CHAPTER 8

ポリシーの設定

（注） IPS SSP を搭載した Cisco ASA 5585-X は、現在、Cisco IPS 7.1 をサポートする唯一のプラットフォームです。他の Cisco IPS センサーは、いずれも現在 IPS 7.1 をサポートしていません。

（注） IPS SSP を搭載した Cisco ASA 5585-X は、ASA 8.2(4.4) 以降および ASA 8.4(2) 以降でサポートされています。ASA 8.3(*x*) ではサポートされていません。

この章では、IPS ポリシーと、仮想センサーを設定する方法について説明します。内容は次のとおりです。

セキュリティ ポリシーの概要

（注） AIM IPS、AIP SSC-5、および NME IPS は、複数のポリシーの適用をサポートしていません。

複数のセキュリティ ポリシーを作成し、個々の仮想センサーに適用することができます。セキュリティ ポリシーは、シグニチャ定義ポリシー、イベント アクション規則ポリシー、および異常検出ポリシーで構成されます。Cisco IPS には、デフォルトのシグニチャ定義（sig0）、デフォルトのイベント アクション規則ポリシー（rules0）、およびデフォルトの異常検出ポリシー（ad0）が含まれています。仮想センサーにデフォルトのポリシーを割り当てることもできれば、新しいポリシーを作成することも

可能です。複数のセキュリティ ポリシーを使用することにより、さまざまな要件に基づいてセキュリティ ポリシーを作成し、これらのカスタマイズしたポリシーを、VLAN または物理インターフェイスごとに適用できます。

IPS ポリシーのコンポーネント

ここでは、IPS ポリシーのさまざまなコンポーネントについて説明します。内容は次のとおりです。

分析エンジンの概要

分析エンジンは、パケット分析とアラート検出を実行します。指定したインターフェイスを流れるトラフィックをモニタします。

仮想センサーは分析エンジンで作成します。各仮想センサーには一意の名前が設定され、インターフェイスのリスト、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 グループが関連付けられます。定義の順序付けに関する問題を避けるため、割り当てでは衝突や重なりは許可されません。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 グループを特定の仮想センサーに割り当て、パケットが複数の仮想センサーで処理されないようにします。各仮想センサーは、明確に名前が設定されたシグニチャ定義、イベント アクション規則、および異常検出設定にも関連付けられます。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、インライン バイパス設定に従って廃棄されます。

（注）　Cisco IPS では、5 個以上の仮想センサーはサポートされません。デフォルトの仮想センサー vs0 は削除できません。

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。

仮想センサーは、複数の設定ポリシーで定義されたデータを集めたものです。仮想センサーは、インターフェイス コンポーネントで定義されたパケットの集合に適用されます。

1 つの仮想センサーは複数のセグメントをモニタでき、1 つの物理センサーの中の仮想センサーごとに異なるポリシーまたは設定を適用できます。分析するモニタ対象セグメントごとに異なるポリシーを設定できます。また、同じポリシーインタンス（たとえば sig0、rules0、または ad0）を、異なる仮想センサーに適用することもできます。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 グループを仮想センサーに割り当てることができます。

（注） デフォルトの仮想センサーは vs0 です。デフォルトの仮想センサーは削除できません。インターフェイス リスト、異常検出動作モード、インライン TCP セッション トラッキング モード、および仮想センサーの記述は、デフォルトの仮想センサーについて変更できる唯一の設定です。シグニチャ定義、イベント アクション規則、異常検出ポリシーは変更できません。

（注） IPS SSP を搭載した Cisco ASA 5585-X は、インライン TCP セッション トラッキング モードをサポートしていません。

仮想化の利点および制約事項

（注） AIM IPS、AIP SSC-5、および NME IPS では仮想化がサポートされていません。

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。

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。

次のセンサーは仮想化をサポートしています。

- AIP SSM

- IPS 4240
- IPS 4255
- IPS 4260
- IPS 4270-20
- IPS SSP

IDSM2 では、インライン インターフェイス ペア上の VLAN グループを除き、仮想化がサポートされています。

（注）　IPS SSP を搭載した Cisco ASA 5585-X は、現在、Cisco IPS 7.1 をサポートする唯一のプラットフォームです。他の Cisco IPS センサーは、いずれも現在 IPS 7.1 をサポートしていません。

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：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 だけ：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。
- 仮想センサー：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。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。

（注）　IPS SSP を搭載した Cisco ASA 5585-X は、インライン TCP セッション トラッキング モードをサポートしていません。

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。

（注）　IPS SSP を搭載した Cisco ASA 5585-X は、ノーマライザ モードをサポートしていません。

イベント アクション オーバーライドの概要

イベント アクション オーバーライドを追加すると、イベントのリスク レーティングに基づいて、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。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しないで、グローバルにイベント アクションを追加する方法です。各イベント アクションには、関連付けられたリスク レーティング範囲があります。シグニチャ イベントが発生し、そのイベントのリスク レーティングがイベント アクションの範囲内に入っていた場合、そのアクションがイベントに追加されます。たとえば、リスク レーティングが 85 以上のイベントで SNMP トラップを生成させる場合、Request SNMP Trap のリスク レーティング範囲を 85 ～ 100 に設定します。アクション オーバーライドを使用しない場合は、イベント アクション オーバーライド コンポーネント全体をディセーブルにします。

（注）　接続ブロックとネットワーク ブロックは、適応型セキュリティ アプライアンスではサポートされていません。適応型セキュリティ アプライアンスは、追加の接続情報があるホスト ブロックだけをサポートします。

リスク レーティングの計算

リスク レーティング（RR）は 0 ～ 100 の範囲の値であり、ネットワーク上の特定のイベントに関係するリスクの数値による定量化を表します。計算では、攻撃対象（たとえば特定のサーバ）のネットワーク資産の価値が考慮されるため、攻撃重大度レーティングとシグニチャ忠実度レーティングを使用してシグニチャごとに設定され、ターゲット価値レーティングを使用してサーバごとに設定されます。リスク レーティングは、いくつかのコンポーネントから計算され、そのうちの一部は設定、収集、計算で得られます。

（注）　リスク レーティングは、シグニチャではなくアラートに関連付けられます。

リスク レーティングを使用すると、注意が必要なアラートに優先順位を付けることができます。これらのリスク レーティング要因では、攻撃が成功した場合の重大度、シグニチャの忠実度、グローバル相関データから得た攻撃者の評判スコア、およびターゲット ホストの各自にとっての全体的な価値が考慮されます。リスク レーティングは evIdsAlert で報告されます。

特定のイベントのリスク レーティングを計算するために次の値が使用されます。

- シグニチャの忠実度評価（SFR）：ターゲットに関する具体的な情報がない場合に、このシグニチャがどの程度忠実に動作するかに関連付ける重みを示します。シグニチャ忠実度レーティングはシグニチャごとに設定され、シグニチャが、それが表しているイベントまたは条件をどれだけ正確に検出するかを示します。

  シグニチャ忠実度レーティングは、シグニチャベースでシグニチャの作成者が計算します。シグニチャの作成者は、ターゲットに関する条件を絞り込んだ情報がない場合に、シグニチャの正確性についての基準となる信頼度ランキングを定義します。これは、分析対象パケットの配送を許可した

場合に、検出された動作がターゲット プラットフォームに対して意図した効果を生み出す信頼度を表します。たとえば、非常に具体的な規則（特定の正規表現）を使用して記述されたシグニチャは、汎用的な規則を使用して記述されたシグニチャよりもシグニチャ忠実度が高くなります。

（注） シグニチャ忠実度レーティングは、検出されたイベントがどれだけ悪影響を及ぼすかを示すものではありません。

- 攻撃重大度レーティング（ASR）：脆弱性の悪用に成功した場合の重大度に関連付ける重み。

  攻撃重大度レーティングは、シグニチャのアラート重大度パラメータ（informational、low、medium、または high）から計算されます。攻撃重大度レーティングはシグニチャごとに設定され、検出されたイベントどれだけ危険かを示します。

  （注） 攻撃重大度レーティングは、イベントがどれだけ正確に検出されるかを示すものではありません。

- ターゲットの価値レーティング（TVR）：ターゲットの考えられる価値に関連付けられる重み。

  ターゲットの価値レーティングはユーザ設定可能な値（zero、low、medium、high、または mission critical）であり、ネットワーク資産の IP アドレスを通じてその重要性を表します。価値の高い企業リソースにはより厳しく、あまり重要でないリソースにはより緩やかなセキュリティ ポリシーを開発できます。たとえば、デスクトップ ノードに割り当てるターゲットの価値レーティングよりも高いターゲットの価値レーティングを会社の Web サーバに割り当てることができます。この場合、会社の Web サーバに対する攻撃には、デスクトップ ノードに対する攻撃よりも高いリスク レーティングが付与されます。ターゲットの価値レーティングは、イベント アクション規則ポリシーで設定します。

- 攻撃関連性レーティング（ARR）：対象となるオペレーティング システムの関連性に関連付ける重み。

  攻撃関連性レーティングは、派生値（relevant、unknown、または not relevant）であり、アラート時に決定されます。関連するオペレーティング システムはシグニチャごとに設定します。

- 無差別デルタ（PD）：無差別デルタに関連付けられる重みであり、無差別モードの全体的なリスク レーティングから差し引くことができます。

  無差別デルタの範囲は 0 ～ 30 であり、シグニチャごとに設定します。

  （注） トリガー パケットがインラインでない場合、無差別デルタがレーティングから差し引かれます。

- ウォッチ リスト レーティング（WLR）：CSA MC ウォッチ リストに関連付けられる、範囲が 0 ～ 100 の重み（CSA MC での範囲は 0 ～ 35）。

  アラートの攻撃者がウォッチ リストに含まれている場合、その攻撃者のウォッチ リスト レーティングがレーティングに加算されます。

図 8-1 にリスク レーティングの式を示します。

図 8-1　リスク レーティングの式

$$RR = \frac{ASR * TVR * SFR}{10000} + ARR - PD + WLR$$

191016

脅威レーティングの概要

脅威レーティングは、実行されたイベント アクションによって引き下げられたリスク レーティングです。非ロギング イベント アクションには脅威レーティングの調整があります。すべてのイベント アクションのうち最も大きな脅威レーティングがリスク レーティングから差し引かれます。

イベント アクションには次の脅威レーティングがあります。

- Deny attacker inline：45
- Deny attacker victim pair inline：40
- Deny attacker service pair inline：40
- Deny connection inline：35
- Deny packet inline：35
- Modify packet inline：35
- Request block host：20
- Request block connection：20
- Reset TCP connection：20
- Request rate limit：20

イベント アクションのサマライズ

サマライズを使用すると、基本集約機能として、複数のイベントを 1 つのアラートにまとめることにより、センサーから送信されたアラートの量が軽減されます。また、シグニチャごとに特別なパラメータを指定することにより、アラートの処理方法をさまざまに変更できます。各シグニチャは、優先される通常動作を反映したデフォルト値を使用して作成されます。ただし、各シグニチャの設定を修正することにより、エンジンのタイプごとに定められた制約の範囲内でこのデフォルトの処理方法を調整できます。

アラートを生成しないアクション（拒否、ブロック、TCP リセット）には、サマライズされない各シグニチャ イベントのフィルタが適用されます。アラートを生成するアクションは、これらの集約されたアラートに対しては実行されず、アクションが 1 つのサマライズされたアラートに適用された後、フィルタが適用されます。

アラートを生成する他のアクションのいずれかを選択し、フィルタで除外しない場合、[Product Alert] を選択しない場合であってもアラートが作成されます。アラートが作成されないようにするには、アラートを生成するすべてのアクションをフィルタで除外する必要があります。

Meta エンジンがコンポーネント イベントを処理してから、サマライズおよびイベント アクションが処理されます。これにより、センサーは、一連のイベントにまたがって発生する疑わしいアクティビティを監視します。

イベント アクションの集約

基本的な集約には 2 つの動作モードがあります。簡易なモードでは、シグニチャに対し、アラートが送信される前に満たされる必要があるヒット数のしきい値を設定します。一方、高度なモードでは、各インターバルにおけるヒット数がカウントされます。このモードでは、センサーにより秒あたりのヒット数が追跡され、そのしきい値を超えた場合にのみアラートが送信されます。この例で、「ヒット」とはイベントを表すために使用した用語で、基本的にはアラートを指します。ただし、ヒット数がしきい値を超過するまでは、センサーからアラートとして送信されることはありません。

次のサマライズ オプションから選択できます。

- [Fire All]：シグニチャが起動されるたびにアラートが起動されます。サマライズにしきい値が設定されている場合、サマライズが発生するまで実行ごとにアラートが起動されます。サマライズが開始された後は、各アドレス セットについて、サマライズ間隔ごとに 1 つのアラートのみが起動されます。他のアドレス セットのアラートは、すべて発生するか、個別にサマライズされます。そのシグニチャのアラートが一定期間ないと、シグニチャはすべてを起動するモードに戻ります。
- [Summary]：初めてシグニチャがトリガーされたときにアラートが起動され、そのシグニチャの以降のアラートは、要約間隔の間サマライズされます。各アドレスセットについて、要約間隔ごとに 1 個のアラートのみが起動されます。グローバル要約しきい値に達した場合、シグニチャはグローバル サマライズ モードになります。
- [Global Summarization]：要約間隔ごとにアラートを起動します。シグニチャは、グローバル サマライズ用に事前設定できます。
- [Fire Once]：アドレス セットごとにアラートを起動します。このモードはグローバル サマライズ モードにアップグレードできます。

IPS ポリシーの設定

ここでは、IPS ポリシーと、仮想センサーを設定する方法について説明します。内容は次のとおりです。

[IPS Policies] ペイン

[IPS Policies] ペインには、上半分に仮想センサーの一覧が表示されます。このペインの上半分では、仮想センサーを追加、編集、削除できます。

仮想センサーごとに、次の情報が表示されます。

- 仮想センサー名
- 割り当てられているインターフェイスまたはペア
- シグニチャ定義ポリシー
- イベント アクション規則オーバーライド ポリシー
  - リスク レーティング
  - 追加するアクション
  - イネーブルまたはディセーブル
- 異常検出ポリシー
- 仮想センサーの説明

（注）　デフォルトの仮想センサーは vs0 です。デフォルトの仮想センサーは削除できません。

ペインの下半分では、ペインの上半分で選択した各仮想センサーのイベント アクション規則を設定できます。イベント アクション規則は、[Configuration] > *sensor_name* > [Policies] > [Event Action rules] > [rules0] ペインでも設定できます。

ペインの [Event Action Rules] 部分には、次のタブが含まれています。

- [Event Action Filters] : イベントから指定を削除するか、イベント全体を廃棄してセンサーによる今後の処理を回避することができます。
- [IPv4 Target Value Rating] : IPv4 ターゲットの価値レーティングをネットワーク資産に割り当てることができます。ターゲットの価値レーティングは、各アラートのリスク レーティング値の計算に使用される要素の 1 つです。
- [IPv6 Target Value Rating] : IPv6 ターゲットの価値レーティングをネットワーク資産に割り当てることができます。ターゲットの価値レーティングは、各アラートのリスク レーティング値の計算に使用される要素の 1 つです。
- [OS Identifications] : IP アドレスを OS タイプに関連付けることができます。これは、センサーが攻撃関連性レーティングを計算するのに役立ちます。
- [Event Variables] : イベント アクション フィルタで使用するイベント変数を作成できます。同じ値を複数のフィルタで使用する場合は、イベント変数を使用できます。
- [Risk Category] : センサーとネットワークの稼動状態をモニタするために使用したり、イベント アクション オーバーライドで使用するための、リスク カテゴリを作成できます。
- [General] : イベント アクション規則に適用されるいくつかのグローバル設定を設定できます。

Deny Packet Inline について

Deny Packet Inline がアクションとして設定されているシグニチャや、Deny Packet Inline をアクションとして追加するイベント アクション オーバーライドでは、次のアクションを実行できます。

- droppedPacket
- deniedFlow
- tcpOneWayResetSent

Deny Packet Inline アクションは、アラート内のドロップされたパケット アクションとして表現されます。Deny Packet Inline が TCP 接続に対して発生した場合、Deny Connection Inline アクションに自動的にアップグレードされ、アラート内で拒否されたフローとして認識されます。IPS により 1 個のパケットのみが拒否された場合、TCP はその同じパケットを何度も送信しようとするため、IPS は接続全体を拒否して、再送により成功しないようにします。

また、Deny Connection Inline が発生した場合、IPS は自動的に TCP の一方向リセットを送信します。これは、アラート内に TCP 一方向リセットが送信されたものとして現れます。IPS が接続を拒否するとき、クライアント（一般に攻撃者）とサーバ（一般に攻撃対象）の両方で接続が開かれたままになります。開かれた状態の接続が多すぎると、攻撃対象でリソースの問題が発生します。そのため、IPS は TCP リセットを攻撃対象に送信し、攻撃対象の側（通常はサーバ）で接続を閉じ、攻撃対象のリソースを保護します。また、フェールオーバーを防ぎ、他のネットワーク パスに接続がフェールオーバーして攻撃対象に到達するのを許してしまわないようにします。攻撃者の側は開かれたままになり、そこからのすべてのトラフィックが拒否されます。

[IPS Policies] ペインのフィールド定義

[IPS Policies] ペインには次のフィールドがあります。

- [Name]：仮想センサーの名前。デフォルトの仮想センサーは vs0 です。
- [Assigned Interfaces (or Pairs)]：この仮想センサーに属するインターフェイスまたはインターフェイス ペア。
- [Signature Definition Policy]：この仮想センサーのシグニチャ定義ポリシーの名前。デフォルトのシグニチャ定義ポリシーは sig0 です。
- [Event Action Override Policy]：この仮想センサーのイベント アクション規則オーバーライド ポリシーの名前。デフォルトのイベント アクション規則ポリシーは rules0 です。
  - [Risk Rating]：このイベント アクション オーバーライドを起動するために使用するリスク レーティング範囲（low、medium、または high risk）を示します。
  - [Actions to Add]：このイベント アクション オーバーライドの条件が満たされている場合にイベントに追加されるイベント アクションを指定します。
  - [Enabled]：このイベント アクション オーバーライド ポリシーがイネーブルかどうかを示します。
- [Anomaly Detection Policy]：この仮想センサーの異常検出ポリシーの名前。デフォルトの異常検出ポリシーは ad0 です。
- [Description]：この仮想センサーの説明。

[Add Virtual Sensor] および [Edit Virtual Sensor] ダイアログボックスのフィールド定義

（注） 仮想センサーを設定するには、管理者またはオペレータであることが必要です。

同じポリシー（たとえば sig0、rules0、および ad0）を、異なる仮想センサーに適用できます。[Add Virtual Sensor] ダイアログボックスには、この仮想センサーに割り当てることができるインターフェイスのみが表示されます。すでに他の仮想センサーに割り当てられているインターフェイスは、このダイアログボックスに表示されません。

また、イベント アクション オーバーライドを仮想センサーに割り当て、次のモードを設定することもできます。

- 異常検出動作モード

  （注） AIP SSC-5 は異常検出をサポートしていません。

- インライン TCP セッション トラッキング モード

  （注） IPS SSP を搭載した Cisco ASA 5585-X は、インライン TCP セッション トラッキング モードをサポートしていません。

- ノーマライザ モード

（注）　IPS SSP を搭載した Cisco ASA 5585-X は、ノーマライザ モードをサポートしていません。

[Add Virtual Sensor] および [Edit Virtual Sensor] ダイアログボックスには次のフィールドがあります。

- [Virtual Sensor Name]：この仮想センサーの名前。
- [Description]：この仮想センサーの説明。
- [Interfaces]：この仮想センサーのインターフェイスを割り当ておよび削除できます。
  - [Assigned]：インターフェイスまたはインターフェイス ペアが仮想センサーに割り当てられているかどうか。
  - [Name]：仮想センサーに割り当て可能なインターフェイスまたはインターフェイス ペアのリスト（GigabitEthernet または FastEthernet）。
  - [Details]：インライン ペアのインターフェイスのモードのリスト（インライン インターフェイスまたは無差別）。
- [Signature Definition Policy]：この仮想センサーに割り当てるシグニチャ定義ポリシーの名前。デフォルトは sig0 です。
- [Event Action Rules Policy]：この仮想センサーに割り当てるイベント アクション規則ポリシーの名前。デフォルトは rules0 です。
- [Use Event Action Overrides]：オンにした場合、[Add] をクリックして [Add Event Action Override] ダイアログボックスを開き、イベント アクション オーバーライドを設定できます。
  - [Risk Rating]：このオーバーライドのリスク レーティングのレベルを示します。
  - [Actions to Add]：このオーバーライドに追加するアクションを示します。
  - [Enabled]：このオーバーライドがイネーブルかディセーブルかを示します。
- [Anomaly Detection Policy]：この仮想センサーに割り当てる異常検出ポリシーの名前。デフォルトは ad0 です。
- [AD Operational Mode]：この仮想センサーについて、異常検出ポリシーが動作するモード。デフォルトは [Detect] です。
- [Inline TCP Session Tracking Mode]：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。
  - インターフェイスおよび 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 だけ：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。
  - 仮想センサー：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。

（注）　IPS SSP を搭載した Cisco ASA 5585-X は、インライン TCP セッション トラッキング モードをサポートしていません。

- [Normalizer Mode]：トラフィックの検査で必要なノーマライザ モードの種類を選択できます。
  - [Strict Evasion Protection]：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。

（注）　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。

（注）　[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。

（注）　IPS SSP を搭載した Cisco ASA 5585-X は、ノーマライザ モードをサポートしていません。

[Add Event Action Override] および [Edit Event Action Override] ダイアログボックスのフィールド定義

（注）　イベント アクション オーバーライドを追加または編集するためには、管理者またはオペレータであることが必要です。

[Add Event Action Override] および [Edit Event Action Override] ダイアログボックスには次のフィールドがあります。

- [Risk Rating]：このイベント アクション オーバーライドを起動するために使用するリスク レーティング範囲（low、medium、または high risk）を追加できます。設定したリスクに対応するリスク レーティングでイベントが発生した場合、イベント アクションがこのイベントに追加されます。追加モードでは、[Risk Rating] フィールドに入力することで数値範囲を作成できます。編集モードでは、作成したカテゴリを選択できます。
- [Available Actions to Add]：このイベント アクション オーバーライドの条件が満たされている場合にイベントに追加されるイベント アクションを指定します。
- [Assigned]：このオーバーライドにイベント アクションを割り当てることができます。
- [Enabled]：アクションをイネーブルにするにはチェックボックスをオンにします。

（注）　接続ブロックとネットワーク ブロックは、適応型セキュリティ アプライアンスではサポートされていません。適応型セキュリティ アプライアンスは、追加の接続情報があるホスト ブロックだけをサポートします。

仮想センサーの追加、編集、削除

（注）　トラフィックをモニタする前に、すべてのインターフェイスを仮想センサーに割り当て、イネーブルにする必要があります。

仮想センサーを追加、編集、および削除するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Policies] > [IPS Policies] の順に選択し、[Add Virtual Sensor] をクリックします。

ステップ 3　[Virtual Sensor Name] フィールドに、仮想センサーの名前を入力します。

ステップ 4　[Description] フィールドに、この仮想センサーの説明を入力します。

ステップ 5　仮想センサーにインターフェイスを割り当てるには、目的のインターフェイスの横のチェックボックスをオンにし、[Assign] をクリックします。

（注）　[Interfaces] リストには、使用可能なインターフェイスのみが表示されます。他のインターフェイスが存在し、すでに仮想センサーに割り当てられている場合、このリストには現れません。

ステップ 6　ドロップダウン リストからシグニチャ定義ポリシーを選択します。デフォルトの sig0 を使用する場合を除き、[Configuration] > *sensor_name* > [Policies] > [Signature Definitions] > [Add] の順に選択してシグニチャ定義ポリシーを追加しておく必要があります。

ステップ 7　ドロップダウン リストからイベント アクション規則ポリシーを選択します。デフォルトの rules0 を使用する場合を除き、[Configuration] > *sensor_name* > [Policies] > [Event Action Rules] > [Add] の順に選択してイベント アクション規則ポリシーを追加しておく必要があります。

ステップ 8　この仮想センサーにイベント アクション オーバーライドを追加するには、[Use Event Action Overrides] チェックボックスをオンにし、[Add] をクリックします。

（注）　[Use Event Action Overrides] チェックボックスをオンにする必要があります。そうしないと、設定した値にかかわらず、イベント アクション オーバーライドがどれもイネーブルになりません。

a.　[Risk Rating] ドロップダウン リストからリスク レーティングを選択します。

b.　[Assigned] 列で、このイベント アクション オーバーライドに割り当てるアクションの横のチェックボックスをオンにします。

c.　[Enabled] 列で、イネーブルにするアクションの横のチェックボックスをオンにします。

（注）　接続ブロックとネットワーク ブロックは、適応型セキュリティ アプライアンスではサポートされていません。適応型セキュリティ アプライアンスは、追加の接続情報があるホスト ブロックだけをサポートします。

ヒント　変更内容を破棄して [Add Event Action Override] ダイアログボックスを閉じるには、[Cancel] をクリックします。

d. [OK] をクリックします。

ステップ 9　ドロップダウン リストから異常検出ポリシーを選択します。デフォルトの ad0 を使用する場合を除き、[Configuration] > *sensor_name* > [Policies] > [Anomaly Detections] > [Add] の順に選択して異常検出ポリシーを追加しておく必要があります。

ステップ 10　ドロップダウン リストから異常検出モード（[Detect]、[Inactive]、[Learn]）を選択します。デフォルトは [Detect] です。

ステップ 11　[Double Arrow] アイコンを選択し、[Advanced Options] のデフォルト値を変更します。

a. センサーがインライン TCP セッションを追跡する方法を選択します（インターフェイスおよび VLAN ごと、VLAN のみ、または仮想センサー）。デフォルトは仮想センサーです。これはほぼ常に最適な選択肢となります。

b. ノーマライザ モードを選択します（厳格な回避保護または非同期モード保護）。

（注） IPS SSP を搭載した Cisco ASA 5585-X は、ノーマライザ モードをサポートしていません。

ヒント 変更内容を破棄して [Add Virtual Sensor] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 12　[OK] をクリックします。仮想センサーが [IPS Policies] ペインのリストに表示されます。

ステップ 13　仮想センサーを編集するには、リスト中の仮想センサーを選択し、[Edit] をクリックします。

ステップ 14　必要な変更を行い、[OK] をクリックします。編集後の仮想センサーが [IPS Policies] ペインの上半分にあるリストに表示されます。

ステップ 15　仮想センサーを削除するには、仮想センサーを選択し、[Delete] をクリックします。仮想センサーが [IPS Policies] ペインの上半分に表示されなくなります。

（注） デフォルトの仮想センサー vs0 は削除できません。

ヒント 変更を破棄するには、[Reset] をクリックします。

ステップ 16　変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

イベント アクション フィルタの設定

ここでは、イベント アクション フィルタの設定方法について説明します。内容は次のとおりです。

- 「イベント アクション フィルタの追加、編集、削除、イネーブル化、ディセーブル化、移動」（P.8-17）

イベント アクション フィルタの概要

イベント アクション フィルタは順序リストとして処理され、フィルタはリスト内で上下に移動できます。フィルタによって、センサーは、イベントに応答して特定のアクションを実行できます。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はありません。フィルタは、イベントからアクションを削除することで機能します。1 つの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、イベントを効率的に消費します。

注意　送信元および宛先 IP アドレスに基づくイベント アクション フィルタは Sweep エンジンでは機能しません。これは、これらのフィルタが、通常のシグニチャとしてフィルタしないためです。送信元および宛先 IP アドレスをスイープ アラートでフィルタするには、Sweep エンジン シグニチャの送信元および宛先 IP アドレス フィルタ パラメータを使用します。

（注）　スイープ シグニチャをフィルタリングする場合は、宛先アドレスをフィルタリングしないことを推奨します。複数の宛先アドレスがある場合、最後のアドレスだけがフィルタとの照合に使用されます。

[Event Action Filters] タブ

特定のアクションをイベントから削除するか、または、イベント全体を廃棄してセンサーによる今後の処理を回避するように、イベント アクション フィルタを設定できます。[Event Variables] ペインで定義した変数を使用して、フィルタに合わせてアドレスをグループ化できます。

（注）　文字列ではなく変数を使用していることを示すために、変数の先頭にドル記号（$）を付ける必要があります。「$」を付けないと、「`Bad source and destination`」エラーが生じます。

[Event Action Filters] タブのフィールド定義

[Event Action Filters] タブには次のフィールドがあります。

- [Name]：追加するフィルタに名前を付けることができます。フィルタをリスト中で移動したり、必要に応じて非アクティブ リストに移動できるように、フィルタに名前を付ける必要があります。
- [Enabled]：このフィルタがイネーブルかどうかを示します。
- [Sig ID]：このシグニチャに割り当てられた一意の数値を示します。この値により、センサーは特定のシグニチャを識別します。シグニチャの範囲を入力することもできます。
- [SubSig ID]：このサブシグニチャに割り当てられた一意の数値を示します。SubSig ID によって、広範なシグニチャのより詳細なバージョンが識別されます。subSig ID の範囲を入力することもできます。
- [Attacker (IPv4/IPv6/port)]：攻撃パケットを送信したホストの IP アドレスまたはポートを示します。アドレスまたはポートの範囲を入力することもできます。
- [Victim (IPv4/IPv6/port)]：攻撃者のホストが使用している IP アドレスまたはポートを示します。アドレスまたはポートの範囲を入力することもできます。

- [Risk Rating]：このイベント アクション フィルタをトリガーするために使用されるリスク レーティング範囲を示します（0 ～ 100）。イベントが発生し、そのリスク レーティングがここで設定した最小 - 最大範囲に入っていた場合、イベントはこのイベント フィルタの規則と比較して処理されます。
- [Actions to Subtract]：イベントの条件がイベント アクション フィルタの基準を満たしている場合に、イベントから削除されるアクションを示します。

[Add Event Action Filter] および [Edit Event Action Filter] ダイアログ ボックスのフィールド定義

[Add Event Action Filter] および [Edit Event Action Filter] ダイアログボックスには次のフィールドがあります。

- [Name]：追加するフィルタに名前を付けることができます。フィルタをリスト中で移動したり、必要に応じて非アクティブ リストに移動できるように、フィルタに名前を付ける必要があります。
- [Enabled]：このフィルタをイネーブルにできます。
- [Signature ID]：このシグニチャに割り当てられた一意の数値を示します。この値により、センサーは特定のシグニチャを識別します。シグニチャの範囲を入力することもできます。
- [Subsignature ID]：このサブシグニチャに割り当てられた一意の数値を示します。サブシグニチャ ID によって、広範なシグニチャのより詳細なバージョンが識別されます。サブシグニチャ ID の範囲を入力することもできます。
- [Attacker IPv4 Address]：攻撃パケットを送信したホストの IP アドレスを示します。アドレスの範囲を入力することもできます。
- [Attacker IPv6 Address]：攻撃パケットを送信したホストの攻撃者 IPv6 アドレスの範囲を次の形式で示します。

  <XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

  例：2001:0db8:1234:1234:1234:1234:1234:1234,2001:0db8:1234:1234:1234:1234:1234:8888。範囲の 2 番目の IPv6 アドレスは、最初の IPv6 アドレス以上である必要があります。

  （注） IPv6 アドレスは、16 進数で表現された 128 ビットであり、コロンにより 8 個の 16 ビット グループに分かれています。先頭のゼロをスキップしたり、中間のゼロのグループを 2 個のコロン（::）で表現できます。アドレスは、プレフィクス 2001:db8 で始める必要があります。

- [Attacker Port]：攻撃者ホストによって使用されるポートを示します。これは、攻撃パケットの発信元のポートです。ポートの範囲を入力することもできます。
- [VictimIPv4 Address]：攻撃対象ホスト（攻撃パケットの受信者）の IP アドレスを示します。アドレスの範囲を入力することもできます。
- [VictimIPv6 Address]：攻撃対象になっているホスト（攻撃パケットの受信者）の攻撃対象 IPv6 アドレスの範囲を次の形式で示します。

  <XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

例：2001:0db8:1234:1234:1234:1234:1234:1234,2001:0db8:1234:1234:1234:1234:1234:8888。範囲の 2 番目の IPv6 アドレスは、最初の IPv6 アドレス以上である必要があります。

（注）　IPv6 アドレスは、16 進数で表現された 128 ビットであり、コロンにより 8 個の 16 ビット グループに分かれています。先頭のゼロをスキップしたり、中間のゼロのグループを 2 個のコロン（::）で表現できます。アドレスは、プレフィクス 2001:db8 で始める必要があります。

- [Victim Port]：攻撃パケットを受信したポートを示します。ポートの範囲を入力することもできます。
- [Risk Rating]：このイベント アクション フィルタをトリガーするために使用されるリスク レーティング範囲を示します（0 ～ 100）。イベントが発生し、そのリスク レーティングがここで設定した最小 - 最大範囲に入っていた場合、イベントはこのイベント フィルタの規則と比較して処理されます。
- [Actions to Subtract]：[Opens the Edit Actions] ダイアログボックスを開きます。このダイアログでは、イベントの条件がイベント アクション フィルタの基準を満たしている場合に、イベントから削除されるアクションを選択できます。
- More Options
  - [Active]：フィルタリング イベントに適用されるように、フィルタ リストにフィルタを追加できます。
  - [OS Relevance]：攻撃が攻撃対象オペレーティング システムに関係しないイベントをフィルタで除外します。
  - [Deny Percentage]：攻撃者拒否機能で拒否するパケットのパーセンテージを決定します。有効な範囲は 0 ～ 100 です。デフォルトは 100% です。
  - [Stop on Match]：このイベントをイベント アクション フィルタ リストの残りのフィルタに対して処理するかどうかを決定します。

    [No] に設定した場合、Stop フラグが見つかるまで残りのフィルタが照合のために処理されます。

    [Yes] の場合、以降の処理は行われません。このフィルタで指定されたアクションは削除され、残りのアクションが実行されます。
  - [Comments]：このフィルタに関連付けられているユーザ コメントを表示します。

イベント アクション フィルタの追加、編集、削除、イネーブル化、ディセーブル化、移動

（注）　グローバル相関インスペクションおよびレピュテーション フィルタリング拒否機能では、IPv6 アドレスがサポートされていません。グローバル相関インスペクションでは、センサーは IPv6 アドレスのレピュテーション データを受信または処理しません。IPv6 アドレスのリスク レーティングは、グローバル相関インスペクション用に変更されません。同様に、ネットワーク参加には、IPv6 アドレスからの攻撃に関するイベント データは含まれていません。また、IPv6 アドレスは拒否リストに表示されません。

（注）　レート制限およびブロッキングは、IPv6 トラフィックではサポートされていません。ブロック アクションまたはレート制限アクションが設定されているシグニチャが IPv6 トラフィックによってトリガーされると、アラートが生成されますが、アクションは実行されません。

イベント アクション フィルタを追加、編集、削除、イネーブル化、ディセーブル化、および移動するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Policies] > [IPS Policies] の順に選択します。

ステップ 3　ペインの上半分で、イベント アクション フィルタを追加する仮想センサーをリストから選択します。

ステップ 4　ペインの [Event Action Rules] 部分で、[Event Action Filters] タブをクリックし、[Add] をクリックします。

ステップ 5　[Name] フィールドに、イベント アクション フィルタの名前を入力します。デフォルト名が設定されますが、より意味のある名前に変更できます。

ステップ 6　[Enabled] フィールドで [Yes] オプション ボタンをクリックし、フィルタをイネーブルにします。

ステップ 7　[Signature ID] フィールドに、このフィルタを適用するすべてのシグニチャのシグニチャ ID を入力します。リスト（2001,2004）または範囲（2001–2004）の他、[Event Variables] タブで定義したいずれかの SIG 変数を使用できます。変数の前には $ を付けます。

ステップ 8　[SubSignature ID] フィールドには、このフィルタを適用するシグニチャのサブシグニチャ ID を入力します。

ステップ 9　[Attacker IPv4 Address] フィールドに、送信元ホストの IP アドレスを入力します。[Event Variables] タブで定義した変数を使用できます。変数の前には $ を付けます。また、アドレスの範囲を入力することもできます（例：0.0.0.0-255.255.255.255）。

ステップ 10　Attacker IPv6 Address フィールドに、送信元ホストの攻撃者 IPv6 アドレスの範囲を次の形式で入力します。

<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

範囲の 2 番目の IPv6 アドレスは、最初の IPv6 アドレス以上である必要があります。

（注）　IPv6 アドレスは、16 進数で表現された 128 ビットであり、コロンにより 8 個の 16 ビット グループに分かれています。先頭のゼロをスキップしたり、中間のゼロのグループを 2 個のコロン（::）で表現できます。アドレスは、プレフィクス 2001:db8 で始める必要があります。

[Event Variables] タブで定義した変数を使用することもできます。変数の前には $ を付けます。

ステップ 11　[Attacker Port] フィールドに、攻撃者が攻撃パケットを送信するために使用するポート番号を入力します。

ステップ 12　[Victim IPv4 Address] フィールドに、受信者ホストの IP アドレスを入力します。[Event Variables] タブで変数を定義済みであれば、そのうちの 1 つを使用できます。変数の前には $ を付けます。また、アドレスの範囲を入力することもできます（例：0.0.0.0-255.255.255.255）。

ステップ 13　[Victim IPv6 Address] フィールドに、受信者ホストの IPv6 アドレスの範囲を次の形式で入力します。

<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

範囲の 2 番目の IPv6 アドレスは、最初の IPv6 アドレス以上である必要があります。

（注） IPv6 アドレスは、16 進数で表現された 128 ビットであり、コロンにより 8 個の 16 ビット グループに分かれています。先頭のゼロをスキップしたり、中間のゼロのグループを 2 個のコロン（::）で表現できます。アドレスは、プレフィクス 2001:db8 で始める必要があります。

[Event Variables] タブで定義した変数を使用できます。変数の前には $ を付けます。

ステップ 14　[Victim Port] フィールドに、攻撃対象ホストが攻撃パケットを受信するために使用するポート番号を入力します。

ステップ 15　[Risk Rating] フィールドに、このフィルタのリスク レーティング範囲を入力します。イベントのリスク レーティングが指定した範囲に収まる場合、イベントはこのフィルタの条件に照らして処理されます。

ステップ 16　[Actions to Subtract] フィールドで、メモ アイコンをクリックし、[Edit Actions] ダイアログボックスを開きます。このフィルタでイベントから削除するアクションのチェックボックスをオンにします。

ヒント　リストで複数のイベント アクションを選択するには、Ctrl キーを押しながらクリックします。

ステップ 17　[Active] フィールドで、[Yes] オプション ボタンをクリックし、このフィルタをリストに追加して、フィルタリング イベントで有効にします。

ステップ 18　[OS Relevance] ドロップダウン リストで、攻撃対象について特定されたオペレーティング システムにアラートが関連するかどうかを知る必要があるかどうかを選択します。

ステップ 19　[Deny Percentage] フィールドに、拒否攻撃者機能で拒否するパケットのパーセンテージを入力します。デフォルトは 100% です。

ステップ 20　[Stop on Match] フィールドに、次のオプション ボタンのいずれかをクリックします。

a. [Yes]：この特定のフィルタのアクションが削除された後に、Event Action Filters コンポーネントで処理を停止するかどうか。残りのフィルタはすべて処理されないため、イベントから他のアクションを削除できません。

b. [No]：他のフィルタの処理を継続するかどうか。

ステップ 21　[Comments] フィールドに、このフィルタの目的や、このフィルタを特定の方法で設定した理由など、このフィルタとともに保存するコメントを入力します。

ヒント　変更内容を破棄して [Add Event Action Filter] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 22　[OK] をクリックします。新しいイベント アクション フィルタが [Event Action Filters] タブのリストに表示されます。

ステップ 23　既存のイベント アクション フィルタを編集するには、リストで選択し、[Edit] をクリックします。

ステップ 24　必要な変更を加えます。

ヒント　変更内容を破棄して [Edit Event Action Filter] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 25　[OK] をクリックします。編集後のイベント アクション フィルタが [Event Action Filters] タブのリストに表示されます。

ステップ 26　イベント アクション フィルタを削除するには、リストで選択し、[Delete] をクリックします。イベント アクション フィルタが [Event Action Filters] タブのリストに表示されなくなります。

ステップ 27　イベント アクション フィルタをリスト中で上下に移動するには、選択し、[Move Up] または [Move Down] 矢印アイコンをクリックします。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 28　変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

IPv4 ターゲットの価値レーティングの設定

ここでは、IPv4 ターゲットの価値レーティングを設定する方法について説明します。内容は次のとおりです。

- 「[IPv4 Target Value Rating] タブ」（P.8-20）
- 「[IPv4 Target Value Rating] タブのフィールド定義」（P.8-20）
- 「[Add Target Value Rating] および [Edit Target Value Rating] ダイアログボックスのフィールド定義」（P.8-21）
- 「IPv4 ターゲットの価値レーティングの追加、編集、および削除」（P.8-21）

[IPv4 Target Value Rating] タブ

（注）　ターゲットの価値レーティングを追加、編集、または削除するためには、管理者またはオペレータであることが必要です。

ネットワーク資産にターゲットの価値レーティングを割り当てることができます。ターゲットの価値レーティングは、各アラートのリスク レーティング値の計算に使用される要素の 1 つです。異なるターゲットに異なるターゲットの価値レーティングを割り当てることができます。イベントのリスク レーティングが高いほど、より厳しいシグニチャ イベント アクションがトリガーされます。

[IPv4 Target Value Rating] タブのフィールド定義

[IPv4 Target Value Rating] タブには次のフィールドがあります。

- [Target Value Rating (TVR)]：このネットワーク資産に割り当てる価値を示します。値は、[High]、[Low]、[Medium]、[Mission Critical]、または [No Value] です。
- [Target IP Address]：ターゲットの価値レーティングを使用して優先順位を付けるネットワーク資産の IP アドレスを示します。

[Add Target Value Rating] および [Edit Target Value Rating] ダイアログボックスのフィールド定義

[Add Target Value Rating] および [Edit Target Value Rating] ダイアログボックスには次のフィールドがあります。

- [Target Value Rating (TVR)] : このネットワーク資産に価値を割り当てます。値は、[High]、[Low]、[Medium]、[Mission Critical]、または [No Value] です。
- [Target IPv4 Address(es)] : ターゲットの価値レーティングを使用して優先順位を付けるネットワーク資産の IP アドレスを示します。

IPv4 ターゲットの価値レーティングの追加、編集、および削除

ネットワーク資産の IPv4 ターゲットの価値レーティングを追加、編集、および削除するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Policies] > [IPS Policies] の順に選択します。

ステップ 3　[IPS Policies] ペインの上半分で、ターゲットの価値レーティングを設定する仮想センサーを選択します。

ステップ 4　ペインの [Event Action Rules] 部分で、[IPv4 Target Value Rating] タブをクリックし、[Add] をクリックします。

ステップ 5　ターゲットの価値レーティングを新しい資産グループに割り当てるには、次の手順を実行します。

a. [Target Value Rating (TVR)] ドロップダウン リストからレーティングを選択します。値は [High]、[Low]、[Medium]、[Mission Critical]、または [No Value] です。

b. [Target IPv4 Address(es)] フィールドに、ネットワーク資産の IP アドレスを入力します。IP アドレスの範囲を入力するには、その範囲の最も小さいアドレス、ハイフン、最も大きいアドレスの順に入力します。例 : 10.10.2.1-10.10.2.30。

ヒント　変更を破棄して [Add IPv4 Target Value Rating] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 6　[OK] をクリックします。新しい資産の新しいターゲットの価値レーティングが [IPv4 Target Value Rating] タブのリストに表示されます。

ステップ 7　既存のターゲットの価値レーティングを編集するには、リストで選択し、[Edit] をクリックします。

ステップ 8　必要な変更を加えます。

ヒント　変更を破棄して [Edit IPv4 Target Value Rating] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 9　[OK] をクリックします。編集したネットワーク資産が [IPv4 Target Value Rating] タブのリストに表示されます。

ステップ 10　ネットワーク資産を削除するには、リスト中で選択し、[Delete] をクリックします。ネットワーク資産が [Ipv4 Target Value Rating] タブのリストに表示されなくなります。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 11　変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

IPv6 ターゲットの価値レーティングの設定

ここでは、IPv6 ターゲットの価値レーティングを設定する方法について説明します。内容は次のとおりです。

[IPv6 Target Value Rating] タブ

（注）　ターゲットの価値レーティングを追加、編集、または削除するためには、管理者またはオペレータであることが必要です。

ネットワーク資産にターゲットの価値レーティングを割り当てることができます。ターゲットの価値レーティングは、各アラートのリスク レーティング値の計算に使用される要素の 1 つです。異なるターゲットに異なるターゲットの価値レーティングを割り当てることができます。イベントのリスク レーティングが高いほど、より厳しいシグニチャ イベント アクションがトリガーされます。

[IPv6 Target Value Rating] タブのフィールド定義

[IPv6 Target Value Rating] タブには次のフィールドがあります。

- [Target Value Rating (TVR)]：このネットワーク資産に割り当てる価値を示します。値は、[High]、[Low]、[Medium]、[Mission Critical]、または [No Value] です。
- [Target IP Address]：ターゲットの価値レーティングを使用して優先順位を付けるネットワーク資産の IP アドレスを示します。

[Add Target Value Rating] および [Edit Target Value Rating] ダイアログボックスのフィールド定義

[Add Target Value Rating] および [Edit Target Value Rating] ダイアログボックスには次のフィールドがあります。

- [Target Value Rating (TVR)]：このネットワーク資産に価値を割り当てます。値は、[High]、[Low]、[Medium]、[Mission Critical]、または [No Value] です。
- [Target IPv6 Address(es)]：ターゲットの価値レーティングを使用して優先順位を付けるネットワーク資産の IPv6 アドレスを次の形式で示します。

  <XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

  例：2001:0db8:1234:1234:1234:1234:1234:1234,2001:0db8:1234:1234:1234:1234:1234:8888。範囲の 2 番目の IPv6 アドレスは、最初の IPv6 アドレス以上である必要があります。

（注） IPv6 アドレスは、16 進数で表現された 128 ビットであり、コロンにより 8 個の 16 ビットグループに分かれています。先頭のゼロをスキップしたり、中間のゼロのグループを 2 個のコロン（::）で表現できます。アドレスは、プレフィクス 2001:db8 で始める必要があります。

IPv6 ターゲットの価値レーティングの追加、編集、および削除

（注） グローバル相関インスペクションおよびレピュテーション フィルタリング拒否機能では、IPv6 アドレスがサポートされていません。グローバル相関インスペクションでは、センサーは IPv6 アドレスのレピュテーション データを受信または処理しません。IPv6 アドレスのリスク レーティングは、グローバル相関インスペクション用に変更されません。同様に、ネットワーク参加には、IPv6 アドレスからの攻撃に関するイベント データは含まれていません。また、IPv6 アドレスは拒否リストに表示されません。

（注） レート制限およびブロッキングは、IPv6 トラフィックではサポートされていません。ブロック アクションまたはレート制限アクションが設定されているシグニチャが IPv6 トラフィックによってトリガーされると、アラートが生成されますが、アクションは実行されません。

ネットワーク資産の IPv6 ターゲットの価値レーティングを追加、編集、および削除するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Policies] > [IPS Policies] の順に選択します。

ステップ 3　[IPS Policies] ペインの上半分で、ターゲットの価値レーティングを設定する仮想センサーを選択します。

ステップ 4　ペインの [Event Action Rules] 部分で、[IPv6 Target Value Rating] タブをクリックし、[Add] をクリックします。

ステップ 5　ターゲットの価値レーティングを新しい資産グループに割り当てるには、次の手順を実行します。

a. [Target Value Rating (TVR)] ドロップダウン リストからレーティングを選択します。値は [High]、[Low]、[Medium]、[Mission Critical]、または [No Value] です。

b. [Target IPv6 Address(es)] フィールドに、ネットワーク資産の IP アドレスを入力します。

<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

[Event Variables] タブで定義した変数を使用することもできます。変数の前には $ を付けます。範囲の 2 番目の IPv6 アドレスは、最初の IPv6 アドレス以上である必要があります。

（注） IPv6 アドレスは、16 進数で表現された 128 ビットであり、コロンにより 8 個の 16 ビット グループに分かれています。先頭のゼロをスキップしたり、中間のゼロのグループを 2 個のコロン（::）で表現できます。アドレスは、プレフィクス 2001:db8 で始める必要があります。

ヒント 変更を破棄して [Add IPv6 Target Value Rating] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 6　[OK] をクリックします。新しい資産の新しいターゲットの価値レーティングが [IPv6 Target Value Rating] タブのリストに表示されます。

ステップ 7　既存のターゲットの価値レーティングを編集するには、リストで選択し、[Edit] をクリックします。

ステップ 8　必要な変更を加えます。

ヒント 変更を破棄して [Edit IPv6 Target Value Rating] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 9　[OK] をクリックします。編集したネットワーク資産が [IPv6 Target Value Rating] タブのリストに表示されます。

ステップ 10　ネットワーク資産を削除するには、リスト中で選択し、[Delete] をクリックします。ネットワーク資産が [IPv6 Target Value Rating] タブのリストに表示されなくなります。

ヒント 変更を破棄するには、[Reset] をクリックします。

ステップ 11　変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

OS ID の設定

ここでは、OS マップを設定する方法について説明します。内容は次のとおりです。

パッシブ OS フィンガープリントについて

パッシブ OS フィンガープリントにより、センサーはホストが稼動している OS を特定できます。センサーはホスト間のネットワーク トラフィックを分析して、これらのホストの OS をその IP アドレスとともに格納します。センサーはネットワーク上で交換される TCP SYN および SYNACK パケットを検査して、OS タイプを特定します。

次に、センサーはターゲット ホスト OS の OS を使用し、リスク レーティングの攻撃関連性レーティング コンポーネントを計算することによって、攻撃対象への攻撃の関連性を決定します。センサーは、攻撃の関連性に基づいて、攻撃に対するアラートのリスク レーティングを変更したり、攻撃のアラートをフィルタリングしたりする場合があります。ここで、リスク レーティングを使用すると、偽陽性アラートの数を減らしたり（IDS モードの利点）、疑わしいパケットを明確にドロップしたり（IPS モードの利点）できます。また、パッシブ OS フィンガープリントでは、攻撃対象 OS、OS ID のソース、および攻撃対象 OS との関連性をアラート内にレポートすることによって、アラート出力が拡張されます。

パッシブ OS フィンガープリントは、次の 3 つのコンポーネントで構成されます。

- Passive OS learning：パッシブ OS ラーニングは、センサーがネットワーク上のトラフィックを監視しているときに行われます。TCP SYN および SYNACK パケットの特性に基づいて、センサーは送信元 IP アドレスのホスト上で稼動している OS を特定します。
- User-configurable OS identification：学習した OS マップよりも優先される OS ホスト マップを設定できます
- Computation of attack relevance rating and risk rating：センサーは OS 情報を使用して攻撃シグニチャのターゲット ホストに対する関連性を決定します。攻撃の関連性は、攻撃アラートのリスク レーティング値を構成する攻撃関連性レーティング コンポーネントです。センサーは、CSA MC からのホスト ポスチャ情報で報告された OS タイプを使用して攻撃関連性レーティングを計算します。

OS 情報には 3 つのソースがあります。センサーは OS 情報のソースを次の順序でランク付けします。

1. 設定された OS マップ：ユーザが入力する OS マップ。

   設定された OS マップはイベント アクション規則ポリシーにあり、1 つ以上の仮想センサーに適用できます。

   （注）　同じ IP アドレスに対し複数のオペレーティング システムを指定できます。リスト中の最後のオペレーティング システムが照合されます。

2. インポートした OS マップ：外部データ ソースからインポートした OS マップ。

   インポートした OS マップはグローバルであり、すべての仮想センサーに適用されます。

   （注）　現在は CSA MC が唯一の外部データ ソースです。

3. 学習した OS マップ：SYN 制御ビットが設定されている TCP パケットのフィンガープリントを介して、センサーが検知した OS マップ。

学習した OS マップは、トラフィックを監視する仮想センサーに対してローカルです。

センサーは、ターゲット IP アドレスの OS を特定する必要がある場合に、設定した OS マップを調べます。ターゲット IP アドレスが設定した OS マップにない場合、センサーはインポートした OS マップを調べます。ターゲット IP アドレスがインポートした OS マップにない場合、センサーは学習した OS マップを調べます。そこでも見つからなかった場合、センサーはターゲット IP の OS を不明として処理します。

（注）　パッシブ OS フィンガープリントはデフォルトでイネーブルになっており、IPS にはシグニチャごとにデフォルトの脆弱な OS リストが含まれています。

パッシブ OS フィンガープリントの設定

パッシブ OS フィンガープリントを使用するために、設定を行う必要はありません。IPS には、各シグニチャについてデフォルトの脆弱な OS のリストが用意されており、パッシブ分析がデフォルトでイネーブルになっています。

パッシブ OS フィンガープリントについて次の側面を設定できます。

- OS マップの定義：OS マップを設定し、重要なシステムで動作している OS の ID を定義することをお勧めします。重要なシステムの OS および IP アドレスが変更される可能性が少ない場合は、OS マップを設定するのが適切です。
- 攻撃関連性レーティング計算を特定の IP アドレス範囲に限定：これにより、攻撃関連性レーティング計算が、保護されたネットワーク上の IP アドレスに限定されます。
- OS マップのインポート：OS マップのインポートは、パッシブ分析を通じて行われる OS ID の学習速度と忠実度を高めるためのメカニズムです。CSA MC などの外部製品インターフェイスがある場合は、そこから OS ID をインポートできます。
- ターゲットの OS 関連性の値を使用したイベント アクション規則フィルタの定義：これは、OS の関連性のみに対してアラートをフィルタするための方法を提供します。
- パッシブ分析のディセーブル化：センサーが新しい OS マップを学習するのを停止します。
- シグニチャ脆弱 OS リストの編集：脆弱 OS リストは、どの OS タイプが各シグニチャに対して脆弱かを指定したものです。デフォルトでは、[General OS] が、脆弱 OS リストを指定しないすべてのシグニチャに適用されます。

[OS Identifications] タブ

（注）　設定済みの OS マップを追加、編集、および削除するためには、管理者またはオペレータであることが必要です。

学習した OS マップよりも優先される OS ホスト マップを設定するには、[OS Identifications] タブを使用します。[OS Identifications] タブで、設定済みの OS マップの追加、編集、および削除を行うことができます。リスト内で OS マップを上下に移動すると、特定の IP アドレスと OS タイプの組み合わせに対する攻撃関連性レーティングおよびリスク レーティングの計算をセンサーが行う順序を変更できます。

また、リスト内で OS マップを上下に移動すると、特定の IP アドレスに関連付けられている OS をセンサーが解決する順序を変更できます。設定した OS マップでは、範囲を設定できます。そのため、ネットワーク 192.168.1.0/24 の場合、次のように定義できます（表 8-1）。

表 8-1　設定された OS マップの例

IP アドレス範囲の設定	OS
192.168.1.1	IOS
192.168.1.2-192.168.1.10、192.168.1.25	UNIX
192.168.1.1-192.168.1.255	Windows

より特定的なマップをリストの先頭に配置する必要があります。IP アドレス範囲設定では重複は許可されませんが、最もリストの先頭に近いエントリが優先されます。

[OS Identifications] タブのフィールド定義

[OS Identifications] タブには次のフィールドがあります。

- [Enable passive OS fingerprinting analysis] : オンにすると、センサーによりパッシブ OS 分析が実行されます。
- [Restrict Attack Relevance Ratings (ARR) to these IP addresses] : OS タイプから特定の IP アドレスへのマッピングを設定し、その IP アドレスの攻撃関連性レーティングをセンサーで計算します。
- [Configured OS Maps] : 設定されている OS マップの属性が表示されます。
  - [Name] : 設定されている OS マップに付けた名前が表示されます。
  - [Active] : この設定された OS マップがアクティブかどうか。
  - [IP Address] : この設定された OS マップの IP アドレス。
  - [OS Type] : この設定された OS マップの OS タイプ。

[Add Configured OS Map] および [Edit Configured OS Map] ダイアログボックスの定義

[Add Configured OS Map] および [Edit Configured OS Map] ダイアログボックスには次のフィールドがあります。

- [Name] : この設定された OS マップの名前。
- [Active] : 設定された OS マップをアクティブまたは非アクティブにします。
- [IP Address] : この設定された OS マップに関連付けられている IP アドレス。設定されている OS マップの IP アドレス（かつ設定されている OS マップのみ）は、IP アドレスのセットおよび IP アドレス範囲になります。次に示すのは、すべて設定された OS マップの有効な IP アドレス値です。
  - 10.1.1.1,10.1.1.2,10.1.1.15
  - 10.1.2.1
  - 10.1.1.1-10.2.1.1,10.3.1.1
  - 10.1.1.1-10.1.1.5
- [OS Type] : IP アドレスに関連付ける次の OS タイプのいずれかを選択できます。

- AIX
- BSD
- General OS
- HP UX
- IOS
- IRIX
- Linux
- Mac OS
- Netware
- その他
- Solaris
- UNIX
- Unknown OS
- Win NT
- Windows
- Windows NT/2K/XP

設定された OS マップの追加、編集、削除、および移動

設定された OS マップを追加、編集、削除、および移動するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Policies] > [IPS Policies] の順に選択します。

ステップ 3　[IPS Policies] ペインの上半分で、OS ID を設定する仮想センサーを選択します。

ステップ 4　ペインの [Event Action Rules] 部分で、[OS Identifications] タブをクリックし、[Add] をクリックします。

ステップ 5　[Name] フィールドに設定される OS マップの名前を入力します。

ステップ 6　[Active] フィールドで、[Yes] オプション ボタンをクリックし、この設定される OS マップをリストに追加して有効にします。

ステップ 7　[IP Address] フィールドに、OS にマッピングするホストの IP アドレスを入力します。たとえば、10.10.5.5,10.10.2.1-10.10.2.30 という形式を使用します。

ステップ 8　[OS Type] ドロップダウン リストから、IP アドレスにマッピングする OS を選択します。

ヒント　変更を破棄して [Add Configured OS Map] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 9　[OK] をクリックします。新たに設定された OS マップが [OS Identifications] タブのリストに表示されます。

ステップ 10　[Enable passive OS fingerprinting analysis] チェックボックスをオンにします。

（注）　[OS Identifications] タブで [Enable passive OS fingerprinting analysis] チェックボックスをオンにしないと、[Add Configured OS Map] ダイアログボックスで設定する値にかかわらず、設定される OS マップがイネーブルになりません。

ステップ 11　設定された OS マップを編集するには、リスト中で選択し、[Edit] をクリックします。

ステップ 12　必要な変更を加えます。

ヒント　変更を破棄して [Edit Configured OS Map] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 13　[OK] をクリックします。編集後の設定された OS マップが [OS Identifications] タブのリストに表示されます。

ステップ 14　[Enable passive OS fingerprinting analysis] チェックボックスをオンにします。

（注）　[OS Identifications] タブで [Enable passive OS fingerprinting analysis] チェックボックスをオンにしないと、[Edit Configured OS Map] ダイアログボックスで設定する値にかかわらず、設定された OS マップがイネーブルになりません。

ステップ 15　設定された OS マップを削除するには、リスト中で選択し、[Delete] をクリックします。設定された OS マップが [OS Identifications] タブのリストに表示されなくなります。

ステップ 16　設定された OS マップをリスト中で上下に移動するには、移動対象を選択し、[Move Up] または [Move Down] 矢印をクリックします。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 17　変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

イベント変数の設定

ここでは、イベント変数の設定方法について説明します。内容は次のとおりです。

[Event Variables] タブ

（注） イベント変数を追加、編集、または削除するためには、管理者またはオペレータであることが必要です。

イベント変数を作成し、イベント アクション フィルタでそれらの変数を使用できます。同じ値を複数のフィルタで使用する場合は、変数を使用します。変数の値を変更した場合、その変数を使用するフィルタが新しい値で更新されます。

（注） 文字列ではなく変数を使用していることを示すために、変数の先頭にドル記号（$）を付ける必要があります。

一部の変数はシグニチャ システムに必要なため削除できません。変数が保護されている場合は、その変数を選択して編集できません。保護された変数を削除しようとするとエラー メッセージが表示されます。一度に編集できる変数は 1 つだけです。

IPv4 アドレス

IPv4 アドレスを設定する場合、完全な IP アドレス、範囲、複数の範囲を指定します。

- 10.89.10.10-10.89.10.23
- 10.90.1.1
- 192.56.10.1-192.56.10.255
- 10.1.1.1-10.2.255.255, 10.89.10.10-10.89.10.23

IPv6 アドレス

IPv6 アドレスを設定する場合は、次の形式を使用します。

<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

（注） IPv6 アドレスは、16 進数で表現された 128 ビットであり、コロンにより 8 個の 16 ビット グループに分かれています。先頭のゼロをスキップしたり、中間のゼロのグループを 2 個のコロン（::）で表現できます。アドレスは、プレフィクス 2001:db8 で始める必要があります。

ワンポイントアドバイス エンジニアリング グループに割り当てられる IP アドレス スペースがあり、そのグループに Windows システムが存在せず、そのグループに対する Windows 関連の攻撃を心配する必要がない場合、変数をそのエンジニアリング グループの IP アドレス スペースとして設定できます。次に、この変数を使用して、このグループに対するすべての Windows 関連の攻撃を無視するフィルタを設定できます。

[Event Variables] タブのフィールド定義

[Event Variables] タブには次のフィールドがあります。

- [Name]：この変数の名前を割り当てることができます。
- [Type]：変数をアドレスとして識別します。
- [Value]：この変数によって表される値を追加できます。

[Add Event Variable] および [Edit Event Variable] ダイアログボックスのフィールド定義

[Add Event Variable] および [Edit Event Variable] ダイアログボックスには次のフィールドがあります。

- [Name]：この変数の名前を割り当てることができます。
- [Type]：変数を IPv4 または IPv6 アドレスとして識別します。
  - [address]：IPv4 アドレスの場合は、完全な IP アドレス、範囲、複数の範囲を使用します。
  - [ipv6-address]：IPv6 アドレスの場合は次の形式を使用します。

    <XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

    （注）　IPv6 アドレスは、16 進数で表現された 128 ビットであり、コロンにより 8 個の 16 ビット グループに分かれています。先頭のゼロをスキップしたり、中間のゼロのグループを 2 個のコロン（::）で表現できます。アドレスは、プレフィクス 2001:db8 で始める必要があります。

  - [Value]：この変数によって表される値を追加できます。

イベント変数の追加、編集、削除

（注）　グローバル相関インスペクションおよびレピュテーション フィルタリング拒否機能では、IPv6 アドレスがサポートされていません。グローバル相関インスペクションでは、センサーは IPv6 アドレスのレピュテーション データを受信または処理しません。IPv6 アドレスのリスク レーティングは、グローバル相関インスペクション用に変更されません。同様に、ネットワーク参加には、IPv6 アドレスからの攻撃に関するイベント データは含まれていません。また、IPv6 アドレスは拒否リストに表示されません。

（注）　レート制限およびブロッキングは、IPv6 トラフィックではサポートされていません。ブロック アクションまたはレート制限アクションが設定されているシグニチャが IPv6 トラフィックによってトリガーされると、アラートが生成されますが、アクションは実行されません。

イベント変数を追加、編集、および削除するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Policies] > [IPS Policies] の順に選択します。

ステップ 3　[IPS Policies] ペインの上半分で、イベント変数を設定する仮想センサーを選択します。

ステップ 4　ペインの [Event Action Rules] 部分で、[Event Variables] タブをクリックし、[Add] をクリックします。

ステップ 5　[Name] フィールドにこの変数の名前を入力します。

（注）　名前には、数字とアルファベットのみを使用できます。また、ハイフン（-）またはアンダースコア（_）も使用できます。

ステップ 6　[Type] ドロップダウン リストから、IPv4 アドレスの場合は [address] を選択し、IPv6 のアドレスの場合は [ipv6-address] を選択します。

ステップ 7　[Value] フィールドにこの変数の値を入力します。

IPv4 アドレスの場合、完全な IP アドレス、範囲、複数の範囲を指定します。例：

- 10.89.10.10-10.89.10.23
- 10.90.1.1
- 192.56.10.1-192.56.10.255

（注）　デリミタにはカンマが使用できます。カンマの後にはスペースを入れないでください。スペースを入力すると、「`Validation failed`」エラーが生じます。

IPv6 アドレスの場合は次の形式を使用します。

<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

（注）　IPv6 アドレスは、16 進数で表現された 128 ビットであり、コロンにより 8 個の 16 ビット グループに分かれています。先頭のゼロをスキップしたり、中間のゼロのグループを 2 個のコロン（::）で表現できます。アドレスは、プレフィクス 2001:db8 で始める必要があります。

ヒント　変更内容を破棄して [Add Event Variable] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 8　[OK] をクリックします。新しい変数が [Event Variables] タブのリストに表示されます。

ステップ 9　既存の変数を編集するには、リストで選択し、[Edit] をクリックします。

ステップ 10　必要な変更を加えます。

ヒント　変更内容を破棄して [Edit Event Variable] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 11　[OK] をクリックします。編集したイベント変数が [Event Variables] タブのリストに表示されます。

ステップ 12　イベント変数を削除するには、リストで選択し、[Delete] をクリックします。イベント変数が [Event Variables] タブのリストに表示されなくなります。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 13　変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

リスク カテゴリの設定

ここでは、リスク カテゴリの設定方法について説明します。内容は次のとおりです。

[Risk Category] タブ

（注）　リスク レベルを追加および編集するには、管理者であることが必要です。

[Risk Category] タブで、定義済みのリスク カテゴリ（HIGHRISK、MEDIUMRISK、および LOWRISK）を使用するか、独自のラベルを定義できます。リスク カテゴリは、カテゴリ名を、リスク レーティングを定義する数値の範囲にリンクします。範囲を連続したものにするには、カテゴリに低いしきい値を指定します。上位のカテゴリは、次に高いカテゴリまたは 100 です。

その後、脅威を赤、黄、緑のカテゴリにグループ分けできます。これらの赤、黄、緑のしきい値統計情報は、イベント アクション オーバーライドで使用され、[Home] ページの [Network Security Gadget] にも表示されます。

（注）　定義済みのリスク カテゴリは削除できません。

赤、黄、緑のしきい値統計情報は、ネットワーク セキュリティの状態を表し、赤が最も重大です。しきい値を変更した場合、リスク カテゴリと同じ範囲のすべてのイベント アクション オーバーライドが、新しい範囲を反映するように変更されます。

新しいカテゴリは、そのしきい値に従って [Risk Category] リストに挿入され、その範囲をカバーするアクションが自動的に割り当てられます。

[Risk Category] タブのフィールド定義

[Risk Category] タブには次のフィールドがあります。

- [Risk Category Name]：このリスク レベルの名前。定義済みのカテゴリには次の値があります。

  - HIGHRISK：90（90 ～ 100）
  - MEDIUMRISK：70（70 ～ 89）
  - LOWRISK：1（1 ～ 69）
- [Risk Threshold]：このリスクのしきい値。値は 0 ～ 100 の数字です。
- [Risk Range]：このリスク カテゴリのリスク レーティング範囲。リスク レーティングとは、ネットワーク上の特定のイベントに関連付けられたリスクを数値化した、0 ～ 100 の範囲の値です。
- [Network Security Health Statistics]：赤、黄、緑のしきい値の数を一覧表示します。ネットワーク全体のセキュリティ値は、最も安全でない値（緑が最も安全で赤が最も安全でない）を表します。これらの色しきい値は、[Home] ペインの [Sensor Health] ガジェットを参照します。
  - Red Threat Threshold
  - Yellow Threat Threshold
  - Green Threat Threshold

[Add Risk Level] および [Edit Risk Level] ダイアログボックスのフィールド定義

[Add Risk Level] および [Edit Risk Level] ダイアログボックスには次のフィールドがあります。

- [Risk Name]：このリスク レベルの名前。
- [Risk Threshold]：このリスク レベルのリスクしきい値を割り当てることができます。リスク カテゴリが連続したものになるように、カテゴリの下限しきい値のみを指定または変更できます。上限しきい値は、次に高いカテゴリまたは 100 です。
- [Active]：このリスク レベルをアクティブにします。

リスク カテゴリの追加、編集、削除

リスク カテゴリを追加、編集、および削除するには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Policies] > [IPS Policies] の順に選択します。

ステップ 3　[IPS Policies] ペインの上半分で、リスク カテゴリを設定する仮想センサーを選択します。

ステップ 4　ペインの [Event Action Rules] 部分で、[Risk Category] タブをクリックし、[Add] をクリックします。

ステップ 5　[Risk Name] フィールドに、このリスク カテゴリの名前を入力します。

ステップ 6　[Risk Threshold] フィールドに、リスクしきい値の数値（最小 0、最大 100）を入力します。この数値はリスクの下限を表します。範囲は [Risk Range] フィールドと、赤、黄、緑のしきい値フィールドに表示されます。

ステップ 7　このリスク カテゴリをアクティブにするには、[Yes] オプション ボタンをクリックします。

ヒント　変更内容を破棄して [Add Risk Category] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 8　[OK] をクリックします。新しいリスク カテゴリが [Risk Category] タブのリストに表示されます。

ステップ 9　既存のリスク カテゴリを編集するには、リストで選択し、[Edit] をクリックします。

ステップ 10　必要な変更を加えます。

ヒント　変更内容を破棄して [EditRisk Category] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 11　[OK] をクリックします。編集したリスク カテゴリが [Risk Category] タブのリストに表示されます。

ステップ 12　リスク カテゴリを削除するには、リスト中で選択し、[Delete] をクリックします。リスク カテゴリが [Risk Category] タブのリストに表示されなくなります。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 13　変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

一般設定

ここでは、一般的な設定を行う方法について説明します。内容は次のとおりです。

[General] タブ

（注）　イベント アクション規則の一般的な設定を行うには、管理者またはオペレータであることが必要です。

Summarizer や Meta Event Generator を使用するかどうかなど、イベント アクション規則全体に適用される一般的な設定を行うことができます。Summarizer はイベントを単一アラートにグループ化するため、センサーが送信するアラートの数が減少します。Meta Event Generator はコンポーネント イベントを処理します。これによって、センサーは一連のイベントで疑わしいアクティビティが発生していないかどうかを監視できます。

注意　トラブルシューティング目的以外では、Summarizer または Meta Event Generator をディセーブルにしないでください。Summarizer をディセーブルにすると、すべてのシグニチャがサマライズなしの [Fire All] に設定されます。Meta Event Generator をディセーブルにすると、すべてのメタ エンジン シグニチャがディセーブルになります。

また、脅威レーティングの調整、イベント アクション フィルタの使用、一方向の TCP リセットのイネーブル化を行うこともできます。一方向の TCP リセットはインライン モードでだけ動作し、Deny Packet Inline アクションに自動追加されます。TCP リセットがアラートの攻撃対象に送信されるため、攻撃者に対してブラック ホールが作成され、攻撃対象の TCP リソースがクリアされます。

（注）　これにより、インライン センサーで、リスク レーティングが 90 以上のアラートのパケットを拒否されるようになります。また、リスク レーティングが 90 以上の TCP アラートで、一方向 TCP リセットを発行します。

攻撃者を拒否する期間、拒否攻撃者の最大数、ブロックの継続期間を設定できます。

[General] タブのフィールド定義

[General] タブには次のフィールドがあります。

- [Use Summarizer]：Summarizer コンポーネントをイネーブルにします。

  デフォルトでは、Summarizer はイネーブルになります。ディセーブルにすると、すべてのシグニチャがサマライズなしの [Fire All] に設定されます。サマライズするように個別のシグニチャを設定しても、この設定は Summarizer がイネーブルになっていない場合は無視されます。
- [Use Meta Event Generator]：Meta Event Generator をイネーブルにします。

  デフォルトでは、Meta Event Generator はイネーブルになります。Meta Event Generator をディセーブルにすると、すべてのメタ エンジン シグニチャがディセーブルになります。
- [Use Threat Rating Adjustment]：脅威レーティングの調整がイネーブルになり、これによってリスク レーティングが調整されます。ディセーブルにすると、リスク レーティングは脅威レーティングと等しくなります。
- [Use Event Action Filters]：イベント アクション フィルタ コンポーネントをイネーブルにします。イネーブルになっているいずれかのフィルタを使用するには、このチェックボックスをオンにする必要があります。
- [Enable One Way TCP Reset]：（インラインのみ）TCP ベースのアラートで、拒否パケット インライン アクションの一方向の TCP リセットをイネーブルにします。TCP リセットがアラートの攻撃対象に送信されるため、攻撃対象の TCP リソースがクリアされます。
- [Deny Attacker Duration]：攻撃者をインラインで拒否する秒数。有効な範囲は 0 ～ 518400 です。デフォルトは 3600 です。
- [Block Action Duration]：ホストまたは接続をブロックする時間（分単位）。有効な範囲は 0 ～ 10000000 です。デフォルトは 30 です。
- [Maximum Denied Attackers]：一度にシステム内に許容できる拒否攻撃者の数を制限します。有効な範囲は 0 ～ 100000000 です。デフォルトは 10000 です。

一般的な設定

注意　一般設定オプションはグローバル レベルで動作するため、イネーブルにするとこれらの機能のすべてのセンサー処理に影響があります。

イベント アクション規則の一般的な設定を行うには、次の手順を実行します。

ステップ 1　管理者権限またはオペレータ権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Policies] > [IPS Policies] の順に選択します。

ステップ 3　[IPS Policies] ペインの上半分で、一般的なカテゴリを設定する仮想センサーを選択します。

ステップ 4　ペインの [Event Action Rules] 部分で、[General] タブをクリックします。

ステップ 5　Summarizer の機能をイネーブルにするには、[Use Summarizer] チェックボックスをオンにします。

注意　Summarizer は、トラブルシューティング目的でのみディセーブルにします。それ以外の場合は、サマライズ用に設定したすべてのシグニチャが実際にサマライズされるように、Summarizer をイネーブルにしてください。

ステップ 6　Meta Event Generator をイネーブルにするには、[Use Meta Event Generator] チェックボックスをオンにします。

注意　Meta Event Generator は、トラブルシューティング目的でのみディセーブルにします。それ以外の場合は、すべての Meta エンジンのシグニチャが機能するように、Meta Event Generator をイネーブルにしてください。

ステップ 7　脅威レーティング調整をイネーブルにするには、[Use Threat Rating Adjustment] チェックボックスをオンにします。

ステップ 8　イベント アクション フィルタをイネーブルにするには、[Use Event Action Filters] チェックボックスをオンにします。

（注）　[Configuration] > se*nsor_name* > [Policies] > [IPS Policies] > [Event Action Filters] ペインで設定したイベント アクション フィルタがアクティブになるように、[General] ペインの [Use Event Action Filters] チェックボックスをオンにする必要があります。

ステップ 9　拒否パケット インライン アクションで一方向の TCP リセットをイネーブルにするには、[Enable One Way TCP Reset] チェックボックスをオンにします。

ステップ 10　[Deny Attacker Duration] フィールドに、攻撃者をインラインで拒否する秒数を入力します。

ステップ 11　[Block Action Duration] フィールドに、ホストまたは接続をブロックする期間を分単位で入力します。

ステップ 12　[Maximum Denied Attackers] フィールドに、同時に拒否する拒否攻撃者の最大数を入力します。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 13　変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。