CHAPTER 8

イベント アクション規則の設定

（注） 現在、Cisco IPS 7.1 をサポートしているプラットフォームは、IPS SSP を搭載した Cisco ASA 5585 のみです。それ以外の Cisco IPS センサーは、IPS 7.1 を現在サポートしていません。

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

この章では、イベント アクション ルール ポリシーの追加方法とイベント アクション ルールの設定方法について説明します。次のような構成になっています。

セキュリティ ポリシーについて

複数のセキュリティ ポリシーを作成し、それらを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、および異常検出ポリシーから構成されます。Cisco IPS には、sig0 という名前のデフォルトのシグニチャ定義ポリシー、rules0 という名前のデフォルトのイベント アクション規則ポリシー、および ad0 という名前のデフォルトの異常検出ポリシーが用意されています。仮想センサーにこれらのデフォルト ポリシーを割り当てることも、新しいポリシーを作成することもできます。複数のセキュリティ ポリシーを使用すれば、それぞれ異なる要件に基づいたセキュリティ ポリシーを作成し、そうしたカスタマイズされたポリシーを VLAN や物理インターフェイスごとに適用することが可能になります。

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に対して行う設定のグループです。これらのルールは、イベント発生時にセンサーが実行するアクションを制御します。イベント アクション処理コンポーネントは、次の機能を提供します。

- リスク レーティングの計算
- 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
- 結果となるイベント アクションの実行
- イベントのサマライズと集約
- 拒否攻撃者リストの保持

（注） IPv6 トラフィックに対するレート制限およびブロッキングはサポートされていません。シグニチャにブロックまたはレート制限イベント アクションが設定されている場合、IPv6 トラフィックによってそのシグニチャがトリガーされると、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。

シグニチャ イベント アクション プロセッサ

シグニチャ イベント アクション プロセッサは、アラーム チャネル内のシグニチャ イベントから、シグニチャ イベント アクション オーバーライド、シグニチャ イベント アクション フィルタの処理を経由してシグニチャ イベント アクション ハンドラで処理されるまでのデータ フローを調整します。シグニチャ イベント アクション プロセッサは、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：sensorApp 検査パスからシグニチャ イベント処理にシグニチャ イベントを伝える領域を表すユニット。
- シグニチャ イベント アクション オーバーライド：リスク レーティング値に基づいてアクションを追加します。シグニチャ イベント アクション オーバーライドは、設定済みのリスク レーティングしきい値の範囲内にあるすべてのシグニチャに適用されます。各シグニチャ イベント アクション オーバーライドは独立しており、各アクション タイプには別個の値が設定されています。
- シグニチャ イベント アクション フィルタ：シグニチャ ID、アドレス、およびシグニチャ イベントのリスク レーティングに基づいてアクションを削除します。シグニチャ イベント アクション フィルタへ入力するのは、シグニチャ イベント アクション オーバーライド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） シグニチャ イベント アクション フィルタが実行できるのはアクションの削除だけであり、新しいアクションの追加はできません。

  シグニチャ イベント アクション フィルタには、次のパラメータが適用されます。

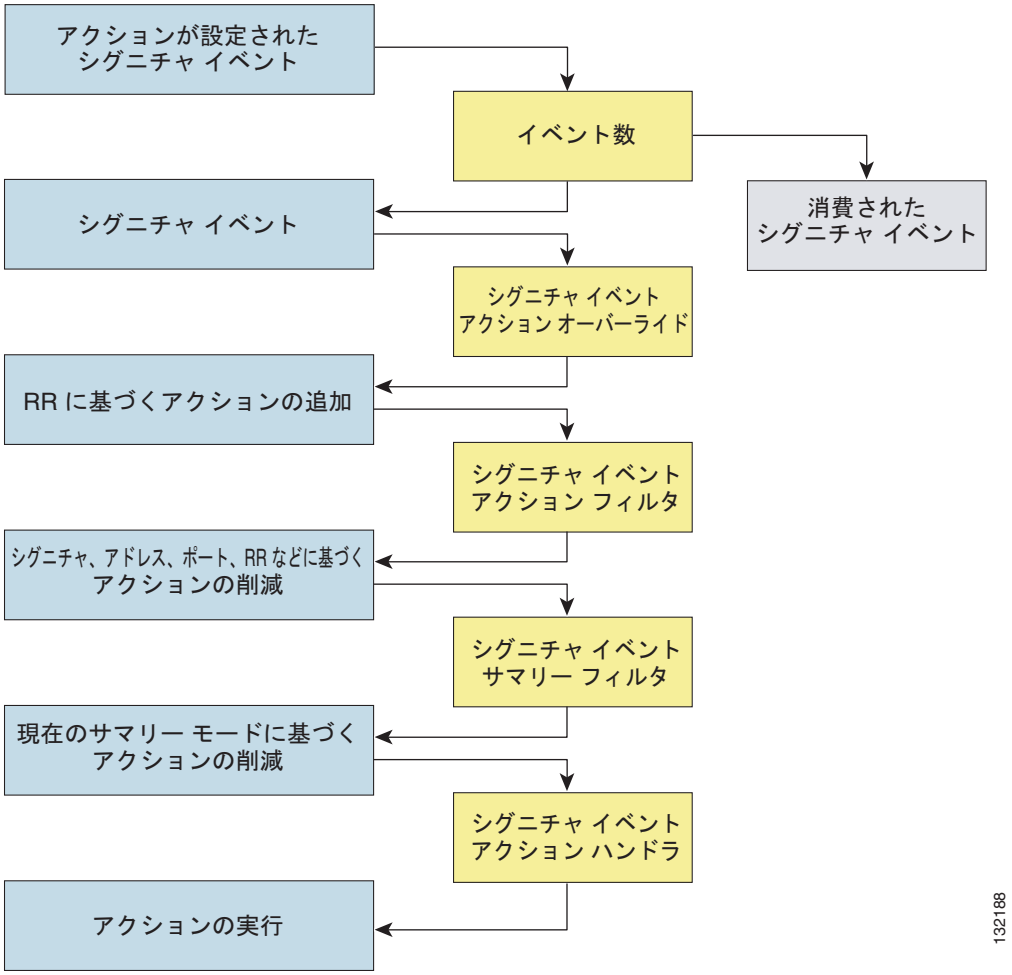
  - シグニチャ ID
  - サブシグニチャ ID
  - 攻撃者のアドレス
  - 攻撃者のポート
  - 攻撃対象のアドレス

- 攻撃対象のポート
- リスク レーティングしきい値の範囲
- 削除するアクション
- シーケンス識別子（任意）
- 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
- 攻撃対象の OS の関連性または OS の関連性

- シグニチャ イベント アクション ハンドラ：要求されたアクションを実行します。シグニチャ イベント アクション ハンドラ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 8-1 に、シグニチャ イベント アクション プロセッサを通過するシグニチャ イベントの論理的なフローと、このイベントのアクションで実行される操作を示します。これは、アラーム チャネルで受信された、アクションが設定されているシグニチャ イベントで開始され、シグニチャ イベントがシグニチャ イベント アクション プロセッサ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 8-1　シグニチャ イベント アクション プロセッサを通過するシグニチャ イベント



詳細情報

リスク レーティングの詳細については、「リスク レーティングの計算」（P.8-12）を参照してください。

イベント アクション

Cisco IPS は、次のイベント アクションをサポートします。ほとんどのイベント アクションは、その特定のエンジンに対して適切である限り、各シグニチャ エンジンに属します。

アラートおよびログ アクション

- 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。

（注）　produce-alert アクションは、シグニチャに対してアラートをイネーブルにした場合に、自動的に実行されません。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。イベント ストアにアラートを送信する場合は、2 番目のアクションを追加するときに、produce-alert を含める必要があります。また、イベント アクションを設定するたびに、新しいリストが作成され、古いリストと置き換わります。各シグニチャに必要なすべてのイベント アクションを含めてください。

（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：アラートの不正なパケットの符号化されたダンプを含みます。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-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-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。
- 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。
- request-snmp-trap：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て SNMP 通知を実行します。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。このアクションを実装するには、センサーで SNMP を設定する必要があります。

拒否アクション

- deny-packet-inline（インラインだけ）：パケットを終了します。

（注）　deny-packet-inline に対するイベント アクション オーバーライドは保護されているため、削除できません。このオーバーライドを使用しない場合は、このエントリに対する override-item-status をディセーブルに設定してください。

- deny-connection-inline（インラインだけ）: この TCP フローで現在と将来のパケットを終了します。
- deny-attacker-victim-pair-inline（インラインだけ）: 指定された期間、攻撃者と攻撃対象のアドレスのペアに対してこのパケットと将来のパケットを送信しません。
- deny-attacker-victim-pair-inline（インラインだけ）: 指定された期間、攻撃者のアドレスと攻撃対象のポートのペアに対してこのパケットと将来のパケットを送信しません。
- deny-attacker-inline（インラインだけ）: 指定された期間、この攻撃者のアドレスからの現在と将来のパケットを終了します。
- センサーによって、システムで拒否される攻撃者のリストは保持されます。拒否攻撃者リストからエントリを削除するために、攻撃者のリストを参照し、リスト全体をクリアしたり、タイマーが期限切れになるのを待ったりすることができます。タイマーは、各エントリのスライディング タイマーです。したがって、攻撃者 A が拒否されても別の攻撃を行う場合、攻撃者 A のタイマーはリセットされ、タイマーの期限が切れるまで攻撃者 A は拒否攻撃者リストに残ります。拒否攻撃者リストがいっぱいになり、新しいエントリを追加できない場合は、パケットは引き続き拒否されます。
- modify-packet-inline（インラインだけ）: エンド ポイントがパケットで行うことを明確にするためにパケット データを変更します。

（注）　イベント アクション フィルタまたはオーバーライドを追加する場合は、modify-packet-inline をアクションとして使用できません。

その他のアクション

- request-block-connection : 要求を ARC に送信してこの接続をブロックします。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。

（注）　適応型セキュリティ アプライアンスでは、接続ブロックとネットワーク ブロック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、接続情報が追加されたホスト ブロックだけがサポートされます。

（注）　IPv6 では、request-block-connection はサポートされません。

- request-block-host : 要求を ARC に送信して、この攻撃者ホストをブロックします。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。

（注）　IPv6 では、request-block-host はサポートされません。

- request-rate-limit : レート制限要求を ARC に送信して、レート制限を実行します。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。

（注）　request-rate-limit アクションは、特定のシグニチャ セットに適用されます。

（注）　IPv6 では、request-rate-limit はサポートされません。

- reset-tcp-connection：TCP リセットを送信して、TCP フローを乗っ取って終了します。reset-tcp-connection アクションは、単一の接続を分析する TCP シグニチャだけで動作します。スイープまたはフラッドに対しては機能しません。

パケットのインライン拒否について

deny-packet-inline がアクションとして設定されているシグニチャの場合、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、次のアクションが実行される場合があります。

- droppedPacket
- deniedFlow
- tcpOneWayResetSent

deny-packet-inline アクションは、アラート内でドロップ パケット アクションとして表示されます。deny-packet-inline が TCP 接続に対して発生すると、自動的に deny-connection-inline アクションにアップグレードされ、アラート内で拒否フローとして表示されます。IPS がパケットを 1 つだけ拒否しても、TCP は同じパケットの送信を繰り返し試みます。そのため、IPS で接続全体を拒否して、再送信が必ず失敗するようにします。

deny-connection-inline が発生すると同時に、IPS は自動的に TCP 単方向リセットを送信します。これは、アラート内で、送信された TCP 単方向リセットとして表示されます。IPS は、接続を拒否するとき、開いている接続をクライアント（一般に攻撃者）とサーバ（一般に攻撃対象）の両方にそのまま残します。開いている接続が多くなりすぎると、攻撃対象にリソースの問題が発生する可能性があります。そのため、IPS は TCP リセットを攻撃対象に送信して、攻撃対象（通常はサーバ）側の接続を閉じます。これにより、攻撃対象のリソースが保護されます。さらに、フェールオーバーも阻止されます。それにより、接続が別のネットワーク パスにフェールオーバーして、攻撃対象に到達するようなことはなくなります。IPS は、攻撃者側を開いたままにし、攻撃者側からのすべてのトラフィックを拒否します。

詳細情報

- 拒否攻撃者の設定手順については、「拒否攻撃者リストのモニタリングとクリア」（P.8-37）を参照してください。
- 一般設定の手順については、「一般設定」（P.8-34）を参照してください。
- ブロッキング デバイスの設定の手順については、第 14 章「Attack Response Controller で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。
- SNMP の設定の手順については、第 15 章「SNMP の設定」を参照してください。

イベント アクション ルールの設定手順

IPS のイベント アクション ルール コンポーネントを設定する場合は、次の手順を実行します。

1. イベント アクション フィルタで使用する任意の変数を作成します。
2. ターゲットの価値レーティングを作成します。ターゲットの価値レーティングをネットワーク資産に割り当て、リスク レーティングを計算できるようにします。
3. リスク レーティング値に基づいてアクションを追加するオーバーライドを作成します。各イベント アクション タイプにリスク レーティングを割り当てます。
4. フィルタを作成します。ID、IP アドレス、およびシグニチャのリスク レーティングに基づいてアクションを削除するフィルタを割り当てます。

5. OS マッピングを作成します。OS マッピングは、アラートのリスク レーティングの計算で攻撃関連性レーティングに対して使用されます。
6. 一般設定を行います。サマライザまたはメタ イベント ジェネレータを使用するかどうか、あるいは拒否攻撃者パラメータを設定するかどうかを指定します。

イベント アクション ルール ポリシーの使用

サービス イベント アクション ルール サブモードで **service event-action-rules** *name* コマンドを使用して、イベント アクション ルール ポリシーを作成します。このイベント アクション ルール ポリシーの値は、編集するまでデフォルトのイベント アクション ルールポリシーである rules0 と同じです。

また、特権 EXEC モードで、**copy event-action-rules** *source_destination* コマンドを使用して、既存のポリシーのコピーを作成し、必要に応じて新しいポリシーの値を編集することもできます。

特権 EXEC モードで **list event-action-rules-configurations** コマンドを使用して、イベント アクション ルール ポリシーをリストします。

グローバル コンフィギュレーション モードで **no service event-action-rules** *name* コマンドを使用して、イベント アクション ルール ポリシーを削除します。グローバル コンフィギュレーション モードで **default service event-action-rules** *name* コマンドを使用して、イベント アクション ルール ポリシーを工場出荷時の設定にリセットします。

イベント アクション ルール ポリシーを作成、コピー、表示、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　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　イベント アクション ルール ポリシーを作成します。

```
ips-ssp# configure terminal
ips-ssp(config)# service event-action-rules MyRules
ips-ssp(config-eve)# exit
Apply Changes?[yes]: yes
ips-ssp(config)# exit
ips-ssp#
```

ステップ 3　既存のイベント アクション ルール ポリシーを新しいイベント アクション ルール ポリシーにコピーします。

```
ips-ssp# copy event-action-rules rules0 rules1
ips-ssp#
```

（注）　ポリシーがすでに存在しているか、新しいポリシーに必要な容量が不足していると、エラーが表示されます。

ステップ 4　デフォルトのイベント アクション ルール ポリシー値を受け入れるか、次のパラメータを編集します。

a. イベント アクション ルール変数を追加します。
b. イベント アクション ルール オーバーライドを設定します。
c. イベント アクション ルール フィルタを設定します。
d. イベント アクション ルールの一般設定を行います。
e. イベント アクション ルールを設定します。
f. イベント アクション ルール OS ID の設定を行います。

ステップ 5　イベント アクション ルール ポリシーのリストをセンサーに表示します。

```
ips-ssp# list event-action-rules-configurations
Event Action Rules
   Instance   Size   Virtual sensor
   rules0     255    vs0
   temp       707    N/A
   MyRules    255    N/A
   rules1     141    vs1
ips-ssp#
```

ステップ 6　イベント アクション ルール ポリシーを削除します。

```
ips-ssp(config)# no service event-action-rules MyRules
ips-ssp(config)#
```

（注）　デフォルトのイベント アクション ルール ポリシーである rules0 を削除することはできません。

ステップ 7　イベント アクション ルール インスタンスが削除されたことを確認します。

```
ips-ssp# list event-action-rules-configurations
Event Action Rules
   Instance   Size   Virtual sensor
   rules0     112    vs0
   rules1     142    N/A
ips-ssp#
```

ステップ 8　イベント アクション ルール ポリシーを工場出荷時の設定にリセットします。

```
ips-ssp# configure terminal
ips-ssp(config)# default service event-action-rules rules1
ips-ssp(config)#
```

詳細情報

- イベント アクション ルール変数を追加する手順については、「イベント アクション変数」（P.8-8）を参照してください。
- イベント アクション ルール オーバーライドの設定手順については、「イベント アクション オーバーライドの設定」（P.8-16）を参照してください。
- イベント アクション ルール フィルタの設定手順については、「イベント アクション フィルタの設定」（P.8-20）を参照してください。
- 一般設定の手順については、「一般設定」（P.8-33）を参照してください。
- イベント アクション ルールのターゲットの価値レーティングの設定手順については、「ターゲットの価値レーティングの設定」（P.8-12）を参照してください。
- OS マップの設定手順については、「OS ID の設定」（P.8-26）を参照してください。

イベント アクション変数

ここでは、イベント アクション変数について説明します。次のような構成になっています。

イベント アクション変数について

（注）　グローバル相関インスペクションとレピュテーション フィルタリング拒否機能では、IPv6 アドレスはサポートされません。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）　IPv6 トラフィックに対するレート制限およびブロッキングはサポートされていません。シグニチャにブロックまたはレート制限イベント アクションが設定されている場合、IPv6 トラフィックによってそのシグニチャがトリガーされると、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、イベント アクション フィルタでこれらの変数を使用できます。同じ値を複数のフィルタで使用する場合は、変数を使用します。この変数の値を変更すると、この変数を使用するすべてのフィルタが新しい値で更新されます。

（注）　文字列でなく変数を使っていることを示すために、変数をドル記号（$）で始める必要があります。

一部の変数は、シグニチャ システムに対して必須であるため、削除することはできません。変数が保護されている場合は、その変数を選択して編集することはできません。保護されている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、次のように完全な IP アドレス、範囲、または範囲のセットを指定します。

- 192.0.2.3-192.0.2.26
- 10.90.1.1
- 192.56.10.1-192.56.10.255
- 10.1.1.1-10.2.255.255, 192.0.2.3-192.0.2.26

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 128 ビットであり、16 進数で表現され、8 個の 16 ビット グループにコロンで区切られます。先頭のゼロを省略することができ、間のゼロのグループを二重コロン（::）で表すことができます。アドレスを 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 グループに適用される IP アドレス空間があり、そのグループに Windows システムが存在せず、そのグループに対する Windows ベースの攻撃について心配する必要がない場合は、そのエンジニアリング グループの IP アドレス空間に変数を設定できます。次に、この変数を使用して、このグループに対するすべての Windows ベースの攻撃を無視するフィルタを設定できます。

イベント アクション変数の追加、編集、および削除

（注）　グローバル相関インスペクションとレピュテーション フィルタリング拒否機能では、IPv6 アドレスはサポートされません。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）　IPv6 トラフィックに対するレート制限およびブロッキングはサポートされていません。シグニチャにブロックまたはレート制限イベント アクションが設定されている場合、IPv6 トラフィックによってそのシグニチャがトリガーされると、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。

サービス イベント アクション ルール サブモードで **variables** *variable_name* **address** *ip_address* コマンドを使用して、IPv4 イベント アクション変数を作成します。IPv4 アドレスは、1 つのアドレス、1 つの範囲、またはカンマで区切られた複数の範囲のいずれかです。

サービス イベント アクション ルール サブモードで **variables** *variable_name* **ipv6-address** *ip_address* コマンドを使用して、IPv6 イベント アクション変数を作成します。IPv6 アドレスは 128 ビットであり、16 進数で表現され、8 個の 16 ビット グループにコロンで区切られます。先頭のゼロを省略することができ、間のゼロのグループを二重コロン（::）で表すことができます。アドレスを 2001:db8 プレフィクスで始める必要があります。

サービス イベント アクション ルール サブモードで **no variables** *variable_name* コマンドを使用して、イベント アクション変数を削除します。

イベント アクション変数を追加、削除、および編集するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　イベント アクション ルール サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service event-action-rules rules0
```

ステップ 3　IPv4 イベント アクション ルール変数を追加します。**address** の有効な値は A.B.C.D-A.B.C.D [,A.B.C.D-A.B.C.D] です。

```
ips-ssp(config-eve)# variables variable-ipv4 address 192.0.2.3
```

ステップ 4　IPv6 イベント アクション ルール変数を追加します。**ipv6-address** の有効な形式は、<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>] です。

```
ips-ssp(config-eve)# variables variable-ipv6 ipv6-address
2001:0db8:3c4d:0015:0000:0000:abcd:ef12
```

ステップ 5　イベント アクション ルール変数が追加されたことを確認します。

```
ips-ssp(config-eve)# show settings
   variables (min: 0, max: 256, current: 2)
   -----------------------------------------------
      variableName: variable-ipv6
      -----------------------------------------------
         ipv6-address: 2001:0db8:3c4d:0015:0000:0000:abcd:ef12 default: ::0-FFFF
:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
      -----------------------------------------------
      variableName: variable-ipv4
      -----------------------------------------------
         address: 192.0.2.3 default: 0.0.0.0-255.255.255.255
      -----------------------------------------------
   -----------------------------------------------
```

ステップ 6　イベント アクション ルール変数を編集するには、IPv6 アドレスを範囲に変更します。

```
ips-ssp(config-eve)# variables variable-ipv6 ipv6-address
::0-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
```

ステップ 7　イベント アクション ルール変数が編集されたことを確認します。

```
ips-ssp(config-eve)# show settings
   variables (min: 0, max: 256, current: 2)
   -----------------------------------------------
      variableName: variable-ipv6
      -----------------------------------------------
         ipv6-address: ::0-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF default: ::0
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
      -----------------------------------------------
```

ステップ 8　イベント アクション ルール変数を削除します。

```
ips-ssp(config-eve)# no variables variable-ipv6
```

ステップ 9　イベント アクション ルール変数が削除されたことを確認します。

```
ips-ssp(config-eve)# show settings
   variables (min: 0, max: 256, current: 1)
   -----------------------------------------------
      variableName: variableipv4
      -----------------------------------------------
         address: 192.0.2.3 default: 0.0.0.0-255.255.255.255
      -----------------------------------------------
   -----------------------------------------------
```

ステップ 10　イベント アクション ルール サブモードを終了します。

```
ips-ssp(config-eve)# exit
Apply Changes:?[yes]:
```

ステップ 11　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

ターゲットの価値レーティングの設定

ここでは、リスク レーティングと、リスク レーティングを使用してターゲットの価値レーティングを設定する方法について説明します。ここでは、次の項目について説明します。

リスク レーティングの計算

リスク レーティング（RR）は、ネットワークでの特定のイベントに関連するリスクの数値化を表す、0 ～ 100 の値です。この計算では、攻撃されるネットワーク資産（特定のサーバなど）の値が考慮され、攻撃の重大度レーティングを使用してシグニチャごと、およびターゲットの価値レーティングを使用してサーバごとに設定が行われます。リスク レーティングは、複数のコンポーネントから計算されます。これらのコンポーネントの一部は設定、収集、および派生されます。

（注）　リスク レーティングは、シグニチャではなくアラートに関連します。

リスク レーティングを使用すると、注意が必要なアラートの優先順位を決定できます。リスク レーティングでは、攻撃の重大度（攻撃に成功した場合）、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 ホストの全体的な値が考慮されます。リスク レーティングは、evIdsAlert で報告されます。

次の値を使用して、特定のイベントのリスク レーティングが計算されます。

- シグニチャ忠実度レーティング（SFR）：ターゲットに関する具体的な知識がない場合のこのシグニチャのパフォーマンスに関連する重み。シグニチャ忠実度レーティングは、シグニチャごとに設定され、イベントや記述する条件をシグニチャがどの程度正確に検出するかを示します。

  シグニチャ忠実度レーティングは、シグニチャの作成者によってシグニチャごとに計算されます。シグニチャの作成者は、ターゲットに関する適切な情報がない場合のシグニチャの正確性に関する基本的な信頼性ランキングを定義します。これは、分析対象のパケットを送信するのが許可された場合に、検出された動作がターゲット プラットフォームで期待された結果をもたらすことに関する信頼性を表します。たとえば、非常に具体的なルール（特定の正規表現）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も高いシグニチャ忠実度レーティングとなります。

  （注）　シグニチャ忠実度レーティングは、検出されたイベントがどれだけ悪いかを示しません。

- 攻撃の重大度レーティング（ASR）：成功した脆弱性攻撃の重大度に関連する重み。攻撃の重大度レーティングは、シグニチャのアラート重大度パラメータ（informational、low、medium、または high）からの派生値です。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度を示します。

  （注）　攻撃の重大度レーティングは、イベントがどれだけ正確に検出されたかを示しません。

- ターゲットの価値レーティング（TVR）：ターゲットの認識された値に関連する重み。

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

- 攻撃関連性レーティング（ARR）：ターゲット オペレーティング システムの重要度に関連する重み。攻撃関連性レーティングは、アラート時に決定される派生値（relevant、unknown、または relevant）です。関連するオペレーティング システムは、シグニチャごとに設定されます。

- 無差別デルタ（PD）：無差別モードで全体のリスク レーティングから削除できる無差別デルタに関連する重み。無差別デルタは 0 ～ 30 の範囲にあり、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は、無差別デルタがレーティングから削除されます。

- ウォッチ リスト レーティング（WLR）：0 ～ 100（CSA MC は範囲 0 ～ 35 だけを使用）の範囲の、CSA MC ウォッチ リストに関連する重み。アラートの攻撃者がウォッチ リストで見つかると、その攻撃者のウォッチ リスト レーティングがこのレーティングに追加されます。

図 8-2 に、リスク レーティングの計算式を図示します。

図 8-2　リスク レーティングの計算式

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

191016

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 アクションにより下がったリスク レーティングです。非ロギング イベント アクションでは、脅威レーティングが調整されます。実行されたすべてのイベント アクションからの最大脅威レーティングは、リスク レーティングから削除されます。

イベント アクションの脅威レーティングは、次のとおりです。

- 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

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とレピュテーション フィルタリング拒否機能では、IPv6 アドレスはサポートされません。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）　IPv6 トラフィックに対するレート制限およびブロッキングはサポートされていません。シグニチャにブロックまたはレート制限イベント アクションが設定されている場合、IPv6 トラフィックによってそのシグニチャがトリガーされると、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。

IPv4 アドレスの場合は、サービス イベント アクション ルール サブモードで、**target-value** {**zerovalue** | **low** | **medium** | **high** | **mission-critical**} **target-address** *ip_address* コマンドを使用してネットワーク資産のターゲットの価値レーティングを追加します。デフォルトは [medium] です。サービス イベント アクション ルール サブモードで **no target-value** {**zerovalue** | **low** | **medium** | **high** | **mission-critical**} コマンドを使用して、ターゲットの価値レーティングを削除します。

IPv6 アドレスの場合は、サービス イベント アクション ルール サブモードで **ipv6-target-value** {**zerovalue** | **low** | **medium** | **high** | **mission-critical**} **ipv6-target-address** *ip_address* コマンドを使用して、ネットワーク資産のターゲットの価値レーティングを追加します。デフォルトは [medium] です。サービス イベント アクション ルール サブモードで **no ipv6-target-value** {**zerovalue** | **low** | **medium** | **high** | **mission-critical**} コマンドを使用して、ターゲットの価値レーティングを削除します。

オプション

次のオプションが適用されます。

- **target-value**：IPv4 ターゲットの価値レーティングを指定します。
  - **zerovalue**：このターゲットの値なし。
  - **low**：このターゲットの低い値。
  - **medium**：このターゲットの通常の値（デフォルト値）。
  - **high**：このターゲットの高い値。
  - **mission-critical**：このターゲットの異常な値。
- **no target-value**：IPv4 ターゲットの価値レーティングを削除します。
- **target-address** *ip_address*：<A.B.C.D>-<A.B.C.D>[,<A.B.C.D>-<A.B.C.D>] という形式で IPv4 アドレス用 IP アドレスの範囲セットを指定します。
- **ipv6-target-value**：IPv6 ターゲットの価値レーティングを指定します。
  - **zerovalue**：このターゲットの値なし。
  - **low**：このターゲットの低い値。
  - **medium**：このターゲットの通常の値（デフォルト値）。
  - **high**：このターゲットの高い値。

  - **mission-critical**：このターゲットの異常な値。
- **no ipv6-target-value**：IPv6 ターゲットの価値レーティングを削除します。
- **ipv6-target-address** *ip_address*：次の形式で IPv6 アドレス用 IP アドレスの範囲セットを指定します。
  <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>]

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　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　イベント アクション ルール サブモードを開始します。

```
sensor# configure terminal
sensor(config)# service event-action-rules rules1
```

ステップ 3　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ます。

```
sensor(config-eve)# target-value mission-critical target-address 192.0.2.3
```

ステップ 4　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ます。

```
sensor(config-eve)# ipv6-target-value mission-critical ipv6-target-address
2001:0db8:3c4d:0015:0000:0000:abcd:ef12
```

ステップ 5　ターゲットの価値レーティングが追加されたことを確認します。

```
sensor(config-eve)# show settings
-----------------------------------------------
   target-value (min: 0, max: 5, current: 1)
   -----------------------------------------------
      target-value-setting: mission-critical
      target-address: 192.0.2.3 default: 0.0.0.0-255.255.255.255
   -----------------------------------------------
   ipv6-target-value (min: 0, max: 5, current: 2)
   -----------------------------------------------
      ipv6-target-value-setting: mission-critical
      ipv6-target-address: 2001:0db8:3c4d:0015:0000:0000:abcd:ef12 default: ::0-
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
   -----------------------------------------------
sensor(config-eve)#
```

ステップ 6　ターゲットの価値レーティングを編集するには、資産のターゲットの価値レーティング設定を変更します。

```
sensor(config-eve)# target-value low target-address 192.0.2.3
```

ステップ 7　ターゲットの価値レーティングが編集されたことを確認します。

```
sensor(config-eve)# show settings
-----------------------------------------------
 target-value (min: 0, max: 5, current: 1)
 -----------------------------------------------
    target-value-setting: low
    target-address: 192.0.2.3 default: 0.0.0.0-255.255.255.255
 -----------------------------------------------
```

ステップ 8　ターゲットの価値レーティングを削除します。

```
sensor(config-eve)# no ipv6-target-value mission-critical
```

ステップ 9　ターゲットの価値レーティングが削除されたことを確認します。

```
sensor(config-eve)# show settings
-----------------------------------------------
 ipv6-target-value (min: 0, max: 5, current: 0)
 -----------------------------------------------
 -----------------------------------------------
```

ステップ 10　イベント アクション ルール サブモードを終了します。

```
sensor(config-rul)# exit
Apply Changes:?[yes]:
```

ステップ 11　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

イベント アクション オーバーライドの設定

ここでは、イベント アクション オーバーライドについて説明します。次のような構成になっています。

イベント アクション オーバーライドについて

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 以上のイベントによって SNMP トラップを生成する場合は、request-snmp-trap のリスク レーティング範囲を 85-100 に設定できます。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）　適応型セキュリティ アプライアンスでは、接続ブロックとネットワーク ブロック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、接続情報が追加されたホスト ブロックだけがサポートされます。

パケットのインライン拒否について

deny-packet-inline がアクションとして設定されているシグニチャの場合、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、次のアクションが実行される場合があります。

- droppedPacket
- deniedFlow
- tcpOneWayResetSent

deny-packet-inline アクションは、アラート内でドロップ パケット アクションとして表示されます。deny-packet-inline が TCP 接続に対して発生すると、自動的に deny-connection-inline アクションにアップグレードされ、アラート内で拒否フローとして表示されます。IPS がパケットを 1 つだけ拒否しても、TCP は同じパケットの送信を繰り返し試みます。そのため、IPS で接続全体を拒否して、再送信が必ず失敗するようにします。

deny-connection-inline が発生すると同時に、IPS は自動的に TCP 単方向リセットを送信します。これは、アラート内で、送信された TCP 単方向リセットとして表示されます。IPS は、接続を拒否するとき、開いている接続をクライアント（一般に攻撃者）とサーバ（一般に攻撃対象）の両方にそのまま残します。開いている接続が多くなりすぎると、攻撃対象にリソースの問題が発生する可能性があります。そのため、IPS は TCP リセットを攻撃対象に送信して、攻撃対象（通常はサーバ）側の接続を閉じます。これにより、攻撃対象のリソースが保護されます。さらに、フェールオーバーも阻止されます。それにより、接続が別のネットワーク パスにフェールオーバーして、攻撃対象に到達するようなことはなくなります。IPS は、攻撃者側を開いたままにし、攻撃者側からのすべてのトラフィックを拒否します。

イベント アクション オーバーライドの追加、編集、イネーブル化、およびディセーブル化

サービス イベント アクション ルール サブモードで **overrides** {**request-block-connection** | **request-block-host** | **deny-attacker-inline** | **deny-packet-inline** | **deny-attacker-service-pair-inline** | **deny-attacker-victim-pair-inline** | **deny-connection-inline** | **log-attacker-packets** | **log-victim-packets** | **log-pair-packets** | **reset-tcp-connection** | **produce-alert** | **produce-verbose-alert** | **request-rate-limit** | **request-snmp-trap**} コマンドを使用して、イベント アクション オーバーライドのパラメータを設定します。サービス イベント アクション ルール サブモードで **no overrides** コマンドを使用して、イベント アクション オーバーライドのパラメータを削除します。

オーバーライド イベント アクション、次にリスク レーティング範囲を設定し、オーバーライドをイネーブルまたはディセーブルにします。

（注）　deny-packet-inline に対するイベント アクション オーバーライドは保護されているため、削除できません。このオーバーライドを使用しない場合は、このエントリに対する override-item-status をディセーブルに設定してください。

オプション

次のオプションが適用されます。

- **no overrides**：エントリまたは選択設定を削除します。
- **override-item-status** {**enabled** | **disabled**}：このオーバーライド アイテムの使用をイネーブルまたはディセーブルにします。デフォルトはイネーブルです。
- **risk-rating-range**：このオーバーライド アイテムのリスク レーティング値の範囲を指定します。デフォルトは 0 ～ 100 です。
- **show**：システム設定または履歴情報を表示します。

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 オーバーライドを追加するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　イベント アクション ルール サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service event-action-rules rules0
ips-ssp(config-eve)#
```

ステップ 3　オーバーライドのアクションを割り当てます。

- 攻撃者の送信元 IP アドレスからのパケットを拒否します。

```
ips-ssp(config-eve)# overrides deny-attacker-inline
ips-ssp(config-eve-ove)#
```

- アラートを引き起こす単一パケットを送信しません。

```
ips-ssp(config-eve)# overrides deny-packet-inline
ips-ssp(config-eve-ove)#
```

- 指定された TCP 接続でパケットを送信しません。

```
ips-ssp(config-eve)# overrides deny-connection-inline
ips-ssp(config-eve-ove)#
```

- 接続を終了するために TCP RST パケットを送信します。

```
ips-ssp(config-eve)# overrides reset-tcp-connection
ips-ssp(config-eve-ove)#
```

- 接続のブロックを要求します。

```
ips-ssp(config-eve)# overrides request-block-connection
ips-ssp(config-eve-ove)#
```

- 攻撃者のホストのブロックを要求します。

```
ips-ssp(config-eve)# overrides request-block-host
ips-ssp(config-eve-ove)#
```

- 攻撃者の IP アドレスからのパケットをログに記録します。

```
ips-ssp(config-eve)# overrides log-attacker-packets
ips-ssp(config-eve-ove)#
```

- 攻撃対象の IP アドレスからのパケットをログに記録します。

```
ips-ssp(config-eve)# overrides log-victim-packets
ips-ssp(config-eve-ove)#
```

- 攻撃者と攻撃対象の両方の IP アドレスからのパケットをログに記録します。

```
ips-ssp(config-eve)# overrides log-pair-packets
ips-ssp(config-eve-ove)#
```

- アラートをイベント ストアに書き込みます。

```
ips-ssp(config-eve)# overrides produce-alert
ips-ssp(config-eve-ove)#
```

- 冗長なアラートをイベント ストアに書き込みます。

```
ips-ssp(config-eve)# overrides produce-verbose-alert
ips-ssp(config-eve-ove)#
```

- SNMP トラップを要求するイベントをイベント ストアに書き込みます。

```
ips-ssp(config-eve)# overrides request-snmp-trap
ips-ssp(config-eve-ove)#
```

ステップ 4　このオーバーライド アイテムのリスク レーティングを設定します。デフォルトのリスク レーティング範囲は 0 ～ 100 です。これを 85 ～ 100 などの異なる値に設定します。

```
ips-ssp(config-eve-ove)# risk-rating-range 85-100
```

ステップ 5　このオーバーライド アイテムの使用をイネーブルまたはディセーブルにします。デフォルトはイネーブルです。

```
ips-ssp(config-eve-ove)# override-item-status {enabled | disabled}
```

ステップ 6　設定を確認できます。

```
ips-ssp(config-eve-ove)# exit
ips-ssp(config-eve)# show settings
   action-to-add: deny-attacker-inline
   -----------------------------------------------
      override-item-status: Enabled default: Enabled
      risk-rating-range: 85-100 default: 0-100
   -----------------------------------------------
```

ステップ 7　イベント アクション オーバーライドのリスク レーティングを編集します。

```
ips-ssp(config-eve)# overrides deny-attacker-inline
ips-ssp(config-eve-ove)# risk-rating 95-100
```

ステップ 8　イベント アクション オーバーライドが編集されたことを確認します。

```
ips-ssp(config-eve-ove)# exit
ips-ssp(config-eve)# show settings
-----------------------------------------------
 overrides (min: 0, max: 14, current: 1)
 -----------------------------------------------

       override-item-status: Enabled <defaulted>
       risk-rating-range: 95-100 default: 0-100
    -----------------------------------------------
```

ステップ 9　イベント アクション オーバーライドを削除します。

```
ips-ssp(config-eve)# no overrides deny-attacker-inline
ips-ssp(config-eve-ove)#
```

ステップ 10　イベント アクション オーバーライドが削除されたことを確認します。

```
ips-ssp(config-eve-ove)# exit
ips-ssp(config-eve)# show settings
overrides (min: 0, max: 14, current: 1)
-----------------------------------------------
   action-to-add: deny-attacker-inline
   -----------------------------------------------
      override-item-status: Enabled <defaulted>
      risk-rating-range: 95 default: 0-100
   -----------------------------------------------
      override-item-status: Enabled <defaulted>
      risk-rating-range: 90-100 <defaulted>
   -----------------------------------------------
-----------------------------------------------
```

ステップ 11　イベント アクション ルール サブモードを終了します。

```
ips-ssp(config-eve)# exit
Apply Changes:?[yes]:
```

ステップ 12　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

すべてのイベント アクションについては、「イベント アクション」（P.8-4）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

ここでは、イベント アクション フィルタについて説明します。次のような構成になっています。

- 「イベント アクション フィルタについて」（P.8-20）
- 「イベント アクション フィルタの設定」（P.8-21）

イベント アクション フィルタについて

（注）　グローバル相関インスペクションとレピュテーション フィルタリング拒否機能では、IPv6 アドレスはサポートされません。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）　IPv6 トラフィックに対するレート制限およびブロッキングはサポートされていません。シグニチャにブロックまたはレート制限イベント アクションが設定されている場合、IPv6 トラフィックによってそのシグニチャがトリガーされると、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 フィルタは順序リストとして処理され、フィルタはリスト内で上下に移動できます。フィルタによって、センサーは、イベントに応答して特定のアクションを実行できます。すべてのアクションを実行したり、イベント全体を削除したりする必要はありません。フィルタは、イベントからアクションを削除することで機能します。1 つのイベントからすべてのアクションを削除するフィルタは、イベントを効率的に消費します。

注意　送信元 IP アドレスおよび宛先 IP アドレスに基づくイベント アクション フィルタは、正規のシグニチャとしてフィルタリングしないので、Sweep エンジンには機能しません。スイープ アラートで送信元 IP アドレスと宛先 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 IP アドレスおよび宛先 IP アドレス フィルタ パラメータを使用します。

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

イベント アクション フィルタの設定

（注）　グローバル相関インスペクションとレピュテーション フィルタリング拒否機能では、IPv6 アドレスはサポートされません。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）　IPv6 トラフィックに対するレート制限およびブロッキングはサポートされていません。シグニチャにブロックまたはレート制限イベント アクションが設定されている場合、IPv6 トラフィックによってそのシグニチャがトリガーされると、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。

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。フィルタに対するアドレスをグループ化するために定義したイベント アクション変数を使用できます。

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

サービス イベント アクション ルール サブモードで **filters {edit | insert | move] name1 [begin | end | inactive | before | after}** コマンドを使用して、イベント アクション フィルタを設定します。

オプション

次のオプションが適用されます。

- **actions-to-remove**：このフィルタ アイテムに対して削除するイベント アクションを指定します。
- **attacker-address-range**：このアイテムに対して IPv4 の攻撃者アドレスの範囲セット（たとえば、192.0.2.0-192.0.2.254,192.3.2.0-192.3.2.254）を指定します。

  （注）　範囲内の 2 番目の IP アドレスは、最初の IP アドレス以上である必要があります。攻撃者のアドレス範囲を指定しない場合は、すべての IPv4 の攻撃者アドレスに一致します。

- **attacker-port-range**：このアイテムに対する攻撃者のポートの範囲セット（たとえば、147-147,8000-10000）を指定します。
- **default**：値をシステムのデフォルト設定に戻します。
- **deny-attacker-percentage**：攻撃者拒否機能で拒否するパケットの割合を指定します。有効な範囲は 0 ～ 100 です。デフォルトは 100 です。
- **filter-item-status** {**enabled** | **disabled**}：このフィルタ アイテムの使用をイネーブルまたはディセーブルにします。
- **ipv6-attacker-address-range**：このアイテムに対する IPv6 の攻撃者アドレスの範囲セットを指定します（たとえば、<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）　範囲内の 2 番目の IPv6 アドレスは、最初の IPv6 アドレス以上である必要があります。IPv6 の攻撃者アドレス範囲を指定しない場合は、すべての IPv6 攻撃者アドレスに一致します。

- **ipv6-victim-address-range**：このアイテムに対する攻撃対象のアドレスの範囲セットを指定します（たとえば、<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）　範囲内の 2 番目の IPv6 アドレスは、最初の IPv6 アドレス以上である必要があります。IPv6 の攻撃対象アドレス範囲を指定しない場合は、すべての IPv6 の攻撃対象アドレスに一致します。

- **no**：エントリまたは選択の設定を削除します。
- **os-relevance**：このフィルタに対するイベント OS 関連性を指定します。
  - **relevant**：イベントはターゲット OS に関連します。
  - **not-relevant**：イベントはターゲット OS に関連しません。
  - **unknown**：イベントがターゲット OS に関連するかどうかわかりません。
- **risk-rating-range**：このフィルタ アイテムのリスク レーティング値の範囲を指定します。
- **signature-id-range**：このアイテムのシグニチャ ID の範囲セット（たとえば、1000-2000,3000-3000）を指定します。
- **stop-on-match {true | false}**：このフィルタ アイテムに一致した場合に、フィルタの評価を続行するか、停止します。
- **subsignature-id-range**：このアイテムのサブシグニチャ ID の範囲セット（たとえば、0-2,5-5）を指定します。
- **user-comment**：このフィルタ アイテムに関するコメントを追加できます。
- **victim-address-range**：このアイテムに対して攻撃対象のアドレスの範囲セット（たとえば、192.0.2.0-192.0.2.254,192.3.2.0-192.3.2.254）を指定します。

（注）　範囲内の 2 番目の IP アドレスは、最初の IP アドレス以上である必要があります。攻撃対象のアドレス範囲を指定しない場合は、すべての IPv4 の攻撃者アドレスに一致します。

- **victim-port-range**：このアイテムに対する攻撃対象のポートの範囲セット（たとえば、147-147,8000-10000）を指定します。

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　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　イベント アクション ルール サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service event-action-rules rules1
ips-ssp(config-eve)#
```

ステップ 3　フィルタ名を作成します。**name1**、**name2** などを使用して、イベント アクション フィルタの名前を指定します。**begin | end | inactive | before | after** キーワードを使用して、フィルタを挿入する場所を指定します。

```
ips-ssp(config-eve)# filters insert name1 begin
```

ステップ 4　このフィルタの値を指定します。デフォルトは 900 ～ 65535 です。

a. シグニチャ ID 範囲を指定します。

```
ips-ssp(config-eve-fil)# signature-id-range 1000-1005
```

b. サブシグニチャ ID 範囲を指定します。デフォルトは 0 ～ 255 です。

```
ips-ssp(config-eve-fil)# subsignature-id-range 1-5
```

c. IPv4 または IPv6 の攻撃者アドレス範囲を指定します。

```
ips-ssp(config-eve-fil)# attacker-address-range 192.0.2.3-192.0.2.26
ips-ssp(config-eve-fil)# ipv6-attacker-address-range
2001:0db8:3c4d:0015:0000:0000:abcd:ef12
```

d. IPv4 または IPv6 の攻撃対象アドレス範囲を指定します。

```
ips-ssp(config-eve-fil)# victim-address-range 192.56.10.1-192.56.10.255
ips-ssp(config-eve-fil)# ipv6-victim-address-range ::0-FFFF:FFFF:FFFF:FFFF:FFFF:
FFFF:FFFF:FFFF
```

e. 攻撃対象ポート範囲を指定します。デフォルトは 0 ～ 65535 です。

```
ips-ssp(config-eve-fil)# victim-port-range 0-434
```

f. OS 関連性を指定します。デフォルトは 0 ～ 100 です。

```
ips-ssp(config-eve-fil)# os-relevance relevant
```

g. リスク レーティング範囲を指定します。デフォルトは 0 ～ 100 です。

```
ips-ssp(config-eve-fil)# risk-rating-range 85-100
```

h. 削除するアクションを指定します。

```
ips-ssp(config-eve-fil)# actions-to-remove reset-tcp-connection
```

i. 拒否アクションをフィルタリングする場合は、必要な拒否アクションの割合を設定します。デフォルトは 100 です。

```
ips-ssp(config-eve-fil)# deny-attacker-percentage 90
```

j. フィルタのステータスをディセーブルまたはイネーブルのいずれかに指定します。デフォルトはイネーブルです。

```
ips-ssp(config-eve-fil)# filter-item-status {enabled | disabled}
```

k. 一致パラメータで停止を指定します。**true** を指定すると、このアイテムが一致する場合にセンサーがフィルタの処理を停止します。**false** を指定すると、このアイテムが一致する場合であってもセンサーはフィルタの処理を続行します。

```
ips-ssp(config-eve-fil)# stop-on-match {true | false}
```

l. このフィルタを説明するために使用するコメントを追加します。

```
ips-ssp(config-eve-fil)# user-comment NEW FILTER
```

ステップ 5　フィルタの設定を確認します。

```
ips-ssp(config-eve-fil)# show settings
NAME: name1
   ------------------------------------------------
      signature-id-range: 1000-10005 default: 900-65535
      subsignature-id-range: 1-5 default: 0-255
      attacker-address-range: 192.0.2.3-192.0.2.26 default: 0.0.0.0-255.255.255.255
      victim-address-range: 192.56.10.1-192.56.10.255 default: 0.0.0.0-255.255.255.255
           ipv6-attacker-address-range: 2001:0db8:3c4d:0015:0000:0000:abcd:ef12 defau
lt: ::0-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
      ipv6-victim-address-range: ::0-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF def
ault: ::0-FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
      attacker-port-range: 0-65535 <defaulted>
      victim-port-range: 1-343 default: 0-65535
      risk-rating-range: 85-100 default: 0-100
      actions-to-remove: reset-tcp-connection default:
      deny-attacker-percentage: 90 default: 100
      filter-item-status: Enabled default: Enabled
      stop-on-match: True default: False
      user-comment: NEW FILTER default:
      os-relevance: relevant default: relevant|not-relevant|unknown
   ------------------------------------------------
senor(config-eve-fil)#
```

ステップ 6　既存のフィルタを編集します。

```
ips-ssp(config-eve)# filters edit name1
```

ステップ 7　パラメータを編集します（ステップ 4a ～ 4l を参照）。

ステップ 8　フィルタ リストでフィルタを上下に移動します。

```
ips-ssp(config-eve-fil)# exit
ips-ssp(config-eve)# filters move name5 before name1
```

ステップ 9　フィルタが移動されたことを確認します。

```
ips-ssp(config-eve-fil)# exit
ips-ssp(config-eve)# show settings
   ------------------------------------------------
   filters (min: 0, max: 4096, current: 5 - 4 active, 1 inactive)
   ------------------------------------------------
   ACTIVE list-contents
   ------------------------------------------------
      NAME: name5
      ------------------------------------------------
         signature-id-range: 900-65535 <defaulted>
         subsignature-id-range: 0-255 <defaulted>
         attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted>
         victim-address-range: 0.0.0.0-255.255.255.255 <defaulted>
         attacker-port-range: 0-65535 <defaulted>
         victim-port-range: 0-65535 <defaulted>
         risk-rating-range: 0-100 <defaulted>
         actions-to-remove: <defaulted>
         filter-item-status: Enabled <defaulted>
         stop-on-match: False <defaulted>
         user-comment: <defaulted>
      ------------------------------------------------
      ------------------------------------------------
      NAME: name1
      ------------------------------------------------
         signature-id-range: 900-65535 <defaulted>
         subsignature-id-range: 0-255 <defaulted>
         attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted>
```

```
            victim-address-range: 0.0.0.0-255.255.255.255 <defaulted>
            attacker-port-range: 0-65535 <defaulted>
            victim-port-range: 0-65535 <defaulted>
            risk-rating-range: 0-100 <defaulted>
            actions-to-remove: <defaulted>
            filter-item-status: Enabled <defaulted>
            stop-on-match: False <defaulted>
            user-comment: <defaulted>
         -----------------------------------------------
         -----------------------------------------------
         NAME: name2
         -----------------------------------------------
            signature-id-range: 900-65535 <defaulted>
            subsignature-id-range: 0-255 <defaulted>
            attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted>
            victim-address-range: 0.0.0.0-255.255.255.255 <defaulted>
            attacker-port-range: 0-65535 <defaulted>
            victim-port-range: 0-65535 <defaulted>
            risk-rating-range: 0-100 <defaulted>
            actions-to-remove: <defaulted>
            filter-item-status: Enabled <defaulted>
            stop-on-match: False <defaulted>
            user-comment: <defaulted>
         -----------------------------------------------
         -----------------------------------------------
      ------------------------------------------------
      INACTIVE list-contents
      ------------------------------------------------
   ------------------------------------------------
   ips-ssp(config-eve)#
```

ステップ 10　フィルタを非アクティブ リストに移動します。

```
ips-ssp(config-eve)# filters move name1 inactive
```

ステップ 11　フィルタが非アクティブ リストに移動されたことを確認します。

```
ips-ssp(config-eve-fil)# exit
ips-ssp(config-eve)# show settings
   ------------------------------------------------
   INACTIVE list-contents
   ------------------------------------------------
      ------------------------------------------------
      NAME: name1
      ------------------------------------------------
         signature-id-range: 900-65535 <defaulted>
         subsignature-id-range: 0-255 <defaulted>
         attacker-address-range: 0.0.0.0-255.255.255.255 <defaulted>
         victim-address-range: 0.0.0.0-255.255.255.255 <defaulted>
         attacker-port-range: 0-65535 <defaulted>
         victim-port-range: 0-65535 <defaulted>
         risk-rating-range: 0-100 <defaulted>
         actions-to-remove: <defaulted>
         filter-item-status: Enabled <defaulted>
         stop-on-match: False <defaulted>
         user-comment: <defaulted>
      ------------------------------------------------
      ------------------------------------------------
ips-ssp(config-eve)#
```

ステップ 12　イベント アクション ルール サブモードを終了します。

```
ips-ssp(config-eve)# exit
Apply Changes:?[yes]:
```

ステップ 13　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

詳細情報

イベント アクション変数の設定手順については、「イベント アクション変数の追加、編集、および削除」（P.8-10）を参照してください。

OS ID の設定

ここでは、OS ID と、OS マップの設定方法について説明します。次のような構成になっています。

パッシブ OS フィンガープリントについて

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できます。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動している OS を特定します。
- ユーザ設定可能な OS ID：学習された OS マップよりも優先される OS ホスト マップを設定できます。
- 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。センサーは、CSA MC からインポートされたホストのポスチャ情報で報告された OS タイプを使用して、攻撃関連性レーティングを計算します。

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

1. 設定された OS マップ：入力する OS マップ。設定された OS マップは、イベント アクション ルール ポリシーに存在し、1 つまたは多くの仮想センサーに適用できます。

   （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。リストの最後のものは、一致したオペレーティング システムです。

2. インポートされた OS マップ：外部のデータ ソースからインポートされた OS マップ。インポートされた 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. 学習された OS マップ：SYN 制御ビットが設定された 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。学習された 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、設定された OS マップを調べます。ターゲット IP アドレスが、設定された OS マップにない場合、センサーはインポートされた OS マップを調べます。ターゲット IP アドレスが、インポートされた OS マップにない場合、センサーはインポートされた 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り、IPS には各シグニチャのデフォルトの脆弱な OS リストが含まれます。

パッシブ OS フィンガープリントの設定に関する留意事項

パッシブ OS フィンガープリントは機能するよう設定する必要はありません。IPS は、各シグニチャに対してデフォルトの脆弱な OS リストを提供し、パッシブ分析がデフォルトでイネーブルになります。

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。

- OS マップを定義：重要なシステムで稼動している OS の ID を定義するよう OS マップを設定することが推奨されます。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 マップを設定することが推奨されます。
- 攻撃関連性レーティングの計算を特定の IP アドレス範囲に制限：これにより、攻撃関連性レーティングの計算が、保護されたネットワークの IP アドレスに制限されます。
- OS マップをインポート：OS マップをインポートすると、パッシブ分析で取得された OS ID の学習レートと忠実度を向上させることができます。CSA MC などの外部の製品インターフェイスがある場合は、そのインターフェイスから OS ID をインポートできます。
- ターゲットの OS 関連性の値を使用してイベント アクション ルール フィルタを定義：これにより、OS 関連性だけに基づいてアラートをフィルタリングできるようになります。
- パッシブ分析をディセーブル化：センサーが新しい OS マップを学習しないようにします。
- シグニチャ脆弱 OS リストを編集：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。デフォルト値である 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。

設定された OS マップの追加、編集、削除、および移動

サービス イベント アクション ルール サブモードで **os-identifications** コマンドを使用して、学習された OS マッピングよりも優先される OS ホスト マッピングを設定します。設定された OS マップは、追加、編集、および削除できます。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。設定された OS マッピングでは、範囲を設定できます。したがって、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 8-1）。

表 8-1　設定された OS マッピングの例

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。

オプション

次のオプションが適用されます。

- **calc-arr-for-ip-range**：この範囲内の攻撃対象に対する攻撃関連性レーティングを計算します。この値は、<A.B.C.D>-<A.B.C.D>[,<A.B.C.D>-<A.B.C.D>]（たとえば、192.0.2.0-192.0.2.254,192.3.2.0-192.3.2.254）のようになります。

  （注） 範囲内の 2 番目の IP アドレスは、最初の IP アドレス以上である必要があります。

- **configured-os-map {edit | insert | move] name1[begin | end | inactive | before | after}**：管理者が定義した IP アドレスと OS ID のマッピングのコレクションを指定します（設定された OS マッピングは、インポートおよび学習された OS マッピングよりも優先されます）。
- **ip**：指定された OS を稼動している 1 つまたは複数のホスト IP アドレスを指定します。この値は、<A.B.C.D>-<A.B.C.D>[,<A.B.C.D>-<A.B.C.D>]（たとえば、192.0.2.0-192.0.2.254,192.3.2.0-192.3.2.254）のようになります。

  （注） 範囲内の 2 番目の IP アドレスは、最初の IP アドレス以上である必要があります。

- **os**：1 つまたは複数のホストが稼動している OS のタイプを指定します。
  - **general-os**：すべての OS タイプ
  - **ios**：各種 Cisco IOS
  - **mac-os**：OS X 以前の各種 Apple System OS
  - **netware**：Netware
  - **other**：その他すべての OS
  - **unix**：各種 UNIX

  - **aix**：各種 AIX
  - **bsd**：各種 BSD
  - **hp-ux**：各種 HP-UX
  - **irix**：各種 IRIX
  - **linux**：各種 Linux
  - **solaris**：各種 Solaris
  - **windows**：各種 Microsoft Windows
  - **windows-nt-2k-xp**：各種 NT、2000、および XP
  - **win-nt**：特定の種類の Windows NT
  - **unknown**：未知の OS
- **default**：値をシステムのデフォルト設定に戻します。
- **no**：エントリまたは選択の設定を削除します。
- **passive-traffic-analysis {enabled | disabled}**：パッシブ OS フィンガープリント分析をイネーブルまたはディセーブルにします。

OS マップの設定

OS マップを設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　イベント アクション ルール サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service event-action-rules rules1
ips-ssp(config-eve)#
```

ステップ 3　OS マップを作成します。**name1**、**name2** などを使用して、OS マップの名前を指定します。**begin | end | inactive | before | after** キーワードを使用して、フィルタを挿入する場所を指定します。

```
ips-ssp(config-eve)# os-identification
ips-ssp(config-eve-os)# configured-os-map insert name1 begin
ips-ssp(config-eve-os-con)#
```

ステップ 4　この OS マップの値を指定します。

a. ホスト IP アドレスを指定します。

```
ips-ssp(config-eve-os-con)# ip 192.0.2.0-192.0.2.255
```

b. ホスト OS タイプを指定します。

```
ips-ssp(config-eve-os-con)# os unix
```

注意　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。リストの最後のものは、一致したオペレーティング システムです。

ステップ 5　OS マップの設定を確認します。

```
ips-ssp(config-eve-os-con)# show settings
   NAME: name1
   -----------------------------------------------
      ip: 192.0.2.0-192.0.2.255 default:
      os: unix
   -----------------------------------------------
ips-ssp(config-eve-os-con)#
```

ステップ 6　IP アドレスに対して攻撃関連性レーティング範囲を指定します。

```
ips-ssp(config-eve-os-con)# exit
ips-ssp(config-eve-os)# calc-arr-for-ip-range 192.0.2.1-192.0.2.25
```

ステップ 7　パッシブ OS フィンガープリントをイネーブルにします。

```
ips-ssp(config-eve-os)# passive-traffic-analysis enabled
```

ステップ 8　既存の OS マップを編集します。

```
ips-ssp(config-eve-os)# configured-os-map edit name1
ips-ssp(config-eve-os-con)#
```

ステップ 9　パラメータを編集します（手順 4 ～ 7 を参照）。

ステップ 10　OS マップ リストで OS マップを上下に移動します。

```
ips-ssp(config-eve-os-con)# exit
ips-ssp(config-eve-os)# configured-os-map move name5 before name1
```

ステップ 11　OS マップが移動されたことを確認します。

```
ips-ssp(config-eve-os)# show settings
   os-identification
   -----------------------------------------------
      calc-arr-for-ip-range: 192.0.2.1-192.0.2.25 default: 0.0.0.0-255.255.255.255
      configured-os-map (ordered min: 0, max: 50, current: 2 - 2 active, 0 inactive)
      ---------------------------------------------
      ACTIVE list-contents
      ---------------------------------------------
         NAME: name2
         ---------------------------------------------
            ip: 192.0.2.33 default:
            os: aix
         ---------------------------------------------
         ---------------------------------------------
         NAME: name1
         ---------------------------------------------
            ip: 192.0.2.0-192.0.2.255 default:
            os: unix
         ---------------------------------------------
         ---------------------------------------------
      -----------------------------------------------
      passive-traffic-analysis: Enabled default: Enabled
   -----------------------------------------------
ips-ssp(config-eve-os)#
```

ステップ 12　OS マップを非アクティブ リストに移動します。

```
ips-ssp(config-eve-os)# configured-os-map move name1 inactive
```

ステップ 13　フィルタが非アクティブ リストに移動されたことを確認します。

```
ips-ssp(config-eve-os)# show settings
   os-identification
```

```
   ------------------------------------------------
      calc-arr-for-ip-range: 192.0.2.33 default: 0.0.0.0-255.255.255.255
      configured-os-map (ordered min: 0, max: 50, current: 2 - 1 active, 1 inactive)
      ------------------------------------------------
      ACTIVE list-contents
      ------------------------------------------------
         NAME: name2
         ------------------------------------------------
            ip: 192.0.2.33 default:
            os: aix
         ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
      INACTIVE list-contents
      ------------------------------------------------
         NAME: name1
         ------------------------------------------------
            ip: 192.0.2.0-192.0.2.255 default:
            os: unix
         ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
      passive-traffic-analysis: Enabled default: Enabled
--MORE--#
```

ステップ 14　OS マップを削除します。

```
ips-ssp(config-eve-os)# no configured-os-map name2
```

ステップ 15　OS マップが削除されたことを確認します。

```
ips-ssp(config-eve-os)# show settings
   os-identification
   ------------------------------------------------
      calc-arr-for-ip-range: 192.0.2.33 default: 0.0.0.0-255.255.255.255
      configured-os-map (ordered min: 0, max: 50, current: 1 - 0 active, 1 inactive)
      ------------------------------------------------
      INACTIVE list-contents
      ------------------------------------------------
         NAME: name1
         ------------------------------------------------
            ip: 192.0.2.0-192.0.2.255 default:
            os: unix
         ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
      passive-traffic-analysis: Enabled default: Enabled
   ------------------------------------------------
ips-ssp(config-eve-os)#
```

ステップ 16　イベント アクション ルール サブモードを終了します。

```
ips-ssp(config-eve-os)# exit
ips-ssp(config-eve)# exit
Apply Changes:?[yes]:
```

ステップ 17　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

OS ID の表示とクリア

EXEC モードで **show os-identification** [*virtual-sensor*] **learned** [*ip-address*] コマンドを使用して、パッシブ分析によりセンサーが学習した IP アドレスに関連する OS ID を表示します。

EXEC モードで **clear os-identification** [*virtual-sensor*] **learned** [*ip-address*] コマンドを使用して、パッシブ分析によりセンサーが学習した IP アドレスに関連する OS ID を削除します。

IP アドレスを指定する場合は、指定された IP アドレスの OS ID だけが表示またはクリアされます。仮想センサーを指定する場合は、指定されたセンサーの OS ID だけが表示またはクリアされます。仮想センサーなしで IP アドレスを指定する場合、IP アドレスはすべての仮想センサーで表示またはクリアされます。

オプション

次のオプションが適用されます。

- *virtual-sensor*：（任意）表示またはクリアする仮想センサーの学習されたアドレスを指定します。
- *ip-address*：（任意）問い合わせる、またはクリアする IP アドレスを指定します。センサーは、指定された IP アドレスにマッピングされた OS ID を表示または削除します。

OS ID の表示とクリア

OS ID を表示またはクリアするには、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 CLI にログインします。

（注）　ビューア権限を持つアカウントは OS ID を表示できます。

ステップ 2　特定の IP アドレスに関連する学習された OS ID を表示します。

```
ips-ssp# show os-identification learned 192.0.2.1
Virtual sensor vs0:
   10.1.1.12 windows
ips-ssp# show os-identification learned
Virtual sensor vs0:
   10.1.1.12 windows
Virtual sensor vs1:
   10.1.0.1   unix
   10.1.0.2   windows
   10.1.0.3   windows
ips-ssp#
```

ステップ 3　すべての仮想センサーで特定の IP アドレスに対する学習された OS ID をクリアします。

```
ips-ssp# clear os-identification learned 192.0.2.1
```

ステップ 4　OS ID がクリアされたことを確認します。

```
ips-ssp# show statistics os-identification
Statistics for Virtual sensor vs0
   OS Identification
      Configured
      Imported
      Learned
Statistics for Virtual sensor vs1
   OS Identification
      Configured
      Imported
      Learned
ips-ssp#
```

一般設定

ここでは、一般設定について説明します。次のような構成になっています。

イベント アクション サマライズについて

サマライズでは、複数のイベントを単一のアラートに単純に集約することによって、センサーから送信されるアラートの量が減少します。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変更できます。各シグニチャは、推奨される通常の動作を反映するデフォルト値で作成されます。ただし、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できます。

アラートを生成しないアクション（拒否、ブロック、TCP リセット）は、サマライズされていない各シグニチャ イベントに対する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、サマライズされたこれらのアラートで実行されません。代わりに、これらのアクションは、1 つのサマリー アラートに適用され、フィルタを通過します。

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

サマライズおよびイベント アクションは、メタ 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。これにより、センサーは一連のイベントで発生する疑わしいアクティビティを監視できます。

イベント アクション集約について

基本的な集約は 2 つの動作モードを提供します。単純モードでは、アラートが送信される前に一致する必要があるシグニチャのヒット数しきい値を設定します。高度なモードは、間隔によるカウントです。このモードでは、センサーは 1 秒間ごとのヒット数を追跡し、そのしきい値が満たされた場合のみアラートを送信します。この例では、ヒットはイベントを説明するために使用される用語であり、基本的にアラートですが、ヒット数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信されません。

次のサマライズ オプションから選択できます。

- fire-all：シグニチャがトリガーされるたびにアラートを起動します。サマライズにこのしきい値が設定された場合は、サマライズが行われるまで各実行に対してアラートが起動されます。サマライズが始まると、各アドレス セットに対してサマリー間隔ごとにアラートが 1 つだけ起動されます。他のアドレス セットのアラートは、すべて表示されるか、個別にサマライズされます。シグニチャに対してアラートが一定時間存在しないと、シグニチャはすべてのモードを起動します。
- summary：シグニチャが初めてトリガーされた場合にアラートを起動し、そのシグニチャの追加アラートがサマリー間隔の間サマライズされます。各アドレス セットに対して各サマリー間隔でアラートを 1 つだけ起動する必要があります。グローバル サマリーしきい値に到達した場合、シグニチャはグローバル サマライズ モードに切り替わります。
- global-summarization：各サマリー間隔に対してアラートを起動します。シグニチャは、グローバル サマライズに対して事前に設定できます。
- fire-once：各アドレス セットに対してアラートを起動します。このモードをグローバル サマライズ モードにアップグレードできます。

一般設定

一般的なイベント アクション ルール設定を行うには、サービス イベント アクション ルール サブモードで、次のコマンドを使用します。

- **global-block-timeout**：ホストまたは接続をブロックする時間（分単位）。有効な範囲は 0 ～ 10000000 です。デフォルトは 30 分です。
- **global-deny-timeout**：攻撃者インラインを拒否する時間（秒単位）。有効な範囲は 0 ～ 518400 です。デフォルトは 3600 です。
- **global-filters-status {enabled | disabled}**：フィルタの使用をイネーブルまたはディセーブルにします。デフォルトはイネーブルです。
- **global-metaevent-status {enabled | disabled}**：メタ イベント ジェネレータの使用をイネーブルまたはディセーブルにします。デフォルトはイネーブルです。
- **global-overrides-status {enabled | disabled}**：オーバーライドの使用をイネーブルまたはディセーブルにします。デフォルトはイネーブルです。
- **global-summarization-status {enabled | disabled}**：サマライザの使用をイネーブルまたはディセーブルにします。デフォルトはイネーブルです。
- **max-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。

イベント アクションの一般設定

イベント アクションの一般設定を行うには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　イベント アクション ルール サブモードを開始します。

```
ips-ssp# configure terminal
ips-ssp(config)# service event-action-rules rules0
```

ステップ 3　一般サブモードを開始します。

```
ips-ssp(config)# general
```

ステップ 4　メタ イベント ジェネレータをイネーブルまたはディセーブルにします。デフォルトはイネーブルです。

```
ips-ssp(config-eve-gen)# global-metaevent-status {enabled | disabled}
```

ステップ 5　サマライザを有効または無効にします。デフォルトはイネーブルです。

```
ips-ssp(config-eve-gen)# global-summarization-status {enabled | disabled}
```

ステップ 6　拒否攻撃者インライン イベント アクションを設定します。

a.　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。デフォルトは 1000 です。

```
ips-ssp(config-eve-gen)# max-denied-attackers 100
```

b.　システムで攻撃者を拒否する時間（秒単位）を設定します。デフォルトは 3600 秒です。

```
ips-ssp(config-eve-gen)# global-deny-timeout 1000
```

ステップ 7　ホストまたは接続をブロックする時間（分単位）を設定します。デフォルトは 30 分です。

```
ips-ssp(config-eve-gen)# global-block-timeout 20
```

ステップ 8　設定したオーバーライドをイネーブルまたはディセーブルにします。デフォルトはイネーブルです。

```
ips-ssp(config-eve-gen)# global-overrides-status {enabled | disabled}
```

ステップ 9　設定したフィルタをイネーブルまたはディセーブルにします。デフォルトはイネーブルです。

```
ips-ssp(config-eve-gen)# global-filters-status {enabled | disabled}
```

ステップ 10　一般サブモードの設定を確認します。

```
ips-ssp(config-eve-gen)# show settings
   general
   ------------------------------------------------
      global-overrides-status: Enabled default: Enabled
      global-filters-status: Enabled default: Enabled
      global-summarization-status: Enabled default: Enabled
      global-metaevent-status: Enabled default: Enabled
      global-deny-timeout: 1000 default: 3600
      global-block-timeout: 20 default: 30
      max-denied-attackers: 100 default: 10000
   ------------------------------------------------
ips-ssp(config-eve-gen)#
```

ステップ 11　イベント アクション ルール サブモードを終了します。

```
ips-ssp(config-eve-gen)# exit
ips-ssp(config-eve)# exit
Apply Changes:?[yes]:
```

ステップ 12　Enter を押して変更を適用するか、**no** を入力して変更を破棄します。

拒否攻撃者リストの設定

ここでは、拒否攻撃者リストと、リストを追加、クリア、およびモニタする方法について説明します。次のような構成になっています。

拒否攻撃者リストへの拒否攻撃者エントリの追加

deny attacker [**virtual-sensor** *name*] [**ip-address** *attacker-ip-address*] | **victim** *victim-ip-address* | **port** *port-number*] コマンドを使用して、拒否攻撃者リストに拒否攻撃者エントリを 1 つ追加します。リストから拒否攻撃者エントリを削除するには、このコマンドの **no** 形式を使用します。

オプション

次のオプションが適用されます。

- *name*：（任意）拒否攻撃者エントリを追加する仮想センサーの名前を指定します。
- *attacker-ip-address*：攻撃者の IP アドレスを指定します。
- *victim-ip-address*：（任意）攻撃対象の IP アドレスを指定します。
- *port-number*：（任意）攻撃対象のポート番号を指定します。有効な範囲は 0 ～ 65535 です。

拒否攻撃者リストへのエントリの追加

拒否攻撃者リストに拒否攻撃者エントリを追加するには、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 CLI にログインします。

ステップ 2　IP アドレスが 192.0.2.1 の拒否攻撃者エントリを追加します。

```
ips-ssp# deny attacker ip-address 192.0.2.1
Warning: Executing this command will add deny attacker address on all virtual sensors.
Continue? [yes]:
```

ステップ 3　**yes** を入力して、すべての仮想センサーに対してこの拒否攻撃者エントリを追加します。

ステップ 4　特定の仮想センサーに拒否攻撃者エントリを追加します。

```
ips-ssp# deny attacker virtual-sensor vs0 ip-address 192.0.2.1
```

ステップ 5　リストから拒否攻撃者エントリを削除します。

```
ips-ssp# no deny attacker ip-address 192.0.2.1
Warning: Executing this command will delete this address from the list of attackers being
denied by all virtual sensors.
Continue? [yes]:
```

ステップ 6　**yes** を入力して、リストから拒否攻撃者エントリを削除します。

（注）　攻撃者の拒否をすぐに止めるには、**clear denied-attackers** コマンドを使用して、拒否攻撃者リストをクリアする必要があります。

詳細情報

拒否攻撃者リストから拒否攻撃者を永久的に削除する手順については、「拒否攻撃者リストのモニタリングとクリア」（P.8-37）を参照してください。

拒否攻撃者リストのモニタリングとクリア

show statistics denied-attackers コマンドを使用して、拒否攻撃者リストを表示します。**clear denied-attackers** [*virtual_sensor*] [**ip-address** *ip_address*] コマンドを使用して、拒否攻撃者リストを削除し、仮想センサー統計情報をクリアします。

センサーがインライン モードで動作するよう設定されている場合、トラフィックはセンサーを通過します。インライン モードでは、パケット、接続、および攻撃者を拒否するようシグニチャを設定できます。この結果、センサーが単一のパケット、接続、および特定の攻撃者を検出した場合に、これらは拒否されます（つまり、送信されません）。

シグニチャが起動されると、攻撃者は拒否され、リストに追加されます。センサー管理の一部として、リストの削除、またはリスト内の統計情報のクリアが必要な場合があります。

オプション

次のオプションが適用されます。

- *virtual_sensor*：（任意）拒否攻撃者リストをクリアする必要がある仮想センサーを指定します。
- *ip_address*：（任意）クリアする IP アドレスを指定します。

拒否攻撃者の表示と削除

拒否攻撃者リストの表示、リストの削除、統計情報のクリアを行うには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　拒否された IP アドレスのリストを表示します。統計情報は、この時点で 2 つの IP アドレスが拒否されていることを示します。

```
ips-ssp# show statistics denied-attackers
Denied Attackers and hit count for each.
   10.20.4.2 = 9
   10.20.5.2 = 5
```

ステップ 3　拒否攻撃者リストを削除します。

```
ips-ssp# clear denied-attackers
Warning: Executing this command will delete all addresses from the list of attackers
currently being denied by the sensor.
Continue with clear? [yes]:
```

ステップ 4　**yes** を入力して、リストをクリアします。

ステップ 5　特定の仮想センサーの拒否攻撃者リストを削除します。

```
ips-ssp# clear denied-attackers vs0
Warning: Executing this command will delete all addresses from the list of attackers being
denied by virtual sensor vs0.
Continue with clear? [yes]:
```

ステップ 6　**yes** を入力して、リストをクリアします。

ステップ 7　特定の仮想センサーの拒否攻撃者リストから、特定の IP アドレスを削除します。

```
ips-ssp# clear denied-attackers vs0 ip-address 192.0.2.1
Warning: Executing this command will delete ip address 10.1.1.1 from the list of attackers
being denied by virtual sensor vs0.
Continue with clear? [yes]:
```

ステップ 8　**yes** を入力して、リストをクリアします。

ステップ 9　リストをクリアしたことを確認します。**show statistics denied-attackers** または **show statistics virtual-sensor** コマンドを使用できます。

```
ips-ssp# show statistics denied-attackers
Denied Attackers and hit count for each.
Denied Attackers and hit count for each.
Statistics for Virtual sensor vs0
   Denied Attackers with percent denied and hit count for each.


   Denied Attackers with percent denied and hit count for each.


Statistics for Virtual sensor vs1
   Denied Attackers with percent denied and hit count for each.


   Denied Attackers with percent denied and hit count for each.
ips-ssp#

ips-ssp# show statistics virtual-sensor
Virtual sensor Statistics
   Statistics for Virtual sensor vs0
      Name of current Signature-Definition instance = sig0
      Name of current Event-Action-Rules instance = rules0
      List of interfaces monitored by this virtual sensor = mypair
      Denied Address Information
         Number of Active Denied Attackers = 0
         Number of Denied Attackers Inserted = 2
         Number of Denied Attackers Total Hits = 287
         Number of times max-denied-attackers limited creation of new entry = 0
         Number of exec Clear commands during uptime = 1
      Denied Attackers and hit count for each.
```

ステップ 10　統計情報のみをクリアします。

```
ips-ssp# show statistics virtual-sensor clear
```

ステップ 11　統計情報をクリアしたことを確認します。`Number of Active Denied Attackers` および `Number of exec Clear commands during uptime` カテゴリ以外の統計情報がすべてクリアされました。リストがクリアされたかどうかを認識することが重要です。

```
ips-ssp# show statistics virtual-sensor
Virtual sensor Statistics
   Statistics for Virtual sensor vs0
      Name of current Signature-Definition instance = sig0
      Name of current Event-Action-Rules instance = rules0
      List of interfaces monitored by this virtual sensor = mypair
      Denied Address Information
         Number of Active Denied Attackers = 2
         Number of Denied Attackers Inserted = 0
         Number of Denied Attackers Total Hits = 0
         Number of times max-denied-attackers limited creation of new entry = 0
         Number of exec Clear commands during uptime = 1
      Denied Attackers and hit count for each.
         10.20.2.5 = 0
         10.20.5.2 = 0
```

イベントのモニタリング

ここでは、イベント ストアからイベントを表示したりクリアしたりする方法について説明します。次のような構成になっています。

イベントの表示

show events [{**alert** [informational] [low] [medium] [high] [**include-traits** ***traits***] [**exclude-traits** ***traits***] [**min-threat-rating** *min-rr*] [**max-threat-rating** *max-rr*] | **error** [warning] [error] [fatal] | **NAC** | **status**}] [*hh:mm:ss* [*month day* [*year*]] | **past** *hh:mm:ss*] コマンドを使用して、イベント ストアのイベントを表示します。

開始時刻に開始されているイベントが表示されます。開始時刻を指定しない場合、現時点で開始されているイベントが表示されます。イベント タイプを指定しないと、すべてのイベントが表示されます。

（注）　イベントは、ライブ フィードとして表示されます。要求をキャンセルするには、Ctrl キーを押した状態で C キーを押します。

オプション

次のオプションが適用されます。

- **alert**：アラートを表示します。攻撃が進行中であるか、試みられたことを示す可能性がある、ある種の疑わしいアクティビティを通知します。シグニチャがネットワーク アクティブによってトリガーされると常に、分析エンジンによってアラート イベントが生成されます。レベルが選択されていない場合（informational、low、medium、または high）、すべてのアラート イベントが表示されます。
- **include-traits**：指定された特徴を持つアラートを表示します。
- **exclude-traits**：指定された特徴を持つアラートを表示しません。
- **traits**：特徴ビット位置を 10 進数で指定します（0 ～ 15）。
- **min-threat-rating**：脅威レーティングがこの値以上であるイベントを表示します。デフォルトは 0 です。有効な範囲は 0 ～ 100 です。
- **max-threat-rating**：脅威レーティングがこの値以下であるイベントを表示します。デフォルトは 100 です。有効な範囲は 0 ～ 100 です。
- **error**：エラー イベントを表示します。エラーの条件が検出されると、サービスによってエラー イベントが生成されます。レベルが選択されていない場合（warning、error、または fatal）、すべてのエラー イベントが表示されます。
- **NAC**：ARC（ブロック）要求を表示します。

  （注）　ARC は、以前は NAC と呼ばれていました。この名前の変更は、Cisco IPS 7.1 の IDM、IME、および CLI に完全には実装されていません。

- **status**：ステータス イベントを表示します。
- **past**：指定した過去の時、分、および秒から開始されたイベントを表示します。
- *hh:mm:ss*：表示を開始する過去の時、分、秒。

（注） **show events** コマンドは、指定したイベントが使用可能になるまで、イベントを表示し続けます。終了するには、Ctrl キーを押した状態で C キーを押します。

イベントの表示

イベント ストアのイベントを表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　現在開始しているイベントをすべて表示します。Ctrl キーを押した状態で C キーを押すまで、フィードはすべてのイベントを表示し続けます。

```
ips-ssp# show events
evError: eventId=1041472274774840147 severity=warning vendor=Cisco
  originator:
    hostId: sensor
    appName: cidwebserver
    appInstanceId: 12075
  time: 2011/01/07 04:41:45 2011/01/07 04:41:45 UTC
  errorMessage: name=errWarning received fatal alert: certificate_unknown

evError: eventId=1041472274774840148 severity=error vendor=Cisco
  originator:
    hostId: sensor
    appName: cidwebserver
    appInstanceId: 351
  time: 2011/01/07 04:41:45 2011/01/07 04:41:45 UTC
  errorMessage: name=errTransport WebSession::sessionTask(6) TLS connection exce
ption: handshake incomplete.
```

ステップ 3　2011 年 2 月 9 日 10:00 a.m に開始されたブロック要求を表示します。

```
ips-ssp# show events NAC 10:00:00 Feb 9 2011
evShunRqst: eventId=1106837332219222281 vendor=Cisco
  originator:
    deviceName: sensor
    appName: NetworkAccessControllerApp
    appInstance: 654
  time: 2011/02/09 10:33:31 2011/08/09 13:13:31
  shunInfo:
    host: connectionShun=false
      srcAddr: 11.0.0.1
      destAddr:
      srcPort:
      destPort:
      protocol: numericType=0 other
    timeoutMinutes: 40
  evAlertRef: hostId=esendHost 123456789012345678
ips-ssp#
```

ステップ 4　2011 年 2 月 9 日 10:00 a.m. に開始された警告レベルのエラーを表示します。

```
ips-ssp# show events error warning 10:00:00 Feb 9 2011
evError: eventId=1041472274774840197 severity=warning vendor=Cisco
  originator:
    hostId: sensor
    appName: cidwebserver
    appInstanceId: 12160
  time: 2011/01/07 04:49:25 2011/01/07 04:49:25 UTC
  errorMessage: name=errWarning received fatal alert: certificate_unknown
```

ステップ 5　45 秒前からのアラートを表示します。

```
ips-ssp# show events alert past 00:00:45

evIdsAlert: eventId=1109695939102805307 severity=medium vendor=Cisco
  originator:
    hostId: sensor
    appName: sensorApp
    appInstanceId: 367
  time: 2011/03/02 14:15:59 2011/03/02 14:15:59 UTC
  signature: description=Nachi Worm ICMP Echo Request id=2156 version=S54
    subsigId: 0
    sigDetails: Nachi ICMP
  interfaceGroup:
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 10.89.228.202
    target:
      addr: locality=OUT 10.89.150.185
  riskRatingValue: 70
  interface: fe0_1
  protocol: icmp


evIdsAlert: eventId=1109695939102805308 severity=medium vendor=Cisco
  originator:
--MORE--
```

ステップ 6　30 秒前に開始されたイベントを表示します。

```
ips-ssp# show events past 00:00:30
evStatus: eventId=1041526834774829055 vendor=Cisco
  originator:
    hostId: sensor
    appName: mainApp
    appInstanceId: 2215
  time: 2011/01/08 02:41:00 2011/01/08 02:41:00 UTC
  controlTransaction: command=getVersion successful=true
    description: Control transaction response.
    requestor:
      user: cids
      application:
        hostId: 64.101.182.101
        appName: -cidcli
        appInstanceId: 2316


evStatus: eventId=1041526834774829056 vendor=Cisco
  originator:
    hostId: sensor
    appName: login(pam_unix)
    appInstanceId: 2315
  time: 2011/01/08 02:41:00 2011/01/08 02:41:00 UTC
  syslogMessage:
    description: session opened for user cisco by cisco(uid=0)
```

イベント ストアからのイベントのクリア

clear events コマンドを使用して、イベント ストアをクリアします。

イベント ストアのイベントをクリアするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　イベント ストアをクリアします。

```
ips-ssp# clear events
Warning: Executing this command will remove all events currently stored in the event
store.
Continue with clear? []:
```

ステップ 3　**yes** を入力して、イベントをクリアします。