IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装

この章では、シスコのネットワーク デバイス用の Cisco IOS IPv6 トラフィック フィルタおよびファイアウォール機能を設定する方法について説明します。これらのセキュリティ機能を使用すると、パフォーマンス低下や障害、さらには悪意のある攻撃や通常のネットワーク ユーザによる悪意はないが破壊的なミスによって引き起こされるデータ損失やセキュリティ侵害からネットワークを守ることができます。

機能情報の確認

ご使用のソフトウェア リリースによっては、この章に記載されている機能の中に、一部サポートされていないものがあります。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装の機能情報」（P.36）を参照してください。

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスしてください。Cisco.com のアカウントは必要ありません。

目次

IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装の前提条件

IPv6 アドレッシングおよび基本設定を熟知している必要があります。詳細については、「*Implementing IPv6 Addressing and Basic Connectivity*」の章を参照してください。

IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装の制約事項

Cisco IOS Release 12.2(2)T から Cisco IOS Release 12.2(13)T、および Cisco IOS Release 12.0(22)S 以降のリリースでは、標準の IPv6 Access Control List（ACL; アクセス コントロール リスト）機能だけがサポートされています。Cisco IOS Release 12.0(23)S および 12.2(13)T 以降のリリースでは、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（IPv4 での拡張 ACL に似た機能）。

IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装に関する情報

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 での標準の ACL 機能は、IPv4 での標準の ACL に似ています。アクセス リストによって、ルータ 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 リストの最後には、暗黙的な deny 文が指定されています。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。

Cisco IOS Release 12.0(23)S および 12.2(13)T 以降では、標準 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（IPv4 での拡張 ACL に似た機能）。

IPsec 認証ヘッダーの IPv6 ACL 拡張

この機能によって、Authentication Header（AH; 認証ヘッダー）の有無にかかわらず、TCP、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）、ICMP、SCTP などの Upper Layer Protocol（ULP; 上位層プロトコル）でマッチングを実行できます。

TCP または UDP トラフィックは、AH が存在する場合でも存在しない場合でも、TCP、UDP、ICMP、SCTP などの Upper Layer Protocol（ULP; 上位層プロトコル）に対してマッチングできます。この機能が導入されるまでは、このようなマッチングは AH が存在しない場合にだけ使用できました。

この機能によって、キーワード **auth** が **permit** コマンドと **deny** コマンドに導入されました。**auth** キーワードを指定すると、特定のプロトコル、つまり TCP や UDP とともに認証ヘッダーが存在するかどうかに照らしてトラフィックをマッチングできます。

AH ヘッダーが存在する場合は、IPv6 トラフィックを ULP に対してマッチングできます。このマッチングを実行するには、**permit** コマンドまたは **deny** コマンドを使用するときに、*protocol* 引数に **ahp** オプションを入力します。

IPv6 でのアクセス クラス フィルタリング

IPv6 ACL に基づく、ルータ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に照らしてマッチングされ、ACL 内の宛先アドレスは、インターフェイス上のローカル ルータ 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 ルータ アドレスに照らしてマッチングされ、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。

Cisco IOS Firewall for IPv6

Cisco IOS Firewall 機能を使用すると、高度なトラフィック フィルタリング機能をネットワークのファイアウォールの不可欠な部分として組み込むことができます。Cisco IOS Firewall for IPv6 によって、Cisco IOS Firewall を IPv6 ネットワークに実装できます。Cisco IOS Firewall は、IPv4 ネットワーク用の Cisco IOS Firewall と共存し、すべてのデュアル スタック ルータでサポートされています。

Cisco IOS Firewall for IPv6 機能は、次のとおりです。

- フラグメント化されたパケット インスペクション：フラグメント ヘッダーを使用して、フラグメント処理をトリガーします。Cisco IOS Firewall Virtual Fragment Reassembly（VFR）は、シーケンスから外れたフラグメントを調べ、それらのパケットを正しい順序に切り替え、一意の識別子が設定された単一の IP からのフラグメント数を調べ（Denial-of-Service（DoS; サービス拒絶）攻撃）、仮想再アセンブリを実行して、パケットを上位層プロトコルに移動します。
- IPv6 DoS 攻撃の軽減：SYN 半開接続を含む、IPv4 実装と同じ方法で、軽減メカニズムが実装されています。
- トンネル化パケット インスペクション：Cisco IOS Firewall ルータで終端するトンネル化 IPv6 パケットは、Cisco IOS Firewall for IPv6 によって検査できます。
- ステートフル パケット インスペクション：この機能によって、TCP、UDP、Internet Control Message Protocol version 6（ICMPv6; インターネット制御メッセージ プロトコル バージョン 6）、および FTP の各セッションのステートフル パケット インスペクションを実行できます。
- IPv4 ネットワークから発信され、IPv6 環境で終端するパケットのステートフル インスペクション：この機能では、IPv4 から IPv6 への変換サービスを使用します。
- 大半の IPv6 拡張ヘッダー情報の解釈または認識：この機能によって、ルーティング ヘッダー、ホップバイホップ オプション ヘッダー、およびフラグメント ヘッダーを含む、IPv6 拡張ヘッダー情報が解釈または認識されます。
- Port-to-Application Mapping（PAM）：Cisco IOS Firewall for IPv6 には PAM が含まれています。

Cisco IOS Firewall for IPv6 での PAM

PAM を使用して、ネットワーク サービスとアプリケーション用の TCP または UDP ポート番号をカスタマイズできます。PAM ではこの情報を使用して、アプリケーションに関連する登録済み、つまり既知のポートと異なるポートを使用しているサービスを実行するネットワーク環境をサポートします。

PAM では、ポート情報を使用して、ポートからアプリケーションへのデフォルト マッピング情報のテーブルをファイアウォールで確立します。PAM テーブルの情報によって、Context-Based Access Control（CBAC; コンテキストベース アクセス コントロール）がサポートしているサービスを非標準ポートで実行できます。CBAC での調査は、アプリケーションに関連付けられている既知のポート、つまり登録済みのポートだけを使用するトラフィックに限定されますが、PAM を使用すると、ネットワーク管理者は、特定のアプリケーションおよびサービスのネットワーク アクセス コントロールをカスタマイズできます。

PAM では、ホストまたはサブネット固有のポート マッピングもサポートしています。これにより、標準 ACL を使用して単一のホストまたはサブネットに PAM を適用できます。ホストまたはサブネット固有のポート マッピングは、標準の ACL を使用して行われます。

Cisco IOS Firewall アラート、監査証跡、およびシステム ロギング

Cisco IOS Firewall によって、ファイアウォールで追跡されたイベントに基づくリアルタイム アラートおよび監査証跡が生成されます。拡張された監査証跡機能では、システム ロギングを使用して、すべてのネットワーク トランザクションを追跡したり、タイムスタンプ、送信元ホスト、宛先ホスト、および使用されたポートを記録したり、高度なセッションベースのレポート用に送信バイト総数を記録したりします。リアルタイム アラートは、システムで疑わしいアクティビティが検出されると、システム ロギング エラー メッセージを中央管理コンソールに送信します。Cisco IOS Firewall インスペクション ルールを使用して、アプリケーション プロトコル単位でアラートと監査証跡情報を設定できます。たとえば、TCP トラフィック用の監査証跡情報を生成する場合、TCP インスペクションを定義する Cisco IOS Firewall ルールで、この情報の生成を指定できます。

Cisco IOS Firewall によって、検査されたセッションの詳細を記録する監査証跡メッセージが提供されます。監査証跡情報は、CBAC インスペクション ルールを使用してアプリケーション単位で設定できます。検査されたプロトコルを識別するには、応答側に関連付けられているポート番号を使用します。ポート番号は、アドレスの直後に表示されます。

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、および送信元アドレスや宛先アドレス）は、すべて 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。

トンネリング サポート

IPv4 でトンネルされる IPv6 パケットは、検査されません。トンネルがルータで終端され、そのトンネルからの IPv6 出トラフィックが終端されない場合、そのトラフィックは検査されます。

仮想フラグメント再アセンブリ

VFR がイネーブルの場合、VFR 処理は、ACL 入力リストが着信パケットに照らしてチェックされたあとに開始されます。入力パケットには、適切な VFR 情報がタグ付けされます。

Cisco IOS Firewall の制約事項

IPv6 では、Cisco IOS Intrusion Detection System（IDS; 侵入検知システム）がサポートされていません。

Cisco IOS Zone-Based Firewall for IPv6

IPv6 トラフィックをサポートするために、Cisco IOS Zone-Based Firewall for IPv6 は Cisco IOS Zone-Based Firewall for IPv4 と共存します。この機能では、TCP、UDP、ICMPv6、および FTP の各セッションに対して MIB サポートが提供されます。

Zone-Based Firewall の詳細については、『*Cisco IOS Security Configuration Guide: Securing the Data Plane*』の「Zone-Based Policy Firewall」を参照してください。

IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装方法

次の各項の作業では、IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装方法を示します。

IPv6 トラフィック フィルタリングの設定

ここでは、IPv6 トラフィック フィルタリングをイネーブルにする方法について説明します。

制約事項

- Cisco IOS Release 12.2(13)T、12.0(23)S、または以降のリリースを実行している場合は、「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」の項に進みます。Cisco IOS Release 12.2(11)T、12.0(22)S、または以前のリリースを実行している場合は、「Cisco IOS Release 12.2(11)T、12.0(22)S、または以前のリリースにおけるトラフィック フィルタリング用 IPv6 ACL の作成」の項に進みます。
- IPv6 ACL は、一意な名前で定義されています（IPv6 では番号付き ACL はサポートしていません）。IPv4 ACL および IPv6 ACL は、同じ名前を共有できません。

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

ここでは、トラフィックをフィルタリングし、ファイアウォールとして機能し、または潜在的なウイルスを検出するようにネットワーキング デバイスを設定する方法について説明します。次の作業では、IPv6 ACL を作成し、Cisco IOS Release 12.2(13)T および 12.0(23)S または以降のリリースでトラフィックをフィルタリングするようにその IPv6 ACL を設定する方法について説明します。

前提条件

Cisco IOS Release 12.2(13)T および 12.0(23)S または以降のリリースでは、下位互換性のために、グローバル コンフィギュレーション モードでの **deny** キーワードと **permit** キーワードを指定した **ipv6 access-list** コマンドが引き続きサポートされています。ただし、グローバル コンフィギュレーション モードで拒否条件と許可条件を使用して定義された IPv6 ACL は、IPv6 アクセス リスト コンフィギュレーション モードに変換されます。変換された IPv6 ACL 設定の例については、「例：IPv6 ACL の作成および適用」の項を参照してください。

制約事項

- 各 IPv6 ACL には、IPv6 ネイバー探索をイネーブルにするための暗黙的な許可ルールが含まれています。ユーザは、ACL 内に deny ipv6 any any 文を配置することでこれらのルールを上書きできます。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利用するため、デフォルトで、インターフェイス上での IPv6 ネイバー探索パケットの送受信が IPv6 ACL によって暗黙的に許可されます。IPv4 の場合、IPv6 ネイバー探索プロセスに相当する Address Resolution Protocol（ARP; アドレス解決プロトコル）では、個別のデータ リンク レイヤ プロトコルを利用するため、デフォルトで、インターフェイス上での ARP パケットの送受信が IPv4 ACL によって暗黙的に許可されます。
- 時間ベースの ACL および再帰 ACL は、Cisco 12000 シリーズ プラットフォーム上の IPv4 または IPv6 ではサポートされていません。Cisco 12000 シリーズでは、IPv6 の **permit** コマンドの **reflect** キーワード、**timeout** キーワード、および **time-range** キーワードが除外されています。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 access-list** *access-list-name*
4. **permit** *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*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*]] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]
   または
   deny *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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：** `Router(config)# ipv6 access-list outbound`	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-list name* 引数には、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	**permit protocol** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*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*]] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]
	
	または
	
	deny *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*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：
	`Router(config-ipv6-acl)# permit tcp 2001:0DB8:0300:0201::/32 eq telnet any reflect reflectout`
	
	または
	
	例：
	`Router(config-ipv6-acl)# deny tcp host 2001:0db8:1::1 any log-input`
		IPv6 ACL の許可条件または拒否条件を指定します。

インターフェイスへの IPv6 ACL の適用

ここでは、Cisco IOS Release 12.2(13)T および 12.0(23)S または以降のリリースで IPv6 ACL をインターフェイスに適用する方法について説明します。

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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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** *type number* **例：** `Router(config)# interface ethernet 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：** `Router(config-if)# ipv6 traffic-filter outbound out`	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

ここでは、ルータ上の vty へのアクセスを制限する方法について説明します。

- 「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」（P.8）
- 「仮想端末回線への IPv6 ACL の適用」（P.10）

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

ここでは、IPv6 ACL を作成してアクセス クラス フィルタリングを提供することで、ルータ上の vty へのアクセスを制限する方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 access-list** *access-list-name*
4. **permit** *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*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*]] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]
   または
   deny *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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：** `Router(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	**permit protocol** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*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*]] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]
	
	または
	
	deny *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*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：
	`Router(config-ipv6-acl)# permit ipv6 host 2001:0DB8:0:4::32 any eq telnet`
	または
	
	例：
	`Router(config-ipv6-acl)# deny ipv6 host 2001:0DB8:0:6::6/32 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

アクセス クラス フィルタリング用の IPv6 ACL を作成したあとに、指定した仮想端末回線にその ACL を適用する必要があります。次の作業では、仮想端末回線に ACL を適用する方法を示します。

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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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：** `Router(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：** `Router(config-line)# ipv6 access-class cisco in`	IPv6 ACL に基づいて、ルータとの間の着信接続と発信接続をフィルタリングします。

TCP または UDP マッチングの設定

AH の有無に関係なく、TCP または UDP トラフィックを ULP（TCP、UDP、ICMP、SCTP など）に対してマッチングできます。この機能が導入されるまでは、このようなマッチングは AH が存在しない場合にだけ使用できました。

AH が存在する場合は、**permit icmp** コマンドおよび **deny icmp** コマンドで **auth** キーワードを使用すると、TCP または UDP トラフィックを ULP に対してマッチングできます。AH が存在しない TCP または UDP トラフィックでは、マッチングは実行されません。

AH ヘッダーが存在する場合は、IPv6 トラフィックを ULP に対してマッチングできます。このマッチングを実行するには、**permit** コマンドまたは **deny** コマンドを使用するときに、*protocol* 引数に **ahp** オプションを入力します。

この作業では、AH が存在する場合に、TCP または UDP トラフィックを ULP に対してマッチングできます。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 access-list** *access-list-name*
4. **permit icmp auth**

   または
   deny icmp auth

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：** `Router# enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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：** `Router(config)# ipv6 access-list list1`	IPv6 アクセス リストを定義し、ルータを IPv6 アクセス リスト コンフィギュレーション モードにします。
ステップ 4	**permit icmp auth** または **deny icmp auth** **例：** `Router(config-ipv6-acl)# permit icmp auth`	AH の存在に照らしたマッチングに使用される **auth** キーワードを使用して、IPv6 ACL の許可条件と拒否条件を指定します。

Cisco IOS Release 12.2(11)T、12.0(22)S、または以前のリリースにおけるトラフィック フィルタリング用 IPv6 ACL の作成

ここでは、Cisco IOS Release 12.2(11)T、12.0(22)S、または以前のリリースで ACL を作成および適用する方法について説明します。

- 「Cisco IOS Release 12.2(11)T、12.0(22)S、または以前のリリースにおける IPv6 ACL の作成」（P.12）
- 「Cisco IOS Release 12.2(11)T、12.0(22)S、または以前のリリースのインターフェイスへの IPv6 ACL の適用」（P.13）

Cisco IOS Release 12.2(11)T、12.0(22)S、または以前のリリースにおける IPv6 ACL の作成

ここでは、IPv6 ACL を作成し、Cisco IOS Release 12.2(11)T、12.0(22)S、または以前のリリースのトラフィックを通過またはブロックするようにこの IPv6 ACL を設定する方法について説明します。

制約事項

- *source-ipv6-prefix* 引数によって、トラフィックがパケット送信元アドレス別にフィルタリングされ、*destination-ipv6-prefix* 引数によって、トラフィックがパケット宛先アドレス別にフィルタリングされます。

- Cisco IOS ソフトウェアでは、アクセス リスト内の許可および拒否の条件文に照らして、IPv6 プレフィクスを比較します。すべての IPv6 アクセス リスト（許可および拒否の条件文が含まれていないアクセス リストを含む）には、最後の一致条件として暗黙的な deny any any 文が含まれています。各条件文に適用されるプライオリティ値またはシーケンス値は、文がアクセス リストで適用される順番を示しています。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 access-list** *access-list-name* {**permit** | **deny**} {*source-ipv6-prefix*/*prefix-length* | **any**} {*destination-ipv6-prefix*/*prefix-length* | **any**} [**priority** *value*]

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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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* {**permit** | **deny**} {*source-ipv6-prefix*/*prefix-length* | **any**} {*destination-ipv6-prefix*/*prefix-length* | **any**} [**priority** *value*] **例：** `Router(config)# ipv6 access-list list2 deny fec0:0:0:2::/64 any`	IPv6 ACL を作成し、ACL の拒否条件または許可条件を設定します。

Cisco IOS Release 12.2(11)T、12.0(22)S、または以前のリリースのインターフェイスへの IPv6 ACL の適用

ここでは、Cisco IOS Release 12.2(11)T、12.0(22)S、または以前のリリースのインターフェイスに IPv6 ACL を適用する方法について説明します。

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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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** *type number* **例：** `Router(config)# interface ethernet 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：** `Router(config-if)# ipv6 traffic-filter list2 out`	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。

Cisco IOS Firewall for IPv6 の設定

ここでは、IPv6 環境用の Cisco IOS Firewall を設定する方法について説明します。この設定シナリオでは、パケット インスペクションと ACL の両方を使用します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **ipv6 inspect name** *inspection-name protocol* [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**timeout** *seconds*]
5. **interface** *type number*
6. **ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*}
7. **ipv6 enable**
8. **ipv6 traffic-filter** *access-list-name* {**in** | **out**}
9. **ipv6 inspect** *inspect-name*
10. **ipv6 access-list** *access-list-name*
11. **permit** *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*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*]] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

または
deny *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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 unicast-routing** **例：** `Router(config)# ipv6 unicast-routing`	IPv6 ユニキャスト ルーティングをイネーブルにします。
ステップ 4	**ipv6 inspect name** *inspection-name protocol* [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**timeout** *seconds*] **例：** `Router(config)# ipv6 inspect name ipv6_test icmp timeout 60`	ファイアウォール用の一連の IPv6 インスペクション ルールを定義します。
ステップ 5	**interface** *type number* **例：** `Router(config)# interface FastEthernet0/0`	インスペクションが実行されるインターフェイスを指定します。
ステップ 6	**ipv6 address** {*ipv6-address*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*} **例：** `Router(config-if)# ipv6 address 3FFE:C000:0:7::/64 eui-64`	インスペクション インターフェイスのアドレスを指定します。
ステップ 7	**ipv6 enable** **例：** `Router(config-if)# ipv6 enable`	IPv6 ルーティングをイネーブルにします。 **（注）** この手順は、IPv6 アドレスをステップ 6 で指定している場合は省略可能です。
ステップ 8	**ipv6 traffic-filter** *access-list-name* {**in** | **out**} **例：** `Router(config-if)# ipv6 traffic-filter outbound out`	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。

	コマンドまたはアクション	目的
ステップ 9	**ipv6 inspect** *inspection-name* {**in** | **out**} **例：** `Router(config)# ipv6 inspect ipv6_test in`	一連のインスペクション ルールを適用します。
ステップ 10	**ipv6 access-list** *access-list-name* **例：** `Router(config)# ipv6 access-list outbound`	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。ルータにより、Router(config-ipv6-acl)# に対する変更が要求されます。

ステップ 11	**permit protocol** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*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*]] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]
	
	または
	
	deny *protocol* {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*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：
	`Router(config-ipv6-acl)# permit tcp 2001:0DB8:0300:0201::/32 any reflect reflectout`
	または
	
	例：
	`Router(config-ipv6-acl)# deny tcp fec0:0:0:0201::/64 any`
		IPv6 ACL の許可条件または拒否条件を指定します。

PAM for IPv6 の設定

PAM 用の IPv6 アクセス クラス フィルタの作成

ここでは、PAM 環境で使用する IPv6 アクセス クラス フィルタを作成する方法について説明します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 access-list** *access-list-name*
4. **permit** *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*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*]] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]
   または
   deny *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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：** `Router(config)# ipv6 access-list outbound`	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。ルータによって、Router(config-ipv6-acl)# への変更が要求されます。

ステップ 4	**permit protocol** {*source-ipv6-prefix/prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*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*]] [**reflect** *name* [**timeout** *value*]] [**routing**] [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]
	
	または
	
	deny *protocol* {*source-ipv6-prefix*/*prefix-length* | **any** | **host** *source-ipv6-address* | **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix*/*prefix-length* | **any** | **host** *destination-ipv6-address* | **auth**} [*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：
	`Router(config-ipv6-acl)# permit tcp 2001:0DB8:0300:0201::/32 any reflect reflectout`
	または
	
	例：
	`Router(config-ipv6-acl)# deny tcp fec0:0:0:0201::/64 any`
		IPv6 ACL の許可条件または拒否条件を指定します。

PAM への IPv6 アクセス クラス フィルタの適用

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 port-map** *application-name* **port** *port-num* [**list** *acl-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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# 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 port-map** *application-name* **port** *port-num* [**list** *acl-name*] **例：** `Router(config)# ipv6 port-map ftp port 8090 list PAMACL`	システムの PAM を確立します。

IPv6 でのゾーンベースのファイアウォールの設定

次の作業では、IPv6 環境に対して Cisco IOS のゾーンベースのファイアウォールを設定する方法を示します。

- 「検査タイプ パラメータ マップの設定」（P.19）
- 「検査タイプ クラス マップの作成と使用」（P.20）
- 「検査タイプ ポリシー マップの作成と使用」（P.21）
- 「セキュリティ ゾーンとゾーン ペアの作成」（P.22）

検査タイプ パラメータ マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **parameter-map type inspect** {*parameter-map-name* | **global** | **default**}
4. **sessions maximum** *sessions*
5. **ipv6 routing-enforcement-header loose**

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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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：** `Router# 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	**parameter-map type inspect** {*parameter-map-name* | **global** | **default**} **例：** `Router(config)# parameter-map type inspect v6-param-map`	検査アクションに関連した接続しきい値、タイムアウトなどといったパラメータ用の検査タイプ パラメータ マップを設定し、ルータをパラメータ マップ コンフィギュレーション モードにします。
ステップ 4	**sessions maximum** *sessions* **例：** `Router(config-profile)# sessions maximum 10000`	ゾーン ペア上に存在可能な最大許容セッション数を設定します。
ステップ 5	**ipv6 routing-enforcement-header loose** **例：** `Router(config-profile)# ipv6 routing-enforcement-header loose`	レガシー IPv6 検査との下位互換性を提供します。

検査タイプ クラス マップの作成と使用

手順の概要

1. **enable**
2. **configure terminal**
3. **class-map type inspect** {**match-any** | **match-all**} *class-map-name*
4. **match protocol tcp**
5. **match protocol udp**
6. **match protocol icmp**
7. **match protocol ftp**

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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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：** `Router# 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	**class-map type inspect** {**match-any** | **match-all**} *class-map-name* **例：** `Router(config-profile)# class-map type inspect match-any v6-class`	検査タイプ クラス マップを作成し、ルータをクラスマップ コンフィギュレーション モードにします。
ステップ 4	**match protocol tcp** **例：** `Router(config-cmap)# match protocol tcp`	TCP に基づいてクラス マップの一致基準を設定します。
ステップ 5	**match protocol udp** **例：** `Router(config-cmap)# match protocol udp`	UDP に基づいてクラス マップの一致基準を設定します。
ステップ 6	**match protocol icmp** **例：** `Router(config-cmap)# match protocol icmp`	ICMP に基づいてクラス マップの一致基準を設定します。
ステップ 7	**match protocol ftp** **例：** `Router(config-cmap)# match protocol ftp`	FTP に基づいてクラス マップの一致基準を設定します。

検査タイプ ポリシー マップの作成と使用

手順の概要

1. **enable**
2. **configure terminal**
3. **policy-map type inspect** *policy-map-name*
4. **class type inspect** *class-map-name*
5. **inspect** [*parameter-map-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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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：** `Router# 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	**policy-map type inspect** *policy-map-name* **例：** `Router(config)# policy-map type inspect v6-policy`	検査タイプ ポリシー マップを作成し、ルータをポリシー マップ コンフィギュレーション モードにします。
ステップ 4	**class type inspect** *class-map-name* **例：** `Router(config-pmap)# class type inspect v6-class`	アクションが実行されるトラフィック（クラス）を指定します。
ステップ 5	**inspect** [*parameter-map-name*] **例：** `Router(config-pmap)# inspect`	Cisco IOS ステートフル パケット インスペクションをイネーブルにします。

セキュリティ ゾーンとゾーン ペアの作成

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security 1**
4. **zone security 2**
5. **zone-pair security** *zone-pair-name* **source** {*source-zone-name* | **self** | **default**} **destination** {*destination-zone-name* | **self** | **default**}
6. **service-policy type inspect** *policy-map-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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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：** `Router# 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	**zone security** {*zone-name* | **default**} **例：** `Router(global)# zone security 1`	セキュリティ ゾーンを作成します。 • ゾーン ペアを作成できるように、少なくとも 2 つのセキュリティ ゾーンを作成することを推奨します。
ステップ 4	**zone security** {*zone-name* | **default**} **例：** `Router(global)# zone security 2`	セキュリティ ゾーンを作成します。 • ゾーン ペアを作成できるように、少なくとも 2 つのセキュリティ ゾーンを作成することを推奨します。
ステップ 5	**zone-pair security** *zone-pair-name* **source** {*source-zone-name* | **self** | **default**} **destination** {*destination-zone-name* | **self** | **default**} **例：** `Router(global)# zone-pair security zp source z1 destination z2`	ゾーン ペアを作成し、ルータをゾーンペア コンフィギュレーション モードにします。
ステップ 6	**service-policy type inspect** *policy-map-name* **例：** `Router(config-sec-zone-pair)# service-policy type inspect v6-policy`	ファイアウォール ポリシー マップをゾーン ペアに付加します。

IPv6 セキュリティの設定と動作の確認

ここでは、IPv6 セキュリティ オプションの設定と動作を確認するための情報を表示する方法について説明します。必要に応じて次のコマンドを使用して、設定と動作を確認します。

手順の概要

1. **show crypto ipsec sa** [**map** *map-name* | **address** | **identity** | **interface** *interface-type interface-number* | **peer** [**vrf** *fvrf-name*] **address** | **vrf** *ivrf-name* | ipv6 [*interface-type interface-number*]] [**detail**]
2. **show crypto isakmp peer** [**config** | **detail**]
3. **show crypto isakmp profile**
4. **show crypto isakmp sa** [**active** | **standby** | **detail** | **nat**]
5. **show ipv6 access-list** [*access-list-name*]
6. **show ipv6 inspect** {**name** *inspection-name* | **config** | **interfaces** | **session** [**detail**] | **all**}

7. **show ipv6 port-map** [*application* | **port** *port-number*]
8. **show ipv6 prefix-list** [**detail** | **summary**] [*list-name*]
9. **show ipv6 virtual-reassembly interface** *interface-type*
10. **show logging** [**slot** *slot-number* | **summary**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show crypto ipsec sa** [**map** *map-name* | **address** | **identity** | **interface** *interface-type interface-number* | **peer** [**vrf** *fvrf-name*] **address** | **vrf** *ivrf-name* | **ipv6** [*interface-type interface-number*]] [**detail**] **例：** `Router# show crypto ipsec sa ipv6`	現在の SA によって使用されている設定を表示します。
ステップ 2	**show crypto isakmp peer** [**config** | **detail**] **例：** `Router# show crypto isakmp peer`	ピアの説明を表示します。
ステップ 3	**show crypto isakmp profile** **例：** `Router# show crypto isakmp profile`	ルータに定義されている ISAKMP プロファイルをすべてリストします。
ステップ 4	**show crypto isakmp sa** [**active** | **standby** | **detail** | **nat**] **例：** `Router# show crypto isakmp sa`	現在の IKE SA を表示します。
ステップ 5	**show ipv6 access-list** [*access-list-name*] **例：** `Router# show ipv6 access-list`	現在のすべての IPv6 アクセス リストの内容を表示します。
ステップ 6	**show ipv6 inspect** {**name** *inspection-name* | **config** | **interfaces** | **session** [**detail**] | **all**} **例：** `Router# show ipv6 inspect interfaces`	CBAC の設定およびセッション情報を表示します。
ステップ 7	**show ipv6 port-map** [*application* | **port** *port-number*] **例：** `Router# show ipv6 port-map ftp`	PAM の設定を表示します。
ステップ 8	**show ipv6 prefix-list** [**detail** | **summary**] [*list-name*] **例：** `Router# show ipv6 prefix-list`	IPv6 プレフィクス リストまたは IPv6 プレフィクス リストのエントリに関する情報を表示します。

	コマンドまたはアクション	目的
ステップ 9	**show ipv6 virtual-reassembly interface** *interface-type* **例：** `Router# show ipv6 virtual-reassembly interface e1/1`	VFR の設定および統計情報を表示します。
ステップ 10	**show logging** [**slot** *slot-number* | **summary**] **例：** `Router# show logging`	システム ロギング（syslog）の状態および標準のシステム ロギング バッファの内容を表示します。 • **log** キーワードまたは **log-input** キーワードが指定されたアクセス リスト エントリは、パケットがそのアクセス リスト エントリに一致した場合に記録されます。

IPv6 セキュリティの設定と動作のトラブルシューティング

この任意の作業では、IPv6 セキュリティ オプションの設定と動作をトラブルシューティングするための情報を表示する方法について説明します。次のコマンドを必要なときにだけ使用して、設定と動作を確認します。

手順の概要

1. **enable**
2. **clear ipv6 access-list** [*access-list-name*]
3. **clear ipv6 inspect** {**session** *session-number* | **all**}
4. **clear ipv6 prefix-list** [*prefix-list-name*] [*ipv6-prefix*/*prefix-length*]
5. **debug crypto ipsec**
6. **debug crypto engine packet** [**detail**]
7. **debug ipv6 inspect** {**function-trace** | **object-creation** | **object-deletion** | **events** | **timers** | **protocol** | **detailed**}
8. **debug ipv6 packet** [**access-list** *access-list-name*] [**detail**]

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：** `Router# enable`	特権 EXEC モードをイネーブルにします。 • 必要に応じてパスワードを入力します。
ステップ 2	**clear ipv6 access-list** [*access-list-name*] **例：** `Router# clear ipv6 access-list tin`	IPv6 アクセス リストの一致カウンタをリセットします。

	コマンドまたはアクション	目的
ステップ 3	**clear ipv6 inspect** {**session** *session-number* | all} **例：** Router# clear ipv6 inspect all	特定の IPv6 セッションまたはすべての IPv6 インスペクション セッションを削除します。
ステップ 4	**clear ipv6 prefix-list** [*prefix-list-name*] [*ipv6-prefix*/*prefix-length*] **例：** Router# clear ipv6 prefix-list	IPv6 プレフィクス リスト エントリのヒット カウントをリセットします。
ステップ 5	**debug crypto ipsec** **例：** Router# debug crypto ipsec	IPsec ネットワーク イベントを表示します。
ステップ 6	**debug crypto engine packet** [**detail**] **例：** Router# debug crypto engine packet	IPv6 パケットの内容を表示します。 **注意** 複数のパケットが暗号化される場合、このコマンドを使用すると、システムのフラッディングが発生し、CPU 使用率が高くなる可能性があります。
ステップ 7	**debug ipv6 inspect** {**function-trace** | **object-creation** | **object-deletion** | **events** | **timers** | **protocol** | **detailed**} **例：** Router# debug ipv6 inspect timers	Cisco IOS Firewall イベントに関するメッセージを表示します。
ステップ 8	**debug ipv6 packet** [**access-list** *access-list-name*] [**detail**] **例：** Router# debug ipv6 packet access-list PAK-ACL	IPv6 パケットのデバッグ メッセージを表示します。

例

ここでは、次の出力例について説明します。

show crypto ipsec sa ipv6 コマンドの出力例

次に、**show crypto ipsec sa ipv6** コマンドの出力例を示します。

```
Router# show crypto ipsec sa ipv6

interface: Tunnel0
     Crypto map tag: Tunnel0-head-0, local addr 3FFE:2002::A8BB:CCFF:FE01:9002

    protected vrf: (none)
    local  ident (addr/mask/prot/port): (::/0/0/0)
    remote ident (addr/mask/prot/port): (::/0/0/0)
    current_peer 3FFE:2002::A8BB:CCFF:FE01:2C02 port 500
      PERMIT, flags={origin_is_acl,}
     #pkts encaps: 133, #pkts encrypt: 133, #pkts digest: 133
     #pkts decaps: 133, #pkts decrypt: 133, #pkts verify: 133
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #send errors 60, #recv errors 0

      local crypto endpt.: 3FFE:2002::A8BB:CCFF:FE01:9002,
      remote crypto endpt.: 3FFE:2002::A8BB:CCFF:FE01:2C02
      path mtu 1514, ip mtu 1514
      current outbound spi: 0x28551D9A(676666778)

      inbound esp sas:
       spi: 0x2104850C(553944332)
         transform: esp-des ,
         in use settings ={Tunnel, }
         conn id: 93, flow_id: SW:93, crypto map: Tunnel0-head-0
         sa timing: remaining key lifetime (k/sec): (4397507/148)
         IV size: 8 bytes
         replay detection support: Y
         Status: ACTIVE

      inbound ah sas:
       spi: 0x967698CB(2524354763)
         transform: ah-sha-hmac ,
         in use settings ={Tunnel, }
         conn id: 93, flow_id: SW:93, crypto map: Tunnel0-head-0
         sa timing: remaining key lifetime (k/sec): (4397507/147)
         replay detection support: Y
         Status: ACTIVE

      inbound pcp sas:

      outbound esp sas:
       spi: 0x28551D9A(676666778)
         transform: esp-des ,
         in use settings ={Tunnel, }
         conn id: 94, flow_id: SW:94, crypto map: Tunnel0-head-0
         sa timing: remaining key lifetime (k/sec): (4397508/147)
         IV size: 8 bytes
         replay detection support: Y
         Status: ACTIVE

      outbound ah sas:
       spi: 0xA83E05B5(2822636981)
         transform: ah-sha-hmac ,
         in use settings ={Tunnel, }
         conn id: 94, flow_id: SW:94, crypto map: Tunnel0-head-0
         sa timing: remaining key lifetime (k/sec): (4397508/147)
         replay detection support: Y
```

```
         Status: ACTIVE

      outbound pcp sas:
```

show crypto isakmp peer コマンドの出力例

次の出力例は、IPv6 ルータ上のピアの説明を示しています。

```
Router# show crypto isakmp peer detail

Peer: 2001:0DB8:0:1::1 Port: 500 Local: 2001:0DB8:0:2::1
Phase1 id: 2001:0DB8:0:1::1
flags:
NAS Port: 0 (Normal)
IKE SAs: 1 IPsec SA bundles: 1
last_locker: 0x141A188, last_last_locker: 0x0
last_unlocker: 0x0, last_last_unlocker: 0x0
```

show crypto isakmp profile コマンドの出力例

次の出力例は、IPv6 ルータで定義されている ISAKMP プロファイルを示しています。

```
Router# show crypto isakmp profile

ISAKMP PROFILE tom
Identities matched are:
ipv6-address 2001:0DB8:0:1::1/32
Certificate maps matched are:
Identity presented is: ipv6-address fqdn
keyring(s): <none>
trustpoint(s): <all>
```

show crypto isakmp sa コマンドの出力例

次の出力例は、アクティブな IPv6 デバイスの SA を示しています。IPv4 デバイスは非アクティブです。

```
Router# show crypto isakmp sa detail

Codes: C - IKE configuration mode, D - Dead Peer Detection
        K - Keepalives, N - NAT-traversal
        X - IKE Extended Authentication
        psk - Preshared key, rsig - RSA signature
        renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local           Remote          I-VRF    Status Encr Hash Auth DH
Lifetime Cap.

IPv6 Crypto ISAKMP SA

  dst: 3FFE:2002::A8BB:CCFF:FE01:2C02
  src: 3FFE:2002::A8BB:CCFF:FE01:9002
  conn-id: 1001  I-VRF:          Status: ACTIVE Encr: des  Hash: sha  Auth:
psk
  DH: 1  Lifetime: 23:45:00 Cap: D    Engine-id:Conn-id = SW:1

  dst: 3FFE:2002::A8BB:CCFF:FE01:2C02
  src: 3FFE:2002::A8BB:CCFF:FE01:9002
  conn-id: 1002  I-VRF:          Status: ACTIVE Encr: des  Hash: sha  Auth:
psk
  DH: 1  Lifetime: 23:45:01 Cap: D    Engine-id:Conn-id = SW:2
```

show ipv6 access-list コマンドの出力例

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ています。

```
Router> show ipv6 access-list

IPv6 access list inbound
    permit tcp any any eq bgp reflect tcptraffic (8 matches) sequence 10
    permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
    permit udp any any reflect udptraffic sequence 30

IPv6 access list tcptraffic (reflexive) (per-user)
    permit tcp host 2001:0DB8:1::32 eq bgp host 2001:0DB8:2::32 eq 11000 timeout 300 (time
        left 243) sequence 1
    permit tcp host 2001:0DB8:1::32 eq telnet host 2001:0DB8:2::32 eq 11001 timeout 300
        (time left 296) sequence 2

IPv6 access list outbound
    evaluate udptraffic
    evaluate tcptraffic
```

show ipv6 prefix-list コマンドの出力例

次に、**detail** キーワードを指定した **show ipv6 prefix-list** コマンドの出力例を示します。

```
Router# show ipv6 prefix-list detail

Prefix-list with the last deletion/insertion: bgp-in
ipv6 prefix-list 6to4:
   count: 1, range entries: 0, sequences: 5 - 5, refcount: 2
   seq 5 permit 2001:0db8::/32 (hit count: 313, refcount: 1)
ipv6 prefix-list aggregate:
   count: 2, range entries: 2, sequences: 5 - 10, refcount: 30
   seq 5 deny 3FFE:C00::/24 ge 25 (hit count: 568, refcount: 1)
   seq 10 permit ::/0 le 48 (hit count: 31310, refcount: 1)
ipv6 prefix-list bgp-in:
   count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
   seq 5 deny 5F00::/8 le 128 (hit count: 0, refcount: 1)
   seq 10 deny ::/0 (hit count: 0, refcount: 1)
   seq 15 deny ::/1 (hit count: 0, refcount: 1)
   seq 20 deny ::/2 (hit count: 0, refcount: 1)
   seq 25 deny ::/3 ge 4 (hit count: 0, refcount: 1)
   seq 30 permit ::/0 le 128 (hit count: 240664, refcount: 0)
```

show ipv6 virtual-reassembly コマンドの出力例

次に、**interface** キーワードを指定した **show ipv6 virtual-reassembly** コマンドの出力例を示します。

```
Router# show ipv6 virtual-reassembly interface e1/1

Configuration Information:
---------------------------------
Virtual Fragment Reassembly (VFR) is ENABLED...
Maximum number of datagram that can be reassembled at a time: 64
Maximum number of fragments per datagram: 8
Timeout value of a datagram: 3 seconds

Statistical Information:
----------------------------
Number of datagram being reassembled:12
Number of fragments being processed:48
Total number of datagram reassembled:6950
Total number of datagram failed: 9
```

show logging コマンドの出力例

次の例では、**show logging** コマンドを使用して、list1 という名前のアクセス リストの最初の行（シーケンス 10）に一致するロギング エントリを表示します。

```
Router> show logging

00:00:36: %IPV6-6-ACCESSLOGP: list list1/10 permitted tcp 2001:0db8:1::1(11001)
(Ethernet0/0) -> 2001:0db8:1::2(179), 1 packet
```

clear ipv6 access-list コマンドの出力例

次の例では、**show ipv6 access-list** コマンドを使用して、list1 という名前のアクセス リスト用の一部の一致カウンタを表示します。**clear ipv6 access-list** コマンドを発行して、list1 という名前のアクセス リスト用の一致カウンタをリセットします。**show ipv6 access-list** コマンドを再度使用して、一致カウンタがリセットされたことを示します。

```
Router> show ipv6 access-list list1

IPv6 access list list1
    permit tcp any any log-input (6 matches) sequence 10
    permit icmp any any echo-request log-input sequence 20
    permit icmp any any echo-reply log-input sequence 30

Router# clear ipv6 access-list list1

Router# show ipv6 access-list list1

IPv6 access list list1
    permit tcp any any log-input sequence 10
    permit icmp any any echo-request log-input sequence 20
    permit icmp any any echo-reply log-input sequence 30
```

IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装の設定例

例：IPv6 ACL の作成および適用

例：Release 12.2(13)T または 12.0(23)S 用の IPv6 ACL の作成および適用

次に、Cisco IOS Release 12.2(13)T を実行しているルータの例を示します。

この例では、OUTBOUND および INBOUND という名前の 2 つの IPv6 ACL を設定し、両方の ACL をイーサネット インターフェイス 0 上の発信トラフィックと着信トラフィックに適用します。OUTBOUND リスト内の最初と 2 番めの許可エントリは、ネットワーク 2001:0DB8:0300:0201::/32 から送信されたすべての TCP および User Datagram Protocol（UDP; ユーザ データグラム プロトコル）パケットがイーサネット インターフェイス 0 から出て行くことを許可します。また、エントリは REFLECTOUT という名前の一時的な IPv6 リフレクシブ ACL を設定して、イーサネット インターフェイス 0 上で回帰（着信）TCP および UDP パケットをフィルタリングします。OUTBOUND リストの最初の拒否エントリは、ネットワーク fec0:0:0:0201::/64 から送信されたすべてのパケット（送信元 IPv6 アドレスの最初の 64 ビットとしてサイトローカル プレフィクス fec0:0:0:0201 を持つパケット）がイーサネット インターフェイス 0 から出て行くことを拒否します。

INBOUND リストの **evaluate** コマンドは、REFLECTOUT という名前の一時的な IPv6 リフレクシブ ACL をイーサネット インターフェイス 0 上の着信 TCP および UDP パケットに適用します。OUTBOUND リストによって発信 TCP または UDP パケットがイーサネット インターフェイス 0 上で許可された場合、INBOUND リストは REFLECTOUT リストを使用して、回帰（着信）TCP および UDP パケットを照合（評価）します。

```
ipv6 access-list OUTBOUND
 permit tcp 2001:0DB8:0300:0201::/32 any reflect REFLECTOUT
 permit udp 2001:0DB8:0300:0201::/32 any reflect REFLECTOUT
 deny fec0:0:0:0201::/64 any

ipv6 access-list INBOUND
 evaluate REFLECTOUT

interface ethernet 0
 ipv6 traffic-filter OUTBOUND out
 ipv6 traffic-filter INBOUND in
```

（注） OUTBOUND または INBOUND ACL の最後のエントリとして **permit any any** 文が含まれていないので、イーサネット インターフェイス 0 への出入りが許可されるのは、ACL に設定された許可エントリに一致する TCP と UDP パケット、および ACL 内の暗黙的な許可条件に一致する ICMP パケットだけになります（ACL の末尾にある暗黙的な deny all 条件は、インターフェイス上の他のすべてのパケット タイプを拒否します）。

次の例は、Cisco IOS Release 12.2(13)T または 12.0(23)S を実行するルータ上で実行できます。

次の例は、HTTP アクセスを日中の特定の時間に制限し、許可時間外のアクティビティを記録するように設定します。

```
time-range lunchtime
 periodic weekdays 12:00 to 13:00

ipv6 access-list OUTBOUND
 permit tcp any any eq www time-range lunchtime
 deny tcp any any eq www log-input
 permit tcp 2001:0DB8::/32 any
 permit udp 2001:0DB8::/32 any
```

例：12.2(11)T、12.0(22)S、または以前のリリース用の IPv6 ACL の作成および適用

次に、Cisco IOS Release 12.2(11)T、12.0(22)S、または以前のリリースを実行するルータでの例を示します。

この例では、list2 という名前の IPv6 ACL を設定し、その ACL をイーサネット インターフェイス 0 上の発信トラフィックに適用します。特に、最初の ACL エントリは、ネットワーク fec0:0:0:2::/64（送信元 IPv6 アドレスの最初の 64 ビットとしてサイトローカル プレフィクス fec0:0:0:2 を持つパケット）

がイーサネット インターフェイス 0 から出て行くことを拒否します。2 番めの ACL エントリは、その他のすべてのトラフィックがイーサネット インターフェイス 0 から出て行くことを許可します。2 番めのエントリは、各 IPv6 ACL の末尾に暗黙的な deny all 条件があるため、必要となります。

```
ipv6 access-list list2 deny fec0:0:0:2::/64 any
ipv6 access-list list2 permit any any

interface ethernet 0
 ipv6 traffic-filter list2 out
```

同じ設定が、Cisco IOS Release 12.2(13)T、12.0(23)S、または以降のリリースを実行しているルータで使用されていた場合、その設定は次のように IPv6 アクセス リスト コンフィギュレーション モードに変換されます。

```
ipv6 access-list list2
 deny ipv6 fec0:0:0:2::/64 any
 permit ipv6 any any

interface ethernet 0
 ipv6 traffic-filter list2 out
```

（注） IPv6 は、グローバル コンフィギュレーション モードから IPv6 アクセス リスト コンフィギュレーション モードに変換される **permit any any** 文および **deny any any** 文でプロトコル タイプとして自動的に設定されます。

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

例：TCP または UDP マッチングの設定

次の例では、AH の有無にかかわらず、すべての TCP トラフィックを許可しています。

```
IPv6 access list example1
    permit tcp any any
```

次の例では、AH ヘッダーが存在する場合にだけ TCP または UDP 解析を許可しています。AH が存在しない TCP または UDP トラフィックでは、マッチングは実行されません。

```
IPv6 access list example2
    deny tcp host 2001::1 any log sequence 5
    permit tcp any any auth sequence 10
    permit udp any any auth sequence 20
```

次の例では、認証ヘッダーを持つすべての IPv6 トラフィックを許可しています。

```
IPv6 access list example3
    permit ahp any any
```

例：Cisco IOS Firewall for IPv6 の設定

この Cisco IOS Firewall 設定例では、インバウンド フィルタおよびアウトバウンド フィルタを検査に使用し、アクセス リストを利用してトラフィックを管理しています。この検査メカニズムは、状態が維持される、既存のセッションの間有効なパケットに基づいて、戻されてくるトラフィックを許可する方法です。

```
enable
configure terminal
 ipv6 unicast-routing
  ipv6 inspect name ipv6_test icmp timeout 60
  ipv6 inspect name ipv6_test tcp timeout 60
  ipv6 inspect name ipv6_test udp timeout 60

interface FastEthernet0/0
  ipv6 address 3FFE:C000:0:7::/64 eui-64
  ipv6 enable
  ipv6 traffic-filter INBOUND out
  ipv6 inspect ipv6_test in

interface FastEthernet0/1
  ipv6 address 3FFE:C000:1:7::/64 eui-64
  ipv6 enable
  ipv6 traffic-filter OUTBOUND in

! This is used for 3745b connection to tftpboot server
interface FastEthernet4/0
  ip address 192.168.17.33 255.255.255.0
  duplex auto
  speed 100

ip default-gateway 192.168.17.8
! end of tftpboot server config

! Access-lists to deny everything except for Neighbor Discovery ICMP messages
ipv6 access-list INBOUND
  permit icmp any any nd-na
  permit icmp any any nd-ns
  deny ipv6 any any log

ipv6 access-list OUTBOUND
  permit icmp any any nd-na
  permit icmp any any nd-ns
  deny ipv6 any any log
```

例：Cisco IOS Zone-Based Firewall for IPv6 の設定

次に、ゾーンベースのファイアウォールをイネーブルにし、ルータを通過する IPv6 トラフィックの検査を実現する例を示します。

```
parameter-map type inspect v6-param-map
 sessions maximum 10000
 ipv6 routing-header-enforcement loose
!
!
class-map type inspect match-any v6-class
 match protocol tcp
 match protocol udp
 match protocol icmp
 match protocol ftp
```

```
!
!
policy-map type inspect v6-policy
 class type inspect v6-class
  inspect
!
zone security z1
zone security z2
!
zone-pair security zp source z1 destination z2
 service-policy type inspect v6-policy
```

その他の関連資料

関連資料

関連項目	参照先
IPv6 IPsec	『*Cisco IOS IPv6 Configuration Guide*』の「Implementing IPsec in IPv6 Security」
基本的な IPv6 設定	『*Cisco IOS IPv6 Configuration Guide*』の「Implementing IPv6 Addressing and Basic Connectivity」
ゾーンベースのファイアウォール	『*Cisco IOS Security Configuration Guide: Securing the Data Plane*』の「Zone-Based Policy Firewall」
IPv6 のサポート機能リスト	『*Cisco IOS IPv6 Configuration Guide*』の「Start Here: Cisco IOS Software Release Specifics for IPv6 Features」
IPv6 コマンド：コマンド構文、コマンド モード、デフォルト、使用上のガイドライン、および例	『*Cisco IOS IPv6 Command Reference*』

規格

規格	タイトル
この機能によってサポートされる新しい規格または変更された規格はありません。またこの機能による既存規格のサポートに変更はありません。	—

MIB

MIB	MIB リンク
• CISCO-UNIFIED-FIREWALL-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、および機能セットの MIB の場所を検索し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

RFC

RFC	タイトル
RFC 2401	『*Security Architecture for the Internet Protocol*』
RFC 2402	『*IP Authentication Header*』
RFC 2428	『*FTP Extensions for IPv6 and NATs*』
RFC 2460	『*Internet Protocol, Version 6 (IPv6) Specification*』
RFC 2474	『*Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*』
RFC 3576	『*Change of Authorization*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装の機能情報

表 1 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。

プラットフォームのサポートおよびソフトウェア 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 により、どのソフトウェア イメージが特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートするか調べることができます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連のソフトウェア リリースのうち、特定の機能が初めて導入されたソフトウェア リリースだけが記載されています。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。

表 1　IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装の機能情報

機能名	リリース	機能情報
IPv6 サービス：標準アクセス コントロール リスト	12.0(22)S 12.2(14)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(17a)SX1 12.2(2)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)S	アクセス リストによって、ルータ 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。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装の制約事項」（P.2） • 「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」（P.2） • 「Cisco IOS Firewall for IPv6 での PAM」（P.4） • 「IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装方法」（P.5） • 「IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装の設定例」（P.30）
IPv6 サービス：拡張アクセス コントロール リスト[1]	12.0(23)S 12.2(14)S 12.2(28)SB 12.2(25)SG 12.2(33)SRA 12.2(17a)SX1 12.2(13)T 12.3 12.3(2)T 12.4 12.4(2)T 15.0(1)S	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。 この機能に関する詳細については、次の各項を参照してください。 • 「IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装の制約事項」（P.2） • 「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」（P.2） • 「IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装方法」（P.5） • 「IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装の設定例」（P.30）
IPv6 サービス：IPv6 IOS ファイアウォール	12.3(7)T 12.4 12.4(2)T	この機能を使用すると、高度なトラフィック フィルタリング機能をネットワークのファイアウォールの不可欠な部分として組み込むことができます。 この機能に関する詳細については、次の各項を参照してください。 • 「Cisco IOS Firewall for IPv6」（P.3） • 「Cisco IOS Firewall for IPv6 の設定」（P.14）
IPv6 サービス：IPv6 IOS ファイアウォール FTP アプリケーション サポート	12.3(11)T 12.4 12.4(2)T	IPv6 は、この機能をサポートします。 この機能に関する詳細については、次の項を参照してください。 • 「Cisco IOS Firewall for IPv6」（P.3）

表 1　IPv6 セキュリティへのトラフィック フィルタおよびファイアウォールの実装の機能情報 （続き）

機能名	リリース	機能情報
IPsec 認証ヘッダー用の IPv6 ACL 拡張	12.4(20)T	IPsec 認証ヘッダー用の IPv6 ACL 拡張機能を使用すると、IPv6 IPsec 認証ヘッダーが存在する場合には、TCP または UDP 解析を実行できます。 この機能に関する詳細については、次の項を参照してください。 • 「IPsec 認証ヘッダーの IPv6 ACL 拡張」（P.2）
IOS ゾーンベース ファイアウォール	15.1(2)T	IPv6 トラフィックをサポートするために、Cisco IOS Zone-Based Firewall for IPv6 は Cisco IOS Zone-Based Firewall for IPv4 と共存します。 この機能に関する詳細については、次の各項を参照してください。 • 「Cisco IOS Zone-Based Firewall for IPv6」（P.5） • 「IPv6 でのゾーンベースのファイアウォールの設定」（P.19） • 「例：Cisco IOS Zone-Based Firewall for IPv6 の設定」（P.33）

1. IPv6 拡張アクセス コントロール リストおよび Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）を介した IPv6 プロバイダー エッジ ルータは、Cisco IOS Release 12.0(25)S 以降のリリースの Cisco IOS ルータでの Cisco 12000 シリーズ インターネット ルータ IP Service Engineer（ISE）ラインカード上のハードウェア アクセラレータを使用して実装されています。