CHAPTER 41

# IPv6 ACL の設定

この章では、Catalyst 3750 スイッチに IPv6 ACL を設定する方法について説明します。IP バージョン 6（IPv6）Access Control List（ACL; アクセス コントロール リスト）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。入力ルータ ACL を作成して適用し、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。

特に明記しないかぎり、*スイッチ*という用語はスタンドアロン スイッチおよびスイッチ スタックを意味します。

（注） IPv6 を使用するには、デュアル IPv4 および IPv6 Switch Database Management（SDM; スイッチ データベース管理）テンプレートが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。

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 8 章「SDM テンプレートの設定」を参照してください。
- スイッチの IPv6 については、第 5 章「スイッチ スタックの管理」を参照してください。
- スイッチの ACL については、第 41 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、このリリースのコマンド 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。

この章で説明する内容は、次のとおりです。

# IPv6 ACL の概要

スイッチ スタック 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、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 などのレイヤ 3 インターフェイスの発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インバウンド トラフィック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。

IP ベース イメージが稼動するスイッチ スタックは、入力ルータ IPv6 ACL だけをサポートします。ポート ACL や出力 IPv6 ルータ ACL をサポートしません。

（注）　未サポートの IPv6 ACL を設定すると、エラー メッセージが表示されて設定が有効になりません。

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

（注）　スイッチでの ACL サポートの詳細については、第 35 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 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。その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。その他のパケットはフィルタリングされません。

（注）　インターフェイスに*任意*のポート ACL（IPv4、IPv6、または MAC）が適用される場合、このポート ACL はパケットのフィルタリングで使用され、ポート VLAN の SVI に付加されたルータ ACL はすべて無視されます。

ここでは、スイッチの IPv6 ACL の特性の一部について説明します。


- 「サポートされる ACL 機能」（P.41-3）
- 「IPv6 ACL の制限事項」（P.41-3）
- 「IPv6 ACL とスイッチ スタック」（P.41-4）

# 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、番号付きの標準 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 のプレフィクスおよびホスト アドレス（/128）だけサポートされます。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。
  - 集約可能なグローバル ユニキャスト アドレス
  - リンクに対してローカルなアドレス
- スイッチは、**flowlabel**、**routing header**、および **undetermined-transport** の各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、スイッチ スタック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関わらず、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 Access Control Entry（ACE; アクセス コントロール エントリ）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 とスイッチ スタック

スタック マスターは IPv6 ACL をハードウェアでサポートし、IPv6 ACL をスタック メンバーに配信します。

（注）　スイッチ スタック内で IPv6 を機能させるには、すべてのスタック メンバーで拡張 IP サービス イメージ を実行している必要があります。

新しいスイッチがスタック マスターを引き継ぐと、ACL 設定がすべてのスタック メンバーに配信されます。メンバー スイッチは、新しいスタック マスターによって配信された設定を同期し、不要なエントリを消去します。

ACL の修正、インターフェイスへの適用、またはインターフェイスからの解除が行われると、スタック マスターは変更内容をすべてのスタック メンバーに配信します。

# IPv6 ACL の設定

IPv6 ACL を設定する場合は、事前にデュアル 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場合は、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**　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。

ここでは、IPv6 ACL の設定および適用方法について説明します。


- 「IPv6 ACL のデフォルト設定」（P.41-4）
- 「他の機能との相互作用」（P.41-5）
- 「IPv6 ACL の作成」（P.41-5）
- 「インターフェイスへの IPv6 ACL の適用」（P.41-8）


## 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。

# 他の機能との相互作用

IPv6 ACL の設定には、他の機能またはスイッチ特性と次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設定されている場合、パケットは廃棄されます。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）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 つのスタックに作成したり、同一インターフェイスに適用したりできます。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。
- 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、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。次に、条件について説明します。<br>• *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。ICMP、TCP、および UDP 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。<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、16 ビット値を使用したコロン区切りの 16 進形式で指定されます（RFC 2373 を参照）。<br>（注）　CLI（コマンドライン インターフェイス）ヘルプでは、/0 ～ /128 の範囲のプレフィクス長が表示されますが、スイッチは、集約可能なグローバル ユニキャスト アドレスとリンクに対してローカルなホスト アドレスの /0 ～ /64 の範囲のプレフィクス、および EUI ベースの /128 プレフィクスに対する IPv6 アドレス照合だけをサポートします。<br>• IPv6 プレフィクス ::/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 16 ビット値を使用したコロン区切りの 16 進形式で指定されます。<br>• （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）などです。<br>*source-ipv6-prefix*/*prefix-length* 引数のあとのオペレータは、送信元ポートに一致する必要があります。*destination-ipv6- prefix/prefix-length* 引数のあとのオペレータは、宛先ポートに一致する必要があります。<br>• （任意）*port-number* は、TCP または UDP のフィルタリングで、それぞれ 0 ～ 65535 の 10 進数または TCP あるいは UDP ポートの名前です。<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>• （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>• （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ギング 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>• （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。<br>• （任意）**time-range** *name* を入力して、ステートメントの時間の範囲を指定します。 |

| | 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。<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 セットが含まれる場合は、照合が行われます。<br>• **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。<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 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。<br>UDP 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 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。<br>ICMP 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。<br>• *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。<br>• *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します。0 ～ 255 の値を使用できます。<br>• *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名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 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。 |

指定のアクセス リストから拒否または許可条件を削除するには、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 コマンドを使用します。

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、2 番めの拒否エントリは、コンソールにすべての一致結果を記録します。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
```

# 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 をレイヤ 3 インターフェイスの発信または着信トラフィック、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することができます。

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。<br>**（注）** IP ベース イメージを稼動中のスイッチは、ポート ACL をサポートしていません。 |
| ステップ 3 | **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* | 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。<br>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* {**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>**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。stack で IP ベース イメージを稼動している場合、**out** キーワードはレイヤ 3 インターフェイス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。 |
| 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。 |

インターフェイスからアクセス リストを削除するには、**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 コマンドを使用します。

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)# interface gigabitethernet1/0/3
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

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するには、表 41-1 に示された 1 つまたは複数の特権 EXEC コマンドを使用します。

**表 41-1　IPv6 アクセス リスト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 リストまたは名前付けされたアクセス 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。出力には、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 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
```