IPv6 アクセス コントロール リスト

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。

RSP3 ポートの関連情報

IPv6 ACL は、RSP3 ではサポートされていません

IPv6 アクセス コントロール リストに関する情報

IPv6 トラフィック フィルタリングのアクセス コントロール リスト

IPv6 での標準 ACL 機能は、IPv4 での標準 ACL に似ています。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いて、特定のインターフェイスへの着信と発信をフィルタリングできます。各アクセス リストの末尾には、暗黙的な deny 文があります。IPv6

ACLを定義し、拒否条件と許可条件を設定するには、グローバルコンフィギュレーションモードで **deny** キーワードと **permit** キーワードを指定して **ipv6 access-list** コマンドを使用します。

IPv6 で拡張された ACL では標準 IPv6 ACL 機能を強化して、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（IPv4 における拡張 ACL に類似した機能です）。

IPv6 パケット インスペクション

ヘッダーフィールド（トラフィック クラス、フローラベル、ペイロード長、次ヘッダー、ホップ リミット、および送信元 IP アドレスや宛先 IP アドレス）は、IPv6 インスペクション用に使用されます。IPv6 ヘッダー フィールドの詳細および説明については、RFC 2474 を参照してください。

IPv6 でのアクセス クラス フィルタリング

IPv6 ACL に基づく、デバイスとの間の着信接続と発信接続のフィルタリングは、ライン コンフィギュレーション モードで **ipv6 access-class** コマンドを使用して実行します。**ipv6 access-class** コマンドは、IPv6 ACL が名前で定義される点を除き、**access-class** コマンドに似ています。IPv6 ACL が着信トラフィックに適用される場合、ACL 内の送信元アドレスは、着信接続の送信元アドレスと照合され、ACL 内の宛先アドレスは、インターフェイス上のローカル デバイス アドレスと照合されます。IPv6 ACL が発信トラフィックに適用される場合、ACL 内の送信元アドレスは、インターフェイス上のローカル デバイス アドレスと照合され、ACL 内の宛先アドレスは、発信接続の送信元アドレスと照合されます。ユーザーが任意の接続を試行できるように、すべての仮想端末回線で同じ制限を設定することを推奨します。

IPv6 アクセス コントロール リストの設定方法

IPv6 トラフィック フィルタリングの設定

トラフィック フィルタリング用の IPv6 ACL の作成および設定

（注） Cisco ASR 1000 プラットフォームの IPv6 ACL には、暗黙の許可ルールは含まれません。IPv6 ネイバー探索プロセスでは、IPv6 ネットワーク層サービスを使用します。したがって、IPv6 ネイバー探索をイネーブルにするには、IPv6 ネイバー探索パケットのインターフェイス上での送受信が許可されるように IPv6 ACL を追加する必要があります。IPv4 では、IPv6 ネイバー探索プロセスと同等のアドレス解決プロトコル（ARP）は、別のデータリンク層プロトコルを使用します。したがってデフォルトでは、IPv4 ACL により、ARP パケットのインターフェイス上での送受信が暗黙的に許可されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 access-list** *access-list-name*
4. 次のいずれかを実行します。
   - **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*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]
   - **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*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**

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： `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 inbound`	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。 • *access-listname* 引数は、IPv6 ACL の名前を指定します。IPv6 ACL の名前にスペースまたは引用符を含めることはできません。また、先頭を数字にすることはできません。
ステップ 4	次のいずれかを実行します。 • **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*]] [**dest-option-type** [*doh-number*	*doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number*	*mh-type*]] [**routing**]	IPv6 ACL の許可条件または拒否条件を指定します。

	コマンドまたはアクション	目的

	[**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]
	• **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*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**
	例：
	`Device(config-ipv6-acl)# permit tcp 2001:DB8:0300:0201::/32 eq telnet any`
	例：
	`Device(config-ipv6-acl)# deny tcp host 2001:DB8:1::1 any log-input`	

インターフェイスへの IPv6 ACL の適用

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 traffic-filter** *access-list-name* {**in**| **out**}

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： `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。

	コマンドまたはアクション	目的
ステップ 3	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0`	インターフェイスのタイプおよび番号を指定し、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 4	**ipv6 traffic-filter** *access-list-name* {**in**| **out**} 例： `Device(config-if)# ipv6 traffic-filter inbound in`	指定した IPv6 アクセス リストを、前のステップで指定したインターフェイスに適用します。

vty へのアクセスの制御

IPv6 ACL の作成によるアクセス クラス フィルタリングの提供

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 access-list** *access-list-name*
4. 次のいずれかを実行します。
   - **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*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*
   - **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*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**

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： `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。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 access-list** *access-list-name* 例： `Device(config)# ipv6 access-list cisco`	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	次のいずれかを実行します。
	• **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*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*
	• **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*]] [**dest-option-type** [*doh-number* | *doh-type*]] [**dscp** *value*] [**flow-label** *value*] [**fragments**] [**log**] [**log-input**] [**mobility**] [**mobility-type** [*mh-number* | *mh-type*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] [**undetermined-transport**
	例：
	`Device(config-ipv6-acl)# permit ipv6 host 2001:DB8:0:4::32 any`
	例：
	`Device(config-ipv6-acl)# deny ipv6 host 2001:DB8:0:6::6 any`
		IPv6 ACL の許可条件または拒否条件を指定します。

仮想端末回線への IPv6 ACL の適用

手順の概要

1. **enable**
2. **configure terminal**
3. **line** [**aux**| **console**| **tty**| **vty**] *line-number*[*ending-line-number*]
4. **ipv6 access-class** *ipv6-access-list-name* {**in**| **out**}

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： `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	**line** [**aux**| **console**| **tty**| **vty**] *line-number*[*ending-line-number*] 例： `Device(config)# line vty 0 4`	設定する特定の回線を識別し、ライン コンフィギュレーション モードを開始します。 • この例では、**vty** キーワードを使用して、リモート コンソール アクセス用の仮想端末回線を指定します。
ステップ 4	**ipv6 access-class** *ipv6-access-list-name* {**in**| **out**} 例： `Device(config-line)# ipv6 access-class cisco in`	IPv6 ACL に基づいて、デバイスとの間の着信接続と発信接続をフィルタリングします。

IPv6 アクセス コントロール リストの設定例

例：IPv6 ACL 設定の確認

次の例では、**show ipv6 access-list** コマンドを使用して、IPv6 ACL が正しく設定されていることを確認します。

```
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 Virtual-Access2.1#427819008151 (per-user)
    permit tcp host 2001:DB8:1::32 eq bgp host 2001:DB8:2::32 eq 11000 sequence 1
    permit tcp host 2001:DB8:1::32 eq telnet host 2001:DB8:2::32 eq 11001 sequence 2
```

例：IPv6 ACL の作成と適用

次に、HTTP アクセスを日中の特定の時間に制限し、許可されていない時間のアクティビティを記録する方法について例を示します。

```
Device# configure terminal
Device(config)# time-range lunchtime
Device(config-time-range)# periodic weekdays 12:00 to 13:00
Device(config-time-range)# exit
Device(config)# ipv6 access-list INBOUND
Device(config-ipv6-acl)# permit tcp any any eq www time-range lunchtime
Device(config-ipv6-acl)# deny tcp any any eq www log-input
Device(config-ipv6-acl)# permit tcp 2001:DB8::/32 any
Device(config-ipv6-acl)# permit udp 2001:DB8::/32 any
Device(config-ipv6-acl)# end
```

例：vty へのアクセスの制御

次の例では、仮想端末回線 0 ～ 4 に着信する接続は、acl1 という名前の IPv6 アクセス リストに基づいてフィルタリングされます。

```
ipv6 access-list acl1
 permit ipv6 host 2001:DB8:0:4::2/32 any
!
line vty 0 4
 ipv6 access-class acl1 in
```

IPv6 アクセス コントロール リストに関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1 : IPv6* アクセス コントロール リストに関する機能情報

機能名	リリース	機能情報
IPv6 サービス：拡張アクセス コントロール リスト	Cisco IOS XE リリース 2.1	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。

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。