CHAPTER 39

IPv6 ACL の設定

Cisco ME 3400E イーサネット アクセス スイッチがメトロ IP アクセス イメージを実行している場合、ACL と呼ばれる IP Version 4（IPv4）を作成して適用する場合と同じ方法で、IPv6 Access Control List（ACL; アクセス コントロール リスト）を作成し、それらをインターフェイスに適用して、IP Version 6（IPv6）トラフィックをフィルタリングできます。また、入力ルータ ACL を作成して適用することで、レイヤ 3 管理トラフィックをフィルタできます。

（注） IPv6 を使用するには、スイッチにデュアル IPv4 および IPv6 Switch Database Management（SDM; スイッチ データベース管理）テンプレートを設定しておく必要があります。**sdm prefer dual-ipv4-and-ipv6** {**default** | **routing** | **vlan**} グローバル コンフィギュレーション コマンドを入力し、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 7 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 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。
- スイッチの ACL 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。

（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。

この章の内容は次のとおりです。

IPv6 ACL の概要

メトロ IP アクセス イメージを実行しているスイッチは、次の 2 種類の 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でサポートされています。これらはルーテッド 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 です。IPv6 ルータ ACL は、ルーテッド IPv6 パケットにだけ適用されます。
- IPv6 ポート ACL は、レイヤ 2 インターフェイスの受信トラフィックでだけサポートされています。IPv6 ポート ACL はインターフェイスに入るすべての IPv6 パケットに適用されます。

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

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、設定は無効となります。

（注）　スイッチでの IPv4 ACL の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。

IPv4 および IPv6 ACL の両方をインターフェイスに適用できます。

IPv4 ACL と同様に、IPv6 ポート ACL は、ルータ ACL より優先されます。

- 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。他のポートで受信したルーティング IP パケットには、ルータ ACL のフィルタが適用されます。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、パケットはポート ACL によってフィルタリングされます。発信するルーティング IPv6 パケットには、ルータ ACL のフィルタが適用されます。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 が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 の特性の一部について説明します。

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

サポートされている ACL の機能

スイッチの IPv6 ACL には次の 3 つの特性があります。

- 分割されたフレーム（IPv4 の **fragments** キーワード）はサポートされていません。
- IPv4 でサポートされている統計情報は IPv6 ACL でサポートされます。
- スイッチでハードウェアの領域が不足している場合、ACL に関連付けられているパケットは 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 オプションによるルーテッド パケットまたはブリッジド パケットでは、IPv6 ACL はソフトウェアで適用されます。

- ロギングは ACL に対してサポートされていますがポート ACL に対してはサポートされていません。
- スイッチでは、全 prefix-length 範囲の IPv6 アドレス照合をサポートしています。

IPv6 ACL の制限事項

IPv4 では、標準番号および拡張番号付き IP ACL、名前付き IP ACL、および MAC ACL を設定できます。IPv6 では、名前付き ACL だけがサポートされています。

スイッチでは、Cisco IOS がサポートする多くの IPv6 ACL がサポートされていますが、次の例外があります。

- スイッチでは、**flowlabel**、**routing header**、および **undetermined-transport** の各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 はサポートされていません。また VLAN ACL（VLAN マップ）はサポートされていません。
- スイッチは、IPv6 フレームに MAC ベース ACL を適用しません。
- IPv6 ポート ACL をレイヤ 2 EtherChannel に適用できません。
- スイッチは、出力ポート ACL をサポートしていません。
- ACL を設定する場合、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、ACL に入力するキーワードに制限はありません。ACL をハードウェア転送（物理ポートまたは SVI）が必要なインターフェイスに適用する場合、スイッチは ACL がインターフェイスでサポートできるかどうかを確認します。サポートされない場合、ACL 付加は拒否されます。
- 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 Access Control Entry（ACE; アクセス制御エントリ）を追加する場合、スイッチは付加 ACL への ACE 追加を許可しません。

IPv6 ACL の設定

IPv6 ACL を設定する前に、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）または許可（permit）するよう、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 には、ACL が適用される レイヤ 3 インターフェイスに IPv6 アドレスを設定する必要もあります。

IPv6 ACL のデフォルト設定

IPv6 ACL は設定も適用もされません。

他の機能およびスイッチとの相互作用

IPv6 ACL を設定すると、他の機能またはスイッチの特性に関して次のような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、フレームに対して ICMP の Unreachable メッセージが生成されます。
- ポート ACL によりブリッジド フレームがドロップされると、フレームはブリッジされません。
- スイッチで IPv4 および IPv6 ACL を作成でき、IPv4 および IPv6 ACL を同じインターフェイスに適用できます。それぞれの ACL には一意な名前を指定する必要があります。すでに設定されている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 および IPv6 ACL を作成し、IPv4 または IPv6 ACL を同じレイヤ 2 またはレイヤ 3 インターフェイスに付加する場合は、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（IPv4 コマンドを使用して IPv6 ACL に付加など）すると、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使用できません。MAC ACL がフィルタリングできるのは、非 IP フレームだけです。
- ハードウェア メモリが満杯の場合、追加で設定された ACL については、パケットが 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** を入力して、条件が一致する場合にパケットを拒否するか許可するかを指定します。次に、条件を示します。 • *protocol* に、インターネット プロトコルの名前または番号 **ahp**、**esp**、**icmp**、**ipv6**、**pcp**、**stcp**、**tcp**、または **udp**、または IPv6 プロトコルの番号を示す整数 0 ～ 255 を入力します。 （注）　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。 • *source-ipv6-prefix*/*prefix-length* または *destination-ipv6-prefix*/*prefix-length* は、deny または permit 条件を設定するネットワークの送信元または宛先 IPv6 ネットワークまたはクラスで、16 進数で 16 ビットの値を指定し、コロンで囲んで指定します。 • IPv6 プレフィックス ::/0 の省略形として **any** と入力します。 • **host** *source-ipv6-address* または *destination-ipv6-address* には、deny または permit 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、16 進数で 16 ビットの値を指定し、コロンで囲んで指定します。 • （任意）*operator* には、指定し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* は 0 ～ 65535 の 10 進数または TCP または UDP ポートの名前です。TCP をフィルタリングする場合にだけ TCP ポート名を使用できます。UDP をフィルタリングする場合にだけ UDP ポート名を使用できます。 • （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 DiffServ コード ポイント（DSCP）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、初期状態でないフラグメントをチェックします。プロトコルが **ipv6** である場合にだけ、このキーワードが表示されます。 • （任意）**log** を入力して、エントリに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します。**log-input** を入力して、ログ エントリに入力インターフェイスを含めるようにします。ロギングは、ルータ ACL にだけサポートされています。 • （任意）**routing** を入力して、ルーティングされる IPv6 パケットを指定します。 • （任意）**sequence** *value* を入力して、アクセス リスト文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、許可または拒否文に適用する時間範囲を指定します。

	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**] [**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。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が、次に示すパラメータが追加されています。 • **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**：終了したビット設定。送信者からのデータはありません。 • **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*}：指定のポート番号の範囲内にある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。 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 の場合、パラメータ **established** 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。 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。 • *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。 • *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使用して、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を確認するには、「?」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。

no {**deny** | **permit**} IPv6 アクセス リスト コンフィギュレーション コマンドとキーワードを使用して、拒否または許可条件を指定のアクセス リストから削除します。

次の例では、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は、5000 より大きい宛先 TCP ポート番号を持ったすべてのパケットを拒否します。2 番目の拒否エントリは、5000 未満の送信元 UDP ポート番号を持った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 番目の許可エントリは、他の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。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）またはレイヤ 3 インターフェイス（ルータ ACLS）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（ルータ ACL）に IPv6 アドレスを設定します。 **（注）** このコマンドは、レイヤ 2 インターフェイス、またはインターフェイスに IPv6 アドレスが明示的に設定されている場合は必要ありません。
ステップ 5	**ipv6 traffic-filter** *access-list-name* {**in** | **out**}	アクセス リストをインターフェイスの受信または発信トラフィックに適用します。 **（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。

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、アクセス リストをインターフェイスから削除します。

次の例では、アクセス リスト *Cisco* をレイヤ 3 インターフェイス上の発信トラフィックに適用する方法を示します。

```
Switch(config)# interface gigabitethernet 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 39-1 の 1 つまたは複数の特権 EXEC コマンドを使用して、設定されているすべてのアクセス 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ためのコマンド

コマンド	目的
show access-lists	スイッチで設定され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*]	設定されたすべての 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。出力には、スイッチまたはスイッチ スタックに設定されている 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
```