CHAPTER 28

Cisco IOS IPS

Cisco IOS 侵入防止システム（Cisco IOS IPS）では、リリース 12.3(8)T4 以降の Cisco IOS を使用するルータで侵入防止を管理できます。Cisco IOS IPS を使用すると、トラフィックを既知の脅威のシグニチャと比較し、脅威が検出されたときにトラフィックをブロックすることによって、侵入を監視および防止できます。

Cisco CP を使用すると、インターフェイスで Cisco IOS IPS のアプリケーションを制御し、Cisco.com からシグニチャ定義ファイル（SDF）をインポートして編集することができます。また、脅威が検出され場合に Cisco IOS IPS で実行されるアクションを設定できます。

IPS のタブ

IPS のウィンドウ上部にあるタブを使用して、作業領域に移動します。

- ［IPS の作成］— IPS ルール ウィザードに移動して新しい Cisco IOS IPS ルールを作成する場合にクリックします。
- ［IPS の編集］— Cisco IOS IPS ルールを編集して、インターフェイスに適用したり、インターフェイスから削除したりする場合にクリックします。
- ［セキュリティ ダッシュボード］— 高脅威テーブルを表示し、その脅威に関連付けられているシグニチャを展開する場合にクリックします。
- ［IPS 移行］— ルータでリリース 12.4(11)T 以降の Cisco IOS イメージが実行されている場合は、それより前のバージョンの Cisco IOS を使用して作成された Cisco IOS IPS 設定を移行できます。

IPS ルール

Cisco IOS IPS ルールでは、インターフェイス、Cisco IOS IPS で検査されるトラフィックのタイプと方向、およびルータで使用されるシグニチャ定義ファイル（SDF）の保存場所を指定します。

IPS の作成

このウィンドウでは、IPS ルール ウィザードを起動できます。

IPS ルール ウィザードでは、次の情報の入力を要求されます。

- ルールを適用するインターフェイス
- Cisco IOS IPS を適用するトラフィック（インバウンド、アウトバウンド、またはその両方）
- シグニチャ定義ファイル（SDF）の保存場所

Cisco IOS 12.4(11) 以降のイメージでは、次の情報の入力も要求されます。

- IOS IPS の設定に対する変更内容が含まれるファイルの保存場所。このタイプの情報が格納されるファイルは、デルタ ファイルと呼ばれます。
- デルタ ファイル内の情報へのアクセスに使用するパブリック キー。
- シグニチャのカテゴリ。128MB 未満のフラッシュ メモリを持つルータには、basic シグニチャ カテゴリが適切です。128MB 以上のフラッシュ メモリを持つルータには、advanced シグニチャ カテゴリが適切です。

ユース ケース シナリオとして、Cisco IOS IPS ルールが使用されている設定が示されます。Cisco IOS IPS ルールを作成し、設定をルータに配信した後、［IPS の編集］タブをクリックしてルールを変更できます。

Cisco IOS IPS の詳細については、次のリンクのドキュメントを参照してください。

http://www.cisco.com/en/US/products/ps6634/prod_white_papers_list.html

開始するには［IPS ルール ウィザードを起動］ボタンをクリックします。

IPS の作成：ようこそ

このウィンドウには、IPS ルール ウィザードを完了したときに実行するタスクの要約が表示されます。

Cisco IOS IPS ルールの設定を開始するには、［次へ］をクリックします。

IPS の作成：インターフェイスの選択

Cisco IOS IPS ルールをインバウンドとアウトバウンドどちらのトラフィックに適用するかを指定して、そのルールを適用するインターフェイスを選択します。インバウンドとアウトバウンド両方のボックスをチェックした場合、このルールは両方向のトラフィックに適用されます。

次に例を示します。次の設定で Cisco IOS IPS が適用されるのは、BRI 0 インターフェイスのインバウンド トラフィックと、FastEthernet 0 インターフェイスのインバウンドとアウトバウンド両方のトラフィックです。

インターフェイス名	インバウンド	アウトバウンド
BRI 0	チェック	—
FastEthernet 0	チェック	チェック

IPS の作成：SDF の場所

Cisco IOS IPS では、トラフィックをシグニチャ定義ファイル（SDF）で定義されたシグニチャと比較して検査します。SDF は、ルータのフラッシュ メモリ、またはルータからアクセスできるリモート システムにあります。SDF の場所は複数指定できます。これによって、ルータが最初の場所にアクセスできない場合は、SDF を取得するまで他の場所へのアクセスを試行できます。

ルータが SDF を取得するためにアクセスを試行する SDF の場所のリストを追加、削除、および整理するには、［追加］、［削除］、［上へ移動］、および［下へ移動］ボタンを使用します。ルータはまずリストの 1 つめのエントリにアクセスし、その後は SDF を取得するまで、リスト内のエントリに順次アクセスします。

Cisco IOS IPS をサポートする Cisco IOS イメージには、ビルトイン シグニチャが含まれています。ウィンドウ下部のボックスをチェックした場合、ルータがビルトイン シグニチャを使用するのは、リスト内の他の場所で SDF ファイルを取得できない場合に限られます。

IPS の作成：シグニチャ ファイル

Cisco IOS IPS シグニチャ ファイルには、Cisco.com 上のファイルに対する各アップデートに存在するデフォルトのシグニチャ情報が含まれます。この設定に対する変更はすべて、デルタ ファイルに保存されます。セキュリティ上の理由から、デルタ ファイルにはデジタル署名が必要です。このウィンドウでは、シグニチャ ファイルの場所を指定し、デルタ ファイルの署名に使用するパブリック キーの名前とテキストを入力します。

このヘルプ トピックでは、ルータで Cisco IOS 12.4(11)T 以降が実行されている場合に表示される［シグニチャ ファイル］ウィンドウについて説明します。

IOS IPS で使用するシグニチャ ファイルを指定します

シグニチャ ファイルがすでに PC、ルータのフラッシュ メモリ、またはリモート システム上に存在する場合は、［IOS IPS で使用するシグニチャ ファイルを指定します］をクリックすると、シグニチャ ファイルの場所を指定できるダイアログが表示されます。

Cisco.com から最新のシグニチャを入手して、PC に保存してください

シグニチャ ファイルが PC またはルータのフラッシュ メモリに存在しない場合は、［Cisco.com から最新のシグニチャを入手して、PC に保存してください］をクリックします。［参照］をクリックしてシグニチャ ファイルの保存先を指定し、［ダウンロード］をクリックしてファイルのダウンロードを開始します。Cisco CP によって、シグニチャ ファイルが指定した場所にダウンロードされます。

パブリック キーの設定

シグニチャの設定に対する変更はすべてデルタ ファイルに保存されます。このファイルは、パブリック キーでデジタル署名されている必要があります。Cisco.com からキーを入手して、情報を［名前］フィールドと［キー］フィールドに貼り付けます。

（注）　Cisco IOS CLI を使用してパブリック キーをすでに設定に追加している場合も、この画面でパブリック キーを入力する必要があります。Cisco IOS IPS ルール ウィザードを完了したら、［IPS の編集］>［グローバル設定］に移動できます。［グローバル設定］画面で、［IPS 必須項目の編集］エリアの［編集］をクリックし、次に［パブリック キー］をクリックして［パブリック キー］ダイアログを表示します。このダイアログで、必要のないパブリック キーを削除できます。

［名前］フィールドと［キー］フィールドにパブリック キーの情報を入力する手順は、次のとおりです。

ステップ 1　次のリンクに移動して、パブリック キーを取得します。

http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup

ステップ 2　PC にキーをダウンロードします。

ステップ 3　「named-key」の次のテキストを［名前］フィールドにコピーします。たとえば、次のような名前を含むテキストの行の場合、

```
named-key realm-cisco.pub signature
```

［名前］フィールドに `realm-cisco.pub signature` をコピーします。

ステップ 4　**key-string** と **quit** の間のテキストを、［キー］フィールドにコピーします。コピーするテキストは、次のようなものです。

```
30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
F3020301 0001
```

IPS の作成：コンフィギュレーションの場所とカテゴリ

Cisco IOS IPS で使用するシグニチャ情報の保存場所を指定します。この情報は、シグニチャ ファイルと、シグニチャ情報に変更が加えられたときに作成されるデルタ ファイルで構成されます。

このヘルプ トピックでは、ルータで Cisco IOS 12.4(11)T 以降が実行されている場合に表示される［コンフィギュレーションの場所］ウィンドウについて説明します。

コンフィグレーションの場所

［コンフィギュレーションの場所］フィールドの右にあるボタンをクリックして表示されるダイアログで、場所を指定できます。ダイアログに情報を入力すると、このフィールドにコンフィギュレーションの場所へのパスが表示されます。

カテゴリの選択

ルータのメモリおよびリソースの制約により、すべての使用可能なシグニチャの使用が制限される場合があるため、シグニチャには **basic** と **advanced** の 2 つのカテゴリがあります。［カテゴリの選択］フィールドで、Cisco IOS IPS がルータで効率的に動作できるようにするカテゴリを選択します。使用可能なフラッシュ メモリが 128MB 未満のルータでは、basic カテゴリが適切です。128MB 以上のフラッシュ メモリが使用可能なルータでは、advanced カテゴリが適切です。

コンフィギュレーションの場所の追加または編集

Cisco IOS IPS で使用するシグニチャ情報とデルタ ファイルの保存場所を指定します。

このルータにコンフィギュレーションの場所を指定します

ルータに場所を指定するには、［ディレクトリ名］フィールドの右のボタンをクリックし、設定情報を保存するディレクトリを選択します。

（注）　ルータに LEFS ベースのファイル システムがある場合は、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。この場合は、flash: がコンフィギュレーションの場所として使用されます。

URL を使用してコンフィギュレーションの場所を指定します

リモート システム上の場所を指定するには、その場所へのアクセスに必要な URL のプロトコルとパスを指定します。たとえば、URL http://172.27.108.5/ips-cfg を指定する場合は、「172.27.108.5/ips-cfg」と入力します。

（注）　入力するパスにプロトコルを含めないでください。Cisco CP では、プロトコルは自動的に追加されます。プロトコルを入力すると、エラー メッセージが表示されます。

［再試行の回数］と［タイムアウト］のフィールドに、ルータがリモート システムにアクセスを試みる回数と、アクセスの試行を停止する前にルータが応答を待機する時間を指定します。

ディレクトリの選択

設定情報を保存するフォルダをクリックします。新しいフォルダを作成する場合は、［新規フォルダ］をクリックし、表示されるダイアログにフォルダの名前を入力し、そのフォルダを選択して、［OK］をクリックします。

シグニチャ ファイル

Cisco IOS IPS で使用するシグニチャ ファイルの場所を指定します。

フラッシュにシグニチャ ファイルを指定

シグニチャ ファイルがルータのフラッシュ メモリ上に保存されている場合は、フィールドの右のボタンをクリックします。適切な形式のシグニチャ ファイル名が表示され、それらの名前を選択できるようになります。

URL を使用してシグニチャ ファイルを指定

シグニチャ ファイルがリモート システム上に保存されている場合は、使用するプロトコルを選択し、そのファイルへのパスを入力します。たとえば、シグニチャ ファイル IOS-S259-CLI.pkg が 10.10.10.5 にあり、FTP プロトコルが使用される場合、プロトコルとして［ftp］を選択し、次のように入力します。

```
10.10.10.5/IOS-S259-CLI.pkg
```

（注） 入力するパスにプロトコルを含めないでください。Cisco CP では、プロトコルは自動的に追加されます。プロトコルを入力すると、エラー メッセージが表示されます。また、URL を使用するときは、上記の例で使用したファイルのように、IOS-Snnn-CLI.pkg のファイル命名規則に準拠するファイル名を指定する必要があります。

PC にシグニチャ ファイルを指定

シグニチャ ファイルが PC 上に保存されている場合は、［参照］をクリックし、ファイルが存在するフォルダに移動して、ファイル名を選択します。sigv5-SDM-S*xxx*.zip という形式の、Cisco CP に固有のパッケージを選択する必要があります（たとえば、sigv5-SDM-S260.zip）。

IPS の作成：要約

次に、121.4(11)T より前の Cisco IOS が実行されているルータ上の、Cisco IOS IPS の要約の表示例を示します。

```
Selected Interface: FastEthernet 0/1

IPS Scanning Direction: Both

Signature Definition File Location: flash//sdmips.sdf

Built-in enabled: yes
```

この例では、Cisco IOS IPS が FastEthernet 0/1 インターフェイスに対して有効で、インバウンドとアウトバウンド両方のトラフィックがスキャンされます。SDF は sdmips.sdf という名前で、ルータのフラッシュ メモリにあります。ルータは、ルータで使用される Cisco IOS イメージに組み込まれたシグニチャ定義を使用するように設定されています。

IPS の作成：要約

［要約］ウィンドウには入力した情報が表示されるので、ルータに変更後の設定を配信する前に内容を確認できます。

このヘルプ トピックでは、ルータで Cisco IOS 12.4(11)T 以降が実行されている場合に表示される［要約］ウィンドウについて説明します。次に、［要約］ウィンドウの表示例を示します。

```
IPS rule will be applied to the outgoing traffic on the following interfaces.
     FastEthernet0/1
IPS rule will be applied to the incoming traffic on the following interfaces.
     FastEthernet0/0
Signature File location:
     C:\SDM-Test-folder\sigv5-SDM-S260.zip
Public Key:
       30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00B8BE84
  33251FA8 F79E393B B2341A13 CAFFC5E6 D5B3645E 7618398A EFB0AC74 11705BEA
  93A96425 CF579F1C EA6A5F29 310F7A09 46737447 27D13206 F47658C7 885E9732
  CAD15023 619FCE8A D3A2BCD1 0ADA4D88 3CBD93DB 265E317E 73BE085E AD5B1A95
  59D8438D 5377CB6A AC5D5EDC 04993A74 53C3A058 8F2A8642 F7803424 9B020301 0001

Config Location
     flash:/configloc/
Selected category of signatures:
     advanced
```

この例では、Cisco IOS IPS ポリシーは FastEthernet 0/0 インターフェイスと FastEthernet 0/1 インターフェイスに適用されます。シグニチャ ファイルは PC 上にあります。コンフィギュレーションの場所は、ルータのフラッシュ メモリ上の configloc というディレクトリです。

IPS の編集

このウィンドウには、Cisco IOS IPS のポリシー、セキュリティ メッセージ、シグニチャなどの設定および管理に使用する Cisco IOS IPS のボタンが表示されます。

IPS ポリシー ボタン

［IPS の編集］ウィンドウを表示する場合にクリックします。このウィンドウでは、インターフェイス上での Cisco IOS IPS の有効 / 無効を切り替えたり、Cisco IOS IPS の適用方法に関する情報を表示したりできます。インターフェイスで Cisco IOS IPS を有効にする場合は、必要に応じて、侵入について検査するトラフィックを指定できます。

グローバル設定ボタン

［IPS の編集 : グローバル設定］ウィンドウを表示する場合にクリックします。ここでは Cisco IOS IPS の全体的な操作に適用される設定を行うことができます。

自動アップデート

このボタンは、ルータ上の Cisco IOS イメージがバージョン 12.4(11)T 以降である場合に表示されます。自動アップデートを使用すると、Cisco セキュリティ センターからシグニチャの最新のアップデート ファイルを自動的に取得するようルータを設定できます。詳細については、「IPS の編集 : 自動アップデート」を参照してください。

SEAP 設定

このボタンは、ルータ上の Cisco IOS イメージがバージョン 12.4(11)T 以降である場合に表示されます。Signature Event Action Processing（SEAP）を使用すると、高度なフィルタリングとオーバーライドにより、IOS IPS をより詳細に制御できます。

SDEE メッセージ ボタン

Secure Device Event Exchange（SDEE）メッセージでは、Cisco IOS IPS の初期化および操作の経過が通知されます。［IPS の編集：SDEE メッセージ］ウィンドウを表示する場合にクリックします。このウィンドウでは、SDEE メッセージを確認できるほか、それらのメッセージをフィルタ処理して、エラー メッセージだけ、ステータス メッセージだけ、またはアラート メッセージだけを表示できます。

シグニチャ ボタン

［IPS の編集：シグニチャ］ウィンドウを表示する場合にクリックします。このウィンドウではルータ上のシグニチャを管理できます。

NM CIDS ボタン

このボタンは、シスコの侵入検知システムのネットワーク モジュールがルータにインストールされている場合に表示されます。IDS モジュールを管理する場合にクリックします。

IPS の編集：IPS ポリシー

このウィンドウには、すべてのルータ インターフェイスについて Cisco IOS IPS のステータスが表示され、インターフェイス上での Cisco IOS IPS の有効 / 無効を切り替えることができます。

インターフェイス

このリストを使用して、［インターフェイス リスト］エリアに表示されているインターフェイスにフィルタを適用できます。次のいずれかを選択します。

- ［すべてのインターフェイス］— ルータのすべてのインターフェイス
- ［IPS インターフェイス］— Cisco IOS IPS が有効になっているインターフェイス

有効ボタン

指定したインターフェイスで Cisco IOS IPS を有効にする場合にクリックします。Cisco IOS IPS が適用されるトラフィックの方向、および検査するトラフィックのタイプの定義に使用される ACL を指定できます。詳細については、「インターフェイスに対して IPS を有効にする、またはインターフェイスの IPS を編集する」を参照してください。

編集ボタン

指定したインターフェイスに適用する Cisco IOS IPS の特性を編集する場合にクリックします。

無効ボタン

指定したインターフェイスで Cisco IOS IPS を無効にする場合にクリックします。コンテキスト メニューに、Cisco IOS IPS が適用されているトラフィックの方向が表示され、Cisco IOS IPS を無効にする方向を選択できます。Cisco IOS IPS が適用されているインターフェイスで Cisco IOS IPS を無効にした場合は、Cisco CP により、そのインターフェイスから Cisco IOS IPS ルールが切り離されます。

すべて無効ボタン

Cisco IOS IPS が有効になっているすべてのインターフェイスで Cisco IOS IPS を無効にする場合にクリックします。Cisco IOS IPS が適用されているインターフェイスで Cisco IOS IPS を無効にした場合は、Cisco CP により、そのインターフェイスから Cisco IOS IPS ルールが切り離されます。

インターフェイス名

インターフェイスの名前です。たとえば、Serial0/0、FE0/1 などです。

IP

このカラムには、次のいずれかのタイプの IP アドレスが表示されます。

- インターフェイスに設定された IP アドレス。

- ［DHCP クライアント］— インターフェイスは、Dynamic Host Configuration Protocol（DHCP）サーバから IP アドレスを受け取ります。
- ［ネゴシエート済み］— インターフェイスはリモート デバイスとのネゴシエーションによって IP アドレスを受け取ります。
- ［アンナンバード］— ルータは、ルータおよび LAN 上のホストに対し、サービス プロバイダから提供された IP アドレス プールの中の 1 つを使用します。
- ［該当なし］— このインターフェイス タイプには IP アドレスを割り当てられません。

インバウンド IPS/ アウトバウンド IPS

- ［有効］— Cisco IOS IPS はこの方向のトラフィックで有効です。
- ［無効］— Cisco IOS IPS はこの方向のトラフィックで無効です。

VFR ステータス

Virtual Fragment Reassembly（VFR）のステータス。値は次のいずれかになります。

- オン — VFR が有効になっています。
- オフ — VFR が無効になっています。

Cisco IOS IPS では、IP フラグメントの内容を識別できません。また、シグニチャと照合するポート情報をフラグメントから収集することもできません。このため、フラグメントは、検査もダイナミック アクセス コントロール リスト（ACL）の作成も行われずにネットワークをそのまま通過します。

VFR によって、Cisco IOS Firewall で適切なダイナミック ACL が作成され、さまざまなフラグメンテーション攻撃からネットワークが保護されるようになります。

説明

追加した場合、接続の説明。

IPS フィルタの詳細

トラフィックにフィルタが適用されていない場合、このエリアには何も表示されません。フィルタが適用されている場合は、かっこ内に ACL の名前または番号が表示されます。

［インバウンド フィルタ］ボタンと［アウトバウンド フィルタ］ボタン

クリックすると、インバウンドまたはアウトバウンド方向のトラフィックに適用されるフィルタのエントリが表示されます。

フィールドの説明

［アクション］— トラフィックが許可されるか、それとも拒否されるか。

送信元トラフィックを許可する。

送信元トラフィックを拒否する。

［送信元］— ネットワークまたはホストのアドレス、あるいは任意のホストまたはネットワーク。

［宛先］— ネットワークまたはホストのアドレス、あるいは任意のホストまたはネットワーク。

［サービス］— フィルタが適用されるサービスのタイプ（IP、TCP、UDP、IGMP、および ICMP）。

［ログ］— 拒否したトラフィックがログに記録されるかどうか。

［属性］— CLI を使用して設定されたオプション。

［説明］— 入力された説明。

インターフェイスに対して IPS を有効にする、またはインターフェイスの IPS を編集する

このウィンドウでは、侵入検知を有効にするインターフェイスを選択し、トラフィックの検査に使用する IPS フィルタを指定します。

両方、インバウンド、アウトバウンドの各ボタン

このボタンを使用すると、Cisco IOS IPS を有効にするのを、インバウンドとアウトバウンドの両方のトラフィックにするか、インバウンド トラフィックだけにするか、またはアウトバウンド トラフィックだけにするかを指定できます。

インバウンド フィルタ

（オプション）検査するインバウンド トラフィックを指定するアクセス ルールの名前または番号を入力します。指定した ACL に関連付けられているインターフェイスが選択されると、［インバウンド フィルタ］ボタンの隣の［IPS フィルタの詳細］エリアにその ACL が表示されます。アクセス ルールを参照するか、新しいルールを作成する必要がある場合は、［...］ボタンをクリックします。

アウトバウンド フィルタ

（オプション）検査するアウトバウンド トラフィックを指定するアクセス ルールの名前または番号を入力します。指定した ACL に関連付けられているインターフェイスが選択されると、［アウトバウンド フィルタ］ボタンの隣の［IPS フィルタの詳細］エリアにその ACL が表示されます。アクセス ルールを参照するか、新しいルールを作成する必要がある場合は、［...］ボタンをクリックします。

... ボタン

このボタンを使用してフィルタを指定します。次のオプションを含むメニューを表示する場合にクリックします。

- ［既存のルールを選択する］。詳細については、「ルールの選択」を参照してください。
- ［新しいルールを作成して選択する］。詳細については、「ルールの追加 / 編集」を参照してください。
- ［なし（ルールの関連付けを解除）］。このオプションを使用すると、フィルタが適用されているトラフィック方向からフィルタを削除できます。

このインターフェイスに対してフラグメント チェックを行う

（デフォルトでは有効です。）Cisco IOS ファイアウォールでこのインターフェイスの IP フラグメントをチェックする場合に選択します。詳細については、「VFR ステータス」を参照してください。

他のインターフェイスに対してフラグメント チェックを行う

アウトバウンド トラフィックに対するフラグメント チェックが有効な場合は、設定されているインターフェイスにアウトバウンド トラフィックを送信するインターフェイスへのインバウンド トラフィックがルータで検査される必要があります。これらのインターフェイスを、この下で指定します。

［インバウンド］ラジオ ボタンが選択されている場合、このエリアは表示されません。

シグニチャファイルの指定

［シグニチャ ファイルの指定］ボックスでは、ルータで使用されている SDF のバージョンについての情報が示され、SDF を最新バージョンに更新できます。新しい SDF を指定するには、［シグニチャ ファイル］フィールドの横にある［...］ボタンをクリックして、表示されたダイアログで新しいファイルを指定します。

IPS の編集：グローバル設定

このウィンドウでは、Cisco IPS のグローバル設定を表示および設定できます。このヘルプ トピックでは、実行されている Cisco IOS イメージが 12.4(11)T より前のバージョンである場合に表示される可能性のある情報について説明します。

グローバル設定テーブル

［グローバル設定］ウィンドウのこのテーブルには、現在のグローバル設定およびその値が表示されます。これらの値のいずれかを変更するには、［編集］をクリックします。

項目名	項目値
シスログ（Syslog）	有効の場合、通知は［システム プロパティ］で指定されたシスログ（Syslog）サーバに送信される。
SDEE	Security Device Event Exchange。有効の場合、SDEE イベントが生成される。
SDEE アラート SDEE メッセージ	ルータのバッファに格納する SDEE イベントの数。
SDEE サブスクリプション	同時 SDEE サブスクリプション数。
エンジン オプション	エンジン オプションは次のとおり。 • ［エンジン　フェイル　クローズの有効化］— デフォルトでは、Cisco IOS により特定のエンジンの新しいシグニチャがコンパイルされている間、そのエンジンに対するパケットは、スキャンなしでそのまま通過する。このオプションを有効にすると、コンパイル中は Cisco IOS でパケットが破棄される。 • ［ビルトイン　　シグニチャをバックアップとして使用する］— Cisco IOS IPS で指定の場所からシグニチャを検出またはロードできなかった場合に、Cisco IOS のビルトイン シグニチャを使用して Cisco IOS IPS を有効にできる。このオプションはデフォルトで有効になっている。 • ［IPS インターフェイス上の拒否アクションの有効化］— ルータで負荷分散を実行している場合は、有効にすることが推奨される。このオプションを有効にすると、攻撃的なトラフィックの送信元のインターフェイスで ACL を有効にする代わりに、Cisco IOS IPS インターフェイスで ACL を有効にできる。
イベントの回避	このオプションでは Shun Time パラメータを使用する。Shun Time とは、回避アクションを有効にしておく時間のことである。回避アクションが発生するのは、ACL にホストまたはネットワークが追加され、そのホストまたはネットワークからのトラフィックが拒否されている場合。

設定されている SDF の場所

シグニチャの場所は、SDF へのパスを示す URL で指定されます。SDF を探す際、ルータはまずリストの 1 つめの場所にアクセスします。アクセスに失敗した場合は、SDF が見つかるまで、リスト内のその次の場所に順番にアクセスします。

追加ボタン

リストに URL を追加する場合にクリックします。

編集ボタン

指定した場所を編集する場合にクリックします。

削除ボタン

指定した場所を削除する場合にクリックします。

［上へ移動］ボタンと［下へ移動］ボタン

リスト内の URL の優先順位を変更する場合に使用します。

シグニチャのリロード

すべてのシグニチャ エンジンのシグニチャを再コンパイルする場合にクリックします。シグニチャ エンジンのシグニチャが再コンパイルされている間、Cisco IOS ソフトウェアでは、エンジンのシグニチャを使用してパケットをスキャンできません。

グローバル設定の編集

このウィンドウの［Syslog と SDEE］タブ、および［グローバル エンジン］タブで、Cisco IOS IPS の全体的な操作に適用される設定を編集します。

シスログ（Syslog）通知の有効化（[Syslog と SDEE] タブ）

アラーム、イベント、およびエラーのメッセージがルータからシスログ（Syslog）サーバに送信されるようにするときに、このチェック ボックスを選択します。この通知方法を使用するには、シスログ（Syslog）サーバを［システム プロパティ］で指定しておく必要があります。

SDEE（[Syslog と SDEE] タブ）

［同時 SDEE サブスクリプション数］フィールドに、1 ～ 3 の範囲で同時 SDEE サブスクリプションの数を入力します。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。

［SDEE アラートの最大保存数］フィールドには、ルータに保存される SDEE アラートの最大数を 10 ～ 2000 の範囲で入力します。保存するアラートの数を増やすとルータのメモリの使用量が増えます。

［SDEE メッセージの最大保存数］フィールドには、ルータに保存される SDEE メッセージの最大数を 10 ～ 500 の範囲で入力します。保存するメッセージの数を増やすとルータのメモリの使用量が増えます。

エンジンフェールクローズの有効化（[グローバル エンジン] タブ）

デフォルトでは、Cisco IOS ソフトウェアにより特定のエンジンの新しいシグニチャがコンパイルされている間、そのエンジンに対するパケットは、スキャンなしでそのまま通過します。コンパイル中、Cisco IOS ソフトウェアでパケットが破棄されるようにするには、このオプションを有効にします。

ビルトイン シグニチャをバックアップとして使用する（[グローバル エンジン] タブ）

Cisco IOS IPS で指定の場所からシグニチャを検出またはロードできなかった場合は、Cisco IOS のビルトイン シグニチャを使用して Cisco IOS IPS を有効にできます。このオプションはデフォルトで有効になっています。

IPS インターフェイス上の拒否アクションを有効にする（[グローバル エンジン] タブ）

このオプションは、シグニチャ アクションが［denyAttackerInline］または［denyFlowInline］に設定されている場合に適用できます。Cisco IOS IPS のデフォルトでは、ACL は Cisco IOS IPS インターフェイスではなく、攻撃的なトラフィックの送信元のインターフェイスに適用されます。このオプションを有効にすると、Cisco IOS IPS により、最初に攻撃的なトラフィックを受信したインターフェイスではなく、Cisco IOS IPS インターフェイスに直接 ACL が適用されます。ルータで負荷分散を実行していない場合は、この設定を有効にしないでください。ルータで負荷分散を実行している場合は、この設定を有効にすることをお勧めします。

タイムアウト（[グローバル エンジン] タブ）

このオプションを使用すると、回避アクションを有効にしておく時間（分）を 0 ～ 65535 の範囲で設定できます。デフォルト値は 30 分です。回避アクションが発生するのは、ACL にホストまたはネットワークが追加され、そのホストまたはネットワークからのトラフィックが拒否されている場合です。

シグニチャの場所の追加または編集

Cisco IOS IPS による SDF のロード元を指定します。SDF の場所を複数指定するには、もう一度このダイアログを開いて、別の SDF の情報を入力します。

このルータで SDF を指定する

［場所］ドロップダウン メニューを使用して、ルータのメモリの中で SDF を格納する部分を指定します。たとえば、このメニューには、*disk0*、*usbflash1*、*flash* のような項目があります。そこで、［ファイル名］フィールドの横にある下矢印をクリックするか、［ファイル名］フィールドにファイル名を入力して、ファイル名を選択します。

SDF を指定する URL

SDF がリモート システムにある場合は、そのシステムの場所を示す URL を指定できます。

プロトコル

http や *https* など、SDF を取得するためにルータで使用するプロトコルを選択します。

URL

URL を次の形式で入力します。

path-to-signature-file

（注） ［プロトコル］メニューで選択したプロトコルが、［URL］フィールドの右側に表示されます。［URL］フィールドには、プロトコルを再入力*しないでください*。

URL 形式の例は、次に示すとおりです。これは、シグニチャ ファイルへの有効な URL では*ありません*。また、フル URL を示すプロトコルが含まれています。

```
https://172.16.122.204/mysigs/vsensor.sdf
```

自動保存

このオプションは、クラッシュ時にルータで SDF が自動的に保存されるように設定する場合に選択します。このオプションを選択すると、ルータが復旧したときに、この SDF を有する Cisco IOS IPS を再設定する必要がなくなります。

IPS の編集：SDEE メッセージ

このウィンドウには、ルータが受信した SDEE メッセージのリストが表示されます。SDEE メッセージは、Cisco IOS IPS の設定に変更があったときに生成されます。

SDEE メッセージ

表示する SDEE メッセージ タイプを選択します。

- ［すべて］— エラー、ステータス、アラートの各 SDEE メッセージが表示されます。
- ［エラー］— SDEE エラー メッセージだけが表示されます。
- ［ステータス］— SDEE ステータス メッセージだけが表示されます。
- ［アラート］— SDEE アラート メッセージだけが表示されます。

選択肢

検索対象の SDEE メッセージ フィールドを選択します。

条件

検索文字列を入力します。

実行ボタン

［条件］フィールドに入力した文字列の検索を開始する場合にクリックします。

タイプ

［エラー］、［ステータス］、および［アラート］のいずれかのタイプを選択できます。表示される SDEE メッセージについては、「SDEE メッセージ テキスト」を参照してください。

時刻

メッセージを受信した時刻です。

説明

該当する説明です。

更新ボタン

新しい SDEE メッセージがあるかどうかチェックする場合にクリックします。

閉じるボタン

［SDEE メッセージ］ウィンドウを閉じる場合にクリックします。

SDEE メッセージ テキスト

ここでは、表示される可能性があるすべての SDEE メッセージを示します。

IDS ステータス メッセージ

エラー メッセージ

`ENGINE_BUILDING: %s - %d シグニチャ - %d/%d エンジン`

説明　Cisco IOS IPS で signature microengine（SME）の構築が開始されたときに生成されます。

エラー メッセージ

`ENGINE_BUILD_SKIPPED: %s -` このエンジンには新しいシグニチャ定義がありません。

説明　侵入検知システム SME で、シグニチャが定義されていないか、既存のシグニチャ定義が変更されていないときに生成されます。

エラー メッセージ

`ENGINE_READY: %s - %d` ミリ秒 - このエンジンのパケットがスキャンされます。

説明　IDS SME が構築され、パケットをスキャンする準備ができたときに生成されます。

エラー メッセージ

SDF_LOAD_SUCCESS: SDF は %s から正常にロードされました。

説明　指定した場所から SDF ファイルが正常にロードされたときに生成されます。

エラー メッセージ

BUILTIN_SIGS: ビルトイン シグニチャをロードするための %s

説明　ルータで最後の手段としてビルトイン シグニチャがロードされるときに生成されます。

IDS エラー メッセージ

エラー メッセージ

ENGINE_BUILD_FAILED: %s - %d ミリ秒 - エンジンの構築に失敗しました - %s

説明　SDF ファイルがロードされた後、Cisco IOS IPS でいずれかのエンジンの構築に失敗したときに生成されます。構築できなかったエンジンのそれぞれについて、メッセージが 1 つずつ送信されます。これは、Cisco IOS IPS エンジンで、メッセージ内に示されたエンジン用のシグニチャのインポートに失敗したことを意味します。この問題の原因として一番可能性が大きいのはメモリの不足です。この問題が発生した場合、新しくインポートされたシグニチャのうち、このエンジンに属するシグニチャが Cisco IOS IPS によって破棄されます。

エラー メッセージ

SDF_PARSE_FAILED: 行 %d カラム %d バイト %d 長さ %d の %s

説明　SDF ファイルが正しく解析されなかったときに生成されます。

エラー メッセージ

`SDF_LOAD_FAILED: %s SDF を %s からロードできませんでした`

説明　何らかの理由で SDF ファイルのロードに失敗したときに生成されます。

エラー メッセージ

`DISABLED: %s - IDS は無効です`

説明　IDS が無効になっています。メッセージには原因が示されます。

エラー メッセージ

`SYSERROR: 予期しないエラー (%s) が行 %d 関数 %s() ファイル %s で発生しました`

説明　予期しない内部システム エラーが発生したときに生成されます。

IPS の編集：グローバル設定

Cisco IOS 12.4(11)T 以降のイメージでは、いくつかの Cisco IOS IPS 設定オプションが使用可能です。このヘルプ トピックではそれらのオプションについて説明します。［Syslog と SDEE］グローバル設定などの、Cisco IOS 12.4(11)T より前のバージョンで使用可能な画面制御と設定のオプションについては「IPS の編集：グローバル設定」で説明しています。

このヘルプ トピックでは、ルータで Cisco IOS 12.4(11)T 以降が実行されている場合に表示される［グローバル設定］ウィンドウについて説明します。

エンジン オプション

Cisco IOS 12.4(11)T 以降のイメージで使用可能なエンジン オプションは、次のとおりです。

- ［エンジン フェイル クローズの有効化］— デフォルトでは、Cisco IOS により特定のエンジンの新しいシグニチャがコンパイルされている間、そのエンジンに対するパケットは、スキャンなしでそのまま通過します。このオプションを有効にすると、コンパイル中は Cisco IOS でパケットが破棄されます。

- ［IPS インターフェイス上の拒否アクションの有効化］— ルータで負荷分散を実行している場合は、有効にすることが推奨されます。このオプションを有効にすると、攻撃的なトラフィックの送信元のインターフェイスで ACL を有効にする代わりに、Cisco IOS IPS インターフェイスで ACL を有効にできます。

IPS 必須項目の編集テーブル

このテーブルには、ルータが Cisco IOS IPS に対してプロビジョニングされる方法に関する情報が表示されます。これらの値のいずれかを変更するには、［編集］をクリックします。次の表のサンプル データは、コンフィギュレーションの場所がフラッシュ メモリ内のディレクトリ configloc であり、ルータでは basic カテゴリのシグニチャが使用され、ルータが confgloc ディレクトリ内の情報にアクセスできるようにパブリック キーが設定されていることを示しています。

項目名	項目値
コンフィグレーションの場所	flash:/configloc/
選択したカテゴリ	basic
パブリック キー	Configured

グローバル設定の編集

［グローバル設定の編集］ダイアログには、［Syslog と SDEE］タブおよび［グローバル エンジン］タブが含まれます。表示する情報のリンクをクリックします。

- ［Syslog と SDEE］タブ
- ［グローバル エンジン］タブ

［Syslog と SDEE］タブ

ルータで Cisco IOS 12.4(11)T 以降のイメージを使用している場合に表示される［Syslog と SDEE］ダイアログを使用すると、SDEE のサブスクリプション、イベント、およびメッセージに、シスログ（Syslog）通知とパラメータを設定できます。

シスログ（Syslog）通知の有効化

アラーム、イベント、およびエラーのメッセージがルータからシスログ（Syslog）サーバに送信されるようにするときに、このチェック ボックスを選択します。この通知方法を使用するには、シスログ（Syslog）サーバを［システム プロパティ］で指定しておく必要があります。

SDEE

［同時 SDEE サブスクリプション数］フィールドには、同時 SDEE サブスクリプションの数を 1 ～ 3 の範囲で入力します。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。

［SDEE アラートの最大保存数］フィールドには、ルータに保存される SDEE アラートの最大数を 10 ～ 2,000 の範囲で入力します。保存するアラートの数を増やすとルータのメモリの使用量が増えます。

［SDEE メッセージの最大保存数］フィールドには、ルータに保存される SDEE メッセージの最大数を 10 ～ 500 の範囲で入力します。保存するメッセージの数を増やすとルータのメモリの使用量が増えます。

［グローバル エンジン］タブ

ルータで Cisco IOS 12.4(11)T 以降のイメージが使用されている場合に表示される［グローバル エンジン］ダイアログでは、次のセクションで説明する設定が可能です。

エンジン フェイル クローズの有効化

デフォルトでは、Cisco IOS ソフトウェアにより特定のエンジンの新しいシグニチャがコンパイルされている間、そのエンジンに対するパケットは、スキャンなしでそのまま通過します。コンパイル中、Cisco IOS ソフトウェアでパケットが破棄されるようにするには、このオプションを有効にします。

IPS インターフェイス上の拒否アクションの有効化

このオプションは、シグニチャ　アクションが［denyAttackerInline］または［denyFlowInline］に設定されている場合に適用できます。Cisco IOS IPS のデフォルトでは、ACL は Cisco IOS IPS インターフェイスではなく、攻撃的なトラフィッ

クの送信元のインターフェイスに適用されます。このオプションを有効にすると、Cisco IOS IPS により、最初に攻撃的なトラフィックを受信したインターフェイスではなく、Cisco IOS IPS インターフェイスに直接 ACL が適用されます。ルータで負荷分散を実行していない場合は、この設定を有効にしないでください。ルータで負荷分散を実行している場合は、この設定を有効にすることをお勧めします。

IPS 必須項目の編集

［IPS 必須項目の編集］ダイアログには、次のカテゴリの情報に対応するタブが含まれます。表示する情報のリンクをクリックします。

- コンフィギュレーションの場所タブ
- カテゴリの選択タブ
- ［パブリック キー］タブ

コンフィギュレーションの場所タブ

コンフィギュレーションの場所がルータに設定されている場合は、それを編集できます。場所が設定されていない場合は、［追加］をクリックして、場所を設定できます。［追加］ボタンは、コンフィギュレーションの場所がすでに設定されている場合は、無効になっています。［編集］ボタンは、コンフィギュレーションの場所が設定されていない場合は、無効になっています。詳細については、「IPS の作成：コンフィギュレーションの場所とカテゴリ」を参照してください。

カテゴリの選択タブ

シグニチャのカテゴリを指定すると、Cisco CP により、特定容量のルータのメモリに対する適切なシグニチャのサブセットがルータに設定されます。シグニチャを選択する際にカテゴリの制約を排除する場合は、既存のカテゴリの設定を削除することもできます。

カテゴリの設定

［カテゴリの設定］をクリックし、**basic** または **advanced** のどちらかを選択します。使用可能なフラッシュ メモリが 128MB 未満のルータでは、basic カテゴリが適切です。128MB 以上のフラッシュ メモリが使用可能なルータでは、advanced カテゴリが適切です。

カテゴリ設定の削除

カテゴリの設定を削除する場合は、［カテゴリ設定の削除］をクリックします。

［パブリック キー］タブ

このダイアログには、Cisco IOS IPS に設定されているパブリック キーが表示されます。このダイアログで、キーを追加または削除できます。キーを追加する場合は、［追加］をクリックして、表示されるダイアログでキーを設定します。

キーを削除する場合は、キー名を選択して［削除］をクリックします。

パブリックキーの追加

Cisco.com の次のサイトからキーの名前とキー自体をコピーできます。

http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup

キーの名前をコピーして、このダイアログの［名前］フィールドに貼り付けます。次に、同じ場所からキーをコピーして、［キー］フィールドに貼り付けます。テキスト内の実際にコピーしたり貼り付けたりする部分の詳細については、「パブリック キーの設定」を参照してください。

IPS の編集：自動アップデート

シグニチャ ファイルのアップデートは、Cisco.com にアップロードされます。Cisco CP では、指定したシグニチャ ファイルのアップデートをダウンロードするか、または定義されたスケジュールで最新のシグニチャ ファイルのアップデートを自動的にダウンロードすることができます。

このヘルプ トピックでは、ルータで Cisco IOS 12.4(11)T 以降が実行されている場合に表示される［自動アップデート］ウィンドウについて説明します。

自動アップデートの設定の前に

自動アップデートを設定する前に、ルータのクロックを PC のクロックと同期させる必要があります。そのためには、次の手順を完了します。

ステップ 1　［設定］>［ルータ］>［時刻］>［日付 / 時刻］の順に選択します。

ステップ 2　［日付 / 時刻］ウィンドウで［設定の変更］をクリックします。

ステップ 3　［ローカル PC の時計と同期をとる］オプションをクリックして、［同期］ボタンをクリックします。

ステップ 4　ダイアログを閉じます。

Cisco.com からのシグニチャ ファイルのダウンロード

Cisco CP を使用して、Cisco.com から PC に特定のシグニチャ ファイルをダウンロードするには、ダウンロードするファイルを指定し、そのファイルの保存場所を指定します。使用中のシグニチャ パッケージによって、Cisco IOS IPS で現在使用しているバージョンが表示されます。シグニチャ ファイルをダウンロードして、Cisco.com の Cisco IOS IPS Web ページからその他の情報を取得するには、CCO へのログインが必要です。

最新のシグニチャ ファイルをダウンロードするには、［最新の Cisco CP ファイルの取得］をクリックします。［参照］をクリックして、ファイルの保存場所を指定し、次に［ダウンロード］をクリックしてファイルを PC に保存します。

最新の CLI パッケージをダウンロードするには、［最新の CLI パッケージの取得］をクリックします。［参照］をクリックして、ファイルの保存場所を指定し、次に［ダウンロード］をクリックしてファイルを PC に保存します。

ダウンロードする前に使用可能なファイルを参照するには、[ダウンロード可能なファイルをリスト] をクリックします。次に、[シグニチャ パッケージのリスト] フィールドの右のボタンをクリックします。使用可能なファイルのリストを参照するには、コンテキスト メニューの [更新] をクリックします。Readme ファイルを表示するには、[Readme の表示] をクリックします。目的のファイルを選択し、[参照] ボタンと [ダウンロード] ボタンを使用して、そのファイルを PC に保存します。

自動アップデート

Cisco CP で、指定したリモート サーバから自動的にアップデート ファイルが取得されるようにするには、[自動アップデートを有効にする] をクリックします。

IPS 自動アップデート URL 設定

サーバへのログインに必要なユーザ名とパスワードを入力し、[IPS 自動アップデート URL 設定] フィールドに、アップデート ファイルへの URL を入力します。次に URL の入力例を示します。

```
tftp//:192.168.0.2/jdoe/ips-auto-update/IOS_update.zip
```

スケジュール

ルータでサーバからアップデート ファイルをいつ取得するようにするかを指定します。各カラムに複数の値を指定して、範囲または複数の時間値を指定できます。日曜日から木曜日まで、毎日午前 1 時にサーバからアップデート ファイルを取得するように指定する場合は、次の表に示すとおりに値を選択します。

分	時間	日付	曜日
0	1	1 と 31 を選択する。	日曜日から木曜日のチェックボックスを選択する。

[自動アップデート] の各フィールドでの変更内容をルータに送信するには、[変更の適用] をクリックします。これらのフィールドに入力したデータを削除するには、[変更の破棄] をクリックします。

IPS の編集：SEAP 設定

Cisco IOS リリース 12.4(11)T 以降で使用可能な Cisco IOS IPS では、Signature Event Action Processing（SEAP）が実装されます。このウィンドウには、設定可能な SEAP 機能が示されます。設定を開始するには、［SEAP 設定］ボタンの下にあるいずれかのボタンをクリックします。

ルータで Cisco IOS 12.4(11)T 以降が実行されている場合には、Cisco IOS IPS の SEAP 設定が可能です。

IPS の編集：SEAP 設定：ターゲットの価値評価

ターゲットの価値評価（TVR）は、ユーザにとってのターゲット ホストの価値を示す、ユーザ定義の値です。これを使用すると、ユーザは重要なシステムに関連するイベントのリスクを高く設定し、価値の低いターゲットのイベントのリスクを低く設定できます。

［ターゲットの価値評価］カラムと［ターゲット IP アドレス］カラムの右にあるボタンを使用して、ターゲット エントリを追加、削除、および編集します。［すべて選択］をクリックすると、ターゲットの価値評価がすべて自動的にハイライトされます。［追加］をクリックすると、新しい TVR エントリを作成できるダイアログが表示されます。［編集］をクリックすると、エントリの IP アドレス情報を変更できます。

ターゲットの価値評価カラム

ターゲットは、high、low、medium、missioncritical、または No Value で評価されます。ターゲット エントリが作成された後で、評価を変更することはできません。評価を変更する必要がある場合は、ターゲット エントリをいったん削除してから、適切な評価を指定して再作成してください。

ターゲット IP アドレス カラム

ターゲット IP アドレスには、1 つの IP アドレスを入力することも、複数の IP アドレスの範囲を入力することもできます。次に 2 つのエントリの例を示します。1 つは単一の IP アドレス エントリで、もう 1 つはアドレスの範囲です。

ターゲットの価値評価	ターゲット IP アドレス
High	192.168.33.2
Medium	10.10.3.1-10.10.3.55

変更の適用

［ターゲットの価値評価］ウィンドウに必要な情報を入力して、［変更の適用］をクリックします。ルータに送信する変更内容がない場合は、［変更の適用］ボタンは無効になっています。

変更の破棄

［ターゲットの価値評価］ウィンドウに入力した、ルータには送信していない情報をクリアするには、［変更の破棄］をクリックします。ルータへの配信待ちの変更内容がない場合は、［変更の破棄］ボタンは無効になっています。

ターゲットの価値評価の追加

TVR エントリを追加するには、ターゲットの価値評価を選択し、ターゲット IP アドレスまたは IP アドレスの範囲を入力します。

ターゲットの価値評価（TVR）

ターゲットは、high、low、medium、missioncritical、または No Value で評価されます。ある評価をいずれかのターゲット エントリに使用した後で、その評価を別のエントリに使用することはできません。このため、同じ評価を付けるすべてのターゲットに、同一のエントリを入力します。

ターゲット IP アドレス

次の例に示すように、1 つのターゲット IP アドレスまたはアドレスの範囲を入力できます。

```
192.168.22.33
10.10.11.4-10.10.11.55
```

入力した IP アドレスは、［ターゲットの価値評価］ウィンドウに表示されます。

IPS の編集：SEAP 設定：イベント アクション オーバーライド

イベント アクション オーバーライドを使用すると、イベントのリスク評価（RR）に基づいてそのイベントに関連付けられているアクションを変更できます。これは、各イベント アクションに RR 範囲を割り当てることによって実行できます。イベントが発生し、RR が定義した範囲内である場合、アクションがそのイベントに追加されます。イベント アクション オーバーライドは、各シグニチャを個別に設定する必要なく、イベント アクションをグローバルに追加する方法です。

イベント アクション オーバーライドの使用

Cisco IOS IPS でイベント アクション オーバーライドを使用できるようにするには、［イベント アクション オーバーライドの使用］チェック ボックスを選択します。イベント アクション オーバーライドは、ルータ上で有効になっているかどうかにかかわらず、追加したり編集したりできます。

すべて選択

［すべて選択］ボタンは、［有効］、［無効］、および［削除］ボタンと連動します。すべてのイベント アクション オーバーライドを有効または無効にするには、［すべて選択］をクリックし、［有効］または［無効］をクリックします。すべてのイベント アクション オーバーライドを削除するには、［すべて選択］をクリックし、［削除］をクリックします。

追加ボタンおよび編集ボタン

［追加］をクリックすると、イベント アクション オーバーライドに関する情報を入力できるダイアログが表示されます。イベント アクション オーバーライドを選択し、［編集］をクリックすると、イベント アクション オーバーライドに関する情報を変更できます。

削除

［削除］をクリックすると、選択したイベント アクション オーバーライドが削除されます。［すべて選択］をクリックすると、すべてのイベント アクション オーバーライドが削除されます。

有効および無効

［有効］ボタンおよび［無効］ボタンを使用すると、イベント アクション オーバーライドを有効または無効にできます。任意のイベント アクションのオーバーライドを選択するか、［すべて選択］をクリックしてすべてのイベント アクションのオーバーライドを有効または無効にします。

変更の適用

［イベント アクション オーバーライド］ウィンドウに必要な情報を入力したら、［変更の適用］をクリックします。ルータに送信する変更内容がない場合は、［変更の適用］ボタンは無効になっています。

変更の破棄

［イベント アクション オーバーライド］ウィンドウに入力した、ルータには送信していない情報をクリアするには、［変更の破棄］をクリックします。ルータへの配信待ちの変更内容がない場合は、［変更の破棄］ボタンは無効になっています。

イベント アクション オーバーライドの追加または編集

イベント アクション オーバーライドを追加するには、イベント アクションを選択し、有効または無効にして、RR 範囲を指定します。イベント アクション オーバーライドを編集する場合は、イベント アクションを変更できません。

イベント アクション

次のいずれかのイベント アクションを選択します。

- ［インラインで攻撃拒否］— 攻撃者のアドレスが送信元である、このパケットおよびこれ以降のパケットを、指定された期間にわたって送信しません（インラインだけ）。
- ［Deny Connection Inline］— このパケットおよびこれ以降のパケットを TCP フローで送信しません（インラインだけ）。
- ［Deny Packet Inline］— このパケットを送信しません。
- ［Produce Alert］— ログに <evIdsAlert> を書き込みます。

- ［Reset TCP Connection］— TCP RESETS を送信して TCP フローをハイジャックおよび終端します。

有効

イベント アクション オーバーライドを有効にする場合は［はい］を、無効にする場合は、［いいえ］をクリックします。［イベント アクション オーバーライド］ウィンドウからイベント アクション オーバーライドを有効または無効にすることもできます。

リスク評価

［最小］ボックスに RR 範囲の下限を入力し、［最大］ボックスに範囲の上限を入力します。イベントの RR 値が指定された範囲内である場合は、［イベント アクション］で指定されたオーバーライドが Cisco IOS IPS により追加されます。たとえば、［Deny Connection Inline］に 90 ～ 100 の RR 範囲が割り当てられていて、RR が 95 のイベントが発生すると、Cisco IOS IPS でインラインの接続が拒否されます。

IPS の編集：SEAP 設定：イベント アクション フィルタ

イベント アクション フィルタを使用すると、Cisco IOS IPS ですべてのアクションを実行したり、イベント全体を削除したりする必要なく、1 つのイベントに対する応答として個別のアクションを実行できます。フィルタは、アクションをイベントから削除する働きをします。イベントからすべてのアクションを削除するフィルタは、実質的にイベントを消滅させます。イベント アクション フィルタは、順序付きのリストとして処理されます。リスト内でフィルタを上下に移動して、あるフィルタがルータで別のフィルタより前に処理されるように設定できます。

［イベント アクション フィルタ］ウィンドウには、設定されているイベント アクション フィルタが表示され、Cisco IOS IPS によって希望の順序でフィルタが処理されるようにフィルタ リストの順番を変更できます。

イベント アクション フィルタの使用

イベント アクション フィルタの使用を有効にするには、[イベント アクション フィルタの使用] チェック ボックスを選択します。イベント アクション フィルタが有効になっているかどうかにかかわらず、イベント アクション フィルタを追加、編集、および削除したり、リストを再編成してルータでフィルタが処理される順序を指定したりできます。

Event Action Filter List エリア

Event Action Filter List エリアのカラムの説明については、「イベント アクション フィルタの追加または編集」を参照してください。

Event Action Filter List のボタン

Event Action Filter List のボタンを使用すると、イベント アクション フィルタを作成、編集、および削除したり、各イベント アクション フィルタを希望の順序でリスト内に配置したりできます。ボタンについては、次のセクションで説明しています。

すべて選択

[すべて選択] ボタンは、[有効]、[無効]、および [削除] ボタンと連動します。すべてのイベント アクション フィルタを有効または無効にするには、[すべて選択] をクリックして、[有効] または [無効] をクリックします。すべてのイベント アクション フィルタを削除するには、[すべて選択] をクリックして、[削除] をクリックします。

追加

リストの最後にイベント アクション フィルタを追加するには、[追加] ボタンをクリックします。フィルタのデータを入力できるダイアログが表示されます。

上に挿入

新しいイベント アクション フィルタを既存のフィルタの上に挿入するには、既存のフィルタ エントリを選択して、[上に挿入] をクリックします。フィルタのデータを入力できるダイアログが表示されます。

下に挿入

新しいイベント アクション フィルタを既存のフィルタの下に挿入するには、既存のフィルタ エントリを選択して、[下に挿入] をクリックします。フィルタのデータを入力できるダイアログが表示されます。

上へ移動

イベント アクション フィルタを選択して、[上へ移動] ボタンをクリックすると、フィルタをリスト内で上に移動できます。

下へ移動

イベント アクション フィルタを選択して、[下へ移動] ボタンをクリックすると、フィルタをリスト内で下に移動できます。

編集

選択したイベント アクション フィルタを編集するには、[編集] ボタンをクリックします。

有効

選択したイベント アクション フィルタを有効にするには、[有効] ボタンをクリックします。すべてのイベント アクション フィルタを有効にするには、[すべて選択] をクリックしてから、[有効] をクリックします。

無効

選択したイベント アクション フィルタを無効にするには、[無効] ボタンをクリックします。すべてのイベント アクション フィルタを無効にするには、[すべて選択] をクリックしてから、[無効] をクリックします。

削除

選択したイベント アクション フィルタを削除するには、[削除] ボタンをクリックします。すべてのイベント アクション フィルタを削除するには、[すべて選択] をクリックしてから、[削除] をクリックします。

変更の適用

このウィンドウに必要な情報を入力したら、［変更の適用］をクリックします。ルータに送信する変更内容がない場合は、［変更の適用］ボタンは無効になっています。

変更の破棄

このウィンドウに入力した、ルータには送信していない情報をクリアするには、［変更の破棄］をクリックします。ルータへの配信待ちの変更内容がない場合は、［変更の破棄］ボタンは無効になっています。

イベント アクション フィルタの追加または編集

次に、［イベント アクション フィルタの追加］および［イベント アクション フィルタの編集］ダイアログのフィールドについて説明します。

名前

Cisco CP では、イベント アクション フィルタに Q00000 で始まる名前が付けられます。イベント アクション フィルタを追加するたびに、名前の数字部分が 1 ずつ増加します。自分で選んだ名前を入力することもできます。イベント アクション フィルタを編集する場合、［名前］フィールドは読み取り専用です。

有効

イベント アクション フィルタを有効にする場合は［はい］を、無効にする場合は、［いいえ］をクリックします。［イベント アクション フィルタ］ウィンドウからイベント アクション フィルタを有効または無効にすることもできます。

シグニチャ ID

［シグニチャ ID］には、900 ～ 65535 のシグニチャ ID の範囲を入力するか、その範囲内の 1 つの ID を入力します。範囲を入力する場合は、範囲の上限と下限をダッシュ（-）で区切って入力します（たとえば、「988-5000」）。

サブシグニチャ ID

［サブシグニチャ ID］には、0 ～ 255 のサブシグニチャ ID の範囲を入力するか、その範囲内の 1 つのサブシグニチャ ID を入力します。範囲を入力する場合は、範囲の上限と下限をダッシュ（-）で区切って入力します（たとえば、「70-200」）。

攻撃者のアドレス

［攻撃者のアドレス］には、0.0.0.0 ～ 255.255.255.255 のアドレスの範囲を入力するか、その範囲内の 1 つのアドレスを入力します。範囲を入力する場合は、範囲の上限と下限をダッシュ（-）で区切って入力します（たとえば、「192.168.7.0-192.168.50.0」）。

攻撃者のポート

［攻撃者のポート］には、0 ～ 65535 のポート番号の範囲を入力するか、その範囲内の 1 つのポート番号を入力します。範囲を入力する場合は、範囲の上限と下限をダッシュ（-）で区切って入力します（たとえば、「988-5000」）。

被害先のアドレス

［被害先のアドレス］には、0.0.0.0 ～ 255.255.255.255 のアドレスの範囲を入力するか、その範囲内の 1 つのアドレスを入力します。範囲を入力する場合は、範囲の上限と下限をダッシュ（-）で区切って入力します（たとえば、「192.168.7.0-192.168.50.0」のように入力します）。

被害先のポート

［被害先のポート］には、0 ～ 65535 のポート番号の範囲を入力するか、その範囲内の 1 つのポート番号を入力します。範囲を入力する場合は、範囲の上限と下限をダッシュ（-）で区切って入力します（たとえば、「988-5000」）。

リスク評価

［リスク評価］には、0 ～ 100 の RR 範囲を入力します。

削除するアクション

一致するイベントから削除するアクションをクリックします。一致するイベントから複数のアクションを削除する場合は、**Ctrl** キーを押したまま対象のイベントを選択します。このフィルタに選択するすべてのイベントは、［イベント アクション フィルタ］ウィンドウに表示されます。

一致で停止

このイベント アクション フィルタに一致するイベントが発生したときに Cisco IOS IPS を停止する場合は、［はい］をクリックします。Cisco IOS IPS で、一致するイベントを他の残りのフィルタに対して評価する場合は、［いいえ］をクリックします。

コメント

このフィルタの目的を説明するコメントを追加できます。このフィールドはオプションです。

IPS の編集：シグニチャ

Cisco IOS IPS では、トラフィックを既知の攻撃のシグニチャと比較することによって、侵入を防ぎます。Cisco IOS IPS をサポートする Cisco IOS イメージには、使用可能なビルトイン シグニチャがあります。また、トラフィックの検査時に使用するルータのシグニチャを Cisco IOS IPS でインポートすることもできます。インポートされたシグニチャは、シグニチャ定義ファイル（SDF）に格納されます。

このウィンドウでは、ルータに設定されている Cisco IOS IPS のシグニチャを表示できます。カスタマイズしたシグニチャを追加することも、Cisco.com からダウンロードした SDF からシグニチャをインポートすることもできます。また、シグニチャの編集、削除、有効化、および無効化も可能です。

Cisco IOS IPS には、ルータが対応しているシグニチャが定義された SDF が付属しています。Cisco IOS IPS に付属している SDF、および Cisco IOS IPS での SDF の使用方法の詳細については、「IPS で用意されているシグニチャ定義ファイル」を参照してください。

シグニチャ ツリー

［シグニチャ］ツリーでは、表示するシグニチャのタイプに応じて、右側のシグニチャ リストにフィルタを適用できます。まず、表示する一般的なタイプのシグニチャのブランチを選択します。シグニチャ リストには、選択したタイプの設定済みシグニチャが表示されます。ブランチの左側にプラス（+）記号が表示されている場合は、フィルタの絞り込みに使用できるサブカテゴリがあります。+ 記号をクリックしてブランチを開いてから、表示するシグニチャのサブカテゴリを選択します。シグニチャ リストが空白の場合は、そのタイプで使用できるシグニチャは設定されていません。

たとえば、攻撃シグニチャをすべて表示する場合は、ブランチの［Attack］フォルダをクリックします。攻撃シグニチャの表示にフィルタを適用するために使用できるサブカテゴリを表示する場合は、［Attack］フォルダの横にある + 記号をクリックします。サービス拒否（DoS）シグニチャを表示する場合は、［DoS］フォルダをクリックします。

インポート ボタン

PC またはルータからシグニチャ定義ファイルをインポートする場合にクリックします。ファイルを指定すると、そのファイル内の使用可能なシグニチャが表示され、その中からルータにインポートするシグニチャを選択できます。インポートするシグニチャの選択方法の詳細については、「シグニチャのインポート」を参照してください。

（注） ルータに DOS ベースのファイル システムがある場合、シグニチャはルータからしかインポートできません。

SDF は、シスコから入手できます。Cisco.com から SDF をダウンロードするには、次の URL をクリックします（ログインが必要です）。

http://www.cisco.com/cgi-bin/tablebuild.pl/ios-sigup

シスコでは、新たな脅威に関する情報を提供する Alert Center を運営しています。詳細については、「Cisco セキュリティ センター」を参照してください。

選択肢リストおよび条件リスト

［選択肢］ドロップダウン リストと［条件］ドロップダウン リストを使用すると、表示するシグニチャのタイプに応じてリストの項目にフィルタを適用できます。まず、［選択肢］ドロップダウン リストで条件を選択し、次に［条件］ドロップダウン リストで条件の値を選択します。

たとえば、［選択肢］リストで［エンジン］を選択すると、条件が［エンジン］に変更され、［Atomic.ICMP］や［Service.DNS］などの使用可能なエンジンのいずれかを選択できます。

［Sig ID］または［Sig Name］（シグニチャ名）を選択した場合は、［条件］フィールドに値を入力する必要があります。

合計［*n*］新規［*n*］削除［*n*］

このテキストは、新しいシグニチャと削除されたシグニチャの合計を示します。

すべて選択

リスト内のすべてのシグニチャを選択する場合にクリックします。

追加

次のいずれかを実行する場合は［追加］をクリックします。

- ［新規追加］— 新しいシグニチャを追加し、表示されたダイアログでシグニチャのパラメータを入力する場合に選択します。
- ［複製］— 複製オプションは、ハードコードされたエンジンに属さないシグニチャが指定された場合に有効になります。このオプションは、シグニチャで Cisco IOS のハードコードされたエンジンのいずれかが使用される場合は無効になります。

編集

指定したシグニチャのパラメータを編集する場合にクリックします。

削除

［削除］をクリックすると、指定したシグニチャに、リストから削除するためのマークを付けることができます。削除したシグニチャを表示するには、［詳細］をクリックします。これらのシグニチャのステータスと処理の詳細については、「削除するシグニチャ」を参照してください。

（注）　TrendMicro OPACL シグニチャについては、表示と監視は可能ですが、編集、削除、有効化、および無効化は不可能です。TrendMicro OPACL シグニチャが指定された場合、［編集］、［削除］、［有効］、［無効］の各ボタンは無効になります。これらのシグニチャは、Cisco Incident Control Server によって制御されます。

有効

指定したシグニチャを有効にする場合は、［有効］をクリックします。有効になっているシグニチャには、緑のチェックマークが付けられます。いったん無効にした後で再度有効にしたシグニチャには、変更をルータに適用しなければならないことを示す黄色の待機アイコンが［!］カラムに表示されます。

無効

指定したシグニチャを無効にする場合は［無効］をクリックします。無効になっているシグニチャには、赤いアイコンが表示されます。シグニチャが現在のセッションの間に無効になった場合は、変更をルータに適用しなければならないことを示す黄色の待機アイコンが［!］カラムに表示されます。

要約 / 詳細ボタン

削除のマークが付けられたシグニチャを表示または非表示にする場合にクリックします。

シグニチャ リスト

ルータから取得されたシグニチャと、SDF から追加されたすべてのシグニチャが表示されます。

（注）　インポートの対象として設定されている、展開済みのシグニチャと同じシグニチャはインポートされず、シグニチャ リストに表示されません。

シグニチャ リストには、選択コントロールを使用してフィルタを適用できます。

有効	有効なシグニチャには、緑のアイコンが表示される。有効な場合は、シグニチャが検出されたときに指定されたアクションが実行される。 無効なシグニチャには、赤いアイコンが表示される。無効な場合、アクションは無効になり実行されない。
アラート（!）	このカラムには、黄色の［Wait］（待機）アイコンが表示される場合がある。  このアイコンは、ルータに配信されていない新しいシグニチャ、またはルータに配信されていない変更済みのシグニチャであることを示す。
Sig ID	数字のシグニチャ ID。たとえば、ICMP Echo Reply のシグニチャ ID は 2000。
SubSig ID	サブシグニチャ ID。
名前	シグニチャの名前。たとえば、ICMP Echo Reply。
アクション	シグニチャが検出されたときに実行するアクション。
フィルタ	対応するシグニチャに関連付けられている ACL。
重大度	イベントの重大度レベル。重大度レベルは、情報、低、中、および高。
エンジン	シグニチャが属するエンジン。

右クリック コンテキスト メニュー

シグニチャを右クリックすると、次のオプションを選択可能な、Cisco CP のコンテキスト メニューが表示されます。

- ［アクション］— シグニチャが一致するときに実行されるアクションを選択する場合にクリックします。詳細については、「アクションの割り当て」を参照してください。
- ［重大度の設定先］— シグニチャの重大度のレベルを高、中、低、または情報に設定する場合にクリックします。
- ［デフォルトの復元］— シグニチャのデフォルト値を復元する場合にクリックします。
- ［フィルタの削除］— シグニチャに適用されているフィルタを削除する場合にクリックします。
- ［NSDB ヘルプ］（CCO アカウントが必要）— ネットワーク セキュリティ データベース（NSDB）についてのヘルプを表示する場合にクリックします。

削除するシグニチャ

このエリアは、［詳細］ボタンをクリックすると、表示されます。ここには、シグニチャ リストから削除したシグニチャ、および削除マーク付きシグニチャが表示されます。インポートされたシグニチャは、ルータにすでに設定されているシグニチャを置き換えるように設定されているためです。詳細については、「シグニチャのインポート方法」を参照してください。

削除マークが付けられたシグニチャは、［変更の適用］をクリックするまでは、Cisco IOS IPS でアクティブに設定されたままになります。［シグニチャ］ウィンドウを閉じて Cisco IOS IPS を無効にした場合は、Cisco IOS IPS が再度有効になったときにマーク付きのシグニチャが削除されます。

すべての削除の取り消しボタン

削除マーク付きシグニチャのリストにあるすべてのシグニチャを復元する場合にクリックします。

削除の取り消しボタン

指定した削除マーク付きシグニチャを復元する場合にクリックします。クリックすると、シグニチャのマークが消え、アクティブなシグニチャのリストに戻されます。

変更の適用ボタン

新たにインポートしたシグニチャ、編集されたシグニチャ、および新たに有効または無効にされたシグニチャをルータに配信する場合にクリックします。変更が適用されると、黄色の［Wait］（待機）アイコンが［!］カラムから削除されます。これらの変更は、ルータのフラッシュ メモリにある sdmips.sdf ファイルに保存されます。このファイルは、［変更の適用］を初めてクリックしたときに自動的に作成されます。

（注） シグニチャのインポートを試みるときに、それらのシグニチャがすべて展開済みのシグニチャと同じである場合には、［変更の適用］ボタンが無効になります。

変更の破棄ボタン

これまでの変更を破棄する場合にクリックします。

（注） シグニチャのインポートを試みるときに、それらのシグニチャがすべて展開済みのシグニチャと同じである場合には、［変更の破棄］ボタンが無効になります。

被害先のポート

［被害先のポート］には、0 ～ 65535 のポート番号の範囲を入力するか、その範囲内の 1 つのポート番号を入力します。範囲を入力する場合は、範囲の上限と下限をダッシュ（-）で区切って入力します（たとえば、「988-5000」）。

リスク評価

［リスク評価］には、0 ～ 100 の RR 範囲を入力します。

削除するアクション

一致するイベントから削除するアクションをクリックします。一致するイベントから複数のアクションを削除する場合は、**Ctrl** キーを押したまま対象のイベントを選択します。このフィルタに選択するすべてのイベントは、［イベント アクション フィルタ］ウィンドウに表示されます。

一致で停止

このイベント アクション フィルタに一致するイベントが発生したときに Cisco IOS IPS を停止する場合は、［はい］をクリックします。Cisco IOS IPS で、一致するイベントを他の残りのフィルタに対して評価する場合は、［いいえ］をクリックします。

コメント

このフィルタの目的を説明するコメントを追加できます。このフィールドはオプションです。

IPS の編集：シグニチャ

Cisco IOS IPS では、トラフィックを既知の攻撃のシグニチャと比較することによって、侵入を防ぎます。Cisco IOS IPS をサポートする Cisco IOS イメージには、使用可能なビルトイン シグニチャがあります。また、トラフィックの検査時に使用するルータのシグニチャを Cisco IOS IPS でインポートすることもできます。インポートされたシグニチャは、シグニチャ定義ファイル（SDF）に格納されます。

このヘルプ トピックでは、ルータで Cisco IOS 12.4(11)T 以降が実行されている場合に表示される［シグニチャ］ウィンドウについて説明します。

［シグニチャ］ウィンドウでは、ルータに設定されている Cisco IOS IPS シグニチャを表示できます。カスタマイズしたシグニチャを追加することも、Cisco.com からダウンロードした SDF からシグニチャをインポートすることもできます。シグニチャの編集、有効化、無効化、リタイア（除外）、およびアンリタイア（除外解除）も実行できます。

シグニチャ ツリー

［シグニチャ］ツリーでは、表示するシグニチャのタイプに応じて、右側のシグニチャ リストにフィルタを適用できます。まず、表示する一般的なタイプのシグニチャのブランチを選択します。シグニチャ リストには、選択したタイプの設定済みシグニチャが表示されます。ブランチの左側にプラス（+）記号が表示されている場合は、フィルタの絞り込みに使用できるサブカテゴリがあります。+ 記号をクリックしてブランチを開いてから、表示するシグニチャのサブカテゴリを選択します。シグニチャ リストが空白の場合は、そのタイプで使用できるシグニチャは設定されていません。

たとえば、攻撃シグニチャをすべて表示する場合は、ブランチの［Attack］フォルダをクリックします。攻撃シグニチャの表示にフィルタを適用するために使用できるサブカテゴリを表示する場合は、［Attack］フォルダの横にある + 記号をクリックします。サービス拒否（DoS）シグニチャを表示する場合は、［DoS］フォルダをクリックします。

インポート ボタン

PC またはルータからシグニチャ定義ファイルをインポートする場合にクリックします。ファイルを指定すると、そのファイル内の使用可能なシグニチャが表示され、その中からルータにインポートするシグニチャを選択できます。インポートするシグニチャの選択方法の詳細については、「シグニチャのインポート」を参照してください。

（注） ルータに DOS ベースのファイル システムがある場合、シグニチャはルータからしかインポートできません。

SDF は、シスコから入手できます。Cisco.com から SDF をダウンロードするには、次の URL をクリックします（ログインが必要です）。

http://www.cisco.com/cgi-bin/tablebuild.pl/ios-sigup

シスコでは、新たな脅威に関する情報を提供する Alert Center を運営しています。詳細については、「Cisco セキュリティ センター」を参照してください。

選択肢リストおよび条件リスト

［選択肢］ドロップダウン リストと［条件］ドロップダウン リストを使用すると、表示するシグニチャのタイプに応じてリストの項目にフィルタを適用できます。まず、［選択肢］ドロップダウン リストで条件を選択し、次に［条件］ドロップダウン リストで条件の値を選択します。

たとえば、［選択肢］リストで［エンジン］を選択すると、条件が［エンジン］に変更され、［Atomic.ICMP］や［Service.DNS］などの使用可能なエンジンのいずれかを選択できます。

［Sig ID］または［Sig Name］（シグニチャ名）を選択した場合は、［条件］フィールドに値を入力する必要があります。

合計［*n*］

このテキストは、ルータ上のシグニチャの合計数を示します。

コンパイル完了［*n*］

このテキストは、ルータ上でコンパイルされたシグニチャの合計数を示します。

すべて選択

リスト内のすべてのシグニチャを選択する場合にクリックします。

無効

指定したシグニチャを無効にする場合は［無効］をクリックします。無効になっているシグニチャには、赤いアイコンが表示されます。シグニチャが現在のセッションの間に無効になった場合は、変更をルータに適用しなければならないことを示す黄色の待機アイコンが［!］カラムに表示されます。

リタイア

シグニチャがスキャンのためにコンパイルされないようにするには、［リタイア］をクリックします。

アンリタイア

シグニチャがスキャンのためにコンパイルされるようにするには、［アンリタイア］をクリックします。

シグニチャ リスト

ルータから取得されたシグニチャと、SDF から追加されたすべてのシグニチャが表示されます。

（注） インポートの対象として設定されている、展開済みのシグニチャと同じシグニチャはインポートされず、シグニチャ リストに表示されません。

シグニチャ リストには、選択コントロールを使用してフィルタを適用できます。

有効	有効なシグニチャには、緑のアイコンが表示される。有効な場合は、シグニチャが検出されたときに指定されたアクションが実行される。 無効なシグニチャには、赤いアイコンが表示される。無効な場合、アクションは無効になり実行されない。
アラート（!）	このカラムには、黄色の［Wait］（待機）アイコンが表示される場合がある。  このアイコンは、ルータに配信されていない新しいシグニチャ、またはルータに配信されていない変更済みのシグニチャであることを示す。
Sig ID	数字のシグニチャ ID。たとえば、ICMP Echo Reply のシグニチャ ID は 2000。
SubSig ID	サブシグニチャ ID。
名前	シグニチャの名前。たとえば、ICMP Echo Reply。
アクション	シグニチャが検出されたときに実行するアクション。
重大度	イベントの重大度レベル。重大度レベルは、情報、低、中、および高。
信頼度評価	シグニチャの信頼度評価。
リタイア	True または False のいずれかの値。シグニチャがリタイアになっている場合は True。そうでない場合は False。リタイアになっているシグニチャは、コンパイルされない。
エンジン	シグニチャが属するエンジン。

右クリック コンテキスト メニュー

シグニチャを右クリックすると、次のオプションを選択可能な、Cisco CP のコンテキスト メニューが表示されます。

- ［アクション］— シグニチャが一致するときに実行されるアクションを選択する場合にクリックします。詳細については、「アクションの割り当て」を参照してください。
- ［信頼度評価］— シグニチャの信頼度評価を入力する場合にクリックします。

- ［重大度の設定先］— シグニチャの重大度のレベルを高、中、低、または情報に設定する場合にクリックします。
- ［デフォルトの復元］— シグニチャのデフォルト値を復元する場合にクリックします。
- ［NSDB ヘルプ］（CCO アカウントが必要）— ネットワーク セキュリティ データベース（NSDB）についてのヘルプを表示する場合にクリックします。

変更の適用

新たにインポートしたシグニチャ、編集されたシグニチャ、および新たに有効または無効にされたシグニチャをルータに配信する場合は、［変更の適用］をクリックします。変更が適用されると、黄色の［Wait］（待機）アイコンが［!］カラムから削除されます。これらの変更は、ルータのフラッシュ　メモリにある sdmips.sdf ファイルに保存されます。このファイルは、［変更の適用］を初めてクリックしたときに自動的に作成されます。

（注） シグニチャのインポートを試みるときに、それらのシグニチャがすべて展開済みのシグニチャと同じである場合には、［変更の適用］ボタンが無効になります。

変更の破棄

これまでの変更を破棄する場合は、［変更の破棄］をクリックします。

（注） シグニチャのインポートを試みるときに、それらのシグニチャがすべて展開済みのシグニチャと同じである場合には、［変更の破棄］ボタンが無効になります。

シグニチャの編集

選択したシグニチャを編集するには、［シグニチャの編集］ダイアログ内のフィールドを使用します。変更内容はデルタ ファイルに格納されます。このファイルはルータのフラッシュ メモリに保存されます。シグニチャの要素については、次のセクションで説明しています。

このヘルプ トピックでは、ルータで Cisco IOS 12.4(11)T 以降が実行されている場合に表示される［シグニチャの編集］ウィンドウについて説明します。

シグニチャ ID

対象のシグニチャに割り当てられた一意の数値です。Cisco IOS IPS では、この値を使用して特定のシグニチャを識別します。

サブシグニチャ ID

対象のサブシグニチャに割り当てられた一意の数値です。サブシグニチャ ID は、広範にわたるシグニチャのバージョンをさらに細かく特定するために使用されます。

Alert Severity

次のいずれかを選択して、アラートの重大度を分類します。高、中、低、または情報。

Sig Fidelity Rating

シグニチャの信頼度評価は、シグニチャが true positive を生成する確実性を数値で表すために、シグニチャの作成者によって設定される値です。この値は、シグニチャが展開される前に設定され、シグニチャのパフォーマンス データが使用可能な場合に調整できます。

Promiscuous Delta

無差別モードの差分は、ルータが無差別モードで動作しているときに、イベントのリスク評価（RR）から削除される要素です。無差別モードの差分は、システムが無差別モードで展開されている場合に、アラートが生成されるたびに RR から削除されます。

（注） 無差別モードの差分はシグニチャごとに再設定できますが、定義済みの無差別モードの差分設定を変更することはお勧めしません。

Sig Description

シグニチャの説明には、シグニチャの名前とリリース、Cisco セキュリティ センター から入手可能なアラートの意味、ユーザのコメント、およびその他の情報が含まれます。

エンジン

対象のシグニチャに関連付けられているシグニチャ エンジン。一般に使用されるエンジンの 1 つは、Atomic IP という名前です。

［エンジン］ボックスの各フィールドでは、さまざまなタイプのシグニチャ パラメータを調整できます。たとえば、対象のシグニチャが一致してイベントが生成されたときに実行されるアクションを指定したり、このシグニチャに一致するイベントを検査するようレイヤ 4 プロトコルを指定したり、ヘッダー長やサービス タイプなどの IP パラメータを指定したりできます。

Event Counter

［Event Counter］ボックスのコントロールを使用すると、以降のセクションで説明するパラメータを指定できます。

Event Count

アラートが生成される前にイベントが発生する回数。

Event Count Key

イベントの発生回数のカウントに使用される情報のタイプ。たとえば、攻撃者と被害先のアドレスとポートを両方選択した場合、各イベントについてこれら 4 つの情報が得られるごとに、カウントは 1 ずつ増加します。攻撃者のアドレスを選択した場合は、その情報だけが必要となります。

Event Interval

イベントがログに送信される間隔（秒数）。［はい］を選択すると、秒数を入力できる追加のフィールドが表示されます。

Alert Frequency

Alert Frequency パラメータの目的は、ログに書き込まれるアラートのボリュームを減らすことです。

Summary Mode

次の 4 つのモードがあります。［Fire All］、［Fire Once］、［Summarize］、および［Global Summarize］です。［Summary Mode］は現在のアラート ボリュームに合わせて、動的に変更されます。たとえば、シグニチャを［Fire All］に設定しても、一定のしきい値に達すると、要約を開始するようになります。

Summary Key

要約を行うタイミングの決定に使用される情報のタイプ。たとえば、攻撃者と被害先のアドレスとポートを両方選択した場合、各イベントについてこれら 4 つの情報が得られるごとに、要約が行われます。攻撃者のアドレスを選択した場合は、その情報だけが必要となります。

Specify Global Summary Threshold

オプションで、イベントをログに要約するタイミングの決定に使用する数字のしきい値を指定できます。［はい］を選択すると、グローバル要約しきい値と、要約の間隔を指定できます。

ステータス

［ステータス］ボックスで、シグニチャを有効にするか、無効にするか、またはリタイアにするかを指定できます。また、［ステータス］ボックスには、廃止したシグニチャを表示できます。

ファイルの選択

このウィンドウでは、ルータからファイルをロードできます。このウィンドウで表示できるのは DOSFS ファイル システムだけです。

ウィンドウの左側には、拡張可能なツリーが表示されます。このツリーは、シスコ ルータのフラッシュ メモリおよびそのルータに接続されている USB デバイスのディレクトリ システムを表します。

ウィンドウの右側には、ウィンドウの左側で指定されたディレクトリ内にあるファイルおよびディレクトリの名前のリストが表示されます。また、各ファイルのサイズ（バイト単位）と、各ファイルおよびディレクトリの最終修正日時も表示されます。

ウィンドウの右側に表示されたリストで、ロードするファイルを選択できます。ファイル リストの下にある［ファイル名］フィールドには、指定したファイルのフル パスが表示されます。

（注） ルータをプロビジョニングするコンフィギュレーション ファイルには、CCCD ファイルまたは拡張子が .cfg のファイルを選択してください。

名前

ファイルやディレクトリを名前のアルファベット順に並べ替える場合は、［名前］をクリックします。［名前］をもう一度クリックすると、順序が逆になります。

サイズ（バイト）

ファイルとディレクトリをサイズ順に並べ替える場合は、［サイズ（バイト）］をクリックします。ディレクトリのサイズは、空白でなくても常にゼロ バイトと表示されます。［サイズ （バイト）］をもう一度クリックすると、順序が逆になります。

修正時刻

ファイルとディレクトリを修正日時の順に並べ替える場合は、［修正時刻］をクリックします。［修正時刻］をもう一度クリックすると、順序が逆になります。

アクションの割り当て

このウィンドウには、シグニチャが一致したときに実行可能なアクションが表示されます。使用可能なアクションはシグニチャによって異なりますが、最も一般的なアクションは、次のとおりです。

- ［alarm］— アラーム メッセージを生成します。［produce-verbose-alert］と同じです。
- ［deny-attacker-inline］— Cisco IOS IPS システムによって攻撃源とみなされる IP アドレスからのトラフィックをすべて拒否する ACL を作成します。［denyAttackerInline］と同じです。
- ［deny-connection-inline］— この TCP フロー上の特定のパケットおよびそれ以降のパケットをすべて破棄します。［produce-alert］および［denyFlowInline］と同じです。
- ［deny-packet-inline］— このパケットを送信しません（インラインのみ）。［drop］と同じです。
- ［denyAttackerInline］— Cisco IOS IPS システムによって攻撃源とみなされる IP アドレスからのトラフィックをすべて拒否する ACL を作成します。［deny-attacker-inline］と同じです。
- ［denyFlowInline］— 5-tuple（送信元および宛先の IP とポート、および 14 プロトコル）に属する攻撃源とみなされる IP アドレスからのトラフィックをすべて拒否する ACL を作成します。［denyFlowInline］では、［denyAttackerInline］よりも詳細な制御が可能です。［produce-alert］および［deny-connection-inline］と同じです。
- ［drop］— 違反パケットを廃棄します。［deny-attacker-inline］と同じです。
- ［produce-alert］— アラートを生成します。［denyFlowInline］および［deny-connection-inline］と同じです。
- ［produce-verbose-alert］— 違反パケットの符号化されたダンプを含むアラートを生成します。［alarm］と同じです。
- ［reset］— 接続をリセットし、違反パケットを破棄します。［reset-tcp-connection］と同じです。
- ［reset-tcp-connection］— TCP RESETS を送信して TCP フローを終端します。［reset］と同じです。

シグニチャのインポート

IPS をインポートするウィンドウを使用して、PC 上の SDF またはその他のファイルからシグニチャをインポートします。このウィンドウには、使用可能な SDF のシグニチャ、およびそのうちのいずれがルータに展開済みであるかが示されます。

シグニチャのインポート方法

シグニチャをインポートするには、次の手順に従ってください。

ステップ 1　［シグニチャ］ツリー、［選択肢］ドロップダウン リスト、および［条件リスト］ドロップダウン リストを使用して、インポートするシグニチャを表示します。

シグニチャのリストで、インポート*しない*シグニチャの［インポート］チェックボックスの選択を解除します。すべてのシグニチャの［インポート］チェックボックスの選択を解除する場合は、［すべての選択を解除］ボタンをクリックします。すると、このボタンは、［すべて選択］に変わります。

ステップ 2　使用するとルータのパフォーマンスが低下する可能性があるシグニチャのインポートを回避する場合には、［無効として定義されているシグニチャをインポートしない］チェック ボックスを選択します。

ステップ 3　ルータにすでに設定されているシグニチャにインポートしたシグニチャをマージするには、［マージ］ボタンをクリックし、インポートしたシグニチャで置き換えるには、［置換］ボタンをクリックします。

詳細については、「マージ ボタン」と「置換ボタン」を参照してください。

ステップ 4　［IPS の編集］ウィンドウの［変更の適用］ボタンをクリックして、インポートされたシグニチャを展開します。

インポートされたシグニチャは、展開する前に変更できます。インポート対象として設定されている、展開済みのシグニチャと同じシグニチャはインポートされません。すべてのインポートされたシグニチャが展開済みのシグニチャと同じである場合には、［変更の適用］ボタンが無効になります。

シグニチャ ツリー

［シグニチャ］ツリーの説明が必要な場合は、「シグニチャ ツリー」を参照してください。このウィンドウの［シグニチャ］ツリーを使用すると、インポートするシグニチャをカテゴリ別に整理できます。

たとえば、OS カテゴリのシグニチャとサービス カテゴリのシグニチャを追加する場合を考えてみます。その場合は、ツリーの **OS** ブランチを選択します。また、必要に応じて、UNIX ブランチや Windows ブランチなど、それ以外のブランチをツリーから選択します。インポートするシグニチャのタイプが表示されていれば、シグニチャ リスト エリアで選択できます。また、［サービス］ブランチを選択したり、必要に応じて、それ以外のサービス シグニチャを選択したりすることもできます。

選択肢リストおよび条件リスト

［選択肢］リスト ボックスおよび［条件］リスト ボックスを使用すると、表示するシグニチャのタイプに応じてリストの項目にフィルタを適用できます。まず、［選択肢］リストで条件を選択し、次に右側のリスト（［条件］リスト）で条件の値を選択します。

たとえば、［選択肢］リストで［エンジン］を選択すると、［条件］リストのラベルが［エンジン］に変わり、［Atomic.ICMP］や［Service.DNS］などの使用可能なエンジンのいずれかを選択できます。

［Sig ID］または［Sig Name］（シグニチャ名）を選択した場合は、［条件］リストに値を入力する必要があります。

シグニチャ リスト エリア

シグニチャ リストには、［シグニチャ］ツリーで選択した条件に基づいて、SDF で使用可能なシグニチャが表示されます。対象ルータですでに見つかっているシグニチャのテキストは青色です。

シグニチャ リスト エリアには次のカラムがあります。

- ［Sig ID］— このシグニチャに割り当てられた一意の数値です。Cisco IOS IPS では、この値を使用して特定のシグニチャを識別します。
- ［名前］— シグニチャの名前です（たとえば、*FTP Improper Address*）。

- ［重大度］— 高、中、低、または情報。
- ［展開済み］— ルータにシグニチャがすでに展開されている場合は［はい］と表示されます。ルータにシグニチャが展開されていない場合は［いいえ］と表示されます。
- ［インポート］— シグニチャごとにチェック ボックスがあります。シグニチャをインポートする場合は、このチェック ボックスを選択します。

（注）　SDF または IOS-S*xxx*.zip という名前の zip ファイルからインポートされたすべてのシグニチャは、シグニチャ リストに表示できます。シグニチャが異なる名前の zip ファイルからインポートされた場合は、［選択肢］および［条件］ドロップダウン リストで見つかったシグニチャのみが表示されます。

マージ ボタン

インポートするシグニチャとルータにすでに設定されているシグニチャをマージする場合にクリックします。

置換ボタン

ルータにすでに設定されているシグニチャを、インポートするシグニチャに置き換える場合にクリックします。ルータにすでに設定されていても、インポート中のシグニチャのリストに*見つからない*シグニチャには削除マークが付けられ、［IPS の編集］>［シグニチャ］の［削除するシグニチャ］に表示されます。詳細については、「削除するシグニチャ」を参照してください。

シグニチャの追加、編集または複製

このウィンドウには、次の「フィールドの定義」セクションで説明するフィールドと値が表示されます。フィールドは、シグニチャによって異なります。したがって、このリストは、表示される可能性があるすべてのフィールドを網羅しているわけではありません。

フィールドの定義

［シグニチャの追加］、［シグニチャの編集］、［シグニチャの複製］の各ウィンドウには、次のフィールドがあります。

- ［SIGID］— このシグニチャに割り当てられた一意の数値です。Cisco IOS IPS では、この値を使用して特定のシグニチャを識別します。
- ［SigName］— シグニチャに割り当てられた名前です。
- ［SubSig］— このサブシグニチャに割り当てられた一意の数値です。subsig ID は、広範にわたるシグニチャのバージョンをさらに細かく特定するために使用されます。
- ［AlarmInterval］— 一定時間後に発行するようにしたイベントに対する特定の処理方法を指定します。Y 秒のインターバルで X 個までのアラームに抑えるには、［AlarmInterval］を Y、［MinHits］を X に設定します。
- ［AlarmSeverity］— このシグニチャのアラームの重大度です。
- ［AlarmThrottle］— アラームの生成に使用されるテクニックです。
- ［AlarmTraits］— このシグニチャについて詳しく説明するユーザ定義の特性です。
- ［ChokeThreshold］— AlarmThrottle のモードの自動切り替えを起動させる、インターバルごとのアラームのしきい値です。［ChokeThreshold］が定義されている場合、［ThrottleInterval］に設定されている間隔で大量のアラームが発生すると、Cisco IOS IPS によって自動的に AlarmThrottle モードが切り替えられます。
- ［Enabled］— シグニチャが有効かどうかを特定します。Cisco IOS IPS では、シグニチャで指定されたトラフィックから保護するには、そのシグニチャが有効になっていなければなりません。
- ［EventAction］— このシグニチャが生成されたときに Cisco IOS IPS で実行されるアクションです。
- ［FlipAddr］— アラーム メッセージで、送信元と宛先のアドレス、および関連付けられているポートがスワップされる場合は［True］です。スワップされない（デフォルト）の場合は［False］です。
- ［MinHits］— アラーム メッセージが送信される前に発生させる必要のあるシグニチャの最小ヒット数を指定します。ヒットとは、アドレス キーにシグニチャが出現することです。
- ［SigComment］— シグニチャのコメントまたは説明テキストです。
- ［SigVersion］— シグニチャのバージョンです。

- ［ThrottleInterval］— アラーム スロットルのインターバルを定義する秒数です。これを［AlarmThrottle］パラメータと組み合わせて使用して、特別なアラーム リミッタをチューニングします。
- ［WantFrag］—［True］に設定すると、フラグメント化されたパケットのみを検査できます。［False］に設定すると、フラグメント化されていないパケットのみを検査できます。フラグメント化されたパケットとフラグメント化されていないパケットの両方を検査する場合には、［undefined］を選択します。

Cisco セキュリティ センター

Cisco セキュリティ センターでは、新たな脅威に関する情報を提供しており、これらの脅威からネットワークを保護するために使用できる Cisco IOS IPS シグニチャへのリンクが用意されています。シグニチャのレポートとダウンロードには、次のリンクからアクセスできます（ログインが必要です）。

http://tools.cisco.com/MySDN/Intelligence/searchSignatures.x

IPS で用意されているシグニチャ定義ファイル

ルータのメモリで対応可能な限り、できるだけ多くのシグニチャをルータで使用できるようにするため、Cisco CP には次の SDF のいずれかが付属しています。

- 256MB.sdf — 使用可能な RAM 容量が 256MB を超えている場合。256MB.sdf ファイルには、500 個のシグニチャが含まれています。
- 128MB.sdf — 使用可能な RAM 容量が 128 ～ 256MB の場合。128MB.sdf ファイルには、300 個のシグニチャが含まれています。
- attack-drop.sdf — 使用可能な RAM 容量が 127MB 未満の場合。attack-drop.sdf ファイルには、82 個のシグニチャが含まれています。

ルータで Cisco IOS バージョン 12.4(11)T 以降が実行されている場合は、sigv5-SDM-S*xxx*.zip という形式の名前が付けられた SDF ファイル（たとえば、sigv5-SDM-S260.zip）を使用する必要があります。

（注） 256MB.sdf ファイルおよび 128MB.sdf ファイルで使用可能なシグニチャ エンジンをすべて使用できるようにするには、ルータでリリース 12.3(14)T 以降の Cisco IOS が実行されている必要があります。それよりも前にリリースされた Cisco IOS がルータで使用されている場合は、シグニチャ エンジンの一部を使用できません。

ルータのメモリで SDF を使用するには、どの SDF がインストールされているかを確認して、その SDF を使用するように Cisco IOS IPS を設定します。この後の手順は、その方法を示したものです。

メモリ内の SDF ファイルの確認

どの SDF ファイルがルータのメモリにあるかを確認するには、ルータへの Telnet セッションを開いて、**show flash** コマンドを入力します。出力結果は、次のようになります。

```
System flash directory:
File  Length   Name/status
  1   10895320  c1710-k9o3sy-mz.123-8.T.bin
  2   1187840  ips.tar
  3   252103   attack-drop.sdf
  4   1038     home.shtml
  5   1814     sdmconfig-1710.cfg
  6   113152   home.tar
  7   758272   es.tar
  8   818176   common.tar
[14028232 bytes used, 2486836 available, 16515068 total]
16384K bytes of processor board System flash (Read/Write)
```

この例では、attack-drop.sdf というファイルがルータのメモリ内にあります。ディスク ファイル システムを搭載したルータなど、一部のルータでは、**dir** コマンドを実行して、ルータのメモリの内容を表示します。

SDF を使用するように IPS を設定

ルータのメモリで SDF を使用するように Cisco IOS IPS を設定するには、次の手順を実行します。

ステップ 1　［グローバル設定］をクリックします。

ステップ 2　［設定されている SDF の場所］リストで、［追加］をクリックします。

ステップ 3　表示されるダイアログ ボックスで、［フラッシュ上の SDF を指定保存］をクリックして、SDF ファイルの名前を入力します。

ステップ 4　［OK］をクリックして、このダイアログ ボックスを閉じます。

セキュリティ ダッシュボード

セキュリティ ダッシュボードを使用すると、最新のセキュリティ脅威に対応するシグニチャでルータを更新できます。セキュリティ ダッシュボードを使用してシグニチャを展開するには、ルータで Cisco IOS IPS を構成しておく必要があります。

高脅威テーブル

高脅威テーブルには、関連付けられたシグニチャのステータスが展開可能または調査中と示されている場合に、シスコから提供される、最新の高脅威のリストが表示されます。テーブルに表示される一部の高脅威は、ルータに展開できるシグニチャに関連付けられています。ルータですでに見つかっているシグニチャのテキストは青色です。

最新の高脅威のリストを取得するには、［高脅威リストの更新］ボタンをクリックします。

（注） Cisco CP の［更新］ボタンまたはブラウザの［更新］コマンドを使用して高脅威のリストを更新することはできません。

高脅威テーブルには、次のカラムがあります。

- ［デバイス ステータス］— 脅威に関連付けられているシグニチャがルータですでに有効になっているかどうかを示します。［デバイス ステータス］カラムには、次の記号が表示されます。

  シグニチャがルータですでに有効になっています。

  シグニチャがルータで使用可能でないか、使用可能であってもルータで有効になっていません。

- ［Sig ID］— 脅威に関連付けられているシグニチャを識別する一意の番号。
- ［SubSig ID］— サブシグニチャを識別する一意の番号。脅威に関連付けられているシグニチャにサブシグニチャがない場合、［SubSig ID］は 0 です。

- ［名前］— 脅威に与えられた名前。
- ［緊急度］— 脅威のレベルが高（優先メンテナンス）か、または標準（標準メンテナンス）かを示します。
- ［脅威ステータス］— 脅威に関連付けられているシグニチャが使用可能か、またはまだ調査中かを示します。
- ［展開］— 脅威に関連付けられているシグニチャが展開可能となっている場合に選択できる、チェック ボックスがあります。

SDF の選択

［参照］ボタンをクリックして、使用する Cisco IOS SDF ファイルを選択します。Cisco IOS SDF ファイルは、PC 上に配置されている必要があります。ファイル名の形式は、ルータで実行されている Cisco IOS のバージョンによって異なります。

- ルータで 12.4(11)T より前の Cisco IOS イメージが実行されている場合、SDF の名前は IOS-S*xxx*.zip という形式である必要があります。*xxx* は 3 桁の数字を表します。たとえば、Cisco IOS IPS SDF ファイルは IOS-S193.zip という名前になります。
- ルータでバージョン 12.4(11)T 以降の Cisco IOS イメージが実行されている場合、SDF の名前は sigv5-SDM-S*xxx*.zip という形式である必要があります。たとえば、sigv5-SDM-S260.zip のようになります。

選択する Cisco IOS SDF ファイルの場所は、SDF ファイルのロケーション フィールドに表示されます。SDF ファイルのロケーション フィールドは読み取り専用です。

Cisco IOS SDF ファイルを最初にダウンロードした後は、Cisco CP でファイルの場所が記憶されます。次回セキュリティ ダッシュボードをロードするとき、Cisco CP ではファイル名の 3 桁の数字に基づいて、最新の Cisco IOS SDF ファイルが選択されます。

（注） 名前に最も大きい 3 桁の数字が含まれる Cisco IOS SDF ファイルが最新のファイルです。

高脅威テーブルからのシグニチャの展開

高脅威テーブルからシグニチャを展開する前に、次のことを確認してください。

- ルータに Cisco IOS IPS が構成されている。
- PC に最新の Cisco IOS ファイルがダウンロードされている。

高脅威テーブルからシグニチャを展開するには、次の手順に従ってください。

ステップ 1　［高脅威リストの更新］ボタンをクリックして、最新の高脅威リストがあることを確認します。

ステップ 2　［展開］カラムで、高脅威テーブルから展開する各高脅威のシグニチャのチェック ボックスを選択します。

ステータスが［シグニチャ使用可能］となっている高脅威のみを選択できます。［デバイスス テータス］カラム内で赤色のアイコンの付いた使用可能なシグニチャが、自動的に［展開］に設定されます。

ステップ 3　最新のシグニチャ ファイルを使用していることを確認する必要がある場合には、［参照］ボタンをクリックして、最新の Cisco IOS ファイルを選択します。

この操作は、セキュリティ ダッシュボードで前回最新の SDF ファイルを設定してから SDF ファイルの場所を変更した場合、またはファイル名の形式が IOS-S*xxx*.zip（*xxx* は 3 桁の数字）でない場合に、実行する必要があります。

ステップ 4　［シグニチャの展開］ボタンをクリックして、選択したシグニチャをルータに展開します。

選択したシグニチャのいずれかが Cisco IOS ファイルに見つからない場合は、警告が表示されます。ただし、見つかったシグニチャはすべて展開できます。ルータに展開した後、シグニチャは自動的に有効となり、ルータのアクティブなシグニチャ リストに追加されます。

IPS 移行

既存の Cisco IOS IPS 設定があり、それを Cisco IOS 12.4(11)T 以降で使用可能な Cisco IOS IPS に移行する場合は、IPS 移行ウィザードを使用できます。

（注）　バージョン 12.4(11)T 以降の Cisco IOS イメージを使用しているルータで Cisco IOS IPS を使用するには、それ以前のバージョンで作成された設定を移行する必要があります。設定を移行しない場合、設定コマンドは変更されませんが、Cisco IOS IPS は動作しません。

移行プロセスを開始するには［IPS 移行ウィザードの起動］ボタンをクリックします。

移行ウィザード：ようこそ

移行ウィザードの［ようこそ］画面には、このウィザードで実行できるタスクが表示されます。IPS 移行ウィザードを実行しない場合は、［キャンセル］をクリックします。

IPS 移行ウィザードは、ルータで Cisco IOS 12.4(11)T 以降が実行されている場合に使用できます。

移行ウィザード：IOS IPS バックアップ シグニチャ ファイルの選択

バックアップ ファイルには、移行される Cisco IOS IPS 情報が含まれます。これは、attack-drop.sdf や 128MB.sdf などの、シグニチャ定義ファイル（SDF）である場合があります。シグニチャを無効にしたり、特定のシグニチャの属性を変更するなど、シグニチャ情報に変更を加えた場合は、変更の記録が別のファイルに保存されます。Cisco CP を使用して変更を行った場合は、変更内容が sdmips.sdf という名前のファイルに保存されます。このファイルはルータのフラッシュ メモリに保存されます。手動で変更を行った場合は、ファイルに別の名前を付け、バックアップ コピーを PC に保存した可能性があります。

バックアップ ファイルのフィールドの横にある［...］ボタンをクリックすると、ダイアログが表示され、ルータのフラッシュ メモリまたは PC 上でこのバックアップ ファイルを参照できます。

シグニチャ ファイル

このダイアログでは、バックアップのシグニチャ ファイルの場所を指定します。

フラッシュにシグニチャ ファイルを指定

バックアップ シグニチャ ファイルがフラッシュ メモリに保存されている場合は、このフィールドの横にある矢印ボタンをクリックして、ファイルを選択します。

PC にシグニチャ ファイルを指定

バックアップ シグニチャ ファイルが PC に保存されている場合は、このフィールドの横にある［参照］ボタンをクリックして、ファイルに移動します。

Java ヒープ サイズ

Cisco CP では、Java のヒープ サイズが SDM の機能をサポートできるだけの大きさでない場合に、Java ヒープ サイズ ウィンドウが表示されます。次の手順を実行して、ヒープ サイズをウィンドウに表示される値に設定します。

ステップ 1　Cisco CP を終了します。

ステップ 2　［スタート］>［コントロール パネル］>［Java］をクリックします。

ステップ 3　［Java ランタイム設定］ダイアログを開きます。このダイアログの場所は、リリースにより異なります。

a.　［詳細］タブをクリックします。［Java ランタイム設定］ダイアログを見つけて、ステップ 4 に進みます。［詳細］タブからダイアログを使用できない場合は、b. に進みます。

b.　［Java］タブをクリックします。［Java ランタイム設定］ダイアログを見つけます。必要に応じて［表示］ボタンをクリックしてダイアログを表示し、ステップ 4 に進みます。

ステップ 4　［Java ランタイム パラメータ］カラムに、ウィンドウに示された値を入力します。たとえば、ウィンドウに値 `-Xmx256m` を使用する必要があると表示されている場合は、その値を［Java ランタイム パラメータ］カラムに入力します。次の表は、値の例を示しています。

製品名	バージョン	場所	Java ランタイム パラメータ
JRE	1.5.0_08	C:\Program Files\java\jre1.5.0_08	-Xmx256m

ステップ 5　［Java ランタイム設定］ダイアログで［OK］をクリックします。

ステップ 6　Java コントロール パネルで［適用］をクリックし、次に［OK］をクリックします。

ステップ 7　Cisco CP を再起動します。