CHAPTER 10

Custom Signature Wizard の使用

（注） IPS SSP を搭載した Cisco ASA 5585-X は、現在、Cisco IPS 7.1 をサポートする唯一のプラットフォームです。他の Cisco IPS センサーは、いずれも現在 IPS 7.1 をサポートしていません。

（注） IPS SSP を搭載した Cisco ASA 5585-X 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、Custom Signature Wizard について、およびこのウィザードを使用してカスタム シグニチャを作成する方法について説明します。内容は次のとおりです。

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。

（注） AIP SSC-5 は、カスタム シグニチャの作成、シグニチャの追加、シグニチャのクローニングをサポートしていません。既存のシグニチャを調整（編集）できます。

Custom Signature Wizard は、カスタム シグニチャを作成する手順をステップバイステップで案内します。カスタム シグニチャを作成するには、シグニチャ エンジンを使用する場合と使用しない場合の 2 つのシーケンスがあります。

詳細情報

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

次のシーケンスは、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　シグニチャ識別パラメータを割り当てます。

- シグニチャ ID
- サブシグニチャ ID
- シグニチャ名
- アラート注釈（任意）
- ユーザ コメント（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はありますが、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。

- シグニチャ忠実度レーティング
- アラートの重大度

ステップ 5　アラートの動作を割り当てます。デフォルトのアラートの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。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。

Custom Signature Wizard でサポートされていないシグニチャ エンジン

Cisco IPS の Custom Signature Wizard は、次のシグニチャ エンジンに基づくカスタム シグニチャの作成をサポートしていません。

- 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

必要なエンジンから既存のシグニチャをクローニングして、これらの既存のシグニチャ エンジンに基づくカスタム シグニチャを作成できます。

詳細情報

- CLI を使用して、これらのシグニチャ エンジンを使用したカスタム シグニチャを作成する方法の詳細については、『*Cisco Intrusion Prevention System Sensor CLI Configuration Guide for IPS 71*』を参照してください。
- シグニチャのクローニングの詳細については、「シグニチャのクローニング」（P.9-16）を参照してください。

シグニチャ エンジンを使用しない方法

次のシーケンスは、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 プロトコルの場合は、トラフィック タイプと検査データ タイプを選択します。TCP プロトコルの場合は、トラフィック タイプを選択します。

ステップ 3　シグニチャ識別パラメータを割り当てます。

- シグニチャ ID
- サブシグニチャ ID
- シグニチャ名
- アラート注釈（任意）
- ユーザ コメント（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はありますが、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。

- シグニチャ忠実度レーティング
- アラートの重大度

ステップ 6　アラートの動作を割り当てます。デフォルトのアラートの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。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） AIP SSC-5 は、カスタム シグニチャの作成、シグニチャの追加、シグニチャのクローニングをサポートしていません。既存のシグニチャを調整（編集）できます。

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に影響を与えることがあります。センサー上の新しいシグニチャの効果をモニタするには、[Configuration] > *sensor_name* > [Interface Configuration] > [Traffic Flow Notifications] を選択し、[Missed Packet Threshold] および [Notification Interval] オプションを設定して、センサーが新しいシグニチャをどのように処理しているかを評価するように設定します。

ヒント チェックボックスが空白の場合、デフォルト値が使用されます。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ステップバイステップで案内します。

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 IME にログインします。

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

ステップ 3　新しいシグニチャの作成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] オプション ボタンをクリックし、[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。手順 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と一致するオプション ボタンをクリックし、[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、次のオプション ボタンの 1 つをクリックし、[Next] をクリックします。

- [Single Packet] : Atomic IP エンジン（ヘッダー データ用）または String ICMP エンジンを使用して 1 つのパケットで攻撃を検査するシグニチャを作成しています。ステップ 11 に進みます。
- [Sweeps] 新しいシグニチャに Sweep エンジンを使用してスイープ攻撃を検出するシグニチャを作成しています。ステップ 12 に進みます。

ステップ 6　[UDP Traffic Type] ウィンドウで、次のオプション ボタンの 1 つをクリックし、[Next] をクリックします。

- [Single Packet]：Atomic IP エンジン（ヘッダー データ用）または String UDP エンジンを使用して 1 つのパケットで攻撃を検査するシグニチャを作成しています。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シグニチャを作成しています。ステップ 7 に進みます。

ステップ 7　[UDP Sweep Type] ウィンドウで、次のオプション ボタンの 1 つをクリックし、[Next] をクリックします。

- [Host Sweep]：スイープを使用して、ホスト上の開いたポートを検索するシグニチャを作成しています。新しい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上のホストを検索するシグニチャを作成しています。新しい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、次のオプション ボタンの 1 つをクリックし、[Next] をクリックします。

- [Single Packet]：1 つのパケットで攻撃を検査するシグニチャを作成しています。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]：1 つの TCP 接続で攻撃を検出するシグニチャを作成しています。ステップ 9 に進みます。
- [Multiple Connections]：複数の接続で攻撃を検査するシグニチャを作成しています。ステップ 10 に進みます。

ステップ 9　[Service Type] ウィンドウで、次のオプション ボタンの 1 つをクリックして、[Next] をクリックし、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シグニチャを作成しています。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シグニチャを作成しています。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シグニチャを作成しています。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シグニチャを作成しています。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、RPC 以外のサービスを使用する攻撃を検出するシグニチャを作成しています。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、次のオプション ボタンの 1 つをクリックして、[Next] をクリックし、ステップ 12 に進みます。

- [Host Sweep]：スイープを使用して、ホスト上の開いたポートを検索するシグニチャを作成しています。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上のホストを検索するシグニチャを作成しています。新しい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　1 つのパケットの場合は、[Inspect Data] ウィンドウで次のオプション ボタンの 1 つをクリックし、[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で識別する属性を指定し、[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] フィールドにデフォルト名が表示されます。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 とともにイベント ビューアに報告されます。

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ている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、このテキストはイベント ビューアに報告されます。

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　エンジン固有のパラメータに値を割り当て、[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。シグニチャ忠実度レーティングの有効値は 0 ～ 100 で、シグニチャに対する信頼度を示します。100 が最も信頼度が高いことを示します。

b. [Severity of the Alert] ドロップダウン リストから、センサーがアラートを送信する際にイベント ビューアで報告す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の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の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、IPS に偽のトラフィックを送り、IPS が短時間に大量のアラートを発生させるようにする「Stick」などの IDS 対抗ツールに対応させる場合があります。

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、このシグニチャについて 1 個のアラートを送信する前にセンサーが受信する必要がある最小ヒット数です。

b. [Event Count Key] ドロップダウン リストから、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、同じ攻撃者から受信したかどうかに基づいてセンサーでイベントをカウントするには、[Event Count Key] として [Attacker address] を選択します。

c. アラート率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、間隔として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、センサーでアラートをどのようにサマライズするかを設定するには、次のオプション ボタンの 1 つをクリックします。

- [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からアラートを送信するように指定します。その後、アラートの量をダイナミックに調整できる追加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ときにセンサーからアラートを送信するように指定します。その後、アラートの量をダイナミックに調整できる追加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せず、センサーからこのシグニチャのサマリー アラートのみを送信するように指定します。その後、アラートの量をダイナミックに調整できる追加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] : 1 つのアドレス セットで初めてシグニチャが起動されたときにセンサーからアラートを送信し、その後、指定した時間間隔ですべてのアドレス セットに関するすべてのアラートのサマリーを含むグローバル サマリー アラートのみを送信するように指定します。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 リストから、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、センサーでイベントが同じ攻撃者からかどうかに基づいてカウントする場合は、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 サマライズでは、センサーは、設定したサマリー パラメータに基づいて送信するアラートの量をダイナミックに調整できます。

c. [Summary Threshold] フィールドに、このシグニチャについて、サマリー アラートを送信する前にセンサーが受信する必要が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. センサーをグローバル サマライズ モードにするには、[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、グローバル サマリー アラートを送信する前にセンサーが受信する必要が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 リストから、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、センサーでイベントが同じ攻撃者からかどうかに基づいてカウントする場合は、サマリー キーとして攻撃者のアドレスを選択します。

b. センサーでダイナミック グローバル サマライズを使用するには、[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、グローバル サマリー アラートを送信する前にセンサーが受信する必要がある最小ヒット数を入力します。

（注）　アラート率が指定秒数内に指定された数のシグニチャを超えると、センサーはシグニチャが最初に起動されたとき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。

d. [Global Summary Interval (seconds)] フィールドに、センサーがサマライズする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する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 リストから、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、センサーでイベントが同じ攻撃者からかどうかに基づいてカウントする場合は、サマリー キーとして攻撃者のアドレスを選択します。

c. センサーでダイナミック グローバル サマライズを使用するには、[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、グローバル サマリー アラートを送信する前にセンサーが受信する必要がある最小ヒット数を入力します。

（注）　アラート率が指定秒数内に指定された数のシグニチャを超えると、センサーはシグニチャが最初に起動されたとき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。

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する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　[Yes] をクリックして、カスタム シグニチャを作成します。作成したシグニチャがイネーブルになり、シグニチャのリストに追加されます。

ヒント　変更を破棄するには、[Cancel] をクリックします。

Custom Signature Wizard のフィールド定義

ここでは、Custom Signature Wizard のウィンドウとフィールド定義について説明します。3 つのサンプル カスタム シグニチャを作成する手順も示します。内容は次のとおりです。

[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] フィールドがアクティブになり、シグニチャ エンジンのリストから選択できます。
- [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。シグニチャの作成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、ドロップダウン リストからエンジンの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 トラフィック用のシグニチャを作成できます。
  - [Service MSRPC]：MSRPC トラフィック用のシグニチャを作成できます。
  - [Service RPC]：RPC トラフィック用のシグニチャを作成できます。
  - [State SMTP]：SMTP トラフィック用のシグニチャを作成できます。
  - [String ICMP]：ICMP 文字列用のシグニチャを作成できます。
  - [String TCP]：TCP 文字列用のシグニチャを作成できます。
  - [String UDP]：UDP 文字列用のシグニチャを作成できます。
  - [Sweep]：スイープ用のシグニチャを作成できます。

- [No] : Custom Signature Wizard の詳細なエンジン選択画面に進むことができます。

[Protocol Type] ウィンドウ

特定のプロトコルで悪意のある動作を探すシグニチャを定義できます。シグニチャで次のプロトコルをデコードし、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および検査するシグニチャを作成します。
- [ICMP] : ICMP トラフィックをデコードおよび検査するシグニチャを作成します。
- [UDP] : UDP トラフィックをデコードおよび検査するシグニチャを作成します。
- [TCP] : TCP トラフィックをデコードおよび検査するシグニチャを作成します。

[Signature Identification] ウィンドウ

シグニチャ識別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オプションです。

フィールド定義

カスタム シグニチャ ウィンドウの [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 により、センサーは特定のシグニチャを識別できます。アラートが生成されると、シグニチャ ID がイベント ビューアに報告されます。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。アラートが生成されると、サブシグニチャがイベント ビューアに報告されます。
- [Signature Name] : このシグニチャに割り当てられた名前を示します。アラートが生成されると、イベント ビューアに報告されます。
- [Alert Notes] :（任意）このシグニチャが起動されたときに、アラートに関連付けられるテキストを指定します。アラートが生成されると、イベント ビューアに報告されます。
- [User Comments] :（任意）シグニチャ パラメータとともに格納する、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、ネットワーク環境での複数のコンピュータ間の連携処理と、使用されるアプリケーション ソフトウェアに対応しています。MSRPC はトランザクションベースのプロトコルです。チャネルを確立し、処理要求および応答を受け渡す一連の通信が発生します。

MSRPC は、ISO レイヤ 5 および 6 のプロトコルで、UDP、TCP、SMB などの他のトランスポート プロトコルの上の階層となります。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処理する機能も含まれます。

この通信チャネルは、最近の Windows NT、Windows 2000、および Window XP の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 タイプについて DCE および RPC プロトコルをデコードするだけです。

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を使用して、非常に一般的なタイプのトラフィックや特定のタイプのトラフィックを検出するシグニチャを作成できます。

- [Event Action]：このシグニチャが検出されたときにセンサーで実行す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** キーを押しながらクリックします。

- [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、最小一致長さを含む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）演算を指定できます。
- [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を記載した表については、「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]：1 つのパケットで攻撃を検査するシグニチャを作成するように指定します。
- [Sweeps]：スイープ攻撃を検出するシグニチャを作成するように指定します。

[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]：1 つのパケットで攻撃を検査するシグニチャを作成するように指定します。
- [Sweeps]：スイープ攻撃を検出するシグニチャを作成するように指定します。

[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]：ネットワーク上のホストを検索するスイープを識別します。
- [Port Sweep]：ホスト上の開かれたポートを検索するスイープを識別します。

[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]：1 つのパケットで攻撃を検査するシグニチャを作成するように指定します。
- [Single TCP Connection]：1 つの TCP 接続で攻撃を検査するシグニチャを作成するように指定します。
- [Multiple Connections]：複数の接続で攻撃を検査するシグニチャを作成するように指定します。

[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シグニチャを作成するように指定します。
- [SMTP]：SMTP サービスを使用する攻撃を説明するシグニチャを作成するように指定します。
- [RPC]：RPC サービスを使用する攻撃を説明するシグニチャを作成するように指定します。
- [MSRPC]：MSRPC サービスを使用する攻撃を説明するシグニチャを作成するように指定します。
- [Other]：HTTP、SMTP、RPC、MSRPC 以外のサービスを使用する攻撃を説明するシグニチャを作成するように指定します。

[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]：ネットワーク上のホストを検索するスイープを識別します。
- [Port Sweep]：ホスト上の開かれたポートを検索するスイープを識別します。

[Atomic IP Engine Parameters] ウィンドウ

Atomic IP エンジンでは、IP プロトコル ヘッダーおよび関連付けられたレイヤ 4 トランスポート プロトコル（TCP、UDP、および ICMP）と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 つのパケットの解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を使用して、非常に一般的なタイプのトラフィックや特定のタイプのトラフィックを検出するシグニチャを作成できます。

- [Event Action]：このシグニチャが検出されたときにセンサーで実行す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** キーを押しながらクリックします。

- [Fragment Status]：フラグメント化されたトラフィックまたはフラグメント化されていないトラフィックのどちらを検査するかを示します。
- [Specify Layer 4 Protocol]：（任意）特定のプロトコルがこのシグニチャに適用されるかどうかを選択できます。

  [Yes] を選択した場合は、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、識別子、および合計長を指定できます。
  - [Other IP Protocols]：識別子を指定できます。
  - [TCP Protocol]：送信元と宛先について、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、予約属性、およびポート範囲を設定できます。
  - [UDP Protocol]：送信元と宛先について、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）タイプ オブ サービスを指定できます。
- [Specify IP Time-to-Live]：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 識別子を指定できます。
- [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]：送信元または宛先としてローカル ホスト アドレスが使用されているトラフィックを識別します。

- [IP Addresses]：送信元または宛先アドレスを指定できます。
- [RFC 1918 Address]：アドレスのタイプを RFC 1918 として識別します。
- [Src IP Equal Dst IP]：送信元アドレスと宛先アドレスが同じトラフィックを識別します。

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-27）を参照してください。

Atomic IP Advanced エンジンのシグニチャの例

ヒント チェックボックスが空白の場合、デフォルト値が使用されます。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

次の例では、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、次のカスタム シグニチャは、ヘッダーがタイプ 1、長さが 8 の HOP オプション ヘッダーを持つ IPv6 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 IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [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、このシグニチャに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、このシグニチャのシグニチャ忠実度レーティングを表す 1 ～ 100 の値を入力します。

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　シグニチャを説明するフィールドに入力し、このシグニチャに関するコメントを追加します。

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、センサーがイベントに応答するときのアクションを選択します。

（注） IPv6 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** キーを押しながらクリックします。

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ます。次に [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ます。次に [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] フィールドから [Yes] を選択し、次に [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長をイネーブルにします。次に [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を入力します（1 ～ 65535）。

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を選択します（[Yes] または [No]）。

d. [Yes] を選択した場合、[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（[Yes]）のままにします。

（注）　センサーがシグニチャで指定されている攻撃を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（[Yes]）のままにします。これで、シグニチャがエンジンに置かれます。

（注）　センサーがシグニチャで指定されている攻撃を検出するには、そのセンサーに対してシグニチャを非アクティブにしないでください。

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** キーを押しながらクリックします。

ステップ 16　[Mars Category] ドロップダウン リストから、このシグニチャで識別する 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** キーを押しながらクリックします。

ヒント　変更内容を破棄して [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] が [Custom] に設定されたリストに、新しいシグニチャが表示されます。

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　変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

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に基づくパターン照合インスペクション 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よく使用されているプロトコルの 1 つです。また、最も長い前処理時間を必要とし、システムの全体的なパフォーマンスにとって必須の検査を必要とするシグニチャの数も最も多くあります。

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 サービスのみに向けられたトラフィック、つまり HTTP 要求を検索します。このエンジンでリターン トラフィックを検査することはできません。このエンジンでは、各シグニチャが対象とする個別の 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用意されています。

フィールド定義

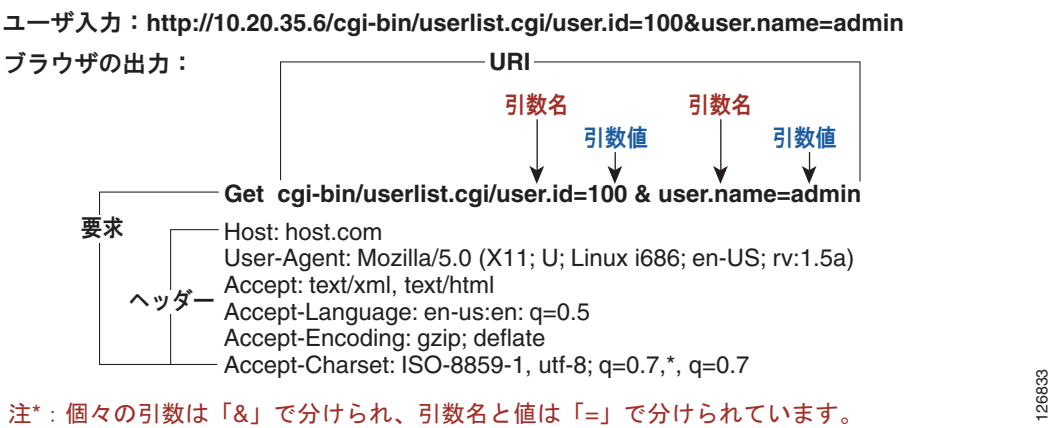
Custom Signature Wizard の [Service HTTP Engine Parameters] ウィンドウには、次のフィールドがあります。これらのオプションを使用して、非常に一般的なタイプのトラフィックや特定のタイプのトラフィックを検出するシグニチャを作成できます。

- [Event Action]：このシグニチャが検出されたときにセンサーで実行す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** キーを押しながらクリックします。

- [De Obfuscate]：検索の前に反回避 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）最大 URI、引数、ヘッダー、および要求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。



注*：個々の引数は「&」で分けられ、引数名と値は「=」で分けられています。

- [Regex]：URI、引数、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]：トラフィックで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 メッセージで、および適用される任意のアクションについて、攻撃者と攻撃対象のアドレスとポート（送信元と宛先）を交換します。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-48）を参照してください。
- シグニチャの正規表現構文を記載した表については、「正規表現の構文」（P.B-10）を参照してください。

Service HTTP エンジンのシグニチャの例

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を与える可能性があります。ネットワークのベースライン センサー パフォーマンスを基準にカスタム シグニチャをテストして、シグニチャの全体的な影響を判断してください。

ヒント　チェックボックスが空白の場合、デフォルト値が使用されます。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 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 IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [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、[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、次の必須値を指定して、[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] フィールドにデフォルト名 My Sig 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 とともにイベント ビューアに報告されます。

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ている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、このテキストはイベント ビューアに報告されます。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、[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、拒否やブロックなどの複数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** キーを押しながらクリックします。

ステップ 6　[De Obfuscate] フィールドのドロップダウン リストから [Yes] を選択して、検索の前に反回避解読を適用するようにシグニチャを設定します。

ステップ 7　（任意）[Max Field Sizes] で、次の最大フィールド サイズ 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 Arg 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 Arg 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] フィールドのドロップダウン リストから [Yes] を選択します。

b. [URI Regex] フィールドで、「[Mm][Yy][Ff][Oo][Oo]」などの URI 正規表現を入力します。

c. 次のオプション パラメータに値を指定できます。

- [Specify Arg Name Regex]：[Arguments] フィールドで特定の正規表現を検索できるようにします。
- [Specify Header Regex]：[Header] フィールドで特定の正規表現を検索できるようにします。
- [Specify Request Regex]：[Request] フィールドで特定の正規表現を検索できるようにします。

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 サービスが常駐する、カンマ区切りのポートのリストまたはポート範囲です。

ステップ 10　（任意）[Swap Attacker Victim] ドロップダウン リストから、[Yes] を選択し、アラート メッセージと実行するアクションにおいて、攻撃者と攻撃対象のアドレスとポート（宛先と送信元）を入れ替えます。

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。シグニチャ忠実度レーティングの有効値は 0 ～ 100 で、シグニチャに対する信頼度を示します。100 が最も信頼度が高いことを示します。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ときにイベント ビューアで報告する重大度を選択します。デフォルトは [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。変更しない場合は、[Finish] をクリックします。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、センサーに適用するかどうかを尋ねるメッセージが表示されます。

ステップ 15　[Yes] をクリックして、カスタム シグニチャを作成します。作成したシグニチャがイネーブルになり、シグニチャのリストに追加されます。

ヒント　変更を破棄するには、[Cancel] をクリックします。

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-48）を参照してください。
- シグニチャの正規表現構文を記載した表については、「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 プロトコル専用で、反回避戦略としてフル デコードを行います。これにより、フラグメント化されたメッセージ（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 スイープと似ていますが、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が異なります。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を使用して、非常に一般的なタイプまたは非常に固有のタイプのトラフィックを検出するシグニチャを作成できます。

- [Event Action]：このシグニチャが検出されたときにセンサーで実行す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** キーを押しながらクリックします。

- [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か、送信元とするトラフィックかを指定します。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 サービスが常駐するポートまたはポート範囲を示します。有効な値は、カンマで区切られたポートまたはポート範囲のリストです。
- [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]：このシグニチャが対象とするポート 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]：このシグニチャが対象とする 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 に設定された場合にアラートを起動します。
- [Specify RPC Max Length]：RPC メッセージ全体の最大許容長を示します。長さがこの値を超えるとアラームが生成されます。有効な範囲は 0 ～ 65535 です。
- [Specify RPC Procedure]：このシグニチャが対象とする 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を記載した表については、「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および正規表現ベースのパターン検査を行います。State エンジン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、出力やアラートを発生させる特定のイベントを記述するために使用されます。State エンジンには、SMTP、シスコ ログイン、および LPR フォーマット ストリングの 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を使用して、非常に一般的なタイプまたは非常に固有のタイプのトラフィックを検出するシグニチャを作成できます。

- [Event Action]：このシグニチャが検出されたときにセンサーで実行す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** キーを押しながらクリックします。

- [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]：状態の名前を識別します。オプションは、[Abort]、[Mail Body]、[Mail Header]、[SMTP Commands]、および [Start] です。
- [Specify Min Match Length]：一致の開始から終わりまでに正規表現文字列が一致している必要がある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の文字列を示します。
- [Direction]：遷移について検査するデータ 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 サービスが常駐するポートまたはポート範囲を示します。有効な値は、カンマで区切られたポートまたはポート範囲のリストです。
- [Swap Attacker Victim]：アラート メッセージで、および適用される任意のアクションについて、攻撃者と攻撃対象のアドレスとポート（送信元と宛先）を交換します。デフォルトは [No] です。
- [Specify Exact Match Offset]：正規表現の文字列が一致していることを報告するために必要な正確なストリーム オフセットをバイト数で示します。[Yes] を選択した場合、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] を選択した場合は、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を記載した表については、「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 の各プロトコルを対象とした、汎用ベースのパターン マッチング インスペクション エンジンです。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。3 つの String エンジン、String ICMP、String TCP、および String UDP 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を使用して、非常に一般的なタイプまたは非常に固有のタイプのトラフィックを検出するシグニチャを作成できます。

- [Event Action]：このシグニチャが検出されたときにセンサーで実行す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** キーを押しながらクリックします。

- [Specify Min Match Length]：一致の開始から終わりまでに正規表現文字列が一致している必要がある最小バイト数を識別します。有効な範囲は 0 ～ 65535 です。
- [Regex String]：1 つのパケットで検索する正規表現の文字列を示します。

- [Direction]：遷移について検査するデータ 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 メッセージで、および適用される任意のアクションについて、攻撃者と攻撃対象のアドレスとポート（送信元と宛先）を交換します。デフォルトは [No] です。
- [Specify Exact Match Offset]：正規表現の文字列が一致していることを報告するために必要な正確なストリーム オフセットをバイト数で示します。[Yes] を選択した場合、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] を選択した場合は、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 アーキテクチャの詳細については、「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を記載した表については、「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 の各プロトコルを対象とした、汎用ベースのパターン マッチング インスペクション エンジンです。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。3 つの String エンジン、String ICMP、String TCP、および String UDP 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を使用して、非常に一般的なタイプまたは非常に固有のタイプのトラフィックを検出するシグニチャを作成できます。

- [Event Action]：このシグニチャが検出されたときにセンサーで実行す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** キーを押しながらクリックします。

- [Strip Telnet Options]：パターン検索の前に、データ ストリームから Telnet オプション制御文字を取り除きます。これは、主に、反回避ツールとして使用されます。デフォルトは [No] です。
- [Specify Min Match Length]：一致の開始から終わりまでに正規表現文字列が一致している必要がある最小バイト数を示します。有効な範囲は 0 ～ 65535 です。
- [Regex String]：1 つのパケットで検索する正規表現の文字列を示します。
- [Service Ports]：ターゲット サービスが常駐するポートまたはポート範囲を示します。有効な値は、カンマで区切られたポートまたはポート範囲のリストです。
- [Direction]：遷移について検査するデータ 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]：正規表現の文字列が一致していることを報告するために必要な正確なストリーム オフセットをバイト数で示します。[Yes] を選択した場合、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] を選択した場合は、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 メッセージで、および適用される任意のアクションについて、攻撃者と攻撃対象のアドレスとポート（送信元と宛先）を交換します。デフォルトは [No] です。

詳細情報

- String ICMP アーキテクチャの詳細については、「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を記載した表については、「正規表現の構文」（P.B-10）を参照してください。

String TCP エンジンのシグニチャの例

（注） 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。

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を与える可能性があります。ネットワークのベースライン センサー パフォーマンスを基準にカスタム シグニチャをテストして、シグニチャの全体的な影響を判断してください。

ヒント チェックボックスが空白の場合、デフォルト値が使用されます。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 を使用して、カスタム String TCP シグニチャを作成します。

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 IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [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、[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、次の必須値を指定して、[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] フィールドにデフォルト名 My Sig 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 とともにイベント ビューアに報告されます。

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ている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、このテキストはイベント ビューアに報告されます。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、拒否やブロックなどの複数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** キーを押しながらクリックします。

ステップ 6　（任意）[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、パターンを検索する前にデータから Telnet オプション文字を除去します。

ステップ 7　（任意）最小一致長をイネーブルにするには、[Specify Min Match Length] フィールドのドロップダウン リストから [Yes] を選択し、[Min Match Length] フィールドに正規表現の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、23 などのポート番号を入力します。値は、ターゲット サービスが常駐する、カンマ区切りのポートの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 リストから、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）完全一致オフセットをイネーブルにするには、[Specify Exact Match Offset] フィールドのドロップダウン リストから [Yes] を選択します。完全一致オフセットは、一致が有効であると認められるために正規表現の文字列が報告する必要がある正確なストリーム オフセットです（0 ～ 65535）。

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] ドロップダウン リストから、[Yes] を選択し、アラート メッセージと実行するアクションにおいて、攻撃者と攻撃対象のアドレスとポート（宛先と送信元）を入れ替えます。

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。

SFR の有効値は 0 ～ 100 で、シグニチャに対する信頼度を示します。100 が最も信頼度が高いことを示します。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ときにイベント ビューアで報告する重大度を選択します。デフォルトは [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。変更しない場合は、[Finish] をクリックします。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、センサーに適用するかどうかを尋ねるメッセージが表示されます。

ステップ 16　[Yes] をクリックして、カスタム シグニチャを作成します。作成したシグニチャがイネーブルになり、シグニチャのリストに追加されます。

ヒント　変更を破棄するには、[Cancel] をクリックします。

詳細情報

- String ICMP アーキテクチャの詳細については、「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を記載した表については、「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 の各プロトコルを対象とした、汎用ベースのパターン マッチング インスペクション エンジンです。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。3 つの String エンジン、String ICMP、String TCP、および String UDP 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を使用して、非常に一般的なタイプまたは非常に固有のタイプのトラフィックを検出するシグニチャを作成できます。

- [Event Action]：このシグニチャが検出されたときにセンサーで実行す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** キーを押しながらクリックします。

- [Specify Min Match Length]：一致の開始から終わりまでに正規表現文字列が一致している必要がある最小バイト数を示します。有効な範囲は 0 ～ 65535 です。
- [Regex String]：1 つのパケットで検索する正規表現の文字列を示します。
- [Service Ports]：ターゲット サービスが常駐するポートまたはポート範囲を示します。有効な値は、カンマで区切られたポートまたはポート範囲のリストです。
- [Direction]：遷移について検査するデータ ストリームの方向を示します。
- [Swap Attacker Victim]：シグニチャの起動時に、アラートで報告される送信元アドレスと宛先アドレスを交換するかどうかを指定します。デフォルトは [No] です。
- [Specify Exact Match Offset]：正規表現の文字列が一致していることを報告するために必要な正確なストリーム オフセットをバイト数で示します。[Yes] を選択した場合、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] を選択した場合は、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 アーキテクチャの詳細については、「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を記載した表については、「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 エンジンでは、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したり、カスタム シグニチャを作成したりすることができます。Sweep エンジンには、ICMP、UDP、および TCP のプロトコル固有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カウントに依存します。一意のパラメータは、スイープのタイプに応じた、個別ホストまたはポートの数のしきい値です。一意のパラメータは、期間内に一意のポート数またはホスト数がアドレス セット上に存在するとアラートをトリガーします。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言います。

Sweep エンジンの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（それぞれの値を含む）の制限値が強制されます。スイープの絶対最小値は 2 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、スイープによってメモリが過剰に消費されないように強制する必要がある場合の実際的な最大値です。一意の範囲の現実的な値は、5 ～ 15 です。

個別接続をカウントするスイープ インスペクタ スロットを判断するために、TCP スイープでは TCP フラグとマスクを指定する必要があります。さまざまなタイプの ICMP パケットを区別するために、ICMP スイープでは ICMP タイプを指定する必要があります。

DataNode

Sweep エンジン シグニチャに関連するアクティビティが検出されると、IPS は DataNode を使用して、そのホストのモニタリングをいつ停止するかを決定します。DataNode には、複数パケットにわたるストリームの再構成と、ストリーム単位、ソース単位、宛先単位で検査状態を追跡するためのさまざまな永続カウンタと変数が含まれています。スイープを含む DataNode は、スイープをいつ失効させるかを決定します。DataNode は、その DataNode で *x* 秒間（プロトコルに依存）トラフィックが発生しないと、スイープを停止します。

DataNode には、複数の適応型タイムアウトがあります。DataNode は、含まれているすべてのオブジェクトが取り除かれてから、アドレス セットでアイドル時間が 30 秒経過すると失効します。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 ストリームの場合、確立した接続には 1 時間のタイムアウトがあります。他のほとんどのオブジェクトの有効期限は非常に短く、5 秒や 60 秒などです。

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を使用して、非常に一般的なタイプまたは非常に固有のタイプのトラフィックを検出するシグニチャを作成できます。

- [Event Action]：このシグニチャが検出されたときにセンサーで実行す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** キーを押しながらクリックします。

- [Unique]：一意のホスト接続の数のしきい値を示します。インターバル中にホスト接続数が [Unique] の値を超えると、アラートが送信されます。
- [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、ストレージ キー（攻撃者のアドレス、攻撃者のアドレスと攻撃対象のポート、または攻撃者と攻撃対象のアドレス）から 1 つを選択できます。
  - [TCP]：リバース抑制、反転スイープ、マスク、TCP フラグ、フラグメント ステータス、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。
  - [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]：フィルタ値で定義された送信元 IP アドレス（または複数のアドレス）が含まれていないパケットを処理します。
- [Dst Addr Filter]：フィルタ値で定義された宛先 IP アドレス（または複数のアドレス）が含まれていないパケットを処理します。
- [Swap Attacker Victim]：シグニチャの起動時に、アラートで報告される送信元アドレスと宛先アドレスを交換するかどうかを指定します。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。シグニチャ忠実度レーティングは、シグニチャベースでシグニチャの作成者が計算します。非常に具体的なルール（特定の正規表現）で作成されたシグニチャは、一般的なルールで作成されたシグニチャよりシグニチャ忠実度レーティングは高くなります。
- [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では、各アドレス セットに最初のアラートが送信され、次の 15 秒にわたって、このアドレス セットに対するすべてのアラートのサマリーを送信します。このアラート動作を変更するには、[Advanced] をクリックします。

[Event Count and Interval] ウィンドウ

Advanced Alert Behavior ウィザードの [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]：このシグニチャについて 1 つのアラートを送信する前にセンサーが受け取る必要のある最小ヒット数を示します。
- [Event Count Key]：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、センサーでイベントが同じ攻撃者からかどうかに基づいてカウントする場合は、[Event Count Key] として [Attacker Address] を選択します。
- [Use Event Interval]：センサーでアラート率に基づいてイベントをカウントするように指定します。たとえば、[Event Count] を 500 イベント、[Event Interval] を 30 秒に設定すると、センサーは、30 秒内に 500 イベントを受け取った場合に、1 つのアラートを送信します。
- [Event Interval (seconds)]：センサーがアラート率ベースでイベントをカウントする際の間隔を識別します。

[Alert Summarization] ウィンドウ

Advanced Alert Behavior ウィザードの [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からアラートを送信するように指定します。その後、センサーがアラートの量をダイナミックに調整できる追加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ときにセンサーからアラートを送信するように指定します。その後、センサーがアラートの量をダイナミックに調整できる追加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せず、センサーからこのシグニチャのサマリー アラートのみを送信するように指定します。その後、センサーがアラートの量をダイナミックに調整できる追加しきい値を指定できます。
- [Send Global Summary Alerts]：1 つのアドレス セットで初めてシグニチャが起動されたときにセンサーからアラートを送信し、その後、指定した時間間隔ですべてのアドレス セットに関するすべてのアラートのサマリーを含むグローバル サマリー アラートのみを送信するように指定します。

[Alert Dynamic Response Fire All] ウィンドウ

[Alert Every Time the Signature Fires] を選択した場合、Advanced Alert Behavior ウィザードの [Alert Dynamic Response] ウィンドウには次のフィールドがあります。

- [Summary Key]：イベントのカウントに使用する属性を示します。たとえば、センサーでイベントが同じ攻撃者からかどうかに基づいてカウントする場合は、[Summary Key] として [Attacker Address] を選択します。
- [Use Dynamic Summarization]：センサーをダイナミックにサマライズ モードに設定できます。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]：サマリーを送信する前にセンサーが受信する必要がある最小ヒット数を示します。

  - [Summary Interval (seconds)]：アラート率に基づいてイベントをカウントするよう指定し、この間隔に使用する秒数を示します。
- [Specify Summary Threshold]：サマリーのしきい値を選択できます。
  - [Global Summary Threshold]：グローバル サマリー アラートを送信する前にセンサーが受信する必要がある最小ヒット数を指定します。

[Alert Dynamic Response Fire Once] ウィンドウ

[Alert the First Time the Signature Fires] を選択した場合、Advanced Alert Behavior ウィザードの [Alert Dynamic Response] ウィンドウには次のフィールドがあります。

- [Summary Key]：イベントのカウントに使用する属性を示します。たとえば、センサーでイベントが同じ攻撃者からかどうかに基づいてカウントする場合は、[Summary Key] として [Attacker Address] を選択します。
- [Use Dynamic Global Summarization]：センサーをダイナミックにグローバル サマライズ モードに設定できます。
  - [Global Summary Threshold]：グローバル サマリー アラートを送信する前にセンサーが受信する必要がある最小ヒット数を指定します。

    アラート率が指定秒数内に指定された数のシグニチャを超えると、センサーはシグニチャが最初に起動されたとき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。
  - [Global Summary Interval (seconds)]：センサーがサマリーを作成するためにイベントをカウントする間隔を示します。

[Alert Dynamic Response Summary] ウィンドウ

[Summary] を選択した場合、Advanced Alert Behavior ウィザードの [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)]：センサーがサマリーを作成するためにイベントをカウントする間隔を指定します。
- [Summary Key]：イベントのカウントに使用する属性を示します。たとえば、センサーでイベントが同じ攻撃者からかどうかに基づいてカウントする場合は、[Summary Key] として [Attacker Address] を選択します。
- [Use Dynamic Global Summarization]：センサーをダイナミックにグローバル サマライズ モードに設定できます。
  - [Global Summary Threshold]：グローバル サマリー アラートを送信する前にセンサーが受信する必要がある最小ヒット数を指定します。アラート率が指定秒数内に指定された数のシグニチャを超えると、センサーは 1 つのサマリー アラートを送信せずに、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。

（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 ウィザードの [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)]：センサーがサマリーを作成するためにイベントをカウントする間隔を示します。