CHAPTER 8

Signature Wizard の使用

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

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

この章では、Signature Wizard と、カスタム シグニチャの作成方法について説明します。次の事項について説明します。

Custom Signature Wizard について

（注） カスタム シグニチャを作成するには、管理者またはオペレータである必要があります。

Custom Signature Wizard は、カスタム シグニチャを作成するプロセスを順に示します。シグニチャ エンジンを使用してカスタム シグニチャを作成するか、シグニチャ エンジンを使用せずにカスタム シグニチャを作成するかの 2 つの手順が考えられます。

詳細情報

個々のシグニチャ エンジンの詳細については、付録 B「シグニチャ エンジンについて」を参照してください。

シグニチャ エンジンの使用

次の手順は、シグニチャ エンジンを使用してカスタム シグニチャを作成する場合に適用されます。

ステップ 1　シグニチャ エンジンを選択します。

- Atomic IP
- Atomic IP Advanced
- Service HTTP
- Service MSRPC
- Service RPC
- State（SMTP など）
- String ICMP
- String TCP
- String UDP
- Sweep

ステップ 2　シグニチャ ID パラメータを割り当てます。

- Signature ID
- Subsignature ID
- Signature Name
- Alert Notes（任意）
- User Comments（任意）

ステップ 3　エンジン固有のパラメータを割り当てます。各エンジンに適用されるマスター パラメータのグループが存在しますが、パラメータはシグニチャ エンジンごとに異なります。

ステップ 4　アラート応答を割り当てます。

- Signature Fidelity Rating
- Severity of the Alert

ステップ 5　アラート動作を割り当てます。デフォルトのアラート動作を受け入れることができます。変更するには、[Advanced] をクリックします。これによって、[Advanced Alert Behavior] ウィザードが開きます。このウィザードを使用して、このシグニチャのアラートの処理方法を設定できます。

ステップ 6　[Finish] をクリックします。

Signature Wizard でサポートされないシグニチャ エンジン

Cisco IPS の Custom Signature Wizard では、次のシグニチャ エンジンに基づいたカスタム シグニチャの作成はサポートされません。

- AIC FTP
- AIC HTTP
- Atomic ARP

- Atomic IP6
- Fixed ICMP
- Fixed TCP
- Fixed UDP
- Flood Host
- Flood Net
- Meta
- Multi String
- Normalizer
- Service DNS
- Service FTP
- Service Generic
- Service H225
- Service IDENT
- Service MSSQL
- Service NTP
- Service P2P
- Service SMB Advanced
- Service SNMP
- Service SSH
- Service TNS
- String XL ICMP
- String XL TCP
- String XL UDP
- Traffic ICMP
- Traffic Anomaly
- Trojan Bo2k
- Trojan Tfn2k
- Trojan UDP

これらの既存のシグニチャ エンジンに基づいてカスタム シグニチャを作成するには、必要なエンジンから既存のシグニチャを複製します。

詳細情報

- CLI を使用して、これらのシグニチャ エンジンによってカスタム シグニチャを作成する方法の詳細については、『*Configuring the Cisco Intrusion Prevention System Security Services Processor Using the Command Line Interface 7.1*』を参照してください。
- シグニチャの複製の詳細については、「シグニチャのクローニング」（P.7-15）を参照してください。

シグニチャ エンジンを使用しない

次の手順は、シグニチャ エンジンを使用せずにカスタム シグニチャを作成する場合に適用されます。

ステップ 1　使用するプロトコルを指定します。

- IP：ステップ 3 に進みます。
- ICMP：ステップ 2 に進みます。
- UDP：ステップ 2 に進みます。
- TCP：ステップ 2 に進みます。

ステップ 2　ICMP および UDP プロトコルでは、トラフィック タイプを選択して、データ タイプを検査します。TCP プロトコルでは、トラフィック タイプを選択します。

ステップ 3　シグニチャ ID パラメータを割り当てます。

- Signature ID
- Subsignature ID
- Signature Name
- Alert Notes（任意）
- User Comments（任意）

ステップ 4　エンジン固有のパラメータを割り当てます。

各エンジンに適用されるマスター パラメータのグループが存在しますが、パラメータはシグニチャ エンジンごとに異なります。

ステップ 5　アラート応答を割り当てます。

- Signature Fidelity Rating
- Severity of the Alert

ステップ 6　アラート動作を割り当てます。デフォルトのアラート動作を受け入れることができます。変更するには、[Advanced] をクリックします。これによって、[Advanced Alert Behavior] ウィザードが開きます。このウィザードを使用して、このシグニチャのアラートの処理方法を設定できます。

ステップ 7　[Finish] をクリックします。

カスタム シグニチャの作成

注意　カスタム シグニチャを追加すると、センサーのパフォーマンスが影響を受ける可能性があります。新規シグニチャがセンサーに与える影響をモニタするには、[Configuration] > [Interface Configuration] > [Traffic Flow Notifications] を選択して、[Missed Packet Threshold] および [Notification Interval] オプションを設定して、センサーによる新規シグニチャの処理方法を判断します。

ヒント　チェックボックスが空の場合、デフォルト値が使用されていることを示します。チェックボックスをオンにして、パラメータを設定します。値のフィールドをクリックして、パラメータを変更します。緑色のチェックは、ユーザが定義した値が使用されていることを示します。緑色のチェックをクリックして、値をデフォルトに戻します。

Custom Signature Wizard は、カスタム シグニチャを設定する手順を順に示します。

Custom Signature Wizard を使用してカスタム シグニチャを作成するには、次の手順を実行します。

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

ステップ 2　[Configuration] > [Policies] > [Signature Definitions] > [sig0] > [Signature Wizard] を選択します。

ステップ 3　新規シグニチャの作成に使用する特定のシグニチャ エンジンがわかっている場合は、[Yes] オプション ボタンをクリックして、[Select Engine] ドロップダウン リストからエンジンを選択して、[Next] をクリックします。ステップ 12 に 進みます。使用するエンジンがわからない場合は、[No] オプション ボタンをクリックして、[Next] をクリックします。

ステップ 4　このシグニチャで検査するトラフィックのタイプに最も適合するオプション ボタンをクリックして、[Next] をクリックします。

- [IP]（IP の場合は、ステップ 12 に進みます）。
- [ICMP]（ICMP の場合は、ステップ 5 に進みます）。
- [UDP]（UDP の場合は、ステップ 6 に進みます）。
- [TCP]（TCP の場合は、ステップ 8 に進みます）。

ステップ 5　[ICMP Traffic Type] ウィンドウで、次のいずれかのオプション ボタンをクリックして、[Next] をクリックします。

- [Single Packet] : Atomic IP エンジン（ヘッダー データの場合）または String ICMP エンジンのいずれかを使用して、単一のパケットで攻撃を検査するためのシグニチャを作成します。ステップ 11 に進みます。
- [Sweeps] : 新規シグニチャに Sweep エンジンを使用して、スイープ攻撃を検出するためのシグニチャを作成します。ステップ 12 に進みます。

ステップ 6　[UDP Traffic Type] ウィンドウで、次のいずれかのオプション ボタンをクリックして、[Next] をクリックします。

- [Single Packet] : Atomic IP エンジン（ヘッダー データの場合）または String UDP エンジンのいずれかを使用して、単一のパケットで攻撃を検査するためのシグニチャを作成します。ステップ 11 に進みます。
- [Sweeps] : シグニチャに Sweep エンジンを使用して、スイープ攻撃を検出するためのシグニチャを作成します。ステップ 7 に進みます。

ステップ 7　[UDP Sweep Type] ウィンドウで、次のいずれかのオプション ボタンをクリックして、[Next] をクリックします。

- [Host Sweep] : スイープを使用してホストで開いているポートを検索するためのシグニチャを作成します。新規シグニチャの作成に Sweep エンジンが使用され、ストレージ キーは [Axxx] に設定されます。ステップ 12 に進みます。
- [Port Sweep] : スイープを使用してネットワークでホストを検索するためのシグニチャを作成します。新規シグニチャの作成に Sweep エンジンが使用され、ストレージ キーは [AxBx] に設定されます。ステップ 12 に進みます。

ステップ 8　[TCP Traffic Type] ウィンドウで、次のいずれかのオプション ボタンをクリックして、[Next] をクリックします。

- [Single Packet]：単一のパケットで攻撃を検査するためのシグニチャを作成します。シグニチャの作成には Atomic IP エンジンが使用されます。ステップ 12 に進みます。
- [Single TCP Connection]：単一の TCP 接続で攻撃を検出するためのシグニチャを作成します。ステップ 9 に進みます。
- [Multiple Connections]：複数の接続で攻撃を検出するためのシグニチャを作成します。ステップ 10 に進みます。

ステップ 9　[Service Type] ウィンドウで、次のいずれかのオプション ボタンをクリックして、[Next] をクリックして、ステップ 12 に進みます。

- [HTTP]：HTTP サービスを使用する攻撃を検出するためのシグニチャを作成します。シグニチャの作成には Service HTTP エンジンが使用されます。
- [SMTP]：SMTP サービスを使用する攻撃を検出するためのシグニチャを作成します。シグニチャの作成には SMTP エンジンが使用されます。
- [RPC]：RPC サービスを使用する攻撃を検出するためのシグニチャを作成します。シグニチャの作成には Service RPC エンジンが使用されます。
- [MSRPC]：MSRPC サービスを使用する攻撃を検出するためのシグニチャを作成します。シグニチャの作成には Service MSRPC エンジンが使用されます。
- [Other]：HTTP、SMTP、または RPC 以外のサービスを使用する攻撃を検出するためのシグニチャを作成します。シグニチャの作成には String TCP エンジンが使用されます。

ステップ 10　[TCP Sweep Type] ウィンドウで、次のいずれかのオプション ボタンをクリックして、[Next] をクリックして、ステップ 12 に進みます。

- [Host Sweep]：スイープを使用してホストで開いているポートを検索するためのシグニチャを作成します。シグニチャの作成に Sweep エンジンが使用され、ストレージ キーは [Axxx] に設定されます。
- [Port Sweep]：スイープを使用してネットワークでホストを検索するためのシグニチャを作成します。新規シグニチャの作成に Sweep エンジンが使用され、ストレージ キーは [AxBx] に設定されます。

ステップ 11　[Inspect Data] ウィンドウで、単一のパケットの場合は次のいずれかのオプション ボタンをクリックして、[Next] をクリックして、ステップ 12 に進みます。

- [Header Data Only]：センサーで検査するパケットの部分としてヘッダーを指定します。
- [Payload Data Only]：センサーで検査するパケットの部分としてペイロードを指定します。

ステップ 12　[Signature Identification] ウィンドウで、このシグニチャを一意に識別する属性を指定して、[Next] をクリックします。

a. [Signature ID] フィールドに、このシグニチャの番号を入力します。カスタム シグニチャの範囲は 60000 ～ 65000 です。

b. [Subsignature ID] フィールドに、このシグニチャの番号を入力します。デフォルトは 0 です。似ているシグニチャをグループにまとめるには、サブシグニチャ ID を割り当てます。

c. [Signature Name] フィールドに、このシグニチャの名前を入力します。[Signature Name] フィールドにはデフォルトの名前が表示されます。それぞれのカスタム シグニチャに合せて、具体的な名前に変更します。

（注）　アラートが生成されると、シグニチャ名はシグニチャ ID およびサブシグニチャ ID とともに Event Viewer に報告されます。

d. （任意）[Alert Notes] フィールドに、アラートに追加するテキストを入力します。このシグニチャに関連付けられた、アラートに含めるテキストを追加できます。アラートが生成されると、このメモは Event Viewer に報告されます。

e. （任意）[User Comments] フィールドに、このシグニチャを説明するテキストを入力します。ここには、必要に応じてどのようなテキストを入力することもできます。このフィールドは、シグニチャやアラートには影響を与えません。

ステップ 13　エンジンに固有のパラメータに値を割り当てて、[Next] をクリックします。

ステップ 14　[Alert Response] ウィンドウで、次のアラート応答オプションを指定します。

a. [Signature Fidelity Rating] フィールドに値を入力します。シグニチャの忠実度レーティングの有効な値は、0 ～ 100 で、シグニチャに対する信頼度を示し、100 が最高の信頼度です。

b. [Severity of the Alert] ドロップダウン リストで、センサーがアラートを送信した際に Event Viewer によって報告される重大度を選択します。

- High
- Informational
- Low
- Medium

ステップ 15　デフォルトのアラート動作を受け入れるには、[Finish] をクリックして、ステップ 22 に進みます。デフォルトのアラート動作を変更するには、[Advanced] をクリックして、ステップ 16 に進みます。

（注）　シグニチャの反応頻度は制御できます。たとえば、センサーから送られるアラートの量を減らす場合があります。または、シグニチャの反応を 1 つのアラートにまとめたい場合があります。また、偽のトラフィックを送信して IPS に短時間で数千ものアラートを発生させることを目的とした「Stick」などの IPS 対抗ツールに対応させることもできます。

ステップ 16　イベント カウント、キー、および間隔を設定します。

a. [Event Count] フィールドにイベント カウントの値を入力します。これは、センサーでこのシグニチャのアラートを 1 つ送信するまでに受信する必要のある最小ヒット数です。

b. [Event Count Key] ドロップダウン リストで、イベント カウント キーとして使用する属性を選択します。たとえば、同じ攻撃者からのイベントかどうかに基づいて、センサーにイベントをカウントさせるには、イベント カウント キーとして攻撃者のアドレスを選択します。

c. レートに基づいてイベントをカウントする場合は、[Use Event Interval] チェックボックスをオンにして、[Event Interval (seconds)] フィールドに、間隔に使用する秒数を入力します。

d. [Next] をクリックして続行します。[Alert Summarization] ウィンドウが表示されます。

ステップ 17　アラートの量を制御して、センサーがアラートをサマライズする方法を設定するには、次のいずれかのオプション ボタンをクリックします。

- [Alert Every Time the Signature Fires] : シグニチャが悪意のあるトラフィックを検出するたびに、センサーにアラートを送信させることを指定します。さらに、センサーでアラートの量を動的に調整できる、追加のしきい値を指定できます。ステップ 18 に進みます。
- [Alert the First Time the Signature Fires] : シグニチャが初めて悪意のあるトラフィックを検出した際に、センサーにアラートを送信させることを指定します。さらに、センサーでアラートの量を動的に調整できる、追加のしきい値を指定できます。ステップ 19 に進みます。
- [Send Summary Alerts] : シグニチャが起動されるたびにアラートを送信するのではなく、このシグニチャのサマリー アラートだけをセンサーに送信させることを指定します。さらに、センサーでアラートの量を動的に調整できる、追加のしきい値を指定できます。ステップ 20 に進みます。

- [Send Global Summary Alerts]：シグニチャが初めてアドレス セットで起動された際に、センサーにアラートを送信させて、その後一定時間におけるすべてのアドレス セットのすべてのアラートのサマリーが含まれているグローバル サマリー アラートだけを送信させることを指定します。ステップ 21 に進みます。

（注）　適応型セキュリティ アプライアンスの複数のコンテキストが 1 つの仮想センサーに含まれている場合、サマリー アラートには、サマライズされた最後のコンテキストのコンテキスト名が含まれています。このため、このサマリーは、サマライズされるすべてのコンテキストのうち、このタイプのすべてのアラートの結果となります。

ステップ 18　[Alert Every Time the Signature Fires] オプションを設定します。

a. [Summary Key] ドロップダウン リストで、サマリー キーのタイプを選択します。サマリー キーは、イベントのカウントに使用する属性を識別します。たとえば、同じ攻撃者からのものかどうかに基づいてセンサーにイベントをカウントさせる場合は、サマリー キーとして攻撃者のアドレスを選択します。

b. ダイナミック サマライズを使用するには、[Use Dynamic Summarization] チェックボックスをオンにします。ダイナミック サマライズを使用すると、設定したサマリー パラメータに基づいて、センサーで送信するアラートの量を動的に調整できます。

c. [Summary Threshold] フィールドに、センサーでこのシグニチャのサマリー アラートを送信するまでに受信する必要のある最小ヒット数を入力します。

d. [Summary Interval (seconds)] フィールドに、時間間隔に使用する秒数を入力します。

e. センサーでグローバル サマライズ モードを開始するには、[Specify Global Summary Threshold] チェックボックスをオンにします。

f. [Global Summary Threshold] フィールドに、センサーでグローバル サマリー アラートを送信するまでに受信する必要のある最小ヒット数を入力します。

ステップ 19　[Alert the First Time the Signature Fires] オプションを設定します。

a. [Summary Key] ドロップダウン リストで、サマリー キーのタイプを選択します。サマリー キーは、イベントのカウントに使用する属性を識別します。たとえば、同じ攻撃者からのものかどうかに基づいてセンサーにイベントをカウントさせる場合は、サマリー キーとして攻撃者のアドレスを選択します。

b. センサーにダイナミック グローバル サマライズを使用させるには、[Use Dynamic Global Summarization] チェックボックスをオンにします。

c. [Global Summary Threshold] フィールドに、センサーでグローバル サマリー アラートを送信するまでに受信する必要のある最小ヒット数を入力します。

アラート レートが指定秒数内に指定された数のシグニチャを超えると、センサーの動作は、シグニチャが初めて起動されたときに 1 つのアラートを送信する動作から、1 つのグローバル サマリー アラートを送信する動作に変わります。指定間隔内にアラートの率がしきい値を下回ると、元のアラート動作に戻ります。

d. [Global Summary Interval (seconds)] フィールドに、センサーがサマライズのためのイベントをカウントする秒数を入力します。

ステップ 20　[Send Summary Alerts] オプションを設定します。

a. [Summary Interval (seconds)] フィールドに、センサーがサマライズのためのイベントをカウントする秒数を入力します。

b. [Summary Key] ドロップダウン リストで、サマリー キーのタイプを選択します。サマリー キーは、イベントのカウントに使用する属性を識別します。たとえば、同じ攻撃者からのものかどうかに基づいてセンサーにイベントをカウントさせる場合は、サマリー キーとして攻撃者のアドレスを選択します。

c. センサーにダイナミック グローバル サマライズを使用させるには、[Use Dynamic Global Summarization] チェックボックスをオンにします。

d. [Global Summary Threshold] フィールドに、センサーでグローバル サマリー アラートを送信するまでに受信する必要のある最小ヒット数を入力します。

アラート レートが指定秒数内に指定された数のシグニチャを超えると、センサーの動作は、シグニチャが初めて起動されたときに 1 つのアラートを送信する動作から、1 つのグローバル サマリー アラートを送信する動作に変わります。指定間隔内にアラートの率がしきい値を下回ると、元のアラート動作に戻ります。

ステップ 21　[Global Summary Interval (seconds)] フィールドに、センサーがサマライズのためのイベントをカウントする秒数を入力します。

ステップ 22　[Finish] をクリックして、アラートの動作の変更を保存します。

ステップ 23　[Finish] をクリックして、カスタム シグニチャを保存します。

ステップ 24　カスタム シグニチャを作成するには、[Yes] をクリックします。

ヒント　変更を破棄するには、[Cancel] をクリックします。

作成したシグニチャは、イネーブルになって、シグニチャのリストに追加されます。

Signature Wizard のフィールド定義

ここでは、Custom Signature Wizard ウィンドウについて説明し、Signature Wizard のフィールド定義を示します。次の事項について説明します。

[Welcome] ウィンドウ

Custom Signature Wizard の [Welcome] ウィンドウには、次のフィールドがあります。

- [Yes] : [Select Engine] フィールドをアクティブ化して、シグニチャ エンジンのリストから選択できるようにします。
- [Select Engine] : 使用可能なシグニチャ エンジンのリストを表示します。シグニチャを作成するために使用するシグニチャ エンジンがわかっている場合は、[Yes] をクリックして、ドロップダウン リストからエンジン タイプを選択します。
  - [Atomic IP] : Atomic IP シグニチャを作成できます。
  - [Service HTTP] : HTTP トラフィックのシグニチャを作成できます。
  - [Service MSRPC] : MSRPC トラフィックのシグニチャを作成できます。
  - [Service RPC] : RPC トラフィックのシグニチャを作成できます。
  - [State SMTP] : SMTP トラフィックのシグニチャを作成できます。
  - [String ICMP] : ICMP 文字列のシグニチャを作成できます。
  - [String TCP] : TCP 文字列のシグニチャを作成できます。
  - [String UDP] : UDP 文字列のシグニチャを作成できます。
  - [Sweep] : スイープのシグニチャを作成できます。
- [No] : Custom Signature Wizard の拡張エンジン選択画面に進みます。

[Protocol Type] ウィンドウ

特定のプロトコルで悪意のある動作を検索するシグニチャを定義できます。シグニチャによって、次のプロトコルをデコードして検査できます。

- IP
- ICMP
- UDP
- TCP

フィールド定義

Custom Signature Wizard の [Protocol Type] ウィンドウには、次のフィールドがあります。

- [IP] : IP トラフィックをデコードして検査するためのシグニチャを作成します。
- [ICMP] : ICMP トラフィックをデコードして検査するためのシグニチャを作成します。
- [UDP] : UDP トラフィックをデコードして検査するためのシグニチャを作成します。
- [TCP] : TCP トラフィックをデコードして検査するためのシグニチャを作成します。

[Signature Identification] ウィンドウ

シグニチャ ID パラメータはシグニチャを説明しますが、シグニチャの動作には影響を与えません。シグニチャ ID、サブシグニチャ ID、およびシグニチャ名が必要です。その他のフィールドは任意です。

フィールド定義

Custom Signature Wizard の [Signature Identification] ウィンドウには、次のフィールドがあります。

- [Signature ID] : このシグニチャに割り当てられた一意の数値を示します。シグニチャ ID によって、センサーは特定のシグニチャを識別できます。シグニチャ ID は、アラートの生成時に Event Viewer に報告されます。有効な範囲は、60000 ～ 65000 です。
- [SubSignature ID] : このサブシグニチャに割り当てられた一意の数値を示します。サブシグニチャ ID によって、広範なシグニチャのより詳細なバージョンが識別されます。有効な値は 0 ～ 255 です。サブシグニチャは、アラートの生成時に Event Viewer に報告されます。
- [Signature Name] : このシグニチャに割り当てられた名前を示します。アラートの生成時に、Event Viewer に報告されます。
- [Alert Notes] :（任意）このシグニチャが起動された場合にアラートに関連付けられたテキストを指定します。アラートの生成時に、Event Viewer に報告されます。
- [User Comments] :（任意）シグニチャ パラメータとともに保存する、このシグニチャに関するメモまたはその他のコメントを指定します。

[Service MSRPC Engine Parameters] ウィンドウ

Service MSRPC エンジンは、MSRPC パケットを処理します。MSRPC は、ネットワーク接続された環境で複数のコンピュータとそのアプリケーション ソフトウェア間で連携処理を可能にします。これは、トランザクションベースのプロトコルです。チャネルを設定し、処理要求と応答を渡す一連の通信があることを意味します。

MSRPC は ISO レイヤ 5 ～ 6 プロトコルであり、UDP、TCP、および SMB などの別のトランスポート プロトコルの最上層にあります。MSRPC エンジンには、MSRPC PDU のフラグメンテーションと再構成を可能にする機能が含まれています。

この通信チャネルは、最近の Windows NT、Windows 2000、および Window XP セキュリティ脆弱性の原因となっています。Service MSRPC エンジンは、最も一般的なトランザクション タイプの DCE および RPC プロトコルだけをデコードします。

フィールド定義

Custom Signature Wizard の [MSRPC Engine Parameters] ウィンドウには、次のフィールドがあります。これらのオプションでは、非常に一般的なタイプであるか、非常に固有のタイプのトラフィックを検出するためのシグニチャを作成できます。

- [Event Action]：このシグニチャの検出時にセンサーに実行させるアクションを指定します。デフォルトは、[Produce Alert] です。

ヒント 複数のアクションを選択するには、Ctrl キーを押しながら選択します。

- [Specify Regex String]：（任意）最小および最大一致オフセット、正規表現文字列、および最小一致長など、完全一致オフセットを指定できます。
- [Protocol]：プロトコルとして TCP または UDP を指定できます。
- [Specify Operation]：（任意）動作を指定できます。
- [Specify UUID]：（任意）UUID を指定できます。

詳細情報

- MSRPC エンジンの詳細については、「Service MSRPC エンジン」（P.B-50）を参照してください。
- シグニチャの正規表現構文がリストされた表については、「正規表現の構文」（P.B-10）を参照してください。

[ICMP Traffic Type] ウィンドウ

Custom Signature Wizard の [ICMP Traffic Type] ウィンドウには、次のフィールドがあります。

- [Packet]：単一のパケットで攻撃を検査するためのシグニチャを作成することを指定します。
- [Sweeps]：スイープ攻撃を検出するためのシグニチャを作成することを指定します。

[Inspect Data] ウィンドウ

Custom Signature Wizard の [Inspect Data] ウィンドウには、次のフィールドがあります。

- [Header Data Only]：センサーで検査するパケットの部分としてヘッダーを指定します。
- [Payload Data Only]：センサーで検査するパケットの部分としてペイロードを指定します。

[UDP Traffic Type] ウィンドウ

Custom Signature Wizard の [UDP Traffic Type] ウィンドウには、次のフィールドがあります。

- [Single Packet]：単一のパケットで攻撃を検査するためのシグニチャを作成することを指定します。
- [Sweeps]：スイープ攻撃を検出するためのシグニチャを作成することを指定します。

[UDP Sweep Type] ウィンドウ

Custom Signature Wizard の [UDP Sweep Type] ウィンドウには、次のフィールドがあります。

- [Host Sweep]：ネットワークでホストを検索するスイープを示します。
- [Port Sweep]：ホストで開いているポートを検索するスイープを示します。

[TCP Traffic Type] ウィンドウ

Custom Signature Wizard の [TCP Traffic Type] ウィンドウには、次のフィールドがあります。

- [Single Packet]：単一のパケットで攻撃を検査するためのシグニチャを作成することを指定します。
- [Single TCP Connection]：単一の TCP 接続で攻撃を検査するためのシグニチャを作成することを指定します。
- [Multiple Connections]：複数の接続で攻撃を検出するためのシグニチャを作成することを指定します。

[Service Type] ウィンドウ

Custom Signature Wizard の [Service Type] ウィンドウには、次のフィールドがあります。

- [HTTP]：HTTP サービスを使用する攻撃を説明するためのシグニチャを作成することを指定します。
- [SMTP]：SMTP サービスを使用する攻撃を説明するためのシグニチャを作成することを指定します。
- [RPC]：RPC サービスを使用する攻撃を説明するためのシグニチャを作成することを指定します。
- [MSRPC]：MSRPC サービスを使用する攻撃を説明するためのシグニチャを作成することを指定します。
- [Other]：HTTP、SMTP、RPC、または MSRPC 以外のサービスを使用する攻撃を説明するためのシグニチャを作成することを指定します。

[TCP Sweep Type] ウィンドウ

Custom Signature Wizard の [TCP Sweep Type] ウィンドウには、次のフィールドがあります。

- [Host Sweep]：ネットワークでホストを検索するスイープを示します。
- [Port Sweep]：ホストで開いているポートを検索するスイープを示します。

[Atomic IP Engine Parameters] ウィンドウ

Atomic IP エンジンは、IP プロトコル ヘッダーと関連するレイヤ 4 トランスポート プロトコル（TCP、UDP、および ICMP）およびペイロードを検査するシグニチャを定義します。Atomic エンジンでは、複数のパケットにまたがる固定データは保存されません。その代わりに、1 つのパケットの分析を基にしてアラートを起動できます。

フィールド定義

Custom Signature Wizard の [Atomic IP Engine Parameters] ウィンドウには、次のフィールドがあります。これらのオプションでは、非常に一般的なタイプであるか、非常に固有のタイプのトラフィックを検出するためのシグニチャを作成できます。

- [Event Action]：このシグニチャの検出時にセンサーに実行させるアクションを指定します。デフォルトは、[Produce Alert] です。

ヒント 複数のアクションを選択するには、Ctrl キーを押しながら選択します。

- [Fragment Status]：フラグメント化トラフィックまたは非フラグメント化トラフィックを検査するかどうかを示します。
- [Specify Layer 4 Protocol]：（任意）特定のプロトコルをこのシグニチャに適用するかどうかを選択できます。

  [Yes] を選択する場合、次のプロトコルから選択できます。

  - [ICMP Protocol]：ICMP シーケンス、タイプ、コード、ID、および合計長を指定できます。
  - [Other IP Protocols]：ID を指定できます。
  - [TCP Protocol]：送信元および宛先の TCP フラグ、ウィンドウ サイズ、マスク、ペイロード長、緊急ポインタ、ヘッダー長、予約済み属性、およびポート範囲を設定できます。
  - [UDP Protocol]：送信元および宛先の有効な UDP 長、長さの不一致、およびポート範囲を指定できます。
- [Specify Payload Inspection]：（任意）次のペイロード検査オプションを指定できます。
- [Specify IP Payload Length]：（任意）ペイロード長を指定できます。
- [Specify IP Header Length]：（任意）ヘッダー長を指定できます。
- [Specify IP Type of Service]：（任意）サービスのタイプを指定できます。
- [Specify IP Time-to-Live]：（任意）パケットの存続可能時間を指定できます。
- [Specify IP Version]：（任意）IP バージョンを指定できます。
- [Specify IP Identifier]：（任意）IP ID を指定できます。
- [Specify IP Total Length]：（任意）合計 IP 長を指定できます。
- [Specify IP Option Inspection]：（任意）次の IP 検査オプションを指定できます。
  - [IP Option]：照合する IP オプション コード。
  - [IP Option Abnormal Options]：オプションの不正なリスト。
- [Specify IP Addr Options]：（任意）次の IP アドレス オプションを指定できます。
  - [Address with Localhost]：送信元または宛先のいずれかとしてローカル ホスト アドレスが使用されるトラフィックを示します。
  - [IP Addresses]：送信元または宛先アドレスを指定できます。
  - [RFC 1918 Address]：アドレスのタイプに RFC 1918 を指定します。
  - [Src IP Equal Dst IP]：送信元アドレスと宛先アドレスが同じであるトラフィックを示します。

詳細情報

Atomic IP エンジンの詳細については、「Atomic IP エンジン」（P.B-26）を参照してください。

Atomic IP Advanced エンジン シグニチャの例

ヒント　チェックボックスが空の場合、デフォルト値が使用されていることを示します。チェックボックスをオンにして、パラメータを設定します。値のフィールドをクリックして、パラメータを変更します。緑色のチェックは、ユーザが定義した値が使用されていることを示します。緑色のチェックをクリックして、値をデフォルトに戻します。

次の例は、Atomic IP Advanced エンジンに基づくシグニチャを作成する方法を示します。たとえば、このカスタム シグニチャは、ヘッダーのタイプが 1 で長さが 8 の HOP オプション ヘッダーを持つ IPv6 のすべてのパケットと一致します。

Atomic IP Advanced エンジンに基づくシグニチャを作成するには、次の手順を実行します。

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

ステップ 2　[Configuration] > [Policies] > [Signature Definitions] > [sig0] > [Active Signatures] を選択し、[Add] をクリックします。

ステップ 3　[Signature ID] フィールドに、新しいシグニチャの一意のシグニチャ ID を入力します。カスタム シグニチャ ID は、60000 から始まります。

ステップ 4　[Subsignature] フィールドに、新しいシグニチャの一意のサブシグニチャ ID を入力します。

ステップ 5　[Alert Severity] ドロップダウン リストから、このシグニチャと関連付ける重大度を選択します。

ステップ 6　[Signature Fidelity Rating] フィールドにシグニチャの忠実度レーティングを表す値（1 ～ 100）を入力します。

ステップ 7　[Promiscuous Delta] フィールドはデフォルト値のままにします。

ステップ 8　シグニチャ説明のフィールドに、このシグニチャに関するコメントを入力します。

ステップ 9　[Engine] ドロップダウン リストから、[Atomic IP Advanced] を選択します。

ステップ 10　Atomic IP Advanced エンジン固有のパラメータを設定します。

a. [Event Action] ドロップダウン リストから、イベントに応答してセンサーが実行するアクションを選択します。

（注）　IPv6 では、イベント アクション Request Block Host、Request Block Connection、Request Rate Limit をサポートしていません。

ヒント　複数のアクションを選択するには、Ctrl キーを押しながら選択します。

b. [IP Version] ドロップダウン リストから [Yes] を選択して IP バージョンをイネーブルにし、さらに [IP Version] ドロップダウン リストから [IPv6] を選択して IPv6 をイネーブルにします。

c. [HOP Options Header] ドロップダウン リストから [Yes] を選択してホップバイホップ オプションをイネーブルにしてから [HOH Present] ドロップダウン リストから [Have HOH] を選択します。

d. [HOH Options] フィールドで [Yes] を選択し、[HOH Option Type] フィールドに **1** を入力します。

e. [HOH Option Length] ドロップダウン リストで [Yes] を選択してホップバイホップの長さをイネーブルにし、さらに [HOH Option Length] フィールドに **8** を入力します。

ステップ 11　イベント カウンタを設定します。

a. [Event Count] フィールドに、カウントするイベントの数（1 ～ 65535）を入力します。

b. [Event Count Key] ドロップダウン リストから使用するキーを選択します。

c. [Specify Alert Interface] ドロップダウン リストから、アラート間隔を指定するかどうか（[Yes] または [No]）を選択します。

d. [Yes] を選択した場合は、[Alert Interval] フィールドにアラート間隔（2 ～ 1000）を入力します。

ステップ 12　アラートの頻度を設定します。

ステップ 13　[Enabled] フィールドはデフォルト値（[Yes]）のままにします。

（注）　シグニチャで指定されている攻撃をセンサーでアクティブに検出するには、シグニチャをイネーブルにする必要があります。

ステップ 14　[Retired] フィールドはデフォルト値（[Yes]）のままにします。

これにより、シグニチャはエンジンに配置されます。

（注）　シグニチャで指定されている攻撃をセンサーでアクティブに検出するには、シグニチャが廃棄されていない必要があります。

ステップ 15　[Vulnerable OS List] ドロップダウン リストから、このシグニチャに対して脆弱なオペレーティング システムを選択します。

ヒント　複数のアクションを選択するには、Ctrl キーを押しながら選択します。

ステップ 16　[Mars Category] ドロップダウン リストから、このシグニチャを識別する MARS カテゴリを選択します。

ヒント　複数のアクションを選択するには、Ctrl キーを押しながら選択します。

ヒント　変更を破棄して [Add Signature] 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。[Type] に [Custom] が設定された、新しいシグニチャがリストに表示されます。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 18　[Apply] をクリックして、変更を適用し、改訂したコンフィギュレーションを保存します。

詳細情報

Atomic IP Advanced エンジンの詳細については、「Atomic IP Advanced エンジン」（P.B-16）を参照してください。

[Service HTTP Engine Parameters] ウィンドウ

Service HTTP エンジンは、サービス固有文字列ベースのパターン マッチング インスペクション エンジンです。HTTP プロトコルは、今日のネットワークで最も一般的に使用されるプロトコルの 1 つです。さらに、最も長い前処理時間が必要であり、システムの全体的なパフォーマンスにとって重要な検査を必要とするシグニチャの数が最も多くなります。

Service HTTP エンジンでは、複数のパターンを 1 つのパターン マッチング テーブルにまとめることでデータ内の検索を一度に実行できる正規表現ライブラリが使用されます。このエンジンは、Web サービスだけに送信されるトラフィックまたは HTTP 要求を検索します。このエンジンでは、リターン トラフィックを検査できません。このエンジンでは、シグニチャごとに対象となる別個の Web ポートを指定できます。

HTTP 解読とは、符号化された文字を ASCII 対応文字に正規化することによって、HTTP メッセージをデコードするプロセスです。このプロセスは、ASCII 正規化と呼ばれることもあります。

HTTP パケットを検査するには、あらかじめそのデータを、ターゲット システムでのデータ処理時に表示されるものと同じデータ表現として解読または正規化しておく必要があります。また、ホスト ターゲット タイプごとにカスタマイズされたデコード方式を用意することが推奨されます。そのためには、ターゲット上で動作しているオペレーティング システムおよび Web サーバのバージョンを確認する必要があります。Service HTTP エンジンには、Microsoft IIS Web サーバ用のデフォルトの解読動作があります。

フィールド定義

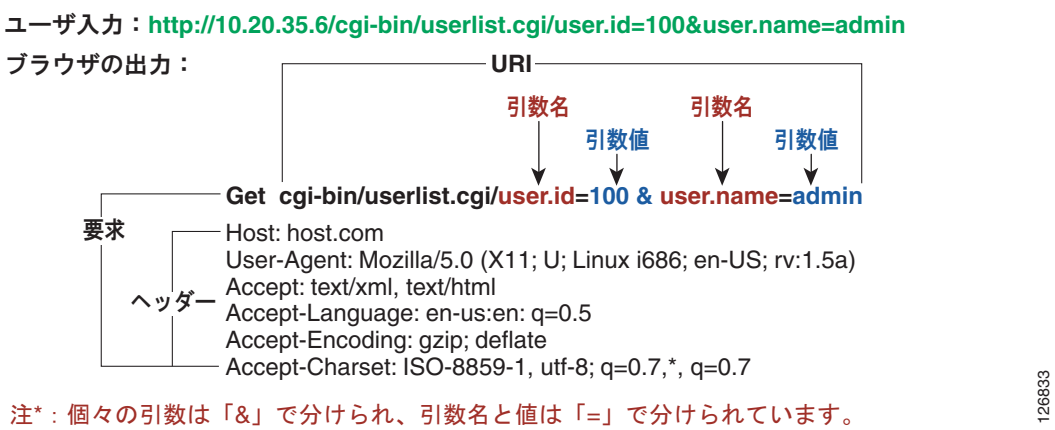
Custom Signature Wizard の [Service HTTP Engine Parameters] ウィンドウには、次のフィールドがあります。これらのオプションでは、非常に一般的なタイプであるか、非常に固有のタイプのトラフィックを検出するためのシグニチャを作成できます。

- [Event Action] : このシグニチャの検出時にセンサーに実行させるアクションを指定します。デフォルトは、[Produce Alert] です。

ヒント 複数のアクションを選択するには、Ctrl キーを押しながら選択します。

- [De Obfuscate] : 検索前に反回避 HTTP 解読を適用するかどうかを指定します。デフォルトは Yes です。
- [Max Field Sizes] :（任意）URI、属性、ヘッダー、および要求の最大フィールド長を指定できます。

  次の図は、最大フィールド サイズを示しています。



- [Regex]：URI、属性、ヘッダー、および要求正規表現の正規表現を指定できます。
- [Service Ports]：トラフィックによって使用される特定のサービス ポートを示します。値は、カンマ区切りのポートのリストです。
- [Swap Attacker Victim]：アラート メッセージおよび行うアクションで攻撃者と攻撃対象のアドレスおよびポート（送信元と宛先）をスワップします。デフォルトは [No] です。

詳細情報

- Service HTTP エンジンの詳細については、「Service HTTP エンジン」（P.B-47）を参照してください。
- シグニチャの正規表現構文がリストされた表については、「正規表現の構文」（P.B-10）を参照してください。

Service HTTP エンジン シグニチャの例

ヒント　チェックボックスが空の場合、デフォルト値が使用されていることを示します。チェックボックスをオンにして、パラメータを設定します。値のフィールドをクリックして、パラメータを変更します。緑色のチェックは、ユーザが定義した値が使用されていることを示します。緑色のチェックをクリックして、値をデフォルトに戻します。

注意　カスタム シグニチャは、センサーのパフォーマンスに影響することがあります。ネットワークのベースライン センサー パフォーマンスに対してカスタム シグニチャをテストすることにより、シグニチャの全体的な影響を判別します。

Custom Signature Wizard を使用して、カスタム Service HTTP シグニチャを作成します。

カスタム Service HTTP シグニチャを作成するには、次の手順を実行します。

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

ステップ 2　[Configuration] > [Policies] > [Signature Definitions] > [sig0] > [Signature Wizard] を選択します。

ステップ 3　[Yes] オプション ボタンをクリックして、[Select Engine] ドロップダウン リストから [Service HTTP] を選択して、[Next] をクリックします。

ステップ 4　このシグニチャを一意に識別する属性を指定するには、次の必要な値を入力して、[Next] をクリックします。

a. [Signature ID] フィールドに、シグニチャの番号を入力します。カスタム シグニチャの範囲は 60000 ～ 65000 です。

b. [Subsignature ID] フィールドに、シグニチャの番号を入力します。デフォルトは 0 です。似ているシグニチャをグループにまとめるには、サブシグニチャ ID を割り当てます。

c. [Signature Name] フィールドに、シグニチャの名前を入力します。[Signature Name] フィールドには、デフォルトの名前 My Sig が表示されています。それぞれのカスタム シグニチャに合せて、具体的な名前に変更します。

（注） アラートが生成されると、シグニチャ名はシグニチャ ID およびサブシグニチャ ID とともに Event Viewer に報告されます。

d. （任意）[Alert Notes] フィールドに、アラートに追加するテキストを入力します。このシグニチャに関連付けられた、アラートに含めるテキストを追加できます。アラートが生成されると、このメモは Event Viewer に報告されます。デフォルトは My Sig Info です。

e. （任意）[User Comments] フィールドに、このシグニチャを説明するテキストを入力して、[Next] をクリックします。ここには、必要に応じてどのようなテキストを入力することもできます。このフィールドは、シグニチャやアラートには影響を与えません。デフォルトは Sig Comment です。

ステップ 5　イベント アクションを割り当てます。

デフォルトは、[Produce Alert] です。セキュリティ ポリシーに基づいて、さらに拒否、ブロックなどのアクションを割り当てることができます。

ヒント 複数のアクションを選択するには、Ctrl キーを押しながら選択します。

ステップ 6　[De Obfuscate] フィールドで、ドロップダウン リストから [Yes] を選択して、検索前に反回避解読を適用するためのシグニチャを設定します。

ステップ 7　（任意）[Max Field Sizes] で、最大フィールド サイズに関する次のオプション パラメータを設定できます。

- [Specify Max URI Field Length]：最大 URI フィールド長をイネーブルにします。
- [Specify Max Arg Field Length]：最大引数フィールド長をイネーブルにします。
- [Specify Max Header Field Length]：最大ヘッダー フィールド長をイネーブルにします。
- [Specify Max Request Field Length]：最大要求フィールド長をイネーブルにします。

ステップ 8　[Regex] で、正規表現パラメータを設定します。

a. [Specify URI Regex] フィールドで、ドロップダウン リストから [Yes] を選択します。

b. [URI Regex] フィールドに、URI 正規表現（たとえば、[Mm][Yy][Ff][Oo][Oo]）を入力します。

c. 次のオプション パラメータの値を指定できます。

- [Specify Arg Name Regex]：特定の正規表現で [Arguments] フィールドの検索をイネーブルにします。
- [Specify Header Regex]：特定の正規表現で [Header] フィールドの検索をイネーブルにします。
- [Specify Request Regex]：特定の正規表現で [Request] フィールドの検索をイネーブルにします。

ステップ 9　[Service Ports] フィールドに、ポート番号を入力します。たとえば、Web ポート変数 $WEBPORTS を使用できます。値は、ターゲット サービスの常駐するポートのカンマ区切りリストまたはポート範囲です。

ステップ 10　（任意）[Swap Attacker Victim] フィールドで、[Yes] を選択して、アラート メッセージおよび行うアクションで攻撃者と攻撃対象のアドレスとポート（宛先および送信元）をスワップします。

ステップ 11　[Next] をクリックします。

ステップ 12　（任意）次のデフォルトのアラート応答オプションを変更できます。

a.　[Signature Fidelity Rating] フィールドに値を入力します。シグニチャの忠実度レーティングの有効な値は、0 ～ 100 で、シグニチャに対する信頼度を示し、100 が最高の信頼度です。デフォルトは 75 です。

b.　[Severity of the Alert] フィールドで、センサーがアラートを送信した際に Event Viewer によって報告される重大度を選択します。デフォルトでは [Medium] です。

ステップ 13　[Next] をクリックします。

ステップ 14　デフォルトのアラート動作を変更するには、[Advanced] をクリックします。それ以外の場合は、[Finish] をクリックすると、カスタム シグニチャが作成されます。[Create Custom Signature] ダイアログボックスが表示され、このカスタム シグニチャを作成してセンサーに適用するかどうか尋ねられます。

ステップ 15　カスタム シグニチャを作成するには、[Yes] をクリックします。

ヒント　変更を破棄するには、[Cancel] をクリックします。

作成したシグニチャは、イネーブルになって、シグニチャのリストに追加されます。

詳細情報

- Service HTTP エンジンの詳細については、「Service HTTP エンジン」（P.B-47）を参照してください。
- シグニチャの正規表現構文がリストされた表については、「正規表現の構文」（P.B-10）を参照してください。

[Service RPC Engine Parameters] ウィンドウ

Service RPC エンジンは、RPC プロトコルに対して使用し、反回避の方式として完全なデコードを行います。これにより、断片化メッセージ（複数パケット内の 1 つのメッセージ）およびバッチ メッセージ（1 つのパケット内の複数メッセージ）を処理できます。

RPC ポート マッパーは、ポート 111 上で動作します。通常の RPC メッセージは、550 より上位であれば任意のポートで送受信できます。RPC スイープは、TCP ポート スイープとほぼ同じものです。異なるのは、有効な RPC メッセージが送信された場合に一意のポートだけをカウントするという点です。RPC は UDP でも動作します。

フィールド定義

Custom Signature Wizard の [Service RPC Engine Parameters] ウィンドウには、次のフィールドがあります。これらのオプションでは、非常に一般的なタイプであるか、非常に固有のタイプのトラフィックを検出するためのシグニチャを作成できます。

- [Event Action]：このシグニチャの検出時にセンサーに実行させるアクションを指定します。デフォルトは、[Produce Alert] です。

ヒント 複数のアクションを選択するには、Ctrl キーを押しながら選択します。

- [Direction]：センサーによる監視対象が、サービス ポートを宛先とするトラフィックであるか、送信元とするトラフィックであるかを示します。デフォルトは [To Service] です。
- [Protocol]：プロトコルとして TCP または UDP を指定できます。
- [Service Ports]：ターゲット サービスがあるポートまたはポート範囲を示します。有効な値は、カンマ区切りのポートのリストまたはポート範囲です。
- [Specify Regex String]：検索する正規表現文字列を指定できます。
- [Specify Port Map Program]：このシグニチャの該当ポート マッパーに送信するプログラム番号を示します。有効な範囲は 0 ～ 999999999 です。
- [Specify RPC Program]：このシグニチャの該当 RPC プログラム番号を示します。有効な範囲は 0 ～ 1000000 です。
- [Specify Spoof Src]：送信元アドレスが 127.0.0.1 に設定されている場合に、アラームを起動します。
- [Specify RPC Max Length]：RPC メッセージ全体の許可される最大長を示します。長さがこの値を超えるとアラートが生成されます。有効な範囲は 0 ～ 65535 です。
- [Specify RPC Procedure]：このシグニチャの該当 RPC プロシージャ番号を示します。有効な範囲は 0 ～ 1000000 です。

詳細情報

- Service RPC エンジンの詳細については、「Service RPC エンジン」（P.B-53）を参照してください。
- シグニチャの正規表現構文がリストされた表については、「正規表現の構文」（P.B-10）を参照してください。

[State Engine Parameters] ウィンドウ

State エンジンは、TCP ストリームのステートベースの正規表現ベースのパターン検査を提供します。State エンジンとは何かの状態を保存するデバイスで、入力があるたびに、その内容に基づいてある状態から別の状態に移行したり、処理や出力を行ったりできます。ステート マシンは、出力やアラームを発生させる特定のイベントを記述するために使用します。State エンジンには、SMTP、Cisco Login、および LPR Format String の 3 つのステート マシンがあります。

フィールド定義

Custom Signature Wizard の [State Engine Parameters] ウィンドウには、次のフィールドがあります。これらのオプションでは、非常に一般的なタイプであるか、非常に固有のタイプのトラフィックを検出するためのシグニチャを作成できます。

- [Event Action]：このシグニチャの検出時にセンサーに実行させるアクションを指定します。デフォルトは、[Produce Alert] です。

ヒント 複数のアクションを選択するには、Ctrl キーを押しながら選択します。

- [State Machine]：正規表現文字列の一致を制限する状態の名前を示します。オプションは、[Cisco Login]、[LPR Format String]、および [SMTP] です。
- [State Name]：状態の名前を示します。オプションは、[Abort]、[Mail Body]、[Mail Header]、[SMTP Commands]、および [Start] です。
- [Specify Min Match Length]：正規表現文字列が一致する必要がある、一致の開始から一致の終わりまでの最小バイト数を示します。有効な範囲は 0 ～ 65535 です。
- [Regex String]：状態遷移をトリガーする正規表現文字列を示します。
- [Direction]：遷移のために検査するデータ ストリームの方向を示します。デフォルトは [To Service] です。
- [Service Ports]：ターゲット サービスがあるポートまたはポート範囲を示します。有効な値は、カンマ区切りのポートのリストまたはポート範囲です。
- [Swap Attacker Victim]：アラート メッセージおよび行うアクションで攻撃者と攻撃対象のアドレスおよびポート（送信元と宛先）をスワップします。デフォルトは [No] です。
- [Specify Exact Match Offset]：正規表現文字列が一致を報告する完全一致オフセット（バイト）を示します。[Yes] を選択する場合は、完全一致オフセットを設定できます。有効な範囲は 0 ～ 65535 です。[No] を選択する場合は、最小および最大一致オフセットを設定できます。

詳細情報

- State エンジンの詳細については、「State エンジン」（P.B-60）を参照してください。
- シグニチャの正規表現構文がリストされた表については、「正規表現の構文」（P.B-10）を参照してください。

[String ICMP Engine Parameters] ウィンドウ

String エンジンは、ICMP、TCP、および UDP プロトコルを対象とした、汎用パターン マッチング インスペクション エンジンです。String エンジンでは、複数のパターンを 1 つのパターン マッチング テーブルにまとめることでデータ内の検索を一度に実行できる正規表現エンジンが使用されます。String エンジンには、String ICMP、String TCP、および String UDP の 3 つがあります。

フィールド定義

Custom Signature Wizard の [String ICMP Engine Parameters] ウィンドウには、次のフィールドがあります。これらのオプションでは、非常に一般的なタイプであるか、非常に固有のタイプのトラフィックを検出するためのシグニチャを作成できます。

- [Event Action]：このシグニチャの検出時にセンサーに実行させるアクションを指定します。デフォルトは、[Produce Alert] です。

ヒント 複数のアクションを選択するには、Ctrl キーを押しながら選択します。

- [Specify Min Match Length]：正規表現文字列が一致する必要がある、一致の開始から一致の終わりまでの最小バイト数を示します。有効な範囲は 0 ～ 65535 です。
- [Regex String]：単一のパケットで検索する正規表現文字列を示します。

- [Direction]：遷移のために検査するデータ ストリームの方向を示します。デフォルトは [To Service] です。
- [ICMP Type]：ICMP ヘッダー TYPE 値。有効な範囲は 0 ～ 18 です。デフォルトは 0 ～ 18 です。
- [Swap Attacker Victim]：アラート メッセージおよび行うアクションで攻撃者と攻撃対象のアドレスおよびポート（送信元と宛先）をスワップします。デフォルトは [No] です。
- [Specify Exact Match Offset]：正規表現文字列が一致を報告する完全一致オフセット（バイト）を示します。[Yes] を選択する場合は、完全一致オフセットを設定できます。有効な範囲は 0 ～ 65535 です。[No] を選択する場合は、最小および最大一致オフセットを設定できます。

詳細情報

- String ICMP エンジンの詳細については、「String エンジン」（P.B-62）を参照してください。
- シグニチャの正規表現構文がリストされた表については、「正規表現の構文」（P.B-10）を参照してください。

[String TCP Engine Parameters] ウィンドウ

String エンジンは、ICMP、TCP、および UDP プロトコルを対象とした、汎用パターン マッチング インスペクション エンジンです。String エンジンでは、複数のパターンを 1 つのパターン マッチング テーブルにまとめることでデータ内の検索を一度に実行できる正規表現エンジンが使用されます。String エンジンには、String ICMP、String TCP、および String UDP の 3 つがあります。

フィールド定義

Custom Signature Wizard の [String TCP Engine Parameters] ウィンドウには、次のフィールドがあります。これらのオプションでは、非常に一般的なタイプであるか、非常に固有のタイプのトラフィックを検出するためのシグニチャを作成できます。

- [Event Action]：このシグニチャの検出時にセンサーに実行させるアクションを指定します。デフォルトは、[Produce Alert] です。

ヒント 複数のアクションを選択するには、Ctrl キーを押しながら選択します。

- [Strip Telnet Options]：パターンを検索する前に、データ ストリームから Telnet オプション制御文字を削除します。これは、主に反回避ツールとして使用します。デフォルトは [No] です。
- [Specify Min Match Length]：正規表現文字列が一致する必要がある、一致の開始から一致の終わりまでの最小バイト数を示します。有効な範囲は 0 ～ 65535 です。
- [Regex String]：単一のパケットで検索する正規表現文字列を示します。
- [Service Ports]：ターゲット サービスがあるポートまたはポート範囲を示します。有効な値は、カンマ区切りのポートのリストまたはポート範囲です。
- [Direction]：遷移のために検査するデータ ストリームの方向を示します。デフォルトは [To Service] です。
- [Specify Exact Match Offset]：正規表現文字列が一致を報告する完全一致オフセット（バイト）を示します。[Yes] を選択する場合は、完全一致オフセットを設定できます。有効な範囲は 0 ～ 65535 です。[No] を選択する場合は、最小および最大一致オフセットを設定できます。
- [Swap Attacker Victim]：アラート メッセージおよび行うアクションで攻撃者と攻撃対象のアドレスおよびポート（送信元と宛先）をスワップします。デフォルトは [No] です。

詳細情報

- String ICMP エンジンの詳細については、「String エンジン」（P.B-62）を参照してください。
- シグニチャの正規表現構文がリストされた表については、「正規表現の構文」（P.B-10）を参照してください。

String TCP エンジン シグニチャの例

ヒント　チェックボックスが空の場合、デフォルト値が使用されていることを示します。チェックボックスをオンにして、パラメータを設定します。値のフィールドをクリックして、パラメータを変更します。緑色のチェックは、ユーザが定義した値が使用されていることを示します。緑色のチェックをクリックして、値をデフォルトに戻します。

注意　カスタム シグニチャは、センサーのパフォーマンスに影響することがあります。ネットワークのベースライン センサー パフォーマンスに対してカスタム シグニチャをテストすることにより、シグニチャの全体的な影響を判別します。

Custom Signature Wizard を使用して、カスタム String TCP シグニチャを作成します。次の手順は、カスタム String ICMP および UDP シグニチャの作成にも適用されます。

カスタム String TCP シグニチャを作成するには、次の手順を実行します。

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

ステップ 2　[Configuration] > [Policies] > [Signature Definitions] > [sig0] > [Signature Wizard] を選択します。

ステップ 3　[Yes] オプション ボタンをクリックして、[Select Engine] ドロップダウン リストから [String TCP] を選択して、[Next] をクリックします。[Signature Identification] ウィンドウが表示されます。

ステップ 4　このシグニチャを一意に識別する属性を指定するには、次の必要な値を入力して、[Next] をクリックします。

a. [Signature ID] フィールドに、シグニチャの番号を入力します。カスタム シグニチャの範囲は 60000 ～ 65000 です。

b. [Subsignature ID] フィールドに、シグニチャの番号を入力します。デフォルトは 0 です。似ているシグニチャをグループにまとめるには、サブシグニチャ ID を割り当てます。

c. [Signature Name] フィールドに、シグニチャの名前を入力します。[Signature Name] フィールドには、デフォルトの名前 My Sig が表示されています。それぞれのカスタム シグニチャに合せて、具体的な名前に変更します。

（注）　アラートが生成されると、シグニチャ名はシグニチャ ID およびサブシグニチャ ID とともに Event Viewer に報告されます。

d. （任意）[Alert Notes] フィールドに、アラートに追加するテキストを入力します。このシグニチャに関連付けられた、アラートに含めるテキストを追加できます。アラートが生成されると、このメモは Event Viewer に報告されます。デフォルトは My Sig Info です。

e. （任意）[User Comments] フィールドに、このシグニチャを説明するテキストを入力します。ここには、必要に応じてどのようなテキストを入力することもできます。このフィールドは、シグニチャやアラートには影響を与えません。デフォルトは Sig Comment です。[Next] をクリックします。[Engine Specific Parameters] ウィンドウが表示されます。

ステップ 5　イベント アクションを割り当てます。デフォルトは、[Produce Alert] です。セキュリティ ポリシーに基づいて、さらに拒否、ブロックなどのアクションを割り当てることができます。

ヒント　複数のアクションを選択するには、Ctrl キーを押しながら選択します。

ステップ 6　（任意）パターンを検索する前にデータから Telnet オプション文字を削除するには、[Strip Telnet Options] フィールドでドロップダウン リストから [Yes] を選択します。

ステップ 7　（任意）[Specify Min Match Length] フィールドで、ドロップダウン リストから [Yes] を選択して、最小一致長をイネーブルにし、[Min Match Length] フィールドに、正規表現文字列が一致する必要がある最小バイト数（0 ～ 65535）を入力します。

ステップ 8　[Regex String] フィールドに、このシグニチャが TCP パケットで検索する文字列を入力します。

ステップ 9　[Service Ports] フィールドに、ポート番号（23 など）を入力します。値は、ターゲット サービスの常駐するポートのカンマ区切りリストまたはポート範囲です。

ステップ 10　[Direction] ドロップダウン リストで、トラフィックの方向を選択します。

- [From Service] : サービス ポートからクライアント ポート宛のトラフィック。
- [To Service] : クライアント ポートからサービス ポート宛のトラフィック。

ステップ 11　（任意）[Specify Exact Match Offset] フィールドで、ドロップダウン リストから [Yes] を選択して、完全一致オフセットをイネーブルにします。完全一致オフセットは、一致を有効にするために正規表現文字列がレポートする必要がある正確なストリーム オフセット（0 ～ 65535）です。

a. [Specify Max Match Offset] フィールドに、最大値を入力します。

b. [Specify Min Match Offset] フィールドに、最小値を入力します。

ステップ 12　[Swap Attacker Victim] フィールドで、[Yes] を選択して、アラート メッセージおよび行うアクションで攻撃者と攻撃対象のアドレスとポート（宛先および送信元）をスワップして、[Next] をクリックします。

ステップ 13　（任意）次のデフォルトのアラート応答オプションを変更できます。

a. [Signature Fidelity Rating] フィールドに値を入力します。シグニチャの忠実度レーティングの有効な値は、0 ～ 100 で、シグニチャに対する信頼度を示し、100 が最高の信頼度です。デフォルトは 75 です。

b. [Severity of the Alert] フィールドで、センサーがアラートを送信した際に Event Viewer によって報告される重大度を選択します。デフォルトでは [Medium] です。

ステップ 14　[Next] をクリックします。

ステップ 15　デフォルトのアラート動作を変更するには、[Advanced] をクリックします。それ以外の場合は、[Finish] をクリックすると、カスタム シグニチャが作成されます。[Create Custom Signature] ダイアログボックスが表示され、このカスタム シグニチャを作成してセンサーに適用するかどうか尋ねられます。

ステップ 16　カスタム シグニチャを作成するには、[Yes] をクリックします。

ヒント　変更を破棄するには、[Cancel] をクリックします。

作成したシグニチャは、イネーブルになって、シグニチャのリストに追加されます。

詳細情報

- String ICMP エンジンの詳細については、「String エンジン」（P.B-62）を参照してください。
- シグニチャの正規表現構文がリストされた表については、「正規表現の構文」（P.B-10）を参照してください。

[String UDP Engine Parameters] ウィンドウ

String エンジンは、ICMP、TCP、および UDP プロトコルを対象とした、汎用パターン マッチング インスペクション エンジンです。String エンジンでは、複数のパターンを 1 つのパターン マッチング テーブルにまとめることでデータ内の検索を一度に実行できる正規表現エンジンが使用されます。String エンジンには、String ICMP、String TCP、および String UDP の 3 つがあります。

フィールド定義

Custom Signature Wizard の [String UDP Engine Parameters] ウィンドウには、次のフィールドがあります。これらのオプションでは、非常に一般的なタイプであるか、非常に固有のタイプのトラフィックを検出するためのシグニチャを作成できます。

- [Event Action]：このシグニチャの検出時にセンサーに実行させるアクションを指定します。デフォルトは、[Produce Alert] です。

ヒント 複数のアクションを選択するには、Ctrl キーを押しながら選択します。

- [Specify Min Match Length]：正規表現文字列が一致する必要がある、一致の開始から一致の終わりまでの最小バイト数を示します。有効な範囲は 0 ～ 65535 です。
- [Regex String]：単一のパケットで検索する正規表現文字列を示します。
- [Service Ports]：ターゲット サービスがあるポートまたはポート範囲を示します。有効な値は、カンマ区切りのポートのリストまたはポート範囲です。
- [Direction]：遷移のために検査するデータ ストリームの方向を示します。
- [Swap Attacker Victim]：アラート メッセージおよび行うアクションで攻撃者と攻撃対象のアドレスおよびポート（送信元と宛先）をスワップします。デフォルトは [No] です。
- [Specify Exact Match Offset]：正規表現文字列が一致を報告する完全一致オフセット（バイト）を示します。[Yes] を選択する場合は、完全一致オフセットを設定できます。有効な範囲は 0 ～ 65535 です。[No] を選択する場合は、最小および最大一致オフセットを設定できます。

詳細情報

- String ICMP エンジンの詳細については、「String エンジン」（P.B-62）を参照してください。
- シグニチャの正規表現構文がリストされた表については、「正規表現の構文」（P.B-10）を参照してください。

[Sweep Engine Parameters] ウィンドウ

Sweep エンジンは、2 つのホスト間、または 1 つのホストから多数のホストへのトラフィックを分析します。既存のシグニチャを調整するか、カスタム シグニチャを作成できます。Sweep エンジンには、ICMP、UDP、および TCP を対象とした、プロトコル固有のパラメータがあります。

Sweep エンジンのアラート条件は、最終的に、一意のパラメータの数によって異なります。一意のパラメータは、スイープのタイプに基づく別個のホストまたはポート数のしきい値です。一意のパラメータは、期間内に設定されたアドレスで一意のポートまたはホスト数を超える数が確認された場合に、アラートを起動します。一意のポートおよびホストのトラッキング処理をカウンティングといいます。

Sweep エンジンでは、すべてのシグニチャに一意のパラメータを指定する必要があります。スイープでは、2 ～ 40 までの制限が適用されます。2 は、スイープの絶対最小値です。それ以外は、（1 つのホストまたはポートの）スイープではありません。40 は、スイープが余分なメモリを消費しないように適用する必要がある実際の最大値です。一意の範囲のより現実的な値は、5 ～ 15 です。

別個の接続をカウントするスイープ インスペクタ スロットを判別するために、TCP スイープには TCP フラグとマスクが指定されている必要があります。さまざまなタイプの ICMP パケットを区別するために、ICMP スイープには ICMP タイプが指定されている必要があります。

DataNode

Sweep エンジン シグニチャに関連するアクティビティが確認されると、IPS は DataNode を使用して、特定のホストのモニタを停止する時期を判別します。DataNode には、ストリームのクロスパケット再構成を行って、ストリーム、送信元、または宛先ごとに検査状態を追跡するために必要なさまざまな固定カウンタと変数が含まれています。スイープが含まれている DataNode によって、スイープの期限が切れる時期が決まります。DataNode は、*x* 秒間（プロトコルによって異なる）トラフィックを確認しないと、スイープを停止します。

DataNode には、適応できるタイムアウトがいくつかあります。DataNode は、含まれているすべてのオブジェクトが削除された後で、アドレス セットでのアイドル時間から 30 秒後に期限切れになります。含まれている各オブジェクトにはさまざまなタイムアウトがあります。たとえば、TCP ストリームには、確立されている接続について 1 時間のタイムアウトがあります。その他ほとんどのオブジェクトの有効期限は、5 秒や 60 秒のようにさらに短くなっています。

フィールド定義

Custom Signature Wizard の [Sweep Engine Parameters] ウィンドウには、次のフィールドがあります。これらのオプションでは、非常に一般的なタイプであるか、非常に固有のタイプのトラフィックを検出するためのシグニチャを作成できます。

- [Event Action]：このシグニチャの検出時にセンサーに実行させるアクションを指定します。デフォルトは、[Produce Alert] です。

ヒント 複数のアクションを選択するには、Ctrl キーを押しながら選択します。

- [Unique]：一意的なホスト接続の数のしきい値。インターバル中にホスト接続数が Unique の値を超えた場合はアラームが送信される。
- [Protocol]：プロトコルを示します。
  - [ICMP]：ICMP ストレージ タイプを指定して、ストレージ キーとして攻撃者アドレス、攻撃者アドレスと攻撃対象ポート、または攻撃者アドレスと攻撃対象アドレスのいずれかを選択します。
  - [TCP]：[Suppress Reverse]、[Inverted Sweep]、[Mask]、[TCP Flags]、[Fragment Status]、[Storage Key] を選択するか、ポート範囲を指定できます。

  - [UDP]：ストレージ キーを選択するか、ポート範囲を指定できます。
- [Src Addr Filter]：送信元 IP アドレスがフィルタ値で定義されていないパケットを処理します。
- [Src Addr Filter]：宛先 IP アドレスがフィルタ値で定義されていないパケットを処理します。
- [Swap Attacker Victim]：アラート メッセージおよび行うアクションで攻撃者と攻撃対象のアドレスおよびポート（送信元と宛先）をスワップします。デフォルトは [No] です。

詳細情報

Sweep エンジンの詳細については、「Sweep エンジン」（P.B-67）を参照してください。

[Alert Response] ウィンドウ

Custom Signature Wizard の [Alert Response] ウィンドウには、次のフィールドがあります。

- [Signature Fidelity Rating]：ターゲットに関する具体的な情報がない場合に、このシグニチャをどの程度忠実に実行するかに関連付ける重みを示します。

  シグニチャの忠実度レーティングは、シグニチャ作成者によってシグニチャごとに計算されます。非常に特定のルール（特定の正規表現）を使用して記述されたシグニチャには、一般的なルールを使用して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が設定されます。
- [Severity of the Alert]：アラートが報告される重大度。
  - [High]：最も深刻なセキュリティ アラート。
  - [Medium]：中程度のセキュリティ アラート。
  - [Low]：最も低いセキュリティ アラート。
  - [Information]：セキュリティ アラートではなく、ネットワーク アクティビティを示します。

[Alert Behavior] ウィンドウ

センサーの通常のアラート動作は、アドレス セットごとに最初のアラートを送信してから、次の 15 秒間にこのアドレス セットについてすべてのアラートのサマリーを送信することです。このアラート動作を変更するには、[Advanced] をクリックします。ここでは、[Alert Behavior] ウィンドウについて説明します。次の事項について説明します。

- 「[Event Count and Interval] ウィンドウ」（P.8-29）
- 「[Alert Summarization] ウィンドウ」（P.8-29）
- 「[Alert Dynamic Response Fire All] ウィンドウ」（P.8-29）
- 「[Alert Dynamic Response Fire Once] ウィンドウ」（P.8-30）
- 「[Alert Dynamic Response Summary] ウィンドウ」（P.8-30）
- 「[Global Summarization] ウィンドウ」（P.8-31）

[Event Count and Interval] ウィンドウ

Advanced Alert Behavior Wizard の [Event Count and Interval] ウィンドウには、次のフィールドがあります。

- [Event Count]：このシグニチャのアラートを 1 つ送信する前にセンサーが受信する最小ヒット数を示します。
- [Event Count Key]：イベントをカウントするために使用する属性を示します。

  たとえば、同じ攻撃者からのイベントかどうかに基づいて、センサーにイベントをカウントさせる場合、イベント カウント キーとして攻撃者アドレスを選択します。
- [Use Event Interval]：レートに基づいてセンサーにイベントをカウントさせることを指定します。

  たとえば、[Event Count] を 500 イベントに設定して、[Event Interval] を 30 秒に設定した場合、相互に 30 秒以内に 500 個のイベントを受信すると、センサーは 1 つのアラートを送信します。
- [Event Interval (seconds)]：レートベース カウンティングでセンサーがイベントをカウントする時間間隔を示します。

[Alert Summarization] ウィンドウ

Advanced Alert Behavior Wizard の [Alert Summarization] ウィンドウには、次のフィールドがあります。

- [Alert Every Time the Signature Fires]：シグニチャが悪意のあるトラフィックを検出するたびに、センサーにアラートを送信させることを指定します。センサーがアラートのボリュームを動的に調整できるようにする追加のしきい値を指定できます。
- [Alert the First Time the Signature Fires]：シグニチャが初めて悪意のあるトラフィックを検出した際に、センサーにアラートを送信させることを指定します。センサーがアラートのボリュームを動的に調整できるようにする追加のしきい値を指定できます。
- [Send Summary Alerts]：シグニチャが起動されるたびにアラートを送信するのではなく、このシグニチャのサマリー アラートだけをセンサーに送信させることを指定します。センサーがアラートのボリュームを動的に調整できるようにする追加のしきい値を指定できます。
- [Send Global Summary Alerts]：シグニチャが初めてアドレス セットで起動された際に、センサーにアラートを送信させて、その後一定時間におけるすべてのアドレス セットのすべてのアラートのサマリーが含まれているグローバル サマリー アラートだけを送信させることを指定します。

[Alert Dynamic Response Fire All] ウィンドウ

[Alert Every Time the Signature Fires] を選択した際には、Advanced Alert Behavior Wizard の [Alert Dynamic Response] ウィンドウには、次のフィールドがあります。

- [Summary Key]：イベントをカウントするために使用する属性を示します。たとえば、同じ攻撃者からのイベントかどうかに基づいて、センサーにイベントをカウントさせる場合、サマリー キーとして攻撃者アドレスを選択します。
- [Use Dynamic Summarization]：センサーが、動的にサマライズ モードを開始できます。

  アラートの率が指定秒数内の指定された数のシグニチャを超えると、センサーはシグニチャごとにアラートを送信せず、アラートを 1 つのグローバル サマリーにまとめて送信します。指定間隔内にアラートの率がしきい値を下回ると、元のアラート動作に戻ります。グローバル サマリーでは、すべての攻撃者の IP アドレスとポート、およびすべての被害先 IP アドレスとポートに対してシグニチャが反応した件数がカウントされます。

  - [Summary Threshold]：センサーがサマリーを送信する前に受信する必要がある最小ヒット数を示します。
  - [Summary Interval (seconds)]：レートに基づいてイベントをカウントすることを指定し、時間間隔に使用する秒数を示します。
- [Specify Summary Threshold]：サマリーしきい値を選択できます。
  - [Global Summary Threshold]：センサーがグローバル サマリー アラートを送信する前に受信する必要がある最小ヒット数を示します。

[Alert Dynamic Response Fire Once] ウィンドウ

[Alert the First Time the Signature Fires] を選択した際には、Advanced Alert Behavior Wizard の [Alert Dynamic Response] ウィンドウには、次のフィールドがあります。

- [Summary Key]：イベントをカウントするために使用する属性を示します。たとえば、同じ攻撃者からのイベントかどうかに基づいて、センサーにイベントをカウントさせる場合、サマリー キーとして攻撃者アドレスを選択します。
- [Use Dynamic Global Summarization]：センサーが、動的にグローバル サマライズ モードを開始できます。
  - [Global Summary Threshold]：センサーがグローバル サマリー アラートを送信する前に受信する必要がある最小ヒット数を示します。

    アラート レートが指定秒数内に指定された数のシグニチャを超えると、センサーの動作は、シグニチャが初めて起動されたときに 1 つのアラートを送信する動作から、1 つのグローバル サマリー アラートを送信する動作に変わります。指定間隔内にアラートの率がしきい値を下回ると、元のアラート動作に戻ります。
  - [Global Summary Interval (seconds)]：センサーがサマライズのためにイベントをカウントする時間間隔を示します。

[Alert Dynamic Response Summary] ウィンドウ

[Summary] を選択した際には、Advanced Alert Behavior Wizard の [Alert Dynamic Response] ウィンドウには、次のフィールドがあります。

- [Summary Interval (seconds)]：センサーがサマライズのためにイベントをカウントする時間間隔を示します。
- [Summary Key]：イベントをカウントするために使用する属性を示します。たとえば、同じ攻撃者からのイベントかどうかに基づいて、センサーにイベントをカウントさせる場合、サマリー キーとして攻撃者アドレスを選択します。
- [Use Dynamic Global Summarization]：センサーが、動的にグローバル サマライズ モードを開始できます。
  - [Global Summary Threshold]：センサーがグローバル サマリー アラートを送信する前に受信する必要がある最小ヒット数を示します。

    アラート レートが指定秒数内に指定された数のシグニチャを超えると、センサーの動作は、1 つのサマリー アラートを送信する動作から、1 つのグローバル サマリー アラートを送信する動作に変わります。指定間隔内にアラートの率がしきい値を下回ると、元のアラート動作に戻ります。

（注）　適応型セキュリティ アプライアンスの複数のコンテキストが 1 つの仮想センサーに含まれている場合、サマリー アラートには、サマライズされた最後のコンテキストのコンテキスト名が含まれています。このため、このサマリーは、サマライズされるすべてのコンテキストのうち、このタイプのすべてのアラートの結果となります。

[Global Summarization] ウィンドウ

Advanced Alert Behavior Wizard の [Global Summarization] ウィンドウには、次のフィールドがあります。

- [Global Summary Interval (seconds)]：センサーがサマライズのためにイベントをカウントする時間間隔を示します。