



P コマンド

この章では、P で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

password strength-check

パスワード長のチェックをイネーブルにするには、**password strength-check** コマンドを使用します。パスワード長のチェックをディセーブルにするには、このコマンドの **no** 形式を使用します。

password strength-check

no password strength-check

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト ディセーブル

コマンド モード グローバル コンフィギュレーション

サポートされるユーザロール network-admin
vdc-admin

コマンド履歴	リリース	変更内容
	4.0(3)	このコマンドが導入されました。

使用上のガイドライン パスワード長のチェックをイネーブルにした場合、NX-OS ソフトウェアで作成できるのは強化パスワードだけです。強化パスワードの特性は、次のとおりです。

- 最低 8 文字の長さとする。
- 多数の連続文字 (“abcd” など) は使用できない。
- 多数の重複文字 (“aaabbb” など) は使用できない。
- 辞書に載っている単語は使用できない。
- 一般的な名前は使用できない。
- 大文字と小文字の両方を使用する。
- 数字を使用する。

次に、強化パスワードの例を示します。

- If2CoM18
- 2004AsdfLkj30
- Cb1955S21

このコマンドには、ライセンスは不要です。

例

次に、パスワード長のチェックをイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# password strength-check
```

次に、パスワード長のチェックをディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# no password strength-check
```

関連コマンド

コマンド	説明
show password strength-check	パスワード長のチェックをイネーブルにします。
show running-config security	実行コンフィギュレーションのセキュリティ機能設定を表示します。

periodic

1 週間に 1 回以上アクティブにする時間範囲を指定するには、**periodic** コマンドを使用します。定期的な時間範囲を削除するには、このコマンドの **no** 形式を使用します。

```
[sequence-number] periodic weekday time to [weekday] time
```

```
no {sequence-number | periodic weekday time to [weekday] time}
```

```
[sequence-number] periodic list-of-weekdays time to time
```

```
no {sequence-number | periodic list-of-weekdays time to time}
```

シンタックスの説明

<i>sequence-number</i>	<p>(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。</p> <p>シーケンス番号は、1 ~ 4294967295 の任意の整数です。</p> <p>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。</p> <p>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。</p> <p>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。</p>
<i>weekday</i>	<p>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。</p> <p><i>weekday</i> 引数の有効値は、次のとおりです。</p> <ul style="list-style-type: none"> • monday • tuesday • wednesday • thursday • friday • saturday • sunday
<i>time</i>	<p>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。</p> <p><i>time</i> 引数は、24 時間表記で指定します。形式は、<i>hours:minutes</i> または <i>hours:minutes:seconds</i> です。たとえば、午前 8: 時は 8:00、午後 8 時は 20:00 になります。</p>
to	<p><i>time</i> 引数の最初の指定と 2 番目の指定を区切ります。</p>
<i>list-of-weekdays</i>	<p>(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。</p> <ul style="list-style-type: none"> • 曜日をスペースで区切って指定します。例： monday thursday friday • daily — すべての曜日 • weekdays — 月曜から金曜まで (Monday – Friday) • weekend — 土曜と日曜 (Saturday – Sunday)

■ periodic

デフォルト to

コマンドモード 時間範囲コンフィギュレーション

サポートされるユーザロール network-admin
vdc-admin

コマンド履歴 **リリース** **変更内容**

4.0(1) このコマンドが導入されました。

使用上のガイドライン このコマンドには、ライセンスは不要です。

例 次に、weekend-remote-access-times という時間範囲を作成し、土曜と日曜の午前 4 時から午後 10 時までの間、トラフィックを許可する定期ルールを設定する例を示します。

```
switch# config t
switch(config)# time-range weekend-remote-access-times
switch(config-time-range)# periodic weekend 04:00:00 to 22:00:00
```

次に、nwf-evening という時間範囲を作成し、月曜、水曜、金曜の午後 6 時から午後 10 時までの間、トラフィックを許可する定期ルールを設定する例を示します。

```
switch# config t
switch(config)# time-range nwf-evening
switch(config-time-range)# periodic monday wednesday friday 18:00:00 to 22:00:00
```

関連コマンド **コマンド** **説明**

absolute 絶対時間範囲のルールを設定します。

time-range IPv4 ACL で使用できる時間範囲を設定します。

permit (ARP)

条件と一致する ARP トラフィックを許可する ARP ACL ルールを作成するには、**permit** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

基本シンタックス

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

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

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

no sequence-number

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

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

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

シンタックスの説明

<i>sequence-number</i>	(任意) permit コマンドのシーケンス番号。アクセス リストの該当番号の位置にコマンドが挿入されます。シーケンス番号により、ACL 内のルールの順序が保持されます。 シーケンス番号は、1 ~ 4294967295 の任意の整数です。 デフォルトでは、ACL 内の最初のルールにシーケンス番号 10 が割り当てられます。 シーケンス番号を指定しないと、ACL の最後にルールが追加され、1 つ前のルールのシーケンス番号に 10 を加算した値が、シーケンス番号として割り当てられます。 ルールのシーケンス番号を再割り当てするには、 resequence コマンドを使用します。
<i>ip</i>	ルールの IP アドレス部分を指定します。
<i>any</i>	任意のホストが、ルールの any キーワードを含む部分と一致することを指定します。送信元 IP アドレス、宛先 IP アドレス、送信元 MAC アドレス、および宛先 MAC アドレスの指定に、 any を使用できます。
<i>host sender-IP</i>	ARP パケットの送信元 IP アドレスが <i>sender-IP</i> 引数の値と一致する場合にのみ、パケットを一致させるルールを指定します。 <i>sender-IP</i> 引数の有効値は、ドット付き 10 進表記の IPv4 アドレスです。
<i>sender-IP</i> <i>sender-IP-mask</i>	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。 <i>sender-IP</i> および <i>sender-IP-mask</i> 引数は、ドット付き 10 進表記で指定する必要があります。 <i>sender-IP-mask</i> 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。
<i>mac</i>	ルールの MAC アドレス部分を指定します。

■ permit (ARP)

<i>host sender-MAC</i>	ARP パケットの送信元 MAC アドレスが <i>sender-MAC</i> 引数の値と一致する場合にのみ、パケットを一致させるルールを指定します。 <i>sender-MAC</i> 引数の有効値は、ドット付き 16 進表記の MAC アドレスです。
<i>sender-MAC</i> <i>sender-MAC-mask</i>	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。 <i>sender-MAC</i> および <i>sender-MAC-mask</i> 引数は、ドット付き 16 進表記で指定する必要があります。 <i>sender-MAC-mask</i> 引数に <i>ffff.ffff.ffff</i> 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。
<i>log</i>	(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。
<i>request</i>	(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)	<i>request</i> および <i>response</i> 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。
<i>response</i>	(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)	<i>request</i> および <i>response</i> 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。
<i>host target-IP</i>	ARP パケットの宛先 IP アドレスが <i>target-IP</i> 引数の値と一致する場合にのみ、パケットを一致させるルールを指定します。 host target-IP を指定できるのは、 response キーワードを使用する場合だけです。 <i>target-IP</i> 引数の有効値は、ドット付き 10 進表記の IPv4 アドレスです。
<i>target-IP</i> <i>target-IP-mask</i>	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。 <i>target-IP target-IP-mask</i> 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。 <i>target-IP</i> および <i>target-IP-mask</i> 引数は、ドット付き 10 進表記で指定する必要があります。 <i>target-IP-mask</i> 引数に <i>255.255.255.255</i> 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。
<i>host target-MAC</i>	ARP パケットの宛先 MAC アドレスが <i>target-MAC</i> 引数の値と一致する場合にのみ、パケットを一致させるルールを指定します。 host target-MAC を指定できるのは、 response キーワードを使用する場合だけです。 <i>target-MAC</i> 引数の有効値は、ドット付き 16 進表記の MAC アドレスです。
<i>target-MAC</i> <i>target-MAC-mask</i>	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。 <i>target-MAC target-MAC-mask</i> 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。 <i>target-MAC</i> および <i>target-MAC-mask</i> 引数は、ドット付き 16 進表記で指定する必要があります。 <i>target-MAC-mask</i> 引数に <i>ffff.ffff.ffff</i> を指定すると、 host キーワードを使用した場合と同じ結果になります。

デフォルト

ip

コマンド モード

ARP ACL コンフィギュレーション

サポートされるユーザロール

network-admin
vdc-admin

コマンド履歴	リリース	変更内容
	4.0(1)	このコマンドが導入されました。

使用上のガイドライン

新しく作成した ARP ACL には、ルールは含まれていません。

シーケンス番号を指定しないと、ACL の最後のルールのシーケンス番号に 10 を加算したシーケンス番号が割り当てられます。

パケットに ARP ACL が適用されると、ACL 内のすべてのルールに対してパケットが評価されます。パケットが条件に一致した最初のルールが施行されます。複数のルールの条件と一致する場合は、シーケンス番号が最も低いルールが施行されます。

response または *request* のキーワードをどちらも指定しないと、任意の ARP メッセージを含むパケットにルールが適用されます。

このコマンドには、ライセンスは不要です。

例

次に、arp-acl-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	ARP ACL を VLAN に適用します。
remark	ACL に備考を設定します。
show arp access-list	すべての ARP ACL または 1 つの ARP ACL を表示します。

permit (IPv4)

条件と一致するトラフィックを許可する IPv4 Access Control List (ACL; アクセス コントロール リスト) ルールを作成するには、**permit** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

基本シンタックス

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

```
no permit protocol source destination [dscp dscp | precedence precedence] [fragments] [log]
[time-range time-range-name]
```

```
no sequence-number
```

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

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

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

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

Internet Protocol v4 (IPv4; インターネット プロトコル v4)

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

Transmission Control Protocol (TCP)

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

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

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


シンタックスの説明

<i>sequence-number</i>	<p>(任意) permit コマンドのシーケンス番号。アクセス リストの該当番号の位置にコマンドが挿入されます。シーケンス番号により、ACL 内のルールが順序が保持されます。</p> <p>シーケンス番号は、1 ~ 4294967295 の任意の整数です。</p> <p>デフォルトでは、ACL 内の最初のルールにシーケンス番号 10 が割り当てられます。</p> <p>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。</p> <p>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。</p>
<i>protocol</i>	<p>ルールで一致させるパケットのプロトコルの名前または番号。有効値は 0 ~ 255 です。有効なプロトコル名は、次のキーワードです。</p> <ul style="list-style-type: none"> • 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、<i>protocol</i> 引数のすべての有効値に使用できるキーワードに加え、<i>icmp-message</i> 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、<i>protocol</i> 引数のすべての有効値に使用できるキーワードに加え、<i>igmp-type</i> 引数を使用できます。 • ip — ルールをすべての IPv4 トラフィックに適用します。このキーワードを使用する場合は、すべての IPv4 プロトコルに適用される他のキーワードおよび引数だけを使用できます。使用できるキーワードおよび引数は、次のとおりです。 <ul style="list-style-type: none"> — <i>dscp</i> — <i>fragments</i> — <i>log</i> — <i>precedence</i> — <i>time-range</i> • 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、<i>protocol</i> 引数のすべての有効値に使用できるキーワードに加え、<i>flags</i> および <i>operator</i> 引数、<i>portgroup</i> および <i>established</i> 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、<i>protocol</i> 引数のすべての有効値に使用できるキーワードに加え、<i>operator</i> 引数および <i>portgroup</i> キーワードを使用できます。
<i>source</i>	<p>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。</p>
<i>destination</i>	<p>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。</p>

<i>dscp dscp</i>	<p>(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。 <i>dscp</i> 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。</p> <ul style="list-style-type: none"> • 0 ~ 63 — DSCP フィールドの 6 ビットと同等の 10 進値。たとえば、10 を指定した場合、DSCP フィールドに次のビットが設定されているパケットだけがルールと一致します：001010。 • <i>af11</i> — Assured Forwarding (AF) クラス 1、低い廃棄確率 (001010) • <i>af12</i> — AF クラス 1、中程度の廃棄確率 (001100) • <i>af13</i> — AF クラス 1、高い廃棄確率 (001110) • <i>af21</i> — AF クラス 2、低い廃棄確率 (010010) • <i>af22</i> — AF クラス 2、中程度の廃棄確率 (010100) • <i>af23</i> — AF クラス 2、高い廃棄確率 (010110) • <i>af31</i> — AF クラス 3、低い廃棄確率 (011010) • <i>af32</i> — AF クラス 3、中程度の廃棄確率 (011100) • <i>af33</i> — AF クラス 3、高い廃棄確率 (011110) • <i>af41</i> — AF クラス 4、低い廃棄確率 (100010) • <i>af42</i> — AF クラス 4、中程度の廃棄確率 (100100) • <i>af43</i> — AF クラス 4、高い廃棄確率 (100110) • <i>cs1</i> — Class-selector (CS) 1、優先順位 1 (001000) • <i>cs2</i> — CS2、優先順位 2 (010000) • <i>cs3</i> — CS3、優先順位 3 (011000) • <i>cs4</i> — CS4、優先順位 4 (100000) • <i>cs5</i> — CS5、優先順位 5 (101000) • <i>cs6</i> — CS6、優先順位 6 (110000) • <i>cs7</i> — CS7、優先順位 7 (111000) • <i>default</i> — デフォルトの DSCP 値 (000000) • <i>if</i> — 緊急フォワーディング (101110)
<i>precedence precedence</i>	<p>(任意) <i>precedence</i> 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。 <i>precedence</i> 引数には、次の数値またはキーワードを指定します。</p> <ul style="list-style-type: none"> • 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 • <i>critical</i> — Precedence 5 (101) • <i>flash</i> — Precedence 3 (011) • <i>flash-override</i> — Precedence 4 (100) • <i>immediate</i> — Precedence 2 (010) • <i>internet</i> — Precedence 6 (110) • <i>network</i> — Precedence 7 (111) • <i>priority</i> — Precedence 1 (001) • <i>routine</i> — Precedence 0 (000)

<i>fragments</i>	(任意) 最初のフラグメントではないパケットだけをルールと一致させます。このキーワードは、TCP ポート番号などのレイヤ 4 オプションを指定したルールには使用できません。これらのオプションを評価するために必要な情報は、最初のフラグメントだけに含まれているからです。
<i>log</i>	(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。 <ul style="list-style-type: none"> • 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
<i>time-range</i> <i>time-range-name</i>	(任意) このルールに適用する時間範囲を指定します。 時間範囲の指定には、 time-range コマンドを使用します。
<i>icmp-message</i>	(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。
<i>igmp-message</i>	(IGMP のみ: (任意) ルールと一致させる IGMP メッセージのタイプ。 <i>igmp-message</i> 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。 <ul style="list-style-type: none"> • <i>dvmrp</i> — 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) • <i>host-query</i> — ホスト クエリー • <i>host-report</i> — ホスト レポート • <i>pim</i> — Protocol Independent Multicast (PIM) • <i>trace</i> — マルチキャスト トレース
<i>operator port [port]</i>	(任意: TCP および UDP のみ) <i>operator</i> および <i>port</i> 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、 <i>source</i> または <i>destination</i> 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。 <i>port</i> 引数には、TCP または UDP ポートの名前または番号を指定します。有効な値は 0 ~ 65535 の整数です。有効なポート名のリストは、「使用上のガイドライン」の「TCP ポート名」および「UDP ポート名」を参照してください。 2 番目の <i>port</i> 引数は、 <i>operator</i> 引数が範囲である場合にのみ必要です。 <i>operator</i> 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。 <ul style="list-style-type: none"> • <i>eq</i> — パケットのポートが <i>port</i> 引数と同等である場合にのみ一致します。 • <i>gt</i> — パケットのポートが <i>port</i> 引数より大きい場合にのみ一致します。 • <i>lt</i> — パケットのポートが <i>port</i> 引数より小さい場合にのみ一致します。 • <i>neq</i> — パケットのポートが <i>port</i> 引数と同等ではない場合にのみ一致します。 • <i>range</i> — 2 つの <i>port</i> 引数が必要です。パケットのポートが最初の <i>port</i> 引数以上で、2 番目の <i>port</i> 引数以下である場合にのみ一致します。

<i>portgroup</i> <i>portgroup</i>	(任意: TCP および UDP のみ) <i>portgroup</i> 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、 <i>source</i> または <i>destination</i> 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。
<i>flags</i>	(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。 <i>flags</i> 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。 <ul style="list-style-type: none"> • <i>ack</i> • <i>fin</i> • <i>psh</i> • <i>rst</i> • <i>syn</i> • <i>urg</i>
<i>established</i>	(TCP のみ; 任意) 確立された TCP 接続に属すパケットだけを、ルールと一致させます。ACK または RST ビットが設定されている TCP パケットは、確立された接続に属しているとみなされます。

デフォルト

新しく作成した IPv4 ACL には、ルールは含まれていません。

シーケンス番号を指定しないと、ACL の最後のルールのシーケンス番号に 10 を加算したシーケンス番号が割り当てられます。

コマンド モード

IPv4 ACL コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

パケットに IPv4 ACL が適用されると、ACL 内のすべてのルールに対してパケットが評価されます。パケットが条件に一致した最初のルールが施行されます。複数のルールの条件と一致する場合は、シーケンス番号が最も低いルールが施行されます。

このコマンドには、ライセンスは不要です。

送信元および宛先

source および *destination* 引数は、次のいずれかの方法で指定できます。どのルールも、一方の引数の指定方法によって、他方の引数の指定方法が決まることはありません。ルールの設定時に使用できる *source* および *destination* 引数の指定方法は、次のとおりです。

- IP アドレス グループ オブジェクト — IPv4 アドレス グループ オブジェクトを使用して、*source* または *destination* 引数を指定できます。IPv4 アドレス グループ オブジェクトを作成および変更するには、**object-group ip address** コマンドを使用します。シンタックスは、次のとおりです。

```
addrgroup address-group-name
```

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

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

- アドレスおよびネットワーク ワイルドカード — IPv4 アドレスおよびネットワーク ワイルドカードを使用して、送信元または宛先とするホストまたはネットワークを指定できます。シンタックスは、次のとおりです。

```
IPv4-address network-wildcard
```

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

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

- アドレスおよび Variable-Length Subnet Mask (VLSM; 可変長サブネット マスク) — IPv4 アドレスおよび VLSM を使用して、送信元または宛先とするホストまたはネットワークを指定できます。シンタックスは、次のとおりです。

```
IPv4-address/prefix-len
```

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

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

- ホスト アドレス — *host* キーワードおよび IPv4 アドレスを使用して、送信元または宛先とするホストを指定できます。シンタックスは、次のとおりです。

```
host IPv4-address
```

このシンタックスは、*IPv4-address/32* および *IPv4-address 0.0.0.0* と同じです。

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

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

- 任意のアドレス — *any* キーワードを使用して、送信元または宛先として任意の IPv4 アドレスを指定できます。*any* キーワードの使用例は、このセクションの例を参照してください。各例に、*any* キーワードを使用した送信元または宛先の指定方法が示されています。

ICMP メッセージ タイプ

icmp-message 引数には、0 ~ 255 の整数である ICMP メッセージ番号を指定します。また、次のいずれかのキーワードを指定できます。

- *administratively-prohibited* — 管理上の禁止
- *alternate-address* — 代替アドレス
- *conversion-error* — データグラム変換
- *dod-host-prohibited* — ホスト禁止
- *dod-net-prohibited* — ネット禁止
- *echo* — エコー (ping)
- *echo-reply* — エコー応答
- *general-parameter-problem* — パラメータの問題
- *host-isolated* — ホスト分離

- *host-precedence-unreachable* — 優先順位のホスト到達不能
- *host-redirect* — ホストリダイレクト
- *host-tos-redirect* — ToS ホストリダイレクト
- *host-tos-unreachable* — ToS ホスト到達不能
- *host-unknown* — ホスト未知
- *host-unreachable* — ホスト到達不能
- *information-reply* — 情報応答
- *information-request* — 情報要求
- *mask-reply* — マスク応答
- *mask-request* — マスク要求
- *mobile-redirect* — モバイルホストリダイレクト
- *net-redirect* — ネットワークリダイレクト
- *net-tos-redirect* — ToS ネットリダイレクト
- *net-tos-unreachable* — ToS ネット到達不能
- *net-unreachable* — ネット到達不能
- *network-unknown* — ネットワーク未知
- *no-room-for-option* — パラメータが必要だが空きなし
- *option-missing* — パラメータが必要だが存在しない
- *packet-too-big* — フラグメンテーションが必要、DF 設定
- *parameter-problem* — すべてのパラメータの問題
- *port-unreachable* — ポート到達不能
- *precedence-unreachable* — 優先順位カットオフ
- *protocol-unreachable* — プロトコル到達不能
- *reassembly-timeout* — 再構成タイムアウト
- *redirect* — すべてのリダイレクト
- *router-advertisement* — ルータディスカバリアドバタイズメント
- *router-advertisement* — ルータディスカバリアドバタイズメント
- *source-quench* — 送信元抑制
- *source-route-failed* — 送信元ルート障害
- *time-exceeded* — すべてのタイム超過メッセージ
- *timestamp-reply* — タイムスタンプ応答
- *timestamp-request* — タイムスタンプ要求
- *traceroute* — トレースルート
- *ttl-exceeded* — TTL 超過
- *unreachable* — すべての到達不能

TCP ポート名

protocol 引数に *tcp* を指定した場合、*port* 引数として 0 ~ 65535 の整数である TCP ポート番号を指定できます。また、次のいずれかのキーワードを指定できます。

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

chargen — キャラクタジェネレータ (19)

cmd — リモートコマンド (rcmd、514)

daytime — デイタイム (13)

- discard* — 廃棄 (9)
- domain* — Domain Name Service (DNS; ドメイン ネーム サービス) (53)
- drip* — Dynamic Routing Information Protocol (DRIP; ダイナミック ルーティング情報プロトコル) (3949)
- echo* — エコー (7)
- exec* — Exec (rsh、512)
- finger* — フィンガー (79)
- ftp* — File Transfer Protocol (FTP; ファイル転送プロトコル) (21)
- ftp-data* — FTP データ接続 (2)
- gopher* — Gopher (7)
- hostname* — NIC ホストネーム サーバ (11)
- ident* — Ident プロトコル (113)
- irc* — Internet Relay Chat (IRC; インターネット リレー チャット) (194)
- klogin* — Kerberos ログイン (543)
- kshell* — Kerberos シェル (544)
- login* — ログイン (rlogin、513)
- lpd* — プリンタ サービス (515)
- nntp* — Network News Transport Protocol (NNTP) (119)
- pim-auto-rp* — PIM Auto-RP (496)
- pop2* — Post Office Protocol v2 (POP2) (19)
- pop3* — Post Office Protocol v3 (POP3) (11)
- smtp* — Simple Mail Transport Protocol (SMTP; シンプル メール転送プロトコル) (25)
- sunrpc* — Sun Remote Procedure Call (RPC; リモート プロシージャ コール) (111)
- tacacs* — TAC Access Control System (49)
- talk* — Talk (517)
- telnet* — Telnet (23)
- time* — Time (37)
- uucp* — UNIX-to-UNIX Copy Program (UUCP; UNIX 間コピー プログラム) (54)
- whois* — WHOIS/NICNAME (43)
- www* — World Wide Web (HTTP、8)

UDP ポート名

protocol 引数に *udp* を指定した場合、*port* 引数として 0 ~ 65535 の整数である UDP ポート番号を指定できます。また、次のいずれかのキーワードを指定できます。

- biff* — BIFF (メール通知、comsat、512)
- bootpc* — Bootstrap Protocol (BOOTP; ブートストラッププロトコル) クライアント (68)

bootps — Bootstrap Protocol (BOOTP; ブートストラップ プロトコル) サーバ (67)

discard — 廃棄 (9)

dnsix — DNSIX セキュリティ プロトコル 監査 (195)

domain — Domain Name Service (DNS; ドメイン ネーム サービス) (53)

echo — エコー (7)

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

mobile-ip — モバイル IP レジストレーション (434)

nameserver — IEN116 ネーム サービス (旧式、42)

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

netbios-ns — NetBIOS ネーム サービス (137)

netbios-ss — NetBIOS セッション サービス (139)

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

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

pim-auto-rp — PIM Auto-RP (496)

rip — Routing Information Protocol (RIP) (ルータ、in.routed、52)

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

snmptrap — SNMP トラップ (162)

sunrpc — Sun Remote Procedure Call (RPC; リモート プロシージャ コール) (111)

syslog — システム ロギング (514)

tacacs — TAC Access Control System (49)

talk — Talk (517)

tftp — Trivial File Transfer Protocol (TFTP; 簡易ファイル転送プロトコル) (69)

time — Time (37)

who — Who サービス (rwho、513)

xdmcp — X Display Manager Control Protocol (XDMCP) (177)

例

次に、*acl-lab-01* という IPv4 ACL を作成し、10.23.0.0 および 192.168.37.0 ネットワークから 10.176.0.0 ネットワークへのすべての TCP および UDP トラフィックを許可するルールを設定する例を示します。

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


次に、`acl-eng-to-marketing` という IPv4 ACL を作成し、`eng_workstations` という IP アドレス オブジェクトグループから `marketing_group` という IP アドレス オブジェクトグループへのすべての IP トラフィックを許可するルールを設定する例を示します。

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

関連コマンド

コマンド	説明
<code>deny (IPv4)</code>	IPv4 ACL に拒否 (deny) ルールを設定します。
<code>ip access-list</code>	IPv4 ACL を設定します。
<code>object-group ip address</code>	IPv4 アドレス オブジェクトグループを設定します。
<code>object-group ip port</code>	IP ポート オブジェクトグループを設定します。
<code>remark</code>	ACL に備考を設定します。
<code>show ip access-list</code>	すべての IPv4 ACL または 1 つの IPv4 ACL を表示します。
<code>statistics per-entry</code>	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。
<code>time-range</code>	時間範囲を設定します。

permit (MAC)

条件と一致するトラフィックを許可する MAC ACL ルールを作成するには、**permit** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

```
[sequence-number] permit source destination [protocol] [cos cos-value] [vlan VLAN-ID]
```

```
no permit source destination [protocol] [cos cos-value] [vlan VLAN-ID]
```

```
no sequence-number
```

シンタックスの説明

<i>sequence-number</i>	(任意) permit コマンドのシーケンス番号。アクセスリストの該当番号の位置にコマンドが挿入されます。シーケンス番号により、ACL 内のルールの順序が保持されます。 シーケンス番号は、1 ~ 4294967295 の任意の整数です。 デフォルトでは、ACL 内の最初のルールにシーケンス番号 10 が割り当てられます。 シーケンス番号を指定しないと、ACL の最後にルールが追加され、1 つ前のルールのシーケンス番号に 10 を加算した値が、シーケンス番号として割り当てられます。 ルールのシーケンス番号を再割り当てするには、 resequence コマンドを使用します。
<i>source</i>	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。
<i>destination</i>	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。
<i>protocol</i>	(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。
<i>cos cos-value</i>	(任意) IEEE 802.1Q ヘッダーに、 <i>cos-value</i> 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。 <i>cos-value</i> 引数は、0 ~ 7 の整数です。
<i>vlan VLAN-ID</i>	(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。 <i>VLAN-ID</i> 引数は、1 ~ 4094 の整数です。

デフォルト

なし

コマンド モード

MAC ACL コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

新しく作成した MAC ACL には、ルールは含まれていません。

シーケンス番号を指定しないと、ACL の最後のルールのシーケンス番号に 10 を加算したシーケンス番号が割り当てられます。

パケットに MAC ACL が適用されると、ACL 内のすべてのルールに対してパケットが評価されます。パケットが条件に一致した最初のルールが施行されます。複数のルールの条件と一致する場合は、シーケンス番号が最も低いルールが施行されます。

このコマンドには、ライセンスは不要です。

送信元および宛先

source および *destination* 引数は、次のどちらかの方法で指定できます。どのルールも、一方の引数の指定方法によって、他方の引数の指定方法が決まることはありません。ルールの設定時に使用できる *source* および *destination* 引数の指定方法は、次のとおりです。

- アドレスおよびマスク — MAC アドレスのあとにマスクを指定して、1 つのアドレスまたはアドレス グループを指定できます。シンタックスは、次のとおりです。

MAC-address MAC-mask

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

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

次に、*destination* 引数に、MAC ベンダー コードが 00603e のすべてのホストの MAC アドレスを指定する例を示します。

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

- 任意のアドレス — *any* キーワードを使用して、送信元または宛先として任意の MAC アドレスを指定できます。*any* キーワードの使用例は、このセクションの例を参照してください。各例に、*any* キーワードを使用した送信元または宛先の指定方法が示されています。

MAC プロトコル

protocol 引数には、MAC プロトコルの番号またはキーワードを指定します。プロトコル番号は、プレフィックスが 0x である 4 バイト 16 進値です。有効なプロトコル番号は 0x0 ~ 0xffff です。有効なキーワードは、次のとおりです。

- *aarp* — Appletalk ARP (0x80f3)
- *appletalk* — Appletalk (0x809b)
- *decnet-iv* — DECnet Phase IV (0x6003)
- *diagnostic* — DEC Diagnostic Protocol (0x6005)
- *etype-6000* — Ethertype 0x6000 (0x6000)
- *etype-8042* — Ethertype 0x8042 (0x8042)
- *ip* — Internet Protocol v4 (0x0800)
- *lat* — DEC LAT (0x6004)
- *lave-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)

■ permit (MAC)

例 次に、`mac-ip-filter` という MAC ACL を作成し、2 つの MAC アドレス グループ間ですべての IPv4 トラフィックを許可するルールを設定する例を示します。

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

関連コマンド

コマンド	説明
<code>deny (MAC)</code>	MAC ACL に拒否 (<code>deny</code>) ルールを設定します。
<code>mac access-list</code>	MAC ACL を設定します。
<code>remark</code>	ACL に備考を設定します。
<code>statistics per-entry</code>	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。
<code>show mac access-list</code>	すべての MAC ACL または 1 つの MAC ACL を表示します。

permit (ロールベース アクセス コントロール リスト)

Security Group Access Control List (SGACL; セキュリティ グループ アクセス コントロール リスト) に許可ルールを設定するには、**permit** コマンドを使用します。ルールを削除するには、このコマンドの **no** 形式を使用します。

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

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

シンタックスの説明

all	すべてのトラフィックを指定します。
icmp	Internet Control Message Protocol (ICMP; インターネット制御メッセージプロトコル) トラフィックを指定します。
igmp	Internet Group Management Protocol (IGMP; インターネット グループ管理プロトコル) トラフィックを指定します。
ip	IP トラフィックを指定します。
tcp	TCP トラフィックを指定します。
udp	User Datagram Protocol (UDP; ユーザ データグラム プロトコル) トラフィックを指定します。
src	送信元ポート番号を指定します。
dest	宛先ポート番号を指定します。
eq	ポート番号と同等の番号を指定します。
gt	ポート番号より大きい番号を指定します。
lt	ポート番号より小さい番号を指定します。
neq	ポート番号と同等ではない番号を指定します。
port-number	TCP または UDP のポート番号。範囲は 0 ~ 65535 です。
range	TCP または UDP のポート範囲を指定します。
port-number1	範囲の開始ポート。範囲は 0 ~ 65535 です。
port-number2	範囲の終了ポート。範囲は 0 ~ 65535 です。

デフォルト

なし

コマンド モード

ロールベース アクセス コントロール リスト

サポートされるユーザロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

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

このコマンドには、アドバンスド サービス ライセンスが必要です。

■ permit (ロールベース アクセス コントロール リスト)

例

次に、SGACL に許可ルールを追加する例を示します。

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

次に、SGACL から許可ルールを削除する例を示します。

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

関連コマンド

コマンド	説明
cts role-based access-list	Cisco TrustSec SGACL を設定します。
deny (ロールベース アクセス コントロール リスト)	SGACL に拒否ルールを設定します。
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts role-based access-list	Cisco TrustSec SGACL の設定を表示します。

permit interface

ユーザ ロール インターフェイス ポリシーでインターフェイスを許可するには、**permit interface** コマンドを使用します。インターフェイスを拒否するには、このコマンドの **no** 形式を使用します。

```
permit interface {ethernet slot/port[- port2] interface-list}
```

```
no permit interface
```

シンタックスの説明

ethernet slot/port	イーサネット インターフェイスの識別名
- port	モジュール上のインターフェイス範囲の最後のインターフェイスを指定します。
interface-list	イーサネット インターフェイスの識別名をカンマで区切ってリストします。

デフォルト

すべてのインターフェイス

コマンド モード

ユーザ ロール インターフェイス ポリシー コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

interface policy deny コマンドを使用すると、**permit interface** コマンドで許可したインターフェイスを除き、すべてのインターフェイスへのユーザ ロール アクセスが拒否されます。

このコマンドには、ライセンスは不要です。

例

次に、ユーザ ロール インターフェイス ポリシーでインターフェイス範囲を許可する例を示します。

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)# permit interface ethernet 2/1 - 8
```

次に、ユーザ ロール インターフェイス ポリシーでインターフェイスのリストを許可する例を示します。

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)# permit interface ethernet 1/1, ethernet 1/3, ethernet 1/5, ethernet 1/7
```

次に、ユーザ ロール インターフェイス ポリシーでインターフェイスを拒否する例を示します。

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)# no permit interface ethernet 2/1
```

関連コマンド

コマンド	説明
interface policy deny	ユーザ ロールのインターフェイス ポリシー コンフィギュレーションモードを開始します。
role name	ユーザ ロールを作成または指定して、ユーザ ロール コンフィギュレーションモードを開始します。
show role	ユーザ ロールの情報を表示します。

permit vlan

ユーザ ロール VLAN ポリシーで VLAN を許可するには、**permit vlan** コマンドを使用します。VLAN を削除するには、このコマンドの **no** 形式を使用します。

```
permit vlan {vlan-id[- vlan-id2] | vlan-list}
```

```
no permit vlan
```

シンタックスの説明

<i> vlan-id </i>	VLAN 識別番号。範囲は 1 ～ 3967 および 4048 ～ 4093 です。
<i>-vlan-id2</i>	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。
<i> vlan-list </i>	VLAN 識別番号をカンマで区切ってリストします。

デフォルト

すべての VLAN

コマンドモード

ユーザ ロール VLAN ポリシー コンフィギュレーション

サポートされるユーザロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

vlan policy deny コマンドを使用すると、**permit vlan** コマンドで許可した VLAN を除き、すべての VLAN へのユーザ ロール アクセスが拒否されます。

このコマンドには、ライセンスは不要です。

例

次に、ユーザ ロール VLAN ポリシーで VLAN 識別番号を許可する例を示します。

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)# permit vlan 8
```

次に、ユーザ ロール VLAN ポリシーで VLAN 識別番号の範囲を許可する例を示します。

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)# permit vlan 1-8
```

次に、ユーザ ロール VLAN ポリシーで VLAN 識別番号のリストを許可する例を示します。

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)# permit vlan 1, 10, 12, 20
```

次に、ユーザ ロール VLAN ポリシーから VLAN を削除する例を示します。

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# vlan policy deny
switch(config-role-vlan)# no permit vlan 2
```

関連コマンド

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

permit vrf

ユーザ ロール VRF ポリシーで、Virtual Routing and Forwarding (VRF) インスタンスを許可するには、**permit vrf** コマンドを使用します。VRF を削除するには、このコマンドの **no** 形式を使用します。

```
permit vrf vrf-name
```

```
no permit vrf vrf-name
```

シンタックスの説明	<i>vrf-name</i> VRF の名前。大文字と小文字を区別して、指定します。
------------------	---

デフォルト	すべての VRF
--------------	----------

コマンド モード	ユーザ ロール VRF ポリシー コンフィギュレーション
-----------------	------------------------------

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

コマンド履歴	リリース 変更内容
	4.0(1) このコマンドが導入されました。

使用上のガイドライン **vrf policy deny** コマンドを使用すると、**permit vrf** コマンドで許可した VRF を除き、すべての VRF へのユーザ ロール アクセスが拒否されます。

ユーザ ロールで複数の VRF 名を許可するには、このコマンドを繰り返して設定します。

このコマンドには、ライセンスは不要です。

例 次に、ユーザ ロール VRF ポリシーで VRF 名を許可する例を示します。

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# vrf policy deny
switch(config-role-vrf)# permit vrf management
```

次に、ユーザ ロール VRF ポリシーから VRF 名を削除する例を示します。

```
switch# config t
switch(config)# role name MyRole
switch(config-role)# vrf policy deny
switch(config-role-vrf)# no permit vrf engineering
```

関連コマンド	コマンド	説明
	vrf policy deny	ユーザ ロールの VRF ポリシー コンフィギュレーション モードを開始します。
	role name	ユーザ ロールを作成または指定して、ユーザ ロール コンフィギュレーション モードを開始します。
	show role	ユーザ ロールの情報を表示します。

platform access-list update

Access Control List (ACL; アクセス コントロール リスト) の変更により、スーパーバイザ モジュールで I/O モジュールをアップデートする方法を設定するには、**platform access-list** コマンドを使用します。アトミック アップデートをディセーブルにするには、このコマンドの **no** 形式を使用します。

platform access-list update {atomic | default-result permit}

no platform access-list update {atomic | default-result permit}

シンタックスの説明	atomic	default-result permit
	トラフィックを中断しないでアップデートを実行する、アトミック アップデートを指定します。NX-OS デバイスは、デフォルトでアトミック ACL アップデートを実行します。	非アトミック アップデートの実行中に、アップデートした ACL が適用されるトラフィックを許可します。

デフォルト **atomic**

コマンド モード グローバル コンフィギュレーション

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

コマンド履歴	リリース	変更内容
	4.0(1)	このコマンドが導入されました。

使用上のガイドライン NX-OS デバイスは、デフォルトで、アップデートした ACL が適用されるトラフィックを中断しない、アトミック ACL アップデートを実行します。ただし、アトミック アップデートでは、アップデート対象の I/O モジュールに、変更する ACL の各アップデート エントリを保管できるだけの十分なリソースが必要になります。アップデートが完了すると、アップデートに使用された追加リソースは解放されます。I/O モジュールのリソースが不足している場合、エラー メッセージが表示され、I/O モジュールの ACL アップデートは失敗します。

I/O モジュールのリソースが不足している場合は、**no platform access-list update atomic** コマンドを使用して、アトミック アップデートをディセーブルにできます。ただし、ACL をアップデートして旧 ACL を削除するまでの短い処理時間中、ACL が適用されるトラフィックはデフォルトでドロップされます。

非アトミック アップデートの実行中に、アップデートした ACL が適用されるすべてのトラフィックを許可したい場合は、**platform access-list update default-result permit** コマンドを使用します。

このコマンドには、ライセンスは不要です。

例

次に、ACL のアトミック アップデートをディセーブルにする例を示します。

```
switch# config t
switch(config)# no platform access-list update atomic
```

次に、ACL の非アトミック アップデート中に、対象トラフィックが許可されるように設定する例を示します。

```
switch# config t
switch(config)# platform access-list update default-result permit
```

次に、再びアトミック アップデートが実行されるように設定する例を示します。

```
switch# config t
switch(config)# no access-list update default-result permit
switch(config)# platform access-list update atomic
```

関連コマンド

コマンド	説明
<code>show running-config all</code>	デフォルト設定を含む、実行コンフィギュレーションを表示します。

platform rate-limit

出力トラフィックのレート制限をパケット / 秒単位で設定するには、**platform rate-limit** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

```
platform rate-limit {access-list-log | copy | layer-2 {port-security | storm-control} | layer-3 {control
| glean | mtu | multicast {directly-connect | local-groups | rpf-leak} | ttl} | receive} packets
```

```
no platform rate-limit {access-list-log | copy | layer-2 {port-security | storm-control} | layer-3
{control | glean | mtu | multicast {directly-connect | local-groups | rpf-leak} | ttl} | receive}
[packets]
```

シンタックスの説明

access-list-log	アクセス リスト ロギングのためにスーパーバイザ モジュールにコピーされるパケットを指定します。デフォルトのレートは 100 パケット / 秒です。
copy	スーパーバイザ モジュールにコピーされるデータ パケットと制御パケットを指定します。デフォルトのレートは 30000 パケット / 秒です。
layer-2 storm-control	ストーム制御パケットを指定します。デフォルトのレートは 0 パケット / 秒です。
layer-2	レイヤ 1 パケットのレート制限を指定します。
port-security	ポート セキュリティ パケットを指定します。デフォルトはディセーブルです。
storm-control layer-3	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。レイヤ 3 パケットを指定します。
control	レイヤ 3 制御パケットを指定します。デフォルトのレートは 10000 パケット / 秒です。
glean	レイヤ 3 グリーニング パケットを指定します。デフォルトのレートは 100 パケット / 秒です。
mtu	レイヤ 3 MTU 障害リダイレクト パケットを指定します。デフォルトのレートは 500 パケット / 秒です。
multicast	レイヤ 3 マルチキャスト パケット / 秒を指定します。
directly-connect	直接接続マルチキャスト パケットを指定します。デフォルトのレートは 10000 パケット / 秒です。
local-groups	ローカル グループ マルチキャスト パケットを指定します。デフォルトのレートは 10000 パケット / 秒です。
rpf-leak	Reverse Path Forwarding (RPF) リーク パケットを指定します。デフォルトのレートは 500 パケット / 秒です。
ttl	レイヤ 3 TTL 障害リダイレクト パケットを指定します。デフォルトのレートは 500 パケット / 秒です。
receive	スーパーバイザ モジュールにリダイレクトされるパケットを指定します。デフォルトのレートは 30000 パケット / 秒です。
packets	パケット数 / 秒。範囲は 1 ~ 33554431 です。

デフォルト

デフォルトのレート制限は、「シンタックスの説明」を参照してください。

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザロール network-admin
vdc-admin

コマンド履歴	リリース	変更内容
	4.0(1)	このコマンドが導入されました。
	4.0(3)	port-security キーワードが追加されました。

使用上のガイドライン このコマンドには、ライセンスは不要です。

例 次に、制御パケットのレート制限を設定する例を示します。

```
switch# config t
switch(config)# platform rate-limit layer-3 control 20000
```

次に、制御パケットのレート制限をデフォルトの設定に戻す例を示します。

```
switch# config t
switch(config)# no platform rate-limit layer-3 control
```

関連コマンド	コマンド	説明
	show running-config	実行コンフィギュレーションを表示します。

police

コントロールプレーン ポリシー マップのクラス マップにポリシングを設定するには、**police** コマンドを使用します。コントロールプレーン ポリシー マップのクラス マップからポリシングを削除するには、このコマンドの **no** 形式を使用します。

```
police [cir] cir-rate [bps | gbps | kbps | mbps | pps]
police [cir] cir-rate [bps | gbps | kbps | mbps] [bc] burst-size [bytes | kbytes | mbytes | ms | packets | us]
police [cir] cir-rate [bps | gbps | kbps | mbps | pps]
    conform {drop | set-cos-transmit cos-value | set-dscp-transmit dscp-value | set-prec-transmit
    prec-value | transmit} [exceed {drop | set dscp dscp table cir-markdown-map | transmit}]
    [violate {drop | set dscp dscp table pir-markdown-map | transmit}]
police [cir] cir-rate [bps | gbps | kbps | mbps | pps]
    pir pir-rate [bps | gbps | kbps | mbps] [[be] extended-burst-size [bytes | kbytes | mbytes | ms |
    packets | us]]
no police [cir] cir-rate [bps | gbps | kbps | mbps | pps]
n o police [cir] cir-rate [bps | gbps | kbps | mbps | pps] [bc] burst-size [bytes | kbytes | mbytes | ms |
    packets | us]
no police [cir] cir-rate [bps | gbps | kbps | mbps | pps]
    conform {drop | set-cos-transmit cos-value | set-dscp-transmit dscp-value | set-prec-transmit
    prec-value | transmit} [exceed {drop | set dscp dscp table cir-markdown-map | transmit}]
    [violate {drop | set dscp dscp table pir-markdown-map | transmit}]
no police [cir] cir-rate [bps | gbps | kbps | mbps | pps]
    pir pir-rate [bps | gbps | kbps | mbps | pps] [[be] extended-burst-size [bytes | kbytes | mbytes | ms
    | packets | us]]
```

シンタックスの説明

cir	(任意) Committed Information Rate (CIR; 認定情報レート) を指定します。
<i>cir-rate</i>	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。
<i>burst-size</i>	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 <i>cos-value</i>	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 <i>dscp-value</i>	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 <i>prec-value</i>	IPv4 および IPv6 パケットの優先順位の値を指定します。範囲は 0 ~ 7 です。
transmit	送信処理を指定します。
exceed	トラフィックが指定のレートおよびバーストを超過したときの処理を設定します。
set dscp dscp table cir-markdown-map	CIR マークダウン マップ上でパケットをフラグ付けします。

violate	(任意) トラフィックが指定のレートおよびバーストに違反したときの処理を設定します。
set dscp dscp table pir-markdown-map	PIR マークダウン マップ上でパケットをフラグ付けします。
pir pir-rate	PIR レートを指定します。
be	(任意) 拡張バーストのサイズを指定します。
extended-burst-size	拡張バーストのサイズ。範囲は 1 ~ 512000000 です。

デフォルト

なし

コマンド モード

ポリシー マップ コンフィギュレーション

サポートされるユーザ ロールnetwork-admin
vdc-admin**コマンド履歴**

リリース	変更内容
4.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用できるのは、デフォルトの VDC だけです。

このコマンドには、ライセンスは不要です。

例

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

```
switch# config t
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# class ClassMapA
switch(config-pmap-c)# police cir 2000 kbps
```

次に、コントロールプレーン ポリシー マップを削除する例を示します。

```
switch# config t
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)# class ClassMapA
switch(config-pmap-c)# no police 2000 kbps
```

関連コマンド

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

policy

Cisco TrustSec デバイス識別情報または Security Group Tag (SGT; セキュリティ グループ タグ) を使用して、インターフェイス上に Cisco TrustSec 認証ポリシーを手動で設定するには、**policy** コマンドを使用します。デフォルトの設定に戻すには、このコマンドの **no** 形式を使用します。

```
policy {dynamic identity device-id | static sgt sgt-value [trusted]}
```

```
no policy {dynamic | static}
```

シンタックスの説明

dynamic identity	Cisco TrustSec デバイス識別情報を使用してダイナミック ポリシーを指定します。
<i>device-id</i>	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。
<i>sgt-value</i>	Cisco TrustSec SGT。形式は、 0xhhh です。範囲は 0x1 ~ 0xfffd です。
trusted	(任意) インターフェイス上で受信したトラフィックに SGT が設定されている場合、タグを上書きしません。

デフォルト

なし

コマンド モード

Cisco TrustSec マニュアル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更内容
4.0(1)	このコマンドが導入されました。
4.0(3)	コマンドの no 形式で、 dynamic および static に続くキーワードとオプションが削除されました。

使用上のガイドライン

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

設定を有効にするには、このコマンドの使用後に、**shutdown/no shutdown** コマンド シーケンスを使用して、インターフェイスをディセーブルにしてから、再びイネーブルにする必要があります。このコマンドには、アドバンスド サービス ライセンスが必要です。

例

次に、インターフェイスにダイナミック Cisco TrustSec ポリシーを手動で設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# cts manual
switch(config-if-cts-manual)# policy dynamic identity DeviceB
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

次に、手動で設定したダイナミック Cisco TrustSec ポリシーをインターフェイスから削除する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/3
switch(config-if)# cts manual
switch(config-if-cts-manual)# no policy dynamic identity DeviceB
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

次に、インターフェイスにスタティック Cisco TrustSec ポリシーを手動で設定する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/4
switch(config-if)# cts manual
switch(config-if-cts-manual)# policy static sgt 0x100
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

次に、手動で設定したスタティック Cisco TrustSec ポリシーをインターフェイスから削除する例を示します。

```
switch# config t
switch(config)# interface ethernet 2/4
switch(config-if)# cts manual
switch(config-if-cts-manual)# no policy static sgt 0x100
switch(config-if-cts-manual)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

関連コマンド

コマンド	説明
cts manual	インターフェイスの Cisco TrustSec マニュアル コンフィギュレーション モードを開始します。
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts interface	インターフェイスの Cisco TrustSec 設定を表示します。

policy-map type control-plane

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

policy-map type control-plane *policy-map-name*

no policy-map type control-plane *policy-map-name*

シンタックスの説明	<i>policy-map-name</i> ポリシーマップの名前。名前は、最大 64 文字で、大文字と小文字を区別した英数字で指定します。
------------------	--

デフォルト	なし
--------------	----

コマンドモード	グローバル コンフィギュレーション
----------------	-------------------

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

コマンド履歴	リリース 変更内容
	4.0(1) このコマンドが導入されました。

使用上のガイドライン	このコマンドを使用できるのは、デフォルトの VDC だけです。 このコマンドには、ライセンスは不要です。
-------------------	---

例	次に、コントロールプレーンポリシーマップを指定して、ポリシーマップコンフィギュレーションモードを開始する例を示します。
----------	---

```
switch# config t
switch(config)# policy-map type control-plane PolicyMapA
switch(config-pmap)#
```

次に、コントロールプレーンポリシーマップを削除する例を示します。

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

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

propagate-sgt

レイヤ 2 Cisco TrustSec インターフェイス上で SGT 伝搬をイネーブルにするには、**propagate-sgt** コマンドを使用します。SGT 伝搬をディセーブルにするには、このコマンドの **no** 形式を使用します。

propagate-sgt

no propagate-sgt

シンタックスの説明 このコマンドには、引数またはキーワードはありません。

デフォルト イネーブル

コマンド モード グローバル コンフィギュレーション

サポートされるユーザロール network-admin
vdc-admin

コマンド履歴	リリース	変更内容
	4.0(3)	このコマンドが導入されました。

使用上のガイドライン インターフェイスに接続しているピアデバイスが SGT タグ付きの Cisco TrustSec パケットを処理できない場合には、インターフェイス上の SGT 伝搬機能をディセーブルに設定できます。

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

設定を有効にするには、このコマンドの使用後に、**shutdown/no shutdown** コマンドシーケンスを使用して、インターフェイスをディセーブルにしてから、再びイネーブルにする必要があります。

このコマンドには、アドバンスド サービス ライセンスが必要です。

例 次に、SGT 伝搬をディセーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# no propagate-sgt
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

次に、SGT 伝搬をイネーブルにする例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 2/1
switch(config-if)# cts dot1x
switch(config-if-cts-dot1x)# propagate-sgt
switch(config-if-cts-dot1x)# exit
switch(config-if)# shutdown
switch(config-if)# no shutdown
```

関連コマンド

コマンド	説明
cts dot1x	インターフェイスの Cisco TrustSec 802.1X コンフィギュレーション モードを開始します。
feature cts	Cisco TrustSec 機能をイネーブルにします。
show cts interface	インターフェイスの Cisco TrustSec 設定を表示します。