# IPv6 RA ガード

IPv6 RA ガード機能は、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ルータ アドバタイズメント（RA）ガード メッセージを、ネットワーク管理者がブロックまたは拒否できるようにするためのサポートを提供します。


- IPv6 RA ガードの制限 （1 ページ）
- IPv6 RA ガードに関する情報 （2 ページ）
- IPv6 RA ガードの設定方法 （2 ページ）
- IPv6 RA ガードの設定例 （6 ページ）
- その他の参考資料 （7 ページ）
- IPv6 RA ガードの機能情報 （8 ページ）


# IPv6 RA ガードの制限

- IPv6 RA ガード機能は、IPv6 トラフィックがトンネリングされる環境では保護を行いません。
- この機能は、TCAM（Ternary Content Addressable Memory）がプログラムされているハードウェアでのみサポートされています。
- この機能は、入力方向のスイッチ ポート インターフェイスで設定できます。
- この機能は、ホスト モードとルータ モードをサポートしています。
- この機能は、入力方向だけでサポートされます。出力方向ではサポートされません。
- この機能は、EtherChannel および EtherChannel ポート メンバーではサポートされません。
- この機能は、マージ モードのトランク ポートではサポートされません。
- この機能は、補助 VLAN およびプライベート VLAN（PVLAN）でサポートされています。PVLAN の場合、プライマリ VLAN の機能が継承され、ポート機能とマージされます。
- IPv6 RA ガード機能によってドロップされたパケットはスパニングできます。
- **platform ipv6 acl icmp optimize neighbor-discovery command** が設定されている場合、IPv6 RA ガード機能は設定できず、エラー メッセージが表示されます。このコマンドは、RA

ガードの ICMP エントリを上書きするデフォルトのグローバル Internet Control Message Protocol（ICMP）エントリを追加します。

# IPv6 RA ガードに関する情報

## IPv6 グローバル ポリシー

IPv6 グローバル ポリシーは、ストレージおよびアクセス ポリシー データベースのサービスを提供します。IPv6 ND 検査と IPv6 RA ガードは、IPv6 グローバル ポリシー機能です。ND インスペクションまたは RA ガードをグローバルに設定するたびに、ポリシーの属性が、ソフトウェア ポリシー データベースに保存されます。その後ポリシーはインターフェイスに適用され、ポリシーが適用されたこのインターフェイスを含めるためにソフトウェア ポリシー データベース エントリが更新されます。

## IPv6 RA ガード

IPv6 RA ガード機能は、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、ネットワーク管理者がブロックまたは拒否できるようにするためのサポートを提供します。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。IPv6 RA ガード機能は、それらの RA を分析して、承認されていないデバイスから送信された RA を除外します。ホスト モードでは、ポート上の RA 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（L2）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。L2 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 はドロップされます。

ワイヤレス展開では、ワイヤレス ポートで受信した RA はドロップされます。ルータはこれらのインターフェイスに存在できないためです。

# IPv6 RA ガードの設定方法

## デバイスでの IPv6 RA ガード ポリシーの設定

（注） **ipv6 nd raguard** コマンドがポートで設定されている場合、ルータ送信要求メッセージはこれらのポートに複製されません。ルータ要請メッセージを複製するには、ルータ側のすべてのポートをルータ ロールに設定する必要があります。

### 手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 nd raguard policy** *policy-name*
4. **device-role** {**host** | **router**}
5. **hop-limit** {**maximum** | **minimum** *limit*}
6. **managed-config-flag** {**on** | **off**}
7. **match ipv6 access-list** *ipv6-access-list-name*
8. **match ra prefix-list** *ipv6-prefix-list-name*
9. **other-config-flag** {**on** | **off**}
10. **router-preference maximum** {**high** | **low** | **medium**}
11. **trusted-port**
12. **exit**

### 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**<br>例：<br>`Device> enable` | 特権 EXEC モードを有効にします。<br>• 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**<br>例：<br>`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*<br>例：<br>`Device(config)# ipv6 nd raguard policy policy1` | RA ガード ポリシー名を定義して、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 | **device-role** {**host** | **router**}<br>例：<br>`Device(config-ra-guard)# device-role router` | ポートに接続されているデバイスの役割を指定します。 |
| ステップ 5 | **hop-limit** {**maximum** | **minimum** *limit*}<br>例：<br>`Device(config-ra-guard)# hop-limit minimum 3` | （任意）アドバタイズされたホップ カウント制限の検証をイネーブルにします。<br>• 設定されていない場合、このチェックは回避されます。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 6 | **managed-config-flag** {**on** \| **off**}<br>例：<br>`Device(config-ra-guard)# managed-config-flag on` | （任意）アドバタイズされた管理アドレスの設定フラグが on であることの検証をイネーブルにします。<br>• 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 | **match ipv6 access-list** *ipv6-access-list-name*<br>例：<br>`Device(config-ra-guard)# match ipv6 access-list list1` | （任意）検査済みメッセージ内の送信者の IPv6 アドレスが設定された承認デバイス ソース アクセス リストからのものであることの検証をイネーブルにします。<br>• 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 | **match ra prefix-list** *ipv6-prefix-list-name*<br>例：<br>`Device(config-ra-guard)# match ra prefix-list listname1` | （任意）検証済みメッセージ内のアドバタイズされたプレフィックスが設定された承認プレフィックス リストからのものであることの検証をイネーブルにします。<br>• 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 9 | **other-config-flag** {**on** \| **off**}<br>例：<br>`Device(config-ra-guard)# other-config-flag on` | （任意）アドバタイズされた [Other] 設定パラメータの検証をイネーブルにします。 |
| ステップ 10 | **router-preference maximum** {**high** \| **low** \| **medium**}<br>例：<br>`Device(config-ra-guard)# router-preference maximum high` | （任意）アドバタイズされたデフォルト ルータの設定パラメータの値が指定された制限値以下であることの検証をイネーブルにします。 |
| ステップ 11 | **trusted-port**<br>例：<br>`Device(config-ra-guard)# trusted-port` | （任意）このポリシーが信頼できるポートに適用されることを指定します。<br>• すべての RA ガード ポリシングが無効になります。 |
| ステップ 12 | **exit**<br>例：<br>`Device(config-ra-guard)# exit` | RA ガード ポリシー コンフィギュレーション モードを終了してグローバル コンフィギュレーション モードに戻ります。 |

# インターフェイスの IPv6 RA ガードの設定

## 手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 nd raguard attach-policy** [*policy-name* [**vlan** {**add** | **except** | **none** | **remove** | **all**} *vlan* [*vlan1, vlan2, vlan3...*]]]
5. **exit**
6. **show ipv6 nd raguard policy** [*policy-name*]
7. **debug ipv6 snooping raguard** [*filter* | *interface* | *vlanid*]

## 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**<br>例：<br>`Device> enable` | 特権 EXEC モードを有効にします。<br>• 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**<br>例：<br>`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*<br>例：<br>`Device(config)# interface fastethernet 3/13` | インターフェイスのタイプと番号を指定し、デバイスをインターフェイス コンフィギュレーション モードにします。 |
| ステップ 4 | **ipv6 nd raguard attach-policy** [*policy-name* [**vlan** {**add** \| **except** \| **none** \| **remove** \| **all**} *vlan* [*vlan1, vlan2, vlan3...*]]]<br>例：<br>`Device(config-if)# ipv6 nd raguard attach-policy` | 指定したインターフェイスに IPv6 RA ガード機能を適用します。 |
| ステップ 5 | **exit**<br>例：<br>`Device(config-if)# exit` | インターフェイス コンフィギュレーション モードを終了します。 |
| ステップ 6 | **show ipv6 nd raguard policy** [*policy-name*]<br>例：<br>`Device# show ipv6 nd raguard policy raguard1` | RA ガードを使用して設定されているすべてのインターフェイスで RA ガード ポリシーを表示します。 |

| | コマンドまたはアクション | 目的 |
|---|---|---|
| ステップ 7 | **debug ipv6 snooping raguard** [*filter* \| *interface* \| *vlanid*]<br>例：<br>`Device# debug ipv6 snooping raguard` | IPv6 RA ガード スヌーピング情報のデバッグをイネーブルにします。 |

# IPv6 RA ガードの設定例

## 例：IPv6 RA ガードの設定

```
Device(config)# interface fastethernet 3/13

Device(config-if)# ipv6 nd raguard attach-policy

Device# show running-config interface fastethernet 3/13

Building configuration...
Current configuration : 129 bytes
!
interface FastEthernet3/13
 switchport
 switchport access vlan 222
 switchport mode access
 access-group mode prefer port
 ipv6 nd raguard
end
```

## 例：IPv6 ND インスペクションおよび RA ガードの設定

この例は、ネイバー探索インスペクションおよびRA ガード機能の両方が設定されているインターフェイスに関する情報を示しています。

```
Device# show ipv6 snooping capture-policy interface ethernet 0/0

Hardware policy registered on Ethernet 0/0
Protocol     Protocol value   Message   Value     Action    Feature
ICMP         58               RS        85        punt      RA Guard
                                                  punt      ND Inspection
ICMP         58               RA        86        drop      RA guard
                                                  punt      ND Inspection
ICMP         58               NS        87        punt      ND Inspection
ICM          58               NA        88        punt      ND Inspection
ICMP         58               REDIR     89        drop      RA Guard
                                                  punt      ND Inspection
```

# その他の参考資料

### 関連資料

| 関連項目 | マニュアル タイトル |
|---|---|
| IPv6 アドレッシングと接続 | 『*IPv6 Configuration Guide*』 |
| Cisco IOS コマンド | 『Cisco IOS Master Commands List, All Releases』 |
| IPv6 コマンド | 『*Cisco IOS IPv6 Command Reference*』 |
| Cisco IOS IPv6 機能 | 『Cisco IOS IPv6 Feature Mapping』 |

### 標準および RFC

| 標準/RFC | タイトル |
|---|---|
| IPv6 に関する RFC | *IPv6 RFCs* |

### MIB

| MIB | MIB のリンク |
|---|---|
| この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存MIBのサポートに変更はありません。 | 選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探して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。<br>http://www.cisco.com/go/mibs |

### 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。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。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/cisco/web/support/index.html |

# IPv6 RA ガードの機能情報

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

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

表 *1 : IPv6 RA* ガードの機能情報

| 機能名 | リリース | 機能情報 |
|---|---|---|
| IPv6 RA ガード | 12.2(33)SXI4<br>12.2(50)SY<br>12.2(54)SG<br>15.0(2)SE<br>15.0(2)SG<br>Cisco IOS XE Release 3.8S<br>Cisco IOS XE Release 3.2SE<br>Cisco IOS XE Release 3.2SG | 次のコマンドが導入または変更されました。**debug ipv6 snooping raguard**、**device-role**、**hop-limit**、**ipv6 nd raguard attach-policy**、**ipv6 nd raguard policy**、**managed-config-flag**、**match ipv6 access-list**、**match ra prefix-list**、**other-config-flag**、**router-preference maximum**、**show ipv6 nd raguard policy**。 |

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。