



IPv6 ACL の設定

- [IPv6 ACL の設定に関する情報 \(1 ページ\)](#)
- [IPv6 ACL の設定 \(2 ページ\)](#)
- [IPv6 ACL の設定例 \(10 ページ\)](#)

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、次のタイプの IPv6 ACL をサポートします。

- 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せん。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。

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。

- スイッチの 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。

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。

- 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 だけです。IPv6 用のルータ ACL および 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。
- 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) 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を判断します。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

-
- 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 (**deny**) または通過させる (**permit**) 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。
-

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 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、パケットはソフトウェアで処理されます。



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）がソフトウェアで処理されます。

- 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	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	configure terminal 例 : Device# 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	ipv6access-listaccess-list-name 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	{deny permit} protocol 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>	<p>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。</p> <ul style="list-style-type: none"> • protocol 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。 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。 • 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)。 • IPv6 プレフィックス ::/0 の短縮形として、 any を入力します。 • 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。 • (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

	コマンドまたはアクション	目的
		<p>定めます。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）、range（包含範囲）があります。</p> <p>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。</p> <ul style="list-style-type: none"> （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。 （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。 （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。 （任意）log を指定すると、エン트리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。 （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。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • (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 ~ 4294967295 です。 • (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 例 : <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>	(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。 TCP の場合は tcp 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。 <ul style="list-style-type: none"> • ack : 確認応答 (ACK) ビットセット • 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。 • fin : 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。 • 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。 • psh : プッシュ機能ビットセット • 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。 • rst : リセットビットセット • syn : 同期ビットセット • urg : 緊急ポインタ ビットセット

	コマンドまたはアクション	目的
ステップ 6	<p>{deny permit} udp</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、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あればなりません。UDP の場合、established パラメータは無効です。</p>
ステップ 7	<p>{deny permit} icmp</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] [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、icmp 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"> • 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。 • 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。 • 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。

	コマンドまたはアクション	目的
ステップ 8	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 9	show ipv6 access-list 例： Device# 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 例： Device# show running-config	入力を確認します。
ステップ 11	copy running-config startup-config 例： Device# 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	configure terminal 例： Device# 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 2	interface interface_id 例： Device# 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) 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	ipv6 traffic-filter access-list-name 例： Device# ipv6 traffic-filter access-list-name in	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。

	コマンドまたはアクション	目的
ステップ 4	end 例： Device(config)# end	特権 EXEC モードに戻ります。
ステップ 5	show running-config 例： Device# show running-config	アクセス リストの設定を確認します。
ステップ 6	copy running-config startup-config 例： Device# 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	enable 例： Device> enable	特権 EXEC モードを有効にします。 パスワードを入力します (要求された場合)。
ステップ 2	configure terminal 例： Device# 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	show access-list 例： Device(config)# show access-lists	デバイス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	show ipv6 access-list <i>acl_name</i> 例： Device(config)# show ipv6 access-list [<i>access-list-name</i>]	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は、その他のすべてのトラフィックを許可します。すべてのパケットを拒否する暗黙の条件が各 IPv6 アクセスリストの末尾にあるため、この 2 番目の許可エントリが必要となります。

```
Device(config)# ipv6 access-list CISCO
Device(config-ipv6-acl)# deny tcp any any gt 5000
Device (config-ipv6-acl)# deny ::/0 lt 5000 ::/0 log
Device(config-ipv6-acl)# permit icmp any any
Device(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、スイッチに設定済みのすべてのアクセスリストが表示されます。

```
Device# 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、スイッチに設定済みの IPv6 アクセスリストだけが表示されます。

```
Device# 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
```