イベント アクション ルールの設定

（注） 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしますが、IPS はサポートが終了しているため、IPS の拡張機能はサポートされません。詳細については、EOL 通知を参照してください。

IPSイベントは、アラート、ブロック要求、ステータスメッセージ、またはエラーメッセージを含むIPSメッセージです。イベントアクションは、イベントに対するセンサーの応答です。イベントがフィルタリングされていない場合にだけ発生します。指定可能なイベントアクションは、TCP リセット、ホストのブロック、接続のブロック、IP ロギング、およびアラート トリガーパケットのキャプチャです。イベントアクションは、5.x よりも前の Cisco IPS バージョンではアラームと呼ばれていました。

IPS Event Actions フォルダで、センサーのイベント アクション処理コンポーネントの設定を指定します。これらの設定により、イベント検出時にセンサーが実行するアクションが定義されます。

（注） Security Manager の Event Action ポリシーに IPv6 アドレスは使用できません。Security Manager での IPv6 サポートの詳細については、Security Manager での IPv6 サポートを参照してください。

この章は次のトピックで構成されています。

IPS イベント アクション プロセスについて

IPS イベントアクション ルールは、イベント発生時にセンサーが実行するアクションを指示します。各シグニチャには実行される特定のアクションが設定されますが、実際に実行されるアクションはその他の要因にも依存します。

検査でシグニチャ イベントが識別されたときに実行される一般的なプロセスは次のとおりです。

1. シグニチャで指定されたアクションで、シグニチャ アラートが発生します。アラートのリスク レーティングが計算されます。

   リスクレーティングの計算方法の詳細については、Cisco.com で Cisco Intrusion Prevention System Device Manager 7.0 のインストールおよび使用法ガイド [英語] の「Calculating the Risk Rating」を参照してください。

   ターゲットの価値レーティングと OS マッピングを設定することにより、リスク レーティングに影響を与えることができます。IPS イベント アクション ネットワーク情報の設定（23 ページ）を参照してください。

2. **イベント アクション オーバーライド**ポリシーが処理されます。イベントのリスクレーティングがオーバーライド ルールと一致すると、オーバーライド ルールで識別されたアクションがシグネチャで定義されているアクションに**追加**されます。オーバーライドは、シグニチャで指定されているアクションに置き換わりません。

   オーバーライドの設定方法の詳細については、イベント アクション オーバーライドの設定 （17 ページ）を参照してください。

3. **イベント アクション フィルタ ポリシー**が処理されます。ルールがイベントに適用されると、ルールによってイベントからアクションが**取り除かれます**。このため、シグニチャ ポリシーまたはオーバーライド ルールに追加したアクションが、フィルタ ルールのいずれかによって削除されることがあります。

   フィルタ ルールの作成の詳細については、イベント アクション フィルタの設定 （6 ページ）を参照してください。

4. イベント アクションの設定 （32 ページ）で示すようにサマライズ機能をオフにしていないかぎり、イベントのサマライズが発生します。

5. アクションが実行されます。指定可能なアクションの説明については、[Edit Action]、[Add Action]、[Replace Action] ダイアログボックスを参照してください。

6. 拒否された攻撃者のリストが保持され、指定可能な設定に基づいて後続のアクセスが防止されます。デフォルト設定を変更する手順については、イベント アクションの設定 （32 ページ）を参照してください。

IPS イベント アクションについて

イベント アクション フィルタやオーバーライド、またはシグニチャの設定時に、ルールを満たしているイベントのアクションを指定します。シグニチャおよびオーバーライドの場合は、イベントに追加するアクションを指定します。フィルタの場合は、イベントから削除するアクションを指定します。

最も一般的なアクションは Produce Alert で、このアクションでは、Security Manager Event Viewer または CS MARS のようなネットワーク管理システムで参照できるアラートが生成されます。ただし、イベントに割り当て可能なアクションは非常に多様です。指定可能なアクションを調べる場合には、次の点に注意します。

- 多数のアクションで、実行される他のアクションに加えて、アラートが作成されます。各アクションの説明には、アラートが作成されるかどうかが記載されています。
- Cisco IOS IPS では、イベント アクション オーバーライドまたはフィルタ ルールに対して少数のアクションしかサポートされません。サポートされるアクションは、Deny Attacker Inline、Deny Connection Inline、Deny Packet Inline、Product Alert、および Reset TCP Connection です。
- 必ずしも、IPS ソフトウェア バージョンおよびデバイス タイプのすべての組み合わせで、すべてのアクションを使用できるわけではありません。アクションを選択する必要がある場合は常に、有効なアクションだけが選択可能になります。
- 拒否およびブロック アクションの場合は、イベント アクション設定ポリシーを使用して、アドレスまたはパケットが拒否される期間を設定します。詳細については、イベント アクションの設定 （32 ページ）を参照してください。

次の表に、指定可能なアクションの説明を示します。

表 *1 : IPS* イベント アクション

メニュー コマンド	説明
Deny Attacker Inline	指定された期間、この攻撃者のアドレスからの、現在のパケットおよび将来のパケットを終了します。 IPS は、インライン モードで動作している必要があります。 Cisco IOS IPS デバイスの場合、遮断時間が経過するまで攻撃者からルータへの接続は確立されません。 **ヒント** これは最も厳しい拒否アクションです。単一の攻撃者アドレスからの現在および将来のパケットが拒否されます。IPS アプライアンスおよびサービス モジュールの場合、IPS Device Manager を使用すると、拒否された攻撃者のリストを表示したり、必要に応じてリストをクリアしたりできます。

メニュー コマンド	説明
Deny Attacker/Service Pair Inline	指定された期間、この攻撃者のアドレスと攻撃対象のポートのペアについては、現在のパケットおよび将来のパケットを送信しません。 IPS は、インライン モードで動作している必要があります。
Deny Attacker/Victim Pair Inline	指定された期間、この攻撃者と攻撃対象のアドレスのペアについては、現在のパケットおよび将来のパケットを送信しません。 IPS は、インライン モードで動作している必要があります。
Deny Connection Inline	TCP フローの現在のパケットおよび将来のパケットを終了します。攻撃者からのその他の接続は確立されます。 IPS は、インライン モードで動作している必要があります。
Deny Packet Inline	パケットを終了します。 IPS は、インライン モードで動作している必要があります。 Cisco IOS IPS デバイスの場合、このアクションにより、リセットを送信しないでパケットが廃棄されます。「drop と reset」はアラームとともに使用することを推奨します。 **ヒント** IPS アプライアンスおよびサービス モジュールの場合、このアクションを高リスク イベントに追加するイベント アクション オーバーライドがあります。このオーバーライドは削除できません。使用しない場合は、オーバーライドをディセーブルにします。詳細については、イベント アクション オーバーライドの設定 （17 ページ）を参照してください。
Log Attacker Packets	攻撃者のアドレスが含まれているパケットに対する IP ロギングを開始し、アラートを送信します。このアクションによって、Produce Alert が選択されていない場合でも、アラートがイベント ストアに書き込まれます。
Log Pair Packets	攻撃者と攻撃対象のアドレスのペアが含まれているパケットに対する IP ロギングを開始します。このアクションによって、Produce Alert が選択されていない場合でも、アラートがイベント ストアに書き込まれます。
Log Victim Packets	攻撃対象のアドレスが含まれているパケットに対する IP ロギングを開始し、アラートを送信します。このアクションによって、Produce Alert が選択されていない場合でも、アラートがイベント ストアに書き込まれます。

メニュー コマンド	説明
Modify Packet Inline	エンドポイントによるパケットの処理に関するあいまいさを取り除くために、パケット データを変更します。 ヒント　このオプションは、イベント アクション オーバーライドまたはフィルタ ルールでは使用できません。シグニチャでは使用できます。
Product Alert	イベントをアラートとしてイベント ストアに書き込みます。Cisco IOS IPS デバイスの場合、syslog または SDEE を介して通知が送信されます。 （注）　Produce Alert イベント アクションは、グローバル相関によってイベントのリスク レーティングが増加し、Deny Packet Inline または Deny Attacker Inline のいずれかのイベント アクションが追加されたときに、イベントに追加されます。
Produce Verbose Alert	攻撃パケットの符号化されたダンプをアラートに含めます。このアクションによって、Produce Alert が選択されていない場合でも、アラートがイベント ストアに書き込まれます。
Request Block Connection	この接続をブロックする要求を送信します。ブロッキング デバイスは、このアクションを実行するように設定されている必要があります。詳細については、IPS のブロッキングおよびレート制限の設定を参照してください。
Request Block Host	この攻撃者ホストをブロックする要求を送信します。ブロッキング デバイスは、このアクションを実行するように設定されている必要があります。
Request Rate Limit	レート制限を実行するレート制限要求を送信します。レート制限デバイスは、このアクションを実行するように設定されている必要があります。
Request SNMP Trap	センサーが設定済みのトラップ宛先に SNMP トラップ通知を送信することを要求します。このアクションを実行すると、Produce Alert が選択されていない場合でも、アラートが書き込まれます。トラップが実際に送信されるようにするには、センサーに SNMP を設定しておく必要があります。詳細については、SNMP の設定を参照してください。
TCP 接続のリセット	TCP リセットを送信して、TCP フローをハイジャックし、終了します。リセットは、発信元アドレスと宛先アドレスの両方に送信されます。Reset TCP Connection は、ハーフオープン SYN 攻撃などの単一の接続を分析する TCP シグニチャでだけ機能します。スイープまたはフラッドに対しては機能しません。

関連項目

- イベント アクション フィルタの設定　（6 ページ）

• イベント アクション オーバーライドの設定 （17 ページ）
• シグニチャの設定

イベント アクション フィルタの設定

特定のアクションをイベントから削除するか、または、イベント全体を破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。

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。フィルタ ルールを設定する前に、イベント アクション フィルタ ルールの管理に関するヒント （8 ページ）を参照してください。

（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。

関連項目

• IPS イベント アクションについて （3 ページ）

ステップ 1 次のいずれかを実行して、Event Action Filters ポリシーを開きます。

- （デバイス ビュー）ポリシー セレクタから [IPS] > [イベント アクション（Event Actions）] > [イベント アクション フィルタ（Event Action Filters）] を選択します。
- （ポリシー ビュー、IPS アプライアンスおよびサービス モジュール）[IPS] > [イベント アクション（Event Actions）] > [イベント アクション フィルタ（Event Action Filters）] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。
- （ポリシー ビュー、Cisco IOS IPS デバイス）[IPS（ルータ）（IPS (Router)）] > [イベント アクション（Event Actions）] > [イベント アクション フィルタ（Event Action Filters）] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。

テーブルに、セクションごとに分類された既存のフィルタ ルールが表示されます。[Local] セクションは、（デバイス ビューで）選択したデバイスに定義されているルール用のセクションです。共有または継承されたポリシーの場合、必須ルールおよびデフォルト ルール用のセクションもあります。このポリシーの内容の詳細については、[Event Action Filters] ページ （9 ページ）を参照してください。

ステップ 2 フィルタ ルールを作成する行を選択して [行の追加（Add Row）] ボタンをクリックするか、または行を右クリックして [行の追加（Add Row）] を選択します。この操作により、[Add Filter Item] ダイアログボック

スが開きます。このダイアログボックスのオプションの詳細については、[Add Filter Item]/[Edit Filter Item] ダイアログボックス （12 ページ）を参照してください。

ヒント

- 行を選択しなかった場合、新しいルールはローカル範囲の最後に追加されます。
- 既存の行を選択して、行全体（[行の編集（Edit Row）] ボタンをクリックする）または特定のセルを編集することもできます。特定のセルを編集するには、セルを右クリックして、コンテキストメニューの一番上からそのセルに関連する**編集**コマンドを選択します。
- ルールを選択して [行の削除（Delete Row）] ボタンをクリックすると、そのルールを削除できます。
- フィルタ ルールのリスト全体を Comma-Separated Values（CSV; カンマ区切り値）ファイルにエクスポートできます。[ファイルへのエクスポート（Export to File）] をクリックして Security Manager サーバーの適切なフォルダにナビゲートし、デフォルト名を使用しない場合はファイル名を変更して [保存（Save）] をクリックします。

ステップ 3 フィルタ ルールを設定します。一般的に設定が必要な重要項目は次のとおりです。フィールドの設定に関する詳細およびここで説明していないフィールドの情報については、[Add Filter Item]/[Edit Filter Item] ダイアログボックス （12 ページ）を参照してください。

- [Name]：ルールの名前を入力する必要があります。意味のある名前を使用してください。
- [Signature, Subsignature ID]：フィルタをすべてのシグニチャに適用する必要がある場合は、デフォルト値を使用します。特定のシグニチャをターゲットにする場合は、そのシグニチャおよびサブシグニチャの ID を入力します。これらの値は、シグニチャ ポリシーでシグニチャを検索することで取得できます（[Signatures] ページを参照）。
- [Attacker and Victim Addresses and Ports]：だれが攻撃しているのか、または攻撃対象はだれかに関係なくフィルタを適用する必要がある場合は、デフォルト値を使用します。攻撃者または攻撃対象に固有のフィルタを作成する場合は、適切なアドレスおよびポートと一致するようにこれらのフィールドを更新します。
- [Risk Rating]：この値は、多くの場合変更が必要です。フィルタは、ここで設定した最小～最大範囲内のイベントに適用されます。デフォルト値（0-100）を指定すると、すべてのイベントにフィルタ ルールが適用されます。特定のシグニチャ ID を設定した場合、レーティングはそのシグニチャのイベントにだけ適用されます（この場合、デフォルトのリスク レーティングをそのまま使用できることがあります）。

たとえば、90 ～ 100 などの高リスク イベントだけをターゲットにできます。

- [Actions to Subtract]：イベントから除外するアクションを選択します。複数のアクションを選択するには、Ctrl を押しながらクリックします。実際にはイベントに割り当てられていないアクションを選択した場合、フィルタ ルールは基本的にはイベントに何の影響も与えません。アクションの詳細については、[Edit Action]、[Add Action]、[Replace Action] ダイアログボックスを参照してください。
- [Stop on Match]：このフィルタ ルールを停止ルールとして定義するかどうかを指定します。この設定によって、イベント アクション フィルタ ルール テーブルに残っているルールを処理する方法が決まります。

- このオプションを選択し、イベントがルールの条件を満たす場合、このルールは、イベントに対してテストされる最後のルールとなります。このルールによって識別されたアクションはイベントから削除され、デバイスは、イベントに割り当てられている残りのすべてのアクションを実行します。
- このオプションを選択していない場合、このフィルタ ルールの条件を満たすイベントも、イベント アクション フィルタ テーブル内の後続のルールと比較されます。後続のルールは、すべてのルールがテストされるか、またはイベントが停止ルールに一致するまでテストされます。

フィルタルールの定義が完了したら、[OK] をクリックします。

ステップ 4 適切な行を選択しないでルールを追加した場合は、追加されたルールを選択し、上下の矢印ボタンを使用して適切な位置にルールを移動します。停止ルールが、停止よりも前に適用させる他のルールのあとに配置されていることを確認します。

イベント アクション フィルタ ルールの管理に関するヒント

次に、イベント アクション フィルタ ルールを効果的に管理するために役立つヒントを示します。

- ディセーブルなルールには、テーブルの行にハッシュ マークが重なって表示されます。ルールのイネーブル/ディセーブルステータスを変更するには、ルールを右クリックし、[有効化（Enable）] または [無効化（Disable）] を必要に応じて選択します。ルールの編集時にステータスを変更することもできます。

ルールを使用停止にする場合はルールをディセーブルにするのが有効ですが、将来、そのルールの使用を再開する可能性があります。ルールを再作成しなくて済むように、ディセーブルにしたルールはそのままテーブル内に保持されます。

- 既存のルールの場合、セルを右クリックしてコンテキストメニューの一番上の部分から適切な編集コマンドを選択することで、イベント アクション フィルタ ルール テーブルから直接フィールドの大部分を編集できます。たとえば、[攻撃者のポート（Attacker Ports）] セルを右クリックし、[攻撃者のポートの編集（Edit Attacker Ports）] を選択します。

これらの右クリック コマンドの多くが、選択したプロパティだけを含む [Edit Filter Item] ダイアログボックスのバージョンです。その他のコマンドは値を変更するだけか、あるいは追加または削除する値を選択するためのサブメニューを開きます。たとえば、[Action]セルを右クリックすると、次の 4 つのコマンドが表示されます。

- [アクションに追加（Add to Actions）]：アクションのリストからアクションを選択して、すでにルールに定義されているアクションに追加します。
- [アクションから削除（Delete from Actions）]：ルールに定義されているアクションのリストからアクションを選択して、ルールから削除します。
- [アクションを置換（Replace Actions With）]：アクションのリストからアクションを選択して、ルールに定義されているアクションを完全に置き換えます。

- [アクションの編集（Edit Actions）]：ルールのすべてのアクションを選択できるダイアログボックスが開きます。選択した内容でセルの内容が置き換わります。

- フィルタルールは順序リストとして設定されますが、ルールは上から下へ順に処理および適用されるものの、「最初に一致したもの勝ち」リストとして処理されるわけではありません。各ルールには Stop プロパティがあり、ルールは停止ルールであるか停止ルールでないかのどちらかになります。処理は、イベントが停止ルールと一致した場合にだけ終了します。イベントが非停止ルールと一致した場合、そのイベントは後続のフィルタ ルールと比較されます。このように、複数のフィルタ ルールを 1 つのイベントに適用できます。停止ルールを作成する場合は、イベントに対して処理される他のすべてのルールの下に停止ルールを配置するようにします。

停止ルールを定義しなかった場合、各イベントがすべてのフィルタ ルールと比較され、一致したすべてのルールが上から下に順にイベントに適用されます。

- イベント アクション フィルタ ルール ポリシーは、継承が可能です。そのため、すべてのデバイスで共有するフィルタ ルールが含まれる共有ポリシーをポリシー ビューで設定し、（デバイス ビューで）そのルールを各デバイスに継承させ、デバイス ビューで各デバイスに固有のローカル フィルタ ルールを設定することが可能です。ポリシーを継承する方法の詳細については、次を参照してください。
  - 新しい共有ポリシーの作成
  - 継承と割り当て
  - ルールの継承または継承の解除

関連項目

- イベント アクション フィルタの設定 （6 ページ）
- [Event Action Filters] ページ （9 ページ）

[Event Action Filters] ページ

[Event Actions Filters] ページを使用して、イベント アクション フィルタ ルールを設定します。フィルタ ルールでは、特定のアクションをイベントから削除することや、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。

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。

イベント アクション フィルタ ルールを設定する前に、次の項を参照してください。

- イベント アクション フィルタの設定 （6 ページ）

- イベント アクション フィルタ ルールの管理に関するヒント （8 ページ）
- IPS イベント アクションについて （3 ページ）

ヒント ディセーブルなルールには、テーブルの行にハッシュ マークが重なって表示されます。ルールのイネーブル/ディセーブルステータスを変更するには、ルールを右クリックし、[有効化（Enable）] または [無効化（Disable）] を必要に応じて選択します。ルールの編集時にステータスを変更することもできます。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから [IPS] > [イベントアクション（Event Actions）] > [イベントアクションフィルタ（Event Action Filters）] を選択します。
- （ポリシービュー、IPS アプライアンスおよびサービスモジュール）[IPS]>[イベントアクション（Event Actions）]>[イベントアクションフィルタ（Event Action Filters）] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。
- （ポリシービュー、Cisco IOS IPS デバイス）[IPS（ルータ）（IPS (Router)）] > [イベントアクション（Event Actions）]>[イベントアクションフィルタ（Event Action Filters）] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 2 : [Event Action Filters] ページ

要素	説明
名前	フィルタ ルールの名前。
Active	シグニチャがアクティブかどうかを示します。 このセルは Cisco IOS IPS ポリシーでは使用できません。
ID（IDs）	このルールを適用するシグニチャ ID。
Subs	サブシグニチャ ID。

要素	説明
攻撃者（Attackers）	フィルタルールをトリガーする攻撃者の IP アドレスで、ホストアドレス、アドレス範囲（IPv4 の場合は 0.0.0.0-255.255.255.255 など、IPv6 の場合は ::0-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF など）、またはネットワーク/ホストポリシーオブジェクトを指定できます。 **ヒント** ネットワーク/ホストオブジェクトを使用している場合は、そのオブジェクトを右クリックし、[コンテンツの表示（Show Contents）] を選択すると、そのオブジェクトの内容を表示できます。 **（注）** IPv4 オブジェクトと IPv6 オブジェクトを同じ名前で作成しないでください。作成すると展開が失敗します。
Attack Ports	フィルタをトリガーする攻撃者ホストによって使用されるポート。
Victims	フィルタルールをトリガーする攻撃対象の IP アドレスで、ホストアドレス、アドレス範囲（IPv4 の場合は 0.0.0.0-255.255.255.255 など、IPv6 の場合は ::0-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF など）、またはネットワーク/ホストポリシーオブジェクトを指定できます。 **ヒント** ネットワーク/ホストオブジェクトを使用している場合は、そのオブジェクトを右クリックし、[コンテンツの表示（Show Contents）] を選択すると、そのオブジェクトの内容を表示できます。 **（注）** IPv4 オブジェクトと IPv6 オブジェクトを同じ名前で作成しないでください。作成すると展開が失敗します。
Victim Ports	フィルタをトリガーする攻撃者ホストによってターゲットにされるポート。
アクション（Actions）	フィルタがトリガーされたときに、イベントから削除する必要があるアクション。
RR	このイベントアクションフィルタをトリガーするリスク レーティング範囲。 リスクレーティングの計算方法の詳細については、Cisco.com で Cisco Intrusion Prevention System Device Manager 7.0 のインストールおよび使用法ガイド [英語] の「Calculating the Risk Rating」を参照してください。
停止（Stop）	これが停止ルールであるかどうかを指定します。[Yes] の場合、イベントがこのルールの条件を満たすと、フィルタがイベントに適用されますが、イベントはイベントアクションフィルタ ルール ポリシー内の残りのルールに対してはテストされません。

要素	説明
[Export to File] ボタン	イベント アクション フィルタ要約を Comma-Separated Values（CSV; カンマ区切り値）ファイルにエクスポートするには、このボタンをクリックします。Security Manager サーバ上のフォルダを選択し、ファイル名を指定するように要求されます。
[Up Row] ボタンと [Down Row] ボタン（矢印アイコン）	選択したルールを範囲内で上下に移動するには、これらのボタンをクリックします。 フィルタ ルールは、イベントごとに上から下に順に処理されます。イベントの条件がフィルタに定義されている条件と一致し、さらにフィルタの [Stop] フィールドが [Yes] に設定されている場合、そのフィルタは適用され、その他のフィルタは検討されません。停止ルールが、イベントに適用させる他のルールのあとに配置されていることを確認します。 テーブルでは、一般的なルールの前により限定的なルールを配置する必要があります。
[Add Row] ボタン	[Add Filter Item] ダイアログボックス（[Add Filter Item]/[Edit Filter Item] ダイアログボックス （12 ページ）を参照）を使用して選択したテーブルの行のあとにフィルタ ルールを追加するには、このボタンをクリックします。行を選択しなかった場合は、ローカル範囲の最後にルールが追加されます。
[Edit Row] ボタン	選択したルールを編集するには、このボタンをクリックします。セルを右クリックして適切な編集コマンドを選択する方法でも、個々のセルを編集できます。
[Delete Row] ボタン	選択したルールを削除するには、このボタンをクリックします。 **ヒント** ルールを削除する代わりに、ルールを右クリックして [無効化（Disable）] を選択できます。これにより、ルールは使用できなくなりますが、あとで再び使用する場合に備えてテーブル内に保持されます。

[Add Filter Item]/[Edit Filter Item] ダイアログボックス

[Add Filter Item]/[Edit Filter Item] ダイアログボックスを使用して、イベント アクション フィルタ ルールを設定します。

ヒント　既存のルールの場合、セルを右クリックしてコンテキスト メニューの一番上の部分から適切なコマンドを選択することで、イベント アクション フィルタ ルール テーブルから直接これらのフィールドの大部分を編集できます。たとえば、[攻撃者のポート（Attacker Ports）] セルを右クリックし、[攻撃者のポートの編集（Edit Attacker Ports）] を選択します。これらの右クリック コマンドの多くが、選択したプロパティだけを含む [Edit Filter Item] ダイアログボックスのバージョンです。これらのコンテキスト編集ダイアログボックスのヘルプを参照するには、下部のテーブル内でプロパティの説明を探します。

ナビゲーション パス

[イベントアクションフィルタ（Event Action Filters）] ページ（[Event Action Filters] ページ（9 ページ）を参照）から、[列の追加（Add Row）] ボタンをクリックするか、またはルールをフィルタして、 [行の編集（Edit Row）] ボタンをクリックします。

関連項目

- イベント アクション フィルタの設定 （6 ページ）
- イベント アクション フィルタ ルールの管理に関するヒント （8 ページ）

フィールド リファレンス

表 3 : [Add Filter Item]/[Edit Filter Item] ダイアログボックス

要素	説明
Active [有効（Enabled）] （[Active] は Cisco IOS IPS デバイスには適用されません）	フィルタ ルールがアクティブであるかどうか、およびイネーブルであるかどうかを示します。アクティブとは、フィルタがフィルタ リストに含まれており、イベントのフィルタリングで実行されることを意味します。デフォルトでは、ルールはアクティブかつイネーブルであり、このことはイベントが処理されるときにそのルールが使用されることを意味します。 **ヒント** • フィルタがアクティブだがイネーブルではない場合、そのフィルタは順序リストに含まれたままになります。つまり、処理されますが、使用されません。 • フィルタがアクティブではない場合、そのフィルタはフィルタの順序に含まれません。つまり、処理されません。 • ディセーブルにしたルールは、イベント アクション フィルタ テーブルに網掛けで表示されます。

要素	説明
名前	フィルタ ルールの名前。フィルタ名に使用できる文字は次のとおりです。 a-z、A-Z、0-9、-、.（ドットまたはピリオド）、:（コロン）、および_（下線）。
Signature IDs	フィルタ ルールを適用する数字のシグニチャ ID。単一のシグニチャ ID、カンマ区切りリスト、またはIDの範囲を入力できます。デフォルトでは、900 ～ 65535 の範囲のシグニチャにルールが適用されます。
サブシグニチャ ID	フィルタ ルールを適用する指定したシグニチャのサブシグニチャ ID。サブシグニチャ ID は広範なシグニチャをより詳細に識別しますが、すべてのシグニチャに使用されるわけではありません。 指定したシグニチャ ID に適したサブシグニチャ ID を入力するか、またはサブシグニチャ ID の範囲を入力します。デフォルト値は 0 ～ 255 の範囲です。
攻撃者の IPv4 アドレス	攻撃パケットを送信するホストの IP アドレス。単一のホスト IP アドレス、アドレス範囲、またはアドレスやアドレス範囲を識別するネットワーク/ホスト ポリシー オブジェクトの名前を指定できます。[選択（Select）] をクリックしてネットワーク/ホストオブジェクトをリストから選択するか、または新しいオブジェクトを作成します。 （注） IPv4 オブジェクトと IPv6 オブジェクトを同じ名前で作成しないでください。作成すると展開が失敗します。 デフォルト値はすべての IPv4 アドレスの範囲（0.0.0.0-255.255.255.255）です。
攻撃者の IPv6 アドレス	攻撃パケットを送信するホストの IP アドレス。単一のホスト IP アドレス、アドレス範囲、またはアドレスやアドレス範囲を識別するネットワーク/ホスト ポリシー オブジェクトの名前を指定できます。[選択（Select）] をクリックしてネットワーク/ホストオブジェクトをリストから選択するか、または新しいオブジェクトを作成します。 （注） IPv4 オブジェクトと IPv6 オブジェクトを同じ名前で作成しないでください。作成すると展開が失敗します。 デフォルト値は、すべての IPv6 アドレスの範囲（::0-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF）です。
Attacker Port	攻撃者ホストによって使用されるポート。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。 デフォルト値はすべてのポートの範囲（0-65535）です。

要素	説明
攻撃対象のIPv4アドレス	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。単一のホスト IP アドレス、アドレス範囲、またはアドレスやアドレス範囲を識別するネットワーク/ホスト ポリシー オブジェクトの名前を指定できます。[選択（Select）] をクリックしてネットワーク/ホストオブジェクトをリストから選択するか、または新しいオブジェクトを作成します。 （注） IPv4 オブジェクトと IPv6 オブジェクトを同じ名前で作成しないでください。作成すると展開が失敗します。 デフォルト値はすべての IPv4 アドレスの範囲（0.0.0.0-255.255.255.255）です。
攻撃対象のIPv6アドレス	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。単一のホスト IP アドレス、アドレス範囲、またはアドレスやアドレス範囲を識別するネットワーク/ホスト ポリシー オブジェクトの名前を指定できます。[選択（Select）] をクリックしてネットワーク/ホストオブジェクトをリストから選択するか、または新しいオブジェクトを作成します。 （注） IPv4 オブジェクトと IPv6 オブジェクトを同じ名前で作成しないでください。作成すると展開が失敗します。 デフォルト値は、すべての IPv6 アドレスの範囲（::0-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF）です。
攻撃対象のポート	攻撃されているホスト（攻撃パケットの受信者）のポート。これは、攻撃パケットの送信先のポートです。ポートの範囲を入力することもできます。 デフォルト値はすべてのポートの範囲（0-65535）です。
リスク レーティングの最小と最大	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）。デフォルト値は範囲全体（0 ～ 100）です。 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 フィルタのルールと比較して処理されます。
OS Relevance	アラートが、攻撃対象用として識別されている OS と関連があるかどうかを示します。指定可能な値は、[Not Relevant]、[Relevant]、[Unknown] のうちの 1 つ以上です。Ctrl を押しながらクリックすることで、複数の値を選択できます。デフォルトでは、すべての値が選択されます。 （注） [OS Relevance] は、IPS 6.x 以降のソフトウェアを実行しているアプライアンスおよびサービス モジュールだけに適用可能です。Cisco IOS IPS デバイスの場合、このフィールドは読み取り専用になり、編集はできません。IPS 5.x デバイスの場合、このフィールドは空白になります。
説明	ルールの目的に関する説明など、このフィルタに関連付けるユーザ コメント。

要素	説明
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。このリスト ボックスから 1 つ以上のアクションを選択できます。選択したすべてのアクションがイベントから削除されます。Ctrl を押しながらクリックすることで、複数の値を選択できます。指定可能なアクションの詳細については、[Edit Action]、[Add Action]、[Replace Action] ダイアログボックスを参照してください。 IOS IPS デバイスの場合、指定できるのは次の値だけです。 • [インラインで攻撃者を拒否（Deny Attacker Inline）] は、攻撃者の送信元 IP アドレスを完全にブロックします。遮断時間が経過するまで攻撃者からルータへの接続は確立されません。この時間は、イベント アクションの設定 （32 ページ）で説明されているように、Event Actions Settings ポリシーで設定できます。 • [インラインで接続を拒否（Deny Connection Inline）] は、攻撃者からの該当する TCP フローをブロックします。攻撃者からルータへのその他の接続は確立されます。 • [インラインでパケットを拒否（Deny Packet Inline）] は、リセットを送信せずにパケットを廃棄します。「drop と reset」はアラームとともに使用することを推奨します。 • [アラートを生成（Produce Alert）] は、syslog または SDEE を介して攻撃に関する通知を送信します。 • [TCP接続をリセット（Reset TCP Connection）] は、TCP ベースの接続に有効で、送信元アドレスおよび宛先アドレスの両方にリセットを送信します。たとえば、ハーフオープン SYN 攻撃の場合に、Cisco IOS IPS は TCP 接続をリセットできます。
% to Deny	攻撃者拒否機能で拒否するパケットのパーセンテージ。範囲は 0 ～ 100 です。デフォルトは 100% です。 （注） IOS IPS デバイスの場合、このフィールドは読み取り専用で、編集はできません。

要素	説明
Stop on Match	このフィルタ ルールを停止ルールとして定義するかどうかを指定します。この設定によって、イベント アクション フィルタ ルール テーブルに残っているルールを処理する方法が決まります。 • このオプションを選択し、イベントがルールの条件を満たす場合、このルールは、イベントに対してテストされる最後のルールとなります。このルールによって識別されたアクションはイベントから削除され、デバイスは、イベントに割り当てられている残りのすべてのアクションを実行します。 • このオプションを選択していない場合、このフィルタ ルールの条件を満たすイベントも、イベント アクション フィルタ テーブル内の後続のルールと比較されます。後続のルールは、すべてのルールがテストされるか、またはイベントが停止ルールに一致するまでテストされます。

イベント アクション オーバーライドの設定

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 のイベント アクション オーバーライドを作成し、そのリスク レーティング 85 ～ 100 を設定します。

ヒント アクション オーバーライドを使用できないようにする場合は、イベント アクションの設定 （32 ページ）の説明に従って、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。

関連項目

- IPS イベント アクションについて （3 ページ）

ステップ 1 次のいずれかを実行して、Event Action Overrides ポリシーを開きます。

- （デバイスビュー）ポリシーセレクタから [IPS] > [イベントアクション（Event Actions）] > [イベントアクションのオーバーライド（Event Action Overrides）] を選択します。

- （ポリシービュー、IPS アプライアンスおよびサービスモジュール）[IPS]>[イベントアクション（Event Actions）] > [イベントアクションのオーバーライド（Event Action Overrides）] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。
- （ポリシービュー、Cisco IOS IPS デバイス）[IPS（ルータ）（IPS (Router)）] > [イベントアクション（Event Actions）] > [イベントアクションのオーバーライド（Event Action Overrides）] を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。

テーブルに既存のオーバーライドが表示され、アクション、アクションが追加されるアラートのリスクレーティング、およびルールがイネーブルかどうかが示されます。ルールの順序は関係しません。アラートに適用されるすべてのオーバーライドによって、関連付けられたアクションが追加されます。

テーブルには、指定可能なアクションごとに最大で 1 つのエントリを含めることができます。

ステップ 2 目的のオーバーライドを設定します。

- 新しいオーバーライドを追加するには、テーブルの下の [行の追加（Add Row）]（+）ボタンをクリックし、[イベントアクションルールの追加（Add Event Action Rule）] ダイアログボックスに入力します。ダイアログボックスでは、追加するアクションを選択し、アクションに追加するアラートのレーティング範囲（90 ～ 100 など）を入力して、[OK] をクリックします。詳細については、[イベントアクションルールの追加または編集（Add or Edit Event Action Rule）] ダイアログボックス （19 ページ）を参照してください。

リスク レーティング範囲は、0 ～ 100 の値である必要があります。80-90 のように、範囲の最小値と最大値をハイフンで区切ります。

新しいオーバーライドを追加するときは、独自のリスクレーティングを定義するか、事前に定義されたリスク レーティング ポリシー オブジェクトを使用できます。バージョン 4.5 以降、Security Manager にはいくつかの事前定義されたリスク レーティング ポリシー オブジェクトがあります。

- [極めて高いリスク（Extreme Risk）]（90 ～ 100）
- [高リスク（High Risk）]（76 ～ 90）
- [中-高リスク（Medium-High Risk）]（61 ～ 75）
- [中リスク（Medium Risk）]（46 ～ 60）
- [中-低リスク（Medium-Low Risk）]（30 ～ 45）
- [低リスク（Low Risk）]（16 ～ 30）
- [非常に低いリスク（Very Low Risk）]（1 ～ 15）

これらの事前定義されたポリシーオブジェクトの詳細については、リスク評価ポリシーオブジェクトの構成 （20 ページ）を参照してください。

これらの事前定義されたポリシーオブジェクトは編集できませんが、ユーザーが定義した独自のポリシーオブジェクトを追加および編集できます。

- オーバーライドを編集するか、オーバーライドを無効にするか、またはリスクレーティングを変更するには、オーバーライドを選択して [行の編集（Edit Row）]（鉛筆）ボタンをクリックします。イベント アクションは変更できません。

（注） IPS デバイスが再検出されると、リスク レーティング ポリシー オブジェクトの値がインライン値に置き換えられます。たとえば、高リスクポリシーオブジェクト（80 ～ 89）をいずれかのイベントアクションに割り当ててデバイスに展開した場合、再検出後、そのポリシーオブジェクトの値はそのインライン値 80 ～ 89 に置き換えられます。

- オーバーライドを削除するには、オーバーライドを選択し、[行の削除（Delete Row）] ボタンをクリックします。

（注） IPS アプライアンスおよびサービスモジュールのポリシーには、Deny Packet Inline のオーバーライドがデフォルトで含まれており、これは削除できません。そのオーバーライドを使用しない場合は、ディセーブルにします。

- オーバーライドのリスト全体をカンマ区切り値（CSV）ファイルにエクスポートするには、[ファイルへのエクスポート（Export to File）] をクリックして Security Manager サーバーの適切なフォルダにナビゲートし、デフォルト名を使用しない場合はファイル名を変更して [保存（Save）] をクリックします。

[イベントアクションルールの追加または編集（Add or Edit Event Action Rule）] ダイアログボックス

[イベントアクションルールの追加（Add Event Action Rule）]/ [イベントアクションルールの編集（Edit Event Action Rule）]ダイアログボックスを使用して、バージョン 4.5 以降の Security Manager で使用できる事前定義されたリスク レーティング ポリシー オブジェクトの 1 つに基づいてイベントアクションルールを追加します。

ナビゲーション パス

[イベントアクションオーバーライド（Event Action Overrides）] ポリシーから、オーバーライドテーブルの下の [行の追加（Add Row）] ボタンをクリックするか、テーブル内の行を選択して [行の編集（Edit Row）] ボタンをクリックします。Event Action Overrides ポリシーを開く方法については、イベント アクション オーバーライドの設定 （17 ページ）を参照してください。

フィールド リファレンス

表 *4 : [*イベントアクションルールの追加または編集（*Add or Edit Event Action Rule***）*]* ダイアログボックス**

要素	説明
Risk Rating	バージョン 4.5 以降の Security Manager で使用できる、次の事前定義されたリスクレーティング ポリシー オブジェクトの 1 つ。 • 極めて高いリスク（90～100）（Extreme Risk (90-100)） • 高リスク （76～90）（High Risk (76-90)） • 中 - 高リスク（61-75）（Medium-High Risk (61-75)） • 中リスク（46～60）（Medium Risk (46-60)） • 中 - 低リスク（30～45）（Medium-Low Risk (30-45)） • 低リスク（16～30）（Low Risk (16-30)） • 非常に低いリスク（1～15）（Very Low Risk (1-15)） これらの事前定義されたリスク レーティング ポリシー オブジェクトのいずれかを使用する方法、または独自に定義する方法の詳細については、イベント アクション オーバーライドの設定 （17 ページ）を参照してください。
割り当て済み（Assigned）	特定のアクションが少なくとも 1 つのリスク レーティング ポリシー オブジェクトに割り当てられているかどうかを指定します。
アクション名	割り当てられたときに特定のリスクレーティングに対して実行されるアクション。
[有効（Enabled）]	特定のアクションがイネーブルかどうかを指定します。アクションを削除せずに一時的にディセーブルにするには、このオプションの選択を解除します。

リスク評価ポリシーオブジェクトの構成

[リスクレーティングポリシーオブジェクト（Risk Rating Policy Object）] ダイアログボックスを使用して、IPS のポリシーオブジェクトを設定します。7 つの事前定義されたポリシーオブジェクトがリスク評価に使用できます。独自に定義することもできます。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] > [すべてのオブジェクトタイプ（All Object Types）] を選択し、次に [オブジェクトタイプセレクタ（Object Type Selector）] から [リスクレーティング（Risk Rating）] を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集

（Edit Object）] を選択します。ただし、事前定義されたポリシーオブジェクトを編集することはできません。

[新規オブジェクト（New Object）] または [オブジェクトの編集（Edit Object）] のどちらを選択したかに応じて、[リスクレーティングの追加（ Add Risk Rating）] または [リスクレーティングの編集（Edit Risk Rating）] ダイアログボックスが表示されます。 [イベントアクションルールの追加または編集（Add or Edit Event Action Rule）] ダイアログボックス （19 ページ）を参照してください。

このトピックの残りの部分では、[リスクレーティングポリシーオブジェクト（Risk Rating Policy Object）] ダイアログボックスに表示されるフィールドについて説明します。

関連項目

- イベント アクション オーバーライドの設定 （17 ページ）
- [イベントアクションルールの追加または編集（Add or Edit Event Action Rule）] ダイアログボックス （19 ページ）

フィールド リファレンス

表 *5 : [*リスクレーティングポリシーオブジェクト（*Risk Rating Policy Object***）*]* ダイアログ ボックス**

要素	説明
名前	「高リスク」などの事前定義されたポリシーオブジェクトの名前、または定義したポリシーオブジェクトの名前。
範囲	数値範囲で表される、特定のポリシーオブジェクトのリスクレーティング。
カテゴリ	Cat-A ～ Cat-G を選択できます。 これは、オブジェクトに割り当てられたカテゴリです。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。
オーバーライド	このポリシーオブジェクトに IPS イベント アクション オーバーライドが設定されているかどうか
説明	提供できるテキストの説明。事前定義されたポリシーオブジェクトではなく、定義したポリシーオブジェクトに適用されます。
最後のチケット	このポリシーオブジェクトに使用された最後のチケット。
最終更新日	このポリシーオブジェクトが最後に変更された日付。

[リスク レーティングの追加または編集] ダイアログボックス

[リスクレーティングの追加または編集（Add or Edit Risk Rating）] ダイアログボックスを使用して、IPS リスクレーティングのポリシーオブジェクトを定義します。

ナビゲーション パス

[管理（Manage）] > [ポリシーオブジェクト（Policy Objects）] > [すべてのオブジェクトタイプ（All Object Types）] を選択し、次に [オブジェクトタイプセレクタ（Object Type Selector）] から [リスク評価（Risk Rating）] を選択します。作業領域内を右クリックしてから [新規オブジェクト（New Object）] を選択するか、行を右クリックしてから [オブジェクトの編集（Edit Object）] を選択します。ただし、事前定義されたポリシーオブジェクトを編集することはできません。

関連項目

- イベント アクション オーバーライドの設定 （17 ページ）
- [イベントアクションルールの追加または編集（Add or Edit Event Action Rule）] ダイアログボックス （19 ページ）

フィールド リファレンス

表 *6: [リスク レーティングの追加または編集] ダイアログボックス*

要素	説明
名前	「高リスク」などの事前定義されたポリシーオブジェクトの名前、または定義したポリシーオブジェクトの名前。
説明	提供できるテキストの説明。事前定義されたポリシーオブジェクトではなく、定義したポリシーオブジェクトに適用されます。
範囲	数値範囲で表される、特定のポリシーオブジェクトのリスクレーティング。
カテゴリ	オブジェクトに割り当てられたカテゴリ。カテゴリを使用すると、ルールとオブジェクトを分類および識別できます。カテゴリ オブジェクトの使用を参照してください。

要素	説明
デバイスごとに値のオーバーライドを許可 オーバーライド [編集（Edit）] ボタン	デバイス レベルでのオブジェクト定義の変更を許可するかどうか。詳細については、ポリシー オブジェクトの上書きの許可および個々のデバイスのポリシー オブジェクト オーバーライドについてを参照してください。 デバイスのオーバーライドを許可した場合は、[編集（Edit）] ボタンをクリックして、オーバーライドを作成、編集、および表示できます。[オーバーライド（Overrides）] フィールドには、このオブジェクトに対するオーバーライドを持つデバイスの数が表示されます。

IPS イベント アクション ネットワーク情報の設定

Event Actions Network Information ポリシーを使用して、次の機能を設定します。

- ターゲットの価値レーティング（[IPv4ターゲットの価値レーティング（IPv4 Target Value Ratings）] タブと [IPv6ターゲットの価値レーティング（IPv6 Target Value Ratings）] タブ）：ネットワーク資産のターゲットの価値レーティングを設定できます。センサーは、アラートの全体的なリスク レーティングを計算するときに、このレーティングを使用します。ミッションクリティカルな資産を識別することによって、より重大なシグニチャイベントアクションをトリガーできます。名前が示すように、適切なタブを選択することにより、IPv4 または IPv6 を使用できます。

ターゲットの価値レーティングは、IPS アプライアンス、サービス モジュール、および Cisco IOS IPS デバイスで使用できます。

詳細については、ターゲットの価値レーティングの設定 （24 ページ）を参照してください。

- パッシブ OS フィンガープリントおよび OS マッピング（[OS ID（OS Identification）] タブ）：デバイス上で稼働しているオペレーティングシステムの情報をセンサーが使用して、全体的なリスクレーティングのコンポーネントである攻撃関連性レーティングを決定できます。

パッシブ OS フィンガープリントおよび OS マッピングは、IPS 6.x 以降のソフトウェアを実行しているデバイスでだけ使用可能で、Cisco IOS IPS デバイスでは使用できません。

詳細については、以下を参照してください。

- パッシブ OS フィンガープリントについて （26 ページ）
- OS ID の設定（Cisco IPS 6.x 以降のセンサー限定） （28 ページ）

Network Information ポリシーを開くには、次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[IPS] > [イベントアクション（Event Actions）] > [ネットワーク情報（Network Information）]** を選択します。

- （ポリシービュー、IPS アプライアンスおよびサービスモジュール）**[IPS] > [イベントアクション（Event Actions）] > [ネットワーク情報（Network Information）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。
- （ポリシービュー、Cisco IOS IPS デバイス）**[IPS（ルータ）（IPS (Router)）] > [イベントアクション（Event Actions）] > [ネットワーク情報（Network Information）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。

ターゲットの価値レーティングの設定

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。IP アドレスで識別されるネットワーク資産の、認識されている重要性を特定します。

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。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。

4 つの価値レーティングを設定できます。最も高い値から最も低い値まで順に、[Mission Critical]、[High]、[Medium]、[Low]、[No Value]（ゼロ値）となります。

リスク レーティングの計算方法の詳細については、Cisco.com で『Installing and Using Cisco Intrusion Prevention System Device Manager 7.0』の「Calculating the Risk Rating」を参照してください。

ヒント 6.0(5) よりも前の IPS 6.0 ソフトウェアを使用しているデバイスでターゲットの価値レーティングを設定する場合は、OS マップを作成する必要がなくても、Network Information ポリシーの [OS Identification] タブを更新してソフトウェア バグを回避することを推奨します。詳細については、OS ID の設定（Cisco IPS 6.x 以降のセンサー限定） （28 ページ）を参照してください。

関連項目

- IPS イベント アクション ネットワーク情報の設定 （23 ページ）
- IPS イベント アクション プロセスについて （2 ページ）

ステップ 1 次のいずれかを実行して、Network Information ポリシーを開きます。

- （デバイスビュー）ポリシーセレクタから **[IPS] > [イベントアクション（Event Actions）] > [ネットワーク情報（Network Information）]** を選択して、[IPv4ターゲットの価値レーティング（IPv4 Target Value Ratings）] タブまたは [IPv6ターゲットの価値レーティング（IPv6 Target Value Ratings] タブをクリックします。

- （ポリシービュー、IPSアプライアンスおよびサービスモジュール）**[IPS]>[イベントアクション（Event Actions）]>[ネットワーク情報（Network Information）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。[IPv4ターゲットの価値レーティング（IPv4 Target Value Ratings）] タブまたは [IPv6ターゲットの価値レーティング（IPv6 Target Value Ratings] タブをクリックします。
- （ポリシービュー、Cisco IOS IPS デバイス）**[IPS（ルータ）（IPS (Router)）]>[イベントアクション（Event Actions）]>[ネットワーク情報（Network Information）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。[IPv4ターゲットの価値レーティング（IPv4 Target Value Ratings）] タブをクリックします。

（注） Cisco IOS IPS デバイスは IPv6 をサポートしていません。

タブに、すでに設定済みのターゲットの価値レーティングが表示され、設定済みの各レーティング カテゴリに関連付けられている IP アドレスが示されます。テーブルには 1 つのレーティング カテゴリに 1 つずつ、最大で 5 つのエントリを含めることができます。

ステップ 2 目的のターゲットの価値レーティング カテゴリを設定します。

- 新しいレーティングカテゴリを追加するには、テーブルの下の [行の追加（Add Row）]（+）ボタンをクリックし、[ターゲットの価値レーティングの追加（Add Target Value Rating）] ダイアログボックスに入力します。このダイアログボックスで、追加するレーティングを選択し、カテゴリに関連付けるホスト、ネットワーク、およびアドレス範囲を入力して、[OK] をクリックします。詳細については、[Add Target Value Rating]/[Edit Target Value Rating] ダイアログボックス （25 ページ）を参照してください。

IPv4 アドレスには、単一のネットワーク/ホストオブジェクトを指定するか、10.10.10.10、10.10.10.0/24、10.10.10.2-10.10.10.254 のようなホスト、ネットワーク、またはアドレス範囲のカンマ区切りリストを指定できます。ネットワーク形式で入力したアドレスは、アドレス範囲に変換されます。IPv6 アドレスの場合は、IPv6 アドレスの表記法を使用します。

- 既存のレーティングカテゴリの IP アドレスを編集するには、カテゴリを選択して、[行の編集（Edit Row）]（鉛筆）ボタンをクリックします。価値レーティングは変更できません。
- レーティングを削除するには、そのレーティングを選択し、[行の削除（Delete Row）] ボタンをクリックします。

[Add Target Value Rating]/[Edit Target Value Rating] ダイアログボックス

[Add Target Value Rating]/[Edit Target Value Rating] ダイアログボックスを使用して、資産の IP アドレスをレーティング カテゴリに関連付けます。[IPv4ターゲットの価値レーティング（IPv4 Target Value Ratings）] タブから [ターゲットの価値レーティング（Target Value Ratings）] ダイアログボックスを開くと、IP アドレスは IPv4 です。[IPv6] タブから開くと、IPv6 です。

ナビゲーション パス

IPS Event Actions Network Information ポリシーの [IPv4ターゲットの価値レーティング（IPv4 Target Value Ratings）] タブまたは [IPv6ターゲットの価値レーティング（IPv6 Target Value

Ratings）] タブから、[ターゲットの価値レーティング（Target Value Ratings）] テーブルの下の [行の追加（Add Row）] ボタンをクリックするか、またはテーブル内の行を選択して [行の編集（Edit Row）] ボタンをクリックします。[IPv4ターゲットの価値レーティング（IPv4 Target Value Ratings）] タブまたは [IPv6ターゲットの価値レーティング（IPv6 Target Value Ratings）] タブを開く方法については、ターゲットの価値レーティングの設定 （24 ページ）を参照してください。

フィールド リファレンス

表 *7: [Add Target Value Rating]/[Edit Target Value Rating]* ダイアログボックス

要素	説明
値	指定したアドレスに関連付けるターゲットの価値レーティング。最も高い重要性から最も低い重要性まで順に、[Mission Critical]、[High]、[Medium]、[Low]、[No Value] となります。 このリストには、ターゲットの価値レーティング テーブルにまだ設定されていない価値レーティングだけが含まれます。 レーティング カテゴリを編集する場合は、このオプションを変更します。
target-address	この価値レーティングに割り当てられるネットワーク資産の IP アドレス。次の方法を使用して、アドレスを指定できます。 • 単一のネットワーク/ホストオブジェクトの名前を入力します。または、[選択（Select）]をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。オブジェクトには、ネットワーク、ホスト、およびアドレス範囲のグループを含めることができます。 • ホストやネットワークのアドレスまたはアドレス範囲の、カンマ区切りのリスト。たとえば、IPv4 を使用する場合、10.10.10.0/24, 10.10.10.10, 10.10.10.2-10.10.10.254 となります。ネットワーク形式で入力したアドレスはアドレス範囲に変換されます。たとえば、10.10.10.0/24 は 10.10.10.0-10.10.10.255 に変換されます。

パッシブ OS フィンガープリントについて

パッシブ Operating System（OS; オペレーティング システム）フィンガープリントは、IPS 6.0 以降のセンサーで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により、センサーはホストが稼働している 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。

- パッシブ OS ラーニング。

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働している OS を特定します。

- ユーザ設定可能な OS ID。

OS ホスト マッピングを設定できます。これは学習した OS マッピングに優先します。

- 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。

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。

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 マッピング：Event Actions Network Information ポリシーの [OS Identification] タブで入力した OS マッピング。仮想センサーごとに異なるマッピングを設定できます。詳細については、OS ID の設定（Cisco IPS 6.x 以降のセンサー限定） （28 ページ）を参照してください。

   OS マッピングを設定して、重要なシステムで稼働している OS の ID を定義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 マッピングを設定するのが適切です。

2. インポートした OS マッピング：Management Center for Cisco Security Agents（CSA MC）からインポートした OS マッピング。

   インポートした OS マッピング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。CSA MC を使用するようにセンサーを設定する方法の詳細については、外部製品インターフェイスの設定を参照してください。

3. 学習した OS マッピング：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 マッピング。

   学習した OS マッピングは、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 マッピングを調べます。ターゲット IP アドレスが設定した OS マッピングにない場合、センサーはインポートした OS マッピングを調べます。ターゲット IP アドレスがインポートした OS マッピングにない場合、センサーは学習した OS マッピングを調べます。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。

ヒント　ターゲットの OS 関連性の値を使用するように、イベント アクション フィルタ ルールを設定できます。また、シグニチャに対する OS の脆弱性を識別するようにシグニチャを設定できます。

OS ID の設定（Cisco IPS 6.x 以降のセンサー限定）

Event Actions Network Information ポリシーの [OS Identification] タブを使用して、オペレーティング システム（OS）のホスト マッピングを設定します。これは、学習した OS マッピングに優先します。[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。

（注）　OS ID は IPS 6.0 以降のセンサーにだけ適用され、Cisco IOS IPS デバイスには適用されません。

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 マッピングでは、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。

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

より特定的なマッピング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。

ヒント 6.0(5) よりも前の IPS 6.0 バージョンには、Network Information ポリシーに関連するバグがあります。[OS ID（OS Identification）] タブで変更を行わなかったが、[脅威値レーティング（Threat Value Ratings）] タブでは設定を変更した場合でも、Security Manager は OS マッピングをアドレスに限定するために **any** 変数を使用するようにデバイスを設定します。この結果、モニタリング アプリケーションでは、すべてのイベントのイベント発生場所として「any」が表示されます。この問題を解決するには、センサーの IPS バージョンをアップグレードします。また、この問題を回避するには、特定の OS マッピングを設定していなくても、[OS ID（OS Identification）] タブの [これらの IP アドレスへの制限（Restrict to these IP Addresses）] フィールドにデフォルト以外の値を入力します。たとえば、「any」の代わりに 0.0.0.1-255.255.255.255 または 0.0.0.0-255.255.255.255 を入力します。

ナビゲーション パス

- （デバイス ビュー）ポリシー セレクタから [IPS] > [イベント アクション（Event Actions）] > [ネットワーク情報（Network Information）] を選択して、[OS ID（OS Identification）] タブをクリックします。
- （ポリシー ビュー、IPS アプライアンスおよびサービス モジュール）**[IPS] > [イベント アクション（Event Actions）] > [ネットワーク情報（Network Information）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。[OS ID（OS Identification）] タブをクリックします。

関連項目

- IPS イベント アクション ネットワーク情報の設定　（23 ページ）
- IPS イベント アクション プロセスについて　（2 ページ）

フィールド リファレンス

表 *8 : [OS Identification]* タブ

要素	説明
Enable Passive OS Fingerprinting	選択すると、センサーはパッシブなOS分析を実行します。このページで設定したマップのいずれかを使用するには、このオプションをイネーブルにする必要があります。 パッシブOSフィンガープリントは、センサーの一部として機能します。ホスト間のネットワーク トラフィックを分析するときに、センサーはホストのIPアドレスとともに、ホスト上で稼働しているOSのIDを格納します。センサーは、ネットワーク上で交換されたパケットの特性を検査することによって、ホスト上のOSのIDを特定します。次に、センサーはターゲットシステムのOS情報を使用して、RR（リスクレーティング）のARR（攻撃関連性レーティング）コンポーネントを計算します。さらに、RRは疑わしいパケットのドロップに使用できます。 パッシブOSフィンガープリントの詳細については、パッシブ OS フィンガープリントについて （26 ページ）を参照してください。
Restricted to these IP Addresses	攻撃関連性レーティングの計算を、指定したアドレスに制限します。次の方法を使用して、アドレスを指定できます。 • 単一のネットワーク/ホストオブジェクトの名前を入力します。または、[選択（Select）] をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。オブジェクトには、ネットワーク、ホスト、およびアドレス範囲のグループを含めることができます。 • ホストやネットワークのアドレスまたはアドレス範囲の、カンマ区切りのリスト。たとえば、10.10.10.0/24, 10.10.10.10, 10.10.10.2-10.10.10.254 となります。

要素	説明
[OS Maps] テーブル	OS マッピングのリストであり、ホストの IP アドレスと、それらがマッピングされるオペレーティング システムが示されます。一致検索時、センサーは上から下の順に検索して、IP アドレスと一致する最初のルールを選択します。 • マッピングを追加するには、[行の追加（Add Row）] ボタンをクリックし、[OS マップの追加（Add OS Map）] ダイアログボックスに入力します（[Add OS Map]/[Edit OS Map] ダイアログボックス （31 ページ）を参照）。 • マッピングを編集するには、ルールを選択し、[行の編集（Edit Row）] ボタンをクリックします。 • マップを削除するには、マップを選択し、[行の削除（Delete Row）] ボタンをクリックします。 • ルールのプライオリティを変更するには、そのルールを選択し、ルールが正しい位置に配置されるまで**上**矢印ボタンまたは**下**矢印ボタンをクリックします。

[Add OS Map]/[Edit OS Map] ダイアログボックス

[Add OS Map]/[Edit OS Map] ダイアログボックスを使用し、ホストの IP アドレスを使用してホストを OS タイプにマッピングします。OS タイプを IP アドレスにスタティックに割り当てる場合にだけ、マッピングを作成します。センサーが、パッシブ OS フィンガープリントを使用して IP アドレスに関連付けられる OS を検出するため、マッピングを作成しないことや、スタティック IP アドレスを持つミッションクリティカルなデバイスに対してだけマッピングを作成することができます。アドレスに別のオペレーティング システムを搭載したデバイスを設置する場合は、作成したすべてのマッピングを更新してください。

ナビゲーション パス

IPS Event Actions Network Information ポリシーの [OS ID（OS Identification）] タブから、[OS マップ（OS Maps）] テーブルの下の [行の追加（Add Row）] ボタンをクリックするか、またはテーブル内の行を選択して [行の編集（Edit Row）] ボタンをクリックします。[OS Identification] タブを開く方法については、OS ID の設定（Cisco IPS 6.x 以降のセンサー限定） （28 ページ）を参照してください。

フィールド リファレンス

表 *9 : [Add OS Map]/[Edit OS Map]* ダイアログボックス

要素	説明
IP Addresses	このマッピングのIPアドレス。次の方法を使用して、アドレスを指定できます。 • 単一のネットワーク/ホストオブジェクトの名前を入力します。または、[選択（Select）]をクリックしてリストからオブジェクトを選択するか、新しいオブジェクトを作成します。オブジェクトには、ネットワーク、ホスト、およびアドレス範囲のグループを含めることができます。 • ホストやネットワークのアドレスまたはアドレス範囲の、カンマ区切りのリスト。たとえば、10.10.10.0/24, 10.10.10.10, 10.10.10.2-10.10.10.254 となります。
OS タイプ	識別されるホストで稼働しているオペレーティング システム。リストから最も適切なオプションを選択します。複数のオプションを選択すると（Ctrl を押しながらクリックする）、可能性のある OS が複数存在することを示すことができます。 **ヒント** これらのマッピングは学習したマッピングに優先するため、[General OS]、[Other]、または [Unknown OS] は割り当てないようにすることを推奨します。センサーがパッシブ OS フィンガープリントを介して実際の OS を学習し、これによってより適切なマッチングを得られる可能性があります。詳細については、パッシブ OS フィンガープリントについて （26 ページ）を参照してください。

イベント アクションの設定

Event Actions Settings ポリシーを使用して、イベント アクション ルールにグローバルに適用される一般的な設定を指定します。これらのオプションのデフォルトはほとんどの状況に適しているため、個々の状況でデフォルト以外の動作を必要とすることが確実な場合にだけ、これらを変更します。

Event Actions Settings ポリシーを設定するには、次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[IPS] > [イベントアクション（Event Actions）] > [設定（Settings）]** を選択します。
- （ポリシービュー、IPS アプライアンスおよびサービスモジュール）**[IPS] > [イベントアクション（Event Actions）] > [設定（Settings）]**を選択してから、既存のポリシーを選択するか、または新しいポリシーを作成します。
- （ポリシービュー、Cisco IOS IPS デバイス）**[IPS（ルータ）（IPS (Router)）] > [イベントアクション（Event Actions）] > [イベントアクション設定（Event Action Settings）]** を選択してから、既存のポリシーを選択するか新しいポリシーを作成します。

次の表に、設定できるオプションを示します。Cisco IOS IPS デバイスで使用可能なオプションは、IPS アプライアンスおよびサービス モジュールで使用可能なオプションよりも制限されていることに注意してください。

ヒント　トラブルシューティング目的以外では、Summarizer 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 の状態を変更する必要はないことに注意してください。シスコではメタシグニチャの使用を中止しており、それらはすべて廃止されました。

表 *10 : Event Actions Settings* ポリシー

要素	説明
Enable Event Action Override （すべてのデバイス タイプ）	選択すると、[Event Action Overrides] ページで定義したオーバーライドルールがイネーブルになります。イベント アクション オーバーライドを追加すると、イベントの具体的な詳細に基づいて、そのイベントにアクションを追加できます。オーバーライド ルールの設定については、イベント アクション オーバーライドの設定 （17 ページ）を参照してください。
Enable Event Action Filters （すべてのデバイス タイプ）	選択すると、[Event Action Filters] ページで定義したフィルタ ルールがイネーブルになります。特定のアクションをイベントから削除するか、または、イベント全体を破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。イベント アクション フィルタ ルールの設定については、イベント アクション フィルタの設定 （6 ページ）を参照してください。

要素	説明
Enable Event Action Summarizer （IPS アプライアンスおよびサービス モジュール限定）	選択すると、Summarizer コンポーネントがイネーブルになります。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。 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。 Cisco Security Manager の Report Manager コンポーネントは、イベントを個別にレポートします。Cisco Security Manager の Event Viewer コンポーネントにアラートが表示されます。上述のとおり、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。 **ヒント** Cisco IPS Manager Express（IME）と Cisco Security Manager は、まったく同じ方法ではイベントを要約しません。
Enable Meta Event Generator （IPS アプライアンスおよびサービス モジュール限定）	シスコでは、Meta Event Generator の状態を変更しないことを推奨しています。シスコではメタシグニチャの使用を中止しており、それらはすべて廃止されました。

要素	説明
Enable Threat Rating Adjustment （IPS アプライアンスおよびサービス モジュール限定）	選択すると、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。IPS 6.0 以降のソフトウェアを実行しているセンサーでだけ使用可能です。 脅威レーティング機能は、ネットワークの脅威環境に関する単一のビューを提供します。脅威レーティングは、脅威レーティングの値が高いイベントだけを表示するカスタマイズ ビューを使用して、アラームおよびイベントの数を最小限に抑えます。脅威レーティングの値は、次のように算出されます。 • 応答アクションの成功に基づいたイベントのリスク レーティングのダイナミック調整 • 応答アクションが適用された場合、リスク レーティングは使用されない（脅威レーティング < リスク レーティング） • 応答アクションが適用されなかった場合、リスク レーティングは変更されない（脅威レーティング = リスク レーティング） この結果、脅威のリスクを決定する単一の値が算出されます。
Deny Attacker Duration in seconds （すべてのデバイス タイプ）	インラインで攻撃者を拒否する秒数。 有効な範囲は 0 ～ 518400 です。デフォルトは 3600 です。
Block Attack Duration in minutes （IPS アプライアンスおよびサービス モジュール限定）	ホストまたは接続をブロックする分数。 指定できる範囲は 0 ～ 10000000 です。デフォルトは 30 です。
Maximum Number of Denied Attackers （IPS アプライアンスおよびサービス モジュール限定）	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。

要素	説明
Enable One Way TCP Reset （IPS アプライアンスおよびサービス モジュール限定）	選択すると、TCP ベースのアラートの Deny Packet Inline アクションに対して一方向の TCP リセットがイネーブルになります。IPS 6.1 以降のソフトウェアを実行しているセンサーでだけ使用可能です。 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。 **ヒント** • インラインモードでは、ネットワークに出入りするすべてのパケットがセンサーを通過する必要があります。 • 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します。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。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。