カスタム シグニチャの作成

この章では、Custom Signature Wizard 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。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」を参照してください。

この章は、次の項で構成されています。

- Custom Signature Wizard について（P.6-2）
- サポートされるユーザのロール（P.6-5）
- フィールド定義（P.6-5）
- カスタム シグニチャの作成（P.6-22）

Custom Signature Wizard について

Custom Signature Wizard は、カスタム シグニチャを作成する手順を順を追って示します。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方法と、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方法の 2 つの手順があります。

IPS 5.1 の Custom Signature Wizard では、次のシグニチャ エンジンを使用してカスタム シグニチャを作成する方法はサポートされていません。

- AIC FTP
- AIC HTTP
- Atomic ARP
- Flood Host
- Flood Net
- Meta
- Multi String
- Normalizer
- Service DNS
- Service FTP
- Service Generic
- Service H224
- Service IDENT
- Service MSSQL
- Service NTP
- Service SMB
- Service SNMP
- Service SSH
- Sweep TCP Other

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、Configuration > Signature Configuration > Clone をクリックしてエンジンから既存のシグニチャを複製します。詳細については、P.5-19 の「シグニチャの複製」を参照してください。

これらのシグニチャ エンジンを使用し、カスタム シグニチャを CLI によって作成する方法の詳細については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』を参照してください。

この項で取り上げる事項は次のとおりです。

- シグニチャ エンジンを使用する方法（P.6-3）
- シグニチャ エンジンを使用しない方法（P.6-4）

シグニチャ エンジンを使用する方法

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
- Service HTTP
- Service MSRPC
- Service RPC
- State (SMTP, ...)
- String ICMP
- String TCP
- String UDP
- Sweep

ステップ 2　シグニチャの識別子を割り当てます。

- シグニチャ ID
- サブシグニチャ ID
- シグニチャ名
- アラートの注釈（オプション）
- ユーザ コメント（オプション）

ステップ 3　エンジン固有のパラメータを割り当てます。

パラメータはシグニチャ エンジンごとに異なりますが、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 1 つあります。

ステップ 4　アラート応答を割り当てます。

- シグニチャ忠実度評価
- アラートの重大度

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もできますし、**Advanced** をクリックして Advanced Alert Behavior Wizard を開き、変更することもできます。このウィザードでは、このシグニチャのアラートを処理する方法を設定できます。

ステップ 6　**Finish** をクリックします。

シグニチャ エンジンを使用しない方法

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　Welcome ウィンドウで **No** を選択します。

ステップ 2　使用するプロトコルを選択します。

- IP：ステップ 4 に進みます。
- ICMP：ステップ 3 に進みます。
- UDP：ステップ 3 に進みます。
- TCP：ステップ 3 に進みます。

ステップ 3　ICMP プロトコルと 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 4　シグニチャの識別子を割り当てます。

- シグニチャ ID
- サブシグニチャ ID
- シグニチャ名
- アラートの注釈（オプション）
- ユーザ コメント（オプション）

ステップ 5　エンジン固有のパラメータを割り当てます。

パラメータはシグニチャ エンジンごとに異なりますが、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 1 つあります。

ステップ 6　アラート応答を割り当てます。

- シグニチャ忠実度評価
- アラートの重大度

ステップ 7　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もできますし、**Advanced** をクリックして Advanced Alert Behavior Wizard を開き、変更することもできます。このウィザードでは、このシグニチャのアラートを処理する方法を設定できます。

ステップ 8　**Finish** をクリックします。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

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。

フィールド定義

次の項では、Custom Signature Wizard のフィールド定義をウィンドウごとに説明します。取り上げる事項は次のとおりです。

- Welcome フィールド定義（P.6-5）
- Protocol Type フィールド定義（P.6-6）
- Signature Identification フィールド定義（P.6-7）
- Atomic IP Engine Parameters フィールド定義（P.6-7）
- Service HTTP Engine Parameters フィールド定義（P.6-8）
- Service MSRPC Engine Parameters フィールド定義（P.6-9）
- Service RPC Engine Parameters フィールド定義（P.6-10）
- State Engine Parameters フィールド定義（P.6-11）
- String ICMP Engine Parameters フィールド定義（P.6-11）
- String TCP Engine Parameters フィールド定義（P.6-12）
- String UDP Engine Parameters フィールド定義（P.6-13）
- Sweep Engine Parameters フィールド定義（P.6-14）
- ICMP Traffic Type フィールド定義（P.6-15）
- UDP Traffic Type フィールド定義（P.6-15）
- TCP Traffic Type フィールド定義（P.6-15）
- UDP Sweep Type フィールド定義（P.6-16）
- TCP Sweep Type フィールド定義（P.6-16）
- Service Type フィールド定義（P.6-16）
- Inspect Data フィールド定義（P.6-17）
- Alert Response フィールド定義（P.6-17）
- Alert Behavior フィールド定義（P.6-18）
- Advanced Alert Behavior ウィザード（P.6-18）

Welcome フィールド定義

Custom Signature Wizard の Welcome ウィンドウには、次のフィールドとボタンがあります。

フィールドの説明：

- **Yes**：**Select Engine** フィールドをアクティブにし、リストからシグニチャ エンジンを選択します。

- **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。シグニチャの作成にどのシグニチャ エンジンを使用するかが不明な場合は、**Yes** をクリックし、リストからエンジンタイプを選択します。
  - **Atomic IP**：Atomic IP シグニチャを作成します。
  - **Service HTTP**：HTTP トラフィック用のシグニチャを作成します。
  - **Service MSRPC**：MSRPC トラフィック用のシグニチャを作成します。
  - **Service RPC**：RPC トラフィック用のシグニチャを作成します。
  - **State SMTP**：SMTP トラフィック用のシグニチャを作成します。
  - **String ICMP**：ICMP 文字列用のシグニチャを作成します。
  - **String TCP**：TCP 文字列用のシグニチャを作成します。
  - **String UDP**：UDP 文字列用のシグニチャを作成します。
  - **Sweep**：スイープ用のシグニチャを作成します。
- **No**：Custom Signature Wizard のエンジン選択画面を継続します。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Protocol Type フィールド定義

特定のプロトコルを使用した悪意のある動作を検出するシグニチャを定義できます。シグニチャによるデコードと検査が可能なプロトコルは、次のとおりです。

- IP
- ICMP
- UDP
- TCP

Custom Signature Wizard の Protocol Type ウィンドウには、次のフィールドとボタンがあります。

フィールドの説明：

- **IP**：IP トラフィックのデコードと検査を行うシグニチャを作成します。
- **ICMP**：ICMP トラフィックのデコードと検査を行うシグニチャを作成します。
- **UDP**：UDP トラフィックのデコードと検査を行うシグニチャを作成します。
- **TCP**：TCP トラフィックのデコードと検査を行うシグニチャを作成します。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Signature Identification フィールド定義

Custom Signature Wizard の Signature Identification ウィンドウには、次のフィールドとボタンがあります。

フィールドの説明：

- **Signature ID**：このシグニチャに割り当てられた固有の数値を示します。

  シグニチャ ID を使用すると、センサーが特定のシグニチャを識別できます。アラートが生成されると、シグニチャ ID は 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固有の数値を示します。

  サブシグニチャ ID は、広い範囲のシグニチャのバージョンをより細かく示すために使用します。有効な値は 0 ～ 255 です。アラートが生成されると、サブシグニチャは 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。

  アラートが生成されると、Event Viewer に報告されます。
- **Alert Notes**：（オプション）このシグニチャが反応した場合、アラートに関連付けられているテキストを指定します。

  アラートが生成されると、Event Viewer に報告されます。
- **User Comments**：（オプション）このシグニチャに関して、シグニチャ パラメータといっしょに保存する注釈などのコメントを指定します。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Atomic IP Engine Parameters フィールド定義

Custom Signature Wizard の Atomic IP Engine Parameters ウィンドウには、次のフィールドとボタンがあります。これらのオプションを使用すると、一般的なタイプまたは特定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。

フィールドの説明：

- **Event Action**：シグニチャが検出された場合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** キーを押したまま選択します。

- **Fragment Status**：フラグメント化されている、またはフラグメント化されていないトラフィックを検査する場合に指定します。
- **Specify Layer 4 Protocol**：（オプション）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します。

  Yes を選択した場合、次のプロトコルから選択できます。

  - **ICMP Protocol**：ICMP のシーケンス、タイプ、コード、識別子、および合計の長さを指定します。

- **Other Protocols**：識別子を選択します。
- **TCP Protocol**：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、予約済みのアトリビュート、および送信元と宛先のポート範囲を設定します。
- **UDP Protocol**：有効な UDP 長、長さのミスマッチ、および送信元と宛先のポート範囲を指定します。

- **Specify Payload Inspection**：（オプション）次のペイロード検査オプションを指定します。
- **Specify IP Payload Length**：（オプション）ペイロード長を指定します。
- **Specify IP Header Length**：（オプション）IP ヘッダー長を指定します。
- **Specify IP Type of Service**：（オプション）サービスのタイプを指定します。
- **Specify IP Time-to-Live**：（オプション）パケットの存続可能時間を指定します。
- **Specify IP Version**：（オプション）IP バージョンを指定します。
- **Specify IP Identifier**：（オプション）IP 識別子を指定します。
- **Specify Total IP Length**：（オプション）IP の合計の長さを指定します。
- **Specify IP Option Inspection Options**：（オプション）IP 検査オプションを指定します。

  次からを選択します。
  - **IP Option**：照合する IP オプション コード。
  - **IP Option Abnormal Options**：オプションの不正形式リスト。
- **Specify IP Addr Options**：（オプション）次の IP アドレス オプションを指定します。
  - **Address with Localhost**：ローカル ホストのアドレスが送信元アドレスまたは宛先アドレスとして使用されているトラフィックを示します。
  - **IP Addresses**：送信元アドレスまたは宛先アドレスを指定します。
  - **RFC 1918 Address**：アドレスのタイプが RFC 1918 であることを示します。
  - **Src IP Equal Dst IP**：送信元アドレスと宛先アドレスが同一のトラフィックを示します。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Service HTTP Engine Parameters フィールド定義

Custom Signature Wizard の Service HTTP Engine Parameters ウィンドウには、次のフィールドとボタンがあります。これらのオプションを使用すると、一般的なタイプまたは特定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。

フィールドの説明：

- **Event Action**：シグニチャが検出された場合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。

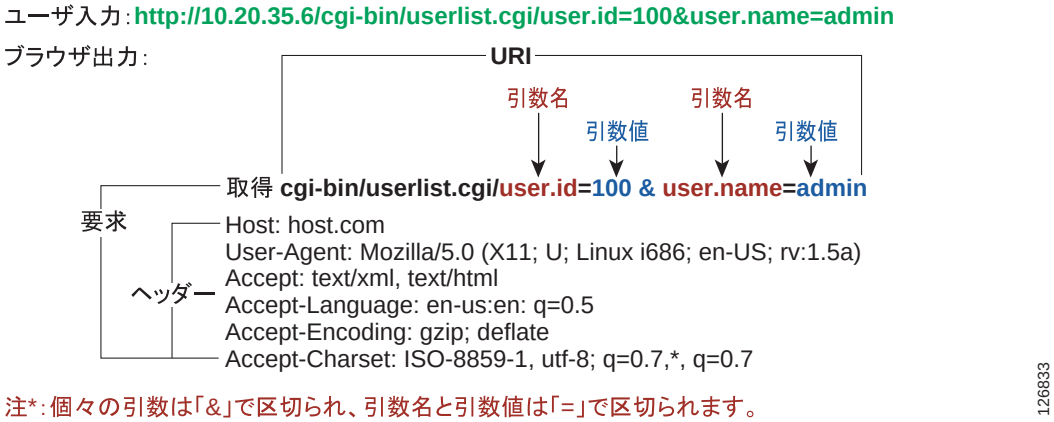
ヒント　複数のアクションを選択するには、**Ctrl** キーを押したまま選択します。

- **De Obfuscate**：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**：（オプション）URI、Arg、Header、および Request フィールドの最大の長さを指定します。

  次の図は、最大フィールド サイズを示しています。



- **Regex**：URI、Arg、Header、および Request Regex の正規表現を指定します。
- **Service Ports**：トラフィックが使用する特定のサービス ポートを指定します。

  値は、ポートのカンマ区切りのリストです。
- **Swap Attacker Victim**：このシグニチャが反応したときに、アラートで報告された送信元アドレスと宛先アドレスをスワップするかどうかを指定します。

  デフォルトは **No** です。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Service MSRPC Engine Parameters フィールド定義

Custom Signature Wizard の MSRPC Engine Parameters ウィンドウには、次のフィールドとボタンがあります。これらのオプションを使用すると、非常に汎用的または非常に特殊な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。

フィールドの説明：

- **Event Action**：シグニチャが検出された場合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** キーを押したまま選択します。

- **Specify Regex String**：（オプション）完全一致オフセットを指定します。これには最小および最大一致オフセット、Regex 文字列、最小一致の長さが含まれます。

- **Protocol**：TCP または UDP をプロトコルとして指定できます。
- **Specify Operation**：（オプション）操作を指定します。
- **Specify UUID**：（オプション）UUID を指定します。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Service RPC Engine Parameters フィールド定義

Custom Signature Wizard の Service RPC Engine Parameters ウィンドウには、次のフィールドとボタンがあります。これらのオプションを使用すると、一般的なタイプまたは特定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**：シグニチャが検出された場合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** キーを押したまま選択します。

- **Direction**：センサーがサービス ポートを宛先または送信元とするトラフィックを監視するかどうかを示します。

  デフォルトは **To Service** です。
- **Protocol**：TCP または UDP をプロトコルとして指定できます。
- **Service Ports**：ターゲット サービスが常駐できるポートまたはポート範囲を示します。

  有効な値は、ポートまたはポート範囲のカンマ区切りのリストです。
- **Specify Port Map Program**：シグニチャの対象ポート マッパーに送信されるプログラム番号を示します。

  有効な範囲は 0 ～ 9999999999 です。
- **Specify RPC Program**：シグニチャの対象 RPC プログラム番号を示します。

  有効な範囲は 0 ～ 1000000 です。
- **Specify Spool Src**：送信元アドレスが 127.0.0.1 に設定された場合、アラームを生成します。
- **Specify RPC Max Length**：RPC メッセージ全体の最大許容長。

  長さがこの値を超えている場合は、アラームが生成されます。有効な範囲は 0 ～ 65535 です。
- **Specify RPC Procedure**：シグニチャの対象 RPC プロシージャ番号を示します。

  有効な範囲は 0 ～ 1000000 です。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

State Engine Parameters フィールド定義

Custom Signature Wizard の State Engine Parameters ウィンドウには、次のフィールドとボタンがあります。これらのオプションを使用すると、一般的なタイプまたは特定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。

フィールドの説明：

- **Event Action**：シグニチャが検出された場合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** キーを押したまま選択します。

- **State Machine**：正規表現文字列の照合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。
- **Specify Min Match Length** : 照合の開始から終了までの間で、正規表現文字列が一致する必要のあるバイトの最小数を示します。

  有効な範囲は 0 ～ 65535 です。
- **Regex String**：状態遷移のトリガーとな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 サービスが常駐できるポートまたはポート範囲を示します。

  有効な値は、ポートまたはポート範囲のカンマ区切りのリストです。
- **Swap Attacker Victim**：このシグニチャが反応したときに、アラートで報告された送信元アドレスと宛先アドレスをスワップ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**：正規表現文字列が一致を報告する必要のある実際のストリーム オフセットをバイト単位で示します。

  有効な範囲は 0 ～ 65535 です。

  No を選択すると、最小および最大一致オフセットを設定できます。

  有効な範囲は 1 ～ 65535 です。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

String ICMP Engine Parameters フィールド定義

Custom Signature Wizard の String ICMP Engine Parameters ウィンドウには、次のフィールドとボタンがあります。これらのオプションを使用すると、一般的なタイプまたは特定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。

フィールドの説明：

- **Event Action**：シグニチャが検出された場合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** キーを押したまま選択します。

- **Specify Min Match Length** : 照合の開始から終了までの間で、正規表現文字列が一致する必要のあるバイトの最小数を示します。

  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 ヘッダーの TYPE 値。

  有効範囲は 0 ～ 18 です。デフォルトは 0 ～ 18 です。
- **Swap Attacker Victim**：このシグニチャが反応したときに、アラートで報告された送信元アドレスと宛先アドレスをスワップ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**：正規表現文字列が一致を報告する必要のある実際のストリーム オフセットをバイト単位で示します。

  No を選択すると、最小および最大一致オフセットを設定できます。

  最大一致オフセットの有効範囲は 1 ～ 65535 です。最小一致オフセットの有効範囲は 0 ～ 65535 です。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

String TCP Engine Parameters フィールド定義

Custom Signature Wizard の String TCP Engine Parameters ウィンドウには、次のフィールドとボタンがあります。これらのオプションを使用すると、非常に汎用的または非常に特殊な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。

フィールドの説明：

- **Event Action**：シグニチャが検出された場合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** キーを押したまま選択します。

- **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** : 照合の開始から終了までの間で、正規表現文字列が一致する必要のあるバイトの最小数を示します。

  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 サービスが常駐できるポートまたはポート範囲を示します。

  有効な値は、ポートまたはポート範囲のカンマ区切りのリストです。
- **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必要のある実際のストリーム オフセットをバイト単位で示します。

  No を選択すると、最小および最大一致オフセットを設定できます。

  最大一致オフセットの有効範囲は 1 ～ 65535 です。最小一致オフセットの有効範囲は 0 ～ 65535 です。
- **Swap Attacker Victim**：このシグニチャが反応したときに、アラートで報告された送信元アドレスと宛先アドレスをスワップするかどうかを指定します。

  デフォルトは **No** です。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

String UDP Engine Parameters フィールド定義

Custom Signature Wizard の String UDP Engine Parameters ウィンドウには、次のフィールドとボタンがあります。これらのオプションを使用すると、一般的なタイプまたは特定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。

フィールドの説明：

- **Event Action**：シグニチャが検出された場合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** キーを押したまま選択します。

- **Specify Min Match Length** : 照合の開始から終了までの間で、正規表現文字列が一致する必要のあるバイトの最小数を示します。

  有効な範囲は 0 ～ 65535 です。
- **Specify Exact Match Offset**：正規表現文字列が一致を報告する必要のある実際のストリーム オフセットをバイト単位で示します。

  有効な範囲は 0 ～ 65535 です。

  No を選択すると、最小および最大一致オフセットを設定できます。

  有効な範囲は 1 ～ 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 サービスが常駐できるポートまたはポート範囲を示します。

  有効な値は、ポートまたはポート範囲のカンマ区切りのリストです。
- **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**：このシグニチャが反応したときに、アラートで報告された送信元アドレスと宛先アドレスをスワップするかどうかを指定します。

  デフォルトは **No** です。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Sweep Engine Parameters フィールド定義

Custom Signature Wizard の Sweep Engine Parameters ウィンドウには、次のフィールドとボタンがあります。これらのオプションを使用すると、一般的なタイプまたは特定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。

フィールドの説明：

- **Event Action**：シグニチャが検出された場合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** キーを押したまま選択します。

- **Unique**：一意なホスト接続数のしきい値を示します。

  インターバル中に一意のホスト接続数を超えた場合には、アラームが生成されます。
- **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、攻撃者アドレス、攻撃者アドレスと被害先ポート、攻撃者と被害者のアドレスのいずれか 1 つのストレージ キーを選択します。
  - **TCP**：サプレス リバース、インバーテッド 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、またはポート範囲を指定します。
  - **UDP**：ストレージ キーを選択するか、またはポート範囲を指定します。
- **Swap Attacker Victim**：このシグニチャが反応したときに、アラートで報告された送信元アドレスと宛先アドレスをスワップするかどうかを指定します。

  デフォルトは **No** です。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

ICMP Traffic Type フィールド定義

Custom Signature Wizard の ICMP Traffic Type ウィンドウには、次のフィールドとボタンがあります。

フィールドの説明：

- **Single Packet**：単一パケットを検査して攻撃を探すためのシグニチャを作成していることを示します。
- **Sweeps**：スイープ攻撃を検出するシグニチャを作成していることを示します。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

UDP Traffic Type フィールド定義

Custom Signature Wizard の UDP Traffic Type ウィンドウには、次のフィールドとボタンがあります。

フィールドの説明：

- **Single Packet**：単一パケットを検査して攻撃を探すためのシグニチャを作成していることを示します。
- **Sweeps**：スイープ攻撃を検出するシグニチャを作成していることを示します。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

TCP Traffic Type フィールド定義

Custom Signature Wizard の TCP Traffic Type ウィンドウには、次のフィールドとボタンがあります。

フィールドの説明：

- **Single Packet**：単一パケットを検査して攻撃を探すためのシグニチャを作成していることを示します。
- **Single TCP Connection**：単一の TCP 接続を検査して攻撃を検出するためのシグニチャを作成するように指定します。
- **Multiple Connections**：複数の接続を検査して攻撃を検出するためのシグニチャを作成するように指定します。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

UDP Sweep Type フィールド定義

Custom Signature Wizard の UDP Sweep Type ウィンドウには、次のフィールドとボタンがあります。

フィールドの説明：

- **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**：ホストでオープン ポートを検索するスイープを示します。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

TCP Sweep Type フィールド定義

Custom Signature Wizard の TCP Sweep Type ウィンドウには、次のフィールドとボタンがあります。

フィールドの説明：

- **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**：ホストでオープン ポートを検索するスイープを示します。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Service Type フィールド定義

Custom Signature Wizard の Service Type ウィンドウには、次のフィールドとボタンがあります。

フィールドの説明：

- **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ための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ための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ための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ためのシグニチャを作成するように指定します。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。

- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Inspect Data フィールド定義

Custom Signature Wizard の Inspect Data ウィンドウには、次のフィールドとボタンがあります。

フィールドの説明：

- **Header Data Only**：センサーが検査するパケットの一部としてヘッダーを指定します。
- **Payload Data Only**：センサーが検査するパケットの一部としてペイロードを指定します。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Alert Response フィールド定義

Custom Signature Wizard の Alert Response ウィンドウには、次のフィールドとボタンがあります。

フィールドの説明：

- **Signature Fidelity Rating**：対象とする特定の情報がない場合にこのシグニチャをどの程度忠実に実行するかに関連付ける重み。

  SFR は、シグニチャ作成者によってシグニチャごとに計算されます。きわめて具体的なルール（特定の Regex など）で記述されたシグニチャは、汎用的なルールで記述されたシグニチャより高い SFR を持ちます。
- **Severity of the Alert**：アラートが報告される重大度。

  次のオプションから選択できます。
  - **High**：最も重大なセキュリティ 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**：ネットワーク アクティビティを示します。セキュリティ アラートではありません。

ボタンの機能：

- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Alert Behavior フィールド定義

Custom Signature Wizard の Alert Behavior ウィンドウには、次のボタンがあります。

- **Advanced**：Advanced Alert Behavior ウィンドウを開きます。このウィンドウでは、デフォルトの動作を変更し、センサーがアラートを送信する頻度を設定できます。
- **Back**：Custom Signature Wizard の前のウィンドウに戻ります。
- **Next**：Custom Signature Wizard の次のウィンドウに進みます。
- **Finish**：Custom Signature Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Custom Signature Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Advanced Alert Behavior ウィザード

次の項では、Advanced Alert Behavior ウィザードのフィールド定義について説明します。取り上げる事項は次のとおりです。

- Event Count and Interval フィールド定義（P.6-18）
- Alert Summarization フィールド定義（P.6-19）
- Alert Dynamic Response Summary フィールド定義（P.6-19）
- Alert Dynamic Response Fire All フィールド定義（P.6-20）
- Alert Dynamic Response Fire Once フィールド定義（P.6-20）
- Global Summarization フィールド定義（P.6-21）

Event Count and Interval フィールド定義

Advanced Alert Behavior ウィザードの Event Count and Interval ウィンドウには、次のフィールドとボタンがあります。

フィールドの説明：

- **Event Count**：このシグニチャのアラートを送信する前に、センサーが受信すべき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アトリビュートを示します。

  たとえば、同一の攻撃者からの攻撃かどうかに基づいてイベントをセンサーで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**：センサーがレート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** に 500 イベントを設定し、**Event Interval** に 30 秒を設定すると、センサーは、30 秒以内に 500 イベントを受信した場合にアラートを送信します。
- **Event Interval (seconds)**：センサーがレートに基づいてイベントをカウントする時間間隔を示します。

ボタンの機能：

- **Back**：Alert Behavior Wizard の前のウィンドウに戻ります。
- **Next**：Alert Behavior Wizard の次のウィンドウに進みます。
- **Finish**：Alert Behavior Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Alert Behavior Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Alert Summarization フィールド定義

Advanced Alert Behavior ウィザードの Alert Summarization ウィンドウには、次のフィールドとボタンがあります。

フィールドの説明：

- **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、センサーが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ボリュームを動的に調整できるようにするため、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ときに、センサーが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ボリュームを動的に調整できるようにするため、追加のしきい値を指定できます。
- **Send Summary Alerts**：シグニチャが反応するたびにアラートを送信するのではなく、センサーがこのシグニチャのサマリー アラートだけ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ボリュームを動的に調整できるようにするため、追加のしきい値を指定できます。
- **Send Global Summary Alerts**：シグニチャがアドレス セットで初めて反応したときにアラートをセンサーが送信し、その後は所定の時間間隔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を示すグローバル サマリー アラートだけを送信するように指定します。

ボタンの機能：

- **Back**：Alert Behavior Wizard の前のウィンドウに戻ります。
- **Next**：Alert Behavior Wizard の次のウィンドウに進みます。
- **Finish**：Alert Behavior Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Alert Behavior Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Alert Dynamic Response Summary フィールド定義

Advanced Alert Behavior ウィザードの Alert Dynamic Response Summary ウィンドウには、次のフィールドとボタンがあります。

フィールドの説明：

- **Summary Interval (seconds)**：センサーが要約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**：カウント イベントに使用するアトリビュートを示します。

  たとえば、同一の攻撃者からの攻撃かどうかに基づいてイベントをセンサーで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**：センサーが動的にグローバル サマリー モードに入るようにします。
- **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べき最小のヒット数を示します。

  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、センサーは単一のサマリー 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。指定間隔内に率がしきい値を下回ると、元のアラート動作に戻ります。

ボタンの機能：

- **Back**：Alert Behavior Wizard の前のウィンドウに戻ります。

- **Next**：Alert Behavior Wizard の次のウィンドウに進みます。
- **Finish**：Alert Behavior Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Alert Behavior Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Alert Dynamic Response Fire All フィールド定義

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、次のフィールドとボタンがあります。

フィールドの説明：

- **Use Dynamic Summarization**：設定するサマリー パラメータに基づいて、センサーが送信するアラートのボリュームを動的に調整するようにします。
- **Summary Threshold**：このシグニチャのサマリー アラートを送信する前に、センサーが受信すべき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ように指定し、時間間隔に使用する秒数を示します。
- **Summary Key**：カウント イベントに使用するアトリビュートを示します。

  たとえば、同一の攻撃者からの攻撃かどうかに基づいてイベントをセンサーでカウントする場合は、**Summary Key** として **Attacker Address** を選択します。
- **Specify Global Summary Threshold：**センサーが動的にグローバル サマリー モードに入るようにします。

  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。
- **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べき最小のヒット数を示します。

ボタンの機能：

- **Back**：Alert Behavior Wizard の前のウィンドウに戻ります。
- **Next**：Alert Behavior Wizard の次のウィンドウに進みます。
- **Finish**：Alert Behavior Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Alert Behavior Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Alert Dynamic Response Fire Once フィールド定義

Alert the First Time the Signature Fires を選択した場合、Alert Behavior ウィザードの Alert Dynamic Response ウィンドウには、次のフィールドとボタンがあります。

フィールドの説明：

- **Summary Key**：カウント イベントに使用するアトリビュートを示します。

  たとえば、同一の攻撃者からの攻撃かどうかに基づいてイベントをセンサーで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**：センサーが動的にグローバル サマリー モードに入るようにします。

- **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べき最小のヒット数を示します。

  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が初めて反応したときに単一のにアラートを送信するのではなく、アラートを 1 つのグローバル サマリー アラートにまとめて送信します。指定間隔内に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)** : センサーが要約のためにイベントをカウントする時間間隔を示します。

ボタンの機能：

- **Back**：Alert Behavior Wizard の前のウィンドウに戻ります。
- **Next**：Alert Behavior Wizard の次のウィンドウに進みます。
- **Finish**：Alert Behavior Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Alert Behavior Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

Global Summarization フィールド定義

Advanced Alert Behavior ウィザードの Global Summarization ウィンドウには、次のフィールドとボタンがあります。

フィールドの説明：

- **Global Summary Interval (seconds)** : センサーが要約のためにイベントをカウントする時間間隔を示します。

ボタンの機能：

- **Back**：Alert Behavior Wizard の前のウィンドウに戻ります。
- **Next**：Alert Behavior Wizard の次のウィンドウに進みます。
- **Finish**：Alert Behavior Wizard を終了し、作成したシグニチャを保存します。
- **Cancel**：Alert Behavior Wizard を終了します。
- **Help**：この機能のヘルプ トピックが表示されます。

カスタム シグニチャの作成

この項では、カスタム シグニチャの例を示します。取り上げる事項は次のとおりです。

- Custom Signature Wizard でサポートされていないシグニチャ エンジン（P.6-22）
- マスター カスタム シグニチャの手順（P.6-23）
- String TCP シグニチャの例（P.6-29）
- Service HTTP シグニチャの例（P.6-34）

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

IPS 5.1 の Custom Signature Wizard では、次のシグニチャ エンジンを使用してカスタム シグニチャを作成する方法はサポートされていません。

- AIC FTP
- AIC HTTP
- Atomic ARP
- Flood Host
- Flood Net
- Meta
- Multi String
- Normalizer
- Service DNS
- Service FTP
- Service Generic
- Service H224
- Service IDENT
- Service MSSQL
- Service NTP
- Service SMB
- Service SNMP
- Service SSH
- Sweep TCP Other

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、Configuration > Signature Configuration > Clone をクリックしてエンジンから既存のシグニチャを複製します。詳細については、P.5-19 の「シグニチャの複製」を参照してください。

これらのシグニチャ エンジンを使用し、カスタム シグニチャを CLI によって作成する方法の詳細については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』を参照してください。

マスター カスタム シグニチャの手順

Custom Signature Wizard は、カスタム シグニチャを設定する手順を順を追って示します。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」を参照してください。

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　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Signature Definition > Custom Signature Wizard** をクリックします。

Start ウィンドウが表示されます。

注意　カスタム シグニチャがセンサーのパフォーマンスに影響する可能性があります。シグニチャの影響全体を判別するため、ネットワークのベースライン センサーのパフォーマンスに対してカスタム シグニチャのテストを実行します。

ステップ 3　**Start the Wizard** をクリックします。

Welcome ウィンドウが表示されます。

ステップ 4　新しい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、**Select Engine** リストからシグニチャ エンジンを選択し、**Next** をクリックします。ステップ 13 に進みます。

使用するエンジンが不明の場合は、**No** オプション ボタンをクリックし、**Next** をクリックします。

Protocol Type ウィンドウが表示されます。

ステップ 5　このシグニチャによる検査の対象となるトラフィック タイプに最適なプロトコルを次から選択し、**Next** をクリックします。

- **IP**（IP を選択した場合は ステップ 13 に進みます）。
- **ICMP**（ICMP を選択した場合は ステップ 6 に進みます）。
- **UDP**（UDP を選択した場合は ステップ 7 に進みます）。
- **TCP**（TCP を選択した場合は ステップ 9 に進みます）。

ステップ 6　ICMP Traffic Type ウィンドウで、次のいずれかのオプションを選択し、**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、単一パケットの攻撃を検査するシグニチャを作成します。

  ステップ 12 に進みます。
- **Sweeps**

  新しいシグニチャにスイープ 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ます。

  ステップ 13 に進みます。

ステップ 7　UDP Traffic Type ウィンドウで、次のいずれかのオプションを選択し、**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、単一パケットの攻撃を検査するシグニチャを作成します。

  ステップ 12 に進みます。
- **Sweeps**

  シグニチャにスイープ 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ます。

  ステップ 8 に進みます。

ステップ 8　UDP Sweep Type ウィンドウで、次のいずれかのオプションを選択し、**Next** をクリックします。

- **Host Sweep**

  ホストでオープン ポートを探すためにスイープを使用するシグニチャを作成しています。スイープ エンジンを使用して新しいシグニチャを作成し、ストレージ キーは Axxx に設定されます。

  ステップ 13 に進みます。
- **Port Sweep**

  ネットワークでホストを探すためにスイープを使用するシグニチャを作成しています。スイープ エンジンを使用して新しいシグニチャを作成し、ストレージ キーは AxBx に設定されます。

  ステップ 13 に進みます。

ステップ 9　TCP Traffic Type ウィンドウで、次のいずれかのオプションを選択し、**Next** をクリックします。

- **Single Packet**

  単一のパケットを検査して攻撃を検出するためのシグニチャを作成します。Atomic IP エンジンを使用してシグニチャを作成します。

  ステップ 13 に進みます。
- **Single TCP Connection**

  TCP 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。

  ステップ 10 に進みます。
- **Multiple Connections**

  複数の接続を検査して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 11 に進みます。

ステップ 10　Service Type ウィンドウで、次のいずれかのオプションを選択し、**Next** をクリックします。

- **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。Service HTTP エンジンを使用してシグニチャを作成します。
- **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。SMTP エンジンを使用してシグニチャを作成します。
- **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。Service RPC エンジンを使用してシグニチャを作成します。

- **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。Service MSRPC エンジンを使用してシグニチャを作成します。

- **Other**

  HTTP、SMTP、RPC 以外のサービスを使用する攻撃を検出するためのシグニチャを作成します。String TCP エンジンを使用してシグニチャを作成します。

ステップ 13 に進みます。

ステップ 11　TCP Sweep Type ウィンドウで、次のいずれかのオプションを選択し、**Next** をクリックします。

- **Host Sweep**

  ホストでオープン ポートを探すためにスイープを使用するシグニチャを作成しています。スイープ エンジンを使用してシグニチャを作成し、ストレージ キーは Axxx に設定されます。

- **Port Sweep**

  ネットワークでホストを探すためにスイープを使用するシグニチャを作成しています。スイープ エンジンを使用して新しいシグニチャを作成し、ストレージ キーは AxBx に設定されます。

ステップ 13 に進みます。

ステップ 12　単一パケットの場合、次のいずれかの検査オプションを選択します。

- **Header Data Only**

  センサーが検査するパケットの一部としてヘッダーを指定します。

- **Payload Data Only**

  センサーが検査するパケットの一部としてペイロードを指定します。

ステップ 13 に進みます。

ステップ 13　このシグニチャを固有に識別するアトリビュートを指定するには、次の必須値を入力してから、**Next** をクリックします。

a. **Signature ID** フィールドに数値を入力します。

カスタム シグニチャの範囲は 60000 ～ 65000 です。

b. **SubSignature ID** フィールドに数値を入力します。

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 を設定します。

c. **Signature Name** フィールドに名前を入力します。

Signature Name フィールドに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 とサブシグニチャ ID とともにイベント ビューアに報告されます。

d. （オプション）**Alert Notes** フィールドにテキストを入力します。

このシグニチャのアラームにテキストが含まれるように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. （オプション）**User Comments** フィールドに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 14 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。

ヒント + アイコンは、このシグニチャに使用可能なパラメータがあることを示しています。+ アイコンをクリックすると、セクションが展開され、残りのパラメータが表示されます。

ヒント 緑のアイコンは、パラメータがデフォルト値を使用していることを示しています。緑色のアイコンをクリックしてこのパラメータのフィールドをアクティブにし、値を編集します。

ステップ 15 次のアラート応答オプションを指定します。

a. **Signature Fidelity Rating** フィールドで値を指定します。

SFR は、シグニチャに対する信頼度を示す 0 ～ 100 の有効な値であり、最も高い信頼は 100 です。

b. センサーがアラートを送信したときにイベント ビューアが報告する重大度を選択します。

- **High**
- **Informational**
- **Low**
- **Medium**

ステップ 16 デフォルト アラート動作を変更するには、**Advanced** をクリックします。

Advanced Alert Behavior ウィザードの Event Count and Interval ウィンドウが表示されます。

（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、IDS 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 IPS 対抗ツールに対応させる場合があります。

ステップ 17 イベント カウント、キー、間隔を設定します。

a. イベント カウントの値を **Event Count** フィールドに入力します。

これは、このシグニチャのアラートを送信する前にセンサーが受信すべき最小ヒット数です。

b. **Event Count Key** として使用するアトリビュートを選択します。

たとえば、同一の攻撃者からの攻撃かどうかに基づいてイベントをセンサーでカウントする場合は、**Event Count Key** として **Attacker address** 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** を選択してから、間隔に使用する秒数を指定します。

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 18 アラートの量を制御し、センサーがアラートを要約する方法を設定するには、次のいずれかのオプションを選択します。

- **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がアラートを送信することを指定します。その後、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ため、追加のしきい値を指定できます。

  ステップ 17a に進みます。

- **Alert the First Time the Signature Fires**

  シグニチャが悪意のあるトラフィックを初めて検出したときにセンサーがアラートを送信することを指定します。その後、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ため、追加のしきい値を指定できます。

  ステップ 17b に進みます。

- **Send Summary Alerts**

  センサーが、シグニチャが反応す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 アラートだけを送信することを指定します。その後、追加のしきい値を指定して、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します。

  ステップ 17c に進みます。

- **Send Global Summary Alerts**

  センサーが、シグニチャがアドレス セットで初めて反応したときにアラートを送信し、その後は所定の時間間隔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を示すグローバル サマリー アラートだけを送信することを指定します。

  ステップ 17d に進みます。

a. Alert Every Time the Signature Fires を設定するには、次のオプションのいずれかを選択します。

- **Summary Key**

  カウント イベントに使用するアトリビュートを示します。

  たとえば、同一の攻撃者からの攻撃かどうかに基づいてイベントをセンサーでカウントする場合は、サマリー キーとして **Attacker Address** を選択します。

- **Use Dynamic Summarization**

  設定するサマリー パラメータに基づいて、センサーが送信するアラートのボリュームを動的に調整するようにします。

- **Summary Threshold**

  このシグニチャのサマリー アラートを送信する前にセンサーが受信すべき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 Global Summary Threshold**

  センサーが動的にグローバル要約モードに入るようにします。

- **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べき最小ヒット数を示します。

b. Alert the First Time the Signature Fires を設定するには、次のオプションのいずれかを選択します。

- **Summary Key**

  カウント イベントに使用するアトリビュートを示します。

  たとえば、同一の攻撃者からの攻撃かどうかに基づいてイベントをセンサーでカウントする場合は、サマリー キーとして **Attacker Address** を選択します。

- **Use Dynamic Global Summarization**

  センサーが動的にグローバル要約モードに入るようにします。

- **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べき最小ヒット数を示します。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が初めて反応したときに単一のにアラートを送信するのではなく、アラートを 1 つのグローバル サマリー アラートにまとめて送信します。指定間隔内に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)**

  センサーが要約のイベントをカウントする時間間隔を示します。

c. Send Summary Alerts を設定するには、次のオプションのいずれかを選択します。

- **Summary Interval (seconds)**

  センサーが要約のイベントをカウントする時間間隔を示します。

- **Summary Key**

  カウント イベントに使用するアトリビュートを示します。

  たとえば、同一の攻撃者からの攻撃かどうかに基づいてイベントをセンサーでカウントする場合は、サマリー キーとして **Attacker Address** を選択します。

- **Use Dynamic Global Summarization**

  センサーが動的にグローバル要約モードに入るようにします。

- **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べき最小ヒット数を示します。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、センサーは単一のサマリー 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 Summarization を設定するには、センサーが要約のためにイベントをカウントする時間間隔を指定します。

e. **Next** をクリックして続行します。

ステップ 19 **Finish** をクリックし、変更を保存します。

Create Custom Signature ダイアログボックスが表示されます。

ステップ 20 **Yes** をクリックして、カスタム シグニチャを作成します。

ヒント 変更を元に戻すには、**Cancel** をクリックします。

作成したシグニチャをイネーブルにして、シグニチャのリストに追加します。

String TCP シグニチャの例

String エンジンは、ICMP、TCP、および UDP の各プロトコル用の汎用のパターン マッチング検査エンジンです。String エンジンは、複数のパターンを結合して単一のパターン マッチング テーブルにし、単一のデータ検索を可能にする、正規表現エンジンを使用します。

String ICMP、String TCP、および String UDP の 3 つの String エンジンがあります。

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

（注） 次の手順は、カスタム String ICMP シグニチャと UDP シグニチャを作成する場合にも適用されます。

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　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Signature Definition > Custom Signature Wizard** をクリックします。

Start ウィンドウが表示されます。

注意　カスタム シグニチャがセンサーのパフォーマンスに影響する可能性があります。シグニチャの影響全体を判別するため、ネットワークのベースライン センサーのパフォーマンスに対してカスタム シグニチャのテストを実行します。

ステップ 3　**Start the Wizard** をクリックします。

Welcome ウィンドウが表示されます。

ステップ 4　**Yes** オプション ボタンをクリックし、**String TCP** を **Select Engine** リストから選択し、**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 5　このシグニチャを固有に識別するアトリビュートを指定するには、次の必須値を入力してから、**Next** をクリックします。

a. **Signature ID** フィールドに数値を入力します。
   カスタム シグニチャの範囲は 60000 ～ 65000 です。
b. **SubSignature ID** フィールドに数値を入力します。
   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 を設定します。
c. **Signature Name** フィールドに名前を入力します。

Signature Name フィールドに、デフォルトの名前である 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 とサブシグニチャ ID とともに Event Viewer に報告されます。

d. （オプション）**Alert Notes** フィールドにテキストを入力します。

このシグニチャのアラームにテキストが含まれるように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. （オプション）**User Comments** フィールドに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。

ヒント　+ アイコンは、このパラメータで使用可能なオプションがあることを示しています。+ アイコンをクリックすると、セクションが展開され、残りのパラメータが表示されます。

ヒント　緑のアイコンは、パラメータがデフォルト値を使用していることを示しています。緑のアイコンをクリックすると赤に変わり、値を編集できるようにパラメータ フィールドがアクティブになります。

ステップ 6　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、より多く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** キーを押したまま選択します。

ステップ 7　**Direction** の横にある緑色のアイコンをクリックし、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 ポートに向かうトラフィック。
- **To Service**：クライアント ポートからサービス ポートに向かうトラフィック。

ステップ 8　**Regex String** フィールドで、シグニチャが TCP パケットに対して検査する文字列を指定します。

ステップ 9　**Service Ports** フィールドに、ポート（23 など）を指定します。

Service Ports 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（オプション）このシグニチャに次のオプション パラメータを設定できます。

- **Specify Exact Match Offset**：完全一致オフセットをイネーブルにします。これは、一致を有効にするために正規表現文字列が報告する必要のある実際のストリーム オフセットです（0 ～ 65535）。
- **Specify Min Match Length**：最小一致の長さをイネーブルにします。これは、正規表現文字列が一致する必要のある最小バイト数です（0 ～ 65535）。
- **Strip Telnet Options**：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します。
- **Swap Attacker Victim**：アドレス（およびポート）の送信元と宛先をアラート メッセージでスワップします。

ステップ 11 **Next** をクリックします。

Alert Response ウィンドウが表示されます。

ステップ 12 必要に応じて、次のデフォルトのアラート応答オプションを変更します。

a. **Signature Fidelity Rating** フィールドで値を指定します。

SFR は、シグニチャに対する信頼度を示す 0 ～ 100 の有効な値であり、最も高い信頼は 100 です。デフォルトは 75 です。

b. センサーがアラートを送信したときにイベント　ビューアが報告する重大度を選択します。デフォルトは Medium です。

- **High**
- **Informational**
- **Low**
- **Medium**

ステップ 13 **Next** をクリックします。

Alert Behavior ウィンドウが表示されます。

ステップ 14 デフォルト アラート動作を変更するには、**Advanced** をクリックします。

Advanced Alert Behavior ウィザードの Event Count and Interval ウィンドウが表示されます。デフォルト アラート動作を変更する場合は、ステップ 15 ～ 21 を実行します。変更しない場合は、**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。

（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、IDS 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 IPS 対抗ツールに対応させる場合があります。

ステップ 15 イベント カウント、キー、間隔を設定します。

a. イベント カウントの値を **Event Count** フィールドに入力します。

これは、このシグニチャのアラートを送信する前にセンサーが受信すべき最小ヒット数です。

b. Event Count Key として使用するアトリビュートを選択します。

たとえば、同一の攻撃者からの攻撃かどうかに基づいてイベントをセンサーでカウントする場合は、Event Count Key として **Attacker Address** 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** を選択してから、間隔に使用する秒数を指定します。

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 16 アラートの量を制御し、センサーがアラートを要約する方法を設定するには、次のいずれかのオプションを選択して、**Next** 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がアラートを送信することを指定します。その後、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ため、追加のしきい値を指定できます。

  ステップ 17a に進みます。

- **Alert the First Time the Signature Fires**

  シグニチャが悪意のあるトラフィックを初めて検出したときにセンサーがアラートを送信することを指定します。その後、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ため、追加のしきい値を指定できます。

  ステップ 17b に進みます。

- **Send Summary Alerts**

  センサーが、シグニチャが反応す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 アラートだけを送信することを指定します。その後、追加のしきい値を指定して、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します。

  ステップ 17c に進みます。

- **Send Global Summary Alerts**

  センサーが、シグニチャがアドレス セットで初めて反応したときにアラートを送信し、その後は所定の時間間隔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を示すグローバル サマリー アラートだけを送信することを指定します。

  ステップ 17d に進みます。

Alert Dynamic Response ウィンドウが表示されます。

ステップ 17 アラートの動的な応答を設定します。

a. Alert Every Time the Signature Fires を設定するには、次のオプションのいずれかを選択します。

- **Summary Key**

  カウント イベントに使用するアトリビュートを示します。

  たとえば、同一の攻撃者からの攻撃かどうかに基づいてイベントをセンサーでカウントする場合は、サマリー キーとして **Attacker Address** を選択します。

- **Use Dynamic Summarization**

  設定するサマリー パラメータに基づいて、センサーが送信するアラートのボリュームを動的に調整するようにします。

- **Summary Threshold**

  このシグニチャのサマリー アラートを送信する前にセンサーが受信すべき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 Global Summary Threshold**

  センサーが動的にグローバル要約モードに入るようにします。

- **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べき最小ヒット数を示します。

b. Alert the First Time the Signature Fires を設定するには、次のオプションのいずれかを選択します。

- **Summary Key**

  カウント イベントに使用するアトリビュートを示します。

  たとえば、同一の攻撃者からの攻撃かどうかに基づいてイベントをセンサーでカウントする場合は、サマリー キーとして **Attacker Address** を選択します。

- **Use Dynamic Global Summarization**

  センサーが動的にグローバル要約モードに入るようにします。

- **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べき最小ヒット数を示します。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が初めて反応したときに単一のにアラートを送信するのではなく、アラートを 1 つのグローバル サマリー アラートにまとめて送信します。指定間隔内に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)**

  センサーが要約のイベントをカウントする時間間隔を示します。

c. Send Summary Alerts を設定するには、次のオプションのいずれかを選択します。

- **Summary Interval (seconds)**

  センサーが要約のイベントをカウントする時間間隔を示します。

- **Summary Key**

  カウント イベントに使用するアトリビュートを示します。

  たとえば、同一の攻撃者からの攻撃かどうかに基づいてイベントをセンサーでカウントする場合は、サマリー キーとして **Attacker Address** を選択します。

- **Use Dynamic Global Summarization**

  センサーが動的にグローバル要約モードに入るようにします。

- **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べき最小ヒット数を示します。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、センサーは単一のサマリー 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 Summarization を設定するには、センサーが要約のためにイベントをカウントする時間間隔を指定します。

ステップ 18　**Finish** をクリックし、変更を保存します。

Alert Behavior ウィンドウが表示されます。

ステップ 19　**Finish** をクリックします。

Create Custom Signature ダイアログボックスが表示され、このカスタム シグニチャがセンサーに適用されます。

ステップ 20　**Yes** をクリックして、カスタム シグニチャを作成します。

ヒント　変更を元に戻すには、**Cancel** をクリックします。

作成したシグニチャをイネーブルにして、シグニチャのリストに追加します。

Service HTTP シグニチャの例

Service HTTP エンジンは、サービス固有で文字列ベースのパターン マッチング検査エンジンです。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です。また、これには最も長い事前処理時間が必要であり、検査を必要とする最大数のシグニチャを持つため、システムのパフォーマンス全体にとって重大となります。

Service HTTP エンジンは、複数のパターンを結合して単一のパターン マッチング テーブルにし、単一のデータ検索を可能にする、正規表現ライブラリを使用します。このエンジンは、Web サービスだけに送られるトラフィック、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。このエンジンの各シグニチャで、該当する個別の Web ポートを指定できます。

HTTP 解読は、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。これは、ASCII 正規化とも呼ばれます。

HTTP パケットを検査するには、まずデータを、ターゲット システムでデータの処理時に表示されるものと同じ表記に解読または正規化する必要があります。どのオペレーティング システムおよび Web サーバ バージョンがターゲットで動作しているかを認識している、カスタマイズされたデコード技術をホスト ターゲット タイプごとに用意することを推奨します。Service HTTP エンジンには、Microsoft IIS Web サーバに対するデフォルトの解読動作があります。

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。Service HTTP エンジンの詳細については、P.B-24 の「Service HTTP エンジン」を参照してください。

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　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Signature Definition > Custom Signature Wizard** をクリックします。

Start ウィンドウが表示されます。

注意　カスタム シグニチャがセンサーのパフォーマンスに影響する可能性があります。シグニチャの影響全体を判別するため、ネットワークのベースライン センサーのパフォーマンスに対してカスタム シグニチャのテストを実行します。

ステップ 3　**Start the Wizard** をクリックします。

Welcome ウィンドウが表示されます。

ステップ 4　**Yes** オプション ボタンをクリックし、**Service HTTP** を Select Engine リストから選択し、**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 5　このシグニチャを固有に識別するアトリビュートを指定するには、次の必須値を入力してから、**Next** をクリックします。

a. **Signature ID** フィールドに数値を入力します。

カスタム シグニチャの範囲は 60000 ～ 65000 です。

b. **SubSignature ID** フィールドに数値を入力します。

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 を設定します。

c. **Signature Name** フィールドに名前を入力します。

Signature Name フィールドに、デフォルトの名前である 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 とサブシグニチャ ID とともにイベント ビューアに報告されます。

d. （オプション）**Alert Notes** フィールドにテキストを入力します。

このシグニチャのアラームにテキストが含まれるように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. （オプション）**User Comments** フィールドに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。

ヒント　+ アイコンは、このパラメータで使用可能なオプションがあることを示しています。+ アイコンをクリックすると、セクションが展開され、残りのパラメータが表示されます。

ヒント　緑のアイコンは、パラメータがデフォルト値を使用していることを示しています。緑のアイコンをクリックすると赤に変わり、値を編集できるようにパラメータ フィールドがアクティブになります。

ステップ 6　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、より多く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** キーを押したまま選択します。

ステップ 7　**De Obfuscate** の横にある緑色のアイコンをクリックし、**Yes** を選択し、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 8　（オプション）Max Field Sizes で、最大フィールド サイズに対して次のオプション 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 9　Regex で、regex パラメータを設定します。

a. Specify URI Regex には **Yes** を選択します。

b. **URI Regex** フィールドで URI Regex を指定します（[Mm][Yy][Ff][Oo][Oo] など）。

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

ステップ 10　**Service Ports** フィールドで、ポートを指定します。たとえば、Web ポート変数の $WEBPORTS を使用します。

Service Ports 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 11　（オプション）**Swap Attacker Victim** の横にある緑色のアイコンをクリックし、**Yes** を選択し、送信元と宛先のアドレス（およびポート）をアラート メッセージでスワップするようにします。

ステップ 12　**Next** をクリックします。

Alert Response ウィンドウが表示されます。

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

a. **Signature Fidelity Rating** フィールドで値を指定します。

SFR は、シグニチャに対する信頼度を示す 0 ～ 100 の有効な値であり、最も高い信頼は 100 です。デフォルトは 75 です。

b. センサーがアラートを送信したときにイベント　ビューアが報告する重大度を選択します。デフォルトは Medium です。

- **High**
- **Informational**
- **Low**
- **Medium**

ステップ 14 **Next** をクリックします。

Alert Behavior ウィンドウが表示されます。

ステップ 15 デフォルト アラート動作を変更するには、**Advanced** をクリックします。

Advanced Alert Behavior ウィザードの Event Count and Interval ウィンドウが表示されます。デフォルト アラート動作を変更する場合は、ステップ 15 ～ 21 を実行します。変更しない場合は、**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。

（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、IDS 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 IPS 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、間隔を設定します。

a. イベント カウントの値を **Event Count** フィールドに入力します。

これは、このシグニチャのアラートを送信する前にセンサーが受信すべき最小ヒット数です。

b. Event Count Key として使用するアトリビュートを選択します。

たとえば、同一の攻撃者からの攻撃かどうかに基づいてイベントをセンサーでカウントする場合は、Event Count Key として **Attacker Address** 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** を選択してから、間隔に使用する秒数を指定します。

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、センサーがアラートを要約する方法を設定するには、次のいずれかのオプションを選択して、**Next** 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がアラートを送信することを指定します。その後、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ため、追加のしきい値を指定できます。

  ステップ 17a に進みます。

- **Alert the First Time the Signature Fires**

  シグニチャが悪意のあるトラフィックを初めて検出したときにセンサーがアラートを送信することを指定します。その後、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ため、追加のしきい値を指定できます。

  ステップ 17b に進みます。

- **Send Summary Alerts**

  センサーが、シグニチャが反応す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 アラートだけを送信することを指定します。その後、追加のしきい値を指定して、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します。

  ステップ 17c に進みます。

- **Send Global Summary Alerts**

  センサーが、シグニチャがアドレス セットで初めて反応したときにアラートを送信し、その後は所定の時間間隔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を示すグローバル サマリー アラートだけを送信することを指定します。

  ステップ 17d に進みます。

Alert Dynamic Response ウィンドウが表示されます。

ステップ 18 アラートの動的な応答を設定します。

a. Alert Every Time the Signature Fires を設定するには、次のオプションのいずれかを選択します。

- **Summary Key**

  カウント イベントに使用するアトリビュートを示します。

  たとえば、同一の攻撃者からの攻撃かどうかに基づいてイベントをセンサーでカウントする場合は、サマリー キーとして **Attacker Address** を選択します。

- **Use Dynamic Summarization**

  設定するサマリー パラメータに基づいて、センサーが送信するアラートのボリュームを動的に調整するようにします。

- **Summary Threshold**

  このシグニチャのサマリー アラートを送信する前にセンサーが受信すべき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 Global Summary Threshold**

  センサーが動的にグローバル要約モードに入るようにします。

- **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べき最小ヒット数を示します。

b. Alert the First Time the Signature Fires を設定するには、次のオプションのいずれかを選択します。

- **Summary Key**

  カウント イベントに使用するアトリビュートを示します。

  たとえば、同一の攻撃者からの攻撃かどうかに基づいてイベントをセンサーでカウントする場合は、サマリー キーとして **Attacker Address** を選択します。

- **Use Dynamic Global Summarization**

  センサーが動的にグローバル要約モードに入るようにします。

- **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べき最小ヒット数を示します。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が初めて反応したときに単一のにアラートを送信するのではなく、アラートを 1 つのグローバル サマリー アラートにまとめて送信します。指定間隔内に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)**

  センサーが要約のイベントをカウントする時間間隔を示します。

c. Send Summary Alerts を設定するには、次のオプションのいずれかを選択します。

- **Summary Interval (seconds)**

  センサーが要約のイベントをカウントする時間間隔を示します。

- **Summary Key**

  カウント イベントに使用するアトリビュートを示します。

  たとえば、同一の攻撃者からの攻撃かどうかに基づいてイベントをセンサーでカウントする場合は、サマリー キーとして **Attacker Address** を選択します。

- **Use Dynamic Global Summarization**

  センサーが動的にグローバル要約モードに入るようにします。

- **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べき最小ヒット数を示します。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、センサーは単一のサマリー 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 Summarization を設定するには、センサーが要約のためにイベントをカウントする時間間隔を指定します。

ステップ 19 **Finish** をクリックし、変更を保存します。

Alert Behavior ウィンドウが表示されます。

ステップ 20 **Finish** をクリックします。

Create Custom Signature ダイアログボックスが表示され、このカスタム シグニチャがセンサーに適用されます。

ステップ 21 **Yes** をクリックして、カスタム シグニチャを作成します。

ヒント 変更を元に戻すには、**Cancel** をクリックします。

作成したシグニチャをイネーブルにして、シグニチャのリストに追加します。