IPv6 ファースト ホップ セキュリティの設定

IPv6 ファースト ホップ セキュリティの前提条件

必要な、IPv6 が有効になっている SDM テンプレートが設定されていること。

IPv6 ファースト ホップ セキュリティの制約事項

- 次の制限は、FHS ポリシーを EtherChannel インターフェイスに適用する場合に該当します（ポート チャネル）。
  - FHS ポリシーがアタッチされた物理ポートは EtherChannel グループに参加することができません。
  - FHS ポリシーは、EtherChannel グループのメンバーである場合に物理ポートにアタッチすることができません。
- デフォルトでは、スヌーピング ポリシーにはセキュリティ レベルのガードがあります。そのようなスヌーピングポリシーがアクセススイッチに設定されると、デバイスまたは DHCP サーバー/リレーに対応するアップリンクポートが信頼できるポートとして設定されていても、IPv6（DHCPv6）サーバーパケットに対する外部 IPv6 ルータアドバタイズメント（RA）または Dynamic Host Configuration Protocol はブロックされます。IPv6 RA または DHCPv6 サーバー メッセージを許可するには、次の手順を実行します。

- IPv6 RA ガードポリシー（RA の場合）または IPv6 DHCP ガードポリシー（DHCP サーバーメッセージの場合）をアップリンクポートに適用します。
- 低いセキュリティ レベルでスヌーピング ポリシーを設定します（たとえば、glean や inspect など）。ただし、FHS 機能の利点が有効でないため、このようなスヌーピング ポリシーでは、低いセキュリティレベルを設定することはお勧めしません。

IPv6 ファースト ホップ セキュリティに関する情報

IPv6 ファースト ホップ セキュリティの概要

IPv6 のファースト ホップ セキュリティ（FHS IPv6）は、ポリシーを物理インターフェイス、EtherChannel インターフェイス、または VLAN に適用できる一連の IPv6 セキュリティ機能です。IPv6 ソフトウェア ポリシー データベース サービスは、これらのポリシーを保存しアクセスします。ポリシーを設定または変更すると、ポリシー属性はソフトウェア ポリシー データベースで保存または更新され、その後指定したとおりに適用されます。次の IPv6 ポリシーが現在サポートされています。

- IPv6 スヌーピング ポリシー：IPv6 スヌーピング ポリシーは、IPv6 内の FHS で使用できるほとんどの機能をイネーブルにできるコンテナ ポリシーとして機能します。

（注） IPv6 スヌーピングポリシー機能は廃止され、Switch Integrated Security Features（SISF）ベースのデバイストラッキングに置き換わり、同じ機能が提供されます。IPv6 スヌーピング ポリシー コマンドは CLI で引き続き使用でき、既存の設定は引き続きサポートされますが、コマンドは今後のリリースで CLI から削除されます。代わりの機能の詳細については、このガイドの「*SISF* ベースのデバイス追跡の設定」を参照してください。

- IPv6 FHS バインディング テーブル コンテンツ：デバイスに接続された IPv6 ネイバーのデータベーステーブルはネイバー探索（ND）プロトコルスヌーピングなどの情報ソースから作成されます。このデータベースまたはバインディングテーブルは、リンク層アドレス（LLA）、IPv4 または IPv6 アドレス、およびスプーフィングやリダイレクト攻撃を防止するためにネイバーのプレフィックス バインディングを検証するために、さまざまな IPv6 ガード機能（IPv6 ND インスペクションなど）によって使用されます。

（注） IPv6 FHS バインディング テーブル コンテンツ機能は、SISF ベースのデバイストラッキングによってサポートされます。詳細については、このガイドの「*SISF* ベースのデバイス追跡の設定」を参照してください。

- IPv6 ネイバー探索検査：IPv6 ND 検査は、レイヤ 2 ネイバー テーブル内のステートレス自動設定アドレスのバインディングを学習し、保護します。IPv6 ND 検査は、信頼できるバインディング テーブル データベースを構築するためにネイバー探索メッセージを分析します。準拠していない IPv6 ネイバー探索メッセージは破棄されます。ND メッセージは、その IPv6 からメディア アクセス コントロール（MAC）へのマッピングが検証可能な場合に信頼できると見なされます。

  この機能によって、DAD、アドレス解決、ルータ ディスカバリ、ネイバー キャッシュに対する攻撃などの、ND メカニズムに固有の脆弱性のいくつかが軽減されます。

（注） Cisco IOS XE Amsterdam 17.1.1 以降、IPv6 ND インスペクション機能は廃止され、SISF ベースのデバイストラッキング機能に置き換えられ、同じ機能が提供されます。IPv6 ND 検査コマンドは CLI で引き続き使用でき、既存の設定は引き続きサポートされますが、コマンドは今後のリリースで CLI から削除されます。代わりの機能の詳細については、このガイドの「*SISF* ベースのデバイス追跡の設定」を参照してください。

- IPv6 ルータ アドバタイズメント ガード：IPv6 ルータアドバタイズメント（RA）ガード機能を使用すると、ネットワーク管理者は、ネットワーク デバイス プラットフォームに到着した不要または不正な RA ガードメッセージをブロックまたは拒否できます。RA は、リンクで自身をアナウンスするためにデバイスによって使用されます。RA ガード機能は、これらの RA を分析して、未承認のデバイスによって送信された偽の RA をフィルタリングして除外します。ホスト モードでは、ポートではルータ アドバタイズメントとルータ リダイレクト メッセージはすべて許可されません。RA ガード機能は、レイヤ 2 デバイスの設定情報を、受信した RA フレームで検出された情報と比較します。レイヤ 2 デバイスは、RA フレームとルータ リダイレクト フレームの内容を設定と照らし合わせて検証した後で、RA をユニキャストまたはマルチキャストの宛先に転送します。RA フレームの内容が検証されない場合は、RA は破棄されます。

- IPv6 DHCP ガード：IPv6 DHCP ガード機能は、承認されない DHCPv6 サーバーおよびリレー エージェントからの返信およびアドバタイズメント メッセージをブロックします。IPv6 DHCP ガードは、偽造されたメッセージがバインディング テーブルに入るのを防ぎ、DHCPv6 サーバーまたは DHCP リレーからデータを受信することが明示的に設定されていないポートで受信された DHCPv6 サーバー メッセージをブロックできます。この機能を使用するには、ポリシーを設定してインターフェイスまたは VLAN にアタッチします。DHCP ガードパケットをデバッグするには、**debug ipv6 snooping dhcp-guard** 特権 EXEC コマンドを使用します。

- IPv6 ソース ガード：IPv4 ソース ガードと同様、IPv6 ソース ガードは送信元アドレス スプーフィングを防ぐために、送信元アドレスまたはプレフィックスを検証します。

  ソース ガードでは、送信元または宛先アドレスに基づいてトラフィックを許可または拒否するようにハードウェアをプログラムします。ここでは、データ パケットのトラフィックのみを処理します。

IPv6 ソース ガード機能は、ハードウェア TCAM テーブルにエントリを格納し、ホストが無効な IPv6 送信元アドレスでパケットを送信しないようにします。

ソースガードパケットをデバッグするには、**debug ipv6 snooping source-guard** 特権 EXEC コマンドを使用します。

（注） IPv6 ソースガード機能およびプレフィックスガード機能は、入力方向でのみサポートされています。つまり、出力方向ではサポートされていません。

次の制約事項が適用されます。

- FHS ポリシーは、EtherChannel グループのメンバである場合に物理ポートに適用できません。
- IPv6 ソース ガードがスイッチ ポートで有効になっている場合は、そのスイッチ ポートが属するインターフェイスで NDP または DHCP スヌーピングを有効にする必要があります。そうしないと、このポートからのすべてのデータ トラフィックがブロックされます。
- IPv6 ソース ガード ポリシーを VLAN に適用することはできません。インターフェイス レベルのみでサポートされています。
- インターフェイスで IPv4 および IPv6 のソース ガードを一緒に設定する場合は、**ip verify source** の代わりに **ip verify source mac-check** の使用を推奨します。2 つの異なるフィルタリング ルール（IPv4（IP フィルタ）用と IPv6（IP-MAC フィルタ）用）が設定されているため、特定のポートの IPv4 接続が切断される可能性があります。
- IPv6 ソース ガードとプレフィックス ガードは同時に使用できません。ポリシーをインターフェイスに付加する際は、「アドレスを確認」するか「プレフィックスを確認」する必要はありますが、両方を確認する必要はありません。
- PVLAN と送信元/プレフィックスガードは同時に適用できません。
- IPv6 送信元ガードとプレフィックス ガードは EtherChannel でサポートされています。

- IPv6 プレフィックスガード：IPv6 プレフィックスガード機能は、IPv6 送信元ガード機能内で動作し、トポロジが正しくないアドレスから発信されたトラフィックをデバイスが拒否できるようにします。IPv6 プレフィックス ガードは、IPv6 プレフィックスが DHCP プレフィックス委任を使用してデバイス（ホーム ゲートウェイなど）に委任される場合によく使用されています。この機能は、リンクに割り当てられたアドレスの範囲を検出し、この範囲に入っていないアドレスを発信元とするトラフィックをブロックします。
- IPv6 宛先ガード：IPv6 宛先ガード機能は、IPv6 ネイバー探索で動作し、リンク上でアクティブであると認識されているアドレスについてのみ、デバイスがアドレスを解決します。アドレス グリーニング機能に依存して、リンク上でアクティブなすべての宛先をバインディング テーブルに挿入してから、バインディング テーブルで宛先が見つからなかったときに実行される解決をブロックします。

（注） IPv6 宛先ガードは、設定された SVI のレイヤ2 VLANに適用することをお勧めします。

IPv6 ファースト ホップ セキュリティの設定方法

IPv6 スヌーピング ポリシーの設定

（注） IPv6 スヌーピングポリシー機能は廃止されました。コマンドはCLIに表示され、設定できますが、代わりにスイッチ統合セキュリティ機能（SISF）ベースのデバイス追跡機能を使用することを推奨します。

IPv6 スヌーピング ポリシーを設定するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 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 snooping policy** *policy-name* 例： `Device(config)# ipv6 snooping policy example_policy`	スヌーピングポリシーを作成し、IPv6 スヌーピング ポリシー 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	{[**default**] | [**device-role** {**node** | **switch**}] | [**limit address-count** *value*] | [**no**] | [**protocol** {**dhcp** | **ndp**}] | [**security-level** {**glean** | **guard** | **inspect**}] | [**tracking** {**disable** [**stale-lifetime** [*seconds* | **infinite**] | **enable** [**reachable-lifetime** [*seconds* | **infinite**] }] | [**trusted-port**] }	データ アドレス グリーニングを有効にし、さまざまな条件に対してメッセージを検証し、メッセージのセキュリティ レベルを指定します。 • （任意）**default**：すべてをデフォルト オプションに設定します。

	コマンドまたはアクション	目的

	例：
	`Device(config-ipv6-snooping)# security-level inspect`
	例：
	`Device(config-ipv6-snooping)# trusted-port`
		• （任意）**device-role**{**node**]	**switch**}：ポートに接続されたデバイスの役割を指定します。デフォルトは **node** です。
			• （任意）**limit address-count** *value*：ターゲットごとに許可されるアドレス数を制限します。
			• （任意）**no**：コマンドを無効にするか、またはそのデフォルトに設定します。
			• （任意）**protocol**{**dhcp**|**ndp**}：分析のために、スヌーピング機能にどのプロトコルをリダイレクトするかを指定します。デフォルトは、**dhcp** および **ndp** です。デフォルトを変更するには、**no protocol** コマンドを使用します。
			• （任意）**security-level**{**glean**|**guard**|**inspect**}：この機能によって適用されるセキュリティのレベルを指定します。デフォルトは **guard** です。
			glean：メッセージからアドレスを収集し、何も確認せずにバインディング テーブルに入力します。
			guard：アドレスを収集し、メッセージを検査します。さらに、RA および DHCP サーバ メッセージを拒否します。これがデフォルトのオプションです。
			inspect：アドレスを収集し、メッセージの一貫性と準拠を検証して、アドレスの所有権を適用します。
			• （任意）**tracking** {**disable**|**enable**}：デフォルトの追跡動作を上書きし、追跡オプションを指定します。

	コマンドまたはアクション	目的
		• （任意）**trusted-port**：信頼できるポートを設定します。これにより、該当するターゲットに対するガードがディセーブルになります。信頼できるポートを経由して学習されたバインディングは、他のどのポートを経由して学習されたバインディングよりも優先されます。テーブル内にエントリを作成しているときに衝突が発生した場合、信頼できるポートが優先されます。
ステップ 5	**end** 例： `Device(config-ipv6-snooping)# end`	IPv6 スヌーピング ポリシー コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**show ipv6 snooping policy** *policy-name* 例： `Device#show ipv6 snooping policy example_policy`	スヌーピング ポリシー設定を表示します。

次のタスク

IPv6 スヌーピング ポリシーをインターフェイスまたは VLAN にアタッチします。

インターフェイスへの IPv6 スヌーピングポリシーの適用

インターフェイスまたはVLANにIPv6スヌーピング ポリシーをアタッチするには、特権EXECモードで次の手順を実行してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *interface_type stack/module/port* 例： `Device(config)# interface gigabitethernet 1/1/4`	インターフェイスのタイプおよび 識別子を指定し、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	**switchport** 例： `Device(config-if)# switchport`	switchport モードを開始します。 （注） インターフェイスがレイヤ 3 モードの場合に、レイヤ 2 パラメータを設定するには、パラメータを指定せずに **switchport** インターフェイス コンフィギュレーション コマンドを入力し、インターフェイスをレイヤ 2 モードにする必要があります。これにより、インターフェイスがいったんシャットダウンしてから再度イネーブルになり、インターフェイスが接続しているデバイスに関するメッセージが表示されることがあります。インターフェイスをレイヤ 3 モードからレイヤ 2 モードに変更した場合、影響のあるインターフェイスに関連する以前の設定情報が消失する可能性があり、インターフェイスはデフォルト設定に戻ります。 switchport コンフィギュレーション モードではコマンド プロンプトは（config-if）# と表示されます。
ステップ 5	**ipv6 snooping** [**attach-policy** *policy_name* [**vlan** {*vlan_id* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids*}] | **vlan** {*vlan_id* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] 例： `Device(config-if)# ipv6 snooping`	インターフェイスまたはそのインターフェイス上の特定の VLAN にカスタム IPv6 スヌーピングポリシーを適用します。デフォルトポリシーをインターフェイスにアタッチするには、**attach-policy** キーワードを指定せずに **ipv6 snooping** コマンドを使用します。デフォルト ポリシーをインターフェイス上の VLAN

	コマンドまたはアクション	目的
	Device(config-if)# **ipv6 snooping attach-policy example_policy** Device(config-if)# **ipv6 snooping vlan 111,112** Device(config-if)# **ipv6 snooping attach-policy example_policy vlan 111,112**	にアタッチするには、**ipv6 snooping vlan** コマンドを使用します。デフォルト ポリシーは、セキュリティ レベル **guard**、デバイス ロール **node**、プロトコル **ndp** および **dhcp** です。
ステップ 6	**end** 例： Device(config-if)# **end**	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： Device# **show running-config**	インターフェイス コンフィギュレーション モードを終了しないで、ポリシーが特定のインターフェイスにアタッチされていることを確認します。

レイヤ2EtherChannelインターフェイスへのIPv6スヌーピングポリシーの適用

EtherChannel インターフェイスまたは VLAN に IPv6 スヌーピング ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： Device> **enable**	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： Device# **configure terminal**	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface range** *interface_name* 例： Device(config)# **interface range Port-channel 11**	EtherChannel の作成時に割り当てられたポートチャネル インターフェイスの名前を指定します。インターフェイス範囲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
		ヒント　インターフェイスの名前とタイプを簡単に参照するには **show interfaces summary** コマンドを入力します。

ステップ 4	**ipv6 snooping** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]
	例：
	`Device(config-if-range)# ipv6 snooping attach-policy example_policy`
	`Device(config-if-range)# ipv6 snooping attach-policy example_policy vlan 222,223,224`
	`Device(config-if-range)# ipv6 snooping vlan 222, 223,224`
		IPv6 スヌーピング ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。

ステップ 5	**end** 例： `Device(config-if-range)# end`	インターフェイス範囲コンフィギュレーション モードを終了し、特権EXECモードに戻ります。
ステップ 6	**show running-config interface***portchannel_interface_name* 例： `Device# show running-config interface portchannel 11`	ポリシーが指定のインターフェイスに適用されていることを確認します。

VLAN への IPv6 スヌーピングポリシーのグローバル適用

複数のインターフェイス上の VLAN に IPv6 スヌーピング ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
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	**vlan configuration** *vlan_list* 例： `Device(config)# vlan configuration 333`	IPv6 スヌーピングポリシーを適用する VLAN を指定し、VLAN 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 snooping** [**attach-policy** *policy_name*] 例： `Device(config-vlan-config)#ipv6 snooping attach-policy example_policy`	すべてのデバイスインターフェイスで、指定した VLAN に IPv6 スヌーピングポリシーを適用します。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。デフォルト ポリシーは、セキュリティ レベル **guard**、デバイス ロール **node**、プロトコル **ndp** および **dhcp** です。
ステップ 5	**end** 例： `Device(config-vlan-config)# end`	VLAN インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IPv6 バインディング テーブルの内容の設定

IPv6 バインディング テーブル コンテンツを設定するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 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	[**no**] **ipv6 neighbor binding** [**vlan** *vlan-id* {*ipv6-address* **interface** interface_type *stack/module/port hw_address*	バインディング テーブル データベースにスタティック エントリを追加します。

	コマンドまたはアクション	目的
	[**reachable-lifetimevalue** [*seconds* | **default** | **infinite**] | [**tracking**{ [default | disable] [**reachable-lifetimevalue** [*seconds* | **default** | **infinite**] | [**enable** [**reachable-lifetimevalue** [*seconds* | **default** | **infinite**] | [**retry-interval** {*seconds*| **default** [**reachable-lifetimevalue** [*seconds* | **default** | **infinite**] }] 例： `Device(config)# ipv6 neighbor binding`	
ステップ 4	[**no**] **ipv6 neighbor binding max-entries** *number* [**mac-limit** *number* | **port-limit** *number* [**mac-limit** *number*] | **vlan-limit** *number* [[**mac-limit** *number*] | [**port-limit** *number* [**mac-limit***number*]]]] 例： `Device(config)# ipv6 neighbor binding max-entries 30000`	バインディング テーブル キャッシュに挿入できるエントリの最大数を指定します。
ステップ 5	**ipv6 neighbor binding logging** 例： `Device(config)# ipv6 neighbor binding logging`	バインディング テーブル メイン イベントのロギングを有効にします。
ステップ 6	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 7	**show ipv6 neighbor binding** 例： `Device# show ipv6 neighbor binding`	バインディング テーブルの内容を表示します。

IPv6 ネイバー探索インスペクションポリシーの設定

Cisco IOS XE Amsterdam 17.1.1 以降、IPv6 ND インスペクション機能は廃止され、SISF ベースのデバイストラッキング機能に置き換えられ、同じ機能が提供されます。対応する置き換えタスクについては、このドキュメントの「*SISF* ベースのデバイス追跡の設定」の章の「カスタム設定を使用したカスタム デバイス追跡ポリシーの作成」を参照してください。

特権 EXEC モードから、IPv6 ND インスペクション ポリシーを設定するには、次の手順に従ってください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 nd inspection policy** *policy-name* 例： `Device(config)# ipv6 nd inspection policy example_policy`	ND検査ポリシー名を指定し、ND検査ポリシー 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	**device-role** {**host** | **switch**} 例： `Device(config-nd-inspection)# device-role switch`	ポートに接続されているデバイスの役割を指定します。デフォルトは **host** です。
ステップ 5	**limit address-count** *value* 例： `Device(config-nd-inspection)# limit address-count 1000`	ポートで使用できる IPv6 アドレスの数を制限します。
ステップ 6	**tracking** {**enable** [**reachable-lifetime** {*value* | **infinite**}] | **disable** [**stale-lifetime** {*value* | **infinite**}]} 例： `Device(config-nd-inspection)# tracking disable stale-lifetime infinite`	ポートのデフォルトのデバイス追跡ポリシーを上書きします。
ステップ 7	**trusted-port** 例： `Device(config-nd-inspection)# trusted-port`	信頼できるポートにするポートを設定します。
ステップ 8	**validate source-mac** 例： `Device(config-nd-inspection)# validate source-mac`	送信元 Media Access Control（MAC）アドレスをリンク層アドレスと照合します。
ステップ 9	**no** {**device-role** | **limit address-count** | **tracking** | **trusted-port** | **validate source-mac**}	このコマンドの **no** 形式を使用してパラメータの現在の設定を削除します。

	コマンドまたはアクション	目的
	例： `Device(config-nd-inspection)# no validate source-mac`	
ステップ 10	**default** {**device-role** | **limit address-count** | **tracking** | **trusted-port** | **validate source-mac**} 例： `Device(config-nd-inspection)# default limit address-count`	設定をデフォルト値に戻します。
ステップ 11	**end** 例： `Device(config-nd-inspection)# end`	ND インスペクション ポリシー コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。
ステップ 12	**show ipv6 nd inspection policy** *policy_name* 例： `Device# show ipv6 nd inspection policy example_policy`	ND インスペクションの設定を確認します。

インターフェイスへの IPv6 ネイバー探索インスペクションポリシーの適用

Cisco IOS XE Amsterdam 17.1.1 以降、IPv6 ND インスペクション機能は廃止され、SISF ベースのデバイストラッキング機能に置き換えられ、同じ機能が提供されます。対応する置き換えタスクについては、このドキュメントの「*SISF* ベースのデバイス追跡の設定」の章の「デバイス追跡ポリシーのインターフェイスへの適用」を参照してください。

インターフェイスまたはそのインターフェイス上の VLAN に IPv6 ND 検査ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**interface** *interface-type interface-number* 例： `Device(config)# interface gigabitethernet 1/1/4`	インターフェイスのタイプおよび ID 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 nd inspection** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]
	例：
	`Device(config-if)# ipv6 nd inspection attach-policy example_policy`
	`Device(config-if)# ipv6 nd inspection attach-policy example_policy vlan 222,223,2`
	`Device(config-if)# ipv6 nd inspection vlan 222, 223,224`
		ネイバー探索検査ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。

ステップ 5	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

レイヤ2EtherChannelインターフェイスへのIPv6ネイバー探索インスペクションポリシーの適用

Cisco IOS XE Amsterdam 17.1.1 以降、IPv6 ND インスペクション機能は廃止され、SISF ベースのデバイストラッキング機能に置き換えられ、同じ機能が提供されます。対応する置き換えタスクについては、このドキュメントの「*SISF*ベースのデバイス追跡の設定」の章の「デバイス追跡ポリシーのインターフェイスへの適用」を参照してください。

EtherChannel インターフェイスまたは VLAN に IPv6 ネイバー探索検査ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
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	**interface range** *interface_name* 例： `Device(config)# interface range Port-channel 11`	EtherChannel の作成時に割り当てられたポートチャネル インターフェイスの名前を指定します。インターフェイス範囲コンフィギュレーション モードを開始します。 ヒント　インターフェイスの名前とタイプを簡単に参照するには **show interfaces summary** コマンドを入力します。

ステップ 4	**ipv6 nd inspection** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]
	例：
	`Device(config-if-range)# ipv6 nd inspection attach-policy example_policy`
	`Device(config-if-range)#ipv6 nd inspection vlan 222, 223,224`
	`Device(config-if-range)# ipv6 nd inspection attach-policy example_policy vlan 222,223,224`
		ND検査ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。

ステップ 5	**end** 例： `Device(config-if-range)# end`	インターフェイス範囲コンフィギュレーションモードを終了し、特権EXECモードに戻ります。

VLAN への IPv6 ネイバー探索インスペクションポリシーのグローバル適用

Cisco IOS XE Amsterdam 17.1.1 以降、IPv6 ND インスペクション機能は廃止され、SISF ベースのデバイストラッキング機能に置き換えられ、同じ機能が提供されます。対応する置き換えタスクについては、このドキュメントの「*SISF* ベースのデバイス追跡の設定」の「デバイス追跡ポリシーの *VLAN* への適用」を参照してください。

複数のインターフェイス上の VLAN に IPv6 ND 探索ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vlan configuration** *vlan_list* 例： `Device(config)# vlan configuration 334`	IPv6 スヌーピングポリシーを適用する VLAN を指定し、VLAN 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 nd inspection** [**attach-policy** *policy_name*] 例： `Device(config-vlan-config)#ipv6 nd inspection attach-policy example_policy`	すべてのスイッチおよびスタック インターフェイスで、IPv6 ネイバー探索ポリシーを指定した VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルトポリシーがアタッチされます。 デフォルトのポリシーは、device-role **host**、no drop-unsecure、limit address-count disabled、sec-level minimum is disabled、tracking is disabled、no trusted-port、no validate source-mac です。
ステップ 5	**end** 例： `Device(config-vlan-config)# end`	VLAN インターフェイス コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

IPv6 ルータ アドバタイズメント ガード ポリシーの設定

IPv6 ルータ アドバタイズメント ポリシーを設定するには、特権 EXEC モードで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：	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
	`Device> enable`	プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 nd raguard policy** *policy-name* 例： `Device(config)# ipv6 nd raguard policy example_policy`	RA ガードポリシー名を指定し、RA ガードポリシー 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**]**device-role** {**host** | **monitor** | **router** | **switch**} 例： `Device(config-nd-raguard)# device-role switch`	ポートに接続されているデバイスの役割を指定します。デフォルトは **host** です。 （注） ホスト側ポートとルータ側ポートの両方を備えたネットワークでは、ホスト側ポートまたは VLAN で **device-role host** を設定した RA ガードポリシーとともに、RA ガード機能が適切に動作できるように、ルータ側のポートで **device-role router** を設定した RA ガードポリシーを設定することが必須です。
ステップ 5	**hop-limit** {**maximum** | **minimum**} *value* 例： `Device(config-nd-raguard)# hop-limit maximum 33`	ホップ制限値によるルータアドバタイズメントメッセージのフィルタリングを有効にします。不正 RA メッセージは低いホップ制限値（IPv4 の Time to Live と同じ）を持つ可能性があるため、ホストによって受け入れられると、ホストが不正 RA メッセージ ジェネレータを超えて宛先にトラフィックを生成することができなくなります。指定されていないホップ制限値を持つ RA メッセージはブロックされます。 （1 ～ 255）最大および最小のホップ制限値の範囲。 設定されていない場合、このフィルタは無効になります。「**minimum**」を設

	コマンドまたはアクション	目的
		定して、指定する値より低いホップ制限値を持つ RA メッセージをブロックします。「**maximum**」を設定して、指定する値より高いホップ制限値を持つ RA メッセージをブロックします。
ステップ 6	**managed-config-flag** {**off** | **on**} 例： `Device(config-nd-raguard)# managed-config-flag on`	管理アドレス設定（「M」フラグ）フィールドに基づいてルータ アドバタイズメント メッセージのフィルタリングを有効にします。「M」フィールドが 1 の不正 RA メッセージの結果としてホストが不正 DHCPv6 サーバーを使用する場合があります。設定されていない場合、このフィルタは無効になります。 **On**：「M」値が 1 の RA メッセージを受け入れて転送し、0 のものをブロックします。 **Off**：「M」値が 0 の RA メッセージを受け入れて転送し、1 のものをブロックします。
ステップ 7	**match** { **ipv6 access-list** *list* | **ra prefix-list** *list*} 例： `Device(config-nd-raguard)# match ipv6 access-list example_list`	指定したプレフィックス リストまたはアクセス リストと照合します。
ステップ 8	**other-config-flag** {**on** | **off**} 例： `Device(config-nd-raguard)# other-config-flag on`	その他の設定（「O」フラグ）フィールドに基づくルータ アドバタイズメント メッセージのフィルタリングを有効にします。「O」フィールドが 1 の不正 RA メッセージの結果としてホストが不正 DHCPv6 サーバーを使用する場合があります。設定されていない場合、このフィルタは無効になります。 **On**：「O」値が 1 の RA メッセージを受け入れて転送し、0 のものをブロックします。 **Off**：「O」値が 0 の RA メッセージを受け入れて転送し、1 のものをブロックします。

	コマンドまたはアクション	目的
ステップ 9	[**no**]**router-preference maximum** {**high** | **medium** | **low**} 例： `Device(config-nd-raguard)# router-preference maximum high`	「Router Preference」フラグを使用したルータ アドバタイズメント メッセージのフィルタリングを有効にします。設定されていない場合、このフィルタはディセーブルになります。 • **high**：「Router Preference」が「high」、「medium」、または「low」に設定された RA メッセージを受け入れます。 • **medium**：「Router Preference」が「high」に設定された RA メッセージをブロックします。 • **low**：「Router Preference」が「medium」または「high」に設定された RA メッセージをブロックします。
ステップ 10	**trusted-port** 例： `Device(config-nd-raguard)# trusted-port`	信頼できるポートとして設定すると、すべての接続デバイスが信頼され、より詳細なメッセージ検証は実行されません。
ステップ 11	**default** {**device-role** | **hop-limit** {**maximum** | **minimum**} | **managed-config-flag** | **match** {**ipv6 access-list** | **ra prefix-list** } | **other-config-flag** | **router-preference maximum**| **trusted-port**} 例： `Device(config-nd-raguard)# default hop-limit`	コマンドをデフォルト値に戻します。
ステップ 12	**end** 例： `Device(config-nd-raguard)# end`	RA ガード ポリシー コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 13	**show ipv6 nd raguard policy** *policy_name* 例： `Device# show ipv6 nd raguard policy example_policy`	（任意）ND ガードポリシーの設定を表示します。

インターフェイスへの IPv6 ルータ アドバタイズメント ガード ポリシーの適用

インターフェイスまたはそのインターフェイス上の VLAN に IPv6 ルータ アドバタイズメント ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface gigabitethernet 1/1/4`	インターフェイスのタイプおよび ID 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 nd raguard** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]
	例：
	`Device(config-if)# ipv6 nd raguard attach-policy example_policy`
	`Device(config-if)# ipv6 nd raguard attach-policy example_policy vlan 222,223,224`
	`Device(config-if)# ipv6 nd raguard vlan 222, 223,224`
		ネイバー探索検査ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。

ステップ 5	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

レイヤ 2 EtherChannel インターフェイスへの IPv6 ルータ アドバタイズメント ガード ポリシーの適用

EtherChannel インターフェイスまたは VLAN に IPv6 ルータ アドバタイズメント ガード ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface range** *type number* 例： `Device(config)# interface Port-channel 11`	EtherChannel の作成時に割り当てられたポートチャネル インターフェイスの名前を指定します。インターフェイス範囲コンフィギュレーション モードを開始します。 ヒント　インターフェイス名やタイプを簡単に参照するには **show interfaces summary** コマンドを特権 EXEC モードで使用します。

ステップ 4	**ipv6 nd raguard** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]
	例：
	`Device(config-if-range)# ipv6 nd raguard attach-policy example_policy`
	`Device(config-if-range)# ipv6 nd raguard attach-policy example_policy vlan 222,223,224`
	`Device(config-if-range)# ipv6 nd raguard vlan 222, 223,224`
		RA ガード ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。

ステップ 5	**end** 例： `Device(config-if-range)# end`	インターフェイス範囲コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

VLAN への IPv6 ルータ アドバタイズメント ガード ポリシーのグローバル適用

インターフェイスに関係なく VLAN に IPv6 ルータ アドバタイズメント ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vlan configuration** *vlan_list* 例： `Device(config)# vlan configuration 335`	IPv6 RA ガードポリシーを適用する VLAN を指定し、VLAN 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 dhcp guard** [**attach-policy** *policy_name*] 例： `Device(config-vlan-config)# ipv6 nd raguard attach-policy example_policy`	すべてのスイッチおよびスタック インターフェイスで、IPv6 RA ガード ポリシーを指定した VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 5	**end** 例： `Device(config-vlan-config)# end`	VLAN インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

IPv6 DHCP ガードポリシーの設定

IPv6 DHCP（DHCPv6）ガード ポリシーを設定するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 dhcp guard policy** *policy-name* 例： `Device(config)# ipv6 dhcp guard policy example_policy`	DHCPv6 ガード ポリシー名を指定し、DHCPv6 ガード ポリシー 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	**device-role** {**client** | **server**} 例： `Device(config-dhcp-guard)# device-role server`	（任意）特定の役割のデバイスからのものではないポート上の DHCPv6 応答および DHCPv6 アドバタイズメントをフィルタします。デフォルトは **client** です。 • **client**：デフォルト値。適用されたデバイスがクライアントであることを指定します。サーバー メッセージにはこのポートで破棄されます。 • **server**：適用されたデバイスが DHCPv6 サーバーであることを指定します。このポートでは、サーバー メッセージが許可されます。

ステップ 5	**match server access-list** *ipv6-access-list-name*
	例：
	`;;Assume a preconfigured IPv6 Access List as follows:`
	`Device(config)# ipv6 access-list my_acls`
	`Device(config-ipv6-acl)# permit host 2001:BD8:::1 any`
	
	`;;configure DCHPv6 Guard to match approved access list.`
	`Device(config-dhcp-guard)# match server access-list my_acls`
		（任意）。アドバタイズされた DHCPv6 サーバーまたはリレーアドレスが認証されたサーバーのアクセスリストからのものであることの確認を有効にします（アクセスリストの宛先アドレスは「any」です）。設定されていない場合、このチェックは回避されます。空のアクセス リストは、permit all として処理されます。

ステップ 6	**match reply prefix-list** *ipv6-prefix-list-name*
	例：
	
	`;;Assume a preconfigured IPv6 prefix list as follows:`
	`Device(config)# ipv6 prefix-list my_prefix permit 2001:DB8::/64 le 128`
	
	`;; Configure DCHPv6 Guard to match prefix`
	`Device(config-dhcp-guard)# match reply prefix-list my_prefix`
		（任意）DHCPv6 応答メッセージ内のアドバタイズされたプレフィクスが設定された承認プレフィクスリストからのものであることの確認を有効にします。設定されていない場合、このチェックは回避されます。空のプレフィクス リストは、permit として処理されます。

	コマンドまたはアクション	目的

ステップ 7	**preference**{ **max** *limit* | **min** *limit* }
	例：
	`Device(config-dhcp-guard)# preference max 250`
	`Device(config-dhcp-guard)#preference min 150`
		device-role が **server** である場合に **max** および **min** を設定して、DHCPv6 サーバーアドバタイズメント値をサーバー優先度値に基づいてフィルタします。デフォルトではすべてのアドバタイズメントが許可されます。
		max *limit*：（0 ～ 255）（任意）アドバタイズされたプリファレンス（[preference] オプション内）が指定された制限未満であるかどうかの検証を有効にします。デフォルトは 255 です。設定されていない場合、このチェックは回避されます。
		min *limit*：（0 ～ 255）（任意）アドバタイズされたプリファレンス（[preference] オプション内）が指定された制限を超過しているかどうかの検証を有効にします。デフォルトは 0 です。設定されていない場合、このチェックは回避されます。

ステップ 8	**trusted-port** 例： `Device(config-dhcp-guard)# trusted-port`	（任意）**trusted-port**：ポートを信頼モードに設定します。このポートでは、これ以上のポリシングは実行されません。 （注） 信頼できるポートを設定した場合、device-role オプションは使用できません。
ステップ 9	**default** {**device-role** | **trusted-port**} 例： `Device(config-dhcp-guard)# default device-role`	（任意）**default**：コマンドをデフォルトに設定します。
ステップ 10	**end** 例： `Device(config-dhcp-guard)# end`	DHCPv6 ガードポリシー コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 11	**show ipv6 dhcp guard policy** *policy_name* 例： `Device# show ipv6 dhcp guard policy example_policy`	（任意）IPv6 DHCP ガードポリシーの設定を表示します。*policy_name* 変数を省略すると、すべての DHCPv6 ポリシーが表示されます。

インターフェイスまたはインターフェイス上の VLAN への IPv6 DHCP ガードポリシーの適用

IPv6 バインディング テーブル コンテンツを設定するには、特権 EXEC モードで次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface gigabitethernet 1/1/4`	インターフェイスのタイプおよび識別子を指定し、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 dhcp guard** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]
	例：
	`Device(config-if)# ipv6 dhcp guard attach-policy example_policy`
	`Device(config-if)# ipv6 dhcp guard attach-policy example_policy vlan 222,223,224`
	`Device(config-if)# ipv6 dhcp guard vlan 222, 223,224`
		DHCP ガード ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。

ステップ 5	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

レイヤ 2 EtherChannel インターフェイスへの IPv6 DHCP ガードポリシーの適用

EtherChannel インターフェイスまたは VLAN に IPv6 DHCP ガード ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface range** *Interface_name* 例： `Device(config)# interface Port-channel 11`	EtherChannel の作成時に割り当てられたポート チャネル インターフェイスの名前を指定します。インターフェイス範囲コンフィギュレーション モードを開始します。 ヒント　インターフェイス名やタイプを簡単に参照するには **show interfaces summary** コマンドを特権 EXEC モードで使用します。

ステップ 4	**ipv6 dhcp guard** [**attach-policy** *policy_name* [**vlan** {*vlan_ids* | **add** *vlan_ids* | **except** *vlan_ids* | **none** | **remove** *vlan_ids* | **all**}] | **vlan** [{*vlan_ids* | **add** *vlan_ids* | **except***vlan_ids* | **none** | **remove** *vlan_ids* | **all**}]
	例：
	`Device(config-if-range)# ipv6 dhcp guard attach-policy example_policy`
	`Device(config-if-range)# ipv6 dhcp guard attach-policy example_policy vlan 222,223,224`
	`Device(config-if-range)# ipv6 dhcp guard vlan 222, 223,224`
		DHCP ガード ポリシーをインターフェイスまたはそのインターフェイス上の特定の VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。

ステップ 5	**end** 例： `Device(config-if-range)# end`	インターフェイス範囲コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

VLAN への IPv6 DHCP ガードポリシーのグローバル適用

複数のインターフェイス上の VLAN に IPv6 DHCP のガード ポリシーをアタッチするには、特権 EXEC モードで次の手順を実行してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**vlan configuration** *vlan_list* 例： `Device(config)# vlan configuration 334`	IPv6 スヌーピングポリシーを適用する VLAN を指定し、VLAN 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 dhcp guard** [**attach-policy** *policy_name*] 例： `Device(config-vlan-config)# ipv6 dhcp guard attach-policy example_policy`	すべてのスイッチおよびスタック インターフェイスで、IPv6 ネイバー探索ポリシーを指定した VLAN にアタッチします。**attach-policy** オプションを使用しない場合、デフォルトポリシーがアタッチされます。デフォルト ポリシーは、device-role **client**、**no** trusted-port です。
ステップ 5	**end** 例： `Device(config-vlan-config)# end`	VLAN インターフェイス コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。

IPv6 ソース ガードの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 source-guard policy** *policy_name* 例：	IPv6 ソース ガード ポリシー名を指定し、IPv6 ソース ガード ポリシー コン

	コマンドまたはアクション	目的
	`Device(config)# ipv6 source-guard policy example_policy`	フィギュレーション モードを開始します。
ステップ 4	[**deny global-autoconf**] [**permit link-local**] [**default**{. . . }] [**exit**] [**no**{. . . }] 例： `Device(config-sisf-sourceguard)# deny global-autoconf`	（任意）IPv6 ソース ガード ポリシーを定義します。 • **deny global-autoconf**：自動設定されたグローバルアドレスからのデータトラフィックを拒否します。これは、リンク上のすべてのグローバルアドレスが DHCP によって割り当てられている際に、管理者が、自己設定されたアドレスを持つホストによるトラフィックの送信をブロックしたい場合に役立ちます。 • **permit link-local**：リンクローカルアドレスから送信されたすべてのデータトラフィックを許可します。 （注） ソース ガード ポリシーでは trusted オプションはサポートされません。
ステップ 5	**end** 例： `Device(config-sisf-sourceguard)# end`	IPv6 ソース ガード ポリシー コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 6	**show ipv6 source-guard policy** *policy_name* 例： `Device# show ipv6 source-guard policy example_policy`	ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。

次のタスク

インターフェイスに IPv6 ソース ガード ポリシーを適用します。

インターフェイスへの IPv6 ソースガードポリシーの適用

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードを有効にします。

	コマンドまたはアクション	目的
	`Device> enable`	プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface gigabitethernet 1/1/4`	インターフェイスのタイプおよび識別子を指定し、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 source-guard** [**attach-policy** <*policy_name*>] 例： `Device(config-if)# ipv6 source-guard attach-policy example_policy`	インターフェイスに IPv6 ソース ガード ポリシーをアタッチします。 **attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 5	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**show ipv6 source-guard policy** *policy_name* 例： `Device#(config)# show ipv6 source-guard policy example_policy`	ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。

レイヤ 2 EtherChannel インターフェイスへの IPv6 ソースガードポリシーの適用

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface port-channel** *port-channel-number* 例：	インターフェイスのタイプとポート番号を指定し、スイッチをポート チャネル

	コマンドまたはアクション	目的
	`Device(config)# interface Port-channel 4`	コンフィギュレーション モードにします。
ステップ 4	**ipv6 source-guard** [**attach-policy** <*policy_name*>] 例： `Device(config-if)# ipv6 source-guard attach-policy example_policy`	インターフェイスに IPv6 ソース ガード ポリシーをアタッチします。 **attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 5	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**show ipv6 source-guard policy** *policy_name* 例： `Device# show ipv6 source-guard policy example_policy`	ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。

IPv6 プレフィックス ガードの設定

（注） プレフィックスガードが適用されている場合にリンクローカルアドレスから送信されたルーティングプロトコル制御パケットを許可するには、ソースガード ポリシー コンフィギュレーション モードで **permit link-local** コマンドを有効にします。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 source-guard policy** *source-guard-policy* 例： `Device(config)# ipv6 source-guard policy my_snooping_policy`	IPv6 ソースガード ポリシー名を定義して、スイッチ統合セキュリティ機能のソースガード ポリシー 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 4	**validate address** 例： `Device(config-sisf-sourceguard)# no validate address`	アドレス検証機能を無効にし、IPv6 プレフィックス ガード機能を設定できるようにします。
ステップ 5	**validate prefix** 例： `Device(config-sisf-sourceguard)# validate prefix`	IPv6 プレフィックスガード動作を実行するよう、IPv6 ソースガードを有効にします。
ステップ 6	**exit** 例： `Device(config-sisf-sourceguard)# exit`	スイッチ統合セキュリティ機能のソースガード ポリシー コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 7	**show ipv6 source-guard policy** [*source-guard-policy*] 例： `Device# show ipv6 source-guard policy policy1`	IPv6 ソースガード ポリシー設定を表示します。

インターフェイスへの IPv6 プレフィックス ガード ポリシーの適用

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface gigabitethernet 1/1/4`	インターフェイスのタイプおよび識別子を指定し、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 source-guard attach-policy** *policy_name* 例：	インターフェイスに IPv6 ソース ガード ポリシーをアタッチします。 **attach-policy** オプションを使用しない場

	コマンドまたはアクション	目的
	`Device(config-if)# ipv6 source-guard attach-policy example_policy`	合、デフォルト ポリシーがアタッチされます。
ステップ 5	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**show ipv6 source-guard policy** *policy_name* 例： `Device(config-if)# show ipv6 source-guard policy example_policy`	ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。

レイヤ 2 EtherChannel インターフェイスへの IPv6 プレフィックス ガード ポリシーの適用

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface port-channel** *port-channel-number* 例： `Device(config)# interface Port-channel 4`	インターフェイスのタイプとポート番号を指定し、スイッチをポート チャネル コンフィギュレーション モードにします。
ステップ 4	**ipv6 source-guard** [**attach-policy** <*policy_name*>] 例： `Device(config-if)# ipv6 source-guard attach-policy example_policy`	インターフェイスに IPv6 ソース ガード ポリシーをアタッチします。 **attach-policy** オプションを使用しない場合、デフォルト ポリシーがアタッチされます。
ステップ 5	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**show ipv6 source-guard policy** *policy_name* 例： `Device(config)# show ipv6 source-guard policy example_policy`	ポリシー設定と、そのポリシーが適用されるすべてのインターフェイスを表示します。

IPv6 ファースト ホップ セキュリティの設定例

例：IPv6 DHCP ガードポリシーの設定

DHCPv6 ガード設定の例

```
Device> enable
Device# configure terminal
Device(config)# ipv6 access-list acl1
Device(config-ipv6-acl)# permit host 2001:DB8:0000:
0000:0000:0000:0000:0001 any
Device(config-ipv6-acl)# exit
Device(config)# ipv6 prefix-list abc permit 2001:0DB8::/64 le 128
Device(config)# ipv6 dhcp guard policy pol1
Device(config-dhcp-guard)# device-role server
Device(config-dhcp-guard)# match server access-list acl1
Device(config-dhcp-guard)# match reply prefix-list abc
Device(config-dhcp-guard)# preference min 0
Device(config-dhcp-guard)# preference max 255
Device(config-dhcp-guard)# trusted-port
Device(config-dhcp-guard)# exit
Device(config)# interface GigabitEthernet 0/2/0
Device(config-if)# switchport
Device(config-if)# ipv6 dhcp guard attach-policy pol1 vlan add 1
Device(config-if)# exit
Device(config)# vlan 1
Device(config-vlan)# ipv6 dhcp guard attach-policy pol1
Device(config-vlan)# end
```

例：レイヤ 2 EtherChannel インターフェイスへの IPv6 ソースガードポリシーの適用

次の例は、IPv6 ソース ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 source-guard policy POL
Device(config-sisf-sourceguard) # validate address
Device(config-sisf-sourceguard)# exit
Device(config)# interface Port-Channel 4
Device(config-if)# ipv6 snooping
```

```
Device(config-if)# ipv6 source-guard attach-policy POL
Device(config-if)# end
Device#
```

例：レイヤ 2 EtherChannel インターフェイスへの IPv6 プレフィックス ガード ポリシーの適用

次の例は、IPv6 プレフィックス ガード ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# ipv6 source-guard policy POL
Device (config-sisf-sourceguard)# no validate address
Device((config-sisf-sourceguard)# validate prefix
Device(config-sisf-sourceguard)# exit
Device(config)# interface Po4
Device(config-if)# ipv6 snooping
Device(config-if)# ipv6 source-guard attach-policy POL

Device(config-if)# end
```

IPv6 ファースト ホップ セキュリティに関する追加情報

関連資料

関連項目	マニュアル タイトル
SISF	『セキュリティ コンフィギュレーション ガイド』の「SISF ベースのデバイス トラッキングの設定」

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 ファースト ホップ セキュリティの機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

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

リリース	機能	機能情報
Cisco IOS XE Everest 16.5.1a	IPv6 ファースト ホップ セキュリティ	IPv6 のファースト ホップ セキュリティは、ポリシーを物理インターフェイス、EtherChannel インターフェイス、または VLAN に適用できる一連の IPv6 セキュリティ機能です。IPv6 ソフトウェア ポリシー データベース サービスは、これらのポリシーを保存しアクセスします。ポリシーを設定または変更すると、ポリシー属性はソフトウェア ポリシー データベースに保存または更新され、その後指定したとおりに適用されます。 IPv6 スヌーピング ポリシー機能は廃止されました。コマンドは CLI に表示され、設定できますが、代わりにスイッチ統合セキュリティ機能（SISF）ベースのデバイス追跡機能を使用することを推奨します。
Cisco IOS XE Amsterdam 17.1.1	IPv6 ND 検査	このリリース以降、IPv6 ND インスペクション機能は廃止され、SISF ベースのデバイス トラッキング機能に置き換えられ、同じ機能が提供されます。IPv6 ND 検査コマンドは CLI で引き続き使用でき、既存の設定は引き続きサポートされますが、コマンドは今後のリリースで CLI から削除されます。代わりの機能の詳細については、このガイドの「*SISF* ベースのデバイス追跡の設定」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ソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn [英語] からアクセスします。

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。