CHAPTER 5

シグニチャの定義

この章では、シグニチャを設定する方法について説明します。この章は、次の項で構成されています。

シグニチャの説明

攻撃またはその他のネットワーク リソースの不正使用は、ネットワークへの侵入として定義付けることができます。シグニチャベースのテクノロジーを使用するセンサーは、ネットワークへの侵入を検出できます。*シグニチャ*は、DoS 攻撃（サービス拒絶攻撃）などの典型的な不正侵入行為を検出するためにセンサーが使用する規則の集まりです。センサーは、ネットワーク パケットをスキャンするときに、シグニチャを使って既知の攻撃を検出し、指定されたアクションに従って対応します。

センサーは、一連のシグニチャとネットワーク アクティビティを比較します。一致した場合、イベントのロギングやアラートの送信などのアクションを実行します。センサーでは、既存のシグニチャを変更したり、新しいシグニチャを定義したりできます。

シグニチャ ベースの侵入検出では、false positive が生じる場合があります。通常のネットワーク アクティビティでも、悪意のあるアクティビティとして誤解される場合があるためです。たとえば、ネットワーク アプリケーションやオペレーティング システムによっては多数の ICMP メッセージを送信する場合がありますが、シグニチャ ベースの検出システムでは、これを攻撃者がネットワーク セグメントを調査しようとしていると解釈してしまう可能性があります。センサーをチューニングすると、false positives を最小限に抑えることができます。

特定のシグニチャを使ってネットワーク トラフィックを監視するようにセンサーを設定するには、そのシグニチャを使用可能にする必要があります。デフォルトでは、重要なシグニチャはシグニチャ アップデートのインストール時に使用可能になります。使用可能になっているシグニチャと一致する攻撃を検出すると、センサーはアラートを生成します。アラートは、センサーのイベント ストアに保存されます。Web ベース クライアントは、アラートやその他のイベントをイベント ストアから取得できます。デフォルトでは、センサーは Informational 以上のすべてのアラートをログに記録します。

シグニチャには、サブシグニチャを持つもの（サブカテゴリに分類されているもの）があります。サブシグニチャを設定した場合、あるサブシグニチャのパラメータを変更しても、変更が適用されるのはそのサブシグニチャだけです。たとえば、シグニチャ 3050 のサブシグニチャ 1 の重大度を変更した場合、重大度の変更はサブシグニチャ 1 だけに適用され、3050 2、3050 3、および 3050 4 には適用されません。

IPS 5.1 には、1000 個を超えるデフォルトの組み込みシグニチャがあります。組み込みシグニチャのリストでシグニチャの名前を変更したり、シグニチャを削除したりすることはできません。ただし、シグニチャをリタイアさせ、センシング エンジンから除去することができます。リタイアにしたシグニチャは後でアクティブ化できます。ただし、このプロセスを実行すると、センシング エンジンは設定を再構築する必要があり時間がかかるため、トラフィック処理が遅れる可能性があります。組み込みシグニチャのチューニングはできます。これには、シグニチャのいくつかのパラメータを変更します。変更された組み込みシグニチャは、*チューニング済み*シグニチャと呼ばれます。

カスタム シグニチャと呼ばれるシグニチャを作成できます。カスタム シグニチャ ID は、60000 から始まります。これらは、UDP 接続におけるストリング照合、ネットワーク フラッドの追跡、および各種スキャンなどの多数の用途について設定できます。シグニチャは、監視するトラフィックの種類に対して特別に設計されたシグニチャ エンジンを使って作成します。

シグニチャ変数の設定

この項では、シグニチャ変数の作成方法について説明します。取り上げる事項は次のとおりです。

概要

複数のシグニチャで同じ値を使用する場合、変数を使用します。変数の値を変更すると、すべてのシグニチャの変数が更新されます。このため、シグニチャを設定するときに変数を繰り返し変更しなくて済みます。

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

シグニチャ システムに必要なため、削除できない変数もあります。変数が保護されている場合は、それを選択して編集することはできません。保護された変数を削除しようとすると、エラー メッセージが表示されます。一度に編集できる変数は 1 つだけです。

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

シグニチャ変数を設定するには、管理者またはオペレータである必要があります。

フィールド定義

この項では、シグニチャ変数のフィールド定義を示します。取り上げる事項は次のとおりです。

Signature Variables パネル

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

フィールドの説明：

- **Name**：この変数に割り当てる名前を指定します。
- **Type**：変数を Web ポートまたは IP アドレス範囲として指定します。
- **Value**：この変数によって表される値を指定します。

  1 つの変数に対して複数のポート番号を指定するには、エントリをカンマで区切ります。たとえば、80, 3128, 8000, 8010, 8080, 8888, 24326 のように指定します。

ボタンの機能：

- **Add**：Add Signature Variable ダイアログボックスを開きます。
  このダイアログボックスで、新しい変数を追加し、この変数に関連付けられた値を指定できます。
- **Edit**：Edit Signature Variable ダイアログボックスを開きます。
  このダイアログボックスで、この変数に関連付けられた値を変更できます。
- **Delete**：選択した変数を使用可能な変数リストから削除します。
- **Apply**：変更を適用し、変更された設定を保存します。
- **Reset**：編集項目を以前に設定した値で置き換えてパネルをリフレッシュします。

Add and Edit Signature Variable ダイアログボックス

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

フィールドの説明：

- **Name**：この変数に割り当てる名前を指定します。
- **Type**：変数を Web ポートまたは IP アドレス範囲として指定します。
- **Value**：この変数によって表される値を指定します。
  1 つの変数に対して複数のポート番号を指定するには、エントリをカンマで区切ります。たとえば、80, 3128, 8000, 8010, 8080, 8888, 24326 のように指定します。

ボタンの機能：

- **OK**：変更を受け入れ、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄しダイアログボックスを閉じます。
- **Help**：この機能のヘルプ トピックを表示します。

シグニチャ変数の設定

シグニチャ変数を設定するには、次の手順を実行します。

ステップ 1　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

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

Signature Variables パネルが表示されます。

ステップ 3　**Add** をクリックして、変数を追加します。

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

ステップ 4　**Name** フィールドに、シグニチャ変数の名前を入力します。

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

ステップ 5　**Value** フィールドに、新しいシグニチャ変数の値を入力します。

（注）　デリミタにはカンマが使用できます。カンマの後にはスペースを入れないでください。スペースを入力すると、`Validation failed` エラーが生じます。

WEBPORTS は Web サーバが実行されているポート群で、あらかじめ定義されているものですが、値は編集できます。この変数は、Web ポートが含まれるすべてのシグニチャに影響します。デフォルトは、80, 3128, 8000, 8010, 8080, 8888, 24326 です。

ステップ 6　**OK** をクリックします。

Signature Variables パネルのシグニチャ変数リストに、新しい変数が表示されます。

ステップ 7　シグニチャ変数リストにある既存の変数を編集するには、それを選択して **Edit** をクリックします。

選択した変数の Edit Signature Variable ダイアログボックスが表示されます。

ステップ 8　**Value** フィールドで必要な変更を行います。

ステップ 9　**OK** をクリックします。

Signature Variables パネルのシグニチャ変数リストに、編集された変数が表示されます。

ステップ 10　シグニチャ変数リストにある既存の変数を削除するには、それを選択して **Delete** をクリックします。

削除された変数は、Signature Variables パネルのシグニチャ変数リストに表示されなくなります。

ヒント　変更を元に戻す場合は、**Reset** をクリックします。

ステップ 11　**Apply** をクリックし、変更を適用して、変更された設定を保存します。

シグニチャの設定

この項では、シグニチャの設定方法について説明します。取り上げる事項は次のとおりです。

概要

Signature Configuration パネルでは、次の作業を実行できます。

- センサーに保存されているすべてのシグニチャのソートと表示。

  攻撃タイプ、プロトコル、サービス、オペレーティング システム、実行するアクション、エンジン、シグニチャ ID、シグニチャ名によるソートが可能です。
- 選択したシグニチャに関する NSDB 情報の表示。

  NSDB ページには、選択したシグニチャのキー アトリビュート、説明、良性トリガー、および推奨されるフィルタが表示されます。
- 既存のシグニチャのパラメータに関連付けられた値（複数可）を変更する、編集（チューニング）。
- 既存のシグニチャを複製し、そのシグニチャのパラメータを新しいシグニチャの始点として使用する方法、または最初から新しいシグニチャを作成する方法のいずれかによる、シグニチャの作成。

  Custom Signature Wizard を使用してシグニチャを作成することもできます。このウィザードは、適切なシグニチャ エンジンの選択のほか、カスタム シグニチャを設定するために必要なパラメータの選択を手引きします。
- 既存のシグニチャのイネーブル化またはディセーブル化。
- シグニチャのデフォルトの復元。
- カスタム シグニチャの削除。

  組み込みシグニチャは削除できません。
- 既存のシグニチャのアクティブ化またはリタイア化。
- シグニチャへのアクションの割り当て。

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

シグニチャを設定するには、管理者またはオペレータである必要があります。

フィールド定義

この項では、シグニチャ変数のフィールド定義を示します。取り上げる事項は次のとおりです。

Signature Configuration パネル

Signature Configuration パネルには、次のフィールドとボタンがあります。

フィールドの説明：

- **Select By**：プロトコル、サービス、またはアクションなどソートするアトリビュートを選択して、シグニチャ リストをソートします。
- **Select Criteria**：カテゴリ内のクラスを選択して、カテゴリ内の詳細なソートを実行します。

  たとえば、プロトコルによるソートを選択した場合、L2/L3/L4 プロトコルを選択でき、L2/L3/L4 プロトコルに関連するシグニチャのみを表示できます。
- **Sig ID**：このシグニチャに割り当てられた固有の数値を示します。

  この値を使用すると、センサーが特定のシグニチャを識別できます。
- **SubSig ID**：このサブシグニチャに割り当てられた固有の数値を示します。

  SubSig ID は、広い範囲のシグニチャのバージョンをより細かく示すために使用します。
- **Name**：このシグニチャに割り当てる名前を示します。
- **Enabled**：このシグニチャがイネーブルであるかどうかを示します。

  シグニチャによって指定されたトラフィックをセンサーが保護するようにするには、シグニチャをイネーブルにする必要があります。
- **Action**：このシグニチャが反応したときにセンサーが行うアクションを示します。
- **Severity**：シグニチャが報告する重大度（High、Informational、Low、Medium）を示します。
- **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値を示します。
- **Base RR**：各シグニチャの基本リスク評価値を表示します。IDM は、忠実度評価と重大度要素を掛けたものを 100 で割って（Fidelity Rating x Severity Factor /100）、基本 RR を自動的に計算します。

  Severity Factor には次の値があります。
  - Severity Factor = 100（シグニチャの重大度が high の場合）
  - Severity Factor = 75（シグニチャの重大度が medium の場合）
  - Severity Factor = 50（シグニチャの重大度が low の場合）
  - Severity Factor = 25（シグニチャの重大度が informational の場合）
- **Type**：このシグニチャがデフォルト（組み込み）、チューニング済み、またはカスタム シグニチャであるかどうかを示します。
- **Engine**：このシグニチャによって指定されたトラフィックを解析および検査するエンジンを示します。
- **Retired**：このシグニチャがリタイアであるかどうかを示します。

  リタイアにしたシグニチャは、シグニチャ エンジンから削除されます。リタイアにしたシグニチャをアクティブにして、シグニチャ エンジンに戻すことができます。

ボタンの機能：

- **Select All**：すべてのシグニチャを選択します。

- **NSDB Link**：選択したシグニチャの NSDB ページを開きます。

  NSDB ページには、選択したシグニチャのキー アトリビュート、説明、良性トリガー、および推奨されるフィルタが表示されます。
- **Add**：Add Signature ダイアログボックスを開きます。

  このダイアログボックスで、適切なパラメータを選択してシグニチャを作成できます。
- **Clone**：Clone Signature ダイアログボックスを開きます。

  このダイアログボックスで、複製元である既存シグニチャの設定済みの値を変更して、シグニチャを作成できます。
- **Edit**：Edit Signature ダイアログボックスを開きます。

  このダイアログボックスで、選択したシグニチャに関連付けらたパラメータを変更し、効率的にシグニチャをチューニングできます。

  一度に編集できるシグニチャは 1 つだけです。
- **Enable**：選択したシグニチャをイネーブルにします。
- **Disable**：選択したシグニチャをディセーブルにします。
- **Actions**：Assign Actions ダイアログボックスを表示します。
- **Restore Defaults**：すべてのパラメータを、選択したシグニチャのデフォルト設定に戻します。
- **Delete**：選択したカスタム シグニチャを削除します。

  組み込みシグニチャは削除できません。
- **Activate**：選択したシグニチャがリタイアになっている場合、アクティブにします。

  このプロセスは、センサーがシグニチャを該当するシグニチャ エンジンに戻し、シグニチャ エンジンを再構築する必要があるため、少々時間がかかる場合があります。
- **Retire**：選択したシグニチャをリタイアにし、シグニチャ エンジンから削除します。
- **Apply**：変更を適用し、変更された設定を保存します。
- **Reset**：編集項目を以前に保存した値で置き換えてパネルをリフレッシュします。

Add Signatures ダイアログボックス

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

フィールドの説明：

- **Signature ID**：このシグニチャに割り当てられた固有の数値を示します。この値を使用すると、センサーが特定のシグニチャを識別できます。

  値は 1000 ～ 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。

  値は 0 ～ 255 です。
- **Alert Severity**：シグニチャの重大度レベルを選択します（High、Informational、Low、Medium）。
- **Sig 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値を選択します。

  値は 0 ～ 100 です。デフォルトは 75 です。
- **Promiscuous Delta**：アラートの重大度を決定します。
- **Sig　Description**：このシグニチャをその他のシグニチャと区別するために次のアトリビュートを指定します。
  - **Signature Name**：シグニチャの名前。デフォルトは MySig です。
  - **Alert Notes**：このフィールドにはアラートの注釈を加えます。
  - **User Comments**：このフィールドにはシグニチャについてのコメントを加えます。

  - **Alarm Traits**：このフィールドにはアラーム特性を指定します。値は 0 ～ 65535 です。デフォルトは 0 です。
  - **Release**：シグニチャが最初に現れたソフトウェア リリースを指定します。
- **Engine**：シグニチャによって指定されたトラフィックを解析および検査するエンジンを選択します。
  - **AIC FTP**：FTP トラフィックを検査します。発行されているコマンドを制御できます。
  - **AIC HTTP**：HTTP プロトコルの不正利用を防止するために、HTTP セッションを精密に制御します。
  - **Atomic ARP**：レイヤ 2 ARP プロトコルを検査します。ほとんどのエンジンはレイヤ 3 IP に基づいているため、Atomic ARP エンジンはその他の大半のエンジンとは異なっています。
  - **Atomic IP**：IP プロトコル パケットと関連付けられたレイヤ 4 転送プロトコルを検査します。
  - **Flood Host**：ホストを宛先とする ICMP および UDP フラッドを検出します。
  - **Flood Net**：ネットワークを宛先とする ICMP および UDP フラッドを検出します。
  - **Meta**：スライドする時間間隔内で、関連する方法で発生するイベントを定義します。このエンジンは、パケットではなくイベントを処理します。
  - **Multi String**：1 つのシグニチャに対して複数の文字列を照合することでレイヤ 4 転送プロトコル（ICMP、TCP、および UDP）のペイロードを検査するシグニチャを定義します。シグニチャを生成するために一致している必要のある一連の正規表現パターンを指定できます。
  - **Normalizer**：IP および TCP 正規化エンジンがどのように機能するかを設定し、IP および TCP 正規化エンジンに関連するシグニチャ イベントの設定を行います。RFC に準拠させることができます。
  - **Service DNS**：DNS（TCP および UDP）トラフィックを検査します。
  - **Service FTP**：FTP トラフィックを検査します。
  - **Service Generic**：カスタム サービスとペイロードをデコードします。
  - **Service H225**：VoIP トラフィックを検査します。
  - **Service HTTP**：HTTP トラフィックを検査します。WEBPORTS 変数が HTTP トラフィックの検査ポートを定義します。
  - **Service IDENT**：IDENT（クライアントおよびサーバ）トラフィックを検査します。
  - **Service MSRPC**：MSRPC トラフィックを検査します。
  - **Service MSSQL**：Microsoft SQL トラフィックを検査します。
  - **Service NTP**：NTP トラフィックを検査します。
  - **Service RPC**：RPC トラフィックを検査します。
  - **Service SMB**：SMB トラフィックを検査します。
  - **Service SNMP**：SNMP トラフィックを検査します。
  - **Service SSH**：SSH トラフィックを検査します。
  - **State**：SMTP などのプロトコル内の文字列をステートフル検索します。
  - **String ICMP**：ICMP プロトコルに基づいて正規表現文字列を検索します。
  - **String TCP**：TCP プロトコルに基づいて正規表現文字列を検索します。
  - **String UDP**：UDP プロトコルに基づいて正規表現文字列を検索します。
  - **Sweep**：1 つのホスト（ICMP および TCP）、宛先ポート（TCP および UDP）、および 2 つのノード間で RPC 要求を送受信する複数のポートからの、ポート、ホスト、およびサービスのスイープを分析します。
  - **Sweep Other TCP**：1 つのホストに関する情報を取得しようとしている監視スキャンから TCP フラグの組み合せを分析します。シグニチャは、フラグ A、B、および C を監視します。3 つのフラグがすべて検出されると、アラートを生成します。

- **Traffic ICMP**：TFN2K、LOKI、および DDOS など、非標準のプロトコルを解析します。パラメータを設定できるのは 2 つのシグニチャだけです。
- **Trojan Bo2k**：非標準プロトコルの BO2K からのトラフィックを解析します。このエンジンにはユーザ設定可能なパラメータはありません。
- **Trojan Tfn2k**：非標準プロトコルの TFN2K からのトラフィックを解析します。このエンジンにはユーザ設定可能なパラメータはありません。
- **Trojan UDP**：UDP プロトコルからのトラフィックを解析します。このエンジンにはユーザ設定可能なパラメータはありません。

• **Event Action**：**センサーがイベントに応答するときに実行するアクションを割り当てます。**

- **Deny Attacker Inline**：（インライン モードのみ）指定された期間、この攻撃者アドレスからの現在のパケットおよび将来のパケットを終了します。

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

  （注）　これは、拒否アクションの中で最も重大です。これは、単一の攻撃者アドレスからの現在および将来のパケットを拒否します。拒否された攻撃者のエントリをすべてクリアするには、**Monitoring** > **Denied Attackers** > **Clear List** をクリックします。これによって、これらのアドレスのネットワークへの再接続が許可されます。手順については、P.11-3 の「拒否された攻撃者リストの監視」を参照してください。

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

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

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

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

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

- **Request Rate Limit**：レート制限を実行するレート制限要求を ARC に送信します。レート制限デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第 8 章「ブロッキングとレート制限のための ARC の設定」を参照してください。

（注）　Request Rate Limit は、選ばれたシグニチャのセットに適用されます。レート制限を要求できるシグニチャのリストについては、P.8-4 の「レート制限について」を参照してください。

- **Request SNMP Trap**：SNMP 通知を実行する要求をセンサーの通知アプリケーション コンポーネントに送信します。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。SNMP は、このアクションを実装するようセンサーで設定されている必要があります。詳細については、第 9 章「SNMP の設定」を参照してください。
- **Reset TCP Connection**：TCP リセットを送信し、TCP フローを乗っ取って終了します。Reset TCP Connection は、単一の接続を分析する TCP シグニチャでのみ機能します。スイープやフラッドに対しては機能しません。

- **Event Counter**：センサーがイベントをカウントする方法を設定します。たとえば、同じシグニチャが同じアドレス セットに対して 5 回カウントを実行した場合にだけ、センサーがアラートを送信するように指定できます。
  - **Event Count**：アラートを生成するまでのイベントの発生回数。値は 1 ～ 65535 です。デフォルトは 1 です。
  - **Event Count Key：シグニチャのイベントをカウントするために使用するストレージ タイプ。**攻撃者アドレス、攻撃者アドレスと被害先のポート、攻撃者および被害先のアドレス、攻撃者および被害先のアドレスとポート、または被害先のアドレスを選択します。デフォルトは、攻撃者アドレスです。
  - **Specify Alert Interval**：イベント カウントをリセットするまでの秒数を指定します。**Yes または No を選択してから、時間を指定します。**
- **Alert Frequency**：シグニチャの動作中にセンサーがアラートを生成する頻度を設定します。次のパラメータをシグニチャに指定します。
  - **Summary Mode**：アラート要約のモード。Fire All、Fire Once、Global Summarize、または Summarize を選択します。
  - **Summary Interval**：各サマリー アラートを生成する間隔（秒数）。値は 1 ～ 65535 です。デフォルトは 15 です。

  - **Summary Key**：アラートの要約に使用するストレージ タイプ。攻撃者アドレス、攻撃者アドレスと被害先のポート、攻撃者および被害先のアドレス、攻撃者および被害先のアドレスとポート、または被害先のアドレスを選択します。デフォルトは、攻撃者アドレスです。
  - **Specify Global Summary Threshold：グローバル サマリーにアラートを組み込むためのイベント数のしきい値を指定します。Yes** または **No** を選択してから、時間を指定します。
- **Status**：シグニチャをイネーブルまたはディセーブルにするか、シグニチャをリタイアまたは非リタイアにします。
  - **Enabled**：シグニチャをイネーブルまたはディセーブルのどちらにするかを選択します。デフォルトは yes です。
  - **Retired**：シグニチャをリタイアにするかどうかを選択します。デフォルトは no です。

Clone and Edit Signature ダイアログボックス

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

フィールドの説明：

- **Signature ID**：このシグニチャに割り当てられた固有の数値を示します。この値を使用すると、センサーが特定のシグニチャを識別できます。

  値は 1000 ～ 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。

  値は 0 ～ 255 です。
- **Alert Severity**：シグニチャの重大度レベルを選択します（High、Informational、Low、Medium）。
- **Sig 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値を選択します。

  値は 0 ～ 100 です。デフォルトは 75 です。
- **Promiscuous Delta**：アラートの重大度を決定します。
- **Sig　Description**：このシグニチャをその他のシグニチャと区別するために次のアトリビュートを指定します。
  - **Signature Name**：シグニチャの名前。デフォルトは MySig です。
  - **Alert Notes**：このフィールドにはアラートの注釈を加えます。
  - **User Comments**：このフィールドにはシグニチャについてのコメントを加えます。
  - **Alarm Traits**：このフィールドにはアラーム特性を指定します。値は 0 ～ 65535 です。デフォルトは 0 です。
  - **Release**：シグニチャが最初に現れたソフトウェア リリースを指定します。
- **Engine**：シグニチャによって指定されたトラフィックを解析および検査するエンジンを選択します。
  - **AIC FTP**：FTP トラフィックを検査します。発行されているコマンドを制御できます。
  - **AIC HTTP**：HTTP プロトコルの不正利用を防止するために、HTTP セッションを精密に制御します。
  - **Atomic ARP**：レイヤ 2 ARP プロトコルを検査します。ほとんどのエンジンはレイヤ 3 IP に基づいているため、Atomic ARP エンジンはその他の大半のエンジンとは異なっています。
  - **Atomic IP**：IP プロトコル パケットと関連付けられたレイヤ 4 転送プロトコルを検査します。
  - **Flood Host**：ホストを宛先とする ICMP および UDP フラッドを検出します。
  - **Flood Net**：ネットワークを宛先とする ICMP および UDP フラッドを検出します。

- **Meta**：スライドする時間間隔内で、関連する方法で発生するイベントを定義します。このエンジンは、パケットではなくイベントを処理します。
- **Multi String**：1 つのシグニチャに対して複数の文字列を照合することでレイヤ 4 転送プロトコル（ICMP、TCP、および UDP）のペイロードを検査するシグニチャを定義します。シグニチャを生成するために一致している必要のある一連の正規表現パターンを指定できます。
- **Normalizer**：IP および TCP 正規化エンジンがどのように機能するかを設定し、IP および TCP 正規化エンジンに関連するシグニチャ イベントの設定を行います。RFC に準拠させることができます。
- **Service DNS**：DNS（TCP および UDP）トラフィックを検査します。
- **Service FTP**：FTP トラフィックを検査します。
- **Service Generic**：カスタム サービスとペイロードをデコードします。
- **Service H225**：VoIP トラフィックを検査します。
- **Service HTTP**：HTTP トラフィックを検査します。WEBPORTS 変数が HTTP トラフィックの検査ポートを定義します。
- **Service IDENT**：IDENT（クライアントおよびサーバ）トラフィックを検査します。
- **Service MSRPC**：MSRPC トラフィックを検査します。
- **Service MSSQL**：Microsoft SQL トラフィックを検査します。
- **Service NTP**：NTP トラフィックを検査します。
- **Service RPC**：RPC トラフィックを検査します。
- **Service SMB**：SMB トラフィックを検査します。
- **Service SNMP**：SNMP トラフィックを検査します。
- **Service SSH**：SSH トラフィックを検査します。
- **State**：SMTP などのプロトコル内の文字列をステートフル検索します。
- **String ICMP**：ICMP プロトコルに基づいて正規表現文字列を検索します。
- **String TCP**：TCP プロトコルに基づいて正規表現文字列を検索します。
- **String UDP**：UDP プロトコルに基づいて正規表現文字列を検索します。
- **Sweep**：1 つのホスト（ICMP および TCP）、宛先ポート（TCP および UDP）、および 2 つのノード間で RPC 要求を送受信する複数のポートからの、ポート、ホスト、およびサービスのスイープを分析します。
- **Sweep Other TCP**：1 つのホストに関する情報を取得しようとしている監視スキャンから TCP フラグの組み合せを分析します。シグニチャは、フラグ A、B、および C を監視します。3 つのフラグがすべて検出されると、アラートを生成します。
- **Traffic ICMP**：TFN2K、LOKI、および DDOS など、非標準のプロトコルを解析します。パラメータを設定できるのは 2 つのシグニチャだけです。
- **Trojan Bo2k**：非標準プロトコルの BO2K からのトラフィックを解析します。このエンジンにはユーザ設定可能なパラメータはありません。
- **Trojan Tfn2k**：非標準プロトコルの TFN2K からのトラフィックを解析します。このエンジンにはユーザ設定可能なパラメータはありません。
- **Trojan UDP**：UDP プロトコルからのトラフィックを解析します。このエンジンにはユーザ設定可能なパラメータはありません。

- **Event Action**：センサーがイベントに応答するときに実行するアクションを割り当てます。
  - **Deny Attacker Inline**：（インライン モードのみ）指定された期間、この攻撃者アドレスからの現在のパケットおよび将来のパケットを終了します。

    センサーは、システムによって拒否されている攻撃者のリストを保持します。拒否された攻撃者のリストからエントリを削除するには、攻撃者のリストを表示してリスト全体をクリアするか、タイマーで有効期限が切れるのを待ちます。タイマーは、エントリごとにスライドするタイマーです。したがって、攻撃者 A が拒否されているときに別の攻撃が発行

されると、攻撃者 A のタイマーはリセットされ、そのタイマーの有効期限が切れるまで攻撃者 A は拒否された攻撃者リストに残ります。拒否された攻撃者のリストがいっぱいになり、新規エントリを追加することができない場合でも、パケットは拒否されます。

（注）　これは、拒否アクションの中で最も重大です。これは、単一の攻撃者アドレスからの現在および将来のパケットを拒否します。拒否された攻撃者のエントリをすべてクリアするには、**Monitoring** > **Denied Attackers** > **Clear List** をクリックします。これによって、これらのアドレスのネットワークへの再接続が許可されます。手順については、P.11-3 の「拒否された攻撃者リストの監視」を参照してください。

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

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

- **Deny Connection Inline**：（インライン モードのみ）この TCP フローの現在のパケットと将来のパケットを終了します。
- **Deny Packet Inline**：（インライン モードのみ）パケットを終了します。
- **Log Attacker Packets**：攻撃者アドレスを含む IP ロギング パケットを開始し、アラートを送信します。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
- **Log Pair Packets**：攻撃者と被害先のアドレスのペアを含む IP ロギング パケットを開始します。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
- **Log Victim Packets**：被害先のアドレスを含む IP ロギング パケットを開始し、アラートを送信します。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
- **Modify Packet Inline**：パケット データを変更して、エンドポイントでパケットがどう処理されるかに関してあいまいな部分を除去します。
- **Produce Alert**：イベントをアラートとしてイベント ストアに書き込みます。
- **Produce Verbose Alert**：違反パケットの符号化ダンプをアラートに組み込みます。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
- **Request Block Connection**：この接続をブロックする要求を ARC に送信します。ブロッキング デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第 8 章「ブロッキングとレート制限のための ARC の設定」を参照してください。
- **Request Block Host**：この攻撃者ホストをブロックする要求を ARC に送信します。ブロッキング デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第8章「ブロッキングとレート制限のための ARC の設定」を参照してください。

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

- **Request Rate Limit**：レート制限を実行するレート制限要求を ARC に送信します。レート制限デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第 8 章「ブロッキングとレート制限のための ARC の設定」を参照してください。

（注）　Request Rate Limit は、選ばれたシグニチャのセットに適用されます。レート制限を要求できるシグニチャのリストについては、P.8-4 の「レート制限について」を参照してください。

- **Request SNMP Trap**：SNMP 通知を実行する要求をセンサーの通知アプリケーション コンポーネントに送信します。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。SNMP は、このアクションを実装するようセンサーで設定されている必要があります。詳細については、第 9 章「SNMP の設定」を参照してください。
- **Reset TCP Connection**：TCP リセットを送信し、TCP フローを乗っ取って終了します。Reset TCP Connection は、単一の接続を分析する TCP シグニチャでのみ機能します。スイープやフラッドに対しては機能しません。

- **Event Counter**：センサーがイベントをカウントする方法を設定します。たとえば、同じシグニチャが同じアドレス セットに対して 5 回カウントを実行した場合にだけ、センサーがアラートを送信するように指定できます。
  - **Event Count**：アラートを生成するまでのイベントの発生回数。値は 1 ～ 65535 です。デフォルトは 1 です。
  - **Event Count Key：シグニチャのイベントをカウントするために使用するストレージ タイプ。**攻撃者アドレス、攻撃者アドレスと被害先のポート、攻撃者および被害先のアドレス、攻撃者および被害先のアドレスとポート、または被害先のアドレスを選択します。デフォルトは、攻撃者アドレスです。
  - **Specify Alert Interval**：イベント カウントをリセットするまでの秒数を指定します。**Yes または No を選択してから、時間を指定します。**
- **Alert Frequency**：シグニチャの動作中にセンサーがアラートを生成する頻度を設定します。次のパラメータをシグニチャに指定します。
  - **Summary Mode**：アラート要約のモード。Fire All、Fire Once、Global Summarize、または Summarize を選択します。
  - **Summary Interval**：各サマリー アラートを生成する間隔（秒数）。値は 1 ～ 65535 です。デフォルトは 15 です。
  - **Summary Key**：アラートの要約に使用するストレージ タイプ。攻撃者アドレス、攻撃者アドレスと被害先のポート、攻撃者および被害先のアドレス、攻撃者および被害先のアドレスとポート、または被害先のアドレスを選択します。デフォルトは、攻撃者アドレスです。
  - **Specify Global Summary Threshold：グローバル サマリーにアラートを組み込むためのイベント数のしきい値を指定します。Yes** または **No** を選択してから、時間を指定します。
- **Status**：シグニチャをイネーブルまたはディセーブルにするか、シグニチャをリタイアまたは非リタイアにします。
  - **Enabled**：シグニチャをイネーブルまたはディセーブルのどちらにするかを選択します。デフォルトは yes です。
  - **Retired**：シグニチャをリタイアにするかどうかを選択します。デフォルトは no です。

ボタンの機能：

- **OK**：変更を受け入れ、ダイアログボックスを閉じます。
- **Cancel**：変更を廃棄しダイアログボックスを閉じます。
- **Help**：この機能のヘルプ トピックを表示します。

Assign Actions ダイアログボックス

Assign Actions ダイアログボックスには、次のフィールドとボタンがあります。

イベント アクションとは、イベントに対するセンサーの応答です。イベント アクションは、シグニチャごとに設定可能です。

フィールドの説明：

- **Deny Attacker Inline**：（インライン モードのみ）指定された期間、この攻撃者アドレスからの現在のパケットおよび将来のパケットを終了します。

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

  （注）　これは、拒否アクションの中で最も重大です。これは、単一の攻撃者アドレスからの現在および将来のパケットを拒否します。拒否された攻撃者のエントリをすべてクリアするには、**Monitoring** > **Denied Attackers** > **Clear List** をクリックします。これによって、これらのアドレスのネットワークへの再接続が許可されます。手順については、P.11-3 の「拒否された攻撃者リストの監視」を参照してください。

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

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

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

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

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

- **Request Rate Limit**：レート制限を実行するレート制限要求を ARC に送信します。レート制限デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第 8 章「ブロッキングとレート制限のための ARC の設定」を参照してください。

（注）　Request Rate Limit は、選ばれたシグニチャのセットに適用されます。レート制限を要求できるシグニチャのリストについては、P.8-4 の「レート制限について」を参照してください。

- **Request SNMP Trap**：SNMP 通知を実行する要求をセンサーの通知アプリケーション コンポーネントに送信します。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。SNMP は、このアクションを実装するようセンサーで設定されている必要があります。詳細については、第 9 章「SNMP の設定」を参照してください。
- **Reset TCP Connection**：TCP リセットを送信し、TCP フローを乗っ取って終了します。Reset TCP Connection は、単一の接続を分析する TCP シグニチャでのみ機能します。スイープやフラッドに対しては機能しません。

ボタンの機能：

- **Select All**：リストにあるすべてのイベント アクションを選択します。
- **Select None**：すべてのイベント アクションの選択をクリアします。

シグニチャの追加

シグニチャを追加するには、次の手順を実行します。

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、パラメータが現在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 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 > Signature Configuration** をクリックします。

Signature Configuration パネルが表示されます。

ステップ 3　既存のシグニチャを使用しないでカスタム シグニチャを追加するには、次の手順を実行します。

a. **Add** をクリックして、Add Signature ダイアログボックスを開きます。
b. **Signature** フィールドで新しいシグニチャに一意のシグニチャ ID を指定します。
c. **Subsignature** フィールドで新しいシグニチャに一意のサブシグニチャ ID を指定します。
d. **Alert Severity** フィールドの隣にある緑のアイコンをクリックし、シグニチャに関連付ける重大度を選択します。
e. **Signature Fidelity Rating** フィールドの隣にある緑のアイコンをクリックし、シグニチャのシグニチャ忠実度評価を表す値（1 ～ 100）を指定します。
f. シグニチャ説明フィールドにシグニチャに関するコメントを入力します。
g. センサーがこのシグニチャを有効にするために使用するエンジンを選択します。

（注）　選択するエンジンが不明な場合、Custom Signature Wizard を使用してカスタム シグニチャを作成してください。詳細については、P.6-22 の「カスタム シグニチャの作成」を参照してください。

h. **Event Actions** フィールドの横にある緑色のアイコンをクリックし、センサーがイベントに応答するときに起こすアクションを選択します。

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

i. イベントをカウントする場合は、Event Counter の下にある **Event Counter** フィールドを設定します。
j. Alert Frequency の下にある **Alert Frequency** フィールドで、アラートを受信する方法を指定します。
k. Status の下で **Yes** を選択し、シグニチャをイネーブルにします。

（注）　シグニチャによって指定された攻撃をセンサーがアクティブに検出できるようにするには、シグニチャをイネーブルにする必要があります。

l. Status の下で、シグニチャをリタイアにするかどうかを指定します。**No** をクリックして、シグニチャをアクティブにします。これによってシグニチャがエンジンに組み込まれます。

（注）　シグニチャによって指定された攻撃をセンサーがアクティブに検出できるようにするには、シグニチャをアクティブにする必要があります。

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

m. **OK** をクリックします。

Type が Custom に設定された新しいシグニチャがリストに現れます。

ヒント　変更を元に戻す場合は、**Reset** をクリックします。

ステップ 4　**Apply** をクリックし、変更を適用して、変更された設定を保存します。

シグニチャの複製

Signature Configuration パネルでは、既存のシグニチャを複製する方法でシグニチャを作成できます。既存のシグニチャと類似したシグニチャを作成する場合、この方法が便利です。

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、パラメータが現在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。

シグニチャを複製するには、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 > Signature Configuration** をクリックします。

Signature Configuration パネルが表示されます。

ステップ 3　シグニチャを見つけるには、**Select By** リストのソート オプションを選択します。

たとえば、UDP Flood シグニチャを検索する場合は、**L2/L3/L4 Protocol** を選択し、その後、**UDP Floods** を選択します。

Signature Configuration パネルがリフレッシュされ、ソート条件に一致するシグニチャが表示されます。

ステップ 4　既存のシグニチャをベースとして使用する方法でシグニチャを作成するには、既存のシグニチャを選択し、次の手順を実行します。

a. **Clone** をクリックして、Clone Signature ダイアログボックスを開きます。

b. **Signature** フィールドで新しいシグニチャに一意のシグニチャ ID を指定します。

c. **Subsignature** フィールドで新しいシグニチャに一意のサブシグニチャ ID を指定します。

d. パラメータの値を確認し、新しいシグニチャ用に変更する場合はパラメータの値を変更します。

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

e. Status の下で **Yes** を選択し、シグニチャをイネーブルにします。

（注）　シグニチャによって指定された攻撃をセンサーがアクティブに検出できるようにするには、シグニチャをイネーブルにする必要があります。

f. Status の下で、シグニチャをリタイアにするかどうかを指定します。**No** をクリックして、シグニチャをアクティブにします。これによってシグニチャがエンジンに組み込まれます。

（注）　シグニチャによって指定された攻撃をセンサーがアクティブに検出できるようにするには、シグニチャをアクティブにする必要があります。

ヒント　変更を元に戻し、Clone 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。

g. **OK** をクリックします。

Type が Custom に設定されている、複製されたシグニチャがリストに表示されます。

ヒント　変更を元に戻す場合は、**Reset** をクリックします。

ステップ 5　**Apply** をクリックし、変更を適用して、変更された設定を保存します。

シグニチャのチューニング

シグニチャをチューニングするには、次の手順を実行します。

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、パラメータが現在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 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 > Signature Configuration** をクリックします。

Signature Configuration パネルが表示されます。

ステップ 3　シグニチャを見つけるには、**Select By** リストのソート オプションを選択します。

たとえば、UDP Flood シグニチャを検索する場合は、**L2/L3/L4 Protocol** を選択し、その後、**UDP Floods** を選択します。

Signature Configuration パネルがリフレッシュされ、ソート条件に一致するシグニチャが表示されます。

ステップ 4　既存のシグニチャをチューニングするには、シグニチャを選択し、次の手順を実行します。

a. **Edit** をクリックして、Edit Signature ダイアログボックスを開きます。
b. パラメータの値を確認し、チューニングするパラメータの値を変更します。

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

c. Status の下で **Yes** を選択し、シグニチャをイネーブルにします。

（注）　シグニチャによって指定された攻撃をセンサーがアクティブに検出できるようにするには、シグニチャをイネーブルにする必要があります。

d. Status の下で、シグニチャをリタイアにするかどうかを指定します。**No** をクリックして、シグニチャをアクティブにします。これによってシグニチャがエンジンに組み込まれます。

（注）　シグニチャによって指定された攻撃をセンサーがアクティブに検出できるようにするには、シグニチャをアクティブにする必要があります。

ヒント　変更を元に戻し、Edit 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。

e. **OK** をクリックします。

Type が Custom に設定されている、編集されたシグニチャがリストに表示されます。

ヒント　変更を元に戻す場合は、**Reset** をクリックします。

ステップ 5　**Apply** をクリックし、変更を適用して、変更された設定を保存します。

シグニチャのイネーブル化とディセーブル化

シグニチャをイネーブルにするには、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 > Signature Configuration** をクリックします。

Signature Configuration パネルが表示されます。

ステップ 3　シグニチャを見つけるには、**Select By** リストのソート オプションを選択します。

たとえば、UDP Flood シグニチャを検索する場合は、**L2/L3/L4 Protocol** を選択し、その後、**UDP Floods** を選択します。

Signature Configuration パネルがリフレッシュされ、ソート条件に一致するシグニチャが表示されます。

ステップ 4　既存のシグニチャをイネーブルまたはディセーブルにするには、シグニチャを選択し、次の手順を実行します。

a. Enabled カラムを表示し、シグニチャのステータスを判断します。イネーブルになっているシグニチャは、このカラムが Yes になっています。

b. ディセーブルになっているシグニチャをイネーブルにするには、シグニチャを選択し、**Enable** をクリックします。

c. イネーブルになっているシグニチャをディセーブルにするには、シグニチャを選択し、**Disable** をクリックします。

ヒント　変更を元に戻す場合は、**Reset** をクリックします。

ステップ 5　**Apply** をクリックし、変更を適用して、変更された設定を保存します。

シグニチャのアクティブ化とリタイア化

注意　シグニチャのアクティブ化およびリタイア化は、非常に時間を要する作業で、30 分以上かかる場合もあります。

シグニチャをアクティブまたはリタイアにするには、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 > Signature Configuration** をクリックします。

Signature Configuration パネルが表示されます。

ステップ 3　シグニチャを見つけるには、**Select By** リストのソート オプションを選択します。

たとえば、UDP Flood シグニチャを検索する場合は、**L2/L3/L4 Protocol** を選択し、その後、**UDP Floods** を選択します。

Signature Configuration パネルがリフレッシュされ、ソート条件に一致するシグニチャが表示されます。

ステップ 4　リタイアになっているシグニチャをアクティブにするには、シグニチャを選択し、**Activate** をクリックします。

ステップ 5　アクティブになっているシグニチャをリタイアにするには、シグニチャを選択し、**Retire** をクリックします。

（注）　シグニチャをリタイアにすると、そのシグニチャはエンジンから削除されますが、シグニチャ コンフィギュレーション リストには保持されます。リタイアにしたシグニチャを後でアクティブにできますが、そのためにはセンサーがエンジンのシグニチャ リストを再構築する必要があり、シグニチャ処理が遅れる可能性があります。

ヒント　変更を元に戻す場合は、**Reset** をクリックします。

ステップ 6　**Apply** をクリックし、変更を適用して、変更された設定を保存します。

シグニチャへのアクションの割り当て

シグニチャにアクションを割り当てるには、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 > Signature Configuration** をクリックします。

Signature Configuration パネルが表示されます。

ステップ 3　シグニチャを見つけるには、**Select By** リストのソート オプションを選択します。

たとえば、UDP Flood シグニチャを検索する場合は、**L2/L3/L4 Protocol** を選択し、その後、**UDP Floods** を選択します。

Signature Configuration パネルがリフレッシュされ、ソート条件に一致するシグニチャが表示されます。

ステップ 4　シグニチャまたはシグニチャ セットにアクションを割り当てるには、シグニチャを選択し、**Actions** をクリックします。

Assign Actions ダイアログボックスが表示されます。

a. シグニチャに割り当てるアクションを選択します。

チェック マークが付いている場合は、そのアクションが選択したシグニチャに割り当てられていることを示します。チェック マークが付いていない場合は、そのアクションが選択したシグニチャのどれにも割り当てられていないことを示します。灰色のチェック マークが付いている場合は、そのアクションが選択したシグニチャのどれかに割り当てられていることを示します。

- **Deny Attacker Inline**：（インライン モードのみ）指定された期間、この攻撃者アドレスからの現在のパケットおよび将来のパケットを終了します。

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

  （注）　これは、拒否アクションの中で最も重大です。これは、単一の攻撃者アドレスからの現在および将来のパケットを拒否します。拒否された攻撃者のエントリをすべてクリアするには、**Monitoring > Denied Attackers > Clear List** をクリックします。これによって、これらのアドレスのネットワークへの再接続が許可されます。手順については、P.11-3 の「拒否された攻撃者リストの監視」を参照してください。

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

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

- **Deny Connection Inline**：（インライン モードのみ）この TCP フローの現在のパケットと将来のパケットを終了します。
- **Deny Packet Inline**：（インライン モードのみ）パケットを終了します。
- **Log Attacker Packets**：攻撃者アドレスを含む IP ロギング パケットを開始し、アラートを送信します。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
- **Log Pair Packets**：攻撃者と被害先のアドレスのペアを含む IP ロギング パケットを開始します。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
- **Log Victim Packets**：被害先のアドレスを含む IP ロギング パケットを開始し、アラートを送信します。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
- **Modify Packet Inline**：パケット データを変更して、エンドポイントでパケットがどう処理されるかに関してあいまいな部分を除去します。
- **Produce Alert**：イベントをアラートとしてイベント ストアに書き込みます。
- **Produce Verbose Alert**：違反パケットの符号化ダンプをアラートに組み込みます。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。
- **Request Block Connection**：この接続をブロックする要求を ARC に送信します。ブロッキング デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第 8 章「ブロッキングとレート制限のための ARC の設定」を参照してください。
- **Request Block Host**：この攻撃者ホストをブロックする要求を ARC に送信します。ブロッキング デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第8章「ブロッキングとレート制限のための ARC の設定」を参照してください。

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

- **Request Rate Limit**：レート制限を実行するレート制限要求を ARC に送信します。レート制限デバイスは、このアクションを実装するよう設定されている必要があります。詳細については、第 8 章「ブロッキングとレート制限のための ARC の設定」を参照してください。

（注）　Request Rate Limit は、選ばれたシグニチャのセットに適用されます。レート制限を要求できるシグニチャのリストについては、P.8-4 の「レート制限について」を参照してください。

- **Request SNMP Trap**：SNMP 通知を実行する要求をセンサーの通知アプリケーション コンポーネントに送信します。このアクションを実行すると、Produce Alert が選択されていない場合でも、イベント ストアにアラートが書き込まれます。SNMP は、このアクションを実装するようセンサーで設定されている必要があります。詳細については、第 9 章「SNMP の設定」を参照してください。

- **Reset TCP Connection** : TCP リセットを送信し、TCP フローを乗っ取って終了します。Reset TCP Connection は、単一の接続を分析する TCP シグニチャでのみ機能します。スイープやフラッドに対しては機能しません。

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

b. 選択したシグニチャにすべてのアクションを割り当てる場合は、**All** をクリックします。または、選択したシグニチャからすべてのアクションを削除する場合は、**None** を選択します。

ヒント　変更を元に戻し、Assign Actions ダイアログボックスを閉じるには、**Cancel** をクリックします。

c. 変更内容を保存してダイアログボックスを閉じるには、**OK** をクリックします。

新しいアクションが Action カラムに表示されます。

Miscellaneous パネルの設定

この項では、Miscellaneous パネルの設定方法について説明します。取り上げる事項は次のとおりです。

概要

Miscellaneous パネルでは、次の作業を実行できます。

- アプリケーション ポリシー パラメータの設定。

  センサーは、Web サービス関連の悪意のある攻撃を防ぐために、レイヤ 4 ～ レイヤ 7 のパケット検査を行うように設定できます。

- IP フラグメント再構成オプションの設定。

  センサーは、複数のパケットにわたってフラグメント化されたデータグラムを再構成するように設定できます。このとき、データグラムの数と、データグラムについてさらにフラグメントが届くのを待つ時間を判断するために使用する境界値が指定できます。これは、センサーがフレーム送信を受信できなかったことや、無作為にフラグメント化されたデータグラムを生成する攻撃が仕掛けられていることが原因で再構成が不十分なデータグラムに対し、センサーのリソースをすべて割り当ててしまわないようにするためのものです。

- TCP ストリーム再構成の設定。

  センサーは、完全な 3 ウェイ ハンドシェイクによって確立された TCP セッションだけを監視するように設定できます。また、ハンドシェイクの完了まで待つ時間の最大値と、パケットがない場合に接続を監視し続ける時間も設定できます。これは、有効な TCP セッションが確立していないときにセンサーがアラートを生成しないようにするためのものです。センサーに対する攻撃には、単純に攻撃を繰り返すだけでセンサーにアラートを生成させようとするものがあります。TCP セッションの再組み立て機能は、センサーに対するこのような攻撃の緩和に役立ちます。

- IP ロギング オプションの設定。

  センサーは、攻撃を検出したときに、IP セッション ログを生成するように設定できます。シグニチャの応答アクションとして IP ロギングが設定されているときにシグニチャが反応すると、アラートの送信元アドレスとの間で送受信されるすべてのパケットがログに記録されます。

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

Miscellaneous パネルでパラメータを設定するには、管理者またはオペレータである必要があります。

フィールド定義

Miscellaneous パネルには、次のフィールドとボタンがあります。

- **Application Policy**：アプリケーション ポリシーの実施を設定します。
  - **Enable HTTP** ：Web サービスの保護をイネーブルにします。HTTP トラフィックが RFC に準拠しているかどうかをセンサーが検査するようにするには、**Yes** を選択します。
  - **Max HTTP Requests**：未処理の HTTP 要求の最大数（1 接続あたり）を指定します。
  - **AIC Web Ports**：AIC トラフィックを監視するポートの変数を指定します。
  - **Enable FTP** ：Web サービスの保護をイネーブルにします。センサーが FTP トラフィックを検査するようにするには、**Yes** を選択します。
- **Fragment Reassembly**：IP フラグメント再構成を設定します。
  - **IP Reassembly Mode**：センサーが使用する、オペレーティング システムに基づくフラグメントの再構成方法を指定します。
- **Stream Reassembly**：TCP ストリーム再構成を設定できます。
  - **TCP Handshake Required**：センサーが、3 ウェイ ハンドシェイクが完了したセッションのみを追跡するように指定します。
  - **TCP Reassembly Mode**：センサーが TCP セッションの再構成に使用するモードを、次のオプション付きで指定します。

    Asymmetric：双方向のトラフィック フローの一方向のみを対象にします。

    （注） Asymmetric モードでは、センサーはトラフィック フローの状態と同期をとり、双方向のうち一方向だけでよいエンジンの検査を継続します。完全に保護するには、トラフィックの双方向を対象にする必要があるため、Asymmetric モードではセキュリティが低下します。

    Strict：何らかの理由でパケットを受信しなかった場合、以後のパケットはすべて処理しません。

    Loose：パケットが廃棄される可能性がある場合に使用します。
- **IP Log**：次のいずれかの条件が満たされた場合、センサーが IP ロギングを停止するように設定します。
  - **Max IP Log Packets**：ログを作成するパケットの数を指定します。
  - **IP Log Time**：ログを作成する時間を指定します。有効な値は、1 ～ 60 秒です。デフォルトは 30 秒です。
  - **Max IP Log Bytes**：ログを作成する最大バイト数を指定します。

ボタンの機能：

- **Apply**：変更を適用し、変更された設定を保存します。
- **Reset**：編集項目を以前に設定した値で置き換えてパネルをリフレッシュします。

アプリケーション ポリシーの設定

この項では、Application Policy（AIC）シグニチャとその設定方法について説明します。シグニチャ エンジンの詳細については、P.B-9 の「AIC エンジン」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。

概要

AIC は Web トラフィックの詳細分析を行います。HTTP プロトコルの不正利用を防止するために、HTTP セッションを精密に制御します。たとえば、インスタント メッセージや、gotomypc などのトンネリング アプリケーションなど、特定のポート上でトンネリングを行うアプリケーションに対する管理制御を行います。これらのアプリケーションが HTTP を介して稼働している場合は、P2P およびインスタント メッセージの検査とポリシー チェックを実行できます。

AIC は、FTP トラフィックを検査し、発行されるコマンドを制御する方法を提供します。

事前定義されたシグニチャをイネーブルまたはディセーブルにすることもできますし、カスタム シグニチャでポリシーを作成することもできます。

（注）　AIC エンジンは、HTTP トラフィックが AIC Web ポートで受信されたときに実行されます。トラフィックが Web トラフィックであっても、AIC Web ポートで受信されない場合は、Service HTTP エンジンが実行されます。AIC 検査は、AIC Web ポートとして設定されている任意のポートで実行できます。検査されるトラフィックは HTTP トラフィックです。

AIC には、次のシグニチャのカテゴリがあります。

- HTTP 要求メソッド
  - 定義要求メソッド
  - 認識済み要求メソッド

  シグニチャ ID のリストとその説明については、AIC 要求メソッド シグニチャ（P.5-30）を参照してください。
- MIME タイプ
  - 定義コンテンツ タイプ
  - 認識されるコンテンツ タイプ

  シグニチャ ID のリストとその説明については、P.5-31 の「AIC MIME 定義コンテンツ タイプ シグニチャ」を参照してください。カスタム MIME シグニチャを作成する手順については、P.5-36 の「認識済みの定義コンテンツ タイプ（MIME）シグニチャの例」を参照してください。
- 定義 Web トラフィック ポリシー

  1 つの事前に定義されたシグニチャ 12674 があります。これは、非準拠の HTTP トラフィックが検出された場合に実行するアクションを指定しています。パラメータ Alarm on Non HTTP Traffic はシグニチャをイネーブルにします。デフォルトでは、このシグニチャはイネーブルです。
- 転送符号化
  - アクションと各メソッドを関連付けます。
  - センサーが認識済みのメソッドのリストを表示します。
  - チャンク符号化エラーが検出された場合に実行する必要のあるアクションを指定します。

  シグニチャ ID のリストとその説明については、P.5-34 の「AIC 転送符号化シグニチャ」を参照してください。

- FTP コマンド

  アクションを FTP コマンドに関連付けます。シグニチャ ID のリストとその説明については、P.5-34 の「AIC FTP コマンド シグニチャ」を参照してください。

AIC 要求メソッド シグニチャ

HTTP 要求メソッドには 2 つのシグニチャのカテゴリがあります。

- 定義要求メソッド：アクションと要求メソッドの関連付けを可能にします。シグニチャを拡張し変更できます（Define Request Method）。
- 認識済み要求メソッド：センサーが認識済みのメソッドのリストを表示します（Recognized Request Methods）。

表 5-1 は、事前定義済みの定義要求メソッド シグニチャを示しています。必要とする事前定義済みのメソッドを持つシグニチャをイネーブルにしてください。シグニチャをイネーブルにする手順は、P.5-22 の「シグニチャのイネーブル化とディセーブル化」を参照してください。

表 5-1　要求メソッド シグニチャ

シグニチャ ID	定義要求メソッド
12676	要求メソッドは認識されていない
12677	定義要求メソッド PUT
12678	定義要求メソッド CONNECT
12679	定義要求メソッド DELETE
12680	定義要求メソッド GET
12681	定義要求メソッド HEAD
12682	定義要求メソッド OPTIONS
12683	定義要求メソッド POST
12685	定義要求メソッド TRACE
12695	定義要求メソッド INDEX
12696	定義要求メソッド MOVE
12697	定義要求メソッド MKDIR
12698	定義要求メソッド COPY
12699	定義要求メソッド EDIT
12700	定義要求メソッド UNEDIT
12701	定義要求メソッド SAVE
12702	定義要求メソッド LOCK
12703	定義要求メソッド UNLOCK
12704	定義要求メソッド REVLABEL
12705	定義要求メソッド REVLOG
12706	定義要求メソッド REVADD
12707	定義要求メソッド REVNUM
12708	定義要求メソッド SETATTRIBUTE
12709	定義要求メソッド GETATTRIBUTENAME
12710	定義要求メソッド GETPROPERTIES
12711	定義要求メソッド STARTENV
12712	定義要求メソッド STOPREV

AIC MIME 定義コンテンツ タイプ シグニチャ

MIME タイプには 2 つのポリシーが関連付けられています。

- 定義コンテンツ タイプ：次の場合に特定のアクションを関連付けます（Define Content Type）。
  - image/jpeg などの特定の MIME タイプを拒否する
  - メッセージ サイズ違反
  - ヘッダーと本体に記述された MIME タイプが一致しない
- 認識されるコンテンツ タイプ（Recognized Content Type）

表 5-2 は、事前定義済みの定義コンテンツ タイプ シグニチャを示しています。必要とする事前定義済みのメソッドを持つシグニチャをイネーブルにしてください。シグニチャをイネーブルにする手順は、P.5-22 の「シグニチャのイネーブル化とディセーブル化」を参照してください。カスタム定義コンテンツ タイプ シグニチャを作成することもできます。手順については、P.5-36 の「認識済みの定義コンテンツ タイプ（MIME）シグニチャの例」を参照してください。

表 5-2　定義コンテンツ タイプ シグニチャ

シグニチャ ID	シグニチャの説明
12621	コンテンツ タイプ image/gif のメッセージ長が無効です。
12622 2	コンテンツ タイプ image/png の検証に失敗しました。
12623 0 12623 1 12623 2	コンテンツ タイプ image/tiff のヘッダー チェック。 コンテンツ タイプ image/tiff のメッセージ長が無効です。 コンテンツ タイプ image/tiff の検証に失敗しました。
12624 0 12624 1 12624 2	コンテンツ タイプ image/x-3ds のヘッダー チェック。 コンテンツ タイプ image/x-3ds のメッセージ長が無効です。 コンテンツ タイプ image/x-3ds の検証に失敗しました。
12626 0 12626 1 12626 2	コンテンツ タイプ image/x-portable-bitmap のヘッダー チェック。 コンテンツ タイプ image/x-portable-bitmap のメッセージ長が無効です。 コンテンツ タイプ image/x-portable-bitmap の検証に失敗しました。
12627 0 12627 1 12627 2	コンテンツ タイプ image/x-portable-graymap のヘッダー チェック。 コンテンツ タイプ image/x-portable-graymap のメッセージ長が無効です。 コンテンツ タイプ image/x-portable-graymap の検証に失敗しました。
12628 0 12628 1 12628 2	コンテンツ タイプ image/jpeg のヘッダー チェック。 コンテンツ タイプ image/jpeg のメッセージ長が無効です。 コンテンツ タイプ image/jpeg の検証に失敗しました。
12629 0 12629 1	コンテンツ タイプ image/cgf のヘッダー チェック。 コンテンツ タイプ image/cgf のメッセージ長が無効です。
12631 0 12631 1	コンテンツ タイプ image/x-xpm のヘッダー チェック。 コンテンツ タイプ image/x-xpm のメッセージ長が無効です。
12633 0 12633 1 12633 2	コンテンツ タイプ audio/midi のヘッダー チェック。 コンテンツ タイプ audio/midi のメッセージ長が無効です。 コンテンツ タイプ audio/midi の検証に失敗しました。
12634 0 12634 1 12634 2	コンテンツ タイプ audio/basic のヘッダー チェック。 コンテンツ タイプ audio/basic のメッセージ長が無効です。 コンテンツ タイプ audio/basic の検証に失敗しました。
12635 0 12635 1 12635 2	コンテンツ タイプ audio/mpeg のヘッダー チェック。 コンテンツ タイプ audio/mpeg のメッセージ長が無効です。 コンテンツ タイプ audio/mpeg の検証に失敗しました。

表 5-2　定義コンテンツ タイプ シグニチャ（続き）

シグニチャ ID	シグニチャの説明
12636 0	コンテンツ タイプ audio/x-adpcm のヘッダー チェック。
12636 1	コンテンツ タイプ audio/x-adpcm のメッセージ長が無効です。
12636 2	コンテンツ タイプ audio/x-adpcm の検証に失敗しました。
12637 0	コンテンツ タイプ audio/x-aiff のヘッダー チェック。
12637 1	コンテンツ タイプ audio/x-aiff のメッセージ長が無効です。
12637 2	コンテンツ タイプ audio/x-aiff の検証に失敗しました。
12638 0	コンテンツ タイプ audio/x-ogg のヘッダー チェック。
12638 1	コンテンツ タイプ audio/x-ogg のメッセージ長が無効です。
12638 2	コンテンツ タイプ audio/x-ogg の検証に失敗しました。
12639 0	コンテンツ タイプ audio/x-wav のヘッダー チェック。
12639 1	コンテンツ タイプ audio/x-wav のメッセージ長が無効です。
12639 2	コンテンツ タイプ audio/x-wav の検証に失敗しました。
12641 0	コンテンツ タイプ text/html のヘッダー チェック。
12641 1	コンテンツ タイプ text/html のメッセージ長が無効です。
12641 2	コンテンツ タイプ text/html の検証に失敗しました。
12642 0	コンテンツ タイプ text/css のヘッダー チェック。
12642 1	コンテンツ タイプ text/css のメッセージ長が無効です。
12643 0	コンテンツ タイプ text/plain のヘッダー チェック。
12643 1	コンテンツ タイプ text/plain のメッセージ長が無効です。
12644 0	コンテンツ タイプ text/plain のヘッダー チェック。
12644 1	コンテンツ タイプ text/richtext のメッセージ長が無効です。
12645 0	コンテンツ タイプ text/sgml のヘッダー チェック。
12645 1	コンテンツ タイプ text/sgml のメッセージ長が無効です。
12645 2	コンテンツ タイプ text/sgml の検証に失敗しました。
12646 0	コンテンツ タイプ text/xml のヘッダー チェック。
12646 1	コンテンツ タイプ text/xml のメッセージ長が無効です。
12646 2	コンテンツ タイプ text/xml の検証に失敗しました。
12648 0	コンテンツ タイプ video/flc のヘッダー チェック。
12648 1	コンテンツ タイプ video/flc のメッセージ長が無効です。
12648 2	コンテンツ タイプ video/flc の検証に失敗しました。
12649 0	コンテンツ タイプ video/mpeg のヘッダー チェック。
12649 1	コンテンツ タイプ video/mpeg のメッセージ長が無効です。
12649 2	コンテンツ タイプ video/mpeg の検証に失敗しました。
12650 0	コンテンツ タイプ text/xmcd のヘッダー チェック。
12650 1	コンテンツ タイプ text/xmcd のメッセージ長が無効です。
12651 0	コンテンツ タイプ video/quicktime のヘッダー チェック。
12651 1	コンテンツ タイプ video/quicktime のメッセージ長が無効です。
12651 2	コンテンツ タイプ video/quicktime の検証に失敗しました。
12652 0	コンテンツ タイプ video/sgi のヘッダー チェック。
12652 1	コンテンツ タイプ video/sgi の検証に失敗しました。
12653 0	コンテンツ タイプ video/x-avi のヘッダー チェック。
12653 1	コンテンツ タイプ video/x-avi のメッセージ長が無効です。
12654 0	コンテンツ タイプ video/x-fli のヘッダー チェック。
12654 1	コンテンツ タイプ video/x-fli のメッセージ長が無効です。
12654 2	コンテンツ タイプ video/x-fli の検証に失敗しました。

表 5-2　定義コンテンツ タイプ シグニチャ（続き）

シグニチャ ID	シグニチャの説明
12655 0	コンテンツ タイプ video/x-mng のヘッダー チェック。
12655 1	コンテンツ タイプ video/x-mng のメッセージ長が無効です。
12655 2	コンテンツ タイプ video/x-mng の検証に失敗しました。
12656 0	コンテンツ タイプ application/x-msvideo のヘッダー チェック。
12656 1	コンテンツ タイプ application/x-msvideo のメッセージ長が無効です。
12656 2	コンテンツ タイプ application/x-msvideo の検証に失敗しました。
12658 0	コンテンツ タイプ application/ms-word のヘッダー チェック。
12658 1	コンテンツ タイプ application/ms-word のメッセージ長が無効です。
12659 0	コンテンツ タイプ application/octet-stream のヘッダー チェック。
12659 1	コンテンツ タイプ application/octet-stream のメッセージ長が無効です。
12660 0	コンテンツ タイプ application/postscript のヘッダー チェック。
12660 1	コンテンツ タイプ application/postscript のメッセージ長が無効です。
12660 2	コンテンツ タイプ application/postscript の検証に失敗しました。
12661 0	コンテンツ タイプ application/vnd.ms-excel のヘッダー チェック。
12661 1	コンテンツ タイプ application/vnd.ms-excel のメッセージ長が無効です。
12662 0	コンテンツ タイプ application/vnd.ms-powerpoint のヘッダー チェック。
12662 1	コンテンツ タイプ application/vnd.ms-powerpoint のメッセージ長が無効です。
12663 0	コンテンツ タイプ application/zip のヘッダー チェック。
12663 1	コンテンツ タイプ application/zip のメッセージ長が無効です。
12663 2	コンテンツ タイプ application/zip の検証に失敗しました。
12664 0	コンテンツ タイプ application/x-gzip のヘッダー チェック。
12664 1	コンテンツ タイプ application/x-gzip のメッセージ長が無効です。
12664 2	コンテンツ タイプ application/x-gzip の検証に失敗しました。
12665 0	コンテンツ タイプ application/x-java-archive のヘッダー チェック。
12665 1	コンテンツ タイプ application/x-java-archive のメッセージ長が無効です。
12666 0	コンテンツ タイプ application/x-java-vm のヘッダー チェック。
12666 1	コンテンツ タイプ application/x-java-vm のメッセージ長が無効です。
12667 0	コンテンツ タイプ application/pdf のヘッダー チェック。
12667 1	コンテンツ タイプ application/pdf のメッセージ長が無効です。
12667 2	コンテンツ タイプ application/pdf の検証に失敗しました。
12668 0	コンテンツ タイプ unknown のヘッダー チェック。
12668 1	コンテンツ タイプ unknown のメッセージ長が無効です。
12669 0	コンテンツ タイプ image/x-bitmap のヘッダー チェック。
12669 1	コンテンツ タイプ image/x-bitmap のメッセージ長が無効です。
12673 0	認識されるコンテンツ タイプ

AIC 転送符号化シグニチャ

転送符号化に関連するポリシーは 3 つあります。

- アクションを各メソッドと関連付ける（Define Transfer Encoding）
- センサーによって認識されたメソッドをリストする（Recognized Transfer Encodings）
- チャンク符号化エラーが検出された場合に、どのアクションを実行するかを指定する（Chunked Transfer Encoding Error）

表 5-3 は、事前定義済みの転送符号化シグニチャを示しています。必要な事前定義済み転送符号化メソッドがあるシグニチャをイネーブルにします。シグニチャをイネーブルにする手順は、P.5-22 の「シグニチャのイネーブル化とディセーブル化」を参照してください。

表 5-3　転送符号化シグニチャ

シグニチャ ID	転送符号化メソッド
12686	Recognized Transfer Encoding
12687	Define Transfer Encoding Deflate
12688	Define Transfer Encoding Identity
12689	Define Transfer Encoding Compress
12690	Define Transfer Encoding GZIP
12693	Define Transfer Encoding Chunked
12694	Chunked Transfer Encoding Error

AIC FTP コマンド シグニチャ

表 5-4 は、事前定義済みの FTP コマンド シグニチャを示しています。必要な事前定義 FTP コマンドを持つシグニチャをイネーブルにします。シグニチャをイネーブルにする手順は、P.5-22 の「シグニチャのイネーブル化とディセーブル化」を参照してください。

表 5-4　FTP コマンド シグニチャ

シグニチャ ID	FTP コマンド
12900	認識されていない FTP コマンド
12901	FTP コマンド abor の定義
12902	FTP コマンド acct の定義
12903	FTP コマンド allo の定義
12904	FTP コマンド appe の定義
12905	FTP コマンド cdup の定義
12906	FTP コマンド cwd の定義
12907	FTP コマンド dele の定義
12908	FTP コマンド help の定義
12909	FTP コマンド list の定義
12910	FTP コマンド mkd の定義
12911	FTP コマンド mode の定義
12912	FTP コマンド nlst の定義
12913	FTP コマンド noop の定義
12914	FTP コマンド pass の定義
12915	FTP コマンド pasv の定義

表 5-4　FTP コマンド シグニチャ（続き）

シグニチャ ID	FTP コマンド
12916	FTP コマンド port の定義
12917	FTP コマンド pwd の定義
12918	FTP コマンド quit の定義
12919	FTP コマンド rein の定義
12920	FTP コマンド rest の定義
12921	FTP コマンド retr の定義
12922	FTP コマンド rmd の定義
12923	FTP コマンド rnfr の定義
12924	FTP コマンド rnto の定義
12925	FTP コマンド site の定義
12926	FTP コマンド smnt の定義
12927	FTP コマンド stat の定義
12928	FTP コマンド stor の定義
12929	FTP コマンド stou の定義
12930	FTP コマンド stru の定義
12931	FTP コマンド syst の定義
12932	FTP コマンド type の定義
12933	FTP コマンド user の定義

アプリケーション ポリシーの設定

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。

アプリケーション ポリシーのパラメータを設定するには、次の手順を実行します。

ステップ 1　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

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

Miscellaneous パネルが表示されます。

ステップ 3　Application Policy で、**Enable HTTP** の横にある緑色のアイコンをクリックし、**Yes** を選択して HTTP トラフィックの検査をイネーブルにします。

ステップ 4　**Max HTTP Requests** の横にある緑色のアイコンをクリックし、サーバからの応答を受信していない未処理状態の未処理 HTTP 要求の数（1 接続あたり）を指定します。

ステップ 5　**AIC Web Ports** の横にある緑色のアイコンをクリックし、アクティブにするポートを指定します。

ステップ 6　**Enable FTP** の横にある緑色のアイコンをクリックし、**Yes** を選択して FTP トラフィックの検査をイネーブルにします。

（注）　HTTP または FTP のアプリケーション ポリシーをイネーブルにすると、トラフィックが RFC に準拠しているかどうかセンサーがチェックします。

ヒント　**Reset** をクリックして、変更を削除します。

ステップ 7　変更を適用し、変更したコンフィギュレーションを保存するには、**Apply** をクリックします。

認識済みの定義コンテンツ タイプ（MIME）シグニチャの例

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。

次の例は、Recognized Content Type（MIME）シグニチャをチューニングする方法を示しています。

シグニチャ 12623 1（コンテンツ タイプ イメージ /tiff のメッセージ長が無効）などの MIME タイプのポリシー シグニチャをチューニングするには、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 > Signature Configuration** をクリックします。

Signature Configuration パネルが表示されます。

ステップ 3　Select By ボックスで、**Engine** を選択します。

ステップ 4　Select Engine ボックスで、**AIC HTTP** を選択します。

ステップ 5　リストをスクロール ダウンして Sig ID 12623 1 を選択し、**Edit** をクリックします。

Edit Signature ダイアログボックスが表示されます。

ステップ 6　Status で、Enabled の横にある緑色のアイコンをクリックし、**Yes** を選択します。

ステップ 7　Content Type Details の横にある緑色のアイコンをクリックし、次のいずれかのオプション、たとえば **Length** を選択します。

ステップ 8　**Length** フィールドで、デフォルトを 30,000 に変更し、長さの値を小さくします。

ステップ 9　**OK** をクリックします。

ステップ 10　**Apply** をクリックして変更内容を保存するか、**Reset** をクリックして変更内容を廃棄します。

IP フラグメント再構成の設定

この項では、IP フラグメント再構成について説明し、設定可能なパラメータを持つ IP フラグメント再構成シグニチャを示し、それらの設定方法について説明します。シグニチャ エンジンの詳細については、P.B-16 の「Normalizer エンジン」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。

概要

センサーは、複数のパケットにわたってフラグメント化されたデータグラムを再構成するように設定できます。このとき、センサーが再構成するデータグラム フラグメントの数と、データグラムについてさらにフラグメントが届くのを待つ時間を判断するために使用する境界値を指定できます。これは、センサーがフレーム送信を受信できなかったり、無作為にフラグメント化されたデータグラムを生成する攻撃が仕掛けられているために完全に再組み立てができなくなっているデータグラムに、センサーのリソースをすべて割り当ててしまわないようにするためのものです。

IP フラグメント再構成はシグニチャごとに設定します。

IP フラグメント再構成と設定可能なパラメータ

表 5-5 は、IP フラグメント再構成用に設定可能なパラメータを持つ IP フラグメント再構成シグニチャを示しています。IP フラグメント再構成シグニチャは、Normalizer エンジンの一部です。

表 5-5　IP フラグメント再構成シグニチャ

IP フラグメント再構成シグニチャ	デフォルト値のあるパラメータ
1200 IP Fragmentation Buffer Full	最大フラグメント 10000 を指定
1201 IP Fragment Overlap	なし
1202 IP Fragment Overrun - Datagram Too Long	最大データグラム サイズ 65536 を指定
1203 IP Fragment Overwrite - Data is Overwritten	なし
1204 IP Fragment Missing Initial Fragment	なし
1205 IP Fragment Too Many Datagrams	最大部分データグラム 1000 を指定
1206 IP Fragment Too Small	小さいフラグメントの最大値 2 を指定 最小フラグメント サイズ 400 を指定
1207 IP Fragment Too Many Datagrams	データグラムごとの最大フラグメント 170 を指定
1208 IP Fragment Incomplete Datagram	フラグメント再構成タイムアウト 60 を指定
1220 Jolt2 Fragment Reassembly DoS attack	最後のフラグメントの最大値 4 を指定
1225 Fragment Flags Invalid	なし

IP フラグメント再構成シグニチャの設定

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。

特定のシグニチャに対して IP フラグメント再構成パラメータを設定するには、次の手順を実行します。

ステップ 1　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

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

ステップ 3　Select By ボックスで、**Engine** を選択します。

ステップ 4　Select Engine ボックスで、**Normalizer** を選択します。

ステップ 5　リストから設定する IP フラグメント再構成シグニチャ、たとえば Sig ID 1200 SubSig 0 などを選択し、**Edit** をクリックします。

Edit Signature ダイアログボックスが表示されます。

ステップ 6　シグニチャ 1200 の設定可能な IP フラグメント再構成パラメータのデフォルト設定を変更します。たとえば、**Max Fragments** の横にある緑色のアイコンをクリックし、設定をデフォルトの 10000 から 20000 に変更します。

シグニチャ 1200 では、次のオプションのパラメータを変更できます。

- **Specify TCP Idle Timeout**
- **Specify Service Ports**
- **Specify SYN Flood Max Embryonic**

ヒント　**Reset** をクリックして、変更を削除します。

ステップ 7　**Apply** をクリックし、変更を適用して、変更された設定を保存します。

IP フラグメント再構成方法の設定

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。

センサーが IP フラグメント再構成に使用する方法を設定するには、次の手順を実行します。

（注）　このオプションは、センサーが混合モードで動作しているときに設定できます。センサーがラインモードで動作している場合、このメソッドは NT 専用です。

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 > Miscellaneous** をクリックします。

Miscellaneous パネルが表示されます。

ステップ 3　Fragment Reassembly で、**IP Reassembly Mode** の横にある緑色のアイコンをクリックし、フラグメントの再構成に使用するオペレーティング システムを選択します。

ヒント　**Reset** をクリックして、変更を削除します。

ステップ 4　**Apply** をクリックし、変更を適用して、変更された設定を保存します。

TCP ストリーム再構成の設定

この項では、TCP ストリーム再構成について説明し、設定可能なパラメータを持つ TCP ストリーム再構成シグニチャを示し、TCP ストリーム シグニチャの設定方法と TCP ストリーム再構成のモードの設定方法について説明します。シグニチャ エンジンの詳細については、P.B-16 の「Normalizer エンジン」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。

概要

センサーは、完全な 3 ウェイ ハンドシェイクによって確立された TCP セッションだけを監視するように設定できます。また、ハンドシェイクの完了まで待つ時間の最大値と、パケットがない場合に接続を監視し続ける時間も設定できます。これは、有効な TCP セッションが確立していないときにセンサーがアラートを生成しないようにするためのものです。センサーに対する攻撃には、単純に攻撃を繰り返すだけでセンサーにアラートを生成させようとするものがあります。TCP セッションの再組み立て機能は、センサーに対するこのような攻撃の緩和に役立ちます。

TCP ストリーム再構成パラメータは、シグニチャごとに設定します。TCP ストリーム再構成のモードを設定できます。

TCP ストリーム再構成シグニチャと設定可能なパラメータ

表 5-6 は、TCP ストリーム再構成用に設定可能なパラメータを持つ TCP ストリーム再構成シグニチャを示しています。TCP ストリーム再構成シグニチャは、Normalizer エンジンの一部です。

表 5-6　TCP ストリーム再構成シグニチャ

TCP ストリーム再構成シグニチャ	デフォルト値のあるパラメータ
1300 TCP Segment Overwrite	なし
1301 TCP Session Inactivity Timeout	tcp-idle-timeout 3600
1302 TCP Session Embryonic Timeout	tcp-embryonic-timeout 15
1303 TCP Session Closing Timeout	tcp-closed-timeout 5
1304 TCP Session Packet Queue Overflow	tcp-max-queue 32
1305 TCP Urgent Flag Set	なし
1306 0 TCP Option Others 1306 1 TCP SACK Allowed Option 1306 2 TCP SACK Data Option 1306 3 TCP Timestamp Option 1306 4 TCP Window Scale Option 1306 5 TCP MSS Option	tcp-option-number 6-7,9-255

表 5-6　TCP ストリーム再構成シグニチャ（続き）

TCP ストリーム再構成シグニチャ	デフォルト値のあるパラメータ
1307 TCP Window Size Variation	なし
1308 TTL Evasion	なし
1309 TCP Reserved Flags Set	なし
1310 TCP Retransmit Data Different	なし
1311 TCP Packet Exceeds MSS	なし
1312 TCP MSS Below Minimum	tcp-min-mss 400
1313 TCP MSS Exceed Maximum	tcp-max-mss 1460
1314 TCP SYN Packet with Data	なし
1330[1] 0 TCP Drop - Bad Checksum 1330 1 TCP Drop - Bad TCP Flags 1330 2 TCP Drop - Urgent Pointer Without Flag 1330 3 TCP Drop - Bad Option List 1330 4 TCP Drop - Bad Option Length 1330 5 TCP Drop - MSS Option in Non-SYN 1330 6 TCP Drop - WinScale Option in Non-SYN 1330 7 TCP Drop - Bad WinScale Option Value 1330 8 TCP Drop - Bad SACK Allow 1330 9 TCP Drop - Data in SYN|ACK 1330 10 TCP Drop - Data Past FIN 1330 11 TCP Drop - Timestamp not Allowed 1330 12 TCP Drop - Segment Out of Order 1330 13 TCP Drop - Invalid TCP Packet 1330 14 TCP Drop - RST or SYN in window 1330 15 TCP Drop - Segment Already ACKed by Peer 1330 16 TCP Drop - PAWS Check Failed 1330 17 TCP Drop - Segment out of State Order 1330 18 TCP Drop - Segment out of Window	なし
3050 Half Open SYN Attack	syn-flood-max-embryonic 5000
3250 TCP Hijack	max-old-ack 200
3251 TCP Hijack Simplex Mode	max-old-ack 100

1. これらのサブシグニチャは、正規化エンジンが TCP パケットをドロップする理由を示しています。デフォルトでは、これらのサブシグニチャはパケットをドロップします。これらのサブシグニチャを使用すると、正規化エンジンで検査に合格しなかったパケットに IPS を通過させることができます。ドロップの理由は、TCP 統計情報内にエントリがあります。デフォルトでは、これらのサブシグニチャはアラートを生成しません。

TCP ストリーム再構成シグニチャの設定

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。

特定のシグニチャに対して TCP ストリーム再構成パラメータを設定するには、次の手順を実行します。

ステップ 1　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

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

ステップ 3　Select By ボックスで、**Engine** を選択します。

ステップ 4　Select Engine ボックスで、**Normalizer** を選択します。

ステップ 5　リストから設定する TCP フラグメント再構成シグニチャ、たとえば Sig ID 1313 SubSig 0 などを選択し、**Edit** をクリックします。

Edit Signature ダイアログボックスが表示されます。

ステップ 6　シグニチャ 1313 の設定可能な IP フラグメント再構成パラメータのデフォルト設定を変更します。たとえば、**TCP Max MSS** の横にある緑色のアイコンをクリックし、設定をデフォルトの 1460 から 1380 に変更します。

（注）　このパラメータをデフォルトの 1460 から 1380 へ変更すると、VPN トンネルを通過するトラフィックのフラグメント化を防ぐことができます。

シグニチャ 1313 0 では、次のオプションのパラメータを変更できます。

- Specify Hijack Max Old Ack
- Specify TCP Idle Timeout
- Specify Service Ports
- Specify SYN Flood Max Embryonic

ヒント　**Reset** をクリックして、変更を削除します。

ステップ 7　**Apply** をクリックし、変更を適用して、変更された設定を保存します。

TCP ストリーム再構成モードの設定

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。

TCP ストリーム再構成モードを設定するには、次の手順を実行します。

ステップ 1　管理者特権またはオペレータ特権を持つアカウントを使用して IDM にログインします。

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

Miscellaneous パネルが表示されます。

ステップ 3　Stream Reassembly で、**TCP Handshake Required** の横にある緑色のアイコンをクリックし、**yes** を選択します。

TCP Handshake Required を選択すると、3 ウェイ ハンドシェイクが完了したセッションのみをセンサーが追跡するように指定します。

ステップ 4　**TCP Reassembly Mode** の横にある緑色のアイコンをクリックし、センサーが TCP セッションの再構成に使用するモードを選択します。

- **Asymmetric**：センサーが、トラフィック　フローの状態と同期をとり、双方向のうち一方向だけでよいエンジンの検査を継続するようにします。
- **Strict**：何らかの理由でパケットを受信しなかった場合でも、以後のパケットをすべて処理します。
- **Loose**：パケットが廃棄される可能性がある場合に使用します。

ヒント　**Reset** をクリックして、変更を削除します。

ステップ 5　**Apply** をクリックし、変更を適用して、変更された設定を保存します。

IP ロギングの設定

センサーが攻撃を検出したときに、IP セッション ログを生成するように設定できます。シグニチャの応答アクションとして IP ロギングが設定されているときにシグニチャが反応すると、アラートの送信元アドレスとの間で送受信されるすべてのパケットがログに記録されます。

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、パラメータが現在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。

IP ロギングのパラメータを設定するには、次の手順を実行します。

（注） センサーは、IP ロギング条件のいずれかを検出すると、IP ロギングを停止します。

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 > Miscellaneous** をクリックします。

Miscellaneous パネルが表示されます。

ステップ 3　IP Log で、**Max IP Log Packets** の横にある緑色のアイコンをクリックし、ログを作成するパケットの数を指定します。

ステップ 4　**IP Log Time** の横にある緑色のアイコンをクリックし、ログを作成する時間を指定します。

有効な値は、1 ～ 60 分です。デフォルトは 30 分です。

ステップ 5　**Max IP Log Bytes** の横にある緑色のアイコンをクリックし、ログを作成する最大バイト数を指定します。

ヒント　**Reset** をクリックして、変更を削除します。

ステップ 6　**Apply** をクリックし、変更を適用して、変更された設定を保存します。

MEG シグニチャの例

Meta エンジンは、スライドする時間間隔内で、関連する方法で発生するイベントを定義します。このエンジンは、パケットではなくイベントを処理します。シグニチャ イベントが生成されると、Meta エンジンがそれらを検査して、1 つまたはいくつかの Meta 定義と一致するかどうかを判別します。Meta エンジンは、このイベントに対するすべての要件が満たされた後に、シグニチャ イベントを生成します。

シグニチャ イベントはすべて SEAP によって Meta エンジンに渡されます。SEAP は、minimum hits オプションを処理した後で、イベントを渡します。要約とイベント アクションは、Meta エンジンがコンポーネント イベントを処理した後に処理されます。SEAP の詳細については、P.7-4 の「Signature Event Action Processor」を参照してください。

注意　多数の Meta シグニチャが、意図せずセンサー パフォーマンス全体に影響を及ぼす可能性があります。

次の例は、Meta エンジンに基づいて MEG シグニチャを作成する方法を示しています。

たとえば、シグニチャ 64000 のサブシグニチャ 0 は、同一送信元アドレスでシグニチャ 2000 のサブシグニチャ 0 とシグニチャ 3000 のサブシグニチャ 0 からのアラートを確認すると、反応します。送信元アドレス選択は、メタ キーのデフォルト値 Axxx の結果です。メタ キー設定を xxBx（宛先アドレス）に変更することによって、動作を変更できます。たとえば、次のようになります。

ヒント　メタ エンジンは、ほとんどのエンジンが入力としてパケットを取るのに対し、入力としてアラートを取る点で、その他のエンジンとは異なります。Meta エンジンの詳細については、P.B-14 の「Meta エンジン」を参照してください。

メタ エンジンに基づいて MEG シグニチャを作成するには、次の手順を実行します。

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、パラメータが現在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 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 > Signature Configuration** をクリックします。

Signature Configuration パネルが表示されます。

ステップ 3　**Add** をクリックして、Add Signature ダイアログボックスを開きます。

ステップ 4　**Signature** フィールドで新しいシグニチャに一意のシグニチャ ID を指定します。

ステップ 5　**Subsignature** フィールドで新しいシグニチャに一意のサブシグニチャ ID を指定します。

ステップ 6　**Alert Severity** フィールドの隣にある緑のアイコンをクリックし、シグニチャに関連付ける重大度を選択します。

ステップ 7　**Signature Fidelity Rating** フィールドの隣にある緑のアイコンをクリックし、シグニチャのシグニチャ忠実度評価を表す値（1 ～ 100）を指定します。

ステップ 8　**Promiscuous Delta** フィールドの値は、デフォルトのままにしておいてください。

ステップ 9　シグニチャ説明フィールドにシグニチャに関するコメントを入力します。

ステップ 10　**Engine** フィールドで Meta を選択します。

ステップ 11　Meta エンジン固有のパラメータを設定します。

a. **Meta Reset Interval** フィールドの横にある緑色のアイコンをクリックし、Meta シグニチャをリセットする時間を秒単位で指定します。

   有効な範囲は 0 ～ 3600 秒です。デフォルトは 60 秒です。

b. **Meta Key** リストから、Meta シグニチャのストレージ タイプを選択します。
   - 攻撃者のアドレス
   - 攻撃者アドレスと被害先アドレス
   - 攻撃者と被害先のアドレスおよびポート
   - 被害先のアドレス

c. **Component List** の横にある鉛筆のアイコンをクリックし、新しい MEG シグニチャを挿入します。

   Component List ダイアログボックスが表示されます。

d. **Add** をクリックして、最初の MEG シグニチャを挿入します。

   Add List Entry ダイアログボックスが表示されます。

e. **Entry Key** フィールドで、Entry1 のようにエントリの名前を指定します。

   デフォルトは MyEntry です。

f. Component Group の下の **Component Count** フィールドで、このコンポーネントが何回反応したら満たされるかを指定します。

g. Component Group の下の **Component Sig ID** フィールドで、このコンポーネントを照合するシグニチャのシグニチャ ID を指定します（この例では 2000）。

h. Component Group の下の **Component SubSig ID** フィールドで、このコンポーネントを照合するシグニチャのサブシグニチャ ID を指定します（この例では 0）。

i. **OK** をクリックします。

   Add List Entry ダイアログボックスが再び表示されます。

j. エントリを強調表示し、**Select** をクリックしてそれを Selected Entries リストに移動します。

k. **OK** をクリックします。

l. **Add** をクリックして、次の MEG シグニチャを挿入します。

Add List Entry ダイアログボックスが表示されます。

m. **Entry Key** フィールドで、Entry2 のようにエントリの名前を指定します。

n. Component Group の下の **Component Count** フィールドで、このコンポーネントが何回反応したら満たされるかを指定します。

o. Component Group の下の **Component Sig ID** フィールドで、このコンポーネントを照合するシグニチャのシグニチャ ID を指定します（この例では 3000）。

p. Component Group の下の **Component SubSig ID** フィールドで、このコンポーネントを照合するシグニチャのサブシグニチャ ID を指定します（この例では 0）。

q. **OK** をクリックします。

Add List Entry ダイアログボックスが再び表示されます。

r. エントリを強調表示し、**Select** をクリックしてそれを Selected Entries リストに移動します。

s. 新しいエントリを強調表示し、**Move Up** または **Move Down** をクリックして新しいエントリの順序を決めます。

ヒント　**Reset Ordering** をクリックすると、エントリは Entry Key リストに戻ります。

t. **OK** をクリックします。

u. **Component List in Order** フィールドの横にある緑色のアイコンをクリックし、**Yes** を選択してコンポーネント リストを順序どおりに並べます。

ステップ 12　**Event Action** フィールドの横にある緑色のアイコンをクリックし、センサーがイベントに応答するときに起こすアクションを選択します。

ヒント　複数のアクションを選択するには、**Ctrl** キーを押してすべてのアクションが選択された状態にします。

ステップ 13　イベントをカウントする場合は、Event Counter の下にある **Event Counter** フィールドを設定します。

ステップ 14　Alert Frequency の下にある **Alert Frequency** フィールドで、アラートを受信する方法を指定します。

ステップ 15　Status の下で **Yes** を選択し、シグニチャをイネーブルにします。

（注）　シグニチャによって指定された攻撃をセンサーがアクティブに検出できるようにするには、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 16　Status の下で、シグニチャをリタイアにするかどうかを指定します。**No** をクリックして、シグニチャをアクティブにします。これによってシグニチャがエンジンに組み込まれます。

（注）　シグニチャによって指定された攻撃をセンサーがアクティブに検出できるようにするには、シグニチャをアクティブにする必要があります。

ヒント　変更を元に戻し、Add Signature ダイアログを閉じるには、**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 に設定された新しいシグニチャがリストに現れます。

ヒント　変更を元に戻す場合は、**Reset** をクリックします。

ステップ 18　**Apply** をクリックし、変更を適用して、変更された設定を保存します。