SISFベースのデバイストラッキングの設定

SISF ベースのデバイストラッキングに関する情報

SISF ベースのデバイストラッキングの概要

スイッチ統合セキュリティ機能ベース（SISF ベース）のデバイストラッキング機能は、一連のファーストホップセキュリティ機能の一部です。

この機能の主な役割は、ネットワーク内のエンドノードの存在、ロケーション、移動を追跡することです。SISF は、スイッチが受信したトラフィックをスヌーピングし、デバイスアイデンティティ（MAC と IP アドレス）を抽出して、バインディングテーブルに保存します。IEEE 802.1X、web 認証、Cisco TrustSec、LISP などの多くの機能は、この情報の正確性に依存して正常に動作します。

SISF ベースのデバイストラッキングは、IPv4 と IPv6 の両方をサポートします。

SISF ベースのデバイストラッキングが導入されても、レガシーデバイストラッキング CLI（IP デバイストラッキング（IPDT）および IPv6 スヌーピング CLI）は引き続き使用できます。スイッチをブートアップすると、使用可能なコマンドのセットは既存の設定によって異なり、次のいずれかのみが使用可能です。

- SISF ベースのデバイストラッキング CLI、または
- IPDT および IPv6 スヌーピング CLI

（注） IPDT および IPv6 スヌーピングコマンドは廃止されましたが、引き続き使用できます。SISF ベースのデバイストラッキングにアップグレードすることを推奨します。

IPDT および IPv6 スヌーピング CLI を使用していて、SISF ベースのデバイストラッキングに移行する場合、詳細については「レガシー *IPDT* と *IPv6* スヌーピングから *SISF* ベースのデバイストラッキングへの移行」を参照してください。

SISF ベースのデバイストラッキングは、手動で（**device-tracking** コマンドを使用して）、またはプログラムで（デバイス トラッキング サービスを他の機能に提供する場合に）有効にできます。

SISF ベースのデバイストラッキングを有効にするオプション

デフォルトでは、SISF ベースのデバイストラッキングは無効になっています。

デバイス トラッキング ポリシーを定義し、そのポリシーを特定のターゲットに適用することで、有効にできます。

（注） ターゲットは、インターフェイスまたは VLAN です。

SISF ベースのデバイストラッキングの手動による有効化

- オプション 1：**default** デバイス トラッキング ポリシーをターゲットに適用します。

  インターフェイス コンフィギュレーション モードまたは VLAN コンフィギュレーション モードで、**device-tracking** コマンドを入力します。次に、システムは**default**ポリシーをインターフェイスまたは VLAN に対応付けます。

  （注） **default**ポリシーは、デフォルト設定の組み込みポリシーです。**default**ポリシーの属性は変更できません。デバイストラッキング ポリシーの属性を設定できるようにするには、カスタムポリシーを作成する必要があります。「オプション *2*：カスタム設定でカスタムポリシーを作成します」を参照してください。

- オプション 2：カスタム設定でカスタムポリシーを作成します。

  グローバル コンフィギュレーション モードで device-tracking policy コマンドを入力し、続けてカスタムポリシー名を入力します。システムにより、指定した名前のポリシーが作成されます。その後、デバイス トラッキング コンフィギュレーション モード（config-device-tracking）で使用可能な設定を行い、指定したターゲットにポリシーをアタッチできます。

プログラムによる SISF ベースのデバイストラッキングの有効化

一部の機能はデバイストラッキングに依存し、SISF ベースのデバイストラッキングが構築および維持するバインディングエントリの信頼性のあるデータベースを利用します。これらの機能

は、デバイス トラッキング クライアントとも呼ばれ、プログラムによりデバイストラッキングを有効にします（デバイス トラッキング ポリシーを作成して対応付けします）。

（注） ここでの例外は、IEEE 802.1X、web 認証、Cisco TrustSec、IP ソースガード（IPSG）です。これらはデバイストラッキングにも依存しますが、有効にはなりません。これらのデバイス トラッキング クライアントでは、**ip dhcp snooping vlan** *vlan* コマンドを入力して、プログラムにより特定のターゲットでデバイストラッキングを有効にする必要があります。

プログラムによる SISF ベースのデバイストラッキングの有効化については、次の点に注意してください。

- デバイス トラッキング クライアントでは、デバイストラッキングを有効にする必要があります。

  複数のデバイス トラッキング クライアントが存在するため、複数のプログラムポリシーを作成できます。各ポリシーの設定は、ポリシーを作成するデバイス トラッキング クライアントによって異なります。

- 作成されるポリシーとその設定はシステム定義です。

  設定可能なポリシー属性は、デバイス トラッキング コンフィギュレーション モード（config-device-tracking）で使用でき、リリースごとに異なります。設定不可能な属性を変更しようとすると、設定変更は拒否され、エラーメッセージが表示されます。

プログラムによって作成されたポリシーのリリース固有の情報については、マニュアルの必要なバージョンの『*Cisco IOS XE <release name> <release number>*』の「Programmatically Enabling SISF-Based Device Tracking」を参照してください。

レガシーコマンドから SISF ベースの Device-Tracking コマンドへの移行

レガシー IPDT と IPv6 スヌーピングから SISF ベースのデバイストラッキングへの移行

Cisco IOS XE Denali 16.1.1 以降では、既存の IPv6 スヌーピングおよび IP デバイストラッキング（IPDT）に、対応する SISF ベースの device-tracking コマンドが用意され、IPv4 と IPv6 の両方のアドレスファミリに設定を適用できるようになりました。

Cisco IOS XE 3.xx リリースから Cisco IOS XE 16.xx リリースにアップグレードした後、**device-tracking upgrade-cli** を入力してレガシー IPDT および IPv6 スヌーピングコマンドを SISF ベースのデバイス トラッキング コマンドに変換します。このコマンドを実行した後は、新しい device-tracking コマンドのみがデバイスで使用でき、レガシーコマンドはサポートされません。

デバイスにあるレガシー設定に基づいて、**device-tracking upgrade-cli** コマンドは CLI を異なる方法でアップグレードします。既存の設定を移行する前に、次の設定シナリオ、および対応する移行結果を検討します。

（注） 古い IPDT IPv6 スヌーピング CLI と新しい SISF ベースデバイストラッキング CLI の両方を設定することはできません。

IPDT 設定のみが存在する

デバイスに IPDT 設定のみがある場合は、**device-tracking upgrade-cli** コマンドを実行すると、設定が変換され、新しく作成されてインターフェイスで適用される SISF ポリシーが使用されます。これにより、この SISF ポリシーを更新できます。

引き続きレガシーコマンドを使用する場合、レガシーモードでの操作が制限されます。このモードでは、レガシー IPDT と IPv6 スヌーピングコマンドのみがデバイスで使用可能になります。

IPv6 スヌーピング設定のみが存在する

既存の IPv6 スヌーピング設定があるデバイスで、古い IPv6 スヌーピングコマンドを以降の設定に使用できます。次のオプションを使用できます。

- （推奨）**device-tracking upgrade-cli** コマンドを使用して、レガシー設定をすべて、新しい SISF ベースの device-tracking コマンドに変換します。変換後は、新しいデバイストラッキング コマンドのみがデバイスで動作します。
- レガシー IPv6 スヌーピングコマンドを今後の設定に使用し、**device-tracking upgrade-cli** コマンドは実行しません。このオプションでは、デバイスで使用可能なのはレガシー IPv6 スヌーピングコマンドのみであり、新しい SISF ベースの device-tracking CLI コマンドは使用できません。

IPDT と IPv6 スヌーピングの両方の設定が存在する

レガシー IPDT 設定と IPv6 スヌーピング設定の両方が存在するデバイスでは、レガシーコマンドを SISF ベースのデバイストラッキング CLI に変換できます。ただし、インターフェイスに適用することができるスヌーピングポリシーは 1 つだけであり、IPv6 スヌーピング ポリシー パラメータは IPDT 設定よりも優先される、ということに注意してください。

（注） 新しい SISF ベースのコマンドに移行しておらず、レガシー IPv6 スヌーピングや IPDT コマンドを使用し続けている場合、IPv4 デバイストラッキング設定情報が IPv6 スヌーピングコマンドに表示される可能性があります。SISF ベースのデバイストラッキング機能では、IPv4 と IPv6 の両方の設定を扱うためです。これを回避するには、レガシー設定を SISF ベースのデバイストラッキング コマンドに変換することを推奨します。

IPDT または IPv6 スヌーピング設定が存在しない

デバイスにレガシー IP デバイストラッキング設定も IPv6 スヌーピング設定もない場合は、今後の設定に使用できるのは新しい SISF ベースの device-tracking コマンドのみです。レガシー IPDT コマンドと IPv6 スヌーピングコマンドは使用できません。

（注） Cisco IOS XE Denali 16.3.1 以降、**ip dhcp snooping vlan** *vlan* コマンドは、IEEE 802.1X、web 認証、Cisco TrustSec、IPSG 機能をサポートするために、プログラムによってデバイス トラッキング ポリシーを作成します。プログラムによって作成されたポリシーは、IPv4 および IPv6 クライアントの両方を追跡します。前述の機能のいずれかを使用している場合、このコマンドが設定されていることを確認します。

IPDT、IPv6 スヌーピング、および SISF ベースのデバイストラッキング CLI の互換性

表 1 : IPDT → IPv6 スヌーピングコマンド （5 ページ） に、**device-tracking upgrade-cli** コマンド（グローバル コンフィギュレーション モード）が実行されていない場合に、レガシー IPDT と、それらが変換される IPv6 スヌーピングコマンドを示します。

表 表 2 : IPDT → SISF コマンド （6 ページ） に、**device-tracking upgrade-cli** コマンドを実行した場合に、レガシー IPDT と、それをシステムが変換する SISF ベースの device-tracking コマンドを示します。

表 *1 : IPDT → IPv6* スヌーピングコマンド

レガシー IP デバイストラッキング（IPDT）	IPv6 スヌーピングコマンド（Cisco IOS XE Denali 16.3.7 以降のすべての Cisco IOS XE 16.xx リリース）。
ip device tracking probe count	デフォルト値に設定されており、変更できません。
ip device tracking probe delay	デフォルト値に設定されており、変更できません。[1]。
ip device tracking probe interval	**ipv6 neighbor binding reachable-lifetime**[2]
ip device tracking probe use-svi	デフォルトの動作に設定されており、変更できません。
ip device tracking probe auto-source [**fallback** *host-ip-address subnet-mask*] [**override**]	**ipv6 neighbor tracking auto-source** [**fallback** *host-ip-address subnet-mask*] [**override**]
ip device tracking trace-buffer	サポート対象外
ip device tracking maximum n	**ipv6 snooping policy** *IPDT_MAX_n* [**limit** *address-count*]
ip device tracking maximum 0	サポート対象外
clear ip device tracking all	サポート対象外

[1] Cisco IOS XE Denali 16.3.6 まで、および Cisco IOS XE Everest 16.5.1a では、システムは **ip device tracking probe delay** コマンドを誤って **ipv6 neighbor binding reachable-lifetime** に変換します。Cisco IOS XE Denali 16.3.7 以降（Cisco IOS XE Everest 16.5.x を除く）では、デフォルト値に設定されており、変更できません。

[2] Cisco IOS XE Denali 16.3.6 まで、および Cisco IOS XE Everest 16.5.1a では、システムが **ip device tracking probe interval** コマンドを誤って **ipv6 snooping tracking retry-interval** に変換します。Cisco IOS XE Denali 16.3.7 以降（Cisco IOS XE Everest 16.5.x を除く）では、**ipv6 neighbor binding reachable-lifetime** に正しく変換されます。

表 *2 : IPDT → SISF* コマンド

レガシー IP デバイストラッキング（IPDT）	SISF 変換後の SISF ベースのデバイストラッキング（Cisco IOS XE Denali 16.3.7 以降のすべての Cisco IOS XE 16.xx リリース）。
ip device tracking probe count	デフォルト値に設定されており、変更できません。
ip device tracking probe delay	デフォルト値に設定されており、変更できません。[3]。
ip device tracking probe interval	**device-tracking binding reachable-lifetime**[4]
ip device tracking probe use-svi	デフォルトの動作に設定されており、変更できません。
ip device tracking probe auto-source [**fallback** *host-ip-address subnet-mask*] [**override**]	**device-tracking tracking auto-source** [**fallback** *host-ip-address subnet-mask*] [**override**]
ip device tracking trace-buffer	未サポート
ip device tracking maximum n	**device-tracking snooping policy** *IPDT_MAX_n* [**limit** *address-count*]
ip device tracking maximum 0	未サポート
clear ip device tracking all	未サポート

[3] Cisco IOS XE Denali 16.3.6 まで、および Cisco IOS XE Everest 16.5.1a では、システムは **ip device tracking probe delay** コマンドを誤って **device-tracking binding reachable-lifetime** に変換します。Cisco IOS XE Denali 16.3.7 以降（Cisco IOS XE Everest 16.5.x を除く）では、デフォルト値に設定されており、変更できません。

[4] Cisco IOS XE Denali 16.3.6 まで、および Cisco IOS XE Everest 16.5.1a では、システムが **ip device tracking probe interval** コマンドを誤って **device-tracking tracking retry-interval** に変換します。Cisco IOS XE Denali 16.3.7 以降（Cisco IOS XE Everest 16.5.1a を除く）では、**device-tracking binding reachable-lifetime** に正しく変換されます。

SISF ベースのデバイストラッキングの設定方法

SISF ベースのデバイストラッキングの手動による有効化

ターゲットへのデフォルト デバイス トラッキング ポリシーの適用

デフォルトのデバイス トラッキング ポリシーをインターフェイスまたは VLAN に適用するには、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	**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 2	インターフェイスまたは VLAN を指定します。
	• **interface** *interface*
	• **vlan configuration** *vlan_list*
	例：
	`Device(config)# interface gigabitethernet 1/1/4`
	OR
	`Device(config)# vlan configuration 333`
		interface *type number*—Specifies the interface and enters the interface configuration mode. デバイス トラッキング ポリシーは、指定されたインターフェイスに適用されます。
		vlan configuration *vlan_list*：VLAN を指定し、VLAN機能コンフィギュレーション モードを開始します。デバイス トラッキング ポリシーは、指定された VLAN に適用されます。

ステップ 3	**device-tracking**
	例：
	`Device(config-if)# device-tracking`
	OR
	`Device(config-vlan-config)# device-tracking`
		SISF ベースのデバイストラッキングを有効にし、デフォルトポリシーをインターフェイスまたは VLAN に適用します。
		デフォルトポリシーは、デフォルト設定の組み込みポリシーです。デフォルトポリシーの属性は変更できません。

ステップ 4	**exit**
	例：
	`Device(config-if)# exit`
	OR
	`Device(config-vlan-config)# exit`
		設定モードを終了します。

	コマンドまたはアクション	目的
ステップ 5	**show device-tracking policy** *policy-name* 例： `Device# show device-tracking policy default`	デバイストラッキング ポリシーの設定と、それが適用されるすべてのターゲットを表示します。

カスタム設定を使用したカスタム デバイス トラッキング ポリシーの作成

デバイス トラッキング ポリシーを作成して設定するには、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	**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 2	[**no**] **device-tracking policy** *policy-name* 例： `Device(config)# device-tracking policy example_policy`	ポリシーを作成し、デバイストラッキング コンフィギュレーション モードを開始します。

ステップ 3	[**data-glean** | **default** | **destination-glean** | **device-role** | **distribution-switch** | **exit** | **limit** | **no** | **prefix-glean** | **protocol** | **security-level** | **tracking** | **trusted-port** | **vpc**]
	例：
	`Device (config-device-tracking)# destination-glean log-only`
		システムプロンプトに疑問符（?）を入力すると、このモードで使用できるオプションのリストが表示されます。IPv4 と IPv6 の両方に対して以下を設定できます。
		• （任意）**data-glean**：ネットワーク内の送信元からスヌーピングされたデータパケットからのアドレスの学習を有効にし、データトラフィックの送信元アドレスとともにバインディングテーブルを読み込みます。次のいずれかのオプションを入力します。
		  • log-only：データパケット通知時に syslog メッセージを生成します。
		  • recovery：プロトコルを使用してバインディングテーブルの回復を有効にします。**NDP**または**DHCP**の入力。

	コマンドまたはアクション	目的
		• （任意）**default**：ポリシー属性をデフォルト値に設定します。次のポリシー属性をデフォルト値に設定できます。**data-glean**、**destination-glean**、**device-role**、**limit**、**prefix-glean**、**protocol**、**security-level**、**tracking**、**trusted-port**。 • （任意）**destination-glean**：データトラフィックの宛先アドレスを収集して、バインディングテーブルを読み込みます。次のいずれかのオプションを入力します。 • log-only：データパケット通知時に syslog メッセージを生成します。 • recovery：プロトコルを使用してバインディングテーブルの回復を有効にします。**DHCP** を入力します。 • （任意）**device-role**；ポートに接続されているデバイスのロールを設定します。ノードまたはスイッチを指定できます。次のいずれかのオプションを入力します。 • node：接続されているデバイスをノードとして設定します。これがデフォルトのオプションです。 • switch：接続されているデバイスをスイッチとして設定します。 • （任意）**distribution-switch**：このオプションは CLI には表示されますが、サポートされていません。行った設定は有効になりません。

	コマンドまたはアクション	目的

		• **exit**：デバイストラッキング ポリシー コンフィギュレーション モードを終了します。
		• **limit** address-count：ポートごとのアドレスカウント制限を指定します。有効な範囲は1～32000です。
		• **no**：コマンドを無効にするか、デフォルト値を設定します。
		•（任意）**prefix-glean**：IPv6 ルータ アドバタイズメントまたは DHCP-PD のどちらかからのプレフィックスの学習を有効にします。次のオプションがあります。
		  • （任意）**only**：プレフィックスのみを収集し、ホストアドレスは収集しません。
		• （任意）**protocol**：収集するプロトコルを設定します。デフォルトでは、すべて収集されます。次のいずれかのオプションを入力します。
		  • **arp** ［**prefix-list** *name*］：ARP パケットのアドレスを収集します。必要に応じて、照合するプレフィックスリストの名前を入力します。
		  • **dhcp4** ［**prefix-list** *name*］：DHCPv4 パケットのアドレスを収集します。必要に応じて、照合するプレフィックスリストの名前を入力します。
		  • **dhcp6** ［**prefix-list** *name*］：DHCPv6 パケットのアドレスを収集します。必要に応じて、照合するプレフィックスリストの名前を入力します。
		  • **ndp** ［**prefix-list** *name*］：NDP パケットのアドレスを収集します。必要に応じて、照合するプ

	コマンドまたはアクション	目的
		レフィックスリストの名前を入力します。 • **udp** ［**prefix-list** *name*］：このオプションは CLI には表示されますが、サポートされていません。行った設定は有効になりません。 • （任意）**security-level**：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。次のいずれかのオプションを入力します。 • **glean** ：アドレスをパッシブに収集します。 • **guard** ：不正なメッセージを検査してドロップします。これはデフォルトです。 • **inspect** ：メッセージを収集して検証します。 • （オプション）**tracking**：トラッキングオプションを指定します。次のいずれかのオプションを入力します。 • **disable** ［**stale-lifetime** ［*1* ー *86400* 秒 | **infinite**］ ］ ：デバイストラッキングをオフにします。 必要に応じて、エントリを削除するまで非アクティブにする期間を入力することも、永続的に非アクティブにすることもできます。 • **enable** ［**reachable-lifetime** ［*1* ー *86400* 秒 | **infinite**］ ］ ：デバイストラッキングをオンにします。 必要に応じて、エントリを到達可能にする期間を入力すること

	コマンドまたはアクション	目的
		も、永続的に到達可能にすることもできます。 • （任意）**trusted-port**：信頼できるポートを設定します。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。 • （任意）**vpc**：このオプションはCLIには表示されますが、サポートされていません。行った設定は有効になりません。
ステップ 4	**end** 例： `Device(config-device-tracking)# exit`	設定モードを終了します。
ステップ 5	**show device-tracking policy** *policy-name* 例： `Device# show device-tracking policy example_policy`	デバイス トラッキング ポリシー設定を表示します。

次のタスク

ポリシーをインターフェイスまたは VLAN に適用します。

デバイス トラッキング ポリシーのインターフェイスへの適用

デバイス トラッキング ポリシーをインターフェイスにアタッチするには、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	**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 2	**interface** *interface* 例： `Device(config)# interface gigabitethernet 1/1/4`	インターフェイスを指定し、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	[**no**] **device-tracking attach-policy** *policy name* 例： `Device(config-if)# device-tracking attach-policy example_policy`	デバイス トラッキング ポリシーをインターフェイスに適用します。 （注） SISF ベースのデバイス トラッキング ポリシーは、カスタム ポリシーである場合にのみ無効にできます。プログラムによって作成されたポリシーは、対応するデバイストラッキング クライアント機能の設定が削除された場合にのみ削除できます。
ステップ 4	**end** 例： `Device# end`	特権 EXEC モードに戻ります。
ステップ 5	**show device-tracking policies** [**interface** *interface*] 例： `Device# show device-tracking policies interface gigabitethernet 1/1/4`	指定されたインターフェイスの種類と番号に一致するポリシーを表示します。

デバイス トラッキング ポリシーの VLAN への適用

複数のインターフェイスでデバイス トラッキング ポリシーを VLAN にアタッチするには、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	**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 2	**vlan configuration** *vlan_list* 例： `Device(config)# vlan configuration 333`	デバイス トラッキング ポリシーを適用する VLAN を指定し、その VLAN インターフェイスのコンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	[no] device-tracking attach-policy *policy_name* 例： `Device(config-vlan-config)# device-tracking attach-policy example_policy`	すべてのスイッチインターフェイスで、デバイス トラッキング ポリシーを指定された VLAN にアタッチします。 （注） SISF ベースのデバイス トラッキング ポリシーは、カスタム ポリシーである場合にのみ無効にできます。プログラムによって作成されたポリシーは、対応するデバイストラッキング クライアント機能の設定が削除された場合にのみ削除できます。
ステップ 4	do show device-tracking policies vlan *vlan-ID* 例： `Device(config-vlan-config)# do show device-tracking policies vlan 333`	VLAN インターフェイス コンフィギュレーション モードを終了しないで、ポリシーが指定された VLAN に割り当てられていることを確認します。

Cisco IOS XE Everest 16.6.x での SISF ベースのデバイストラッキングのプログラムによる有効化

表 *3 : Cisco IOS XE Everest 16.6.x* での *SISF* ベースのデバイストラッキングのプログラムによる有効化

SISF ベースのデバイストラッキングを有効にできるデバイス トラッキング クライアント機能	このリリースでは、次の機能に対して SISF ベースのデバイストラッキングをプログラムで有効にできます。 • IEEE 802.1X、web 認証、Cisco TrustSec、IPSG 機能：**ip dhcp snooping vlan** *vlan* コマンドを入力します。 • Cisco Locator/ID Separation Protocol（LISP）。 （注） プログラムによって作成されたポリシーが複数ある場合、LISP 設定は有効です。これは、他のデバイス トラッキング クライアント機能の動作に悪影響を与えることはありません。たとえば、IEEE 802.1X の **ip dhcp snooping vlan** *vlan* コマンドを設定し、LISP を設定して SISF ベースのデバイストラッキングを有効にした場合も、IEEE 802.1X 機能は予期どおりに動作し続けます。

[Policy Name]	DT-PROGRAMMATIC 複数のデバイス トラッキング クライアント機能がありますが、システムによって生成されたポリシーは同一です。設定のリストは、プログラムによって作成されたポリシーにより異なる場合があります。詳細については、例を参照してください。

ユーザ オプション	• 同じインターフェイスまたは VLAN に適用することができるのは、1 つのポリシーだけです。
	• ポリシーを別のポリシーに置き換えることはできません。
	• デバイストラッキング クライアント機能の設定が削除されない限り、ポリシーは削除できません。
	• プログラムによって作成されたポリシーの次の設定を変更できます（デバイス トラッキング コンフィギュレーション モード（config-device-tracking）での **device-tracking policy** コマンド）。
	  • **data-glean**
	  • **default**
	  • **device-role**
	  • **destination-glean**
	  • **exit**
	  • **limit**
	  • **no**
	  • **prefix-glean**
	  • **protocol**
	  • **security-level**
	  • **tracking**
	  • trusted-port
	  • **distribution-switch** および **vpc** は CLI に表示されますが、設定の変更は有効になりません。
	• MAC設定ごとのアドレスカウント制限は変更できません（これは**limit address-count for IPv4 per mac** および **limit address-count for IPv6 per mac** コマンドを参照）が、ポートまたはインターフェイスごとのアドレスカウント制限は変更できます。
	• デバイストラッキング ポリシーが VLAN のインターフェイスに適用されると、インターフェイスのポリシー設定がVLANのポリシー設定よりも優先されます。ここでの例外は、**limit address-count for IPv4 per mac** と **limit address-count for IPv6 per mac** の値で、インターフェイスと VLAN の両方のポリシーから集約されます。

トランクポートからのバインディングエントリの作成を停止するためのマルチスイッチネットワークの設定

マルチスイッチネットワークでは、SISF ベースのデバイストラッキングにより、機能を実行しているスイッチ間でバインディング テーブル エントリを分散できます。バインディングエントリは、ホストがアクセスポートに表示されるスイッチでのみ作成されます。トランクポート経由で表示されるホストのエントリは作成されません。これは、**trusted-port** および **device-role switch** オプションを使用してポリシーを設定し、トランクポートに適用することで実現されます。

重要 ポリシーで、**trusted-port** および **device-role switch** オプションの両方を設定する必要があります。

さらに、SISF ベースのデバイストラッキングが有効になっているデバイス側のポートに、このようなポリシーを適用することを推奨します。

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	**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 2	**device-tracking policy** *policy-name* **例：** `Device(config)# device-tracking policy example_trusted_policy`	指定されたポリシーのデバイストラッキング 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 3	**device-role switch** **例：** `Device(config-device-tracking)# device-role switch`	ポートに接続されているデバイスのロールを指定します。デフォルトは node です。ポートのバインディングエントリの作成を停止する **device-role switch** オプションを入力します。
ステップ 4	**trusted-port** **例：** `Device(config-device-tracking)# trusted-port`	信頼できるポートを設定します。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

	コマンドまたはアクション	目的
		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-device-tracking)# end`	デバイストラッキング ポリシー コンフィギュレーション モードを終了します。続いて、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 6	**interface** *interface* 例： `Device(config)# interface gigabitethernet 1/0/25`	インターフェイスを指定し、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 7	**device-tracking attach-policy** *policy-name* 例： `Device(config-if)# device-tracking attach-policy example_trusted_policy`	デバイス トラッキング 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で指定された VLAN にアタッチします。

SISF ベースのデバイストラッキングの設定例

次の例は、デバイストラッキングの設定例と、特定の状況で推奨される、または関連するその他の設定を示しています。

例：Cisco IOS XE Everest 16.6.x での SISF ベースのデバイストラッキングのプログラムによる有効化

例の出力例は、プログラムによって作成されたポリシーのさまざまな設定を示しています。

デバイス トラッキング クライアント：LISP

ここでの LISP の設定は、あくまでも一例です。

LISP を設定した後、特権 EXEC モードで **show device-tracking policy** コマンドを入力して、作成された DT-PROGRAMMATIC ポリシーと対応する設定を表示します。

```
Device(config)# router lisp
<output truncated>
Device(config-router-lisp)# instance-id 3
Device(config-router-lisp-instance)# service ethernet
Device(config-router-lisp-instance-service)# eid-table vlan 10
Device(config-router-lisp-instance-dynamic-eid)# database-mapping 10.1.1.0/24 locator-set
 set1
Device(config-router-lisp-instance-service)# exit-service-ethernet
Device(config-router-lisp-instance)# exit-instance-id
Device(config-router-lisp)# exit-router-lisp
```

```
Device# show device-tracking policy DT-PROGRAMMATIC
Policy DT-PROGRAMMATIC configuration:
  security-level guard (*)
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  limit address-count for IPv4 per mac 1 (*)
  limit address-count for IPv6 per mac 8 (*)
  tracking enable
Policy DT-PROGRAMMATIC is applied on the following targets:
Target      Type  Policy             Feature           Target range
vlan 10     VLAN  DT-PROGRAMMATIC    Device-tracking   vlan all
 note:
 Binding entry Down timer: 10 minutes (*)
 Binding entry Stale timer:   30 minutes (*)
```

デバイス トラッキング クライアント：IEEE 802.1X、web 認証、Cisco TrustSec、IPSG

グローバル コンフィギュレーション モードで **ip dhcp snooping vlan** *vlan* コマンドを設定して、IEEE 802.1X、web 認証、Cisco TrustSec、IPSG 機能のデバイストラッキングを有効にします。特権 EXEC モードで **show device-tracking policy** コマンドを入力し、作成された DT-PROGRMMATIC ポリシーとポリシーに応じて行った設定を表示します。

```
Device# configure terminal
Device(config)# ip dhcp snooping vlan 10
Device(config)# end

Device# show device-tracking policy DT-PROGRAMMATIC
Policy DT-PROGRAMMATIC configuration:
  security-level glean (*)
  device-role node
  gleaning from Neighbor Discovery
  gleaning from DHCP
  gleaning from ARP
  gleaning from DHCP4
  NOT gleaning from protocol unkn
  limit address-count for IPv4 per mac 1 (*)

  tracking enable
Policy DT-PROGRAMMATIC is applied on the following targets:
Target   Type    Policy             Feature          Target range
vlan 10  VLAN    DT-PROGRAMMATIC    Device-tracking  vlan all
  note:
  Binding entry Down timer: 24 hours (*)
  Binding entry Stale timer:   24 hours (*)
```

例：ターゲットでの IPv6 デバイストラッキングの無効化

デフォルトでは、SISF ベースのデバイストラッキングは IPv4 と IPv6 の両方をサポートします。次の設定例は、必要な場合に IPv6 デバイストラッキングを無効にする方法を示しています。

ターゲットがカスタムポリシーに適用されている場合の**IPv6**デバイストラッキングの無効化：

```
Device(config)# device-tracking policy example-policy
 Device(config-device-tracking)# no protocol ndp
 Device(config-device-tracking)# no protocol dhcp6
 Device(config-device-tracking)# end
```

ターゲットがプログラムによるポリシーに適用されている場合の**IPv6**デバイストラッキングの無効化：

（注） Cisco IOS XE Denali 16.3.x および Cisco IOS XE Everest 16.5.x のリリースで IPv6 デバイストラッキングを無効にすることはできません。

Cisco IOS XE Everest 16.6.x では、プログラムによるポリシーを変更することで、IPv6 デバイストラッキングを無効にできます。

```
Device(config)# device-tracking policy DT-PROGRAMMATIC
Device(config-device-tracking)# no protocol ndp
Device(config-device-tracking)# no protocol dhcp6
Device(config-device-tracking)# end
```

例：VLAN 上の SVI に対する IPv6 の有効化（重複アドレスの問題を軽減するため）

ネットワークで IPv6 が有効になっており、VLAN 上でスイッチ仮想インターフェイス（SVI）が設定されている場合は、SVI 設定に次の内容を追加することを推奨します。これにより、SVI はリンクローカルアドレスを自動的に取得できます。このアドレスは SISF プローブの送信元 IP アドレスとして使用されるため、重複 IP アドレスの問題を防止できます。

```
Device(config)# interface vlan 10
Device(config-if)# ipv6 enable
Device(config-if)# end
```

例：IPv4 重複アドレスの問題の緩和

次に、Microsoft Windows を実行しているクライアントによって発生した重複 IP アドレス 0.0.0.0 エラーメッセージの問題に対応する例を示します。

device-tracking tracking auto-source コマンドを設定します。このコマンドは、デバイストラッキングテーブル内のエントリを維持するために、スイッチがクライアントをプローブするよう送信するアドレス解決パケット（ARP）要求で使用される送信元 IP および MAC アドレスを決定します。その目的は、送信元 IP アドレスとして 0.0.0.0 を使用しないようにすることです。

（注） スイッチ仮想インターフェイス（SVI）が設定されていない場合にのみ、**device-tracking tracking auto-source** コマンドを設定します。SVI が VLAN で IPv4 アドレスを使用して設定されている場合は、設定する必要はありません。

コマンド	Action （デバイストラッキング ARP プローブの送信元 IP および MAC アドレスを選択するため）	注記
device-tracking tracking auto-source	• 存在する場合、VLAN SVI に送信元を設定します。 • 同じサブネットからデバイストラッキング テーブルで IP および MAC バインディングを検索します。 • 0.0.0.0 を使用します。	MAC フラッピングを回避するために、すべてのトランクポートでデバイストラッキングを無効にすることを推奨します。
device-tracking tracking auto-source override	• 存在する場合、VLAN SVI に送信元を設定します。 • 0.0.0.0 を使用します。	SVI がない場合は推奨しません。
device-tracking tracking auto-source fallback 0.0.0.X 255.255.255.0	• 存在する場合、VLAN SVI に送信元を設定します。 • 同じサブネットからデバイストラッキング テーブルで IP および MAC バインディングを検索します。 • 提供されたホストビットとマスクを使用して、クライアント IP から送信元 IP を計算します。送信元 MAC は、クライアント側のスイッチポートの MAC アドレスから取得されます*。	MAC フラッピングを回避するために、すべてのトランクポートでデバイストラッキングを無効にすることを推奨します。 計算された IPv4 アドレスは、クライアントまたはネットワークデバイスに割り当てることはできません。

コマンド	Action （デバイストラッキング ARP プローブの送信元 IP および MAC アドレスを選択するため）	注記
device-tracking tracking auto-source fallback 0.0.0.X 255.255.255.0 override	• 存在する場合、VLAN SVI に送信元を設定します。 提供されたホストビットとマスクを使用して、クライアント IP から送信元 IP を計算します*。送信元 MAC は、クライアント側のスイッチポートの MAC アドレスから取得されます*。	

* クライアント IP アドレスによっては、IPv4 アドレスを送信元 IP 用に予約する必要があります。

予約済み送信元 IPv4 アドレス = (client-ip and mask) | host-ip

- クライアント IP = 192.0.2.25
- 送信元 IP = (192.0.2.25 and 255.255.255.0) | (0.0.0.1) = 192.0.2.1

IP アドレス 192.0.2.1 をクライアントまたはネットワークデバイスに割り当てないでください。

例：短いデバイストラッキング バインディング到達可能時間の回避

以前のリリースから移行する場合、次の設定が存在している可能性があります。

```
device-tracking binding reachable-time 10
```

コマンドの **no** バージョンを入力して、これを削除します。

SISF ベースのデバイストラッキングの機能履歴と情報

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。

リリース	変更内容
Cisco IOS XE Denali 16.1.1	この機能が導入されました。

リリース	変更内容
Cisco IOS XE Denali 16.3.7	IPv6 スヌーピングコマンドおよび SISF ベースのデバイストラッキング コマンドのシステム変換を修正。 IPDT → IPv6 スヌーピング変換の修正： • Cisco IOS XE Denali 16.3.6 までは、システムは **ip device tracking probe delay** コマンドを誤って **ipv6 neighbor tracking retry-interval** に変換します。Cisco IOS XE Denali 16.3.7 以降では、デフォルト値に設定されており、変更できません。 • Cisco IOS XE Denali 16.3.6 までは、システムは **ip device tracking probe interval** コマンドを誤って **ipv6 neighbor tracking retry-interval** に変換します。Cisco IOS XE Denali 16.3.7 以降では、に正しく変換されます。 **ipv6 snooping tracking retry-interval** IPDT → SISF 変換の修正： • Cisco IOS XE Denali 16.3.6 までは、システムは **ip device tracking probe delay** コマンドを誤って **device-tracking binding reachable-lifetime** に変換します。指定のリリースでは、このコマンドを引き続き使用できますが、エントリの reachable-lifetime のみを設定できます。Cisco IOS XE Denali 16.3.7 以降では、デフォルト値に設定されており、変更できません。 • Cisco IOS XE Denali 16.3.6 までは、システムは **ip device tracking probe interval** コマンドを誤って **device-tracking tracking retry-interval** に変換します。Cisco IOS XE Denali 16.3.7 以降では、**device-tracking binding reachable-lifetime** に正しく変換されます。
Cisco IOS XE Everest 16.5.1a	LISP を設定することで、この機能をプログラムで有効にできるようになりました。 システムによって生成されたポリシー名が DT-PROGRAMMATIC に変更されます。イネーブラは複数ありますが、システムによって生成されたポリシーは同一です。設定のリストは各イネーブラによって異なります。 カスタムポリシーを作成して、インターフェイスまたは VLAN に付加することもできます。 （注） IPDT → IPv6 および IPDT → SISF のシステム変換の修正は、Cisco IOS XE Denali 16.3.7 から導入されましたが、これらの修正は Cisco IOS XE Everest 16.5.1a では利用できません。
Cisco IOS XE Everest 16.6.1	このリリース以降、DT_PROGRAMMATIC の特定の設定を変更できます（デバイス トラッキング コンフィギュレーション モード（config-device-tracking）で **device-tracking policy** コマンドを使用）。