IPv6 スヌーピング

IPv6 スヌーピング機能は、複数のレイヤ 2 IPv6 ファーストホップ セキュリティ機能（IPv6 ネイバー探索インスペクション、IPv6 デバイス トラッキング、IPv6 アドレス収集、および IPv6 バインディング テーブルのリカバリを含む）をバンドルして、セキュリティと拡張性を提供します。IPv6 ND インスペクションは、レイヤ 2（またはレイヤ 2 とレイヤ 3 の間）で動作し、IPv6 の機能にセキュリティと拡張性を提供します。

IPv6 スヌーピングの制限

IPv6 スヌーピング機能は、EtherChannel ポートではサポートされません。

IPv6 スヌーピングに関する情報

ここでは、IPv6 スヌーピングについて説明します。

IPv6 スヌーピング

IPv6 スヌーピング機能によって、複数のレイヤ 2 IPv6 ファーストホップ セキュリティ機能（IPv6 アドレス収集と IPv6 デバイス トラッキングを含む）がバンドルされます。この機能は、レイヤ 2（またはレイヤ 2 とレイヤ 3 の間）で動作し、IPv6 の機能にセキュリティと拡張性を提供します。この機能によって、Duplicate Address Detection（DAD）、アドレス解決、デバイス検出やネイバー キャッシュに対する攻撃といった、ネイバー探索メカニズムに固有のいくつかの脆弱性が軽減されます。

IPv6 スヌーピングは、レイヤ 2 ネイバー テーブル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て保護し、信頼できるバインディング テーブルを構築するために ND メッ

セージを分析します。有効なバインディングのないIPv6NDメッセージはドロップされます。ND メッセージは、その IPv6 から 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。

ターゲット（プラットフォームのターゲット サポートによって異なり、デバイス ポート、スイッチ ポート、レイヤ 2 インターフェイス、レイヤ 3 インターフェイス、および VLAN が含まれることがある）に IPv6 スヌーピングが設定されている場合、IPv6 トラフィックの ND プロトコルと Dynamic Host Configuration Protocol（DHCP）をルーティング デバイスのスイッチ統合セキュリティ機能（SISF）インフラストラクチャにリダイレクトするためのキャプチャ命令がハードウェアにダウンロードされます。ND トラフィックの場合、NS、NA、RS、RA、REDIRECT などのメッセージが SISF にリダイレクトされます。DHCP の場合、ポート 546 または 547 から送信された UDP メッセージがリダイレクトされます。

IPv6 スヌーピングはその「キャプチャ ルール」を分類子に登録します。分類子では、特定のターゲットにあるすべての機能のルールがすべて集約され、対応する ACL がプラットフォーム依存モジュールにインストールされます。分類子は、リダイレクトされたトラフィックを受信すると、（トラフィックを受信しているターゲットに対して）登録されているすべての機能からすべてのエントリ ポイント（IPv6 スヌーピングのエントリ ポイントを含む）を呼び出します。IPv6 スヌーピングのエントリ ポイントは最後に呼び出されるため、他の機能によって行われた決定が IPv6 スヌーピングの決定よりも優先されます。

IPv6 デバイス トラッキング

IPv6 デバイス トラッキングは、IPv6 ホストが非表示になったときにネイバー テーブルを即時に更新できるように、IPv6 ホストの活性トラッキングを提供します。

IPv6 ファーストホップ セキュリティ バインディング テーブル

IPv6 ファーストホップ セキュリティ バインディング テーブルのリカバリ メカニズム機能を使用すると、デバイスのリブート時にバインディングテーブルをリカバリできます。デバイスに接続されている IPv6 ネイバーのデータベース テーブルは、ND スヌーピングなどの情報源から作成されます。このデータベース（またはバインディング）テーブルは、スプーフィングやリダイレクト攻撃を防止するために、リンク層アドレス（LLA）、IPv4 またはIPv6アドレス、および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 ガード機能によって使用されます。

このメカニズムにより、デバイスのリブート時にバインディング テーブルをリカバリできます。リカバリ メカニズムは、不明な送信元、（バインディング テーブルにまだ指定されていない送信元や、ND または DHCP グリーニングを使用して学習されていない送信元）からのデータ トラフィックをブロックします。この機能は、宛先ガードで宛先アドレスの解決に失敗したときに、不足しているバインディングテーブルのエントリをリカバリします。障害が発生すると、バインディングテーブルのエントリは、設定に応じて、DHCP サーバーまたは宛先ホストにクエリを実行することでリカバリできます。

リカバリ プロトコルとプレフィックス リスト

IPv6 ファーストホップ セキュリティ バインディング テーブルのリカバリ メカニズム機能は、DHCP と NDP の両方でリカバリを試みる前に、一致するプレフィックス リストを提供する機能を導入します。

アドレスがプロトコルと関連付けられているプレフィックス リストと一致しない場合、そのプロトコルではバインディング テーブル エントリのリカバリは試行されません。プレフィックス リストは、プロトコルを使用してレイヤ2 ドメインに割り当てられているアドレスに対して有効なプレフィックスに対応している必要があります。デフォルトではプレフィックス リストは存在せず、すべてのアドレスのリカバリが試行されます。プロトコルにプレフィックス リストを関連付けるコマンドは、**protocol** {**dhcp** | **ndp**} [**prefix-list** *prefix-list-name*] です。

IPv6 デバイス トラッキング

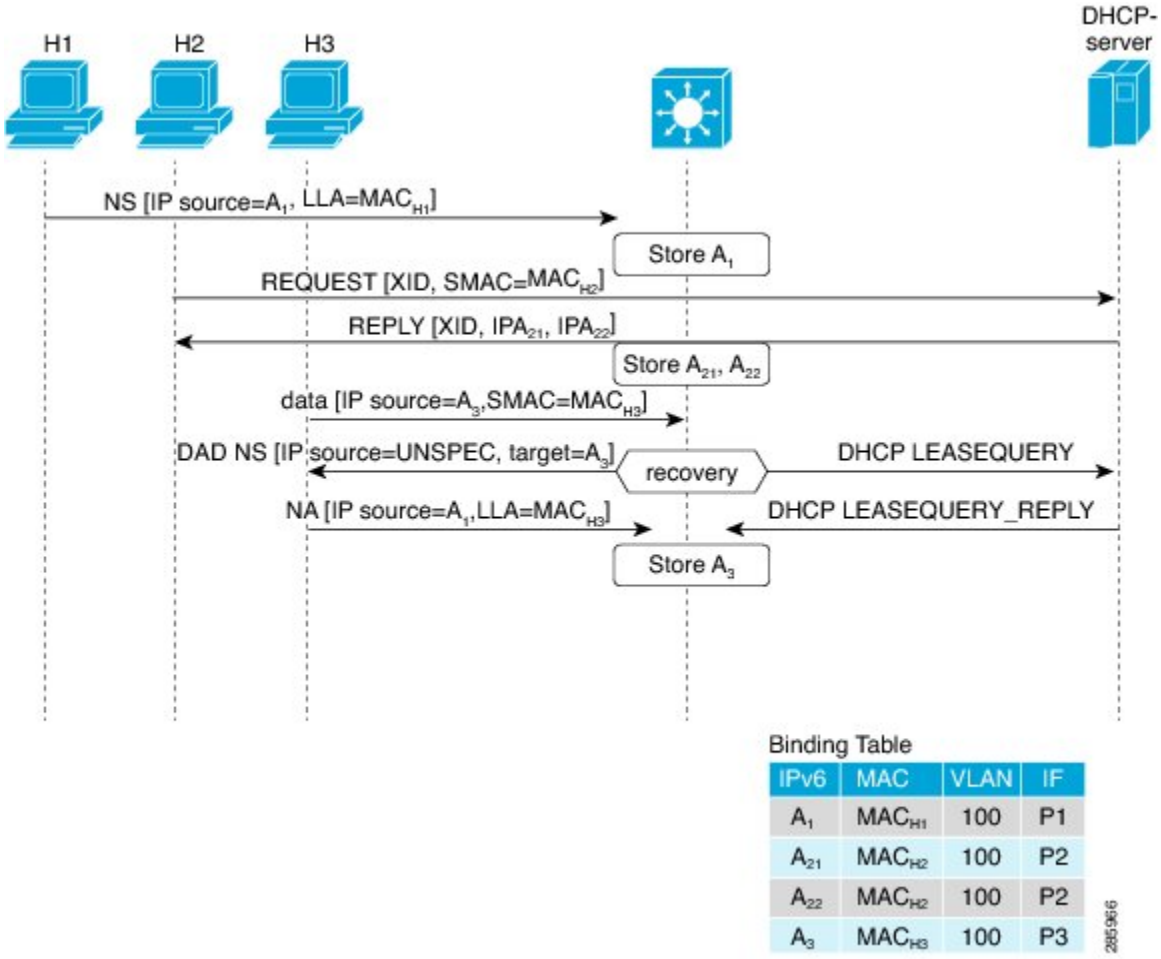
IPv6 デバイス トラッキングは、IPv6 ホストが非表示になったときにネイバー テーブルを即時に更新できるように、IPv6 ホストの活性トラッキングを提供します。

IPv6 アドレス収集

IPv6 アドレス収集は、正確なバインディング テーブルに依存するその他多くの IPv6 の機能の基盤です。この機能は、アドレス収集のためにリンク上の ND および DHCP メッセージを検査した後に、それらのアドレスをバインディング テーブルに入力します。また、この機能は、アドレスの所有権を強制し、特定のノードが要求可能なアドレスの数を制限します。

次の図は、IPv6 アドレス収集の仕組みを示しています。

図 *1 : IPv6* アドレス収集



複数の IA_NA および IA_PD のサポート

場合によっては、ネットワークデバイスが DHCP サーバーから複数の IPv6 アドレスを要求して受信することがあります。これは、レジデンシャルゲートウェイがアドレスをその LAN クライアントに配布することを要求する場合など、デバイスの複数のクライアントにアドレスを提供するために実行できます。デバイスが DHCPv6 パケットを送信すると、パケットにはデバイスに割り当てられているすべてのアドレスが含まれます。

SISF は DHCPv6 パケットを分析する際に、パケットの IA_NA（Identity Association-Nontemporary Address）および IA_PD（Identity Association-Prefix Delegation）コンポーネントを検査し、パケットに含まれる各 IPv6 アドレスを抽出します。SISF は、抽出された各アドレスをバインディングテーブルに追加します。

IPv6 スヌーピングの設定方法

インターフェイスの IPv6 スヌーピングの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 snooping policy** *snooping-policy*
4. **exit**
5. **interface** *type number*
6. **ipv6 snooping attach-policy** *snooping-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	**ipv6 snooping policy** *snooping-policy* 例： `Device(config)# ipv6 snooping policy policy1`	IPv6 スヌーピング ポリシーを設定し、IPv6 スヌーピング 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	**exit** 例： `Device(config-ipv6-snooping)# exit`	IPv6 スヌーピング コンフィギュレーション モードを終了します。
ステップ 5	**interface** *type number* 例： `Device(config)# interface Gigabitethernet 0/0/1`	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 6	**ipv6 snooping attach-policy** *snooping-policy* 例： `Device(config-if)# ipv6 snooping attach-policy policy1`	インターフェイスに IPv6 スヌーピング ポリシーを対応付けます。

IPv6 ND インスペクションの確認とトラブルシューティング

手順の概要

1. **enable**
2. **show ipv6 snooping capture-policy** [**interface** *type number*]
3. **show ipv6 snooping counter** [**interface** *type number*]
4. **show ipv6 snooping features**
5. **show ipv6 snooping policies** [**interface** *type number*]
6. **debug ipv6 snooping**

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	**show ipv6 snooping capture-policy** [**interface** *type number*] 例： `Device# show ipv6 snooping capture-policy interface ethernet 0/0`	スヌーピング ND メッセージキャプチャポリシーを表示します。
ステップ 3	**show ipv6 snooping counter** [**interface** *type number*] 例： `Device# show ipv6 snooping counter interface FastEthernet 4/12`	インターフェイスカウンタによってカウントされたパケットに関する情報を表示します。
ステップ 4	**show ipv6 snooping features** 例： `Device# show ipv6 snooping features`	デバイスに設定されているスヌーピング機能に関する情報を表示します。
ステップ 5	**show ipv6 snooping policies** [**interface** *type number*] 例： `Device# show ipv6 snooping policies`	設定されているポリシーと、ポリシーが接続されているインターフェイスに関する情報を表示します。
ステップ 6	**debug ipv6 snooping** 例： `Device# debug ipv6 snooping`	IPv6 でスヌーピング情報のデバッグをイネーブルにします。

IPv6 デバイス トラッキングの設定

IPv6 ファーストホップ セキュリティ バインディング テーブルの内容の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 neighbor binding** {*ipv6-address* | *ipv6-prefix*} **interface** *type number* [*hardware-address* | *mac-address*][**tracking** [**disable** | **enable** | **retry-interval** *value*] | **reachable-lifetime** *value*]
4. **ipv6 neighbor binding max-entries** *entries*
5. **ipv6 neighbor binding logging**
6. **exit**
7. **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	**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 neighbor binding** {*ipv6-address* | *ipv6-prefix*} **interface** *type number* [*hardware-address* | *mac-address*][**tracking** [**disable** | **enable** | **retry-interval** *value*] | **reachable-lifetime** *value*] 例： `Device(config)# ipv6 neighbor binding 2001:DB8:0:ABCD::1 interface GigabitEthernet 0/0/1 reachable-lifetime 100`	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。
ステップ 4	**ipv6 neighbor binding max-entries** *entries* 例： `Device(config)# ipv6 neighbor binding max-entries 100`	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：	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。

	コマンドまたはアクション	目的
	`Device(config)# ipv6 neighbor binding logging`	
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 モードを開始します。
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 ファーストホップ セキュリティ バインディング テーブルのリカバリ メカニズムの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 neighbor binding** *ipv6-address* **interface** *type number*
4. **ipv6 prefix-list** *list-name* **permit** *ipv6-prefix/prefix-length* **ge** *ge-value*
5. **ipv6 snooping policy** *snooping-policy-id*
6. **destination-glean** {**recovery** | **log-only**} [**dhcp**]
7. **data-glean** {**recovery** | **log-only**} [**ndp** | **dhcp**]
8. **prefix-glean**
9. **protocol dhcp** [**prefix-list** *prefix-list-name*]
10. **exit**
11. **ipv6 destination-guard policy** *policy-name*
12. **enforcement** {**always** | **stressed**}
13. **exit**
14. **interface** *type number*
15. **ipv6 snooping attach-policy** *snooping-policy*
16. **ipv6 destination-guard attach-policy** *policy-name*
17. **end**

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）。

	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	**ipv6 neighbor binding** *ipv6-address* **interface** *type number* 例： `Device(config)# ipv6 neighbor binding 2001:db8::1 interface Gigabitethernet3/0/1`	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。
ステップ 4	**ipv6 prefix-list** *list-name* **permit** *ipv6-prefix/prefix-length* **ge** *ge-value* 例： `Device(config)# ipv6 prefix-list abc permit 2001:DB8::/64 ge 128`	IPv6 プレフィックスリストのエントリを作成します。
ステップ 5	**ipv6 snooping policy** *snooping-policy-id* 例： `Device(config)# ipv6 snooping policy xyz`	IPv6 スヌーピング コンフィギュレーション モードを開始し、指定されたスヌーピング ポリシーの設定を変更できるようします。
ステップ 6	**destination-glean** {**recovery** | **log-only**} [**dhcp**] 例： `Device(config-ipv6-snooping)# destination-glean recovery dhcp`	宛先アドレスは DHCP からリカバリする必要があることを指定します。 （注） ロギング（リカバリなし）が必要な場合は、**destination-glean log-only** コマンドを使用します。
ステップ 7	**data-glean** {**recovery** | **log-only**} [**ndp** | **dhcp**] 例： `Device(config-ipv6-snooping)# data-glean recovery ndp`	ソース（または「データ」）アドレス グリーニングを使用して、IPv6 ファーストホップ セキュリティ バインディング テーブルのリカバリをイネーブルにします。 （注） ロギング（リカバリなし）が必要な場合は、**data-glean log-only** コマンドを使用します。
ステップ 8	**prefix-glean** 例： `Device(config-ipv6-snooping)# prefix-glean`	デバイスが IPv6 ルータ アドバタイズメント（RA）または Dynamic Host Configuration Protocol（DHCP）からプレフィックスを収集できるようにします。

	コマンドまたはアクション	目的
ステップ 9	**protocol dhcp** [**prefix-list** *prefix-list-name*] 例： `Device(config-ipv6-snooping)# protocol dhcp prefix-list abc`	（任意）アドレスを DHCP で収集し、プロトコルを特定の IPv6 プレフィックス リストと関連付ける必要があることを指定します。
ステップ 10	**exit** 例： `Device(config-ipv6-snooping)# exit`	IPv6 スヌーピング コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**ipv6 destination-guard policy** *policy-name* 例： `Device(config)# ipv6 destination-guard policy xyz`	（任意）宛先ガード コンフィギュレーション モードを開始し、指定した宛先ガード ポリシーの設定を変更できるようにします。
ステップ 12	**enforcement** {**always** | **stressed**} 例： `Device(config-destguard)# enforcement stressed`	ポリシーの強制レベルを、すべての条件下で強制するか、システムに負荷がかかっている場合のみ強制するか設定します。
ステップ 13	**exit** 例： `Device(config-destguard)# exit`	宛先ガード コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 14	**interface** *type number* 例： `Device(config)# interface Gigabitethernet 0/0/1`	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 15	**ipv6 snooping attach-policy** *snooping-policy* 例： `Device(config-if)# ipv6 snooping attach-policy xyz`	インターフェイスに IPv6 スヌーピング ポリシーを対応付けます。
ステップ 16	**ipv6 destination-guard attach-policy** *policy-name* 例： `Device(config-if)# ipv6 destination-guard attach-policy xyz`	指定したインターフェイスに宛先ガード ポリシーを対応付けます。 （注） IPv6 宛先ガード ポリシーの設定方法の詳細については、「IPv6 宛先ガード」を参照してください。
ステップ 17	**end** 例：	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
	`Device(config-if)# end`	

アドレス収集の設定およびリカバリ プロトコルとプレフィックス リストの関連付け

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 snooping policy** *snooping-policy-id*
4. **protocol** {**dhcp** | **ndp**} [**prefix-list** *prefix-list-name*]
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ipv6 snooping policy** *snooping-policy-id* 例： `Device(config)# ipv6 snooping policy 200`	IPv6 スヌーピング コンフィギュレーション モードを開始し、指定されたスヌーピング ポリシーの設定を変更できるようします。
ステップ 4	**protocol** {**dhcp**	**ndp**} [**prefix-list** *prefix-list-name*] 例： `Device(config-ipv6-snooping)# protocol dhcp prefix-list dhcp_prefix_list`	Dynamic Host Configuration Protocol（DHCP）で収集される必要があるアドレスを指定し、リカバリ プロトコル（DHCP）とプレフィックス リストを関連付けます。
ステップ 5	**end** 例： `Device(config-ipv6-snooping)# end`	IPv6 スヌーピング 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 デバイス トラッキングの設定

IPv6 デバイス トラッキング機能のバインディング テーブルでエントリのライフ サイクルを細かく調整するには、次の作業を実行します。IPv6 デバイス トラッキングが機能するには、バインディング テーブルにデータを入力する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 neighbor tracking** [**retry-interval** *value*]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `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 neighbor tracking** [**retry-interval** *value*] 例： `Device(config)# ipv6 neighbor tracking`	バインディング テーブルのエントリを追跡します。

IPv6 プレフィックス収集の設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 snooping policy** *snooping-policy*
4. **prefix-glean** ［**only**］

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：	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
	`Device> enable`	
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** *snooping-policy* 例： `Device(config)# ipv6 snooping policy policy1`	IPv6 スヌーピング ポリシーを設定し、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	**prefix-glean** ［**only**］ 例： `Device(config-ipv6-snooping)# prefix-glean`	デバイスが IPv6 RA または DHCPv6 トラフィックからプレフィックスを収集できるようにします。

IPv6 スヌーピングの設定例

例：インターフェイスの IPv6 ND インスペクションの設定

```
Device(config)# ipv6 snooping policy policy1
Device(config-ipv6-snooping)# exit
Device(config)# interface Gigabitethernet 0/0/1
Device(config-if)# ipv6 snooping attach-policy policy1
.
.
.
Device# show ipv6 snooping policies interface gigabitethernet 0/0/1
Target               Type  Policy               Feature        Target range
Gi0/0/1              PORT  my_policy            Destination Gu vlan all
Gi0/0/1              PORT  policy1              Snooping       vlan all
```

例：IPv6 バインディング テーブルの内容の設定

```
Device(config)# ipv6 neighbor binding 2001:DB8:0:ABCD::1 interface GigabitEthernet 0/0/1
 reachable-lifetime 100
Device(config)# ipv6 neighbor binding max-entries 100
Device(config)# ipv6 neighbor binding logging
Device(config)# exit
```

例：IPv6 ファーストホップ セキュリティ バインディング テーブルのリカバリの設定

```
Device> enable
Device# configure terminal
Device(config)# ipv6 neighbor binding 2001:db8::1 interface Gigabitethernet3/0/1
Device(config)# ipv6 prefix-list abc permit 2001:DB8::/64 ge 128
Device(config)# ipv6 snooping policy xyz
Device(config-ipv6-snooping)# destination-glean recovery dhcp
Device(config-ipv6-snooping)# data-glean recovery ndp
Device(config-ipv6-snooping)# prefix-glean
Device(config-ipv6-snooping)# protocol dhcp prefix-list abc
Device(config-ipv6-snooping)# exit
Device(config)# ipv6 destination-guard policy xyz
Device(config-destguard)# enforcement stressed
Device(config-destguard)# exit
Device(config)# interface Gigabitethernet 0/0/1
Device(config-if)# ipv6 snooping attach-policy xyz
Device(config-if)# ipv6 destination-guard attach-policy xyz
Device(config-if)# end
```

例：アドレス収集の設定およびリカバリプロトコルとプレフィックスリストの関連付け

次の例は、NDP がすべてのアドレスのリカバリに使用され、DHCP が dhcp_prefix_list という名前のプレフィックス リストと一致するアドレスのリカバリに使用されることを示しています。

```
Device(config-ipv6-snooping)# protocol ndp
Device(config-ipv6-snooping)# protocol dhcp prefix-list dhcp_prefix_list
```

Cisco TrustSec の概要の機能情報

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 : Cisco TrustSec* の概要の機能情報

機能名	リリース	機能情報
IPv6 の有効化 - インライン タギング	Cisco IOS XE Fuji 16.8.1	IPv6 のサポートが導入されました。

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。