# IOS IPS ルータの設定

サービス統合型ルータ（ISR）などの一部の Cisco IOS ルータは、IPS 5.1 ソフトウェアに基づいたネイティブな IPS 機能を備えています。これらのデバイス上で基本的な IPS インスペクションを設定することにより、IPSセンサーによるインスペクションを補強したり、小規模ネットワークをサポートしたりできます。

この章は次のトピックで構成されています。


- Cisco IOS IPS について　（1 ページ）
- Cisco IOS IPS 設定の概要　（4 ページ）


## Cisco IOS IPS について

Cisco Security Manager を Cisco IOS Intrusion Prevention System（IOS IPS; IOS 侵入防御システム）とともに使用して、サポートされている Cisco IOS ソフトウェアリリース 12.4(11)T2 以降を使用する Cisco ルータで侵入防御を管理できます。

Cisco IOS IPS は、インライン侵入防御センサーとして機能し、パケットとセッションがルータを通過するときに監視し、各パケットをスキャンして Cisco IOS IPS シグニチャと照合します。疑わしいアクティビティを検出すると、ネットワークセキュリティが侵害される前に対応し、Cisco IOS syslog メッセージまたは Security Device Event Exchange（SDEE）を使用してイベントを記録します。

さまざまな脅威に対して適切な対応を選択するように Cisco IOS IPS を設定できます。Signature Event Action Processor（SEAP）は、忠実度、重大度、ターゲットの価値レーティングなどのパラメータに基づいて、シグニチャイベントが実行するアクションを動的に制御できます。これらのアクションは、[Signatures] ポリシーおよび [Event Actions] ポリシーを使用して Security Manager で設定できます。

セッション内のパケットがシグニチャと一致すると、Cisco IOS IPS は必要に応じて次のいずれかのアクションを実行できます。

- syslog サーバまたは中央管理インターフェイスにアラームを送信する。
- パケットをドロップします。
- 接続をリセットする。

- 指定した期間、攻撃者の送信元 IP アドレスからのトラフィックを拒否する。
- 指定した期間、シグニチャが確認された接続上のトラフィックを拒否する。

シスコでは、柔軟性を念頭に置いてCisco IOS ソフトウェアベースの侵入防御機能およびCisco IOS Firewall を開発しているため、false positive の場合にシグニチャを個別にディセーブルにできます。通常は、ネットワーク セキュリティ ポリシーをサポートするために、ファイアウォールと Cisco IOS IPS の両方をイネーブルにすることを推奨します。ただし、異なるルータ インターフェイス上で、これらの機能を個別にイネーブルにすることもできます。

Cisco IOS IPS 設定プロセスの全般的な説明については、を参照してください。 Cisco IOS IPS 設定の概要 （4 ページ）

ここでは、次の内容について説明します。

- IPS サブシステムおよび IOS IPS リビジョンのサポートについて （2 ページ）
- ライトウェイト シグニチャによる Cisco IOS IPS シグニチャ スキャン （2 ページ）
- ルータ設定ファイルおよびシグニチャ イベント アクション プロセッサ（SEAP） （3 ページ）
- Cisco IOS IPS の制限事項および制約事項 （3 ページ）

# IPS サブシステムおよび IOS IPS リビジョンのサポートについて

Cisco Security Manager では IOS IPS のマイナー リビジョンが自動的にサポートされます。サポートされているマイナーリビジョンを確認するには、IPS サブシステム バージョンが必要です。

IPS サブシステム バージョンは、Cisco IOS IPS 機能の変更の追跡に使用されるバージョン番号です。サブシステム番号は、デバイスのプロパティで表示されます（デバイスを右クリックして [デバイスプロパティ（Device Properties）] を選択）。Cisco IOS IPS を実行しているルータ上のコマンドラインで **show subsys name ips** コマンドを使用して、詳細な Cisco IOS IPS サブシステムのバージョンを表示することもできます。3.x サブシステムは、IPS 5.x に相当します。Cisco IOS ソフトウェアリリースでサポートされているサブシステムのリストについては、Cisco.com で、該当するリリースの Security Manager の『*Supported Devices and Software Versions for Cisco Security Manager*』を参照してください。

IPS サブシステムのバージョンは、バージョンの相違がポストフィックスだけである場合は、マイナーとなります。たとえば、3.0.1 から 3.0.2 へのリビジョンはマイナーと見なされます。別の例として、3.0.1 から 3.1.1 もマイナーなバージョン変更と見なされます。ただし、新機能を含むマイナーリビジョンは、Cisco Security Manager によって自動的にサポートされません。

# ライトウェイト シグニチャによる Cisco IOS IPS シグニチャ スキャン

ライトウェイト シグニチャによる Cisco IOS IPS シグニチャ スキャンを Cisco IOS Release 15.0(1)M に追加することにより、Cisco IOS IPS の機能が拡張されます。この機能拡張により、既存のシグニチャ セットと機能的に同等だがより軽量なシグニチャをロードして、より大規模なシグニ

チャセットをロードできるようになります。このとき、追加メモリを大幅に消費したり、既存のシグニチャセットによって消費されるメモリ量を減らしたりする必要はありません。これらのシグニチャは、ライトウェイト シグニチャと呼ばれています。

Security Manager は、ISR およびモジュラ アクセス ルータ上で、LWE のカスタム シグニチャを検出および調整できます。また、ISR およびモジュラ アクセス ルータ上の LWE シグニチャ向けに、次の機能をサポートしています。

- 新しいシグニチャ タイプ
- シグニチャ カテゴリ
- デフォルトの新しいシグニチャ カテゴリ認識
- 新しいエンジン更新レベル
- ライセンス ステータス：バイパス、期限切れ、または未インストール

# ルータ設定ファイルおよびシグニチャ イベント アクション プロセッサ（SEAP）

Cisco IOS Release 12.4(11)T 以降、Cisco IOS IPS では、Signature Definition File（SDF; シグニチャ定義ファイル）が使用されなくなりました。このため、Security Manager では、廃止予定の組み込みシグニチャ セットである 128.sdf、256.sdf、および attack-drop.sdf を使用できません。

代わりに、ルータは、3つの設定ファイル（デフォルト設定、デルタ設定、およびSEAP設定）が含まれているディレクトリを介して、シグニチャ定義情報にアクセスします。この場所は、[IPS] > [一般設定（General Settings）] ポリシーを使用して設定できます。

SEAP は、シグネチャイベントのデータフローの調整をする制御ユニットです。SEAP を使用すると、Event Risk Rating（ERR; イベント リスク レーティング）フィードバックに基づく高度なフィルタリングおよびシグニチャの上書きを実行できます。ERR は、false positive を最小限に抑えるために、ユーザが選択するアクション適用レベルを制御するために使用します。

シグニチャは、以前はNVRAMに格納されていましたが、現在はデルタ設定ファイルに格納されます。

# Cisco IOS IPS の制限事項および制約事項

Cisco IOS IPS ルータは、専用 IPS センサー アプライアンスおよびサービス モジュールでサポートされているすべての機能をサポートしているわけではありません。また、IOS IPS をサポートするルータが IPS 機能に割り当てるメモリの量は、IPS センサーが割り当てるメモリの量よりも多くはない可能性があります。次の制限事項および制約事項を考慮する必要があります。

- IOS IPS デバイスを設定する場合は、必要なシグニチャだけを選択します。Security Manager で使用可能なシグニチャをすべて選択すると、IOS IPS ルータで使用できるメモリを超過する可能性があります。これにより、配布が失敗したり、デバイスが一部のシグニチャしかロードできなかったり、パフォーマンスが大幅に低下したりする可能性があります。配

布に失敗した場合は、選択するシグニチャセットの数を減らしてから、デバイスに設定を再配布します。

- 初めて IOS-IPS を使用するように設定されている Cisco Security Manager 管理対象ルータでは、シグネチャの更新に自動更新プロセスを使用できません。自動更新プロセスを使用する前に、ルータを更新する必要があります。次の手順に従ってください。

  1. E3 シグネチャ（S317 など）をプッシュします。
  2. S470 などの中間シグネチャをプッシュします。
  3. 最初の E4 シグネチャ（S485 など）をプッシュします。
  4. 目的のレベルに達するまで、後続の E4 シグネチャをプッシュします。各差分のサイズは 10 MB 未満にする必要があります。

ルータを更新したら、自動更新プロセスを使用してシグネチャを更新できます。各増分変更がルータで使用可能なメモリを超えないため、自動更新プロセスは成功します。自動更新の設定については、IPS 更新の自動化を参照してください。

- 仮想センサーは、IOS IPS ではサポートされていません。
- IOS IPS ルータでイベント アクション フィルタを使用する場合は、イベント アクション フィルタの基準に一致したイベントから IPS アクションのサブセットだけを削除できます。使用可能なイベント アクションの詳細については、[Add Filter Item]/[Edit Filter Item] ダイアログボックスおよびIPS イベント アクションについてを参照してください。
- IOS IPS は、IPS ソフトウェア 5.1 に基づいています。したがって、これ以降のバージョンの IPS ソフトウェアで導入された機能は、通常、IOS IPS では使用できません。たとえば、次の機能は設定できません。
  - グローバル相関。
  - 異常検出。
  - イベント アクション ネットワーク識別ポリシーでの OS ID。

# Cisco IOS IPS 設定の概要

さまざまなデバイスに侵入防御システムを設定できます。設定の視点から、デバイスは2つのグループに分けられます。1 つは、完全な IPS ソフトウェアを実行する専用アプライアンスおよびサービス モジュール（ルータ、スイッチ、および ASA デバイスの場合）です。もう 1 つは、Cisco IOS ソフトウェア 12.4(11)T 以降（Cisco IOS IPS）を実行する IPS 対応ルータです。

次の手順では、Cisco IOS IPS ルータでの IPS 設定の概要について説明します。ルータにインストールされている IPS サービス モジュールを含む、専用 IPS デバイスについては、IPS 設定の概要を参照してください。

Cisco IOS IPS は機能が限定されています。ブランチ オフィスや中小規模のネットワーク向けであり、1 つのネットワークで IPS を展開するときに使用します。Cisco IOS IPS ルータでは、通常、専用アプライアンスと同数のシグニチャを使用することはできません。また、Cisco IOS IPS は IPS ソフトウェア バージョン 5.1 に基づいているため、グローバル相関などの高度な機能を設定できません。Cisco IOS IPS デバイスを設定する場合、このデバイスは少数の IPS 機能を実行するルータであるため、通常は標準のルータ ポリシーを設定します。一方、IPS アプライアンスおよびサービスモジュール用のプラットフォーム ポリシーは、IPS ソフトウェア専用となります。

ヒント Cisco IOS IPS を設定する前に、Cisco.com で『*Cisco IOS Intrusion Prevention System Deployment Guide*』を読んでください。

**ステップ 1** デバイスを設置し、ネットワークに接続します。デバイス ソフトウェアをインストールし、基本的なデバイス構成を実行します。デバイス上で実行するすべてのサービスに必要なライセンスをインストールします。最初に実行する設定量は、Security Manager で設定する必要がある内容に影響します。必要な基本設定については、次を参照してください。

- Cisco IOS ルータでの SSL の設定
- SSH の設定
- Cisco IOS デバイスでのライセンスの設定
- Cisco IOS IPS ルータでの最初の準備 （6 ページ）
- Cisco IOS IPS のシグニチャ カテゴリの選択 （7 ページ）

**ステップ 2** デバイスを Security Manager のデバイス インベントリに追加します（デバイス インベントリへのデバイスの追加を参照してください）。デバイスを追加するときは、必ず次の選択を行ってください。

- ネットワークまたはエクスポートファイルから追加する場合は、ポリシー検出に [IPS ポリシー（IPS Policies）] を選択します。
- 設定ファイルから、または手動定義によって追加する場合は、[オプション（Options）] リストから [IPS] を選択します。そうしないと、Security Manager から見て、デバイスが IPS 対応ではなくなります。

**ステップ 3** ルータ上の IPS ファイルの場所を指定するように、IPS の一般的な設定値を設定します。詳細については、Cisco IOS IPS の一般的な設定値の設定 （8 ページ）を参照してください。

**ステップ 4** IPS をイネーブルにし、IPS インスペクションの適用対象トラフィックのインターフェイスを識別するように、IPS インターフェイス ルールを設定します。詳細については、 IOS IPS インターフェイス ルールの設定 （11 ページ）を参照してください。

**ステップ 5** IPS シグニチャおよびイベント アクションを設定します。イベント アクション ポリシーの設定は、カスタムのシグニチャの作成よりも簡単であるため、特定のシグニチャを編集する前に、イベント アクション

フィルタを使用して、シグニチャの動作を変更するように上書きしてみてください。詳細は、次のトピックを参照してください。

- イベント アクション ルールの設定
- シグニチャの設定

**ステップ 6** デバイスを次のように保守します。

- 必要に応じて、設定を更新および再配布します。
- 更新したシグニチャおよびエンジン パッケージを適用します。更新の確認、更新の適用、および定期的な自動更新の設定については、IPS 更新の管理を参照してください。

# Cisco IOS IPS ルータでの最初の準備

Cisco IOS IPS ルータを Security Manager インベントリに追加する前に、いくつかの準備手順を実行する必要があります。ホワイト ペーパー『Getting Started with Cisco IOS IPS with 5.x Format Signatures』では、基本設定の各手順について説明しています。ルータを Security Manager に追加した後で、インターフェイスルールの設定など、いくつかの手順を実行できますが、少なくとも基本的な手順を実行する必要があります。

次の手順では、CLI で実行する必要がある手順について説明しています。Security Manager でこれらの手順を完了することができないか、CLI で（1 回限りの設定として）実行する方が簡単であるため、これらの手順が必要です。このホワイト ペーパーには、CLI で実行できる追加の手順が含まれており、デバイスをインベントリに追加したときに Security Manager によってこれらの設定が検出されます。多くの設定を CLI で実行しておくと、Security Manager で実行する必要がある設定が少なくなります。

**ヒント** Cisco IOS ルータでの SSL の設定、SSH の設定、およびCisco IOS デバイスでのライセンスの設定で説明されている基本的なルータ設定手順も完了する必要があります。次に示すのは、IPS 設定だけに適用される手順です。

**ステップ 1** フラッシュ上にIPSファイルのディレクトリを作成します。たとえば、次のコマンドによってipsという名前のディレクトリが作成されます。

**例**：

```
router# mkdir ips
Create directory filename [ips]?
Created dir flash:ips
```

この時点で、IPS 用のこのディレクトリをルータが使用するように任意で設定できます。または、あとで Security Manager で設定することもできます（[IPS] > [General Settings] ポリシー）。次のコマンドを使用して、CLI でこの設定を行います。

例：

```
router# configure terminal
router(config)# ip ips config location flash:ips
```

**ステップ 2** Cisco IOS IPS 暗号化キーを設定します。暗号化キーは、メインシグニチャファイル（sigdef-default.xml）のデジタル署名を検証するために使用されます。メインシグニチャファイルの内容は、すべてのリリースでの真正性および完全性を保証するために、シスコの秘密キーによって署名されています。

キーに必要な CLI は、http://download-sj.cisco.com/cisco/ciscosecure/ids/sigup/5.0/ios/realm-cisco.pub.key.txt から取得できます（Cisco.com へのログインが必要）。

**ヒント** 暗号化キーの設定は、CLIを使用して行うのが最も簡単な方法です。または、IOS_IPS_PUBLIC_KEY 事前定義 FlexConfig オブジェクトをルータの FlexConfig ポリシーに割り当てて、Security Manager で設定することもできます。FlexConfig の詳細については、FlexConfig の管理を参照してください。

a) テキスト ファイルを開き、その内容をクリップボードにコピーします（すべてのテキストを選択し、Ctrl を押した状態で C を押します）。
b) 必要に応じて、ルータ CLI プロンプトで **configure terminal** を入力します。
c) コピーしたテキスト ファイルをルータ プロンプトに貼り付けます。
d) コンフィギュレーション モードを終了します。
e) **show run** コマンドを入力して、キーが正しく設定されたことを確認します。

**ステップ 3** Syslog は、デフォルトで IPS 通知用に構成されています。SDEE を通知に使用する場合は、次のように SDEE をイネーブルにします。

例：

```
router# configure terminal
router(config)# ip ips notify sdee
```

**ステップ 4** 編集するシグニチャ カテゴリを選択します。詳細については、Cisco IOS IPS のシグニチャ カテゴリの選択 （7 ページ）を参照してください。

# Cisco IOS IPS のシグニチャ カテゴリの選択

IPS 5.x 形式のシグニチャを使用する Cisco IPS アプライアンスおよび Cisco IOS IPS は、シグニチャ カテゴリで機能します。すべての署名はカテゴリに分類されます。カテゴリは階層的です。個々のシグニチャは、複数のカテゴリに属することができます。最上位のカテゴリによって、一般的なシグニチャ タイプを定義できます。各最上位シグニチャ カテゴリの下には、サブカテゴリが存在します（サポートされているトップレベルカテゴリのリストについては、ルータの CLI ヘルプ （?）と **category** コマンドを使用してください。）

ルータにはメモリとリソースの制約があるため、一部の Cisco IOS IPS シグニチャしかロードできません。したがって、カテゴリによって定義された選択された一連の署名のみをロードすることをお勧めします。カテゴリは、「上から下」の順に適用されるため、最初にすべてのシグニチャを廃棄してから、特定のカテゴリの廃棄を「解除」します。シグニチャが廃棄された

場合、ルータは、すべてのシグニチャに関する情報をロードできますが、並行スキャンデータ構造を構築しません。

廃棄されたシグニチャは Cisco IOS IPS によってスキャンされないため、アラームは起動しません。シグニチャがご使用のネットワークに関係ない場合、またはルータのメモリを節約する必要がある場合は、必要に応じてシグニチャを廃棄してください。

Security Manager では、シグニチャ カテゴリ コマンドは管理されません。このコマンドは、ポリシーを使用して直接設定できません。ただし、このコマンドを設定する FlexConfig オブジェクトを含めるように、FlexConfig ポリシーを設定できます。使用できる事前定義されたオブジェクト IOS_IPS_SIGNATURE_CATEGORY があります。基本とは異なるカテゴリを設定する場合は、このオブジェクトをコピーして、編集します。FlexConfig の使用方法については、FlexConfig の管理を参照してください。

ヒント　デバイスによって編集が試行される IPS シグニチャのサブセットの選択に **category** コマンドを使用しない場合は、Security Manager によって、デバイスリソースのオーバーロードを回避するための IOS IPS 基本カテゴリをイネーブルにするようにカテゴリコマンドが設定されます。デバイスでカテゴリを手動で変更して、編集する別のシグニチャ セットを選択できます。カテゴリを設定してから、デバイスを Security Manager に追加することを推奨します。ただし、これは、デバイスを手動定義で追加している場合は実行できません。

次の例は、最初にすべてのシグニチャを廃棄し、次に基本的なカテゴリを設定し、基本的なシグニチャの廃棄を解除する方法を示しています。

```
Router> enable
Router# configure terminal
Router(config)# ip ips signature-category
Router(config-ips-category)# category all
Router(config-ips-category-action)# retired true
Router(config-ips-category-action)# exit
Router(config-ips-category)# category ios_ips basic
Router(config-ips-category-action)# retired false
Router(config-ips-category-action)# exit
```

# Cisco IOS IPS の一般的な設定値の設定

[General Settings] ページを使用して、特定のルータ用に定義された Cisco IOS IPS プロパティに対して使用するグローバル設定を指定します。デフォルト設定は、大半の状況に適していますが、IPS 設定ファイルの場所を指定する必要があります。設定ファイルをルータに格納する場合は、Cisco IOS IPS ルータでの最初の準備 （6 ページ）で説明しているように、最初にディレクトリを作成する必要があります。

### ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [IPS] > [一般設定（General Settings）] を選択します。

- （ポリシービュー）[IPS（ルータ）（IPS (Router)）] > [一般設定（General Settings）] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。

## 関連項目

- Cisco IOS IPS 設定の概要 （4 ページ）
- Cisco IOS IPS について （1 ページ）

## フィールド リファレンス

***表 1 : [General Settings] ページ***

| 要素 | 説明 |
|---|---|
| Block Traffic when IPS engine is unavailable | IPS エンジンが使用できない場合（シグニチャ エンジンが構築中であったり、構築に失敗した場合など）に、検査されていないすべてのトラフィックをブロックするかどうか。<br><br>このオプションをオンにすると、インスペクションに指定されたトラフィックは、IPSが処理できない場合にすべてドロップされます（「フェールクローズモード」とも呼ばれます）。選択しなかった場合、トラフィックはルータ上の他のルールに従って通過を許可されます（デフォルト）。 |
| Apply Deny Action On | [インラインで攻撃者を拒否（Deny Attacker Inline）] イベントまたは [インラインでフローを拒否（Deny Flow Inline）] イベントの場合にトラフィックをドロップするには、ここでACLエントリを適用します。次のいずれかの値を選択します。<br><br>• [入力インターフェイス（Ingress Interface）]（デフォルト）：トラフィックの発信元ネットワークに接続されたインターフェイスで拒否アクションを強制的に実行します。<br><br>• [IPS 有効インターフェイス（IPS enabled interfaces）]：トリガーされた IPS ルールが適用されるインターフェイスで拒否アクションを強制的に実行します。<br><br>このオプションをイネーブルにすると、IOS IPS は、ACL を IPS インターフェイスに直接適用し、攻撃トラフィックを最初に受信したインターフェイスには適用しません。ルータでロードバランシングが実行されていない場合は、この設定をイネーブルにしないでください。ルータでロードバランシングが実行されている場合は、この設定をイネーブルにすることを推奨します。 |
| SDEE Properties | |

| 要素 | 説明 |
|---|---|
| [最大サブスクリプション（Maximum Subscriptions）] | 許可される同時 SDEE サブスクリプションの最大数（1 ～ 3 の範囲）。SDEE サブスクリプションは、SDEE イベントのライブ フィードです。<br>デフォルトは 1 です。 |
| Maximum Alerts | ルータが格納する SDEE アラートの最大数。10 ～ 2000 の範囲で指定します。格納するアラートの数が増えると、より多くのルータメモリが使用されます。<br>デフォルトは 200 です。 |
| Maximum Messages | ルータが格納する SDEE メッセージの最大数。10 ～ 500 の範囲で指定します。格納するメッセージの数が増えると、より多くのルータ メモリが使用されます。<br>デフォルトは 200 です。 |
| [IPS 設定ロケーションのプロパティ（IPS Config Location Properties）] | |
| IPS Config Location | ルータが IOS IPS 固有の設定ファイルを保存する場所。これらの設定ファイルは、IOS IPS 設定が Security Manager で変更または更新されるたびに、自動的に更新されます。ルータが再起動すると、これらの設定ファイルから IOS IPS 設定が取得および復元されます。<br>ルータ上の場所を指定するには、ディレクトリの名前を入力します。すでに存在しているディレクトリである必要があります。Security Manager によってディレクトリは作成されません。flash:ips などです。<br>（注） ルータに LEFS ベースのファイル システムがある場合、ルータのメモリにディレクトリを作成することはできません。この場合、flash: は設定場所として使用されます。<br>リモート システム上の場所を指定する場合は、その場所に到達するために必要なプロトコルおよび URL のパスを指定します。たとえば、設定ファイルを HTTP サーバに保存する場合は、http://172.27.108.5/ips-cfg と入力します。<br>IOS IPS 設定ファイルを保存するためにサポートされるサーバーは、http://、https://、ftp://、rcp://、scp://、および tftp:// です。 |
| Max retries | リモート システムに設定ファイルを保存する場合に、ルータがそのリモート システムへの接続を試行する回数。<br>デフォルトは 1 です。 |
| Timeout seconds between retries | リモート システムに設定ファイルを保存する場合に、設定場所への接続を再試行するまでにルータが待機する時間。<br>デフォルトは 1 です。 |

# IOS IPS インターフェイス ルールの設定

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IOS および IPS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

IPS インターフェイス ルール ポリシーを使用して、IPS インスペクションを Cisco IOS IPS ルータでイネーブルにし、IPS インスペクションが適用されるインターフェイスを指定します。ACL を設定し、インターフェイスに対するトラフィックの方向を指定することにより、インスペクションの対象となるインターフェイス上のトラフィックのサブセットを特定できます。

**関連項目**

- Cisco IOS IPS 設定の概要 （4 ページ）
- Cisco IOS IPS について （1 ページ）

**ステップ 1** 次のいずれかを実行して、変更するインターフェイス ルール ポリシーを開きます。

- （デバイスビュー）ポリシーセレクタから [IPS] > [インターフェイスルール（Interface Rules）] を選択します。
- （ポリシービュー）ポリシーセレクタから [IPS（ルータ）（IPS (Router)）] > [インターフェイスルール（Interface Rules）] を選択します。既存のポリシーを選択するか、または新しいポリシーを作成します。

ポリシーには、ルールの名前、検査されるトラフィックを定義する ACL の名前（ある場合）、検査されるインターフェイスやトラフィック方向など、既存のインターフェイス ルールが示されます。ACL が指定されていない場合、指定された方向のインターフェイス上のすべてのトラフィックが検査されます。

ルールには番号が付けられていますが、ルールの順序は IPS 処理に影響しません。

**ステップ 2** [IPS の有効化（Enable IPS）] を選択して、IOS IPS 設定のデバイスへの展開を有効にします。

[Enable IPS] が選択されていない場合、IPS ルールはすべてのルータ インターフェイスから削除され、IPS はディセーブルになります。また、署名またはイベントアクションポリシーは展開されません。

**ステップ 3** インターフェイス ルールを設定します。このルールにより、IPS によって検査されるインターフェイス（およびインターフェイス上のトラフィックの方向）が特定されます。これらのルールには、検査するトラフィックのサブセットを識別するための ACL を任意で含めることができます。

- ルールを追加するには、[行の追加（Add Row）]（+）ボタンをクリックし、[IP ルールの追加（Add IPS Rule）] ダイアログボックスに入力します。詳細については、[IPS Rule] ダイアログボックス （12 ページ）を参照してください。
- ルールを編集するには、ルールを選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックします。

- ルールを削除するには、ルールを選択し、[行の削除（Delete Row）]（ゴミ箱）ボタンをクリックします。

# [IPS Rule] ダイアログボックス

（注） バージョン 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしますが、バグの修正や拡張はサポートしていません。

[Add IPS Rule] または [Edit IPS Rule] ダイアログボックスを使用して、アクティブ シグニチャ ポリシーを使用して検査するトラフィック フローを特定します。

## ナビゲーション パス

[インターフェイスルールポリシー（Interface Rules policy）] から、[行の追加（Add Row）] ボタンをクリックして新しいルールを追加するか、行を選択して [行の編集（Edit Row）] ボタンをクリックします。[インターフェイスルールポリシー（Interface Rules policy）] を開く詳細については、IOS IPS インターフェイス ルールの設定 （11 ページ）を参照してください。

## フィールド リファレンス

表 *2 : [Add IPS Rule]/[Edit IPS Rule]* ダイアログボックス

| 要素 | 説明 |
|---|---|
| ルール名（Rule Name） | この IPS ルールの一意の名前。<br>IPS ルール名では、大文字と小文字が区別されません。以前に定義された別の文字と同じ文字を含むけれど、大文字と小文字が異なるルール名を使用することはできません。たとえば、MYRULE と MyRule は同じです。 |
| ACL Name | IPS インスペクションの対象となるトラフィックを定義する ACL ポリシーオブジェクトの名前。ACL を指定しなかった場合は、[Interface Pairs] テーブルに示されているインターフェイス/方向のペアに該当するすべてのトラフィックに対してインスペクションが適用されます。<br>ヒント ACL を作成している場合は、許可エントリによって、検査が適用されるトラフィックが特定され、拒否エントリによって、検査が免除されるトラフィックが特定されます。ACL の最後には暗黙的な deny any any ルールがあるため、免除トラフィックを特定する場合は、permit any any ルールを ACL の最後に必ず追加してください。<br>ACL ポリシーオブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストから選択するか、新しいオブジェクトを作成します。 |

| 要素 | 説明 |
|---|---|
| [Interface Pairs] テーブル | IPS インスペクションの対象となるインターフェイスとトラフィック方向のペア。<br>• ペアを追加するには、[行の追加（+）（Add Row (+)）] ボタンをクリックし、[ペアの追加（Adding Pair）] ダイアログボックスに入力します。ペアのダイアログボックス （13 ページ）を参照してください。<br>• ペアを編集するには、URL を選択し、[行の編集（Edit Row）]（鉛筆）ボタンをクリックします。<br>• ペアを削除するには、ペアを選択し、[Delete Row（行の削除）]（ゴミ箱）ボタンをクリックします。 |

# ペアのダイアログボックス

[ペアの追加または編集（Adding or Editing Pair）] ダイアログボックスを使用して、Cisco IOS IPS インターフェイスルールに追加するインターフェイスとトラフィック方向のペアを特定します。インターフェイスルールの設定の詳細については、IOS IPS インターフェイス ルールの設定 （11 ページ）を参照してください。

## ナビゲーション パス

[IPSルールの追加または編集（Add or Edit IPS Rule）] ダイアログボックスで、[行の追加（Add Row）]ボタンをクリックして新しいペアを追加するか、またはペアを選択して [行の編集（Edit Row）] ボタンをクリックします。[IPSルールの追加または編集（Add or Edit IPS Rule）] ダイアログボックスを開く方法については、[IPS Rule] ダイアログボックス （12 ページ）を参照してください。

## フィールド リファレンス

***表 3 : [Adding Pair]/[Editing Pair] ダイアログボックス***

| 要素 | 説明 |
|---|---|
| 方向（Direction） | IPS インスペクションが実行される、インターフェイスにおけるトラフィック方向。次のいずれかを選択します。<br>• [イン（In）]（デフォルト）：IPS ルールは、インバウンドトラフィックに適用されます。<br>• [アウト（Out）]：IPS ルールは、アウトバウンドトラフィックに適用されます。<br>• [両方（Both）]：IPS ルールは、インバウンドとアウトバウンドトラフィックの両方に適用されます。 |

| 要素 | 説明 |
| --- | --- |
| インターフェイス | IPS ルールを適用するインターフェイス。インターフェイスまたはインターフェイスロールオブジェクトの名前を入力します。あるいは、[選択（Select）] をクリックして、リストからインターフェイスまたはインターフェイスロールを選択するか、または新しいインターフェイスロールを作成します。<br><br>インターフェイスロールを使用する場合、ルールは、ロールによって定義されたデバイス上のすべてのインターフェイスに適用されます。ロールに一致するインターフェイスは、既存のルールと競合できません。複数のインターフェイス ルールに同じインターフェイスを指定することはできません。 |

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。