IPv6 ACL の設定

IPv6 ACL の設定の前提条件

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。また、スイッチが Network Essentials ライセンスで稼働している場合、入力ルータ ACL を作成し、それを適用してレイヤ 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。

IPv6 ACL の設定の制約事項

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。

device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。

- deviceは、**flowlabel**、**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。

- deviceは再帰 ACL（**reflect** キーワード）をサポートしません。
- device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（物理ポートまたは SVI）に ACL を適用する場合、deviceはインターフェイスで ACL がサポートされるかどうかを判別します。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、deviceは現在インターフェイスに適用されている ACL に ACE が追加されることを許可しません。

IPv6 ACL について

アクセス コントロール リスト（ACL）とは、特定のインターフェイスへのアクセスを制限するために使用されるルール セットのことです。ACLは device に設定され、管理インターフェイスおよび任意の動的インターフェイスに適用されます。

Web 認証用に事前認証 ACL を作成することもできます。このような ACL は、認証が完了するまでに特定のタイプのトラフィックを許可するために使用されます。

IPv6 ACL は、送信元、宛先、送信元ポート、宛先ポートなど、IPv4 ACL と同じオプションをサポートします。

（注） ネットワーク内で IPv4 トラフィックだけを有効にするには、IPv6 トラフィックをブロックします。つまり、すべての IPv6 トラフィックを拒否するように IPv6 ACL を設定し、これを特定またはすべての WLAN 上で適用します。

IPv6 ACL の概要

スイッチは、次の 2 種類の IPv6 ACL をサポートします。

- IPv6 ルータ ACL は、ルーテッド ポート、スイッチ仮想インターフェイス（SVI）、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アウトバウンド トラフィックまたはインバウンド 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インバウンド トラフィックでだけサポートされます。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。

Network Essentials ライセンスで稼働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 または出力ルータ IPv6 ACL はサポートされません。

（注） サポートされない IPv6 ACL を設定した場合、エラー メッセージが表示され、その設定は有効になりません。

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。

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。

ACL のタイプ

ユーザーあたりの IPv6 ACL

ユーザあたりの ACL の場合、テキスト文字列として、完全アクセス制御エントリ（ACE）が ACS で設定されます。

フィルタ ID IPv6 ACL

filter-Id ACL の場合、完全な ACE および `acl name(filter-id)` がdeviceで設定され、`filter-id` のみが ACS で設定されます。

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 を完全に機能させるには、すべてのスタック メンバで Network Advantage ライセンス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 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との同期をとり、不要なエントリを一掃します。

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 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。

始める前に

IPv6 ACL を設定する場合は、事前にデュアル 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。

手順の概要

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。
2. IPv6 ACL が、トラフィックをブロックする（deny）または通過させる（permit）よう設定します。
3. トラフィックをフィルタリングする必要があるインターフェイスに IPv6 ACL を適用します。
4. 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。

手順の詳細

	コマンドまたはアクション	目的
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（deny）または通過させる（permit）よう設定します。	
ステップ 3	トラフィックをフィルタリングする必要があるインターフェイスに IPv6 ACL を適用します。	
ステップ 4	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	

	コマンドまたはアクション	目的
	フェイスにも IPv6 アドレスを設定する必要があります。	

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。

他の機能およびスイッチとの相互作用

- 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インターネット制御メッセージ プロトコル（ICMP）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（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、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。ハードウェアが一杯になると、ACL がアンロードされたことを示すメッセージがコンソールに出力され、パケットはインターフェイスでドロップされます。

IPv6 ACL の設定方法

IPv6 ACL の作成

IPv6 ACL を作成するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**

3. **ipv6 access-list** *acl_name*
4. **{deny|permit} protocol**
5. **{deny|permit} tcp**
6. **{deny|permit} udp**
7. **{deny|permit} icmp**
8. **end**
9. **show ipv6 access-list**
10. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **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： デバイス# **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** *acl_name* 例： デバイス# **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 4	**{deny|permit} protocol** 例： `{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]`	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。

	コマンドまたはアクション	目的
		• 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。

	コマンドまたはアクション	目的
		• （任意）routing を入力して、IPv6 パケットのルーティングを指定します。 • （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 ～ 4294967295 です。 • （任意）time-range name を入力して、拒否または許可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** 例： `{deny | permit} tcp {source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length | any |hostdestination-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。パラメータはステップ 3 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（ACK）ビット セット • 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** 例： `{deny | permit} udp {source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length`	（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、

	コマンドまたはアクション	目的
		[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 7	**{deny|permit} icmp** 例： `{deny | permit} icmp {source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length | any | hostdestination-ipv6-address} [operator [port-number]][icmp-type [icmp-code] |icmp-message] [dscpvalue] [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 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** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 9	**show ipv6 access-list** 例： `show ipv6 access-list`	アクセス リストの設定を確認します。
ステップ 10	**copy running-config startup-config** 例： `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。

インターフェイスへの IPv6 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。レイヤ 2 およびレイヤ 3 インターフェイスの発信または着信トラフィックに IPv6 ACL を適用できます。IPv6 ACL はレイヤ 3 インターフェイスの着信管理トラフィックにだけ適用できます。

インターフェイスへのアクセスを制御するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *interface_id*
4. **no switchport**
5. **ipv6 address** *ipv6_address*
6. **ipv6 traffic-filter** *acl_name*
7. **end**
8. **show running-config interface tenGigabitEthernet 1/0/3**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `デバイス> 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： `デバイス# 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	**interface** *interface_id* 例： `デバイス# 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 スイッチ仮想インターフェイス（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。
ステップ 4	**no switchport** 例： `デバイス# no switchport`	レイヤ 2 モード（デフォルト）からレイヤ 3 モードにインターフェイスを変更します（ルータ ACL を適用する場合のみ）。

	コマンドまたはアクション	目的
ステップ 5	**ipv6 address** *ipv6_address* 例： デバイス# **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。 （注） 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 6	**ipv6 traffic-filter** *acl_name* 例： デバイス# **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。
ステップ 7	**end** 例： Device(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 8	**show running-config interface tenGigabitEthernet 1/0/3** 例： デバイス# show running-config interface tenGigabitEthernet 1/0/3 .... Building configuration .... Current configuration : 98 bytes ! interface TenGigabitEthernet1/0/3 switchport mode trunk ipv6 traffic-filter MyFilter out end	設定の概要を示します。
ステップ 9	**copy running-config startup-config** 例： 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。

IPv6 ACL の確認

IPv6 ACL の表示

IPv6 ACL を表示するには、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： デバイス> **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： デバイス# **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	**show access-list** 例： デバイス# **show access-lists**	deviceに設定されたすべてのアクセス リストを表示します。
ステップ 4	**show ipv6 access-list** *acl_name* 例： デバイス# **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。

RA ガード ポリシーの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 nd raguard policy** *policy name*
4. **trusted-port**
5. **device-role router**
6. **interface** *interface-id*
7. **ipv6 nd raguard attach-policy** *policy name*
8. **vlan** *vlan-id*
9. **ipv6 nd suppress**
10. **ipv6 snooping**
11. **ipv6 nd raguard attach-policy** *policy name*
12. **ipv6 nd ra-throttler attach-policy** *policy name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **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： デバイス# **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 nd raguard policy** *policy name* 例： デバイス(config)# **ipv6 nd raguard policy MyPolicy**	
ステップ 4	**trusted-port** 例： デバイス(config-nd-raguard)# **trusted-port**	上記で作成したポリシーの信頼できるポートを設定します。
ステップ 5	**device-role router** 例： デバイス(config-nd-raguard)# **device-role [host|monitor|router|switch]** デバイス(config-nd-raguard)# **device-role router** d	上記で作成した信頼できるポートにRA を送信可能な信頼できるデバイスを定義します。
ステップ 6	**interface** *interface-id* 例： デバイス(config)# **interface tenGigabitEthernet 1/0/1**	信頼できるデバイスにインターフェイスを設定します。
ステップ 7	**ipv6 nd raguard attach-policy** *policy name* 例： デバイス(config-if)# **ipv6 nd raguard attach-policy Mypolicy**	ポートから受信したRA を信頼するようにポリシーを設定し、接続します。
ステップ 8	**vlan** *vlan-id* 例： デバイス(config)# **vlan configuration 19-21,23**	ワイヤレス クライアントの vlan を設定します。
ステップ 9	**ipv6 nd suppress** 例： デバイス(config-vlan-config)# **ipv6 nd suppress**	無線上で ND メッセージを抑制します。

	コマンドまたはアクション	目的
ステップ 10	**ipv6 snooping** 例： デバイス(config-vlan-config)# **ipv6 snooping**	IPv6 トラフィックをキャプチャします。
ステップ 11	**ipv6 nd raguard attach-policy** *policy name* 例： デバイス(config-vlan-config)# **ipv6 nd raguard attach-policy Mypolicy**	ワイヤレス クライアントの vlan に RA ガード ポリシーを接続します。
ステップ 12	**ipv6 nd ra-throttler attach-policy** *policy name* 例： デバイス(config-vlan-config)# **ipv6 nd ra-throttler attach-policy Mythrottle**	ワイヤレス クライアントの vlan に RA スロットリング ポリシーを接続します。

IPv6 ネイバー バインディングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 neighbor binding** [vlan] **19 2001:db8::25:4 interface tenGigabitEthernet 1/0/3 aaa.bbb.ccc**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： デバイス> **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： デバイス# **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 neighbor binding** [vlan] **19 2001:db8::25:4 interface tenGigabitEthernet 1/0/3 aaa.bbb.ccc** 例：	送信元 MAC アドレスとして aaa.bbb.ccc が設定されたインターフェイス te1/0/3 を介して VLAN 19 で送信する場合にのみ有効なネイバー 2001:db8::25: 4 を設定して検証します。

	コマンドまたはアクション	目的
	デバイス(config)# **ipv6 neighbor binding vlan 19 2001:db8::25:4 interface tenGigabitEthernet 1/0/3 aaa.bbb.ccc**	

IPv6 ACL の設定例

例：IPv6 ACL の作成

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。

（注） ロギングは、レイヤ 3 インターフェイスでのみサポートされます。

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

例：IPv6 ACL の適用

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。

```
デバイス(config)# interface TenGigabitEthernet 1/0/3

デバイス(config-if)# no switchport
デバイス(config-if)# ipv6 address 2001::/64 eui-64
デバイス(config-if)# ipv6 traffic-filter CISCO out
```

例：IPv6 ACL の表示

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。

```
デバイス #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 アクセス リストだけが表示されます。

```
デバイス# 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
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

IPv6 ACL の機能情報

次の表に、このモジュールで説明した機能をリストし、個別の設定情報へのリンクを示します。

機能	リリース	変更内容
IPv6 ACL 機能	Cisco IOS XE Everest 16.5.1a	この機能が導入されました。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。