イベント アクション ルールの設定

この章では、イベント アクション ルールを設定する方法を説明します。この章は、次の項で構成されています。

イベント アクション ルールについて

イベント アクション ルールは、センサーのイベント アクション処理コンポーネント用の設定のグループです。これらのルールは、イベントが発生したときにセンサーが実行するアクションを指定します。

イベント アクション処理コンポーネントは、次の機能を担当します。

- リスク評価の計算
- イベント アクション オーバーライドの追加
- イベント アクションのフィルタリング
- 結果のイベント アクションの実行
- イベントの要約と集約
- 拒否された攻撃者リストの管理

この項で取り上げる事項は次のとおりです。

リスク評価の計算

RR 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、0 から 100 の間の数値で表した評価です。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（ASR および SFR）およびサーバ単位（TVR）で設定されます。

RR を使用すると、注意の必要なアラートの優先順位を高くすることができます。このような RR の要素としては、成功した場合の攻撃の重大度、シグニチャの忠実度、およびターゲット ホストの全体の価値が考慮に入れられています。RR は evIdsAlert で報告されます。

特定のイベントの RR の計算には、次の値が使用されます。

- **Attack Severity Rating（ASR）**：脆弱性の不正利用に成功した場合の重大度に関連付ける重み値。

  ASR は、シグニチャのアラート重大度パラメータから取得されます。
- **Sig Fidelity Rating（SFR）**：対象とする特定の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かに関連付ける重み値。

  SFR 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、資格を与える情報がターゲットにない場合のシグニチャの精度について、基本的な信頼度を定義します。この信頼度は、分析中のパケットの送達が許可された場合に、検出された動作がどの程度確実にターゲット プラットフォームに目的とする効果を与えるかを表します。たとえば、きわめて具体的なルール（特定の正規表現など）で記述されたシグニチャは、汎用的なルールで記述されたシグニチャより高い SFR を持ちます。
- **Target Value Rating（TVR）**：明確化されたターゲットの価値に関連付ける重み値。

  TVR は、ネットワーク資産（IP アドレスを経由する）の重要性を示す、ユーザが設定可能な値です。価値の高い企業リソースにはより厳しいセキュリティ ポリシーを作成し、そうでないリソースにはある程度緩やかなポリシーを作成できます。たとえば、企業の Web サーバには、デ

スクトップ ノードに割り当てる TVR より高い TVR を割り当てることができます。この場合、企業の Web サーバに対する攻撃は、デスクトップ ノードに対する攻撃よりも高い RR を持ちます。

（注）　RR は、ASR、SFR、TVR、およびオプションの Promiscuous Delta（PD; 混合デルタ）から計算されます。

イベント オーバーライド

イベントの RR に基づいて、イベントに関連付けられたアクションを変更するために、イベント アクション オーバーライドを追加できます。イベント アクション オーバーライドを使用すると、各シグニチャを個別に設定しなくても、グローバルにイベント アクションを追加することができます。各イベント アクションには、一定範囲の RR が関連付けられています。シグニチャ イベントが発生し、そのイベントの RR が特定のイベント アクションの範囲内にある場合は、そのアクションがイベントに追加されます。たとえば、RR が 85 以上のイベントでは SNMP トラップを生成する場合には、**Request SNMP Trap** の RR 範囲を **85 ～ 100** に設定できます。アクションの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。

イベント アクション フィルタ

イベント アクション フィルタは、順番に並べられたリストとして処理されます。フィルタのリスト内の順番は上下に移動できます。

センサーは、フィルタの使用により、イベントに応答してすべてのアクションを実行せずに特定のアクションを実行したり、イベント全体を削除することができます。フィルタは、イベントからアクションを削除することによって機能します。イベントからすべてのアクションを削除するフィルタは、効果的にイベントを消滅させます。

（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お勧めします。複数の宛先アドレスが存在する場合は、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。

イベント アクションの要約と集約

この項では、イベント アクションの要約方法と集約方法について説明します。取り上げる事項は次のとおりです。

- イベント アクションの要約（P.7-3）
- イベント アクションの集約（P.7-4）

イベント アクションの要約

要約すると、センサーから送出されるアラームの量を減らし、多数のイベントを 1 つのアラームにまとめる基本的な集約を実行します。各シグニチャに対して特別なパラメータが指定され、それぞれアラートの処理に影響を与えます。各シグニチャは、最適な通常の動作を反映したデフォルトの設定で作成されます。ただし、各シグニチャを調整して、各エンジン タイプの制限内でこのデフォルトの動作を変更できます。

要約されていない各シグニチャ イベントでは、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）はフィルタを通過します。このような要約されたアラートでは、アラートを生成するアクションは実行されません。代わりに、そのようなアクションは 1 つのサマリー アラートに適用され、その後フィルタにかけられます。

その他のアラート生成アクションのいずれかを選択し、それにフィルタを適用しない場合は、**Produce Alert** を選択していない場合でもアラートが作成されます。アラートが生成されないようするには、アラートを生成するすべてのアクションがフィルタリングによって排除されるようにする必要があります。

要約とイベント アクションは、META エンジンがコンポーネント イベントを処理した後に処理されます。この処理により、センサーは一連のイベントにまたがって発生する不審なアクティビティを監視することができます。

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、いくつのヒットがあるとアラートが送信されるかを示すしきい値をシグニチャに設定します。より高度なモードでは、間隔カウントを行います。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。この例では、「ヒット」とはイベントを表すために使用する用語で、基本的にはアラートのことです。ただし、ヒットのしきい値を超えるまで、アラートとしてセンサーから送出されません。

次の要約オプションを選択できます。

- **Fire All** : Fire All モードではシグニチャがトリガーされるたびにアラートが送出されます。要約にしきい値が設定されている場合は、要約が発生するまでは実行のたびにアラートが発生します。要約が開始されると、各アドレス セットで要約の間隔ごとに 1 つのアラートのみが発生します。異なるアドレス セットのアラートは、すべて表示されるか、個別に要約されます。該当のシグニチャで一定期間アラートが発生しないと、シグニチャは Fire All モードに戻ります。
- **Summary** : Summary モードでは、最初にシグニチャがトリガーされたときにアラートを送出します。そのシグニチャのそれ以降のアラートは、要約間隔ごとに要約されます。各アドレス セットで要約の間隔ごとに 1 つのアラートのみが発生します。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** : Global Summarization モードでは、要約間隔ごとに 1 つのアラートを送出します。シグニチャにグローバル サマリーを事前設定しておくこともできます。
- **Fire Once** : Fire Once モードではアドレス セットごとにアラートを送出します。このモードを Global Summarization モードにアップグレードすることができます。

Signature Event Action Processor

SEAP は、アラーム チャネル内のシグニチャ イベントから、SEAO、SEAF の処理を経由して SEAH で処理されるまでのデータ フローを調整します。これは次のコンポーネントから構成されます。

- アラーム チャネル

  Sensor App 検査パスからシグニチャ イベント処理へ向かうシグニチャ イベントと通信するエリアを表す単位。
- シグニチャ イベント アクション オーバーライド（SEAO）

  RR 値に基づいて、アクションを追加します。SEAO は、設定済みの RR しきい値の範囲に該当するすべてのシグニチャに適用されます。各 SEAO は独立しており、各アクション タイプには別個の値が設定されています。詳細については、P.7-2 の「リスク評価の計算」を参照してください。

- シグニチャ イベント アクション フィルタ（SEAF）

  シグニチャ イベントのシグニチャ ID、アドレス、および RR に基づいてアクションを削除します。SEAF へ入力するのは、SEAO によって追加される可能性のあるアクションを持つシグニチャ イベントです。

  （注）　SEAF が実行できるのはアクションの削除だけであり、新規アクションの追加はできません。

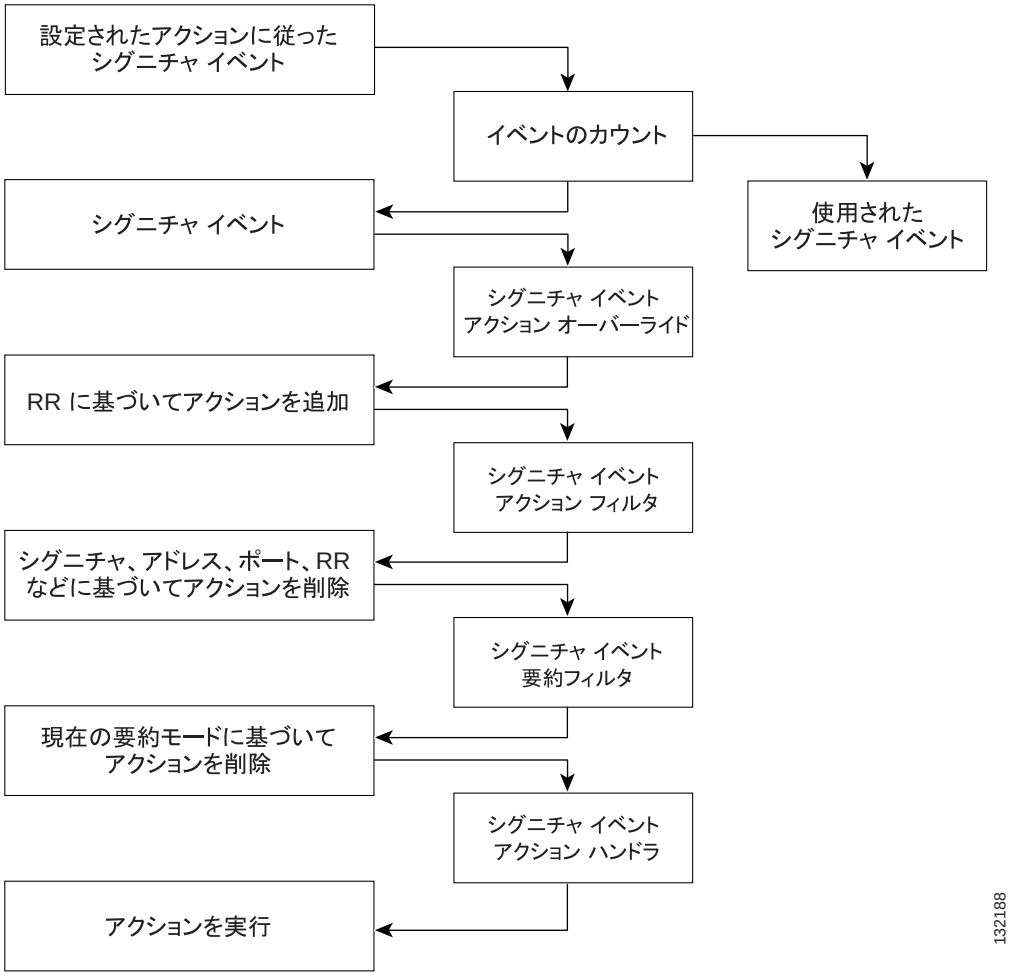
  SEAF には、次のパラメータが適用されます。

  - シグニチャ ID
  - サブシグニチャ ID
  - 攻撃者のアドレス
  - 攻撃者のポート
  - 被害先のアドレス
  - 被害先のポート
  - RR しきい値の範囲
  - 削除するアクション
  - シーケンス識別子（オプション）
  - ストップ ビットまたは継続ビット
  - アクション フィルタ行をイネーブルにするビット
- シグニチャ イベント アクション ハンドラ（SEAH）

  要求されたアクションを実行します。SEAH から出力されるのは、実行中のアクションだけでなく、イベント ストアに書き込まれる <evIdsAlert> である可能性があります。

図 7-1 は、SEAP を通過するシグニチャ イベントの論理フローと、このイベントのアクションで実行される操作を示しています。これは、アラーム チャネルで受信された設定済みアクションを持つシグニチャ イベントで開始され、シグニチャ イベントが SEAP の機能コンポーネントを通過するときに上から下へ流れます。

図 7-1　SEAP を通過するシグニチャ イベント



イベント アクション

表 7-1 は、イベント アクションについて説明しています。

表 7-1　イベント アクション

イベント アクション名	説明
Deny Attacker Inline	（インライン モードのみ）指定された期間、攻撃者アドレスから発信されたこのパケットおよび将来のパケットを送信しません。[1] **（注）** これは、拒否アクションの中で最も重大です。これは、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を拒否します。拒否された攻撃者のエントリをすべてクリアするには、**Monitoring** > **Denied Attackers** > **Clear List** をクリックします。これによって、これらのアドレスのネットワークへの再接続が許可されます。手順については、P.11-3 の「拒否された攻撃者リストの監視」を参照してください。
Deny Attacker Service Pair Inline	（インライン モードのみ）指定された期間、攻撃者アドレスと被害先ポートのペアで、このパケットおよび将来のパケットを送信しません。
Deny Attacker Victim Pair Inline	（インライン モードのみ）指定された期間、攻撃者と被害先のアドレスのペアで、このパケットおよび将来のパケットを送信しません。 **（注）** 拒否アクションの場合、指定された期間と拒否された攻撃者の最大数を指定するには、**Configuration > Event Action Rules > General Settings** をクリックします。手順については、P.7-30 の「一般的な設定値の設定」を参照してください。
Deny Connection Inline	（インライン モードのみ）TCP フローで、このパケットおよび将来のパケットを送信しません。
Deny Packet Inline	（インライン モードのみ）このパケットを送信しません。
Log Attacker Packets	攻撃者アドレスを含む IP ロギング パケットを開始します。 **（注）** 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、イベント ストアにアラートが書き込まれます。
Log Pair Packets	攻撃者と被害先のアドレスのペアを含む IP ロギング パケットを開始します。 **（注）** 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、イベント ストアにアラートが書き込まれます。
Log Victim Packets	被害先アドレスを含む IP ロギング パケットを開始します。

表 7-1　イベント アクション（続き）

イベント アクション名	説明
Modify Packet Inline	パケット データを変更して、エンドポイントでパケットがどう処理されるかに関してあいまいな部分を除去します。 （注）　Modify Packet Inline は、Add Event Action Filter または Add Event Action Override のオプションではありません。
Produce 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。
Produce Verbose Alert	違反パケットの符号化ダンプをアラートに組み込みます。 （注）　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、イベント ストアにアラートが書き込まれます。
Request Block Connection	この接続をブロックする要求を ARC に送信します。 （注）　ブロッキング デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第 8 章「ブロッキングとレート制限のための ARC 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 ARC に送信します。 （注）　ブロッキング デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第 8 章「ブロッキングとレート制限のための ARC の設定」を参照してください。 （注）　ブロック アクションの場合、ブロックの期間を設定するには、**Configuration > Event Action Rules > General Settings** をクリックします。手順については、P.7-30 の「一般的な設定値の設定」を参照してください。
Request Rate Limit	レート制限を実行するレート制限要求を ARC に送信します。レート制限デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第 8 章「ブロッキングとレート制限のための ARC の設定」を参照してください。 （注）　Request Rate Limit は、選ばれたシグニチャのセットに適用されます。レート制限を要求できるシグニチャのリストについては、P.8-4 の「レート制限について」を参照してください。

表 7-1　イベント アクション（続き）

イベント アクション名	説明
Request SNMP Trap	SNMP 通知を実行する要求を NotificationApp に送信します。 （注）　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、イベント ストアにアラートが書き込まれます。SNMP は、このアクションを実装するようセンサーで設定されている必要があります。詳細については、第 9 章「SNMP の設定」を参照してください。
Reset TCP Connection	TCP リセットを送信し、TCP フローを乗っ取って終了します。 （注）　Reset TCP Connection は、単一の接続を分析する TCP シグニチャでのみ機能します。スイープやフラッドに対しては機能しません。

1. センサーは、システムによって拒否されている攻撃者のリストを保持します。拒否された攻撃者のリストからエントリを削除するには、攻撃者のリストを表示してリスト全体をクリアするか、タイマーで有効期限が切れるのを待ちます。タイマーは、エントリごとにスライドするタイマーです。したがって、攻撃者 A が拒否されているときに別の攻撃が発行されると、攻撃者 A のタイマーはリセットされ、そのタイマーの有効期限が切れるまで攻撃者 A は拒否された攻撃者リストに残ります。拒否された攻撃者のリストがいっぱいになり、新規エントリを追加することができない場合でも、パケットは拒否されます。

注意　シグニチャに対してアラートをイネーブルにした場合、Produce Alert アクションは自動にはなりません。イベント ストアでアラートを作成するには、Produce Alert を選択する必要があります。2 番目のアクションを追加する場合、イベント ストアにアラートを送信するには、Produce Alert を組み込む必要があります。また、イベント アクションを設定するたびに、新規リストが作成され、古いリストが置換されます。各シグニチャに必要なイベント アクションを必ずすべて組み込んでください。

イベント アクション ルールの例

次の例は、イベント アクション ルールの個々のコンポーネントがどのように連携して動作するかを示しています。

例 1 のリスク評価範囲

- **Produce Alert**：1 ～ 100
- **Produce Verbose Alert**：90 ～ 100
- **Request SNMP Trap**：50 ～ 100
- **Log Pair Packets**：90 ～ 100
- **Log Victim Packets**：90 ～ 100
- **Log Attacker Packets**：90 ～ 100
- **Reset TCP Connection**：90 ～ 100
- **Request Block Connection**：70 ～ 89
- **Request Block Host**：90 ～ 100
- **Deny Attacker Inline**：0 ～ 0
- **Deny Connection Inline**：90 ～ 100
- **Deny Packet Inline**：90 ～ 100

例 1 のイベント アクション フィルタ

1. SigID=2004, Attacker Address=*, Victim Address=20.1.1.1, Actions to Remove=ALL, Risk Rating Range=1-100, StopOnMatch=True
2. SigID=2004, Attacker Address=30.1.1.1, Victim Address=*, Actions to Remove=ALL, Risk Rating Range=1-100, StopOnMatch=True
3. SigID=2004, Attacker Address=*, Victim Address=*, Actions to Remove=None, Risk Rating Range=95-100, StopOnMatch=True
4. SigID=2004, Attacker Address=*, Victim Address=*, Actions to Remove=denyAttackerInline, requestBlockHost, requestBlockConnection, Risk Rating Range=56-94, StopOnMatch=True
5. SigID=2004, Attacker Address=*, Victim Address=*, Actions to Remove=denyAttackerInline, requestBlockHost, produceAlert, resetTcpConnection, logAttackerPackets, Risk Rating Range=1-55, StopOnMatch=True

例 1 の結果

SIG 2004 が検出された場合：

- 攻撃者アドレスが 30.1.1.1 であるか、または被害先のアドレスが 20.1.1.1 である場合、イベントは消滅します（ALL アクションは削除されます）。

攻撃者アドレスが 30.1.1.1 以外で、被害先アドレスが 20.1.1.1 以外である場合：

- RR が 50 の場合、**Produce Alert** および **Request SNMP Trap** はイベント アクション オーバーライド コンポーネントによって追加されますが、**Produce Alert** はイベント アクション フィルタによって削除されます。ただし、**Request SNMP Trap** は <evIdsAlert> に依存しているため、イベント アクション ポリシーがアラート アクションを強制的に適用します。
- RR が 89 の場合、**Request SNMP Trap** および **Request Block Connection** はイベント アクション オーバーライド コンポーネントによって追加されます。ただし、**Request Block Connection** はイベント アクション フィルタによって削除されます。
- RR が 96 の場合、**Deny Attacker Inline** および **Request Block Connection** を除くすべてのアクションがイベント アクション オーバーライド コンポーネントによって追加され、イベント アクション フィルタは何も削除しません。フィルタ アクションが NONE に指定された 3 番目のフィルタ行はオプションですが、このタイプのフィルタを定義するより明確な方法として示されています。

イベント変数の設定

この項では、イベント変数の設定方法について説明します。取り上げる事項は次のとおりです。

概要

イベント変数を作成し、イベント アクション フィルタの中でそれらの変数を使用できます。複数のフィルタで同じ値を使用する場合、変数を使用します。変数の値を変更すると、その変数を使用しているフィルタは新しい値で更新されます。

（注）　変数の前にドル記号($)を付けて、文字列ではなく変数を使用していることを示す必要があります。

シグニチャ システムに必要なため、削除できない変数もあります。変数が保護されている場合は、それを選択して編集することはできません。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。

IP アドレスを設定する場合は、完全な IP アドレス、範囲、または範囲のセットを指定します。次の例を参考にしてください。

- 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

ワンポイント・アドバイス　たとえば、社内の技術グループに対応する　IP　アドレス空間があるとします。グループ内には Windows システムがなく、Windows ベースの攻撃を心配する必要はありません。このような場合、変数を技術グループの IP アドレス空間として設定します。その後、この変数を使用して、このグループに対するすべての Windows ベースの攻撃を無視するフィルタを設定できます。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

イベント変数を設定するには、管理者またはオペレータである必要があります。

フィールド定義

この項では、イベント変数のフィールドの定義を示します。取り上げる事項は次のとおりです。

Event Variables パネル

Event Variables パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **Name**：この変数に名前を割り当てます。
- **Type**：変数をアドレスとして指定します。
- **Value**：この変数によって表される値を追加します。

ボタンの機能：

- **Add**：Add Variable ダイアログボックスを表示します。
  このダイアログボックスで、変数を追加し、その変数に関連付ける値を指定できます。
- **Edit**：Edit Variable ダイアログボックスを表示します。
  このダイアログボックスで、この変数に関連付けられた値を変更できます。
- **Delete**：使用可能な変数のリストから選択した変数を削除します。
- **Apply**：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。
- **Reset**:作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

Add and Edit Event Variable ダイアログボックス

Add and Edit Event Variable ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **Name**：この変数に名前を割り当てます。
- **Type**：変数をアドレスとして指定します。
- **Value**：この変数によって表される値を追加します。

ボタンの機能：

- **OK**：変更を確定し、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

イベント変数の設定

イベント変数を設定するには、次の手順を実行します。

ステップ 1　管理者特権またはオペレータ特権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 > Event Action Rules > Event Variables** をクリックします。

Event Variables パネルが表示されます。

ステップ 3　**Add** をクリックして、変数を作成します。

Add Variable ダイアログボックスが表示されます。

ステップ 4　**Name** フィールドに変数の名前を入力します。

（注）　名前には、数字または文字だけを使用できます。ハイフン（-）または下線（_）は使用できます。

ステップ 5　**Value** フィールドに変数の値を入力します。

完全な IP アドレス、範囲、または範囲のセットを指定します。次の例を参考にしてください。

- 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。

ヒント　変更を元に戻し、Add Variable ダイアログを閉じるには、**Cancel** をクリックします。

ステップ 6　**OK** をクリックします。

Event Variables パネルのリストに新しい変数が表示されます。

ステップ 7　既存の変数を編集するには、リスト内でそれを選択して **Edit** をクリックします。

Edit Event Variable ダイアログボックスが表示されます。

ステップ 8　**Value** フィールドの値を変更します。

ヒント　変更を元に戻し、Edit Variable ダイアログを閉じるには、**Cancel** をクリックします。

ステップ 9　**OK** をクリックします。

Event Variables パネルのリストに編集したイベント変数が表示されます。

ヒント　**Reset** をクリックして、変更を削除します。

ステップ 10　変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。

Target Value Rating の設定

この項では、ターゲットの価値評価を設定する方法について説明します。取り上げる事項は次のとおりです。

概要

TVR をネットワーク資産に割り当てることができます。TVR は各アラートの RR 値の計算に使用される要素の 1 つです。ターゲットごとに異なる TVR を割り当てることができます。RR の高いイベントほど、より厳しいシグニチャ イベント アクションをトリガーします。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

ターゲットの価値評価を設定するには、管理者またはオペレータである必要があります。

フィールド定義

この項では、TVR のフィールドの定義を示します。取り上げる事項は次のとおりです。

Target Value Rating パネル

Target Value Rating パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **Target Value Rating (TVR)**：このネットワーク資産に割り当てる値を示します。値は、High、Low、Medium、Mission Critical、No Value のいずれかになります。
- **Target IP Address**：TVR によって優先順位付けするネットワーク資産の IP アドレスを示します。

ボタンの機能：

- **Select All**：設定済みのターゲットをすべて選択します。
- **Add**：Add Target Value Rating ダイアログボックスを表示します。

  このダイアログボックスで、ネットワーク資産の IP アドレスを追加し、その資産に TVR を割り当てることができます。
- **Edit**：Edit Target Value Rating ダイアログボックスを表示します。

  このダイアログボックスで、ネットワーク資産の IP アドレスを変更できます。
- **Delete**：使用可能な評価のリストから選択した TVR を削除します。

- **Apply**：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。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

Add and Edit Target Value Rating ダイアログボックス

Add and Edit Target Value Rating ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **Target Value Rating (TVR)**：このネットワーク資産に割り当てる値を示します。値は、High、Low、Medium、Mission Critical、No Value のいずれかになります。
- **Target IP Address(es)**：TVR によって優先順位付けするネットワーク資産の IP アドレスを示します。

ボタンの機能：

- **OK**：変更を確定し、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

Target Value Rating の設定

TVR を設定するには、次の手順を実行します。

ステップ 1　管理者特権またはオペレータ特権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 > Event Action Rules > Target Value Rating** をクリックします。

Target Value Rating パネルが表示されます。

ステップ 3　**Add** をクリックして、TVR を作成します。

Add Target Value Rating ダイアログボックスが表示されます。

ステップ 4　新しい資産グループに TVR を割り当てるには、次の手順を実行します。

a. **Add** をクリックして、新しいネットワーク資産のグループを追加します。
b. Target Value Rating リスト ボックスから評価を選択します。

   値は、**High**、**Low**、**Medium**、**Mission Critical**、**No Value** のいずれかになります。
c. **Target IP 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、範囲の最小のアドレスに続けて、ハイフンと範囲の最大のアドレスを入力します。例：10.10.2.1-10.10.2.30。

ヒント　変更を元に戻して 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 5　**OK** をクリックします。

Target Value Rating パネルのリストに新しい資産の新しい TVR が表示されます。

ステップ 6　既存の TVR を編集するには、リスト内でそれを選択して **Edit** をクリックします。

Edit Target Value Rating ダイアログボックスが表示されます。

ステップ 7　**Target IP Address(es)** フィールドの値を変更します。

ヒント　変更を元に戻して 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 8　**OK** をクリックします。

Target Value Rating パネルのリストに編集したネットワーク資産が表示されます。

ステップ 9　ネットワーク資産を削除するには、リスト内でそれを選択して **Delete** をクリックします。

このネットワーク資産は Target Value Rating パネルのリストから消去されます。

ヒント　**Reset** をクリックして、変更を削除します。

ステップ 10　変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。

イベント アクション オーバーライドの設定

この項では、イベント アクション オーバーライドの設定方法について説明します。取り上げる事項は次のとおりです。

概要

イベントの詳細に基づいてイベントに関連付けられたアクションを変更するために、イベント アクション オーバーライドを追加できます。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

イベント アクション オーバーライドを設定するには、管理者またはオペレータである必要があります。

フィールド定義

この項では、イベント アクション オーバーライドのフィールドの定義を示します。取り上げる事項は次のとおりです。

Event Action Overrides パネル

Event Action Overrides パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **Use Event Action Overrides**：選択すると、イネーブルなイベント アクション オーバーライドをすべて使用できます。
- **Event Action**：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た場合に、イベントに追加するイベント アクションを指定します。
- **Enabled**：このオーバーライドがイネーブルであるかどうかを示します。
- **Risk Rating**：このイベント アクション オーバーライドをトリガーするために使用する必要のある 0 ～ 100 までの RR 範囲を示します。

  ここで設定した最小値から最大値までの範囲内の RR を持つイベントが発生した場合に、イベント アクションをこのイベントに追加します。

ボタンの機能：

- **Select All**：テーブルに表示されたすべてのイベント アクション オーバーライドを選択します。

- **Add**：Add Event Action Override ダイアログボックスを表示します。

  このダイアログボックスで、イベント アクション オーバーライドを追加し、そのオーバーライドに関連付ける値を指定できます。
- **Edit**：Edit Event Action Override ダイアログボックスを表示します。

  このダイアログボックスで、このイベント アクション オーバーライドに関連付けられた値を変更できます。
- **Enable**：選択したイベント アクション オーバーライドをイネーブルにします。

  Event Action Overrides パネルの **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。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。
- **Disable**：選択したイベント アクション オーバーライドをディセーブルにします。
- **Delete**：使用可能なオーバーライドのリストから選択したイベント アクションを削除します。
- **Apply**：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。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

Add and Edit Event Action Overrides ダイアログボックス

Add and Edit Event Action Overrides ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **Event Action**：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た場合に、イベントに追加するイベント アクションを指定します。
  - **Deny Attacker Inline**：（インライン モードのみ）指定された期間、この攻撃者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。

    センサーは、システムによって拒否されている攻撃者のリストを保持します。拒否された攻撃者のリストからエントリを削除するには、攻撃者のリストを表示してリスト全体をクリアするか、タイマーで有効期限が切れるのを待ちます。タイマーは、エントリごとにスライドするタイマーです。したがって、攻撃者 A が拒否されているときに別の攻撃が発行されると、攻撃者 A のタイマーはリセットされ、そのタイマーの有効期限が切れるまで攻撃者 A は拒否された攻撃者リストに残ります。拒否された攻撃者のリストがいっぱいになり、新規エントリを追加することができない場合でも、パケットは拒否されます。

    （注）　これは、拒否アクションの中で最も重大です。これは、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を拒否します。拒否された攻撃者のエントリをすべてクリアするには、**Monitoring** > **Denied Attackers** > **Clear List** をクリックします。これによって、これらのアドレスのネットワークへの再接続が許可されます。手順については、P.11-3 の「拒否された攻撃者リストの監視」を参照してください。
  - **Deny Attacker Service Pair Inline**：（インライン モードのみ）指定された期間、攻撃者アドレスと被害先ポートのペアで、このパケットおよび将来のパケットを送信しません。
  - **Deny Attacker Victim Pair Inline**：（インライン モードのみ）指定された期間、攻撃者と被害先のアドレスのペアで、このパケットおよび将来のパケットを送信しません。

    （注）　拒否アクションの場合、指定された期間と拒否された攻撃者の最大数を指定するには、**Configuration** > **Event Action Rules** > **General Settings** をクリックします。手順については、P.7-30 の「一般的な設定値の設定」を参照してください。

- **Deny Connection Inline**：（インライン モードのみ）この TCP フローの現在のパケットと将来のパケットを終了します。
- **Deny Packet Inline**：（インライン モードのみ）パケットを終了します。
- **Log Attacker Packets**：攻撃者アドレスを含む IP ロギング パケットを開始し、アラートを送信します。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、イベント ストアにアラートが書き込まれます。
- **Log Pair Packets**：攻撃者と被害先のアドレスのペアを含む IP ロギング パケットを開始します。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、イベント ストアにアラートが書き込まれます。
- **Log Victim Packets**：被害先のアドレスを含む IP ロギング パケットを開始し、アラートを送信します。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、イベント ストアにアラートが書き込まれます。
- **Modify Packet Inline**：パケット データを変更して、エンドポイントでパケットがどう処理されるかに関してあいまいな部分を除去します。

（注）　Modify Packet Inline は、Add Event Action Filter または Add Event Action Override のオプションではありません。

- **Produce 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。
- **Produce Verbose Alert**：違反パケットの符号化ダンプをアラートに組み込みます。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、イベント ストアにアラートが書き込まれます。
- **Request Block Connection**：この接続をブロックする要求を ARC に送信します。ブロッキング デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第 8 章「ブロッキングとレート制限のための ARC 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 ARC に送信します。ブロッキング デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第8章「ブロッキングとレート制限のための ARC の設定」を参照してください。

（注）　ブロック アクションの場合、ブロックの期間を設定するには、**Configuration > Event Action Rules > General Settings** をクリックします。手順については、P.7-30 の「一般的な設定値の設定」を参照してください。

- **Request Rate Limit**：レート制限を実行するレート制限要求を ARC に送信します。レート制限デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第 8 章「ブロッキングとレート制限のための ARC の設定」を参照してください。
- **Request SNMP Trap**：SNMP 通知を実行する要求をセンサーの通知アプリケーション コンポーネントに送信します。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、イベント ストアにアラートが書き込まれます。SNMP は、このアクションを実装するようセンサーで設定されている必要があります。詳細については、第 9 章「SNMP の設定」を参照してください。
- **Reset TCP Connection**：TCP リセットを送信し、TCP フローを乗っ取って終了します。Reset TCP Connection は、単一の接続を分析する TCP シグニチャでのみ機能します。スイープやフラッドに対しては機能しません。

- **Enabled**：**Yes** チェックボックスをオンにするとオーバーライドはイネーブルになり、**No** チェックボックスをオンにするとオーバーライドはディセーブルになります。
- **Risk Rating**：このイベント アクション オーバーライドをトリガーするために使用する必要のある 0 ～ 100 までの RR 範囲を示します。

ここで設定した最小値から最大値までの範囲内の RR を持つイベントが発生した場合に、イベント アクションをこのイベントに追加します。

ボタンの機能：

- **OK**：変更を確定し、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

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 オーバーライドを設定するには、次の手順を実行します。

ステップ 1　管理者特権またはオペレータ特権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 > Event Action Rules > Event Action Overrides** をクリックします。

Event Action Overrides パネルが表示されます。

ステップ 3　**Add** をクリックして、イベント アクション オーバーライドを作成します。

Add Event Action Override ダイアログボックスが表示されます。

ステップ 4　**Event Action** リストから、このイベント アクション オーバーライドに対応するイベント アクションを選択します。

ステップ 5　Enabled の下の **Yes** チェックボックスをオンにします。

ステップ 6　Risk Rating の下の **Minimum** フィールドおよび **Maximum** フィールドで、RR 範囲をこのネットワークに割り当てます。

値はすべて 0 ～ 100 までで、**Minimum** フィールドの値は **Maximum** フィールドの値以下にする必要があります。

ヒント　変更を元に戻して 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。

ステップ 7　**OK** をクリックします。

Event Action Overrides パネルのリストに新しいイベント アクション オーバーライドが表示されます。

ステップ 8　**Use Event Action Overrides** チェックボックスをオンにします。

（注）　Event Action Overrides パネルの **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。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。

ステップ 9　既存のイベント アクション オーバーライドを編集するには、リスト内でそれを選択して **Edit** をクリックします。

Edit Event Action Override ダイアログボックスが表示されます。

ステップ 10　Enabled の下の **Yes** チェックボックスをオンにします。

ステップ 11　Risk Rating の下の **Minimum** フィールドおよび **Maximum** フィールドで、RR 範囲をこのネットワークに割り当てます。

値はすべて 0 ～ 100 までで、**Minimum** フィールドの値は **Maximum** フィールドの値以下にする必要があります。

ヒント　変更を元に戻して Edit 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。

ステップ 12　**OK** をクリックします。

Event Action Overrides パネルのリストに編集したイベント アクション オーバーライドが表示されます。

ステップ 13　**Use Event Action Overrides** チェックボックスをオンにします。

（注）　Event Action Overrides パネルの **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。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。

ステップ 14　既存のイベント アクション オーバーライドを削除するには、リスト内でそれを選択して **Delete** をクリックします。

Event Action Overrides パネルのリストからそのイベント アクション オーバーライドが消去されます。

ステップ 15　イベント アクション オーバーライドをイネーブルまたはディセーブルにするには、**Enable** または **Disable** をクリックします。

ヒント　**Reset** をクリックして、変更を削除します。

ステップ 16　変更を適用し、改訂したコンフィギュレーションを保存するには、**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

この項では、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。取り上げる事項は次のとおりです。

概要

イベント アクション フィルタを設定して、イベントから特定のアクションを削除したり、センサーがそれ以上処理しないようにイベント全体を廃棄したりすることができます。Event Variables パネルで定義した変数を使用すれば、アドレスをグループ化してフィルタを適用できます。

（注）　変数の前にドル（$）記号を付けて、文字列ではなく変数を使用していることを示す必要があります。「$」を付けないと、`Bad source and destination` エラーが生じます。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

イベント アクション フィルタを設定するには、管理者またはオペレータである必要があります。

フィールド定義

この項では、イベント アクション フィルタのフィールドの定義を示します。取り上げる事項は次のとおりです。

Event Action Filters パネル

Event Action Filters パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **Use Event Action Filters**：イベント アクション フィルタのコンポーネントをイネーブルにします。

  イネーブルな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。
- **Name**：追加するフィルタに名前を指定します。

  必要に応じてフィルタをリスト内で移動したり、非アクティブ リストへ移動したりできるように、フィルタに名前を付けておく必要があります。

- **Active**：フィルタがフィルタ リストに配置されており、イベントのフィルタリングにおいて有効であるかどうかを示します。
- **Enabled**：このフィルタがイネーブルであ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固有の数値を示します。

  この値を使用すると、センサーが特定のシグニチャを識別できます。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固有の数値を示します。

  subSig ID は、広い範囲のシグニチャのバージョンをより細かく示すために使用します。subSig ID の範囲を入力することもできます。
- **Attacker (address/port)** : 違反パケットを送信したホストの IP アドレスまたはポート、もしくはその両方を示します。

  アドレスの範囲を入力することもできます。
- **Attacker (address/port)** : 攻撃者のホストによって使用された IP アドレスまたはポート、もしくはその両方を示します。

  これは、違反パケットの発信元ポートです。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する必要のある 0 ～ 100 までの RR 範囲を示します。

  ここで設定した最小値から最大値までの範囲内の RR を持つイベントが発生した場合、そのイベントはこのイベント フィルタのルールに従って処理されます。
- **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す場合に、イベントから除去する必要のあるアクションを示します。
- **Deny Pct**：拒否攻撃者機能によって拒否するパケットの率を示します。
- **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ついても処理するかどうかを決定します。

  No に設定すると、ストップ フラグが見つかるまで、残りのフィルタに対しても照合されます。

  Yes に設定すると、それ以上は処理されません。このフィルタによって指定されたアクションは除去され、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 コメントを示します。

ボタンの機能：

- **Select All**：リストに示されたイベント アクション フィルタをすべて選択します。
- **Add**：Add Event Action Filter ダイアログボックスを開きます。このダイアログボックスで、イベント アクション フィルタを追加し、そのフィルタに関連付ける値を指定できます。
- **Insert Before**：選択したイベント アクション フィルタの上にイベント アクション フィルタを追加します。

  Add Event Action Filter ダイアログボックスを開きます。
- **Insert After**：選択したイベント アクション フィルタの後ろにイベント アクション フィルタを追加します。

  Add Event Action Filter ダイアログボックスを開きます。
- **Move Up** : 選択したフィルタをリスト内で 1 行上に移動し、フィルタの処理順序を変更します。
- **Move Down**：選択したフィルタをリスト内で 1 行下に移動し、フィルタの処理順序を変更します。
- **Edit**：Edit Event Action Filter ダイアログボックスを表示します。このダイアログボックスで、このフィルタに関連付けられた値を変更できます。
- **Active**：イベントのフィルタリングにおいて有効となるように、フィルタをフィルタ リストに追加します。
- **Inactive**：イベントのフィルタリングにおいて無効となるようにフィルタをリストから外します。

- **Enable**：選択したイベント アクション フィルタをイネーブルにします。

  Event Action Filters パネルの **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。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 フィルタはイネーブルになりません。
- **Disable**：選択したイベント アクション フィルタをディセーブルにします。
- **Delete**：使用可能なフィルタのリストからこのイベント アクション フィルタを削除します。
- **Apply**：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。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

Add and Edit Event Action Filters ダイアログボックス

Add and Edit Event Action Filters ダイアログボックスには、次のフィールドとボタンがあります。

フィールドの説明：

- **Name**：追加するフィルタに名前を指定します。

  必要に応じてフィルタをリスト内で移動したり、非アクティブ リストへ移動したりできるように、フィルタに名前を付けておく必要があります。
- **Active**：イベントのフィルタリングにおいて有効となるように、フィルタをフィルタ リストに追加します。
- **Enabled**：このフィルタがイネーブルであるかどうかを示します。
- **Signature ID**：このシグニチャに割り当てられた固有の数値を示します。

  この値を使用すると、センサーが特定のシグニチャを識別できます。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固有の数値を示します。

  subSig ID は、広い範囲のシグニチャのバージョンをより細かく示すために使用します。subSig ID の範囲を入力することもできます。
- **Attacker Address**：違反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 Port**：攻撃者のホストによって使用されたポートを示します。

  これは、違反パケットの発信元ポートです。ポートの範囲を入力することもできます。
- **Victim Address**：攻撃を受けたホスト（違反パケットの受信者）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。
- **Victim Port**：違反パケットを受信した場合にそのパケットが経由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する必要のある 0 ～ 100 までの RR 範囲を示します。

  ここで設定した最小値から最大値までの範囲内の RR を持つイベントが発生した場合、そのイベントはこのイベント フィルタのルールに従って処理されます。
- **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す場合に、イベントから除去する必要のあるアクションを示します。
  - **Deny Attacker Inline**：（インライン モードのみ）指定された期間、この攻撃者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。

    センサーは、システムによって拒否されている攻撃者のリストを保持します。拒否された攻撃者のリストからエントリを削除するには、攻撃者のリストを表示してリスト全体をクリアするか、タイマーで有効期限が切れるのを待ちます。タイマーは、エントリごとにスライドするタイマーです。したがって、攻撃者 A が拒否されているときに別の攻撃が発行されると、攻撃者 A のタイマーはリセットされ、そのタイマーの有効期限が切れるまで攻撃者 A は拒否された攻撃者リストに残ります。拒否された攻撃者のリストがいっぱいになり、新規エントリを追加することができない場合でも、パケットは拒否されます。

（注）　これは、拒否アクションの中で最も重大です。これは、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を拒否します。拒否された攻撃者のエントリをすべてクリアするには、**Monitoring** > **Denied Attackers** > **Clear List** をクリックします。これによって、これらのアドレスのネットワークへの再接続が許可されます。手順については、P.11-3 の「拒否された攻撃者リストの監視」を参照してください。

- **Deny Attacker Service Pair Inline**：（インライン モードのみ）指定された期間、攻撃者アドレスと被害先ポートのペアで、このパケットおよび将来のパケットを送信しません。
- **Deny Attacker Victim Pair Inline**：（インライン モードのみ）指定された期間、攻撃者と被害先のアドレスのペアで、このパケットおよび将来のパケットを送信しません。

（注）　拒否アクションの場合、指定された期間と拒否された攻撃者の最大数を指定するには、**Configuration > Event Action Rules > General Settings** をクリックします。手順については、P.7-30 の「一般的な設定値の設定」を参照してください。

- **Deny Connection Inline**：（インライン モードのみ）この TCP フローの現在のパケットと将来のパケットを終了します。
- **Deny Packet Inline**：（インライン モードのみ）パケットを終了します。
- **Log Attacker Packets**：攻撃者アドレスを含む IP ロギング パケットを開始し、アラートを送信します。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、イベント ストアにアラートが書き込まれます。
- **Log Pair Packets**：攻撃者と被害先のアドレスのペアを含む IP ロギング パケットを開始します。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、イベント ストアにアラートが書き込まれます。
- **Log Victim Packets**：被害先のアドレスを含む IP ロギング パケットを開始し、アラートを送信します。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、イベント ストアにアラートが書き込まれます。
- **Modify Packet Inline**：パケット データを変更して、エンドポイントでパケットがどう処理されるかに関してあいまいな部分を除去します。

（注）　Modify Packet Inline は、Add Event Action Filter または Add Event Action Override のオプションではありません。

- **Produce 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。
- **Produce Verbose Alert**：違反パケットの符号化ダンプをアラートに組み込みます。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、イベント ストアにアラートが書き込まれます。
- **Request Block Connection**：この接続をブロックする要求を ARC に送信します。ブロッキング デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第 8 章「ブロッキングとレート制限のための ARC 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 ARC に送信します。ブロッキング デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第8章「ブロッキングとレート制限のための ARC の設定」を参照してください。

（注）　ブロック アクションの場合、ブロックの期間を設定するには、**Configuration > Event Action Rules > General Settings** をクリックします。手順については、P.7-30 の「一般的な設定値の設定」を参照してください。

  - **Request Rate Limit**：レート制限を実行するレート制限要求を ARC に送信します。レート制限デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第 8 章「ブロッキングとレート制限のための ARC の設定」を参照してください。
  - **Request SNMP Trap**：SNMP 通知を実行する要求をセンサーの通知アプリケーション コンポーネントに送信します。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、イベント ストアにアラートが書き込まれます。SNMP は、このアクションを実装するようセンサーで設定されている必要があります。詳細については、第 9 章「SNMP の設定」を参照してください。
  - **Reset TCP Connection**：TCP リセットを送信し、TCP フローを乗っ取って終了します。Reset TCP Connection は、単一の接続を分析する TCP シグニチャでのみ機能します。スイープやフラッドに対しては機能しません。

- **Deny Percentage**：拒否攻撃者機能によって拒否するパケットの率を決定します。有効範囲は 1 ～ 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ついても処理するかどうかを決定します。

  No に設定すると、ストップ フラグが見つかるまで、残りのフィルタに対しても照合されます。

  Yes に設定すると、それ以上は処理されません。このフィルタによって指定されたアクションは除去され、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 コメントを示します。

ボタンの機能：

- **OK**：変更を確定し、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄してダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

イベント アクション フィルタの設定

イベント アクション フィルタを設定するには、次の手順を実行します。

ステップ 1　管理者特権またはオペレータ特権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 > Event Action Rules > Event Action Filters** をクリックします。

Event Action Filters パネルが表示されます。

ステップ 3　イベント アクション フィルタを作成するには、次のいずれかを実行します。

- 新しいイベント アクション フィルタを追加するには、**Add** をクリックします。
- もしくは、フィルタを現在のフィルタの上または下に追加するには、フィルタを右クリックして、**Insert Before** または **Insert After** を選択します。

Add Event Action Filter ダイアログボックスが表示されます。

ステップ 4　**Signature ID** フィールドに、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。

シグニチャはリスト（2001, 2004）または範囲（2001–2004）で指定するか、Event Variables パネルで定義してあれば SIG 変数を使用して指定することもできます。変数の前には $ を付けます。

ステップ 5　**SubSignature ID** フィールドに、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 6　**Attacker 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 パネルで定義した場合は、変数のいずれかを使用できます。変数の前には $ を付けます。アドレスの範囲を入力することもできます（0.0.0.0 ～ 255.255.255.255）。

ステップ 7　**Attacker Port** フィールドに違反パケットを送信した攻撃者によって使用されたポート番号を入力します。

ステップ 8　**Victim Address** フィールドに受信側ホストの IP アドレスを入力します。

Event Variables パネルで定義した場合は、変数のいずれかを使用できます。変数の前には $ を付けます。アドレスの範囲を入力することもできます（0.0.0.0 ～ 255.255.255.255）。

ステップ 9　**Victim Port** フィールドに違反パケットを受信した被害先ホストによって使用されたポート番号を入力します。

ステップ 10　**Risk Rating** フィールドで、RR 範囲をこのフィルタに割り当てます。

イベントの RR が指定した範囲内の場合、イベントはこのフィルタの条件に従って処理されます。

ステップ 11　**Actions to Subtract** リストで、このフィルタによってイベントから削除するアクションを選択します。

ヒント　リスト内で複数のイベント アクションを選択するには、**Ctrl** キーを押した状態で選択します。

ステップ 12　**Deny Percentage** フィールドに、拒否攻撃者機能によって拒否するパケットの率を入力します。デフォルトは 100% です。

ステップ 13　Stop on Match の隣にある次のチェックボックスのいずれかをオンにします。

a. **Yes**：この特定のフィルタのアクションが削除された後、イベント アクション フィルタ コンポーネントの処理を停止する場合。

   残りのフィルタは処理されません。したがって、イベントからそれ以上のアクションは削除できません。

b. **No**：追加のフィルタも継続して処理する場合。

ステップ 14　Enabled の隣にある **Yes** をオンにして、このフィルタをイネーブルにします。

（注）　Event Action Filters パネルの **Use Event Action Filters** チェックボックスもオンにする必要があります。オンにしないと、Add Event Action Filter ダイアログボックスで **Yes** をオンにしたかどうかに関係なくイベント アクション フィルタはイネーブルになりません。

ステップ 15　Active の隣にある **Yes** をオンにして、イベントのフィルタリングにおいて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 16　**Comments** フィールドについてこのフィルタとともに保存するコメントを入力します。コメントには、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を記述します。

ヒント　変更を元に戻して 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 17　**OK** をクリックします。

Event Action Filters パネルのリストに新しいイベント アクション フィルタが表示されます。

ステップ 18　**Use Event Action Overrides** チェックボックスをオンにします。

（注）　Event Action Overrides パネルの **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。オンにしないと、Add Event Action Filter ダイアログボックスで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。

ステップ 19　既存のイベント アクション フィルタを編集するには、リスト内でそれを選択して **Edit** をクリックします。

Edit Event Action Filter ダイアログボックスが表示されます。

ステップ 20　必要に応じてフィールドの値を変更します。

フィールドの入力を完了する手順については、手順 3 ～ 14 を参照してください。

ヒント　変更を元に戻して 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 21　**OK** をクリックします。

Event Action Filters パネル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 22　**Use Event Action Overrides** チェックボックスをオンにします。

（注） Event Action Overrides パネルの **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。オンにしないと、Edit Event Action Filter ダイアログボックスで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。

ステップ 23 イベント アクション フィルタを削除するには、リスト内でそれを選択して **Delete** をクリックします。

Event Action Filters パネルのリストからそのイベント アクション フィルタが消去されます。

ステップ 24 イベント アクション フィルタをイネーブルまたはディセーブルにするには、**Enable** または **Disable** をクリックします。

ステップ 25 イベント アクション フィルタをリスト内で上または下に移動するには、**Move Up** または **Move Down** をクリックします。

ヒント **Reset** をクリックして、変更を削除します。

ステップ 26 変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。

一般的な設定値の設定

この項では、一般的な設定値の設定方法について説明します。取り上げる事項は次のとおりです。

概要

Summarizer および Meta Event Generator を使用するかどうかなど、イベント アクション ルールに適用する一般的な設定値を設定できます。Summarizer はイベントを 1 つのアラートにグループ化するため、センサーが送出するアラート数を削減できます。Meta Event Generator はコンポーネント イベントを処理します。コンポーネント イベントによって、センサーは一連のイベントにまたがって発生する不審なアクティビティを監視することができます。

注意　トラブルシューティングを目的とする場合以外、Summarizer や Meta Event Generator はオフにしないでください。Summarizer をオフにすると、すべてのシグニチャが要約なしの Fire All に設定されます。Meta Event Generator をオフにすると、すべての Meta エンジン シグニチャがディセーブルになります。

攻撃者を拒否する期間、拒否された攻撃者の最大数、ブロックを続ける期間を設定できます。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

イベント アクション ルールの一般的な設定値を設定するには、管理者またはオペレータである必要があります。

フィールド定義

General Settings パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **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 はイネーブルです。ディセーブルにすると、すべてのシグニチャが要約なしの **Fire All** に設定されます。個々のシグニチャを要約するように設定しても、Summarizer がイネーブルでない場合は、この設定は無視されます。
- **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 はイネーブルです。Meta Event Generator をディセーブルにすると、すべての Meta エンジン シグニチャがディセーブルになります。

- **Deny Attacker Duration**：インラインで攻撃者を拒否する秒数。
  有効範囲は 1 ～ 518400 です。デフォルトは 3600 です。
- **Block Attack Duration**：ホストまたは接続をブロックする分数。
  有効範囲は 1 ～ 10000000 です。デフォルトは 30 です。
- **Maximum Denied Attackers**：あらゆる時点において、システム内で拒否された攻撃者の数を制限します。
  有効範囲は 1 ～ 10000000 です。デフォルトは 10000 です。

ボタンの機能：

- **Apply**：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。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

イベント アクション ルールの一般的な設定値の設定

注意　Summarizer および Meta Event Generator はグローバル レベルで動作するため、それらを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します。

イベント アクション ルールの一般的な設定値を設定するには、次の手順を実行します。

ステップ 1　管理者特権またはオペレータ特権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 > Event Action Rules > General Settings** をクリックします。

General Settings パネルが表示されます。

ステップ 3　**Use Summarizer** を選択して Summarizer 機能をイネーブルにします。

注意　Summarizer をディセーブルにするのは、トラブルシューティングを目的とする場合だけです。それ以外の場合は、要約対象として設定するすべてのシグニチャが実際に要約されるように、必ず Summarizer をイネーブルにします。

ステップ 4　**Use Meta Event Generator** を選択して、Meta Event Generator をイネーブルにします。

注意　Meta Event Generator をディセーブルにするのは、トラブルシューティングを目的とする場合だけです。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、必ず Meta Event Generator をイネーブルにします。

ステップ 5　**Deny Attacker Duration** フィールドにインラインで攻撃者を拒否する秒数を入力します。

ステップ 6　**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 7　**Maximum Denied Attackers** フィールドに、すべての時点におけるシステム内で拒否された攻撃者の最大数を入力します。

ヒント　**Reset** をクリックして、変更を削除します。

ステップ 8　変更を適用し、改訂したコンフィギュレーションを保存するには、**Apply** をクリックします。

イベントの監視

この項では、イベントを監視する方法について説明します。取り上げる事項は次のとおりです。

概要

Events パネルで、イベント データをフィルタしたり表示したりできます。イベントの種類、時間、またはその両方に基づいて、イベントをフィルタリングできます。デフォルトでは、過去 1 時間のすべてのアラートとエラー イベントが表示されます。**View** をクリックすると、これらのイベントを表示できます。

View をクリックすると、IDM がイベントの時間範囲を定義します（未設定の場合）。範囲の終了時間を指定しなかった場合には、**View** をクリックした時点で終了するものとして定義されます。

センサーから多数のイベントを取得するときにシステム エラーが発生するのを防ぐために、IDM は 1 回に表示可能なイベント数を制限しています（ページあたりの最大行数は 500）。**Back** および **Next** をクリックすれば、さらに多くのイベントを表示できます。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

イベントの表示を設定するには、管理者である必要があります。

フィールド定義

この項では、イベントを設定および表示するためのフィールドの定義を示します。取り上げる事項は次のとおりです。

Events パネル

Events パネルには次のフィールドとボタンがあります。

フィールドの説明：

- **Show alert events**：表示するアラートのレベルを設定します。
  - **Informational**
  - **Low**
  - **Medium**
  - **High**

    デフォルトではすべてのレベルがイネーブルです。

- **Show error events**：表示するエラーの種類を設定します。
  - **Warning**
  - **Error**
  - **Fatal**

  デフォルトではすべてのレベルがイネーブルです。
- **Show Network Access Controller events**：ARC（以前は Network Access Controller と呼ばれていました）イベントを表示します。

  デフォルトはディセーブルです。
- **Show status events**：ステータス イベントを表示します。

  デフォルトはディセーブルです。
- **Select the number of the rows per page**：ページごとに表示する行数を決定します。

  有効範囲は 1 ～ 500 です。デフォルトは 100 です。
- **Show all events currently stored on the sensor**：センサーに保存されたすべてのイベントを取得します。
- **Show past events**：指定した時間数または分数を遡って、過去のイベントを表示します。
- **Show events from the following time range**：指定した時間範囲のイベントを取得します。

ボタンの機能：

- **View**：Event Viewer を表示します。
- **Reset**：作成した編集を前に設定した値と置換することによって、パネルをリフレッシュします。

Event Viewer ページ

Event Viewer ページには次のフィールドとボタンがあります。

- **#**：結果クエリーでのイベントのオーダー番号を示します。
- **Type**：イベントの種類を Error、NAC、Status、または Alert として示します。
- **Sensor UTC Time**：イベントがいつ発生したかを示します。
- **Event ID**：センサーがイベントに割り当てた数値の識別子。
- **Events**：イベントを簡潔に説明します。
- **Sig ID**：生成されアラート イベントを引き起こしたシグニチャを示します。

ボタンの機能：

- **Details**：選択したイベントの詳細を個別のダイアログボックスで表示します。

  アプリケーション、攻撃者、ターゲット、およびシグニチャの詳細を表示します。
- **Refresh**：Event Viewer を新しいイベントでリフレッシュします。
- **Back**：Event Viewer で前のページを表示します。
- **Next**：Event Viewer で次のページを表示します。
- **Close**：開いているダイアログボックスを閉じます。
- **Help**：該当の機能のヘルプ トピックを表示します。

イベント表示の設定

イベントの表示方法を設定するには、次の手順を実行します。

ステップ 1　管理者特権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　**Monitoring > Events** をクリックします。

Events パネルが表示されます。

ステップ 3　Events の下で、表示するアラートのレベルを選択します。

ステップ 4　Events の下で、表示するエラーの種類を選択します。

ステップ 5　ARC（以前は Network Access Controller と呼ばれていました）イベントを表示する場合は、**Show Network Access Controller events** を選択します。

ステップ 6　ステータス イベントを表示する場合は、**Show status events** を選択します。

ステップ 7　表示するページあたりの行数を選択します。

デフォルトは 100 です。有効な値は、100、200、300、400、または 500 です。

ステップ 8　イベントを表示する時間を設定する場合は、次のいずれかを選択します。

- **Show all events currently stored on the sensor**
- **Show past events**
  過去のイベントを表示するために遡る時間数と分数を入力します。
- **Show events from the following time range**
  開始時間と終了時間を選択します。

ヒント　**Reset** をクリックして、変更を削除します。

ステップ 9　**View** をクリックして、設定したイベントを表示します。

Event Viewer が表示されます。

ステップ 10　1 つの列で昇順または降順にソートするには、右側にある上向き矢印または下向き矢印をクリックします。

ステップ 11　**Next** または **Back** をクリックして、100 行ずつ表示されたページを移動します。

ステップ 12　イベントの詳細を表示するには、それを選択して **Details** をクリックします。

イベントの詳細は、別のダイアログボックスに表示されます。ダイアログボックスにはタイトルとしてイベント ID が示されます。