IPv6 アクセス コントロール リストの設定

IPv6 ACL の制限

IPv4 では、番号制の標準 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。

- スイッチは、**routing header**、および **undetermined-transport** というキーワードの照合をサポートしません。
- スイッチは、再帰 ACL（**reflect** キーワード）をサポートしません。
- このリリースは、IPv6 のルータ ACL および VLAN ACL（VLAN マップ）をサポートしています。
- スイッチは、IPv6 フレームに MAC ベース ACL を適用しません。
- 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）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アクセス コントロールエントリ（ACE）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適用されている ACL に ACE が追加されるのを許可しません。

スイッチの IPv6 ACL には、次の特性があります。

- 分割フレーム（IPv6 では **fragments** キーワード）がサポートされません。
- 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スペースが不足している場合、ACLに関連付けられたパケットはCPU で処理され、ACL はソフトウェアで適用されます。
- スイッチは、プレフィックス長の最大範囲の IPv6 アドレス一致をサポートしません。

IPv6 ACL の設定に関する情報

アクセス リストによって、デバイス インターフェイスでブロックされるトラフィックおよび転送されるトラフィックが決定され、送信元アドレスと宛先アドレスに基づくトラフィックのフィルタリング、および特定のインターフェイスへの着信および発信トラフィックのフィルタリングを行うことができます。標準のIPv6 ACL機能が拡張されて、IPv6オプションヘッダー、および任意でより細かい制御を行うための上位層プロトコルタイプ情報に基づくトラフィックフィルタリングがサポートされています。標準の IPv6 ACL 機能が拡張されて、IPv6 オプション ヘッダー、および任意でより細かい制御を行うための上位層プロトコル タイプ情報に基づくトラフィック フィルタリングがサポートされています。

このモジュールは、仮想端末回線へのアクセスを制御する IPv6 トラフィック フィルタリングの設定方法について説明します。

ACL の概要

パケット フィルタリングは、ネットワーク トラフィックを限定し、特定のユーザまたはデバイスによるネットワークの使用を制限するうえで役立ちます。ACLはルータまたはスイッチを通過するトラフィックをフィルタリングし、特定のインターフェイスまたは VLAN（仮想 LAN）でパケットを許可、または拒否します。ACL は、パケットに適用される許可条件および拒否条件の順序付けられた集まりです。パケットがインターフェイスに着信すると、スイッチはパケット内のフィールドを適用される ACL と比較し、アクセス リストに指定された基準に基づいて、パケットが転送に必要な権限を持っているかどうかを確認します。アクセスリスト内の条件を1つずつ調べ、パケットをテストします。最初に一致した条件によって、スイッチがパケットを受け入れるか拒否するかが決定されます。スイッチは最初に一致した時点でテストを中止するので、リストに条件を指定する順序が重要です。一致する条件がない場合、スイッチはパケットを拒否します。スイッチは、制限条件がない場合はパケットを転送し、制限条件がある場合はパケットをドロップします。スイッチは、VLAN内でブリッジングされるパケットを含めて、転送されるすべてのパケットに ACL を使用します。

ネットワークに基本的なセキュリティを導入する場合は、ルータにアクセスリストを設定します。ACLを設定しなければ、スイッチを通過するすべてのパケットがネットワークのあらゆる部分で許可される可能性があります。ACLを使用すると、ネットワークの場所ごとにアクセス可能なホストを制御したり、ルータインターフェイスで転送またはブロックされるトラフィックの種類を決定したりできます。たとえば、電子メール トラフィックの転送を許可し、Telnet

トラフィックの転送を拒否することもできます。ACL を着信トラフィック、発信トラフィック、またはその両方をブロックするように設定することもできます。

IPv6 ACL の概要

IP Version 6（IPv6）アクセス コントロール リスト（ACL）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。

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。

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

他の機能およびスイッチとの相互作用

- 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 つのスイッチに作成したり、同一の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（例えば、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 に関連付けられたパケットは CPU に向けて処理され、ACL はソフトウェアで適用されます。

IPv6 ACL のデフォルト設定

デフォルトの IPv6 ACL 設定は次のとおりです。

```
Device# show access-lists preauth_ipv6_acl
IPv6 access list preauth_ipv6_acl (per-user)
permit udp any any eq domain sequence 10
permit tcp any any eq domain sequence 20
permit icmp any any nd-ns sequence 30
permit icmp any any nd-na sequence 40
permit icmp any any router-solicitation sequence 50
permit icmp any any router-advertisement sequence 60
permit icmp any any redirect sequence 70
permit udp any eq 547 any eq 546 sequence 80
permit udp any eq 546 any eq 547 sequence 90
deny ipv6 any any sequence 100
```

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。

IPv6 ポートベースのアクセス コントロール リスト サポート

IPv6 PACL 機能は、IPv6 トラフィック用のレイヤ 2 スイッチ ポートでアクセス コントロール（許可または拒否）を提供する機能を備えています。IPv6 PACL は、IPv4 トラフィック用のレイヤ 2 スイッチ ポートでアクセス コントロールを提供する IPv4 PACL と似ています。これらは、入力方向とハードウェアだけでサポートされます。

ACL およびトラフィック転送

ホップ バイ ホップ フィルタリングに対応するための IPv6 ACL の拡張機能により、ホップ バイ ホップ拡張ヘッダーを含む可能性がある IPv6 トラフィックを制御することができます。アクセス コントロール リスト（ACL）を設定して、すべてのホップ バイ ホップ トラフィックを拒否するか、またはプロトコルに基づいて選択的にトラフィックを許可することができます。

IPv6 アクセス コントロール リスト（ACL）は、デバイス インターフェイスでブロックされるトラフィックと転送されるトラフィックを決定します。ACL を使用すると、特定のインターフェイスへの着信および発信を、送信元アドレスと宛先アドレスに基づいてフィルタリングできます。**ipv6 access-list** コマンドを使用して IPv6 ACL を定義し、**deny** および **permit** コマンドを使用してその条件を構成します。

ホップ バイ ホップ フィルタリングに対応するための IPv6 ACL の拡張機能は、上位層プロトコル タイプでのトラフィック フィルタリングをサポートするために RFC 2460 を実装します。

IPv6 ACL の設定方法

この項では、IPv6 ACL の設定方法について説明します。

IPv6 ACL の設定

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。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# 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 3	{ **ipv6 access-list** *list-name* 例： `Device(config)# ipv6 access-list example_acl_list`	IPv6 ACL 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。
ステップ 4	{**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場合は deny、許可する場合は permit 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。 • *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、コロン区切りの 16 ビット値を使用した 16 進形式で指定します（RFC 2373 を参照）。 • IPv6 プレフィックス ::/0 の短縮形として、any を入力します。 • **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

	コマンドまたはアクション	目的
		信元または宛先 IPv6 ホスト アドレスを入力します。アドレスはコロン区切りの 16 ビット値を使用した 16 進形式で指定します。 • （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。オペランドには、**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）があります。 *source-ipv6-prefix/prefix-length* 引数のあとの operator 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 operator は、宛先ポートに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 あるいは UDP ポートの名前です。TCP ポート名を使用できるのは、TCP のフィルタリング時だけです。UDP ポート名を使用できるのは、UDP のフィルタリング時だけです。 • （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。 • （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。 • （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グ メッセージがコンソールに送信

	コマンドまたはアクション	目的
		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。 • （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 ～ 4,294,967,295 です。 • （任意）**time-range** name を入力して、deny または permit ステートメントに適用される時間の範囲を指定します。
ステップ 5	{**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*] [**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。 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。 • **ack**：確認応答ビット セット • **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。 • **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。 • **psh**：プッシュ機能ビット セット • **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。 • **rst**：リセット ビット セット • **syn**：同期ビット セット • **urg**：緊急ポインタ ビット セット
ステップ 6	{**deny** | **permit**} **udp** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address*} [operator	（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。

	コマンドまたはアクション	目的
	[*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*]]	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の説明にあるパラメータと同じです。ただし、[operator [*port*]] ポートの番号または名前は、UDPポートの番号または名前でなければなりません。
ステップ **7**	{**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 1 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 タイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。 • *icmp-code*：ICMP パケットを ICMP メッセージコードタイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。 • *icmp-message*：ICMP パケットを ICMP メッセージ タイプ名または ICMP メッセージ タイプとコード名でフィルタリングする場合に入力します。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 **8**	**end**	特権 EXEC モードに戻ります。
ステップ **9**	**show ipv6 access-list**	アクセスリストの設定を確認します。

	コマンドまたはアクション	目的
ステップ 10	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 11	**copy running-config startup-config** 例： `Device# 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。

次のタスク

インターフェイスに IPv6 ACL をアタッチします。

IPv6 ACL のモニタリング

次の表に示された 1 つまたは複数の特権 EXEC コマンドを使用して、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。

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。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。

```
Device# 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。

```
Device# 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
```

インターフェイスでの PACL モードの設定および IPv6 PACL の適用

始める前に

IPv6 PACL 機能を設定する前に、IPv6 アクセス リストを設定する必要があります。IPv6 アクセス リストを設定した後、指定された IPv6 レイヤ 2 インターフェイスでポートベース アクセス コントロール リスト（PACL）モードを設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# 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 3	**ipv6 access-list** *access-list-name* 例： `Device(config)# ipv6 access-list list1`	IPv6 ACL 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 4	**exit** 例： `Device(config-ipv6-acl)# exit`	IPv6 アクセス リスト コンフィギュレーション モードを終了し、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 5	**interface** *type number* 例： `Device(config)# interface gigabitethernet 1/0/1`	インターフェイスのタイプと番号を指定し、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 6	**ipv6 traffic-filter** *access-list-name* **in** 例： `Device(config-if)# ipv6 traffic-filter list1 in`	インターフェイス上の着信 IPv6 トラフィックをフィルタリングします。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ホップ バイ ホップ フィルタリングに対応するための IPv6 ACL の拡張の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**ipv6 access-list** *access-list-name* 例： `Device(config)# ipv6 access-list hbh-acl`	IPv6 ACL 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 4	**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*] [**hbh**] [**log**] [**log-input**] [**reflect** *name* [**timeout** *value*]] [**sequence** *value*] [**time-range** *name*] 例： `Device(config-ipv6-acl)# permit icmp any any`	IPv6 ACL の許可条件を設定します。
ステップ 5	**deny** *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*] [**hbh**] [**log**]	IPv6 ACL の拒否条件を設定します。

	コマンドまたはアクション	目的
	[**log-input**] [**sequence** *value*] [**time-range** *name*] 例： `Device(config-ipv6-acl)# deny icmp any any`	
ステップ 6	**end** 例： `Device (config-ipv6-acl)# end`	特権EXECコンフィギュレーションモードに戻ります。

IPv6 ACL の設定例

この項では、IPv6 ACL の設定例を示します。

例：IPv6 ACL の設定

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、この2番めの拒否エントリは、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。

```
Device(config)# ipv6 access-list CISCO
Device(config-ipv6-acl)# deny tcp any any gt 5000
Device(config-ipv6-acl)# deny ::/0 lt 5000 ::/0 log
Device(config-ipv6-acl)# permit icmp any any
Device(config-ipv6-acl)# permit any any
```

例：インターフェイスでの PACL モードの設定および IPv6 PACL の適用

```
Device# configure terminal
Device(config)# ipv6 access-list list1
Device(config-ipv6-acl)# exit
Device(config-if)# ipv6 traffic-filter list1 in
```

例：ホップ バイ ホップ フィルタリングに対応するための IPv6 ACL の拡張

```
Device(config)# ipv6 access-list hbh_acl
```

```
Device(config-ipv6-acl)# permit tcp any any hbh
Device(config-ipv6-acl)# permit tcp any any
Device(config-ipv6-acl)# permit udp any any
Device(config-ipv6-acl)# permit udp any any hbh
Device(config-ipv6-acl)# permit hbh any any
Device(config-ipv6-acl)# permit any any
Device(config-ipv6-acl)# exit

! Assign an IP address and add the ACL on the interface.

Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# ipv6 address 1001::1/64
Device(config-if)# ipv6 traffic-filter hbh_acl in
Device(config-if)# exit
Device(config)# exit
Device# clear counters
Clear "show interface" counters on all interfaces [confirm]
Device#

! Verify the configurations.

Device# show running-config interface gigabitethernet 1/0/1

Building configuration...

Current configuration : 114 bytes
!
interface gigabitethernet 1/0/1
no switchport
ipv6 address 1001::1/64
ipv6 traffic-filter hbh_acl
end
```

IPv6 アクセスコントロールリストに関する追加情報

関連資料

関連項目	マニュアル タイトル
この章で使用するコマンドの完全な構文および使用方法の詳細。	*Consolidated Platform Command Reference, Cisco IOS Release 15.2(7)Ex (Catalyst Micro Switches)*
ACL	詳細については、以下を参照してください。 • 『Security Configuration Guide』の「Access Control Lists Overview」 • 『Security Configuration Guide』の「Configuring IPv4 Access Control Lists」

IPv6 アクセスコントロールリストの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS Release 15.2(7)E3k	IPv6 アクセス コントロール リスト	IPv6 ACL を作成して、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、IPv4 の名前付き ACL を作成し、適用する方法と類似しています。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。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn [英語] からアクセスします。