CHAPTER 6

ポリシーの設定

（注） IPS SSP を搭載した Cisco ASA 5585-X は、現在のところ、Cisco IPS 7.1 をサポートする唯一のプラットフォームです。現時点では、他に IPS バージョン 7.1 をサポートしている Cisco IPS センサーはありません。

（注） IPS SSP を搭載した Cisco ASA 5585 は、ASA 8.2(4.4) 以上および ASA 8.4(2) 以上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 ポリシーの概要と、仮想センサーの設定方法について説明します。次の事項について説明します。

セキュリティ ポリシーの概要

複数のセキュリティ ポリシーを作成して、個々の仮想センサーに適用できます。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、異常検出ポリシー、それぞれ 1 つで構成されます。Cisco IPS には、sig0 というデフォルトのシグニチャ定義ポリシー、rules0 というデフォルトのイベント アクション規則ポリシー、ad0 というデフォルトの異常検出ポリシーが含まれています。デフォルト ポリシーを仮想センサーに割り当てるか、新しいポリシーを作成することができます。セキュリティ ポリシーを複数使用すると、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。次の事項について説明します。

分析エンジンについて

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、分析エンジン内に作成します。各仮想センサーには一意の名前が付けられ、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 グループのリストが関連付けられます。定義の順位付けの問題を回避するため、割り当てに競合またはオーバーラップは許可されません。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 グループは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ることがないようにします。また、各仮想センサーには、特に指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 でサポートされる仮想センサーは最大 4 つです。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

（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。デフォルトの仮想センサーで変更できる設定機能は、インターフェイス リスト、異常検出運用モード、および仮想センサーの説明のみです。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、異常検出ポリシーは変更できません。

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、設定ポリシーのセットにより定義されたデータの集まりです。仮想センサーは、インターフェイス コンポーネントの定義に従って、パケットのセットに適用されます。

仮想センサーは複数のセグメントをモニタでき、1 つの物理センサー内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。分析中の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 インスタンス（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。仮想センサーには、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 グループを割り当てることができます。

仮想化の利点および制約事項

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。

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 以上のすべてのイベントで SNMP トラップを生成させる場合、[Request SNMP Trap] のリスク レーティングに 85 ～ 100 を設定します。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できます。

（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ません。適応型セキュリティ アプライアンスでは、追加の接続情報があるホスト ブロックだけがサポートされます。

リスク レーティングの計算

リスク レーティング（RR）は、ネットワーク上の特定のイベントと関連するリスクの数値定量化を表す 0 ～ 100 の範囲の値です。この計算では、攻撃されているネットワーク資産（特定のサーバなど）の価値も考慮されるため、RR はシグニチャ単位（攻撃の重大度レーティングおよびシグニチャの忠実度レーティングを使用）およびサーバ単位（ターゲットの価値レーティングを使用）で設定されます。リスク レーティングは、複数の要素から計算され、設定される要素、収集される要素、および派生される要素を含みます。

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

リスク レーティングによって、注意する必要のある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 ファクタによって、成功した場合の攻撃の重大度、シグニチャの忠実度、グローバル相関データから得られた攻撃者の評価スコア、およびターゲット ホスト全体の主観的な価値が考慮されます。リスク レーティングは、evIdsAlert にレポートされます。

特定のイベントについてリスク レーティングを計算するときは、次の値が使用されます。

- [Signature fidelity rating]（SFR）：ターゲットに関する具体的な情報がない場合に、このシグニチャをどの程度忠実に実行するのかに関連付ける重みを示します。シグニチャの忠実度レーティングは、シグニチャごとに設定され、シグニチャでイベントまたはシグニチャが記述している状態を検出する精度を示します。

  シグニチャの忠実度レーティングは、シグニチャ作成者によってシグニチャごとに計算されます。シグニチャ作成者は、ターゲットに関する裏付けとなる情報がない場合のシグニチャの精度について、ベースラインとなる信頼度を定義します。この信頼度は、分析中のパケットの配信を許可した場合に、検出された動作によってターゲット プラットフォームに与えられる、意図された影響の信頼度を表します。たとえば、きわめて具体的な規則（詳細な正規表現など）で記述されたシグニチャは、汎用的な規則で記述されたシグニチャより高いシグニチャの忠実度レーティングを持ちます。

  （注）　シグニチャの忠実度レーティングは、検出したイベントの危険性を示すものではありません。

- [Attack severity rating]（ASR）：脆弱性の不正利用が成功した場合の重大度に関連する重み値。

  攻撃の重大度レーティングは、シグニチャの Alert Severity パラメータ（informational、low、medium、または high）から得られます。攻撃の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の危険性を示します。

  （注）　攻撃の重大度レーティングは、イベント検出の精度を示すものではありません。

- [Target value rating]（TVR）：ターゲットの知覚価値に関連する重み値。

ターゲットの価値レーティングは、ネットワーク資産（IP アドレスによる）の重要度を示す、ユーザ設定可能な値です（0、low、medium、high、または mission critical）。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。

- [Attack relevance rating]（ARR）：ターゲット オペレーティング システムの関連性に関連する重み値。

  攻撃関連性レーティングは、アラート時点に決定される派生値です（relevant、unknown、または not relevant）。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されます。

- [Promiscuous delta]（PD）：無差別モード時に全体的なリスク レーティング全体から削除できる、混合デルタに関連する重み値。

  混合デルタの範囲は、0 ～ 30 で、シグニチャごとに設定されます。

（注）　トリガー パケットがインラインでない場合、混合デルタはレーティングから削除されます。

- [Watch list rating]（WLR）：CSA MC ウォッチ リストに関連する 0 ～ 100 の範囲の重み値（CSA MC では範囲 0 ～ 35 だけを使用）。

  アラートの攻撃者がウォッチ リストに存在する場合、この攻撃者のウォッチ リスト評価がレーティングに追加されます。

図 6-1 にリスク レーティングの数式を示します。

図 6-1　　リスク レーティング式

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

191016

詳細情報

グローバル相関の詳細については、第 11 章「グローバル相関の設定」を参照してください。

脅威レーティングについて

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低下されたリスク レーティングです。ロギングされないイベント 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 アクションのうちで最大の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

サマライズで基本集約機能によっ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るアラートの量が削減されます。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、優先される正常な動作を反映するデフォルトを使用して作成されます。一方、各シグニチャを調整して、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動作を変更することは可能です。

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）の場合は、サマライズなしで各シグニチャ イベントのフィルタを通過します。アラートを生成するアクションは、このサマライズされるアラートに対しては実行されません。代わりに、サマリー アラート 1 つに対してアクションが適用されてからフィルタを通されます。

その他のアラート アクションのいずれかを選択し、このアクションをフィルタリングで除外しなかった場合、そのアラートは、[Product Alert] を選択しなくても作成されます。アラートを作成させないためには、アラートを生成するすべてのアクションをフィルタリングによって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 アクションは処理されます。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。

イベント アクションの集約

基本集約機能には 2 種類の動作モードがあります。簡易モードでは、アラートが送信されるまでに満たす必要のある、単一シグニチャの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、センサーは 1 秒あたりのヒット数を追跡し、そのしきい値に達したときのみアラートを送信します。この例で、ヒットとは基本的にはアラートを示す一方で、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のないイベントを表す用語です。

次のサマライズ オプションの中から選択できます。

- [Fire All]：シグニチャがトリガーされるたびにアラートを起動します。サマライズにしきい値を設定した場合は、サマライズの発生までは、実行のたびにアラートが起動されます。サマライズが開始されると、各アドレス セットでサマリー間隔ごとにアラート 1 つだけが起動されます。その他のアドレス セットに対するアラートは、すべて表示されるか、個別にサマライズされます。該当のシグニチャで一定期間アラートがないと、シグニチャは Fire All モードに戻ります。
- [Summary]：シグニチャが最初にトリガーされたときにアラートを起動し、それ以降は、サマリー間隔の期間ごとにそのシグニチャの追加のアラートをサマライズします。各アドレス セットでサマリー間隔ごとにアラート 1 つだけが起動されます。グローバル サマリーのしきい値に達すると、シグニチャは Global Summarization モードに入ります。
- [Global Summarization]：サマリー間隔ごとに 1 つのアラートが起動されます。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 1 つのアラートが起動されます。このモードは Global Summarization 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 ポリシーの概要と、仮想センサーの設定方法について説明します。次の事項について説明します。

[IPS Policies] ペイン

[IPS Policies] ペインの上半分には、仮想センサーのリストが表示されています。このペインの上半分で、仮想センサーを追加、編集、または削除できます。

見つかった仮想センサーごとに、次の情報が表示されます。

- 仮想センサーの名前
- 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に、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] > [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、次のタブが含まれます。

- [Event Action Filters]：イベントから指定を削除するか、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できます。
- [IPv4 Target Value Rating]：ネットワーク資産に IPv4 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。
- [IPv6 Target Value Rating]：ネットワーク資産に IPv6 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。

- [OS Identifications] : IP アドレスに OS タイプを関連付けることができます。これは、センサーによる攻撃関連性レーティングの計算に役立ちます。
- [Event Variables] : イベント変数を作成して、イベント アクション フィルタで使用できます。同じ値を複数のフィルタで使用する場合は、イベント変数を使用します。
- [Risk Category] : センサーとネットワーク ヘルスのモニタ、およびイベント アクションのオーバーライドに使用するリスク 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する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または [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 オーバーライドの場合は、次のアクションが実行される可能性があります。

- droppedPacket
- deniedFlow
- tcpOneWayResetSent

[Deny Packet Inline] アクションは、アラート内では、ドロップされたパケットのアクションとして表されます。TCP 接続で発生した [Deny Packet Inline] は、[Deny Connection Inline] アクションに自動的にアップグレードされ、アラート内では、拒否されたフローとして表示されます。IPS でパケット 1 個だけを拒否した場合、TCP は同じパケットの再送信を試行し続けるため、IPS は接続全体を拒否して、再送信による成功を決して発生させません。

[Deny Connection Inline] が発生した場合、IPS は、TCP 一方向リセットの自動送信も行います。これは、送信された TCP 一方向リセットとしてアラート内に表示されます。IPS が接続を拒否する場合、IPS は、クライアント（通常は攻撃者）とサーバ（通常は攻撃対象）の両側にオープン接続を残します。オープン接続の数が多すぎると、攻撃される側でリソースの問題を引き起こすことがあります。したがって、IPS では、TCP リセットを攻撃対象に送信して攻撃される側（通常はサーバ）の接続を閉じます。これにより、攻撃される側のリソースが温存されます。別のネットワーク パスに接続をフェールオーバーして攻撃対象まで到達させることがないように、フェールオーバーも防止されます。IPS では、攻撃者側をオープンしたままにし、攻撃者からのすべてのトラフィックを拒否します。

[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] : この仮想センサーに対するイベント 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 オーバーライドのトリガーに使用されるリスク レーティング範囲（リスク低、中、高）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]/[Edit Virtual Sensor] ダイアログボックスのフィールドの定義

（注） IPS SSP を搭載した Cisco ASA 5585-X は、現在のところ、Cisco IPS 7.1 をサポートする唯一のプラットフォームです。現時点では、他に IPS バージョン 7.1 をサポートしている Cisco IPS センサーはありません。

（注） IPS SSP を搭載した Cisco ASA 5585 は、ASA 8.2(4.4) 以上および ASA 8.4(2) 以上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。

注意 IPS SSP には、4 種類のポート（コンソール、管理、GigabitEthernet、10GE）があります。IPS SSP の右前面パネルにあるコンソール ポートと管理ポートは、IPS ソフトウェアを使用して設定および制御します。IPS SSP の左前面パネルにある GigabitEthernet ポートと 10GE ポートは、IPS ソフトウェアではなく、ASA ソフトウェアを使用して設定および制御します。ただし、IPS SSP をリセットまたはシャットダウンした場合は、GigabitEthernet ポートと 10GE ポートもリンク ダウンします。スケジュールされたメンテナンスの時間帯は IPS SSP をリセットまたはシャットダウンして、これらのポートがリンク ダウンする影響を最小化する必要があります。

（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必要があります。

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。他の仮想センサーに割り当て済みのインターフェイスは、このダイアログボックスには表示されません。

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

- 異常検出運用モード

[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]：この仮想センサーにインターフェイスを割り当てたり、削除したりできます。
  - [Assigned]：この仮想センサーにインターフェイスまたはインターフェイス ペアが割り当て済みかどうかを示します。

  - [Name]：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またはインターフェイス ペア（GigabitEthernet または FastEthernet）のリスト。
  - [Details]：インターフェイスおよびインライン ペアのインターフェイスのモード（インライン インターフェイスまたは無差別）をリストします。
- [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]：オンにすると、[Add] をクリックして [Add Event Action Override] ダイアログボックスを開いたときに、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に対するリスク 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]：この仮想センサーで運用する異常検出ポリシーのモード。デフォルトは Detect です。

詳細情報

ASA ソフトウェアの詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html

[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には、管理者またはオペレータである必要があります。

[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 オーバーライドのトリガーに使用されるリスク レーティング範囲（リスク低、中、高）を追加できます。設定したリスクに対応するリスク レーティングを持つイベントが発生した場合は、このイベントにイベント アクションが追加されます。追加モードでは、[Risk Rating] フィールドに値を入力して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できます。
- [Enabled]：チェックボックスをオンにして、アクションをイネーブルにします。

（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ません。適応型セキュリティ アプライアンスでは、追加の接続情報があるホスト ブロックだけがサポートされます。

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または [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 オーバーライドの場合は、次のアクションが実行される可能性があります。

- droppedPacket
- deniedFlow
- tcpOneWayResetSent

Deny Packet Inline アクションは、アラートではドロップされたパケット アクションとして表されます。TCP 接続の Deny Packet Inline が発生すると、Deny Connection Inline アクションに自動的にアップグレードされ、アラートでは拒否されたフローとして表示されます。IPS でパケット 1 個だけを拒否した場合、TCP は同じパケットの再送信を試行し続けるため、IPS は接続全体を拒否して、再送信による成功を決して発生させません。

Deny Connection Inline が発生すると、IPS も一方向 TCP リセットを自動的に送信します。これは、アラートで送信された一方向 TCP リセットとして表示されます。IPS が接続を拒否する場合、IPS は、クライアント（通常は攻撃者）とサーバ（通常は攻撃対象）の両側にオープン接続を残します。オープン接続の数が多すぎると、攻撃される側でリソースの問題を引き起こすことがあります。したがって、IPS では、TCP リセットを攻撃対象に送信して攻撃される側（通常はサーバ）の接続を閉じます。これにより、攻撃される側のリソースが温存されます。別のネットワーク パスに接続をフェールオーバーして攻撃対象まで到達させることがないように、フェールオーバーも防止されます。IPS では、攻撃者側をオープンしたままにし、攻撃者からのすべてのトラフィックを拒否します。

仮想センサーの追加、編集、削除

仮想センサーでトラフィックをモニタするには、仮想センサーにすべてのインターフェイスを割り当て、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 IDM にログインします。

ステップ 2　[Configuration] > [Policies] > [IPS Policies] を選択して、[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、必要なインターフェイスの隣にあるチェックボックスをオンにして、[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リストされます。他のインターフェイスが存在していても、別の仮想センサーに割り当て済みであれば、そのインターフェイスはこのリストには表示されません。

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 を使用する場合以外は、事前に [Configuration] > [Policies] > [Signature Definitions] > [Add] を選択して、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 を使用する場合以外は、事前に [Configuration] > [Policies] > [Event Action Rules] > [Add] を選択して、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て、[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しないと、設定した値に関係なく、イベント アクション オーバーライドは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] カラムの下で、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隣にあるチェックボックスをオンにします。

c.　[Enabled] カラムの下で、イネーブルにするアクションの隣にある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ません。適応型セキュリティ アプライアンスでは、追加の接続情報があるホスト ブロックだけがサポートされます。

ヒント　変更を廃棄して [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 を使用する場合以外は、事前に [Configuration] > [Policies] > [Anomaly Detections] > [Add] を選択して、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。

ヒント　変更を破棄して [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 11　[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 12　仮想センサーを編集するには、リストから仮想センサーを選択して、[Edit] をクリックします。

ステップ 13　必要な変更を加え、[OK] をクリックします。編集された仮想センサーが [IPS Policies] ペインの上半分に表示されます。

ステップ 14　仮想センサーを削除するには、仮想センサーを選択して、[Delete] をクリックします。削除した仮想センサーは [IPS Policies] ペインの上半分には表示されません。

（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 15　[Apply] をクリックして、変更を適用し、改訂したコンフィギュレーションを保存します。

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。次の事項について説明します。

イベント アクション フィルタについて

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）　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

（注）　イベント アクション フィルタを追加、編集、イネーブル化、ディセーブル化、または削除するには、管理者またはオペレータである必要があります。

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、フィルタのアドレスをグループ化できます。

注意　送信元および宛先 IP アドレスに基づいたイベント アクション フィルタは、通常のシグニチャとしてフィルタリングしないため、Sweep エンジンでは機能しません。スイープ アラートで送信元および宛先 IP アドレスをフィルタリングするには、Sweep エンジン シグニチャで送信元および宛先 IP アドレス フィルタ パラメータを使用します。

（注）　文字列ではなく変数を使用していることを示すために、変数はドル記号（$）で始める必要があります。「$」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

（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 イベント アクションまたはレート制限イベント アクションを指定してシグニチャを設定し、IPv6 トラフィックによってトリガーされた場合、アラートは生成されますが、アクションは実行されません。

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

- [Name]：追加するフィルタの名前を付けることができます。リスト内で移動したり、必要に応じて非アクティブ リストに移動したりできるように、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になっている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。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/IPv6/port)]：攻撃パケットを送信するホストの IP アドレスまたはポート、あるいはその両方を示します。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)]：攻撃者ホストによって使用される IP アドレスまたはポート、あるいはその両方を示します。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（0 ～ 100）を示します。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

（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 イベント アクションまたはレート制限イベント アクションを指定してシグニチャを設定し、IPv6 トラフィックによってトリガーされた場合、アラートは生成されますが、アクションは実行されません。

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

- [Name]：追加するフィルタの名前を付けることができます。リスト内で移動したり、必要に応じて非アクティブ リストに移動したりできるように、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 アドレスの範囲設定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。範囲内の 2 番目の IPv6 アドレスは、最初の IPv6 アドレス以上でなければなりません。

  （注）　IPv6 アドレスは、16 進数で表される 128 ビットで、コロンで区切られた 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て、二重のコロン（::）を使用して中央のゼロ化グループを表すことができます。アドレスは、2001:db8 プレフィクス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]：攻撃されているホスト（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]：攻撃されているホスト（攻撃パケットの受信者）の攻撃対象 IPv6 アドレスの範囲設定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。範囲内の 2 番目の IPv6 アドレスは、最初の IPv6 アドレス以上でなければなりません。

（注）　IPv6 アドレスは、16 進数で表される 128 ビットで、コロンで区切られた 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て、二重のコロン（::）を使用して中央のゼロ化グループを表すことができます。アドレスは、2001:db8 プレフィクス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（0 ～ 100）を示します。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] : [Edit Actions] ダイアログボックスを開き、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す場合にイベントから削除する必要があるアクションを選択できます。
- More Options
  - [Active] : フィルタリング イベントで有効になるように、フィルタをフィルタ リストに追加できます。
  - [OS Relevance] : 攻撃が攻撃対象のオペレーティング システムに関係しないイベントをフィルタリングして除外できます。
  - [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判別します。有効な範囲は 0 ～ 100 です。デフォルトは 100% です。
  - [Stop on Match]：このイベントがイベント アクション フィルタ リストの残りのフィルタと比較して処理されるかどうかを決定します。

    [No] に設定すると、残りのフィルタは、Stop フラグが検出されるまで一致のために処理されます。

    [Yes] に設定すると、これ以上の処理は行われません。このフィルタによって指定される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たユーザの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、および移動

（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 イベント アクションまたはレート制限イベント アクションを指定してシグニチャを設定し、IPv6 トラフィックによってトリガーされた場合、アラートは生成されますが、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 IDM にログインします。

ステップ 2　[Configuration] > [Policies] > [IPS Policies] を選択します。

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　ペイン半分の [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。デフォルトの名前が指定されていますが、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て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）、範囲（2001–2004）、または [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サブ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。アドレスの範囲（たとえば、0.0.0.0-255.255.255.255）を入力することもできます。

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 アドレスの範囲設定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>].

範囲内の 2 番目の IPv6 アドレスは、最初の IPv6 アドレス以上でなければなりません。

（注）　IPv6 アドレスは、16 進数で表される 128 ビットで、コロンで区切られた 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て、二重のコロン（::）を使用して中央のゼロ化グループを表すことができます。アドレスは、2001:db8 プレフィクス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] タブで変数を定義した場合は、いずれかの変数を使用できます。変数の前には $ を付けます。アドレスの範囲（たとえば、0.0.0.0-255.255.255.255）を入力することもできます。

ステップ 13　[Victim IPv6 Address] フィールドに、受信者ホストの IPv6 アドレス範囲設定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>].

範囲内の 2 番目の IPv6 アドレスは、最初の IPv6 アドレス以上でなければなりません。

（注） IPv6 アドレスは、16 進数で表される 128 ビットで、コロンで区切られた 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て、二重のコロン（::）を使用して中央のゼロ化グループを表すことができます。アドレスは、2001:db8 プレフィクス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内に入る場合は、イベントは、このフィルタの基準と比較して処理されます。

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て [Edit Actions] ダイアログボックスを開きます。イベントからこのフィルタを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て、フィルタリング イベントで有効になるようにこのフィルタをリストに追加します。

ステップ 18 [OS Relevance] ドロップダウン リストで、アラートが標的対象であると識別されたオペレーティング システムに関連してい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、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] フィールドで、次のいずれかのオプション ボタンをクリックします。

a. [Yes]：この特定のフィルタのアクションを削除した後で、Event Action Filters コンポーネントで処理を停止します。残りのフィルタは処理されません。そのため、追加のアクションをイベントから削除できません。

b. [No]：追加のフィルタの処理を続行します。

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格納するコメントを入力します。

ヒント 変更を廃棄し、[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。これで、[Event Action Filters] タブのリストに新規イベント アクション フィルタが表示されます。

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、リストで選択して、[Edit] をクリックします。

ステップ 24 必要な変更を行います。

ヒント 変更を廃棄して、[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。これで、[Event Action Filters] タブのリストに編集したイベント アクション フィルタが表示されます。

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、リストで選択して、[Delete] をクリックします。

[Event Action Filters] タブのリストにイベント アクション フィルタが表示されなくなります。

ステップ 27　イベント アクション フィルタをリストで上下に移動するには、選択してから、[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　[Apply] をクリックして、変更を適用し、改訂したコンフィギュレーションを保存します。

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の設定方法について説明します。次の事項について説明します。

[IPv4 Target Value Rating] タブ

（注）　IPv4 ターゲットの価値レーティングを追加、編集、または削除するには、管理者またはオペレータである必要があります。

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られた価値を示します。値には、[High]、[Low]、[Medium]、[Mission Critical]、または [No Value] があります。
- [Target IP Address]：ターゲットの価値レーティングを使用してプライオリティを指定するネットワーク資産の IP アドレスを示します。

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

[Add and 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値を割り当てることができます。値には、[High]、[Low]、[Medium]、[Mission Critical]、または [No Value] があります。
- [Target IPv4 Address(es)]：ターゲットの価値レーティングを使用してプライオリティを指定す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 IDM にログインします。

ステップ 2　[Configuration] > [Policies] > [IPS Policies] を選択します。

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　ペイン半分の [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　資産の新規グループにターゲットの価値レーティングを割り当てるには、次の手順を実行します。

a. [Target Value Rating (TVR)] ドロップダウン リストで、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、範囲内で最も小さいアドレス、その後にハイフンを入力してから、最も大きいアドレスを入力します。たとえば、10.10.2.1-10.10.2.30 です。

ヒント　変更を廃棄し、[Add 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。新規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、リストで選択して、[Edit] をクリックします。

ステップ 8　必要な変更を行います。

ヒント　変更を廃棄し、[Edit 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。これで、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、リストで選択して、[Delete] をクリックします。[Ipv4 Target Value Rating] タブのリストにネットワーク資産が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　[Apply] をクリックして、変更を適用し、改訂したコンフィギュレーションを保存します。

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の設定方法について説明します。次の事項について説明します。

[IPv6 Target Value Rating] タブ

（注）　IPv6 ターゲットの価値レーティングを追加、編集、または削除するには、管理者またはオペレータである必要があります。

（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 イベント アクションまたはレート制限イベント アクションを指定してシグニチャを設定し、IPv6 トラフィックによってトリガーされた場合、アラートは生成されますが、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られた価値を示します。値には、[High]、[Low]、[Medium]、[Mission Critical]、または [No Value] があります。
- [Target IP Address]：ターゲットの価値レーティングを使用してプライオリティを指定するネットワーク資産の IP アドレスを示します。

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

[Add and 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値を割り当てることができます。値には、[High]、[Low]、[Medium]、[Mission Critical]、または [No Value] があります。
- [Target IPv6 Address(es)]：ターゲットの価値レーティングを使用してプライオリティを指定す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。範囲内の 2 番目の IPv6 アドレスは、最初の IPv6 アドレス以上でなければなりません。

（注） IPv6 アドレスは、16 進数で表される 128 ビットで、コロンで区切られた 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て、二重のコロン（::）を使用して中央のゼロ化グループを表すことができます。アドレスは、2001:db8 プレフィクス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 イベント アクションまたはレート制限イベント アクションを指定してシグニチャを設定し、IPv6 トラフィックによってトリガーされた場合、アラートは生成されますが、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 IDM にログインします。

ステップ 2　[Configuration] > [Policies] > [IPS Policies] を選択します。

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　ペイン半分の [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　資産の新規グループにターゲットの価値レーティングを割り当てるには、次の手順を実行します。

a. [Target Value Rating (TVR)] ドロップダウン リストで、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。範囲内の 2 番目の IPv6 アドレスは、最初の IPv6 アドレス以上でなければなりません。

（注） IPv6 アドレスは、16 進数で表される 128 ビットで、コロンで区切られた 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て、二重のコロン（::）を使用して中央のゼロ化グループを表すことができます。アドレスは、2001:db8 プレフィクスで始める必要があります。

ヒント　変更を廃棄し、[Add 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。新規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、リストで選択して、[Edit] をクリックします。

ステップ 8　必要な変更を行います。

ヒント　変更を廃棄し、[Edit 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。これで、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、リストで選択して、[Delete] をクリックします。[IPv6 Target Value Rating] タブのリストにネットワーク資産が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　[Apply] をクリックして、変更を適用し、改訂したコンフィギュレーションを保存します。

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。次の事項について説明します。

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、false positive 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]：OS ホスト マップを設定できます。これは学習した OS マップに優先します。
- [Computation of attack relevance rating and risk rating]：センサーは、OS 情報を使用して、ターゲット ホストに対する攻撃シグニチャの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 からインポートしたホスト 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. 設定した OS マップ：入力する OS マップ。設定した OS マップは、イベント アクション規則ポリシーにあり、1 つ以上の仮想センターに適用できます。

   （注）　同じ IP アドレスに複数のオペレーティング システムを指定できます。リストで最後のオペレーティング システムは、一致するオペレーティング システムです。

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された 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、CSA MC は唯一の外部データ 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は、機能させるために設定する必要はありません。IPS には、シグニチャごとにデフォルトの脆弱な OS リストが用意されており、パッシブ分析は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の次の側面を設定できます。

- [Define OS maps]：重要なシステムで実行中の OS の ID を定義するよう OS マップを設定することを推奨します。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。
- [Limit the attack relevance rating calculation to a specific IP address range]：これは、攻撃関連性レーティングの計算を、保護されたネットワークの IP アドレスに制限します。
- [Import OS maps]：OS マップをインポートすると、パッシブ分析によって行った OS ID の学習レートと忠実度を加速するためのメカニズムが提供されます。CSA MC などの外部製品インターフェイスがある場合、そこから OS ID をインポートできます。
- [Define event action rules filters using the OS relevance value of the target]：これは、OS 関連性だけに関するアラートをフィルタリングする方法を提供します。
- [Disable passive analysis]：センサーが新規 OS マップを学習しないようにします。
- [Edit signature vulnerable OS lists]：脆弱な OS リストは、各シグニチャに対して脆弱な OS タイプを指定します。デフォルトの [General OS] は、脆弱な 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）　設定した OS マップを追加、編集、および削除するには、管理者またはオペレータである必要があります。

[OS Identifications] タブを使用して、OS ホスト マップを設定します。これは学習した OS マップに優先します。[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、管理者は次のように定義できます（表 6-1）。

表 6-1　設定した 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、センサーはパッシブ OS 分析を実行できます。
- [Restrict Attack Relevance Ratings (ARR) to these IP addresses] : 特定の IP アドレスへの OS タイプのマッピングを設定して、センサーでその IP アドレスの攻撃関連性レーティングを計算できます。
- [Configured OS Maps] : 設定した OS マップの属性を表示します。
  - [Name] : 設定した OS マップに付ける名前。
  - [Active] : 設定したこの OS マップがアクティブか非アクティブか。
  - [IP Address] : 設定したこの OS マップの IP アドレス。
  - [OS Type] : 設定したこの OS マップの OS タイプ。

[Add and Edit Configured OS Map] ダイアログボックスのフィールド定義

[Add and 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] : 設定したこの OS マップの名前。
- [Active] : 設定した OS マップをアクティブにするか非アクティブにするかを選択できます。
- [IP Address] : 設定したこの OS マップに関連付けられた IP アドレス。設定した OS マップ（および設定した OS マップだけ）の IP アドレスを IP アドレス セットと IP アドレスの範囲にできます。次に、設定した OS マップで有効なすべての IP アドレス値を示します。
  - 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いずれかの OS タイプを選択できます。
  - 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

設定した OS マップの追加、編集、削除、および移動

設定した 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 IDM にログインします。

ステップ 2　[Configuration] > [Policies] > [IPS Policies] を選択します。

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　ペイン半分の [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、設定した 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、設定したこの 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 にマップするホストの IP アドレスを入力します。たとえば、形式 10.10.5.5,10.10.2.1-10.10.2.30 を使用します。

ステップ 8　[OS Type] ドロップダウン リストで、IP アドレスにマップする OS を選択します。

ヒント　変更を廃棄して、[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。新たに設定した 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する必要があります。そうしないと、[Add Configured OS Map] ダイアログボックスで設定した値に関係なく、設定したどの OS マップもイネーブルになりません。

ステップ 11　設定した OS マップを編集するには、リストで選択して、[Edit] をクリックします。

ステップ 12　必要な変更を行います。

ヒント　変更を廃棄し、[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。編集した設定済みの 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する必要があります。そうしないと、[Edit Configured OS Map] ダイアログボックスで設定した値に関係なく、設定したどの OS マップもイネーブルになりません。

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

ステップ 16　設定した OS マップをリスト内で上下に移動するには、選択して、[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　[Apply] をクリックして、変更を適用し、改訂したコンフィギュレーションを保存します。

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。次の事項について説明します。

[Event Variables] タブ

（注）　イベント変数を追加、編集、または削除するには、管理者またはオペレータである必要があります。

（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 イベント アクションまたはレート制限イベント アクションを指定してシグニチャを設定し、IPv6 トラフィックによってトリガーされた場合、アラートは生成されますが、アクションは実行されません。

イベント変数を作成してから、これらの変数をイベント アクション フィルタで使用できます。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。変数の値を変更すると、その変数を使用するすべてのフィルタが新規の値で更新されます。

（注）　変数の前にはドル記号（$）を付けて、ストリングではなく変数を使用することを示す必要があります。

一部の変数は、シグニチャ システムで必要であるため削除できません。変数が保護されている場合は、編集用に選択できません。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は、完全な IP アドレスまたは範囲あるいは範囲セットを指定します。

- 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 進数で表される 128 ビットで、コロンで区切られた 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て、二重のコロン（::）を使用して中央のゼロ化グループを表すことができます。アドレスは、2001:db8 プレフィクス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 グループに適用する IP アドレス空間があり、そのグループに Windows システムがない場合は、そのグループに対する Windows ベースの攻撃については心配せずに、エンジニアリング グループの IP アドレス空間にする変数を設定できます。その後、この変数を使用して、このグループの Windows ベースの攻撃をすべて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]：この変数に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示します。
- [Value]：この変数によって表される値を追加できます。

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

[Add and 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]：この変数に名前を割り当てることができます。
- [Type]：変数を IPv4 または IPv6 アドレスとして示します。
  - [address]：IPv4 アドレスの場合は、完全な IP アドレスまたは範囲あるいは範囲セットを使用します。
  - [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 進数で表される 128 ビットで、コロンで区切られた 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て、二重のコロン（::）を使用して中央のゼロ化グループを表すことができます。アドレスは、2001:db8 プレフィクス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、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 イベント アクションまたはレート制限イベント アクションを指定してシグニチャを設定し、IPv6 トラフィックによってトリガーされた場合、アラートは生成されますが、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 IDM にログインします。

ステップ 2　[Configuration] > [Policies] > [IPS Policies] を選択します。

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　ペイン半分の [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）　有効な名前は、数字と英字だけを含むことができます。ハイフン（-）または下線（_）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]、または IPv6 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 アドレスの場合は、完全な IP アドレスまたは範囲あるいは範囲セットを指定します。次に例を示します。

- 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 進数で表される 128 ビットで、コロンで区切られた 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て、二重のコロン（::）を使用して中央のゼロ化グループを表すことができます。アドレスは、2001:db8 プレフィクスで始める必要があります。

ヒント　変更を廃棄し、[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。新規変数が、[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、リストで選択して、[Edit] をクリックします。

ステップ 10　必要な変更を行います。

ヒント　変更を廃棄して、[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。これで、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、リストで選択して、[Delete] をクリックします。[Event Variables] タブのリストにイベント変数が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　[Apply] をクリックして、変更を適用し、改訂したコンフィギュレーションを保存します。

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。次の事項について説明します。

[Risk Category] タブ

（注）　リスク レベルを追加および編集するには、管理者でなければなりません。

[Risk Category] タブで、事前定義済みのリスク 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範囲にリンクします。範囲が連続するように、カテゴリの下限しきい値を指定します。上限カテゴリは、次に高いカテゴリまたは 100 のいずれかです。

その後、脅威をレッド、イエロー、グリーンというカテゴリにグループ化できます。これらのレッド、イエロー、グリーン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）　事前定義済みのリスク カテゴリは削除できません。

レッド、イエロー、グリーン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、レッドが最も重大です。しきい値を変更すると、リスク カテゴリと同じ範囲を持つイベント アクション オーバーライドは、新しい範囲を反映するよう変更されます。

新規カテゴリは、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。事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の数。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の数値定量化を表す 0 ～ 100 の範囲です。
- [Network Security Health Statistics]：レッド、イエロー、グリーンのしきい値の数をリストします。全体的なネットワーク セキュリティ値は、最小のセキュリティ値を表します（グリーンが最も安全性が高く、レッドが最も低い）。次の色しきい値は、[Home] ペインの [Sensor Health gadget] を参照します。
  - Red Threat Threshold
  - Yellow Threat Threshold
  - Green Threat Threshold

[Add Risk Level]/[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 カテゴリが連続するように、カテゴリの下限しきい値だけを指定または変更します。上限しきい値は、次に高いカテゴリまたは 100 のいずれかです。
- [Active]：このリスク レベルをアクティブにできます。

リスク カテゴリの追加、編集、および削除

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 IDM にログインします。

ステップ 2　[Configuration] > [Policies] > [IPS Policies] を選択します。

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　ペイン半分の [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、レッド、イエロー、グリーン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　変更を廃棄して、[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。新規リスク 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、リストで選択して、[Edit] をクリックします。

ステップ 10　必要な変更を行います。

ヒント　変更を廃棄し、[Edit 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 11　[OK] をクリックします。これで、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、リストで選択して、[Delete] をクリックします。[Risk Category] タブのリストにリスク カテゴリが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　[Apply] をクリックして、変更を適用し、改訂したコンフィギュレーションを保存します。

一般設定

ここでは、一般設定を行う方法について説明します。次の事項について説明します。

[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必要があります。

Summarizer と Meta Event Generator を使用するかどうかなど、イベント アクション規則にグローバルに適用する一般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やイベント アクション フィルタを使用したり、一方向の TCP リセットをイネーブルにしたりできます。一方向の TCP リセットはインライン モードだけで動作し、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）　インライン センサーは、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するようになります。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、拒否した攻撃者の最大数、およびブロックを続ける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をイネーブルにします。これは、リスク レーティングを調整します。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。イネーブルにした任意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] :（インラインだけ）TCP ベースのアラートの Deny Packet Inline アクションで一方向の TCP リセットをイネーブルにします。これは、TCP リセットをアラートの攻撃対象に送信するため、攻撃対象の TCP リソースをクリアします。

- [Deny Attacker Duration] : 攻撃者インラインを拒否する秒数。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分数。有効な範囲は 0 ～ 10000000 です。デフォルトは 30 です。

- [Maximum Denied Attackers]：一度にシステム内で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。

一般設定

注意　一般設定オプションは、グローバル レベルだけで動作するため、オプションをイネーブルにすると、これらの機能のセンサー処理すべてに影響します。

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 IDM にログインします。

ステップ 2　[Configuration] > [Policies] > [IPS Policies] を選択します。

ステップ 3　[IPS Policies] ペインの上半分で、一般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　ペイン半分の [Event Action Rules] 部分で [General] タブをクリックします。

ステップ 5　Summarizer 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 のディセーブル化は、トラブルシューティングのためだけに行います。それ以外の場合は、サマライズのため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 のディセーブル化は、トラブルシューティングのためだけに行います。それ以外の場合は、すべての Meta エンジン シグニチャが機能するように、Meta Event Generator をイネーブルにします。

ステップ 7　脅威レーティングの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）　[General] ペインの [Use Event Action Filters] チェックボックスをオンにして、[Configuration] > [Policies] > [IPS Policies] > [Event Action Filters] ペインで設定したイベントアクションをアクティブにする必要があります。

ステップ 9　Deny Packet Inline アクションで一方向 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、攻撃者インラインを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分数を入力します。

ステップ 12　[Maximum Denied Attackers] フィールドに、一度に可能な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　[Apply] をクリックして、変更を適用し、改訂したコンフィギュレーションを保存します。