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。

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**

no *sequence-number*

no permit ip {**any** | **host** *sender-IP* | *sender-IP sender-IP-mask*} **mac any**

構文の説明

sequence-number	（任意）**permit** コマンドのシーケンス番号。デバイスによってアクセス 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。 シーケンス番号には、1 ～ 4294967295 の間の整数を指定できます。 デフォルトでは、ACL の最初のルールには、10 のシーケンス番号が与えられます。 シーケンス番号を指定しないと、デバイスによって、ACL の最後にルールが追加され、1 つ前のルールのシーケンス番号に 10 を加算した値が、シーケンス番号として割り当てられます。 ルールのシーケンス番号を再割り当てするには、**resequence** コマンドを使用します。
ip	ルールの IP アドレス部分を指定します。
any	任意のホストが、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 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。

コマンド デフォルト

なし

コマンド モード

ARP ACL コンフィギュレーション モード

コマンド履歴

リリース	変更内容
5.1(3)N1(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

（注） Cisco NX-OS Release 5.1(3)N1(1) 以降、ARP アクセス リストは、Control Plane Policing（CoPP）に対してだけサポートされます。**permit** コマンドは CoPP ARP ACL では無視されます。

新しく作成した ARP ACL には、ルールは含まれていません。

シーケンス番号を指定しないと、デバイスは ACL の最後のルールのシーケンス番号に 10 を加算したシーケンス番号を割り当てます。

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

例

次に、copp-arp-acl という名前の ARP ACL の ARP アクセス リスト コンフィギュレーション モードを開始し、192.0.32.14/24 サブネット内にある送信者の IP アドレスを含み、それを copp-arp-acl クラスに関連づける 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# configure terminal
switch(config)# arp access-list copp-arp-acl
switch(config-arp-acl)# permit ip 192.0.32.14 255.255.255.0 mac any
switch(config-arp-acl)#
```

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。
remark	ACL に備考を設定します。
show arp access-lists	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 アクセス コントロール リスト（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*] | [**precedence** *precedence*]} [**fragments**] [**time-range** *time-range-name*]

no permit *protocol source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**time-range** *time-range-name*]

no *sequence-number*

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

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

インターネット プロトコル v4（IPv4）

[*sequence-number*] **permit ip** *source destination* {[**dscp** *dscp*] | [**precedence** *precedence*]} [**fragments**] [**time-range** *time-range-name*]

伝送制御プロトコル（TCP）

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

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

構文の説明

sequence-number	（任意）**permit** コマンドのシーケンス番号。スイッチによってアクセス 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。 シーケンス番号には、1 ～ 4294967295 の間の整数を指定できます。 デフォルトでは、ACL の最初のルールには、10 のシーケンス番号が与えられます。 シーケンス番号を指定しない場合、スイッチは ACL の最後にルールを追加し、前のルールのシーケンス番号より 10 大きいシーケンス番号を割り当てます。 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。 • **icmp**：ルールを ICMP トラフィックだけに適用するように指定します。このキーワードを使用すると、*protocol* 引数のすべての有効値に使用できるキーワードに加え、*icmp-message* 引数を使用できます。 • **igmp**：ルールを IGMP トラフィックだけに適用するように指定します。このキーワードを使用すると、*protocol* 引数のすべての有効値に使用できるキーワードに加え、*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するように指定します。このキーワードを使用する場合は、すべての 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には次のものがあります。 – **dscp** – **fragments** – **log** – **precedence** – **time-range** • **tcp**：ルールを TCP トラフィックだけに適用するように指定します。このキーワードを使用すると、*protocol* 引数のすべての有効値に使用できるキーワードに加え、*flags* 引数および *operator* 引数、**portgroup** キーワードおよび **established** キーワードを使用できます。 • **udp**：ルールを UDP トラフィックだけに適用するように指定します。このキーワードを使用すると、*protocol* 引数のすべての有効値に使用できるキーワードに加え、*operator* 引数および **portgroup** キーワードを使用できます。
source	ルールで一致させる送信元 IPv4 アドレス。この引数の指定方法の詳細については、「使用上のガイドライン」の「送信元と宛先」の説明を参照してください。
destination	ルールで一致させる宛先 IPv4 アドレス。この引数の指定方法の詳細については、「使用上のガイドライン」の「送信元と宛先」の説明を参照してください。

dscp *dscp*	（任意）IP ヘッダーの DSCP フィールドに特定の 6 ビット diffserv（ディファレンシエーテッド サービス）値が設定されているパケットだけをルールと一致させるように指定します。*dscp* 引数には、次の数値またはキーワードのいずれかを指定します。 • 0 ～ 63：DSCP フィールドの 6 ビットと同等の 10 進数。たとえば 10 を指定した場合、ルールは DSCP フィールドのビットが 001010 であるパケットだけに一致します。 • **af11**：Assured Forwarding（AF）クラス 1、低い廃棄確率（001010） • **af12**：AF クラス 1、中程度の廃棄確率（001100） • **af13**：AF クラス 1、高い廃棄確率（001110） • **af21**：AF クラス 2、低い廃棄確率（010010） • **af22**：AF クラス 2、中程度の廃棄確率（010100） • **af23**：AF クラス 2、高い廃棄確率（010110） • **af31**：AF クラス 3、低い廃棄確率（011010） • **af32**：AF クラス 3、中程度の廃棄確率（011100） • **af33**：AF クラス 3、高い廃棄確率（011110） • **af41**：AF クラス 4、低い廃棄確率（100010） • **af42**：AF クラス 4、中程度の廃棄確率（100100） • **af43**：AF クラス 4、高い廃棄確率（100110） • **cs1**：Class-selector（CS）1、優先順位 1（001000） • **cs2**：CS2、優先順位 2（010000） • **cs3**：CS3、優先順位 3（011000） • **cs4**：CS4、優先順位 4（100000） • **cs5**：CS5、優先順位 5（101000） • **cs6**：CS6、優先順位 6（110000） • **cs7**：CS7、優先順位 7（111000） • **default**：デフォルトの DSCP 値（000000） • **ef**：Expedited Forwarding（EF; 緊急転送）（101110）

precedence *precedence*	（任意）*precedence* 引数で指定された値が IP Precedence フィールドに設定されているパケットだけをルールと一致させるように指定します。*precedence* 引数には、次の数値またはキーワードを指定します。 • 0 ～ 7 : IP Precedence フィールドの 3 ビットと同等の 10 進数。たとえば、3 を指定した場合、DSCP フィールドに次のビットが設定されているパケットだけがルールと一致します : 011 • **critical**：優先順位 5（101） • **flash**：優先順位 3（011） • **flash-override**：優先順位 4（100） • **immediate**：優先順位 2（010） • **internet**：優先順位 6（110） • **network**：優先順位 7（111） • **priority**：優先順位 1（001） • **routine**：優先順位 0（000）
fragments	（任意）非初期フラグメントであるパケットだけをルールと一致させるように指定します。このキーワードは、TCP ポート番号などのレイヤ 4 オプションを指定したルールには指定できません。これらのオプションをスイッチが評価するために必要な情報は、初期フラグメントだけに含まれているからです。
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。
icmp-message	（任意 : IGMP 限定）指定した ICMP メッセージ タイプのパケットだけに対して一致するルールです。この引数には、0 ～ 255 の整数、または「使用上のガイドライン」の「ICMP メッセージ タイプ」にリストされているキーワードの 1 つを指定します。
igmp-message	（任意 : IGMP 限定）指定した IGMP メッセージ タイプのパケットだけに対して一致するルールです。*igmp-message* 引数には、0 ～ 15 の整数である IGMP メッセージ番号を指定します。また、次のいずれかのキーワードを指定できます。 • **dvmrp** : Distance Vector Multicast Routing Protocol（DVMRP; ディスタンス ベクトル マルチキャスト ルーティング プロトコル） • **host-query**：ホスト クエリー • **host-report**：ホスト レポート • **pim**：Protocol Independent Multicast（PIM） • **trace**：マルチキャスト トレース

operator port [*port*]	（任意：TCP および UDP 限定）*operator* 引数および *port* 引数の条件と一致する送信元ポートから送信されたパケット、または一致する宛先ポートに送信されたパケットだけを、ルールと一致させます。これらの引数が送信元ポートまたは宛先ポートのどちらに適用されるかは、*source* 引数または *destination* 引数のどちらの後に指定したかによって異なります。 *port* 引数には、TCP または UDP ポートの名前または番号を指定します。有効な番号は 0 ～ 65535 の整数です。有効なポート名のリストは、「使用上のガイドライン」の「TCP ポート名」および「UDP ポート名」を参照してください。 2 番目の *port* 引数は、*operator* 引数が範囲である場合だけ必要です。 *operator* 引数には、次のいずれかのキーワードを指定する必要があります。 • **eq**：パケットのポートが *port* 引数と同等である場合だけ一致します。 • **gt**：パケットのポートが *port* 引数より大きい場合だけ一致します。 • **lt**：パケットのポートが *port* 引数より小さい場合だけ一致します。 • **neq**：パケットのポートが *port* 引数と同等ではない場合だけ一致します。 • **range**：2 つの *port* 引数が必要です。パケットのポートが最初の *port* 引数以上で、2 番目の *port* 引数以下である場合だけ一致します。
portgroup *portgroup*	（任意：TCP および UDP 限定）*portgroup* 引数で指定された IP ポート グループ オブジェクトのメンバである送信元ポートから送信されたパケット、またはメンバである宛先ポートに送信されたパケットだけを、ルールと一致させるように指定します。ポート グループ オブジェクトが送信元ポートまたは宛先ポートのどちらに適用されるかは、*source* 引数または *destination* 引数のどちらの後に指定したかによって異なります。 IP ポート グループ オブジェクトを作成および変更するには、**object-group ip port** コマンドを使用します。
flags	（任意：TCP 限定）特定の TCP コントロール ビット フラグがオンに設定されたパケットだけを、ルールと一致させます。*flags* 引数の値には、次の 1 つ以上のキーワードを指定する必要があります。 • **ack** • **fin** • **psh** • **rst** • **syn** • **urg**
established	（任意：TCP 限定）確立された TCP 接続に属するパケットだけをルールと一致させるように指定します。スイッチは、ACK または RST ビットが設定されている TCP パケットが、確立された接続に属していると見なします。

コマンド 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、デバイスは ACL の最後のルールのシーケンス番号に 10 を加算したシーケンス番号を割り当てます。

コマンド モード IPv4 ACL コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン スイッチは、パケットに IPv4 ACL を適用すると、ACL 内のすべてのルールに対してパケットを評価します。スイッチで、パケットが条件に一致した最初のルールが施行されます。複数のルールの条件と一致する場合は、スイッチはシーケンス番号が最も低いルールを施行します。

送信元と宛先

source 引数および *destination* 引数は、次のいずれかの方法で指定できます。各ルールでは、これらの引数の 1 つを指定する際に使用した方法が、他の引数の指定方法に影響を与えることはありません。ルールの設定時に使用できる *source* 引数および *destination* 引数の指定方法は、次のとおりです。

- 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

igmp-message 引数には、0 ～ 255 の整数である ICMP メッセージ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。

- **administratively-prohibited**：管理上の禁止
- **alternate-address**：代替アドレス
- **conversion-error**：データグラム変換
- **dod-host-prohibited**：ホスト禁止
- **dod-net-prohibited**：ネット禁止
- **echo**：エコー（ping）
- **echo-reply**：エコー応答
- **general-parameter-problem**：パラメータの問題
- **host-isolated**：ホスト分離
- **host-precedence-unreachable**：優先順位のホスト到達不能
- **host-redirect**：ホスト リダイレクト
- **host-tos-redirect**：ToS ホスト リダイレクト
- **host-tos-unreachable**：ToS ホスト到達不能
- **host-unknown**：ホスト未知
- **host-unreachable**：ホスト到達不能
- **information-reply**：情報応答
- **information-request**：情報要求
- **mask-reply**：マスク応答
- **mask-request**：マスク要求
- **mobile-redirect**：モバイル ホスト リダイレクト
- **net-redirect**：ネットワーク リダイレクト
- **net-tos-redirect**：ToS ネット リダイレクト
- **net-tos-unreachable**：ToS ネット到達不能
- **net-unreachable**：ネット到達不能
- **network-unknown**：ネットワーク未知
- **no-room-for-option**：パラメータが必要だが空きなし
- **option-missing**：パラメータが必要だが存在しない
- **packet-too-big**：フラグメンテーションが必要、DF 設定
- **parameter-problem**：すべてのパラメータの問題
- **port-unreachable**：ポート到達不能
- **precedence-unreachable**：優先順位カットオフ
- **protocol-unreachable**：プロトコル到達不能
- **reassembly-timeout**：再構成タイムアウト
- **redirect**：すべてのリダイレクト
- **router-advertisement**：ルータ ディスカバリ アドバタイズメント
- **router-solicitation**：ルータ ディスカバリ要求
- **source-quench**：送信元抑制
- **source-route-failed**：送信元ルート障害

- **time-exceeded**：すべての時間超過メッセージ
- **timestamp-reply**：タイム スタンプ付きの応答
- **timestamp-request**：タイム スタンプ付きの要求
- **traceroute**：トレースルート
- **ttl-exceeded**：TTL 超過
- **unreachable**：すべての到達不能

TCP ポート名

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

- **bgp**：Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）（179）
- **chargen**：キャラクタ ジェネレータ（19）
- **cmd**：リモート コマンド（rcmd、514）
- **daytime**：デイタイム（13）
- **discard**：廃棄（9）
- **domain**：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**：ブートストラップ プロトコル（BOOTP）サーバ（67）
- **discard**：廃棄（9）
- **dnsix**：DNSIX セキュリティ プロトコル監査（195）
- **domain**：Domain Name Service（DNS; ドメイン ネーム サービス）（53）
- **echo**：エコー（7）
- **isakmp**：Internet Security Association and Key Management Protocol（ISAKMP）（5）
- **mobile-ip**：モバイル IP レジストレーション（434）
- **nameserver**：IEN116 ネーム サービス（旧式、42）
- **netbios-dgm**：NetBIOS データグラム サービス（138）
- **netbios-ns**：NetBIOS ネーム サービス（137）
- **netbios-ss**：NetBIOS セッション サービス（139）
- **non500-isakmp**：Internet Security Association and Key Management Protocol（ISAKMP）（45）
- **ntp**：Network Time Protocol（NTP; ネットワーク タイム プロトコル）（123）
- **pim-auto-rp**：PIM Auto-RP（496）
- **rip**：Routing Information Protocol（RIP）（ルータ、in.routed、52）
- **snmp**：Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）（161）
- **snmptrap**：SNMP トラップ（162）
- **sunrpc**：Sun Remote Procedure Call（RPC; リモート プロシージャ コール）（111）
- **syslog**：システム ロギング（514）
- **tacacs**：TAC Access Control System（49）
- **talk**：Talk（517）
- **tftp**：Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）（69）
- **time**：Time（37）
- **who**：Who サービス（rwho、513）
- **xdmcp**：X Display Manager Control Protocol（XDMCP）（177）

例

次に、acl-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)# 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
```

関連コマンド

コマンド	説明
deny（IPv4）	IPv4 ACL に拒否（deny）ルールを設定します。
ip access-list	IPv4 ACL を設定します。
remark	ACL に備考を設定します。
show ip access-lists	すべての IPv4 ACL または 1 つの IPv4 ACL を表示します。

permit（IPv6）

条件と一致するトラフィックを許可する IPv6 アクセス コントロール リスト（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**] [**time-range** *time-range-name*]

no permit *protocol source destination* [**dscp** *dscp*] [**flow-label** *flow-label-value*]
[**fragments**] [**time-range** *time-range-name*]

no *sequence-number*

インターネット制御メッセージ プロトコル

[*sequence-number* | **no**] **permit icmp** *source destination* [*icmp-message*] [**dscp** *dscp*]
[**flow-label** *flow-label-value*] [**fragments**] [**time-range** *time-range-name*]

インターネット プロトコル v6（IPv6）

[*sequence-number*] **permit ipv6** *source destination* [**dscp** *dscp*]
[**flow-label** *flow-label-value*] [**fragments**] [**time-range** *time-range-name*]

Stream Control Transmission Protocol

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

伝送制御プロトコル（TCP）

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

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

構文の説明

sequence-number	（任意）**permit** コマンドのシーケンス番号。デバイスによってアクセス 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。 シーケンス番号には、1 ～ 4294967295 の間の整数を指定できます。 デフォルトでは、ACL の最初のルールには、10 のシーケンス番号が与えられます。 シーケンス番号を指定しないと、デバイスによって、ACL の最後にルールが追加され、1 つ前のルールのシーケンス番号に 10 を加算した値が、シーケンス番号として割り当てられます。 ルールのシーケンス番号を再割り当てするには、**resequence** コマンドを使用します。
protocol	ルールで一致させるパケットのプロトコルの名前または番号。有効な番号は、0 ～ 255 です。有効なプロトコル名は、次のキーワードです。 • **ahp**：ルールを Authentication Header Protocol（AHP; 認証ヘッダー プロトコル）トラフィックだけに適用するように指定します。このキーワードを使用する場合は、すべての IPv6 プロトコルに適用される他のキーワードおよび引数だけを使用できます。 • **esp**：ルールを Encapsulating Security Payload（ESP）トラフィックだけに適用するように指定します。このキーワードを使用する場合は、すべての IPv6 プロトコルに適用される他のキーワードおよび引数だけを使用できます。 • **icmp**：ルールを ICMP トラフィックだけに適用するように指定します。このキーワードを使用すると、*protocol* 引数のすべての有効値に使用できるキーワードに加え、*icmp-message* 引数を使用できます。 • **ipv6**：ルールをすべての IPv6 トラフィックに適用するように指定します。このキーワードを使用する場合は、すべての IPv6 プロトコルに適用される他のキーワードおよび引数だけを使用できます。 • **pcp**：ルールを Payload Compression Protocol（PCP; ペイロード圧縮プロトコル）トラフィックだけに適用するように指定します。このキーワードを使用する場合は、すべての IPv6 プロトコルに適用される他のキーワードおよび引数だけを使用できます。 • **sctp**：ルールを Stream Control Transmission Protocol（SCTP）トラフィックだけに適用するように指定します。このキーワードを使用すると、*protocol* 引数のすべての有効値に使用できるキーワードに加え、*operator* 引数および **portgroup** キーワードを使用できます。 • **tcp**：ルールを TCP トラフィックだけに適用するように指定します。このキーワードを使用すると、*protocol* 引数のすべての有効値に使用できるキーワードに加え、*flags* 引数および *operator* 引数、**portgroup** キーワードおよび **established** キーワードを使用できます。 • **udp**：ルールを UDP トラフィックだけに適用するように指定します。このキーワードを使用すると、*protocol* 引数のすべての有効値に使用できるキーワードに加え、*operator* 引数および **portgroup** キーワードを使用できます。
source	ルールで一致させる送信元 IPv6 アドレス。この引数の指定方法の詳細については、「使用上のガイドライン」の「送信元と宛先」の説明を参照してください。

destination	ルールで一致させる宛先 IPv6 アドレス。この引数の指定方法の詳細については、「使用上のガイドライン」の「送信元と宛先」の説明を参照してください。
dscp *dscp*	（任意）IPv6 ヘッダーの DSCP フィールドに特定の 6 ビット diffserv（ディファレンシエーテッド サービス）値が設定されているパケットだけをルールと一致させるように指定します。*dscp* 引数には、次の数値またはキーワードのいずれかを指定します。 • 0 ～ 63 : DSCP フィールドの 6 ビットと同等の 10 進数。たとえば、10 を指定した場合、DSCP フィールドに次のビットが設定されているパケットだけがルールと一致します：001010 • **af11**：Assured Forwarding（AF）クラス 1、低い廃棄確率（001010） • **af12**：AF クラス 1、中程度の廃棄確率（001100） • **af13**：AF クラス 1、高い廃棄確率（001110） • **af21**：AF クラス 2、低い廃棄確率（010010） • **af22**：AF クラス 2、中程度の廃棄確率（010100） • **af23**：AF クラス 2、高い廃棄確率（010110） • **af31**：AF クラス 3、低い廃棄確率（011010） • **af32**：AF クラス 3、中程度の廃棄確率（011100） • **af33**：AF クラス 3、高い廃棄確率（011110） • **af41**：AF クラス 4、低い廃棄確率（100010） • **af42**：AF クラス 4、中程度の廃棄確率（100100） • **af43**：AF クラス 4、高い廃棄確率（100110） • **cs1**：Class-selector（CS）1、優先順位 1（001000） • **cs2**：CS2、優先順位 2（010000） • **cs3**：CS3、優先順位 3（011000） • **cs4**：CS4、優先順位 4（100000） • **cs5**：CS5、優先順位 5（101000） • **cs6**：CS6、優先順位 6（110000） • **cs7**：CS7、優先順位 7（111000） • **default**：デフォルトの DSCP 値（000000） • **ef**：Expedited Forwarding（EF; 緊急転送）（101110）
flow-label *flow-label-value*	（任意）*flow-label-value* 引数で指定された値がフロー ラベル ヘッダー フィールドに設定されている IPv6 パケットだけをルールと一致させるように指定します。*flow-label-value* 引数は、0 ～ 1048575 の整数です。
fragments	（任意）非初期フラグメントであるパケットだけをルールと一致させるように指定します。デバイスでは、非初期フラグメントであるパケットが、ゼロと同等ではないフラグメント オフセットが含まれるフラグメント拡張ヘッダーを持つパケットと見なされます。このキーワードは、TCP ポート番号などのレイヤ 4 オプションを指定したルールには指定できません。これらのオプションをデバイスが評価するために必要な情報は、初期フラグメントだけに含まれているためです。
time-range *time-range-name*	（任意）このルールに適用する時間範囲を指定します。**time-range** コマンドを使用して時間範囲を設定できます。

icmp-message	（ICMP 限定：任意）ルールと一致させる ICMPv6 メッセージのタイプ。この引数には、0 ～ 255 の整数、または「使用上のガイドライン」の「ICMPv6 メッセージ タイプ」にリストされているキーワードの 1 つを指定します。
operator port [*port*]	（任意：TCP、UDP および SCTP 限定）*operator* 引数および *port* 引数の条件と一致する送信元ポートから送信されたパケット、または一致する宛先ポートに送信されたパケットだけを、ルールと一致させます。これらの引数が送信元ポートまたは宛先ポートのどちらに適用されるかは、*source* 引数または *destination* 引数のどちらの後に指定したかによって異なります。 *port* 引数には、TCP または UDP ポートの名前または番号を指定します。有効な番号は 0 ～ 65535 の整数です。有効なポート名のリストは、「使用上のガイドライン」の「TCP ポート名」および「UDP ポート名」を参照してください。 2 番目の *port* 引数は、*operator* 引数が範囲である場合だけ必要です。 *operator* 引数には、次のいずれかのキーワードを指定する必要があります。 • **eq**：パケットのポートが *port* 引数と同等である場合だけ一致します。 • **gt**：パケットのポートが *port* 引数より大きい場合だけ一致します。 • **lt**：パケットのポートが *port* 引数より小さい場合だけ一致します。 • **neq**：パケットのポートが *port* 引数と同等ではない場合だけ一致します。 • **range**：2 つの *port* 引数が必要です。パケットのポートが最初の *port* 引数以上で、2 番目の *port* 引数以下である場合だけ一致します。
portgroup *portgroup*	（任意：TCP、UDP、および SCTP 限定）*portgroup* 引数で指定された IP ポート グループ オブジェクトのメンバである送信元ポートから送信されたパケット、またはメンバである宛先ポートに送信されたパケットだけを、ルールと一致させるように指定します。ポート グループ オブジェクトが送信元ポートまたは宛先ポートのどちらに適用されるかは、*source* 引数または *destination* 引数のどちらの後に指定したかによって異なります。 IP ポート グループ オブジェクトを作成および変更するには、**object-group ip port** コマンドを使用します。
flags	（TCP 限定：任意）特定の TCP コントロール ビット フラグがオンに設定されたパケットだけを、ルールと一致させます。*flags* 引数の値には、次の 1 つ以上のキーワードを指定する必要があります。 • **ack** • **fin** • **psh** • **rst** • **syn** • **urg**
established	（TCP 限定：任意）確立された TCP 接続に属すパケットだけをルールと一致させるように指定します。デバイスは、ACK または RST ビットが設定されている TCP パケットが、確立された接続に属していると見なします。

コマンド 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 モード

コマンド履歴

リリース	変更内容
4.0(1a)N1(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 IPv6 ACL には、ルールは含まれていません。

デバイスは、パケットに IPv6 ACL を適用すると、ACL 内のすべてのルールに対してパケットを評価します。デバイスで、パケットが条件に一致した最初のルールが施行されます。複数のルールの条件と一致する場合は、デバイスはシーケンス番号が最も低いルールを施行します。

送信元と宛先

source 引数および *destination* 引数は、次のいずれかの方法で指定できます。どのルールも、1 つの引数の指定方法によって、他の引数の指定方法が決まることはありません。ルールの設定時に使用できる *source* 引数および *destination* 引数の指定方法は、次のとおりです。

- 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、このセクションの例を参照してください。各例に、**any** キーワードを使用した送信元または宛先の指定方法が示されています。

ICMPv6 メッセージ タイプ

igmp-message 引数には、0 ～ 255 の整数である ICMPv6 メッセージ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。

- **beyond-scope**：範囲外の宛先
- **destination-unreachable**：宛先アドレスに到達不能
- **echo-reply**：エコー応答
- **echo-request**：エコー要求（ping）
- **header**：パラメータ ヘッダーの問題
- **hop-limit**：中継時にホップ制限を超過

- **mld-query**：マルチキャスト リスナー ディスカバリ クエリー
- **mld-reduction**：マルチキャスト リスナー ディスカバリ リダクション
- **mld-reduction**：マルチキャスト リスナー ディスカバリ レポート
- **nd-na**：ネイバー探索のネイバー アドバタイズメント
- **nd-ns**：ネイバー探索のネイバー送信要求
- **next-header**：パラメータの次のヘッダーの問題
- **no-admin**：管理者が宛先を禁止
- **no-route**：宛先へのルートなし
- **packet-too-big**：パケット サイズ超過
- **parameter-option**：パラメータ オプションの問題
- **parameter-problem**：すべてのパラメータの問題
- **port-unreachable**：ポート到達不能
- **reassembly-timeout**：再構成タイムアウト
- **redirect**：ネイバーのリダイレクト
- **renum-command**：ルータの番号付けコマンド
- **renum-result**：ルータの番号付けの結果
- **renum-seq-number**：ルータの番号付けのシーケンス番号リセット
- **router-advertisement**：ネイバー探索のルータ アドバタイズメント
- **router-renumbering**：すべてのルータの再番号付け
- **router-solicitation**：ネイバー探索のルータ送信要求
- **time-exceeded**：すべてのタイム超過メッセージ
- **unreachable**：すべての到達不能

TCP ポート名

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

- **bgp**：Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）（179）
- **chargen**：キャラクタ ジェネレータ（19）
- **cmd**：リモート コマンド（rcmd、514）
- **daytime**：デイタイム（13）
- **discard**：廃棄（9）
- **domain**：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**：ブートストラップ プロトコル（BOOTP）サーバ（67）
- **discard**：廃棄（9）
- **dnsix**：DNSIX セキュリティ プロトコル監査（195）
- **domain**：Domain Name Service（DNS; ドメイン ネーム サービス）（53）
- **echo**：エコー（7）
- **isakmp**：Internet Security Association and Key Management Protocol（ISAKMP）（5）
- **mobile-ip**：モバイル IP レジストレーション（434）
- **nameserver**：IEN116 ネーム サービス（旧式、42）
- **netbios-dgm**：NetBIOS データグラム サービス（138）
- **netbios-ns**：NetBIOS ネーム サービス（137）
- **netbios-ss**：NetBIOS セッション サービス（139）
- **non500-isakmp**：Internet Security Association and Key Management Protocol（ISAKMP）（45）

- **ntp**：Network Time Protocol（NTP; ネットワーク タイム プロトコル）（123）
- **pim-auto-rp**：PIM Auto-RP（496）
- **rip**：Routing Information Protocol（RIP）（ルータ、in.routed、52）
- **snmp**：Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）（161）
- **snmptrap**：SNMP トラップ（162）
- **sunrpc**：Sun Remote Procedure Call（RPC; リモート プロシージャ コール）（111）
- **syslog**：システム ロギング（514）
- **tacacs**：TAC Access Control System（49）
- **talk**：Talk（517）
- **tftp**：Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）（69）
- **time**：Time（37）
- **who**：Who サービス（rwho、513）
- **xdmcp**：X Display Manager Control Protocol（XDMCP）（177）

例

次に、acl-lab13-ipv6 という IPv6 ACL を作成し、2001:0db8:85a3:: ネットワークおよび 2001:0db8:69f2:: ネットワークから 2001:0db8:be03:2112:: ネットワークへのすべての TCP トラフィックおよび UDP トラフィックを許可するルールを設定する例を示します。

```
switch# configure terminal
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# configure terminal
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。
ipv6 access-list	IPv6 ACL を設定します。
remark	ACL に備考を設定します。

permit（MAC）

条件と一致するトラフィックを許可する MAC アクセス コントロール リスト（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*

構文の説明

sequence-number	（任意）**permit** コマンドのシーケンス番号。スイッチによってアクセス 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。 シーケンス番号には、1 ～ 4294967295 の間の整数を指定できます。 デフォルトでは、ACL の最初のルールには、10 のシーケンス番号が与えられます。 シーケンス番号を指定しない場合、スイッチは ACL の最後にルールを追加し、前のルールのシーケンス番号より 10 大きいシーケンス番号を割り当てます。 ルールのシーケンス番号を再割り当てするには、**resequence** コマンドを使用します。
source	ルールで一致させる送信元 MAC アドレス。この引数の指定方法の詳細については、「使用上のガイドライン」の「送信元と宛先」の説明を参照してください。
destination	ルールで一致させる宛先 MAC アドレス。この引数の指定方法の詳細については、「使用上のガイドライン」の「送信元と宛先」の説明を参照してください。
protocol	（任意）ルールで一致させるプロトコルの番号。有効なプロトコル番号は 0x0 ～ 0xffff です。有効なプロトコル名のリストは、「使用上のガイドライン」の「MAC プロトコル」を参照してください。
cos *cos-value*	（任意）IEEE 802.1Q ヘッダーに、*cos-value* 引数で指定したサービス クラス（CoS）値が含まれているパケットだけにルールが一致するように指定します。*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にルールが一致するように指定します。*vlan-id* 引数は、1 ～ 4094 の整数に指定できます。

コマンド デフォルト

新しく作成した MAC ACL には、ルールは含まれていません。

シーケンス番号を指定しないと、スイッチで 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

MAC ACL コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

スイッチは、パケットに MAC ACL を適用すると、ACL 内のすべてのルールに対してパケットを評価します。スイッチで、パケットが条件に一致した最初のルールが施行されます。複数のルールの条件と一致する場合は、スイッチはシーケンス番号が最も低いルールを施行します。

送信元と宛先

source 引数および *destination* 引数は、次のいずれかの方法で指定できます。どのルールも、1 つの引数の指定方法によって、他の引数の指定方法が決まることはありません。ルールの設定時に使用できる *source* 引数および *destination* 引数の指定方法は、次のとおりです。

- アドレスおよびマスク：MAC アドレスの後にマスクを指定して、1 つのアドレスまたはアドレスグループを指定できます。構文は次のとおりです。

  ```
  MAC-address MAC-mask
  ```

  次に、MAC アドレス 00c0.4f03.0a72 を持つ *source* 引数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 進数です。有効なプロトコル番号は 0x0 ～ 0xffff です。有効なキーワードは、次のとおりです。

- **aarp**：Appletalk ARP（0x80f3）
- **appletalk**：Appletalk（0x809b）
- **decnet-iv**：DECnet Phase IV（0x6003）
- **diagnostic**：DEC 診断プロトコル（0x6005）
- **etype-6000**：EtherType 0x6000（0x6000）
- **etype-8042**：EtherType 0x8042（0x8042）
- **ip**：インターネット プロトコル v4（0x0800）
- **lat**：DEC LAT（0x6004）
- **lavc-sca**：DEC LAVC、SCA（0x6007）
- **mop-console**：DEC MOP リモート コンソール（0x6002）
- **mop-dump**：DEC MOP ダンプ（0x6001）
- **vines-echo**：VINES エコー（0x0baf）

例

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

```
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
switch(config-mac-acl)#
```

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。
show mac access-list	すべての MAC ACL または 1 つの MAC ACL を表示します。

permit 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追加するには、**permit interface** コマンドを使用します。インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

permit interface *interface-list*

no permit interface

構文の説明

interface-list	ユーザ ロールがアクセスを許可されているインターフェイスのリストです。

コマンド デフォルト

すべてのインターフェイス

コマンド モード

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

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

permit interface ステートメントを機能させるには、次の例のように、コマンド ルールを設定してインターフェイス アクセスを許可する必要があります。

```
switch(config-role)# rule number permit command configure terminal ; interface *
```

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設定する例を示します。

```
switch(config)# role name MyRole
switch(config-role)# interface policy deny
switch(config-role-interface)# permit interface ethernet 1/2 - 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設定する例を示します。

```
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
```

次に、ユーザ ロール インターフェイス ポリシーからインターフェイスを削除する例を示します。

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

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 を追加するには、**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-list*

no permit vlan

構文の説明

vlan-list	ユーザ ロールがアクセスを許可されている VLAN のリストです。

コマンド デフォルト

すべての VLAN

コマンド モード

VLAN ポリシー コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

permit vlan ステートメントを機能させるには、次の例のように、コマンド **rule** を設定して VLAN アクセスを許可する必要があります。

```
switch(config-role)# rule number permit command configure terminal ; vlan *
```

例

次に、ユーザ ロール VLAN ポリシーで VLAN の範囲を設定する例を示します。

```
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 のリストを設定する例を示します。

```
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)# 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; 仮想ルーティングおよび転送）インスタンスを追加するには、**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-list*

no permit vrf

構文の説明

vrf-list	ユーザ ロールがアクセスを許可されている VRF のリストです。

コマンド デフォルト

すべての VRF

コマンド モード

VRF ポリシー コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

例

次に、ユーザ ロール VRF ポリシーで VRF の範囲を設定する例を示します。

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

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。

permit vsan

ユーザ ロールに VSAN ポリシーへのアクセスを許可するには、**permit vsan** コマンドを使用します。ユーザ ロールのデフォルトの VSAN ポリシー設定に戻すには、このコマンドの **no** 形式を使用します。

permit vsan *vsan-list*

no permit vsan *vsan-list*

構文の説明

vsan-list	ユーザ ロールがアクセスできる VSAN の範囲です。有効な範囲は 1 ～ 4093 です。 次の区切り記号を使用して範囲を区切ることができます。 • **,** は、1-5, 10, 12, 100-201 のように複数の範囲を区切る記号です。 • **-** は、101-201 のように範囲を区切る記号です。

コマンド デフォルト

なし

コマンド モード

ユーザ ロール コンフィギュレーション モード

コマンド履歴

リリース	変更内容
4.0(0)N1(1a)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、**vsan policy deny** コマンドを使用して VSAN ポリシーを拒否した後にのみイネーブルになります。

例

次に、ユーザ ロールに VSAN ポリシーへのアクセスを許可する例を示します。

```
switch(config)# role name MyRole
switch(config-role)# vsan policy deny
switch(config-role-vsan)# permit vsan 10, 12, 100-104
switch(config-role-vsan)#
```

関連コマンド

コマンド	説明
vsan policy deny	ユーザの VSAN ポリシーへのアクセスを拒否します。
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。