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*

構文の説明

minutes	間隔の分数です。有効な範囲は 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	変更箇所
4.0(1)	このコマンドが追加されました。

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、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# configure terminal
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# configure terminal
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# configure terminal
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。

delete ca-certificate

認証局の証明書を削除するには、**delete ca-certificate** コマンドを使用してください。

delete ca-certificate

構文の説明

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

トラストポイント コンフィギュレーション

コマンド履歴

リリース	変更箇所
4.1(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、トラストポイント CA に対応する CA 証明書または証明書チェーンを削除します。その結果、トラストポイント CA は信頼されなくなります。CA からのアイデンティティ証明書がある場合、これを削除してから、CA 証明書を削除する必要があります。これによって、CA から取得したアイデンティティ証明書をまだ削除していない場合に、CA 証明書を誤って削除することを防げます。CA の状況が悪化したか、または CA 証明書の期限が切れたため、CA の信頼を継続しない場合は、CA 証明書を削除する必要が生じる場合があります。

（注） トラストポイント設定、証明書、およびキー ペアの設定は、スタートアップ コンフィギュレーションの保存後だけ、永続的に有効になります。実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存後だけ、削除は永続的に有効になります。

証明書とキー ペアの削除を永続的に有効にするには、**copy running-config startup-config** コマンドを入力します。

このコマンドには、ライセンスは必要ありません。

例

次に、認証局の証明書を削除する例を示します。

```
switch# configure terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# delete ca-certificate
```

関連コマンド

コマンド	説明
delete certificate	アイデンティティ証明書を削除します。
delete crl	トラストポイントから CRL を削除します。

delete certificate

アイデンティティ証明書を削除するには、**delete certificate** コマンドを使用します。

delete certificate [**force**]

構文の説明

force	（任意）アイデンティティ証明書を削除します。

デフォルト

なし

コマンド モード

トラストポイント コンフィギュレーション

コマンド履歴

リリース	変更箇所
4.1(2)	このコマンドが追加されました。

使用上のガイドライン

アイデンティティ証明書の期限が切れた場合、または対応するキー ペアが含まれている場合、**delete certificate** コマンドを使用すると、トラストポイント CA から取得したアイデンティティ証明書を削除できます。デバイス上のアプリケーションは、存在する最後の、または存在する唯一のアイデンティティ証明書を削除したあとは、アイデンティティ証明書なしで残されます。削除しようとしている証明書が、存在する唯一の証明書か、チェーンの中の最後のアイデンティティ証明書の場合、Cisco NX-OS ソフトウェアでは、エラー メッセージが生成されます。オプションの **force** キーワードを使用すると、証明書を削除できます。

（注） トラストポイント設定、証明書、およびキー ペアの設定は、スタートアップ コンフィギュレーションの保存後だけ、永続的に有効になります。実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存後だけ、削除は永続的に有効になります。

証明書とキー ペアの削除を永続的に有効にするには、**copy running-config startup-config** コマンドを入力します。

このコマンドには、ライセンスは必要ありません。

例

次の例では、アイデンティティ証明書を削除する方法を示します。

```
switch# configure terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# delete certificate
```

次の例では、アイデンティティ証明書の削除を実行する方法を示します。

```
switch# configure terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# delete certificate force
```

関連コマンド

コマンド	説明
delete ca-certificate	認証局の証明書を削除します。
delete crl	トラストポイントから CRL を削除します。

delete crl

トラストポイントから証明書失効リスト（CRL）を削除するには、**delete crl** コマンドを使用します。

delete crl

構文の説明

このコマンドには引数や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

トラストポイント コンフィギュレーション

コマンド履歴

リリース	変更箇所
4.1(2)	このコマン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、ライセンスは必要ありません。

例

次の例では、トラストポイントから CRL を削除する方法を示します。

```
switch# configure terminal
switch(config)# crypto ca trustpoint admin-ca
switch(config-trustpoint)# delete crl
```

関連コマンド

コマンド	説明
delete ca-certificate	認証局の証明書を削除します。
delete certificate	アイデンティティ証明書を削除します。

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。

基本構文

[*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**]

構文の説明

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。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 の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と、デバイスによって、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）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** を使用すると、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だけ、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 アドレスの部分を指定します。
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だけ、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*	（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だけ、ルールが ARP パケットに一致するように指定します。**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*	（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。*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* 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*	（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だけ、ルールが ARP パケットに一致するように指定します。**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*	（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。*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* 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　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	変更箇所
4.0(1)	このコマンドが追加されました。

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、デバイスは 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を割り当てます。

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、デバイスはシーケンス番号が最も低いルールを施行します。

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	VLAN に ARP ACL を適用します。
permit（ARP）	ARP ACL の許可ルールを設定します。
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。

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。

基本構文

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

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

no *sequence-number*

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* | *icmp-type* [*icmp-code*]] [**dscp** *dscp* | **precedence** *precedence*] [**fragments**] [**log**] [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

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*] [**packet-length** *operator packet-length* [*packet-length*]]

インターネット プロトコル v4

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

伝送制御プロトコル

[*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**] [**packet-length** *operator packet-length* [*packet-length*]]

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*] [**packet-length** *operator packet-length* [*packet-length*]]

構文の説明

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。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 の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と、デバイスによって、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。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「プロトコル」の説明を参照してください。
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「送信元と宛先」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「送信元と宛先」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 であるパケットだけに一致します。 • **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） • **ef**：Expedited Forwarding（EF; 緊急転送）（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るように指定します。*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 進数。たとえば、3 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：011 • **critical**：優先順位 5（101） • **flash**：優先順位 3（011） • **flash-override**：優先順位 4（100） • **immediate**：優先順位 2（010） • **internet**：優先順位 6（110） • **network**：優先順位 7（111） • **priority**：優先順位 1（001） • **routine**：優先順位 0（000）
fragments	（任意）非初期フラグメントであるパケットだけをルールと一致させるように指定します。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指定できません。これらのオプションをデバイスが評価するために必要な情報は、初期フラグメントだけに含まれているためです。
log	（任意）ルールと一致する各パケットについて、デバイスが情報ロギング メッセージを生成するように指定します。メッセージに含まれる情報は、次のとおりです。 • プロトコルの内容（TCP、UDP、ICMP、または数値） • 送信元アドレスおよび宛先アドレス • 送信元と宛先のポート番号（該当する場合）
time-range *time-range-name*	（任意）このルールに適用す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。
icmp-type [*icmp-code*]	（ICMP のみ：任意）ルールと一致させる ICMP メッセージのタイプ。*icmp-type* 引数の有効値は、0 ～ 255 です。ICMP メッセージ タイプでメッセージ コードがサポートされている場合、*icmp-code* 引数を使用して、ルールに一致するコードを指定できます。 ICMP メッセージ タイプとコードについての詳細は、http://www.iana.org/assignments/icmp-parameters を参照してください。

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* 引数および *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* 引数または *destination* 引数のどちらの後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。有効な番号は 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だけ必要です。 *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だけ一致します。 • **gt**：パケットのポートが *port* 引数より大きい場合および同等ではない場合だけ一致します。 • **lt**：パケットのポートが *port* 引数より小さい場合および同等ではない場合だけ一致します。 • **neq**：パケットのポートが *port* 引数と同等ではない場合だけ一致します。 • **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だけ一致します。
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* 引数の値には、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 限定：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るように指定します。デバイスは、ACK または RST ビットが設定されている TCP パケットが、確立された接続に属していると見なします。
packet-length *operator packet-length* [*packet-length*]	（任意）*operator* 引数および *packet-length* 引数の条件と一致するバイト単位での長さがあるパケットだけを、ルールと一致させます。 *packet-length* 引数の有効値は、20 ～ 9210 の整数です。 *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**：バイト単位でのパケットの長さが *packet-legnth* 引数と同等である場合だけ一致します。 • **gt**：バイト単位でのパケットの長さが *packet-legnth* 引数より大きい場合だけ一致します。 • **lt**：バイト単位でのパケットの長さが *packet-legnth* 引数より小さい場合だけ一致します。 • **neq**：バイト単位でのパケットの長さが *packet-legnth* 引数と同等ではない場合だけ一致します。 • **range**：2 つの *packet-length* 引数が必要です。バイト単位でのパケットの長さが最初の *packet-length* 引数以上で、2 番目の *packet-length* 引数以下である場合だけ一致します。

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	変更箇所
4.1(2)	次のサポートが追加されました。 • **ahp**、**eigrp**、**esp**、**gre**、**nos**、**ospf**、**pcp**、および **pim** のプロトコル キーワード。 • **packet-length** キーワード。
4.0(1)	このコマンドが追加されました。

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、デバイスはシーケンス番号が最も低いルールを施行します。

このコマンドには、ライセンスは必要ありません。

プロトコル

ルールによって適用されるパケットのプロトコルは、プロトコル名またはプロトコル番号で指定できます。ルールをすべての IPv4 トラフィックに適用する場合、**ip** キーワードを使用します。

指定するプロトコル キーワードは、使用可能な別のキーワードおよび引数に影響を及ぼします。特に指定のない場合、すべての IPv4 プロトコルに適用される他のキーワードだけを使用できます。これらのキーワードには、次のものが含まれます。

- **dscp**
- **fragments**
- **log**
- **packet-length**
- **precedence**
- **time-range**

有効なプロトコル番号は、0 ～ 255 です。

有効なプロトコル名は、次のキーワードです。

- **ahp**：ルールを認証ヘッダー プロトコル（AHP）トラフィックだけに適用するように指定します。
- **eigrp**：ルールを Enhanced Interior Gateway Routing Protocol（EIGRP）トラフィックだけに適用します。
- **esp**：ルールを Encapsulating Security Protocol（ESP）トラフィックだけに適用します。
- **gre**：ルールを General Routing Encapsulation（GRE）トラフィックだけに適用します。
- **icmp**：ルールを ICMP トラフィックだけに適用するように指定します。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。
- **nos**：ルールを KA9Q NOS 互換の IP over IP トンネリング トラフィックだけに適用します。
- **ospf**：ルールを Open Shortest Path First（OSPF）トラフィックだけに適用します。
- **pcp**：ルールをペイロード圧縮プロトコル（PCP）トラフィックだけに適用するように指定します。
- **pim**：ルールを Protocol Independent Multicast（PIM）だけに適用します。
- **tcp**：ルールを TCP トラフィックだけに適用するように指定します。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*** 引数および **operator** 引数、**portgroup** キーワードおよび ***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するように指定します。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。

送信元と宛先

source 引数および *destination* 引数は、次のいずれかの方法で指定できます。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。ルールの設定時に使用できる *source* 引数および *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* 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 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)# 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。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 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。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、送信元または宛先とするホストを指定できます。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)# 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、次のキーワードのいずれかを指定します。

- **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-solicitation**：ルータ ディスカバリ要求
- **source-quench**：送信元抑制
- **source-route-failed**：送信元ルート障害
- **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**：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：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：ブートストラップ プロトコル（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：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、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 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# configure terminal
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ろに、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# configure terminal
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
fragments	IP ACL が非初期フラグメントを処理する方法を設定します。
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。
permit（IPv4）	IPv4 ACL に許可（permit）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（IPv6）

条件に一致するトラフィックを拒否する IPv6 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。

基本構文

[*sequence-number*] **deny** *protocol source destination* [**dscp** *dscp*] [**flow-label** *flow-label-value*] [**fragments**] [**log**] [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

no deny *protocol source destination* [**dscp** *dscp*] [**flow-label** *flow-label-value*] [**fragments**] [**log**] [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

no *sequence-number*

インターネット制御メッセージ プロトコル

[*sequence-number* | **no**] **deny icmp** *source destination* [*icmp-message* | *icmp-type* [*icmp-code*]] [**dscp** *dscp*] [**flow-label** *flow-label-value*] [**fragments**] [**log**] [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

インターネット プロトコル v6

[*sequence-number*] **deny ipv6** *source destination* [**dscp** *dscp*] [**flow-label** *flow-label-value*] [**fragments**] [**log**] [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

Stream Control Transmission Protocol

[*sequence-number* | **no**] **deny sctp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp*] [**flow-label** *flow-label-value*] [**fragments**] [**log**] [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

伝送制御プロトコル

[*sequence-number*] **deny tcp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp*] [**flow-label** *flow-label-value*] [**fragments**] [**log**] [**time-range** *time-range-name*] [*flags*] [**established**] [**packet-length** *operator packet-length* [*packet-length*]]

ユーザ データグラム プロトコル

[*sequence-number* | **no**] **deny udp** *source* [*operator port* [*port*] | **portgroup** *portgroup*] *destination* [*operator port* [*port*] | **portgroup** *portgroup*] [**dscp** *dscp*] [**flow-label** *flow-label-value*] [**fragments**] [**log**] [**time-range** *time-range-name*] [**packet-length** *operator packet-length* [*packet-length*]]

構文の説明

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。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 の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と、デバイスによって、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、次のキーワードです。 • **ahp**：ルールを認証ヘッダー プロトコル（AHP）トラフィックだけに適用するように指定します。このキーワードを使用する場合は、すべての IPv6 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。 • **esp**：ルールを Encapsulating Security Payload（ESP）トラフィックだけに適用するように指定します。このキーワードを使用する場合は、すべての IPv6 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。 • **icmp**：ルールを ICMP トラフィックだけに適用するように指定します。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。 • **ipv6**：ルールをすべての IPv6 トラフィックに適用するように指定します。このキーワードを使用する場合は、すべての IPv6 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。 • **pcp**：ルールをペイロード圧縮プロトコル（PCP）トラフィックだけに適用するように指定します。このキーワードを使用する場合は、すべての IPv6 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。 • **sctp**：ルールを Stream Control Transmission Protocol（SCTP）トラフィックだけに適用するように指定します。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。 • **tcp**：ルールを TCP トラフィックだけに適用するように指定します。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* 引数および *operator* 引数、**portgroup** キーワードおよび **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するように指定します。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 IPv6 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「送信元と宛先」の説明を参照してください。
destination	ルールで一致させる宛先 IPv6 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「送信元と宛先」の説明を参照してください。

dscp *dscp*	（任意）IPv6 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 進数。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） • **ef** : Expedited Forwarding（EF; 緊急転送）（101110）
flow-label *flow-label-value*	（任意）*flow-label-value* 引数で指定された値がフロー ラベル ヘッダー フィールドに設定されている IPv6 パケットだけをルールと一致させるように指定します。*flow-label-value* 引数は、0 ～ 1048575 の整数です。
fragments	（任意）非初期フラグメントであるパケットだけをルールと一致させるように指定します。デバイスでは、非初期フラグメントであるパケットが、ゼロと同等ではないフラグメント オフセットが含まれるフラグメント拡張ヘッダーを持つパケットと見なされます。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指定できません。これらのオプションをデバイスが評価するために必要な情報は、初期フラグメントだけに含まれているためです。

log	（任意）ルールと一致する各パケットについて、デバイスが情報ロギング メッセージを生成するように指定します。メッセージに含まれる情報は、次のとおりです。 • 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。**time-range** コマンドを使用して時間範囲を設定できます。
icmp-message	（ICMP 限定：任意）ルールと一致させる ICMPv6 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「ICMPv6 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。
icmp-type [*icmp-code*]	（ICMP のみ：任意）ルールと一致させる ICMP メッセージのタイプ。*icmp-type* 引数の有効値は、0 ～ 255 です。ICMP メッセージ タイプでメッセージ コードがサポートされている場合、*icmp-code* 引数を使用して、ルールに一致するコードを指定できます。 ICMP メッセージ タイプとコードについての詳細は、http://www.iana.org/assignments/icmp-parameters を参照してください。
operator port [*port*]	（任意：TCP、UDP および SCTP 限定）*operator* 引数および *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* 引数または *destination* 引数のどちらの後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。有効な番号は 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だけ必要です。 *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だけ一致します。 • **gt**：パケットのポートが *port* 引数より大きい場合および同等ではない場合だけ一致します。 • **lt**：パケットのポートが *port* 引数より小さい場合および同等ではない場合だけ一致します。 • **neq**：パケットのポートが *port* 引数と同等ではない場合だけ一致します。 • **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だけ一致します。
portgroup *portgroup*	（任意：TCP、UDP、および SCTP 限定）*portgroup* 引数で指定された IP ポート グループ オブジェクトのメンバ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、ルールと一致させるように指定します。ポート グループ オブジェクト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* 引数または *destination* 引数のどちらの後に指定したかによって異なります。 IP ポート 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 port** コマンドを使用します。

established	（TCP 限定：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るように指定します。デバイスは、ACK または RST ビットが設定されている TCP パケットが、確立された接続に属していると見なします。
flags	（TCP 限定：任意）特定の TCP コントロール ビット フラグがオンに設定されたパケットだけを、ルールと一致させます。*flags* 引数の値には、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**
packet-length *operator packet-length* [*packet-length*]	（任意）*operator* 引数および *packet-length* 引数の条件と一致するバイト単位での長さがあるパケットだけを、ルールと一致させます。 *packet-length* 引数の有効値は、20 ～ 9210 の整数です。 *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**：バイト単位でのパケットの長さが *packet-legnth* 引数と同等である場合だけ一致します。 • **gt**：バイト単位でのパケットの長さが *packet-legnth* 引数より大きい場合だけ一致します。 • **lt**：バイト単位でのパケットの長さが *packet-legnth* 引数より小さい場合だけ一致します。 • **neq**：バイト単位でのパケットの長さが *packet-legnth* 引数と同等ではない場合だけ一致します。 • **range**：2 つの *packet-length* 引数が必要です。バイト単位でのパケットの長さが最初の *packet-length* 引数以上で、2 番目の *packet-length* 引数以下である場合だけ一致します。

デフォルト

なし

コマンド モード

IPv6 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	変更箇所
4.1(2)	このコマンドが追加されました。

使用上のガイドライン 新しく作成した IPv6 ACL には、ルールは含まれていません。

デバイスは、パケットに IPv6 ACL を適用すると、ACL 内のすべてのルールに対してパケットを評価します。デバイスで、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、デバイスはシーケンス番号が最も低いルールを施行します。

このコマンドには、ライセンスは必要ありません。

送信元と宛先

source 引数および *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、1 つの引数の指定方法によって、他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* 引数および *destination* 引数の指定方法は、次のとおりです。

- IPv6 アドレス グループ オブジェクト：IPv6 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。IPv6 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 ipv6 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-svrs-1301 という名前の IPv6 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)# deny ipv6 any addrgroup lab-svrs-1301
  ```

- アドレスおよび Variable-Length Subnet Mask（VLSM; 可変長サブネット マスク）: IPv6 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。構文は、次のとおりです。

  IPv6-address/prefix-len

  次に、2001:0db8:85a3:: ネットワークの IPv6 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 2001:0db8:85a3::/48 any
  ```

- ホスト アドレス：**host** キーワードおよび IPv6 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。構文は、次のとおりです。

  host *IPv6-address*

  この構文は、*IPv6-address*/128 と同じです。

  次に、*host* キーワードおよび 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 IPv6 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 2001:0db8:85a3:08d3:1319:8a2e:0370:7344 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 IPv6 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。

ICMPv6 メッセージ タイプ

icmp-message 引数には、次のキーワードのいずれかを指定します。

- **beyond-scope**：範囲外の宛先
- **destination-unreachable**：宛先アドレスに到達不能
- **echo-reply**：エコー応答
- **echo-request**：エコー要求（ping）
- **header**：パラメータ ヘッダーの問題

- **hop-limit**：中継時にホップ制限を超過
- **mld-query**：マルチキャスト リスナー ディスカバリ クエリー
- **mld-reduction**：マルチキャスト リスナー ディスカバリ リダクション
- **mld-reduction**：マルチキャスト リスナー ディスカバリ レポート
- **nd-na**：ネイバー探索のネイバー アドバタイズメント
- **nd-ns**：ネイバー探索のネイバー送信要求
- **next-header**：パラメータの次のヘッダーの問題
- **no-admin**：管理者が宛先を禁止
- **no-route**：宛先へのルートなし
- **packet-too-big**：パケット サイズ超過
- **parameter-option**：パラメータ オプションの問題
- **parameter-problem**：すべてのパラメータの問題
- **port-unreachable**：ポート到達不能
- **reassembly-timeout**：再構成タイムアウト
- **redirect**：ネイバーのリダイレクト
- **renum-command**：ルータの番号付けコマンド
- **renum-result**：ルータの番号付けの結果
- **renum-seq-number**：ルータの番号付けのシーケンス番号リセット
- **router-advertisement**：ネイバー探索のルータ アドバタイズメント
- **router-renumbering**：すべてのルータの再番号付け
- **router-solicitation**：ネイバー探索のルータ送信要求
- **time-exceeded**：すべてのタイム超過メッセージ
- **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：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：ブートストラップ プロトコル（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：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-lab13-ipv6 という IPv6 ACL を作成し、2001:0db8:85a3:: ネットワークおよび 2001:0db8:69f2:: ネットワークから 2001:0db8:be03:2112:: ネットワークへのすべての TCP トラフィックおよび UDP トラフィックを拒否するルールを設定する例を示します。

```
switch# config t
switch(config)# ipv6 access-list acl-lab13-ipv6
switch(config-ipv6-acl)# deny tcp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# deny udp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# deny tcp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# deny udp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
```

次に、ipv6-eng-to-marketing という IPv6 ACL を作成し、eng_ipv6 という IPv6 アドレス オブジェクト グループから marketing_group という IPv6 アドレス オブジェクト グループへのすべての IPv6 トラフィックを拒否するルールを設定する例を示します。

```
switch# config t
switch(config)# ipv6 access-list ipv6-eng-to-marketing
switch(config-ipv6-acl)# deny ipv6 addrgroup eng_ipv6 addrgroup marketing_group
```

関連コマンド

コマンド	説明
fragments	IP ACL が非初期フラグメントを処理する方法を設定します。
ipv6 access-list	IPv6 ACL を設定します。
object-group ipv6 address	IPv6 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（IPv6）	IPv6 ACL に許可（permit）ルールを設定します。
remark	ACL に備考を設定します。
show ipv6 access-list	すべての IPv6 ACL または 1 つの IPv6 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*] [**time-range** *time-range-name*]

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

no *sequence-number*

構文の説明

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。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 の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と、デバイスによって、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「送信元と宛先」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「送信元と宛先」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。
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。**time-range** コマンドを使用して時間範囲を設定できます。

デフォルト

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	変更箇所
4.0(1)	このコマンドが追加されました。

使用上のガイドライン 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、デバイスはシーケンス番号が最も低いルールを施行します。

このコマンドには、ライセンスは必要ありません。

送信元と宛先

source 引数および *destination* 引数は、次のいずれかの方法で指定できます。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。ルールの設定時に使用できる *source* 引数および *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 アドレスの後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。構文は、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)# deny 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)# 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、プレフィクスが 0x である 4 バイト 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 診断プロトコル（0x6005）
- **etype-6000**：EtherType 0x6000（0x6000）
- **etype-8042**：EtherType 0x8042（0x8042）
- **ip**：インターネット プロトコル 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、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# configure terminal
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 に拒否（deny）ルールを設定します。
remark	ACL に備考を設定します。
show mac access-list	すべての MAC ACL または 1 つの MAC ACL を表示します。
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（ロールベース アクセス コントロール リスト）

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。この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** | **dst**} {{**eq** | **gt** | **lt** | **neq**} *port-number*} | **range** *port-number1 port-number2*}]} [**log**]

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

構文の説明

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。
dst	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。指定できる範囲は 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。指定できる範囲は 0 ～ 65535 です。
port-number2	範囲の終了ポート。指定できる範囲は 0 ～ 65535 です。
log	（任意）この設定に一致するパケットをログに記録することを指定します。

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	変更箇所
5.0(2)	ロールベース アクセス コントロール リスト（RBACL）のログのイネーブル化をサポートするために、**log** キーワードが追加されました。
4.0(1)	このコマン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。

RBACL ログをイネーブルにするには、VLAN および VRF への RBACL ポリシーの適用をイネーブルにする必要があります。

RBACL ログをイネーブルにするには、ACLLOG syslog のログレベルを 6、CTS マネージャ syslog のログ レベルを 5 に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 に拒否アクションを追加し、RBACL ログをイネーブルにする例を示します。

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

次に、SGACL から拒否アクションを削除する例を示します。

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

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 の設定を表示します。

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

構文の説明

"*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。最大長は 100 文字です。

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	変更箇所
4.0(1)	このコマン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# configure terminal
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# configure terminal
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。
show identity policy	アイデンティティ ポリシーの情報を表示します。

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

構文の説明

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。最大長は、128 文字です。

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	変更箇所
4.0(1)	このコマンドが追加されました。

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。

このコマンドには、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# configure terminal
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# configure terminal
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 ロールの情報を表示します。

destination interface

ACL キャプチャ パケットの宛先を設定するには、**destination interface** コマンドを使用します。

destination interface ethernet *slot/port*

構文の説明

ethernet	イーサネット IEEE 802.3z を指定します。
slot/port	インターフェイスのスロットおよびポートの ID。有効範囲は 1 ～ 253 です。

デフォルト

なし

コマンド モード

ACL キャプチャコンフィギュレーション モード（config-acl-capture）

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	変更箇所
5.2(1)	このコマンドが追加されました。

使用上のガイドライン

物理インターフェイスだけが宛先に使用できます。ポートチャネル インターフェイス、およびスーパーバイザ インバンド ポートはサポートされません。

ポートチャネル インターフェイス、およびスーパーバイザ インバンド ポートは ACL キャプチャの宛先としてサポートされません。

ACL キャプチャ セッションの宛先インターフェイスは、入力転送と入力の MAC の学習をサポートしません。宛先インターフェイスでこれらオプションが設定されている場合、モニタが ACL のキャプチャ セッションをダウン状態にし続けます。入力転送および MAC の学習がイネーブルになっているかどうかを確認するには、**show monitor session all** コマンドを使用します。

（注） インターフェイスで入力転送および MAC 学習をディセーブルにするには、**no switchport monitor** コマンドを使用できます。

パケットの送信元ポートと ACL キャプチャの宛先ポートは、同じ ASIC の一部であってはなりません。ポートが両方とも同じ ASIC に属する場合、ACL キャプチャの宛先ポートを設定するときにメッセージが表示され、パケットはキャプチャされません。

複数の宛先を追加するには **destination interface** コマンドを複数回入力できます。

このコマンドには、ライセンスは必要ありません。

例

次に、ACL キャプチャ パケットの宛先を設定する例を示します。

```
switch# configure terminal
switch(config)# monitor session 7 type acl-capture
switch(config-acl-capture)# destination interface ethernet 5/5
```

関連コマンド

コマンド	説明
monitor session *session* **type acl-capture**	ACL キャプチャ セッションを設定します。

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*

構文の説明

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	変更箇所
4.0(1)	このコマン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# configure terminal
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# configure terminal
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。
show identity policy	アイデンティティ ポリシーの情報を表示します。

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

構文の説明

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	変更箇所
4.0(1)	このコマンドが追加されました。

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。

このコマンドには、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# configure terminal
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# configure terminal
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

構文の説明

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	変更箇所
4.0(1)	このコマンドが追加されました。

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。

このコマンドには、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# configure terminal
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# configure terminal
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*]

構文の説明

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	変更箇所
4.0(1)	このコマンドが追加されました。

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。

このコマンドには、ライセンスは必要ありません。

例

Cisco 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

構文の説明

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	変更箇所
4.0(1)	このコマンドが追加されました。

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。

このコマンドには、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# configure terminal
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# configure terminal
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 Cisco 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

構文の説明

retry-count	再認証要求リトライ回数。指定できる範囲は 1 ～ 10 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	変更箇所
4.0(1)	このコマンドが追加されました。

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。

このコマンドには、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# configure terminal
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# configure terminal
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 Cisco 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

構文の説明

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。指定できる範囲は 1 ～ 10 です。

デフォルト

グローバル コンフィギュレーション：2 回試行

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	変更箇所
4.0(1)	このコマンドが追加されました。

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。

このコマンドには、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# configure terminal
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# configure terminal
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# configure terminal
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# configure terminal
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 pae authenticator

インターフェイスに対して 802.1X オーセンティケータ Port Access Entity（PAE）ロールを作成するには、**dot1x pae authenticator** コマンドを使用します。802.1X オーセンティケータ PAE 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。

dot1x pae authenticator

no dot1x pae authenticator

構文の説明

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

インターフェイス上でこの機能をイネーブルにするときに、802.1X では、オーセンティケータ PAE が自動的に作成されます。

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	変更箇所
4.2(1)	このコマンドが追加されました。

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。

インターフェイスで 802.1X をイネーブルにすると、Cisco NX-OS ソフトウェアにより、オーセンティケータ Port Access Entity（PAE）インスタンスが作成されます。オーセンティケータ PAE は、インターフェイスでの認証をサポートするプロトコル エンティティです。インターフェイスで 802.1X をディセーブルにしても、オーセンティケータ PAE インスタンスは自動的にクリアされません。必要に応じ、オーセンティケータ PAE をインターフェイスから明示的に削除し、再度適用することができます。

このコマンドには、ライセンスは必要ありません。

例

次に、インターフェイス上で 802.1X オーセンティケータ PAE ロールを作成する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/4
switch(config-if)# dot1x pae authenticator
```

次に、インターフェイスから 802.1X オーセンティケータ PAE ロールを削除する例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/4
switch(config-if)# no dot1x pae authenticator
```

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	インターフェイスの 802.1X 機能のステータス情報を表示します。

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**}

構文の説明

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の 802.1X 認証をディセーブルにし、認証を行わずにインターフェイス上のすべてのトラフィックを許可します。
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	変更箇所
4.0(1)	このコマンドが追加されました。

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。

このコマンドには、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# configure terminal
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# configure terminal
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

構文の説明

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	変更箇所
4.0(1)	このコマンドが追加されました。

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。

このコマンドには、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# configure terminal
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# configure terminal
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*]

構文の説明

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

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	変更箇所
4.0(1)	このコマンドが追加されました。

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。

このコマンドには、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

構文の説明

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	変更箇所
4.0(1)	このコマンドが追加されました。

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、Cisco 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だけの定期的な再認証が設定されます。

このコマンドには、ライセンスは必要ありません。

例

次に、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# configure terminal
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# configure terminal
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# configure terminal
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# configure terminal
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

構文の説明

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	変更箇所
4.0(1)	このコマンドが追加されました。

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。

このコマンドには、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# configure terminal
switch(config)# no dot1x system-auth-control
```

次の例では、802.1X 認証をイネーブルにする方法を示します。

```
switch# configure terminal
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

構文の説明

seconds	802.1X 待機時間タイムアウトの秒数。有効な範囲は 1 ～ 65535 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	変更箇所
4.0(1)	このコマンドが追加されました。

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あとで、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。

このコマンドには、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# configure terminal
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# configure terminal
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# configure terminal
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# configure terminal
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

構文の説明

seconds	802.1X レート制限時間タイムアウトの秒数。有効な範囲は 1 ～ 65535 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	変更箇所
4.0(1)	このコマンドが追加されました。

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。

このコマンドには、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# configure terminal
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# configure terminal
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

構文の説明

seconds	802.1X 再認証時間タイムアウトの秒数。有効な範囲は 1 ～ 65535 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	変更箇所
4.0(1)	このコマンドが追加されました。

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。

このコマンドには、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# configure terminal
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# configure terminal
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

構文の説明

seconds	802.1X サーバ タイムアウトの秒数。有効な範囲は 1 ～ 65535 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	変更箇所
4.0(1)	このコマンドが追加されました。

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 Cisco 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。

このコマンドには、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# configure terminal
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# configure terminal
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

構文の説明

seconds	802.1X サプリカント タイムアウトの秒数。有効な範囲は 1 ～ 65535 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	変更箇所
4.0(1)	このコマンドが追加されました。

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、Cisco 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 Cisco 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。

このコマンドには、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# configure terminal
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# configure terminal
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

構文の説明

seconds	802.1X 送信時間タイムアウトの秒数。有効な範囲は 1 ～ 65535 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	変更箇所
4.0(1)	このコマンドが追加されました。

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、Cisco 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。

このコマンドには、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# configure terminal
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# configure terminal
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# configure terminal
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# configure terminal
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。