



IPv6 ACL

- [IPv6 ACL について \(1 ページ\)](#)
- [IPv6 ACL の設定の前提条件 \(2 ページ\)](#)
- [IPv6 ACL の設定の制約事項 \(3 ページ\)](#)
- [IPv6 ACL の設定 \(3 ページ\)](#)
- [IPv6 ACL の設定方法 \(4 ページ\)](#)
- [IPv6 ACL の確認 \(9 ページ\)](#)
- [IPv6 ACL の設定例 \(10 ページ\)](#)

IPv6 ACL について

アクセス コントロール リスト (ACL) 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一連のルールです (たとえば、無線クライアントからコントローラの管理インターフェイスに ping が実行されるのを制限する場合などに使用されます)。device で設定した ACL は、管理インターフェイス、AP マネージャインターフェイス、任意の動的インターフェイス、またはワイヤレスクライアントとやり取りするデータトラフィックの制御用の WLAN、あるいは中央処理装置 (CPU) 宛のすべてのトラフィックの制御用のコントローラ CPU に適用できます。

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

ACL のタイプ

ユーザーあたりの IPv6 ACL

ユーザーあたりの ACL の場合、テキスト文字列としての完全なアクセス コントロール エントリ (ACE) が Cisco Secure Access Control Server (Cisco Secure ACS) で設定されます。

ACE はコントローラ 組み込みワイヤレスコントローラで設定されません。ACE は ACCESS-Accept 属性で device に送信され、クライアント用に直接適用されます。ワイヤレスクライアントが外部 device にローミングするときに、ACE が、AAA 属性としてモビリティ ハンドオフ メッセージで外部 device に送信されます。ユーザーあたりの ACL を使用した出力方向はサポートされていません。

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 Cisco Secure ACS で設定されます。

`filter-id` は ACCESS-Accept 属性で device に送信され、device は ACE の `filter-id` をルックアップしてから、クライアントに ACE を適用します。クライアント L2 が外部 device にローミングするときに、`filter-id` だけがモビリティ ハンドオフ メッセージで外部 device に送信されます。ユーザーあたりの ACL を使用した出力フィルタ ACL はサポートされていません。外部 device は `filter-id` と ACE を事前に設定する必要があります。

ダウンロード可能 IPv6 ACL

ダウンロード可能 ACL (dACL) の場合、完全な ACE および `dacl` 名は Cisco Secure ACS のみで設定されます。

Cisco Secure ACS はその ACCESS-Accept 属性で `dacl` 名を device に送信します。デバイスは `dacl` 名を取得し、ACE のために `dACL` 名を ACCESS-request 属性を使用して Cisco Secure ACS に送り返します。

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 の設定

IPv6 トラフィックをフィルタリングするには、次の手順に従います。

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。

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

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。

	コマンドまたはアクション	目的
ステップ 3	ipv6 access-list <i>acl_name</i> 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 : <pre>{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]</pre>	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。 <ul style="list-style-type: none"> • 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。

	コマンドまたはアクション	目的
		<p>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。</p> <ul style="list-style-type: none"> • (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트리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。 • (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。

	コマンドまたはアクション	目的
		<ul style="list-style-type: none"> • (任意) <code>time-range name</code> 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	<p>{deny permit} tcp</p> <p>例 :</p> <pre>{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]</pre>	<p>(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。</p> <p>TCP の場合は <code>tcp</code> 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。</p> <ul style="list-style-type: none"> • <code>ack</code> : 確認応答 (ACK) ビットセット • <code>established</code> : 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。 • <code>fin</code> : 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。 • <code>neq {port protocol}</code> : 所定のポート番号上にないパケットだけを照合します。 • <code>psh</code> : プッシュ機能ビットセット • <code>range {port protocol}</code> : ポート番号の範囲内のパケットだけを照合します。 • <code>rst</code> : リセット ビットセット • <code>syn</code> : 同期ビットセット • <code>urg</code> : 緊急ポインタ ビットセット
ステップ 6	<p>{deny permit} udp</p> <p>例 :</p> <pre>{deny permit} udp {source-ipv6-prefix/prefix-length any hostsource-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length</pre>	<p>(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。</p> <p>ユーザデータグラムプロトコルの場合は、<code>udp</code> 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、<code>[operator</code></p>

	コマンドまたはアクション	目的
	<pre> any hostdestination-ipv6-address} [operator [port-number]][dscp value] [log][log-input] [neq {port protocol}] [range {port protocol}] [routing][sequence value][time-range name]</pre>	<p>[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はなければなりません。UDP の場合、established パラメータは無効です。</p>
ステップ 7	<p>{deny permit} icmp</p> <p>例 :</p> <pre>{deny permit} icmp {source-ipv6-prefix/prefix-length any hostsourc-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]</pre>	<p>(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。</p> <p>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。</p> <p>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。</p> <ul style="list-style-type: none"> • 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	<p>end</p> <p>例 :</p> <pre>Device(config)# end</pre>	<p>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。</p>
ステップ 9	<p>show ipv6 access-list</p> <p>例 :</p>	<p>アクセスリストの設定を確認します。</p>

	コマンドまたはアクション	目的
	<code>show ipv6 access-list</code>	
ステップ 10	copy running-config startup-config 例： <code>copy running-config startup-config</code>	(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。

WLAN IPv6 ACL の作成

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： <code>デバイス> enable</code>	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： <code>デバイス# configure terminal</code>	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： <code>デバイス# show access-lists</code>	<code>device</code> 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 <i>acl_name</i> 例： <code>デバイス# show ipv6 access-list [access-list-name]</code>	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。

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 番目の拒否エントリは、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 番目の許可エントリは、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 番目の許可エントリは必要です。



(注) ログイングは、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
```