CHAPTER 36

IPv6 ACL の設定

IP Version 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 Version 4（IPv4）の名前付き ACL を作成し、適用する方法と同じです。また、スイッチが IP サービスまたは IP ベース フィーチャ セットを実行している場合に、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。この章では、スイッチに IPv6 ACL を設定する方法について説明します。特に記述がない限り、*スイッチ*という用語はスタンドアロン スイッチとスイッチ スタックを意味しています。

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 dual-ipv4-and-ipv6** {**default** | **vlan**} 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 については、第 40 章「IPv6 ホスト機能とユニキャスト 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 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。

（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。

この章の内容は次のとおりです。

サポートされる IPv6 ACL

表 36-1 に、各スイッチでサポートされている IPv6 ACL を示します。

表 36-1　サポートされる IPv6 ACL 機能

機能	Catalyst Switch Module 3110	Catalyst Switch Module 3012
入力ルータ IPv6 ACL	あり	あり
出力ルータ IPv6 ACL	あり	なし
入力ポート IPv6 ACL	あり	なし
出力ポート IPv6 ACL	なし	なし
MAC ACL	なし	なし
VLAN ACL（VLAN マップ）	なし	なし

IPv6 ACL の概要

ここでは、次の情報について説明します。

サポートされる ACL 機能

Catalyst Switch Module 3110 または 3012 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。
- スイッチのハードウェア メモリが不足している場合、ACL 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。

Catalyst Switch Module 3110 の IPv6 ACL には、次の特性があります。

- 次の IPv6 ACL がサポートされています。
  - IPv6 ルータ ACL は、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 に設定できるレイヤ 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。IPv6 ルータ ACL は、ルーティングされる IPv6 パケットに対してだけ適用されます。
  - 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だけでサポートされます。IPv6 ポート ACL は、インターフェイスに着信するすべての IPv6 パケットに対して適用されます。
- IP ベース フィーチャ セットを実行しているスイッチは、入力ルータ IPv6 ACL だけをサポートしています。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。

- 出力ルータ ACL または入力ポート ACL を、IP ベース フィーチャ セットまたは IP サービス フィーチャ セットを実行しているスイッチ上で作成または適用すると、ACL はスイッチ コンフィギュレーションに追加されますが、有効にならず、エラー メッセージが表示されます。出力ルータ ACL または入力ポート ACL を使用する必要がある場合は、スイッチ コンフィギュレーションを保存し、ACL をサポートしている IP サービス フィーチャ セットをイネーブルにします。
- スイッチは、IPv6 トラフィックの VLAN ACL（VLAN マップ）をサポートしません。

（注）　スイッチの 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。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。

- 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。
- すべてのプレフィクス長に対し、IPv6 アドレス照合がサポートされます。

Catalyst Switch Module 3012 の IPv6 ACL には、次の特性があります。

- レイヤ 3 インターフェイスで受信するすべての IPv6 管理パケットに適用される、入力ルータ IPv6 ACL だけがサポートされます。
- IPv6 トラフィックに対する IPv6 ポート ACL、出力 IPv6 ルータ ACL、VLAN ACL（VLAN マップ）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。

Cisco IOS でサポートされる IPv6 ACL の大部分がサポートされますが、次の例外があります。

- IPv6 送信元および宛先アドレス：ACL 照合は、Extended Unique 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）だけでサポートされます。Catalyst Switch Module 3012 は、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 ローカル アドレス
- キーワード **flowlabel**、**routing header**、**undetermined-transport** に対する照合はサポートされません。
- 再起 ACL（**reflect** キーワード）はサポートされません。
- IPv6 フレームには MAC ベース ACL が適用されません。
- レイヤ 2 EtherChannel に IPv6 ポート ACL を適用できません。
- IPv6 の出力ルータ ACL および入力ポート ACL は、Catalyst Switch Module 3110 が IP サービス フィーチャ セットを実行している場合にだけサポートされます。IP ベース フィーチャ セットを実行しているスイッチでは、IPv6 管理トラフィックに対する入力ルータ ACL だけがサポートされます。
- 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 ACL が適用されており、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）を追加しようとした場合、スイッチは ACL への ACE の追加を拒否します。

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 IP サービス フィーチャ セットを実行している必要があります。IP サービス フィーチャ セットまたは IP ベース フィーチャ セットを実行しているスイッチは、IPv6 管理トラフィックの入力ルータ IPv6 ACL だけをサポートしています。

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）ように設定します。

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

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 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、パケットはルーティングされません。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 によって廃棄される場合、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、ACL が設定された追加のパケットは CPU に転送され、ACL が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*	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。

	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**] [**routing**] [**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。 • *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**、または **udp**、あるいは 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。 **（注）** 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）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。 • *source-ipv6-prefix/prefix-length* または *destination-ipv6-prefix/ prefix-length* は、コロン間で 16 ビット値を使用して 16 進数で指定された deny または permit 条件を設定するネットワークの発信元 / 宛先 IPv6 ネットワークまたはクラスです（RFC 2373 を参照してください）。 • IPv6 プレフィクス ::/0 の省略形として、**any** を使用できます。 • **host** *source-ipv6-address* または *destination-ipv6-address* には、コロン間に 16 ビット値を使用して 16 進数で指定された deny または permit 条件を設定する発信元 / 宛先 IPv6 ホストアドレスを入力します。 • （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。オペランドは、**lt**（less than：未満）、**gt**（greater than：より大きい）、**eq**（equal：一致）、**neq**（not equal：不一致）、**range** です。 *source-ipv6-prefix/prefix-length* 引数の後ろに演算子が置かれた場合、送信元ポートと一致する必要があります。 *destination-ipv6-prefix/prefix-length* 引数の後ろに演算子が置かれた場合、宛先ポートと一致する必要があります。 • （任意）*port-number* に 10 進数（0 ～ 65535）として入力するか、TCP または UDP ポート名を入力します。TCP ポート名は TCP をフィルタリングする場合にだけ使用できます。UDP ポート名は UDP をフィルタリングする場合にだけ使用できます。 • （任意）**dscp** *value* を入力して、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 Services Code Point 値を照合します。指定できる範囲は 0 ～ 63 です。 • （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。このキーワードが表示されるのは、プロトコルが **ipv6** の場合だけです。 • （任意）エントリと一致するパケットに関するログ 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。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。ロギングはルータ ACL だけでサポートされます。 • （任意）IPv6 パケットがルーティングされるように指定するには、**routing** を入力します。 • （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）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。

	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**] [**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。 伝送制御プロトコルの場合は **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、他にも次の任意のパラメータを使用できます。 • **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*}：指定されたポート番号以外のポート上の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*}] [**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*]] 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 では、flag および **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**] [**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。 • *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。指定できる範囲は 0 ～ 255 です。 • *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。指定できる範囲は 0 ～ 255 です。 • *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**	特権 EXEC モードに戻ります。

	コマンド	目的
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。

指定したアクセス リストから拒否条件または許可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。リストの最初の拒否エントリにより、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 番目の拒否エントリにより、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、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 番目の許可エントリにより、その他のすべてのトラフィックが許可されます。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ので、この 2 番目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。スイッチが IP サービス フィーチャ セットを実行している場合、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。スイッチが IP サービス フィーチャ セットまたは IP ベース フィーチャ セットを実行している場合、ACL をレイヤ 3 インターフェイスの着信管理トラフィックだけ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、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、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。 **（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。 **（注）** **out** キーワードはレイヤ 2 インターフェイス（ポート ACL）ではサポートされません。スイッチで IP サービスまたは IP ベース フィーチャ セットが稼動している場合、レイヤ 3 インターフェイスで **out** キーワードはサポートされません。

	コマンド	目的
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、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 36-2 に記載のいずれかまたは両方の特権 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 36-2　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	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*]	設定済みのすべての 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** 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 入力および出力アクセス 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
```