



## IPv6 ACL の設定

- [機能情報の確認 \(1 ページ\)](#)
- [IPv6 ACL の設定に関する情報 \(1 ページ\)](#)
- [IPv6 ACL の設定 \(3 ページ\)](#)
- [IPv6 ACL の設定例 \(10 ページ\)](#)

### 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](#) には、<http://www.cisco.com/go/cfn> からアクセスします。[Cisco.com](#) のアカウントは必要ありません。

### IPv6 ACL の設定に関する情報

IPバージョン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バージョン4 (IPv4) の名前付き ACL を作成し、適用する方法と同じです。

### IPv6 ACL の概要

スイッチ イメージは、次の2種類の IPv6 ACL をサポートします。

- **IPv6 ルータ ACL** : 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送信トラフィックまたは着信トラフィックでサポートされます。経路選択済みのIPv6パケットだけに適用されます。

- IPv6 ポート ACL : レイヤ 2 インターフェイスの着信トラフィックでだけサポートされます。インターフェイスに届くすべての IPv6 パケットに適用されます。



(注) サポートされない IPv6 ACL を設定した場合、エラーメッセージが表示され、その設定は有効になりません。

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

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。

- SVI に入力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートに着信したパケットはポート ACL によってフィルタリングされます。その他のポートに着信したルーテッド IP パケットは、ルータ ACL によってフィルタリングされます。他のパケットはフィルタリングされません。
- SVI に出力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートに着信したパケットはポート ACL によってフィルタリングされます。発信ルーテッド IPv6 パケットは、ルータ ACL によってフィルタリングされます。他のパケットはフィルタリングされません。



(注) いずれかのポート ACL (IPv4、IPv6、または MAC) がインターフェイスに適用された場合、そのポート ACL を使用してパケットをフィルタリングし、ポート VLAN の SVI に適用されたルータ ACL は無視されます。

## サポートされる ACL 機能

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witchの Ternary CAM (TCAM) スペースが不足している場合、ACL ラベルに対応付けられたパケットは CPU に転送され、ACL はソフトウェアで適用されます。
- 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。

## IPv6 ACL の制限事項

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。

- IPv6 送信元および宛先アドレス：ACL 照合は、Extended Universal Identifier (EUI) -64 形式の /0 ~ /64 のプレフィックスおよびホスト アドレス (/128) だけでサポートされます。スイッチは、情報損失のない次のホスト アドレスだけをサポートします。

集約グローバルユニキャスト アドレス

リンク ローカルアドレス

- スイッチは、**flowlabel**、**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。
- スイッチは再起 ACL (**reflect** キーワード) をサポートしません。
- このリリースが IPv6 用にサポートしているのは、ポート ACL およびルータ ACL だけです。VLAN ACL (VLAN マップ) はサポートしていません。
- スイッチは IPv6 フレームに MAC ベース ACL を適用しません。
- レイヤ 2 EtherChannel に IPv6 ポート ACL を適用できません。
- スイッチは出力ポート ACL をサポートしません。
- IPv6 の出力ルータ ACL および入力ポート ACL は、だけでサポートされます。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。
- 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。

## IPv6 ACL の設定

IPv6 トラフィックをフィルタリングする場合は、次の手順を実行します。

### 手順の概要

1. IPv6 ACL を作成し、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。
2. IPv6 ACL が、トラフィックをブロックする (拒否) または通過させる (許可) よう設定します。
3. インターフェイスに IPv6 ACL を適用します。ルータ ACL では、ACL が適用されるレイヤ 3 インターフェイスにも IPv6 アドレスを設定する必要があります。

## 手順の詳細

	コマンドまたはアクション	目的
ステップ 1	IPv6 ACL を作成し、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 2	IPv6 ACL が、トラフィックをブロックする（拒否）または通過させる（許可）よう設定します。	
ステップ 3	インターフェイスに IPv6 ACL を適用します。ルータ ACL では、ACL が適用されるレイヤ 3 インターフェイスにも IPv6 アドレスを設定する必要があります。	

## IPv6 ACL のデフォルト設定

デフォルトでは、IPv6 ACL は設定または適用されていません。

## 他の機能およびスイッチとの相互作用

- 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が満杯の場合、設定済みの ACL を追加すると、パケットは CPU に転送され、ACL はソフトウェアで適用されます。ハードウェアが一杯になると、ACL がアンロードされたことを示すメッセージがコンソールに出力され、パケットはインターフェイスでドロップされます。



(注) 追加できなかった ACL と同じタイプのパケットのみ (ipv4、ipv6、MAC) がインターフェイスでドロップされます。

- TCAM が満杯の場合、設定済みの ACL を追加すると、パケットは CPU に転送され、ACL はソフトウェアで適用されます。

## IPv6 ACL の作成

IPv6 ACL を作成するには、次の手順に従ってください。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Switch> <b>enable</b>	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"> <li>パスワードを入力します（要求された場合）。</li> </ul>
ステップ 2	<b>configureterminal</b> 例： Switch# <b>configure terminal</b>	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	<b>ipv6access-listaccess-list-name</b> 例： ipv6 access-list access-list-name	IPv6 アクセス リスト名を定義し、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	<b>{deny permit} protocol</b> 例： <pre>{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]</pre>	条件が一致した場合にパケットを拒否する場合は <b>deny</b> 、許可する場合は <b>permit</b> を指定します。次に、条件について説明します。 <ul style="list-style-type: none"> <li><b>protocol</b> には、インターネットプロトコルの名前または番号を入力します。 <b>ahp</b>、 <b>esp</b>、 <b>icmp</b>、 <b>ipv6</b>、 <b>pcp</b>、 <b>step</b>、 <b>tcp</b>、 <b>udp</b>、 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。</li> <li><b>source-ipv6-prefix/prefix-length</b> または <b>destination-ipv6-prefix/ prefix-length</b> 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）。</li> <li>IPv6 プレフィックス <b>::/0</b> の短縮形として、 <b>any</b> を入力します。</li> <li><b>host source-ipv6-address</b> または <b>destination-ipv6-address</b> 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</li> </ul>

	コマンドまたはアクション	目的
		<p>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。</p> <ul style="list-style-type: none"> <li>• (任意) <b>operator</b> 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、<b>lt</b> (より小さい)、<b>gt</b> (より大きい)、<b>eq</b> (等しい)、<b>neq</b> (等しくない)、<b>range</b> (包含範囲) があります。</li> </ul> <p><b>source-ipv6-prefix/prefix-length</b> 引数のあとの <b>operator</b> は、送信元ポートに一致する必要があります。  <b>destination-ipv6- prefix/prefix-length</b> 引数のあとの <b>operator</b> は、宛先ポートに一致する必要があります。</p> <ul style="list-style-type: none"> <li>• (任意) <b>port-number</b> 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。</li> <li>• (任意) <b>dscp value</b> 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。</li> <li>• (任意) <b>fragments</b> 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 <b>ipv6</b> の場合だけです。</li> <li>• (任意) <b>log</b> 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。<b>log-input</b> 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。</li> <li>• (任意) <b>routing</b> を入力して、IPv6 パケットのルーティングを指定します。</li> <li>• (任意) <b>sequence value</b> 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</li> </ul>

	コマンドまたはアクション	目的
		<p>定めます。指定できる範囲は 1 ~ 4294967295 です。</p> <ul style="list-style-type: none"> <li>• (任意) <code>time-range name</code> 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。</li> </ul>
<p>ステップ 5</p>	<p><b>{deny permit} tcp</b></p> <p>例 :</p> <pre>{deny   permit} tcp {source-ipv6-prefix/prefix-length   any   hostsource-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length   any   hostdestination-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]</pre>	<p>(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。</p> <p>TCP の場合は <code>tcp</code> を入力します。パラメータはステップ 3 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。</p> <ul style="list-style-type: none"> <li>• <code>ack</code> : 確認応答 (ACK) ビットセット</li> <li>• <code>established</code> : 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。</li> <li>• <code>fin</code> : 終了ビットセット。送信元からのデータはそれ以上ありません。</li> <li>• <code>neq {port   protocol}</code> : 所定のポート番号上にならないパケットだけを照合します。</li> <li>• <code>psh</code> : プッシュ機能ビットセット</li> <li>• <code>range {port   protocol}</code> : ポート番号の範囲内のパケットだけを照合します。</li> <li>• <code>rst</code> : リセット ビットセット</li> <li>• <code>syn</code> : 同期ビットセット</li> <li>• <code>urg</code> : 緊急ポインタ ビットセット</li> </ul>
<p>ステップ 6</p>	<p><b>{deny permit} udp</b></p> <p>例 :</p> <pre>{deny   permit} udp {source-ipv6-prefix/prefix-length   any   hostsource-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length   any   hostdestination-ipv6-address} [operator [port-number]][dscp value] [log][log-input] [neq {port   protocol}] [range {port   protocol}] [routing][sequence value][time-range name]</pre>	<p>(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。</p> <p>ユーザ データグラム プロトコルの場合は、<code>udp</code> 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、<code>[operator [port]]</code> 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あればなりません。UDP の場合、<code>established</code> パラメータは無効です。</p>

	コマンドまたはアクション	目的
ステップ 7	<p><b>{deny permit} icmp</b></p> <p>例 :</p> <pre>{deny   permit} icmp {source-ipv6-prefix/prefix-length   any   hostsource-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length   any   hostdestination-ipv6-address} [operator [port-number]][icmp-type [icmp-code] icmp-message] [dscpvalue] [log] [log-input] [routing] [sequence value][time-range name]</pre>	<p>(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。</p> <p>インターネット制御メッセージプロトコルの場合は、<b>icmp</b> を入力します。ICMP パラメータはステップ 3a 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。</p> <ul style="list-style-type: none"> <li>• <b>icmp-type</b> : 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。</li> <li>• <b>icmp-code</b> : 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。</li> <li>• <b>icmp-message</b> : 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。</li> </ul>
ステップ 8	<p><b>end</b></p> <p>例 :</p> <pre>Switch(config)# end</pre>	特権 EXEC モードに戻ります。
ステップ 9	<p><b>show ipv6 access-list</b></p> <p>例 :</p> <pre>show ipv6 access-list</pre>	アクセスリストの設定を確認します。
ステップ 10	<p><b>show running-config</b></p> <p>例 :</p> <pre>Switch# show running-config</pre>	入力を確認します。
ステップ 11	<p><b>copy running-config startup-config</b></p> <p>例 :</p>	(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。



	コマンドまたはアクション	目的
	Switch# <code>copy running-config startup-config</code>	

## インターフェイスへの IPv6 ACL の適用

ここでは、ネットワーク インターフェイスに IPv6 ACL を適用する手順について説明します。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、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 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管理には、特権 EXEC モードで次の手順を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>configure terminal</b> 例： Switch# <code>configure terminal</code>	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 2	<b>interface interface_id</b> 例： Switch# <code>interface interface-id</code>	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 3	<b>no switchport</b> 例： Switch# <code>no switchport</code>	ルータ ACL を適用する場合は、インターフェイスをレイヤ2 モード（デフォルト）からレイヤ3 モードに変更します。
ステップ 4	<b>ipv6 address ipv6_address</b> 例： Switch# <code>ipv6 address ipv6-address</code>	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。このコマンドは、レイヤ2 インターフェイスでは、またはインターフェイスに明示的な IPv6 アドレスが設定されている場合には、必要ありません。
ステップ 5	<b>ipv6 traffic-filter access-list-name</b> 例： Switch# <code>ipv6 traffic-filter access-list-name {in   out}</code>	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。 <b>out</b> 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 6	<b>end</b> 例： Switch(config)# <code>end</code>	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバルコンフィギュレーションモードを終了できます。
ステップ 7	<b>show running-config</b>	アクセス リストの設定を確認します。

	コマンドまたはアクション	目的
ステップ 8	<b>copy running-config startup-config</b> 例： 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 の表示

IPv6 ACL を表示するには、次の手順を実行します。

### 手順

	コマンドまたはアクション	目的
ステップ 1	<b>enable</b> 例： Switch> enable	特権 EXEC モードをイネーブルにします。 パスワードを入力します (要求された場合)。
ステップ 2	<b>configureterminal</b> 例： Switch# 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	<b>show access-list</b> 例： Switch# 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。
ステップ 4	<b>show ipv6 access-list acl_name</b> 例： Switch# show ipv6 access-list [access-list-name]	設定済みのすべての IPv6 アクセス リストまたは名前付けされたアクセス リストを表示します。

## IPv6 ACL の設定例

### 例 : IPv6 ACL の作成

次に、CISCO と名前が付けられた IPv6 アクセス リストを設定する例を示します。リスト内の最初の拒否エントリは、宛先 TCP ポート番号が 5000 より大きいパケットをすべて拒否します。2 番目の拒否エントリは、送信元 UDP ポート番号が 5000 未満のパケットを拒否します。また、この 2 番目の拒否エントリは、すべての一致をコンソールに表示します。リスト内の最初の許可エントリは、すべての ICMP パケットを許可します。リスト内の 2 番目の許可エントリ

リは、その他のすべてのトラフィックを許可します。暗黙の全否定の条件が各 IPv6 アクセスリストの末尾にあるため、2 番めの許可エントリは必要です。



(注) ログギングは、レイヤ 3 インターフェイスでのみサポートされます。

```
Switch(config)# ipv6 access-list CISCO
Switch(config-ipv6-acl)# deny tcp any any gt 5000
Switch (config-ipv6-acl)# deny ::/0 lt 5000 ::/0 log
Switch(config-ipv6-acl)# permit icmp any any
Switch(config-ipv6-acl)# permit any any
```

## 例 : IPv6 ACL の表示

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
```

例：IPv6 ACL の表示