仮想センサーの設定

すべての IPS デバイスおよびサービス モジュールに、vs0 という名前の基本仮想センサーがあります。IPS アプライアンスまたはサービス モジュールの設定時に、基本の vs0 センサーを設定してインターフェイスを割り当てる必要があります。この割り当てによって、検査するインターフェイスがデバイスに示されます。また、仮想センターには指定できるその他の設定があります。

基本の vs0 仮想センサー以外に、数多くの IPS アプライアンスおよびサービス モジュールで、ユーザ定義の仮想センサーを作成できます。これらの仮想センサーを使用すると、単一の物理センサーが複数のセンサーのように機能できるように、トラフィックごとに別々のポリシーを作成できます。仮想センサーは、シグニチャ エンジンおよびイベント アクション フィルタを適用するための検知インターフェイスと設定ポリシーの論理グループです。

この章は次のトピックで構成されています。

仮想センサーについて

センサーは1つまたは多数のモニタ対象データ ストリームからのデータ入力を受信できます。これらのモニタ対象データ ストリームは、物理インターフェイス ポートまたは仮想インターフェイス ポートのどちらでも構いません。たとえば、単一のセンサーでファイアウォールの前からのトラフィック、ファイアウォールの後ろからのトラフィック、またはファイアウォールの前後からのトラフィックを同時にモニタできます。単一のセンサーで1つ以上のデータ ストリームをモニタできます。この場合、単一のセンサー ポリシーまたは設定がすべてのモニタ対象データストリームに適用されます。

仮想センサーでは、特定のトラフィック フィードに適用するための、別々のポリシーを作成できます。たとえば、データセンターのポリシーを作成し、キャンパス ネットワークに別のまったく異なるポリシーを作成して、両方のポリシーを同じハードウェア デバイスで実行する場合は、別々の仮想センサーを設定してこれらのポリシーを実装できます。

仮想センサーに対して次のポリシーおよび設定を別々に設定します。

- シグニチャおよびシグニチャ設定（[IPS] のポリシー > [Signatures] フォルダ）
- イベント アクション ポリシー（[IPS] のポリシー > [Event Actions] フォルダ）
- 異常検出ポリシー（[IPS] > [Anomaly Detection] ポリシー）および異常検出モード（[Virtual Sensors] ポリシー）
- 仮想センサーでモニタする無差別インターフェイス、インライン インターフェイス ペア、インライン VLAN ペア、インライン VLAN グループ、または無差別 VLAN グループ

（注） パケットが複数の仮想センサーで処理されることはありません。つまり、同じ物理または論理インターフェイスを複数のセンサーに割り当てることはできません。どの仮想センサーにも割り当てられていないインターフェイス、インライン インターフェイス ペア、インライン VLAN ペア、および VLAN グループからのパケットは、[インターフェイス（Interfaces）] ポリシーで定義したインラインバイパス設定に従って破棄されます。

- インライン TCP セッション トラッキングおよびノーマライザ モード（[Virtual Sensors] ポリシー）

（注） シグネチャ、イベントアクション、または異常検出のために IPS デバイスでポリシーインスタンスを作成し、そのデバイスのどの仮想センサーにも割り当てない場合（つまり、そのポリシーインスタンスを使用しない場合）、そのポリシーインスタンスは展開中に Cisco Security Manager によって削除されます。

他のポリシーおよび設定はすべて、仮想センサーをホストする親デバイス上で設定します。たとえば、グローバル相関を使用する場合、親デバイスでグローバル相関を設定して、仮想センサーでその設定を共有します。

1 台のアプライアンスに最大 4 つの仮想センサーを設定できますが、ユーザ定義の仮想センサーは 3 つしか追加できません。最初の仮想センサーである vs0 は基本センサーであり、これは削除できません。Security Manager では、仮想センサーは次のように表示されます。

- デバイス ビューのデバイス セレクタには親デバイスが含まれており、これが基本仮想センサー vs0 を兼ねています。このデバイスを選択してすべてのデバイスレベル ポリシーを設定し、[Virtual Sensors] ポリシーで仮想センサーを作成します。
- ユーザ定義の仮想センサーもまた、デバイス ビューのデバイス セレクタに表示されます。リアルデバイスの表示名が、仮想センサー名の先頭に追加されます。その結果、通常は仮想センサーが存在する親（リアル）デバイスの横に仮想センサーが表示されます。たとえば、「bob」という名前のホスト（リアルデバイス）では、「vs1」という名前の仮想センサーは「bob_vs1」としてデバイスリストに表示されます。

仮想センサーのシグニチャ、異常検出、およびイベントアクションポリシーを設定するには、デバイスセレクタでその仮想センサーを選択する必要があります。親デバイスを選択してもこれらのポリシーは設定できません。親デバイスのポリシーは、vs0 基本センサー用です。

ここでは、仮想センサーについて詳しく説明します。

仮想化の利点および制約事項

仮想センサーを使用することの利点は、1 台のアプライアンスで複数の仮想センサーを操作する一方で、シグニチャの動作およびトラフィック フィードに関して個々の仮想センサーをそれぞれ異なるように設定できることです。たとえば、データセンターのポリシーを作成し、キャンパス ネットワークに別のまったく異なるポリシーを作成して、両方のポリシーを同じハードウェア デバイスで実行する場合は、別々の仮想センサーを設定してこれらのポリシーを実装できます。

仮想化には次の利点があります。

- 個々のトラフィック セットにそれぞれ異なる設定を適用できます。
- IP スペースが重複している 2 つのネットワークを 1 つのセンサーでモニタできます。
- ファイアウォールまたは NAT デバイスの内側と外側の両方をモニタできます。

仮想化には次の制約事項があります。

- 非対称トラフィックの両側を同じ仮想センサーに割り当てる必要があります。
- VACL キャプチャまたは SPAN（無差別モニタリング）の使用は、VLAN タギングに関して矛盾しており、これによって VLAN グループの問題が発生します。
  - Cisco IOS ソフトウェアを使用している場合、VACL キャプチャ ポートまたは SPAN ターゲットは、トランキング用に設定されていても、常にタグ付きパケットを受信するわけではありません。
  - MSFC を使用している場合、学習したルートの高速パス スイッチングによって、VACL キャプチャおよび SPAN の動作が変わります。

- 固定ストアが制限されます。
- すべての IPS センサーで複数の仮想センサーがサポートされているわけではありません。[Virtual Sensors] ポリシーはすべての IPS アプライアンスおよびサービス モジュールで表示されますが、これは、インターフェイスを基本の vs0 センサーに割り当てるために、このポリシーを使用する必要があるためです。ポリシーの [Add] ボタンがデバイスに対してディセーブルであり、ユーザ定義の仮想センサーを設定していない場合、そのデバイスでは仮想化がサポートされません。仮想化がサポートされていないデバイスの例として、Cisco IPS 4215、NM-CIDS、AIM-IPS、NME-IPS、および AIP-SSC を挙げることができます。IDSM2 では仮想化はサポートされていますが、VLAN グループとインラインインターフェイス ペアはサポートされません。
- IPS 6.0+ ソフトウェアを使用する必要があります。古いソフトウェア バージョンでは仮想化がサポートされていません。
- Cisco IOS IPS デバイスでは仮想化がサポートされていません。[IPS] > [インターフェイス ルール（Interface Rules）] ポリシーを使用して、IPS でモニターする必要があるインターフェイスを指定します。

仮想化には次のトラフィック キャプチャ要件があります。

- 仮想センサーで 802.1q ヘッダーを含むトラフィックを受信する必要があります（キャプチャ ポートのネイティブ VLAN 上のトラフィック以外）。
- センサーで、指定したセンサーの同じ仮想センサーに含まれる同じ VLAN グループの両方向のトラフィックをモニタする必要があります。

関連項目

- 仮想センサーについて （1 ページ）
- 仮想センサーの定義 （7 ページ）

インライン TCP セッション トラッキング モード

インラインでのパケット変更を選択している場合、ノーマライザエンジンでは、ストリームからのパケットを2回認識すると、ストリームの状態を適切に追跡できません。このような場合は、ストリームが頻繁にドロップされます。この状況は、ストリームが、IPS によってモニタされている複数の VLAN またはインターフェイスを介してルーティングされている場合に、最もよく発生します。また、いずれかの方向のトラフィックがそれぞれ異なる VLAN またはインターフェイスから受信された場合に、ストリームを適切に追跡するために非対称トラフィックをマージできるようにする必要があり、これにより、状況がより複雑化します。

この状況を処理するために、ストリームが別々のインターフェイスまたはVLAN（またはVLAN ペアのサブインターフェイス）で受信された場合には、これらを一意のストリームとして認識するように、モードを設定できます。

次のインライン TCP セッション トラッキング モードが適用されます。

- [インターフェイスおよびVLAN（Interface and VLAN）]：同じ VLAN（またはインライン VLAN ペア）内および同じインターフェイス上で同じセッションキー（AaBb）を持つすべてのパケットは、同じセッションに属します。同じキーを持ち、VLANが異なるパケットは、別々に追跡されます。
- [VLANのみ（VLAN Only）]：同じ VLAN（またはインライン VLAN ペア）内で同じセッションキー（AaBb）を持つすべてのパケットは、インターフェイスにかかわらず同じセッションに属します。同じキーを持ち、VLANが異なるパケットは、別々に追跡されます。
- [仮想センサー（Virtual Sensor）]：仮想センサー内で同じセッションキー（AaBb）を持つすべてのパケットは、同じセッションに属します。これがデフォルトであり、ほとんどの場合、最良のオプションです。

仮想センサーの定義 （7 ページ）で示すように、インライン TCP セッション トラッキング モードは、仮想センサーのプロパティとして設定します。

ノーマライザ モードについて

ノーマライザ モードは、センサーがインライン モードで動作している場合にだけ適用されます。デフォルトは [Strict Evasion Protection] であり、これは、TCP ステートとシーケンスのトラッキングが完全に強制されることを意味します。ノーマライザによって、重複パケット、変更されたパケット、順序が正しくないパケットなどの検査が強制されます。このことは、攻撃者が IPS を回避することを阻止するのに役立ちます。

非対称モードでは、ノーマライザのチェックの大部分がディセーブルになります。非対称モードはストリーム全体を検査できない場合にだけ使用してください。この状況では、攻撃者が IPS を回避できるためです。

仮想センサーの定義 （7 ページ）で示すように、ノーマライザ モードは、仮想センサーのプロパティとして設定します。

仮想センサーへのインターフェイスの割り当て

IPS センサーは、仮想センサーに割り当てられたインターフェイス、インターフェイス ペア、または VLAN ペアを通過するトラフィックをモニタします。

次のタイプの 1 つ以上のインターフェイスを仮想センサーに割り当てることができます。

- 無差別インターフェイス：VLAN グループがなく、インライン インターフェイス ペアに含まれない物理インターフェイス。
- インライン インターフェイス ペア：2 つの物理インターフェイスからなる論理インターフェイス。
- インライン VLAN ペア：2 つの VLAN からなる論理インターフェイス。
- 無差別 VLAN グループ：物理インターフェイス上のサブインターフェイスに割り当てられている VLAN グループ。

物理インターフェイスは、インライン インターフェイスまたは VLAN ペアにはまだ使用できません。同じ無差別インターフェイスに多数の無差別VLAN グループを設定できますが、VLAN を重複して割り当てることはできません。VLAN グループを無差別インターフェイスに割り当てると、このインターフェイスは単なる無差別インターフェイスではなくなり、無差別VLAN グループにだけ使用できるようになります。

- インライン VLAN グループ：インライン インターフェイス ペアのサブインターフェイスに割り当てられている VLAN グループ。

同じインライン インターフェイス ペアに多数のインライン VLAN グループを設定できますが、VLAN を重複して割り当てることはできません。VLAN グループをインライン インターフェイス ペアに割り当てると、このインターフェイス ペアは単なるインライン インターフェイス ペアではなくなり、インライン VLAN グループにだけ使用できるようになります。

VLAN グループをインライン VLAN ペアに割り当てることはできません。

インターフェイスを仮想センサーに割り当てる前に、これらを設定する必要があります。これらすべてのタイプのインターフェイスの設定については、インターフェイスの設定を参照してください。インターフェイスを仮想センサーに割り当てる方法の詳細については、仮想センサーの定義 （7 ページ）を参照してください。

デバイスに対する仮想センサーの識別

IPS アプライアンスまたはサービス モジュールでユーザ定義の仮想センサーを設定すると、その仮想センサーはデバイス ビューのデバイス セレクタに表示されます。

通常、仮想センサーの表示名は、device-name_virtual-sensor-name の形式になります。ここで、device-name は親デバイスの名前、virtual-sensor-name は仮想センサーの名前です。たとえば、デバイス 10.100.10.10 上の仮想センサー vs1 は 10.100.10.10_vs1 になります。

このため、通常、デバイスセレクタ内で、デバイスの仮想センサーは親デバイスのすぐあとに表示されます。ただし、仮想センサーの表示名は、デバイスのプロパティを編集して変更できます。デフォルト名を変更した場合、デバイスセレクタ内で、仮想センサーが親デバイスの近くに表示されなくなる可能性があります。

次の方法を使用すると、デバイスに定義されている仮想センサーを識別したり、仮想センサーの親デバイスを識別したりできます。

- IPS デバイスに定義されている仮想センサーのリストを表示するには、そのデバイスの [仮想センサー（Virtual Sensors）] ポリシーを選択します。テーブルに、基本の vs0 センサーを含むすべての仮想センサーが表示されます。vs0 センサーはデバイス セレクタに単独では表示されないことに注意してください。このセンサーは親デバイス自体によって示されます。

仮想センサーの表示名を根本的に変更しないかぎり、仮想センサー名と親デバイスの表示名は、デバイスセレクタ内で仮想センサーを見つけるのに役立ちます。

- 仮想センサーのホストである IPS デバイスを判断するには、デバイスセレクタで仮想センサーを右クリックして [デバイスのプロパティ（Device Properties）] を選択します。[General]

タブにある表示専用の [Hostname] フィールドに、ホスト デバイスの表示名と、デバイスに定義されている仮想センサー名が表示されます。

仮想センサーの定義

[Virtual Sensors] ポリシーを使用して、Cisco IPS デバイスに仮想センサーを設定します。IPS デバイスで複数の仮想センサーがサポートされていない場合でも、このポリシーを使用してインターフェイスを基本センサー vs0 に割り当て、その仮想センサーに関連付けられているプロパティを設定する必要があります。

ヒント　Cisco IOS IPS デバイスの場合、**[IPS] > [インターフェイスルール（Interface Rules）]** ポリシーで IPS が検査するインターフェイスを設定します。IOS IPS デバイスでは仮想センサーは設定できません。

はじめる前に

インライン インターフェイス ペア、インライン VLAN ペア、無差別 VLAN グループ、およびインライン VLAN グループなどのインターフェイスをセンサーに設定します。インターフェイスは、仮想センサーに割り当てる前に設定する必要があります。インターフェイス、インターフェイスのモード、およびこれらの設定方法については、IPS デバイスインターフェイスの管理を参照してください。

関連項目

- インターフェイスについて
- インターフェイス モードについて
- 仮想化の利点および制約事項　（3 ページ）
- インライン TCP セッション トラッキング モード　（4 ページ）
- インライン TCP セッション トラッキング モード　（4 ページ）
- ノーマライザ モードについて　（5 ページ）
- 仮想センサーへのインターフェイスの割り当て　（5 ページ）
- デバイスに対する仮想センサーの識別　（6 ページ）
- 仮想センサーのポリシーの編集　（12 ページ）

ステップ 1　（デバイス ビューだけ）ポリシーセレクタから [仮想センサー（Virtual Sensors）] を選択して、[仮想センサー（Virtual Sensors）] ポリシーを開きます。

削除できない基本の vs0 センサーを含むすべての既存仮想センサーがポリシーに一覧表示されます。各センサーの情報には、センサーに割り当てられているインターフェイス、異常検出モード、インライン TCP

トラッキング モード、ノーマライザ モードおよび説明が表示されます（ある場合）。[Assignments] セルが空白の場合、その仮想センサーにはインターフェイスが割り当てられていません。このことは、仮想センサーでトラフィックを分析できないことを意味します。

ステップ 2 次のいずれかを実行します。

- 仮想センサーを追加するには、[行の追加（Add Row）] ボタンをクリックします。[Add Virtual Sensor] ダイアログボックスが開きます。

最大で 3 つのセンサーを追加できます。デバイスでは、基本の vs0 センサーを含めて 4 つの仮想センサーがサポートされます。[Add Row] ボタンがディセーブルになっている場合は、センサーを最大数まで設定してあるか、またはデバイスで複数の仮想センサーがサポートされていないかのいずれかです。

- 仮想センサーを編集するには、仮想センサーを選択し、[行の編集（Edit Row）] ボタンをクリックします。[Edit Virtual Sensor] ダイアログボックスが開きます。

ヒント また、仮想センサーを選択して [行の削除（Delete Row）] ボタンをクリックすると、その仮想センサーを削除できます。基本の vs0 センサーは削除できません。仮想センサーを削除する方法の詳細については、仮想センサーの削除 （12 ページ）を参照してください。

ステップ 3 [Add Virtual Sensor]/[Edit Virtual Sensor] ダイアログボックスで、少なくとも次のオプションを設定します。その他のオプションについては、たいていの場合、デフォルトが適切です。使用可能なすべてのオプションの詳細については、仮想センサー ダイアログボックス （9 ページ）を参照してください。

- [Virtual Sensor Name]：仮想センサーの名前。仮想センサー名には、最大 64 文字を使用できますが、スペースは使用できません。
- [Interface Assignments]（[Available]、[Assigned] リスト）：この仮想センターで使用する無差別インターフェイス、インライン インターフェイス ペア、インライン VLAN ペア、無差別 VLAN グループ、またはインライン VLAN グループ。使用可能なインターフェイスのリストに表示されるのは、インターフェイス ポリシーに設定されているインターフェイスと、まだ別の仮想センサーに割り当てられていないインターフェイスだけです。
  - インターフェイスを割り当てるには、使用可能リストでインターフェイスを選択し、[>>] をクリックします。
  - 割り当てを解除するには、割り当て済みリストでインターフェイスを選択し、[<<] をクリックします。インターフェイスを別の仮想センサーに割り当てるには、事前に割り当てを解除する必要があります。

ヒント：特定のインターフェイスの内容（たとえば、モードや割り当てられている VLAN など）がわからない場合は、ダイアログボックスを閉じて [インターフェイス（Interfaces）] ポリシーに移動し、さまざまなタブを確認します。

ステップ 4 [OK] をクリックして変更を保存し、[仮想センサー（Virtual Sensors）] ポリシーに追加します。

ステップ 5 [保存（Save）] をクリックして、[仮想センサー（Virtual Sensors）] ポリシーを保存します。

ステップ 6 新しい仮想センサーを作成した場合、新しい仮想センサーがデバイス ビューのデバイス セレクタに表示されるように、変更内容をデータベースに送信する必要があります。

- Workflow 以外のモード：[ファイル（File）] > [送信（Submit）] を選択します。
- Workflow モード：[アクティビティ（Activities）] > [アクティビティの承認（Approve Activity）] を選択するか、アクティビティ承認者で操作している場合は [アクティビティ（Activities）] > [アクティビティの送信（Submit Activity）] を選択します。アクティビティは、仮想センサーがデバイス セレクタに表示される前に承認されている必要があります。

（注） デバイスセレクタでは、リアルデバイスの表示名が、仮想センサー名の先頭に追加されます。その結果、通常は仮想センサーが存在する親（リアル）デバイスの横に仮想センサーが表示されます。たとえば、「bob」という名前のホスト（リアルデバイス）では、「vs1」という名前の仮想センサーは「bob_vs1」としてデバイスリストに表示されます。

ステップ 7 仮想センサーに関連付けるポリシーを設定するには、デバイス ビューのデバイス セレクタでそのポリシーを選択します。これで、関連付けるポリシーを設定できます。次のトピックを参照してください。

- IPS シグニチャの定義
- イベント アクション ルールの設定
- 異常検出シグニチャの設定

仮想センサー ダイアログボックス

[Add Virtual Sensor]/[Edit Virtual Sensor] ダイアログボックスを使用して、仮想センサーのプロパティを設定します。

ナビゲーション パス

（デバイス ビューだけ）ポリシーセレクタから [仮想センサー（Virtual Sensors）] を選択します。[行の追加（Add Row）] ボタンをクリックするか、既存の仮想センサーを選択して [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- 仮想センサーの定義 （7 ページ）
- 仮想化の利点および制約事項 （3 ページ）
- 仮想センサーへのインターフェイスの割り当て （5 ページ）
- IPS デバイスインターフェイスの管理
- インターフェイスについて
- インターフェイス モードについて

フィールド リファレンス

表 *1 : [Add Virtual Sensor]/[Edit Virtual Sensor]* ダイアログボックス

要素	説明
Virtual Sensor Name	仮想センサーの名前。仮想センサー名には、最大64文字を使用できますが、スペースは使用できません。デフォルトの仮想センサーの名前は **vs0** です。 この名前は、仮想センサーを作成したあとには変更できません。仮想センサー名を変更するには、センサーを削除してから、目的の名前で新しいセンサーを作成します。すでにセンサーのローカル ポリシー（つまり、シグニチャ、イベント アクション、および異常検出ポリシー）を設定してある場合は、最初にポリシーを共有ポリシーとして保存し、センサーを削除して、新しいセンサーを作成してから、共有ポリシーを新しい仮想センサーに割り当てます。ローカル ポリシーから共有ポリシーを作成する方法の詳細については、ローカル ポリシーの共有を参照してください。
Interface Assignments （[Available]、[Assigned]）	この仮想センターで使用する無差別インターフェイス、インライン インターフェイス ペア、インライン VLAN ペア、無差別 VLAN グループ、またはインライン VLAN グループ。使用可能なインターフェイスのリストに表示されるのは、インターフェイス ポリシーに設定されているインターフェイスと、まだ別の仮想センサーに割り当てられていないインターフェイスだけです。 • インターフェイスを割り当てるには、使用可能リストでインターフェイスを選択し、[>>] をクリックします。 • 割り当てを解除するには、割り当て済みリストでインターフェイスを選択し、[<<] をクリックします。インターフェイスを別の仮想センサーに割り当てるには、事前に割り当てを解除する必要があります。 **ヒント** 特定のインターフェイスの内容（たとえば、そのモードや割り当てられている VLAN など）がわからない場合は、ダイアログボックスを閉じて [Interfaces] ポリシーに移動し、それぞれのタブを確認します。
Anomaly Detection Mode	この仮想センサーに対する異常検出ポリシーの動作モード：[Detect]、[Inactive]、[Learn]。デフォルトの通常の動作モードは [Detect] です。ただし、非対称ノーマライザ モードを使用している場合は、異常検出モードを非アクティブに設定する必要がある場合があります。これらのモードの詳細については、異常検出モードを参照してください。

要素	説明
インライン TCP セッション トラッキング モード	同じストリームが複数回センサーを通過した場合に、同じストリームに対するビューを複数に分けるために使用されるモード。デフォルト モードは[Virtual Sensor] です。詳細については、インライン TCP セッション トラッキング モード （4 ページ）を参照してください。次のいずれかを選択します。 • [Interface and VLAN]：同じ VLAN（またはインライン VLAN ペア）内および同じインターフェイス上で同じセッション キー（AaBb）を持つすべてのパケットは、同じセッションに属しています。同じキーを持ち、VLAN が異なるパケットは、別々に追跡されます。 • [VLAN Only]：同じ VLAN（またはインライン VLAN ペア）内で同じセッション キー（AaBb）を持つすべてのパケットは、インターフェイスにかかわらず同じセッションに属しています。同じキーを持ち、VLAN が異なるパケットは、別々に追跡されます。 • [Virtual Sensor]：仮想センサー内で同じセッション キー（AaBb）を持つすべてのパケットは、同じセッションに属しています。
Normalizer Mode	トラフィック検査に必要なノーマライザ モードのタイプ。詳細については、ノーマライザ モードについて （5 ページ）を参照してください。 • [Strict Evasion Protection]：（デフォルト）何らかの理由でパケットが失われた場合、失われたパケット以降のすべてのパケットが処理されなくなります。[Strict Evasion Protection] を指定すると、TCP ステートとシーケンスのトラッキングの完全な施行が提供されます。 パケットの順序が正しくないか、またはパケットが失われていると、ノーマライザ エンジンのシグニチャ 1300 または 1330 が起動する場合があります。この処理によって状況の修正が試行されますが、結果として接続が拒否されることがあります。 • [Asymmetric Mode Protection]：双方向トラフィック フローのいずれかの方向だけをモニタできます。[Asymmetric Mode Protection] を指定すると、TCP レイヤでの回避防止が緩和されます。 Asymmetric モードの場合、センサーは状態をフローと同期し、双方向を必要としないエンジンの検査を継続します。完全な保護には双方向のトラフィックを確認する必要があるため、Asymmetric モードではセキュリティが低下します。
説明	仮想センサーの説明。

仮想センサーのポリシーの編集

仮想センサーには 2 つのタイプのポリシーがあります。1 つは仮想センサーのプロパティで、もう 1 つは仮想センサーに割り当てられているポリシーです。それぞれ異なる方法を使用して、これらの項目を編集します。

- 仮想センサーのプロパティを編集するには、デバイスビューのデバイスセレクタで仮想センサーの親デバイスを選択します。次に、[仮想センサー（Virtual Sensors）]ポリシーを選択します。テーブル内で仮想センターを選択して、[行の編集（Edit Row）]ボタンをクリックできます。

[Virtual Sensors] ポリシーを使用すると、センサーに割り当てられているインターフェイス、異常検出モード、インライン TCP セッション トラッキング モードおよびノーマライザ モードを変更できます。詳細は、次のトピックを参照してください。

- 仮想センサーの定義　（7 ページ）
- 仮想センサー ダイアログボックス　（9 ページ）

- 仮想センサーに割り当てられているポリシーを編集するには、デバイス ビューのデバイス セレクタで仮想センサーを選択します。仮想センサーの名前は、device-name_virtual-sensor-name の形式になります。device-name は親デバイスの名前、virtual-sensor-name は仮想センサーの名前です。たとえば、デバイス 10.100.10.10 上の仮想センサー vs1 は 10.100.10.10_vs1 になります。

（注）　基本仮想センサー vs0 は、親デバイスに統合されており、デバイス セレクタに単独では表示されません。基本仮想センサーを設定するには、親デバイスを選択します。

次に、ポリシーセレクタでポリシーを選択して、設定します。詳細は、次のトピックを参照してください。

- IPS シグニチャの定義
- イベント アクション ルールの設定
- 異常検出の設定

その他のすべてのポリシーは親デバイスで設定します。設定は、そのデバイスに設定されているすべての仮想センサーに適用されます。

仮想センサーの削除

仮想センサーはデバイス ビューのデバイス セレクタに表示されます。ただし、他のデバイスに使用するコマンドと同じコマンドを使用しても、セレクタから仮想センサーを削除できませ

ん。代わりに、親デバイス（仮想センサーが定義されているデバイス）の [Virtual Sensors] ポリシーから仮想センサーを削除する必要があります。次の手順では、ユーザ定義の仮想センサーを削除する方法について説明します。

ヒント　基本仮想センサー vs0 は、デバイス セレクタには表示されません。代わりに、親の IPS センサーによって示されます。つまり、このセンサーが基本の IPS デバイスと見なされます。基本の vs0 センサーを削除するには、インベントリからデバイス全体を削除します。インベントリからデバイスを削除する方法の詳細については、Security Manager インベントリからのデバイスの削除を参照してください。

はじめる前に

仮想センサーを削除する場合は、シグニチャ、イベントアクション、および異常検出ポリシーなど、そのセンサーに定義されているポリシーも削除します。デフォルト以外のローカルポリシーを設定しており、他の仮想センサーで使用できるようにこれらを保持する場合は、最初にローカルポリシーを共有ポリシーに変換する必要があります。これで、仮想センサーを削除したあと、ポリシーは未割り当ての共有ポリシーとして存続するようになります。このあと、このポリシーを別の仮想センサーに割り当てることができます。ローカルポリシーから共有ポリシーを作成する方法の詳細については、ローカル ポリシーの共有を参照してください。

単に仮想センサーの名前を変更する手段として仮想センサーを削除する場合は、この方法を使用するのが最適です。仮想センサーの名前は変更できないため、これを削除してから、目的の名前で新しい仮想センサーを作成する必要があります。共有ポリシーを作成した場合は、これらの共有ポリシーを新しいセンサーに割り当てることができ、このセンサーは古い名前で持っていた設定と同じ設定を持つことになります。

ステップ 1　（デバイス ビューだけ）ポリシーセレクタから [仮想センサー（Virtual Sensors）] を選択して、[仮想センサー（Virtual Sensors）] ポリシーを開きます。

ステップ 2　削除するユーザー定義の仮想センサーを選択し、[行の削除（Delete Row）] ボタンをクリックします。

ステップ 3　2 段階で確認が要求されます。最初に、ポリシーを保存してポリシーとデバイスを同期させておく必要があることを示す警告が表示されます。[OK] をクリックして続行すると、ノードを削除するかどうかの確認が求められます。

削除を確定すると、ポリシーとデバイスセレクタの両方から仮想センサーが削除されます。デバイス ビューが更新され、仮想センサーがデバイス リストに表示されなくなるまでに、しばらく時間がかかります。

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。