Cisco Catalyst IE3x00 および IE3100 高耐久性、IE3400 Heavy Duty、ESS3300 シリーズ スイッチ セキュリティ コンフィギュレーション ガイド

最終更新：2024 年 8 月 8 日

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

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

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

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

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

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

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

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

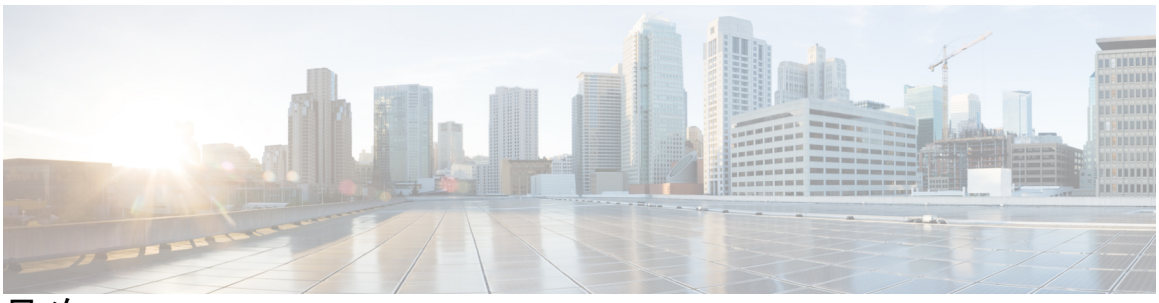
All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

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

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

© 2020–2024 Cisco Systems, Inc. All rights reserved.

注：この製品のマニュアルセットは、偏向のない言語を使用するように配慮されています。このドキュメントセットでの偏向のない言語とは、年齢、障害、性別、人種的アイデンティティ、民族的アイデンティティ、性的指向、社会経済的地位、およびインターセクショナリティに基づく差別を意味しない言語として定義されています。製品ソフトウェアのユーザインターフェイスにハードコードされている言語、RFPのドキュメントに基づいて使用されている言語、または参照されているサードパーティ製品で使用されている言語によりドキュメントに例外が存在する場合があります。



目 次

Full Cisco Trademarks with Software License ?

iii

第 1 章

RADIUS の設定 1

RADIUS を設定するための前提条件 1

RADIUS の設定に関する制約事項 2

RADIUS に関する情報 3

RADIUS およびスイッチ アクセス 3

RADIUS の概要 3

RADIUS の動作 4

RADIUS 許可の変更 5

Change-of-Authorization 要求 7

CoA 要求応答コード 8

CoA 要求コマンド 9

RADIUS のデフォルト設定 12

RADIUS サーバ ホスト 12

RADIUS ログイン認証 13

AAA サーバグループ 13

AAA 許可 14

RADIUS アカウンティング 14

ベンダー固有の RADIUS 属性 14

ベンダー独自仕様の RADIUS サーバ通信 29

RADIUS パケットの DSCP マーキング 29
RADIUS の設定 30
RADIUS サーバ ホストの識別 30
RADIUS ログイン認証の設定 32
AAA サーバ グループの定義 35
ユーザー特権アクセスおよびネットワークサービスに関する RADIUS 許可の設定 36
RADIUS アカウンティングの起動 37
すべての RADIUS サーバの設定 38
ベンダー固有の RADIUS 属性を使用するデバイスの設定 40
ベンダー独自仕様の RADIUS サーバ通信に関するデバイスの設定 40
RADIUS サーバーでの DSCP マーキングの設定 42
RADIUS サーバーグループでの送信元インターフェイスと DSCP マーキングの設定 43
デバイス上での CoA の設定 45
CoA 機能のモニタリング 47
RADIUS の機能の履歴 48

第 2 章 **無遅延 IPDT** 49
無遅延 IPDT について 49
注意事項と制約事項 50
IPDT の設定例 50
IPDT の確認 51
機能の履歴 51

第 3 章 **IPv6 ファースト ホップ セキュリティの設定** 53
IPv6 でのファースト ホップ セキュリティの前提条件 53
IPv6 でのファースト ホップ セキュリティの制約事項 53
IPv6 でのファースト ホップ セキュリティに関する情報 54
IPv6 スヌーピング ポリシーの設定方法 56
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 58
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 60

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 61
IPv6 バインディング テーブルの内容を設定する方法 61
IPv6 ネイバー探索検査ポリシーの設定方法 63
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 64
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 66
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 67
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 68
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 71
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 72
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 73
IPv6 DHCP ガード ポリシーの設定方法 74
IPv6 DHCP ガード ポリシーを全体的に VLAN にアタッチする方法 76
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 77
IPv6 DHCP ガード ポリシーを全体的に VLAN にアタッチする方法 78
IPv6 ソース ガードの設定方法 79
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 80
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 81
IPv6 プレフィックス ガードの設定方法 82
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 83
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 84
IPv6 ファースト ホップ セキュリティの設定例 84
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 84
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 85

第 4 章 レイヤ 2 NAT の設定 87

レイヤ 2 ネットワークアドレス変換 87

レイヤ 2 NAT スイッチサポート 90

注意事項と制約事項 91

デフォルト設定 92

レイヤ 2 NAT の設定 92

設定の確認 93

基本的な内部から外部への通信の例 94

重複する IP アドレスの例 96

第 5 章 MACsec の暗号化 101

MACsec and the MACsec Key Agreement (MKA) Protocol 101

MKA ポリシー 102

シングルホスト モード 102

スイッチ間 MKA MACsec マストセキュアポリシー 102

ポートチャネルの MKA/MACsec 103

MACsec 暗号アナウンスメント 103

MACsec 暗号アナウンスメントに関する制約事項 104

MKA 統計情報 104

証明書ベースの MACsec 109

MACsec 暗号化の設定方法 109

制限事項と制約事項 109

MACsec 暗号化の前提条件 110

MKA および MACsec の設定 110

MACsec MKA のデフォルト設定 110

MKA-PSK：CKN 動作の変更 110

MKA ポリシーの設定 112

スイッチからホストへの MACsec の暗号化設定 113

事前共有鍵（PSK）を使用した MACsec MKA の設定 116

PSK を使用した、インターフェイスでの MACsec MKA の設定 117

証明書ベース MACsec の設定 119
証明書ベース MACsec の前提条件 120
鍵ペアの生成 120
SCEP による登録の設定 121
登録の手動設定 123
802.1x 認証の有効化と AAA の設定 126
EAP-TLS プロファイルと 802.1x クレデンシャルの設定 128
インターフェイスでの 802.1x MKA MACsec 設定の適用 129
例：スイッチ間証明書ベース MACsec 131
ポートチャネル用の MKA/MACsec の設定 135
PSK を使用したポートチャネルの MKA/MACsec の設定 135
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 136
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 137
例：PSK を使用したポートチャネルの MACsec MKA の設定 137
MACsec 暗号アナウンスメントの設定 142
セキュアアナウンスメントの MKA ポリシーの設定 142
セキュアアナウンスメントのグローバル設定（すべての MKA ポリシー） 143
インターフェイスでの EAPoL アナウンスメントの設定 144
例：MACsec 暗号アナウンスメントの設定 144

第 6 章 **Cisco Secure Cloud Analytics コネクタの設定 149**
Cisco Connector for Secure Cloud Analytics の設定 149
トラブルシューティング 151

第 7 章 **SGACL ロギングの設定 153**
SGACL ロギング 153
前提条件 155
注意事項と制約事項 155
SGACL ロギングの設定 155
機能の履歴 156

第 8 章 **Cisco TrustSec VRF 対応 SGT** 157

VRF-Aware SXP 157

VRF 対応 SGT および SGACL の IPv6 サポート 158

IPv4 と IPv6 が SGT および SGACL テーブルを共有する方法 158

SGT および SGACL スケール値 159

Cisco TrustSec VRF 対応 SGT の設定方法 160

VRF と SGT のマッピングの設定 160

Cisco TrustSec VRF 対応 SGT の設定例 161

例：VRF と SGT のマッピングの設定 161

例：ロールベース アクセス リスト コマンド 161

ACE ポート範囲 161

例：ACE ポート範囲のロールベース アクセス リスト コマンド 162

Cisco TrustSec VRF 対応 SGT の機能履歴 162

第 9 章 **Cisco Umbrella 統合** 165

Cisco Umbrella 統合の前提条件 165

Cisco Umbrella 統合の制限 166

Cisco Umbrella 統合に関する情報 167

Cisco Umbrella 統合のメリット 167

Cisco Umbrella 統合を使用したクラウドベースのセキュリティサービス 167

Cisco Umbrella クラウドによるトラフィックの処理 168

DNS パケット暗号化 169

DNSCrypt と公開鍵 170

Cisco Umbrella 統合の設定方法 171

Umbrella Connector の設定 171

Cisco Umbrella タグの登録 173

Cisco デバイスをパススルーサーバとして設定 175

Cisco Umbrella 統合の設定の確認 177

Cisco Umbrella 統合のトラブルシューティング 179

Cisco Umbrella 統合の機能情報 179

第 10 章 Network Edge Access Topology（NEAT）の設定 181

Network Edge Access Topology 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 スイッチ 181

注意事項と制約事項 183

NEAT を使用したオーセンティケータ スイッチの設定 184

NEAT を使用したサプリカント スイッチの設定 186

設定の確認 188

設定例 190

機能の履歴 191

第 11 章 Web ベース認証の設定 193

Web ベース認証について 193

Web ベース認証の概要 193

デバイスのロール 195

ホストの検出 195

セッションの作成 195

認証プロセス 196

ローカル Web 認証バナー 197

Web 認証カスタマイズ可能な Web ページ 199

ガイドライン 199

認証プロキシ Web ページの注意事項 201

その他の機能と Web ベース認証の相互作用 202

ポート セキュリティ 202

LAN ポート IP 202

ゲートウェイ IP 202

ACL 202

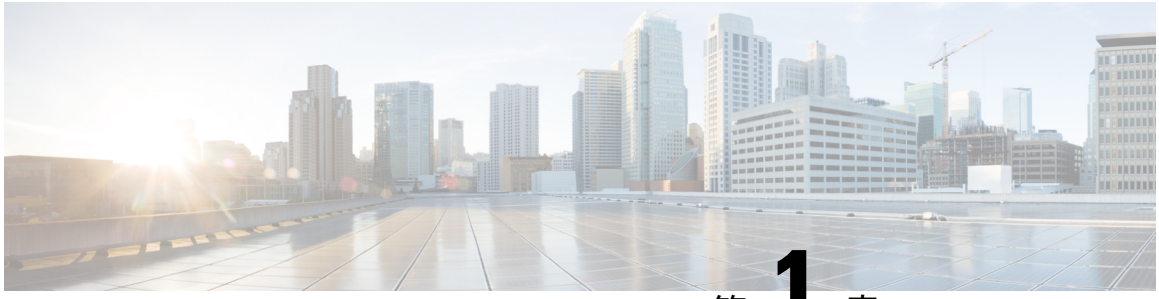
コンテキストベース アクセス コントロール 203

EtherChannel 203

Web ベース認証の設定方法 203

デフォルトの Web ベース認証の設定 203

Web ベース認証の設定に関する注意事項と制約事項 203
認証ルールとインターフェイスの設定 205
AAA 認証の設定 207
スイッチ/RADIUS サーバー間通信の設定 209
HTTP サーバーの設定 210
認証プロキシ Web ページのカスタマイズ 212
Web ベース認証パラメータの設定 213
Web ベース認証ローカル バナーの設定 214
Web ベース認証キャッシュ エントリの削除 215
Web ベース認証の確認 216
Web ベース認証に関するその他の参考資料 216



第 1 章

RADIUS の設定

- RADIUS を設定するための前提条件 （1 ページ）
- RADIUS の設定に関する制約事項 （2 ページ）
- RADIUS に関する情報 （3 ページ）
- RADIUS の設定 （30 ページ）
- CoA 機能のモニタリング （47 ページ）
- RADIUS の機能の履歴 （48 ページ）

RADIUS を設定するための前提条件

ここでは、RADIUS によるdevice 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、ならびにアカウンティング（AAA）を有効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有効にできます。
- **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 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有効にします。
- 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ティングの方式リストを定義できます。
- device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 の動作：

- ユーザーは 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（有効になっている場合）。
- RADIUS over IPv6 構成の場合、ユーザーは **ipv6 unicast-routing** コマンドを有効にして、IPv6 ユニキャストルーティングを有効にする必要があります。

RADIUS の設定に関する制約事項

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 および AAA サーバーは、標準のデフォルトポートでのみ実行するように設定できます。
  - 1812 および 1813
  - 1645 および 1646

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 パケットの DSCP マーキングサポート：

- 認証とアカウンティングの DSCP マーキングは、プライベートサーバー、完全修飾ドメイン名（FQDN）サーバー、および radsec サーバーではサポートされていません。

- 有線IEEE 802.1x認証の場合、送信元ポート拡張が有効になっていないと、デフォルトポートが使用されます。DSCP マーキングはデフォルトポートに設定され、すべての要求は同じ DSCP 値でマーキングされます。
- 送信元ポート拡張がデフォルトで有効になっている無線 IEEE 802.1x 認証の場合、DSCP マーキングはサポートされません。

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 を有効にし、設定する方法について説明します。RADIUS を使用すると、アカウンティング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。

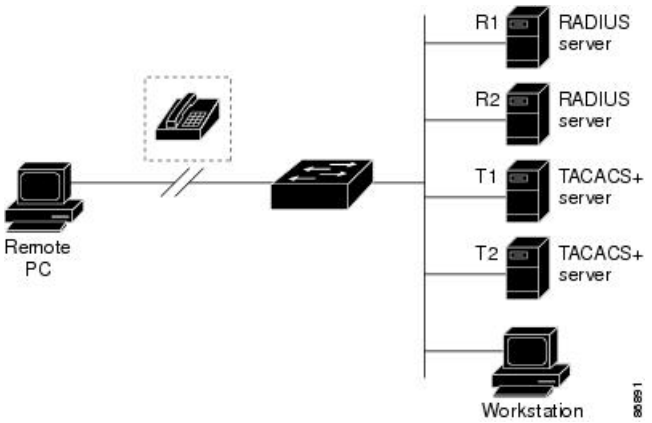
RADIUS の概要

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。

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。
- 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 deviceを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。

図 *1 : RADIUS* サービスから *TACACS+* サービスへの移行



- 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 ポートベースの認証の設定」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。

RADIUS の動作

RADIUS サーバによってアクセス コントロールされるdeviceに、ユーザ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要求されるか、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、およびアカウンティング（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。シスコ デバイスは、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。

シスコ デバイスは、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。

シスコデバイスで、RADIUS インターフェイスはデフォルトで有効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。

- アカウンティング：このガイドの「スイッチベース認証の設定」の章の「RADIUS アカウンティングの起動」の項を参照してください。

Cisco IOS XE 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動的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 *1 : 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 モデルで使用することによって、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 *2 :* サポートされている *IETF* 属性

属性番号	属性名
24	State
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 *3 : 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
404	無効な要求

値	説明
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、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

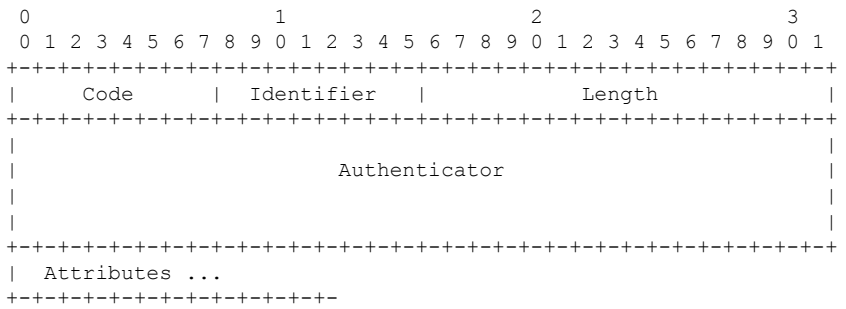
特定のセッションに向けられた切断と CoA 要求については、スイッチは 1 つ以上の次の属性に基づいて、セッションを検索します。

- 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、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、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 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 *4*：サポートされる *CoA* コマンド

コマンド [1]	シスコの VSA
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"

コマンド [1]	シスコの VSA
Disable host port	Cisco:Avpair="subscriber:command=disable-host-port"

[1] 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。

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。

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、ホストポートを無効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有効にします。

プリンタなどのサプ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（ポートを一時的に無効した後、再び有効にする）。

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、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 を返します。

デバイスがクライアントに接続解除 ACK を返す前にスタンバイデバイス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、新しいアクティブデバイス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：ホストポートの無効化

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有効にします。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、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。

（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するか、または元のコマンドが実行されてスタンバイデバイス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、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 秒間無効にし、再び有効にし（ポートバウンス）、CoA-ACK 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 のデフォルト設定

RADIUS および AAA は、デフォルトでは無効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 を有効にすると、CLI 経由でデバイスにアクセスするユーザーを認証できます。

RADIUS サーバ ホスト

デバイスと RADIUS サーバー間の通信には、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
- 鍵文字列
- 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

がアカウンティングサービスを提供できなかった場合、デバイスは「%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 番目に設定されたホストエントリでアカウン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 サーバーとデバイスは、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 サーバーデーモンが稼働するホストと、そのホストがデバイスと共有する秘密テキスト（鍵）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、および暗号鍵の値は、すべての RADIUS サーバーに対してグローバルに設定することもできますし、サーバー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ー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 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デバイスを設定できます。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使用できるサービスが制限されます。AAA 許可が有効になっていると、デバイスはユーザ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、ローカルのユーザデータベースまたはセキュリティサーバ上にあり、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 アカウンティング

AAA アカウンティング機能は、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 アカウンティングを有効にすると、デバイスはユーザーアクティビティをアカウンティングレコードの形式でRADIUS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、デバイスと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文字列です。

```
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“
```

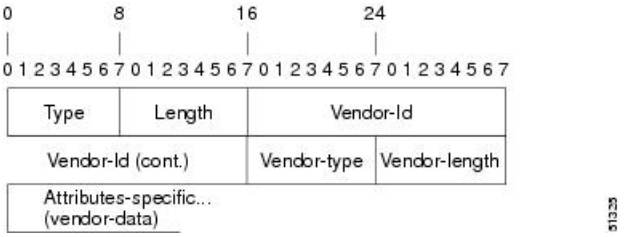
他のベンダーにも、それぞれ独自のベンダー ID、オプション、および対応する VSA があります。ベンダー ID および VSA の詳細については、RFC 2138『Remote Authentication Dial-In User Service (RADIUS)』を参照してください。

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
- 文字列（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 *2 :* 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 とも呼ばれる）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 *5 :* 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。

フィールド	説明
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 番めのレイヤ」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 文字列名。
説明	属性の説明。

表 *6 :* 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				
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。

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-drop-out-of-order	正しくない順序で受信したデータパケットを破棄して、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	有効にすると、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。
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。

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-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	**mmoip aaa receive-id** コマンドまたは **mmoip aaa send-id** 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。
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。

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	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。
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。

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	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 が有効にされているかどうかを示します。true は DSN が有効にされていることを示します。false は DSN が有効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）が有効にされているかどうかを示します。true は MDN が有効にされていることを示します。false は MDN が有効にされていないことを示します。
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、success、failed、bypassed、または unknown 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	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、hostname.domain-name 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、fax receive または fax send 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 **telephony** と **VoIP** 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
				PPP 名前認証。PAP に適用する場合、インターフェイスで **ppp pap sent-name password** 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、「preauth:send-name」および「preauth:send-secret」が使用されます。CHAP の場合、「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、「preauth:send-name」で定義された名前を使用します。 （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。remote-name 属性が追加されたため、send-name 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
				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とを確認し、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	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、**radius-server vsa send** 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） 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。
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、**ip mobile secure host <addr>** 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）、鍵、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、デバイスと RADIUS サーバー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 XE 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。

前述のように、（ベンダー固有か IETF ドラフト準拠かに関係なく）RADIUS を設定するには、RADIUS サーバーデーモンを実行するホストと、デバイスと共有する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 パケットの DSCP マーキング

差別化サービス（DiffServ）は、他のトラフィッククラスよりも優先的に処理するためにトラフィックを分類および管理する Quality of Service（QoS）モデルです。DiffServ は、IP パケットの 6 ビット DiffServ コードポイント（DSCP）設定を使用して、トラフィッククラスに相対的な優先順位をマークします。Cisco IOS XE ソフトウェアは、RADIUS パケットの DSCP マーキングをサポートして、RADIUS パケットの認証とアカウンティングを高速化します。

RADIUS サーバー、RADIUS サーバーグループ、およびグローバル コンフィギュレーション モードで DSCP マーキングを設定できます。DSCP マーキングが RADIUS サーバー、サーバー グループ、およびグローバル コンフィギュレーション モードに設定されると、RADIUS サーバーに入力された DSCP マーキング値が優先されます。

- RADIUS サーバーに DSCP マーキング設定がない場合、サーバーグループに設定された DSCP マーキング値が RADIUS パケットに適用されます。
- RADIUS サーバーまたは RADIUS サーバーグループに DSCP マーキング設定がない場合、グローバル コンフィギュレーション モードで設定された DSCP マーキング値が RADIUS パケットに適用されます。

RADIUS の設定

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。

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 サーバー グループを使用するようにデバイスを設定できます。

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。deviceの IP アドレス、およびサーバーとdeviceの双方で共有する鍵文字列などの設定値です。

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上にグローバルな機能とサーバ単位での機能（タイムアウト、再送信回数、および鍵コマンド）を設定した場合、サーバ単位で設定したタイムアウト、再送信回数、および鍵値コマンドは、グローバルに設定したタイムアウト、再送信回数、および鍵値コマンドを上書きします。

（注） RADIUS および AAA サーバーは、標準のデフォルトポートでのみ実行するように設定できます。

- 1812 および 1813
- 1645 および 1646

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. **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	**enable** 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	**configure terminal** 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	**radius server** *server name* 例： `Device(config)# radius server rsim`	RADIUS サーバ設定の名前を 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。
ステップ 4	**address** {**ipv4	ipv6**}*ip address*{ **auth-port** *port number*	**acct-port** *port number*} 例： `Device(config-radius-server)# address ipv4 124.2.2.12 auth-port 1612`	（任意）RADIUS サーバーのパラメータを指定します。 **auth-port** *port-number* 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。 **acct-port** *port-number* には、アカウンティング要求の 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	**key** *string* 例： `Device(config-radius-server)# key rad123`	（任意）**key** *string* には、デバイスと RADIUS サーバーで動作する RADIUS デーモンの間で使用される認証と暗号鍵を指定します。

	コマンドまたはアクション	目的
		（注） 鍵は、RADIUS サーバーで使用する暗号鍵に一致するテキスト文字列でなければなりません。必ず **radius server** コマンドの最終項目として鍵を設定してください。先頭のスペースは無視されますが、鍵の中間および末尾のスペースは使用されます。鍵にスペースを使用する場合は、引用符が鍵の一部分である場合を除き、引用符で鍵を囲まないでください。
ステップ 6	**retransmit** *value* 例： `Device(config-radius-server)# retransmit 10`	（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、**radius-server retransmit** 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 7	**timeout** *seconds* 例： `Device(config-radius-server)# timeout 60`	（任意）deviceが要求を再送信する前にRADIUSサーバ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、**radius-server timeout** 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	**end** 例： `Device(config-radius-server)# end`	RADIUS サーバー コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

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 アクセスに対しデバイス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 アクセスに対しデバイスのセキュリティは確保されません。

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**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 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	**configure terminal** 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	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA を有効にします。
ステップ 4	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] 例： `Device(config)# aaa authentication login default local`	ログイン認証方式リストを作成します。 • **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。 • *list-name* 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。 • *method1...* 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。 • *enable*：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 **enable** *password* 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。

	コマンドまたはアクション	目的
		• *group radius*：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。 • *line*：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。**password** *password* ライン コンフィギュレーション コマンドを使用します。 • *local*：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名情報を入力しておく必要があります。**username** *name* **password** 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。 • *local-case*：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。**username** *password* 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。 • *none*：ログインに認証を使用しません。
ステップ 5	**line** [**console** | **tty** | **vty**] *line-number* [*ending-line-number*] 例： `Device(config)# line 1 4`	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	**login authentication** {**default** | *list-name*} 例： `Device(config-line)# login authentication default`	1 つの回線または複数回線に認証リストを適用します。 • **default** を指定する場合は、**aaa authentication login** コマンドで作成したデフォルトのリストを使用します。 • *list-name* には、**aaa authentication login** コマンドで作成したリストを指定します。
ステップ 7	**end** 例： `Device(config-line)# end`	ラインコンフィギュレーションモードを終了して、特権 EXEC モードを開始します。

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**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 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	**configure terminal** 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	**radius server** *name* 例： `Device(config)# radius server ISE`	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 対応の RADIUS をサポートしています。
ステップ 4	**address** {**ipv4** | **ipv6**} {*ip-address* | *hostname*} **auth-port** *port-number* **acct-port** *port-number* 例： `Device(config-radius-server)# address ipv4 10.1.1.1 auth-port 1645 acct-port 1646`	RADIUS サーバのアカウンティングおよび認証パラメータの IPv4 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 5	**key** *string* 例： `Device(config-radius-server)# key cisco123`	デバイスと RADIUS サーバーとの間におけるすべての RADIUS 通信用の認証および暗号鍵を指定します。
ステップ 6	**end** 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。

ユーザー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** *authorization-list***radius**
4. **aaa authorization exec** *authorization-list***radius**
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	**enable** 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	**configure terminal** 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。

	コマンドまたはアクション	目的
ステップ 3	**aaa authorization network** *authorization-list***radius** 例： `Device(config)# aaa authorization network list1 radius`	ネットワーク関連のすべてのサービス要求に対して、ユーザーが RADIUS 許可を受けるように device を設定します。
ステップ 4	**aaa authorization exec** *authorization-list***radius** 例： `Device(config)# aaa authorization exec list1 radius`	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。 **exec** キーワードを指定すると、ユーザープロファイル情報（**autocommand** 情報など）が返される場合があります。
ステップ 5	**end** 例： `Device(config)# end`	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。

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** *accounting-list***start-stop radius**
4. **aaa accounting exec** *accounting-list***start-stop radius**
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	**enable** 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	**configure terminal** 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	**aaa accounting network** *accounting-list***start-stop radius** 例： `Device(config)# aaa accounting network start-stop radius`	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有効にします。
ステップ 4	**aaa accounting exec** *accounting-list***start-stop radius** 例： `Device(config)# aaa accounting exec acc-list start-stop radius`	RADIUSアカウンティングを有効にして、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	**end** 例： `Device(config)# end`	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。

すべての RADIUS サーバの設定

すべての RADIUS サーバーを設定するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius server** *server name*
4. **key** *string*
5. **retransmit** *retries*
6. **timeout** *seconds*
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	**enable** 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	**configure terminal** 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	**radius server** *server name* 例： `Device(config)# radius server rsim`	RADIUS サーバ設定の名前を 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。
ステップ 4	**key** *string* 例： `Device(config-radius-server)# key your_server_key`	スイッチとすべての RADIUS サーバ間で共有される秘密テキスト文字列を指定します。 （注） 鍵は、RADIUS サーバで使用する暗号鍵に一致するテキスト文字列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、鍵の中間および末尾のスペースは使用されます。鍵にスペースを使用する場合は、引用符が鍵の一部分である場合を除き、引用符で鍵を囲まないでください。
ステップ 5	**retransmit** *retries* 例： `Device(config-radius-server)# retransmit 5`	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 6	**timeout** *seconds* 例： `Device(config-radius-server)# timeout 3`	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 7	**end** 例： `Device(config-radius-server)# end`	RADIUS サーバー コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ベンダー固有の RADIUS 属性を使用するデバイスの設定

ベンダー固有の RADIUS 属性を設定するには、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**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 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	**configure terminal** 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	**radius-server vsa send** [**accounting**	**authentication**] 例： `Device(config)# radius-server vsa send accounting`	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。 • （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、**accounting** キーワードを使用します。 • （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、**authentication** キーワードを使用します。 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	**end** 例： `Device(config)# end`	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 モードを開始します。

ベンダー独自仕様の RADIUS サーバ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. **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	**enable** 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	**configure terminal** 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	**radius server** *server name* 例： `Device(config)# radius server rsim`	RADIUS サーバ設定の名前を 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。
ステップ 4	**address** { **ipv4	ipv6** } *ip address* 例： `Device(config-radius-server)# address ipv4 172.24.25.10`	（任意）RADIUS サーバの IP アドレスを指定します。
ステップ 5	**non-standard** 例： `Device(config-radius-server)# non-standard`	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	**key** *string* 例： `Device(config-radius-server)# key rad123`	デバイス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。デバイスと 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。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： `Device(config-radius-server)# end`	RADIUS サーバーモードを終了し、特権 EXEC モードを開始します。

RADIUS サーバーでの DSCP マーキングの設定

RADIUS サーバーでの認証とアカウンティング用の DSCP マーキングを設定するには、次の手順に従います。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius server** *server_name*
4. **address** { **ipv4 | ipv6** } *ip address* [**auth-port** *auth_port_number* **acct-port** *acct_port_number*]
5. **dscp** {**acct** *dscp_acct_value* | **auth** *dscp_auth_value*}
6. **key** *string*
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。
ステップ 2	**configure terminal** 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	**radius server** *server_name* 例： `Device(config)# radius server rsim`	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	**address** { **ipv4	ipv6** } *ip address* [**auth-port** *auth_port_number* **acct-port** *acct_port_number*] 例： `Device(config-radius-server)# address ipv4`	（任意）RADIUS サーバーの IP アドレスを指定します。 • **auth-port** は、RADIUS 認証サーバーのポート値を設定します。デフォルト値は 1812 です。

	コマンドまたはアクション	目的
	`10.1.1.1 auth-port 1645 acct-port 1646`	• **acct-port** は、RADIUS アカウンティングサーバーのポート値を設定します。デフォルト値は 1813 です。
ステップ 5	**dscp** {**acct** *dscp_acct_value* | **auth** *dscp_auth_value*} 例： `Device(config-radius-server)# dscp auth 10 acct 20`	RADIUS サーバーでの認証とアカウンティング用の DSCP マーキングを設定します。 • **acct** はアカウンティングの RADIUS DSCP マーキング値を設定します。有効な範囲は 1 ～ 63 です。デフォルト値は 0 です • **auth** は認証の RADIUS DSCP マーキング値を設定します。有効な範囲は 1 ～ 63 です。デフォルト値は 0 です
ステップ 6	**key** *string* 例： `Device(config-radius-server)# key rad123`	デバイス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。デバイスと 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	**end** 例： `Device(config-radius-server)# end`	RADIUS サーバーモードを終了し、特権 EXEC モードを開始します。

RADIUS サーバーグループでの送信元インターフェイスと DSCP マーキングの設定

次の手順に従って、RADIUS サーバーグループでの認証とアカウンティング用の送信元インターフェイスと DSCP マーキングを設定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa group server radius** *group_name*
4. **server name** *name*
5. {**ip** | **ipv6**} **radius source-interface** *type number*
6. **dscp** {**acct** *dscp_acct_value* | **auth** *dscp_auth_value*}
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	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。
ステップ 2	**configure terminal** 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	**aaa group server radius** *group_name* 例： `Device(config)# aaa group server radius abc`	RADIUS サーバー グループ コンフィギュレーションを定義し、RADIUS サーバー グループ コンフィギュレーション モードを開始します。
ステップ 4	**server name** *name* 例： `Device(config-sg-radius)# server name serv1`	RADIUS サーバーをサーバーグループに関連付けます。
ステップ 5	{**ip** | **ipv6**} **radius source-interface** *type number* 例： `Device(config-sg-radius)# ipv6 radius source-interface ethernet 0/0`	RADIUS サーバーの送信元アドレスに使用するインターフェイスを指定します。
ステップ 6	**dscp** {**acct** *dscp_acct_value* | **auth** *dscp_auth_value*} 例： `Device(config-sg-radius)# dscp auth 10 acct 20`	RADIUS サーバーグループでの認証とアカウンティング用の DSCP マーキングを設定します。 • **acct** はアカウンティングの RADIUS DSCP マーキング値を設定します。有効な範囲は 1 ～ 63 です。デフォルト値は 0 です • **auth** は認証の RADIUS DSCP マーキング値を設定します。有効な範囲は 1 ～ 63 です。デフォルト値は 0 です
ステップ 7	**end** 例： `Device(config-radius-server)# end`	RADIUS サーバーモードを終了し、特権 EXEC モードを開始します。

デバイス上での CoA の設定

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 server-key**
10. **exit**
11. **authentication command bounce-port ignore**
12. **authentication command disable-port ignore**
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	**enable** 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	**configure terminal** 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	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA を有効にします。
ステップ 4	**aaa server radius dynamic-author** 例： `Device(config)# aaa server radius dynamic-author`	デバイスを認証、許可、アカウンティング（AAA）サーバーとして設定して外部ポリシーサーバーとの通信を容易にし、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 モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**client** {*ip-address* | *name*} [**vrf** *vrfname*] [**server-key** *string*] 例： `Device(config-locsvr-da-radius)# client client1 vrf vrf1`	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	**server-key** [**0** | **7**] *string* 例： `Device(config-locsvr-da-radius)# server-key your_server_key`	RADIUS 鍵をデバイスと 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	**port** *port-number* 例： `Device(config-locsvr-da-radius)# port 25`	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	**auth-type** {**any** | **all** | **session-key**} 例： `Device(config-locsvr-da-radius)# auth-type any`	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	**ignore server-key** 例： `Device(config-locsvr-da-radius)# ignore server-key`	（任意）server-key を無視するように device を設定します。
ステップ 10	**exit** 例： `Device(config-locsvr-da-radius)# exit`	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	**authentication command bounce-port ignore** 例： `Device(config)# authentication command bounce-port ignore`	（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無効にするようにdeviceを設定します。ポートを一時的に無効にする目的は、VLAN の変更が発生しても、その変更を検出するサプ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。

	コマンドまたはアクション	目的
ステップ 12	**authentication command disable-port ignore** 例： `Device(config)# authentication command disable-port ignore`	（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device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。 ポートを再び有効にするには、標準の CLI または SNMP コマンドを使用します。
ステップ 13	**end** 例： `Device(config)# end`	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。

CoA 機能のモニタリング

表 *7*：特権 *EXEC* 表示コマンド

コマンド	目的
show aaa attributes protocol radius	RADIUS コマンドの AAA 属性を表示します。

表 *8*：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
debug radius	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。
debug aaa coa	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。
debug aaa pod	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。
debug aaa subsys	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。
debug cmdhd[**detail** |**error** |**events**]	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。

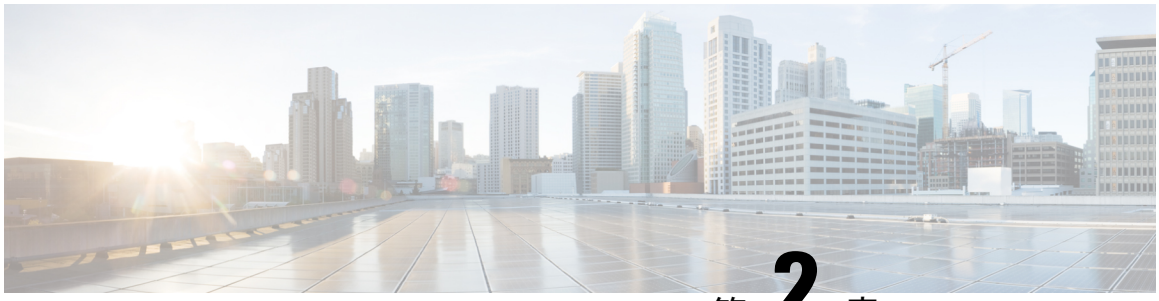
RADIUS の機能の履歴

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。

機能	機能情報	リリース
RADIUS サーバーでの DSCP マーキング	**dscp** コマンドを使用して、RADIUS サーバーおよび RADIUS サーバーグループで DiffServ コードポイント（DSCP）マーキングを設定できます。**radius-server dscp** コマンドは、グローバル コンフィギュレーション モードで RADIUS サーバーの認証およびアカウンティングのために DSCP マーキングを設定するために使用します。	IE 3x00 および ESS 3300：Cisco IOS XE Cupertino 17.8.1
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。	IE 3x00：Cisco IOS XE Gibraltar 16.11.1 ESS 3300：Cisco IOS XE Gibraltar 16.9.1

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 2 章

無遅延 IPDT

- 無遅延 IPDT について （49 ページ）
- 注意事項と制約事項 （50 ページ）
- IPDT の設定例 （50 ページ）
- IPDT の確認 （51 ページ）
- 機能の履歴 （51 ページ）

無遅延 IPDT について

無遅延 IP デバイストラッキング（IPDT）機能を使用すると、IPDT が有効になっているネットワークで ARP パケットをより高速に処理できます。無遅延 IPDT は、すべての IE3x00 スイッチでサポートされます。無遅延 IPDT には、IPDT を有効にする以外の設定は必要ありません。また、遅延なし IPDT を確認するための特定のコマンドはありません。

IPDT は、DHCP スヌーピングおよび ARP スヌーピング機能を使用して、スイッチに存在する IP-to-MAC バインディングのデータベースを構築します。無遅延 IPDT 機能を使用しない場合、IPDT が設定されていると、すべての ARP パケットは処理のために CPU にパントされ、パケットは CPU から最終的な宛先に転送されます。これにより、ARP 配信が遅延し、ホスト間の通信エラーが発生したり、実稼働が停止したりする可能性があります。

無遅延 IPDT 機能を使用する場合、IPDT が設定されていると、元の ARP トラフィックはハードウェアを介して転送され、ARP パケットのコピーだけが IP-MAC バインディングの作成のためにソフトウェアに送信されます。これにより、ARP 配信時間が短縮されます。無遅延 IPDT は、IPv6 ネイバー探索の動作を変更しません。

DAI（ダイナミック ARP インスペクション）が有効になっている場合、無遅延 IPDT は機能しません。DAI は、ARP キャッシュポイズニングなどのレイヤ 2 攻撃を防ぐために、ARP 要求と応答をフィルタリングするメカニズムを提供するセキュリティ機能です。フィルタリングは、DHCP スヌーピング バインディング データベースまたはユーザーが設定した ARP アクセスコントロールリスト（ACL）に基づいて実行されます。

次の表に、IPDT および DAI の設定に基づいて ARP パケットがどのように処理されるかを示します。

機能の設定	ARP パケット処理
IPDT のみ有効	ARP パケットはハードウェアを介して転送され、コピーが CPU にパントされます（無遅延 IPDT）。 （注） コピーされたパケットは、処理後に廃棄されます。
DAI のみ有効	ARP パケットは、処理のために CPU にパントされます（無遅延 IPDT なし）。DAI を有効にすると、CPU が処理するときに ARP パケットがわずかに遅延します。
IPDT および DAI が有効	ARP パケットは、処理のために CPU にパントされます（無遅延 IPDT なし）。

注意事項と制約事項

- 無遅延 IPDT は、IPDT ポリシーが少なくとも 1 つのインターフェイスまたは VLAN で有効になっている場合に自動的に有効になります。

  この機能は、IPDT ポリシーがアタッチされているインターフェイスまたは VLAN に関係なく、グローバルに有効になります。

- 無遅延 IPDT は、アクセスモードとトランクモードの両方で動作します。
- スイッチの DAI がいずれかの VLAN で有効になっている場合、無遅延 IPDT は機能しません。
- 無遅延 IPDT は、インターフェイスまたは VLAN ごとに有効または無効にすることはできません。

IPDT の設定例

無遅延 IPDT 機能には、設定するための特定の CLI はありません。IPDT を設定して有効にするだけで済みます。次に、IPDT ポリシーを設定し、インターフェイスまたは VLAN にアタッチするための基本的なコマンドの例を示します。

```
configure terminal
device-tracking policy test
 limit address-count <count>
 security-level glean
 tracking enable
exit
interface GigabitEthernet1/5
 device-tracking attach-policy test
 exit
```

```
vlan configuration 5
 device-tracking attach-policy test
exit
```

IPDT の確認

無遅延 IPDT を確認するための特定のコマンドはありません。次の IPDT **show** コマンドを使用して、IPDT データベースに関する詳細を表示できます。

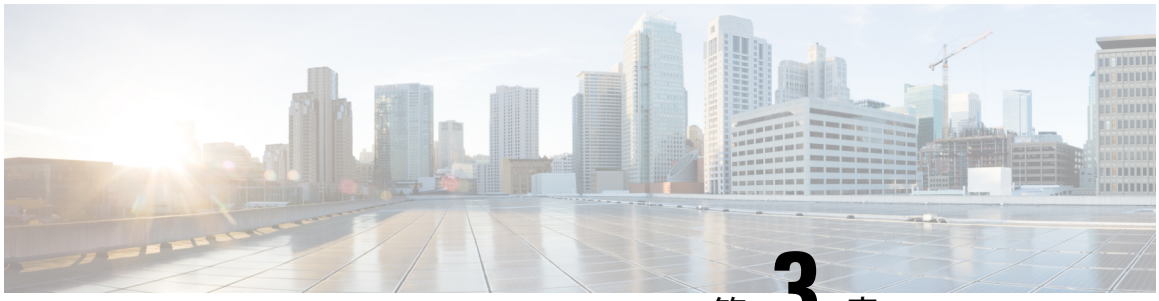
- show device-tracking database
- show device-tracking database interface <interfaceid>
- show device-tracking database details
- show device-tracking database vlanid <vlanid>

次に、**show device-tracking database interface** コマンドの出力例を示します。

```
Switch#show device-tracking database interface GigabitEthernet1/5
portDB has 4 entries for interface Gi1/5, 4 dynamic
Codes: L - Local, S - Static, ND - Neighbor Discovery, ARP - Address Resolution Protocol,
 DH4 - IPv4 DHCP, DH6 - IPv6 DHCP, PKT - Other Packet, API - API created
Preflevel flags (prlvl):
0001:MAC and LLA match     0002:Orig trunk            0004:Orig access
0008:Orig trusted trunk    0010:Orig trusted access   0020:DHCP assigned
0040:Cga authenticated     0080:Cert authenticated    0100:Statically assigned


    Network Layer Address                    Link Layer Address     Interface  vlan
   prlvl      age        state      Time left
ARP 3.1.1.10                                 0000.1100.0004         Gi1/5      30
   0005       12s        REACHABLE  297 s
ARP 3.1.1.9                                  0000.1100.0003         Gi1/5      30
   0005       17s        REACHABLE  289 s
ARP 3.1.1.8                                  0000.1100.0002         Gi1/5      30
   0005       21s        REACHABLE  292 s
ARP 3.1.1.7                                  0000.1100.0001         Gi1/5      30
   0005       25s        REACHABLE  276 s
```

機能の履歴

機能名	リリース	機能情報
無遅延 IPDT	Cisco IOS XE 17.14.1	IE3x00 での初期サポート



第 3 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 （53 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 （53 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 （54 ページ）
- IPv6 スヌーピング ポリシーの設定方法 （56 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 （58 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 （60 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 （61 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 （61 ページ）
- IPv6 ネイバー探索検査ポリシーの設定方法 （63 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 （68 ページ）
- IPv6 DHCP ガード ポリシーの設定方法 （74 ページ）
- IPv6 ソース ガードの設定方法 （79 ページ）
- IPv6 プレフィックス ガードの設定方法 （82 ページ）
- IPv6 ファースト ホップ セキュリティの設定例 （84 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 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。

- 同じノードにおけるホストとガードの設定はサポートされていません。
- DHCPv6 ガードを機能させるには、同じスイッチ上の対応する VLAN で SVI を設定する必要があります。

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、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。

（注） 以降、IPv6 スヌーピングポリシー機能は廃止され、Switch Integrated Security Features（SISF）ベースのデバイス追跡に置き換わります。IPv6 スヌーピング ポリシー コマンドは CLI で引き続き使用でき、既存の設定は引き続きサポートされますが、コマンドは今後のリリースで CLI から削除されます。代わりの機能の詳細については、このガイドの「*SISF* ベースのデバイス追跡の設定」を参照してください。

- 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。

（注） 以降、IPv6 FHS バインディング テーブル コンテンツ機能は、SISF ベースのデバイス追跡によってサポートされます。詳細については、このガイドの「*SISF* ベースのデバイス追跡の設定」を参照してください。

- 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） Cisco IOS XE Amsterdam 17.1.1 以降、IPv6 ND 検査機能は廃止され、SISF ベースのデバイス追跡機能に置き換えられます。IPv6 ND 検査コマンドは CLI で引き続き使用でき、既存の設定は引き続きサポートされますが、コマンドは今後のリリースで CLI から削除されます。代わりの機能の詳細については、このガイドの「*SISF* ベースのデバイス追跡の設定」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 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	**configure terminal** 例： `# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 snooping policy** *policy-name* 例： `(config)# ipv6 snooping policy example_policy`	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	{[**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**] } 例： `(config-ipv6-snooping)# security-level inspect` 例：	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。 • （任意）**default**：すべてをデフォルト オプションに設定します。 • （任意）**device-role**{**node**]|**switch**}：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 **node** です。

	コマンドまたはアクション	目的
	(config-ipv6-snooping)# trusted-port	• （任意）**limit address-count** *value*：ターゲットごとに許可されるアドレス数を制限します。 • （任意）**no**：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。 • （任意）**protocol**{**dhcp** | **ndp**}：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、**dhcp** および **ndp** です。デフォルトを変更するには、**no protocol** コマンドを使用します。 • （任意）**security-level**{**glean**|**guard**|**inspect**}：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 **guard** です。 **glean**：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。 **guard**：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。 **inspect**：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。 • （任意）**tracking** {**disable** | **enable**}：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。 • （任意）**trusted-port**：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無効になります。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。
ステップ 4	**end** 例： `(config-ipv6-snooping)# exit`	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	**show ipv6 snooping policy** *policy-name* 例：	スヌーピング ポリシー設定を表示します。

	コマンドまたはアクション	目的
	#**show ipv6 snooping policy example_policy**	

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	**configure terminal** 例： # **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** Interface_type *stack/module/port* 例： (config)# **interface gigabitethernet 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	**switchport** 例：	switchport モードを開始します。

	コマンドまたはアクション	目的
	(config-if)# **switchport**	（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 switchport 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、インターフェイスはデフォルト設定に戻ります。switchport 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）#と表示されます。
ステップ 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**}] 例： (config-if)# **ipv6 snooping** or (config-if)# **ipv6 snooping attach-policy example_policy** or (config-if)# **ipv6 snooping vlan 111,112** or (config-if)# **ipv6 snooping attach-policy example_policy vlan 111,112**	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、**attach-policy** キーワードを指定せずに **ipv6 snooping** 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、**ipv6 snooping vlan** 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 **guard**、デバイス ロール **node**、プロトコル **ndp** および **dhcp** です。
ステップ 5	**do show running-config** 例： #(config-if)# **do show running-config**	インターフェイス コンフィギュレーション モードを終了しないで、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	**configure terminal** 例： `# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface range** *Interface_name* 例： `(config)# interface range Po11`	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 **do show interfaces summary** コマンドを使用します。

ステップ 3	**ipv6 snooping** [**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**}]
	例：
	`(config-if-range)# ipv6 snooping attach-policy example_policy`
	or
	`(config-if-range)# ipv6 snooping attach-policy example_policy vlan 222,223,224`
	or
	`(config-if-range)#ipv6 snooping vlan 222, 223,224`
		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。**attach-policy** 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	**do show running-config interface***portchannel_interface_name* 例： `#(config-if-range)# do show running-config int po11`	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	**configure terminal** 例： `# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan configuration** *vlan_list* 例： `(config)# vlan configuration 333`	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	**ipv6 snooping** [**attach-policy** *policy_name*] 例： `(config-vlan-config)#ipv6 snooping attach-policy example_policy`	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。**attach-policy** 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 **guard**、デバイス ロール **node**、プロトコル **ndp** および **dhcp** です。
ステップ 4	**do show running-config** 例： `#(config-if)# do show running-config`	インターフェイス コンフィギュレーション モードを終了しないで、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

1. **configure terminal**
2. [**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**] }]
3. [**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-limit***number*]]]]
4. **ipv6 neighbor binding logging**
5. **exit**
6. **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	**configure terminal** 例： `# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**] **ipv6 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**] }] 例： `(config)# ipv6 neighbor binding`	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	[**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-limit***number*]]]] 例： `(config)# ipv6 neighbor binding max-entries 30000`	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	**ipv6 neighbor binding logging** 例： `(config)# ipv6 neighbor binding logging`	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	**exit** 例：	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。

	コマンドまたはアクション	目的
	(config)# **exit**	
ステップ 6	**show ipv6 neighbor binding** 例： # **show ipv6 neighbor binding**	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

17.1.1 以降、IPv6 ND 検査機能は廃止され、SISF ベースのデバイス追跡に置き換えられます。対応する置き換えタスクについては、このドキュメントの「*SISF* ベースのデバイス追跡の設定」の章の「カスタム設定を使用したカスタムデバイス追跡ポリシーの作成」を参照してください。

特権 EXEC モードから、IPv6 ND インスペクション 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	**configure terminal** 例： # **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**]**ipv6 nd inspection policy** *policy-name* 例： (config)# **ipv6 nd inspection policy example_policy**	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	**device-role** {**host**	**switch**} 例：	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 **host** です。

	コマンドまたはアクション	目的
	(config-nd-inspection)# **device-role switch**	
ステップ 4	**limit address-count** *value* 例： (config-nd-inspection)# **limit address-count 1000**	1 ～ 10,000 を入力します。
ステップ 5	**tracking** {**enable** [**reachable-lifetime** {*value* | **infinite**}] | **disable** [**stale-lifetime** {*value* | **infinite**}]} 例： (config-nd-inspection)# **tracking disable stale-lifetime infinite**	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	**trusted-port** 例： (config-nd-inspection)# **trusted-port**	信頼できるポートにするポートを設定します。
ステップ 7	**validate source-mac** 例： (config-nd-inspection)# **validate source-mac**	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	**no** {**device-role** | **limit address-count** | **tracking** | **trusted-port** | **validate source-mac**} 例： (config-nd-inspection)# **no validate source-mac**	このコマンドの **no** 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	**default** {**device-role** | **limit address-count** | **tracking** | **trusted-port** | **validate source-mac**} 例： (config-nd-inspection)# **default limit address-count**	設定をデフォルト値に戻します。
ステップ 10	**do show ipv6 nd inspection policy** *policy_name* 例： (config-nd-inspection)# **do show ipv6 nd inspection policy example_policy**	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

17.1.1 以降、IPv6 ND 検査機能は廃止され、SISF ベースのデバイス追跡に置き換えられます。対応する置き換えタスクについては、このドキュメントの「*SISF* ベースのデバイス追跡の設定」の章の「デバイス追跡ポリシーのインターフェイスへの適用」を参照してください。

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	**configure terminal** 例： `# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** Interface_type *stack/module/port* 例： `(config)# interface gigabitethernet 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	**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**}]
	例：
	`(config-if)# ipv6 nd inspection attach-policy example_policy`
	or
	`(config-if)# ipv6 nd inspection attach-policy example_policy vlan 222,223,224`
	or
	`(config-if)# ipv6 nd inspection vlan 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。**attach-policy** 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	**do show running-config** 例： `#(config-if)# do show running-config`	インターフェイス コンフィギュレーション モードを終了しないで、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

17.1.1 以降、IPv6 ND 検査機能は廃止され、SISF ベースのデバイス追跡機能に置き換えられます。対応する置き換えタスクについては、このドキュメントの「*SISF* ベースのデバイス追跡の設定」の章の「デバイス追跡ポリシーのインターフェイスへの適用」を参照してください。

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	**configure terminal** 例： `# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface range** *Interface_name* 例： `(config)# interface Po11`	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 **do show interfaces summary** コマンドを使用します。

ステップ 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**}]
	例：
	`(config-if-range)# ipv6 nd inspection attach-policy example_policy`
	or
	`(config-if-range)# ipv6 nd inspection attach-policy example_policy vlan 222,223,224`
		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。**attach-policy** 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。

	コマンドまたはアクション	目的
	or (config-if-range)#**ipv6 nd inspection vlan 222, 223,224**	
ステップ 4	**do show running-config interface***portchannel_interface_name* 例： #(config-if-range)# **do show running-config int po11**	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

17.1.1 以降、IPv6 ND 検査機能は廃止され、SISF ベースのデバイス追跡に置き換えられます。対応する置き換えタスクについては、このドキュメントの「*SISF* ベースのデバイス追跡の設定」の「デバイス追跡ポリシーの *VLAN* への適用」を参照してください。

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	**configure terminal** 例： # **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan configuration** *vlan_list* 例： (config)# **vlan configuration 334**	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	**ipv6 nd inspection** [**attach-policy** *policy_name*] 例： (config-vlan-config)#**ipv6 nd inspection attach-policy example_policy**	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。**attach-policy** 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。

	コマンドまたはアクション	目的
		デフォルトのポリシーは、device-role **host**、no drop-unsecure、limit address-count disabled、sec-level minimum is disabled、tracking is disabled、no trusted-port、no validate source-mac です。
ステップ 4	**do show running-config** 例： `#(config-if)# do show running-config`	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 raguard 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 raguard 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	**configure terminal** 例： `# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**]**ipv6 nd raguard policy** *policy-name* 例： `(config)# ipv6 nd raguard policy example_policy`	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。

	コマンドまたはアクション	目的
ステップ 3	[**no**]**device-role** {**host** | **monitor** | **router** | **switch**} 例： `(config-nd-raguard)# device-role switch`	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 **host** 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 **device-role host** 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 **device-role router** 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	[**no**]**hop-limit** {**maximum** | **minimum**} *value* 例： `(config-nd-raguard)# hop-limit maximum 33`	（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。 設定されていない場合、このフィルタは無効になります。「**minimum**」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。「**maximum**」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	[**no**]**managed-config-flag** {**off** | **on**} 例： `(config-nd-raguard)# managed-config-flag on`	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。 **On**：「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。 **Off**：「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	[**no**]**match** {**ipv6 access-list** *list* | **ra prefix-list** *list*} 例：	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。

	コマンドまたはアクション	目的
	(config-nd-raguard)# **match ipv6 access-list example_list**	
ステップ 7	[**no**]**other-config-flag** {**on** | **off**} 例： (config-nd-raguard)# **other-config-flag on**	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。 **On**：「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。 **Off**：「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	[**no**]**router-preference maximum** {**high** | **medium** | **low**} 例： (config-nd-raguard)# **router-preference maximum high**	「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。 • **high**：「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。 • **medium**：「Router Preference」が「high」に設定された RA メッセージをブロックします。 • **low**：「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。
ステップ 9	[**no**]**trusted-port** 例： (config-nd-raguard)# **trusted-port**	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	**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**} 例： (config-nd-raguard)# **default hop-limit**	コマンドをデフォルト値に戻します。

	コマンドまたはアクション	目的
ステップ 11	**do show ipv6 nd raguard policy** *policy_name* 例： `(config-nd-raguard)# do show ipv6 nd raguard policy example_policy`	（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ース上の 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* | **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	**configure terminal** 例： `# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** Interface_type *stack/module/port* 例： `(config)# interface gigabitethernet 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	**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* | **except***vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]
	例：
	`(config-if)# ipv6 nd raguard attach-policy example_policy`
	or
	`(config-if)# ipv6 nd raguard attach-policy example_policy vlan 222,223,224`
	or
		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。**attach-policy** 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。

	コマンドまたはアクション	目的
	`(config-if)# ipv6 nd raguard vlan 222, 223,224`	
ステップ 4	**do show running-config** 例： `#(config-if)# do show running-config`	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2EtherChannel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 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* | **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	**configure terminal** 例： `# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface range** *Interface_name* 例： `(config)# interface Po11`	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 do show interfaces summary コマンドを使用します。
ステップ 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* | **except***vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] 例：	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。**attach-policy** 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。

	コマンドまたはアクション	目的
	(config-if-range)# **ipv6 nd raguard attach-policy example_policy** or (config-if-range)# **ipv6 nd raguard attach-policy example_policy vlan 222,223,224** **or** (config-if-range)#**ipv6 nd raguard vlan 222, 223,224**	
ステップ 4	**do show running-config interface***portchannel_interface_name* 例： #(config-if-range)# **do show running-config int po11**	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	**configure terminal** 例： # **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan configuration** *vlan_list* 例： (config)# **vlan configuration 335**	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。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 dhcp guard** [**attach-policy** *policy_name*] 例： `(config-vlan-config)#ipv6 nd raguard attach-policy example_policy`	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。**attach-policy** 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	**do show running-config** 例： `#(config-if)# do show running-config`	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	**configure terminal** 例： `# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	[**no**]**ipv6 dhcp guard policy** *policy-name* 例： `(config)# ipv6 dhcp guard policy example_policy`	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	[**no**]**device-role** {**client**	**server**} 例： `(config-dhcp-guard)# device-role server`	（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 **client** です。

	コマンドまたはアクション	目的
		• **client**：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。 • **server**：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。

ステップ 4	[**no**] **match server access-list** *ipv6-access-list-name*
	例：
	`;;Assume a preconfigured IPv6 Access List as follows:`
	`(config)# ipv6 access-list my_acls`
	`(config-ipv6-acl)# permit host FE80::A8BB:CCFF:FE01:F700 any`
	`;;configure DCHPv6 Guard to match approved access list.`
	`(config-dhcp-guard)# match server access-list my_acls`
		（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、permit allとして処理されます。

ステップ 5	[**no**] **match reply prefix-list** *ipv6-prefix-list-name*
	例：
	`;;Assume a preconfigured IPv6 prefix list as follows:`
	`(config)# ipv6 prefix-list my_prefix permit 2001:0DB8::/64 le 128`
	`;; Configure DCHPv6 Guard to match prefix`
	`(config-dhcp-guard)# match reply prefix-list my_prefix`
		（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クスが設定された承認プレフィ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。空のプレフィクスリストは、permitとして処理されます。

ステップ 6	[**no**]**preference**{ **max** *limit* | **min** *limit* }
	例：
	`(config-dhcp-guard)# preference max 250`
	`(config-dhcp-guard)#preference min 150`
		device-role が **server** である場合に **max** および **min** 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。
		max *limit*：（0～255）（任意）アドバタイズされたプリファレンス（[preference]オプション内）が指定された制限未満であるかどうかの検証を有効にします。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。
		min *limit*：（0～255）（任意）アドバタイズされたプリファレンス（[preference]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

	コマンドまたはアクション	目的
		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。
ステップ 7	[**no**] **trusted-port** 例： `(config-dhcp-guard)# trusted-port`	（任意）**trusted-port**：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。 （注） 信頼できるポートを設定した場合、device-role オプションは使用できません。
ステップ 8	**default** {**device-role** | **trusted-port**} 例： `(config-dhcp-guard)# default device-role`	（任意）**default**：コマンドをデフォルトに設定します。
ステップ 9	**do show ipv6 dhcp guard policy** *policy_name* 例： `(config-dhcp-guard)# do show ipv6 dhcp guard policy example_policy`	（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。*policy_name* 変数を省略すると、すべての DHCPv6 ポリシーが表示されます。

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 pol1
 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 pol1 vlan add 1
 vlan 1
  ipv6 dhcp guard attach-policy pol1
show ipv6 dhcp guard policy pol1
```

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	**configure terminal** 例： `# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan configuration** *vlan_list* 例： `(config)# vlan configuration 334`	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	**ipv6 dhcp guard** [**attach-policy** *policy_name*] 例： `(config-vlan-config)#ipv6 dhcp guard attach-policy example_policy`	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。**attach-policy** 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 **client**、**no** trusted-port です。
ステップ 4	**do show running-config** 例： `#(config-if)# do show running-config`	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	**configure terminal** 例： `# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface range** *Interface_name* 例： `(config)# interface Po11`	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 **do show interfaces summary** コマンドを使用します。

ステップ 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**}]
	例：
	`(config-if-range)# ipv6 dhcp guard attach-policy example_policy`
	or
	`(config-if-range)# ipv6 dhcp guard attach-policy example_policy vlan 222,223,224`
	or
	`(config-if-range)#ipv6 dhcp guard vlan 222, 223,224`
		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。**attach-policy** 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	**do show running-config interface***portchannel_interface_name* 例： `#(config-if-range)# do show running-config int po11`	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	**configure terminal** 例： `# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**vlan configuration** *vlan_list* 例： `(config)# vlan configuration 334`	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	**ipv6 dhcp guard** [**attach-policy** *policy_name*] 例： `(config-vlan-config)#ipv6 dhcp guard attach-policy example_policy`	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。**attach-policy** 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 **client**、**no** trusted-port です。
ステップ 4	**do show running-config** 例： `#(config-if)# do show running-config`	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. **configure terminal**
2. [**no**] **ipv6 source-guard policy** *policy_name*
3. [**deny global-autoconf**] [**permit link-local**] [**default**{. . . }] [**exit**] [**no**{. . . }]
4. **end**
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	**configure terminal** 例： `# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	[**no**] **ipv6 source-guard policy** *policy_name* 例： `(config)# ipv6 source-guard policy example_policy`	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 3	[**deny global-autoconf**] [**permit link-local**] [**default**{. . . }] [**exit**] [**no**{. . . }] 例： `(config-sisf-sourceguard)# deny global-autoconf`	（任意）IPv6 ソース ガード ポリシーを定義します。 • **deny global-autoconf**：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。 • **permit link-local**：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。 （注） ソース ガード ポリシーでは trusted オプションはサポートされません。
ステップ 4	**end** 例： `(config-sisf-sourceguard)# end`	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 5	**show ipv6 source-guard policy** *policy_name* 例： `# show ipv6 source-guard policy example_policy`	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. **configure terminal**
2. **interface** Interface_type *stack/module/port*
3. **ipv6 source-guard**［**attach-policy** <*policy_name*> ］
4. **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	**configure terminal** 例： `# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** Interface_type *stack/module/port* 例： `(config)# interface gigabitethernet 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	**ipv6 source-guard** [**attach-policy** <*policy_name*>] 例： `(config-if)# ipv6 source-guard attach-policy example_policy`	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。**attach-policy** 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	**show ipv6 source-guard policy** *policy_name* 例： `#(config-if)# show ipv6 source-guard policy example_policy`	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. **configure terminal**
2. **interface port-channel** *port-channel-number*
3. **ipv6 source-guard** [**attach-policy** <*policy_name*>]
4. **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	**configure terminal** 例： `# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface port-channel** *port-channel-number* 例： `(config)# interface Po4`	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。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 source-guard**［**attach-policy** <*policy_name*> ］ 例： `(config-if) # ipv6 source-guard attach-policy example_policy`	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。**attach-policy** 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	**show ipv6 source-guard policy** *policy_name* 例： `(config-if) #show ipv6 source-guard policy example_policy`	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. ［**no**］**ipv6 source-guard policy** *source-guard-policy*
2. ［ **no** ］**validate address**
3. **validate prefix**
4. **exit**
5. **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	［**no**］**ipv6 source-guard policy** *source-guard-policy* 例： `(config)# ipv6 source-guard policy my_snooping_policy`	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 2	［ **no** ］**validate address** 例： `(config-sisf-sourceguard)# no validate address`	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 3	**validate prefix** 例： `(config-sisf-sourceguard)# validate prefix`	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。

	コマンドまたはアクション	目的
ステップ 4	**exit** 例： `(config-sisf-sourceguard)# exit`	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 5	**show ipv6 source-guard policy** ［*source-guard-policy*］ 例： `# show ipv6 source-guard policy policy1`	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. **configure terminal**
2. **interface** Interface_type *stack/module/port*
3. **ipv6 source-guard attach-policy** *policy_name*
4. **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	**configure terminal** 例： `# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** Interface_type *stack/module/port* 例： `(config)# interface gigabitethernet 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	**ipv6 source-guard attach-policy** *policy_name* 例： `(config-if)# ipv6 source-guard attach-policy example_policy`	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。**attach-policy** 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	**show ipv6 source-guard policy** *policy_name* 例： `(config-if)# show ipv6 source-guard policy example_policy`	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. **configure terminal**
2. **interface port-channel** *port-channel-number*
3. **ipv6 source-guard**［**attach-policy** <*policy_name*> ］
4. **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	**configure terminal** 例： `# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface port-channel** *port-channel-number* 例： `(config)# interface Po4`	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 3	**ipv6 source-guard**［**attach-policy** <*policy_name*> ］ 例： `(config-if)# ipv6 source-guard attach-policy example_policy`	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。**attach-policy** 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	**show ipv6 source-guard policy** *policy_name* 例： `(config-if)# show ipv6 source-guard policy example_policy`	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
```

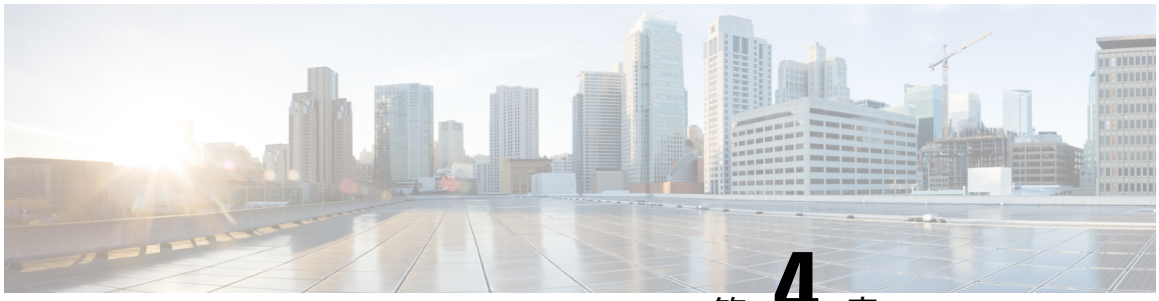
```
Switch(config)# interface Po4
Switch(config)# ipv6 snooping
Switch(config-if)# ipv6 source-guard attach-policy POL
Switch(config-if)# exit
switch(config)#
```

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
```

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



第 4 章

レイヤ 2 NAT の設定

- レイヤ 2 ネットワークアドレス変換 （87 ページ）
- レイヤ 2 NAT スイッチサポート （90 ページ）
- 注意事項と制約事項 （91 ページ）
- デフォルト設定 （92 ページ）
- レイヤ 2 NAT の設定 （92 ページ）
- 設定の確認 （93 ページ）
- 基本的な内部から外部への通信の例 （94 ページ）
- 重複する IP アドレスの例 （96 ページ）

レイヤ 2 ネットワークアドレス変換

1 対 1（1:1）レイヤ 2 ネットワークアドレス変換（NAT）は、固有のパブリック IP アドレスを既存のプライベート IP アドレス（エンドデバイス）に割り当てるサービスです。この割り当てにより、エンドデバイスがプライベートサブネットおよびパブリックサブネット上で通信できます。このサービスは、NAT 対応デバイスで設定され、エンドデバイスに物理的にプログラムされた IP アドレスのパブリックでの「エイリアス」です。これは、通常 NAT デバイスでテーブルとして表されます。

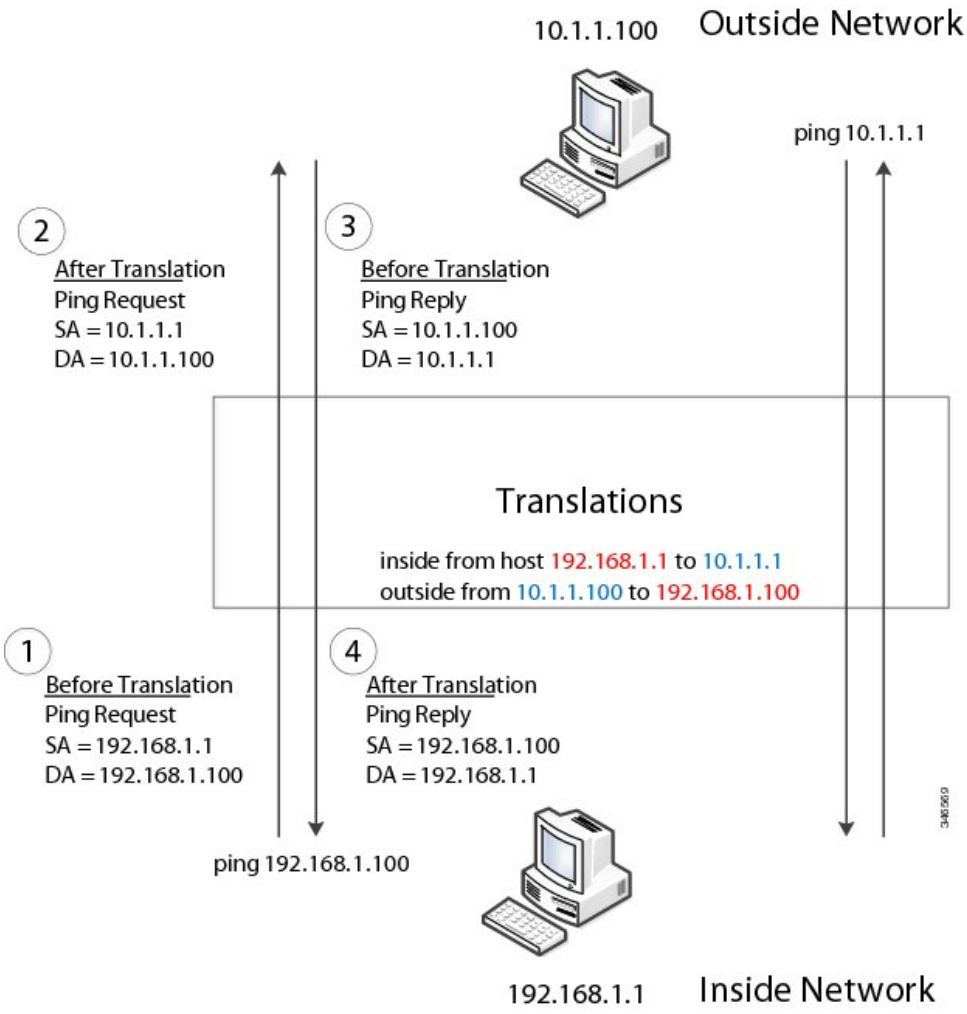
レイヤ 2 NAT はテーブルを使用して、IPv4 アドレスをパブリックからプライベートおよびプライベートからパブリックの両方にラインレートで変換します。レイヤ 2 NAT は、一貫した高レベルの（bump-in-the-wire）ワイヤスピードのパフォーマンスを提供するハードウェアベースの機能です。またこの機能は、拡張されたネットワーク セグメンテーション用の NAT 境界で複数の VLAN をサポートします。

次に、レイヤ 2 NAT で 192.168.1.x ネットワークのセンサーと 10.1.1.x ネットワークの通信制御装置間のアドレスを変換する例を示します。

1. 192.168.1.x ネットワークは内側/内部 IP アドレス空間、10.1.1.x ネットワークは外側または外部 IP アドレス空間です。
2. 192.168.1.1 のセンサーが、「内部」アドレス 192.168.1.100 を使用して通信制御装置に ping 要求を送信します。

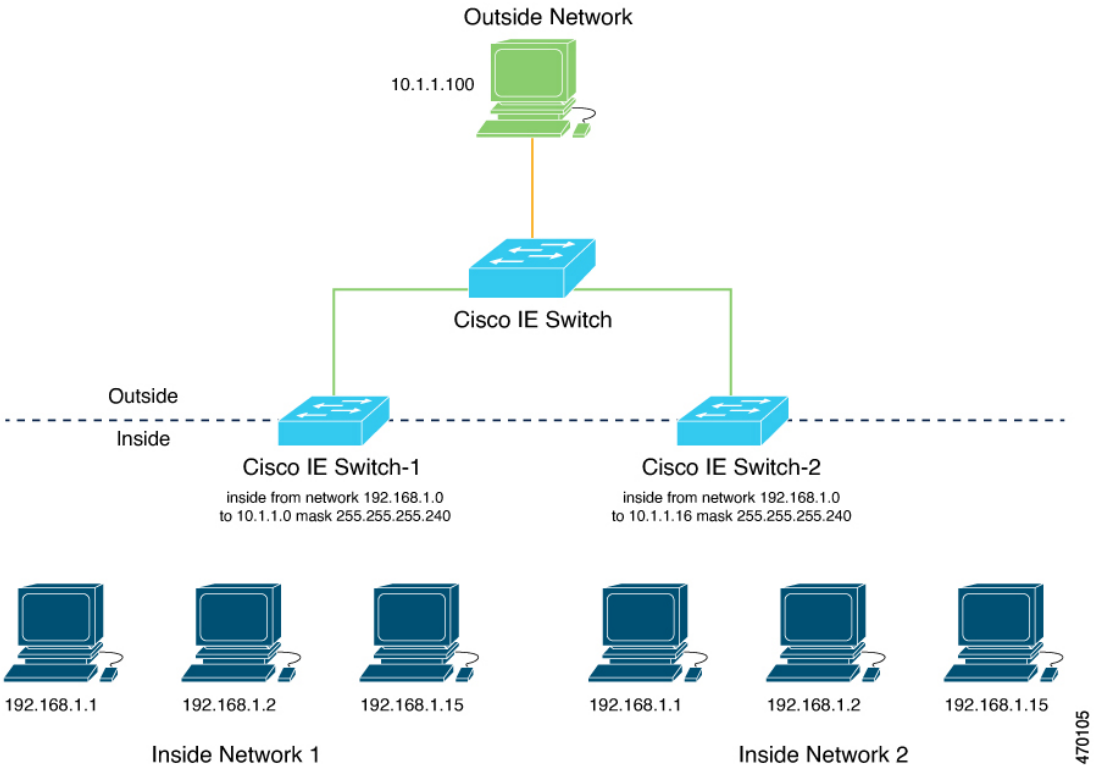
3. パケットが内部ネットワークから送信される前に、レイヤ2NATは送信元アドレス（SA）を 10.1.1.1 へ、宛先アドレス（DA）を 10.1.1.100 へと変換します。
4. 通信制御装置は 10.1.1.1 へ ping 応答を送信します。
5. パケットが内部ネットワークで受信されると、レイヤ 2 NAT は送信元アドレスを 192.168.1.100 へ、宛先アドレスを 192.168.1.1 へ変換します。

図 *3:* ネットワーク間のアドレス変換



多数のノードに対して、サブネット内のすべてのデバイスの変換をまとめて有効にできます。この場合、内部ネットワーク 1 からのアドレスは 10.1.1.0/28 サブネットで外部アドレスに変換することができ、内部ネットワーク 2 からのアドレスは 10.1.1.16/28 サブネットで外部アドレスに変換することができます。各サブネットのアドレスはすべて1つのコマンドを使って変換できます。サブネットベースの変換を使用すると、レイヤ L2 NAT ルールを節約できます。スイッチには、レイヤ 2 NAT ルールの数に制限があります。サブネットを含むルールでは、1 つのルールで複数のエンドデバイスを変換できます。

図 *4* : 内部-外部アドレス変換



次の図は、レイヤ2MACアドレスに基づいてイーサネットパケットを転送するアグリゲーションレイヤでの Cisco Catalyst IE3400 高耐久性シリーズ スイッチを示しています。この例では、ルータはすべてのサブネットと VLAN のレイヤ 3 ゲートウェイです。

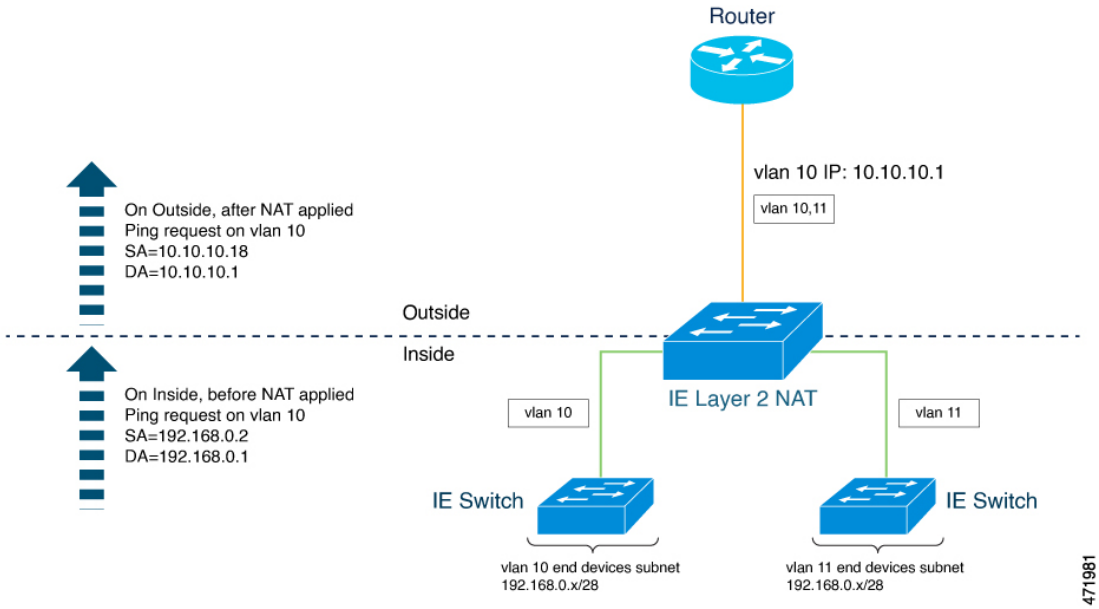
L2NAT インスタンス定義では、`network` コマンドを使用して、同じサブネット内の複数のデバイスの変換行を定義します。この場合は、/28 サブネットです。このサブネットマスクでは、内部 IP アドレスの 4 番目のバイトの最後のニブルは変更されません。変換後の IP アドレスは 10.10.10.16 であるため、最後のバイトは 16 ～ 31 の範囲になります。

VLAN のゲートウェイは、IP アドレスの最後のバイトが .1 で終わるルータです。外部ホスト変換は、ゲートウェイルータに提供されます。レイヤ 2 NAT 定義の `network` コマンドは、1 つのコマンドでサブネットに相当するホストを変換し、レイヤ2NAT変換ルールを節約します。

Gi1/1 アップリンク インターフェイスには、VLAN 10 および VLAN 11 サブネット用の 2 つのレイヤ 2 NAT 変換インスタンスがあります。インターフェイスは、複数のレイヤ 2 NAT インスタンス定義をサポートできます。

下流の IE スイッチは、レイヤ 2 NAT を実行しないスイッチの例で、レイヤ 2 NAT を上流のアグリゲーション レイヤ スイッチに依存しています。

図 *5 : IE3400* スイッチの *NAT*



上の図に表示されている IE3400 NAT の設定は次のとおりです。

```
!
l2nat instance Subnet10-NAT
 instance-id 1
 permit all
 fixup all
 outside from host 10.10.10.1 to 192.168.0.1
 inside from network 192.168.0.0 to 10.10.10.16 mask 255.255.255.240
!
l2nat instance Subnet11-NAT
 instance-id 1
 permit all
 fixup all
 outside from host 10.10.11.1 to 192.168.0.1
 inside from network 192.168.0.0 to 10.10.11.16 mask 255.255.255.240
!
interface GigabitEthernet1/1
 switchport mode trunk
 l2nat Subnet10-NAT 10
 l2nat Subnet11-NAT 11
!
Interface vlan 1
  ip address 10.10.1.2
```

レイヤ 2 NAT スイッチサポート

- IE3105：レイヤ 2 NAT 機能は、アップリンクポート（Gig 1/1 および Gig 1/2）でのみサポートされており、両方の（Essential および Advantage）ライセンスで使用できます。
- IE3300：レイヤ 2 NAT 機能は、アップリンクポート（Gig 1/1 および Gig 1/2）でのみサポートされており、両方の（Essential および Advantage）ライセンスで使用できます。

- IE3400：レイヤ 2 NAT 機能は、アップリンクポート（Gig 1/1 および Gig 1/2）でのみサポートされており、両方の（Essential および Advantage）ライセンスで使用できます。

注意事項と制約事項

- IPv4 アドレスのみ変換できます。
- レイヤ 2 NAT はユニキャストトラフィックにのみ適用されます。未変換のユニキャストトラフィック、マルチキャストトラフィック、およびIGMPトラフィックを通過することができます。
- レイヤ 2 NAT は、1 対多および多対 1 の IP アドレスのマッピングをサポートしていません。
- レイヤ 2 NAT は、外部 IP アドレスと内部 IP アドレス間の 1 対 1 のマッピングをサポートしています。
- レイヤ 2 NAT ではパブリック IP アドレスを節約できません。
- レイヤ 2 NAT のホストの変換を設定する場合は、DHCP クライアントとして設定しないでください。
- ARP、ICMP などの特定のプロトコルは、レイヤ 2 NAT 越しに透過的に機能しませんが、これはデフォルトで「フィックスアップ」されます。「フィックスアップ」とは、プロトコルが機能するように IP パケットのペイロードに組み込まれた IP アドレスが変更されることを意味します。
- ダウンリンクポートには、VLAN、トランク、レイヤ 2 チャネルなどがあります。
- スイッチには、128 のレイヤ 2 NAT ルールを設定できます。
- レイヤ 2 NAT 設定では最大 128 の VLAN が利用できます。
- 管理インターフェイスはレイヤ2NAT機能の背後にあります。そのためこのインターフェイスはプライベート ネットワーク VLAN 上に置かないようにしてください。プライベート ネットワーク VLAN 上に存在する場合は、内部アドレスを割り当て、内部の変換を設定します。
- L2NATは外部アドレスと内部アドレスを分けるように設計されているため、同じサブネットのアドレスを外部アドレスと内部アドレスの両方に設定しないことを推奨します。
- NAT インスタンス設定をサポートするインターフェイスは、Gig 1/1 および Gig 1/2（アップリンク）です。

デフォルト設定

機能	デフォルト設定
一致しないトラフィックまたは変換するよう設定されていないトラフィックタイプのパケットの通過または破棄。	すべての一致しない、マルチキャストの IGMP パケットを破棄する。
プロトコル フィックスアップ	フィックスアップは、ARP および ICMP に対して有効になっています。

（注） 上記の表で、「一致しない」は、インターフェイスに適用されるレイヤ 2 NAT インスタンスのルールとして変換用に定義された IP アドレスを持たないホストを指します。

レイヤ 2 NAT の設定

アドレスの変換を指定するレイヤ 2 NAT インスタンスを設定する必要があります。次に、これらのルールをアップリンク インターフェイスにアタッチします。一致しないトラフィック及び変換するよう設定されていないトラフィックタイプに対して、トラフィックの通過または破棄を選択できます。IE スイッチ管理インターフェイスは、管理インターフェイス（CLI/SNMP/CIP/WebUI）の背後にあります。送受信されたパケットに関する詳細な統計情報を確認できます（設定の確認 （93 ページ）を参照）。

レイヤ 2 NAT を設定するには、次の手順を実行します。詳細については、基本的な内部から外部への通信の例 （94 ページ）および重複する IP アドレスの例 （96 ページ）の例を参照してください。

ステップ 1 グローバル コンフィギュレーション モードを開始します。

configure terminal

ステップ 2 新しいレイヤ 2 NAT インスタンスを作成します。

l2nat instance *instance_name*

インスタンスを作成した後、そのインスタンスのサブモードを開始する場合もこのコマンドを使用します。

ステップ 3 内部アドレスを外部アドレスへ変換します。

inside from [*host* | *range* | *network*] *original ip* to *translated ip* [*mask*] *number* | *mask*

単一のホストアドレス、ホストアドレスの範囲、またはサブネット内のすべてのアドレスを変換できます。発信トラフィックの送信元アドレスと着信トラフィックの宛先アドレスを変換します。ホストが内部に物理的に存在し、プライベート IP アドレスを持つ場合は、`inside from` コマンドを使用します。

ステップ 4 外部アドレスを内部アドレスへ変換します。

outside from [*host* | *range* | *network*] *original ip* to *translated ip* [*mask*] *number* | *mask*

単一のホストアドレス、ホストアドレスの範囲、またはサブネット内のすべてのアドレスを変換できます。発信トラフィックの宛先アドレスと着信トラフィックの送信元アドレスを変換します。ホストが外部に物理的に存在し、パブリック IP アドレスを持つ場合は、`outside from` コマンドを使用します。

ステップ 5 NAT 変換によって ICMP および IGMP の変換が修正されます。デフォルトでは、ARP と ICMP の両方のフィックスアップが有効になっているため、通常はデフォルトを変更しない限りこのコマンドは必要ありません。

fixup arp | icmp | all

（注） ICMP では、ICMP エラーメッセージに対するフィックスアップのみがサポートされます。

ステップ 6 （オプション）未変換のユニキャストトラフィックを通過します（デフォルトでは破棄されます）。

permit { **multicast** | **igmp** | **all** }

ステップ 7 config-l2nat モードを終了します。

exit

ステップ 8 指定したインターフェイス（IE3105、IE3300、および IE3400 の場合は gi1/1 および gi1/2）のインターフェイス コンフィギュレーション モードにアクセスします。

interface *interface-id*

ステップ 9 VLAN または VLAN 範囲に指定されたレイヤ 2 NAT のインスタンスを適用します。このパラメータが欠落している場合、レイヤ 2 NAT インスタンスはネイティブ VLAN に適用されます。

l2nat *instance_name* [*vlan* | *vlan_range*]

ステップ 10 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。

end

設定の確認

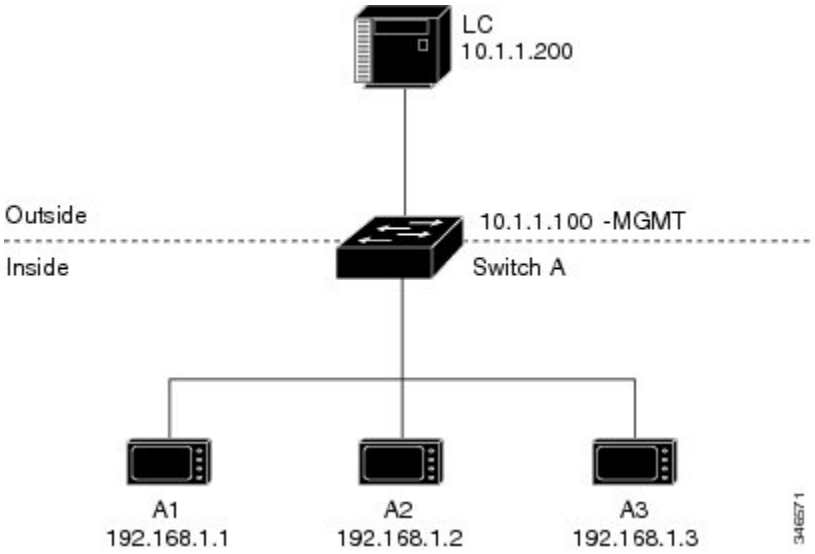
コマンド	目的
show l2nat instance	指定されたレイヤ 2 NAT インスタンスの設定の詳細を表示します。

コマンド	目的
show l2nat interface	1 つまたは複数のインターフェイスでのレイヤ 2 NAT インスタンスの設定の詳細を表示します。
show l2nat statistics	すべてのインターフェイスのレイヤ 2 NAT 統計情報を表示します。
show l2nat statistics interface	指定したインターフェイスのレイヤ 2 NAT 統計情報を表示します。
debug l2nat	設定が適用されたときにリアルタイムでのレイヤ 2 NAT 設定の詳細の表示を有効にします。

基本的な内部から外部への通信の例

ここでは、A1 はアップリンクポートに直接接続されたロジックコントローラ（LC）と通信する必要があります。レイヤ 2 NAT インスタンスは、外部ネットワーク（10.1.1.1）上での A1 のアドレスと内部ネットワーク（192.168.1.250）上での LC のアドレスを提供するように設定されています。

図 *6:* 基本的な内部から外部への通信



ここで次の通信が発生します。

1. A1 が「SA: 192.168.1.1 DA: 192.168.1.250」という ARP 要求を送信します。
2. Cisco スイッチ A は「SA: 10.1.1.1 DA: 10.1.1.200」という ARP 要求をフィックスアップします。
3. LC は要求を受信し、10.1.1.1 の MAC アドレスを学習します。

4. LC が「SA: 10.1.1.200 DA: 10.1.1.1」という応答を送信します。
5. Cisco スイッチ A は「SA: 192.168.1.250 DA: 192.168.1.1」という ARP 応答をフィックスアップします。
6. A1 は 192.168.1.250 の MAC アドレスを学習し、通信を開始します。

（注） スイッチの管理インターフェイスは内部ネットワーク 192.168.1.x. とは別の VLAN に属することをお勧めします。

次の表は、このシナリオの設定作業を示しています。レイヤ 2 NAT インスタンスが作成され、2 つの変換エントリを追加し、インスタンスをインターフェイスに適用します。ARP フィックスアップはデフォルトで有効です。

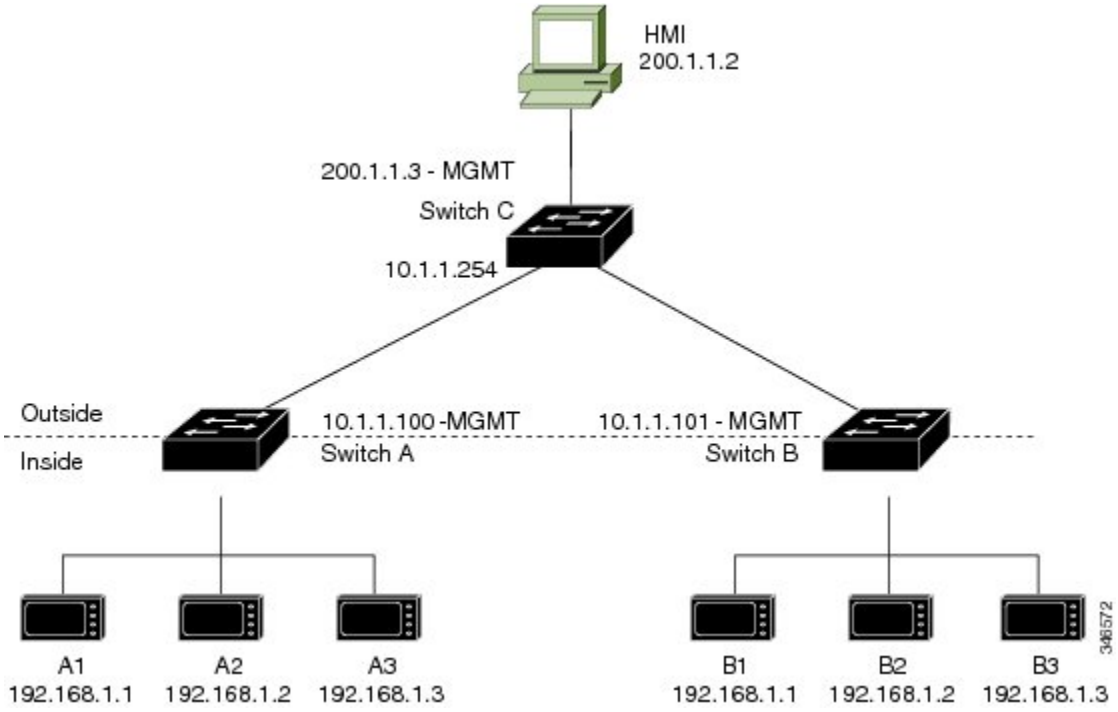
表 *9* : 基本的な内部から外部への *Cisco* スイッチ *A* の設定例

	コマンド	目的
1.	Switch# **configure**	グローバル コンフィギュレーション モードを開始します。
2.	Switch(config)# **l2nat instance A-LC**	A-LC という新しいレイヤ 2 NAT インスタンスを作成します。
3.	Switch(config-l2nat)# **inside from host 192.168.1.1 to 10.1.1.1**	A1 の内部アドレスを外部アドレスへ変換します。
4.	Switch(config-l2nat)# **inside from host 192.168.1.2 to 10.1.1.2**	A2 の内部アドレスを外部アドレスへ変換します。
5.	Switch(config-l2nat)# **inside from host 192.168.1.3 to 10.1.1.3**	A3 の内部アドレスを外部アドレスへ変換します。
6.	Switch(config-l2nat)# **outside from host 10.1.1.200 to 192.168.1.250**	LC の外部アドレスを内部アドレスへ変換します。
7.	Switch(config-l2nat)# **exit**	config-l2nat モードを終了します。
8.	Switch(config)# **interface Gi1/1**	アップリンク ポートのインターフェイス コンフィギュレーション モードにアクセスします。
9.	Switch(config-if)# **l2nat A-LC**	このインターフェイスのネイティブ VLAN に、先ほどのレイヤ 2 NAT インスタンスを適用します。 （注） トランク上のタグ付きトラフィックの場合は、インターフェイスへインスタンスを適用するときに、次のように VLAN 番号を追加します。 l2nat *instance vlan*
10.	Switch# **end**	特権 EXEC モードに戻ります。

重複する IP アドレスの例

ここでは、2 台のマシンノードで 192.168.1.x 領域のアドレスが事前設定されています。レイヤ 2 NAT により、これらのアドレスが外部ネットワークの別のサブネット上で一意のアドレスに変換されます。また、マシン間の通信では、ノード A のマシンはノード B の領域で一意のアドレスを必要とし、ノード B のマシンはノード A の領域で一意のアドレスが必要です。

図 *7: IP* アドレスの重複



- スイッチ C がプライベートネットワークのゲートウェイとして機能するには、スイッチ C に 192.168.1.x スペースのアドレスが必要です。パケットがノード A またはノード B で受信されると、スイッチ C の 10.1.1.254 というアドレスが 192.168.1.254 に変換されます。パケットがノード A またはノード B から送信されると、スイッチ C の 192.168.1.254 というアドレスは 10.1.1.254 に変換されます。
- ノード A とノード B のマシンは 10.1.1.x 領域で一意のアドレスが必要です。設定の容易さと使いやすさを実現するために、10.1.1.x 領域は 10.1.1.0、10.1.1.16、10.1.1.32 などのサブネットに分割されます。各サブネットは異なるノードに使用できます。この例では、10.1.1.16 はノード A に使用され、10.1.1.32 はノード B に使用されます。
- ノード A とノード B のマシンはデータを交換するための一意のアドレスが必要です。使用可能なアドレスはサブネットに分割されます。便宜上、ノード A のマシンの 10.1.1.16 サブネットアドレスは、ノード B の 192.168.1.16 サブネットアドレスに変換され、ノード B のマシンの 10.1.1.32 サブネットアドレスはノード A の 192.168.1.32 アドレスに変換されます。

• マシンは各ネットワークで一意のアドレスを持ちます。

表 *10 : IP* アドレスの変換

ノード	ノード A のアドレス	外部ネットワークのアドレス	ノード B のアドレス
スイッチ A のネットワークアドレス	192.168.1.0	10.1.1.16	192.168.1.16
A1	192.168.1.1	10.1.1.17	192.168.1.17
A2	192.168.1.2	10.1.1.18	192.168.1.18
A3	192.168.1.3	10.1.1.19	192.168.1.19
Cisco スイッチ B のネットワークアドレス	192.168.1.32	10.1.1.32	192.168.1.0
B1	192.168.1.33	10.1.1.33	192.168.1.1
B2	192.168.1.34	10.1.1.34	192.168.1.2
B3	192.168.1.35	10.1.1.35	192.168.1.3
スイッチ C	192.168.1.254	10.1.1.254	192.168.1.254

表 11 : アドレスが重複するスイッチ A の設定例 （97 ページ）に、スイッチ A の設定作業を示します。スイッチ B の設定作業については、表 12 : サブネットのスイッチ B の設定例 （98 ページ）に示します。

（注） この例は、IE 2000 スイッチに基づいています。IE3x00 および ESS3300 スイッチでは、インターフェイスの番号が異なる場合があります。

表 *11 :* アドレスが重複するスイッチ *A* の設定例

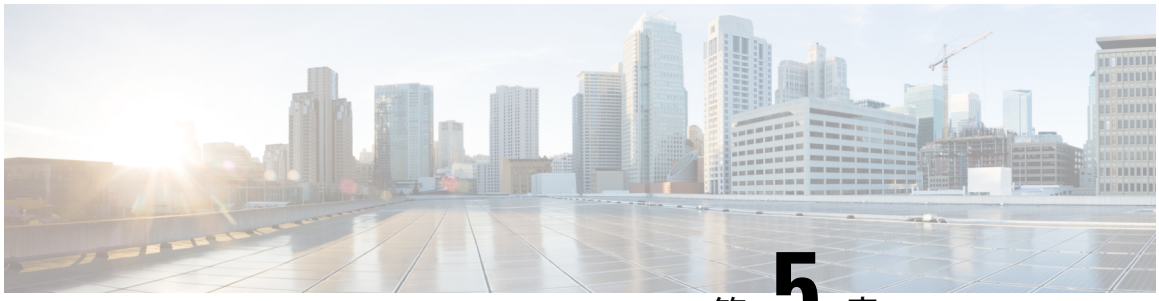
	コマンド	目的
1.	Switch# **configure**	グローバル コンフィギュレーション モードを開始します。
2.	Switch(config)# **l2nat instance A-Subnet**	A-Subnet という新しいレイヤ 2 NAT インスタンスを作成します。
3.	Switch(config-l2nat)# **inside from network 192.168.1.0 to 10.1.1.16 mask 255.255.255.240**	ノード A のマシンの内部アドレスを 10.1.1.16 255.255.255.240 サブネットのアドレスへ変換します。
4.	Switch(config-l2nat)# **outside from host 10.1.1.254 to 192.168.1.254**	スイッチ C の外部アドレスを内部アドレスへ変換します。

	コマンド	目的
5.	Switch(config-l2nat)# **outside from network 10.1.1.32 to 192.168.1.32 255.255.255.240**	ノード B のマシンの外部アドレスを内部アドレスへ変換します。
6.	Switch(config-l2nat)# **exit**	config-l2nat モードを終了します。
7.	Switch(config)# **interface Gi1/1**	アップリンク ポートのインターフェイス コンフィギュレーション モードにアクセスします。
8.	Switch(config-if)# **l2nat A-Subnet**	このインターフェイスのネイティブ VLAN に、先ほどのレイヤ 2 NAT インスタンスを適用します。 （注） トランク上のタグ付きトラフィックの場合は、インターフェイスへインスタンスを適用するときに、次のように VLAN 番号を追加します。 l2nat *instance vlan*
9.	Switch# **end**	特権 EXEC モードに戻ります。

表 *12* : サブネットのスイッチ *B* の設定例

	コマンド	目的
1.	Switch# **configure**	グローバル コンフィギュレーション モードを開始します。
2.	Switch(config)# **l2nat instance B-Subnet**	B-Subnet という新しいレイヤ 2 NAT インスタンスを作成します。
3.	Switch(config-l2nat)# **inside from network 192.168.1.0 to 10.1.1.32 255.255.255.240**	ノード B のマシンの内部アドレスを 10.1.1.32 255.255.255.240 サブネットのアドレスへ変換します。
4.	Switch(config-l2nat)# **outside from host 10.1.1.254 to 192.168.1.254**	スイッチ C の外部アドレスを内部アドレスへ変換します。
5.	Switch(config-l2nat)# **outside from network 10.1.1.16 to 192.168.1.16 255.255.255.240**	ノード A のマシンの外部アドレスを内部アドレスへ変換します。
6.	Switch(config-l2nat)# **exit**	config-l2nat モードを終了します。
7.	Switch(config)# **interface Gi1/1**	アップリンク ポートのインターフェイス コンフィギュレーション モードにアクセスします。

	コマンド	目的
8.	Switch(config-if)# **l2nat B-Subnet**	このインターフェイスのネイティブ VLAN に、先ほどのレイヤ 2 NAT インスタンスを適用します。 （注） トランク上のタグ付きトラフィックの場合は、インターフェイスへインスタンスを適用するときに、次のように VLAN 番号を追加します。 l2nat *instance vlan*
9.	Switch# **show l2nat instance name1**	指定されたレイヤ 2 NAT インスタンスの設定の詳細を表示します。
10.	Switch# **show l2nat statistics**	レイヤ 2 NAT の統計情報を表示します。
11.	Switch# **end**	特権 EXEC モードに戻ります。



第 5 章

MACsec の暗号化

この章は、次の項で構成されています。

- MACsec and the MACsec Key Agreement (MKA) Protocol （101 ページ）
- 証明書ベースの MACsec （109 ページ）
- MACsec 暗号化の設定方法 （109 ページ）

MACsec and the MACsec Key Agreement (MKA) Protocol

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。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、MKA ベースの鍵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。MKA プロトコルでは、必要なセッション鍵を提供し、必要な暗号鍵を管理します。

（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。

重要 ESS-3300 では、MACsec は 1 ギガビット イーサネット ダウンリンク ポートでのみサポートされます。

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）。

表 *13* : スイッチ ポートの *MACsec* サポート

接続	MACsec のサポート
スイッチからホストへ	MACsec MKA の暗号化

スイッチからスイッチへ	MACsec MKA の暗号化

Cisco TrustSec 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。ネットワーク エッジ アクセス トポロジ（NEAT）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されます。

MACsec と MACsec Key Agreement（MKA）は、証明書ベース MACsec または事前共有鍵（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。

MKA ポリシー

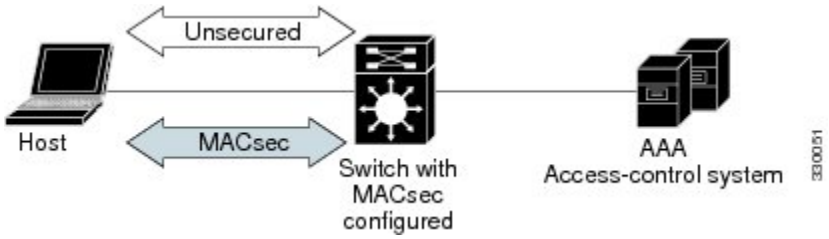
インターフェイスで MKA を有効にするには、定義された MKA ポリシーをインターフェイスに適用する必要があります。次のオプションを設定可能です。

- 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。

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 *8:* 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*



スイッチ間 MKA MACsec マストセキュアポリシー

MACsec がインターフェイスで有効になっている場合、EAPoL トラフィックを除くすべてのインターフェイス トラフィックは、入力と出力の両方でデフォルトで保護されます（デフォルトは「must-secure」です）。暗号化されていないパケットは、MKA セッションが保護されるまで破棄されます。ただし、選択したインターフェイスで MACsec を有効にするには、**macsec access-control** を **should-secure** に設定することで、同じ物理インターフェイスからの暗号化されていないパケットの送受信を許可できます。このオプションにより、MKA セッションが保

護されるまで、暗号化されていないトラフィックのフローが許可されます。MKA セッションが保護された後、暗号化されたトラフィックのフローのみが許可されます。設定の詳細については、PSK を使用した、インターフェイスでの MACsec MKA の設定 （117 ページ）を参照してください。

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、すべてのメンバーポートで 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、サプ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。サプ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 セッションの鍵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プ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鍵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。

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す。
- サプ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。

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。

次の例では、show mka statistics コマンドの出力を示します。

```
Switch# show mka sessions

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
=========================================================================================================
Gi1/0/1        204c.9e85.ede4/002b p2               NO                YES
43             c800.8459.e764/002a 1                Secured
0100000000000000000000000000000000000000000000000000000000000000

Switch#show mka sessions interface G1/0/1

Summary of All Currently Active MKA Sessions on Interface GigabitEthernet1/0/1...

=========================================================================================================
Interface      Local-TxSCI         Policy-Name      Inherited         Key-Server
Port-ID        Peer-RxSCI          MACsec-Peers     Status            CKN
=========================================================================================================
Gi1/0/1        204c.9e85.ede4/002b p2               NO                YES
43             c800.8459.e764/002a 1                Secured
0100000000000000000000000000000000000000000000000000000000000000


Switch#show mka sessions interface G1/0/1 de

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)...... 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
  ------------------------------------------------------------------------

Switch#show mka sessions de
Switch#show mka sessions 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)........... 01000000000000000000000000000000000000000000000000000000000000000000
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
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
  ------------------------------------------------------------------------

Switch#sh mka pol

MKA Policy Summary...

Policy            KS       Delay   Replay  Window Conf   Cipher          Interfaces
Name              Priority Protect Protect Size   Offset Suite(s)        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


Switch#sh mka poli
Switch#sh mka policy p2
Switch#sh mka policy p2 ?
  detail    Detailed configuration/information for MKA Policy
  sessions  Summary of all active MKA Sessions with policy applied
  |         Output modifiers
  <cr>

Switch#sh mka policy p2 de

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

Switch#sh mka policy p2

MKA Policy Summary...

Policy            KS       Delay   Replay  Window Conf   Cipher          Interfaces
Name              Priority Protect Protect Size   Offset Suite(s)        Applied
================================================================================================
p2                2        FALSE   TRUE    0      0      GCM-AES-128     Gi1/0/1


Switch#sh mka se?
sessions

Switch#sh mka ?
  default-policy  MKA Default Policy details
  keychains       MKA Pre-Shared-Key Key-Chains
  policy          MKA Policy configuration information
  presharedkeys   MKA Preshared Keys
  sessions        MKA Sessions summary
  statistics      Global MKA statistics
  summary         MKA Sessions summary & global statistics

Switch#sh mka statis
Switch#sh mka statistics ?
  interface  Statistics for a MKA Session on an interface
  local-sci  Statistics for a MKA Session identified by its Local Tx-SCI
  |          Output modifiers
  <cr>

Switch#sh mka statistics inter
Switch#show mka statistics interface G1/0/1

MKA Statistics for Session
==========================
Reauthentication Attempts.. 0

CA Statistics
   Pairwise CAKs Derived... 0
   Pairwise CAK Rekeys..... 0
   Group CAKs Generated.... 0
   Group CAKs Received..... 0

SA Statistics
   SAKs Generated.......... 1
   SAKs Rekeyed............ 0
   SAKs Received........... 0
   SAK Responses Received.. 1

MKPDU Statistics
   MKPDUs Validated & Rx... 89585
      "Distributed SAK".. 0
      "Distributed CAK".. 0
   MKPDUs Transmitted...... 89596
      "Distributed SAK".. 1
      "Distributed CAK".. 0


Switch#show mka ?
  default-policy  MKA Default Policy details
  keychains       MKA Pre-Shared-Key Key-Chains
  policy          MKA Policy configuration information
```

```
  presharedkeys   MKA Preshared Keys
  sessions        MKA Sessions summary
  statistics      Global MKA statistics
  summary         MKA Sessions summary & global statistics

Switch#show mka summ
Switch#show mka summary

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
=============================================================================================
Gi1/0/1        204c.9e85.ede4/002b p2               NO                YES
43             c800.8459.e764/002a 1                Secured
01000000000000000000000000000000000000000000000000000000000000000000



MKA Global Statistics
=====================
MKA Session Totals
   Secured.................... 1
   Reauthentication Attempts.. 0

   Deleted (Secured).......... 0
   Keepalive Timeouts......... 0

CA Statistics
   Pairwise CAKs Derived...... 0
   Pairwise CAK Rekeys........ 0
   Group CAKs Generated....... 0
   Group CAKs Received........ 0

SA Statistics
   SAKs Generated............. 1
   SAKs Rekeyed............... 0
   SAKs Received.............. 0
   SAK Responses Received..... 1

MKPDU Statistics
   MKPDUs Validated & Rx...... 89589
      "Distributed SAK"..... 0
      "Distributed CAK"..... 0
   MKPDUs Transmitted......... 89600
      "Distributed SAK"..... 1
      "Distributed CAK"..... 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

Switch#
```

証明書ベースの MACsec

証明書ベースの MACsec 暗号化機能は、Extensible Authentication Protocol – Transport Layer Security（EAP-TLS）による 802.1X ポートベース認証を使用して、MACsec 暗号化が必要なポートの証明書を伝送します。EAP-TLS メカニズムを相互認証のために使用し、マスターセッション鍵（MSK）を取得します。この MSK から、MACsec Key Agreement（MKA）プロトコル用の接続アソシエーション鍵（CAK）が導出されます。

この機能により、PSK（事前共有鍵）ベースの MACsec を介して集中型サーバー（CA）で鍵を管理できます。スイッチ間 MACsec がサポートされています。詳細については、「証明書ベース MACsec の設定 （119 ページ）」を参照してください。

MACsec 暗号化の設定方法

制限事項と制約事項

MACsec には、次の制限事項があります。

- ポートはアクセスモードまたはトランクモードである必要があります。
- MKA は、ポート チャネルではサポートされていません。ポートチャネルを構成する個々のリンクは MACsec を使用できます。
- MKA のハイ アベイラビリティはサポートされません。
- **no switchport** が指定されたポートはサポートされません。
- ESS3300 アップリンクポートには PHY がないため、MACSec はサポートされません。

MACsec 暗号化の前提条件

MACsec 暗号化の前提条件は次のとおりです。

- 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。

MKA および MACsec の設定

MACsec MKA のデフォルト設定

MACsec は無効です。MKA ポリシーは設定されていません。

MKA-PSK：CKN 動作の変更

Cisco IOS XE では、Cisco IOS Classic での CKN（「鍵」）の実装方法が変更されました。Cisco IOS XE を実行している IE スイッチが Cisco IOS Classic を実行している IE スイッチと事前共有鍵（PSK）MACSec 接続を確立する必要がある場合、設定する「鍵」値は 64 文字の 16 進数にする必要があります。また、「鍵」値は、Cisco IOS Classic を実行している IE スイッチでの同じ鍵値と一致する必要があります。Cisco IOS Classic 側の同じ「鍵」値にゼロを埋め込む必要はありません。

次の Cisco IOS XE の例は、2 つの Cisco IOS XE デバイスを接続する場合の鍵チェーン設定を示しています。

```
configure terminal
key chain KEYCHAINONE macsec
key 1234
cryptographic-algorithm aes-128-cmac
key-string 123456789ABCDEF0123456789ABCDEF0
lifetime local 12:21:00 Sep 9 2015 infinite
end
```

上記の例で、2 つの Cisco IOS XE 接続デバイスでの **show mka session** コマンドの出力を次に示します。

```
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
|
=========================================================================
Gi1/1        34c0.f983.6c81/0001  POLICYONE       NO             YES
1            54a2.7498.5b01/0001  1               Secured        1234
```

CKN key-string は、hex-string として鍵に設定されたものとまったく同じであることに注意してください。これは、CKN がゼロパディングされていない Cisco IOS XE から Cisco IOS XE PSK への例です。

Cisco IOS XE を実行しているデバイスと Cisco IOS Classic を実行しているデバイス間の相互運用性を実現するために、Cisco IOS XE デバイスは、設定 CKN 鍵をゼロパディングする必要がない Cisco IOS Classic と一致するように CKN 値（「鍵」）をゼロパディングする必要があります。Cisco IOS Classic は、ユーザーの CKN 鍵値をゼロパディングし、設定された CKN 値の後にゼロを追加して 64 桁の 16 進数にします。CKN 鍵値は、64 桁の 16 進数にする必要があります。

次に、Cisco IOS Classic デバイスでの CKN key-string の設定例を示します。

```
config t
key chain KEYCHAINONE macsec
key 1234
cryptographic-algorithm aes-128-cmac
key-string 123456789ABCDEF0123456789ABCDEF0
lifetime local 12:21:00 Sep 9 2015 infinite
```

上記の例で、Cisco IOS Classic デバイスでの **show mka session** コマンドの出力を次に示します。

```
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
===============================================================================
Gi1/1        4c0.f983.6c81/0001   POLICYONE       NO              YES
1            54a2.7498.5b01/0001  1               Secured         123400000000000
                                                                  0000000000000000
                                                                  00000000000000000
                                                                  0000000000000000
```

次に、Cisco IOS Classic デバイスとの相互運用性を実現するための Cisco IOS XE デバイスの設定例を示します。

```
config t
key chain KEYCHAINONE macsec
key 12340000000000000000000000000000000000000000000000000000000000000000
cryptographic-algorithm aes-128-cmac
key-string 123456789ABCDEF0123456789ABCDEF0
lifetime local 12:21:00 Sep 9 2015 infinite
```

上記の例で、Cisco IOS XE デバイスでの **show mka session** コマンドの出力を次に示します。

```
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
=========================================================================
Gi1/1        34c0.f983.6c81/0001  POLICYONE       NO             YES
1            54a2.7498.5b01/0001  1               Secured        1234000000000000000
                                                                 0000000000000000000
                                                                 0000000000000000
                                                                 0000000000000
```

MKA ポリシーの設定

手順の概要

1. **configure terminal**
2. **mka policy** *policy name*
3. **send-secure-announcements**
4. **key-server** *priority*
5. **include-icv-indicator**
6. **macsec-cipher-suite** *gcm-aes-128*
7. **confidentiality-offset** *Offset value*
8. **end**
9. **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	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mka policy** *policy name*	MKA ポリシーを指定し、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 ビットのみの暗号を含めることを強くお勧めします。

	コマンドまたはアクション	目的
ステップ 3	**send-secure-announcements**	セキュアなアナウンスを有効にしました。 （注） デフォルトでは、セキュアなアナウンスは無効になっています。
ステップ 4	**key-server** *priority*	MKA 鍵サーバーオプションを設定し、プライオリティを設定します（0 ～ 255 の間）。 （注） 鍵サーバープライオリティの値を 255 に設定した場合、ピアは鍵サーバーになることはできません。鍵サーバーの優先順位の値は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	**include-icv-indicator**	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 no 形式（**no include-icv-indicator**）を使用します。
ステップ 6	**macsec-cipher-suite** *gcm-aes-128*	128 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。
ステップ 7	**confidentiality-offset** *Offset value*	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。
ステップ 8	**end**	特権 EXEC モードに戻ります。
ステップ 9	**show mka policy**	入力内容を確認します。

例

次に、MKA ポリシーを設定する例を示します。

```
Switch(config)# mka policy mka_policy
Switch(config-mka-policy)# key-server priority 200
Switch(config-mka-policy)# macsec-cipher-suite gcm-aes-128
Switch(config-mka-policy)# confidentiality-offset 30
Switch(config-mka-policy)# end
```

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. **configureterminal**
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*
19. **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	**enable** 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	**configureterminal** 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	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 1/0/1`	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	**switchport access vlan***vlan-id* 例： `Device(config-if)# switchport access vlan 1`	このポートのアクセス VLAN を設定します。
ステップ 5	**switchport mode access** 例： `Device(config-if)# switchport mode access`	インターフェイスをアクセス ポートとして設定します。

	コマンドまたはアクション	目的
ステップ 6	**macsec** 例： `Device(config-if)# macsec`	インターフェイス上で 802.1ae MACsec を有効にします。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	**authentication event linksec fail action authorize vlan** *vlan-id* 例： `Device(config-if)# authentication event linksec fail action authorize vlan 1`	（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	**authentication host-mode multi-domain** 例： `Device(config-if)# authentication host-mode multi-domain`	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	**authentication linksec policy must-secure** 例： `Device(config-if)# authentication linksec policy must-secure`	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 *should secure* です。
ステップ 10	**authentication port-control auto** 例： `Device(config-if)# authentication port-control auto`	ポートでの 802.1x 認証を有効にします。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	**authentication periodic** 例： `Device(config-if)# authentication periodic`	（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	**authentication timer reauthenticate** 例： `Device(config-if)# authentication timer reauthenticate`	（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	**authentication violation protect** 例： `Device(config-if)# configure terminal`	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	**mka policy** *policy-name* 例： `Device(config-if)# mka policy mka_policy`	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 を有効にします。MKA ポリシーを設定しなかった場合

	コマンドまたはアクション	目的
		（**mka policy** 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	**dot1x pae authenticator** 例： `Device(config-if)# dot1x pae authenticator`	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	**spanning-tree portfast** 例： `Device(config-if)# spanning-tree portfast`	関連するすべてのVLAN内のインターフェイスで、スパニングツリー Port Fast を有効にします。Port Fast機能が有効の場合、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、中間のスパニングツリーステートは変わりません
ステップ 17	**end** 例： `Device(config)# 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。
ステップ 18	**show authentication session interface** *interface-id* 例： `Device# show authentication session interface GigabitEthernet 1/0/1`	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。
ステップ 19	**show mka sessions** 例： `Device# show mka sessions`	確立された MKA セッションを確認します。

事前共有鍵（PSK）を使用した MACsec MKA の設定

手順の概要

1. **configure terminal**
2. **key chain** *key-chain-name* **macsec**
3. **key** *hex-string*
4. **cryptographic-algorithm** {*gcm-aes-128* | *gcm-aes-256*}
5. **key-string** { [0|6|7] *pwd-string* | *pwd-string*}
6. **lifetime local** [*start timestamp {hh::mm::ss* | *day* | *month* | *year}*] [**duration** *seconds* | *end timestamp {hh::mm::ss* | *day* | *month* | *year*}]
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	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**key chain** *key-chain-name* **macsec**	鍵チェーンを設定して、鍵 チェーン コンフィギュレーション モードを開始します。
ステップ 3	**key** *hex-string*	鍵チェーン内の各キーの固有識別子を設定し、鍵チェーンのキー コンフィギュレーション モードを開始します。 （注） 128 ビット暗号の場合は、32 文字の 16 進数 key-string を使用します。256 ビット暗号の場合は、64 文字の 16 進数 key-string を使用します。
ステップ 4	**cryptographic-algorithm** {*gcm-aes-128* | *gcm-aes-256*}	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 5	**key-string** { [0|6|7] *pwd-string* | *pwd-string*}	鍵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 6	**lifetime local** [*start timestamp {hh::mm::ss | day | month | year}*] [**duration** *seconds* | *end timestamp {hh::mm::ss | day | month | year}*]	事前共有鍵の有効期間を設定します。
ステップ 7	**end**	特権 EXEC モードに戻ります。

例

次に例を示します。

```
Switch(config)# Key chain keychain1 macsec
Switch(config-key-chain)# key 1000
Switch(config-keychain-key)# cryptographic-algorithm gcm-aes-128
Switch(config-keychain-key)# key-string 12345678901234567890123456789012
Switch(config-keychain-key)# lifetime local 12:12:00 July 28 2016 12:19:00 July 28 2016

Switch(config-keychain-key)# end
```

PSK を使用した、インターフェイスでの MACsec MKA の設定

（注） セッション間でトラフィックが破棄されないようにするには、**mka policy** コマンドを、**mka pre-shared-key key-chain** コマンドの前に設定する必要があります。

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **macsec access-control should-secure**
4. **macsec**
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	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	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	**macsec access-control should-secure**	（任意）MKA セッションが保護されるまで、暗号化されていないトラフィックのフローを許可します。MKA セッションが保護された後、暗号化されたトラフィックのフローのみが許可されます。デフォルトでは、MKAセッションが保護されるまで、トラフィックは破棄されます。 デフォルトの動作に戻すには、**no macsec access-control should-secure** コマンドを使用します。
ステップ 4	**macsec**	インターフェイス上で MACsec を有効にします。
ステップ 5	**mka policy** *policy-name*	MKA ポリシーを設定します。
ステップ 6	**mka pre-shared-key key-chain** *key-chain name*	MKA 事前共有鍵の鍵チェーン名を設定します。
ステップ 7	**macsec replay-protection window-size** *frame number*	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	**end**	特権 EXEC モードに戻ります。

例

次に、MKA ポリシーと MKA 事前共有鍵の鍵チェーン名を設定し、リプレイ保護の MACsec ウィンドウサイズを設定する例を示します。

```
Switch(config)# interface GigabitEthernet 1/1
Switch(config-if)# mka policy mka_policy
```

```
Switch(config-if)# mka pre-shared-key key-chain key-chain-name
Switch(config-if)# macsec replay-protection window-size 10
Switch(config-if)# end
```

（注） 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** コマンドを使用して、各参加ノードの macsec 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** 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。

次の例は、デフォルトの **must-secure** の代わりに **should-secure** を使用するようにインターフェイスを設定する方法と、デフォルトの **must-secure** に戻す方法を示しています。

（注） セッションが稼働している場合、**access-control** を変更することはできません。最初に **no macsec** コマンドを使用して MACsec 設定を削除し、次に **access-control** を設定する必要があります。

例 1：**must-secure** から **should-secure** に変更するには、次の手順を実行します。

```
Switch(config-if)#no macsec
Switch(config-if)#macsec access-control should-secure
Switch(config-if)#macsec // this switches the access-control from must-secure & restarts
 the macsec session with new behaviour.
```

例 2：**should-secure** から **must-secure** に変更するには、次の手順を実行します。

```
Switch(config-if)#no macsec
Switch(config-if)#no macsec access-control
Switch(config-if)#macsec
```

証明書ベース MACsec 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。

- 鍵ペアの生成
- SCEP による登録の設定
- 登録の手動設定
- 802.1x 認証の有効化と AAA の設定 （126 ページ）

• EAP-TLS プロファイルと 802.1x クレデンシャルの設定 （128 ページ）
• インターフェイスでの 802.1x MKA MACsec 設定の適用 （129 ページ）

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 証明書を生成するか、サードパーティ証明書を取得します。
• Cisco Identity Services Engine（ISE）が設定されていることを確認します。
• 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。

鍵ペアの生成

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto key generate rsa label** *label-name* **general-keys modulus** *size*
4. **end**
5. **show authentication session interface** *interface-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	**enable** 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	**configure terminal** 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	**crypto key generate rsa label** *label-name* **general-keys modulus** *size* 例： `Device(config)# crypto key generate rsa label general-keys modulus 2048`	署名および暗号化用に RSA 鍵ペアを作成します。 label キーワードを使用すると、各鍵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、鍵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、鍵ペアには <Default-RSA-Key> というラベルが自動的に付けられます。 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 鍵ペアを 1 つ生成します。法（modulus）が指定されていない場合は、デフォルトの鍵の法で

	コマンドまたはアクション	目的
		ある 1024 が使用されます。その他の法サイズを指定するには、modulus キーワードを使用します。
ステップ 4	**end** 例： `Device(config)# end`	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	**show authentication session interface** *interface-id* 例： `Device# show authentication session interface gigabitethernet 0/1/1`	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用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	**enable** 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	**configure terminal** 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	**crypto pki trustpoint** *server name* 例： `Device(config)# crypto pki trustpoint ka`	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	**enrollment url** *url name pem* 例： `Device(ca-trustpoint)# enrollment url http://url:80`	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、http:// [2001:DB8:1:1::1]:80 です。 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	**rsakeypair** key-label key-sizeencryption-key-size 例：	証明書に関連付ける鍵ペアを指定します。

	コマンドまたはアクション	目的
	`Device(ca-trustpoint)# rsakeypair exampleCAkeys`	• key-label 引数付きの鍵ペアがまだ存在しない、あるいは **auto-enroll regenerate** コマンドが発行された場合、登録時に key-label 引数付きの鍵ペアが生成されます。 • 鍵を生成するための *key-size* 引数を指定し、*encryption-key-size* 引数を指定して、個別の暗号化、署名鍵、および証明書を要求します。key-size と encryption-key-size は同じサイズでなければなりません。2048 未満の長さを指定することは推奨されません。 （注） **rsakeypair** 名は、信頼ポイント名と一致している必要があります。 （注） このコマンドが有効でない場合に、FQDN 鍵ペアが使用されます。
ステップ 6	**serial-number none** 例： `Device(ca-trustpoint)# serial-number none`	**none** 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	**ip-address none** 例： `Device(ca-trustpoint)# ip-address none`	**none** 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	**revocation-check crl** 例： `Device(ca-trustpoint)# revocation-check crl`	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	**auto-enroll** *percent* **regenerate** 例： `Device(ca-trustpoint)# auto-enroll 90 regenerate`	自動登録を有効にします。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。 自動登録が有効でない場合、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。

	コマンドまたはアクション	目的
		名前付きの鍵がすでに存在する場合でも、証明書の新しい鍵を生成するには、regenerate キーワードを使用します。 ロールオーバー中の鍵ペアがエクスポート可能な場合、新しい鍵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、鍵ペアがエクスポート可能かどうかが示されます。「! RSA key pair associated with trustpoint is exportable.」 新しい鍵ペアは、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。
ステップ 10	**exit** 例： `Device(ca-trustpoint)# exit`	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	**crypto pki authenticate** *name* 例： `Device(config)# crypto pki authenticate myca`	CA 証明書を取得して、認証します。
ステップ 12	**end** 例： `Device(config)# end`	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	**show crypto pki certificate** *trustpoint name* 例： `Device# show crypto pki certificate ka`	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	**enable** 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	**configure terminal** 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# configure terminal`	
ステップ 3	**crypto pki trustpoint** *server name* 例： `Device# crypto pki trustpoint ka`	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	**enrollment url** *url-name* 例： `Device(ca-trustpoint)# enrollment url http://url:80`	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、http:// [2001:DB8:1:1::1]:80 です。 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	**rsakeypair** key-label key-sizeencryption-key-size 例： `Device(ca-trustpoint)# rsakeypair exampleCAkeys`	証明書に関連付ける鍵ペアを指定します。 • key-label 引数付きの鍵ペアがまだ存在しない、あるいは **auto-enroll regenerate** コマンドが発行された場合、登録時に key-label 引数付きの鍵ペアが生成されます。 • 鍵を生成するための *key-size* 引数を指定し、*encryption-key-size* 引数を指定して、個別の暗号化、署名鍵、および証明書を要求します。key-size と encryption-key-size は同じサイズでなければなりません。2048 未満の長さを指定することは推奨されません。 （注） **rsakeypair** 名は、信頼ポイント名と一致している必要があります。 （注） このコマンドが有効でない場合に、FQDN 鍵ペアが使用されます。
ステップ 6	**serial-number none** 例： `Device(ca-trustpoint)# serial-number none`	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	**ip-address none** 例： `Device(ca-trustpoint)# ip-address none`	**none** 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	**revocation-check crl** 例： `Device(ca-trustpoint)# revocation-check crl`	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。

	コマンドまたはアクション	目的
ステップ 9	**exit** 例： `Device(ca-trustpoint)# exit`	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	**crypto pki authenticate** *name* 例： `Device(config)# crypto pki authenticate myca`	CA 証明書を取得して、認証します。
ステップ 11	**crypto pki enroll** *name* 例： `Device(config)# crypto pki enroll myca`	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	**crypto pki import** *name* **certificate** 例： `Device(config)# crypto pki import myca certificate`	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。用途鍵証明書の場合、拡張子「-sign.crt」および「-encr.crt」が使用されます。 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。 （注） 一部の CA は、証明書要求の用途鍵情報を無視し、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鍵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 つの鍵ペアのいずれも使用しません。
ステップ 13	**end** 例： `Device(config)# end`	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。

	コマンドまたはアクション	目的
ステップ 14	**show crypto pki certificate** *trustpoint name* 例： `Device# show crypto pki certificate  ka`	信頼ポイントの証明書に関する情報を表示します。

802.1x 認証の有効化と AAA の設定

手順の概要

1. enable
2. configure terminal
3. aaa new-model
4. dot1x system-auth-control
5. radius server *name*
6. address *ip-address* auth-port *port-number* acct-port *port-number*
7. automate-tester username username
8. key *string*
9. radius-server deadtime *minutes*
10. exit
11. aaa group server radius *group-name*
12. server *name*
13. exit
14. aaa authentication dot1x default group *group-name*
15. aaa authorization network default group *group-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	enable 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	configure terminal 例： `Device# configure terminal`	グローバル設定モードを開始します。
ステップ 3	aaa new-model 例： `Device(config)# aaa new-model`	AAA を有効にします。
ステップ 4	dot1x system-auth-control 例： `Device(config)# dot1x system-auth-control`	デバイス上で 802.1X を有効にします。

	コマンドまたはアクション	目的
ステップ 5	radius server *name* 例： `Device(config)# radius server ISE`	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。
ステップ 6	address *ip-address* auth-port *port-number* acct-port *port-number* 例： `Device(config-radius-server)# address ipv4 <ISE ipv4 address> auth-port 1645 acct-port 1646`	RADIUS サーバのアカウンティング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 7	automate-tester username username 例： `Device(config-radius-server)# automate-tester username dummy`	RADIUS サーバーの自動テスト機能を有効にします。 このようにすると、デバイスは RADIUS サーバーにテスト認証メッセージを定期的に送信し、サーバーからの RADIUS 応答を待機します。成功メッセージは必須ではありません。認証失敗であっても、サーバーが稼働していることを示しているため問題ありません。
ステップ 8	key *string* 例： `Device(config-radius-server)# key dummy123`	デバイスと RADIUS サーバーとの間におけるすべての RADIUS 通信用の認証および暗号鍵を指定します。
ステップ 9	radius-server deadtime *minutes* 例： `Device(config-radius-server)# radius-server deadtime 2`	いくつかのサーバが使用不能になったときの RADIUS サーバの応答時間を短くし、使用不能になったサーバがすぐにスキップされるようにします。
ステップ 10	exit 例： `Device(config-radius-server)# 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 11	aaa group server radius *group-name* 例： `Device(config)# aaa group server radius ISEGRP`	異なる RADIUS サーバ ホストを別々のリストと方式にグループ化し、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 12	server *name* 例： `Device(config-sg)# server name ISE`	RADIUS サーバ名を割り当てます。
ステップ 13	exit 例： `Device(config-sg)# 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。

	コマンドまたはアクション	目的
ステップ 14	aaa authentication dot1x default group *group-name* 例： `Device(config)# aaa authentication dot1x default group ISEGRP`	IEEE 802.1x 用にデフォルトの認証サーバ グループを設定します。
ステップ 15	aaa authorization network default group *group-name* 例： `aaa authorization network default group ISEGRP`	ネットワーク認証のデフォルト グループを設定します。

EAP-TLS プロファイルと 802.1x クレデンシャルの設定

手順の概要

1. enable
2. configure terminal
3. eap profile *profile-name*
4. method tls
5. pki-trustpoint name
6. exit
7. dot1x credentials *profile-name*
8. username username
9. pki-trustpoint 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	enable 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	configure terminal 例： `Device# configure terminal`	グローバル設定モードを開始します。
ステップ 3	eap profile *profile-name* 例： `Device(config)# eap profile EAPTLS-PROF-IOSCA`	EAP プロファイルを設定し、EAP 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 4	method tls 例： `Device(config-eap-profile)# method tls`	デバイスで EAP-TLS 方式を有効にします。

	コマンドまたはアクション	目的
ステップ 5	pki-trustpoint name 例： `Device(config-eap-profile)# pki-trustpoint POLESTAR-IOS-CA`	デフォルトの PKI トラストポイントを設定します。
ステップ 6	exit 例： `Device(config-eap-profile)# 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 7	dot1x credentials *profile-name* 例： `Device(config)# dot1x credentials EAPTLSCRED-IOSCA`	802.1x クレデンシャルプロファイルを設定し、dot1x クレデンシャル 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	username username 例： `Device(config-dot1x-cred)# username asr1000@polestar.company.com`	認証ユーザ ID を設定します。
ステップ 9	pki-trustpoint name 例： `Device(config-dot1x-cred)# pki-trustpoint POLESTAR-IOS-CA`	デフォルトの PKI トラストポイントを設定します。
ステップ 10	end 例： `Device(config-dot1x-cred)# end`	特権 EXEC モードに戻ります。

インターフェイスでの 802.1x MKA MACsec 設定の適用

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	enable 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	configure terminal 例： `Device# configure terminal`	グローバル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 3	interface *interface-id* 例： `Device(config)# interface gigabitethernet 2/9`	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	macsec 例： `Device(config-if)# macsec`	インターフェイス上で MACsec を有効にします。
ステップ 5	authentication periodic 例： `Device(config-if)# authentication periodic`	（任意）このポートの再認証を有効にします。
ステップ 6	authentication timer reauthenticate interval 例： `Device(config-if)# authentication timer reauthenticate interval`	（任意）再認証間隔を設定します。
ステップ 7	access-session host-mode multi-domain 例： `Device(config-if)# access-session host-mode multi-domain`	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	**access-session closed** 例： `Device(config-if)# access-session closed`	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	access-session port-control auto 例： `Device(config-if)# access-session port-control auto`	ポートの認可状態を設定します。
ステップ 10	dot1x pae both 例： `Device(config-if)# dot1x pae both`	ポートを 802.1X ポート アクセス エンティティ（PAE）のサプ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	dot1x credentials profile 例： `Device(config-if)# dot1x credentials EAPTLSCRED-IOSCA`	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	dot1x supplicant eap profile name 例： `Device(config-if)# dot1x supplicant eap profile EAPTLS-PROF-IOSCA`	EAP-TLS プロファイルをインターフェイスに割り当てます。

	コマンドまたはアクション	目的
ステップ 13	dot1x authenticator eap profile name 例： `Device(config-if)# dot1x authenticator eap profile EAPTLS-PROF-IOSCA`	802.1x 認証時に使用する EAP プロファイルを割り当てます。
ステップ 14	service-policy type control subscriber control-policy name 例： `Device(config-if)# service-policy type control subscriber DOT1X_POLICY_RADIUS`	インターフェイスに加入者制御ポリシーを適用します。
ステップ 15	exit 例： `Device(config-if)# exit`	特権 EXEC モードに戻ります。
ステップ 16	show macsec interface interface-id 例： `Device# show macsec interface GigabitEthernet 2/9`	インターフェイスの MACsec の詳細を表示します。
ステップ 17	**show access-session interface** *interface-id* **details** 例： `Device# show access-session interface GigabitEthernet 2/9 details`	dot1x 認証および認可が成功したことを確認します。これは最初に確認することです。dot1x 認証が失敗すると、MKA は開始されません。
ステップ 18	**show mka session interface** *interface-id* **details** 例： `Device# show mka session interface GigabitEthernet 2/9 details`	詳細な MKA セッションステータスを表示します。

例：スイッチ間証明書ベース MACsec

スイッチ間証明書ベースの MACsec の設定例を次に示します。

```
configure terminal
aaa new-model
aaa local authentication default authorization default
!
!
aaa authentication dot1x default group radius local
aaa authorization exec default local
aaa authorization network default group radius local
aaa authorization auth-proxy default group radius
aaa authorization credential-download default local
aaa accounting identity default start-stop group radius
!
!
aaa attribute list MUSTS
 attribute type linksec-policy must-secure
!
aaa attribute list macsec-dot1-credentials
```

```
 attribute type linksec-policy must-secure
!
aaa attribute list MUSTS_CA
 attribute type linksec-policy must-secure
!
aaa attribute list SHOULDS_CA
 attribute type linksec-policy should-secure
!
aaa attribute list mkadt_CA
 attribute type linksec-policy must-secure
!
aaa session-id common

username MUST aaa attribute list MUSTS_CA
username MUSTS.mkadt.cisco.com

crypto pki trustpoint demo
 enrollment terminal
 serial-number
 fqdn MUSTS.mkadt.cisco.com
 subject-name cn=MUSTS.mkadt.cisco.com,OU=CSG Security,O=Cisco
Systems,L=Bengaluru,ST=KA,C=IN
 subject-alt-name MUSTS.mkadt.cisco.com
 revocation-check none
 rsakeypair demo 2048
 hash sha256

eap profile EAP_P
  method tls
 pki-trustpoint demo

dot1x system-auth-control
dot1x credentials MUSTS-CA
 username MUST
 password 0 MUST_CA
!
dot1x credentials MUSTS
 username MUSTS.mkadt.cisco.comcrypto pki authenticate demo

crypto pki authenticate
crypto pki enroll demo
crypto pki import demo certificate

policy-map type control subscriber MUSTS_1
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x both
 event authentication-failure match-all
  10 class always do-until-failure
   10 terminate dot1x
   20 authentication-restart 10
 event authentication-success match-all
  10 class always do-until-failure
   10 activate service-template DEFAULT_LINKSEC_POLICY_MUST_SECURE

interface GigabitEthernet2/9
 switchport mode access
 macsec
 access-session host-mode multi-host
 access-session closed
 access-session port-control auto
 dot1x pae both
 dot1x authenticator eap profile EAP_P
 dot1x credentials MUSTS
```

```
 dot1x supplicant eap profile EAP_P
 service-policy type control subscriber MUSTS_1
```

次に、スイッチ間証明書ベースの MACsec に対する **show mka sessions** コマンドの出力例を示します。

```
show mka sessions

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

=========================================================================================
Gi2/14          40ce.24b7.617d/0002  pol_1             NO                 YES

2               f8b7.e2e5.ad88/0002  1                 Secured
80690202D09A9801BE98FC89D5380098



show mka sessions interface GigabitEthernet2/14 detail

MKA Detailed Status for MKA Session
===================================
Status: SECURED - Secured MKA Session with MACsec

Local Tx-SCI.............. 40ce.24b7.617d/0002
Interface MAC Address.... 40ce.24b7.617d
MKA Port Identifier...... 2
Interface Name........... GigabitEthernet2/14
Audit Session ID......... 6514030B000000998FEDD629
CAK Name (CKN)........... 80690202D09A9801BE98FC89D538009800000000000000000000000000000000
Member Identifier (MI)... 534A6ECFBBA318B6423E49EB
Message Number (MN)...... 166
EAP Role................. Authenticator
Key Server............... YES
MKA Cipher Suite......... AES-128-CMAC

Latest SAK Status........ Rx & Tx
Latest SAK AN............ 0
Latest SAK KI (KN)....... 534A6ECFBBA318B6423E49EB00000001 (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)
SAK Rekey Time........... 0s (SAK Rekey interval not applicable)

MKA Policy Name.......... pol_1
Key Server Priority...... 0
Delay Protection......... NO
Delay Protection Timer.......... 0s (Not enabled)

Confidentiality Offset... 0
Algorithm Agility........ 80C201
SAK Rekey On Live Peer Loss........ NO
Send Secure Announcement.. DISABLED
SCI Based SSCI Computation.... NO
```

```
SAK Cipher Suite..... 0080C20001000002 (GCM-AES-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        RxSA
SSCI
                                                             Priority  Installed
  ---------------------------------------------------------------------------------------

  96E534A06B405442034B846E  163         f8b7.e2e5.ad88/0002  0         YES            0

Potential Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA
SSCI
                                                             Priority  Installed
  ---------------------------------------------------------------------------------------

Dormant Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA
SSCI
                                                             Priority  Installed
  ---------------------------------------------------------------------------------------

show access-session interface GigabitEthernet2/14 detail
            Interface:  GigabitEthernet2/14
               IIF-ID:  0x1398D40E
          MAC Address:  f8b7.e2e5.ad88
         IPv6 Address:  Unknown
         IPv4 Address:  Unknown
            User-Name:  MUST
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-host
     Oper control dir:  both
      Session timeout:  1800s (local), Remaining: 1470s
       Timeout action:  Reauthenticate
    Common Session ID:  6514030B000000998FEDD629
      Acct Session ID:  0x0000000e
               Handle:  0x5900003a
       Current Policy:  MUSTS_1


Local Policies:
                Service Template: DEFAULT_LINKSEC_POLICY_MUST_SECURE (priority 150)

Server Policies:
      Security Policy:  Must Secure
      Security Status:  Link Secured


Method status list:
       Method           State
        dot1x           Authc Success
     dot1xSup           Authc Success
```

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. **configure terminal**
2. **interface** *interface-id*
3. **macsec**
4. **mka policy** *policy-name*
5. **mka pre-shared-key key-chain** *key-chain-name*
6. **channel-group** *channel-group-number* **mode {active | passive } | {on }**
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	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	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	**macsec**	インターフェイス上で MACsec を有効にします。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 4	**mka policy** *policy-name*	MKA ポリシーを設定します。
ステップ 5	**mka pre-shared-key key-chain** *key-chain-name*	MKA 事前共有鍵の鍵チェーン名を設定します。 （注） MKA 事前共有鍵は、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。
ステップ 6	**channel-group** *channel-group-number* **mode {active | passive } | {on }**	チャネル グループ内にポートを設定し、モードを設定します。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。 • **on**：PAgP または LACP を使用せずにポートが強制的にチャネル化されます。on モードでは、使用可能な EtherChannel が存在するのは、on モードのポート グループが、on モードの別のポート グループに接続する場合だけです。

	コマンドまたはアクション	目的
		• **active**：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。 • **passive**：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。
ステップ 7	**end**	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. **configure terminal**
2. **[no] interface port-channel** *channel-group-number*
3. **switchport**
4. **switchport mode {access | trunk }**
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	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**[no] interface port-channel** *channel-group-number*	ポート チャネル インターフェイスを作成します。 （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 no 形式を使用します。
ステップ 3	**switchport**	レイヤ 3 モードになっているインターフェイスを、レイヤ 2 設定のレイヤ 2 モードに切り替えます。

	コマンドまたはアクション	目的
ステップ 4	**switchport mode {access | trunk }**	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 5	**end**	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. **configure terminal**
2. **interface port-channel** *interface-id*
3. **no switchport**
4. **ip address** *ip-address subnet_mask*
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	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface port-channel** *interface-id*	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no switchport**	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 4	**ip address** *ip-address subnet_mask*	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 5	**end**	特権 EXEC モードに戻ります。

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。

```
key chain KC macsec
  key 1000
    cryptographic-algorithm aes-128-cmac
    key-string FC8F5B10557C192F03F60198413D7D45
    end
```

```
mka policy POLICY
  key-server priority 0
  macsec-cipher-suite gcm-aes-128
  confidentiality-offset 0
  end

interface Te1/0/1
  channel-group 2 mode on
  macsec
  mka policy POLICY
  mka pre-shared-key key-chain KC
  end

interface Te1/0/2
  channel-group 2 mode on
  macsec
  mka policy POLICY
  mka pre-shared-key key-chain KC
  end
```

レイヤ 2 EtherChannel 設定

デバイス 1

```
interface port-channel 2
 switchport
 switchport mode trunk
 no shutdown
 end
```

デバイス 2

```
interface port-channel 2
 switchport
 switchport mode trunk
 no shutdown
 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)
```

レイヤ 3 EtherChannel 設定

デバイス 1

```
interface port-channel 2
 no switchport
 ip address 10.25.25.3 255.255.255.0
 no shutdown
 end
```

デバイス 2

```
interface port-channel 2
 no switchport
 ip address 10.25.25.4 255.255.255.0
 no shutdown
 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。

```
key chain KC macsec
  key 1000
    cryptographic-algorithm aes-128-cmac
    key-string FC8F5B10557C192F03F60198413D7D45
    end

mka policy POLICY
  key-server priority 0
  macsec-cipher-suite gcm-aes-128
  confidentiality-offset 0
  end

interface Te1/0/1
  channel-group 2 mode active
  macsec
  mka policy POLICY
  mka pre-shared-key key-chain KC
  end

interface Te1/0/2
  channel-group 2 mode active
  macsec
  mka policy POLICY
  mka pre-shared-key key-chain KC
  end
```

レイヤ 2 EtherChannel 設定

デバイス 1

```
interface port-channel 2
 switchport
 switchport mode trunk
 no shutdown
 end
```

デバイス 2

```
interface port-channel 2
 switchport
 switchport mode trunk
 no shutdown
 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

```
interface port-channel 2
 no switchport
 ip address 10.25.25.3 255.255.255.0
 no shutdown
 end
```

デバイス 2

```
interface port-channel 2
 no switchport
 ip address 10.25.25.4 255.255.255.0
 no shut
```

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)          LACP      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。

```
# 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
```

MACsec 暗号アナウンスメントの設定

セキュアアナウンスメントの MKA ポリシーの設定

手順の概要

1. **configure terminal**
2. **mka policy** *policy-name*
3. **key-server** *priority*
4. **[no] send-secure-announcements**
5. **macsec-cipher-suite** {*gcm-aes-128* | *gcm-aes-256*}
6. **end**
7. **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	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**mka policy** *policy-name*	MKA ポリシーを指定し、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 ビットのみの暗号を含めることを強くお勧めします。

	コマンドまたはアクション	目的
ステップ 3	**key-server** *priority*	MKA 鍵サーバーオプションを設定し、プライオリティを設定します（0 ～ 255 の間）。 （注） 鍵サーバープライオリティの値を 255 に設定した場合、ピアは鍵サーバーになることはできません。鍵サーバーの優先順位の値は 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 4	**[no] send-secure-announcements**	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 no 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 5	**macsec-cipher-suite** {*gcm-aes-128* | *gcm-aes-256*}	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 6	**end**	特権 EXEC モードに戻ります。
ステップ 7	**show mka policy**	入力内容を確認します。

セキュアアナウンスメントのグローバル設定（すべての MKA ポリシー）

手順の概要

1. **configure terminal**
2. **[no] mka defaults policy send-secure-announcements**
3. **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	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**[no] mka defaults policy send-secure-announcements**	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 3	**end**	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

手順の概要

1. **configure terminal**
2. **interface** *interface-id*
3. **[no] eapol annoucement**
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	**configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** *interface-id*	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 3	**[no] eapol annoucement**	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 no 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 4	**end**	特権 EXEC モードに戻ります。

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。

```
# configure terminal
(config)# mka policy mka_policy
(config-mka-policy)# key-server 2
(config-mka-policy)# send-secure-announcements
(config-mka-policy)#macsec-cipher-suite gcm-aes-128confidentiality-offset 0
(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。

```
# configure terminal
(config)# mka defaults policy send-secure-announcements
(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。

```
# configure terminal
(config)# interface GigabitEthernet 1/0/1
(config-if)# eapol announcement
(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。

```
# 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。

```
# 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)...........
0100000000000000000000000000000000000000000000000000000000000000
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。

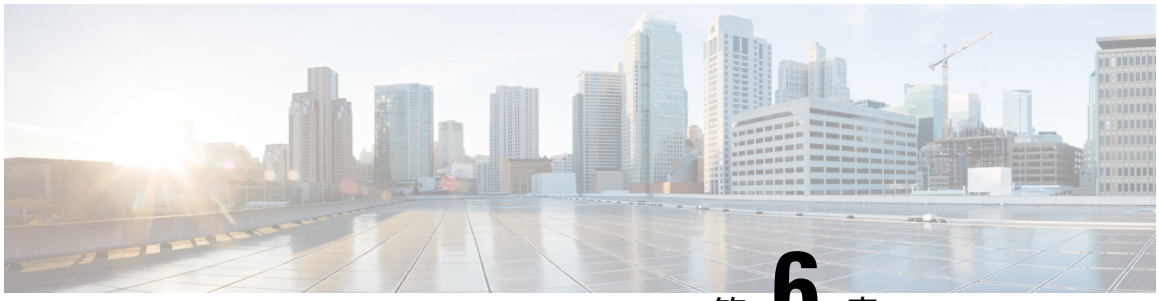
```
# show mka sessions details
MKA Detailed Status for MKA Session
===================================
Status: SECURED - Secured MKA Session with MACsec

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、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。

```
# 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
```



第 6 章

Cisco Secure Cloud Analytics コネクタの設定

- Cisco Connector for Secure Cloud Analytics の設定 （149 ページ）
- トラブルシューティング （151 ページ）

Cisco Connector for Secure Cloud Analytics の設定

Cisco Secure Cloud Analytics（旧称 Stealthwatch Cloud）は、悪意のある各種アクティビティをリアルタイムで特定するために必要な、実用的なセキュリティインテリジェンスと可視性を提供します。セキュリティインシデントが壊滅的な侵害になる前に迅速に対応できます。このガイドでは、シスコ産業用イーサネットスイッチでの IOS-XE での Cisco Cloud Connector の設定手順について説明します。

（注） Cisco Secure Cloud Analytics（Stealthwatch Cloud）または Cisco Secure Network Analytics（Stealthwatch）の詳細については、次の URL を参照してください。https://www.cisco.com/c/en/us/products/security/stealthwatch/index.html

制限事項と制約事項

- 事前に定義された一連のフィールドのみを収集できます。対象のフィールドには、送信元 IP、送信元ポート、宛先 IP、宛先ポートおよびプロトコルの 9 タプルフローデータと、フロー開始、フロー終了、パケット数、およびバイト数が含まれます。
- 必須フィールドは、CLI の制限では適用されません。レコードにすべての必須フィールドがなく、9 タプルデータを収集できない場合、そのフローは破棄されます。
- Cisco Secure Cloud Analytics 用の StealthWatch コネクタは、スイッチのルーティング機能を使用して、クラウドサーバにパケットを送信します。追加のチェックは行われません。適切なルートが存在することを前提としています。

- モニタアプリケーションの観点から Flexible NetFlow 固有のモニタアプリケーションの制限は、Cisco Secure Cloud Analytics にも当てはまります。例：SVI なし、VLAN なし、送信モニタなし。
- クラウドエクスポータを他のエクスポータと一緒に使用することはできません。
- アップロードされたファイルの命名規則には、すべてのファイルを一意に識別し、ファイルの上書きを防ぐためのランダムな文字列が含まれています。例：https://sensor.ext.obsrvbl.com/sign/ios-xe-17-2/2019/7/5/00:00:00/hostname-random_suffix.csv.gz。1 分ごとに集約されてアップロードされます。

始める前に

Cisco Secure Cloud Analytics コネクタは、IE3300、IE3400、IE3400H スイッチでのみサポートされます。

- Network Advantage および Cisco DNA Advantage ライセンス

手順の概要

1. stealthwatch-cloud-monitor service-key <you service key> hostname my_sensor
2. flow record SWCRec
3. flow exporter SWCExp
4. interface gi1/0/3

手順の詳細

	コマンドまたはアクション	目的

ステップ 1	stealthwatch-cloud-monitor service-key <you service key> hostname my_sensor
	例：
	`stealthwatch-cloud-monitor`
	`  service-key <you service key>`
	`  hostname my_sensor`
	`  url https://sensor.ext.obsrvbl.com`
	`openssl s_client -showcerts -connect https://sensor.ext.obsrvbl.com:443`
	`openssl s_client -showcerts -connect s3.ap-southeast-2.amazonaws.com:443`
	例：
	`openssl s_client -showcerts -connect https://sensor.ext.obsrvbl.com:443`
	`openssl s_client -showcerts -connect s3.ap-southeast-2.amazonaws.com:443`
		URL に基づいて有効なルート CA をインストールしてください。以下の CLI を使用して、URL に従ってルート CA を把握してください
		センサーの登録に使用されるサービス鍵とホスト名を設定します。ホスト名を指定しない場合は、ボックスのシリアル番号が登録に使用されます。

ステップ 2	flow record SWCRec
	例：
	`flow record SWCRec`
	`match ipv4 source address`
		Cisco Secure Cloud Analytics レコードのデータを収集するためのフローレコードのフィールドを設定します。

	コマンドまたはアクション	目的
	match ipv4 destination address match transport source-port match transport destination-port match ipv4 protocol collect counter bytes long collect counter packets long collect timestamp sys first collect timestamp sys last	
ステップ 3	flow exporter SWCExp 例： flow exporter SWCExp destination stealthwatch-cloud flow monitor SWCMon flow record SWCRec flow exporter SWCExp	Cisco Secure Cloud Analytics エクスポータを設定し、フローモニタに接続して、Secure Cloud へのエクスポートを開始します。
ステップ 4	interface gi1/0/3 例： Interface gi1/0/3 ip flow monitor SWCMon input	フローをモニタするインターフェイスを特定し、Cisco Secure Cloud Analytics エクスポータがあるモニタをそのインターフェイスに接続します。

次のタスク

Cisco Secure Cloud Analytics の詳細情報については、該当するコンフィギュレーション ガイドを参照してください。https://www.cisco.com/c/en/us/support/security/stealthwatch-cloud/products-installation-and-configuration-guides-list.html

トラブルシューティング

- デバッグログは「debug Stealthwatch」CLI を使用して有効にできます。

```
switch#debug stealthwatch-cloud ?
  all          All debugs for SWC
  cert         Certificate Validation
  error        errors
  event        Events
  file-events  File notifications
```

- プラットフォームレベルのデバッグでは、「debug platform software swc」CLI を使用できます。

```
switch#debug platform software swc ?
  all         all
  errors      Stealthwatch Cloud errors
  events      Stealthwatch Cloud events
  pkt-events  Stealthwatch Cloud data collection events
```

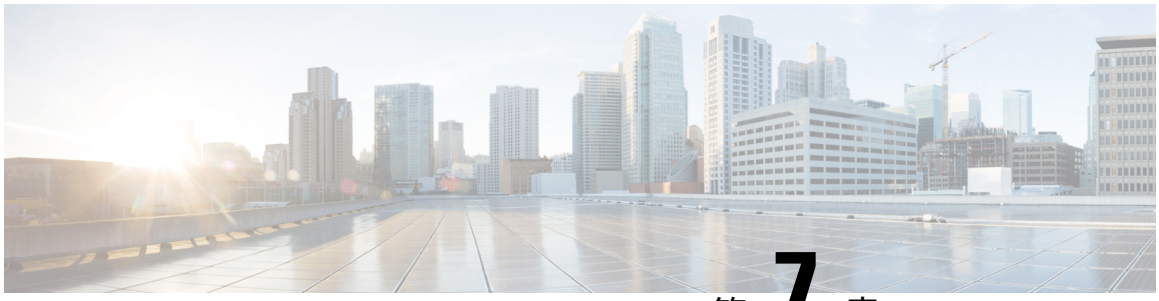
コマンドの表示

- **Switch-1# show stealthwatch-cloud detail**

```
========================================
Stealthwatch Cloud Parameters
========================================
   Service Key  : x8SS2q7e4twpcNWT35AsL6i6xHd24iXJvICo3N4sGx1U1pCqqs
   Sensor Name  : petra
   URL          : https://sensor.anz-prod.obsrvbl.com
========================================
Stealthwatch Cloud Sensor Info
========================================
   Sensor Status    : Registered
   Last heartbeat   : 2020-05-08T12:11:50
```

- **Switch-1# show platform software swc stats**

```
==========================
SWC Upload Statistics:
==========================
1 : Last file uploaded          :  202005081212_ufihi2
2 : Time of upload              :  202005081213 UTC
3 : Current file uploading      :
4 : Files queued for upload     :
5 : Number of files queued      :  0
6 : Last failed upload          :
7 : Files failed to upload      :  0
8 : Files successfully uploaded :  416
==========================
SWC File Creation Statistics:
==========================
9 : Last file created           :  202005081212_ufihi2
10: Time of creation            :  202005081212 UTC
==========================
SWC Flow Statistics:
==========================
11: Number of flows in prev file:  1
12: Number of flows in curr file:  0
13: Invalid dropped flows       :  0
==========================
SWC Flags:
==========================
14: Is Registered               :  Registered
15: File Delete         :  Enabled
16: Exporter            :  Enabled
```



第 7 章

SGACL ロギングの設定

- SGACL ロギング （153 ページ）
- 前提条件 （155 ページ）
- 注意事項と制約事項 （155 ページ）
- SGACL ロギングの設定 （155 ページ）
- 機能の履歴 （156 ページ）

SGACL ロギング

セキュリティグループベースのアクセスコントロールリスト（SGACL）ロギングは、Cisco IOS XE リリース 17.8.1 以降の Cisco IE3400 および IE3400H シリーズ スイッチでサポートされています。SGACL ロギングのサポートには、次の FPGA プロファイルのいずれかがスイッチでアクティブ化されていることも必要です。

- デフォルト プロファイル
- CTS-IPv6 プロファイル

FPGA プロファイルの詳細については、『System Management Configuration Guide, Cisco Catalyst IE3x00 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches』を参照してください。

セキュリティグループアクセスコントロールリスト（SGACL）はポリシーの適用方法です。これによって管理者は、セキュリティグループの割り当てと宛先リソースに基づいてユーザーが実行する操作を制御できます。SGACL は Cisco TrustSec セキュリティアーキテクチャのコンポートで、信頼できるネットワークデバイスのドメインを確立することによって安全なネットワークを構築します。TrustSec の前提条件、ガイドラインと制限事項、設定手順など、TrustSec に関する包括的な情報については、『Cisco TrustSec Configuration Guide』を参照してください。

ロギング対応アクセスコントロールリスト（ACL）により、ネットワークを通過する、またはネットワークデバイスによって廃棄されたときのトラフィックを詳細に理解できます。ロールベースの IPv4/v6 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、デバイスによって表示されます。つまり、SGACL 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。アクセスコントロール エントリ（ACE）に log キーワードが含まれている場合のみ、ロギングがトリガーされま

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。

次に、ロギング用に設定された特定の ACE が一致した後に生成される syslog メッセージの例を示します。

```
*Jun 18 10:17:22.205: %RBM-6-SGACLHIT: ingress_interface='' sgacl_name='testv4'
action='Permit'
 protocol='udp' src-vrf='default' src-ip='25.1.1.1' src-port='96' dest-vrf='default'
dest-ip='25.1.1.2'
dest-port='0' sgt='100' dgt='200' logging_interval_hits='12'
```

ロギングメッセージには、アクセスリスト名、パケットが許可されたか拒否されたか、パケットの送信元と宛先の IP アドレス、およびセキュリティグループタグ（SGT）と宛先グループタグ（DGT）に関する情報が含まれます。

次の表に、スイッチでサポートされる IPv4/v6 ロールベース ACL の ACE 動作のタイプを示します。log キーワードは個々の ACE に適用され、ACE に一致するパケットがログに記録されます。**log** キーワードで記録された最初のパケットは、syslog メッセージを生成します。

（注） SGACL ロギングは、OR 論理演算子を使用した ACE でサポートされます。SGACL ロギングは、AND 論理演算子を使用した操作ではサポートされません。

SGACL コマンド	説明
permit/deny tcp src eq <src-port> または dst eq <dst-port> log	指定された送信元ポートまたは宛先ポートに基づいて TCP パケットを照合します。
permit/deny udp src eq <src-port> または dst eq <dst-port> log	指定された送信元ポートまたは宛先ポートに基づいて UDP パケットを照合します。
permit/deny tcp src range <start-port> <end-port> または dst range <start-port> <end-port> log	指定された送信元ポートまたは宛先ポートの範囲に基づいて TCP パケットを照合します。
permit/deny udp src range <start-port> <end-port> または dst range <start-port> <end-port> log	指定された送信元ポートまたは宛先ポートの範囲に基づいて UDP パケットを照合します。
Permit/deny tcp src gt/lt <src-port> または dst gt/lt <dst-port> log	指定された送信元ポートより大きいか小さい、または指定された宛先ポートより大きいか小さい TCP パケットを照合します。
Permit/deny udp src gt/lt <src-port> または dst gt/lt <dst-port> log	指定された送信元ポートより大きいか小さい、または指定された宛先ポートより大きいか小さい UDP パケットを照合します。

前提条件

- SGACL ロギングには、次の FPGA プロファイルのいずれかがスイッチでアクティブ化されていることが必要です。
  - デフォルト プロファイル
  - CTS-IPv6 プロファイル

  FPGA プロファイルの詳細については、『System Management Configuration Guide, Cisco Catalyst IE3x00 Rugged, IE3400 Heavy Duty, and ESS3300 Series Switches』を参照してください。
- 「How to Configure Security Group ACL Policies」の説明に従って、セキュリティグループ ACL ポリシーを設定します

注意事項と制約事項

- FPGA は、インスタンスごとに最大 254 のエントリをサポートできます。
- ハードウェアの制限により、入力インターフェイスの Syslog エントリは空です。

SGACL ロギングの設定

SGACL ロギングを設定するには、次の手順を実行します。

ステップ 1 グローバル コンフィギュレーション モードを開始します。

例：

```
Switch# configure terminal
```

ステップ 2 システムで Cisco TrustSec 対応インターフェイスの SGACL 適用をグローバルに有効または無効にするには、**cts role-based enforcement** コマンドを使用します。

ステップ 3 SGACL のロギング間隔を設定するには、次のように入力します。

cts role-based enforcement [logging-interval *interval*]

interval 引数の有効な値は 5 ～ 86400 秒です。デフォルトは 300 秒です。

例：

```
Switch(config)# cts role-based enforcement logging-interval 90
```

ステップ 4 （任意）**logging rate-limit** コマンドを使用して、1 秒あたりに記録されるメッセージのレートを制限できます。

例：

```
Switch(config)# logging rate-limit <seconds>
```

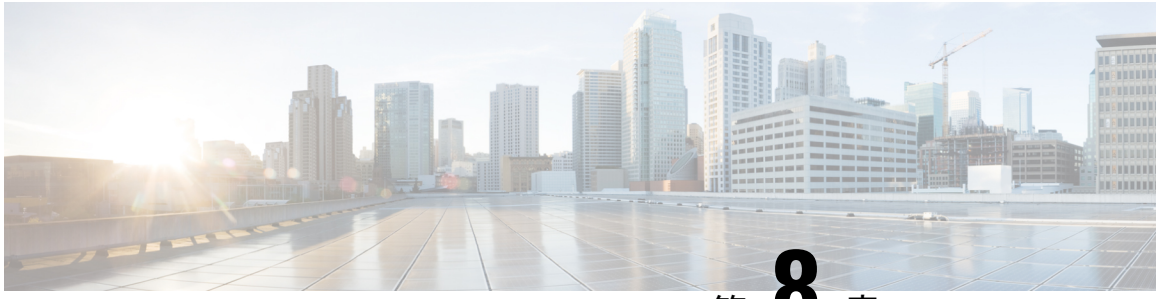
例

次に、送信元と宛先の SGT を表示するサンプルログを示します。ACE は拒否アクションと一致します。**logging rate-limit** コマンドを使用して、1 秒あたりに記録されるメッセージのレートを制限できます。

```
Switch(config)# cts role-based enforcement logging-interval 90
Switch(config)# logging rate-limit 20
May 27 10:19:21.509: %RBM-6-SGACLHIT:
ingress_interface='GigabitEthernet1/0' sgacl_name='sgacl2' action='Deny'
protocol='icmp' src-ip='16.16.1.3' src-port='8' dest-ip='17.17.1.2' dest-port='0'
sgt='101' dgt='202' logging_interval_hits='5'
```

機能の履歴

機能名	リリース	機能情報
SGACL ロギング	Cisco IOS XE 17.8.1	IE3400 および IE3400H での初期サポート



第 8 章

Cisco TrustSec VRF 対応 SGT

- VRF-Aware SXP （157 ページ）
- VRF 対応 SGT および SGACL の IPv6 サポート （158 ページ）
- Cisco TrustSec VRF 対応 SGT の設定方法 （160 ページ）
- Cisco TrustSec VRF 対応 SGT の設定例 （161 ページ）
- ACE ポート範囲 （161 ページ）
- 例：ACE ポート範囲のロールベース アクセス リスト コマンド （162 ページ）
- Cisco TrustSec VRF 対応 SGT の機能履歴 （162 ページ）

VRF-Aware SXP

仮想ルーティングおよびフォワーディング（VRF）のセキュリティグループタグ（SGT）Exchange Protocol（SXP）の実装は、特定の VRF と SXP 接続をバインドします。Cisco TrustSec を有効にする前に、ネットワーク トポロジがレイヤ 2 またはレイヤ 3 の VPN に対して正しく設定されており、すべての VRF が設定されていることを前提としています。

SXP VRF サポートは、次のようにまとめることができます。

- 1 つの VRF には 1 つの SXP 接続のみをバインドできます。
- 別の VRF が重複する SXP ピアまたは送信元 IP アドレス持つ可能性があります。
- 1 つの VRF で学習（追加または削除）された IP-SGT マッピングは、同じ VRF ドメインでのみ更新できます。SXP 接続は異なる VRF にバインドされたマッピングを更新できません。SXP 接続が VRF で終了しない場合は、その VRF の IP-SGT マッピングは SXP によって更新されません。
- VRF ごとに複数のアドレス ファミリがサポートされています。そのため、VRF ドメインの 1 つの SXP 接続が IPV4 および IPV6 両方の IP-SGT マッピングを転送できます。
- SXP には VRF あたりの接続数および IP-SGT マッピング数の制限はありません。

VRF 対応 SGT および SGACL の IPv6 サポート

Cisco IOS XE Bengaluru 17.6.x リリース以降では、VRF 対応セキュリティグループタグ（SGT）および SG アクセスコントロールリスト（SGACL）で IPv6 がサポートされています。この機能は、IPv4 の場合と同じ機能を IPv6 に対して拡張します。

SGT および SGACL 機能に対する IPv6 サポートにより、次の機能が有効になります。

- SGT バインディング
  - SGT への IPv6 アドレス間の静的バインディング
  - VLAN から SGT へのバインディング
  - IPv6 アドレスと SGT 間のマッピングの動的学習
- 施行
  - UDP または TCP ポートに基づく IPv6 トラフィックに対する SGACL 適用
  - 上位層プロトコルタイプに基づく IPv6 トラフィックに対する SGACL 適用

（注）
- SGT バインディングは、リンクローカルアドレスではサポートされていません。
- SGACL はマルチキャストトラフィックには適用されません。

IPv6 SGT と SGACL のスケール値は IPv4 と IPv6 の両方で同じであり、ほとんどの CLI コマンドは変更されていません。

IPv6 サポートの詳細については、次の項を参照してください。

- IPv4 と IPv6 が SGT および SGACL テーブルを共有する方法 （158 ページ）
- SGT および SGACL スケール値 （159 ページ）

Cisco.com の Cisco TrustSec コンフィギュレーション ガイド、Cisco IOS XE 17 [英語] も参照してください。

IPv4 と IPv6 が SGT および SGACL テーブルを共有する方法

IPv4 と IPv6 は、FPGA で SGT および SGACL テーブルを共有します。次のリストに、共有の管理方法を示します。

- IPv4 または IPv6 を有効にすると、設定に基づいてテーブル全体が使用されます。
- IPv4 と IPv6 を有効にすると、最初の要求を行う機能に基づいてテーブルが共有されます。

- SGT および SGACL テーブルの上限を超えると、適切な syslog が生成されます。
- サポートされていないポリシーを設定すると、適切な syslog が生成されます。

SGT および SGACL スケール値

次の表に、IPv4 と IPv6 のスケール値を示します。

エントリの種類	スケール値	説明
ホストから SGT	1024	ホストから SGT へのバインド
サブネットから SGT	64	ネットワークから SGT へのバインド
SGT X DGT マトリックス	21 X 21	SGT から DGT へのマッピング
SGACL ポリシーリストサイズ	15	各 SGACL の最大 ACE
ロギングカウンタ [31:0] SGT および DGT ペアの数	32	最大ペア数

（注） デフォルトでは、ロギングは 32 の SGT と DGT のペアに対してのみ有効になっています。ただし、ロギングを有効にするペアを指定できます。32ペアのうち任意のペアに対するロギングを無効にし、異なるペアのロギングを有効にできます。

- ロギングが有効になっている SGT と DGT のペアを表示するには、show platform hardware cts cell-logging コマンドを使用します。
- 特定の SGT および DGT ペアのロギングを無効にするには、no platform cts logging コマンドを使用します。
- 特定の SGT と DGT のペアのロギングを有効にするには、platform cts logging コマンドを使用します。

次のテキストは、no platform cts logging コマンドのオプションを示しています。

```
Device> enable
Device#configure terminal
Device(config)#no platform cts logging ?
all Disable logging for all the cells
default default logging list
from Source Group Tag (SGT) for enabling logging
```

Cisco TrustSec VRF 対応 SGT の設定方法

このセクションでは、Cisco TrustSec VRF 対応 SGT の設定方法について説明します。

VRF と SGT のマッピングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **cts role-based sgt-map vrf** *vrf-name* {**ip4_netaddress** | *ipv6_netaddress* | **host** {*ip4_address* | *ip6_address*}}] **sgt** *sgt_number*
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	**enable** 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	**configure terminal** 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	**cts role-based sgt-map vrf** *vrf-name* {**ip4_netaddress**	*ipv6_netaddress*	**host** {*ip4_address*	*ip6_address*}}] **sgt** *sgt_number*
				例：
				`Device(config)# cts role-based sgt-map vrf red 10.0.0.3 sgt 23`
				例：
				`Device(config)# cts role-based sgt-map vrf VRF_1 2405:201:c::f115 sgt 1201`
					指定された VRF のパケットに SGT を適用します。
					IP-SGT バインドは、指定された VRF と、IP アドレスのタイプによって示される IP プロトコルのバージョンに関連付けられた IP-SGT のテーブルに入力されます。

ステップ 4	**end** 例： `Device(config)# end`	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。

Cisco TrustSec VRF 対応 SGT の設定例

このセクションでは、Cisco TrustSec VRF 対応 SGT の設定例を示します。

例：VRF と SGT のマッピングの設定

IPv4 の例：

```
Device> enable
Device# configure terminal
Device(config)# cts role-based sgt-map vrf VRF_1 22.1.1.1 sgt 1204
Device(config)# end
```

IPv6 の例：

```
Device> enable
Device# configure terminal
Device(config)# cts role-based sgt-map vrf VRF_1 2405:201:c::f115 sgt 1201
Device(config)# end
```

例：ロールベース アクセス リスト コマンド

```
Switch(config)# ipv6 access-list role-based acl-name
Switch(config-rb-acl)#?
Role-based Access List configuration commands:
<1-2147483647> Sequence Number
default    Set a command to its defaults
deny       Specify packets to reject
exit       Exit from access-list configuration mode
no         Negate a command or set its defaults
permit     Specify packets to forward
remark     Access list entry comment
Switch(config-rb-acl)#
```

ACE ポート範囲

Cisco IOS XE Bengaluru 17.6.x リリース以降、TrustSec FPGA モジュールは、いくつかのスケーリングの問題に対処するためにポリシー要素のポート範囲オプションをサポートしています。

FPGA モジュールは、TrustSec の一部として IP-to-SGT バインディングと SGACL ポリシーを維持します。Cisco IE3400 スイッチは、各セルで 21 X 21 SGT または DGT ペアと 15 個のポリシーをサポートし、IP プロトコルフィールド、L4 送信元ポート、および L4 宛先ポートを照合します。

ただし、一致基準を指定すると、ユーザーアクセス権限を拡張できない場合があります。そのため、TrustSec FPGA モジュールは、各セルでサポートされるポリシーを15 個に維持することで、各ポリシー要素のポート範囲オプションをサポートします。

この機能強化により、次のリストに示すように複数のルールを組み合わせることができます。

- IP プロトコルフィールドの照合
- L4 送信元開始ポートと終了ポートの照合
- L4 宛先開始ポートと終了ポートの照合

例：ACE ポート範囲のロールベース アクセス リスト コマンド

次のコマンドを使用して、送信元ポートと宛先ポートの ACE ポート範囲を設定できます。

```
Switch(config)# ip access-list role-based rbacl
Switch(config-rb-acl)#10 deny tcp dst range ftp-data telnet
Switch(config-rb-acl)#20 permit tcp dst lt 10
Switch(config-rb-acl)#30 deny tcp dst gt 50
```

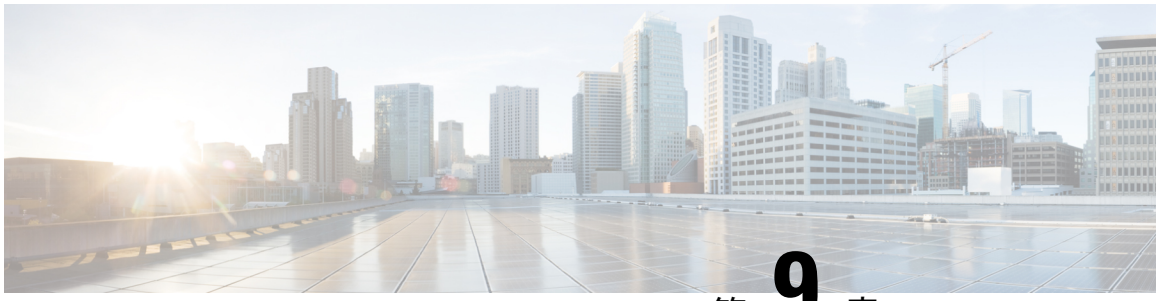
Cisco TrustSec VRF 対応 SGT の機能履歴

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	機能説明
Cisco IOS XE リリース 17.6.1	SGT および SGACL の IPv6 サポートの拡張	ホストから SGT へのマッピングとバインディング、およびサブネットから SGT へのバインディングを有効にします。
	SGACL 適用に対する IPv6 サポートの拡張	UDP ポート、TCP ポート、および上位層プロトコルタイプに基づいて、IPv6 トラフィックに SGACL を適用します。
	TrustSec FPGA モジュールでのポート範囲オプションのサポート	オプションは、スケーリングの問題に対処するためにポリシー要素でサポートされています。

リリース	機能	機能説明
Cisco IOS XE リリース 17.5.1	Cisco TrustSec VRF 対応 SGT	Cisco TrustSec VRF 対応 SGT 機能は、SGT SXP 接続を特定の VRF インスタンスにバインドします。



第 9 章

Cisco Umbrella 統合

•
• Cisco Umbrella 統合の前提条件 （165 ページ）
• Cisco Umbrella 統合の制限 （166 ページ）
• Cisco Umbrella 統合に関する情報 （167 ページ）
• Cisco Umbrella 統合の設定方法 （171 ページ）
• Cisco Umbrella 統合の設定の確認 （177 ページ）
• Cisco Umbrella 統合のトラブルシューティング （179 ページ）
• Cisco Umbrella 統合の機能情報 （179 ページ）

Cisco Umbrella 統合の前提条件

- Cisco Umbrella サブスクリプション ライセンスが利用可能である必要があります。https://umbrella.cisco.com/products/umbrella-enterprise-security-packages に移動し、[Request a quote] をクリックしてライセンスを取得します。
- デバイスはデフォルトのドメインネームシステム（DNS）サーバゲートウェイとして設定する必要があり、ドメインネームサーバのトラフィックはシスコデバイスを通過する必要があります。
- Umbrella サーバーへのデバイス登録に使用する通信は HTTPS 経由です。HTTPS 通信を行うには、デバイスにルート証明書がインストールされている必要があります。次のリンクを使用して証明書をダウンロードできます。https://www.digicert.com/CACerts/DigiCertSHA2SecureServerCA.crt
- シスコ産業用イーサネットスイッチは、Cisco IOS XE リリース 17.2.1 以降のソフトウェアイメージを実行します。
- Cisco Umbrella を有効にするには、シスコ産業用イーサネットスイッチに Cisco DNA Advantage 以上のライセンスが必要です。

次のネットワーク要件を満たす必要があります。

- デバイスをデフォルトの DNS サーバゲートウェイとして設定し、ドメインネームサーバ（DNS）トラフィックがシスコ産業用イーサネットスイッチを通過するようにします。
- Cisco Umbrella サーバへのデバイス登録に使用する通信は HTTPS 経由です。HTTPS 通信を行うには、ルータにルート証明書がインストールされている必要があります。この証明書をペーストする代わりに、次のリンクから証明書を直接ダウンロードすることができます。

  https://www.digicert.com/CACerts/DigiCertSHA2SecureServerCA.crt
- 最初の登録の場合、「umbrella out」として設定されたインターフェイスは、最初の登録を完了するために、ポート 443 を介して api.opendns.com にアクセスできる必要があります。

Cisco Umbrella 統合の制限

- Cisco Umbrella 統合は、次のシナリオでは機能しません。
  - アプリケーションまたはホストが、DNS の代わりに IP アドレスを使用してドメイン名をクエリしている場合。
  - クライアントが Web プロキシに接続されていて、サーバアドレスを解決するための DNS クエリを送信しない場合。
  - DNS クエリがシスコスイッチデバイスによって生成される場合。
  - DNS クエリが TCP 経由で送信される場合。
  - DNS クエリに、アドレスマッピングとテキスト以外のレコードタイプがある場合。
- DNSv6 クエリはサポートされていません。
- DNS64 および DNS46 拡張はサポートされていません。
- 拡張 DNS は、ホストの IPv4 アドレスのみを伝達し、IPv6 アドレスは伝達しません。
- ポートチャネルでの Cisco Umbrella 設定はサポートされていません
- Cisco Umbrella は、10G アップリンクポートを送信専用として使用するように設定できます。
- Cisco Umbrella インターフェイスを経由する DNS トラフィックの DSCP マーキングは行われません。これは、Cisco Umbrella インターフェイス上のすべてのパントされたトラフィックに適用されます。
- Cisco Umbrella インターフェイスの場合、すべての送信 ACL ルールは DNS トラフィックに影響を及ぼしません。これは、DNS の CPU 処理されるトラフィックに適用されます。
- DNS パケットのフラグメンテーションはサポートされていません。
- QinQ およびセキュリティグループタグ（SGT）パケットはサポートされていません。

- Cisco Umbrella の統合ポリシーによって DNS クエリがブロックされると、クライアントは Cisco Umbrella ブロックページにリダイレクトされます。これらのブロックページは、HTTPS サーバによって提供され、IP アドレス範囲は Cisco Umbrella ポータルによって定義されます。
- ユーザ認証とアイデンティティは、現在サポートされていません。
- Cisco Umbrella Connector は、悪意のあるトラフィックに関する既知の IP アドレスのリストを保持します。Cisco Umbrella ローミングクライアントは、これらのアドレスが宛先のパケットを検出すると、各アドレスを Cisco Umbrella クラウドに転送して、さらに検査します。
- 現在、直接クラウドアクセスはサポートされていません。
- 更新されたリゾルバ IP は有効になりません。DNS トラフィックは、ユーザが設定したリゾルバ IP に関係なく、Cisco Umbrella クラウドにリダイレクトされます。
- ネットワークアドレス変換（NAT）は、Cisco Umbrella が有効になっているインターフェイスではサポートされません。

Cisco Umbrella 統合に関する情報

ここでは、Cisco Umbrella 統合機能の詳細を説明します。

Cisco Umbrella 統合のメリット

Cisco Umbrella 統合は、DNS レベルでのセキュリティとポリシーの適用を提供します。これにより、管理者は DNS トラフィックを分割して、DNS トラフィックの一部をエンタープライズネットワーク内にある特定の DNS サーバに直接送信することができます。これにより、管理者は Cisco Umbrella 統合をバイパスできます。

Cisco Umbrella 統合を使用したクラウドベースのセキュリティサービス

Cisco Umbrella 統合機能は、Cisco デバイスを介して DNS サーバーに送信される DNS クエリを検査する、クラウドベースのセキュリティサービスを提供します。ホストがトラフィックを開始し、DNS クエリを送信すると、デバイスの Cisco Umbrella コネクタは DNS クエリを横取りして検査します。Umbrella コネクタは、DNS トラフィックを横取りして、セキュリティ検査およびポリシー適用のために Cisco Umbrella クラウドへのリダイレクトを行うシスコ デバイス内のコンポーネントです。Umbrella クラウドは、Umbrella コネクタから受信したクエリを検査するクラウドベースのセキュリティサービスであり、完全修飾ドメイン名（FQDN）に基づいて、コンテンツプロバイダーの IP アドレスを応答に含めるかどうかを決定します。

ローカルドメインへの DNS クエリの場合、DNS パケットを変更せずに企業ネットワーク内の DNS サーバーにクエリが転送されます。Cisco Umbrella リゾルバは、外部ドメインから送信さ

れた DNS クエリを検査します。デバイス ID 情報、組織 ID、クライアント IP アドレスを含む拡張 DNS レコードがクエリに追加され、Cisco Umbrella リゾルバに送信されます。Umbrella クラウドは、このすべての情報に基づいて、DNS クエリにさまざまなポリシーを適用します。

Umbrella 統合クラウドは、ポータルで設定されたポリシーと DNS FQDN のレピュテーションに基づいて、次のいずれかのアクションを実行します。

- ブラックリストのアクション：FQDN が悪意のあるものであるか、カスタマイズされたエンタープライズセキュリティポリシーによってブロックされていると判明した場合、Cisco Umbrella クラウドのブロックランディングページの IP アドレスが DNS 応答で返されます。
- ホワイトリストのアクション：FQDN が悪意のないものであると判明した場合、コンテンツプロバイダーの IP アドレスが DNS 応答で返されます。
- グレーリストのアクション：FQDN が疑わしいと判明した場合、インテリジェントプロキシのユニキャスト IP アドレスが DNS 応答で返されます。

DNS 応答を受信すると、デバイスは応答をホストに転送します。ホストは応答から IP アドレスを抽出し、HTTP または HTTPS 要求をこの IP アドレスに送信します。

Cisco Umbrella クラウドによるトラフィックの処理

Cisco Umbrella 統合機能を使用すると、HTTP および HTTPS クライアント要求は次のように処理されます。

- DNS クエリの FQDN が悪意のあるものである場合（ブラックリストに登録されたドメインに含まれる場合）、Cisco Umbrella クラウドは DNS 応答でブロック時用ランディングページの IP アドレスを返します。HTTP クライアントがこの IP アドレスに要求を送信すると、Umbrella クラウドは、要求されたページがブロックされたことをユーザに通知するページと、ブロックの理由を表示します。
- DNS クエリの FQDN が悪意のないものである場合（ホワイトリストに登録されたドメインに含まれる場合）、Cisco Umbrella クラウドはコンテンツプロバイダーの IP アドレスを返します。HTTP クライアントはこの IP アドレスに要求を送信し、要求されたコンテンツを取得します。
- DNS クエリの FQDN がグレーリストのドメインに該当する場合、Umbrella DNS リゾルバは DNS 応答でインテリジェントプロキシのユニキャスト IP アドレスを返します。ホストからグレードメインへのすべての HTTP トラフィックは、インテリジェントプロキシを介してプロキシされ、Uniform Resource Locator（URL）フィルタリングが実行されます。

（注） インテリジェントプロキシのユニキャスト IP アドレスを使用する場合の潜在的な制限の 1 つは、クライアントがインテリジェントプロキシのユニキャスト IP アドレスにトラフィックを送信しようとしたときにデータセンターがダウンする可能性です。このシナリオでは、クライアントはグレーリストのドメインに該当するドメインの DNS 解決を完了し、クライアントの HTTP または HTTPS トラフィックは、取得されたインテリジェントプロキシのユニキャスト IP アドレスのいずれかに送信されます。そのデータセンターがダウンしている場合、クライアントはそれを知る方法がありません。

Umbrella コネクタは、HTTP および HTTPS トラフィックに対して動作しません。コネクタは、Web トラフィックをリダイレクトしたり、HTTP または HTTPS パケットを変更したりしません。

DNS パケット暗号化

Cisco デバイスから Cisco Umbrella 統合サーバに送信される DNS パケットは、パケット内の拡張 DNS 情報にユーザ ID、内部ネットワーク IP アドレスなどの情報が含まれている場合、暗号化する必要があります。DNS 応答が DNS サーバから戻されると、デバイスはパケットを復号化してからホストに転送します。

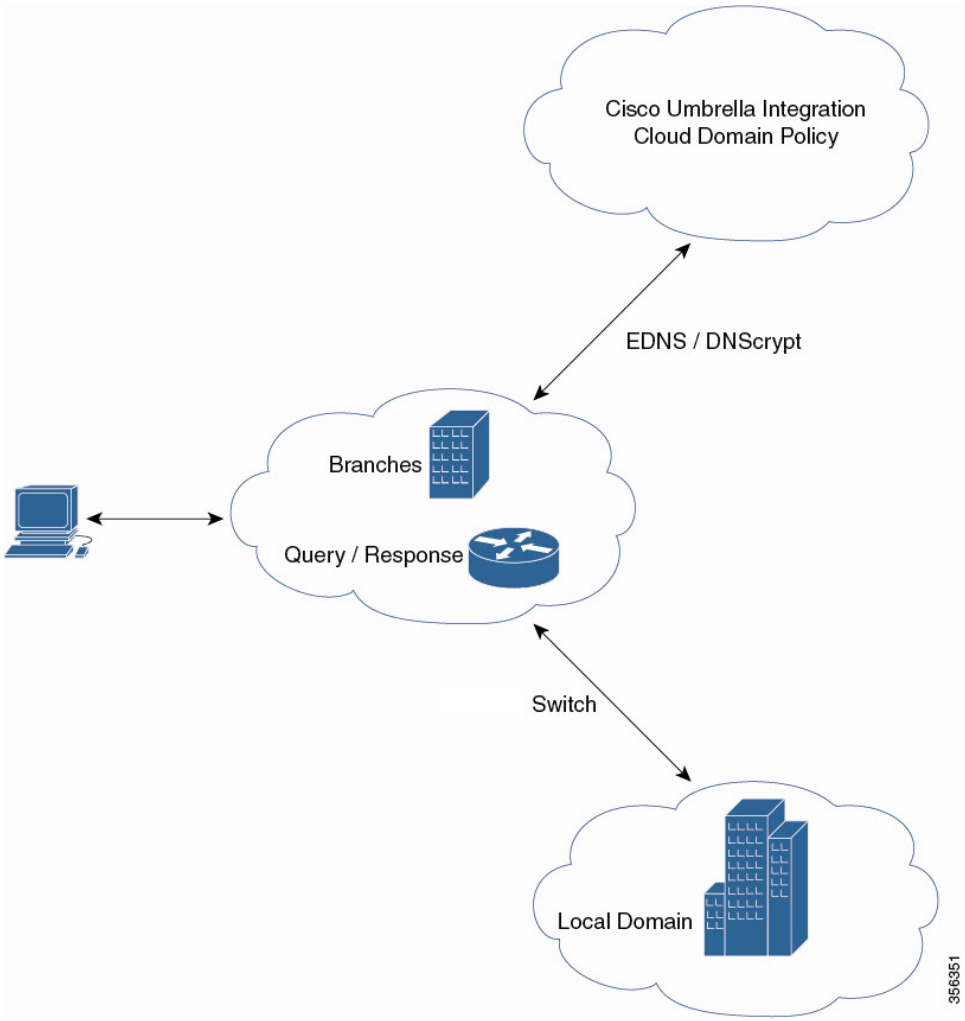
（注）
- DNS パケットは、DNScrypt 機能が Cisco デバイスで有効化されている場合にのみ暗号化できます。
- 統計情報を追跡するために、クライアントの IP アドレスが Umbrella クラウドにエクスポートされます。IP は暗号化されずに送信されるため、DNScrypt を無効にしないことを推奨します。

Cisco デバイスは次の Anycast 再帰型 Cisco Umbrella 統合サーバを使用します。

- 208.67.222.222
- 208.67.220.220
- 2620:119:53::53
- 2620:119:35::35

次の図に、Cisco Umbrella 統合のトポロジを示します。

図 *9 : Cisco Umbrella* 統合のトポロジ



DNSCrypt と公開鍵

次のサブセクションでは、DNScrypt と公開鍵について詳しく説明します。

DNSCrypt

DNSCrypt は、Cisco デバイスと Cisco Umbrella 統合機能間の通信を認証する暗号化プロトコルです。**parameter-map type umbrella** が設定され、WAN インターフェイスで **umbrella out** コマンドが有効化されると、DNSCrypt がトリガーされ、証明書のダウンロード、検証、解析が行われます。次に、DNS クエリの暗号化に使用される共有秘密鍵のネゴシエーションが行われます。一時間おきにこの証明書が自動的にダウンロードされ、アップグレードのために検証され、その都度新しい共有秘密鍵がネゴシエートされ、DNS クエリが暗号化されます。

DNSCrypt を使用する場合は、DNS 要求パケットサイズが 512 バイトよりも大きくなります。これらのパケットが中間デバイスを通過できることを確認します。そうしないと、応答が目的の受信者に到達しない可能性があります。

公開鍵

公開鍵は、Umbrella クラウドから DNSCrypt 証明書をダウンロードするために使用されます。この値は、B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79（Cisco Umbrella Integration Anycast サーバーの公開鍵）に事前に設定されています。公開鍵に変更があり、**public-key** コマンドを変更する場合、デフォルト値に戻すときは変更されたコマンドを削除する必要があります。

⚠

注意 この値を変更すると、DNSCrypt 証明書のダウンロードは失敗することがあります。

parameter-map type umbrella global コマンドは、Umbrella モードでパラメータマップタイプを設定します。このコマンドを使用してデバイスを設定すると、DNSCrypt と公開鍵の値が自動入力されます。

ラボで特定のテストを実行するときは、**parameter-map type umbrella global** パラメータのみを変更することをお勧めします。これらのパラメータを変更すると、デバイスの正常な機能に影響が及ぶことがあります。

Cisco Umbrella 統合の設定方法

ここでは、Cisco Umbrella 統合を構成するさまざまな作業について説明します。

Umbrella Connector の設定

始める前に

Cisco Umbrella 登録サーバからアプリケーションプログラミングインターフェイス（API）トークンを取得します。

Cisco Umbrella 登録サーバとの間で HTTPS 接続を確立するために、ルート証明書を取得します。グローバル コンフィギュレーション モードで **crypto pki trustpool import terminal** コマンドを使用して、DigiCert のルート証明書をデバイスにインポートします。

証明書をインポートする方法は 2 つあります。

1. URL からインポートする
2. 端末で直接インポートする

URL からインポートするには、コマンドを発行し、産業用イーサネットスイッチが証明書を取得できるようにします。

crypto pki trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b

端末からインポートするには、次の手順を実行します。

DigiCert のルート証明書は次のとおりです。

```
-----BEGIN CERTIFICATE-----
MIIElDCCA3ygAwIBAgIQAf2j627KdciIQ4tyS8+8kTANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAeFw0xMzAzMDgxMjAwMDBaFw0yMzAzMDgxMjAwMDBaME0xCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxJzAlBgNVBAMTHkRpZ2lDZXJ0IFNIQTIg
U2VjdXJlIFNlcnZlciBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
ANyuWJBNwcQwFZA1W248ghX1LFy949v/cUP6ZCWA1O4Yok3wZtAKc24RmDYXZK83
nf36QYSvx6+M/hpzTc8zl5CilodTgyu5pnVILR1WN3vaMTIa16yrBvSqXUu3R0bd
KpPDkC55gIDvEwRqFDu1m5K+wgdlTvza/P96rtxcflUxDOg5B6TXvi/TC2rSsd9f
/ld0Uzs1gN2ujkSYs58O09rg1/RrKatEp0tYhG2SS4HD2nOLEpdIkARFdRrdNzGX
kujNVA075ME/OV4uuPNcfhCOhkEAjUVmR7ChZc6gqikJTvOX6+guqw9ypzAO+sf0
/RR3w6RbKFfCs/mC/bdFWJsCAwEAAaOCAVowggFWMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDgYDVR0PAQH/BAQDAgGGMDQGCCsGAQUFBwEBBCgwJjAkBggrBgEFBQcwAYYY
aHR0cDovL29jc3AuZGlnaWNlcnQuY29tMHsGA1UdHwR0MHIwN6A1oDOGMWh0dHA6
Ly9jcmwzLmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RDQS5jcmwwN6A1
oDOGMWh0dHA6Ly9jcmw0LmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RD
QS5jcmwwPQYDVR0gBDYwNDAyBgRVHSAAMCowKAYIKwYBBQUHAgEWHGh0dHBzOi8v
d3d3LmRpZ2ljZXJ0LmNvbS9DUFMwHQYDVR0OBBYEFA+AYRyCMWHVLyjnjUY4tCzh
xtniMB8GA1UdIwQYMBaAFAPeUDVW0Uy7ZvCj4hsbw5eyPdFVMA0GCSqGSIb3DQEB
CwUAA4IBAQAjPt9L0jFCpbZ+QlwaRMxp0Wi0XUvgBCFsS+JtzLHgl4+mUwnNqipl
5TlPHoOlblyYoiQm5vuh7ZPHLgLGTUq/sELfeNqzqPlt/yGFUzZgTHbO7Djc1lGA
8MXW5dRNJ2Srm8c+cftIl7gzbckTB+6WohsYFfZcTEDts8Ls/3HB40f/1LkAtDdC
2iDJ6m6K7hQGrn2iWZiIqBtvLfTyyRRfJs8sjX7tN8Cp1Tm5gr8ZDOo0rwAhaPit
c+LJMto4JQtV05od8GiG7S5BNO98pVAdvzr508EIDObtHopYJeS4d60tbvVS3bR0
j6tJLp07kzQoH3jOlOrHvdPJbRzeXDLz
-----END CERTIFICATE-----
```

プライバシー強化メール（PEM）インポートが正常に行われたことを確認します。証明書をインポートすると、確認メッセージが表示されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type umbrella global**
4. **dnscrypt**
5. **token** *value*
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	**enable** 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。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 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	**parameter-map type umbrella global** 例： `Device(config)# parameter-map type umbrella global`	パラメータマップタイプを umbrella モードに設定し、パラメータマップタイプ検査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	**dnscrypt** 例： `Device(config-profile)# dnscrypt`	デバイスで DNS パケット暗号化を有効にします。
ステップ 5	**token** *value* 例： `Device(config-profile)# token AABBA59A0BDE1485C912AFE472952641001EEECC`	Cisco Umbrella 登録サーバによって発行された API トークンを指定します。
ステップ 6	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査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。

Cisco Umbrella タグの登録

始める前に

- Umbrella Connector を設定します。
- **umbrella in** コマンドを設定する前に **umbrella out** コマンドを設定します。登録は、ポート 443 がオープン状態にあり、既存のファイアウォールへのトラフィックのパススルーが許可される場合にのみ成功します。
- タグを指定して **umbrella in** コマンドを設定すると、デバイスは api.opendns.com を解決して登録プロセスを開始します。**ip name-server** コマンドを使用してネームサーバを設定し、デバイスで設定された **ip domain-lookup** コマンドを使用してドメインルックアップを設定して、FQDN を正常に解決します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-type interface-number*
4. **umbrella out**
5. **exit**
6. **interface** *interface-type interface-number*
7. **umbrella in** *tag-name*
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	**enable** 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	**configure terminal** 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	**interface** *interface-type interface-number* 例： `Device(config)# interface gigabitEthernet 1/1`	WAN 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	**umbrella out** 例： `Device(config-if)# umbrella out`	Umbrella クラウドサーバに接続するためのインターフェイスで Umbrella Connector を設定します。
ステップ 5	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバルコンフィギュレーションモードを開始します。
ステップ 6	**interface** *interface-type interface-number* 例： `Device(config)# interface gigabitEthernet 1/2`	LAN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 7	**umbrella in** *tag-name* 例： `Device(config-if)# umbrella in mydevice_tag`	クライアントに接続されているインターフェイスで Umbrella Connector を設定します。 • Umbrella タグの長さは 49 文字までです。 • タグを使用して **umbrella in** コマンドを設定すると、デバイスは Cisco Umbrella 統合サーバにタグを登録します。
ステップ 8	**end** 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。

Cisco デバイスをパススルーサーバとして設定

ドメイン名を使用して、バイパスされるトラフィックを特定することができます。Cisco デバイスでは、正規表現形式でこれらのドメインを定義できます。デバイスによって横取りされた DNS クエリが、設定済みの正規表現の 1 つにマッチすると、このクエリは、Umbrella クラウドにリダイレクトされずに、指定された DNS サーバにバイパスされます。

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type regex** *parameter-map-name*
4. **pattern** *expression*
5. **exit**
6. **parameter-map type umbrella global**
7. **token** *value*
8. **local-domain** *regex_param_map_name*
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	**enable** 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。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 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	**parameter-map type regex** *parameter-map-name* 例： `Device(config)# parameter-map type regex dns_bypass`	パラメータマップタイプを指定されたトラフィックパターンに一致するように設定し、パラメータマップタイプ検査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	**pattern** *expression*
	例：
	`Device(config-profile)# pattern www.cisco.com`
	`Device(config-profile)# pattern .*example.cisco.*`
		Umbrella クラウドをバイパスするために使用するローカルドメインまたは URL を設定します。

ステップ 5	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査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 モードを開始します。
ステップ 6	**parameter-map type umbrella global** 例： `Device(config)# parameter-map type umbrella global`	パラメータマップタイプを umbrella モードに設定し、パラメータマップタイプ検査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	**token** *value* 例： `Device(config-profile)# token AADDD5FF6E510B28921A20C9B98EEEFF`	Cisco Umbrella 登録サーバによって発行された API トークンを指定します。
ステップ 8	**local-domain** *regex_param_map_name* 例： `Device(config-profile)# local-domain dns_bypass`	正規表現パラメータマップを Umbrella グローバル コンフィギュレーションにアタッチします。

	コマンドまたはアクション	目的
ステップ 9	**end** 例： `Device(config-profile)# end`	パラメータ マップ タイプ検査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。

Cisco Umbrella 統合の設定の確認

Cisco Umbrella 統合の設定を表示および確認するには、次のコマンドを任意の順序で使用します。

次に、**show umbrella config** コマンドの出力例を示します。

```
Device# show umbrella config
Umbrella Configuration
=======================
Token: EB74330C50767B6A63770EA6C3408DCF00282D8E
API-KEY: NONE
OrganizationID: 2633102
Local Domain Regex parameter-map name: NONE
DNSCrypt: Enabled
Public-key: B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79
UDP Timeout: 5 seconds
Resolver address:
1. 208.67.220.220
2. 208.67.222.222
3. 2620:119:53::53
4. 2620:119:35::35
Umbrella Interface Config:
Number of interfaces with "umbrella out" config: 1
1. GigabitEthernet1/4
Mode : OUT
VRF : global(Id: 0)
Number of interfaces with "umbrella in" config: 2
1. GigabitEthernet1/9
Mode : IN
DCA : Disabled
Tag : IE_uniquetag
Device-id : 010a424c1597fe09
VRF : global(Id: 0)
2. GigabitEthernet2/3
Mode : IN
DCA : Disabled
Tag : IE_tag_2
Device-id : 010adaf012a36ad6
VRF : global(Id: 0)
Configured Umbrella Parameter-maps:
1. global
```

次に、**show umbrella deviceid** コマンドの出力例を示します。

```
Device# show umbrella deviceid

Device registration details
Interface Name Tag Status Device-id
```

```
GigabitEthernet1/9 IE_uniquetag 200 SUCCESS 010a424c1597fe09
GigabitEthernet2/3 IE_tag_2 200 SUCCESS 010adaf012a36ad6
```

次に、**show umbrella dnscrypt** コマンドの出力例を示します。

```
Device#show umbrella dnscrypt
DNSCrypt: Enabled
Public-key: B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79
Certificate Update Status:
Last Successfull Attempt: 20:01:18 IST Dec 17 2019
Certificate Details:
Certificate Magic : DNSC
Major Version : 0x0001
Minor Version : 0x0000
Query Magic : 0x7163373861576F6F
Serial Number : 1574811744
Start Time : 1574811744 (05:12:24 IST Nov 27 2019)
End Time : 1606347744 (05:12:24 IST Nov 26 2020)
Server Public Key :
88B4:E44B:35E9:64B4:90BD:DABA:E825:A24B:0415:A08B:E19D:7DDB:87A3:3CD7:7EDF:8E2F
Client Secret Key Hash:
0FB9:520E:5228:FB2C:D521:1E9E:2ACB:AC3D:B520:A795:F54C:C608:604B:A410:17F1:1284
Client Public key :
E42F:507E:F052:72DD:1BC8:4857:2AE0:2F9F:ED87:1687:AAE4:095D:D933:48F0:5D60:3662
NM key Hash :
EDC3:25DD:4D21:103E:7E49:1EFA:75ED:4D6F:A450:107D:C6E8:1C41:9CF7:4039:FA89:2CED
```

次に、**show umbrella deviceid detailed** コマンドの出力例を示します。

```
Device# show umbrella deviceid detailed

Device registration details
1.GigabitEthernet1/9
Tag : IE_uniquetag
Device-id : 010a424c1597fe09
Description : Device Id recieved successfully
WAN interface : GigabitEthernet1/4
WAN VRF used : global(Id: 0)
2.GigabitEthernet2/3
Tag : IE_tag_2
Device-id : 010adaf012a36ad6
Description : Device Id recieved successfully
WAN interface : GigabitEthernet1/4
WAN VRF used : global(Id: 0)
```

次に、**show platform software dns-umbrella statistics** コマンドの出力例を示します。コマンド出力には、送信されたクエリの数、受信した応答の数などのトラフィック関連の情報が表示されます。

```
Device# show platform software dns-umbrella statistics

========================================
Umbrella Statistics
========================================
Total Packets : 7848
DNSCrypt queries : 3940
DNSCrypt responses : 0
DNS queries : 0
DNS bypassed queries(Regex) : 0
DNS responses(Umbrella) : 0
DNS responses(Other) : 3906
```

```
Aged queries : 34
Dropped pkts : 0
```

Cisco Umbrella 統合のトラブルシューティング

次のコマンドを使用して、Cisco Umbrella 統合機能の設定に関連する問題をトラブルシューティングできます。

表 *14 : Cisco Umbrella* 統合機能のデバッグコマンド

コマンド	目的
debug umbrella config	Umbrella 設定のデバッグを有効にします。
debug umbrella device-registration	Umbrella デバイス登録のデバッグを有効にします。
debug umbrella dnscrypt	Umbrella DNSCrypt 暗号化のデバッグを有効にします。

Windows マシンのコマンドプロンプト、または Linux マシンのターミナルウィンドウもしくはシェルから、**nslookup -type=txt debug.opendns.com** コマンドを実行します。**nslookup -type=txt debug.opendns.com** コマンドで指定する IP アドレスは、DNS サーバの IP アドレスである必要があります。

```
nslookup -type=txt debug.opendns.com 10.0.0.1
Server: 10.0.0.1
Address: 10.0.0.1#53
Non-authoritative answer:
debug.opendns.com text = "server r6.xx"
debug.opendns.com text = "device 010A826AAABB6C3D"
debug.opendns.com text = "organization id 1892929"
debug.opendns.com text = "remoteip 10.0.1.1"
debug.opendns.com text = "flags 436 0 6040 39FF000000000000000"
debug.opendns.com text = "originid 119211936"
debug.opendns.com text = "orgid 1892929"
debug.opendns.com text = "orgflags 3"
debug.opendns.com text = "actype 0"
debug.opendns.com text = "bundle 365396"
debug.opendns.com text = "source 10.1.1.1:36914"
debug.opendns.com text = "dnscrypt enabled (713156774457306E)"
```

Cisco Umbrella 統合の機能情報

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。

表 *15 : Cisco Umbrella* 統合の機能情報

機能名	リリース	機能情報
Cisco Umbrella 統合	Cisco IOS XE Amsterdam 17.2.1	Cisco Umbrella 統合機能により、Cisco デバイスを介して任意の DNS サーバに送信される DNS クエリを検査する、クラウドベースのセキュリティサービスを利用できるようになります。セキュリティ管理者は、FQDN へのトラフィックを許可または拒否するポリシーを Cisco Umbrella クラウドに設定します。

第 10 章

Network Edge Access Topology（NEAT）の設定

- Network Edge Access Topology 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 スイッチ （181 ページ）
- 注意事項と制約事項 （183 ページ）
- NEAT を使用したオーセンティケータ スイッチの設定 （184 ページ）
- NEAT を使用したサプリカント スイッチの設定 （186 ページ）
- 設定の確認 （188 ページ）
- 設定例 （190 ページ）
- 機能の履歴 （191 ページ）

Network Edge Access Topology 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スイッチ

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。設定情報を含む、802.1x の詳細については、「Configuring IEEE 802.1x Port-Based Authentication」を参照してください。

Network Edge Access Topology（NEAT）機能は、ワイヤリングクローゼット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。NEAT では、サプリカントスイッチとオーセンティケータ間でクライアントの MAC と VLAN 情報を伝播するために Client Information Signalling Protocol（CISP）が使用されます。CISP および NEAT は L2 ポートでのみサポートされ、L3 ポートではサポートされません。IE3x00 および ESS3300 スイッチで NEAT を設定できます。

- 802.1x スイッチ サプリカント：802.1x サプリカント機能を使用することで、別のスイッチのサプ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 サプ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。サプリカント 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。サプ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 スイッチにサプ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プリカント スイッチが認証する前にスパニングツリー 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。認証中にサプ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プリカントのポートをブロックします。認証に失敗すると、サプ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、認証期間中にサプリカント 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、サプリカント 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、サプリカントスイッチで **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 モードを有効にできます。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。

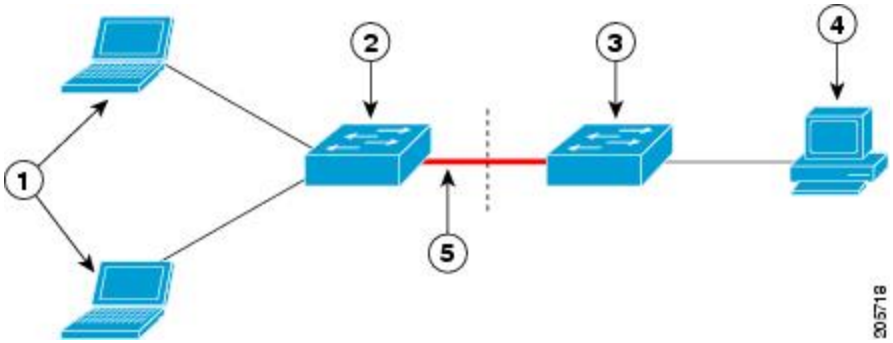
インターフェイスで有効になっているシングルホスト モードでオーセンティケータ スイッチをリブートすると、インターフェイスが認証前に err-disabled 状態に移行する場合があります。err-disabled 状態から回復するには、オーセンティケータ ポートをフラップしてインターフェイスを再度アクティブにし、認証を開始します。

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 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、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 *10 : 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 クローゼット外）
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 を使用したサプ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、トポロジのサプ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。

注意事項と制約事項

次に、NEAT の設定および使用に関する注意事項と制約事項を示します。

- シスコの Identity Server Engine（ISE）などの RADIUS サーバーが必要です。
- CISP および NEAT は L2 ポートでのみサポートされ、L3 ポートではサポートされません。
- NEAT および 802.1x は、EtherChannel ポートではサポートされません。
- NEAT はダイナミック ポートではサポートされません。
- MACsec は NEAT でサポートされます。
- NEAT は PTP と併用できます。

- 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。

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 つのスイッチがサプ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）
- *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、サプ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. **enable**
2. **configure terminal**
3. **cisp enable**
4. **interface** *interface-id*
5. **switchport mode access**
6. **authentication port-control auto**
7. **dot1x pae authenticator**
8. **spanning-tree portfast**
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	**enable** 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	**configure terminal** 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。

	コマンドまたはアクション	目的
ステップ 3	**cisp enable** 例： `Device(config)# cisp enable`	CISP を有効にします。
ステップ 4	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet 1/2`	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 5	**switchport mode access** 例： `Device(config-if)# switchport mode access`	ポートモードを **access** に設定します。
ステップ 6	**authentication port-control auto** 例： `Device(config-if)# authentication port-control auto`	ポート認証モードを auto に設定します。
ステップ 7	**dot1x pae authenticator** 例： `Device(config-if)# dot1x pae authenticator`	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 8	**spanning-tree portfast** 例： `Device(config-if)# spanning-tree portfast trunk`	インターフェイスを、複数の VLAN のメンバーであるインターフェイスのスパニングツリー フォワーディング ステートにすばやく移行できるようにします。このコマンドは、スイッチ間接続がレイヤ 2 ループの一部ではないことが確実な場合にのみ使用します。
ステップ 9	**end** 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。

NEAT を使用したサプリカント スイッチの設定

スイッチをサプ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. **enable**
2. **configure terminal**
3. **cisp enable**
4. **eap profile** *profile-name*
5. **method** *type*
6. **exit**
7. **dot1x credentials** *profile*
8. **username** *suppswitch*
9. **password** *password*
10. **dot1x supplicant force-multicast**
11. **interface** *interface-id*
12. **switchport trunk encapsulation dot1q**
13. **switchport mode trunk**
14. **dot1x pae supplicant**
15. **dot1x credentials** *profile-name*
16. **dot1x supplicant eap profile** *profile-name*
17. **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	**enable** 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	**configure terminal** 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	**cisp enable** 例： `Device(config)# cisp enable`	CISP を有効にします。

	コマンドまたはアクション	目的
ステップ 4	**eap profile** *profile-name* 例： `Device(config)# eap profile CISP`	Extensible Authentication Protocol（EAP）プロファイルを作成し、EAP 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	**method** *type* 例： `Device(config-eap-profile)# method md5`	EAP 認証方式を指定します。
ステップ 6	**exit** 例： `Device(config-eap-profile)# exit`	EAP プロファイル コンフィギュレーション モードを終了します。
ステップ 7	**dot1x credentials** *profile* 例： `Device(config)# dot1x credentials test`	802.1x クレデンシャルプロファイルを作成します。これは、サプ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 8	**username** *suppswitch* 例： `Device(config)# username suppswitch`	ユーザ名を作成します。
ステップ 9	**password** *password* 例： `Device(config)# password myswitch`	新しいユーザ名のパスワードを作成します。
ステップ 10	**dot1x supplicant force-multicast** 例： `Device(config)# dot1x supplicant force-multicast`	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 モードでのサプリカント スイッチで機能できるようにもなります。
ステップ 11	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet1/1`	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 12	**switchport trunk encapsulation dot1q** 例： `Device(config-if)# switchport trunk encapsulation dot1q`	ポートをトランク モードに設定します。
ステップ 13	**switchport mode trunk** 例： `Device(config-if)# switchport mode trunk`	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 14	**dot1x pae supplicant** 例： `Device(config-if)# dot1x pae supplicant`	インターフェイスをポート アクセス エンティティ（PAE）サプリカントとして設定します。
ステップ 15	**dot1x credentials** *profile-name* 例： `Device(config-if)# dot1x credentials test`	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対応付けます。
ステップ 16	**dot1x supplicant eap profile** *profile-name* 例： `Device(config-if)# dot1x supplicant eap profile cisp`	EAP-TLS プロファイルを 802.1X インターフェイスに割り当てます。
ステップ 17	**end** 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。

設定の確認

Client Information Signaling Protocol（CISP）および Network Edge Access Topology（NEAT）の設定に関する情報を確認するには、次の show コマンドを使用します。

- show cisp interface <interface name>
- show cisp clients
- show cisp summary

- show cisp registrations

次に、**show cisp** コマンドの出力例を示します。GigabitEthernet 1/1 はオーセンティケータとして設定され、GigabitEthernet 1/2 はサプリカントとして設定されます。

```
Auth# show cisp interface Gi1/2

CISP Status for interface Gi1/2
 -------------------------------------
Version: 1
Mode: Supplicant Peer
Mode: Authenticator
Supp State: Idle

Auth# show cisp clients

Authenticator Client Table:
 ------------------------
 MAC Address VLAN Interface
 --------------------------------
 0050.5695.4de8 1 Gi1/10
6c03.09e7.3947 1 Gi1/10
6c03.09e7.3954 11 Gi1/10
6c03.09e7.4485 1 Gi1/10
 9077.ee4a.8567 1 Gi1/10
e41f.7ba1.bbd4 1 Gi1/10

Supplicant Client Table:
------------------------
MAC Address VLAN Interface
--------------------------------
9077.ee4a.856b 11 Vl11
9077.ee4a.8572 1 Ap1/1
e41f.7bc7.2f03 1 Gi1/9

Auth# show cisp summary

CISP is running on the following interface(s):
---------------------------------------------
Gi1/2 (Authenticator)

Supp# show cisp summary

CISP is running on the following interface(s):
---------------------------------------------
Gi1/1 (Supplicant)

Auth# show cisp registrations

Interface(s) with CISP registered user(s):
-----------------------------------------
Gi1/2
Auth Mgr (Authenticator)

Supp# show cisp registration

Interface(s) with CISP registered user(s):
-----------------------------------------
Gi1/1
802.1x Sup (Supplicant)
```

CISP および NEAT をトラブルシューティングするには、次の debug コマンドを使用します。

- debug access-session errors
- debug access-session event
- debug dot1x errors
- debug dot1x packets
- debug dot1x events

設定例

次に、オーセンティケータスイッチでの Client Information Signaling Protocol（CISP）および Network Edge Access Topology（NEAT）の設定例を示します。

```
conf t
aaa new-model
cisp enable
radius server RADIUS_CWA
address ipv4 <ISE-IP> auth-port 1645 acct-port 1646
key <ISE KEY>
exit
aaa group server radius ISE
server name RADIUS_CWA
exit
aaa authentication dot1x default group radius
aaa authorization exec default group radius
aaa authorization network default group radius
aaa server radius dynamic-author
client <ISE-IP> server-key cisco123
dot1x system-auth-control
policy-map type control subscriber Policy_dot1x
event session-started match-all
10 class always do-until-failure
10 authenticate using dot1x
exit

interface <interface name>
switchport mode access
access-session closed
access-session port-control auto
dot1x pae authenticator
spanning-tree portfast
service-policy type control subscriber Policy_dot1x
exit
```

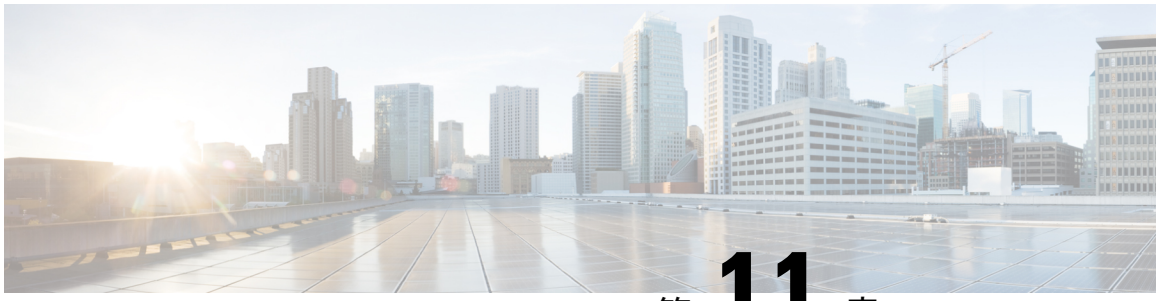
次に、サプリカントスイッチでの CISP および NEAT の設定例を示します。

```
conf t
cisp enable
eap profile CISP
method md5
exit
dot1x system-auth-control
dot1x supplicant controlled transient
dot1x credentials SWITCH
username <user configured in ISE>
password 0 <Password configured in ISE>
exit
interface <interface name>
```

```
switchport mode trunk
dot1x pae supplicant
dot1x credentials SWITCH
dot1x supplicant eap profile CISP
spanning-tree portfast trunk
exit
```

機能の履歴

機能名	リリース	機能情報
Network Edge Access Topology（NEAT）	Cisco IOS XE 17.8.1	IE3x00 での初期サポート



第 11 章

Web ベース認証の設定

- Web ベース認証について （193 ページ）
- Web ベース認証の設定方法 （203 ページ）
- Web ベース認証の確認 （216 ページ）
- Web ベース認証に関するその他の参考資料 （216 ページ）

Web ベース認証について

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。

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、アカウンティング（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）を使用するときに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。

（注） このリリースでは、外部 Web 認証はサポートされていません。

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] ボタンとともにユーザー名とパスワード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。

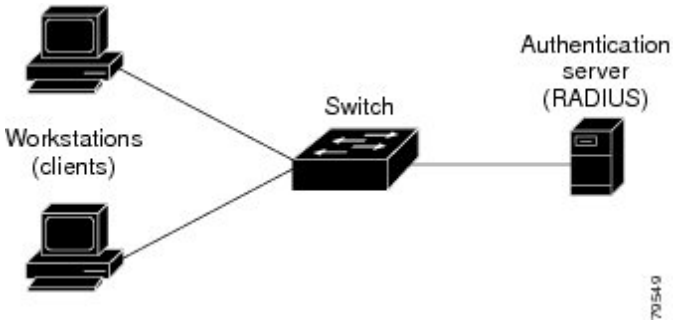
デバイスのロール

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 *11 : 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 プローブに応答しなかった場合、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。
- ホストがレイヤ 2 インターフェイス上の ARP プローブに応答しない場合、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。
- 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。

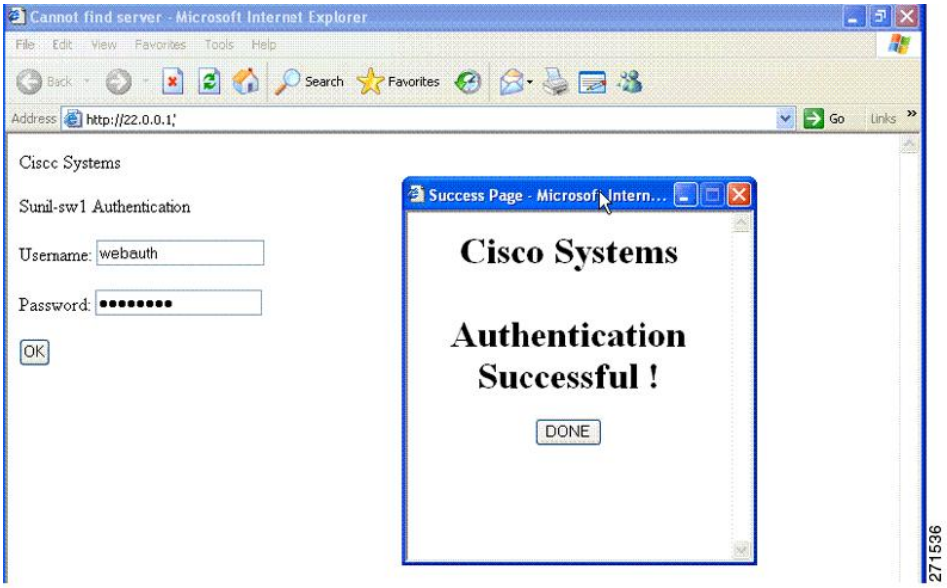
- 認証成功
- 認証失敗
- 認証期限切れ

ローカル Web 認証バナーは、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 *12* : 認証成功バナー



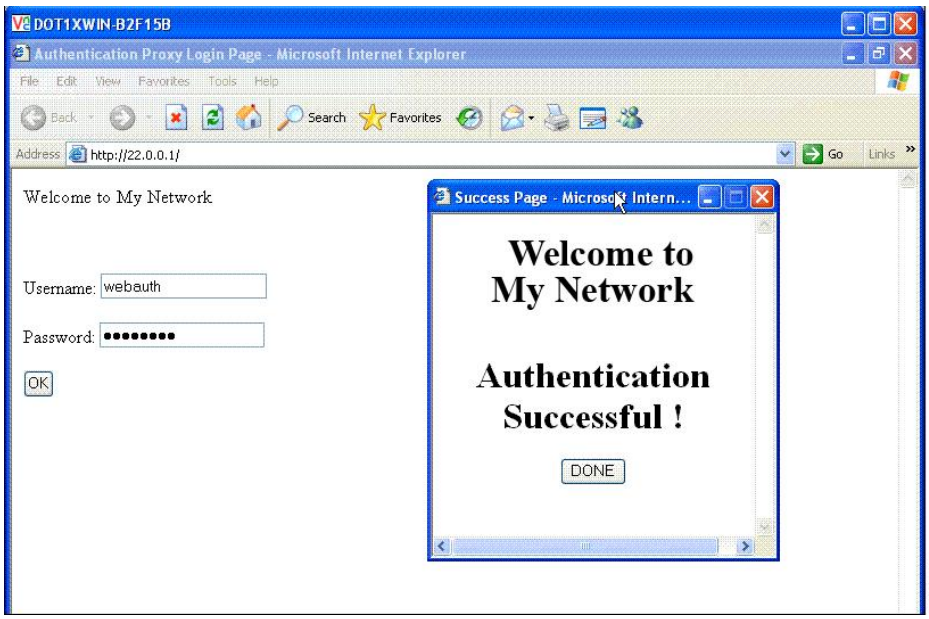
バナーは次のようにカスタマイズ可能です。

- 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。

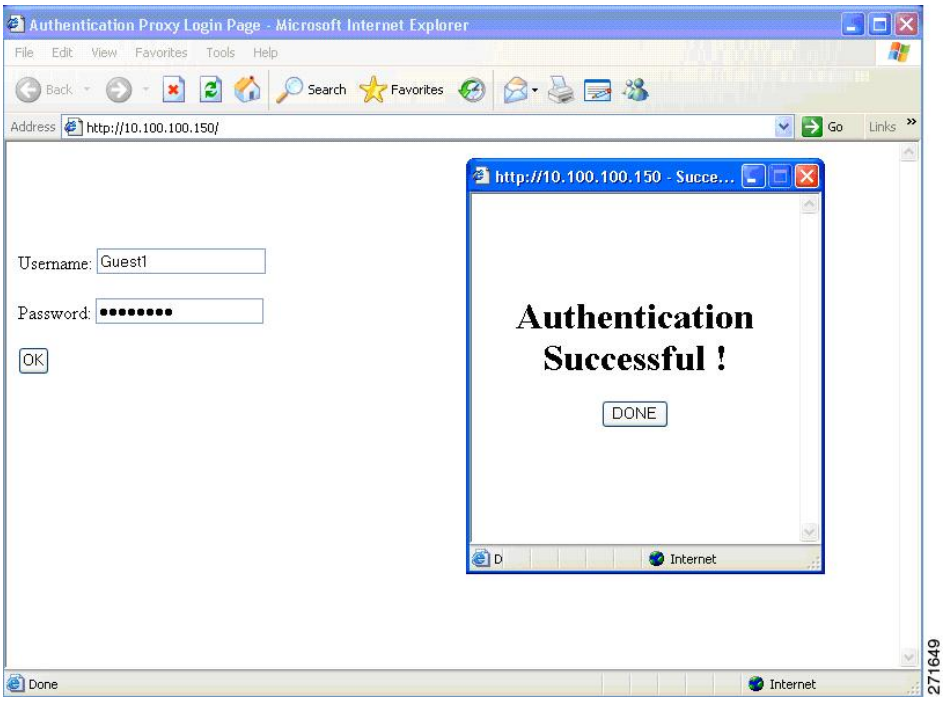
- ロゴまたはテキスト ファイルをバナーに追加する。
  - レガシーモード：**ip admission auth-proxy-banner http** *file-path* グローバル コンフィギュレーション コマンドを使用します。
  - 新スタイル モード：**parameter-map type webauth global banner** グローバル コンフィギュレーション コマンドを使用します。

図 *13* : 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 *14* : 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。

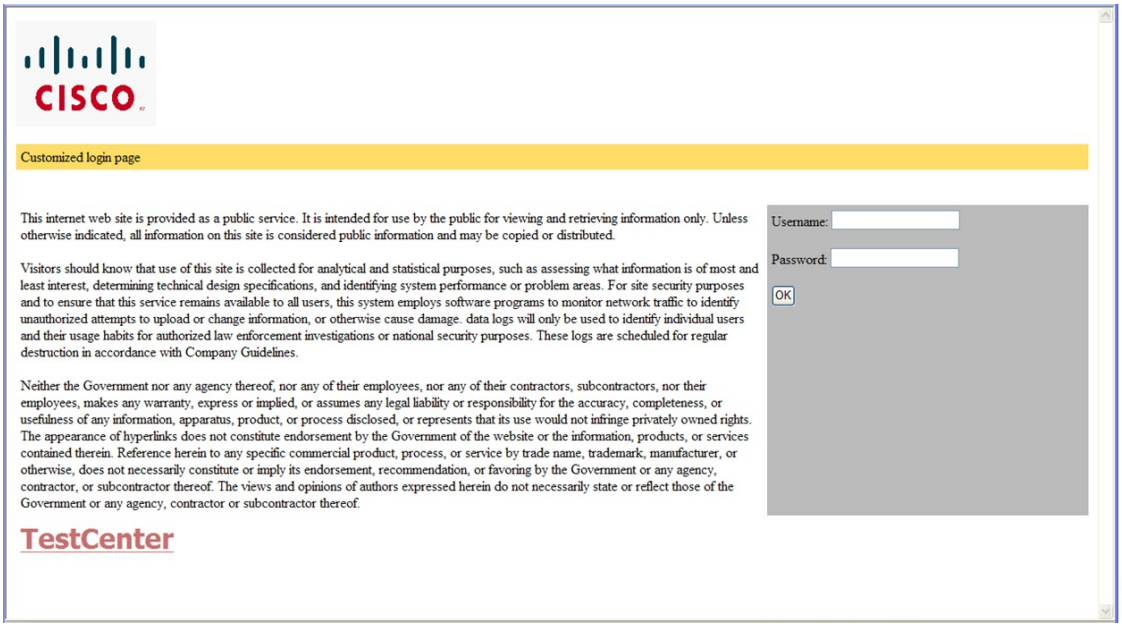
ガイドライン

- 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。
- ログイン ページを 1 つのフラッシュ上に、成功ページと失敗ページを別のフラッシュ（たとえば、スタック マスター、またはメンバのフラッシュ）にすることができます。
- 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 *15* : 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。

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2Web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3VLAN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2Web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 *16 :* 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 • IP アドレス • UDP 認証ポート • 鍵	• 指定なし • 指定なし
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もあります。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。
- IPv6 Web ベース認証はサポートされていません。
- 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。
- 仮想 IP 設定はサポートされていません。この制限により、ログアウトページはサポートされていません。
- 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、認証および暗号鍵を指定します。鍵は、RADIUS サーバーで使用する暗号鍵に一致するテキスト文字列でなければなりません。
- **key** *string* を指定する場合、鍵の中間、および末尾にスペースを使用します。鍵にスペースを使用する場合は、引用符が鍵の一部分である場合を除き、引用符で鍵を囲まないでください。鍵は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、および暗号鍵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。

（注） ACE の数が 20 以上の場合、IE3xxx プラットフォームで DACL のダウンロードが失敗します。この制限により、フラグメント化された RADIUS パケットが処理されないため、ISE からの DACL を完全にダウンロードすることができません。

回避策は、MTU を増やすか、DACL を 20 行未満に保つことです。

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. **exit**
8. **show ip admission**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 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	**configure terminal** 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	**ip admission name** *name* **proxy http** 例： `Device(config)# ip admission name webauth1 proxy http`	Web ベース許可の認証ルールを設定します。
ステップ 4	**interface** *type slot/port* 例： `Device(config)# interface gigabitethernet 1/0/1`	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。 *type* には、FastEthernet、GigabitEthernet、または TenGigabitEthernet を指定できます。
ステップ 5	**ip access-group** *name* 例： `Device(config-if)# ip access-group webauthag`	デフォルト ACL を適用します。
ステップ 6	**ip admission name** 例： `Device(config)# ip admission name`	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	**exit** 例：	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。

	コマンドまたはアクション	目的
	`Device# exit`	
ステップ 8	**show ip admission** 例： `Device# show ip admission`	ネットワークアドミッションのキャッシュエントリと Web 認証セッションに関する情報を表示します。

AAA 認証の設定

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 設定に追加する必要があります。

```
Device(config)# line vty 0 4
Device(config-line)# authorization commands 15 list1
Device(config-line)# exit
Device(config)# aaa authorization commands 15 list1 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 設定に追加する必要があります。

```
Device(config)# line vty 0 4
Device(config-line)# exit
Device(config)# aaa authorization commands 15 default group tacacs+
```

AAA 認証を設定するには、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 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** *string*
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	**enable** 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	**configure terminal** 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	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA 機能を有効にします。
ステップ 4	**aaa authentication login default group** {**tacacs+** | **radius**} 例： `Device(config)# aaa authentication login default group tacacs+`	ログイン時の認証方法のリストを定義します。 **named_authentication_list** は、31 文字未満の名前を示します。 **AAA_group_name** はサーバー グループ名を示します。サーバーグループ **server_name** をその先頭で定義する必要があります。
ステップ 5	**aaa authorization auth-proxy default group** {**tacacs+** | **radius**} 例： `Device(config)# aaa authorization auth-proxy default group tacacs+`	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	**tacacs server** *server-name* 例： `Device(config)# tacacs server yourserver`	AAA サーバーを指定します。
ステップ 7	**address** {**ipv4 | ipv6**} *ip address* 例： `Device(config-server-tacacs)# address ipv4 10.0.1.12`	TACACS サーバーの IP アドレスを設定します。
ステップ 8	**key** *string* 例：	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鍵を設定します。

	コマンドまたはアクション	目的
	`Device(config-server-tacacs)# key cisco123`	
ステップ 9	**end** 例： `Device(config-server-tacacs)# end`	TACACS サーバモードを終了し、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 vlan** *vlan interface number*
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	**enable** 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	**configure terminal** 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	**ip radius source-interface vlan** *vlan interface number* 例： `Device(config)# ip radius source-interface vlan`	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
	`80`	
ステップ 4	**radius server** *server name* 例： `Device(config)# radius server rsim address ipv4 172.16.0.1`	（任意）RADIUS サーバーの IP アドレスを指定します。
ステップ 5	**address** {**ipv4** | **ipv6**} *ip address* 例： `Device(config-radius-server)# address ipv4 10.0.1.2 auth-port 1550 acct-port 1560`	RADIUS サーバーの IP アドレスを設定します。
ステップ 6	**key** *string* 例： `Device(config-radius-server)# key rad123`	（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鍵を指定します。
ステップ 7	**exit** 例： `Device(config-radius-server)# exit`	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	**radius-server dead-criteria tries** *num-tries* 例： `Device(config)# radius-server dead-criteria tries 30`	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 *num-tries* の範囲は 1 ～ 100 です。
ステップ 9	**end** 例： `Device(config)# end`	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。

HTTP サーバーの設定

Web ベース認証を使用するには、device で HTTP サーバを有効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 のいずれかについてサーバーを有効にするには、次の手順に従います。

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	**enable** 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	**configure terminal** 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	**ip http server** 例： `Device(config)# ip http server`	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	**ip http secure-server** 例： `Device(config)# ip http secure-server`	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） **ip http secure-server** 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。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device# end`	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。

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、デフォルト HTML ページではなく、代わりの 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

device 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	**enable** 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	**configure terminal** 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	**ip admission proxy http login page file** *device:login-filename* 例：	device 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。*device:* はフラッシュ メモリです。

	コマンドまたはアクション	目的
	`Device(config)# ip admission proxy http login page file disk1:login.htm`	
ステップ 4	**ip admission proxy http success page file** *device:success-filename* 例： `Device(config)# ip admission proxy http success page file disk1:success.htm`	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	**ip admission proxy http failure page file** *device:fail-filename* 例： `Device(config)# ip admission proxy http fail page file disk1:fail.htm`	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	**ip admission proxy http login expired page file** *device:expired-filename* 例： `Device(config)# ip admission proxy http login expired page file disk1:expired.htm`	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	**end** 例： `Device# end`	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。

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. **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	**enable** 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	**configure terminal** 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	**ip admission max-login-attempts** *number* 例： `Device(config)# ip admission max-login-attempts 10`	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	**exit** 例： `Device# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

Web ベース認証ローカル 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**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 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	**configure terminal** 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	**ip admission auth-proxy-banner http** [*banner-text* | *file-path*] 例： `Device(config)# ip admission auth-proxy-banner http C My Switch C`	ローカル バナーを有効にします。 （任意）*C banner-text C*（*C* 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。
ステップ 4	**end** 例： `Device# end`	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。

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	**enable** 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	**clear ip auth-proxy cache** {*	*host ip address*} 例：	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
	`Device# clear ip auth-proxy cache 192.168.4.5`	
ステップ 3	**clear ip admission cache** {* | *host ip address*} 例： `# clear ip admission cache 192.168.4.5`	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 ベース認証の確認

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 *17*：特権 *EXEC* 表示コマンド

コマンド	目的
show authentication sessions method webauth	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。
show authentication sessions interface *type slot/port*[**details**]	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、**show access-session interface** コマンドを使用します。

Web ベース認証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
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

シスコのテクニカル サポート

説明	リンク
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。 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。 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。	http://www.cisco.com/support

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。