CHAPTER 38

# IPv6 ACL の設定

アドバンスト IP サービス イメージを Catalyst 3750 スイッチにインストールしている場合、IP バージョン 4（IPv4）名前付き Access Control List（ACL; アクセス制御リスト）を作成および適用するのと同様に、IPv6 ACL を作成してインターフェイスに適用すると、IP バージョン 6（IPv6）トラフィックをフィルタリングできます。ここでは、スイッチ上で IPv6 ACL を設定する方法を説明します。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、スイッチまたはスタック マスターでアドバンスト IP サービス イメージを実行し、スイッチにデュアル IPv4/IPv6 Switch Database Management（SDM; スイッチ データベース管理）テンプレートを設定する必要があります。テンプレートの選択は、**sdm prefer dual-ipv4-and-ipv6** {**default** | **vlan**} [**desktop**] 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。
- スイッチ上の IPv6 の設定については、第 36 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 の設定については、第 32 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。

（注） この章で使用され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、または手順で参照している Cisco IOS 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

このスイッチは 2 つのタイプの IPv6 ACL をサポートしています。

- IPv6 ルータ 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対してサポートされます。レイヤ 3 インターフェイスには、ルーテッド ポート、Switch Virtual Interfaces（SVI; スイッチ仮想インターフェイス）、またはレイヤ 3 EtherChannel があります。IPv6 ルータ ACL は、ルーティングされた IPv6 パケットに対してのみ適用されます。
- IPv6 ポート ACL は、レイヤ 2 インターフェイスの着信トラフィックに対してのみサポートされます。IPv6 ポート ACL は、インターフェイスで受信されるすべての IPv6 パケットに適用されます。

このスイッチは IPv6 トラフィックに対する VLAN ACL（VLAN マップ）はサポートしていません。

（注）　スイッチ上の ACL サポートの詳細については、第 32 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。

インターフェイスには、IPv4 ACL と IPv6 ACL の両方を適用できます。

IPv4 ACL と同様、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 と入力ポート ACL が存在する場合、ポート ACL が適用されたポートで受信したパケットは、ポート ACL によってフィルタリングされます。その他のポートで受信したルーテッド 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 と入力ポート ACL が存在する場合、ポート ACL が適用されたポートで受信したパケットは、ポート ACL によってフィルタリングされます。送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。その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 がパケットのフィルタリングに使用され、ポート VLAN の SVI に適用されたルータ ACL はすべて無視されます。

ここでは、スイッチの IPv6 ACL の特性を説明します。



## サポートされる ACL 機能

このスイッチの IPv6 ACL には次の特性があります。

- 分割されたフレーム（IPv4 と同様の **fragments** キーワード）がサポートされます。
- IPv4 でサポートされている同一の統計情報が IPv6 ACL でもサポートされます。
- スイッチが TCAM スペースを使い果たした場合、ACL ラベルに関連付けられたパケットは CPU に転送され、ソフトウェアで ACL が適用されます。
- hop-by-hop オプション付きのルーテッド 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 にはサポートされますが、ポート ACL にはサポートされません。

## IPv6 ACL の制限事項

IPv4 の場合、標準番号付き ACL、拡張番号付き ACL、名前付き ACL、および MAC ACL を設定できます。IPv6 の場合は、名前付き ACL のみがサポートされます。

スイッチは、いくつかの例外を除き、Cisco IOS をサポートするほとんどの IPv6 ACL に対応しています。

- IPv6 の送信元アドレスと宛先アドレス **—** ACL の照合は、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）のみでサポートされます。スイッチは、次の情報を持つホスト アドレスのみをサポートします。
  - 集約可能なグローバル ユニキャスト アドレス
  - リンク ローカル アドレス
- **flowlabel** キーワード、**routing header** キーワード、および **undetermined-transport** キーワードでの照合はサポートされません。
- 再帰 ACL（**reflect** キーワード）はサポートされません。
- このリリースでは、IPv6 へのポート ACL とルータ ACL のみがサポートされ、VLAN ACL（VLAN マップ）はサポートされません。
- MAC ベース ACL は、IPv6 フレームでは適用されません。
- IPv6 ポート ACL をレイヤ 2 EtherChannel に適用することはできません。
- このリリースの IPv6 ACL は、拡張 IP サービス イメージを稼働するスイッチ スタックのみでサポートされます。
- ACL を設定する際は、プラットフォームでサポートされているかどうかにかかわらず、ACL にキーワードを無制限に入力できます。ハードウェア転送を必要とするインターフェイス（物理ポートまたは SVI）に ACL を適用する際は、スイッチはそのインターフェイスで ACL をサポートできるかどうかを判断するためのチェックを行います。サポートできない場合は、ACL を適用することはできません。
- ACL がインターフェイスに適用され、サポートされていないキーワードで ACE を追加しようとすると、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 の追加を行なうことを許可しません。

## 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 メンバーでアドバンスト 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 を設定する前に、デュアル IPv4/IPv6 SDM テンプレートを選択する必要があります。ルータ ACL を設定する場合は、スイッチ スタックで IPv6 ルーティングもイネーブルに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**　トラフィックのブロック（拒否）または通過（許可）のために 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 インターフェイスに IPv6 アドレスも設定します。

ここでは、IPv6 ACL を設定し、適用する方法を説明します。



## IPv6 ACL のデフォルト設定

デフォルトでは、IPv6 ACL の設定または適用は行われません。

## 他の機能との相互作用

IPv6 ACL の設定は、他の機能またはスイッチの特性と次のように相互作用します。

- パケットを拒否するために IPv6 ルータ ACL を設定すると、拒否されたパケットはルーティングされません。そのフレームに対して ICMP unreachable メッセージを生成するために、パケットのコピーが Internet Control Message Protocol（ICMP）キューに送られます。
- ブリッジド フレームがポート ACL によって破棄される場合、そのフレームはブリッジ処理されません。
- スタック上に IPv4 ACL と IPv6 ACL の両方を作成し、両方の ACL を同一のインターフェイスに適用することができます。各 ACL には一意の名前を付ける必要があり、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 と IPv6 の ACL を作成する場合、同一のレイヤ 2 またはレイヤ 3 インターフェイスに適用するときには、異なるコマンドを使用します。ACL を適用する際に不適切なコマンドを使用すると（IPv6 ACL を適用するために IPv4 コマンドを使用した場合など）、エラー メッセージが表示されます。
- MAC ACL は IPv6 フレームのフィルタリングには使用できません。MAC ACL は非 IP フレームのフィルタリングのみに使用できます。
- TCAM が満杯の場合、追加設定された ACL 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、イネーブル EXEC モードで次の手順を実行します。

| | コマンド | 説明 |
|---|---|---|
| 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* | 名前を使用して IPv6 アクセス リストを定義し、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 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*] | 条件が一致した場合にパケットを拒否するか許可するかを指定するため、**deny** または **permit** を入力します。このコマンドには次の条件があります。<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**、または **udp**、または IPv6 プロトコル番号を示す 0 ～ 255 の範囲の整数です。<br>（注）　ICMP、TCP、および UDP に対する追加の固有パラメータについては、手順 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、拒否または許可条件の設定対象となる、送信元または宛先 IPv6 ネットワークまたはネットワークのクラスで、コロンで区切られた 16 進数表記の 16 ビット値（RFC 2373 参照）で指定されます。<br>（注）　CLI ヘルプでは、プレフィクス長の範囲は /0 ～ /128 と表示されますが、スイッチは /0 ～ /64 の範囲のプレフィクスに対応する IPv6 アドレス、および集約グローバル ユニキャストとリンクローカル ホスト アドレス用の EUI ベース /128 プレフィクスのみをサポートします。<br>• IPv6 プレフィクス ::/0 の省略形として、**any** を使用できます。<br>• **host** *source-ipv6-address* または *destination-ipv6-address* には、コロンで区切られた 16 進数表記の 16 ビット値で指定された、拒否または許可条件の設定対象となる、送信元または宛先 IPv6 ホスト アドレスを入力します。<br>• （任意）*operator* には、指定されたプロトコルの送信元または宛先ポートを比較するオペランドを指定します。使用可能なオペランドは **lt**（より小さい）、**gt**（より大きい）、**eq**（等しい）、**neq**（等しくない）、および **range** です。<br>*source-ipv6-prefix/prefix-length* 引数のあとに演算子が続く場合は、送信元ポートと一致する必要があります。*destination-ipv6-prefix/prefix-length* 引数のあとに演算子が続く場合は、宛先ポートと一致する必要があります。<br>• （任意）*port-number* は、0 ～ 65535 の範囲の 10 進数、または TCP ポートまたは UDP ポートの名前です。TCP ポート名は TCP をフィルタリングする場合にのみ使用できます。UDP ポート名は UDP をフィルタリングする場合にのみ使用できます。 |

| | コマンド | 説明 |
|---|---|---|
| **ステップ 3a**<br>（続き） | | • （任意）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、Differentiated Services（DiffServ; 差別化サービス）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。<br>• （任意）先頭以外の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** の場合にのみ使用できます。<br>• （任意）エントリと一致するパケットに関するロギング　メッセージをコンソールに送信するには、**log** を指定します。ログ エントリに入力インターフェイスを含めるには、**log-input** を入力します。ロギングはルータ ACL に対してのみサポートされます。<br>• （任意）アクセス リストのステートメントへ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。<br>• （任意）deny または permit ステートメントに適用される時間範囲を指定するには、**time-range** *name* を入力します。 |
| **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 で説明するパラメータと同じで、ほかにも以下の任意のパラメータを使用できます。<br>• **ack** — 応答確認ビット 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、照合が行われます。<br>• **fin** — 完了ビット セット。送信者からのデータはこれで終わりです。<br>• ***neq*** {*port* \| *protocol*} — 指定されたポート番号以外のポート上のパケットのみ照合<br>• **psh** — プッシュ機能ビット セット<br>• ***range*** {*port* \| *protocol*} — 指定されたポート番号範囲内のパケットのみ照合<br>• **rst** — リセット ビット セット<br>• **syn** — 同期ビット セット<br>• ***urg*** — アージェント 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とします。UDP では、**established** パラメータは無効です。 |

| | コマンド | 説明 |
|---|---|---|
| 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 のほとんどの IP プロトコルで説明されているパラメータと同じですが、ICMP メッセージ タイプとコード 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 タイプを使用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 タイプを使用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。<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およびコード名で、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、? キーワードを使用するか、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** | イネーブル 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。 |

指定されたアクセス リストから deny または permit 条件を削除するには、**no deny** | **permit** IPv6 access-list コンフィギュレーション コマンドとキーワードを使用します。

この例では、CISCO という名前の IPv6 アクセス リストを設定します。リストの最初の deny エントリにより、宛先 TCP ポート番号が 5000 より大きいパケットがすべて拒否されます。2 番めの deny エントリにより、送信元 UDP ポート番号が 5000 より小さいパケットが拒否されます。また、2 番めの deny エントリにより、すべての一致がコンソールに出力されます。リストの最初の permit エントリにより、すべての ICMP パケットが許可されます。リストの 2 番めの permit エントリにより、その他のすべてのトラフィックが許可されます。各 IPv6 アクセス リストの末尾には deny-all 条件が存在するため、2 番めの permit エントリが必要になります。

```
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 をレイヤ 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に適用できます。ACL はレイヤ 2 インターフェイスの着信トラフィックに対してのみ適用できます。

インターフェイスへのアクセスを制御するには、イネーブル EXEC モードで次の手順を実行します。

| | コマンド | 説明 |
|---|---|---|
| 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、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。 |

| | コマンド | 説明 |
|---|---|---|
| ステップ 3 | **no switchport** | ルータ ACL を適用する場合、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 インターフェイスで IPv6 アドレスを設定します（ルータ ACL 用）。<br>（注）　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にすでに明示的に IPv6 アドレスが設定されている場合は、このコマンドは必要ありません。 |
| 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>（注）　**out** キーワードは、レイヤ 2 インターフェイス（ポート ACL）ではサポートされていません。 |
| ステップ 6 | **end** | イネーブル 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、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 gigabitethernet 1/0/3
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

表 38-1 に記載の 1 つまたは複数のイネーブル EXEC コマンドを使用して、すべての設定済みアクセス 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 38-1　IPv6 アクセス リスト情報を表示するためのコマンド**

| コマンド | 説明 |
|---|---|
| **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*] | すべての設定済み IPv6 アクセス リストまたは名前で指定されたアクセス リストを表示します。 |

次に、**show access-lists** イネーブル 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** イネーブル 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 リストのみが表示されます。

```
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
```