IPv6 ファースト ホップ セキュリティの設定

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、使用するプラットフォームおよびソフトウェア リリースの Bug Search Tool およびリリース ノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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

IPv6 でのファースト 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。

- **mls qos** コマンドを使用して CoPP ポリシーを設定する前に、スイッチで QoS を有効にする必要があります。

IPv6 でのファースト 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、ルータまたは 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）。しかし、ファースト ホップ セキュリティ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。
- CSCvk32439 で報告された制限により、IPv6 SISF ベースのデバイス トラッキング ポリシーを使用した CoPP ポリシーには、次の制限が適用されます。
  - スイッチで IPv6 SISF ポリシーが設定されている場合、IPv6 NDP トラフィックを制限するには CoPP ポリシーが必要です。
  - NDP CoPP ポリシーが設定された後、制限されたトラフィックが CPU にヒットします。接続されているエンドポイントの合計に対応するには、NDP CoPP ポリシーの数を、スタック内の各スイッチに接続するユーザーの数よりわずかに多くする必要があります。スイッチに接続されているエンドポイントの数よりも少ない NDP CoPP ポリシーを設定すると、エンドポイントへの IP 割り当ては遅延しますが、完全に無視されるわけではありません。

（注） たとえば、5 つのスイッチのスタックに約 300 のユーザーがいる場合、NDP CoPP ポリシーは 300 を超える必要があります。

- DHCPv6（サーバーからクライアントおよびクライアントからサーバー）CoPP ポリシーは、Lightweight DHCPv6 リレーエージェント（LDRA）がスイッチの IPv6 SISF ベースのデバイス トラッキング ポリシーで設定されている場合にのみ必要です。

IPv6 でのファースト ホップ セキュリティに関する情報

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、または VLAN にアタッチできる一連の 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。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有効にできるコンテナ ポリシーとして機能します。
- IPv6 FHS バインディング テーブルの内容：スイッチに接続された 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 検査など）によって使用されます。
- 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。
- 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 スイッチ 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ルータ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、未承認のルータ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。

  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。

  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。
  - 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 送信元ガードの詳細については、Cisco.comで『Cisco IOS IPv6 Configuration Guide Library』の「IPv6 Source Guard」の章を参照してください。

- IPv6 プレフィックス ガード：IPv6 プレフィックス ガードは、IPv6 送信元ガード機能内で動作し、デバイスがトポロジに不正なアドレスから発信されたトラフィックを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 プレフィックス ガードの詳細については、Cisco.comで『Cisco IOS IPv6 Configuration Guide Library』の「IPv6 Prefix Guard」の章を参照してください。

- 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。

  IPv6 宛先ガードに関する詳細については、Cisco.comで『Cisco IOS IPv6 Configuration Guide Library』の「IPv6 Destination Guard」の章を参照してください。

- IPv6 ネイバー検索マルチキャスト抑制：IPv6 ネイバー検索マルチキャスト抑制機能は、IPv6 のスヌーピング機能で、スイッチまたはワイヤレス コントローラで実行し、適切なリンク動作に必要な制御トラフィック量を削減するために使用されます。

- DHCPv6 リレー：Lightweight DHCPv6 リレー エージェント：Lightweight DHCPv6 リレー エージェント機能を使用するとリンクレイヤブリッジング（非ルーティング）機能を実行するアクセス ノードによってリレーエージェント情報が挿入されます。Lightweight DHCPv6 リレー エージェント（LDRA）機能は、DSL アクセス マルチプレクサ（DSLAM）や IPv6 制御やルーティング機能をサポートしないイーサネット スイッチなどの既存のアクセス ノードに実装できます。LDRA を使用して、DHCP バージョン 6（DHCPv6）メッセージ交換にリレーエージェント オプションを挿入して、主にクライアント側のインターフェイスを特定します。LDRA 機能は、インターフェイスと VLAN でイネーブルにできます。

（注） LDRA デバイスがクライアントに直接接続されている場合は、サーバー側で特定のサブネットまたはリンク情報を取得するために、インターフェイスにプール設定が必要です。この場合、LDRA デバイスが異なるサブネットまたはリンクに存在する場合、サーバーは正しいサブネットを取得できない場合があります。インターフェイスでプール名を設定して、クライアントに適切なサブネットまたはリンクを選択できるようになりました。

DHCPv6 リレーの詳細については、『IP Addressing: DHCP Configuration Guide, Cisco IOS Release 15.1SG』の「DHCPv6 Relay—Lightweight DHCPv6 Relay Agent」の項を参照してください。

IPv6 スヌーピング ポリシーの設定方法

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。

手順の概要

1. **configure terminal**

2. **ipv6 snooping policy** *policy-name*
3. {[**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**] }
4. **end**
5. **show ipv6 snooping policy** *policy-name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **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 2	**ipv6 snooping policy** *policy-name* 例： スイッチ(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 モードに移行します。
ステップ 3	{[**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**] } 例： スイッチ**(config-ipv6-snooping)# security-level inspect** 例： スイッチ**(config-ipv6-snooping)# 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。 • （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。

	コマンドまたはアクション	目的
		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。 • （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 4	**end** 例： `スイッチ(config-ipv6-snooping)# exit`	コンフィギュレーション モードから特権 EXEC モードに戻ります。
ステップ 5	**show ipv6 snooping policy** *policy-name* 例： `スイッチ#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。

IPv6 スヌーピング ポリシーをインターフェイスにアタッチする方法

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。

手順の概要

1. **configure terminal**

2. **interface** Interface_type *stack/module/port*
3. **switchport**
4. **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**}]
5. **do show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# 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 2	**interface** Interface_type *stack/module/port* 例： `スイッチ(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 3	**switchport** 例： `スイッチ(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有効になり、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。レイヤ 3 モードのインターフェイスをレイヤ 2 モードにした場合、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 4	**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：	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 ポリシーをアタッチします。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

	コマンドまたはアクション	目的
	スイッチ(config-if)# **ipv6 snooping** or スイッチ(config-if)# **ipv6 snooping attach-policy example_policy** or スイッチ(config-if)# **ipv6 snooping vlan 111,112** or スイッチ(config-if)# **ipv6 snooping attach-policy example_policy vlan 111,112**	す。デフォルト ポリシーをインターフェイス上の VLAN 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 5	**do show running-config** 例： スイッチ#(config-if)# **do 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。

IPv6 スヌーピング 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

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	**configure terminal** 例： スイッチ# **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 2	**interface range** *Interface_name* 例： スイッチ(config)# **interface range Po11**	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 **do show interfaces summary** コマンドを使用します。
ステップ 3	**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**}]	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。

	コマンドまたはアクション	目的
	例： スイッチ(config-if-range)# **ipv6 snooping attach-policy example_policy** or スイッチ(config-if-range)# **ipv6 snooping attach-policy example_policy vlan 222,223,224** **or** スイッチ(config-if-range)#**ipv6 snooping vlan 222, 223,224**	
ステップ 4	**do show running-config interface***portchannel_interface_name* 例： スイッチ#(config-if-range)# **do show running-config int po11**	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。

IPv6 スヌーピング ポリシーを VLAN にグローバルにアタッチする方法

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。

手順の概要

1. **configure terminal**
2. **vlan configuration** *vlan_list*
3. **ipv6 snooping** [**attach-policy** *policy_name*]
4. **do show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **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 2	**vlan configuration** *vlan_list* 例： スイッチ(config)# **vlan configuration 333**	VLAN インターフェイスのコンフィギュレーション モードを開始し、IPv6 スヌーピング ポリシーをアタッチする VLAN を指定します。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 snooping** [**attach-policy** *policy_name*] 例： `スイッチ(config-vlan-config)#ipv6 snooping 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 スヌーピング 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、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 4	**do show running-config** 例： `スイッチ#(config-if)# do 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 VLAN にアタッチされていることを確認します。

IPv6 バインディング テーブルの内容を設定する方法

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。

手順の概要

1. **configure terminal**
2. [**no**] **ipv6 neighbor binding** [**vlan** *vlan-id* {*ipv6-address* **interface** interface_type *stack/module/port hw_address* [**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**] }]
3. [**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*]]]]
4. **ipv6 neighbor binding logging**
5. **exit**
6. **show ipv6 neighbor binding**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# 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 2	[**no**] **ipv6 neighbor binding** [**vlan** *vlan-id* {*ipv6-address* **interface** interface_type *stack/module/port hw_address* [**reachable-lifetimevalue** [*seconds*	**default**	**infinite**]	[**tracking**{ [default	disable] [**reachable-lifetimevalue** [*seconds*	**default**	**infinite**]	[**enable**	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**] | [**retry-interval** {*seconds*| **default** [**reachable-lifetimevalue** [*seconds* | **default** | **infinite**] }] 例： `スイッチ(config)# ipv6 neighbor binding`	
ステップ 3	[**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： `スイッチ(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 4	**ipv6 neighbor binding logging** 例： `スイッチ(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 5	**exit** 例： `スイッチ(config)# exit`	グローバル コンフィギュレーション モードを終了して、ルータを特権 EXEC モードにします。
ステップ 6	**show ipv6 neighbor binding** 例： `スイッチ# 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 ネイバー探索検査ポリシーの設定方法

特権 EXEC モードから、IPv6 ND 検査ポリシーを設定するには、次の手順に従ってください。

手順の概要

1. **configure terminal**
2. [**no**]**ipv6 nd inspection policy** *policy-name*
3. **device-role** {**host** | **monitor** | **router** | **switch**}
4. **drop-unsecure**
5. **limit address-count** *value*
6. **sec-level minimum** *value*
7. **tracking** {**enable** [**reachable-lifetime** {*value* | **infinite**}] | **disable** [**stale-lifetime** {*value* | **infinite**}]}
8. **trusted-port**
9. **validate source-mac**

10. **no** {**device-role** | **drop-unsecure** | **limit address-count** | **sec-level minimum** | **tracking** | **trusted-port** | **validate source-mac**}
11. **default** {**device-role** | **drop-unsecure** | **limit address-count** | **sec-level minimum** | **tracking** | **trusted-port** | **validate source-mac**}
12. **do show ipv6 nd inspection policy** *policy_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# 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 2	[**no**]**ipv6 nd inspection policy** *policy-name* 例： `スイッチ(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 3	**device-role** {**host**	**monitor**	**router**	**switch**} 例： `スイッチ(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 4	**drop-unsecure** 例： `スイッチ(config-nd-inspection)# drop-unsecure`	オプションが指定されていないか無効なオプションが指定されているか、またはシグニチャが無効なメッセージをドロップします。
ステップ 5	**limit address-count** *value* 例： `スイッチ(config-nd-inspection)# limit address-count 1000`	1 ～ 10,000 を入力します。
ステップ 6	**sec-level minimum** *value* 例： `スイッチ(config-nd-inspection)# limit address-count 1000`	暗号化生成アドレス（CGA）オプションを使用する場合の最小のセキュリティ レベル パラメータ値を指定します。
ステップ 7	**tracking** {**enable** [**reachable-lifetime** {*value*	**infinite**}]	**disable** [**stale-lifetime** {*value*	**infinite**}]} 例： `スイッチ(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 8	**trusted-port** 例： `スイッチ(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。

	コマンドまたはアクション	目的
ステップ 9	**validate source-mac** 例： `スイッチ(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 10	**no** {**device-role** | **drop-unsecure** | **limit address-count** | **sec-level minimum** | **tracking** | **trusted-port** | **validate source-mac**} 例： `スイッチ(config-nd-inspection)# no 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。
ステップ 11	**default** {**device-role** | **drop-unsecure** | **limit address-count** | **sec-level minimum** | **tracking** | **trusted-port** | **validate source-mac**} 例： `スイッチ(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 12	**do show ipv6 nd inspection policy** *policy_name* 例： `スイッチ(config-nd-inspection)# do show ipv6 nd inspection policy example_policy`	ND検査コンフィギュレーションモードを終了しないで ND 検査の設定を確認します。

IPv6 ネイバー探索検査ポリシーをインターフェイスにアタッチする方法

Cisco IOS XE Amsterdam 17.1.1 以降、IPv6 ND 検査機能は廃止され、SISF ベースのデバイス追跡機能に置き換えられます。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。

手順の概要

1. **configure terminal**
2. **interface** Interface_type *stack/module/port*
3. **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**}]
4. **do show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# 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 2	**interface** Interface_type *stack/module/port* 例： `スイッチ(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 3	**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：
	`スイッチ(config-if)# ipv6 nd inspection attach-policy example_policy`
	or
	`スイッチ(config-if)# ipv6 nd inspection attach-policy example_policy vlan 222,223,224`
	or
	`スイッチ(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 4	**do show running-config** 例： `スイッチ#(config-if)# do 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。

IPv6 ネイバー探索検査ポリシーをレイヤ 2 EtherChannel インターフェイスにアタッチする方法

Cisco IOS XE Amsterdam 17.1.1 以降、IPv6 ND 検査機能は廃止され、SISF ベースのデバイス追跡機能に置き換えられます。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。

手順の概要

1. **configure terminal**
2. **interface range** *Interface_name*
3. **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**}]
4. **do show running-config interface***portchannel_interface_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	**configure terminal** 例： `スイッチ# 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 2	**interface range** *Interface_name* 例： `スイッチ(config)# interface Po11`	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 **do show interfaces summary** コマンドを使用します。

ステップ 3	**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：
	`スイッチ(config-if-range)# ipv6 nd inspection attach-policy example_policy`
	or
	`スイッチ(config-if-range)# ipv6 nd inspection attach-policy example_policy vlan 222,223,224`
	or
	`スイッチ(config-if-range)#ipv6 nd inspection 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 4	**do show running-config interface***portchannel_interface_name* 例：	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。

	コマンドまたはアクション	目的
	スイッチ#(config-if-range)# **do show running-config int po11**	

IPv6 ネイバー探索検査ポリシーを全体的に VLAN にアタッチする方法

Cisco IOS XE Amsterdam 17.1.1 以降、IPv6 ND 検査機能は廃止され、SISF ベースのデバイス追跡機能に置き換えられます。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。

手順の概要

1. **configure terminal**
2. **vlan configuration** *vlan_list*
3. **ipv6 nd inspection** [**attach-policy** *policy_name*]
4. **do show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **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 2	**vlan configuration** *vlan_list* 例： スイッチ(config)# **vlan configuration 334**	VLAN インターフェイスのコンフィギュレーション モードを開始し、IPv6 スヌーピング ポリシーをアタッチする VLAN を指定します。
ステップ 3	**ipv6 nd inspection** [**attach-policy** *policy_name*] 例： スイッチ(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。

	コマンドまたはアクション	目的
ステップ 4	**do show running-config** 例： スイッチ#(config-if)# **do show running-config**	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 VLAN にアタッチされていることを確認します。

IPv6 ルータ アドバタイズメント ガード ポリシーの設定方法

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。

手順の概要

1. **configure terminal**
2. [**no**]**ipv6 nd raguard policy** *policy-name*
3. [**no**]**device-role** {**host** | **monitor** | **router** | **switch**}
4. [**no**]**hop-limit** {**maximum** | **minimum**} *value*
5. [**no**]**managed-config-flag** {**off** | **on**}
6. [**no**]**match** {**ipv6 access-list** *list* | **ra prefix-list** *list*}
7. [**no**]**other-config-flag** {**on** | **off**}
8. [**no**]**router-preference maximum** {**high** | **medium** | **low**}
9. [**no**]**trusted-port**
10. **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**}
11. **do show ipv6 nd raguard policy** *policy_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： スイッチ# **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 2	[**no**]**ipv6 nd raguard policy** *policy-name* 例： スイッチ(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 3	[**no**]**device-role** {**host**	**monitor**	**router**	**switch**} 例： スイッチ(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。

	コマンドまたはアクション	目的
ステップ 4	[**no**]**hop-limit** {**maximum** | **minimum**} *value* 例： スイッチ(config-nd-raguard)# **hop-limit maximum 33**	（1～255）最大および最小のホップ制限値の範囲。 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。 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 5	[**no**]**managed-config-flag** {**off** | **on**} 例： スイッチ(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 6	[**no**]**match** {**ipv6 access-list** *list* | **ra prefix-list** *list*} 例： スイッチ(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 7	[**no**]**other-config-flag** {**on** | **off**} 例： スイッチ(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。

	コマンドまたはアクション	目的
		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。
ステップ 8	[**no**]**router-preference maximum** {**high** | **medium** | **low**} 例： `スイッチ(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、このフィルタは無効になります。 • **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 9	[**no**]**trusted-port** 例： `スイッチ(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 10	**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： `スイッチ(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 11	**do show ipv6 nd raguard policy** *policy_name* 例： `スイッチ(config-nd-raguard)# do show ipv6 nd raguard policy example_policy`	（任意）：RA ガード ポリシー コンフィギュレーション モードを終了しないで ND ガード ポリシー設定を表示します。

IPv6 ルータ アドバタイズメント ガード ポリシーをインターフェイスにアタッチする方法

インターフェイスまたはそのインターフェース上の 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。

手順の概要

1. **configure terminal**
2. **interface** Interface_type *stack/module/port*
3. **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**}]
4. **do show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# 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 2	**interface** Interface_type *stack/module/port* 例： `スイッチ(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 3	**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： `スイッチ(config-if)# ipv6 nd raguard attach-policy example_policy` or `スイッチ(config-if)# ipv6 nd raguard attach-policy example_policy vlan 222,223,224` **or** `スイッチ(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 4	**do show running-config** 例： `スイッチ#(config-if)# do show running-config`	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。

IPv6ルータアドバタイズメントガードポリシーをレイヤ2EtherChannelインターフェイスにアタッチする方法

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。

手順の概要

1. **configure terminal**
2. **interface range** *Interface_name*
3. **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**}]
4. **do show running-config interface***portchannel_interface_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	**configure terminal** 例： `スイッチ# 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 2	**interface range** *Interface_name* 例： `スイッチ(config)# interface Po11`	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 **do show interfaces summary** コマンドを使用します。

ステップ 3	**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：
	`スイッチ(config-if-range)# ipv6 nd raguard attach-policy example_policy`
	or
	`スイッチ(config-if-range)# ipv6 nd raguard attach-policy example_policy vlan 222,223,224`
	or
	`スイッチ(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。

	コマンドまたはアクション	目的
ステップ 4	**do show running-config interface***portchannel_interface_name* 例： `スイッチ#(config-if-range)# do show running-config int po11`	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。

IPv6 ルータ アドバタイズメント ガード ポリシーを VLAN にグローバルにアタッチする方法

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。

手順の概要

1. **configure terminal**
2. **vlan configuration** *vlan_list*
3. **ipv6 dhcp guard** [**attach-policy** *policy_name*]
4. **do show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# 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 2	**vlan configuration** *vlan_list* 例： `スイッチ(config)# vlan configuration 335`	VLAN インターフェイスのコンフィギュレーション モードを開始し、IPv6 RA ガード ポリシーをアタッチする VLAN を指定します。
ステップ 3	**ipv6 dhcp guard** [**attach-policy** *policy_name*] 例： `スイッチ(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 4	**do show running-config** 例： `スイッチ#(config-if)# do show running-config`	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 VLAN にアタッチされていることを確認します。

IPv6 DHCP ガード ポリシーの設定方法

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。

手順の概要

1. **configure terminal**
2. [**no**]**ipv6 dhcp guard policy** *policy-name*
3. [**no**]**device-role** {**client** | **server**}
4. [**no**] **match server access-list** *ipv6-access-list-name*
5. [**no**] **match reply prefix-list** *ipv6-prefix-list-name*
6. [**no**]**preference**{ **max** *limit* | **min** *limit* }
7. [**no**] **trusted-port**
8. **default** {**device-role** | **trusted-port**}
9. **do show ipv6 dhcp guard policy** *policy_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# 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 2	[**no**]**ipv6 dhcp guard policy** *policy-name* 例： `スイッチ(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 3	[**no**]**device-role** {**client** | **server**} 例： `スイッチ(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。アタッチ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。

	コマンドまたはアクション	目的

ステップ 4	[**no**] **match server access-list** *ipv6-access-list-name*
	例：
	`;;Assume a preconfigured IPv6 Access List as follows:`
	`スイッチ(config)# ipv6 access-list my_acls`
	`スイッチ(config-ipv6-acl)# permit host FE80::A8BB:CCFF:FE01:F700 any`
	`;;configure DCHPv6 Guard to match approved access list.`
	`スイッチ(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 5	[**no**] **match reply prefix-list** *ipv6-prefix-list-name*
	例：
	`;;Assume a preconfigured IPv6 prefix list as follows:`
	`スイッチ(config)# ipv6 prefix-list my_prefix permit 2001:0DB8::/64 le 128`
	`;; Configure DCHPv6 Guard to match prefix`
	`スイッチ(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。

ステップ 6	[**no**]**preference**{ **max** *limit* | **min** *limit* }
	例：
	`スイッチ(config-dhcp-guard)# preference max 250`
	`スイッチ(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 7	[**no**] **trusted-port** 例： `スイッチ(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。

	コマンドまたはアクション	目的
ステップ 8	**default** {**device-role** | **trusted-port**} 例： スイッチ(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 9	**do show ipv6 dhcp guard policy** *policy_name* 例： スイッチ(config-dhcp-guard)# **do show ipv6 dhcp guard policy example_policy**	（任意）コンフィギュレーション サブモードを終了せずに IPv6 DHCP のガード 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。

DHCPv6 ガード設定の例

```
enable
configure terminal
ipv6 access-list acl1
 permit host FE80::A8BB:CCFF:FE01:F700 any
ipv6 prefix-list abc permit 2001:0DB8::/64 le 128
ipv6 dhcp guard policy pol1
 device-role server
 match server access-list acl1
 match reply prefix-list abc
 preference min 0
 preference max 255
 trusted-port
interface GigabitEthernet 0/2/0
 switchport
 ipv6 dhcp guard attach-policy pol1 vlan add 1
 vlan 1
  ipv6 dhcp guard attach-policy pol1
show ipv6 dhcp guard policy pol1
```

IPv6 DHCP ガード ポリシーをインターフェイスまたはインターフェイス上の VLAN にアタッチする方法

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。

手順の概要

1. **configure terminal**
2. **interface** Interface_type *stack/module/port*
3. **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**}]
4. **do show running-config interface** Interface_type *stack/module/port*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# 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 2	**interface** Interface_type *stack/module/port* 例： `スイッチ(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 3	**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：
	`スイッチ(config-if)# ipv6 dhcp guard attach-policy example_policy`
	or
	`スイッチ(config-if)# ipv6 dhcp guard attach-policy example_policy vlan 222,223,224`
	or
	`スイッチ(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 4	**do show running-config interface** Interface_type *stack/module/port* 例： `スイッチ#(config-if)# do show running-config gig 1/1/4`	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。

IPv6 DHCP 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

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。

手順の概要

1. **configure terminal**

2. **interface range** *Interface_name*
3. **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**}]
4. **do show running-config interface***portchannel_interface_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	**configure terminal** 例： `スイッチ# 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 2	**interface range** *Interface_name* 例： `スイッチ(config)# interface Po11`	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 **do show interfaces summary** コマンドを使用します。

ステップ 3	**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：
	`スイッチ(config-if-range)# ipv6 dhcp guard attach-policy example_policy`
	or
	`スイッチ(config-if-range)# ipv6 dhcp guard attach-policy example_policy vlan 222,223,224`
	or
	`スイッチ(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 4	**do show running-config interface***portchannel_interface_name* 例： `スイッチ#(config-if-range)# do show running-config int po11`	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。

IPv6 DHCP ガード ポリシーを全体的に VLAN にアタッチする方法

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。

手順の概要

1. **configure terminal**
2. **vlan configuration** *vlan_list*
3. **ipv6 dhcp guard** [**attach-policy** *policy_name*]
4. **do show running-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `スイッチ# 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 2	**vlan configuration** *vlan_list* 例： `スイッチ(config)# vlan configuration 334`	VLAN インターフェイスのコンフィギュレーション モードを開始し、IPv6 スヌーピング ポリシーをアタッチする VLAN を指定します。
ステップ 3	**ipv6 dhcp guard** [**attach-policy** *policy_name*] 例： `スイッチ(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 4	**do show running-config** 例： `スイッチ#(config-if)# do show running-config`	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 VLAN にアタッチされていることを確認します。

IPv6 ソース ガードの設定方法

手順の概要

1. **enable**
2. **configure terminal**
3. [**no**] **ipv6 source-guard policy** *policy_name*
4. [**deny global-autoconf**] [**permit link-local**] [**default**{. . . }] [**exit**] [**no**{. . . }]
5. **end**

6. **show ipv6 source-guard policy** *policy_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `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 source-guard policy** *policy_name* 例： `Device(config)# ipv6 source-guard policy example_policy`	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。

IPv6 ソース ガード ポリシーをインターフェイスにアタッチする方法

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** Interface_type *stack/module/port*
4. **ipv6 source-guard** [**attach-policy** <*policy_name*>]
5. **show ipv6 source-guard policy** *policy_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `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** 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 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 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	**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。

IPv6 ソース ガードの設定方法

手順の概要

1. **enable**
2. **configure terminal**
3. [**no**] **ipv6 source-guard policy** *policy_name*
4. [**deny global-autoconf**] [**permit link-local**] [**default**{. . . }] [**exit**] [**no**{. . . }]
5. **end**
6. **show ipv6 source-guard policy** *policy_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `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 source-guard policy** *policy_name* 例： `Device(config)# ipv6 source-guard policy example_policy`	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。

	コマンドまたはアクション	目的
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。

IPv6 ソース ガード ポリシーをインターフェイスにアタッチする方法

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** Interface_type *stack/module/port*
4. **ipv6 source-guard** [**attach-policy** <*policy_name*>]
5. **show ipv6 source-guard policy** *policy_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `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** 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 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 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

	コマンドまたはアクション	目的
	`Device(config-if)# ipv6 source-guard attach-policy example_policy`	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	**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。

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

手順の概要

1. **enable**
2. **configure terminal**
3. **interface port-channel** *port-channel-number*
4. **ipv6 source-guard**［**attach-policy** <*policy_name*> ］
5. **show ipv6 source-guard policy** *policy_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `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 port-channel** *port-channel-number* 例： `Device (config)# interface Po4`	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。

	コマンドまたはアクション	目的
ステップ 5	**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。

IPv6 プレフィックス ガードの設定方法

（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。

手順の概要

1. **enable**
2. **configure terminal**
3. ［**no**］**ipv6 source-guard policy** *source-guard-policy*
4. ［ **no** ］**validate address**
5. **validate prefix**
6. **exit**
7. **show ipv6 source-guard policy**［*source-guard-policy*］

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	［**no**］**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	［ **no** ］**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。

IPv6プレフィックスガードポリシーをインターフェイスにアタッチする方法

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** Interface_type *stack/module/port*
4. **ipv6 source-guard attach-policy** *policy_name*
5. **show ipv6 source-guard policy** *policy_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `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 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 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	**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。

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

手順の概要

1. **enable**
2. **configure terminal**
3. **interface port-channel** *port-channel-number*
4. **ipv6 source-guard** [**attach-policy** <*policy_name*>]
5. **show ipv6 source-guard policy** *policy_name*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `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 port-channel** *port-channel-number* 例： `Device (config)# interface Po4`	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。

	コマンドまたはアクション	目的
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	**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。

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。