CHAPTER 39

IPv6 ACL の設定

この章では、Catalyst 3750 Metro スイッチで IPv6 ACL を設定する方法について説明します。IP version 6（IPv6）のトラフィックは、IPv6 の Access Control List（ACL; アクセス コントロール リスト）を作成してインターフェイスに適用することでフィルタリングできます。これは、IP version 4（IPv4）の名前付き ACL を作成して適用する方法と似ています。また、入力ルータ ACL を作成および適用して、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。

（注） IPv6 を使用するには、スイッチ上でデュアル IPv4/IPv6 Switch Database Management（SDM）テンプレートを設定する必要があります。**sdm prefer dual-ipv4-and-ipv6** グローバル コンフィギュレーション コマンドを入力して、テンプレートを選択します。

関連情報については、次の章を参照してください。

- SDM テンプレートの詳細については、第 6 章「SDM テンプレートの設定」を参照してください。
- スイッチ上の IPv6 の詳細については、第 37 章「IPv6 ユニキャスト ルーティングの設定」を参照してください。
- スイッチ上の ACL の詳細については、第 39 章「IPv6 ACL の設定」を参照してください。

（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で参照されている Cisco IOS マニュアルを参照してください。

この章の内容は次のとおりです。

IPv6 ACL の概要

スイッチでは、次の 2 種類の IPv6 ACL がサポートされています。

- IPv6 ルータ ACL
  - レイヤ 3 インターフェイスの発信または着信トラフィック（ルーテッド ポート、Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）、またはレイヤ 3 EtherChannel）でサポートされています。
  - ルーティングされる IPv6 パケットにだけ適用されます。

- 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ています。
  - インターフェイスに着信するすべての IPv6 パケットに適用されます。

スイッチでは、入力ポート ACL だけがサポートされています。

（注）　サポートされていない IPv6 ACL を設定すると、エラー メッセージが表示され、設定は無効になります。

スイッチでは、IPv6 トラフィックの VLAN ACL（VLAN マップ）はサポートされていません。

（注）　スイッチの ACL サポートの詳細については、第 33 章「ACL によるネットワーク セキュリティの設定」を参照してください。

1 つのインターフェイスに IPv4 と IPv6 の両方の ACL を適用できます。

IPv4 ACL と同様に、IPv6 のポート ACL はルータ ACL に優先します。

- 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パケットが着信すると、このパケットはポート 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パケットが着信すると、このパケットはポート ACL によってフィルタリングされます。発信されるルーテッド 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。

ここでは、スイッチの IPv6 ACL に関する特性について説明します。

- 「サポートされている ACL 機能」（P.39-2）
- 「IPv6 ACL の制限事項」（P.39-3）

サポートされている 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 と同様の **fragments** キーワード）がサポートされています。
- IPv4 でサポートされている統計情報と同じ統計情報が IPv6 ACL でもサポートされています。
- スイッチの Ternary Content Addressable Memory（TCAM; Ternary CAM）スペースが不足している場合、ACL ラベルに関連付けられているパケットは CPU に転送され、ソフトウェアで ACL が適用されます。
- ホップバイホップ オプションが設定されているルーテッド パケットまたはブリッジド パケットの場合、ソフトウェアで IPv6 ACL が適用されます。
- 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、標準および拡張の番号制 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。

スイッチでは、Cisco IOS でサポートされているほとんどの IPv6 ACL がサポートされていますが、次の例外があります。

- IPv6 の送信元および宛先アドレス：ACL の照合は、/0 ～ /64 のプレフィクスおよび Extended Universal Identifier（EUI）-64 フォーマットのホスト アドレス（/128）でだけサポートされます。スイッチでは、情報損失のない次のホスト アドレスだけがサポートされています。
  - 集約可能なグローバル ユニキャスト アドレス
  - リンク ローカル アドレス
- スイッチでは、**flowlabel**、**routing header**、および **undetermined-transport** キーワードでの照合はサポートされていません。
- スイッチでは、再帰 ACL（**reflect** キーワード）はサポートされていません。
- このリリースでは、IPv6 のポート ACL およびルータ ACL だけがサポートされています。VLAN ACL（VLAN マップ）はサポートされていません。
- スイッチでは、IPv6 フレームには MAC ベース ACL が適用されません。
- IPv6 のポート ACL はレイヤ 2 EtherChannel には適用できません。
- スイッチでは、出力ポート ACL がサポートされていません。
- ACL を設定するときに ACL に入力するキーワードには、そのプラットフォームでサポートされているかどうかに関係なく、制限がありません。ハードウェア転送（物理ポートまたは SVI）を必要とするインターフェイスに ACL を適用する場合、スイッチはそのインターフェイスで ACL がサポート可能かどうかを判別します。サポートできない場合、ACL の付加は拒否されます。
- ACL をインターフェイスに適用して、サポートされていないキーワードを含む Access Control Entry（ACE; アクセス コントロール エントリ）を付加しようとした場合、スイッチでは、現在インターフェイスに付加されている ACL に ACE を追加することが許可されません。

IPv6 ACL の設定

IPv6 ACL を設定する前に、デュアル IPv4/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には、次の手順を実行します。

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　トラフィックをブロック（deny）または渡す（permit）ように IPv6 ACL を設定します。

ステップ 3　IPv6 ACL をインターフェイスに適用します。ルータ ACL の場合は、ACL を適用するレイヤ 3 インターフェイスの IPv6 アドレスも設定する必要があります。

ここでは、IPv6 ACL を設定および適用する方法について説明します。

- 「IPv6 ACL のデフォルト設定」（P.39-4）
- 「他の機能との相互作用」（P.39-4）

IPv6 ACL のデフォルト設定

IPv6 ACL は、デフォルトでは設定も適用も行われません。

他の機能との相互作用

IPv6 ACL の設定には、次のような機能またはスイッチ特性との相互作用があります。

- IPv6 ルータ ACL がパケットを拒否するように設定されている場合、パケットはドロップされます。パケットのコピーが Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）のキューに送信され、フレームに対する ICMP 到達不能メッセージが生成されます。
- ブリッジングされたフレームがポート 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。
- 1 つのスイッチで IPv4 と IPv6 の両方の ACL を作成したり、同じインターフェイスに IPv4 と IPv6 の両方の ACL を適用したりできます。それぞれの ACL に一意の名前を指定する必要があります。すでに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 の作成と IPv6 ACL の作成、および同じレイヤ 2 またはレイヤ 3 インターフェイスへの IPv4 ACL の適用または IPv6 ACL の適用には、それぞれ異なるコマンドを使用します。誤ったコマンドを使用して ACL を付加すると（IPv4 コマンドを使用して IPv6 ACL を付加するなど）、エラー メッセージが表示されます。
- IPv6 フレームのフィルタリングに MAC ACL は使用できません。MAC ACL は非 IP フレームだけをフィルタリングできます。
- TCAM が満杯の場合、さらに設定済みの 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。

	コマンド	目的
ステップ 1	**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	**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。

	コマンド	目的
ステップ 3a	**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**] [**sequence** *value*] [**time-range** *name*]	**deny** または **permit** を入力し、条件と一致した場合にパケットを拒否するかまたは許可するかを指定します。条件は次のとおりです。 • *protocol* には、インターネット プロトコルの名前（**ahp**、**esp**、**icmp**、**ipv6**、**pcp**、**stcp**、**tcp**、**udp**）、または IPv6 プロトコル番号を示す 0 ～ 255 の範囲の整数を入力します。ICMP、Transmission Control Protocol（TCP; 伝送制御プロトコル）、および User Datagram Protocol（UDP; ユーザ データグラム プロトコル）の具体的なパラメータについては、ステップ 3b ～ 3d を参照してください。 • *source-ipv6-prefix*/*prefix-length* または *destination-ipv6-prefix*/ *prefix-length* は、拒否または許可の条件を設定する送信元または宛先の IPv6 ネットワークまたはネットワーク クラスで、16 ビット値をコロンで区切った 16 進数で指定する必要があります（RFC 2373 を参照）。 （注）　CLI ヘルプでは /0 ～ /128 のプレフィクス長が表示されますが、スイッチでは、集約可能なグローバル ユニキャストとリンク ローカル ホスト アドレスの /0 ～ /64 のプレフィクス、および EUI ベースの /128 プレフィクスに対してだけ IPv6 アドレス照合がサポートされます。 • **any** は IPv6 プレフィクス ::/0 の省略形として入力します。 • **host** *source-ipv6-address* または *destination-ipv6-address* には、拒否または許可条件を設定する送信元または宛先の IPv6 ホスト アドレスを、16 ビット値をコロンで区切った 16 進数で入力します。 • （任意）*operator* には、指定のプロトコルの送信元または宛先ポートを比較する演算子を指定します。演算子は、**lt**（less than：未満）、**gt**（greater than：より大きい）、**eq**（equal：一致）、**neq**（not equal：不一致）、**range**（inclusive range：包含範囲）です。 演算子が *source-ipv6-prefix*/*prefix-length* 引数の後ろに置かれた場合は、送信元ポートと一致する必要があります。演算子が *destination-ipv6-prefix/prefix-length* 引数の後ろに置かれた場合は、宛先ポートと一致する必要があります。 • （任意）*port-number* は 0 ～ 65535 の 10 進数か、TCP または UDP ポートをフィルタリングする場合にはそれぞれの TCP または UDP の名前です。 • （任意）各 IPv6 パケット ヘッダーのトラフィック クラス フィールドのトラフィック クラス値と Differentiated Service Code Point（DSCP; DiffServ コード ポイント）値を照合するには、**dscp** *value* を入力します。指定できる範囲は 0 ～ 63 です。 • （任意）初期状態でないフラグメントをチェックするには、**fragments** を入力します。このキーワードは、プロトコルが **ipv6** の場合にかぎり認識されます。 • （任意）設定と一致したパケットのロギング メッセージをコンソールに送信するように指定するには、**log** を入力します。入力インターフェイスをログ エントリに含めるには、**log-input** を入力します。ロギングがサポートされるのは、ルータ ACL だけです。 • （任意）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するには、**sequence** *value* を入力します。指定できる範囲は 1 ～ 4294967295 です。 • （任意）ステートメントの時間範囲を指定するには、**time-range** *name* を入力します。

	コマンド	目的
ステップ 3b	**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**] [**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。 伝送制御プロトコルの場合は **tcp** を入力します。次に示す任意の追加パラメータを除き、ステップ 3a で説明するパラメータと同じパラメータを使用します。 • **ack** *:* ACK ビット設定。 • **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**：FIN ビット設定。送信元からのデータはこれ以上ありません。 • **neq** {*port* | *protocol*} *:* 指定のポート番号上にないパケットだけを照合します。 • **psh**：PSH ビット設定。 • **range** {*port* | *protocol*}：ポート番号範囲のパケットだけを照合します。 • **rst**：RST ビット設定。 • **syn**：SYN ビット設定。 • **urg** *:* URG ビット設定。
ステップ 3c	**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*}] [**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*]] で指定する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とします。UDP の場合、**established** パラメータは無効です。
ステップ 3d	**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**] [**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 タイプを基準にしてフィルタリングします。0 ～ 255 の値を使用できます。 • *icmp-code*：ICMP メッセージ コード タイプを基準にしてフィルタリングされた ICMP パケットをフィルタリングします。0 ～ 255 の値を使用できます。 • *icmp-message*：ICMP メッセージ タイプ名または ICMP メッセージのタイプおよびコード名を基準にして、ICMP パケットをフィルタリングします。ICMP メッセージ タイプ名およびコード名のリストを表示するには、? キーを使用するか、このリリースのコマンド リファレンスを参照します。

	コマンド	目的
ステップ 4	**end**	特権 EXEC モードに戻ります。
ステップ 5	**show ipv6 access-list**	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**	（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。

キーワードを指定して **no deny** | **permit** IPv6 アクセスリスト コンフィギュレーション コマンドを使用すると、指定したアクセス リストから拒否または許可の条件が削除されます。

次に、CISCO という名前の IPv6 アクセス リストを設定する例を示します。リストの最初の拒否エントリは、5000 より大きい宛先 TCP ポート番号を持つすべてのパケットを拒否します。2 番めの拒否エントリは、5000 未満の送信元 UDP ポート番号を持つ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。リストの 2 番めの許可エントリは、その他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 番めの許可エントリが必要となります。

```
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
```

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。ACL は、レイヤ 3 インターフェイスの発信または着信トラフィックに、あるいはレイヤ 2 インターフェイスの着信トラフィックに適用できます。

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。

	コマンド	目的
ステップ 1	**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*	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）を指定し、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**	ルータ ACL を適用する場合は、レイヤ 2 モード（デフォルト）からレイヤ 3 モードにインターフェイスを変更します。
ステップ 4	**ipv6 address** *ipv6-address*	レイヤ 3 インターフェイス（ルータ ACL 用）の IPv6 アドレスを設定します。 このコマンドは、レイヤ 2 インターフェイスの場合、またはインターフェイスが明示的な IPv6 アドレスですでに設定されている場合には不要です。
ステップ 5	**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**	特権 EXEC モードに戻ります。

	コマンド	目的
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**	（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。

no ipv6 traffic-filter *access-list-name* インターフェイス コンフィギュレーション コマンドを使用して、インターフェイスからアクセス リストを削除します。

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

```
Switch(config)# interface gigabitethernet1/1/1
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001::/64 eui-64
Switch(config-if)# ipv6 traffic-filter CISCO out
```

IPv6 ACL の表示

表 39-1 に示す 1 つまたは複数の特権 EXEC コマンドをすると、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 39-1　IPv6 アクセス リストの情報を表示するコマンド

コマンド	目的
show access-lists	スイッチに設定されているすべてのアクセス リストを表示します。
show ipv6 access-list [*access-list-name*]	設定されているすべての IPv6 アクセス リストまたは名前で指定したアクセス リストを表示します。

次に、**show access-lists** 特権 EXEC コマンドの出力例を示します。スイッチに設定されているすべてのアクセス 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。スイッチに設定されている 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
```