Cisco NX-OS Security コマンド リファレンス Release 4.0

September 18, 2008

Text Part Number: OL-15811-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。
米国サイト掲載ドキュメントとの差異が生じる場合があるため、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。

Cisco NX-OS Security コマンド リファレンス Release 4.0

CONTENTS

新規および変更された情報

この章では、『*Cisco NX-OS Security Command Reference, Release 4.0*』の新規および変更された機能のリリース固有の情報について説明しています。このマニュアルの最新バージョンは、次の Web サイトから入手できます。
http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/security/command/reference/sec_cmd_ref.html

Cisco NX-OS リリース 4.0 に関する追加情報を確認するには、次の Web サイトから入手可能な『*Cisco NX-OS Release Notes*』を参照してください。
http://www.cisco.com/en/US/docs/switches/datacenter/sw/4_0/nx-os/release/notes/401_nx-os_release_note.html

次の表に『*Cisco NX-OS Security Command Reference, Release 4.0*』の新規および変更された機能の要約および参照先を示します。

表 1　　リリースの新規および変更された情報 4.0

機能	変更内容	対象リリース	参照先
リモート ユーザの AAA 認証のデフォルト ユーザ ロール	**aaa user default-role** および **show aaa default-user role** コマンドが追加されました。	4.0(3)	A コマンド show コマンド
コントロール プレーン クラス マップでの IPv6 パケット ポリシング	**match**（クラス マップ）コマンドに対する IPv6 サポートが追加されました。	4.0(3)	M コマンド
パスワード強度のチェック	**password strength-check** および **show password strength-check** コマンドが追加されました。	4.0(3)	P コマンド show コマンド
Cisco TrustSec	**propagate-sgt** コマンドが追加されました。	4.0(3)	P コマンド
IPv6 の Telnet	**telnet6** コマンドが追加されました。	4.0(2)	T コマンド
コントロール プレーン ポリシング（CoPP）設定ステータス情報	**show copp status** コマンドが追加されました。	4.0(2)	show コマンド

はじめに

ここでは、『*Cisco NX-OS Security コマンド リファレンス Release 4.0*』の対象読者、構成、および表記法について説明します。また、関連資料の入手方法についても説明します。

この章は、次の内容で構成されています。

対象読者

このマニュアルは、NX-OS デバイスを設定および管理する経験豊富な管理者の方を対象としています。

マニュアルの構成

このマニュアルは、次の章で構成されています。

タイトル	説明
新規および変更された情報	新しい Cisco NX-OS ソフトウェア リリースの新規および変更された情報について説明します。
A コマンド	A で始まる Cisco NX-OS Security コマンドについて説明します。
C コマンド	B で始まる Cisco NX-OS Security コマンドについて説明します。
D コマンド	D で始まる Cisco NX-OS Security コマンドについて説明します。
E コマンド	E で始まる Cisco NX-OS Security コマンドについて説明します。
F コマンド	F で始まる Cisco NX-OS Security コマンドについて説明します。
G コマンド	G で始まる Cisco NX-OS Security コマンドについて説明します。
H コマンド	H で始まる Cisco NX-OS Security コマンドについて説明します。
I コマンド	I で始まる Cisco NX-OS Security コマンドについて説明します。
K コマンド	K で始まる Cisco NX-OS Security コマンドについて説明します。
L コマンド	L で始まる Cisco NX-OS Security コマンドについて説明します。
M コマンド	M で始まる Cisco NX-OS Security コマンドについて説明します。
N コマンド	N で始まる Cisco NX-OS Security コマンドについて説明します。
O コマンド	O で始まる Cisco NX-OS Security コマンドについて説明します。
P コマンド	P で始まる Cisco NX-OS Security コマンドについて説明します。
R コマンド	R で始まる Cisco NX-OS Security コマンドについて説明します。
S コマンド	S で始まる Cisco NX-OS Security コマンドについて説明します（**show** コマンドは除きます）。
show コマンド	Cisco NX-OS Security の **show** コマンドについて説明します。
T コマンド	T で始まる Cisco NX-OS Security コマンドについて説明します。
U コマンド	U で始まる Cisco NX-OS Security コマンドについて説明します。
V コマンド	V で始まる Cisco NX-OS Security コマンドについて説明します。

表記法

コマンドの説明では、次の表記法を使用しています。

表記	説明
太字	コマンドおよびキーワードは**太字**で示しています。
斜体	ユーザが値を指定する引数は、*イタリック体*で示しています。
[ ]	角カッコの中の要素は、省略可能です。
[x|y|z]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
ストリング	引用符を付けない一組の文字。ストリングの前後には引用符を使用しません。引用符を使用すると、その引用符も含めてストリングとみなされます。

出力例では、次の表記法を使用しています。

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

このマニュアルでは、次の表記法を使用しています。

（注） 「*注釈*」を意味します。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

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

ヒント 「*問題解決に役立つ情報*」です。

関連資料

Cisco NX-OS のマニュアルは、次の URL から入手できます。

http://www.cisco.com/en/US/products/ps9372/tsd_products_support_series_home.html

Cisco NX-OS のマニュアル セットは、次のマニュアルで構成されています。

リリース ノート

『*Cisco NX-OS Release Notes Release 4.0*』

NX-OS コンフィギュレーション ガイド

『*Cisco NX-OS Getting Started with Virtual Device Contexts Release 4.0*』

『*Cisco NX-OS Fundamentals Configuration Guide Release 4.0*』

『*Cisco NX-OS Interfaces Configuration Guide Release 4.0*』

『*Cisco NX-OS Layer 2 Switching Configuration Guide Release 4.0*』

『*Cisco NX-OS Quality of Service Configuration Guide Release 4.0*』

『*Cisco NX-OS Unicast Routing Configuration Guide Release 4.0*』

『*Cisco NX-OS Multicast Routing Configuration Guide Release 4.0*』

『*Cisco NX-OS Security Configuration Guide Release 4.0*』

『*Cisco NX-OS Virtual Device Context Configuration Guide Release 4.0*』

『*Cisco NX-OS Software Upgrade Guide Release 4.0*』

『*Cisco NX-OS Licensing Guide Release 4.0*』

『*Cisco NX-OS High Availability and Redundancy Guide Release 4.0*』

『*Cisco NX-OS System Management Configuration Guide Release 4.0*』

『*Cisco NX-OS XML Management Interface User Guide Release 4.0*』

『*Cisco NX-OS System Messages Reference*』

『*Cisco NX-OS MIB Quick Reference*』

NX-OS コマンド リファレンス

『*Cisco NX-OS Command Reference Master Index Release 4.0*』

『*Cisco NX-OS Fundamentals Command Reference Release 4.0*』

『*Cisco NX-OS Interfaces Command Reference Release 4.0*』

『*Cisco NX-OS Layer 2 Switching Command Reference Release 4.0*』

『*Cisco NX-OS Quality of Service Command Reference Release 4.0*』

『*Cisco NX-OS Unicast Routing Command Reference Release 4.0*』

『*Cisco NX-OS Multicast Routing Command Reference Release 4.0*』

『*Cisco NX-OS Security Command Reference Release 4.0*』

『*Cisco NX-OS Virtual Device Context Command Reference Release 4.0*』

『*Cisco NX-OS High Availability and Redundancy Command Reference Release 4.0*』

『*Cisco NX-OS System Management Command Reference Release 4.0*』

その他のソフトウェアのマニュアル

『*Cisco NX-OS Troubleshooting Guide Release 4.0*』

マニュアルの入手方法、テクニカル サポート、およびセキュリティ ガイドライン

マニュアルの入手方法、テクニカル サポート、マニュアルに関するフィードバックの提供、セキュリティ ガイドライン、および推奨エイリアスや一般的なシスコのマニュアルについては、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

シスコのテクニカル サポート

次の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。

http://www.cisco.com/en/US/support/index.html

以下を含むさまざまな作業にこの Web サイトが役立ちます。

- テクニカル サポートを受ける
- ソフトウェアをダウンロードする
- セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける
- ツールおよびリソースへアクセスする
  - Product Alert の受信登録
  - Field Notice の受信登録
  - Bug Toolkit を使用した既知の問題の検索
- Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する
- トレーニング リソースへアクセスする
- TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する

Japan テクニカル サポート Web サイトでは、Technical Support Web サイト（http://www.cisco.com/techsupport）の、利用頻度の高いドキュメントを日本語で提供しています。

Japan テクニカル サポート Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

Service Request ツールの使用

Service Request ツールには、次の URL からアクセスできます。

http://www.cisco.com/techsupport/servicerequest

日本語版の Service Request ツールは次の URL からアクセスできます。

http://www.cisco.com/jp/go/tac/sr/

シスコの世界各国の連絡先一覧は、次の URL で参照できます。

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

その他の情報の入手方法

シスコの製品、サービス、テクノロジー、ネットワーキング ソリューションに関する情報について、さまざまな資料をオンラインで入手できます。

- シスコの E メール ニュースレターなどの配信申し込みについては、Cisco Subscription Center にアクセスしてください。

  http://www.cisco.com/offer/subscribe

- 日本語の月刊 Email ニュースレター「Cisco Customer Bridge」については、下記にアクセスください。

  http://www.cisco.com/web/JP/news/cisco_news_letter/ccb/

- シスコ製品に関する変更やアップデートの情報を受信するには、Product Alert Tool にアクセスし、プロファイルを作成して情報の配信を希望する製品を選択してください。Product Alert Tool には、次の URL からアクセスできます。

  http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

- 『*Cisco Product Quick Reference Guide*』はリファレンス ツールで、パートナーを通じて販売されている多くのシスコ製品に関する製品概要、主な機能、製品番号、および簡単な技術仕様が記載されています。『*Cisco Product Quick Reference Guide*』を発注するには、次の URL にアクセスしてください。

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

- ネットワークの運用面の信頼性を向上させることのできる最新の専門的サービス、高度なサービス、リモート サービスに関する情報については、Cisco Services Web サイトを参照してください。Cisco Services Web サイトには、次の URL からアクセスできます。

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

- Cisco Marketplace では、さまざまなシスコの書籍、参考資料、マニュアル、ロゴ入り商品を提供しています。Cisco Marketplace には、次の URL からアクセスできます。

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

- DVD に収録されたシスコの技術マニュアル（Cisco Product Documentation DVD）は、Product Documentation Store で発注できます。Product Documentation Store には、次の URL からアクセスできます。

  http://www.cisco.com/go/marketplace/docstore

- 日本語マニュアルの DVD は、マニュアルセンターから発注できます。マニュアルセンターには下記よりアクセスください。

  http://www.cisco.com/japanese/warp/public/3/jp/service/manual_j/manual_center/index.shtml

- Cisco Press では、ネットワーク、トレーニング、認定関連の出版物を発行しています。Cisco Press には、次の URL からアクセスできます。

  http://www.ciscopress.com

- 日本語のシスコプレスの情報は以下にアクセスください。

  http://www.seshop.com/se/ciscopress/default.asp

- 『*Internet Protocol Journal*』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『*Internet Protocol Journal*』には、次の URL からアクセスできます。

  http://www.cisco.com/ipj

- 『*What's New in Cisco Product Documentation*』は、シスコ製品の最新マニュアル リリースに関する情報を提供するオンライン資料です。毎月更新されるこの資料は、製品カテゴリ別にまとめられているため、目的の製品マニュアルを見つけることができます。

  http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

- シスコの Web サイトの各国語版へは、次の URL からアクセスしてください。

  http://www.cisco.com/public/countries_languages.shtml

A コマンド

この章では、A で始まる Cisco NX-OS Security コマンドについて説明します。

aaa accounting default

アカウンティングの Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）方式を設定するには、**aaa accounting default** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

aaa accounting default {**group** *group-list* | **local**}

no aaa accounting default {**group** *group-list* | **local**}

シンタックスの説明

group	アカウンティングにサーバ グループを使用するように指定します。
group-list	サーバ グループをスペースで区切って指定します。リストには、次のようなサーバ グループを含めることができます。 • **radius** ― 設定済みのすべての RADIUS サーバ。 • 設定済みの任意の RADIUS または TACACS+ サーバ グループ名。 リストには、最大 8 つのグループ名を格納できます。
local	アカウンティングにローカル データベースを使用するように指定します。

デフォルト

local

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

group *group-list* 方式は、以前に定義された一連のサーバを指します。ホスト サーバを設定するには、**radius-server host** および **tacacs-server host** コマンドを使用します。サーバのネームド グループを作成するには、**aaa group server** コマンドを使用します。

デバイス上の RADIUS サーバ グループを表示するには、**show aaa group** コマンドを使用します。

group 方式、**local** 方式、または両方を指定した場合にそれらの方式が失敗すると、アカウンティング認証は失敗します。

複数のサーバ グループを指定した場合には、リストに指定した順番どおりに NX-OS ソフトウェアが各グループをチェックします。

このコマンドにライセンスは必要ありません。

例

次に、AAA アカウンティングに任意の RADIUS サーバを設定する例を示します。

```
switch# config t
switch(config)# aaa accounting default group radius
```

関連コマンド

コマンド	説明
aaa group server	AAA RADIUS サーバ グループを設定します。
radius-server host	RADIUS サーバを設定します。
show aaa accounting	AAA アカウンティング ステータス情報を表示します。
show aaa group	AAA サーバ グループ情報を表示します。
tacacs-server host	TACACS+ サーバを設定します。

aaa accounting dot1x

802.1X 認証の AAA アカウンティング方式を設定するには、**aaa accounting dot1x** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

aaa accounting dot1x {**group** *group-list* | **local**}

no aaa accounting dot1x {**group** *group-list* | **local**}

シンタックスの説明

group	アカウンティングにサーバ グループを使用するように指定します。
group-list	RADIUS サーバ グループをスペースで区切って指定します。リストには、次のようなサーバ グループを含めることができます。 • **radius** ― 設定済みのすべての RADIUS サーバ • 設定済みの任意の RADIUS サーバ グループ名 リストには、最大 8 つのグループ名を格納できます。
local	アカウンティングにローカル データベースを使用するように指定します。

デフォルト

local

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

group *group-list* 方式は、以前に定義された一連の RADIUS サーバを指します。ホスト サーバを設定するには、**radius-server host** コマンドを使用します。サーバのネームド グループを作成するには、**aaa group server** コマンドを使用します。

デバイス上の RADIUS サーバ グループを表示するには、**show aaa group** コマンドを使用します。

group 方式、**local** 方式、または両方を指定した場合にそれらの方式が失敗すると、アカウンティング認証は失敗します。

複数のサーバ グループを指定した場合には、リストに指定した順番どおりに NX-OS ソフトウェアが各グループをチェックします。

このコマンドにライセンスは必要ありません。

例

次に、AAA アカウンティングに任意の RADIUS サーバを設定する例を示します。

```
switch# config t
switch(config)# aaa accounting default group radius
```

関連コマンド

コマンド	説明
aaa group server radius	AAA RADIUS サーバ グループを設定します。
radius-server host	RADIUS サーバを設定します。
show aaa accounting	AAA アカウンティング ステータス情報を表示します。
show aaa group	AAA サーバ グループ情報を表示します。

aaa authentication cts default group

Cisco TrustSec 認証のデフォルト AAA RADIUS サーバ グループを設定するには、**aaa authentication cts default group** コマンドを使用します。デフォルト AAA 認証サーバ グループ リストからサーバ グループを削除するには、このコマンドの **no** 形式を使用します。

aaa authentication cts default group *group-list*

no aaa authentication cts default group *group-list*

シンタックスの説明

group-list	RADIUS サーバ グループをスペースで区切って指定します。リストには、次のようなサーバ グループを含めることができます。 • **radius** ― 設定済みのすべての RADIUS サーバ • 設定済みの任意の RADIUS サーバ グループ名 リストには、最大 8 つのグループ名を格納できます。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

group-list は、以前に定義された一連の RADIUS サーバを指します。ホスト サーバを設定するには、**radius-server host** コマンドを使用します。サーバのネームド グループを作成するには、**aaa group server** コマンドを使用します。

デバイス上の RADIUS サーバ グループを表示するには、**show aaa group** コマンドを使用します。

複数のサーバ グループを指定した場合には、リストに指定した順番どおりに NX-OS ソフトウェアが各グループをチェックします。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、Cisco TrustSec のデフォルト AAA 認証 RADIUS サーバ グループを設定する例を示します。

```
switch# config t
swtich(config)# aaa authentication cts default group RadGroup
```

関連コマンド

コマンド	説明
aaa group server	AAA サーバ グループを設定します。
feature cts	Cisco TrustSec 機能をイネーブルにします。
radius-server host	RADIUS サーバを設定します。
show aaa authentication	AAA 認証設定を表示します。
show aaa group	AAA サーバ グループを表示します。

aaa authentication dot1x default group

802.1X の AAA 認証方式を設定するには、**aaa authentication dot1x default group** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

aaa authentication dot1x default group *group-list*

no aaa authentication dot1x default group *group-list*

シンタックスの説明

group-list	RADIUS サーバ グループをスペースで区切って指定します。リストには、次のようなサーバ グループを含めることができます。 • **radius** ― 設定済みのすべての RADIUS サーバ • 設定済みの任意の RADIUS サーバ グループ名 リストには、最大 8 つのグループ名を格納できます。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

group-list は、以前に定義された一連の RADIUS サーバを指します。ホスト サーバを設定するには、**radius-server host** コマンドを使用します。サーバのネームド グループを作成するには、**aaa group server** コマンドを使用します。

デバイス上の RADIUS サーバ グループを表示するには、**show aaa group** コマンドを使用します。

複数のサーバ グループを指定した場合には、リストに指定した順番どおりに NX-OS ソフトウェアが各グループをチェックします。

このコマンドにライセンスは必要ありません。

例

次に、802.1X 認証方式を設定する例を示します。

```
switch# config t
switch(config)# aaa authentication do1x default group Dot1xGroup
```

次に、デフォルトの 802.1X 認証方式に戻す例を示します。

```
switch# config t
switch(config)# no aaa authentication do1x default group Dot1xGroup
```

関連コマンド

コマンド	説明
feature dot1x	802.1X をイネーブルにします。
radius-server host	RADIUS サーバを設定します。
show aaa authentication	AAA 認証設定を表示します。
show aaa group	AAA サーバ グループを表示します。

aaa authentication eou default group

EAP over UDP（EoU）の AAA 認証方式を設定するには、**aaa authentication eou default group** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

aaa authentication eou default group *group-list*

no aaa authentication eou default group *group-list*

シンタックスの説明

group-list	RADIUS サーバ グループをスペースで区切って指定します。リストには、次のようなサーバ グループを含めることができます。 • **radius** ― 設定済みのすべての RADIUS サーバ • 設定済みの任意の RADIUS サーバ グループ名 リストには、最大 8 つのグループ名を格納できます。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルト EAPoUDP 認証方式を設定する前に、**feature eou** コマンドを使用して EAPoUDP をイネーブルにする必要があります。

group-list は、以前に定義された一連の RADIUS サーバを指します。ホスト サーバを設定するには、**radius-server host** コマンドを使用します。サーバのネームド グループを作成するには、**aaa group server** コマンドを使用します。

デバイス上の RADIUS サーバ グループを表示するには、**show aaa group** コマンドを使用します。

複数のサーバ グループを指定した場合には、リストに指定した順番どおりに NX-OS ソフトウェアが各グループをチェックします。

このコマンドにライセンスは必要ありません。

例

次に、EAPoUDP 認証方式を設定する例を示します。

```
switch# config t
switch(config)# aaa authentication eou default group EoUGroup
```

次に、デフォルトの EAPoUDP 認証方式に戻す例を示します。

```
switch# config t
switch(config)# no aaa authentication eou default group EoUGroup
```

関連コマンド

コマンド	説明
feature eou	EAPoUDP をイネーブルにします。
radius-server host	RADIUS サーバを設定します。
show aaa authentication	AAA 認証設定を表示します。
show aaa group	AAA サーバ グループを表示します。

aaa authentication login console

コンソール ログインの AAA 認証方式を設定するには、**aaa authentication login console** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

aaa authentication login console {**group** *group-list*} [**none**] | **local** | **none**}

no aaa authentication login console {**group** *group-list* [**none**] | **local** | **none**}

シンタックスの説明

group	認証にサーバ グループを使用するように指定します。
group-list	サーバ グループをスペースで区切って指定します。リストには、次のようなサーバ グループを含めることができます。 • **radius** ― 設定済みのすべての RADIUS サーバ • **tacacs+** ― 設定済みのすべての TACACS+ サーバ • 設定済みの任意の RADIUS または TACACS+ サーバ グループ名
none	認証にユーザ名を使用するように指定します。
local	認証にローカル データベースを使用するように指定します。

デフォルト

local

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

group radius、***group tacacs+***、および ***group*** *group-list* 方式は、以前に定義された RADIUS または TACACS+ サーバを指します。ホスト サーバを設定するには、**radius-server host** または **tacacs-server host** コマンドを使用します。サーバのネームド グループを作成するには、**aaa group server** コマンドを使用します。

デバイス上の RADIUS サーバ グループを表示するには、**show aaa group** コマンドを使用します。

複数のサーバ グループを指定した場合には、リストに指定した順番どおりに NX-OS ソフトウェアが各グループをチェックします。

group 方式または **local** 方式を指定した場合にそれらの方式が失敗すると、認証は失敗する可能性があります。**none** 方式を単独または **group** 方式の後ろに指定した場合、認証は常に成功します。

このコマンドは、デフォルト VDC（VDC 1）でのみ機能します。

このコマンドにライセンスは必要ありません。

例

次に、コンソール ログインの AAA 認証方式を設定する例を示します。

```
switch# config t
switch(config)# aaa authentication login console group radius
```

次に、デフォルトのコンソール ログインの AAA 認証方式に戻す例を示します。

```
switch# config t
switch(config)# no aaa authentication login console group radius
```

関連コマンド

コマンド	説明
aaa group server	AAA サーバ グループを設定します。
radius-server host	RADIUS サーバを設定します。
show aaa authentication	AAA 認証情報を表示します。
show aaa group	AAA サーバ グループを表示します。
tacacs-server host	TACACS+ サーバを設定します。

aaa authentication login default

デフォルト AAA 認証方式を設定するには、**aaa authentication login default** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

aaa authentication login default {**group** *group-list*} [**none**] | **local** | **none**}

no aaa authentication login default {**group** *group-list* [**none**] | **local** | **none**}

シンタックスの説明

group	認証に使用するサーバ グループ リストを指定します。
group-list	サーバ グループをスペースで区切って指定します。リストには、次のようなサーバ グループを含めることができます。 • **radius** ― 設定済みのすべての RADIUS サーバ • **tacacs+** ― 設定済みのすべての TACACS+ サーバ • 設定済みの任意の RADIUS または TACACS+ サーバ グループ名
none	（任意）認証にユーザ名を使用するように指定します。
local	認証にローカル データベースを使用するように指定します。

デフォルト

local

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

group radius、***group tacacs+***、および ***group*** *group-list* 方式は、以前に定義された RADIUS または TACACS+ サーバを指します。ホスト サーバを設定するには、**radius-server host** または **tacacs-server host** コマンドを使用します。サーバのネームド グループを作成するには、**aaa group server** コマンドを使用します。

デバイス上の RADIUS サーバ グループを表示するには、**show aaa group** コマンドを使用します。

複数のサーバ グループを指定した場合には、リストに指定した順番どおりに NX-OS ソフトウェアが各グループをチェックします。

group 方式または **local** 方式を指定した場合にそれらの方式が失敗すると、認証は失敗します。**none** 方式を単独または **group** 方式の後ろに指定した場合、認証は常に成功します。

このコマンドにライセンスは必要ありません。

例

次に、コンソール ログインの AAA 認証方式を設定する例を示します。

```
switch# config t
switch(config)# aaa authentication login default group radius
```

次に、デフォルトのコンソール ログインの AAA 認証方式に戻す例を示します。

```
switch# config t
switch(config)# no aaa authentication login default group radius
```

関連コマンド

コマンド	説明
aaa group server	AAA サーバ グループを設定します。
radius-server host	RADIUS サーバを設定します。
show aaa authentication	AAA 認証情報を表示します。
show aaa group	AAA サーバ グループを表示します。
tacacs-server host	TACACS+ サーバを設定します。

aaa authentication login error-enable

コンソールに AAA 認証失敗メッセージが表示されるように設定するには、**aaa authentication login error-enable** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

aaa authentication login error-enable

no aaa authentication login error-enable

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

ログイン時にリモート AAA サーバからの応答がない場合には、ローカル ユーザ データベースへのロールオーバーによってログインが続行されます。そのような場合に、ログイン失敗メッセージの表示がイネーブルになっていると、ユーザ端末に次のメッセージが表示されます。

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

このコマンドにライセンスは必要ありません。

例

次に、AAA 認証失敗メッセージのコンソールへの表示をイネーブルにする例を示します。

```
switch# config t
switch(config)# aaa authentication login error-enable
```

次に、AAA 認証失敗メッセージのコンソールへの表示をディセーブルにする例を示します。

```
switch# config t
switch(config)# no aaa authentication login error-enable
```

関連コマンド

コマンド	説明
show aaa authentication login error-enable	AAA 認証失敗メッセージ表示のステータスを表示します。

aaa authentication login mschap

ログイン時の Microsoft Challenge Handshake Authentication Protocol（MS-CHAP; マイクロソフト チャレンジ ハンドシェーク認証プロトコル）認証をイネーブルにするには、**aaa authentication login mschap** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

aaa authentication login mschap

no aaa authentication login mschap

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドにライセンスは必要ありません。

例

次に、MSCHAP 認証をイネーブルにする例を示します。

```
switch# config t
switch(config)# aaa authentication login mschap
```

次に、MSCHAP 認証をディセーブルにする例を示します。

```
switch# config t
switch(config)# no aaa authentication login mschap
```

関連コマンド

コマンド	説明
show aaa authentication login mschap	MSCHAP 認証のステータスを表示します。

aaa authorization cts default group

Cisco TrustSec 認可のデフォルト AAA RADIUS サーバ グループを設定するには、**aaa authorization cts default group** コマンドを使用します。デフォルト AAA 認可サーバ グループ リストからサーバ グループを削除するには、このコマンドの **no** 形式を使用します。

aaa authorization cts default group *group-list*

no aaa authorization cts default group *group-list*

シンタックスの説明

group-list	RADIUS サーバ グループをスペースで区切って指定します。リストには、次のようなサーバ グループを含めることができます。 • **radius** ― 設定済みのすべての RADIUS サーバ • 設定済みの任意の RADIUS サーバ グループ名 リストには、最大 8 つのグループ名を格納できます。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

group-list は、以前に定義された一連の RADIUS サーバを指します。ホスト サーバを設定するには、**radius-server host** コマンドを使用します。サーバのネームド グループを作成するには、**aaa group server** コマンドを使用します。

デバイス上の RADIUS サーバ グループを表示するには、**show aaa group** コマンドを使用します。

複数のサーバ グループを指定した場合には、リストに指定した順番どおりに NX-OS ソフトウェアが各グループをチェックします。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、Cisco TrustSec のデフォルト AAA 認可 RADIUS サーバ グループを設定する例を示します。

```
switch# config t
swtich(config)# aaa authorization cts default group RadGroup
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show aaa authorization	AAA 認可設定を表示します。
show aaa group	AAA サーバ グループを表示します。

aaa group server radius

RADIUS サーバ グループを作成して、RADIUS サーバ グループ コンフィギュレーション モードを開始するには、**aaa group server radius** コマンドを使用します。RADIUS サーバ グループを削除するには、このコマンドの **no** 形式を使用します。

aaa group server radius *group-name*

no aaa group server radius *group-name*

シンタックスの説明

group-name	RADIUS サーバ グループ名。名前には英数字を使用します。大文字と小文字が区別され、最大 64 文字まで可能です。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドにライセンスは必要ありません。

例

次に、RADIUS サーバ グループを作成し、RADIUS サーバ設定モードを開始する例を示します。

```
switch# config t
switch(config)# aaa group server radius RadServer
switch(config-radius)#
```

次に、RADIUS サーバ グループを削除する例を示します。

```
switch# config t
switch(config)# no aaa group server radius RadServer
```

関連コマンド

コマンド	説明
show aaa groups	サーバ グループ情報を表示します。

aaa group server tacacs+

TACACS+ サーバ グループを作成して、TACACS+ サーバ グループ コンフィギュレーション モードを開始するには、**aaa group server tacacs+** コマンドを使用します。TACACS+ サーバ グループを削除するには、このコマンドの **no** 形式を使用します。

aaa group server tacacs+ *group-name*

no aaa group server tacacs+ *group-name*

シンタックスの説明

group-name	TACACS+ サーバ グループ名。名前には英数字を使用します。大文字と小文字が区別され、最大 64 文字まで可能です。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

TACACS+ を設定する前に **feature tacacs+** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

例

次に、TACACS+ サーバ グループを作成し、TACACS+ サーバ設定モードを開始する例を示します。

```
switch# config t
switch(config)# aaa group server tacacs+ TacServer
switch(config-radius)#
```

次に、TACACS+ サーバ グループを削除する例を示します。

```
switch# config t
switch(config)# no aaa group server tacacs+ TacServer
```

関連コマンド

コマンド	説明
feature tacacs+	TACACS+ をイネーブルにします。
show aaa groups	サーバ グループ情報を表示します。

aaa user default-role

ユーザ ロールを持たないリモート ユーザが、RADIUS または TACACS+ 経由でデフォルト ユーザ ロールを使用してデバイスにログインできるようにするには、**aaa user default-role** コマンドを使用します。リモート ユーザのデフォルト ユーザ ロールをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa user default-role

no aaa user default-role

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

イネーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(3)	このコマンドが導入されました。

使用上のガイドライン

Virtual Device Context（VDC; バーチャル デバイス コンテキスト）のこの機能は、必要に応じてイネーブルまたはディセーブルにできます。デフォルト VDC の場合、デフォルト ロールは network-operator です。非デフォルト VDC の場合、デフォルト VDC は vdc-operator です。AAA デフォルト ユーザ ロール機能がディセーブルの場合は、ユーザ ロールを持たないリモート ユーザはデバイスにログインできません。

このコマンドにライセンスは必要ありません。

例

次に、リモート ユーザの AAA 認証のデフォルト ユーザ ロールをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# aaa user default-role
```

次に、リモート ユーザの AAA 認証のデフォルト ユーザ ロールをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no aaa user default-role
```

関連コマンド

コマンド	説明
show aaa user default-role	AAA デフォルト ユーザ ロール機能のステータスを表示します。

absolute

特定の開始日時、特定の終了日時、またはその両方が指定された時間範囲を指定するには、**absolute** コマンドを使用します。絶対時間範囲を削除するには、このコマンドの **no** 形式を使用します。

[*sequence-number*] **absolute** [**start** *time date*] [**end** *time date*]

no {*sequence-number* | **absolute** [**start** *time date*] [**end** *time date*]}

シンタックスの説明

sequence-number	（任意）ルールのシーケンス番号。この番号により、時間範囲内の番号が振られた場所にデバイスがコマンドを挿入します。時間範囲内のルールの順序は、シーケンス番号によって維持されます。 シーケンス番号には、1 から 4294967295 までの任意の整数を使用できます。 時間範囲内の最初のルールは、デフォルトでシーケンス番号 10 を持ちます。 シーケンス番号を指定しない場合は、デバイスによってそのルールが時間範囲の最後に追加され、そのルールの直前のルールのシーケンス番号よりも 10 大きい番号が割り当てられます ルールにシーケンス番号を再割り当てするには、**resequence** コマンドを使用します。
start *time date*	（任意）デバイスが、時間範囲に関連付けられた **permit**（許可）ルールおよび **deny**（拒否）ルールの実行を開始する正確な日時を指定します。開始日時を指定しない場合、デバイスは **permit** ルールまたは **deny** ルールを即座に実行します。 *time* 引数と *date* 引数の値についての詳細は、「使用上のガイドライン」セクションを参照してください。
end *time date*	（任意）デバイスが、時間範囲に関連付けられた **permit** コマンドおよび **deny** コマンドの実行を停止する正確な日時を指定します。終了日時を指定しない場合、デバイスは毎回、開始日時が過ぎた時点で **permit** ルールまたは **deny** ルールを実行します。 *time* 引数と *date* 引数の値についての詳細は、「使用上のガイドライン」セクションを参照してください。

デフォルト

なし

コマンド モード

時間範囲コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバイスは、すべての時間範囲ルールを現地時間で解釈します。

start キーワードおよび ***end*** キーワードの両方を省略すると、デバイスは絶対時間範囲が常にアクティブであるとみなします。

time 引数は、*hours*:*minutes* または *hours*:*minutes*:*seconds* の形式で 24 時間表記で指定します。たとえば、24 時間表記では 8:00 a.m. は 8:00、8:00 p.m. は 20:00 になります。

date 引数は、*day month year* の形式で指定します。最小有効開始日時は 00:00:00 1 January 1970、最大有効開始日時は 23:59:59 31 December 2037 です。

このコマンドにライセンスは必要ありません。

例

次に、2007 年 9 月 17 日の午前 7 時に開始され、2007 年 9 月 19 日の午後 11 時 59 分 59 秒に終了する絶対時間ルールを作成する例を示します。

```
switch# config t
switch(config)# time-range conference-remote-access
switch(config-time-range)# absolute start 07:00 17 September 2007 end 23:59:59 19
September 2007
```

関連コマンド

コマンド	説明
periodic	定期的な時間範囲ルールを設定します。
time-range	IPv4 ACL で使用される時間範囲を設定します。

accept-lifetime

別のデバイスとのキー交換時にデバイスがそのキーを受け入れる期間を指定するには、**accept-lifetime** コマンドを使用します。期間を削除するには、このコマンドの **no** 形式を使用します。

accept-lifetime [**local**] *start-time* [**duration** *duration-value* | **infinite** | *end-time*]

no accept-lifetime [**local**] *start-time* [**duration** *duration-value* | **infinite** | *end-time*]

シンタックスの説明

local	（任意）デバイスが設定された時間を現地時間として扱うように指定します。デフォルトでは、デバイスは *start-time* 引数および *end-time* 引数を UTC として扱います。
start-time	デバイスがキーの受け入れを開始する時刻と日付。 *start-time* 引数の値についての詳細は、「使用上のガイドライン」セクションを参照してください。
duration *duration-value*	（任意）ライフタイムの長さを秒単位で指定します。最大値は 2147483646 秒です（約 68 年）。
infinite	（任意）キーが期限切れにならないように指定します。
end-time	（任意）デバイスがキーの受け入れを停止する時刻と日付。 *time of day* 引数と *date* 引数の値についての詳細は、「使用上のガイドライン」セクションを参照してください。

デフォルト

infinite

コマンド モード

キー コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトで、デバイスはすべての時間範囲ルールを UTC で解釈します。

デフォルトでは、別のデバイスとのキー交換時にデバイスがキーを受け入れる期間（受け入れライフタイム）は infinite です。つまり、キーは永久に有効です。

start-time 引数および *end-time* 引数の両方に、次の形式で時間と日付の要素が必要です。

hour[:*minute*[:*second*]] *month day year*

24 時間表記で指定します。たとえば、24 時間表記では 8:00 a.m. は 8:00、8:00 p.m. は 20:00 になります。最小有効 *start-time* は 00:00:00 Jan 1 1970 であり、最大有効 *start-time* は 23:59:59 Dec 31 2037 です。

このコマンドにライセンスは必要ありません。

例

次に、2008 年 6 月 13 日の午前零時に開始され、2008 年 8 月 12 日の午後 11 時 59 分 59 秒に終了する受け入れライフタイムを作成する例を示します。

```
switch# configure terminal
switch(config)# key chain glbp-keys
switch(config-keychain)# key 13
switch(config-keychain-key)# accept-lifetime 00:00:00 Jun 13 2008 23:59:59 Sep 12 2008
switch(config-keychain-key)#
```

関連コマンド

コマンド	説明
key	キーを設定します。
keychain	キーチェーンを設定します。
key-string	キーストリングを設定します。
send-lifetime	キーの送信ライフタイムを設定します。
show key chain	キーチェーン設定を表示します。

action

パケットが VLAN Access Control List（VACL; VLAN アクセス コントロール リスト）の **permit** コマンドと一致した場合にデバイスが実行する処理を指定するには、**action** コマンドを使用します。**action** コマンドを削除するには、このコマンドの **no** 形式を使用します。

action drop [**log**]

no action drop [**log**]

action forward [**capture**]

no action forward [**capture**]

action redirect {**ethernet** *slot/port* | **port-channel** *channel-number.subinterface-number*}

no action redirect {**ethernet** *slot/port* | **port-channel** *channel-number.subinterface-number*}

シンタックスの説明

drop	デバイスがパケットをドロップするように指定します。
log	（任意）デバイスが、***drop*** キーワードに基づいてドロップしたパケットを記録するように指定します。
forward	デバイスがパケットをその宛先ポートに転送するように指定します。
capture	（任意）デバイスが、パケットの宛先ポートに加え、キャプチャ機能がイネーブルになっているポートにパケットを転送するように指定します。
redirect	デバイスがパケットをインターフェイスにリダイレクトするように指定します。
ethernet *slot/port*	デバイスがパケットをリダイレクトするイーサネット インターフェイスを指定します。
port-channel *channel-number.subinterface-number*	デバイスがパケットをリダイレクトするポート チャネル インターフェイスを指定します。 **（注）** *channel-number* 引数と *subinterface-number* 引数間には、ドット区切り文字が必要です。

デフォルト

なし

コマンド モード

VALN アクセス マップ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

action コマンドでは、パケットが **match** コマンドによって指定された ACL 内の条件に一致した場合にデバイスが実行する処理を指定します。

このコマンドにライセンスは必要ありません。

例

次に、vlan-map-01 という名前の VLAN アクセス マップを作成し、ip-acl-01 という名前の IPv4 ACL をマップに割り当て、デバイスが ACL と一致したパケットを転送するように指定し、マップと一致するトラフィックの統計情報をイネーブルにする例を示します。

```
switch# config t
switch(config)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-01
switch(config-access-map)# action forward
switch(config-access-map)# statistics
```

関連コマンド

コマンド	説明
match	VLAN アクセス マップでのトラフィック フィルタリング用の ACL を指定します。
show vlan access-map	すべてまたは 1 つの VLAN アクセス マップを表示します。
show vlan filter	VLAN アクセス マップの適用方法についての情報を表示します。
statistics	Access Control List（ACL; アクセス コントロール リスト）または VLAN アクセス マップの統計情報をイネーブルにします。
vlan access-map	VLAN アクセス マップを設定します。
vlan filter	1 つ以上の VLAN に VLAN アクセス マップを適用します。

arp access-list

Address Resolution Protocol（ARP; アドレス解決プロトコル）ACL を作成するか、特定の ARP ACL の ARP アクセス リスト コンフィギュレーション モードを開始するには、**arp access-list** コマンドを使用します。ARP ACL を削除するには、このコマンドの **no** 形式を使用します。

arp access-list *access-list-name*

no arp access-list *access-list-name*

シンタックスの説明

access-list-name	ARP ACL の名前。最大で 64 文字の英数字を使用でき、大文字と小文字が区別されます。名前にはスペースまたは引用符を含めることはできません。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

DHCP スヌーピングを使用できない場合は、ARP ACL を使用して ARP トラフィックをフィルタリングします。

デフォルトでは、ARP ACL は定義されていません。

arp access-list コマンドを使用すると、デバイスによって ARP アクセス リスト コンフィギュレーション モードが開始されます。このモードでは、ARP **deny** コマンドおよび **permit** コマンドを使用して、ACL のルールを設定できます。指定の ACL が存在しない場合は、このコマンドを入力した時点でデバイスによって作成されます。

ARP ACL を VLAN に適用するには、**ip arp inspection filter** コマンドを使用します。

このコマンドにライセンスは必要ありません。

例

次に、arp-acl-01 という名前の ARP ACL の ARP アクセス リスト コンフィギュレーション モードを開始する例を示します。

```
switch# conf t
switch(config)# arp access-list arp-acl-01
switch(config-arp-acl)#
```

関連コマンド

コマンド	説明
deny（ARP）	ARP ACL の拒否ルールを設定します。
ip arp inspection filter	ARP ACL を VLAN に適用します。
permit（ARP）	ARP ACL の許可ルールを設定します。
show arp access-lists	すべての ARP ACL または特定の ARP ACL を表示します。

C コマンド

この章では、C で始まる Cisco NX-OS Security コマンドについて説明します。

class（ポリシー マップ）

コントロール プレーン ポリシー マップのコントロール プレーン クラス マップを指定するには、**class** コマンドを使用します。コントロール プレーン ポリシー マップからコントロール プレーン クラス マップを削除するには、このコマンドの **no** 形式を使用します。

class {*class-map-name* [**insert-before** *class-map-name2*] | **class-default**}

no class *class-map-name*

シンタックスの説明

class-map-name	クラス マップの名前
insert-before *class-map-name2*	（任意）コントロール プレーン ポリシー マップの別のコントロール プレーン クラス マップの前にコントロール プレーン クラス マップを挿入します。
class-default	デフォルト クラスを指定します。

デフォルト

なし

コマンド モード

ポリシー マップ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、デフォルト Virtual Device Context（VDC; バーチャル デバイス コンテキスト）でのみ使用できます。

このコマンドにライセンスは必要ありません。

例

次に、コントロール プレーン ポリシー マップのクラス マップを設定する例を示します。

```
switch# config t
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# class ClassMapA
swtich(config-pmap-c)
```

次に、コントロール プレーン ポリシー マップからクラス マップを削除する例を示します。

```
switch# config t
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# no class ClassMapA
```

関連コマンド

コマンド	説明
policy-map type control-plane	コントロール プレーン ポリシー マップを指定して、ポリシー マップ コンフィギュレーション モードを開始します。
show policy-map type control-plane	コントロール プレーン ポリシー マップの設定情報を表示します。

class-map type control-plane

コントロール プレーン クラス マップを作成または指定して、クラス マップ コンフィギュレーション モードを開始するには、**class-map type control-plane** コマンドを使用します。コントロール プレーン クラス マップを削除するには、このコマンドの **no** 形式を使用します。

class-map type control-plane [**match-all** | **match-any**] *class-map-name*

no class-map type control-plane [**match-all** | **match-any**] *class-map-name*

シンタックスの説明

match-all	（任意）クラス マップのすべての一致条件と一致するように指定します。
match-any	（任意）クラス マップの任意の一致条件と一致するように指定します。
class-map-name	クラス マップの名前。名前には英数字を使用します。大文字と小文字が区別され、最大 64 文字まで可能です。

デフォルト

match-any

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

コントロール プレーン クラス マップの名前として、match-all、match-any、または class-default は使用できません。

このコマンドは、デフォルト VDC でのみ使用できます。

このコマンドにライセンスは必要ありません。

例

次に、コントロール プレーン クラス マップを指定して、クラス マップ コンフィギュレーション モードを開始する例を示します。

```
switch# config t
switch(config)# class-map type control-plane ClassMapA
switch(config-cmap)#
```

次に、コントロール プレーン クラス マップを削除する例を示します。

```
switch# config t
switch(config)# no class-map type control-plane ClassMapA
```

関連コマンド

コマンド	説明
show class-map type control-plane	コントロール プレーン ポリシー マップの設定情報を表示します。

clear access-list counters

すべてまたは 1 つの IPv4 Access Control List（ACL; アクセス コントロール リスト）および MAC ACL のカウンタをクリアするには、**clear access-list counters** コマンドを使用します。

clear access-list counters [*access-list-name*]

シンタックスの説明

access-list-name	（任意）デバイスがそのカウンタをクリアする ACL の名前。最大で 64 文字の英数字を使用でき、大文字と小文字が区別されます。

デフォルト

なし

コマンド モード

特権 EXEC

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドにライセンスは必要ありません。

例

次に、すべての IPv4 ACL および MAC ACL のカウンタをクリアする例を示します。

```
switch# clear access-list counters
switch#
```

次に、acl-ipv4-01 という名前の IPv4 ACL のカウンタをクリアする例を示します。

```
switch# clear access-list counters acl-ipv4-01
switch#
```

関連コマンド

コマンド	説明
clear ip access-list counters	IPv4 ACL のカウンタをクリアします。
clear mac access-list counters	MAC ACL のカウンタをクリアします。
show access-lists	1 つまたはすべての IPv4 ACL および MAC ACL に関する情報を表示します。

clear accounting log

アカウンティング ログをクリアするには、**clear accounting log** コマンドを使用します。

clear accounting log

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト なし

コマンド モード 任意のコマンド モード

サポートされるユーザ ロール network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン このコマンドは、デフォルト VDC（VDC 1）でのみ機能します。

このコマンドにライセンスは必要ありません。

例 次に、アカウンティング ログをクリアする例を示します。

```
switch# clear accounting log
```

関連コマンド

コマンド	説明
show accounting log	アカウンティング ログの内容を表示します。

clear copp statistics

コントロール プレーン ポリシング（CoPP）統計情報をクリアするには、**clear copp statistics** コマンドを使用します。

clear copp statistics

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト なし

コマンド モード 任意のコンフィギュレーション モード

サポートされるユーザ ロール network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン このコマンドは、デフォルト VDC でのみ使用できます。

このコマンドにライセンスは必要ありません。

例 次に、コントロール プレーン クラス マップを指定して、クラス マップ コンフィギュレーション モードを開始する例を示します。

```
switch# clear copp statistics
```

関連コマンド

コマンド	説明
show policy-map interface control-plane	インターフェイスの CoPP 統計情報を表示します。

clear dot1x

802.1X オーセンティケータ インスタンスをクリアするには、**clear dot1x** コマンドを使用します。

clear dot1x {**all** | **interface ethernet** *slot*/*port*}

シンタックスの説明

all	すべての 802.1X オーセンティケータ インスタンスを指定します。
interface ethernet *slot*/*port*	指定のインターフェイスの 802.1X オーセンティケータ インスタンスを指定します。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

例

次に、すべての 802.1X オーセンティケータ インスタンスをクリアする例を示します。

```
switch# clear dot1x all
```

次に、インターフェイスの 802.1X オーセンティケータ インスタンスをクリアする例を示します。

```
switch# clear dot1x interface ethernet 1/1
```

関連コマンド

コマンド	説明
feature dot1x	802.1X 機能をイネーブルにします。
show dot1x all	すべての 802.1X 情報を表示します。

clear eou

Extensible Authentication Protocol over User Datagram Protocol（EAPoUDP）セッションをクリアするには、**clear eou** コマンドを使用します。

clear eou {**all** | **authentication** {**clientless** | **eap** | **static**} | **interface ethernet** *slot/port* | **ip-address** *ipv4-address* | **mac-address** *mac-address* | **posturetoken** *type*}

シンタックスの説明

all	すべての EAPoUDP セッションを指定します。
authentication	EAPoUDP 認証を指定します。
clientless	クライアントレス ポスチャ検証を使用して認証するセッションを指定します。
eap	EAPoUDP を使用して認証するセッションを指定します。
static	静的に設定された例外リストを使用して認証するセッションを指定します。
interface ethernet *slot/port*	インターフェイスを指定します。
ip-address *ipv4-address*	IPv4 アドレスを A.B.C.D 形式で指定します。
mac-address *mac-address*	MAC アドレスを指定します。
posturetoken *type*	ポスチャ トークン名を指定します。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

feature eou コマンドを使用して EAPoUDP をイネーブルにしてから、**clear eou** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

例

次に、すべての EAPoUDP セッションをクリアする例を示します。

```
switch# clear eou all
```

次に、静的に認証された EAPoUDP セッションをクリアする例を示します。

```
switch# clear eou authentication static
```

次に、インターフェイスの EAPoUDP セッションをクリアする例を示します。

```
switch# clear eou interface ethernet 1/1
```

次に、IP アドレスの EAPoUDP セッションをクリアする例を示します。

```
switch# clear eou ip-address 10.10.1.1
```

次に、MAC アドレスの EAPoUDP セッションをクリアする例を示します。

```
switch# clear eou mac-address 0019.076c.dac4
```

次に、ポスチャ トークンのタイプが Checkup である EAPoUDP セッションをクリアする例を示します。

```
switch# clear eou posturetoken healthy
```

関連コマンド

コマンド	説明
feature eou	EAPoUDP をイネーブルにします。
show eou	EAPoUDP 情報を表示します。

clear hardware rate-limiter

レート制限統計情報をクリアするには、**clear hardware rate-limiter** コマンドを使用します。

clear rate-limiter {**access-list-log** | **all** | **copy** | **layer-2 storm-control** | **layer-3** {**control** | **glean** | **mtu** | **multicast** {**directly-connected** | **local-groups** | **rpf-leak**} | **ttl**} | **receive**}

シンタックスの説明

access-list-log	アクセス リスト ロギング パケットのレート制限統計情報をクリアします。
all	すべてのレート制限統計情報をクリアします。
copy	コピーパケットのレート制限統計情報をクリアします。
layer-2 storm-control	レイヤ 2 ストーム制御パケットのレート制限統計情報をクリアします。
layer-3	レイヤ 3 パケットのレート制限を指定します。
control	レイヤ 3 制御パケットのレート制限統計情報をクリアします。
glean	レイヤ 3 グリーニング パケットのレート制限統計情報をクリアします。
mtu	レイヤ 3 最大伝送ユニット（maximum transmission unit; MTU）パケットのレート制限統計情報をクリアします。
multicast	レイヤ 3 マルチキャストのレート制限を指定します。
directly-connected	レイヤ 3 マルチキャスト直接接続パケットのレート制限統計情報をクリアします。
local-groups	レイヤ 3 マルチキャスト ローカル グループ パケットのレート制限統計情報をクリアします。
rpf-leak	レイヤ 3 マルチキャスト RPF リーク パケットのレート制限統計情報をクリアします。
ttl	レイヤ 3 Time-to-Live（TTL; 存続可能時間）パケットのレート制限統計情報をクリアします。
receive	受信パケットのレート制限統計情報をクリアします。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、デフォルト VDC でのみ使用できます。

このコマンドにライセンスは必要ありません。

例

次に、すべてのレート制限統計情報をクリアする例を示します。

```
switch# clear hardware rate-limiter all
```

次に、アクセス リスト ロギング パケットのレート制限統計情報をクリアする例を示します。

```
switch# clear hardware rate-limiter access-list-log
```

次に、レイヤ 2 ストーム制御パケットのレート制限統計情報をクリアする例を示します。

```
switch# clear hardware rate-limiter layer-2 storm-control
```

次に、レイヤ 3 グリーニング パケットのレート制限統計情報をクリアする例を示します。

```
switch# clear hardware rate-limiter layer-3 glean
```

次に、レイヤ 3 マルチキャスト直接接続パケットのレート制限統計情報をクリアする例を示します。

```
switch# clear hardware rate-limiter layer-3 multicast directly-connected
```

次に、受信パケットのレート制限統計情報をクリアする例を示します。

```
switch# clear hardware rate-limiter receive
```

関連コマンド

コマンド	説明
platform rate-limit	レート制限を設定します。
show hardware rate-limit	レート制限情報を表示します。

clear ip access-list counters

すべてまたは 1 つの IPv4 ACL のカウンタをクリアするには、**clear ip access-list counters** コマンドを使用します。

clear ip access-list counters [*access-list-name*]

シンタックスの説明

access-list-name	（任意）デバイスがそのカウンタをクリアする IPv4 ACL の名前。最大で 64 文字の英数字を使用でき、大文字と小文字が区別されます。

デフォルト

なし

コマンド モード

特権 EXEC

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドにライセンスは必要ありません。

例

次に、すべての IPv4 ACL のカウンタをクリアする例を示します。

```
switch# clear ip access-list counters
switch#
```

次に、acl-ipv4-101 という名前の IP ACL のカウンタをクリアする例を示します。

```
switch# clear ip access-list counters acl-ipv4-101
switch#
```

関連コマンド

コマンド	説明
clear access-list counters	IPv4 ACL および MAC ACL のカウンタをクリアします。
clear mac access-list counters	MAC ACL のカウンタをクリアします。
show access-lists	1 つまたはすべての IPv4 ACL および MAC ACL に関する情報を表示します。
show ip access-lists	1 つまたはすべての IPv4 ACL に関する情報を表示します。

clear ip arp inspection log

Dynamic Address Resolution Protocol（ARP; アドレス解決プロトコル）Inspection（DAI; ダイナミック ARP 検査）ログ バッファをクリアするには、**clear ip arp inspection log** コマンドを使用します。

clear ip arp inspection log

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドにライセンスは必要ありません。

例

次に、DAI ログ バッファをクリアする例を示します。

```
switch# clear ip arp inspection log
switch#
```

関連コマンド

コマンド	説明
ip arp inspection log-buffer	DAI ログ バッファ サイズを設定します。
show ip arp inspection	DAI 設定ステータスを表示します。
show ip arp inspection log	DAI ログ設定を表示します。
show ip arp inspection statistics	DAI 統計情報を表示します。

clear ip arp inspection statistics vlan

指定の VLAN の DAI 統計情報をクリアするには、**clear ip arp inspection statistics vlan** コマンドを使用します。

clear ip arp inspection statistics vlan *vlan-list*

シンタックスの説明

vlan *vlan-list*	このコマンドによってその DAI 統計情報がクリアされる VLAN を指定します。*vlan-list* 引数では、単一の VLAN ID、VLAN ID の範囲、またはカンマで区切った ID と範囲を指定できます（「Examples」セクションを参照）。有効な VLAN ID は、1 ～ 4094 です。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドにライセンスは必要ありません。

例

次に、VLAN 2 の DAI 統計情報をクリアする例を示します。

```
switch# clear ip arp inspection statistics vlan 2
switch#
```

次に、VLAN 5 ～ 12 の DAI 統計情報をクリアする例を示します。

```
switch# clear ip arp inspection statistics vlan 5-12
switch#
```

次に、VLAN 2 および VLAN 5 ～ 12 の DAI 統計情報をクリアする例を示します。

```
switch# clear ip arp inspection statistics vlan 2,5-12
switch#
```

関連コマンド

コマンド	説明
clear ip arp inspection log	DAI ログ バッファをクリアします。
ip arp inspection log-buffer	DAI ログ バッファ サイズを設定します。
show ip arp inspection	DAI 設定ステータスを表示します。
show ip arp inspection vlan	指定リストの VLAN の DAI ステータスを表示します。

clear ip device tracking

IP デバイス トラッキング情報をクリアするには、**clear ip device tracking** コマンドを使用します。

clear ip device tracking {**all** | **interface ethernet** *slot/port* | **ip-address** *ipv4-address* | **mac-address** *mac-address*}

シンタックスの説明

all	すべての IP デバイス トラッキング情報をクリアします。
interface ethernet *slot/port*	インターフェイスの IP デバイス トラッキング情報をクリアします。
ip-address *ipv4-address*	A.B.C.D 形式の IPv4 アドレスの IP デバイス トラッキング情報をクリアします。
mac-address *mac-address*	XXXX.XXXX.XXXX 形式の MAC アドレスの IP トラッキング情報をクリアします。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin
VDC ユーザ

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドにライセンスは必要ありません。

例

次に、すべての IP デバイス トラッキング情報をクリアする例を示します。

```
switch# clear ip device tracking all
```

次に、インターフェイスの IP デバイス トラッキング情報をクリアする例を示します。

```
switch# clear ip device tracking interface ethernet 1/1
```

次に、IP アドレスの IP デバイス トラッキング情報をクリアする例を示します。

```
switch# clear ip device tracking ip-address 10.10.1.1
```

次に、MAC アドレスの IP デバイス トラッキング情報をクリアする例を示します。

```
switch# clear ip device tracking mac-address 000c.30da.86f4
```

関連コマンド

コマンド	説明
ip device tracking	IP デバイス トラッキングをイネーブルにします。
show ip device tracking	IP デバイス トラッキング情報を表示します。

clear ip dhcp snooping binding

DHCP スヌーピング バインディング データベースをクリアするには、**clear ip dhcp snooping binding** コマンドを使用します。

clear ip dhcp snooping binding

clear ip dhcp snooping binding [**vlan** *vlan-id* **mac** *mac-address* **ip** *ip-address* **interface ethernet** *slot*/*port*[**.***subinterface-number*]]

clear ip dhcp snooping binding [**vlan** *vlan-id* **mac** *mac-address* **ip** *ip-address* **interface port-channel** *channel-number*[**.***subchannel-number*]]

シンタックスの説明

***vlan** vlan-id*	（任意）*vlan-id* 引数およびその後に続く追加のキーワードと引数によって指定された VLAN ID で識別されるエントリの DHCP スヌーピング バインディング データベースをクリアします。
mac-address *mac-address*	クリアするバインディング データベース エントリの MAC アドレスを指定します。ドット付き 16 進表記で *mac-address* 引数を入力します。
ip *ip-address*	クリアするバインディング データベース エントリの IPv4 アドレスを指定します。ドット付き 10 進表記で *ip-address* 引数を入力します。
***interface ethernet** slot/port*	（任意）クリアするバインディング データベース エントリのイーサネット インターフェイスを指定します。
.subinterface-number	（任意）イーサネット インターフェイスのサブインターフェイスの番号 **（注）** *port* 引数と *subinterface-number* 引数間には、ドット区切り文字が必要です。
***interface port-channel** channel-number*	（任意）クリアするバインディング データベース エントリのイーサネット ポートチャネルを指定します。
.subchannel-number	（任意）イーサネット ポートチャネルのサブチャネルの番号 **（注）** *channel-number* 引数と *subchannel-number* 引数間には、ドット区切り文字が必要です。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin
VDC ユーザ

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。
4.0(3)	このコマンドは、特定のバインディング データベース エントリのクリアをサポートするように変更されました。オプションの **vlan** キーワードおよびそれに続く引数とキーワードが追加されました。

使用上のガイドライン

このコマンドにライセンスは必要ありません。

例

次に、DHCP スヌーピング バインディング データベースをクリアする例を示します。

```
switch# clear ip dhcp snooping binding
switch#
```

次に、DHCP スヌーピング バインディング データベースの特定のエントリをクリアする例を示します。

```
switch# clear ip dhcp snooping binding vlan 23 mac 0060.3aeb.54f0 ip 10.34.54.9
interface ethernet 2/11
switch#
```

関連コマンド

コマンド	説明
ip dhcp snooping	デバイスで DHCP スヌーピングをグローバルにイネーブルにします。
show ip dhcp snooping	DHCP スヌーピングに関する一般情報を表示します。
show ip dhcp snooping binding	スタティック IP ソース エントリを含む、IP-MAC アドレス バインディングを表示します。
show ip dhcp snooping statistics	DHCP スヌーピング統計情報を表示します。
show running-config dhcp	IP ソース ガード設定を含む、DHCP スヌーピング設定を表示します。

clear mac access-list counters

すべてまたは 1 つの MAC ACL のカウンタをクリアするには、**clear mac access-list counters** コマンドを使用します。

clear mac access-list counters [*access-list-name*]

シンタックスの説明

access-list-name	（任意）デバイスがそのカウンタをクリアする MAC ACL の名前。最大で 64 文字の英数字を使用でき、大文字と小文字が区別されます。

デフォルト

なし

コマンド モード

特権 EXEC

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドにライセンスは必要ありません。

例

次に、すべての MAC ACL のカウンタをクリアする例を示します。

```
switch# clear mac access-list counters
switch#
```

次に、acl-mac-0060 という名前の MAC ACL のカウンタをクリアする例を示します。

```
switch# clear mac access-list counters acl-ipv4-0060
switch#
```

関連コマンド

コマンド	説明
clear access-list counters	IPv4 ACL および MAC ACL のカウンタをクリアします。
clear ip access-list counters	IPv4 ACL のカウンタをクリアします。
show access-lists	1 つまたはすべての IPv4 ACL および MAC ACL に関する情報を表示します。
show mac access-lists	1 つまたはすべての MAC ACL に関する情報を表示します。

clear port-security

動的に学習された単一のセキュア MAC アドレス、または特定のインターフェイスの動的に学習されたすべてのセキュア MAC アドレスをクリアするには、**clear port-security** を使用します。

clear port-security {**dynamic**} {**interface ethernet** *slot*/*port* | **address** *address*} [**vlan** *vlan-id*]

シンタックスの説明

dynamic	動的に学習されたセキュア MAC アドレスをクリアするように指定します。
interface ethernet *slot*/*port*	クリアする対象の動的に学習されたセキュア MAC アドレスのインターフェイスを指定します。
address *address*	クリアする単一の MAC アドレスを指定します。*address* は MAC アドレスです。
vlan *vlan-id*	クリアするセキュア MAC アドレスの VLAN を指定します。有効な VLAN ID は、1 ～ 4096 です。

デフォルト

dynamic

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

feature port-security コマンドを使用してポート セキュリティをイネーブルにしてから、**clear port-security** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

例

次に、動的に学習されたセキュア MAC アドレスをイーサネット 2/1 インターフェイスから削除する例を示します。

```
switch# config t
switch(config)# clear port-security dynamic interface ethernet 2/1
```

次に、動的に学習されたセキュア MAC アドレス 0019.D2D0.00AE を削除する例を示します。

```
switch# config t
switch(config)# clear port-security dynamic address 0019.D2D0.00AE
```

関連コマンド

コマンド	説明
debug port-security	ポート セキュリティのデバッグ情報を指定します。
feature port-security	ポート セキュリティをグローバルにイネーブルにします。
show port-security	ポート セキュリティに関する情報を表示します。
switchport port-security	レイヤ 2 インターフェイスのポート セキュリティをイネーブルにします。

clear ssh hosts

VDC の Secure Shell（SSH; セキュア シェル）ホスト セッションをクリアするには、**clear ssh hosts** コマンドを使用します。

clear ssh hosts

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト なし

コマンド モード 任意のコマンド モード

サポートされるユーザ ロール network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン このコマンドにライセンスは必要ありません。

例 次に、すべての SSH ホスト セッションをクリアする例を示します。

```
switch# clear ssh hosts
```

関連コマンド

コマンド	説明
ssh server enable	SSH サーバをイネーブルにします。

clear user

VDC のユーザ セッションをクリアするには、**clear user** コマンドを使用します。

clear user *user-id*

シンタックスの説明

user-id	ユーザ ID

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバイスで現在のユーザ セッションを表示するには、**show users** コマンドを使用します。

このコマンドにライセンスは必要ありません。

例

次に、すべての SSH ホスト セッションをクリアする例を示します。

```
switch# clear user user1
```

関連コマンド

コマンド	説明
show users	ユーザ セッション情報を表示します。

cts device-id

Cisco TrustSec デバイス ID を設定するには、**cts device-id** コマンドを使用します。

cts device-id *device-id* **password** [**7**] *password*

シンタックスの説明

device-id	Cisco TrustSec デバイス ID 名。名前には英数字を使用します。大文字と小文字が区別され、最大 32 文字まで可能です。
7	（任意）パスワードを暗号化します。
password *password*	EAP-FAST 処理の間に使用するパスワードを指定します。名前には英数字を使用します。大文字と小文字が区別され、最大 32 文字まで可能です。

デフォルト

Cisco TrustSec デバイス ID はなし
クリア テキスト パスワード

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

Cisco TrustSec デバイス ID 名は、Cisco TrustSec ネットワーク クラウド内で一意でなければなりません。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、Cisco TrustSec デバイス ID を設定する例を示します。

```
switch# config t
swtich(config)# cts device-id DeviceA password Cisco321
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts credentials	Cisco TrustSec クレデンシャル情報を表示します。

cts dot1x

インターフェイスで Cisco TrustSec 認証をイネーブルにして、Cisco TrustSec 802.1X コンフィギュレーション モードを開始するには、**cts dot1x** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

cts dot1x

no cts dot1x

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドを使用した後で、**shutdown**/**no shutdown** コマンド シーケンスを使用して、インターフェイスをイネーブルおよびディセーブルにして、設定を有効にする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、インターフェイスで Cisco TrustSec 認証をイネーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

次に、インターフェイスで Cisco TrustSec 認証をディセーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# no cts dot1x
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts interface	インターフェイスの Cisco TrustSec 設定情報を表示します。

cts manual

インターフェイスの Cisco TrustSec 手動設定を開始するには、**cts manual** コマンドを使用します。手動設定を削除するには、このコマンドの **no** 形式を使用します。

cts manual

no cts manual

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドを使用した後で、**shutdown**/**no shutdown** コマンド シーケンスを使用して、インターフェイスをイネーブルおよびディセーブルにして、設定を有効にする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、インターフェイスの Cisco TrustSec 手動設定モードを開始する例を示します。

```
switch# config t
switch(config)# interface etherent 2/4
switch(config-if)# cts manual
switch(config-if-cts-manual)#
```

次に、インターフェイスから Cisco TrustSec 手動設定を削除する例を示します。

```
switch# config t
switch(config)# interface etherent 2/4
switch(config-if)# no cts manual
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts interface	インターフェイスの Cisco TrustSec 設定情報を表示します。

cts refresh role-based-policy

Cisco Secure ACS からダウンロードした Cisco TrustSec Security Group ACL（SGACL; セキュリティ グループ ACL）ポリシーをリフレッシュするには、**cts refresh role-based-policy** コマンドを使用します。

cts refresh role-based-policy

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

任意のコンフィギュレーション モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、インターフェイスの Cisco TrustSec 手動設定モードを開始する例を示します。

```
switch# cts refresh role-based-policy
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts role-based policy	Cisco TrustSec SGACL ポリシー設定を表示します。

cts rekey

Cisco TrustSec ポリシーのインターフェイス キーを再生成するには、**cts rekey** コマンドを使用します

cts rekey ethernet *slot/port*

シンタックスの説明

ethernet *slot/port*	イーサネット インターフェイスを指定します。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、Cisco TrustSec のインターフェイス キーを再生成する例を示します。

```
switch# cts rekey ethernet 2/3
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts interface	インターフェイスの Cisco TrustSec 設定情報を表示します。

cts role-based access-list

Cisco TrustSec SGACL を作成また指定して、ロールベース ACL コンフィギュレーション モードを開始するには、**cts role-based access-list** コマンドを使用します。SGACL を削除するには、このコマンドの **no** 形式を使用します。

cts role-based access-list *list-name*

no cts role-based access-list *list-name*

シンタックスの説明

list-name	SGACL の名前。名前には英数字を使用します。大文字と小文字が区別され、最大 32 文字まで可能です。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、Cisco TrustSec SGACL を作成して、ロールベース アクセス リスト コンフィギュレーション モードを開始する例を示します。

```
switch# config t
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)#
```

次に、Cisco TrustSec SGACL を削除する例を示します。

```
switch# config t
switch(config)# no cts role-based access-list MySGACL
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts role-based access-list	Cisco TrustSec SGACL 設定を表示します。

cts role-based enforcement

VLAN または Virtual Routing and Forwarding Instance（VRF; 仮想ルーティング / 転送インスタンス）で Cisco TrustSec SGACL 強制をイネーブルにするには、**cts role-based enforcement** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

cts role-based enforcement

no cts role-based enforcement

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション
VLAN コンフィギュレーション
VRF コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、デフォルト VRF で Cisco TrustSec SGACL 強制をイネーブルにする例を示します。

```
switch# config t
switch(config)# cts role-based enforcement
```

次に、VLAN で Cisco TrustSec SGACL 強制をイネーブルにする例を示します。

```
switch# config t
switch(config)# vlan 1
switch(config-vlan)# cts role-based enforcement
```

次に、非デフォルト VRF で Cisco TrustSec SGACL 強制をイネーブルにする例を示します。

```
switch# config t
switch(config)# vrf context MyVRF
switch(config-vrf)# cts role-based enforcement
```

次に、Cisco TrustSec SGACL 強制をディセーブルにする例を示します。

```
switch# config t
switch(config)# no cts role-based enforcement
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts role-based enable	Cisco TrustSec SGACL ポリシー強制の設定を表示します。

cts role-based sgt

SGACL と Cisco TrustSec Security Group Tag（SGT; セキュリティ グループ タグ）のマッピングを手動で設定するには、**cts role-based sgt** コマンドを使用します。SGACL と SGT のマッピングを削除するには、このコマンドの **no** 形式を使用します。

cts role-based sgt {*sgt-value* | **any** | **unknown**} **dgt** {*dgt-value* | **unknown**}
access-list *list-name*

no cts role-based sgt {*sgt-value* | **any** | **unknown**} **dgt** {*dgt-value* | **unknown**}

シンタックスの説明

sgt-value	送信元 SGT の値。有効範囲は 0 ～ 65533 です。
any	任意の SGT を指定します。
unknown	未知の SGT を指定します。
dgt	宛先 SGT を指定します。
dgt-value	宛先 SGT の値。有効範囲は 0 ～ 65533 です。
access-list *list-name*	SGACL の名前を指定します。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

SGT のマッピングを設定する前に SGACL を設定する必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、SGACL の SGT マッピングを設定する例を示します。

```
switch# config t
switch(config)# cts role-based sgt 3 dgt 10 access-list MySGACL
```

次に、SGACL の SGT マッピングを削除する例を示します。

```
switch# config t
switch(config)# no cts role-based sgt 3 sgt 10
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts role-based policy	SGACL の Cisco TrustSec SGT マッピングを表示します。

cts role-based sgt-map

IP アドレスと Cisco TrustSec SGT のマッピングを手動で設定するには、**cts role-based sgt-map** コマンドを使用します。SGT を削除するには、このコマンドの **no** 形式を使用します。

cts role-based sgt-map *ipv4-address sgt-value*

no cts role-based sgt-map *ipv4-address*

シンタックスの説明

ipv4-address	IPv4 アドレス。形式は、*A.B.C.D* です。
sgt-value	SGT 値。有効範囲は 0 ～ 65533 です。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション
VLAN コンフィギュレーション
VRF コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

Cisco TrustSec では、IPv4 アドレッシングだけを使用できます。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、Cisco TrustSec SGT のマッピングを設定する例を示します。

```
switch# config t
switch(config)# cts role-based sgt-map 10.10.1.1 3
switch(config-rbacl)#
```

次に、Cisco TrustSec SGT のマッピングを削除する例を示します。

```
switch# config t
switch(config)# no ccts role-based sgt-map 10.10.1.1
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts role-based sgt-map	Cisco TrustSec SGT のマッピングを表示します。

cts sgt

Cisco TrustSec SGT を設定するには、**cts sgt** コマンドを使用します。

cts sgt *tag*

シンタックスの説明

tag	**0x***hhhh* 形式の 16 進値であるデバイスのローカル SGT。有効範囲は 0x0 ～ 0xffff です。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、デバイスの Cisco TrustSec SGT を設定する例を示します。

```
switch# config t
switch(config)# cts sgt 0x3
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts environment-data	Cisco TrustSec 環境データを表示します。

cts sxp connection peer

Cisco TrustSec の SGT Exchange Protocol（SXP）ピア接続を設定するには、**cts sxp connection peer** コマンドを使用します。SXP 接続を削除するには、このコマンドの **no** 形式を使用します。

cts sxp connection peer *peer-ipv4-addr* [**source** *src-ipv4-addr*] **password** [**default** | **none** | **required** *password*] **mode** {**speaker** | **listener**} [**vrf** *vrf-name*]

no cts sxp connection peer *peer-ipv4-addr* [**vrf** *vrf-name*]

シンタックスの説明

peer-ipv4-addr	ピア デバイスの IPv4 アドレス。
source *src-ipv4-addr*	（任意）送信元デバイスの IPv4 アドレスを指定します。
password	SXP 認証に使用するパスワード オプションを指定します。
default	（任意）SXP がデバイスのデフォルト SXP パスワードを使用するように指定します。
none	（任意）SXP がパスワードを使用しないように指定します。
required *password*	（任意）SXP がこのパスワードを使用するように指定します。
mode	ピア デバイスのモードを指定します。
speaker	ピアがスピーカとなるように指定します。
listener	ピアがリスナーとなるように指定します。
vrf *vrf-name*	（任意）ピアの VRF を指定します。

デフォルト

デバイスの設定済みデフォルト SXP パスワード
デバイスの設定済みデフォルト SXP 送信元 IPv4 アドレス
デフォルト VRF

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

Cisco TrustSec では、IPv4 アドレッシングだけを使用できます。

送信元 IPv4 アドレスを指定しない場合は、**cts sxp default source-ip** コマンドを使用してデフォルト SXP 送信元 IPv4 アドレスを設定する必要があります。

デフォルトをパスワード モードで指定する場合は、**cts sxp default password** コマンドを使用してデフォルト SXP パスワードを設定する必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、SXP ピア接続を設定する例を示します。

```
switch# config t
switch(config)# cts sxp connection peer 10.10.1.1 source 10.10.2.2 password default
mode listener
```

次に、SXP ピア接続を削除する例を示します。

```
switch# config t
switch(config)# no cts sxp connection peer 10.10.1.1
```

関連コマンド

コマンド	説明
cts sxp default password	デバイスのデフォルト SXP パスワードを設定します。
cts sxp default source-ip	デバイスのデフォルト SXP 送信元 IPv4 アドレスを設定します。
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts sxp connection	Cisco TrustSec SXP ピア接続情報を表示します。

cts sxp default password

デバイスのデフォルト SGT SXP パスワードを設定するには、**cts sxp default password** コマンドを使用します。デフォルトを削除するには、このコマンドの **no** 形式を使用します。

cts sxp default password *password*

no cts sxp default password

シンタックスの説明

password	デフォルト SXP パスワード。パスワードには英数字を使用します。大文字と小文字が区別され、最大 32 文字まで可能です。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、デバイスのデフォルト SXP パスワードを設定する例を示します。

```
switch# config t
switch(config)# cts sxp default password Cisco654
```

次に、デフォルト SXP パスワードを削除する例を示します。

```
switch# config t
switch(config)# no cts sxp default password
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts sxp	Cisco TrustSec SXP 設定情報を表示します。

cts sxp default source-ip

デバイスのデフォルト SGT SXP 送信元 IPv4 アドレスを設定するには、**cts sxp default source-ip** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

cts sxp default source-ip *ipv4-address*

no cts sxp default source-ip *ipv4-address*

シンタックスの説明

ipv4-address	デバイスのデフォルト SXP IPv4 アドレス

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

Cisco TrustSec では、IPv4 アドレッシングだけを使用できます。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、デバイスのデフォルト SXP 送信元 IP アドレスを設定する例を示します。

```
switch# config t
switch(config)# cts sxp default source-ip 10.10.3.3
```

次に、デフォルト SXP 送信元 IP アドレスを削除する例を示します。

```
switch# config t
switch(config)# no cts sxp default source-ip
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts sxp	Cisco TrustSec SXP 設定情報を表示します。

cts sxp enable

デバイス上の SGT SXP ピアをイネーブルにするには、**cts sxp enable** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

cts sxp enable

no cts sxp enable

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、SXP をイネーブルにする例を示します。

```
switch# config t
switch(config)# cts sxp enable
```

次に、SXP をディセーブルにする例を示します。

```
switch# config t
switch(config)# no cts sxp enable
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts sxp	Cisco TrustSec SXP 設定情報を表示します。

cts sxp reconcile-period

SGT SXP 復帰期間タイマーを設定するには、**cts sxp reconcile-period** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

cts sxp reconcile-period *seconds*

no cts sxp reconcile-period

シンタックスの説明

seconds	秒数。有効範囲は 0 ～ 64000 秒です。

デフォルト

60 秒（1 分）

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

ピアが SXP 接続を終了すると、内部ホールドダウン タイマーが開始されます。内部ホールドダウン タイマーが終了する前にピアが再接続すると、SXP 復帰期間タイマーが開始されます。SXP 復帰期間タイマーがアクティブな間、NX-OS ソフトウェアは前回の接続で学習した SGT マッピング エントリを保持し、無効なエントリを削除します。

（注） SXP 復帰期間を 0 秒に設定すると、タイマーがディセーブルになり、前回の接続のすべてのエントリが削除されます。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、SXP 復帰期間を設定する例を示します。

```
switch# config t
switch(config)# cts sxp reconcile-period 120
```

次に、SXP 復帰期間をデフォルト値に戻す例を示します。

```
switch# config t
switch(config)# no cts sxp reconcile-period
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts sxp connection	Cisco TrustSec SXP 設定情報を表示します。

cts sxp retry-period

SGT SXP リトライ期間タイマーを設定するには、**cts sxp retry-period** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

cts sxp retry-period *seconds*

no cts sxp retry-period

シンタックスの説明

seconds	秒数。有効範囲は 0 ～ 64000 秒です。

デフォルト

120 秒（2 分）

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

SXP リトライ期間によって、NX-OS ソフトウェアが SXP 接続を再試行する頻度が決まります。SXP 接続が正常に確立されなかった場合、NX-OS ソフトウェアは SXP リトライ期間タイマーの終了後に、新たな接続の確立を試行します。

（注） SXP リトライ期間を 0 秒に設定すると、タイマーがディセーブルになり、再試行は実行されません。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、SXP リトライ期間を設定する例を示します。

```
switch# config t
switch(config)# cts sxp retry-period 120
```

次に、SXP リトライ期間をデフォルト値に戻す例を示します。

```
switch# config t
switch(config)# no cts sxp retry-period
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts sxp connection	Cisco TrustSec SXP ピア接続情報を表示します。

D コマンド

この章では、D で始まる Cisco NX-OS Security コマンドについて説明します。

deadtime

RADIUS または TACACS+ サーバ グループのデッド タイム間隔を設定するには、**deadtime** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

deadtime *minutes*

no deadtime *minutes*

シンタックスの説明

minutes	間隔の分数。有効範囲は 0 ～ 1440 分です。

（注） デッド タイム間隔をゼロ（0）に設定すると、タイマーがディセーブルになります。

デフォルト

0 分

コマンド モード

RADIUS サーバ グループ コンフィギュレーション
TACACS+ サーバ グループ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

TACACS+ を設定する前に **feature tacacs+** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

例

次に、RADIUS サーバ グループのデッド タイム間隔を 2 分に設定する例を示します。

```
switch# config t
switch(config)# aaa group server radius RadServer
switch(config-radius)# deadtime 2
```

次に、TACACS+ サーバ グループのデッド タイム間隔を 5 分に設定する例を示します。

```
switch# config t
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# deadtime 5
```

次に、デッド タイム間隔をデフォルト値に戻す例を示します。

```
switch# config t
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# no deadtime 5
```

関連コマンド

コマンド	説明
aaa group server	AAA サーバ グループを設定します。
radius-server host	RADIUS サーバを設定します。
show radius-server groups	RADIUS サーバ グループ情報を表示します。
show tacacs-server groups	TACACS+ サーバ グループ情報を表示します。
feature tacacs+	TACACS+ をイネーブルにします。
tacacs-server host	TACACS+ サーバを設定します。

deny（ARP）

条件に一致する ARP トラフィックを拒否する ARP ACL ルールを作成するには、**deny** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

一般的な構文

[*sequence-number*] **deny ip** {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} **mac** {**any** | **host** *sender-MAC* | *sender-MAC sender-MAC-mask*} [**log**]

[*sequence-number*] **deny request ip** {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} **mac** {**any** | **host** *sender-MAC* | *sender-MAC sender-MAC-mask*} [**log**]

[*sequence-number*] **deny response ip** {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} {**any** | **host** *target-IP* | *target-IP target-IP-mask*} **mac** {**any** | **host** *sender-MAC* | *sender-MAC sender-MAC-mask*} [**any** | **host** *target-MAC* | *target-MAC target-MAC-mask*] [**log**]

no *sequence-number*

no deny ip {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} **mac** {**any** | **host** *sender-MAC* | *sender-MAC sender-MAC-mask*} [**log**]

no deny request ip {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} **mac** {**any** | **host** *sender-MAC* | *sender-MAC sender-MAC-mask*} [**log**]

no deny response ip {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} {**any** | **host** *target-IP* | *target-IP target-IP-mask*} **mac** {**any** | **host** *sender-MAC* | *sender-MAC sender-MAC-mask*} [**any** | **host** *target-MAC* | *target-MAC target-MAC-mask*] [**log**]

シンタックスの説明

sequence-number	（任意）**deny** コマンドのシーケンス番号。この番号により、アクセス リスト内の番号が振られた場所にデバイスがコマンドを挿入します。ACL 内のルールの順序は、シーケンス番号によって維持されます。 シーケンス番号には、1 から 4294967295 までの任意の整数を使用できます。 ACL 内の最初のルールは、デフォルトでシーケンス番号 10 を持ちます。 シーケンス番号を指定しない場合は、デバイスによってそのルールが ACL の最後に追加され、そのルールの直前のルールのシーケンス番号よりも 10 大きい番号が割り当てられます。 ルールにシーケンス番号を再割り当てするには、**resequence** コマンドを使用します。
ip	ルールの IP アドレス部分を示します。
any	（任意）任意のホストがルールの ***any*** キーワードが含まれる部分に一致するように指定します。***any*** を使用して、送信元 IP アドレス、宛先 IP アドレス、送信元 MAC アドレス、および宛先 MAC アドレスを指定できます。
host *sender-IP*	（任意）ARP パケットの送信元 IP アドレスが *sender-IP* 引数の値に一致する場合にのみ、ルールが ARP パケットに一致するように指定します。*sender-IP* 引数の有効値は、ドット付き 10 進表記の IPv4 アドレスです。
sender-IP *sender-IP-mask*	（任意）パケットの送信元 IP アドレスが一致する可能性のある IPv4 アドレスおよび IPv4 アドレス セットのマスク。*sender-IP* 引数と *sender-IP-mask* 引数は、ドット付き 10 進表記で指定する必要があります。*sender-IP-mask* 引数に 255.255.255.255 を指定することと、***host*** キーワードを使用することは同じです。
mac	ルールの MAC アドレス部分を示します。

host *sender-MAC*	（任意）ARP パケットの送信元 MAC アドレスが *sender-MAC* 引数の値に一致する場合にのみ、ルールが ARP パケットに一致するように指定します。*sender-MAC* 引数の有効値は、ドット付き 16 進表記の MAC アドレスです。
sender-MAC *sender-MAC-mask*	（任意）パケットの送信元 MAC アドレスが一致する可能性のある MAC アドレスおよび MAC アドレス セットのマスク。*sender-MAC* 引数と *sender-MAC-mask* 引数は、ドット付き 16 進表記で指定する必要があります。*sender-MAC-mask* 引数に ffff.ffff.ffff を指定することと、***host*** キーワードを使用することは同じです。
log	（任意）ルールに一致する ARP パケットをデバイスが記録するように指定します。
request	（任意）ARP 要求メッセージが含まれるパケットのみにルールが適用されるように指定します。 **（注）** ***request*** キーワードと ***response*** キーワードの両方を省略すると、すべての ARP メッセージにルールが適用されます。
response	（任意）ARP 応答メッセージが含まれるパケットのみにルールが適用されるように指定します。 **（注）** ***request*** キーワードと ***response*** キーワードの両方を省略すると、すべての ARP メッセージにルールが適用されます。
host *target-IP*	（任意）ARP パケットの宛先 IP アドレスが *target-IP* 引数の値に一致する場合にのみ、ルールが ARP パケットに一致するように指定します。***response*** キーワードを使用する場合にのみ、***host*** *target-IP* を指定できます。*target-IP* 引数の有効値は、ドット付き 10 進表記の IPv4 アドレスです。
target-IP *target-IP-mask*	（任意）パケットの宛先 IP アドレスが一致する可能性のある IPv4 アドレスおよび IPv4 アドレス セットのマスク。***response*** キーワードを使用する場合にのみ、*target-IP target-IP-mask* を指定できます。*target-IP* 引数と *target-IP-mask* 引数は、ドット付き 10 進表記で指定する必要があります。*target-IP-mask* 引数に 255.255.255.255 を指定することと、***host*** キーワードを使用することは同じです。
host *target-MAC*	（任意）ARP パケットの宛先 MAC アドレスが *target-MAC* 引数の値に一致する場合にのみ、ルールが ARP パケットに一致するように指定します。***response*** キーワードを使用する場合にのみ、***host*** *target-MAC* を指定できます。*target-MAC* 引数の有効値は、ドット付き 16 進表記の MAC アドレスです。
target-MAC *target-MAC-mask*	（任意）パケットの宛先 MAC アドレスが一致する可能性のある MAC アドレスおよび MAC アドレス セットのマスク。***response*** キーワードを使用する場合にのみ、*target-MAC target-MAC-mask* を指定できます。*target-MAC* 引数と *target-MAC-mask* 引数は、ドット付き 16 進表記で指定する必要があります。*target-MAC-mask* 引数に ffff.ffff.ffff を指定することと、***host*** キーワードを使用することは同じです。

デフォルト なし

コマンド モード ARP ACL コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

新規に作成された ARP ACL にはルールが含まれません。

シーケンス番号を指定しない場合は、デバイスによって ACL の最後のルールのシーケンス番号よりも 10 大きい番号がルールに割り当てられます

デバイスは、パケットに ARP ACL を適用する時点で、ACL 内のすべてのルールを使用してパケットを評価します。デバイスは、パケットに一致する条件を持つ最初のルールを実行します。複数のルールの条件が一致した場合、デバイスは最も低いシーケンス番号のルールを実行します。

response キーワードまたは ***request*** キーワードのいずれかを指定しない場合は、ARP メッセージが含まれるパケットにルールが適用されます。

このコマンドにライセンスは必要ありません。

例

次に、arp-acl-01 という名前の ARP ACL の ARP アクセス リスト コンフィギュレーション モードを開始して、10.32.143.0 サブネットに存在する送信元 IP アドレスが含まれる ARP 要求メッセージを拒否するルールを追加する例を示します。

```
switch# conf t
switch(config)# arp access-list arp-acl-01
switch(config-arp-acl)# deny request ip 10.32.143.0 255.255.255.0 mac any
```

関連コマンド

コマンド	説明
arp access-list	ARP ACL を設定します。
ip arp inspection filter	ARP ACL を VLAN に適用します。
permit（ARP）	ARP ACL の許可ルールを設定します。
remark	ACL でリマークを設定します。
show arp access-list	すべてまたは 1 つの ARP ACL を表示します。

deny（IPv4）

条件に一致するトラフィックを拒否する IPv4 ACL ルールを作成するには、**deny** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

一般的な構文

[*sequence-number*] **deny** *protocol source destination* [**dscp** *dscp* | **precedence** *precedence*] [**fragments**] [**log**] [**time-range** *time-range-name*]

no deny *protocol source destination* [**dscp** *dscp* | **precedence** *precedence*] [**fragments**] [**log**] [**time-range** *time-range-name*]

no *sequence-number*

Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）

[*sequence-number*] **deny icmp** *source destination* [*icmp-message*] [**dscp** *dscp* | **precedence** *precedence*] [**fragments**] [**log**] [**time-range** *time-range-name*]

Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）

[*sequence-number*] **deny igmp** *source destination* [*igmp-message*] [**dscp** *dscp* | **precedence** *precedence*] [**fragments**] [**log**] [**time-range** *time-range-name*]

IP バージョン 4（IPv4）

[*sequence-number*] **deny ip** *source destination* [**dscp** *dscp* | **precedence** *precedence*] [**fragments**] [**log**] [**time-range** *time-range-name*]

Transmission Control Protocol（TCP）

[*sequence-number*] **deny tcp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp* | **precedence** *precedence*] [**fragments**] [**log**] [**time-range** *time-range-name*] [*flags*] [**established**]

User Datagram Protocol（UDP; ユーザ データグラム プロトコル）

[*sequence-number*] **deny udp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp* | **precedence** *precedence*] [**fragments**] [**log**] [**time-range** *time-range-name*]

シンタックスの説明

sequence-number	（任意）**deny** コマンドのシーケンス番号。この番号により、アクセス リスト内の番号が振られた場所にデバイスがコマンドを挿入します。ACL 内のルールの順序は、シーケンス番号によって維持されます。 シーケンス番号には、1 から 4294967295 までの任意の整数を使用できます。 ACL 内の最初のルールは、デフォルトでシーケンス番号 10 を持ちます。 シーケンス番号を指定しない場合は、デバイスによってそのルールが ACL の最後に追加され、そのルールの直前のルールのシーケンス番号よりも 10 大きい番号が割り当てられます。 ルールにシーケンス番号を再割り当てするには、**resequence** コマンドを使用します。
protocol	ルールが一致するパケットのプロトコルの名前または番号。有効な番号は、0 ～ 255 です。有効なプロトコル名は、次のキーワードのとおりです。 • ***icmp*** ― ルールが ICMP トラフィックのみに適用されるように指定します。このキーワードを使用した場合は、*protocol* 引数のすべての有効値に使用できるキーワードに加え、*icmp-message* 引数が使用可能です。 • ***igmp*** ― ルールが IGMP トラフィックのみに適用されるように指定します。このキーワードを使用した場合は、***protocol*** 引数のすべての有効値に使用できるキーワードに加え、***igmp-type*** 引数が使用可能です。 • ***ip*** ― ルールがすべての IPv4 トラフィックに適用されるように指定します。このキーワードを使用した場合は、すべての IPv4 プロトコルに適用されるその他のキーワードおよび引数のみが使用可能です。キーワードは次のとおりです。 ― ***dscp*** ― ***fragments*** ― ***log*** ― ***precedence*** ― ***time-range*** • ***tcp*** ― ルールが TCP トラフィックのみに適用されるように指定します。このキーワードを使用した場合は、***protocol*** 引数のすべての有効値に使用できるキーワードに加え、***flags*** 引数と ***operator*** 引数、および ***portgroup*** キーワードと ***established*** キーワードが使用可能です。 • ***udp*** ― ルールが UDP トラフィックのみに適用されるように指定します。このキーワードを使用した場合は、***protocol*** 引数のすべての有効値に使用できるキーワードに加え、***operator*** 引数および ***portgroup*** キーワードが使用可能です。
source	ルールが一致する送信元 IPv4 アドレス。この引数を指定する方法の詳細については、「使用上のガイドライン」セクションの「送信元および宛先」を参照してください。
destination	ルールが一致する宛先 IPv4 アドレス。この引数を指定する方法の詳細については、「使用上のガイドライン」セクションの「送信元および宛先」を参照してください。

***dscp** dscp*	（任意）パケットの IP ヘッダーの DSCP フィールドの値が指定した 6 ビットの Differentiated Service（DiffServ; ディファレンシエーテッド サービス）値である場合にのみ、ルールがパケットに一致するように指定します。*dscp* 引数には、次の数値またはキーワードの 1 つを指定できます。 • 0 ～ 63 ― DSCP フィールドの 6 ビットと等価の 10 進数。たとえば 10 を指定した場合、ルールは DSCP フィールドのビットが 001010 であるパケットのみに一致します。 • ***af11*** ― Assured Forwarding（AF; 保証型転送）クラス 1、「低」の廃棄確率（001010） • ***af12*** ― AF クラス 1、「中」のドロップ率（001100） • ***af13*** ― AF クラス 1、「高」のドロップ率（001110） • ***af21*** ― AF クラス 2、「低」のドロップ率（010010） • ***af22*** ― AF クラス 2、「中」のドロップ率（010100） • ***af23*** ― AF クラス 2、「高」のドロップ率（010110） • ***af31*** ― AF クラス 3、「低」のドロップ率（011010） • ***af32*** ― AF クラス 3、「中」のドロップ率（011100） • ***af33*** ― AF クラス 3、「高」のドロップ率（011110） • ***af41*** ― AF クラス 4、「低」のドロップ率（100010） • ***af42*** ― AF クラス 4、「中」のドロップ率（100100） • ***af43*** ― AF クラス 4、「高」のドロップ率（100110） • ***cs1*** ― Class Selector（CS; クラスセレクタ）1、優先度 1（001000） • ***cs2*** ― CS2、優先度 2（010000） • ***cs3*** ― CS3、優先度 3（011000） • ***cs4*** ― CS4、優先度 4（100000） • ***cs5*** ― CS5、優先度 5（101000） • ***cs6*** ― CS6、優先度 6（110000） • ***cs7*** ― CS7、優先度 7（111000） • ***default*** ― デフォルト DSCP 値（000000） • ***ef*** ― Expedited Forwarding（EF; 緊急転送）（101110）
***precedence** precedence*	（任意）パケットの IP precedence フィールドの値が *precedence* 引数で指定された値である場合にのみ、ルールがパケットに一致するように指定します。*precedence* 引数には、次の番号またはキーワードを指定できます。 • 0 ～ 7 ― IP precedence フィールドの 3 ビットと等価の 10 進数。たとえば 3 を指定した場合、ルールは DSCP フィールドのビットが 011 であるパケットのみに一致します。 • ***critical*** ― 優先度 5（101） • ***flash*** ― 優先度 3（011） • ***flash-override*** ― 優先度 4（100） • ***immediate*** ― 優先度 2（010） • ***internet*** ― 優先度 6（110） • ***network*** ― 優先度 7（111） • ***priority*** ― 優先度 1（001） • ***routine*** ― 優先度 0（000）

fragments	（任意）非初期フラグメントであるパケットにのみルールが一致するように指定します。デバイスがレイヤ 4 オプションを評価するために必要な情報は初期フラグメントのみに含まれているため、このキーワードは、TCP ポート番号などのレイヤ 4 オプションを指定するのと同じルールで指定することはできません。
log	（任意）ルールに一致する各パケットについての情報ログ メッセージをデバイスが生成するように指定します。メッセージには、次の情報が含まれます。 • ACL 名 • パケットが許可されたか拒否されたか • プロトコルが TCP、UDP、ICMP、または番号のいずれであったか • 送信元および宛先アドレス。送信元および宛先ポート番号（該当する場合）
time-range *time-range-name*	（任意）このルールに適用される時間範囲を指定します。**time-range** コマンドを使用して時間範囲を設定できます。*time-range-name* 引数には、最大で 64 文字の英数字を使用でき、大文字と小文字が区別されます。
icmp-message	（ICMP のみ：任意）ルールが一致する ICMP メッセージ タイプ。この引数には、0 ～ 255 の整数、または「使用上のガイドライン」セクションの「ICMP メッセージ タイプ」に記載されているキーワードの 1 つを指定できます。
igmp-message	（IGMP のみ：任意）ルールが一致する IGMP メッセージ タイプ。*igmp-message* 引数には、IGMP メッセージ番号（0 ～ 15 の整数）、または次のキーワードのいずれか 1 つを指定できます。 • ***dvmrp*** ― Distance Vector Multicast Routing Protocol（DVMRP; ディスタンス ベクトル マルチキャスト ルーティング プロトコル） • ***host-query*** ― ホスト クエリー • ***host-report*** ― ホスト レポート • ***pim*** ― PIM • ***trace*** ― マルチキャスト トレース
operator port [*port*]	（任意：TCP および UDP のみ）*operator* 引数および *port* 引数の条件に一致する送信元ポートまたは宛先ポートとの間で送受信されるパケットにのみルールが一致します。これらの引数が送信元ポートまたは宛先ポートのいずれに適用されるかは、*source* または *destination* のどちらの引数の後ろに指定したかにより決まります。 *port* 引数には、TCP または UDP ポートの名前または番号を指定できます。有効な番号は、0 ～ 65535 です。有効なポート名のリストについては、「使用上のガイドライン」セクションの「TCP ポート名」および「UDP ポート名」を参照してください。 2 番めの *port* 引数は、*operator* 引数が範囲の場合にのみ必要になります。 *operator* 引数には、次のキーワードのいずれか 1 つを指定する必要があります。 • ***eq*** ― パケットのポートが *port* 引数の値と同じ場合にのみ一致します。 • ***gt*** ― パケットのポートが *port* 引数の値より大きい場合にのみ一致します。 • ***lt*** ― パケットのポートが *port* 引数の値より小さい場合にのみ一致します。 • ***neq*** ― パケットのポートが *port* 引数の値と同じでない場合にのみ一致します。 • ***range*** ― 2 つの *port* 引数が必要です。パケットのポートが最初の *port* 引数の値以上で、2 番めの *port* 引数の値以下である場合にのみ一致します。

portgroup *portgroup*	（任意：TCP および UDP のみ）*portgroup* 引数によって指定される IP ポート オブジェクト グループのメンバーである送信元ポートまたは宛先ポートとの間でパケットが送受信される場合にのみ、ルールがパケットに一致するように指定します。portgroup 引数には、64 文字の英数字を使用でき、大文字と小文字が区別されます。IP ポート オブジェクト グループが送信元ポートまたは宛先ポートのいずれに適用されるかは、*source* または *destination* のどちらの引数の後ろに指定したかにより決まります。 IP ポート オブジェクト グループを作成または変更するには、**object-group ip port** コマンドを使用します。
flags	（TCP のみ：任意）ルールが一致する TCP 制御ビット フラグ。*flags* 引数の値には、次のキーワードの 1 つ以上を指定する必要があります。 • ***ack*** • ***fin*** • ***psh*** • ***rst*** • ***syn*** • ***urg***
established	（TCP のみ：任意）確立された TCP 接続に属するパケットのみにルールが一致するように指定します。デバイスは、ACK または RST ビットを持つ TCP パケットは、確立された接続に属するものとみなします。

デフォルト

新規に作成された IPv4 ACL にはルールが含まれません。

シーケンス番号を指定しない場合は、デバイスによって ACL の最後のルールのシーケンス番号よりも 10 大きい番号がルールに割り当てられます。

コマンド モード

IPv4 ACL コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバイスは、パケットに IPv4 ACL を適用する時点で、ACL 内のすべてのルールを使用してパケットを評価します。デバイスは、パケットに一致する条件を持つ最初のルールを実行します。複数のルールの条件が一致した場合、デバイスは最も低いシーケンス番号のルールを実行します。

このコマンドにライセンスは必要ありません。

送信元および宛先

source 引数および *destination* 引数は、複数の方法のいずれか 1 つによって指定できます。各ルールでは、これらの引数の 1 つを指定する際に使用した方法が、他の引数の指定方法に影響を与えることはありません。ルールを設定する場合には、次の方法を使って *source* 引数および *destination* 引数を指定します。

- IP アドレス グループ オブジェクト ― IPv4 アドレス グループ オブジェクトを使用して、*source* 引数または *destination* 引数を指定できます。IPv4 アドレス グループ オブジェクトを作成または変更するには、**object-group ip address** コマンドを使用します。構文は、次のとおりです。

  addrgroup *address-group-name*

  次に、lab-gateway-svrs という名前の IPv4 アドレス グループ オブジェクトを使用して *destination* 引数を指定する例を示します。

  ```
  switch(config-acl)# deny ip any addrgroup lab-gateway-svrs
  ```

- アドレスおよびネットワーク ワイルドカード ― IPv4 アドレスおよびその後ろに続けてネットワーク ワイルドカードを使用することで、ホストまたはネットワークを送信元または宛先として指定できます。構文は、次のとおりです。

  IPv4-address network-wildcard

  次に、192.168.67.0 サブネットの IPv4 アドレスおよびネットワーク ワイルドカードを使用して *source* 引数を指定する例を示します。

  ```
  switch(config-acl)# deny tcp 192.168.67.0 0.0.0.255 any
  ```

- アドレスおよび Variable-Length Subnet Mask（VLSM; 可変長サブネット マスク）― IPv4 アドレスおよびその後ろに続けて VLSM を使用することで、ホストまたはネットワークを送信元または宛先として指定できます。構文は、次のとおりです。

  IPv4-address/prefix-len

  次に、192.168.67.0 サブネットの IPv4 アドレスおよび VLSM を使用して *source* 引数を指定する例を示します。

  ```
  switch(config-acl)# deny udp 192.168.67.0/24 any
  ```

- ホスト アドレス ― ***host*** キーワードおよび IPv4 アドレスを使用して、ホストを送信元または宛先として指定できます。構文は、次のとおりです。

  host *IPv4-address*

  この構文は、*IPv4-address*/32 および *IPv4-address* 0.0.0.0 と等価です。

  次に、***host*** キーワードおよび 192.168.67.132 IPv4 アドレスを使用して、*source* 引数を指定する例を示します。

  ```
  switch(config-acl)# deny icmp host 192.168.67.132 any
  ```

- 任意のアドレス ― ***any*** キーワードを使用して、送信元または宛先が任意の IPv4 アドレスとなるように指定できます。***any*** キーワードを使用した例については、このセクションの例を参照してください。それぞれの例には、***any*** キーワードを使用して送信元または宛先を指定する方法が示されています。

ICMP メッセージ タイプ

icmp-message 引数には、ICMP メッセージ番号（0 ～ 255 の整数）、または次のキーワードのいずれか 1 つを指定できます。

- ***administratively-prohibited*** ― 管理上の禁止
- ***alternate-address*** ― 代替アドレス
- ***conversion-error*** ― データグラム変換
- ***dod-host-prohibited*** ― ホストの拒否
- ***dod-net-prohibited*** ― ネットワークの拒否
- ***echo*** ― エコー（PING）
- ***echo-reply*** ― エコー応答
- ***general-parameter-problem*** ― パラメータの問題

- ***host-isolated*** ― 分離されているホスト
- ***host-precedence-unreachable*** ― 優先度が Host Unreachable
- ***host-redirect*** ― ホストへのリダイレクト
- ***host-tos-redirect*** ― ToS ベースでのホストへのリダイレクト
- ***host-tos-unreachable*** ― ToS ベースでホストに到達不能
- ***host-unknown*** ― 未知のホスト
- ***host-unreachable*** ― ホストに到達不能
- ***information-reply*** ― 応答についての情報
- ***information-request*** ― 要求についての情報
- ***mask-reply*** ― マスクの応答
- ***mask-request*** ― マスクの要求
- ***mobile-redirect*** ― モバイル ホストへのリダイレクト
- ***net-redirect*** ― ネットワークへのリダイレクト
- ***net-tos-redirect*** ― ToS ベースでのネットワークへのリダイレクト
- ***net-tos-unreachable*** ― ToS ベースでネットワークに到達不能
- ***net-unreachable*** ― ネットワークに到達不能
- ***network-unknown*** ― 未知のネットワーク
- ***no-room-for-option*** ― パラメータが必須であるが指定する余地がない
- ***option-missing*** ― パラメータが必須であるが存在しない
- ***packet-too-big*** ― フラグメンテーションが必要だが DF が設定されている
- ***parameter-problem*** ― すべてのパラメータの問題
- ***port-unreachable*** ― ポートに到達不能
- ***precedence-unreachable*** ― 優先順位が使用できない
- ***protocol-unreachable*** ― プロトコルに到達不能
- ***reassembly-timeout*** ― 再構成時のタイムアウト
- ***redirect*** ― すべてリダイレクト
- ***router-advertisement*** ― ルータ ディスカバリのためのアドバタイズメント
- ***router-solicitation*** ― ルータ ディスカバリのためのソリシテーション
- ***source-quench*** ― ソース クエンチ
- ***source-route-failed*** ― 送信元ルートの障害
- ***time-exceeded*** ― すべての時間超過メッセージ
- ***timestamp-reply*** ― タイム スタンプ付きの応答
- ***timestamp-request*** ― タイム スタンプ付きの要求
- ***traceroute*** ― トレースルート
- ***ttl-exceeded*** ― Time-To-Live（TTL; 存続可能時間）を超過
- ***unreachable*** ― すべて到達不能

TCP ポート名

protocol 引数に ***tcp*** を指定した場合は、*port* 引数に TCP ポート番号（0 ～ 65535 の整数）または次のキーワードのいずれか 1 つを指定できます。

bgp ― Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）（179）

chargen ― Character Generator（19）

cmd ― リモートコマンド（rcmd、514）

daytime ― 日付と時刻（13）

discard ― 廃棄（9）

domain ― ドメイン ネーム サービス（53）

drip ― ダイナミック RIP（3949）

echo ― エコー（7）

exec ― EXEC（rsh、512）

finger ― Finger（79）

ftp ― Fingerile Transfer Protocol（FTP; ファイル転送プロトコル）（21）

ftp-data ― FTP データ接続（2）

gopher ― Gopher（7）

hostname ― NIC ホストネーム サーバ（11）

ident ― Ident プロトコル（113）

irc ― Internet Relay Chat（IRC; インターネット リレー チャット）（194）

klogin ― Kerberos ログイン（543）

kshell ― Kerberos シェル（544）

login ― ログイン（rlogin、513）

lpd ― プリンタ サービス（515）

nntp ― Network News Transport Protocol（NNTP）（119）

pim-auto-rp ― PIM Auto-RP（496）

pop2 ― POP v2（19）

pop3 ― POP v3（11）

smtp ― Simple Mail Transport Protocol（SMTP）（25）

sunrpc ― Sun Remote Procedure Call（SunRPC）（111）

tacacs ― TAC Access Control System（TACACS）（49）

talk ― Talk（517）

telnet ― Telnet（23）

time ― Time（37）

uucp ― UNIX-to-UNIX Copy Program（54）

whois ― WHOIS/NICNAME（43）

www ― World Wide Web（HTTP、8）

UDP ポート名

protocol 引数に ***udp*** を指定した場合は、*port* 引数に UDP ポート番号（0 ～ 65535 の整数）または次のキーワードのいずれか 1 つを指定できます。

biff ― biff（メール通知、comsat、512）

bootpc ― Bootstrap Protocol（BOOTP; ブートストラップ プロトコル）クライアント（68）

bootps ― BOOTP サーバ（67）

discard ― 廃棄（9）

dnsix ― DNSIX セキュリティ プロトコル監査（195）

domain ― ドメイン ネーム サービス（DNS、53）

echo ― エコー（7）

isakmp ― Internet Security Association and Key Management Protocol（ISAKMP）（5）

mobile-ip ― Mobile IP 登録（434）

nameserver ― IEN116 ネームサービス（廃止、42）

netbios-dgm ― NetBIOS データグラム サービス（138）

netbios-ns ― NetBIOS ネーム サービス（137）

netbios-ss ― NetBIOS セッション サービス（139）

non500-isakmp ― Internet Security Association and Key Management Protocol（ISAKMP）（45）

ntp ― Network Time Protocol（NTP; ネットワーク タイム プロトコル）（123）

pim-auto-rp ― PIM Auto-RP（496）

rip ― RIP（ルータ、in.routed、52）

snmp ― Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）（161）

snmptrap ― SNMP トラップ（162）

sunrpc ― Sun Remote Procedure Call（SunRPC）（111）

syslog ― システム ロガー（514）

tacacs ― TAC Access Control System（TACACS）（49）

talk ― Talk（517）

tftp ― TFTP（69）

time ― Time（37）

who ― who サービス（rwho、513）

xdmcp ― X DMCP（177）

例

次に、10.23.0.0 ～ 10.176.0.0 および 192.168.37.0 ～ 10.176.0.0 ネットワークのすべての TCP と UDP のトラフィックを拒否するルール、およびその他のすべての IPv4 トラフィックを許可する最後のルールを持つ、acl-lab-01 という名前の IPv4 ACL を設定する例を示します。

```
switch# config t
switch(config)# ip access-list acl-lab-01
switch(config-acl)# deny tcp 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# deny udp 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# deny tcp 192.168.37.0/16 10.176.0.0/16
switch(config-acl)# deny udp 192.168.37.0/16 10.176.0.0/16
switch(config-acl)# permit ip any any
```

次に、eng_workstations という名前の IPv4 アドレス オブジェクト グループから marketing_group という名前の IP アドレス オブジェクト グループまでのすべての IP トラフィックを拒否するルールの後に、その他のすべての IPv4 トラフィックを許可するルールが続く、acl-eng-to-marketing という名前の IPv4 ACL を設定する例を示します。

```
switch# config t
switch(config)# ip access-list acl-eng-to-marketing
switch(config-acl)# deny ip addrgroup eng_workstations addrgroup marketing_group
switch(config-acl)# permit ip any any
```

関連コマンド

コマンド	説明
ip access-list	IPv4 ACL を設定します。
object-group ip address	IPv4 アドレス オブジェクト グループを設定します。
object-group ip port	IP ポート オブジェクト グループを設定します。
permit（IPv4）	IPv4 ACL の許可ルールを設定します。
remark	IPv4 ACL でリマークを設定します。
show ip access-list	すべての IPv4 ACL または 1 つの IPv4 ACL を表示します。
statistics per-entry	ACL の各エントリの統計情報の収集をイネーブルにします。
time-range	時間範囲を設定します。

deny（MAC）

条件に一致するトラフィックを拒否する MAC Access Control List（ACL; アクセス コントロール リスト）+ ルールを作成するには、**deny** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

[*sequence-number*] **deny** *source destination* [*protocol*] [**cos** *cos-value*] [**vlan** *VLAN-ID*]

no deny *source destination* [*protocol*] [**cos** *cos-value*] [**vlan** *VLAN-ID*]

no *sequence-number*

シンタックスの説明

sequence-number	（任意）**deny** コマンドのシーケンス番号。この番号により、アクセス リスト内の番号が振られた場所にデバイスがコマンドを挿入します。ACL 内のルールの順序は、シーケンス番号によって維持されます。 シーケンス番号には、1 から 4294967295 までの任意の整数を使用できます。 ACL 内の最初のルールは、デフォルトでシーケンス番号 10 を持ちます。 シーケンス番号を指定しない場合は、デバイスによってそのルールが ACL の最後に追加され、そのルールの直前のルールのシーケンス番号よりも 10 大きい番号が割り当てられます。 ルールにシーケンス番号を再割り当てするには、**resequence** コマンドを使用します。
source	ルールが一致する送信元 MAC アドレス。この引数を指定する方法の詳細については、「使用上のガイドライン」セクションの「送信元および宛先」を参照してください。
destination	ルールが一致する宛先 MAC アドレス。この引数を指定する方法の詳細については、「使用上のガイドライン」セクションの「送信元および宛先」を参照してください。
protocol	（任意）ルールが一致するプロトコル番号。有効なプロトコル番号は、0x0 ～ 0xffff です。有効なプロトコル名のリストについては、「使用上のガイドライン」セクションの「MAC プロトコル」を参照してください。
***cos** cos-value*	（任意）*cos-value* 引数に指定された Class of Service（CoS; サービス クラス）値がパケットの IEEE 802.1Q ヘッダーに含まれる場合にのみ、ルールがパケットに一致するように指定します。*cos-value* 引数には、0 ～ 7 の整数を指定できます。
***vlan** VLAN-ID*	（任意）指定された VLAN ID がパケットの IEEE 802.1Q ヘッダーに含まれる場合にのみ、ルールがパケットに一致するように指定します。*VLAN-ID* 引数には、1 ～ 4094 の整数を指定できます。

デフォルト

新規に作成された MAC ACL にはルールが含まれません。

シーケンス番号を指定しない場合は、デバイスによって ACL の最後のルールのシーケンス番号よりも 10 大きい番号がルールに割り当てられます。

コマンド モード

MAC ACL コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバイスは、パケットに MAC ACL を適用する時点で、ACL 内のすべてのルールを使用してパケットを評価します。デバイスは、パケットに一致する条件を持つ最初のルールを実行します。複数のルールの条件が一致した場合、デバイスは最も低いシーケンス番号のルールを実行します。

このコマンドにライセンスは必要ありません。

送信元および宛先

source 引数および *destination* 引数は、2 つの方法のうちのいずれかによって指定できます。各ルールでは、これらの引数の 1 つを指定する際に使用した方法が、他の引数の指定方法に影響を与えることはありません。ルールを設定する場合には、次の方法を使って *source* 引数および *destination* 引数を指定します。

- アドレスおよびマスク — MAC アドレスおよびその後ろにマスクを続けて使用して、1 つのアドレスまたはアドレス グループを指定できます。構文は、次のとおりです。

  MAC-address MAC-mask

  次に、MAC アドレス 00c0.4f03.0a72 で *source* 引数を指定する例を示します。

  ```
  switch(config-acl)# deny 00c0.4f03.0a72 0000.0000.0000 any
  ```

  次に、MAC ベンダー コードが 00603e のすべてのホストに対応する MAC アドレスで *destination* 引数を指定する例を示します。

  ```
  switch(config-acl)# deny any 0060.3e00.0000 0000.0000.0000
  ```

- 任意のアドレス — ***any*** キーワードを使用して、送信元または宛先が任意の MAC アドレスとなるように指定できます。***any*** キーワードを使用した例については、このセクションの例を参照してください。それぞれの例には、***any*** キーワードを使用して送信元または宛先を指定する方法が示されています。

MAC プロトコル

protocol 引数には、MAC プロトコル番号またはキーワードを指定できます。プロトコル番号は、0x というプレフィクスを持つ 4 バイトの 16 進数です。有効なプロトコル番号は、0x0 ～ 0xffff です。有効なキーワードは、次のとおりです。

- ***aarp*** — AppleTalk ARP（0x80f3）
- ***appletalk*** — AppleTalk（0x809b）
- ***decnet-iv*** — DECnet Phase IV（0x6003）
- ***diagnostic*** — DEC Diagnostic Protocol（0x6005）
- ***etype-6000*** — EtherType 0x6000（0x6000）
- ***etype-8042*** — EtherType 0x8042（0x8042）
- ***ip*** — IPv4（0x0800）
- ***lat*** — DEC LAT（0x6004）
- ***lavc-sca*** — DEC LAVC、SCA（0x6007）
- ***mop-console*** — DEC MOP Remote Console（0x6002）
- ***mop-dump*** — DEC MOP Dump（0x6001）
- ***vines-echo*** — VINES Echo（0x0baf）

例

次に、2 つの MAC アドレス グループ間で非 IPv4 トラフィックを許可するルールが含まれる mac-ip-filter という名前の MAC ACL を設定する例を示します。

```
switch# config t
switch(config)# mac access-list mac-ip-filter
switch(config-mac-acl)# deny 00c0.4f00.0000 0000.00ff.ffff 0060.3e00.0000
0000.00ff.ffff ip
switch(config-mac-acl)# permit any any
```

関連コマンド

コマンド	説明
mac access-list	MAC ACL を設定します。
permit（MAC）	MAC ACL で拒否ルールを設定します。
remark	ACL でリマークを設定します。
show mac access-list	すべてまたは 1 つの MAC ACL を表示します。
statistics per-entry	ACL の各エントリの統計情報の収集をイネーブルにします。

deny（ロールベース ACL）

SGACL（セキュリティ グループ アクセス コントロール リスト）で拒否アクションを設定するには、**deny** コマンドを使用します。アクションを削除するには、このコマンドの **no** 形式を使用します。

deny {**all** | **icmp** | **igmp** | **ip** | {{**tcp** | **udp**} [{**src** | **dest**} {{**eq** | **gt** | **lt** | **neq**} *port-number*} | **range** *port-number1 port-number2*}]}

no deny {**all** | **icmp** | **igmp** | **ip** | {{**tcp** | **udp**} [{**src** | **dest**} {{**eq** | **gt** | **lt** | **neq**} *port-number*} | **range** *port-number1 port-number2*}]}

シンタックスの説明

all	すべてのトラフィックを指定します。
icmp	ICMP トラフィックを指定します。
igmp	IGMP トラフィックを指定します。
ip	IP トラフィックを指定します。
tcp	TCP トラフィックを指定します。
udp	UDP トラフィックを指定します。
src	送信元ポート番号を指定します。
dest	宛先ポート番号を指定します。
eq	指定した値と同じポート番号を指定します。
gt	指定した値より大きいポート番号を指定します。
lt	指定した値より小さいポート番号を指定します。
neq	指定した値以外のすべてのポート番号を指定します。
port-number	TCP または UDP のポート番号。有効範囲は 0 ～ 65535 です。
range	TCP または UDP のポート範囲を指定します。
port-number1	範囲内の最初のポート。有効範囲は 0 ～ 65535 です。
port-number2	範囲内の最後のポート。有効範囲は 0 ～ 65535 です。

デフォルト

なし

コマンド モード

ロールベース ACL

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、SGACL に拒否アクションを追加する例を示します。

```
switch# config t
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)# deny icmp
```

次に、SGACL から拒否アクションを削除する例を示します。

```
switch# config t
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)# no deny icmp
```

関連コマンド

コマンド	説明
cts role-based access-list	Cisco TrustSec SGACL を設定します。
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts role-based access-list	Cisco TrustSec SGACL 設定を表示します。

description（アイデンティティ ポリシー）

アイデンティティ ポリシーの説明を設定するには、**description** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

description "*text*"

no description

シンタックスの説明

"*text*"	アイデンティティ ポリシーについて説明するテキスト ストリング。ストリングには、英数字を使用します。最大 100 文字まで可能です。

デフォルト

なし

コマンド モード

アイデンティティ ポリシー コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin
VDC ユーザ

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドにライセンスは必要ありません。

例

次に、アイデンティティ ポリシーの説明を設定する例を示します。

```
switch# config t
switch(config)# identity policy AdminPolicy
switch(config-id-policy)# description "Administrator identity policy"
```

次に、アイデンティティ ポリシーから説明を削除する例を示します。

```
switch# config t
switch(config)# identity policy AdminPolicy
switch(config-id-policy)# no description
```

関連コマンド

コマンド	説明
identity policy	アイデンティティ ポリシーを設定または指定し、アイデンティティ ポリシー コンフィギュレーション モードを開始します。
show identity policy	アイデンティティ ポリシー情報を表示します。

description（ユーザ ロール）

ユーザ ロールの説明を設定するには、**description** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

description *text*

no description

シンタックスの説明

text	ユーザ ロールについて説明するテキスト ストリング。ストリングには、英数字を使用します。最大 128 文字まで可能です。

デフォルト

なし

コマンド モード

ユーザ ロール コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

ユーザ ロールの説明テキストには、空白スペースを使用できます。

このコマンドにライセンスは必要ありません。

例

次に、ユーザ ロールの説明を設定する例を示します。

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# description User role for my user account.
```

次に、ユーザ ロールから説明を削除する例を示します。

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# no description
```

関連コマンド

コマンド	説明
role name	ユーザ ロールを作成または指定して、ユーザ ロール コンフィギュレーション モードを開始します。
show role	ユーザ ロール情報を表示します。

device

Extensible Authentication Protocol over User Datagram Protocol（EAPoUDP）アイデンティティ プロファイルの例外リストにサプリカント デバイスを追加するには、**device** コマンドを使用します。サプリカント デバ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。

device {**authenticate** | **not-authenticate**} {**ip-address** *ipv4-address* [*subnet-mask*] | **mac-address** *mac-address* [*mac-address-mask*]} **policy** *policy-name*

no device {**authenticate** | **not-authenticate**} {**ip-address** *ipv4-address* [*subnet-mask*] | **mac-address** *mac-address* [*mac-address-mask*]} **policy** *policy-name*

シンタックスの説明

authenticate	ポリシーを使用するデバイス認証を許可するように指定します。
not-authenticate	ポリシーを使用するデバイス認証を許可しないように指定します。
ip-address *ipv4-address*	サプリカント デバイスの IPv4 アドレスを A.B.C.D 形式で指定します。
subnet-mask	（任意）IPv4 アドレスの IPv4 サブネット マスク
mac-address *mac-address*	サプリカント デバイスの MAC アドレスを XXXX.XXXX.XXXX 形式で指定します。
mac-address-mask	（任意）MAC アドレスのマスク
policy *policy-name*	サプリカント デバイスに使用するポリシーを指定します。

デフォルト

なし

コマンド モード

アイデンティティ ポリシー コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin
VDC ユーザ

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドにライセンスは必要ありません。

例

次に、EAPoUDP アイデンティティ プロファイルにデバイスを追加する例を示します。

```
switch# config t
switch(config)# identity profile eapoupd
switch(config-id-policy)# device authenticate 10.10.1.1 255.255.255.245 policy
AdminPolicy
```

次に、EAPoUDP アイデンティティ プロファイルからデバイスを削除する例を示します。

```
switch# config t
switch(config)# identity profile eapoupd
switch(config-id-policy)# no device authenticate 10.10.2.2 255.255.255.245 policy
UserPolicy
```

関連コマンド

コマンド	説明
identity policy	アイデンティティ ポリシーを設定または指定し、アイデンティティ ポリシー コンフィギュレーション モードを開始します。
show identity policy	アイデンティティ ポリシー情報を表示します。

dot1x default

802.1X グローバル設定またはインターフェイス設定をデフォルトにリセットするには、**dot1x default** コマンドを使用します。

dot1x default

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション
インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

例

次に、グローバル 802.1X パラメータをデフォルトに設定する例を示します。

```
switch# config t
switch(config)# dot1x default
```

次に、インターフェイス 802.1X パラメータをデフォルトに設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x default
```

関連コマンド

コマンド	説明
feature dot1x	802.1X 機能をイネーブルにします。
show dot1x	802.1X 機能ステータス情報を表示します。

dot1x host-mode

インターフェイス上の 1 つまたは複数のサプリカントの 802.1X 認証を許可するには、**dot1x host-mode** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x host-mode {**multi-host** | **single-host**}

no dot1x host-mode

シンタックスの説明

mutli-host	インターフェイス上の複数のサプリカントの 802.1X 認証を許可します。
single-host	インターフェイス上の 1 つだけのサプリカントの 802.1X 認証を許可します。

デフォルト

single-host

コマンド モード

インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

例

次に、インターフェイス上の複数のサプリカントの 802.1X 認証を許可する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x host-mode multi-host
```

次に、インターフェイス上でデフォルトのホスト モードに戻す例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# no dot1x host-mode
```

関連コマンド

コマンド	説明
feature dot1x	802.1X 機能をイネーブルにします。
show dot1x all	すべての 802.1X 情報を表示します。

dot1x initialize

サプリカントの 802.1X 認証を初期化するには、**dot1x initialize** コマンドを使用します。

dot1x initialize [**interface ethernet** *slot/port*]

シンタックスの説明

interface ethernet *slot/port*	（任意）802.1X 認証初期化のインターフェイスを指定します。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

例

NX-OS デバイス上でサプリカントの 802.1X 認証を初期化する例を示します。

```
switch# dot1x initialize
```

次に、インターフェイス上でサプリカントの 802.1X 認証を初期化する例を示します。

```
switch# dot1x initialize interface ethernet 2/1
```

関連コマンド

コマンド	説明
feature dot1x	802.1X 機能をイネーブルにします。
show dot1x all	すべての 802.1X 情報を表示します。

dot1x mac-auth-bypass

802.1X サプリカントがないインターフェイス上で MAC アドレス認証バイパスをイネーブルにするには、**dot1x mac-auth-bypass** コマンドを使用します。MAC アドレス認証バイパスをディセーブルにするには、このコマンドの **no** 形式を使用します。

dot1x mac-auth-bypass [**eap**]

no dot1x mac-auth-bypass

シンタックスの説明

eap	バイパスで Extensible Authentication Protocol（EAP）を使用するように指定します。

デフォルト

ディセーブル

コマンド モード

インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

例

次に、MAC アドレス認証バイパスをイネーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# dot1x mac-auth-bypass
```

次に、MAC アドレス認証バイパスをディセーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# no dot1x mac-auth-bypass
```

関連コマンド

コマンド	説明
feature dot1x	802.1X 機能をイネーブルにします。
show dot1x all	すべての 802.1X 情報を表示します。

dot1x max-reauth-req

セッションがタイムアウトになるまでに NX-OS デバイスがインターフェイス上のサプリカントに再認証要求を再送信する最大回数を変更するには、**dot1x max-reauth-req** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x max-reauth-req *retry-count*

no dot1x max-reauth-req

シンタックスの説明

retry-count	再認証要求リトライ回数。有効範囲は 1 ～ 10 回です。

デフォルト

リトライ 2 回

コマンド モード

インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

例

次に、インターフェイスの最大再許可要求リトライ回数を変更する例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# dot1x max-reauth-req 3
```

次に、インターフェイスの最大再許可要求リトライ回数をデフォルトに戻す例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# no dot1x max-reauth-req
```

関連コマンド

コマンド	説明
feature dot1x	802.1X 機能をイネーブルにします。
show dot1x all	すべての 802.1X 情報を表示します。

dot1x max-req

802.1X 認証が再開するまでに NX-OS デバイスがサプリカントに送信する最大要求回数を変更するには、**dot1x max-req** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x max-req *retry-count*

no dot1x max-req

シンタックスの説明

retry-count	802.1X 再認証が再開するまでにサプリカントに送信する要求リトライ回数。有効範囲は 1 ～ 10 回です。

デフォルト

グローバル コンフィギュレーション：リトライ 2 回

インターフェイス コンフィギュレーション：グローバル コンフィギュレーション設定

コマンド モード

グローバル コンフィギュレーション
インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

例

次に、グローバル 802.1X コンフィギュレーションの最大要求リトライ回数を変更する例を示します。

```
switch# config t
switch(config)# dot1x max-req 3
```

次に、グローバル 802.1X コンフィギュレーションの最大要求リトライ回数をデフォルトに戻す例を示します。

```
switch# config t
switch(config)# no dot1x max-req
```

次に、インターフェイスの最大要求リトライ回数を変更する例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# dot1x max-req 4
```

次に、インターフェイスの最大要求リトライ回数をデフォルトに戻す例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# no dot1x max-req
```

関連コマンド

コマンド	説明
feature dot1x	802.1X 機能をイネーブルにします。
show dot1x all	すべての 802.1X 情報を表示します。

dot1x port-control

インターフェイス上で実行される 802.1X 認証を制御するには、**dot1x port-control** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x port-control {**auto** | **force-authorized** | **force-unauthorized**}

no dot1x port-control {**auto** | **force-authorized** | **force-unauthorized**}

シンタックスの説明

auto	インターフェイス上で 802.1X 認証をイネーブルにします。
force-authorized	インターフェイス上で 802.1X 認証をディセーブルにして、認証なしでインターフェイス上のすべてのトラフィックを許可します。
force-unauthorized	インターフェイス上ですべての認証をディセーブルにします。

デフォルト

force-authorized

コマンド モード

インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

例

次に、インターフェイス上で実行される 802.1X 認証処理を変更する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x port-control auto
```

次に、インターフェイス上で実行される 802.1X 認証処理の設定をデフォルトに戻す例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x port-control auto
```

関連コマンド

コマンド	説明
feature dot1x	802.1X 機能をイネーブルにします。
show dot1x interface ethernet	インターフェイスの 802.1X 情報を表示します。

dot1x radius-accounting

802.1X の RADIUS アカウンティングをイネーブルにするには、**dot1x radius-accounting** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x radius-accounting

no dot1x radius-accounting

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

例

次に、802.1X 認証の RADIUS アカウンティングをイネーブルにする例を示します。

```
switch# config t
switch(config)# dot1x radius-accounting
```

次に、802.1X 認証の RADIUS アカウンティングをディセーブルにする例を示します。

```
switch# config t
switch(config)# no dot1x radius-accounting
```

関連コマンド

コマンド	説明
feature dot1x	802.1X 機能をイネーブルにします。
show running-config dot1x all	実行コンフィギュレーションですべての 802.1X 情報を表示します。

dot1x re-authentication（EXEC）

802.1X サプリカントを手動で再認証するには、**dot1x re-authentication** コマンドを使用します。

dot1x re-authentication [**interface ethernet** *slot/port*]

シンタックスの説明

interface ethernet *slot/port*	（任意）手動再認証のインターフェイスを指定します。

デフォルト

なし

コマンド モード

EXEC モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

例

次に、802.1X サプリカントを手動で再認証する例を示します。

```
switch# dot1x re-authentication
```

次に、インターフェイス上の 802.1X サプリカントを手動で再認証する例を示します。

```
switch# dot1x re-authentication interface ethernet 2/1
```

関連コマンド

コマンド	説明
feature dot1x	802.1X 機能をイネーブルにします。
show dot1x all	すべての 802.1X 情報を表示します。

dot1x re-authentication（グローバル コンフィギュレーション、インターフェイス コンフィギュレーション）

802.1X サプリカントの定期的な再認証をイネーブルにするには、**dot1x re-authentication** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x re-authentication

no dot1x re-authentication

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

グローバル コンフィギュレーション：ディセーブル

インターフェイス コンフィギュレーション：グローバル コンフィギュレーション設定

コマンド モード

グローバル コンフィギュレーション
インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

このコマンドをグローバル コンフィギュレーション モードで使用すると、NX-OS デバイス上のすべてのサプリカントの定期的な再認証が設定されます。このコマンドをインターフェイス コンフィギュレーション モードで使用すると、インターフェイス上のサプリカントのみの定期的な再認証が設定されます。

このコマンドにライセンスは必要ありません。

例

次に、802.1X サプリカントの定期的な再認証をイネーブルにする例を示します。

```
switch# config t
switch(config)# dot1x re-authentication
```

次に、802.1X サプリカントの定期的な再認証をディセーブルにする例を示します。

```
switch# config t
switch(config)# no dot1x re-authentication
```

次に、インターフェイス上の 802.1X サプリカントの定期的な再認証をイネーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x re-authentication
```

次に、インターフェイス上の 802.1X サプリカントの定期的な再認証をディセーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# no dot1x re-authentication
```

関連コマンド

コマンド	説明
feature dot1x	802.1X 機能をイネーブルにします。
show dot1x all	すべての 802.1X 情報を表示します。

dot1x system-auth-control

802.1X 認証をイネーブルにするには、**dot1x system-auth-control** コマンドを使用します。802.1X 認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

dot1x system-auth-control

no dot1x system-auth-control

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

イネーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

dot1x system-auth-control コマンドにより 802.1X 設定は削除されません。

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

例

次に、802.1X 認証をディセーブルにする例を示します。

```
switch# config t
switch(config)# no dot1x system-auth-control
```

次に、802.1X 認証をイネーブルにする例を示します。

```
switch# config t
switch(config)# dot1x system-auth-control
```

関連コマンド

コマンド	説明
feature dot1x	802.1X 機能をイネーブルにします。
show dot1x	802.1X 機能ステータス情報を表示します。

dot1x timeout quiet-period

802.1X 待機時間タイムアウトをグローバルに、またはインターフェイス単位で設定するには、**dot1x timeout quiet-period** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x timeout quiet-period *seconds*

no dot1x timeout quiet-period

シンタックスの説明

seconds	802.1X 待機時間タイムアウトの秒数。有効範囲は 1 ～ 65535 秒です。

デフォルト

グローバル コンフィギュレーション：60 秒

インターフェイス コンフィギュレーション：グローバル コンフィギュレーションの値

コマンド モード

グローバル コンフィギュレーション
インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

802.1X 待機時間タイムアウトは、サプリカントとの認証の交換に失敗した後で、デバイスが待機状態にとどまる秒数です。

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

（注） 信頼できないリンクまたは特定のサプリカントや認証サーバに関する固有の動作の問題など、通常とは異なる状況を調整する場合に限りデフォルト値を変更します。

このコマンドにライセンスは必要ありません。

例

次に、グローバル 802.1X 待機時間タイムアウトを設定する例を示します。

```
switch# config t
switch(config)# dot1x timeout quiet-period 45
```

次に、グローバル 802.1X 待機時間タイムアウトの設定をデフォルトに戻す例を示します。

```
switch# config t
switch(config)# no dot1x timeout quiet-period
```

次に、インターフェイスの 802.1X 待機時間タイムアウトを設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# dot1x timeout quiet-period 50
```

次に、インターフェイスの 802.1X 待機時間タイムアウトの設定をデフォルトに戻す例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# no dot1x timeout quiet-period
```

関連コマンド

コマンド	説明
feature dot1x	802.1X 機能をイネーブルにします。
show dot1x all	すべての 802.1X 情報を表示します。

dot1x timeout ratelimit-period

インターフェイス上のサプリカントの 802.1X レート制限時間タイムアウトを設定するには、**dot1x timeout ratelimit-period** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x timeout ratelimit-period *seconds*

no dot1x timeout ratelimit-period

シンタックスの説明

seconds	802.1X レート制限時間タイムアウトの秒数。有効範囲は 1 ～ 65535 秒です。

デフォルト

0 秒

コマンド モード

インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

802.1X レート制限タイムアウト時間は、オーセンティケータが、正常に認証されたサプリカントの EAPOL-Start パケットを無視する秒数です。この値は、グローバル待機時間タイムアウトを上書きします。

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

（注） 信頼できないリンクまたは特定のサプリカントや認証サーバに関する固有の動作の問題など、通常とは異なる状況を調整する場合に限りデフォルト値を変更します。

このコマンドにライセンスは必要ありません。

例

次に、インターフェイスの 802.1X レート制限時間タイムアウトを設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x timeout ratelimit-period 60
```

次に、インターフェイスの 802.1X レート制限時間タイムアウトの設定をデフォルトに戻す例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x timeout ratelimit-period 60
```

関連コマンド

コマンド	説明
feature dot1x	802.1X 機能をイネーブルにします。
show dot1x interface ethernet	インターフェイスの 802.1X 情報を表示します。

dot1x timeout re-authperiod

802.1X 再認証時間タイムアウトをグローバルに、またはインターフェイス単位で設定するには、**dot1x timeout re-authperiod** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x timeout re-authperiod *seconds*

no dot1x timeout re-authperiod

シンタックスの説明

seconds	802.1X 再認証時間タイムアウトの秒数。有効範囲は 1 ～ 65535 秒です。

デフォルト

グローバル コンフィギュレーション：3600 秒

インターフェイス コンフィギュレーション：グローバル コンフィギュレーション設定

コマンド モード

グローバル コンフィギュレーション
インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

802.1X 再認証タイムアウト時間は、再認証の試行間の秒数です。

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

（注） 信頼できないリンクまたは特定のサプリカントや認証サーバに関する固有の動作の問題など、通常とは異なる状況を調整する場合に限りデフォルト値を変更します。

このコマンドにライセンスは必要ありません。

例

次に、グローバル 802.1X 再認証時間タイムアウトを設定する例を示します。

```
switch# config t
switch(config)# dot1x timeout re-authperiod 3000
```

次に、インターフェイスの 802.1X 再認証時間タイムアウトを設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# dot1x timeout re-authperiod 3300
```

関連コマンド

コマンド	説明
feature dot1x	802.1X 機能をイネーブルにします。
show dot1x all	すべての 802.1X 情報を表示します。

dot1x timeout server-timeout

インターフェイスの 802.1X サーバ タイムアウトを設定するには、**dot1x timeout server-timeout** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x timeout server-timeout *seconds*

no dot1x timeout server-timeout

シンタックスの説明

seconds	802.1X サーバ タイムアウトの秒数。有効範囲は 1 ～ 65535 秒です。

デフォルト

30 秒

コマンド モード

インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

インターフェイスの 802.1X サーバ タイムアウトは、認証サーバにパケットを再送信するまでに NX-OS デバイスが待機する秒数です。この値は、グローバル再認証時間タイムアウトを上書きします。

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

（注） 信頼できないリンクまたは特定のサプリカントや認証サーバに関する固有の動作の問題など、通常とは異なる状況を調整する場合に限りデフォルト値を変更します。

このコマンドにライセンスは必要ありません。

例

次に、グローバル 802.1X サーバ タイムアウト間隔を設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x timeout server-timeout 45
```

次に、グローバル 802.1X サーバ タイムアウト間隔の設定をデフォルトに戻す例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x timeout server-timeout 45
```

関連コマンド

コマンド	説明
feature dot1x	802.1X 機能をイネーブルにします。
show dot1x interface ethernet	インターフェイスの 802.1X 情報を表示します。

dot1x timeout supp-timeout

インターフェイスの 802.1X サプリカント タイムアウトを設定するには、**dot1x timeout supp-timeout** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x timeout supp-timeout *seconds*

no dot1x timeout supp-timeout

シンタックスの説明

seconds	802.1X サプリカント タイムアウトの秒数。有効範囲は 1 ～ 65535 秒です。

デフォルト

30 秒

コマンド モード

インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

インターフェイスの 802.1X サプリカント タイムアウトは、NX-OS デバイスがフレームを再送信するまでに、サプリカントが EAP 要求フレームに応答するのを NX-OS デバイスが待機する秒数です。

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

（注） 信頼できないリンクまたは特定のサプリカントや認証サーバに関する固有の動作の問題など、通常とは異なる状況を調整する場合に限りデフォルト値を変更します。

このコマンドにライセンスは必要ありません。

例

次に、インターフェイスの 802.1X サーバ タイムアウト間隔を設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# dot1x timeout supp-timeout 45
```

次に、インターフェイスの 802.1X サーバ タイムアウト間隔の設定をデフォルトに戻す例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# no dot1x timeout supp-timeout
```

関連コマンド

コマンド	説明
feature dot1x	802.1X 機能をイネーブルにします。
show dot1x interface ethernet	インターフェイスの 802.1X 情報を表示します。

dot1x timeout tx-period

802.1X 送信時間タイムアウトをグローバルに、またはインターフェイス単位で設定するには、**dot1x timeout tx-period** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

dot1x timeout tx-period *seconds*

no dot1x timeout tx-period

シンタックスの説明

seconds	802.1X 送信時間タイムアウトの秒数を指定します。有効範囲は 1 ～ 65535 秒です。

デフォルト

グローバル コンフィギュレーション：60 秒

インターフェイス コンフィギュレーション：グローバル コンフィギュレーション設定

コマンド モード

グローバル コンフィギュレーション
インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

802.1X 送信タイムアウト時間は、要求を再送信するまでに、NX-OS デバイスがサプリカントからの EAP 要求 / アイデンティティ フレームへの応答を待機する秒数です。

802.1X を設定する前に **feature dot1x** コマンドを使用する必要があります。

（注） 信頼できないリンクまたは特定のサプリカントや認証サーバに関する固有の動作の問題など、通常とは異なる状況を調整する場合に限りデフォルト値を変更します。

このコマンドにライセンスは必要ありません。

例

次に、グローバル 802.1X 送信時間タイムアウトを設定する例を示します。

```
switch# config t
switch(config)# dot1x timeout tx-period 45
```

次に、グローバル 802.1X 送信時間タイムアウトの設定をデフォルトに戻す例を示します。

```
switch# config t
switch(config)# no dot1x timeout tx-period
```

次に、インターフェイスの 802.1X 送信時間タイムアウトを設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# dot1x timeout tx-period 45
```

次に、インターフェイスの 802.1X 送信時間タイムアウトの設定をデフォルトに戻す例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# no dot1x timeout tx-period
```

関連コマンド

コマンド	説明
feature dot1x	802.1X 機能をイネーブルにします。
show dot1x all	すべての 802.1X 情報を表示します。

E コマンド

この章では、E で始まる Cisco NX-OS Security コマンドについて説明します。

eou allow clientless

クライアントレス エンドポイント デバイスの Extensible Authentication Protocol over User Datagram Protocol（EAPoUDP）ポスチャ検証をイネーブルにするには、**eou allow clientless** コマンドを使用します。クライアントレス エンドポイント デバイスのポスチャ検証をディセーブルにするには、コマンドの **no** 形式を使用します。

eou allow clientless

no eou allow clientless

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト ディセーブル

コマンド モード グローバル コンフィギュレーション

サポートされるユーザ ロール network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン EAPoUDP を設定する前に **feature eou** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

例

次に、クライアントレス エンドポイント デバイスの EAPoUDP ポスチャ検証を許可する例を示します。

```
switch# config t
switch(config)# eou allow clientless
```

次に、クライアントレス エンドポイント デバイスの EAPoUDP ポスチャ検証が行われないようにする例を示します。

```
switch# config t
switch(config)# no eou allow clientless
```

関連コマンド

コマンド	説明
feature eou	EAPoUDP をイネーブルにします。
show eou	EAPoUDP 情報を表示します。

eou default

EAPoUDP のグローバルまたはインターフェイスの設定値をデフォルトに戻すには、**eou default** コマンドを使用します。

eou default

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション
インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

EAPoUDP を設定する前に **feature eou** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

例

次に、グローバル EAPoUDP 設定をデフォルトに変更する例を示します。

```
switch# config t
switch(config)# eou default
```

次に、インターフェイスの EAPoUDP 設定をデフォルトに変更する例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# eou default
```

関連コマンド

コマンド	説明
feature eou	EAPoUDP をイネーブルにします。
show eou	EAPoUDP 情報を表示します。

eou initialize

EAPoUDP セッションを初期化するには、**eou initialize** コマンドを使用します。

eou initialize {**all** | **authentication** {**clientless** | **eap** | **static**} | **interface ethernet** *slot/port* | **ip-address** *ipv4-address* | **mac-address** *mac-address* | **posturetoken** *name*}

シンタックスの説明

all	すべての EAPoUDP セッションを初期化します。
authentication	特定の認証タイプの EAPoUDP セッションを初期化します。
clientless	クライアントレス ポスチャ検証を使用して認証するセッションを指定します。
eap	EAPoUDP を使用して認証するセッションを指定します。
static	静的に設定された例外リストを使用して認証するセッションを指定します。
interface ethernet *slot/port*	特定のインターフェイスの EAPoUDP セッションを初期化します。
ip-address *ipv4-address*	特定の IPv4 アドレスの EAPoUDP セッションを初期化します。
mac-address *mac-address*	特定の MAC アドレスの EAPoUDP セッションを初期化します。
posturetoken *name*	特定のポスチャ トークンの EAPoUDP セッションを初期化します。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

EAPoUDP を設定する前に **feature eou** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

例

次に、すべての EAPoUDP セッションを初期化する例を示します。

```
switch# eou initialize all
```

次に、静的に認証された EAPoUDP セッションを初期化する例を示します。

```
switch# eou initialize authentication static
```

次に、インターフェイスの EAPoUDP セッションを初期化する例を示します。

```
switch# eou initialize interface ethernet 1/1
```

次に、IP アドレスの EAPoUDP セッションを初期化する例を示します。

```
switch# eou initialize ip-address 10.10.1.1
```

次に、MAC アドレスのすべての EAPoUDP セッションを初期化する例を示します。

```
switch# eou initialize mac-address 0019.076c.dac4
```

次に、ポスチャ トークンのすべての EAPoUDP セッションを初期化する例を示します。

```
switch# eou initialize posturetoken healthy
```

関連コマンド

コマンド	説明
feature eou	EAPoUDP をイネーブルにします。
show eou	EAPoUDP 情報を表示します。

eou logging

EAPoUDP ロギングをイネーブルにするには、**eou logging** コマンドを使用します。EAPoUDP ロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

eou logging

no eou logging

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

グローバル コンフィギュレーション：ディセーブル

インターフェイス コンフィギュレーション：グローバル コンフィギュレーション設定

コマンド モード

グローバル コンフィギュレーション
インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

インターフェイス上の EAPoUDP ロギングの設定はグローバル設定を上書きします。

EAPoUDP を設定する前に **feature eou** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

例

次に、グローバル EAPoUDP ロギングをイネーブルにする例を示します。

```
switch# config t
switch(config)# eou logging
```

次に、グローバル EAPoUDP ロギングをディセーブルにする例を示します。

```
switch# config t
switch(config)# no eou logging
```

次に、インターフェイスの EAPoUDP ロギングをイネーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# eou logging
```

次に、インターフェイスの EAPoUDP ロギングをディセーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# no eou logging
```

関連コマンド

コマンド	説明
feature eou	EAPoUDP をイネーブルにします。
show eou	EAPoUDP 情報を表示します。

eou max-retry

EAPoUDP の最大試行回数をグローバルに、またはインターフェイス単位で設定するには、**eou max-retry** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

eou max-retry *count*

no eou max-retry

シンタックスの説明

count	最大リトライ試行回数。有効範囲は 1 ～ 3 回です。

デフォルト

グローバル コンフィギュレーション：3

インターフェイス コンフィギュレーション：グローバル コンフィギュレーション値

コマンド モード

グローバル コンフィギュレーション
インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

インターフェイスの最大リトライ回数は、グローバル設定値より優先されます。

EAPoUDP を設定する前に **feature eou** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

例

次に、EAPoUDP のグローバル最大リトライ試行回数を変更する例を示します。

```
switch# config t
switch(config)# eou max-retry 2
```

次に、EAPoUDP のグローバル最大リトライ試行回数の設定をデフォルトに戻す示します。

```
switch# config t
switch(config)# no eou max-retry
```

次に、インターフェイスの EAPoUDP 最大リトライ試行回数を変更する例を示します。

```
switch# config t
switch(config) interface ethernet 1/1
switch(config-if)# eou max-retry 3
```

次に、インターフェイスの EAPoUDP 最大リトライ試行回数の設定をデフォルトに戻す例を示します。

```
switch# config t
switch(config) interface ethernet 1/1
switch(config-if)# no eou max-retry
```

関連コマンド

コマンド	説明
feature eou	EAPoUDP をイネーブルにします。
show eou	EAPoUDP 情報を表示します。

eou port

EAPoUDP の User Datagram Protocol（UDP; ユーザ データグラム プロトコル）ポート番号を設定するには、**eou port** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

eou port *udp-port*

no eou port

シンタックスの説明

udp-port	UDP ポート番号。有効範囲は 1 ～ 65535 です。

デフォルト

21862（0x5566）

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

EAPoUDP を設定する前に **feature eou** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

例

次に、EAPoUDP の UDP ポート番号を変更する例を示します。

```
switch# config t
switch(config)# eou port 21856
```

次に、EAPoUDP の UDP ポート番号をデフォルトに戻す例を示します。

```
switch# config t
switch(config)# no eou port
```

関連コマンド

コマンド	説明
feature eou	EAPoUDP をイネーブルにします。
show eou	EAPoUDP 情報を表示します。

eou ratelimit

EAPoUDP ポスチャ検証の同時セッション数を設定するには、**eou ratelimit** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

eou ratelimit *sessions*

no eou ratelimit

シンタックスの説明

sessions	EAPoUDP ポスチャ検証の最大同時セッション数。有効範囲は 0 ～ 200 です。

デフォルト

グローバル コンフィギュレーション：20

インターフェイス コンフィギュレーション：グローバル コンフィギュレーション設定

コマンド モード

グローバル コンフィギュレーション
インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

EAPoUDP レート制限をゼロ（0）に設定すると、ポスチャ検証の同時セッションは許可されません。

インターフェイスの EAPoUDP レート制限設定は、グローバル EAPoUDP レート制限設定を上書きします。

EAPoUDP を設定する前に **feature eou** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

例

次に、EAPoUDP ポスチャ検証のグローバル最大同時セッション数を変更する例を示します。

```
switch# config t
switch(config)# eou ratelimit 30
```

次に、EAPoUDP ポスチャ検証のグローバル最大同時セッション数をデフォルトに戻す例を示します。

```
switch# config t
switch(config)# no eou ratelimit
```

次に、インターフェイスの EAPoUDP ポスチャ検証の最大同時セッション数を変更する例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# eou ratelimit 30
```

次に、インターフェイスの EAPoUDP ポスチャ検証の最大同時セッション数をデフォルトに戻す例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# no eou ratelimit
```

関連コマンド

コマンド	説明
feature eou	EAPoUDP をイネーブルにします。
show eou	EAPoUDP 情報を表示します。

eou revalidate（EXEC）

EAPoUDP セッションを再検証するには、**eou revalidate** コマンドを使用します。

eou revalidate {**all** | **authentication** {**clientless** | **eap** | **static**} | **interface ethernet** *slot/port* | **ip-address** *ipv4-address* | **mac-address** *mac-address* | **posturetoken** *name*}

シンタックスの説明

all	すべての EAPoUDP セッションを再検証します。
authentication	特定の認証タイプの EAPoUDP セッションを再検証します。
clientless	クライアントレス ポスチャ検証を使用して認証するセッションを指定します。
eap	EAPoUDP を使用して認証するセッションを指定します。
static	静的に設定された例外リストを使用して認証するセッションを指定します。
interface ethernet *slot/port*	特定のインターフェイスの EAPoUDP セッションを再検証します。
ip-address *ipv4-address*	特定の IPv4 アドレスの EAPoUDP セッションを再検証します。
mac-address *mac-address*	特定の MAC アドレスの EAPoUDP セッションを再検証します。
posturetoken *name*	特定のポスチャ トークンの EAPoUDP セッションを再検証します。

デフォルト

なし

コマンド モード

任意のコマンド モード

（注） NX-OS ソフトウェアは、グローバル コンフィギュレーション モードの **eou revalidate** コマンドをサポートします。グローバル コンフィギュレーション モードで EXEC レベルの **eou revalidate** コマンドを使用するには、必須キーワードを指定します。

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

EAPoUDP を設定する前に **feature eou** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

例

次に、すべての EAPoUDP セッションを再検証する例を示します。

```
switch# eou revalidate all
```

次に、すべての EAPoUDP セッションを再検証する例を示します。

```
switch# eou revalidate authentication static
```

次に、すべての EAPoUDP セッションを再検証する例を示します。

```
switch# eou revalidate interface ethernet 1/1
```

次に、すべての EAPoUDP セッションを再検証する例を示します。

```
switch# eou revalidate ip-address 10.10.1.1
```

次に、すべての EAPoUDP セッションを再検証する例を示します。

```
switch# eou revalidate mac-address 0019.076c.dac4
```

次に、すべての EAPoUDP セッションを再検証する例を示します。

```
switch# eou revalidate posturetoken healthy
```

関連コマンド

コマンド	説明
feature eou	EAPoUDP をイネーブルにします。
show eou	EAPoUDP 情報を表示します。

eou revalidate（グローバル コンフィギュレーション、インターフェイス コンフィギュレーション）

EAPoUDP セッションの定期的な自動再検証をグローバルに、または特定のインターフェイスでイネーブルにするには、**eou revalidate** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

eou revalidate

no eou revalidate

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

グローバル コンフィギュレーション：イネーブル

インターフェイス コンフィギュレーション：グローバル コンフィギュレーション値

コマンド モード

グローバル コンフィギュレーション
インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

インターフェイスの自動再検証の設定は、グローバル自動再検証の設定を上書きします。

（注） NX-OS ソフトウェアは、EXEC コンフィギュレーション モードの **eou revalidate** コマンドをサポートします。グローバル コンフィギュレーション モードで EXEC レベルの **eou revalidate** コマンドを使用するには、必須キーワードを指定します。

EAPoUDP を設定する前に **feature eou** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

例

次に、EAPoUDP セッションのグローバル自動再検証をディセーブルにする例を示します。

```
switch# config t
switch(config)# no eou revalidate
```

次に、EAPoUDP セッションのグローバル自動再検証をイネーブルにする例を示します。

```
switch# config t
switch(config)# eou revalidate
```

次に、インターフェイスの EAPoUDP セッションの自動再検証をディセーブルにする例を示します。

```
switch# config t
switch(config)# no eou revalidate
```

次に、インターフェイスの EAPoUDP セッションの自動再検証をイネーブルにする例を示します。

```
switch# config t
switch(config)# eou revalidate
```

関連コマンド

コマンド	説明
feature eou	EAPoUDP をイネーブルにします。
eou timeout	EAPoUDP の定期的な自動再検証のタイムアウト間隔を設定します。
show eou	EAPoUDP 情報を表示します。

eou timeout

EAPoUDP グローバル タイマーまたはインターフェイスの EAPoUDP タイマーのタイムアウト間隔を設定するには、**eou timeout** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

eou timeout {**aaa** *seconds* | **hold-period** *seconds* | **retransmit** *seconds* | **revalidation** *seconds* | **status-query** *seconds*}

no eou timeout {**aaa** | **hold-period** | **retransmit** | **revalidation** | **status-query**}

シンタックスの説明

aaa *seconds*	AAA タイムアウト間隔を指定します。有効範囲は 0 ～ 60 秒です。 **（注）** AAA タイムアウト間隔をゼロ（0）に設定すると、AAA タイマーがディセーブルになります。
hold-period *seconds*	ホールド タイムアウト間隔を指定します。有効範囲は 60 ～ 86400 秒です。
retransmit *seconds*	再送信タイムアウト間隔を指定します。有効範囲は 1 ～ 60 秒です。
revalidation *seconds*	定期的な自動再検証タイムアウト間隔を指定します。有効範囲は 5 ～ 86400 秒です。
status-query *seconds*	ステータス クエリー タイムアウト間隔を指定します。有効範囲は 10 ～ 1800 秒です。

デフォルト

グローバル AAA タイムアウト間隔：60 秒（1 分）

グローバル ホールド時間タイムアウト：180 秒（3 分）

グローバル再送信タイムアウト間隔：3 秒

グローバル再検証タイムアウト間隔：36000 秒（10 時間）

グローバル ステータス クエリー タイムアウト間隔：300 秒（5 分）

インターフェイス タイムアウト間隔：グローバル コンフィギュレーション値

コマンド モード

グローバル コンフィギュレーション
インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

インターフェイス タイマーのタイムアウト間隔値は、グローバル タイムアウト値を上書きします。

EAPoUDP を設定する前に **feature eou** コマンドを使用する必要があります。

このコマンドにライセンスは必要ありません。

例

次に、グローバル AAA タイムアウト間隔を変更する例を示します。

```
switch# config t
switch(config)# eou timeout aaa 50
```

次に、インターフェイスの AAA タイムアウト間隔を変更する例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# eou timeout aaa 60
```

次に、グローバル ホールド時間タイムアウト間隔を変更する例を示します。

```
switch# config t
switch(config)# eou timeout hold-period 480
```

次に、インターフェイスのホールド時間タイムアウト間隔を変更する例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# eou timeout hold-period 540
```

次に、グローバル再送信タイムアウト間隔を変更する例を示します。

```
switch# config t
switch(config)# eou timeout retransmit 5
```

次に、インターフェイスの再送信タイムアウト間隔を変更する例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# eou timeout retransmit 4
```

次に、グローバル再検証タイムアウト間隔を変更する例を示します。

```
switch# config t
switch(config)# eou timeout revalidation 34000
```

次に、インターフェイスの再検証タイムアウト間隔を変更する例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# eou timeout revalidation 30000
```

次に、グローバル ステータス クエリー タイムアウト間隔を変更する例を示します。

```
switch# config t
switch(config)# eou timeout status-query 240
```

次に、インターフェイスのステータス クエリー タイムアウト間隔を変更する例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# eou timeout status-query 270
```

関連コマンド

コマンド	説明
feature eou	EAPoUDP をイネーブルにします。
eou revalidate（グローバル コンフィギュレーション）	エンドポイント デバイスの定期的な自動再検証をイネーブルにします。
show eou	EAPoUDP 情報を表示します。

eq

単一ポートを IP ポート オブジェクト グループのグループ メンバーとして指定するには、**eq** コマンドを使用します。ポート オブジェクト グループから単一のポート グループ メンバーを削除するには、このコマンドの **no** 形式を使用します。

[*sequence-number*] **eq** *port-number*

no {*sequence-number* | **eq** *port-number*}

シンタックスの説明

sequence-number	（任意）このグループ メンバーのシーケンス番号。オブジェクト グループ内のグループ メンバーの順序は、シーケンス番号によって維持されます。有効なシーケンス番号は 1 ～ 4294967295 です。シーケンス番号を指定しない場合は、デバイスによって現在のオブジェクト グループで最も大きいシーケンス番号よりも 10 大きい番号が割り当てられます。
port-number	このグループ メンバーが一致するポート番号。有効なポート番号は、0 ～ 65535 です。

デフォルト

なし

コマンド モード

IP ポート オブジェクト グループ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

IP ポート オブジェクト グループには方向がありません。**eq** コマンドが送信元ポートまた宛先ポートのいずれに一致するか、またインバウンドとアウトバウンドのいずれのトラフィックに適用されるかは、ACL でオブジェクト グループをどのように使用するかによって決まります。

このコマンドにライセンスは必要ありません。

例

次に、ポート 443 から送受信されるトラフィックに一致するグループ メンバーを持つ port-group-05 という名前の IP ポート オブジェクト グループを設定する例を示します。

```
switch# config t
switch(config)# object-group ip port port-group-05
switch(config-port-ogroup)# eq 443
```

関連コマンド

コマンド	説明
gt	IP ポート オブジェクト グループの指定値より大きい値のグループ メンバーを指定します。
lt	IP ポート オブジェクト グループの指定値より小さい値のグループ メンバーを指定します。
neq	IP ポート オブジェクト グループの指定値に一致しないグループ メンバーを指定します。
object-group ip port	IP ポート オブジェクト グループを設定します。
range	IP ポート オブジェクト グループのポート範囲内のグループ メンバーを指定します。
show object-group	オブジェクト グループを表示します。

F コマンド

この章では、F で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

feature（ユーザ ロール機能グループ）

ユーザ ロール機能グループに機能を設定するには、**feature** コマンドを使用します。ユーザ ロール機能グループから機能を削除するには、このコマンドの **no** 形式を使用します。

feature *feature-name*

no feature *feature-name*

シンタックスの説明

feature-name	**show role feature** コマンドの出力に表示される NX-OS 機能名

デフォルト

なし

コマンド モード

ユーザ ロール機能グループ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドで使用できる有効な機能名を表示するには、show role feature コマンドを使用します。

このコマンドには、ライセンスは不要です。

例

次に、ユーザ ロール機能グループに機能を追加する例を示します。

```
switch# config t
switch(config)# role feature-group name SecGroup
switch(config-role-featuregrp)# feature aaa
switch(config-role-featuregrp)# feature radius
switch(config-role-featuregrp)# feature tacacs
```

次に、ユーザ ロール機能グループから機能を削除する例を示します。

```
switch# config t
switch(config)# role feature-group name MyGroup
switch(config-role-featuregrp)# no feature callhome
```

関連コマンド

コマンド	説明
show role feature-group	ユーザ ロール機能グループを表示します。

feature cts

Cisco TrustSec 機能をイネーブルにするには、**feature cts** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

feature cts

no feature cts

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature dot1x** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

（注） Cisco TrustSec 機能には、ライセンス猶予期間はありません。この機能を設定するには、アドバンスト サービス ライセンスをインストールする必要があります。

このコマンドには、アドバンスト サービス ライセンスが必要です。

例

次に、Cisco TrustSec 機能をイネーブルにする例を示します。

```
switch# config t
switch(config)# feature cts
```

次に、Cisco TrustSec 機能をディセーブルにする例を示します。

```
switch# config t
switch(config)# no feature cts
```

関連コマンド

コマンド	説明
feature dot1x	802.1X 機能をイネーブルにします。
show cts	Cisco TrustSec のステータス情報を表示します。

feature dhcp

デバイス上で DHCP スヌーピング機能をイネーブルにするには、**feature dhcp** コマンドを使用します。DHCP スヌーピング機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

feature dhcp

no feature dhcp

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトの設定では、DHCP スヌーピング機能はディセーブルです。

DHCP スヌーピング機能をイネーブルにしないと、DHCP スヌーピングの関連コマンドを使用できません。

ダイナミック APR インスペクションおよび IP ソース ガードは、DHCP スヌーピング機能に依存します。

DHCP スヌーピング機能をディセーブルにすると、デバイス上のすべての DHCP スヌーピング設定が廃棄されます。DHCP スヌーピング設定を保持したまま、DHCP スヌーピング機能をオフにしたい場合には、**no ip dhcp snooping** コマンドを使用して、DHCP スヌーピングをグローバルにディセーブルにします。

このコマンドには、ライセンスは不要です。

例

次に、DHCP スヌーピングをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# feature dhcp
switch(config)#
```

関連コマンド

コマンド	説明
clear ip dhcp snooping binding	DHCP スヌーピング バインディング データベースをクリアします。
ip dhcp snooping	デバイス上で DHCP スヌーピングをグローバルにイネーブルにします。
service dhcp	DHCP リレー エージェントをイネーブルまたはディセーブルにします。
show ip dhcp snooping	DHCP スヌーピングの全般情報を表示します。
show running-config dhcp	IP ソース ガード設定を含む、DHCP スヌーピング設定を表示します。

feature dot1x

802.1X 機能をイネーブルにするには、**feature dot1x** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

feature dot1x

no feature dot1x

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

802.1X を設定する前に、**feature dot1x** コマンドを使用する必要があります。

（注） 802.1X 機能をディセーブルにすると、すべての 802.1X 設定が失われます。802.1X 認証をディセーブルにする場合は、**no dot1x system-auth-control** コマンドを使用します。

このコマンドには、ライセンスは不要です。

例

次に、802.1X をイネーブルにする例を示します。

```
switch# config t
switch(config)# feature dot1x
```

次に、802.1X をディセーブルにする例を示します。

```
switch# config t
switch(config)# no feature dot1x
```

関連コマンド

コマンド	説明
show dot1x	802.1X のステータス情報を表示します。

feature eou

Extensible Authentication Protocol over User Datagram Protocol（EAPoUDP）をイネーブルにするには、**feature eou** コマンドを使用します。EAPoUDP をディセーブルにするには、このコマンドの **no** 形式を使用します。

feature eou

no feature eou

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

EAPoUDP を設定する前に、**feature eou** コマンドを使用する必要があります。

（注） EAPoUDP をディセーブルにすると、NX-OS ソフトウェアにより EXPoUDP 設定が削除されます。

このコマンドには、ライセンスは不要です。

例

次に、EAPoUDP をイネーブルにする例を示します。

```
switch# config t
switch(config)# feature eou
```

次に、EAPoUDP をディセーブルにする例を示します。

```
switch# config t
switch(config)# no feature eou
```

関連コマンド

コマンド	説明
feature eou	EAPoUDP をイネーブルにします。
show eou	EAPoUDP 情報を表示します。

feature port-security

ポート セキュリティ機能をグローバルでイネーブルにするには、**feature port-security** コマンドを使用します。ポート セキュリティ機能をグローバルでディセーブルにするには、このコマンドの **no** 形式を使用します。

feature port-security

no feature port-security

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト なし

コマンド モード グローバル コンフィギュレーション

サポートされるユーザ ロール network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン デフォルトの設定では、ポート セキュリティはグローバルでディセーブルです。

ポート セキュリティは、各 Virtual Device Context（VDC; バーチャル デバイス コンテキスト）に対してローカルです。必要に応じて、このコマンドを使用する前に、対応する VDC に切り換えてください。

このコマンドには、ライセンスは不要です。

ポート セキュリティのイネーブル化

ポート セキュリティをグローバルでイネーブルにすると、ポート セキュリティに関連する他のすべてのコマンドが使用可能になります。

ポート セキュリティを再イネーブル化する場合、ポート セキュリティが最後にイネーブルだった時点のポート セキュリティ設定は復元されません。

ポート セキュリティのディセーブル化

ポート セキュリティをグローバルでディセーブルにすると、すべてのポート セキュリティ設定が削除されます。デバイスがアドレスをどのように学習したかに関係なく、ポート セキュリティのすべてのインターフェイス設定、およびすべてのセキュア MAC アドレスが削除されます。

例

次に、ポート セキュリティをグローバルでイネーブルにする例を示します。

```
switch# config t
switch(config)# feature port-security
switch(config)#
```

関連コマンド

コマンド	説明
clear port-security	ダイナミックに学習されたセキュア MAC アドレスをクリアします。
debug port-security	ポート セキュリティのデバッグ情報を提供します。
show port-security	ポート セキュリティの関連情報を表示します。
switchport port-security	レイヤ 2 インターフェイス上でポート セキュリティをイネーブルにします。

feature tacacs+

TACACS+ をイネーブルにするには、**feature tacacs+** コマンドを使用します。TACACS+ をディセーブルにするには、このコマンドの **no** 形式を使用します。

feature tacacs+

no feature tacacs+

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

ディセーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

TACACS+ を設定する前に、**feature tacacs+** コマンドを使用する必要があります。

（注） TACACS+ をディセーブルにすると、NX-OS ソフトウェアにより TACACS+ 設定が削除されます。

このコマンドには、ライセンスは不要です。

例

次に、TACACS+ をイネーブルにする例を示します。

```
switch# config t
switch(config)# feature tacacs+
```

次に、TACACS+ をディセーブルにする例を示します。

```
switch# config t
switch(config)# no feature tacacs+
```

関連コマンド

コマンド	説明
show tacacs+	TACACS+ 情報を表示します。

G コマンド

この章では、G で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

gt

IP ポート オブジェクト グループの greater-than グループ メンバーを指定するには、**gt** コマンドを使用します。greater-than グループ メンバーは、メンバーに指定されたポート番号より大きいポート番号と一致します。ポート オブジェクト グループから greater-than グループ メンバーを削除するには、このコマンドの **no** 形式を使用します。

[*sequence-number*] **gt** *port-number*

no {*sequence-number* | **gt** *port-number*}

シンタックスの説明

sequence-number	（任意）このグループ メンバーのシーケンス番号。シーケンス番号により、オブジェクト グループ内のグループ メンバーの順序を保持します。有効なシーケンス番号は、1 ～ 4294967295 です。シーケンス番号を指定しないと、現在のオブジェクト グループの最大シーケンス番号に 10 を加算した番号が割り当てられます。
port-number	このグループ メンバーと一致するトラフィックの、この番号より大きいポート番号。*port-number* 引数には、0 ～ 65535 の整数を指定できます。

デフォルト

なし

コマンド モード

IP ポート オブジェクト グループ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

IP ポート オブジェクト グループには、方向は設定されません。**gt** コマンドを、送信元ポートと宛先ポートのどちらと一致させるか、またはインバウンドとアウトバウンドのどちらのトラフィックに適用するかは、ACL でのオブジェクト グループの使用方法によって異なります。

このコマンドには、ライセンスは不要です。

例

次に、port-group-05 という名前の IP ポート オブジェクト グループに、ポート 49151 ～ 65535 で送受信されたトラフィックと一致させるグループ メンバーを設定する例を示します。

```
switch# config t
switch(config)# object-group ip port port-group-05
switch(config-port-ogroup)# gt 49151
```

関連コマンド

コマンド	説明
eq	IP ポート オブジェクト グループに equal-to グループ メンバーを指定します。
lt	IP ポート オブジェクト グループに less-than グループ メンバーを指定します。
neq	IP ポート オブジェクト グループに not-equal-to グループ メンバーを指定します。
object-group ip port	IP ポート オブジェクト グループを設定します。
range	IP ポート オブジェクト グループに port-range グループ メンバーを指定します。
show object-group	オブオジェクト グループを表示します。

H コマンド

この章では、H で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

host（IPv4）

ホストまたはサブネットを IPv4 アドレス オブジェクト グループのメンバーとして指定するには、**host** コマンドを使用します。IPv4 アドレス オブジェクト グループからグループ メンバーを削除するには、このコマンドの **no** 形式を使用します。

[*sequence-number*] **host** *IPv4-address*

no {*sequence-number* | **host** *IPv4-address*}

[*sequence-number*] *IPv4-address network-wildcard*

no *IPv4-address network-wildcard*

[*sequence-number*] *IPv4-address/prefix-len*

no *IPv4-address/prefix-len*

シンタックスの説明

sequence-number	（任意）このグループ メンバーのシーケンス番号。シーケンス番号により、オブジェクト グループ内のグループ メンバーの順序を保持します。有効なシーケンス番号は、1 ～ 4294967295 です。シーケンス番号を指定しないと、現在のオブジェクト グループの最大シーケンス番号に 10 を加算した番号が割り当てられます。
host *IPv4-address*	グループ メンバーを単一 IPv4 アドレスで指定します。*IPv4-address* を、ドット付き 10 進表記で入力します。
IPv4-address network-wildcard	IPv4 アドレスおよびネットワーク ワイルドカード。*IPv4-address* および *network-wildcard* を、ドット付き 10 進表記で入力します。*IPv4-address* のどのビットがネットワーク部分であるかを指定するには、*network-wildcard* を次のように使用します。 `switch(config-ipaddr-ogroup)# 10.23.176.0 0.0.0.255` *network-wildcard* 値が 0.0.0.0 の場合、グループ メンバーが特定の IPv4 アドレスであることを示します。

IPv4-address/prefix-len	IPv4 アドレスおよび可変長サブネット マスク。*IPv4-address* を、ドット付き 10 進表記で入力します。*IPv4-address* のネットワーク部分のビット数を指定するには、*prefix-len* を次のように使用します。 `switch(config-ipaddr-ogroup)# 10.23.176.0/24` *prefix-len* 値が 32 の場合、グループ メンバーが特定の IPv4 アドレスであることを示します。

デフォルト

なし

コマンド モード

IPv4 アドレス オブジェクト グループ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

グループ メンバーとしてサブネットを指定するには、このコマンドを、次のいずれかの形式で使用します。

[*sequence-number*] *IPv4-address network-wildcard*

[*sequence-number*] *IPv4-address/prefix-len*

サブネットを指定したコマンド形式に関係なく、**show object-group** コマンドを使用すると、グループ メンバーの *IP-address/prefix-len* 形式が表示されます。

グループ メンバーとして単一 IPv4 アドレスを指定するには、このコマンドを、次のいずれかの形式で使用します。

[*sequence-number*] **host** *IPv4-address*

[*sequence-number*] *IPv4-address* **0.0.0.0**

[*sequence-number*] *IPv4-address*/**32**

単一 IPv4 アドレスを指定したコマンド形式に関係なく、**show object-group** コマンドを使用すると、グループ メンバーの **host** *IP-address* 形式が表示されます。

このコマンドには、ライセンスは不要です。

例

次に、ipv4-addr-group-13 という IPv4 アドレス オブジェクト グループに、グループ メンバーとして 2 つの特定の IPv4 アドレスと、1 つのサブネット 10.23.176.0 を設定する例を示します。

```
switch# config t
switch(config)# object-group ip address ipv4-addr-group-13
switch(config-ipaddr-ogroup)# host 10.121.57.102
switch(config-ipaddr-ogroup)# 10.121.57.234/32
switch(config-ipaddr-ogroup)# 10.23.176.0 0.0.0.255
switch(config-ipaddr-ogroup)# show object-group ipv4-addr-group-13
        10 host 10.121.57.102
        20 host 10.121.57.234
        30 10.23.176.0/24
switch(config-ipaddr-ogroup)#
```

関連コマンド

コマンド	説明
object-group ip address	IPv4 アドレス グループを設定します。
show object-group	オブジェクト グループを表示します。

host（IPv6）

ホストまたはサブネットを IPv6 アドレス オブジェクト グループのメンバーとして指定するには、**host** コマンドを使用します。IPv6 アドレス オブジェクト グループからグループ メンバーを削除するには、このコマンドの **no** 形式を使用します。

[*sequence-number*] **host** *IPv6-address*

no {*sequence-number* | **host** *IPv6-address*}

[*sequence-number*] *IPv6-address/network-prefix*

no *IPv6-address/network-prefix*

シンタックスの説明

sequence-number	（任意）このグループ メンバーのシーケンス番号。シーケンス番号により、オブジェクト グループ内のグループ メンバーの順序を保持します。有効なシーケンス番号は、1 ～ 4294967295 です。シーケンス番号を指定しないと、現在のオブジェクト グループの最大シーケンス番号に 10 を加算した番号が割り当てられます。
host *IPv6-address*	グループ メンバーを単一 IPv6 アドレスで指定します。*IPv6-address* を、ドット付き 10 進表記で入力します。
IPv6-address/network-prefix	IPv6 アドレスおよび可変長サブネット マスク。*IPv6-address* を、コロンで区切った 16 進表記で入力します。*IPv6-address* のネットワーク部分のビット数を指定するには、*network-prefix* を次のように使用します。 `switch(config-ipv6addr-ogroup)# 2001:db8:0:3ab7::/96` *network-prefix* 値が 128 の場合、グループ メンバーが特定の IPv6 アドレスであることを示します。

デフォルト

なし

コマンド モード

IPv6 アドレス オブジェクト グループ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

グループ メンバーとしてサブネットを指定するには、このコマンドを、次の形式で使用します。

[*sequence-number*] *IPv6-address*/*network-prefix*

グループ メンバーとして単一 IPv6 アドレスを指定するには、このコマンドを、次のいずれかの形式で使用します。

[*sequence-number*] **host** *IPv6-address*

[*sequence-number*] *IPv6-address*/**128**

単一 IPv6 アドレスを指定したコマンド形式に関係なく、**show object-group** コマンドを使用すると、グループ メンバーの **host** *IPv6-address* 形式が表示されます。

このコマンドには、ライセンスは不要です。

例

次に、ipv6-addr-group-A7 という IPv6 アドレス オブジェクト グループに、グループ メンバーとして 2 つの特定の IPv6 アドレスと、1 つのサブネット 2001:db8:0:3ab7:: を設定する例を示します。

```
switch# config t
switch(config)# object-group ipv6 address ipv6-addr-group-A7
switch(config-ipv6addr-ogroup)# host 2001:db8:0:3ab0::1
switch(config-ipv6addr-ogroup)# 2001:db8:0:3ab0::2/128
switch(config-ipv6addr-ogroup)# 2001:db8:0:3ab7::/96
switch(config-ipv6addr-ogroup)# show object-group ipv6-addr-group-A7
        10 host 2001:db8:0:3ab0::1
        20 host 2001:db8:0:3ab0::2
        30 2001:db8:0:3ab7::/96
switch(config-ipv6addr-ogroup)#
```

関連コマンド

コマンド	説明
object-group ipv6 address	IPv6 アドレス グループを設定します。
show object-group	オブジェクト グループを表示します。

I コマンド

この章では、I で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

identity policy

アイデンティティ ポリシーを作成または指定して、アイデンティティ ポリシー コンフィギュレーション モードを開始するには、**identity policy** コマンドを使用します。アイデンティティ ポリシーを削除するには、このコマンドの **no** 形式を使用します。

identity policy *policy-name*

no identity policy *policy-name*

シンタックスの説明

policy-name	アイデンティティ ポリシーの名前。名前は、最大 100 文字で、大文字と小文字を区別した英数字で指定します。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin
VDC user

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは不要です。

例

次に、アイデンティティ ポリシーを作成して、アイデンティティ ポリシー コンフィギュレーション モードを開始する例を示します。

```
switch# config t
switch(config)# identity policy AdminPolicy
switch(config-id-policy)#
```

次に、アイデンティティ ポリシーを削除する例を示します。

```
switch# config t
switch(config)# no identity policy AdminPolicy
```

関連コマンド

コマンド	説明
show identity policy	アイデンティティ ポリシーの情報を表示します。

identity profile eapoudp

Extensible Authentication Protocol over User Datagram Protocol（EAPoUDP）アイデンティティ プロファイルを作成して、アイデンティティ プロファイル コンフィギュレーション モードを開始するには、**identity profile eapoudp** コマンドを使用します。EAPoUDP アイデンティティ プロファイル設定を削除するには、このコマンドの **no** 形式を使用します。

identity profile eapoudp

no identity profile eapoudp

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin
VDC user

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは不要です。

例

次に、EAPoUDP アイデンティティ プロファイルを作成して、アイデンティティ プロファイル コンフィギュレーション モードを開始する例を示します。

```
switch# config t
switch(config)# identity profile eapoudp
switch(config-id-policy)#
```

次に、EAPoUDP アイデンティティ プロファイル設定を削除する例を示します。

```
switch# config t
switch(config)# no identity profile eapoudp
```

関連コマンド

コマンド	説明
show identity profile	アイデンティティ プロファイルの情報を表示します。

interface policy deny

ユーザ ロールに対してインターフェイス ポリシー コンフィギュレーション モードを開始するには、**interface policy deny** コマンドを使用します。ユーザ ロールのインターフェイス ポリシーをデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

interface policy deny

no interface policy deny

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

すべてのインターフェイス

コマンド モード

ユーザ ロール コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、ユーザ ロール インターフェイス ポリシー コンフィギュレーション モードで **permit interface** コマンドを使用して許可したインターフェイスを除き、ユーザ ロールへのすべてのインターフェイスが拒否されます。

このコマンドには、ライセンスは不要です。

例

次に、ユーザ ロールに対して、ユーザ ロール インターフェイス ポリシー コンフィギュレーション モードを開始する例を示します。

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)#
```

次に、ユーザ ロールのインターフェイス ポリシーをデフォルト設定に戻す例を示します。

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# no interface policy deny
```

関連コマンド

コマンド	説明
permit interface	ロール インターフェイス ポリシーでインターフェイスを許可します。
role name	ユーザ ロールを作成または指定して、ユーザ ロール コンフィギュレーション モードを開始します。
show role	ユーザ ロールの情報を表示します。

ip access-group

IPv4 Access Control List（ACL; アクセス コントロール リスト）をインターフェイスのルータ ACL として適用するには、**ip access-group** コマンドを使用します。インターフェイスから IPv4 ACL を削除するには、このコマンドの **no** 形式を使用します。

ip access-group *access-list-name* {**in** | **out**}

no ip access-group *access-list-name* {**in** | **out**}

シンタックスの説明

access-list-name	IPv4 ACL の名前。最大 64 文字で、大文字と小文字を区別した英数字で指定します。
in	（任意）ACL をインバウンド トラフィックに適用します。
out	（任意）ACL をアウトバウンド トラフィックに適用します。

デフォルト

なし

コマンド モード

インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、インターフェイスに IPv4 ACL は適用されません。

ip access-group コマンドを使用することにより、次のインターフェイス タイプに対して、IPv4 ACL をルータ ACL として適用できます。

- VLAN インターフェイス

（注） VLAN インターフェイスを設定する前に、VLAN インターフェイスをグローバルでイネーブルにする必要があります。詳細については、『*Cisco NX-OS Interfaces Command Reference*』の **feature interface-vlan** コマンドを参照してください。

- レイヤ 3 イーサネット インターフェイス
- レイヤ 3 イーサネット サブインターフェイス
- レイヤ 3 イーサネット ポートチャネル インターフェイスおよびサブインターフェイス
- トンネル
- ループバック インターフェイス
- 管理インターフェイス

また、**ip access-group** コマンドを使用して、次のインターフェイス タイプに対しても、IPv4 ACL をルータ ACL として適用できます。

- レイヤ 2 イーサネット インターフェイス

- レイヤ 2 イーサネット ポートチャネル インターフェイス

ただし、**ip access-group** コマンドを使用してレイヤ 2 に適用した ACL は、ポート モードをルーテッド（レイヤ 3）モードに変更しない限り、アクティブになりません。IPv4 ACL をポート ACL として適用するには、**ip port access-group** コマンドを使用します。

IPv4 ACL を VLAN ACL として適用することもできます。詳細については、「match（VLAN アクセス マップ）」（p.191）を参照してください。

ルータ ACL は、アウトバウンドまたはインバウンドのどちらかのトラフィックに適用されます。ACL がインバウンド トラフィックに適用されると、インバウンド パケットが ACL のルールに対してチェックされます。最初の一致ルールによってパケットが許可されると、そのパケットは引き続き処理されます。最初の一致ルールによってパケットが拒否されると、そのパケットはドロップされ、ICMP ホスト到達不能メッセージが戻されます。

アウトバウンド アクセス リストの場合は、受信したパケットはインターフェイスにルーティングされたあとで、ACL に対してチェックされます。最初の一致ルールによってパケットが許可されると、そのパケットは指定された宛先に送信されます。最初の一致ルールによってパケットが拒否されると、そのパケットはドロップされ、ICMP ホスト到達不能メッセージが戻されます。

デバイスから特定の ACL を削除した場合、インターフェイスからその ACL を削除しなくても、削除した ACL はインターフェイス上のトラフィックには影響しません。

このコマンドには、ライセンスは不要です。

例

次に、イーサネット インターフェイス 2/1 に対して、ip-acl-01 という IPv4 ACL を適用する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# ip access-group ip-acl-01 in
```

次に、イーサネット インターフェイス 2/1 から、ip-acl-01 という IPv4 ACL を削除する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# no ip access-group ip-acl-01 in
```

関連コマンド

コマンド	説明
ip access-list	IPv4 ACL を設定します。
ip port access-group	IPv4 ACL をポート ACL として適用します。
show access-lists	すべての ACL を表示します。
show ip access-lists	特定の IPv4 ACL またはすべての IPv4 ACL を表示します。
show running-config interface	すべてのインターフェイスまたは特定のインターフェイスの実行コンフィギュレーションを表示します。

ip access-list

IPv4 Access Control List（ACL; アクセス コントロール リスト）を作成して、特定の ACL の IP アクセス リスト コンフィギュレーション モードを開始するには、**ip access-list** コマンドを使用します。IPv4 ACL を削除するには、このコマンドの **no** 形式を使用します。

ip access-list *access-list-name*

no ip access-list *access-list-name*

シンタックスの説明

access-list-name	IPv4 ACL の名前。名前は最大 64 文字で、大文字と小文字を区別した英数字で指定します。スペースまたは引用符は使用できません。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、IPv4 ACL は定義されません。

IPv4 トラフィックをフィルタリングするには、IPv4 ACL を使用します。

ip access-list コマンドを使用すると、IP アクセス リスト コンフィギュレーション モードが開始されます。このモードで、IPv4 **deny** および **permit** コマンドを使用し、ACL のルールを設定します。指定した ACL が存在しない場合は、このコマンドの入力時に新しい ACL が作成されます。

ACL をルータ ACL としてインターフェイスに適用するには、**ip access-group** コマンドを使用します。ACL をポート ACL としてインターフェイスに適用するには、**ip port access-group** コマンドを使用します。

すべての IPv4 ACL は、最終ルールとして、次の暗黙ルールが設定されます。

```
deny ip any any
```

この暗黙ルールにより、一致しなかった IP トラフィックはすべて拒否されます。

IPv4 ACL には、近隣探索プロセスをイネーブルにする暗黙ルールは追加されません。Address Resolution Protocol（ARP; アドレス解決プロトコル）は、別のデータ リンク レイヤ プロトコルを使用します。デフォルトでは、IPv4 ACL は、インターフェイス上での ARP パケットの送受信を暗黙で許可します。

IPv4 ACL の各ルールの統計情報を記録するには、**statistics per-entry** コマンドを使用します。暗黙ルールの統計情報は記録されません。暗黙の **deny ip any any** ルールに一致したパケットの統計情報を記録するには、まったく同じルールを明示的に設定する必要があります。

このコマンドには、ライセンスは不要です。

例

次に、ip-acl-01 という IPv4 ACL の IP アクセス リスト コンフィギュレーション モードを開始する例を示します。

```
switch# conf t
switch(config)# ip access-list ip-acl-01
switch(config-acl)#
```

関連コマンド

コマンド	説明
access-class	IPv4 ACL を VTY 回線に適用します。
deny（IPv4）	IPv4 ACL に拒否（deny）ルールを設定します。
ip access-group	IPV4 ACL をルータ ACL としてインターフェイスに適用します。
ip port access-group	IPV4 ACL をポート ACL としてインターフェイスに適用します。
permit（IPv4）	IPv4 ACL に許可（permit）ルールを設定します。
show ip access-lists	すべての IPv4 ACL または特定の IPv4 ACL を表示します。
statistics per-entry	ACL の各エントリの統計情報の収集をイネーブルにします。

ip arp inspection filter

ARP Access Control List（ACL; アクセス コントロール リスト）を VLAN リストに適用するには、**ip arp inspection filter** コマンドを使用します。VLAN リストから ARP ACL を削除するには、このコマンドの **no** 形式を使用します。

ip arp inspection filter *acl-name* **vlan** *vlan-list*

no ip arp inspection filter *acl-name* **vlan** *vlan-list*

シンタックスの説明

acl-name	ARP ACL の名前。最大 64 文字で、大文字と小文字を区別した英数字で指定します。
vlan *vlan-list*	ARP ACL でフィルタリングする VLAN を指定します。*vlan-list* 引数には、単一 VLAN ID、VLAN ID 範囲、またはカンマで区切った ID と範囲を指定できます（例のセクションを参照）。有効な VLAN ID は、1 ～ 4096 です。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは不要です。

例

次に、VLAN 15 および 37 ～ 48 に対して、arp-acl-01 という ARP ACL を適用する例を示します。

```
switch# configure terminal
switch(config)# ip arp inspection filter arp-acl-01 vlan 15,37-48
switch(config)#
```

関連コマンド

コマンド	説明
arp access-list	ARP ACL を設定します。
ip arp inspection vlan	指定した VLAN リストの Dynamic ARP Inspection（DAI）をイネーブルにします。
show ip arp inspection	DAI 設定ステータスを表示します。
show running-config dhcp	DAI 設定を含む、DHCP スヌーピング設定を表示します。

ip arp inspection log-buffer

Dynamic ARP Inspection（DAI）ロギング バッファのサイズを設定するには、**ip arp inspection log-buffer** コマンドを使用します。DAI ロギング バッファをデフォルトのサイズに戻すには、このコマンドの **no** 形式を使用します。

ip arp inspection log-buffer entries *number*

no ip arp inspection log-buffer entries *number*

シンタックスの説明

entries *number*	0 ～ 1024 メッセージの範囲で、バッファ サイズを指定します。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

DAI ロギング バッファのデフォルトのサイズは、32 メッセージです。

このコマンドには、ライセンスは不要です。

例

次に、DAI ロギング バッファのサイズを設定する例を示します。

```
switch# configure terminal
switch(config)# ip arp inspection log-buffer entries 64
switch(config)#
```

関連コマンド

コマンド	説明
clear ip arp inspection log	DAI ロギング バッファをクリアします。
show ip arp inspection	DAI の設定ステータスを表示します。
show running-config dhcp	DAI 設定を含む、DHCP スヌーピング設定を表示します。

ip arp inspection trust

レイヤ 2 インターフェイスを信頼できる ARP インターフェイスとして設定するには、**ip arp inspection trust** コマンドを使用します。レイヤ 2 インターフェイスを信頼できない ARP インターフェイスとして設定するには、このコマンドの **no** 形式を使用します。

ip arp inspection trust

no ip arp inspection trust

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトでは、すべてのインターフェイスが信頼できない ARP インターフェイスです。

コマンド モード

インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

信頼できる ARP インターフェイスとして設定できるのは、レイヤ 2 イーサネット インターフェイスだけです。

このコマンドには、ライセンスは不要です。

例

次に、レイヤ 2 インターフェイスを信頼できる ARP インターフェイスとして設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ip arp inspection trust
switch(config-if)#
```

関連コマンド

コマンド	説明
show ip arp inspection	Dynamic ARP Inspection（DAI）の設定ステータスを表示します。
show ip arp inspection interface	特定のインターフェイスの信頼状態および ARP パケット レートを表示します。
show running-config dhcp	DAI 設定を含む、DHCP スヌーピング設定を表示します。

ip arp inspection validate

追加の Dynamic ARP Inspection（DAI）検証をイネーブルにするには、**ip arp inspection validate** コマンドを使用します。追加の DAI をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip arp inspection validate {**dst-mac** [**ip**] [**src-mac**]}

ip arp inspection validate {[**dst-mac**] **ip** [**src-mac**]}

ip arp inspection validate {[**dst-mac**] [**ip**] **src-mac**}

no ip arp inspection validate {**dst-mac** [**ip**] [**src-mac**]}

no ip arp inspection validate {[**dst-mac**] **ip** [**src-mac**]}

no ip arp inspection validate {[**dst-mac**] [**ip**] **src-mac**}

シンタックスの説明

dst-mac	（任意）イーサネット ヘッダーの宛先 MAC アドレスを、ARP 応答の ARP 本文にあるターゲット MAC アドレスと照合します。MAC アドレスが一致していないパケットは無効として分類され、ドロップされます。
ip	（任意）ARP 本文が有効で、予期された IP アドレスかどうかを検証します。アドレスには、0.0.0.0、255.255.255.255、およびすべての IP マルチキャスト アドレスが含まれます。送信側 IP アドレスは、すべての ARP 要求および ARP 応答でチェックされます。ターゲット IP アドレスは ARP 応答でのみチェックされます。
src-mac	（任意）イーサネット ヘッダーの送信元 MAC アドレスを、ARP 要求および応答の ARP 本文にある送信側 MAC アドレスと照合します。MAC アドレスが一致していないパケットは無効として分類され、ドロップされます。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

最小限、1 つのキーワードを指定する必要があります。複数のキーワードを指定する場合、順序は影響しません。

このコマンドには、ライセンスは不要です。

例

次に、追加の DAI 検証をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# ip arp inspection validate src-mac dst-mac ip
switch(config)#
```

関連コマンド

コマンド	説明
show ip arp inspection	DAI の設定ステータスを表示します。
show running-config dhcp	DAI 設定を含む、DHCP スヌーピング設定を表示します。

ip arp inspection vlan

VLAN リストに対して Dynamic ARP Inspection（DAI）をイネーブルにするには、**ip arp inspection vlan** コマンドを使用します。VLAN リストの DAI をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip arp inspection vlan *vlan-list* [**logging dhcp-bindings** {**permit | all | none**}]

no ip arp inspection vlan *vlan-list* [**logging dhcp-bindings** {**permit | all | none**}]

シンタックスの説明

vlan-list	DAI をアクティブにする VLAN。*vlan-list* 引数には、単一 VLAN ID、VLAN ID 範囲、またはカンマで区切った ID と範囲を指定できます（例のセクションを参照）。有効な VLAN ID は、1 ～ 4096 です。
logging	（任意）指定した VLAN の DAI ロギングをイネーブルにします。 — **all** — DHCP バインディングと一致するすべてのパケットをロギングします。 — **none** — DHCP バインディング パケットをロギングしません（このオプションは、ロギングをディセーブルにする場合に使用します）。 — **permit** — DHCP バインディングで許可されたパケットをロギングします。
dhcp-bindings	DHCP バインディングの一致に基づくロギングをイネーブルにします。
permit	DHCP バインディング一致による許可パケットのロギングをイネーブルにします。
all	すべてのパケットのロギングをイネーブルにします。
none	ロギングをディセーブルにします。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、DAI によって検査されたパケットはロギングされません。

このコマンドには、ライセンスは不要です。

例

次に、VLAN 13、15、および 17 ～ 23 で DAI をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# ip arp inspection vlan 13,15,17-23
switch(config)#
```

関連コマンド

コマンド	説明
ip arp inspection validate	追加の DAI 検証をイネーブルにします。
show ip arp inspection	DAI の設定ステータスを表示します。
show ip arp inspection vlan	特定の VLAN リストの DAI ステータスを表示します。
show running-config dhcp	DAI 設定を含む、DHCP スヌーピング設定を表示します。

ip dhcp relay address

インターフェイス上に DHCP サーバの IP アドレスを設定するには、**ip dhcp relay address** コマンドを使用します。DHCP サーバの IP アドレスを削除するには、このコマンドの **no** 形式を使用します。

ip dhcp relay address *IP-address*

no ip dhcp relay address *IP-address*

シンタックスの説明

IP-address	DHCP サーバの IPv4 アドレス

デフォルト

なし

コマンド モード

インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。
4.0(3)	レイヤ 3 イーサネット インターフェイスまたはサブインターフェイスの設定に、最大 4 つの **ip dhcp relay address** コマンドを追加できるようになりました。

使用上のガイドライン

このコマンドを使用するには、DHCP スヌーピング機能をイネーブルにする必要があります（**feature dhcp** コマンドを参照）。

レイヤ 3 イーサネット インターフェイスおよびサブインターフェイス、VLAN インターフェイス、およびレイヤ 3 ポート チャネルに、それぞれ最大 4 つの DHCP サーバ IP アドレスを設定できます。Cisco NX-OS Release 4.0.2 以前のリリースでは、1 つのインターフェイスに設定できる DHCP サーバ IP アドレスは 1 つだけです。

インターフェイス上にインバウンド DHCP BOOTREQUEST パケットが到達すると、リレー エージェントによって、そのインターフェイスに設定されているすべての DHCP サーバ IP アドレスに、パケットが転送されます。また、リレー エージェントにより、すべての DHCP サーバからの応答が、要求を送信したホストに戻されます。

このコマンドには、ライセンスは不要です。

例

次に、特定のレイヤ 3 イーサネット インターフェイス上で受信した BOOTREQUEST がリレー エージェントによって転送されるように、インターフェイスに 2 つの DHCP サーバ IP アドレスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ip dhcp relay address 10.132.7.120
switch(config-if)# ip dhcp relay address 10.132.7.175
switch(config-if)#
```

次に、VLAN インターフェイス上に DHCP サーバの IP アドレスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface vlan 13
switch(config-if)# ip dhcp relay address 10.132.7.120
switch(config-if)#
```

次に、レイヤ 3 ポートチャネル インターフェイス上に DHCP サーバの IP アドレスを設定する例を示します。

```
switch# configure terminal
switch(config)# interface port-channel 7
switch(config-if)# ip dhcp relay address 10.132.7.120
switch(config-if)#
```

関連コマンド

コマンド	説明
ip dhcp relay information option	DHCP パケットの option-82 情報の挿入および削除をイネーブルにします。
ip dhcp snooping	デバイス上で DHCP スヌーピングをグローバルにイネーブルにします。
service dhcp	DHCP リレー エージェントをイネーブルまたはディセーブルにします。
show ip dhcp snooping	DHCP スヌーピングの全般情報を表示します。
show running-config dhcp	IP ソース ガード設定を含む、DHCP スヌーピング設定を表示します。

ip dhcp relay information option

リレー エージェントによって転送された DHCP パケットでの option-82 情報の挿入および削除をイネーブルにするには、**ip dhcp relay information option** コマンドを使用します。option-82 情報の挿入および削除をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip dhcp relay information option

no ip dhcp relay information option

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトでは、リレー エージェントによって転送された DHCP パケットでの option-82 情報の挿入および削除は実行されません。

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、DHCP スヌーピング機能をイネーブルにする必要があります（**feature dhcp** コマンドを参照）。

このコマンドには、ライセンスは不要です。

例

次に、DHCP リレー エージェントによって転送されるパケットでの option-82 情報の挿入および削除をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# ip dhcp relay information option
switch(config)#
```

関連コマンド

コマンド	説明
ip dhcp relay address	インターフェイス上に DHCP サーバの IP アドレスを設定します。
ip dhcp snooping	デバイス上で DHCP スヌーピングをグローバルにイネーブルにします。
ip dhcp snooping information option	DHCP リレー エージェントを使用しないで転送された DHCP パケットでの option-82 情報の挿入および削除をイネーブルにします。
service dhcp	DHCP リレー エージェントをイネーブルまたはディセーブルにします。
show running-config dhcp	IP ソース ガード設定を含む、DHCP スヌーピング設定を表示します。

ip dhcp snooping

デバイス上で DHCP スヌーピングをグローバルでイネーブルにするには、**ip dhcp snooping** コマンドを使用します。DHCP スヌーピングをグローバルでディセーブルにするには、このコマンドの **no** 形式を使用します。

ip dhcp snooping

no ip dhcp snooping

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトでは、DHCP スヌーピングはグローバルでディセーブルです。

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、DHCP スヌーピング機能をイネーブルにする必要があります（**feature dhcp** コマンドを参照）。

no ip dhcp snooping コマンドを使用して DHCP スヌーピングをディセーブルにすると、デバイスの DHCP スヌーピング設定が保持されます。

このコマンドには、ライセンスは不要です。

例

次に、DHCP スヌーピングをグローバルでイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# ip dhcp snooping
switch(config)#
```

関連コマンド

コマンド	説明
feature dhcp	デバイス上で DHCP スヌーピング機能をイネーブルにします。
ip dhcp snooping information option	DHCP リレー エージェントを使用しないで転送された DHCP パケットでの option-82 情報の挿入および削除をイネーブルにします。
ip dhcp snooping trust	インターフェイスを、DHCP メッセージの信頼できる送信元として設定します。
ip dhcp snooping vlan	特定の VLAN 上で DHCP スヌーピングをイネーブルにします。
service dhcp	DHCP リレー エージェントをイネーブルまたはディセーブルにします。
show ip dhcp snooping	DHCP スヌーピングの全般情報を表示します。
show running-config dhcp	IP ソース ガード設定を含む、DHCP スヌーピング設定を表示します。

ip dhcp snooping information option

DHCP パケットの option-82 情報の挿入および削除をイネーブルにするには、**ip dhcp snooping information option** コマンドを使用します。option-82 情報の挿入および削除をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip dhcp snooping information option

no ip dhcp snooping information option

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトでは、option-82 情報の挿入および削除は実行されません。

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、DHCP スヌーピング機能をイネーブルにする必要があります（**feature dhcp** コマンドを参照）。

このコマンドには、ライセンスは不要です。

例

次に、DHCP パケットの opiton-82 情報の挿入および削除をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# ip dhcp snooping information option
switch(config)#
```

関連コマンド

コマンド	説明
ip dhcp relay information option	DHCP パケットの option-82 情報の挿入および削除をイネーブルにします。
ip dhcp snooping	デバイス上で DHCP スヌーピングをグローバルにイネーブルにします。
ip dhcp snooping trust	インターフェイスを、DHCP メッセージの信頼できる送信元として設定します。
ip dhcp snooping vlan	特定の VLAN 上で DHCP スヌーピングをイネーブルにします。
show ip dhcp snooping	DHCP スヌーピングの全般情報を表示します。
show running-config dhcp	IP ソース ガード設定を含む、DHCP スヌーピング設定を表示します。

ip dhcp snooping trust

インターフェイスを DHCP メッセージの信頼できる送信元として設定するには、**ip dhcp snooping trust** コマンドを使用します。インターフェイスを DHCP メッセージの信頼できない送信元として設定するには、このコマンドの **no** 形式を使用します。

ip dhcp snooping trust

no ip dhcp snooping trust

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトでは、DHCP メッセージの信頼できる送信元として設定されるインターフェイスはありません。

コマンド モード

インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、DHCP スヌーピング機能をイネーブルにする必要があります（**feature dhcp** コマンドを参照）。

DHCP メッセージの信頼できる送信元として設定できるのは、次のタイプのインターフェイスです。

- レイヤ 3 イーサネット インターフェイスおよびサブインターフェイス
- レイヤ 2 イーサネット インターフェイス
- プライベート VLAN インターフェイス

このコマンドには、ライセンスは不要です。

例

次に、インターフェイスを DHCP メッセージの信頼できる送信元として設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ip dhcp snooping trust
switch(config-if)#
```

関連コマンド

コマンド	説明
ip dhcp snooping	デバイス上で DHCP スヌーピングをグローバルにイネーブルにします。
ip dhcp snooping information option	DHCP リレー エージェントを使用しないで転送された DHCP パケットでの option-82 情報の挿入および削除をイネーブルにします。
ip dhcp snooping verify mac-address	MAC アドレス検証を、DHCP スヌーピングの一部としてイネーブルにします。
ip dhcp snooping vlan	特定の VLAN 上で DHCP スヌーピングをイネーブルにします。
show ip dhcp snooping	DHCP スヌーピングの全般情報を表示します。
show running-config dhcp	IP ソース ガード設定を含む、DHCP スヌーピング設定を表示します。

ip dhcp snooping verify mac-address

DHCP スヌーピングの MAC アドレス検証をイネーブルにするには、**ip dhcp snooping verify mac-address** コマンドを使用します。DHCP スヌーピングの MAC アドレス検証をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip dhcp snooping verify mac-address

no ip dhcp snooping verify mac-address

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、DHCP スヌーピングでの MAC アドレス検証はディセーブルです。

このコマンドを使用するには、DHCP スヌーピング機能をイネーブルにする必要があります（**feature dhcp** コマンドを参照）。

信頼できないインターフェイス上でパケットを受信し、パケットの送信元 MAC アドレスと DHCP クライアント ハードウェア アドレスが一致しない場合、そのパケットはアドレス検証によってドロップされます。

このコマンドには、ライセンスは不要です。

例

次に、DHCP スヌーピングの MAC アドレス検証をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# ip dhcp snooping verify mac-address
switch(config)#
```

関連コマンド

コマンド	説明
ip dhcp snooping	デバイス上で DHCP スヌーピングをグローバルにイネーブルにします。
ip dhcp snooping information option	DHCP リレー エージェントを使用しないで転送された DHCP パケットでの option-82 情報の挿入および削除をイネーブルにします。
ip dhcp snooping trust	インターフェイスを、DHCP メッセージの信頼できる送信元として設定します。
ip dhcp snooping vlan	特定の VLAN 上で DHCP スヌーピングをイネーブルにします。
service dhcp	DHCP リレー エージェントをイネーブルまたはディセーブルにします。
show ip dhcp snooping	DHCP スヌーピングの全般情報を表示します。
show running-config dhcp	IP ソース ガード設定を含む、DHCP スヌーピング設定を表示します。

ip dhcp snooping vlan

1 つまたは複数の VLAN 上で DHCP スヌーピングをイネーブルにするには、**ip dhcp snooping vlan** コマンドを使用します。1 つまたは複数の VLAN 上で DHCP スヌーピングをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip dhcp snooping vlan *vlan-list*

no ip dhcp snooping vlan *vlan-list*

シンタックスの説明

vlan-list	DHCP スヌーピングをイネーブルにする VLAN 範囲。*vlan-list* 引数には、単一 VLAN ID、VLAN ID 範囲、またはカンマで区切った ID と範囲を指定できます（例のセクションを参照）。有効な VLAN ID は、1 ～ 4096 です。

デフォルト

デフォルトでは、すべての VLAN 上で DHCP スヌーピングはディセーブルです。

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、DHCP スヌーピング機能をイネーブルにする必要があります（**feature dhcp** コマンドを参照）。

このコマンドには、ライセンスは不要です。

例

次に、VLAN 100、200、および 250 ～ 252 で DHCP スヌーピングをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# ip dhcp snooping vlan 100,200,250-252
switch(config)#
```

関連コマンド

コマンド	説明
ip dhcp snooping	デバイス上で DHCP スヌーピングをグローバルにイネーブルにします。
ip dhcp snooping information option	DHCP リレー エージェントを使用しないで転送された DHCP パケットでの option-82 情報の挿入および削除をイネーブルにします。
ip dhcp snooping trust	インターフェイスを、DHCP メッセージの信頼できる送信元として設定します。
ip dhcp snooping verify mac-address	MAC アドレス検証を、DHCP スヌーピングの一部としてイネーブルにします。
show ip dhcp snooping	DHCP スヌーピングの全般情報を表示します。
show running-config dhcp	IP ソース ガード設定を含む、DHCP スヌーピング設定を表示します。

ip port access-group

IPv4 Access Control List（ACL; アクセス コントロール リスト）をインターフェイスのポート ACL として適用するには、**ip port access-group** コマンドを使用します。インターフェイスから IPv4 ACL を削除するには、このコマンドの **no** 形式を使用します。

ip port access-group *access-list-name* **in**

no ip port access-group *access-list-name* **in**

シンタックスの説明

access-list-name	IPv4 ACL の名前。最大 64 文字で、大文字と小文字を区別した英数字で指定します。
in	ACL をインバウンド トラフィックに適用します。

デフォルト

in

コマンド モード

インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、インターフェイスに IPv4 ACL は適用されません。

ip port access-group コマンドを使用することにより、次のインターフェイス タイプに対して、IPv4 ACL をポート ACL として適用できます。

- レイヤ 2 イーサネット インターフェイス
- レイヤ 2 イーサネット ポートチャネル インターフェイス

また、**ip port access-group** コマンドを使用して、次のインターフェイス タイプにも、IPv4 ACL をポート ACL として適用できます。

- VLAN インターフェイス

（注） VLAN インターフェイスを設定する前に、VLAN インターフェイスをグローバルでイネーブルにする必要があります。詳細については、『*Cisco NX-OS Interfaces Command Reference*』の **feature interface-vlan** コマンドを参照してください。

- レイヤ 3 イーサネット インターフェイス
- レイヤ 3 イーサネット サブインターフェイス
- レイヤ 3 イーサネット ポートチャネル インターフェイスおよびサブインターフェイス
- トンネル
- ループバック インターフェイス
- 管理インターフェイス

ただし、**ip port access-group** コマンドを使用してレイヤ 3 インターフェイスに適用した ACL は、ポート モードをアクセスまたはトランク（レイヤ 2）モードに変更しない限り、アクティブになりません。IPv4 ACL をルータ ACL として適用するには、**ip access-group** コマンドを使用します。

IPv4 ACL を VLAN ACL として適用することもできます。詳細については、「match（VLAN アクセス マップ）」（p.191）を参照してください。

ポート ACL が適用されるのは、インバウンド トラフィックだけです。インバウンド パケットは、デバイス上で ACL のルールに対してチェックされます。最初の一致ルールによってパケットが許可されると、そのパケットは引き続き処理されます。最初の一致ルールによってパケットが拒否されると、そのパケットはドロップされ、ICMP ホスト到達不能メッセージが戻されます。

デバイスから特定の ACL を削除した場合、インターフェイスからその ACL を削除しなくても、削除した ACL はインターフェイス上のトラフィックには影響しません。

このコマンドには、ライセンスは不要です。

例

次に、イーサネット インターフェイス 2/1 に対して、ip-acl-01 という IPv4 ACL をポート ACL として適用する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# ip port access-group ip-acl-01 in
```

次に、イーサネット インターフェイス 2/1 から、ip-acl-01 という IPv4 ACL を削除する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# no ip port access-group ip-acl-01 in
```

関連コマンド

コマンド	説明
ip access-group	IPV4 ACL をルータ ACL としてインターフェイスに適用します。
ip access-list	IPv4 ACL を設定します。
show access-lists	すべての ACL を表示します。
show ip access-lists	特定の IPv4 ACL またはすべての IPv4 ACL を表示します。
show running-config interface	すべてのインターフェイスまたは特定のインターフェイスの実行コンフィギュレーションを表示します。
statistics per-entry	ACL の各エントリの統計情報の収集をイネーブルにします。

ip source binding

レイヤ 2 イーサネット インターフェイス用の固定 IP ソース エントリを作成するには、**ip source binding** コマンドを使用します。固定 IP ソース エントリをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip source binding *IP-address MAC-address* **vlan** *vlan-id* **interface ethernet** *slot/port*

no ip source binding *IP-address MAC-address* **vlan** *vlan-id* **interface ethernet** *slot/port*

シンタックスの説明

IP-address	特定のインターフェイス上で使用する IPv4 アドレス。有効なエントリは、ドット付き 10 進表記です。
MAC-address	特定のインターフェイス上で使用する MAC アドレス。有効なエントリは、ドット付き 16 進表記です。
vlan *vlan-id*	IP ソース エントリに関連付ける VLAN を指定します。
interface ethernet *slot/port*	固定 IP エントリに関連付けるレイヤ 2 イーサネット インターフェイスを指定します。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、固定 IP ソース エントリは作成されません。

このコマンドには、ライセンスは不要です。

例

次に、イーサネット インターフェイス 2/3 上に、VLAN 100 に関連付ける固定 IP ソース エントリを作成する例を示します。

```
switch# configure terminal
switch(config)# ip source binding 10.5.22.7 001f.28bd.0013 vlan 100 interface ethernet
2/3
switch(config)#
```

関連コマンド

コマンド	説明
ip verify source dhcp-snooping-vlan	インターフェイス上で IP ソース ガードをイネーブルにします。
show ip verify source	IP と MAC アドレスのバインディングを表示します。
show running-config dhcp	IP ソース ガード設定を含む、DHCP スヌーピング設定を表示します。

ip verify source dhcp-snooping-vlan

レイヤ 2 イーサネット インターフェイス上で IP ソース ガードをイネーブルにするには、**ip verify source dhcp-snooping-vlan** コマンドを使用します。インターフェイス上で IP ソース ガードをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip verify source dhcp-snooping-vlan

no ip verify source dhcp-snooping-vlan

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、すべてのインターフェイス上で IP ソース ガードはディセーブルです。

このコマンドには、ライセンスは不要です。

例

次に、インターフェイス上で IP ソース ガードをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# ip verify source dhcp-snooping-vlan
switch(config-if)#
```

関連コマンド

コマンド	説明
ip source binding	特定のイーサネット インターフェイス用の固定 IP ソース エントリを作成します。
show ip verify source	IP と MAC アドレスのバインディングを表示します。

ip verify unicast source reachable-via

インターフェイス上で Unicast Reverse Path Forwarding（ユニキャスト RPF）を設定するには、**ip verify unicast source reachable-via** コマンドを使用します。インターフェイスからユニキャスト RPF を削除するには、このコマンドの **no** 形式を使用します。

ip verify unicast source reachable-via {**any** [**allow-default**] | **rx**}

no ip verify unicast source reachable-via {**any** [**allow-default**] | **rx**}

シンタックスの説明

any	ルーズ チェックを指定します。
allow-default	（任意）特定のインターフェイス上で使用する MAC アドレスを指定します。
rx	ストリクト チェックを指定します。

デフォルト

なし

コマンド モード

インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

入力側インターフェイスで、次のユニキャスト RPF モードの 1 つを設定できます。

ストリクト ユニキャスト RPF モード ― ストリクト モード チェックは、次の一致が検出された場合に成功します。

- ユニキャスト RPF が、Forwarding Information Base（FIB; 転送情報ベース）でパケット送信元アドレスの一致を検出。
- パケットを受信した入力側インターフェイスが、FIB 一致のユニキャスト PRF インターフェイスの 1 つと一致。

これらのチェックに失敗すると、パケットは廃棄されます。このタイプのユニキャスト RPF チェックは、パケット フローが対称であると想定される場所で使用できます。

ルーズ ユニキャスト RPF モード ― ルーズ モード チェックは、FIB でのパケット送信元アドレスの検索が一致し、最低 1 つの実インターフェイスを経由して送信元に到達可能であるという FIB 結果が示された場合に成功します。パケットを受信した入力側インターフェイスが、FIB 結果のいずれかのインターフェイスと一致する必要はありません。

このコマンドには、ライセンスは不要です。

例

次に、インターフェイス上にルーズ ユニキャスト RPF チェックを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# ip verify unicast source reachable-via any
```

次に、インターフェイス上にストリクト ユニキャスト RPF チェックを設定する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/3
switch(config-if)# ip verify unicast source reachable-via rx
```

関連コマンド

コマンド	説明
show ip interface ethernet	インターフェイスの IP 関連情報を表示します。
show running-config interface ethernet	実行コンフィギュレーションのインターフェイス設定を表示します。
show running-config ip	実行コンフィギュレーションの IP 設定を表示します。
show startup-config interface ethernet	スタートアップ コンフィギュレーションのインターフェイス設定を表示します。
show startup-config ip	スタートアップ コンフィギュレーションの IP 設定を表示します。

K コマンド

この章では、K で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

key

キーを作成する、または既存キーのコンフィギュレーション モードを開始するには、**key** コマンドを使用します。キーを削除するには、このコマンドの **no** 形式を使用します。

key *key-ID*

no key *key-ID*

シンタックスの説明

key-ID	設定するキーの ID。ID は、0 ～ 65535 の整数を指定する必要があります。

デフォルト

なし

コマンド モード

キーチェーン コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

新しいキーにはキー ストリングは含まれていません。

このコマンドには、ライセンスは不要です。

例

次に、glbp-keys キーチェーンのキー 13 で、キー コンフィギュレーション モードを開始する例を示します。

```
switch# configure terminal
switch(config)# key chain glbp-keys
switch(config-keychain)# key 13
switch(config-keychain-key)#
```

関連コマンド

コマンド	説明
accept-lifetime	キーの許容ライフタイムを設定します。
key chain	キーチェーンを作成して、キーチェーン コンフィギュレーション モードを開始します。
key-string	特定のキーの共有秘密（テキスト）を設定します。
send-lifetime	キーの送信ライフタイムを設定します。
show key chain	キーチェーン設定を表示します。

key-string

キーのテキストを設定するには、**key-string** コマンドを使用します。テキストを削除するには、このコマンドの **no** 形式を使用します。

key-string [*encryption-type*] *text-string*

no key-string *text-string*

シンタックスの説明

encryption-type	（任意）使用する暗号化のタイプを指定します。*encryption-type* 引数に、次のいずれかの値を指定します。 • 0 — 暗号化されていないテキスト文字列を入力します。これがデフォルトです。 • 7 — 暗号化されたテキスト文字を入力します。暗号化方式は、シスコの独自方式です。このオプションは、別の NX-OS デバイス上で実行した **show key chain** コマンドの暗号化出力に基づいて、テキスト文字列を入力する場合に役立ちます。
text-string	キー ストリングのテキスト。最大 63 文字の大文字と小文字を区別した英数字で指定します。

デフォルト

なし

コマンド モード

キー コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

キー ストリングのテキストは、共有秘密です。キー ストリングは安全な形式で保管されます。

暗号化されたキー ストリングは、別の NX-OS デバイスで **show key chain** コマンドを実行することにより、取得できます。

このコマンドには、ライセンスは不要です。

例

次に、キー 13 の暗号化共有秘密を入力する例を示します。

```
switch# configure terminal
switch(config)# key chain glbp-keys
switch(config-keychain)# key 13
switch(config-keychain-key)# key-string 7
071a33595c1d0c1702170203163e3e21213c20361a021f11
switch(config-keychain-key)#
```

関連コマンド

コマンド	説明
accept-lifetime	キーの許容ライフタイムを設定します。
key	キーを設定します。
key chain	キーチェーンを設定します。
send-lifetime	キーの送信ライフタイムを設定します。
show key chain	キーチェーン設定を表示します。

key chain

キーチェーンを作成する、または既存のキーチェーンを設定するには、**key chain** コマンドを使用します。キーチェーンを削除するには、このコマンドの **no** 形式を使用します。

key chain *keychain-name*

no key chain *keychain-name*

シンタックスの説明

keychain-name	キーチェーンの名前。最大 63 文字の英数字で、大文字と小文字を区別して指定します。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

キーチェーンが存在しない場合は、このコマンドによりキーチェーンが作成されます。新しいキーチェーンにはキーは含まれていません。

キーチェーンを削除すると、そのキーチェーンに含まれているキーも削除されます。

キーチェーンを削除する前に、そのキーチェーンを使用する機能が存在しないことを確認してください。機能が使用するキーチェーンが削除された場合、その機能は他のデバイスと通信できなくなる可能性があります。

このコマンドには、ライセンスは不要です。

例

次に、glbp-keys というキーチェーンを設定する例を示します。

```
switch# configure terminal
switch(config)# key chain glbp-keys
switch(config-keychain)#
```

関連コマンド

コマンド	説明
accept-lifetime	キーの許容ライフタイムを設定します。
key	キーを設定します。
key-string	キー ストリングを設定します。
send-lifetime	キーの送信ライフタイムを設定します。
show key chain	キーチェーンの設定を表示します。

L コマンド

この章では、L で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

lt

IP ポート オブジェクト グループの less-than グループ メンバーを指定するには、**lt** コマンドを使用します。less-than グループ メンバーは、エントリに指定されたポート番号より小さいポート番号と一致します。ポート オブジェクト グループから less-than グループ メンバーを削除するには、このコマンドの **no** 形式を使用します。

[*sequence-number*] **lt** *port-number*

no {*sequence-number* | **lt** *port-number*}

シンタックスの説明

sequence-number	（任意）このグループ メンバーのシーケンス番号。シーケンス番号により、オブジェクト グループ内のグループ メンバーの順序を保持します。有効なシーケンス番号は、1 ～ 4294967295 です。シーケンス番号を指定しないと、現在のオブジェクト グループの最大シーケンス番号に 10 を加算した番号が割り当てられます。
port-number	このグループ メンバーと一致するトラフィックが、この番号以下となるポート番号。有効な値は、0 ～ 65535 です。

デフォルト

なし

コマンド モード

IP ポート オブジェクト グループ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

IP ポート オブジェクト グループには、方向は設定されません。**lt** コマンドを、送信元ポートと宛先ポートのどちらと一致させるか、またはインバウンドとアウトバウンドのどちらのトラフィックに適用するかは、ACL でのオブジェクト グループの使用方法によって異なります。

このコマンドには、ライセンスは不要です。

例

次に、port-group-05 という名前の IP ポート オブジェクト グループに、ポート 1 ～ 49151 で送受信されたトラフィックと一致させるグループ メンバーを設定する例を示します。

```
switch# config t
switch(config)# object-group ip port port-group-05
switch(config-port-ogroup)# lt 49152
```

関連コマンド

コマンド	説明
eq	IP ポート オブジェクト グループに equal-to グループ メンバーを指定します。
gt	IP ポート オブジェクト グループに greater-than グループ メンバーを指定します。
neq	IP ポート オブジェクト グループに not-equal-to グループ メンバーを指定します。
object-group ip port	IP ポート オブジェクト グループを設定します。
range	IP ポート オブジェクト グループに port-range グループ メンバーを指定します。
show object-group	オブジェクト グループを表示します。

M コマンド

この章では、M で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

mac access-list

Mac Access Control List（ACL; アクセス コントロール リスト）を作成するか、または特定の ACL の MAC アクセス リスト コンフィギュレーション モードを開始するには、**mac access-list** コマンドを使用します。MAC ACL を削除するには、このコマンドの **no** 形式を使用します。

mac access-list *access-list-name*

no mac access-list *access-list-name*

シンタックスの説明

access-list-name	MAC ACL の名前。最大 64 文字で、大文字と小文字を区別した英数字で指定します。スペースまたは引用符は使用できません。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、MAC ACL は定義されません。

非 IP トラフィックをフィルタリングするには、MAC ACL を使用します。パケットの分類をディセーブルにした場合は、MAC ACL を使用して、すべてのトラフィックをフィルタリングできます。

mac access-list コマンドを使用すると、MAC アクセス リスト コンフィギュレーション モードが開始されます。このモードで、MAC **deny** および **permit** コマンドを使用し、ACL のルールを設定します。指定した ACL が存在しない場合は、このコマンドの入力時に新しい ACL が作成されます。

ACL をインターフェイスに適用するには、**mac port access-group** コマンドを使用します。

すべての MAC ACL は、最終ルールとして、次の暗黙ルールが設定されます。

```
deny any any protocol
```

この暗黙のルールにより、トラフィックのレイヤ 2 ヘッダーに指定されたプロトコルに関係なく、一致しないトラフィックが確実に拒否されます。

MAC ACL の各ルールの統計情報を記録するには、**statistics per-entry** コマンドを使用します。暗黙ルールの統計情報は記録されません。暗黙ルールに一致したパケットの統計情報を記録するには、パケットの deny（拒否）ルールを明示的に設定する必要があります。

このコマンドには、ライセンスは不要です。

例

次に、mac-acl-01 という MAC ACL の MAC アクセス リスト コンフィギュレーション モードを開始する例を示します。

```
switch# conf t
switch(config)# mac access-list mac-acl-01
switch(config-acl)#
```

関連コマンド

コマンド	説明
deny（MAC）	MAC ACL に deny（拒否）ルールを設定します。
mac port access-group	MAC ACL をインターフェイスに適用します。
permit（MAC）	MAC ACL に permit（許可）ルールを設定します。
show mac access-lists	すべての MAC ACL または特定の MAC ACL を表示します。
statistics per-entry	ACL の各エントリの統計情報の収集をイネーブルにします。

mac port access-group

MAC Access Control List（ACL; アクセス コントロール リスト）をインターフェイスに適用するには、**mac port access-group** コマンドを使用します。インターフェイスから MAC ACL を削除するには、このコマンドの **no** 形式を使用します。

mac port access-group *access-list-name*

no mac port access-group *access-list-name*

シンタックスの説明

access-list-name	MAC ACL の名前。最大 64 文字で、大文字と小文字を区別した英数字で指定します。

デフォルト

なし

コマンド モード

インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、インターフェイスに MAC ACL は適用されません。

デバイス上にレイヤ 3 ヘッダーに基づくトラフィック分類が設定されていない場合を除き、MAC ACL は非 IP トラフィックに適用されます。パケット分類がディセーブルの場合は、MAC ACL がすべてのトラフィックに適用されます。

mac port access-group コマンドを使用することにより、次のインターフェイス タイプに対して、MAC ACL をポート ACL として適用できます。

- レイヤ 2 インターフェイス
- レイヤ 2 イーサネット ポートチャネル インターフェイス

MAC ACL を VLAN ACL として適用することもできます。詳細については、「match（VLAN アクセス マップ）」（p.191）を参照してください。

MAC ACL が適用されるのは、インバウンド トラフィックだけです。MAC ACL が適用されると、パケットが ACL のルールに対してチェックされます。最初の一致ルールによってパケットが許可されると、そのパケットは引き続き処理されます。最初の一致ルールによってパケットが拒否されると、そのパケットはドロップされ、ICMP ホスト到達不能メッセージが戻されます。

デバイスから特定の ACL を削除した場合、インターフェイスからその ACL を削除しなくても、削除した ACL はインターフェイス上のトラフィックには影響しません。

このコマンドには、ライセンスは不要です。

例

次に、イーサネット インターフェイス 2/1 に対して、mac-acl-01 という MAC ACL を適用する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# mac port access-group mac-acl-01
```

次に、イーサネット インターフェイス 2/1 から、mac-acl-01 という MAC ACL を削除する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# no mac port access-group mac-acl-01 in
```

関連コマンド

コマンド	説明
mac access-list	MAC ACL を設定します。
show access-lists	すべての ACL を表示します。
show mac access-lists	特定の MAC ACL またはすべての MAC ACL を表示します。
show running-config interface	すべてのインターフェイスまたは特定のインターフェイスの実行コンフィギュレーションを表示します。

match（VLAN アクセス マップ）

VLAN アクセス マップ内のトラフィック フィルタリング用として Access Control List（ACL; アクセス コントロール リスト）を指定するには、**match** コマンドを使用します。VLAN アクセス マップから **match** コマンドを削除するには、このコマンドの **no** 形式を使用します。

match {**ip | mac**} **address** *access-list-name*

no match {**ip | mac**} **address** *access-list-name*

シンタックスの説明

address *access-list-name*	ACL の名前。最大 64 文字で、大文字と小文字を区別した英数字で指定します。
ip	ACL が IPv4 ACL であることを指定します。
mac	ACL が MAC ACL であることを指定します。

デフォルト

なし

コマンド モード

VLAN アクセスマップ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

1 つのアクセス マップについて、1 つの **match** コマンドだけを指定できます。

デフォルトでは、デバイスによりトラフィックが分類され、IPv4 トラフィックには IPv4 ACL が、その他のすべてのトラフィックには MAC ACL が適用されます。

このコマンドには、ライセンスは不要です。

例

次に、vlan-map-01 という VLAN アクセス マップを作成し、このマップに ip-acl-01 という IPv4 ACL を割り当て、ACL と一致するパケットを転送し、マップと一致したトラフィックの統計情報を記録する例を示します。

```
switch# config t
switch(config)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-01
switch(config-access-map)# action forward
switch(config-access-map)# statistics per-entry
```

関連コマンド

コマンド	説明
action	VLAN アクセス マップ内のトラフィック フィルタリング用の処理を指定します。
show vlan access-map	すべての VLAN アクセス マップまたは 1 つの VLAN アクセス マップを表示します。
show vlan filter	VLAN アクセス マップの適用方法に関する情報を表示します。
vlan access-map	VLAN アクセス マップを設定します。
vlan filter	1 つ以上の VLAN に VLAN アクセス マップを適用します。

match（クラス マップ）

コントロール プレーン クラス マップの一致基準を設定するには、**match** コマンドを使用します。コントロール プレーン クラス マップの一致基準を削除するには、このコマンドの **no** 形式を使用します。

match access-group name *access-list*

match exception {[**ip** | **ipv6**] {**icmp** {**redirect** | **unreachable**} | **option**}}

match protocol arp

match redirect {**arp-inspect** | **dhcp-snoop**}

no match access-group name *access-list*

no match exception {[**ip** | **ipv6**] {**icmp** {**redirect** | **unreachable**} | **option**}}

no match protocol arp

no match redirect {**arp-inspect** | **dhcp-snoop**}

シンタックスの説明

access-group name *access-list*	IP ACL または MAC ACL と一致させます。
exception	例外パケットを一致させます。
ip	IPv4 例外パケットを一致させます。
ipv6	IPv6 例外パケットを一致させます。
icmp	IPv4 または IPv6 ICMP パケットを一致させます。
redirect	IPv4 または IPv6 ICMP リダイレクト パケットを一致させます。
unreachable	IPv4 または IPv6 ICMP 到達不能パケットを一致させます。
option	IPv4 または IPv6 ICMP オプション パケットを一致させます。
protocol arp	Address Resolution Protocol（ARP; アドレス解決プロトコル）パケットを一致させます。
redirect {**arp-inspect** | **dhcp-snoop**}	ダイナミック ARP インスペクションまたは DHCP スヌーピング リダイレクト パケットを一致させます。

デフォルト

なし

コマンド モード

クラス マップ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。
4.0(3)	ポリシング IPv6 パケットのサポートが追加されました。

使用上のガイドライン

このコマンドで ACL を指定するには、事前に IP ACL または MAC ACL を作成しておく必要があります。

このコマンドを使用できるのは、デフォルトの VDC だけです。

このコマンドには、ライセンスは不要です。

例

次に、コントロール プレーン クラス マップの一致基準を指定する例を示します。

```
switch# config t
switch(config)# class-map type control-plane ClassMapA
switch(config-pmap)# match exception ip icmp redirect
switch(config-pmap)# match redirect arp-inspect
```

次に、コントロール プレーン クラス マップの一致基準を削除する例を示します。

```
switch# config t
switch(config)# class-map type control-plane ClassMapA
switch(config-pmap)# no match exception ip icmp redirect
```

関連コマンド

コマンド	説明
class-map type control-plane	コントロール プレーン クラス マップを作成または指定して、クラス マップ コンフィギュレーション モードを開始します。
show class-map type control-plane	コントロール プレーン ポリシー マップの設定情報を表示します。

N コマンド

この章では、N で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

nac enable

インターフェイス上で Network Admission Control（NAC）をイネーブルにするには、**nac enable** コマンドを使用します。NAC をディセーブルにするには、このコマンドの **no** 形式を使用します。

nac enable

no nac enable

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト ディセーブル

コマンド モード インターフェイス コンフィギュレーション

サポートされるユーザ ロール network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン **nac enable** コマンドを使用する前に、**feature eou** コマンドを使用し、スイッチポート モードをアクセス モードに設定しておく必要があります。

EAPoUDP をイネーブルに設定できるのは、アクセス モード インターフェイスだけです。

このコマンドには、ライセンスは不要です。

例

次に、インターフェイス上で NAC をイネーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# switchport
switch(config-if)# switchport mode access
switch(config-if)# nac enable
```

次に、インターフェイス上で NAC をディセーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# no nac enable
```

関連コマンド

コマンド	説明
feature eou	EAPoUDP をイネーブルにします。
show eou	EAPoUDP 情報を表示します。

neq

IP ポート オブジェクト グループの not-equal-to グループ メンバーを指定するには、**neq** コマンドを使用します。ポート オブジェクト グループから not-equal-to グループ メンバーを削除するには、このコマンドの **no** 形式を使用します。

[*sequence-number*] **neq** *port-number*

no {*sequence-number* | **neq** *port-number*}

シンタックスの説明

sequence-number	（任意）このグループ メンバーのシーケンス番号。シーケンス番号により、オブジェクト グループ内のグループ メンバーの順序を保持します。有効なシーケンス番号は、1 ～ 4294967295 です。シーケンス番号を指定しないと、現在のオブジェクト グループの最大シーケンス番号に 10 を加算した番号が割り当てられます。
port-number	このグループ メンバーと一致させないポート番号。有効な値は、0 ～ 65535 です。

デフォルト

なし

コマンド モード

IP ポート オブジェクト グループ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

not-equal-to グループ メンバーは、エントリに指定されたポート番号とは異なるポート番号と一致します。

IP ポート オブジェクト グループには、方向は設定されません。**neq** コマンドを、送信元ポートと宛先ポートのどちらと一致させるか、またはインバウンドとアウトバウンドのどちらのトラフィックに適用するかは、ACL でのオブジェクト グループの使用方法によって異なります。

このコマンドには、ライセンスは不要です。

例

次に、port-group-05 という名前の IP ポート オブジェクト グループに、ポート 80 以外のポートに送信されたトラフィックと一致させるグループ メンバーを設定する例を示します。

```
switch# config t
switch(config)# object-group ip port port-group-05
switch(config-port-ogroup)# neq 80
```

関連コマンド

コマンド	説明
eq	IP ポート オブジェクト グループに equal-to グループ メンバーを指定します。
gt	IP ポート オブジェクト グループに greater-than グループ メンバーを指定します。
lt	IP ポート オブジェクト グループに less-than グループ メンバーを指定します。
object-group ip port	IP ポート オブジェクト グループを設定します。
range	IP ポート オブジェクト グループに port-range グループ メンバーを指定します。
show object-group	オブジェクト グループを表示します。

O コマンド

この章では、O で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

object-group（アイデンティティ ポリシー）

アイデンティティ ポリシー用の MAC Access Control List（ACL; アクセス コントロール リスト）を指定するには、**object-group** コマンドを使用します。アイデンティティ ポリシーから ACL を削除するには、このコマンドの **no** 形式を使用します。

object-group *acl-name*

no object-group *acl-name*

シンタックスの説明

acl-name	MAC ACL の名前。大文字と小文字を区別して、指定します。

デフォルト

なし

コマンド モード

アイデンティティ ポリシー コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin
VDC user

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

mac access-list コマンドでは、アイデンティティ ポリシーに割り当てる MAC ACL を作成します。

このコマンドには、ライセンスは不要です。

例

次に、アイデンティティ ポリシー用の ACL を設定する例を示します。

```
switch# config t
switch(config)# identity policy AdminPolicy
switch(config-id-policy)# object-group
```

次に、アイデンティティ ポリシーから ACL を削除する例を示します。

```
switch# config t
switch(config)# identity policy AdminPolicy
switch(config-id-policy)# no object-group
```

関連コマンド

コマンド	説明
identity policy	アイデンティティ ポリシーを作成または指定して、アイデンティティ ポリシー コンフィギュレーション モードを開始します。
mac access-list	MAC ACL を作成して、MAC ACL コンフィギュレーション モードを開始します。
show identity policy	アイデンティティ ポリシーの情報を表示します。

object-group ip address

IPv4 アドレス オブジェクト グループを定義する、または特定の IPv4 アドレス オブジェクト グループでオブジェクト グループ コンフィギュレーション モードを開始するには、**object-group ip address** コマンドを使用します。IPv4 アドレス オブジェクト グループを削除するには、このコマンドの **no** 形式を使用します。

object-group ip address *name*

no object-group ip address *name*

シンタックスの説明

name	IPv4 アドレス オブジェクト グループの名前。最大 64 文字で、大文字と小文字を区別した英数字で指定します。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

IPv4 オブジェクト グループは、Ipv4 Access Control List（ACL; アクセス コントロール リスト）の **permit** および **deny** コマンドで使用できます。

IP アドレス オブジェクト グループには、方向は設定されません。グループ メンバーを送信元または宛先のどちらのアドレスと一致させるか、またはオブジェクト グループをインバウンドまたはアウトバウンドのどちらのトラフィックに適用するかは、IPv4 ACL でのオブジェクト グループの使用方法によって異なります。

このコマンドには、ライセンスは不要です。

例

次に、ipv4-addr-group-13 という IPv4 アドレス オブジェクト グループを作成し、グループ メンバーとして 2 つの特定の IPv4 アドレスと、1 つのサブネット 10.23.176.0 を設定する例を示します。

```
switch# config t
switch(config)# object-group ip address ipv4-addr-group-13
switch(config-ipaddr-ogroup)# host 10.121.57.102
switch(config-ipaddr-ogroup)# 10.121.57.234/32
switch(config-ipaddr-ogroup)# 10.23.176.0 0.0.0.255
switch(config-ipaddr-ogroup)# show object-group ipv4-addr-group-13
        10 host 10.121.57.102
        20 host 10.121.57.234
        30 10.23.176.0/24
switch(config-ipaddr-ogroup)#
```

関連コマンド

コマンド	説明
host（IPv4）	IPv4 アドレス オブジェクト グループのグループ メンバーを設定します。
show object-group	オブジェクト グループを表示します。

object-group ip port

IP ポート オブジェクト グループを定義する、または特定の IP ポート オブジェクト グループでオブジェクト グループ コンフィギュレーション モードを開始するには、**object-group ip port** コマンドを使用します。IP ポート オブジェクト グループを削除するには、このコマンドの **no** 形式を使用します。

object-group ip port *name*

no object-group ip port *name*

シンタックスの説明

name	IP ポート オブジェクト グループの名前。最大 64 文字で、大文字と小文字を区別した英数字で指定します。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

IP ポート オブジェクト グループは、Ipv4 Access Control List（ACL; アクセス コントロール リスト）の **permit** および **deny** コマンドで使用できます。

IP ポート オブジェクト グループには、方向は設定されません。グループ メンバーを送信元または宛先のどちらのポートと一致させるか、またはオブジェクト グループをインバウンドまたはアウトバウンドのどちらのトラフィックに適用するかは、ACL でのオブジェクト グループの使用方法によって異なります。

このコマンドには、ライセンスは不要です。

例

次に、port-group-05 という名前の IP ポート オブジェクト グループを作成し、ポート 443 で送受信されたトラフィックと一致させるグループ メンバーを設定する例を示します。

```
switch# config t
switch(config)# object-group ip port port-group-05
switch(config-port-ogroup)# eq 443
switch(config-port-ogroup)# show object-group port-group-05
        10 eq 443
switch(config-port-ogroup)#
```

関連コマンド

コマンド	説明
eq	IP ポート オブジェクト グループに equal-to グループ メンバーを指定します。
gt	IP ポート オブジェクト グループに greater-than グループ メンバーを指定します。
lt	IP ポート オブジェクト グループに less-than グループ メンバーを指定します。
neq	IP ポート オブジェクト グループに not-equal-to グループ メンバーを指定します。
range	IP ポート オブジェクト グループに port-range グループ メンバーを指定します。
show object-group	オブジェクト グループを表示します。

object-group ipv6 address

IPv6 アドレス オブジェクト グループを定義する、または特定の IPv6 アドレス オブジェクト グループで IPv6 オブジェクト グループ コンフィギュレーション モードを開始するには、**object-group ipv6 address** コマンドを使用します。IPv6 アドレス オブジェクト グループを削除するには、このコマンドの **no** 形式を使用します。

object-group ipv6 address *name*

no object-group ipv6 address *name*

シンタックスの説明

name	IPv6 アドレス オブジェクト グループの名前。最大 64 文字で、大文字と小文字を区別した英数字で指定します。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは不要です。

例

次に、ipv6-addr-group-A7 という IPv6 アドレス オブジェクト グループを作成し、グループ メンバーとして 2 つの特定の IPv6 アドレスと、1 つのサブネット 2001:db8:0:3ab7:: を設定する例を示します。

```
switch# config t
switch(config)# object-group ipv6 address ipv6-addr-group-A7
switch(config-ipv6addr-ogroup)# host 2001:db8:0:3ab0::1
switch(config-ipv6addr-ogroup)# 2001:db8:0:3ab0::2/128
switch(config-ipv6addr-ogroup)# 2001:db8:0:3ab7::/96
switch(config-ipv6addr-ogroup)# show object-group ipv6-addr-group-A7
        10 host 2001:db8:0:3ab0::1
        20 host 2001:db8:0:3ab0::2
        30 2001:db8:0:3ab7::/96
switch(config-ipv6addr-ogroup)#
```

関連コマンド

コマンド	説明
host（IPv6）	IPv6 アドレス オブジェクト グループのグループ メンバーを設定します。
show object-group	オブジェクト グループを表示します。

P コマンド

この章では、P で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

password strength-check

パスワード長のチェックをイネーブルにするには、**password strength-check** コマンドを使用します。パスワード長のチェックをディセーブルにするには、このコマンドの **no** 形式を使用します。

password strength-check

no password strength-check

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト ディセーブル

コマンド モード グローバル コンフィギュレーション

サポートされるユーザ ロール network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(3)	このコマンドが導入されました。

使用上のガイドライン パスワード長のチェックをイネーブルにした場合、NX-OS ソフトウェアで作成できるのは強化パスワードだけです。強化パスワードの特性は、次のとおりです。

- 最低 8 文字の長さとする。
- 多数の連続文字（“abcd” など）は使用できない。
- 多数の重複文字（“aaabbb” など）は使用できない。
- 辞書に載っている単語は使用できない。
- 一般的な名前は使用できない。
- 大文字と小文字の両方を使用する。
- 数字を使用する。

次に、強化パスワードの例を示します。

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

このコマンドには、ライセンスは不要です。

例

次に、パスワード長のチェックをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# password strength-check
```

次に、パスワード長のチェックをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no password strength-check
```

関連コマンド

コマンド	説明
show password strength-check	パスワード長のチェックをイネーブルにします。
show running-config security	実行コンフィギュレーションのセキュリティ機能設定を表示します。

periodic

1 週間に 1 回以上アクティブにする時間範囲を指定するには、**periodic** コマンドを使用します。定期的な時間範囲を削除するには、このコマンドの **no** 形式を使用します。

[*sequence-number*] **periodic** *weekday time* **to** [*weekday*] *time*

no {*sequence-number* | **periodic** *weekday time* **to** [*weekday*] *time*}

[*sequence-number*] **periodic** *list-of-weekdays time* **to** *time*

no {*sequence-number* | **periodic** *list-of-weekdays time* **to** *time*}

シンタックスの説明

sequence-number	（任意）ルールのシーケンス番号。時間範囲内の該当番号の位置にコマンドが挿入されます。シーケンス番号により、時間範囲内のルールの順序が保持されます。 シーケンス番号は、1 ～ 4294967295 の任意の整数です。 デフォルトでは、時間範囲内の最初のルールにシーケンス番号 10 が割り当てられます。 シーケンス番号を指定しないと、時間範囲の最後にルールが追加され、1 つ前のルールのシーケンス番号に 10 を加算した値が、シーケンス番号として割り当てられます。 ルールのシーケンス番号を再割り当てするには、**resequence** コマンドを使用します。
weekday	範囲を開始または終了する曜日。この引数の最初の指定は、範囲を開始する曜日です。この引数の 2 番目の指定は、範囲を終了する曜日です。2 番目の指定を省略すると、範囲を終了する曜日は、範囲を開始する曜日と同じになります。 *weekday* 引数の有効値は、次のとおりです。 • ***monday*** • ***tuesday*** • ***wednesday*** • ***thursday*** • ***friday*** • ***saturday*** • ***sunday***
time	範囲を開始または終了する時刻この引数の最初の指定は、範囲を開始する時刻です。この引数の 2 番目の指定は、範囲を終了する時刻です。 *time* 引数は、24 時間表記で指定します。形式は、*hours*:*minutes* または *hours*:*minutes*:*seconds* です。たとえば、午前 8: 時は 8:00、午後 8 時は 20:00 になります。
to	*time* 引数の最初の指定と 2 番目の指定を区切ります。
list-of-weekdays	（任意）範囲を有効にする曜日。この引数の有効値は、次のとおりです。 • 曜日をスペースで区切って指定します。例： `monday thursday friday` • ***daily*** ― すべての曜日 • ***weekdays*** ― 月曜から金曜まで（Monday – Friday） • ***weekend*** ― 土曜と日曜（Saturday – Sunday）

デフォルト **to**

コマンド モード 時間範囲コンフィギュレーション

サポートされるユーザ ロール network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン このコマンドには、ライセンスは不要です。

例 次に、weekend-remote-access-times という時間範囲を作成し、土曜と日曜の午前 4 時から午後 10 時までの間、トラフィックを許可する定期ルールを設定する例を示します。

```
switch# config t
switch(config)# time-range weekend-remote-access-times
switch(config-time-range)# periodic weekend 04:00:00 to 22:00:00
```

次に、nwf-evening という時間範囲を作成し、月曜、水曜、金曜の午後 6 時から午後 10 時までの間、トラフィックを許可する定期ルールを設定する例を示します。

```
switch# config t
switch(config)# time-range mwf-evening
switch(config-time-range)# periodic monday wednesday friday 18:00:00 to 22:00:00
```

関連コマンド

コマンド	説明
absolute	絶対時間範囲のルールを設定します。
time-range	IPv4 ACL で使用できる時間範囲を設定します。

permit（ARP）

条件と一致する ARP トラフィックを許可する ARP ACL ルールを作成するには、**permit** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

基本シンタックス

[*sequence-number*] **permit ip** {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} **mac** {**any** | **host** *sender-MAC* | *sender-MAC sender-MAC-mask*} [**log**]

[*sequence-number*] **permit request ip** {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} **mac** {**any** | **host** *sender-MAC* | *sender-MAC sender-MAC-mask*} [**log**]

[*sequence-number*] **permit response ip** {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} {**any** | **host** *target-IP* | *target-IP target-IP-mask*} **mac** {**any** | **host** *sender-MAC* | *sender-MAC sender-MAC-mask*} [**any** | **host** *target-MAC* | *target-MAC target-MAC-mask*] [**log**]

no *sequence-number*

no permit ip {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} **mac** {**any** | **host** *sender-MAC* | *sender-MAC sender-MAC-mask*} [**log**]

no permit request ip {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} **mac** {**any** | **host** *sender-MAC* | *sender-MAC sender-MAC-mask*} [**log**]

no permit response ip {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} {**any** | **host** *target-IP* | *target-IP target-IP-mask*} **mac** {**any** | **host** *sender-MAC* | *sender-MAC sender-MAC-mask*} [**any** | **host** *target-MAC* | *target-MAC target-MAC-mask*] [**log**]

シンタックスの説明

sequence-number	（任意）**permit** コマンドのシーケンス番号。アクセス リストの該当番号の位置にコマンドが挿入されます。シーケンス番号により、ACL 内のルールの順序が保持されます。 シーケンス番号は、1 ～ 4294967295 の任意の整数です。 デフォルトでは、ACL 内の最初のルールにシーケンス番号 10 が割り当てられます。 シーケンス番号を指定しないと、ACL の最後にルールが追加され、1 つ前のルールのシーケンス番号に 10 を加算した値が、シーケンス番号として割り当てられます。 ルールのシーケンス番号を再割り当てするには、**resequence** コマンドを使用します。
ip	ルールの IP アドレス部分を指定します。
any	任意のホストが、ルールの ***any*** キーワードを含む部分と一致することを指定します。送信元 IP アドレス、宛先 IP アドレス、送信元 MAC アドレス、および宛先 MAC アドレスの指定に、***any*** を使用できます。
host *sender-IP*	ARP パケットの送信元 IP アドレスが *sender-IP* 引数の値と一致する場合にのみ、パケットを一致させるルールを指定します。*sender-IP* 引数の有効値は、ドット付き 10 進表記の IPv4 アドレスです。
sender-IP *sender-IP-mask*	パケットの送信元 IP アドレスと一致させる IPv4 アドレス セットの IPv4 アドレスおよびマスク。*sender-IP* および *sender-IP-mask* 引数は、ドット付き 10 進表記で指定する必要があります。*sender-IP-mask* 引数に 255.255.255.255 を指定すると、***host*** キーワードを使用した場合と同じ結果になります。
mac	ルールの MAC アドレス部分を指定します。

host *sender-MAC*	ARP パケットの送信元 MAC アドレスが *sender-MAC* 引数の値と一致する場合にのみ、パケットを一致させるルールを指定します。*sender-MAC* 引数の有効値は、ドット付き 16 進表記の MAC アドレスです。
sender-MAC *sender-MAC-mask*	パケットの送信元 MAC アドレスと一致させる MAC アドレス セットの MAC アドレスおよびマスク。*sender-MAC* および *sender-MAC-mask* 引数は、ドット付き 16 進表記で指定する必要があります。*sender-MAC-mask* 引数に ffff.ffff.ffff を指定すると、***host*** キーワードを使用した場合と同じ結果になります。
log	（任意）ルールと一致した ARP パケットのロギングを指定します。
request	（任意）ルールを、ARP 要求メッセージを含むパケットだけに適用します。 **（注）** ***request*** および ***response*** のキーワードを両方とも省略すると、ルールはすべての ARP メッセージに適用されます。
response	（任意）ルールを、ARP 応答メッセージを含むパケットだけに適用します。 **（注）** ***request*** および ***response*** のキーワードを両方とも省略すると、ルールはすべての ARP メッセージに適用されます。
host *target-IP*	ARP パケットの宛先 IP アドレスが *target-IP* 引数の値と一致する場合にのみ、パケットを一致させるルールを指定します。***host*** *target-IP* を指定できるのは、***response*** キーワードを使用する場合だけです。*target-IP* 引数の有効値は、ドット付き 10 進表記の IPv4 アドレスです。
target-IP *target-IP-mask*	パケットの宛先 IP アドレスと一致させる IPv4 アドレス セットの IPv4 アドレスおよびマスク。*target-IP target-IP-mask* を指定できるのは、***response*** キーワードを使用する場合だけです。*target-IP* および *target-IP-mask* 引数は、ドット付き 10 進表記で指定する必要があります。*target-IP-mask* 引数に 255.255.255.255 を指定すると、***host*** キーワードを使用した場合と同じ結果になります。
host *target-MAC*	ARP パケットの宛先 MAC アドレスが *target-MAC* 引数の値と一致する場合にのみ、パケットを一致させるルールを指定します。***host*** *target-MAC* を指定できるのは、***response*** キーワードを使用する場合だけです。*target-MAC* 引数の有効値は、ドット付き 16 進表記の MAC アドレスです。
target-MAC *target-MAC-mask*	パケットの宛先 MAC アドレスと一致させる MAC アドレス セットの MAC アドレスおよびマスク。*target-MAC target-MAC-mask* を指定できるのは、***response*** キーワードを使用する場合だけです。*target-MAC* および *target-MAC-mask* 引数は、ドット付き 16 進表記で指定する必要があります。*target-MAC-mask* 引数に ffff.ffff.ffff を指定すると、***host*** キーワードを使用した場合と同じ結果になります。

デフォルト

ip

コマンド モード

ARP ACL コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

新しく作成した ARP ACL には、ルールは含まれていません。

シーケンス番号を指定しないと、ACL の最後のルールのシーケンス番号に 10 を加算したシーケンス番号が割り当てられます。

パケットに ARP ACL が適用されると、ACL 内のすべてのルールに対してパケットが評価されます。パケットが条件に一致した最初のルールが施行されます。複数のルールの条件と一致する場合は、シーケンス番号が最も低いルールが施行されます。

response または ***request*** のキーワードをどちらも指定しないと、任意の ARP メッセージを含むパケットにルールが適用されます。

このコマンドには、ライセンスは不要です。

例

次に、arp-acl-o1 という ARP ACL の ARP アクセス リスト コンフィギュレーション モードを開始し、10.32.143.0 サブネット内の送信元 IP アドレスを含む ARP 要求メッセージを許可するルールを追加する例を示します。

```
switch# conf t
switch(config)# arp access-list arp-acl-01
switch(config-arp-acl)# permit request ip 10.32.143.0 255.255.255.0 mac any
```

関連コマンド

コマンド	説明
deny（ARP）	ARP ACL に拒否（deny）ルールを設定します。
arp access-list	ARP ACL を設定します。
ip arp inspection filter	ARP ACL を VLAN に適用します。
remark	ACL に備考を設定します。
show arp access-list	すべての ARP ACL または 1 つの ARP ACL を表示します。

permit（IPv4）

条件と一致するトラフィックを許可する IPv4 Access Control List（ACL; アクセス コントロール リスト）ルールを作成するには、**permit** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

基本シンタックス

[*sequence-number*] **permit** *protocol source destination* [**dscp** *dscp* | **precedence** *precedence*] [**fragments**] [**log**] [**time-range** *time-range-name*]

no permit *protocol source destination* [**dscp** *dscp* | **precedence** *precedence*] [**fragments**] [**log**] [**time-range** *time-range-name*]

no *sequence-number*

Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）

[*sequence-number*] **permit icmp** *source destination* [*icmp-message*] [**dscp** *dscp* | **precedence** *precedence*] [**fragments**] [**log**] [**time-range** *time-range-name*]

Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）

[*sequence-number*] **permit igmp** *source destination* [*igmp-message*] [**dscp** *dscp* | **precedence** *precedence*] [**fragments**] [**log**] [**time-range** *time-range-name*]

Internet Protocol v4（IPv4; インターネット プロトコル v4）

[*sequence-number*] **permit ip** *source destination* [**dscp** *dscp* | **precedence** *precedence*] [**fragments**] [**log**] [**time-range** *time-range-name*]

Transmission Control Protocol（TCP）

[*sequence-number*] **permit tcp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp* | **precedence** *precedence*] [**fragments**] [**log**] [**time-range** *time-range-name*] [*flags*] [**established**]

User Datagram Protocol（UDP; ユーザ データグラム プロトコル）

[*sequence-number*] **permit udp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp* | **precedence** *precedence*] [**fragments**] [**log**] [**time-range** *time-range-name*]

シンタックスの説明

sequence-number	（任意）**permit** コマンドのシーケンス番号。アクセス リストの該当番号の位置にコマンドが挿入されます。シーケンス番号により、ACL 内のルールの順序が保持されます。 シーケンス番号は、1 ～ 4294967295 の任意の整数です。 デフォルトでは、ACL 内の最初のルールにシーケンス番号 10 が割り当てられます。 シーケンス番号を指定しないと、ACL の最後にルールが追加され、1 つ前のルールのシーケンス番号に 10 を加算した値が、シーケンス番号として割り当てられます。 ルールのシーケンス番号を再割り当てするには、**resequence** コマンドを使用します。
protocol	ルールで一致させるパケットのプロトコルの名前または番号。有効値は 0 ～ 255 です。有効なプロトコル名は、次のキーワードです。 • ***icmp*** ― ルールを ICMP トラフィックだけに適用します。このキーワードを使用すると、*protocol* 引数のすべての有効値に使用できるキーワードに加え、*icmp-message* 引数を使用できます。 • ***igmp*** ― ルールを IGMP トラフィックだけに適用します。このキーワードを使用すると、***protocol*** 引数のすべての有効値に使用できるキーワードに加え、***igmp-type*** 引数を使用できます。 • ***ip*** ― ルールをすべての IPv4 トラフィックに適用します。このキーワードを使用する場合は、すべての IPv4 プロトコルに適用される他のキーワードおよび引数だけを使用できます。使用できるキーワードおよび引数は、次のとおりです。 　― ***dscp*** 　― ***fragments*** 　― ***log*** 　― ***precedence*** 　― ***time-range*** • ***tcp*** ― ルールを TCP トラフィックだけに適用します。このキーワードを使用すると、***protocol*** 引数のすべての有効値に使用できるキーワードに加え、***flags*** および ***operator*** 引数、***portgroup*** および ***established*** キーワードを使用できます。 • ***udp*** ― ルールを UDP トラフィックだけに適用します。このキーワードを使用すると、***protocol*** 引数のすべての有効値に使用できるキーワードに加え、***operator*** 引数および ***portgroup*** キーワードを使用できます。
source	ルールで一致させる送信元 IPv4 アドレス。この引数の指定方法の詳細については、「使用上のガイドライン」の「送信元および宛先」の説明を参照してください。
destination	ルールで一致させる宛先 IPv4 アドレス。この引数の指定方法の詳細については、「使用上のガイドライン」の「送信元および宛先」の説明を参照してください。

dscp *dscp*	（任意）IP ヘッダーの DSCP フィールドに特定の 6 ビット diffserv（ディファレンシエーテッド サービス）値が設定されているパケットだけを、ルールと一致させます。*dscp* 引数には、次の数値またはキーワードのいずれかを指定します。 • 0 ～ 63 ― DSCP フィールドの 6 ビットと同等の 10 進値。たとえば、10 を指定した場合、DSCP フィールドに次のビットが設定されているパケットだけがルールと一致します：001010. • ***af11*** ― Assured Forwarding（AF）クラス 1、低い廃棄確率（001010） • ***af12*** ― AF クラス 1、中程度の廃棄確率（001100） • ***af13*** ― AF クラス 1、高い廃棄確率（001110） • ***af21*** ― AF クラス 2、低い廃棄確率（010010） • ***af22*** ― AF クラス 2、中程度の廃棄確率（010100） • ***af23*** ― AF クラス 2、高い廃棄確率（010110） • ***af31*** ― AF クラス 3、低い廃棄確率（011010） • ***af32*** ― AF クラス 3、中程度の廃棄確率（011100） • ***af33*** ― AF クラス 3、高い廃棄確率（011110） • ***af41*** ― AF クラス 4、低い廃棄確率（100010） • ***af42*** ― AF クラス 4、中程度の廃棄確率（100100） • ***af43*** ― AF クラス 4、高い廃棄確率（100110） • ***cs1*** ― Class-selector（CS）1、優先順位 1（001000） • ***cs2*** ― CS2、優先順位 2（010000） • ***cs3*** ― CS3、優先順位 3（011000） • ***cs4*** ― CS4、優先順位 4（100000） • ***cs5*** ― CS5、優先順位 5（101000） • ***cs6*** ― CS6、優先順位 6（110000） • ***cs7*** ― CS7、優先順位 7（111000） • ***default*** ― デフォルトの DSCP 値（000000） • ***if*** ― 緊急フォワーディング（101110）
precedence *precedence*	（任意）*precedence* 引数で指定された値が IP Precedence フィールドに設定されているパケットだけを、ルールと一致させます。*precedence* 引数には、次の数値またはキーワードを指定します。 • 0 ～ 7 ― IP Precedence フィールドの 3 ビットと同等の 10 進値。たとえば、3 を指定した場合、IP Precedence フィールドに次のビットが設定されているパケットだけがルールと一致します：011 • ***critical*** ― Precedence 5（101） • ***flash*** ― Precedence 3（011） • ***flash-override*** ― Precedence 4（100） • ***immediate*** ― Precedence 2（010） • ***internet*** ― Precedence 6（110） • ***network*** ― Precedence 7（111） • ***priority*** ― Precedence 1（001） • ***routine*** ― Precedence 0（000）

fragments	（任意）最初のフラグメントではないパケットだけをルールと一致させます。このキーワードは、TCP ポート番号などのレイヤ 4 オプションを指定したルールには使用できません。これらのオプションを評価するために必要な情報は、最初のフラグメントだけに含まれているからです。
log	（任意）ルールと一致する各パケットについて、情報ロギング メッセージを生成します。メッセージには、次の情報が含まれます。 • ACL 名 • パケットの許可または拒否の結果 • プロトコルの内容（TCP、UDP、ICMP、または数値） • 送信元アドレスと宛先アドレス、および（該当する場合は）送信元ポート番号と宛先ポート番号
time-range *time-range-name*	（任意）このルールに適用する時間範囲を指定します。 時間範囲の指定には、**time-range** コマンドを使用します。
icmp-message	（ICMP のみ：（任意）ルールと一致させる ICMP メッセージのタイプ。この引数には、0 ～ 255 の整数、または「使用上のガイドライン」の「ICMP メッセージ タイプ」にリストされているキーワードの 1 つを指定します。
igmp-message	（IGMP のみ：（任意）ルールと一致させる IGMP メッセージのタイプ。*igmp-message* 引数には、0 ～ 15 の整数である IGMP メッセージ番号を指定します。また、次のいずれかのキーワードを指定できます。 • ***dvmrp*** ― Distance Vector Multicast Routing Protocol（DVMRP; ディスタンス ベクトル マルチキャスト ルーティング プロトコル） • ***host-query*** ― ホスト クエリー • ***host-report*** ― ホスト レポート • ***pim*** ― Protocol Independent Multicast（PIM） • ***trace*** ― マルチキャスト トレース
operator port [*port*]	（任意：TCP および UDP のみ）*operator* および *port* 引数の条件と一致する送信元ポートから送信されたパケット、または一致する宛先ポートに送信されたパケットだけを、ルールと一致させます。これらの引数が送信元ポートまたは宛先ポートのどちらに適用されるかは、*source* または *destination* のどちらの引数のあとに指定したかによって異なります。 *port* 引数には、TCP または UDP ポートの名前または番号を指定します。有効な値は 0 ～ 65535 の整数です。有効なポート名のリストは、「使用上のガイドライン」の「TCP ポート名」および「UDP ポート名」を参照してください。 2 番目の *port* 引数は、*operator* 引数が範囲である場合にのみ必要です。 *operator* 引数には、次のいずれかのキーワードを指定する必要があります。 • ***eq*** ― パケットのポートが *port* 引数と同等である場合にのみ一致します。 • ***gt*** ― パケットのポートが *port* 引数より大きい場合にのみ一致します。 • ***lt*** ― パケットのポートが *port* 引数より小さい場合にのみ一致します。 • ***neq*** ― パケットのポートが *port* 引数と同等ではない場合にのみ一致します。 • ***range*** ― 2 つの *port* 引数が必要です。パケットのポートが最初の *port* 引数以上で、2 番目の *port* 引数以下である場合にのみ一致します。

portgroup *portgroup*	（任意：TCP および UDP のみ）*portgroup* 引数で指定された IP ポート オブジェクト グループのメンバーである送信元ポートから送信されたパケット、またはメンバーである宛先ポートに送信されたパケットだけを、ルールと一致させます。IP ポート オブジェクト グループは、最大 64 文字の大文字と小文字を区別した名前です。IP ポート オブジェクト グループが送信元ポートまたは宛先ポートのどちらに適用されるかは、*source* または *destination* のどちらの引数のあとに指定したかによって異なります。 IP ポート オブジェクト グループを作成および変更するには、**object-group ip port** コマンドを使用します。
flags	（TCP のみ；任意）ルールと一致させる TCP 制御コントロール ビット フラグ。*flags* 引数には、次の 1 つ以上のキーワードを指定する必要があります。 • ***ack*** • ***fin*** • ***psh*** • ***rst*** • ***syn*** • ***urg***
established	（TCP のみ；任意）確立された TCP 接続に属すパケットだけを、ルールと一致させます。ACK または RST ビットが設定されている TCP パケットは、確立された接続に属しているとみなされます。

デフォルト

新しく作成した IPv4 ACL には、ルールは含まれていません。

シーケンス番号を指定しないと、ACL の最後のルールのシーケンス番号に 10 を加算したシーケンス番号が割り当てられます。

コマンド モード

IPv4 ACL コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

パケットに IPv4 ACL が適用されると、ACL 内のすべてのルールに対してパケットが評価されます。パケットが条件に一致した最初のルールが施行されます。複数のルールの条件と一致する場合は、シーケンス番号が最も低いルールが施行されます。

このコマンドには、ライセンスは不要です。

送信元および宛先

source および *destination* 引数は、次のいずれかの方法で指定できます。どのルールも、一方の引数の指定方法によって、他方の引数の指定方法が決まることはありません。ルールの設定時に使用できる *source* および *destination* 引数の指定方法は、次のとおりです。

- IP アドレス グループ オブジェクト ― IPv4 アドレス グループ オブジェクトを使用して、*source* または *destination* 引数を指定できます。IPv4 アドレス グループ オブジェクトを作成および変更するには、**object-group ip address** コマンドを使用します。シンタックスは、次のとおりです。

  addrgroup *address-group-name*

  次に、lab-gateway-svrs という名前の IPv4 アドレス オブジェクト グループを使用して *destination* 引数を指定する例を示します。

  ```
  switch(config-acl)# permit ip any addrgroup lab-gateway-svrs
  ```

- アドレスおよびネットワーク ワイルドカード ― IPv4 アドレスおよびネットワーク ワイルドカードを使用して、送信元または宛先とするホストまたはネットワークを指定できます。シンタックスは、次のとおりです。

  IPv4-address network-wildcard

  次に、192.168.67.0 サブネットの IPv4 アドレスおよびネットワーク ワイルドカードを使用して、*source* 引数を指定する例を示します。

  ```
  switch(config-acl)# permit tcp 192.168.67.0 0.0.0.255 any
  ```

- アドレスおよび Variable-Length Subnet Mask（VLSM; 可変長サブネット マスク）― IPv4 アドレスおよび VLSM を使用して、送信元または宛先とするホストまたはネットワークを指定できます。シンタックスは、次のとおりです。

  IPv4-address/prefix-len

  次に、192.168.67.0 サブネットの IPv4 アドレスおよび VLSM を使用して、*source* 引数を指定する例を示します。

  ```
  switch(config-acl)# permit udp 192.168.67.0/24 any
  ```

- ホスト アドレス ― ***host*** キーワードおよび IPv4 アドレスを使用して、送信元または宛先とするホストを指定できます。シンタックスは、次のとおりです。

  host *IPv4-address*

  このシンタックスは、*IPv4-address*/32 および *IPv4-address* 0.0.0.0 と同じです。

  次に、***host*** キーワードおよび 192.168.67.132 IPv4 アドレスを使用して、*source* 引数を指定する例を示します。

  ```
  switch(config-acl)# permit icmp host 192.168.67.132 any
  ```

- 任意のアドレス ― ***any*** キーワードを使用して、送信元または宛先として任意の IPv4 アドレスを指定できます。***any*** キーワードの使用例は、このセクションの例を参照してください。各例に、***any*** キーワードを使用した送信元または宛先の指定方法が示されています。

ICMP メッセージ タイプ

icmp-message 引数には、0 ～ 255 の整数である ICMP メッセージ番号を指定します。また、次のいずれかのキーワードを指定できます。

- ***administratively-prohibited*** ― 管理上の禁止
- ***alternate-address*** ― 代替アドレス
- ***conversion-error*** ― データグラム変換
- ***dod-host-prohibited*** ― ホスト禁止
- ***dod-net-prohibited*** ― ネット禁止
- ***echo*** ― エコー（ping）
- ***echo-reply*** ― エコー応答
- ***general-parameter-problem*** ― パラメータの問題
- ***host-isolated*** ― ホスト分離

- ***host-precedence-unreachable*** ― 優先順位のホスト到達不能
- ***host-redirect*** ― ホスト リダイレクト
- ***host-tos-redirect*** ― ToS ホスト リダイレクト
- ***host-tos-unreachable*** ― ToS ホスト到達不能
- ***host-unknown*** ― ホスト未知
- ***host-unreachable*** ― ホスト到達不能
- ***information-reply*** ― 情報応答
- ***information-request*** ― 情報要求
- ***mask-reply*** ― マスク応答
- ***mask-request*** ― マスク要求
- ***mobile-redirect*** ― モバイル ホスト リダイレクト
- ***net-redirect*** ― ネットワーク リダイレクト
- ***net-tos-redirect*** ― ToS ネット リダイレクト
- ***net-tos-unreachable*** ― ToS ネット到達不能
- ***net-unreachable*** ― ネット到達不能
- ***network-unknown*** ― ネットワーク未知
- ***no-room-for-option*** ― パラメータが必要だが空きなし
- ***option-missing*** ― パラメータが必要だが存在しない
- ***packet-too-big*** ― フラグメンテーションが必要、DF 設定
- ***parameter-problem*** ― すべてのパラメータの問題
- ***port-unreachable*** ― ポート到達不能
- ***precedence-unreachable*** ― 優先順位カットオフ
- ***protocol-unreachable*** ― プロトコル到達不能
- ***reassembly-timeout*** ― 再構成タイムアウト
- ***redirect*** ― すべてのリダイレクト
- ***router-advertisement*** ― ルータ ディスカバリ アドバタイズメント
- ***router-advertisement*** ― ルータ ディスカバリ アドバタイズメント
- ***source-quench*** ― 送信元抑制
- ***source-route-failed*** ― 送信元ルート障害
- ***time-exceeded*** ― すべてのタイム超過メッセージ
- ***timestamp-reply*** ― タイムスタンプ応答
- ***timestamp-request*** ― タイムスタンプ要求
- ***traceroute*** ― トレースルート
- ***ttl-exceeded*** ― TTL 超過
- ***unreachable*** ― すべての到達不能

TCP ポート名

protocol 引数に ***tcp*** を指定した場合、*port* 引数として 0 ～ 65535 の整数である TCP ポート番号を指定できます。また、次のいずれかのキーワードを指定できます。

bgp ― Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）（179）

chargen ― キャラクタ ジェネレータ（19）

cmd ― リモート コマンド（rcmd、514）

daytime ― デイタイム（13）

discard — 廃棄（9）

domain — Domain Name Service（DNS; ドメイン ネーム サービス）（53）

drip — Dynamic Routing Information Protocol（DRIP; ダイナミック ルーティング情報プロトコル）（3949）

echo — エコー（7）

exec — Exec（rsh、512）

finger — フィンガー（79）

ftp — File Transfer Protocol（FTP; ファイル転送プロトコル）（21）

ftp-data — FTP データ接続（2）

gopher — Gopher（7）

hostname — NIC ホストネーム サーバ（11）

ident — Ident プロトコル（113）

irc — Internet Relay Chat（IRC; インターネット リレー チャット）（194）

klogin — Kerberos ログイン（543）

kshell — Kerberos シェル（544）

login — ログイン（rlogin、513）

lpd — プリンタ サービス（515）

nntp — Network News Transport Protocol（NNTP）（119）

pim-auto-rp — PIM Auto-RP（496）

pop2 — Post Office Protocol v2（POP2）（19）

pop3 — Post Office Protocol v3（POP3）（11）

smtp — Simple Mail Transport Protocol（SMTP; シンプル メール転送プロトコル）（25）

sunrpc — Sun Remote Procedure Call（RPC; リモート プロシージャ コール）（111）

tacacs — TAC Access Control System（49）

talk — Talk（517）

telnet — Telnet（23）

time — Time（37）

uucp — UNIX-to-UNIX Copy Program（UUCP; UNIX 間コピー プログラム）（54）

whois — WHOIS/NICNAME（43）

www — World Wide Web（HTTP、8）

UDP ポート名

protocol 引数に ***udp*** を指定した場合、*port* 引数として 0 ～ 65535 の整数である UDP ポート番号を指定できます。また、次のいずれかのキーワードを指定できます。

biff — BIFF（メール通知、comsat、512）

bootpc — Bootstrap Protocol（BOOTP; ブートストラップ プロトコル）クライアント（68）

bootps ― Bootstrap Protocol（BOOTP; ブートストラップ プロトコル）サーバ（67）

discard ― 廃棄（9）

dnsix ― DNSIX セキュリティ プロトコル監査（195）

domain ― Domain Name Service（DNS; ドメイン ネーム サービス）（53）

echo ― エコー（7）

isakmp ― Internet Security Association and Key Management Protocol（ISAKMP）（5）

mobile-ip ― モバイル IP レジストレーション（434）

nameserver ― IEN116 ネーム サービス（旧式、42）

netbios-dgm ― NetBIOS データグラム サービス（138）

netbios-ns ― NetBIOS ネーム サービス（137）

netbios-ss ― NetBIOS セッション サービス（139）

non500-isakmp ― Internet Security Association and Key Management Protocol（ISAKMP）（45）

ntp ― Network Time Protocol（NTP; ネットワーク タイム プロトコル）（123）

pim-auto-rp ― PIM Auto-RP（496）

rip ― Routing Information Protocol（RIP）（ルータ、in.routed、52）

snmp ― Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）（161）

snmptrap ― SNMP トラップ（162）

sunrpc ― Sun Remote Procedure Call（RPC; リモート プロシージャ コール）（111）

syslog ― システム ロギング（514）

tacacs ― TAC Access Control System（49）

talk ― Talk（517）

tftp ― Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）（69）

time ― Time（37）

who ― Who サービス（rwho、513）

xdmcp ― X Display Manager Control Protocol（XDMCP）(177)

例

次に、acl-lab-01 という IPv4 ACL を作成し、10.23.0.0 および 192.168.37.0 ネットワークから 10.176.0.0 ネットワークへのすべての TCP および UDP トラフィックを許可するルールを設定する例を示します。

```
switch# config t
switch(config)# ip access-list acl-lab-01
switch(config-acl)# permit tcp 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# permit udp 10.23.0.0/16 10.176.0.0/16
switch(config-acl)# permit tcp 192.168.37.0/16 10.176.0.0/16
switch(config-acl)# permit udp 192.168.37.0/16 10.176.0.0/16
```

次に、acl-eng-to-marketing という IPv4 ACL を作成し、eng_workstations という IP アドレス オブジェクト グループから marketing_group という IP アドレス オブジェクト グループへのすべての IP トラフィックを許可するルールを設定する例を示します。

```
switch# config t
switch(config)# ip access-list acl-eng-to-marketing
switch(config-acl)# permit ip addrgroup eng_workstations addrgroup marketing_group
```

関連コマンド

コマンド	説明
deny（IPv4）	IPv4 ACL に拒否（deny）ルールを設定します。
ip access-list	IPv4 ACL を設定します。
object-group ip address	ＩＰv4 アドレス オブジェクト グループを設定します。
object-group ip port	IP ポート オブジェクト グループを設定します。
remark	ACL に備考を設定します。
show ip access-list	すべての IPv4 ACL または 1 つの IPv4 ACL を表示します。
statistics per-entry	ACL の各エントリの統計情報の収集をイネーブルにします。
time-range	時間範囲を設定します。

permit（MAC）

条件と一致するトラフィックを許可する MAC ACL ルールを作成するには、**permit** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

[*sequence-number*] **permit** *source destination* [*protocol*] [**cos** *cos-value*] [**vlan** *VLAN-ID*]

no permit *source destination* [*protocol*] [**cos** *cos-value*] [**vlan** *VLAN-ID*]

no *sequence-number*

シンタックスの説明

sequence-number	（任意）**permit** コマンドのシーケンス番号。アクセス リストの該当番号の位置にコマンドが挿入されます。シーケンス番号により、ACL 内のルールの順序が保持されます。 シーケンス番号は、1 ～ 4294967295 の任意の整数です。 デフォルトでは、ACL 内の最初のルールにシーケンス番号 10 が割り当てられます。 シーケンス番号を指定しないと、ACL の最後にルールが追加され、1 つ前のルールのシーケンス番号に 10 を加算した値が、シーケンス番号として割り当てられます。 ルールのシーケンス番号を再割り当てするには、**resequence** コマンドを使用します。
source	ルールで一致させる送信元 MAC アドレス。この引数の指定方法の詳細については、「使用上のガイドライン」の「送信元および宛先」の説明を参照してください。
destination	ルールで一致させる宛先 MAC アドレス。この引数の指定方法の詳細については、「使用上のガイドライン」の「送信元および宛先」の説明を参照してください。
protocol	（任意）ルールで一致させるプロトコルの番号。有効なプロトコル番号は 0x0 ～ 0xffff です。有効なプロトコル名のリストは、「使用上のガイドライン」の「MAC プロトコル」を参照してください。
***cos** cos-value*	（任意）IEEE 802.1Q ヘッダーに、*cos-value* 引数で指定した Class of Service（CoS; サービス クラス）値が含まれているパケットだけを一致させるルールを指定します。*cos-value* 引数は、0 ～ 7 の整数です。
***vlan** VLAN-ID*	（任意）IEEE 802.1Q ヘッダーに、指定した VLAN ID が含まれているパケットだけを一致させるルールを指定します。*VLAN-ID* 引数は、1 ～ 4094 の整数です。

デフォルト

なし

コマンド モード

MAC ACL コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン 新しく作成した MAC ACL には、ルールは含まれていません。

シーケンス番号を指定しないと、ACL の最後のルールのシーケンス番号に 10 を加算したシーケンス番号が割り当てられます。

パケットに MAC ACL が適用されると、ACL 内のすべてのルールに対してパケットが評価されます。パケットが条件に一致した最初のルールが施行されます。複数のルールの条件と一致する場合は、シーケンス番号が最も低いルールが施行されます。

このコマンドには、ライセンスは不要です。

送信元および宛先

source および *destination* 引数は、次のどちらかの方法で指定できます。どのルールも、一方の引数の指定方法によって、他方の引数の指定方法が決まることはありません。ルールの設定時に使用できる *source* および *destination* 引数の指定方法は、次のとおりです。

- アドレスおよびマスク ― MAC アドレスのあとにマスクを指定して、1 つのアドレスまたはアドレス グループを指定できます。シンタックスは、次のとおりです。

  MAC-address MAC-mask

  次に、*source* 引数に、MAC アドレス 00c0.4f03.0a72 を指定する例を示します。

  ```
  switch(config-acl)# permit 00c0.4f03.0a72 0000.0000.0000 any
  ```

  次に、*destination* 引数に、MAC ベンダー コードが 00603e のすべてのホストの MAC アドレスを指定する例を示します。

  ```
  switch(config-acl)# permit any 0060.3e00.0000 0000.0000.0000
  ```

- 任意のアドレス ― ***any*** キーワードを使用して、送信元または宛先として任意の MAC アドレスを指定できます。***any*** キーワードの使用例は、このセクションの例を参照してください。各例に、***any*** キーワードを使用した送信元または宛先の指定方法が示されています。

MAC プロトコル

protocol 引数には、MAC プロトコルの番号またはキーワードを指定します。プロトコル番号は、プレフィックスが 0x である 4 バイト 16 進値です。有効なプロトコル番号は 0x0 ～ 0xffff です。有効なキーワードは、次のとおりです。

- ***aarp*** ― Appletalk ARP（0x80f3）
- ***appletalk*** ― Appletalk（0x809b）
- ***decnet-iv*** ― DECnet Phase IV（0x6003）
- ***diagnostic*** ― DEC Diagnostic Protocol（0x6005）
- ***etype-6000*** ― Ethertype 0x6000（0x6000）
- ***etype-8042*** ― Ethertype 0x8042（0x8042）
- ***ip*** ― Internet Protocol v4（0x0800）
- ***lat*** ― DEC LAT（0x6004）
- ***lavc-sca*** ― DEC LAVC、SCA（0x6007）
- ***mop-console*** ― DEC MOP リモート コンソール（0x6002）
- ***mop-dump*** ― DEC MOP ダンプ（0x6001）
- ***vines-echo*** ― VINES エコー（0x0baf）

例

次に、mac-ip-filter という MAC ACL を作成し、2 つの MAC アドレス グループ間ですべての IPv4 トラフィックを許可するルールを設定する例を示します。

```
switch# config t
switch(config)# mac access-list mac-ip-filter
switch(config-mac-acl)# permit 00c0.4f00.0000 0000.00ff.ffff 0060.3e00.0000
0000.00ff.ffff ip
```

関連コマンド

コマンド	説明
deny（MAC）	MAC ACL に拒否（deny）ルールを設定します。
mac access-list	MAC ACL を設定します。
remark	ACL に備考を設定します。
statistics per-entry	ACL の各エントリの統計情報の収集をイネーブルにします。
show mac access-list	すべての MAC ACL または 1 つの MAC ACL を表示します。

permit（ロールベース アクセス コントロール リスト）

Security Group Access Control List（SGACL; セキュリティ グループ アクセス コントロール リスト）に許可ルールを設定するには、**permit** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

permit {**all** | **icmp** | **igmp** | **ip** | {{**tcp** | **udp**} [{**src** | **dest**} {{**eq** | **gt** | **lt** | **neq**} *port-number*} | **range** *port-number1 port-number2*}]}

no permit {**all** | **icmp** | **igmp** | **ip** | {{**tcp** | **udp**} [{**src** | **dest**} {{**eq** | **gt** | **lt** | **neq**} *port-number*} | **range** *port-number1 port-number2*}]}

シンタックスの説明

all	すべてのトラフィックを指定します。
icmp	Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）トラフィックを指定します。
igmp	Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）トラフィックを指定します。
ip	IP トラフィックを指定します。
tcp	TCP トラフィックを指定します。
udp	User Datagram Protocol（UDP; ユーザ データグラム プロトコル）トラフィックを指定します。
src	送信元ポート番号を指定します。
dest	宛先ポート番号を指定します。
eq	ポート番号と同等の番号を指定します。
gt	ポート番号より大きい番号を指定します。
lt	ポート番号より小さい番号を指定します。
neq	ポート番号と同等ではない番号を指定します。
port-number	TCP または UDP のポート番号。範囲は 0 ～ 65535 です。
range	TCP または UDP のポート範囲を指定します。
port-number1	範囲の開始ポート。範囲は 0 ～ 65535 です。
port-number2	範囲の終了ポート。範囲は 0 ～ 65535 です。

デフォルト

なし

コマンド モード

ロールベース アクセス コントロール リスト

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドには、アドバンスト サービス ライセンスが必要です。

例

次に、SGACL に許可ルールを追加する例を示します。

```
switch# config t
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)# permit icmp
```

次に、SGACL から許可ルールを削除する例を示します。

```
switch# config t
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)# no permit icmp
```

関連コマンド

コマンド	説明
cts role-based access-list	Cisco TrustSec SGACL を設定します。
deny（ロールベース アクセス コントロール リスト）	SGACL に拒否ルールを設定します。
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts role-based access-list	Cisco TrustSec SGACL の設定を表示します。

permit interface

ユーザ ロール インターフェイス ポリシーでインターフェイスを許可するには、**permit interface** コマンドを使用します。インターフェイスを拒否するには、このコマンドの **no** 形式を使用します。

permit interface {**ethernet** *slot*/*port*[**-** *port2*]| *interface-list*}

no permit interface

シンタックスの説明

ethernet *slot*/*port*	イーサネット インターフェイスの識別名
- *port*	モジュール上のインターフェイス範囲の最後のインターフェイスを指定します。
interface-list	イーサネット インターフェイスの識別名をカンマで区切ってリストします。

デフォルト

すべてのインターフェイス

コマンド モード

ユーザ ロール インターフェイス ポリシー コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

interface policy deny コマンドを使用すると、**permit interface** コマンドで許可したインターフェイスを除き、すべてのインターフェイスへのユーザ ロール アクセスが拒否されます。

このコマンドには、ライセンスは不要です。

例

次に、ユーザ ロール インターフェイス ポリシーでインターフェイス範囲を許可する例を示します。

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)# permit interface ethernet 2/1 - 8
```

次に、ユーザ ロール インターフェイス ポリシーでインターフェイスのリストを許可する例を示します。

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)# permit interface ethernet 1/1, ethernet 1/3, ethernet
1/5, ethernet 1/7
```

次に、ユーザ ロール インターフェイス ポリシーでインターフェイスを拒否する例を示します。

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)# no permit interface ethernet 2/1
```

関連コマンド

コマンド	説明
interface policy deny	ユーザ ロールのインターフェイス ポリシー コンフィギュレーション モードを開始します。
role name	ユーザ ロールを作成または指定して、ユーザ ロール コンフィギュレーション モードを開始します。
show role	ユーザ ロールの情報を表示します。

permit vlan

ユーザ ロール VLAN ポリシーで VLAN を許可するには、**permit vlan** コマンドを使用します。VLAN を削除するには、このコマンドの **no** 形式を使用します。

permit vlan {*vlan-id*[- *vlan-id2*] | *vlan-list*}

no permit vlan

シンタックスの説明

vlan-id	VLAN 識別番号。範囲は 1 ～ 3967 および 4048 ～ 4093 です。
- *vlan-id2*	範囲の最後の VLAN 識別番号を指定します。この VLAN 識別番号は、範囲の最初の VLAN 識別番号より大きい数値でなければなりません。
vlan-list	VLAN 識別番号をカンマで区切ってリストします。

デフォルト

すべての VLAN

コマンド モード

ユーザ ロール VLAN ポリシー コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

vlan policy deny コマンドを使用すると、**permit vlan** コマンドで許可した VLAN を除き、すべての VLAN へのユーザ ロール アクセスが拒否されます。

このコマンドには、ライセンスは不要です。

例

次に、ユーザ ロール VLAN ポリシーで VLAN 識別番号を許可する例を示します。

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)# permit vlan 8
```

次に、ユーザ ロール VLAN ポリシーで VLAN 識別番号の範囲を許可する例を示します。

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)# permit vlan 1-8
```

次に、ユーザ ロール VLAN ポリシーで VLAN 識別番号のリストを許可する例を示します。

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)# permit vlan 1, 10, 12, 20
```

次に、ユーザ ロール VLAN ポリシーから VLAN を削除する例を示します。

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)# no permit vlan 2
```

関連コマンド

コマンド	説明
vlan policy deny	ユーザ ロールの VLAN ポリシー コンフィギュレーション モードを開始します。
role name	ユーザ ロールを作成または指定して、ユーザ ロール コンフィギュレーション モードを開始します。
show role	ユーザ ロールの情報を表示します。

permit vrf

ユーザ ロール VRF ポリシーで、Virtual Routing and Forwarding（VRF）インスタンスを許可するには、**permit vrf** コマンドを使用します。VRF を削除するには、このコマンドの **no** 形式を使用します。

permit vrf *vrf-name*

no permit vrf *vrf-name*

シンタックスの説明

vrf-name	VRF の名前。大文字と小文字を区別して、指定します。

デフォルト

すべての VRF

コマンド モード

ユーザ ロール VRF ポリシー コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

vrf policy deny コマンドを使用すると、**permit vrf** コマンドで許可した VRF を除き、すべての VRF へのユーザ ロール アクセスが拒否されます。

ユーザ ロールで複数の VRF 名を許可するには、このコマンドを繰り返して設定します。

このコマンドには、ライセンスは不要です。

例

次に、ユーザ ロール VRF ポリシーで VRF 名を許可する例を示します。

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# vrf policy deny
switch(config-role-vrf)# permit vrf management
```

次に、ユーザ ロール VRF ポリシーから VRF 名を削除する例を示します。

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# vrf policy deny
switch(config-role-vrf)# no permit vrf engineering
```

関連コマンド

コマンド	説明
vrf policy deny	ユーザ ロールの VRF ポリシー コンフィギュレーション モードを開始します。
role name	ユーザ ロールを作成または指定して、ユーザ ロール コンフィギュレーション モードを開始します。
show role	ユーザ ロールの情報を表示します。

platform access-list update

Access Control List（ACL; アクセス コントロール リスト）の変更により、スーパーバイザ モジュールで I/O モジュールをアップデートする方法を設定するには、**platform access-list** コマンドを使用します。アトミック アップデートをディセーブルにするには、このコマンドの **no** 形式を使用します。

platform access-list update {**atomic** | **default-result permit**}

no platform access-list update {**atomic** | **default-result permit**}

シンタックスの説明

atomic	トラフィックを中断しないでアップデートを実行する、アトミック アップデートを指定します。NX-OS デバイスは、デフォルトでアトミック ACL アップデートを実行します。
default-result permit	非アトミック アップデートの実行中に、アップデートした ACL が適用されるトラフィックを許可します。

デフォルト

atomic

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

NX-OS デバイスは、デフォルトで、アップデートした ACL が適用されるトラフィックを中断しない、アトミック ACL アップデートを実行します。ただし、アトミック アップデートでは、アップデート対象の I/O モジュールに、変更する ACL の各アップデート エントリを保管できるだけの十分なリソースが必要になります。アップデートが完了すると、アップデートに使用された追加リソースは解放されます。I/O モジュールのリソースが不足している場合、エラー メッセージが表示され、I/O モジュールの ACL アップデートは失敗します。

I/O モジュールのリソースが不足している場合は、**no platform access-list update atomic** コマンドを使用して、アトミック アップデートをディセーブルにできます。ただし、ACL をアップデートして旧 ACL を削除するまでの短い処理時間中、ACL が適用されるトラフィックはデフォルトでドロップされます。

非アトミック アップデートの実行中に、アップデートした ACL が適用されるすべてのトラフィックを許可したい場合は、**platform access-list update default-result permit** コマンドを使用します。

このコマンドには、ライセンスは不要です。

例

次に、ACL のアトミック アップデートをディセーブルにする例を示します。

```
switch# config t
switch(config)# no platform access-list update atomic
```

次に、ACL の非アトミック アップデート中に、対象トラフィックが許可されるように設定する例を示します。

```
switch# config t
switch(config)# platform access-list update default-result permit
```

次に、再びアトミック アップデートが実行されるように設定する例を示します。

```
switch# config t
switch(config)# no access-list update default-result permit
switch(config)# platform access-list update atomic
```

関連コマンド

コマンド	説明
show running-config all	デフォルト設定を含む、実行コンフィギュレーションを表示します。

platform rate-limit

出力トラフィックのレート制限をパケット / 秒単位で設定するには、**platform rate-limit** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

platform rate-limit {**access-list-log** | **copy** | **layer-2** {**port-security** | **storm-control**} | **layer-3** {**control** | **glean** | **mtu** | **multicast** {**directly-connect** | **local-groups** | **rpf-leak**} | **ttl**} | **receive**} *packets*

no platform rate-limit {**access-list-log** | **copy** | **layer-2** {**port-security** | **storm-control**} | **layer-3** {**control** | **glean** | **mtu** | **multicast** {**directly-connect** | **local-groups** | **rpf-leak**} | **ttl**} | **receive**} [*packets*]

シンタックスの説明

access-list-log	アクセス リスト ロギングのためにスーパーバイザ モジュールにコピーされるパケットを指定します。デフォルトのレートは 100 パケット / 秒です。
copy	スーパーバイザ モジュールにコピーされるデータ パケットと制御パケットを指定します。デフォルトのレートは 30000 パケット / 秒です。
layer-2 storm-control	ストーム制御パケットを指定します。デフォルトのレートは 0 パケット / 秒です。
layer-2	レイヤ 1 パケットのレート制限を指定します。
port-security	ポート セキュリティ パケットを指定します。デフォルトはディセーブルです。
storm-control	ストーム制御パケットを指定します。デフォルトはディセーブルです。
layer-3	レイヤ 3 パケットを指定します。
control	レイヤ 3 制御パケットを指定します。デフォルトのレートは 10000 パケット / 秒です。
glean	レイヤ 3 グリーニング パケットを指定します。デフォルトのレートは 100 パケット / 秒です。
mtu	レイヤ 3 MTU 障害リダイレクト パケットを指定します。デフォルトのレートは 500 パケット / 秒です。
multicast	レイヤ 3 マルチキャスト パケット / 秒を指定します。
directly-connect	直接接続マルチキャスト パケットを指定します。デフォルトのレートは 10000 パケット / 秒です。
local-groups	ローカル グループ マルチキャスト パケットを指定します。デフォルトのレートは 10000 パケット / 秒です。
rpf-leak	Reverse Path Forwarding（RPF）リーク パケットを指定します。デフォルトのレートは 500 パケット / 秒です。
ttl	レイヤ 3 TTL 障害リダイレクト パケットを指定します。デフォルトのレートは 500 パケット / 秒です。
receive	スーパーバイザ モジュールにリダイレクトされるパケットを指定します。デフォルトのレートは 30000 パケット / 秒です。
packets	パケット数 / 秒。範囲は 1 ～ 33554431 です。

デフォルト

デフォルトのレート制限は、「シンタックスの説明」を参照してください。

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。
4.0(3)	**port-security** キーワードが追加されました。

使用上のガイドライン このコマンドには、ライセンスは不要です。

例

次に、制御パケットのレート制限を設定する例を示します。

```
switch# config t
switch(config)# platform rate-limit layer-3 control 20000
```

次に、制御パケットのレート制限をデフォルトの設定に戻す例を示します。

```
switch# config t
switch(config)# no platform rate-limit layer-3 control
```

関連コマンド

コマンド	説明
show running-config	実行コンフィギュレーションを表示します。

police

コントロール プレーン ポリシー マップのクラス マップにポリシングを設定するには、**police** コマンドを使用します。コントロール プレーン ポリシー マップのクラス マップからポリシングを削除するには、このコマンドの **no** 形式を使用します。

police [**cir**] *cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]

police [**cir**] *cir-rate* [**bps** | **gbps** | **kbps** | **mbps**] [**bc**] *burst-size* [**bytes** | **kbytes** | **mbytes** | **ms** | **packets** | **us**]

police [**cir**] *cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]
conform {**drop** | **set-cos-transmit** *cos-value* | **set-dscp-transmit** *dscp-value* | **set-prec-transmit** *prec-value* | **transmit**} [**exceed** {**drop** | **set dscp dscp table cir-markdown-map** | **transmit**}] [**violate** {**drop** | **set dscp dscp table pir-markdown-map** | **transmit**}]

police [**cir**] *cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]
pir *pir-rate* [**bps** | **gbps** | **kbps** | **mbps**] [[**be**] *extended-burst-size* [**bytes** | **kbytes** | **mbytes** | **ms** | **packets** | **us**]]

no police [**cir**] *cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]

n o police [**cir**] *cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**] [**bc**] *burst-size* [**bytes** | **kbytes** | **mbytes** | **ms** | **packets** | **us**]

no police [**cir**] *cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]
conform {**drop** | **set-cos-transmit** *cos-value* | **set-dscp-transmit** *dscp-value* | **set-prec-transmit** *prec-value* | **transmit**} [**exceed** {**drop** | **set dscp dscp table cir-markdown-map** | **transmit**}] [**violate** {**drop** | **set dscp dscp table pir-markdown-map** | **transmit**}]

no police [**cir**] *cir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**]
pir *pir-rate* [**bps** | **gbps** | **kbps** | **mbps** | **pps**] [[**be**] *extended-burst-size* [**bytes** | **kbytes** | **mbytes** | **ms** | **packets** | **us**]]

シンタックスの説明

cir	（任意）Commited Information Rate（CIR; 認定情報レート）を指定します。
cir-rate	CIR レート。範囲は 0 ～ 80000000000 です。
bps | **gbps** | **kbps** | **mbps** | **pps**	（任意）トラフィック レートの単位として、ビット / 秒、ギガビット / 秒、キロビット / 秒、メガビット / 秒、またはパケット / 秒を指定します。
bc	（任意）認定バーストのサイズを指定します。
burst-size	認定バーストのサイズ。範囲は 1 ～ 512000000 です。
bytes | **kbytes** | **mbytes** | **ms** | | **packets** | **us**	（任意）バーストの単位として、バイト、キロバイト、メガバイト、ミリ秒、パケット、またはマイクロ秒を指定します。
conform	トラフィックが指定のレートおよびバーストと一致したときの処理を設定します。
drop	ドロップ処理を指定します。
set-cos-transmit *cos-value*	Class of Service（CoS; サービス クラス）の値を設定します。範囲は 0 ～ 7 です。
set-dscp-transmit *dscp-value*	IPv4 および IPv6 パケットの Differentiated Services Code Point（DSCP; DiffServ コード ポイント）を指定します。範囲は 0 ～ 63 です。
set-prec-transmit *prec-value*	IPv4 および IPv6 パケットの優先順位の値を指定します。範囲は 0 ～ 7 です。
transmit	送信処理を指定します。
exceed	トラフィックが指定のレートおよびバーストを超過したときの処理を設定します。
set dscp dscp table cir-markdown-map	CIR マークダウン マップ上でパケットをフラグ付けします。

violate	（任意）トラフィックが指定のレートおよびバーストに違反したときの処理を設定します。
set dscp dscp table pir-markdown-map	PIR マークダウン マップ上でパケットをフラグ付けします。
pir *pir-rate*	PIR レートを指定します。
be	（任意）拡張バーストのサイズを指定します。
extended-burst-size	拡張バーストのサイズ。範囲は 1 ～ 512000000 です。

デフォルト

なし

コマンド モード

ポリシー マップ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用できるのは、デフォルトの VDC だけです。

このコマンドには、ライセンスは不要です。

例

次に、コントロール プレーン ポリシー マップを指定して、ポリシー マップ コンフィギュレーション モードを開始する例を示します。

```
switch# config t
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# class ClassMapA
switch(config-pmap-c)# police cir 2000 kbps
```

次に、コントロール プレーン ポリシー マップを削除する例を示します。

```
switch# config t
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# class ClassMapA
switch(config-pmap-c)# no police 2000 kbps
```

関連コマンド

コマンド	説明
class（ポリシー マップ）	コントロール プレーン ポリシー マップにコントロール プレーン クラス マップを指定して、ポリシー マップ クラス コンフィギュレーション モードを開始します。
show policy-map type control-plane	コントロール プレーン ポリシー マップの設定情報を表示します。

policy

Cisco TrustSec デバイス識別情報または Security Group Tag（SGT; セキュリティ グループ タグ）を使用して、インターフェイス上に Cisco TrustSec 認証ポリシーを手動で設定するには、**policy** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

policy {**dynamic identity** *device-id* | **static sgt** *sgt-value* [**trusted**]}

no policy {**dynamic** | **static**}

シンタックスの説明

dynamic identity	Cisco TrustSec デバイス識別情報を使用してダイナミック ポリシーを指定します。
device-id	Cisco TrustSec デバイス識別情報。デバイス識別情報は、大文字と小文字を区別して指定します。
static sgt	SGT を使用してスタティック ポリシーを指定します。
sgt-value	Cisco TrustSec SGT。形式は、**0x***hhhh* です。範囲は 0x1 ～ 0xfffd です。
trusted	（任意）インターフェイス上で受信したトラフィックに SGT が設定されている場合、タグを上書きしません。

デフォルト

なし

コマンド モード

Cisco TrustSec マニュアル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。
4.0(3)	コマンドの **no** 形式で、**dynamic** および **static** に続くキーワードとオプションが削除されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

設定を有効にするには、このコマンドの使用後に、**shutdown**/**no shutdown** コマンド シーケンスを使用して、インターフェイスをディセーブルにしてから、再びイネーブルにする必要があります。、

このコマンドには、アドバンスト サービス ライセンスが必要です。

例

次に、インターフェイスにダイナミック Cisco TrustSec ポリシーを手動で設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# cts manual
switch(config-if-cts-manual)# policy dynamic identity DeviceB
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

次に、手動で設定したダイナミック Cisco TrustSec ポリシーをインターフェイスから削除する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# cts manual
switch(config-if-cts-manual)# no policy dynamic identity DeviceB
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

次に、インターフェイスにスタティック Cisco TrustSec ポリシーを手動で設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/4
switch(config-if)# cts manual
switch(config-if-cts-manual)# policy static sgt 0x100
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

次に、手動で設定したスタティック Cisco TrustSec ポリシーをインターフェイスから削除する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/4
switch(config-if)# cts manual
switch(config-if-cts-manual)# no policy static sgt 0x100
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

関連コマンド

コマンド	説明
cts manual	インターフェイスの Cisco TrustSec マニュアル コンフィギュレーション モードを開始します。
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts interface	インターフェイスの Cisco TrustSec 設定を表示します。

policy-map type control-plane

コントロール プレーン ポリシー マップを作成または指定して、ポリシー マップ コンフィギュレーション モードを開始するには、**policy-map type control-plane** コマンドを使用します。コントロール プレーン ポリシー マップを削除するには、このコマンドの **no** 形式を使用します。

policy-map type control-plane *policy-map-name*

no policy-map type control-plane *policy-map-name*

シンタックスの説明

policy-map-name	ポリシー マップの名前。名前は、最大 64 文字で、大文字と小文字を区別した英数字で指定します。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用できるのは、デフォルトの VDC だけです。

このコマンドには、ライセンスは不要です。

例

次に、コントロール プレーン ポリシー マップを指定して、ポリシー マップ コンフィギュレーション モードを開始する例を示します。

```
switch# config t
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)#
```

次に、コントロール プレーン ポリシー マップを削除する例を示します。

```
switch# config t
switch(config)# no policy-map type control-plane PolicyMapA
```

関連コマンド

コマンド	説明
show policy-map type control-plane	コントロール プレーン ポリシー マップの設定情報を表示します。

propagate-sgt

レイヤ 2 Cisco TrustSec インターフェイス上で SGT 伝搬をイネーブルにするには、**propagate-sgt** コマンドを使用します。SGT 伝搬をディセーブルにするには、このコマンドの **no** 形式を使用します。

propagate-sgt

no propagate-sgt

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

イネーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(3)	このコマンドが導入されました。

使用上のガイドライン

インターフェイスに接続しているピア デバイスが SGT タグ付きの Cisco TrustSec パケットを処理できない場合には、インターフェイス上の SGT 伝搬機能をディセーブルに設定できます。

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

設定を有効にするには、このコマンドの使用後に、**shutdown**/**no shutdown** コマンド シーケンスを使用して、インターフェイスをディセーブルにしてから、再びイネーブルにする必要があります。、

このコマンドには、アドバンスト サービス ライセンスが必要です。

例

次に、SGT 伝搬をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# no propagate-sgt
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

次に、SGT 伝搬をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# propagate-sgt
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

関連コマンド

コマンド	説明
cts dot1x	インターフェイスの Cisco TrustSec 802.1X コンフィギュレーション モードを開始します。
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts interface	インターフェイスの Cisco TrustSec 設定を表示します。

R コマンド

この章では、R で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

radius-server deadtime

NX-OS デバイスにすべての RADIUS サーバのデッド タイム間隔を設定するには、**radius-server deadtime** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

radius-server deadtime *minutes*

no radius-server deadtime *minutes*

シンタックスの説明

minutes	デッド タイム間隔の分数。有効範囲は 1 ～ 1440 分です。

デフォルト

0 分

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

デッド タイム間隔は、NX-OS デバイスが応答のなかった RADIUS サーバを確認するまでの分数です。

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

このコマンドには、ライセンスは必要ありません。

例

次に、すべての RADIUS サーバの定期的なモニタリングを実行するグローバル デッド タイム間隔を設定する例を示します。

```
switch# config t
switch(config)# radius-server deadtime 5
```

次に、すべての RADIUS サーバのグローバル デッド タイム間隔をデフォルトに戻して、サーバの定期的なモニタリングをディセーブルにする例を示します。

```
switch# config t
switch(config)# no radius-server deadtime 5
```

関連コマンド

コマンド	説明
show radius-server	RADIUS サーバ情報を表示します。

radius-server directed-request

ログイン時にユーザが認証要求を特定の RADIUS サーバに送信できるようにするには、**radius-server directed-request** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

radius-server directed-request

no radius-server directed-request

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

設定した RADIUS サーバ グループに認証要求を送信します。

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

ログイン時、*username@vrfname*:*hostname* を指定できます。*vrfname* は、使用する Virtual Routing and Forwarding（VRF; VPN ルーティングおよび転送）インスタンスで、*hostname* は、設定した RADIUS サーバ名です。ユーザ名が認証用に RADIUS サーバに送信されます。

このコマンドには、ライセンスは必要ありません。

例

次に、ログイン時にユーザが認証要求を特定の RADIUS サーバに送信できるようにする例を示します。

```
switch# config t
switch(config)# radius-server directed-request
```

次に、ログイン時にユーザが認証要求を特定の RADIUS サーバに送信できないようにする例を示します。

```
switch# config t
switch(config)# no radius-server directed-request
```

関連コマンド

コマンド	説明
show radius-server directed-request	指定要求 RADIUS サーバ設定を表示します。

radius-server host

RADIUS サーバ パラメータを設定するには、**radius-server host** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

radius-server host {*hostname* | *ipv4-address* | *ipv6-address*}
[**key** [**0** | **7**] *shared-secret* [**pac**]] [**accounting**]
[**acct-port** *port-number*] [**auth-port** *port-number*] [**authentication**] [**retransmit** *count*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds* [**retransmit** *count*]]

no radius-server host {*hostname* | *ipv4-address* | *ipv6-address*}
[**key** [**0** | **7**] *shared-secret* [**pac**]] [**accounting**]
[**acct-port** *port-number*] [**auth-port** *port-number*] [**authentication**] [**retransmit** *count*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds* [**retransmit** *count*]]

シンタックスの説明

hostname	RADIUS サーバの Domain Name Server（DNS）名。名前は、英数字で指定します。大文字と小文字が区別され、最大文字数は 256 です。
ipv4-address	*A.B.C.D* フォーマットの RADIUS サーバの IPv4 アドレス
ipv6-address	*X*:*X*:*X*::*X* フォーマットの RADIUS サーバの IPv6 アドレス
key	（任意）RADIUS サーバ事前共有秘密鍵を設定します。
0	（任意）RADIUS クライアントとサーバ間の通信を認証する、クリア テキストで指定された事前共有鍵を設定します。これがデフォルトです。
7	（任意）RADIUS クライアントとサーバ間の通信を認証する、暗号文で指定された事前共有鍵（7 で表示）を設定します。
shared-secret	RADIUS クライアントとサーバ間の通信を認証する事前共有鍵。事前共有鍵には、出力可能な ASCII 文字の使用が可能です（空白文字は使用できません）。大文字と小文字が区別され、長さは 63 文字に制限されています。
pac	（任意）Cisco TrustSec と連動させるために、RADIUS Cisco Access Control Server（ACS）で Protected Access Credentials（PAC）の生成をイネーブルにします。
accounting	（任意）アカウンティングを設定します。
acct-port *port-number*	（任意）アカウンティング用の RADIUS サーバのポートを設定します。範囲は 0 ～ 65535 です。
auth-port *port-number*	（任意）認証用の RADIUS サーバのポートを設定します。範囲は 0 ～ 65535 です。
authentication	（任意）認証を設定します。
retransmit *count*	（任意）デバイスがローカル認証に戻る前に RADIUS サーバ（複数可）への接続試行を行う回数を設定します。有効範囲は 1 ～ 5 回で、デフォルトは 1 回です。
test	（任意）テスト パケットを RADIUS サーバに送信するようにパラメータを設定します。
idle-time *time*	サーバをモニタリングするための時間間隔を分で指定します。範囲は 1 ～ 1440 分です。
password *password*	テスト パケット内のユーザ パスワードを指定します。パスワードは、英数字で指定します。大文字と小文字が区別され、最大文字数は 32 です。
username *name*	テスト パケット内のユーザ名を指定します。ユーザ名は、英数字で指定します。大文字と小文字の区別がなく、最大文字数は 32 です。
timeout *seconds*	RADIUS サーバへの再送信タイムアウト（秒単位）を設定します。デフォルトは 5 秒で、有効な範囲は 1 ～ 60 秒です。

デフォルト

アカウンティング ポート：1813

認証ポート：1812

アカウンティング：イネーブル

認証：イネーブル

再送信数：1

アイドル時間：なし

サーバのモニタリング：ディセーブル

タイムアウト：5 秒

テスト ユーザ名：test

テスト パスワード：test

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

アイドル タイム インターバルが 0 分の場合、RADIUS サーバの定期的なモニタリングは実行されません。

このコマンドには、ライセンスは必要ありません。

例

次に、RADIUS サーバの認証とアカウンティングのパラメータを設定する例を示します。

```
switch# config terminal
switch(config)# radius-server host 10.10.2.3 key HostKey
switch(config)# radius-server host 10.10.2.3 auth-port 2003
switch(config)# radius-server host 10.10.2.3 acct-port 2004
switch(config)# radius-server host 10.10.2.3 accounting
switch(config)# radius-server host radius2 key 0 abcd
switch(config)# radius-server host radius3 key 7 1234
switch(config)# radius-server host 10.10.2.3 test idle-time 10
switch(config)# radius-server host 10.10.2.3 test username tester
switch(config)# radius-server host 10.10.2.3 test password 2B9ka5
```

関連コマンド

コマンド	説明
show radius-server	RADIUS サーバ情報を表示します。

radius-server key

RADIUS 共有秘密鍵を設定するには、**radius-server key** コマンドを使用します。設定した共有秘密鍵を削除するには、このコマンドの **no** 形式を使用します。

radius-server key [**0** | **7**] *shared-secret*

no radius-server key [**0** | **7**] *shared-secret*

シンタックスの説明

0	（任意）RADIUS クライアントとサーバ間の通信を認証する、クリア テキストで指定された事前共有鍵を設定します。
7	（任意）RADIUS クライアントとサーバ間の通信を認証する、暗号文で指定された事前共有鍵を設定します。
shared-secret	RADIUS クライアントとサーバ間の通信を認証するのに使用される事前共有鍵。事前共有鍵には、出力可能な ASCII 文字の使用が可能です（空白文字は使用できません）。大文字と小文字が区別され、長さは 63 文字に制限されています。

デフォルト

クリア テキスト

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

RADIUS 事前共有鍵を設定して、RADIUS サーバに対してスイッチを認証する必要があります。鍵の長さは 63 文字に制限されており、出力可能な ASCII 文字の使用が可能です（空白文字は使用できません）。グローバル鍵は、スイッチにあるすべての RADIUS サーバ コンフィギュレーションで使用するよう設定できます。**radius-server host** コマンドで **key** キーワードを使用することでこのグローバル鍵の割り当てを上書きできます。

このコマンドには、ライセンスは必要ありません。

例

次に、RADIUS 認証を設定する各種のシナリオを提供する例を示します。

```
switch# config terminal
switch(config)# radius-server key AnyWord
switch(config)# radius-server key 0 AnyWord
switch(config)# radius-server key 7 public pac
```

関連コマンド

コマンド	説明
show radius-server	RADIUS サーバ情報を表示します。

radius-server retransmit

デバイスが RADIUS サーバで要求を試行する回数を指定するには、**radius-server retransmit** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

radius-server retransmit *count*

no radius-server retransmit *count*

シンタックスの説明

count	デバイスがローカル認証に戻る前に RADIUS サーバ（複数可）への接続試行を行う回数。有効範囲は 1 ～ 5 回です。

デフォルト

再送信 1 回

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、RADIUS サーバに再送信回数を設定する例を示します。

```
switch# config t
switch(config)# radius-server retransmit 3
```

次に、RADIUS サーバに再送信のデフォルト数を設定する例を示します。

```
switch# config t
switch(config)# no radius-server retransmit 3
```

関連コマンド

コマンド	説明
show radius-server	RADIUS サーバ情報を表示します。

radius-server timeout

RADIUS サーバへの再送信間隔を指定するには、**radius-server timeout** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

radius-server timeout *seconds*

no radius-server timeout *seconds*

シンタックスの説明

seconds	RADIUS サーバへの再送信間隔の秒数。有効範囲は 1 ～ 60 秒です。

デフォルト

1 秒

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、タイムアウト間隔を設定する例を示します。

```
switch# config t
switch(config)# radius-server timeout 30
```

次に、デフォルトの間隔に戻す例を示します。

```
switch# config t
switch(config)# no radius-server timeout 30
```

関連コマンド

コマンド	説明
show radius-server	RADIUS サーバ情報を表示します。

range

IP ポート オブジェクト グループにグループ メンバーとしてポートの範囲を指定するには、**range** コマンドを使用します。ポート オブジェクト グループからポート範囲のグループ メンバーを削除するには、このコマンドの **no** 形式を使用します。

[*sequence-number*] **range** *starting-port-number ending-port-number*

no {*sequence-number* | **range** *starting-port-number ending-port-number*}

シンタックスの説明

sequence-number	（任意）このグループ メンバーのシーケンス番号。シーケンス番号は、オブジェクト グループ内でグループ メンバーの順序を保ちます。有効なシーケンス番号は 1 ～ 4294967295 です。シーケンス番号を指定しない場合、デバイスは最大シーケンス番号より 10 大きい番号を現在のオブジェクト グループに割り当てます。
starting-port-number	このグループ メンバーに一致する最小ポート番号。有効値は、0 ～ 65535 です。
ending-port-number	このグループ メンバーに一致する最大ポート番号。有効値は、0 ～ 65535 です。

デフォルト

なし

コマンド モード

IP ポート オブジェクト グループ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

IP ポート オブジェクト グループには方向性がありません。**range** コマンドが送信元ポートまたは宛先ポートに一致するかどうか、または着信または発信トラフィックに適用するかどうかは、ACL 内のオブジェクト グループの使用方法によって異なります。

このコマンドには、ライセンスは必要ありません。

例

次に、ポート 137 ～ 139 間で送信されるトラフィックに一致するグループ メンバーで port-group-05 という名前の IP ポート オブジェクト グループを設定する例を示します。

```
switch# config t
switch(config)# object-group ip port port-group-05
switch(config-port-ogroup)# range 137 139
```

関連コマンド

コマンド	説明
eq	IP ポート オブジェクト グループに eq（等しい）グループ メンバーを指定します。
gt	IP ポート オブジェクト グループに gt（より大きい）グループ メンバーを指定します。
lt	IP ポート オブジェクト グループに lt（より小さい）グループ メンバーを指定します。
neq	IP ポート オブジェクト グループに neq（等しくない）グループ メンバーを指定します。
object-group ip port	IP ポート オブジェクト グループを設定します。
show object-group	オブジェクト グループを表示します。

remark

IPv4 または MAC Access Control List（ACL; アクセス コントロール リスト）にコメントを入力するには、**remark** コマンドを使用します。**remark** コマンドを削除するには、このコマンドの **no** 形式を使用します。

[*sequence-number*] **remark** *remark*

no {*sequence-number* | **remark** *remark*}

シンタックスの説明

sequence-number	（任意）**remark** コマンドのシーケンス番号。これにより、デバイスはアクセス リストの番号が指定された位置にコマンドを挿入します。シーケンス番号は、ACL 内でルールの順序を保ちます。 シーケンス番号には、1 ～ 4294967295 間の整数を指定できます。 デフォルトでは、ACL の最初のルールには、10 のシーケンス番号が与えられます。 シーケンス番号を指定しない場合、デバイスは ACL の最後にルールを追加し、前のルールのシーケンス番号より 10 大きいシーケンス番号を割り当てます。 **resequence** コマンドを使用して、シーケンス番号をリマークとルールに再度割り当てます。
remark	リマークのテキスト。この引数は、最大で 100 文字の英数字を使用でき、大文字と小文字が区別されます。

デフォルト

デフォルトでは、ACL にリマークが含まれません。

コマンド モード

IP アクセスリスト コンフィギュレーション
MAC アクセスリスト コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

remark 引数には、最大 100 文字を指定できます。*remark* 引数に 100 より多い文字を入力すると、デバイスは最初の 100 文字を受け入れ、それ以上の文字を廃棄します。

例

次に、IPv4 ACL にリマークを作成して、結果を表示する例を示します。

```
switch# config t
switch(config)# ip access-list acl-ipv4-01
switch(config-acl)# 100 remark this ACL denies the marketing department access to the
lab
switch(config-acl)# show access-list acl-ipv4-01

IP access list acl-ipv4-01
        100 remark this ACL denies the marketing department access to the lab
ciscobox(config-acl)#
```

関連コマンド

コマンド	説明
ip access-list	IPv4 ACL を設定します。
mac access-list	MAC ACL を設定します。
show access-list	すべての ACL または 1 つの ACL を表示します。
statistics per-entry	ACL の各エントリの統計情報の収集をイネーブルにします。

replay-protection

インターフェイス上の Cisco TrustSec 認証のデータパス リプレイ保護機能をイネーブルにするには、**replay-protection** コマンドを使用します。データパス レプレイ保護機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

replay-protection

no replay-protection

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

イネーブル

コマンド モード

Cisco TrustSec 802.1X コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドを使用したあと、**shutdown**/**no shutdown** コマンド シーケンスを使用してインターフェイスをイネーブルおよびディセーブルにして、設定を有効にする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、インターフェイス上の Cisco TrustSec 認証のデータパス保護をイネーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# replay-protection
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

次に、インターフェイス上の Cisco TrustSec 認証のデータパス保護をディセーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# no replay-protection
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

関連コマンド

コマンド	説明
cts dot1x	インターフェイスの Cisco TrustSec 802.1X コンフィギュレーション モードを開始します。
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts interface	インターフェイスの Cisco TrustSec 設定を表示します。

resequence

Access Control List（ACL; アクセス コントロール リスト）のすべてのルールまたは時間の範囲にシーケンス番号を再度割り当てるには、**resequence** コマンドを使用します。

resequence *access-list-type* **access-list** *access-list-name starting-sequence-number increment*

resequence time-range *time-range-name starting-sequence-number increment*

シンタックスの説明

access-list-type	ACL のタイプ。この引数の有効値は、次のキーワードです。 • ***arp*** • ***ip*** • ***mac***
access-list *access-list-name*	ACL の名前を指定します。名前では最大で 64 文字の英数字を使用でき、大文字と小文字が区別されます。
time-range *time-range-name*	時間の範囲の名前を指定します。名前では最大で 64 文字の英数字を使用でき、大文字と小文字が区別されます。
starting-sequence-number	ACL の最初のルールまたは時間の範囲のシーケンス番号
increment	デバイスが後続の各シーケンス番号に追加する数

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

resequence コマンドを使用すると、ACL のルールまたは時間の範囲にシーケンス番号を再度割り当てることができます。最初のルールの新しいシーケンス番号は、*starting-sequence-number* 引数によって決まります。その他の各ルールは、*increment* 引数によって決まる新しいシーケンス番号を受け取ります。最大シーケンス番号がシーケンス番号の許容最大値を超えると、シーケンスが実行されず、次のメッセージが表示されます。

```
ERROR: Exceeded maximum sequence number.
```

最大シーケンス番号は、4294967295 です。

このコマンドには、ライセンスは必要ありません。

例

次に、**show ip access-lists** コマンドを使用して、100 のシーケンス番号で開始し、10 ずつ増える ip-acl-01 という名前の IPv4 ACL のシーケンスを再度実行し、**resequence** コマンドの使用の前後のシーケンス番号を確認する例を示します。

```
switch# config t
switch(config)# show ip access-lists ip-acl-01

IP access list ip-acl-01
        7 permit tcp addrgroup lab-machines any
        10 permit udp addrgroup lab-machines any
        13 permit icmp addrgroup lab-machines any
        17 deny igmp any any
switch(config)# resequence ip access-list ip-acl-01 100 10
switch(config)# show ip access-lists ip-acl-01

IP access list ip-acl-01
        100 permit tcp addrgroup lab-machines any
        110 permit udp addrgroup lab-machines any
        120 permit icmp addrgroup lab-machines any
        130 deny igmp any any
```

関連コマンド

コマンド	説明
arp access-list	ARP ACL を設定します。
ip access-list	IPv4 ACL を設定します。
mac access-list	MAC ACL を設定します。
show access-lists	すべての ACL または特定の ACL を表示します。

role feature-group name

ユーザ ロール機能グループを作成または指定し、ユーザ ロール機能グループ コンフィギュレーション モードを開始するには、**role feature-group name** コマンドを使用します。ユーザ ロール機能グループを削除するには、このコマンドの **no** 形式を使用します。

role feature-group name *group-name*

no role feature-group name *group-name*

シンタックスの説明

group-name	ユーザ ロール機能グループ名。*group-name* の最大文字数は 32 で、大文字と小文字が区別され、英数字文字列で指定します。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

NX-OS ソフトウェアは、レイヤ 3 機能のデフォルト ユーザ ロール機能グループを備えています。L3 ユーザ ロール機能グループを変更または削除できません。

このコマンドには、ライセンスは必要ありません。

例

次に、ユーザ ロール機能グループを作成して、ユーザ ロール機能グループ コンフィギュレーション モードを開始する例を示します。

```
switch# config t
switch(config)# role feature-group name MyGroup
switch(config-role-featuregrp)#
```

次に、ユーザ ロール機能グループを削除する例を示します。

```
switch# config t
switch(config)# no role feature-group name MyGroup
```

関連コマンド

コマンド	説明
feature-group name	ユーザ ロール機能グループを指定または作成して、ユーザ ロール機能グループ コンフィギュレーション モードを開始します。
show role feature-group	ユーザ ロール機能グループを表示します。

role name

ユーザ ロールを作成または指定し、ユーザ ロール コンフィギュレーション モードを開始するには、**role name** コマンドを使用します。ユーザ ロールを削除するには、このコマンドの **no** 形式を使用します。

role name *role-name*

no role name *role-name*

シンタックスの説明

role-name	ユーザ ロール名。*role-name* の最大文字数は 16 で、大文字と小文字が区別され、英数字文字列で指定します。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

NX-OS ソフトウェアは、4 つのデフォルト ユーザ ロールを備えています。

- network-admin ― NX-OS デバイス全体に対する読み取り / 書き込みアクセスを実行できます（デフォルト DVC でのみ使用可能）
- network-operator ― NX-OS デバイス全体に対する読み取りアクセスを実行できます（デフォルト DVC でのみ使用可能）
- vdc-admin ― VDC に限定した読み取り / 書き込みアクセス
- vdc-operator ― VDC に限定した読み取りアクセス

デフォルトのユーザ ロールは変更または削除できません。

このコマンドには、ライセンスは必要ありません。

例

次に、ユーザ ロールを作成して、ユーザ ロール コンフィギュレーション モードを開始する例を示します。

```
switch# config t
switch(config)# role MyRole
switch(config-role)#
```

次に、ユーザ ロールを削除する例を示します。

```
switch# config t
switch(config)# no role name MyRole
```

関連コマンド

コマンド	説明
show role	ユーザ ロールを表示します。

rule

ユーザ ロールのルールを設定するには、**rule** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

rule *number* {**deny** | **permit**} {**command** *command-string* | {**read** | **read-write**} [**feature** *feature-name* | **feature-group** *group-name*]}

no rule *number*

シンタックスの説明

number	ルールのシーケンス番号。NX-OS ソフトウェアは、最初に最大値を使用してルールを適用し、それ以降は降順で適用されます。有効範囲は 1 ～ 256 です。
deny	コマンドまたは機能へのアクセスを拒否します。
permit	コマンドまたは機能へのアクセスを許可します。
command *command-string*	コマンド ストリングを指定します。
read	読み取りアクセスを指定します。
read-write	読み取り / 書き込みアクセスを指定します。
feature *feature-name*	（任意）機能名を指定します。NX-OS 機能名を表示するには、**show role feature** コマンドを使用します。
feature-group *group-name*	（任意）機能グループを指定します。

デフォルト

なし

コマンド モード

ユーザ ロール コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

各ロールに最大 256 のルールを設定できます。

指定するルール番号は、適用したルールの順序を決めます。ルールは降順で適用されます。たとえば、1 つのロールに 3 つのルールがある場合は、ルール 3、ルール 2、ルール 1 の順に適用されます。

このコマンドには、ライセンスは必要ありません。

例

次に、ユーザ ロールにルールを追加する例を示します。

```
switch# config t
switch(config)# role MyRole
switch(config-role)# rule 1 deny command clear users
switch(config-role)# rule 1 permit read-write feature-group L3
```

次に、ユーザ ロールからルールを削除する例を示します。

```
switch# config t
switch(config)# role MyRole
switch(config-role)# no rule 10
```

関連コマンド

コマンド	説明
role name	ユーザ ロール名を作成または指定して、ユーザ ロール コンフィギュレーション モードを開始します。
show role	ユーザ ロールを表示します。

S コマンド

この章では、**show** コマンドを除く S で始まる Cisco NX-OS セキュリティ コマンドについて説明します（show コマンドは、「show コマンド」で説明します）。

sap pmk

Cisco TrustSec Security Association Protocol（SAP）の Pairwise Master Key（PMK）を手動で設定するには、**sap** コマンドを使用します。SAP 設定を削除するには、このコマンドの **no** 形式を使用します。

sap pmk [*key* | **use-dot1x**} [**modelist** {**gcm-encrypt** | **gmac** | **no-encap** | **none**}]

no sap

シンタックスの説明

key	鍵の値。この値は、偶数で構成される 16 進文字列です。最大 32 文字まで指定可能です。
use-dot1x	ピア デバイスが Cisco TrustSec 802.1X 認証または許可をサポートしていないが、SAP データ パス暗号化と認証をサポートしていることを指定します。
modelist	（任意）SAP 動作モードを指定します。
gcm-encrypt	Galois/Counter Mode（GCM）暗号化と認証モードを指定します。
gmac	GCM 認証モードを指定します。
no-encap	暗号化および Security Group Tag（SGT）を挿入しないことを指定します。
none	認証または暗号化なしの SGT のカプセル化を指定します。

デフォルト

gcm-encrypt

コマンド モード

Cisco TrustSec 手動コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(3)	**use-dot1x** キーワードが追加されました。
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドを使用したあと、**shutdown/no shutdown** コマンド シーケンスを使用してインターフェイスをイネーブルおよびディセーブルにして、設定を有効にする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、インターフェイスに Cisco TrustSec SAP を手動で設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# cts manual
switch(config-if-cts-manual)# sap pmk fedbaa modelist gmac
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

次に、インターフェイスから Cisco TrustSec SAP 設定を手動で削除する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# cts manual
switch(config-if-cts-manual)# no sap
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

関連コマンド

コマンド	説明
cts manual	インターフェイスの Cisco TrustSec 手動コンフィギュレーション モードを開始します。
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts interface	インターフェイスの Cisco TrustSec 設定を表示します。

sap modelist

Cisco TrustSec Security Association Protocol（SAP）の動作モードを設定するには、**sap modelist** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

sap modelist {**gcm-encrypt** | **gmac** | **no-encap** | **none**}

no sap modelist {**gcm-encrypt** | **gmac** | **no-encap** | **none**}

シンタックスの説明

gcm-encrypt	Galois/Counter Mode（GCM）暗号化と認証モードを指定します。
gmac	GCM 認証モードを指定します。
no-encap	暗号化および Security Group Tag（SGT）を挿入しないことを指定します。
none	認証または暗号化なしの SGT のカプセル化を指定します。

デフォルト

gcm-encrypt

コマンド モード

Cisco TrustSec 802.1X コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドを使用したあと、**shutdown**/**no shutdown** コマンド シーケンスを使用してインターフェイスをイネーブルおよびディセーブルにして、設定を有効にする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、インターフェイスに Cisco TrustSec SAP 動作モードを設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# sap modelist gmac
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

次に、インターフェイスのデフォルトの Cisco TrustSec SAP 動作モードに戻す例を示します。

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# no sap modelist gmac
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

関連コマンド

コマンド	説明
cts dot1x	インターフェイスの Cisco TrustSec 802.1X コンフィギュレーション モードを開始します。
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts interface	インターフェイスの Cisco TrustSec 設定を表示します。

send-lifetime

デバイスが別のデバイスとの鍵の交換時に鍵を送信する時間間隔を指定するには、**send-lifetime** コマンドを使用します。時間間隔を削除するには、このコマンドの **no** 形式を使用します。

send-lifetime [**local**] *start-time* [**duration** *duration-value* **| infinite |** *end-time*]

シンタックスの説明

local	（任意）デバイスがローカル時間として設定された時間を扱うことを指定します。デフォルトでは、デバイスは UTC として *start-time* および *end-time* 引数を扱います。
start-time	鍵がアクティブになる時刻および日付 *start-time* 引数の値の詳細については、「使用上のガイドライン」を参照してください。
duration *duration-value*	（任意）ライフタイムの長さを秒単位で指定します。最大の長さは、2147483646 秒です（約 68 年）。
infinite	（任意）鍵が期限切れにならないように指定します。
end-time	（任意）鍵が非アクティブになる時刻および日付 *end-time* 引数の有効値の詳細については、「使用上のガイドライン」を参照してください。

デフォルト

infinite

コマンド モード

鍵コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

デフォルトでは、デバイスはすべての時間範囲のルールを UTC として扱います。

デフォルトでは、デバイスが別のデバイスとの鍵の交換時に鍵を送信する時間間隔（送信ライフタイム）は、infinite です。つまり、鍵は期限切れになりません。

start-time および *end-time* 引数の両方には、次のフォーマットの時間と日付のコンポーネントが必要です。

hour[:*minute*[:*second*]] *month day year*

24 時間表記で指定します。たとえば、24 時間表記では、8:00 a.m. は 8:00 で、8:00 p.m. は 20:00 です。最小の有効な *start-time* 値は 00:00:00 Jan 1 1970 で、最大の有効な *start-time* 値は 23:59:59 Dec 31 2037 です。

例

次に、2008 年 6 月 13 日の午前零時に開始し、2008 年 8 月 12 日の 11:59:59 p.m. に終了する送信ライフタイムを作成する例を示します。

```
switch# configure terminal
switch(config)# key chain glbp-keys
switch(config-keychain)# key 13
switch(config-keychain-key)# send-lifetime 00:00:00 Jun 13 2008 23:59:59 Aug 12 2008
switch(config-keychain-key)#
```

関連コマンド

コマンド	説明
accept-lifetime	鍵の受け入れライフタイムを設定します。
key	鍵を設定します。
key chain	キーチェーンを設定します。
key-string	鍵のストリングを設定します。
show key chain	キーチェーンの設定を表示します。

server

RADIUS または TACACS+ サーバ グループにサーバを追加するには、**server** コマンドを使用します。サーバ グループからサーバを削除するには、このコマンドの **no** 形式を使用します。

server {*ipv4-address* | *ipv6-address* | *hostname*}

no server {*ipv4-address* | *ipv6-address* | *hostname*}

シンタックスの説明

ipv4-address	*A.B.C.D* フォーマットのサーバの IPv4 アドレス
ipv6-address	*X:X:X::X* フォーマットのサーバの IPv6 アドレス
hostname	サーバ名。名前は、英数字で指定します。大文字と小文字が区別され、最大文字数は 256 です。

デフォルト

なし

コマンド モード

RADlUS サーバ グループ コンフィギュレーション
TACACS+ サーバ グループ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

サーバ グループには、最大 64 のサーバを設定できます。

RADIUS サーバ グループ コンフィギュレーション モードを開始するには、**aaa group server radius** コマンドを使用します。TACACS+ サーバ グループ コンフィギュレーション モードを開始するには、**aaa group server tacacs+** コマンドを使用します。

サーバを検索できなかった場合、**radius-server host** コマンドまたは **tacacs-server host** コマンドを使用してサーバを設定します。

（注） TACACS+ を設定する前に、**feature tacacs+** コマンドを使用する必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、RADIUS サーバ グループにサーバを追加する例を示します。

```
switch# config t
switch(config)# aaa group server radius RadServer
switch(config-radius)# server 10.10.1.1
```

次に、RADIUS サーバ グループからサーバを削除する例を示します。

```
switch# config t
switch(config)# aaa group server radius RadServer
switch(config-radius)# no server 10.10.1.1
```

次に、TACACS+ サーバ グループにサーバを追加する例を示します。

```
switch# config t
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# server 10.10.2.2
```

次に、TACACS+ サーバ グループからサーバを削除する例を示します。

```
switch# config t
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# no server 10.10.2.2
```

関連コマンド

コマンド	説明
aaa group server	AAA サーバ グループを設定します。
radius-server host	RADIUS サーバを設定します。
show radius-server groups	RADIUS サーバ グループ情報を表示します。
show tacacs-server groups	TACACS+ サーバ グループ情報を表示します。
feature tacacs+	TACACS+ をイネーブルにします。
tacacs-server host	TACACS+ サーバを設定します。

service dhcp

DHCP リレー エージェントをイネーブルにするには、**service dhcp** コマンドを使用します。DHCP リレー エージェントをディセーブルにするには、このコマンドの **no** 形式を使用します。

service dhcp

no service dhcp

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、DHCP スヌーピングをグローバルにイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# service dhcp
switch(config)#
```

関連コマンド

コマンド	説明
feature dhcp	デバイスの DHCP スヌーピング機能をイネーブルにします。
ip dhcp relay address	インターフェイスの DHCP サーバの IP アドレスを設定します。
ip dhcp relay information option	DHCP パケットの option-82 情報の挿入および削除をイネーブルにします。
ip dhcp snooping	デバイスの DHCP スヌーピングをグローバルにイネーブルにします。
show ip dhcp snooping	DHCP スヌーピングの一般情報を表示します。
show running-config dhcp	IP ソース ガード設定を含めて、DHCP スヌーピング設定を表示します。

service-policy input

コントロール プレーンにコントロール プレーン ポリシー マップを付加するには、**service-policy input** コマンドを使用します。コントロール プレーン ポリシー マップを削除するには、このコマンドの **no** 形式を使用します。

service-policy input *policy-map-name*

no service-policy input *policy-map-name*

シンタックスの説明

policy-map-name	コントロール プレーン ポリシー マップの名前

デフォルト

なし

コマンド モード

コントロール プレーン コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、デフォルトの Virtual Device Context（VDC）でのみ使用できます。

コントロール プレーンに割り当てることができるのは、1 つのコントロール プレーン ポリシー マップだけです。コントロール プレーンに新しいコントロール プレーン ポリシー マップを割り当てるには、古いコントロール プレーン ポリシー マップを削除する必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、コントロール プレーンにコントロール プレーン ポリシー マップを割り当てる例を示します。

```
switch# config t
switch(config)# control-plane
switch(config-cp)# service-policy input PolicyMapA
```

次に、コントロール プレーンからコントロール プレーン ポリシー マップを削除する例を示します。

```
switch# config t
switch(config)# control-plane
switch(config-cp)# no service-policy input PolicyMapA
```

関連コマンド

コマンド	説明
policy-map type control-plane	コントロール プレーン ポリシー マップを指定して、ポリシー マップ コンフィギュレーション モードを開始します。
show policy-map type control-plane	コントロール プレーン ポリシー マップの設定情報を表示します。

set cos

コントロール プレーン ポリシー マップの IEEE 802.1Q Class of Service（CoS; サービス クラス）値を設定するには、**set cos** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

set cos [**inner**] *cos-value*

no set cos [**inner**] *cos-value*

シンタックスの説明

inner	（任意）Q-in-Q 環境には inner 802.1Q を指定します。
cos-value	コントロール プレーン ポリシー マップの CoS の数値。範囲は 0 ～ 7 です。

デフォルト

0

コマンド モード

ポリシー マップ クラス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、デフォルトの Virtual Device Context（VDC）でのみ使用できます。

このコマンドには、ライセンスは必要ありません。

例

次に、コントロール プレーン ポリシー マップの CoS 値を設定する例を示します。

```
switch# config t
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# class ClassMapA
switch(config-pmap-c)# set cos 4
```

次に、コントロール プレーン ポリシー マップのデフォルトの CoS 値に戻す例を示します。

```
switch# config t
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# class ClassMapA
switch(config-pmap-c)# no set cos 4
```

関連コマンド

コマンド	説明
class（ポリシー マップ）	コントロール プレーン ポリシー マップのコントロール プレーン クラス マップを指定して、ポリシー マップ クラス コンフィギュレーション モードを開始します。
policy-map type control-plane	コントロール プレーン ポリシー マップを指定して、ポリシー マップ コンフィギュレーション モードを開始します。
show policy-map type control-plane	コントロール プレーン ポリシー マップの設定情報を表示します。

set dscp

コントロール プレーン ポリシー マップに IPv4 および IPv6 パケットの Differentiated Services Code Point（DSCP; DiffServ コード ポイント）値を設定するには、**set dscp** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

set dscp [**tunnel**] {*dscp-value* | **af11** | **af12** | **af13** | **af21** | **af22** | **af23** | **af31** | **af32** | **af33** | **af41** | **af42** | **af43** | **cs1** | **cs2** | **cs3** | **cs4** | **cs5** | **cs6** | **cs7** | **ef** | **default**}

no set dscp [**tunnel**] {*dscp-value* | **af11** | **af12** | **af13** | **af21** | **af22** | **af23** | **af31** | **af32** | **af33** | **af41** | **af42** | **af43** | **cs1** | **cs2** | **cs3** | **cs4** | **cs5** | **cs6** | **cs7** | **ef** | **default**}

シンタックスの説明

tunnel	（任意）トンネル カプセル化に DSCP を設定します。
dscp-value	コントロール プレーン ポリシー マップの CoS の数値。範囲は 0 ～ 63 です。
af11	相対的優先転送 11 DSCP（001010）を指定します。
af12	相対的優先転送 12 DSCP（001100）を指定します。
af13	相対的優先転送 13 DSCP（001110）を指定します。
af21	相対的優先転送 21 DSCP（010010）を指定します。
af22	相対的優先転送 22 DSCP（010100）を指定します。
af23	相対的優先転送 23 DSCP（010110）を指定します。
af31	相対的優先転送 31 DSCP（011010）を指定します。
af32	相対的優先転送 32 DSCP（011100）を指定します。
af33	相対的優先転送 33 DSCP（011110）を指定します。
af41	相対的優先転送 41 DSCP（100010）を指定します。
af42	相対的優先転送 42 DSCP（100100）を指定します。
af43	相対的優先転送 43 DSCP（100110）を指定します。
cs1	クラス セレクタ 1（precedence 1）DSCP（001000）を指定します。
cs2	クラス セレクタ 2（precedence 2）DSCP（010000）を指定します。
cs3	クラス セレクタ 3（precedence 3）DSCP（011000）を指定します。
cs4	クラス セレクタ 4（precedence 4）DSCP（100000）を指定します。
cs5	クラス セレクタ 5（precedence 5）DSCP（101000）を指定します。
cs6	クラス セレクタ 6（precedence 6）DSCP（110000）を指定します。
cs7	クラス セレクタ 7（precedence 7）DSCP（111000）を指定します。
ef	完全優先転送 DSCP（101110）を指定します。
default	デフォルトの DSCP（000000）を指定します。

デフォルト

default

コマンド モード

ポリシー マップ クラス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、デフォルトの Virtual Device Context（VDC）でのみ使用できます。

このコマンドには、ライセンスは必要ありません。

例

次に、コントロール プレーン ポリシー マップの DHCP 値を設定する例を示します。

```
switch# config t
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# class ClassMapA
switch(config-pmap-c)# set dscp 4
```

次に、コントロール プレーン ポリシー マップのデフォルトの DHCP 値に戻す例を示します。

```
switch# config t
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# class ClassMapA
switch(config-pmap-c)# no set dscp 4
```

関連コマンド

コマンド	説明
class（ポリシー マップ）	コントロール プレーン ポリシー マップのコントロール プレーン クラス マップを指定して、ポリシー マップ クラス コンフィギュレーション モードを開始します。
policy-map type control-plane	コントロール プレーン ポリシー マップを指定して、ポリシー マップ コンフィギュレーション モードを開始します。
show policy-map type control-plane	コントロール プレーン ポリシー マップの設定情報を表示します。

set precedence

コントロール プレーン ポリシー マップに IPv4 および IPv6 パケットの precedence 値を設定するには、**set precedence** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

set precedence [**tunnel**] {*prec-value* | **critical** | **flash** | **flash-override** | **immediate** | **internet** | **network** | **priority** | **routine**}

no set precedence [**tunnel**] {*prec-value* | **critical** | **flash** | **flash-override** | **immediate** | **internet** | **network** | **priority** | **routine**}

シンタックスの説明

tunnel	（任意）トンネル カプセル化に precedence を設定します。
prec-value	コントロール プレーン ポリシー マップの DSCP precedence の数値。範囲は 0 ～ 7 です。
critical	precedence 値 5 に等しい critical precedence を指定します。
flash	precedence 値 3 に等しい flash precedence を指定します。
flash-override	precedence 値 4 に等しい flash override precedence を指定します。
immediate	precedence 値 2 に等しい immediate precedence を指定します。
internet	precedence 値 6 に等しい internet precedence を指定します。
network	precedence 値 7 に等しい network precedence を指定します。
priority	precedence 値 1 に等しい priority precedence を指定します。
routine	precedence 値 0 に等しい routine precedence を指定します。

デフォルト

0 または **routine**

コマンド モード

ポリシー マップ クラス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、デフォルトの Virtual Device Context（VDC）でのみ使用できます。

このコマンドには、ライセンスは必要ありません。

例

次に、コントロール プレーン ポリシー マップの CoS 値を設定する例を示します。

```
switch# config t
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# class ClassMapA
switch(config-pmap-c)# set precedence critical
```

次に、コントロール プレーン ポリシー マップのデフォルトの CoS 値に戻す例を示します。

```
switch# config t
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# class ClassMapA
switch(config-pmap-c)# no set precedence critical
```

関連コマンド

コマンド	説明
class（ポリシー マップ）	コントロール プレーン ポリシー マップのコントロール プレーン クラス マップを指定して、ポリシー マップ クラス コンフィギュレーション モードを開始します。
policy-map type control-plane	コントロール プレーン ポリシー マップを指定して、ポリシー マップ コンフィギュレーション モードを開始します。
show policy-map type control-plane	コントロール プレーン ポリシー マップの設定情報を表示します。

ssh

NX-OS デバイス上に IPv4 による Secure Shell（SSH; セキュア シェル）セッションを作成するには、**ssh** コマンドを使用します。

ssh [*username***@**]{*ipv4-address* | *hostname*} [**vrf** *vrf-name*]

シンタックスの説明

username	（任意）SSH セッションのユーザ名。ユーザ名は、大文字と小文字の区別がありません。
ipv4-address	リモート デバイスの IPv4 アドレス
hostname	リモート デバイスのホスト名。ホスト名では、大文字と小文字が区別されます。
vrf *vrf-name*	（任意）SSH セッションで使用する Virtual Routing and Forwarding（VRF; VPN ルーティングおよび転送）名を指定します。VRF 名では、大文字と小文字が区別されます。

デフォルト

デフォルト VRF

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

NX-OS ソフトウェアは、SSH バージョン 2 をサポートしています。

SSH セッションの IPv6 アドレスを使用するには、**ssh6** コマンドを使用します。

このコマンドには、ライセンスは必要ありません。

例

次に、IPv4 を使用して SSH セッションを開始する例を示します。

```
switch# ssh 10.10.1.1 vrf management
The authenticity of host '10.10.1.1 (10.10.1.1)' can't be established.
RSA key fingerprint is 9b:d9:09:97:f6:40:76:89:05:15:42:6b:12:48:0f:d6.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.1.1' (RSA) to the list of known hosts.
User Access Verification
Password:
```

関連コマンド

コマンド	説明
clear ssh session	SSH セッションを消去します。
ssh server enable	SSH サーバをイネーブルにします。
ssh6	IPv6 アドレスを使用して SSH セッションを開始します。

ssh key

Virtual Device Contex（VDC）の Secure Shell（SSH; セキュア シェル）サーバ鍵を作成するには、**ssh key** コマンドを使用します。SSH サーバ鍵を削除するには、このコマンドの **no** 形式を使用します。

ssh key {**dsa** [**force**] | **rsa** [*length* [**force**]]}

no ssh key [**dsa** | **rsa**]

シンタックスの説明

dsa	Digital System Algrorithm（DSA）SSH サーバ鍵を指定します。
force	（任意）SSH 鍵の交換を強制します。
rsa	RSA 公開鍵暗号法の SSH サーバ鍵を指定します。
length	（任意）SSH サーバ鍵を作成するときに使用するビット数。範囲は 768 ～ 2048 です。

デフォルト

1024 ビットの長さ

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

NX-OS ソフトウェアは、SSH バージョン 2 をサポートしています。

SSH サーバ鍵を削除または交換する場合、**no ssh server enable** コマンドを使用してまず SSH サーバをディセーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、DSA を使用して SSH サーバ鍵を作成する例を示します。

```
switch# config t
switch(config)# ssh key dsa
generating dsa key(1024 bits).....
..
generated dsa key
```

次に、デフォルトの鍵の長さで RSA を使用して SSH サーバ鍵を作成する例を示します。

```
switch# config t
switch(config)# ssh key rsa
generating rsa key(1024 bits).....
.
generated rsa key
```

次に、指定した鍵の長さで RSA を使用して SSH サーバ鍵を作成する例を示します。

```
switch# config t
switch(config)# ssh key rsa 768
generating rsa key(768 bits).....
.
generated rsa key
```

次に、force オプションで DSA を使用して SSH サーバ鍵を交換する例を示します。

```
switch# config t
switch(config)# no ssh server enable
switch(config)# ssh key dsa force
deleting old dsa key.....
generating dsa key(1024 bits).....
.
generated dsa key
switch(config)# ssh server enable
```

次に、DSA SSH サーバ鍵を削除する例を示します。

```
switch# config t
switch(config)# no ssh server enable
XML interface to system may become unavailable since ssh is disabled
switch(config)# no ssh key dsa
switch(config)# ssh server enable
```

次に、すべての SSH サーバ鍵を削除する例を示します。

```
switch# config t
switch(config)# no ssh server enable
XML interface to system may become unavailable since ssh is disabled
switch(config)# no ssh key
switch(config)# ssh server enable
```

関連コマンド

コマンド	説明
show ssh key	SSH サーバ鍵の情報を表示します。
ssh server enable	SSH サーバをイネーブルにします。

ssh server enable

Virtual Device Context（VDC）の Secure Shell（SSH; セキュア シェル）サーバをイネーブルにするには、**ssh server enable** コマンドを使用します。SSH サーバをディセーブルにするには、このコマンドの **no** 形式を使用します。

ssh server enable

no ssh server enable

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

イネーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

NX-OS ソフトウェアは、SSH バージョン 2 をサポートしています。

このコマンドには、ライセンスは必要ありません。

例

次に、SSH サーバをイネーブルにする例を示します。

```
switch# config t
switch(config)# ssh server enable
```

次に、SSH サーバをディセーブルにする例を示します。

```
switch# config t
switch(config)# no ssh server enable
XML interface to system may become unavailable since ssh is disabled
```

関連コマンド

コマンド	説明
show ssh server	SSH サーバ鍵の情報を表示します。

ssh6

NX-OS デバイス上に IPv6 による Secure Shell（SSH; セキュア シェル）セッションを作成するには、**ssh6** コマンドを使用します。

ssh6 [*username***@**]{*ipv6-address* | *hostname*} [**vrf** *vrf-name*]

シンタックスの説明

username	（任意）SSH セッションのユーザ名。ユーザ名は、大文字と小文字の区別がありません。
ipv6-address	リモート デバイスの IPv6 アドレス
hostname	リモート デバイスのホスト名
vrf *vrf-name*	（任意）SSH セッションで使用する Virtual Routing and Forwarding（VRF; VPN ルーティングおよび転送）名を指定します。VRF 名では、大文字と小文字が区別されます。

デフォルト

デフォルト VRF

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

NX-OS ソフトウェアは、SSH バージョン 2 をサポートしています。

SSH セッションを開始するために IPv4 アドレスを使用するには、**ssh** コマンドを使用します。

このコマンドには、ライセンスは必要ありません。

例

次に、IPv6 を使用して SSH セッションを開始する例を示します。

```
switch# ssh host2 vrf management
```

関連コマンド

コマンド	説明
clear ssh session	SSH セッションを消去します。
ssh	IPv4 アドレスを使用して SSH セッションを開始します。
ssh server enable	SSH サーバをイネーブルにします。

statistics per-entry

IP または MAC Access Control List（ACL; アクセス コントロール リスト）の各エントリで許可または拒否されたパケット数の統計情報の記録を開始するには、**statistics per-entry** コマンドを使用します。エントリ単位の統計情報の記録を停止するには、このコマンドの **no** 形式を使用します。

statistics per-entry

no statistics per-entry

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

IP アクセスリスト コンフィギュレーション
IPv6 アクセスリスト コンフィギュレーション
MAC アクセスリスト コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。
4.0(3)	**statistics** から **statistics per-entry** にコマンドが変更されました。

使用上のガイドライン

IPv4、IPv6、または MAC ACL がパケットに適用されるとデバイスが判別すると、ACL 内のすべてのエントリの条件に対してパケットのテストが実行されます。ACL エントリは、適用可能な **permit** および **deny** コマンドで設定するルールから抽出されます。最初の一致ルールは、パケットが許可または拒否されるかを判別します。**statistics per-entry** コマンドを入力して、ACL の各エントリで許可または拒否されるパケット数の記録を開始します。

デバイスは、暗黙ルールの統計情報を記録しません。これらのルールの統計情報を記録するには、各暗黙ルールの一致するルールを明示的に設定する必要があります。暗黙ルールの詳細については、次のコマンドを参照してください。

- **ip access-list**
- **ipv6 access-list**
- **mac access-list**

ACL のエントリ単位の統計情報を表示するには、**show access-lists** コマンドまたは適用可能な次のコマンドを使用します。

- **show ip access-lists**
- **show ipv6 access-lists**
- **show mac access-lists**

ACL のエントリ単位の統計情報を消去するには、**clear access-list counters** コマンドまたは適用可能な次のコマンドを使用します。

- **clear ip access-list counters**
- **clear ipv6 access-list counters**
- **clear mac access-list counters**

このコマンドには、ライセンスは必要ありません。

例

次に、ip-acl-101 という名前の IPv4 ACL に対するエントリ単位の統計情報の記録を開始する例を示します。

```
switch# config t
switch(config)# ip access-list ip-acl-101
switch(config-acl)# statistics per-entry
switch(config-acl)#
```

次に、ip-acl-101 という名前の IPv4 ACL に対するエントリ単位の統計情報の記録を停止する例を示します。

```
switch# config t
switch(config)# ip access-list ip-acl-101
switch(config-acl)# no statistics per-entry
switch(config-acl)#
```

関連コマンド

コマンド	説明
show access-lists	すべての IPv4、IPv6、および MAC ACL、または特定の ACL を表示します。
clear access-list counters	すべての IPv4、IPv6、および MAC ACL、または特定の ACL のエントリ単位の統計情報を消去します。

storm-control level

トラフィック ストーム制御の抑制レベルを設定するには、**storm-control level** コマンドを使用します。抑制モードをオフにしたり、デフォルトの設定に戻したりするには、このコマンドの **no** 形式を使用します。

storm-control {**broadcast** | **multicast** | **unicast**} **level** *percentage* [**.** *fraction*]

no storm-control {**broadcast** | **multicast** | **unicast**} **level**

シンタックスの説明

broadcast	ブロードキャスト トラフィックを指定します。
multicast	マルチキャスト トラフィックを指定します。
unicast	ユニキャスト トラフィックを指定します。
percentage	抑制レベルの割合。範囲は 0 ～ 100% です。
. *fraction*	（任意）抑制レベルの端数。範囲は 0 ～ 99 です。

デフォルト

すべてのパケットが渡されます。

コマンド モード

インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

storm-control level コマンドを入力して、インターフェイス上のトラフィック ストーム制御をイネーブルにし、トラフィック ストーム制御レベルを設定し、インターフェイスでイネーブルにされているすべてのトラフィック ストーム制御モードにトラフィック ストーム制御レベルを適用します。

3 つすべての抑制モードで共有されている抑制レベルは、1 つだけです。たとえば、ブロードキャスト レベルを 30 に設定し、マルチキャスト レベルを 40 に設定する場合、両方のレベルがイネーブルにされ、40 に設定されます。

端数の抑制レベルを入力する場合、ピリオド（.）が必要になります。

抑制レベルは、合計帯域幅の割合です。100% のしきい値は、トラフィックに制限がないことを意味します。0 または 0.0（端数）パーセントのしきい値は、指定されたすべてのトラフィックがポートでブロックされることを意味します。

廃棄カウントを表示するには、**show interfaces counters broadcast** コマンドを使用します。

指定したトラフィック タイプの抑制をオフにするには、次のいずれかの方式を使用します。

- 指定したトラフィック タイプのレベルを 100% に設定する。
- このコマンドの **no** 形式を使用する。

このコマンドには、ライセンスは必要ありません。

例

次に、ブロードキャスト トラフィックの抑制をイネーブルにし、抑制しきい値レベルを設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# storm-control broadcast level 30
```

次に、マルチキャスト トラフィックの抑制モードをディセーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 1/1
switch(config-if)# no storm-control multicast level
```

関連コマンド

コマンド	説明
show interface	インターフェイスのストーム制御抑制カウンタを表示します。
show running-config	インターフェイスの設定を表示します。

switchport port-security

レイヤ 2 インターフェイスのポート セキュリティをイネーブルにするには、**switchport port-security** コマンドを使用します。ポート セキュリティ設定を削除するには、このコマンドの **no** 形式を使用します。

switchport port-security

no switchport port-security

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、インターフェイス単位でポート セキュリティがディセーブルにされています。

インターフェイスでポート セキュリティをイネーブルにすると、セキュア MAC アドレスの学習のデフォルト方式（ダイナミック方式）もイネーブルになります。スティッキ学習方式をイネーブルにするには、**switchport port-security mac-address sticky** コマンドを使用します。

ポートセキュリティ設定は、各 Virtual Device Context（VDC）でローカルです。必要な場合、このコマンドを使用する前に正しい VDC に切り替えます。

switchport port-security コマンドを使用する前に、**feature port-security** コマンドを使用して、ポート セキュリティをイネーブルにする必要があります。

このコマンドを使用する前に、**switchport** コマンドを使用してインターフェイスをイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、イーサネット 2/1 インターフェイスのポート セキュリティをイネーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# switchport port-security
switch(config-if)#
```

関連コマンド

コマンド	説明
feature port-security	ポート セキュリティをグローバルにイネーブルにします。
show port-security	ポート セキュリティに関する情報を表示します。
switchport port-security aging time	動的に学習されたセキュア MAC アドレスのエージング タイムを設定します。
switchport port-security aging type	動的に学習されたセキュア MAC アドレスのエージング タイプを設定します。
switchport port-security mac-address	スタティック MAC アドレスを設定します。
switchport port-security mac-address sticky	セキュア MAC アドレスを学習するスティッキ方式をイネーブルにします。
switchport port-security maximum	インターフェイスにセキュア MAC アドレスのインターフェイスまたは VLAN の最大値を設定します。
switchport port-security violation	インターフェイスのセキュリティ違反処理を設定します。

switchport port-security aging time

動的に学習したセキュア MAC アドレスのエージング タイムを設定するには、**switchport port-security aging time** コマンドを使用します。デフォルトのエージング タイムである 1440 分に戻すには、このコマンドの **no** 形式を使用します。

switchport port-security aging time *minutes*

no switchport port-security aging time *minutes*

シンタックスの説明

minutes	デバイスがアドレスをドロップするまでの動的に学習されたセキュア MAC アドレス のエージング タイムを指定します。有効値は、1 ～ 1440 です。

デフォルト

なし

コマンド モード

インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトのエージング タイムは、1440 分です。

ポート セキュリティ設定は、各 Virtual Device Context（VDC）でローカルです。必要な場合、このコマンドを使用する前に正しい VDC に切り替えます。

switchport port-security aging time コマンドを使用する前に、**feature port-security** コマンドを使用して、ポート セキュリティをイネーブルにする必要があります。

このコマンドを使用する前に、**switchport** コマンドを使用してインターフェイスをイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、イーサネット 2/1 インターフェイス上に 120 分のエージング タイムを設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# switchport port-security aging time 120
switch(config-if)#
```

関連コマンド

コマンド	説明
feature port-security	ポート セキュリティをグローバルにイネーブルにします。
show port-security	ポート セキュリティに関する情報を表示します。
switchport port-security	レイヤ 2 インターフェイス上のポート セキュリティをイネーブルにします。
switchport port-security aging type	動的に学習されたセキュア MAC アドレスのエージング タイプを設定します。
switchport port-security mac-address	スタティック MAC アドレスを設定します。
switchport port-security mac-address sticky	セキュア MAC アドレスを学習するスティッキ方式をイネーブルにします。
switchport port-security maximum	インターフェイスにセキュア MAC アドレスのインターフェイスまたは VLAN の最大値を設定します。
switchport port-security violation	インターフェイスのセキュリティ違反処理を設定します。

switchport port-security aging type

動的に学習したセキュア MAC アドレスのエージング タイプを設定するには、**switchport port-security aging type** コマンドを使用します。デフォルトのエージング タイプ（absolute エージング）に戻すには、このコマンドの **no** 形式を使用します。

switchport port-security aging type {**absolute | inactivity**}

no switchport port-security aging type {**absolute | inactivity**}

シンタックスの説明

absolute	動的に学習されたセキュア MAC アドレスのエージングが、デバイスがアドレスの学習を開始した時点からの時間に基づいていることを指定します。
inactivity	動的に学習されたセキュア MAC アドレスのエージングが、デバイスが現在のインターフェイスで MAC アドレスから最後にトラフィックを受信した時点からの時間に基づいていることを指定します。

デフォルト

absolute

コマンド モード

インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトのエージング タイプは、absolute エージングです。

ポート セキュリティ設定は、各 Virtual Device Context（VDC）でローカルです。必要な場合、このコマンドを使用する前に正しい VDC に切り替えます。

switchport port-security aging type コマンドを使用する前に、**feature port-security** コマンドを使用して、ポート セキュリティをイネーブルにする必要があります。

このコマンドを使用する前に、**switchport** コマンドを使用してインターフェイスをイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、イーサネット 2/1 インターフェイス上に [inactivity] のエージング タイプを設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# switchport port-security aging type inactivity
switch(config-if)#
```

関連コマンド

コマンド	説明
feature port-security	ポート セキュリティをグローバルにイネーブルにします。
show port-security	ポート セキュリティに関する情報を表示します。
switchport port-security	ポート セキュリティにレイヤ 2 インターフェイスを設定します。
switchport port-security aging time	動的に学習されたセキュア MAC アドレスのエージング タイムを設定します。
switchport port-security mac-address	スタティック MAC アドレスを設定します。
switchport port-security mac-address sticky	セキュア MAC アドレスを学習するスティッキ方式をイネーブルにします。
switchport port-security maximum	インターフェイスにセキュア MAC アドレスのインターフェイスまたは VLAN の最大値を設定します。
switchport port-security violation	インターフェイスのセキュリティ違反処理を設定します。

switchport port-security mac-address

インターフェイスにスタティック、セキュア MAC アドレスを設定するには、**switchport port-security mac-address** コマンドを使用します。インターフェイスからスタティック、セキュア MAC アドレスを削除するには、このコマンドの **no** 形式を使用します。

switchport port-security mac-address *address* [**vlan** *vlan-w*]

no switchport port-security mac-address *address* [**vlan** *vlan-ID*]

シンタックスの説明

address	現在のインターフェイスにスタティック、セキュア MAC アドレスとして指定する MAC アドレス
vlan *vlan-ID*	（任意）MAC アドレスからのトラフィックが許可される VLAN を指定します。有効な VLAN ID は、1 ～ 4096 です。

デフォルト

なし

コマンド モード

インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトのスタティック、セキャア MAC アドレスはありません。

ポート セキュリティ設定は、各 Virtual Device Context（VDC）でローカルです。必要な場合、このコマンドを使用する前に正しい VDC に切り替えます。

switchport port-security mac-address コマンドを使用する前に、**feature port-security** コマンドを使用して、ポート セキュリティをイネーブルにする必要があります。

このコマンドを使用する前に、**switchport** コマンドを使用してインターフェイスをイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、イーサネット 2/1 インターフェイスにスタティック、セキュア MAC アドレスとして 0019.D2D0.00AE を設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# switchport port-security mac-address 0019.D2D0.00AE
switch(config-if)#
```

関連コマンド

コマンド	説明
feature port-security	ポート セキュリティをグローバルにイネーブルにします。
show port-security	ポート セキュリティに関する情報を表示します。
switchport port-security	ポート セキュリティにレイヤ 2 インターフェイスを設定します。
switchport port-security aging time	動的に学習されたセキュア MAC アドレスのエージング タイムを設定します。
switchport port-security aging type	動的に学習されたセキュア MAC アドレスのエージング タイプを設定します。
switchport port-security mac-address sticky	セキュア MAC アドレスを学習するスティッキ方式をイネーブルにします。
switchport port-security maximum	インターフェイスにセキュア MAC アドレスのインターフェイスまたは VLAN の最大値を設定します。
switchport port-security violation	インターフェイスのセキュリティ違反処理を設定します。

switchport port-security mac-address sticky

レイヤ 2 インターフェイスのセキュア MAC アドレスを学習するスティッキ方式をイネーブルにするには、**switchport port-security mac-address sticky** コマンドを使用します。スティッキ方式をディセーブルにし、ダイナミック方式に戻すには、このコマンドの **no** 形式を使用します。

switchport port-security mac-address sticky

no switchport port-security mac-address sticky

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

デフォルトでは、セキュア MAC アドレスを学習するスティッキ方式がディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

ポート セキュリティ設定は、各 Virtual Device Context（VDC）でローカルです。必要な場合、このコマンドを使用する前に正しい VDC に切り替えます。

switchport port-security mac-address sticky コマンドを使用する前に、**feature port-security** コマンドを使用して、ポート セキュリティをイネーブルにする必要があります。

このコマンドを使用する前に、**switchport** コマンドを使用してインターフェイスをイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、イーサネット 2/1 インターフェイスのセキュア MAC アドレスを学習するスティッキ方式をイネーブルにする例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# switchport port-security mac-address sticky
switch(config-if)#
```

関連コマンド

コマンド	説明
feature port-security	ポート セキュリティをグローバルにイネーブルにします。
show port-security	ポート セキュリティに関する情報を表示します。
switchport port-security	レイヤ 2 インターフェイス上のポート セキュリティをイネーブルにします。
switchport port-security aging time	動的に学習されたセキュア MAC アドレスのエージング タイムを設定します。
switchport port-security aging type	動的に学習されたセキュア MAC アドレスのエージング タイプを設定します。
switchport port-security mac-address	スタティック MAC アドレスを設定します。
switchport port-security maximum	インターフェイスにセキュア MAC アドレスのインターフェイスまたは VLAN の最大値を設定します。
switchport port-security violation	インターフェイスのセキュリティ違反処理を設定します。

switchport port-security maximum

レイヤ 2 インターフェイスにセキュア MAC アドレスのインターフェイスまたは VLAN の最大値を設定するには、**switchport port-security maximum** コマンドを使用します。ポート セキュリティ設定を削除するには、このコマンドの **no** 形式を使用します。

switchport port-security maximum *number* [**vlan** *vlan-ID*]

no switchport port-security maximum *number* [**vlan** *vlan-ID*]

シンタックスの説明

maximum *number*	セキュア MAC アドレスの最大数を指定します。*number* 引数の有効値に関する詳細については、「使用上のガイドライン」を参照してください。
vlan *vlan-ID*	（任意）最大値が適用される VLAN を指定します。**vlan** キーワードを省略する場合、最大値がインターフェイスの最大値として適用されます。

デフォルト

なし

コマンド モード

インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトのインターフェイスの最大値は、1 つのセキュア MAC アドレスです。

インターフェイスでポート セキュリティをイネーブルにすると、セキュア MAC アドレスの学習のデフォルト方式（ダイナミック方式）もイネーブルになります。スティッキ学習方式をイネーブルにするには、**switchport port-security mac-address sticky** コマンドを使用します。

ポート セキュリティ設定は、各 Virtual Device Context（VDC）でローカルです。必要な場合、このコマンドを使用する前に正しい VDC に切り替えます。

switchport port-security maximum コマンドを使用する前に、**feature port-security** コマンドを使用して、ポート セキュリティをイネーブルにする必要があります。

このコマンドを使用する前に、**switchport** コマンドを使用してインターフェイスをイネーブルにする必要があります。

デフォルトの VLAN の最大値はありません。

システム全体の、設定不可のセキュア MAC アドレスが最大 4096 あります。

このコマンドには、ライセンスは必要ありません。

アクセス ポートおよびトランク ポートの最大値

アクセス ポートして使用されるインターフェイスの場合、1 つのセキュア MAC アドレスにデフォルトのインターフェイスの最大値を使用することを推奨します。

トランク ポートして使用されるインターフェイスの場合、インターフェイスに使用できる実際のホスト数を反映する数にインターフェイスの最大値を設定します。

インターフェイスの最大値、VLAN の最大値、およびデバイスの最大値

インターフェイスに設定するすべての VLAN の最大値の合計は、インターフェイスの最大値を超えません。たとえば、インターフェイスの最大値を 10 セキュア MAC アドレス、VLAN 1 に対する VLAN の 最大値 を 5 セキュア MAC アドレスでトランクポート インターフェイスを設定する場合、VLAN 2 に設定するセキュア MAC アドレスの最大数も 5 になります。VLAN 2 に対して 6 セキュア MAC アドレスの最大値を設定しようとすると、デバイスはコマンドを受け入れません。

例

次に、イーサネット 2/1 インターフェイス上に 10 セキュア MAC アドレスのインターフェイスの最大値を設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# switchport port-security maximum 10
switch(config-if)#
```

関連コマンド

コマンド	説明
feature port-security	ポート セキュリティをグローバルにイネーブルにします。
show port-security	ポート セキュリティに関する情報を表示します。
switchport port-security	レイヤ 2 インターフェイス上のポート セキュリティをイネーブルにします。
switchport port-security aging time	動的に学習されたセキュア MAC アドレスのエージング タイムを設定します。
switchport port-security aging type	動的に学習されたセキュア MAC アドレスのエージング タイプを設定します。
switchport port-security mac-address	スタティック MAC アドレスを設定します。
switchport port-security mac-address sticky	セキュア MAC アドレスを学習するスティッキ方式をイネーブルにします。
switchport port-security violation	インターフェイスのセキュリティ違反処理を設定します。

switchport port-security violation

セキュリティ違反イベントがインターフェイス上で発生するときにデバイスが実行する処理を設定するには、**switchport port-security violation** コマンドを使用します。ポート セキュリティ違反処理の設定を削除するには、このコマンドの **no** 形式を使用します。

switchport port-security violation {**protect | restrict | shutdown**}

no switchport port-security violation {**protect | restrict | shutdown**}

シンタックスの説明

protect	パケットが通常セキュリティ違反イベントをトリガーするときにデバイスがセキュリティ違反を発生させないことを指定します。その代わりに、デバイスはインターフェイスの最大 MAC アドレス数に達するまでアドレスの学習を継続します。到達後は、デバイスはインターフェイスの学習をディセーブルにして、セキュア以外の MAC アドレスからすべての入力トラフィックをドロップします。
restrict	セキュリティ違反イベントのあと、デバイスはセキュア MAC アドレス以外のアドレスから入力トラフィックをドロップすることを指定します。デバイスは、ドロップされたパケット数のカウントを維持します。
shutdown	セキュリティ違反をトリガーしているパケットを受信すると、デバイスがインターフェイスをシャットダウンするように指定します。インターフェイスは、errdisable 状態です。これがデフォルトの処理です。インターフェイスを再度イネーブルにしたあと、セキュア MAC アドレスを含めて、ポート セキュリティ設定は維持されます。

デフォルト

なし

コマンド モード

インターフェイス コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトのセキュリティ違反処理は、インターフェイスをシャットダウンすることです。

ポート セキュリティ設定は、各 Virtual Device Context（VDC）でローカルです。必要な場合、このコマンドを使用する前に正しい VDC に切り替えます。

switchport port-security violation コマンドを使用する前に、**feature port-security** コマンドを使用して、ポート セキュリティをイネーブルにする必要があります。

このコマンドを使用する前に、**switchport** コマンドを使用してインターフェイスをイネーブルにする必要があります。

次の 2 つのいずれかのイベントが発生したときにポート セキュリティはセキュリティ違反をトリガーします。

- セキュア MAC アドレス以外のアドレスから入力トラフィックがインターフェイスに着信し、そのアドレスを学習するとセキュア MAC アドレスの適用可能な最大数を超えてしまう場合

VLAN とインターフェイスの両方の最大値が設定されていて、どちらかの最大数を超える場合。たとえば、ポート セキュリティが設定されている単一のインターフェイスについて、次のように想定します。

- VLAN 1 の最大アドレス値は 5 です。
- このインターフェイスの最大アドレス値は 10 です。

デバイスは、次のいずれかが発生すると違反を検出します。

- VLAN 1 のアドレスをすでに 5 つ学習していて、6 つめのアドレスからのインバウンド トラフィックが VLAN 1 のインターフェイスに着信した場合
- このインターフェイス上のアドレスをすでに 10 個学習していて、11 番めのアドレスからのインバウンド トラフィックがこのインターフェイスに着信した場合

- あるインターフェイスのセキュア MAC アドレスになっているアドレスからの入力トラフィックが、そのインターフェイスと同じ VLAN 内の別のインターフェイスに着信した場合

(注) あるセキュア ポートでセキュア MAC アドレスが設定または学習されたあと、同じ VLAN 内の別のポート上でこのセキュア MAC アドレスが検出された場合に発生する一連のイベントを、MAC の移行違反と呼びます。

セキュリティ違反が発生すると、デバイスは、該当するインターフェイスのポート セキュリティ設定に指定されている処理を実行します。デバイスが実行できる処理は次のとおりです。

- シャットダウン ― 違反をトリガーしたパケットの受信インターフェイスをシャットダウンします。インターフェイスは、errdisable 状態です。これがデフォルトの処理です。インターフェイスを再度イネーブルにしたあと、セキュア MAC アドレスを含めて、ポート セキュリティ設定は維持されます。

  シャットダウン後にデバイスが自動的にインターフェイスを再度イネーブルするように設定するには、**errdisable** グローバル コンフィギュレーション コマンドを使用します。あるいは、**shutdown** および **no shut down** のインターフェイス コンフィギュレーション コマンドを入力することにより、手動でインターフェイスを再度イネーブルにすることもできます。
- 制限 ― セキュア MAC アドレス以外のアドレスからの入力トラフィックをドロップします。デバイスは、ドロップされたパケット数のカウントを維持します。
- 保護 ― 違反の発生を防止します。インターフェイスの最大 MAC アドレス数に達するまでアドレス学習を継続します。到達後はそのインターフェイスでの学習をディセーブルにして、セキュア MAC アドレスイが以外のアドレスからの入力トラフィックをすべてドロップします。

セキュア MAC アドレスからの入力トラフィックが、そのアドレスをセキュア アドレスにしたインターフェイスとは異なるインターフェイスに着信したことにより違反が発生した場合、デバイスはトラフィックを受信したインターフェイスに対して処理を実行します。

このコマンドには、ライセンスは必要ありません。

例

次に、保護処理でセキュリティ違反イベントに応答するようにインターフェイスを設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/1
switch(config-if)# switchport port-security violation protect
switch(config-if)#
```

関連コマンド

コマンド	説明
feature port-security	ポート セキュリティをグローバルにイネーブルにします。
show port-security	ポート セキュリティに関する情報を表示します。
switchport port-security	レイヤ 2 インターフェイス上のポート セキュリティをイネーブルにします。
switchport port-security aging time	動的に学習されたセキュア MAC アドレスのエージング タイムを設定します。
switchport port-security aging type	動的に学習されたセキュア MAC アドレスのエージング タイプを設定します。
switchport port-security mac-address	スタティック MAC アドレスを設定します。
switchport port-security mac-address sticky	セキュア MAC アドレスを学習するスティッキ方式をイネーブルにします。
switchport port-security maximum	インターフェイスにセキュア MAC アドレスのインターフェイスまたは VLAN の最大値を設定します。

show コマンド

この章では、Cisco NX-OS セキュリティの **show** コマンドについて説明します。

show aaa accounting

AAA アカウンティング設定情報を表示するには、**show aaa accounting** コマンドを使用します。

show aaa accounting

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト なし

コマンド モード 任意のコマンド モード

サポートされるユーザ ロール
network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン このコマンドには、ライセンスは必要ありません。

例 次に、アカウンティング ログの設定を表示する例を示します。

```
switch# show aaa accounting
         default: local
```

show aaa authentication

AAA 認証設定情報を表示するには、**show aaa authentication** コマンドを使用します。

show aaa authentication [**login error-enable** | **login mschap**]

シンタックスの説明

login error-enable	（任意）認証ログイン エラー メッセージ イネーブル コンフィギュレーションを表示します。
login mschap	（任意）認証ログイン MS-CHAP イネーブル コンフィギュレーションを表示します。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、設定された認証パラメータを表示する例を示します。

```
switch# show aaa authentication
         default: local
         console: local
         dot1x: not configured
         eou: not configured
```

次に、認証ログイン エラーイネーブル設定を表示する例を示します。

```
switch# show aaa authentication login error-enable
disabled
```

次に、認証ログイン MSCHAP 設定を表示する例を示します。

```
switch# show aaa authentication login mschap
disabled
```

show aaa groups

AAA サーバ グループ設定を表示するには、**show aaa groups** コマンドを使用します。

show aaa groups

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト なし

コマンド モード 任意のコマンド モード

サポートされるユーザ ロール network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン このコマンドには、ライセンスは必要ありません。

例 次に、AAA グループ情報を表示する例を示します。

```
switch# show aaa groups
radius
TacServer
```

show aaa user default-role

AAA ユーザ デフォルト ロール設定を表示するには、**show aaa user default-role** コマンドを使用します。

show aaa user default-role

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト なし

コマンド モード 任意のコマンド モード

サポートされるユーザ ロール network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(3)	このコマンドが導入されました。

使用上のガイドライン AAA ユーザ デフォルト ロールを設定するには、**aaa user default-role** コマンドを使用します。

このコマンドには、ライセンスは必要ありません。

例 次に、AAA ユーザ デフォルト ロール設定を表示する例を示します。

```
switch# show aaa user default-role
enabled
```

関連コマンド

コマンド	説明
aaa user default-role	AAA ユーザ デフォルト ロールをイネーブルにします。

show access-lists

すべての IPv4 および MAC Access Control List（ACL; アクセス コントロール リスト）または特定の ACL を表示するには、**show access-lists** コマンドを使用します。

show access-lists [*access-list-name*] [**expanded** | **summary**]

シンタックスの説明

access-list-name	（任意）ACL の名前。名前では最大で 64 文字の英数字を使用でき、大文字と小文字が区別されます。
expanded	（任意）オブジェクト グループの名前だけでなく、オブジェクト グループの内容を表示することを指定します。
summary	（任意）コマンドが ACL に関する情報を表示することを指定します。詳細については、「使用上のガイドライン」を参照してください。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

access-list-name 引数を使用して ACL を指定する場合を除いて、デバイスはすべての ACL を表示します。

expanded キーワードを使用すると、オブジェクト グループの名前だけでなく、ACL で使用されているオブジェクト グループの詳細を表示できます。オブジェクト グループに関する詳細については、**object-group ip address** および **object-group ip port** コマンドを参照してください。

summary キーワードを使用すると、ACL 設定ではなく ACL に関する情報を表示できます。表示される情報には、次の内容が含まれます。

- エントリ単位の統計情報が ACL に対して設定されているかどうか
- ACL 設定内のルール数。この数は、デバイスがインターフェイスに適用されるときに ACL 内に含まれるエントリ数を反映しません。ACL 内のルールがオブジェクト グループを使用する場合、適用されるときの ACL 内のエントリ数は、ルール数よりはるかに大きくなります。
- ACL が適用されているインターフェイス
- ACL がアクティブ状態のインターフェイス

show access-lists コマンドは、次の両方の状態が真の場合に、ACL 内の各エントリの統計情報を表示します。

- ACL 設定に **statistics per-entry** コマンドが含まれている
- 管理上アップ状態のインターフェイスに ACL が適用されている

このコマンドには、ライセンスは必要ありません。

例

次に、IP ACL および MAC ACL が 1 つずつ設定されたデバイスで、ACL 名を指定せずに **show access-lists** コマンドを使用する例を示します。

```
switch# show access-lists

IP access list ip-v4-filter
        10 permit ip any any
MAC access list mac-filter
        10 permit 00c0.4f00.0000 0000.00ff.ffff 0060.3e00.0000 0000.00ff.ffff ip
```

次に、**show access-lists** コマンドを使用して、MainLab オブジェクト グループを除くエントリのエントリ単位の統計情報を含めて、ipv4-RandD-outbound-web という名前の IPv4 ACL を表示する例を示します。

```
switch# show access-lists ipv4-RandD-outbound-web

IP access list ipv4-RandD-outbound-web
        statistics per-entry
        1000 permit ahp any any [match=732]
        1005 permit tcp addrgroup MainLab any eq telnet
        1010 permit tcp any any eq www [match=820421]
```

次に、**show access-lists** コマンドを使用して、ipv4-RandD-outbound-web という名前の IPv4 ACL を表示する例を示します。**expanded** キーワードを使用すると、エントリ単位の統計情報を含めて、前の例のオブジェクト グループの内容が表示されます。

```
switch# show access-lists ipv4-RandD-outbound-web expanded

IP access list ipv4-RandD-outbound-web
        statistics per-entry
        1000 permit ahp any any [match=732]
        1005 permit tcp 10.52.34.4/32 any eq telnet [match=5032]
        1005 permit tcp 10.52.34.27/32 any eq telnet [match=433]
        1010 permit tcp any any eq www [match=820421]
```

次に、**summary** キーワードとともに **show access-lists** コマンドを使用して、ACL が適用されているインターフェイス、ACL がアクティブ状態のインターフェイスなどの ipv4-RandD-outbound-web という名前の IPv4 ACL に関する情報を表示する例を示します。

```
switch# show access-lists ipv4-RandD-outbound-web summary
IPV4 ACL ipv4-RandD-outbound-web

        Statistics enabled
        Total ACEs Configured: 4
        Configured on interfaces:
                Ethernet2/4 - ingress (Router ACL)
        Active on interfaces:
                Ethernet2/4 - ingress (Router ACL)
```

関連コマンド

コマンド	説明
ip access-list	IPv4 ACL を設定します。
mac access-list	MAC ACL を設定します。
show ip access-lists	すべての IPv4 ACL または特定の IPv4 ACL を表示します。
show mac access-lists	すべての MAC ACL または特定の MAC ACL を表示します。

show accounting log

アカウンティングのログ内容を表示するには、**show accounting log** コマンドを使用します。

show accounting log [*size*] [**start-time** *year month day HH*:*MM*:*SS*]

シンタックスの説明

size	（任意）表示するログのサイズ（バイト単位）。範囲は 0 ～ 250000 です。
start-time *year month day HH*:*MM*:*SS*	（任意）開始時間を指定します。*year* 引数は、*yyyy* フォーマットです。*month* 引数は、3 文字の英語の略語です。*day* 引数の範囲は 1 ～ 31 です。*HH*:*MM*:*SS* 引数は、標準 24 時間フォーマットです。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、アカウンティング ログ全体を表示する例を示します。

```
switch# show accounting log

Sat Feb 16 10:44:24 2008:update:/dev/pts/1_172.28.254.254:admin:show system uptime
Sat Feb 16 10:44:25 2008:update:/dev/pts/1_172.28.254.254:admin:show clock
Sat Feb 16 10:45:20 2008:update:/dev/pts/1_172.28.254.254:admin:show logging log
file start-time 2008 Feb 16 10:44:11
Sat Feb 16 10:45:23 2008:update:/dev/pts/1_172.28.254.254:admin:show accounting
log start-time 2008 Feb 16 10:08:57
Sat Feb 16 10:45:24 2008:update:/dev/pts/1_172.28.254.254:admin:show system uptime
Sat Feb 16 10:45:25 2008:update:/dev/pts/1_172.28.254.254:admin:show clock
Sat Feb 16 10:46:20 2008:update:/dev/pts/1_172.28.254.254:admin:show logging log
file start-time 2008 Feb 16 10:45:11
Sat Feb 16 10:46:22 2008:update:/dev/pts/1_172.28.254.254:admin:show accounting
```

次に、アカウンティング ログの 400 バイトを表示する例を示します。

```
switch# show accounting log 400

Sat Feb 16 21:15:24 2008:update:/dev/pts/1_172.28.254.254:admin:show accounting log
start-time 2008 Feb 16 18:31:21
Sat Feb 16 21:15:25 2008:update:/dev/pts/1_172.28.254.254:admin:show system uptime
Sat Feb 16 21:15:26 2008:update:/dev/pts/1_172.28.254.254:admin:show clock
```

次に、2008 年 2 月 16 日の 16:00:00 に開始するアカウンティング ログを表示する例を示します。

```
switch(config)# show accounting log start-time 2008 Feb 16 16:00:00

Sat Feb 16 16:00:18 2008:update:/dev/pts/1_172.28.254.254:admin:show logging log file
start-time 2008 Feb 16 15:59:16
Sat Feb 16 16:00:26 2008:update:/dev/pts/1_172.28.254.254:admin:show accounting log
start-time 2008 Feb 16 12:05:16
Sat Feb 16 16:00:27 2008:update:/dev/pts/1_172.28.254.254:admin:show system uptime
Sat Feb 16 16:00:28 2008:update:/dev/pts/1_172.28.254.254:admin:show clock
Sat Feb 16 16:01:18 2008:update:/dev/pts/1_172.28.254.254:admin:show logging log file
start-time 2008 Feb 16 16:00:16
Sat Feb 16 16:01:26 2008:update:/dev/pts/1_172.28.254.254:admin:show accounting log
start-time 2008 Feb 16 12:05:16
Sat Feb 16 16:01:27 2008:update:/dev/pts/1_172.28.254.254:admin:show system uptime
Sat Feb 16 16:01:29 2008:update:/dev/pts/1_172.28.254.254:admin:show clock
Sat Feb 16 16:02:18 2008:update:/dev/pts/1_172.28.254.254:admin:show logging log file
start-time 2008 Feb 16 16:01:16
Sat Feb 16 16:02:26 2008:update:/dev/pts/1_172.28.254.254:admin:show accounting log
start-time 2008 Feb 16 12:05:16
Sat Feb 16 16:02:28 2008:update:/dev/pts/1_172.28.254.254:admin:show system uptime
```

関連コマンド

コマンド	説明
clear accounting log	アカウンティング ログを消去します。

show arp access-lists

すべての ARP Access Control List（ACL; アクセス コントロール リスト）または特定の ARP ACL を表示するには、**show arp access-lists** コマンドを使用します。

show arp access-lists [*access-list-name*]

シンタックスの説明

access-list-name	（任意）ARP ACL の名前。名前では最大で 64 文字の英数字を使用でき、大文字と小文字が区別されます。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

access-list-name 引数を使用して ACL を指定する場合を除いて、デバイスはすべての ARP ACL を表示します。

このコマンドには、ライセンスは必要ありません。

例

次に、**show arp access-lists** コマンドを使用して、2 つの ARP ACL を持つデバイスですべての ARP ACL を表示する例を示します。

```
switch# show arp access-lists

ARP access list arp-permit-all
10 permit ip any mac any
ARP access list arp-lab-subnet
10 permit request ip 10.32.143.0 255.255.255.0 mac any
```

次に、**show arp access-lists** コマンドを使用して、arp-permit-all という名前の ARP ACL を表示する例を示します。

```
switch# show arp access-lists arp-permit-all

ARP access list arp-permit-all
10 permit ip any mac any
```

関連コマンド

コマンド	説明
arp access-list	ARP ACL を設定します。
ip arp inspection filter	VLAN に ARP ACL を適用します。

show class-map type control-plane

コントロール プレーン クラス マップ情報を表示するには、**show class-map type control-plane** コマンドを使用します。

show class-map type control-plane [*class-map-name*]

シンタックスの説明

class-map-name	（任意）コントロール プレーン クラス マップの名前

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、デフォルトの Virtual Device Context（VDC）でのみ使用できます。

このコマンドには、ライセンスは必要ありません。

例

次に、コントロール プレーン クラス マップ情報を表示する例を示します。

```
switch# show class-map type control-plane

    class-map type control-plane match-any copp-system-class-critical
      match access-grp name copp-system-acl-arp
      match access-grp name copp-system-acl-msdp

    class-map type control-plane match-any copp-system-class-important
      match access-grp name copp-system-acl-gre
      match access-grp name copp-system-acl-tacas

    class-map type control-plane match-any copp-system-class-normal
      match access-grp name copp-system-acl-icmp
      match redirect dhcp-snoop
      match redirect arp-inspect
      match exception ip option
      match exception ip icmp redirect
      match exception ip icmp unreachable
```

show copp status

Control Plane Policing（CoPP）設定ステータスを表示するには、**show copp status** コマンドを使用します。

show copp status

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト なし

コマンド モード 任意のコンフィギュレーション モード

サポートされるユーザ ロール network-admin
vdc-admin
network-operator
vdc-operator

コマンド履歴

リリース	変更内容
4.0(2)	このコマンドが導入されました。

使用上のガイドライン このコマンドは、デフォルトの Virtual Device Context（VDC）でのみ使用できます。

このコマンドには、ライセンスは必要ありません。

例 次に、CoPP 設定ステータス情報を表示する例を示します。

```
switch# show copp status
Last Config Operation: service-policy input copp-system-policy
Last Config Operation Timestamp: 21:57:58 UTC Jun  4 2008
Last Config Operation Status: Success
Policy-map attached to the control-plane: new-copp-policy
```

show cts

グローバル Cisco TrustSec 設定を表示するには、**show cts** コマンドを使用します。

show cts

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト なし

コマンド モード 任意のコンフィギュレーション モード

サポートされるユーザ ロール network-admin
vdc-admin
network-operator
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例 次に、Cisco TrustSec グローバル設定を表示する例を示します。

```
switch# show cts
CTS Global Configuration
==============================
  CTS support           : enabled
  CTS device identity   : Device1
  CTS caching support   : disabled

  Number of CTS interfaces in
    DOT1X mode : 0
    Manual mode : 0
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。

show cts credentials

Cisco TrustSec デバイスの証明書設定を表示するには、**show cts credentials** コマンドを使用します。

show cts credentials

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト なし

コマンド モード 任意のコンフィギュレーション モード

サポートされるユーザ ロール network-admin
vdc-admin
network-operator
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例 次に、Cisco TrustSec 証明書設定を表示する例を示します。

```
switch# show cts credentials
CTS password is defined in keystore, device-id = Device1
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。

show cts environment-data

グローバル Cisco TrustSec 環境データを表示するには、**show cts environment-data** コマンドを使用します。

show cts environment-data

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

任意のコンフィギュレーション モード

サポートされるユーザ ロール

network-admin
vdc-admin
network-operator
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

NX-OS デバイスは、デバイスの Cisco TrustSec 証明書を設定し、Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）を設定したあと、ACS から Cisco TrustSec 環境データをダウンロードします。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、Cisco TrustSec 環境データを表示する例を示します。

```
switch# show cts environment-data
CTS Environment Data
================================
  Current State           : CTS_ENV_DNLD_ST_ENV_DOWNLOAD_DONE
  Last Status             : CTS_ENV_SUCCESS
  Local Device SGT        : 0x0002
  Transport Type          : CTS_ENV_TRANSPORT_DIRECT
  Data loaded from cache  : FALSE
  Env Data Lifetime       : 300 seconds after last update
  Last Update Time        : Sat Jan  5 16:29:52 2008

  Server List             : ACSServerList1
     AID:74656d706f72617279 IP:10.64.65.95 Port:1812
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。

show cts interface

インターフェイスの Cisco TrustSec 情報を表示するには、**show cts interface** コマンドを使用します。

show cts interface {**all** | **ethernet** *slot*/*port*}

シンタックスの説明

all	すべてのインターフェイスの Cisco TrustSec 情報を表示します。
interface *slot*/*port*	特定のインターフェイスの Cisco TrustSec 情報を表示します。

デフォルト

なし

コマンド モード

任意のコンフィギュレーション モード

サポートされるユーザ ロール

network-admin
vdc-admin
network-operator
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、すべてのインターフェイスの Cisco TrustSec 設定を表示する例を示します。

```
switch# show cts interface all
CTS Information for Interface Ethernet2/24:
    CTS is enabled, mode:   CTS_MODE_DOT1X
    IFC state:              CTS_IFC_ST_CTS_OPEN_STATE
    Authentication Status:  CTS_AUTHC_SUCCESS
      Peer Identity:        india1
      Peer is:              CTS Capable
      802.1X role:          CTS_ROLE_AUTH
      Last Re-Authentication:
    Authorization Status:   CTS_AUTHZ_SUCCESS
      PEER SGT:             2
      Peer SGT assignment:  Trusted
      Global policy fallback access list:
    SAP Status:             CTS_SAP_SUCCESS
      Configured pairwise ciphers: GCM_ENCRYPT
      Replay protection: Enabled
      Replay protection mode: Strict
      Selected cipher: GCM_ENCRYPT
      Current receive SPI: sci:1b54c1fbff0000 an:0
      Current transmit SPI: sci:1b54c1fc000000 an:0

CTS Information for Interface Ethernet2/25:
    CTS is enabled, mode:   CTS_MODE_DOT1X
    IFC state:              CTS_IFC_ST_CTS_OPEN_STATE
    Authentication Status:  CTS_AUTHC_SUCCESS
      Peer Identity:        india1
      Peer is:              CTS Capable
      802.1X role:          CTS_ROLE_SUP
      Last Re-Authentication:
    Authorization Status:   CTS_AUTHZ_SUCCESS
      PEER SGT:             2
      Peer SGT assignment:  Trusted
      Global policy fallback access list:
    SAP Status:             CTS_SAP_SUCCESS
      Configured pairwise ciphers: GCM_ENCRYPT
      Replay protection: Enabled
      Replay protection mode: Strict
      Selected cipher: GCM_ENCRYPT
      Current receive SPI: sci:1b54c1fc000000 an:0
      Current transmit SPI: sci:1b54c1fbff0000 an:0
```

次に、特定のインターフェイスの Cisco TrustSec 設定を表示する例を示します。

```
switch# show cts interface ethernet 2/24
CTS Information for Interface Ethernet2/24:
    CTS is enabled, mode:   CTS_MODE_DOT1X
    IFC state:              CTS_IFC_ST_CTS_OPEN_STATE
    Authentication Status:  CTS_AUTHC_SUCCESS
      Peer Identity:        india1
      Peer is:              CTS Capable
      802.1X role:          CTS_ROLE_AUTH
      Last Re-Authentication:
    Authorization Status:   CTS_AUTHZ_SUCCESS
      PEER SGT:             2
      Peer SGT assignment:  Trusted
      Global policy fallback access list:
    SAP Status:             CTS_SAP_SUCCESS
      Configured pairwise ciphers: GCM_ENCRYPT
      Replay protection: Enabled
      Replay protection mode: Strict
      Selected cipher: GCM_ENCRYPT
      Current receive SPI: sci:1b54c1fbff0000 an:0
      Current transmit SPI: sci:1b54c1fc000000 an:0
```

表 1 は、**show cts interface** コマンド出力で表示される値に関する情報を提供します。

表 1　show cts interface コマンド出力の値の説明

値	説明
認証ステータス フィールド	
CTS_AUTHC_INIT	認証エンジンは、初期状態です。
CTS_AUTHC_SUCCESS	認証が正常に行われました。
CTS_AUTHC_NO_RESPONSE	Cisco Access Control Server（ACS）に到達できません。Cisco ACS から応答がありません。
CTS_AUTHC_UNAUTHORIZED	認証が進行中です。
CTS_AUTHC_SKIPPED_CONFIG	Cisco TrustSec 設定は、デバイスが認証プロセスを省略する必要があることを示しています。
CTS_AUTHC_REJECT	Cisco ACS は、認証要求を拒否しました。
許可ステータス フィールド	
CTS_AUTHZ_INIT	許可エンジンは、初期状態です。
CTS_AUTHZ_SUCCESS	許可が正常に行われました。
CTS_AUTHZ_REJECT	ACS が許可要求を拒否しました。
CTS_AUTHZ_SKIPPED_CONFIG	Cisco TrustSec 設定は、デバイスが許可プロセスを省略する必要があることを示しています。
CTS_AUTHZ_POL_ACQ_FAILURE	許可ポリシー獲得が失敗しました。
CTS_AUTHZ_HW_FAILURE	ハードウェア許可プログラミングが失敗しました。
CTS_AUTHZ_RBACL_FAILURE	Security Group Access Control Group（SGACL）のダウンロードとインストールが失敗しました。
CTS_AUTHZ_INCOMPLETE	許可が進行中です。
SAP ステータス フィールド	
CTS_SAP_INIT	Security Association Protocol（SAP）ネゴシエーションが初期状態です。
CTS_SAP_SUCCESS	SAP ネゴシエーションが正常に行われました。
CTS_SAP_FAILURE	SAP ネゴシエーションが失敗しました。
CTS_SAP_SKIPPED_CONFIG	Cisco TrustSec 設定は、デバイスが SAP ネゴシエーションを省略する必要があることを示しています。
CTS_SAP_REKEY	SAP キーの再生成が進行中です。
CTS_SAP_INCOMPLETE	SAP ネゴシエーションが進行中です。

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。

show cts pacs

EAP-FAST によってプロビジョニングされた Cisco TrustSec Protect Access Credentials（PAC）を表示するには、**show cts pacs** コマンドを使用します。

show cts pacs

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

任意のコンフィギュレーション モード

サポートされるユーザ ロール

network-admin
vdc-admin
network-operator
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、Cisco TrustSec グローバル設定を表示する例を示します。

```
switch# show cts pacs
PAC Info :
================================
  PAC Type             : unknown
  AID                  : 74656d706f72617279
  I-ID                 : india1
  AID Info             : ACS Info
  Credential Lifetime : Thu Apr  3 00:36:04 2008

  PAC Opaque           : 0002008300020004000974656d706f726172790006007000010100 1d
6321a2a55fa81e05cd705c714bea116907503aab89490b07fcbb2bd455b8d873f21b5b6b403eb1d8
125897d93b94669745cfe1abb0baf01a00b77aacf0bda9fbaf7dcd54528b782d8206a7751afdde42
1ff4a3db6a349c652fea81809fba4f30b1fffb7bfffaf9a6608
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。

show cts role-based access-list

グローバル Cisco TrustSec Security Group Access Control List（SGACL）設定を表示するには、**show cts role-based access-list** コマンドを使用します。

show cts role-based access-list

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

任意のコンフィギュレーション モード

サポートされるユーザ ロール

network-admin
vdc-admin
network-operator
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、Cisco TrustSec SGACL 設定を表示する例を示します。

```
switch# show cts role-based access-list
rbacl:test-3
        deny ip
rbacl:test-1
        deny ip
        deny icmp
        deny tcp src eq 1000 dest eq 2000
        deny udp src range 1000 2000
rbacl:test-2
        permit icmp
        permit igmp
        permit tcp src lt 2000
        permit udp dest gt 4000
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。

show cts role-based enable

VLAN および Virtual Routing and Forwarding（VRF）インスタンスの Cisco TrustSec Security Group Access Control List（SGACL）イネーブル ステータスを表示するには、**show cts role-based enable** コマンドを使用します。

show cts role-based enable

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

任意のコンフィギュレーション モード

サポートされるユーザ ロール

network-admin
vdc-admin
network-operator
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、Cisco TrustSec SGACL 強制ステータスを表示する例を示します。

```
switch# show cts role-based enable

vlan:1
vrf:1
vrf:3
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。

show cts role-based policy

グローバル Cisco TrustSec Security Group Access Control List（SGACL）ポリシーを表示するには、**show cts role-based policy** コマンドを使用します。

show cts role-based policy

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

任意のコンフィギュレーション モード

サポートされるユーザ ロール

network-admin
vdc-admin
network-operator
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、Cisco TrustSec SGACL ポリシーを表示する例を示します。

```
switch# show cts role-based policy

sgt:unknown
dgt:unknown     rbacl:test-2
        permit icmp
        permit igmp
        permit tcp src lt 2000
        permit udp dest gt 4000

sgt:1000
dgt:2000        rbacl:test-1
        deny ip
        deny icmp
        deny tcp src eq 1000 dest eq 2000
        deny udp src range 1000 2000

sgt:any
dgt:any rbacl:test-3
        deny ip
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。

show cts role-based sgt-map

グローバル Cisco TrustSec Security Group Tag（SGT）マッピング設定を表示するには、**show cts role-based sgt-map** コマンドを使用します。

show cts role-based sgt-map

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

任意のコンフィギュレーション モード

サポートされるユーザ ロール

network-admin
vdc-admin
network-operator
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、Cisco TrustSec SGT マッピング設定を表示する例を示します。

```
switch# show cts role-based sgt-map
IP ADDRESS              SGT              VRF/VLAN        SGT CONFIGURATION
5.5.5.5                 5                vlan:10         CLI Configured
5.5.5.6                 6                vlan:10         CLI Configured
5.5.5.7                 7                vlan:10         CLI Configured
5.5.5.8                 8                vlan:10         CLI Configured
10.10.10.10             10               vrf:3           CLI Configured
10.10.10.20             20               vrf:3           CLI Configured
10.10.10.30             30               vrf:3           CLI Configured
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。

show cts sxp

Cisco TrustSec Security Group Tag（SGT）Exchange Protocol（SXP）設定を表示するには、**show cts sxp** コマンドを使用します。

show cts sxp

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

任意のコンフィギュレーション モード

サポートされるユーザ ロール

network-admin
vdc-admin
network-operator
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、Cisco TrustSec SXP 設定を表示する例を示します。

```
switch# show cts sxp
CTS SXP Configuration:
SXP enabled
SXP retry timeout:60
SXP reconcile timeout:120
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。

show cts sxp connection

Cisco TrustSec Security Group Tag（SGT）Exchange Protocol（SXP）接続情報を表示するには、**show cts sxp connection** コマンドを使用します。

show cts sxp connection

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

任意のコンフィギュレーション モード

サポートされるユーザ ロール

network-admin
vdc-admin
network-operator
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例

次に、Cisco TrustSec Security Group Tag（SGT）Exchange Protocol（SXP）接続情報を表示する例を示します。

```
switch# show cts sxp connection
PEER_IP_ADDR    VRF             PEER_SXP_MODE   SELF_SXP_MODE   CONNECTION STATE
10.10.3.3       default         listener        speaker         initializing
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。

show dot1x

802.1X 機能ステータスを表示するには、**show dot1x** コマンドを使用します。

show dot1x

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト なし

コマンド モード 任意のコマンド モード

サポートされるユーザ ロール network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン このコマンドを使用する前に、**feature dot1x** コマンドを使用して 802.1X 機能をイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例 次に、802.1X 機能ステータスを表示する例を示します。

```
switch# show dot1x
           Sysauthcontrol Enabled
   Dot1x Protocol Version 2
```

関連コマンド

コマンド	説明
feature dot1x	802.1X 機能をイネーブルにします。

show dot1x all

すべての 802.1X 機能ステータスおよび設定情報を表示するには、**show dot1x all** コマンドを使用します。

show dot1x all [**details** | **statistics** | **summary**]

シンタックスの説明

details	（任意）802.1X 設定に関する詳細情報を表示します。
statistics	（任意）802.1X 統計情報を表示します。
summary	（任意）802.1X 情報の要約を表示します。

デフォルト

グローバルおよびインターフェイスの 802.1X 設定を表示します。

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、**feature dot1x** コマンドを使用して 802.1X 機能をイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、すべての 802.1X 機能ステータスおよび設定情報を表示する例を示します。

```
switch# show dot1x all
           Sysauthcontrol Enabled
   Dot1x Protocol Version 2

Dot1x Info for Ethernet2/1
-----------------------------------
                      PAE = AUTHENTICATOR
              PortControl = FORCE_AUTH
                 HostMode = SINGLE HOST
         ReAuthentication = Disabled
              QuietPeriod = 60
           ServerTimeout = 30
             SuppTimeout = 30
            ReAuthPeriod = 3600 (Locally configured)
               ReAuthMax = 2
                  MaxReq = 2
                TxPeriod = 30
          RateLimitPeriod = 0
```

関連コマンド

コマンド	説明
feature dot1x	802.1X 機能をイネーブルにします。

show dot1x interface ethernet

イーサネット インターフェイスの 802.1X 機能ステータスおよび設定情報を表示するには、**show dot1x interface ethernet** コマンドを使用します。

show dot1x interface ethernet *slot/port* [**details** | **statistics** | **summary**]

シンタックスの説明

slot/port	インターフェイスのスロットおよびポートの ID
details	（任意）インターフェイスの詳細な 802.1X 情報を表示します。
statistics	（任意）インターフェイスの 802.1X 統計情報を表示します。
summary	（任意）インターフェイスの 802.1X 情報の要約を表示します。

デフォルト

インターフェイス 802.1X 設定を表示します。

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、**feature dot1x** コマンドを使用して 802.1X 機能をイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、イーサネット インターフェイスの 802.1X 機能ステータスおよび設定情報を表示する例を示します。

```
switch# show dot1x interface ethernet 2/1

Dot1x Info for Ethernet2/1
-----------------------------------
                      PAE = AUTHENTICATOR
              PortControl = FORCE_AUTH
                 HostMode = SINGLE HOST
         ReAuthentication = Disabled
              QuietPeriod = 60
           ServerTimeout = 30
              SuppTimeout = 30
            ReAuthPeriod = 3600 (Locally configured)
               ReAuthMax = 2
                  MaxReq = 2
                 TxPeriod = 30
          RateLimitPeriod = 0
```

関連コマンド

コマンド	説明
feature dot1x	802.1X 機能をイネーブルにします。

show eou

Extensible Authentication Protocol over User Datagram Protocol（EAPoUDP）ステータスおよび設定情報を表示するには、**show eou** コマンドを使用します。

show eou [**all** | **authentication** {**clientless** | **eap** | **static**} | **interface ethernet** *slot/port* | **ip-address** *ipv4-address* | **mac-address** *mac-address* | **posturetoken** [*name*]]

シンタックスの説明

all	（任意）すべての EAPoUDP セッションを表示します。
authentication	（任意）特定の認証タイプの EAPoUDP セッションを表示します。
clientless	クライアントレス ポスチャ検証を使用して認証されたセッションを指定します。
eap	EAPoUDP を使用して認証されたセッションを指定します。
static	静的に設定された例外リストを使用して静的に認証されたセッションを指定します。
interface ethernet *slot/port*	（任意）特定のインターフェイスの EAPoUDP セッションを表示します。
ip-address *ipv4-address*	（任意）特定の IPv4 アドレスの EAPoUDP セッションを表示します。
mac-address *mac-address*	（任意）特定の MAC アドレスの EAPoUDP セッションを表示します。
posturetoken [*name*]	（任意）ポスチャ トークンの EAPoUDP セッションを表示します。
name	（任意）トークン名

デフォルト

グローバル EAPoUDP 設定を表示します。

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、**feature eou** コマンドを使用して 802.1X 機能をイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、すべての 802.1X 機能ステータスおよび設定情報を表示する例を示します。

```
switch# show eou all
```

次に、802.1X クライアントレス認証情報を表示する例を示します。

```
switch# show eou authentication clientless
```

次に、802.1X EAP 認証情報を表示する例を示します。

```
switch# show eou authentication eap
```

次に、802.1X スタティック認証情報を表示する例を示します。

```
switch# show eou interface ethernet 2/1
```

次に、イーサネット インターフェイスの 802.1X 情報を表示する例を示します。

```
switch# show eou ip-address 10.10.10.1
```

次に、MAC アドレスの 802.1X 情報を表示する例を示します。

```
switch# show eou mac-address 0019.076c.dac4
```

次に、MAC アドレスの 802.1X 情報を表示する例を示します。

```
switch# show eou posturetoken healthy
```

関連コマンド

コマンド	説明
feature eou	802.1X 機能をイネーブルにします。

show hardware rate-limit

レート制限の設定と統計情報を表示するには、**show hardware rate-limit** コマンドを使用します。

show rate-limit [**access-list-log** | **copy** | **layer-2 storm-control** | **layer-3** {**control** | **glean** | **mtu** | **multicast** {**directly-connected** | **local-groups** | **rpf-leak**} | **ttl**} | **receive**]

シンタックスの説明

access-list-log	（任意）アクセス リスト ロギング パケットのレート制限統計情報を表示します。
copy	（任意）コピー パケットのレート制限統計情報を表示します。
layer-2 storm-control	（任意）レイヤ 2 ストーム制御パケットのレート制限統計情報を表示します。
layer-3	レイヤ 3 パケットのレート制限を指定します。
control	（任意）レイヤ 3 制御パケットのレート制限統計情報を表示します。
glean	（任意）レイヤ 3 グリーニング パケットのレート制限統計情報を表示します。
mtu	（任意）レイヤ 3 最大伝送ユニット（Maximum Transmission Unit; MTU）パケットのレート制限統計情報を表示します。
multicast	レイヤ 3 マルチキャストのレート制限を指定します。
directly-connected	（任意）レイヤ 3 直接接続マルチキャスト パケットのレート制限統計情報を表示します。
local-groups	（任意）レイヤ 3 ローカル グループ マルチキャスト パケットのレート制限統計情報を表示します。
rpf-leak	（任意）レイヤ 3 Reverse Path Forwarding（RPF）リーク マルチキャスト パケットのレート制限統計情報を表示します。
ttl	（任意）レイヤ 3 Time-to-Live（TTL; 存続可能時間）パケットのレート制限統計情報を表示します。
receive	（任意）受信パケットのレート制限統計情報を表示します。

デフォルト

すべてのレート制限統計情報を表示します。

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、デフォルトの Virtual Device Context（VDC）でのみ使用できます。

このコマンドには、ライセンスは必要ありません。

例

次に、すべてのレート制限設定および統計情報を表示する例を示します。

```
switch# show hardware rate-limit

Units for Config: packets per second
Allowed & Total: aggregated since last clear counters

Rate Limiter Class                      Config          Allowed              Total
--------------------------------------+---------------+--------------------+----------
----
layer-3 mtu                             500             0                    0

layer-3 ttl                             500             0                    0

layer-3 control                         10000           0                    0

layer-3 glean                           100             0                    0

layer-3 multicast directly-connected    10000           0                    0

layer-3 multicast local-groups          10000           0                    0

layer-3 multicast rpf-leak              500             0                    0

layer-2 storm-control                   Disabled
access-list-log                         100             0                    0

copy                                    30000           0                    0

receive                                 30000           0                    0
```

次に、アクセス リスト ロギング パケットのレート制限設定および統計情報を表示する例を示します。

```
switch# show hardware rate-limit access-list-log

Units for Config: packets per second
Allowed & Total: aggregated since last clear counters

Rate Limiter Class                      Config          Allowed              Total
--------------------------------------+---------------+--------------------+----------
----
access-list-log                         100             0                    0
```

関連コマンド

コマンド	説明
platform rate-limit	レート制限を設定します。
show hardware rate-limit	レート制限情報を表示します。

show identity policy

アイデンティティ ポリシーを表示するには、**show identity policy** コマンドを使用します。

show identity policy [*policy-name*]

シンタックスの説明

policy-name	（任意）ポリシーの名前。名前では、大文字と小文字が区別されます。

デフォルト

すべてのアイデンティティ ポリシーの情報を表示します。

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin
VDC user

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、アイデンティティ ポリシーのすべての情報を表示する例を示します。

```
switch# show identity policy
```

次に、特定のアイデンティティ ポリシーの情報を表示する例を示します。

```
switch# show identity policy AdminPolicy
```

関連コマンド

コマンド	説明
identity policy	アイデンティティ ポリシーを設定します。

show identity profile

アイデンティティ ポリシーを表示するには、**show identity profile** コマンドを使用します。

show identity profile [**eapoudp**]

シンタックスの説明

eapoudp	（任意）Extensible Authentication Protocol over User Datagram Protocol（EAPoUDP）アイデンティティ プロファイルを表示します。

デフォルト

すべてのアイデンティティ プロファイルの情報を表示します。

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin
VDC user

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、アイデンティティ プロファイルを表示する例を示します。

```
switch# show identity profile
```

次に、EAPoUDP アイデンティティ プロファイル設定を表示する例を示します。

```
switch# show identity profile eapoudp
```

関連コマンド

コマンド	説明
identity profile eapoudp	EAPoUDP アイデンティティ プロファイルを設定します。

show ip access-lists

すべての IPv4 Access Control List（ACL; アクセス コントロール リスト）または特定の IPv4 ACL を表示するには、**show ip access-lists** コマンドを使用します。

show ip access-lists [*access-list-name*] [**expanded** | **summary**]

シンタックスの説明

access-list-name	（任意）IPv4 ACL の名前。名前では最大で 64 文字の英数字を使用でき、大文字と小文字が区別されます。
expanded	（任意）オブジェクト グループの名前だけでなく、IPv4 アドレス グループまたはポート グループの内容を表示することを指定します。
summary	（任意）コマンドが ACL 設定ではなく、ACL に関する情報を表示することを指定します。詳細については、「使用上のガイドライン」を参照してください。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

access-list-name 引数を使用して ACL を指定する場合を除いて、デバイスはすべての IPv4 ACL を表示します。

expanded キーワードを使用する場合を除いて、IPv4 アドレス オブジェクト グループおよび IP ポート オブジェクト グループは名前だけで表示されます。

expanded キーワードを使用すると、オブジェクト グループの名前だけでなく、ACL で使用されているオブジェクト グループの詳細を表示できます。オブジェクト グループに関する詳細については、**object-group ip address** および **object-group ip port** コマンドを参照してください。

summary キーワードを使用すると、ACL 設定ではなく ACL に関する情報を表示できます。表示される情報には、次の内容が含まれます。

- エントリ単位の統計情報が ACL に対して設定されているかどうか
- ACL 設定内のルール数。この数は、デバイスがインターフェイスに適用されるときに ACL 内に含まれるエントリ数を反映しません。ACL 内のルールがオブジェクト グループを使用する場合、適用されるときの ACL 内のエントリ数は、ルール数よりはるかに大きくなります。
- ACL が適用されているインターフェイス
- ACL がアクティブ状態のインターフェイス

show ip access-lists コマンドは、次の両方の状態が真の場合に、ACL 内の各エントリの統計情報を表示します。

- ACL 設定に **statistics per-entry** コマンドが含まれている

- 管理上アップ状態のインターフェイスに ACL が適用されている

このコマンドには、ライセンスは必要ありません。

例

次に、**show ip access-lists** コマンドを使用して、単一の IPv4 ACL を持つデバイスですべての IPv4 ACL を表示する例を示します。

```
switch# show ip access-lists

IP access list ipv4-open-filter
        10 permit ip any any
```

次に、**show ip access-lists** コマンドを使用して、MainLab オブジェクト グループを除くエントリのエントリ単位の統計情報を含めて、ipv4-RandD-outbound-web という名前の IPv4 ACL を表示する例を示します。

```
switch# show ip access-lists ipv4-RandD-outbound-web

IP access list ipv4-RandD-outbound-web
        statistics per-entry
        1000 permit ahp any any [match=732]
        1005 permit tcp addrgroup MainLab any eq telnet
        1010 permit tcp any any eq www [match=820421]
```

次に、**show ip access-lists** コマンドを使用して、ipv4-RandD-outbound-web という名前の IPv4 ACL を表示する例を示します。**expanded** キーワードを使用すると、エントリ単位の統計情報を含めて、前の例のオブジェクト グループの内容が表示されます。

```
switch# show ip access-lists ipv4-RandD-outbound-web expanded

IP access list ipv4-RandD-outbound-web
        statistics per-entry
        1000 permit ahp any any [match=732]
        1005 permit tcp 10.52.34.4/32 any eq telnet [match=5032]
        1005 permit tcp 10.52.34.27/32 any eq telnet [match=433]
        1010 permit tcp any any eq www [match=820421]
```

次に、**summary** キーワードとともに **show ip access-lists** コマンドを使用して、ACL が適用されているインターフェイス、ACL がアクティブ状態のインターフェイスなどの ipv4-RandD-outbound-web という名前の IPv4 ACL に関する情報を表示する例を示します。

```
switch# show ip access-lists ipv4-RandD-outbound-web summary
IPV4 ACL ipv4-RandD-outbound-web

        Statistics enabled
        Total ACEs Configured: 4
        Configured on interfaces:
                Ethernet2/4 - ingress (Router ACL)
        Active on interfaces:
                Ethernet2/4 - ingress (Router ACL)
```

関連コマンド

コマンド	説明
ip access-list	IPv4 ACL を設定します。
show access-lists	すべての ACL または特定の ACL を表示します。
show mac access-lists	すべての MAC ACL または特定の MAC ACL を表示します。
statistics per-entry	ACL 内の各エントリで許可または拒否されたパケットの統計情報の記録を開始します。

show ip arp inspection

Dynamic ARP Inspection（DAI; ダイナミック ARP インスペクション）設定ステータスを表示するには、**show ip arp inspection** コマンドを使用します。

show ip arp inspection

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト なし

コマンド モード 任意のコマンド モード

サポートされるユーザ ロール network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン このコマンドには、ライセンスは必要ありません。

例 次に、DAI 設定のステータスを表示する例を示します。

```
switch# show ip arp inspection

Source Mac Validation      : Enabled
Destination Mac Validation : Enabled
IP Address Validation      : Enabled

Vlan : 1
-----------
Configuration    : Enabled
Operation State  : Active

ARP Req Forwarded  = 0
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 0
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
```

関連コマンド

コマンド	説明
ip arp inspection vlan	VLAN の指定されたリストの DAI をイネーブルにします。
show ip arp inspection interface	指定されたインターフェイスの信頼状態および ARP パケットレートを表示します。
show ip arp inspection log	DAI ログ設定を表示します。
show ip arp inspection statistics	DAI 統計情報を表示します。
show ip arp inspection vlan	VLAN の指定されたリストの DAI ステータスを表示します。
show running-config dhcp	DAI 設定を含めて、DHCP スヌーピング設定を表示します。

show ip arp inspection interface

指定されたインターフェイスの信頼状態を表示するには、**show ip arp inspection interface** コマンドを使用します。

show ip arp inspection interface {**ethernet** *slot*/*port* | **port-channel** *channel-number*}

シンタックスの説明

ethernet *slot*/*port*	（任意）出力はイーサネット インターフェイス用であることを指定します。
port-channel *channel-number*	（任意）出力はポートチャネル インターフェイス用であることを指定します。有効なポートチャネル番号は、1 ～ 4096 です。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、信頼できるインターフェイスの信頼状態を表示する例を示します。

```
switch# show ip arp inspection interface ethernet 2/1

 Interface        Trust State
 -------------    -----------
 Ethernet2/46        Trusted
switch#
```

関連コマンド

コマンド	説明
ip arp inspection vlan	VLAN の指定されたリストの Dynamic ARP Inspection（DAI; ダイナミック ARP インスペクション）をイネーブルにします。
show ip arp inspection	DAI 設定ステータスを表示します。
show ip arp inspection log	DAI ログ設定を表示します。
show ip arp inspection statistics	DAI 統計情報を表示します。
show ip arp inspection vlan	VLAN の指定されたリストの DAI ステータスを表示します。
show running-config dhcp	DAI 設定を含めて、DHCP スヌーピング設定を表示します。

show ip arp inspection log

Dynamic ARP Inspection（DAI; ダイナミック ARP インスペクション）ログ設定を表示するには、**show ip arp inspection log** コマンドを使用します。

show ip arp inspection log

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、DAI ログ設定を表示する例を示します。

```
switch# show ip arp inspection log

Syslog Buffer Size : 32
Syslog Rate        : 5 entries per 1 seconds
switch#
```

関連コマンド

コマンド	説明
clear ip arp inspection log	DAI ロギング バッファを消去します。
ip arp inspection log-buffer	DAI ロギング バッファ サイズを設定します。
show ip arp inspection	DAI 設定ステータスを表示します。
show ip arp inspection interface	指定されたインターフェイスの信頼状態および ARP パケット レートを表示します。
show running-config dhcp	DAI 設定を含めて、DHCP スヌーピング設定を表示します。

show ip arp inspection statistics

Dynamic ARP Inspection（DAI; ダイナミック ARP インスペクション）統計情報を表示するには、**show ip arp inspection statistics** コマンドを使用します。1 つの VLAN または VLAN の範囲を指定できます。

show ip arp inspection statistics [**vlan** *vlan-list*]

シンタックスの説明

vlan *vlan-list*	（任意）DAI 統計情報を表示する VLAN のリストを指定します。有効な VLAN ID は、1 ～ 4096 です。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、VLAN 1 の DAI 統計情報を表示する例を示します。

```
switch# show ip arp inspection statistics vlan 1

Vlan : 1
-----------
ARP Req Forwarded  = 0
ARP Res Forwarded  = 0
ARP Req Dropped    = 0
ARP Res Dropped    = 0
DHCP Drops         = 0
DHCP Permits       = 0
SMAC Fails-ARP Req = 0
SMAC Fails-ARP Res = 0
DMAC Fails-ARP Res = 0
IP Fails-ARP Req   = 0
IP Fails-ARP Res   = 0
switch#
```

関連コマンド

コマンド	説明
clear ip arp inspection statistics vlan	指定された VLAN の DAI 統計情報を消去します。
show ip arp inspection	DAI 設定ステータスを表示します。
show ip arp inspection interface	指定されたインターフェイスの信頼状態および ARP パケットレートを表示します。
show ip arp inspection log	DAI ログ設定を表示します。
show running-config dhcp	DAI 設定を含めて、DHCP スヌーピング設定を表示します。

show ip arp inspection vlan

指定された VLAN のリストの Dynamic ARP Inspection（DAI; ダイナミック ARP インスペクション）ステータスを表示するには、**show ip arp inspection vlan** コマンドを使用します。

show ip arp inspection vlan *vlan-list*

シンタックスの説明

vlan-list	このコマンドが DAI ステータスを表示する VLAN。*vlan-list* 引数を使用すると、単一の VLAN ID、VLAN ID の範囲、またはカンマで区別された ID および範囲を指定できます（「例」を参照）。有効な VLAN ID は、1 ～ 4096 です。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

例

次に、VLAN 1 および VLAN 13 の DAI ステータスを表示する例を示します。

```
switch# show ip arp inspection vlan 1,13

Source Mac Validation      : Enabled
Destination Mac Validation : Enabled
IP Address Validation      : Enabled

Vlan : 1
-----------
Configuration    : Enabled
Operation State  : Active

Vlan : 13
-----------
Configuration    : Enabled
Operation State  : Inactive
switch#
```

関連コマンド

コマンド	説明
clear ip arp inspection statistics vlan	指定された VLAN の DAI 統計情報を消去します。
ip arp inspection vlan	VLAN の指定されたリストの DAI をイネーブルにします。
show ip arp inspection	DAI 設定ステータスを表示します。
show ip arp inspection interface	指定されたインターフェイスの信頼状態および ARP パケット レートを表示します。
show running-config dhcp	DAI 設定を含めて、DHCP スヌーピング設定を表示します。

show ip device tracking

IP デバイス トラッキング情報を表示するには、**show ip device tracking** コマンドを使用します。

show ip device tracking {**all** | **interface ethernet** *slot*/*port* | **ip-address** *ipv4-address* | **mac-address** *mac-address*}

シンタックスの説明

all	すべての IP デバイス トラッキング情報を表示します。
interface ethernet *slot*/*port*	インターフェイスの IP トラッキング デバイス情報を表示します。
ip-address *ipv4-address*	A.B.C.D フォーマットの IPv4 アドレスの IP トラッキング デバイス情報を表示します。
mac-address *mac-address*	XXXX.XXXX.XXXX フォーマットの MAC アドレスの IP トラッキング情報を表示します。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin
VDC user

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、すべての IP デバイス トラッキング情報を表示する例を示します。

```
switch# show ip device tracking all
```

次に、インターフェイスの IP デバイス トラッキング情報を表示する例を示します。

```
switch# show ip device tracking ethernet 1/2
```

次に、IP アドレスの IP デバイス トラッキング情報を表示する例を示します。

```
switch# show ip device tracking ip-address 10.10.1.1
```

次に、MAC アドレスの IP デバイス トラッキング情報を表示する例を示します。

```
switch# show ip device tracking mac-address 0018.bad8.3fbd
```

関連コマンド

コマンド	説明
ip device tracking	IP デバイス トラッキングを設定します。

show ip dhcp snooping

DHCP スヌーピングの一般ステータス情報を表示するには、**show ip dhcp snooping** コマンドを使用します。

show ip dhcp snooping

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト なし

コマンド モード 任意のコマンド モード

サポートされるユーザ ロール network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン このコマンドには、ライセンスは必要ありません。

例 次に、DHCP スヌーピングに関する一般ステータス情報を表示する例を示します。

```
switch# show ip dhcp snooping
DHCP snooping service is enabled
Switch DHCP snooping is enabled
DHCP snooping is configured on the following VLANs:
1,13
DHCP snooping is operational on the following VLANs:
1
Insertion of Option 82 is disabled
Verification of MAC address is enabled
DHCP snooping trust is configured on the following interfaces:
Interface             Trusted
------------          -------
Ethernet2/3           Yes

switch#
```

関連コマンド

コマンド	説明
feature dhcp	デバイスの DHCP スヌーピング機能をイネーブルにします。
ip dhcp snooping	デバイスの DHCP スヌーピングをグローバルにイネーブルにします。
show ip dhcp snooping binding	スタティック IP ソース エントリを含めて、IP-MAC アドレス バインディングを表示します。
show ip dhcp snooping statistics	DHCP スヌーピング統計情報を表示します。
show running-config dhcp	DHCP スヌーピング設定を表示します。

show ip dhcp snooping binding

すべてのインターフェイスまたは特定のインターフェイスの IP-to-MAC アドレス バインディングを表示するには、**show ip dhcp snooping binding** コマンドを使用します。スタティック IP ソース エントリが含まれます。スタティック エントリは、Type カラムの [static] 用語に表示されます。

show ip dhcp snooping binding [*IP-address*] [*MAC-address*] [**interface ethernet** *slot*/*port*] [**vlan** *vlan-id*]

show ip dhcp snooping binding [**dynamic**]

show ip dhcp snooping binding [**static**]

シンタックスの説明

IP-address	（任意）表示されるバインディングに含める IPv4 アドレス。有効なエントリは、ドット付き 10 進表記です。
MAC-address	（任意）表示されるバインディングに含める MAC アドレス。有効なエントリは、ドット付き 16 進表記です。
interface ethernet *slot*/*port*	（任意）表示されるバインディングに関連付けるイーサネット インターフェイスを指定します。
vlan *vlan-id*	（任意）表示されるバインディングに関連付ける VLAN ID を指定します。有効な VLAN ID は、1 ～ 4096 です。
dynamic	（任意）すべてのダイナミック IP-MAC アドレス バインディングに出力を制限します。
static	（任意）すべてのスタティック IP-MAC アドレス バインディングに出力を制限します。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、すべてのバインディングを表示する例を示します。

```
switch# show ip dhcp snooping binding
MacAddress          IpAddress        LeaseSec  Type         VLAN  Interface
------------------  ---------------  --------  -----------  ----  -------------
0f:00:60:b3:23:33   10.3.2.2         infinite  static       13    Ethernet2/46
0f:00:60:b3:23:35   10.2.2.2         infinite  static       100   Ethernet2/10
switch#
```

関連コマンド

コマンド	説明
clear ip dhcp snooping binding	DHCP スヌーピング バインディング データベースを消去します。
feature dhcp	デバイスの DHCP スヌーピング機能をイネーブルにします。
ip dhcp snooping	デバイスの DHCP スヌーピングをグローバルにイネーブルにします。
service dhcp	DHCP リレー エージェントをイネーブルまたはディセーブルにします。
show ip dhcp snooping	DHCP スヌーピングに関する一般情報を表示します。
show ip dhcp snooping statistics	DHCP スヌーピング統計情報を表示します。
show running-config dhcp	IP ソース ガード設定を含めて、DHCP スヌーピング設定を表示します。

show ip dhcp snooping statistics

DHCP スヌーピング統計情報を表示するには、**show ip dhcp snooping statistics** コマンドを使用します。

show ip dhcp snooping statistics

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト なし

コマンド モード 任意のコマンド モード

サポートされるユーザ ロール network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン このコマンドには、ライセンスは必要ありません。

例 次に、DHCP スヌーピング統計情報を表示する例を示します。

```
switch# show ip dhcp snooping statistics
Packets processed 0
Packets forwarded 0
Total packets dropped 0
Packets dropped from untrusted ports 0
Packets dropped due to MAC address check failure 0
Packets dropped due to Option 82 insertion failure 0
Packets dropped due to o/p intf unknown 0
Packets dropped which were unknown 0
switch#
```

関連コマンド

コマンド	説明
feature dhcp	デバイスの DHCP スヌーピング機能をイネーブルにします。
ip dhcp snooping	デバイスの DHCP スヌーピングをグローバルにイネーブルにします。
service dhcp	DHCP リレー エージェントをイネーブルまたはディセーブルにします。
show ip dhcp snooping	DHCP スヌーピングに関する一般情報を表示します。
show ip dhcp snooping binding	スタティック IP ソース エントリを含めて、IP-MAC アドレス バインディングを表示します。
show running-config dhcp	DHCP スヌーピング設定を表示します。

show ip verify source

IP-to-MAC アドレス バインディングを表示するには、**show ip verify source** コマンドを使用します。

show ip verify source [**interface** {**ethernet** *slot/port* | **port-channel** *channel-number*}]

シンタックスの説明

interface	（任意）出力が特定のインターフェイスの IP-to-MAC アドレス バインディングに制限されていることを指定します。
ethernet *slot/port*	（任意）出力が所定のイーサネット インターフェイスのバインディングに制限されていることを指定します。
port-channel *channel-number*	（任意）出力が所定のポートチャネル インターフェイスのバインディングに制限されていることを指定します。有効なポートチャネル番号は、1 ～ 4096 です。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、IP-to-MAC アドレス バインディングを表示する例を示します。

```
switch# show ip verify source
switch#
```

関連コマンド

コマンド	説明
ip source binding	指定したイーサネット インターフェイスのスタティック IP ソース エントリを作成します。
ip verify source dhcp-snooping-vlan	インターフェイスの IP ソース ガードをイネーブルにします。
show running-config dhcp	IP ソース ガード設定を含めて、DHCP スヌーピング設定を表示します。

show key chain

特定のキーチェーンの設定を表示するには、**show keychain** コマンドを使用します。

show key chain *keychain-name* [**mode decrypt**]

シンタックスの説明

keychain-name	設定するキーチェーンの名前。最大 63 文字の英数字を指定できます。
mode decrypt	（任意）クリアテキストでキー テキスト設定を表示します。このオプションは、network-admin または vdc-admin ユーザ ロールが割り当てられたユーザ アカウントでデバイスにアクセスするときにのみ使用できます。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、特定の受け入れライフタイムおよび送信ライフタイムを持つ 1 つの鍵（鍵 13）を含むキーチェーン glbp-key のキーチェーン設定を表示する例を示します。

```
switch# show key chain
Key-Chain glbp-keys
  Key 13 -- text 7 071a33595c1d0c1702170203163e3e21213c20361a021f11
    accept lifetime UTC (00:00:00 Jun 13 2008) - (23:59:59 Sep 12 2008)
    send lifetime UTC (00:00:00 Jun 13 2008) - (23:59:59 Aug 12 2008)
```

関連コマンド

コマンド	説明
accept-lifetime	鍵の受け入れライフタイムを設定します。
key	鍵を設定します。
key chain	キーチェーンを設定します。
key-string	鍵のストリングを設定します。
send-lifetime	鍵の送信ライフタイムを設定します。

show mac access-lists

すべての MAC Access Control List（ACL; アクセス コントロール リスト）または特定の MAC ACL を表示するには、**show mac access-lists** コマンドを使用します。

show mac access-lists [*access-list-name*] [**summary**]

シンタックスの説明

access-list-name	（任意）MAC ACL の名前。名前では最大で 64 文字の英数字を使用でき、大文字と小文字が区別されます。
summary	（任意）コマンドが ACL 設定ではなく、ACL に関する情報を表示することを指定します。詳細については、「使用上のガイドライン」を参照してください。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

access-list-name 引数を使用して ACL を指定する場合を除いて、デバイスはすべての MAC ACL を表示します。

summary キーワードを使用すると、ACL 設定ではなく ACL に関する情報を表示できます。表示される情報には、次の内容が含まれます。

- エントリ単位の統計情報が ACL に対して設定されているかどうか
- ACL 設定内のルール数。この数は、デバイスがインターフェイスに適用されるときに ACL 内に含まれるエントリ数を反映しません。ACL 内のルールがオブジェクト グループを使用する場合、適用されるときの ACL 内のエントリ数は、ルール数よりはるかに大きくなります。
- ACL が適用されているインターフェイス
- ACL がアクティブ状態のインターフェイス

show mac access-lists コマンドは、次の両方の状態が真の場合に、ACL 内の各エントリの統計情報を表示します。

- ACL 設定に **statistics per-entry** コマンドが含まれている
- 管理上アップ状態のインターフェイスに ACL が適用されている

このコマンドには、ライセンスは必要ありません。

例

次に、**show mac access-lists** コマンドを使用して、単一の MAC ACL を持つデバイスですべての MAC ACL を表示する例を示します。

```
switch# show mac access-lists

MAC access list mac-filter
        10 permit any any ip
```

次に、**show mac access-lists** コマンドを使用して、エントリ単位の統計情報を含めて、mac-lab-filter という名前の MAC ACL を表示する例を示します。

```
switch# show mac access-lists mac-lab-filter

MAC access list mac-lab-filter
        statistics per-entry
        10 permit 0600.ea5f.22ff 0000.0000.0000 any [match=820421]
        20 permit 0600.050b.3ee3 0000.0000.0000 any [match=732]
```

次に、**summary** キーワードとともに **show mac access-lists** コマンドを使用して、ACL が適用されているインターフェイス、ACL がアクティブ状態のインターフェイスなどの mac-lab-filter という名前の MAC ACL に関する情報を表示する例を示します。

```
switch# show mac access-lists mac-lab-filter summary

MAC ACL mac-lab-filter

        Statistics enabled
        Total ACEs Configured: 2
        Configured on interfaces:
                Ethernet2/3 - ingress (Port ACL)
        Active on interfaces:
                Ethernet2/3 - ingress (Port ACL)
```

関連コマンド

コマンド	説明
mac access-list	MAC ACL を設定します。
show access-lists	すべての ACL または特定の ACL を表示します。
show ip access-lists	すべての IPv4 ACL または特定の IPv4 ACL を表示します。

show password strength-check

パスワードの強度の確認ステータスを表示するには、**show password strength-check** コマンドを使用します。

show password strength-check

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト なし

コマンド モード 任意のコマンド モード

サポートされるユーザ ロール network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(3)	このコマンドが導入されました。

使用上のガイドライン このコマンドには、ライセンスは必要ありません。

例 次に、パスワードの強度の確認ステータスを表示する例を示します。

```
switch# show password strength-check
Password strength check enabled
```

関連コマンド

コマンド	説明
password strength-check	パスワードの強度の確認をイネーブルにします。
show running-config security	実行コンフィギュレーションのセキュリティ機能設定を表示します。

show policy-map type control-plane

コントロール プレーン ポリシー マップ情報を表示するには、**show policy-map type control-plane** コマンドを使用します。

show policy-map type control-plane [**expand**] [**name** *policy-map-name*]

シンタックスの説明

expand	（任意）拡張されたコントロール プレーン ポリシー マップ情報を表示します。
name *policy-map-name*	（任意）コントロール プレーン ポリシー マップの名前を指定します。名前では、大文字と小文字が区別されます。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、デフォルトの Virtual Device Context（VDC）でのみ使用できます。

このコマンドには、ライセンスは必要ありません。

例

次に、コントロール プレーン ポリシー マップ情報を表示する例を示します。

```
switch# show policy-map type control-plane

  policy-map type control-plane copp-system-policy
    class copp-system-class-critical
      police cir 2000 kbps bc 1500 bytes pir 3000 kbps be 1500 bytes conform transmit
        exceed transmit violate drop
    class copp-system-class-important
      police cir 1000 kbps bc 1500 bytes pir 1500 kbps be 1500 bytes conform transmit
        exceed transmit violate drop
    class copp-system-class-normal
      police cir 400 kbps bc 1500 bytes pir 600 kbps be 1500 bytes conform transmit
        exceed transmit violate drop
    class class-default
      police cir 200 kbps bc 1500 bytes pir 300 kbps be 1500 bytes conform transmit
        exceed transmit violate drop
```

show radius-server

RADIUS サーバ情報を表示するには、**show radius-server** コマンドを表示します。

show radius-server [*hostname* | *ipv4-address* | *ipv6-address*]
[**directed-request** | **groups** | **sorted** | **statistics**]

シンタックスの説明

hostname	（任意）RADIUS サーバの Domain Name Server（DNS）名。名前では、大文字と小文字が区別されます。
ipv4-address	(任意）*A.B.C.D* フォーマットの RADIUS サーバの IPv4 アドレス
ipv6-address	（任意）*X*:*X*:*X*::*X* フォーマットの RADIUS サーバの IPv6 アドレス
directed-request	（任意）指定要求設定を表示します。
groups	（任意）設定された RADIUS サーバ グループに関する情報を表示します。
sorted	（任意）RADIUS サーバに関する名前でソートされた情報を表示します。
statistics	（任意）RADIUS サーバの RADIUS 統計情報を表示します。

デフォルト

グローバル RADIUS サーバ設定を表示します。

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

RADIUS 事前共有鍵は、**show radius-server** コマンド出力には表示されません。RADIUS 事前共有鍵を表示するには、**show running-config radius** コマンドを使用します。

このコマンドには、ライセンスは必要ありません。

例

次に、すべての RADIUS サーバの情報を表示する例を示します。

```
switch# show radius-server
Global RADIUS shared secret:********
retransmission count:1
timeout value:5
deadtime value:0
total number of servers:2

following RADIUS servers are configured:
        10.10.1.1:
                available for authentication on port:1812
                available for accounting on port:1813
        10.10.2.2:
                available for authentication on port:1812
                available for accounting on port:1813
```

次に、指定された RADIUS サーバの情報を表示する例を示します。

```
switch# show radius-server 10.10.1.1
        10.10.1.1:
                available for authentication on port:1812
                available for accounting on port:1813
                idle time:0
                test user:test
                test password:********
```

次に、RADIUS 指定要求設定を表示する例を示します。

```
switch# show radius-server directed-request
enabled
```

次に、RADIUS サーバ グループの情報を表示する例を示します。

```
switch# show radius-server groups
total number of groups:2

following RADIUS server groups are configured:
        group radius:
                server: all configured radius servers
        group RadServer:
                deadtime is 0
                vrf is management
```

次に、指定された RADIUS サーバ グループの情報を表示する例を示します。

```
switch# show radius-server groups RadServer
        group RadServer:
                deadtime is 0
                vrf is management
```

次に、すべての RADIUS サーバのソートされた情報を表示する例を示します。

```
switch# show radius-server sorted
Global RADIUS shared secret:********
retransmission count:1
timeout value:5
deadtime value:0
total number of servers:2

following RADIUS servers are configured:
        10.10.0.0:
                available for authentication on port:1812
                available for accounting on port:1813
        10.10.1.1:
                available for authentication on port:1812
                available for accounting on port:1813
```

次に、指定された RADIUS サーバの統計情報を表示する例を示します。

```
switch# show radius-server statistics 10.10.1.1
Server is not monitored

Authentication Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0

Accounting Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0
```

関連コマンド

コマンド	説明
show running-config radius	実行コンフィギュレーション ファイルの RADIUS 情報を表示します。

show role

ユーザ ロール設定を表示するには、**show role** コマンドを使用します。

show role [**name** *role-name*]

シンタックスの説明

name *role-name*	（任意）特定のユーザ ロール名の情報を表示します。ロール名では、大文字と小文字が区別されます。

デフォルト

すべてのユーザ ロールの情報を表示します。

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、特定のユーザ ロールの情報を表示する例を示します。

```
switch(config)# show role name MyRole

role: MyRole
  description: new role
  vlan policy: deny
  permitted vlan
  1-10
  interface policy: deny
  permitted interface
  Ethernet2/1-8
  vrf policy: permit (default)
```

次に、デフォルトの Virtual Device Context（VDC）のすべてのユーザ ロールの情報を表示する例を示します。

```
switch(config)# show role

role: network-admin
  description: Predefined network admin role has access to all commands
  on the switch
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read-write
```

```
role: network-operator
  description: Predefined network operator role has access to all read
  commands on the switch
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read

role: vdc-admin
  description: Predefined vdc admin role has access to all commands within
  a VDC instance
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read-write

role: vdc-operator
  description: Predefined vdc operator role has access to all read commands
  within a VDC instance
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read

role: MyRole
  description: new role
  vlan policy: deny
  permitted vlan
  1-10
  interface policy: deny
  permitted interface
  Ethernet2/1-8
  vrf policy: permit (default)
```

次に、デフォルト以外の VDC のすべてのユーザ ロールの情報を表示する例を示します。

```
switch-MyVDC# show role

role: vdc-admin
  description: Predefined vdc admin role has access to all commands within
  a VDC instance
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read-write

role: vdc-operator
  description: Predefined vdc operator role has access to all read commands
  within a VDC instance
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read
```

関連コマンド

コマンド	説明
role name	ユーザ ロールを設定します。

show role feature

ユーザ ロール機能を表示するには、**show role feature** コマンドを使用します。

show role feature [**detail** | **name** *feature-name*]

シンタックスの説明

detail	（任意）すべての機能の詳細情報を表示します。
name *feature-name*	（任意）特定の機能の詳細情報を表示します。機能名では、大文字と小文字が区別されます。

デフォルト

ユーザ ロール機能名のリストを表示します。

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、ユーザ ロール機能を表示する例を示します。

```
switch(config)# show role feature
feature: aaa
feature: access-list
feature: arp
feature: callhome
feature: cdp
feature: crypto
feature: gold
feature: install
feature: l3vm
feature: license
feature: ping
feature: platform
feature: qosmgr
feature: radius
feature: scheduler
feature: snmp
feature: syslog
（テキスト出力は省略）
```

次に、すべてのユーザ ロール機能の詳細情報を表示する例を示します。

```
switch(config)# show role feature detail
feature: aaa
  show aaa *
  config t ; aaa *
  aaa *
  clear aaa *
  debug aaa *
  show accounting *
  config t ; accounting *
  accounting *
  clear accounting *
  debug accounting *
feature: access-list
  show ip access-list *
  show ipv6 access-list *
  show mac access-list *
  show arp access-list *
  show vlan access-map *
  config t ; ip access-list *
  config t ; ipv6 access-list *
  config t ; mac access-list *
  config t ; arp access-list *
  config t ; vlan access-map *
  clear ip access-list *
  clear ipv6 access-list *
  clear mac access-list *
  clear arp access-list *
  clear vlan access-map *
  debug aclmgr *
feature: arp
  show arp *
  show ip arp *
  config t; ip arp *
  clear ip arp *
  debug ip arp *
  debug-filter ip arp *
（テキスト出力は省略）
```

次に、特定のユーザ ロール機能の詳細情報を表示する例を示します。

```
switch(config)# show role feature name dot1x
feature: dot1x
  show dot1x *
  config t ; dot1x *
  dot1x *
  clear dot1x *
  debug dot1x *
```

関連コマンド

コマンド	説明
role feature-group	ユーザ ロールの機能グループを設定します。
rule	ユーザ ロールのルールを設定します。

show role feature-group

ユーザ ロール機能グループを表示するには、**show role feature-group** コマンドを使用します。

show role feature-group [**detail** | **name** *group-name*]

シンタックスの説明

detail	（任意）すべての機能グループの詳細情報を表示します。
name *group-name*	（任意）特定の機能グループの詳細情報を表示します。グループ名では、大文字と小文字が区別されます。

デフォルト

ユーザ ロール機能グループのリストを表示します。

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、ユーザ ロール機能グループを表示する例を示します。

```
switch(config)# show role feature-group

feature group: L3
feature: router-bgp
feature: router-eigrp
feature: router-isis
feature: router-ospf
feature: router-rip

feature group: SecGroup
feature: aaa
feature: radius
feature: tacacs
```

次に、すべてのユーザ ロール機能グループに関する詳細情報を表示する例を示します。

```
switch(config)# show role feature-group detail

feature group: L3
feature: router-bgp
  show bgp *
  config t ; bgp *
  bgp *
  clear bgp *
  debug bgp *
  show ip bgp *
  show ip mbgp *
  show ipv6 bgp *
  show ipv6 mbgp *
  clear ip bgp *
  clear ip mbgp *
  debug-filter ip *
  debug-filter ip bgp *
  config t ; router bgp *
feature: router-eigrp
  show eigrp *
  config t ; eigrp *
  eigrp *
  clear eigrp *
  debug eigrp *
  show ip eigrp *
  clear ip eigrp *
  debug ip eigrp *
  config t ; router eigrp *
feature: router-isis
  show isis *
  config t ; isis *
  isis *
  clear isis *
  debug isis *
  debug-filter isis *
  config t ; router isis *
feature: router-ospf
  show ospf *
  config t ; ospf *
  ospf *
  clear ospf *
  debug ospf *
  show ip ospf *
  show ospfv3 *
  show ipv6 ospfv3 *
  debug-filter ip ospf *
  debug-filter ospfv3 *
  debug ip ospf *
  debug ospfv3 *
  clear ip ospf *
  clear ip ospfv3 *
  config t ; router ospf *
  config t ; router ospfv3 *
feature: router-rip
  show rip *
  config t ; rip *
  rip *
  clear rip *
  debug rip *
  show ip rip *
  show ipv6 rip *
  overload rip *
  debug-filter rip *
  clear ip rip *
  clear ipv6 rip *
  config t ; router rip *
```

次に、特定のユーザ ロール機能グループの情報を表示する例を示します。

```
switch(config)# show role feature-group name SecGroup

feature group: SecGroup
feature: aaa
feature: radius
feature: tacacs
```

関連コマンド

コマンド	説明
role feature-group	ユーザ ロールの機能グループを設定します。
rule	ユーザ ロールのルールを設定します。

show running-config aaa

実行コンフィギュレーションの Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）設定情報を表示するには、**show running-config aaa** コマンドを使用します。

show running-config aaa [**all**]

シンタックスの説明

all	（任意）設定済みおよびデフォルトの情報を表示します。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、実行コンフィギュレーションの設定済み AAA 情報を表示する例を示します。

```
switch# show running-config aaa
version 4.0(1)
```

show running-config copp

実行コンフィギュレーションのコントロール プレーン ポリシング設定情報を表示するには、**show running-config copp** コマンドを使用します。

show running-config copp [**all**]

シンタックスの説明

all	（任意）設定済みおよびデフォルトの情報を表示します。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、デフォルトの Virtual Device Context（VDC）でのみ使用できます。

このコマンドには、ライセンスは必要ありません。

例

次に、実行コンフィギュレーションの設定済みコントロール プレーン ポリシング情報を表示する例を示します。

```
switch# show running-config copp
version 4.0(1)
class-map type control-plane match-any copp-system-class-critical
  match access-group name copp-system-acl-arp
  match access-group name copp-system-acl-msdp
class-map type control-plane match-any copp-system-class-important
  match access-group name copp-system-acl-gre
  match access-group name copp-system-acl-tacas
class-map type control-plane match-any copp-system-class-normal
  match access-group name copp-system-acl-icmp
  match redirect dhcp-snoop
  match redirect arp-inspect
  match exception ip option
  match exception ip icmp redirect
  match exception ip icmp unreachable
policy-map type control-plane copp-system-policy
  class copp-system-class-critical
    police cir 2000 kbps bc 1500 bytes pir 3000 kbps be 1500 bytes conform transmit
exceed transmit violate drop
  class copp-system-class-important
    police cir 1000 kbps bc 1500 bytes pir 1500 kbps be 1500 bytes conform transmit
exceed transmit violate drop
  class copp-system-class-normal
    police cir 400 kbps bc 1500 bytes pir 600 kbps be 1500 bytes conform transmit
exceed transmit violate drop
  class class-default
    police cir 200 kbps bc 1500 bytes pir 300 kbps be 1500 bytes conform transmit
exceed transmit violate drop
```

次に、実行コンフィギュレーションの設定済みおよびデフォルトのコントロール プレーン ポリシング情報を表示する例を示します。

```
switch# show running-config copp all
version 4.0(1)
class-map type control-plane match-any copp-system-class-critical
  match access-group name copp-system-acl-arp
  match access-group name copp-system-acl-msdp
class-map type control-plane match-any copp-system-class-important
  match access-group name copp-system-acl-gre
  match access-group name copp-system-acl-tacas
class-map type control-plane match-any copp-system-class-normal
  match access-group name copp-system-acl-icmp
  match redirect dhcp-snoop
  match redirect arp-inspect
  match exception ip option
  match exception ip icmp redirect
  match exception ip icmp unreachable
policy-map type control-plane copp-system-policy
  class copp-system-class-critical
    police cir 2000 kbps bc 1500 bytes pir 3000 kbps be 1500 bytes conform transmit
exceed transmit violate drop
  class copp-system-class-important
    police cir 1000 kbps bc 1500 bytes pir 1500 kbps be 1500 bytes conform transmit
exceed transmit violate drop
  class copp-system-class-normal
    police cir 400 kbps bc 1500 bytes pir 600 kbps be 1500 bytes conform transmit
exceed transmit violate drop
  class class-default
    police cir 200 kbps bc 1500 bytes pir 300 kbps be 1500 bytes conform transmit
exceed transmit violate drop
```

show running-config cts

実行コンフィギュレーションの Cisco TrustSec 設定を表示するには、**show running-config cts** コマンドを使用します。

show running-config cts

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト なし

コマンド モード 任意のコンフィギュレーション モード

サポートされるユーザ ロール network-admin
vdc-admin
network-operator
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン このコマンドを使用するには、**feature cts** コマンドを使用して Cisco TrustSec 機能をイネーブルにする必要があります。

このコマンドには、Advanced Services ライセンスが必要です。

例 次に、実行コンフィギュレーションの Cisco TrustSec 設定を表示する例を示します。

```
switch# show running-config cts
version 4.0(1)
feature cts
cts role-based enforcement
cts role-based sgt-map 10.10.1.1 10
cts role-based access-list MySGACL
  permit icmp
cts role-based sgt 65535 dgt 65535 access-list MySGACL
cts sxp enable
cts sxp connection peer 10.10.3.3 source 10.10.2.2 password default mode listener
vlan 1
  cts role-based enforcement
vrf context MyVRF
  cts role-based enforcement
```

関連コマンド

コマンド	説明
feature cts	Cisco TrustSec 機能をイネーブルにします。

show running-config dhcp

実行コンフィギュレーションの DHCP スヌーピング設定を表示するには、**show running-config dhcp** コマンドを使用します。

show running-config dhcp [**all**]

シンタックスの説明

all	（任意）設定済みおよびデフォルトの情報を表示します。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin
network-operator
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature dhcp** コマンドを使用して DHCP スヌーピング機能をイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、DHCP スヌーピング情報を表示する例を示します。

```
switch# show running-config dhcp
version 4.0(1)
feature dhcp

interface Ethernet2/46
  ip verify source dhcp-snooping-vlan
  ip arp inspection trust
ip dhcp snooping
ip arp inspection validate src-mac dst-mac ip
ip source binding 10.3.2.2 0f00.60b3.2333 vlan 13 interface Ethernet2/46
ip source binding 10.2.2.2 0060.3454.4555 vlan 100 interface Ethernet2/10
ip dhcp snooping vlan 1
ip arp inspection vlan 1
ip dhcp snooping vlan 13
ip arp inspection vlan 13

switch#
```

関連コマンド

コマンド	説明
feature dhcp	デバイスの DHCP スヌーピング機能をイネーブルにします。
ip dhcp snooping	デバイスの DHCP スヌーピングをグローバルにイネーブルにします。
service dhcp	DHCP リレー エージェントをイネーブルまたはディセーブルにします。
show ip dhcp snooping	DHCP スヌーピングに関する一般情報を表示します。
show ip dhcp snooping binding	スタティック IP ソース エントリを含めて、IP-MAC アドレス バインディングを表示します。

show running-config dot1x

実行コンフィギュレーションの 802.1X 設定情報を表示するには、**show running-config dot1x** コマンドを使用します。

show running-config dotx1 [**all**]

シンタックスの説明

all	（任意）設定済みおよびデフォルトの情報を表示します。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、**feature dot1x** コマンドを使用して 802.1X 機能をイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、実行コンフィギュレーションの設定済み 802.1X 情報を表示する例を示します。

```
switch# show running-config dot1x
version 4.0(1)
```

show running-config eou

実行コンフィギュレーションの Extensible Authentication Protocol over User Datagram Protocol（EAPoUDP）設定情報を表示するには、**show running-config eou** コマンドを使用します。

show running-config eou [**all**]

シンタックスの説明

all	（任意）設定済みおよびデフォルトの情報を表示します。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、**feature eou** コマンドを使用して EAPoUDP 機能をイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、実行コンフィギュレーションの設定済み EAPoUDP 情報を表示する例を示します。

```
switch# show running-config eou
version 4.0(1)
```

show running-config port-security

実行コンフィギュレーションのポートセキュリティ情報を表示するには、**show running-config port-security** コマンドを使用します。

show running-config port-security [**all**]

シンタックスの説明

all	（任意）デフォルトのポートセキュリティ設定情報を表示します。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(3)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、実行コンフィギュレーションのポートセキュリティの情報を表示する例を示します。

```
switch# show running-port-security
version 4.0(3)
feature port-security
logging level port-security 5

interface Ethernet2/3
  switchport port-security
```

関連コマンド

コマンド	説明
show startup-config port-security	スタートアップ コンフィギュレーションのポートセキュリティ情報を表示します。

show running-config radius

実行コンフィギュレーションの RADIUS サーバ情報を表示するには、**show running-config radius** コマンドを使用します。

show running-config radius [**all**]

シンタックスの説明

all	（任意）デフォルトの RADIUS 設定情報を表示します。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、実行コンフィギュレーションの RADIUS の情報を表示する例を示します。

```
switch# show running-config radius
```

関連コマンド

コマンド	説明
show radius-server	RADIUS 情報を表示します。

show running-config security

実行コンフィギュレーションのユーザ アカウント、SSH サーバ、および Telnet サーバ情報を表示するには、**show running-config security** コマンドを使用します。

show running-config security [**all**]

シンタックスの説明

all	（任意）デフォルトのユーザ アカウント、SSH サーバ、および Telnet サーバ設定情報を表示します。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、実行コンフィギュレーションのユーザ アカウント、SSH サーバ、および Telnet サーバ情報を表示する例を示します。

```
switch# show running-config security
version 4.0(1)
username admin password 5 $1$7Jwq/LDM$XF0M/UWeT43DmtjZy8VP91  role network-admin
username adminbackup password 5 $1$Oip/C5Ci$oOdx7oJSlBCFpNRmQK4na.  role
network-operator
username user1 password 5 $1$qEclQ5Rx$CAX9fXiAoFPYSvbVzpazj/  role network-operator
telnet server enable
ssh key rsa 768 force
```

show running-config tacacs+

実行コンフィギュレーションの TACACS+ サーバ情報を表示するには、**show running-config tacacs+** コマンドを使用します。

show running-config tacacs+ [**all**]

シンタックスの説明

all	（任意）デフォルトの TACACS+ 設定情報を表示します。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

TACACS+ 情報を表示する前に、**feature tacacs+** コマンドを使用する必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、実行コンフィギュレーションの TACACS+ 情報を表示する例を示します。

```
switch# show running-config tacacs+
```

関連コマンド

コマンド	説明
show tacacs-server	TACACS+ 情報を表示します。

show ssh key

Virtual Device Contex（VDC）の Secure Shell（SSH; セキュア シェル）サーバ鍵を表示するには、**show ssh key** コマンドを使用します。

show ssh key

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト なし

コマンド モード 任意のコマンド モード

サポートされるユーザ ロール network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン このコマンドは、**ssh server enable** コマンドを使用して SSH がイネーブルのときにのみ使用できます。

このコマンドには、ライセンスは必要ありません。

例 次に、SSH サーバ鍵を表示する例を示します。

```
switch# show ssh key
**************************************
rsa Keys generated:Mon Mar 17 15:02:44 2008

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAGEAqyiGkvwk0xyAXUl/OmeIrSq0QIYYYD1oO5F2lwDjfkVQfOq8Sl0q6LW4Uv
5+0m1vvUjoI002SsdG7tCA6VpGtD/cuPTdQSMpdu6MF9H2TYTuC5TyFGYiLf/0vYTeHe+9

bitcount:768
fingerprint:
9b:d9:09:97:f6:40:76:89:05:15:42:6b:12:48:0f:d6
**************************************
could not retrieve dsa key information
**************************************
```

関連コマンド

コマンド	説明
ssh server key	SSH サーバ鍵を設定します。

show ssh server

Virtual Device Contex（VDC）の Secure Shell（SSH; セキュア シェル）サーバ ステータスを表示するには、**show ssh server** コマンドを使用します。

show ssh server

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト なし

コマンド モード 任意のコマンド モード

サポートされるユーザ ロール network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン このコマンドには、ライセンスは必要ありません。

例 次に、SSH サーバ ステータスを表示する例を示します。

```
switch# show ssh server
ssh is enabled
version 2 enabled
```

関連コマンド

コマンド	説明
ssh server enable	SSH サーバをイネーブルにします。

show startup-config aaa

スタートアップ コンフィギュレーションの Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）設定情報を表示するには、**show startup-config aaa** コマンドを使用します。

show startup-config aaa

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、スタートアップ コンフィギュレーションの AAA 情報を表示する例を示します。

```
switch# show startup-config aaa
version 4.0(1)
```

show startup-config copp

スタートアップ コンフィギュレーションのコントロール プレーン ポリシング設定情報を表示するには、**show startup-config copp** コマンドを使用します。

show startup-config copp

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト なし

コマンド モード 任意のコマンド モード

サポートされるユーザ ロール network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン このコマンドは、デフォルトの Virtual Device Context（VDC）でのみ使用できます。

このコマンドには、ライセンスは必要ありません。

例

次に、スタートアップ コンフィギュレーションのコントロール プレーン ポリシング情報を表示する例を示します。

```
switch# show startup-config copp
version 4.0(1)
class-map type control-plane match-any MyClassMap
  match redirect dhcp-snoop
class-map type control-plane match-any copp-system-class-critical
  match access-group name copp-system-acl-arp
  match access-group name copp-system-acl-msdp
class-map type control-plane match-any copp-system-class-important
  match access-group name copp-system-acl-gre
  match access-group name copp-system-acl-tacas
class-map type control-plane match-any copp-system-class-normal
  match access-group name copp-system-acl-icmp
  match redirect dhcp-snoop
  match redirect arp-inspect
  match exception ip option
  match exception ip icmp redirect
  match exception ip icmp unreachable
policy-map type control-plane MyPolicyMap
  class MyClassMap
    police cir 0 bps bc 0 bytes conform drop violate drop
policy-map type control-plane copp-system-policy
  class copp-system-class-critical
    police cir 2000 kbps bc 1500 bytes pir 3000 kbps be 1500 bytes conform transmit
exceed transmit violate drop
  class copp-system-class-important
    police cir 1000 kbps bc 1500 bytes pir 1500 kbps be 1500 bytes conform transmit
exceed transmit violate drop
  class copp-system-class-normal
    police cir 400 kbps bc 1500 bytes pir 600 kbps be 1500 bytes conform transmit
exceed transmit violate drop
  class class-default
    police cir 200 kbps bc 1500 bytes pir 300 kbps be 1500 bytes conform transmit
exceed transmit violate drop
policy-map type control-plane x
  class class-default
    police cir 0 bps bc 0 bytes conform drop violate drop
```

show startup-config dhcp

スタートアップ コンフィギュレーションの DHCP スヌーピング設定を表示するには、**show startup-config dhcp** コマンドを使用します。

show startup-config dhcp [**all**]

シンタックスの説明

all	（任意）設定済みおよびデフォルトの情報を表示します。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin
network-operator
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**feature dhcp** コマンドを使用して DHCP スヌーピング機能をイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、スタートアップ コンフィギュレーションの DHCP スヌーピング設定を表示する例を示します。

```
switch# show startup-config dhcp
version 4.0(1)
feature dhcp

interface Ethernet2/46
  ip verify source dhcp-snooping-vlan
  ip arp inspection trust
ip dhcp snooping
ip arp inspection validate src-mac dst-mac ip
ip source binding 10.3.2.2 0f00.60b3.2333 vlan 13 interface Ethernet2/46
ip source binding 10.2.2.2 0060.3454.4555 vlan 100 interface Ethernet2/10
ip dhcp snooping vlan 1
ip arp inspection vlan 1
ip dhcp snooping vlan 13
ip arp inspection vlan 13

switch#
```

関連コマンド

コマンド	説明
feature dhcp	デバイスの DHCP スヌーピング機能をイネーブルにします。
show running-config dhcp	実行コンフィギュレーションの DHCP スヌーピング設定を表示します。

show startup-config dot1x

スタートアップ コンフィギュレーションの 802.1X 設定情報を表示するには、**show startup-config dot1x** コマンドを使用します。

show startup-config dot1x

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、**feature dot1x** コマンドを使用して 802.1X 機能をイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、スタートアップ コンフィギュレーションの 802.1X 情報を表示する例を示します。

```
switch# show startup-config dot1x
version 4.0(1)
```

show startup-config eou

スタートアップ コンフィギュレーションの Extensible Authentication Protocol over User Datagram Protocol（EAPoUDP）設定情報を表示するには、**show startup-config eou** コマンドを使用します。

show startup-config eou

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する前に、**feature eou** コマンドを使用して EAPoUDP 機能をイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、スタートアップ コンフィギュレーションの EAPoUDP 情報を表示する例を示します。

```
switch# show startup-config eou
version 4.0(1)
```

show startup-config port-security

スタートアップ コンフィギュレーションのポートセキュリティ情報を表示するには、**show startup-config port-security** コマンドを使用します。

show startup-config port-security [**all**]

シンタックスの説明

all	（任意）デフォルトのポートセキュリティ設定情報を表示します。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(3)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、スタートアップ コンフィギュレーションのポートセキュリティの情報を表示する例を示します。

```
switch# show startup-port-security
version 4.0(3)
feature port-security
logging level port-security 5

interface Ethernet2/3
  switchport port-security
```

関連コマンド

コマンド	説明
show running-config port-security	実行コンフィギュレーションのポートセキュリティ情報を表示します。

show startup-config radius

スタートアップ コンフィギュレーションの RADIUS 設定情報を表示するには、**show startup-config radius** コマンドを使用します。

show startup-config radius

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、スタートアップ コンフィギュレーションの RADIUS 情報を表示する例を示します。

```
switch# show startup-config radius
version 4.0(1)
```

show startup-config security

スタートアップ コンフィギュレーションのユーザ アカウント、Secure Shell（SSH; セキュア シェル）サーバ、および Telnet サーバ設定情報を表示するには、**show startup-config security** コマンドを使用します。

show startup-config security

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、スタートアップ コンフィギュレーションのユーザ アカウント、SSH サーバ、および Telnet サーバ情報を表示する例を示します。

```
switch# show startup-config security
version 4.0(1)
username admin password 5 $1$7Jwq/LDM$XF0M/UWeT43DmtjZy8VP91  role network-admin
username adminbackup password 5 $1$Oip/C5Ci$oOdx7oJSlBCFpNRmQK4na.  role
network-operator
username user1 password 5 $1$qEclQ5Rx$CAX9fXiAoFPYSvbVzpazj/  role network-operator
telnet server enable
ssh key rsa 768 force
```

show startup-config tacacs+

スタートアップ コンフィギュレーションの TACACS+ 設定情報を表示するには、**show startup-config tacacs+** コマンドを使用します。

show startup-config tacacs+

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト なし

コマンド モード 任意のコマンド モード

サポートされるユーザ ロール network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン このコマンドには、ライセンスは必要ありません。

例 次に、スタートアップ コンフィギュレーションの TACACS+ 情報を表示する例を示します。

```
switch# show startup-config tacacs+
version 4.0(1)
```

show tacacs-server

TACACS+ サーバ情報を表示するには、**show tacacs-server** コマンドを表示します。

show tacacs-server [*hostname* | *ip4-address* | *ipv6-address*]
[**directed-request** | **groups** | **sorted** | **statistics**]

シンタックスの説明

hostname	（任意）TACACS+ サーバの Domain Name Server（DNS）名。最大文字サイズは 256 です。
ipv4-address	（任意）*A.B.C.D* フォーマットの TACACS+ サーバの IPv4 アドレス
ipv6-address	（任意）*X*:*X*:*X*::*X* フォーマットの TACACS+ サーバの IPv6 アドレス
directed-request	（任意）指定要求設定を表示します。
groups	（任意）設定された TACACS+ サーバ グループに関する情報を表示します。
sorted	（任意）TACACS+ サーバに関する名前でソートされた情報を表示します。
statistics	（任意）TACACS+ サーバの TACACS+ 統計情報を表示します。

デフォルト

グローバル TACACS+ サーバ設定を表示します。

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

TACACS+ 事前共有鍵は、**show tacacs-server** コマンド出力には表示されません。TACACS+ 事前共有鍵を表示するには、**show running-config tacacs+** コマンドを使用します。

TACACS+ 情報を表示する前に、**feature tacacs+** コマンドを使用する必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、すべての TACACS+ サーバの情報を表示する例を示します。

```
switch# show tacacs-server
Global TACACS+ shared secret:********
timeout value:5
deadtime value:0
total number of servers:2

following TACACS+ servers are configured:
        10.10.2.2:
                available on port:49
        10.10.1.1:
                available on port:49
```

次に、指定された TACACS+ サーバの情報を表示する例を示します。

```
switch# show tacacs-server 10.10.2.2
        10.10.2.2:
                available for authentication on port:1812
                available for accounting on port:1813
                idle time:0
                test user:test
                test password:********
```

次に、TACACS+ 指定要求設定を表示する例を示します。

```
switch# show tacacs-server directed-request
enabled
```

次に、TACACS+ サーバ グループの情報を表示する例を示します。

```
switch# show tacacs-server groups
total number of groups:1

following TACACS+ server groups are configured:
        group TacServer:
                server 10.10.2.2 on port 49
                deadtime is 0
                vrf is vrf3
```

次に、指定された TACACS+ サーバ グループの情報を表示する例を示します。

```
switch# show tacacs-server groups TacServer
        group TacServer:
                server 10.10.2.2 on port 49
                deadtime is 0
                vrf is vrf3
```

次に、すべての TACACS+ サーバのソートされた情報を表示する例を示します。

```
switch# show tacacs-server sorted
Global TACACS+ shared secret:********
timeout value:5
deadtime value:0
total number of servers:2

following TACACS+ servers are configured:
        10.10.1.1:
                available on port:49
        10.10.2.2:
                available on port:49
```

次に、指定された TACACS+ サーバの統計情報を表示する例を示します。

```
switch# show tacacs-server statistics 10.10.2.2
Server is not monitored

Authentication Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0

Authorization Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0

Accounting Statistics
        failed transactions: 0
        sucessfull transactions: 0
        requests sent: 0
        requests timed out: 0
        responses with no matching requests: 0
        responses not processed: 0
        responses containing errors: 0
```

関連コマンド

コマンド	説明
show running-config tacacs+	実行コンフィギュレーション ファイルの TACACS+ 情報を表示します。

show telnet server

Virtual Device Context（VDC）の Telnet サーバ ステータスを表示するには、**show telnet server** コマンドを使用します。

show telnet server

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、Telnet サーバ ステータスを表示する例を示します。

```
switch# show telnet server
telnet service enabled
```

関連コマンド

コマンド	説明
telnet server enable	telnet サーバをイネーブルにします。

show user-account

Virtual Device Context（VDC）のユーザ アカウントの情報を表示するには、**show user-account** コマンドを使用します。

show user-account

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、デフォルトの Virtual Device Context（VDC）のユーザ アカウントの情報を表示する例を示します。

```
switch# show user-account
user:admin
        this user account has no expiry date
        roles:network-admin
user:adminbackup
        this user account has no expiry date
        roles:network-operator
```

次に、デフォルト以外の VDC のユーザ アカウントの情報を表示する例を示します。

```
switch-MyVDC# show user-account
user:admin
        this user account has no expiry date
        roles:vdc-admin
```

関連コマンド

コマンド	説明
telnet server enable	telnet サーバをイネーブルにします。

show users

Virtual Device Context（VDC）のユーザ セッション情報を表示するには、**show users** コマンドを使用します。

show users

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト なし

コマンド モード 任意のコマンド モード

サポートされるユーザ ロール network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン このコマンドには、ライセンスは必要ありません。

例 次に、デフォルトの VDC のユーザ セッション情報を表示する例を示します。

```
switch# show users
NAME     LINE         TIME         IDLE          PID COMMENT
admin    pts/1        Mar 17 15:18   .          5477 (172.28.254.254)
admin    pts/9        Mar 19 11:19   .         23101 (10.82.234.56)*
```

次に、デフォルト以外の VDC のユーザ アカウントの情報を表示する例を示します。

```
switch-MyVDC# show users
admin     pts/10       Mar 19 12:54   .         30965 (10.82.234.56)*
```

関連コマンド

コマンド	説明
username	ユーザ アカウントを設定します。

show vlan access-list

IPv4 Access Control List（ACL; アクセス コントロール リスト）の内容または特定の VLAN アクセス マップに関連付けられている MAC ACL を表示するには、**show vlan access-list** コマンドを使用します。

show vlan access-list *access-list-name*

シンタックスの説明

access-list-name	VLAN アクセス マップの名前。名前では最大で 64 文字の英数字を使用でき、大文字と小文字が区別されます。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、**show vlan access-list** コマンドを使用して、vacl-01 という名前の VLAN アクセス マップが使用されるように設定されている ACL の内容を表示する例を示します。

```
switch# show vlan access-list vacl-01

IP access list ipv4acl
        5 deny ip 10.1.1.1/32 any
        10 permit ip any any
```

関連コマンド

コマンド	説明
vlan access-map	VLAN アクセス マップを設定します。
show access-lists	すべての ACL または特定の ACL を表示します。
show ip access-lists	すべての IPv4 ACL または特定の IPv4 ACL を表示します。
show mac access-lists	すべての MAC ACL または特定の MAC ACL を表示します。
show vlan access-map	すべての VLAN アクセス マップまたは特定の VLAN アクセス マップを表示します。

show vlan access-map

すべての VLAN アクセス マップまたは 1 つの VLAN アクセス マップを表示するには、**show vlan access-map** コマンドを使用します。

show vlan access-map *map-name*

シンタックスの説明

map-name	VLAN アクセス マップ。最大で 64 文字の英数字を使用でき、大文字と小文字が区別されます。

デフォルト

なし

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

map-name 引数を使用してアクセス マップを指定する場合を除いて、デバイスはすべての VLAN アクセス マップを表示します。

表示される各 VLAN アクセス マップに対して、デバイスはアクセスマップ名、**match** コマンドで指定された ACL、および **action** コマンドで指定された処理を表示します。

VLAN アクセス マップが適用されている VLAN を確認するには、**show vlan filter** コマンドを使用します。

このコマンドには、ライセンスは必要ありません。

例

次に、イーサネット 2/1 インターフェイスから動的に学習されたセキュア MAC アドレスを削除する例を示します。

```
switch# show vlan access-map

Vlan access-map austin-vlan-map

        match ip: austin-corp-acl
        action: forward
```

関連コマンド

コマンド	説明
action	VLAN アクセス マップにトラフィック フィルタリングの処理を指定します。
match	VLAN アクセス マップにトラフィック フィルタリングの ACL を指定します。
show vlan filter	VLAN アクセス マップが適用されている方法に関する情報を表示します。
vlan access-map	VLAN アクセス マップを設定します。
vlan filter	1 つまたは複数の VLAN に VLAN アクセス マップを適用します。

show vlan filter

コマンドによって影響される VLAN アクセスマップおよび VLAN ID を含めて、**vlan filter** コマンドのインスタンスに関する情報を表示するには、**show vlan filter** コマンドを使用します。

show vlan filter [**access-map** *map-name* | **vlan** *vlan-ID*]

シンタックスの説明

access-map *map-name*	（任意）指定されたアクセス マップが適用されている VLAN に出力を制限します。
vlan *vlan-ID*	（任意）指定された VLAN にのみ適用されているアクセス マップに出力を制限します。有効な VLAN ID は、1 ～ 4096 です。

デフォルト

access-map キーワードを使用してアクセス マップを指定する場合、または ***vlan*** キーワードを使用して VLAN ID を指定する場合を除いて、デバイスは VLAN に適用されている VLAN アクセス マップのすべてのインスタンスを表示します。

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
network-operator
vdc-admin
vdc-operator

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、1 つの VLAN アクセス マップ（austin-vlan-map）だけが VLAN 20 ～ 35 および 42 ～ 80 に適用されているデバイスのすべての VLAN アクセス マップ情報を表示する例を示します。

```
switch# show vlan filter

vlan map austin-vlan-map:
        Configured on VLANs:    20-35,42-80
```

関連コマンド

コマンド	説明
action	VLAN アクセス マップにトラフィック フィルタリングの処理を指定します。
match	VLAN アクセス マップにトラフィック フィルタリングの ACL を指定します。
show vlan access-map	すべての VLAN アクセス マップまたは 1 つの VLAN アクセス マップを表示します。
vlan access-map	VLAN アクセス マップを設定します。
vlan filter	1 つまたは複数の VLAN に VLAN アクセス マップを適用します。

T コマンド

この章では、T で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

tacacs-server deadtime

応答性について到達不能（非応答）TACACS+ サーバを監視する定期的な時間間隔を設定するには、**tacacs-server deadtime** コマンドを使用します。非応答 TACACS+ サーバのモニタリングをディセーブルにするには、このコマンドの **no** 形式を使用します。

tacacs-server deadtime *minutes*

no tacacs-server deadtime *minutes*

シンタックスの説明

time	時間間隔を分で指定します。範囲は 1 ～ 1440 です。

デフォルト

0 分

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

時間間隔の設定をゼロにすると、タイマーがディセーブルになります。個別の TACACS+ サーバのデッド タイム間隔がゼロ（0）よりも大きい場合は、サーバ グループに設定された値よりもその値が優先されます。

デッド タイム間隔が 0 分の場合、TACACS+ サーバがサーバ グループの一部でグループのデット時間間隔が 0 分を超えていない限り、TACACS+ サーバ モニタリングは実行されません。

TACACS+ を設定する前に、**feature tacacs+** コマンドを使用する必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、デッド タイム間隔を設定して、定期的なモニタリングをイネーブルにする例を示します。

```
switch# config terminal
switch(config)# tacacs-server deadtime 10
```

次に、デッド タイム間隔をデフォルトに戻して、定期的なモニタリングをディセーブルにする例を示します。

```
switch# config terminal
switch(config)# no tacacs-server deadtime 10
```

関連コマンド

コマンド	説明
deadtime	非応答 TACACS+ サーバをモニタリングするデッド タイム間隔を設定します。
show tacacs-server	TACACS+ サーバ情報を表示します。
feature tacacs+	TACACS+ をイネーブルにします。

tacacs-server directed-request

ログイン時にユーザが認証要求を特定の TACACS+ サーバに送信できるようにするには、**tacacs-server directed-request** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

tacacs-server directed-request

no tacacs-server directed-request

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

設定した TACACS+ サーバ グループに認証要求を送信します。

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

TACACS+ を設定する前に、**feature tacacs+** コマンドを使用する必要があります。

ユーザは、ログイン中に *username@vrfname*:*hostname* を指定することができます。*vrfname* は使用する Virtual Routing and Forwarding（VRF; VPN ルーティングおよび転送）名で、*hostname* は設定した TACACS+ サーバ名です。ユーザ名が認証用にサーバ名に送信されます。

（注） 指定要求オプションをイネーブルにする場合、NX-OS デバイスは認証用に RADIUS 方式のみを使用し、デフォルトのローカル方式を使用しません。

このコマンドには、ライセンスは必要ありません。

例

次に、ログイン時にユーザが認証要求を特定の TACACS+ サーバに送信できるようにする例を示します。

```
switch# config terminal
switch(config)# tacacs-server directed-request
```

次に、ログイン時にユーザが認証要求を特定の TACACS+ サーバに送信できないようにする例を示します。

```
switch# config terminal
switch(config)# no tacacs-server directed-request
```

関連コマンド

コマンド	説明
show tacacs-server directed request	指定要求 TACACS+ サーバ コンフィギュレーションを表示します。
feature tacacs+	TACACS+ をイネーブルにします。

tacacs-server host

TACACS+ サーバ ホスト パラメータを設定するには、コンフィギュレーション モードで **tacacs-server host** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

tacacs-server host {*hostname* | *ipv4-address* | *ipv6-address*}
[**key** [**0** | **7**] *shared-secret*] [**port** *port-number*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds*]

no tacacs-server host {*hostname* | *ipv4-address* | *ipv6-address*}
[**key** [**0** | **7**] *shared-secret*] [**port** *port-number*]
[**test** {**idle-time** *time* | **password** *password* | **username** *name*}]
[**timeout** *seconds*]

シンタックスの説明

hostname	TACACS+ サーバの Domain Name Server（DNS）名。名前は、英数字で指定します。大文字と小文字が区別され、最大文字数は 256 です。
ipv4-address	*A.B.C.D* フォーマットの TACACS+ サーバの IPv4 アドレス
ipv6-address	*X*:*X*:*X*::*X* フォーマットの TACACS+ サーバの IPv6 アドレス
key	（任意）TACACS+ サーバ用の共有秘密鍵を設定します。
0	（任意）TACACS+ クライアントとサーバ間の通信を認証する、クリア テキストで指定された事前共有鍵（0 で表示）を設定します。これがデフォルトです。
7	（任意）TACACS+ クライアントとサーバ間の通信を認証する、暗号文で指定された事前共有鍵（7 で表示）を設定します。
shared-secret	TACACS+ クライアントとサーバ間の通信を認証する事前共有鍵。事前共有鍵は、英数字で指定します。大文字と小文字が区別され、最大文字数は 63 です。
port *port-number*	（任意）認証用の TACACS+ サーバのポートを設定します。範囲は 1 ～ 65535 です。
test	（任意）テスト パケットを TACACS+ サーバに送信するようにパラメータを設定します。
idle-time *time*	（任意）サーバをモニタリングするための時間間隔を分数で指定します。時間の範囲は 1 ～ 1440 分です。
password *password*	（任意）テスト パケット内のユーザ パスワードを指定します。パスワードは、英数字で指定します。大文字と小文字が区別され、最大文字数は 32 です。
username *name*	（任意）テスト パケット内のユーザ名を指定します。ユーザ名は、英数字で指定します。大文字と小文字が区別され、最大文字数は 32 です。
timeout *seconds*	（任意）TACACS+ サーバへの再送信 TACACS+ サーバ タイムアウト期間（秒単位）を設定します。有効範囲は 1 ～ 60 秒です。

デフォルト

アイドル時間は、ディセーブルです。

サーバ モニタリングは、ディセーブルです。

タイムアウトは、1 秒です。

テスト ユーザ名は、test です。

テスト パスワードは、test です。

コマンド モード　グローバル コンフィギュレーション

サポートされるユーザ ロール　network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン　TACACS+ を設定する前に、**feature tacacs+** コマンドを使用する必要があります。

アイドル時間間隔が 0 分の場合、TACACS+ サーバの定期モニタリングは実行されません。

このコマンドには、ライセンスは必要ありません。

例　次に、TACACS+ サーバ ホスト パラメータを設定する例を示します。

```
switch# config terminal
switch(config)# tacacs-server host 10.10.2.3 key HostKey
switch(config)# tacacs-server host tacacs2 key 0 abcd
switch(config)# tacacs-server host tacacs3 key 7 1234
switch(config)# tacacs-server host 10.10.2.3 test idle-time 10
switch(config)# tacacs-server host 10.10.2.3 test username tester
switch(config)# tacacs-server host 10.10.2.3 test password 2B9ka5
```

関連コマンド

コマンド	説明
show tacacs-server	TACACS+ サーバ情報を表示します。
feature tacacs+	TACACS+ をイネーブルにします。

tacacs-server key

グローバル TACACS+ 共有秘密鍵を設定するには、**tacacs-server key** コマンドを使用します。設定した共有秘密鍵を削除するには、このコマンドの **no** 形式を使用します。

tacacs-server key [**0** | **7**] *shared-secret*

no tacacs-server key [**0** | **7**] *shared-secret*

シンタックスの説明

0	（任意）TACACS+ クライアントとサーバ間の通信を認証する、クリア テキストで指定された事前共有鍵を設定します。これがデフォルトです。
7	（任意）TACACS+ クライアントとサーバ間の通信を認証する、暗号文で指定された事前共有鍵を設定します。
shared-secret	TACACS+ クライアントとサーバ間の通信を認証する事前共有鍵。事前共有鍵は、英数字で指定します。大文字と小文字が区別され、最大文字数は 63 です。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

TACACS+ 事前共有鍵を設定して TACACS+ サーバに対してデバイスを認証する必要があります。鍵の長さは 63 文字に制限されており、出力可能な ASCII 文字の使用が可能です（空白文字は使用できません）。グローバル鍵を設定して、デバイスにあるすべての TACACS+ サーバ コンフィギュレーションで使用するようにできます。**tacacs-server host** コマンドで **key** キーワードを使用することでこのグローバル鍵の割り当てを上書きできます。

TACACS+ を設定する前に、**feature tacacs+** コマンドを使用する必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、TACACS+ サーバ共有鍵を設定する例を示します。

```
switch# config terminal
switch(config)# tacacs-server key AnyWord
switch(config)# tacacs-server key 0 AnyWord
switch(config)# tacacs-server key 7 public
```

関連コマンド

コマンド	説明
show tacacs-server	TACACS+ サーバ情報を表示します。
feature tacacs+	TACACS+ をイネーブルにします。

tacacs-server timeout

TACACS+ サーバへの再送信間隔を指定するには、**tacacs-server timeout** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

tacacs-server timeout *seconds*

no tacacs-server timeout *seconds*

シンタックスの説明

seconds	TACACS+ サーバへの再送信間隔を秒単位で設定します。有効範囲は 1 ～ 60 秒です。

デフォルト

1 秒

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

TACACS+ を設定する前に、**feature tacacs+** コマンドを使用する必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、TACACS+ サーバのタイムアウト値を設定する例を示します。

```
switch# config terminal
switch(config)# tacacs-server timeout 3
```

次に、TACACS+ サーバのタイムアウト値に戻す例を示します。

```
switch# config terminal
switch(config)# no tacacs-server timeout 3
```

関連コマンド

コマンド	説明
show tacacs-server	TACACS+ サーバ情報を表示します。
feature tacacs+	TACACS+ をイネーブルにします。

telnet

NX-OS デバイス上に IPv4 による Telnet セッションを作成するには、**telnet** コマンドを使用します。

telnet {*ipv4-address* | *hostname*} [*port-number*] [**vrf** *vrf-name*]

シンタックスの説明

ipv4-address	リモート デバイスの IPv4 アドレス
hostname	リモート デバイスのホスト名。名前は、英数字で指定します。大文字と小文字が区別され、最大文字数は 64 です。
port-number	（任意）Telnet セッションのポート番号。範囲は 1 ～ 65535 です。
vrf *vrf-name*	（任意）Telnet セッションで使用する Virtual Routing and Forwarding（VRF; VPN ルーティングおよび転送）名を指定します。名前では、大文字と小文字が区別されます。

デフォルト

ポート 23

デフォルト VRF

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**telnet server enable** コマンドを使用して Telnet サーバをイネーブルにする必要があります。

IPv6 アドレスで Telnet セッションを作成するには、**telnet6** コマンドを使用します。

このコマンドには、ライセンスは必要ありません。

例

次に、IPv4 アドレスで Telnet セッションを開始する例を示します。

```
switch# telnet 10.10.1.1 vrf management
```

関連コマンド

コマンド	説明
clear line	Telnet セッションを消去します。
telnet6	IPv6 アドレスで Telnet セッションを作成します。
telnet server enable	telnet サーバをイネーブルにします。

telnet server enable

Virtual Device Context（VDC）の Telnet サーバをイネーブルにするには、**telnet server enable** コマンドを使用します。Telnet サーバをディセーブルにするには、このコマンドの **no** 形式を使用します。

telnet server enable

no telnet server enable

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

イネーブル

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

例

次に、Telnet サーバをイネーブルにする例を示します。

```
switch# config t
switch(config)# telnet server enable
```

次に、Telnet サーバをディセーブルにする例を示します。

```
switch# config t
switch(config)# no telnet server enable
XML interface to system may become unavailable since ssh is disabled
```

関連コマンド

コマンド	説明
show telnet server	SSH サーバ鍵の情報を表示します。

telnet6

NX-OS デバイス上に IPv6 による Telnet セッションを作成するには、**telnet6** コマンドを使用します。

telnet6 {*ipv6-address* | *hostname*} [*port-number*] [**vrf** *vrf-name*]

シンタックスの説明

ipv6-address	リモート デバイスの IPv6 アドレス
hostname	リモート デバイスのホスト名。名前は、英数字で指定します。大文字と小文字が区別され、最大文字数は 64 です。
port-number	（任意）Telnet セッションのポート番号。範囲は 1 ～ 65535 です。
vrf *vrf-name*	（任意）Telnet セッションで使用する Virtual Routing and Forwarding（VRF; VPN ルーティングおよび転送）名を指定します。名前では、大文字と小文字が区別されます。

デフォルト

ポート 23

デフォルト VRF

コマンド モード

任意のコマンド モード

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(2)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用するには、**telnet server enable** コマンドを使用して Telnet サーバをイネーブルにする必要があります。

IPv4 アドレスで Telnet セッションを作成するには、**telnet** コマンドを使用します。

このコマンドには、ライセンスは必要ありません。

例

次に、IPv6 アドレスで Telnet セッションを開始する例を示します。

```
switch# telnet6 2001:0DB8:0:0:E000::F vrf management
```

関連コマンド

コマンド	説明
clear line	Telnet セッションを消去します。
telnet	IPv4 アドレスで Telnet セッションを作成します。
telnet server enable	telnet サーバをイネーブルにします。

time-range

時間の範囲を設定するには、**time-range** コマンドを使用します。時間の範囲を削除するには、このコマンドの **no** 形式を使用します。

time-range *time-range-name*

no time-range *time-range-name*

シンタックスの説明

time-range-name	時間の範囲名。範囲名では最大で 64 文字の英数字を使用でき、大文字と小文字が区別されます。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには、ライセンスは必要ありません。

IPv4 ACL では、**permit** および **deny** コマンドで時間の範囲を使用できます。

例

次に、**time-range** コマンドを使用して、時間範囲のコンフィギュレーション モードを開始する例を示します。

```
switch# config t
switch(config)# time-range workweek-vpn-access
switch(config-time-range)#
```

関連コマンド

コマンド	説明
absolute	特定の開始日時を持つ時間範囲を指定します。
deny（IPv4）	IPv4 拒否規則を設定します。
periodic	1 週間に 1 回または複数回アクティブである時間の範囲を指定します。
permit（IPv4）	IPv4 許可規則を設定します。

U コマンド

この章では、U で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

use-vrf

RADIUS または TACACS+ サーバ グループの Virtual Routing and Forwarding（VRF; VPN ルーティングおよび転送）インスタンス名を指定するには、**use-vrf** コマンドを使用します。VRF 名を削除するには、このコマンドの **no** 形式を使用します。

use-vrf *vrf-name*

no use-vrf *vrf-name*

シンタックスの説明

vrf-name	VRF 名。名前では、大文字と小文字が区別されます。

デフォルト

なし

コマンド モード

RADlUS サーバ グループ コンフィギュレーション
TACACS+ サーバ グループ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

サーバ グループに設定できるのは、1 つの VRF インスタンスだけです。

RADIUS サーバ グループ コンフィギュレーション モードを開始するには、**aaa group server radius** コマンドを使用します。あるいは、TACACS+ サーバ グループ コンフィギュレーション モードを開始するには、**aaa group server tacacs+** コマンドを使用します。

サーバを検索できなかった場合、**radius-server host** コマンドまたは **tacacs-server host** コマンドを使用してサーバを設定します。

(注) TACACS+ を設定する前に、**feature tacacs+** コマンドを使用する必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、RADIUS サーバ グループの VRF 名を指定する例を示します。

```
switch# config t
switch(config)# aaa group server radius RadServer
switch(config-radius)# use-vrf vrf1
```

次に、TACACS+ サーバ グループの VRF 名を指定する例を示します。

```
switch# config t
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# use-vrf vrf2
```

次に、TACACS+ サーバ グループから VRF 名を削除する例を示します。

```
switch# config t
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# no use-vrf vrf2
```

関連コマンド

コマンド	説明
aaa group server	AAA サーバ グループを設定します。
radius-server host	RADIUS サーバを設定します。
show radius-server groups	RADIUS サーバ情報を表示します。
show tacacs-server groups	TACACS+ サーバ情報を表示します。
feature tacacs+	TACACS+ をイネーブルにします。
tacacs-server host	TACACS+ サーバを設定します。
vrf	VRF インスタンスを設定します。

username

Virtual Device Context（VDC）にユーザ アカウントを作成および設定するには、**username** コマンドを使用します。ユーザ アカウントを削除するには、このコマンドの **no** 形式を使用します。

username *user-id* [**expire** *date*] [**password** [**0** | **5**] *password*] [**role** *role-name*]

username *user-id* **sshkey** {*key* | **file** *filename*}]

no username *user-id*

シンタックスの説明

user-id	ユーザ アカウントのユーザ ID。*user-id* 引数は、大文字と小文字が区別され、英数字文字列で指定します。最大文字数は 28 です。
expire *date*	（任意）ユーザ アカウントが満了する日付を指定します。*date* 引数のフォーマットは、YYYY-MM-DD です。
password	（任意）アカウントのパスワードを指定します。デフォルトでは、パスワードは設定されていません。
0	（任意）パスワードがクリア テキストであること指定します。クリア テキストのパスワードは、実行コンフィギュレーションに保存される前に暗号化されます。
5	（任意）パスワードが暗号化形式であること指定します。暗号化パスワードは、実行コンフィギュレーションに保存されるまで変更されません。
password	パスワードのストリング。パスワードは英数字で指定し、大文字と小文字が区別されます。
role *role-name*	（任意）SSH セッションで使用する VRF 名を指定します。
sshkey	ユーザ アカウントの SSH 鍵を指定します。
key	SSH 鍵のストリング
file *filename*	SSH 鍵のストリングを含むファイル名を指定します。

デフォルト

指定しないかぎり、ユーザ名には満了日、パスワード、または SSH 鍵が存在しません。

デフォルトの VDC では、作成するユーザに network-admin ロールがある場合、デフォルトのロールは network-operator で、作成するユーザに vdc-admin ロールがある場合、デフォルトのロールは vdc-operator です。

デフォルトでない VDC では、デフォルトのユーザ ロールは vdc-operator です。

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

NX-OS ソフトウェアは、admin および adminbackup の 2 つのデフォルト ユーザ アカウントを VDC に作成します。デフォルトでない VDC には、1 つのデフォルト ユーザ アカウント（admin）があります。デフォルト ユーザ アカウントを削除することはできません。

ユーザ アカウントは、VDC に対してローカルです。異なる VDC に同じユーザ ID を持つユーザ アカウントを作成できます。

NX-OS ソフトウェアは、**password strength-check** コマンドを使用してパスワードの強度の確認をイネーブルにした場合にのみ、強力なパスワードを許可します。強力なパスワードは、次の特性を備えています。

- 最低 8 文字の長さ
- 連続した文字（「abcd」など）が多数含まれない
- 文字の繰り返し（「aaabbb」など）が多数含まれない
- 辞書で確認できる単語が含まれない
- 固有名詞が含まれない
- 大文字と小文字が両方とも含まれる
- 数字が含まれる

注意 ユーザ アカウントのパスワードを指定しない場合、ユーザがアカウントにログインできない可能性があります。

このコマンドには、ライセンスは必要ありません。

例

次に、パスワードおよびユーザ ロールを持つユーザ アカウントを作成する例を示します。

```
switch# config t
switch(config)# username user1 password Ci5co321 role vdc-admin
```

次に、ユーザ アカウントの SSH 鍵を設定する例を示します。

```
switch# config t
switch(config)# username user1 sshkey file bootflash:key_file
```

関連コマンド

コマンド	説明
password strength-check	パスワードのセキュリティ強度を確認します。
show user-account	ユーザ アカウントの設定を表示します。

V コマンド

この章では、V で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

vlan access-map

新規の VLAN アクセス マップを作成したり、既存の VLAN アクセス マップを設定したりするには、**vlan access-map** コマンドを使用します。VLAN アクセス マップを削除するには、このコマンドの **no** 形式を使用します。

vlan access-map *map-name*

no vlan access-map *map-name*

シンタックスの説明

map-name	作成または設定する VLAN アクセス マップ名。*map-name* 引数は、最大で 64 文字の英数字を使用でき、大文字と小文字が区別されます。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

それぞれの VLAN アクセス マップには、**match** コマンドと **action** コマンドを 1 つずつ含めることができます。

このコマンドには、ライセンスは必要ありません。

例

次に、vlan-map-01 という名前の VLAN アクセス マップを作成し、ip-acl-01 という名前の IPv4 ACL をマップに割り当て、ACL に一致するパケットをデバイスが転送することを指定し、マップに一致するトラフィックの統計情報をイネーブルにする例を示します。

```
switch# config t
switch(config)# vlan access-map vlan-map-01
switch(config-access-map)# match ip address ip-acl-01
switch(config-access-map)# action forward
switch(config-access-map)# statistics
```

関連コマンド

コマンド	説明
action	VLAN アクセス マップにトラフィック フィルタリングのアクションを指定します。
match	VLAN アクセス マップにトラフィック フィルタリングの ACL を指定します。
show vlan access-map	すべての VLAN アクセス マップまたは 1 つの VLAN アクセス マップを表示します。
show vlan filter	VLAN アクセス マップが適用されている方法に関する情報を表示します。
vlan filter	1 つまたは複数の VLAN に VLAN アクセス マップを適用します。

vlan filter

VLAN アクセス マップを 1 つまたは複数の VLAN に適用するには、**vlan filter** コマンドを使用します。VLAN アクセス マップの適用を解除するには、このコマンドの **no** 形式を使用します。

vlan filter *map-name* **vlan-list** *VLAN-list*

no vlan filter *map-name* **vlan-list** *VLAN-list*

シンタックスの説明

map-name	作成または設定する VLAN アクセス マップ名
vlan-list *VLAN-list*	VLAN アクセス マップがフィルタリングする 1 つまたは複数の VLAN の ID を指定します。有効な VLAN ID は、1 ～ 4096 です。 ハイフン（-）を使用して、VLAN ID の範囲の開始 ID と終了 ID を区別します（たとえば、70-100）。 カンマ（,）を使用して、各 VLAN ID および VLAN ID の範囲を区別します（たとえば、20,70-100,142）。

（注） このコマンドの **no** 形式を使用する場合、*VLAN-list* 引数を省略できます。この引数を省略する場合、デバイスはアクセス マップが適用されているすべての VLAN からアクセス マップを削除します。

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

1 つまたは複数の VLAN に VLAN アクセス マップを適用できます。

VLAN に適用できるのは、1 つの VLAN アクセス マップだけです。

このコマンドの **no** 形式を使用すると、アクセス マップを適用したときに指定したすべてまたは一部分の VLAN リストから VLAN アクセス マップの適用を解除できます。適用されたすべての VLAN からアクセス マップの適用を解除する場合、*VLAN-list* 引数を省略できます。現在適用されている VLAN のサブセットからアクセス マップの適用を解除する場合、*VLAN-list* 引数を使用して、アクセス マップを削除する VLAN を指定します。

このコマンドには、ライセンスは必要ありません。

例

次に、vlan-map-01 という名前の VLAN アクセス マップを VLAN 20 ～ 45 に適用する例を示します。

```
switch# config t
switch(config)# vlan filter vlan-map-01 20-45
```

次に、このコマンドの **no** 形式を使用して、vlan-map-01 という名前の VLAN アクセス マップの適用を VLAN 30 ～ 32 から解除する例を示します（VLAN 20 ～ 29、33 ～ 45 に適用されたアクセス マップはそのまま残します）。

```
switch# show vlan filter

vlan map vlan-map-01:
        Configured on VLANs:    20-45
switch(config)# no vlan filter vlan-map-01 30-32
switch# show vlan filter

vlan map vlan-map-01:
        Configured on VLANs:    20-29,33-45
```

関連コマンド

コマンド	説明
action	VLAN アクセス マップにトラフィック フィルタリングのアクションを指定します。
match	VLAN アクセス マップにトラフィック フィルタリングの ACL を指定します。
show vlan access-map	すべての VLAN アクセス マップまたは 1 つの VLAN アクセス マップを表示します。
show vlan filter	VLAN アクセス マップが適用されている方法に関する情報を表示します。
vlan access-map	VLAN アクセス マップを設定します。

vlan policy deny

ユーザ ロールの VLAN ポリシー コンフィギュレーション モードを開始するには、**vlan policy deny** コマンドを使用します。ユーザ ロールのデフォルトの VLAN ポリシーに戻すには、このコマンドの **no** 形式を使用します。

vlan policy deny

no vlan policy deny

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

すべての VLAN

コマンド モード

ユーザ ロール コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、ユーザ ロール VLAN ポリシー コンフィギュレーション モードで **permit vlan** コマンドを使用して許可する VLAN を除くすべての VLAN を拒否します。

このコマンドには、ライセンスは必要ありません。

例

次に、ユーザ ロールのユーザ ロール VLAN ポリシー コンフィギュレーション モードを開始する例を示します。

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)#
```

次に、ユーザ ロールのデフォルトの VLAN ポリシーに戻す例を示します。

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# no vlan policy deny
```

関連コマンド

コマンド	説明
permit vlan	ユーザ ロール VLAN ポリシーの VLAN を許可します。
role name	ユーザ ロールを作成または指定して、ユーザ ロール コンフィギュレーション モードを開始します。
show role	ユーザ ロールの情報を表示します。

vrf policy deny

ユーザ ロールの Virtual Routing and Forwarding（VRF; VPN ルーティングおよび転送）インスタンス ポリシー コンフィギュレーション モードを開始するには、**vrf policy deny** コマンドを使用します。ユーザ ロールのデフォルトの VRF ポリシーに戻すには、このコマンドの **no** 形式を使用します。

vrf policy deny

no vrf policy deny

シンタックスの説明

このコマンドには、引数またはキーワードはありません。

デフォルト

すべての VRF

コマンド モード

ユーザ ロール コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、ユーザ ロール VRF ポリシー コンフィギュレーション モードで **permit vrf** コマンドを使用して許可する VRF を除くすべての VRF を拒否します。

このコマンドには、ライセンスは必要ありません。

例

次に、ユーザ ロールの VRF ポリシー コンフィギュレーション モードを開始する例を示します。

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# vrf policy deny
switch(config-role-vrf)#
```

次に、ユーザ ロールのデフォルトの VRF ポリシーに戻す例を示します。

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# no vrf policy deny
```

関連コマンド

コマンド	説明
vrf permit	ユーザ ロール VRF ポリシーの VRF を許可します。
role name	ユーザ ロールを作成または指定して、ユーザ ロール コンフィギュレーション モードを開始します。
show role	ユーザ ロールの情報を表示します。

INDEX

A

C

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

か

ま

ゆ