# IPv6 ACL



## 機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、https://cfnng.cisco.com/に進みます。Cisco.com のアカウントは必要ありません。

## IPv6 ACL の概要

IP Version 6（IPv6）アクセス コントロール リスト（ACL）を作成し、それをインターフェイスに適用することによって、IPv6 トラフィックをフィルタリングできます。これは、IP Version 4（IPv4）の名前付き ACL を作成し、適用する方法と同じです。また、スイッチで IP ベースおよび LAN ベース フィーチャ セットが稼働している場合、入力ルータ ACL を作成し、それを適用してレイヤ 3 管理トラフィックをフィルタリングすることもできます。

スイッチは、次の 3 種類の IPv6 ACL をサポートします。

- IPv6 ルータ ACL は、ルーテッド ポート、スイッチ仮想インターフェイス（SVI）、またはレイヤ 3 EtherChannel に設定できるレイヤ 3 インターフェイスのアウトバウンド トラ

フィックまたはインバウンド トラフィックでサポートされます。IPv6 ルータ ACL は、ルーティングされる IPv6 パケットに対してだけ適用されます。

- IPv6 ポート ACL は、アウトバウンドおよびインバウンドのレイヤ 2 インターフェイスでサポートされます。IPv6 ポート ACL は、インターフェイスに着信するすべての IPv6 パケットに対して適用されます。
- VLAN ACL または VLAN マップは、VLAN 内のすべてのパケットのアクセスを制御します。VLAN マップを使用すると、同じ VLAN 内のデバイス間で転送されるトラフィックをフィルタリングできます。ACL VLANマップは、L2 VLANに適用されます。VLANマップは、IPv6 のレイヤ 3 アドレスに基づいてアクセス コントロールするように設定されています。イーサネットACEを使用するとMACアドレスにより、サポートされていないプロトコルがアクセスコントロールされます。VLANマップをVLANに適用すると、VLANに入るすべてのパケットが VLAN マップと照合されます。

スイッチは、IPv6 トラフィックの VLAN ACL（VLAN マップ）をサポートします。

1 つのインターフェイスに、IPv4 ACL および IPv6 ACL の両方を適用できます。IPv4 ACL の場合と同様に、IPv6 ポート ACL はルータ ACL よりも優先されます。

# 他の機能およびスイッチとの相互作用

- IPv6 ルータ ACL がパケットを拒否するよう設定されている場合、パケットはルーティングされません。パケットのコピーがインターネット制御メッセージ プロトコル（ICMP）キューに送信され、フレームに ICMP 到達不能メッセージが生成されます。
- ブリッジド フレームがポート ACL によってドロップされる場合、このフレームはブリッジングされません。
- IPv4 ACL および IPv6 ACL の両方を 1 つのスイッチまたはスイッチスタックに作成したり、同一インターフェイスに適用できます。各 ACL には一意の名前が必要です。設定済みの名前を使用しようとすると、エラー メッセージが表示されます。

  IPv4 ACL と IPv6 ACL の作成、および同一のレイヤ 2 インターフェイスまたはレイヤ 3 インターフェイスへの IPv4 ACL または IPv6 ACL の適用には、異なるコマンドを使用します。ACL を付加するのに誤ったコマンドを使用すると（例えば、IPv6 ACL の付加に IPv4 コマンドを使用するなど）、エラー メッセージが表示されます。
- MAC ACL を使用して、IPv6 フレームをフィルタリングできません。MAC ACL は非 IP フレームだけをフィルタリングできます。
- ハードウェア メモリに空きがない場合、パケットはインターフェイスでドロップされ、アンロードのエラー メッセージが記録されます。

# IPv6 ACL の制限

IPv4 では、番号制の標準 IP ACL および拡張 IP ACL、名前付き IP ACL、および MAC ACL を設定できます。IPv6 がサポートするのは名前付き ACL だけです。

スイッチは Cisco IOS がサポートする IPv6 ACL の大部分をサポートしますが、一部例外もあります。

- スイッチは、**routing header**、および **undetermined-transport** というキーワードの照合をサポートしません。
- スイッチは、再帰 ACL（**reflect** キーワード）をサポートしません。
- 
- 
- このリリースは、IPv6 のポート ACL、ルータ ACL および VLAN ACL（VLAN マップ）をサポートしています。
- 
- IPv6 の出力ルータ ACL および入力ポート ACL は、スイッチ スタックでだけサポートされています。スイッチは、コントロール プレーン（着信）IPv6 ACL だけをサポートします。
- スイッチは、IPv6 フレームに MAC ベース ACL を適用しません。
- ACL を設定する場合、ACL に入力されるキーワードには、それがプラットフォームでサポートされるかどうかにかかわらず、制限事項はありません。ハードウェア転送が必要なインターフェイス（物理ポートまたは SVI）に ACL を適用する場合、スイッチはインターフェイスで ACL がサポートされるかどうか判別します。サポートされない場合、ACL の付加は拒否されます。
- インターフェイスに適用される ACL に、サポートされないキーワードを持つアクセス コントロールエントリ（ACE）を追加しようとする場合、スイッチは現在インターフェイスに適用されている ACL に ACE が追加されるのを許可しません。

スイッチの IPv6 ACL には、次の特性があります。

- 分割フレーム（IPv4 では **fragments** キーワード）がサポートされます。
- IPv6 ACL では、IPv4 と同じ統計情報がサポートされます。
- スイッチのハードウェア スペースがなくなった場合、ACL に関連付けられたパケットはインターフェイスでドロップされます。
- ホップバイホップ オプションがあるルーテッドパケットまたはブリッジドパケットには、ソフトウェアで適用される IPv6 ACL が設定されます。
- ロギングは、ルータ ACL ではサポートされますが、ポート ACL ではサポートされません。

- スイッチは、プレフィックス長の最大範囲の IPv6 アドレス一致をサポートしません。

# IPv6 ACL のデフォルト設定

デフォルトの IPv6 ACL 設定は次のとおりです。

```
Switch# show access-lists preauth_ipv6_acl
IPv6 access list preauth_ipv6_acl (per-user)
permit udp any any eq domain sequence 10
permit tcp any any eq domain sequence 20
permit icmp any any nd-ns sequence 30
permit icmp any any nd-na sequence 40
permit icmp any any router-solicitation sequence 50
permit icmp any any router-advertisement sequence 60
permit icmp any any redirect sequence 70
permit udp any eq 547 any eq 546 sequence 80
permit udp any eq 546 any eq 547 sequence 90
deny ipv6 any any sequence 100
```

# IPv6 ACL の設定

IPv6 トラフィックをフィルタリングするには、次の手順を実行します。

### 手順の概要

1. **enable**
2. **configure terminal**
3. {**ipv6 access-list** *list-name*
4. {**deny** | **permit**} protocol {*source-ipv6-prefix/ |prefix-length* |**any**| **host** *source-ipv6-address*} [ operator [ *port-number* ]] { *destination-ipv6-prefix/ prefix-length* | **any** | **host** *destination-ipv6-address*} [operator [*port-number*]][ **dscp** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [ **sequence** *value*] [ **time-range** *name*]
5. {**deny** | **permit**} **tcp** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [**operator** [**port-number**]] {*destination-ipv6- prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [operator [*port-number*]] [**ack**] [ **dscp** *value*] [**established**] [**fin**] [**log**] [**log-input**] [**neq** {**port** | protocol}] [**psh**] [**range** {**port** | protocol}] [**rst**] [**routing**] [ **sequence** *value*] [**syn**] [ **time-range** *name*] [**urg**]
6. {**deny** | **permit**} **udp** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [operator [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [operator [*port-number*]] [ **dscp** *value*] [**log**] [**log-input**] [**neq** {*port* | *protocol*}] [**range** {*port* | *protocol*}] [**routing**] [ **sequence** *value*] [ **time-range** *name*]]
7. {**deny** | **permit**} **icmp** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [operator [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address*} [operator [*port-number*]] [*icmp-type* [*icmp-code*] | icmp-message] [ **dscp** *value*] [**log**] [**log-input**] [**routing**] [ **sequence** *value*] [ **time-range** *name*]
8. **end**
9. **show ipv6 access-list**
10. **show running-config**

11. **copy running-config startup-config**

手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>スイッチ> **enable** | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>スイッチ# **configure terminal** | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | {**ipv6 access-list** *list-name*<br>例：<br>スイッチ(config)# **ipv6 access-list example_acl_list** | IPv6 ACL 名を定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。 |
| ステップ 4 | {**deny** \| **permit**} protocol {*source-ipv6-prefix/ \|prefix-length* \|**any**\| **host** *source-ipv6-address*} [ operator [ *port-number* ]] { *destination-ipv6-prefix/ prefix-length* \| **any** \| **host** *destination-ipv6-address*} [operator [*port-number*]][ **dscp** *value*] [**fragments**] [**log**] [**log-input**] [**routing**] [ **sequence** *value*] [ **time-range** *name*] | 条件が一致した場合にパケットを拒否する場合は deny、許可する場合は permit を指定します。次に、条件について説明します。<br>• protocol には、IP の名前または番号を入力します。 **ahp**、**esp**、**icmp**、**ipv6**、**pcp**、**stcp**、**tcp**、**udp** または IPv6 プロトコル番号を表す 0 ～ 255 の整数を使用できます。<br>• *source-ipv6-prefix/prefix-length* または *destination-ipv6-prefix/ prefix-length* は、拒否条件または許可条件を設定する送信元または宛先 IPv6 ネットワークあるいはネットワーク クラスで、コロン区切りの 16 ビット値を使用した 16 進形式で指定します（RFC 2373 を参照）。<br>• IPv6 プレフィックス ::/0 の短縮形として、**any** を入力します。<br>• **host** *source-ipv6-address* または *destination-ipv6-address* には、拒否条件または許可条件を設定する送信元または宛先 IPv6 ホストアドレスを入力します。アドレスはコロン区切りの 16 ビット値を使用した 16 進形式で指定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | • （任意）operator には、指定のプロトコルの送信元ポートまたは宛先ポートを比較するオペランドを指定します。オペランドには、**lt**（より小さい）、**gt**（より大きい）、**eq**（等しい）、**neq**（等しくない）、および**range**（包含範囲）があります。<br><br>*source-ipv6-prefix/prefix-length* 引数のあとの operator は、送信元ポートに一致する必要があります。*destination-ipv6- prefix/prefix-length* 引数のあとの operator は、宛先ポートに一致する必要があります。<br><br>• （任意）**port-number** は、0 ～ 65535 の 10 進数または TCP あるいは UDP ポートの名前です。TCP ポート名を使用できるのは、TCP のフィルタリング時だけです。UDP ポート名を使用できるのは、UDP のフィルタリング時だけです。<br><br>• （任意）**dscp** value を入力して、各 IPv6 パケットヘッダーの Traffic Class フィールド内のトラフィッククラス値と DiffServ コードポイント値を照合します。指定できる範囲は 0 ～ 63 です。<br><br>• （任意）**fragments** を入力して、先頭ではないフラグメントを確認します。このキーワードが表示されるのは、プロトコルが ipv6 の場合だけです。<br><br>• （任意）**log** を指定すると、エントリと一致するパケットに関するログメッセージがコンソールに送信されます。**log-input** を指定すると、ログエントリに入力インターフェイスが追加されます。ロギングはルータ ACL でだけサポートされます。<br><br>• （任意）**routing** を入力して、IPv6 パケットのルーティングを指定します。<br><br>• （任意）**sequence** *value* を入力して、アクセスリスト ステートメントのシーケンス番号を指定します。指定できる範囲は 1 ～ 4,294,967,295 です。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | | • （任意）**time-range** name を入力して、拒否または許可ステートメントに適用される時間の範囲を指定します。 |
| ステップ 5 | {**deny** \| **permit**} **tcp** {*source-ipv6-prefix/prefix-length* \| **any** \| **host** *source-ipv6-address*} [**operator** [**port-number**]] {*destination-ipv6- prefix/prefix-length* \| **any** \| **host** *destination-ipv6-address*} [operator [*port-number*]] [**ack**] [ **dscp** *value*] [**established**] [**fin**] [**log**] [**log-input**] [**neq** {**port** \| protocol}] [**psh**] [**range** {**port** \| protocol}] [**rst**] [**routing**] [ **sequence** *value*] [**syn**] [ **time-range** *name*] [**urg**] | （任意）TCP アクセス リストおよびアクセス条件を定義します。<br>TCP の場合は **tcp** を入力します。パラメータはステップ 3a で説明されているパラメータと同じですが、次に示すオプションのパラメータが追加されています。<br>• **ack**：確認応答（ACK）ビットセット。<br>• **established**：確立された接続。TCP データグラムに ACK または RST ビットが設定されている場合、照合が行われます。<br>• **fin**：終了ビットセット。送信者からのデータはそれ以上ありません。<br>• **neq** {*port*\|**protocol**}：所定のポート番号上にないパケットだけを照合します。<br>• **psh**：プッシュ機能ビットセット<br>• **range** {*port*\|**protocol**}：ポート番号の範囲内のパケットだけを照合します。<br>• **rst**：リセットビットセット<br>• **syn**：同期ビットセット<br>• **urg**：緊急ポインタビットセット |
| ステップ 6 | {**deny** \| **permit**} **udp** {*source-ipv6-prefix/prefix-length* \| **any** \| **host** *source-ipv6-address*} [operator [*port-number*]] {*destination-ipv6-prefix/prefix-length* \| **any** \| **host** *destination-ipv6-address*} [operator [*port-number*]] [ **dscp** *value*] [**log**] [**log-input**] [**neq** {*port* \| *protocol*}] [**range** {*port* \| *protocol*}] [**routing**] [ **sequence** *value*] [ **time-range** *name*]] | （任意）UDP アクセス リストおよびアクセス条件を定義します。<br>ユーザ データグラム プロトコルの場合は、**udp** を入力します。UDP パラメータは TCP に関して説明されているパラメータと同じです。ただし、[operator [*port*]] のポート番号またはポート名は、UDP ポートの番号または名前でなければなりません。UDP の場合、established パラメータは無効です。 |
| ステップ 7 | {**deny** \| **permit**} **icmp** {*source-ipv6-prefix/prefix-length* \| **any** \| **host** *source-ipv6-address*} [operator [*port-number*]] {*destination-ipv6-prefix/prefix-length* \| **any** \| **host** | （任意）ICMP アクセス リストおよびアクセス条件を定義します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| | *destination-ipv6-address*} [operator [*port-number*]] [*icmp-type* [*icmp-code*] \| icmp-message] [ **dscp** *value*] [**log**] [**log-input**] [**routing**] [ **sequence** *value*] [ **time-range** *name*] | インターネット制御メッセージプロトコルの場合は、**icmp** を入力します。ICMP パラメータはステップ 1 の IP プロトコルの説明にあるパラメータとほとんど同じですが、ICMP メッセージ タイプおよびコード パラメータが追加されています。オプションのキーワードの意味は次のとおりです。<br>• *icmp-type*：ICMP メッセージタイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。<br>• *icmp-code*：ICMP パケットを ICMP メッセージコードタイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。<br>• *icmp-message*：ICMP パケットを ICMP メッセージタイプ名または ICMP メッセージタイプとコード名でフィルタリングする場合に入力します。ICMP メッセージのタイプ名およびコード名のリストについては、?キーを使用するか、またはこのリリースのコマンド リファレンスを参照してください。 |
| ステップ 8 | **end** | 特権 EXEC モードに戻ります。 |
| ステップ 9 | **show ipv6 access-list** | アクセス リストの設定を確認します。 |
| ステップ 10 | **show running-config**<br>例：<br>`スイッチ# show running-config` | 入力を確認します。 |
| ステップ 11 | **copy running-config startup-config**<br>例：<br>`スイッチ# copy running-config startup-config` | （任意）コンフィギュレーション ファイルに設定を保存します。 |

# インターフェイスへの IPv6 ACL の付加

レイヤ 3 インターフェイスで発信または着信トラフィックに ACL を、あるいはレイヤ 2 インターフェイスで着信トラフィックに を適用できます。レイヤ 3 インターフェイスで着信トラフィックにだけ ACL を適用できます。

インターフェイスへのアクセスを制御するには、次の手順を実行します。

## 手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface-id*
4. **no switchport**
5. **ipv6 address** *ipv6-address*
6. **ipv6 traffic-filter** *access-list-name* {**in** | **out**}
7. **end**
8. **show running-config**
9. **copy running-config startup-config**

## 手順の詳細

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 1 | **enable**<br>例：<br>`スイッチ> enable` | 特権 EXEC モードを有効にします。<br>• パスワードを入力します（要求された場合）。 |
| ステップ 2 | **configure terminal**<br>例：<br>`スイッチ# configure terminal` | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | **interface** *interface-id* | アクセスリストを適用するレイヤ 2 インターフェイス（ポート ACL 用）またはレイヤ 3 インターフェイス（ルータ ACL 用）を特定して、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | **no switchport** | ルータ ACL を適用する場合は、これによってインターフェイスがレイヤ 2 モード（デフォルト）からレイヤ 3 モードに変化します。 |
| ステップ 5 | **ipv6 address** *ipv6-address* | レイヤ 3 インターフェイス（ルータ ACL 用）で IPv6 アドレスを設定します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 6 | **ipv6 traffic-filter** *access-list-name* {**in** \| **out**} | インターフェイスの着信トラフィックまたは発信トラフィックにアクセスリストを適用します。<br>（注） out キーワードはレイヤ 2 インターフェイス（ポート ACL）ではサポートされません。 |
| ステップ 7 | **end**<br>例：<br>`スイッチ(config)# end` | 特権 EXEC モードに戻ります。 |
| ステップ 8 | **show running-config**<br>例：<br>`スイッチ# show running-config` | 入力を確認します。 |
| ステップ 9 | **copy running-config startup-config**<br>例：<br>`スイッチ# copy running-config startup-config` | （任意）コンフィギュレーションファイルに設定を保存します。 |

# IPv6 ACL のモニタリング

次の表に示された 1 つまたは複数の特権 EXEC コマンドを使用して、設定済みのすべてのアクセス リスト、すべての IPv6 アクセス リスト、または特定のアクセス リストに関する情報を表示できます。

**表 *1 : show ACL* コマンド**

| コマンド | 目的 |
|---|---|
| **show access-lists** | スイッチに設定されたすべてのアクセス リストを表示します。 |
| **show ipv6 access-list** [*access-list-name*] | 設定済みのすべての IPv6 アクセス リストまたは名前で指定されたアクセス リストを表示します。 |
| **show vlan access-map** [*map-name*] | VLAN アクセス マップ設定を表示します。 |
| **show vlan filter** [**access-map** *access-map* \| **vlan** *vlan-id*] | VACL と VLAN 間のマッピングを表示します。 |

次に、show access-lists 特権 EXEC コマンドの出力例を示します。出力には、スイッチまたはスイッチ スタックに設定済みのすべてのアクセス リストが表示されます。

```
Switch # show access-lists
Extended IP access list hello
    10 permit ip any any
IPv6 access list ipv6
    permit ipv6 any any sequence 10
```

次に、**show ipv6 access-lists** 特権 EXEC コマンドの出力例を示します。出力には、スイッチまたはスイッチ スタックに設定済みの IPv6 アクセス リストだけが表示されます。

```
Switch# show ipv6 access-list
IPv6 access list inbound
    permit tcp any any eq bgp (8 matches) sequence 10
    permit tcp any any eq telnet (15 matches) sequence 20
    permit udp any any sequence 30
IPv6 access list outbound
    deny udp any any sequence 10
    deny tcp any any eq telnet sequence 20
```

次に、show vlan access-map 特権 EXEC コマンドの出力例を示します。出力には、VLAN アクセス マップ情報が表示されます。

```
Switch# show vlan access-map
Vlan access-map "m1"  10
  Match clauses:
    ipv6 address: ip2
  Action: drop
```

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。