5622329483"
  Acct-Status-Type = Start
  Acct-Authentic = RADIUS
  Service-Type = Exec-User
  Acct-Session-Id = "00000006"
  Acct-Delay-Time = 0
  User-Id = "username1"
  NAS-Identifier = "172.16.25.15"
Wed Jun 27 04:27:25 2001
  NAS-IP-Address = "172.16.25.15"
  NAS-Port = 1
  User-Name = "username1"
  Client-Port-DNIS = "4327528"
  Caller-ID = "5622329483"
  Acct-Status-Type = Stop
  Acct-Authentic = RADIUS
  Service-Type = Exec-User
  Acct-Session-Id = "00000006"
  Acct-Session-Time = 62
  Acct-Delay-Time = 0
  User-Id = "username1"
  NAS-Identifier = "172.16.25.15"

```

次に、ダイヤルインユーザの TACACS+ EXEC アカウンティング レコードに含まれる情報の例を示します。

```

Wed Jun 27 03:46:21 2001      172.16.25.15      username1      tty3      5622329430/4327528
start      task_id=2      service=shell
Wed Jun 27 04:08:55 2001      172.16.25.15      username1      tty3      5622329430/4327528
stop      task_id=2      service=shell      elapsed_time=1354

```

次に、Telnet ユーザの RADIUS EXEC アカウンティング レコードに含まれる情報の例を示します。

```

Wed Jun 27 04:48:32 2001
  NAS-IP-Address = "172.16.25.15"
  NAS-Port = 26
  User-Name = "username1"
  Caller-ID = "10.68.202.158"
  Acct-Status-Type = Start
  Acct-Authentic = RADIUS

```

```

Service-Type = Exec-User
Acct-Session-Id = "00000010"
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identififier = "172.16.25.15"

Wed Jun 27 04:48:46 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 26
User-Name = "username1"
Caller-ID = "10.68.202.158"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Exec-User
Acct-Session-Id = "00000010"
Acct-Session-Time = 14
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identififier = "172.16.25.15"

```

次に、Telnet ユーザの TACACS+ EXEC アカウントング レコードに含まれる情報の例を示します。

```

Wed Jun 27 04:06:53 2001      172.16.25.15      username1      tty26      10.68.202.158
starttask_id=41      service=shell
Wed Jun 27 04:07:02 2001      172.16.25.15      username1      tty26      10.68.202.158
stoptask_id=41      service=shell      elapsed_time=9

```

## コマンドアカウントング

コマンドアカウントングは、ネットワーク アクセス サーバで実行される各特権レベルの EXEC シェル コマンドに関する情報を提供します。各コマンドアカウントング レコードには、その特権レベルで実行されるコマンド、各コマンドが実行された日時、および実行したユーザのリストが含まれます。

次に、特権レベル 1 の TACACS+ コマンドアカウントング レコードに含まれる情報の例を示します。

```

Wed Jun 27 03:46:47 2001      172.16.25.15      username1      tty3      5622329430/4327528
stop      task_id=3      service=shell      priv-lvl=1      cmd=show version <cr>
Wed Jun 27 03:46:58 2001      172.16.25.15      username1      tty3      5622329430/4327528
stop      task_id=4      service=shell      priv-lvl=1      cmd=show interfaces Ethernet
0 <cr>
Wed Jun 27 03:47:03 2001      172.16.25.15      username1      tty3      5622329430/4327528
stop      task_id=5      service=shell      priv-lvl=1      cmd=show ip route <cr>

```

次に、特権レベル 15 の TACACS+ コマンドアカウントング レコードに含まれる情報の例を示します。

```

Wed Jun 27 03:47:17 2001      172.16.25.15      username1      tty3      5622329430/4327528
stop      task_id=6      service=shell      priv-lvl=15      cmd=configure terminal <cr>
Wed Jun 27 03:47:21 2001      172.16.25.15      username1      tty3      5622329430/4327528
stop      task_id=7      service=shell      priv-lvl=15      cmd=interface Serial 0 <cr>
Wed Jun 27 03:47:29 2001      172.16.25.15      username1      tty3      5622329430/4327528
stop      task_id=8      service=shell      priv-lvl=15      cmd=ip address 10.1.1.1
255.255.255.0 <cr>

```



(注) Cisco の RADIUS 実装は、コマンドアカウントティングをサポートしていません。

## 接続アカウントティング

接続アカウントティングは、Telnet、LAT、TN3270、PAD、rlogin などのネットワーク アクセスサーバから行われるすべての発信接続に関する情報を提供します。

次に、発信 Telnet 接続の RADIUS 接続アカウントティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:28:00 2001
  NAS-IP-Address = "172.16.25.15"
  NAS-Port = 2
  User-Name = "username1"
  Client-Port-DNIS = "4327528"
  Caller-ID = "5622329477"
  Acct-Status-Type = Start
  Acct-Authentic = RADIUS
  Service-Type = Login
  Acct-Session-Id = "00000008"
  Login-Service = Telnet
  Login-IP-Host = "10.68.202.158"
  Acct-Delay-Time = 0
  User-Id = "username1"
  NAS-Identifier = "172.16.25.15"
```

```
Wed Jun 27 04:28:39 2001
  NAS-IP-Address = "172.16.25.15"
  NAS-Port = 2
  User-Name = "username1"
  Client-Port-DNIS = "4327528"
  Caller-ID = "5622329477"
  Acct-Status-Type = Stop
  Acct-Authentic = RADIUS
  Service-Type = Login
  Acct-Session-Id = "00000008"
  Login-Service = Telnet
  Login-IP-Host = "10.68.202.158"
  Acct-Input-Octets = 10774
  Acct-Output-Octets = 112
  Acct-Input-Packets = 91
  Acct-Output-Packets = 99
  Acct-Session-Time = 39
  Acct-Delay-Time = 0
  User-Id = "username1"
  NAS-Identifier = "172.16.25.15"
```

次に、発信 Telnet 接続の TACACS+ 接続アカウントティング レコードに含まれる情報の例を示します。

```
Wed Jun 27 03:47:43 2001      172.16.25.15      username1  tty3      5622329430/4327528
  start      task_id=10      service=connection      protocol=telnet  addr=10.68.202.158
cmd=telnet  username1-sun
Wed Jun 27 03:48:38 2001      172.16.25.15      username1  tty3      5622329430/4327528
  stop      task_id=10      service=connection      protocol=telnet  addr=10.68.202.158
```

```
cmd=telnet username1-sun      bytes_in=4467  bytes_out=96   paks_in=61    paks_out=72
elapsed_time=55
```

次に、発信 rlogin 接続の RADIUS 接続アカウントング レコードに含まれる情報の例を示します。

```
Wed Jun 27 04:29:48 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 2
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "5622329477"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
Service-Type = Login
Acct-Session-Id = "0000000A"
Login-Service = Rlogin
Login-IP-Host = "10.68.202.158"
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"
```

```
Wed Jun 27 04:30:09 2001
NAS-IP-Address = "172.16.25.15"
NAS-Port = 2
User-Name = "username1"
Client-Port-DNIS = "4327528"
Caller-ID = "5622329477"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
Service-Type = Login
Acct-Session-Id = "0000000A"
Login-Service = Rlogin
Login-IP-Host = "10.68.202.158"
Acct-Input-Octets = 18686
Acct-Output-Octets = 86
Acct-Input-Packets = 90
Acct-Output-Packets = 68
Acct-Session-Time = 22
Acct-Delay-Time = 0
User-Id = "username1"
NAS-Identifier = "172.16.25.15"
```

次に、発信 rlogin 接続の TACACS+ 接続アカウントング レコードに含まれる情報の例を示します。

```
Wed Jun 27 03:48:46 2001      172.16.25.15  username1  tty3  5622329430/4327528
start  task_id=12  service=connection  protocol=rlogin  addr=10.68.202.158
cmd=rlogin username1-sun /user username1
Wed Jun 27 03:51:37 2001      172.16.25.15  username1  tty3  5622329430/4327528
stop   task_id=12  service=connection  protocol=rlogin  addr=10.68.202.158
cmd=rlogin username1-sun /user username1 bytes_in=659926 bytes_out=138  paks_in=2378
      paks_
out=1251      elapsed_time=171
```

次に、発信 LAT 接続の TACACS+ 接続アカウントング レコードに含まれる情報の例を示します。

```
Wed Jun 27 03:53:06 2001      172.16.25.15  username1  tty3  5622329430/4327528
start  task_id=18  service=connection  protocol=lat  addr=VAX  cmd=lat
VAX
```



```
Wed Jun 27 03:54:15 2001      172.16.25.15      username1  tty3      5622329430/4327528
stop      task_id=18      service=connection  protocol=lat  addr=VAX      cmd=lat
VAX  bytes_in=0      bytes_out=0      paks_in=0      paks_out=0      elapsed_time=6
```

## システム アカウンティング

システム アカウンティングは、すべてのシステムレベル イベント（たとえば、システムのリブート時やアカウントティングのオン/オフ時）に関する情報を提供します。

次のアカウントティング レコードは、AAA アカウンティングがオフになったことを示す一般的な TACACS+ システム アカウンティング レコード サーバを示します。

```
Wed Jun 27 03:55:32 2001      172.16.25.15      unknown unknown unknown start  task_id=25
service=system event=sys_acct  reason=reconfigure
```



- (注) アカウンティング パケット レコードの正確なフォーマットは、TACACS+ デーモンに応じて変わります。

次のアカウントティング レコードは、AAA アカウンティングがオンになったことを示す TACACS+ システム アカウンティング レコードを示します。

```
Wed Jun 27 03:55:22 2001      172.16.25.15      unknown unknown unknown stop  task_id=23
service=system event=sys_acct  reason=reconfigure
```

システム リソースを測定する追加のタスクについては、他の Cisco IOS ソフトウェア コンフィギュレーション ガイドを参照してください。たとえば、IP アカウンティング タスクについては、『Cisco IOS Application Services Configuration Guide』の「Configuring IP Services」を参照してください。

## リソース アカウンティング

シスコが採用している AAA アカウンティングでは、ユーザー認証を通過したコールに対する「開始」レコードと「終了」レコードがサポートされます。ユーザー認証の一部として認証に失敗したコールの「終了」レコードを生成する追加機能もサポートされます。このようなレコードは、ネットワークを管理およびモニタするアカウントティング レコードを採用する場合に必要です。

ここでは、次の内容について説明します。

### AAA リソース失敗終了アカウントティング

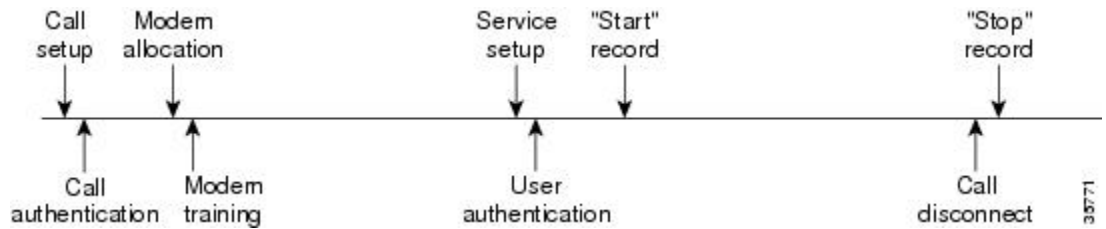
AAA リソース失敗終了アカウントティングの前には、コール設定シーケンスのユーザー認証段階に到達できなかったコールについて、アカウントティング レコードを提供する方式がありませんでした。このようなレコードは、ネットワークおよびその卸売りの顧客を管理およびモニターするアカウントティング レコードを採用する場合に必要です。

この機能によって、ユーザー認証に到達しなかったコールの「終了」アカウントティング レコードが生成されます。「終了」レコードは、コール設定の時点から生成されます。ユーザー認証

に成功したすべてのコールは、従来と同様に動作します。つまり、追加のアカウントINGレコードは確認されません。

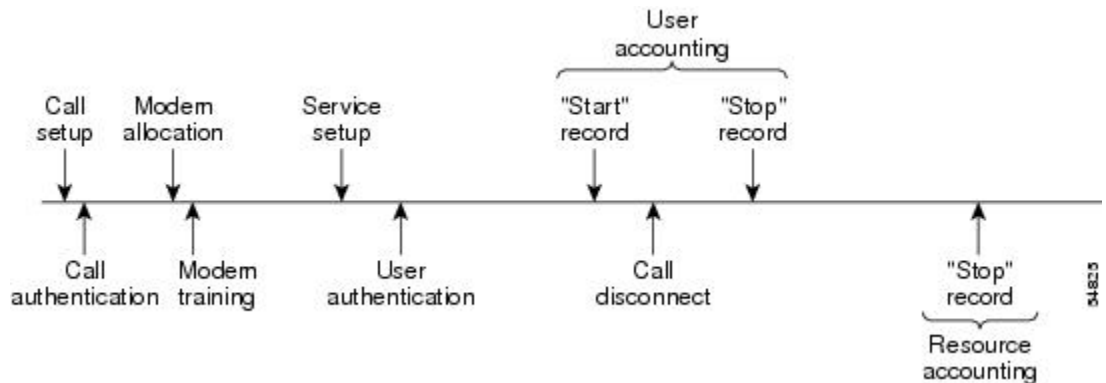
次の図に、通常のコールフローで、AAA リソース失敗終了アカウントINGを有効にしているコールシーケンスを示します。

図4:通常のフローでAAAリソース失敗終了アカウントINGを有効にしているモデムダイヤルインコール設定シーケンス



次の図に、通常のコールフローで、AAA リソース失敗終了アカウントINGを有効にしたコールシーケンスを示します。

図5:通常のフローでAAAリソース失敗終了アカウントINGを有効にしたモデムダイヤルインコール設定シーケンス



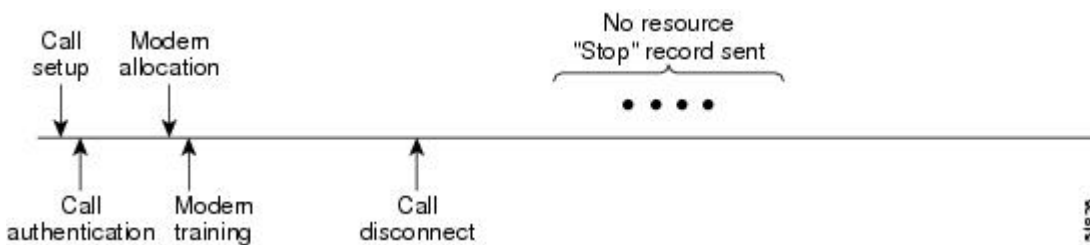
次の図に、ユーザー認証前にコールの接続解除が発生し、AAA リソース失敗終了アカウントINGを有効にしたコール設定シーケンスを示します。

図6:ユーザー認証前にコールの接続解除が発生し、AAAリソース失敗終了アカウントINGを有効にしたモデムダイヤルインコール設定シーケンス



次の図に、ユーザー認証前にコールの接続解除が発生し、AAA リソース失敗終了アカウントINGを有効にしているコール設定シーケンスを示します。

図 7: ユーザー認証前にコールの接続解除が発生し、AAA リソース失敗終了アカウントティングをイネーブルにしていないモデムダイヤルインコール設定シーケンス



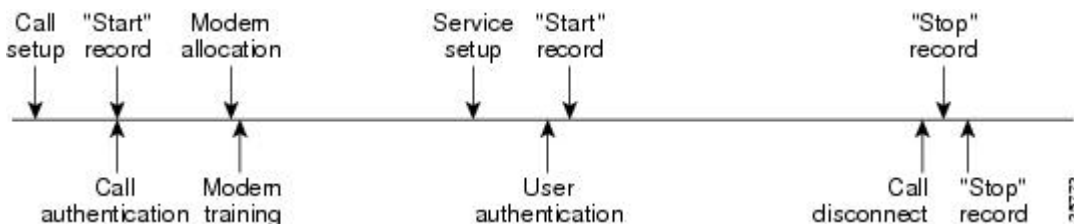
### 開始 - 終了レコードの AAA リソース アカウントティング

開始 - 終了レコードの AAA リソース アカウントティングは、各コール設定時に「開始」レコードを送信し、コールの接続解除時に対応する「終了」レコードを送信する機能をサポートしています。この機能は、アカウントティングレコードなどを報告するデータの発信元の1つから、卸売りの顧客を管理およびモニターするために使用できます。

この機能を使用すると、コール設定およびコールの接続解除の「開始 - 終了」アカウントティングレコードは、デバイスに対するリソース接続の進行状況を追跡します。個別のユーザー認証「開始 - 終了」アカウントティングレコードが、ユーザー管理の進行状況を追跡します。これら2セットのアカウントティングレコードは、そのコールで固有のセッションIDを使用して相互リンクされます。

次の図は、AAA リソース開始 - 終了アカウントティングを有効にしたコール設定シーケンスを示します。

図 8: リソース開始 - 終了アカウントティングを有効にしたモデムダイヤルインコール設定シーケンス



## AAA アカウントティングの強化

### AAA ブロードキャストアカウントティング

AAA ブロードキャストアカウントティングを有効にすると、アカウントティング情報を複数のAAA サーバに同時に送信できます。つまり、アカウントティング情報を1つまた複数のAAA サーバに同時にブロードキャストすることが可能です。この機能を使用すると、サービスプロバイダーは自社使用のプライベートAAA サーバやエンドユーザのAAA サーバにアカウントティング情報を送信できるようになります。この機能では、音声アプリケーションによる課金情報も提供されます。

ブロードキャストは、RADIUS または TACACS+ サーバのグループに使用できます。また、各サーバグループは、他のグループとは関係なく、フェールオーバーの場合のバックアップサーバを定義できます。

したがって、サービスプロバイダーとそのエンドユーザは、アカウントングサーバに異なるプロトコル (RADIUS または TACACS+) を使用できます。また、サービスプロバイダーとそのエンドユーザは、それぞれ単独でバックアップサーバを指定することもできます。音声アプリケーションについては、独自のフェールオーバーシーケンスを持つ個別のグループを介して、冗長的なアカウントング情報を単独で管理できます。

## AAA セッション MIB

ユーザが AAA セッション MIB 機能を使用すると、簡易ネットワーク管理プロトコル (SNMP) を使用して自身の認証済みクライアント接続をモニタおよび終了できます。そのクライアントのデータが提示されるため、RADIUS または TACACS+ サーバから報告される AAA アカウントング情報に直接関連付けることができます。AAA セッション MIB は、次の情報を提供します。

- 各 AAA 機能の統計情報 (**show radius statistics** コマンドと併用する場合)
- AAA 機能を提供するサーバのステータス
- 外部 AAA サーバの ID
- (アイドル時間などの) リアルタイム情報 (アクティブコールを終了するかどうかを評価する SNMP ネットワークが使用する追加基準を提供します)



(注) このコマンドがサポートされるのは、Cisco AS5300 および Cisco AS5800 ユニバーサルアクセス サーバプラットフォームだけです。

次の表に、認証済みクライアントと AAA セッション MIB 機能との接続をモニタおよび終了するために使用できる SNMP ユーザエンドデータ オブジェクトを示します。

表 14: SNMP エンドユーザ データ オブジェクト

SessionId	AAA アカウントングプロトコルに使用されるセッション ID (RADIUS 属性 44 (Acct-Session-ID) から報告される値と同じ)
UserId	ユーザ ログイン ID または (ログインが使用できない場合) 長さがゼロの文字列
IpAddr	セッションの IP アドレスまたは (IP アドレスが適用されない場合、または使用できない場合) 0.0.0.0
IdleTime	セッションがアイドルになってからの経過時間
Disconnect	そのクライアントとの接続を解除するために使用されるセッション終了オブジェクト

CallId	コールトラッカーレコードが保存した、このアカウントティングセッションに対応するエントリインデックス
--------	---

次の表に、システム別に SNMP を使用する AAA セッション MIB 機能から提供される AAA の概要情報を示します。

表 15: SNMP AAA セッションの概要

ActiveTableEntries	現在アクティブなセッションの数
ActiveTableHighWaterMark	システムが最後に再インストールされてからの同時接続セッションの最大数
TotalSessions	システムが最後に再インストールされてからのセッションの合計数
DisconnectedSessions	システムが最後に再インストールされてから接続解除されたセッションの合計数

## アカウントティング属性と値のペア

ネットワークアクセスサーバは、TACACS+ AV のペアまたは RADIUS 属性（実装しているセキュリティ方式によって異なります）に定義されたアカウントティング機能をモニタします。

# AAA アカウントティングの設定方法

## 名前付き方式リストによる AAA アカウントティングの設定

名前付き方式リストを使用して AAA アカウントティングを設定するには、次の手順を実行します。



(注) システムアカウントティングは、名前付き方式リストを使用しません。システムアカウントティングの場合、デフォルトの方式リストだけを定義します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **aaa accounting {system | network | exec | connection | commands level} {default | list-name} {start-stop | stop-only | none} [method1 [method2... ]]**
4. 次のいずれかを実行します。
  - **line [aux | console | tty | vty] line-number [ending-line-number]**

- 
- 
- 
- **interface** *interface-type interface-number*

5. 次のいずれかを実行します。

- **accounting** {**arap** | **commands** *level* | **connection** | **exec**} {**default** | *list-name*}
- 
- 
- **ppp accounting**{**default** | *list-name*}

6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<p><b>enable</b></p> <p>例 :</p> <pre>Device&gt; enable</pre>	<p>特権 EXEC モードを有効にします。</p> <ul style="list-style-type: none"> <li>• パスワードを入力します (要求された場合)。</li> </ul>
ステップ 2	<p><b>configure terminal</b></p> <p>例 :</p> <pre>Device# configure terminal</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>
ステップ 3	<p><b>aaa accounting</b> {<b>system</b>   <b>network</b>   <b>exec</b>   <b>connection</b>   <b>commands</b> <i>level</i>} {<b>default</b>   <i>list-name</i>} {<b>start-stop</b>   <b>stop-only</b>   <b>none</b>} [<i>method1</i> [<i>method2...</i> ]]</p> <p>例 :</p> <pre>Device(config)# aaa accounting system default start-stop</pre>	<p>アカウントング方式リストを作成し、アカウントングを有効にします。引数 <i>list-name</i> は、作成したリストに名前を付けるときに使用される文字列です。</p>
ステップ 4	<p>次のいずれかを実行します。</p> <ul style="list-style-type: none"> <li>• <b>line</b> [<b>aux</b>   <b>console</b>   <b>tty</b>   <b>vty</b>] <i>line-number</i> [<i>ending-line-number</i>]</li> <li>•</li> <li>•</li> <li>• <b>interface</b> <i>interface-type interface-number</i></li> </ul> <p>例 :</p> <pre>Device(config)# line aux line1</pre>	<p>アカウントング方式リストを適用する回線について、ライン コンフィギュレーション モードを開始します。</p> <p>または</p> <p>アカウントング方式リストを適用するインターフェイスについて、インターフェイス コンフィギュレーション モードを開始します。</p>

	コマンドまたはアクション	目的
ステップ 5	<p>次のいずれかを実行します。</p> <ul style="list-style-type: none"> <li>• <b>accounting {arap   commands level   connection   exec} {default   list-name}</b></li> <li>•</li> <li>•</li> <li>•</li> <li>• <b>ppp accounting {default   list-name}</b></li> </ul> <p>例：</p> <pre>Device(config-line)# accounting arap default</pre>	<p>1つの回線または複数回線にアカウントティング方式リストを適用します。</p> <p>または</p> <p>1つのインターフェイスまたは複数インターフェイスにアカウントティング方式リストを適用します。</p>
ステップ 6	<p><b>end</b></p> <p>例：</p> <pre>Device(config-line)# end</pre>	<p>(任意) ライン 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。</p>

#### 次のタスク

ここでは、次の内容について説明します。

## マルチユーザセッション時のアカウントティングレコード生成の抑制

AAA アカウントティングをアクティブにすると、Cisco IOS ソフトウェアは、システム上のすべてのユーザにアカウントティングレコードを発行します。このとき、プロトコル変換のためユーザ名文字列がヌルになっているユーザも含まれます。この例では、**aaa authentication login method-list none** コマンドが適用される回線で着信するユーザがそれに該当します。関連付けられているユーザ名がないセッションについて、アカウントティングレコードが生成されないようにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
<pre>Device(config)# <b>aaa accounting suppress null-username</b></pre>	ユーザ名文字列がヌルのユーザについて、アカウントティングレコードが生成されないようにします。

## 中間アカウントティングレコードの生成

アカウントティング サーバに定期的な中間アカウントティングレコードを送信できるようにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
<pre>Device(config)# <b>aaa accounting update [newinfo] [periodic] number</b></pre>	アカウントティング サーバに送信される定期的な中間アカウントティングレコードをイネーブルにします。

**aaa accounting update** コマンドをアクティブにすると、Cisco IOS ソフトウェアによってシステム上のすべてのユーザーの中間アカウントングレコードが発行されます。**newinfo** キーワードを使用した場合は、レポートする新しいアカウントング情報が発生するたびに、中間アカウントングレコードがアカウントングサーバに送信されます。たとえば、IPCP がリモートピアとの間で IP アドレスのネゴシエーションを完了したときなどです。中間アカウントングレコードには、リモートピアに使用されるネゴシエート済み IP アドレスが含まれます。

キーワード **periodic** と一緒に使用した場合は、*number* 引数による定義に基づいて、中間アカウントングレコードが定期的送信されます。中間アカウントングレコードには、中間アカウントングレコードが送信される時間までに、そのユーザについて記録されたすべてのアカウントング情報が含まれます。



**注意** 多数のユーザがネットワークにログインしている場合には、**aaa accounting update periodic** コマンドを使用すると、重度の輻輳が発生する可能性があります。

## 定期的アカウントングレコードを有効化する代替手段の設定

次の代替手段を使用して、アカウントングサーバに送信される定期的中間アカウントングレコードをイネーブルにできます。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **aaa accounting network default**
4. **action-type {none | start-stop [periodic {disable | interval *minutes*}] | stop-only}**
5. **exit**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  Router> enable	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  Router# 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 3	<b>aaa accounting network default</b> 例：	すべてのネットワーク関連のサービス要求のデフォルトのアカウントングを設定し、アカウントイン



	コマンドまたはアクション	目的
	<code>Router(config)# aaa accounting network default</code>	グローバルリスト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 4	<p><b>action-type</b> {none   start-stop [periodic {disable   interval <i>minutes</i>}]   stop-only}</p> <p>例 :</p> <pre>Router(cfg-acct-mlist)# action-type start-stop</pre> <p>例 :</p> <pre>periodic interval 5</pre>	<p>アカウントティングレコードに対して実行されるアクションのタイプを指定します。</p> <ul style="list-style-type: none"> <li>• (任意) <b>periodic</b> キーワードは、定期的なアカウントティングアクションを示します。</li> <li>• <b>interval</b> キーワードは、定期的なアカウントティング間隔を指定します。</li> <li>• <b>value</b> 引数は、アカウントティング更新レコードの間隔を指定します (分単位)。</li> <li>• <b>disable</b> キーワードは、定期的なアカウントティングをディセーブルにします。</li> </ul>
ステップ 5	<p><b>exit</b></p> <p>例 :</p> <pre>Router(cfg-acct-mlist)# exit</pre>	グローバル コンフィギュレーション モードに戻ります。

## 中間サービス アカウンティング レコードの生成

このタスクを実行して、サブスクライバに対する定期的な間隔での中間サービスアカウントティングレコードの生成をイネーブルにします。

### 始める前に

ユーザー サービス プロファイルの RADIUS 属性 85 は設定済みの中間の間隔値よりも常に優先されます。RADIUS 属性 85 は、ユーザー サービス プロファイル内にある必要があります。詳細については、RADIUS 属性の概要および RADIUS IETF 属性の機能のドキュメントを参照してください。



- (注) RADIUS 属性 85 がユーザー サービス プロファイル内にない場合、中間アカウントティングレコードの生成で設定された中間の間隔値がサービスの中間アカウントティングレコードに使用されます。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **subscriber service accounting interim-interval *minutes***

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Router> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： Router# 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 3	<b>subscriber service accounting interim-interval minutes</b> 例： Router(config)# subscriber service accounting interim-interval 10	サブスクリイバに対する定期的な間隔での中間サービス アカウントティング レコードの生成をイネーブにします。 <i>minutes</i> 引数は、アカウントティング更新レコードを送信する定期的な間隔を 1 ~ 71582 分で示します。

## 失敗したログインまたはセッションに対するアカウントティングレコードの生成

AAA アカウントティングをアクティブにすると、Cisco IOS XE ソフトウェアは、ログイン認証に失敗したシステム ユーザー、またはログイン認証には成功しても何らかの理由で PPP ネゴシエーションに失敗したユーザーのアカウントティングレコードを生成しません。

ログイン時またはセッションネゴシエーション中の認証に失敗したユーザーについて、アカウントティング終了レコードを生成するように指定するには、グローバルコンフィギュレーションモードで次のコマンドを使用します。

コマンドまたはアクション	目的
<b>aaa accounting send stop-record authentication failure</b>	ログイン時またはセッションネゴシエーション中の認証に失敗したユーザについて、「終了」レコードを生成します。

## EXEC-Stop レコードよりも前のアカウントティング NETWORK-Stop レコードの指定

EXEC 終了セッションを開始する PPP ユーザーの場合、EXEC-stop レコードの前に、NETWORK レコードを生成するように指定できます。特定のサービスについて顧客に課金する場合など、状況によっては、ネットワークの開始レコードと終了レコードを一緒に保持する方が望ましいことがあります。その際、基本的に、EXEC の開始メッセージと終了メッセージのフレームワーク内に「ネスト」にします。たとえば、PPP を使用するユーザーダイヤルインによって、

EXEC-start、NETWORK-start、EXEC-stop、NETWORK-stop というレコードを作成できます。ネットワーク アカウンティング レコードをネストにすることで、NETWORK-stop レコードは NETWORK-start メッセージ (EXEC-start、NETWORK-start、NETWORK-stop、EXEC-stop) に従います。

ユーザーセッションのアカウントティングレコードをネストするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンドまたはアクション	目的
<b>aaa accounting nested</b>	ネットワーク アカウンティングレコードをネストします。

## スイッチオーバー上のシステム アカウンティング レコードの抑制

スイッチオーバー中のシステム アカウンティングオンおよびアカウントティングオフ メッセージを抑制するには、グローバル コンフィギュレーションモードで次のコマンドを使用します。

コマンドまたはアクション	目的
<b>aaa accounting redundancy suppress system-records</b>	スイッチオーバー中のシステム アカウンティングレコードを抑制します。

## AAA リソース失敗終了アカウントティングの設定

リソース失敗終了アカウントティングを有効にするには、グローバル コンフィギュレーションモードで次のコマンドを使用します。

コマンド	目的
Device(config)# <b>aaa accounting resource method-list stop-failure group server-group</b>	<p>ユーザー認証に到達しないコールについて、「終了」レコードを生成します。</p> <p>(注) この機能を設定する前に、<a href="#">アカウントティングを設定するための前提条件 (103 ページ)</a> のセクションに記載されている作業を実行し、ネットワーク アクセス サーバー上で SNMP を有効にしてください。Cisco ルータまたはアクセスサーバーで SNMP を有効にする方法の詳細については、『Cisco IOS Network Management Configuration Guide』の「SNMP サポートの設定」の章を参照してください。</p>

## 開始 - 終了レコードの AAA リソース アカウンティングの設定

開始 - 終了レコードのフル リソース アカウンティングをイネーブルにするには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンド	目的
<pre>Device(config)# <b>aaa</b> <b>accounting resource</b> <b>method-list start-stop</b> <b>group server-group</b></pre>	<p>各コール設定時に「開始」レコードを送信し、コールの接続解除時に対応する「終了」レコードを送信する機能をサポートします。</p> <p>(注) この機能を設定する前に、<a href="#">アカウントिंगを設定するための前提条件 (103 ページ)</a> のセクションに記載されている作業を実行し、ネットワークアクセスサーバー上で SNMP を有効にしてください。Cisco ルータまたはアクセスサーバーで SNMP を有効にする方法の詳細については、『Cisco IOS Network Management Configuration Guide』の「SNMP サポートの設定」の章を参照してください。</p> <p>(注)</p>

## AAA ブロードキャスト アカウンティング

AAA ブロードキャスト アカウンティングを有効にすると、アカウントング情報を複数の AAA サーバに同時に送信できます。つまり、アカウントング情報を 1 つまた複数の AAA サーバに同時にブロードキャストすることが可能です。この機能を使用すると、サービスプロバイダーは自社使用のプライベート AAA サーバやエンドユーザの AAA サーバにアカウントング情報を送信できるようになります。この機能では、音声アプリケーションによる課金情報も提供されます。

ブロードキャストは、RADIUS または TACACS+ サーバのグループに使用できます。また、各サーバグループは、他のグループとは関係なく、フェールオーバーの場合のバックアップサーバを定義できます。

したがって、サービスプロバイダーとそのエンドユーザは、アカウントングサーバに異なるプロトコル (RADIUS または TACACS+) を使用できます。また、サービスプロバイダーとそのエンドユーザは、それぞれ単独でバックアップサーバを指定することもできます。音声アプリケーションについては、独自のフェールオーバーシーケンスを持つ個別のグループを介して、冗長的なアカウントング情報を単独で管理できます。

## DNIS による AAA ブロードキャスト アカウンティングの設定

AAA ブロードキャストアカウントングを設定するには、グローバルコンフィギュレーションモードで `aaa dnis map accounting network` コマンドを使用します。

コマンド	目的
<pre>Device(config)# <b>aaa dnis map</b>   dnis-number <b>accounting</b> <b>network</b> [<b>start-stop</b>   <b>stop-only</b>   <b>none</b>] [<b>broadcast</b>] method1 [method2...]</pre>	<p>DNIS によるアカウントティングの設定を許可します。このコマンドは、グローバルの <b>aaa accounting</b> コマンドよりも優先されます。</p> <p>複数の AAA サーバに対するアカウントティングレコードの送信をイネーブルにします。各グループの最初のサーバに対し、アカウントティングレコードを同時に送信します。最初のサーバが使用できない場合はフェールオーバーが発生し、そのグループ内に定義されているバックアップサーバが使用されます。</p>

## AAA セッション MIB

ユーザが AAA セッション MIB 機能を使用すると、簡易ネットワーク管理プロトコル (SNMP) を使用して自身の認証済みクライアント接続をモニタおよび終了できます。そのクライアントのデータが提示されるため、RADIUS または TACACS+ サーバから報告される AAA アカウントティング情報に直接関連付けることができます。AAA セッション MIB は、次の情報を提供します。

- 各 AAA 機能の統計情報 (**show radius statistics** コマンドと併用する場合)
- AAA 機能を提供するサーバのステータス
- 外部 AAA サーバの ID
- (アイドル時間などの) リアルタイム情報 (アクティブコールを終了するかどうかを評価する SNMP ネットワークが使用する追加基準を提供します)



(注) このコマンドがサポートされるのは、Cisco AS5300 および Cisco AS5800 ユニバーサルアクセス サーバー プラットフォームだけです。

次の表に、認証済みクライアントと AAA セッション MIB 機能との接続をモニタおよび終了するために使用できる SNMP ユーザエンドデータ オブジェクトを示します。

表 16: SNMP エンドユーザ データ オブジェクト

SessionId	AAA アカウントティング プロトコルに使用されるセッション ID (RADIUS 属性 44 (Acct-Session-ID) から報告される値と同じ)
UserId	ユーザ ログイン ID または (ログインが使用できない場合) 長さがゼロの文字列
IpAddr	セッションの IP アドレスまたは (IP アドレスが適用されない場合、または使用できない場合) 0.0.0.0

AAA サーバが到達不能な場合のルータとのセッションの確立

IdleTime	セッションがアイドルになってからの経過時間
Disconnect	そのクライアントとの接続を解除するために使用されるセッション終了オブジェクト
CallId	コールトラッカーレコードが保存した、このアカウントングセッションに対応するエントリインデックス

次の表に、システム別に SNMP を使用する AAA セッション MIB 機能から提供される AAA の概要情報を示します。

表 17: SNMP AAA セッションの概要

ActiveTableEntries	現在アクティブなセッションの数
ActiveTableHighWaterMark	システムが最後に再インストールされてからの同時接続セッションの最大数
TotalSessions	システムが最後に再インストールされてからのセッションの合計数
DisconnectedSessions	システムが最後に再インストールされてから接続解除されたセッションの合計数

## AAA サーバが到達不能な場合のルータとのセッションの確立

AAA サーバが到達不能の場合に、ルータとの間にコンソールセッションを確立するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。

コマンドまたはアクション	目的
<b>no aaa accounting system guarantee-first</b>	<p><b>aaa accounting system guarantee-first</b> コマンドは、システムアカウントを最初のレコードとして保証します。これは、デフォルトの条件です。</p> <p>状況によっては、システムの再ロードが完了するまで（3分よりも長くかかる可能性があります）、ユーザーがコンソールまたは Telnet 接続でセッションを開始できない可能性があります。この問題を解決するには、<b>no aaa accounting system guarantee-first</b> コマンドを使用します。</p>

## アカウントティングのモニタリング

RADIUS または TACACS+ アカウントティングの場合、特定の **show** コマンドは存在しません。ログインしているユーザーに関する情報を表示するアカウントティングレコードを取得するには、特権 EXEC モードで次のコマンドを使用します。

コマンドまたはアクション	目的
<b>show accounting</b>	ネットワークでアクティブなアカウント可能なイベントの表示を許可し、アカウントティングサーバでデータが損失した場合に情報を収集できます。

## アカウントティングのトラブルシューティング

アカウントティング情報の問題を解決するには、特権 EXEC モードで次のコマンドを使用します。

コマンドまたはアクション	目的
<b>debug aaa accounting</b>	説明の義務があるイベントが発生したときに、その情報を表示します。

## AAA アカウントティングの設定例

### 例：名前付き方式リストの設定

次に、RADIUS サーバーから AAA サービスを提供するためにシスコ デバイス（AAA および RADIUS セキュリティサーバーとの通信で有効）を設定する例を示します。RADIUS サーバーが応答に失敗すると、認証情報と認可情報についてローカルデータベースへの照会が行われ、アカウントティング サービスは TACACS+ サーバーによって処理されます。

```
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication login admins local
Device(config)# aaa authentication ppp dialins group radius local
Device(config)# aaa authorization network network1 group radius local
Device(config)# aaa accounting network network2 start-stop group radius group tacacs+
Device(config)# username root password ALongPassword
Device(config)# tacacs server server1
Device(config-server-tacacs)# address ipv4 172.31.255.0
Device(config-server-tacacs)# key goaway
Device(config-server-tacacs)# exit
Device(config)# radius server isp
Device(config-sg-radius)# key myRaDiUSpassWoRd
Device(config-sg-radius)# exit
Device(config)# interface group-async 1
Device(config-if)# group-range 1 16
Device(config-if)# encapsulation ppp
```

```

Device(config-if)# ppp authentication chap dialins
Device(config-if)# ppp authorization network1
Device(config-if)# ppp accounting network2
Device(config-if)# exit
Device(config)# line 1 16
Device(config-line)# autoselect ppp
Device(config-line)# autoselect during-login
Device(config-line)# login authentication admins
Device(config-line)# modem dialin
Device(config-line)# end

```

この RADIUS AAA 設定のサンプル行は、次のように定義されます。

- **aaa new-model** コマンドは、AAA ネットワーク セキュリティ サービスをイネーブルにします。
- **aaa authentication login admins local** コマンドは、ログイン認証に方式リスト「admins」を定義します。
- **aaa authentication ppp dialins group radius local** コマンドで、認証方式リスト「dialins」を定義します。このリストは、最初に RADIUS 認証を指定して、次に（RADIUS サーバーが応答しない場合）PPP を使用してシリアル回線上でローカル認証が使用されます。
- **aaa authorization network network1 group radius local** コマンドで、「network1」というネットワーク許可方式リストを定義します。これにより、PPP を使用してシリアル回線上で RADIUS 許可を使用するよう指定されます。RADIUS サーバーが応答に失敗すると、ローカル ネットワークの認可が実行されます。
- **aaa accounting network network2 start-stop group radius group tacacs+** コマンドで、「network2」というネットワーク アカウンティング方式リストを定義します。これにより、PPP を使用してシリアル回線上で RADIUS アカウンティングサービス（この場合、特定のイベントに対する開始レコードと終了レコード）を使用するよう指定されます。RADIUS サーバが応答に失敗すると、アカウンティングサービスは TACACS+ サーバによって処理されます。
- **username** コマンドはユーザ名とパスワードを定義します。これらの情報は、PPP パスワード認証プロトコル（PAP）の発信元身元確認に使用されます。
- **tacacs server** コマンドは TACACS+ サーバーホストの名前を定義します。
- **key** コマンドは、ネットワーク アクセス サーバーと TACACS+ サーバーホストの間の共有秘密テキスト文字列を定義します。
- **radius server** コマンドは RADIUS サーバー ホストの名前を定義します。
- **key** コマンドは、ネットワーク アクセス サーバーと RADIUS サーバー ホストの間の共有秘密テキスト文字列を定義します。
- **interface group-async** コマンドは、非同期インターフェイス グループを選択して定義します。
- **group-range** コマンドは、インターフェイス グループ内のメンバ非同期インターフェイスを定義します。



- **encapsulation ppp** コマンドは、指定のインターフェイスに使用されるカプセル化方式として PPP を設定します。
- **ppp authentication chap dialins** コマンドは、PPP 認証方式としてチャレンジハンドシェイク認証プロトコル (CHAP) を選択し、指定したインターフェイスに「dialins」方式リストを適用します。
- **ppp authorization network1** コマンドによって、blue1 ネットワーク許可方式リストが、指定したインターフェイスに適用されます。
- **ppp accounting network2** コマンドによって、red1 ネットワーク アカウンティング方式リストが、指定したインターフェイスに適用されます。
- **line** コマンドはコンフィギュレーション モードをグローバル コンフィギュレーションからライン コンフィギュレーションに切り替え、設定対象の回線を指定します。
- **autoselect ppp** コマンドは、選択した回線上で PPP セッションを自動的に開始できるように Cisco IOS XE ソフトウェアを設定します。
- **autoselect during-login** コマンドを使用すると、Return キーを押さずにユーザ名およびパスワードのプロンプトが表示されます。ユーザがログインすると、autoselect 機能（この場合は PPP）が開始します。
- **login authentication admins** コマンドは、ログイン認証に admins 方式リストを適用します。
- **modem dialin** コマンドは、選択した回線に接続されているモデムを設定し、着信コールだけを受け入れるようにします。

**show accounting** コマンドを使用すると、前述の設定に関する出力が次のように生成されます。

```
Active Accounted actions on tty1, User username2 Priv 1
Task ID 5, Network Accounting record, 00:00:52 Elapsed
task_id=5 service=ppp protocol=ip address=10.0.0.98
```

次の表に、前述の出力に含まれるフィールドについて説明します。

表 18: **show accounting** のフィールドの説明

フィールド	説明
Active Accounted actions on	ユーザがログインに使用する端末回線またはインターフェイス名
User	ユーザの ID。
Priv	ユーザの特権レベル。
Task ID	各アカウントティングセッションの固有識別情報
Accounting Record	アカウントティングセッションタイプ
Elapsed	このセッションタイプの期間 (hh:mm:ss)
attribute=value	このアカウントティングセッションに関連付けられている AV ペア

## 例 : AAA リソース アカウンティングの設定

次に、リソース失敗終了アカウントティング、および 開始 - 終了レコード機能のリソース アカウンティングを設定する例を示します。

```
!Enable AAA on your network access server.
aaa new-model
!Enable authentication at login and list the AOL string name to use for login
authentication.
aaa authentication login AOL group radius local
!Enable authentication for ppp and list the default method to use for PPP authentication.
aaa authentication ppp default group radius local
!Enable authorization for all exec sessions and list the AOL string name to use for
authorization.
aaa authorization exec AOL group radius if-authenticated
!Enable authorization for all network-related service requests and list the default
method to use for all network-related authorizations.
aaa authorization network default group radius if-authenticated
!Enable accounting for all exec sessions and list the default method to use for all
start-stop accounting services.
aaa accounting exec default start-stop group radius
!Enable accounting for all network-related service requests and list the default method
to use for all start-stop accounting services.
aaa accounting network default start-stop group radius
!Enable failure stop accounting.
aaa accounting resource default stop-failure group radius
!Enable resource accounting for start-stop records.
aaa accounting resource default start-stop group radius
```

## 例 : AAA ブロードキャスト アカウンティングの設定

次に、グローバル **aaa accounting** コマンドを使用して、ブロードキャストアカウントティングを有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# aaa group server radius isp
Device(config-sg-radius)# server 10.0.0.1
Device(config-sg-radius)# server 10.0.0.2
Device(config-sg-radius)# exit
Device(config)# aaa group server tacacs+ isp_customer
Device config-sg-tacacs+)# server 172.0.0.1
Device config-sg-tacacs+)# exit
Device(config)# aaa accounting network default start-stop broadcast group isp group
isp_customer
Device(config)# tacacs server server1
Device(config-server-tacacs)# address ipv4 172.0.0.1
Device(config-server-tacacs)# key key2
Device(config-server-tacacs)# end
```

**broadcast** キーワードによって、ネットワーク接続に関する「開始」および「終了」アカウントティングレコードが、グループ **isp** ではサーバー 10.0.0.1 に、グループ **isp\_customer** ではサーバー 172.0.0.1 に同時送信されます。サーバ 10.0.0.1 が使用できなくなると、サーバ 10.0.0.2 へのフェールオーバーが行われます。サーバ 172.0.0.1 が使用できなくなっても、グループ **isp\_customer** にはバックアップサーバが設定されていないため、フェールオーバーは行われません。

## 例：DNIS による AAA ブロードキャスト アカウントティングの設定

次に、グローバル `aaa dnis map accounting network` コマンドを使用して、DNIS ごとのブロードキャスト アカウントティングを有効にする例を示します。

```
Device> enable
Device# configure terminal
Device(config)# aaa group server radius isp
Device(config-sg-radius)# server 10.0.0.1
Device(config-sg-radius)# server 10.0.0.2
Device(config-sg-radius)# exit
Device(config)# aaa group server tacacs+ isp_customer
Device config-sg-tacacs+)# server 172.0.0.1
Device config-sg-tacacs+)# exit
Device(config)# aaa dnis map enable
Device(config)# aaa dnis map 7777 accounting network start-stop broadcast group isp group
isp_customer
Device(config)# tacacs server server1
Device(config-server-tacacs)# address ipv4 172.0.0.1
Device(config-server-tacacs)# key key_2
Device(config-server-tacacs)# end
```

**broadcast** キーワードによって、DNIS 番号 7777 のネットワーク接続コールに関する「開始」および「終了」アカウントティング レコードが、グループ `isp` ではサーバー 10.0.0.1 に、グループ `isp_customer` ではサーバー 172.0.0.1 に同時送信されます。サーバ 10.0.0.1 が使用できなくなると、サーバ 10.0.0.2 へのフェールオーバーが行われます。サーバ 172.0.0.1 が使用できなくなっても、グループ `isp_customer` にはバックアップサーバが設定されていないため、フェールオーバーは行われません。

## 例：AAA セッション MIB

次に、AAA セッション MIB 機能を設定して、PPP ユーザの認証済みクライアント接続を解除する例を示します。

```
aaa new-model
aaa authentication ppp default group radius
aaa authorization network default group radius
aaa accounting network default start-stop group radius
aaa session-mib disconnect
```

## アカウントティングの設定に関するその他の参考資料

ここでは、アカウントティングの設定機能に関する関連資料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
IOS コマンド	『 <a href="#">Cisco IOS Master Command List, All Releases</a> 』 [英語]

**MIB**

MIB	MIB のリンク
<ul style="list-style-type: none"> <li>• CISCO-AAA-SESSION-MIB</li> </ul>	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、および機能セットの MIB を検索してダウンロードする場合は、次の URL にある Cisco MIB Locator を使用します。  <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

**RFC**

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

**シスコのテクニカル サポート**

説明	リンク
<p>シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。</p> <p>お使いの製品のセキュリティ情報や技術情報入手するために、Cisco Notification Service (Field Notice からアクセス)、Cisco Technical Services Newsletter、Really Simple Syndication (RSS) フィードなどの各種サービスに加入できます。</p> <p>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。</p>	<a href="http://www.cisco.com/en/US/support/index.html">http://www.cisco.com/en/US/support/index.html</a>

## アカウントティングの設定の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	AAA ブロードキャスト アカウンティング	AAA ブロードキャスト アカウンティングを有効にすると、アカウントティング情報を複数の AAA サーバーに同時に送信できます。つまり、アカウントティング情報を1つまた複数の AAA サーバーに同時にブロードキャストすることが可能です。
Cisco IOS XE Everest 16.5.1a	AAA セッション MIB	ユーザーが AAA セッション MIB 機能を使用すると、SNMP を使用して自身の認証済みクライアント接続をモニターおよび終了できます。
Cisco IOS XE Everest 16.5.1a	接続アカウントティング	接続アカウントティングは、Telnet、ローカルエリアトランスポート、TN3270、Packet Assembler/disassembler (PAD)、rlogin など、ネットワークアクセスサーバーからのアウトバウンド接続すべてに関する情報を提供します。
Cisco IOS XE Everest 16.5.1a	AAA 中間アカウントティング	AAA 中間アカウントティングにより、レポートする必要がある新しいアカウントティング情報が発生するたびに、または定期的に、アカウントティングサーバーに中間アカウントティング レコードを送信できます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。





## 第 6 章

# ローカル認証および許可の設定

- ローカル認証および許可の設定方法 (137 ページ)
- ローカル認証および許可のモニタリング (139 ページ)
- ローカル認証および許可の機能履歴 (140 ページ)

## ローカル認証および許可の設定方法

### スイッチのローカル認証および許可の設定

ローカルモードで AAA を実装するようにスイッチを設定すると、サーバーがなくても動作するように AAA を設定できます。この場合、スイッチは認証および許可の処理を行います。この設定ではアカウントिंग機能は使用できません。



(注) AAA 方式を使用して HTTP アクセスに対しスイッチのセキュリティを確保するには、**ip http authentication aaa** グローバル コンフィギュレーション コマンドでスイッチを設定する必要があります。AAA 認証を設定しても、AAA 方式を使用した HTTP アクセスに対しスイッチのセキュリティは確保しません。

ローカルモードで AAA を実装するようにスイッチを設定して、サーバーがなくても動作するように AAA を設定するには、次の手順を実行します。

#### 手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login default local**
5. **aaa authorization exec default local**
6. **aaa authorization network default local**
7. **username name [ privilege level ] { password encryption-type password }**
8. **end**

9. **show running-config**
10. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： デバイス> <b>enable</b>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>• パスワードを入力します（要求された場合）。</li> </ul>
ステップ 2	<b>configure terminal</b> 例： デバイス# <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 3	<b>aaa new-model</b> 例： デバイス (config)# <b>aaa new-model</b>	AAA をイネーブルにします。
ステップ 4	<b>aaa authentication login default local</b> 例： デバイス (config)# <b>aaa authentication login default local</b>	ローカル ユーザ名データベースを使用するログイン認証を設定します。 <b>default</b> キーワードにより、ローカルユーザデータベース認証がすべてのポートに適用されます。
ステップ 5	<b>aaa authorization exec default local</b> 例： デバイス (config)# <b>aaa authorization exec default local</b>	ユーザの AAA 許可を設定し、ローカルデータベースを確認して、そのユーザに EXEC シェルの実行を許可します。
ステップ 6	<b>aaa authorization network default local</b> 例： デバイス (config)# <b>aaa authorization network default local</b>	ネットワーク関連のすべてのサービス要求に対してユーザ AAA 許可を設定します。
ステップ 7	<b>username name [ privilege level] { password encryption-type password}</b> 例：	ローカル データベースを入力し、ユーザ名ベースの認証システムを設定します。 ユーザごとにコマンドを繰り返し入力します。



	コマンドまたはアクション	目的
	デバイス (config)# <b>username your_user_name privilege 1 password 7 secret567</b>	<ul style="list-style-type: none"> <li>• <i>name</i> には、ユーザー ID を 1 ワードで指定します。スペースと引用符は使用できません。</li> <li>• (任意) <i>level</i> には、アクセス権を得たユーザーに設定する権限レベルを指定します。指定できる範囲は 0 ~ 15 です。レベル 15 では特権 EXEC モードでのアクセスが可能です。レベル 0 では、ユーザ EXEC モードでのアクセスとなります。</li> <li>• <i>encryption-type</i> には、暗号化されていないパスワードが後ろに続く場合は 0 を、暗号化されたパスワードが後ろに続く場合は 7 を指定します。</li> <li>• <i>password</i> には、ユーザーがスイッチにアクセスする場合に入力する必要があるパスワードを指定します。パスワードは 1 ~ 25 文字で、埋め込みスペースを使用でき、<b>username</b> コマンドの最後のオプションとして指定します。</li> </ul>
ステップ 8	<b>end</b> 例： デバイス (config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 9	<b>show running-config</b> 例： デバイス# <b>show running-config</b>	入力を確認します。
ステップ 10	<b>copy running-config startup-config</b> 例： デバイス# <b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。

## ローカル認証および許可のモニタリング

ローカル認証および許可の設定を表示するには、**show running-config** 特権 EXEC コマンドを使用します。

## ローカル認証および許可の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	ローカル認証および許可	ローカルモードで AAA を実装するようにデバイスを設定すると、サーバがなくても動作するように AAA を設定できます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



## 第 7 章

# TACACS+ の設定

- [TACACS+ の前提条件 \(141 ページ\)](#)
- [TACACS+ によるスイッチ アクセスの制御について \(142 ページ\)](#)
- [TACACS+ とスイッチ アクセスを設定する方法 \(146 ページ\)](#)
- [TACACS+ のモニタリング \(154 ページ\)](#)
- [TACACS+ によるスイッチ アクセスの制御に関するその他の参考資料 \(155 ページ\)](#)
- [TACACS+ の機能の履歴 \(155 ページ\)](#)

## TACACS+ の前提条件

TACACS+によるスイッチアクセスのセットアップと設定の前提条件は、次のとおりです（示されている順序で実行する必要があります）。

1. スイッチに TACACS+ サーバー アドレスとスイッチを設定します。
2. 認証キーを設定します。
3. TACACS+ サーバでステップ 2 からキーを設定します。
4. 認証、許可、アカウントिंग (AAA) をイネーブルにする。
5. ログイン認証方式リストを作成します。
6. 端末回線にリストを適用します。
7. 認証およびアカウントिंग方式のリストを作成します。

TACACS+ によるスイッチ アクセスの制御の前提条件は、次のとおりです。

- スイッチ上で TACACS+ 機能を設定するには、設定済みの TACACS+ サーバーにアクセスする必要があります。また、通常 LINUX または Windows ワークステーション上で稼働する TACACS+ デーモンのデータベースで管理されている TACACS+ サービスにもアクセスする必要があります。
- スイッチで TACACS+ を使用するには、TACACS+ デーモン ソフトウェアが稼働するシステムが必要です。

- TACACS+ を使用するには、それをイネーブルにする必要があります。
- 許可は、使用するスイッチでイネーブルにする必要があります。
- 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。
- このセクションに記載されている AAA コマンドのいずれかを使用するには、まず **aaa new-model** コマンドを使用して AAA をイネーブルにする必要があります。
- 最低限、TACACS+ デーモンを維持するホスト（1つまたは複数）を特定し、TACACS+ 認証の方式リストを定義する必要があります。また、任意で TACACS+ 許可およびアカウントिंगの方式リストを定義できます。
- 方式リストは実行される認証のタイプと実行順序を定義します。このリストを特定のポートに適用してから、定義済み認証方式を実行する必要があります。唯一の例外はデフォルトの方式リスト（偶然に *default* と名前が付けられている）です。デフォルトの方式リストは、名前付き方式リストを明示的に定義されたインターフェイスを除いて、自動的にすべてのポートに適用されます。定義済みの方式リストは、デフォルトの方式リストに優先します。
- TACACS+ を使用して認証を行った場合は、TACACS+ を使用して特権 EXEC アクセスを許可します。
- 認証に TACACS+ を使用しなかった場合は、ローカル データベースを使用します。

## TACACS+ によるスイッチ アクセスの制御について

### TACACS+ およびスイッチ アクセス

ここでは、TACACS+ について説明します。TACACS+ は詳細なアカウントング情報を提供し、認証と許可のプロセスを柔軟に管理します。TACACS+ は、認証、許可、アカウントング（AAA）機能により拡張されており、TACACS+ をイネーブルにするには AAA コマンドを使用する必要があります。

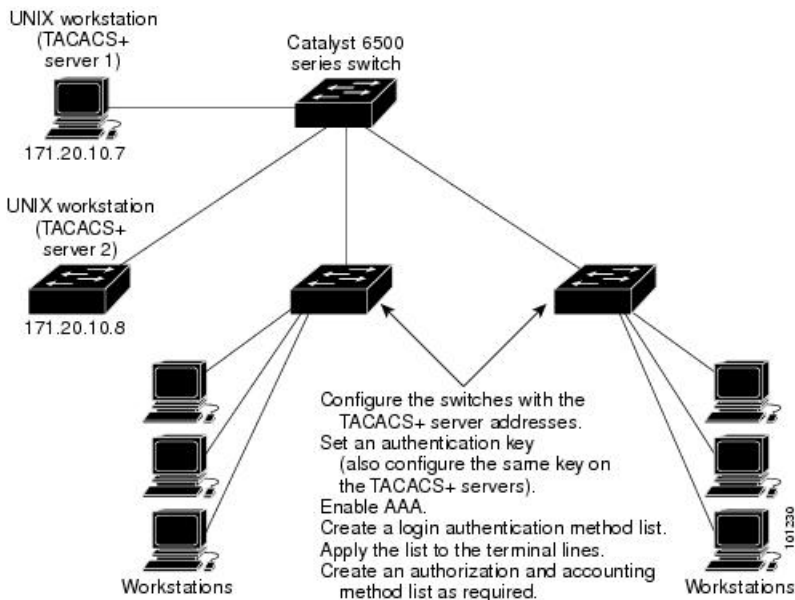
### TACACS+ の概要

TACACS+ は、スイッチにアクセスしようとするユーザー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+ では、独立したモジュラ型の認証、許可、アカウントング機能が提供されます。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、およびアカウントング）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+ の目的は、1 つの管理サービスから複数のネットワーク アクセス ポイントを管理する方式を提供することです。スイッチは、他の Cisco ルータやアクセス サーバとともにネットワーク アクセス サーバにできます。

図 9: 一般的な TACACS+ ネットワーク 構成



TACACS+ は、AAA セキュリティ サービスによって管理され、次のようなサービスを提供します。

- 認証：ログインおよびパスワードダイアログ、チャレンジおよび応答、メッセージサポートによって認証の完全制御を行います。

認証機能は、ユーザとの対話を実行できます（たとえば、ユーザ名とパスワードが入力された後、自宅の住所、母親の旧姓、サービスタイプ、社会保険番号などのいくつかの質問をすることによりユーザを試します）。TACACS+ 認証サービスは、ユーザ画面にメッセージを送信することもできます。たとえば、会社のパスワード有効期間ポリシーに従い、パスワードの変更の必要があることをユーザに通知することもできます。

- 許可：autocommand、アクセスコントロール、セッション期間、プロトコルサポートの設定といった、ユーザーセッション時のユーザー機能についてきめ細かく制御します。また、TACACS+ 許可機能によって、ユーザーが実行できるコマンドを制限することもできます。
- アカウンティング：課金、監査、およびレポートに使用する情報を収集して TACACS+ デーモンに送信します。ネットワークの管理者は、アカウンティング機能を使用して、セキュリティ監査のためにユーザの活動状況をトラッキングしたり、ユーザ課金用の情報を提供したりできます。アカウンティングレコードには、ユーザ ID、開始時刻および終了時刻、実行されたコマンド（PPP など）、パケット数、およびバイト数が含まれます。

TACACS+ プロトコルは、スイッチと TACACS+ デーモン間の認証を行い、スイッチと TACACS+ デーモン間のプロトコル交換をすべて暗号化することによって機密保持を実現します。

## TACACS+ の動作

ユーザーが、TACACS+ を使用しているスイッチに対して簡易 ASCII ログインを試行し、認証が必要になると、次のプロセスが発生します。

1. 接続が確立されると、スイッチは TACACS+ デーモンに接続してユーザー名プロンプトを取得し、これをユーザーに表示します。ユーザーがユーザー名を入力すると、スイッチは TACACS+ デーモンに接続してパスワードプロンプトを取得します。スイッチによってパスワードプロンプトが表示され、ユーザーがパスワードを入力すると、そのパスワードが TACACS+ デーモンに送信されます。

TACACS+ によって、デーモンとユーザとの間の対話が可能になり、デーモンはユーザを認証できるだけの情報を取得できるようになります。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、ユーザの母親の旧姓など、その他の項目を含めることもできます。

2. スイッチは、最終的に TACACS+ デーモンから次のいずれかの応答を得ます。
  - **ACCEPT** : ユーザーが認証され、サービスを開始できます。許可を必要とするようにスイッチが設定されている場合は、この時点で許可処理が開始されます。
  - **REJECT** : ユーザーは認証されません。TACACS+ デーモンに応じて、ユーザーはアクセスを拒否されるか、ログインシーケンスを再試行するように求められます。
  - **ERROR** : デーモンによる認証サービスのある時点で、またはデーモンとスイッチの間のネットワーク接続においてエラーが発生しました。ERROR 応答が表示された場合は、スイッチは、通常別の方法でユーザーを認証しようとします。
  - **CONTINUE** : ユーザーは、さらに認証情報の入力を求められます。

認証後、スイッチで許可がイネーブになっている場合、ユーザーは追加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+ 許可が必要な場合は、再び TACACS+ デーモンに接続し、デーモンが **ACCEPT** または **REJECT** の許可応答を返します。ACCEPT 応答が返された場合は、その応答に、そのユーザおよびそのユーザがアクセスできるサービスの、EXEC または NETWORK セッション宛ての属性の形式でデータが含まれています。
  - Telnet、セキュア シェル (SSH)、rlogin、または特権 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、アクセスリスト、およびユーザタイムアウトを含む)

## 方式リスト

方式リストによって、ユーザの認証、許可、またはアカウント維持のための順序と方式を定義します。方式リストを使用して、使用するセキュリティプロトコルを1つまたは複数指定できるので、最初の方式が失敗した場合のバックアップシステムが確保されます。ソフトウェア

は、リスト内の最初の方式を使用してユーザの認証、許可、アカウントの維持を行います。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の方式を選択します。このプロセスは、リスト内の方式による通信が成功するか、方式リストの方式をすべて試し終わるまで続きます。

VTY 回線で方式リストを設定する場合、対応する方式リストを AAA に追加する必要があります。次の例は、VTY 回線の下に方式リストを設定する方法を示しています。

```
Device# configure terminal
Device(config)# line vty 0 4
Device(config)# authorization commands 15 auth1
```

次の例は、AAA で方式リストを設定する方法を示しています。

```
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authorization commands 15 auth1 group tacacs+
```

VTY 回線で方式リストを設定しない場合、デフォルトの方式リストを AAA に追加する必要があります。次の例は、方式リストを使用しない VTY 設定を示しています。

```
Device# configure terminal
Device(config)# line vty 0 4
```

次の例は、デフォルトの方式リストを設定する方法を示しています。

```
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authorization commands 15 default group tacacs+
```

## TACACS+ 設定オプション

認証用に1つのサーバーを使用することも、また、既存のサーバーホストをグループ化するために AAA サーバー グループを使用するように設定することもできます。サーバをグループ化して設定済みサーバホストのサブセットを選択し、特定のサービスにそのサーバを使用できます。サーバグループは、グローバルサーバホストリストとともに使用され、選択されたサーバホストの IP アドレスのリストが含まれています。

## TACACS+ ログイン認証

方式リストは、ユーザ認証のためクエリ送信を行う手順と認証方式を記述したものです。認証に使用する1つまたは複数のセキュリティプロトコルを指定できるので、最初の方式が失敗した場合のバックアップシステムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の認証方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。この処理のある時点で認証が失敗した場合（つまり、セキュリティサーバまたはローカルのユーザ名データベースがユーザアクセスを拒否すると応答した場合）、認証プロセスは停止し、それ以上認証方式が試行されることはありません。

## 特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可

AAA 許可によってユーザが利用できるサービスが制限されます。AAA 許可がイネーブルに設定されていると、スイッチはユーザーのプロファイルから取得した情報を使用します。このプロファイルは、ローカルのユーザーデータベースまたはセキュリティサーバー上にあり、ユーザーのセッションを設定します。ユーザは、ユーザプロファイル内の情報で認められている場合限り、要求したサービスのアクセスが認可されます。

## TACACS+ Accounting

AAA アカウンティング機能は、ユーザがアクセスしたサービスと、消費したネットワークリソース量をトラッキングします。AAA アカウンティングをイネーブルにすると、スイッチはユーザーの活動状況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ーに報告します。各アカウンティングレコードにはアカウンティングの Attribute-Value (AV) ペアが含まれ、レコードはセキュリティサーバに格納されます。このデータを、ネットワーク管理、クライアント請求、または監査のために分析できます。

## TACACS+ のデフォルト設定

TACACS+ および AAA は、デフォルトではディセーブルに設定されています。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して TACACS+ を設定することはできません。TACACS+ をイネーブルに設定した場合、CLI を通じてスイッチにアクセスするユーザを認証できます。



(注) TACACS+ の設定は CLI を使用して行いますが、TACACS+ サーバは権限レベル 15 に設定された HTTP 接続を許可します。

## TACACS+ とスイッチ アクセスを設定する方法

ここでは、TACACS+ をサポートするようにスイッチを設定する方法について説明します。

## TACACS+ サーバホストの指定および認証キーの設定

TACACS+ サーバホストを特定し、認証キーを設定するには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **tacacs server *server-name***
4. **address {ipv4 | ipv6} *ip address***



5. **key** [*encryption-type*] [*key-string*]
6. **exit**
7. **aaa new-model**
8. **aaa group server tacacs+ group-name**
9. **server name server-name**
10. **end**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例： Device# <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 3	<b>tacacs server server-name</b> 例： Device(config)# <b>tacacs server yourserver</b>	TACACS+ サーバを維持する IP ホストを特定します。このコマンドを複数回入力して、優先ホストのリストを作成します。ソフトウェアは、指定された順序でホストを検索します。 <i>server-name</i> にはサーバ名を指定します。
ステップ 4	<b>address {ipv4   ipv6} ip address</b> 例： Device(config-server-tacacs)# <b>address ipv4 10.0.1.12</b>	TACACS サーバの IP アドレスを設定します。
ステップ 5	<b>key [encryption-type] [key-string]</b> 例： Device(config-server-tacacs)# <b>key 0 auth-key</b>	アクセス サーバと TACACS+ デーモンとのすべての TACACS+ 通信に使用される認証暗号キーを設定します。この暗号化キーは、TACACS+ デーモンで使用するキーと一致している必要があります。 <i>encryption-type</i> はオプションで、何も指定されていない場合はクリアテキストと見なされます。暗号化されていないキーが後ろに続くよう指定するには、 <b>0</b> を入力します。暗号化されたキーが後ろに続くよう指定するには、 <b>6</b> を入力します。隠れたキーが後ろに続くよう指定するには、 <b>7</b> を入力します。
ステップ 6	<b>exit</b> 例： Device(config-server-tacacs)# <b>exit</b>	TACACS サーバモードを終了して、グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 7	<b>aaa new-model</b> 例： Device(config)# <b>aaa new-model</b>	AAA をイネーブルにします。
ステップ 8	<b>aaa group server tacacs+ group-name</b> 例： Device(config)# <b>aaa group server tacacs+ your_server_group</b>	(任意) グループ名を使用して AAA サーバグループを定義し、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 9	<b>server name server-name</b> 例： Device(config-sg-tacacs)# <b>server name yourserver</b>	(任意) 特定の TACACS+ サーバを定義済みサーバグループに関連付けます。AAA サーバグループの TACACS+ サーバごとに、このステップを繰り返します。  グループの各サーバは、ステップ 3 で定義済みのものでなければなりません。
ステップ 10	<b>end</b> 例： Device(config-sg-tacacs)# <b>end</b>	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、特権 EXEC モードに戻ります。

## TACACS+ ログイン認証の設定

TACACS+ ログイン認証を設定するには、次の手順を実行します。

### 始める前に

AAA 認証を設定するには、認証方式の名前付きリストを作成してから、各種ポートにそのリストを適用します。



- (注) AAA 方式を使用して HTTP アクセスに対するセキュリティを確保するには、**ip http authentication aaa** グローバル コンフィギュレーション コマンドで設定する必要があります。AAA 認証を設定しても、AAA 方式を使用した HTTP アクセスに対するセキュリティは確保しません。

**ip http authentication** コマンドの詳細については、『Cisco IOS Security Command Reference, Release 12.4』を参照してください。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login {default | list-name} method1 [method2... ]**

5. `line [console | tty | vty] line-number [ending-line-number]`
6. `login authentication {default | list-name}`
7. `end`
8. `show running-config`
9. `copy running-config startup-config`

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： デバイス> <b>enable</b>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>• パスワードを入力します（要求された場合）。</li> </ul>
ステップ 2	<b>configure terminal</b> 例： デバイス# <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 3	<b>aaa new-model</b> 例： デバイス(config)# <b>aaa new-model</b>	AAA をイネーブルにします。
ステップ 4	<b>aaa authentication login {default   list-name} method1 [method2... ]</b> 例： デバイス(config)# <b>aaa authentication login default tacacs+ local</b>	ログイン認証方式リストを作成します。 <ul style="list-style-type: none"> <li>• <b>login authentication</b> コマンドにリストが指定されていない場合に使用するデフォルトのリストを作成するには、<b>default</b> キーワードの後ろにデフォルト状況で使用される方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。</li> <li>• <b>list-name</b> には、作成するリストの名前として使用する文字列を指定します。</li> <li>• <b>method1...</b> には、認証アルゴリズムが試行する実際の方式を指定します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。</li> </ul> 次のいずれかの方式を選択します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <b>enable</b> : イネーブルパスワードを認証に使用します。この認証方式を使用するには、あらかじめ <b>enable password</b> グローバルコンフィギュレーションコマンドを使用してイネーブルパスワードを定義しておく必要があります。</li> <li>• <b>group tacacs+</b> : TACACS+ 認証を使用します。この認証方式を使用するには、あらかじめ TACACS+ サーバーを設定しておく必要があります。</li> <li>• <b>line</b> : 回線パスワードを認証に使用します。この認証方式を使用するには、あらかじめ回線パスワードを定義しておく必要があります。 <b>password password</b> ラインコンフィギュレーションコマンドを使用します。</li> <li>• <b>local</b> : ローカルユーザー名データベースを認証に使用します。データベースにユーザー名情報を入力しておく必要があります。<b>username password</b> 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。</li> <li>• <b>local-case</b> : 大文字と小文字が区別されるローカルユーザー名データベースを認証に使用します。<b>username name password</b> グローバルコンフィギュレーションコマンドを使用して、ユーザー名情報をデータベースに入力する必要があります。</li> <li>• <b>none</b> : ログインに認証を使用しません。</li> </ul>
ステップ 5	<b>line [console   tty   vty] line-number [ending-line-number]</b> 例 :  デバイス (config) # <b>line 2 4</b>	ラインコンフィギュレーションモードを開始し、認証リストを適用する回線を設定します。
ステップ 6	<b>login authentication {default   list-name}</b> 例 :  デバイス (config-line) # <b>login authentication default</b>	1つの回線または複数回線に認証リストを適用します。 <ul style="list-style-type: none"> <li>• <b>default</b> を指定する場合は、<b>aaa authentication login</b> コマンドで作成したデフォルトのリストを使用します。</li> <li>• <b>list-name</b> には、<b>aaa authentication login</b> コマンドで作成したリストを指定します。</li> </ul>

	コマンドまたはアクション	目的
ステップ 7	<b>end</b> 例：  デバイス(config-line)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 8	<b>show running-config</b> 例：  デバイス# <b>show running-config</b>	入力を確認します。
ステップ 9	<b>copy running-config startup-config</b> 例：  デバイス# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## 特権 EXEC アクセスおよびネットワーク サービス用の TACACS+ 許可の設定

**aaa authorization** グローバル コンフィギュレーション コマンドと **tacacs+** キーワードを使用すると、ユーザのネットワークアクセスを特権 EXEC モードに制限するパラメータを設定できます。



(注) 許可が設定されていても、CLI を使用してログインし、認証されたユーザに対しては、許可は省略されます。

特権 EXEC アクセスおよびネットワーク サービスに関する TACACS+ 許可を指定するには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **aaa authorization network tacacs+**
4. **aaa authorization exec tacacs+**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  デバイス> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  デバイス# <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 3	<b>aaa authorization network tacacs+</b> 例：  デバイス(config)# <b>aaa authorization network tacacs+</b>	ネットワーク関連のすべてのサービス要求に対してユーザー TACACS+ 認可を行うことを設定します。
ステップ 4	<b>aaa authorization exec tacacs+</b> 例：  デバイス(config)# <b>aaa authorization exec tacacs+</b>	ユーザーの特権 EXEC アクセスに対してユーザー TACACS+ 許可を行うことを設定します。  <b>exec</b> キーワードを指定すると、ユーザープロファイル情報（ <b>autocommand</b> 情報など）が返される場合があります。
ステップ 5	<b>end</b> 例：  デバイス(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 6	<b>show running-config</b> 例：  デバイス# <b>show running-config</b>	入力を確認します。
ステップ 7	<b>copy running-config startup-config</b> 例：  デバイス# <b>copy running-config startup-config</b>	（任意）コンフィギュレーションファイルに設定を保存します。

## TACACS+ アカウンティングの起動

TACACS+ アカウンティングを開始するには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **aaa accounting network start-stop tacacs+**
4. **aaa accounting exec start-stop tacacs+**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  デバイス> <b>enable</b>	特権 EXEC モードを有効にします。  <ul style="list-style-type: none"> <li>• パスワードを入力します（要求された場合）。</li> </ul>
ステップ 2	<b>configure terminal</b> 例：  デバイス# <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 3	<b>aaa accounting network start-stop tacacs+</b> 例：  デバイス(config)# <b>aaa accounting network start-stop tacacs+</b>	ネットワーク関連のすべてのサービス要求について、TACACS+ アカウンティングをイネーブルにします。
ステップ 4	<b>aaa accounting exec start-stop tacacs+</b> 例：  デバイス(config)# <b>aaa accounting exec start-stop tacacs+</b>	TACACS+ アカウンティングをイネーブルにして、特権 EXEC プロセスの最初に記録開始アカウンティング通知、最後に記録停止通知を送信します。
ステップ 5	<b>end</b> 例：  デバイス(config)# <b>end</b>	特権 EXEC 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 6	<b>show running-config</b> 例： デバイス# <b>show running-config</b>	入力を確認します。
ステップ 7	<b>copy running-config startup-config</b> 例： デバイス# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

### 次のタスク

AAA サーバが到達不能な場合にルータとのセッションを確立するには、**aaa accounting system guarantee-first** コマンドを使用します。これは、最初のレコードとしてシステムアカウンティングを保証します（これがデフォルトの条件です）。場合によっては、システムがリロードされるまでコンソールまたは端末接続でセッションを開始できない場合があります。システムのリロードにかかる時間は3分を超えることがあります。

ルータのリロード時に AAA サーバが到達不能な場合に、ルータとのコンソールセッションまたは Telnet セッションを確立するには、**no aaa accounting system guarantee-first** コマンドを使用します。

## AAA サーバが到達不能な場合のルータとのセッションの確立

AAA サーバが到達不能な場合にルータとのセッションを確立するには、**aaa accounting system guarantee-first** コマンドを使用します。これは、最初のレコードとしてシステムアカウンティングを保証します（これがデフォルトの条件です）。場合によっては、システムがリロードされるまでコンソールまたは端末接続でセッションを開始できない場合があります。システムのリロードにかかる時間は3分を超えることがあります。

ルータのリロード時に AAA サーバが到達不能な場合に、ルータとのコンソールセッションまたは Telnet セッションを確立するには、**no aaa accounting system guarantee-first** コマンドを使用します。

## TACACS+ のモニタリング

表 19: TACACS+ 情報を表示するためのコマンド

コマンド	目的
<b>show tacacs</b>	TACACS+ サーバの統計情報を表示します。



# TACACS+によるスイッチアクセスの制御に関するその他の参考資料

## 関連資料

関連項目	マニュアル タイトル
AAA の設定	<a href="#">ローカル認証および許可の設定</a>

## MIB

MIB	MIB のリンク
	<p>選択したプラットフォーム、Cisco IOS リリース、およびフィーチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

## シスコのテクニカル サポート

説明	リンク
<p>シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。</p> <p>お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service (Field Notice からアクセス)、Cisco Technical Services Newsletter、Really Simple Syndication (RSS) フィードなどの各種サービスに加入できます。</p> <p>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。</p>	<a href="http://www.cisco.com/support">http://www.cisco.com/support</a>

## TACACS+ の機能の履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	TACACS+	TACACS+ は、認証および認可プロセスについて詳細なアカウント情報と柔軟な管理コントロールを提供します。TACACS+は、AAA を介して実装され、AAA コマンドを使用するのみイネーブルにできます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



## 第 8 章

# RADIUS の設定

- RADIUS を設定するための前提条件 (157 ページ)
- RADIUS の設定に関する制約事項 (158 ページ)
- RADIUS に関する情報 (158 ページ)
- RADIUS の設定方法 (187 ページ)
- CoA 機能のモニタリング (205 ページ)
- RADIUS の機能の履歴 (205 ページ)

## RADIUS を設定するための前提条件

ここでは、RADIUS による デバイス アクセスの制御の前提条件を示します。

全般：

- この章のいずれかのコンフィギュレーションコマンドを使用するには、RADIUS および認証、許可、ならびにアカウントिंग (AAA) をイネーブルにする必要があります。
- RADIUS は、AAA を介して実装され、AAA コマンドを使用してのみイネーブルにできません。
- **aaa new-model** グローバル コンフィギュレーション コマンドを使用して、AAA をイネーブルにします。
- **aaa authentication** グローバル コンフィギュレーション コマンドを使用して、RADIUS 認証の方式リストを定義します。
- **line** および **interface** コマンドを使用して、使用する定義済みの方式リストをイネーブルにします。
- 最低限、RADIUS サーバソフトウェアが稼働するホスト (1 つまたは複数) を特定し、RADIUS 認証の方式リストを定義する必要があります。また、任意で RADIUS 許可およびアカウントिंगの方式リストを定義できます。
- デバイス 上で RADIUS 機能の設定を行う前に、RADIUS サーバにアクセスし、サーバを設定する必要があります。

- RADIUS ホストは、通常、シスコ（Cisco Secure Access Control Server バージョン 3.0）、Livingston、Merit、Microsoft、または他のソフトウェアプロバイダーの RADIUS サーバソフトウェアが稼働しているマルチユーザシステムです。詳細については、RADIUS サーバのマニュアルを参照してください。
- Change-of-Authorization (CoA) インターフェイスを使用するには、スイッチにセッションがすでに存在している必要があります。CoA を使用すると、セッションの識別と接続解除要求を実行できます。アップデートは、指定されたセッションにだけ作用します。

RADIUS 操作の場合：

- ユーザは RADIUS 許可に進む前に、まず RADIUS 認証を正常に完了する必要があります（イネーブルに設定されている場合）。

## RADIUS の設定に関する制約事項

ここでは、RADIUS による デバイス アクセスの制御の制約事項について説明します。

全般：

- セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して RADIUS を設定することはできません。

RADIUS は次のネットワーク セキュリティ状況には適していません。

- マルチプロトコルアクセス環境。RADIUS は、AppleTalk Remote Access (ARA)、NetBIOS Frame Control Protocol (NBFCP)、NetWare Asynchronous Services Interface (NASI)、または X.25 PAD 接続をサポートしません。
- スイッチ間またはルータ間状態。RADIUS は、双方向認証を行いません。RADIUS は、他社製のデバイスが認証を必要とする場合に、あるデバイスから他社製のデバイスへの認証に使用できます。
- 各種のサービスを使用するネットワーク。RADIUS は、一般に 1 人のユーザを 1 つのサービス モデルにバインドします。

## RADIUS に関する情報

### RADIUS およびスイッチ アクセス

この項では、RADIUS をイネーブルにし、設定する方法について説明します。RADIUS を使用すると、アカウントの詳細を取得したり、認証および許可プロセスの柔軟な管理制御を実現できます。

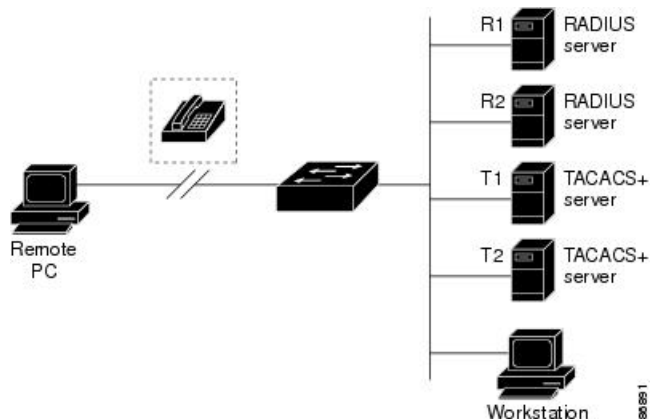
## RADIUS の概要

RADIUS は、不正なアクセスからネットワークのセキュリティを保護する分散クライアント/サーバシステムです。RADIUS クライアントは、サポート対象の Cisco ルータおよびスイッチ上で稼働します。クライアントは中央の RADIUS サーバに認証要求を送ります。中央の RADIUS サーバにはすべてのユーザ認証情報、ネットワーク サービス アクセス情報が登録されています。

RADIUS は、アクセスのセキュリティが必要な、次のネットワーク環境で使用します。

- それぞれが RADIUS をサポートする、マルチベンダー アクセス サーバによるネットワーク。たとえば、複数のベンダーのアクセスサーバが、1つの RADIUS サーバベースセキュリティ データベースを使用します。複数ベンダーのアクセスサーバからなる IP ベースのネットワークでは、ダイヤルインユーザは RADIUS サーバを通じて認証されます。RADIUS サーバは、Kerberos セキュリティシステムで動作するようにカスタマイズされています。
- アプリケーションが RADIUS プロトコルをサポートするターンキー ネットワーク セキュリティ環境。たとえば、スマートカードアクセス コントロールシステムを使用するアクセス環境。あるケースでは、RADIUS は Enigma のセキュリティカードとともに使用してユーザを確認し、ネットワーク リソースのアクセスを許可します。
- すでに RADIUS を使用中のネットワーク。RADIUS クライアント装備のシスコ デバイス ネットワークに追加できます。これが TACACS+ サーバへの移行の最初のステップとなることもあります。下の図「RADIUS サービスから TACACS+ サービスへの移行」を参照してください。
- ユーザが 1つのサービスにしかアクセスできないネットワーク。RADIUS を使用すると、ユーザのアクセスを 1つのホスト、Telnet などの 1つのユーティリティ、または IEEE 802.1x などのプロトコルを使用するネットワークに制御できます。このプロトコルの詳細については、「IEEE 802.1x ポートベース認証の設定」の章を参照してください。
- リソース アカウンティングが必要なネットワーク。RADIUS 認証または許可とは別個に RADIUS アカウンティングを使用できます。RADIUS アカウンティング機能によって、サービスの開始および終了時点でデータを送信し、このセッション中に使用されるリソース（時間、パケット、バイトなど）の量を表示できます。インターネット サービス プロバイダーは、RADIUS アクセス コントロールおよびアカウンティング ソフトウェアのフリーウェアバージョンを使用して、特殊なセキュリティおよび課金に対するニーズを満たすこともできます。

図 10: RADIUS サービスから TACACS+ サービスへの移行



## RADIUS の動作

RADIUS サーバーによってアクセスコントロールされる デバイス に、ユーザーがログインおよび認証を試みると、次のイベントが発生します。

1. ユーザ名およびパスワードの入力を要求するプロンプトが表示されます。
2. 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。
3. 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 : ユーザーが認証されたことを表します。
  - REJECT : ユーザーの認証が失敗し、ユーザー名およびパスワードの再入力が必要されるか、またはアクセスが拒否されます。
  - CHALLENGE : ユーザーに追加データを要求します。
  - CHALLENGE PASSWORD : ユーザーは新しいパスワードを選択するように要求されます。

ACCEPT または REJECT 応答には、特権 EXEC またはネットワーク許可に使用する追加データがバンドルされています。ACCEPT または REJECT パケットには次の追加データが含まれます。

- Telnet、SSH、rlogin、または特権 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、アクセスリスト、およびユーザタイムアウトを含む)

## RADIUS 許可の変更

RADIUS 許可の変更 (CoA) は、認証、認可、およびアカウントリング (AAA) セッションの属性を認証された後に変更するためのメカニズムを提供します。AAA でユーザー、またはユーザーグループのポリシーが変更された場合、管理者は、AAA サーバーから Cisco Secure Access Control Server (ACS) などの RADIUS CoA パケットを送信し、認証を再初期化して新しいポリシーを適用することができます。このセクションでは、使用可能なプリミティブおよびそれらの CoA での使用方法を含む、RADIUS インターフェイスの概要について説明します。

- Change-of-Authorization 要求
- CoA 要求応答コード
- CoA 要求コマンド
- セッション再認証
- セッション強制終了のスタック構成ガイドライン

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、クエリーが送信されたサーバーが応答するプルモデルで使用されます。Catalyst は、RFC 5176 で規定された (通常はプッシュモデルで使用される) RADIUS CoA 拡張機能をサポートし、外部の AAA またはポリシーサーバーからのセッションを動的に再設定できるようにします。

は、次のセッション単位の CoA 要求をサポートしています。

- セッション再認証
- セッションの終了
- ポート シャットダウンでのセッション終了
- ポート バウンスでのセッション終了

この機能は、Cisco Secure Access Control Server (ACS) 5.1 に統合されています。

Catalyst で、RADIUS インターフェイスはデフォルトでイネーブルに設定されています。ただし、次の属性については、一部の基本的な設定が必要になります。

- セキュリティおよびパスワード：このガイドの「スイッチへの不正アクセスの防止」を参照してください。
- アカウントリング：このガイドの「スイッチベース認証の設定」の章の「RADIUS アカウントリングの起動」の項を参照してください。

Cisco IOS ソフトウェアは、RFC 5176 で定義されている RADIUS CoA の拡張をサポートします。この拡張は、一般に、外部 AAA またはポリシーサーバーからのセッションのダイナミックな再構成を可能にするプッシュモデルで使用されます。セッションの特定、セッションの終了、ホストの再認証、ポートのシャットダウン、およびポートバウンスでは、セッションごとの CoA 要求がサポートされます。このモデルは、次のように、1 つの要求 (CoA-Request) と 2 つの考えられる応答コードで構成されます。

- CoA acknowledgement (ACK) [CoA-ACK]
- CoA nonacknowledgement (NAK) [CoA-NAK]

要求は CoA クライアント（通常は AAA またはポリシーサーバー）から開始されて、リスナーとして動作するデバイスに転送されます。

次の表は、Identity-Based Networking Services でサポートされている RADIUS CoA コマンドとベンダー固有属性（VSA）を示します。すべての CoA コマンドには、デバイスと CoA クライアント間のセッション ID が含まれている必要があります。

表 20: Identity-Based Networking Services でサポートされている RADIUS CoA コマンド

CoA コマンド	シスコの VSA
Activate service	Cisco:Avpair="subscriber:command=activate-service" Cisco:Avpair="subscriber:service-name=<service-name>" Cisco:Avpair="subscriber:precedence=<precedence-number>" Cisco:Avpair="subscriber:activation-mode=replace-all"
Deactivate service	Cisco:Avpair="subscriber:command=deactivate-service" Cisco:Avpair="subscriber:service-name=<service-name>"
Bounce host port	Cisco:Avpair="subscriber:command=bounce-host-port"
Disable host port	Cisco:Avpair="subscriber:command=disable-host-port"
Session query	Cisco:Avpair="subscriber:command=session-query"
Session reauthenticate	Cisco:Avpair="subscriber:command=reauthenticate" Cisco:Avpair="subscriber:reauthenticate-type=last" または Cisco:Avpair="subscriber:reauthenticate-type=rerun"
Session terminate	これは、VSA を必要としない、標準の接続解除要求です。
Interface template	Cisco:AVpair="interface-template-name=<interfacetemplate>"

## Change-of-Authorization 要求

Change of Authorization (CoA) 要求は、RFC 5176 に記載されているように、プッシュモデルで使用するによって、セッション識別、ホスト再認証、およびセッション終了を行うことができます。このモデルは、1つの要求（CoA-Request）と2つの可能な応答コードで構成されています。

- CoA acknowledgment (ACK) [CoA-ACK]
- CoA non-acknowledgment (NAK) [CoA-NAK]



要求は CoA クライアント（通常は RADIUS またはポリシー サーバー）から発信されて、リスナーとして動作するスイッチに送信されます。

## RFC 5176 規定

Disconnect Request メッセージは Packet of Disconnect (POD) とも呼ばれますが、セッション終了に対してスイッチでサポートされています。

次の表に、この機能でサポートされている IETF 属性を示します。

表 21: サポートされている IETF 属性

属性番号	属性名
24	状態
31	Calling-Station-ID
44	Acct-Session-ID
80	Message-Authenticator
101	Error-Cause

次の表に、Error-Cause 属性で取ることができる値を示します。

表 22: Error-Cause の値

値	説明
<del>21</del>	削除された残留セッション コンテキスト
<del>22</del>	無効な EAP パケット（無視）
<del>41</del>	サポートされていない属性
<del>42</del>	見つからない属性
<del>43</del>	NAS 識別情報のミスマッチ
<del>44</del>	無効な要求
<del>45</del>	サポートされていないサービス
<del>46</del>	サポートされていない拡張機能
<del>47</del>	無効な属性値
<del>31</del>	管理上の禁止
<del>32</del>	ルート不可能な要求（プロキシ）

値	説明
3B	セッション コンテキストが検出されない
3C	セッション コンテキストが削除できない
3D	その他のプロキシ処理エラー
3E	リソースが使用不可能
3F	要求が発信された
38	マルチセッションの選択がサポートされていない

## CoA 要求応答コード

CoA 要求応答コードを使用すると、スイッチにコマンドを伝達できます。

RFC 5176 で定義されている CoA 要求応答コードの packets の形式は、コード、ID、長さ、オーセンティケータ、およびタイプ、長さ、値 (TLV) 形式の属性から構成されます。属性フィールドは、シスコのベンダー固有属性 (VSA) を送信するために使用します。

### セッションの識別

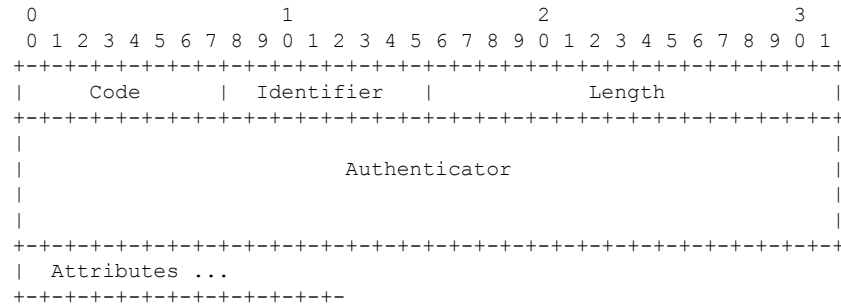
特定のセッションに向けられた切断と CoA 要求については、スイッチは 1 つ以上の次の属性に基づいて、セッションを検索します。

- Acct-Session-Id (IETF 属性 #44)
- Audit-Session-Id VSA (シスコの VSA)
- Calling-Station-Id (ホスト MAC アドレスを含む IETF 属性 #31)
- 次のいずれかの IPv6 属性。
  - Framed-IPv6-Prefix (IETF 属性 #97) および Framed-Interface-Id (IETF 属性 #96) 。ともに RFC 3162 に従った完全な IPv6 アドレスを作成する
  - Framed-IPv6-Address
- プレーン IP アドレス (IETF 属性 #8)

CoA メッセージに含まれるすべてのセッション ID 属性がそのセッションと一致しない限り、スイッチは「Invalid Attribute Value」エラーコード属性を含む Disconnect-NAK または CoA-NAK を返します。

複数のセッション ID 属性がメッセージに含まれる場合は、すべての属性がセッションと一致しなければなりません。そうでない場合は、スイッチが Disconnect - negative acknowledgement (NAK) または CoA -NAK と、「Invalid Attribute Value」エラーコードを返します。

RFC 5176 で定義されている CoA 要求コードの packets の形式は、コード、ID、長さ、オーセンティケータ、およびタイプ、長さ、値 (TLV) 形式の属性から構成されます。



属性フィールドは、シスコのベンダー固有属性（VSA）を送信するために使用します。

特定の適用ポリシーを対象とする CoA 要求の場合、上記のセッション ID 属性のいずれかがメッセージに含まれていると、デバイスはエラーコードが「Invalid Attribute Value」の CoA-NAK を返します。

### CoA ACK 応答コード

許可ステートの変更が成功した場合は、肯定確認応答（ACK）が送信されます。CoA ACK 内で返される属性は CoA 要求によって異なり、個々の CoA コマンドで検討されます。

### CoA NAK 応答コード

否定応答（NAK）は許可ステートの変更が失敗したことを示し、エラーの理由を示す属性を含めることができます。CoA が成功したかを確認するには、**show** コマンドを使用します。

## CoA 要求コマンド

表 23: でサポートされる CoA コマンド

コマンド	シスコの VSA
<a href="#">1</a>	
Reauthenticate host	Cisco:Avpair="subscriber:command=reauthenticate"
Terminate session	これは、VSA を要求しない、標準の接続解除要求です。
Bounce host port	Cisco:Avpair="subscriber:command=bounce-host-port"
Disable host port	Cisco:Avpair="subscriber:command=disable-host-port"

<sup>1</sup> すべての CoA コマンドには、と CoA クライアント間のセッション識別情報が含まれている必要があります。

### セッション再認証

不明な ID またはポスチャを持つホストがネットワークに加入して、制限されたアクセス許可プロファイル（たとえば、ゲスト VLAN）に関連付けられると、AAA サーバーは通常、セッ

セッション再認証要求を生成します。再認証要求は、クレデンシャルが不明である場合にホストが適切な認証グループに配置されることを許可します。

セッション認証を開始するために、AAA サーバーは `Cisco:Avpair="subscriber:command=reauthenticate"` の形式で 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。

現在のセッションステートは、メッセージに対するスイッチの応答を決定します。セッションが現在、IEEE 802.1x によって認証されている場合、スイッチは EAPOL (LAN 経由の拡張認証プロトコル) RequestId メッセージをサーバーに送信することで応答します。

現在、セッションが MAC 認証バイパス (MAB) で認証されている場合は、スイッチはサーバーにアクセス要求を送信し、初期正常認証で使用されるものと同じ ID 属性を渡します。

スイッチ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、スイッチ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。

セッションがまだ認証されていない、あるいはゲスト VLAN、クリティカル VLAN、または同様のポリシーで認証されている場合は、再認証メッセージがアクセス コントロール方式を再開し、最初に試行されるように設定された方式で開始します。セッションの現在の許可は、再認証によって異なる認証結果になるまで維持されます。

## スイッチ スタックでのセッションの再認証

スイッチ スタックでセッション再認証メッセージを受信すると、次の動作が発生します。

- 確認応答 (ACK) を戻す前に、再認証の必要性がチェックされます。
- 適切なセッションで再認証が開始されます。
- 認証が成功または失敗のいずれかで完了すると、再認証をトリガーする信号がスタックのメンバースイッチから削除されます。
- 認証の完了前にスタックのアクティブスイッチに障害が発生すると、(後で削除される) 元のコマンドに基づいたアクティブスイッチの切り替え後、再認証が開始されます。
- ACK の送信前にアクティブスイッチに障害が発生した場合、新たなアクティブスイッチでは、再送信コマンドが新しいコマンドとして扱われます。

## セッションの終了

セッションを終了させる 3 種類の CoA 要求があります。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。このコマンドを使用すると、指定され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、そのホストのネットワークへのアクセスは制限されません。

ホストのネットワークへのアクセスを制限するには、`Cisco:Avpair="subscriber:command=disable-host-port"` VSA の設定で CoA 要求を使用します。このコマンドは、ネットワーク上で障害を引き起こしたと認識されているホストがある場合に便利であり、そのホストに対してネットワークアクセスをただちにブロックする必要があります。

ポートへのネットワーク アクセスを復旧する場合は、非 RADIUS メカニズムを使用して再びイネーブルにします。

プリンタなどのサブリカントを持たないデバイスが新しい IP アドレスを取得する必要がある場合（たとえば、VLAN 変更後）は、ポート バウンスでホスト ポート上のセッションを終了します（ポートを一時的にディセーブルした後、再びイネーブルにする）。

## CoA 接続解除要求

このコマンドは標準の接続解除要求です。セッションが見つからない場合、スイッチは Disconnect-NAK メッセージと「Session Context Not Found」エラーコード属性を返します。セッションがある場合は、スイッチ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た後、スイッチは接続解除 ACK を返します。

スイッチがクライアントに接続解除 ACK を返す前にスタンバイ スイッチにフェールオーバーする場合は、クライアントから要求が再送信される際に、新しいアクティブスイッチ上でそのプロセスが繰り返されます。再送信後もセッションが見つからない場合は、Disconnect-ACK と「Session Context Not Found」エラーコード属性が送信されます。

## CoA 要求：ホスト ポートのディセーブル化

RADIUS サーバーの CoA disable port コマンドを実行すると、セッションをホストしている認証ポートが管理的にシャットダウンされます。その結果、セッションは終了します。このコマンドは、ホストがネットワーク上で問題を起こしていることを把握し、ホストのネットワーク アクセスを即座にブロックする必要がある場合に便利です。ポートのネットワークアクセスを復元するには、非 RADIUS メカニズムを使用して再びイネーブルにします。このコマンドは、次の新しいベンダー固有属性（VSA）が含まれている標準 CoA 要求メッセージで伝達されます。

```
Cisco:Avpair="subscriber:command=disable-host-port"
```

このコマンドはセッション指向であるため、「セッション ID」セクションに示されている 1 つ以上のセッション ID 属性とともに使用する必要があります。セッションが見つからない場合、スイッチは CoA-NAK メッセージと「Session Context Not Found」エラーコード属性を返します。このセッションがある場合は、スイッチはホストポートをディセーブルにし、CoA-ACK メッセージを返します。

スイッチが CoA-ACK をクライアントに返す前にスイッチに障害が発生した場合は、クライアントから要求が再送信される際に、新しいアクティブスイッチ上でそのプロセスが繰り返されます。スイッチが CoA-ACK メッセージをクライアントに返した後で、かつその動作が完了していないときにスイッチに障害が発生した場合は、新しいアクティブスイッチ上でその動作が再開されます。



- (注) 再送信コマンドの後に接続解除要求が失敗すると、（接続解除 ACK が送信されていない場合に）チェンジオーバー前にセッションが正常終了し、または元のコマンドが実行されてスタンバイスイッチがアクティブになるまでの間に発生した他の方法（たとえば、リンク障害）によりセッションが終了することがあります。

## CoA 要求 : バウンス ポート

RADIUS サーバーの CoA bounce port が RADIUS サーバーから送信されると、認証ポートでリンクのフラップが発生します。その結果、このポートに接続している1つまたは複数のホストから、DHCPの再ネゴシエーションが開始されます。この状況は、VLANの変更があり、この認証ポートに関する変化を検出するメカニズムがないデバイス（プリンタなど）がエンドポイントの場合に発生する可能性があります。CoA bounce port は、次の新しい VSA を含む標準の CoA-Request メッセージで伝達されます。

```
Cisco:Avpair="subscriber:command=bounce-host-port"
```

このコマンドはセッション指向であるため、1つ以上のセッション ID 属性とともに使用する必要があります。セッションが見つからない場合、スイッチは CoA-NAK メッセージと「Session Context Not Found」エラーコード属性を返します。このセッションがある場合は、スイッチはホストポートを10秒間ディセーブルし、再びイネーブルにし（ポートバウンス）、CoA-ACK を返します。

スイッチが CoA-ACK をクライアントに返す前にスイッチに障害が発生した場合は、クライアントから要求が再送信される際に、新しいアクティブスイッチ上でそのプロセスが繰り返されます。スイッチが CoA-ACK メッセージをクライアントに返した後で、かつその動作が完了していないときにスイッチに障害が発生した場合は、新しいアクティブスイッチ上でその動作が再開されます。

## セッション強制終了のスタック構成ガイドライン

スイッチ スタックでは、CoA 接続解除要求メッセージに必要な特別な処理はありません。

### CoA 要求バウンス ポートのスタック構成ガイドライン

**bounce-port** コマンドのターゲットはポートではなくセッションのため、セッションが見つからなかった場合、コマンドは実行できません。

アクティブスイッチで Auth Manager コマンドハンドラが有効な **bounce-port** コマンドを受信すると、CoA-ACK メッセージを返す前に次の情報が確認されます。

- ポートバウンスの必要性
- ポート ID（ローカルセッションコンテキストで検出された場合）

スイッチで、ポートバウンスが開始されます（ポートが10秒間ディセーブルになり、再びイネーブルにされます）。

ポートバウンスが正常に実行された場合、ポートバウンスをトリガーした信号がスタンバイスイッチから削除されます。

ポートバウンスの完了前にアクティブスイッチに障害が発生すると、（後で削除される）元のコマンドに基づいたアクティブスイッチの切り替え後、ポートバウンスが開始されます。

CoA-ACK メッセージの送信前にアクティブスイッチに障害が発生した場合、新たなアクティブスイッチでは、再送信コマンドが新しいコマンドとして扱われます。

## CoA 要求ディセーブル ポートのスタック構成ガイドライン

**disable-port** コマンドのターゲットはポートではなくセッションのため、セッションが見つからなかった場合、コマンドは実行できません。

アクティブスイッチで **Auth Manager** コマンドハンドラが有効な **disable-port** コマンドを受信すると、CoA-ACK メッセージを返す前に次の情報が確認されます。

- ポート ディセーブルの必要性
- ポート ID (ローカルセッション コンテキストで検出された場合)

スイッチで、ポートをディセーブルする操作が試行されます。

ポートを無効にする操作が正常に実行された場合、ポートを無効にする操作をトリガーした信号がスタンバイスイッチから削除されます。

ポートを無効にする操作の完了前にアクティブスイッチに障害が発生すると、(後で削除される) 元のコマンドに基づいたアクティブスイッチの切り替え後、ポートが無効にされます。

CoA-ACK メッセージの送信前にアクティブスイッチに障害が発生した場合、新たなアクティブスイッチでは、再送信コマンドが新しいコマンドとして扱われます。

## RADIUS のデフォルト設定

RADIUS および AAA は、デフォルトではディセーブルに設定されています。

セキュリティの失効を防止するため、ネットワーク管理アプリケーションを使用して RADIUS を設定することはできません。RADIUS をイネーブルに設定した場合、CLI を通じてスイッチにアクセスするユーザを認証できます。

## RADIUS サーバ ホスト

スイッチと RADIUS サーバの通信には、次の要素が関係します。

- ホスト名または IP アドレス
- 認証の宛先ポート
- アカウンティングの宛先ポート
- キー文字列
- タイムアウト時間
- 再送信回数

RADIUS セキュリティサーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号によって特定します。IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、特定の AAA サービスを提供する RADIUS ホストとして個々のポートを定義できます。この一意の ID を使用することによって、同じ IP アドレスにあるサーバ上の複数の UDP ポートに、RADIUS 要求を送信できます。

同じ RADIUS サーバー上の異なる 2 つのホスト エントリに同じサービス（たとえばアカウントティング）を設定した場合、2 番めに設定したホスト エントリは、最初に設定したホスト エントリのフェールオーバー バックアップとして動作します。この例では、最初のホスト エントリがアカウントティング サービスを提供できなかった場合、スイッチは

「%RADIUS-4-RADIUS\_DEAD」メッセージを表示し、その後、同じデバイス上で 2 番めに設定されたホスト エントリでアカウントティング サービスを試みます（RADIUS ホスト エントリは、設定した順序に従って試行されます）。

RADIUS サーバとスイッチは、共有秘密テキスト文字列を使用して、パスワードの暗号化および応答の交換を行います。RADIUS で AAA セキュリティ コマンドを使用するように設定するには、RADIUS サーバデーモンが稼働するホストと、そのホストがスイッチと共有する秘密テキスト（キー）文字列を指定する必要があります。

タイムアウト、再送信回数、および暗号キーの値は、すべての RADIUS サーバに対してグローバルに設定することもできますし、サーバ単位で設定することもできます。また、グローバルな設定とサーバ単位での設定を組み合わせることもできます。

## RADIUS ログイン認証

AAA 認証を設定するには、認証方式の名前付きリストを作成してから、各種ポートにそのリストを適用します。方式リストは実行される認証のタイプと実行順序を定義します。このリストを特定のポートに適用してから、定義済み認証方式を実行する必要があります。唯一の例外は、デフォルトの方式リストです。デフォルトの方式リストは、名前付き方式リストを明示的に定義されたインターフェイスを除いて、自動的にすべてのポートに適用されます。

方式リストは、ユーザ認証のためクエリ送信を行う手順と認証方式を記述したものです。認証に使用する 1 つまたは複数のセキュリティプロトコルを指定できるので、最初の方式が失敗した場合のバックアップシステムが確保されます。ソフトウェアは、リスト内の最初の方式を使用してユーザを認証します。その方式で応答が得られなかった場合、ソフトウェアはそのリストから次の認証方式を選択します。このプロセスは、リスト内の認証方式による通信が成功するか、定義された方式をすべて試し終わるまで繰り返されます。この処理のある時点で認証が失敗した場合（つまり、セキュリティサーバまたはローカルのユーザ名データベースがユーザアクセスを拒否すると応答した場合）、認証プロセスは停止し、それ以上認証方式が試行されることはありません。

## AAA サーバグループ

既存のサーバー ホストを認証用にグループ化するため、AAA サーバグループを使用するようにスイッチを設定できます。設定済みのサーバホストのサブセットを選択して、それを特定のサービスに使用します。サーバグループは、選択されたサーバホストの IP アドレスのリストを含むグローバルなサーバホストリストとともに使用されます。

サーバグループには、同じサーバの複数のホスト エントリを含めることもできますが、各エントリが一意の ID（IP アドレスと UDP ポート番号の組み合わせ）を持っていることが条件です。この場合、個々のポートをそれぞれ特定の AAA サービスを提供する RADIUS ホストとして定義できます。この一意の ID を使用することによって、同じ IP アドレスにあるサーバ上の異なる UDP ポートに、RADIUS 要求を送信できます。同じ RADIUS サーバ上の異なる 2 つの



ホストエントリに同じサービス（たとえばアカウントティング）を設定した場合、2番めに設定したホストエントリは、最初に設定したホストエントリのフェールオーバーバックアップとして動作します。最初のホストエントリがアカウントティングサービスの提供に失敗すると、ネットワークアクセスサーバは同じデバイスに設定されている2番めのホストエントリを使用してアカウントティングサービスを提供するように試行します。（試行されるRADIUSホストエントリの順番は、設定されている順序に従います）。

## AAA 許可

AAA 許可によってユーザが利用できるサービスが制限されます。AAA 許可をイネーブルにすると、スイッチは（ローカルユーザデータベースまたはセキュリティサーバ上に存在する）ユーザのプロファイルから取得した情報を使用して、ユーザのセッションを設定します。ユーザは、ユーザプロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

## RADIUS アカウントティング

AAA アカウントティング機能は、ユーザが使用したサービスと、消費したネットワークリソース量を追跡します。AAA アカウントティングをイネーブルにすると、スイッチはユーザの活動状況をアカウントティングレコードの形式でRADIUSセキュリティサーバに報告します。各アカウントティングレコードにはアカウントティングのAttribute-Value (AV) ペアが含まれ、レコードはセキュリティサーバに格納されます。これらのデータは、ネットワーク管理、クライアントへの課金、または監査のために後で分析できます。

## ベンダー固有の RADIUS 属性

Internet Engineering Task Force (IETF) ドラフト規格に、ベンダー固有の属性（属性 26）を使用して、スイッチとRADIUSサーバ間でベンダー固有の情報を通信するための方式が定められています。各ベンダーは、Vendor-Specific Attribute (VSA) を使用することによって、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。シスコが実装するRADIUSでは、この仕様で推奨されるフォーマットを使用して、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 であり、サポート対象のオプションはベンダータイプ 1（名前は *cisco-avpair*）です。この値は、次のフォーマットのストリングです。

```
protocol : attribute sep value *
```

*protocol* は、特定の認証タイプに使用するシスコのプロトコル属性の値です。*attribute* および *value* は、シスコの TACACS+ 仕様で定義されている適切な属性値 (AV) ペアです。*sep* は、必須の属性の場合は =、任意指定の属性の場合は \* です。TACACS+ 認証で使用できるすべての機能は、RADIUS でも使用できます。

たとえば、次の AV ペアにより、IP 認証中（PPP の IPCP アドレス割り当て中）には、シスコの「multiple named IP address pools」機能がアクティブになります。

```
cisco-avpair= "ip:addr-pool=first"
```

「\*」を挿入すると、AV ペア「ip:addr-pool=first」は省略可能になります。任意の AV ペアを省略可能にすることができます。

```
cisco-avpair= "ip:addr-pool*first"
```

次に、ネットワーク アクセス サーバからユーザがログインしたときに、すぐに EXEC コマンドを実行する方法の例を示します。

```
cisco-avpair= "shell:priv-lvl=15"
```

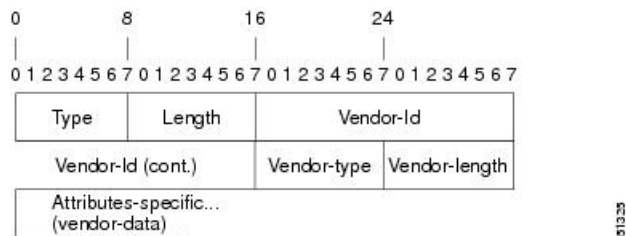
他のベンダーにも、それぞれ独自のベンダー ID、オプション、および対応する VSA があります。ベンダー ID および VSA の詳細については、RFC 2138 『Remote Authentication Dial-In User Service (RADIUS)』を参照してください。

属性 26 には、次の 3 つの要素が含まれています。

- タイプ
- 長さ
- スtring (またはデータ)
  - Vendor-Id
  - Vendor-Type
  - Vendor-Length
  - Vendor-Data

次の図は、属性 26 の「背後で」カプセル化される VSA のパケット形式を示します。

図 11: 属性 26 の背後でカプセル化される VSA



(注) VSA の形式はベンダーが指定します。Attribute-Specific フィールド (Vendor-Data と呼ばれる) は、ベンダーによるその属性の定義によって異なります。

次の表に、「ベンダー固有 RADIUS IETF 属性テーブル」(次の 2 番目の表) で表示される重要なフィールドを示します。これは、サポート対象のベンダー固有 RADIUS 属性 (IETF 属性 26) を表示します。

表 24:ベンダー固有属性表のフィールドの説明

フィールド	説明
番号	次の表に示されるすべての属性は、IETF 属性 26 の拡張です。
ベンダー固有のコマンドコード	特定のベンダーの識別に使用する定義されたコード。コード 9 は Cisco VSA、311 は Microsoft VSA、529 は Ascend VSA を定義します。
サブタイプ番号	属性 ID 番号。この番号は、属性 26 の背後でカプセル化される「2 番目のレイヤ」の ID 番号であること以外、IETF 属性の ID 番号に似ています。
属性	属性の ASCII スtring 名。
説明	属性の説明。

表 25:ベンダー固有 RADIUS IETF 属性

番号	ベンダー固有の 企業コード	サブタイプ番号	属性	説明
MS-CHAP 属性				
26	311	1	MSCHAP-Response	PPP MS-CHAP ユーザが チャレンジに対する応 答で提供するレスポ ンス値が含まれます。 Access-Request パケッ トでしか使用されませ ん。この属性は、PPP CHAP ID と同じです (RFC 2548)
26	311	11	MSCHAP-Challenge	ネットワーク アクセス サーバが MS-CHAP ユーザに送信するチャ レンジが含まれます。 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。(RFC 2548)
VPDN 属性				

番号	ベンダー固有の 企業コード	サブタイプ番号	属性	説明
26	9	1	l2tp-cm-local-window-size	L2TP 制御メッセージの最大受信ウィンドウサイズを指定します。この値は、トンネルの確立中にピアにアドバタイズされます。
26	9	1	l2tp-drop-out-of-order	正しくない順序で受信したデータパケットをドロップして、シーケンス番号を順守します。これは受信した場合の処理方法であって、データパケット上でシーケンス番号が送信されるわけではありません。
26	9	1	l2tp-hello-interval	hello キープアライブインターバルの秒数を指定します。ここで指定した秒数、トンネルでデータが送信されないと、hello パケットが送信されます。
26	9	1	l2tp-hidden-avp	イネーブルにすると、L2TP 制御メッセージで、大文字小文字を区別する AVP にスクランブルがかけられるか、または非表示になります。
26	9	1	l2tp-nosession-timeout	タイムアウトおよびシャットダウンまでに、セッションなしでトンネルがアクティブのままになる秒数を指定します。

番号	ベンダー固有の 企業コード	サブタイプ番号	属性	説明
26	9	1	tunnel-tos-reflect	LNS でトンネルに入る パケットに対して、IP ToS フィールドを各ペ イロードパケットの IP ヘッダーからトンネル パケットの IP ヘッダー にコピーします。
26	9	1	l2tp-tunnel-authen	この属性を設定する と、L2TP トンネル認証 が実行されます。
26	9	1	l2tp-tunnel-password	L2TP トンネル認証およ び AVP 隠蔽に使用され る共有秘密。
26	9	1	l2tp-udp-checksum	これは認可属性で、 L2TP がデータパケッ トに対して UDP チェッ クサムを実行する必要 があるかどうかを定義 します。有効な値は 「yes」と「no」です。 デフォルトは「no」で す。
Store and Forward Fax 属性				
26	9	3	Fax-Account-Id-Origin	<b>mmoip aaa receive-id</b> コ マンドまたは <b>mmoip aaa send-id</b> コマンドに ついて、システム管理 者によって定義された ものとしてアカウント ID の発信元を示しま す。
26	9	4	Fax-Msg-Id=	Store and Forward Fax 機 能によって割り当てら れた一意のファクス メッセージ識別番号を 示します。

番号	ベンダー固有の 企業コード	サブタイプ番号	属性	説明
26	9	5	Fax-Pages	このファクスセッション中に送信または受信したページ数を示します。このページ数には、カバーページも含まれます。
26	9	6	Fax-Coverpage-Flag	カバー ページがこのファクスセッションのオフランプゲートウェイで生成されたかどうかを示します。true はカバー ページが生成されたことを示します。false はカバー ページが生成されなかったことを意味します。
26	9	7	Fax-Modem-Time	モデムがファクス データを送信した時間 (x)、およびファクスセッションの合計時間 (y) を秒単位で示します。これには、fax-mail および PSTN 時間が x/y の形式で含まれます。たとえば、10/15 は送信時間が 10 秒で、合計ファクスセッションが 15 秒であったことを示します。
26	9	8	Fax-Connect-Speed	この fax-mail が最初に送信または受信された時点のモデム速度を示します。有効値は、1200、4800、9600、および 14400 です。

番号	ベンダー固有の 企業コード	サブタイプ番号	属性	説明
26	9	9	Fax-Recipient-Count	このファクス送信の受信者数を示します。Eメールサーバがセッションモードをサポートするまで、この数字は1にする必要があります。
26	9	10	Fax-Process-Abort-Flag	ファクスセッションが中断したこと、または正常に終了したことを示します。true はセッションが中断したことを示します。false はセッションが成功したことを示します。
26	9	11	Fax-Dsn-Address	DSN の送信先のアドレスを示します。
26	9	12	Fax-Dsn-Flag	DSN がイネーブルにされているかどうかを示します。true は DSN がイネーブルにされていることを示します。false は DSN がイネーブルにされていないことを示します。
26	9	13	Fax-Mdn-Address	MDN の送信先のアドレスを示します。
26	9	14	Fax-Mdn-Flag	メッセージ配信通知 (MDN) がイネーブルにされているかどうかを示します。true は MDN がイネーブルにされていることを示します。false は MDN がイネーブルにされていないことを示します。

番号	ベンダー固有の 企業コード	サブタイプ番号	属性	説明
26	9	15	Fax-Auth-Status	このファクスセッションに対する認証が成功したかどうかを示します。このフィールドに対する有効値は、 <b>success</b> 、 <b>failed</b> 、 <b>bypassed</b> 、または <b>unknown</b> です。
26	9	16	Email-Server-Address	オンランプ fax-mail メッセージを処理する E メールサーバの IP アドレスを示します。
26	9	17	Email-Server-Ack-Flag	オンランプゲートウェイが fax-mail メッセージを受け入れる E メールサーバから肯定確認応答を受信したことを示します。
26	9	18	Gateway-Id	ファクスセッションを処理したゲートウェイの名前を示します。名前は、 <b>hostname.domain-name</b> という形式で表示されます。
26	9	19	Call-Type	ファクスのアクティビティのタイプを、 <b>fax receive</b> または <b>fax send</b> のどちらかで記述します。
26	9	20	Port-Used	この fax-mail の送受信いずれかに使用される Cisco AS5300 のスロット/ポート番号を示します。



番号	ベンダー固有の 企業コード	サブタイプ番号	属性	説明
26	9	21	Abort-Cause	ファクスセッションが 中断した場合、中断操 作の信号を送信したシ ステムコンポーネント を示します。中断する 可能性のあるシステム コンポーネントには、 FAP (Fax Application Process)、TIFF (TIFF リーダーまたは TIFF ラ イター)、fax-mail クラ イアント、fax-mail サー バー、ESMTP クライア ント、ESMTP サーバー などがあります。
H323 属性				
26	9	23	Remote-Gateway-ID (h323-remote-address)	リモート ゲートウェイ の IP アドレスを示しま す。
26	9	24	Connection-ID (h323-conf-id)	会議 ID を識別します。
26	9	25	Setup-Time (h323-setup-time)	以前、グリニッジ標準 時 (GMT) およびズー ル タイムと呼ばれてい た協定世界時 (UTC) でのこの接続のセット アップ時間を示しま す。
26	9	26	Call-Origin (h323-call-origin)	ゲートウェイに対する コールの発行元を示し ます。有効値は、 originating および terminating です (回 答)。
26	9	27	Call-Type (h323-call-type)	コールのレグタイプを 示します。使用可能な 値は <b>telephony</b> と <b>VoIP</b> です。

番号	ベンダー固有の 企業コード	サブタイプ番号	属性	説明
26	9	28	Connect-Time (h323-connect-time)	このコール レッグの UTC での接続時間を示 します。
26	9	29	Disconnect-Time (h323-disconnect-time)	このコール レッグが UTC で接続解除された 時間を示します。
26	9	30	Disconnect-Cause (h323-disconnect-cause)	Q.931 仕様によって、 接続がオフラインにさ れた理由を示します。
26	9	31	Voice-Quality (h323-voice-quality)	コールの音声品質に影 響する Impairment Factor (ICPIF) を指定しま す。
26	9	33	Gateway-ID (h323-gw-id)	下位のゲートウェイの 名前を示します。
大規模のダイヤルアウト属性				
26	9	1	callback-dialstring	コールバックに使用す るダイヤリング文字列 を定義します。
26	9	1	data-service	説明はありません。
26	9	1	dial-number	ダイヤルする番号を定 義します。
26	9	1	force-56	チャンネルの 64 K すべ てが使用可能に見える場 合でも、ネットワーク アクセスサーバが 56 K の部分のみを使用する かどうかを指定しま す。

番号	ベンダー固有の 企業コード	サブタイプ番号	属性	説明
26	9	1	map-class	ユーザ プロファイルに、ダイヤルアウトするネットワーク アクセス サーバ上で同じ名前のマップクラスで設定される情報の参照を許可します。
26	9	1	send-auth	CLID 認証に続く、username-password 認証で使用するプロトコル (PAP または CHAP) を定義します。

番号	ベンダー固有の 企業コード	サブタイプ番号	属性	説明
26	9	1	send-name	

番号	ベンダー固有の 企業コード	サブタイプ番号	属性	説明
				<p>PPP 名前認証。PAP に適用する場合、インターフェイスで <b>ppp pap sent-name password</b> コマンドは設定しないでください。PAP の場合、アウトバウンド認証の PAP ユーザ名および PAP パスワードとして、</p> <p>「preauth:send-name」および 「preauth:send-secret」が使用されます。CHAP の場合、</p> <p>「preauth:send-name」は、アウトバウンド認証だけでなく、インバウンド認証にも使用されます。CHAP インバウンドの場合、NAS は発信元のボックスへのチャレンジパケットに、</p> <p>「preauth:send-name」で定義された名前を使用します。</p> <p>(注) send-name 属性は時間の経過とともに変わっています。最初は、現在 send-name および remote-name 属性の両方で提供されている機能を実行していました。</p>

番号	ベンダー固有の 企業コード	サブタイプ番号	属性	説明
				remote-name 属性が追加 されたた め、 send-name 属性は現在 の動作に制 限されてい ます。
26	9	1	send-secret	PPP パスワード認証。 ベンダー固有属性 (VSA) の場合、アウ トバウンド認証の PAP ユーザ名および PAP パ スワードとして、 「preauth:send-name」お よび 「preauth:send-secret」 が使用されます。CHAP アウトバウンドの場 合、 「preauth:send-name」と 「preauth:send-secret」 の両方が応答パケット で使用されます。
26	9	1	remote-name	大規模のダイヤルアウ トで使用するリモート ホストの名前を提供し ます。ダイヤラは、大 規模のダイヤルアウト のリモート名が認証さ れた名前と一致するこ を確認し、偶発的な ユーザ RADIUS 設定ミ スから保護します (有 効な電話番号にダイヤ ルしたが誤ったデバイ スに接続されるなどの ミスです)。
その他の属性				

番号	ベンダー固有の 企業コード	サブタイプ番号	属性	説明
26	9	2	Cisco-NAS-Port	<p>NAS-Port アカウンティングに追加的なベンダー固有属性 (VSA) を指定します。追加的な NAS-Port 情報を属性値ペア (AVPair) の形式で指定するには、<b>radius-server vsa send</b> 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。</p> <p>(注) この VSA は、通常アカウンティングで使用されますが認証 (Access-Request) パケットで使用される場合もあります。</p>
26	9	1	min-links	MLP に対するリンクの最小数を設定します。
26	9	1	proxyacl#<n>	ダウンロード可能なユーザ プロファイル (ダイナミック ACL) を、認証プロキシを使用して設定でき、これにより設定されたインターフェイスのトラフィックの通過を許可するよう、認証を設定できます。

番号	ベンダー固有の 企業コード	サブタイプ番号	属性	説明
26	9	1	spi	登録中にホーム エージェントがモバイルノードの認証で必要とする認証情報を伝送します。この情報は、 <b>ip mobile secure host &lt;addr&gt;</b> コンフィギュレーションコマンドと同じ構文です。基本的に、この文字列に続く残りのコンフィギュレーションコマンドはそのまま含まれます。これにはセキュリティパラメータ インデックス (SPI)、キー、認証アルゴリズム、認証モード、およびリプレイ保護タイムスタンプ範囲が含まれています。

## ベンダー独自仕様の RADIUS サーバ通信

RADIUS に関する IETF ドラフト規格では、スイッチと RADIUS サーバ間でベンダー独自仕様の情報を通信する方式について定められていますが、RADIUS 属性セットを独自に機能拡張しているベンダーもあります。Cisco IOS ソフトウェアは、ベンダー独自仕様の RADIUS 属性のサブセットをサポートしています。

前述したように、RADIUS (ベンダーの独自仕様によるものか、IETF ドラフトに準拠するものかを問わず) を設定するには、RADIUS サーバデーモンが稼働しているホストと、そのホストがスイッチと共有秘密テキスト文字列を指定する必要があります。RADIUS ホストおよび秘密テキスト文字列を指定するには、**radius server** 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。



# RADIUS の設定方法

## RADIUS サーバホストの識別

デバイスと通信するすべての RADIUS サーバーにこのような設定をグローバルに適用するには、**radius-server timeout**、**radius-server retransmit**、および **key string** という 3 つの固有なグローバル コンフィギュレーション コマンドを使用します。

認証時に AAA サーバーグループを使用して既存のサーバーホストをグループ化するようにデバイスを設定できます。詳細については、次の関連項目を参照してください。

RADIUS サーバ上でも、いくつかの値を設定する必要があります。これらの設定値としては、デバイスの IP アドレス、およびサーバーとデバイスの双方で共有するキー ストリングがあります。詳細については、RADIUS サーバのマニュアルを参照してください。

サーバ単位で RADIUS サーバとの通信を設定するには、次の手順を実行します。

### 始める前に

device にグローバルな機能とサーバー単位での機能（タイムアウト、再送信回数、およびキー コマンド）を設定した場合、サーバー単位で設定したタイムアウト、再送信回数、およびキーに関するコマンドは、グローバルに設定したタイムアウト、再送信回数、およびキーに関するコマンドを上書きします。すべての RADIUS サーバーに対してこれらの値を設定する方法については、次の関連項目を参照してください。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **radius server server name**
4. **address {ipv4 | ipv6} ip address { auth-port port number | acct-port port number }**
5. **key string**
6. **retransmit value**
7. **timeout seconds**
8. **exit**
9. **end**
10. **show running-config**
11. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 :	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>• パスワードを入力します（要求された場合）。</li> </ul>

	コマンドまたはアクション	目的
	デバイス> <code>enable</code>	
ステップ 2	<b>configure terminal</b> 例： デバイス# <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 3	<b>radius server server name</b> 例： デバイス (config)# <code>radius server rsim</code>	
ステップ 4	<b>address {ipv4   ipv6} ip address { auth-port port number   acct-port port number}</b> 例： デバイス (config-radius-server)# <code>address ipv4 124.2.2.12 auth-port 1612</code>	(任意) RADIUS サーバーのパラメータを指定します。  <b>auth-port port-number</b> には、認証要求の UDP 宛先ポートを指定します。デフォルトは 1645 です。指定できる範囲は 0 ~ 65536 です。  <b>acct-port port-number</b> には、認証要求の UDP 宛先ポートを指定します。デフォルトは 1646 です。
ステップ 5	<b>key string</b> 例： デバイス (config-radius-server)# <code>key rad123</code>	(任意) <b>key string</b> には、デバイスと RADIUS サーバーで動作する RADIUS デーモンの中で使用される認証と暗号キーを指定します。  (注) キーは、RADIUS サーバーで使用する暗号化キーに一致するテキストストリングでなければなりません。必ず <b>radius server</b> コマンドの最終項目としてキーを設定してください。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部である場合を除き、引用符でキーを囲まないでください。
ステップ 6	<b>retransmit value</b> 例： デバイス (config-radius-server)# <code>retransmit 10</code>	(任意) サーバが応答しない、または応答が遅い場合に、RADIUS 要求をリセットする回数を指定します。指定できる範囲は 1 ~ 100 です。この設定は、 <b>radius-server retransmit</b> グローバル コンフィギュレーション コマンドによる設定を上書きします。

	コマンドまたはアクション	目的
ステップ 7	<b>timeout seconds</b> 例： デバイス(config-radius-server)# <b>timeout 60</b>	(任意) デバイスが要求を再送信する前に RADIUS サーバーからの応答を待機する時間間隔を指定します。指定できる範囲は 1～1000 です。この設定は、 <b>radius-server timeout</b> グローバル コンフィギュレーション コマンドによる設定を上書きします。
ステップ 8	<b>exit</b> 例： デバイス(config-server-tacacs)# <b>exit</b>	RADIUS サーバーモードを終了して、グローバル コンフィギュレーション モードを開始します。
ステップ 9	<b>end</b> 例： デバイス(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 10	<b>show running-config</b> 例： デバイス# <b>show running-config</b>	入力を確認します。
ステップ 11	<b>copy running-config startup-config</b> 例： デバイス# <b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。

## RADIUS ログイン認証の設定

RADIUS ログイン認証を設定するには、次の手順を実行します。

### 始める前に

AAA 方式を使用して HTTP アクセスに対し device のセキュリティを確保するには、**ip http authentication aaa** グローバル コンフィギュレーション コマンドで device を設定する必要があります。AAA 認証を設定しても、AAA 方式を使用した HTTP アクセスに対し device のセキュリティは確保しません。

### 手順の概要

1. **enable**
2. **configure terminal**

3. **aaa new-model**
4. **aaa authentication login {default | list-name} method1 [method2... ]**
5. **line [console | tty | vty] line-number [ending-line-number]**
6. **login authentication {default | list-name}**
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 :  デバイス> <b>enable</b>	特権 EXEC モードを有効にします。  <ul style="list-style-type: none"> <li>• パスワードを入力します（要求された場合）。</li> </ul>
ステップ 2	<b>configure terminal</b> 例 :  デバイス# <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 3	<b>aaa new-model</b> 例 :  デバイス (config)# <b>aaa new-model</b>	AAA をイネーブルにします。
ステップ 4	<b>aaa authentication login {default   list-name} method1 [method2... ]</b> 例 :  デバイス (config)# <b>aaa authentication login default local</b>	ログイン認証方式リストを作成します。  <ul style="list-style-type: none"> <li>• <b>login authentication</b> コマンドにリストが指定されていない場合に使用するデフォルトのリストを作成するには、<b>default</b> キーワードの後ろにデフォルト状況で使用される方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。</li> <li>• <b>list-name</b> には、作成するリストの名前として使用する文字列を指定します。</li> <li>• <b>method1...</b> には、認証アルゴリズムが試行する実際の方式を指定します。追加の認証方式は、その前の方式でエラーが返された場合に限り使用されます。前の方式が失敗した場合は使用されません。               次のいずれかの方式を選択します。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <b>enable</b> : イネーブルパスワードを認証に使用します。この認証方式を使用するには、あらかじめ <b>enable password</b> グローバル コンフィギュレーションコマンドを使用してイネーブルパスワードを定義しておく必要があります。</li> <li>• <b>group radius</b> : RADIUS 認証を使用します。この認証方式を使用するには、あらかじめ RADIUS サーバーを設定しておく必要があります。</li> <li>• <b>line</b> : 回線パスワードを認証に使用します。この認証方式を使用するには、あらかじめ回線パスワードを定義しておく必要があります。 <b>password password</b> ライン コンフィギュレーション コマンドを使用します。</li> <li>• <b>local</b> : ローカルユーザー名データベースを認証に使用します。データベースにユーザー名情報を入力しておく必要があります。 <b>username name password</b> 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。</li> <li>• <b>local-case</b> : 大文字と小文字が区別されるローカルユーザー名データベースを認証に使用します。 <b>username password</b> グローバル コンフィギュレーション コマンドを使用して、ユーザー名情報をデータベースに入力する必要があります。</li> <li>• <b>none</b> : ログインに認証を使用しません。</li> </ul>
ステップ 5	<b>line [console   tty   vty] line-number [ending-line-number]</b> 例 :  デバイス(config)# <b>line 1 4</b>	ライン コンフィギュレーション モードを開始し、認証リストを適用する回線を設定します。
ステップ 6	<b>login authentication {default   list-name}</b> 例 :  デバイス(config)# <b>login authentication default</b>	1つの回線または複数回線に認証リストを適用します。 <ul style="list-style-type: none"> <li>• <b>default</b> を指定する場合は、 <b>aaa authentication login</b> コマンドで作成したデフォルトのリストを使用します。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <i>list-name</i> には、<b>aaa authentication login</b> コマンドで作成したリストを指定します。</li> </ul>
ステップ 7	<b>end</b> 例： デバイス (config) # <b>end</b>	特権 EXEC モードに戻ります。
ステップ 8	<b>show running-config</b> 例： デバイス # <b>show running-config</b>	入力を確認します。
ステップ 9	<b>copy running-config startup-config</b> 例： デバイス # <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## AAA サーバグループの定義

定義したグループサーバに特定のサーバを対応付けるには、**server** グループサーバコンフィギュレーションコマンドを使用します。サーバを IP アドレスで特定することもできますし、任意指定の **auth-port** および **acct-port** キーワードを使用して複数のホストインスタンスまたはエントリを特定することもできます。

AAA サーバグループを定義するには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **radius server name**
4. **address {ipv4 | ipv6} {ip-address | hostname} auth-port port-number acct-port port-number**
5. **key string**
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  デバイス> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  デバイス# <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 3	<b>radius server name</b> 例：  デバイス(config)# <b>radius server ISE</b>	RADIUS サーバの設定の名前を Protected Access Credential (PAC) のプロビジョニング用に指定し、RADIUS サーバ設定モードを開始します。  deviceは、IPv6 用の RADIUS もサポートしています。
ステップ 4	<b>address {ipv4   ipv6} {ip-address   hostname} auth-port port-number acct-port port-number</b> 例：  デバイス(config-radius-server)# <b>address ipv4 10.1.1.1 auth-port 1645 acct-port 1646</b>	RADIUS サーバのアカウントingおよび認証パラメータの IPv4 アドレスを設定します。
ステップ 5	<b>key string</b> 例：  デバイス(config-radius-server)# <b>key cisco123</b>	デバイスと RADIUS サーバとの間におけるすべての RADIUS 通信用の認証および暗号キーを指定します。
ステップ 6	<b>end</b> 例：  デバイス(config-radius-server)# <b>end</b>	RADIUS サーバ 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 7	<b>show running-config</b> 例：  デバイス# <b>show running-config</b>	入力を確認します。

	コマンドまたはアクション	目的
ステップ 8	<b>copy running-config startup-config</b> 例 :  デバイス# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## ユーザイネーブルアクセスおよびネットワーク サービスに関する RADIUS 許可の設定



(注) 許可が設定されていても、CLI を使用してログインし、認証されたユーザに対しては、許可は省略されます。

ユーザ特権アクセスおよびネットワーク サービスに関する RADIUS 許可を設定するには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **aaa authorization network radius**
4. **aaa authorization exec radius**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 :  デバイス> <b>enable</b>	特権 EXEC モードを有効にします。  <ul style="list-style-type: none"> <li>• パスワードを入力します (要求された場合)。</li> </ul>
ステップ 2	<b>configure terminal</b> 例 :  デバイス# <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。



	コマンドまたはアクション	目的
ステップ 3	<b>aaa authorization network radius</b> 例 : デバイス (config) # <b>aaa authorization network radius</b>	ネットワーク関連のすべてのサービス要求に対して、ユーザが RADIUS 許可を受けるように device を設定します。
ステップ 4	<b>aaa authorization exec radius</b> 例 : デバイス (config) # <b>aaa authorization exec radius</b>	ユーザに特権 EXEC のアクセス権限がある場合、ユーザが RADIUS 許可を受けるように device を設定します。 <b>exec</b> キーワードを指定すると、ユーザープロファイル情報 ( <b>autocommand</b> 情報など) が返される場合があります。
ステップ 5	<b>end</b> 例 : デバイス (config) # <b>end</b>	特権 EXEC モードに戻ります。
ステップ 6	<b>show running-config</b> 例 : デバイス # <b>show running-config</b>	入力を確認します。
ステップ 7	<b>copy running-config startup-config</b> 例 : デバイス # <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

### 次のタスク

**aaa authorization** グローバル コンフィギュレーション コマンドと **radius** キーワードを使用すると、ユーザのネットワーク アクセスを特権 EXEC モードに制限するパラメータを設定できます。

**aaa authorization exec radius local** コマンドは、次の許可パラメータを設定します。

- RADIUS を使用して認証を行った場合は、RADIUS を使用して特権 EXEC アクセスを許可します。
- 認証に RADIUS を使用しなかった場合は、ローカル データベースを使用します。

## RADIUS アカウンティングの起動

RADIUS アカウンティングを開始するには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **aaa accounting network start-stop radius**
4. **aaa accounting exec start-stop radius**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  デバイス> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  デバイス# <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 3	<b>aaa accounting network start-stop radius</b> 例：  デバイス(config)# <b>aaa accounting network start-stop radius</b>	ネットワーク関連のあらゆるサービス要求に関して、RADIUS アカウンティングをイネーブルにします。
ステップ 4	<b>aaa accounting exec start-stop radius</b> 例：  デバイス(config)# <b>aaa accounting exec start-stop radius</b>	RADIUS アカウンティングをイネーブルにして、特権 EXEC プロセスの最初に記録開始アカウンティング通知、最後に記録停止通知を送信します。
ステップ 5	<b>end</b> 例：  デバイス(config)# <b>end</b>	特権 EXEC 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 6	<b>show running-config</b> 例：  デバイス# <code>show running-config</code>	入力を確認します。
ステップ 7	<b>copy running-config startup-config</b> 例：  デバイス# <code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

## すべての RADIUS サーバの設定

すべての RADIUS サーバを設定するには、特権 EXEC モードで次の手順を実行します。

### 手順の概要

1. **configure terminal**
2. **radius-server key *string***
3. **radius-server retransmit *retries***
4. **radius-server timeout *seconds***
5. **radius-server deadtime *minutes***
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例：  デバイス# <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>radius-server key <i>string</i></b> 例：	スイッチとすべての RADIUS サーバ間で共有されるシークレット テキスト スtring を指定します。

	コマンドまたはアクション	目的
	デバイス (config) # <b>radius-server key your_server_key</b>  デバイス (config) # <b>key your_server_key</b>	(注) キーは、RADIUS サーバで使用する暗号化キーに一致するテキスト ストリングでなければなりません。先頭のスペースは無視されますが、キーの中間および末尾のスペースは使用されます。キーにスペースを使用する場合は、引用符がキーの一部である場合を除き、引用符でキーを囲まないでください。
ステップ 3	<b>radius-server retransmit retries</b>  例 :  デバイス (config) # <b>radius-server retransmit 5</b>	スイッチが RADIUS 要求をサーバに再送信する回数を指定します。デフォルトは 3 です。指定できる範囲は 1 ~ 1000 です。
ステップ 4	<b>radius-server timeout seconds</b>  例 :  デバイス (config) # <b>radius-server timeout 3</b>	スイッチが RADIUS 要求に対する応答を待って、要求を再送信するまでの時間 (秒) を指定します。デフォルトは 5 秒です。指定できる範囲は 1 ~ 1000 です。
ステップ 5	<b>radius-server deadtime minutes</b>  例 :  デバイス (config) # <b>radius-server deadtime 0</b>	RADIUS サーバが認証要求に応答していない場合、このコマンドはそのサーバに対する要求を停止する時刻を指定します。これにより、要求がタイムアウトするまで待たずとも、次に設定されているサーバを試行することができます。デフォルトは 0 です。指定できる範囲は 1 ~ 1440 分です。
ステップ 6	<b>end</b>  例 :  デバイス (config) # <b>end</b>	特権 EXEC モードに戻ります。
ステップ 7	<b>show running-config</b>  例 :  デバイス # <b>show running-config</b>	入力を確認します。
ステップ 8	<b>copy running-config startup-config</b>  例 :  デバイス # <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## ベンダー固有の RADIUS 属性を使用するデバイス設定

ベンダー固有の RADIUS 属性を使用するように device を設定するには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **radius-server vsa send [accounting | authentication]**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： デバイス> <b>enable</b>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>• パスワードを入力します（要求された場合）。</li> </ul>
ステップ 2	<b>configure terminal</b> 例： デバイス# <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 3	<b>radius-server vsa send [accounting   authentication]</b> 例： デバイス(config)# <b>radius-server vsa send accounting</b>	device が VSA（RADIUS IETF 属性 26 で定義）を認識して使用できるようにします。 <ul style="list-style-type: none"> <li>• （任意）認識されるベンダー固有属性の集合を アカウンティング属性だけに限定するには、<b>accounting</b> キーワードを使用します。</li> <li>• （任意）認識されるベンダー固有属性の集合を 認証属性だけに限定するには、<b>authentication</b> キーワードを使用します。</li> </ul> キーワードを指定せずにこのコマンドを入力すると、アカウンティングおよび認証のベンダー固有属性の両方が使用されます。
ステップ 4	<b>end</b> 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	デバイス(config)# end	
ステップ 5	<b>show running-config</b> 例： デバイス# show running-config	入力を確認します。
ステップ 6	<b>copy running-config startup-config</b> 例： デバイス# copy running-config startup-config	(任意) コンフィギュレーションファイルに設定を保存します。

## ベンダー独自の RADIUS サーバーとの通信に関するデバイスの設定

ベンダー独自仕様の RADIUS サーバー通信を使用するように device を設定するには、次の手順を実行します。

### 手順の概要

1. enable
2. configure terminal
3. radius server *server name*
4. address { ipv4 | ipv6 } *ip address*
5. non-standard
6. key *string*
7. exit
8. end
9. show running-config
10. copy running-config startup-config

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： デバイス> enable	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	<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
	デバイス# <code>configure terminal</code>	
ステップ 3	<b>radius server</b> <i>server name</i> 例 : デバイス (config)# <code>radius server rsim</code>	RADIUS サーバーを指定します。
ステップ 4	<b>address</b> { <b>ipv4</b>   <b>ipv6</b> } <i>ip address</i> 例 : デバイス (config-radius-server)# <code>address ipv4 172.24.25.10</code>	(任意) RADIUS サーバの IP アドレスを指定します。
ステップ 5	<b>non-standard</b> 例 : デバイス (config-radius-server)# <code>non-standard</code>	RADIUS サーバが RADIUS ベンダー独自の実装を使用していることを示します。
ステップ 6	<b>key string</b> 例 : デバイス (config-radius-server)# <code>key rad123</code>	device とベンダー独自仕様の RADIUS サーバーとの間で使用される共有秘密テキスト文字列を指定します。device と RADIUS サーバーはこのテキスト文字列を使用してパスワードを暗号化し、応答を交換します。
ステップ 7	<b>exit</b> 例 : デバイス (config-radius-server)# <code>exit</code>	RADIUS サーバーモードを終了して、グローバル コンフィギュレーション モードを開始します。
ステップ 8	<b>end</b> 例 : デバイス (config)# <code>end</code>	特権 EXEC モードに戻ります。
ステップ 9	<b>show running-config</b> 例 : デバイス# <code>show running-config</code>	入力を確認します。

	コマンドまたはアクション	目的
ステップ 10	<b>copy running-config startup-config</b> 例 :  デバイス# <b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。

## 次の上での CoA の設定 デバイス

CoA を device で設定するには、次の手順を実行します。この手順は必須です。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa server radius dynamic-author**
5. **client** {*ip-address* | *name*} [ *vrf vrfname*] [ **server-key string**]
6. **server-key** [0 | 7] *string*
7. **port** *port-number*
8. **auth-type** {*any* | *all* | *session-key*}
9. **ignore session-key**
10. **ignore server-key**
11. **authentication command bounce-port ignore**
12. **authentication command disable-port ignore**
13. **end**
14. **show running-config**
15. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 :  デバイス> <b>enable</b>	特権 EXEC モードを有効にします。  <ul style="list-style-type: none"> <li>• パスワードを入力します (要求された場合)。</li> </ul>
ステップ 2	<b>configure terminal</b> 例 :  デバイス# <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。



	コマンドまたはアクション	目的
ステップ 3	<b>aaa new-model</b> 例 :  デバイス (config) # <b>aaa new-model</b>	AAA をイネーブルにします。
ステップ 4	<b>aaa server radius dynamic-author</b> 例 :  デバイス (config) # <b>aaa server radius dynamic-author</b>	device を認証、許可、アカウントिंग (AAA) サーバーに設定し、外部ポリシーサーバーとの相互作用を実行します。
ステップ 5	<b>client {ip-address   name} [ vrf vrfname] [ server-key string]</b>	ダイナミック許可ローカル サーバー コンフィギュレーションモードを開始し、デバイスが CoA を受け取り、要求を取り外す RADIUS クライアントを指定します。
ステップ 6	<b>server-key [0   7] string</b> 例 :  デバイス (config-sg-radius) # <b>server-key your_server_key</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。
ステップ 7	<b>port port-number</b> 例 :  デバイス (config-sg-radius) # <b>port 25</b>	設定された RADIUS クライアントから RADIUS 要求をデバイスが受信するポートを指定します。
ステップ 8	<b>auth-type {any   all   session-key}</b> 例 :  デバイス (config-sg-radius) # <b>auth-type any</b>	device が RADIUS クライアントに使用する許可のタイプを指定します。  クライアントは、許可用に設定されたすべての属性と一致していなければなりません。
ステップ 9	<b>ignore session-key</b>	(任意) セッションキーを無視するように device を設定します。  <b>ignore</b> コマンドの詳細については、Cisco.com 上の『Cisco IOS Intelligent Services Gateway Command Reference』を参照してください。
ステップ 10	<b>ignore server-key</b> 例 :	(任意) サーバキーを無視するように device を設定します。

	コマンドまたはアクション	目的
	デバイス (config-sg-radius) # <code>ignore server-key</code>	<b>ignore</b> コマンドの詳細については、Cisco.com 上の『Cisco IOS Intelligent Services Gateway Command Reference』を参照してください。
ステップ 11	<b>authentication command bounce-port ignore</b> 例： デバイス (config-sg-radius) # <code>authentication command bounce-port ignore</code>	(任意) CoA 要求を無視して、セッションをホスティングするポートを一時的にディセーブルにするように <code>device</code> を設定します。ポートを一時的にディセーブルにする目的は、VLAN の変更が発生しても、その変更を検出するサブリカントがエンドポイント上にない場合に、ホストから DHCP 再ネゴシエーションを行わせることです。
ステップ 12	<b>authentication command disable-port ignore</b> 例： デバイス (config-sg-radius) # <code>authentication command disable-port ignore</code>	(任意) セッションをホスティングしているポートを管理上のシャットダウン状態にするよう要求する非標準コマンドを無視するように <code>device</code> を設定します。ポートをシャットダウンすると、セッションが終了します。  ポートを再びイネーブルにするには、標準の CLI または SNMP コマンドを使用します。
ステップ 13	<b>end</b> 例： デバイス (config-sg-radius) # <code>end</code>	特権 EXEC モードに戻ります。
ステップ 14	<b>show running-config</b> 例： デバイス # <code>show running-config</code>	入力を確認します。
ステップ 15	<b>copy running-config startup-config</b> 例： デバイス # <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

## CoA 機能のモニタリング

表 26: 特権 EXEC 表示コマンド

コマンド	目的
<b>show aaa attributes protocol radius</b>	RADIUS コマンドの AAA 属性を表示します。

表 27: グローバルトラブルシューティングコマンド

コマンド	目的
<b>debug radius</b>	RADIUS のトラブルシューティングを行うための情報を表示します。
<b>debug aaa coa</b>	CoA 処理のトラブルシューティングを行うための情報を表示します。
<b>debug aaa pod</b>	POD パケットのトラブルシューティングを行うための情報を表示します。
<b>debug aaa subsys</b>	POD パケットのトラブルシューティングを行うための情報を表示します。
<b>debug cmdhd[detail  error  events]</b>	コマンドヘッダーのトラブルシューティングを行うための情報を表示します。

出力フィールドの詳細については、このリリースに対応するコマンドリファレンスを参照してください。

## RADIUS の機能の履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	RADIUS	RADIUS は、不正なアクセスからネットワークのセキュリティを保護する分散クライアント/サーバシステムです。RADIUS クライアントは、サポート対象のシスコデバイス上で稼働します。クライアントは中央の RADIUS サーバに認証要求を送ります。中央の RADIUS サーバにはすべてのユーザ認証情報、ネットワークサービスアクセス情報が登録されています。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



## 第 9 章

# RadSec の設定

この章では、RadSec over Transport Layer Security (TLS) および Datagram Transport Layer Security (DTLS) サーバーを設定する方法について説明します。

- [RadSec の設定に関する制限事項 \(207 ページ\)](#)
- [RadSec に関する情報 \(207 ページ\)](#)
- [RadSec の設定方法 \(207 ページ\)](#)
- [RadSec のモニタリング \(213 ページ\)](#)
- [RadSec の設定例 \(213 ページ\)](#)
- [RadSec 設定の機能履歴 \(214 ページ\)](#)

## RadSec の設定に関する制限事項

RadSec 機能には、次のような制限事項が適用されます。

- RADIUS クライアントは、送信元ポートとして一時ポートを使用します。この送信元ポートは、UDP、データグラムトランスポート層セキュリティ (DTLS)、およびトランスポート層セキュリティ (TLS) に同時に使用しないでください。
- 設定上の制限はありませんが、認証、認可、およびアカウントティング (AAA) サーバークラウド内のサーバーには、同じタイプ (TLS のみまたは DTLS のみ) を使用することをお勧めします。
- RadSec は、IPv4 接続でのみサポートされます。

## RadSec に関する情報

## RadSec の設定方法

次のセクションでは、RadSec の設定を構成するさまざまな作業について説明します。

## RadSec over TLS の設定

### 手順の概要

1. **enable**
2. **configure terminal**
3. **radius server** *radius-server-name*
4. **tls** [**connectiontimeout** *connection-timeout-value*] [**idletimeout** *idle-timeout-value*] [**ip** {**radius source-interface** *interface-name* |**vrf forwarding** *forwarding-table-name*} ] [**port** *port-number*] [**retries** *number-of-connection-retries*] [**trustpoint** {**client** *trustpoint name* | **server** *trustpoint name*}]
5. **end**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> enable	特権 EXEC モードを有効にします。  • プロンプトが表示されたらパスワードを入力します。
ステップ 2	<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 3	<b>radius server</b> <i>radius-server-name</i> 例： Device(config)# radius server R1	RADIUS サーバー設定の名前を Protected Access Credential (PAC) のプロビジョニング用に指定し、RADIUS サーバー設定モードを開始します。
ステップ 4	<b>tls</b> [ <b>connectiontimeout</b> <i>connection-timeout-value</i> ] [ <b>idletimeout</b> <i>idle-timeout-value</i> ] [ <b>ip</b> { <b>radius source-interface</b> <i>interface-name</i>   <b>vrf forwarding</b> <i>forwarding-table-name</i> } ] [ <b>port</b> <i>port-number</i> ] [ <b>retries</b> <i>number-of-connection-retries</i> ] [ <b>trustpoint</b> { <b>client</b> <i>trustpoint name</i>   <b>server</b> <i>trustpoint name</i> }] 例： Device(config-radius-server)# tls connectiontimeout 10 Device(config-radius-server)# tls idletimeout 75 Device(config-radius-server)# tls retries 15 Device(config-radius-server)# tls ip radius source-interface GigabitEthernet 1/0/1 Device(config-radius-server)# tls ip vrf forwarding table-1 Device(config-radius-server)# tls port 10 Device(config-radius-server)# tls trustpoint client TP-self-signed-721943660	TLS パラメータを設定します。次のパラメータを設定できます：  • <b>connectiontimeout</b> : TLS 接続タイムアウト値を設定します。デフォルトは 5 秒です。  • <b>idletimeout</b> : TLS アイドルタイムアウト値を設定します。デフォルトは 60 秒です。  • <b>ip</b> : IP 送信元パラメータを設定します。  • <b>port</b> : TLS ポート番号を設定します。デフォルトは 2083 です。  • <b>retries</b> : TLS 接続再試行の回数を設定します。デフォルトは 5 です。  • <b>trustpoint</b> : クライアントとサーバーに TLS トラストポイントを設定します。クライアントとサーバーの TLS トラストポイントが同じ場合、

	コマンドまたはアクション	目的
	Device(config-radius-server)# tls trustpoint server isetp	トラストポイント名も両方で同じである必要があります。
ステップ 5	<b>end</b> 例： Device(config-radius-server)# end	RADIUS サーバ 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。

## TLS CoA の動的認可の設定

### 手順の概要

1. **enable**
2. **configure terminal**
3. **aaa server radius dynamic-author**
4. **client {ip-addr | hostname} [tls [client-tp client-tp-name] [idletimeout idletimeout-interval] [server-tp server-tp-name] | vrf vrf-id ]**
5. **end**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： デバイス> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"><li>• パスワードを入力します（要求された場合）。</li></ul>
ステップ 2	<b>configure terminal</b> 例： デバイス# 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 3	<b>aaa server radius dynamic-author</b> 例： デバイス(config)# aaa server radius dynamic-author	ダイナミック認可ローカル サーバ コンフィギュレーション モードを開始し、デバイスが認可変更 (CoA) を受け入れ、要求を取り外す RADIUS クライアントを指定します。デバイスを AAA サーバ として設定し、外部ポリシーサーバとの連携を可能にする。
ステップ 4	<b>client {ip-addr   hostname} [tls [client-tp client-tp-name] [idletimeout idletimeout-interval] [server-tp server-tp-name]   vrf vrf-id ]</b> 例： デバイス(config-locsvr-da-radius)# client 10.104.49.14 tls idletimeout 100 client-tp tls_ise	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。次のオプションのパラメータを設定できます。 <ul style="list-style-type: none"><li>• <b>tls</b> : クライアントの TLS を有効にします。</li></ul>

	コマンドまたはアクション	目的
	<code>server-tp tls_client</code>	<ul style="list-style-type: none"> <li>• <b>client-tp</b> : クライアント トラストポイントを設定します。</li> <li>• <b>idletimeout</b> : DTLS アイドルタイムアウト値を設定します。</li> <li>• <b>server-tp</b> : サーバートラストポイントを設定します。</li> <li>• <b>vrf</b> : クライアントの Virtual Routing and Forwarding (VRF) ID。</li> </ul>
ステップ 5	<b>end</b> 例 : デバイス(config-radius-server)# end	ダイナミック認可ローカル サーバー コンフィギュレーション モードから特権 EXEC モードに戻ります。

## RadSec over DTLS の設定

### 手順の概要

1. **enable**
2. **configure terminal**
3. **radius server** *radius-server-name*
4. **dtls** [**connectiontimeout** *connection-timeout-value*] [**idletimeout** *idle-timeout-value*] [**ip** {**radius source-interface** *interface-name* | **vrf forwarding** *forwarding-table-name*} ] [**port** *port-number*] [**retries** *number-of-connection-retries*] [**trustpoint** {**client** *trustpoint name* | **server** *trustpoint name*}]
5. **end**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>• プロンプトが表示されたらパスワードを入力します。</li> </ul>
ステップ 2	<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 3	<b>radius server</b> <i>radius-server-name</i> 例 : Device(config)# radius server R1	RADIUS サーバー設定の名前を Protected Access Credential (PAC) のプロビジョニング用に指定し、RADIUS サーバー設定モードを開始します。



	コマンドまたはアクション	目的
ステップ 4	<p><b>dtls</b> [<b>connectiontimeout</b> <i>connection-timeout-value</i>] [<b>idletimeout</b> <i>idle-timeout-value</i>] [<b>ip</b> {<b>radius source-interface</b> <i>interface-name</i>   <b>vrf forwarding forwarding-table-name</b>} ] [<b>port</b> <i>port-number</i>] [<b>retries</b> <i>number-of-connection-retries</i>] [<b>trustpoint</b> {<b>client</b> <i>trustpoint name</i>   <b>server</b> <i>trustpoint name</i>}]</p> <p>例 :</p> <pre>Device(config-radius-server)# dtls connectiontimeout 10  Device(config-radius-server)# dtls idletimeout 75  Device(config-radius-server)# dtls retries 15  Device(config-radius-server)# dtls ip radius source-interface GigabitEthernet 1/0/1  Device(config-radius-server)# dtls ip vrf forwarding table-1  Device(config-radius-server)# dtls port 10  Device(config-radius-server)# dtls trustpoint client TP-self-signed-721943660  Device(config-radius-server)# dtls trustpoint server isetp</pre>	<p>DTLS パラメータを設定します。次のパラメータを設定できます。</p> <ul style="list-style-type: none"> <li>• <b>connectiontimeout</b> : DTLS 接続タイムアウト値を設定します。デフォルトは 5 秒です。</li> <li>• <b>idletimeout</b> : DTLS アイドルタイムアウト値を設定します。デフォルトは 60 秒です。</li> <li>• <b>ip</b> : IP 送信元パラメータを設定します。</li> <li>• <b>port</b> : DTLS ポート番号を設定します。デフォルトは 2083 です。</li> <li>• <b>retries</b> : DTLS 接続再試行の回数を設定します。デフォルトは 5 です。</li> <li>• <b>trustpoint</b> : クライアントとサーバーに DTLS トラストポイントを設定します。クライアントとサーバーの DTLS トラストポイントが同じ場合、トラストポイント名も両方で同じである必要があります。</li> </ul>
ステップ 5	<p><b>end</b></p> <p>例 :</p> <pre>Device(config-radius-server)# end</pre>	<p>RADIUS サーバ 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。</p>

## DTLS CoA の動的認可の設定

### 手順の概要

1. **enable**
2. **configure terminal**
3. **aaa server radius dynamic-author**
4. **client** {**ip-addr** | **hostname**} [**dtls** [**client-tp** *client-tp-name*] [**idletimeout** *idletimeout-interval*] [**server-tp** *server-tp-name*] | **vrf** *vrf-id* ]
5. **dtls** {**ip radius source-interface** *interface-name* | **port** *radius-dtls-server-port-number*}
6. **end**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<p><b>enable</b></p> <p>例 :</p>	<p>特権 EXEC モードを有効にします。</p> <ul style="list-style-type: none"> <li>• パスワードを入力します (要求された場合)。</li> </ul>

	コマンドまたはアクション	目的
	デバイス> enable	
ステップ 2	<b>configure terminal</b> 例： デバイス# 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 3	<b>aaa server radius dynamic-author</b> 例： デバイス(config)# aaa server radius dynamic-author	ダイナミック認可ローカル サーバー コンフィギュレーション モードを開始し、デバイスが認可変更 (CoA) を受け入れ、要求を取り外す RADIUS クライアントを指定します。デバイスを AAA サーバーとして設定し、外部ポリシーサーバーとの連携を可能にする。
ステップ 4	<b>client {ip-addr   hostname} [dtls [client-tp client-tp-name] [idletimeout idletimeout-interval] [server-tp server-tp-name]   vrf vrf-id ]</b> 例： デバイス(config-locsvr-da-radius)# client 10.104.49.14 dtls idletimeout 100 client-tp dtls_ise server-tp dtls_client	AAA サーバー 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。次のオプションのパラメータを設定できます。 <ul style="list-style-type: none"> <li>• <b>dtls</b> : クライアントの DTLS を有効にします。</li> <li>• <b>client-tp</b> : クライアント トラストポイントを設定します。</li> <li>• <b>idletimeout</b> : DTLS アイドルタイムアウト値を設定します。</li> <li>• <b>server-tp</b> : サーバートラストポイントを設定します。</li> <li>• <b>vrf</b> : クライアントの Virtual Routing and Forwarding (VRF) ID。</li> </ul>
ステップ 5	<b>dtls {ip radius source-interface interface-name   port radius-dtls-server-port-number}</b> 例： デバイス(config-locsvr-da-radius)# dtls ip radius source-interface GigabitEthernet 1/0/24 デバイス(config-locsvr-da-radius)# dtls port 100	RADIUS CoA サーバを設定します。次のパラメータを設定できます。 <ul style="list-style-type: none"> <li>• <b>ip radius source-interface interface-name</b> : RADIUS CoA サーバーの送信元アドレスのインターフェイスを指定します。</li> <li>• <b>port radius-dtls-server-port-number</b> : ローカル DTLS RADIUS サーバーがリスンするポートを指定します。</li> </ul>
ステップ 6	<b>end</b> 例： デバイス(config-radius-server)# end	ダイナミック認可ローカル サーバー コンフィギュレーション モードから特権 EXEC モードに戻ります。

## RadSec のモニタリング

次のコマンドを使用して、TLS および DTLS サーバーの統計を監視します。

表 28: TLS および DTLS サーバー統計コマンドの監視

コマンド	目的
<code>show aaa servers</code>	TLS および DTLS サーバーに関連する情報を表示します。
<code>clear aaa counters servers radius {server id   all}</code>	RADIUS TLS 固有または DTLS 固有の統計情報をクリアします。
<code>debug radius radsec</code>	RADIUS RadSec デバッグを有効にします。

## RadSec の設定例

次の例は、RadSec の設定を理解するのに役立ちます。

### 例 : RadSec over TLS の設定

```
Device> enable
Device# configure terminal
Device(config)# radius server R1
Device(config-radius-server)# tls connectiontimeout 10
Device(config-radius-server)# tls idletimeout 75
Device(config-radius-server)# tls retries 15
Device(config-radius-server)# tls ip radius source-interface GigabitEthernet 1/0/1
Device(config-radius-server)# tls ip vrf forwarding table-1
Device(config-radius-server)# tls port 10
Device(config-radius-server)# tls trustpoint client TP-self-signed-721943660
Device(config-radius-server)# tls trustpoint server isetp
Device(config-radius-server)# end
```

### 例 : TLS CoA の動的認可の設定

```
Device> enable
Device# configure terminal
Device(config)# aaa server radius dynamic-author
Device(config-locsvr-da-radius)# client 10.104.49.14 tls idletimeout 100 client-tp tls_ise
server-tp tls_client
Device(config-locsvr-da-radius)# dtls port 100
Device(config-radius-server)# end
```

## 例 : RadSec over DTLS の設定

```

Device> enable
Device# configure terminal
Device(config)# radius server R1
Device(config-radius-server)# dtls connectiontimeout 10
Device(config-radius-server)# dtls idletimeout 75
Device(config-radius-server)# dtls retries 15
Device(config-radius-server)# dtls ip radius source-interface GigabitEthernet 1/0/1
Device(config-radius-server)# dtls ip vrf forwarding table-1
Device(config-radius-server)# dtls port 10
Device(config-radius-server)# dtls trustpoint client TP-self-signed-721943660
Device(config-radius-server)# dtls trustpoint server isetp
Device(config-radius-server)# end

```

## 例 : DTLS CoA の動的認可の設定

```

Device> enable
Device# configure terminal
Device(config)# aaa server radius dynamic-author
Device(config-locsvr-da-radius)# client 10.104.49.14 dtls idletimeout 100 client-tp
dtls_ise server-tp dtls_client
Device(config-locsvr-da-radius)# dtls ip radius source-interface GigabitEthernet 1/0/24
Device(config-locsvr-da-radius)# dtls port 100
Device(config-radius-server)# end

```

## RadSec 設定の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.6.1	RadSec over DTLS の設定	RadSec over DTLS は、安全なトンネルを介して転送される RADIUS サーバー上で暗号化サービスを提供します。
Cisco IOS XE Fuji 16.9.1	RadSec over TLS の設定	RadSec over TLS は、安全なトンネルを介して転送される RADIUS サーバー上で暗号化サービスを提供します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



## 第 10 章

# Kerberos の設定

- [Kerberos によるスイッチ アクセスの制御の前提条件](#) (215 ページ)
- [Kerberos に関する情報](#) (215 ページ)
- [Kerberos を設定する方法](#) (220 ページ)
- [Kerberos 設定の監視](#) (220 ページ)
- [Kerberos の機能履歴](#) (220 ページ)

## Kerberos によるスイッチ アクセスの制御の前提条件

次に、Kerberos を使用してスイッチ アクセスを制御するための前提条件を示します。

- リモート ユーザーがネットワーク サービスに対して認証を得るには、Kerberos レルム内のホストと KDC を設定し、ユーザーとネットワーク サービスの両方に通信を行い、相互に認証させる必要があります。これを実現するには、互いの識別が必要です。KDC 上の Kerberos データベースにホストのエントリを追加し、Kerberos レルム内のすべてのホストに KDC が生成した KEYTAB ファイルを追加します。また、KDC データベースにユーザー用のエントリも作成します。
- Kerberos サーバーには、ネットワーク セキュリティ サーバーとして設定されていて、Kerberos プロトコルを用いてユーザーを認証できるスイッチを使用できます。

ホストおよびユーザーのエントリを追加または作成する場合の注意事項は次のとおりです。

- Kerberos プリンシパル名はすべて小文字でなければなりません。
- Kerberos インスタンス名はすべて小文字でなければなりません。
- Kerberos レルム名はすべて大文字でなければなりません。

## Kerberos に関する情報

ここでは、Kerberos の情報を提供します。

## Kerberos とスイッチ アクセス

ここでは、Kerberos セキュリティ システムをイネーブルにして設定する方法について説明します。Kerberos セキュリティ システムは、信頼できるサードパーティを使用してネットワーク リソースに対する要求を認証します。



- (注) Kerberos の設定例では、信頼できるサードパーティを、Kerberos をサポートし、ネットワーク セキュリティ サーバーとして設定され、Kerberos プロトコルを使用してユーザーを認証するスイッチとすることができます。

## Kerberos の概要

Kerberos はマサチューセッツ工科大学 (MIT) が開発した秘密キーによるネットワーク 認証 プロトコルです。データ暗号規格 (DES) という暗号化アルゴリズムを暗号化と認証に使用し、ネットワーク リソースに対する要求を認証します。Kerberos は、信頼できるサードパーティという概念を使ってユーザーとサービスに対してセキュリティの検証を実行します。この信頼できるサードパーティをキー発行局 (KDC) と呼びます。

Kerberos は、ユーザーが誰であるか、そのユーザーが使用しているネットワーク サービスは何であるかを検証します。これを実行するために、KDC (つまり信頼できる Kerberos サーバー) がユーザーにチケットを発行します。これらのチケットには有効期限があり、ユーザー クレデンシャルのキャッシュに保存されます。Kerberos サーバーは、ユーザー名やパスワードの代わりにチケットを使ってユーザーとネットワーク サービスを認証します。



- (注) Kerberos サーバーには、ネットワーク セキュリティ サーバーとして設定されていて、Kerberos プロトコルを用いてユーザーを認証できるのであれば、どのスイッチも使用できます。

Kerberos のクレデンシャル発行スキームでは、*single logon* という手順を使用します。この手順では、ユーザーを 1 回認証すると、ユーザー クレデンシャルが有効な間は (他のパスワードの暗号化を行わずに) セキュア認証が可能になります。

このソフトウェア リリースは Kerberos 5 に対応しています。Kerberos 5 では、すでに Kerberos 5 を使用している組織が、(UNIX サーバーや PC などの) 他のネットワーク ホストが使用している KDC 上の Kerberos 認証データベースを使用できます。

Kerberos は次のネットワーク サービスをサポートしています。

- Telnet
- rlogin
- rsh

次の表に、一般的な Kerberos 関連用語とその定義を示します。

表 29 : Kerberos の用語

用語	定義
認証	ユーザーやサービスが他のサービスに対して自分自身の身元を証明する手順。たとえば、クライアントはスイッチに対して認証を得て、スイッチは他のスイッチに対して認証を得ます。
許可	ユーザーがネットワークやスイッチにおいてどのような権限を有しており、またどのような動作を実行できるかを、スイッチが識別する手段
クレデンシヤル	認証チケット (TSG <sup>2</sup> 、サービスクレデンシヤルなど) を表す総称。Kerberos クレデンシヤルで、ユーザーまたはサービスの ID を検証します。ネットワーク サービスがチケットを発行した Kerberos サーバーを信頼することにした場合、ユーザー名やパスワードを再入力する代わりにこれを使用できます。証明書の有効期限は、8 時間がデフォルトの設定です。
インスタンス	Kerberos プリンシパルの承認レベル ラベル。ほとんどの Kerberos プリンシパルは、 <code>user@REALM</code> という形式です (たとえば、 <code>smith@EXAMPLE.COM</code> )。Kerberos インスタンスのある Kerberos プリンシパルは、 <code>user/instance@REALM</code> という形式です (たとえば、 <code>smith/admin@EXAMPLE.COM</code> )。Kerberos インスタンスは、認証が成功した場合のユーザーの承認レベルを指定するために使用できます。各ネットワーク サービスのサーバーは、Kerberos インスタンスの許可マッピングを適用し実行できますが、必須ではありません。  (注) Kerberos プリンシパル名およびインスタンス名はすべて小文字でなければなりません。  (注) Kerberos レルム名はすべて大文字でなければなりません。
KDC <sup>3</sup>	ネットワーク ホストで稼働する Kerberos サーバーおよびデータベースプログラムで構成されるキー発行局
Kerberos 対応	Kerberos クレデンシヤルのインフラストラクチャをサポートするために変更されたアプリケーションやサービスのことを指す用語
Kerberos レルム	Kerberos サーバーに登録されたユーザー、ホスト、およびネットワーク サービスで構成されるドメイン。Kerberos サーバーを信頼して、ユーザーまたはネットワーク サービスに対する別のユーザーまたはネットワーク サービスの ID を検証します。  (注) Kerberos レルム名はすべて大文字でなければなりません。

用語	定義
Kerberos サーバー	ネットワーク ホストで稼働しているデーモン。ユーザーおよびネットワーク サービスはそれぞれ Kerberos サーバーに ID を登録します。ネットワーク サービスは Kerberos サーバーにクエリーを送信して、他のネットワーク サービスの認証を得ます。
KEYTAB <sup>4</sup>	ネットワーク サービスが KDC と共有するパスワード。Kerberos 5 以降のバージョンでは、ネットワーク サービスは KEYTAB を使って暗号化されたサービス クレデンシヤルを暗号解除して認証します。Kerberos 5 よりも前のバージョンでは、KEYTAB は SRVTAB <sup>5</sup> と呼ばれます。
プリンシパル	Kerberos ID と呼ばれ、Kerberos サーバーに基づき、ユーザーが誰であるか、サービスが何であるかを表します。  (注) Kerberos プリンシパル名はすべて小文字でなければなりません。
サービス クレデンシヤル	ネットワーク サービスのクレデンシヤル。KDC からクレデンシヤルが発行されると、ネットワーク サービスと KDC が共有するパスワードで暗号化されます。ユーザー TGT ともパスワードを共有します。
SRVTAB	ネットワーク サービスが KDC と共有するパスワード。SRVTAB は、Kerberos 5 以降のバージョンでは KEYTAB と呼ばれています。
TGT	身分証明書のこと、KDC が認証済みユーザーに発行するクレデンシヤル。TGT を受け取ったユーザーは、KDC が示した Kerberos レalm 内のネットワーク サービスに対して認証を得ることができます。

<sup>2</sup> チケット認可チケット

<sup>3</sup> キー発行局

<sup>4</sup> キー テーブル

<sup>5</sup> サーバー テーブル

## Kerberos の動作

リモートユーザーが device を Kerberos サーバーとして使用してネットワークサービスで認証されるには、次の手順を実行する必要があります。Kerberos をカスタマイズする方法はいくつかありますが、ネットワーク サービスにアクセスしようとするリモートユーザーは、3つのセキュリティ レイヤを通過しないとネットワーク サービスにアクセスできません。

リモートユーザーが device を Kerberos サーバーとして使用してネットワークサービスで認証されるには、次の手順を実行する必要があります。



## 境界スイッチに対する認証の取得

ここでは、リモートユーザーが通過しなければならない最初のセキュリティレイヤについて説明します。ユーザーは、まず境界スイッチに対して認証を得なければなりません。リモートユーザーが境界スイッチに対して認証を得る場合、次のプロセスが発生します。

1. ユーザーが境界スイッチに対して、Kerberos 未対応の Telnet 接続を開始します。
2. ユーザー名とパスワードの入力を求めるプロンプトをスイッチが表示します。
3. スイッチが、このユーザーの TGT を KDC に要求します。
4. KDC がユーザー ID を含む暗号化された TGT をスイッチに送信します。
5. スイッチは、ユーザーが入力したパスワードを使って TGT の暗号解除を試行します。
  - 暗号解除に成功した場合は、ユーザーはスイッチに対して認証を得ます。
  - 暗号解除に成功しない場合は、ユーザー名とパスワードを再入力（Caps Lock または NumLock のオン/オフに注意）するか、別のユーザー名とパスワードを入力してステップ 2 の手順を繰り返します。

Kerberos 未対応の Telnet セッションを開始し、境界スイッチの認証を得ているリモートユーザーはファイアウォールの内側にいますが、ネットワークサービスにアクセスするには、KDC から直接認証を得る必要があります。ユーザーが KDC から認証を得なければならないのは、KDC が発行する TGT はスイッチに保存されており、ユーザーがこのスイッチにログオンしないかぎり、追加の認証に使用できないからです。

## KDC からの TGT の取得

ここでは、リモートユーザーが通過しなければならない 2 番目のセキュリティレイヤについて説明します。ユーザーは、ネットワークサービスにアクセスするために、このレイヤで KDC の認証を得て、KDC から TGT を取得しなければなりません。

KDC に対して認証を得る方法については、『*Cisco IOS Security Configuration Guide, Release 12.4*』の「Security Server Protocols」の章にある「Obtaining a TGT from a KDC」を参照してください。

## ネットワーク サービスに対する認証の取得

ここでは、リモートユーザーが通過しなければならない 3 番目のセキュリティレイヤについて説明します。TGT を取得したユーザーは、このレイヤで Kerberos レルム内のネットワークサービスに対して認証を得なければなりません。

ネットワーク サービスに対して認証を得る方法については、『*Cisco IOS Security Configuration Guide, Release 12.4*』の「Security Server Protocols」の章の「Authenticating to Network Services」を参照してください。

## Kerberos を設定する方法

Kerberos 認証済みサーバー/クライアント システムを設定する手順は、次のとおりです。

- Kerberos コマンドを使用して KDC を設定します。
- Kerberos プロトコルを使用するようにスイッチを設定します。

## Kerberos 設定の監視

Kerberos 設定を表示するには、次のコマンドを使用します。

- **show running-config**
- **show kerberos creds** : 現在のユーザーの認定証キャッシュに含まれる認定証を一覧表示します。
- **clear kerberos creds** : 転送済みの認定証を含め、現在のユーザーの認定証キャッシュに含まれるすべての認定証を破棄します。

## Kerberos の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	Kerberos	Kerberos はマサチューセッツ工科大学 (MIT) が開発した秘密キーによるネットワーク認証プロトコルです。データ暗号規格 (DES) という暗号化アルゴリズムを暗号化と認証に使用し、ネットワーク リソースに対する要求を認証します。Kerberos は、信頼できるサードパーティという概念を使ってユーザーとサービスに対してセキュリティの検証を実行します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



## 第 11 章

# MACsec の暗号化

- [MACsec 暗号化の前提条件](#) (221 ページ)
- [MACsec 暗号化の制約事項](#) (221 ページ)
- [MACsec 暗号化の概要](#) (222 ページ)
- [MACsec 暗号化の設定方法](#) (231 ページ)
- [MACsec 暗号化の設定例](#) (258 ページ)
- [MACsec 暗号化の機能情報](#) (280 ページ)

## MACsec 暗号化の前提条件

### 証明書ベース MACsec の前提条件

- 認証局 (CA) サーバーがネットワークに設定されていることを確認します。
- CA 証明書を生成します。
- Cisco Identity Services Engine (ISE) リリース 2.0 が設定されていることを確認します。
- 両方の参加デバイス (CA サーバーと Cisco Identity Services Engine (ISE)) が Network Time Protocol (NTP) を使用して同期されていることを確認します。時間がすべてのデバイスで同期されていないと、証明書は検証されません。
- 802.1x 認証と AAA がデバイスに設定されていることを確認します。

## MACsec 暗号化の制約事項

- C9300-48UXM および C9300-48UN スイッチモデルの MACsec は、最初の 16 のダウンリンク ネットワーク ポートとすべてのアップリンク ネットワーク モジュールポートでのみサポートされます。MACsec は、C9300-48UXM および C9300-48UN スイッチモデルの最後の 32 個のダウンリンク ネットワーク ポートではサポートされません。
- MACsec 設定は、EtherChannel ポートではサポートされません。代わりに、EtherChannel の個々のメンバポートに MACsec 設定を適用できます。MACsec 設定を削除するには、最

初に EtherChannel からメンバポートをバンドル解除してから、個々のメンバポートから削除する必要があります。

- 証明書ベースの MACsec は、アクセスセッションがクローズドとして、またはマルチホストモードで設定されている場合にのみサポートされます。他のコンフィギュレーションモードはサポートされていません。
- MACsec Key Agreement (MKA) はハイアベイラビリティではサポートされません。
- MKA を使用した MACsec は、ポイントツーポイントリンクでのみサポートされます。
- GCM-AES-256 および XPN 暗号スイート (GCM-AES-XPN-128 および GCM-AES-XPN-256) は、Network Advantage ライセンスでのみサポートされます。
- MACsec 暗号アナウンスメントは、MACsec 拡張パケット番号 (XPN) 暗号およびスイッチ間 MACsec 接続ではサポートされません。
- MACsec XPN 暗号スイートは、スイッチからホストへの MACsec 接続ではサポートされていません。
- `dot1q tag vlan native` コマンドがグローバルレベルで設定されている場合、トランクポートでの `dot1x` 再認証は失敗します。
- MACsec XPN 暗号スイートは、機密性オフセットを含む機密性保護を提供しません。
- Precision Time Protocol (PTP) を備えた MACsec はサポートされません。
- MACsec は、Locator ID Separation Protocol (LISP) インターフェイスおよび Cisco Software-Defined Access (SD-Access) ソリューションではサポートされません。
- MACsec はマルチキャスト VPN (mVPN) ではサポートされません。
- MACsec は、ソフトウェア デファインド アクセスの展開ではサポートされていません。
- `should-secure` アクセスモードは、PSK 認証を使用するスイッチ間ポートでのみサポートされます。

## MACsec 暗号化の概要

MACsec は 2 台の MACsec 対応デバイス間のパケットの認証と暗号化の IEEE 802.1AE 規格です。Catalyst スイッチは、スイッチとホストデバイス間の暗号化に、スイッチからホストへのリンクでの MACsec Key Agreement (MKA) による 802.1AE 暗号化をサポートします。また、スイッチは、Cisco TrustSec ネットワーク デバイス アドミッション コントロール (NDAC)、Security Association Protocol (SAP) および MKA ベースのキー交換プロトコルを使用して、スイッチ間 (ネットワーク間デバイス) セキュリティの MACsec 暗号化をサポートします。



- 
- (注) スイッチ間 MACsec が有効な場合、EAP-over-LAN (EAPOL) パケットを除くすべてのトラフィックが暗号化されます。
-

リンク層セキュリティはスイッチ間のパケット認証とスイッチ間のMACsec暗号化の両方を含みます（暗号化は任意です）。リンク層セキュリティは、SAPベースのMACsecでサポートされます。

表 30: スイッチポートのMACsecサポート

Connections	MACsec のサポート
Switch-to-Host	MACsec MKA の暗号化
Switch-to-Switch	MACsec MKA の暗号化（推奨） Cisco TrustSec SAP

Cisco TrustSec と Cisco SAP はスイッチ間のリンクにのみ使用され、PC や IP フォンなどのエンドホストに接続されたスイッチポートではサポートされません。MKA は、スイッチからホストへのリンクとスイッチ間リンクでサポートされます。ホスト側のリンクは、IEEE 802.1x の有無にかかわらず異種デバイスを扱うために、一般に柔軟な認証順序を使用し、オプションで MKA ベースの MACsec 暗号化を使用できます。Cisco NDAC および SAP は、コンパクトなスイッチがワイヤリングクローゼットの外側にセキュリティを拡張するために使用する、ネットワーク エッジアクセス トポロジ (NEAT) と相互排他的です。

## MACsec 暗号化の推奨事項

ここでは、MACsec 暗号化の設定に関する推奨事項を示します。

- スイッチとホスト間の接続では、機密性（暗号化）オフセットを 0 として使用します。
- 双方向フォワーディングおよび検出 (BFD) タイマー値は、10 Gbps ポートでは 750 ミリ秒、10 Gbps を超える速度のポートでは 1.25 秒として使用します。
- アクティブセッションの MKA ポリシーまたは MACsec 設定を変更した後、ポートで **shutdown** コマンドを実行し、**no shutdown** コマンドを実行して、変更がアクティブセッションに適用されるようにします。
- 40Gbps 以上のポート速度には、Extended Packet Numbering (XPN) 暗号スイートを使用します。
- 接続アソシエーションキー (CAK) キー再生成オーバーラップタイマーを 30 秒以上に設定します。
- 10Gbps を超えるポート速度には、Cisco TrustSec Security Association Protocol (SAP) MACsec 暗号化を使用しないでください。
- どのインターフェイスでも、Cisco TrustSec SAP とアップリンク MKA の両方を同時に有効にしないでください。
- MACsec MKA 暗号化を使用することをお勧めします。

## Media Access Control Security と MACsec Key Agreement

802.1AE で定義された MACsec では、暗号化キー入力のためにアウトオブバンド方式を使用することによって、有線ネットワーク上で MAC レイヤの暗号化を実現します。MACsec Key Agreement (MKA) プロトコルでは、必要なセッションキーを提供し、必要な暗号化キーを管理します。MKA と MACsec は、802.1x 拡張認証プロトコル (EAP-TLS) または事前共有キー (PSK) フレームワークを使用した認証に成功した後に実装されます。

MACsec を使用するスイッチでは、MKA ピアに関連付けられたポリシーに応じて、MACsec フレームまたは非 MACsec フレームを許可します。MACsec フレームは暗号化され、整合性チェック値 (ICV) で保護されます。スイッチは MKA ピアからフレームを受信すると、MKA によって提供されたセッションキーを使用してこれらのフレームを暗号化し、正しい ICV を計算します。スイッチはこの ICV をフレーム内の ICV と比較します。一致しない場合は、フレームが破棄されます。また、スイッチは現在のセッションキーを使用して、ICV を暗号化し、セキュアなポート (セキュアな MAC サービスを MKA ピアに提供するために使用されるアクセス ポイント) を介して送信されたフレームに追加します。

MKA プロトコルは、基礎となる MACsec プロトコルで使用される暗号キーを管理します。MKA の基本的な要件は 802.1x-REV で定義されています。MKA プロトコルでは 802.1x を拡張し、相互認証の確認によってピアを検出し、MACsec 秘密キーを共有してピアで交換されるデータを保護できます。

EAP フレームワークでは、新しく定義された EAP-over-LAN (EAPOL) パケットとして MKA を実装します。EAP 認証では、データ交換で両方のパートナーで共有されるマスターセッションキー (MSK) を生成します。EAP セッション ID を入力すると、セキュアな接続アソシエーション キー名 (CKN) が生成されます。スイッチは、アップリンクおよびダウンリンクの両方のオーセンティケータとして機能します。また、ダウンリンクのキーサーバとして機能します。これによってランダムなセキュアアソシエーションキー (SAK) が生成され、クライアントパートナーに送信されます。クライアントはキーサーバではなく、単一の MKA エンティティであるキーサーバとだけ対話できます。キーの派生と生成の後で、スイッチは定期的にトランスポートをパートナーに送信します。デフォルトの間隔は 2 秒間です。

EAPOL プロトコル データ ユニット (PDU) のパケット本体は、MACsec Key Agreement PDU (MKPDU) と呼ばれます。MKA セッションと参加者は、MKA ライフタイム (6 秒間) が経過しても参加者から MKPDU を受信していない場合に削除されます。たとえば、MKA ピアが接続を解除した場合、スイッチ上の参加者は MKA ピアから最後の MKPDU を受信した後、6 秒間経過するまで MKA の動作を継続します。



(注) MKPDU の整合性チェック値 (ICV) インジケータはオプションです。トラフィックが暗号化されている場合、ICV はオプションではありません。

### MKA ポリシー

定義済みの MKA ポリシーをインターフェイスに適用すると、インターフェイス上で MKA がイネーブルになります。MKA ポリシーを削除すると、そのインターフェイス上で MKA がディセーブルになります。次のオプションを設定可能です。

- 16 ASCII 文字未満のポリシー名。
- 物理インターフェイスごとの 0 バイト、30 バイト、または 50 バイトの機密保持（暗号化）オフセット。

## ポリシーマップアクションの定義

ここでは、ポリシーマップアクションとその定義について説明します。

- **Activate** : サービステンプレートをセッションに適用します。
- **Authenticate** : セッションの認証を開始します。
- **Authorize** : セッションを明示的に許可します。
- **Set-domain** : クライアントのドメインを明示的に設定します。
- **Terminate** : 実行中のメソッドを終了し、セッションに関連付けられているすべてのメソッドの詳細を削除します。
- **Deactivate** : セッションに適用されたサービステンプレートを削除します。適用されない場合、アクションは実行されません。
- **Set-timer** : タイマーを開始し、セッションに関連付けます。タイマーが期限切れになると、開始する必要があるアクションを処理できます。
- **Authentication-restart** : 認証を再開します。
- **Clear-session** : セッションを削除します。
- **Pause** : 認証を一時停止します。

残りのアクションについては説明の必要はなく、認証に関連したものです。

## 仮想ポート

仮想ポートは、1つの物理ポート上の複数のセキュアな接続アソシエーションに使用します。各接続アソシエーション（ペア）は仮想ポートを表します。スイッチ間では、物理ポートごとに1つの仮想ポートのみを指定できます。スイッチとホスト間では、物理ポートごとに最大2つの仮想ポートを指定でき、一方の仮想ポートはデータ VLAN の一部にできます。もう一方は音声 VLAN に対してパケットを外部的にタグ付けする必要があります。同じポートで同じ VLAN 内のセキュアなセッションとセキュアでないセッションを同時にホストすることはできません。この制限のため、802.1x マルチ認証モードはサポートされません。

この制限の例外は、マルチホストモードで最初の MACsec サプリカントが正常に認証され、スイッチに接続されたハブに接続される場合です。ハブに接続された非 MACsec ホストでは、マルチホストモードであるため、認証なしでトラフィックを送信できます。最初にクライアントが成功した後、他のクライアントでは認証が必要ないため、マルチホストモードの使用は推奨しません。

仮想ポートは、接続アソシエーションの任意の ID を表し、MKA プロトコル外では意味を持ちません。仮想ポートは個々の論理ポート ID に対応します。仮想ポートの有効なポート ID は

0x0002 ~ 0xFFFF です。各仮想ポートは、16 ビットのポート ID に連結された物理インターフェイスの MAC アドレスに基づいて、一意のセキュア チャネル ID (SCI) を受け取ります。

## MKA 統計情報

一部の MKA カウンタはグローバルに集約され、その他のカウンタはグローバルとセッション単位の両方で更新されます。また、MKA セッションのステータスに関する情報も取得できます。詳細については、例：MKA 情報の表示 (273 ページ) を参照してください。

## 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には、キーが期限切れになる時刻が指定されます。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る場合、ライフタイムの期限が切れた後に、MKA はキー チェーン内の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。デフォルトのタイムゾーンは UTC です。

キー チェーン内に 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、同じキーチェーン内の次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る場合、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。

すべての参加デバイスで、MACsec キーチェーンを Network Time Protocol (NTP) を使用して同期し、同じタイムゾーンを使用する必要があります。参加しているすべてのデバイスが同期されていない場合、接続アソシエーションキー (CAK) のキー再生成はすべてのデバイスで同時に開始されません。



(注) キーのライフタイムは、ヒットレス キー ロールオーバーを実現するためにオーバーラップする必要があります。

## リプレイ保護ウィンドウ サイズ

リプレイ保護は、リプレイ攻撃に対抗するために MACsec により提供される機能です。暗号化された各パケットには一意のシーケンス番号が割り当てられ、シーケンスはリモートエンドで確認されます。メトロイーサネット サービス プロバイダー ネットワークを介して送信されるフレームは、順序が変更されることが多くあります。これは、ネットワーク内で使用されている優先順位付けとロードバランシングのメカニズムによるものです。

フレームの順序が変更されるプロバイダー ネットワーク上で MACsec の使用をサポートするには、リプレイウィンドウが必要です。ウィンドウ内のフレームは順不同で受信できますが、リプレイ保護されません。デフォルトのウィンドウサイズは 0 で、厳密な受信順序が適用されません。リプレイウィンドウのサイズは、 $0 - 2^{32} - 1$  の範囲で設定できます。XPN 暗号スイートの場合、最大リプレイウィンドウサイズは  $2^{30} - 1$  で、より大きなウィンドウサイズが設定されて



いる場合、ウィンドウサイズは  $2^{30}-1$  に制限されます。暗号スイートが非 XPN 暗号スイートに変更された場合、制限はなく、設定されたウィンドウサイズが使用されます。

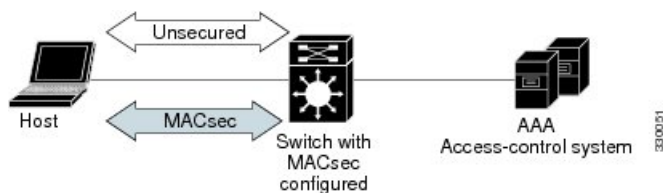
## MACsec、MKA、および 802.1x ホストモード

MACsec と MKA プロトコルは、802.1x シングルホストモード、マルチホストモード、またはマルチドメイン認証 (MDA) モードで使用できます。マルチ認証モードはサポートされません。

### シングルホストモード

次の図に、MKA を使用して、MACsec で 1 つの EAP 認証済みセッションをセキュアにする方法を示します。

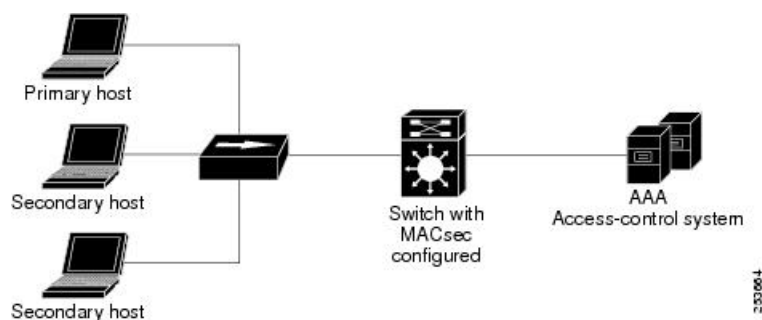
図 12: セキュアなデータセッションでのシングルホストモードの MACsec



### マルチホストモード

標準の (802.1x REV ではない) 802.1x マルチホストモードでは、1 つの認証に基づいてポートが開いているか、閉じられています。1 人のユーザー (プライマリセキュアクライアントサービスのクライアントホスト) が認証される場合は、同じポートに接続されているホストに同じレベルのネットワークアクセスが提供されます。セカンダリホストが MACsec サプリカントの場合、認証できず、トラフィックフローは発生しません。非 MACsec ホストであるセカンダリホストは、マルチホストモードであるため、認証なしでネットワークにトラフィックを送信できます。次の図に、標準のマルチホスト非セキュアモードにおける MACsec を示します。

図 13: マルチホストモードの MACsec: 非セキュア



(注) マルチホストモードは推奨されていません。これは最初にクライアントが成功した後、他のクライアントでは認証が必要ないことから、安全性が低いためです。

標準の（802.1x REV ではない）802.1x マルチドメインモードでは、1つの認証に基づいてポートが開いているか、閉じられています。プライマリユーザー（データドメインのPC）が認証されると、同じレベルのネットワークアクセスが同じポートに接続されているドメインに提供されます。セカンダリユーザーが MACsec サプリカントの場合、認証できず、トラフィックフローは発生しません。非MACsecホストであるセカンダリユーザー（音声ドメインのIPフォン）は、マルチドメインモードであるため、認証なしでネットワークにトラフィックを送信できます。

## マルチドメインモード

標準の（802.1x REV ではない）802.1x マルチドメインモードでは、1つの認証に基づいてポートが開いているか、閉じられています。プライマリユーザー（データドメインのPC）が認証されると、同じレベルのネットワークアクセスが同じポートに接続されているドメインに提供されます。セカンダリユーザーが MACsec サプリカントの場合、認証できず、トラフィックフローは発生しません。非MACsecホストであるセカンダリユーザー（音声ドメインのIPフォン）は、マルチドメインモードであるため、認証なしでネットワークにトラフィックを送信できます。

## 証明書ベースの MACsec 暗号化

証明書ベースの MACsec 暗号化を使用して、デバイスのスイッチ間ポート間で MACsec MKA を設定できます。証明書ベースの MACsec 暗号化は相互認証を許可し、MSK（マスターセッションキー）を取得します。そのキーから、MKA操作の接続アソシエーションキー（CAK）が取得されます。デバイスの証明書は、AAAサーバーへの認証用に、証明書ベースの MACsec 暗号化を使用して伝送されます。

## MACsec 暗号化の前提条件

### 証明書ベース MACsec の前提条件

- 認証局（CA）サーバーがネットワークに設定されていることを確認します。
- CA 証明書を生成します。
- Cisco Identity Services Engine（ISE）リリース 2.0 が設定されていることを確認します。
- 両方の参加デバイス（CAサーバーと Cisco Identity Services Engine（ISE））が Network Time Protocol（NTP）を使用して同期されていることを確認します。時間がすべてのデバイスで同期されていないと、証明書は検証されません。
- 802.1x 認証と AAA がデバイスに設定されていることを確認します。

## スイッチ間 MKA MACsec マストセキュアポリシー

Cisco IOS XE Fuji 16.8.1a 以降、入力と出力の両方で must-secure のサポートが有効になります。MKA および SAP では、Must-secure がサポートされています。must-secure を有効にすると、

EAPoL トラフィックのみが暗号化されません。他のトラフィックは暗号化されます。暗号化されないパケットはドロップされます。



(注) デフォルトでは、Must-secure モードが有効になっています。

Cisco IOS XE Fuji 16.8.1a よりも前のリリースでは、MKA と SAP で `should-secure` がサポートされていました。 `should-secure` を有効にすると、ピアが MACsec に設定されている場合はデータトラフィックが暗号化され、それ以外の場合はクリアテキストで送信されます。

## MACsec Extended Packet Numbering (XPN)

各 MACsec フレームには 32 ビットパケット番号 (PN) が含まれており、特定のセキュリティアソシエーションキー (SAK) に対して一意です。PN が枯渇すると ( $2^{31}-1$  の 75% に達した後)、SAK キーが再生成されてデータプレーンキーが更新されます。40 Gb/s などの高容量リンクの場合は数秒以内に PN が枯渇し、コントロールプレーンに対する SAK キーの頻繁な再生成が必要になります。XPN が使用されている場合、 $2^{63}-1$  の 75% に達した後、MACsec フレームの PN は 64 ビット値であるため、PN が枯渇するまで数年を要します。これにより、高速リンクで頻繁な SAK キー再生成が発生しなくなります。MKA/MACsec の XPN 機能により、大容量リンクで発生する可能性のある頻繁な SAK キー再生成が不要になります。XPN は、40 Gb/s、100 Gb/s などの高速リンクでの FIPS/CC コンプライアンスの必須要件です。



(注) MACsec XPN は、スイッチ間ポートでのみサポートされます。

XPN では次のキー再生成が可能です。

- **ボリュームベースのキー再生成**：頻繁な SAK キー再生成が発生しないようにするために、定義された MKA ポリシーの下で GCM-AES-XPN-128 または GCM-AES-XPN-256 暗号スイートを使用して XPN を設定できます。これらの暗号スイートを使用すると、1つの SAK で  $2^{32}$  以上のフレームを保護できます。XPN では、64 ビット値の PN がサポートされています。MACsec フレームには最下位 32 ビットのみが含まれ、最上位 32 ビットはピア自身、つまり送信側と受信側のピアの両方により維持されます。それぞれのピアの LAPN (許容される最小パケット番号) の MSB (最上位ビット) が設定され、MACsec フレームで受信した PN 値の MSB が 0 の場合、PN の最上位 32 ビットが受信側で増分されます。したがって、送信側と受信側の両方のピアが、MACsec フレーム構造を変更せずに同じ PN 値を維持します。
- **時間ベースのキー再生成**：SAK キー再生成を手動で設定するために、タイマーベースのキー再生成がサポートされており、指定された間隔で SAK キー再生成を開始することができます。インターフェイスに適用される定義済み MKA ポリシーの SAK キー再生成間隔を設定するには、MKA ポリシーコンフィギュレーションモードで `sak rekey interval time-interval` コマンドを使用します。

## ポートチャネルの MKA/MACsec

MKA/MACsec は、ポートチャネルのポートメンバで設定できます。ポートチャネルのポートメンバ間でMKAセッションが確立されるため、MKA/MACsecはポートチャネルに依存しません。



- (注) ポートチャネルの一部として形成される EtherChannel リンクは、合同または異種のいずれかです。つまり、リンクは MACsec セキュアまたは非 MACsec セキュアのいずれかになります。ポートチャネルの一方のポートメンバが MACsec に設定されていない場合でも、ポートメンバ間の MKA セッションが確立されます。

ポートチャネルのセキュリティを強化するために、すべてのメンバポートで MKA/MACsec を有効にすることをお勧めします。

## MACsec 暗号アナウンスメント

暗号アナウンスメントを使用すると、サブリカントとオーセンティケータは、それぞれの MACsec 暗号スイート機能を相互にアナウンスできます。サブリカントとオーセンティケータの両方が、サポートされる最大の共通 MACsec 暗号スイートを計算し、MKA セッションのキー情報と同じものを使用します。



- (注) MKA ポリシーで設定されている MACsec 暗号スイート機能だけが、オーセンティケータからサブリカントにアナウンスされます。

EAPOL アナウンスメントには 2 つのタイプがあります。

- 非セキュアアナウンスメント (EAPOL PDU) : 非セキュアアナウンスメントは、MACsec 暗号スイート機能を非セキュアな方法で伝送する EAPOL アナウンスメントです。これらのアナウンスメントは、認証の前に MKA セッションに使用するキーの幅を決定するために使用されます。
- セキュアアナウンスメント (MKPDU) : セキュアアナウンスメントは、以前は非セキュアアナウンスメントで共有されていた MACsec 暗号スイート機能を再検証します。

セッションが認証されると、EAPOL アナウンスメントを介して受信されたピア機能がセキュアアナウンスメントで再検証されます。機能に不一致がある場合、MKA セッションは切断されます。



- (注) サブリカントとオーセンティケータ間の MKA セッションは、両方に設定された MACsec 暗号スイート機能が共通の暗号スイートにならない場合でも切断されません。

## MACsec 暗号アナウンスメントに関する制約事項

- MACsec 暗号アナウンスメントは、スイッチからホストへのリンクでのみサポートされません。
- サプリカントとオーセンティケーター間の MKA セッションは、両方に設定された MACsec 暗号スイート機能が共通の暗号スイートにならない場合でも切断されません。

## MACsec 暗号化の設定方法

以降のセクションでは、MACsec 暗号化を構成するさまざまなタスクに関する情報を示します。

## MKA および MACsec の設定

デフォルトでは、MACsec は無効です。MKA ポリシーは設定されていません。

### MKA ポリシーの設定

MKA プロトコルポリシーを作成するには、特権 EXEC モードで次の手順を実行します。MKA では 802.1x をイネーブルにすることも必要であることに注意してください。

#### 手順の概要

1. **enable**
2. **configure terminal**
3. **mka policy *policy-name***
4. **key-server *priority***
5. **include-icv-indicator**
6. **macsec-cipher-suite {*gcm-aes-128* | *gcm-aes-256*}**
7. **confidentiality-offset *offset-value***
8. **ssci-based-on-sci**
9. **end**
10. **show mka policy**

#### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	<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
	Device# <b>configure terminal</b>	
ステップ 3	<b>mka policy</b> <i>policy-name</i> 例： Device(config)# <b>mka policy mka_policy</b>	MKA ポリシーを指定して、MKA ポリシーコンフィギュレーションモードを開始します。ポリシー名の長さは最大で 16 文字です。  (注) MKA ポリシー内のデフォルトの MACsec 暗号スイートは常に「GCM-AES-128」です。デバイスが「GCM-AES-128」および「GCM-AES-256」の両方の暗号方式をサポートしている場合は、ユーザー定義の MKA ポリシーを定義して使用し、必要に応じて、128 および 256 ビット両方の暗号を含めるか、または 256 ビットのみを含めることを強くお勧めします。
ステップ 4	<b>key-server priority</b> 例： Device(config-mka-policy)# <b>key-server priority 200</b>	MKA キーサーバオプションを設定し、優先順位を設定します (0 ~ 255 の値)。  (注) キーサーバプライオリティの値を 255 に設定した場合、ピアはキーサーバになることはできません。キーサーバの優先順位の値は MKA PSK に対してのみ有効です。MKA EAPTLS に対しては有効ではありません。
ステップ 5	<b>include-icv-indicator</b> 例： Device(config-mka-policy)# <b>include-icv-indicator</b>	MKPDU の ICV インジケータを有効にします。ICV インジケータを無効にするには、このコマンドの <b>no</b> 形式を使用します。
ステップ 6	<b>macsec-cipher-suite</b> { <i>gcm-aes-128</i>   <i>gcm-aes-256</i> } 例： Device(config-mka-policy)# <b>macsec-cipher-suite gcm-aes-128</b>	128 ビットまたは 256 ビット暗号化により SAK を取得するための暗号スイートを設定します。
ステップ 7	<b>confidentiality-offset</b> <i>offset-value</i> 例： Device(config-mka-policy)# <b>confidentiality-offset 0</b>	各物理インターフェイスに機密性 (暗号化) オフセットを設定します。  (注) オフセット値は、0、30、または 50 を指定できます。クライアントで Anyconnect を使用している場合は、オフセット 0 を使用することをお勧めします。

	コマンドまたはアクション	目的
ステップ 8	<b>ssci-based-on-sci</b> 例： Device(config-mka-policy) # <b>ssci-based-on-sci</b>	(任意) Secure Channel Identifier (SCI) 値に基づいて Short Secure Channel Identifier (SSCI) 値を計算します。SCI 値が高いほど、SSCI 値は低くなります。
ステップ 9	<b>end</b> 例： Device(config-mka-policy) # <b>end</b>	MKA ポリシー 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 10	<b>show mka policy</b> 例： Device# <b>show mka policy</b>	MKA ポリシー設定情報を表示します。

## スイッチからホストへの MACsec の暗号化設定

音声用に 1 つの MACsec セッションとデータ用に 1 つの MACsec セッションが存在するインターフェイスで MACsec を設定するには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **interface *type number***
4. **switchport access vlan *vlan-id***
5. **switchport mode access**
6. **macsec**
7. **authentication event linksec fail action authorize vlan *vlan-id***
8. **authentication host-mode multi-domain**
9. **authentication linksec policy must-secure**
10. **authentication port-control auto**
11. **authentication periodic**
12. **authentication timer reauthenticate**
13. **authentication violation protect**
14. **mka policy *policy-name***
15. **dot1x pae authenticator**
16. **spanning-tree portfast**
17. **end**
18. **show authentication session interface *interface-id* details**
19. **show macsec interface *interface-id***
20. **show mka sessions**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードをイネーブルにします。  • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	<b>configure terminal</b> 例： Device# <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 3	<b>interface type number</b> 例： Device(config)# <b>interface GigabitEthernet 1/0/1</b>	MACsec 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。インターフェイスは物理インターフェイスでなければなりません。
ステップ 4	<b>switchport access vlan vlan-id</b> 例： Device(config-if)# <b>switchport access vlan 1</b>	このポートのアクセス VLAN を設定します。
ステップ 5	<b>switchport mode access</b> 例： Device(config-if)# <b>switchport mode access</b>	インターフェイスをアクセス ポートとして設定します。
ステップ 6	<b>macsec</b> 例： Device(config-if)# <b>macsec</b>	インターフェイス上で 802.1ae MACsec をイネーブルにします。macsec コマンドを使用すると、スイッチからホストへのリンクでのみ MKA MACsec が有効になります。
ステップ 7	<b>authentication event linksec fail action authorize vlan vlan-id</b> 例： Device(config-if)# <b>authentication event linksec fail action authorize vlan 1</b>	(任意) 認証の試行に失敗した後で、ポート上の制限付き VLAN を許可することによって、ユーザー証明書が認識されない認証リンク セキュリティの問題をスイッチが処理することを指定します。
ステップ 8	<b>authentication host-mode multi-domain</b> 例： Device(config-if)# <b>authentication host-mode multi-domain</b>	ホストと音声デバイスの両方が、802.1x で許可されたポート上で認証されるように、ポート上の認証マネージャ モードを設定します。設定されていない場合、デフォルトのホストモードはシングルです。
ステップ 9	<b>authentication linksec policy must-secure</b> 例： Device(config-if)# <b>authentication linksec policy must-secure</b>	LinkSec セキュリティ ポリシーを設定して、ピアを利用できる場合に、MACsec でセッションをセキュアにします。設定されていない場合、デフォルト値は <i>should secure</i> です。



	コマンドまたはアクション	目的
ステップ 10	<b>authentication port-control auto</b> 例： Device(config-if)# <b>authentication port-control auto</b>	ポートでの 802.1x 認証をイネーブルにします。スイッチとクライアント間の認証交換に基づいてポートが許可ステートまたは無許可ステートに変わります。
ステップ 11	<b>authentication periodic</b> 例： Device(config-if)# <b>authentication periodic</b>	(任意) このポートの再認証を有効または無効にします。
ステップ 12	<b>authentication timer reauthenticate</b> 例： Device(config-if)# <b>authentication timer reauthenticate</b>	(任意) 1 から 65535 までの値 (秒) を入力します。サーバーから再認証タイムアウト値を取得します。デフォルトの再認証時間は 3600 秒です。
ステップ 13	<b>authentication violation protect</b> 例： Device(config-if)# <b>authentication violation protect</b>	新しいデバイスがポートに接続された場合、または最大数のデバイスがポートに接続された後に新しいデバイスがそのポートに接続された場合に、予期しない着信 MAC アドレスを破棄するようポートを設定します。設定されていない場合、デフォルトではポートをシャットダウンします。
ステップ 14	<b>mka policy policy-name</b> 例： Device(config-if)# <b>mka policy mka_policy</b>	既存の MKA プロトコル ポリシーをインターフェイスに適用し、インターフェイス上で MKA をイネーブルにします。MKA ポリシーを設定しなかった場合 ( <b>mka policy</b> グローバル コンフィギュレーション コマンドを入力して)。
ステップ 15	<b>dot1x pae authenticator</b> 例： Device(config-if)# <b>dot1x pae authenticator</b>	ポートを 802.1x ポートアクセスエンティティ (PAE) オーセンティケータとして設定します。
ステップ 16	<b>spanning-tree portfast</b> 例： Device(config-if)# <b>spanning-tree portfast</b>	関連するすべての VLAN 内のインターフェイスで、スパンニングツリー PortFast をイネーブルにします。PortFast 機能がイネーブルの場合、インターフェイスはブロッキングステートからフォワーディングステートに直接移行します。その際に、中間のスパンニングツリーステートは変わりません
ステップ 17	<b>end</b> 例： Device(config)# <b>end</b>	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、特権 EXEC 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 18	<b>show authentication session interface <i>interface-id</i> details</b>  例 : Device# <b>show authentication session interface GigabitEthernet 1/0/1</b>	許可されたセッションのセキュリティステータスの詳細を確認します。
ステップ 19	<b>show macsec interface <i>interface-id</i></b>  例 : Device# <b>show macsec interface GigabitEthernet 1/0/1</b>	インターフェイスの MACsec ステータスを確認します。
ステップ 20	<b>show mka sessions</b>  例 : Device# <b>show mka sessions</b>	確立された MKA セッションを確認します。

## PSK を使用した MKA MACsec の設定

### PSK を使用した MACsec MKA の設定

#### 手順の概要

1. **enable**
2. **configure terminal**
3. **key chain *key-chain-name* macsec**
4. **key *hex-string***
5. **cryptographic-algorithm {*aes-128-cmac* | *aes-256-cmac*}**
6. **key-string { [*0/6/7*] *pwd-string* | *pwd-string*}**
7. **lifetime local [*start timestamp* {*hh::mm::ss* | *day* | *month* | *year*}] [ **duration** *seconds* | *end timestamp* {*hh::mm::ss* | *day* | *month* | *year*}]**
8. **end**

#### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b>  例 : Device> <b>enable</b>	特権 EXEC モードを有効にします。  <ul style="list-style-type: none"> <li>• パスワードを入力します（要求された場合）。</li> </ul>
ステップ 2	<b>configure terminal</b>  例 : Device# <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。

	コマンドまたはアクション	目的
ステップ 3	<b>key chain</b> <i>key-chain-name</i> <b>macsec</b> 例： Device(config)# <b>key chain</b> <i>keychain1</i> <b>macsec</b>	キーチェーンを設定して、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 4	<b>key</b> <i>hex-string</i> 例： Device(config-key-chain)# <b>key</b> <i>1000</i>	キーチェーン内の各キーの固有識別子を設定し、キーチェーンのキーコンフィギュレーションモードを開始します。  (注) 128ビット暗号化の場合は、1～32文字の16進数キー文字列を使用します。256ビット暗号化の場合は、64文字の16進数キー文字列を使用します。
ステップ 5	<b>cryptographic-algorithm</b> { <i>aes-128-cmac</i> / <i>aes-256-cmac</i> } 例： Device(config-key-chain)# <b>cryptographic-algorithm</b> <i>aes-128-cmac</i>	128ビットまたは256ビット暗号による暗号化認証アルゴリズムを設定します。
ステップ 6	<b>key-string</b> { [0/6/7] <i>pwd-string</i> / <i>pwd-string</i> } 例： Device(config-key-chain)# <b>key-string</b> <i>12345678901234567890123456789012</i>	キー文字列のパスワードを設定します。16進数の文字のみを入力する必要があります。
ステップ 7	<b>lifetime local</b> [ <i>start timestamp {hh::mm::ss / day / month / year}</i> ] [ <b>duration</b> <i>seconds</i>   <i>end timestamp {hh::mm::ss / day / month / year}</i> ] 例： Device(config-key-chain)# <b>lifetime local</b> <i>12:12:00 July 28 2016 12:19:00 July 28 2016</i>	事前共有キーの有効期間を設定します。
ステップ 8	<b>end</b> 例： Device(config-key-chain)# <b>end</b>	キーチェーンコンフィギュレーションモードを終了して、特権 EXEC モードに戻ります。

## PSK を使用した、インターフェイスでの MACsec MKA の設定

### 手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **macsec network-link**
5. **mka policy** *policy-name*
6. **mka pre-shared-key** *key-chain key-chain name*

7. `macsec replay-protection window-size frame number`
8. `end`

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： Device# <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 3	<b>interface type number</b> 例： Device(config-if)# <b>interface GigabitEthernet 0/0/0</b>	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>macsec network-link</b> 例： Device(config-if)# <b>macsec network-link</b>	インターフェイス上で MACsec をイネーブルにします。
ステップ 5	<b>mka policy policy-name</b> 例： Device(config-if)# <b>mka policy mka_policy</b>	MKA ポリシーを設定します。
ステップ 6	<b>mka pre-shared-key key-chain key-chain name</b> 例： Device(config-if)# <b>mka pre-shared-key key-chain key-chain-name</b>	MKA 事前共有キーのキーチェーン名を設定します。
ステップ 7	<b>macsec replay-protection window-size frame number</b> 例： Device(config-if)# <b>macsec replay-protection window-size 10</b>	リプレイ保護の MACsec ウィンドウサイズを設定します。
ステップ 8	<b>end</b> 例： Device(config-if)# <b>end</b>	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、特権 EXEC モードに戻ります。

## 次のタスク

セッションの実行中に MKA PSK が設定されたインターフェイスで MKA ポリシーを変更することは推奨されません。ただし、変更が必要な場合は、次のようにポリシーを再設定する必要があります。

1. **no macsec network-link** コマンドを使用して、各参加ノードの **macsec network-link** 設定を削除し、既存のセッションを無効にします。
2. **mka policy policy-name** コマンドを使用して、各参加ノードのインターフェイスで MKA ポリシーを設定します。
3. **macsec network-link** コマンドを使用して、各参加ノードで新しいセッションを有効にします。

## 証明書ベース MACsec 暗号化の設定

ポイントツーポイントリンクで MKA による MACsec を設定するには、次のタスクを実行します。

- 証明書登録の設定
  - キー ペアの生成
  - SCEP 登録の設定
  - 証明書の手動設定
- 認証ポリシーの設定
- 証明書ベース MACsec 暗号化プロファイルと IEEE 802.1x ログイン情報の設定
- インターフェイスで証明書ベース MACsec 暗号化を使用する MACsec MKA の設定

## キー ペアの生成

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： Device# <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 3	<b>crypto key generate rsa label label-name general-keys modulus size</b> 例： Device(config)# <b>crypto key generate rsa label general-keys modulus 2048</b>	署名および暗号化用に RSA キーペアを作成します。 <b>label</b> キーワードを使用すると、各キーペアにラベルを割り当てることもできます。このラベルは、キーペアを使用するトラストポイントによって参照されます。ラベルを割り当てなかった場合、キーペアに

	コマンドまたはアクション	目的
		<p>は &lt;Default-RSA-Key&gt; というラベルが自動的に付けられます。</p> <p>追加のキーワードを使用しない場合、このコマンドは汎用 RSA キーペアを 1 つ生成します。係数が指定されていない場合は、デフォルトのキー係数である 1024 が使用されます。その他の係数サイズを指定するには、<code>modulus</code> キーワードを使用します。</p>
ステップ 4	<b>end</b> 例： Device(config)# <b>end</b>	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 5	<b>show authentication session interface interface-id</b> 例： Device# <b>show authentication session interface gigabitethernet 0/1/1</b>	許可されたセッションのセキュリティステータスを確認します。

## SCEP による登録の設定

Simple Certificate Enrollment Protocol (SCEP) は、HTTP を使用して認証局 (CA) または登録局 (RA) と通信する、シスコが開発した登録プロトコルです。SCEP は、要求および証明書の送受信に最も一般的に使用される方式です。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>パスワードを入力します (要求された場合)。</li> </ul>
ステップ 2	<b>configure terminal</b> 例： Device# <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 3	<b>crypto pki trustpoint server name</b> 例： Device(config)# <b>crypto pki trustpoint ka</b>	トラストポイントおよび設定された名前を宣言して、CA 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 4	<b>enrollment url url name pem</b> 例： Device(ca-trustpoint)# <b>enrollment url http://url:80</b>	デバイスが証明書要求を送信する CA の URL を指定します。  URL 内の IPv6 アドレスは括弧で囲む必要があります。たとえば、 <code>http://[2001:DB8:1:1::1]:80</code> です。

	コマンドまたはアクション	目的
		pem キーワードは、証明書要求に Privacy Enhanced Mail (PEM) の境界を追加します。
ステップ 5	<b>rsa-keypair label</b> 例： Device(ca-trustpoint)# <b>rsa-keypair exampleCAkeys</b>	証明書に関連付けるキー ペアを指定します。  (注) <b>rsa-keypair</b> 名は、信頼ポイント名と一致している必要があります。
ステップ 6	<b>serial-number none</b> 例： Device(ca-trustpoint)# <b>serial-number none</b>	<b>none</b> キーワードは、証明書要求にシリアル番号が含まれないことを指定します。
ステップ 7	<b>ip-address none</b> 例： Device(ca-trustpoint)# <b>ip-address none</b>	<b>none</b> キーワードは、証明書要求に IP アドレスが含まれないことを指定します。
ステップ 8	<b>revocation-check crl</b> 例： Device(ca-trustpoint)# <b>revocation-check crl</b>	ピアの証明書が取り消されていないことを確認する方法として CRL を指定します。
ステップ 9	<b>auto-enroll percent regenerate</b> 例： Device(ca-trustpoint)# <b>auto-enroll 90 regenerate</b>	自動登録をイネーブルにします。これにより、クライアントは CA から自動的にロールオーバー証明書を要求できます。  自動登録がイネーブルでない場合、証明書の失効時にクライアントを手動で PKI に再登録する必要があります。  デフォルトでは、デバイスのドメイン ネーム システム (DNS) 名だけが証明書に含められます。  現行の証明書の有効期間が指定のパーセンテージに達したときに、新しい証明書が要求されるように指定するには、percent 引数を使用します。  名前付きのキーがすでに存在する場合でも、証明書の新しいキーを生成するには、regenerate キーワードを使用します。  ロールオーバー中のキー ペアがエクスポート可能な場合、新しいキーペアもエクスポート可能です。次のコメントがトラストポイントコンフィギュレーションに表示され、キー ペアがエクスポート可能かどうかを示されます。「! RSA key pair associated with trustpoint is exportable.」  新しいキー ペアは、セキュリティ上の問題に対処するために生成することを推奨します。

	コマンドまたはアクション	目的
ステップ 10	<b>exit</b> 例： Device(ca-trustpoint)# <b>exit</b>	CA 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、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 11	<b>crypto pki authenticate name</b> 例： Device(config)# <b>crypto pki authenticate myca</b>	CA 証明書を取得して、認証します。
ステップ 12	<b>end</b> 例： Device(config)# <b>end</b>	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 13	<b>show crypto pki certificate trustpoint name</b> 例： Device# <b>show crypto pki certificate ka</b>	信頼ポイントの証明書に関する情報を表示します。

## 登録の手動設定

CA が SCEP をサポートしない場合、またはルータと CA 間のネットワーク接続が不可能な場合。手動での証明書登録を設定するには、次の作業を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"><li>パスワードを入力します（要求された場合）。</li></ul>
ステップ 2	<b>configure terminal</b> 例： Device# <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 3	<b>crypto pki trustpoint server name</b> 例： Device# <b>crypto pki trustpoint ka</b>	トラストポイントおよび設定された名前を宣言して、CA 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 4	<b>enrollment url url-name</b> 例： Device(ca-trustpoint)# <b>enrollment url http://url:80</b>	デバイスが証明書要求を送信する CA の URL を指定します。  URL 内の IPv6 アドレスは括弧で囲む必要があります。たとえば、 <code>http://[2001:DB8:1:1::1]:80</code> です。  <code>pem</code> キーワードは、証明書要求に Privacy Enhanced Mail (PEM) の境界を追加します。



	コマンドまたはアクション	目的
ステップ 5	<b>rsa keypair label</b> 例： Device(ca-trustpoint)# <b>rsa keypair exampleCAkeys</b>	証明書に関連付けるキー ペアを指定します。
ステップ 6	<b>serial-number none</b> 例： Device(ca-trustpoint)# <b>serial-number none</b>	証明書要求にシリアル番号が含まれないことを指定します。
ステップ 7	<b>ip-address none</b> 例： Device(ca-trustpoint)# <b>ip-address none</b>	<b>none</b> キーワードは、証明書要求に IP アドレスが含まれないことを指定します。
ステップ 8	<b>revocation-check crl</b> 例： Device(ca-trustpoint)# <b>revocation-check crl</b>	ピアの証明書が取り消されていないことを確認する方法として CRL を指定します。
ステップ 9	<b>exit</b> 例： Device(ca-trustpoint)# <b>exit</b>	CA 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、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>crypto pki authenticate name</b> 例： Device(config)# <b>crypto pki authenticate myca</b>	CA 証明書を取得して、認証します。
ステップ 11	<b>crypto pki enroll name</b> 例： Device(config)# <b>crypto pki enroll myca</b>	証明書要求を生成し、証明書サーバーにコピーおよびペーストするために要求を表示します。  プロンプトが表示されたら、登録情報を入力します。たとえば、証明書要求にデバイスの FQDN および IP アドレスを含めるかどうかを指定します。  コンソール端末に対して証明書要求を表示するかについても選択できます。  必要に応じて、Base 64 符号化証明書を PEM ヘッダーを付けて、または付けずに表示します。
ステップ 12	<b>crypto pki import name certificate</b> 例： Device(config)# <b>crypto pki import myca certificate</b>	許可された証明書を取得するコンソール端末で、TFTP によって証明書をインポートします。  デバイスは、拡張子が「.req」から「.crt」に変更されたことを除いて、要求の送信に使用した同じファイル名を使用して、許可された証明書を TFTP によって取得しようと試みます。用途キー証明書の場 合、拡張子「-sign.crt」および「-encr.crt」が使用されます。

	コマンドまたはアクション	目的
		<p>デバイスは、受信したファイルを解析して証明書を検証し、証明書をスイッチの内部証明書データベースに挿入します。</p> <p>(注) 一部の CA は、証明書要求の用途キー情報を無視し、汎用目的の証明書を発行します。ご使用の CA が証明書要求の用途キー情報を無視する場合は、汎用目的の証明書だけをインポートしてください。ルータは、生成される2つのキーペアのいずれも使用しません。</p>
ステップ 13	<b>end</b> 例： Device(config)# <b>end</b>	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 14	<b>show crypto pki certificate trustpoint name</b> 例： Device# <b>show crypto pki certificate ka</b>	信頼ポイントの証明書に関する情報を表示します。

## スイッチ間の MACsec の暗号化設定

証明書ベース MACsec 暗号化を使用して MKA MACsec をインターフェイスに適用するには、次のタスクを実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>パスワードを入力します（要求された場合）。</li> </ul>
ステップ 2	<b>configure terminal</b> 例： Device# <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 3	<b>interface type number</b> 例： Device(config)# <b>interface gigabitethernet 0/2/1</b>	MACsec 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。インターフェイスは物理インターフェイスでなければなりません。
ステップ 4	<b>macsec network-link</b> 例：	インターフェイス上で MACsec をイネーブルにします。

	コマンドまたはアクション	目的
	Device (config-if) # <b>macsec network-link</b>	
ステップ 5	<b>authentication periodic</b> 例 : Device (config-if) # <b>authentication periodic</b>	このポートの再認証をイネーブルにします。
ステップ 6	<b>authentication timer reauthenticate interval</b> 例 : Device (config-if) # <b>authentication timer reauthenticate interval</b>	再認証間隔を設定します。
ステップ 7	<b>access-session host-mode multi-host</b> 例 : Device (config-if) # <b>access-session host-mode multi-host</b>	ホストにインターフェイスへのアクセスを許可します。
ステップ 8	<b>access-session closed</b> 例 : Device (config-if) # <b>access-session closed</b>	インターフェイスへの事前認証アクセスを防止します。
ステップ 9	<b>access-session port-control auto</b> 例 : Device (config-if) # <b>access-session port-control auto</b>	ポートの認可状態を設定します。
ステップ 10	<b>dot1x pae both</b> 例 : Device (config-if) # <b>dot1x pae both</b>	ポートを 802.1X ポート アクセス エンティティ (PAE) のサブリカントおよびオーセンティケータとして設定します。
ステップ 11	<b>dot1x credentials profile</b> 例 : Device (config-if) # <b>dot1x credentials profile</b>	802.1x クレデンシャルプロファイルをインターフェイスに割り当てます。
ステップ 12	<b>end</b> 例 : Device (config-if) # <b>end</b>	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、特権 EXEC モードに戻ります。
ステップ 13	<b>show macsec interface interface-id</b> 例 : Device# <b>show macsec interface GigabitEthernet 1/0/1</b>	インターフェイスの MACsec の詳細を表示します。

## MACsec XPN の設定

### XPN の MKA ポリシーの設定

MKA ポリシーで XPN を設定するには、次の手順を実行します。

#### 手順の概要

1. **enable**
2. **configure terminal**
3. **mka policy *policy-name***
4. **macsec-cipher-suite { *gcm-aes-128* | *gcm-aes-256* | *gcm-aes-xpn-128* | *gcm-aes-xpn-256* }**
5. **sak-rekey interval *time-interval***
6. **end**

#### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例： Device# <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 3	<b>mka policy <i>policy-name</i></b> 例： Device(config)# <b>mka policy <i>mka_policy</i></b>	MKA ポリシーを指定して、MKA ポリシーコンフィギュレーションモードを開始します。ポリシー名の長さは最大で 16 文字です。  (注) MKA ポリシー内のデフォルトの MACsec 暗号スイートは常に「GCM-AES-128」です。デバイスが「GCM-AES-128」および「GCM-AES-256」の両方の暗号方式をサポートしている場合は、ユーザー定義の MKA ポリシーを定義して使用し、必要に応じて、128 および 256 ビット両方の暗号を含めるか、または 256 ビットのみを含めることを強くお勧めします。
ステップ 4	<b>macsec-cipher-suite { <i>gcm-aes-128</i>   <i>gcm-aes-256</i>   <i>gcm-aes-xpn-128</i>   <i>gcm-aes-xpn-256</i> }</b> 例：	XPN 用の 128 ビットおよび 256 ビット暗号により SAK を取得するための暗号スイートを設定します。

	コマンドまたはアクション	目的
	Device (config-mka-policy) # <b>macsec-cipher-suite gcm-aes-xpn-256</b>	
ステップ 5	<b>sak-rekey interval time-interval</b> 例 : Device (config-mka-policy) # <b>sak-rekey interval 50</b>	(任意) SAK キー再生成間隔を秒単位で設定します。範囲は 30 ~ 65535 です。デフォルトでは、SAK キー再生成間隔は、インターフェイス速度に応じて自動的に発生します。  SAK キー再生成タイマーを停止するには、このコマンドの <b>no</b> 形式を使用します。
ステップ 6	<b>end</b> 例 : Device (config-mka-policy) # <b>end</b>	MKA ポリシー 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。

## XPN MKA ポリシーをインターフェイスに適用する

XPN MKA ポリシーをインターフェイスに適用するには、次のタスクを実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します (要求された場合)。
ステップ 2	<b>configure terminal</b> 例 : Device# <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 3	<b>interface interface-name</b> 例 : Device (config) # <b>interface gigabitethernet 1/0/1</b>	MACsec 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。インターフェイスは物理インターフェイスでなければなりません。
ステップ 4	<b>mka policy policy-name</b> 例 : Device (config-if) # <b>mka policy mka-xpn-policy</b>	XPNMKA プロトコルポリシーをインターフェイスに適用します。
ステップ 5	<b>end</b> 例 : Device (config-if) # <b>end</b>	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、特権 EXEC モードに戻ります。

## ポートチャネル用の MKA/MACsec の設定

### PSK を使用したポートチャネルの MKA/MACsec の設定

#### 手順の概要

1. **enable**
2. **configure terminal**
3. **interface *interface-id***
4. **macsec network-link**
5. **mka policy *policy-name***
6. **mka pre-shared-key key-chain *key-chain-name***
7. **macsec replay-protection window-size *frame number***
8. **channel-group *channel-group-number* mode {auto | desirable} | {active | passive} | {on}**
9. **end**

#### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： Device# <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 3	<b>interface <i>interface-id</i></b> 例： Device(config-if)# <b>interface gigabitethernet 1/0/3</b>	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>macsec network-link</b> 例： Device(config-if)# <b>macsec network-link</b>	インターフェイス上で MACsec をイネーブルにします。レイヤ 2 およびレイヤ 3 ポートチャネルをサポートします。
ステップ 5	<b>mka policy <i>policy-name</i></b> 例： Device(config-if)# <b>mka policy mka_policy</b>	MKA ポリシーを設定します。
ステップ 6	<b>mka pre-shared-key key-chain <i>key-chain-name</i></b> 例： Device(config-if)# <b>mka pre-shared-key key-chain key-chain-name</b>	MKA 事前共有キーのキーチェーン名を設定します。  (注) MKA 事前共有キーは、物理インターフェイスまたはサブインターフェイスで設定できますが、両方で設定することはできません。

	コマンドまたはアクション	目的
ステップ 7	<b>macsec replay-protection window-size</b> <i>frame number</i> 例 : Device(config-if)# <b>macsec replay-protection window-size 0</b>	リプレイ保護の MACsec ウィンドウサイズを設定します。
ステップ 8	<b>channel-group</b> <i>channel-group-number</i> <b>mode</b> { <b>auto</b>   <b>desirable</b> }   { <b>active</b>   <b>passive</b> }   { <b>on</b> } 例 : Device(config-if)# <b>channel-group 3 mode auto active on</b>	チャンネルグループ内にポートを設定し、モードを設定します。 (注) インターフェイスで MACsec を設定しないと、チャンネルグループのポートを設定できません。このステップの前に、ステップ 3、4、5、および 6 のコマンドを設定する必要があります。 channel-number の指定できる範囲は 1 ~ 4096 です。ポートチャネルがない場合は、このチャンネルグループに関連付けられたポートチャネルが自動的に作成されます。モードは、以下のキーワードのいずれかを選択します。 <ul style="list-style-type: none"> <li>• <b>auto</b> : PAgP デバイスが検出された場合に限り、PAgP を有効にします。ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する PAgP パケットに応答しますが、PAgP パケットネゴシエーションを開始することはありません。                (注) EtherChannel メンバが、スイッチスタックにある異なるスイッチのメンバである場合、<b>auto</b> キーワードはサポートされません。</li> <li>• <b>desirable</b> : 無条件に PAgP を有効にします。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは PAgP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。                (注) EtherChannel メンバが、スイッチスタックにある異なるスイッチのメンバである場合、<b>desirable</b> キーワードはサポートされません。</li> <li>• <b>on</b> : PAgP または LACP を使用せずにポートが強制的にチャンネル化されます。on モードでは、EtherChannel が存在するのは、on モードのポー</li> </ul>

	コマンドまたはアクション	目的
		<p>トグループが、<b>on</b> モードの別のポートグループに接続する場合だけです。</p> <ul style="list-style-type: none"> <li>• <b>active</b> : LACP デバイスが検出された場合に限り、LACP を有効にします。ポートをアクティブ ネゴシエーション ステートにします。この場合、ポートは LACP パケットを送信することによって、相手ポートとのネゴシエーションを開始します。</li> <li>• <b>passive</b> : ポート上で LACP を有効にして、ポートをパッシブ ネゴシエーション ステートにします。この場合、ポートは受信する LACP パケットに応答しますが、LACP パケットネゴシエーションを開始することはありません。</li> </ul>
ステップ 9	<b>end</b> 例 : Device(config-if)# <b>end</b>	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、特権 EXEC モードに戻ります。

## レイヤ 2 EtherChannel のポートチャネル論理インターフェイスの設定

レイヤ 2 EtherChannel 用のポートチャネルインターフェイスを作成するには、次の作業を行います。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **interface port-channel** *channel-group-number*
4. **switchport**
5. **switchport mode** {**access** | **trunk**}
6. **end**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device> <b>enable</b>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>• パスワードを入力します（要求された場合）。</li> </ul>
ステップ 2	<b>configure terminal</b> 例 : Device# <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。



	コマンドまたはアクション	目的
ステップ 3	<b>interface port-channel</b> <i>channel-group-number</i> 例： Device(config)# <b>interface port-channel 1</b>	ポート チャネル インターフェイスを作成し、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。  (注) ポート チャネル インターフェイスを削除するには、このコマンドの <b>no</b> 形式を使用します。
ステップ 4	<b>switchport</b> 例： Device(config-if) # <b>switchport</b>	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 設定のレイヤ 2 モードに切り替えます。
ステップ 5	<b>switchport mode</b> { <b>access</b>   <b>trunk</b> } 例： Device(config-if) # <b>switchport mode access</b>	すべてのポートをスタティックアクセスポートとして同じ VLAN に割り当てるか、またはトランクとして設定します。
ステップ 6	<b>end</b> 例： Device(config-if) # <b>end</b>	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、特権 EXEC モードに戻ります。

## レイヤ 3 EtherChannel のポートチャネル論理インターフェイスの設定

レイヤ 3 EtherChannel 用のポート チャネルインターフェイスを作成するには、次の作業を行います。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **no switchport**
5. **ip address** *ip-address subnet-mask*
6. **end**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<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
	Device# <b>configure terminal</b>	
ステップ 3	<b>interface</b> <i>interface-id</i> 例 : Device(config)# <b>interface</b> <b>gigabitethernet</b> 1/0/2	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 switchport</b> 例 : Device(config-if)# <b>no switchport</b>	レイヤ 2 モードになっているインターフェイスを、レイヤ 3 設定用にレイヤ 3 モードに切り替えます。
ステップ 5	<b>ip address</b> <i>ip-address subnet-mask</i> 例 : Device(config-if)# <b>ip address</b> 10.2.2.3 255.255.255.254	EtherChannel に IP アドレスおよびサブネットマスクを割り当てます。
ステップ 6	<b>end</b> 例 : Device(config-if)# <b>end</b>	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、特権 EXEC モードに戻ります。

## MACsec 暗号アナウンスメントの設定

以降のセクションでは、MACsec 暗号アナウンスを設定するためのさまざまなタスクに関する情報を示します。

### セキュアアナウンスメントの MKA ポリシーの設定

MKA プロトコルポリシーを作成して MKPDU でセキュアアナウンスメントを有効にするには、特権 EXEC モードで次の手順を実行します。デフォルトでは、セキュアアナウンスメントは無効になっています。

#### 手順の概要

1. **enable**
2. **configure terminal**
3. **mka policy** *policy-name*
4. **key-server** *priority*
5. **send-secure-announcements**
6. **macsec-cipher-suite** {*gcm-aes-128* | *gcm-aes-256*}
7. **end**
8. **show mka policy**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例： Device# <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 3	<b>mka policy <i>policy-name</i></b> 例： Device(config)# <b>mka policy mka_policy</b>	MKA ポリシーを指定して、MKA ポリシー コンフィギュレーション モードを開始します。ポリシー名の長さは最大で 16 文字です。  (注) MKA ポリシーのデフォルトの MACsec 暗号スイートは GCM-AES-128 です。デバイスが GCM-AES-128 および GCM-AES-256 の両方の暗号方式をサポートしている場合は、ユーザー定義の MKA ポリシーを定義して使用し、必要に応じて、128 および 256 ビット両方の暗号を含めるか、または 256 ビットの暗号のみを含めることを推奨します。
ステップ 4	<b>key-server <i>priority</i></b> 例： Device(config-mka-policy)# <b>key-server priority 200</b>	MKA キーサーバー オプションを設定し、0～255 の間で優先順位を設定します。  (注) キーサーバーの優先順位の値を 255 に設定した場合、ピアはキーサーバーになることはできません。キーサーバーの優先順位の値は MKA PSK に対してのみ有効です。これは MKA EAP-TLS には適用されません。
ステップ 5	<b>send-secure-announcements</b> 例： Device(config-mka-policy)# <b>send-secure-announcements</b>	セキュアアナウンスメントの送信を有効にします。セキュアアナウンスメントの送信を無効にするには、このコマンドの <b>no</b> 形式を使用します。デフォルトでは、セキュアアナウンスメントは無効になっています。
ステップ 6	<b>macsec-cipher-suite {<i>gcm-aes-128</i>   <i>gcm-aes-256</i>}</b> 例： Device(config-mka-policy)# <b>macsec-cipher-suite gcm-aes-128</b>	128 ビットまたは 256 ビット暗号化により SAK を取得するための暗号スイートを設定します。

	コマンドまたはアクション	目的
ステップ 7	<b>end</b> 例： Device (config-mka-policy) # <b>end</b>	MKA ポリシー 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 8	<b>show mka policy</b> 例： Device# <b>show mka policy</b>	MKA ポリシーを表示します。

## セキュアアナウンスメントのグローバル設定

特権 EXEC モードから始めて、次の手順に従って、すべての MKA ポリシーにわたって安全なアナウンスメントをグローバルに有効にします。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **mka defaults policy send-secure-announcements**
4. **end**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例： Device# <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 3	<b>mka defaults policy send-secure-announcements</b> 例： Device (config) # <b>mka defaults policy send-secure-announcements</b>	MKA ポリシーを介した MKPDU でのセキュアアナウンスメントの送信を有効にします。デフォルトでは、セキュアアナウンスメントは無効になっています。
ステップ 4	<b>end</b> 例： Device (config) # <b>end</b>	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。

## インターフェイスでの EAPOL アナウンスメントの設定

インターフェイスで EAPOL アナウンスメントを設定するには、特権 EXEC モードで開始し、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **interface *interface-id***
4. **eapol announcement**
5. **end**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例： Device# <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 3	<b>interface <i>interface-id</i></b> 例： Device(config)# <b>interface gigabitethernet 1/0/1</b>	MACsec 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。インターフェイスは物理インターフェイスでなければなりません。
ステップ 4	<b>eapol announcement</b> 例： Device(config-if)# <b>eapol announcement</b>	EAPOL アナウンスメントを有効にします。EAPOL アナウンスメントを無効にするには、コマンドの <b>no</b> 形式を使用します。デフォルトでは、EAPOL アナウンスメントは無効になっています。
ステップ 5	<b>end</b> 例： Device(config-if)# <b>configure terminal</b>	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、特権 EXEC モードに戻ります。

# Cisco TrustSec MACsec の設定

## 手動モードでの Cisco TrustSec スイッチ間リンク セキュリティの設定

### 始める前に

インターフェイスの Cisco TrustSec を手動で設定する場合は、次のような使用上の注意事項、および制約事項を考慮してください。

- SAP パラメータが定義されていない場合、Cisco TrustSec カプセル化または暗号化は行われません。
- SAP 動作モードとして GCM を選択すると、シスコの MACsec 暗号化ソフトウェアライセンスが必要です。必要なライセンスなしで GCM を選択した場合、インターフェイスはリンク ダウン状態になります。
- これらの保護レベルは、SAP の Pairwise Master Key (sap pmk) を設定する場合にサポートされます。
  - SAP が設定されていない：保護は行われません。
  - **sap mode-list gcm-encrypt gmac no-encap**：保護が望ましいが必須ではない。
  - **sap mode-list gcm-encrypt gmac**：機密性が推奨され、完全性は必須。保護はサブリカントの設定に応じてサブリカントによって選択されます。
  - **sap mode-list gmac**：完全性のみ。
  - **sap mode-list gcm-encrypt**：機密性が必須。
  - **sap mode-list gmac gcm-encrypt**：完全性が必須であり推奨される。機密性は任意。
- MKA から Cisco TrustSec SAP (またはその逆) に設定を変更する前に、インターフェイスの設定を削除することを推奨します。

別の Cisco TrustSec デバイスへのインターフェイスで Cisco TrustSec を手動で設定するには、特権 EXEC モードで次の手順を実行します。

### 手順の概要

1. **configure terminal**
2. **interface *interface-id***
3. **cts manual**
4. **sap pmk key [mode-list *mode1* [*mode2* [*mode3* [*mode4*]]]]**
5. **no propagate sgt**
6. **exit**
7. **end**
8. **show cts interface [*interface-id* | **brief** | **summary**]**
9. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： Device# <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>interface interface-id</b> 例： Device(config)# <b>interface tengigabitethernet 1/1/2</b>	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<b>cts manual</b> 例： Device(config-if)# <b>cts manual</b>	Cisco TrustSec 手動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>sap pmk key [mode-list mode1 [mode2 [mode3 [mode4]]]]</b> 例： Device(config-if-cts-manual)# <b>sap pmk 1234abcdef mode-list gcm-encrypt no-encap</b>	<p>(任意) SAP の Pairwise Master Key (PMK) と動作モードを設定します。Cisco TrustSec の手動モードでは、SAP はデフォルトでディセーブルになっています。</p> <ul style="list-style-type: none"> <li>• <b>key</b> : 文字数が偶数個で最大 32 文字の 16 進値。</li> </ul> <p>SAP 動作モードのオプションは次のとおりです。</p> <ul style="list-style-type: none"> <li>• <b>gcm-encrypt</b> : 認証および暗号化 <ul style="list-style-type: none"> <li>(注) ソフトウェアライセンスが MACsec 暗号化をサポートする場合、MACsec の認証と暗号化にこのモードを選択します。</li> </ul> </li> <li>• <b>gmac</b> : 認証、暗号化なし</li> <li>• <b>no-encap</b> : カプセル化なし</li> </ul>
ステップ 5	<b>no propagate sgt</b> 例： Device(config-if-cts-manual)# <b>no propagate sgt</b>	ピアが SGT を処理できない場合、このコマンドの <b>no</b> 形式を使用します。 <b>no propagate sgt</b> コマンドを使用すると、インターフェイスからピアに SGT が送信されなくなります。
ステップ 6	<b>exit</b> 例： Device(config-if-cts-manual)# <b>exit</b>	Cisco TrustSec 802.1x 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	<b>end</b> 例： Device(config-if)# <b>end</b>	特権 EXEC 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 8	<code>show cts interface [interface-id   brief   summary]</code>	(任意) TrustSec 関連のインターフェイス特性を表示して、設定を確認します。
ステップ 9	<code>copy running-config startup-config</code> 例 : Device# <code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

## MACsec 暗号化の設定例

以降のセクションでは、MACsec 暗号化の設定例を示します。

### 例 : MKA および MACsec の設定

次に、MKA ポリシーを作成する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# mka policy mka_policy
Device(config-mka-policy)# key-server priority 200
Device(config-mka-policy)# macsec-cipher-suite gcm-aes-128
Device(config-mka-policy)# confidentiality-offset 30
Device(config-mka-policy)# ssci-based-on-sci
Device(config-mka-policy)#end
```

次は、インターフェイスに MACsec を設定する例です。

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# switchport access vlan 1
Device(config-if)# switchport mode access
Device(config-if)# macsec
Device(config-if)# authentication event linksec fail action authorize vlan 1
Device(config-if)# authentication host-mode multi-domain
Device(config-if)# authentication linksec policy must-secure
Device(config-if)# authentication port-control auto
Device(config-if)# authentication periodic
Device(config-if)# authentication timer reauthenticate
Device(config-if)# authentication violation protect
Device(config-if)# mka policy mka_policy
Device(config-if)# dot1x pae authenticator
Device(config-if)# spanning-tree portfast
Device(config-if)# end
```

### 例 : PSK を使用した MACsec MKA の設定

次に、PSK を使用して、MKA MACsec を設定する例を示します。

```
Device> enable
Device# configure terminal
```



```
Device(config)# key chain keychain1 macsec
Device(config-keychain)# key 1000
Device(config-keychain-key)# cryptographic-algorithm aes-128-cmac
Device(config-keychain-key)# key-string 12345678901234567890123456789012
Device(config-keychain-key)# lifetime local 12:12:00 July 28 2016 12:19:00 July 28 2016
Device(config-keychain-key)# end
```

次に、PSK を使用して、インターフェイスに MACsec MKA を設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# mka policy mka_policy
Device(config-if)# mka pre-shared-key key-chain key-chain-name
Device(config-if)# macsec replay-protection window-size 10
Device(config-if)# end
```

### MKA-PSK : CKN 動作の変更

Cisco IOS XE Fuji 16.8.1 リリース以降、MKA PSK セッションの場合、CKN は、固定の 32 バイトではなく、キーの 16 進文字列として設定されている CKN とまったく同じ文字列を使用します。

```
Device> enable
Device# configure terminal
Device(config)# key chain abc macsec
Device(config-keychain)# key 11
Device(config-keychain-key)# cryptographic-algorithm aes-128-cmac
Device(config-keychain-key)# key-string 12345678901234567890123456789013
Device(config-keychain-key)# lifetime local 12:21:00 Sep 9 2015 infinite
Device(config-keychain-key)# end
```

以下は、上記の設定に対する `show mka session` コマンドの出力例です。

```
Device# show mka session

Total MKA Sessions..... 1
Secured Sessions... 1
Pending Sessions... 0
```

Interface	Local-TxSCI	Policy-Name	Inherited	Key-Server
Port-ID	Peer-RxSCI	MACsec-Peers	Status	CKN
Et0/0	aabb.cc00.6600/0002	icv	NO	NO
2	aabb.cc00.6500/0002	1	Secured	11 *Note that the CKN key-string is exactly the same that has been configured for the key as hex-string.*

一方で CKN 動作が変更され、もう一方で CKN 動作が変更されていない 2 つのイメージ間の相互運用性の場合、キーの 16 進数文字列は 64 文字の 16 進数文字列である必要があります。この文字列は、CKN 動作が変更されたイメージを持つデバイスで動作するようにゼロパディングされている必要があります。次の例を参照してください。

CKN キー文字列の動作が変更されていない設定 :

```
Device# configure terminal
Device(config)# key chain abc macsec
Device(config-keychain)# key 11
Device(config-keychain-key)# cryptographic-algorithm aes-128-cmac
```



```
Local Tx-SCI..... 204c.9e85.ede4/002b
Interface MAC Address... 204c.9e85.ede4
MKA Port Identifier..... 43
Interface Name..... GigabitEthernet1/0/1
Audit Session ID.....
CAK Name (CKN)..... 010000000000000000000000000000000000000000000000000000000000000000000000000000000000000
Member Identifier (MI)... D46CBEC05D5D67594543CEAE
Message Number (MN)..... 89572
EAP Role..... NA
Key Server..... YES
MKA Cipher Suite..... AES-128-CMAC

Latest SAK Status..... Rx & Tx
Latest SAK AN..... 0
Latest SAK KI (KN)..... D46CBEC05D5D67594543CEAE00000001 (1)
Old SAK Status..... FIRST-SAK
Old SAK AN..... 0
Old SAK KI (KN)..... FIRST-SAK (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time..... 0s (No Old SAK to retire)

MKA Policy Name..... p2
Key Server Priority..... 2
Delay Protection..... NO
Replay Protection..... YES
Replay Window Size..... 0
Confidentiality Offset... 0
Algorithm Agility..... 80C201
Send Secure Announcement.. DISABLED
SAK Cipher Suite..... 0080C20001000003 (GCM-AES-XPN-128)
MACsec Capability..... 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired..... YES

# of MACsec Capable Live Peers..... 1
# of MACsec Capable Live Peers Responded.. 1

Live Peers List:
    MI              MN              Rx-SCI (Peer)      KS Priority
    -----
    38046BA37D7DA77E06D006A9 89560      c800.8459.e764/002a  10

Potential Peers List:
    MI              MN              Rx-SCI (Peer)      KS Priority
    -----

Dormant Peers List:
    MI              MN              Rx-SCI (Peer)      KS Priority
    -----
```

次に、256 ビット XPN 暗号スイートを設定した場合の **show mka sessions details** コマンドの出力例を示します。

```
Device# show mka sessions details

MKA Detailed Status for MKA Session
=====
Status: SECURED - Secured MKA Session with MACsec

Local Tx-SCI..... 204c.9e85.ede4/002b
Interface MAC Address... 204c.9e85.ede4
MKA Port Identifier..... 43
Interface Name..... GigabitEthernet1/0/1
```

## 例 : PSK を使用したポートチャネルの MACsec MKA の設定

```

Audit Session ID.....
CAK Name (CKN)..... 0100000000000000000000000000000000000000000000000000000000000000
Member Identifier (MI)... D46CBEC05D5D67594543CEAE
Message Number (MN)..... 89572
EAP Role..... NA
Key Server..... YES
MKA Cipher Suite..... AES-128-CMAC

Latest SAK Status..... Rx & Tx
Latest SAK AN..... 0
Latest SAK KI (KN)..... D46CBEC05D5D67594543CEAE00000001 (1)
Old SAK Status..... FIRST-SAK
Old SAK AN..... 0
Old SAK KI (KN)..... FIRST-SAK (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time..... 0s (No Old SAK to retire)

MKA Policy Name..... p2
Key Server Priority..... 2
Delay Protection..... NO
Replay Protection..... YES
Replay Window Size..... 0
Confidentiality Offset... 0
Algorithm Agility..... 80C201
Send Secure Announcement.. DISABLED
SAK Cipher Suite..... 0080C20001000004 (GCM-AES-XPB-256)
MACsec Capability..... 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired..... YES

# of MACsec Capable Live Peers..... 1
# of MACsec Capable Live Peers Responded.. 1

Live Peers List:
MI                MN                Rx-SCI (Peer)    KS Priority
-----
38046BA37D7DA77E06D006A9  89560            c800.8459.e764/002a  10

Potential Peers List:
MI                MN                Rx-SCI (Peer)    KS Priority
-----

Dormant Peers List:
MI                MN                Rx-SCI (Peer)    KS Priority
-----
```

## 例 : PSK を使用したポートチャネルの MACsec MKA の設定

**Etherchannel モード - Static/On**

次に、EtherChannel モードがオンのデバイス 1 およびデバイス 2 の設定例を示します。

```

Device> enable
Device# configure terminal
Device(config)# key chain KC macsec
Device(config-key-chain)# key 1000
Device(config-key-chain)# cryptographic-algorithm aes-128-cmac
Device(config-key-chain)# key-string FC8F5B10557C192F03F60198413D7D45
Device(config-key-chain)# exit
Device(config)# mka policy POLICY
```

```

Device(config-mka-policy)# key-server priority 0
Device(config-mka-policy)# macsec-cipher-suite gcm-aes-128
Device(config-mka-policy)# confidentiality-offset 0
Device(config-mka-policy)# exit
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# channel-group 2 mode on
Device(config-if)# macsec network-link
Device(config-if)# mka policy POLICY
Device(config-if)# mka pre-shared-key key-chain KC
Device(config-if)# exit
Device(config)# interface gigabitethernet 1/0/2
Device(config-if)# channel-group 2 mode on
Device(config-if)# macsec network-link
Device(config-if)# mka policy POLICY
Device(config-if)# mka pre-shared-key key-chain KC
Device(config-if)# end

```

## レイヤ 2 EtherChannel 設定

### デバイス 1

```

Device> enable
Device# configure terminal
Device(config)# interface port-channel 2
Device(config-if)# switchport
Device(config-if)# switchport mode trunk
Device(config-if)# no shutdown
Device(config-if)# end

```

### デバイス 2

```

Device> enable
Device# configure terminal
Device(config)# interface port-channel 2
Device(config-if)# switchport
Device(config-if)# switchport mode trunk
Device(config-if)# no shutdown
Device(config-if)# end

```

次に、**show etherchannel summary** コマンドの出力例を示します。

```

Flags:  D - down          P - bundled in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG

Number of channel-groups in use: 1
Number of aggregators:          1

```

例：PSK を使用したポートチャネルの MACsec MKA の設定

```

Group  Port-channel  Protocol  Ports
-----+-----+-----+-----
2      Po2 (RU)         -         Te1/0/1 (P)  Te1/0/2 (P)

```

### レイヤ 3 EtherChannel 設定

デバイス 1

```

Device> enable
Device# configure terminal
Device(config)# interface port-channel 2
Device(config-if)# no switchport
Device(config-if)# ip address 10.25.25.3 255.255.255.0
Device(config-if)# no shutdown
Device(config-if)# end

```

デバイス 2

```

Device> enable
Device# configure terminal
Device(config)# interface port-channel 2
Device(config-if)# no switchport
Device(config-if)# ip address 10.25.25.4 255.255.255.0
Device(config-if)# no shutdown
Device(config-if)# end

```

次に、**show etherchannel summary** コマンドの出力例を示します。

```

Flags:  D - down          P - bundled in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG

```

```

Number of channel-groups in use: 1
Number of aggregators:           1

```

```

Group  Port-channel  Protocol  Ports
-----+-----+-----+-----
2      Po2 (RU)         -         Te1/0/1 (P)  Te1/0/2 (P)

```

## EtherChannel モード - LACP

次に、EtherChannel モードが LACP のデバイス 1 およびデバイス 2 の設定例を示します。

```
Device> enable
Device# configure terminal
Device(config)# key chain KC macsec
Device(config-key-chain)# key 1000
Device(config-key-chain)# cryptographic-algorithm aes-128-cmac
Device(config-key-chain)# key-string FC8F5B10557C192F03F60198413D7D45
Device(config-key-chain)# exit
Device(config)# mka policy POLICY
Device(config-mka-policy)# key-server priority 0
Device(config-mka-policy)# macsec-cipher-suite gcm-aes-128
Device(config-mka-policy)# confidentiality-offset 0
Device(config-mka-policy)# exit
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# channel-group 2 mode active
Device(config-if)# macsec network-link
Device(config-if)# mka policy POLICY
Device(config-if)# mka pre-shared-key key-chain KC
Device(config-if)# exit
Device(config)# interface gigabitethernet 1/0/2
Device(config-if)# channel-group 2 mode active
Device(config-if)# macsec network-link
Device(config-if)# mka policy POLICY
Device(config-if)# mka pre-shared-key key-chain KC
Device(config-if)# end
```

## レイヤ 2 EtherChannel 設定

### デバイス 1

```
Device> enable
Device# configure terminal
Device(config)# interface port-channel 2
Device(config-if)# switchport
Device(config-if)# switchport mode trunk
Device(config-if)# no shutdown
Device(config-if)# end
```

### デバイス 2

```
Device> enable
Device# configure terminal
Device(config)# interface port-channel 2
Device(config-if)# switchport
Device(config-if)# switchport mode trunk
Device(config-if)# no shutdown
Device(config-if)# end
```

次に、**show etherchannel summary** コマンドの出力例を示します。

```
Flags:  D - down          P - bundled in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
```

```

w - waiting to be aggregated
d - default port

A - formed by Auto LAG

```

```

Number of channel-groups in use: 1
Number of aggregators:          1

```

```

-----+-----+-----+-----+-----+-----+-----+-----+-----+-----
2       Po2(SU)        LACP       Te1/1/1(P)  Te1/1/2(P)

```

### レイヤ 3 EtherChannel 設定

#### デバイス 1

```

Device> enable
Device# configure terminal
Device(config)# interface port-channel 2
Device(config-if)# no switchport
Device(config-if)# ip address 10.25.25.3 255.255.255.0
Device(config-if)# no shutdown
Device(config-if)# end

```

#### デバイス 2

```

Device> enable
Device# configure terminal
Device(config)# interface port-channel 2
Device(config-if)# no switchport
Device(config-if)# ip address 10.25.25.4 255.255.255.0
Device(config-if)# no shutdown
Device(config-if)# end

```

次に、**show etherchannel summary** コマンドの出力例を示します。

```

Flags:  D - down           P - bundled in port-channel
        I - stand-alone   s - suspended
        H - Hot-standby  (LACP only)
        R - Layer3       S - Layer2
        U - in use       f - failed to allocate aggregator

```

```

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

```

```
A - formed by Auto LAG
```

```

Number of channel-groups in use: 1
Number of aggregators:          1

```

```

Group  Port-channel  Protocol  Ports

```





```

    U - in use          f - failed to allocate aggregator

    M - not in use, minimum links not met
    u - unsuitable for bundling
    w - waiting to be aggregated
    d - default port

    A - formed by Auto LAG

```

```

Number of channel-groups in use: 1
Number of aggregators:           1

```

```

-----+-----+-----+-----+-----+-----+
          2      Po2 (SU)          PAgP      Te1/1/1 (P)  Te1/1/2 (P)

```

### レイヤ 3 EtherChannel 設定

#### デバイス 1

```

Device> enable
Device# configure terminal
Device(config)# interface port-channel 2
Device(config-if)# no switchport
Device(config-if)# ip address 10.25.25.3 255.255.255.0
Device(config-if)# no shutdown
Device(config-if)# end

```

#### デバイス 2

```

Device> enable
Device# configure terminal
Device(config)# interface port-channel 2
Device(config-if)# no switchport
Device(config-if)# ip address 10.25.25.4 255.255.255.0
Device(config-if)# no shutdown
Device(config-if)# end

```

次に、**show etherchannel summary** コマンドの出力例を示します。

```

Flags:  D - down          P - bundled in port-channel
        I - stand-alone  s - suspended
        H - Hot-standby (LACP only)
        R - Layer3       S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port

        A - formed by Auto LAG

```

```

Number of channel-groups in use: 1

```

```

Number of aggregators:          1

Group  Port-channel  Protocol  Ports
-----+-----+-----+-----
2      Po2 (RU)         PAgP      Te1/1/1 (P)  Te1/1/2 (P)

```

### アクティブな MKA セッションの表示

次に、すべてのアクティブな MKA セッションを表示します。

```
Device# show mka sessions interface Te1/0/1
```

```

=====
Interface          Local-TxSCI          Policy-Name          Inherited
Key-Server
Port-ID            Peer-RxSCI           MACsec-Peers         Status
CKN
=====
Te1/0/1            00a3.d144.3364/0025 POLICY                NO
NO
37                 701f.539b.b0c6/0032 1                Secured
1000

```

## 例 : MACsec 暗号アナウンスメントの設定

次に、セキュアアナウンスメントの MKA ポリシーの設定例を示します。

```

Device> enable
Device# configure terminal
Device(config)# mka policy mka_policy
Device(config-mka-policy)# key-server 2
Device(config-mka-policy)# send-secure-announcements
Device(config-mka-policy)# macsec-cipher-suite gcm-aes-128confidentiality-offset 0
Device(config-mka-policy)# end

```

次に、セキュアアナウンスメントのグローバル設定例を示します。

```

Device> enable
Device# configure terminal
Device(config)# mka defaults policy send-secure-announcements
Device(config)# end

```

次に、インターフェイスでの EAPoL アナウンスメントの設定例を示します。

```

Device> enable
Device# configure terminal
Device(config)# interface GigabitEthernet 1/0/1
Device(config-if)# eapol announcement
Device(config-if)# end

```

次に、EAPoL アナウンスメントが有効になっている `show running-config interface interface-name` コマンドの出力例を示します。

```
Device# show running-config interface GigabitEthernet 1/0/1
```

```
switchport mode access
 macsec
 access-session host-mode multi-host
 access-session closed
 access-session port-control auto
 dot1x pae authenticator
 dot1x timeout quiet-period 10
 dot1x timeout tx-period 5
 dot1x timeout supp-timeout 10
 dot1x supplicant eap profile peap
 eapol announcement
 spanning-tree portfast
 service-policy type control subscriber Dot1X
```

次に、セキュアアナウンスメントが無効になっている **show mka sessions interface interface-name detail** コマンドの出力例を示します。

```
Device# show mka sessions interface GigabitEthernet 1/0/1 detail
```

```
MKA Detailed Status for MKA Session
=====
Status: SECURED - Secured MKA Session with MACsec

Local Tx-SCI..... 204c.9e85.ede4/002b
Interface MAC Address.... 204c.9e85.ede4
MKA Port Identifier..... 43
Interface Name..... GigabitEthernet1/0/1
Audit Session ID.....
CAK Name (CKN).....
010000000000000000000000000000000000000000000000000000000000000000000000000000000000
Member Identifier (MI)... D46CBEC05D5D67594543CEAE
Message Number (MN)..... 89567
EAP Role..... NA
Key Server..... YES
MKA Cipher Suite..... AES-128-CMAC

Latest SAK Status..... Rx & Tx
Latest SAK AN..... 0
Latest SAK KI (KN)..... D46CBEC05D5D67594543CEAE00000001 (1)
Old SAK Status..... FIRST-SAK
Old SAK AN..... 0
Old SAK KI (KN)..... FIRST-SAK (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time..... 0s (No Old SAK to retire)

MKA Policy Name..... p2
Key Server Priority..... 2
Delay Protection..... NO
Replay Protection..... YES
Replay Window Size..... 0
```

```

Confidentiality Offset... 0
Algorithm Agility..... 80C201
Send Secure Announcement.. DISABLED
SAK Cipher Suite..... 0080C20001000001 (GCM-AES-128)
MACsec Capability..... 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired..... YES

# of MACsec Capable Live Peers..... 1
# of MACsec Capable Live Peers Responded.. 1

Live Peers List:
      MI                               MN                    Rx-SCI (Peer)            KS Priority
-----
      38046BA37D7DA77E06D006A9      89555                c800.8459.e764/002a     10

Potential Peers List:
      MI                               MN                    Rx-SCI (Peer)            KS Priority
-----

Dormant Peers List:
      MI                               MN                    Rx-SCI (Peer)            KS Priority
-----

```

次に、セキュアアナウンスメントが無効になっている **show mka sessions details** コマンドの出力例を示します。

```

Device# show mka sessions details

MKA Detailed Status for MKA Session
=====
Status: SECURED - Secured MKA Session with MACsec

Local Tx-SCI..... 204c.9e85.ede4/002b
Interface MAC Address... 204c.9e85.ede4
MKA Port Identifier..... 43
Interface Name..... GigabitEthernet1/0/1
Audit Session ID.....
CAK Name (CKN).....
01000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
Member Identifier (MI)... D46CBEC05D5D67594543CEAE
Message Number (MN)..... 89572
EAP Role..... NA
Key Server..... YES
MKA Cipher Suite..... AES-128-CMAC

Latest SAK Status..... Rx & Tx
Latest SAK AN..... 0

```

```

Latest SAK KI (KN)..... D46CBEC05D5D67594543CEAE00000001 (1)
Old SAK Status..... FIRST-SAK
Old SAK AN..... 0
Old SAK KI (KN)..... FIRST-SAK (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time..... 0s (No Old SAK to retire)

MKA Policy Name..... p2
Key Server Priority..... 2
Delay Protection..... NO
Replay Protection..... YES
Replay Window Size..... 0
Confidentiality Offset... 0
Algorithm Agility..... 80C201
Send Secure Announcement.. DISABLED
SAK Cipher Suite..... 0080C20001000001 (GCM-AES-128)
MACsec Capability..... 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired..... YES

# of MACsec Capable Live Peers..... 1
# of MACsec Capable Live Peers Responded.. 1

Live Peers List:
  MI                               MN           Rx-SCI (Peer)           KS Priority
-----
  38046BA37D7DA77E06D006A9  89560           c800.8459.e764/002a    10

Potential Peers List:
  MI                               MN           Rx-SCI (Peer)           KS Priority
-----

Dormant Peers List:
  MI                               MN           Rx-SCI (Peer)           KS Priority
-----

```

次に、セキュアアナウンスメントが無効になっている **show mka policy policy-name detail** コマンドの出力例を示します。

```

Device# show mka policy p2 detail

MKA Policy Configuration ("p2")
=====
MKA Policy Name..... p2
Key Server Priority.... 2
Confidentiality Offset. 0
Send Secure Announcement..DISABLED

```

```
Cipher Suite(s)..... GCM-AES-128

Applied Interfaces...
  GigabitEthernet1/0/1
```

## 例 : Cisco TrustSec スイッチ間リンクセキュリティ

この例は、Cisco TrustSec スイッチ間のセキュリティに必要な設定を示しています。リンクセキュリティ用に AAA および RADIUS を設定する必要があります。この例では、ACS-1 から ACS-3 は任意のサーバー名、cts-radius は Cisco TrustSec サーバーです。

```
Switch(config)#aaa new-model
Switch(config)#radius server ACS-1
Switch(config-radius-server)#address ipv4 10.5.120.12 auth-port 1812 acct-port
1813
Switch(config-radius-server)#pac key cisco123
Switch(config-radius-server)#exit
Switch(config)#radius server ACS-2
Switch(config-radius-server)#address ipv4 10.5.120.14 auth-port 1812 acct-port
1813
Switch(config-radius-server)#pac key cisco123
Switch(config-radius-server)#exit
Switch(config)#radius server ACS-3
Switch(config-radius-server)#address ipv4 10.5.120.15 auth-port 1812 acct-port
1813
Switch(config-radius-server)#pac key cisco123
Switch(config-radius-server)#exit
Switch(config)#aaa group server radius cts-radius
Switch(config-sg-radius)#server name ACS-1
Switch(config-sg-radius)#server name ACS-2
Switch(config-sg-radius)#server name ACS-3
Switch(config-sg-radius)#exit
Switch(config)#aaa authentication login default none
Switch(config)#aaa authentication dot1x default group cts-radius
Switch(config)#aaa authorization network cts-radius group cts-radius
Switch(config)#aaa session-id common
Switch(config)#cts authorization list cts-radius
Switch(config)#dot1x system-auth-control
```

次に、インターフェイスに Cisco TrustSec 認証を手動モードで設定する例を示します。

```
Switch# configure terminal
Switch(config)# interface tengigabitethernet 1/1/2
Switch(config-if)# cts manual
Switch(config-if-cts-manual)# sap pmk 1234abcdef mode-list gcm-encrypt null no-encap
Switch(config-if-cts-manual)# no propagate sgt
Switch(config-if-cts-manual)# exit
Switch(config-if)# end
```

## 例 : MKA 情報の表示

次に、`show mka sessions` コマンドの出力例を示します。





```
Send Secure Announcement.. DISABLED
SAK Cipher Suite..... 0080C20001000001 (GCM-AES-128)
MACsec Capability..... 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired..... YES
```

```
# of MACsec Capable Live Peers..... 1
# of MACsec Capable Live Peers Responded.. 1
```

```
Live Peers List:
   MI                             MN                    Rx-SCI (Peer)           KS Priority
-----
   38046BA37D7DA77E06D006A9 89555               c800.8459.e764/002a   10
```

```
Potential Peers List:
   MI                             MN                    Rx-SCI (Peer)           KS Priority
-----
```

```
Dormant Peers List:
   MI                             MN                    Rx-SCI (Peer)           KS Priority
-----
```

次に、**show mka sessions details** コマンドの出力例を示します。

```
Device# show mka sessions details

MKA Detailed Status for MKA Session
=====
Status: SECURED - Secured MKA Session with MACsec

Local Tx-SCI..... 204c.9e85.ede4/002b
Interface MAC Address.... 204c.9e85.ede4
MKA Port Identifier..... 43
Interface Name..... GigabitEthernet1/0/1
Audit Session ID.....
CAK Name (CKN)..... 0100000000000000000000000000000000000000000000000000000000000000
Member Identifier (MI)... D46CBEC05D5D67594543CEAE
Message Number (MN)..... 89572
EAP Role..... NA
Key Server..... YES
MKA Cipher Suite..... AES-128-CMAC

Latest SAK Status..... Rx & Tx
Latest SAK AN..... 0
Latest SAK KI (KN)..... D46CBEC05D5D67594543CEAE00000001 (1)
Old SAK Status..... FIRST-SAK
Old SAK AN..... 0
Old SAK KI (KN)..... FIRST-SAK (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time..... 0s (No Old SAK to retire)

MKA Policy Name..... p2
Key Server Priority..... 2
Delay Protection..... NO
Replay Protection..... YES
Replay Window Size..... 0
Confidentiality Offset... 0
Algorithm Agility..... 80C201
Send Secure Announcement.. DISABLED
SAK Cipher Suite..... 0080C20001000001 (GCM-AES-128)
MACsec Capability..... 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired..... YES

# of MACsec Capable Live Peers..... 1
# of MACsec Capable Live Peers Responded.. 1
```

```

Live Peers List:
  MI                               MN           Rx-SCI (Peer)      KS Priority
-----
  38046BA37D7DA77E06D006A9  89560       c800.8459.e764/002a  10

Potential Peers List:
  MI                               MN           Rx-SCI (Peer)      KS Priority
-----

Dormant Peers List:
  MI                               MN           Rx-SCI (Peer)      KS Priority
-----

```

次に、**show mka policy** コマンドの出力例を示します。

```
Device# show mka policy
```

```
MKA Policy Summary...
```

Policy Name	KS Priority	Delay Protect	Replay Protect	Window Size	Conf Offset	Cipher Suite(s)	Interfaces Applied
*DEFAULT POLICY*	0	FALSE	TRUE	0	0	GCM-AES-128	
p1	1	FALSE	TRUE	0	0	GCM-AES-128	
p2	2	FALSE	TRUE	0	0	GCM-AES-128	Gi1/0/1

次に、**show mka policy policy-name** コマンドの出力例を示します。

```
Device# show mka policy p2
```

```
MKA Policy Summary...
```

Policy Name	KS Priority	Delay Protect	Replay Protect	Window Size	Conf Offset	Cipher Suite(s)	Interfaces Applied
p2	2	FALSE	TRUE	0	0	GCM-AES-128	Gi1/0/1

次に、**show mka policy policy-name detail** コマンドの出力例を示します。

```
Device# show mka policy p2 detail
```

```
MKA Policy Configuration ("p2")
```

```

=====
MKA Policy Name..... p2
Key Server Priority... 2
Confidentiality Offset. 0
Send Secure Announcement..DISABLED
Cipher Suite(s)..... GCM-AES-128

```

```
Applied Interfaces...
```

```
GigabitEthernet1/0/1
```

次に、**show mka statistics interface interface-name** コマンドの出力例を示します。

```
Device# show mka statistics interface GigabitEthernet 1/0/1
```

```

MKA Statistics for Session
=====
Reauthentication Attempts.. 0

CA Statistics
Pairwise CAKeys Derived... 0

```



```

MKA Error Counter Totals
=====
Session Failures
  Bring-up Failures..... 0
  Reauthentication Failures..... 0
  Duplicate Auth-Mgr Handle..... 0

SAK Failures
  SAK Generation..... 0
  Hash Key Generation..... 0
  SAK Encryption/Wrap..... 0
  SAK Decryption/Unwrap..... 0
  SAK Cipher Mismatch..... 0

CA Failures
  Group CAK Generation..... 0
  Group CAK Encryption/Wrap..... 0
  Group CAK Decryption/Unwrap..... 0
  Pairwise CAK Derivation..... 0
  CKN Derivation..... 0
  ICK Derivation..... 0
  KEK Derivation..... 0
  Invalid Peer MACsec Capability... 0

MACsec Failures
  Rx SC Creation..... 0
  Tx SC Creation..... 0
  Rx SA Installation..... 0
  Tx SA Installation..... 0

MKPDU Failures
  MKPDU Tx..... 0
  MKPDU Rx Validation..... 0
  MKPDU Rx Bad Peer MN..... 0
  MKPDU Rx Non-recent Peerlist MN.. 0

```

次に、**show macsec interface** コマンドの出力例を示します。

```
Device# show macsec interface HundredGigE 2/0/4
```

```

MACsec is enabled
Replay protect : enabled
Replay window : 0
Include SCI : yes
Use ES Enable : no
Use SCB Enable : no
Admin Pt2Pt MAC : forceTrue(1)
Pt2Pt MAC Operational : no
Cipher : GCM-AES-128
Confidentiality Offset : 0

Capabilities
ICV length : 16
Data length change supported: yes
Max. Rx SA : 16
Max. Tx SA : 16
Max. Rx SC : 8
Max. Tx SC : 8
Validate Frames : strict
PN threshold notification support : Yes
Ciphers supported : GCM-AES-128
                   GCM-AES-256
                   GCM-AES-XPN-128
                   GCM-AES-XPN-256

```

Access control : must secure

Transmit Secure Channels

SCI : 3C5731BBB5850475  
SC state : inUse(1)  
Elapsed time : 7w0d  
Start time : 7w0d  
Current AN: 0  
Previous AN: -  
Next PN: 149757  
SA State: inUse(1)  
Confidentiality : yes  
SAK Unchanged : yes  
SA Create time : 00:04:41  
SA Start time : 7w0d  
SC Statistics  
Auth-only Pkts : 0  
Auth-only Bytes : 0  
Encrypted Pkts : 0  
Encrypted Bytes : 0  
SA Statistics  
Auth-only Pkts : 0  
Auth-only Bytes : 0  
Encrypted Pkts : 149756  
Encrypted Bytes : 16595088

Port Statistics

Egress untag pkts 0  
Egress long pkts 0

Receive Secure Channels

SCI : 3C5731BBB5C504DF  
SC state : inUse(1)  
Elapsed time : 7w0d  
Start time : 7w0d  
Current AN: 0  
Previous AN: -  
Next PN: 149786  
RX SA Count: 0  
SA State: inUse(1)  
SAK Unchanged : yes  
SA Create time : 00:04:39  
SA Start time : 7w0d  
SC Statistics  
Notvalid pkts 0  
Invalid pkts 0  
Valid pkts 0  
Late pkts 0  
Uncheck pkts 0  
Delay pkts 0  
UnusedSA pkts 0  
NousingSA pkts 0  
Validated Bytes 0  
Decrypted Bytes 0  
SA Statistics  
Notvalid pkts 0  
Invalid pkts 0  
Valid pkts 149784  
Late pkts 0  
Uncheck pkts 0  
Delay pkts 0  
UnusedSA pkts 0  
NousingSA pkts 0  
Validated Bytes 0

```
Decrypted Bytes 16654544
```

```
Port Statistics
Ingress untag pkts 0
Ingress notag pkts 631726
Ingress badtag pkts 0
Ingress unknownSCI pkts 0
Ingress noSCI pkts 0
Ingress overrun pkts 0
```

## MACsec 暗号化の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリース だけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、[www.cisco.com/go/cfn](http://www.cisco.com/go/cfn) に移動します。Cisco.com のアカウントは必要ありません。

表 31: MACsec 暗号化の機能情報

機能名	リリース	機能情報
MACsec の暗号化	Cisco IOS XE Everest 16.5.1a	MACsec は 2 台の MACsec 対応デバイス間のパケットの認証と暗号化の IEEE 802.1AE 規格です。Catalyst スイッチは、スイッチとホストデバイス間の MACsec Key Agreement (MKA) 暗号化による 802.1AE 暗号化をサポートします。



## 第 12 章

# セキュア シェル (SSH) の設定

- [セキュア シェルを設定するための前提条件 \(281 ページ\)](#)
- [セキュア シェルの設定に関する制約事項 \(282 ページ\)](#)
- [セキュア シェルの設定について \(282 ページ\)](#)
- [セキュア シェルの設定方法 \(285 ページ\)](#)
- [SSH の設定およびステータスのモニタリング \(289 ページ\)](#)
- [セキュア シェルの機能情報 \(289 ページ\)](#)

## セキュア シェルを設定するための前提条件

セキュア シェル (SSH) 用にスイッチを設定するための前提条件は、次のとおりです。

- SSH を動作させるには、スイッチに Rivest、Shamir、および Adleman (RSA) の公開キーと秘密キーのペアが必要です。これは SSH が必要なセキュア コピー プロトコル (SCP) も同様に、セキュアな転送を実現させるには、これらのキーのペアが必要です。
- SCP をイネーブルにする前に、スイッチの SSH、認証、許可、およびアカウントिंगを適切に設定してください。
- SCP は SSH を使用してセキュアな転送を実行するため、ルータには RSA キーのペアが必要です。
- SCP はセキュリティについて SSH に依存します。
- SCP の設定には認証、許可、およびアカウントिंग (AAA) の許可も必要なため、ルータはユーザが正しい権限レベルを保有しているか確認する必要があります。
- ユーザが SCP を使用するには適切な許可が必要です。
- 適切な許可を得ているユーザは、SCP を使用して Cisco IOS File System (IFS) のファイルをスイッチに (またはスイッチから) 自由にコピーできます。コピーには **copy** コマンドを使用します。また、許可されている管理者もこの作業をワークステーションから実行できます。

- セキュア シェル (SSH) サーバは、IPsec (データ暗号規格 (DES) または 3DES) の暗号化ソフトウェアイメージを必要とします。SSH クライアントは、IPsec (DES または 3DES) の暗号化ソフトウェア イメージが必要です。
- グローバル コンフィギュレーション モードで **hostname** および **ip domain-name** コマンドを使用して、デバイスのホスト名とホスト ドメインを設定します。

## セキュア シェルの設定に関する制約事項

セキュアシェル用に デバイス を設定するための制約事項は、次のとおりです。

- スイッチは、Rivest, Shamir, and Adelman (RSA) 認証をサポートします。
- SSH は、実行シェル アプリケーションだけをサポートします。
- SSH サーバおよび SSH クライアントは、データ暗号規格 (DES) (56 ビット) および 3DES (168 ビット) データ暗号化ソフトウェアでのみサポートされます。DES ソフトウェア イメージの場合、使用できる暗号化アルゴリズムは DES だけです。3DES ソフトウェア イメージの場合、DES と 3DES の両方の暗号化アルゴリズムを使用できます。
- デバイスは、128 ビットキー、192 ビットキー、または 256 ビットキーの Advanced Encryption Standard (AES) 暗号化アルゴリズムをサポートします。ただし、キーを暗号化する対称暗号化 AES はサポートされません。
- SCP を使用する場合、**copy** コマンドにパスワードを入力することはできません。プロンプトが表示されたときに、入力する必要があります。
- ログイン バナーはセキュア シェルバージョン 1 ではサポートされません。セキュア シェルバージョン 2 ではサポートされています。
- リバース SSH の代替手段をコンソール アクセス用に設定する場合、-I キーワード、userid :{number} {ip-address} デリミタ、および引数が必須です。

## セキュア シェルの設定について

セキュアシェル (SSH) は、デバイスに対する安全なリモート接続を可能にするプロトコルです。SSH は、デバイスの認証時に強力な暗号化を行うことで、リモート接続について Telnet 以上のセキュリティを実現します。このソフトウェア リリースは、SSH バージョン 2 (SSHv2) をサポートします。

## SSH およびスイッチ アクセス

セキュアシェル (SSH) は、デバイスに対する安全なリモート接続を可能にするプロトコルです。SSH は、デバイスの認証時に強力な暗号化を行うことで、リモート接続について Telnet 以上のセキュリティを実現します。このソフトウェア リリースは、SSH バージョン 2 (SSHv2) をサポートします。



IPv6 の SSH 機能は IPv4 における機能と同じです。IPv6 の場合、SSH は IPv6 アドレスをサポートし、IPv6 トランスポート上において、リモート IPv6 ノードとのセキュリティ保護および暗号化された接続を有効化します。

## SSH サーバ、統合クライアント、およびサポートされているバージョン

セキュアシェル (SSH) 統合クライアント機能は、SSH プロトコル上で動作し、デバイスの認証および暗号化を実現するアプリケーションです。SSH クライアントによって、シスコ デバイスは別のシスコ デバイスなど SSH サーバを実行するデバイスに対して、セキュアで暗号化された接続を実行できます。この接続は、接続が暗号化される点を除いて Telnet のアウトバウンド接続と同様の機能を提供します。SSH クライアントは、認証および暗号化により、保護されていないネットワーク上でもセキュアな通信ができます。

SSH サーバおよび SSH 統合クライアントは、スイッチ上で実行されるアプリケーションです。SSH サーバは、このリリースでサポートされている SSH クライアントおよび、他社製の SSH クライアントと使用します。SSH クライアントは、市販の一般的な SSH サーバと連動します。SSH クライアントは、Data Encryption Standard (DES)、3DES、およびパスワード認証の暗号をサポートします。



(注) SSH クライアント機能を使用できるのは、SSH サーバがイネーブルの場合だけです。

ユーザ認証は、デバイスに対する Telnet セッションの認証と同様に実行されます。SSH は、次のユーザ認証方式もサポートします。

- TACACS+
- RADIUS
- ローカル認証および許可

## SSH 設定時の注意事項

スイッチを SSH サーバまたは SSH クライアントとして設定する場合は、次の注意事項に従ってください。

- SSHv2 サーバは、SSHv1 サーバで生成される RSA キーのペアを使用できます (逆の場合も同様です)。
- SSH サーバがアクティブスイッチ上で動作しており、アクティブスイッチに障害が発生した場合、新しいアクティブスイッチは、以前のアクティブスイッチによって生成された RSA キーペアを使用します。
- **crypto key generate rsa** グローバル コンフィギュレーション コマンドを入力した後、CLI エラーメッセージが表示される場合、RSA キーペアは生成されていません。ホスト名およびドメインを再設定してから、**crypto key generate rsa** コマンドを入力してください。

- RSA キーのペアを生成する場合に、メッセージ「No host name specified」が表示されることがあります。このメッセージが表示された場合は、**hostname** グローバル コンフィギュレーション コマンドを使用してホスト名を設定する必要があります。
- RSA キーのペアを生成する場合に、メッセージ「No domain specified」が表示されることがあります。このメッセージが表示された場合は、**ip domain-name** グローバル コンフィギュレーション コマンドを使用して IP ドメイン名を設定する必要があります。
- ローカル認証および許可の方法を設定する場合に、コンソール上で AAA がディセーブルにされていることを確認してください。

## Secure Copy Protocol の概要

Secure Copy Protocol (SCP) 機能は、スイッチの設定やイメージファイルのコピーにセキュアな認証方式を提供します。SCP にはセキュア シェル (SSH) が必要です (Berkeley の r-tool に代わるセキュリティの高いアプリケーションおよびプロトコルです)。

SSH を動作させるには、スイッチに RSA の公開キーと秘密キーのペアが必要です。これは SSH が必要な SCP も同様で、セキュアな転送を実現させるには、これらのキーのペアが必要です。

また、SSH には AAA 許可が必要のため、適切に設定するには、SCP にも AAA 認証が必要になります。

- SCP をイネーブルにする前に、スイッチの SSH、認証、許可、およびアカウントिंगを適切に設定してください。
- SCP は SSH を使用してセキュアな転送を実行するため、ルータには RSA キーのペアが必要です。



(注) SCP を使用する場合、copy コマンドにパスワードを入力することはできません。プロンプトが表示されたときに、入力する必要があります。

## Secure Copy Protocol

セキュア コピー プロトコル (SCP) 機能は、device の設定やスイッチ イメージファイルのコピーにセキュアな認証方式を提供します。SCP は一連の Berkeley の r-tools に基づいて設計されているため、その動作内容は、SCP が SSH のセキュリティに対応している点を除けば、Remote Copy Protocol (RCP) と類似しています。また、SCP では認証、許可、およびアカウントिंग (AAA) の設定が必要なため、device はユーザーが正しい権限レベルを保有しているかどうかを特定できます。セキュア コピー機能を設定するには、SCP の概念を理解する必要があります。

# セキュアシェルの設定方法

## SSH を実行するためのデバイスのセットアップ

SSH を実行するようにデバイスをセットアップするには、次の手順を実行してください。

### 始める前に

ローカルアクセスまたはリモートアクセス用にユーザ認証を設定します。この手順は必須です。詳細については、次の関連項目を参照してください。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **hostname *hostname***
4. **ip domain-name *domain\_name***
5. **crypto key generate rsa**
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： デバイス> <b>enable</b>	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： デバイス# <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 3	<b>hostname <i>hostname</i></b> 例： デバイス(config)# <b>hostname your_hostname</b>	デバイスのホスト名および IP ドメイン名を設定します。 (注) この手順を実行するのは、デバイスを SSH サーバーとして設定する場合だけです。

	コマンドまたはアクション	目的
ステップ 4	<b>ip domain-name</b> <i>domain_name</i> 例 : デバイス (config) # <b>ip domain-name</b> <i>your_domain</i>	デバイスのホスト ドメインを設定します。
ステップ 5	<b>crypto key generate rsa</b> 例 : デバイス (config) # <b>crypto key generate rsa</b>	<p>デバイス上でローカルおよびリモート認証用に SSH サーバーを有効にし、RSA キーペアを生成します。デバイスの RSA キーペアを生成すると、SSH が自動的に有効になります。</p> <p>最小モジュラス サイズは、1024 ビットにすることを推奨します。</p> <p>RSA キーのペアを生成する場合に、モジュラスの長さの入力を求められます。モジュラスが長くなるほど安全ですが、生成と使用に時間がかかります。</p> <p>(注) この手順を実行するのは、デバイスを SSH サーバーとして設定する場合だけです。</p>
ステップ 6	<b>end</b> 例 : デバイス (config) # <b>end</b>	特権 EXEC モードに戻ります。
ステップ 7	<b>show running-config</b> 例 : デバイス # <b>show running-config</b>	入力を確認します。
ステップ 8	<b>copy running-config startup-config</b> 例 : デバイス # <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## SSH サーバの設定

SSH サーバーを設定するには、次の手順を実行します。



(注) デバイスを SSH サーバーとして設定する場合にのみ、この手順が必要です。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **ip ssh version [2]**
4. **ip ssh {time-out *seconds* | authentication-retries *number*}**
5. 次のいずれかまたは両方を使用します。
  - `line vty line_number[ending_line_number]`
  - **transport input ssh**
6. **end**
7. 次のいずれかを使用します。
  - **show ip ssh**
  - **show ssh**
8. **show running-config**
9. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 :  デバイス> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します (要求された場合) 。
ステップ 2	<b>configure terminal</b> 例 :  デバイス# <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 3	<b>ip ssh version [2]</b> 例 :  デバイス (config)# <b>ip ssh version 2</b>	(任意) SSH バージョン 2 を実行するようにデバイスを設定します。  このコマンドを入力しない場合、またはキーワードを指定しない場合、SSH サーバーは、SSH クライアントでサポートされている最新バージョンの SSH を選択します。

	コマンドまたはアクション	目的
ステップ 4	<p><b>ip ssh {time-out seconds   authentication-retries number}</b></p> <p>例 :</p> <pre>デバイス(config)# ip ssh time-out 90 OR デバイス(config)# ip ssh authentication-retries 2</pre>	<p>SSH 制御パラメータを設定します。</p> <ul style="list-style-type: none"> <li>• <b>time-out seconds</b> : タイムアウト値は秒単位で指定します (デフォルト値は 120 秒)。指定できる範囲は 0 ~ 120 秒です。このパラメータは、SSH ネゴシエーションフェーズに適用されます。接続が確立されると、デバイスは CLI ベースセッションのデフォルトのタイムアウト値を使用します。</li> <li>• <b>authentication-retries number</b> : クライアントをサーバーへ再認証できる回数を指定します。デフォルトは 3 です。指定できる範囲は 0 ~ 5 です。</li> </ul> <p>両方のパラメータを設定する場合はこの手順を繰り返します。</p>
ステップ 5	<p>次のいずれかまたは両方を使用します。</p> <ul style="list-style-type: none"> <li>• <b>line vty line_number[ending_line_number]</b></li> <li>• <b>transport input ssh</b></li> </ul> <p>例 :</p> <pre>デバイス(config)# line vty 1 10</pre> <p>または</p> <pre>デバイス(config-line)# transport input ssh</pre>	<p>(任意) 仮想端末回線設定を設定します。</p> <ul style="list-style-type: none"> <li>• ライン コンフィギュレーション モードを開始して、仮想端末回線設定を設定します。 <i>line_number</i> 引数と <i>ending_line_number</i> 引数の有効な範囲は 0 ~ 15 です。</li> <li>• デバイス で SSH 以外の Telnet 接続を防ぎ、デバイスを SSH 接続のみに限定するように指定します。</li> </ul>
ステップ 6	<p><b>end</b></p> <p>例 :</p> <pre>デバイス(config-line)# end</pre>	<p>回線コンフィギュレーションモードを終了します。続いて、特権 EXEC モードに戻ります。</p>
ステップ 7	<p>次のいずれかを使用します。</p> <ul style="list-style-type: none"> <li>• <b>show ip ssh</b></li> <li>• <b>show ssh</b></li> </ul>	<ul style="list-style-type: none"> <li>• SSH サーバのバージョンおよび設定情報を表示します。</li> </ul>

	コマンドまたはアクション	目的
	例： デバイス# <code>show ip ssh</code>  または デバイス# <code>show ssh</code>	<ul style="list-style-type: none"> <li>• デバイス上の SSH サーバーの接続ステータスを表示します。</li> </ul>
ステップ 8	<b>show running-config</b>  例：  デバイス# <code>show running-config</code>	入力を確認します。
ステップ 9	<b>copy running-config startup-config</b>  例：  デバイス# <code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

## SSH の設定およびステータスのモニタリング

次の表に、SSH サーバの設定およびステータスを示します。

表 32: SSH サーバの設定およびステータスを表示するコマンド

コマンド	目的
<code>show ip ssh</code>	SSH サーバのバージョンおよび設定情報を表示します。
<code>show ssh</code>	SSH サーバのステータスを表示します。

## セキュアシェルの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、[www.cisco.com/go/cfn](http://www.cisco.com/go/cfn) に移動します。Cisco.com のアカウントは必要ありません。

表 33:セキュア シェルの機能情報

機能名	リリース	機能情報
セキュア シェル	Cisco IOS XE Everest 16.5.1a	SSH は、デバイスに対する安全なリモート接続を可能にするプロトコルです。SSH は、デバイスの認証時に強力な暗号化を行うことで、リモート接続について Telnet 以上のセキュリティを実現します。このソフトウェアリリースは SSHv2 をサポートしています。





## 第 13 章

# SSH 認証の X.509v3 証明書

- SSH 認証の X.509v3 証明書 (291 ページ)
- SSH 認証用の X.509v3 証明書に関する情報 (292 ページ)
- SSH 認証用の X.509v3 証明書の設定方法 (292 ページ)
- SSH 認証用の X.509v3 証明書の設定例 (296 ページ)
- SSH 認証用の X.509v3 証明書の機能履歴 (297 ページ)

## SSH 認証の X.509v3 証明書

SSH 認証の X.509v3 証明書機能は、サーバー内で X.509v3 デジタル証明書を使用し、セキュアシェル (SSH) サーバー側でユーザー認証を使用します。

このモジュールでは、デジタル証明書用のサーバおよびユーザ証明書プロファイルを設定する方法について説明します。

## SSH 認証の X.509v3 証明書の前提条件

- SSH 認証の X.509v3 証明書機能では、**ip ssh server authenticate user** コマンドの代わりに **ip ssh server algorithm authentication** コマンドが導入されます。 **ip ssh server authenticate user** コマンドを使用すると、次の警告メッセージが表示されます。

```
Warning: SSH command accepted but this CLI will be deprecated soon. Please move to new CLI "ip ssh server algorithm authentication". Please configure "default ip ssh server authenticate user" to make CLI ineffective.
```

- **default ip ssh server authenticate user** コマンドを使用して、**ip ssh server authenticate user** コマンドを無効にします。その後、IOS セキュアシェル (SSH) サーバーは **ip ssh server algorithm authentication** コマンドを使用して起動します。

## SSH 認証の X.509v3 証明書の制約事項

- SSH 認証の X.509v3 証明書機能の実装は、IOS セキュアシェル (SSH) サーバー側へのみ適用できます。

- IOS SSH サーバーは、IOS SSH サーバー側のサーバーおよびユーザー認証について、x509v3-ssh-rsa アルゴリズム ベースの証明書のみをサポートします。

## SSH 認証用の X.509v3 証明書に関する情報

次に、デジタル証明書、およびサーバーとユーザーの認証について説明します。

### デジタル証明書

認証の有効性は、公開署名キーとその署名者のアイデンティティとの関連の強さに依存します。X.509v3 形式 (RFC5280) のデジタル証明書は、アイデンティティの管理を実行するために使用されます。信頼できるルート証明機関とその中間証明機関による署名の連鎖によって、指定の公開署名キーと指定のデジタルアイデンティティがバインドされます。

公開キーインフラストラクチャ (PKI) のトラストポイントは、デジタル証明書の管理に役立ちます。証明書とトラストポイントを関連付けることによって、証明書を追跡できます。トラストポイントには、認証局 (CA)、さまざまなアイデンティティパラメータ、およびデジタル証明書に関する情報が含まれています。複数のトラストポイントを作成して、異なる証明書に関連付けることができます。

### X.509v3 を使用したサーバーおよびユーザー認証

サーバー認証の場合、IOS セキュア シェル (SSH) が確認のためにそれ自体の証明書を SSH クライアントに送信します。このサーバ証明書は、サーバ証明書プロファイル (ssh-server-cert-profile-server コンフィギュレーションモード) で設定されたトラストポイントに関連付けられます。

ユーザー認証の場合、SSH クライアントが確認のためにユーザの証明書を IOS SSH サーバに送信します。SSH サーバは、サーバ証明書プロファイル (ssh-server-cert-profile-user コンフィギュレーションモード) で設定された公開キーインフラストラクチャ (PKI) トラストポイントを使用して、受信したユーザ証明書を確認します。

デフォルトでは、証明書ベースの認証が、IOS SSH サーバ端末でサーバおよびユーザに対して有効になっています。

## SSH 認証用の X.509v3 証明書の設定方法

ここでは、SSH 認証用の X.509v3 証明書の設定方法について説明します。

## サーバー認証にデジタル証明書を使用するための IOS SSH サーバーの設定

サーバー認証にデジタル証明書を使用するように IOS SSH サーバーを設定するには、次の手順を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： デバイス> <b>enable</b>	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： デバイス# <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 3	<b>ip ssh server algorithm hostkey {x509v3-ssh-rsa [ssh-rsa]   ssh-rsa [x509v3-ssh-rsa]}</b> 例： デバイス(config)# <b>ip ssh server algorithm hostkey x509v3-ssh-rsa</b>	ホスト キー アルゴリズムの順序を定義します。セキュアシェル (SSH) クライアントとネゴシエートされるのは、設定済みのアルゴリズムのみです。 (注) IOS SSH サーバーには、1 つ以上の設定済みホスト キー アルゴリズムが必要です。 <ul style="list-style-type: none"> <li>• ssh-rsa : 公開キーベース認証</li> <li>• x509v3-ssh-rsa : 証明書ベース認証</li> </ul>
ステップ 4	<b>ip ssh server certificate profile</b> 例： デバイス(config)# <b>ip ssh server certificate profile</b>	サーバー証明書プロファイルおよびユーザー証明書プロファイルを設定し、SSH 証明書プロファイル コンフィギュレーション モードを開始します。
ステップ 5	<b>server</b> 例： デバイス(ssh-server-cert-profile)# <b>server</b>	サーバー証明書プロファイルを設定し、SSH サーバー証明書プロファイルのユーザー コンフィギュレーション モードを開始します。
ステップ 6	<b>trustpoint sign PKI-trustpoint-name</b> 例： デバイス(ssh-server-cert-profile-server)# <b>trustpoint sign trust1</b>	公開キー インフラストラクチャ (PKI) トラストポイントにサーバ証明書プロファイルにアタッチします。SSH サーバは、この PKI トラストポイントに関連付けられた証明書をサーバ認証に使用します。

	コマンドまたはアクション	目的
ステップ 7	<b>ocsp-response include</b> 例： デバイス (ssh-server-cert-profile-server) # <b>ocsp-response include</b>	(任意) Online Certificate Status Protocol (OCSP) の応答または OCSP ステープリングをサーバ証明書と一緒に送信します。  (注) デフォルトではこのコマンドの「no」形式が設定されており、OCSP 応答はサーバ証明書と一緒に送信されません。
ステップ 8	<b>end</b> 例： デバイス (ssh-server-cert-profile-server) # <b>end</b>	SSH サーバ証明書プロファイルのサーバ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

## ユーザ認証用のユーザのデジタル証明書を確認するための IOS SSH サーバの設定

ユーザ認証にデジタル証明書を使用するように IOS SSH サーバを設定するには、次の手順を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： デバイス > <b>enable</b>	特権 EXEC モードを有効にします。  パスワードを入力します (要求された場合)。
ステップ 2	<b>configure terminal</b> 例： デバイス # <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 3	<b>ip ssh server algorithm authentication {publickey   keyboard   password}</b> 例： デバイス (config) # <b>ip ssh server algorithm authentication publickey</b>	ユーザ認証アルゴリズムの順序を定義します。セキュアシェル (SSH) クライアントとネゴシエートされるのは、設定済みのアルゴリズムのみです。  (注) IOS SSH サーバには、1 つ以上の設定済みユーザ認証アルゴリズムが必要です。  (注) ユーザ認証に証明書方式を使用するには、 <b>publickey</b> キーワードを設定する必要があります。

	コマンドまたはアクション	目的
		(注) <b>ip ssh server algorithm authentication</b> コマンドは <b>ip ssh server authenticate user</b> コマンドの代わりに使用します。
ステップ 4	<b>ip ssh server algorithm publickey {x509v3-ssh-rsa [ssh-rsa]   ssh-rsa [x509v3-ssh-rsa]}</b> 例： デバイス (config) # <b>ip ssh server algorithm publickey x509v3-ssh-rsa</b>	公開キーアルゴリズムの順序を定義します。SSH クライアントによってユーザ認証に許可されるのは、設定済みのアルゴリズムのみです。 (注) IOS SSH クライアントには、1 つ以上の設定済み公開キー アルゴリズムが必要です。 <ul style="list-style-type: none"> <li>• ssh-rsa : 公開キーベース認証</li> <li>• x509v3-ssh-rsa : 証明書ベース認証</li> </ul>
ステップ 5	<b>ip ssh server certificate profile</b> 例： デバイス (config) # <b>ip ssh server certificate profile</b>	サーバ証明書プロファイルおよびユーザ証明書プロファイルを設定し、SSH 証明書プロファイル コンフィギュレーション モードを開始します。
ステップ 6	<b>user</b> 例： デバイス (ssh-server-cert-profile) # <b>user</b>	ユーザ証明書プロファイルを設定し、SSH サーバ証明書プロファイルのユーザ 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>trustpoint verify PKI-trustpoint-name</b> 例： デバイス (ssh-server-cert-profile-user) # <b>trustpoint verify trust2</b>	受信したユーザ証明書の確認に使用される公開キー インフラストラクチャ (PKI) トラストポイントを設定します。 (注) 同じコマンドを複数回実行することで、複数のトラストポイントを設定します。最大 10 のトラストポイントを設定できます。
ステップ 8	<b>ocsp-response required</b> 例： デバイス (ssh-server-cert-profile-user) # <b>ocsp-response required</b>	(任意) 受信したユーザ証明書による Online Certificate Status Protocol (OCSP) の応答の有無を要求します。 (注) デフォルトではこのコマンドの「no」形式が設定されており、ユーザー証明書は OCSP 応答なしで受け入れられます。
ステップ 9	<b>end</b> 例： デバイス (ssh-server-cert-profile-user) # <b>end</b>	SSH サーバ証明書プロファイルのユーザ コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

## デジタル証明書を使用したサーバーおよびユーザー認証の設定の確認

デジタル証明書を使用したサーバーおよびユーザー認証の設定を確認するには、次の手順を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： デバイス> <b>enable</b>	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	<b>show ip ssh</b> 例： デバイス# <b>show ip ssh</b>  SSH Enabled - version 1.99 Authentication methods:publickey,keyboard-interactive,password Authentication Publickey Algorithms:x509v3-ssh-rsa,ssh-rsa Hostkey Algorithms:x509v3-ssh-rsa,ssh-rsa Authentication timeout: 120 secs; Authentication retries: 3 Minimum expected Diffie Hellman key size : 1024 bits	現在設定されている認証方式を表示します。証明書ベース認証の使用を確認するには、x509v3-ssh-rsa アルゴリズムが設定済みのホストキーアルゴリズムであることを確認します。

## SSH 認証用の X.509v3 証明書の設定例

ここでは、デジタル証明書を使用したユーザーおよびサーバー認証の例を示します。

### 例：サーバー認証にデジタル証明書を使用するための IOS SSH サーバーの設定

この例では、サーバー認証用のデジタル証明書を使用するための IOS SSH サーバーの設定方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm hostkey x509v3-ssh-rsa
Device(config)# ip ssh server certificate profile
Device(ssh-server-cert-profile)# server
Device(ssh-server-cert-profile-server)# trustpoint sign trust1
Device(ssh-server-cert-profile-server)# exit
```

## 例：ユーザ認証用のユーザのデジタル証明書を確認するための IOS SSH サーバの設定

この例では、ユーザー認証用のユーザーのデジタル証明書を確認するための IOS SSH サーバの設定方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm authentication publickey
Device(config)# ip ssh server algorithm publickey x509v3-ssh-rsa
Device(config)# ip ssh server certificate profile
Device(ssh-server-cert-profile)# user
Device(ssh-server-cert-profile-user)# trustpoint verify trust2
Device(ssh-server-cert-profile-user)# end
```

## SSH 認証用の X.509v3 証明書の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	SSH 認証の X.509v3 証明書	SSH 認証の X.509v3 証明書機能は、サーバ内で X.509v3 デジタル証明書を使用し、SSH サーバ側でユーザ認証を使用します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。







## 第 14 章

# コモンクライテリア認定用の SSH アルゴリズム

- [コモンクライテリア認定用の SSH アルゴリズムに関する情報 \(299 ページ\)](#)
- [コモンクライテリア認定用の SSH アルゴリズムの設定方法 \(301 ページ\)](#)
- [コモンクライテリア認定用の SSH アルゴリズムの設定例 \(305 ページ\)](#)
- [コモンクライテリア認定用の SSH アルゴリズムの確認 \(306 ページ\)](#)
- [コモンクライテリア認定用のセキュアシェルアルゴリズムの機能情報 \(307 ページ\)](#)

## コモンクライテリア認定用の SSH アルゴリズムに関する情報

ここでは、コモンクライテリア認定のセキュアシェル (SSH) アルゴリズム、Cisco IOS SSH サーバーアルゴリズム、および Cisco IOS SSH クライアントアルゴリズムについて説明します。

### コモンクライテリア認定用の SSH アルゴリズム

セキュアシェル (SSH) 設定によって、Cisco IOS SSH サーバーおよびクライアントは、許可リストから設定されたアルゴリズムのネゴシエーションのみを許可することができます。リモートパーティが許可リストに含まれていないアルゴリズムのみを使用してネゴシエーションしようとすると、要求は拒否され、セッションは確立されません。

### Cisco IOS SSH サーバー アルゴリズム

Cisco IOS セキュア シェル (SSH) サーバーは、次の順序で暗号化アルゴリズム (Advanced Encryption Standard カウンタ モード [AES-CTR]、AES 暗号ブロック連鎖 [AES-CBC]、Triple Data Encryption Standard [3DES]) をサポートします。

サポートされるデフォルトの暗号化の順序 :

1. aes128-ctr

2. aes192-ctr
3. aes256-ctr

サポートされるデフォルト以外の暗号化の順序：

1. aes128-cbc
2. aes192-cbc
3. aes256-cbc
4. 3des

Cisco IOS SSH クライアントは、次の順序でメッセージ認証コード（MAC）アルゴリズムをサポートします。

サポートされるデフォルトの HMAC の順序：

1. hmac-sha2-256
2. hmac-sha2-512
3. hmac-sha1
4. hmac-sha1-96

Cisco IOS SSH クライアントがサポートするホストキーアルゴリズムは 1 つのみで、CLI 設定は必要ありません。

サポートされるデフォルトのホストキーの順序：

1. x509v3-ssh-rsa
2. ssh-rsa

## Cisco IOS SSH クライアント アルゴリズム

Cisco IOS セキュア シェル（SSH）クライアントは、次の順序で暗号化アルゴリズム（Advanced Encryption Standard カウンタ モード [AES-CTR]、AES 暗号ブロック連鎖 [AES-CBC]、Triple Data Encryption Standard [3DES]）をサポートします。

サポートされるデフォルトの暗号化の順序：

1. aes128-ctr
2. aes192-ctr
3. aes256-ctr

サポートされるデフォルト以外の暗号化の順序：

1. aes128-cbc
2. aes192-cbc
3. aes256-cbc

#### 4. 3des

Cisco IOS SSH クライアントは、次の順序でメッセージ認証コード (MAC) アルゴリズムをサポートします。

サポートされるデフォルトの HMAC の順序 :

1. hmac-sha2-256
2. hmac-sha2-512
3. hmac-sha1
4. hmac-sha1-96

Cisco IOS SSH クライアントがサポートするホストキーアルゴリズムは1つのみで、CLI 設定は必要ありません。

サポートされるデフォルトのホストキーの順序 :

1. x509v3-ssh-rsa
2. ssh-rsa

## コモンクライテリア認定用の SSH アルゴリズムの設定方法

ここでは、設定とトラブルシューティング方法に関する情報を提供します。

- Cisco IOS SSH サーバーおよびクライアントの暗号キーアルゴリズム
- Cisco IOS SSH サーバーおよびクライアントの MAC アルゴリズム
- Cisco IOS SSH サーバーのホストキーアルゴリズム

## Cisco IOS SSH サーバーおよびクライアントの暗号キーアルゴリズムの設定

### 手順の概要

1. **enable**
2. **configure terminal**
3. **ip ssh {server | client} algorithm encryption {aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc | aes192-cbc | aes256-cbc | 3des-cbc }**
4. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<p><b>enable</b></p> <p>例 :</p> <pre>Device&gt; enable</pre>	<p>特権 EXEC モードを有効にします。</p> <p>パスワードを入力します (要求された場合)。</p>
ステップ 2	<p><b>configure terminal</b></p> <p>例 :</p> <pre>Device# configure terminal</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>
ステップ 3	<p><b>ip ssh {server   client} algorithm encryption {aes128-ctr   aes192-ctr   aes256-ctr   aes128-cbc   aes192-cbc   aes256-cbc   3des-cbc }</b></p> <p>例 :</p> <pre>Device(config)# ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr aes128-cbc 3des-cbc aes192-cbc aes256-cbc</pre> <pre>Device(config)# ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr aes128-cbc 3des-cbc aes192-cbc aes256-cbc</pre>	<p>SSH サーバーおよびクライアントでの暗号化アルゴリズムの順序を定義します。この順序は、アルゴリズムのネゴシエーション時に指定されます。</p> <p>(注) Cisco IOS SSH サーバーおよびクライアントには、1つ以上の設定済み暗号化アルゴリズムが必要です。</p> <p>(注) 以前設定したアルゴリズムのリストから1つのアルゴリズムを無効にするには、このコマンドの <b>no</b> 形式を使用します。複数のアルゴリズムを無効にするには、このコマンドの <b>no</b> 形式を異なるアルゴリズム名で複数回使用します。</p> <p>(注) デフォルト設定では、次に示すようにこのコマンドのデフォルト形式を使用します。</p> <pre>Device(config)# ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr aes128-cbc 3des-cbc aes192-cbc aes256-cbc</pre>
ステップ 4	<p><b>end</b></p> <p>例 :</p> <pre>Device(config)# end</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、特権 EXEC モードに戻ります。</p>

トラブルシューティングのヒント

設定で最後の暗号化アルゴリズムを無効にしようとする、次のメッセージが表示されてコマンドが拒否されます。

% SSH command rejected: All encryption algorithms cannot be disabled

## Cisco IOS SSH サーバーおよびクライアントの MAC アルゴリズムの設定

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : Device> <b>enable</b>	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合) 。
ステップ 2	<b>configure terminal</b> 例 : Device# <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 3	<b>ip ssh {server   client} algorithm mac {hmac-sha2-256   hmac-sha2-512   hmac-sha1   hmac-sha1-96}</b> 例 : Device(config)# <b>ip ssh server algorithm mac hmac-sha2-256 hmac-sha2-512 hmac-sha1 hmac-sha1-96</b> Device(config)# <b>ip ssh client algorithm mac hmac-sha2-256 hmac-sha2-512 hmac-sha1 hmac-sha1-96</b>	SSH サーバーおよびクライアントでの MAC (メッセージ認証コード) アルゴリズムの順序を定義します。この順序は、アルゴリズムのネゴシエーション時に指定されます。 (注) Cisco IOS SSH サーバーおよびクライアントには、1つ以上の設定済みハッシュメッセージ認証コード (HMAC) アルゴリズムが必要です。 (注) 以前設定したアルゴリズムのリストから1つのアルゴリズムを無効にするには、このコマンドの <b>no</b> 形式を使用します。複数のアルゴリズムを無効にするには、このコマンドの <b>no</b> 形式を異なるアルゴリズム名で複数回使用します。 (注) デフォルト設定では、次に示すようにこのコマンドのデフォルト形式を使用します。 Device(config)# <b>ip ssh server algorithm mac hmac-sha2-256 hmac-sha2-512 hmac-sha1 hmac-sha1-96</b>

	コマンドまたはアクション	目的
ステップ 4	<b>end</b> 例：  Device (config) # <b>end</b>	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。

## トラブルシューティングのヒント

設定で最後の MAC アルゴリズムを無効にしようとする、次のメッセージが表示されてコマンドが拒否されます。

```
% SSH command rejected: All mac algorithms cannot be disabled
```

## Cisco IOS SSH サーバーのホスト キー アルゴリズムの設定

### 手順の概要

1. **enable**
2. **configure terminal**
3. **ip ssh server algorithm hostkey {x509v3-ssh-rsa | ssh-rsa}**
4. **end**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  Device> <b>enable</b>	特権 EXEC モードを有効にします。  パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  Device# <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 3	<b>ip ssh server algorithm hostkey {x509v3-ssh-rsa   ssh-rsa}</b> 例：  Device (config) # <b>ip ssh server algorithm hostkey x509v3-ssh-rsa ssh-rsa</b>	ホストキーアルゴリズムの順序を定義します。Cisco IOS セキュア シェル (SSH) クライアントとネゴシエートされるのは、設定済みのアルゴリズムのみです。

	コマンドまたはアクション	目的
		<p>(注) Cisco IOS SSH サーバーには、1つ以上の設定済みホストキーアルゴリズムが必要です。</p> <ul style="list-style-type: none"> <li>• x509v3-ssh-rsa : X.509v3 証明書ベース認証</li> <li>• ssh-rsa : 公開キーベース認証</li> </ul> <p>(注) 以前設定したアルゴリズムのリストから1つのアルゴリズムを無効にするには、このコマンドの <b>no</b> 形式を使用します。複数のアルゴリズムを無効にするには、このコマンドの <b>no</b> 形式を異なるアルゴリズム名で複数回使用します。</p> <p>(注) デフォルト設定では、次に示すようにこのコマンドのデフォルト形式を使用します。</p> <pre>Device(config)# ip ssh server algorithm hostkey x509v3-ssh-rsa ssh-rsa</pre>
ステップ 4	<p><b>end</b></p> <p>例 :</p> <pre>Device(config)# end</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、特権 EXEC モードに戻ります。</p>

## トラブルシューティングのヒント

設定で最後のホストキーアルゴリズムを無効にしようとするすると、次のメッセージが表示されてコマンドが拒否されます。

```
% SSH command rejected: All hostkey algorithms cannot be disabled
```

## コモンクライテリア認定用のSSHアルゴリズムの設定例

ここでは、コモン認定用のSSHアルゴリズムの設定例を示します。

## 例 : Cisco IOS SSH サーバーの暗号キー アルゴリズムの設定

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr
aes128-cbc aes192-cbc aes256-cbc 3des
Device(config)# end
```

## 例 : Cisco IOS SSH クライアントの暗号キー アルゴリズムの設定

```
Device> enable
Device# configure terminal
Device(config)# ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr
aes128-cbc aes192-cbc aes256-cbc 3des

Device(config)# end
```

## 例 : Cisco IOS SSH サーバーの MAC アルゴリズムの設定

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm mac hmac-sha2-256, hmac-sha2-512, hmac-sha1,
hmac-sha1-96
Device(config)# end
```

## 例 : Cisco IOS SSH サーバーのホスト キー アルゴリズムの設定

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm hostkey x509v3-ssh-rsa ssh-rsa
Device(config)# end
```

# コモンクライテリア認定用の SSH アルゴリズムの確認

### 手順の概要

1. enable
2. show ip ssh



## 手順の詳細

---

### ステップ 1 enable

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

例：

```
Device> enable
```

### ステップ 2 show ip ssh

設定済みのセキュアシェル（SSH）暗号化、ホストキー、およびメッセージ認証コード（MAC）アルゴリズムを表示します。

例：

次の **show ip ssh** コマンドの出力例は、デフォルトの順序で設定された暗号化アルゴリズムを示しています。

```
Device# show ip ssh
```

```
Encryption Algorithms: aes128-ctr, aes192-ctr, aes256-ctr, aes128-cbc, aes192-cbc, aes256-cbc, 3des
```

次の **show ip ssh** コマンドの出力例は、デフォルトの順序で設定された MAC アルゴリズムを示しています。

```
Device# show ip ssh
```

```
MAC Algorithms: hmac-sha2-256, hmac-sha2-512, hmac-sha1, hmac-sha1-96
```

次の **show ip ssh** コマンドの出力例は、デフォルトの順序で設定されたホストキー アルゴリズムを示しています。

```
Device# show ip ssh
```

```
Hostkey Algorithms: x509v3-ssh-rsa, ssh-rsa
```

---

# コモンクライテリア認定用のセキュアシェルアルゴリズムの機能情報

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	コモンクライテリア認定用のセキュアシェルアルゴリズム	コモンクライテリア認定用の SSH アルゴリズム機能によって、コモンクライテリア認定を取得したアルゴリズムのリストおよび順序が提供されます。このモジュールでは、認定されたアルゴリズムのリストに基づいて SSH 接続を制限できるように、セキュアシェル (SSH) サーバーおよびクライアントの暗号化、メッセージ認証コード (MAC)、およびホストキーアルゴリズムの設定方法について説明します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



## 第 15 章

# Secure Socket Layer HTTP の設定

- [Secure Socket Layer HTTP について \(309 ページ\)](#)
- [Secure Socket Layer HTTP の設定方法 \(313 ページ\)](#)
- [セキュア HTTP サーバおよびクライアントのステータスのモニタリング \(321 ページ\)](#)
- [Secure Socket Layer HTTP に関するその他の参考資料 \(321 ページ\)](#)
- [Secure Socket Layer HTTP の機能履歴 \(322 ページ\)](#)

## Secure Socket Layer HTTP について

### セキュア HTTP サーバおよびクライアントの概要

セキュア HTTP 接続の場合、HTTP サーバが送受信するデータは暗号化されてインターネットに送信されます。SSL 暗号化を伴う HTTP は、Web ブラウザからスイッチを設定するような機能に、セキュアな接続を提供します。シスコが実装するセキュア HTTP サーバおよび HTTP クライアントでは、アプリケーション層の暗号化に SSL バージョン 3.0 を使用します。HTTP over SSL は、HTTPS と省略されます (セキュアな接続の場合、URL が `http://` の代わりに `https://` で始まります)。



(注) SSL は 1999 年に Transport Layer Security (TLS) に発展しましたが、このような特定のコンテキストでまだ使用されています。

セキュア HTTP サーバ (スイッチ) の主な役割は、指定のポート (デフォルトの HTTPS ポートは 443) で HTTPS 要求を待ち受けて、HTTP 1.1 Web サーバへその要求を渡すことです。HTTP 1.1 サーバはその要求を処理して、セキュア HTTP サーバへ応答 (呼び出す) します。セキュア HTTP サーバは HTTP 1.1 サーバの代わりに、元の要求に応えます。

セキュア HTTP クライアント (Web ブラウザ) の主な役割は、Cisco IOS アプリケーション要求に応答して、そのアプリケーションが要求した HTTPS User Agent サービスを実行し、応答を (そのアプリケーションに) 返すことです。

## CA のトラストポイント

認証局 (CA) は、要求を認可して参加するネットワーク デバイスに証明書を発行します。これらのサービスは、参加するデバイスに対する中央集約的なセキュリティキーおよび証明書の管理を提供します。特定の CA サーバはトラストポイントと呼ばれます。

接続が実行されると、HTTPS サーバは、トラストポイントとなる特定の CA から得た X.509v3 の証明書を発行することで、セキュアな接続をクライアントに提供します。クライアント (通常、Web ブラウザ) は、その証明書の認証に必要な公開キーを保有しています。

セキュア HTTP 接続には、CA のトラストポイントを設定することを強く推奨します。HTTPS サーバを実行しているデバイスに CA のトラストポイントが設定されていないと、サーバは自身を認証して必要な RSA のキーのペアを生成します。自身で認証した (自己署名) 証明書は適切なセキュリティではないので、接続するクライアントはその証明書が自己証明書であることを通知し、ユーザに接続の選択 (確立または拒否) をさせる必要があります。この選択肢は内部ネットワーク トポロジ (テスト用など) に役立ちます。

CA のトラストポイントを設定していないと、セキュア HTTP 接続を有効にした場合、そのセキュア HTTP サーバ (またはクライアント) に対する一時的または永続的な自己署名証明書が自動的に生成されます。

- スイッチにホスト名とドメイン名が設定されていない場合、生成される自己署名証明書は一時的なものです。スイッチを再起動すると、この一時的な自己署名証明書は失われ、新たに自己署名証明書 (一時的に) が割り当てられます。
- スイッチにホスト名とドメイン名が設定されている場合、生成される自己署名証明書は永続的なものです。この証明書は、スイッチを再起動しても、セキュア HTTP サーバを無効にしても有効のままです。そのため、再度セキュア HTTP 接続を有効にしたときに使用できます。



(注) 認証局およびトラストポイントは、個々のデバイスで設定する必要があります。他のデバイスからコピーすると、それらはスイッチ上で無効になります。

新しい証明書を登録した場合、新しい設定の変更は、サーバが再起動するまで HTTPS サーバに適用されません。**reload** コマンドを使用して DCNM サーバを再起動できます。

新しい証明書を登録した場合、新しい設定の変更は、サーバが再起動するまで HTTPS サーバに適用されません。CLI を使用するか、または物理的な再起動によって、サーバを再起動できます。サーバを再起動すると、スイッチは新しい証明書の使用を開始します。

自己署名証明書が生成された場合、その情報は **show running-config** 特権 EXEC コマンドで出力できます。自己署名証明書を表示するコマンドの出力 (**show running-config** コマンド) を例として一部示します。

```
デバイス# show running-config
Building configuration...
```

```
<output truncated>
```

```
crypto pki trustpoint TP-self-signed-3080755072
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-3080755072
  revocation-check none
  rsakeypair TP-self-signed-3080755072
!
!
crypto ca certificate chain TP-self-signed-3080755072
certificate self-signed 01
  3082029F 30820208 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  59312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 33303830 37353530 37323126 30240609 2A864886 F70D0109
  02161743 45322D33 3535302D 31332E73 756D6D30 342D3335 3530301E 170D3933
  30333031 30303030 35395A17 0D323030 31303130 30303030 305A3059 312F302D
```

<output truncated>

自己署名証明書は、セキュア HTTP サーバを無効にして、**no crypto pki trustpoint TP-self-signed-30890755072** グローバル コンフィギュレーション コマンドを入力することで削除できます。その後、セキュア HTTP サーバを再度有効にすると、自己署名証明書が新たに生成されます。



(注) *TP self-signed* の後ろに表示されている値は、デバイスのシリアル番号によって異なります。

オプションのコマンド (**ip http secure-client-auth**) を使用すると、HTTPS サーバがクライアントからの X.509v3 証明書を要求します。クライアントの認証は、サーバ自身の認証よりも高いセキュリティを提供します。

## CipherSuite

CipherSuite は暗号化アルゴリズムおよびダイジェストアルゴリズムを指定して、SSL 接続に使用します。HTTPS サーバに接続すると、クライアントの Web ブラウザは、サポート対象の CipherSuite のリストを提供します。その後クライアントとサーバは、両方でサポートされている暗号化アルゴリズムで最適なものをリストから選択してネゴシエートします。たとえば、Netscape Communicator 4.76 は、米国のセキュリティ (RSA 公開キー暗号 MD2、MD5、RC2-CBC、RC4、DES-CBC、および DES-EDE3-CBC) をサポートしています。

最適な暗号化には、128 ビット暗号化をサポートするクライアントブラウザ (Microsoft Internet Explorer バージョン 5.5 以降または Netscape Communicator バージョン 4.76 以降など) が必要です。SSL\_RSA\_WITH\_DES\_CBC\_SHA CipherSuite は、128 ビット暗号化を提供しないため、他の CipherSuite よりもセキュリティが低くなります。

CipherSuite は、よりセキュリティが高く、複雑になればなるほど、わずかですが処理時間が必要になります。次に、スイッチでサポートされる CipherSuite およびルータの処理負荷 (速さ) による CipherSuite のランク (速い順) を定義します。

1. **SSL\_RSA\_WITH\_DES\_CBC\_SHA** : メッセージの暗号化に DES-CBC、およびメッセージダイジェストに SHA を使用した RSA のキー交換 (RSA 公開キー暗号化)

2. `SSL_RSA_WITH_NULL_SHA` : メッセージの暗号化に NULL、およびメッセージダイジェストに SHA を使用したキー交換 (SSL 3.0 専用)。
3. `SSL_RSA_WITH_NULL_MD5` : メッセージの暗号化に NULL、およびメッセージダイジェストに MD5 を使用したキー交換 (SSL 3.0 専用)。
4. `SSL_RSA_WITH_RC4_128_MD5` : RC4 128 ビット暗号化、およびメッセージダイジェストに MD5 を使用した RSA のキー交換
5. `SSL_RSA_WITH_RC4_128_SHA` : RC4 128 ビット暗号化、およびメッセージダイジェストに SHA を使用した RSA のキー交換
6. `SSL_RSA_WITH_3DES_EDE_CBC_SHA` : メッセージの暗号化に 3DES と DES-EDE3-CBC、およびメッセージダイジェストに SHA を使用した RSA のキー交換 (RSA 公開キー暗号化)
7. `SSL_RSA_WITH_AES_128_CBC_SHA` : AES 128 ビット暗号化、およびメッセージダイジェストに SHA を使用した RSA のキー交換 (SSL 3.0 専用)。
8. `SSL_RSA_WITH_AES_256_CBC_SHA` : AES 256 ビット暗号化、およびメッセージダイジェストに SHA を使用した RSA のキー交換 (SSL 3.0 専用)。
9. `SSL_RSA_WITH_AES_128_CBC_SHA` : AES 128 ビット暗号化、およびメッセージダイジェストに SHA を使用した RSA のキー交換 (SSL 3.0 専用)。
10. `SSL_RSA_WITH_AES_256_CBC_SHA` : AES 256 ビット暗号化、およびメッセージダイジェストに SHA を使用した RSA のキー交換 (SSL 3.0 専用)。



(注) Chrome の最新バージョンは4つの元の暗号スイートをサポートしません。そのため、Web GUI とゲストポータル両方へのアクセスが拒否されます。

(暗号化およびダイジェストアルゴリズムをそれぞれ指定して組み合わせた) RSA は、SSL 接続においてキーの生成および認証の両方に使用されます。これは、CA のトラストポイントが設定されているかどうかにかかわらず。

## SSL のデフォルト設定

標準の HTTP サーバはイネーブルに設定されています。

SSL はイネーブルに設定されています。

CA のトラストポイントは設定されていません。

自己署名証明書は生成されていません。

## SSL の設定時の注意事項

SSL をスイッチ クラスタで使用すると、SSL セッションがクラスタ コマンドで終了します。クラスタ メンバのスイッチは標準の HTTP で動作させる必要があります。

CA のトラストポイントを設定する前に、システムクロックが設定されていることを確認してください。クロックが設定されていないと、不正な日付により証明書が拒否されます。

スイッチスタック内のアクティブスイッチで、SSL セッションが終了します。

## Secure Socket Layer HTTP の設定方法

### CA のトラストポイントの設定

セキュア HTTP 接続には、CA のトラストポイントを正式に設定することを推奨します。CA のトラストポイントは、自己署名証明書より高いセキュリティがあります。

CA のトラストポイントを設定するには、特権 EXEC モードで次の手順を実行します。

#### 手順の概要

1. **configure terminal**
2. **hostname** *hostname*
3. **ip domain-name** *domain-name*
4. **crypto key generate rsa**
5. **crypto ca trustpoint** *name*
6. **enrollment url** *url*
7. **enrollment http-proxy** *host-name port-number*
8. **crl query** *url*
9. **primary** *name*
10. **exit**
11. **crypto ca authentication** *name*
12. **crypto ca enroll** *name*
13. **end**

#### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 : デバイス# <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。

	コマンドまたはアクション	目的
ステップ 2	<b>hostname</b> <i>hostname</i> 例 : デバイス (config) # <b>hostname</b> <i>your_hostname</i>	スイッチのホスト名を指定します (以前ホスト名を設定していない場合のみ必須)。ホスト名はセキュリティ キーと証明書に必要です。
ステップ 3	<b>ip domain-name</b> <i>domain-name</i> 例 : デバイス (config) # <b>ip domain-name</b> <i>your_domain</i>	スイッチの IP ドメイン名を指定します (以前 IP ドメイン名を設定していない場合のみ必須)。IP ドメイン名はセキュリティ キーと証明書に必要です。
ステップ 4	<b>crypto key generate rsa</b> 例 : デバイス (config) # <b>crypto key generate rsa</b>	(任意) RSA キー ペアを生成します。RSA キーのペアは、スイッチの証明書を入手する前に必要です。RSA キーのペアは自動的に生成されます。必要であれば、このコマンドを使用してキーを再生成できます。
ステップ 5	<b>crypto ca trustpoint</b> <i>name</i> 例 : デバイス (config) # <b>crypto ca trustpoint</b> <i>your_trustpoint</i>	CA のトラストポイントにローカルの設定名を指定して、CA 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 6	<b>enrollment url</b> <i>url</i> 例 : デバイス (ca-trustpoint) # <b>enrollment url</b> <i>http://your_server:80</i>	スイッチによる証明書要求の送信先の URL を指定します。
ステップ 7	<b>enrollment http-proxy</b> <i>host-name port-number</i> 例 : デバイス (ca-trustpoint) # <b>enrollment http-proxy</b> <i>your_host 49</i>	(任意) HTTP プロキシサーバーを経由して CA から証明書を入手するようにスイッチを設定します。 <ul style="list-style-type: none"> <li>• <i>host-name</i> には、CA を取得するために使用するプロキシサーバを指定します。</li> <li>• <i>port-number</i> には、CA にアクセスするために使用するポート番号を指定します。</li> </ul>
ステップ 8	<b>crl query</b> <i>url</i> 例 : デバイス (ca-trustpoint) # <b>crl query</b> <i>ldap://your_host:49</i>	ピアの証明書が取り消されていないかを確認するために、証明書失効リスト (CRL) を要求するようにスイッチを設定します。



	コマンドまたはアクション	目的
ステップ 9	<b>primary name</b> 例 : デバイス (ca-trustpoint) # <b>primary your_trustpoint</b>	(任意) トラストポイントが CA 要求に対してプライマリ (デフォルト) トラストポイントとして使用されるように指定します。 • <i>name</i> には、設定したトラストポイントを指定します。
ステップ 10	<b>exit</b> 例 : デバイス (ca-trustpoint) # <b>exit</b>	CA 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、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 11	<b>crypto ca authentication name</b> 例 : デバイス (config) # <b>crypto ca authentication your_trustpoint</b>	CA の公開キーを取得して CA を認証します。ステップ 5 で使用した名前と同じものを使用します。
ステップ 12	<b>crypto ca enroll name</b> 例 : デバイス (config) # <b>crypto ca enroll your_trustpoint</b>	指定した CA トラストポイントから証明書を取得します。このコマンドは、各 RSA キーのペアに対して 1 つの署名入りの証明書を要求します。
ステップ 13	<b>end</b> 例 : デバイス (config) # <b>end</b>	特権 EXEC モードに戻ります。

## セキュア HTTP サーバの設定

セキュア HTTP サーバを設定するには、特権 EXEC モードで次の手順を実行します。

### 始める前に

証明に証明書の認証を使用する場合、前の手順を使用してスイッチの CA トラストポイントを設定してから、HTTP サーバを有効にする必要があります。CA のトラストポイントを設定していない場合、セキュア HTTP サーバを最初に有効にした時点で、自己署名証明書が生成されます。サーバを設定した後、標準およびセキュア HTTP サーバ両方に適用するオプション (パス、適用するアクセスリスト、最大接続数、またはタイムアウト ポリシー) を設定できます。

Web ブラウザを使用してセキュア HTTP 接続を確認するには、`https://URL` を入力します (URL は IP アドレス、またはサーバー スイッチのホスト名)。デフォルトポート以外のポートを設定している場合、URL の後ろにポート番号も指定する必要があります。次に例を示します。



(注) AES256\_SHA2 はサポートされません。

```
https://209.165.129:1026
```

または

```
https://host.domain.com:1026
```

アクセスリスト (IPv4 ACL のみ) を指定するための従来の `ip http access-class access-list-number` コマンドは廃止予定です。引き続きこのコマンドを使用して、HTTP サーバへのアクセスを許可するアクセスリストを指定できます。2つの新しいコマンドは、IPv4 および IPv6 ACL を指定するためのサポートを有効にするために導入されました。これらは、IPv4 ACL を指定するための `ip http access-class ipv4 access-list-name | access-list-number` と、IPv6 ACL を指定するための `ip http access-class ipv6 access-list-name` です。警告メッセージの受信を防ぐために、新しい CLI の使用をお勧めします。

アクセス リストを指定する際は、次の考慮事項があります。

- 存在しないアクセスリストを指定すると、設定は実行されますが、次の警告メッセージを受信します。

```
ACL being attached does not exist, please configure it
```

- HTTP サーバにアクセスリストを指定するために `ip http access-class` コマンドを使用すると、次の警告メッセージが表示されます。

```
This CLI will be deprecated soon, Please use new CLI ip http access-class ipv4/ipv6 <access-list-name>| <access-list-number>
```

- `ip http access-class ipv4 access-list-name | access-list-number` または `ip http access-class ipv6 access-list-name` を使用した場合に、アクセスリストがすでに `ip http access-class` を使用して設定されていた場合は、次の警告メッセージが表示されます。

```
Removing ip http access-class <access-list-number>
```

`ip http access-class access-list-number` と `ip http access-class ipv4 access-list-name | access-list-number` は同じ機能を共有しています。コマンドを実行するごとに、その前のコマンドのコンフィギュレーションは上書きされます。2つのコマンドの設定間の次の組み合わせによって、実行コンフィギュレーションへの影響が説明されます。

- `ip http access-class access-list-number` がすでに設定されている場合に、`ip http access-class ipv4 access-list-number` コマンドを使用して設定を行おうとした場合、`ip http access-class access-list-number` の設定は削除され、`ip http access-class ipv4 access-list-number` の設定が実行コンフィギュレーションに追加されます。

- **ip http access-class access-list-number** がすでに設定されている場合に、**ip http access-class ipv4 access-list-name** コマンドを使用して設定を行おうとした場合、**ip http access-class access-list-number** の設定は削除され、**ip http access-class ipv4 access-list-name** の設定が実行コンフィギュレーションに追加されます。
- **ip http access-class ipv4 access-list-number** がすでに設定されている場合に、**ip http access-class access-list-name** を使用して設定を行おうとした場合、**ip http access-class ipv4 access-list-number** の設定は削除され、**ip http access-class access-list-name** の設定が実行コンフィギュレーションに追加されます。
- **ip http access-class ipv4 access-list-name** がすでに設定されている場合に、**ip http access-class access-list-number** を使用して設定を行おうとした場合、**ip http access-class ipv4 access-list-name** の設定は削除され、**ip http access-class access-list-number** の設定が実行コンフィギュレーションに追加されます。

## 手順の概要

1. **show ip http server status**
2. **configure terminal**
3. **ip http secure-server**
4. **ip http secure-port port-number**
5. **ip http secure-ciphersuite {[3des-ede-cbc-sha] [rc4-128-md5] [rc4-128-sha] [des-cbc-sha]}**
6. **ip http secure-client-auth**
7. **ip http secure-trustpoint name**
8. **ip http path path-name**
9. **ip http access-class access-list-number**
10. **ip http access-class { ipv4 {access-list-number | access-list-name} | ipv6 {access-list-name} }**
11. **ip http max-connections value**
12. **ip http timeout-policy idle seconds life seconds requests value**
13. **end**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>show ip http server status</b> 例 : デバイス# <b>show ip http server status</b>	(任意) HTTPサーバのステータスを表示して、セキュアHTTPサーバの機能がソフトウェアでサポートされているかどうかを判断します。出力で、次のラインのどちらかを確認してください。  HTTP secure server capability: Present  または  HTTP secure server capability: Not present

	コマンドまたはアクション	目的
ステップ 2	<b>configure terminal</b> 例：  デバイス# <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 3	<b>ip http secure-server</b> 例：  デバイス (config)# <code>ip http secure-server</code>	HTTPS サーバがディセーブルの場合、イネーブルにします。HTTPS サーバは、デフォルトでイネーブルに設定されています。
ステップ 4	<b>ip http secure-port <i>port-number</i></b> 例：  デバイス (config)# <code>ip http secure-port 443</code>	(任意) HTTPS サーバに使用するポート番号を指定します。デフォルトのポート番号は 443 です。443 または 1025 ~ 65535 の範囲で指定できます。
ステップ 5	<b>ip http secure-ciphersuite {[3des-ede-cbc-sha] [rc4-128-md5] [rc4-128-sha] [des-cbc-sha]}</b> 例：  デバイス (config)# <code>ip http secure-ciphersuite rc4-128-md5</code>	(任意) HTTPS 接続の暗号化に使用する CipherSuite (暗号化アルゴリズム) を指定します。特定の CipherSuite を指定する理由がなければ、サーバとクライアントが、両方がサポートする CipherSuite でネゴシエートするように設定します。これがデフォルトです。
ステップ 6	<b>ip http secure-client-auth</b> 例：  デバイス (config)# <code>ip http secure-client-auth</code>	(任意) HTTP サーバを設定して、接続処理の間、認証のために、クライアントからの X.509v3 証明書を要求します。デフォルトでは、クライアントがサーバからの証明書を要求する設定になっていますが、サーバはクライアントを認証しないようになっています。
ステップ 7	<b>ip http secure-trustpoint <i>name</i></b> 例：  デバイス (config)# <code>ip http secure-trustpoint your_trustpoint</code>	X.509v3 セキュリティ証明書の取得およびクライアントの証明書接続の認証に使用する CA のトラストポイントを指定します。  (注) このコマンドの使用は、前の手順に従って CA のトラストポイントをすでに設定しているという前提を踏まえて説明しています。
ステップ 8	<b>ip http path <i>path-name</i></b> 例：	(任意) HTML ファイルのベースとなる HTTP パスを設定します。パスは、ローカル システムにある HTTP サーバファイルの場所を指定します (通常、システムのフラッシュメモリを指定します)。

	コマンドまたはアクション	目的
	デバイス (config) # <code>ip http path /your_server:80</code>	
ステップ 9	<b>ip http access-class</b> <i>access-list-number</i> 例 : デバイス (config) # <code>ip http access-class 2</code>	(任意) HTTP サーバへのアクセスの許可に使用するアクセス リストを指定します。
ステップ 10	<b>ip http access-class</b> { <b>ipv4</b> { <i>access-list-number</i>   <i>access-list-name</i> }   <b>ipv6</b> { <i>access-list-name</i> } } 例 : デバイス (config) # <code>ip http access-class ipv4 4</code>	(任意) HTTP サーバへのアクセスの許可に使用するアクセス リストを指定します。
ステップ 11	<b>ip http max-connections</b> <i>value</i> 例 : デバイス (config) # <code>ip http max-connections 4</code>	(任意) HTTP サーバへの同時最大接続数を指定します。値は 10 以上にすることを推奨します。これは、UI が想定どおりに機能するために必要な値です。
ステップ 12	<b>ip http timeout-policy idle</b> <i>seconds</i> <b>life</b> <i>seconds</i> <b>requests</b> <i>value</i> 例 : デバイス (config) # <code>ip http timeout-policy idle 120 life 240 requests 1</code>	(任意) 指定の状況下における、HTTP サーバへの接続最大時間を指定します。  <ul style="list-style-type: none"> <li>• <b>idle</b> : データの受信がないか、応答データが送信できない場合の最大時間。指定できる範囲は 1 ~ 600 秒です。デフォルト値は 180 秒 (3 分) です。</li> <li>• <b>life</b> : 接続を確立している最大時間。指定できる範囲は 1 ~ 86400 秒 (24 時間) です。デフォルト値は 180 秒です。</li> <li>• <b>requests</b> : 永続的な接続で処理される要求の最大数。最大値は 86400 です。デフォルトは 1 です。</li> </ul>
ステップ 13	<b>end</b> 例 : デバイス (config) # <code>end</code>	特権 EXEC モードに戻ります。

## セキュア HTTP クライアントの設定

セキュア HTTP クライアントを設定するには、特権 EXEC モードで次の手順を実行します。

## 始める前に

標準の HTTP クライアントおよびセキュア HTTP クライアントは常にイネーブルです。証明書の認証にはセキュア HTTP クライアントの証明書が必要です。次の手順では、前の手順で CA のトラストポイントをスイッチに設定していることを前提にしています。CA のトラストポイントが設定されておらず、リモートの HTTPS サーバーがクライアントの認証を要求した場合、セキュア HTTP クライアントへの接続は失敗します。

## 手順の概要

1. **configure terminal**
2. **ip http client secure-trustpoint *name***
3. **ip http client secure-ciphersuite {[3des-ede-cbc-sha] [rc4-128-md5] [rc4-128-sha] [des-cbc-sha]}**
4. **end**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例：  デバイス# <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>ip http client secure-trustpoint <i>name</i></b> 例：  デバイス (config)# <b>ip http client secure-trustpoint <i>your_trustpoint</i></b>	(任意) リモートの HTTP サーバがクライアント認証を要求した場合に使用する、CA のトラストポイントを指定します。このコマンドの使用は、前の手順を使用して CA のトラストポイントをすでに設定しているという前提を踏まえて説明しています。クライアント認証が必要ない場合、またはプライマリ のトラストポイントがすでに設定されている場合は、このコマンドは任意です。
ステップ 3	<b>ip http client secure-ciphersuite {[3des-ede-cbc-sha] [rc4-128-md5] [rc4-128-sha] [des-cbc-sha]}</b> 例：  デバイス (config)# <b>ip http client secure-ciphersuite <i>rc4-128-md5</i></b>	(任意) HTTPS 接続の暗号化に使用する CipherSuite (暗号化アルゴリズム) を指定します。特定の CipherSuite を指定する理由がなければ、サーバとクライアントが、両方がサポートする CipherSuite でネゴシエートするように設定します。これがデフォルトです。
ステップ 4	<b>end</b> 例：  デバイス (config)# <b>end</b>	特権 EXEC モードに戻ります。

# セキュア HTTP サーバおよびクライアントのステータスのモニタリング

SSLセキュアサーバおよびクライアントのステータスをモニタするには、次の表の特権 EXEC コマンドを使用します。

表 34: SSLセキュアサーバおよびクライアントのステータスを表示するコマンド

コマンド	目的
<code>show ip http client secure status</code>	セキュア HTTP クライアントの設定を表示します。
<code>show ip http server secure status</code>	セキュア HTTP サーバの設定を表示します。
<code>show running-config</code>	セキュア HTTP 接続に対して生成された自己署名証明書を表示します。

## Secure Socket Layer HTTP に関するその他の参考資料

### 関連資料

関連項目	マニュアルタイトル
証明機関	<a href="#">「Configuring Certification Authority Interoperability」</a>

### MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## シスコのテクニカル サポート

説明	リンク
<p>シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。</p> <p>お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service (Field Notice からアクセス)、Cisco Technical Services Newsletter、Really Simple Syndication (RSS) フィードなどの各種サービスに加入できます。</p> <p>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。</p>	<a href="http://www.cisco.com/support">http://www.cisco.com/support</a>

## Secure Socket Layer HTTP の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	Secure Socket Layer HTTP	シスコが実装するセキュア HTTP サーバおよび HTTP クライアントでは、アプリケーション層の暗号化に SSL バージョン 3.0 を使用します。セキュア HTTP 接続の場合、HTTP サーバが送受信するデータは暗号化されてインターネットに送信されます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。





## 第 16 章

### IPv4 ACL

- [ACL によるネットワーク セキュリティに関する情報 \(323 ページ\)](#)
- [IPv4 アクセスコントロールリストの制約事項 \(324 ページ\)](#)
- [ACL を使用したネットワーク セキュリティについて理解する \(325 ページ\)](#)
- [サポートされる ACL \(326 ページ\)](#)
- [ACE およびフラグメント化されたトラフィックとフラグメント化されていないトラフィック \(330 ページ\)](#)
- [ACL とスイッチ スタック \(331 ページ\)](#)
- [標準 IPv4 ACL および拡張 IPv4 ACL \(332 ページ\)](#)
- [ハードウェアおよびソフトウェアによる IP ACL の処理 \(336 ページ\)](#)
- [VLAN マップの設定時の注意事項 \(337 ページ\)](#)
- [VLAN マップとルータ ACL \(338 ページ\)](#)
- [ACL の時間範囲 \(339 ページ\)](#)
- [IPv4 ACL のインターフェイスに関する注意事項 \(340 ページ\)](#)
- [ACL によるネットワーク セキュリティに関する情報 \(340 ページ\)](#)
- [ACL の設定方法 \(340 ページ\)](#)
- [IPv4 ACL のモニタリング \(363 ページ\)](#)
- [ACL の設定例 \(364 ページ\)](#)
- [IPv4 ACL の設定例 \(365 ページ\)](#)
- [ACL および VLAN マップの設定例 \(372 ページ\)](#)
- [ネットワークでの VLAN マップの使用方法の設定例 \(374 ページ\)](#)
- [ACL の設定例 \(377 ページ\)](#)
- [IPv4 アクセスコントロールリストの機能履歴 \(377 ページ\)](#)

## ACL によるネットワーク セキュリティに関する情報

この章では、アクセス コントロール リスト (ACL) を使用して、スイッチのネットワーク セキュリティを設定する方法について説明します。コマンドや表では、ACL をアクセス リストと呼ぶこともあります。

# IPv4 アクセスコントロールリストの制約事項

## 一般的なネットワーク セキュリティ

次は、ACL によるネットワーク セキュリティの設定の制約事項です。

- 番号付き ACL で使用できるすべてのコマンドが名前付き ACL でも使用できるわけではありません。インターフェイスの packets フィルタおよびルート フィルタ用の ACL では、名前を使用できます。また、VLAN マップでも名前を指定できます。
- 標準 ACL と拡張 ACL に同じ名前は使用できません。
- **appletalk** は、コマンドラインのヘルプ スtring に表示されますが、**deny** および **permit** MAC アクセスリスト コンフィギュレーション モード コマンドの一致条件としてサポートされていません。
- ACL ワイルドカードは、ダウンストリーム クライアント ポリシーではサポートされていません。
- プロトコルの TCAM をプログラムしないインターフェイスと、アンロードされた ACL にスケール ACL を適用すると、他のプロトコルのトラフィックの既存の通常移動に影響を与える可能性があります。IPv6 および MAC アドレストラフィックにこの制限は適用されません。
- ルータ ACL は、CPU 生成トラフィックを含むすべてのタイプのトラフィックに適用されます。
- 存続可能時間 (TTL) 分類は、ACL ではサポートされていません。

## IPv4 ACL ネットワーク インターフェイス

次の制限事項が、ネットワーク インターフェイスへの IPv4 ACL に適用されます。

- インターフェイスへのアクセスを制御する場合、名前付き ACL または番号付き ACL を使用できます。
- VLAN に属しているレイヤ 2 インターフェイスに ACL を適用した場合、レイヤ 2 (ポート) ACL は VLAN インターフェイスに適用された入力方向のレイヤ 3 ACL、または VLAN に適用された VLAN マップよりも優先します。
- レイヤ 3 インターフェイスに ACL が適用され、スイッチ上でルーティングがイネーブルになっていない場合は、SNMP、Telnet、Web トラフィックなど、CPU で処理されるパケットだけがフィルタリングされます。
- パケットをフィルタリングするために **preauth\_ipv4\_acl** ACL が設定されている場合、ACL は認証後に削除されます。
- レイヤ 2 インターフェイスに ACL を適用する場合、ルーティングをイネーブルにする必要はありません。

### レイヤ2 インターフェイスの MAC ACL

MAC ACL を作成し、それをレイヤ2 インターフェイスに適用すると、そのインターフェイスに着信する非IP トラフィックをフィルタリングできます。MAC ACL を適用するときには、次の注意事項に留意してください。

- 同じレイヤ2 インターフェイスには、IP アクセス リストと MAC アクセス リストを1つずつしか適用できません。IP アクセス リストはIP パケットだけをフィルタリングし、MAC アクセス リストは非IP パケットをフィルタリングします。
- 1つのレイヤ2 インターフェイスに適用できる MAC アドレス リストは1つだけです。すでに MAC ACL が設定されているレイヤ2 インターフェイスに MAC アクセス リストを適用すると、設定済みの ACL が新しい ACL に置き換えられます。



(注) **mac access-group** インターフェイス コンフィギュレーション コマンドは、物理レイヤ2 インターフェイスに適用される場合のみ有効です。このコマンドは、EtherChannel ポートチャネルでは使用できません。

### IP アクセス リスト エントリ シーケンス番号

- この機能は、ダイナミックアクセスリスト、再帰アクセスリスト、またはファイアウォールアクセス リストをサポートしていません。

# ACL を使用したネットワーク セキュリティについて理解する

## ACL の概要

パケットフィルタリングは、ネットワーク トラフィックを限定し、特定のユーザまたはデバイスによるネットワークの使用を制限するうえで役立ちます。ACL はルータまたはスイッチを通過するトラフィックをフィルタリングし、特定のインターフェイスを通過するパケットを許可または拒否します。ACL は、パケットに適用される許可条件および拒否条件の順序付けられた集まりです。パケットがインターフェイスに着信すると、スイッチはパケット内のフィールドを適用される ACL と比較し、アクセス リストに指定された基準に基づいて、パケットが転送に必要な権限を持っているかどうかを確認します。アクセス リスト内の条件を1つずつ調べ、パケットをテストします。最初に一致した条件によって、スイッチがパケットを受け入れるか拒否するかが決定されます。スイッチは最初に一致した時点でテストを中止するので、リストに条件を指定する順序が重要です。一致する条件がない場合、スイッチはパケットを拒否します。スイッチは、制限条件がない場合はパケットを転送し、制限条件がある場合はパケットをドロップします。スイッチは、転送されるすべてのパケットに ACL を使用します。

ネットワークに基本的なセキュリティを導入する場合は、ルータまたはレイヤ3スイッチにアクセスリストを設定します。ACLを設定しなければ、スイッチを通過するすべてのパケットがネットワークのあらゆる部分で許可される可能性があります。ACLを使用すると、ネットワークの場所ごとにアクセス可能なホストを制御したり、ルータインターフェイスで転送またはブロックされるトラフィックの種類を決定したりできます。たとえば、電子メールトラフィックの転送を許可し、Telnet トラフィックの転送を拒否することもできます。

## アクセスコントロール エントリ

ACLには、アクセスコントロールエントリ（ACE）の順序付けられたリストが含まれています。各ACEには、*permit*または*deny*と、パケットがACEと一致するために満たす必要のある一連の条件を指定します。*permit*または*deny*の意味は、ACLが使用されるコンテキストによって変わります。

## ACLでサポートされるタイプ

スイッチは、IP ACL とイーサネット（MAC）ACL をサポートします。

- IP ACL は、TCP、ユーザデータグラムプロトコル（UDP）、インターネットグループ管理プロトコル（IGMP）、およびインターネット制御メッセージプロトコル（ICMP）などのIPv4トラフィックをフィルタリングします。
- イーサネット ACL は非IPトラフィックをフィルタリングします。

このスイッチは、Quality of Service（QoS）分類ACLもサポートしています。

## サポートされる ACL

スイッチでは、トラフィックをフィルタリングするために、次に示す3種類のACLがサポートされています。

- ポート ACL は、レイヤ2インターフェイスに入るトラフィックをアクセスコントロールします。IPv4とMACどちらのアクセスリストタイプのどの方向に対してでも、レイヤ2インターフェイスにポートACLを適用できます。
- ルータ ACL は、VLAN間でルーティングされたトラフィックのアクセスを制御し、レイヤ3インターフェイスで特定の方向（着信または発信）に適用されます。
- VLAN ACL または VLAN マップはレイヤ2 VLANにのみ適用され、ブリッジされたトラフィックにのみ影響します。VLAN マップを使用すると、同じVLAN内のデバイス間で転送されるトラフィックをフィルタリングできます。VLAN マップは、IPv4のレイヤ3アドレスに基づいてアクセスコントロールするように設定されています。イーサネットACEを使用するとMACアドレスにより、サポートされていないプロトコルがアクセスコントロールされます。VLAN マップをVLANに適用すると、VLANに入るすべてのパケット（ルーテッドパケットまたはブリッジドパケット）がVLANマップと照合されます。パ

ケットは、スイッチポートを介して、または、ルーティングされたパケットの場合、ルーテッドポートを介して、VLAN に入ることができます。

## ACL 優先順位

VLAN マップ、ポート ACL、およびルータ ACL が同じスイッチに設定されている場合、入力トラフィックの場合のフィルタの優先順位は上からポート ACL、VLAN マップ、およびルータ ACL です。出力トラフィックの場合、フィルタの優先順位は、ルータ ACL、VLAN マップ、ポート ACL です。

次の例で、簡単な使用例を説明します。

- 入力ポート ACL と VLAN マップが両方とも適用されている場合に、ポート ACL が適用されたポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。その他のパケットは、VLAN マップによってフィルタリングされます。
- スイッチ仮想インターフェイス (SVI) に入力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。他のポートで受信した着信のルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- SVI に出力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。発信するルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- SVI に VLAN マップ、入力ルータ ACL、および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL だけによってフィルタリングされます。他のポートで受信した着信のルーティング IP パケットには、VLAN マップおよびルータ ACL のフィルタが適用されます。他のパケットには、VLAN マップのフィルタだけが適用されます。
- SVI に VLAN マップ、出力ルータ ACL、および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL だけによってフィルタリングされます。発信するルーティング IP パケットには、VLAN マップおよびルータ ACL のフィルタが適用されます。他のパケットには、VLAN マップのフィルタだけが適用されます。

## ポート ACL

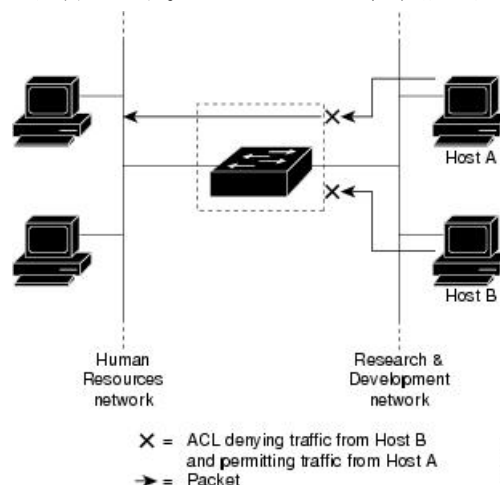
ポート ACL は、スイッチのレイヤ 2 インターフェイスに適用される ACL です。ポート ACL は、物理インターフェイスおよび EtherChannel インターフェイス上でサポートされていますが、EtherChannel メンバーインターフェイスではサポートされていません。ポート ACL は、インバウンド方向とアウトバウンド方向のインターフェイスに適用できます。次のアクセスリストがサポートされています。

- 送信元アドレスを使用する IP アクセス リスト
- 送信元および宛先のアドレスと任意でプロトコル タイプ情報を使用できる拡張 IP アクセス リスト
- 送信元および宛先の MAC アドレスと任意でプロトコル タイプ情報を使用できる MAC 拡張アクセス リスト

スイッチは、インターフェイス上の ACL を調べ、パケットが ACL 内のエントリとどのように一致するかに基づいてパケットの転送を許可または拒否します。このように、ACL がネットワークまたはネットワークの部分へのアクセスを制御します。

図 14: ACL によるネットワーク内のトラフィックの制御

次に、すべてのワークステーションが同じ VLAN にある場合にポート ACL を使用してネットワークへのアクセスを制御する例を示します。レイヤ 2 の着信方向に適用された ACL は、ホスト A がヒューマンリソース ネットワークにアクセスすることを許可しますが、ホスト B が同一のネットワークにアクセスすることは拒否します。ポート ACL は、着信方向のレイヤ 2



インターフェイスだけに適用できます。

ポート ACL をトランク ポートに適用すると、ACL はそのトランク ポート上のすべての VLAN でトラフィックをフィルタリングします。ポート ACL を音声 VLAN ポートに適用すると、ACL はデータ VLAN と音声 VLAN の両方でトラフィックをフィルタリングします。

ポート ACL では、IP アクセスリストを使用して IP トラフィックをフィルタリングでき、MAC アドレスを使用して非 IP トラフィックをフィルタリングできます。同じレイヤ 2 インターフェイス上で IP トラフィックと非 IP トラフィックの両方をフィルタリングするには、そのインターフェイスに IP アクセスリストと MAC アクセスリストの両方を適用します。



- (注) レイヤ 2 インターフェイスに適用できるのは、IP アクセスリスト 1 つと MAC アクセスリスト 1 つだけです。すでに IP アクセス リストまたは MAC アクセス リストが設定されているレイヤ 2 インターフェイスに、新しい IP アクセス リストまたは MAC アクセス リストを適用すると、前に設定した ACL が新しい ACL に置き換わります。

## ルータ ACL

VLAN へのレイヤ 3 インターフェイスであるスイッチ仮想インターフェイス (SVI)、物理層 3 インターフェイス、およびレイヤ 3 EtherChannel インターフェイスに、ルータ ACL を適用できます。ルータ ACL はインターフェイスの特定の方向 (着信または発信) に対して適用されます。1 つのインターフェイスの方向ごとに、ルータ ACL を 1 つ適用できます。

スイッチは、IPv4 トラフィックの次のアクセス リストをサポートしています。

- 標準 IP アクセス リストでは、照合操作に送信元アドレスを使用します。
- 拡張 IP アクセス リストは、送信元アドレス、宛先アドレス、およびオプションのプロトコル タイプ情報を使用して一致処理を行います。

ポート ACL の場合と同様、スイッチはインターフェイスに設定されている機能に関連付けられている ACL が照合されます。パケットがスイッチのインターフェイスに着信すると、そのインターフェイスに設定されているすべての着信機能に対応する ACL が照合されます。パケットがルーティングされてからネクストホップに転送されるまでの間に、出力インターフェイスに設定された発信機能に対応するすべての ACL が照合されます。

ACL は ACL 内のエントリとパケットの一致結果に応じて、パケット転送を許可するか、拒否するかを決めます。ACL を使用すると、ネットワーク全体またはネットワークの一部に対するアクセス コントロールが行えます。

## VLAN マップ

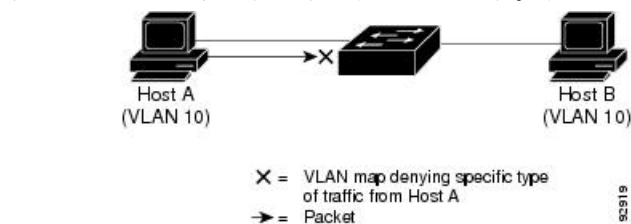
VLAN ACL または VLAN マップは、VLAN 内のネットワークトラフィックを制御するために使用されます。スイッチまたはスイッチ スタックの VLAN 内でブリッジされるすべてのパケットに VLAN マップを適用できます。VACL は、セキュリティ パケット フィルタリング および特定の物理インターフェイスへのトラフィックのリダイレクトだけを目的としたものです。VACL は方向 (入力または出力) で定義されることはありません。

すべての非 IP プロトコルは、MAC VLAN マップを使用して、MAC アドレスおよび Ethertype によってアクセス コントロールされます (IP トラフィックは、MAC VLAN マップではアクセス制御されません)。VLAN マップはスイッチを通過するパケットにだけ適用できます。ハブ上またはこのスイッチに接続された別のスイッチ上のホスト間のトラフィックには、VLAN マップを適用できません。

VLAN マップを使用すると、マップに指定されたアクションに基づいてパケットの転送が許可または拒否されます。

図 15: VLAN マップによるトラフィックの制御

次の図に、VLAN マップを適用して、特定のトラフィック タイプを VLAN 10 のホスト A から転送できないように設定する例を示します。各 VLAN には、VLAN マップを 1 つだけ適用で



きます。

## ACE およびフラグメント化されたトラフィックとフラグメント化されていないトラフィック

IP パケットは、ネットワークを通過するときにフラグメント化されることがあります。その場合、TCP または UDP ポート番号や ICMP タイプおよびコードなどのレイヤ 4 情報は、パケットの最初の部分があるフラグメントだけに含まれます。他のフラグメントには、この情報はありません。

アクセス コントロール エントリ (ACE) には、レイヤ 4 情報をチェックしないため、すべてのパケットフラグメントに適用されるものがあります。レイヤ 4 情報を調べる ACE は、フラグメント化された IP パケットのほとんどのフラグメントに標準的な方法では適用できません。フラグメントにレイヤ 4 情報が含まれておらず、ACE が一部のレイヤ 4 情報をチェックする場合、一致ルールは次のように変更されます。

- フラグメント内のレイヤ 3 情報 (TCP や UDP などのプロトコルタイプを含む) をチェックする許可 ACE は、含まれていないレイヤ 4 情報の種類にかかわらず、フラグメントと一致すると見なされます。



(注) L4 Ops をともなう ACE の TCP では、フラグメント化パケットは RFC 1858 ごとにドロップします。

- レイヤ 4 情報をチェックする拒否 ACE は、フラグメントにレイヤ 4 情報が含まれていない限り、フラグメントと一致しません。

## ACE およびフラグメント化されたトラフィックとフラグメント化されていないトラフィックの例

次のコマンドで構成され、フラグメント化された 3 つのパケットに適用されるアクセスリスト 102 を例にとって説明します。



```
デバイス(config)# access-list 102 permit tcp any host 10.1.1.1 eq smtp
デバイス(config)# access-list 102 deny tcp any host 10.1.1.2 eq telnet
デバイス(config)# access-list 102 permit tcp any host 10.1.1.2
デバイス(config)# access-list 102 deny tcp any any
```



(注) 最初の2つのACEには宛先アドレスの後に *eq* キーワードがありますが、これは既知のTCP宛先ポート番号がそれぞれシンプルメール転送プロトコル (SMTP) およびTelnetと一致するかどうかをチェックすることを意味します。

- パケットAは、ホスト10.2.2.2のポート65000からホスト10.1.1.1のSMTPポートに送信されるTCPパケットです。このパケットがフラグメント化された場合、レイヤ4情報がすべて揃っているため、完全なパケットである場合と同じように最初のフラグメントが最初のACE (permit) と一致します。残りのフラグメントも最初のACEと一致します。これは、それらのフラグメントにSMTPポート情報が含まれていなくても、最初のACEが適用されたときにレイヤ3情報だけをチェックするからです。この例の情報は、パケットがTCPであることと、宛先が10.1.1.1であることです。
- パケットBは、ホスト10.2.2.2のポート65001からホスト10.1.1.2のTelnetポートに送信されます。このパケットがフラグメント化された場合、レイヤ3情報とレイヤ4情報がすべて揃っているため、最初のフラグメントが2つめのACE (deny) と一致します。残りのフラグメントは、レイヤ4情報が含まれていないため、2つめのACEと一致しません。残りのフラグメントは3つめのACE (permit) と一致します。

最初のフラグメントが拒否されたため、ホスト10.1.1.2は完全なパケットを再構成できず、その結果、パケットBは拒否されます。ただし、以降の許可されたフラグメントがネットワークの帯域幅を使用し、ホスト10.1.1.2がパケットを再構成しようとするときにホストのリソースが消費されます。

- フラグメント化されたパケットCは、ホスト10.2.2.2のポート65001からホスト10.1.1.3のポートftpに送信されます。このパケットがフラグメント化された場合、最初のフラグメントが4つめのACE (deny) と一致します。ACEはレイヤ4情報をチェックせず、すべてのフラグメントのレイヤ3情報に宛先がホスト10.1.1.3であることが示され、前のpermitACEは異なるホストをチェックしていたため、他のフラグメントもすべて4つめのACEと一致します。

## ACLとスイッチスタック

スイッチスタックのACLサポートは、スタンドアロンスイッチと同じです。ACLの構成情報は、スタック内のすべてのスイッチに送信されます。アクティブスイッチを含むスタック内のすべてのスイッチでは、情報が処理され、ハードウェアがプログラムされます。

## アクティブスイッチおよび ACL の機能

アクティブスイッチにより、次の ACL 機能が実行されます。

- ACL 構成情報が処理され、情報がすべてのスタックメンバに送信されます。
- ACL 情報は、スタックに加入しているすべてのスイッチに配信されます。
- (たとえば、十分なハードウェアリソースがないなど) 何らかの理由で、ソフトウェアによってパケットが送信される必要がある場合、ACL をパケットに適用後にのみ、アクティブスイッチによってパケットが転送されます。
- そのハードウェアは、処理する ACL 情報でプログラムされます。

## スタックメンバおよび ACL の機能

スタックメンバにより、次の ACL 機能が実行されます。

- スタックメンバでは、アクティブスイッチから ACL 情報を受信し、ハードウェアがプログラムされます。
- スタンバイスイッチとして設定されたスタックメンバがアクティブスイッチが失敗したイベント内のアクティブスイッチ機能を実行します。

## アクティブスイッチの障害および ACL

アクティブとスタンバイの両方のスイッチに ACL 情報があります。アクティブスイッチに障害が発生すると、スタンバイが役割を引き継ぎます。新しいアクティブスイッチにより、すべてのスタックメンバに ACL 情報が配信されます。

## 標準 IPv4 ACL および拡張 IPv4 ACL

ここでは、IP ACL について説明します。

ACL は、許可条件と拒否条件の順序付けられた集まりです。スイッチは、アクセスリスト内の条件を1つずつ調べ、パケットをテストします。最初に一致した条件によって、スイッチがパケットを受け入れるか拒否するかが決定されます。スイッチは一致する最初の条件が見つかった時点でパケットのテストを停止するため、条件の順序が重要な意味を持ちます。一致する条件がない場合、スイッチはパケットを拒否します。

このソフトウェアは、IPv4 について次の ACL (アクセスリスト) をサポートします。

- 標準 IP アクセスリストでは、照合操作に送信元アドレスを使用します。
- 拡張 IP アクセスリストでは、照合操作に送信元アドレスと宛先アドレスを使用し、任意でプロトコルタイプ情報を使用して制御のきめ細かさを高めることもできます。

## IPv4 ACL スイッチでサポートされていない機能

このスイッチで IPv4 ACL を設定する手順は、他の Cisco スイッチやルータで IPv4 ACL を設定する手順と同じです。

以下の ACL 関連の機能はサポートされていません。

- 非 IP プロトコル ACL または
- IP アカウンティング
- 再帰 ACL およびダイナミック ACL はサポートされていません。

## アクセス リスト番号

ACL を識別するために使用する番号は、作成するアクセス リストのタイプを表します。

次の一覧に、アクセス リスト番号と対応するアクセス リスト タイプを挙げ、このスイッチでサポートされているかどうかを示します。このスイッチは、IPv4 標準アクセス リストおよび拡張アクセス リスト（1～199 および 1300～2699）をサポートします。

表 35: アクセス リスト番号

アクセス リスト番号	タイプ	サポートあり
1～99	IP 標準アクセス リスト	あり
100～199	IP 拡張アクセス リスト	あり
200～299	プロトコルタイプコードアクセス リスト	なし
300～399	DECnet アクセス リスト	なし
400～499	XNS 標準アクセス リスト	なし
500～599	XNS 拡張アクセス リスト	なし
600～699	AppleTalk アクセス リスト	なし
700～799	48 ビット MAC アドレス アクセス リスト	なし
800～899	IPX 標準アクセス リスト	なし
900～999	IPX 拡張アクセス リスト	なし
1000～1099	IPX SAP アクセス リスト	なし
1100～1199	拡張 48 ビット MAC サマリー アドレス アクセス リスト	なし
1200～1299	IPX サマリー アドレス アクセス リスト	なし

アクセス リスト番号	タイプ	サポートあり
1300 ~ 1999	IP 標準アクセス リスト (拡張範囲)	あり
2000 ~ 2699	IP 拡張アクセス リスト (拡張範囲)	あり

番号付き標準 ACL および番号付き拡張 ACL に加え、サポートされる番号を使用して名前付き標準 ACL および名前付き拡張 ACL も作成できます。標準 IP ACL の名前は 1 ~ 99 で、拡張 IP ACL の名前は 100 ~ 199 です。番号付きリストの代わりに名前付き ACL を使用することには、エントリを個別に削除できるという利点があります。

## 番号付き標準 IPv4 ACL

ACL を作成するときには、ACL の末尾にデフォルトで暗黙的な `deny` ステートメントが追加され、ACL の終わりに到達するまで一致する条件が見つからなかったすべてのパケットに適用されることに注意してください。標準アクセス リストでは、関連付けられた IP ホストアドレス ACL の指定からマスクを省略すると、`0.0.0.0` がマスクと見なされます。

スイッチは、**host** 一致条件があるエントリと `don't care` マスク `0.0.0.0` を含む一致条件があるエントリがリストの先頭に移動し、**0** 以外の `don't care` マスクを含むエントリよりも前に位置するように、標準アクセス リストの順序を書き換えます。そのため、`show` コマンドの出力やコンフィギュレーション ファイルでは、ACE が必ずしも入力されたとおりの順序で配置されません。

作成した番号付き標準 IPv4 ACL を、端末回線、またはインターフェイスに適用できます。

## 番号付き拡張 IPv4 ACL

標準 ACL では照合に送信元アドレスだけを使用しますが、拡張 ACL では、照合操作に送信元アドレスと宛先アドレスを使用でき、任意でプロトコルタイプ情報を使用して制御のきめ細かさが高めることができます。番号付き拡張アクセス リストの ACE を作成するときには、作成した ACE がリストの末尾に追加されることに注意してください。番号付きリストでは、ACE の順序を変更したり、リスト内の特定の場所に対して ACE を追加または削除したりできません。

このスイッチは、ダイナミックまたは再帰アクセス リストをサポートしていません。また、タイプ オブ サービス (ToS) の `minimize-monetary-cost` ビットに基づくフィルタリングもサポートしていません。

一部のプロトコルには、特定のパラメータやキーワードも適用されます。

拡張 TCP、UDP、ICMP、IGMP、またはその他の IP ACL を定義できます。また、このスイッチはこれらの IP プロトコルをサポートします。



(注) ICMP エコー応答はフィルタリングできません。他の ICMP コードまたはタイプは、すべてフィルタリングできます。

これらの IP プロトコルがサポートされます。

- 認証ヘッダー プロトコル (**ahp**)
- カプセル化セキュリティペイロード (**esp**)
- Enhanced Interior Gateway Routing Protocol (**eigrp**)
- 総称ルーティング カプセル化 (**gre**)
- インターネット制御メッセージプロトコル (**icmp**)
- インターネット グループ管理プロトコル (**igmp**)
- すべての内部プロトコル (**ip**)
- IP-in-IP トンネリング (**ipinip**)
- KA9Q NOS 互換 IP over IP トンネリング (**nos**)
- Open Shortest Path First ルーティング (**ospf**)
- ペイロード圧縮プロトコル (**pcp**)
- プロトコル独立マルチキャスト (**pim**)
- 伝送制御プロトコル (**tcp**)
- ユーザ データグラム プロトコル (**udp**)

## 名前付き IPv4 ACL

IPv4 ACL を識別する手段として、番号ではなく英数字のストリング (名前) を使用できます。名前付き ACL を使用すると、ルータ上で番号付きアクセスリストの場合より多くの IPv4 アクセス リストを設定できます。アクセス リストの識別手段として名前を使用する場合のモードとコマンド構文は、番号を使用する場合とは多少異なります。ただし、IP アクセス リストを使用するすべてのコマンドを名前付きアクセス リストで使用できるわけではありません。



- (注) 標準 ACL または拡張 ACL に指定する名前は、アクセスリスト番号のサポートされる範囲内の番号にすることもできます。標準 IP ACL の名前は 1 ~ 99 です。番号付きリストの代わりに名前付き ACL を使用することには、エントリを個別に削除できるという利点があります。

名前付き ACL を設定するときには、次の注意事項に留意してください。

- また、番号付き ACL も使用できます。
- 標準 ACL と拡張 ACL に同じ名前は使用できません。

## ACL ロギング

標準 IP アクセスリストによって許可または拒否されたパケットに関するログメッセージが、デバイスのソフトウェアによって表示されます。つまり、ACL と一致するパケットがあった場合は、そのパケットに関するログ通知メッセージがコンソールに送信されます。コンソールに表示されるメッセージのレベルは、syslog メッセージを管理する **logging console** コマンドで管理されます。



(注) ACL ロギングは、Unicast Reverse Path Forwarding (uRPF) で使用される ACL ではサポートされません。ルータ ACL でのみサポートされます。



(注) ルーティングはハードウェアで、ロギングはソフトウェアで実行されます。したがって、**log** キーワードを含む許可 (*permit*) または拒否 (*deny*) ACE と一致するパケットが多数存在する場合、ソフトウェアはハードウェアの処理速度に追いつくことができないため、一部のパケットはロギングされない場合があります。

ACL を起動した最初のパケットについては、ログメッセージがすぐに表示されますが、それ以降のパケットについては、5 分間の収集時間が経過してから表示またはロギングされます。ログメッセージにはアクセス リスト番号、パケットの許可または拒否に関する状況、パケットの送信元 IP アドレス、および直前の 5 分間に許可または拒否された送信元からのパケット数が示されます。



(注) ロギングメッセージが多すぎて処理できない場合、または 1 秒以内に処理する必要があるロギングメッセージが複数ある場合、ロギング設備ではロギングメッセージパケットの一部をドロップすることがあります。この動作によって、ロギングメッセージが多すぎてデバイスがクラッシュすることを回避します。そのため、課金ツールや、アクセスリストと一致する数の正確な情報源としてロギング設備を使用しないでください。

## ハードウェアおよびソフトウェアによる IP ACL の処理

ACL 処理はハードウェアで実行されます。ハードウェアで ACL の設定を保存する領域が不足すると、そのインターフェイス上のすべてのパケットがドロップします。



(注) スイッチまたはスタック メンバーのリソース不足が原因でハードウェアに ACL を設定できない場合、影響を受けるのは、スイッチに着信した該当 VLAN 内のトラフィックだけです。

ルータ ACL の場合は、次の場合にパケットが CPU に送信されることがあります。

- **log** キーワードの使用
- ICMP 到達不能メッセージを生成する。

**show ip access-lists** 特権 EXEC コマンドを入力した場合、表示される一致カウントには、ハードウェアでアクセスが制御されるパケットは含まれません。スイッチドパケットおよびルーテッドパケットに関するハードウェアの ACL の基本的な統計情報を取得する場合は、**show platform software fed switch { switch\_num | active | standby } acl counters hardware** 特権 EXEC コマンドを使用します。

ルータ ACL の機能は、次のとおりです。

- 標準 ACL および拡張 ACL (入力および出力) の許可アクションや拒否アクションをハードウェアで制御し、アクセスコントロールのセキュリティを強化します。
- *ip unreachable* が無効の場合、**log** を指定しないと、セキュリティ ACL の *deny* ステートメントと一致するフローがハードウェアによってドロップされます。許可ステートメントと一致するフローは、ハードウェアでスイッチングされます。
- ルータ ACL の ACE に **log** キーワードを追加すると、パケットのコピーが CPU に送信され、ロギングだけが行われます。ACE が許可ステートメントの場合も、パケットはハードウェアでスイッチングおよびルーティングされます。

## VLAN マップの設定時の注意事項

VLAN マップは、VLAN 内でフィルタリングを制御する唯一の方法です。VLAN マップには方向の指定がありません。VLAN マップを使用して、特定の方向のトラフィックをフィルタリングするには、特定の送信元または宛先アドレスが指定された ACL を追加する必要があります。VLAN マップ内に該当パケットタイプ (IP または MAC) に対する **match** 句がある場合、デフォルトでは、マップ内のどのエントリにも一致しないパケットはドロップされます。該当パケットタイプに対する **match** コマンドがない場合、デフォルトでは、パケットが転送されます。

次は、VLAN マップ設定の注意事項です。

- インターフェイスでトラフィックを拒否するように設定された ACL がなく、VLAN マップが設定されていない場合、すべてのトラフィックが許可されます。
- 各 VLAN マップは一連のエントリで構成されます。VLAN マップのエントリの順序は重要です。スイッチに着信したパケットは、VLAN マップの最初のエントリに対してテストされます。一致した場合は、VLAN マップのその部分に指定されたアクションが実行されます。一致しなかった場合、パケットはマップ内の次のエントリに対してテストされます。
- 該当パケットタイプ (IP または MAC) に対する **match** 句が VLAN マップに 1 つまたは複数ある場合でも、パケットがそれらの **match** 句に一致しない場合、デフォルトではパケットがドロップされます。該当パケットタイプに対する **match** 句が VLAN マップ内にない場合、デフォルトではパケットが転送されます。

- VLAN マップのロギングはサポートされていません。
- レイヤ 2 インターフェイスに適用された IP アクセス リスト または MAC アクセス リストがスイッチにあって、ポートが属する VLAN に VLAN マップを適用する場合、ポート ACL が VLAN マップに優先します。
- ハードウェアに VLAN マップの設定を適用できない場合は、その VLAN 内のすべてのパケットがドロップします。

## VLAN マップとルータ ACL

ブリッジングされたトラフィックおよびルーティングされたトラフィックの両方に対してアクセスコントロールを行うには、VLAN マップを単独で使用するか、またはルータ ACL と VLAN マップを組み合わせて使用します。入力と出力両方のルーテッド VLAN インターフェイスでルータ ACL を定義したり、ブリッジングされたトラフィックのアクセスをコントロールする VLAN マップを定義したりできます。

パケットフローが ACL 内 VLAN マップの deny ステートメントと一致した場合、ルータ ACL の設定に関係なく、パケットフローは拒否されます。



- (注) ルータ ACL を VLAN マップと組み合わせて使用し、ルータ ACL でのロギングを必要とするパケットが VLAN マップで拒否された場合、これらのパケットはロギングされません。

該当パケットタイプ (IP または MAC) に対する match 句が VLAN マップにある場合でも、パケットがそのタイプに一致しない場合、デフォルトではパケットがドロップされます。VLAN マップ内に match 句がなく、アクションが指定されていない場合、どの VLAN マップ エントリとも一致しないパケットは転送されます。

## VLAN マップとルータ ACL の設定時の注意事項

ここに記載された注意事項は、ルータ ACL および VLAN マップを同じ VLAN 上で使用する必要がある設定に適用されます。ルータ ACL および VLAN マップを異なる VLAN に割り当てる設定には、これらの注意事項は適用されません。

ルータ ACL および VLAN マップを同じ VLAN に設定する必要がある場合は、ルータ ACL と VLAN マップの両方の設定に関し、ここで説明する注意事項に従ってください。

- VLAN インターフェイス上の各方向 (入力および出力) に VLAN マップおよびルータの ACL を 1 つずつに限り設定できます。
- 可能な限り、すべてのエントリのアクションが同一で、末尾のデフォルトアクションだけが反対のタイプとなるように ACL を記述します。次のいずれかの形式を使用して、ACL を記述します。

```
permit... permit... permit... deny ip any any
```



または

```
deny... deny... deny... permit ip any any
```

- ACL 内で複数のアクション（許可、拒否）を定義する場合は、それぞれのアクションタイプをまとめて、エントリ数を削減します。
- ACL 内にレイヤ 4 情報を指定しないでください。レイヤ 4 情報を追加すると、統合プロセスが複雑になります。ACL のフィルタリングが、full-flow（送信元 IP アドレス、宛先 IP アドレス、プロトコル、およびプロトコルポート）でなく、IP アドレス（送信元および宛先）に基づいて行われる場合に、最適な統合結果が得られます。可能な限り、IP アドレスには *don't care* ビットを使用してください。

IP ACE とレイヤ 4 情報を含む TCP/UDP/ICMP ACE が両方とも ACL 内に存在し、full-flow モードを指定する必要があるときは、レイヤ 4 ACE をリストの末尾に配置します。この結果、IP アドレスに基づくトラフィックのフィルタリングが優先されます。

## ACL の時間範囲

**time-range** グローバル コンフィギュレーション コマンドを使用することによって、時刻および曜日に基づいて拡張 ACL を選択的に適用できます。まず、時間範囲の名前を定義し、その時間範囲内の時刻および日付または曜日を設定します。次に、ACL を適用してアクセスリストに制限を設定するときに時間範囲を入力します。時間範囲を使用すると、ACL の許可ステートメントまたは拒否ステートメントの有効期間（指定期間内や指定曜日など）を定義できます。**time-range** キーワードおよび引数については、名前付きおよび番号付き拡張 ACL タスクの表を参照してください。

時間範囲を使用するいくつかの利点を次に示します。

- アプリケーションなどのリソース（IP アドレスとマスクのペア、およびポート番号で識別）へのユーザアクセスをより厳密に許可または拒否できます。
- ログメッセージを制御できます。ACL エントリを使用して特定の時刻に関してのみトラフィックをロギングできるため、ピーク時間に生成される多数のログを分析しなくても、簡単にアクセスを拒否できます。

時間ベースのアクセスリストを使用すると、CPU に負荷が生じます。これは、アクセスリストの新規設定を他の機能や、ハードウェアメモリにロードされた結合済みの設定とマージする必要があるのでです。そのため、複数のアクセスリストが短期間に連続して（互いに数分以内に）有効となるような設定とならないように注意する必要があります。



- (注) 時間範囲は、スイッチのシステムクロックに基づきます。したがって、信頼できるクロックソースが必要です。ネットワーク タイム プロトコル (NTP) を使用してスイッチクロックを同期させることを推奨します。

## IPv4 ACL のインターフェイスに関する注意事項

**ip access-group** インターフェイス コンフィギュレーション コマンドをレイヤ3 インターフェイス (SVI、レイヤ3 EtherChannel、またはルーテッドポート) に適用するには、そのインターフェイスに IP アドレスが設定されている必要があります。レイヤ3 アクセスグループは、CPU のレイヤ3 プロセスによってルーティングまたは受信されるパケットをフィルタリングします。このグループは、VLAN 内でブリッジングされるパケットに影響を与えません。

インバウンド ACL の場合、パケットの受信後スイッチはパケットを ACL と照合します。ACL がパケットを許可する場合、スイッチはパケットの処理を継続します。ACL がパケットを拒否する場合、スイッチはパケットを廃棄します。

アウトバウンド ACL の場合、パケットを受信し制御対象インターフェイスにルーティングしたあと、スイッチはパケットを ACL と照合します。ACL がパケットを許可する場合、スイッチはパケットを送信します。ACL がパケットを拒否する場合、スイッチはパケットを廃棄します。

デフォルトでは、パケットが廃棄された場合は、その原因が入力インターフェイスの ACL または発信インターフェイスの ACL のいずれであっても、常に入力インターフェイスから ICMP 到達不能メッセージが送信されます。ICMP 到達不能メッセージは通常、入力インターフェイス 1 つにつき、0.5 秒ごとに 1 つだけ生成されます。ただし、この設定は **ip icmp rate-limit unreachable** グローバル コンフィギュレーション コマンドを使用して変更できます。

未定義の ACL をインターフェイスに適用すると、スイッチは ACL がインターフェイスに適用されていないと判断し、すべてのパケットを許可します。ネットワークセキュリティのために未定義の ACL を使用する場合は、このような結果が生じることに注意してください。

## ACL によるネットワーク セキュリティに関する情報

この章では、アクセス コントロール リスト (ACL) を使用して、スイッチのネットワーク セキュリティを設定する方法について説明します。コマンドや表では、ACL をアクセス リストと呼ぶこともあります。

## ACL の設定方法

### IPv4 ACL の設定

このスイッチで IP ACL を使用する手順は次のとおりです。

#### 手順の概要

1. アクセス リストの番号または名前とアクセス条件を指定して、ACL を作成します。

- その ACL をインターフェイスまたは端末回線に適用します。標準および拡張 IP ACL を VLAN マップに適用することもできます。

### 手順の詳細

**ステップ 1** アクセス リストの番号または名前とアクセス条件を指定して、ACL を作成します。

**ステップ 2** その ACL をインターフェイスまたは端末回線に適用します。標準および拡張 IP ACL を VLAN マップに適用することもできます。

## 番号付き標準 ACL の作成

番号付き標準 ACL を作成するには、次の手順に従ってください。

### 手順の概要

- enable**
- configure terminal**
- access-list *access-list-number* {deny | permit} source source-wildcard ]**
- end**
- show running-config**
- copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  デバイス> <b>enable</b>	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  デバイス# <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 3	<b>access-list <i>access-list-number</i> {deny   permit} source source-wildcard ]</b> 例：  デバイス(config)# <b>access-list 2 deny your_host</b>	送信元アドレスとワイルドカードを使用して標準 IPv4 アクセス リストを定義します。  <i>access-list-number</i> には、1 ~ 99 または 1300 ~ 1999 の 10 進数を指定します。

	コマンドまたはアクション	目的
		<p>条件が一致した場合にアクセスを拒否する場合は <b>deny</b> を指定し、許可する場合は <b>permit</b> を指定します。</p> <p><i>source</i> には、パケットの送信元となるネットワークまたはホストのアドレスを次の形式で指定します。</p> <ul style="list-style-type: none"> <li>ドット付き 10 進表記による 32 ビット長の値。</li> <li>キーワード <b>any</b> は 0.0.0.0 255.255.255.255 という <i>source</i> および <i>source-wildcard</i> の省略形です。 <i>source-wildcard</i> を入力する必要はありません。</li> <li>キーワード <b>host</b> は送信元および <i>source</i> 0.0.0.0 の <i>source-wildcard</i> の省略形です。</li> </ul> <p>(任意) <i>source-wildcard</i> は、ワイルドカードビットを送信元アドレスに適用します。</p> <p>(注) ログイングは、レイヤ3インターフェイスに割り当てられた ACL でだけサポートされます。</p>
ステップ 4	<b>end</b> 例： デバイス(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show running-config</b> 例： デバイス# <b>show running-config</b>	入力を確認します。
ステップ 6	<b>copy running-config startup-config</b> 例： デバイス# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## 番号付き拡張 ACL の作成

番号付き拡張 ACL を作成するには、次の手順に従ってください。

## 手順の概要

1. **configure terminal**
2. **access-list** *access-list-number* {deny | permit} *protocol source source-wildcard destination destination-wildcard* [ precedence *precedence*] [tos *tos*] [fragments] [ time-range *time-range-name*] [ dscp *dscp*]
3. **access-list** *access-list-number* {deny | permit} **tcp** *source source-wildcard* [*operator port*] *destination destination-wildcard* [*operator port*] [established] [precedence *precedence*] [tos *tos*] [fragments] [time-range *time-range-name*] [dscp *dscp*] [*flag*]
4. **access-list** *access-list-number* {deny | permit} **udp** *source source-wildcard* [*operator port*] *destination destination-wildcard* [*operator port*] [ precedence *precedence*] [ tos *tos*] [fragments] [ time-range *time-range-name*] [ dscp *dscp*]
5. **access-list** *access-list-number* {deny | permit} **icmp** *source source-wildcard destination destination-wildcard* [*icmp-type* | [[*icmp-type icmp-code*] | [*icmp-message*]]] [ precedence *precedence*] [ tos *tos*] [fragments] [ time-range *time-range-name*] [ dscp *dscp*]
6. **access-list** *access-list-number* {deny | permit} **igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [ precedence *precedence*] [ tos *tos*] [fragments] [ time-range *time-range-name*] [ dscp *dscp*]
7. **end**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例：  デバイス# <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>access-list</b> <i>access-list-number</i> {deny   permit} <i>protocol source source-wildcard destination destination-wildcard</i> [ precedence <i>precedence</i> ] [tos <i>tos</i> ] [fragments] [ time-range <i>time-range-name</i> ] [ dscp <i>dscp</i> ] 例：  デバイス(config)# <b>access-list 101 permit ip host 10.1.1.2 any precedence 0 tos 0 log</b>	拡張 IPv4 アクセス リストおよびアクセス条件を定義します。  <i>access-list-number</i> には、100 ～ 199 または 2000 ～ 2699 の 10 進数を指定します。  条件が一致した場合にパケットを拒否する場合は <b>deny</b> を指定し、許可する場合は <b>permit</b> を指定します。  <i>protocol</i> には、インターネット プロトコルの名前または番号を入力します。 <b>ahp</b> 、 <b>eigrp</b> 、 <b>esp</b> 、 <b>gre</b> 、 <b>icmp</b> 、 <b>igmp</b> 、 <b>igrp</b> 、 <b>ip</b> 、 <b>ipinip</b> 、 <b>nos</b> 、 <b>ospf</b> 、 <b>pcp</b> 、 <b>pim</b> 、 <b>tcp</b> 、 <b>udp</b> 、または IP プロトコル番号を表す 0 ～ 255 の整数を使用できます。一致条件としてインターネット プロトコル (ICMP、TCP、UDP など) を指定するには、キーワード <b>ip</b> を使用します。

	コマンドまたはアクション	目的
		<p>(注) この手順には、ほとんどの IP プロトコルのオプションが含まれています。TCP、UDP、ICMP、および IGMP の追加の特定パラメータについては、次のステップを参照してください。</p> <p><i>source</i> には、パラメータの送信元であるネットワークまたはホストの番号を指定します。</p> <p><i>source-wildcard</i> は、ワイルドカードビットを送信元アドレスに適用します。</p> <p><i>destination</i> には、パラメータの宛先であるネットワークまたはホストの番号を指定します。</p> <p><i>destination-wildcard</i> は、ワイルドカードビットを宛先アドレスに適用します。</p> <p><i>source</i>、<i>source-wildcard</i>、<i>destination</i>、および <i>destination-wildcard</i> の値は、次の形式で指定します。</p> <ul style="list-style-type: none"> <li>• ドット付き 10 進表記による 32 ビット長の値。</li> <li>• 0.0.0.0 255.255.255.255 (任意のホスト) を表すキーワード <b>any</b>。</li> <li>• 単一のホスト 0.0.0.0 を表すキーワード <b>host</b>。</li> </ul> <p>その他のキーワードはオプションであり、次の意味を持ちます。</p> <ul style="list-style-type: none"> <li>• <b>precedence</b> : パケットを 0 ~ 7 の番号または名前で指定する優先度と一致させる場合に入力します。指定できる値は、<b>routine</b> (0)、<b>priority</b> (1)、<b>immediate</b> (2)、<b>flash</b> (3)、<b>flash-override</b> (4)、<b>critical</b> (5)、<b>internet</b> (6)、<b>network</b> (7) です。</li> <li>• <b>fragments</b> : 2つ目以降のフラグメントをチェックする場合に入力します。</li> <li>• <b>tos</b> : パケットを 0 ~ 15 の番号または名前で指定するサービス タイプ レベルと一致させる場合に入力します。指定できる値は、<b>normal</b> (0)、<b>max-reliability</b> (2)、<b>max-throughput</b> (4)、<b>min-delay</b> (8) です。</li> <li>• <b>time-range</b> : 時間範囲の名前を指定します。</li> </ul>

	コマンドまたはアクション	目的
		<p>• <b>dscp</b> : パケットを 0 ～ 63 の番号で指定する DSCP 値と一致させる場合に入力します。または、指定できる値のリストを表示するには、疑問符 (?) を使用します。</p> <p>(注) <b>dscp</b> 値を入力する場合は、<b>tos</b> または <b>precedence</b> を入力できません。<b>dscp</b> を入力せずに <b>tos</b> と <b>precedence</b> の両方の値を入力できます。</p>
<p>ステップ 3</p>	<p><b>access-list</b> <i>access-list-number</i> {<b>deny</b>   <b>permit</b>} <b>tcp</b> <i>source source-wildcard</i> [<i>operator port</i>] <i>destination destination-wildcard</i> [<i>operator port</i>] [<b>established</b>] [<b>precedence precedence</b>] [<b>tos tos</b>] [<b>fragments</b>] [<b>time-range time-range-name</b>] [<b>dscp dscp</b>] [<i>flag</i>]</p> <p>例 :</p> <pre>デバイス(config)# access-list 101 permit tcp any any eq 500</pre>	<p>拡張 TCP アクセス リストおよびアクセス条件を定義します。</p> <p>次に示す例外を除き、拡張 IPv4 ACL に対して説明するパラメータと同じパラメータを使用します。</p> <p>(任意) <i>operator</i> および <i>port</i> を入力すると、送信元ポート (<i>source source-wildcard</i> の後に入力した場合) または宛先ポート (<i>destination destination-wildcard</i> の後に入力した場合) が比較されます。演算子の候補には、<b>eq</b> (次の値に等しい)、<b>gt</b> (次の値より大きい)、<b>lt</b> (次の値より小さい)、<b>neq</b> (次の値に等しくない)、および <b>range</b> (次の範囲) があります。演算子にはポート番号を指定する必要があります (range の場合は 2 つのポート番号をスペースで区切って指定する必要があります)。</p> <p><i>port</i> には、10 進数 (0 ～ 65535) のポート番号または TCP ポート名を入力します。TCP をフィルタリングするときには、TCP ポートの番号または名前だけを使用します。</p> <p>他のオプションのキーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> <li>• <b>established</b> : 確立された接続と照合する場合に入力します。このキーワードは、<b>ack</b> または <b>rst</b> フラグでの照合と同じ機能を果たします。</li> <li>• <b>flag</b> : 指定された TCP ヘッダー ビットを基準にして照合します。入力できるフラグは、<b>ack</b> (確認応答)、<b>fin</b> (終了)、<b>psh</b> (プッシュ)、<b>rst</b> (リセット)、<b>syn</b> (同期)、または <b>urg</b> (緊急) です。</li> </ul>

	コマンドまたはアクション	目的
ステップ 4	<p><b>access-list</b> <i>access-list-number</i> {<b>deny</b>   <b>permit</b>} <b>udp</b> <i>source source-wildcard</i> [<i>operator port</i>] <i>destination destination-wildcard</i> [<i>operator port</i>] [<b>precedence precedence</b>] [<b>tos tos</b>] [<b>fragments</b>] [<b>time-range time-range-name</b>] [<b>dscp dscp</b>]</p> <p>例 :</p> <pre>デバイス(config)# access-list 101 permit udp any any eq 100</pre>	<p>(任意) 拡張 UDP アクセス リストおよびアクセス条件を定義します。</p> <p>UDP パラメータは TCP の説明にあるパラメータと同じです。ただし、[<b>operator [port]</b>] ポート番号またはポート名は、UDP ポートの番号または名前を指定する必要があります。また、UDP では、<b>flag</b> キーワードと <b>established</b> キーワードは無効です。</p>
ステップ 5	<p><b>access-list</b> <i>access-list-number</i> {<b>deny</b>   <b>permit</b>} <b>icmp</b> <i>source source-wildcard destination destination-wildcard</i> [<i>icmp-type</i>   [[<i>icmp-type icmp-code</i>]   [<i>icmp-message</i>]]] [<b>precedence precedence</b>] [<b>tos tos</b>] [<b>fragments</b>] [<b>time-range time-range-name</b>] [<b>dscp dscp</b>]</p> <p>例 :</p> <pre>デバイス(config)# access-list 101 permit icmp any any 200</pre>	<p>拡張 ICMP アクセス リストおよびアクセス条件を定義します。</p> <p>ICMP パラメータは拡張 IPv4 ACL の IP プロトコルの説明にあるパラメータとほとんど同じですが、ICMP メッセージタイプおよびコードパラメータが追加されています。オプションのキーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> <li>• <i>icmp-type</i> : ICMP メッセージタイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ~ 255 です。</li> <li>• <i>icmp-code</i> : ICMP パケットを ICMP メッセージコードタイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ~ 255 です。</li> <li>• <i>icmp-message</i> : ICMP パケットを ICMP メッセージタイプ名または ICMP メッセージタイプとコード名でフィルタリングする場合に入力します。</li> </ul>
ステップ 6	<p><b>access-list</b> <i>access-list-number</i> {<b>deny</b>   <b>permit</b>} <b>igmp</b> <i>source source-wildcard destination destination-wildcard</i> [<i>igmp-type</i>] [<b>precedence precedence</b>] [<b>tos tos</b>] [<b>fragments</b>] [<b>time-range time-range-name</b>] [<b>dscp dscp</b>]</p> <p>例 :</p> <pre>デバイス(config)# access-list 101 permit igmp any any 14</pre>	<p>(任意) 拡張 IGMP アクセス リストおよびアクセス条件を定義します。</p> <p>IGMP パラメータは拡張 IPv4 ACL の IP プロトコルの説明にあるパラメータとほとんど同じですが、次に示すオプションのパラメータが追加されています。</p> <p><i>igmp-type</i> IGMP メッセージタイプと比較するには、0 ~ 15 の番号またはメッセージ名 (<b>dvmrp</b>、<b>host-query</b>、<b>host-report</b>、<b>pim</b>、または <b>trace</b>) を入力します。</p>



	コマンドまたはアクション	目的
ステップ 7	<b>end</b> 例 :  デバイス (config) # <b>end</b>	特権 EXEC モードに戻ります。

## 名前付き標準 ACL の作成

名前を使用して標準 ACL を作成するには、次の手順に従ってください。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **ip access-list standard name**
4. 次のいずれかを使用します。
  - **deny {source [source-wildcard] | host source | any} [log]**
  - **permit {source [source-wildcard] | host source | any} [log]**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 :  デバイス > <b>enable</b>	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例 :  デバイス # <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 3	<b>ip access-list standard name</b> 例 :  デバイス (config) # <b>ip access-list standard 20</b>	名前を使用して標準 IPv4 アクセスリストを定義し、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。  名前には、1 ~ 99 の番号を使用できます。

	コマンドまたはアクション	目的
ステップ 4	<p>次のいずれかを使用します。</p> <ul style="list-style-type: none"> <li>• <b>deny</b> {source [source-wildcard]   host source   any} [log]</li> <li>• <b>permit</b> {source [source-wildcard]   host source   any} [log]</li> </ul> <p>例 :</p> <pre>デバイス(config-std-nacl)# deny 192.168.0.0 0.0.255.255 255.255.0.0 0.0.255.255</pre> <p>または</p> <pre>デバイス(config-std-nacl)# permit 10.108.0.0 0.0.0.0 255.255.255.0 0.0.0.0</pre>	<p>アクセスリストコンフィギュレーションモードで、パケットを転送するかドロップするかを決定する 1 つ以上の拒否条件または許可条件を指定します。</p> <ul style="list-style-type: none"> <li>• <b>host source</b> : 送信元および送信元ワイルドカードの値である source 0.0.0.0。</li> <li>• <b>any</b> : 送信元および送信元ワイルドカードの値である 0.0.0.0 255.255.255.255</li> </ul>
ステップ 5	<p><b>end</b></p> <p>例 :</p> <pre>デバイス(config-std-nacl)# end</pre>	特権 EXEC モードに戻ります。
ステップ 6	<p><b>show running-config</b></p> <p>例 :</p> <pre>デバイス# show running-config</pre>	入力を確認します。
ステップ 7	<p><b>copy running-config startup-config</b></p> <p>例 :</p> <pre>デバイス# copy running-config startup-config</pre>	(任意) コンフィギュレーションファイルに設定を保存します。

## 名前付き拡張 ACL の作成

名前を使用して拡張 ACL を作成するには、次の手順に従ってください。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **ip access-list extended name**

4. `{deny | permit} protocol {source [source-wildcard] | host source | any} {destination [destination-wildcard] | host destination | any} [precedence precedence] [tos tos] [established] [log] [time-range time-range-name]`
5. `end`
6. `show running-config`
7. `copy running-config startup-config`

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  デバイス> <code>enable</code>	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  デバイス# <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 3	<b>ip access-list extended name</b> 例：  デバイス(config)# <code>ip access-list extended 150</code>	名前を使用して拡張 IPv4 アクセスリストを定義し、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。  名前には、100 ~ 199 の番号を使用できます。
ステップ 4	<b>{deny   permit} protocol {source [source-wildcard]   host source   any} {destination [destination-wildcard]   host destination   any} [precedence precedence] [tos tos] [established] [log] [time-range time-range-name]</b> 例：  デバイス(config-ext-nacl)# <code>permit 0 any any</code>	アクセスリストコンフィギュレーションモードで、許可条件または拒否条件を指定します。 <b>log</b> キーワードを使用すると、違反を含むアクセスリストのログメッセージを取得できます。  <ul style="list-style-type: none"> <li>• <b>host source</b> : 送信元および送信元ワイルドカードの値である <code>source 0.0.0.0</code>。</li> <li>• <b>host destination</b> : 接続先および接続先ワイルドカードの値である <code>destination 0.0.0.0</code>。</li> <li>• <b>any</b> : source および source wildcard の値または destination および destination wildcard の値である <code>0.0.0.0 255.255.255.255</code></li> </ul>
ステップ 5	<b>end</b> 例：  デバイス(config-ext-nacl)# <code>end</code>	特権 EXEC 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 6	<b>show running-config</b> 例： デバイス# <b>show running-config</b>	入力を確認します。
ステップ 7	<b>copy running-config startup-config</b> 例： デバイス# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

拡張 ACL を作成するときには、ACL の末尾にデフォルトで暗黙的な **deny** ステートメントが追加され、ACL の終わりに到達するまで一致する条件が見つからなかったすべてのパケットに適用されることに注意してください。標準 ACL では、関連付けられた IP ホストアドレスアクセスリストの指定からマスクを省略すると、**0.0.0.0** がマスクと見なされます。

ACL の作成後に追加したエントリは、リストの末尾に追加されます。ACL エントリを特定の ACL に選択的に追加できません。ただし、**no permit** および **no deny** アクセスリスト コンフィギュレーションモードコマンドを使用すると、名前付き ACL からエントリを削除できます。

番号付き ACL ではなく名前付き ACL を使用する理由の 1 つとして、名前付き ACL では行を選択して削除できることがあります。

### 次のタスク

作成した名前付き ACL は、インターフェイスまたは VLAN に適用できます。

## ACL の時間範囲の設定

ACL の時間範囲パラメータを設定するには、次の手順に従ってください。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **time-range** *time-range-name*
4. 次のいずれかを使用します。
  - **absolute** [ *start time date* ] [ *end time date* ]
  - **periodic** *day-of-the-week hh:mm to [day-of-the-week] hh:mm*
  - **periodic** { *weekdays* | *weekend* | *daily* } *hh:mm to hh:mm*
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 :  デバイス (config) # <b>enable</b>	特権 EXEC モードを有効にします。パスワードを入力します (要求された場合)。
ステップ 2	<b>configure terminal</b> 例 :  デバイス # <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 3	<b>time-range time-range-name</b> 例 :  デバイス (config) # <b>time-range workhours</b>	作成する時間範囲には意味のある名前 ( <i>workhours</i> など) を割り当て、時間範囲コンフィギュレーションモードを開始します。名前にスペースや疑問符を含めることはできません。また、文字から始める必要があります。
ステップ 4	次のいずれかを使用します。 <ul style="list-style-type: none"> <li>• <b>absolute</b> [ <i>start time date</i> ] [ <i>end time date</i> ]</li> <li>• <b>periodic</b> <i>day-of-the-week hh:mm to [day-of-the-week] hh:mm</i></li> <li>• <b>periodic</b> { <i>weekdays</i>   <i>weekend</i>   <i>daily</i> } <i>hh:mm to hh:mm</i></li> </ul> 例 :  デバイス (config-time-range) # <b>absolute start 00:00 1 Jan 2006 end 23:59 1 Jan 2006</b>  または  デバイス (config-time-range) # <b>periodic weekdays 8:00 to 12:00</b>	適用対象の機能がいつ動作可能になるかを指定します。 <ul style="list-style-type: none"> <li>• 時間範囲には、<b>absolute</b> ステートメントを 1 つだけ使用できます。複数の <b>absolute</b> ステートメントを設定した場合は、最後に設定したステートメントだけが実行されます。</li> <li>• 複数の <b>periodic</b> ステートメントを入力できます。たとえば、平日と週末に異なる時間を設定できます。</li> </ul> 設定例を参照してください。
ステップ 5	<b>end</b> 例 :  デバイス (config) # <b>end</b>	特権 EXEC モードに戻ります。
ステップ 6	<b>show running-config</b> 例 :	入力を確認します。

	コマンドまたはアクション	目的
	デバイス# <code>show running-config</code>	
ステップ 7	<b>copy running-config startup-config</b> 例 : デバイス# <code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

### 次のタスク

複数の項目をそれぞれ異なる時間に有効にする場合は、上記の手順を繰り返してください。

## 端末回線への IPv4 ACL の適用

番号付き ACL を使用して、1つまたは複数の端末回線へのアクセスを制御できます。端末回線には名前付き ACL を適用できません。すべての仮想端末回線にユーザが接続する可能性があるため、すべてに同じ制限を設定する必要があります。

仮想端末回線と ACL に指定されたアドレス間の着信接続および発信接続を制限するには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **line [console | vty] line-number**
4. **access-class access-list-number {in | out}**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : デバイス (config)# <b>enable</b>	特権 EXEC モードを有効にします。パスワードを入力します (要求された場合)。
ステップ 2	<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
	デバイス# <code>configure terminal</code>	
ステップ 3	<b>line [console   vty] line-number</b> 例 : デバイス(config)# <code>line console 0</code>	設定する回線を指定し、インライン コンフィギュレーションモードを開始します。 <ul style="list-style-type: none"> <li>• <b>console</b> : コンソール端末回線を指定します。コンソールポートは DCE です。</li> <li>• <b>vty</b> : リモート コンソール アクセス用の仮想端末を指定します。</li> </ul> <i>line-number</i> は、回線タイプを指定する場合に、設定する連続グループ内で最初の回線番号です。指定できる範囲は 0 ~ 16 です。
ステップ 4	<b>access-class access-list-number {in   out}</b> 例 : デバイス(config-line)# <code>access-class 10 in</code>	(デバイスへの) 特定の仮想端末回線とアクセスリストに指定されたアドレス間の着信接続および発信接続を制限します。
ステップ 5	<b>end</b> 例 : デバイス(config-line)# <code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<b>show running-config</b> 例 : デバイス# <code>show running-config</code>	入力を確認します。
ステップ 7	<b>copy running-config startup-config</b> 例 : デバイス# <code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

## インターフェイスへの IPv4 ACL の適用

ここでは、IPv4 ACL をネットワーク インターフェイスへ適用する方法について説明します。インターフェイスへのアクセスを制御する管理には、特権 EXEC モードで次の手順を実行します。

## 手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **ip access-group** {*access-list-number* | *name*} {**in** | **out**}
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例：  デバイス# <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>interface</b> <i>interface-id</i> 例：  デバイス(config)# <b>interface</b> <b>gigabitethernet1/0/1</b>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。 インターフェイスには、レイヤ 2 インターフェイス (ポート ACL) またはレイヤ 3 インターフェイス (ルータ ACL) を指定できます。
ステップ 3	<b>ip access-group</b> { <i>access-list-number</i>   <i>name</i> } { <b>in</b>   <b>out</b> } 例：  デバイス(config-if)# <b>ip access-group</b> <b>2 in</b>	指定されたインターフェイスへのアクセスを制御します。
ステップ 4	<b>end</b> 例：  デバイス(config-if)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show running-config</b> 例：  デバイス# <b>show running-config</b>	アクセス リストの設定を表示します。
ステップ 6	<b>copy running-config startup-config</b> 例：  デバイス# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。



## 名前付き MAC 拡張 ACL の作成

VLAN またはレイヤ 2 インターフェイスで非 IPv4 トラフィックをフィルタリングするには、MAC アドレスおよび名前付き MAC 拡張 ACL を使用します。その手順は、他の名前付き拡張 ACL を設定する場合と同様です。

名前付き MAC 拡張 ACL を作成するには、次の手順に従ってください。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **mac access-list extended name**
4. **{deny | permit} {any | host source MAC address | source MAC address mask} {any | host destination MAC address | destination MAC address mask} [type mask | lsap lsap mask | aarp | amber | dec-spanning | decnet-iv | diagnostic | dsm | etype-6000 | etype-8042 | lat | lavc-sca | mop-console | mop-dump | msdos | mumps | netbios | vines-echo | vines-ip | xns-idp | 0-65535] [cos cos]**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  デバイス> <b>enable</b>	特権 EXEC モードを有効にします。パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  デバイス# <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 3	<b>mac access-list extended name</b> 例：  デバイス(config)# <b>mac access-list extended macl</b>	名前を使用して MAC 拡張アクセス リストを定義します。
ステップ 4	<b>{deny   permit} {any   host source MAC address   source MAC address mask} {any   host destination MAC address   destination MAC address mask} [type mask   lsap lsap mask   aarp   amber   dec-spanning   decnet-iv   diagnostic   dsm   etype-6000   etype-8042   lat   lavc-sca</b>	拡張 MAC アクセス リスト コンフィギュレーション モードでは、すべての送信元 MAC アドレス、マスク付き送信元 MAC アドレス、または特定の <b>host</b> の送信元 MAC アドレスと、 <b>any</b> の宛先 MAC アドレス、マスク付き宛先 MAC アドレス、または特定の

	コマンドまたはアクション	目的
	<p>  <b>mop-console</b>   <b>mop-dump</b>   <b>msdos</b>   <b>mumps</b>   <b>netbios</b>   <b>vines-echo</b>   <b>vines-ip</b>   <b>xns-idp</b>   0-65535] [ <b>cos</b> <i>cos</i>]</p> <p>例 :</p> <pre>デバイス(config-ext-macl)# deny any any decnet-iv</pre> <p>または</p> <pre>デバイス(config-ext-macl)# permit any any</pre>	<p>宛先 MAC アドレスに、<b>permit</b> または <b>deny</b> を指定します。</p> <p>(任意) 次のオプションを入力することもできます。</p> <ul style="list-style-type: none"> <li>• <b>type mask</b> : Ethernet II または SNAP でカプセル化されたパケットの任意の EtherType 番号。10 進数、16 進数、または 8 進数で表記できます。一致検査の前に、任意で指定できる <i>don't care</i> ビットのマスクが EtherType に適用されます。</li> <li>• <b>lsap lsap mask</b> : IEEE 802.2 でカプセル化されたパケットの LSAP 番号。10 進数、16 進数、または 8 進数で表記できます。任意で <i>don't care</i> ビットのマスクを指定できます。</li> <li>• <b>aarp</b>   <b>amber</b>   <b>dec-spanning</b>   <b>decnet-iv</b>   <b>diagnostic</b>   <b>dsm</b>   <b>etype-6000</b>   <b>etype-8042</b>   <b>lat</b>   <b>lavc-sca</b>   <b>mop-console</b>   <b>mop-dump</b>   <b>msdos</b>   <b>mumps</b>   <b>netbios</b>   <b>vines-echo</b>   <b>vines-ip</b>   <b>xns-idp</b> : 非 IP プロトコル。</li> <li>• <b>cos</b> <i>cos</i> : プライオリティを設定する 0 ~ 7 の IEEE 802.1Q CoS 番号。</li> </ul>
ステップ 5	<p><b>end</b></p> <p>例 :</p> <pre>デバイス(config-ext-macl)# end</pre>	<p>特権 EXEC モードに戻ります。</p>
ステップ 6	<p><b>show running-config</b></p> <p>例 :</p> <pre>デバイス# show running-config</pre>	<p>入力を確認します。</p>
ステップ 7	<p><b>copy running-config startup-config</b></p> <p>例 :</p> <pre>デバイス# copy running-config startup-config</pre>	<p>(任意) コンフィギュレーションファイルに設定を保存します。</p>

## レイヤ2 インターフェイスへの MAC ACL の適用

レイヤ2 インターフェイスへのアクセスを制御するために MAC アクセス リストを適用するには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **interface *interface-id***
4. **mac access-group {*name*} {*in*}**
5. **end**
6. **show mac access-group [ interface *interface-id*]**
7. **show running-config**
8. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  デバイス> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  デバイス# <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 3	<b>interface <i>interface-id</i></b> 例：  デバイス(config)# <b>interface gigabitethernet1/0/2</b>	特定の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。指定するインターフェイスは物理レイヤ2 インターフェイス（ポート ACL）でなければなりません。
ステップ 4	<b>mac access-group {<i>name</i>} {<i>in</i>}</b> 例：  デバイス(config-if)# <b>mac access-group mac1 in</b>	MAC アクセス リストを使用して、指定されたインターフェイスへのアクセスを制御します。  ポート ACL は着信方向サポートされます。
ステップ 5	<b>end</b> 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	デバイス (config-if) # <b>end</b>	
ステップ 6	<b>show mac access-group [ interface interface-id]</b> 例 :  デバイス # <b>show mac access-group interface gigabitethernet1/0/2</b>	そのインターフェイスまたはすべてのレイヤ 2 インターフェイスに適用されている MAC アクセス リストを表示します。
ステップ 7	<b>show running-config</b> 例 :  デバイス # <b>show running-config</b>	入力を確認します。
ステップ 8	<b>copy running-config startup-config</b> 例 :  デバイス # <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

スイッチは、パケットを受信すると、着信 ACL とパケットを照合します。ACL がパケットを許可する場合、スイッチはパケットの処理を継続します。ACL がパケットを拒否する場合、スイッチはパケットを廃棄します。未定義の ACL をインターフェイスに適用すると、スイッチは ACL がインターフェイスに適用されていないと判断し、すべてのパケットを許可します。ネットワーク セキュリティのために未定義の ACL を使用する場合は、このような結果が生じることに注意してください。

## VLAN マップの設定

VLAN マップを作成して、1 つまたは複数の VLAN に適用するには、次のステップを実行します。

### 始める前に

VLAN に適用する標準 IPv4 ACL または拡張 IP ACL、または名前付き MAC 拡張 ACL を作成します。

### 手順の概要

1. **vlan access-map name [number]**
2. **match {ip | mac} address {name | number} [name | number]**

3. IP パケットまたは非 IP パケットを（既知の 1 MAC アドレスのみを使って）指定し、1 つ以上の ACL（標準または拡張）とそのパケットを照合するには、次のコマンドのいずれかを入力します。

- **action { forward }**

```
デバイス(config-access-map)# action forward
```

- **action { drop }**

```
デバイス(config-access-map)# action drop
```

#### 4. `vlan filter mapname vlan-list list`

#### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<p><b>vlan access-map name [number]</b></p> <p>例 :</p> <pre>デバイス(config)# vlan access-map map_1 20</pre>	<p>VLAN マップを作成し、名前と、任意で番号を付けます。番号は、マップ内のエントリのシーケンス番号です。</p> <p>同じ名前の VLAN マップを作成すると、10 ずつ増加する番号が順に割り当てられます。マップを変更または削除するときは、該当するマップエントリの番号を入力できます。</p> <p>VLAN マップでは、特定の <code>permit</code> または <code>deny</code> キーワードを使用しません。VLAN マップを使用してパケットを拒否するには、パケットを照合する ACL を作成して、アクションをドロップに設定します。ACL 内の <code>permit</code> は、一致するという意味です。ACL 内の <code>deny</code> は、一致しないという意味です。</p> <p>このコマンドを入力すると、アクセス マップ コンフィギュレーション モードに変わります。</p>
ステップ 2	<p><b>match {ip   mac} address {name   number} [name   number]</b></p> <p>例 :</p> <pre>デバイス(config-access-map)# match ip address ip2</pre>	<p>1 つまたは複数の標準または拡張アクセスリストに対してパケットを照合します（IP または MAC アドレスを使用）。パケットの照合は、対応するプロトコルタイプのアクセスリストに対してだけ行われます。IP パケットは、標準または拡張 IP アクセスリストに対して照合されます。非 IP パケットは、名前付き MAC 拡張アクセスリストに対してだけ照合されます。</p>

	コマンドまたはアクション	目的
		<p>(注) パケットタイプ (IP または MAC) に対する <b>match</b> 句が VLAN マップに設定されている場合で、そのマップアクションがドロップの場合は、そのタイプに一致するすべてのパケットがドロップされます。<b>match</b> 句が VLAN マップになく、設定されているアクションがドロップの場合は、すべての IP およびレイヤ 2 パケットがドロップされます。</p>
<b>ステップ 3</b>	<p>IP パケットまたは非 IP パケットを (既知の 1 MAC アドレスのみを使って) 指定し、1 つ以上の ACL (標準または拡張) とそのパケットを照合するには、次のコマンドのいずれかを入力します。</p> <ul style="list-style-type: none"> <li>• <b>action { forward }</b></li> </ul> <pre>デバイス(config-access-map) # action forward</pre> <ul style="list-style-type: none"> <li>• <b>action { drop }</b></li> </ul> <pre>デバイス(config-access-map) # action drop</pre>	<p>マップエントリに対するアクションを設定します。</p>
<b>ステップ 4</b>	<p><b>vlan filter mapname vlan-list list</b></p> <p>例 :</p> <pre>デバイス(config) # vlan filter map 1 vlan-list 20-22</pre>	<p>VLAN マップを 1 つまたは複数の VLAN に適用します。</p> <p>list には単一の VLAN ID (22)、連続した範囲 (10 ~ 22)、または VLAN ID のストリング (12、22、30) を指定できます。カンマやハイフンの前後にスペースを挿入することもできます。</p>

## VLAN マップの作成

各 VLAN マップは順番に並べられた一連のエントリで構成されます。VLAN マップ エントリを作成、追加、または削除するには、特権 EXEC モードで次の手順を実行します。

### 手順の概要

1. **configure terminal**
2. **vlan access-map name [number]**
3. **match {ip | mac} address {name | number} [name | number]**
4. **action {drop | forward}**
5. **end**

6. show running-config
7. copy running-config startup-config

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 :  デバイス# <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>vlan access-map name [number]</b> 例 :  デバイス (config)# <b>vlan access-map map_1 20</b>	<p>VLAN マップを作成し、名前と、任意で番号を付けます。番号は、マップ内のエントリのシーケンス番号です。</p> <p>同じ名前の VLAN マップを作成すると、10 ずつ増加する番号が順に割り当てられます。マップを変更または削除するときは、該当するマップエントリの番号を入力できます。</p> <p>VLAN マップでは、特定の permit または deny キーワードを使用しません。VLAN マップを使用してパケットを拒否するには、パケットを照合する ACL を作成して、アクションをドロップに設定します。ACL 内の permit は、一致するという意味です。ACL 内の deny は、一致しないという意味です。</p> <p>このコマンドを入力すると、アクセス マップ コンフィギュレーション モードに変わります。</p>
ステップ 3	<b>match {ip   mac} address {name   number} [name   number]</b> 例 :  デバイス (config-access-map)# <b>match ip address ip2</b>	1 つまたは複数の標準または拡張アクセスリストに対してパケットを照合します (IP または MAC アドレスを使用)。パケットの照合は、対応するプロトコルタイプのアクセスリストに対してだけ行われます。IP パケットは、標準または拡張 IP アクセスリストに対して照合されます。非 IP パケットは、名前付き MAC 拡張アクセスリストに対してだけ照合されます。
ステップ 4	<b>action {drop   forward}</b> 例 :  デバイス (config-access-map)# <b>action forward</b>	(任意) マップエントリに対するアクションを設定します。デフォルトは転送 (forward) です。
ステップ 5	<b>end</b> 例 :	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
	デバイス (config-access-map) # <b>end</b>	
ステップ 6	<b>show running-config</b> 例： デバイス # <b>show running-config</b>	アクセス リストの設定を表示します。
ステップ 7	<b>copy running-config startup-config</b> 例： デバイス # <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## VLAN への VLAN マップの適用

VLAN マップを 1 つまたは複数の VLAN に適用するには、次の手順に従います。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **vlan filter mapname vlan-list list**
4. **end**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例： Device# <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 3	<b>vlan filter mapname vlan-list list</b> 例： Device(config)# <b>vlan filter map 1 vlan-list 20-22</b>	VLAN マップを 1 つまたは複数の VLAN に適用します。 list には単一の VLAN ID (22)、連続した範囲 (10 ~ 22)、または VLAN ID のストリング (12、22、30) を指定できます。カンマやハイフンの前後にスペースを挿入することもできます。



	コマンドまたはアクション	目的
ステップ 4	<b>end</b> 例 : Device(config)# <b>end</b>	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。

## IPv4 ACL のモニタリング

スイッチに設定されている ACL、およびインターフェイスと VLAN に適用された ACL を表示して IPv4 ACL をモニターできます。

**ip access-group** インターフェイス コンフィギュレーション コマンドを使用して、レイヤ 2 またはレイヤ 3 インターフェイスに ACL を適用した場合は、そのインターフェイスのアクセスグループを表示できます。また、レイヤ 2 インターフェイスに適用された MAC ACL も表示できます。この情報を表示するには、次の表に記載された特権 EXEC コマンドを使用します。

表 36: アクセス リストおよびアクセスグループを表示するコマンド

コマンド	目的
<b>show access-lists</b> [ <i>number</i>   <i>name</i> ]	最新の IP および MAC アドレス アクセス リストの全体または特定のアクセスリスト（番号付きまたは名前付き）を表示します。
<b>show ip access-lists</b> [ <i>number</i>   <i>name</i> ]	最新の IP アクセスリスト全体、または特定の IP アクセスリスト（番号付きまたは名前付き）を表示します。
<b>show ip interface</b> <i>interface-id</i>	インターフェイスの詳細設定およびステータスを表示します。ネーブルになっているインターフェイスに、 <b>ip access-group</b> コマンドを使用してアクセスグループが適用されている場合は、アクセスグループも表示に含まれます。
<b>show running-config</b> [ <i>interface interface-id</i> ]	スイッチまたは指定されたインターフェイスのコンフィギュレーション ファイルの内容（設定されたすべての MAC および IP アクセスリストや、どのアクセスグループがインターフェイスに適用されているか）を表示します。
<b>show mac access-group</b> [ <i>interface interface-id</i> ]	すべてのレイヤ 2 インターフェイスまたは指定されたインターフェイスに適用されている MAC アクセス リストを表示します。

## ACL の設定例

### 例：ACL での時間範囲を使用

次の例に、*workhours*（営業時間）の時間範囲および会社の休日（2006年1月1日）を設定し、設定を確認する例を示します。

```
デバイス# show time-range
time-range entry: new_year_day_2003 (inactive)
    absolute start 00:00 01 January 2006 end 23:59 01 January 2006
time-range entry: workhours (inactive)
    periodic weekdays 8:00 to 12:00
    periodic weekdays 13:00 to 17:00
```

時間範囲を適用するには、時間範囲を実装できる拡張 ACL 内に時間範囲名を入力します。次に、拡張アクセス リスト 188 を作成して確認する例を示します。このアクセス リストでは、定義された休業時間中はすべての送信元からすべての宛先への TCP トラフィックを拒否し、営業時間中はすべての TCP トラフィックを許可します。

```
デバイス(config)# access-list 188 deny tcp any any time-range new_year_day_2006
デバイス(config)# access-list 188 permit tcp any any time-range workhours
デバイス(config)# end
デバイス# show access-lists
Extended IP access list 188
    10 deny tcp any any time-range new_year_day_2006 (inactive)
    20 permit tcp any any time-range workhours (inactive)
```

次に、名前付き ACL を使用して同じトラフィックを許可および拒否する例を示します。

```
デバイス(config)# ip access-list extended deny_access
デバイス(config-ext-nacl)# deny tcp any any time-range new_year_day_2006
デバイス(config-ext-nacl)# exit
デバイス(config)# ip access-list extended may_access
デバイス(config-ext-nacl)# permit tcp any any time-range workhours
デバイス(config-ext-nacl)# end
デバイス# show ip access-lists
Extended IP access list lpip_default
    10 permit ip any any
Extended IP access list deny_access
    10 deny tcp any any time-range new_year_day_2006 (inactive)
Extended IP access list may_access
    10 permit tcp any any time-range workhours (inactive)
```

## 例：ACL へのコメントの挿入

**remark** キーワードを使用すると、任意の IP 標準または拡張 ACL にエントリーに関するコメント（注釈）を追加できます。コメントを使用すると、ACL の理解とスキャンが容易になります。1 つのコメント行の最大長は 100 文字です。

コメントは、**permit** ステートメントまたは **deny** ステートメントの前後どちらにでも配置できます。コメントがどの **permit** ステートメントまたは **deny** ステートメントの説明であるのかが明確になるように、コメントの位置に関して一貫性を保つ必要があります。たとえば、あるコメントは対応する **permit** または **deny** ステートメントの前にあり、他のコメントは対応するステートメントの後ろにあると、混乱を招く可能性があります。

番号付き IP 標準または拡張 ACL にコメントを挿入するには、**access-list access-list number remark remark** 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。コメントを削除するには、このコマンドの **no** 形式を使用します。

次の例では、Jones のワークステーションにはアクセスを許可し、Smith のワークステーションにはアクセスを許可しません。

```
デバイス(config)# access-list 1 remark Permit only Jones workstation through
デバイス(config)# access-list 1 permit 171.69.2.88
デバイス(config)# access-list 1 remark Do not allow Smith through
デバイス(config)# access-list 1 deny 171.69.3.13
```

名前付き IP ACL のエントリーには、**remark** アクセスリスト コンフィギュレーション コマンドを使用します。コメントを削除するには、このコマンドの **no** 形式を使用します。

次の例では、Jones のサブネットには発信 Telnet の使用が許可されません。

```
デバイス(config)# ip access-list extended telnetting
デバイス(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
デバイス(config-ext-nacl)# deny tcp host 171.69.2.88 any eq telnet
```

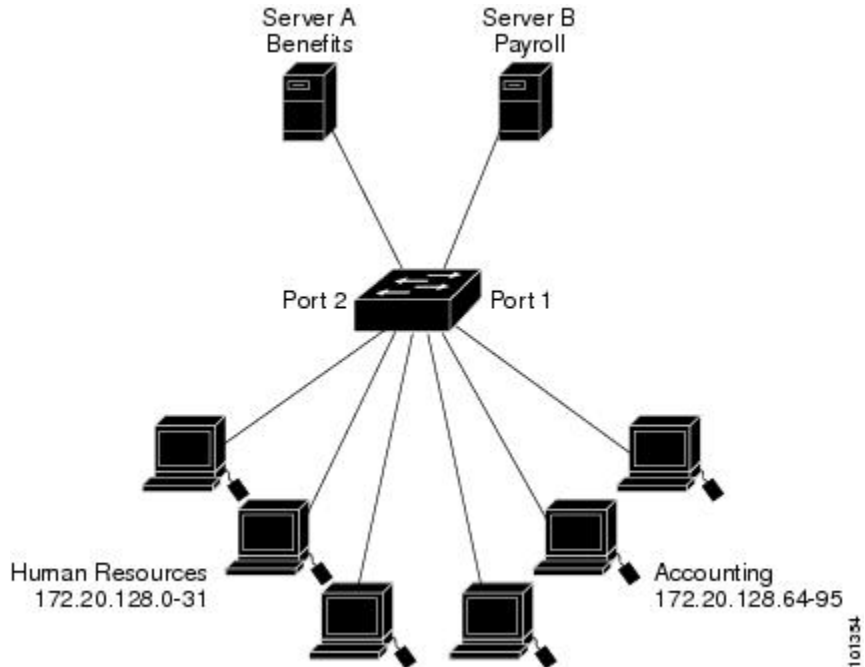
## IPv4 ACL の設定例

### 小規模ネットワークが構築されたオフィス用の ACL

図 16: ルータ ACL によるトラフィックの制御

次に、小規模ネットワークが構築されたオフィス環境を示します。ルーテッドポート 2 に接続されたサーバー A には、すべての従業員がアクセスできる収益などの情報が格納されています。ルーテッドポート 1 に接続されたサーバー B には、機密扱いの給与支払いデータが格納されています。サーバー A にはすべてのユーザーがアクセスできますが、サーバー B にアク

セスできるユーザーは制限されています。



ルータ ACL を使用して上記のように設定するには、次のいずれかの方法を使用します。

- 標準 ACL を作成し、ポート 1 からサーバーに着信するトラフィックをフィルタリングします。
- 拡張 ACL を作成し、サーバーからポート 1 に着信するトラフィックをフィルタリングします。

## 例：小規模ネットワークが構築されたオフィスの ACL

次に、標準 ACL を使用してポートからサーバー B に着信するトラフィックをフィルタリングし、経理部の送信元アドレス 172.20.128.64 ~ 172.20.128.95 から送信されるトラフィックだけを許可する例を示します。この ACL は、指定された送信元アドレスを持つルーテッドポート 1 から送信されるトラフィックに適用されます。

```

デバイス(config)# access-list 6 permit 172.20.128.64 0.0.0.31
デバイス(config)# end
デバイス# show access-lists
Standard IP access list 6
  10 permit 172.20.128.64, wildcard bits 0.0.0.31
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ip access-group 6 out

```

次に、拡張 ACL を使用してサーバー B からポートに着信するトラフィックをフィルタリングし、任意の送信元アドレス（この場合はサーバー B）から経理部の宛先アドレス 172.20.128.64 ~ 172.20.128.95 に送信されるトラフィックだけを許可する例を示します。この ACL は、ルー

テッドポート1に着信するトラフィックに適用され、指定の宛先アドレスに送信されるトラフィックだけを許可します。拡張 ACL を使用する場合は、送信元および宛先情報の前に、プロトコル (IP) を入力する必要があります。

```
デバイス(config)# access-list 106 permit ip any 172.20.128.64 0.0.0.31
デバイス(config)# end
デバイス# show access-lists
Extended IP access list 106
    10 permit ip any 172.20.128.64 0.0.0.31
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ip access-group 106 in
```

## 例：番号付き ACL

次の例のネットワーク 36.0.0.0 は、2 番目のオクテットがサブネットを指定するクラス A ネットワークです。つまり、サブネットマスクは 255.255.0.0 です。ネットワークアドレス 36.0.0.0 の 3 番めおよび 4 番目のオクテットは、特定のホストを指定します。アクセスリスト 2 を使用して、サブネット 48 のアドレスを 1 つ許可し、同じサブネットの他のアドレスはすべて拒否します。このアクセスリストの最終行は、ネットワーク 36.0.0.0 の他のすべてのサブネット上のアドレスが許可されることを示します。この ACL は、ポートに着信するパケットに適用されます。

```
デバイス(config)# access-list 2 permit 36.48.0.3
デバイス(config)# access-list 2 deny 36.48.0.0 0.0.255.255
デバイス(config)# access-list 2 permit 36.0.0.0 0.255.255.255
デバイス(config)# interface gigabitethernet2/0/1
デバイス(config-if)# ip access-group 2 in
```

## 例：拡張 ACL

次の例の先頭行は、1023 よりも大きい宛先ポートへの着信 TCP 接続を許可します。2 番目の行は、ホスト 128.88.1.2 のシンプルメール転送プロトコル (SMTP) ポートへの着信 TCP 接続を許可します。3 番目の行は、エラー フィードバック用の着信 ICMP メッセージを許可します。

```
デバイス(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 gt 1023
デバイス(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
デバイス(config)# access-list 102 permit icmp any any
デバイス(config)# interface gigabitethernet2/0/1
デバイス(config-if)# ip access-group 102 in
```

次の例では、インターネットに接続されたネットワークがあり、そのネットワーク上の任意のホストがインターネット上の任意のホストと TCP 接続を確立できるようにする場合を想定しています。ただし、IP ホストからは、専用メールホストのメール (SMTP) ポートを除き、ネットワーク上のホストと TCP 接続を確立できないようにします。

SMTPは、接続の一端ではTCPポート25、もう一端ではランダムなポート番号を使用します。接続している間は、同じポート番号が使用されます。インターネットから着信するメールパケットの宛先ポートは25です。安全なネットワークシステムでは常にポート25でのメール接続が使用されているため、着信サービスとを個別に制御できます。

```
デバイス(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 23
デバイス(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 25
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ip access-group 102 in
```

次の例では、ネットワークはアドレスが128.88.0.0のクラスBネットワークで、メールホストのアドレスは128.88.1.2です。**established** キーワードは、確立された接続を表示するTCP専用のキーワードです。TCPデータグラムにACKまたはRSTビットが設定され、パケットが既存の接続に属していることが判明すると、一致と見なされます。スタックメンバー1のギガビットイーサネットインターフェイス1は、ルータをインターネットに接続するインターフェイスです。

```
デバイス(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 established
デバイス(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ip access-group 102 in
```

## 例：名前付き ACL

### 名前付き標準 ACL および名前付き拡張 ACL の作成

次に、*Internet\_filter* という名前の標準 ACL および *marketing\_group* という名前の拡張 ACL を作成する例を示します。*Internet\_filter* ACL は、送信元アドレス 1.2.3.4 から送信されるすべてのトラフィックを許可します。

```
デバイス(config)# ip access-list standard Internet_filter
デバイス(config-ext-nacl)# permit 1.2.3.4
デバイス(config-ext-nacl)# exit
```

*marketing\_group* ACL は、宛先アドレスとワイルドカードの値 171.69.0.0 0.0.255.255 への任意の TCP Telnet トラフィックを許可し、その他の TCP トラフィックを拒否します。ICMP トラフィックを許可し、任意の送信元から、宛先ポートが 1024 より小さい 171.69.0.0 ~ 179.69.255.255 の宛先アドレスへ送信される UDP トラフィックを拒否します。それ以外のすべての IP トラフィックを拒否して、結果を示すログが表示されます。

```
デバイス(config)# ip access-list extended marketing_group
デバイス(config-ext-nacl)# permit tcp any 171.69.0.0 0.0.255.255 eq telnet
デバイス(config-ext-nacl)# deny tcp any any
デバイス(config-ext-nacl)# permit icmp any any
デバイス(config-ext-nacl)# deny udp any 171.69.0.0 0.0.255.255 lt 1024
```

```

デバイス(config-ext-nacl)# deny ip any any log
デバイス(config-ext-nacl)# exit

```

*Internet\_filter* ACL は発信トラフィックに適用され、*marketing\_group* ACL はレイヤ 3 ポートの着信トラフィックに適用されます。

```

デバイス(config)# interface gigabitethernet3/0/2
デバイス(config-if)# no switchport
デバイス(config-if)# ip address 2.0.5.1 255.255.255.0
デバイス(config-if)# ip access-group Internet_filter out
デバイス(config-if)# ip access-group marketing_group in

```

### 名前付き ACL からの個別 ACE の削除

次に、名前付きアクセス リスト *border-list* から ACE を個別に削除する例を示します。

```

デバイス(config)# ip access-list extended border-list
デバイス(config-ext-nacl)# no permit ip host 10.1.1.3 any

```

## 例：IP ACL に適用される時間範囲

次に、月曜日から金曜日の午前 8 時～午後 6 時（18 時）の間、IP の HTTP トラフィックを拒否する例を示します。UDP トラフィックは、土曜日および日曜日の正午～午後 8 時（20 時）の間だけ許可されます。

```

デバイス(config)# time-range no-http
デバイス(config)# periodic weekdays 8:00 to 18:00
!
デバイス(config)# time-range udp-yes
デバイス(config)# periodic weekend 12:00 to 20:00
!
デバイス(config)# ip access-list extended strict
デバイス(config-ext-nacl)# deny tcp any any eq www time-range no-http
デバイス(config-ext-nacl)# permit udp any any time-range udp-yes
!
デバイス(config-ext-nacl)# exit
デバイス(config)# interface gigabitethernet2/0/1
デバイス(config-if)# ip access-group strict in

```

## 例：コメント付き IP ACL エントリの設定

次に示す番号付き ACL の例では、Jones が所有するワークステーションにはアクセスを許可し、Smith が所有するワークステーションにはアクセスを許可しません。

```

デバイス(config)# access-list 1 remark Permit only Jones workstation through
デバイス(config)# access-list 1 permit 171.69.2.88

```

## 例 : ACL ロギング

```

デバイス(config)# access-list 1 remark Do not allow Smith workstation through
デバイス(config)# access-list 1 deny 171.69.3.13

```

次に示す番号付き ACL の例では、Winter および Smith のワークステーションに Web 閲覧を許可しません。

```

デバイス(config)# access-list 100 remark Do not allow Winter to browse the web
デバイス(config)# access-list 100 deny host 171.69.3.85 any eq www
デバイス(config)# access-list 100 remark Do not allow Smith to browse the web
デバイス(config)# access-list 100 deny host 171.69.3.13 any eq www

```

次に示す名前付き ACL の例では、Jones のサブネットにアクセスを許可しません。

```

デバイス(config)# ip access-list standard prevention
デバイス(config-std-nacl)# remark Do not allow Jones subnet through
デバイス(config-std-nacl)# deny 171.69.0.0 0.0.255.255

```

次に示す名前付き ACL の例では、Jones のサブネットに発信 Telnet の使用を許可しません。

```

デバイス(config)# ip access-list extended telnetting
デバイス(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
デバイス(config-ext-nacl)# deny tcp 171.69.0.0 0.0.255.255 any eq telnet

```

## 例 : ACL ロギング

ルータ ACL では、2 種類のロギングがサポートされています。**log** キーワードを指定すると、エントリと一致するパケットに関するログ通知メッセージがコンソールに送信されます。**log-input** キーワードを指定すると、ログ エントリに入力インターフェイスが追加されます。

次の例では、名前付き標準アクセスリスト *stan1* は 10.1.1.0 0.0.0.255 からのトラフィックを拒否し、その他のすべての送信元からのトラフィックを許可します。**log** キーワードも指定されています。

```

デバイス(config)# ip access-list standard stan1
デバイス(config-std-nacl)# deny 10.1.1.0 0.0.0.255 log
デバイス(config-std-nacl)# permit any log
デバイス(config-std-nacl)# exit
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# ip access-group stan1 in
デバイス(config-if)# end
デバイス# show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
  Console logging: level debugging, 37 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 37 messages logged
  File logging: disabled
  Trap logging: level debugging, 39 message lines logged

Log Buffer (4096 bytes):

```



```
00:00:48: NTP: authentication delay calculation problems

<output truncated>

00:09:34:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet
00:09:59:%SEC-6-IPACCESSLOGS:list stan1 denied 10.1.1.15 1 packet
00:10:11:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet
```

次に、名前付き拡張アクセス リスト *ext1* によって、任意の送信元から 10.1.1.0 0.0.0.255 への ICMP パケットを許可し、すべての UDP パケットを拒否する例を示します。

```
デバイス(config)# ip access-list extended ext1
デバイス(config-ext-nacl)# permit icmp any 10.1.1.0 0.0.0.255 log
デバイス(config-ext-nacl)# deny udp any any log
デバイス(config-std-nacl)# exit
デバイス(config)# interface gigabitethernet1/0/2
デバイス(config-if)# ip access-group ext1 in
```

次に、拡張 ACL のログの例を示します。

```
01:24:23:%SEC-6-IPACCESSLOGDP:list ext1 permitted icmp 10.1.1.15 -> 10.1.1.61 (0/0), 1
packet
01:25:14:%SEC-6-IPACCESSLOGDP:list ext1 permitted icmp 10.1.1.15 -> 10.1.1.61 (0/0), 7
packets
01:26:12:%SEC-6-IPACCESSLOGP:list ext1 denied udp 0.0.0.0(0) -> 255.255.255.255(0), 1
packet
01:31:33:%SEC-6-IPACCESSLOGP:list ext1 denied udp 0.0.0.0(0) -> 255.255.255.255(0), 8
packets
```

IP ACL のすべてのロギング エントリは %SEC-6-IPACCESSLOG で開始します。エントリの形式は、一致した ACL やアクセス エントリの種類に応じて若干異なります。

次に、**log-input** キーワードを指定した場合の出力メッセージの例を示します。

```
00:04:21:%SEC-6-IPACCESSLOGDP:list inputlog permitted icmp 10.1.1.10 (Vlan1 0001.42ef.a400)
->
10.1.1.61 (0/0), 1 packet
```

**log** キーワードを指定した場合、同様のパケットに関するログ メッセージには入力インターフェイス情報が含まれません。

```
00:05:47:%SEC-6-IPACCESSLOGDP:list inputlog permitted icmp 10.1.1.10 -> 10.1.1.61 (0/0),
1 packet
```

## ACL および VLAN マップの設定例

### 例：パケットを拒否する ACL および VLAN マップの作成

ここでは、パケットを拒否する ACL および VLAN マップを作成する例を示します。最初のマップでは、*ip1* ACL (TCP パケット) に一致するすべてのパケットがドロップされます。最初に、すべての TCP パケットを許可し、それ以外のパケットをすべて拒否する *ip1* ACL を作成します。VLAN マップには IP パケットに対する *match* 句が存在するため、デフォルトのアクションでは、どの *match* 句とも一致しない IP パケットがすべてドロップされます。

```
デバイス(config)# ip access-list extended ip1
デバイス(config-ext-nacl)# permit tcp any any
デバイス(config-ext-nacl)# exit
デバイス(config)# vlan access-map map_1 10
デバイス(config-access-map)# match ip address ip1
デバイス(config-access-map)# action drop
```

### 例：パケットを許可する ACL および VLAN マップの作成

次に、パケットを許可する VLAN マップを作成する例を示します。ACL *ip2* は UDP パケットを許可し、*ip2* ACL と一致するすべてのパケットが転送されます。このマップでは、これ以前のどの ACL とも一致しないすべての IP パケット (TCP でも UDP でもないパケット) がドロップされます。

```
デバイス(config)# ip access-list extended ip2
デバイス(config-ext-nacl)# permit udp any any
デバイス(config-ext-nacl)# exit
デバイス(config)# vlan access-map map_1 20
デバイス(config-access-map)# match ip address ip2
デバイス(config-access-map)# action forward
```

### 例：IP パケットのドロップおよび MAC パケットの転送のデフォルトアクション

次の例の VLAN マップでは、デフォルトで IP パケットがドロップされ、MAC パケットが転送されます。標準の ACL 101 および名前付き拡張アクセス リスト *igmp-match* および *tcp-match* をこのマップと組み合わせて使用すると、次のようになります。

- すべての UDP パケットが転送されます。
- すべての IGMP パケットがドロップされます。
- すべての TCP パケットが転送されます。
- その他のすべての IP パケットがドロップされます。

- すべての非 IP パケットが転送されます。

```

デバイス(config)# access-list 101 permit udp any any
デバイス(config)# ip access-list extended igmp-match
デバイス(config-ext-nacl)# permit igmp any any

デバイス(config)# action forward
デバイス(config-ext-nacl)# permit tcp any any
デバイス(config-ext-nacl)# exit
デバイス(config)# vlan access-map drop-ip-default 10
デバイス(config-access-map)# match ip address 101
デバイス(config-access-map)# action forward
デバイス(config-access-map)# exit
デバイス(config)# vlan access-map drop-ip-default 20
デバイス(config-access-map)# match ip address igmp-match
デバイス(config-access-map)# action drop
デバイス(config-access-map)# exit
デバイス(config)# vlan access-map drop-ip-default 30
デバイス(config-access-map)# match ip address tcp-match
デバイス(config-access-map)# action forward

```

## 例：MAC パケットのドロップおよび IP パケットの転送のデフォルトアクション

次の例の VLAN マップでは、デフォルトで MAC パケットがドロップされ、IP パケットが転送されます。MAC 拡張アクセス リスト **good-hosts** および **good-protocols** をこのマップと組み合わせると、次のようになります。

- ホスト 0000.0c00.0111 および 0000.0c00.0211 からの MAC パケットが転送されます。
- decnet-iv または vines-ip プロトコルを使用する MAC パケットが転送されます。
- その他のすべての非 IP パケットがドロップされます。
- すべての IP パケットが転送されます。

## 例：すべてのパケットをドロップするデフォルトアクション

次の例の VLAN マップでは、デフォルトですべてのパケット（IP および非 IP）がドロップされます。例 2 および例 3 のアクセス リスト **tcp-match** および **good-hosts** をこのマップと組み合わせると、次のようになります。

- すべての TCP パケットが転送されます。
- ホスト 0000.0c00.0111 および 0000.0c00.0211 からの MAC パケットが転送されます。
- その他のすべての IP パケットがドロップされます。
- その他のすべての MAC パケットがドロップされます。

```

デバイス(config)# vlan access-map drop-all-default 10
デバイス(config-access-map)# match ip address tcp-match
デバイス(config-access-map)# action forward
デバイス(config-access-map)# exit
デバイス(config)# vlan access-map drop-all-default 20
デバイス(config-access-map)# match mac address good-hosts
デバイス(config-access-map)# action forward

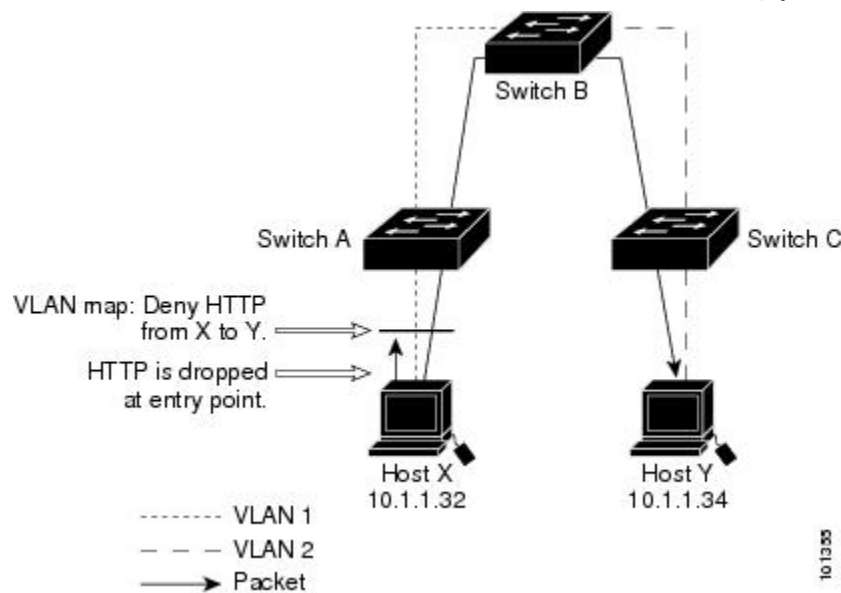
```

## ネットワークでの VLAN マップの使用方法の設定例

### 例：ワイヤリングクローゼットの設定

図 17: ワイヤリングクローゼットの設定

ワイヤリングクローゼット構成では、ルーティングがスイッチ上で有効にされていない場合があります。ただし、この設定でも VLAN マップおよび QoS 分類 ACL はサポートされています。ホスト X およびホスト Y は異なる VLAN 内にあり、ワイヤリングクローゼットスイッチ A およびスイッチ C に接続されていると想定します。ホスト X からホスト Y へのトラフィックは、ルーティングが有効に設定されたレイヤ3スイッチであるスイッチ B によって最終的にルーティングされます。ホスト X からホスト Y へのトラフィックは、トラフィックのエントリポイントであるスイッチ A でアクセスコントロールできます。



HTTP トラフィックをホスト X からホスト Y へスイッチングしない場合は、ホスト X (IP アドレス 10.1.1.32) からホスト Y (IP アドレス 10.1.1.34) に向かうすべての HTTP トラフィックがスイッチ A でドロップされ、スイッチ B にブリッジングされないように、スイッチ A の VLAN マップを設定できます。

最初に、HTTP ポート上ですべての TCP トラフィックを許可（一致）する IP アクセス リスト *http* を定義します。

```
デバイス(config)# ip access-list extended http
デバイス(config-ext-nacl)# permit tcp host 10.1.1.32 host 10.1.1.34 eq www
デバイス(config-ext-nacl)# exit
```

次に、*http* アクセス リストと一致するトラフィックがドロップされ、その他のすべての IP トラフィックが転送されるように、VLAN アクセス マップ *map2* を作成します。

```
デバイス(config)# vlan access-map map2 10
デバイス(config-access-map)# match ip address http
デバイス(config-access-map)# action drop
デバイス(config-access-map)# exit
デバイス(config)# ip access-list extended match_all
デバイス(config-ext-nacl)# permit ip any any
デバイス(config-ext-nacl)# exit
デバイス(config)# vlan access-map map2 20
デバイス(config-access-map)# match ip address match_all
デバイス(config-access-map)# action forward
```

次に、VLAN アクセス マップ *map2* を VLAN 1 に適用します。

```
デバイス(config)# vlan filter map2 vlan 1
```

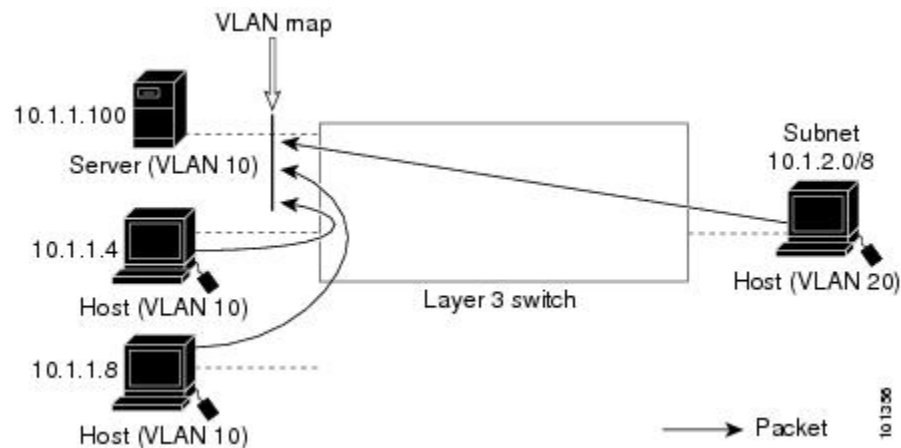
## 例：別の VLAN にあるサーバーへのアクセスの制限

図 18:別の VLAN 上のサーバーへのアクセスの制限

別の VLAN にあるサーバーへのアクセスを制限できます。たとえば、VLAN 10 内のサーバー 10.1.1.100 では、次のホストへのアクセスを拒否する必要があります。

- VLAN 20 内のサブネット 10.1.2.0/8 にあるホストのアクセスを禁止します。
- VLAN 10 内のホスト 10.1.1.4 および 10.1.1.8 のアクセスを禁止します。

## 例：別の VLAN にあるサーバーへのアクセスの拒否



## 例：別の VLAN にあるサーバーへのアクセスの拒否

次に、サブネット 10.1.2.0/8 内のホスト、ホスト 10.1.1.4、およびホスト 10.1.1.8 のアクセスを拒否し、その他の IP トラフィックを許可する VLAN マップ SERVER1-ACL を作成して、別の VLAN 内のサーバーへのアクセスを拒否する例を示します。最後のステップでは、マップ SERVER1 を VLAN 10 に適用します。

正しいパケットと一致する IP ACL を定義します。

```

デバイス(config)# ip access-list extended SERVER1_ACL
デバイス(config-ext-nacl)# permit ip 10.1.2.0 0.0.0.255 host 10.1.1.100
デバイス(config-ext-nacl)# permit ip host 10.1.1.4 host 10.1.1.100
デバイス(config-ext-nacl)# permit ip host 10.1.1.8 host 10.1.1.100
デバイス(config-ext-nacl)# exit

```

SERVER1\_ACL と一致する IP パケットをドロップして、この ACL と一致しない IP パケットを転送する ACL を使用して、VLAN マップを定義します。

```

デバイス(config)# vlan access-map SERVER1_MAP
デバイス(config-access-map)# match ip address SERVER1_ACL
デバイス(config-access-map)# action drop
デバイス(config)# vlan access-map SERVER1_MAP 20
デバイス(config-access-map)# action forward
デバイス(config-access-map)# exit

```

VLAN 10 に VLAN マップを適用します。

```

デバイス(config)# vlan filter SERVER1_MAP vlan-list 10

```

## ACL の設定例

### IPv4 アクセスコントロールリストの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	IPv4 アクセスコントロールリスト	この章では、ACL を使用して、スイッチのネットワークセキュリティを設定する方法について説明します。パケットフィルタリングは、ネットワークトラフィックを限定し、特定のユーザまたはデバイスによるネットワークの使用を制限するうえで役立ちます。ACL は、トラフィックをデバイスの通過時にフィルタリングし、パケットが指定されたインターフェイスを通過することを許可または拒否します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。







## 第 17 章

# IPv6 ACL

- IPv6 ACL の概要 (379 ページ)
- IPv6 ACL の制限 (382 ページ)
- IPv6 ACL のデフォルト設定 (383 ページ)
- IPv6 ACL の設定 (383 ページ)
- インターフェイスへの IPv6 ACL の付加 (388 ページ)
- VLAN マップの設定 (389 ページ)
- VLAN への VLAN マップの適用 (391 ページ)
- IPv6 ACL のモニタリング (392 ページ)
- IPv6 ACL の機能履歴 (393 ページ)

## IPv6 ACL の概要

IP Version 6 (IPv6) アクセス コントロール リスト (ACL) を作成し、それをインターフェイスに適用することによって、IPv6 トラフィックをフィルタリングできます。これは、IP Version 4 (IPv4) の名前付き ACL を作成し、適用する方法と同じです。また、スイッチで IP ベースおよび LAN ベース フィーチャセットが稼働している場合、入力ルータ ACL を作成し、それを適用してレイヤ 3 管理トラフィックをフィルタリングすることもできます。

スイッチは、次の 3 種類の IPv6 ACL をサポートします。

- IPv6 ルータ ACL は、ルーテッドポート、スイッチ仮想インターフェイス (SVI)、またはレイヤ 3 EtherChannel に設定できるレイヤ 3 インターフェイスのアウトバウンドトラフィックまたはインバウンドトラフィックでサポートされます。IPv6 ルータ ACL は、ルーティングされる IPv6 パケットに対してだけ適用されます。
- IPv6 ポート ACL は、アウトバウンドおよびインバウンドのレイヤ 2 インターフェイスでサポートされます。IPv6 ポート ACL は、インターフェイスに着信するすべての IPv6 パケットに対して適用されます。
- VLAN ACL または VLAN マップは、VLAN 内のすべてのパケットのアクセスを制御します。VLAN マップを使用すると、同じ VLAN 内のデバイス間で転送されるトラフィックをフィルタリングできます。ACL VLAN マップは、L2 VLAN に適用されます。VLAN マップは、IPv6 のレイヤ 3 アドレスに基づいてアクセス コントロールするように設定されて

います。イーサネット ACE を使用すると MAC アドレスにより、サポートされていないプロトコルがアクセスコントロールされます。VLAN マップを VLAN に適用すると、VLAN に入るすべてのパケットが VLAN マップと照合されます。

スイッチは、IPv6 トラフィックの VLAN ACL (VLAN マップ) をサポートします。

1 つのインターフェイスに、IPv4 ACL および IPv6 ACL の両方を適用できます。IPv4 ACL の場合と同様に、IPv6 ポート ACL はルータ ACL よりも優先されます。

## スイッチスタックおよび IPv6 ACL

アクティブスイッチは IPv6 ACL をハードウェアでサポートし、IPv6 ACL をスタックメンバーに配信します。

スタンバイスイッチがアクティブスイッチを引き継ぐと、ACL 設定がすべてのスタックメンバーに配信されます。メンバースイッチは、新しいアクティブスイッチによって配信された設定を同期し、不要なエントリを消去します。

ACL の修正、インターフェイスへの適用、またはインターフェイスからの解除が行われると、アクティブスイッチは変更内容をすべてのスタックメンバーに配信します。

## ACL 優先順位

VLAN マップ、ポート ACL、およびルータ ACL が同じスイッチに設定されている場合、入力トラフィックの場合のフィルタの優先順位は上からポート ACL、VLAN マップ、およびルータ ACL です。出力トラフィックの場合、フィルタの優先順位は、ルータ ACL、VLAN マップ、ポート ACL です。

次の例で、簡単な使用例を説明します。

- 入力ポート ACL と VLAN マップが両方とも適用されている場合に、ポート ACL が適用されたポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。その他のパケットは、VLAN マップによってフィルタリングされます。
- スイッチ仮想インターフェイス (SVI) に入力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。他のポートで受信した着信のルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- SVI に入力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。発信するルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。
- SVI に VLAN マップ、入力ルータ ACL、および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL だけによってフィルタリングされます。他のポートで受信した着信のルーティン

IP パケットには、VLAN マップおよびルータ ACL のフィルタが適用されます。他のパケットには、VLAN マップのフィルタだけが適用されます。

- SVI に VLAN マップ、出力ルータ ACL、および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL だけによってフィルタリングされます。発信するルーティング IP パケットには、VLAN マップおよびルータ ACL のフィルタが適用されます。他のパケットには、VLAN マップのフィルタだけが適用されます。

## VLAN マップ

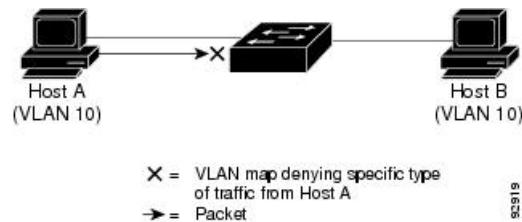
VLAN ACL または VLAN マップは、VLAN 内のネットワーク トラフィックを制御するために使用されます。スイッチまたはスイッチ スタックの VLAN 内でブリッジングされるすべてのパケットに VLAN マップを適用できます。VACL は、セキュリティ パケット フィルタリング および特定の物理インターフェイスへのトラフィックのリダイレクトだけを目的としたものです。VACL は方向（入力または出力）で定義されることはありません。

すべての非 IP プロトコルは、MAC VLAN マップを使用して、MAC アドレスおよび Ethertype によってアクセス コントロールされます（IP トラフィックは、MAC VACL マップではアクセス制御されません）。VLAN マップはスイッチを通過するパケットにだけ適用できます。ハブ上またはこのスイッチに接続された別のスイッチ上のホスト間のトラフィックには、VLAN マップを適用させることができません。

VLAN マップを使用すると、マップに指定されたアクションに基づいてパケットの転送が許可または拒否されます。

図 19: VLAN マップによるトラフィックの制御

次の図に、VLAN マップを適用して、特定のトラフィック タイプを VLAN 10 のホスト A から転送できないように設定する例を示します。各 VLAN には、VLAN マップを 1 つだけ適用で



きます。

## 他の機能およびスイッチとの相互作用

- IPv6 ルータ ACL がパケットを拒否するよう設定されている場合、パケットはルーティングされません。パケットのコピーがインターネット制御メッセージプロトコル (ICMP) キューに送信され、フレームに ICMP 到達不能メッセージが生成されます。
- ブリッジドフレームがポート ACL によってドロップされる場合、このフレームはブリッジングされません。

- IPv4 ACL および IPv6 ACL の両方を 1 つのスイッチまたはスイッチスタックに作成したり、同一インターフェイスに適用できます。各 ACL には一意の名前が必要です。設定済みの名前を使用しようとすると、エラーメッセージが表示されます。

IPv4 ACL と IPv6 ACL の作成、および同一のレイヤ 2 インターフェイスまたはレイヤ 3 インターフェイスへの IPv4 ACL または IPv6 ACL の適用には、異なるコマンドを使用します。ACL を付加するのに誤ったコマンドを使用すると（例えば、IPv6 ACL の付加に IPv4 コマンドを使用するなど）、エラーメッセージが表示されます。

- MAC ACL を使用して、IPv6 フレームをフィルタリングできません。MAC ACL は非 IP フレームだけをフィルタリングできます。
- ハードウェアメモリに空きがない場合、パケットはインターフェイスでドロップされ、アンロードのエラーメッセージが記録されます。

## IPv6 ACL の制限

IPv4 では、番号制の標準 IP ACL および拡張 IP ACL、名前付き IP ACL、および MAC ACL を設定できます。IPv6 がサポートするのは名前付き ACL だけです。

スイッチは Cisco IOS がサポートする IPv6 ACL の大部分をサポートしますが、一部例外もあります。

- スイッチは、**routing header**、および **undetermined-transport** というキーワードの照合をサポートしません。
- スイッチは、再帰 ACL (**reflect** キーワード) をサポートしません。
- このリリースは、IPv6 のポート ACL、ルータ ACL および VLAN ACL (VLAN マップ) をサポートしています。
- スイッチは、IPv6 フレームに MAC ベース ACL を適用しません。
- ACL を設定する場合、ACL に入力されるキーワードには、それがプラットフォームでサポートされるかどうかにかかわらず、制限事項はありません。ハードウェア転送が必要なインターフェイス（物理ポートまたは SVI）に ACL を適用する場合、スイッチはインターフェイスで ACL がサポートされるかどうか判別します。サポートされない場合、ACL の付加は拒否されます。
- インターフェイスに適用される ACL に、サポートされないキーワードを持つアクセス コントロールエントリ (ACE) を追加しようとする場合、スイッチは現在インターフェイスに適用されている ACL に ACE が追加されるのを許可しません。

スイッチの IPv6 ACL には、次の特性があります。

- 分割フレーム (IPv4 では **fragments** キーワード) がサポートされます。
- IPv6 ACL では、IPv4 と同じ統計情報がサポートされます。

- スイッチのハードウェア スペースがなくなった場合、ACL に関連付けられたパケットはインターフェイスでドロップされます。
- ロギングは、ルータ ACL ではサポートされますが、ポート ACL ではサポートされません。
- スイッチは、プレフィックス長の最大範囲の IPv6 アドレス一致をサポートしません。

## IPv6 ACL のデフォルト設定

デフォルトの IPv6 ACL 設定は次のとおりです。

```
Switch# show access-lists preauth_ipv6_acl
IPv6 access list preauth_ipv6_acl (per-user)
permit udp any any eq domain sequence 10
permit tcp any any eq domain sequence 20
permit icmp any any nd-ns sequence 30
permit icmp any any nd-na sequence 40
permit icmp any any router-solicitation sequence 50
permit icmp any any router-advertisement sequence 60
permit icmp any any redirect sequence 70
permit udp any eq 547 any eq 546 sequence 80
permit udp any eq 546 any eq 547 sequence 90
deny ipv6 any any sequence 100
```

## IPv6 ACL の設定

IPv6 トラフィックをフィルタリングするには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **{ipv6 access-list list-name**
4. **{deny | permit} protocol {source-ipv6-prefix/|prefix-length|any} host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/|prefix-length|any} host destination-ipv6-address} [operator [port-number]][ dscp value] [fragments] [log] [log-input][sequence value] [time-range name]**
5. **{deny | permit} tcp {source-ipv6-prefix/|prefix-length|any} host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/|prefix-length|any} host destination-ipv6-address} [operator [port-number]] [ack] [dscp value] [established] [fin] [log] [log-input] [neq {port | protocol}] [psh] [range {port | protocol}] [rst] [sequence value] [syn] [time-range name] [urg]**
6. **{deny | permit} udp {source-ipv6-prefix/|prefix-length|any} host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/|prefix-length|any} host destination-ipv6-address} [operator [port-number]] [dscp value] [log] [log-input] [neq {port | protocol}] [range {port | protocol}] [sequence value] [time-range name]**
7. **{deny | permit} icmp {source-ipv6-prefix/|prefix-length|any} host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/|prefix-length|any} host destination-ipv6-address} [operator**

[*port-number*] [*icmp-type* [*icmp-code*] | *icmp-message*] [*dscp value*] [*log*] [*log-input*] [*sequence value*] [*time-range name*]

8. **end**
9. **show ipv6 access-list**
10. **show running-config**
11. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： デバイス> <b>enable</b>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>• パスワードを入力します（要求された場合）。</li> </ul>
ステップ 2	<b>configure terminal</b> 例： デバイス# <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 3	<b>{ipv6 access-list list-name}</b> 例： デバイス (config) # <b>ipv6 access-list example_acl_list</b>	IPv6 ACL 名を定義し、IPv6 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 4	<b>{deny   permit} protocol {source-ipv6-prefix/ prefix-length   any} host source-ipv6-address} [ operator [ port-number ] ] { destination-ipv6-prefix/ prefix-length   any   host destination-ipv6-address} [operator [port-number]][ dscp value] [fragments] [log] [log-input][ sequence value] [ time-range name]</b>	条件が一致した場合にパケットを拒否する場合は <b>deny</b> 、許可する場合は <b>permit</b> を指定します。次に、条件について説明します。 <ul style="list-style-type: none"> <li>• <b>protocol</b> には、IP の名前または番号を入力します。 <b>ahp</b>、<b>esp</b>、<b>icmp</b>、<b>ipv6</b>、<b>pcp</b>、<b>step</b>、<b>tcp</b>、<b>udp</b> または IPv6 プロトコル番号を表す 0～255 の整数を使用できます。</li> <li>• <b>source-ipv6-prefix/prefix-length</b> または <b>destination-ipv6-prefix/ prefix-length</b> は、拒否条件または許可条件を設定する送信元または宛先 IPv6 ネットワークあるいはネットワーク クラスで、コロン区切りの 16 ビット値を使用した 16 進形式で指定します（RFC 2373 を参照）。</li> <li>• IPv6 プレフィックス <b>::/0</b> の短縮形として、<b>any</b> を入力します。</li> <li>• <b>host source-ipv6-address</b> または <b>destination-ipv6-address</b> には、拒否条件または許可条件を設定する送信元または宛先 IPv6 ホ</li> </ul>

	コマンドまたはアクション	目的
		<p>ストアドレスを入力します。アドレスはコロンの区切りの16ビット値を使用した16進形式で指定します。</p> <ul style="list-style-type: none"> <li>• (任意) <b>operator</b> には、指定のプロトコルの送信元ポートまたは宛先ポートを比較するオペランドを指定します。オペランドには、<b>lt</b> (より小さい)、<b>gt</b> (より大きい)、<b>eq</b> (等しい)、<b>neq</b> (等しくない)、および<b>range</b> (包含範囲)があります。</li> </ul> <p><i>source-ipv6-prefix/prefix-length</i> 引数のあとの <b>operator</b> は、送信元ポートに一致する必要があります。<i>destination-ipv6-prefix/prefix-length</i> 引数のあとの <b>operator</b> は、宛先ポートに一致する必要があります。</p> <ul style="list-style-type: none"> <li>• (任意) <b>port-number</b> は、0 ~ 65535 の10進数またはTCPあるいはUDPポートの名前です。TCPポート名を使用できるのは、TCPのフィルタリング時だけです。UDPポート名を使用できるのは、UDPのフィルタリング時だけです。</li> <li>• (任意) <b>dscp value</b> を入力して、各IPv6パケットヘッダーのTraffic Classフィールド内のトラフィッククラス値とDiffServコードポイント値を照合します。指定できる範囲は0 ~ 63です。</li> <li>• (任意) <b>fragments</b> を入力して、先頭ではないフラグメントを確認します。このキーワードが表示されるのは、プロトコルが <b>ipv6</b> の場合だけです。</li> <li>• (任意) <b>log</b> を指定すると、エントリと一致するパケットに関するログメッセージがコンソールに送信されます。<b>log-input</b> を指定すると、ログエントリに入力インターフェイスが追加されます。ロギングはルータ ACL でだけサポートされます。</li> <li>• (任意) <b>sequence value</b> を入力して、アクセスリストステートメントのシーケンス番号を指定します。指定できる範囲は1 ~ 4,294,967,295です。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• (任意) <b>time-range name</b> を入力して、拒否または許可ステートメントに適用される時間の範囲を指定します。</li> </ul>
ステップ 5	<pre>{deny   permit} tcp {source-ipv6-prefix/prefix-length   any   host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length   any   host destination-ipv6-address} [operator [port-number]] [ack] [ dscp value] [established] [fin] [log] [log-input] [neq {port   protocol}] [psh] [range {port   protocol}] [rst] [ sequence value] [syn] [ time-range name] [urg]</pre>	<p>(任意) TCP アクセス リストおよびアクセス条件を定義します。</p> <p>TCP の場合は <b>tcp</b> を入力します。パラメータはステップ 3a で説明されているパラメータと同じですが、次に示すオプションのパラメータが追加されています。</p> <ul style="list-style-type: none"> <li>• <b>ack</b> : 確認応答 (ACK) ビットセット。</li> <li>• <b>established</b> : 確立された接続。TCP データグラムに ACK または RST ビットが設定されている場合、照合が行われます。</li> <li>• <b>fin</b> : 終了ビットセット。送信者からのデータはそれ以上ありません。</li> <li>• <b>neq {port   protocol}</b> : 所定のポート番号上にならないパケットだけを照合します。</li> <li>• <b>psh</b> : プッシュ機能ビットセット</li> <li>• <b>range {port   protocol}</b> : ポート番号の範囲内のパケットだけを照合します。</li> <li>• <b>rst</b> : リセットビットセット</li> <li>• <b>syn</b> : 同期ビットセット</li> <li>• <b>urg</b> : 緊急ポインタビットセット</li> </ul>
ステップ 6	<pre>{deny   permit} udp {source-ipv6-prefix/prefix-length   any   host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length   any   host destination-ipv6-address} [operator [port-number]] [ dscp value] [log] [log-input] [neq {port   protocol}] [range {port   protocol}] [ sequence value] [ time-range name]</pre>	<p>(任意) UDP アクセス リストおよびアクセス条件を定義します。</p> <p>ユーザ データグラム プロトコルの場合は、<b>udp</b> を入力します。UDP パラメータは TCP に関して説明されているパラメータと同じです。ただし、[operator [port]] のポート番号またはポート名は、UDP ポートの番号または名前であればなりません。UDP の場合、established パラメータは無効です。</p>
ステップ 7	<pre>{deny   permit} icmp {source-ipv6-prefix/prefix-length   any   host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length   any   host</pre>	<p>(任意) ICMP アクセス リストおよびアクセス条件を定義します。</p>



	コマンドまたはアクション	目的
	<code>destination-ipv6-address} [operator [port-number]]  [icmp-type [icmp-code]   icmp-message] [ dscp value]  [log] [log-input] [ sequence value] [ time-range name]</code>	<p>インターネット制御メッセージプロトコルの場合は、<b>icmp</b>を入力します。ICMPパラメータはステップ1のIPプロトコルの説明にあるパラメータとほとんど同じですが、ICMPメッセージタイプおよびコードパラメータが追加されています。オプションのキーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> <li>• <i>icmp-type</i> : ICMPメッセージタイプでフィルタリングする場合に入力します。指定できる値の範囲は、0～255です。</li> <li>• <i>icmp-code</i> : ICMPパケットをICMPメッセージコードタイプでフィルタリングする場合に入力します。指定できる値の範囲は、0～255です。</li> <li>• <i>icmp-message</i> : ICMPパケットをICMPメッセージタイプ名またはICMPメッセージタイプとコード名でフィルタリングする場合に入力します。ICMPメッセージのタイプ名およびコード名のリストについては、?キーを使用するか、またはこのリリースのコマンドリファレンスを参照してください。</li> </ul>
ステップ 8	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 9	<b>show ipv6 access-list</b>	アクセス リストの設定を確認します。
ステップ 10	<b>show running-config</b> 例 :  デバイス# <b>show running-config</b>	入力を確認します。
ステップ 11	<b>copy running-config startup-config</b> 例 :  デバイス# <b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。

## インターフェイスへの IPv6 ACL の付加

レイヤ3 インターフェイスで発信または着信トラフィックに ACL を、あるいはレイヤ2 インターフェイスで着信トラフィックに を適用できます。レイヤ3 インターフェイスで着信トラフィックにだけ ACL を適用できます。

インターフェイスへのアクセスを制御するには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **interface interface-id**
4. **no switchport**
5. **ipv6 address ipv6-address**
6. **ipv6 traffic-filter access-list-name {in | out}**
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  デバイス> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  デバイス# <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 3	<b>interface interface-id</b>	アクセスリストを適用するレイヤ2 インターフェイス（ポート ACL 用）またはレイヤ3 インターフェイス（ルータ ACL 用）を特定して、インターフェイス コンフィギュレーションモードを開始します。
ステップ 4	<b>no switchport</b>	ルータ ACL を適用する場合は、これによってインターフェイスがレイヤ2 モード（デフォルト）からレイヤ3 モードに変化します。
ステップ 5	<b>ipv6 address ipv6-address</b>	レイヤ3 インターフェイス（ルータ ACL 用）で IPv6 アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 6	<b>ipv6 traffic-filter</b> <i>access-list-name</i> { <b>in</b>   <b>out</b> }	インターフェースの着信トラフィックまたは発信トラフィックにアクセスリストを適用します。
ステップ 7	<b>end</b> 例：  デバイス(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 8	<b>show running-config</b> 例：  デバイス# <b>show running-config</b>	入力を確認します。
ステップ 9	<b>copy running-config startup-config</b> 例：  デバイス# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## VLAN マップの設定

VLAN マップを作成して、1つまたは複数の VLAN に適用するには、次のステップを実行します。

始める前に

VLAN に適用する IPv6 ACL を作成します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **vlan access-map** *name* [*number*]
4. **match** {**ip** | **ipv6** | **mac**} **address** {*name* | *number*} [*name* | *number*]
5. IP パケットまたは非 IP パケットを（既知の 1 MAC アドレスのみを使って）指定し、1つ以上の ACL とそのパケットを照合するには、次のコマンドのいずれかを入力します。

- **action** { **forward** }

```
デバイス(config-access-map)# action forward
```

- **action** { **drop** }

```
デバイス(config-access-map)# action drop
```

6. `vlan filter mapname vlan-list list`

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : デバイス> <b>enable</b>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>パスワードを入力します (要求された場合)。</li> </ul>
ステップ 2	<b>configure terminal</b> 例 : デバイス# <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 3	<b>vlan access-map name [number]</b> 例 : デバイス (config)# <b>vlan access-map map_1 20</b>	<p>VLAN マップを作成し、名前と、任意で番号を付けます。番号は、マップ内のエントリのシーケンス番号です。</p> <p>同じ名前の VLAN マップを作成すると、10 ずつ増加する番号が順に割り当てられます。マップを変更または削除するときは、該当するマップエントリの番号を入力できます。</p> <p>VLAN マップでは、特定の <code>permit</code> または <code>deny</code> キーワードを使用しません。VLAN マップを使用してパケットを拒否するには、パケットを照合する ACL を作成して、アクションをドロップに設定します。ACL 内の <code>permit</code> は、一致するという意味です。ACL 内の <code>deny</code> は、一致しないという意味です。</p> <p>このコマンドを入力すると、アクセス マップ コンフィギュレーション モードに変わります。</p>
ステップ 4	<b>match {ip   ipv6   mac} address {name   number} [name   number]</b> 例 : デバイス (config-access-map)# <b>match ipv6 address ip_net</b>	パケットを1つまたは複数のアクセスリストに対して照合します。パケットの照合は、対応するプロトコルタイプのアクセスリストに対してだけ行われます。IP パケットは、IP アクセスリストに対して照合されます。非 IP パケットは、名前付き MAC アクセスリストに対してだけ照合されます。

	コマンドまたはアクション	目的
		(注) パケットタイプ (IP または MAC) に対する <code>match</code> 句が VLAN マップに設定されている場合で、そのマップアクションがドロップの場合は、そのタイプに一致するすべてのパケットがドロップされます。 <code>match</code> 句が VLAN マップになく、設定されているアクションがドロップの場合は、すべての IP およびレイヤ 2 パケットがドロップされます。
ステップ 5	<p>IP パケットまたは非 IP パケットを (既知の 1 MAC アドレスのみを使って) 指定し、1 つ以上の ACL とそのパケットを照合するには、次のコマンドのいずれかを入力します。</p> <ul style="list-style-type: none"> <li>• <b>action { forward }</b>            デバイス (config-access-map) # action forward</li> <li>• <b>action { drop }</b>            デバイス (config-access-map) # action drop</li> </ul>	マップエントリに対するアクションを設定します。
ステップ 6	<p><b>vlan filter mapname vlan-list list</b></p> <p>例 :</p> <pre>デバイス (config) # vlan filter map 1 vlan-list 20-22</pre>	<p>VLAN マップを 1 つまたは複数の VLAN に適用します。</p> <p><code>list</code> には単一の VLAN ID (22)、連続した範囲 (10 ~ 22)、または VLAN ID のストリング (12、22、30) を指定できます。カンマやハイフンの前後にスペースを挿入することもできます。</p>

## VLAN への VLAN マップの適用

VLAN マップを 1 つまたは複数の VLAN に適用するには、次の手順に従います。

### 手順の概要

- 1.
2. **configure terminal**
3. **vlan filter mapname vlan-list list**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1		
ステップ 2	<b>configure terminal</b> 例：  デバイス# <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 3	<b>vlan filter mapname vlan-list list</b> 例：  デバイス(config)# <b>vlan filter map 1 vlan-list 20-22</b>	VLAN マップを 1 つまたは複数の VLAN に適用します。  list には単一の VLAN ID (22)、連続した範囲 (10 ~ 22)、または VLAN ID のストリング (12、22、30) を指定できます。カンマやハイフンの前後にスペースを挿入することもできます。
ステップ 4	<b>end</b> 例：  デバイス(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show running-config</b> 例：  デバイス# <b>show running-config</b>	アクセス リストの設定を表示します。
ステップ 6	<b>copy running-config startup-config</b> 例：  デバイス# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## IPv6 ACL のモニタリング

次の表に示された 1 つまたは複数の特権 EXEC コマンドを使用して、設定済みのすべてのアクセスリスト、すべての IPv6 アクセスリスト、または特定のアクセスリストに関する情報を表示できます。

表 37: *show ACL* コマンド

コマンド	目的
<b>show access-lists</b>	スイッチに設定されたすべてのアクセス リストを表示します。
<b>show ipv6 access-list</b> [ <i>access-list-name</i> ]	設定済みのすべての IPv6 アクセス リストまたは名前指定されたアクセス リストを表示します。
<b>show vlan access-map</b> [ <i>map-name</i> ]	VLAN アクセス マップ設定を表示します。
<b>show vlan filter</b> [ <i>access-map access-map</i>   <i>vlan vlan-id</i> ]	VACL と VLAN 間のマッピングを表示します。

次に、`show access-lists` 特権 EXEC コマンドの出力例を示します。出力には、スイッチまたはスイッチ スタックに設定済みのすべてのアクセス リストが表示されます。

```
Switch # show access-lists
Extended IP access list hello
  10 permit ip any any
IPv6 access list ipv6
  permit ipv6 any any sequence 10
```

次に、`show ipv6 access-lists` 特権 EXEC コマンドの出力例を示します。出力には、スイッチまたはスイッチ スタックに設定済みの IPv6 アクセス リストだけが表示されます。

```
Switch# show ipv6 access-list
IPv6 access list inbound
  permit tcp any any eq bgp (8 matches) sequence 10
  permit tcp any any eq telnet (15 matches) sequence 20
  permit udp any any sequence 30
IPv6 access list outbound
  deny udp any any sequence 10
  deny tcp any any eq telnet sequence 20
```

次に、`show vlan access-map` 特権 EXEC コマンドの出力例を示します。出力には、VLAN アクセス マップ情報が表示されます。

```
Switch# show vlan access-map
Vlan access-map "m1" 10
  Match clauses:
    ipv6 address: ip2
  Action: drop
```

## IPv6 ACL の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	IPv6 ACL	IPv6 ACL を作成して、インターフェイスに適用することによって、IPv6 トラフィックをフィルタリングできます。これは、IPv4 の名前付き ACL を作成し、適用する方法と類似しています。レイヤ 3 管理トラフィックをフィルタリングするために、入ルータ ACL を作成し、適用することもできます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。





## 第 18 章

# DHCP の設定

- DHCP の設定に関する制限 (395 ページ)
- DHCP に関する情報 (395 ページ)
- DHCP 機能の設定方法 (403 ページ)
- DHCP サーバー ポートベースのアドレス割り当ての設定 (411 ページ)
- DHCP の機能情報 (416 ページ)

## DHCP の設定に関する制限

DHCP スヌーピング、DHCP リレーエージェントをサポートする送信 (Tx) スイッチドポートアナライザ (SPAN) または出力 SPAN は使用しないことを推奨します。Tx での SPAN が必要な場合は、DHCP パケットの転送パスに含まれる VLAN ポートを使用しないでください。

## DHCP に関する情報

### DHCP サーバ

DHCP サーバーは、スイッチまたはルータ上の指定されたアドレス プールから DHCP クライアントに IP アドレスを割り当て、それらのアドレスを管理します。DHCP サーバーがそのデータベースから要求された設定パラメータを取得して DHCP クライアントに渡すことができない場合は、ネットワーク管理者が定義した 1 つまたは複数のセカンダリ DHCP サーバーに要求を転送します。スイッチは、DHCP サーバーとして機能できます。

### DHCP リレー エージェント

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 パケットを転送するレイヤ 3 デバイスです。リレー エージェントは、同じ物理サブネット上にないクライアントとサーバの間で要求および応答を転送します。リレー エージェントによる転送は、IP データグラムをネットワーク間で透過的に交換するレイヤ 2 での通常の転送とは異なります。リレー エ

ジェントは、DHCP メッセージを受け取ると、新しい DHCP メッセージを生成して、出力インターフェイス上で送信します。

## DHCP スヌーピング

DHCP スヌーピングは、信頼できない DHCP メッセージのフィルタリングと 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 バインディング テーブルとも呼ばれる）の作成および管理によってネットワーク セキュリティを確保する DHCP セキュリティ機能です。

DHCP スヌーピングは、信頼できないホストと DHCP サーバの間でファイアウォールに似た役割を果たします。DHCP スヌーピングを使用することにより、エンドユーザーに接続された信頼できないインターフェイスと DHCP サーバーまたは別のスイッチに接続された信頼できるインターフェイスを区別できます。



- (注) DHCP スヌーピングが正常に機能するには、すべての DHCP サーバを信頼できるインターフェイスを介してスイッチに接続し、信頼できない DHCP メッセージが信頼できるインターフェイスにだけ転送されるようにする必要があります。

信頼できない DHCP メッセージとは、信頼できないインターフェイス経由で送信されたメッセージのことです。デフォルトでは、スイッチはすべてのインターフェイスを信頼できないものと見なします。そのため、スイッチはいくつかのインターフェイスを信頼して DHCP スヌーピングを使用するように設定する必要があります。サービス プロバイダ環境で DHCP スヌーピングを使用する場合は、カスタマーのスイッチなど、サービス プロバイダ ネットワーク内には存在しないデバイスから送信されたメッセージが信頼できないメッセージとなります。不明なデバイスから送信されたメッセージは、トラフィック攻撃の原因になりうるため、信頼できません。

DHCP スヌーピング バインディング データベースには、MAC アドレス、IP アドレス、リース期間、バインディングの種類、VLAN 番号、およびスイッチの信頼できないローカルインターフェイスのインターフェイス情報が含まれています。このデータベースには、信頼できるインターフェイスに接続されたホストの情報はありません。

サービス プロバイダー ネットワークでは、信頼できるインターフェイスとして設定できるものの例として、同じネットワーク内のデバイスのポートに接続されたインターフェイスがあります。信頼できないインターフェイスには、ネットワーク内の信頼できないインターフェイスまたはネットワークに属さないデバイスのインターフェイスに接続されたインターフェイスがあります。

スイッチが信頼できないインターフェイスでパケットを受信し、そのインターフェイスが属している VLAN で DHCP スヌーピングがイネーブルに設定されている場合、スイッチは送信元 MAC アドレスと DHCP クライアントのハードウェアアドレスを比較します。アドレスが一致した場合（デフォルト）、スイッチはパケットを転送します。アドレスが一致しない場合、スイッチはパケットをドロップします。

スイッチは、次のいずれかの状況が発生した場合に DHCP パケットをドロップします。

- DHCP OFFER パケット、DHCP ACK パケット、DHCP NAK パケット、DHCP LEASE QUERY パケットなど、DHCP サーバからのパケットがネットワークまたはファイアウォールの外側から着信した。
- パケットが信頼できないインターフェイスに着信し、送信元 MAC アドレスと DHCP クライアントのハードウェア アドレスが一致しない。
- スイッチが DHCP RELEASE または DHCP DECLINE ブロードキャスト メッセージを受信し、その MAC アドレスは DHCP スヌーピング バインディング データベースに含まれているが、バインディング データベース内のインターフェイス情報がメッセージを受信したインターフェイスと一致しない。
- DHCP リレー エージェントが 0.0.0.0 以外のリレー エージェント IP アドレスを含む DHCP パケットを転送し、Option 82 情報が含まれないパケットを信頼できないポートに転送する。

DHCP スヌーピングをサポートする集約スイッチであり、DHCP オプション 82 情報を挿入するエッジスイッチに接続されているスイッチは、オプション 82 情報を含むパケットが信頼できないインターフェイスに着信した場合、それらのパケットをドロップします。DHCP スヌーピングがイネーブルに設定されている場合に、パケットが信頼できるポートに着信しても、集約スイッチは接続されたデバイスの DHCP スヌーピング バインディングを認識せず、完全な DHCP スヌーピング バインディング データベースを作成できません。

集約スイッチを信頼できないインターフェイス経由でエッジスイッチに接続できる場合、**ip dhcp snooping information option allow-untrusted** グローバル コンフィギュレーション コマンドを入力すると、集約スイッチはエッジスイッチによって挿入されたオプション 82 情報を含むパケットを受け入れます。集約スイッチは、信頼できないスイッチインターフェイスを介して接続されたホストのバインディングを認識します。集約スイッチで、ダイナミック ARP インスペクションや IP ソース ガードなど、DHCP セキュリティ機能をイネーブルに設定することもできますが、その場合でもスイッチは Option 82 情報を含むパケットをホストが接続されている信頼できない入力インターフェイスで受信します。集約スイッチ上のエッジスイッチとの接続ポートは、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。

## オプション 82 データ挿入

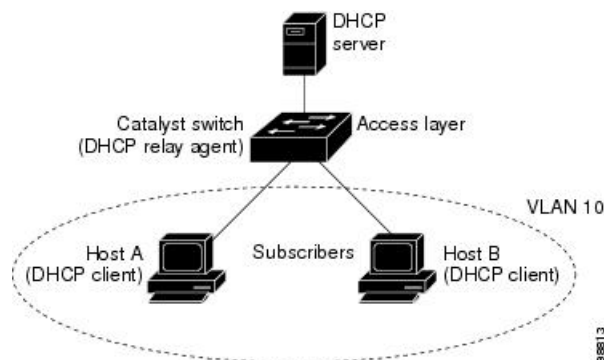
住宅地域にあるメトロポリタンイーサネットアクセス環境では、DHCP は多数の加入者に対し、IP アドレスの割り当てを一元的に管理できます。スイッチで DHCP スヌーピングの Option 82 機能をイネーブルにすると、加入者装置は MAC アドレスだけでなく、その装置をネットワークに接続するスイッチポートによっても識別されます。サブスクライバ LAN 上の複数のホストをアクセススイッチの同じポートに接続できます。これらのホストは一意に識別されません。



- (注) DHCP オプション 82 機能は、DHCP スヌーピングがグローバルに有効であり、オプション 82 を使用する加入者装置が割り当てられた VLAN で有効である場合に限りサポートされます。

次の図に、一元的な DHCP サーバーがアクセスレイヤのスイッチに接続された加入者に IP アドレスを割り当てるメトロポリタンイーサネットネットワークを示します。DHCP クライアントとそれらに関連付けられた DHCP サーバは同じ IP ネットワークまたはサブネット内に存在しないため、DHCP リレーエージェント (Catalyst スイッチ) にヘルパーアドレスを設定することにより、ブロードキャスト転送をイネーブルにし、クライアントとサーバ間で DHCP メッセージを転送します。

図 20: メトロポリタンイーサネットネットワークにおける DHCP リレーエージェント



スイッチで DHCP スヌーピング情報 オプション 82 を有効にすると、次のイベントがこの順序で発生します。

- ホスト (DHCP クライアント) は DHCP 要求を生成し、これをネットワーク上にブロードキャストします。
- スイッチは、この DHCP 要求を受信すると、パケットに Option 82 情報を追加します。デフォルトでは、リモート ID サブオプションがスイッチの MAC アドレスで、回線 ID サブオプションはパケットを受信するポート ID (**vlan-mod-port**) です。リモート ID および回線 ID は設定できます。
- リレーエージェントの IP アドレスが設定されている場合、スイッチはこの IP アドレスを DHCP パケットに追加します。
- スイッチは、オプション 82 フィールドを含む DHCP 要求を DHCP サーバーに転送します。
- DHCP サーバはこのパケットを受信します。Option 82 に対応しているサーバであれば、リモート ID と回線 ID のいずれか一方または両方を使用して、IP アドレスを割り当てたり、1つのリモート ID または回線 ID に割り当てることができる IP アドレスの数を制限するようなポリシーを実装したりできます。次に DHCP サーバは、DHCP 応答内にオプション 82 フィールドをエコーします。
- スイッチによって要求がサーバーにリレーされた場合、DHCP サーバは応答をスイッチにユニキャストします。スイッチは、リモート ID フィールドと、場合によっては回線 ID フィールドを調べ、Option 82 データが挿入済みであることを確認します。スイッチは Option 82 フィールドを削除してから、DHCP 要求を送信した DHCP クライアントに接続するスイッチポートにパケットを転送します。

デフォルトのサブオプション設定では、前述のイベントのシーケンスが発生すると、次のフィールドの値は変化しません（図「サブオプションの packets 形式」を参照）。

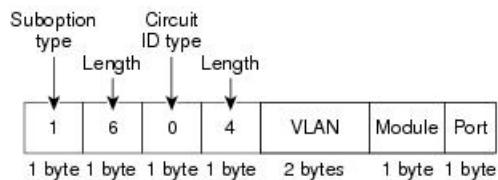
- 回線 ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - 回線 ID タイプ
  - 回線 ID タイプの長さ
  
- リモート ID サブオプション フィールド
  - サブオプション タイプ
  - サブオプション タイプの長さ
  - リモート ID タイプ
  - リモート ID タイプの長さ

回線 ID サブオプションのポートフィールドでは、ポート番号が 3 から始まります。たとえば、24 個の 10/100/1000 ポートおよび 4 つの Small Form-Factor Pluggable (SFP) モジュール スロットを搭載するスイッチでは、ポート 3 がギガビットイーサネット 1/0/1 ポート、ポート 4 がギガビットイーサネット 1/0/2 ポートとなり、以降同様に続きます。ポート 27 は SFP モジュール スロットのギガビットイーサネット 1/0/25 となり、以降同様に続きます。

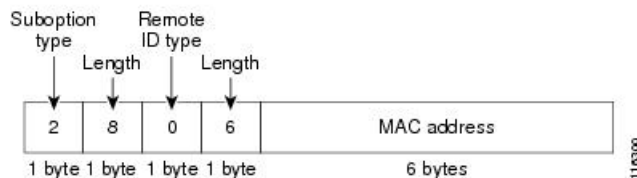
図「サブオプションの packets 形式」に、デフォルトのサブオプション設定が使用されている場合のリモート ID サブオプションおよび回線 ID サブオプションの packets 形式を示します。回線 ID サブオプションでは、モジュール番号は、スタックにあるスイッチ番号に対応します。スイッチがこれらの packets 形式を使用するのは、DHCP スヌーピングをグローバルに有効にし、`ip dhcp snooping information option` グローバル コンフィギュレーション コマンドを入力した場合です。

図 21: サブオプションの packets 形式

## Circuit ID Suboption Frame Format



## Remote ID Suboption Frame Format

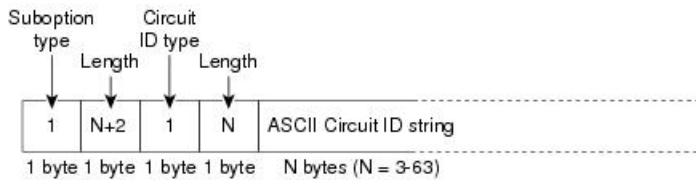
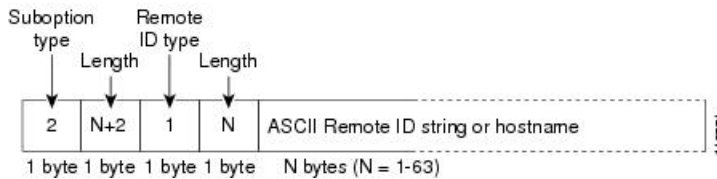


図「ユーザー設定のサブオプションの packets 形式」は、ユーザー設定のリモート ID サブオプション、および回線 ID サブオプションの packets 形式を示しています。スイッチでは、DHCP スヌーピングをグローバルにイネーブルにし、**ip dhcp snooping information option format remote-id** グローバル コンフィギュレーション コマンド、および **ip dhcp snooping vlan information option format-type circuit-id string** インターフェイス コンフィギュレーション コマンドを入力した場合に、これらの packets 形式が使用されます。

packets では、リモート ID および回線 ID サブオプションを次のように設定した場合、これらのフィールドの値がデフォルト値から変更されます。

- 回線 ID サブオプション フィールド
  - 回線 ID タイプが 1 である。
  - 設定した文字列の長さに応じて、長さの値が変化する。
- リモート ID サブオプション フィールド
  - リモート ID タイプが 1 である。
  - 設定した文字列の長さに応じて、長さの値が変化する。

図 22: ユーザ設定のサブオプションの packets 形式

**Circuit ID Suboption Frame Format (for user-configured string):****Remote ID Suboption Frame Format (for user-configured string):**

## Cisco IOS DHCP サーバ データベース

DHCP ベースの自動設定プロセスの間、指定 DHCP サーバは Cisco IOS DHCP サーバデータベースを使用します。これには IP アドレス、アドレスバインディング、およびブートファイルなどの設定パラメータが含まれます。

アドレスバインディングは、Cisco IOS DHCP サーバデータベース内のホストの IP アドレスおよび MAC アドレス間のマッピングです。クライアント IP アドレスを手動で割り当てること、または、DHCP サーバが DHCP アドレスプールから IP アドレスを割り当てるのが可能です。手動および自動アドレスバインディングの詳細については、『*Cisco IOS IP Configuration Guide, Release 12.4*』の「Configuring DHCP」の章を参照してください。

Cisco IOS DHCP サーバデータベースをイネーブルにして設定する手順については、『*Cisco IOS IP Configuration Guide, Release 12.4*』の「Configuring DHCP」の章にある「DHCP Configuration Task List」の項を参照してください。

## DHCP スヌーピングバインディングデータベース

DHCP スヌーピングをイネーブルにすると、スイッチは信頼できないインターフェイスに関する情報を DHCP スヌーピングバインディングデータベースに保存します。データベースには、64,000 のバインディングを含めることができます。

各データベースエントリ（バインディング）は、IP アドレス、それに関連付けられた MAC アドレス、リース期間（16 進形式）、バインディングが適用されるインターフェイス、およびインターフェイスが属する VLAN で構成されます。データベースエージェントは、設定された場所のファイルにバインディングを保存します。各エントリの末尾にあるチェックサムは、ファイルの先頭のバイトを含め、エントリに関連付けられたすべてのバイトを対象として計算されます。各エントリは、まず 77 バイトのデータがあり、その後 1 つのスペースとチェックサム値と EOL 記号が続きます。

スイッチのリロード後もバインディングを保持するには、DHCP スヌーピング データベース エージェントを使用する必要があります。エージェントがディセーブルで、ダイナミック ARP インスペクションまたは IP ソース ガードがイネーブルにされ、DHCP スヌーピング バインディング データベースがダイナミックバインディングされている場合、スイッチは接続を切断されます。このエージェントがディセーブルで、DHCP スヌーピングだけがイネーブルである場合、スイッチの接続は切断されませんが、DHCP スヌーピングは DHCP スプーフィング攻撃を防止できないことがあります。

リロードすると、スイッチはバインディング ファイルを読み込み、DHCP スヌーピング バインディング データベースを作成します。スイッチは、データベースに変更が加えられたときにはバインディング ファイルを更新します。

スイッチは、新しいバインディングを認識するか、バインディングを失うと、ただちにデータベース内のエントリを更新します。スイッチはバインディングファイル内のエントリも更新します。バインディングファイルの更新頻度は設定可能な遅延時間によって決まり、更新はバッチ処理されます。ファイルが指定された時間内（書き込み遅延およびキャンセルタイムアウトの値によって設定される）に更新されない場合、更新は停止します。

バインディングが含まれるファイルの形式は次のとおりです。

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<entry-1> <checksum-1>
<entry-2> <checksum-1-2>
...
...
<entry-n> <checksum-1-2-...-n>
END
```

このファイルの各エントリにはチェックサム値を示すタグが付けられます。スイッチは、ファイルを読み取るときに、このチェックサムを使用してエントリを検証します。最初の行の `initial-checksum` エントリは、最新のファイル更新に関連するエントリを以前のファイル更新に関連するエントリと区別します。

次に、バインディング ファイルの例を示します。

```
3ebe1518
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
10.1.1.1 512 001.0001.0005 3EBE2881 Gi1/1                e5e1e733
10.1.1.1 512 001.0001.0002 3EBE2881 Gi1/1                4b3486ec
10.1.1.1 1536 001.0001.0004 3EBE2881 Gi1/1              f0e02872
10.1.1.1 1024 001.0001.0003 3EBE2881 Gi1/1              ac41adf9
10.1.1.1 1 001.0001.0001 3EBE2881 Gi1/1                 34b3273e
END
```

スイッチが起動し、計算されたチェックサム値が保存されているチェックサム値と一致した場合、スイッチはバインディング ファイルのエントリを読み取り、バインディングを DHCP スヌーピング バインディング データベースに追加します。次のいずれかの状況が発生した場合、スイッチはエントリを無視します。



- スイッチがエントリを読み取り、計算されたチェックサム値が保存されているチェックサム値と一致しない。この場合、そのエントリとそれ以降のエントリは無視されます。
- エントリに含まれているリース期間が終了している（スイッチはリース期間の終了時にバインディング エントリを削除しないことがある）。
- エントリに含まれるインターフェイスが現在はシステムに存在しない。
- インターフェイスがルーテッド インターフェイスまたは DHCP スヌーピングにおける信頼できるインターフェイスである。

## DHCP スヌーピングおよびスイッチ スタック

DHCP スヌーピングは、アクティブスイッチで管理されます。新しいスイッチは、スタックに追加されると、アクティブスイッチから DHCP スヌーピング設定を受信します。メンバースイッチがスタックから除外されると、スイッチに関連付けられているすべての DHCP スヌーピング アドレス バインディングがエージングアウトします。

すべてのスヌーピング統計情報は、アクティブスイッチ上で生成されます。新しいアクティブスイッチが選定された場合、統計カウンタはリセットされます。

スタックのマージが発生し、アクティブスイッチではなくなった場合、アクティブスイッチにあったすべての DHCP スヌーピング バインディングが失われます。スタックパーティションを使用すると、既存のアクティブスイッチは変更されず、パーティション分割されたスイッチに属しているバインディングはエージングアウトします。パーティション分割されたスタックの新しいアクティブスイッチで、新たな着信 DHCP パケットの処理が開始されます。

## DHCP 機能の設定方法

### DHCP スヌーピングのデフォルト設定

表 38: DHCP のデフォルト設定

機能	デフォルト設定
DHCP サーバ	Cisco IOS ソフトウェアではイネーブル、設定が必要 <sup>6</sup>
DHCP リレー エージェント	イネーブル <sup>7</sup>
DHCP パケット転送アドレス	未設定
リレー エージェント情報の確認	イネーブル（無効なメッセージは廃棄）
DHCP リレー エージェント転送ポリシー	既存のリレー エージェント情報を置換。

機能	デフォルト設定
DHCP スヌーピングをグローバルにイネーブル	ディセーブル
DHCP スヌーピング情報オプション	イネーブル
パケットを信頼できない入力インターフェイスで受け取る DHCP スヌーピング オプション <sup>8</sup>	ディセーブル
DHCP スヌーピング レート制限	未設定
DHCP スヌーピング信頼状態	信頼できない
DHCP スヌーピング VLAN	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
Cisco IOS DHCP サーバ バインディング データベース	Cisco IOS ソフトウェアではイネーブル、設定が必要。  (注) スイッチは、DHCP サーバとして設定されているデバイスからだけ、ネットワークアドレスおよび設定パラメータを取得します。
DHCP スヌーピングバインディングデータベース エージェント	Cisco IOS ソフトウェアではイネーブル、設定が必要。この機能は宛先が設定されている場合に限り有効。

- <sup>6</sup> スイッチは、DHCP サーバとして設定されている場合に限り DHCP 要求に応答します。
- <sup>7</sup> スイッチは、DHCP サーバの IP アドレスが DHCP クライアントの SVI に設定されている場合に限り DHCP パケットをリレーします。
- <sup>8</sup> この機能は、スイッチがエッジスイッチによってオプション 82 情報が挿入されたパケットを受信する集約スイッチである場合に使用します。

## DHCP スヌーピング設定時の注意事項

- スイッチポートが DHCP サーバに接続されている場合は、**ip dhcp snooping trust interface** コンフィギュレーションコマンドを入力して、ポートを信頼できるポートとして設定してください。
- スイッチポートが DHCP クライアントに接続されている場合は、**no ip dhcp snooping trust** インターフェイス コンフィギュレーション コマンドを入力して、ポートを信頼できないポートとして設定してください。
- **show ip dhcp snooping statistics** ユーザー EXEC コマンドを入力して DHCP スヌーピング統計情報を表示したり、**clear ip dhcp snooping statistics** 特権 EXEC コマンドを入力してスヌーピング統計情報をクリアしたりできるようになりました。

## DHCP サーバの設定

スイッチは、DHCP サーバーとして機能できます。

スイッチを DHCP サーバーとして設定するときの手順については、『*Cisco IOS IP Configuration Guide, Release 12.4*』の「IP Addressing and Services」の項の「Configuring DHCP」を参照してください。

## DHCP サーバーとスイッチ スタック

DHCP バインディングデータベースは、スタックのアクティブスイッチで管理されます。新しいアクティブスイッチが割り当てられると、新しいアクティブスイッチに、TFTP サーバーで保存されているバインディングデータベースがダウンロードされます。スイッチオーバーが発生した場合、新しいアクティブスイッチスタックは SSO 機能を使用して以前のアクティブスイッチスタックから同期されたデータベースファイルを使用します。失われたバインディングに関連付けられていた IP アドレスは、解放されます。自動バックアップは、**ip dhcp database url [ timeout seconds | write-delay seconds ]** グローバル コンフィギュレーション コマンドを使用して設定する必要があります。

## DHCP リレー エージェントの設定

スイッチ上で DHCP リレー エージェントをイネーブルにするには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **service dhcp**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  デバイス> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  デバイス# <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。

	コマンドまたはアクション	目的
ステップ 3	<b>service dhcp</b> 例：  デバイス(config)# <b>service dhcp</b>	スイッチ上で DHCP サーバおよび DHCP リレーエージェントをイネーブルにします。デフォルトでは、この機能はイネーブルです。
ステップ 4	<b>end</b> 例：  デバイス(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show running-config</b> 例：  デバイス# <b>show running-config</b>	入力を確認します。
ステップ 6	<b>copy running-config startup-config</b> 例：  デバイス# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

#### 次のタスク

- リレー エージェント情報のチェック (検証)
- リレー エージェント転送ポリシーの設定

## パケット転送アドレスの指定

DHCP サーバおよび DHCP クライアントが異なるネットワークまたはサブネットにある場合、スイッチを **ip helper-address address** インターフェイス コンフィギュレーション コマンドで設定する必要があります。一般的なルールは、クライアントに最も近いレイヤ 3 インターフェイス上にコマンドを設定することです。 **ip helper-address** コマンドで使用されているアドレスは、特定の DHCP サーバ IP アドレスか、または他の DHCP サーバが宛先ネットワークセグメントにある場合はネットワークアドレスにすることができます。ネットワークアドレスを使用することで、どの DHCP サーバも要求に応答できるようになります。

パケット転送アドレスを指定するには、特権 EXEC モードで次の手順を実行します。

#### 手順の概要

1. **enable**
2. **configure terminal**

3. **interface vlan** *vlan-id*
4. **ip address** *ip-address subnet-mask*
5. **ip helper-address** *address*
6. **end**
7. 次のいずれかを使用します。
  - **interface range** *port-range*
  - **interface** *interface-id*
8. **switchport mode access**
9. **switchport access vlan** *vlan-id*
10. **end**
11. **show running-config**
12. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  デバイス> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  デバイス# <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 3	<b>interface vlan</b> <i>vlan-id</i> 例：  デバイス(config)# <b>interface vlan</b> 1	VLAN ID を入力してスイッチ仮想インターフェイスを作成し、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 address</b> <i>ip-address subnet-mask</i> 例：  デバイス(config-if)# <b>ip address</b> 192.108.1.27 255.255.255.0	インターフェイスに IP アドレスおよび IP サブネットを設定します。
ステップ 5	<b>ip helper-address</b> <i>address</i> 例：  デバイス(config-if)# <b>ip helper-address</b> 172.16.1.2	DHCP パケット転送アドレスを指定します。  ヘルパー アドレスは特定の DHCP サーバアドレスにするか、他の DHCP サーバが宛先ネットワークセグメントにある場合は、ネットワーク アドレスにすることができます。ネットワーク アドレスを

	コマンドまたはアクション	目的
		<p>使用することで、他のサーバも DHCP 要求に応答できるようになります。</p> <p>複数のサーバがある場合、各サーバに 1 つのヘルパー アドレスを設定できます。</p>
ステップ 6	<p><b>end</b></p> <p>例 :</p> <p>デバイス (config-if) # end</p>	<p>グローバル コンフィギュレーション モードに戻ります。</p>
ステップ 7	<p>次のいずれかを使用します。</p> <ul style="list-style-type: none"> <li>• <b>interface range port-range</b></li> <li>• <b>interface interface-id</b></li> </ul> <p>例 :</p> <p>デバイス (config) # interface gigabitethernet1/0/2</p>	<p>DHCP クライアントに接続されている複数の物理ポートを設定し、インターフェイス範囲コンフィギュレーションモードを開始します。</p> <p>または</p> <p>DHCP クライアントに接続されている単一の物理ポートを設定し、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。</p>
ステップ 8	<p><b>switchport mode access</b></p> <p>例 :</p> <p>デバイス (config-if) # switchport mode access</p>	<p>ポートの VLAN メンバーシップモードを定義します。</p>
ステップ 9	<p><b>switchport access vlan vlan-id</b></p> <p>例 :</p> <p>デバイス (config-if) # switchport access vlan 1</p>	<p>ステップ 2 で設定したのと同じ VLAN をポートに割り当てます。</p>
ステップ 10	<p><b>end</b></p> <p>例 :</p> <p>デバイス (config-if) # end</p>	<p>特権 EXEC モードに戻ります。</p>
ステップ 11	<p><b>show running-config</b></p> <p>例 :</p> <p>デバイス # show running-config</p>	<p>入力を確認します。</p>
ステップ 12	<p><b>copy running-config startup-config</b></p> <p>例 :</p> <p>デバイス # copy running-config startup-config</p>	<p>(任意) コンフィギュレーション ファイルに設定を保存します。</p>

## DHCP スヌーピングおよびオプション 82 を設定するための前提条件

DHCP スヌーピングおよびオプション 82 の前提条件は次のとおりです。

- DHCP スヌーピングは、スイッチ上でグローバルにイネーブルにする必要があります。
- スwitch上でDHCP スヌーピングをグローバルにイネーブルにする前に、DHCP サーバーや DHCP リレー エージェントとして機能するデバイスが設定され、イネーブルになっていることを確認してください。
- スwitchを DHCP 要求に応答するようにする場合は、DHCP サーバーとして設定する必要があります。
- スwitchでDHCP スヌーピング情報オプションを設定する前に、DHCP サーバーとして機能するデバイスを設定してください。DHCP サーバーが割り当てたり除外したりできる IP アドレスを指定するか、またはそれらのデバイスの DHCP オプションを設定する必要があります。
- DHCP スヌーピングが正常に機能するには、すべての DHCP サーバを信頼できるインターフェイスを介してスイッチに接続し、信頼できない DHCP メッセージが信頼できるインターフェイスにだけ転送されるようにする必要があります。サービス プロバイダ ネットワークでは、同じネットワーク内のデバイスのポートに接続されたインターフェイスが信頼できるインターフェイスとなります。
- DHCP スヌーピングで Cisco IOS DHCP サーバー バインディング データベースを使用するには、Cisco IOS DHCP サーバー バインディング データベースを使用するようにスイッチを設定する必要があります。
- 信頼できない入力でパケットを受け入れる DHCP スヌーピング オプションを使用するには、スイッチがエッジ スwitchからオプション 82 情報を含むパケットを受信する集約 スwitchである必要があります。
- 次の前提条件が DHCP スヌーピング バインディング データベースの設定に適用されます。
  - DHCP スヌーピング用にスイッチを使用するには、DHCP スヌーピング バインディング データベースで宛先を設定する必要があります。
  - NVRAM とフラッシュ メモリは、いずれも記憶容量が限られているため、バインディング ファイルを TFTP サーバーに保存することを推奨します。
  - ネットワーク ベースの URL (TFTP や FTP など) については、スイッチがバインディングをその URL のバインディング ファイルに初めて書き込む前に、設定された URL に空のファイルを作成する必要があります。空のファイルをサーバ上に作成する必要があるかどうかについては、TFTP サーバのマニュアルを参照してください。TFTP サーバによっては、そのように設定できないことがあります。
  - データベースに正しいリース期間が記録されるように、ネットワーク タイム プロトコル (NTP) をイネーブルにし、設定することを推奨します。

- NTP が設定されている場合、スイッチのシステム クロックが NTP と同期化されたときにだけ、スイッチがバインディングの変更内容をバインディングファイルに書き込みます。
- スイッチで DHCP リレー エージェントを設定する前に、DHCP サーバとして機能するデバイスを設定してください。DHCP サーバが割り当てたり除外したりできる IP アドレスを指定するか、デバイスの DHCP オプションを設定するか、または DHCP データベース エージェントをセットアップする必要があります。
- スイッチが DHCP パケットをリレーするようにする場合は、DHCP サーバの IP アドレスは DHCP クライアントのスイッチ仮想インターフェイス (SVI) に設定する必要があります。
- スイッチポートが DHCP サーバに接続されている場合は、**ip dhcp snooping trust interface** コンフィギュレーション コマンドを入力して、ポートを信頼できるポートとして設定してください。
- スイッチポートが DHCP クライアントに接続されている場合は、**no ip dhcp snooping trust** インターフェイス コンフィギュレーション コマンドを入力して、ポートを信頼できないポートとして設定してください。

## Cisco IOS DHCP サーバ データベースのイネーブル化

Cisco IOS DHCP サーバ データベースをイネーブルにして設定する手順については、『Cisco IOS IP Configuration Guide, Release 12.4』の「Configuring DHCP」の章にある「DHCP Configuration Task List」の項を参照してください。

## DHCP スヌーピング情報のモニタリング

表 39: DHCP 情報を表示するためのコマンド

<b>show ip dhcp snooping</b>	スイッチの DHCP スヌーピングの設定を表示します。
<b>show ip dhcp snooping binding</b>	DHCP スヌーピング バインディング データベース内の動的に設定されたバインディングだけを表示します。このようなバインディングは、バインディングとも呼ばれます。
<b>show ip dhcp snooping database</b>	DHCP スヌーピング バインディング データベースのステータスおよびパスを表示します。
<b>show ip dhcp snooping statistics</b>	DHCP スヌーピングの統計情報を要約または詳細形式で表示します。
<b>show ip source binding</b>	動的および静的に設定されたバインディングを表示します。





- (注) DHCP スヌーピングがイネーブルでインターフェイスがダウンステートに変更された場合、静的に設定されたバインディングは削除されません。

## DHCP サーバー ポートベースのアドレス割り当ての設定

### DHCP サーバー ポートベースのアドレス割り当ての

DHCP サーバー ポートベースのアドレス割り当ては、接続されたデバイス クライアントの ID またはクライアント ハードウェア アドレスに関係なく、DHCP がイーサネット スイッチ ポートで同じ IP アドレスを維持できるようにする機能です。

ネットワークに導入されたイーサネットスイッチは、直接接続されたデバイスに接続を提供します。工場の作業場など、一部の環境では、あるデバイスで不具合が発生した場合は、それと同時に、そのネットワークで代替りのデバイスが動作を開始しなければなりません。現在の DHCP 実装では、この代替りのデバイスに、DHCP が同じ IP アドレスを提供する保証はありません。コントロールやモニタリングなどを行うソフトウェアは、各デバイスに関連付けられた IP アドレスが一定であることを期待しています。デバイスを交換した場合、DHCP クライアントが変更された場合でも、アドレスの割り当ては一定のままではなりません。

DHCP サーバポートベースのアドレス割り当て機能が設定されている場合、この機能により、ある接続ポートで受信された DHCP メッセージでクライアント ID やクライアント ハードウェア アドレスが変更されたとしても、同じ接続ポートには常に同じ IP アドレスが提供されることが保証されます。DHCP プロトコルは、DHCP パケットのクライアント ID オプションにより、DHCP クライアントを識別します。クライアント ID オプションを含まないクライアントは、クライアント ハードウェア アドレスにより識別されます。この機能を設定すると、インターフェイスのポート名が、クライアント ID またはハードウェア アドレスよりも優先され、実際の接続ポイントであるスイッチ ポートがクライアント ID になります。

すべてのケースで、同じポートにイーサネットケーブルを接続することにより、接続されたデバイスに、DHCP 経由で同じ IP アドレスが割り当てられます。

DHCP サーバポートベースのアドレス割り当て機能がサポートされているのは、Cisco IOS DHCP サーバだけです。サードパーティ製のサーバではサポートされていません。

### ポートベースのアドレス テーブルのデフォルト設定

デフォルトでは、DHCP サーバポートベースのアドレス割り当てはディセーブルにされています。

## ポートベースのアドレス割り当て設定時の注意事項

- デフォルトでは、DHCP サーバポートベースのアドレス割り当てはディセーブルにされています。
- DHCP プールから事前に設定された予約への割り当てを制限する（予約されていないアドレスはクライアントに提供されず、その他のクライアントはプールによるサービスを受けない）ために、**reserved-only** DHCP プール コンフィギュレーション コマンドを入力することができます。

## DHCP スヌーピング バインディング データベース エージェントのイネーブル化

スイッチ上で DHCP スヌーピング バインディング データベース エージェントをイネーブルにし、設定するには、特権 EXEC モードで次の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **ip dhcp snooping database {flash[number]:/filename | ftp://user:password@host/filename | http://[[username:password]@]{hostname | host-ip}[/directory] /image-name.tar | rcp://user@host/filename} | tftp://host/filename**
4. **ip dhcp snooping database timeout seconds**
5. **ip dhcp snooping database write-delay seconds**
6. **end**
7. **ip dhcp snooping binding mac-address vlan vlan-id ip-address interface interface-id expiry seconds**
8. **show ip dhcp snooping database [detail]**
9. **show running-config**
10. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  デバイス> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<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
	デバイス# <code>configure terminal</code>	
ステップ 3	<p><b>ip dhcp snooping database {flash[number]:/filename   ftp://user:password@host/filename   http://[[username:password]@]{hostname / host-ip}[/directory] /image-name.tar   rcpx://user@host/filename}   tftp://host/filename</b></p> <p>例 :</p> <pre>デバイス (config)# ip dhcp snooping database tftp://10.90.90.90/snooping-rp2</pre>	<p>次のいずれかの形式を使用して、データベースエージェントまたはバインディングファイルの URL を指定します。</p> <ul style="list-style-type: none"> <li>• <b>flash[number]:/filename</b> (任意) アクティブスイッチのスタックメンバー番号を指定するには、<i>number</i> パラメータを使用します。<i>number</i> の指定できる範囲は 1 ~ 9 です。</li> <li>• <b>ftp://user:password@host/filename</b></li> <li>• <b>http://[[username:password]@]{hostname / host-ip}[/directory] /image-name.tar</b></li> <li>• <b>rcpx://user@host/filename</b></li> <li>• <b>tftp://host/filename</b></li> </ul>
ステップ 4	<p><b>ip dhcp snooping database timeout seconds</b></p> <p>例 :</p> <pre>デバイス (config)# ip dhcp snooping database timeout 300</pre>	<p>データベース転送プロセスが完了するのを待ち、それまでに完了しない場合はプロセスを停止する時間 (秒数) を指定します。</p> <p>デフォルトは 300 秒です。指定できる範囲は 0 ~ 86400 です。無期限の期間を定義するには、0 を使用します。これは転送を無期限に試行することを意味します。</p>
ステップ 5	<p><b>ip dhcp snooping database write-delay seconds</b></p> <p>例 :</p> <pre>デバイス (config)# ip dhcp snooping database write-delay 15</pre>	<p>バインディング データベースが変更されてから転送を開始するまでの遅延時間を指定します。指定できる範囲は 15 ~ 86400 秒です。デフォルトは 300 秒 (5 分) です。</p>
ステップ 6	<p><b>end</b></p> <p>例 :</p> <pre>デバイス (config)# end</pre>	<p>特権 EXEC モードに戻ります。</p>
ステップ 7	<p><b>ip dhcp snooping binding mac-address vlan vlan-id ip-address interface interface-id expiry seconds</b></p> <p>例 :</p>	<p>(任意) DHCP スヌーピング バインディング データベースにバインディングエントリを追加します。<i>vlan-id</i> に指定できる範囲は 1 ~ 4904 です。<i>seconds</i> の範囲は 1 ~ 4294967295 です。</p>

	コマンドまたはアクション	目的
	<pre>デバイス# ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5 interface gi1/1 expiry 1000</pre>	<p>このコマンドは、追加するエントリごとに入力します。</p> <p>このコマンドは、スイッチをテストまたはデバッグするときに使用します。</p>
ステップ 8	<p><b>show ip dhcp snooping database [detail]</b></p> <p>例 :</p> <pre>デバイス# show ip dhcp snooping database detail</pre>	DHCP スヌーピング バインディング データベース エージェントのステータスおよび統計情報を表示します。
ステップ 9	<p><b>show running-config</b></p> <p>例 :</p> <pre>デバイス# show running-config</pre>	入力を確認します。
ステップ 10	<p><b>copy running-config startup-config</b></p> <p>例 :</p> <pre>デバイス# copy running-config startup-config</pre>	(任意) コンフィギュレーション ファイルに設定を保存します。

## DHCP サーバ ポートベースのアドレス割り当てのイネーブル化

ポートベースのアドレス割り当てをグローバルにイネーブル化し、インターフェイス上で加入者 ID を自動的に生成するには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **ip dhcp use subscriber-id client-id**
4. **ip dhcp subscriber-id interface-name**
5. **interface *interface-id***
6. **ip dhcp server use subscriber-id client-id**
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  デバイス> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  デバイス# <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 3	<b>ip dhcp use subscriber-id client-id</b> 例：  デバイス(config)# <b>ip dhcp use subscriber-id client-id</b>	すべての着信 DHCP メッセージで、加入者 ID がクライアント ID としてグローバルに使用されるように DHCP サーバを設定します。
ステップ 4	<b>ip dhcp subscriber-id interface-name</b> 例：  デバイス(config)# <b>ip dhcp subscriber-id interface-name</b>	インターフェイスの短い名前に基づいて、加入者 ID を自動的に生成します。  特定のインターフェイスで設定された加入者 ID は、このコマンドで優先されます。
ステップ 5	<b>interface interface-id</b> 例：  デバイス(config)# <b>interface gigabitethernet1/0/1</b>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	<b>ip dhcp server use subscriber-id client-id</b> 例：  デバイス(config-if)# <b>ip dhcp server use subscriber-id client-id</b>	インターフェイス上ですべての着信 DHCP メッセージで、加入者 ID がクライアント ID として使用されるように DHCP サーバを設定します。
ステップ 7	<b>end</b> 例：  デバイス(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 8	<b>show running-config</b> 例：	入力を確認します。

	コマンドまたはアクション	目的
	デバイス# <code>show running-config</code>	
ステップ 9	<b>copy running-config startup-config</b> 例 : デバイス# <code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

### 次のタスク

スイッチ上での DHCP ポートベースのアドレス割り当てをイネーブルにした後で、**ip dhcp pool** グローバル コンフィギュレーション コマンドを使用して、IP アドレスの事前割り当てと、クライアントへの関連付けを行います。

## DHCP サーバポートベースのアドレス割り当てのモニタリング

表 40: DHCP ポートベースのアドレス割り当て情報を表示するためのコマンド

コマンド	目的
<code>show interface interface id</code>	特定のインターフェイスのステータスおよび設定を表示します。
<code>show ip dhcp pool</code>	DHCP アドレス プールを表示します。
<code>show ip dhcp binding</code>	Cisco IOS DHCP サーバのアドレス バインディングを表示します。

## DHCP の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、[www.cisco.com/go/cfn](http://www.cisco.com/go/cfn) に移動します。Cisco.com のアカウントは必要ありません。

表 41: DHCP の機能情報

機能名	リリース	機能情報
DHCP	Cisco IOS XE Everest 16.5.1a	DHCP はインターネット ホストに設定パラメータを提供します。DHCPは2つのコンポーネントで構成されます。1つはホスト固有の設定パラメータを DHCP サーバーからホストに配信するためのプロトコルで、もう1つはホストにネットワークアドレスを割り当てるためのメカニズムです。DHCP はクライアント/サーバーモデルに基づいています。指定された DHCP サーバーホストが、ダイナミックに設定されるホストに対して、ネットワークアドレスを割り当て、設定パラメータを提供します。
DHCP クライアントオプション 12	Cisco IOS XE Fuji 16.8.1a	DHCP クライアントオプション 12 機能により、クライアントのホスト名が指定されます。Dynamic Host Configuration Protocol (DHCP) サーバーからインターフェイスの IP アドレスを取得する際に、クライアントデバイスが応答内の DHCP Hostname オプションを受信すると、このオプションのホスト名が設定されます。DHCP は、IP ネットワークにおける動作のための設定情報を取得するために DHCP クライアントによって使用されます。







## 第 19 章

# DHCPv6 オプションのサポート

このモジュールでは、CAPWAP アクセスコントローラ DHCPv6 オプション (DHCPv6 オプション 52)、DHCPv6 クライアントのリンク層のアドレスオプション、および DNS 検索リストの機能について説明します。

CAPWAP は標準の相互運用プロトコルであり、コントローラによるワイヤレスアクセスポイントの集合の管理を可能にします。

RFC 6939 は、ファーストホップ DHCPv6 リレーエージェント (クライアントと同じリンクに接続されているリレーエージェント) が、サーバーに送信されている DHCPv6 メッセージでクライアントのリンク層アドレスを提供できるようにするメカニズムを定義しています。DHCP リレーが設定されている場合、この機能はデフォルトで有効になっています。

DNS 検索リスト (DNSSL) は、ドメインネームシステム (DNS) サフィックスドメイン名のリストであり、IPv6 ホストで短い、修飾子を持たないドメイン名に対する DNS クエリ検索を実行する際に使用されます。

- [DHCPv6 オプションのサポートに関する情報 \(419 ページ\)](#)
- [DHCPv6 オプションサポートの設定方法 \(421 ページ\)](#)
- [DHCPv6 オプションサポートの設定例 \(424 ページ\)](#)
- [DHCPv6 オプションサポートの確認 \(424 ページ\)](#)
- [DHCPv6 オプションサポートの機能情報 \(426 ページ\)](#)

## DHCPv6 オプションのサポートに関する情報

### CAPWAP アクセスコントローラ DHCPv6 オプション

Control And Provisioning of Wireless Access Points (CAPWAP) プロトコルでは、中央管理型アクセスポイントが接続可能なワイヤレスコントローラを DHCP を使用して検出できます。CAPWAP は標準の相互運用プロトコルであり、コントローラによるワイヤレスアクセスポイントの集合の管理を可能にします。

ワイヤレスアクセスポイントは、プライマリ、セカンダリ、およびターシャリ ワイヤレス コントローラの IPv6 管理インターフェイスアドレスを提供する DHCPv6 オプション 52 (RFC 5417) を使用します。

ステートレスとステートフル両方の DHCPv6 アドレッシングモードがサポートされています。ステートレスモードでは、アクセスポイントがステートレスアドレス自動設定 (SLAAC) を使用して IPv6 アドレスを取得する一方で、(ルータアドバタイズメントから取得されない) その他のネットワーク情報は DHCPv6 サーバーから取得されます。ステートフルモードでは、アクセスポイントが IPv6 アドレスと他のネットワーク情報の両方を DHCPv6 サーバーのみから取得します。どちらのモードでも、DHCPv6 を使用してワイヤレスコントローラを検出する必要がある場合、オプション 52 を可能にするには DHCPv6 サーバーが必要です。

MAX\_PACKET\_SIZE が 15 を超えており、オプション 52 が設定されている場合、DHCPv6 サーバーは DHCP パケットを送信しません。

## DNS 検索リストのオプション

DNS 検索リスト (DNSSL) は、ドメインネームシステム (DNS) サフィックスドメイン名のリストであり、IPv6 ホストで短い、修飾子を持たないドメイン名に対する DNS クエリ検索を実行する際に使用されます。DNSSL オプションには、1 つ以上のドメイン名が含まれます。すべてのドメイン名が同じライフタイム値を共有します。ライフタイム値とは、DNSSL を使用できる最大時間を秒単位で示したものです。異なるライフタイム値が必要な場合は、複数の DNSSL オプションを使用できます。最大 5 つの DNSSL を設定できます。

長い DNSSL 名を持つ DHCP メッセージはデバイスによって破棄されます。



(注) 複数のルータアドバタイズメント (RA) や DHCP から DNS 情報を入手できる場合、ホストはこの DNS 情報の順序付きリストを保持する必要があります。

RFC 6106 は、拡張 DNS 設定のため、IPv6 ルータが IPv6 ホストに DNS 検索リスト (DNSSL) をアドバタイズできるようにする IPv6 ルータアドバタイズメント (RA) オプションを指定しています。

DNS ライフタイムの範囲は、次の例に示すように、最大 RA 間隔の値と最大 RA 間隔を 2 倍にした値の間に設定する必要があります。

```
(max ra interval) <= dns lifetime <= (2*(max ra interval))
```

最大 RA 間隔の値は 4 ~ 1800 秒の間で指定できます (デフォルトは 240 秒)。次の例は、範囲外のライフタイムを示しています。

```
Device(config-if)# ipv6 nd ra dns search list sss.com 3600
! Lifetime configured out of range for the interface that has the default maximum RA interval.!
```

## DHCPv6 クライアントのリンク層アドレスオプション

Cisco IOS XE Fuji 16.8.1a は、DHCPv6 クライアントのリンク層アドレスオプション (RFC 6939) をサポートします。これは、ファーストホップ DHCPv6 リレーエージェント (クライアントと同じリンクに接続されているリレーエージェント) が、サーバーに送信される DHCPv6 メッセージでクライアントのリンク層アドレスを提供できるようにする、オプションのメカニズムと関連する DHCPv6 オプションを定義します。

クライアントのリンク層アドレスオプションは、リレーエージェントとサーバー間でのみ交換されます。DHCPv6 クライアントは、クライアントのリンク層アドレスオプションの使用を認識しません。DHCPv6 クライアントは、クライアントのリンク層アドレスオプションを送信してはならず、クライアントのリンク層アドレスオプションを無視する必要があります。

各 DHCPv6 クライアントとサーバーは、DHCP 固有識別子 (DUID) によって識別されます。DUID は、クライアント識別子およびサーバー識別子オプションで伝送されます。DUID はすべての DHCP クライアントとサーバーで一意であり、特定のクライアントまたはサーバーに固定されます。DHCPv6 では、クライアントとサーバーの両方の識別子にリンク層アドレスに基づく DUID を使用します。デバイスは、最も小さい番号のインターフェイスの MAC アドレスを使用して DUID を形成します。ネットワークインターフェイスは、デバイスに永続的に接続されていると見なされます。

## DHCPv6 リレー エージェント

クライアントのリンク上に常駐する DHCPv6 リレーエージェントは、クライアントとサーバー間のメッセージの中継に使用されます。DHCPv6 リレーエージェントの動作は、クライアントに対して透過的です。DHCPv6 クライアントは、リンクスコープを持つ予約済みのマルチキャストアドレスを使用して DHCPv6 サーバーを探します。DHCPv6 クライアントと DHCPv6 サーバの間で直接通信するには、両方を同じリンクに接続する必要があります。ただし、管理の容易さ、経済性、または拡張性が懸念される状況では、DHCPv6 クライアントが同じリンクに接続されていない DHCPv6 サーバーにメッセージを送信できるようにすることが望ましい場合があります。IPv6 アドレスが設定されている場合でも、IPv6 DHCP リレーには IPv6 を有効にする必要があります。

## DHCPv6 オプションサポートの設定方法

### CAPWAP アクセスポイントの設定

#### 手順の概要

1. `enable`
2. `configure terminal`
3. `ipv6 dhcp pool poolname`
4. `capwap-ac address ipv6-address`
5. `end`

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> enable	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<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 3	<b>ipv6 dhcp pool poolname</b> 例： Device(config)# ipv6 dhcp pool pool1	DHCPv6 サーバー設定情報プールを設定し、DHCPv6 プール コンフィギュレーション モードを開始します。
ステップ 4	<b>capwap-ac address ipv6-address</b> 例： Device(config-dhcpv6)# capwap-ac address 2001:DB8::1	CAPWAP アクセス コントローラ アドレスを設定します。
ステップ 5	<b>end</b> 例： Device(config-dhcpv6)# end	DHCPv6 プール 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。

## IPv6 ルータ アドバタイズメント オプションを使用した DNS 検索リストの設定



(注) ドメイン名の設定は、RFC 1035 に従って行う必要があります。そうでない場合、設定が拒否されます。たとえば、次のドメイン名の設定はエラーになります。

```
Device(config-if)# ipv6 nd ra dns search list .example.example.com infinite-lifetime
```

インターフェイスで単一の DNS 検索リストを削除するには、**no ipv6 nd ra dns search list name** コマンドを使用します。インターフェイスで単一の DNS 検索リストを削除するには、**no ipv6 nd ra dns search list** コマンドを使用します。

## 手順の概要

1. **enable**
2. **configure terminal**
3. **interface interface-type interface-number**
4. **ipv6 nd prefix ipv6-prefix/prefix-length**

5. `ipv6 nd ra lifetime seconds`
6. `ipv6 nd ra dns search list list-name [infinite-lifetime]`
7. `end`

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	<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 3	<b>interface interface-type interface-number</b> 例： Device(config)# interface GigabitEthernet 0/2/0	インターフェイスを設定し、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>ipv6 nd prefix ipv6-prefix/prefix-length</b> 例： Device(config-if)# ipv6 nd prefix 2001:DB8::1/64 1111 222	IPv6 ネイバー探索 (ND) ルータアドバタイズメントに含める IPv6 プレフィックスを設定します。
ステップ 5	<b>ipv6 nd ra lifetime seconds</b> 例： Device(config-if)# ipv6 nd ra lifetime 9000	インターフェイス上の IPv6 ルータアドバタイズメントに含まれるデバイスのライフタイム値を設定します。
ステップ 6	<b>ipv6 nd ra dns search list list-name [infinite-lifetime]</b> 例： Device(config-if)# ipv6 nd ra dns search list example.example.com infinite-lifetime	DNS 検索リストを設定します。検索リストのライフタイムを指定できます。
ステップ 7	<b>end</b> 例： Device(config-if)# end	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、特権 EXEC モードに戻ります。

## 次のタスク

IPv6 RA オプションに基づいて DNS 検索リストの設定を確認するには、**show ipv6 nd idb interface** コマンドを使用します。

```
Device# show ipv6 nd idb interface gigabitEthernet 0/2/0/0 detail location 0/2/CPU0
Mon Jul 4 14:28:53.422 IST
ifname: Gi0/2/0/0, ifh: 0x01000300, iftype: 15, VI-type: 0, Pseudo IDB: FALSE
```

```

vrf-id: 0x60000000, table-id: 0xe0800000
Mac Addr: 02d1.1e2b.0baf, size: 6, Vlan tag set: FALSE

Media Name: ether, Media Encap: 0x1 (ARPA)
Mac Length: 6, Media Header Len: 14, Media Proto: 0xdd86
Current Encap: 0x1 (ARPA), Mcast Encap : 0x1 (ARPA)

IPv6 Interface: Enabled, IPv6: Enabled, MPLS: Disabled
Link local address: 2001::d1:1eff:fe2b:baf, Global Addr count: 1
Global Addresses:1::1(0x2),
Default Prefix Address: ::, Prefix Addr Count: 3,
Prefix addresses: 1::(0x401), 2001:db8:e8:1011::(0x4), 2001:db8:e8:1011::(0x4)

RA Specific Route Count: 1,
RA Specific Route : Address 3:: Prefix Length 116 Lifetime 1112 Preference Low

RA DNS Search List Count: 3,
RA DNS Search List : Name example.example.com Lifetime 240
RA DNS Search List : Name example1.example1.com Lifetime 240
RA DNS Search List : Name example2.example2.com Lifetime 4294967295

```

## DHCPv6 オプションサポートの設定例

### 例：CAPWAP アクセスポイントの設定

次に、CAPWAP アクセスポイントの設定方法の例を示します。

```

Device> enable
Device# configure terminal
Device(config)# ipv6 dhcp pool pool1
Device(config-dhcpv6)# capwap-ac address 2001:DB8::1
Device(config-dhcpv6)# end
Device#

```

## DHCPv6 オプションサポートの確認

### オプション 52 サポートの確認

次に、**show ipv6 dhcp pool** コマンドの出力例として DHCPv6 設定プールの情報を表示します。

```

Device# show ipv6 dhcp pool

DHCPv6 pool: svr-p1
Static bindings:
Binding for client 000300010002FCA5C01C
  IA PD: IA ID 00040002,
    Prefix: 2001:db8::3/72
    preferred lifetime 604800, valid lifetime 2592000
  IA PD: IA ID not specified; being used by 00040001
    Prefix: 2001:db8::1/72
    preferred lifetime 240, valid lifetime 54321

```

```

Prefix: 2001:db8::2/72
      preferred lifetime 300, valid lifetime 54333
Prefix: 2001:db8::3/72
      preferred lifetime 280, valid lifetime 51111
Prefix from pool: local-p1, Valid lifetime 12345, Preferred lifetime 180
DNS server: 1001::1
DNS server: 1001::2
CAPWAP-AC Controller address: 2001:DB8::1
Domain name: example1.com
Domain name: example2.com
Domain name: example3.com
Active clients: 2

```

次に、DHCPv6 のデバッグを有効にする例を示します。

```

Device# debug ipv6 dhcp detail

IPv6 DHCP debugging is on (detailed)

```

### DNS 検索リストのトラブルシューティング

再帰 DNS サーバーと DNS 検索リストは、RA メッセージの一部として送信されます。IPv6 ND トレースを実行して、DNS サーバーおよび DNS 検索リストに関連する特定の問題をデバッグします。

```

Device# show ipv6 nd trace location 0/2/CPU0

Jun 30 20:07:03.508 nd/fevent 0/2/CPU0 t26702 Sending RA to ff02::1 on
GigabitEthernet0/2/0/0 (0x1000300)
Jun 30 20:07:03.508 nd/fevent 0/2/CPU0 t26702 hoplimit 64 lifetime 9000 reachable 0
retrans 0
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 1::/64 Onlink Auto
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 valid 2592000 pref 604800
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 2002:4898:e8:1011::/64 Onlink Auto
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 valid 1111 pref 222
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 2002:4899:e8:1011::/64 Onlink Auto
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 valid 1111 pref 222
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 ra specific route address 3:: lifetime
1112 preference Low
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 ra dns server address 5::6 lifetime 240
first
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 ra dns server address 5::5 lifetime 240
part of same ra dns server option
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 ra dns server address 4::4 lifetime
4294967295 first
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 ra dns search list name example.example.com
lifetime 240 first
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 ra dns search list name example1.example1.com
lifetime 240 part of
same ra dns search list option
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 ra dns search list name example2.example2.com
lifetime 4294967295 first
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 nd_send_ra: sending RA paksz=320, plen=280
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 nd_pak_send: size=320, ifh
GigabitEthernet0/2/0/0 (0x1000300) ,
priority=2 to ipv6-io
Jun 30 20:07:03.509 nd/fevent 0/2/CPU0 t26702 nd_pak_send: sending pak=0x60c07d8b with
NO FVS set, size=320,
ifh GigabitEthernet0/2/0/0 (0x1000300) to ipv6-io

```

## DHCPv6 オプションサポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレーンで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、[www.cisco.com/go/cfn](http://www.cisco.com/go/cfn) に移動します。Cisco.com のアカウントは必要ありません。

表 42: DHCPv6 オプションサポートの機能情報

機能名	リリース	機能情報
CAPWAP アクセスコントローラ DHCPv6 オプション 52	Cisco IOS XE Fuji 16.8.1a	CAPWAP プロトコルでは、中央管理型アクセスポイントの接続先ワイヤレスコントローラを DHCPv6 を使用して検出できます。CAPWAP は標準の相互運用プロトコルであり、コントローラによるワイヤレスアクセスポイントの集合の管理を可能にします。
DHCPv6 クライアントのリンク層アドレスオプション	Cisco IOS XE Fuji 16.8.1a	DHCPv6 クライアントのリンク層アドレスオプション (RFC 6939) は、ファーストホップ DHCPv6 リレーエージェント (クライアントと同じリンクに接続されたリレーエージェント) がサーバーに送信されている DHCPv6 メッセージでクライアントのリンク層アドレスを提供できるようにするための、オプションのメカニズムと関連 DHCPv6 オプションを定義します。
DNS 検索リスト	Cisco IOS XE Fuji 16.8.1a	DNS 検索リスト (DNSSL) は、ドメインネームシステム (DNS) サフィックスドメイン名のリストであり、IPv6 ホストで短い、修飾子を持たないドメイン名に対する DNS クエリ検索を実行する際に使用されます。DNSSL オプションには、1つ以上のドメイン名が含まれます。





## 第 20 章

# IP ソース ガードの設定

- [IP ソース ガードの概要 \(427 ページ\)](#)
- [IP ソース ガードの設定方法 \(430 ページ\)](#)
- [IP ソース ガードのモニタリング \(433 ページ\)](#)
- [IP ソース ガードの機能の履歴 \(434 ページ\)](#)

## IP ソース ガードの概要

### IP ソース ガード

ネイバーの IP アドレスを使用する場合に、トラフィック攻撃を防ぐために IP ソース ガードを使用でき、そして信頼できないインターフェイスで DHCP スヌーピングがイネーブルの場合に、IP アドレスを使用しようとすると、IP ソース ガードをイネーブルにできます。

インターフェイス上で IPSG をイネーブルにすると、スイッチは、DHCP スヌーピングにより許可された DHCP パケットを除き、このインターフェイスで受信したすべての IP トラフィックをブロックします。

スイッチは IP アドレスをポートにバインドするためにハードウェアの発信元 IP 検索テーブルを使用します。IP および MAC のフィルタリングでは、送信元 IP 検索および送信元 MAC 検索の組み合わせが使用されます。バインディングテーブル内の送信元 IP アドレスを使用する IP トラフィックは許可され、他のすべてのトラフィックは拒否されます。

IP ソース バインディング テーブルには、DHCP スヌーピングで学習されたバインディング、または手動で設定されたバインディング (スタティック IP 送信元バインディング) があります。このテーブルのエントリには IP アドレスと、関連 MAC アドレス、および関連 VLAN 番号があります。スイッチは、IP ソース ガードがイネーブルにされている場合だけ、IP ソース バインディング テーブルを使用します。

IPSG は、アクセス ポートおよびトランク ポートを含むレイヤ 2 ポートだけでサポートされます。送信元 IP アドレスと送信元 IP および MAC アドレス フィルタリングで IPSG を設定できます。

## スタティック ホスト用 IP ソース ガード



- (注) アップリンク ポート、またはトランク ポートで、スタティック ホスト用 IP ソース ガード (IPSG) を使用しないでください。

スタティック ホスト用 IPSG は、IPSG の機能を DHCP ではない、スタティックな環境に拡張するものです。これまでの IPSG は、DHCP スヌーピングにより作成されたエントリを使用して、スイッチに接続されたホストを検証していました。ホストから受信したトラフィックのうち、有効な DHCP を持たないものはすべてドロップされます。このセキュリティ機能によって、ルーティングされないレイヤ 2 インターフェイス上の IP トラフィックが制限されます。この機能は、DHCP スヌーピング バインディング データベース、および手動で設定された IP ソース バインディングに基づいてトラフィックをフィルタリングします。前バージョンの IPSG では、IPSG を動作させるために DHCP 環境が必要でした。

スタティック ホスト用 IPSG では、DHCP なしで IPSG を動作させることができます。スタティック ホスト用 IPSG は、ポート ACL をインストールするために IP デバイス トラッキング テーブル エントリに依存しています。このスイッチは、指定されたポートで有効なホストのリストを維持するために、ARP リクエスト、またはその他の IP パケットに基づいてスタティック エントリを作成します。また、指定されたポートにトラフィックを送信できるホストの数を指定することもできます。これはレイヤ 3 でのポートセキュリティと同じです。

スタティック ホスト用 IPSG はダイナミック ホストもサポートしています。ダイナミック ホストが、IP DHCP スヌーピング テーブルに存在する DHCP が割り当てられた IP アドレスを受信すると、IP デバイス トラッキング テーブルは同じエントリを学習します。スタック化環境では、アクティブスイッチのフェールオーバーが発生すると、メンバポートに接続されたスタティックホストの IP ソースガードエントリは、そのまま残ります。 **show device-tracking database** 特権 EXEC コマンドを入力すると、IP デバイス トラッキング テーブルには、これらのエントリが ACTIVE であると表示されます。



- (注) 複数のネットワーク インターフェイスを持つ IP ホストの一部は、ネットワーク インターフェイスに無効なパケットを注入することができます。この無効なパケットには、ソースアドレスとして、別のホスト ネットワーク インターフェイスの IP アドレス、または MAC アドレスが含まれます。この無効パケットは、スタティック ホスト用 IPSG がホストに接続され、無効な IP アドレス バインディングまたは MAC アドレス バインディングが学習されて、有効なバインディングが拒否される原因となります。ホストによる無効なパケットの注入を回避する方法については、対応するオペレーティングシステムとネットワーク インターフェイスのベンダーにお問い合わせください。

最初、スタティック ホスト用 IPSG は ACL ベースのスヌーピング メカニズムを通じて、動的に IP バインディング、または MAC バインディングを学習します。IP バインディング、または MAC バインディングは、ARP パケット、および IP パケットにより、スタティック ホストから学習されます。これらはデバイス トラッキング データベースに保存されます。指定されたポートで動的に学習、または静的に設定された IP アドレスの数が最大値に達した場合、新

しい IP アドレスを持つパケットはすべて、ハードウェアによりドロップされます。何らかの理由で移動された、またはなくなったホストを解決するために、スタティック ホスト用 IPSPG は IP デバイス トラッキングを活用して、動的に学習した IP アドレス バインディングをエーピングアウトします。この機能は、DHCP スヌーピングとともに使用できます。複数バインディングは、DHCP ホストとスタティック ホストの両方に接続されたポートに確立されます。たとえば、バインディングは、デバイス トラッキング データベースと DHCP スヌーピング バインディング データベースの両方に保存されます。

## IP ソース ガードの設定時の注意事項

- スタティック IP バインディングは、非ルーテッド ポートだけで設定できます。ルーテッド インターフェイスで **ip source binding mac-address vlan vlan-id ip-address interface interface-id** グローバル コンフィギュレーション コマンドを入力すると、次のエラーメッセージが表示されます。

```
Static IP source binding can only be configured on switch port.
```

- 送信元 IP フィルタリング機能を持つ IP ソース ガードがインターフェイスでイネーブルにされている場合、このインターフェイスのアクセス VLAN で、DHCP スヌーピングをイネーブルにしておく必要があります。
- 複数の VLAN を持つトランク インターフェイス上で IP ソース ガードをイネーブルにし、これらすべての VLAN で DHCP スヌーピングをイネーブルにした場合、すべての VLAN に、送信元 IP アドレス フィルタが適用されます。



(注) IP ソース ガードがイネーブルにされているときに、トランク インターフェイスの VLAN 上で DHCP スヌーピングをイネーブル、またはディセーブルにした場合、スイッチは適切にトラフィックをフィルタリングできない可能性があります。

- この機能は、802.1x ポートベースの認証がイネーブルにされている場合にイネーブルにできます。
- IP ソース ガード スマート ロギングを設定すると、指定されたアドレスや DHCP によって学習されたアドレス以外の送信元アドレスを持つパケットは拒否され、そのパケットの内容が NetFlow 収集装置に送信されます。この機能を設定する場合は、スマート ロギングがグローバルにイネーブルになっていることを確認してください。
- スイッチスタックでは、IP ソースガードがスタック メンバ インターフェイスに設定されていて、**no switch stack-member-number provision** グローバル コンフィギュレーション コマンドの入力によりそのスイッチの設定を削除した場合、インターフェイススタティック バインディングはバインディングテーブルから削除されますが、実行コンフィギュレーションからは削除されません。**switch stack-member-number provision** コマンドを入力する

ことによって、スイッチを再度プロビジョニングした場合、バインディングは復元されません。

実行コンフィギュレーションからバインディングを削除するには、**no switch provision** コマンドを入力する前に IP ソースガードを無効化する必要があります。インターフェイスがバインディングテーブルから削除される間にスイッチがリロードされると、設定も削除されます。

## IP ソース ガードの設定方法

### IP ソース ガードのイネーブル化

#### 手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **ip verify source** [**mac-check** ]
5. **exit**
6. **ip source binding** *mac-address* **vlan** *vlan-id* *ip-address* **interface** *interface-id*
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

#### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  デバイス> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  デバイス# <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 3	<b>interface</b> <i>interface-id</i> 例：  デバイス(config)# <b>interface</b> <b>gigabitethernet</b> 1/0/1	設定するインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	<b>ip verify source [mac-check]</b> 例： デバイス(config-if)# <b>ip verify source</b>	送信元 IP アドレス フィルタリングによる IP ソースガードを有効にします。  (任意) <b>mac-check</b> : 送信元 IP アドレスによる IP ソースガードおよびMACアドレスフィルタリングをイネーブルにします。
ステップ 5	<b>exit</b> 例： デバイス(config-if)# <b>exit</b>	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 6	<b>ip source binding mac-address vlan vlan-id ip-address interface interface-id</b> 例： デバイス(config)# <b>ip source binding 0100.0230.0002 vlan 11 10.0.0.4 interface gigabitethernet1/0/1</b>	スタティック IP ソース バインディングを追加します。  スタティック バインディングごとにこのコマンドを入力します。
ステップ 7	<b>end</b> 例： デバイス(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 8	<b>show running-config</b> 例： デバイス# <b>show running-config</b>	入力を確認します。
ステップ 9	<b>copy running-config startup-config</b> 例： デバイス# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## レイヤ2アクセスポートでのスタティックホスト用IPソースガードの設定

スタティックホスト用IPSGを動作させるには、**ip device tracking maximum limit-number** インターフェイス コンフィギュレーション コマンドをグローバルに設定する必要があります。こ

のコマンドをポートに対して実行したが、IP デバイス トラッキングをグローバルに有効にしている、または `IP device tracking maximum` をそのインターフェイスに対して設定していない場合は、スタティック ホストの IPSG によって、そのインターフェイスからの IP トラフィックはすべて拒否されます。

## 手順の概要

1. `enable`
2. `configure terminal`
3. `ip device tracking`
4. `interface interface-id`
5. `switchport mode access`
6. `switchport access vlan vlan-id`
7. `ip device tracking maximum number`
8. `end`

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  デバイス> <code>enable</code>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  デバイス# <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 3	<b>ip device tracking</b> 例：  デバイス(config)# <code>ip device tracking</code>	IP ホスト テーブルをオンにし、IP デバイス トラッキングをグローバルに有効にします。
ステップ 4	<b>interface interface-id</b> 例：  デバイス(config)# <code>interface gigabitethernet 1/0/1</code>	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 5	<b>switchport mode access</b> 例：	アクセスとしてポートを設定します。

	コマンドまたはアクション	目的
	デバイス (config-if) # <code>switchport mode access</code>	
ステップ 6	<code>switchport access vlan vlan-id</code> 例 : デバイス (config-if) # <code>switchport access vlan 10</code>	このポートに VLAN を設定します。
ステップ 7	<code>ip device tracking maximum number</code> 例 : デバイス (config-if) # <code>ip device tracking maximum 8</code>	そのポートで、IP デバイス トラッキング テーブルにより許可されるスタティック IP 数の上限を設定します。指定できる範囲は 1 ~ 10 です。最大値は 10 です。  (注) <code>ip device tracking maximum limit-number</code> インターフェイス コンフィギュレーション コマンドを設定する必要があります。
ステップ 8	<code>end</code> 例 : デバイス (config) # <code>end</code>	特権 EXEC モードに戻ります。

## IP ソース ガードのモニタリング

表 43: 特権 EXEC 表示コマンド

コマンド	目的
<code>show ip verify source [ interface interface-id ]</code>	スイッチ上または特定のインターフェイス上の IP ソース ガードの設定を表示します。
<code>show ip device tracking { all   interface interface-id   ip ip-address   mac mac-address }</code>	IP デバイス トラッキング テーブル内のエントリに関する情報を表示します。

表 44: インターフェイス コンフィギュレーション コマンド

コマンド	目的
<code>ip verify source tracking</code>	データ ソースを確認します。

出力フィールドの詳細については、このリリースに対応するコマンドリファレンスを参照してください。

## IP ソース ガードの機能の履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	IP ソース ガード	ネイバーの IP アドレスを使用する場合に、トラフィック攻撃を防ぐために IP ソース ガードを使用でき、そして信頼できないインターフェイスで DHCP スヌーピングがイネーブルの場合に、IP アドレスを使用しようとすると、IP ソース ガードをイネーブルにできます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。





## 第 21 章

# ダイナミック ARP インспекションの設定

- [ダイナミック ARP インспекションの制約事項 \(435 ページ\)](#)
- [ダイナミック ARP インспекションの概要 \(437 ページ\)](#)
- [ダイナミック ARP インспекションのデフォルト設定 \(441 ページ\)](#)
- [ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ \(442 ページ\)](#)
- [非 DHCP 環境での ARP ACL の設定 \(442 ページ\)](#)
- [DHCP 環境でのダイナミック ARP インспекションの設定 \(445 ページ\)](#)
- [着信 ARP パケットのレート制限 \(448 ページ\)](#)
- [ダイナミック ARP インспекション検証チェックの実行 \(451 ページ\)](#)
- [DAI のモニタリング \(453 ページ\)](#)
- [DAI の設定の確認 \(453 ページ\)](#)
- [ダイナミック ARP インспекションの機能方法 \(454 ページ\)](#)

## ダイナミック ARP インспекションの制約事項

ここでは、スイッチにダイナミック ARP インспекションを設定するときの制約事項および注意事項を示します。

- ダイナミック ARP インспекションは入力セキュリティ機能です。出力チェックはまったく行いません。
- ダイナミック ARP インспекションは、ダイナミック ARP インспекションをサポートしていないスイッチ、またはこの機能がイネーブルにされていないスイッチに接続されるホストに対しては有効ではありません。中間者攻撃は単一のレイヤ2ブロードキャストドメインに制限されているため、チェックされないドメインと、ダイナミック ARP インспекションによりチェックされるドメインは区別します。このアクションは、ダイナミック ARP インспекションのためにイネーブルにされているドメインでホストの ARP キャッシュを保護します。
- 着信 ARP 要求、および ARP 応答で IP/MAC アドレス バインディングを検証するために、ダイナミック ARP インспекション DHCP スヌーピング バインディング データベースの

エントリに依存します。IP アドレスがダイナミックに割り当てられた ARP パケットを許可する際は、DHCP スヌーピングをイネーブルにしてください。

DHCP スヌーピングをディセーブルにしている場合、または DHCP 以外の環境では、ARP ACL を使用してパケットの許可または拒否を行います。

- ダイナミック ARP インспекションは、アクセス ポート、トランク ポート、および EtherChannel ポートでサポートされます。



(注) RSPAN VLAN では、ダイナミック ARP インспекションをイネーブルにしないでください。RSPAN VLAN でダイナミック ARP インспекションをイネーブルにすると、ダイナミック ARP インспекション パケットが RSPAN 宛先ポートに届かない可能性があります。

- 物理ポートを EtherChannel ポート チャンネルに結合するには、この物理ポートとチャンネルポートの信頼状態が一致する必要があります。そうでない物理ポートは、ポートチャンネル内で中断状態のままとなります。ポート チャンネルは、チャンネルと結合された最初の物理ポートの信頼状態を継承します。したがって、最初の物理ポートの信頼状態は、チャンネルの信頼状態と一致する必要はありません。

逆に、ポートチャンネルで信頼状態を変更すると、スイッチは、チャンネルを構成するすべての物理ポートで新しい信頼状態を設定します。

- レート制限は、スイッチ スタックの各スイッチで別々に算出されます。クロススタック EtherChannel の場合、これは実際のレート制限が設定値よりも高い可能性があることを意味します。たとえば、レート制限が 30 pps に設定された EtherChannel で、スイッチ 1 に 1 つのポート、およびスイッチ 2 に 1 つのポートがある場合、EtherChannel が errdisable にならずに、各ポートは 29 pps でパケットを受信できます。
- ポートチャンネルの動作レートは、チャンネル内のすべての物理ポートによる累積値です。たとえば、ポートチャンネルの ARP レート制限を 400 pps に設定すると、このチャンネルに結合されたすべてのインターフェイスは、合計で 400 pps を受信します。EtherChannel ポートで受信される ARP パケットのレートは、すべてのチャンネル メンバーからの受信パケットレートの合計となります。EtherChannel ポートのレート制限は、各チャンネル ポート メンバーが受信する ARP パケットのレートを確認してから設定してください。

物理ポートで受信されるパケットのレートは、物理ポートの設定ではなく、ポートチャンネルの設定に照合して検査されます。ポートチャンネルのレート制限設定は、物理ポートの設定には依存しません。

EtherChannel が、設定したレートより多くの ARP パケットを受信すると、このチャンネル (すべての物理ポートを含む) は errdisable ステートとなります。

- 着信トランク ポートでは、ARP パケットを必ずレート制限してください。トランク ポートの集約を反映し、複数のダイナミック ARP インспекションがイネーブルにされた VLAN にわたってパケットを処理するために、トランク ポートのレートをより高く設定します。また、**ip arp inspection limit none** インターフェイス コンフィギュレーション コ

マンドを使用して、レートを無制限に設定することもできます。1つのVLANに高いレート制限値を設定すると、ソフトウェアによってこのポートが errdisable ステートにされた場合に、他のVLANへのDoS攻撃を招く可能性があります。

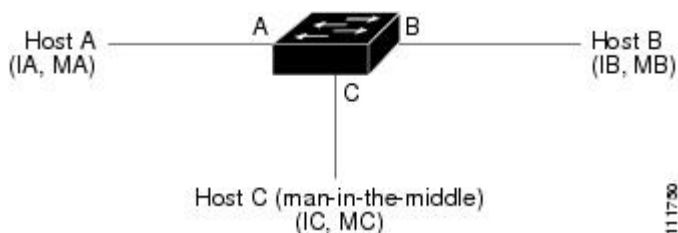
- スイッチで、ダイナミック ARP インспекションをイネーブルにすると、ARPトラフィックをポリシングするように設定されたポリサーの有効性は失われます。この結果、すべてのARPトラフィックはCPUに送信されます。

## ダイナミック ARP インспекションの概要

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はホストAに情報を送信する必要がありますが、ARPキャッシュにホストAのMACアドレスを持っていないとします。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。しかし、ARPは、ARP要求を受信されなかった場合でも、ホストからの余分な応答を許可するため、ARPスプーフィング攻撃やARPキャッシュのポイズニングが発生することがあります。攻撃が開始されると、攻撃を受けたデバイスからのすべてのトラフィックは、攻撃者のコンピュータを経由してルータ、スイッチ、またはホストに送信されるようになります。

悪意のあるユーザーは、サブネットに接続されているシステムのARPキャッシュをポイズニングし、このサブネット上の他のホストを目的とするトラフィックを代行受信することにより、レイヤ2ネットワークに接続されているホスト、スイッチ、およびルータを攻撃することができます。図26-1に、ARPキャッシュポイズニングの例を示します。

図 23: ARP キャッシュ ポイズニング



ホストA、B、およびCは、インターフェイスA、B、およびC上にあるスイッチに接続されています。これらはすべて同一のサブネット上にあります。カッコ内に示されているのは、これらのIPアドレス、およびMACアドレスです。たとえば、ホストAが使用するIPアドレスはIA、MACアドレスはMAです。ホストAがIPレイヤにあるホストBと通信する必要がある場合、ホストAはIPアドレスIBと関連付けられているMACアドレスにARP要求をブロードキャストします。スイッチとホストBは、このARP要求を受信すると、IPアドレスがIAで、MACアドレスがMAのホストに対するARPバインディングをARPキャッシュに読み込みます。たとえば、IPアドレスIAは、MACアドレスMAにバインドされています。ホストBが応答すると、スイッチ、およびホストAは、IPアドレスがIBで、MACアドレスがMBのホストに対するバインディングをARPに読み込みます。

ホスト C は、IP アドレスが IA (または IB) で、MAC アドレスが MC のホストに対するバインディングを持つ偽造 ARP 応答をブロードキャストすることにより、スイッチ、ホスト A、およびホスト B の ARP キャッシュをポイズニングすることができます。ARP キャッシュがポイズニングされたホストは、IA または IB 宛でのトラフィックに、宛先 MAC アドレスとして MAC アドレス MC を使用します。つまり、ホスト C がこのトラフィックを代行受信することになります。ホスト C は IA および IB に関連付けられた本物の MAC アドレスを知っているため、正しい MAC アドレスを宛先として使用することで、代行受信したトラフィックをこれらのホストに転送できます。ホスト C は自身をホスト A からホスト B へのトラフィック ストリームに挿入します。従来の中間者攻撃です。

ダイナミック ARP インспекションは、ネットワーク内の ARP パケットの正当性を確認するセキュリティ機能です。不正な IP/MAC アドレス バインディングを持つ ARP パケットを代行受信し、ログに記録して、廃棄します。この機能により、ネットワークをある種の中間者攻撃から保護することができます。

ダイナミック ARP インспекションにより、有効な ARP 要求と応答だけが確実にリレーされるようになります。スイッチが実行する機能は次のとおりです。

- 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。

ダイナミック ARP インспекションは、信頼できるデータベースである 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ている有効な IP/MAC アドレス バインディングに基づいて、ARP パケットの正当性を判断します。このデータベースは、VLAN およびスイッチ上で DHCP スヌーピングが有効になっている場合に、DHCP スヌーピングにより構築されます。信頼できるインターフェイスで ARP パケットが受信されると、スイッチは何もチェックせずに、このパケットを転送します。信頼できないインターフェイスでは、スイッチはこのパケットが有効である場合だけ、このパケットを転送します。

**ip arp inspection vlan *vlan-range*** グローバル コンフィギュレーション コマンドを使用して、VLAN ごとにダイナミック ARP インспекションを有効にすることができます。

非 DHCP 環境では、ダイナミック ARP インспекションは、静的に設定された IP アドレスを持つホストに対するユーザー設定の ARP アクセス コントロール リスト (ACL) と照らし合わせて、ARP パケットの正当性を確認することができます。ARP ACL を定義するには、**arp access-list *acl-name*** 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。

パケットの IP アドレスが無効である場合、または ARP パケットの本文にある MAC アドレスが、イーサネット ヘッダーで指定されたアドレスと一致しない場合、ARP パケットをドロップするようにダイナミック ARP インспекションを設定することができます。このためには、**ip arp inspection validate {[*src-mac*] [*dst-mac*] [*ip*]}** 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。

## インターフェイスの信頼状態とネットワーク セキュリティ

ダイナミック ARP インспекションは、スイッチの各インターフェイスに信頼状態を関連付けます。信頼できるインターフェイスに到着するパケットは、ダイナミック ARP インспекションの確認検査をすべてバイパスし、信頼できないインターフェイスに到着するパケットには、ダイナミック ARP インспекションの検証プロセスを受けます。

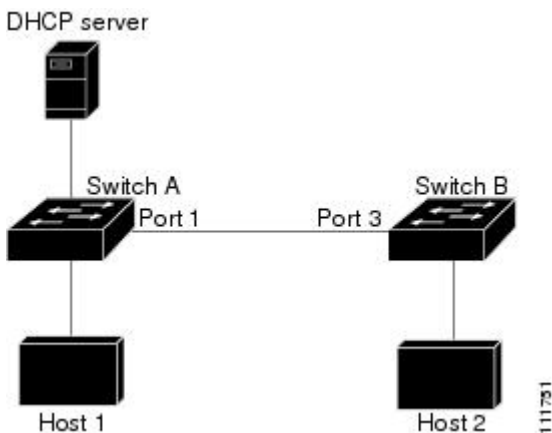
一般的なネットワーク構成では、ホストポートに接続されているスイッチポートすべてを信頼できないものに設定し、スイッチに接続されているスイッチポートすべてを信頼できるものに設定します。この構成では、指定されたスイッチからネットワークに入ってくる ARP パケットはすべて、セキュリティチェックをバイパスします。VLAN 内、またはネットワーク内のその他の場所では、他の検査を実行する必要はありません。信頼状態を設定するには、`ip arp inspection trust` インターフェイス コンフィギュレーション コマンドを使用します。



**注意** 信頼状態の設定は、慎重に行ってください。信頼すべきインターフェイスを信頼できないインターフェイスとして設定すると、接続が失われる場合があります。

次の図では、スイッチ A とスイッチ B の両方が、ホスト 1 とホスト 2 を含む VLAN でダイナミック ARP インспекションを実行しているとします。ホスト 1 とホスト 2 が、スイッチ A に接続している DHCP サーバーから IP アドレスを取得している場合、スイッチ A だけが、ホスト 1 の IP/MAC アドレスをバインディングします。したがって、スイッチ A とスイッチ B 間のインターフェイスが信頼できない場合は、ホスト 1 からの ARP パケットはスイッチ B ではドロップされ、ホスト 1 およびホスト 2 の間の接続は切断されます。

図 24: ダイナミック ARP インспекションのために有効にされた VLAN 上の ARP パケット検証



実際には信頼できないインターフェイスを信頼できるインターフェイスとして設定すると、ネットワーク内にセキュリティホールが生じます。スイッチ A でダイナミック ARP インспекションが実行されていない場合、ホスト 1 はスイッチ B の ARP キャッシュを簡単にポイズニングできます（および、これらのスイッチの間のリンクが信頼できるものとして設定されている場合はホスト 2）。この状況は、スイッチ B がダイナミック ARP インспекションを実行している場合でも発生します。

ダイナミック ARP インспекションは、ダイナミック ARP インспекションを実行しているスイッチに接続された（信頼できないインターフェイス上の）ホストが、そのネットワークにあるその他のホストの ARP キャッシュをポイズニングしていないことを保証します。しかし、ダイナミック ARP インспекションにより、ネットワークの他の部分にあるホストが、ダイナミック ARP インспекションを実行しているスイッチに接続されているホストのキャッシュをポイズニングできないようにすることはできません。

VLAN のスイッチの一部がダイナミック ARP インспекションを実行し、残りのスイッチは実行していない場合、このようなスイッチに接続しているインターフェイスは信頼できないものとして設定します。ただし、非ダイナミック ARP インспекションスイッチからパケットのバインディングを検証するには、ARP ACL を使用して、ダイナミック ARP インспекションを実行するスイッチを設定します。このようなバインディングが判断できない場合は、レイヤ 3 で、ダイナミック ARP インспекションスイッチを実行していないスイッチから、ダイナミック ARP インспекションを実行しているスイッチを分離します。



(注) DHCP サーバーとネットワークの設定によっては、VLAN 上のすべてのスイッチで指定された ARP パケットを検証できない可能性があります。

## ARP パケットのレート制限

スイッチの CPU は、ダイナミック ARP インспекション確認検査を実行します。したがって、DoS 攻撃を阻止するために、着信 ARP パケット数はレート制限されます。デフォルトでは、信頼できないインターフェイスのレートは 15 パケット/秒 (pps) です。信頼できるインターフェイスはレート制限されません。この設定を変更するには、**ip arp inspection limit** インターフェイス コンフィギュレーション コマンドを使用します。

着信 ARP パケットのレートが設定された制限を超えると、スイッチはポートを **errdisable** ステートにします。ユーザーが介入するまで、ポートはこの状態を維持します。**errdisable recovery** グローバルコンフィギュレーションコマンドを使用すると、**errdisable** ステートの回復をイネーブルにできます。これによって、ポートは指定のタイムアウト時間が経過すると、この状態から自動的に回復するようになります。



(注) EtherChannel のレート制限は、スタックにある各スイッチに個別に適用されます。たとえば、EtherChannel で 20 pps の制限が設定されている場合、EtherChannel にあるポートの各スイッチでは、最大 20 pps まで実行できます。スイッチが制限を超過した場合、EtherChannel 全体が **errdisable** ステートになります。

## ARPA CL および DHCP スヌーピング エントリの相対的なプライオリティ

ダイナミック ARP インспекションでは、有効な IP/MAC アドレス バインディングのリストとして、DHCP スヌーピング バインディング データベースが使用されます。

DHCP スヌーピング バインディング データベース内のエントリより、ARP ACL の方が優先されます。スイッチが ACL を使用するのには、ACL が `ip arp inspection filter vlan` グローバル コンフィギュレーション コマンドを使用して作成されている場合だけです。スイッチは、まず、ARP パケットをユーザー設定の ARP ACL と比較します。DHCP スヌーピングによりデータが入力されたデータベースに有効なバインディングが存在していても、ARP ACL が ARP パケットを拒否する場合、スイッチもこのパケットを拒否します。

## 廃棄パケットのロギング

スイッチがパケットをドロップすると、ログバッファにエントリが記録され、その割合に応じて、システム メッセージが生成されます。メッセージの生成後、スイッチにより、ログ バッファからこのエントリが消去されます。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。

`ip arp inspection log-buffer` グローバルコンフィギュレーションコマンドを使用して、バッファ内のエントリ数や、システムメッセージ生成までの指定のインターバルに必要なとされるエントリ数を設定します。記録されるパケットの種類を指定するには、`ip arp inspection vlan logging` 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。

## ダイナミック ARP インспекションのデフォルト設定

機能	デフォルト設定
ダイナミック ARP インспекション	すべての VLAN でディセーブル。
インターフェイスの信頼状態	すべてのインターフェイスは untrusted。
着信 ARP パケットのレート制限	1 秒間に 15 台の新規ホストに接続するホストが配置されたスイッチドネットワークの場合、信頼できないインターフェイスのレートは 15 pps に設定されます。  信頼できるすべてのインターフェイスでは、レート制限は行われません。  バースト インターバルは 1 秒です。
非 DHCP 環境に対する ARP ACL	ARP ACL は定義されません。
有効性検査	検査は実行されません。

機能	デフォルト設定
ログ バッファ	ダイナミック ARP インспекションがイネーブル化されると、拒否またはドロップされた ARP パケットはすべてが記録されます。 ログ内のエントリ数は 32 です。 システム メッセージ数は、毎秒 5 つに制限されます。 ロギング レート インターバルは 1 秒です。
VLAN 単位のロギング	拒否または廃棄されたすべての ARP パケットが記録されます。

## ARP ACL および DHCP スヌーピング エントリの相対的なプライオリティ

ダイナミック ARP インспекションでは、有効な IP/MAC アドレス バインディングのリストとして、DHCP スヌーピング バインディング データベースが使用されます。

DHCP スヌーピング バインディング データベース内のエントリより、ARP ACL の方が優先されます。スイッチが ACL を使用するのには、ACL が `ip arp inspection filter vlan` グローバル コンフィギュレーション コマンドを使用して作成されている場合だけです。スイッチは、まず、ARP パケットをユーザー設定の ARP ACL と比較します。DHCP スヌーピングによりデータが入力されたデータベースに有効なバインディングが存在していても、ARP ACL が ARP パケットを拒否する場合、スイッチもこのパケットを拒否します。

## 非 DHCP 環境での ARP ACL の設定

この手順は、図 2 に示すスイッチ B がダイナミック ARP インспекション、または DHCP スヌーピングをサポートしていないときにダイナミック ARP インспекションを設定する方法を示しています。

スイッチ A のポート 1 を信頼できるものとして設定した場合、スイッチ A とホスト 1 は両方とも、スイッチ B またはホスト 2 により攻撃される可能性があるため、セキュリティ ホールが作り出されます。これを阻止するには、スイッチ A のポート 1 を信頼できないものとして設定する必要があります。ホスト 2 からの ARP パケットを許可するには、ARP ACL をセットアップして、これを VLAN 1 に適用する必要があります。ホスト 2 の IP アドレスがスタティックではない（スイッチ A で ACL 設定を適用することは不可能である）場合、レイヤ 3 でスイッチ A をスイッチ B から分離し、これらの間では、ルータを使用してパケットをルートする必要があります。



スイッチ A で ARP ACL を設定するには、次の手順を実行します。この手順は、非 DHCP 環境では必須です。

#### 手順の概要

1. **enable**
2. **configure terminal**
3. **arp access-list *acl-name***
4. **permit ip host *sender-ip* mac host *sender-mac***
5. **exit**
6. **ip arp inspection filter *arp-acl-name* vlan *vlan-range* [static]**
7. **interface *interface-id***
8. **no ip arp inspection trust**
9. **end**
10. 次の show コマンドを使用します。
  - **show arp access-list *acl-name***
  - **show ip arp inspection vlan *vlan-range***
  - **show ip arp inspection interfaces**
11. **show running-config**
12. **copy running-config startup-config**

#### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  デバイス> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  デバイス# <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 3	<b>arp access-list <i>acl-name</i></b>	ARP ACL を定義し、ARP 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。デフォルトでは、ARP アクセスリストは定義されません。  (注) ARP アクセスリストの末尾に暗黙的な <b>deny ip any mac any</b> コマンドが指定されています。
ステップ 4	<b>permit ip host <i>sender-ip</i> mac host <i>sender-mac</i></b>	指定されたホスト（ホスト 2）からの ARP パケットを許可します。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <i>sender-ip</i> には、ホスト 2 の IP アドレスを入力します。</li> <li>• <i>sender-mac</i> には、ホスト 2 の MAC アドレスを入力します。</li> </ul>
ステップ 5	<b>exit</b>	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 6	<b>ip arp inspection filter</b> <i>arp-acl-name</i> <b>vlan</b> <i>vlan-range</i> [ <b>static</b> ]	<p>VLAN に ARP ACL を適用します。デフォルトでは、定義済みの ARP ACL は、どのような VLAN にも適用されません。</p> <ul style="list-style-type: none"> <li>• <i>arp-acl-name</i> には、ステップ 2 で作成した ACL の名前を指定します。</li> <li>• <i>vlan-range</i> では、スイッチとホストが存在する VLAN を指定します。VLAN ID 番号により識別される単一の VLAN、ハイフンで区切られた VLAN 範囲、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ~ 4094 です。</li> <li>• (任意) <b>static</b> を指定すると、ARP ACL 内の暗黙的な拒否が明示的な拒否と見なされ、それ以前に指定された ACL 句に一致しないパケットは廃棄されます。DHCP バインディングは使用されません。</li> </ul> <p>このキーワードを指定しない場合は、ACL 内にはパケットを拒否する明示的な拒否が存在しないこととなります。この場合は、ACL 句に一致しないパケットを許可するか拒否するかは、DHCP バインディングによって決定されます。</p> <p>IP アドレスと MAC アドレスとのバインディングしかなかった ARP パケットは、ACL に照合されません。パケットは、アクセス リストで許可された場合だけに許可されます。</p>
ステップ 7	<b>interface</b> <i>interface-id</i>	スイッチ B に接続されたスイッチ A の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 8	<b>no ip arp inspection trust</b>	スイッチ B に接続されたスイッチ A のインターフェイスを <b>untrusted</b> として設定します。

	コマンドまたはアクション	目的
		<p>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。</p> <p>信頼できないインターフェイスでは、スイッチはすべての ARP 要求と応答を代行受信します。ルータは、代行受信した各パケットが、IP アドレスと MAC アドレスと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 キャッシュを更新するか、適切な宛先にパケットを転送します。スイッチは、無効なパケットをドロップし、<b>ip arp inspection vlan logging</b> グローバル コンフィギュレーション コマンドで指定されたロギング設定に従ってログバッファに記録します。</p>
ステップ 9	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 10	次の show コマンドを使用します。 <ul style="list-style-type: none"> <li>• <b>show arp access-list acl-name</b></li> <li>• <b>show ip arp inspection vlan <i>vlan-range</i></b></li> <li>• <b>show ip arp inspection interfaces</b></li> </ul>	入力を確認します。
ステップ 11	<b>show running-config</b> 例：  デバイス# <b>show running-config</b>	入力を確認します。
ステップ 12	<b>copy running-config startup-config</b> 例：  デバイス# <b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。

## DHCP 環境でのダイナミック ARP インспекションの設定

### 始める前に

この手順では、2つのスイッチがダイナミック ARP インспекションをサポートしているときに、この機能を設定する方法を示します。ホスト 1 はスイッチ A に、ホスト 2 はスイッチ B にそれぞれ接続されています。スイッチは両方とも、ホストが配置されている VLAN 1 でダイナミック ARP インспекションを実行しています。DHCP サーバーはスイッチ A に接続されています。両方のホストは、同一の DHCP サーバーから IP アドレスを取得します。したがっ

て、スイッチ A はホスト 1 およびホスト 2 に対するバインディングを、スイッチ B はホスト 2 に対するバインディングを持ちます。



(注) 着信 ARP 要求、および ARP 応答で IP/MAC アドレスバインディングを検証するために、ダイナミック ARP インспекション DHCP スヌーピングバインディングデータベースのエントリに依存します。IP アドレスがダイナミックに割り当てられた ARP パケットを許可する際は、DHCP スヌーピングをイネーブルにしてください。

ダイナミック ARP インспекションを設定するには、次の手順を実行します。この処理は、両方のスイッチで行う必要があります。この手順は必須です。

手順の概要

1. **enable**
2. **show cdp neighbors**
3. **configure terminal**
4. **ip arp inspection vlan *vlan-range***
5. **Interface *interface-id***
6. **ip arp inspection trust**
7. **end**
8. **show ip arp inspection interfaces**
9. **show ip arp inspection vlan *vlan-range***
10. **show ip dhcp snooping binding**
11. **show ip arp inspection statistics vlan *vlan-range***
12. **configure terminal**
13. **configure terminal**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  デバイス> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>show cdp neighbors</b> 例：  デバイス (config-if) # <b>show cdp neighbors</b>	スイッチ間の接続を確認します。
ステップ 3	<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
	デバイス# <code>configure terminal</code>	
ステップ 4	<b>ip arp inspection vlan <i>vlan-range</i></b> 例： デバイス(config)# <code>ip arp inspection vlan 1</code>	VLAN 単位で、ダイナミック ARP インспекションをイネーブルにします。デフォルトでは、すべての VLAN 上でダイナミック ARP インспекションはディセーブルになっています。vlan-range には、VLAN ID 番号で識別された単一の VLAN、ハイフンで区切られた範囲の VLAN、またはカンマで区切られた一連の VLAN を指定できます。指定できる範囲は 1 ~ 4094 です。両方のスイッチに同じ VLAN ID を指定します。
ステップ 5	<b>Interface <i>interface-id</i></b> 例： デバイス(config)# <code>interface gigabitethernet1/0/1</code>	他のスイッチに接続されるインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	<b>ip arp inspection trust</b> 例： デバイス(config-if)# <code>ip arp inspection trust</code>	<p>スイッチ間の接続を trusted に設定します。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。</p> <p>スイッチは、信頼できるインターフェイスにあるもう 1 つのスイッチから受信した ARP パケットは確認しません。この場合、パケットはそのまま転送されます。</p> <p>信頼できないインターフェイスでは、スイッチはすべての ARP 要求と応答を代行受信します。ルータは、代行受信した各パケットが、IP アドレスと MAC アドレスと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 キャッシュを更新するか、適切な宛先にパケットを転送します。スイッチは、無効なパケットをドロップし、ip arp inspection vlan logging グローバル コンフィギュレーション コマンドで指定されたロギング設定に従ってログ バッファに記録します。</p>
ステップ 7	<b>end</b> 例： デバイス(config-if)# <code>end</code>	特権 EXEC モードに戻ります。
ステップ 8	<b>show ip arp inspection interfaces</b> 例：	インターフェイスでダイナミック ARP インспекションの設定を検証します。

	コマンドまたはアクション	目的
ステップ 9	<b>show ip arp inspection vlan <i>vlan-range</i></b> 例： デバイス (config-if) # <b>show ip arp inspection vlan 1</b>	VLAN でダイナミック ARP インспекションの設定を検証します。
ステップ 10	<b>show ip dhcp snooping binding</b> 例： デバイス (config-if) # <b>show ip dhcp snooping binding</b>	DHCP バインディングを確認します。
ステップ 11	<b>show ip arp inspection statistics vlan <i>vlan-range</i></b> 例： デバイス (config-if) # <b>show ip arp inspection statistics vlan 1</b>	VLAN でダイナミック ARP インспекションの統計情報を確認します。
ステップ 12	<b>configure terminal</b> 例： デバイス # <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 13	<b>configure terminal</b> 例： デバイス # <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。

## 着信 ARP パケットのレート制限

スイッチの CPU は、ダイナミック ARP インспекション確認検査を実行します。したがって、DoS 攻撃を阻止するために、着信 ARP パケット数はレート制限されます。

着信 ARP パケットのレートが設定された制限を超えると、スイッチはポートを **errdisable** ステートにします。 **errdisable** 回復をイネーブルにして、指定されたタイムアウト時間の後にポートがこのステートから自動的に抜け出すようにするまで、ポートはこのステートのままです。



(注) インターフェイス上のレート制限を設定しない限り、インターフェイスの信頼状態を変更することは、レート制限をその信頼状態のデフォルト値に変更することになります。レート制限を設定すると、信頼状態が変更された場合でもインターフェイスはレート制限を保ちます。 **no ip arp inspection limit** 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と、インターフェイスはデフォルトのレート制限に戻ります。

着信 ARP パケットのレートを制限するには、次の手順を実行します。この手順は任意です。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **interface *interface-id***
4. **ip arp inspection limit {rate pps [burst interval seconds] | none}**
5. **exit**
6. 次のコマンドを使用します。
  - **errdisable detect cause arp-inspection**
  - **errdisable recovery cause arp-inspection**
  - **errdisable recovery interval *interval***
7. **exit**
8. 次の show コマンドを使用します。
  - **show ip arp inspection interfaces**
  - **show errdisable recovery**
9. **show running-config**
10. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： デバイス> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： デバイス# <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 3	<b>interface <i>interface-id</i></b>	レート制限されるインターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<b>ip arp inspection limit {rate pps [burst interval seconds]   none}</b>	インターフェイス上の着信 ARP 要求および ARP 応答のレートを制限します。デフォルト レートは、信頼できないインターフェイスでは 15 pps、信頼できるインターフェイスでは無制限です。バースト インターバルは 1 秒です。

	コマンドまたはアクション	目的
		<p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> <li>• <b>ratepps</b> には、1 秒あたりに処理される着信パケット数の上限を指定します。有効な範囲は 0 ~ 2048 pps です。</li> <li>• (任意) <b>burst intervalseconds</b> は、レートの高い ARP パケットの有無についてインターフェイスがモニタリングされる間隔 (秒) を指定します。指定できる範囲は 1 ~ 15 です。</li> <li>• <b>rate none</b> には、処理可能な着信 ARP パケットのレートに上限を指定しません。</li> </ul>
ステップ 5	<b>exit</b>	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 6	<p>次のコマンドを使用します。</p> <ul style="list-style-type: none"> <li>• <b>errdisable detect cause arp-inspection</b></li> <li>• <b>errdisable recovery cause arp-inspection</b></li> <li>• <b>errdisable recovery interval interval</b></li> </ul>	<p>(任意) ダイナミック ARP インспекションの <b>errdisable</b> ステートからのエラー回復をイネーブルにし、ダイナミック ARP インспекションの回復メカニズムで使用する変数を設定します。</p> <p>デフォルトでは、回復はディセーブルで、回復のインターバルは 300 秒です。</p> <p><b>interval interval</b> には、<b>error-disabled</b> ステートから回復する時間を秒単位で指定します。指定できる範囲は 30 ~ 86400 です。</p>
ステップ 7	<b>exit</b>	特権 EXEC モードに戻ります。
ステップ 8	<p>次の show コマンドを使用します。</p> <ul style="list-style-type: none"> <li>• <b>show ip arp inspection interfaces</b></li> <li>• <b>show errdisable recovery</b></li> </ul>	設定を確認します。
ステップ 9	<p><b>show running-config</b></p> <p>例 :</p> <p>デバイス# <b>show running-config</b></p>	入力を確認します。
ステップ 10	<p><b>copy running-config startup-config</b></p> <p>例 :</p> <p>デバイス# <b>copy running-config startup-config</b></p>	(任意) コンフィギュレーション ファイルに設定を保存します。



# ダイナミック ARP インспекション検証チェックの実行

ダイナミック ARP インспекションは、不正な IP/MAC アドレス バインディングを持つ ARP パケットを代行受信し、ログに記録して、廃棄します。宛先 MAC アドレス、送信側および宛先の IP アドレス、および送信元 MAC アドレスで追加検証を実行するように、スイッチを設定できます。

着信 ARP パケットで特定のチェックを実行するには、次の手順を実行します。この手順は任意です。

## 手順の概要

1. **enable**
2. **configure terminal**
3. **ip arp inspection validate {[src-mac] [dst-mac] [ip]}**
4. **exit**
5. **show ip arp inspection vlan *vlan-range***
6. **show running-config**
7. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  デバイス> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  デバイス# <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 3	<b>ip arp inspection validate {[src-mac] [dst-mac] [ip]}</b>	着信 ARP パケットで特定の検査を実行します。デフォルトでは、検証は実行されません。  キーワードの意味は次のとおりです。  • <b>src-mac</b> では、イーサネットヘッダーの送信元 MAC アドレスと ARP 本文の送信元 MAC アドレスが比較されます。この検査は、ARP 要求および ARP 応答の両方に対して実行されます。イネーブルにすると、異なる MAC アドレスを持

	コマンドまたはアクション	目的
		<p>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。</p> <ul style="list-style-type: none"> <li>• <b>dst-mac</b> では、イーサネットヘッダーの宛先 MAC アドレスと ARP 本文の宛先 MAC アドレスが比較されます。この検査は、ARP 応答に対して実行されます。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。</li> <li>• <b>ip</b> では、ARP 本文から、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。</li> </ul> <p>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。コマンドを実行するたびに、その前のコマンドの設定は上書きされます。つまり、コマンドが <b>src</b> および <b>dst mac</b> の検証をイネーブルにし、別のコマンドが IP 検証だけをイネーブルにすると、2 番目のコマンドによって <b>src</b> および <b>dst mac</b> の検証がディセーブルになります。</p>
ステップ 4	<b>exit</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show ip arp inspection vlan <i>vlan-range</i></b>	設定を確認します。
ステップ 6	<b>show running-config</b> 例 :  デバイス# <b>show running-config</b>	入力を確認します。
ステップ 7	<b>copy running-config startup-config</b> 例 :  デバイス# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## DAI のモニタリング

DAI をモニターするには、次のコマンドを使用します。

コマンド	説明
<b>clear ip arp inspection statistics</b>	ダイナミック ARP インспекション統計情報をクリアします。
<b>show ip arp inspection statistics [vlan vlan-range]</b>	指定の VLAN において、転送されたパケット、廃棄されたパケット、MAC 検証に失敗したパケット、IP 検証に失敗したパケット、ACL によって許可および拒否されたパケット、DHCP によって許可および拒否されたパケットの統計情報を表示します。VLAN が指定されていない場合、または範囲が指定されている場合は、ダイナミック ARP インспекションがイネーブルにされた (アクティブ) VLAN だけの情報を表示します。
<b>clear ip arp inspection log</b>	ダイナミック ARP インспекションログバッファをクリアします。
<b>show ip arp inspection log</b>	ダイナミック ARP インспекションログバッファの設定と内容を表示します。

**show ip arp inspection statistics** コマンドでは、スイッチは信頼されたダイナミック ARP インспекションポート上の各 ARP 要求および応答パケットの転送済みパケット数を増加させます。スイッチは、送信元 MAC、宛先 MAC、または IP 検証チェックによって拒否された各パケットの ACL または DHCP 許可済みパケット数を増加させ、適切な失敗数を増加させます。

## DAI の設定の確認

DAI の設定を表示して確認するには、次のコマンドを使用します。

コマンド	説明
<b>show arp access-list [acl-name]</b>	ARP ACL についての詳細情報を表示します。
<b>show ip arp inspection interfaces [interface-id]</b>	指定されたインターフェイスまたはすべてのインターフェイスの ARP パケットの信頼状態およびレート制限を表示します。

コマンド	説明
<code>show ip arp inspection vlan <i>vlan-range</i></code>	指定された VLAN のダイナミック ARP インспекションの設定および動作ステータスを表示します。VLAN が指定されていない場合、または範囲が指定されている場合は、ダイナミック ARP インспекションがイネーブルにされた（アクティブ）VLAN だけの情報を表示します。

## ダイナミック ARP インспекションの機能方法

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレーンで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、[www.cisco.com/go/cfn](http://www.cisco.com/go/cfn) に移動します。Cisco.com のアカウントは必要ありません。

表 45: ダイナミック ARP インспекションの機能方法

機能名	リリース	機能情報
ダイナミック ARP インспекション	Cisco IOS XE Everest 16.5.1a	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。ダイナミック ARP インспекションは、ネットワーク内の ARP パケットの正当性を確認するセキュリティ機能です。不正な IP/MAC アドレス バインディングを持つ ARP パケットを代行受信し、ログに記録して、廃棄します。この機能により、ネットワークをある種の間接攻撃から保護することができます。



## 第 22 章

# IPv6 ファースト ホップ セキュリティの設定

- IPv6 でのファースト ホップ セキュリティの前提条件 (455 ページ)
- IPv6 でのファースト ホップ セキュリティの制約事項 (455 ページ)
- IPv6 でのファースト ホップ セキュリティに関する情報 (456 ページ)
- IPv6 スヌーピング ポリシーの設定方法 (458 ページ)
- IPv6 スヌーピング ポリシーをインターフェイスにアタッチする方法 (460 ページ)
- IPv6 スヌーピング ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法 (462 ページ)
- IPv6 スヌーピング ポリシーを VLAN にグローバルにアタッチする方法 (463 ページ)
- IPv6 バインディング テーブルの内容を設定する方法 (464 ページ)
- IPv6 ネイバー探索検査ポリシーの設定方法 (465 ページ)
- IPv6 ルータ アドバタイズメント ガード ポリシーの設定方法 (470 ページ)
- IPv6 DHCP ガード ポリシーの設定方法 (476 ページ)
- IPv6 ソース ガードの設定方法 (482 ページ)
- IPv6 プレフィックス ガードの設定方法 (485 ページ)
- IPv6 ファースト ホップ セキュリティの設定例 (488 ページ)
- IPv6 ファースト ホップ セキュリティの機能履歴 (489 ページ)

## IPv6 でのファースト ホップ セキュリティの前提条件

- 必要な、IPv6 が有効になっている SDM テンプレートが設定されていること。
- IPv6 ネイバー探索機能についての知識が必要です。

## IPv6 でのファースト ホップ セキュリティの制約事項

- 次の制限は、FHS ポリシーを EtherChannel インターフェイスに適用する場合に該当します (ポート チャネル)。

- FHS ポリシーがアタッチされた物理ポートは EtherChannel グループに参加することができません。
- FHS ポリシーは、EtherChannel グループのメンバーである場合に物理ポートにアタッチすることができません。
- デフォルトでは、スヌーピング ポリシーにはセキュリティ レベルのガードがあります。そのようなスヌーピング ポリシーがアクセス スイッチに設定されると、ルータまたは DHCP サーバー/リレーに対応するアップリンク ポートが信頼できるポートとして設定されていても、IPv6 (DHCPv6) サーバー パケットに対する外部 IPv6 ルータ アドバタイズメント(RA)または Dynamic Host Configuration Protocol はブロックされます。IPv6 RA または DHCPv6 サーバー メッセージを許可するには、次の手順を実行します。
  - IPv6 RA ガード ポリシー (RA の場合) または IPv6 DHCP ガード ポリシー (DHCP サーバー メッセージの場合) をアップリンク ポートに適用します。
  - 低いセキュリティ レベルでスヌーピング ポリシーを設定します (たとえば、`glean` や `inspect` など)。しかし、ファースト ホップ セキュリティ機能の利点が有効でないため、このようなスヌーピング ポリシーでは、低いセキュリティ レベルを設定することはお勧めしません。

## IPv6 でのファースト ホップ セキュリティ に関する情報

IPv6 のファーストホップセキュリティ (FHS IPv6) は、ポリシーを物理インターフェイス、EtherChannel インターフェイス、または VLAN にアタッチできる一連の IPv6 セキュリティ機能です。IPv6 ソフトウェア ポリシー データベース サービスは、これらのポリシーを保存しアクセスします。ポリシーを設定または変更すると、ポリシー属性はソフトウェアポリシーデータベースに保存または更新され、その後指定したとおりに適用されます。次の IPv6 ポリシーが現在サポートされています。

- IPv6 スヌーピング ポリシー : IPv6 スヌーピング ポリシーは、IPv6 内の FHS で使用できるほとんどの機能を有効にできるコンテナ ポリシーとして機能します。
- IPv6 FHS バインディング テーブルの内容 : スイッチに接続された IPv6 ネイバーのデータベース テーブルはネイバー探索 (ND) プロトコルスヌーピングなどの情報ソースから作成されます。このデータベースまたはバインディング テーブルは、リンク層アドレス (LLA)、IPv4 または IPv6 アドレス、およびスプーフィングやリダイレクト攻撃を防止するために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 (IPv6 ND 検査など) によって使用されます。
- IPv6 ネイバー探索検査 : IPv6 ND 検査は、レイヤ 2 ネイバー テーブル内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、保護します。IPv6 ND 検査は、信頼できるバインディング テーブル データベースを構築するためにネイバー探索メッセージを分析します。準拠していない IPv6 ネイバー探索メッセージは破棄されます。ND メッセージは、その IPv6 からメディアアクセスコントロール (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。

この機能によって、DAD、アドレス解決、ルータ ディスカバリ、ネイバー キャッシュに対する攻撃などの、ND メカニズムに固有の脆弱性のいくつかが軽減されます。



(注) 有効な Cisco IOS XE Release 16.3.1、ND インスペクション機能、IPv6 スヌーピングポリシー、IPv6 FHS バインディング テーブル コンテンツは、スイッチ統合セキュリティ機能 (SISF) ベースの デバイストラッキングによってサポートされます。詳細については、『Software Configuration Guide』の「*Configuring SISF based device tracking*」の項を参照してください。

- IPv6 ルータ アドバタイズメント ガード : IPv6 ルータ アドバタイズメント (RA) ガード機能を使用すると、ネットワーク管理者は、ネットワーク スイッチ 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 メッセージをブロックまたは拒否できます。RA は、リンクで自身をアナウンスするためにルータによって使用されます。RA ガード機能は、これらの RA を分析して、未承認のルータによって送信された偽の RA をフィルタリングして除外します。ホスト モードでは、ポートではルータ アドバタイズメントとルータ 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 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。レイヤ 2 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 は破棄されます。
- IPv6 DHCP ガード : IPv6 DHCP ガード機能は、承認されない DHCPv6 サーバーおよびリレー エージェントからの返信およびアドバタイズメント メッセージをブロックします。IPv6 DHCP ガードは、偽造されたメッセージがバインディング テーブルに入るのを防ぎ、DHCPv6 サーバーまたは DHCP リレーからデータを受信することが明示的に設定されていないポートで受信された DHCPv6 サーバー メッセージをブロックできます。この機能を使用するには、ポリシーを設定してインターフェイスまたは VLAN にアタッチします。DHCP ガード パケットをデバッグするには、**debug ipv6 snooping dhcp-guard** 特権 EXEC コマンドを使用します。

- IPv6 ソース ガード : IPv4 ソース ガードと同様、IPv6 ソース ガードは送信元アドレス プルーフィングを防ぐために、送信元アドレスまたはプレフィックスを検証します。

ソース ガードでは、送信元または宛先アドレスに基づいてトラフィックを許可または拒否するようにハードウェアをプログラムします。ここでは、データパケットのトラフィックのみを処理します。

ソース ガード パケットをデバッグするには、**debug ipv6 snooping source-guard** 特権 EXEC コマンドを使用します。

次の制約事項が適用されます。

- FHS ポリシーは、EtherChannel グループのメンバーである場合に物理ポートにアタッチすることができません。

- IPv6 ソース ガードがスイッチ ポートで有効になっている場合は、そのスイッチ ポートが属するインターフェイスで NDP または DHCP スヌーピングを有効にする必要があります。そうしないと、このポートからのすべてのデータトラフィックがブロックされます。
- IPv6 ソース ガードポリシーを VLAN に適用することはできません。インターフェイス レベルのみでサポートされています。
- インターフェイスで IPv4 および IPv6 のソース ガードを一緒に設定する場合は、**ip verify source** の代わりに **ip verify source mac-check** の使用を推奨します。2つの異なるフィルタリングルール (IPv4 (IP フィルタ) 用と IPv6 (IP-MAC フィルタ) 用) が設定されているため、特定のポートの IPv4 接続が切断される可能性があります。
- IPv6 ソース ガードとプレフィックス ガードは同時に使用できません。ポリシーをインターフェイスに付加する際は、「アドレスを確認」するか「プレフィックスを確認」する必要はありますが、両方を確認する必要はありません。
- PVLAN と送信元/プレフィックス ガードは同時に適用できません。

IPv6 送信元ガードの詳細については、Cisco.comで『Cisco IOS IPv6 Configuration Guide Library』の「[IPv6 Source Guard](#)」の章を参照してください。

- IPv6 プレフィックス ガード : IPv6 プレフィックス ガードは、IPv6 送信元ガード機能内で動作し、デバイスがトポロジに不正なアドレスから発信されたトラフィックを拒否できるようにします。IPv6 プレフィックス ガードは、IPv6 プレフィックスが DHCP プレフィックス委任を使用してデバイス (ホームゲートウェイなど) に委任される場合によく使用されています。この機能は、リンクに割り当てられたアドレスの範囲を検出し、この範囲に入っていないアドレスを発信元とするトラフィックをブロックします。

IPv6 プレフィックス ガードの詳細については、Cisco.comで『Cisco IOS IPv6 Configuration Guide Library』の「[IPv6 Prefix Guard](#)」の章を参照してください。

- IPv6 宛先ガード : IPv6 宛先ガード機能は、IPv6 ネイバー探索で動作し、リンク上でアクティブであると認識されているアドレスについてのみ、デバイスがアドレスを解決します。アドレスグリーンアップ機能に依存して、リンク上でアクティブなすべての宛先をバインディング テーブルに挿入してから、バインディング テーブルで宛先が見つからなかったときに実行される解決をブロックします。

IPv6 宛先ガードに関する詳細については、Cisco.comで『Cisco IOS IPv6 Configuration Guide Library』の「[IPv6 Destination Guard](#)」の章を参照してください。

## IPv6 スヌーピング ポリシーの設定方法

IPv6 スヌーピングポリシー機能は廃止されました。コマンドはCLIに表示され、設定できますが、代わりにスイッチ統合セキュリティ機能 (SISF) ベースのデバイス追跡機能を使用することを推奨します。

IPv6 スヌーピング ポリシーを設定するには、特権 EXEC モードで次の手順を実行します。



## 手順の概要

1. **configure terminal**
2. **ipv6 snooping policy *policy-name***
3. **{[default ]|[device-role {node | switch}]|[ limit address-count *value*]|[no] |[protocol {dhcp | ndp} ]|[security-level {glean | guard | inspect} ]|[tracking {disable [stale-lifetime [*seconds* | infinite] ]| enable [reachable-lifetime [*seconds* | infinite] } ]|[trusted-port ] }**
4. **end**
5. **show ipv6 snooping policy *policy-name***

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： デバイス# <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 snooping policy <i>policy-name</i></b> 例： デバイス(config)# <b>ipv6 snooping policy example_policy</b>	スヌーピング ポリシーを作成し、IPv6 スヌーピング ポリシー コンフィギュレーション モードに移行します。
ステップ 3	<b>{[default ] [device-role {node   switch}] [ limit address-count <i>value</i>] [no]  [protocol {dhcp   ndp} ] [security-level {glean   guard   inspect} ] [tracking {disable [stale-lifetime [<i>seconds</i>   infinite] ]  enable [reachable-lifetime [<i>seconds</i>   infinite] } ] [trusted-port ] }</b> 例： デバイス( <b>config-ipv6-snooping</b> )# <b>security-level inspect</b> 例： デバイス( <b>config-ipv6-snooping</b> )# <b>trusted-port</b>	データアドレス グリーニングを有効にし、さまざまな条件に対してメッセージを検証し、メッセージのセキュリティ レベルを指定します。 <ul style="list-style-type: none"> <li>• (任意) <b>default</b> : すべてをデフォルト オプションに設定します。</li> <li>• (任意) <b>device-role {node} switch</b> : ポートに接続されたデバイスの役割を指定します。デフォルトは <b>node</b> です。</li> <li>• (任意) <b>limit address-count <i>value</i></b> : ターゲットごとに許可されるアドレス数を制限します。</li> <li>• (任意) <b>no</b> : コマンドを無効にするか、またはそのデフォルトに設定します。</li> <li>• (任意) <b>protocol {dhcp   ndp}</b> : 分析のために、スヌーピング機能にどのプロトコルをリダイレクトするかを指定します。デフォルトは、<b>dhcp</b> および <b>ndp</b> です。デフォルトを変更するには、<b>no protocol</b> コマンドを使用します。</li> <li>• (任意) <b>security-level {glean guard inspect}</b> : この機能によって適用されるセキュリティのレベルを指定します。デフォルトは <b>guard</b> です。</li> </ul>

	コマンドまたはアクション	目的
		<p><b>glean</b> : メッセージからアドレスを収集し、何も確認せずにバインディング テーブルに入力します。</p> <p><b>guard</b> : アドレスを収集し、メッセージを検査します。さらに、RA および DHCP サーバメッセージを拒否します。これがデフォルトのオプションです。</p> <p><b>inspect</b> : アドレスを収集し、メッセージの一貫性と準拠を検証して、アドレスの所有権を適用します。</p> <ul style="list-style-type: none"> <li>• (任意) <b>tracking {disable enable}</b> : デフォルトの追跡動作を上書きし、追跡オプションを指定します。</li> <li>• (任意) <b>trusted-port</b> : 信頼できるポートを設定します。これにより、該当するターゲットに対するガードがディセーブルになります。信頼できるポートを経由して学習されたバインディングは、他のどのポートを経由して学習されたバインディングよりも優先されます。テーブル内にエントリを作成しているときに衝突が発生した場合、信頼できるポートが優先されます。</li> </ul>
ステップ 4	<b>end</b> 例 : デバイス (config-ipv6-snooping) # <b>exit</b>	コンフィギュレーションモードから特権 EXEC モードに戻ります。
ステップ 5	<b>show ipv6 snooping policy policy-name</b> 例 : デバイス # <b>show ipv6 snooping policy example_policy</b>	スヌーピング ポリシー設定を表示します。

#### 次のタスク

IPv6 スヌーピング ポリシーをインターフェイスまたは VLAN にアタッチします。

## IPv6 スヌーピング ポリシーをインターフェイスにアタッチする方法

インターフェイスまたは VLAN に IPv6 スヌーピング ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

## 手順の概要

1. **configure terminal**
2. **interface** Interface\_type stack/module/port
3. **switchport**
4. **ipv6 snooping** [ **attach-policy** policy\_name [ **vlan** {vlan\_id | **add** vlan\_ids | **except** vlan\_ids | **none** | **remove** vlan\_ids} ] | **vlan** {vlan\_id | **add** vlan\_ids | **except** vlan\_ids | **none** | **remove** vlan\_ids | **all** } ]
5. **do show running-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： デバイス# <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>interface</b> Interface_type stack/module/port 例： デバイス(config)# <b>interface gigabitethernet 1/1/4</b>	インターフェイスのタイプおよび ID を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<b>switchport</b> 例： デバイス(config-if)# <b>switchport</b>	switchport モードを開始します。  (注) インターフェイスがレイヤ3モードの場合に、レイヤ2パラメータを設定するには、パラメータを指定せずに <b>switchport</b> インターフェイスコンフィギュレーション コマンドを入力し、インターフェイスをレイヤ2モードにする必要があります。これにより、インターフェイスがいったんシャットダウンしてから再度有効になり、インターフェイスが接続しているデバイスに関するメッセージが表示されることがあります。レイヤ3モードのインターフェイスをレイヤ2モードにした場合、影響のあるインターフェイスに関連する以前の設定情報が消失する可能性があります。インターフェイスはデフォルト設定に戻ります。 <b>switchport</b> コンフィギュレーション モードではコマンドプロンプトは (config-if) # と表示されません。

	コマンドまたはアクション	目的
ステップ 4	<p><b>ipv6 snooping</b> [ <b>attach-policy</b> <i>policy_name</i> [ <b>vlan</b> {<i>vlan_id</i>   <b>add</b> <i>vlan_ids</i>   <b>except</b> <i>vlan_ids</i>   <b>none</b>   <b>remove</b> <i>vlan_ids</i>}] ] <b>vlan</b> {<i>vlan_id</i>   <b>add</b> <i>vlan_ids</i>   <b>except</b> <i>vlan_ids</i>   <b>none</b>   <b>remove</b> <i>vlan_ids</i>   <b>all</b>} ]</p> <p>例 :</p> <pre>デバイス(config-if)# ipv6 snooping</pre> <p>or</p> <pre>デバイス(config-if)# ipv6 snooping attach-policy example_policy</pre> <p>or</p> <pre>デバイス(config-if)# ipv6 snooping vlan 111,112</pre> <p>or</p> <pre>デバイス(config-if)# ipv6 snooping attach-policy example_policy vlan 111,112</pre>	<p>インターフェイスまたはそのインターフェイス上の特定の VLAN にカスタム IPv6 スヌーピングポリシーをアタッチします。デフォルトポリシーをインターフェイスにアタッチするには、<b>attach-policy</b> キーワードを指定せずに <b>ipv6 snooping</b> コマンドを使用します。デフォルトポリシーをインターフェイス上の VLAN にアタッチするには、<b>ipv6 snooping vlan</b> コマンドを使用します。デフォルトポリシーは、セキュリティ レベル <b>guard</b>、デバイス ロール <b>node</b>、プロトコル <b>ndp</b> および <b>dhcp</b> です。</p>
ステップ 5	<p><b>do show running-config</b></p> <p>例 :</p> <pre>デバイス#(config-if)# do show running-config</pre>	<p>インターフェイス コンフィギュレーション モードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。</p>

## IPv6 スヌーピング ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

EtherChannel インターフェイスまたは VLAN に IPv6 スヌーピング ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<p><b>configure terminal</b></p> <p>例 :</p> <pre>デバイス# configure terminal</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>
ステップ 2	<p><b>interface range</b> <i>Interface_name</i></p> <p>例 :</p> <pre>デバイス(config)# interface range Po11</pre>	<p>EtherChannel の作成時に割り当てられたポート チャネル インターフェイスの名前を指定します。インターフェイス範囲コンフィギュレーションモードを開始します。</p>

	コマンドまたはアクション	目的
		ヒント インターフェイス名やタイプを簡単に参照するには <b>do show interfaces summary</b> コマンドを使用します。
ステップ 3	<p><b>ipv6 snooping</b> [ <b>attach-policy</b> <i>policy_name</i> [ <b>vlan</b> {<i>vlan_ids</i>   <b>add</b> <i>vlan_ids</i>   <b>except</b> <i>vlan_ids</i>   <b>none</b>   <b>remove</b> <i>vlan_ids</i>   <b>all</b>} ] ]   <b>vlan</b> [ {<i>vlan_ids</i>   <b>add</b> <i>vlan_ids</i>   <b>except</b> <i>vlan_ids</i>   <b>none</b>   <b>remove</b> <i>vlan_ids</i>   <b>all</b>} ] ]</p> <p>例 :</p> <pre> デバイス(config-if-range)# ipv6 snooping attach-policy example_policy  or  デバイス(config-if-range)# ipv6 snooping attach-policy example_policy vlan 222,223,224  or  デバイス(config-if-range)#ipv6 snooping vlan 222, 223,224 </pre>	IPv6 スヌーピング ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。 <b>attach-policy</b> オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 4	<p><b>do show running-config</b> <b>interface</b><i>portchannel_interface_name</i></p> <p>例 :</p> <pre> デバイス#(config-if-range)# do show running-config int poll </pre>	コンフィギュレーションモードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

## IPv6 スヌーピング ポリシーを VLAN にグローバルにアタッチする方法

複数のインターフェイス上の VLAN に IPv6 スヌーピング ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

### 手順の概要

1. **configure terminal**
2. **vlan configuration** *vlan\_list*
3. **ipv6 snooping** [ **attach-policy** *policy\_name* ]
4. **do show running-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： デバイス# <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>vlan configuration <i>vlan_list</i></b> 例： デバイス (config)# <b>vlan configuration 333</b>	VLAN インターフェイスのコンフィギュレーション モードを開始し、IPv6 スヌーピング ポリシーをアタッチする VLAN を指定します。
ステップ 3	<b>ipv6 snooping [ attach-policy <i>policy_name</i>]</b> 例： デバイス (config-vlan-config)# <b>ipv6 snooping attach-policy example_policy</b>	すべてのスイッチおよびスタック インターフェイスで、IPv6 スヌーピング ポリシーを指定した VLAN にアタッチします。 <b>attach-policy</b> オプションを使用しない場合、デフォルト ポリシーがアタッチされます。デフォルト ポリシーは、セキュリティ レベル <b>guard</b> 、デバイス ロール <b>node</b> 、プロトコル <b>ndp</b> および <b>dhcp</b> です。
ステップ 4	<b>do show running-config</b> 例： デバイス# (config-if)# <b>do show running-config</b>	インターフェイス コンフィギュレーション モードを終了しないで、ポリシーが特定の VLAN にアタッチされていることを確認します。

## IPv6 バインディング テーブルの内容を設定する方法

IPv6 バインディング テーブル コンテンツを設定するには、特権 EXEC モードで次の手順を実行します。

## 手順の概要

- configure terminal**
- [no] ipv6 neighbor binding [ vlan *vlan-id* {*ipv6-address* interface interface\_type stack/module/port hw\_address [reachable-lifetimevalue [*seconds* | default | infinite] | [tracking { [default | disable] [reachable-lifetimevalue [*seconds* | default | infinite] | [enable [reachable-lifetimevalue [*seconds* | default | infinite] | [retry-interval {*seconds* | default [reachable-lifetimevalue [*seconds* | default | infinite] } ]**
- [no] ipv6 neighbor binding max-entries number [ mac-limit number | port-limit number [ mac-limit number ] | vlan-limit number [ [ mac-limit number ] | [ port-limit number [mac-limitnumber] ] ] ]**
- ipv6 neighbor binding logging**
- exit**
- show ipv6 neighbor binding**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： デバイス# <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] ipv6 neighbor binding [ vlan vlan-id {ipv6-address interface interface_type stack/module/port hw_address [reachable-lifetimevalue [seconds   default   infinite]   [tracking { [default   disable] [ reachable-lifetimevalue [seconds   default   infinite]   [enable [reachable-lifetimevalue [seconds   default   infinite]   [retry-interval {seconds  default [reachable-lifetimevalue [seconds   default   infinite] } ]</b> 例： デバイス(config)# <b>ipv6 neighbor binding</b>	バインディングテーブルデータベースにスタティック エントリを追加します。
ステップ 3	<b>[no] ipv6 neighbor binding max-entries number [ mac-limit number   port-limit number [ mac-limit number]   vlan-limit number [ [ mac-limit number]   [ port-limit number [mac-limitnumber] ] ] ]</b> 例： デバイス(config)# <b>ipv6 neighbor binding max-entries 30000</b>	バインディング テーブル キャッシュに挿入できる エントリの最大数を指定します。
ステップ 4	<b>ipv6 neighbor binding logging</b> 例： デバイス(config)# <b>ipv6 neighbor binding logging</b>	バインディング テーブル メイン イベントのロギングを有効にします。
ステップ 5	<b>exit</b> 例： デバイス(config)# <b>exit</b>	グローバル コンフィギュレーション モードを終了して、ルータを特権 EXEC モードにします。
ステップ 6	<b>show ipv6 neighbor binding</b> 例： デバイス# <b>show ipv6 neighbor binding</b>	バインディング テーブルの内容を表示します。

## IPv6 ネイバー探索検査ポリシーの設定方法

特権 EXEC モードから、IPv6 ND 検査ポリシーを設定するには、次の手順に従ってください。

## 手順の概要

1. **configure terminal**
2. **[no]ipv6 nd inspection policy *policy-name***
3. **device-role {host | switch}**
4. **limit address-count *value***
5. **tracking {enable [reachable-lifetime {*value* | infinite}] | disable [stale-lifetime {*value* | infinite}]}**
6. **trusted-port**
7. **validate source-mac**
8. **no {device-role | limit address-count | tracking | trusted-port | validate source-mac}**
9. **default {device-role | limit address-count | tracking | trusted-port | validate source-mac}**
10. **do show ipv6 nd inspection policy *policy\_name***

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： デバイス# <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]ipv6 nd inspection policy <i>policy-name</i></b> 例： デバイス (config)# <b>ipv6 nd inspection policy example_policy</b>	ND 検査ポリシー名を指定し、ND 検査ポリシー 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   switch}</b> 例： デバイス (config-nd-inspection)# <b>device-role switch</b>	ポートに接続されているデバイスの役割を指定します。デフォルトは <b>host</b> です。
ステップ 4	<b>limit address-count <i>value</i></b> 例： デバイス (config-nd-inspection)# <b>limit address-count 1000</b>	1 ~ 10,000 を入力します。
ステップ 5	<b>tracking {enable [reachable-lifetime {<i>value</i>   infinite}]   disable [stale-lifetime {<i>value</i>   infinite}]}</b> 例： デバイス (config-nd-inspection)# <b>tracking disable stale-lifetime infinite</b>	ポートのデフォルトのデバイス追跡ポリシーを上書きします。
ステップ 6	<b>trusted-port</b> 例： デバイス (config-nd-inspection)# <b>trusted-port</b>	信頼できるポートにするポートを設定します。



	コマンドまたはアクション	目的
ステップ 7	<b>validate source-mac</b> 例： デバイス(config-nd-inspection)# <b>validate source-mac</b>	送信元 Media Access Control (MAC) アドレスをリンク層アドレスと照合します。
ステップ 8	<b>no {device-role   limit address-count   tracking   trusted-port   validate source-mac}</b> 例： デバイス(config-nd-inspection)# <b>no validate source-mac</b>	このコマンドの <b>no</b> 形式を使用してパラメータの現在の設定を削除します。
ステップ 9	<b>default {device-role   limit address-count   tracking   trusted-port   validate source-mac}</b> 例： デバイス(config-nd-inspection)# <b>default limit address-count</b>	設定をデフォルト値に戻します。
ステップ 10	<b>do show ipv6 nd inspection policy policy_name</b> 例： デバイス(config-nd-inspection)# <b>do show ipv6 nd inspection policy example_policy</b>	ND 検査コンフィギュレーションモードを終了しないで ND 検査の設定を確認します。

## IPv6 ネイバー探索検査ポリシーをインターフェイスにアタッチする方法

インターフェイスまたはそのインターフェイス上の VLAN に IPv6 ND 検査ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

### 手順の概要

1. **configure terminal**
2. **interface** Interface\_type stack/module/port
3. **ipv6 nd inspection** [ **attach-policy** policy\_name [ **vlan** {vlan\_ids | **add** vlan\_ids | **except** vlan\_ids | **none** | **remove** vlan\_ids | **all**} ] | **vlan** [ {vlan\_ids | **add** vlan\_ids | **except** vlan\_ids | **none** | **remove** vlan\_ids | **all**} ] ]
4. **do show running-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： デバイス# <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。

	コマンドまたはアクション	目的
ステップ 2	<b>interface</b> <i>Interface_type stack/module/port</i> 例： デバイス(config)# <b>interface</b> <b>gigabitethernet</b> 1/1/4	インターフェイスのタイプおよび ID を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<b>ipv6 nd inspection</b> [ <b>attach-policy</b> <i>policy_name</i> [ <b>vlan</b> { <i>vlan_ids</i>   <b>add</b> <i>vlan_ids</i>   <b>except</b> <i>vlan_ids</i>   <b>none</b>   <b>remove</b> <i>vlan_ids</i>   <b>all</b> } ] ]   <b>vlan</b> [ { <i>vlan_ids</i>   <b>add</b> <i>vlan_ids</i>   <b>except</b> <i>vlan_ids</i>   <b>none</b>   <b>remove</b> <i>vlan_ids</i>   <b>all</b> } ] ] 例： デバイス(config-if)# <b>ipv6 nd inspection</b> <b>attach-policy</b> <b>example_policy</b>  or デバイス(config-if)# <b>ipv6 nd inspection</b> <b>attach-policy</b> <b>example_policy</b> <b>vlan</b> 222,223,224  or デバイス(config-if)# <b>ipv6 nd inspection</b> <b>vlan</b> 222,223,224	ネイバー探索検査ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。 <b>attach-policy</b> オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 4	<b>do show running-config</b> 例： デバイス#(config-if)# <b>do show running-config</b>	インターフェイス コンフィギュレーション モードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

## IPv6 ネイバー探索検査ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

EtherChannel インターフェイスまたは VLAN に IPv6 ネイバー探索検査ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

### 手順の概要

1. **configure terminal**
2. **interface range** *Interface\_name*
3. **ipv6 nd inspection** [ **attach-policy** *policy\_name* [ **vlan** {*vlan\_ids* | **add** *vlan\_ids* | **except** *vlan\_ids* | **none** | **remove** *vlan\_ids* | **all**} ] ] | **vlan** [ {*vlan\_ids* | **add** *vlan\_ids* | **except** *vlan\_ids* | **none** | **remove** *vlan\_ids* | **all**} ] ]
4. **do show running-config interface***portchannel\_interface\_name*

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： デバイス# <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>interface range</b> <i>Interface_name</i> 例： デバイス(config)# <b>interface Po11</b>	EtherChannel の作成時に割り当てられたポート チャネル インターフェイスの名前を指定します。インターフェイス範囲コンフィギュレーションモードを開始します。  ヒント インターフェイス名やタイプを簡単に参照するには <b>do show interfaces summary</b> コマンドを使用します。
ステップ 3	<b>ipv6 nd inspection</b> [ <b>attach-policy</b> <i>policy_name</i> [ <b>vlan</b> { <i>vlan_ids</i>   <b>add</b> <i>vlan_ids</i>   <b>except</b> <i>vlan_ids</i>   <b>none</b>   <b>remove</b> <i>vlan_ids</i>   <b>all</b> } ] ]   <b>vlan</b> [ { <i>vlan_ids</i>   <b>add</b> <i>vlan_ids</i>   <b>except</b> <i>vlan_ids</i>   <b>none</b>   <b>remove</b> <i>vlan_ids</i>   <b>all</b> } ] 例： デバイス(config-if-range)# <b>ipv6 nd inspection attach-policy example_policy</b>  or デバイス(config-if-range)# <b>ipv6 nd inspection attach-policy example_policy vlan 222,223,224</b>  or デバイス(config-if-range)# <b>ipv6 nd inspection vlan 222, 223,224</b>	ND 検査ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。 <b>attach-policy</b> オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 4	<b>do show running-config interface</b> <i>portchannel_interface_name</i> 例： デバイス#(config-if-range)# <b>do show running-config int po11</b>	コンフィギュレーションモードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

## IPv6 ネイバー探索検査ポリシーを全体的に VLAN にアタッチする方法

複数のインターフェイス上の VLAN に IPv6 ND 探索ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

## 手順の概要

1. `configure terminal`
2. `vlan configuration vlan_list`
3. `ipv6 nd inspection [ attach-policy policy_name]`
4. `do show running-config`

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： デバイス# <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>vlan configuration vlan_list</b> 例： デバイス(config)# <code>vlan configuration 334</code>	VLAN インターフェイスのコンフィギュレーション モードを開始し、IPv6 スヌーピング ポリシーをアタッチする VLAN を指定します。
ステップ 3	<b>ipv6 nd inspection [ attach-policy policy_name]</b> 例： デバイス(config-vlan-config)# <code>ipv6 nd inspection attach-policy example_policy</code>	すべてのスイッチおよびスタックインターフェイスで、IPv6 ネイバー探索ポリシーを指定した VLAN にアタッチします。 <b>attach-policy</b> オプションを使用しない場合、デフォルト ポリシーがアタッチされます。  デフォルトのポリシーは、 <code>device-role host</code> 、 <code>no drop-unsecure</code> 、 <code>limit address-count disabled</code> 、 <code>sec-level minimum is disabled</code> 、 <code>tracking is disabled</code> 、 <code>no trusted-port</code> 、 <code>no validate source-mac</code> です。
ステップ 4	<b>do show running-config</b> 例： デバイス#(config-if)# <code>do show running-config</code>	コンフィギュレーションモードを終了しないで、ポリシーが特定の VLAN にアタッチされていることを確認します。

## IPv6 ルータ アドバタイズメント ガード ポリシーの設定方法

IPv6 ルータ アドバタイズメント ポリシーを設定するには、特権 EXEC モードで次の手順を実行します。

## 手順の概要

1. `configure terminal`
2. `[no]ipv6 nd rguard policy policy-name`

3. `[no]device-role {host | monitor | router | switch}`
4. `[no]hop-limit {maximum | minimum} value`
5. `[no]managed-config-flag {off | on}`
6. `[no]match {ipv6 access-list list | ra prefix-list list}`
7. `[no]other-config-flag {on | off}`
8. `[no]router-preference maximum {high | medium | low}`
9. `[no]trusted-port`
10. `default {device-role | hop-limit {maximum | minimum} | managed-config-flag | match {ipv6 access-list | ra prefix-list } | other-config-flag | router-preference maximum | trusted-port}`
11. `do show ipv6 nd rguard policy policy_name`

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>configure terminal</code> 例： デバイス# <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	<code>[no]ipv6 nd rguard policy policy-name</code> 例： デバイス(config)# <code>ipv6 nd rguard policy example_policy</code>	RA ガード ポリシー名を指定し、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	<code>[no]device-role {host   monitor   router   switch}</code> 例： デバイス(config-nd-rguard)# <code>device-role switch</code>	ポートに接続されているデバイスの役割を指定します。デフォルトは <b>host</b> です。  (注) ホスト側ポートとルータ側ポートの両方を備えたネットワークでは、ホスト側ポートまたは VLAN で <b>device-role host</b> を設定した RA ガードポリシーとともに、RA ガード機能が適切に動作できるように、ルータ側のポートで <b>device-role router</b> を設定した RA ガードポリシーを設定することが必須です。
ステップ 4	<code>[no]hop-limit {maximum   minimum} value</code> 例： デバイス(config-nd-rguard)# <code>hop-limit maximum 33</code>	(1~255) 最大および最小のホップ制限値の範囲。 ホップ制限値によるルータアドバタイズメントメッセージのフィルタリングを有効にします。不正 RA メッセージは低いホップ制限値 (IPv4 の Time to Live と同じ) を持つ可能性があるため、ホストによって受け入れられると、ホストが不正 RA メッセージジェネレータを超えて宛先にトラフィックを生成することができなくなります。指定されていないホップ制限値を持つ RA メッセージはブロックされます。

	コマンドまたはアクション	目的
		設定されていない場合、このフィルタは無効になります。「 <b>minimum</b> 」を設定して、指定する値より低いホップ制限値を持つRAメッセージをブロックします。「 <b>maximum</b> 」を設定して、指定する値より高いホップ制限値を持つRAメッセージをブロックします。
ステップ 5	<code>[no]managed-config-flag {off   on}</code> 例： デバイス (config-nd-raguard) # <code>managed-config-flag on</code>	管理アドレス設定（「M」フラグ）フィールドに基づいてルータアドバタイズメントメッセージのフィルタリングを有効にします。「M」フィールドが1の不正 RA メッセージの結果としてホストが不正 DHCPv6 サーバーを使用する場合があります。設定されていない場合、このフィルタは無効になります。  <b>On</b> ：「M」値が1の RA メッセージを受け入れて転送し、0のものをブロックします。  <b>Off</b> ：「M」値が0の RA メッセージを受け入れて転送し、1のものをブロックします。
ステップ 6	<code>[no]match {ipv6 access-list list   ra prefix-list list}</code> 例： デバイス (config-nd-raguard) # <code>match ipv6 access-list example_list</code>	指定したプレフィックス リストまたはアクセス リストと照合します。
ステップ 7	<code>[no]other-config-flag {on   off}</code> 例： デバイス (config-nd-raguard) # <code>other-config-flag on</code>	その他の設定（「O」フラグ）フィールドに基づくルータアドバタイズメントメッセージのフィルタリングを有効にします。「O」フィールドが1の不正 RA メッセージの結果としてホストが不正 DHCPv6 サーバーを使用する場合があります。設定されていない場合、このフィルタは無効になります。  <b>On</b> ：「O」値が1の RA メッセージを受け入れて転送し、0のものをブロックします。  <b>Off</b> ：「O」値が0の RA メッセージを受け入れて転送し、1のものをブロックします。
ステップ 8	<code>[no]router-preference maximum {high   medium   low}</code> 例： デバイス (config-nd-raguard) # <code>router-preference maximum high</code>	「Router Preference」フラグを使用したルータアドバタイズメントメッセージのフィルタリングを有効にします。設定されていない場合、このフィルタは無効になります。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <b>high</b> : 「Router Preference」が「high」、 「medium」、または「low」に設定された RA メッセージを受け入れます。</li> <li>• <b>medium</b> : 「Router Preference」が「high」に設定された RA メッセージをブロックします。</li> <li>• <b>low</b> : 「Router Preference」が「medium」または「high」に設定された RA メッセージをブロックします。</li> </ul>
ステップ 9	<b>[no]trusted-port</b> 例 : デバイス (config-nd-raguard) # <b>trusted-port</b>	信頼できるポートとして設定すると、すべての接続デバイスが信頼され、より詳細なメッセージ検証は実行されません。
ステップ 10	<b>default {device-role   hop-limit {maximum   minimum}   managed-config-flag   match {ipv6 access-list   ra prefix-list }   other-config-flag   router-preference maximum   trusted-port}</b> 例 : デバイス (config-nd-raguard) # <b>default hop-limit</b>	コマンドをデフォルト値に戻します。
ステップ 11	<b>do show ipv6 nd raguard policy policy_name</b> 例 : デバイス (config-nd-raguard) # <b>do show ipv6 nd raguard policy example_policy</b>	(任意) : RA ガードポリシー コンフィギュレーション モードを終了しないで ND ガードポリシー設定を表示します。

## IPv6 ルータ アドバタイズメント ガード ポリシーをインターフェイスにアタッチする方法

インターフェイスまたはそのインターフェイス上の VLAN に IPv6 ルータ アドバタイズメントポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

### 手順の概要

1. **configure terminal**
2. **interface** Interface\_type stack/module/port
3. **ipv6 nd raguard [ attach-policy policy\_name [ vlan {vlan\_ids | add vlan\_ids | except vlan\_ids | none | remove vlan\_ids | all} ] | vlan [ {vlan\_ids | add vlan\_ids | exceptvlan\_ids | none | remove vlan\_ids | all} ] ]**
4. **do show running-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： デバイス# <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>interface</b> Interface_type <i>stack/module/port</i> 例： デバイス (config)# <code>interface gigabitethernet 1/1/4</code>	インターフェイスのタイプおよび ID を指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<b>ipv6 nd rguard</b> [ <b>attach-policy</b> <i>policy_name</i> [ <b>vlan</b> { <i>vlan_ids</i>   <b>add</b> <i>vlan_ids</i>   <b>except</b> <i>vlan_ids</i>   <b>none</b>   <b>remove</b> <i>vlan_ids</i>   <b>all</b> } ] ]   <b>vlan</b> [ { <i>vlan_ids</i>   <b>add</b> <i>vlan_ids</i>   <b>except</b> <i>vlan_ids</i>   <b>none</b>   <b>remove</b> <i>vlan_ids</i>   <b>all</b> } ] 例： デバイス (config-if)# <code>ipv6 nd rguard attach-policy example_policy</code> or デバイス (config-if)# <code>ipv6 nd rguard attach-policy example_policy vlan 222,223,224</code> or デバイス (config-if)# <code>ipv6 nd rguard vlan 222,223,224</code>	ネイバー探索検査ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。 <b>attach-policy</b> オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 4	<b>do show running-config</b> 例： デバイス# (config-if)# <code>do show running-config</code>	コンフィギュレーションモードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

## IPv6 ルータ アドバタイズメント ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

EtherChannel インターフェイスまたは VLAN に IPv6 ルータ アドバタイズメント ガード ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

## 手順の概要

1. **configure terminal**
2. **interface range** *Interface\_name*



3. `ipv6 nd rguard [ attach-policy policy_name [ vlan {vlan_ids | add vlan_ids | except vlan_ids | none | remove vlan_ids | all} ] | vlan [ {vlan_ids | add vlan_ids | exceptvlan_ids | none | remove vlan_ids | all} ] ]`
4. `do show running-config interfaceportchannel_interface_name`

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： デバイス# <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>interface range Interface_name</b> 例： デバイス(config)# <code>interface Po11</code>	EtherChannel の作成時に割り当てられたポート チャネル インターフェイスの名前を指定します。インターフェイス範囲コンフィギュレーションモードを開始します。  ヒント インターフェイス名やタイプを簡単に参照するには <b>do show interfaces summary</b> コマンドを使用します。
ステップ 3	<b>ipv6 nd rguard [ attach-policy policy_name [ vlan {vlan_ids   add vlan_ids   except vlan_ids   none   remove vlan_ids   all} ]   vlan [ {vlan_ids   add vlan_ids   exceptvlan_ids   none   remove vlan_ids   all} ] ]</b> 例： デバイス(config-if-range)# <code>ipv6 nd rguard attach-policy example_policy</code> or デバイス(config-if-range)# <code>ipv6 nd rguard attach-policy example_policy vlan 222,223,224</code> or デバイス(config-if-range)# <code>ipv6 nd rguard vlan 222,223,224</code>	RA ガード ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。 <b>attach-policy</b> オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 4	<b>do show running-config interfaceportchannel_interface_name</b> 例： デバイス#(config-if-range)# <code>do show running-config int po11</code>	コンフィギュレーションモードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

## IPv6 ルータ アドバタイズメント ガード ポリシーを VLAN にグローバルにアタッチする方法

インターフェイスに関係なく VLAN に IPv6 ルータ アドバタイズメント ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

### 手順の概要

1. `configure terminal`
2. `vlan configuration vlan_list`
3. `ipv6 dhcp guard [ attach-policy policy_name]`
4. `do show running-config`

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<code>configure terminal</code> 例： デバイス# <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	<code>vlan configuration vlan_list</code> 例： デバイス(config)# <code>vlan configuration 335</code>	VLAN インターフェイスのコンフィギュレーション モードを開始し、IPv6 RA ガード ポリシーをアタッチする VLAN を指定します。
ステップ 3	<code>ipv6 dhcp guard [ attach-policy policy_name]</code> 例： デバイス(config-vlan-config)# <code>ipv6 nd rguard attach-policy example_policy</code>	すべてのスイッチおよびスタックインターフェイスで、IPv6 RA ガード ポリシーを指定した VLAN にアタッチします。 <b>attach-policy</b> オプションを使用しない場合、デフォルトポリシーがアタッチされます。
ステップ 4	<code>do show running-config</code> 例： デバイス#(config-if)# <code>do show running-config</code>	コンフィギュレーションモードを終了しないで、ポリシーが特定の VLAN にアタッチされていることを確認します。

## IPv6 DHCP ガード ポリシーの設定方法

IPv6 DHCP (DHCPv6) ガード ポリシーを設定するには、特権 EXEC モードで次の手順を実行します。

### 手順の概要

1. `configure terminal`
2. `[no]ipv6 dhcp guard policy policy-name`

3. `[no]device-role {client | server}`
4. `[no] match server access-list ipv6-access-list-name`
5. `[no] match reply prefix-list ipv6-prefix-list-name`
6. `[no]preference { max limit | min limit }`
7. `[no] trusted-port`
8. `default {device-role | trusted-port}`
9. `do show ipv6 dhcp guard policy policy_name`

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： デバイス# <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>[no]ipv6 dhcp guard policy policy-name</b> 例： デバイス(config)# <code>ipv6 dhcp guard policy example_policy</code>	DHCPv6 ガード ポリシー名を指定し、DHCPv6 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>[no]device-role {client   server}</b> 例： デバイス(config-dhcp-guard)# <code>device-role server</code>	(任意) 特定の役割のデバイスからのものではないポート上の DHCPv6 応答および DHCPv6 アドバタイズメントをフィルタします。デフォルトは <b>client</b> です。 <ul style="list-style-type: none"> <li>• <b>client</b> : デフォルト値。アタッチされたデバイスがクライアントであることを指定します。サーバー メッセージにはこのポートで破棄されます。</li> <li>• <b>server</b> : 適用されたデバイスが DHCPv6 サーバーであることを指定します。このポートでは、サーバー メッセージが許可されます。</li> </ul>
ステップ 4	<b>[no] match server access-list ipv6-access-list-name</b> 例： <pre>;;Assume a preconfigured IPv6 Access List as follows: デバイス(config)# <code>ipv6 access-list my_acls</code> デバイス(config-ipv6-acl)# <code>permit host FE80::A8BB:CCFF:FE01:F700 any</code>  ;;configure DHCPv6 Guard to match approved access list. デバイス(config-dhcp-guard)# <code>match server access-list my_acls</code></pre>	(任意)。アドバタイズされた DHCPv6 サーバーまたはリレーアドレスが認証されたサーバーのアクセスリストからのものであることの確認を有効にします (アクセスリストの宛先アドレスは「any」です)。設定されていない場合、このチェックは回避されます。空のアクセスリストは、 <code>permit all</code> として処理されます。

	コマンドまたはアクション	目的
ステップ 5	<p><b>[no] match reply prefix-list <i>ipv6-prefix-list-name</i></b></p> <p>例 :</p> <pre>;;Assume a preconfigured IPv6 prefix list as follows: デバイス(config)# ipv6 prefix-list my_prefix permit 2001:0DB8::/64 le 128  ;; Configure DHCPv6 Guard to match prefix デバイス(config-dhcp-guard)# match reply prefix-list my_prefix</pre>	<p>(任意) DHCPv6 応答メッセージ内のアドバタイズされたプレフィックスが設定された承認プレフィックスリストからのものであることの確認を有効にします。設定されていない場合、このチェックは回避されます。空のプレフィックスリストは、<b>permit</b>として処理されます。</p>
ステップ 6	<p><b>[no]preference { max limit   min limit }</b></p> <p>例 :</p> <pre>デバイス(config-dhcp-guard)# preference max 250 デバイス(config-dhcp-guard)#preference min 150</pre>	<p><b>device-role</b> が <b>server</b> である場合に <b>max</b> および <b>min</b> を設定して、DHCPv6 サーバーアドバタイズメント値をサーバー優先度値に基づいてフィルタします。デフォルトではすべてのアドバタイズメントが許可されます。</p> <p><b>max limit</b> : (0～255) (任意) アドバタイズされたプリファレンス ([<b>preference</b>] 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有効にします。デフォルトは 255 です。設定されていない場合、このチェックは回避されます。</p> <p><b>min limit</b> : (0～255) (任意) アドバタイズされたプリファレンス ([<b>preference</b>] 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有効にします。デフォルトは 0 です。設定されていない場合、このチェックは回避されます。</p>
ステップ 7	<p><b>[no] trusted-port</b></p> <p>例 :</p> <pre>デバイス(config-dhcp-guard)# trusted-port</pre>	<p>(任意) <b>trusted-port</b> : ポートを信頼モードに設定します。このポートでは、これ以上のポリシングは実行されません。</p> <p>(注) 信頼できるポートを設定した場合、<b>device-role</b> オプションは使用できません。</p>
ステップ 8	<p><b>default {device-role   trusted-port}</b></p> <p>例 :</p> <pre>デバイス(config-dhcp-guard)# default device-role</pre>	<p>(任意) <b>default</b> : コマンドをデフォルトに設定します。</p>
ステップ 9	<p><b>do show ipv6 dhcp guard policy <i>policy_name</i></b></p> <p>例 :</p> <pre>デバイス(config-dhcp-guard)# do show ipv6 dhcp guard policy example_policy</pre>	<p>(任意) コンフィギュレーションサブモードを終了せずに IPv6 DHCP のガードポリシーの設定を表示します。<b>policy_name</b> 変数を省略すると、すべての DHCPv6 ポリシーが表示されます。</p>

**DHCPv6 ガード設定の例**

```
enable
configure terminal
ipv6 access-list acl1
  permit host FE80::A8BB:CCFF:FE01:F700 any
ipv6 prefix-list abc permit 2001:0DB8::/64 le 128
ipv6 dhcp guard policy poll
  device-role server
  match server access-list acl1
  match reply prefix-list abc
  preference min 0
  preference max 255
  trusted-port
interface GigabitEthernet 0/2/0
  switchport
  ipv6 dhcp guard attach-policy poll vlan add 1
  vlan 1
  ipv6 dhcp guard attach-policy poll
show ipv6 dhcp guard policy poll
```

**IPv6 DHCP ガード ポリシーをインターフェイスまたはインターフェイス上の VLAN にアタッチする方法**

IPv6 バインディング テーブル コンテンツを設定するには、特権 EXEC モードで次の手順を実行します。

## 手順の概要

1. **configure terminal**
2. **interface** Interface\_type stack/module/port
3. **ipv6 dhcp guard** [ **attach-policy** policy\_name [ **vlan** {vlan\_ids | **add** vlan\_ids | **except** vlan\_ids | **none** | **remove** vlan\_ids | **all**} ] | **vlan** [ {vlan\_ids | **add** vlan\_ids | **except** vlan\_ids | **none** | **remove** vlan\_ids | **all**} ]
4. **do show running-config interface** Interface\_type stack/module/port

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： デバイス# <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>interface</b> Interface_type stack/module/port 例： デバイス(config)# <b>interface gigabitethernet 1/1/4</b>	インターフェイスのタイプおよび ID 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。

	コマンドまたはアクション	目的
ステップ 3	<p><b>ipv6 dhcp guard [ attach-policy <i>policy_name</i> [ vlan {<i>vlan_ids</i>   add <i>vlan_ids</i>   except <i>vlan_ids</i>   none   remove <i>vlan_ids</i>   all} ]   vlan [ {<i>vlan_ids</i>   add <i>vlan_ids</i>   except <i>vlan_ids</i>   none   remove <i>vlan_ids</i>   all} ]</b></p> <p>例 :</p> <pre>デバイス(config-if)# ipv6 dhcp guard attach-policy example_policy</pre> <p>or</p> <pre>デバイス(config-if)# ipv6 dhcp guard attach-policy example_policy vlan 222,223,224</pre> <p>or</p> <pre>デバイス(config-if)# ipv6 dhcp guard vlan 222, 223,224</pre>	DHCP ガードポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。 <b>attach-policy</b> オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 4	<p><b>do show running-config interface <i>Interface_type stack/module/port</i></b></p> <p>例 :</p> <pre>デバイス#(config-if)# do show running-config gig 1/1/4</pre>	コンフィギュレーションモードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

## IPv6 DHCP ガードポリシーをレイヤ2 EtherChannel インターフェイスにアタッチする方法

EtherChannel インターフェイスまたは VLAN に IPv6 DHCP ガードポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

### 手順の概要

1. **configure terminal**
2. **interface range *Interface\_name***
3. **ipv6 dhcp guard [ attach-policy *policy\_name* [ vlan {*vlan\_ids* | add *vlan\_ids* | except *vlan\_ids* | none | remove *vlan\_ids* | all} ] | vlan [ {*vlan\_ids* | add *vlan\_ids* | except *vlan\_ids* | none | remove *vlan\_ids* | all} ]**
4. **do show running-config interface *portchannel\_interface\_name***

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<p><b>configure terminal</b></p> <p>例 :</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。

	コマンドまたはアクション	目的
	デバイス# <code>configure terminal</code>	
ステップ 2	<b>interface range</b> <i>Interface_name</i> 例 : デバイス(config)# <code>interface Po11</code>	EtherChannel の作成時に割り当てられたポート チャネル インターフェイスの名前を指定します。インターフェイス範囲コンフィギュレーションモードを開始します。  ヒント インターフェイス名やタイプを簡単に参照するには <b>do show interfaces summary</b> コマンドを使用します。
ステップ 3	<b>ipv6 dhcp guard</b> [ <b>attach-policy</b> <i>policy_name</i> [ <b>vlan</b> { <i>vlan_ids</i>   <b>add</b> <i>vlan_ids</i>   <b>except</b> <i>vlan_ids</i>   <b>none</b>   <b>remove</b> <i>vlan_ids</i>   <b>all</b> } ] ] <b>vlan</b> [ { <i>vlan_ids</i>   <b>add</b> <i>vlan_ids</i>   <b>except</b> <i>vlan_ids</i>   <b>none</b>   <b>remove</b> <i>vlan_ids</i>   <b>all</b> } ] 例 : デバイス(config-if-range)# <code>ipv6 dhcp guard attach-policy example_policy</code> or デバイス(config-if-range)# <code>ipv6 dhcp guard attach-policy example_policy vlan 222,223,224</code> or デバイス(config-if-range)# <code>ipv6 dhcp guard vlan 222,223,224</code>	DHCP ガードポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。 <b>attach-policy</b> オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 4	<b>do show running-config interface</b> <i>portchannel_interface_name</i> 例 : デバイス#(config-if-range)# <code>do show running-config int po11</code>	コンフィギュレーションモードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

## IPv6 DHCP ガード ポリシーを全体的に VLAN にアタッチする方法

複数のインターフェイス上の VLAN に IPv6 DHCP のガード ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

### 手順の概要

1. `configure terminal`
2. `vlan configuration` *vlan\_list*
3. `ipv6 dhcp guard` [ `attach-policy` *policy\_name* ]
4. `do show running-config`

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： デバイス# <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>vlan configuration</b> <i>vlan_list</i> 例： デバイス(config)# <code>vlan configuration 334</code>	VLAN インターフェイスのコンフィギュレーション モードを開始し、IPv6 スヌーピング ポリシーをアタッチする VLAN を指定します。
ステップ 3	<b>ipv6 dhcp guard</b> [ <b>attach-policy</b> <i>policy_name</i> ] 例： デバイス(config-vlan-config)# <code>ipv6 dhcp guard attach-policy example_policy</code>	すべてのスイッチおよびスタック インターフェイスで、IPv6 ネイバー探索ポリシーを指定した VLAN にアタッチします。 <b>attach-policy</b> オプションを使用しない場合、デフォルト ポリシーがアタッチされます。デフォルト ポリシーは、device-role <b>client</b> 、 <b>no trusted-port</b> です。
ステップ 4	<b>do show running-config</b> 例： デバイス#(config-if)# <code>do show running-config</code>	コンフィギュレーション モードを終了しないで、ポリシーが特定の VLAN にアタッチされていることを確認します。

## IPv6 ソース ガードの設定方法

## 手順の概要

1. `enable`
2. `configure terminal`
3. `[no] ipv6 source-guard policy policy_name`
4. `[deny global-autoconf] [permit link-local] [default{...}] [exit] [no{...}]`
5. `end`
6. `show ipv6 source-guard policy policy_name`

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： デバイス> <code>enable</code>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。



	コマンドまたはアクション	目的
ステップ 2	<b>configure terminal</b> 例： デバイス# <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 3	<b>[no] ipv6 source-guard policy policy_name</b> 例： デバイス(config)# <b>ipv6 source-guard policy example_policy</b>	IPv6 ソース ガード ポリシー名を指定し、IPv6 ソース 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 4	<b>[deny global-autoconf] [permit link-local] [default{...}] [exit] [no{...}]</b> 例： デバイス(config-sisf-sourceguard)# <b>deny global-autoconf</b>	(任意) IPv6 ソース ガード ポリシーを定義します。  <ul style="list-style-type: none"> <li>• <b>deny global-autoconf</b> : 自動設定されたグローバルアドレスからのデータ トラフィックを拒否します。これは、リンク上のすべてのグローバルアドレスが DHCP によって割り当てられている際に、管理者が、自己設定されたアドレスを持つホストによるトラフィックの送信をブロックしたい場合に役立ちます。</li> <li>• <b>permit link-local</b> : リンクローカルアドレスから送信されたすべてのデータ トラフィックを許可します。</li> </ul> (注) ソース ガード ポリシーでは <b>trusted</b> オプションはサポートされません。
ステップ 5	<b>end</b> 例： デバイス(config-sisf-sourceguard)# <b>end</b>	IPv6 ソース ガード ポリシー コンフィギュレーション モードを終了します。
ステップ 6	<b>show ipv6 source-guard policy policy_name</b> 例： デバイス# <b>show ipv6 source-guard policy example_policy</b>	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。

### 次のタスク

インターフェイスに IPv6 ソース ガード ポリシーを適用します。

## IPv6 ソース ガード ポリシーをインターフェイスにアタッチする方法

### 手順の概要

#### 1. enable

2. **configure terminal**
3. **interface** Interface\_type *stack/module/port*
4. **ipv6 source-guard** [**attach-policy** <policy\_name> ]
5. **show ipv6 source-guard policy** policy\_name

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： デバイス> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： デバイス# <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 3	<b>interface</b> Interface_type <i>stack/module/port</i> 例： デバイス (config)# <b>interface gigabitethernet 1/1/4</b>	インターフェイスのタイプおよび ID 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>ipv6 source-guard</b> [ <b>attach-policy</b> <policy_name> ] 例： デバイス (config-if)# <b>ipv6 source-guard attach-policy example_policy</b>	インターフェイスに IPv6 ソース ガード ポリシーをアタッチします。 <b>attach-policy</b> オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 5	<b>show ipv6 source-guard policy</b> policy_name 例： デバイス# (config-if)# <b>show ipv6 source-guard policy example_policy</b>	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 ソース ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

## 手順の概要

1. **enable**
2. **configure terminal**
3. **interface** port-channel *port-channel-number*
4. **ipv6 source-guard** [**attach-policy** <policy\_name> ]
5. **show ipv6 source-guard policy** policy\_name

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： Device# <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 3	<b>interface port-channel</b> <i>port-channel-number</i> 例： Device (config)# <b>interface Po4</b>	インターフェイスのタイプとポート番号を指定し、スイッチをポート チャネル コンフィギュレーション モードにします。
ステップ 4	<b>ipv6 source-guard</b> [ <b>attach-policy</b> < <i>policy_name</i> > ] 例： Device(config-if) # <b>ipv6 source-guard attach-policy example_policy</b>	インターフェイスに IPv6 ソース ガード ポリシーをアタッチします。 <b>attach-policy</b> オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 5	<b>show ipv6 source-guard policy</b> <i>policy_name</i> 例： Device(config-if) # <b>show ipv6 source-guard policy example_policy</b>	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 プレフィックス ガードの設定方法



- (注) プレフィックス ガードが適用されている場合にリンクローカルアドレスから送信されたルーティングプロトコル制御パケットを許可するには、ソースガードポリシー コンフィギュレーション モードで **permit link-local** コマンドを有効にします。

## 手順の概要

1. **enable**
2. **configure terminal**
3. [**no**] **ipv6 source-guard policy** *source-guard-policy*
4. [**no**] **validate address**
5. **validate prefix**
6. **exit**
7. **show ipv6 source-guard policy** [*source-guard-policy*]

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： Device# <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 3	<b>[no] ipv6 source-guard policy source-guard-policy</b> 例： Device(config)# <b>ipv6 source-guard policy my_snooping_policy</b>	IPv6 ソースガードポリシー名を定義して、スイッチ統合セキュリティ機能のソースガードポリシー コンフィギュレーション モードを開始します。
ステップ 4	<b>[ no ] validate address</b> 例： Device(config-sisf-sourceguard)# <b>no validate address</b>	アドレス検証機能を無効にし、IPv6 プレフィックスガード機能を設定できるようにします。
ステップ 5	<b>validate prefix</b> 例： Device(config-sisf-sourceguard)# <b>validate prefix</b>	IPv6 プレフィックスガード動作を実行するよう、IPv6 ソースガードを有効にします。
ステップ 6	<b>exit</b> 例： Device(config-sisf-sourceguard)# <b>exit</b>	スイッチ統合セキュリティ機能のソースガードポリシー コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 7	<b>show ipv6 source-guard policy [source-guard-policy]</b> 例： Device# <b>show ipv6 source-guard policy policy1</b>	IPv6 ソースガードポリシー設定を表示します。

## IPv6 プレフィックスガードポリシーをインターフェイスにアタッチする方法

## 手順の概要

1. **enable**
2. **configure terminal**
3. **interface** Interface\_type *stack/module/port*

4. `ipv6 source-guard attach-policy policy_name`
5. `show ipv6 source-guard policy policy_name`

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  デバイス> <code>enable</code>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  デバイス# <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 3	<b>interface Interface_type stack/module/port</b> 例：  デバイス(config)# <code>interface gigabitethernet 1/1/4</code>	インターフェイスのタイプおよび ID 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>ipv6 source-guard attach-policy policy_name</b> 例：  デバイス(config-if)# <code>ipv6 source-guard attach-policy example_policy</code>	インターフェイスに IPv6 ソース ガード ポリシーをアタッチします。 <b>attach-policy</b> オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 5	<b>show ipv6 source-guard policy policy_name</b> 例：  デバイス(config-if)# <code>show ipv6 source-guard policy example_policy</code>	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 プレフィックス ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

## 手順の概要

1. `enable`
2. `configure terminal`
3. `interface port-channel port-channel-number`
4. `ipv6 source-guard [attach-policy <policy_name> ]`
5. `show ipv6 source-guard policy policy_name`

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： Device# <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 3	<b>interface port-channel port-channel-number</b> 例： Device (config)# <b>interface Po4</b>	インターフェイスのタイプとポート番号を指定し、スイッチをポート チャネル コンフィギュレーション モードにします。
ステップ 4	<b>ipv6 source-guard [attach-policy &lt;policy_name&gt; ]</b> 例： Device(config-if)# <b>ipv6 source-guard attach-policy example_policy</b>	インターフェイスに IPv6 ソース ガード ポリシーをアタッチします。 <b>attach-policy</b> オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 5	<b>show ipv6 source-guard policy policy_name</b> 例： Device(config-if)# <b>show ipv6 source-guard policy example_policy</b>	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 ファースト ホップ セキュリティの設定例

## 例：IPv6 ソース ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

次の例は、IPv6 ソース ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法を示しています。

```
Switch# configure terminal
Switch(config)# ipv6 source-guard policy POL
Switch(config-sisf-sourceguard) # validate address
switch(config-sisf-sourceguard)# exit
Switch(config)# interface Po4
Switch(config)# ipv6 snooping
Switch(config-if)# ipv6 source-guard attach-policy POL
Switch(config-if)# exit
switch(config)#
```

## 例：IPv6 プレフィックス ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

次の例は、IPv6 プレフィックス ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法を示しています。

```
Switch# configure terminal
Switch(config)# ipv6 source-guard policy POL
Switch (config-sisf-sourceguard)# no validate address
Switch((config-sisf-sourceguard)# validate prefix
Switch(config)# interface Po4
Switch(config-if)# ipv6 snooping
Switch(config-if)# ipv6 source-guard attach-policy POL
```

## IPv6 ファースト ホップ セキュリティの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	IPv6 ファースト ホップ セキュリティ	<p>IPv6 のファースト ホップ セキュリティは、ポリシーを物理インターフェイス、EtherChannel インターフェイス、または VLAN に適用できる一連の IPv6 セキュリティ機能です。IPv6 ソフトウェア ポリシー データベースサービスは、これらのポリシーを保存しアクセスします。ポリシーを設定または変更すると、ポリシー属性はソフトウェアポリシー データベースに保存または更新され、その後指定したとおりに適用されます。</p> <p>IPv6 スヌーピングポリシー機能は廃止されました。コマンドは CLI に表示され、設定できますが、代わりにスイッチ統合セキュリティ機能 (SISF) ベースのデバイス追跡機能を使用することを推奨します。</p>

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。







## 第 23 章

# SISF ベースのデバイストラッキングの設定

- SISF ベースのデバイストラッキングに関する情報 (491 ページ)
- SISF ベースのデバイストラッキングの設定方法 (495 ページ)
- SISF ベースのデバイストラッキングの設定例 (505 ページ)
- SISF の機能履歴 (510 ページ)

## SISF ベースのデバイストラッキングに関する情報

### SISF ベースのデバイストラッキングの概要

スイッチ統合セキュリティ機能ベース (SISF ベース) のデバイストラッキング機能は、一連のファーストホップセキュリティ機能の一部です。

この機能の主な役割は、ネットワーク内のエンドノードの存在、ロケーション、移動を追跡することです。SISF は、スイッチが受信したトラフィックをスヌーピングし、デバイスアイデンティティ (MAC と IP アドレス) を抽出して、バインディングテーブルに保存します。IEEE 802.1X、web 認証、Cisco TrustSec、LISP などの多くの機能は、この情報の正確性に依存して正常に動作します。

SISF ベースのデバイストラッキングは、IPv4 と IPv6 の両方をサポートします。

SISF ベースのデバイストラッキングが導入されても、レガシーデバイストラッキング CLI (IP デバイストラッキング (IPDT) および IPv6 スヌーピング CLI) は引き続き使用できます。スイッチをブートアップすると、使用可能なコマンドのセットは既存の設定によって異なり、次のいずれかのみが使用可能です。

- SISF ベースのデバイストラッキング CLI、または
- IPDT および IPv6 スヌーピング CLI



(注) IPDT および IPv6 スヌーピングコマンドは廃止されましたが、引き続き使用できます。SISF ベースのデバイストラッキングにアップグレードすることを推奨します。

IPDT および IPv6 スヌーピング CLI を使用していて、SISF ベースのデバイストラッキングに移行する場合、詳細については「レガシー IPDT と IPv6 スヌーピングから SISF ベースのデバイストラッキングへの移行」を参照してください。

SISF ベースのデバイストラッキングは、手動で (**device-tracking** コマンドを使用して)、またはプログラムで (デバイス トラッキング サービスを他の機能に提供する場合に) 有効にできます。

## SISF ベースのデバイストラッキングを有効にするオプション

デフォルトでは、SISF ベースのデバイストラッキングは無効になっています。

これを有効にするには、デバイストラッキングポリシーを定義し、そのポリシーを特定のターゲットに適用します。



(注) ターゲットは、インターフェイスまたは VLAN です。

### SISF ベースのデバイストラッキングの手動による有効化

- **オプション 1** : **default** デバイス トラッキング ポリシーをターゲットに適用します。

インターフェイス コンフィギュレーション モードまたは VLAN コンフィギュレーション モードで、**device-tracking** コマンドを入力します。次に、システムは **default** ポリシーをインターフェイスまたは VLAN に適用します。



(注) **default** ポリシーは、デフォルト設定の組み込みポリシーです。**default** ポリシーの属性は変更できません。デバイストラッキングポリシーの属性を設定できるようにするには、カスタムポリシーを作成する必要があります。「オプション 2 : カスタム設定でカスタムポリシーを作成します」を参照してください。

- **オプション 2** : カスタム設定でカスタムポリシーを作成します。

グローバル コンフィギュレーション モードで **device-tracking policy** コマンドを入力し、続けてカスタムポリシー名を入力します。システムにより、指定した名前のポリシーが作成されます。その後、デバイストラッキング コンフィギュレーション モード (**config-device-tracking**) で使用可能な設定を行い、指定したターゲットにポリシーを適用できます。

### プログラムによる SISF ベースのデバイストラッキングの有効化

一部の機能はデバイストラッキングに依存し、SISF ベースのデバイストラッキングが構築および維持するバインディングエントリの信頼性のあるデータベースを利用します。これらの機能

は、デバイストラッキングクライアントとも呼ばれ、プログラムによりデバイストラッキングを有効にします（デバイストラッキングポリシーを作成して適用します）。



- (注) ここでの例外は、IEEE 802.1X、web 認証、Cisco TrustSec、IP ソースガード (IPSG) です。これらもデバイストラッキングに依存しますが、有効にはしません。これらのデバイストラッキングクライアントでは、**ip dhcp snooping vlan vlan** コマンドを入力して、プログラムにより特定のターゲットでデバイストラッキングを有効にする必要があります。

プログラムによる SISF ベースのデバイストラッキングの有効化については、次の点に注意してください。

- デバイストラッキングクライアントでは、デバイストラッキングを有効にする必要があります。

複数のデバイストラッキングクライアントが存在するため、複数のプログラムポリシーを作成できます。各ポリシーの設定は、ポリシーを作成するデバイストラッキングクライアントによって異なります。

- 作成されるポリシーとその設定はシステム定義です。

設定可能なポリシー属性は、デバイストラッキングコンフィギュレーションモード (**config-device-tracking**) で使用でき、リリースごとに異なります。設定不可能な属性を変更しようとする、設定変更は拒否され、エラーメッセージが表示されます。

プログラムで作成されたポリシーの詳細については、[Cisco IOS XE Fuji 16.9.x 以降のリリースでの SISF ベースのデバイストラッキングのプログラムによる有効化 \(502 ページ\)](#) を参照してください。

## レガシー IPDT と IPv6 スヌーピングから SISF ベースのデバイストラッキングへの移行

デバイスにあるレガシー設定に基づいて、**device-tracking upgrade-cli** コマンドは CLI を異なる方法でアップグレードします。既存の設定を移行する前に、次の設定シナリオ、および対応する移行結果を検討します。



- (注) 古い IPDT と IPv6 スヌーピング CLI を SISF ベースのデバイストラッキング CLI と併用することはできません。

### IPDT 設定のみが存在する

デバイスに IPDT 設定のみがある場合は、**device-tracking upgrade-cli** コマンドを実行すると、設定が変換され、新しく作成されてインターフェイスで適用される SISF ポリシーが使用されます。これにより、この SISF ポリシーを更新できます。

引き続きレガシーコマンドを使用する場合、レガシーモードでの操作に制限されます。このモードでは、レガシー IPDT と IPv6 スヌーピングコマンドのみがデバイスで使用可能になります。

### IPv6 スヌーピング設定のみが存在する

既存の IPv6 スヌーピング設定があるデバイスで、古い IPv6 スヌーピングコマンドを以降の設定に使用できます。次のオプションを使用できます。

- (推奨) **device-tracking upgrade-cli** コマンドを使用して、レガシー設定をすべて、新しい SISF ベースのデバイストラッキング コマンドに変換します。変換後は、新しいデバイストラッキング コマンドのみがデバイスで動作します。
- レガシー IPv6 スヌーピングコマンドを今後の設定に使用し、**device-tracking upgrade-cli** コマンドは実行しません。このオプションでは、デバイスで使用可能なのはレガシー IPv6 スヌーピングコマンドのみであり、新しい SISF ベースのデバイストラッキング CLI コマンドは使用できません。

### IPDT と IPv6 スヌーピングの両方の設定が存在する

レガシー IPDT 設定と IPv6 スヌーピング設定の両方が存在するデバイスでは、レガシーコマンドを SISF ベースのデバイストラッキング CLI コマンドに変換できます。ただし、インターフェイスに適用することができるスヌーピングポリシーは 1 つだけであり、IPv6 スヌーピング ポリシー パラメータは IPDT 設定よりも優先される、ということに注意してください。



- (注) 新しい SISF ベースのコマンドに移行しておらず、レガシー IPv6 スヌーピングや IPDT コマンドを使用し続けている場合、IPv4 デバイストラッキング設定情報が IPv6 スヌーピングコマンドに表示される可能性があります。SISF ベースのデバイストラッキング機能では、IPv4 と IPv6 の両方の設定を扱うためです。これを回避するには、レガシー設定を SISF ベースのデバイストラッキング コマンドに変換することを推奨します。

### IPDT または IPv6 スヌーピング設定が存在しない

デバイスにレガシー IP デバイストラッキング設定も IPv6 スヌーピング設定もない場合は、今後の設定に使用できるのは新しい SISF ベースのデバイストラッキング コマンドのみです。レガシー IPDT コマンドと IPv6 スヌーピングコマンドは使用できません。

# SISF ベースのデバイストラッキングの設定方法

## SISF ベースのデバイストラッキングの手動による有効化

### ターゲットへのデフォルト デバイス トラッキング ポリシーの適用

デフォルトのデバイス トラッキング ポリシーをインターフェイスまたは VLAN に適用するには、特権 EXEC モードで次の手順を実行します。

#### 手順の概要

1. **configure terminal**
2. インターフェイスまたは VLAN を指定します。
  - **interface** *interface*
  - **vlan configuration** *vlan\_list*
3. **device-tracking**
4. **exit**
5. **show device-tracking policy** *policy-name*

#### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： Device# <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	インターフェイスまたは VLAN を指定します。  • <b>interface</b> <i>interface</i> • <b>vlan configuration</b> <i>vlan_list</i>  例： Device(config)# <b>interface gigabitethernet 1/1/4</b> OR Device(config)# <b>vlan configuration 333</b>	<b>interface</b> <i>type number</i> —Specifies the interface and enters the interface configuration mode. デバイス トラッキングポリシーは、指定されたインターフェイスに適用されます。  <b>vlan configuration</b> <i>vlan_list</i> : VLAN を指定し、VLAN 機能コンフィギュレーションモードを開始します。デバイス トラッキングポリシーは、指定された VLAN に適用されます。
ステップ 3	<b>device-tracking</b> 例： Device(config-if)# <b>device-tracking</b> OR Device(config-vlan-config)# <b>device-tracking</b>	SISF ベースのデバイストラッキングを有効にし、デフォルトポリシーをインターフェイスまたは VLAN に適用します。  デフォルトポリシーは、デフォルト設定の組み込みポリシーです。デフォルトポリシーの属性は変更できません。

	コマンドまたはアクション	目的
ステップ 4	<b>exit</b> 例： Device(config-if)# <b>exit</b> OR Device(config-vlan-config)# <b>exit</b>	設定モードを終了します。
ステップ 5	<b>show device-tracking policy policy-name</b> 例： Device# <b>show device-tracking policy default</b>	デバイストラッキングポリシーの設定と、それが適用されるすべてのターゲットを表示します。

## カスタム設定を使用したカスタム デバイストラッキング ポリシーの作成

デバイストラッキングポリシーを作成して設定するには、特権 EXEC モードで次の手順を実行します。

### 手順の概要

1. **configure terminal**
2. **[no] device-tracking policy policy-name**
3. **[data-glean | default | destination-glean | device-role | distribution-switch | exit | limit | no | prefix-glean | protocol | security-level | tracking | trusted-port | vpc]**
4. **end**
5. **show device-tracking policy policy-name**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： Device# <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] device-tracking policy policy-name</b> 例： Device(config)# <b>device-tracking policy example_policy</b>	ポリシーを作成し、デバイストラッキング 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>[data-glean   default   destination-glean   device-role   distribution-switch   exit   limit   no   prefix-glean   protocol   security-level   tracking   trusted-port   vpc]</b> 例： Device (config-device-tracking)# <b>destination-glean log-only</b>	システムプロンプトに疑問符 (?) を入力すると、このモードで使用できるオプションのリストが表示されます。IPv4 と IPv6 の両方に対して以下を設定できます。 <ul style="list-style-type: none"> <li>• (任意) <b>data-glean</b> : ネットワーク内の送信元からスヌーピングされたデータパケットからのアドレスの学習を有効にし、データトラフィックの送信元アドレスとともにバインディング</li> </ul>

	コマンドまたはアクション	目的
		<p>テーブルを読み込みます。次のいずれかのオプションを入力します。</p> <ul style="list-style-type: none"> <li>• <b>log-only</b> : データパケット通知時に syslog メッセージを生成します。</li> <li>• <b>recovery</b> : プロトコルを使用してバインディングテーブルの回復を有効にします。 <b>NDP</b> または <b>DHCP</b> の入力。</li> </ul> <p>• (任意) <b>default</b> : ポリシー属性をデフォルト値に設定します。次のポリシー属性をデフォルト値に設定できます。 <b>data-glean</b>、<b>destination-glean</b>、<b>device-role</b>、<b>limit</b>、<b>prefix-glean</b>、<b>protocol</b>、<b>security-level</b>、<b>tracking</b>、<b>trusted-port</b>。</p> <p>• (任意) <b>destination-glean</b> : データトラフィックの宛先アドレスを収集して、バインディングテーブルを読み込みます。次のいずれかのオプションを入力します。</p> <ul style="list-style-type: none"> <li>• <b>log-only</b> : データパケット通知時に syslog メッセージを生成します。</li> <li>• <b>recovery</b> : プロトコルを使用してバインディングテーブルの回復を有効にします。 <b>DHCP</b> を入力します。</li> </ul> <p>• (任意) <b>device-role</b> : ポートに接続されているデバイスのロールを設定します。ノードまたはスイッチを指定できます。次のいずれかのオプションを入力します。</p> <ul style="list-style-type: none"> <li>• <b>node</b> : 接続されているデバイスをノードとして設定します。これがデフォルトのオプションです。</li> <li>• <b>switch</b> : 接続されているデバイスをスイッチとして設定します。</li> </ul> <p>• (任意) <b>distribution-switch</b> : このオプションは CLI には表示されますが、サポートされていません。行った設定は有効になりません。</p> <ul style="list-style-type: none"> <li>• <b>exit</b> : デバイストラッキング ポリシー コンフィギュレーション モードを終了します。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <b>limit address-count</b> : ポートごとのアドレスカウント制限を指定します。有効な範囲は1～32000です。</li> <li>• <b>no</b> : コマンドを無効にするか、デフォルト値を設定します。</li> <li>• (任意) <b>prefix-glean</b> : IPv6 ルータアドバタイズメントまたは DHCP-PD のどちらかからのプレフィックスの学習を有効にします。次のオプションがあります。 <ul style="list-style-type: none"> <li>• (任意) <b>only</b> : プレフィックスのみを収集し、ホストアドレスは収集しません。</li> </ul> </li> <li>• (任意) <b>protocol</b> : 収集するプロトコルを設定します。デフォルトでは、すべて収集されます。次のいずれかのオプションを入力します。 <ul style="list-style-type: none"> <li>• <b>arp [prefix-list name]</b> : ARP パケットのアドレスを収集します。必要に応じて、照合するプレフィックスリストの名前を入力します。</li> <li>• <b>dhcp4 [prefix-list name]</b> : DHCPv4 パケットのアドレスを収集します。必要に応じて、照合するプレフィックスリストの名前を入力します。</li> <li>• <b>dhcp6 [prefix-list name]</b> : DHCPv6 パケットのアドレスを収集します。必要に応じて、照合するプレフィックスリストの名前を入力します。</li> <li>• <b>ndp [prefix-list name]</b> : NDP パケットのアドレスを収集します。必要に応じて、照合するプレフィックスリストの名前を入力します。</li> <li>• <b>udp [prefix-list name]</b> : このオプションは CLI には表示されますが、サポートされていません。行った設定は有効になりません。</li> </ul> </li> <li>• (任意) <b>security-level</b> : この機能によって適用されるセキュリティのレベルを指定します。次のいずれかのオプションを入力します。</li> </ul>



	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <b>glean</b> : アドレスをパッシブに収集します。</li> <li>• <b>guard</b> : 不正なメッセージを検査してドロップします。これはデフォルトです。</li> <li>• <b>inspect</b> : メッセージを収集して検証します。</li> <li>• (任意) <b>tracking</b> : トラッキングオプションを指定します。次のいずれかのオプションを入力します。 <ul style="list-style-type: none"> <li>• <b>disable</b> [<b>stale-lifetime</b> [1-86400-seconds infinite] ] : デバイストラッキングをオフにします。 必要に応じて、エントリを削除するまで非アクティブにする期間を入力することも、永続的に非アクティブにすることもできます。</li> <li>• <b>enable</b> [<b>reachable-lifetime</b> [1-86400-seconds infinite] ] : デバイストラッキングをオンにします。 必要に応じて、エントリを到達可能にする期間を入力することも、永続的に到達可能にすることもできます。</li> </ul> </li> <li>• (任意) <b>trusted-port</b> : 信頼できるポートを設定します。該当するターゲットに対するガードがディセーブルになります。信頼できるポートを経由して学習されたバインディングは、他のどのポートを経由して学習されたバインディングよりも優先されます。テーブル内にエントリを作成しているときに衝突が発生した場合、信頼できるポートが優先されます。</li> <li>• (任意) <b>vpc</b> : このオプションは CLI には表示されますが、サポートされていません。行った設定は有効になりません。</li> </ul>
ステップ 4	<b>end</b> 例 : Device(config-device-tracking)# <b>exit</b>	設定モードを終了します。

	コマンドまたはアクション	目的
ステップ 5	<b>show device-tracking policy</b> <i>policy-name</i> 例 : Device# <b>show device-tracking policy example_policy</b>	デバイストラッキングポリシー設定を表示します。

### 次のタスク

ポリシーをインターフェイスまたは VLAN に適用します。

## デバイストラッキングポリシーのインターフェイスへの適用

デバイストラッキングポリシーをインターフェイスにアタッチするには、特権 EXEC モードで次の手順を実行します。

### 手順の概要

1. **configure terminal**
2. **interface** *interface*
3. **[no] device-tracking attach-policy** *policy name*
4. **end**
5. **show device-tracking policies** [*interface interface*]

### 手順の詳細

	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# <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>interface</b> <i>interface</i> 例 : Device(config)# <b>interface gigabitethernet 1/1/4</b>	インターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<b>[no] device-tracking attach-policy</b> <i>policy name</i> 例 : Device(config-if)# <b>device-tracking attach-policy example_policy</b>	インターフェイスにデバイストラッキングポリシーを適用します。デバイストラッキングは、EtherChannel でもサポートされます。  (注) SISF ベースのデバイストラッキングポリシーは、カスタムポリシーである場合にのみ無効にできます。プログラムによって作成されたポリシーは、対応するデバイストラッキングクライアント機能の設定が削除された場合にのみ削除できます。

	コマンドまたはアクション	目的
ステップ 4	<b>end</b> 例： Device# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show device-tracking policies [interface interface]</b> 例： Device# <b>show device-tracking policies interface gigabitethernet 1/1/4</b>	指定されたインターフェイスの種類と番号に一致するポリシーを表示します。

## デバイストラッキングポリシーの VLAN への適用

複数のインターフェイスでデバイストラッキングポリシーを VLAN にアタッチするには、特権 EXEC モードで次の手順を実行します。

### 手順の概要

1. **configure terminal**
2. **vlan configuration vlan\_list**
3. **[no] device-tracking attach-policy policy\_name**
4. **do show device-tracking policies vlan vlan-ID**

### 手順の詳細

	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# <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>vlan configuration vlan_list</b> 例： Device(config)# <b>vlan configuration 333</b>	デバイストラッキングポリシーを適用する VLAN を指定し、その VLAN インターフェイス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	<b>[no] device-tracking attach-policy policy_name</b> 例： Device(config-vlan-config)# <b>device-tracking attach-policy example_policy</b>	すべてのスイッチ インターフェイスで、デバイストラッキングポリシーを指定された VLAN にアタッチします。  (注) SISF ベースのデバイストラッキングポリシーは、カスタムポリシーである場合にのみ無効にできます。プログラムによって作成されたポリシーは、対応するデバイストラッキングクライアント機能の設定が削除された場合にのみ削除できます。

	コマンドまたはアクション	目的
ステップ 4	<b>do show device-tracking policies vlan <i>vlan-ID</i></b> 例 : Device(config-vlan-config)# <b>do show device-tracking policies vlan 333</b>	VLAN インターフェイス コンフィギュレーション モードを終了しないで、ポリシーが指定された VLAN に割り当てられていることを確認します。

## Cisco IOS XE Fuji 16.9.x 以降のリリースでの SISF ベースのデバイストラッキングのプログラムによる有効化

表 46: Cisco IOS XE Fuji 16.9.x 以降のリリースでの SISF ベースのデバイストラッキングのプログラムによる有効化

SISF ベースのデバイストラッキングを有効にできるデバイストラッキング クライアント機能	<p>Cisco IOS XE Fuji 16.9.x 以降のリリースでは、次の機能について SISF ベースのデバイストラッキングをプログラムで有効にできます。</p> <ul style="list-style-type: none"> <li>• IEEE 802.1X、web 認証、Cisco TrustSec、IPSG 機能 : <b>ip dhcp snooping vlan <i>vlan</i></b> コマンドを入力します。</li> <li>• Cisco Locator/ID Separation Protocol (LISP)。</li> <li>• EVPN on VLAN</li> </ul> <p>(注) プログラムによって作成されたポリシーが複数ある場合は、優先順位が最も高いポリシーが有効になります。</p>
ポリシー名	<ul style="list-style-type: none"> <li>• IEEE 802.1X、web 認証、Cisco TrustSec、および IPSG 機能は、ポリシー <b>DT-PROGRAMMATIC</b> を使用します。</li> <li>• LISP 機能は、<b>LISP-DT-GUARD-VLAN</b> または <b>LISP-DT-GLEAN-VLAN</b> を作成します。</li> <li>• EVPN on VLAN 機能は <b>evpn-sisf-policy</b> を作成します</li> </ul> <p>設定のリストは、各プログラムポリシーによって異なります。詳細については、例を参照してください。</p>

ユーザー オプション	<ul style="list-style-type: none"> <li>• ポリシーの優先順位がサポートされます。優先順位は、ポリシーの作成方法によって決まります。手動で作成されたポリシーが最も優先されます。これにより、プログラムで生成されたポリシーとは異なるポリシー設定を適用できます。</li> <li>• 複数のポリシーを同じ VLAN に適用できます。</li> <li>• 優先順位が異なる複数のポリシーが同じ VLAN に適用されている場合、優先順位が最も高いポリシーの設定が有効になります。ここでの例外は <b>limit address-count for IPv4 per mac</b> と <b>limit address-count for IPv6 per mac</b> の設定です。優先順位が最も低いポリシーの設定が有効になります。</li> <li>• デバイストラッキングクライアント機能の設定が削除されない限り、ポリシーは削除できません。</li> <li>• ポリシー属性は変更できません。</li> <li>• MAC ごとのアドレスカウント制限は変更できません。これは <b>limit address-count for IPv4 per mac</b> および <b>limit address-count for IPv6 per mac</b> コマンドに該当します。</li> <li>• VLAN のポリシー設定を変更するには、カスタマイズされたデバイストラッキング ポリシーを作成し、VLAN に適用します。</li> <li>• デバイストラッキング ポリシーが VLAN のインターフェイスに適用されると、インターフェイスのポリシー設定が VLAN のポリシー設定よりも優先されます。ここでの例外は、<b>limit address-count for IPv4 per mac</b> と <b>limit address-count for IPv6 per mac</b> の値で、インターフェイスと VLAN の両方のポリシーから集約されます。</li> </ul>
------------	--

## トランクポートからのバインディングエントリの作成を停止するためのマルチスイッチネットワークの設定

マルチスイッチネットワークでは、SISF ベースのデバイストラッキングにより、機能を実行しているスイッチ間でバインディングテーブルエントリを分散できます。バインディングエントリは、ホストがアクセスポートに表示されるスイッチでのみ作成されます。トランクポート経由で表示されるホストのエントリは作成されません。これは、**trusted-port** および **device-role switch** オプションを使用してポリシーを設定し、トランクポートに適用することで実現されます。



**重要** ポリシーで、**trusted-port** および **device-role switch** オプションの両方を設定する必要があります。

さらに、SISF ベースのデバイストラッキングが有効になっているデバイス側のポートに、このようなポリシーを適用することを推奨します。

次の手順を実行します。

## 手順の概要

1. **configure terminal**
2. **device-tracking policy** *policy-name*
3. **device-role switch**
4. **trusted-port**
5. **end**
6. **interface** *interface*
7. **device-tracking attach-policy** *policy-name*

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： Device# <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>device-tracking policy</b> <i>policy-name</i> 例： Device(config)# <b>device-tracking policy</b> <b>example_trusted_policy</b>	指定されたポリシーのデバイストラッキング 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 switch</b> 例： Device(config-device-tracking)# <b>device-role switch</b>	ポートに接続されているデバイスのロールを指定します。デフォルトは <b>node</b> です。ポートのバインディングエントリの作成を停止する <b>device-role switch</b> オプションを入力します。
ステップ 4	<b>trusted-port</b> 例： Device(config-device-tracking)# <b>trusted-port</b>	信頼できるポートを設定します。該当するターゲットに対するガードがディセーブルになります。信頼できるポートを経由して学習されたバインディングは、他のどのポートを経由して学習されたバインディングよりも優先されます。テーブル内にエントリを作成しているときに衝突が発生した場合、信頼できるポートが優先されます。

	コマンドまたはアクション	目的
ステップ 5	<b>end</b> 例： Device(config-device-tracking)# <b>end</b>	デバイストラッキング ポリシー コンフィギュレーション モードを終了します。続いて、グローバル 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>interface interface</b> 例： Device(config)# <b>interface gigabitethernet 1/0/25</b>	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 7	<b>device-tracking attach-policy policy-name</b> 例： Device(config-if)# <b>device-tracking attach-policy example_trusted_policy</b>	デバイス トラッキング ポリシーをインターフェイス またはそのインターフェイス上で指定された VLAN にアタッチします。

## SISF ベースのデバイストラッキングの設定例

次の例は、デバイストラッキングの設定例と、特定の状況で推奨される、または関連するその他の設定を示しています。

### 例：Cisco IOS XE Everest 16.9.x 以降のリリースでの SISF ベースのデバイストラッキングのプログラムによる有効化

この出力例は、プログラムによって作成されたポリシーのさまざまな設定を示しています。

#### デバイス トラッキング クライアント：VLAN での LISP

LISP を設定したら、特権 EXEC モードで **show device-tracking policy** コマンドを入力して、作成された LISP-DT-GUARD-VLAN ポリシーと対応する設定を表示します。

```
Device# show device-tracking policy LISP-DT-GUARD-VLAN
Policy LISP-DT-GUARD-VLAN configuration:
 security-level guard (*)
 device-role node
 gleaning from Neighbor Discovery
 gleaning from DHCP
 gleaning from ARP
 gleaning from DHCP4
 NOT gleaning from protocol unkn
 limit address-count for IPv4 per mac 4 (*)
 limit address-count for IPv6 per mac 12 (*)
 tracking enable
Policy LISP-DT-GUARD-VLAN is applied on the following targets:
Target      Type      Policy          Feature          Target range
vlan 10     VLAN     LISP-DT-GUARD-VLAN  Device-tracking  vlan all
note:
Binding entry Down timer: 10 minutes (*)
Binding entry Stale timer: 30 minutes (*)
```

### デバイストラッキングクライアント : VLAN での LISP

LISP を設定したら、特権 EXEC モードで **show device-tracking policy** コマンドを入力して、作成された LISP-DT-GLEAN-VLAN ポリシーと対応する設定を表示します。

```
Device# show device-tracking policy LISP-DT-GLEAN-VLAN
Policy LISP-DT-GLEAN-VLAN configuration:
  security-level glean (*)
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  limit address-count for IPv4 per mac 4 (*)
  limit address-count for IPv6 per mac 12 (*)
  tracking enable
Policy LISP-DT-GUARD-VLAN is applied on the following targets:
Target      Type      Policy          Feature          Target range
vlan 10     VLAN     LISP-DT-GLEAN-VLAN  Device-tracking  vlan all

note:
Binding entry Down timer: 10 minutes (*)
Binding entry Stale timer: 30 minutes (*)
```

### デバイストラッキングクライアント : VLAN での EVPN

EVPN を設定した後、特権 EXEC モードで **show device-tracking policy** コマンドを入力して、作成された evpn-sisf-policy ポリシーとポリシーに応じて行った設定を表示します。

```
Device# show device-tracking policy evpn-sisf-policy
Policy evpn-sisf-policy configuration:
  security-level glean (*)
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  tracking enable
Policy evpn-sisf-policy is applied on the following targets:
Target      Type      Policy          Feature          Target range
vlan 10     VLAN     evpn-sisf-policy  Device-tracking  vlan all

note:
Binding entry Down timer: 24 hours (*)
Binding entry Stale timer: 24 hours (*)
```

### デバイストラッキングクライアント : IEEE 802.1X、web 認証、Cisco TrustSec、IPSG

グローバルコンフィギュレーションモードで **ip dhcp snooping vlan** *vlan* コマンドを設定して、IEEE 802.1X、web 認証、Cisco TrustSec、IPSG 機能のデバイストラッキングを有効にします。特権 EXEC モードで **show device-tracking policy** コマンドを入力し、作成された DT-PROGRAMMATIC ポリシーとポリシーに応じて行った設定を表示します。

```
Device# configure terminal
Device(config)# ip dhcp snooping vlan 10
Device(config)# end
Device# show device-tracking policy DT-PROGRAMMATIC
```



```

Policy DT-PROGRAMMATIC configuration:
  security-level glean (*)
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  limit address-count for IPv4 per mac 1 (*)
  tracking enable
Policy DT-PROGRAMMATIC is applied on the following targets:
Target      Type      Policy      Feature      Target range
vlan 10     VLAN     DT-PROGRAMMATIC  Device-tracking  vlan all

note:
Binding entry Down timer: 24 hours (*)
Binding entry Stale timer: 24 hours (*)

```

### ターゲットに複数のポリシーが適用されている場合のアクティブポリシーの識別

この例では、複数のポリシーが同じ VLAN に適用されている場合にアクティブポリシーを指定する方法を示します。

この例では、2つのポリシーが VLAN 10 に適用されており、LISP-DT-GUARD-VLAN がアクティブポリシーです。

```

Device# show device-tracking policies
Target      Type      Policy      Feature      Target range
vlan 10     VLAN     DT-PROGRAMMATIC  Device-tracking  vlan all
vlan 10     VLAN     LISP-DT-GUARD-VLAN  Device-tracking  vlan all

Device# show device-tracking capture-policy vlan 10
HW Target vlan 10 HW policy signature 0001DF9F policies#:2 rules 14 sig 0001DF9F
SW policy DT-PROGRAMMATIC feature Device-tracking -
SW policy LISP-DT-GUARD-VLAN feature Device-tracking - Active

```

## 例：ターゲットでの IPv6 デバイストラッキングの無効化

デフォルトで、SISF ベースのデバイストラッキングは IPv4 と IPv6 の両方をサポートします。次の設定例は、サポートされている場合に IPv6 デバイストラッキングを無効にする方法を示しています。

カスタムポリシーがターゲットに適用されている場合に、IPv6 のデバイストラッキングを無効にする（すべてのリリース）：

```

Device(config)# device-tracking policy example-policy
Device(config-device-tracking)# no protocol ndp
Device(config-device-tracking)# no protocol dhcp6
Device(config-device-tracking)# end

```

プログラムポリシーがターゲットに適用されている場合に、IPv6 のデバイストラッキングを無効にする（Cisco IOS XE Everest 16.6.x および Cisco IOS XE Fuji 16.8.x のみ）：

```

Device(config)# device-tracking policy DT-PROGRAMMATIC
Device(config-device-tracking)# no protocol ndp

```

例：VLAN 上の SVI に対する IPv6 の有効化（重複アドレスの問題を軽減するため）

```
Device(config-device-tracking)# no protocol dhcp6
Device(config-device-tracking)# end
```



- (注)
- Cisco IOS XE Everest 16.5.x リリースでは、プログラムポリシーが適用されている場合、IPv6 のデバイストラッキングを無効にすることはできません。
  - Cisco IOS XE Everest 16.6.x および Cisco IOS XE Fuji 16.8.x では、プログラムポリシーが適用されている場合、上の例に示すように、IPv6 のデバイストラッキングを無効にすることができます。
  - Cisco IOS XE Fuji 16.9.x 以降では、プログラムポリシーの設定を変更できません。

## 例：VLAN 上の SVI に対する IPv6 の有効化（重複アドレスの問題を軽減するため）

ネットワークで IPv6 が有効になっており、VLAN 上でスイッチ仮想インターフェイス（SVI）が設定されている場合は、SVI 設定に次の内容を追加することを推奨します。これにより、SVI はリンクローカルアドレスを自動的に取得できます。このアドレスは SISF プローブの送信元 IP アドレスとして使用されるため、重複 IP アドレスの問題を防止できます。

```
Device(config)# interface vlan 10
Device(config-if)# ipv6 enable
Device(config-if)# end
```

## 例：IPv4 重複アドレスの問題の緩和

次に、Microsoft Windows を実行しているクライアントによって発生した重複 IP アドレス 0.0.0.0 エラーメッセージの問題に対応する例を示します。

**device-tracking tracking auto-source** コマンドをグローバル コンフィギュレーション モードで設定します。このコマンドは、デバイストラッキング テーブル内のエントリを維持するために、スイッチがクライアントをプローブするよう送信するアドレス解決パケット（ARP）要求で使用される送信元 IP および MAC アドレスを決定します。その目的は、送信元 IP アドレスとして 0.0.0.0 を使用しないようにすることです。



- (注) スイッチ仮想インターフェイス（SVI）が設定されていない場合に、**device-tracking tracking auto-source** コマンドを設定します。SVI が VLAN で IPv4 アドレスを使用して設定されている場合は、設定する必要はありません。

コマンド	アクション (デバイストラッキング ARP プローブの送信元 IP および MAC アドレスを選択するた め)	注記
<b>device-tracking tracking auto-source</b>	<ul style="list-style-type: none"> <li>• 存在する場合、VLAN SVI に送信元を設定します。</li> <li>• 同じサブネットからデバイストラッキングテーブルで IP および MAC バインディングを検索します。</li> <li>• 0.0.0.0 を使用します</li> </ul>	MAC フラッピングを回避するために、すべてのトランクポートでデバイストラッキングを無効にすることを推奨します。
<b>device-tracking tracking auto-source override</b>	<ul style="list-style-type: none"> <li>• 存在する場合、VLAN SVI に送信元を設定します。</li> <li>• 0.0.0.0 を使用します。</li> </ul>	SVI がない場合は推奨しません。
<b>ip device tracking probe auto-source fallback 0.0.0.X 255.255.255.0</b>	<ul style="list-style-type: none"> <li>• 存在する場合、VLAN SVI に送信元を設定します。</li> <li>• 同じサブネットからデバイストラッキングテーブルで IP および MAC バインディングを検索します。</li> <li>• 提供されたホストビットとマスクを使用して、クライアント IP から送信元 IP を計算します。送信元 MAC は、クライアント側のスイッチポートの MAC アドレスから取得されます*。</li> </ul>	MAC フラッピングを回避するために、すべてのトランクポートでデバイストラッキングを無効にすることを推奨します。  計算された IPv4 アドレスは、クライアントまたはネットワークデバイスに割り当てることはできません。

## 例：短いデバイストラッキング バインディング到達可能時間の回避

コマンド	アクション	注記
	(デバイストラッキング ARP プロブの送信元 IP および MAC アドレスを選択するため)	
<b>device-tracking tracking auto-source fallback 0.0.0.X 255.255.255.0 override</b>	<ul style="list-style-type: none"> <li>存在する場合、VLAN SVI に送信元を設定します。</li> </ul> 提供されたホストビットとマスクを使用して、クライアント IP から送信元 IP を計算します*。送信元 MAC は、クライアント側のスイッチポートの MAC アドレスから取得されます*。	

\* クライアント IP アドレスによっては、IPv4 アドレスを送信元 IP 用に予約する必要があります。

予約済み送信元 IPv4 アドレス = (host-ip and mask) | client-ip

- クライアント IP = 192.0.2.25
- 送信元 IP = (192.0.2.25 and 255.255.255.0) | (0.0.0.1) = 192.0.2.1

IP アドレス 192.0.2.1 をクライアントまたはネットワークデバイスに割り当てないでください。

## 例：短いデバイストラッキング バインディング到達可能時間の回避

以前のリリースから移行する場合、次の設定が存在している可能性があります。

```
device-tracking binding reachable-time 10
```

コマンドの **no** バージョンを入力して、これを削除します。

## SISF の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	SISF ベースのデバイストラッキング	<p>この機能が導入されました。</p> <p>SISF ベースのデバイストラッキングは、ネットワーク内のエンドノードの存在、ロケーション、移動を追跡します。この機能は、スイッチが受信したトラフィックをスヌーピングし、デバイスアイデンティティ (MAC と IP アドレス) を抽出して、バインディングテーブルに保存します。(デバイストラッキングクライアントと呼ばれる) その他の機能の適切な動作は、この情報の正確性に依存します。</p> <p>IPv4 および IPv6 のどちらもサポートされています。</p> <p>デフォルトでは、SISF ベースのデバイストラッキングは無効になっています。</p>
Cisco IOS XE Everest 16.6.1	DT_PROGRAMMATIC のパラメータを変更するオプション	<p>このリリース以降、プログラムで作成されたデバイストラッキングポリシー (DT_PROGRAMMATIC) の特定の設定をデバイストラッキングコンフィギュレーションモード (config-device-tracking) で変更できます。</p>
Cisco IOS XE Fuji 16.9.1	ポリシーの優先順位追加のデバイス追跡クライアント プログラムで作成されたポリシーの変更	<p>ポリシーの優先順位のサポートが導入されました。優先順位は、ポリシーの作成方法によって決まります。手動で作成されたポリシーが最も優先されます。これにより、プログラムで生成されたポリシーとは異なるポリシー設定を適用できます。</p> <p>デバイストラッキングクライアント機能が追加されました。プログラムで作成されるポリシーは、デバイストラッキングクライアントごとに異なります。</p> <p>任意のプログラムで作成されるポリシーのパラメータを変更するオプションは廃止されました。</p>

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator にアクセスするには、<https://cfmng.cisco.com> に進みます。





## 第 24 章

# IEEE 802.1x ポートベースの認証の設定

この章では、IEEE 802.1x ポートベース認証を設定する方法について説明します。IEEE 802.1x 認証は、不正なデバイス（クライアント）によるネットワークアクセスを防止します。別途記載のないかぎり、スイッチという用語はスタンドアロンスイッチまたはスイッチスタックを意味します。

- [IEEE 802.1x ポートベース認証の制約事項 \(513 ページ\)](#)
- [802.1x ポートベース認証について \(514 ページ\)](#)
- [802.1x ポートベース認証の設定方法 \(549 ページ\)](#)
- [802.1x の統計情報およびステータスのモニターリング \(606 ページ\)](#)
- [IEEE 802.1x ポートベースの認証の機能履歴 \(607 ページ\)](#)

## IEEE 802.1x ポートベース認証の制約事項

- プライベート VLAN で使用する場合、スイッチポートは常に許可されません。認証、許可、およびアカウントिंग (AAA) サーバーからプッシュされるダイナミック VLAN は、プライベート VLAN ポートではサポートされません。データ クライアントセッションは、プライベート VLAN の dot1x ポートのセカンダリ VLAN で許可されることが期待されます。
- 通常のアクセス VLAN ポートでは、インターフェイスで設定されたプライベート VLAN ベースの許可とダイナミック VLAN だけがサポートされます。
- **dot1q tag vlan native** コマンドがグローバルレベルで設定されている場合、トランクポートでの dot1x 再認証は失敗します。
- 認証の失敗を引き起こす可能性があるため、音声 VLAN とアクセス VLAN の両方に同じ VLAN ID を同時に設定しないでください。
- 管理 VRF は、RADIUS の送信元インターフェイスとして使用できません。
- ポートセキュリティは、IEEE 802.1x ポートベース認証ではサポートされていません。

## 802.1x ポートベース認証について

802.1x 規格では、一般の人がアクセス可能なポートから不正なクライアントが LAN に接続しないように規制する（適切に認証されている場合を除く）、クライアント/サーバ型のアクセスコントロールおよび認証プロトコルを定めています。認証サーバーがスイッチポートに接続する各クライアントを認証したうえで、スイッチまたは LAN が提供するサービスを利用できるようにします。



(注) TACACS は、802.1x 認証ではサポートされていません。

802.1x アクセスコントロールでは、クライアントを認証するまでの間、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)、Cisco Discovery Protocol (CDP)、およびスパンニングツリープロトコル (STP) 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。

クライアントセッション	サポートされる最大セッション数
dot1x または MAB クライアントセッションの最大数	2000
Web ベース認証セッションの最大数	2000
クリティカル認証 VLAN を有効にしてサーバを再初期化した dot1x セッションの最大数	2000
さまざまなセッション機能が適用される MAB セッションの最大数	2000
サービス テンプレートまたはセッション機能が適用される dot1x セッションの最大数	2000

## ポートベース認証プロセス

IEEE 802.1X ポートベース認証を設定するには、認証、認可、およびアカウントティング (AAA) を有効にし、認証方式リストを指定する必要があります。方式リストは、ユーザ認証のためにクエリ送信を行う手順と認証方式を記述したものです。

AAA プロセスは認証から始まります。802.1x ポートベース認証がイネーブルであり、クライアントが 802.1x 準拠のクライアントソフトウェアをサポートしている場合、次のイベントが発生します。

- クライアント ID が有効で 802.1x 認証に成功した場合、スイッチ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。



- EAPOL メッセージ交換の待機中に 802.1x 認証がタイムアウトし、MAC 認証バイパスがイネーブルの場合、スイッチはクライアント MAC アドレスを認証用に使います。このクライアント MAC アドレスが有効で認証に成功した場合、スイッチ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。クライアント MAC アドレスが無効で認証に失敗した場合、ゲスト VLAN が設定されていれば、スイッチはクライアントに限定的なサービスを提供するゲスト VLAN を割り当てます。
- スイッチが 802.1x 対応クライアントから無効な ID を取得し、制限付き VLAN が指定されている場合、スイッチはクライアントに限定的なサービスを提供する制限付き VLAN を割り当てることができます。
- RADIUS 認証サーバーが使用できず（ダウンしていて）アクセスできない認証バイパスがイネーブルの場合、スイッチは、RADIUS 設定 VLAN またはユーザー指定アクセス VLAN で、ポートをクリティカル認証状態にして、クライアントにネットワークのアクセスを許可します。



---

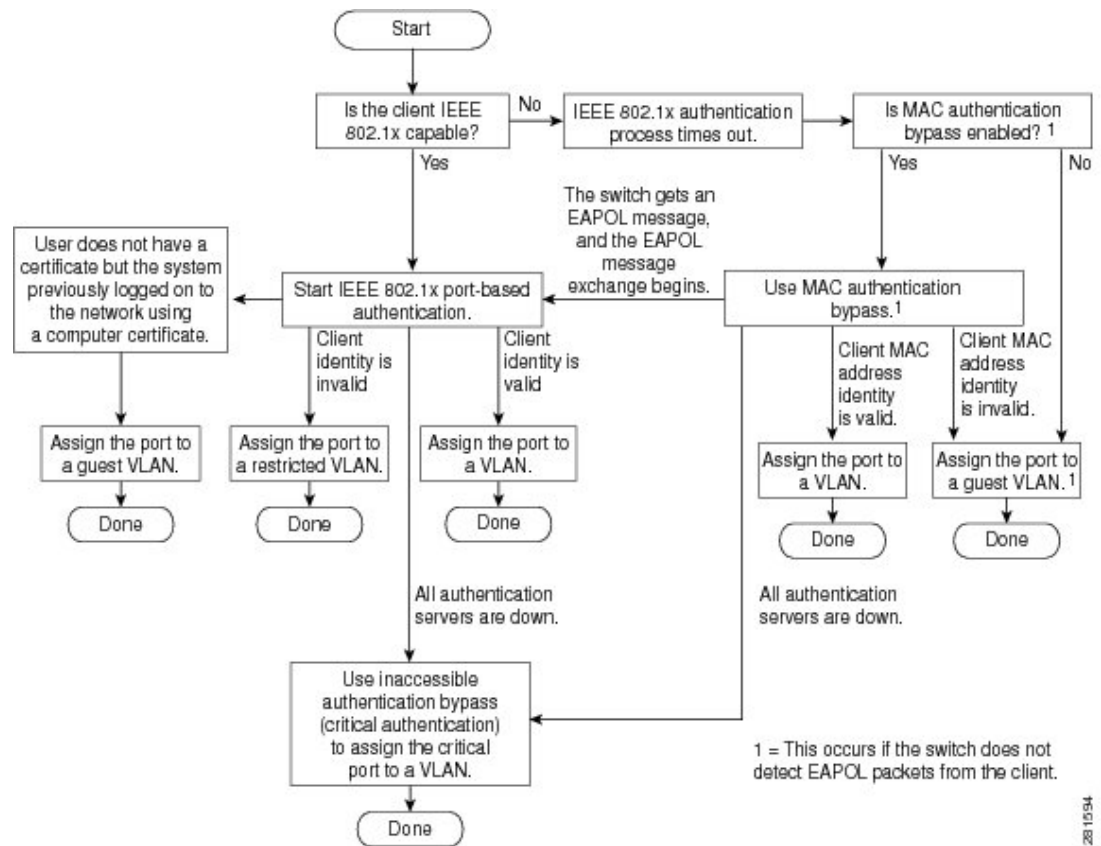
(注) アクセスできない認証バイパスは、クリティカル認証、または AAA 失敗ポリシーとも呼ばれます。

---

ポートで Multi Domain Authentication (MDA) が有効になっている場合、音声許可に該当する例外をいくつか伴ったフローを使用できます。

図 25: 認証フローチャート

次の図は認証プロセスを示します。



次の状況のいずれかが発生すると、スイッチはクライアントを再認証します。

- 定期的な再認証がイネーブルで、再認証タイマーの期限が切れている場合。

スイッチ固有の値を使用するか、RADIUS サーバーからの値に基づいて再認証タイマーを設定できます。

RADIUS サーバーを使用した 802.1x 認証の後で、スイッチは Session-Timeout RADIUS 属性 (Attribute[27])、および Termination-Action RADIUS 属性 (Attribute[29]) に基づいてタイマーを使用します。

Session-Timeout RADIUS 属性 (Attribute[27]) には再認証が行われるまでの時間を指定します。指定できる範囲は 1 ~ 65535 秒です。

Termination-Action RADIUS 属性 (Attribute[29]) には、再認証中に行われるアクションを指定します。アクションは *Initialize* および *ReAuthenticate* に設定できます。アクションに *Initialize* (属性値は *DEFAULT*) を設定した場合、802.1x セッションは終了し、認証中、接続は失われます。アクションに *ReAuthenticate* (属性値は *RADIUS-Request*) を設定した場合、セッションは再認証による影響を受けません。

- クライアントを手動で再認証するには、**dot1x re-authenticate interface interface-id** 特権 EXEC コマンドを入力します。

## ポートベース認証の開始およびメッセージ交換

802.1x 認証中に、スイッチまたはクライアントは認証を開始できます。**authentication port-control auto** インターフェイス コンフィギュレーション コマンドを使用してポート上で認証をイネーブルにすると、スイッチは、リンクステートがダウンからアップに移行したときに認証を開始し、ポートがアップしていて認証されていない場合は定期的に認証を開始します。スイッチはクライアントに EAP-Request/Identity フレームを送信し、その ID を要求します。クライアントはフレームを受信すると、EAP-Response/Identity フレームで応答します。

ただし、クライアントが起動時にスイッチからの EAP-Request/Identity フレームを受信しなかった場合、クライアントは EAPOL-Start フレームを送信して認証を開始できます。このフレームはスイッチに対し、クライアントの識別情報を要求するように指示します。



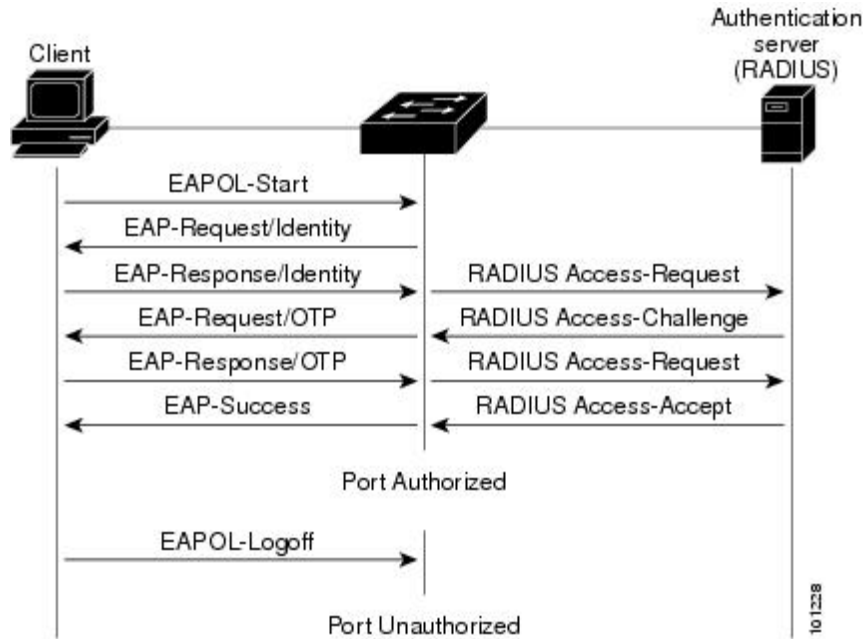
- (注) ネットワークアクセスデバイスで 802.1x 認証がイネーブルに設定されていない、またはサポートされていない場合には、クライアントからの EAPOL フレームはすべて廃棄されます。クライアントが認証の開始を 3 回試みても EAP-Request/Identity フレームを受信しなかった場合、クライアントはポートが許可ステートであるものとしてフレームを送信します。ポートが許可ステートであるということは、クライアントの認証が成功したことを実質的に意味します。

クライアントが自らの識別情報を提示すると、スイッチは仲介デバイスとしての役割を開始し、認証が成功または失敗するまで、クライアントと認証サーバーの間で EAP フレームを送受信します。認証が成功すると、スイッチポートは許可ステートになります。認証に失敗した場合、認証が再試行されるか、ポートが限定的なサービスを提供する VLAN に割り当てられるか、あるいはネットワーク アクセスが許可されないかのいずれかになります。

実際に行われる EAP フレーム交換は、使用する認証方式によって異なります。

図 26: メッセージ交換

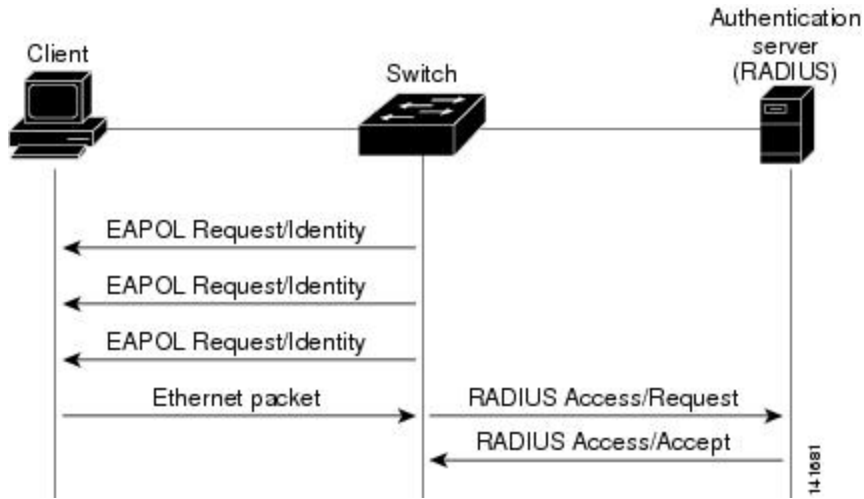
次の図に、クライアントが RADIUS サーバとの間で OTP (ワンタイムパスワード) 認証方式を使用する際に行われるメッセージ交換を示します。



EAPOL メッセージ交換の待機中に 802.1x 認証がタイムアウトし、MAC 認証バイパスがイネーブルの場合、スイッチはクライアントからイーサネットパケットを検出するとそのクライアントを認証できません。スイッチは、クライアントの MAC アドレスを ID として使用し、RADIUS サーバーに送信される RADIUS Access/Request フレームにこの情報を保存します。サーバーがスイッチに RADIUS Access/Accept フレームを送信（認証が成功）すると、ポートが許可されます。認証に失敗してゲスト VLAN が指定されている場合、スイッチはポートをゲスト VLAN に割り当てます。イーサネットパケットの待機中にスイッチが EAPOL パケットを検出すると、スイッチは MAC 認証バイパスプロセスを停止して、802.1x 認証を開始します。

図 27: MAC 認証バイパス中のメッセージ交換

次の図に、MAC 認証バイパス中のメッセージ交換を示します。



## ポートベース認証の認証マネージャ

### ポートベース認証方法

表 47: 802.1x 機能

認証方法	モード			
	シングルホスト	マルチホスト	MDA	複数
802.1x	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL	VLAN 割り当て	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL	VL ユー Filt ダウ AC リタ
MAC 認証バイパス	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL	VLAN 割り当て	VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL	VL ユー Filt ダウ AC リタ
スタンドアロン Web 認証	プロキシ ACL、Filter-ID 属性、ダウンロード可能な ACL			

認証方法	モード			
	シングル ホスト	マルチ ホスト	MDA	複数認
NAC レイヤ 2 IP 検証	Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL	Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL	Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL	Filter-ID ダウンロード可能 ACL リダイ
フォールバック方式としての Web 認証	プロキシ ACL Filter-ID 属性 ダウンロード可能 ACL	プロキシ ACL Filter-ID 属性 ダウンロード可能 ACL	プロキシ ACL Filter-ID 属性 ダウンロード可能 ACL	プロキシ Filter-ID ダウンロード可能 ACL

<sup>9</sup> Cisco IOS リリース 12.2(50)SE 以降でサポートされています。

<sup>10</sup> 802.1x 認証をサポートしないクライアント用。

## ユーザー単位 ACL および Filter-Id



(注) Filter-Id としてロールベース ACL を使用することは推奨されません。

MDA 対応ポートおよびマルチ認証ポートでは、複数のホストを認証できます。ホストに適用される ACL ポリシーは、別のホストのトラフィックには影響を与えません。マルチ ホストポートで認証されるホストが1つだけで、他のホストが認証なしでネットワークアクセスを取得する場合、発信元アドレスに any を指定することで、最初のホストの ACL ポリシーを他の接続ホストに適用できます。

## ポートベース認証マネージャ CLI コマンド

認証マネージャ インターフェイス コンフィギュレーション コマンドは、802.1x、MAC 認証バイパスおよび Web 認証など、すべての認証方法を制御します。認証マネージャ コマンドは、接続ホストに適用される認証方法のプライオリティと順序を決定します。

認証マネージャ コマンドは、ホスト モード、違反モードおよび認証タイマーなど、一般的な認証機能を制御します。一般的な認証コマンドには、**authentication host-mode**、**authentication violation**、および **authentication timer** インターフェイス コンフィギュレーション コマンドが含まれます。

802.1x 専用コマンドは、先頭に **dot1x** キーワードが付きます。たとえば、**authentication port-control auto** インターフェイス コンフィギュレーション コマンドは、インターフェイスでの認証をイネーブルにします。

スイッチでの **dot1x** を無効にするには、**no dot1x system-auth-control** コマンドを使用して、設定をグローバルに削除し、設定されているすべてのインターフェイスからも削除します。



- (注) 802.1x 認証がグローバルにディセーブル化されても、Web 認証など他の認証方法はそのポートでイネーブルのままです。

**authentication manager** コマンドは、以前の 802.1x コマンドと同じ機能を提供します。

認証マネージャが生成する冗長なシステムメッセージをフィルタリングすると、通常は、フィルタリングされた内容が認証の成功に結びつきます。802.1x 認証および MAB 認証の冗長なメッセージをフィルタリングすることもできます。認証方式ごとに異なるコマンドが用意されています。

- **no authentication logging verbose** グローバル コンフィギュレーション コマンドは、認証マネージャからの詳細メッセージをフィルタリングします。
- **no dot1x logging verbose** グローバル コンフィギュレーション コマンドは、802.1x 認証の詳細メッセージをフィルタリングします。
- **no mab logging verbose** グローバル コンフィギュレーション コマンドは、MAC 認証バイパス (MAB) の詳細メッセージをフィルタリングします。

表 48: 認証マネージャ コマンドおよび以前の 802.1x コマンド

Cisco IOS Release 12.2(50)SE 以降での認証マネージャ コマンド	Cisco IOS Release 12.2(46)SE 以前での同等の 802.1x コマンド	説明
<b>authentication control-direction</b> {both   in}	<b>dot1x control-direction</b> {both   in}	Wake-on-LAN (WoL) 機能を使用をイネーブルにし、ポート制は双方向に設定します。
<b>authentication event</b>	<b>dot1x auth-fail vlan</b> <b>dot1x critical (interface configuration)</b> <b>dot1x guest-vlan6</b>	ポート上で制限付き VLAN をイネーブルにします。 アクセス不能認証バイパス機能を使用します。 アクティブ VLAN を 802.1x ゲストとして指定します。
<b>authentication fallback</b> <i>fallback-profile</i>	<b>dot1x fallback</b> <i>fallback-profile</i>	802.1x 認証をサポートしていない用に、Web 認証をフォールバックするようにポートを設定します。
<b>authentication host-mode</b> [multi-auth   multi-domain   multi-host   single-host]	<b>dot1x host-mode</b> {single-host   multi-host   multi-domain}	802.1x 許可ポートで単一のホスト) または複数のホストの接続
<b>authentication order</b>	<b>mab</b>	使用される認証方法の順序を柔軟にします。

Cisco IOS Release 12.2(50)SE 以降での認証マネージャコマンド	Cisco IOS Release 12.2(46)SE 以前での同等の 802.1x コマンド	説明
<code>authentication periodic</code>	<code>dot1x reauthentication</code>	クライアントの定期的再認証をイネキス。
<code>authentication port-control {auto   force-authorized   force-unauthorized}</code>	<code>dot1x port-control {auto   force-authorized   force-unauthorized}</code>	ポートの許可状態の手動制御をにします。
<code>authentication timer</code>	<code>dot1x timeout</code>	802.1x タイマーを設定します。
<code>authentication violation {protect   restrict   shutdown}</code>	<code>dot1x violation-mode {shutdown   restrict   protect}</code>	新しいデバイスがポートに接続されたは最大数のデバイスがポートに接続に新しいデバイスがそのポートに接続に発生する違反モードを設定しま

## 許可状態および無許可状態のポート

802.1x 認証中に、スイッチのポート状態によって、スイッチはネットワークへのクライアントアクセスを許可します。ポートは最初、無許可状態です。この状態では、音声 VLAN（仮想 LAN）ポートとして設定されていないポートは 802.1x 認証、CDP、および STP パケットを除くすべての入力および出力トラフィックを禁止します。クライアントの認証が成功すると、ポートは許可状態に変更し、クライアントのトラフィック送受信を通常どおりに許可します。ポートが音声 VLAN ポートとして設定されている場合、VoIP トラフィックおよび 802.1x プロトコルパケットが許可された後クライアントが正常に認証されます。



(注) CDP バイパスはサポートされていないため、ポートが `error-disabled` 状態になる場合があります。

802.1x 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 ポートに接続すると、スイッチはその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 標準が稼働していないポートに接続すると、クライアントは EAPOL-Start 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。

**authentication port-control** インターフェイス コンフィギュレーション コマンドおよび次のキーワードを使用して、ポートの許可状態を制御できます。

- **force-authorized** : 802.1x 認証をディセーブルにし、認証情報の交換を必要とせずに、ポートを許可状態に変更します。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。これがデフォルト設定です。



- **force-unauthorized** : ポートが無許可ステータスのままになり、クライアントからの認証の試みをすべて無視します。スイッチはポートを介してクライアントに認証サービスを提供できません。
- **auto** : 802.1x 認証をイネーブルにします。ポートは最初、無許可ステータスであり、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変更した際、または EAPOL-Start フレームを受信した際に、認証プロセスが開始されます。スイッチ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。スイッチはクライアントの 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クライアントを一意に識別します。

クライアントが認証に成功すると（認証サーバから **Accept** フレームを受信すると）、ポートが許可ステータスに変わり、認証されたクライアントからの全フレームがポート経由での送受信を許可されます。認証が失敗すると、ポートは無許可ステータスのままですが、認証を再試行することはできません。認証サーバに到達できない場合、スイッチは要求を再送信します。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、ネットワークアクセスは許可されません。

クライアントはログオフするとき、EAPOL-Logoff メッセージを送信します。このメッセージによって、スイッチ ポートが無許可ステータスになります。

ポートのリンク ステータスがアップからダウンに変更した場合、または EAPOL-Logoff フレームを受信した場合に、ポートは無許可ステータスに戻ります。

## ポートベース認証とスイッチ スタック

スイッチが、スイッチ スタックに追加されるか、スイッチ スタックから削除される場合、RADIUS サーバーとスタックとの間の IP 接続が正常な場合、802.1x 認証は影響を受けません。これは、スタックのアクティブスイッチがスイッチスタックから削除される場合も、適用されます。アクティブスイッチに障害が発生した場合、スタックメンバーは、選択プロセスを使用することによってスタックの新しいアクティブスイッチになり、802.1x 認証プロセスは通常どおり続行されます。

サーバーに接続されていたスイッチが削除されたか、そのスイッチに障害が発生したために、RADIUS サーバーへの IP 接続が中断された場合、これらのイベントが発生します。

- すでに認証済みで、定期的な再認証がイネーブルではないポートは、認証ステータスのままです。RADIUS サーバーとの通信は、必要ではありません。
- すでに認証済みで、（**dot1x re-authentication** グローバル コンフィギュレーション コマンドを使用）定期的な再認証がイネーブルにされているポートは、再認証の発生時に、認証プロセスに失敗します。ポートは、再認証プロセス中に、非認証ステータスに戻ります。RADIUS サーバーとの通信が必要です。

進行中の認証については、サーバー接続が行われていないため、認証はただちに失敗します。

障害が発生したスイッチが実行状態になり、スイッチスタックに再加入した場合、ブートアップの時刻と、認証の試行時までには RADIUS サーバーへの接続が再確立されたかどうかによって、認証は失敗する場合と、失敗しない場合があります。

RADIUS サーバーへの接続を失うことを避けるには、冗長接続を設定する必要があります。たとえば、スタックのアクティブスイッチへの冗長接続と、スタックメンバーへの別の接続を設定できます。アクティブスイッチに障害が発生した場合でも、スイッチスタックは、RADIUS サーバーに接続されたままです。

## 802.1X のホストモード

802.1x ポートは、シングルホストモードまたはマルチホストモードで設定できます。シングルホストモードでは、802.1x 対応のスイッチポートに接続できるのはクライアント1つだけです。スイッチは、ポートのリンクステートがアップに変化したときに、EAPOL フレームを送信することでクライアントを検出します。クライアントがログオフしたとき、または別のクライアントに代わったときには、スイッチ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。

マルチホストモードでは、複数のホストを単一の 802.1x 対応ポートに接続できます。このモードでは、接続されたクライアントのうち1つが許可されれば、クライアントすべてのネットワークアクセスが許可されます。ポートが無許可ステートになると（再認証が失敗するか、または EAPOL-Logoff メッセージを受信した場合）、スイッチは接続しているクライアントのネットワークアクセスをすべて禁止します。

スイッチはマルチドメイン認証（MDA）をサポートしています。これにより、データ装置と IP Phone などの音声装置（シスコ製品またはシスコ以外の製品）の両方を同じスイッチポートに接続できます。

## 802.1x マルチ認証モード

マルチ認証（multiauth）モードでは、データ VLAN および音声 VLAN で複数のクライアントを認証できます。各ホストは個別に認証されます。マルチ認証ポートで認証できるデータデバイスまたは音声デバイスの数には制限はありません。

次の条件で、RADIUS サーバから提供された VLAN をマルチ認証モードで割り当てることができます。

- ホストがポートで最初に許可されたホストであり、RADIUS サーバが VLAN 情報を提供している。
- 後続のホストが、動作 VLAN に一致する VLAN を使用して許可される。
- ホストは VLAN が割り当てられていないポートで許可され、後続のホストでは VLAN 割り当てが設定されていないか、VLAN 情報が動作 VLAN と一致している。
- ポートで最初に許可されたホストにはグループ VLAN が割り当てられ、後続のホストでは VLAN 割り当てが設定されていないか、グループ VLAN がポート上のグループ VLAN と一致している。後続のホストが、最初のホストと同じ VLAN グループの VLAN を使用

する必要がある。VLAN リストが使用されている場合、すべてのホストは VLAN リストで指定された条件に従う。

- VLAN がポート上のホストに割り当てられると、後続のホストは一致する VLAN 情報を持つ必要があり、この情報がなければポートへのアクセスを拒否される。
- クリティカル認証 VLAN の動作が、マルチ認証モード用に変更されない。ホストが認証を試みたときにサーバに到達できない場合、許可されたすべてのホストは、設定された VLAN で再初期化される。

## ユーザーごとのマルチ認証 VLAN 割り当て

ユーザーごとのマルチ認証 VLAN 割り当て機能を使用すると、単一の設定済みアクセス VLAN を持つポート上のクライアントに割り当てられた VLAN に基づいて複数の運用アクセス VLAN を作成することができます。データ ドメインに関連付けられたすべての VLAN に対するトラフィックが dot1q とタグ付けされていないアクセス ポートとして設定されているポートおよびこれらの VLAN は、ネイティブ VLAN として処理されます。

マルチ認証ポート 1 つあたりのホストの数は 8 ですが、さらに多くのホストが存在する場合があります。

次のシナリオは、ユーザーごとのマルチ認証 VLAN 割り当てに関連しています。

### シナリオ 1

ハブがアクセス ポートに接続されている場合、およびポートがアクセス VLAN (V0) で設定されている場合。

ホスト (H1) は、ハブを介して VLAN (V1) に割り当てられます。ポートの運用 VLAN は V1 に変更されます。この動作は、単一ホストポートまたはマルチ ドメイン認証ポートと同様です。

2 番目のホスト (H2) が接続され、VLAN (V2) に割り当てられる場合、ポートには 2 つの運用 VLAN があります (V1 および V2)。H1 と H2 がタグなし入力トラフィックを送信すると、H1 トラフィックは VLAN (V1) に、H2 トラフィックは VLAN (V2) にマッピングされ、VLAN (V1) および VLAN (V2) のポートからの出トラフィックはすべてタグなしになります。

両方のホスト H1 と H2 がログアウトするか、またはセッションがなんらかの理由で削除されると、VLAN (V1) と VLAN (V2) がポートから削除され、設定された VLAN (V0) がポートに復元されます。

### シナリオ 2

ハブがアクセス ポートに接続されている場合、およびポートがアクセス VLAN (V0) で設定されている場合。ホスト (H1) は、ハブを介して VLAN (V1) に割り当てられます。ポートの運用 VLAN は V1 に変更されます。

2 番目のホスト (H2) が接続され明示的な VLAN ポリシーなしで承認されると、H2 はポート上で復元される設定済み VLAN (V0) を使用することを予期されます。2 つの運用 VLAN、VLAN (V0) および VLAN (V1) からの出トラフィックはすべてタグなしになります。

ホスト (H2) がログアウトするか、またはセッションがなんらかの理由で削除されると、設定された VLAN (V0) がポートから削除され、VLAN (V1) がそのポートでの唯一の運用 VLAN になります。

### シナリオ 3

ハブがオープン モードでアクセス ポートに接続されている場合、およびポートがアクセス VLAN (V0) で設定されている場合。

ホスト (H1) は、ハブを介して VLAN (V1) に割り当てられます。ポートの運用 VLAN は V1 に変更されます。2 番目のホスト (H2) が接続され無許可のままだと、オープン モードにより、運用 VLAN (V1) に引き続きアクセスできます。

ホスト H1 がログアウトするか、またはセッションがなんらかの理由で削除されると、VLAN (V1) はポートから削除され、ホスト (H2) は VLAN (V0) に割り当てられます。



(注) オープン モードと VLAN 割り当ての組み合わせは、ホスト (H2) に悪影響を与えます。そのホストは VLAN (V1) に対応するサブネット内に IP アドレスを含んでいるからです。

### ユーザーごとのマルチ認証 VLAN 割り当ての制限

ユーザーごとのマルチ認証 VLAN 割り当て機能では、複数の VLAN からの出トラフィックは、ホストが自分宛てではないトラフィックを受信するポート上ではタグなしになります。これは、ブロードキャストおよびマルチキャストトラフィックで問題になる可能性があります。

- **IPv4 ARP** : ホストは他のサブネットからの ARP パケットを受信します。これは、IP アドレス範囲が重複する異なる仮想ルーティングおよび転送 (VRF) テーブルの 2 個のサブネットがポート上でアクティブな場合に問題となります。ホスト ARP キャッシュのエントリが無効になる可能性があります。
- **IPv6 制御パケット** : IPv6 の導入環境では、ルータアドバタイズメント (RA) は、その受信を想定されていないホストによって処理されます。ある VLAN からのホストが別の VLAN からの RA を受信すると、ホストはそれ自身に間違った IPv6 アドレスを割り当てます。このようなホストは、ネットワークにアクセスできません。

回避策は、IPv6 ファースト ホップ セキュリティをイネーブルにして、ブロードキャスト ICMPv6 パケットがユニキャストに変換され、マルチ認証がイネーブルのポートから送信されるようにすることです。パケットは VLAN に属するマルチ認証ポートの各クライアント用に複製され、宛先 MAC が個々のクライアントに設定されます。1 つの VLAN を持つポートで、ICMPv6 パケットは正常にブロードキャストされます。

- **IP マルチキャスト** : 送信先のマルチキャスト グループへのマルチキャストトラフィックは、異なる VLAN 上のホストがそのマルチキャストグループに参加している場合それらの VLAN 用に複製されます。異なる VLAN の 2 つのホストが (同じマルチ認証ポート上の) マルチキャストグループに参加している場合、各マルチキャストパケットのコピー 2 部がそのポートから送信されます。

## MAC 移動

あるスイッチポートでMACアドレスが認証されると、そのアドレスは同じスイッチの別の認証マネージャ対応ポートでは許可されません。スイッチが同じMACアドレスを別の認証マネージャ対応ポートで検出すると、そのアドレスは許可されなくなります。

場合によっては、MACアドレスを同じスイッチ上のポート間で移動する必要があります。たとえば、認証ホストとスイッチポート間に別のデバイス（ハブまたはIP Phoneなど）がある場合、ホストをデバイスから接続して、同じスイッチの別のポートに直接接続する必要があります。

デバイスが新しいポートで再認証されるように、MAC移動をグローバルにイネーブルにできます。ホストが別のポートに移動すると、最初のポートのセッションが削除され、ホストは新しいポートで再認証されます。MAC移動はすべてのホストモードでサポートされます（認証ホストは、ポートでイネーブルにされているホストモードに関係なく、スイッチの任意のポートに移動できます）。MACアドレスがあるポートから別のポートに移動すると、スイッチは元のポートで認証済みセッションを終了し、新しいポートで新しい認証シーケンスを開始します。MAC移動の機能は、音声およびデータホストの両方に適用されます。



- 
- (注) オープン認証モードでは、MACアドレスは、新しいポートでの許可を必要とせずに、元のポートから新しいポートへただちに移動します。
- 

## MAC 置換

MAC置換機能は、ホストが、別のホストがすでに認証済みであるポートに接続しようとする発生する違反に対処するように設定できます。



- 
- (注) 違反はマルチ認証モードでは発生しないため、マルチ認証モードのポートにこの機能は適用されません。マルチホストモードで認証が必要なのは最初のホストだけなので、この機能はこのモードのポートには適用されません。
- 

**replace** キーワードを指定して **authentication violation** インターフェイス コンフィギュレーション コマンドを設定すると、マルチドメインモードのポートでの認証プロセスは、次のようになります。

- 既存の認証済みMACアドレスを使用するポートで新しいMACアドレスが受信されます。
- 認証マネージャは、ポート上の現在のデータホストのMACアドレスを、新しいMACアドレスで置き換えます。
- 認証マネージャは、新しいMACアドレスに対する認証プロセスを開始します。
- 認証マネージャによって新しいホストが音声ホストであると判断された場合、元の音声ホストは削除されます。

ポートがオープン認証モードになっている場合、MACアドレスはただちにMACアドレステーブルに追加されます。

## 802.1x アカウンティング

802.1x 標準では、ユーザの認証およびユーザのネットワークアクセスに対する許可方法を定義しています。ただし、ネットワークの使用法についてはトラッキングしません。802.1x アカウンティングは、デフォルトでディセーブルです。802.1x アカウンティングをイネーブルにすると、次の処理を 802.1x 対応のポート上でモニタできます。

- 正常にユーザを認証します。
- ユーザがログ オフします。
- リンクダウンが発生します。
- 再認証が正常に行われます。
- 再認証が失敗します。

スイッチは 802.1x アカウンティング情報を記録しません。その代わりに、スイッチはこの情報を RADIUS サーバに送信します。RADIUS サーバは、アカウンティングメッセージを記録するように設定する必要があります。

## 802.1x アカウンティング属性値ペア

RADIUS サーバに送信された情報は、属性値 (AV) ペアの形式で表示されます。これらの AV ペアのデータは、各種アプリケーションによって使用されます (たとえば課金アプリケーションの場合、RADIUS パケットの Acct-Input-Octets または Acct-Output-Octets 属性の情報が必要です)。

AV ペアは、802.1x アカウンティングが設定されているスイッチによって自動的に送信されます。次の種類の RADIUS アカウンティング パケットがスイッチによって送信されます。

- START : 新規ユーザー セッションが始まると送信されます。
- INTERIM : 既存のセッションが更新されると送信されます。
- STOP : セッションが終了すると送信されます。



---

(注) RADIUS および AAA のデバッグのログを表示するには、**show platform software trace message smd** コマンドを使用します。詳細については、『*Command Reference Guide*』のセクション「Tracing Commands」を参照してください。

---

次の表に、AV ペアおよびスイッチによって送信される AV ペアの条件を示します。

表 49: アカウンティング AV ペア

属性番号	AV ペア名	START	INTERIM	STOP
属性 [1]	User-Name	送信	送信	送信
属性 [4]	NAS-IP-Address	送信	送信	送信
属性 [5]	NAS-Port	送信	送信	送信
属性 [8]	Framed-IP-Address	非送信	条件に応じて送信 <sup>11</sup>	条件に応じて送信
属性 [30]	Called-Station-ID	送信	送信	送信
属性 [31]	Calling-Station-ID	送信	送信	送信
属性 [40]	Acct-Status-Type	送信	送信	送信
属性 [41]	Acct-Delay-Time	送信	送信	送信
属性 [42]	Acct-Input-Octets	非送信	送信	送信
属性 [43]	Acct-Output-Octets	非送信	送信	送信
属性 [47]	Acct-Input-Packets	非送信	送信	送信
属性 [48]	Acct-Output-Packets	非送信	送信	送信
属性 [44]	Acct-Session-ID	送信	送信	送信
属性 [45]	Acct-Authentic	送信	送信	送信
属性 [46]	Acct-Session-Time	非送信	送信	送信
属性 [49]	Acct-Terminate-Cause	非送信	非送信	送信
属性 [61]	NAS-Port-Type	送信	送信	送信

<sup>11</sup> 有効な静的 IP アドレスが設定されているか、ホストに対する Dynamic Host Control Protocol (DHCP) バインディングが DHCP スヌーピング バインディング テーブルに存在している場合に、Framed-IP-Address の AV ペアが送信されます。

## 802.1x 準備状態チェック

802.1x 準備状態チェックは、すべてのスイッチ ポートの 802.1x アクティビティをモニタリングし、802.1x をサポートするポートに接続されているデバイスの情報を表示します。この機能を使用して、スイッチ ポートに接続されているデバイスが 802.1x に対応できるかどうかを判

別できます。802.1x 機能をサポートしていないデバイスでは、MAC 認証バイパスまたは Web 認証などの代替認証を使用します。

この機能が有用なのは、クライアントのサブリカントで NOTIFY EAP 通知パケットでのクエリーがサポートされている場合だけです。クライアントは、802.1x タイムアウト値内に応答しなければなりません。

## スイッチと RADIUS サーバー間の通信

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号によって識別します。IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、同一 IP アドレスのサーバ上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。同じ RADIUS サーバ上の異なる 2 つのホスト エントリに同じサービス（たとえば認証）を設定した場合、2 番めに設定されたホスト エントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作します。RADIUS ホスト エントリは、設定した順序に従って試行されます。

## VLAN 割り当てを使用した 802.1x 認証

スイッチは、VLAN 割り当てを使用した 802.1x 認証をサポートしています。ポートの 802.1x 認証が成功すると、RADIUS サーバは VLAN 割り当てを送信し、スイッチ ポートを設定します。RADIUS サーバ データベースは、ユーザー名と VLAN のマッピングを維持し、スイッチ ポートに接続するクライアントのユーザー名に基づいて VLAN を割り当てます。この機能を使用して、特定のユーザーのネットワーク アクセスを制限できます。

音声デバイス認証は、Cisco IOS Release 12.2(37)SE のマルチドメイン ホスト モードでサポートされています。Cisco IOS Release 12.2(40)SE 以降、音声デバイスが許可されており、RADIUS サーバが許可された VLAN を返した場合、割り当てられた音声 VLAN 上でパケットを送受信するようにポート上の音声 VLAN が設定されます。音声 VLAN 割り当ては、マルチドメイン認証 (MDA) 対応のポートでのデータ VLAN 割り当てと同じように機能します。

スイッチと RADIUS サーバ上で設定された場合、VLAN 割り当てを使用した 802.1x 認証には次の特性があります。

- RADIUS サーバから VLAN が提供されない場合、または 802.1x 認証がディセーブルの場合、認証が成功するとポートはアクセス VLAN に設定されます。アクセス VLAN とは、アクセス ポートに割り当てられた VLAN です。このポート上で送受信されるパケットはすべて、この VLAN に所属します。
- 802.1x 認証がイネーブルで、RADIUS サーバからの VLAN 情報が有効でない場合、認証に失敗して、設定済みの VLAN が引き続き使用されます。これにより、設定エラーによって不適切な VLAN に予期せぬポートが現れることを防ぎます。

設定エラーには、ルーテッドポートの VLAN、間違った VLAN ID、存在しないまたは内部 (ルーテッドポート) の VLAN ID、RSPAN VLAN、シャットダウンしている VLAN、あるいは一時停止している VLAN ID の指定などがあります。マルチドメイン ホストポートの場合、設定エラーには、設定済みまたは割り当て済み VLAN ID と一致するデータ VLAN の割り当て試行（またはその逆）のために発生するものもあります。



- 802.1x 認証がイネーブルで、RADIUS サーバからのすべての情報が有効の場合、許可されたデバイスは認証後、指定した VLAN に配置されます。
- 802.1x ポートでマルチ ホスト モードがイネーブルの場合、すべてのホストは最初に認証されたホストと同じ VLAN (RADIUS サーバにより指定) に配置されます。
- ポート セキュリティをイネーブル化しても、RADIUS サーバが割り当てられた VLAN の動作には影響しません。
- 802.1x 認証がポートでディセーブルの場合、設定済みのアクセス VLAN と設定済みの音声 VLAN に戻ります。
- 802.1x ポートが認証され、RADIUS サーバによって割り当てられた VLAN に配置されると、そのポートのアクセス VLAN 設定への変更は有効になりません。マルチドメインホストの場合、ポートが完全にこれらの例外で許可されている場合、同じことが音声デバイスに適用されます。
  - あるデバイスで VLAN 設定を変更したことにより、他のデバイスに設定済みまたは割り当て済みの VLAN と一致した場合、ポート上の全デバイスの認証が中断して、データおよび音声デバイスに設定済みの VLAN が一致しなくなるような有効な設定が復元されるまで、マルチドメインホストモードがディセーブルになります。
  - 音声デバイスが許可されて、ダウンロードされた音声 VLAN を使用している場合、音声 VLAN 設定を削除したり設定値を *dot1p* または *untagged* に修正したりすると、音声デバイスが未許可になり、マルチドメインホストモードがディセーブルになります。

ポートが、強制許可 (force-authorized) ステート、強制無許可 (force-unauthorized) ステート、無許可ステート、またはシャットダウンステートの場合、ポートは設定済みのアクセス VLAN に配置されます。

VLAN 割り当てを設定するには、次の作業を実行する必要があります。

- **network** キーワードを使用して AAA 認証をイネーブルにし、RADIUS サーバからのインターフェイス設定を可能にします。
- 802.1x 認証をイネーブルにします。(アクセスポートで 802.1x 認証を設定すると、VLAN 割り当て機能は自動的にイネーブルになります)。
- RADIUS サーバにベンダー固有のトンネル属性を割り当てます。RADIUS サーバは次の属性をスイッチに返す必要があります。
  - [64] Tunnel-Type = VLAN
  - [65] Tunnel-Medium-Type = 802
  - [81] Tunnel-Private-Group-ID = VLAN 名または VLAN ID
  - [83] Tunnel-Preference

属性 [64] は、値 *VLAN* (タイプ 13) でなければなりません。属性 [65] は、値 802 (タイプ 6) でなければなりません。属性 [81] は、IEEE 802.1x 認証ユーザに割り当てられた *VLAN* 名または *VLAN ID* を指定します。

## ユーザー単位 ACL を使用した 802.1x 認証

ユーザー単位アクセスコントロールリスト (ACL) をイネーブルにして、異なるレベルのネットワーク アクセスおよびサービスを 802.1x 認証ユーザーに提供できます。RADIUS サーバーは、802.1x ポートに接続されるユーザーを認証する場合、ユーザー ID に基づいて ACL 属性を受け取り、これらをスイッチに送信します。スイッチは、ユーザーセッションの期間中、その属性を 802.1x ポートに適用します。セッションが終了すると、認証が失敗した場合、またはリンクダウン状態の発生時に、ユーザー単位 ACL 設定が削除されます。スイッチは、RADIUS 指定の ACL を実行コンフィギュレーションには保存しません。ポートが無許可の場合、スイッチはそのポートから ACL を削除します。

ユーザーは同一のスイッチ上で、ルータ ACL および入力ポート ACL を使用できます。ただし、ポートの ACL はルータ ACL より優先されます。入力ポート ACL を VLAN に属するインターフェイスに適用する場合、ポート ACL は VLAN インターフェイスに適用する入力ルータ ACL よりも優先されます。ポート ACL が適用されたポート上で受信した着信パケットは、ポート ACL によってフィルタリングされます。その他のポートに着信したルーテッドパケットは、ルータ ACL によってフィルタリングされます。発信するルーテッドパケットには、ルータ ACL のフィルタが適用されます。コンフィギュレーションの矛盾を回避するには、RADIUS サーバーに保存するユーザー プロファイルを慎重に計画しなければなりません。

RADIUS は、ベンダー固有属性などのユーザー単位属性をサポートします。ベンダー固有属性 (VSA) は、オクテット スtring 形式で、認証プロセス中にスイッチに渡されます。ユーザー単位 ACL に使用される VSA は、入力方向では `inacl#<n>` で、出力方向では `outacl#<n>` です。MAC ACL は、入力方向に限りサポートされます。VSA は入力方向に限りサポートされません。レイヤ 2 ポートの出力方向ではポート ACL をサポートしません。

拡張 ACL 構文形式だけを使用して、RADIUS サーバに保存するユーザー単位コンフィギュレーションを定義します。RADIUS サーバから定義が渡される場合、拡張命名規則を使用して作成されます。ただし、Filter-Id 属性を使用する場合、標準 ACL を示すことができます。

Filter-Id 属性を使用して、すでにスイッチに設定されているインバウンドまたはアウトバウンド ACL を指定できます。属性には、ACL 番号と、その後ろに入力フィルタリング、出力フィルタリングを示す `.in` または `.out` が含まれています。RADIUS サーバが `.in` または `.out` 構文を許可しない場合、アクセスリストはデフォルトで発信 ACL に適用されます。RADIUS サーバから送信された Filter-Id がデバイスで設定されていない場合、ユーザーは未承認としてマークされます。スイッチでの Cisco IOS のアクセスリストに関するサポートが制限されているため、Filter-ID 属性は 1 ~ 199 (IP 標準 ACL) および 1300 ~ 2699 (IP 拡張 ACL) の範囲の IP ACL に対してだけサポートされます。

ユーザー単位 ACL の最大サイズは、4000 ASCII 文字ですが、RADIUS サーバのユーザー単位 ACL の最大サイズにより制限されます。

ユーザー単位の ACL を設定するには、次の前提条件を満たす必要があります。

- AAA 認証をイネーブルにします。
- **network** キーワードを使用して AAA 認証をイネーブルにし、RADIUS サーバからのインターフェイス設定を可能にします。
- 802.1x 認証をイネーブルにします。

- RADIUS サーバにユーザ プロファイルと VSA を設定します。
- 802.1x ポートをシングル ホスト モードに設定します。



(注) ユーザー単位 ACL がサポートされるのはシングル ホスト モードだけです。

## ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証

ACL およびリダイレクト URL は、ホストの 802.1x 認証または MAC 認証バイパス中に、RADIUS サーバーからスイッチにダウンロードできます。また、Web 認証中に ACL をダウンロードすることもできます。



(注) ダウンロード可能な ACL は *dACL* と呼ばれます。

ACL およびリダイレクト URL は、802.1x 対応のポートに接続されるすべてのデバイスに適用できます。

ACL が 802.1x 認証中にダウンロードされない場合、スイッチは、ポートのスタティックデフォルト ACL をホストに適用します。マルチ認証モードまたは MDA モードで設定された音声 VLAN ポートでは、スイッチは ACL を認証ポリシーの一部として電話にだけ適用します。

URL リダイレクト ACL の場合：

- 許可アクセス コントロール エントリ (ACE) ルールに一致するパケットは、AAA サーバーに転送するために CPU に送信されます。
- 拒否 ACE ルールに一致するパケットは、スイッチを介して転送されます。
- 許可 ACE ルールにも拒否 ACE ルールにも一致しないパケットは、次の *dACL* によって処理されます。*dACL* がない場合、パケットは暗黙的拒否 ACL にヒットしてドロップされません。

## VLAN ID ベース MAC 認証

ダウンロード可能な VLAN ではなくスタティック VLAN ID に基づいてホストを認証する場合、VLAN ID ベース MAC 認証を使用できます。スタティック VLAN ポリシーがスイッチで設定されている場合、認証用の各ホストの MAC アドレスとともに、VLAN 情報が IAS

(Microsoft) RADIUS サーバーに送信されます。接続ポートに設定されている VLAN ID は MAC 認証に使用されます。VLAN ID ベース MAC 認証を IAS サーバーで使用することで、ネットワークで一定数の VLAN を使用できます。

機能は、STP によってモニターおよび処理される VLAN の数も制限します。ネットワークは固定 VLAN として管理できます。

## ゲスト VLAN を使用した 802.1x 認証

スイッチ上の各 802.1x ポートにゲスト VLAN を設定し、クライアントに対して限定的なサービスを提供できます (802.1x クライアントのダウンロードなど)。これらのクライアントは 802.1x 認証用にシステムをアップグレードできる場合がありますが、一部のホスト (Windows 98 システムなど) は IEEE 802.1x 対応ではありません。

スイッチが EAP Request/Identity フレームに対する応答を受信していない場合、または EAPOL パケットがクライアントによって送信されない場合に、802.1x ポート上でゲスト VLAN をイネーブルにすると、スイッチはクライアントにゲスト VLAN を割り当てます。

スイッチは EAPOL パケット履歴を保持します。EAPOL パケットがリンクの存続時間中にインターフェイスで検出された場合、スイッチはそのインターフェイスに接続されているデバイスが IEEE 802.1x 対応のものであると判断します。インターフェイスはゲスト VLAN ステートにはなりません。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。EAPOL パケットがインターフェイスで検出されない場合、そのインターフェイスはゲスト VLAN のステートになります。

スイッチが 802.1x 対応の音声デバイスを許可しようとしたが、AAA サーバーが使用できない場合、許可は失敗します。ただし、EAPOL パケットの検出は EAPOL 履歴に保存されます。この音声デバイスは、AAA サーバーが使用可能になると許可されます。ただし、他のデバイスによるゲスト VLAN へのアクセスは許可されなくなります。この状況を防ぐには、次のいずれかのコマンドシーケンスを使用します。

- **authentication event no-response action authorize vlan *vlan-id*** インターフェイス コンフィギュレーション コマンドを入力し、ゲスト VLAN へのアクセスを許可します。
- **shutdown** インターフェイス コンフィギュレーション コマンドを入力し、さらに **noshutdown** インターフェイス コンフィギュレーション コマンドを入力してポートを再起動します。

リンクの存続時間中にデバイスが EAPOL パケットを送信した場合、スイッチはゲスト VLAN への認証アクセスに失敗したクライアントを許可しません。



- (注) インターフェイスがゲスト VLAN に変わってから EAPOL パケットが検出された場合、無許可ステートに戻って 802.1x 認証を再起動します。

スイッチ ポートがゲスト VLAN に変わると、802.1x 非対応クライアントはすべてアクセスを許可されます。ゲスト VLAN が設定されているポートに 802.1x 対応クライアントが加入すると、ポートは、ユーザ設定によるアクセス VLAN で無許可ステートになり、認証が再起動されます。

ゲスト VLAN は、単一のホスト、複数のホスト、複数認証、またはマルチドメイン モードにおける 802.1x ポートでサポートされています。

RSPAN VLAN、プライベート VLAN、音声 VLAN を除いて、アクティブ VLAN を 802.1x ゲスト VLAN として設定できます。ゲスト VLAN 機能は、内部 VLAN (ルーテッドポート) またはトランクポートではサポートされていません。アクセスポート上でだけサポートされます。

スイッチは MAC 認証バイパスをサポートします。MAC 認証バイパスが 802.1x ポートでイネーブルの場合、スイッチは、IEEE 802.1x 認証のタイムアウト時に EAPOL メッセージ交換を待機している間、クライアント MAC アドレスに基づいてクライアントを許可できます。スイッチは、802.1x ポート上のクライアントを検出したあとで、クライアントからのイーサネットパケットを待機します。スイッチは、MAC アドレスに基づいたユーザー名およびパスワードを持つ RADIUS-access/request フレームを認証サーバーに送信します。認証に成功すると、スイッチ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。認証に失敗すると、スイッチはポートにゲスト VLAN を割り当てます（指定されていない場合）。

## 制限付き VLAN を使用した 802.1x 認証

ゲスト VLAN にアクセスできないクライアント向けに、限定されたサービスを提供するために、スイッチスタックまたはスイッチの各 IEEE 802.1x ポートに対して制限付き VLAN（認証失敗 VLAN と呼ばれることもあります）を設定できます。これらのクライアントは、認証プロセスに失敗したため他の VLAN にアクセスできない 802.1x 対応クライアントです。制限付き VLAN を使用すると、認証サーバーの有効なクレデンシャルを持っていないユーザ（通常、企業にアクセスするユーザ）に、サービスを制限したアクセスを提供できます。管理者は制限付き VLAN のサービスを制御できます。



- (注) 両方のタイプのユーザに同じサービスを提供する場合、ゲスト VLAN と制限付き VLAN の両方を同じに設定できます。

この機能がないと、クライアントは認証失敗を永遠に繰り返すことになるため、スイッチポートがスパンニングツリーのブロッキングステートから変わることができなくなります。制限付き VLAN の機能を使用することで、クライアントの認証試行回数を指定し（デフォルト値は 3 回）、一定回数後にスイッチポートを制限付き VLAN の状態に移行させることができます。

認証サーバーはクライアントの認証試行回数をカウントします。このカウントが設定した認証試行回数を超えると、ポートが制限付き VLAN の状態に変わります。失敗した試行回数は、RADIUS サーバが *EAP failure* で応答したときや、EAP パケットなしの空の応答を返したときからカウントされます。ポートが制限付き VLAN に変わったら、このカウント数はリセットされます。

認証に失敗したユーザの VLAN は、もう一度認証を実行するまで制限された状態が続きます。VLAN 内のポートは設定された間隔に従って再認証を試みます（デフォルトは 60 秒）。再認証に失敗している間は、ポートの VLAN は制限された状態が続きます。再認証に成功した場合、ポートは設定された VLAN もしくは RADIUS サーバによって送信された VLAN に移行します。再認証はディセーブルにすることもできますが、ディセーブルにすると、*link down* または *EAP logoff* イベントを受信しない限り、ポートの認証プロセスを再起動できません。クライアントがハブを介して接続している場合、再認証機能はイネーブルにしておくことを推奨します。クライアントの接続をハブから切り離すと、ポートに *link down* や *EAP logoff* イベントが送信されない場合があります。

ポートが制限付き VLAN に移行すると、EAP 成功の疑似メッセージがクライアントに送信されます。このメッセージによって、繰り返し実行している再認証を停止させることができま

す。クライアントによっては（Windows XPが稼働しているデバイスなど）、EAPなしでDHCPを実装できません。

制限付き VLAN は、すべてのホストモードでの 802.1x ポート上、およびレイヤ 2 ポート上でサポートされます。

RSPAN VLAN、プライマリプライベート VLAN、音声 VLAN を除いて、アクティブ VLAN を 802.1x 制限付き VLAN として設定できます。制限付き VLAN 機能は、内部 VLAN（ルーテッドポート）またはトランクポートではサポートされていません。アクセスポート上でだけサポートされます。

ダイナミック ARP インスペクション、DHCP スヌーピング、IP 送信元ガードなどの他のセキュリティポート機能は、制限付き VLAN に対して個別に設定できます。

## アクセス不能認証バイパスを使用した 802.1x 認証

スイッチが設定された RADIUS サーバーに到達できず、新しいホストを認証できない場合、アクセス不能認証バイパス機能を使用します。この機能は、クリティカル認証または AAA 失敗ポリシーとも呼ばれます。これらのホストをクリティカルポートに接続するようにスイッチを設定できます。

新しいホストがクリティカルポートに接続しようとする、そのホストはユーザ指定のアクセス VLAN、クリティカル VLAN に移動されます。管理者はこれらのホストに制限付き認証を付与します。

スイッチは、クリティカルポートに接続されているホストを認証しようとする場合、設定されている RADIUS サーバーのステータスをチェックします。利用可能なサーバーが 1 つあれば、スイッチはホストを認証できます。ただし、すべての RADIUS サーバーが利用不可能な場合は、スイッチはホストへのネットワークアクセスを許可して、ポートを認証ステートの特別なケースであるクリティカル認証ステートにします。



- 
- (注) クリティカル認証をインターフェイスで設定する場合は、クリティカル承認（クリティカル *vlan*）に使用する *vlan* をスイッチでアクティブにする必要があります。クリティカル *vlan* が非アクティブまたはダウンしていると、クリティカル認証セッションは非アクティブな *vlan* の有効化を試行し続け、繰り返し失敗します。これは大量のメモリ保持の原因となる可能性があります。
- 

## 複数認証ポートのアクセス不能認証バイパスのサポート

ポートが任意のホストモードで設定されていて、AAA サーバーを使用できない場合、ポートはマルチホストモードに設定され、クリティカル VLAN に移動されます。マルチ認証（*multiauth*）ポートで、このアクセス不能バイパスをサポートするには、**authentication event server dead action reinitialize vlan *vlan-id*** コマンドを使用します。新しいホストがクリティカルポートに接続しようとする、そのポートは再初期化され、接続されているすべてのホストがユーザ指定のアクセス VLAN に移動されます。

このコマンドは、すべてのホスト モードでサポートされます。

## アクセス不能認証バイパスの認証結果

アクセス不能認証バイパス機能の動作は、ポートの許可ステートにより異なります。

- クリティカルポートに接続されているホストが認証しようとする際にポートが無許可ですべてのサーバーが利用できない場合、スイッチはRADIUS設定済みVLANまたはユーザー指定のアクセスVLANにあるポートをクリティカル認証ステートにします。
- ポートが許可済みで、再認証が行われた場合、スイッチは現在のVLAN（事前にRADIUSサーバーにより割り当てられた）でクリティカルポートをクリティカル認証ステートにします。
- 認証交換中にRADIUSサーバーが利用不可能となった場合、現在の交換はタイムアウトとなり、スイッチは次の認証試行の間にクリティカルポートをクリティカル認証ステートとします。

RADIUSサーバーが再び使用可能になったときにホストを再初期化し、クリティカルVLANから移動するように、クリティカルポートを設定できます。このように設定した場合、クリティカル認証ステートのすべてのクリティカルポートは自動的に再認証されます。

## アクセス不能認証バイパス機能の相互作用

アクセス不能認証バイパスは、次の機能と相互に作用します。

- **ゲスト VLAN** : アクセス不能認証バイパスは、ゲスト VLAN と互換性があります。ゲスト VLAN が 8021.x ポートでイネーブルの場合、この機能は次のように相互に作用します。
  - スイッチが EAP Request/Identity フレームへの応答を受信しないとき、または EAPOL パケットがクライアントによって送信されないときに、少なくとも 1 つの RADIUS サーバーが使用できれば、スイッチはクライアントにゲスト VLAN を割り当てます。
  - すべての RADIUS サーバーが使用できず、クライアントがクリティカルポートに接続されている場合、スイッチはクライアントを認証して、クリティカルポートを RADIUS 認証済み VLAN またはユーザー指定のアクセス VLAN でクリティカル認証ステートにします。
  - すべての RADIUS サーバーが使用できず、クライアントがクリティカルポートに接続されていない場合、ゲスト VLAN が設定されていても、スイッチはクライアントにゲスト VLAN を割り当てられません。
  - すべての RADIUS サーバーが使用できず、クライアントがクリティカルポートに接続されていて、すでにゲスト VLAN が割り当てられている場合、スイッチはそのポートをゲスト VLAN に保持します。
- **制限付き VLAN** : ポートがすでに制限付き VLAN で許可されていて RADIUS サーバーが使用できない場合、スイッチはクリティカルポートを制限付き VLAN でクリティカル認証ステートにします。

- 802.1x アカウンティング：RADIUS サーバーが使用できない場合、アカウンティングは影響を受けません。
- プライベート VLAN：プライベート VLAN ホスト ポートにアクセス不能認証バイパスを設定できます。アクセス VLAN は、セカンダリ VLAN でなければなりません。
- 音声 VLAN：アクセス不能認証バイパスは音声 VLAN と互換性がありますが、RADIUS 設定済み VLAN またはユーザー指定のアクセス VLAN は、音声 VLAN と異ならないければなりません。
- Remote Switched Port Analyzer (RSPAN)：アクセス不能認証バイパスの RADIUS 設定またはユーザー指定のアクセス VLAN として RSPAN VLAN を指定しないでください。

## 802.1x クリティカル音声 VLAN

ポートに接続されている IP フォンが Cisco Identity Services Engine (ISE) によって認証される際、その IP フォンは音声ドメインに参加します。ISE が到達不能である場合、スイッチはデバイスが音声デバイスなのかどうかを判断できません。サーバーが使用できない場合、電話機は音声ネットワークにアクセスできないため、動作できません。

データトラフィックの場合、アクセス不能認証バイパス（クリティカル認証）を設定し、サーバーが使用できない場合にトラフィックがネイティブ VLAN を通過できるようにすることができます。RADIUS 認証サーバーが使用できず（ダウンして）、アクセスできない認証バイパスがイネーブルの場合、スイッチは、クライアントにネットワークのアクセスを許可し、RADIUS 設定 VLAN またはユーザー指定アクセス VLAN でポートをクリティカル認証ステータスにします。設定された RADIUS サーバーにスイッチが到達できず、新しいホストを認証できない場合、スイッチはこれらのホストをクリティカルポートに接続します。クリティカルポートに接続を試行している新しいホストは、ユーザー指定のアクセス VLAN（クリティカル VLAN）に移動され、制限付き認証を許可されます。

**authentication event server dead action authorize voice** インターフェイス コンフィギュレーション コマンドを使用して、クリティカル音声 VLAN 機能を設定できます。ISE が応答しない場合、ポートはクリティカル認証モードになります。ホストからのトラフィックが音声 VLAN でタグ付けされると、接続デバイス（電話機）は、ポートに対して設定された音声 VLAN に配置されます。IP フォンは Cisco Discovery Protocol（シスコデバイス）や LLDP または DHCP を介して音声 VLAN ID を学習します。

**switchport voice vlan vlan-id** インターフェイス コンフィギュレーション コマンドを入力して、ポートの音声 VLAN を設定できます。

この機能は、マルチドメイン モードおよびマルチ認証ホスト モードでサポートされます。スイッチがシングルホスト モードまたはマルチホスト モードの場合にコマンドを入力できますが、デバイスがマルチドメインまたはマルチ認証ホスト モードに変わらない限りコマンドは無効になりません。



## 802.1x ユーザ ディストリビューション

802.1x ユーザ ディストリビューションを設定すると、複数の異なる VLAN で同じグループ名のユーザのロード バランシングを行うことができます。

VLAN は、RADIUS サーバーにより提供されるか、VLAN グループ名でスイッチ CLI を介して設定します。

- RADIUS サーバを設定して、ユーザの複数の VLAN 名を送信します。複数の VLAN 名は、ユーザへの応答の一部として送信できます。802.1x ユーザ ディストリビューションは、特定の VLAN のすべてのユーザを追跡し、許可されたユーザをユーザ数が最も少ない VLAN に移動することでロード バランシングを行います。
- RADIUS サーバを設定してユーザの VLAN グループ名を送信します。VLAN グループ名は、ユーザへの応答の一部として送信できます。スイッチ CLI を使用して設定した VLAN グループ名で、選択された VLAN グループ名を検索できます。VLAN グループ名が検出されると、この VLAN グループ名で対応する VLAN を検索して、ユーザ数が最も少ない VLAN が検出されます。ロード バランシングは、対応する許可済みユーザをその VLAN に移動することで行われます。



(注) RADIUS サーバーは、VLAN-ID、VLAN 名または VLAN グループを任意に組み合わせて VLAN 情報を送信できます。

### 802.1x ユーザ ディストリビューションの設定時の注意事項

- 少なくとも1つの VLAN が VLAN グループにマッピングされることを確認してください。
- 複数の VLAN を VLAN グループにマッピングできます。
- VLAN を追加または削除することで、VLAN グループを変更できます。
- 既存の VLAN を VLAN グループ名からクリアする場合、VLAN の認証済みポートはクリアされませんが、既存の VLAN グループからマッピングが削除されます。
- 最後の VLAN を VLAN グループ名からクリアすると、VLAN グループがクリアされます。
- アクティブ VLAN がグループにマッピングされても VLAN グループをクリアできます。VLAN グループをクリアすると、グループ内で任意の VLAN の認証ステートであるポートまたはユーザはクリアされませんが、VLAN の VLAN グループへのマッピングはクリアされます。

## 音声 VLAN ポートを使用した IEEE 802.1x 認証

音声 VLAN ポートは特殊なアクセス ポートで、次の2つの VLAN ID が対応付けられています。

- IP Phone との間で音声トラフィックを伝送する VVID。VVID は、ポートに接続された IP Phone を設定するために使用されます。
- IP Phone を通じて、スイッチと接続しているワークステーションとの間でデータトラフィックを伝送する PVID。PVID は、ポートのネイティブ VLAN です。

ポートの許可ステートにかかわらず、IP Phone は音声トラフィックに対して VVID を使用します。これにより、IP Phone は IEEE 802.1x 認証とは独立して動作できます。

シングルホストモードでは、IP Phone だけが音声 VLAN で許可されます。マルチホストモードでは、サブリカントが PVID で認証された後、追加のクライアントがトラフィックを音声 VLAN 上で送信できます。マルチホストモードがイネーブルの場合、サブリカント認証は PVID と VVID の両方に影響します。

リンクがあるとき、音声 VLAN ポートはアクティブになり、IP Phone からの最初の CDP メッセージを受け取るとデバイスの MAC アドレスが表示されます。Cisco IP Phone は、他のデバイスから受け取った CDP メッセージをリレーしません。その結果、複数の IP Phone が直列に接続されている場合、スイッチは直接接続されている 1 台の IP Phone のみを認識します。音声 VLAN ポートで IEEE 802.1x 認証がイネーブルの場合、スイッチは 2 ホップ以上離れた認識されない IP Phone からのパケットをドロップします。

IEEE 802.1x 認証をスイッチポート上でイネーブルにすると、音声 VLAN でもあるアクセスポート VLAN を設定できます。

IP 電話がシングルホストモードで 802.1x 対応のスイッチポートに接続されている場合、スイッチは認証を行わずに電話ネットワークアクセスを承認します。ポートで Multidomain Authentication (MDA) を使用して、データデバイスと IP フォンなどの音声デバイスの両方を認証することを推奨します。



- (注) 音声 VLAN が設定され、Cisco IP Phone が接続されているアクセスポートで IEEE 802.1x 認証をイネーブルにした場合、Cisco IP Phone のスイッチへの接続が最大 30 秒間失われます。

## VoL 機能を使用した IEEE 802.1x 認証

IEEE 802.1x 認証の Wake-on-LAN (WoL) 機能を使用すると、スイッチにマジックパケットと呼ばれる特定のイーサネットフレームを受信させて、休止状態の PC を起動させることができます。この機能は、管理者が休止状態のシステムへ接続しなければならない場合に役立ちます。

WoL を使用するホストが IEEE 802.1x ポートを通じて接続され、ホストの電源がオフになると、IEEE 802.1x ポートは無許可になります。無許可になったポートは EAPOL パケットしか送受信できないため、WoL マジックパケットはホストに届きません。さらに PC が休止状態になると、PC が認証されなくなるため、スイッチポートは閉じたままになります。

スイッチが WoL 機能を有効にした IEEE 802.1x 認証を使用している場合、スイッチはマジックパケットを含むトラフィックを無許可の IEEE 802.1x ポートに転送します。ポートが無許可の

間、スイッチは EAPOL パケット以外の入力トラフィックをブロックし続けます。ホストはパケットを受信できますが、パケットをネットワーク内にある他のデバイスに送信できません。



- (注) PortFast がポートでイネーブルになっていないと、そのポートは強制的に双方向ステートになります。

**authentication control-direction in** インターフェイス コンフィギュレーション コマンドを使用してポートを単一方向として設定すると、ポートはスパニングツリーフォワーディングステートに変更されます。ポートは、ホストにパケットを送信できますが、受信はできません。

**authentication control-direction both** インターフェイス コンフィギュレーション コマンドを使用してポートを双方向として設定すると、ポートは、両方向でアクセスコントロールされます。ポートは、ホストとの間でパケットを送受信しません。

## MAC 認証バイパスを使用した IEEE 802.1x 認証

MAC 認証バイパス機能を使用し、クライアント MAC アドレスに基づいてクライアントを許可するようにスイッチを設定できます。たとえば、プリンタなどのデバイスに接続された IEEE 802.1x ポートでこの機能をイネーブルにできます。

クライアントからの EAPOL 応答の待機中に IEEE 802.1x 認証がタイムアウトした場合、スイッチは MAC 認証バイパスを使用してクライアントを許可しようとします。

MAC 認証バイパス機能が IEEE 802.1x ポートでイネーブルの場合、スイッチはクライアント ID として MAC アドレスを使用します。認証サーバーには、ネットワーク アクセスを許可されたクライアント MAC アドレスのデータベースがあります。スイッチは、IEEE 802.1x ポート上のクライアントを検出した後で、クライアントからのイーサネットパケットを待機します。スイッチは、MAC アドレスに基づいたユーザー名およびパスワードを持つ RADIUS-access/request フレームを認証サーバーに送信します。認証に成功すると、スイッチはクライアントにネットワークへのアクセスを許可します。許可が失敗した場合、ゲスト VLAN が設定されていれば、スイッチはポートをゲスト VLAN に割り当てます。このプロセスは、ほとんどのクライアントデバイスで動作します。ただし、代替の MAC アドレス形式を使用しているクライアントでは動作しません。標準の形式とは異なる MAC アドレスを持つクライアントに対して MAB 認証をどのように実行するかや、RADIUS の設定のどこでユーザー名とパスワードが異なるかが要求されるかを設定できます。

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上で検出された場合、スイッチは、そ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確認し、(MAC 認証バイパス機能ではなく) 802.1x 認証を使用してインターフェイスを認証します。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。

スイッチがすでに MAC 認証バイパスを使用してポートを許可し、IEEE 802.1x サブリカントを検出している場合、スイッチはポートに接続されているクライアントを許可します。再認証が発生するときに、Termination-Action RADIUS 属性値が DEFAULT であるために前のセッションが終了した場合、スイッチはポートに設定されている認証または再認証手法を使用します。

MAC 認証バイパスで認証されたクライアントは再認証できます。再認証プロセスは、IEEE 802.1x を使用して認証されたクライアントに対するプロセスと同じです。再認証中は、ポートは前に割り当てられた VLAN のままです。再認証に成功すると、スイッチはポートを同じ VLAN に保持します。再認証に失敗した場合、ゲスト VLAN が設定されていれば、スイッチはポートをゲスト VLAN に割り当てます。

再認証が Session-Timeout RADIUS 属性 (Attribute[27])、および Termination-Action RADIUS 属性 (Attribute[29]) に基づいて行われるときに、Termination-Action RADIUS 属性 (Attribute[29]) のアクションが *Initialize* (属性値は *DEFAULT*) である場合、MAC 認証バイパスセッションは終了し、再認証の間の接続は失われます。MAC 認証バイパス機能が IEEE 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認証を開始します。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、次の機能と相互に作用します。

- IEEE 802.1x 認証：802.1x 認証がポートでイネーブルの場合にのみ MAC 認証バイパスをイネーブルにできます。
- ゲスト VLAN：クライアントの MAC アドレス ID が無効な場合、ゲスト VLAN が設定されていれば、スイッチは VLAN にクライアントを割り当てます。
- 制限付き VLAN：IEEE 802.1x ポートに接続されているクライアントが MAC 認証バイパスで認証されている場合には、この機能はサポートされません。
- ポート セキュリティ
- 音声 VLAN
- プライベート VLAN：クライアントをプライベート VLAN に割り当てられます。
- Network Edge Access Topology (NEAT)：MAB と NEAT は相互に排他的です。インターフェイス上で NEAT が有効の場合は、MAB を有効にすることはできません。また、インターフェイス上で MAB が有効の場合は、NEAT を有効にすることはできません。

Cisco IOS Release 12.2(55)SE 以降では、冗長 MAB システム メッセージのフィルタリングをサポートします。

## Network Admission Control レイヤ 2 IEEE 802.1x 検証

スイッチは、デバイスのネットワーク アクセスを許可する前にエンドポイント システムやクライアントのウイルス対策の状態またはポスチャを調べる Network Admission Control (NAC) レイヤ 2 IEEE 802.1x 検証をサポートしています。NAC レイヤ 2 IEEE 802.1x 検証を使用すると、以下の作業を実行できます。

- Session-Timeout RADIUS 属性 (属性 [27]) と Termination-Action RADIUS 属性 (属性 [29]) を認証サーバーからダウンロードします。
- Session-Timeout RADIUS 属性 (属性 [27]) の値として再認証試行間の秒数を指定し、RADIUS サーバーからクライアントのアクセス ポリシーを取得します。

- スイッチが Termination-Action RADIUS 属性（属性[29]）を使用してクライアントを再認証する際のアクションを設定します。値が *DEFAULT* であるか、値が設定されていない場合、セッションは終了します。値が RADIUS 要求の場合、再認証プロセスが開始します。
- VLAN の番号や名前、または VLAN グループ名のリストを Tunnel Group Private ID（属性 [81]）の値として設定し、VLAN の番号や名前、または VLAN グループ名のプリファレンスを Tunnel Preference（属性 [83]）の値として設定します。Tunnel Preference を設定しない場合、最初の Tunnel Group Private ID（属性 [81]）属性がリストから選択されます。
- NAC ポスチャトークンを表示します。これは、**show authentication** 特権 EXEC コマンドを使用して、クライアントのポスチャを示します。
- ゲスト VLAN としてセカンダリ プライベート VLAN を設定します。

NAC レイヤ 2 IEEE 802.1x 検証の設定は、RADIUS サーバーにポスチャ トークンを設定する必要があることを除いて、IEEE 802.1x ポートベース認証と似ています。

## 柔軟な認証の順序設定

柔軟な認証の順序設定を使用して、ポートが新しいホストを認証するときを使用する方法の順序を設定できます。The IEEE 802.1X の柔軟な認証機能では、以下の 3 つの認証方法をサポートしています。

- dot1X : IEEE 802.1X 認証はレイヤ 2 の認証方式です。
- mab : MAC 認証バイパスはレイヤ 2 の認証方式です。
- webauth : Web 認証はレイヤ 3 の認証方式です。

この機能を使用すると、各ポートでどの認証方式を使用するかを制御できます。また、そのポートの方式についてフェールオーバー順も制御できます。たとえば、MAC 認証バイパスおよび 802.1x は、プライマリまたはセカンダリ認証方法として使用し、Web 認証は、これらの認証のいずれか、または両方が失敗した場合のフォールバック方法として使用できます。

The IEEE 802.1X の柔軟な認証機能では、以下のホスト モードをサポートしています。

- multi-auth : マルチ認証では、音声 VLAN に 1 つの認証、データ VLAN に複数の認証を使用できます。
- multi-domain : マルチドメイン認証では、音声 VLAN に 1 つ、データ VLAN に 1 つ、計 2 つの認証を使用できます。

## Open1x 認証

Open1x 認証によって、デバイスが認証される前に、そのデバイスがポートにアクセスできるようになります。オープン認証が設定されている場合、新しいホストはポートに定義されているアクセス コントロールリスト (ACL) に基づいてトラフィックを渡します。ホストが認証されると、RADIUS サーバに設定されているポリシーがそのホストに適用されます。

オープン認証を次の状況で設定できます。

- シングルホストモードでのオープン認証：1人のユーザーだけが認証の前後にネットワークにアクセスできます。
- MDA モードでのオープン認証：音声ドメインの1人のユーザーだけ、およびデータドメインの1人のユーザーだけが許可されます。
- マルチホストモードでのオープン認証：任意のホストがネットワークにアクセスできます。
- 複数認証モードでのオープン認証：MDAの場合と似ていますが、複数のホストを認証できます。



(注) オープン認証が設定されている場合は、他の認証制御よりも優先されます。これは、**authentication open** インターフェイスコンフィギュレーション コマンドを使用した場合、**authentication port-control** インターフェイス コンフィギュレーション コマンドに関係なく、ポートがホストにアクセス権を付与することを意味します。

## マルチドメイン認証

スイッチはマルチドメイン認証 (MDA) をサポートしています。これにより、データ装置と IP Phone などの音声装置 (シスコ製品またはシスコ以外の製品) の両方を同じスイッチポート上で認証できます。ポートはデータドメインと音声ドメインに分割されます。



(注) すべてのホストモードで、ポートベース認証が設定されている場合、ラインプロトコルは許可の前にアップのままです。

MDA では、デバイス認証の順序が指定されません。ただし、最適な結果を得るには、MDA 対応のポート上のデータ デバイスよりも前に音声デバイスを認証することを推奨します。

MDA を設定するときには、次の注意事項に従ってください。

- MDA のスイッチ ポートを設定する必要があります。
- ホスト モードがマルチドメインに設定されている場合、IP Phone の音声 VLAN を設定する必要があります。
- MDA 対応ポートでの音声 VLAN 割り当ては、Cisco IOS Release 12.2(40)SE 以降でサポートされています。

- 音声デバイスを認可するには、値を *device-traffic-class=voice* に設定した Cisco 属性値 (AV) ペア属性を送信するように AAA サーバーを設定する必要があります。この値を使用しない場合、音声デバイスはデータ デバイスとして扱われます。



(注) *traffic-class=voice* が AAA サーバーから *service-template* としてダウンロードされると、音声ドメインではなくデータドメインでセッションが作成されます。

- ゲスト VLAN および制限付き VLAN 機能は、MDA 対応のポートのデータ デバイスだけに適用されます。許可に失敗した音声デバイスは、データ デバイスとして扱われます。
- 複数のデバイスでポートの音声またはデータ ドメインの許可を行おうとすると、*errordisable* になります。
- デバイスが許可されるまで、ポートはそのトラフィックをドロップします。他社製 IP Phone または音声デバイスはデータおよび音声 VLAN の両方に許可されます。データ VLAN では、音声デバイスを DHCP サーバーに接続して IP アドレスおよび音声 VLAN 情報を取得することができます。音声デバイスが音声 VLAN で送信を開始すると、データ VLAN へのアクセスはブロックされます。
- データ VLAN とバインドしている音声デバイス MAC アドレスは、ポートセキュリティ MAC アドレス制限にカウントされません。
- MDA では、IEEE 802.1x 認証をサポートしていないデバイスへのスイッチポートの接続を許可するフォールバック メカニズムとして、MAC 認証バイパスを使用できます。
- データまたは音声デバイスがポートで検出されると、認証に成功するまでその MAC アドレスがブロックされます。許可に失敗した場合、MAC アドレスが 5 分間ブロックされたままになります。
- ポートが未認証中に 6 つ以上のデバイスがデータ VLAN で検出された場合や、複数の音声デバイスが音声 VLAN で検出された場合、ポートは *errdisable* になります。
- ポートのホスト モードをシングルホスト モードまたはマルチホスト モードからマルチドメイン モードに変更すると、ポートでは許可されたデータ デバイスは許可されたままになります。ただし、ポートの音声 VLAN で許可されている Cisco IP Phone は自動的に削除されるので、そのポートでは再認証を行う必要があります。
- ゲスト VLAN や制限付き VLAN などのアクティブ フォールバック メカニズムは、ポートをシングル モードまたはマルチホスト モードからマルチドメイン モードに変更したあとも設定されたままになります。
- ポートのホスト モードをマルチドメイン モードからシングル モードまたはマルチホスト モードに変更すると、許可されているすべてのデバイスがポートから削除されます。
- まずデータ ドメインを許可してゲスト VLAN に参加させる場合、IEEE 802.1x 非対応の音声デバイスは、音声 VLAN のパケットをタグ付けして、認証を開始する必要があります。

- MDA 対応ポートでは、ユーザー単位 ACL を推奨しません。ユーザー単位 ACL ポリシーを備えた、許可されたデバイスは、ポートの音声 VLAN とデータ VLAN の両方のトラフィックに影響を与えることがあります。このようなデバイスを使用する場合は、ポートでユーザー単位 ACL を適用するデバイスは 1 台だけにしてください。

## Network Edge Access Topology (NEAT) を使用した 802.1x サブリカントおよびオーセンティケータ

Network Edge Access Topology (NEAT) 機能は、ワイヤリングクローゼット（会議室など）外の領域まで識別を拡張します。これにより、任意のタイプのデバイスをポートで認証できます。

- 802.1x スイッチ サブリカント：802.1x サブリカント機能を使用することで、別のスイッチのサブリカントとして機能するようにスイッチを設定できます。この設定は、たとえば、スイッチがワイヤリングクローゼット外にあり、トランクポートを介してアップストリームスイッチに接続される場合に役に立ちます。802.1x スイッチ サブリカント機能を使用して設定されたスイッチは、セキュアな接続のためにアップストリームスイッチで認証します。サブリカントスイッチが認証に成功すると、オーセンティケータスイッチでポートモードがアクセスからトランクに変更されます。サブリカントスイッチでは、CISP を有効にするときに手動でトランクを設定する必要があります。
- アクセス VLAN は、オーセンティケータスイッチで設定されている場合、認証が成功した後にトランクポートのネイティブ VLAN になります。

デフォルトでは、BPDU ガードが有効にされたオーセンティケータスイッチにサブリカントのスイッチを接続する場合、オーセンティケータのポートはサブリカントスイッチが認証する前にスパンニングツリープロトコル (STP) のブリッジプロトコルデータユニット (BPDU) を受信した場合、errdisable 状態になる可能性があります。Cisco IOS Release 15.0(1)SE 以降では、認証中にサブリカントのポートから送信されるトラフィックを制御できます。**dot1x supplicant controlled transient** グローバルコンフィギュレーションコマンドを入力すると、認証が完了する前にオーセンティケータポートがシャットダウンすることがないように、認証中に一時的にサブリカントのポートをブロックします。認証に失敗すると、サブリカントのポートが開きます。**no dot1x supplicant controlled transient** グローバルコンフィギュレーションコマンドを入力すると、認証期間中にサブリカントポートが開きます。これはデフォルトの動作です。

BPDU ガードが **spanning-tree bpduguard enable** インターフェイスコンフィギュレーションコマンドによりオーセンティケータのスイッチポートで有効になっている場合、サブリカントスイッチで **dot1x supplicant controlled transient** コマンドを使用することを強く推奨します。



- (注) **spanning-tree portfast bpduguard default** グローバルコンフィギュレーションコマンドを使用して、グローバルにオーセンティケータスイッチで BPDU ガードを有効にした場合、**dot1x supplicant controlled transient** コマンドを入力すると、BPDU の違反が避けられなくなります。



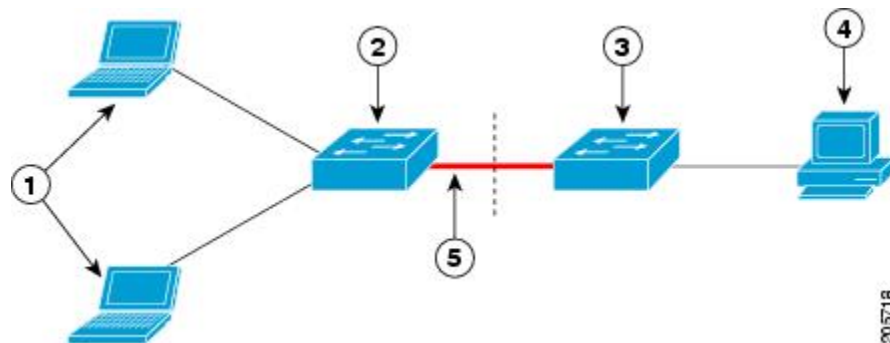
1 つ以上のサプリカント スイッチに接続するオーセンティケータ スイッチ インターフェイスで MDA または `multiauth` モードをイネーブルにできます。マルチホストモードはオーセンティケータ スイッチ インターフェイスではサポートされていません。

インターフェイスで有効になっているシングルホスト モードでオーセンティケータ スイッチをリブートすると、インターフェイスが認証前に `err-disabled` 状態に移行する場合があります。`err-disabled` 状態から回復するには、オーセンティケータ ポートをフラップしてインターフェイスを再度アクティブにし、認証を開始します。

すべてのホストモードで機能するように `dot1x supplicant force-multicast` グローバル コンフィギュレーション コマンドを Network Edge Access Topology (NEAT) のサプリカントスイッチで使用します。

- **ホスト許可**：許可済み（サプリカントでスイッチに接続する）ホストからのトラフィックだけがネットワークで許可されます。これらのスイッチは、Client Information Signalling Protocol (CISP) を使用して、サプリカント スイッチに接続する MAC アドレスをオーセンティケータ スイッチに送信します。
- **自動有効化**：オーセンティケータ スイッチでのトランク コンフィギュレーションを自動的に有効化します。これにより、サプリカントスイッチから着信する複数の VLAN のユーザートラフィックが許可されます。ISE で `cisco-av-pair` を `device-traffic-class=switch` として設定します（この設定は `group` または `user` 設定で行うことができます）。

図 28: CISP を使用したオーセンティケータまたはサプリカントスイッチ



1	ワークステーション (クライアント)	2	サプリカントスイッチ (ワイヤリング クロゼット外)
3	オーセンティケータ スイッチ	4	Cisco ISE
5	トランク ポート		



- (注) **switchport nonegotiate** コマンドは、NEAT を使用したサブリカントおよびオーセンティケータスイッチではサポートされません。このコマンドは、トポロジのサブリカント側で設定しないでください。オーセンティケータサーバ側で設定した場合は、内部マクロによってポートからこのコマンドが自動的に削除されます。

## 音声認識 802.1x セキュリティ



- (注) 音声認識 IEEE 802.1x 認証を使用するには、スイッチが LAN Base イメージを実行している必要があります。

音声認識 802.1x セキュリティ機能を使用して、セキュリティ違反が発生した場合にデータまたは音声 VLAN に関係なく VLAN だけをディセーブルにするようにスイッチを設定します。以前のリリースでは、セキュリティ違反の原因であるデータクライアントを認証しようとする、ポート全体がシャットダウンし、接続が完全に切断されます。

この機能は、PC が IP Phone に接続されている IP Phone 環境で使用できます。データ VLAN でセキュリティ違反が検出されると、データ VLAN だけがシャットダウンされます。音声 VLAN のトラフィックは中断することなくスイッチで送受信されます。

## コモンセッション ID

認証マネージャは、使用された認証方式が何であれ、クライアントの単一のセッション ID (共通セッション ID) を使用します。この ID は、表示コマンドや MIB などのすべてのレポートに使用されます。セッション ID は、セッション単位のすべての Syslog メッセージに表示されません。

セッション ID には、次の情報が含まれます。

- ネットワーク アクセス デバイス (NAD) の IP アドレス
- 一意の 32 ビット整数 (機械的に増加します)
- セッション開始タイム スタンプ (32 ビット整数)

次に、`show authentication` コマンドの出力に表示されたセッション ID の例を示します。この例では、セッション ID は 160000050000000B288508E5 です。

```

デバイス# show authentication sessions
Interface  MAC Address      Method  Domain  Status      Session ID
Fa4/0/4    0000.0000.0203  mab     DATA   Authz Success 160000050000000B288508E5

```

次に、Syslog 出力にセッション ID が表示される例を示します。この例でも、セッション ID は 160000050000000B288508E5 です。

```

1w0d: %AUTHMGR-5-START: Starting 'mab' for client (0000.0000.0203) on Interface Fa4/0/4
AuditSessionID 160000050000000B288508E5
1w0d: %MAB-5-SUCCESS: Authentication successful for client (0000.0000.0203) on Interface
Fa4/0/4 AuditSessionID 160000050000000B288508E5
1w0d: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client
(0000.0000.0203) on Interface Fa4/0/4 AuditSessionID 160000050000000B288508E5

```

セッションIDは、NAD、AAA サーバー、その他のレポート分析アプリケーションでクライアントを識別するために使用されます。ID は自動的に表示されます。設定は必要ありません。

## 802.1x ポートベース認証の設定方法

### 802.1x 認証のデフォルト設定

表 50: 802.1x 認証のデフォルト設定

機能	デフォルト設定
スイッチの 802.1x イネーブル ステート	ディセーブル
ポート単位の 802.1x イネーブル ステート	ディセーブル (force-authorized) ポートはクライアントとの 802.1x ベース認証を行わずにトラフィックを送受信します。
AAA	ディセーブル
RADIUS サーバ <ul style="list-style-type: none"> <li>• IP アドレス</li> <li>• UDP 認証ポート</li> <li>• デフォルトのアカウントिंग ポート</li> <li>• キー</li> </ul>	<ul style="list-style-type: none"> <li>• 指定なし</li> <li>• 1645</li> <li>• 1646</li> <li>• 指定なし</li> </ul>
ホスト モード	シングル ホスト モード
制御方向	双方向制御
定期的な再認証	ディセーブル。
再認証の間隔 (秒)	3600 秒
再認証回数	2 回 (ポートが無許可ステートに変わる前に、スイッチを再開する回数)

機能	デフォルト設定
待機時間	60 秒 (スイッチがクライアントとの認証情報の交換に失敗した場合、待機状態を続ける秒数)
再送信時間	30 秒 (スイッチが EAP-Request/Identity フレームに対するクライア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 (スイッチが認証プロセスを再開する前に、EAP-Request/Identity フレームを送信する回数)
クライアント タイムアウト時間	30 秒 (認証サーバーからの要求をクライアントにリリースするまで、スイッチが返答を待ち、クライアントに要求を再送信するまでの時間)
認証サーバー タイムアウト時間	30 秒 (クライアントからの応答を認証サーバーにリリースするまで、スイッチが応答を待ち、応答をサーバーに再送信するまでの時間)  dot1x timeout server-timeout インターフェイス コンフィギュレーション コマンドを使用して、このタイムアウト時間を変更
無活動タイムアウト	ディセーブル
ゲスト VLAN	指定なし
アクセス不能認証バイパス	ディセーブル
制限付き VLAN	指定なし
オーセンティケータ (スイッチ) モード	指定なし
MAC 認証バイパス	ディセーブル
音声認識セキュリティ	ディセーブル

## 802.1x 認証設定時の注意事項

### 802.1X 認証

802.1x 認証を設定する場合の注意事項は、次のとおりです。

- 802.1x 認証を使用するには、SISF ベースのデバイストラッキングを有効にする必要があります。デフォルトでは、SISF ベースのデバイストラッキングはスイッチで無効になっています。
- 802.1x 認証をイネーブルにすると、他のレイヤ 2 またはレイヤ 3 機能がイネーブルになる前に、ポートが認証されます。

- 802.1x 対応ポートが割り当てられている VLAN が変更された場合、この変更は透過的でスイッチには影響しません。たとえば、ポートが RADIUS サーバに割り当てられた VLAN に割り当てられ、再認証後に別の VLAN に割り当てられた場合に、この変更が発生します。  
802.1x ポートが割り当てられている VLAN がシャットダウン、ディセーブル、または削除される場合、ポートは無許可になります。たとえば、ポートが割り当てられたアクセス VLAN がシャットダウンまたは削除された後、ポートは無許可になります。
- 802.1x プロトコルは、レイヤ 2 スタティックアクセス ポート、音声 VLAN ポート、およびレイヤ 3 ルーテッド ポートでサポートされますが、次のポート タイプではサポートされません。
  - ダイナミック ポート：ダイナミック モードのポートは、ネイバーとトランク ポートへの変更をネゴシエートする場合があります。ダイナミック ポートで 802.1x 認証をイネーブルにしようとする、エラーメッセージが表示され、802.1x 認証はイネーブルになりません。802.1x 対応ポートのモードをダイナミックに変更しようとしても、エラーメッセージが表示され、ポート モードは変更されません。
  - EtherChannel ポート：アクティブまたはアクティブでない EtherChannel メンバを 802.1x ポートとして設定しないでください。EtherChannel ポートで 802.1x 認証をイネーブルにしようとする、エラーメッセージが表示され、802.1x 認証はイネーブルになりません。
  - スイッチド ポート アナライザ (SPAN) およびリモート SPAN (RSPAN) 宛先ポート：SPAN または RSPAN 宛先ポートであるポートの 802.1x 認証をイネーブルにすることができます。ただし、ポートを SPAN または RSPAN 宛先ポートとして削除するまでは、802.1x 認証はディセーブルになります。SPAN または RSPAN 送信元ポートでは 802.1x 認証をイネーブルにすることができます。
- スイッチ上で、**dot1x system-auth-control** グローバル コンフィギュレーション コマンドを入力して 802.1x 認証をグローバルにイネーブルにする前に、802.1x 認証と EtherChannel が設定されているインターフェイスから、EtherChannel の設定を削除してください。
- Cisco IOS Release 12.2(55)SE 以降のリリースでは、802.1x 認証に関連するシステム メッセージのフィルタリングがサポートされています。



(注) 802.1x に準拠したすべての CLI を同じインターフェイスまたは同じテンプレートで設定することを推奨します。

## VLAN 割り当て、ゲスト VLAN、制限付き VLAN、アクセス不能認証バイパス

VLAN 割り当て、ゲスト VLAN、制限付き VLAN、およびアクセス不能認証バイパス設定時の注意事項は、次のとおりです。

- 802.1x 認証をポート上でイネーブルにすると、音声 VLAN の機能を持つポート VLAN は設定できません。
- RSPAN VLAN または音声 VLAN を除くあらゆる VLAN を、802.1x ゲスト VLAN として設定できます。ゲスト VLAN 機能は、内部 VLAN (ルーテッドポート) またはトランクポートではサポートされていません。アクセスポート上でだけサポートされます。
- DHCP クライアントが接続されている 802.1x ポートのゲスト VLAN を設定した後、DHCP サーバからホスト IP アドレスを取得する必要があります。クライアント上の DHCP プロセスが時間切れとなり DHCP サーバからホスト IP アドレスを取得しようとする前に、スイッチ上の 802.1x 認証プロセスを再起動する設定を変更できます。802.1x 認証プロセスの設定を減らします (**authentication timer inactivity** および **authentication timer reauthentication** インターフェイス コンフィギュレーション コマンド)。設定の減少量は、接続された 802.1x クライアントのタイプによって異なります。
- アクセス不能認証バイパス機能を設定する際には、次の注意事項に従ってください。
  - この機能はシングル ホスト モードおよびマルチホスト モードの 802.1x ポートでサポートされます。
  - Windows XP を稼働しているクライアントに接続されたポートがクリティカル認証ステータスの場合、Windows XP はインターフェイスが認証されないと報告する場合があります。
  - Windows XP クライアントで DHCP が設定され、DHCP サーバからの IP アドレスがある場合、クリティカルポートで EAP 認証成功メッセージを受信しても DHCP 設定プロセスを再初期化しません。
  - アクセス不能認証バイパス機能および制限 VLAN を 802.1x ポート上に設定できます。スイッチが制限付き VLAN 内でクリティカルポートを再認証しようとし、すべての RADIUS サーバが利用不可能な場合、スイッチはポートステータスをクリティカル認証ステータスに変更し、制限付き VLAN に残ります。
  - CTS リンクがクリティカル認証モードである場合にアクティブスイッチがリロードすると、SGT をデバイスに設定したポリシーは新しいアクティブスイッチでは使用できません。これは、内部バインドが 3750-X スイッチスタックのスタンバイスイッチと同期しないためです。
- RSPAN VLAN または音声 VLAN を除くあらゆる VLAN を、802.1x 制限付き VLAN として設定できます。制限付き VLAN 機能は、内部 VLAN (ルーテッドポート) またはトランクポートではサポートされていません。アクセスポート上でだけサポートされます。

## MAC 認証バイパス

MAC 認証バイパス設定時の注意事項は次のとおりです。

- 特に明記していないかぎり、MAC 認証バイパスの注意事項は 802.1x 認証のものと同じです。

- ポートが MAC アドレスで許可された後に、ポートから MAC 認証バイパスをディセーブルにしても、ポート ステータスに影響はありません。
- ポートが未許可ステータスであり、クライアント MAC アドレスが認証サーバデータベースにない場合、ポートは未許可ステータスのままです。ただし、クライアント MAC アドレスがデータベースに追加されると、スイッチは MAC 認証バイパス機能を使用してポートを再認証できます。
- ポートが認証ステータスにない場合、再認証が行われるまでポートはこのステータスを維持します。
- MAC 認証バイパスにより接続されているが、非アクティブなホストのタイムアウト時間を設定できます。指定できる範囲は 1 ～ 65535 秒です。

## ポートあたりのデバイスの最大数

802.1x 対応のポートに接続できるデバイスの最大数です。

- シングル ホスト モードの場合、アクセス VLAN で接続できるデバイスは 1 台だけです。ポートが音声 VLAN でも設定されている場合、音声 VLAN を介して送受信できる Cisco IP Phone の数には制限はありません。
- マルチドメイン認証 (MDA) モードの場合、アクセス VLAN で 1 台のデバイス、音声 VLAN で 1 台の IP Phone が許可されます。
- マルチホストモードでは、1つの 802.1x サブリカントだけがポートで許可されますが、非 802.1x ホストは数に制限なく、アクセス VLAN で許可されます。音声 VLAN で許可されるデバイスの数には制限はありません。

## 802.1x 準備状態チェックの設定

802.1x 準備状態チェックは、すべてのスイッチ ポートの 802.1x アクティビティをモニタリングし、802.1x をサポートするポートに接続されているデバイスの情報を表示します。この機能を使用して、スイッチ ポートに接続されているデバイスが 802.1x に対応できるかどうかを判別できます。

802.1x 準備状態チェックは、802.1x で設定できるすべてのポートで使用できます。準備状態チェックは、**dot1x force-unauthorized** として設定されるポートでは使用できません。

802.1x 準備状態チェックをスイッチでイネーブルにする場合には、次の手順に従ってください。

### 始める前に

準備状態チェックをスイッチでイネーブルにする場合、次の注意事項に従ってください。

- 準備状態チェックは通常、802.1x がスイッチでイネーブルにされる前に使用されます。
- インターフェイスを指定せずに **dot1x test eapol-capable** 特権 EXEC コマンドを使用すると、スイッチ スタックのすべてのポートがテストされます。

- **dot1x test eapol-capable** コマンドを 802.1x 対応のポートで設定し、リンクがアップになると、ポートは、802.1xに対応するかどうか、接続クライアントでクエリーを実行します。クライアントが通知パケットに応答すると、802.1x対応です。クライアントがタイムアウト時間内に応答すると Syslog メッセージが生成されます。クライアントがクエリーに応答しない場合、クライアントは 802.1x 対応ではありません。Syslog メッセージは生成されません。
- **dot1x test eapol-capable** コマンドを 802.1x 対応のポートで設定し、リンクがアップになると、ポートは、802.1xに対応するかどうか、接続クライアントでクエリーを実行します。クライアントが通知パケットに応答すると、802.1x対応です。クライアントがタイムアウト時間内に応答すると Syslog メッセージが生成されます。クライアントがクエリーに応答しない場合、クライアントは 802.1x 対応ではありません。Syslog メッセージは生成されません。
- 準備状態チェックは、複数のホスト（たとえば、IP Phone に接続される PC）を扱うポートに送信できます。Syslog メッセージは、タイマー時間内に準備状態チェックに応答する各クライアントに生成されます。

## 手順の概要

1. **enable**
2. **configure terminal**
3. **dot1x test eapol-capable [ interface interface-id]**
4. **dot1x test timeout timeout**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  デバイス> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  デバイス# <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 3	<b>dot1x test eapol-capable [ interface interface-id]</b> 例：  デバイス# <b>dot1x test eapol-capable interface gigabitethernet1/0/13</b> DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC	スイッチ上で 802.1x 準備状態チェックをイネーブルにします。  (任意) <i>interface-id</i> では、IEEE 802.1x の準備状態をチェックするポートを指定します。



	コマンドまたはアクション	目的
	00-01-02-4b-f1-a3 on gigabitethernet1/0/13 is EAPOL capable	(注) オプションの <b>interface</b> キーワードを省略した場合、スイッチのすべてのインターフェイスがテストされます。
ステップ 4	<b>dot1x test timeout</b> <i>timeout</i>	(任意) EAPOL 応答の待機に使用するタイムアウトを設定します。範囲は 1 ~ 65535 秒です。デフォルトは 10 秒です。
ステップ 5	<b>end</b> 例：  デバイス (config) # <b>end</b>	特権 EXEC モードに戻ります。
ステップ 6	<b>show running-config</b> 例：  デバイス # <b>show running-config</b>	入力を確認します。
ステップ 7	<b>copy running-config startup-config</b> 例：  デバイス # <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## 音声認識 802.1x セキュリティの設定



- (注) 音声認識 IEEE 802.1x 認証を使用するには、スイッチが LAN Base イメージを実行している必要があります。

音声認識 802.1x セキュリティ機能をスイッチで使用して、セキュリティ違反が発生した場合にデータまたは音声 VLAN に関係なく VLAN だけをディセーブルにします。この機能は、PC が IP Phone に接続されている IP Phone 環境で使用できます。データ VLAN でセキュリティ違反が検出されると、データ VLAN だけがシャットダウンされます。音声 VLAN のトラフィックは中断することなくスイッチで送受信されます。

スイッチで音声認識 802.1x 音声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。

- 音声認識 802.1x セキュリティをイネーブルにするには、**errdisable detect cause security-violation shutdown vlan** グローバル コンフィギュレーション コマンドを入力します。音声認識 802.1x セキュリティをディセーブルにするには、このコマンドの **no** バー

ジョンを入力します。このコマンドは、スイッチの 802.1x 設定ポートのすべてに適用されます。



(注) **shutdown vlan** キーワードを指定しない場合、**error-disabled** ステータスになった際にポート全体がシャットダウンされます。

- **errdisable recovery cause security-violation** グローバル コンフィギュレーション コマンドを使用して、**error-disabled** リカバリを設定すると、ポートは自動的に再びイネーブルにされます。**error-disabled** リカバリがポートで設定されていない場合、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを使用してポートを再びイネーブルにします。
- 個々の VLAN を再びイネーブルにするには、**clear errdisable interface interface-id vlan [vlan-list]** 特権 EXEC コマンドを使用します。範囲を指定しない場合、ポートのすべての VLAN がイネーブルにされます。

音声認識 802.1x セキュリティをイネーブルにするには、特権 EXEC モードで次の手順を実行します。

#### 手順の概要

1. **configure terminal**
2. **errdisable detect cause security-violation shutdown vlan**
3. **errdisable recovery cause security-violation**
4. **clear errdisable interface interface-id vlan [vlan-list]**
5. 次を入力します。
  - **shutdown**
  - **no shutdown**
6. **end**
7. **show errdisable detect**

#### 手順の詳細

	コマンドまたはアクション	目的
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>errdisable detect cause security-violation shutdown vlan</b>	セキュリティ違反エラーが発生したすべての VLAN をシャットダウンします。  (注) <b>shutdown vlan</b> キーワードを指定しない場合、すべてのポートが <b>errdisable</b> ステータスになり、シャットダウンされます。

	コマンドまたはアクション	目的
ステップ 3	<b>errdisable recovery cause security-violation</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 4	<b>clear errdisable interface interface-id vlan [vlan-list]</b>	(任意) errdisable になっている個々の VLAN を再びイネーブルにします。 <ul style="list-style-type: none"> <li>• interface-id の場合、個々の VLAN を再びイネーブルにするポートを指定します。</li> <li>• (任意) vlan-list の場合、再びイネーブルにする VLAN のリストを指定します。vlan-list を指定しない場合は、すべての VLAN が再びイネーブルになります。</li> </ul>
ステップ 5	次を入力します。 <ul style="list-style-type: none"> <li>• <b>shutdown</b></li> <li>• <b>no shutdown</b></li> </ul>	(任意) errdisable の VLAN を再びイネーブルにして、すべての errdisable 指示をクリアします。
ステップ 6	<b>end</b>	特権 EXEC モードに戻ります。
ステップ 7	<b>show errdisable detect</b>	入力内容を確認します。

### 例

次に、セキュリティ違反エラーが発生した任意の VLAN をシャットダウンするようにスイッチを設定する例を示します。

```
Switch(config)# errdisable detect cause security-violation shutdown vlan
```

次に、ポート ギガビット イーサネット 40/2 で errdisable ステートであったすべての VLAN を再度イネーブルにする方法を示します。

```
Switch# clear errdisable interface gigabitethernet40/2  
vlan
```

**show errdisable detect** 特権 EXEC コマンドを入力すると、設定を確認できます。

## 802.1x 違反モードの設定

次に示す状況で、シャットダウン、Syslog エラーを生成、または新しいデバイスからのパケットを廃棄するように 802.1x ポートを設定できます。

- デバイスが 802.1x 対応のポートに接続した
- ポートで認証されるデバイスの最大数に達した

スイッチ上にセキュリティ違反アクションを設定するには、特権 EXEC モードで次の手順を実行します。

## 手順の概要

1. **configure terminal**
2. **aaa new-model**
3. **aaa authentication dot1x{ default } method1**
4. **interface interface-id**
5. **switchport mode access**
6. **authentication violation {shutdown | restrict | protect | replace}**
7. **end**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例：  デバイス# <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 new-model</b> 例：  デバイス(config)# <b>aaa new-model</b>	AAA をイネーブルにします。
ステップ 3	<b>aaa authentication dot1x{ default } method1</b> 例：  デバイス(config)# <b>aaa authentication dot1x default group radius</b>	802.1x 認証方式リストを作成します。  <b>authentication</b> コマンドにリストが指定されていない場合に使用するデフォルトのリストを作成するには、 <b>default</b> キーワードの後ろにデフォルト状況で使用される方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。  <i>method1</i> には、 <b>group radius</b> キーワードを入力して、認証用のすべての RADIUS サーバリストを使用できるようにします。
ステップ 4	<b>interface interface-id</b> 例：  デバイス(config)# <b>interface gigabitethernet1/0/4</b>	IEEE 802.1x 認証をイネーブルにするクライアントに接続しているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 5	<b>switchport mode access</b> 例：  デバイス(config-if)# <b>switchport mode access</b>	ポートをアクセス モードに設定します。

	コマンドまたはアクション	目的
ステップ 6	<b>authentication violation {shutdown   restrict   protect   replace}</b> 例： デバイス (config-if) # <b>authentication violation restrict</b>	違反モードを設定します。キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> <li>• <b>shutdown</b> : エラーによってポートがディセーブルになります。</li> <li>• <b>restrict</b> : Syslog エラーを生成します。</li> <li>• <b>protect</b> : トラフィックをポートに送信するすべての新しいデバイスからパケットをドロップします。</li> <li>• <b>replace</b> : 現在のセッションを削除し、新しいホストで認証します。</li> </ul>
ステップ 7	<b>end</b> 例： デバイス (config-if) # <b>end</b>	特権 EXEC モードに戻ります。

## 802.1X 認証の設定

ユーザー単位 ACL または VLAN 割り当てを可能にするには、AAA 許可をイネーブルにしてネットワーク関連のすべてのサービス要求に対してスイッチを設定する必要があります。

次に、802.1x の AAA プロセスを示します。

### 始める前に

802.1x ポートベース認証を設定するには、認証、許可、アカウントिंग (AAA) をイネーブルにして認証方式リストを指定する必要があります。方式リストは、ユーザ認証のためにクエリー送信を行う手順と認証方式を記述したものです。

### 手順の概要

1. ユーザーがスイッチのポートに接続します。
2. 認証が実行されます。
3. RADIUS サーバ設定に基づいて、VLAN 割り当てが適宜イネーブルになります。
4. スイッチが開始メッセージをアカウントング サーバーに送信します。
5. 必要に応じて、再認証が実行されます。
6. スイッチが仮のアカウントングアップデートを、再認証結果に基づいたアカウントング サーバーに送信します。
7. ユーザーがポートから切断します。
8. スイッチが停止メッセージをアカウントング サーバーに送信します。

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	ユーザーがスイッチのポートに接続します。	
ステップ 2	認証が実行されます。	
ステップ 3	RADIUS サーバ設定に基づいて、VLAN 割り当てが適宜イネーブルになります。	
ステップ 4	スイッチが開始メッセージをアカウントिंगサーバーに送信します。	
ステップ 5	必要に応じて、再認証が実行されます。	
ステップ 6	スイッチが仮のアカウントングアップデートを、再認証結果に基づいたアカウントングサーバーに送信します。	
ステップ 7	ユーザーがポートから切断します。	
ステップ 8	スイッチが停止メッセージをアカウントングサーバーに送信します。	

## 802.1x ポートベース認証の設定

802.1x ポートベース認証を設定するには、特権 EXEC モードで次の手順を実行します。

## 手順の概要

1. **configure terminal**
2. **aaa new-model**
3. **aaa authentication dot1x { default } method1**
4. **dot1x system-auth-control**
5. **aaa authorization network {default} group radius**
6. **radius server *server name***
7. **address {ipv4 | ipv6} *ip address***
8. **key *string***
9. **exit**
10. **interface *interface-id***
11. **switchport mode access**
12. **authentication port-control auto**
13. **dot1x pae authenticator**
14. **end**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： デバイス# <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 new-model</b> 例： デバイス (config)# <b>aaa new-model</b>	AAA をイネーブルにします。
ステップ 3	<b>aaa authentication dot1x{ default } method1</b> 例： デバイス (config)# <b>aaa authentication dot1x default group radius</b>	802.1x 認証方式リストを作成します。 <b>authentication</b> コマンドにリストが指定されていない場合に使用するデフォルトのリストを作成するには、 <b>default</b> キーワードの後ろにデフォルト状況で使用される方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 <b>method1</b> には、 <b>group radius</b> キーワードを入力して、認証用のすべての RADIUS サーバリストを使用できるようにします。 (注) コマンドラインのヘルプストリングには他のキーワードも表示されますが、サポートされるのは <b>group radius</b> キーワードのみです。
ステップ 4	<b>dot1x system-auth-control</b> 例： デバイス (config)# <b>dot1x system-auth-control</b>	スイッチで 802.1x 認証をグローバルに有効にします。
ステップ 5	<b>aaa authorization network {default} group radius</b> 例： デバイス (config)# <b>aaa authorization network default group radius</b>	(任意) ユーザー単位 ACL や VLAN 割り当てなど、ネットワーク関連のすべてのサービス要求に対するユーザー RADIUS 許可をスイッチに設定します。
ステップ 6	<b>radius server server name</b> 例：	(任意) RADIUS サーバーの IP アドレスを指定します。

	コマンドまたはアクション	目的
	デバイス(config)# <b>radius server rsim address ipv4 124.2.2.12</b>	
ステップ 7	<b>address {ipv4   ipv6} ip address</b> 例： デバイス(config-radius-server)# <b>address ipv4 10.0.1.12</b>	RADIUS サーバーの IP アドレスを設定します。
ステップ 8	<b>key string</b> 例： デバイス(config-radius-server)# <b>key rad123</b>	(任意) RADIUS サーバー上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号キーを指定します。
ステップ 9	<b>exit</b> 例： デバイス(config-radius-server)# <b>exit</b>	RADIUS サーバーモードを終了して、グローバル コンフィギュレーション モードを開始します。
ステップ 10	<b>interface interface-id</b> 例： デバイス(config)# <b>interface gigabitethernet1/0/2</b>	IEEE 802.1x 認証をイネーブ爾にするクライアントに接続しているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	<b>switchport mode access</b> 例： デバイス(config-if)# <b>switchport mode access</b>	(任意) ステップ 6 および 7 で RADIUS サーバを設定した場合のみ、ポートをアクセス モードに設定します。
ステップ 12	<b>authentication port-control auto</b> 例： デバイス(config-if)# <b>authentication port-control auto</b>	ポートでの 802.1x 認証を有効にします。
ステップ 13	<b>dot1x pae authenticator</b> 例： デバイス(config-if)# <b>dot1x pae authenticator</b>	インターフェイスのポート アクセス エンティティを、オーセンティケータとしてのみ動作し、サブリカント用のメッセージは無視するように設定します。



	コマンドまたはアクション	目的
ステップ 14	<b>end</b> 例 : デバイス (config-if) # <b>end</b>	特権 EXEC モードに戻ります。

## スイッチ/RADIUS サーバー間通信の設定

RADIUS サーバーのパラメータを設定するには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **ip radius source-interface**
4. **radius server** *server name*
5. **address** {*ipv4* | *ipv6*} *ip address*
6. **key** *string*
7. **exit**
8. **radius-server dead-criteria tries** *num-tries*
9. **end**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : デバイス > <b>enable</b>	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	<b>configure terminal</b> 例 : デバイス # <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 3	<b>ip radius source-interface</b> 例 : デバイス (config) # <b>ip radius source-interface vlan 80</b>	RADIUS パケットが、指定されたインターフェイスの IP アドレスを含むように指定します。

	コマンドまたはアクション	目的
ステップ 4	<b>radius server</b> <i>server name</i> 例：  デバイス(config)# <b>radius server</b> <i>rsim</i> <b>address</b> <i>ipv4</i> <b>124.2.2.12</b>	(任意) RADIUS サーバーの IP アドレスを指定します。
ステップ 5	<b>address</b> { <i>ipv4</i>   <i>ipv6</i> } <i>ip address</i> 例：  デバイス(config-radius-server)# <b>address</b> <i>ipv4</i> <b>10.0.1.2</b> <b>auth-port</b> <i>1550</i> <b>acct-port</b> <i>1560</i>	RADIUS サーバーの IP アドレスを設定します。
ステップ 6	<b>key</b> <i>string</i> 例：  デバイス(config-radius-server)# <b>key</b> <i>rad123</i>	(任意) RADIUS サーバー上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号キーを指定します。
ステップ 7	<b>exit</b> 例：  デバイス(config-radius-server)# <b>exit</b>	RADIUS サーバーモードを終了して、グローバルコンフィギュレーションモードを開始します。
ステップ 8	<b>radius-server dead-criteria</b> <i>tries num-tries</i> 例：  デバイス(config)# <b>radius-server dead-criteria</b> <i>tries</i> <b>30</b>	RADIUS サーバーに送信されたメッセージへの応答がない場合に、このサーバーが非アクティブであると見なすまでの送信回数を指定します。指定できる <i>num-tries</i> の範囲は 1 ~ 100 です。
ステップ 9	<b>end</b> 例：  デバイス(config)# <b>end</b>	特権 EXEC モードに戻ります。

## ホストモードの設定

**authentication port-control** インターフェイス コンフィギュレーション コマンドが **auto** に設定されている IEEE 802.1x 許可ポート上で、複数のホスト (クライアント) を許可するには、特権 EXEC モードで次の手順を実行します。マルチドメイン認証 (MDA) を設定してイネーブルにするには、**multi-domain** キーワードを使用します。これにより、ホストデバイス、および

IP Phone（シスコ製または他社製）など音声デバイスの両方が同じスイッチポートで許可されます。この手順は任意です。

### 手順の概要

1. **configure terminal**
2. **interface *interface-id***
3. **authentication host-mode[*multi-auth* |*multi-domain* |*multi-host* |*single-host*]**
4. **end**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： デバイス# <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>interface <i>interface-id</i></b> 例： デバイス(config)# <b>interface gigabitethernet2/0/1</b>	複数ホストが間接的に接続されているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<b>authentication host-mode[<i>multi-auth</i>  <i>multi-domain</i>  <i>multi-host</i>  <i>single-host</i>]</b> 例： デバイス(config-if)# <b>authentication host-mode multi-host</b>	<p>単一の 802.1x 許可ポートで複数のホスト（クライアント）を許可することができます。</p> <p>キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> <li>• <b>multi-auth</b> : 音声 VLAN とデータ VLAN の両方で複数の認証クライアントを許可します。                (注) <b>multi-auth</b> キーワードは、<b>authentication host-mode</b> コマンドでのみ使用できます。</li> <li>• <b>multi-host</b> : シングル ホストの認証後に 802.1x 許可ポートで複数のホスト（クライアント）の接続を許可します。</li> <li>• <b>multi-domain</b> : ホストデバイスと IP Phone（シスコ製または他社製）など音声デバイスの両方が、IEEE 802.1x 許可ポートで認証されるようにします。                (注) ホストモードが <b>multi-domain</b> に設定されている場合、IP Phone の音声 VLAN を設定する必要があります。</li> </ul>

	コマンドまたはアクション	目的
		指定のインターフェイスに対し <b>authentication port-control</b> インターフェイス コンフィギュレーション 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>end</b> 例：  デバイス(config-if)# <b>end</b>	特権 EXEC モードに戻ります。

## 定期的な再認証の設定

802.1x クライアントの定期的な再認証をイネーブルにし、再認証の間隔を指定できます。再認証を行う間隔を指定しない場合、3600 秒おきに再認証が試みられます。

クライアントの定期的な再認証をイネーブルにし、再認証を行う間隔（秒）を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

### 手順の概要

1. **configure terminal**
2. **interface interface-id**
3. **authentication periodic**
4. **authentication timer** {[inactivity | reauthenticate | restart | unauthorized]} {value}
5. **end**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例：  デバイス# <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>interface interface-id</b> 例：  デバイス(config)# <b>interface gigabitethernet2/0/1</b>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<b>authentication periodic</b> 例：	クライアントの定期的な再認証（デフォルトではディセーブル）をイネーブルにします。

	コマンドまたはアクション	目的
	デバイス(config-if)# <b>authentication periodic</b>	(注) デフォルト値は 3600 秒です。再認証タイマーの値を変更するか、スイッチに RADIUS-provided セッションタイムアウトを使用させるには、 <b>authentication timer reauthenticate</b> コマンドを入力します。
ステップ 4	<b>authentication timer</b> {[inactivity   reauthenticate   restart   unauthorized]} {value} 例： デバイス(config-if)# <b>authentication timer reauthenticate 180</b>	再認証の試行の間隔 (秒) を設定します。 <b>authentication timer</b> キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> <li>• <b>inactivity</b> : クライアントからのアクティビティがなくなり無許可になるまでの間隔 (秒)</li> <li>• <b>reauthenticate</b> : 自動再認証試行が開始されるまでの時間 (秒)</li> <li>• <b>restart value</b> : 無許可ポートの認証の試行が行われるまでの間隔 (秒)</li> <li>• <b>unauthorized value</b> : 不正セッションが削除されるまでの間隔 (秒)</li> </ul> このコマンドがスイッチの動作に影響するのは、定期的な再認証をイネーブルに設定した場合だけです。
ステップ 5	<b>end</b> 例： デバイス(config-if)# <b>end</b>	特権 EXEC モードに戻ります。

## 待機時間の変更

スイッチはクライアントを認証できなかった場合に、所定の時間だけアイドル状態を続け、その後再び認証を試みます。**authentication timer restart** インターフェイスコンフィギュレーションコマンドは、アイドル状態の期間を制御します。認証が失敗する理由としては、クライアントが無効なパスワードを提示した場合などが考えられます。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。

待機時間を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

### 手順の概要

#### 1. configure terminal

2. **interface** *interface-id*
3. **authentication timer restart** *seconds*
4. **end**
5. **show authentication sessions interface** *interface-id*
6. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例：  デバイス# <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>interface</b> <i>interface-id</i> 例：  デバイス(config)# <b>interface gigabitethernet2/0/1</b>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<b>authentication timer restart</b> <i>seconds</i> 例：  デバイス(config-if)# <b>authentication timer restart 30</b>	クライアントとの認証のやり取りに失敗した場合に、スイッチが待機状態のままの秒数を設定します。  指定できる範囲は 1 ~ 65535 秒です。デフォルトは 60 秒です。
ステップ 4	<b>end</b> 例：  デバイス(config-if)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show authentication sessions interface</b> <i>interface-id</i> 例：  デバイス# <b>show authentication sessions interface gigabitethernet2/0/1</b>	入力を確認します。
ステップ 6	<b>copy running-config startup-config</b> 例：  デバイス# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## スイッチからクライアントへの再送信時間の変更

クライアントはスイッチからの EAP-Request/Identity フレームに対し、EAP-Response/Identity フレームで応答します。スイッチ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、その後フレームを再送信します。



(注) このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバー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必要があるときに限って変更してください。

スイッチがクライアントからの通知を待機する時間を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

### 手順の概要

1. **configure terminal**
2. **interface *interface-id***
3. **authentication timer reauthenticate *seconds***
4. **end**
5. **show authentication sessions interface *interface-id***
6. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例：  デバイス# <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>interface <i>interface-id</i></b> 例：  デバイス(config)# <b>interface gigabitethernet2/0/1</b>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<b>authentication timer reauthenticate <i>seconds</i></b> 例：  デバイス(config-if)# <b>authentication timer reauthenticate 60</b>	スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数を設定します。  指定できる範囲は 1 ~ 65535 秒です。デフォルトは 5 秒です。

	コマンドまたはアクション	目的
ステップ 4	<b>end</b> 例：  デバイス(config-if)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show authentication sessions interface interface-id</b> 例：  デバイス# <b>show authentication sessions interface gigabitethernet2/0/1</b>	入力を確認します。
ステップ 6	<b>copy running-config startup-config</b> 例：  デバイス# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## スイッチからクライアントへのフレーム再送信回数の設定

スイッチからクライアントへの再送信時間を変更できるだけでなく、(クライアントから応答が得られなかった場合に) スイッチが認証プロセスを再起動する前に、クライアントに EAP-Request/Identity フレームを送信する回数を変更できます。



(注) このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバー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必要があるときに限って変更してください。

スイッチからクライアントへのフレーム再送信回数を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

### 手順の概要

1. **configure terminal**
2. **interface interface-id**
3. **dot1x max-reauth-req count**
4. **end**



## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例：  デバイス# <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>interface interface-id</b> 例：  デバイス(config)# <b>interface gigabitethernet2/0/1</b>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<b>dot1x max-reauth-req count</b> 例：  デバイス(config-if)# <b>dot1x max-reauth-req 5</b>	スイッチが認証処理を再開するまでに、クライアントへ EAP 要求/アイデンティティ フレームを送信する回数を変更できます。指定できる範囲は 1 ~ 10 です。デフォルトは 2 です。
ステップ 4	<b>end</b> 例：  デバイス(config-if)# <b>end</b>	特権 EXEC モードに戻ります。

再認証回数の設定

ポートが無許可状態に変わる前に、スイッチが認証プロセスを再開する回数を変更することもできます。



(注) このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライア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必要がある際に限って変更してください。

再認証回数を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

## 手順の概要

1. **configure terminal**
2. **interface interface-id**
3. **switchport mode access**
4. **dot1x max-req count**

## 5. end

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例：  デバイス# <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>interface interface-id</b> 例：  デバイス# <code>interface gigabitethernet2/0/1</code>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<b>switchport mode access</b> 例：  デバイス (config-if) # <code>switchport mode access</code>	RADIUS サーバを事前に設定した場合に限り、ポートをアクセス モードに設定します。
ステップ 4	<b>dot1x max-req count</b> 例：  デバイス (config-if) # <code>dot1x max-req 4</code>	ポートが無許可ステートになる前に、スイッチが認証プロセスを再開する回数を設定します。指定できる範囲は 0 ~ 10 です。デフォルトは 2 です。
ステップ 5	<b>end</b> 例：  デバイス (config-if) # <code>end</code>	特権 EXEC モードに戻ります。

## MAC 移動のイネーブル化

MAC 移動を使用すると、認証されたホストをスイッチのポート間で移動できます。

スイッチで MAC 移動をグローバルにイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

## 手順の概要

1. `configure terminal`
2. `authentication mac-move permit`
3. `end`

4. `show running-config`
5. `copy running-config startup-config`

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： デバイス# <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>authentication mac-move permit</b> 例： デバイス(config)# <code>authentication mac-move permit</code>	スイッチでMAC移動をイネーブルにします。デフォルトは <b>deny</b> です。 セッション認識型ネットワークモードでは、デフォルト CLI は <b>access-session mac-move deny</b> です。セッション認識型ネットワークで MAC 移動をイネーブルにするには、 <b>no access-session mac-move</b> 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。 <b>mac-move</b> のデフォルト値は、レガシーモード (IBNS 1.0) の場合は <b>deny</b> で、C3PL モード (IBNS 2.0) の場合は <b>permit</b> です。
ステップ 3	<b>end</b> 例： デバイス(config)# <code>end</code>	特権 EXEC モードに戻ります。
ステップ 4	<b>show running-config</b> 例： デバイス# <code>show running-config</code>	入力を確認します。
ステップ 5	<b>copy running-config startup-config</b> 例： デバイス# <code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

## MAC 置換のイネーブル化

MAC 置換を使用すると、ホストはポート上の認証ホストを置換できます。

インターフェイス上で MAC 置換をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

### 手順の概要

1. **configure terminal**
2. **interface interface-id**
3. **authentication violation {protect | replace | restrict | shutdown}**
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例：  デバイス# <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>interface interface-id</b> 例：  デバイス(config)# <b>interface gigabitethernet2/0/2</b>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<b>authentication violation {protect   replace   restrict   shutdown}</b> 例：  デバイス(config-if)# <b>authentication violation replace</b>	インターフェイス上で MAC 置換をイネーブルにするには、 <b>replace</b> キーワードを使用します。ポートが現在のセッションを削除し、新しいホストを使用して認証を開始します。  他のキーワードは、次のような機能があります。 <ul style="list-style-type: none"> <li>• <b>protect</b> : ポートは、システムメッセージを生成せずに、予期しない MAC を使用するパケットをドロップします。</li> <li>• <b>restrict</b> : 違反パケットが CPU によってドロップされ、システムメッセージが生成されます。</li> <li>• <b>shutdown</b> : ポートは、予期しない MAC アドレスを受信すると <b>error disabled</b> になります。</li> </ul>
ステップ 4	<b>end</b> 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	デバイス(config-if)# <b>end</b>	
ステップ 5	<b>show running-config</b> 例： デバイス# <b>show running-config</b>	入力を確認します。
ステップ 6	<b>copy running-config startup-config</b> 例： デバイス# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## 802.1x アカウンティングの設定

802.1x アカウンティングを使用して、AAA システム アカウンティングをイネーブルにすると、ロギングのためにシステム リロード イベントをアカウンティング RADIUS サーバに送信できます。サーバは、アクティブな 802.1x セッションすべてが終了したものと判断します。



- (注) Cisco IOS XE Denali 16.3.x および Cisco IOS XE Everest 16.6.x では、定期的な AAA アカウンティングのアップデートはサポートされていません。スイッチは、定期的な中間アカウンティングレコードをアカウンティングサーバに送信しません。定期的な AAA アカウンティングのアップデートは、Cisco IOS XE Fuji 16.9.x 以降のリリースで利用できます。

RADIUS は信頼性の低い UDP トランスポート プロトコルを使用するため、ネットワーク状態が良好でないと、アカウンティングメッセージが失われることがあります。設定した回数のアカウンティング要求の再送信後、スイッチが RADIUS サーバからアカウンティング応答メッセージを受信しない場合、次のメッセージが表示されます。

```
Accounting message %s for session %s failed to receive Accounting Response.
```

このストップメッセージが正常に送信されない場合、次のメッセージが表示されます。

```
00:09:55: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.201:1645,1646 is not responding.
```



- (注) ログインの開始、停止、仮のアップデートメッセージ、タイムスタンプなどのアカウンティングタスクを実行するように、RADIUS サーバを設定する必要があります。これらの機能をオンにするには、RADIUS サーバの [Network Configuration] タブの [Update/Watchdog packets from this AAA client] のログインをイネーブルにします。次に、RADIUS サーバの [System Configuration] タブの [CVS RADIUS Accounting] をイネーブルにします。

AAA がスイッチでイネーブルになった後、802.1x アカウンティングを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

### 手順の概要

1. **configure terminal**
2. **interface interface-id**
3. **aaa accounting dot1x default start-stop group radius**
4. **aaa accounting system default start-stop group radius**
5. **end**
6. **show running-config**
7. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例：  デバイス# <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>interface interface-id</b> 例：  デバイス(config)# <b>interface gigabitethernet1/0/3</b>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<b>aaa accounting dot1x default start-stop group radius</b> 例：  デバイス(config-if)# <b>aaa accounting dot1x default start-stop group radius</b>	すべての RADIUS サーバのリストを使用して 802.1x アカウンティングをイネーブルにします。
ステップ 4	<b>aaa accounting system default start-stop group radius</b> 例：  デバイス(config-if)# <b>aaa accounting system default</b>	(任意) システムアカウンティングをイネーブルにし (すべての RADIUS サーバのリストを使用)、スイッチがリロードするときにシステム アカ

	コマンドまたはアクション	目的
	<code>start-stop group radius</code>	タイミングリロードイベントメッセージを生成します。
ステップ 5	<b>end</b> 例：  デバイス (config-if) # <b>end</b>	特権 EXEC モードに戻ります。
ステップ 6	<b>show running-config</b> 例：  デバイス # <b>show running-config</b>	入力を確認します。
ステップ 7	<b>copy running-config startup-config</b> 例：  デバイス # <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## ゲスト VLAN の設定

サーバが EAP Request/Identity フレームに対する応答を受信しない場合、ゲスト VLAN を設定すると、802.1x 対応でないクライアントはゲスト VLAN に配置されます。802.1x 対応であっても、認証に失敗したクライアントは、ネットワークへのアクセスが許可されません。スイッチは、シングルホストモードまたはマルチホストモードでゲスト VLAN をサポートします。

ゲスト VLAN を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

### 手順の概要

1. **configure terminal**
2. **interface interface-id**
3. 次のいずれかを使用します。
  - **switchport mode access**
  - **switchport mode private-vlan host**
4. **authentication event no-response action authorize vlan vlan-id**
5. **end**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： デバイス# <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>interface interface-id</b> 例： デバイス(config)# <b>interface gigabitethernet 2/0/2</b>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかを使用します。 • <b>switchport mode access</b> • <b>switchport mode private-vlan host</b> 例： デバイス(config-if)# <b>switchport mode private-vlan host</b>	<ul style="list-style-type: none"> <li>• ポートをアクセス モードに設定します。</li> <li>• レイヤ 2 ポートをプライベート VLAN ホストポートとして設定します。</li> </ul>
ステップ 4	<b>authentication event no-response action authorize vlan vlan-id</b> 例： デバイス(config-if)# <b>authentication event no-response action authorize vlan 2</b>	アクティブ VLAN を 802.1x ゲスト VLAN として指定します。指定できる範囲は 1 ~ 4094 です。 内部 VLAN (ルーテッドポート)、RSPAN VLAN、音声 VLAN を除くあらゆるアクティブ VLAN を 802.1x ゲスト VLAN として設定できます。
ステップ 5	<b>end</b> 例： デバイス(config-if)# <b>end</b>	特権 EXEC モードに戻ります。

## 制限付き VLAN の設定

スイッチスタックまたはスイッチ上に制限付き VLAN を設定している場合、認証サーバーが有効なユーザー名またはパスワードを受信できないと、IEEE 802.1x に準拠しているクライアントは制限付き VLAN に移されます。スイッチは、シングル ホスト モードでのみ制限付き VLAN をサポートします。

制限付き VLAN を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。



## 手順の概要

1. **configure terminal**
2. **interface *interface-id***
3. 次のいずれかを使用します。
  - **switchport mode access**
  - **switchport mode private-vlan host**
4. **authentication port-control auto**
5. **authentication event fail action authorize vlan *vlan-id***
6. **end**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例：  デバイス# <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>interface <i>interface-id</i></b> 例：  デバイス(config)# <b>interface gigabitethernet 2/0/2</b>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかを使用します。  • <b>switchport mode access</b> • <b>switchport mode private-vlan host</b> 例：  デバイス(config-if)# <b>switchport mode access</b>	<ul style="list-style-type: none"> <li>• ポートをアクセス モードに設定します。</li> <li>• レイヤ 2 ポートをプライベート VLAN ホストポートとして設定します。</li> </ul>
ステップ 4	<b>authentication port-control auto</b> 例：  デバイス(config-if)# <b>authentication port-control auto</b>	ポートでの 802.1x 認証をイネーブルにします。
ステップ 5	<b>authentication event fail action authorize vlan <i>vlan-id</i></b> 例：  デバイス(config-if)# <b>authentication event fail action authorize vlan 2</b>	アクティブ VLAN を 802.1x 制限付き VLAN として指定します。指定できる範囲は 1 ~ 4094 です。  内部 VLAN (ルーテッドポート)、RSPAN VLAN または音声 VLAN を除き、任意のアクティブ VLAN を 802.1x 制限 VLAN として設定できます。

	コマンドまたはアクション	目的
ステップ 6	<b>end</b> 例：  デバイス(config-if)# <b>end</b>	特権 EXEC モードに戻ります。

## 制限付き VLAN の認証試行回数の設定

ユーザーに制限付き VLAN を割り当てる前に、**authentication event retry retry count** インターフェイスコンフィギュレーションコマンドを使用して、認証試行回数を最大に設定できます。指定できる試行回数は 1～3 です。デフォルトは 3 回に設定されています。

認証試行回数を最大に設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

### 手順の概要

1. **configure terminal**
2. **interface interface-id**
3. 次のいずれかを使用します。
  - **switchport mode access**
  - **switchport mode private-vlan host**
4. **authentication port-control auto**
5. **authentication event fail action authorize vlan vlan-id**
6. **authentication event retry retry count**
7. **end**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例：  デバイス# <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>interface interface-id</b> 例：  デバイス(config)# <b>interface gigabitethernet 2/0/3</b>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	次のいずれかを使用します。  • <b>switchport mode access</b>	• ポートをアクセス モードに設定します。

	コマンドまたはアクション	目的
	<ul style="list-style-type: none"> <li>• <b>switchport mode private-vlan host</b></li> </ul> 例： または デバイス (config-if) # <b>switchport mode access</b>	<ul style="list-style-type: none"> <li>• レイヤ 2 ポートをプライベート VLAN ホストポートとして設定します。</li> </ul>
ステップ 4	<b>authentication port-control auto</b> 例： デバイス (config-if) # <b>authentication port-control auto</b>	ポートでの 802.1x 認証をイネーブルにします。
ステップ 5	<b>authentication event fail action authorize vlan <i>vlan-id</i></b> 例： デバイス (config-if) # <b>authentication event fail action authorize vlan 8</b>	アクティブ VLAN を 802.1x 制限付き VLAN として指定します。指定できる範囲は 1 ~ 4094 です。 内部 VLAN (ルーテッドポート)、RSPAN VLAN または音声 VLAN を除き、任意のアクティブ VLAN を 802.1x 制限 VLAN として設定できます。
ステップ 6	<b>authentication event retry <i>retry count</i></b> 例： デバイス (config-if) # <b>authentication event retry 2</b>	ポートが制限付き VLAN に移行するための認証試行回数を指定します。指定できる範囲は 1 ~ 3 秒です。デフォルトは 3 回に設定されています。
ステップ 7	<b>end</b> 例： デバイス (config-if) # <b>end</b>	特権 EXEC モードに戻ります。

## クリティカル音声 VLAN を使用した 802.1x アクセス不能認証バイパスの設定

ポートにクリティカル音声 VLAN を設定し、アクセス不能認証バイパス機能をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

### 手順の概要

1. **configure terminal**
2. **aaa new-model**
3. **radius-server dead-criteria {time seconds} [tries number]**
4. **radius-server deadtime**分

5. **radius server** *server name*
6. **address** {*ipv4* | *ipv6*} *ip address* **auth-port** *port\_number* **acct-port** *port\_number*
7. **key** *string*
8. **exit**
9. **dot1x critical** {*eapol* | **recovery delay** *milliseconds*}
10. **interface** *interface-id*
11. **authentication event server dead action** {**authorize** | **reinitialize**} **vlan** *vlan-id*
12. **switchport voice vlan** *vlan-id*
13. **authentication event server dead action authorize voice**
14. **show authentication interface** *interface-id*
15. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例：  デバイス# <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 new-model</b> 例：  デバイス (config)# <b>aaa new-model</b>	AAA をイネーブルにします。
ステップ 3	<b>radius-server dead-criteria</b> { <i>time seconds</i> } [ <b>tries</b> <i>number</i> ] 例：  デバイス (config)# <b>radius-server dead-criteria time</b> <b>20 tries 10</b>	RADIUS サーバーが使用不可またはダウン (切断) と見なされる条件を設定します。  <ul style="list-style-type: none"> <li>• <b>time</b> : 1 ~ 120 秒。スイッチは、デフォルトの <i>seconds</i> 値を 10 ~ 60 の間で動的に決定します。</li> <li>• <b>number</b> : 1 ~ 100 の試行回数。スイッチは、デフォルトの <b>triesnumber</b> を 10 ~ 100 の間で動的に決定します。</li> </ul>
ステップ 4	<b>radius-server deadtime</b> 分 例：  デバイス (config)# <b>radius-server deadtime 60</b>	(任意) RADIUS サーバに要求が送信されない分数を設定します。指定できる範囲は 0 ~ 1440 分 (24 時間) です。デフォルト値は 0 分です。
ステップ 5	<b>radius server</b> <i>server name</i> 例：  デバイス (config)# <b>radius server rsim address ipv4</b>	(任意) RADIUS サーバーの IP アドレスを指定します。

	コマンドまたはアクション	目的
	124.2.2.12	
ステップ 6	<b>address {ipv4   ipv6} ip address auth-port port_number acct-port port_number</b> 例： デバイス (config-radius-server) # <b>address ipv4 10.0.1.2 auth-port 1550 acct-port 1560</b>	RADIUS サーバーの IP アドレスを設定します。
ステップ 7	<b>key string</b> 例： デバイス (config-radius-server) # <b>key rad123</b>	(任意) RADIUS サーバー上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号キーを指定します。
ステップ 8	<b>exit</b> 例： デバイス (config-radius-server) # <b>exit</b>	RADIUS サーバーモードを終了して、グローバル コンフィギュレーション モードを開始します。
ステップ 9	<b>dot1x critical {eapol   recovery delay milliseconds}</b> 例： デバイス (config) # <b>dot1x critical eapol</b> (config) # <b>dot1x critical recovery delay 2000</b>	(任意) アクセス不能認証バイパスのパラメータを設定します。 <ul style="list-style-type: none"> <li>• <b>eapol</b> : スイッチがクリティカル ポートを正常に認証すると、スイッチが EAPOL 成功メッセージを送信するように指定します。</li> <li>• <b>recovery delay milliseconds</b> : 使用できない RADIUS サーバーが使用できるようになったときに、スイッチがクリティカル ポートを再初期化するために待機する回復遅延期間を設定します。指定できる範囲は 1 ~ 10000 ミリ秒です。デフォルトは 1000 ミリ秒です (ポートは毎秒再初期化できます)。</li> </ul>
ステップ 10	<b>interface interface-id</b> 例： デバイス (config) # <b>interface gigabitethernet 1/0/1</b>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 11	<b>authentication event server dead action {authorize   reinitialize} vlan vlan-id]</b> 例：	これらのキーワードを使用して、RADIUS サーバが到達不能な場合にポートでホストを移動します。

	コマンドまたはアクション	目的
	デバイス (config-if) # <b>authentication event server dead action reinitialize vlan 20</b>	<ul style="list-style-type: none"> <li>• <b>authorize</b> : 認証しようとする新しいホストをユーザー指定のクリティカル VLAN に移動します。</li> <li>• <b>reinitialize</b> : ポートのすべての許可済みホストをユーザー指定のクリティカル VLAN に移動します。</li> </ul>
ステップ 12	<b>switchport voice vlan <i>vlan-id</i></b> 例 : デバイス (config-if) # <b>switchport voice vlan</b>	ポートの音声 VLAN を指定します。音声 VLAN はステップ 6 で設定されたクリティカルデータ VLAN と同じにはできません。
ステップ 13	<b>authentication event server dead action authorize voice</b> 例 : デバイス (config-if) # <b>authentication event server dead action authorize voice</b>	RADIUS サーバが到達不能な場合、ポートのデータトラフィックを音声 VLAN に移動するために、クリティカル音声 VLAN を設定します。
ステップ 14	<b>show authentication interface <i>interface-id</i></b> 例 : デバイス (config-if) # <b>do show authentication interface gigabit 1/0/1</b>	(任意) 設定を確認します。
ステップ 15	<b>copy running-config startup-config</b> 例 : デバイス (config-if) # <b>do copy running-config startup-config</b>	(任意) 設定を確認します。

### 例

RADIUS サーバーのデフォルト設定に戻すには、**no radius-server dead-criteria**、**no radius-server deadtime**、および **no radius-server** 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。アクセス不能な認証バイパスをディセーブルにするには、**no authentication event server dead action** インターフェイス コンフィギュレーション コマンドを使用します。クリティカル音声 VLAN をディセーブルにするには、**authentication event server dead action authorize voice** インターフェイス コンフィギュレーション コマンドを使用します。

## アクセス不能認証バイパスの設定例

次に、アクセス不能認証バイパス機能を設定する例を示します。

```

デバイス(config)# radius-server dead-criteria time 30 tries 20
デバイス(config)# radius-server deadtime 60
デバイス(config)# radius server server1
デバイス(config-radius-server)# address ipv4 172.29.36.49 acct-port 1618 auth-port 1612
デバイス(config-radius-server)# key abc1234
デバイス(config-radius-server)# exit
デバイス(config)# dot1x critical eapol
デバイス(config)# dot1x critical recovery delay 2000
デバイス(config)# interface gigabitethernet 1/0/1
デバイス(config-if)# dot1x critical
デバイス(config-if)# dot1x critical recovery action reinitialize
デバイス(config-if)# dot1x critical vlan 20
デバイス(config-if)# end

```

## WoL を使用した 802.1x 認証の設定

WoL を使用した 802.1x 認証をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

### 手順の概要

1. **configure terminal**
2. **interface *interface-id***
3. **authentication control-direction {both | in}**
4. **end**
5. **show authentication sessions interface *interface-id***
6. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： デバイス# <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>interface <i>interface-id</i></b> 例： デバイス(config)# <b>interface gigabitethernet2/0/3</b>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	<b>authentication control-direction {both   in}</b> 例： デバイス (config-if) # <b>authentication control-direction both</b>	ポートで WoL を使用して 802.1x 認証をイネーブルにし、次のキーワードを使用してポートを双方向または単方向に設定します。 <ul style="list-style-type: none"> <li>• <b>both</b> : ポートを双方向に設定します。ポートは、ホストにパケットを送受信できません。デフォルトでは、ポートは双方向です。</li> <li>• <b>in</b> : ポートを単方向に設定します。ポートは、ホストにパケットを送信できますが、受信はできません。</li> </ul>
ステップ 4	<b>end</b> 例： デバイス (config-if) # <b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show authentication sessions interface <i>interface-id</i></b> 例： デバイス # <b>show authentication sessions interface gigabitethernet2/0/3</b>	入力を確認します。
ステップ 6	<b>copy running-config startup-config</b> 例： デバイス # <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## MAC 認証バイパスの設定

MAC 認証バイパスをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

### 手順の概要

1. **configure terminal**
2. **interface *interface-id***
3. **authentication port-control auto**
4. **mab [eap]**
5. **end**



## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例：  デバイス# <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>interface interface-id</b> 例：  デバイス(config)# <b>interface gigabitethernet 2/0/1</b>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<b>authentication port-control auto</b> 例：  デバイス(config-if)# <b>authentication port-control auto</b>	ポートでの 802.1x 認証をイネーブルにします。
ステップ 4	<b>mab [eap]</b> 例：  デバイス(config-if)# <b>mab</b>	MAC 認証バイパスをイネーブルにします。  (任意) <b>eap</b> キーワードを使用して、認可用に EAP を使用できるようにスイッチを設定します。
ステップ 5	<b>end</b> 例：  デバイス(config-if)# <b>end</b>	特権 EXEC モードに戻ります。

## 802.1x ユーザー ディストリビューションの設定

VLAN グループを設定して、VLAN をそのグループにマッピングするには、特権 EXEC モードで次の手順を実行します。

## 手順の概要

1. **configure terminal**
2. **vlan group vlan-group-name vlan-list vlan-list**
3. **end**
4. **no vlan group vlan-group-name vlan-list vlan-list**

## VLAN グループの設定例

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例：  デバイス# <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>vlan group <i>vlan-group-name</i> vlan-list <i>vlan-list</i></b> 例：  デバイス (config) # <b>vlan group eng-dept vlan-list 10</b>	VLAN グループを設定し、単一の VLAN または VLAN の範囲をそのグループにマッピングします。
ステップ 3	<b>end</b> 例：  デバイス (config) # <b>end</b>	特権 EXEC モードに戻ります。
ステップ 4	<b>no vlan group <i>vlan-group-name</i> vlan-list <i>vlan-list</i></b> 例：  デバイス (config) # <b>no vlan group eng-dept vlan-list 10</b>	VLAN グループ コンフィギュレーションまたは VLAN グループコンフィギュレーションの要素をクリアします。

## VLAN グループの設定例

次に、VLAN グループを設定し、そのグループに VLAN をマッピングし、VLAN グループ コンフィギュレーションおよび指定 VLAN とのマッピングを確認する例を示します。

```

デバイス (config) # vlan group eng-dept vlan-list 10

デバイス (config) # show vlan group group-name eng-dept
Group Name          Vlans Mapped
-----
eng-dept             10

デバイス (config) # show dot1x vlan-group all
Group Name          Vlans Mapped
-----
eng-dept            10
hr-dept             20

```

次に、VLAN を既存の VLAN グループに追加し、VLAN が追加されたことを確認する例を示します。

```
デバイス(config)# vlan group eng-dept vlan-list 30
デバイス(config)# show vlan group eng-dept
Group Name                               Vlans Mapped
-----
eng-dept                                 10,30
```

次に、VLAN を VLAN グループから削除する例を示します。

```
デバイス# no vlan group eng-dept vlan-list 10
```

次に、すべての VLAN が VLAN グループからクリアされたときに、その VLAN グループもクリアされる例を示します。

```
デバイス(config)# no vlan group eng-dept vlan-list 30
Vlan 30 is successfully cleared from vlan group eng-dept.
```

```
デバイス(config)# show vlan group group-name eng-dept
```

次の例では、すべての VLAN グループをクリアする方法を示します。

```
デバイス(config)# no vlan group eng-dept vlan-list all
デバイス(config)# show vlan-group all
```

これらのコマンドの詳細については、『Cisco IOS Security Command Reference』を参照してください。

## NAC レイヤ 2 802.1x 検証の設定

NAC レイヤ 2 802.1x 検証を設定できます。これは、RADIUS サーバーを使用した 802.1x 認証とも呼ばれます。

NAC レイヤ 2 802.1x 検証を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

### 手順の概要

1. **configure terminal**
2. **interface *interface-id***
3. **switchport mode access**
4. **authentication event no-response action authorize vlan *vlan-id***
5. **authentication periodic**
6. **authentication timer reauthenticate**
7. **end**
8. **show authentication sessions interface *interface-id***
9. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例：  デバイス# <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>interface interface-id</b> 例：  デバイス(config)# <b>interface gigabitethernet2/0/3</b>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<b>switchport mode access</b> 例：  デバイス(config-if)# <b>switchport mode access</b>	RADIUS サーバを設定した場合に限り、ポートをアクセス モードに設定します。
ステップ 4	<b>authentication event no-response action authorize vlan vlan-id</b> 例：  デバイス(config-if)# <b>authentication event no-response action authorize vlan 8</b>	アクティブ VLAN を 802.1x ゲスト VLAN として指定します。指定できる範囲は 1 ~ 4094 です。  内部 VLAN (ルーテッドポート)、RSPAN VLAN、音声 VLAN を除くあらゆるアクティブ VLAN を 802.1x ゲスト VLAN として設定できます。
ステップ 5	<b>authentication periodic</b> 例：  デバイス(config-if)# <b>authentication periodic</b>	クライアントの定期的な再認証 (デフォルトではディセーブル) をイネーブルにします。
ステップ 6	<b>authentication timer reauthenticate</b> 例：  デバイス(config-if)# <b>authentication timer reauthenticate</b>	クライアントに対する再認証試行を設定します (1 時間に設定)。  このコマンドがスイッチの動作に影響するのは、定期的な再認証をイネーブルに設定した場合だけです。
ステップ 7	<b>end</b> 例：  デバイス(config-if)# <b>end</b>	特権 EXEC 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 8	<b>show authentication sessions interface <i>interface-id</i></b> 例 : デバイス# <b>show authentication sessions interface gigabitethernet2/0/3</b>	入力を確認します。
ステップ 9	<b>copy running-config startup-config</b> 例 : デバイス# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## NEAT を使用したオーセンティケータ スイッチの設定

この機能を設定するには、ワイヤリングクローゼット外の1つのスイッチがサブリカントとして設定され、オーセンティケータ スイッチに接続されている必要があります。



- (注)
- CISP または NEAT セッションがアクティブなときにラインカードを取り外してシャーシに挿入する場合は、オーセンティケータ スイッチ インターフェイスの設定を明示的にフラッピングすることによって、アクセスモードに復元する必要があります。
  - *cisco-av-pairs* は、ISE で *device-traffic-class=switch* として設定されている必要があります。これにより、サブリカントが正常に認証された後でトランクとしてインターフェイスが設定されます。

スイッチをオーセンティケータに設定するには、特権 EXEC モードで次の手順を実行します。

### 手順の概要

1. **configure terminal**
2. **cisp enable**
3. **interface *interface-id***
4. **switchport mode access**
5. **authentication port-control auto**
6. **dot1x pae authenticator**
7. **spanning-tree portfast**
8. **end**
9. **show running-config interface *interface-id***
10. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例：  デバイス# <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>cisp enable</b> 例：  デバイス (config)# <b>cisp enable</b>	CISP をイネーブルにします。
ステップ 3	<b>interface interface-id</b> 例：  デバイス (config)# <b>interface gigabitethernet 2/0/1</b>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<b>switchport mode access</b> 例：  デバイス (config-if)# <b>switchport mode access</b>	ポートモードを <b>access</b> に設定します。
ステップ 5	<b>authentication port-control auto</b> 例：  デバイス (config-if)# <b>authentication port-control auto</b>	ポート認証モードを <b>auto</b> に設定します。
ステップ 6	<b>dot1x pae authenticator</b> 例：  デバイス (config-if)# <b>dot1x pae authenticator</b>	インターフェイスをポート アクセス エンティティ (PAE) オーセンティケータとして設定します。
ステップ 7	<b>spanning-tree portfast</b> 例：  デバイス (config-if)# <b>spanning-tree portfast trunk</b>	単一ワーク ステーションまたはサーバに接続されたアクセス ポート上で Port Fast をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 8	<b>end</b> 例：  デバイス(config-if)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 9	<b>show running-config interface interface-id</b> 例：  デバイス# <b>show running-config interface gigabitethernet 2/0/1</b>	設定を確認します。
ステップ 10	<b>copy running-config startup-config</b> 例：  デバイス# <b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。  (注) 変更をコンフィギュレーション ファイルに保存すると、オーセンティケータ インターフェイスがリロード後も引き続きトランク モードになることを意味します。オーセンティケータ インターフェイスをアクセスポートとして維持する場合は、コンフィギュレーション ファイルに変更を保存しないでください。

## NEAT を使用したサブリカント スイッチの設定

スイッチをサブリカントに設定するには、特権 EXEC モードで次の手順を実行します。

### 手順の概要

1. **configure terminal**
2. **cisp enable**
3. **dot1x credentials profile**
4. **username suppswitch**
5. **password password**
6. **dot1x supplicant force-multicast**
7. **interface interface-id**
8. **switchport trunk encapsulation dot1q**
9. **switchport mode trunk**
10. **dot1x pae supplicant**
11. **dot1x credentials profile-name**
12. **end**
13. **show running-config interface interface-id**

## 14. copy running-config startup-config

## 15. Auto Smartport マクロを使用した NEAT の設定

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例：  デバイス# <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>cisp enable</b> 例：  デバイス(config)# <b>cisp enable</b>	CISP をイネーブルにします。
ステップ 3	<b>dot1x credentials profile</b> 例：  デバイス(config)# <b>dot1x credentials test</b>	802.1x クレデンシャル プロファイルを作成します。これは、サブリカントとして設定されるポートに接続する必要があります。
ステップ 4	<b>username suppswitch</b> 例：  デバイス(config)# <b>username suppswitch</b>	ユーザ名を作成します。
ステップ 5	<b>password password</b> 例：  デバイス(config)# <b>password myswitch</b>	新しいユーザ名のパスワードを作成します。
ステップ 6	<b>dot1x supplicant force-multicast</b> 例：  デバイス(config)# <b>dot1x supplicant force-multicast</b>	ユニキャストまたはマルチキャスト パケットのいずれかを受信した場合にスイッチに強制的にマルチキャスト EAPOL だけを送信させます。  これにより、NEAT がすべてのホスト モードでのサブリカント スイッチで機能できるようになります。
ステップ 7	<b>interface interface-id</b> 例：	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。



	コマンドまたはアクション	目的
	デバイス (config) # <code>interface gigabitethernet1/0/1</code>	
ステップ 8	<b>switchport trunk encapsulation dot1q</b> 例： デバイス (config-if) # <code>switchport trunk encapsulation dot1q</code>	ポートをトランク モードに設定します。
ステップ 9	<b>switchport mode trunk</b> 例： デバイス (config-if) # <code>switchport mode trunk</code>	インターフェイスを VLAN トランク ポートとして設定します。
ステップ 10	<b>dot1x pae supplicant</b> 例： デバイス (config-if) # <code>dot1x pae supplicant</code>	インターフェイスをポート アクセス エンティティ (PAE) サブリカントとして設定します。
ステップ 11	<b>dot1x credentials profile-name</b> 例： デバイス (config-if) # <code>dot1x credentials test</code>	802.1x クレデンシヤル プロファイルをインターフェイスに対応付けます。
ステップ 12	<b>end</b> 例： デバイス (config-if) # <code>end</code>	特権 EXEC モードに戻ります。
ステップ 13	<b>show running-config interface interface-id</b> 例： デバイス # <code>show running-config interface gigabitethernet1/0/1</code>	設定を確認します。
ステップ 14	<b>copy running-config startup-config</b> 例： デバイス # <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

	コマンドまたはアクション	目的
ステップ 15	Auto Smartport マクロを使用した NEAT の設定	スイッチ VSA ではなく Auto Smartport ユーザー定義マクロを使用して、オーセンティケータ スイッチを設定することもできます。詳細については、このリリースに対応する『 <i>Auto Smartports Configuration Guide</i> 』を参照してください。

## ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証の設定



(注) スイッチにダウンロードする前に、ダウンロード可能な ACL を ACS で設定する必要があります。

ポートでの認証後、**show ip access-list** 特権 EXEC コマンドを使用して、ポートにダウンロードした ACL を表示できます。



(注) **show ip access-lists interface** コマンドの出力には、dACL フィルタ ID や ACL フィルタ ID は表示されません。これは、物理インターフェイスではなく、各認証セッションのマルチドメイン認証によって作成された仮想ポートに ACL が接続されるためです。dACL フィルタ ID や ACL フィルタ ID を表示するには、**show ip access-lists access-list-name** コマンドを使用します。

### ダウンロード可能な ACL の設定

これらのポリシーは、クライアントが認証され、クライアント IP アドレスが IP デバイストラッキングテーブルに追加された後で有効になります。その後スイッチがダウンロード可能な ACL をポートに適用します。

特権 EXEC モードで次の手順を実行します。

#### 始める前に

SISF ベースのデバイストラッキングは、802.1x 認証を設定するための前提条件です。デバイストラッキングをプログラムまたは手動で有効にしていることを確認します。詳細については、「*SISF ベースのトラッキングの設定*」の章を参照してください。

#### 手順の概要

1. **configure terminal**
2. **aaa new-model**
3. **aaa authorization network default local group radius**
4. **radius-server vsa send authentication**

5. **interface** *interface-id*
6. **ip access-group** *acl-id* **in**
7. **show running-config interface** *interface-id*
8. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例：  デバイス# <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 new-model</b> 例：  デバイス(config)# <b>aaa new-model</b>	AAA をイネーブルにします。
ステップ 3	<b>aaa authorization network default local group radius</b> 例：  デバイス(config)# <b>aaa authorization network default local group radius</b>	許可の方法をローカルに設定します。認可方式を削除するには、 <b>no aaa authorization network default local group radius</b> コマンドを使用します。
ステップ 4	<b>radius-server vsa send authentication</b> 例：  デバイス(config)# <b>radius-server vsa send authentication</b>	RADIUS VSA 送信認証を設定します。
ステップ 5	<b>interface interface-id</b> 例：  デバイス(config)# <b>interface gigabitethernet2/0/4</b>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 6	<b>ip access-group acl-id in</b> 例：  デバイス(config-if)# <b>ip access-group default_acl in</b>	ポートの入力方向のデフォルト ACL を設定します。  (注) <i>acl-id</i> はアクセス リストの名前または番号です。

	コマンドまたはアクション	目的
ステップ 7	<b>show running-config interface <i>interface-id</i></b> 例 : デバイス (config-if) # <b>show running-config interface gigabitethernet2/0/4</b>	設定を確認します。
ステップ 8	<b>copy running-config startup-config</b> 例 : デバイス # <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## ダウンロードポリシーの設定

特権 EXEC モードで次の手順を実行します。

### 始める前に

SISF ベースのデバイストラッキングは、802.1x 認証を設定するための前提条件です。デバイストラッキングをプログラムまたは手動で有効にしていることを確認します。

詳細については、「*SISF* ベースの追跡の設定」を参照してください。

### 手順の概要

1. **configure terminal**
2. **access-list *access-list-number* { deny | permit } { hostname | any | host } log**
3. **interface *interface-id***
4. **ip access-group *acl-id* in**
5. **exit**
6. **aaa new-model**
7. **aaa authorization network default group radius**
8. **radius-server vsa send authentication**
9. **end**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 : デバイス # <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。

	コマンドまたはアクション	目的
ステップ 2	<p><b>access-list</b> <i>access-list-number</i> { <b>deny</b>   <b>permit</b> } { <b>hostname</b>   <b>any</b>   <b>host</b> } <b>log</b></p> <p>例 :</p> <pre>デバイス(config)# access-list 1 deny any log</pre>	<p>デフォルト ポート ACL を定義します。</p> <p><i>access-list-number</i> には、1 ~ 99 または 1300 ~ 1999 の 10 進数を指定します。</p> <p>条件が一致した場合にアクセスを拒否する場合は <b>deny</b> を指定し、許可する場合は <b>permit</b> を指定します。</p> <p><i>source</i> は、次のようなパケットを送信するネットワークまたはホストの送信元アドレスです。</p> <ul style="list-style-type: none"> <li>• <b>hostname</b> : ドット付き 10 進表記による 32 ビット長の値。</li> <li>• <b>any</b> : <i>source</i> および <i>source-wildcard</i> の値 0.0.0.0 255.255.255.255 の省略形を意味するキーワード <i>any</i>。 <i>source-wildcard</i> 値を入力する必要はありません。</li> <li>• <b>host</b> : <i>source</i> および <i>source-wildcard</i> の値 <i>source</i> 0.0.0.0 の省略形を意味するキーワード <i>host</i>。</li> </ul> <p>(任意) <i>source-wildcard</i> ビットを送信元アドレスに適用します。</p> <p>(任意) ログを入力して、エントリと一致するパケットに関する情報ロギングメッセージをコンソールに送信します。</p>
ステップ 3	<p><b>interface</b> <i>interface-id</i></p> <p>例 :</p> <pre>デバイス(config)# interface gigabitethernet2/0/2</pre>	<p>インターフェイス コンフィギュレーション モードを開始します。</p>
ステップ 4	<p><b>ip access-group</b> <i>acl-id</i> <b>in</b></p> <p>例 :</p> <pre>デバイス(config-if)# ip access-group default_acl in</pre>	<p>ポートの入力方向のデフォルト ACL を設定します。</p> <p>(注) <i>acl-id</i> はアクセス リストの名前または番号です。</p>
ステップ 5	<p><b>exit</b></p> <p>例 :</p> <pre>デバイス(config-if)# exit</pre>	<p>グローバル コンフィギュレーション モードに戻ります。</p>

## VLAN ID ベース MAC 認証の設定

	コマンドまたはアクション	目的
ステップ 6	<b>aaa new-model</b> 例：  デバイス(config)# <b>aaa new-model</b>	AAA をイネーブルにします。
ステップ 7	<b>aaa authorization network default group radius</b> 例：  デバイス(config)# <b>aaa authorization network default group radius</b>	許可の方法をローカルに設定します。認可方式を削除するには、 <b>no aaa authorization network default group radius</b> コマンドを使用します。
ステップ 8	<b>radius-server vsa send authentication</b> 例：  デバイス(config)# <b>radius-server vsa send authentication</b>	ベンダー固有属性を認識し使用するために、ネットワーク アクセス サーバーを設定します。  (注) ダウンロード可能な ACL が機能する必要があります。
ステップ 9	<b>end</b> 例：  デバイス(config)# <b>end</b>	特権 EXEC モードに戻ります。

## VLAN ID ベース MAC 認証の設定

特権 EXEC モードで次の手順を実行します。

## 手順の概要

1. **configure terminal**
2. **mab request format attribute 32 vlan access-vlan**
3. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例：  デバイス# <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。

	コマンドまたはアクション	目的
ステップ 2	<b>mab request format attribute 32 vlan access-vlan</b> 例 :  デバイス(config)# <b>mab request format attribute 32 vlan access-vlan</b>	VLAN ID ベース MAC 認証をイネーブルにします。
ステップ 3	<b>copy running-config startup-config</b> 例 :  デバイス# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## 柔軟な認証順序の設定

下の手順で使用される例は、MAB が IEEE 802.1x 認証 (dot1x) の前に試行されるように柔軟な認証の順序設定の順序を変更します。MAB は最初の認証方式として設定されているため、MAB は他のすべての認証方式よりも優先されます。

特権 EXEC モードで次の手順を実行します。

### 手順の概要

1. **configure terminal**
2. **interface *interface-id***
3. **switchport mode access**
4. **authentication order [ dot1x | mab ] | {webauth}**
5. **authentication priority [ dot1x | mab ] | {webauth}**
6. **end**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例 :  デバイス# <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>interface <i>interface-id</i></b> 例 :  デバイス(config)# <b>interface gigabitethernet 1/0/1</b>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	<b>switchport mode access</b> 例：  デバイス(config-if)# <b>switchport mode access</b>	RADIUS サーバを事前に設定した場合に限り、ポートをアクセス モードに設定します。
ステップ 4	<b>authentication order [ dot1x   mab ]   {webauth}</b> 例：  デバイス(config-if)# <b>authentication order mab dot1x</b>	(任意) ポート上で使用される認証方式の順序を設定します。
ステップ 5	<b>authentication priority [ dot1x   mab ]   {webauth}</b> 例：  デバイス(config-if)# <b>authentication priority mab dot1x</b>	(任意) 認証方式をポートプライオリティリストに追加します。
ステップ 6	<b>end</b> 例：  デバイス(config-if)# <b>end</b>	特権 EXEC モードに戻ります。

## Open1x の設定

ポートの許可ステータスの手動制御をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

### 手順の概要

1. **configure terminal**
2. **interface *interface-id***
3. **switchport mode access**
4. **authentication control-direction {both | in}**
5. **authentication fallback *name***
6. **authentication host-mode[multi-auth |multi-domain |multi-host |single-host]**
7. **authentication open**
8. **authentication order [ dot1x | mab ] | {webauth}**
9. **authentication periodic**
10. **authentication port-control {auto | force-authorized | force-un authorized}**
11. **end**



## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例：  デバイス# <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>interface interface-id</b> 例：  デバイス (config)# <b>interface gigabitethernet 1/0/1</b>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<b>switchport mode access</b> 例：  デバイス (config-if)# <b>switchport mode access</b>	RADIUS サーバを設定した場合に限り、ポートをアクセス モードに設定します。
ステップ 4	<b>authentication control-direction {both   in}</b> 例：  デバイス (config-if)# <b>authentication control-direction both</b>	(任意) ポート制御を単方向モードまたは双方向モードに設定します。
ステップ 5	<b>authentication fallback name</b> 例：  デバイス (config-if)# <b>authentication fallback profile1</b>	(任意) 802.1x 認証をサポートしないクライアント用のフォールバック方法として Web 認証を使用するようポートを設定します。
ステップ 6	<b>authentication host-mode[multi-auth  multi-domain  multi-host  single-host]</b> 例：  デバイス (config-if)# <b>authentication host-mode multi-auth</b>	(任意) ポート上で認証マネージャ モードを設定します。
ステップ 7	<b>authentication open</b> 例：  デバイス (config-if)# <b>authentication open</b>	(任意) ポート上でオープン アクセスをイネーブルまたはディセーブルにします。

	コマンドまたはアクション	目的
ステップ 8	<b>authentication order [ dot1x   mab ]   {webauth}</b> 例： デバイス (config-if) # <b>authentication order dot1x webauth</b>	(任意) ポート上で使用される認証方式の順序を設定します。
ステップ 9	<b>authentication periodic</b> 例： デバイス (config-if) # <b>authentication periodic</b>	(任意) ポート上で再認証をイネーブルまたはディセーブルにします。
ステップ 10	<b>authentication port-control {auto   force-authorized   force-un authorized}</b> 例： デバイス (config-if) # <b>authentication port-control auto</b>	(任意) ポートの許可ステータスの手動制御をイネーブルにします。
ステップ 11	<b>end</b> 例： デバイス (config-if) # <b>end</b>	特権 EXEC モードに戻ります。

## ポート上での 802.1x 認証のディセーブル化

802.1x 認証をポートでディセーブルにするには、**no dot1x pae** インターフェイス コンフィギュレーション コマンドを使用します。

ポートで 802.1x 認証をディセーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

### 手順の概要

1. **configure terminal**
2. **interface interface-id**
3. **switchport mode access**
4. **no dot1x pae authenticator**
5. **end**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例：  デバイス# <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>interface interface-id</b> 例：  デバイス(config)# <b>interface gigabitethernet 2/0/1</b>	設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	<b>switchport mode access</b> 例：  デバイス(config-if)# <b>switchport mode access</b>	(任意) RADIUS サーバを設定した場合に限り、ポートをアクセス モードに設定します。
ステップ 4	<b>no dot1x pae authenticator</b> 例：  デバイス(config-if)# <b>no dot1x pae authenticator</b>	ポートでの 802.1x 認証をディセーブルにします。
ステップ 5	<b>end</b> 例：  デバイス(config-if)# <b>end</b>	特権 EXEC モードに戻ります。

## 802.1x 認証設定のデフォルト値へのリセット

802.1x 認証設定をデフォルト値に戻すには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

## 手順の概要

1. **configure terminal**
2. **interface interface-id**
3. **dot1x default**
4. **end**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例：  デバイス# <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>interface interface-id</b> 例：  デバイス (config)# <b>interface gigabitethernet 1/0/2</b>	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、設定するポートを指定します。
ステップ 3	<b>dot1x default</b> 例：  デバイス (config-if)# <b>dot1x default</b>	設定可能な 802.1x のパラメータをデフォルト値へ戻します。
ステップ 4	<b>end</b> 例：  デバイス (config-if)# <b>end</b>	特権 EXEC モードに戻ります。

## 802.1x の統計情報およびステータスのモニターリング

表 51: 特権 EXEC 表示コマンド

コマンド	目的
<b>show dot1x all statistics</b>	すべてのポートの 802.1x 統計情報を表示します。
<b>show dot1x interface interface-id statistics</b>	指定されたポートの 802.1x 統計情報を表示します。
<b>show dot1x all[count  details  statistics  summary]</b>	スイッチの 802.1x 管理ステータスおよび動作ステータスを表示します。
<b>show dot1x interface interface-id</b>	指定されたポートの 802.1x 管理ステータスおよび動作ステータスを表示します。

表 52: グローバル コンフィギュレーション コマンド

コマンド	目的
<b>no dot1x logging verbose</b>	冗長な 802.1x 認証メッセージをフィルタに掛けます (Cisco IOS Release 12.2(55) SE 以降)

出力フィールドの詳細については、このリリースに対応するコマンドリファレンスを参照してください。

## IEEE 802.1x ポートベースの認証の機能履歴

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	IEEE 802.1x ポートベースの認証	IEEE 802.1x 認証は、不正なデバイス (クライアント) によるネットワークアクセスを防止します。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。





## 第 25 章

# Web ベース認証

この章では、デバイスで Web ベース認証を設定する方法について説明します。この章の内容は、次のとおりです。

- [Web ベース認証の概要 \(609 ページ\)](#)
- [Web ベース認証の設定方法 \(620 ページ\)](#)
- [Web ベース認証ステータスの監視 \(635 ページ\)](#)

## Web ベース認証の概要

IEEE 802.1x サプリカントが実行されていないホストシステムでエンドユーザーを認証するには、Web 認証プロキシとして知られている Web ベース認証機能を使用します。



(注) Web ベース認証は、レイヤ 2 およびレイヤ 3 インターフェイス上に設定できます。

HTTP セッションを開始すると、Web ベース認証は、ホストからの受信 HTTP パケットを横取りし、ユーザーに HTML ログイン ページを送信します。ユーザーはクレデンシャルを入力します。このクレデンシャルは、Web ベース認証機能により、認証のために認証、許可、アカウントインテグレーション (AAA) サーバーに送信されます。

認証が成功すると、Web ベース認証はログイン成功 HTML ページをホストに送信し、AAA サーバーから返されたアクセス ポリシーを適用します。

認証に失敗した場合、Web ベース認証は、ログインの失敗を示す HTML ページをユーザーに転送し、ログインを再試行するように、ユーザーにプロンプトを表示します。最大試行回数を超過した場合、Web ベース認証は、ログインの期限切れを示す HTML ページをホストに転送し、このユーザーは待機期間中、ウォッチ リストに載せられます。



(注) 中央 Web 認証リダイレクト用の HTTPS トラフィック インターセプションはサポートされていません。



(注) グローバルパラメータマップ (method-type、custom、redirect) は、すべてのクライアントおよび SSID で同じ Web 認証方式 (consent、web consent、webauth など) を使用するときのみ使用する必要があります。これにより、すべてのクライアントが同じ Web 認証方式になります。

要件により、1つの SSID に consent、別の SSID に webauth を使用する場合、名前付きパラメータマップを2つ使用する必要があります。1番目のパラメータマップには consent を設定し、2番目のパラメータマップには webauth を設定する必要があります。



(注) Webauth クライアントの認証試行時に受信する traceback には、パフォーマンスや行動への影響はありません。これは、ACL アプリケーションの EPM に FFM が返信したコンテキストがすでにキュー解除済み (タイマーの有効期限切れの可能性あり) で、セッションが「未承認」になった場合にまれに発生します。

Web ページがホストされている場所に基づいて、ローカル Web 認証は次のように分類できます。

- 内部：ローカル Web 認証時に、コントローラの内部デフォルト HTML ページ (ログイン、成功、失敗、および期限切れ) が使用されます。
- カスタマイズ：ローカル Web 認証時に、カスタマイズされた Web ページ (ログイン、成功、失敗、および期限切れ) がコントローラにダウンロードされ、使用されます。
- 外部：組み込みまたはカスタム Web ページを使用する代わりに、外部 Web サーバー上でカスタマイズされた Web ページがホストされます。

さまざまな Web 認証ページに基づき、Web 認証のタイプは次のように分類できます。

- *Webauth*：これが基本的な Web 認証です。この場合、コントローラはユーザー名とパスワードの入力が必要なポリシーページを提示します。ネットワークにアクセスするには、ユーザーは正しいクレデンシャルを入力する必要があります。
- *Consent* または *web-passthrough*：この場合、コントローラは [Accept] ボタンまたは [Deny] ボタンが表示されたポリシー ページを提示します。ネットワークにアクセスするには、ユーザーは [Accept] ボタンをクリックする必要があります。
- *Webconsent*：これは webauth と consent の Web 認証タイプの組み合わせです。この場合、コントローラは [Accept] ボタンまたは [Deny] ボタンがあり、ユーザー名とパスワードの入力が必要なポリシーページを提示します。ネットワークにアクセスするには、ユーザーは正しいクレデンシャルを入力して [Accept] ボタンをクリックする必要があります。

## デバイスのロール

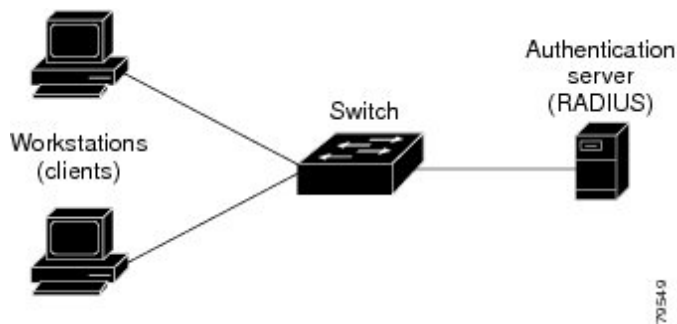
Web ベース認証では、ネットワーク上のデバイスに次のような固有の役割があります。



- クライアント：LAN およびサービスへのアクセスを要求し、スイッチからの要求に応答するデバイス（ワークステーション）。このワークステーションでは、Java Script が有効な HTML ブラウザが実行されている必要があります。
- 認証サーバー：クライアントを認証します。認証サーバーはクライアントの識別情報を確認し、そのクライアントが LAN およびスイッチのサービスへのアクセスを許可されたか、あるいはクライアントが拒否されたのかをスイッチに通知します。
- スイッチ：クライアントの認証ステータスに基づいて、ネットワークへの物理アクセスを制御します。スイッチはクライアントと認証サーバーとの仲介デバイス（プロキシ）として動作し、クライアントに識別情報を要求し、その情報を認証サーバーで確認し、クライアントに応答をリレーします。

図 29: Web ベース認証デバイスの役割

次の図は、ネットワーク上でのこれらのデバイスの役割を示します。



## ホストの検出

スイッチは、検出されたホストに関する情報を格納するために、IP デバイス追跡 テーブルを維持します。

レイヤ 2 インターフェイスでは、Web ベース認証は、これらのメカニズムを使用して、IP ホストを検出します。

- ARP ベースのトリガー：ARP リダイレクト ACL により、Web ベース認証は、スタティック IP アドレス、またはダイナミック IP アドレスを持つホストを検出できます。
- ダイナミック ARP 検査
- DHCP スヌーピング：スイッチがホストの DHCP バインディング エントリを作成するときに Web ベース認証が通知されます。

## セッションの作成

Web ベース認証により、新しいホストが検出されると、次のようにセッションが作成されます。

- 例外リストをレビューします。

ホスト IP が例外リストに含まれている場合、この例外リスト エントリからポリシーが適用され、セッションが確立されます。

- 認証バイパスをレビューします。

ホスト IP が例外リストに含まれていない場合、Web ベース認証は応答しないホスト (NRH) 要求をサーバーに送信します。

サーバーの応答が **access accepted** であった場合、認証はこのホストにバイパスされます。セッションが確立されます。

- HTTP インターセプト ACL を設定します。

NRH 要求に対するサーバーの応答が **access rejected** であった場合、HTTP インターセプト ACL がアクティブ化され、セッションはホストからの HTTP トラフィックを待機します。

## 認証プロセス

Web ベース認証を有効にすると、次のイベントが発生します。

- ユーザーが HTTP セッションを開始します。
- HTTP トラフィックが横取りされ、認証が開始されます。スイッチは、ユーザーにログインページを送信します。ユーザーはユーザー名とパスワードを入力します。スイッチはこのエントリを認証サーバーに送信します。
- 認証に成功した場合、スイッチは認証サーバーからこのユーザーのアクセスポリシーをダウンロードし、アクティブ化します。ログインの成功ページがユーザーに送信されます。
- 認証に失敗した場合は、スイッチはログインの失敗ページを送信します。ユーザーはログインを再試行します。失敗の回数が試行回数の最大値に達した場合、スイッチはログイン期限切れページを送信します。このホストはウォッチリストに入れられます。ウォッチリストのタイムアウト後、ユーザーは認証プロセスを再試行することができます。
- 認証サーバーがスイッチに応答せず、AAA 失敗ポリシーが設定されている場合、スイッチはホストに失敗アクセスポリシーを適用します。ログインの成功ページがユーザーに送信されます。
- ホストがレイヤ 2 インターフェイス上の ARP プローブに回答しなかった場合、またはホストがレイヤ 3 インターフェイスでアイドルタイムアウト内にトラフィックを送信しなかった場合、スイッチはクライアントを再認証します。
- この機能は、ダウンロードされたタイムアウト、またはローカルに設定されたセッションタイムアウトを適用します。



- 
- (注) Cisco IOS XE Denali 16.1.1 以降では、WLC での Web ベース認証のデフォルトのセッションタイムアウト値は 1800 秒です。Cisco IOS XE Denali 16.1.1 より前は、デフォルトのセッションタイムアウト値は無限の秒数でした。
-

- Termination-Action が RADIUS である場合、この機能は、サーバーに NRH 要求を送信します。Termination-Action は、サーバーからの応答に含まれます。
- Termination-Action がデフォルトである場合、セッションは廃棄され、適用されたポリシーは削除されます。

## ローカル Web 認証バナー

Web 認証を使用して、デフォルトのカスタマイズ済み Web ブラウザ バナーを作成して、スイッチにログインしたときに表示するようにできます。

このバナーは、ログインページと認証結果ポップアップページの両方に表示されます。デフォルトのバナー メッセージは次のとおりです。

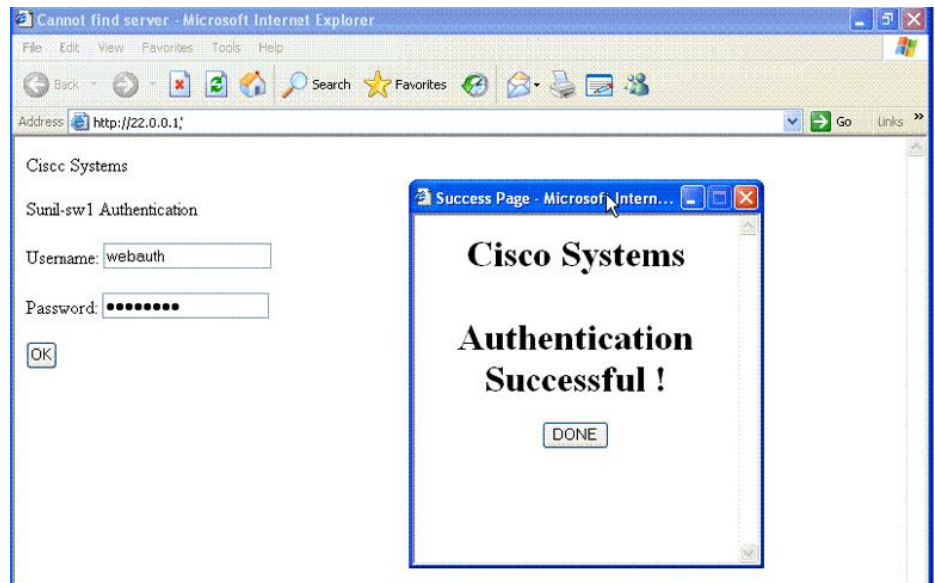
- 認証成功
- 認証失敗
- 認証期限切れ

ローカル ネットワーク 認証バナーは、レガシーおよび新スタイル（セッション アウェア）の CLI で次のように設定できます。

- レガシー モード : **ip admission auth-proxy-banner http** 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。
- 新スタイル モード : **parameter-map type webauth global banner** 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。

ログインページには、デフォルトのバナー、*Cisco Systems*、および *Switch host-name Authentication* が表示されます。*Cisco Systems* は認証結果ポップアップ ページに表示されます。

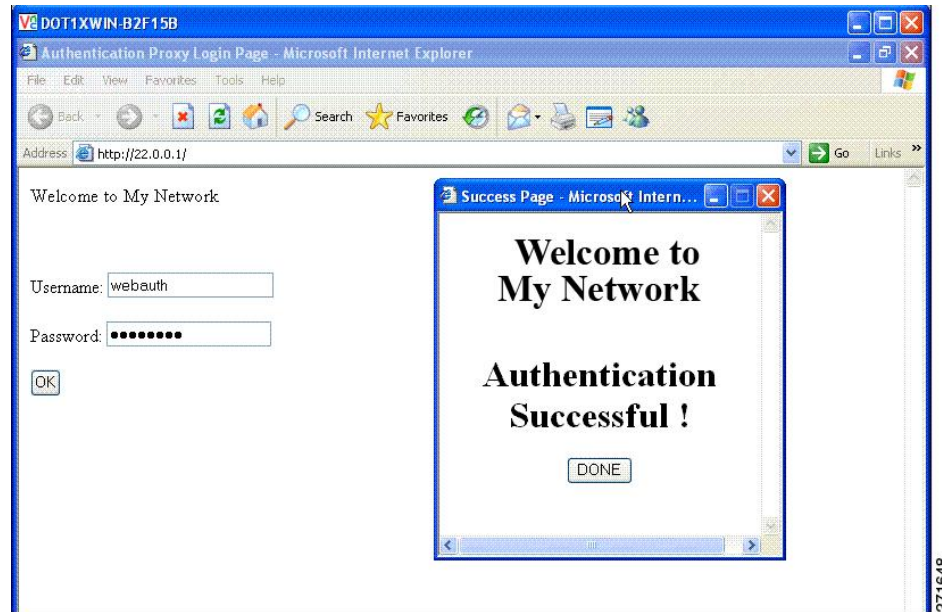
図 30: 認証成功バナー



バナーは次のようにカスタマイズ可能です。

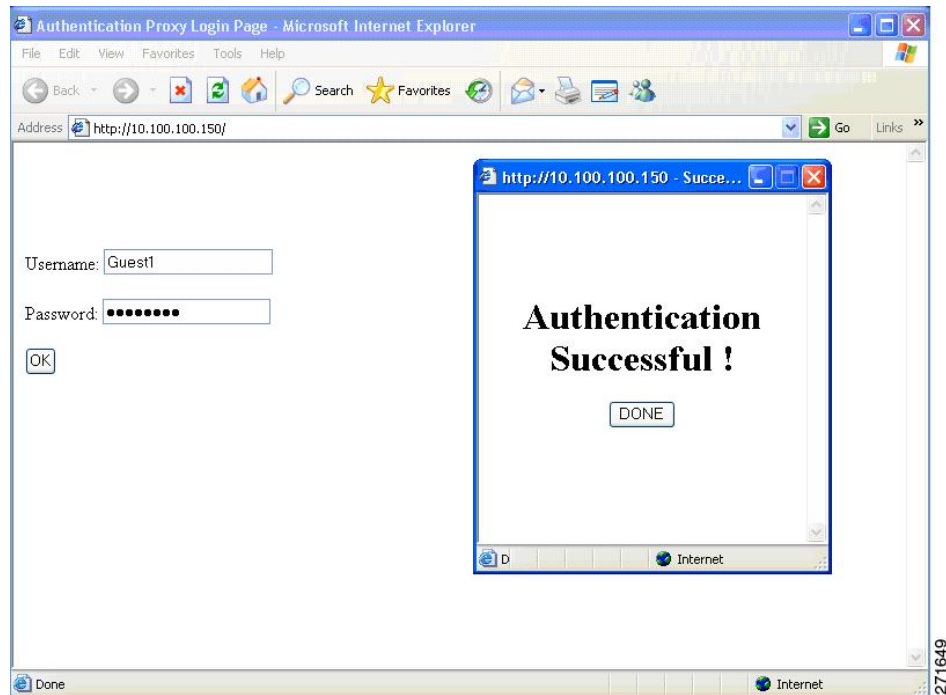
- スイッチ名、ルータ名、または会社名などのメッセージをバナーに追加する。
  - レガシーモード : **ip admission auth-proxy-banner http banner-text** グローバル コンフィギュレーション コマンドを使用します。
  - 新スタイル モード : **parameter-map type webauth global banner** グローバル コンフィギュレーション コマンドを使用します。
- ログまたはテキスト ファイルをバナーに追加する。
  - レガシーモード : **ip admission auth-proxy-banner http file-path** 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。
  - 新スタイル モード : **parameter-map type webauth global banner** 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。

図 31: カスタマイズされた Web バナー



バナーが有効にされていない場合、Web 認証ログイン画面にはユーザー名とパスワードのダイアログボックスだけが表示され、スイッチにログインしたときにはバナーは表示されません。

図 32: バナーが表示されていないログイン画面



## Web 認証カスタマイズ可能な Web ページ

Web ベース認証プロセスでは、スイッチ内部の HTTP サーバーは、認証中のクライアントに配信される 4 種類の HTML ページをホストします。サーバーはこれらのページを使用して、ユーザーに次の 4 種類の認証プロセス ステートを通知します。

- ログイン：資格情報が要求されています。
- 成功：ログインに成功しました。
- 失敗：ログインに失敗しました。
- 期限切れ：ログインの失敗回数が多すぎて、ログインセッションが期限切れになりました。

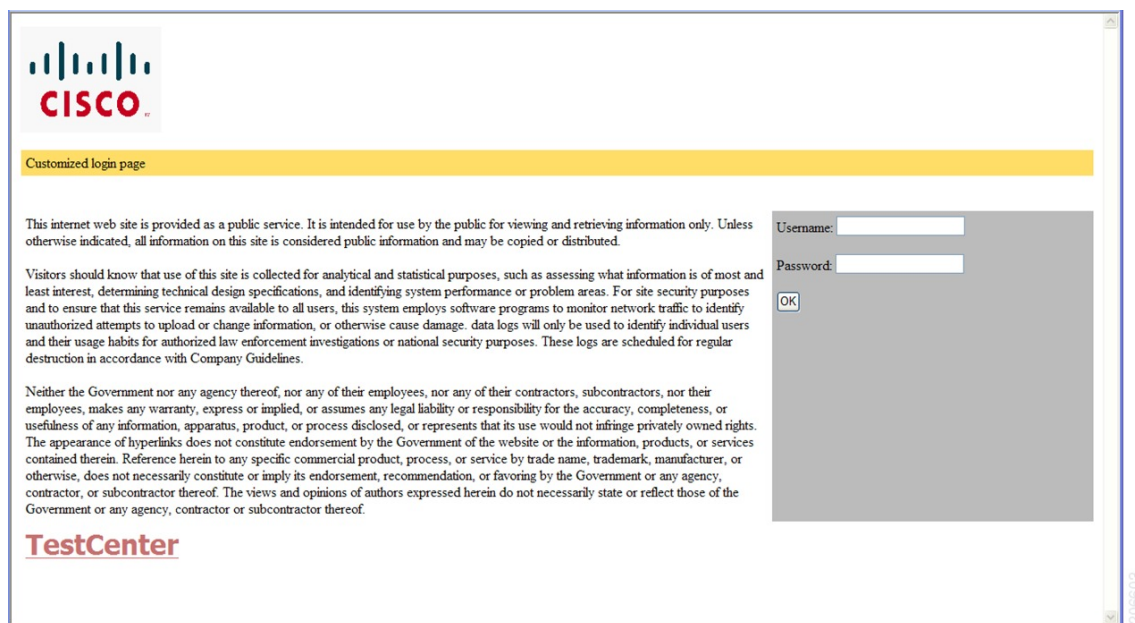
### ガイドライン

- デフォルトの内部 HTML ページの代わりに、独自の HTML ページを使用することができます。
- ロゴを使用することもできますし、ログイン、成功、失敗、および期限切れ Web ページでテキストを指定することもできます。
- バナー ページで、ログイン ページのテキストを指定できます。
- これらのページは、HTML で記述されています。
- 成功ページには、特定の URL にアクセスするための HTML リダイレクト コマンドを記入する必要があります。
- この URL 文字列は有効な URL（例：<http://www.cisco.com>）でなければなりません。不完全な URL は、Web ブラウザで、「ページが見つかりません」またはこれに類似するエラーの原因となる可能性があります。
- HTTP 認証で使用される Web ページを設定する場合、これらのページには適切な HTML コマンド（例：ページのタイムアウトを設定、暗号化されたパスワードの設定、同じページが 2 回送信されていないことの確認など）を記入する必要があります。
- 設定されたログイン フォームが有効な場合、特定の URL にユーザーをリダイレクトする CLI コマンドは使用できません。管理者は、Web ページにリダイレクトが設定されていることを保証する必要があります。
- 認証後、特定の URL にユーザーをリダイレクトする CLI コマンドを入力してから、Web ページを設定するコマンドを入力した場合、特定の URL にユーザーをリダイレクトする CLI コマンドは効力を持ちません。
- 設定された Web ページは、スイッチのブート フラッシュ、またはフラッシュにコピーできます。
- スタック可能なスイッチでは、アクティブスイッチまたはメンバスイッチのフラッシュから設定済みのページにアクセスできます。

- ログインページを任意のフラッシュ上に、成功ページと失敗ページを別のフラッシュ（たとえば、アクティブスイッチ、またはメンバスイッチのフラッシュ）に配置できます。
- 4 ページすべてを設定する必要があります。
- Web ページを使ってバナー ページを設定した場合、このバナー ページには効果はありません。
- システムディレクトリ（たとえば、flash、disk0、disk）に保存されていて、ログインページに表示する必要のあるロゴファイル（イメージ、フラッシュ、オーディオ、ビデオなど）すべてには、必ず、`web_auth_<filename>` の形式で名前をつけてください。
- 設定された認証プロキシ機能は、HTTP と SSL の両方をサポートしています。

デフォルトの内部 HTML ページの代わりに、自分の HTML ページを使用することができます。認証後のユーザーのリダイレクト先で、内部成功ページの代わりとなる URL を指定することもできます。

図 33: カスタマイズ可能な認証ページ



## 認証プロキシ Web ページの注意事項

カスタマイズされた認証プロキシ Web ページを設定する際には、次の注意事項に従ってください。

- カスタム Web ページ機能を有効にするには、カスタム HTML ファイルを 4 個すべて指定します。指定したファイルの数が 4 個未満の場合、内部デフォルト HTML ページが使用されます。
- これら 4 個のカスタム HTML ファイルは、スイッチのフラッシュ メモリ内に存在しなければなりません。各 HTML ファイルの最大サイズは 8 KB です。

- カスタム ページ上のイメージはすべて、アクセス可能はHTTPサーバー上に存在しなければなりません。インターセプト ACL は、管理ルール内で設定します。
- カスタム ページからの外部リンクはすべて、管理ルール内でのインターセプト ACL の設定を必要とします。
- 有効な DNS サーバーにアクセスするには、外部リンクまたはイメージに必要な名前解決で、管理ルール内にインターセプト ACL を設定する必要があります。
- カスタム Web ページ機能が有効に設定されている場合、設定された auth-proxy-banner は使用されません。
- カスタム Web ページ機能が有効に設定されている場合、ログインの成功に対するリダイレクション URL は使用できません。
- カスタム ファイルの指定を解除するには、このコマンドの **no** 形式を使用します。

カスタム ログイン ページはパブリック Web フォームであるため、このページについては、次の注意事項に従ってください。

- ログインフォームは、ユーザーによるユーザー名とパスワードの入力を受け付け、これらを **uname** および **pwd** として示す必要があります。
- カスタム ログイン ページは、ページタイムアウト、暗号化されたパスワード、冗長送信の防止など、Web フォームに対するベストプラクティスに従う必要があります。

## 成功ログインに対するリダイレクト URL の注意事項

成功ログインに対するリダイレクション URL を設定する場合、次の注意事項に従ってください。

- カスタム認証プロキシ Web ページ機能がイネーブルに設定されている場合、リダイレクション URL 機能はディセーブルにされ、CLI では使用できません。リダイレクションは、カスタム ログイン成功ページで実行できます。
- リダイレクション URL 機能が有効に設定されている場合、設定された auth-proxy-banner は使用されません。
- リダイレクション URL の指定を解除するには、このコマンドの **no** 形式を使用します。
- Web ベースの認証クライアントが正常に認証された後にリダイレクション URL が必要な場合、URL 文字列は有効な URL (たとえば `http://`) で開始し、その後に URL 情報が続く必要があります。 `http://` を含まない URL が指定されると、正常に認証が行われても、そのリダイレクション URL によって Web ブラウザでページが見つからないまたは同様のエラーが生じる場合があります。



## その他の機能と Web ベース認証の相互作用

### ポートセキュリティ

Web ベース認証とポートセキュリティは、同じポートに設定できます。Web ベース認証はポートを認証し、ポートセキュリティは、クライアントの MAC アドレスを含むすべての MAC アドレスに対するネットワーク アクセスを管理します。この場合、このポートを介してネットワークへアクセスできるクライアントの数とグループを制限できます。

### LAN ポート IP

LAN ポート IP (LPIP) とレイヤ 2 Web ベース認証は、同じポートに設定できます。ホストは、まず Web ベース認証、次に LPIP ポスチャ検証を使用して認証されます。LPIP ホストポリシーは、Web ベース認証のホストポリシーに優先されます。

Web ベース認証のアイドル時間が満了すると、NAC ポリシーは削除されます。ホストが認証され、ポスチャが再度検証されます。

### ゲートウェイ IP

VLAN のいずれかのスイッチポートで Web ベース認証が設定されている場合、レイヤ 3 VLAN インターフェイス上にゲートウェイ IP (GWIP) を設定することはできません。

Web ベース認証はゲートウェイ IP と同じレイヤ 3 インターフェイスに設定できます。ソフトウェアで、両方の機能のホストポリシーが適用されます。GWIP ホストポリシーは、Web ベース認証のホストポリシーに優先されます。

### ACL

インターフェイスで VLAN ACL、または Cisco IOS ACL を設定した場合、ACL は、Web ベース認証のホストポリシーが適用された後だけ、ホストトラフィックに適用されます。

レイヤ 2 Web ベース認証では、ポートに接続されたホストからの受信トラフィックについて、ポート ACL (PACL) をデフォルトのアクセスポリシーとして設定することが必須ではないものの、より安全です。認証後、Web ベース認証のホストポリシーは、PACL に優先されます。ポートに設定された ACL がなくても、ポリシー ACL はセッションに適用されます。

MAC ACL と Web ベース認証を同じインターフェイスに設定することはできません。

アクセス VLAN が VACL キャプチャ用に設定されているポートには Web ベース認証は設定できません。

### コンテキストベース アクセス コントロール

コンテキストベース アクセス コントロール (CBAC) が、ポート VLAN のレイヤ 3 VLAN インターフェイスで設定されている場合、レイヤ 2 ポートで Web ベース認証は設定できません。

## EtherChannel

Web ベース認証は、レイヤ 2 EtherChannel インターフェイス上に設定できます。Web ベース認証設定は、すべてのメンバチャンネルに適用されます。

# Web ベース認証の設定方法

## デフォルトの Web ベース認証の設定

次の表に、デフォルトの Web ベース認証の設定を示しています。

表 53: デフォルトの Web ベース認証の設定

機能	デフォルト設定
AAA	無効
RADIUS サーバ <ul style="list-style-type: none"> <li>• IP アドレス</li> <li>• UDP 認証ポート</li> <li>• キー</li> </ul>	<ul style="list-style-type: none"> <li>• 指定なし</li> <li>• 指定なし</li> </ul>
無活動タイムアウトのデフォルト値	3600 秒
無活動タイムアウト	有効

## Web ベース認証の設定に関する注意事項と制約事項

- Web ベース認証は受信時だけの機能です。
- Web ベース認証は、アクセス ポートだけで設定できます。Web ベース認証は、トランクポート、EtherChannel メンバポート、またはダイナミック トランクポートではサポートされていません。
- スイッチが特定のホストまたは Web サーバーにクライアントをリダイレクトしてログインメッセージを表示する場合、外部 Web 認証はサポートされません。
- スタティックな ARP キャッシュが割り当てられているレイヤ 2 インターフェイス上のホストは認証できません。これらのホストは ARP メッセージを送信しないため、Web ベース認証機能では検出されません。
- デフォルトでは、スイッチの IP デバイス追跡機能は無効にされています。Web ベース認証を使用するには、IP デバイス追跡機能を有効にする必要があります。

- Web ベース認証を使用するには、SISF ベースのデバイス追跡を有効にする必要があります。デフォルトでは、SISF ベースのデバイス追跡はスイッチで無効になっています。
- スイッチ HTTP サーバーを実行するには、IP アドレスを少なくとも 1 つ設定する必要があります。また、各ホスト IP アドレスに到達するようにルートを設定する必要があります。HTTP サーバーは、ホストに HTTP ログイン ページを送信します。
- 2 ホップ以上離れたところにあるホストでは、STP トポロジの変更により、ホストトラフィックの到着するポートが変わってしまった場合、トラフィックが停止する可能性があります。これは、レイヤ 2 (STP) トポロジの変更後に、ARP および DHCP の更新が送信されていない場合に発生します。
- Web ベース認証は、ダウンロード可能なホストポリシーとして、VLAN 割り当てをサポートしていません。
- Web ベース認証はセッション認識型ポリシー モードで IPv6 をサポートします。IPv6 Web 認証には、スイッチで設定された少なくとも 1 つの IPv6 アドレスおよびスイッチ ポートに設定された IPv6 スヌーピングが必要です。
- Web ベース認証および Network Edge Access Topology (NEAT) は、相互に排他的です。インターフェイス上で NEAT が有効の場合、Web ベース認証を使用できず、インターフェイス上で Web ベース認証が実行されている場合は、NEAT を使用できません。
- スイッチから RADIUS サーバーへの通信の設定に使用される次の RADIUS セキュリティサーバー設定を確認します。
  - ホスト名
  - ホスト IP アドレス
  - ホスト名と特定の UDP ポート番号
  - IP アドレスと特定の UDP ポート番号

IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、サーバーの同一 IP アドレス上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。同じ RADIUS サーバー上の異なる 2 つのホスト エントリに同じサービス（たとえば認証）を設定した場合、2 番めに設定されたホスト エントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作します。RADIUS ホスト エントリは、設定した順序に従って選択されます。

- RADIUS サーバー パラメータを設定する場合は、次の点に注意してください。
  - 別のコマンドラインに、**key string** を指定します。
  - **key string** には、スイッチと、RADIUS サーバー上で動作する RADIUS デーモンとの間で使用する、認証および暗号キーを指定します。キーは、RADIUS サーバーで使用する暗号化キーに一致するテキスト スtring でなければなりません。
  - **key string** を指定する場合、キーの中間、および末尾にスペースを使用します。キーにスペースを使用する場合は、引用符がキーの一部である場合を除き、引用符で

キーを囲まないでください。キーはRADIUSデーモンで使用する暗号に一致している必要があります。

- すべてのRADIUSサーバーについて、タイムアウト、再送信回数、および暗号キー値をグローバルに設定するには、**radius-server host** 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。これらのオプションをサーバー単位で設定するには、**radius-server timeout**、**radius-server transmit**、および **radius-server key** 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。



(注) RADIUS サーバーでは、スイッチの IP アドレス、サーバーとスイッチで共有される **key string**、およびダウンロード可能な ACL (DACL) などの設定を行う必要があります。詳細については、RADIUS サーバーのマニュアルを参照してください。

- URL リダイレクト ACL の場合：
  - 許可アクセス コントロール エントリ (ACE) ルールに一致するパケットは、AAA サーバーに転送するために CPU に送信されます。
  - 拒否 ACE ルールに一致するパケットは、スイッチを介して転送されます。
  - 許可 ACE ルールにも拒否 ACE ルールにも一致しないパケットは、次の dACL によって処理されます。dACL がない場合、パケットは暗黙的拒否 ACL にヒットしてドロップされます。

## 認証ルールとインターフェイスの設定

認証ルールおよびインターフェイスを設定するには、次の手順を実行します。

### 始める前に

SISF ベースのデバイス追跡は、web 認証の前提条件です。デバイス追跡をプログラムまたは手動で有効にしていることを確認します。

詳細については、「*SISF* ベースの追跡の設定」を参照してください。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **ip admission name name proxy http**
4. **interface type slot/port**
5. **ip access-group name**
6. **ip admission name**
7. **end**

8. **show ip admission**
9. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  デバイス> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  デバイス# <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 3	<b>ip admission name name proxy http</b> 例：  デバイス(config)# <b>ip admission name webauth1 proxy http</b>	Web ベース許可の認証ルールを設定します。
ステップ 4	<b>interface type slot/port</b> 例：  デバイス(config)# <b>interface gigabitethernet 1/0/1</b>	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、Web ベース認証を有効にする受信レイヤ 2 またはレイヤ 3 インターフェイスを指定します。  <i>type</i> には、fastethernet、gigabit ethernet、または tengigabitethernet を指定できます。
ステップ 5	<b>ip access-group name</b> 例：  デバイス(config-if)# <b>ip access-group webauthag</b>	デフォルト ACL を適用します。
ステップ 6	<b>ip admission name</b> 例：  デバイス(config)# <b>ip admission name</b>	インターフェイスの Web ベース認可の認証ルールを設定します。
ステップ 7	<b>end</b> 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	デバイス(config)# <b>end</b>	
ステップ 8	<b>show ip admission</b> 例： デバイス# <b>show ip admission</b>	設定を表示します。
ステップ 9	<b>copy running-config startup-config</b> 例： デバイス# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## AAA 認証の設定

### 手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authentication login default group {tacacs+ | radius}**
5. **aaa authorization auth-proxy default group {tacacs+ | radius}**
6. **tacacs server *server-name***
7. **address {ipv4 | ipv6} *ip address***
8. **key** 文字列
9. **exit**
10. **end**
11. **show running-config**
12. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： デバイス> <b>enable</b>	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	<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
	デバイス# <code>configure terminal</code>	
ステップ 3	<b>aaa new-model</b> 例 : デバイス (config)# <code>aaa new-model</code>	AAA 機能をイネーブルにします。
ステップ 4	<b>aaa authentication login default group {tacacs+   radius}</b> 例 : デバイス (config)# <code>aaa authentication login default group tacacs+</code>	ログイン時の認証方法のリストを定義します。 <b>named_authentication_list</b> は、31 文字未満の名前を示します。 <b>AAA_group_name</b> はサーバー グループ名を示します。サーバーグループ <b>server_name</b> をその先頭で定義する必要があります。
ステップ 5	<b>aaa authorization auth-proxy default group {tacacs+   radius}</b> 例 : デバイス (config)# <code>aaa authorization auth-proxy default group tacacs+</code>	Web ベース許可の許可方式リストを作成します。
ステップ 6	<b>tacacs server server-name</b> 例 : デバイス (config)# <code>tacacs server yourserver</code>	AAA サーバーを指定します。
ステップ 7	<b>address {ipv4   ipv6} ip address</b> 例 : デバイス (config-server-tacacs)# <code>address ipv4 10.0.1.12</code>	TACACS サーバーの IP アドレスを設定します。
ステップ 8	<b>key 文字列</b> 例 : デバイス (config-server-tacacs)# <code>key cisco123</code>	スイッチと TACACS サーバーとの間で使用される許可および暗号キーを設定します。
ステップ 9	<b>exit</b> 例 :	TACACS サーバーモードを終了して、グローバル コンフィギュレーションモードを開始します。

	コマンドまたはアクション	目的
	デバイス (config-server-tacacs) # <b>exit</b>	
ステップ 10	<b>end</b> 例 : デバイス (config) # <b>end</b>	特権 EXEC モードに戻ります。
ステップ 11	<b>show running-config</b> 例 : デバイス # <b>show running-config</b>	入力を確認します。
ステップ 12	<b>copy running-config startup-config</b> 例 : デバイス # <b>copy running-config startup-config</b>	(任意) コンフィギュレーション ファイルに設定を保存します。

## スイッチ/RADIUS サーバー間通信の設定

RADIUS サーバーのパラメータを設定するには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **ip radius source-interface**
4. **radius server** *server name*
5. **address** {*ipv4* | *ipv6*} *ip address*
6. **key** *string*
7. **exit**
8. **radius-server dead-criteria tries** *num-tries*
9. **end**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 :	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。



	コマンドまたはアクション	目的
	デバイス> <code>enable</code>	
ステップ 2	<b>configure terminal</b> 例：  デバイス# <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 3	<b>ip radius source-interface</b> 例：  デバイス(config)# <code>ip radius source-interface vlan 80</code>	RADIUS パケットが、指定されたインターフェイスの IP アドレスを含むように指定します。
ステップ 4	<b>radius server <i>server name</i></b> 例：  デバイス(config)# <code>radius server rsim address ipv4 124.2.2.12</code>	(任意) RADIUS サーバーの IP アドレスを指定します。
ステップ 5	<b>address {ipv4   ipv6} <i>ip address</i></b> 例：  デバイス(config-radius-server)# <code>address ipv4 10.0.1.2 auth-port 1550 acct-port 1560</code>	RADIUS サーバーの IP アドレスを設定します。
ステップ 6	<b>key <i>string</i></b> 例：  デバイス(config-radius-server)# <code>key rad123</code>	(任意) RADIUS サーバー上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号キーを指定します。
ステップ 7	<b>exit</b> 例：  デバイス(config-radius-server)# <code>exit</code>	RADIUS サーバーモードを終了して、グローバル コンフィギュレーション モードを開始します。
ステップ 8	<b>radius-server dead-criteria tries <i>num-tries</i></b> 例：  デバイス(config)# <code>radius-server dead-criteria tries</code>	RADIUS サーバーに送信されたメッセージへの応答がない場合に、このサーバーが非アクティブであると見なすまでの送信回数を指定します。指定できる <i>num-tries</i> の範囲は 1 ~ 100 です。

	コマンドまたはアクション	目的
	30	
ステップ 9	<b>end</b> 例：  デバイス(config)# <b>end</b>	特権 EXEC モードに戻ります。

## HTTP サーバーの設定

Web ベース認証を使用するには、デバイスで HTTP サーバをイネーブルにする必要があります。このサーバーは HTTP または HTTPS のいずれかについて有効にできます。



(注) Apple の疑似ブラウザは、**ip http secure-server** コマンドを設定するだけでは開きません。**ip http server** コマンドも設定する必要があります。

HTTP または HTTPS のいずれかでサーバーを有効にするには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **ip http server**
4. **ip http secure-server**
5. **end**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  デバイス> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  デバイス# <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。

	コマンドまたはアクション	目的
ステップ 3	<b>ip http server</b> 例 :  デバイス (config) # <b>ip http server</b>	HTTP サーバーを有効にします。Web ベース認証機能は、HTTP サーバーを使用してホストと通信し、ユーザー認証を行います。
ステップ 4	<b>ip http secure-server</b> 例 :  デバイス (config) # <b>ip http secure-server</b>	HTTPS を有効にします。  カスタム認証プロキシ Web ページを設定するか、成功ログインのリダイレクション URL を指定します。  (注) <b>ip http secure-server</b> コマンドを入力したときに、セキュア認証が確実に行われるようにするには、ユーザーが HTTP 要求を送信した場合でも、ログイン ページは必ず HTTPS (セキュア HTTP) 形式になるようにします。
ステップ 5	<b>end</b> 例 :  デバイス (config) # <b>end</b>	特権 EXEC モードに戻ります。

## 認証プロキシ Web ページのカスタマイズ

Web ベースの認証中、デバイスのデフォルト HTML ページではなく、代替の HTML ページがユーザーに表示されるように、Web 認証を設定できます。

カスタム認証プロキシ Web ページの使用を指定するには、次の手順を実行してください。

### 始める前に

デバイスのフラッシュ メモリにカスタム HTML ファイルを保存します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **ip admission proxy http login page file device:login-filename**
4. **ip admission proxy http success page file device:success-filename**
5. **ip admission proxy http failure page file device:fail-filename**
6. **ip admission proxy http login expired page file device:expired-filename**
7. **end**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : デバイス> <b>enable</b>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>パスワードを入力します (要求された場合)。</li> </ul>
ステップ 2	<b>configure terminal</b> 例 : デバイス# <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 3	<b>ip admission proxy http login page file</b> <i>device:login-filename</i> 例 : デバイス (config)# <b>ip admission proxy http login page file disk1:login.htm</b>	デバイスのメモリ ファイル システム内で、デフォルトのログインページの代わりに使用するカスタム HTML ファイルの場所を指定します。 <i>device:</i> はフラッシュ メモリです。
ステップ 4	<b>ip admission proxy http success page file</b> <i>device:success-filename</i> 例 : デバイス (config)# <b>ip admission proxy http success page file disk1:success.htm</b>	デフォルトのログイン成功ページの代わりに使用するカスタム HTML ファイルの場所を指定します。
ステップ 5	<b>ip admission proxy http failure page file</b> <i>device:fail-filename</i> 例 : デバイス (config)# <b>ip admission proxy http fail page file disk1:fail.htm</b>	デフォルトのログイン失敗ページの代わりに使用するカスタム HTML ファイルの場所を指定します。
ステップ 6	<b>ip admission proxy http login expired page file</b> <i>device:expired-filename</i> 例 : デバイス (config)# <b>ip admission proxy http login expired page file disk1:expired.htm</b>	デフォルトのログイン失効ページの代わりに使用するカスタム HTML ファイルの場所を指定します。
ステップ 7	<b>end</b> 例 :	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	デバイス(config)# <b>end</b>	

## 成功ログインに対するリダイレクション URL の指定

認証後に内部成功 HTML ページを効果的に置き換えユーザーのリダイレクト先となる URL を指定するためには、次の手順を実行してください。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **ip admission proxy http success redirect *url-string***
4. **end**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： デバイス> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例： デバイス# <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 3	<b>ip admission proxy http success redirect <i>url-string</i></b> 例： デバイス(config)# <b>ip admission proxy http success redirect www.example.com</b>	デフォルトのログイン成功ページの代わりにユーザーをリダイレクトする URL を指定します。
ステップ 4	<b>end</b> 例： デバイス(config)# <b>end</b>	特権 EXEC モードに戻ります。

## Web ベース認証パラメータの設定

クライアントが待機時間中にウォッチリストに掲載されるまで許容される失敗ログイン試行の最大回数を設定するには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **ip admission max-login-attempts *number***
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  デバイス> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  デバイス# <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 3	<b>ip admission max-login-attempts <i>number</i></b> 例：  デバイス(config)# <b>ip admission max-login-attempts 10</b>	失敗ログイン試行の最大回数を設定します。指定できる範囲は 1 ～ 2147483647 回です。デフォルトは 5 分です。
ステップ 4	<b>end</b> 例：  デバイス(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show running-config</b> 例：  デバイス# <b>show running-config</b>	入力を確認します。

	コマンドまたはアクション	目的
ステップ 6	<b>copy running-config startup-config</b> 例： デバイス# <code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

## Web ベースの認証ローカル バナーの設定

Web 認証が設定されているスイッチにローカル バナーを設定するには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **ip admission auth-proxy-banner http** [*banner-text* | *file-path*]
4. **end**
5. **show running-config**
6. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： デバイス> <code>enable</code>	特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> <li>• パスワードを入力します (要求された場合)。</li> </ul>
ステップ 2	<b>configure terminal</b> 例： デバイス# <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 3	<b>ip admission auth-proxy-banner http</b> [ <i>banner-text</i>   <i>file-path</i> ] 例： デバイス (config)# <code>ip admission auth-proxy-banner http C My Switch C</code>	ローカル バナーを有効にします。 (任意) <i>C banner-text C</i> ( <i>C</i> は区切り文字)、またはバナーに表示されるファイル (たとえばロゴまたはテキストファイル) のファイルパスを入力して、カスタムバナーを作成します。

	コマンドまたはアクション	目的
ステップ 4	<b>end</b> 例：  デバイス(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show running-config</b> 例：  デバイス# <b>show running-config</b>	入力を確認します。
ステップ 6	<b>copy running-config startup-config</b> 例：  デバイス# <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## Web ベース認証キャッシュ エントリの削除

Web ベース認証キャッシュ エントリを削除するには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **clear ip auth-proxy cache** *{\*| host ip address}*
3. **clear ip admission cache** *{\*| host ip address}*

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  デバイス> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します (要求された場合)。
ステップ 2	<b>clear ip auth-proxy cache</b> <i>{*  host ip address}</i> 例：  デバイス# <b>clear ip auth-proxy cache 192.168.4.5</b>	Delete 認証プロキシエントリを削除します。キャッシュエントリすべてを削除するには、アスタリスクを使用します。シングルホストのエントリを削除するには、具体的な IP アドレスを入力します。



	コマンドまたはアクション	目的
ステップ 3	<b>clear ip admission cache</b> <i>{*  host ip address}</i> 例： デバイス# <b>clear ip admission cache 192.168.4.5</b>	Delete 認証プロキシエントリを削除します。キャッシュエントリすべてを削除するには、アスタリスクを使用します。シングルホストのエントリを削除するには、具体的な IP アドレスを入力します。

## Web ベース認証ステータスの監視

すべてのインターフェイスまたは特定のポートに対する Web ベース認証設定を表示するには、このトピックのコマンドを使用します。

表 54: 特権 EXEC 表示コマンド

コマンド	目的
<b>show authentication sessions method webauth</b>	FastEthernet、ギガビットイーサネット、または 10 ギガビットイーサネットのすべてのインターフェイスに対する Web ベースの認証設定を表示します。
<b>show authentication sessions interface type slot/port[details]</b>	FastEthernet、ギガビットイーサネット、または 10 ギガビットイーサネットの特定のインターフェイスに対する Web ベースの認証設定を表示します。  セッション認識型ネットワーク モードでは、 <b>show access-session interface</b> コマンドを使用します。





## 第 26 章

# ポート単位のトラフィック制御の設定

- [ポートベースのトラフィック制御の概要 \(637 ページ\)](#)

## ポートベースのトラフィック制御の概要

ポートベースのトラフィック制御は、特定トラフィック状態に応じてポートレベルでパケットをフィルタまたはブロックするために使用する Cisco Catalyst スイッチ上のレイヤ 2 機能の組み合わせです。次のポートベースのトラフィック制御機能がサポートされています。

- ストーム制御
- 保護ポート
- ポートブロッキング

## ストーム制御に関する情報

### ストーム制御

ストーム制御は、物理インターフェイスの 1 つで発生したブロードキャスト、マルチキャスト、またはユニキャストストームによって LAN 上のトラフィックが混乱することを防ぎます。LAN ストームは、LAN にパケットがフラッディングした場合に発生します。その結果、トラフィックが極端に増えてネットワークパフォーマンスが低下します。プロトコルスタックの実装エラー、ネットワーク構成の間違い、またはユーザによって引き起こされる DoS 攻撃もストームの原因になります。

ストームコントロール（またはトラフィック抑制）は、インターフェイスからスイッチングバスを通過するパケットをモニタし、パケットがユニキャスト、マルチキャスト、またはブロードキャストのいずれであるかを判別します。スイッチは、1 秒間に受け取った特定のタイプのパケットの数をカウントして、事前に定義された抑制レベルのしきい値とその測定結果を比較します。

## トラフィック アクティビティの測定方法

ストーム コントロールは、次のうちのいずれかをトラフィック アクティビティの測定方法に使用します。

- 帯域幅（ブロードキャスト、マルチキャスト、またはユニキャストトラフィックが使用できるポートの総帯域幅の割合）。
- 秒単位で受信するパケット（ブロードキャスト、マルチキャスト、またはユニキャスト）のトラフィック レート
- 秒単位で受信するビット（ブロードキャスト、マルチキャスト、またはユニキャスト）のトラフィック レート

上記の方法のいずれを使用しても、しきい値に到達すると、ポートはトラフィックをブロックします。トラフィック レートが下限しきい値（指定されている場合）を下回らない限り、ポートはブロックされたままになり、その後、通常の転送が再開されます。下限抑制レベルが指定されていない場合、トラフィック レートが上限抑制レベルを下回らない限り、スイッチはすべてのトラフィックをブロックします。一般に、そのレベルが高ければ高いほど、ブロードキャストストームに対する保護効果は薄くなります。

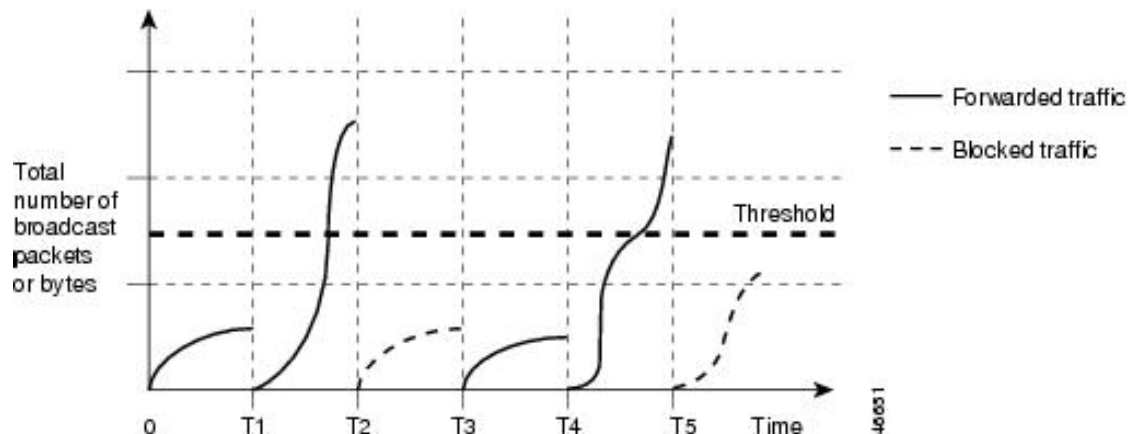


- (注) マルチキャストトラフィックのストーム制御しきい値に達した場合、ブリッジプロトコルデータ ユニット (BPDU) および Cisco Discovery Protocol フレームなどの制御トラフィック以外のマルチキャストトラフィックはすべてブロックされます。ただし、スイッチでは Open Shortest Path First (OSPF) などのルーティング アップデートと、正規のマルチキャスト データ トラフィックは区別されないため、両方のトラフィック タイプがブロックされます。

## トラフィック パターン

図 34: ブロードキャストストーム制御の例

次の例は、一定時間におけるインターフェイス上のブロードキャスト トラフィック パターンを示しています。



T1 から T2、T4 から T5 のタイムインターバルで、転送するブロードキャストトラフィックが設定されたしきい値を上回っています。指定のトラフィック量がしきい値を上回ると、次のインターバルで、そのタイプのトラフィックがすべてドロップされます。したがって、T2 と T5 の後のインターバルの間、ブロードキャストトラフィックがブロックされます。その次のインターバル（たとえば、T3）では、しきい値を上回らない限り、ブロードキャストトラフィックが再び転送されます。

ストーム制御抑制レベルと1秒間のインターバルを組み合わせると、ストーム制御アルゴリズムの動作を制御します。しきい値が高いほど、通過できるパケット数が多くなります。しきい値が100%であれば、トラフィックに対する制限はありません。値を0.0にすると、そのポート上ではすべてのブロードキャスト、マルチキャスト、またはユニキャストトラフィックがブロックされます。



(注) パケットは一定の間隔で届くわけではないので、トラフィックアクティビティを測定する1秒間のインターバルがストーム制御の動作を左右する可能性があります。

各トラフィックタイプのしきい値を設定するには、**storm-control** インターフェイス コンフィギュレーション コマンドを使用します。

## ストーム制御の設定方法

### ストーム制御およびしきい値レベルの設定

ポートにストーム制御を設定し、特定のトラフィックタイプで使用するしきい値レベルを入力します。

ただし、ハードウェアの制約とともに、さまざまなサイズのパケットをどのように数えるかという問題があるので、しきい値の割合はあくまでも近似値です。着信トラフィックを形成するパケットのサイズによって、実際に適用されるしきい値は設定されたレベルに対して、数%の差異が生じる可能性があります。



(注) ストーム制御は、物理インターフェイスでサポートされています。また、EtherChannel でもストーム制御を設定できます。ストーム制御をEtherChannelで設定する場合、ストーム制御設定はEtherChannel物理インターフェイスに伝播します。

ストーム制御としきい値レベルを設定するには、次の手順を実行します。

#### 始める前に

ストーム制御は、物理インターフェイスでサポートされています。また、EtherChannel でもストーム制御を設定できます。ストーム制御をEtherChannelで設定する場合、ストーム制御設定はEtherChannel物理インターフェイスに伝播します。

## 手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **storm-control** {**broadcast** | **multicast** | **unicast**} **level** {*level* [*level-low*] | **bps** *bps* [*bps-low*] | **pps** *pps* [*pps-low*]}
5. **storm-control action** {**shutdown** | **trap**}
6. **end**
7. **show storm-control** [*interface-id*] [**broadcast** | **multicast** | **unicast**]
8. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  デバイス> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  デバイス# <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 3	<b>interface</b> <i>interface-id</i> 例：  デバイス(config)# <b>interface</b> <b>gigabitethernet1/0/1</b>	設定するインターフェイスを指定し、インターフェイスコンフィギュレーションモードを開始します。
ステップ 4	<b>storm-control</b> { <b>broadcast</b>   <b>multicast</b>   <b>unicast</b> } <b>level</b> { <i>level</i> [ <i>level-low</i> ]   <b>bps</b> <i>bps</i> [ <i>bps-low</i> ]   <b>pps</b> <i>pps</i> [ <i>pps-low</i> ]} 例：  デバイス(config-if)# <b>storm-control unicast level</b> <b>87 65</b>	ブロードキャスト、マルチキャスト、またはユニキャストストーム制御を設定します。デフォルトでは、ストーム制御はディセーブルに設定されています。 キーワードの意味は次のとおりです。  • <i>level</i> には、ブロードキャスト、マルチキャスト、またはユニキャストトラフィックの上限しきい値レベルを帯域幅のパーセンテージで指定します（小数点第 2 位まで）。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.00～100.00 です。  • （任意） <i>level-low</i> には、下限しきい値レベルを帯域幅のパーセンテージで指定します（小数点

	コマンドまたはアクション	目的
		<p>第2位まで)。この値は上限抑制値より小さいか、または等しくなければなりません。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。下限抑制レベルを設定しない場合、上限抑制レベルの値に設定されます。指定できる範囲は 0.00 ~ 100.00 です。</p> <p>しきい値に最大値 (100%) を指定した場合、トラフィックの制限はなくなります。しきい値に 0.0 を設定すると、そのポート上のすべてのブロードキャスト、マルチキャスト、またはユニキャストトラフィックがブロックされます。</p> <ul style="list-style-type: none"> <li>• <b>bps</b> <i>bps</i> には、ブロードキャスト、マルチキャスト、またはユニキャストトラフィックの上限しきい値レベルをビット/秒で指定します (小数点第1位まで)。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.0 ~ 10000000000.0 です。</li> <li>• (任意) <i>bps-low</i> には、下限しきい値レベルをビット/秒で指定します (小数点第1位まで)。この値は上限しきい値レベル以下の値である必要があります。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。指定できる範囲は 0.0 ~ 10000000000.0 です。</li> <li>• <b>pps</b> <i>pps</i> には、ブロードキャスト、マルチキャスト、またはユニキャストトラフィックの上限しきい値レベルをパケット/秒で指定します (小数点第1位まで)。上限しきい値に到達すると、ポートはトラフィックをブロックします。指定できる範囲は 0.0 ~ 10000000000.0 です。</li> <li>• (任意) <i>pps-low</i> には、下限しきい値レベルをパケット/秒で指定します (小数点第1位まで)。この値は上限しきい値レベル以下の値である必要があります。トラフィックがこのレベルを下回っていれば、ポートはトラフィックを転送します。指定できる範囲は <b>0.0</b> ~ 10000000000.0 です。</li> </ul>

	コマンドまたはアクション	目的
		BPS および PPS の設定には、しきい値の数値を大きく設定できるように、サフィックスに測定記号 (k、m、g など) を使用できます。
ステップ 5	<b>storm-control action {shutdown   trap}</b> 例 : デバイス (config-if) # <b>storm-control action trap</b>	ストーム検出時に実行するアクションを指定します。デフォルトではトラフィックにフィルタリングを実行し、トラップは送信しない設定です。 <ul style="list-style-type: none"> <li>• ストーム中、ポートを <b>errdisable</b> の状態にするには、<b>shutdown</b> キーワードを選択します。</li> <li>• ストームが検出された場合、SNMP トラップを生成するには、<b>trap</b> キーワードを選択します。</li> </ul>
ステップ 6	<b>end</b> 例 : デバイス (config-if) # <b>end</b>	特権 EXEC モードに戻ります。
ステップ 7	<b>show storm-control [interface-id] [broadcast   multicast   unicast]</b> 例 : デバイス # <b>show storm-control gigabitethernet1/0/1 unicast</b>	指定したトラフィック タイプについて、インターフェイスで設定したストーム制御抑制レベルを確認します。トラフィックタイプを入力しない場合は、すべてのトラフィックタイプ (ブロードキャスト、マルチキャスト、ユニキャスト) の詳細が表示されます。
ステップ 8	<b>copy running-config startup-config</b> 例 : デバイス # <b>copy running-config startup-config</b>	(任意) コンフィギュレーションファイルに設定を保存します。

## 保護ポートに関する情報

### 保護ポート

アプリケーションによっては、あるネイバーが生成したトラフィックが別のネイバーにわからないように、同一スイッチ上のポート間でレイヤ2トラフィックが転送されないように設定する必要があります。このような環境では、保護ポートを使用すると、スイッチ上のポート間でユニキャスト、ブロードキャスト、またはマルチキャストトラフィックの交換が確実になくなります。

保護ポートには、次の機能があります。

- 保護ポートは、同様に保護ポートになっている他のポートに対して、ユニキャスト、マルチキャスト、またはブロードキャストトラフィックを転送しません。データトラフィック



クはレイヤ2の保護ポート間で転送されません。PIM パケットなどは CPU で処理されてソフトウェアで転送されるため、このような制御トラフィックだけが転送されます。保護ポート間を通過するすべてのデータトラフィックは、レイヤ3デバイスを介して転送されなければなりません。

- 保護ポートと非保護ポート間の転送動作は、通常どおりに進みます。

スイッチスタックは論理的には1つのスイッチを表しているため、レイヤ2トラフィックは、スタック内の同一スイッチか異なるスイッチかにかかわらず、スイッチスタックの保護ポート間では転送されません。

## 保護ポートのデフォルト設定

デフォルトでは、保護ポートは定義されません。

## 保護ポートのガイドライン

保護ポートは、物理インターフェイス（GigabitEthernet ポート 1 など）または EtherChannel グループ（port-channel 5 など）に設定できます。ポート チャンネルで保護ポートをイネーブルにした場合は、そのポート チャンネル グループ内のすべてのポートでイネーブルになります。

## 保護ポートの設定方法

### 保護ポートの設定

始める前に

保護ポートは事前定義されていません。これは設定する必要があるタスクです。

#### 手順の概要

1. **enable**
2. **configure terminal**
3. **interface *interface-id***
4. **switchport protected**
5. **end**
6. **show interfaces *interface-id* switchport**
7. **show running-config**
8. **copy running-config startup-config**

#### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 :	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
	デバイス> <code>enable</code>	
ステップ 2	<b>configure terminal</b> 例： デバイス# <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 3	<b>interface interface-id</b> 例： デバイス (config)# <code>interface gigabitethernet 1/0/1</code>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	<b>switchport protected</b> 例： デバイス (config-if)# <code>switchport protected</code>	インターフェイスを保護ポートとして設定します。
ステップ 5	<b>end</b> 例： デバイス (config)# <code>end</code>	特権 EXEC モードに戻ります。
ステップ 6	<b>show interfaces interface-id switchport</b> 例： デバイス# <code>show interfaces gigabitethernet 1/0/1 switchport</code>	入力を確認します。
ステップ 7	<b>show running-config</b> 例： デバイス# <code>show running-config</code>	入力を確認します。
ステップ 8	<b>copy running-config startup-config</b> 例： デバイス# <code>copy running-config startup-config</code>	(任意) コンフィギュレーション ファイルに設定を保存します。

## 保護ポートの監視

表 55: 保護ポートの設定を表示するコマンド

コマンド	目的
<code>show interfaces [interface-id] switchport</code>	すべてのスイッチング（非ルーティング）ポートまたはポートの管理ステータスまたは動作ステータス、ブロッキングおよびポート保護の設定を含めて表示

## ポート ブロッキングに関する情報

### ポート ブロッキング

デフォルトでは、スイッチは未知の宛先 MAC アドレスが指定されたパケットをすべてのポートからフラッディングします。未知のユニキャストおよびマルチキャストトラフィックが保護ポートに転送されると、セキュリティ上、問題になる可能性があります。未知のユニキャストおよびマルチキャストトラフィックがあるポートから別のポートに転送されないようにするために、（保護または非保護）ポートをブロックし、未知のユニキャストまたはマルチキャストパケットが他のポートにフラッディングされないようにします。



(注) マルチキャストトラフィックでは、ポートブロッキング機能は純粋なレイヤ2パケットだけをブロックします。ヘッダーにIPv4またはIPv6の情報を含むマルチキャストパケットはブロックされません。

## ポート ブロッキングの設定方法

### インターフェイスでのフラッディングトラフィックのブロッキング

#### 始める前に

インターフェイスは物理インターフェイスまたはEtherChannelグループのいずれも可能です。ポートチャネル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。

#### 手順の概要

1. `enable`
2. `configure terminal`
3. `interface interface-id`
4. `switchport block multicast`
5. `switchport block unicast`

6. **end**
7. **show interfaces interface-id switchport**
8. **show running-config**
9. **copy running-config startup-config**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  デバイス> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  デバイス# <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 3	<b>interface interface-id</b> 例：  デバイス(config)# <b>interface gigabitethernet 1/0/1</b>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。
ステップ 4	<b>switchport block multicast</b> 例：  デバイス(config-if)# <b>switchport block multicast</b>	ポートからの未知のマルチキャストの転送をブロックします。
ステップ 5	<b>switchport block unicast</b> 例：  デバイス(config-if)# <b>switchport block unicast</b>	ポートからの未知のユニキャストの転送をブロックします。
ステップ 6	<b>end</b> 例：  デバイス(config)# <b>end</b>	特権 EXEC モードに戻ります。
ステップ 7	<b>show interfaces interface-id switchport</b> 例：	入力を確認します。

	コマンドまたはアクション	目的
	デバイス# <code>show interfaces gigabitethernet 1/0/1 switchport</code>	
ステップ 8	<b>show running-config</b> 例： デバイス# <code>show running-config</code>	入力を確認します。
ステップ 9	<b>copy running-config startup-config</b> 例： デバイス# <code>copy running-config startup-config</code>	(任意) コンフィギュレーションファイルに設定を保存します。

## ポートブロッキングの監視

表 56: ポートブロッキングの設定を表示するコマンド

コマンド	目的
<code>show interfaces [interface-id] switchport</code>	すべてのスイッチング (非ルーティング) ポートまたはポートの管理ステータスまたは動作ステータス、ブロッキングおよびポート保護の設定を含めて表示

## ポートベースのトラフィック制御に関するその他の関連資料

### MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィチャーセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

## シスコのテクニカル サポート

説明	リンク
<p>シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。</p> <p>お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service (Field Notice からアクセス)、Cisco Technical Services Newsletter、Really Simple Syndication (RSS) フィードなどの各種サービスに加入できます。</p> <p>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。</p>	<a href="http://www.cisco.com/support">http://www.cisco.com/support</a>

## ポートベースのトラフィック制御の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	ポートベースのトラフィック制御	ポートベースのトラフィック制御は、特定トラフィック状態に応じてポートレベルでパケットをフィルタまたはブロックするために使用する Cisco Catalyst スイッチ上のレイヤ 2 機能の組み合わせです。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。



## 第 27 章

# ポート セキュリティ

---

- [ポート セキュリティの前提条件 \(649 ページ\)](#)
- [ポート セキュリティの制約事項 \(649 ページ\)](#)
- [ポート セキュリティの概要 \(650 ページ\)](#)
- [ポート セキュリティの設定方法 \(655 ページ\)](#)
- [ポート セキュリティの設定例 \(663 ページ\)](#)

## ポート セキュリティの前提条件



---

(注) 最大値をインターフェイス上ですでに設定されているセキュアアドレスの数より小さい値に設定しようとする、コマンドが拒否されます。

---

## ポート セキュリティの制約事項

- スイッチに設定できるセキュア MAC アドレスの最大数は、システムで許可されている MAC アドレスの最大数によって決まります。この値は、使用可能な MAC アドレス（その他のレイヤ 2 機能やインターフェイスに設定されたその他のセキュア MAC アドレスで使用される MAC アドレスを含む）の総数を表します。
- ポートセキュリティは、EtherChannel 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、プライベート VLAN ポートではサポートされていません。

# ポートセキュリティの概要

## ポートセキュリティ

ポートセキュリティ機能を使用すると、ポートへのアクセスを許可するステーションの MAC アドレスを制限および識別して、インターフェイスへの入力を制限できます。セキュアポートにセキュア MAC アドレスを割り当てると、ポートは定義されたアドレスグループ以外の送信元アドレスを持つパケットを転送しません。セキュア MAC アドレス数を 1 つに制限し、単一のセキュア MAC アドレスを割り当てると、そのポートに接続されたワークステーションに、ポートの帯域幅全体が保証されます。

セキュアポートとしてポートを設定し、セキュア MAC アドレスが最大数に達した場合、ポートにアクセスを試みるステーションの MAC アドレスが識別されたセキュア MAC アドレスのいずれとも一致しないので、セキュリティ違反が発生します。また、あるセキュアポート上でセキュア MAC アドレスが設定または学習されているステーションが、別のセキュアポートにアクセスしようとしたときにも、違反のフラグが立てられます。

## セキュア MAC アドレスのタイプ

スイッチは、次のセキュア MAC アドレス タイプをサポートします。

- **スタティックセキュア MAC アドレス** : `switchport port-security mac-address mac-address` インターフェイス コンフィギュレーション コマンドを使用して手動で設定され、アドレステーブルに保存された後、スイッチの実行コンフィギュレーションに追加されます。
- **ダイナミックセキュア MAC アドレス** : 動的に設定されてアドレステーブルにのみ保存され、スイッチの再起動時に削除されます。
- **スティッキーセキュア MAC アドレス** : 動的に学習することも、手動で設定することもできます。アドレステーブルに保存され、実行コンフィギュレーションに追加されます。このアドレスがコンフィギュレーションファイルに保存されていると、スイッチの再起動時にインターフェイスはこれらを動的に再設定する必要がありません。

## スティッキーセキュア MAC アドレス

スティッキーラーニングをイネーブルにすると、ダイナミック MAC アドレスをスティッキーセキュア MAC アドレスに変換して実行コンフィギュレーションに追加するようにインターフェイスを設定できます。インターフェイスはスティッキーラーニングがイネーブルになる前に学習したものを含め、すべてのダイナミックセキュア MAC アドレスをスティッキーセキュア MAC アドレスに変換します。すべてのスティッキーセキュア MAC アドレスは実行コンフィギュレーションに追加されます。

スティッキーセキュア MAC アドレスは、コンフィギュレーションファイル（スイッチが再起動されるたびに使用されるスタートアップコンフィギュレーション）に、自動的に反映さ



れません。スティッキーセキュア MAC アドレスをコンフィギュレーションファイルに保存すると、スイッチの再起動時にインターフェイスはこれらを再び学習する必要がありません。スティッキーセキュア アドレスを保存しない場合、アドレスは失われます。

スティッキーラーニングがディセーブルの場合、スティッキーセキュア MAC アドレスはダイナミックセキュアアドレスに変換され、実行コンフィギュレーションから削除されます。

## セキュリティ違反

次のいずれかの状況が発生すると、セキュリティ違反になります。

- 最大数のセキュア MAC アドレスがアドレステーブルに追加されている状態で、アドレステーブルに未登録の MAC アドレスを持つステーションがインターフェイスにアクセスしようとした場合。
- あるセキュア インターフェイスで学習または設定されたアドレスが、同一 VLAN 内の別のセキュア インターフェイスで使用された場合。
- ポートセキュリティが有効な状態で診断テストを実行しています。

違反が発生した場合の対処に基づいて、次の3種類の違反モードのいずれかにインターフェイスを設定できます。

- **protect (保護)** : セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさないうえ、未知の送信元アドレスを持つパケットはドロップされます。セキュリティ違反が起こっても、ユーザには通知されません。



(注) トランク ポートに **protect** 違反モードを設定することは推奨しません。保護モードでは、ポートが最大数に達していなくても VLAN が保護モードの最大数に達すると、ラーニングがディセーブルになります。

- **restrict (制限)** : セキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさないうえ、未知の送信元アドレスを持つパケットはドロップされます。このモードでは、セキュリティ違反が発生したことが通知されます。SNMP トラップが送信されます。Syslog メッセージがロギングされ、違反カウンタが増加します。
- **shutdown (シャットダウン)** : ポートセキュリティ違反により、インターフェイスが **error-disabled** になり、ただちにシャットダウンされます。そのあと、ポートの LED が消灯します。セキュアポートが **error-disabled** 状態の場合は、**errdisable recovery cause psecure-violation** グローバル コンフィギュレーション コマンドを入力してこの状態を解消するか、**shutdown** および **no shut down** インターフェイス コンフィギュレーション コマンドを入力して手動で再度有効にできます。これは、デフォルトのモードです。

- **shutdown vlan** (VLAN シャットダウン) : VLAN 単位でセキュリティ違反モードを設定するために使用します。このモードで違反が発生すると、ポート全体ではなく、VLAN が **errdisable** になります。

次の表に、ポートセキュリティをインターフェイスに設定した場合の違反モードおよび対処について示します。

表 57: セキュリティ違反モードの処置

違反モード	トラフィックの転送 <a href="#">12</a>	SNMP トラップの送信	Syslog メッセージの送信	エラーメッセージの表示 <a href="#">13</a>	違反カウンタの増加	ポ ト
protect	非対応	非対応	非対応	非対応	非対応	非
restrict	非対応	対応	対応	非対応	対応	非
shutdown	非対応	非対応	非対応	非対応	対応	対
shutdown vlan	非対応	非対応	対応	非対応	対応	非 <a href="#">14</a>

<sup>12</sup> 十分な数のセキュア MAC アドレスを削除するまで未知の送信元アドレスを持つパケットがドロップされます。

<sup>13</sup> セキュリティ違反を引き起こすアドレスを手動で設定した場合、スイッチがエラーメッセージを返します。

<sup>14</sup> 違反が発生した VLAN のみシャットダウンします。

## ポートセキュリティ エージング

ポート上のすべてのセキュアアドレスにエージングタイムを設定するには、ポートセキュリティエージングを使用します。ポートごとに2つのタイプのエージングがサポートされています。

- **absolute** : 指定されたエージングタイムの経過後に、ポート上のセキュアアドレスが削除されます。
- **inactivity** : 指定されたエージングタイムの間、セキュアアドレスが非アクティブであった場合に限り、ポート上のセキュアアドレスが削除されます。

## ポートセキュリティとスイッチスタック

スタックに新規に加入したスイッチは、設定済みのセキュアアドレスを取得します。他のスタックメンバーから新しいスタックメンバーに、ダイナミックセキュアアドレスがすべてダウンロードされます。

スイッチ（アクティブスイッチまたはスタックメンバのいずれか）がスタックから離れると、その他のスタックメンバに通知が行き、そのスイッチが設定または学習したセキュア MAC アドレスがセキュア MAC アドレス テーブルから削除されます。

## デフォルトのポートセキュリティ設定

表 58: デフォルトのポートセキュリティ設定

機能	デフォルト設定
ポートセキュリティ	ポート上でディセーブル
スティッキー アドレス ラーニング	ディセーブル
ポートあたりのセキュア MAC アドレスの最大数	1 つのアドレス
違反モード	shutdown。セキュア MAC アドレスが最大数を上回ると、ポートがシャットダウンします。
ポートセキュリティ エージング	ディセーブルエージング タイムは 0 スタティック エージングはディセーブル タイプは absolute

## ポートセキュリティの設定時の注意事項

- ポートセキュリティを設定できるのは、スタティック アクセス ポートまたはトランク ポートに限られます。セキュア ポートをダイナミック アクセス ポートにすることはできません。
- セキュア ポートをスイッチド ポートアナライザ (SPAN) の宛先ポートにすることはできません。
- 音声 VLAN はアクセス ポートでのみサポートされており、設定可能であってもトランク ポートではサポートされていません。
- 音声 VLAN が設定された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場合は、ポートの最大セキュアアドレス許容数を 2 に設定します。ポートを Cisco IP Phone に接続する場合は、IP Phone に MAC アドレスが 1 つ必要です。Cisco IP Phone のアドレスは音声 VLAN 上で学習されますが、アクセス VLAN 上では学習されません。1 台の PC を Cisco IP Phone に接続する場合、MAC アドレスの追加は必要ありません。複数の PC を Cisco IP Phone に接続する場合、各 PC と IP Phone に 1 つずつ使用できるように、十分な数のセキュアアドレスを設定する必要があります。

- トランクポートがポートセキュリティで設定され、データトラフィック用のアクセス VLAN と音声トラフィック用の音声 VLAN に割り当てられている場合、**switchport voice** および インターフェイス コンフィギュレーション コマンドを入力して **switchport priority extend** も効果はありません。

接続装置が同じ MAC アドレスを使用してアクセス VLAN の IP アドレス、音声 VLAN の IP アドレスの順に要求すると、アクセス VLAN だけが IP アドレスに割り当てられます。

- インターフェイスの最大セキュアアドレス値を入力したときに、新しい値がそれまでの値より大きいと、それまで設定されていた値が新しい値によって上書きされます。新しい値が前回の値より小さく、インターフェイスで設定されているセキュアアドレス数が新しい値より大きい場合、コマンドは拒否されます。
- スイッチはスティッキセキュア MAC アドレスのポートセキュリティエージングをサポートしていません。

次の表に、他のポートベース機能と互換性のあるポートセキュリティについてまとめます。

表 59: ポートセキュリティと他のポートベース機能との互換性

ポート タイプまたはポートの機能	ポートセキュリティとの互換性
DTP <sup>15</sup> ポート <sup>16</sup>	なし
トランク ポート	あり
ダイナミックアクセスポート <sup>17</sup>	なし
ルーテッド ポート	なし
SPAN 送信元ポート	あり
SPAN 宛先ポート	なし
EtherChannel	非対応
トンネリング ポート	あり
保護ポート	あり
IEEE 802.1x ポート	あり
音声 VLAN ポート <sup>18</sup>	あり
IP ソース ガード	あり
ダイナミック アドレス解決プロトコル (ARP) インスタレーション	あり
Flex Link	対応

<sup>15</sup> DTP = Dynamic Trunking Protocol

- <sup>16</sup> **switchport mode dynamic** インターフェイス コンフィギュレーション コマンドで設定されたポート A。
- <sup>17</sup> **switchport access vlan dynamic** インターフェイス コンフィギュレーション コマンドで設定される VLAN Query Protocol (VQP) ポート。
- <sup>18</sup> ポートに最大限可能なセキュアなアドレスを設定します (アクセス VLAN で可能なセキュアなアドレスの最大数に 2 を加えた数)。

## ポートセキュリティの設定方法

### ポートセキュリティのイネーブル化および設定

#### 始める前に

このタスクは、ポートにアクセスできるステーションの MAC アドレスを制限および識別して、インターフェイスへの入力を制約します。

#### 手順の概要

1. **enable**
2. **configure terminal**
3. **interface interface-id**
4. **switchport mode {access | trunk}**
5. **switchport voice vlan vlan-id**
6. **switchport port-security**
7. **switchport port-security [maximum value [vlan {vlan-list | {access | voice}}]]**
8. **switchport port-security violation {protect | restrict | shutdown | shutdown vlan}**
9. **switchport port-security [mac-address mac-address [vlan {vlan-id | {access | voice}}]]**
10. **switchport port-security mac-address sticky**
11. **switchport port-security mac-address sticky [mac-address | vlan {vlan-id | {access | voice}}]**
12. **end**
13. **show port-security**
14. **show running-config**
15. **copy running-config startup-config**

#### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例 : デバイス> <b>enable</b>	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。

	コマンドまたはアクション	目的
ステップ 2	<b>configure terminal</b> 例 : デバイス# <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 3	<b>interface interface-id</b> 例 : デバイス (config)# <b>interface gigabitethernet1/0/1</b>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。
ステップ 4	<b>switchport mode {access   trunk}</b> 例 : デバイス (config-if)# <b>switchport mode access</b>	インターフェイス スイッチポートモードを <b>access</b> または <b>trunk</b> に設定します。デフォルトモード ( <b>dynamic auto</b> ) のインターフェイスは、セキュアポートとして設定できません。
ステップ 5	<b>switchport voice vlan vlan-id</b> 例 : デバイス (config-if)# <b>switchport voice vlan 22</b>	ポート上で音声 VLAN をイネーブルにします。 <b>vlan-id</b> : 音声トラフィックに使用する VLAN を指定します。
ステップ 6	<b>switchport port-security</b> 例 : デバイス (config-if)# <b>switchport port-security</b>	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。 (注) 特定の条件下では、スイッチスタックのメンバー ポートでポートセキュリティが有効になっていると、DHCP および ARP パケットがドロップされます。これを解決するには、インターフェイスで <b>shut</b> と <b>no shut</b> を設定します。
ステップ 7	<b>switchport port-security [maximum value [vlan {vlan-list   {access   voice}}]]</b> 例 : デバイス (config-if)# <b>switchport port-security maximum 20</b>	(任意) インターフェイスの最大セキュア MAC アドレス数を設定します。スイッチまたはスイッチスタックに設定できるセキュア MAC アドレスの最大数は、システムで許可されている MAC アドレスの最大数によって決まります。この値は、使用可能な MAC アドレス (その他のレイヤ 2 機能やインターフェイスに設定されたその他のセキュア MAC アドレスで使用される MAC アドレスを含む) の総数を表します。 (任意) <b>vlan</b> : VLAN 当たりの最大値を設定します。

	コマンドまたはアクション	目的
		<p><b>vlan</b> キーワードを入力後、次のいずれかのオプションを入力します。</p> <ul style="list-style-type: none"> <li>• <b>vlan-list</b> : トランク ポート上で、ハイフンで区切った範囲の VLAN、またはカンマで区切った一連の VLAN における、VLAN 単位の最大値を設定できます。VLAN を指定しない場合、VLAN ごとの最大値が使用されます。</li> <li>• <b>access</b> : アクセスポートで、VLAN をアクセス VLAN として指定します。</li> <li>• <b>voice</b> : アクセスポートで、VLAN を音声 VLAN として指定します。</li> </ul> <p>(注) <b>voice</b> キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。インターフェイスに音声 VLAN が設定されている場合、セキュア MAC アドレスの最大数を 2 に設定します。</p>
<p>ステップ 8</p>	<p><b>switchport port-security violation {protect   restrict   shutdown   shutdown vlan}</b></p> <p>例 :</p> <pre>デバイス(config-if)# switchport port-security violation restrict</pre>	<p>(任意) 違反モードを設定します。セキュリティ違反が発生した場合に、次のいずれかのアクションを実行します。</p> <ul style="list-style-type: none"> <li>• <b>protect</b> : ポートセキュア MAC アドレスの数がポートで許可されている最大限度に達すると、最大値を下回るまで十分な数のセキュア MAC アドレスを削除するか、許可アドレス数を増やさない限り、未知の送信元アドレスを持つパケットはドロップされます。セキュリティ違反が起こっても、ユーザには通知されません。</li> </ul> <p>(注) トランク ポート上に保護モードを設定することは推奨できません。保護モードでは、ポートが最大数に達していなくても VLAN が保護モードの最大数に達すると、ラーニングがディセーブルになります。</p> <ul style="list-style-type: none"> <li>• <b>restrict</b> : セキュア MAC アドレス数がポートで許可されている最大数に到達した場合、不明な送信元アドレスのパケットはドロップされま</li> </ul>

	コマンドまたはアクション	目的
		<p>す。セキュアMACアドレス数を上限よりも少なくするか、許容できるアドレスの最大数を増やさない限り、この状態が続きます。SNMPトラップが送信されます。Syslogメッセージがロギングされ、違反カウンタが増加します。</p> <ul style="list-style-type: none"> <li>• <b>shutdown</b> : 違反が発生すると、インターフェイスが <b>error-disabled</b> になり、ポートのLEDが消灯します。SNMPトラップが送信されます。Syslogメッセージがロギングされ、違反カウンタが増加します。</li> <li>• <b>shutdown vlan</b> : VLAN単位でセキュリティ違反モードを設定するために使用します。このモードで違反が発生すると、ポート全体ではなく、VLANが <b>errdisable</b> になります。</li> </ul> <p>(注) セキュアポートが <b>error-disabled</b> ステートの場合は、<b>errdisable recovery cause psecure-violation</b> グローバルコンフィギュレーションコマンドを入力して、このステートから回復させることができます。手動で再びイネーブルにするには、<b>shutdown</b> および <b>no shutdown</b> 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か、<b>clear errdisable interface vlan</b> 特権 EXEC コマンドを入力します。</p>
ステップ 9	<p><b>switchport port-security [mac-address mac-address [vlan {vlan-id   {access   voice}}]</b></p> <p>例 :</p> <pre>デバイス(config-if)# switchport port-security mac-address 00:A0:C7:12:C9:25 vlan 3 voice</pre>	<p>(任意) インターフェイスのセキュアMACアドレスを入力します。このコマンドを使用すると、最大数のセキュアMACアドレスを入力できます。設定したセキュアMACアドレスが最大数より少ない場合、残りのMACアドレスは動的に学習されます。</p> <p>(注) このコマンドの入力後にスティッキーラーニングをイネーブルにすると、動的に学習されたセキュアアドレスがスティッキーセキュアMACアドレスに変換されて実行コンフィギュレーションに追加されます。</p>



	コマンドまたはアクション	目的
		<p>(任意) <b>vlan</b> : VLAN 当たりの最大値を設定します。</p> <p><b>vlan</b> キーワードを入力後、次のいずれかのオプションを入力します。</p> <ul style="list-style-type: none"> <li>• <b>vlan-id</b> : トランク ポートで、VLAN ID および MAC アドレスを指定できます。VLAN ID を指定しない場合、ネイティブ VLAN が使用されます。</li> <li>• <b>access</b> : アクセス ポートで、VLAN をアクセス VLAN として指定します。</li> <li>• <b>voice</b> : アクセス ポートで、VLAN を音声 VLAN として指定します。</li> </ul> <p>(注) <b>voice</b> キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。インターフェイスに音声 VLAN が設定されている場合、セキュア MAC アドレスの最大数を 2 に設定します。</p>
<p>ステップ 10</p>	<p><b>switchport port-security mac-address sticky</b></p> <p>例 :</p> <pre>デバイス(config-if)# switchport port-security mac-address sticky</pre>	<p>(任意) インターフェイス上でスティッキー ラーニングをイネーブルにします。</p>
<p>ステップ 11</p>	<p><b>switchport port-security mac-address sticky</b> [<i>mac-address</i>   <b>vlan</b> {<i>vlan-id</i>   {<b>access</b>   <b>voice</b>}}]</p> <p>例 :</p> <pre>デバイス(config-if)# switchport port-security mac-address sticky 00:A0:C7:12:C9:25 vlan voice</pre>	<p>(任意) スティックキーセキュア MAC アドレスを入力し、必要な回数だけコマンドを繰り返します。設定したセキュア MAC アドレスの数が最大数より少ない場合、残りの MAC アドレスは動的に学習されてスティッキーセキュア MAC アドレスに変換され、実行コンフィギュレーションに追加されます。</p> <p>(注) このコマンドの入力前にスティッキー ラーニングをイネーブルにしないと、エラー メッセージが表示されてスティッキーセキュア MAC アドレスを入力できません。</p> <p>(任意) <b>vlan</b> : VLAN 当たりの最大値を設定します。</p>

	コマンドまたはアクション	目的
		<p><b>vlan</b> キーワードを入力後、次のいずれかのオプションを入力します。</p> <ul style="list-style-type: none"> <li>• <b>vlan-id</b> : トランク ポートで、VLAN ID および MAC アドレスを指定できます。VLAN ID を指定しない場合、ネイティブ VLAN が使用されます。</li> <li>• <b>access</b> : アクセス ポートで、VLAN をアクセス VLAN として指定します。</li> <li>• <b>voice</b> : アクセス ポートで、VLAN を音声 VLAN として指定します。</li> </ul> <p>(注) <b>voice</b> キーワードは、音声 VLAN がポートに設定されていて、さらにそのポートがアクセス VLAN でない場合のみ有効です。</p>
ステップ 12	<p><b>end</b></p> <p>例 :</p> <pre>デバイス (config) # end</pre>	特権 EXEC モードに戻ります。
ステップ 13	<p><b>show port-security</b></p> <p>例 :</p> <pre>デバイス # show port-security</pre>	入力を確認します。
ステップ 14	<p><b>show running-config</b></p> <p>例 :</p> <pre>デバイス # show running-config</pre>	入力を確認します。
ステップ 15	<p><b>copy running-config startup-config</b></p> <p>例 :</p> <pre>デバイス # copy running-config startup-config</pre>	(任意) コンフィギュレーション ファイルに設定を保存します。

## ポートセキュリティ エージングのイネーブル化および設定

この機能を使用すると、既存のセキュア MAC アドレスを手動で削除しなくても、セキュアポート上のデバイスを削除および追加し、なおかつポート上のセキュアアドレス数を制限できます。セキュアアドレスのエージングは、ポート単位でイネーブルまたはディセーブルにできます。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **interface *interface-id***
4. **switchport port-security aging {static | time *time* | type {absolute | inactivity}}**
5. **end**
6. **show port-security [ interface *interface-id*] [address]**
7. **show running-config**
8. **copy running-config startup-config**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  デバイス> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  デバイス# <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 3	<b>interface <i>interface-id</i></b> 例：  デバイス(config)# <b>interface gigabitethernet1/0/1</b>	設定するインターフェイスを指定し、インターフェイス コンフィギュレーションモードを開始します。
ステップ 4	<b>switchport port-security aging {static   time <i>time</i>   type {absolute   inactivity}}</b> 例：  デバイス(config-if)# <b>switchport port-security aging time 120</b>	セキュアポートのスタティックエージングをイネーブルまたはディセーブルにします。またはエージング タイムやタイプを設定します。  (注) スイッチは、スティッキーセキュアアドレスのポートセキュリティ エージングをサポートしていません。

	コマンドまたはアクション	目的
		<p>このポートに、スタティックに設定されたセキュアアドレスのエージングをイネーブルにする場合は、<b>static</b> を入力します。</p> <p><i>time</i> には、このポートのエージングタイムを指定します。指定できる範囲は、0 ~ 1440 分です。</p> <p><b>type</b> には、次のキーワードのいずれか 1 つを選択します。</p> <ul style="list-style-type: none"> <li>• <b>absolute</b> : (任意) エージングタイプを絶対エージングとして設定します。このポートのセキュアアドレスはすべて、指定した時間 (分単位) が経過すると期限切れになり、セキュアアドレスリストから削除されます。</li> <li>• <b>inactivity</b> : (任意) エージングタイプを非アクティブエージングとして設定します。指定された <i>time</i> 期間中にセキュア送信元アドレスからのデータトラフィックがない場合に限り、このポートのセキュアアドレスが期限切れになります。</li> </ul>
ステップ 5	<p><b>end</b></p> <p>例 :</p> <pre>デバイス(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 6	<p><b>show port-security [ interface <i>interface-id</i>] [address]</b></p> <p>例 :</p> <pre>デバイス# show port-security interface gigabitethernet1/0/1</pre>	入力を確認します。
ステップ 7	<p><b>show running-config</b></p> <p>例 :</p> <pre>デバイス# show running-config</pre>	入力を確認します。
ステップ 8	<p><b>copy running-config startup-config</b></p> <p>例 :</p> <pre>デバイス# copy running-config startup-config</pre>	(任意) コンフィギュレーションファイルに設定を保存します。

## ポートセキュリティの設定例

次に、ポート上でポートセキュリティをイネーブルにし、セキュアアドレスの最大数を 50 に設定する例を示します。違反モードはデフォルトです。スタティックセキュア MAC アドレスは設定せず、スティッキー ラーニングはイネーブルです。

```
デバイス(config)# interface gigabitethernet1/0/1
デバイス(config-if)# switchport mode access
デバイス(config-if)# switchport port-security
デバイス(config-if)# switchport port-security maximum 50
デバイス(config-if)# switchport port-security mac-address sticky
```

次に、ポートの VLAN 3 上にスタティックセキュア MAC アドレスを設定する例を示します。

```
デバイス(config)# interface gigabitethernet1/0/2
デバイス(config-if)# switchport mode trunk
デバイス(config-if)# switchport port-security
デバイス(config-if)# switchport port-security mac-address 0000.0200.0004 vlan 3
```

次に、ポートのスティッキー ポートセキュリティをイネーブルにする例を示します。データ VLAN および音声 VLAN の MAC アドレスを手動で設定し、セキュアアドレスの総数を 20 に設定します（データ VLAN に 10、音声 VLAN に 10 を割り当てます）。

```
デバイス(config)# interface tengigabitethernet1/0/1
デバイス(config-if)# switchport access vlan 21
デバイス(config-if)# switchport mode access
デバイス(config-if)# switchport voice vlan 22
デバイス(config-if)# switchport port-security
デバイス(config-if)# switchport port-security maximum 20
デバイス(config-if)# switchport port-security violation restrict
デバイス(config-if)# switchport port-security mac-address sticky
デバイス(config-if)# switchport port-security mac-address sticky 0000.0000.0002
デバイス(config-if)# switchport port-security mac-address 0000.0000.0003
デバイス(config-if)# switchport port-security mac-address sticky 0000.0000.0001 vlan voice

デバイス(config-if)# switchport port-security mac-address 0000.0000.0004 vlan voice
デバイス(config-if)# switchport port-security maximum 10 vlan access
デバイス(config-if)# switchport port-security maximum 10 vlan voice
```





## 第 28 章

# コントロールプレーンポリシングの設定

- [CoPP の制約事項 \(665 ページ\)](#)
- [CoPP の概要 \(666 ページ\)](#)
- [CoPP の設定方法 \(678 ページ\)](#)
- [CoPP の設定例 \(682 ページ\)](#)
- [CoPP のモニタリング \(686 ページ\)](#)
- [CoPP の機能履歴 \(686 ページ\)](#)

## CoPP の制約事項

コントロールプレーンポリシング (CoPP) の制約事項は、次のとおりです。

- 入力 CoPP だけがサポートされます。 **system-cpp-policy** ポリシーマップは、入力方向でのみ、コントロールプレーンインターフェイスで使用可能です。
- コントロールプレーンインターフェイスにインストールできるのは、 **system-cpp-policy** ポリシーマップのみです。
- **system-cpp-policy** ポリシーマップおよびシステム定義のクラスは、変更または削除することはできません。
- **system-cpp-policy** ポリシーマップの下で許可されるのは、 **police** アクションのみです。システム定義クラスのポリシングレートは、秒単位のパケット/秒 (pps)
- ポリサーレートを設定する場合、クロック周波数の制限により、一部のクラスで表示されるデフォルトレートと設定レートの値に違いが生じることに注意してください (すべてのクラスにデフォルトレートを設定した場合でも)。詳細については、この章の「ユーザー設定可能な CoPP の特徴」および「例: すべての CPU キューに対するデフォルトのポリサーレートの設定」を参照してください。
- 1 つ以上の CPU キューがそれぞれのクラスマップの一部となります。複数の CPU キューが 1 つのクラスマップに属している場合、クラスマップのポリサーレートを変更すると、そのクラスマップに属しているすべての CPU キューに影響します。同様に、クラスマップでポリサーを無効にすると、そのクラスマップに属するすべてのキューが無効になります。

す。各クラスマップに属するCPUキューの詳細については、「CoPPのシステム定義値」の表を参照してください。

- システム定義のクラスマップのポリサーを無効にすることはお勧めできません。つまり、**no police rate rate pps** コマンドを設定しないでください。これを行うと、CPU へのトラフィックが多い場合に、システム全体の正常性に影響します。さらに、システム定義のクラスマップのポリサーレートを無効にした場合でも、システム起動プロセスを保護するために、システムはシステムのブートアップ後にデフォルトのポリサーレートに自動的に戻ります。
- `system-cpp` ポリシーの下で設定されたクラスがデフォルト値のままの場合、それらのクラスに関する情報は `show run` コマンドで表示されません。代わりに `show policy-map system-cpp-policy` または `show policy-map control-plane` コマンドを使用します。  
引き続き `show run` コマンドを使用して、カスタムポリシーに関する情報を表示できます。
- 大量の CPU バウンドパケットを使用するプロトコルは、同じクラスの他のプロトコルに影響を与える可能性があります。これらのプロトコルの一部は同じポリサーを共有するためです。たとえば、Address Resolution Protocol (ARP) は、`system-cpp-police-forus` クラスの Telnet、Internet Control Message Protocol (ICMP)、SSH、FTP、SNMP などのホストプロトコルの配列と 4000 個のハードウェアポリサーを共有します。ARP ポイズニングまたは ICMP 攻撃が発生すると、ハードウェアポリサーは、4000 パケット/秒を超える着信トラフィックのスロットリングを開始し、CPU とシステムの全体的な完全性を保護します。その結果、ARP および ICMP ホストプロトコルは、同じクラスを共有する他のホストプロトコルとともにドロップされます。
- Cisco IOS XE Fuji 16.8.1a 以降、ユーザー定義のクラスマップの作成はサポートされていません。

## CoPP の概要

この章では、コントロールプレーンポリシング (CoPP) が device で機能する仕組みと、その設定方法について説明します。

### CoPP の概要

CoPP 機能は、不要なトラフィックおよび DoS 攻撃から CPU を保護する device のセキュリティを向上させます。また、他の優先順位の低い大量のトラフィックによって発生するトラフィックのドロップから、制御および管理トラフィックを保護することもできます。

device は通常、3 つの操作プレーンにセグメント化され、それぞれに独自の目的があります。

- データ パケットを転送するための、データ プレーン。
- データを適切にルーティングするための、コントロールプレーン。
- ネットワーク要素を管理するための、管理プレーン。



CoPP を使用することで、大半の CPU 行きトラフィックを保護し、ルーティングの安定性と信頼性を確保し、パケットを確実に配信することができます。特に重要なのは、DoS 攻撃から CPU を保護するために CoPP を使用できることです。

CoPP は、モジュラ QoS コマンドライン インターフェイス (MQC) および CPU キューを使用して、これらの目的を達成します。さまざまなタイプのコントロールプレーントラフィックが特定の条件に基づいてグループ化され、CPU キューに割り当てられます。ハードウェアに専用のポリサーを設定することで、これらの CPU キューを管理できます。たとえば、特定の CPU キュー (トラフィック タイプ) のポリサー レートを変更したり、特定のタイプのトラフィックに対するポリサーを無効にしたりできます。

ポリサーはハードウェアに設定されていますが、CoPP は CPU のパフォーマンスやデータプレーンのパフォーマンスには影響しません。しかし、CPU に着信するパケット数は制限されるため、CPU 負荷が制御されます。これは、ハードウェアからのパケットを待っているサービスが、より制御された着信パケットのレート (ユーザー設定可能なレート) を確認する可能性があることを意味します。

## システム定義の CoPP の特徴

device の初回の電源投入時は、システムによって次のタスクが自動的に実行されます。

- ポリシーマップ **system-cpp-policy** を検索します。見つからない場合、システムはそれを作成してコントロールプレーンにインストールします。
- **system-cpp-policy** の下に 18 個のクラスマップを作成します。  
次に device の電源を入れたときに、すでに作成済みのポリシーとクラスマップがシステムによって検出されます
- デフォルトで、すべての CPU キューをそれぞれのデフォルトレートで有効にします。デフォルトのレートを「CoPP のシステム定義値」の表に示します。

**system-cpp-policy** ポリシーマップはシステム デフォルト ポリシー マップであり、通常はデバイスのスタートアップ コンフィギュレーションに明示的に保存する必要はありません。ただし、スタンバイデバイスとのバルク同期に失敗すると、コンフィギュレーションがスタートアップ コンフィギュレーションから消去される可能性があります。この場合、手動で **system-cpp-policy** ポリシーマップをスタートアップ コンフィギュレーションに保存する必要があります。 **show running-config** 特権 EXEC コマンドを使用して、保存されていることを確認します。

```
policy-map system-cpp-policy
```

次の表に、device をロードしたときにシステムが作成するクラスマップを示します。各クラスマップに対応するポリサーと、各クラスマップの下にグループ化された 1 つ以上の CPU キューを示します。ポリサーへのクラスマップの 1 対 1 のマッピングと、CPU キューへのクラスマップの 1 対多マッピングがあります。

表 60: CoPP のシステム定義された値

クラス マップ名	ポリサー インデックス (ポリサー No.)	CPU キュー (キュー No.)
system-cpp-police-data	WK_CPP_POLICE_DATA(0)	WK_CPU_Q_ICMP_GEN(3) WK_CPU_Q_BROADCAST(12) WK_CPU_Q_ICMP_REDIRECT (6)
system-cpp-police-l2- control	WK_CPP_POLICE_L2_ CONTROL(1)	WK_CPU_Q_L2_CONTROL(1)
system-cpp-police-routing-control	WK_CPP_POLICE_ROUTING_CONTROL(0)	WK_CPU_Q_ROUTING_ CONTROL(4) WK_CPU_Q_LOW_LATENCY (27)
system-cpp-police-punt-webauth	WK_CPP_POLICE_PU NT_WEBAUTH(7)	WK_CPU_Q_PUNT_WEBAUTH(22)
system-cpp-police-topology-control	WK_CPP_POLICE_TOPOLOGY_CONTROL(8)	WK_CPU_Q_TOPOLOGY_CONTROL(15)
system-cpp-police- multicast	WK_CPP_POLICE_MULTICAST(9)	WK_CPU_Q_TRANSIT_ TRAFFIC(18) WK_CPU_Q_MCAST_DATA(30)
system-cpp-police-sys- data	WK_CPP_POLICE_SYS_ DATA(10)	WK_CPU_Q_OPENFLOW (13) WK_CPU_Q_CRYPTO_ CONTROL(23) WK_CPU_Q_EXCEPTION(24) WK_CPU_Q_EGR_EXCEPTION(28) WK_CPU_Q_NFL_SAMPLED_ DATA(26) WK_CPU_Q_GOLD_PKT(31) WK_CPU_Q_RPF_FAILED(19)
system-cpp-police-dot1x-auth	WK_CPP_POLICE_DOT1X(11)	WK_CPU_Q_DOT1X_AUTH(0)
system-cpp-police- protocol-snooping	WK_CPP_POLICE_PR(12)	WK_CPU_Q_PROTO_ SNOOPING(16)
system-cpp-police-dhcp-snooping	WK_CPP_DHCP_SNOOPING(6)	WK_CPU_Q_DHCP_SNOOPING(17)
system-cpp-police-sw-forward	WK_CPP_POLICE_SW_FWD(13)	WK_CPU_Q_SW_FORWARDING_Q(14) WK_CPU_Q_LOGGING(21) WK_CPU_Q_L2_LVX_DATA_PACK (11)

クラス マップ名	ポリサー インデックス (ポリサー No.)	CPU キュー (キュー No.)
system-cpp-police-forus	WK_CPP_POLICE_FORUS(14)	WK_CPU_Q_FORUS_ADDR_RESOLUTION(5) WK_CPU_Q_FORUS_TRAFFIC(2)
system-cpp-police-multicast-end-station	WK_CPP_POLICE_MULTICAST_END_STATION(6)	WK_CPU_Q_MCAST_END_STATION_SERVICE(20)
system-cpp-default	WK_CPP_POLICE_DEFAULT(12)	WK_CPU_Q_INTER_FED_TRAFFIC(7) WK_CPU_Q_EWLC_CONTROL(9) WK_CPU_Q_EWLC_DATA(10)
system-cpp-police-stackwise-virt-control	WK_CPP_STACKWISE_VIRTUAL_CONTROL(16)	WK_CPU_Q_STACKWISE_VIRTUAL_CONTROL(29)
system-cpp-police-l2lvx-control	WK_CPP_L2_LVX_CONT_PACK(4)	WK_CPU_Q_L2_LVX_CONT_PACK(8)
system-cpp-police-high-rate-app	WK_CPP_HIGH_RATE_APP(18)	WK_CPU_Q_HIGH_RATE_APP(23)
system-cpp-police-system-critical	WK_CPP_SYSTEM_CRITICAL(3)	WK_CPU_Q_SYSTEM_CRITICAL(25)

次の表に、CPU キューと、各 CPU キューに関連付けられた機能を示します。

表 61: CPU キューと関連機能

CPU キュー (キュー No.)	機能
WK_CPU_Q_DOT1X_AUTH(0)	IEEE 802.1x ポートベースの認証

CPU キュー (キュー No.)	機能
WK_CPU_Q_L2_CONTROL(1)	ダイナミック トランッキング プロトコル (DTP) VLAN トランッキング プロトコル (VTP) ポート集約プロトコル (PAgP) Client Information Signalling Protocol (CISP) メッセージセッションリレープロトコル マルチ VLAN 登録プロトコル (MVRP) Metropolitan Mobile Network (MMN) リンクレベル検出プロトコル (LLDP) 単一方向リンク検出 (UDLD) リンク集約制御プロトコル (LACP) Cisco Discovery Protocol (CDP) スパニング ツリー プロトコル (STP)
WK_CPU_Q_FORUS_TRAFFIC(2)	Telnet、Pingv4 および Pingv6、SNMP などのホスト キープアライブ/ループバック検出 開始 - インターネット キー エクスチェンジ (IKE) プロトコル (IPSec)
WK_CPU_Q_ICMP_GEN(3)	ICMP - 接続先到達不能 ICMP - TTL 期限切れ

CPU キュー (キュー No.)	機能
WK_CPU_Q_ROUTING_CONTROL(4)	

CPU キュー (キュー No.)	機能
	Routing Information Protocol バージョン 1 (RIPv1) RIPv2 Interior Gateway Routing Protocol (IGRP) Border Gateway Protocol (BGP) PIM-UDP 仮想ルータ冗長プロトコル (VRRP) Hot Standby Router Protocol バージョン 1 (HSRPv1) HSRPv2 ゲートウェイ ロード バランシング プロトコル (GLBP) ラベル配布プロトコル (LDP) Web Cache Communication Protocol (WCCP) 次世代 Routing Information Protocol (RIPng) Open Shortest Path First (OSPF) Open Shortest Path First バージョン 3 (OSPFv3) Enhanced Interior Gateway Routing Protocol (EIGRP) Enhanced Interior Gateway Routing Protocol バージョン 6 (EIGRPv6) DHCPv6 プロトコルに依存しないマルチキャスト (PIM) Protocol Independent Multicast バージョン 6 (PIMv6) 次世代 Hot Standby Router Protocol (HSRPng) IPv6 制御 Generic Routing Encapsulation (GRE) キーペアライブ

CPU キュー (キュー No.)	機能
	ネットワークアドレス変換 (NAT) パン ト  Intermediate System-to-Intermediate System (IS-IS)
WK_CPU_Q_FORUS_ADDR_RESOLUTION(5)	アドレス解決プロトコル (ARP)  IPv6 ネイバーアドバタイズメントおよび ネイバー勧誘
WK_CPU_Q_ICMP_REDIRECT(6)	インターネット制御メッセージプロトコ ル (ICMP) リダイレクト
WK_CPU_Q_INTER_FED_TRAFFIC(7)	内部通信用のレイヤ2ブリッジドメイン 注入。
WK_CPU_Q_L2_LVX_CONT_PACK(8)	Exchange ID (XID) パケット
WK_CPU_Q_EWLC_CONTROL(9)	Embedded Wirelss Controller (eWLC) [ワ イヤレスアクセスポイントの制御とプロ ビジョンング (CAPWAP) (UDP 5246) ]
WK_CPU_Q_EWLC_DATA(10)	eWLC データパケット (CAPWAP DATA、UDP 5247)
WK_CPU_Q_L2_LVX_DATA_PACK(11)	不明なユニキャストパケットがマップ要 求のためにパントされました。
WK_CPU_Q_BROADCAST(12)	すべてのタイプのブロードキャスト
WK_CPU_Q_OPENFLOW(13)	学習キャッシュオーバーフロー (レイヤ 2+レイヤ3)
WK_CPU_Q_CONTROLLER_PUNT(14)	データ - アクセスコントロールリスト (ACL) フル  データ - IPv4 オプション  データ - IPv6 ホップバイホップ  データ - リソース不足/すべてをキャッチ  データ - リバースパス フォワーディン グ (RPF) が不完全  収集パケット

CPU キュー (キュー No.)	機能
WK_CPU_Q_TOPOLOGY_CONTROL(15)	スパニング ツリー プロトコル (STP) Resilient Ethernet Protocol (REP) Shared Spanning Tree Protocol (SSTP)
WK_CPU_Q_PROTO_SNOOPING(16)	ダイナミック ARP インスペクション (DAI) の Address Resolution Protocol (ARP) スヌーピング
WK_CPU_Q_DHCP_SNOOPING(17)	DHCP スヌーピング
WK_CPU_Q_TRANSIT_TRAFFIC(18)	これは、ソフトウェアパスで処理する必要がある NAT によってパントされたパケットに使用されます。
WK_CPU_Q_RPF_FAILED(19)	データ - mRPF (マルチキャスト RPF) が失敗しました
WK_CPU_Q_MCAST_END_STATION_SERVICE(20)	Internet Group Management Protocol (IGMP) /Multicast Listener Discovery (MLD) 制御
WK_CPU_Q_LOGGING(21)	アクセスコントロールリスト (ACL) ロギング
WK_CPU_Q_PUNT_WEBAUTH(22)	Web 認証
WK_CPU_Q_HIGH_RATE_APP(23)	有線アプリケーションの可視性と制御 (WDAVC) トラフィック ネットワークベースのアプリケーション認識 (NBAR) トラフィック トラフィック分析および分類のための暗号化トラフィック分析 (ETA)
WK_CPU_Q_EXCEPTION(24)	IKE の表示 IP ラーニング違反 IP ポートのセキュリティ違反 IP スタティックアドレス違反 IPv6 スコープチェック リモートコピープロトコル (RCP) 例外 ユニキャスト RPF 失敗



CPU キュー (キュー No.)	機能
WK_CPU_Q_SYSTEM_CRITICAL(25)	メディアシグナリング/ワイヤレスプロキシ ARP
WK_CPU_Q_NFL_SAMPLED_DATA(26)	Netflow サンプルデータと Media Services Proxy (MSP)
WK_CPU_Q_LOW_LATENCY(27)	双方向フォワーディング検出 (BFD)、Precision Time Protocol (PTP)
WK_CPU_Q_EGR_EXCEPTION(28)	出力解決例外
WK_CPU_Q_STACKWISE_VIRTUAL_CONTROL(29)	前面スタッキングプロトコル、つまり SVL
WK_CPU_Q_MCAST_DATA(30)	データ - (S、G) の作成 データ - ローカル結合 データ - PIM 登録 データ - SPT スイッチオーバー データ - マルチキャスト
WK_CPU_Q_GOLD_PKT(31)	Gold

## ユーザー設定可能な CoPP の特徴

次のタスクを実行して、コントロールプレーントラフィックを管理できます。



- (注) すべての `system-cpp-policy` コンフィギュレーションは、再起動後も保持されるように保存する必要があります。

### CPU キューのポリサーの有効化と無効化

CPU キューのポリサーを有効にするには、`system-cpp-policy` ポリシーマップ内で、対応するクラスマップの下にポリサーアクション (パケット/秒) を設定します。

CPU キューのポリサーを無効にするには、`system-cpp-policy` ポリシーマップ内で、対応するクラスマップの下にポリサーアクションを削除します。



- (注) デフォルトのポリサーがすでに存在する場合は、その削除を慎重に考慮して制御します。そうしないと、システムが CPU 占有や制御パケットドロップなどのその他の異常を検出する場合があります。

### ポリサーレートの変更

これは、`system-cpp-policy` ポリシーマップ内で、対応するクラスマップの下にポリサーレートアクション（パケット/秒単位）を設定することで実行できます。

ポリサーレートを設定する場合、設定したレートは最も近い200の倍数に自動的に変換されることに注意してください。たとえば、CPU キューのポリサーレートを `100 pps` に設定すると、システムは `200` に変更します。または、ポリサーレートを `650` に設定すると、システムは `600` に変更します。この動作を示す出力例については、この章の「例：すべての CPU キューに対するデフォルトのポリサーレートの設定」を参照してください。

### ポリサーレートをデフォルトに設定

グローバル コンフィギュレーション モードで `cpp system-default` コマンドを入力することによって、CPU キューのポリサーをデフォルト値に設定します。

## ソフトウェアバージョンのアップグレードまたはダウングレード

### ソフトウェアバージョンのアップグレードと CoPP

デバイスのソフトウェアバージョンをアップグレードすると、システムは CoPP に必要な更新を確認して実行します（たとえば、`system-cpp-policy` ポリシーマップを確認し、欠落している場合は作成します）。また、アップグレードアクティビティの前後に特定のタスクを完了する必要があります。これにより、設定の更新が正しく反映され、CoPP が期待どおりに動作し続けることが保証されます。ソフトウェアのアップグレードに使用する方法に応じて、アップグレード関連のタスクはオプションのシナリオまたは推奨されるシナリオもあれば、必須のシナリオもあります。

ここでは、アップグレードのシステムアクションとユーザーアクションについて説明します。また、リリース固有の警告も含まれます。

#### アップグレードのシステムアクション

デバイスのソフトウェアバージョンをアップグレードすると、システムは以下のアクションを実行します。これはすべてのアップグレード方法で共通です。

- アップグレード前のデバイスに `system-cpp-policy` ポリシーマップがなかった場合、アップグレード時にシステムはデフォルトポリシーを作成します。
- アップグレード前のデバイスに `system-cpp-policy` ポリシーマップがあった場合、アップグレード時にシステムはポリシーを再生成しません。

#### アップグレードのユーザーアクション

アップグレードのユーザーアクション（アップグレード方法に応じて）：

アップグレード方法	条件	アクション時間とアクション	目的
標準 <sup>19</sup>	なし	アップグレード後（必須） グローバル コンフィギュレーション モードで <b>cpp system-default</b> コマンドを入力します。	最新のデフォルトのポリサーレートを取得します。

<sup>19</sup> スイッチのリロードを伴うソフトウェアアップグレードの方法を指します。インストールモードまたはバンドルモードにすることができます。

## ソフトウェアバージョンのダウングレードと CoPP

ダウングレードのシステムアクションとユーザーアクションについて、ここで説明します。

### ダウングレードのシステムアクション

デバイスのソフトウェアバージョンをダウングレードすると、これらのアクションが実行されます。これはすべてのダウングレード方法に適用されます。

- システムは `system-cpp-policy` ポリシーマップをデバイスに保持し、コントロールプレーンにインストールします。

### ダウングレードのユーザーアクション

ダウングレードのユーザーアクション：

アップグレード方法	条件	アクション時間とアクション	目的
標準 <sup>20</sup>	なし	操作は不要です。	N/A

<sup>20</sup> スイッチのリロードを伴うソフトウェアアップグレードの方法を指します。インストールモードまたはバンドルモードにすることができます。

ソフトウェアバージョンをダウングレードしてからアップグレードする場合、適用されるシステムアクションとユーザーアクションは、アップグレードについて説明したものと同じです。

# CoPP の設定方法

## CPU キューの有効化またはポリサー レートの変更

CPU キューを有効にし、CPU キューのポリサー レートを変更する手順は、同じです。手順は次のとおりです。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** *class-name*
5. **police rate** *rate* **pps**
6. **exit**
7. **control-plane**
8. **service-policy input** *policy-name*
9. **end**
10. **show policy-map control-plane**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  デバイス> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  デバイス# <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 3	<b>policy-map</b> <i>policy-map-name</i> 例：  デバイス (config)# <b>policy-map system-cpp-policy</b> デバイス (config-pmap)#	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。
ステップ 4	<b>class</b> <i>class-name</i> 例：	クラスアクション コンフィギュレーション モードを開始します。有効にする CPU キューに対応する

	コマンドまたはアクション	目的
	<pre>デバイス (config-pmap) # class system-cpp-police-protocol-snooping デバイス (config-pmap-c) #</pre>	<p>クラスの名前を入力します。「CoPPのシステム定義値」の表を参照してください。</p>
ステップ 5	<p><b>police rate rate pps</b></p> <p>例 :</p> <pre>デバイス (config-pmap-c) # police rate 100 pps デバイス (config-pmap-c-police) #</pre>	<p>指定したトラフィッククラスに対し、1秒間に処理される着信パケット数の上限を指定します。</p> <p>(注) 指定するレートは、指定したクラスマップに属するすべてのCPUキューに適用されます。</p>
ステップ 6	<p>exit</p> <p>例 :</p> <pre>デバイス (config-pmap-c-police) # exit デバイス (config-pmap-c) # exit デバイス (config-pmap) # exit デバイス (config) #</pre>	<p>グローバル コンフィギュレーション モードに戻ります。</p>
ステップ 7	<p><b>control-plane</b></p> <p>例 :</p> <pre>デバイス (config) # control-plane デバイス (config-cp) #</pre>	<p>制御プレーン (config-cp) コンフィギュレーション モードを開始します。</p>
ステップ 8	<p><b>service-policy input policy-name</b></p> <p>例 :</p> <pre>デバイス (config) # control-plane デバイス (config-cp) # service-policy input system-cpp-policy デバイス (config-cp) #</pre>	<p>system-cpp-policy を FED にインストールします。このコマンドは、FED ポリシーを表示するために必要です。このコマンドを設定しないと、エラーになります。</p>
ステップ 9	<p>end</p> <p>例 :</p> <pre>デバイス (config-cp) # end</pre>	<p>特権 EXEC モードに戻ります。</p>
ステップ 10	<p><b>show policy-map control-plane</b></p> <p>例 :</p> <pre>デバイス # show policy-map control-plane</pre>	<p>system-cpp ポリシーの下で設定されたすべてのクラス、さまざまなトラフィックタイプに設定されたレート、および統計情報を表示します。</p>

## CPU キューの無効化

CPU キューを無効にするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** *class-name*
5. **no police rate** *rate* **pps**
6. **end**
7. **show policy-map control-plane**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例：  デバイス> <b>enable</b>	特権 EXEC モードを有効にします。  • パスワードを入力します（要求された場合）。
ステップ 2	<b>configure terminal</b> 例：  デバイス# <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 3	<b>policy-map</b> <i>policy-map-name</i> 例：  デバイス (config)# <b>policy-map system-cpp-policy</b> デバイス (config-pmap)#	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。
ステップ 4	<b>class</b> <i>class-name</i> 例：  デバイス (config-pmap)# <b>class</b> <b>system-cpp-police-protocol-snooping</b> デバイス (config-pmap-c)#	クラス アクション コンフィギュレーション モードを開始します。無効にする CPU キューに対応するクラスの名前を入力します。「CoPP のシステム定義値」の表を参照してください。
ステップ 5	<b>no police rate</b> <i>rate</i> <b>pps</b> 例：  デバイス (config-pmap-c)# <b>no police rate 100 pps</b>	指定したトラフィッククラスの着信パケットの処理を無効にします。  (注) これにより、指定したクラス マップに属するすべての CPU キューが無効になります。
ステップ 6	<b>end</b> 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	デバイス (config-pmap-c) # <b>end</b>	
<b>ステップ 7</b>	<b>show policy-map control-plane</b> 例 : デバイス # <b>show policy-map control-plane</b>	system-cpp ポリシーの下で設定されたすべてのクラス、およびさまざまなトラフィックタイプと統計情報に設定されたレートを表示します。

## すべての CPU キューに対するデフォルトのポリサー レートの設定

すべての CPU キューのポリサー レートをデフォルトのレートに設定するには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **cpp system-default**
4. **end**
5. **show platform hardware fed switch {switch-number} qos que stats internal cpu policer**

### 手順の詳細

	コマンドまたはアクション	目的
<b>ステップ 1</b>	<b>enable</b> 例 : デバイス > <b>enable</b>	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合) 。
<b>ステップ 2</b>	<b>configure terminal</b> 例 : デバイス # <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。
<b>ステップ 3</b>	<b>cpp system-default</b> 例 : デバイス (config) # <b>cpp system-default</b> Defaulting CPP : Policer rate for all classes will be set to their defaults	すべてのクラスのポリサー レートをデフォルトのレートに設定します。

	コマンドまたはアクション	目的
ステップ 4	<b>end</b> 例 : デバイス (config) # <b>end</b>	特権 EXEC モードに戻ります。
ステップ 5	<b>show platform hardware fed switch {switch-number} qos            que stats internal cpu policer</b> 例 : デバイス # <b>show platform hardware fed switch 1 qos            que stat internal cpu policer</b>	さまざまなトラフィックタイプに設定されたレートを表示します。

## CoPP の設定例

### 例 : CPU キューの有効化または CPU キューのポリサー レートの変更

次の例に、CPU キューを有効にする方法、または CPU キューのポリサー レートを変更する方法を示します。ここでは、**class system-cpp-police-protocol-snooping** CPU キューが有効になり、ポリサー レートは **2000 pps** です。

```

デバイス> enable
デバイス# configure terminal
デバイス (config) # policy-map system-cpp-policy
デバイス (config-pmap) # class system-cpp-police-protocol-snooping
デバイス (config-pmap-c) # police rate 2000 pps
デバイス (config-pmap-c-police) # end

```

```

デバイス# show policy-map control-plane
Control Plane

```

```

Service-policy input: system-cpp-policy

```

```

<output truncated>

```

```

Class-map: system-cpp-police-dot1x-auth (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
  Match: none
  police:
    rate 1000 pps, burst 244 packets
    conformed 0 bytes; actions:
      transmit
    exceeded 0 bytes; actions:
      drop

```



```
Class-map: system-cpp-police-protocol-snooping (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
Match: none
police:
  rate 2000 pps, burst 488 packets
  conformed 0 bytes; actions:
    transmit
  exceeded 0 bytes; actions:
    drop

<output truncated>

Class-map: class-default (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0000 bps, drop rate 0000 bps
Match: any
```

## 例：CPU キューの無効化

次に、CPU キューをディセーブルにする例を示します。ここでは、**class system-cpp-police-protocol-snooping** CPU キューが無効になります。

```
デバイス> enable
デバイス# configure terminal
デバイス(config)# policy-map system-cpp-policy
デバイス(config-pmap)# class system-cpp-police-protocol-snooping
デバイス(config-pmap-c)# no police rate 100 pps
デバイス(config-pmap-c)# end
```

```
デバイス# show running-config | begin system-cpp-policy
```

```
policy-map system-cpp-policy
class system-cpp-police-data
  police rate 200 pps
class system-cpp-police-sys-data
  police rate 100 pps
class system-cpp-police-sw-forward
  police rate 1000 pps
class system-cpp-police-multicast
  police rate 500 pps
class system-cpp-police-multicast-end-station
  police rate 2000 pps
class system-cpp-police-punt-webauth
class system-cpp-police-l2-control
class system-cpp-police-routing-control
  police rate 500 pps
class system-cpp-police-control-low-priority
class system-cpp-police-wireless-priority1
class system-cpp-police-wireless-priority2
class system-cpp-police-wireless-priority3-4-5
class system-cpp-police-topology-control
class system-cpp-police-dot1x-auth
class system-cpp-police-protocol-snooping
class system-cpp-police-forus
class system-cpp-default
```

例：すべての CPU キューに対するデフォルトのポリサー レートの設定

<output truncated>

## 例：すべてのCPUキューに対するデフォルトのポリサーレートの設定

次に、すべての CPU キューのポリサー レートをデフォルトに設定し、その後に設定を確認する例を示します。



- (注) 一部の CPU キューでは、すべてのクラスにデフォルトレートを設定しても、デフォルトレートと設定レートの値は同じにはなりません。これは、設定レートが最も近い200の倍数に丸められるためです。この動作は、デバイスのクロック速度によって制御されます。下の出力例では、DHCP スヌーピングと NFL SAMPLED DATA のデフォルトレートと設定レートの値にこの違いが示されています。

```

デバイス> enable
デバイス# configure terminal
デバイス(config)# cpp system-default
Defaulting CPP : Policer rate for all classes will be set to their defaults
デバイス(config)# end
    
```

```

Device# show platform hardware fed switch 1 qos queue stats internal cpu policer
CPU Queue Statistics
    
```

QId	PlcIdx	Queue Name	Enabled	(default) Rate	(set) Rate	Queue Drop (Bytes)	Queue Drop (Frames)
0	11	DOT1X Auth	Yes	1000	1000	0	0
1	1	L2 Control	Yes	2000	2000	0	0
2	14	Forus traffic	Yes	4000	4000	0	0
3	0	ICMP GEN	Yes	600	600	0	0
4	2	Routing Control	Yes	5400	5400	0	0
5	14	Forus Address resolution	Yes	4000	4000	0	0
6	0	ICMP Redirect	Yes	600	600	0	0
7	16	Inter FED Traffic	Yes	2000	2000	0	0
8	4	L2 LVX Cont Pack	Yes	1000	1000	0	0
9	16	EWLC Control	Yes	2000	2000	0	0
10	16	EWLC Data	Yes	2000	2000	0	0
11	13	L2 LVX Data Pack	Yes	1000	1000	0	0
12	0	BROADCAST	Yes	600	600	0	0

13	10	Openflow	Yes	100	200	0	0
14	13	Sw forwarding	Yes	1000	1000	0	0
15	8	Topology Control	Yes	13000	13000	0	0
16	12	Proto Snooping	Yes	2000	2000	0	0
17	6	DHCP Snooping	Yes	500	400	0	0
18	9	Transit Traffic	Yes	500	400	0	0
19	10	RPF Failed	Yes	100	200	0	0
20	15	MCAST END STATION	Yes	2000	2000	0	0
21	13	LOGGING	Yes	1000	1000	0	0
22	7	Punt Webauth	Yes	1000	1000	0	0
23	18	High Rate App	Yes	13000	13000	0	0
24	10	Exception	Yes	100	200	0	0
25	3	System Critical	Yes	1000	1000	0	0
26	10	NFL SAMPLED DATA	Yes	100	200	0	0
27	2	Low Latency	Yes	5400	5400	0	0
28	10	EGR Exception	Yes	100	200	0	0
29	5	Stackwise Virtual OOB	Yes	8000	8000	0	0
30	9	MCAST Data	Yes	500	400	0	0
31	10	Gold Pkt	Yes	100	200	0	0

\* NOTE: CPU queue policer rates are configured to the closest hardware supported value

CPU Queue Policer Statistics

```

=====
Policer      Policer Accept  Policer Accept  Policer Drop  Policer Drop
Index        Bytes          Frames          Bytes          Frames
-----
0            0              0              0              0
1            0              0              0              0
2            0              0              0              0
3            0              0              0              0
4            0              0              0              0
5            0              0              0              0
6            0              0              0              0
7            0              0              0              0
8            0              0              0              0
9            0              0              0              0
10           0              0              0              0
11           0              0              0              0
12           0              0              0              0
13           0              0              0              0
14           0              0              0              0
15           0              0              0              0
16           0              0              0              0
17           0              0              0              0
    
```

```

18          0          0          0          0
=====
                        CPP Classes to queue map
=====
PlcIdx CPP Class                               : Queues
-----
0      system-cpp-police-data                   : ICMP GEN/BROADCAST/ICMP Redirect/
10     system-cpp-police-sys-data                : Openflow/Exception/EGR Exception/NFL
      SAMPLED DATA/Gold Pkt/RPF Failed/
13     system-cpp-police-sw-forward             : Sw forwarding/LOGGING/L2 LVX Data
Pack/
9      system-cpp-police-multicast              : Transit Traffic/MCAST Data/
15     system-cpp-police-multicast-end-station  : MCAST END STATION /
7      system-cpp-police-punt-webauth           : Punt Webauth/
1      system-cpp-police-l2-control             : L2 Control/
2      system-cpp-police-routing-control        : Routing Control/Low Latency/
3      system-cpp-police-system-critical        : System Critical/
4      system-cpp-police-l2lvx-control          : L2 LVX Cont Pack/
8      system-cpp-police-topology-control       : Topology Control/
11     system-cpp-police-dot1x-auth             : DOT1X Auth/
12     system-cpp-police-protocol-snooping      : Proto Snooping/
6      system-cpp-police-dhcp-snooping          : DHCP Snooping/
14     system-cpp-police-forus                  : Forus Address resolution/Forus traffic/
5      system-cpp-police-stackwise-virt-control : Stackwise Virtual OOB/
16     system-cpp-default                       : Inter FED Traffic/EWLC Control/EWLC
Data/
18     system-cpp-police-high-rate-app          : High Rate App/

```

## CoPPのモニタリング

CPUキューのトラフィックタイプやポリサーレート（ユーザーが設定したレートやデフォルトのレート）などのポリサー設定を表示するには、次のコマンドを使用します。

コマンド	目的
<b>show policy-map control-plane</b>	さまざまなトラフィックタイプに設定されたレートを表示します。
<b>show policy-map system-cpp-policy</b>	system-cpp ポリシーの下で設定されたすべてのクラスとポリサーレートを表示します。
<b>show platform hardware fed switch {switch-number} qos que stats internal cpu policer</b>	さまざまなトラフィックタイプに設定されたレートを表示します。
<b>show platform software fed {switch-number} qos policy target status</b>	ポリシーステータスとターゲットポートタイプに関する情報を表示します。

## CoPPの機能履歴

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェアリリーストレインで各機能のサポートが導入されたときのソフトウェアリリースだ

けを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェアリリースでもサポートされます。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigatorを使用します。Cisco Feature Navigatorにアクセスするには、[www.cisco.com/go/cfn](http://www.cisco.com/go/cfn)に移動します。Cisco.comのアカウントは必要ありません。

機能	リリース	機能情報
コントロールプレーンポリシング (CoPP) または CPP	Cisco IOS XE Everest 16.5.1a	この機能が導入されました。  CoPP機能によって、不要なトラフィックまたはDoSトラフィックからCPUを保護し、コントロールプレーンおよび管理トラフィックを優先させることにより、デバイスのセキュリティが向上します。  この機能は、CPUキューの有効化および無効化、ポリサーレートの変更、ポリサーレートのデフォルトへの設定、ユーザー定義のクラスマップの作成を行うためのCLI設定オプションを提供します。
CoPPのシステム定義値の変更	Cisco IOS XE Everest 16.6.1	次の新しいシステム定義のクラスが導入されました。  <ul style="list-style-type: none"> <li>• system-cpp-police-stackwise-virt-control</li> <li>• system-cpp-police-l2lvs-control</li> </ul> 次の新しいCPUキューが既存のsystem-cpp-defaultクラスに追加されました。  <ul style="list-style-type: none"> <li>• WK_CPU_Q_UNUSED (7)</li> <li>• WK_CPU_Q_EWLC_CONTROL(9)</li> <li>• WK_CPU_Q_EWLC_DATA(10)</li> </ul> この新しいCPUキューが既存のsystem-cpp-police-sw-forwardに追加されました。WK_CPU_Q_L2_LVX_DATA_PACK (11) このCPUキューは使用できなくなりました。WK_CPU_Q_SGT_CACHE_FULL(27)
設定されているポリサーレートのシステム動作の変更。	Cisco IOS XE Everest 16.6.4	一部のCPUキューでは、すべてのクラスにデフォルトレートを設定しても、デフォルトレートと設定レートの値は同じにはなりません。これは、設定レートが最も近い200の倍数に丸められるためです。

機能	リリース	機能情報
<p>ユーザー定義のクラスマップのサポート停止、および CoPP のシステム定義値の変更</p>	<p>Cisco IOS XE Fuji 16.8.1a</p>	<ul style="list-style-type: none"> <li>• このリリース以降、ユーザー定義のクラスマップの作成はサポートされません。</li> <li>• 新しいシステム定義クラス <code>system-cpp-police-dhcp-snooping</code> が導入されました。</li> <li>• 新しい CPU キュー <code>WK_CPU_Q_INTER_FED_TRAFFIC</code> が既存の <code>system-cpp-default</code> クラスに追加されました。</li> <li>• 次の CPU キューは使用できなくなりました。             <ul style="list-style-type: none"> <li>• <code>WK_CPU_Q_SHOW_FORWARD</code></li> <li>• <code>WK_CPU_Q_UNUSED</code></li> </ul> </li> <li>• 一部の CPU キューのデフォルトポリサーレート (pps) が変更されました。             <ul style="list-style-type: none"> <li>• <code>WK_CPU_Q_EXCEPTION(24)</code> のデフォルトレートが 100 に変更されました。</li> <li>• <code>system-cpp-default</code> の下のすべての CPU キューのデフォルトレートが 2000 に増えました。</li> <li>• <code>system-cpp-police-forus</code> の下のすべての CPU キューのデフォルトレートが 4000 に増えました。</li> </ul> </li> </ul>

機能	リリース	機能情報
CoPP のシステム定義値の変更	Cisco IOS XE Fuji 16.9.1	<p>このリリース以降、18 個のシステム定義クラスが <code>system-cpp-policy</code> の下に作成されます。</p> <p>次の新しいシステム定義のクラスが導入されました。</p> <ul style="list-style-type: none"> <li>• <code>system-cpp-police-high-rate-app</code></li> <li>• <code>system-cpp-police-system-critical</code></li> </ul> <p>これはクラス <code>system-cpp-police-sys- data: CPU queue WK_CPU_Q_OPENFLOW (13)</code> に追加されました。</p> <p>この CPU キューは使用できなくなりました： <code>WK_CPU_Q_LEARNING_CACHE_OVFL(13)</code>。</p>
システム定義のクラスマップの廃止	Cisco IOS XE Fuji 16.9.4	<p>システム定義のクラスマップ <code>system-cpp-police-control-low-priority</code> は廃止されました。</p>







## 第 29 章

# PKI での証明書の許可および失効の設定

- [PKI での証明書の許可および失効の設定 \(691 ページ\)](#)

## PKI での証明書の許可および失効の設定

### 証明書の許可および失効に関する前提条件

#### PKI ストラテジの計画



**ヒント** 実際の証明書の展開を開始する前に、全体の PKI ストラテジを計画することを強く推奨します。

ユーザーまたはネットワーク管理者が次の作業を完了した後に、許可および失効が発生します。

- 認証局 (CA) の設定。
- ピア デバイスの CA への登録。
- ピアツーピア通信に使用される (IP セキュリティ (IPsec) またはセキュア ソケット レイヤ (SSL) などの) プロトコルの確認および設定。

許可および失効に固有の情報をピアデバイス証明書に含めなければならない場合があるため、ピア デバイスを登録する前に、設定する許可および失効ストラテジを決定する必要があります。

#### 高可用性

ハイ アベイラビリティのため、IPsec 保護された Stream Control Transmission Protocol (SCTP) はアクティブ ルータとスタンバイ ルータの両方で設定する必要があります。同期を機能させるには、SCTP を設定した後に、証明書サーバーの冗長性モードを ACTIVE/STANDBY に設定する必要があります。

## 証明書の許可および失効に関する制約事項

- Cisco IOS リリースに応じて、Lightweight Directory Access Protocol (LDAP) がサポートされます。

## 証明書の許可および失効に関する情報

### PKI の許可

PKI 認証では、許可を行いません。多くの場合、一元的に管理されるソリューションが必要ですが、現在の許可用のソリューションは、設定対象のルータに固有です。

それによって証明書を特定の作業に対して許可し、その他の作業に対しては許可しない、と定義できる標準的なメカニズムはありません。アプリケーションが証明書ベースの許可情報を認識する場合、この許可情報を証明書自体に取り込みます。このソリューションでは、許可情報をリアルタイムで更新するための簡単なメカニズムを提供していないため、証明書に組み込まれた固有の許可情報を認識するように各アプリケーションに強制します。

証明書ベースの ACL メカニズムがトラストポイント認証の一部として設定される場合、該当アプリケーションは、この許可情報を判別する役割を担うことはなく、どのアプリケーションに対して証明書を許可するのか指定できません。ルータ上の証明書ベースの ACL は、大きくなりすぎて管理できないことがあります。また、外部サーバーから証明書ベースの ACL 指示を取得する方が有利です。

許可の問題にリアルタイムで対処する現在のソリューションでは、新しいプロトコルの指定や新しいサーバーの構築（それとともに管理およびデータ配布などの関連作業）が必要になります。

### 証明書ステータスのための PKI と AAA サーバーの統合

PKI を認証、許可、アカウントिंग (AAA) サーバーと統合することにより、既存の AAA インフラストラクチャを活用する代替オンライン証明書ステータスソリューションを実現します。証明書を適切な許可レベルで AAA データベースに一覧表示できます。PKI-AAA を明示的にサポートしないコンポーネントでは、デフォルト ラベルの「all」を指定すると、AAA サーバーからの許可が可能になります。また、AAA データベースのラベルが「none」の場合、指定された証明書が有効でないことを示します（アプリケーションラベルが欠如していることと同じですが、「none」は完全性および明確性のために含まれます）。アプリケーション コンポーネントが PKI-AAA をサポートしている場合、コンポーネントを直接指定できる場合があります。たとえば、アプリケーション コンポーネントを「ipsec」、「ssl」、または「osp」に指定できます（ipsec = IP セキュリティ、ssl = セキュア ソケット レイヤ、および osp = Open Settlement Protocol）。



- (注) 現在、アプリケーション ラベルの指定をサポートするアプリケーション コンポーネントはありません。

- AAA サーバーにアクセスしたときに、時間遅延が生じる場合があります。AAA サーバーを利用できない場合、許可は失敗します。

## RADIUS または TACACS+ : AAA サーバー プロトコルの選択

AAA サーバーは、RADIUS または TACACS+ プロトコルと連動するように設定できます。PKI 統合用に AAA サーバーを設定する場合、許可に必要な RADIUS または TACACS 属性を設定する必要があります。

RADIUS プロトコルが使われている場合は、AAA サーバーのユーザー名に設定するパスワードを「cisco」に設定する必要があります。証明書の検証が認証を行い、AAA データベースは許可の目的だけに使用されているので、このパスワードは受け入れ可能です。TACACS プロトコルを使用する場合、TACACS では認証が不要な許可をサポートする（認証にパスワードを使用）ので、AAA サーバーのユーザー名に対して設定されるパスワードとは無関係です。

さらに、TACACS を使用する場合は、AAA サーバーに PKI サービスを追加する必要があります。カスタム属性「cert-application=all」が、PKI サービスの特定のユーザーまたはユーザーグループに追加され、特定のユーザー名が許可されます。

## PKI と AAA サーバー統合用の属性値ペア

次の表に、AAA サーバーと PKI との統合を設定する場合に使用される属性値 (AV) ペアを示します (表に示す値は、可能な値であることに注意してください)。AV ペアはクライアント設定と一致する必要があります。AV ペアが一致しない場合、ピア証明書は許可されません。



- (注) 場合によっては、ユーザーは、他のすべてのユーザーの AV ペアとは異なる AV ペアを持つことができます。その場合、ユーザーごとに一意のユーザー名が必要になります。(authorization username コマンド内に) all パラメータを設定すると、証明書のサブジェクト名全体を許可ユーザー名として使用するよう指定できます。

表 62: 一致する必要がある AV ペア

AV ペア	値
cisco-avpair=pki:cert-application=all	有効な値は、[all] および [none] です。

AV ペア	値
cisco-avpair=pki:cert-trustpoint=msca	<p>この値は、Cisco IOS コマンドライン インターフェイス (CLI) 設定のトラストポイント ラベルです。</p> <p>(注) cert-trustpoint AV ペアの指定は、通常任意です。このペアが指定されている場合、Cisco IOS ルータクエリーは、一致するラベルを持つ証明書トラストポイントから受信する必要があり、認証された証明書は、指定された証明書シリアル番号を持っている必要があります。</p>
cisco-avpair=pki:cert-serial=16318DB7000100001671	<p>この値は証明書のシリアル番号です。</p> <p>(注) cert-serial AV ペアの指定は、通常任意です。このペアが指定されている場合、Cisco IOS ルータクエリーは、一致するラベルを持つ証明書トラストポイントから受信する必要があり、認証された証明書は、指定された証明書シリアル番号を持っている必要があります。</p>
cisco-avpair=pki:cert-lifetime-end=1:00 jan 1, 2003	<p>cert-lifetime-end AV ペアは、証明書で指示された期間を越えた証明書のライフタイムを人為的に延長する場合に使用できます。cert-lifetime-end AV ペアを使用する場合は、cert-trustpoint および cert-serial AV ペアも指定する必要があります。この値は、時/分/月/日/年の形式と一致する必要があります。</p> <p>(注) 月を表す最初の 3 文字 (Jan、Feb、Mar、Apr、May、Jun、Jul、Aug、Sep、Oct、Nov、Dec) だけが使用されます。月を表す文字として 4 文字以上入力すると、残りの文字は無視されます (たとえば、Janxxxx)。</p>

## CRL または OCSP サーバー：証明書失効メカニズムの選択

証明書が適切に署名された証明書として有効になった後、証明書失効方法を実行して、証明書が発行元 CA によって無効にされていないことを確認します。Cisco IOS ソフトウェアは、2 つの失効メカニズムとして証明書失効リスト (CRL) と Online Certificate Status Protocol (OCSP) をサポートします。Cisco IOS ソフトウェアも、証明書のチェックのために AAA 統合をサポートしますが、これには追加の許可機能が含まれます。PKI と AAA 証明書の許可とステータス確認に関する詳細については、「証明書ステータスのための PKI と AAA サーバーの統合」を参照してください。

次の項では、各失効メカニズムの機能方法について説明します。

### CRL とは

CRL とは、失効した証明書のリストです。CRL は、証明書を発行した CA によって作成され、デジタル署名されます。CRL には、各証明書の発行日と失効日が含まれています。

CA は、新しい CRL を定期的に、あるいは CA が責任を負う証明書が失効したときに公開します。デフォルトでは、現在キャッシュされている CRL が失効すると、新しい CRL がダウンロードされます。管理者は、CRL がルータのメモリにキャッシュされる時間を設定したり、CRL キャッシングを完全にディセーブルにしたりできます。CRL キャッシング設定は、トラストポイントに関連付けられたすべての CRL に適用されます。

CRL が失効すると、ルータはキャッシュから CRL を削除します。証明書が検証用に表示されると、新しい CRL がダウンロードされます。ただし、検証中の証明書を記載した新しいバージョンの CRL がサーバー上にあるにもかかわらず、ルータがキャッシュ内の CRL を使用し続ける場合、ルータは証明書が失効したことを認識しません。証明書は拒否されるはずのもので、失効チェックに合格します。

CA は、証明書を発行すると、証明書にその CRL 配布ポイント (CDP) を含めることができます。Cisco IOS クライアントデバイスは、CDP を使用して適切な CRL を見つけ、ロードします。Cisco IOS クライアントは複数の CDP をサポートしますが、Cisco IOS CA は現在 1 つの CDP しかサポートしません。ただし、サードパーティベンダー製の CA には、証明書ごとに複数の CDP または異なる CDP をサポートするものがあります。CDP が証明書に指定されていない場合、クライアントデバイスは、デフォルトの Simple Certificate Enrollment Protocol (SCEP) 方式を使用して CRL を取得します (CDP の場所は、**cdp-url** コマンドを使用して指定できます)。

CRL を実装する際は、次の設計上の注意事項を考慮する必要があります。

- CRL ライフタイムとセキュリティアソシエーション (SA) およびインターネットキー交換 (IKE) ライフタイム
- CRL ライフタイムにより、CA が CRL の更新を発行する時間間隔が決まります。デフォルト CRL ライフタイム値は 168 時間 (1 週間) です。これは、**lifetime crl** コマンドで変更できます。
- CDP のこの方式により、CRL の取得方法が決まり、この方式として、HTTP、Lightweight Directory Access Protocol (LDAP)、SCEP、または TFTP を選択できます。最も一般的に使用されている方式は、HTTP、TFTP、および LDAP です。Cisco IOS ソフトウェアでは、

SCEP にデフォルト設定されていますが、CRL を使用して大容量のインストールを実行する場合、HTTP CDP を推奨します。HTTP では高いスケーラビリティを実現できるからです。

- CDP のこの場所は、CRL の取得先を決定します。たとえば、サーバーおよび CRL の取得先となるファイルパスを指定できます。

### 失効チェック中にすべての CDP を照会

CDP サーバが要求に返答しない場合、Cisco IOS ソフトウェアはエラーを報告し、その結果、ピアの証明書が拒否されることがあります。証明書に複数の CDP がある場合、証明書が拒否されないようにするために、Cisco IOS ソフトウェアは、証明書に表示されている順序で CDP を使用しようと試みます。ルータは、それぞれの CDP URL またはディレクトリ指定を使用して CRL を取得しようと試みます。ある CDP を使用してエラーが発生すると、次の CDP を使用して試行します。



**ヒント** Cisco IOS ソフトウェアは、指示された CDP のいずれかから CRL を取得するためにあらゆる試行を行いますが、CDP 応答の遅延によりアプリケーションのタイムアウトを避けるために、HTTP CDP サーバを高速の冗長 HTTP サーバと併用することを推奨します。

### OCSP とは

OCSP は、証明書の有効性を判別するために使用されるオンラインのメカニズムであり、失効メカニズムとして次のような柔軟性を備えています。

- OCSP では、証明書ステータスをリアルタイムでチェックできます。
- OCSP を使用すると、ネットワーク管理者は、中央 OCSP サーバを指定でき、これにより、ネットワーク内のすべてのデバイスにサービスを提供できます。
- また、OCSP により、ネットワーク管理者は、クライアント証明書ごと、またはクライアント証明書のグループごとに複数の OCSP サーバを柔軟に指定できます。
- OCSP サーバの検証は通常、ルート CA 証明書または有効な下位 CA 証明書に基づいて実行されますが、外部の CA 証明書または自己署名証明書を使用できるように設定することもできます。外部の CA 証明書または自己署名証明書を使用すると、代替の PKI 階層から OCSP サーバ証明書を発行し、有効にできます。

ネットワーク管理者は、さまざまな CA サーバから CRL を収集し、更新するように OCSP サーバを設定できます。ネットワーク内のデバイスは、OCSP サーバに依存して、ピアごとに CRL を取得してキャッシュすることなく証明書ステータスをチェックできます。ピアは、証明書の失効ステータスをチェックする必要がある場合、OCSP 要求に関して疑わしい証明書のシリアル番号およびオプションの固有識別情報（ナンズ）を含む OCSP サーバにクエリーを送信します。OCSP サーバは、CRL のコピーを保持して、CA がその証明書を無効として記載しているかどうか判別します。次に、サーバは、ナンズを含むピアに応答します。応答のナンズが OCSP サーバからピアによって送信された元のナンズと一致しない場合、応答は

無効と見なされ、証明書の検証が失敗します。OCSP サーバーとピア間の対話での帯域幅の消費量は、ほとんどの場合、CRL ダウンロードより少なくなります。

OCSP サーバーが CRL を使用する場合は、CRL 時間の制約事項が適用されます。つまり、追加の証明書失効情報を含む CRL によって新しい CRL が発行されていても、まだ有効な CRL が OCSP サーバーで使用されることがあります。CRL 情報を定期的にダウンロードするデバイスが少なくなっているため、CRL ライフタイム値を小さくするか、CRL をキャッシュしないように OCSP サーバーを設定できます。詳細は、OCSP サーバーのマニュアルを参照してください。



- (注) OCSP の複数応答処理：応答パケットの OCSP レスポンダからの複数の OCSP 単一応答の処理はサポートされています。このデバッグログメッセージに加えて、次のデバッグログメッセージが表示されます。
- CRYPTO\_PKI : OCSP 応答の単一応答の数 : 1 (この値は応答の数に応じて変化します)。

### OCSP サーバーを使用する場合

PKI に次のいずれかの特性がある場合、CRL よりも OCSP の方が適している場合があります。

- リアルタイムの証明書失効ステータスが必要。CRL が定期的にしか更新されず、必ずしも最新の CRL がクライアント デバイスでキャッシュされていない場合があります。たとえば、最新の CRL がまだクライアントにキャッシュされておらず、また、新たに無効にされた証明書がチェック中の場合は、無効にされた証明書が失効チェックに合格します。
- 無効にされた大量の証明書または複数の CRL があります。大きな CRL をキャッシュすると、Cisco IOS メモリの大部分が消費されてしまい、他のプロセスに使用できるリソースが減少することがあります。
- CRL が頻繁に失効するため、CDP は大量の CRL を処理します。

### 許可または失効用に証明書ベースの ACL を使用する場合

証明書には、指定された処理の実行をデバイスまたはユーザーが許可されているかどうかの判別に使用されるフィールドがいくつか含まれています。

証明書ベース ACL はデバイス上に設定されるため、大量の ACL を十分にスケーリングしません。ただし、証明書ベースの ACL では、特定のデバイスの動作を非常に細かく制御できます。また、証明書ベース ACL は追加機能で活用され、失効、許可、またはトラストポイントなどの PKI コンポーネントを使用するタイミングを判別するのに役立ちます。証明書ベース ACL は全般的なメカニズムを提供しており、このメカニズムによりユーザーは、許可または追加処理に対して有効になっている特定の証明書または証明書のグループを選択できます。

証明書ベース ACL では、証明書内の 1 つ以上のフィールドおよび指定された各フィールドで許可される値を指定します。証明書内でチェックする必要があるフィールドと、それらのフィールドで認められる値または認められない値を指定できます。

フィールドと値との比較には、6つの論理テスト（Equal（等しい）、Notequal（等しくない）、Contains（含む）、Less than（未満）、Does not contain（含まない）、Greater than or equal（以上））を使用できます。1つの証明書ベース ACL で複数のフィールドを指定した場合、その ACL と一致するには、ACL 内のすべてのフィールド条件に合致しなければなりません。同じ ACL 内で、同じフィールドを複数回指定できます。複数の ACL を指定できます。一致するものが見つかるか、または ACL の処理がすべて完了するまで、各 ACL が順に処理されます。

## 証明書ベース ACL を使用した失効チェックの無視

証明書ベース ACL を設定して、有効なピアの失効チェックおよび失効した証明書を無視するようルータに指示できます。したがって、指定基準を満たす証明書は、証明書の有効期間にかかわらず受け入れることができます。また、証明書が指定基準を満たしている場合は失効チェックを実行する必要がなくなります。AAA サーバーとの通信が証明書で保護される場合にも、証明書ベース ACL を使用して失効チェックを無視できます。

### 失効リストの無視

トラストポイントが特定の証明書を除いて CRL を適用できるようにするには、**skip revocation-check** キーワードを指定して **match certificate** コマンドを入力します。このような適用は、スポークツースポークの直接接続も可能なハブアンドスポーク設定に最も便利です。純粋なハブアンドスポーク設定では、すべてのスポークはハブだけに接続するので、CRL チェックはハブ上だけで済みます。スポークが別のスポークと直接通信する場合、ネイバーピア証明書に対して、各スポーク上で CRL を要求する代わりに、**skip revocation-check** キーワードを指定して **match certificate** コマンドを使用できます。

### 失効した証明書の無視

失効した証明書を無視するようにルータを設定するには、**allow expired-certificate** キーワードを指定して **match certificate** コマンドを入力します。このコマンドには、次のような目的があります。

- このコマンドは、ピアの証明書が失効した場合にピアが新しい証明書を取得するまで、失効した証明書を「許可する」ために使用できます。
- ルータクロックがまだ正しい時間に設定されていない場合、クロックが設定されるまで、ピアの証明書はまだ有効ではないものとして表示されます。このコマンドは、ルータクロックが未設定であっても、ピアの証明書を許可する場合に使用できます。



(注) ネットワークタイムプロトコル (NTP) が IPSec 接続だけで（通常、ハブアンドスポーク設定のハブによって）利用可能な場合は、ルータクロックを絶対に設定できません。ハブの証明書がまだ有効でないため、ハブへのトンネルを「アップ」状態にできません。

- 「失効」とは、失効している証明書またはまだ有効ではない証明書の総称です。証明書には、開始時刻と終了時刻が指定されます。ACL を目的とした、失効証明書は、ルータの現在時刻が証明書で指定された開始および終了時刻の範囲外の証明書です。



### 証明書の AAA チェックのスキップ

AAA サーバーとの通信が証明書で保護され、証明書の AAA チェックをスキップする場合は、**skip authorization-check** キーワードを指定して **match certificate** コマンドを使用します。たとえば、すべての AAA トラフィックがバーチャルプライベートネットワーク (VPN) トンネルを通過するように設定され、このトンネルが証明書で保護されている場合は、**skip authorization-check** キーワードを指定して **match certificate** コマンドを使用すると、証明書チェックをスキップしてトンネルを確立できます。

AAA サーバーとの PKI 統合が設定されると、**match certificate** コマンドと **skip authorization-check** キーワードを設定する必要があります。



- (注) AAA サーバーが IPSec 接続によってのみ使用可能な場合は、IPSec 接続が確立されるまで AAA サーバーとは通信できません。AAA サーバーの証明書がまだ有効でないため、IPSec 接続を「アップ」状態にできません。

## PKI 証明書チェーンの検証

証明書チェーンにより、ピア証明書からルート CA 証明書までの、一連の信頼できる証明書を確立します。階層型 PKI 内では、登録されているすべてのピアが信頼できるルート CA 証明書または共通の下位 CA を共有している場合、証明書を相互に検証できます。各 CA が 1 つのラストポイントに対応します。

証明書チェーンをピアから受信すると、最初の信頼できる証明書またはラストポイントに到達するまで、証明書チェーンパスのデフォルト処理が続けられます。管理者は証明書チェーンが、すべての証明書（下位 CA 証明書を含む）で処理されるレベルを設定できます。

証明書チェーンの処理レベルを設定すると、信頼できる証明書の再認証、信頼できる証明書チェーンの延長、および欠落のある証明書チェーンの補完が可能になります。

### 信頼できる証明書の再認証

このデフォルト動作でルータは、チェーンを検証する前に、ピアによって送信された証明書チェーンから任意の信頼できる証明書を削除します。管理者は証明書チェーンパス処理を設定して、チェーン検証の前にすでに信頼されている CA 証明書をルータが削除しないようにできます。そのため、チェーン内のすべての証明書は現在のセッションに対して再度認証されます。

### 信頼できる証明書チェーンの延長

このデフォルト動作でルータは、ピアによって送信された証明書チェーンに欠落している証明書がある場合、その信頼できる証明書を使用して証明書チェーンを延長します。ルータが検証するのは、ピアによって送信されたチェーンの証明書だけです。管理者は証明書チェーンパス処理を設定して、ピアの証明書チェーンの証明書およびルータの信頼できる証明書を、指定したポイントに対して有効にできます。

### 証明書チェーンの欠落の補完

管理者は証明書チェーン処理を設定して、設定済みの Cisco IOS トラストポイント階層に欠落がある場合、ピアによって送信された証明書を使用して証明書のセットを有効にできます。



(注) 親検証を要求するようにトラストポイントが設定され、ピアが完全な証明書チェーンを提示しない場合、欠落を補完できないため証明書チェーンは拒否され、無効になります。



(注) 親検証を要求するようにトラストポイントが設定されていて、設定済みの親トラストポイントがない場合は、設定エラーです。発生する証明書チェーンの欠落を補完できず、下位 CA 証明書を有効にできません。この証明書チェーンは無効です。

## PKI に対して証明書の許可および失効を設定する方法

### AAA サーバーとの PKI 統合の設定

ピアによって提出された証明書から AAA ユーザー名を生成し、証明書内で AAA データベース ユーザー名の作成に使用するフィールドを指定するには、次の作業を実行します。



(注) **authorization username** コマンドでサブジェクト名として **all** キーワードを使用する際に、次の制約事項を考慮する必要があります。

- 一部の AAA サーバーでは、ユーザー名の長さが制限されます（たとえば、64 文字まで）。その結果、証明書の全体のサブジェクト名は、サーバーの制約条件より長くできません。
- 一部の AAA サーバーでは、ユーザー名に使用できる文字セットが制限されます（たとえば、スペース ( ) および等号 (=) を使用できない場合があります）。このような文字セットの制限がある AAA サーバーでは、**all** キーワードを使用できません。
- トラストポイント設定の **subject-name** コマンドは、必ずしも最終の AAA サブジェクト名とは限りません。証明書要求に完全修飾ドメイン名 (FQDN)、シリアル番号、またはルータの IP アドレスが含まれている場合は、発行された証明書のサブジェクト名フィールドにもこれらのコンポーネントが含まれます。コンポーネントをオフにするには、**fqdn**、**serial-number**、および **ip-address** の各コマンドに **none** キーワードを使用します。
- CA サーバーが証明書を発行すると、CA サーバーは、要求したサブジェクト名フィールドを変更することがあります。たとえば、一部のベンダーの CA サーバーが要求したサブジェクト名の相対識別名 (RDN) を CN、OU、O、L、ST、および C に切り替えます。ただし、別の CA サーバーは、設定した LDAP ディレクトリルート (O=cisco.com など) を要求したサブジェクト名の最後に追加する場合があります。
- 証明書の表示用に選択するツールによっては、サブジェクト名の RDN の印刷順序が異なることがあります。Cisco IOS ソフトウェアでは、重要度が最低の RDN を先頭に表示しますが、Open Source Secure Socket Layer (OpenSSL) などの、他のソフトウェアでは、重要度が最高の RDN を先頭に表示します。したがって、完全な識別名 (DN) (サブジェクト名) を持つ AAA サーバーを対応するユーザー名として設定する場合は、Cisco IOS ソフトウェアスタイル (つまり、重要度が最低の RDN を先頭に表示) が使用されていることを確認してください。

## 手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authorization network listname [method]**
5. **crypto pki trustpoint name**
6. **enrollment [mode] [ retry period minutes] [ retry count number] url url [pem]**
7. **revocation-check method**
8. **exit**
9. **authorization username subjectname subjectname**
10. **authorization list listname**
11. **tacacs server server-name**
12. **address {ipv4 | ipv6} ip-address**
13. **key string**

## 14. end

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> <b>enable</b>	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	<b>configure terminal</b> 例： Device# <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 3	<b>aaa new-model</b> 例： Device(config)# <b>aaa new-model</b>	AAA アクセスコントロールモデルをイネーブルにします。
ステップ 4	<b>aaa authorization network listname [method]</b> 例： Device(config)# <b>aaa authorization network maxaaa group tacacs+</b>	ネットワークへのユーザー アクセスを制限するパラメータを設定します。  • <b>method</b> : <b>group radius</b> 、 <b>group tacacs+</b> 、または <b>group group-name</b> のいずれか。
ステップ 5	<b>crypto pki trustpoint name</b> 例： Device(config)# <b>crypto pki trustpoint msca</b>	トラストポイントおよび設定された名前を宣言して、CA 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 6	<b>enrollment [mode] [retry period minutes] [retry count number] url url [pem]</b> 例： Device(ca-trustpoint)# <b>enrollment url http://caserver.myexample.com</b>  または Device(ca-trustpoint)# <b>enrollment url http://[2001:DB8:1:1::1]:80</b>	CA の次の登録パラメータを指定します。  • (任意) CA システムが登録局 (RA) を提供する場合、 <b>mode</b> キーワードとして RA モードを指定します。デフォルトでは、RA モードは無効です。  • (任意) <b>retry period</b> キーワードおよび <i>minutes</i> 引数は、CA に別の証明書要求を送信するまでルータが待機する期間を分単位で指定します。有効値は 1 ~ 60 です。デフォルトは 1 です。  • (任意) <b>retry count</b> キーワードおよび <i>number</i> 引数は、直前の要求に対する応答をルータが受信しない場合、ルータが証明書要求を再送信する回数を指定します。有効な値は、1 ~ 100 です。デフォルトは 10 です。  • <i>url</i> 引数は、ルータが証明書要求を送信する CA の URL です。

	コマンドまたはアクション	目的
		<p>(注) IPv6 アドレスは <b>http:</b> 登録方式に追加できます。たとえば、 http://[ipv6-address]:80 です。URL 内の IPv6 アドレスは括弧で囲む必要があります。</p> <ul style="list-style-type: none"> <li>(任意) <b>pem</b> キーワードは、証明書要求にプライベート強化メール (PEM) の境界を追加します。</li> </ul>
ステップ 7	revocation-check method 例 : Device(ca-trustpoint)# <b>revocation-check crl</b>	(任意) 証明書の失効ステータスをチェックします。
ステップ 8	<b>exit</b> 例 : Device(ca-trustpoint)# <b>exit</b>	CA 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、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 9	<b>authorization username subjectname subjectname</b> 例 : Device(config)# <b>authorization username subjectname serialnumber</b>	AAA ユーザー名の構築に使用する異なる証明書フィールドのパラメータを設定します。 <i>subjectname</i> 引数には、次のいずれかを指定できます。 <ul style="list-style-type: none"> <li><b>all</b> : 証明書の識別名 (サブジェクト名) 全体。</li> <li><b>commonname</b> : 証明書の共通名。</li> <li><b>country</b> : 証明書の国。</li> <li><b>email</b> : 証明書の電子メール。</li> <li><b>ipaddress</b> : 証明書の IP アドレス。</li> <li><b>locality</b> : 証明書の地域。</li> <li><b>organization</b> : 証明書の組織。</li> <li><b>organizationalunit</b> : 証明書の組織単位。</li> <li><b>postalcode</b> : 証明書の郵便番号。</li> <li><b>serialnumber</b> : 証明書のシリアル番号。</li> <li><b>state</b> : 証明書の州フィールド。</li> <li><b>streetaddress</b> : 証明書の住所。</li> <li><b>title</b> : 証明書のタイトル。</li> </ul>

## ■ トラブルシューティングのヒント

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <b>unstructuredname</b> : 証明書の非公式名。</li> </ul>
ステップ 10	<b>authorization list listname</b> 例 : Device(config)# <b>authorization list maxaaa</b>	AAA 認可リストを指定します。
ステップ 11	<b>tacacs server server-name</b> 例 : Device(config)# <b>tacacs server yourserver</b>	TACACS+ サーバーを指定します。
ステップ 12	<b>address {ipv4   ipv6} ip-address</b> 例 : Device(config-server-tacacs)# <b>address ipv4 192.0.2.2</b>	TACACS サーバーの IP アドレスを設定します。
ステップ 13	<b>key string</b> 例 : Device(config-server-tacacs)# <b>key a_secret_key</b>	スイッチと TACACS サーバーとの間で使用される許可および暗号キーを設定します。
ステップ 14	<b>end</b> 例 : Device(config-server-tacacs)# <b>end</b> 例 :	特権 EXEC モードに戻ります。

## ■ トラブルシューティングのヒント

CA とルータ間のインタラクションのトレース (メッセージタイプ) に関するデバッグメッセージを表示するには、**debug crypto pki transactions** コマンドを使用します (サンプル出力を参照してください。ここでは、AAA サーバー交換との成功した PKI 統合、および AAA サーバー交換との失敗した PKI 統合を示します)。

### 成功した交換

```
Device# debug crypto pki transactions
Apr 22 23:15:03.695: CRYPTO_PKI: Found a issuer match
Apr 22 23:15:03.955: CRYPTO_PKI: cert revocation status unknown.
Apr 22 23:15:03.955: CRYPTO_PKI: Certificate validated without revocation check
```

「CRYPTO\_PKI\_AAA」と表示されている各行は、AAA 認可チェックの状態を示します。各 AAA AV ペアが示され、認可チェックの結果が表示されます。

```
Apr 22 23:15:04.019: CRYPTO_PKI_AAA: checking AAA authorization (ipsecca_script_aalist,
PKIAAA-L, <all>)
Apr 22 23:15:04.503: CRYPTO_PKI_AAA: reply attribute ("cert-application" = "all")
Apr 22 23:15:04.503: CRYPTO_PKI_AAA: reply attribute ("cert-trustpoint" = "CA1")
Apr 22 23:15:04.503: CRYPTO_PKI_AAA: reply attribute ("cert-serial" = "15DE")
```

```
Apr 22 23:15:04.503: CRYPTO_PKI_AAA: authorization passed
Apr 22 23:12:30.327: CRYPTO_PKI: Found a issuer match
```

### 失敗した交換

```
Device# debug crypto pki transactions
Apr 22 23:11:13.703: CRYPTO_PKI_AAA: checking AAA authorization =
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: reply attribute ("cert-application" = "all")
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: reply attribute ("cert-trustpoint"= "CA1")
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: reply attribute ("cert-serial" = "233D")
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: parsed cert-lifetime-end as: 21:30:00
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: timezone specific extended
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: cert-lifetime-end is expired
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: cert-lifetime-end check failed.
Apr 22 23:11:14.203: CRYPTO_PKI_AAA: authorization failed
```

上記の失敗した交換では、証明書が失効しています。

## PKI 証明書ステータス チェックの失効メカニズムの設定

証明書失効メカニズム（CRL または OCSP）として CRL を設定し、PKI の証明書のステータスをチェックするには、次の作業を実行します。

### revocation-check コマンド

**revocation-check** コマンドを使用し、ピアの証明書が無効にされていないことを確認するための方式（OCSP、CRL、または失効チェックのスキップ）を少なくとも 1 つ指定します。複数の方式を指定する場合、方式を適用する順序は、このコマンドで指定した順序になります。

ルータに適用可能な CRL がなく、いずれの CRL も取得できない場合、あるいは OCSP サーバーがエラーを返す場合、設定に **none** キーワードを含めないかぎり、ルータはピアの証明書を拒否します。**none** キーワードを設定した場合、失効チェックは実行されず、証明書は常に受け入れられます。

### OCSP サーバーとのナンスおよびピア通信

OCSP を使用すると、OCSP サーバーとのピア通信時に、OCSP 要求に関するナンス（固有識別情報）がデフォルトで送信されます。ナンスを使用することにより、ピアと OCSP サーバー間にセキュアで信頼性の高い通信チャネルが確立されます。

OCSP サーバーがナンスをサポートしていない場合は、ナンスの送信をディセーブルにできません。詳細は、OCSP サーバのマニュアルを参照してください。

### 始める前に

- クライアント証明書を発行する前に、サーバーで適切な設定（CDP の設定など）を行う必要があります。
- OCSP サーバーから CA サーバーの失効ステータスを返すように設定するときは、CA サーバーが発行した OCSP 応答署名証明書を OCSP サーバーに設定する必要があります。署名証明書が正しいフォーマットであることを確認してください。署名証明書のフォーマットが正しくない場合、ルータは、OCSP 応答を受理しません。詳細については、OCSP のマニュアルを参照してください。



- (注)
- OCSP は、HTTP を使用してメッセージを転送するので、OCSP サーバーにアクセスする際に遅延が発生する場合があります。
  - OCSP サーバーが、失効ステータスのチェックを通常の CRL 処理に依存している場合、CRL の遅延は OCSP にも適用されます。

## 手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint name**
4. **ocsp url url**
5. **revocation-check method1 [method2 method3]**
6. **ocsp disable-nonce**
7. **exit**
8. **exit**
9. **show crypto pki certificates**
10. **show crypto pki trustpoints [status | label [status]]**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	<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 3	<b>crypto pki trustpoint name</b> 例： Device(config)# crypto pki trustpoint hazel	トラストポイントおよび設定された名前を宣言して、CA 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 4	<b>ocsp url url</b> 例： Device(ca-trustpoint)# ocsp url http://ocsp-server または	<i>url</i> 引数は、トラストポイントが証明書ステータスをチェックできるように OCSP サーバーの URL を指定します。この URL は、証明書の AIA 拡張部に指定されている OCSP サーバーの URL（存在する場合）を上書きします。設定したトラストポイントに関連するすべての証明書は、OCSP サーバーに



	コマンドまたはアクション	目的
	<pre>Device(ca-trustpoint)# obsp url http://10.10.10.1:80</pre> <p>または</p> <pre>Device(ca-trustpoint)# obsp url http://[2001DB8:1:1::2]:80</pre>	<p>よって確認されます。使用可能な URL は、ホスト名、IPv4 アドレス、または IPv6 アドレスです。</p>
ステップ 5	<p><b>revocation-check</b> <i>method1</i> [<i>method2 method3</i>]</p> <p>例 :</p> <pre>Device(ca-trustpoint)# revocation-check obsp none</pre>	<p>証明書の失効ステータスをチェックします。</p> <ul style="list-style-type: none"> <li>• <b>crl</b> : CRL によって証明書をチェックします。これがデフォルトのオプションです。</li> <li>• <b>none</b> : 証明書のチェックを無視します。</li> <li>• <b>osp</b> : OCSP サーバーによって証明書をチェックします。</li> </ul> <p>2 番目と 3 番目の方法を指定した場合、各方法はその直前の方法でエラーが返された場合（サーバーがダウンしている場合など）にだけ使用されます。</p>
ステップ 6	<p><b>osp disable-nonce</b></p> <p>例 :</p> <pre>Device(ca-trustpoint)# obsp disable-nonce</pre>	<p>(任意) OCSP サーバーとピアが通信するときに、ナンス (OCSP 要求に関する固有識別情報) が送信されないように指定します。</p>
ステップ 7	<p><b>exit</b></p> <p>例 :</p> <pre>Device(ca-trustpoint)# exit</pre>	<p>グローバル コンフィギュレーション モードに戻ります。</p>
ステップ 8	<p><b>exit</b></p> <p>例 :</p> <pre>Device(config)# exit</pre>	<p>特権 EXEC モードに戻ります。</p>
ステップ 9	<p><b>show crypto pki certificates</b></p> <p>例 :</p> <pre>Device# show crypto pki certificates</pre>	<p>(任意) 証明書に関する情報を表示します。</p>
ステップ 10	<p><b>show crypto pki trustpoints</b> [<i>status</i>   <i>label</i> [<i>status</i>]]</p> <p>例 :</p> <pre>Device# show crypto pki trustpoints</pre>	<p>ルータに設定されているトラストポイントに関する情報を表示します。</p>

## 証明書の許可および失効の設定

証明書ベース ACL の指定、失効チェックまたは失効した証明書の無視、手動によるデフォルトの CDP の場所の上書き、手動による OCSP サーバー設定の上書き、CRL キャッシングの設定、あるいは証明書シリアル番号に基づくセッションの受理/拒否の設定を行うには、必要に応じて次の作業を実行します。

### 失効チェックを無視するように証明書ベース ACL を設定

証明書ベース ACL を使用して、失効チェックおよび失効証明書を無視するようにルータを設定するには、次の手順を実行します。

- 既存のトラストポイントの識別またはピアの証明書の検証に使用される新しいトラストポイントを作成します。トラストポイントがまだ認証されていない場合は、認証してください。必要に応じて、ルータをこのトラストポイントに登録できます。**match certificate** コマンドと **skip revocation-check** キーワードを使用する場合は、トラストポイントにオプションの CRL を設定しないでください。
- 証明書自体の CRL をチェックする必要がない証明書の固有の特性と、許可する必要がある失効証明書の固有の特性を判別します。
- 前のステップで確認した特性と一致する証明書マップを定義します。
- 最初の手順で作成または指定したトラストポイントに、**match certificate** コマンドと **skip revocation-check** キーワード、**match certificate command** と **allow expired-certificate** キーワードを追加できます。



(注) 証明書マップは、ピアの公開キーがキャッシュされている場合でも確認されます。たとえば、ピアによって公開キーがキャッシュされており、証明書マップがトラストポイントに追加されて証明書が禁止されると、証明書マップが有効になります。これにより、過去に一度接続され、現在は禁止されている証明書を持つクライアントが再接続することを防ぎます。

### 証明書内の CDP の手動による上書き

ユーザーは、手動で設定した CDP で証明書内の CDP を上書きできます。証明書の CDP の手動による上書きは、特定のサーバーが長時間利用できない場合に便利です。元の CDP を含む証明書のすべてを再発行しなくても、証明書の CDP を URL またはディレクトリ指定に置き換えることができます。

### 手動による証明書の OCSP サーバー設定の上書き

管理者はクライアント証明書の Authority Information Access (AIA) フィールドに指定された、または **ocsp url** コマンドを発行して設定された OCSP サーバーの設定値を上書きできます。**match certificate override ocsp** コマンドを使用すると、1つまたは複数の OCSP サーバーをクライアント証明書ごとに、またはクライアント証明書のグループごとに手動で指定できます。失効チェック時にクライアント証明書が証明書マップに正常に照合された場合、**match certificate**

**override ocspl** コマンドを発行すると、クライアント証明書 AIA フィールドまたは **ocsp url** コマンド設定が上書きされます。



(注) 1つのクライアント証明書には、OCSP サーバーを1つだけ指定できます。

## CRL キャッシュ コントロールの設定

デフォルトでは、現在キャッシュされている CRL が失効すると、新しい CRL がダウンロードされます。管理者は、**crl cache delete-after** コマンドを発行して、CRL がキャッシュに保持される最大時間（分単位）を設定するか、**crl cache none** コマンドを発行して CRL キャッシュを無効にできます。**crl-cache delete-after** コマンドまたは **crl-cache none** コマンドのみを指定できます。トラストポイントに両方のコマンドを入力した場合は、後に実行されたコマンドが有効になり、メッセージが表示されます。

**crl-cache none** コマンドまたは **crl-cache delete-after** コマンドのいずれを実行しても現在キャッシュされている CRL に影響はありません。**crl-cache none** コマンドを設定した場合、このコマンドを発行すると、ダウンロードされたすべての CRL はキャッシュされません。**crl-cache delete-after** コマンドを設定した場合、このコマンドの発行後に設定されたライフタイムだけがダウンロードされた CRL に影響します。

この機能は、CA が失効日を指定せずに CRL を発行する場合、あるいは失効日が数日後または数週間後に迫っている場合に役立ちます。

## 証明書のシリアル番号セッションコントロールの設定

証明書検証要求がセッションのトラストポイントによって受け入れられる、または拒否されるように証明書シリアル番号を指定できます。証明書のシリアル番号セッションコントロールによっては、証明書がまだ有効であっても、セッションが拒否される場合があります。証明書のシリアル番号セッションコントロールは、**serial-number** フィールドを持つ証明書マップまたは AAA 属性のいずれかを使用して **cert-serial-not** コマンドで設定できます。

セッションコントロールに証明書マップを使用すると、管理者は、1つの証明書シリアル番号を指定できます。AAA 属性を使用すると、管理者は、セッションコントロールに証明書シリアル番号を指定できます。

### 始める前に

- 証明書マップをトラストポイントに関連付ける前に、トラストポイントを定義し、認証する必要があります。
- CDP オーバライド機能を有効にする、または **serial-number** コマンドを発行する前に、証明書マップを設定する必要があります。
- PKI と AAA サーバーとの統合は、「証明書ステータスのための PKI と AAA サーバーの統合」の説明のとおり AAA 属性を使用して正常に完了する必要があります。

## 手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki certificate map** *label sequence-number*
4. *field-name match-criteria match-value*
5. **exit**
6. **crypto pki trustpoint** *name*
7. 次のいずれかを実行します。
  - **crl-cache none**
  - **crl-cache delete-after** *time*
8. **match certificate** *certificate-map-label* [**allow expired-certificate** | **skip revocation-check** | **skip authorization-check**]
9. **match certificate** *certificate-map-label* **override cdp** {*url* | *directory*} *string*
10. **match certificate** *certificate-map-label* **override oosp** [*trustpoint trustpoint-label*] *sequence-number url oosp-url*
11. **exit**
12. **aaa new-model**
13. **aaa attribute list** *list-name*
14. **attribute type** {*name*} {*value*}
15. **exit**
16. **exit**
17. **show crypto pki certificates**

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	<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 3	<b>crypto pki certificate map</b> <i>label sequence-number</i> 例： Device(config)# crypto pki certificate map Group 10	証明書において、一致する必要がある値または一致する必要がない値を定義し、CA 証明書マップ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 4	<p><i>field-name match-criteria match-value</i></p> <p>例 :</p> <pre>Device(ca-certificate-map)# subject-name co MyExample</pre>	<p>1 つまたは複数の証明書フィールドと、これらのフィールドの一致基準および照合する値を指定します。</p> <p><i>field-name</i> には、次のいずれかの名前文字列（大文字と小文字を区別しない）または日付を指定します。</p> <ul style="list-style-type: none"> <li>• <b>alt-subject-name</b></li> <li>• <b>expires-on</b></li> <li>• <b>issuer-name</b></li> <li>• <b>name</b></li> <li>• <b>serial-number</b></li> <li>• <b>subject-name</b></li> <li>• <b>unstructured-subject-name</b></li> <li>• <b>valid-start</b></li> </ul> <p>(注) 日付フィールドのフォーマットは、dd mm yyyy hh:mm:ss または mmm dd yyyy hh:mm:ss です。</p> <p><i>match-criteria</i> には、次の論理演算子のいずれかを指定します。</p> <ul style="list-style-type: none"> <li>• <b>co</b> : 含む（名前およびシリアル番号フィールドでのみ有効）</li> <li>• <b>eq</b> : 等しい（名前、シリアル番号、および日付フィールドで有効）</li> <li>• <b>ge</b> : 以上（日付フィールドでのみ有効）</li> <li>• <b>lt</b> : 未満（日付フィールドでのみ有効）</li> <li>• <b>nc</b> : 含まない（名前およびシリアル番号フィールドでのみ有効）</li> <li>• <b>ne</b> : 等しくない（名前、シリアル番号、および日付フィールドで有効）</li> </ul> <p><i>match-value</i> は、<i>match-criteria</i> で割り当てられた論理演算子を使用してテストする名前または日付です。</p>

	コマンドまたはアクション	目的
		(注) このコマンドは、証明書ベース ACL を設定する場合にだけ使用し、失効チェックまたは失効した証明書を無視するように証明書ベース ACL を設定する場合には使用しないでください。
ステップ 5	<b>exit</b> 例：  Device(ca-certificate-map)# exit	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 6	<b>crypto pki trustpoint name</b> 例：  Device(config)# crypto pki trustpoint Access2	トラストポイントおよび設定された名前を宣言して、CA 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 7	次のいずれかを実行します。  • <b>crl-cache none</b>  • <b>crl-cache delete-after time</b> 例：  Device(ca-trustpoint)# crl-cache none 例：  Device(ca-trustpoint)# crl-cache delete-after 20	(任意) トラストポイントに関連付けられたすべての CRL の CRL キャッシングを完全にディセーブルにします。  <b>crl-cache none</b> コマンドを実行しても、現在キャッシュされている CRL に影響はありません。このコマンドが設定された後にダウンロードされるすべての CRL は、キャッシュされません。  (任意) トラストポイントに関連付けられたすべての CRL に関して、CRL がキャッシュに保持される最大時間を指定します。  • <i>time</i> : CRL が削除されるまでの時間 (分単位)。  <b>crl-cache delete-after</b> コマンドを実行しても、現在キャッシュされている CRL に影響はありません。設定されたライフタイムは、このコマンドが設定された後にダウンロードされた CRL だけに影響します。
ステップ 8	<b>match certificate certificate-map-label [allow expired-certificate   skip revocation-check   skip authorization-check]</b> 例：  Device(ca-trustpoint)# match certificate Group skip revocation-check	(任意) 証明書ベース ACL ( <b>crypto pki certificate map</b> コマンドによって定義されている) をトラストポイントに関連付けます。  • <i>certificate-map-label</i> : <b>crypto pki certificate map</b> コマンドを使用して指定した <i>label</i> 引数と一致する必要があります。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <b>allowexpired-certificate</b> : 失効した証明書を無視します。</li> <li>• <b>skip revocation-check</b> : トラストポイントが、特定の証明書を除く CRL を適用できるようにします。</li> <li>• <b>skip authorization-check</b> : AAA サーバーとの PKI 統合を設定すると、証明書の AAA チェックをスキップします。</li> </ul>
ステップ 9	<p><b>match certificate</b> <i>certificate-map-label</i> <b>override cdp</b> <b>{url   directory}</b> <i>string</i></p> <p>例 :</p> <pre>Device(ca-trustpoint)# match certificate Group1 override cdp url http://server.cisco.com</pre>	<p>(任意) URL またはディレクトリが指定された証明書の、既存の CDP エントリを手動で上書きします。</p> <ul style="list-style-type: none"> <li>• <b>certificate-map-label</b> : ユーザー指定のラベル。事前に定義された <b>crypto pki certificate map</b> コマンドに指定した <i>label</i> 引数と一致する必要があります。</li> <li>• <b>url</b> : 証明書の CDP が HTTP または LDAP URL で上書きされるように指定します。</li> <li>• <b>directory</b> : 証明書の CDP が LDAP ディレクトリ指定で上書きされるように指定します。</li> <li>• <b>string</b> : URL またはディレクトリ指定。</li> </ul> <p>(注) 一部のアプリケーションは、すべての CDP が試行される前にタイムアウトすることがあり、エラーメッセージで報告します。エラーメッセージはルータに影響を及ぼしません。また、Cisco IOS ソフトウェアは、すべての CDP が試行されるまで CRL の取得を続行します。</p>
ステップ 10	<p><b>match certificate</b> <i>certificate-map-label</i> <b>override ocsp</b> [<b>trustpoint</b> <i>trustpoint-label</i>] <i>sequence-number</i> <b>url</b> <i>ocsp-url</i></p> <p>例 :</p> <pre>Device(ca-trustpoint)# match certificate mycertmapname override ocsp trustpoint mytp 15 url http://192.0.2.2</pre>	<p>(任意) OCSP サーバーをクライアント証明書ごとに、またはクライアント証明書のグループごとに指定し、複数回発行して、追加の OCSP サーバーおよびクライアント証明書の設定 (代替の PKI 階層を含む) を指定できます。</p> <ul style="list-style-type: none"> <li>• <b>certificate-map-label</b> : 既存の証明書マップ名。</li> <li>• <b>trustpoint</b> : OCSP サーバー証明書を検証するときに使用されるトラストポイント。</li> </ul>

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> <li>• <i>sequence-number</i> : <b>match certificate override</b> <b>ocsp</b> コマンド文を検証対象の証明書に適用する順序。照合が最低のシーケンス番号から最高のシーケンス番号に実行されます。同じシーケンス番号で複数のコマンドを発行すると、前の OCSP サーバー オーバライド設定が上書きされます。</li> <li>• <b>url</b> : OCSP サーバーの URL。</li> </ul> <p>証明書が設定された証明書マップと一致すると、クライアント証明書の AIA フィールドおよび以前に発行された <b>ocsp url</b> コマンド設定値は、指定された OCSP サーバーで上書きされます。</p> <p>マップベースの一致が発生しない場合、引き続き次の2つのケースがクライアント証明書に適用されます。</p> <ul style="list-style-type: none"> <li>• OCSP を失効方法として指定すると、AIA フィールド値がクライアント証明書に引き続き適用されます。</li> <li>• <b>ocsp url</b> 設定が存在する場合は、<b>ocsp url</b> 設定が引き続きクライアント証明書に適用されます。</li> </ul>
ステップ 11	<b>exit</b> 例 : <pre>Device(ca-trustpoint)# exit</pre>	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>aaa new-model</b> 例 : <pre>Device(config)# aaa new-model</pre>	(任意) AAA アクセス コントロール モデルをイネーブルにします。
ステップ 13	<b>aaa attribute list</b> <i>list-name</i> 例 : <pre>Device(config)# aaa attribute list crl</pre>	(任意) ルータにローカルで AAA 属性リストを定義し、 <b>config-attr-list</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 14	<b>attribute type</b> <i>{name}</i> <i>{value}</i> 例 : <pre>Device(config-attr-list)# attribute type cert-serial-not 6C4A</pre>	<p>(任意) ルータの AAA 属性リストにローカルに追加される AAA 属性タイプを定義します。</p> <p>証明書のシリアル番号セッションコントロールを設定するために、管理者は、<i>value</i> フィールドの特定</p>



	コマンドまたはアクション	目的
		<p>の証明書を、<i>name</i> が <b>cert-serial-not</b> に設定されているシリアル番号に基づき受け入れるか、拒否するか指定できます。証明書のシリアル番号が属性タイプ設定で指定されたシリアル番号と一致した場合、証明書は拒否されます。</p> <p>使用可能な AAA 属性タイプのリストを表示するには、<b>show aaa attributes</b> コマンドを実行してください。</p>
ステップ 15	<b>exit</b> 例： Device(ca-trustpoint)# exit 例： Device(config-attr-list)# exit	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 16	<b>exit</b> 例： Device(config)# exit	特権 EXEC モードに戻ります。
ステップ 17	<b>show crypto pki certificates</b> 例： Device# show crypto pki certificates	(任意) CA 証明書が認証されたら、ルータにインストールされた証明書のコンポーネントを表示します。

## 例

次に、サンプル証明書を示します。OCSP 関連の拡張子は感嘆符を使用して示されません。

```
Certificate:
  Data:
    Version: v3
    Serial Number:0x14
    Signature Algorithm:SHAwithRSA - 1.2.840.113549.1.1.4
    Issuer:CN=CA server,OU=PKI,O=Cisco Systems
    Validity:
      Not Before:Thursday, August 8, 2002 4:38:05 PM PST
      Not After:Tuesday, August 7, 2003 4:38:05 PM PST
    Subject:CN=OCSP server,OU=PKI,O=Cisco Systems
    Subject Public Key Info:
      Algorithm:RSA - 1.2.840.113549.1.1.1
      Public Key:
        Exponent:65537
        Public Key Modulus:(2048 bits) :
          <snip>
```

```

Extensions:
  Identifier:Subject Key Identifier - 2.5.29.14
    Critical:no
    Key Identifier:
      <snip>
  Identifier:Authority Key Identifier - 2.5.29.35
    Critical:no
    Key Identifier:
      <snip>
!
  Identifier:OCSP NoCheck:- 1.3.6.1.5.5.7.48.1.5
    Critical:no
  Identifier:Extended Key Usage:- 2.5.29.37
    Critical:no
    Extended Key Usage:
      OCSPSigning
!

  Identifier:CRL Distribution Points - 2.5.29.31
    Critical:no
    Number of Points:1
    Point 0
      Distribution Point:
[URIName:ldap://CA-server/CN=CA server,OU=PKI,O=Cisco Systems]
  Signature:
    Algorithm:SHAwithRSA - 1.2.840.113549.1.1.4
  Signature:
    <snip>

```

次の例は、既存のシーケンスの先頭に **match certificate override oosp** コマンドを追加したときの実行コンフィギュレーション出力の抜粋を示します。

```

match certificate map3 override oosp 5 url http://192.0.2.3/
show running-configuration
.
.
.
      match certificate map3 override oosp 5 url http://192.0.2.3/
      match certificate map1 override oosp 10 url http://192.0.2.1/
      match certificate map2 override oosp 15 url http://192.0.2.2/

```

次の例は、既存の **match certificate override oosp** コマンドが置き換えられ、トラストポイントが代替のPKI階層を使用するように指定された場合の、実行コンフィギュレーション出力の抜粋を示します。

```

match certificate map4 override oosp trustpoint tp4 10 url http://192.0.2.4/newvalue
show running-configuration
.
.
.
      match certificate map3 override oosp trustpoint tp3 5 url http://192.0.2.3/
      match certificate map1 override oosp trustpoint tp1 10 url http://192.0.2.1/
      match certificate map4 override oosp trustpoint tp4 10 url
http://192.0.2.4/newvalue
      match certificate map2 override oosp trustpoint tp2 15 url http://192.0.2.2/

```

## トラブルシューティングのヒント

失効チェックまたは失効した証明書を無視した場合は、慎重に設定を確認する必要があります。証明書マップが、当該の証明書または許可する証明書、あるいはスキップするAAAチェッ

クのいずれかと適切に一致していることを確認してください。管理された環境で、証明書マップを変更して想定どおりに機能していないものを判別します。

## 証明書チェーンの設定

ピア証明書の証明書チェーンパスに処理レベルを設定するには、次の作業を実行します。

### 始める前に

- デバイスを PKI 階層に登録する必要があります。
- 適切なキーペアを証明書に関連付ける必要があります。



- (注)
- ルート CA に関連付けられたトラストポイントは、次のレベルに対して有効になるように設定できません。

**chain-validation** コマンドは、ルート CA に関連付けられたトラストポイント用に **continue** キーワードを指定して設定します。エラーメッセージが表示され、チェーン検証はデフォルトの **chain-validation** コマンド設定に戻ります。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki trustpointname**
4. **chain-validation** [{stop | continue} [parent-trustpoint]]
5. **exit**

### 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Device> enable	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	<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 3	<b>crypto pki trustpointname</b> 例： Device(config)# crypto pki trustpoint ca-sub1	トラストポイントおよび設定された名前を宣言して、CA 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。

	コマンドまたはアクション	目的
ステップ 4	<b>chain-validation</b> [{stop   continue} [parent-trustpoint]] 例： <pre>Device(ca-trustpoint)# chain-validation continue ca-sub1</pre>	証明書チェーンが、すべての証明書（下位 CA 証明書を含む）で処理されるレベルを設定します。 <ul style="list-style-type: none"> <li>• <b>stop</b> キーワードを使用して、証明書がすでに信頼できることを明示します。これがデフォルトの設定です。</li> <li>• <b>continue</b> キーワードを使用して、トラストポイントに関連付けられた下位 CA 証明書を有効にする必要があることを明示します。</li> <li>• <b>parent-trustpoint</b> 引数は、証明書を照合する必要がある親トラストポイント名を指定します。</li> </ul>
ステップ 5	<b>exit</b> 例： <pre>Device(ca-trustpoint)# exit</pre>	グローバル コンフィギュレーション モードに戻ります。

## 証明書の許可および失効の設定例

### PKI AAA 許可の設定および確認の例

ここでは、PKI AAA 認可の設定例を示します。

例：ルータ設定

次の **show running-config** コマンド出力は、AAA サーバー機能との PKI 統合を使用して、VPN 接続を許可するように設定されたルータの動作設定を示します。

```
Device#show running-config

Building configuration...
!
version 12.3
!
hostname router7200router7200
!
aaa new-model
!
!
aaa authentication login default group tacacs+
aaa authentication login no_tacacs enable
aaa authentication ppp default group tacacs+
aaa authorization exec ACSLab group tacacs+
aaa authorization network ACSLab group tacacs+
aaa accounting exec ACSLab start-stop group tacacs+
aaa accounting network default start-stop group ACSLab
aaa session-id common
!
```

```

ip domain name example.com
!
crypto pki trustpoint EM-CERT-SERV
enrollment url http://192.0.2.33:80
serial-number
crl optional
rsakeypair STOREVPN 2048
auto-enroll
authorization list ACSLab
!
crypto pki certificate chain EM-CERT-SERV
certificate 04
 30820214 3082017D A0030201 02020104 300D0609 2A864886 F70D0101 04050030
17311530 13060355 0403130C 454D2D43 4552542D 53455256 301E170D 30343031
31393232 30323535 5A170D30 35303131 38323230 3235355A 3030312E 300E0603
55040513 07314437 45424434 301C0609 2A864886 F70D0109 02160F37 3230302D
312E6772 696C2E63 6F6D3081 9F300D06 092A8648 86F70D01 01010500 03818D00
30818902 818100BD F3B837AA D925F391 2B64DA14 9C2EA031 5A7203C4 92F8D6A8
7D2357A6 BCC8596F A38A9B10 47435626 D59A8F2A 123195BB BE5A1E74 B1AA5AE0
5CA162FF 8C3ACA4F B3EE9F27 8B031642 B618AE1B 40F2E3B4 F996BEFE 382C7283
3792A369 236F8561 8748AA3F BC41F012 B859BD9C DB4F75EE 3CEE2829 704BD68F
FD904043 0F555702 03010001 A3573055 30250603 551D1F04 1E301C30 1AA018A0
16861468 7474703A 2F2F3633 2E323437 2E313037 2E393330 0B060355 1D0F0404
030205A0 301F0603 551D2304 18301680 1420FC4B CF0B1C56 F5BD4C06 0AFD4E67
341AE612 D1300D06 092A8648 86F70D01 01040500 03818100 79E97018 FB955108
12F42A56 2A6384BC AC8E22FE F1D6187F DA5D6737 C0E241AC AAAEC75D 3C743F59
08DEEFF2 0E813A73 D79E0FA9 D62DC20D 8E2798CD 2C1DC3EC 3B2505A1 3897330C
15A60D5A 8A13F06D 51043D37 E56E45DF A65F43D7 4E836093 9689784D C45FD61D
EC1F160C 1ABC8D03 49FB11B1 DA0BED6C 463E1090 F34C59E4
quit
certificate ca 01
30820207 30820170 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
17311530 13060355 0403130C 454D2D43 4552542D 53455256 301E170D 30333132
31363231 34373432 5A170D30 36313231 35323134 3734325A 30173115 30130603
55040313 0C454D2D 43455254 2D534552 5630819F 300D0609 2A864886 F70D0101
01050003 818D0030 81890281 8100C14D 833641CF D784F516 DA6B50C0 7B3CB3C9
589223AB 99A7DC14 04F74EF2 AAEE8F5 E3BFAE97 F2F980F7 D889E6A1 2C726C69
54A29870 7E7363FF 3CD1F991 F5A37CFF 3FFDD3D0 9E486C44 A2E34595 C2D078B8
E9DE981E B733B868 AA8916C0 A8048607 D34B83C0 64BDC101 161FC103 13C06500
22D6EE75 7D6CF133 7F1B515F 32830203 010001A3 63306130 0F060355 1D130101
FF040530 030101FF 300E0603 551D0F01 01FF0404 03020186 301D0603 551D0E04
16041420 FC4BCF0B 1C56F5BD 4C060AFD 4E67341A E612D130 1F060355 1D230418
30168014 20FC4BCF 0B1C56F5 BD4C060A FD4E6734 1AE612D1 300D0609 2A864886
F70D0101 04050003 81810085 D2E386F5 4107116B AD3AC990 CBE84063 5FB2A6B5
BD572026 528E92ED 02F3A0AE 1803F2AE AA4C0ED2 0F59F18D 7B50264F 30442C41
0AF19C4E 70BD3CB5 0ADD8DE8 8EF636BD 24410DF4 DB62DAFC 67DA6E58 3879AA3E
12AFB1C3 2E27CB27 EC74E1FC AEE2F5CF AA80B439 615AA8D5 6D6DEDC3 7F9C2C79
3963E363 F2989FB9 795BA8
quit
!
!
crypto isakmp policy 10
  encr aes
  group 14
!
!
crypto ipsec transform-set ISC_TS_1 esp-aes esp-sha-hmac
!
crypto ipsec profile ISC_IPSEC_PROFILE_2
  set security-association lifetime kilobytes 53000000
  set security-association lifetime seconds 14400
  set transform-set ISC_TS_1
!
!

```

## 例：成功した PKI AAA 許可のデバッグ

```

controller ISA 1/1
!
!
interface Tunnel0
  description MGRE Interface provisioned by ISC
  bandwidth 10000
  ip address 192.0.2.172 255.255.255.0
  no ip redirects
  ip mtu 1408
  ip nhrp map multicast dynamic
  ip nhrp network-id 101
  ip nhrp holdtime 500
  ip nhrp server-only
  no ip split-horizon eigrp 101
  tunnel source FastEthernet2/1
  tunnel mode gre multipoint
  tunnel key 101
  tunnel protection ipsec profile ISC_IPSEC_PROFILE_2
!
interface FastEthernet2/0
  ip address 192.0.2.1 255.255.255.0
  duplex auto
  speed auto
!
interface FastEthernet2/1
  ip address 192.0.2.2 255.255.255.0
  duplex auto
  speed auto
!
!
tacacs-server host 192.0.2.55 single-connection
tacacs-server directed-request
tacacs-server key company lab
!
ntp master 1
!
end

```

## 例：成功した PKI AAA 許可のデバッグ

次の **show debugging** コマンド出力は、AAA サーバー機能との PKI 統合を使用して、成功した許可を示します。

```

Device#show debugging

General OS:
  TACACS access control debugging is on
  AAA Authentication debugging is on
  AAA Authorization debugging is on
Cryptographic Subsystem:
  Crypto PKI Trans debugging is on
Device#
May 28 19:36:11.117: CRYPTO_PKI: Trust-Point EM-CERT-SERV picked up
May 28 19:36:12.789: CRYPTO_PKI: Found a issuer match
May 28 19:36:12.805: CRYPTO_PKI: cert revocation status unknown.
May 28 19:36:12.805: CRYPTO_PKI: Certificate validated without revocation check
May 28 19:36:12.813: CRYPTO_PKI_AAA: checking AAA authorization (ACSLab, POD5.example.com,
<all>)
May 28 19:36:12.813: AAA/BIND(00000042): Bind i/f
May 28 19:36:12.813: AAA/AUTHOR (0x42): Pick method list 'ACSLab'
May 28 19:36:12.813: TPLUS: Queuing AAA Authorization request 66 for processing
May 28 19:36:12.813: TPLUS: processing authorization request id 66
May 28 19:36:12.813: TPLUS: Protocol set to None .....Skipping

```

```

May 28 19:36:12.813: TPLUS: Sending AV service=pki
May 28 19:36:12.813: TPLUS: Authorization request created for 66(POD5.example.com)
May 28 19:36:12.813: TPLUS: Using server 192.0.2.55
May 28 19:36:12.813: TPLUS(00000042)/0/NB_WAIT/203A4628: Started 5 sec timeout
May 28 19:36:12.813: TPLUS(00000042)/0/NB_WAIT: wrote entire 46 bytes request
May 28 19:36:12.813: TPLUS: Would block while reading pak header
May 28 19:36:12.817: TPLUS(00000042)/0/READ: read entire 12 header bytes (expect 27
bytes)
May 28 19:36:12.817: TPLUS(00000042)/0/READ: read entire 39 bytes response
May 28 19:36:12.817: TPLUS(00000042)/0/203A4628: Processing the reply packet
May 28 19:36:12.817: TPLUS: Processed AV cert-application=all
May 28 19:36:12.817: TPLUS: received authorization response for 66: PASS
May 28 19:36:12.817: CRYPTO_PKI_AAA: reply attribute ("cert-application" = "all")
May 28 19:36:12.817: CRYPTO_PKI_AAA: authorization passed
Device#
Device#
May 28 19:36:18.681: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 101: Neighbor 192.0.2.171 (Tunnel0)
is up: new adjacency
Device#
Device# show crypto isakmp sa
dst          src          state          conn-id slot
192.0.2.22   192.0.2.102  QM_IDLE        84         0

```

### 例：失敗した PKI AAA 許可のデバッグ

次の **show debugging** コマンド出力は、ルータが、VPN を使用しての接続を許可されていないことを示します。このメッセージは、このような状況で表示される典型的なメッセージです。

この例においてピア ユーザ名は、Cisco Secure ACS の VPN\_Router\_Disabled と呼ばれる Cisco Secure ACS グループに移動することにより、許可されていないものとして設定されました。ルータ (router7200.example.com) は、任意のピアに VPN 接続を確立する前に、Cisco Secure ACS AAA サーバに確認するように設定されています。

```

Device#show debugging

General OS:
  TACACS access control debugging is on
  AAA Authentication debugging is on
  AAA Authorization debugging is on
Cryptographic Subsystem:
  Crypto PKI Trans debugging is on

Device#
May 28 19:48:29.837: CRYPTO_PKI: Trust-Point EM-CERT-SERV picked up
May 28 19:48:31.509: CRYPTO_PKI: Found a issuer match
May 28 19:48:31.525: CRYPTO_PKI: cert revocation status unknown.
May 28 19:48:31.525: CRYPTO_PKI: Certificate validated without revocation check
May 28 19:48:31.533: CRYPTO_PKI_AAA: checking AAA authorization (ACSLab, POD5.example.com,
<all>)
May 28 19:48:31.533: AAA/BIND(00000044): Bind i/f
May 28 19:48:31.533: AAA/AUTHOR (0x44): Pick method list 'ACSLab'
May 28 19:48:31.533: TPLUS: Queuing AAA Authorization request 68 for processing
May 28 19:48:31.533: TPLUS: processing authorization request id 68
May 28 19:48:31.533: TPLUS: Protocol set to None .....Skipping
May 28 19:48:31.533: TPLUS: Sending AV service=pki
May 28 19:48:31.533: TPLUS: Authorization request created for 68(POD5.example.com)
May 28 19:48:31.533: TPLUS: Using server 192.0.2.55
May 28 19:48:31.533: TPLUS(00000044)/0/NB_WAIT/203A4C50: Started 5 sec timeout
May 28 19:48:31.533: TPLUS(00000044)/0/NB_WAIT: wrote entire 46 bytes request
May 28 19:48:31.533: TPLUS: Would block while reading pak header
May 28 19:48:31.537: TPLUS(00000044)/0/READ: read entire 12 header bytes (expect 6 bytes)

```

## 例：失効メカニズムの設定

```

May 28 19:48:31.537: TPLUS(00000044)/0/READ: read entire 18 bytes response
May 28 19:48:31.537: TPLUS(00000044)/0/203A4C50: Processing the reply packet
May 28 19:48:31.537: TPLUS: received authorization response for 68: FAIL
May 28 19:48:31.537: CRYPTO_PKI_AAA: authorization declined by AAA, or AAA server not
found.
May 28 19:48:31.537: CRYPTO_PKI_AAA: No cert-application attribute found. Failing.
May 28 19:48:31.537: CRYPTO_PKI_AAA: authorization failed
May 28 19:48:31.537: CRYPTO_PKI: AAA authorization for list 'ACSLab', and user
'POD5.example.com' failed.
May 28 19:48:31.537: %CRYPTO-5-IKMP_INVALID_CERT: Certificate received from 192.0.2.162
is bad: certificate invalid
May 28 19:48:39.821: CRYPTO_PKI: Trust-Point EM-CERT-SERV picked up
May 28 19:48:41.481: CRYPTO_PKI: Found a issuer match
May 28 19:48:41.501: CRYPTO_PKI: cert revocation status unknown.
May 28 19:48:41.501: CRYPTO_PKI: Certificate validated without revocation check
May 28 19:48:41.505: CRYPTO_PKI_AAA: checking AAA authorization (ACSLab, POD5.example.com,
<all>)
May 28 19:48:41.505: AAA/BIND(00000045): Bind i/f
May 28 19:48:41.505: AAA/AUTHOR (0x45): Pick method list 'ACSLab'
May 28 19:48:41.505: TPLUS: Queuing AAA Authorization request 69 for processing
May 28 19:48:41.505: TPLUS: processing authorization request id 69
May 28 19:48:41.505: TPLUS: Protocol set to None .....Skipping
May 28 19:48:41.505: TPLUS: Sending AV service=pki
May 28 19:48:41.505: TPLUS: Authorization request created for 69(POD5.example.com)
May 28 19:48:41.505: TPLUS: Using server 198.168.244.55
May 28 19:48:41.509: TPLUS(00000045)/0/IDLE/63B22834: got immediate connect on new 0
May 28 19:48:41.509: TPLUS(00000045)/0/WRITE/63B22834: Started 5 sec timeout
May 28 19:48:41.509: TPLUS(00000045)/0/WRITE: wrote entire 46 bytes request
May 28 19:48:41.509: TPLUS(00000045)/0/READ: read entire 12 header bytes (expect 6 bytes)
May 28 19:48:41.509: TPLUS(00000045)/0/READ: read entire 18 bytes response
May 28 19:48:41.509: TPLUS(00000045)/0/63B22834: Processing the reply packet
May 28 19:48:41.509: TPLUS: received authorization response for 69: FAIL
May 28 19:48:41.509: CRYPTO_PKI_AAA: authorization declined by AAA, or AAA server not
found.
May 28 19:48:41.509: CRYPTO_PKI_AAA: No cert-application attribute found. Failing.
May 28 19:48:41.509: CRYPTO_PKI_AAA: authorization failed
May 28 19:48:41.509: CRYPTO_PKI: AAA authorization for list 'ACSLab', and user
'POD5.example.com' failed.
May 28 19:48:41.509: %CRYPTO-5-IKMP_INVALID_CERT: Certificate received from 192.0.2.162
is bad: certificate invalid
Device#
Device# show crypto iskmp sa
dst          src          state          conn-id slot
192.0.2.2    192.0.2.102 MM_KEY_EXCH    95      0

```

## 例：失効メカニズムの設定

ここでは、PKIの失効メカニズムを指定する際に使用できる設定例を示します。

## 例：OCSPサーバーの設定

次の例では、証明書のAIA拡張部で指定されたOCSPサーバーを使用するようにルータを設定する方法を示します。

```

Device(config)#crypto pki trustpoint mytp
Device(ca-trustpoint)#revocation-check ocsf

```



### 例：CRL の指定後の OCSP サーバーの指定

次の例では、CRL を CDP からダウンロードするようにルータを設定する方法を示します。CRL を利用できない場合は、証明書の AIA 拡張部で指定される OCSP サーバーが使用されます。両方のオプションが失敗した場合、証明書の検証も失敗します。

```
Device(config)#crypto pki trustpoint mytp
Device(ca-trustpoint)#revocation-check crl ocsf
```

### 例：OCSP サーバーの指定

以下に、HTTP URL 「http://myocspserver:81」にある OCSP サーバーを使用するようにルータを設定する例を示します。このサーバーがダウンしている場合は、失効チェックは行われません。

```
Device(config)# crypto pki trustpoint mytp
Device(ca-trustpoint)# ocsf url http://myocspserver:81
Device(ca-trustpoint)# revocation-check ocsf none
```

### 例：OCSP サーバーとの通信でのナンスの無効化

次の例は、OCSP 要求に関するナンス（固有識別情報）が、OCSP サーバーとの通信でディセーブルになっている場合の通信を示します。

```
Device(config)# crypto pki trustpoint mytp
Device(ca-trustpoint)# ocsf url http://myocspserver:81
Device(ca-trustpoint)# revocation-check ocsf none
Device(ca-trustpoint)# ocsf disable-nonce
```

### 例：証明書失効チェック用に中央サイトでハブルータを構成する

次の例では、複数のブランチ オフィスにセントラルサイトへの接続を提供しているセントラルサイトにあるハブルータを示します。

ブランチ オフィスも追加の IPSec トンネルを使用して、ブランチ オフィス間で直接相互に通信できます。

CA は、セントラルサイトにある HTTP サーバーの CRL を公開します。セントラルサイトは、各ピアと IPSec トンネルを設定する場合、そのピアの CRL をチェックします。

次の例では、IPSec 設定を示しません。PKI 関連の設定だけを示します。

#### ホーム オフィスのハブ設定

```
crypto pki trustpoint VPN-GW
enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
serial-number none
fqdn none
ip-address none
subject-name o=Home Office Inc,cn=Central VPN Gateway
revocation-check crl
```

例：証明書失効チェック用に中央サイトでハブルータを構成する

## セントラルサイトのハブルータ

```
Device# show crypto ca certificate
Certificate
  Status: Available
  Certificate Serial Number: 2F62BE14000000000CA0
  Certificate Usage: General Purpose
  Issuer:
    cn=Central Certificate Authority
    o=Home Office Inc
  Subject:
    Name: Central VPN Gateway
    cn=Central VPN Gateway
    o=Home Office Inc
  CRL Distribution Points:
    http://ca.home-office.com/CertEnroll/home-office.crl
  Validity Date:
    start date: 00:43:26 GMT Sep 26 2003
    end   date: 00:53:26 GMT Sep 26 2004
    renew date: 00:00:00 GMT Jan 1 1970
  Associated Trustpoints: VPN-GW
CA Certificate
  Status: Available
  Certificate Serial Number: 1244325DE0369880465F977A18F61CA8
  Certificate Usage: Signature
  Issuer:
    cn=Central Certificate Authority
    o=Home Office Inc
  Subject:
    cn=Central Certificate Authority
    o=Home Office Inc
  CRL Distribution Points:
    http://ca.home-office.com/CertEnroll/home-office.crl
  Validity Date:
    start date: 22:19:29 GMT Oct 31 2002
    end   date: 22:27:27 GMT Oct 31 2017
  Associated Trustpoints: VPN-GW
```

## ブランチオフィスルータのトラストポイント

```
crypto pki trustpoint home-office
  enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
  serial-number none
  fqdn none

ip-address none
  subject-name o=Home Office Inc,cn=Branch 1
  revocation-check crl
```

証明書マップがブランチ オフィス ルータに入力されます。

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
branch1(config)# crypto pki certificate map central-site 10
branch1(ca-certificate-map)#
```

セントラルサイトのハブルータ上で発行された **show certificate** コマンドの出力では、証明書が以下によって発行されたことを示しています。

```
cn=Central Certificate Authority
o=Home Office Inc
```

この2行は、行を区切るためのカンマ (,) を使用して1行に結合され、元の2行が最初の一致基準として追加されています。

```
Device(ca-certificate-map)# issuer-name co cn=Central Certificate Authority, ou=Home
Office Inc
!The above line wrapped but should be shown on one line with the line above it.
```

セントラル サイト ルータの証明書の所有者名についても、同じように組み合わせられています（「Name:」で始まる行は、所有者名の一部ではなく、証明書マップ基準を作成する際に無視する必要があることに注意してください）。これが証明書マップで使用されるサブジェクト名です。

```
cn=Central VPN Gateway
o=Home Office Inc
```

```
Device(ca-certificate-map)# subject-name eq cn=central vpn gateway, o=home office inc
```

これで、以前に設定された証明書マップがトラストポイントに追加されます。

```
Device(ca-certificate-map)# crypto pki trustpoint home-office
Device(ca-trustpoint)# match certificate central-site skip revocation-check
Device(ca-trustpoint)# exit
Device(config)# exit
```

設定がチェックされます（大部分の設定は示されていません）。

```
Device# write term
!Many lines left out
.
.
.
crypto pki trustpoint home-office
  enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
  serial-number none
  fqdn none
  ip-address none
  subject-name o=Home Office Inc,cn=Branch 1
  revocation-check crl
  match certificate central-site skip revocation-check
!
!
crypto pki certificate map central-site 10
  issuer-name co cn = Central Certificate Authority, ou = Home Office Inc
  subject-name eq cn = central vpn gateway, o = home office inc
!many lines left out
```

今後のピアの証明書との照合のために、発行者名の行とサブジェクト名の行が矛盾しないように再フォーマットされていることに注意してください。

ブランチ オフィスが AAA をチェックする場合は、トラストポイントには次のような行があります。

```
crypto pki trustpoint home-office
```

例：証明書失効チェック用に中央サイトでハブルータを構成する

```
auth list allow_list
auth user subj commonname
```

証明書マップが上記のように定義されると、次のコマンドがトラストポイントに追加され、セントラルサイトハブの AAA チェックがスキップされます。

```
match certificate central-site skip authorization-check
```

両方のケースにおいてブランチサイトルータは、CRL のチェックまたは AAA サーバと通信するために、セントラルサイトに IPSec トンネルを確立する必要があります。ただし、**match certificate** コマンドと **central-site skip authorization-check (argument and keyword)** を使用しないと、ブランチオフィスが CRL または AAA サーバを確認するまで、トンネルを確立することはできません (**match certificate** コマンドと **central-site skip authorization-check** 引数およびキーワードを使用しない限り、トンネルは確立されません)。

ブランチサイトにあるデバイスの証明書が失効していて、その証明書を更新するためにセントラルサイトにトンネルを確立する必要がある場合、セントラルサイトで **match certificate** コマンドと **allow expired-certificate** キーワードを使用できます。

### セントラルサイトルータのトラストポイント

```
crypto pki trustpoint VPN-GW
enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
serial-number none
fqdn none
ip-address none
subject-name o=Home Office Inc,cn=Central VPN Gateway
revocation-check crl
```

### ブランチ 1 サイトルータのトラストポイント

```
Device# show crypto ca certificate
Certificate
  Status: Available
  Certificate Serial Number: 2F62BE1400000000CA0
  Certificate Usage: General Purpose
  Issuer:
    cn=Central Certificate Authority
    o=Home Office Inc
  Subject:
    Name: Branch 1 Site
    cn=Branch 1 Site
    o=Home Office Inc
  CRL Distribution Points:
    http://ca.home-office.com/CertEnroll/home-office.crl
  Validity Date:
    start date: 00:43:26 GMT Sep 26 2003
    end date: 00:53:26 GMT Oct 3 2003
    renew date: 00:00:00 GMT Jan 1 1970
  Associated Trustpoints: home-office
CA Certificate
  Status: Available
  Certificate Serial Number: 1244325DE0369880465F977A18F61CA8
  Certificate Usage: Signature
  Issuer:
    cn=Central Certificate Authority
    o=Home Office Inc
```

```

Subject:
  cn=Central Certificate Authority
  o=Home Office Inc
CRL Distribution Points:
  http://ca.home-office.com/CertEnroll/home-office.crl
Validity Date:
  start date: 22:19:29 GMT Oct 31 2002
  end   date: 22:27:27 GMT Oct 31 2017
Associated Trustpoints: home-office

```

証明書マップがセントラル サイト ルータに入力されます。

```

Device# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Device(config)# crypto pki certificate map branch1 10
Device(ca-certificate-map)# issuer-name co cn=Central Certificate Authority, ou=Home Office Inc
!The above line wrapped but should be part of the line above it.
Device(ca-certificate-map)# subject-name eq cn=Brahcn 1 Site,o=home office inc

```

証明書マップがトラストポイントに追加されます。

```

Device(ca-certificate-map)# crypto pki trustpoint VPN-GW
Device(ca-trustpoint)# match certificate branch1 allow expired-certificate
Device(ca-trustpoint)# exit
Router (config) #exit

```

設定がチェックされます（設定の大部分は示されていません）。

```

Device# write term
!many lines left out
crypto pki trustpoint VPN-GW
  enrollment url http://ca.home-office.com:80/certsrv/mscep/mscep.dll
  serial-number none
  fqdn none
  ip-address none
  subject-name o=Home Office Inc,cn=Central VPN Gateway
  revocation-check crl
  match certificate branch1 allow expired-certificate
!
!
crypto pki certificate map central-site 10
  issuer-name co cn = Central Certificate Authority, ou = Home Office Inc
  subject-name eq cn = central vpn gateway, o = home office inc
! many lines left out

```

**match certificate** コマンド、**branch1 allow expired-certificate**（引数とキーワード）および証明書マップは、ブランチルータが新しい証明書を取得した後すぐに削除する必要があります。

## 例：証明書の許可および失効の設定

この項では、CRL キャッシュ コントロールの設定または証明書のシリアル番号セッション コントロールを指定する場合に使用する設定例を示します。

### CRL キャッシュ コントロールの設定

次の例では、CA1 トラストポイントに関連付けられたすべての CRL の CRL キャッシングをディセーブルにする方法を示します。

```
crypto pki trustpoint CA1
enrollment url http://CA1:80
ip-address FastEthernet0/0
crl query ldap://ldap_CA1
revocation-check crl
crl-cache none
```

上記の例の設定を実行した直後は、まだ現在の CRL がキャッシュされています。

#### Device# show crypto pki crls

```
CRL Issuer Name:
cn=name Cert Manager,ou=pki,o=example.com,c=US
LastUpdate: 18:57:42 GMT Nov 26 2005
NextUpdate: 22:57:42 GMT Nov 26 2005
Retrieved from CRL Distribution Point:
ldap://ldap.example.com/CN=name Cert Manager,O=example.com
```

現在の CRL が失効すると、次の更新時に新しい CRL がルータにダウンロードされます。**crl-cache none** コマンドが有効になり、トラストポイントの CRL はすべてキャッシュされなくなります。また、キャッシュは無効になります。**show crypto pki crls** コマンドを実行して、CRL がキャッシュされていないことを確認できます。キャッシュされている CRL がないため、出力は表示されません。

次の例では、CA1 トラストポイントに関連付けられたすべての CRL に 2 分の最大ライフタイムを設定する方法を示します。

```
crypto pki trustpoint CA1
enrollment url http://CA1:80
ip-address FastEthernet0/0
crl query ldap://ldap_CA1
revocation-check crl
crl-cache delete-after 2
```

CRL の最大ライフタイムを設定するために上記例の設定を実行した直後でも、依然現在の CRL がキャッシュされます。

#### Device# show crypto pki crls

```
CRL Issuer Name:
cn=name Cert Manager,ou=pki,o=example.com,c=US
LastUpdate: 18:57:42 GMT Nov 26 2005
NextUpdate: 22:57:42 GMT Nov 26 2005
Retrieved from CRL Distribution Point:
ldap://ldap.example.com/CN=name Cert Manager,O=example.com
When the current CRL expires, a new CRL is downloaded to the router at the next update
and the crl-cache delete-after
command takes effect. This newly cached CRL and all subsequent CRLs will be deleted after
a maximum lifetime of 2 minutes.
You can verify that the CRL will be cached for 2 minutes by executing the show crypto
pki crls
command. Note that the NextUpdate time is 2 minutes after the LastUpdate time.
```

#### Device# show crypto pki crls

```
CRL Issuer Name:
cn=name Cert Manager,ou=pki,o=example.com,c=US
LastUpdate: 22:57:42 GMT Nov 26 2005
```

```
NextUpdate: 22:59:42 GMT Nov 26 2005
Retrieved from CRL Distribution Point:
```

```
ldap://ldap.example.com/CN=name Cert Manager,O=example.com
```

## 証明書のシリアル番号セッションコントロールの設定

次の例では、CA1 トラストポイントの証明書マップを使用した証明書のシリアル番号セッションコントロールの設定を示します。

```
crypto pki trustpoint CA1
  enrollment url http://CA1
  chain-validation stop
  crl query ldap://ldap_server
  revocation-check crl
  match certificate crl
!
crypto pki certificate map crl 10
  serial-number co 279d
```



- (注) *match-criteria* 値が **co** (含む) ではなく **eq** (等しい) に設定されている場合、シリアル番号はスペースを含めて、証明書マップのシリアル番号に正確に一致する必要があります。

次の例では、AAA 属性を使用した証明書のシリアル番号セッションコントロールの設定を示します。この場合、証明書にシリアル番号「4ACA」がなければ、有効な証明書はすべて受け入れられません。

```
crypto pki trustpoint CA1
  enrollment url http://CA1
  ip-address FastEthernet0/0
  crl query ldap://ldap_CA1
  revocation-check crl
  aaa new-model
!
aaa attribute list crl
attribute-type aaa-cert-serial-not 4ACA
```

サーバーログは、シリアル番号「4ACA」を持つ証明書が拒否されたことを示しています。証明書の拒否は、感嘆符で表示されます。

```
.
.
.
Dec 3 04:24:39.051: CRYPTO_PKI: Trust-Point CA1 picked up
Dec 3 04:24:39.051: CRYPTO_PKI: locked trustpoint CA1, refcount is 1
Dec 3 04:24:39.051: CRYPTO_PKI: unlocked trustpoint CA1, refcount is 0
Dec 3 04:24:39.051: CRYPTO_PKI: locked trustpoint CA1, refcount is 1
Dec 3 04:24:39.135: CRYPTO_PKI: validation path has 1 certs
Dec 3 04:24:39.135: CRYPTO_PKI: Found a issuer match
Dec 3 04:24:39.135: CRYPTO_PKI: Using CA1 to validate certificate
Dec 3 04:24:39.135: CRYPTO_PKI: Certificate validated without revocation check
Dec 3 04:24:39.135: CRYPTO_PKI: Selected AAA username: 'PKIAAA'
Dec 3 04:24:39.135: CRYPTO_PKI: Anticipate checking AAA list:'CRL'
Dec 3 04:24:39.135: CRYPTO_PKI_AAA: checking AAA authorization (CRL, PKIAAA-L1, <all>)
Dec 3 04:24:39.135: CRYPTO_PKI_AAA: pre-authorization chain validation status (0x4)
```

## 例：証明書チェーン検証の設定

```

Dec 3 04:24:39.135: AAA/BIND(00000021): Bind i/f
Dec 3 04:24:39.135: AAA/AUTHOR (0x21): Pick method list 'CRL'
.
.
.
Dec 3 04:24:39.175: CRYPTO_PKI_AAA: reply attribute ("cert-application" = "all")
Dec 3 04:24:39.175: CRYPTO_PKI_AAA: reply attribute ("cert-trustpoint" = "CA1")
!
Dec 3 04:24:39.175: CRYPTO_PKI_AAA: reply attribute ("cert-serial-not" = "4ACA")
Dec 3 04:24:39.175: CRYPTO_PKI_AAA: cert-serial doesn't match ("4ACA" != "4ACA")
!
Dec 3 04:24:39.175: CRYPTO_PKI_AAA: post-authorization chain validation status (0x7)
!
Dec 3 04:24:39.175: CRYPTO_PKI: AAA authorization for list 'CRL', and user 'PKIAAA'
failed.
Dec 3 04:24:39.175: CRYPTO_PKI: chain cert was anchored to trustpoint CA1, and chain
validation result was: CRYPTO_PKI_CERT_NOT_AUTHORIZED
!
Dec 3 04:24:39.175: %CRYPTO-5-IKMP_INVALID_CERT: Certificate received from 192.0.2.43 is
bad: certificate invalid
Dec 3 04:24:39.175: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main mode failed with
peer at 192.0.2.43
.
.
.

```

## 例：証明書チェーン検証の設定

この項では、デバイス証明書の証明書チェーン処理レベルを指定する場合に使用する設定例を示します。

## ピアからルート CA への証明書チェーン検証の設定

次の設定例では、ピア、SubCA11、SubCA1、および RootCA のすべての証明書が検証されます。

```

crypto pki trustpoint RootCA
  enrollment terminal
  chain-validation stop
  revocation-check none
  rsa-keypair RootCA
crypto pki trustpoint SubCA1
  enrollment terminal
  chain-validation continue RootCA
  revocation-check none
  rsa-keypair SubCA1
crypto pki trustpoint SubCA11
  enrollment terminal
  chain-validation continue SubCA1
  revocation-check none
  rsa-keypair SubCA11

```

## ピアから下位 CA への証明書チェーン検証の設定

次の設定例では、ピア証明書および SubCA1 証明書が有効にされます。

```

crypto pki trustpoint RootCA
  enrollment terminal
  chain-validation stop
  revocation-check none

```



```

rsa-keypair RootCA
crypto pki trustpoint SubCA1
  enrollment terminal
  chain-validation continue RootCA
  revocation-check none
rsa-keypair SubCA1
crypto pki trustpoint SubCA11
  enrollment terminal
  chain-validation continue SubCA1
  revocation-check none
rsa-keypair SubCA11

```

## 証明書チェーンの欠落確認の設定

次の設定例では、SubCA1 が、設定済みの Cisco IOS 階層にはないが、提出された証明書チェーンでピアによって提示されたと想定しています。

ピアが、提出された証明書チェーンで SubCA1 証明書を提示した場合、ピア、SubCA11、および SubCA1 の各証明書が有効になります。

ピアが、提出された証明書チェーンで SubCA1 証明書を提示しない場合、チェーンの検証は失敗します。

```

crypto pki trustpoint RootCA
  enrollment terminal
  chain-validation stop
  revocation-check none
rsa-keypair RootCA
crypto pki trustpoint SubCA11
  enrollment terminal
  chain-validation continue RootCA
  revocation-check none
rsa-keypair SubCA11

```

## PKI での証明書の許可および失効の追加リファレンス

### シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカルサポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	<a href="https://www.cisco.com/cisco/web/support/index.html">https://www.cisco.com/cisco/web/support/index.html</a>

## PKI での証明書の許可および失効の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
	PKIでの証明書の許可および失効	証明書には、指定された処理の実行をデバイスまたはユーザーが許可されているかどうかの判別を使用されるフィールドがいくつか含まれています。また、証明書ベース ACL は失効、許可、またはトラストポイントなどの PKI コンポーネントを使用するタイミングを判別するのに役立ちます。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。

## 翻訳について

このドキュメントは、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。