# 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**

**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 | 変更内容 |
|---|---|
| 4.0(3) | このコマンドが追加されました。 |

**使用上のガイドライン**

パスワード長のチェックをイネーブルにした場合、Cisco 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
- 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

次に、強化パスワードの例を示します。

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

**（注）** パスワード長のチェックをイネーブルにした場合、Cisco NX-OS ソフトウェアでは、既存パスワードの強度はチェックされません。

このコマンドには、ライセンスは不要です。

## 例

次に、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。 |

# 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*}

## 構文の説明

| | |
|---|---|
| *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。<br>シーケンス番号には、1 ～ 4294967295 の間の整数を指定できます。<br>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。<br>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。<br>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。<br>*weekday* 引数の有効値は、次のとおりです。<br>• **monday**<br>• **tuesday**<br>• **wednesday**<br>• **thursday**<br>• **friday**<br>• **saturday**<br>• **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。<br>*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、8:00 a.m. は 8:00 で、8:00 p.m. は 20:00 です。 |
| **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。<br>• 曜日を次のようにスペースで区切って指定します。<br>`monday thursday friday`<br>• **daily**：すべての曜日<br>• **weekdays**：月曜から金曜まで（Monday ～ Friday）<br>• **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、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 および IPv6 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。

### 基本構文

[*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**]

### 構文の説明

| | |
|---|---|
| *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。シーケンス番号は、ACL 内でルールの順序を保ちます。<br>シーケンス番号には、1 ～ 4294967295 の間の整数を指定できます。<br>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。<br>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。<br>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ように指定します。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だけ、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*<br>*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* 引数および *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 アドレスの部分を指定します。 |
| **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だけ、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*<br>*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* 引数および *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。<br>**（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。<br>**（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だけ、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*<br>*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* 引数および *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だけ、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*<br>*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* 引数および *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、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-01 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** | VLAN に ARP ACL を適用します。 |
| **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。

### 基本構文

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

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

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

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

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

### Transmission Control Protocol（TCP; 伝送制御プロトコル）

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

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

## 構文の説明

| | |
|---|---|
| *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。シーケンス番号は、ACL 内でルールの順序を保ちます。<br>シーケンス番号には、1 ～ 4294967295 の間の整数を指定できます。<br>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。<br>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。<br>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。<br>• 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、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。<br>• **af11**：Assured Forwarding（AF）クラス 1、低い廃棄確率（001010）<br>• **af12**：AF クラス 1、中程度の廃棄確率（001100）<br>• **af13**：AF クラス 1、高い廃棄確率（001110）<br>• **af21**：AF クラス 2、低い廃棄確率（010010）<br>• **af22**：AF クラス 2、中程度の廃棄確率（010100）<br>• **af23**：AF クラス 2、高い廃棄確率（010110）<br>• **af31**：AF クラス 3、低い廃棄確率（011010）<br>• **af32**：AF クラス 3、中程度の廃棄確率（011100）<br>• **af33**：AF クラス 3、高い廃棄確率（011110）<br>• **af41**：AF クラス 4、低い廃棄確率（100010）<br>• **af42**：AF クラス 4、中程度の廃棄確率（100100）<br>• **af43**：AF クラス 4、高い廃棄確率（100110）<br>• **cs1**：Class-selector（CS）1、優先順位 1（001000）<br>• **cs2**：CS2、優先順位 2（010000）<br>• **cs3**：CS3、優先順位 3（011000）<br>• **cs4**：CS4、優先順位 4（100000）<br>• **cs5**：CS5、優先順位 5（101000）<br>• **cs6**：CS6、優先順位 6（110000）<br>• **cs7**：CS7、優先順位 7（111000）<br>• **default**：デフォルトの DSCP 値（000000）<br>• **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。<br>• 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<br>• **critical**：優先順位 5（101）<br>• **flash**：優先順位 3（011）<br>• **flash-override**：優先順位 4（100）<br>• **immediate**：優先順位 2（010）<br>• **internet**：優先順位 6（110）<br>• **network**：優先順位 7（111）<br>• **priority**：優先順位 1（001）<br>• **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、初期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。<br>• プロトコルの内容（TCP、UDP、ICMP、または番号のプロトコル）<br>• 送信元アドレスおよび宛先アドレス<br>• 該当する場合は、送信元アドレスおよび宛先アドレス |
| **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。<br>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。この引数には、「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。<br>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。<br>• **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）<br>• **host-query**：ホスト クエリー<br>• **host-report**：ホスト レポート<br>• **pim**：Protocol Independent Multicast（PIM）<br>• **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* 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。<br><br>*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。<br><br>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。<br><br>*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。<br>• **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。<br>• **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。<br>• **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。<br>• **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。<br>• **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。<br><br>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。<br>• **ack**<br>• **fin**<br>• **psh**<br>• **rst**<br>• **syn**<br>• **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見なされます。 |
| **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。<br>*packet-length* 引数の有効値は、20 ～ 9210 の整数です。<br>*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。<br>• **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。<br>• **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。<br>• **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。<br>• **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。<br>• **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 |
|---|---|
| 4.1(2) | 次のサポートが追加されました。<br>• **ahp**、**eigrp**、**esp**、**gre**、**nos**、**ospf**、**pcp**、および **pim** のプロトコル キーワード。<br>• **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、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。

### 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 Payload Compression Protocol（PCP）トラフィックだけに適用します。
- **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。

### 送信元および宛先

*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、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* 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)# 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。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)# 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。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)# 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。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)# 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、この項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。 |
| **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。 |
| **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（IPv6）

条件と一致するトラフィックを許可する IPv6 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。

### 基本構文

[*sequence-number*] **permit** *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 permit** *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*

### 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* | **no**] **permit 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*]]

### Internet Protocol v6（IPv6; インターネット プロトコル v6）

[*sequence-number*] **permit 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（SCTP）

[*sequence-number* | **no**] **permit 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*]]

### Transmission Control Protocol（TCP; 伝送制御プロトコル）

[*sequence-number*] **permit 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*]]

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

[*sequence-number* | **no**] **permit 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）**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。シーケンス番号は、ACL 内でルールの順序を保ちます。<br>シーケンス番号には、1 ～ 4294967295 の間の整数を指定できます。<br>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。<br>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。<br>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。<br>• **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。<br>• **esp**：ルールを Encapsulating Security Payload（ESP）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。<br>• **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。<br>• **ipv6**：ルールをすべての IPv6 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 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。<br>• **pcp**：ルールを Payload Compression Protocol（PCP）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。<br>• **sctp**：ルールを Stream Control Transmission Protocol（SCTP）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。<br>• **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* 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。<br>• **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 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 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「送信元および宛先」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。<br>• 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、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：001010<br>• **af11**：Assured Forwarding（AF）クラス 1、低い廃棄確率（001010）<br>• **af12**：AF クラス 1、中程度の廃棄確率（001100）<br>• **af13**：AF クラス 1、高い廃棄確率（001110）<br>• **af21**：AF クラス 2、低い廃棄確率（010010）<br>• **af22**：AF クラス 2、中程度の廃棄確率（010100）<br>• **af23**：AF クラス 2、高い廃棄確率（010110）<br>• **af31**：AF クラス 3、低い廃棄確率（011010）<br>• **af32**：AF クラス 3、中程度の廃棄確率（011100）<br>• **af33**：AF クラス 3、高い廃棄確率（011110）<br>• **af41**：AF クラス 4、低い廃棄確率（100010）<br>• **af42**：AF クラス 4、中程度の廃棄確率（100100）<br>• **af43**：AF クラス 4、高い廃棄確率（100110）<br>• **cs1**：Class-selector（CS）1、優先順位 1（001000）<br>• **cs2**：CS2、優先順位 2（010000）<br>• **cs3**：CS3、優先順位 3（011000）<br>• **cs4**：CS4、優先順位 4（100000）<br>• **cs5**：CS5、優先順位 5（101000）<br>• **cs6**：CS6、優先順位 6（110000）<br>• **cs7**：CS7、優先順位 7（111000）<br>• **default**：デフォルトの DSCP 値（000000）<br>• **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、ルールと一致させます。<br>*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、初期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。<br>• プロトコルの内容（TCP、UDP、ICMP、または番号のプロトコル）<br>• 送信元アドレスおよび宛先アドレス<br>• 該当する場合は、送信元アドレスおよび宛先アドレス |

| | |
|---|---|
| **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 のみ：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。<br><br>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 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* 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。<br><br>*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。<br><br>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。<br><br>*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。<br>• **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。<br>• **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。<br>• **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。<br>• **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。<br>• **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 のみ）*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。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* 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。<br><br>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 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見なされます。 |

| | |
|---|---|
| *flags* | （TCP のみ：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。<br>• **ack**<br>• **fin**<br>• **psh**<br>• **rst**<br>• **syn**<br>• **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。<br>*packet-length* 引数の有効値は、20 ～ 9210 の整数です。<br>*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。<br>• **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。<br>• **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。<br>• **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。<br>• **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。<br>• **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 | 変更内容 |
|---|---|
| 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。

パケットに IPv6 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* 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、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* 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)# permit 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)# permit 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)# permit 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、この項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**：ネイバー探索とネイバー アドバタイズメント
- **nd-ns**：ネイバー探索とネイバー送信要求
- **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 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**：ネイバー探索とルータ 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**：ネイバー探索とルータ送信要求
- **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**：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-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 トラフィックを許可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)# permit tcp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# permit udp 2001:0db8:85a3::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# permit tcp 2001:0db8:69f2::/48 2001:0db8:be03:2112::/64
switch(config-ipv6-acl)# permit 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 トラフィックを許可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)# permit ipv6 addrgroup eng_ipv6 addrgroup marketing_group
```

## 関連コマンド

| コマンド | 説明 |
|---|---|
| **deny（IPv6）** | IPv6 ACL に拒否（deny）ルールを設定します。 |
| **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。 |
| **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。 |

# 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*] [**time-range** *time-range-name*]

**no permit** *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）**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。シーケンス番号は、ACL 内でルールの順序を保ちます。<br>シーケンス番号には、1 ～ 4294967295 の間の整数を指定できます。<br>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。<br>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。<br>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。 |
| **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

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) | このコマンドが追加されました。 |

**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* 引数および *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* 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。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)# 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、この項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 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、mac-filter という MAC ACL を作成し、2 つの MAC アドレス グループ間で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-filter
switch(config-mac-acl)# permit 00c0.4f00.0000 0000.00ff.ffff 0060.3e00.0000 0000.00ff.ffff
```

## 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。 |
| **time-range** | 時間範囲を設定します。 |

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

**no permit** {**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 | 変更内容 |
|---|---|
| 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 に許可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# config t
switch(config)# cts role-based access-list MySGACL
switch(config-rbacl)# permit icmp log
```

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 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。 |
| **deny（ロールベース アクセス コントロール リスト）** | SGACL に拒否アクションを設定します。 |
| **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**

## 構文の説明

| | |
|---|---|
| **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) | このコマンドが追加されました。 |

## 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**

## 構文の説明

| | |
|---|---|
| *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) | このコマンドが追加されました。 |

## 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*

## 構文の説明

| | |
|---|---|
| *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

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) | このコマンドが追加されました。 |

## 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)# 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 update** 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**}

## 構文の説明

| | |
|---|---|
| **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。Cisco 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 |
|---|---|
| 4.1(2) | このコマンドは廃止予定で、**hardware access-list update** コマンドに置き換えられます。 |
| 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

Cisco 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 platform 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*]

## 構文の説明

| | |
|---|---|
| **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 2 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、「構文の説明」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 |
|---|---|
| 4.1(2) | このコマンドは廃止予定で、**hardware rate-limit** コマンドに置き換えられます。 |
| 4.0(3) | **port-security** 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（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**]]

## 構文の説明

| | |
|---|---|
| **cir** | （任意）Committed 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。 |
| **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**}

## 構文の説明

| | |
|---|---|
| **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 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) | 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。 |
| 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。

このコマンドを使用したあと、設定を有効にするには、**shutdown**/**no shutdown** コマンド シーケンスを使用することによっ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 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。 |

# 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*

## 構文の説明

| | |
|---|---|
| *policy-map-name* | クラス マップ名です。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。 |

## 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**

## 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 | 変更内容 |
|---|---|
| 4.0(3) | 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。

このコマンドを使用したあと、設定を有効にするには、**shutdown**/**no shutdown** コマンド シーケンスを使用することによっ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、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。 |