IPv6 ACL の設定

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。 最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノート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。 レイヤ 3 管理トラフィックをフィルタリングするために、入力ルータ ACL を作成し、適用することもできます。

（注） IPv6 を使用するには、デュアル IPv4 および IPv6 スイッチング データベース管理（SDM）テンプレートがスイッチに設定されている必要があります。 テンプレートの選択は、**sdm prefer {default | dual-ipv4-and-ipv6}** グローバル コンフィギュレーション コマンドで行います。

（注） この章で使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスまたは手順に記載された Cisco IOS のマニュアルを参照してください。

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。
- 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。

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接続されている ACL に ACE が追加されるのを許可しません。

IPv6 ACL の設定

IPv6 ACL を設定する場合は、事前にデュアル IPv4 および IPv6 SDM テンプレートのいずれかを選択する必要があります。

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

- 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（たとえば、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。

IPv6 ACL の作成

IPv6 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 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 2	**ipv6access-list***access-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 3	**{deny|permit} protocol** 例： `{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。 • 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。

	コマンドまたはアクション	目的
		• 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）、range（包含範囲）があります。 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。 • （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。 • （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
		• （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 4	**{deny|permit} tcp** 例： `{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]`	（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。 • 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

ステップ 5	**{deny|permit} udp**
	
	例：
	`{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]`
		（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。
		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。

	コマンドまたはアクション	目的
ステップ 6	**{deny|permit} icmp** 例： `{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]`	（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。 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。 • 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。
ステップ 7	**end** 例： `Switch(config)# end`	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 8	**show ipv6 access-list** 例： `show ipv6 access-list`	アクセス リストの設定を確認します。
ステップ 9	**copy running-config startup-config** 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。

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には、特権 EXEC モードで次の手順を実行します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 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 2	**interface** interface_id 例： `Switch# 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 3	**no switchport** 例： `Switch# no switchport`	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	**ipv6 address** *ipv6_address* 例： `Switch# 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。 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	**ipv6 traffic-filter** *access-list-name* 例： `Switch# 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。 **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 6	**end** 例： `Switch(config)# end`	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	**show running-config**	アクセス リストの設定を確認します。
ステップ 8	**copy running-config startup-config** 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

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。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show access-list** 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 2	**show ipv6 access-list** *acl_name* 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 番めの拒否エントリは、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 番めの拒否エントリは、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 番めの許可エントリは、その他のすべてのトラフィックを許可します。 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。

```
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 の適用

次に、レイヤ 3 インターフェイスの発信トラフィックに対して、アクセス リスト Cisco を適用する例を示します。

```
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001::/64 eui-64
Switch(config-if)# ipv6 traffic-filter CISCO out
```

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
```