CHAPTER 9

シグニチャの定義

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

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

この章では、シグニチャ定義ポリシーの作成方法とシグニチャの設定方法について説明します。内容は次のとおりです。

セキュリティ ポリシーの概要

（注） AIM IPS、AIP SSC-5、および NME IPS は、複数のポリシーの適用をサポートしていません。

複数のセキュリティ ポリシーを作成し、個々の仮想センサーに適用することができます。セキュリティ ポリシーは、シグニチャ定義ポリシー、イベント アクション規則ポリシー、および異常検出ポリシーで構成されます。Cisco IPS には、デフォルトのシグニチャ定義（sig0）、デフォルトのイベント アクション規則ポリシー（rules0）、およびデフォルトの異常検出ポリシー（ad0）が含まれています。仮想センサーにデフォルトのポリシーを割り当てることもできれば、新しいポリシーを作成することも可能です。複数のセキュリティ ポリシーを使用することにより、さまざまな要件に基づくセキュリティ ポリシーを作成し、そのカスタマイズしたポリシーを個々の VLAN または物理インターフェイスに適用できます。

シグニチャ定義ポリシーの設定

ここでは、シグニチャ定義ポリシーの設定方法について説明します。内容は次のとおりです。

[Signature Definitions] ペイン

（注）　シグニチャ ポリシーを追加、クローニング、または削除するためには、管理者またはオペレータであることが必要です。

注意　AIM IPS、AIP SSC-5、および NME IPS は、センサーの仮想化をサポートしていないため、複数のポリシーをサポートしません。

[Signature Definitions] ペインでは、シグニチャ定義ポリシーを追加、クローニング、削除できます。デフォルトのシグニチャ定義ポリシーは sig0 です。ポリシーを追加すると、センサーに制御トランザクションが送信され、ポリシー インスタンスが作成されます。応答が成功した場合は、[Signature Definitions] に新しいポリシー インスタンスが追加されます。リソースの制限などにより、制御トランザクションが失敗した場合は、エラー メッセージが表示されます。

プラットフォームが仮想ポリシーをサポートしていない場合は、コンポーネントごとに 1 つのインスタンスしか追加できず、新しいインスタンスを作成したり既存のインスタンスを削除したりすることはできません。この場合、[Add]、[Clone]、および [Delete] ボタンは使用できません。

[Signature Definitions] ペインのフィールド定義

[Signature Definitions] ペインには次のフィールドがあります。

- [Policy Name]：このシグニチャ定義ポリシーの名前を示します。
- [Assigned Virtual Sensor]：このシグニチャ定義ポリシーを割り当てる仮想センサーを示します。

[Add Policy] および [Clone Policy] ダイアログボックスのフィールド定義

[Add Policy] および [Clone Policy] ダイアログボックスには次のフィールドがあります。

- [Name]：仮想センサーの名前。デフォルトの仮想センサーは vs0 です。
- [Assigned Interfaces (or Pairs)]：この仮想センサーに属するインターフェイスまたはインターフェイス ペア。
- [Signature Definition Policy]：この仮想センサーのシグニチャ定義ポリシーの名前。デフォルトのシグニチャ定義ポリシーは sig0 です。

- [Event Action Override Policy]：この仮想センサーのイベント アクション規則オーバーライド ポリシーの名前。デフォルトのイベント アクション規則ポリシーは rules0 です。
  - [Risk Rating]：このイベント アクション オーバーライドを起動するために使用するリスク レーティング範囲（low、medium、または high risk）を示します。
  - [Actions to Add]：このイベント アクション オーバーライドの条件が満たされている場合にイベントに追加されるイベント アクションを指定します。
  - [Enabled]：このイベント アクション オーバーライド ポリシーがイネーブルかどうかを示します。
- [Anomaly Detection Policy]：この仮想センサーの異常検出ポリシーの名前。デフォルトの異常検出ポリシーは ad0 です。
- [Description]：この仮想センサーの説明。

シグニチャ ポリシーの追加、クローニング、削除

シグニチャ定義ポリシーを追加、クローニング、または削除するには、次の手順を実行します。

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

ステップ 2　[Configuration] > *sensor_name* > [Policies] > [Signature Definitions] の順に選択し、[Add] をクリックします。

ステップ 3　[Policy Name] フィールドに、シグニチャ定義ポリシーの名前を入力します。

ヒント　変更内容を破棄して [Add Policy] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 4　[OK] をクリックします。シグニチャ定義ポリシーが [Signature Definitions] ペインのリストに表示されます。

ステップ 5　既存のシグニチャ定義ポリシーをクローニングするには、リストで選択し、[Clone] をクリックします。[Clone Policy] ダイアログボックスが表示され、既存のシグニチャ定義ポリシー名の後に「_copy」が追加されます。

ステップ 6　[Policy Name] フィールドに、一意の名前を入力します。

ヒント　変更内容を破棄して [Clone Policy] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 7　[OK] をクリックします。クローニングしたシグニチャ定義ポリシーが [Signature Definitions] ペインのリストに表示されます。

ステップ 8　シグニチャ定義ポリシーを削除するには、ポリシーを選択し、[Delete] をクリックします。そのポリシーを完全に削除するかどうかを確認する [Delete Policy] ダイアログボックスが表示されます。

注意　デフォルトのシグニチャ定義ポリシー sig0 は削除できません。

ステップ 9　[Yes] をクリックします。

シグニチャ定義ポリシーが [Signature Definitions] ペインのリストに表示されなくなります。

[sig0] ペイン

左側のナビゲーション ペインにある [sig0] メニューには、シグニチャのリストが、アクティブなシグニチャ、シグニチャ タイプ、すべてのシグニチャなど、カテゴリごとに一覧表示されています。メニューでシグニチャ タイプを選択すると、[sig0] ペインにシグニチャを設定するためのツールが表示されます。シグニチャはさまざまなカテゴリでフィルタできます。たとえば、シグニチャ ID、シグニチャ名、シグニチャがイネーブルかどうか、重大度、充実度レーティング、基本リスク レーティング、アクション、タイプ、エンジンなどです。

（注） シグニチャの設定を確認したり、シグニチャを追加、クローニング、編集するには、シグニチャ カテゴリを選択する必要があります。

各列のデータをソートするには、列見出しをクリックします。デフォルトでは次の列が表示されています。

- [ID]
- [Name]
- [Enabled]
- [Severity]
- [Fidelity Rating]
- [Base RR]
- [Signature Actions]（Alert and Log、Deny、および Other）
- [Type]
- [Engine]
- [Retired]

  デフォルトの列表示を変更するには、ペインの右上にある [Column] アイコンをクリックし、[Choose Columns to Display] ダイアログボックスでチェックボックスをオンまたはオフにします。また、列を選択してテーブル中の別の場所にドラッグすることで、列を新しい場所に移動することもできます。

設定ボタンは次の設定アクションにグループ分けされています。

- [Signature Configuration]：イベント アクションの編集、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 デフォルトの復元、MySDN でのシグニチャ情報の表示、シグニチャの編集、追加、削除、クローニング、エクスポートが可能です。
- [Signature Wizard]：ウィザードを使用してカスタム シグニチャを作成できます。
- [Advanced]
  - [Signature Variables]：複数のシグニチャで使用するための変数を設定できます。
  - [Miscellaneous]：アプリケーション ポリシー シグニチャの設定、IP フラグメンテーションと TCP ストリームの再構成のためのモードの設定、IP ロギングの設定を行うことができます。

シグニチャについて

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によって、ネットワーク侵入を検出できます。シグニチャは、DoS 攻撃などの典型的な侵入行為を検出するためにセンサーが使用する一連の規則です。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ム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、偽陽性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、一部のネットワーク アプリケーションやオペレーティング システムは、多数の ICMP メッセージを送信することがありますが、シグニチャベースの検出システムでは、このメッセージが攻撃者によるネットワーク セグメント特定の試みであると解釈されてしまう可能性があります。シグニチャをチューニングすると、偽陽性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 トラフィックをモニタするようにセンサーを設定するには、そのシグニチャをイネーブル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更新のインストール時にイネーブルになります。イネーブルなシグニチャに一致する攻撃が検出されると、センサーはアラートを生成します。生成された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 を編集し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。

Cisco IPS には、10,000 を超えるデフォルトの組み込みシグニチャが含まれています。組み込みシグニチャのリストにあるシグニチャの名前の変更および削除はできません。ただし、シグニチャをセンシング エンジンから削除して廃棄できます。あとで廃棄されたシグニチャをアクティブにできます。ただし、このプロセスにはセンシング エンジンの設定の再構築が必要です。この再構築には時間がかかり、トラフィックの処理を遅延させ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可能です。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。

（注） 使用していないシグニチャを廃棄することを推奨します。廃棄によって、センサーのパフォーマンスが向上します。

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。いくつかの項目に対して、カスタム シグニチャを設定できます。たとえば、UDP 接続の文字列との一致やネットワーク フラッドの追跡、スキャンなどです。シグニチャは、モニタ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。

MySDN

（注）　現在、[MySDN] をクリックすると MySDN が表示されますが、最終的に IntelliShield のサイトにリダイレクトされます。

MySDN は、個々のシグニチャのための情報リポジトリです。MySDN は、シグニチャに関する次の情報を提供します。

- シグニチャ ID
- リリース バージョン
- 元のリリース日
- 最新のリリース日
- デフォルトがイネーブル
- デフォルトが廃棄
- CVE
- Bugtraq ID
- アラーム重大度
- 忠実度
- 説明
- 推奨されるフィルタ
- 良性フィルタ
- IntelliShield アラート

MySDN から得た情報は、[sig0] ペインの下半分に表示されます。リスト中でシグニチャを選択すると、下半分に情報が表示されます。または、[Configuration] > *sensor_name* > [Policies] > [Signature Definitions] > [sig0] > [Active Signatures] でシグニチャを選択し、[MySDN] をクリックします。Cisco.com にログインした後、MySDN サイトを通じて（このサイトは最終的に IntelliShield サイトになります）、そのシグニチャに関する詳細な情報が表示されます。

IME では、最後に開いたブラウザ ウィンドウで MySDN が起動されます。これは、Windows のデフォルトの設定です。このデフォルトの動作を変更するには、Internet Explorer で、[Tools] > [Internet Options] の順に選択し、[Advanced] タブをクリックします。下にスクロールし、[Reuse windows for launching shortcuts] チェックボックスをオフにします。

（注）　MySDN の Web サイトは廃止され、Cisco.com ユーザは使用できなくなりました。情報は、IME を通じてのみ入手できます。

シグニチャの設定

ここでは、シグニチャの設定方法について説明します。内容は次のとおりです。

[Sig0] ペインのフィールド定義

[Sig0] ペインには次のフィールドがあります。

- [Filter]：フィルタする属性を選択することにより、シグニチャのリストをソートできます。
- [ID]：このシグニチャおよびサブシグニチャに割り当てられた一意の数値を示します。この値により、センサーは特定のシグニチャを識別します。
- [Name]：シグニチャに割り当てられる名前を示します。
- [Enabled]：シグニチャがイネーブルかどうかを示します。シグニチャで指定されている攻撃からの保護をセンサーが提供するには、シグニチャをイネーブルにする必要があります。
- [Severity]：シグニチャによって報告される重大度レベル（[High]、[Informational]、[Low]、または [Medium]）を示します。
- [Fidelity Rating]：ターゲットに関する具体的な情報がない場合に、このシグニチャがどの程度忠実に動作するかに関連付ける重みを示します。
- [Base RR]：各シグニチャの基本リスク レーティング値を表示します。基本リスク レーティング値は、忠実度評価と重大度係数を掛け合わせたものを 100 で割ることによって（忠実度評価 × 重大度係数 /100）、IDM により自動的に計算されます。重大度係数の値は次のとおりです。
  - シグニチャの重大度レベルが High の場合、重大度係数は 100
  - シグニチャの重大度レベルが Medium の場合、重大度係数は 75
  - シグニチャの重大度レベルが Low の場合、重大度係数は 50
  - シグニチャの重大度レベルが Informational の場合、重大度係数は 25
- [Signature Actions]：このシグニチャが起動されたときにセンサーが実行するアクションを示します。

- [Type]：このシグニチャがデフォルト（組み込み）シグニチャ、チューニング済みシグニチャ、カスタム シグニチャのいずれなのかを示します。
- [Engine]：このシグニチャによって指定されたトラフィックの解析と検査を行うエンジンを示します。
- [Retired]：シグニチャが廃止されたかどうかを示します。廃棄されたシグニチャは、シグニチャ エンジンから削除されます。廃棄され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。

（注）　使用していないシグニチャを廃棄することを推奨します。廃棄によって、センサーのパフォーマンスが向上します。

ボタンと右クリック メニューの機能

- [Edit Actions]：[Edit Actions] ダイアログボックスを表示します。
- [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。
- [Set Severity To]：シグニチャによって報告される重大度レベル（[High]、[Medium]、[Low]、または [Informational]）を選択できます。
- [Restore Default]：選択したシグニチャのすべてのパラメータをデフォルト設定に戻します。
- [Show Events]：このシグニチャに関連するイベントを、最後の 10 分から、または最後の時間からリアル タイムに表示します。
- [MySDN]：そのシグニチャの説明を、Cisco.com の MySDN サイトで表示します。
- [Edit]：[Edit Signature] ダイアログボックスを開きます。[Edit Signature] ダイアログボックスでは、選択したシグニチャに関連付けられているパラメータを変更したり、シグニチャを効果的に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。
- [Add]：[Add Signature] ダイアログボックスを開きます。[Add Signature] ダイアログボックスでは、選択したシグニチャに関連付けるパラメータを追加したり、シグニチャを効果的にチューニングできます。
- [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。
- [Clone]：[Clone Signature] ダイアログボックスを開きます。[Clone Signature] ダイアログボックスでは、クローニング元として選択した既存のシグニチャのあらかじめ設定された値を変更することで、シグニチャを作成できます。
- [Change Status To]：ステータスを [Active]、[Retired]、[Low Memory Retired]、[Medium Memory Retired] に変更できます。
- [Export]：現在表示されている、テーブル内のシグニチャを、カンマ区切りの Excel ファイル（CSV を使用）または HTML ファイルにエクスポートします。また、**Ctrl-C** を使用して内容をクリップボードにコピーし、後で **Ctrl-V** を使用してメモ帳や Word に貼り付けることもできます。

[Add Signatures]、[Clone Signatures]、および [Edit Signatures] ダイアログボックスのフィールド定義

[Add Signature]、[Clone Signature]、および [Edit Signature] ダイアログボックスには次のフィールドがあります。

- [Signature Definition]
  - [Signature ID]：このシグニチャに割り当てられた一意の数値を示します。この値により、センサーは特定のシグニチャを識別します。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一意の数値を示します。サブシグニチャ ID によって、広範なシグニチャのより詳細なバージョンが識別されます。値は 0 ～ 255 です。
  - [Alert Severity]：シグニチャの重大度レベルを、[High]、[Informational]、[Low]、[Medium] から選択します。
  - [Sig Fidelity Rating]：ターゲットに関する具体的な情報がない場合に、このシグニチャをどの程度忠実に実行するかに関連付ける重みを選択します。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。

注意　シグニチャの無差別デルタ設定は変更しないことをお勧めします。

- [Sig Description]：このシグニチャを他のシグニチャから区別するのに役立つ次の属性を指定します。
  - [Signature Name]：シグニチャの名前。デフォルトは MySig です。
  - [Alert Notes]：このフィールドにアラートのメモを追加します。
  - [User Comments]：このシグニチャに関するコメントをこのフィールドに追加します。
  - [Alarm Traits]：アラームの特性をこのフィールドに追加します。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 リリースを追加します。
  - [Signature Creation Date]：このシグニチャが作成された日付。
  - [Signature Type]：シグニチャのタイプ（anomaly、component、exploit、other、vulnerability）。
- [Engine]：このシグニチャによって指定されたトラフィックの解析と検査を行うエンジンを選択できます。
- [Event Action]：イベントに応答するときにセンサーが実行するアクションを指定できます。
- [Event Counter]：センサーがイベントをカウントする方法を設定できます。たとえば、センサーが、同じシグニチャが同じアドレス セットに対して 5 回起動した場合にだけ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されるストレージ タイプ。攻撃者のアドレス、攻撃者のアドレスと攻撃対象のポート、攻撃者と攻撃対象のアドレス、攻撃者と攻撃対象のアドレスおよびポート、または攻撃対象のアドレスを選択します。デフォルトは、攻撃者のアドレスです。

  - [Specify Alert Interval]：イベント カウントをリセットするまでの時間（秒数）を指定します。ドロップダウン リストから [Yes] または [No] を選択し、時間を指定します。
- [Alert Frequency]：シグニチャが起動した場合に、センサーがアラートを送信する回数を設定できます。シグニチャに対して次のパラメータを指定します。
  - [Summary Mode]：アラートのサマライズのモード。[Fire All]、[Fire Once]、[Global Summarize]、または [Summarize] を選択します。

    （注）　適応型セキュリティ アプライアンスの複数のコンテキストが 1 つの仮想センサーに含まれている場合、サマリー アラートには、サマライズされた最後のコンテキストのコンテキスト名が含まれています。このため、このサマリーは、サマライズされるすべてのコンテキストのうち、このタイプのすべてのアラートの結果となります。
  - [Summary Interval]：各サマリー アラートで使用される時間間隔（秒数）。値は 1 ～ 65535 です。デフォルトは 15 です。
  - [Summary Key]：アラートのサマライズに使用されるストレージ タイプ。攻撃者のアドレス、攻撃者のアドレスと攻撃対象のポート、攻撃者と攻撃対象のアドレス、攻撃者と攻撃対象のアドレスおよびポート、または攻撃対象のアドレスを選択します。デフォルトは、攻撃者のアドレスです。
  - [Specify Global Summary Threshold]：アラートをグローバル サマリーにサマライズするための、イベント数のしきい値を指定できます。[Yes] または [No] を選択し、イベント数のしきい値を指定します。
- [Status]：シグニチャをイネーブルまたはディセーブルにしたり、シグニチャの廃棄または廃棄の解除を行うことができます。
  - [Enabled]：シグニチャがイネーブルかディセーブルかを選択できます。デフォルトは [yes]（イネーブル）です。
  - [Retired]：シグニチャが廃棄されているかどうかと、低メモリ廃棄と中メモリ廃棄のどちらなのかを選択できます。デフォルトは [no]（廃棄しない）です。

    低メモリ廃棄プラットフォームの最大センサー メモリは 1 GB 未満です。中メモリ廃棄プラットフォームの最大センサー メモリは、1 GB 以上 2 GB 未満です。シグニチャがロードされるとき、シグニチャをロードしているプラットフォームに基づいて廃棄の値が評価されます。
  - [Obsoletes]：このシグニチャによって廃止されるシグニチャが一覧表示されます。
  - [Vulnerable OS List]：このシグニチャの脆弱 OS を選択できます。
- [Mars Category]：シグニチャを MARS 攻撃カテゴリにマッピングします。これは、コンフィギュレーションに設定しアラートで表示できる静的な情報カテゴリです。

[Edit Actions] ダイアログボックスのフィールド定義

[Edit Actions] ダイアログボックスには、次のフィールドがあります。

- Alert and Log Actions
  - [Product Alert]：イベントをアラートとしてイベント ストアに書き込みます。

（注）　シグニチャのアラートをイネーブルにした場合、[Product Alert] アクションは自動ではありません。イベント ストアにアラートを作成するには、[Product Alert] を選択する必要があります。第 2 のアクションを追加する場合、アラートをイベント ストアに送信するには、[Product Alert] を含める必要があります。また、イベント アクションを設定するたびに、新しいリストが作成され古いリストが置き換えられます。各シグニチャに必要なすべてのイベント アクションを必ず含めてください。

（注）　[Produce Alert] イベント アクションは、グローバル相関によってイベントのリスクレーティングが増加し、[Deny Packet Inline] または [Deny Attacker Inline] のいずれかのイベント アクションが追加されたときに、イベントに追加されます。

- [Produce Verbose Alert] : 攻撃パケットの符号化されたダンプをアラートに含めます。このアクションによって、[Product Alert] が選択されていない場合でも、アラートがイベント ストアに書き込まれます。
- [Log Attacker Packets] : 攻撃者のアドレスが含まれているパケットに対する IP ロギングを開始し、アラートを送信します。このアクションによって、[Product Alert] が選択されていない場合でも、アラートがイベント ストアに書き込まれます。
- [Log Victim Packets] : 攻撃対象のアドレスが含まれているパケットに対する IP ロギングを開始し、アラートを送信します。このアクションによって、[Product Alert] が選択されていない場合でも、アラートがイベント ストアに書き込まれます。
- [Log Pair Packets] : 攻撃者と攻撃対象のアドレスのペアが含まれているパケットに対する IP ロギングを開始します。このアクションによって、[Product Alert] が選択されていない場合でも、アラートがイベント ストアに書き込まれます。
- [Request SNMP Trap] : センサーの Notification Application コンポーネントに SNMP 通知を実行するための要求を送信します。このアクションによって、[Product Alert] が選択されていない場合でも、アラートがイベント ストアに書き込まれます。このアクションを実行するには、センサーで SNMP が設定されている必要があります。

- [Deny Actions]
  - [Deny Packet Inline]（インラインのみ）: パケットを終了します。

    （注）　[Deny Packet Inline] のイベント アクション オーバーライドは、保護されているため削除できません。そのオーバーライドを使用しない場合は、ディセーブルにします。

  - [Deny Connection Inline]（インラインのみ）: TCP フローの現在のパケットおよび将来のパケットを終了します。
  - [Deny Attacker Victim Pair Inline]（インラインのみ）: 指定された期間、この攻撃者と攻撃対象のアドレスのペアについては、現在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、指定した期間と拒否攻撃者の最大数を設定するには、[Configuration] > *sensor_name* > [Policies] > [Event Action Rules] > [rules0] > [General Settings] の順に選択します。

  - [Deny Attacker Service Pair Inline]（インラインのみ）: 指定された期間、この攻撃者のアドレスと攻撃対象のポートのペアについては、現在のパケットおよび将来のパケットを送信しません。

- [Deny Attacker Inline]（インラインのみ）：指定された期間、この攻撃者のアドレスからの、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ています。拒否攻撃者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、リスト全体をクリアするか、タイマーが期限切れになるのを待ちます。タイマーは各エントリのスライディング タイマーです。そのため、攻撃者 A が拒否されており、別の攻撃を実行する場合、攻撃者 A のタイマーがリセットされ、タイマーが期限切れになるまで、攻撃者 A は拒否攻撃者リストに登録されたままになります。拒否攻撃者リストが最大容量に達し新しいエントリを追加できない場合でも、パケットは引き続き拒否されます。

  （注）　これは最も厳しい拒否アクションです。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が拒否されます。すべての拒否攻撃者エントリをクリアするには、[Configuration] > *sensor_name* > [Sensor Monitoring] > [Time-Based Actions] > [Denied Attackers] > [Clear List] の順に選択することにより、ネットワーク上でアドレスが元のとおり許可されます。

- [Modify Packet Inline]（インラインのみ）：エンドポイントによるパケットの処理に関するあいまいさを取り除くために、パケット データを変更します。

  （注）　[Modify Packet Inline] は、イベント アクション フィルタまたはオーバーライドを追加するときに使用できません。

- [Other Actions]

  （注）　IPv6 は、イベント アクション [Request Block Host]、[Request Block Connection]、[Request Rate Limit] をサポートしません。

  - [Request Block Connection]：この接続をブロックするように ARC に要求を送信します。ブロッキング デバイスは、このアクションを実行するように設定されている必要があります。

    （注）　接続ブロックとネットワーク ブロックは、適応型セキュリティ アプライアンスではサポートされていません。適応型セキュリティ アプライアンスは、追加の接続情報があるホスト ブロックだけをサポートします。

  - [Request Block Host]：この攻撃者ホストをブロックするように ARC に要求を送信します。ブロッキング デバイスは、このアクションを実行するように設定されている必要があります。

    （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] > *sensor_name* > [Policies] > [Event Action Rules] > [rules0] > [General Settings] の順に選択します。

  - [Request Rate Limit]：レート制限を実行するように、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行するように設定されている必要があります。

    （注）　[Request Rate Limit] は、選択した複数のシグニチャに適用されます。

– [Reset TCP Connection]：TCP リセットを送信し、TCP フローを乗っ取って終了させます。[Reset TCP Connection] は、単一の接続を分析する TCP シグニチャのみで動作します。スイープまたはフラッドに対しては機能しません。

Deny Packet Inline について

Deny Packet Inline がアクションとして設定されているシグニチャや、Deny Packet Inline をアクションとして追加するイベント アクション オーバーライドでは、次のアクションを実行できます。

- droppedPacket
- deniedFlow
- tcpOneWayResetSent

Deny Packet Inline アクションは、アラート内のドロップされたパケット アクションとして表現されます。Deny Packet Inline が TCP 接続に対して発生した場合、Deny Connection Inline アクションに自動的にアップグレードされ、アラート内で拒否されたフローとして認識されます。IPS により 1 個のパケットのみが拒否された場合、TCP はその同じパケットを何度も送信しようとするため、IPS は接続全体を拒否して、再送により成功しないようにします。

また、Deny Connection Inline が発生した場合、IPS は自動的に TCP の一方向リセットを送信します。これは、アラート内に TCP 一方向リセットが送信されたものとして現れます。IPS が接続を拒否するとき、クライアント（一般に攻撃者）とサーバ（一般に攻撃対象）の両方で接続が開かれたままになります。開かれた状態の接続が多すぎると、攻撃対象でリソースの問題が発生します。そのため、IPS は TCP リセットを攻撃対象に送信し、攻撃対象の側（通常はサーバ）で接続を閉じ、攻撃対象のリソースを保護します。また、フェールオーバーを防ぎ、他のネットワーク パスに接続がフェールオーバーして攻撃対象に到達するのを許してしまわないようにします。攻撃者の側は開かれたままになり、そこからのすべてのトラフィックが拒否されます。

詳細情報

- 一般的な設定のための手順については、「一般設定」（P.11-35）を参照してください。
- SNMP の設定手順については、第 16 章「SNMP の設定」を参照してください。
- 拒否攻撃者を設定するための手順については、「拒否攻撃者の設定とモニタリング」（P.19-4）を参照してください。

シグニチャのイネーブル化、ディセーブル化、廃止

注意　AIP SSC-5 では、デフォルトで廃止されているシグニチャの廃止解除はサポートされていません。デフォルトで廃止されているシグニチャをアクティブ化しようとすると、警告メッセージが表示されます。デフォルトで廃止されているシグニチャではなく、自分で廃止したシグニチャは、アクティブ化できます。

シグニチャをイネーブル化、ディセーブル化、および廃止するには、次の手順を実行します。

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

ステップ 2　[Configuration] > *sensor_name* > [Policies] > [Signature Definitions] > [sig0] > [Active Signatures] の順に選択します。

ステップ 3　シグニチャを探すには、[Filter] ドロップダウン リストからソート オプションを選択します。たとえば、[Flood Host] シグニチャを探している場合、ドロップダウン リストから [Engine]、[Flood Host] の順に選択し、次に個別のシグニチャを選択します。[sig0] ペインが更新され、ソート条件に一致するシグニチャのみが表示されます。

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] 列を参照して、シグニチャのステータスを確認します。イネーブルになっているシグニチャのチェックボックスはオンになります。

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、[Enabled] チェックボックスをオンにします。

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、[Enabled] チェックボックスをオフにします。

d. 1 つ以上のシグニチャを廃止するには、シグニチャを選択し、右クリックして、[Change Status To] > [Retired] の順に選択します。

（注）　使用していないシグニチャを廃棄することを推奨します。廃棄によって、センサーのパフォーマンスが向上します。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 5　変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

シグニチャの追加

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

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

既存のシグニチャを基にせずにカスタム シグニチャを作成するには、次の手順を実行します。

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

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

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

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

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

ステップ 6　[Sig Fidelity Rating] フィールドに、このシグニチャのシグニチャ忠実度レーティングを表す 1 ～ 100 の範囲の値を入力します。

ステップ 7　[Promiscuous Delta] フィールドに、このシグニチャに関連付ける無差別デルタ（0 ～ 30）を入力します。

注意　シグニチャの無差別デルタ設定は変更しないことをお勧めします。

ステップ 8　[Sig Description] フィールドに説明を入力し、このシグニチャに関するコメントを追加します。

ステップ 9　[Engine] ドロップダウン リストから、このシグニチャを適用するためにセンサーが使用するエンジンを選択します。

（注）　どのエンジンを選択すべきかわからない場合は、Custom Signature Wizard を使用してカスタム シグニチャを作成します。

ステップ 10　このシグニチャにアクションを割り当てます。

ステップ 11　このシグニチャのエンジン固有のパラメータを設定します。

ステップ 12　イベント カウンタを設定します。

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

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

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

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

ステップ 13　アラートの頻度を設定します。

ステップ 14　シグニチャのステータスの設定

a.　[Enabled] ドロップダウン リストから、[Yes] を選択し、シグニチャをイネーブルにします。

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

b.　[Retired] ドロップダウン リストから、[Yes] を選択し、シグニチャがアクティブであることを確認します。

これで、シグニチャがエンジンに置かれます。

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

c.　脆弱な OS を選択します。

ヒント　複数の OS を選択するには、**Ctrl** キーを押しながらクリックします。

ステップ 15　MARS カテゴリを選択し、[OK] をクリックします。

ヒント 変更内容を破棄して [Add Signature] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 16 [OK] をクリックします。[Type] が [Custom] に設定されたリストに、新しいシグニチャが表示されます。

ヒント 変更を破棄するには、[Reset] をクリックします。

ステップ 17 変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

シグニチャのクローニング

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

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

注意 組み込みシグニチャの中の一部のシグニチャ値は保護されており、値をコピーできません。シグニチャのクローニングはできますが、いくつかの値は設定できません。シグニチャ値を設定できない場合は、次のようなエラー メッセージが表示されます。

```
[Obsoletes] is protected, cannot copy the value. [Mars Category] is protected, cannot copy the value.
```

[sig0] ペインで、既存のシグニチャをクローニングしてシグニチャを作成できます。この作業では、類似するシグニチャを作成する場合の時間を節約できます。

既存のシグニチャを開始点として使用しシグニチャを作成するには、次の手順を実行します。

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

ステップ 2 [Configuration] > *sensor_name* > [Policies] > [Signature Definitions] > [sig0] > [Active Signatures] の順に選択します。

ステップ 3 シグニチャを探すには、[Filter] ドロップダウン リストからソート オプションを選択します。たとえば、[Flood Host] シグニチャを探している場合、ドロップダウン リストから [Engine]、[Flood Host] の順に選択し、次に個別のシグニチャを選択します。[sig0] ペインが更新され、ソート条件に一致するシグニチャのみが表示されます。

ステップ 4 シグニチャを選択し、[Clone] をクリックします。

ステップ 5 [Signature] フィールドに、新しいシグニチャの一意のシグニチャ ID を入力します。カスタム シグニチャ ID は、60000 から始まります。

ステップ 6　[Subsignature] フィールドに、新しいシグニチャの一意のサブシグニチャ ID を入力します。

ステップ 7　パラメータ値を確認し、この新しいシグニチャで異なる値を使用するパラメータ値を変更します。

ヒント　複数の OS またはイベント アクションを選択するには、**Ctrl** キーを押しながらクリックします。

ステップ 8　シグニチャのステータスの設定

a.　[Enabled] ドロップダウン リストから、[Yes] を選択し、シグニチャをイネーブルにします。

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

b.　[Retired] ドロップダウン リストから、[Yes] を選択し、シグニチャがアクティブであることを確認します。これで、シグニチャがエンジンに置かれます。

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

ヒント　変更内容を破棄して [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。

c.　[OK] をクリックします。[Type] が [Custom] に設定された状態でクローニングしたシグニチャが表示されます。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 9　変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

シグニチャの調整

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

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

（注） 組み込みシグニチャのチューニングは可能です。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。

[sig0] ペインで、シグニチャを編集（*調整*）できます。

既存のシグニチャを調整するには、次の手順を実行します。

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

ステップ 2　[Configuration] > *sensor_name* > [Policies] > [Signature Definitions] > [sig0] > [Active Signatures] の順に選択します。

ステップ 3　シグニチャを探すには、[Filter] ドロップダウン リストからソート オプションを選択します。たとえば、[Flood Host] シグニチャを探している場合、ドロップダウン リストから [Engine]、[Flood Host] の順に選択し、次に個別のシグニチャを選択します。[sig0] ペインが更新され、ソート条件に一致するシグニチャのみが表示されます。

ステップ 4　シグニチャを選択し、[Edit] をクリックします。

ステップ 5　パラメータ値を確認し、調整するパラメータの値を変更します。

ヒント 複数の OS、イベント アクション、脆弱 OS、または MARS カテゴリを選択するには、**Ctrl** キーを押しながらクリックします。

ステップ 6　シグニチャのステータスの設定

a. [Enabled] ドロップダウン リストから、[Yes] を選択し、シグニチャをイネーブルにします。

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

b. [Retired] ドロップダウン リストから、[Yes] を選択し、シグニチャがアクティブであることを確認します。これで、シグニチャがエンジンに置かれます。

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

ヒント 変更内容を破棄して [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。

ステップ 7　[OK] をクリックします。[Type] が [Tuned] に設定された状態で、編集したシグニチャが表示されます。

ヒント 変更を破棄するには、[Reset] をクリックします。

ステップ 8　変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

シグニチャへのアクションの割り当て

[sig0] ペインで、シグニチャにアクションを割り当てることができます。

1 つ以上のシグニチャのアクションを編集するには、次の手順を実行します。

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

ステップ 2　[Configuration] > *sensor_name* > [Policies] > [Signature Definitions] > [sig0] > [Active Signatures] の順に選択します。

ステップ 3　シグニチャを探すには、[Filter] ドロップダウン リストからソート オプションを選択します。たとえば、[Flood Host] シグニチャを探している場合、ドロップダウン リストから [Engine]、[Flood Host] の順に選択し、次に個別のシグニチャを選択します。[sig0] ペインが更新され、ソート条件に一致するシグニチャのみが表示されます。

ステップ 4　シグニチャを選択し、[Edit Actions] をクリックします。

ステップ 5　シグニチャに割り当てるアクションの横にあるチェックボックスをオンにします。

（注）　チェック マークは、選択したシグニチャにアクションが割り当てられていることを示します。チェック マークがない場合、選択したシグニチャのいずれにもアクションが割り当てられていないことを示します。灰色のチェック マークは、選択したシグニチャの一部にアクションが割り当てられていることを示します。

ヒント　複数のアクションを選択するには、**Ctrl** キーを押しながらクリックします。

次のアクションのいずれかを選択します。

- [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] : 攻撃パケットの符号化されたダンプをアラートに含めます。このアクションによって、[Produce Alert] が選択されていない場合でも、アラートがイベント ストアに書き込まれます。
- [Log Attacker Packets] : 攻撃者のアドレスが含まれているパケットに対する IP ロギングを開始し、アラートを送信します。このアクションによって、[Produce Alert] が選択されていない場合でも、アラートがイベント ストアに書き込まれます。
- [Log Victim Packets] : 攻撃対象のアドレスが含まれているパケットに対する IP ロギングを開始し、アラートを送信します。このアクションによって、[Produce Alert] が選択されていない場合でも、アラートがイベント ストアに書き込まれます。
- [Log Pair Packets] : 攻撃者と攻撃対象のアドレスのペアが含まれているパケットに対する IP ロギングを開始します。このアクションによって、[Produce Alert] が選択されていない場合でも、アラートがイベント ストアに書き込まれます。
- [Request SNMP Trap] : NotificationApp に、SNMP 通知を実行するための要求を送信します。このアクションによって、[Produce Alert] が選択されていない場合でも、アラートがイベント ストアに書き込まれます。このアクションを実行するには、センサーで SNMP が設定されている必要があります。
- [Deny Packet Inline]（インラインのみ）: このパケットを送信しません。
- [Deny Connection Inline]（インラインのみ）: このパケットと将来のパケットを TCP フロー上で送信しません。

- [Deny Attacker Victim Pair Inline]（インラインのみ）：指定された期間、この攻撃者と攻撃対象のアドレスのペアについては、現在のパケットおよび将来のパケットを送信しません。
- [Deny Attacker Service Pair Inline]（インラインのみ）：指定された期間、この攻撃者のアドレスと攻撃対象のポートのペアについては、現在のパケットおよび将来のパケットを送信しません。
- [Deny Attacker Inline]（インラインのみ）：指定された期間、この攻撃者のアドレスから発生した現在のパケットおよび将来のパケットを送信しません。
- [Modify Packet Inline]（インラインのみ）：エンドポイントによるパケットの処理に関するあいまいさを取り除くために、パケット データを変更します。
- [Request Block Connection]：この接続をブロックするように ARC に要求を送信します。ブロッキング デバイスは、このアクションを実行するように設定されている必要があります。
- [Request Block Host]：この攻撃者ホストをブロックするように ARC に要求を送信します。ブロッキング デバイスは、このアクションを実行するように設定されている必要があります。
- [Request Rate Limit]：レート制限を実行するように、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行するように設定されている必要があります。
- [Reset TCP Connection] : TCP リセットを送信し、TCP フローを乗っ取って終了させます。[Reset TCP Connection] は、単一の接続を分析する TCP シグニチャのみで動作します。スイープまたはフラッドに対しては機能しません。

ヒント 変更内容を破棄して [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。

ステップ 6 [OK] をクリックして変更内容を保存し、ダイアログボックスを閉じます。新しいアクションが [Action] 列に表示されます。

ヒント 変更を破棄するには、[Reset] をクリックします。

ステップ 7 変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

詳細情報

- 一般的な設定のための手順については、「一般設定」（P.11-35）を参照してください。
- SNMP の設定手順については、第 16 章「SNMP の設定」を参照してください。
- 拒否攻撃者を設定するための手順については、「拒否攻撃者の設定とモニタリング」（P.19-4）を参照してください。

アラート頻度の設定

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

シグニチャの反応頻度は制御できます。たとえば、センサーから送られるアラートの量を減らす場合があります。または、シグニチャの反応を 1 つのアラートにまとめたい場合があります。また、IPS に偽のトラフィックを送り、IPS が短時間に大量のアラートを発生させるようにする「Stick」などの IDS 対抗ツールに対応させる場合があります。

シグニチャのアラート頻度を設定するには、次の手順を実行します。

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

ステップ 2　[Configuration] > *sensor_name* > [Policies] > [Signature Definitions] > [sig0] > [Active Signatures] の順に選択します。

ステップ 3　[Add] をクリックしてシグニチャを追加するか、クローニングするシグニチャを選択して [Clone] をクリックするか、編集するシグニチャを選択して [Edit] をクリックします。

ステップ 4　イベント カウント、キー、アラート間隔を設定します。

a. [Event Count] フィールドに、イベント カウントの値を入力します。これは、このシグニチャについて 1 個のアラートを送信する前にセンサーが受信する必要がある最小ヒット数です。

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

c. レートに基づいてイベントをカウントするには、[Specify Event Interval] ドロップダウン リストから [Yes] を選択し、[Alert Interval] フィールドに間隔として使用する秒数を入力します。

ステップ 5　アラートの量を制御しセンサーがアラートをサマライズする方法を設定するには、[Summary Mode] ドロップダウン リストから次のいずれかのオプションを選択します。

- [Fire All]：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アラートを送信するよう指定します。その後、アラートの量をダイナミックに調整できる追加しきい値を指定できます。ステップ 6 に進みます。
- [Fire Once]：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アラートを送信するよう指定します。その後、アラートの量をダイナミックに調整できる追加しきい値を指定できます。ステップ 7 に進みます。
- [Summarize]：このシグニチャについて、シグニチャが起動されるたびにアラートを送信するのではなく、サマリー アラートのみを送信するようにセンサーに指定します。その後、アラートの量をダイナミックに調整できる追加しきい値を指定できます。ステップ 8 に進みます。
- [Global Summarize]：1 つのアドレス セットに対して初めてシグニチャが起動されたときにアラートを送信し、指定された期間にわたって、すべてのアドレス セットについてのすべてのアラートのサマリーを含むグローバル サマリー アラートのみを送信するようにセンサーに指定します。ステップ 9 に進みます。

ステップ 6　次のように [Fire All] オプションを設定します。

a. [Specify Summary Threshold] ドロップダウン リストから、[Yes] を選択します。

b. [Summary Threshold] フィールドに、このシグニチャについて、サマリー アラートを送信する前にセンサーが受信する必要がある最小ヒット数を入力します。

c. [Summary Interval] フィールドに、期間として使用する秒数を入力します。

d. センサーをグローバル集約モードにするには、[Specify Global Summary Threshold] ドロップダウン リストで [Yes] を選択します。

e. [Global Summary Threshold] フィールドに、グローバル サマリー アラートを送信する前にセンサーが受信する必要がある最小ヒット数を入力します。

f. [Summary Key] ドロップダウン リストから、サマリー キーのタイプを選択します。サマリー キーは、イベントのカウントに使用する属性を識別します。たとえば、センサーでイベントが同じ攻撃者からかどうかに基づいてカウントする場合は、サマリー キーとして攻撃者のアドレスを選択します。

ステップ 7　次のように [Fire Once] オプションを設定します。

a. [Summary Key] ドロップダウン リストから、サマリー キーのタイプを選択します。サマリー キーは、イベントのカウントに使用する属性を識別します。たとえば、センサーでイベントが同じ攻撃者からかどうかに基づいてカウントする場合は、サマリー キーとして攻撃者のアドレスを選択します。

b. センサーでグローバル サマライズを使用するには、[Specify Global Summary Threshold] ドロップダウン リストで [Yes] を選択します。

c. [Global Summary Threshold] フィールドに、グローバル サマリー アラートを送信する前にセンサーが受信する必要がある最小ヒット数を入力します。

（注） アラート率が指定秒数内に指定された数のシグニチャを超えると、センサーはシグニチャが最初に起動されたときにアラートを送信せず、アラートを 1 つのグローバル サマリーにまとめて送信します。指定間隔内にアラートの率がしきい値を下回ると、元のアラート動作に戻ります。

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

d. [Summary Interval] フィールドに、センサーがサマライズ用にイベントをカウントする秒数を入力します。

ステップ 8　次のように [Summarize] オプションを設定します。

a. [Summary Interval] フィールドに、センサーがサマライズ用にイベントをカウントする秒数を入力します。

b. [Summary Key] ドロップダウン リストから、サマリー キーのタイプを選択します。サマリー キーは、イベントのカウントに使用する属性を識別します。たとえば、センサーでイベントが同じ攻撃者からかどうかに基づいてカウントする場合は、サマリー キーとして攻撃者のアドレスを選択します。

c. センサーで動的グローバル サマライズを使用するには、[Specify Global Summary Threshold] ドロップダウン リストで [Yes] を選択します。

d. [Global Summary Threshold] フィールドに、グローバル サマリー アラートを送信する前にセンサーが受信する必要がある最小ヒット数を入力します。

（注） アラート率が指定秒数内に指定された数のシグニチャを超えると、センサーはシグニチャが最初に起動されたときにアラートを送信せず、アラートを 1 つのグローバル サマリーにまとめて送信します。指定間隔内にアラートの率がしきい値を下回ると、元のアラート動作に戻ります。

ステップ 9　[Global Summarize] オプションを設定するには、[Summary Interval] フィールドに、センサーがサマライズ用にイベントをカウントする秒数を入力します。

ステップ 10　[OK] をクリックしてアラートの動作変更を保存します。再度 [sig0] ペインが表示されます。

ヒント　変更を破棄するには、[Cancel] をクリックします。

ステップ 11　アラート動作変更をシグニチャの設定に適用するには、[Apply] をクリックします。

追加または編集したシグニチャがイネーブルになり、シグニチャのリストに追加されます。

Meta エンジンのシグニチャの例

注意　Meta エンジンのシグニチャの数が多いと、センサー全体のパフォーマンスに悪影響が出るおそれがあります。

Meta エンジンでは、スライディング時間間隔内に、関連した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 エンジンはシグニチャ イベントを検査して、1 つ以上の Meta 定義に一致するかどうかを判定します。Meta エンジンは、すべてのイベント要件が満たされるとシグニチャ イベントを生成します。

すべてのシグニチャ イベントは、シグニチャ イベント アクション プロセッサによって Meta エンジンに渡されます。シグニチャ イベント アクション プロセッサは、最小ヒット数オプションを処理してからイベントを渡します。Meta エンジンがコンポーネント イベントを処理してから、サマライズおよびイベント アクションは処理されます。

（注）　Meta エンジンは、ほとんどのエンジンがパケットを入力としているにもかかわらず、アラートを入力としている点が他のエンジンとは異なります。

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

次の例は、Meta エンジンに基づいてシグニチャを作成する方法を示しています。たとえば、次のカスタム シグニチャが起動されるのは、シグニチャ 2000 サブシグニチャ 0 とシグニチャ 3000 サブシグニチャ 0 が同じ送信元アドレスに対して起動された場合です。送信元アドレスの選択は、メタ キー デフォルト値 Axxx の結果です。たとえば、メタ キー設定を xxBx（宛先アドレス）に変更することで動作を変更できます。

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

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

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

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

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

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

ステップ 6　[Signature Fidelity Rating] フィールドに、このシグニチャのシグニチャ忠実度レーティングを表す 1 ～ 100 の値を入力します。

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

ステップ 8　シグニチャを説明するフィールドに入力し、このシグニチャに関するコメントを追加します。

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

ステップ 10　Meta エンジン固有のパラメータを設定します。

a. [Event Action] ドロップダウン リストから、センサーがイベントに応答するときのアクションを選択します。

ヒント　複数のアクションを選択するには、**Ctrl** キーを押しながらクリックします。

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

c. [Meta Reset Interval] フィールドに、Meta シグニチャをリセットする秒数を入力します。有効な値の範囲は 0 ～ 3600 秒です。デフォルトは 60 秒です。

d. [Component List] の横にある鉛筆アイコンをクリックし、新しい [Meta] 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。

e. [Add] をクリックして最初の Meta 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。

f. [Entry Key] フィールドに、エントリの名前を入力します（例：Entry1）。デフォルトは MyEntry です。

g. [Component Sig ID] フィールドに、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（この例では 2000）を入力します。

h. [Component SubSig ID] フィールドに、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（この例では 0）を指定します。

i. [Component Count] フィールドに、このコンポーネントが満たされる前に、このコンポーネントが起動される必要がある回数を入力します。

j. [OK] をクリックします。再度 [Add List Entry] ダイアログボックスが表示されます。

k. エントリを選択し、[Select] をクリックして [Selected Entries] リストに移動します。

l. [OK] をクリックします。

m. [Add] をクリックして次の Meta 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。

n. [Entry Key] フィールドに、エントリの名前を入力します（例：Entry2）。

o. [Component Sig ID] フィールドに、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（この例では 3000）を入力します。

p. [Component SubSig ID] フィールドに、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（この例では 0）を入力します。

q. [Component Count] フィールドに、このコンポーネントが満たされる前に、このコンポーネントが起動される必要がある回数を入力します。

r. [OK] をクリックします。再度 [Add List Entry] ダイアログボックスが表示されます。

s. エントリを選択し、[Select] をクリックして [Selected Entries] リストに移動します。

t. 新しいエントリを選択し、[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変更します。

ヒント エントリを [Entry Key] に戻すには、[Reset Ordering] をクリックします。

u. [OK] をクリックします。

v. [Meta Key] ドロップダウン 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
- 攻撃者と攻撃対象のアドレス
- 攻撃者と攻撃対象のアドレスおよびポート
- 攻撃対象のアドレス

w. [Unique Victims] フィールドに、このシグニチャで必要な一意の攻撃対象の数を入力します。有効な値は 1 ～ 256 です。デフォルトは 1 です。

x. コンポーネント リストが順番に起動されるようにするには、[Component List in Order] ドロップダウン リストで [Yes] を選択します。

ステップ 11 イベント カウンタを設定します。

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

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

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

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

ステップ 12 アラートの頻度を設定します。

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

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

ステップ 14 [Retired] フィールドはデフォルト（[Yes]）のままにします。これで、シグニチャがエンジンに置かれます。

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

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

ヒント 複数のアクションを選択するには、**Ctrl** キーを押しながらクリックします。

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

ヒント 複数のアクションを選択するには、**Ctrl** キーを押しながらクリックします。

ヒント 変更内容を破棄して [Add Signature] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 17 [OK] をクリックします。[Type] が [Custom] に設定されたリストに、新しいシグニチャが表示されます。

ヒント 変更を破棄するには、[Reset] をクリックします。

ステップ 18 変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

詳細情報

Meta エンジンの詳細については、「Meta エンジン」（P.B-36）を参照してください。

Atomic IP Advanced エンジンのシグニチャの例

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

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

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

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

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

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

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

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

ステップ 6 [Signature Fidelity Rating] フィールドに、このシグニチャのシグニチャ忠実度レーティングを表す 1 ～ 100 の値を入力します。

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

ステップ 8 シグニチャを説明するフィールドに入力し、このシグニチャに関するコメントを追加します。

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

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

a. [Event Action] ドロップダウン リストから、センサーがイベントに応答するときのアクションを選択します。

（注） IPv6 は、イベント アクション [Request Block Host]、[Request Block Connection]、[Request Rate Limit] をサポートしません。

ヒント 複数のアクションを選択するには、**Ctrl** キーを押しながらクリックします。

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

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

d. [HOH Options] フィールドから [Yes] を選択し、次に [HOH Option Type] フィールドに、「1」を入力します。

e. [HOH Option Length] ドロップダウン リストで [Yes] を選択してホップバイホップ長をイネーブルにします。次に [HOH Option Length] フィールドに「8」を入力します。

ステップ 11　イベント カウンタを設定します。

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

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

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

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

ステップ 12　アラートの頻度を設定します。

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

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

ステップ 14　[Retired] フィールドはデフォルト（[Yes]）のままにします。これで、シグニチャがエンジンに置かれます。

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

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

ヒント 複数のアクションを選択するには、**Ctrl** キーを押しながらクリックします。

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

ヒント　複数のアクションを選択するには、**Ctrl** キーを押しながらクリックします。

ヒント　変更内容を破棄して [Add Signature] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 17　[OK] をクリックします。[Type] が [Custom] に設定されたリストに、新しいシグニチャが表示されます。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 18　変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

詳細情報

Atomic IP エンジンの詳細については、「Atomic エンジン」（P.B-14）を参照してください。

String XL エンジンの Match Offset シグニチャの例

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

カスタム String XL TCP シグニチャを作成するには、既存の String XL TCP シグニチャをクローニングして調整するか、新しいシグニチャを追加して String XL TCP シグニチャ エンジンを割り当てます。

（注）　この手順は、String XLUDP シグニチャおよび String XL ICMP シグニチャにも適用されます。ただし、パラメータ **service-ports** は、String XL ICMP シグニチャには適用されません。

次の例は、完全、最大、最小オフセットを検索するカスタム String XL TCP シグニチャを作成する方法を示しています。このカスタム String XLTCP シグニチャの次のオプション一致オフセット パラメータを変更できます。

- Specify Exact Match Offset
- Specify Maximum Match Offset
- Specify Minimum Match Offset

一致を検索するカスタム String XL TCP シグニチャを作成するには、次の手順を実行します。

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

ステップ 2　[Configuration] > *sensor_name* > [Policies] > [Signature Definitions] > [sig0] > [Active Signatures] の順に選択します。

ステップ 3　既存の String XL TCP シグニチャをクローニングすることでカスタム シグニチャを作成するには、[Filter] ドロップダウン リストから [Engine] を選択し、シグニチャ エンジン ドロップダウン リストから [String TCP XL] を選択し、クローニングするシグニチャを強調表示させて、[Clone] をクリックします。ステップ 5 に進みます。

ステップ 4　String XL TCP 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、[Add] をクリックし、[Add Signature] ダイアログボックスの [Engine] フィールドで、[Click to edit] をクリックし、ドロップダウン リストから [String XL TCP] を選択します。ステップ 5 に進みます。

ステップ 5　[Signature ID] フィールドに、シグニチャの番号を入力します。カスタム シグニチャの範囲は 60000 ～ 65000 です。

ステップ 6　[Subsignature ID] フィールドに、シグニチャの番号を入力します。デフォルトは 0 です。似ているシグニチャをグループにまとめるには、サブシグニチャ ID を割り当てます。

ステップ 7　（任意）[Severity Alert] フィールドで、センサーがアラートを送信するときに Event Viewer によって報告される重大度を選択します。デフォルトは [Medium] です。

ステップ 8　（任意）[Sig Fidelity Rating] フィールドに値を入力します。シグニチャ忠実度レーティングの有効値は 0 ～ 100 で、シグニチャに対する信頼度を示します。100 が最も信頼度が高いことを示します。デフォルトは 75 です。

ステップ 9　[Promiscuous Delta] フィールドに値を入力します。無差別デルタは、アラートの重大度を決定するために使用される値です。有効な範囲は 0 ～ 30 です。デフォルトは 0 です。

注意　シグニチャの無差別デルタ設定は変更しないことをお勧めします。

ステップ 10　[Sig Description] で、このシグニチャを一意に識別する属性を指定します。

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

（注）　アラートが生成されると、シグニチャ名はシグニチャ ID およびサブシグニチャ ID とともにイベント ビューアに報告されます。

b.　（任意）[Alert Notes] フィールドに、アラートに追加するテキストを入力します。このシグニチャに関連付けられているアラートに含めるテキストを追加できます。アラートが生成されると、このテキストはイベント ビューアに報告されます。デフォルトは、My Sig Info です。

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

ステップ 11　[Engine] で、エンジン固有のパラメータを割り当てます。

a.　（任意）[Event Action] フィールドで、シグニチャによって報告するイベント アクションを割り当てます。デフォルトは [Produce Alert] です。セキュリティ ポリシーに基づいて、拒否やブロックなどの複数のアクションを割り当てることができます。

ヒント 複数のアクションを選択するには、**Ctrl** キーを押しながらクリックします。

b. （任意）[Strip Telnet Options] フィールドで、ドロップダウン リストから [Yes] を選択し、パターンを検索する前にデータから Telnet オプション文字を除去します。

c. [Direction] ドロップダウン リストから、トラフィックの方向を選択します。

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

d. [Service Ports] フィールドに、ポート番号（たとえば 80）を入力します。値は、ターゲット サービスが常駐する、カンマ区切りのポートのリストまたはポート範囲です。

ステップ 12 正規表現を指定するには、[Specify Raw Regex String] で、ドロップダウン リストから [No] を選択します。

（注） Raw Regex は raw モードの処理で使用される正規表現構文です。これはエキスパート モード専用であり、Cisco IPS シグニチャ開発チームや、Cisco IPS シグニチャ開発チームの監督下にある人のみが使用することを目的としています。String XL シグニチャは通常の正規表現または raw 正規表現のどちらかで設定できます。

a. [Regex String] フィールドに、このシグニチャが TCP パケット内で探す文字列を入力します（たとえば tcpstring）。

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

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

ステップ 13 （任意）[Specify Exact Match Offset] フィールドでドロップダウン リストから [Yes] を選択して完全一致オフセットをイネーブルにし、[Exact Match Offset] フィールドに、このシグニチャが一致と見なされるために正規表現が起動する必要がある完全オフセットを入力します（0 ～ 65535）。

（注） 完全一致オフセットを [Yes] に設定した場合、最大または最小一致オフセットは設定できません。完全一致オフセットを [No] に設定した場合、最大および最小一致オフセットを同時に設定できます。

ステップ 14 （任意）[Specify Max Match Offset] フィールドでドロップダウン リストから [Yes] を選択して最大一致オフセットをイネーブルにし、[Specify Max Match Offset] フィールドに、このシグニチャが一致と見なされるために正規表現が起動する必要がある最大オフセットを入力します（0 ～ 65535）。

ステップ 15 （任意）[Specify Min Match Offset] フィールドでドロップダウン リストから [Yes] を選択して最小一致オフセットをイネーブルにし、[Specify Min Match Offset] フィールドに、このシグニチャが一致と見なされるために正規表現が起動する必要がある最小オフセットを入力します（0 ～ 65535）。

ステップ 16 （任意）[Alert Frequency] フィールドで、デフォルト アラート頻度を変更できます。

ステップ 17 [OK] をクリックしてカスタム シグニチャを作成します。作成したシグニチャがイネーブルになり、シグニチャのリストに追加されます。

ヒント　変更を破棄するには、[Cancel] をクリックします。

詳細情報

- String XL エンジンの詳細については、「String XL エンジン」（P.B-64）を参照してください。
- シグニチャの正規表現の一覧表については、「正規表現の構文」（P.B-10）を参照してください。
- String XL エンジンのシグニチャで使用できる特殊文字列の一覧表については、「特殊文字」（P.B-11）を参照してください。

String XL エンジンの最小一致長シグニチャの例

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

（注）　この手順は、String XLUDP シグニチャおよび String XL ICMP シグニチャにも適用されます。ただし、パラメータ **service-ports** は、String XL ICMP シグニチャには適用されません。

カスタム String XL TCP シグニチャを作成するには、既存の String XL TCP シグニチャをクローニングして調整するか、新しいシグニチャを追加して String XL TCP シグニチャ エンジンを割り当てます。

特定の正規表現文字列とともに動作する次のオプションを設定できます。

- Dot All
- End Optional
- No Case
- Stingy
- UTF-8

次の例は、最小一致長を検索する、stingy、dot all、および UTF-8 を有効にした、カスタム String XL TCP シグニチャを作成する方法を示しています。

stingy、dot all、および UTF-8 を有効にし、最小一致長を検索する String XL TCP エンジンに基づくカスタム シグニチャを作成するには、次の手順を実行します。

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

ステップ 2　[Configuration] > *sensor_name* > [Policies] > [Signature Definitions] > [sig0] > [Active Signatures] の順に選択します。

ステップ 3　既存の String XL TCP シグニチャをクローニングすることでカスタム シグニチャを作成するには、[Filter] ドロップダウン リストから [Engine] を選択し、シグニチャ エンジン ドロップダウン リストから [String TCP XL] を選択し、クローニングするシグニチャを強調表示させて、[Clone] をクリックします。ステップ 5 に進みます。

ステップ 4　String XL TCP 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、[Add] をクリックし、[Add Signature] ダイアログボックスの [Engine] フィールドで、[Click to edit] をクリックし、ドロップダウン リストから [String XL TCP] を選択します。ステップ 5 に進みます。

ステップ 5　[Signature ID] フィールドに、シグニチャの番号を入力します。

カスタム シグニチャの範囲は 60000 ～ 65000 です。

ステップ 6　[Subsignature ID] フィールドに、シグニチャの番号を入力します。

デフォルトは 0 です。似ているシグニチャをグループにまとめるには、サブシグニチャ ID を割り当てます。

ステップ 7　（任意）[Severity Alert] フィールドで、センサーがアラートを送信するときに Event Viewer によって報告される重大度を選択します。デフォルトは [Medium] です。

ステップ 8　（任意）[Sig Fidelity Rating] フィールドに値を入力します。

シグニチャ忠実度レーティングの有効値は 0 ～ 100 で、シグニチャに対する信頼度を示します。100 が最も信頼度が高いことを示します。デフォルトは 75 です。

ステップ 9　[Promiscuous Delta] フィールドに値を入力します。

無差別デルタは、アラートの重大度を決定するために使用される値です。有効な範囲は 0 ～ 30 です。デフォルトは 0 です。

注意　シグニチャの無差別デルタ設定は変更しないことをお勧めします。

ステップ 10　[Sig Description] で、このシグニチャを一意に識別する属性を指定します。

d.　（任意）[Signature Name] フィールドに、シグニチャの名前を入力します。

[Signature Name] フィールドにデフォルト名 My Sig が表示されます。それぞれのカスタム シグニチャに合せて、具体的な名前に変更します。

（注）　アラートが生成されると、シグニチャ名はシグニチャ ID およびサブシグニチャ ID とともにイベント ビューアに報告されます。

e.　（任意）[Alert Notes] フィールドに、アラートに追加するテキストを入力します。

このシグニチャに関連付けられているアラートに含めるテキストを追加できます。アラートが生成されると、このテキストはイベント ビューアに報告されます。デフォルトは、My Sig Info です。

f.　（任意）[User Comments] フィールドに、このシグニチャを説明するテキストを入力します。

ここには、必要に応じてどのようなテキストを入力することもできます。このフィールドは、シグニチャやアラートには影響を与えません。デフォルトは [Sig Comment] です。

ステップ 11　[Engine] で、エンジン固有のパラメータを割り当てます。

a.　（任意）[Event Action] フィールドで、シグニチャによって報告するイベント アクションを割り当てます。

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

ヒント　複数のアクションを選択するには、**Ctrl** キーを押しながらクリックします。

b.　（任意）[Strip Telnet Options] フィールドで、ドロップダウン リストから [Yes] を選択し、パターンを検索する前にデータから Telnet オプション文字を除去します。

c. [Direction] ドロップダウン リストから、トラフィックの方向を選択します。
   - [From Service] : サービス ポートからクライアント ポート宛のトラフィック。
   - [To Service] : クライアント ポートからサービス ポート宛のトラフィック。

d. [Service Ports] フィールドに、23 などのポート番号を入力します。値は、ターゲット サービスが常駐する、カンマ区切りのポートのリストまたはポート範囲です。

ステップ 12　正規表現を指定するには、[Specify Raw Regex String] で、ドロップダウン リストから [No] を選択します。

（注） Raw Regex は raw モードの処理で使用される正規表現構文です。これはエキスパート モード専用であり、Cisco IPS シグニチャ開発チームや、Cisco IPS シグニチャ開発チームの監督下にある人のみが使用することを目的としています。String XL シグニチャは通常の正規表現または raw 正規表現のどちらかで設定できます。

a. [Regex String] フィールドに、このシグニチャが TCP パケット内で探す文字列を入力します（たとえば ht+p[¥r].）。

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

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

ステップ 13　（任意）ドロップダウン リストで [Yes] を選択し、次のオプションを有効にします。
- [Dot All]
- [Stingy]
- [UTF-8]

ステップ 14　（任意）[Alert Frequency] フィールドで、デフォルト アラート頻度を変更できます。

ステップ 15　[OK] 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　変更を破棄するには、[Cancel] をクリックします。

作成したシグニチャがイネーブルになり、シグニチャのリストに追加されます。

詳細情報

- String XL エンジンの詳細については、「String XL エンジン」（P.B-64）を参照してください。
- シグニチャの正規表現の一覧表については、「正規表現の構文」（P.B-10）を参照してください。
- String XL エンジンのシグニチャで使用できる特殊文字列の一覧表については、「特殊文字」（P.B-11）を参照してください。

シグニチャ変数の設定

ここでは、シグニチャ変数の設定方法について説明します。内容は次のとおりです。

シグニチャ変数のテーブル

（注）　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ことが必要です。

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。変数の値を変更した場合、その変数は、それが使用されているすべてのシグニチャで更新されます。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）　文字列ではなく変数を使用していることを示すために、変数の先頭にドル記号（$）を付ける必要があります。

一部の変数はシグニチャ システムに必要なため削除できません。変数が保護されている場合は、その変数を選択して編集できません。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。

[Signature Variables] タブのフィールド定義

[Signature Variables] タブと [Add Signature Variable] および [Edit Signature Variable] ダイアログボックスには次のフィールドがあります。

- [Name]：この変数に割り当てられる名前を示します。
- [Type]：変数を Web ポートまたは IP アドレス範囲として識別します。
- [Value]：この変数によって表される値を示します。

（注）　1 つの変数に複数のポート番号を指定する場合は、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 と入力します。

シグニチャ変数の追加、編集、削除

シグニチャ変数を追加、編集、および削除するには、次の手順を実行します。

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

ステップ 2　[Configuration] > *sensor_name* > [Policies] > [Signature Definitions] > [sig0] > [Active Signatures] > [Advanced] > [Signature Variables] の順に選択し、[Add] をクリックして変数を作成します。

ステップ 3　[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、数字とアルファベットのみを使用できます。また、ハイフン（-）またはアンダースコア（_）も使用できます。

ステップ 4　[Type] ドロップダウン リストで、シグニチャ変数のタイプを選択します。

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。

web-ports タイプは 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。

ヒント　変更内容を破棄して [Add Signature Variable] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 6　[OK] をクリックします。新しい変数が [Signature Variables] タブのシグニチャ変数リストに表示されます。

ステップ 7　既存の変数を編集するには、シグニチャ変数リストで変数を選択し、[Edit] をクリックします。

ステップ 8　[Value] フィールドに必要な変更を加えます。

ヒント　変更内容を破棄して [Edit Signature Variable] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 9　[OK] をクリックします。編集した変数が [Signature Variables] タブのシグニチャ変数リストに表示されます。

ステップ 10　変数を削除するには、リスト中のシグニチャ変数を選択し、[Delete] をクリックします。変数が [Signature Variables] タブ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　変更を破棄するには、[Reset] をクリックします。

ステップ 11　変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

その他の設定

ここでは、[Miscellaneous] タブと、Application Inspection および Control（AIC）シグニチャ、IP フラグメント再構成シグニチャ、TCP ストリーム再構成シグニチャ、および IP ロギングの設定方法について説明します。内容は次のとおりです。

- 「IP フラグメント再構成のシグニチャの設定」（P.9-46）
- 「TCP ストリーム再構成シグニチャの設定」（P.9-49）
- 「IP ロギングの設定」（P.9-57）

[Miscellaneous] タブ

（注）　[Miscellaneous] タブの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ことが必要です。

[Miscellaneous] タブ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（AIC シグニチャとも呼びます）の設定

  Web サービスに関連する悪意のある攻撃を防ぐため、レイヤ 4 からレイヤ 7 のパケット検査を行うようにセンサーを設定できます。AIC パラメータを設定した後、デフォルトの AIC シグニチャを使用または調整できます。

- 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。まず IP フラグメントの再構成にセンサーが使用する方法を選択し、Normalizer エンジンに含まれている IP フラグメント再構成シグニチャを調整します。

- TCP ストリーム再構成の設定

  センサーは、完了した 3 ウェイ ハンドシェイクによって確立された TCP セッションだけをモニタ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モニタ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 セッションの再構成機能は、センサーに対するこのような攻撃の緩和に役立ちます。まず TCP ストリームの再構成にセンサーが使用する方法を選択し、Normalizer エンジンに含まれている TCP ストリーム再構成シグニチャを調整します。

  （注）　シグニチャ 3050 Half Open SYN Attack では、アクションとして Modify Packet Inline を選択した場合、保護がアクティブな間パフォーマンスが 20 ～ 30% 低下する場合があります。保護は、実際の SYN フラッドの間のみアクティブになります。

- IP ロギング オプションの設定

  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、指定された時間の間ログに記録されます。

[Miscellaneous] タブのフィールド定義

[Miscellaneous] タブ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 ポリシー強制を設定できます。
  - [Enable HTTP]：Web サービスの保護をイネーブルにします。RFC に準拠するために、センサーで HTTP トラフィックを検査する必要がある場合は、[Yes] チェックボックスをオンにします。
  - [Max HTTP Requests]：接続あたりの未処理の HTTP 要求の最大数を指定します。
  - [AIC Web Ports]：AIC トラフィックを探す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。センサーで FTP トラフィックを検査する必要がある場合は、[Yes] チェックボックスをオンにします。
- [Fragment Reassembly]：IP フラグメント再構成のモードを設定できます。
  - [IP Reassembly Mode]：オペレーティング システムに基づいて、センサーがフラグメントの再構成に使用する方式を示します。
- [Stream Reassembly]：TCP ストリーム再構成のモードを設定できます。
  - [TCP Handshake Required]：センサーが、スリーウェイ ハンドシェイクが実行されたセッションだけを追跡することを指定します。
  - [TCP Reassembly Mode]：センサーが、次のオプションを使用する TCP セッションの再構成に使用するモードを指定します。
  - [Asymmetric]：双方向トラフィック フローのいずれかの方向だけをモニタできます。

    （注）　[Asymmetric] モードの場合、センサーは状態をフローと同期し、双方向を必要としないエンジンの検査を継続します。完全な保護には双方向のトラフィックを確認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が失われた場合、失われたパケット以降のすべてのパケットが処理されなくなります。
  - [Loose]：パケットがドロップ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に IP ロギングを停止するようにセンサーを設定できます。
  - [Max IP Log Packets]：ログに記録するパケット数を示します。
  - [IP Log Time]：センサーでログに記録する期間を示します。有効な値は、1 ～ 60 秒です。デフォルトは 30 秒です。
  - [Max IP Log Bytes]：記録する最大バイト数を示します。

Application Policy シグニチャの設定

ここでは、Application Policy（AIC）シグニチャと、それを設定する方法について説明します。内容は次のとおりです。

AIC シグニチャについて

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
  - 要求メソッドの定義
  - 認識された要求メソッド
- MIME タイプ
  - コンテンツ タイプの定義
  - 認識されたコンテンツ タイプ
- Web トラフィック ポリシーの定義

  準拠しない 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た、1 つのシグニチャ 12674 が事前に定義されています。パラメータ [Alarm on Non HTTP Traffic] によりこのシグニチャがイネーブルになります。デフォルトでは、このシグニチャはイネーブルになっています。
- 転送符号化
  - アクションを各メソッドに関連付け
  - センサーによって認識された方法の一覧表示
  - チャンク エンコーディング エラーが見つかった場合に実行するアクションの指定
- FTP コマンド
  - アクションを FTP コマンドに関連付けます。

AIC エンジンのセンサーのパフォーマンス

アプリケーション ポリシー強制は、センサー固有の機能です。悪用、脆弱性、および異常を検査する従来の IPS テクノロジーを基にするのではなく、AIC ポリシー強制は、HTTP および FTP サービス ポリシーを強制するように設計されています。このポリシー強制に必要な検査作業は、従来の IPS 検査作業と比べると非常に負荷が高いものになります。この機能を使用すると、大幅なパフォーマンス低下を招きます。AIC をイネーブルにした場合、センサーの全体的な帯域幅キャパシティが下がります。

AIC ポリシー強制は、IPS のデフォルト設定ではディセーブルになっています。AIC ポリシー強制をアクティブにする場合、関心がある正確なポリシーを慎重に選び、不要なポリシーをディセーブルにすることを強くお勧めします。また、センサーが最大検査容量に達している場合は、センサーがオーバーサブスクライブされるおそれがあるため、この機能を使用しないことをお勧めします。この種のポリシー強制を扱うには、適応型セキュリティ アプライアンス ファイアウォールを使用することをお勧めします。

詳細情報

AIC シグニチャ エンジンの詳細については、「AIC エンジン」（P.B-12）を参照してください。

AIC 要求メソッドのシグニチャ

HTTP 要求メソッドには次の 2 つのシグニチャ カテゴリがあります。

- 要求メソッドの定義：アクションを要求メソッドに関連付けることができます。シグニチャを拡張および変更できます（Define Request Method）。
- 認識されている要求メソッド：センサーによって認識されているメソッドを一覧表示します（Recognized Request Methods）。

表 9-1 に、定義済みの要求メソッド シグニチャの一覧を示します。必要な定義済みメソッドがあるシグニチャをイネーブルにしてください。

表 9-1　要求メソッドのシグニチャ

シグニチャ ID	定義済みの要求メソッド
12676	Request Method Not Recognized
12677	Define Request Method PUT
12678	Define Request Method CONNECT
12679	Define Request Method DELETE
12680	Define Request Method GET
12681	Define Request Method HEAD
12682	Define Request Method OPTIONS
12683	Define Request Method POST
12685	Define Request Method TRACE
12695	Define Request Method INDEX
12696	Define Request Method MOVE
12697	Define Request Method MKDIR
12698	Define Request Method COPY
12699	Define Request Method EDIT
12700	Define Request Method UNEDIT
12701	Define Request Method SAVE
12702	Define Request Method LOCK
12703	Define Request Method UNLOCK
12704	Define Request Method REVLABEL
12705	Define Request Method REVLOG
12706	Define Request Method REVADD
12707	Define Request Method REVNUM
12708	Define Request Method SETATTRIBUTE
12709	Define Request Method GETATTRIBUTENAME
12710	Define Request Method GETPROPERTIES
12711	Define Request Method STARTENV
12712	Define Request Method STOPREV

AIC MIME コンテンツ タイプの定義

MIME タイプに関連付けられているポリシーには次の 2 つがあります。

- コンテンツ タイプの定義：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
  - ヘッダーと本文で指定されている MIME タイプが一致しない
- 認識されたコンテンツ タイプ（Recognized Content Type）

表 9-2 に、定義済みのコンテンツ タイプ シグニチャの一覧を示します。必要な定義済みコンテンツ タイプがあるシグニチャをイネーブルにしてください。また、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。

表 9-2　コンテンツ タイプ シグニチャの定義

シグニチャ ID	シグニチャの説明
12621	Content Type image/gif Invalid Message Length
12622 2	Content Type image/png Verification Failed
12623 0 12623 1 12623 2	Content Type image/tiff Header Check Content Type image/tiff Invalid Message Length Content Type image/tiff Verification Failed
12624 0 12624 1 12624 2	Content Type image/x-3ds Header Check Content Type image/x-3ds Invalid Message Length Content Type image/x-3ds Verification Failed
12626 0 12626 1 12626 2	Content Type image/x-portable-bitmap Header Check Content Type image/x-portable-bitmap Invalid Message Length Content Type image/x-portable-bitmap Verification Failed
12627 0 12627 1 12627 2	Content Type image/x-portable-graymap Header Check Content Type image/x-portable-graymap Invalid Message Length Content Type image/x-portable-graymap Verification Failed
12628 0 12628 1 12628 2	Content Type image/jpeg Header Check Content Type image/jpeg Invalid Message Length Content Type image/jpeg Verification Failed
12629 0 12629 1	Content Type image/cgf Header Check Content Type image/cgf Invalid Message Length
12631 0 12631 1	Content Type image/x-xpm Header Check Content Type image/x-xpm Invalid Message Length
12633 0 12633 1 12633 2	Content Type audio/midi Header Check Content Type audio/midi Invalid Message Length Content Type audio/midi Verification Failed
12634 0 12634 1 12634 2	Content Type audio/basic Header Check Content Type audio/basic Invalid Message Length Content Type audio/basic Verification Failed
12635 0 12635 1 12635 2	Content Type audio/mpeg Header Check Content Type audio/mpeg Invalid Message Length Content Type audio/mpeg Verification Failed

表 9-2　コンテンツ タイプ シグニチャの定義（続き）

シグニチャ ID	シグニチャの説明
12636 0	Content Type audio/x-adpcm Header Check
12636 1	Content Type audio/x-adpcm Invalid Message Length
12636 2	Content Type audio/x-adpcm Verification Failed
12637 0	Content Type audio/x-aiff Header Check
12637 1	Content Type audio/x-aiff Invalid Message Length
12637 2	Content Type audio/x-aiff Verification Failed
12638 0	Content Type audio/x-ogg Header Check
12638 1	Content Type audio/x-ogg Invalid Message Length
12638 2	Content Type audio/x-ogg Verification Failed
12639 0	Content Type audio/x-wav Header Check
12639 1	Content Type audio/x-wav Invalid Message Length
12639 2	Content Type audio/x-wav Verification Failed
12641 0	Content Type text/html Header Check
12641 1	Content Type text/html Invalid Message Length
12641 2	Content Type text/html Verification Failed
12642 0	Content Type text/css Header Check
12642 1	Content Type text/css Invalid Message Length
12643 0	Content Type text/plain Header Check
12643 1	Content Type text/plain Invalid Message Length
12644 0	Content Type text/richtext Header Check
12644 1	Content Type text/richtext Invalid Message Length
12645 0	Content Type text/sgml Header Check
12645 1	Content Type text/sgml Invalid Message Length
12645 2	Content Type text/sgml Verification Failed
12646 0	Content Type text/xml Header Check
12646 1	Content Type text/xml Invalid Message Length
12646 2	Content Type text/xml Verification Failed
12648 0	Content Type video/flc Header Check
12648 (1)	Content Type video/flc Invalid Message Length
12648 2	Content Type video/flc Verification Failed
12649 0	Content Type video/mpeg Header Check
12649 1	Content Type video/mpeg Invalid Message Length
12649 2	Content Type video/mpeg Verification Failed
12650 0	Content Type text/xmcd Header Check
12650 1	Content Type text/xmcd Invalid Message Length
12651 0	Content Type video/quicktime Header Check
12651 1	Content Type video/quicktime Invalid Message Length
12651 2	Content Type video/quicktime Verification Failed
12652 0	Content Type video/sgi Header Check
12652 1	Content Type video/sgi Verification Failed
12653 0	Content Type video/x-avi Header Check
12653 1	Content Type video/x-avi Invalid Message Length
12654 0	Content Type video/x-fli Header Check
12654 1	Content Type video/x-fli Invalid Message Length
12654 2	Content Type video/x-fli Verification Failed

表 9-2　コンテンツ タイプ シグニチャの定義（続き）

シグニチャ ID	シグニチャの説明
12655 0	Content Type video/x-mng Header Check
12655 1	Content Type video/x-mng Invalid Message Length
12655 2	Content Type video/x-mng Verification Failed
12656 0	Content Type application/x-msvideo Header Check
12656 1	Content Type application/x-msvideo Invalid Message Length
12656 2	Content Type application/x-msvideo Verification Failed
12658 0	Content Type application/ms-word Header Check
12658 1	Content Type application/ms-word Invalid Message Length
12659 0	Content Type application/octet-stream Header Check
12659 1	Content Type application/octet-stream Invalid Message Length
12660 0	Content Type application/postscript Header Check
12660 1	Content Type application/postscript Invalid Message Length
12660 2	Content Type application/postscript Verification Failed
12661 0	Content Type application/vnd.ms-excel Header Check
12661 1	Content Type application/vnd.ms-excel Invalid Message Length
12662 0	Content Type application/vnd.ms-powerpoint Header Check
12662 1	Content Type application/vnd.ms-powerpoint Invalid Message Length
12663 0	Content Type application/zip Header Check
12663 1	Content Type application/zip Invalid Message Length
12663 2	Content Type application/zip Verification Failed
12664 0	Content Type application/x-gzip Header Check
12664 1	Content Type application/x-gzip Invalid Message Length
12664 2	Content Type application/x-gzip Verification Failed
12665 0	Content Type application/x-java-archive Header Check
12665 1	Content Type application/x-java-archive Invalid Message Length
12666 0	Content Type application/x-java-vm Header Check
12666 1	Content Type application/x-java-vm Invalid Message Length
12667 0	Content Type application/pdf Header Check
12667 1	Content Type application/pdf Invalid Message Length
12667 2	Content Type application/pdf Verification Failed
12668 0	Content Type unknown Header Check
12668 1	Content Type unknown Invalid Message Length
12669 0	Content Type image/x-bitmap Header Check
12669 1	Content Type image/x-bitmap Invalid Message Length
12673 0	認識されたコンテンツ タイプ

AIC 転送符号化のシグニチャ

転送符号化に関連付けられているポリシーには次の 3 つがあります。

- アクションを各メソッドに関連付け（Define Transfer Encoding）
- センサーによって認識された方法の一覧表示（Recognized Transfer Encodings）
- チャンク エンコーディング エラーが見つかった場合に実行するアクションの指定（Chunked Transfer Encoding Error）

表 9-3 に、定義済みの転送符号化シグニチャの一覧を示します。必要な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てください。

表 9-3　転送符号化のシグニチャ

シグニチャ ID	転送符号化方法
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 コマンドのシグニチャ

表 9-4 に、定義済みの FTP コマンドのシグニチャの一覧を示します。必要な定義済み FTP コマンドがあるシグニチャをイネーブルにしてください。

表 9-4　FTP コマンドのシグニチャ

シグニチャ ID	FTP コマンド
12900	認識されない 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
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

表 9-4　FTP コマンドのシグニチャ（続き）

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

アプリケーション ポリシーを設定するには、次の手順を実行します。

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

ステップ 2　[Configuration] > *sensor_name* > [Policies] > [Signature Definitions] > [sig0] > [Active Signatures] > [Advanced] > [Miscellaneous] の順に選択します。

ステップ 3　[Enable HTTP] フィールドで、ドロップダウン リストから [Yes] を選択し、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] フィールドに、接続あたりの、サーバからの応答を受信せずに処理待ちになることができる未処理の HTTP 要求の数を入力します。

ステップ 5　[AIC Web Ports] フィールドに、アクティブにするポートを入力します。

ステップ 6　[Enable FTP] フィールドで、ドロップダウン リストから [Yes] を選択し、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、センサーは、トラフィックが RFC に準拠していることを確認します。

ヒント　変更を破棄するには、[Cancel] をクリックします。

ステップ 7　[OK] をクリックします。

ヒント　変更を破棄するには、[Reset] をクリックします。

ステップ 8　変更を適用し、変更後の設定を保存するには、[Apply] をクリックします。

AIC シグニチャの調整

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

次の例は、AIC シグニチャ、Recognized Content Type（MIME）シグニチャ、特にシグニチャ 12,623 1 Content Type image/tiff Invalid Message Length を調整する方法を示しています。

MIME タイプ ポリシー シグニチャを調整するには、次の手順を実行します。

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

ステップ 2　[Configuration] > *sensor_name* > [Policies] > [Signature Definitions] > [sig0] > [Active Signatures] の順に選択します。

ステップ 3　[Filter] ドロップダウン リストから [Engine] を選択し、エンジンとして [AIC HTTP] を選択します。

ステップ 4　リストを下にスクロールして [Sig ID 12,623 Subsig ID 1 Content Type image/tiff Invalid Message Length] を選択し、[Edit] をクリックします。

ヒント　[Sig ID] 列見出しをクリックすると、シグニチャ ID が順番に表示されます。

ステップ 5　[Status] で、[Enabled] フィールドのドロップダウン リストから [Yes] を選択します。

ステップ 6　[Engine] の下で、いずれかのオプション（たとえば [Content Type Details] フィールドの [Length]）を選択します。

ステップ 7　[Length] フィールドで、デフォルトを 30,000 に変更することで長さを短くします。

ヒント　変更内容を破棄して [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。

ステップ 8　[OK]、[Apply] の順にクリックし、変更内容を保存します。

ヒント　変更を破棄するには、[Reset] をクリックします。

IP フラグメント再構成のシグニチャの設定

ここでは、IP フラグメント再構成について説明し、IP フラグメント再構成のシグニチャとその設定可能なパラメータの一覧を示し、それらの設定方法について説明します。内容は次のとおりです。

IP フラグメント再構成シグニチャの概要

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、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。

（注）　IP フラグメント再構成はシグニチャごとに設定します。

詳細情報

Normalizer シグニチャ エンジンの詳細については、「Normalizer エンジン」（P.B-38）を参照してください。

IP フラグメント再構成シグニチャと設定可能パラメータ

表 9-5 に、IP フラグメント再構成シグニチャと、IP フラグメント再構成で設定可能なパラメータの一覧を示します。IP フラグメント再構成シグニチャは Normalizer エンジンに含まれています。

表 9-5　IP フラグメント再構成シグニチャ

シグニチャの ID と名前	説明	パラメータとそのデフォルトおよび範囲	デフォルト アクション
1200 IP Fragmentation Buffer Full	システム内のフラグメントの総数が、Max Fragments で設定されたしきい値を超えた場合に起動されます。	Specify Max Fragments 10000（0 ～ 42000）	Deny Packet Inline Produce Alert[1]
1201 Fragment Overlap	1 つのデータグラムに対しキューに格納された複数のフラグメントが互いに重なる場合に起動されます。	なし[2]	
1202 Datagram Too Long	フラグメント データ（オフセットとサイズ）が、Max Datagram Size で設定されているしきい値を超えた場合に起動されます。	Specify Max Datagram Size 65536（2000 ～ 65536）	Deny Packet Inline Produce Alert[3]

表 9-5　IP フラグメント再構成シグニチャ（続き）

シグニチャの ID と名前	説明	パラメータとそのデフォルトおよび範囲	デフォルト アクション
1203 Fragment Overwrite	1 つのデータグラムに対しキューに格納された複数のフラグメントが互いに重なっており、重なっているデータが異なる場合に起動されます。[4]	なし	Deny Packet Inline Produce Alert[5]
1204 No Initial Fragment	データグラムが不完全で最初のフラグメントが不足している場合に起動されます。	なし	Deny Packet Inline Produce Alert[6]
1205 Too Many Datagrams	システム内の部分的なデータグラムの総数が、Max Partial Datagrams で設定されたしきい値を超えた場合に起動されます。	Specify Max Partial Datagrams 1000（0 ～ 10000）	Deny Packet Inline Produce Alert[7]
1206 Fragment Too Small	1 つのデータグラム中で、Min Fragment Size よりも小さいフラグメントの数が Max Small Frags を超えた場合に起動されます。[8]	Specify Max Small Frags 2（8 ～ 1500） Specify Min Fragment Size 400（1 ～ 8）	Deny Packet Inline Produce Alert[9]
1207 Too Many Fragments	1 つのデータグラム中に、Max Fragments per Datagram を超えるフラグメントがある場合に起動されます。	Specify Max Fragments per Datagram 170（0 ～ 8192）	Deny Packet Inline Produce Alert[10]
1208 Incomplete Datagram	あるデータグラムのすべてのフラグメントが Fragment Reassembly Timeout で指定された時間内に到着しなかった場合に起動されます。[11]	Specify Fragment Reassembly Timeout 60（0 ～ 360）	Deny Packet Inline Produce Alert[12]
1220 Jolt2 Fragment Reassembly DoS attack	複数のフラグメントが受信され、すべてが IP データグラムの最後のフラグメントであることを示している場合に起動されます。	Specify Max Last Fragments 4（1 ～ 50）	Deny Packet Inline Produce Alert[13]
1225 Fragment Flags Invalid	フラグメント フラグの不正な組み合わせが検出された場合に起動されます。	なし[14]	

1. Modify Packet Inline および Deny Connection Inline は、このシグニチャに影響を与えません。Deny Packet Inline は、このパケットと、このデータグラムの関連するすべてのフラグメントをドロップします。このシグニチャをディセーブルにした場合、デフォルト値が引き続き使用され、パケットはドロップされるか（インライン モード）分析されず（無差別モード）、アラートは送信されません。
2. このシグニチャは、データグラムが完全に重複している場合は起動されません。完全な重複は、インライン モードでは設定にかかわらずドロップされます。Modify Packet Inline では、重なっているデータが、1 つを除きすべて削除されるため、エンドポイントがデータグラムを処理する方法について曖昧さはありません。Deny Connection Inline は、このシグニチャに影響を与えません。Deny Packet Inline は、このパケットと、このデータグラムの関連するすべてのフラグメントをドロップします。
3. Modify Packet Inline および Deny Connection Inline は、このシグニチャに影響を与えません。Deny Packet Inline は、このパケットと、このデータグラムの関連するすべてのフラグメントをドロップします。設定されたアクションにかかわらず、データグラムが Max Datagram Size よりも大きい場合、データグラムは IPS によって処理されません。
4. これは非常にまれなイベントです。
5. Modify Packet Inline では、重なっているデータが、1 つを除きすべて削除されるため、エンドポイントがデータグラムを処理する方法について曖昧さはありません。Deny Connection Inline は、このシグニチャに影響を与えません。Deny Packet Inline は、このパケットと、このデータグラムの関連するすべてのフラグメントをドロップします。
6. IPS は、設定にかかわらず、先頭フラグメントが不足しているデータグラムを検査しません。Modify Packet Inline および Deny Connection Inline は、このシグニチャに影響を与えません。Deny Packet Inline は、このパケットと、このデータグラムの関連するすべてのフラグメントをドロップします。

7. Modify Packet Inline および Deny Connection Inline は、このシグニチャに影響を与えません。Deny Packet Inline は、このパケットと、このデータグラムの関連するすべてのフラグメントをドロップします。
8. このシグニチャがオンであり、小さなフラグメントの数が超えた場合、IPS はデータグラムを検査しません。
9. Modify Packet Inline および Deny Connection Inline は、このシグニチャに影響を与えません。Deny Packet Inline は、このパケットと、このデータグラムの関連するすべてのフラグメントをドロップします。
10. Modify Packet Inline および Deny Connection Inline は、このシグニチャに影響を与えません。Deny Packet Inline は、このパケットと、このデータグラムの関連するすべてのフラグメントをドロップします。
11. データグラムのパケットが到着するとタイマーが開始されます。
12. Modify Packet Inline および Deny Connection Inline は、このシグニチャに影響を与えません。Deny Packet Inline は、このパケットと、このデータグラムの関連するすべてのフラグメントをドロップします。
13. Modify Packet Inline および Deny Connection Inline は、このシグニチャに影響を与えません。Deny Packet Inline は、このパケットと、このデータグラムの関連するすべてのフラグメントをドロップします。
14. Modify Packet Inline は、フラグを有効な組み合わせに変更します。Deny Connection Inline は、このシグニチャに影響を与えません。Deny Packet Inline は、このパケットと、このデータグラムの関連するすべてのフラグメントをドロップします。

IP フラグメント再構成モードの設定

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

（注）　IP フラグメント再構成モードは、センサーが無差別モードで動作している場合に設定できます。センサーがインライン モードで動作している場合、方法は NT のみです。

センサーが IP フラグメント再構成のために使用する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　管理者権限またはオペレータ権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Policies] > [Signature Definitions] > [sig0] > [Active Signatures] > [Advanced] > [Miscellaneous] の順に選択します。

ステップ 3　[Fragment Reassembly] で、[IP Reassembly Mode] フィールドから、フラグメントを再構成するため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　選択を破棄して [Advanced] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 4　変更を適用し、変更後の設定を保存するには、[OK] をクリックし、[Apply] をクリックします。

ヒント　変更を破棄するには、[Reset] をクリックします。

IP フラグメント再構成シグニチャの調整

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

次の手順は、IP フラグメント再構成シグニチャ、特にシグニチャ 1200 0 IP Fragmentation Buffer Full の調整方法を示しています。

IP フラグメント再構成シグニチャを調整するには、次の手順を実行します。

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

ステップ 2　[Configuration] > *sensor_name* > [Policies] > [Signature Definitions] > [sig0] > [Active Signatures] の順に選択します。

ステップ 3　[Filter] フィールドで、ドロップダウン リストから [Engine] を選択し、エンジンとして [Normalizer] を選択します。

ステップ 4　リスト中で設定する IP フラグメント アセンブリ シグニチャを選択し（たとえば [Sig ID 1200 Subsig ID 0 IP Fragmentation Buffer Full]）、[Edit] をクリックします。

ステップ 5　シグニチャ 1200 に対して設定可能な、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] フィールドで、デフォルトの 10000 から 20000 に設定を変更します。

シグニチャ 1200 では、次のオプションのパラメータも変更できます。

- [Specify TCP Idle Timeout]
- [Specify Service Ports]
- [Specify SYN Flood Max Embryonic]

ヒント　変更内容を破棄して [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。

ステップ 6　変更を適用し、変更後の設定を保存するには、[OK] をクリックし、[Apply] をクリックします。

ヒント　変更を破棄するには、[Reset] をクリックします。

TCP ストリーム再構成シグニチャの設定

ここでは、TCP ストリーム再構成について説明し、TCP ストリーム再構成シグニチャと設定可能パラメータの一覧を示し、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。ここでは、次の項目について説明します。

- 「TCP ストリーム再構成シグニチャの概要」（P.9-50）
- 「TCP ストリーム再構成シグニチャと設定可能パラメータ」（P.9-50）

- 「TCP ストリーム再構成モードの設定」（P.9-55）
- 「TCP ストリーム再構成シグニチャの調整」（P.9-56）

TCP ストリーム再構成シグニチャの概要

センサーは、完了した 3 ウェイ ハンドシェイクによって確立された TCP セッションだけをモニタ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モニタ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 セッションの再構成機能は、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。

詳細情報

Normalizer シグニチャ エンジンの詳細については、「Normalizer エンジン」（P.B-38）を参照してください。

TCP ストリーム再構成シグニチャと設定可能パラメータ

表 9-6 に、TCP ストリーム再構成シグニチャと、TCP ストリーム再構成で設定可能なパラメータの一覧を示します。TCP ストリーム再構成シグニチャは Normalizer エンジンに含まれています。

表 9-6　TCP ストリーム再構成シグニチャ

シグニチャの ID と名前	説明	パラメータとそのデフォルトおよび範囲	デフォルト アクション
1300 TCP Segment Overwrite[1]	重なっている TCP セグメント（再送など）のデータが、すでにこのセッションで検出されているデータと異なるデータを送信する場合に起動されます。	—	Deny Connection Inline Product Alert[2]
1301 TCP Inactive Timeout[3]	TCP セッションが TCP Idle Timeout で指定された時間アイドルだった場合に起動されます。	TCP Idle Timeout 3600（15 ～ 3600）	なし[4]
1302 TCP Embryonic Timeout[5]	TCP セッションが、TCP 初期接続タイムアウト内にスリーウェイ ハンドシェイクを完了しなかった場合に起動されます。	TCP Embryonic Timeout 15（3 ～ 300）	なし[6]
1303 TCP Closing Timeout[7]	TCP セッションが、最初の FIN から TCP Closed Timeout 秒以内に完全にクローズされなかった場合に起動されます。	TCP Closed Timeout 5（1 ～ 60）	なし[8]

表 9-6　TCP ストリーム再構成シグニチャ（続き）

シグニチャの ID と名前	説明	パラメータとそのデフォルトおよび範囲	デフォルト アクション
1304 TCP Max Segments Queued Per Session	1 つのセッションについて、キューに格納されている順序が不正なセグメントの数が、TCP Max Queue を超えた場合に起動されます。期待されるシーケンスから最も遠いシーケンスが含まれるセグメントがドロップされます。	TCP Max Queue 32（0 ～ 128）	Deny Packet Inline Product Alert[9]
1305 TCP Urgent Flag[10]	TCP 緊急フラグが検出された場合に起動されます。	—	Modify Packet Inline はディセーブルになります[11]
1306 0 TCP Option Other	TCP Option Number の範囲内の TCP オプションが検出された場合に起動されます。	TCP Option Number 6 ～ 7、9 ～ 255（Integer Range Allow Multiple 0 ～ 255 制約）	Modify Packet Inline Produce Alert[12]
1306 1 TCP SACK Allowed Option	TCP 選択 ACK 許可オプションが検出された場合に起動されます。	—	Modify Packet Inline はディセーブルになります[13]
1306 2 TCP SACK Data Option	TCP 選択 ACK データ オプションが検出された場合に起動されます。	—	Modify Packet Inline はディセーブルになります[14]
1306 3 TCP Timestamp Option	TCP タイムスタンプ オプションが検出された場合に起動されます。	—	Modify Packet Inline はディセーブルになります[15]
1306 4 TCP Window Scale Option	TCP ウィンドウ スケール オプションが検出された場合に起動されます。	—	Modify Packet Inline はディセーブルになります[16]
1307 TCP Window Size Variation	TCP の recv ウィンドウの右端が右に移動（減少）した場合に起動されます。	—	Deny Connection Inline Produce Alert がディセーブルになります[17]
1308 TTL Varies[18]	セッションの一方で検出された TTL が、観察された最小値よりも大きい場合に起動されます。	—	Modify Packet Inline[19]
1309 TCP Reserved Bits Set	予約ビット（ECN が使用するビットを含む）が TCP ヘッダーで設定されている場合に起動されます。	—	Modify Packet Inline Produce Alert がディセーブルになります[20]

表 9-6　TCP ストリーム再構成シグニチャ（続き）

シグニチャの ID と名前	説明	パラメータとそのデフォルトおよび範囲	デフォルト アクション
1310 TCP Retransmit Protection[21]	再送されたセグメントのデータが元のセグメントと異なることをセンサーが検出した場合に起動されます。	—	Deny Connection Inline Produce Alert[22]
1311 TCP Packet Exceeds MSS	パケットが、スリーウェイ ハンドシェイクの最中に交換された MSS を超えた場合に起動されます。	—	Deny Connection Inline Produce Alert[23]
1312 TCP Min MSS	SYN フラグが含まれているパケット中の MSS 値が TCP Min MSS よりも小さい場合に起動されます。	TCP Min MSS 400（0 ～ 16000）	Modify Packet Inline はディセーブルになります[24]
1313 TCP Max MSS	SYN フラグが含まれているパケット中の MSS 値が TCP Max MSS よりも大きい場合に起動されます。	TCP Max MSS1460（0 ～ 16000）	Modify Packet Inline はディセーブルになります[25]
1314 TCP Data SYN	TCP ペイロードが SYN パケットで送信された場合に起動されます。	—	Deny Packet Inline はディセーブルになります[26]
1315 ACK Without TCP Stream	ストリームに属さない ACK パケットが送信された場合に起動されます。	—	Produce Alert がディセーブルになります[27]
1317 Zero Window Probe	ゼロ ウィンドウ プローブ パケットが検出された場合に起動されます。	Modify Packet Inline は、ゼロ ウィンドウ プローブ パケットからデータを削除します。	Modify Packet Inline
1330[28] 0 TCP Drop - Bad Checksum	TCP パケットのチェックサムが不正な場合に起動されます。	Modify Packet Inline はチェックサムを訂正します。	Deny Packet Inline
1330 1 TCP Drop - Bad TCP Flags	TCP パケットのフラグの組み合わせが不正な場合に起動されます。	—	Deny Packet Inline
1330 2 TCP Drop - Urgent Pointer With No Flag	TCP パケットに URG ポインタがあり URG フラグがない場合に起動されます。	Modify Packet Inline はポインタをクリアします。	Modify Packet Inline はディセーブルになります
1330 3 TCP Drop - Bad Option List	TCP パケットのオプション リストが不正な場合に起動されます。	—	Deny Packet Inline

表 9-6　TCP ストリーム再構成シグニチャ（続き）

シグニチャの ID と名前	説明	パラメータとそのデフォルトおよび範囲	デフォルト アクション
1330 4 TCP Drop - Bad Option Length	TCP パケットのオプションの長さが不正な場合に起動されます。	—	Deny Packet Inline
1330 5 TCP Drop - MSS Option Without SYN	TCP MSS オプションがパケット内に検出され、SYN フラグが設定されていない場合に起動されます。	Modify Packet Inline は MSS オプションをクリアします。	Modify Packet Inline
1330 6 TCP Drop - WinScale Option Without SYN	TCP ウィンドウ スケール オプションがパケット内に検出され、SYN フラグが設定されていない場合に起動されます。	Modify Packet Inline はウィンドウ スケール オプションをクリアします。	Modify Packet Inline
1330 7 TCP Drop - Bad WinScale Option Value	TCP パケットのウィンドウ スケール値が不正な場合に起動されます。	Modify Packet Inline は、値を最も近い制約値に設定します。	Modify Packet Inline
1330 8 TCP Drop - SACK Allow Without SYN	TCP SACK 許可オプションが、SYN フラグが設定されていないパケット中に検出された場合に起動されます。	Modify Packet Inline は SACK 許可オプションをクリアします。	Modify Packet Inline
1330 9 TCP Drop - Data in SYN|ACK	SYN フラグと ACK フラグが設定されている TCP パケットにデータも含まれている場合に起動されます。	—	Deny Packet Inline
1330 10 TCP Drop - Data Past FIN	TCP データのシーケンスが FIN の後になっている場合に起動されます。	—	Deny Packet Inline
1330 11 TCP Drop - Timestamp not Allowed	タイムスタンプ オプションが許可されていないときに、TCP パケットにタイムスタンプ オプションが設定されている場合に起動されます。	—	Deny Packet Inline
1330 12 TCP Drop - Segment Out of Order	TCP セグメントの順序が不正でキューに格納できない場合に起動されます。	—	Deny Packet Inline
1330 13 TCP Drop - Invalid TCP Packet	TCP パケットのヘッダーが不正な場合に起動されます。	—	Deny Packet Inline

表 9-6　TCP ストリーム再構成シグニチャ（続き）

シグニチャの ID と名前	説明	パラメータとそのデフォルトおよび範囲	デフォルト アクション
1330 14 TCP Drop - RST or SYN in window	RST または SYN フラグが設定された TCP パケットがシーケンス ウィンドウ中で送信されたものの、次のシーケンスでない場合に起動されます。	—	Deny Packet Inline
1330 15 TCP Drop - Segment Already ACKed	TCP パケット シーケンスが、ピアによってすでに肯定応答済みである場合に起動されます（キープアライブを除く）。	—	Deny Packet Inline
1330 16 TCP Drop - PAWS Failed	TCP パケットが PAWS チェックに失敗した場合に起動されます。	—	Deny Packet Inline
1330 17 TCP Drop - Segment out of State Order	TCP パケットが TCP セッション状態に対して正しくない場合に起動されます。	—	Deny Packet Inline
1330 18 TCP Drop - Segment out of Window	TCP パケットのシーケンス番号が許可されたウィンドウに収まっていない場合に起動されます。	—	Deny Packet Inline
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. IPS は、TCP セッションの各方向で最後の 256 バイトを保持しています。
2. Modify Packet Inline は、このシグニチャに影響を与えません。Deny Connection Inline は現在のパケットと TCP セッションをドロップします。Deny Packet Inline はパケットをドロップします。
3. TCP セッションの各パケットの後、タイマーは 0 にリセットされます。デフォルトでは、このシグニチャはアラートを生成しません。必要に応じて、期限切れの TCP 接続に対してアラートを生成することを選択できます。期限満了フローの総数の統計情報は、フローの期限が満了するたびに更新されます。
4. Modify Packet Inline、Deny Connection Inline、および Deny Packet Inline は、このシグニチャに影響を与えません。
5. タイマーは最初の SYN パケットで開始され、リセットされません。セッションの状態がリセットされ、このフローの以降のすべてのパケットは順序が不正になります（SYN 以外）。
6. Modify Packet Inline、Deny Connection Inline、および Deny Packet Inline は、このシグニチャに影響を与えません。
7. タイマーは最初の FIN パケットで開始され、リセットされません。セッションの状態がリセットされ、このフローの以降のすべてのパケットは順序が不正になります（SYN 以外）。
8. Modify Packet Inline、Deny Connection Inline、および Deny Packet Inline は、このシグニチャに影響を与えません。
9. Modify Packet Inline および Deny Packet Inline は、このシグニチャに影響を与えません。Deny Connection Inline は現在のパケットと TCP セッションをドロップします。
10. Phrak 57 には、URG ポインタを使用してセキュリティ ポリシーを回避する方法が記述されています。インライン モードの場合、このシグニチャを使用してパケットを正規化できます。
11. Modify Packet Inline は URG フラグを除去し、パケットの URG ポインタをゼロにします。Deny Connection Inline は現在のパケットと TCP セッションをドロップします。Deny Packet Inline はパケットをドロップします。

12. Modify Packet Inline は、選択したオプションをパケットから除去します。Deny Connection Inline は現在のパケットと TCP セッションをドロップします。Deny Packet Inline はパケットをドロップします。
13. Modify Packet Inline は、選択 ACK 許可オプションをパケットから除去します。Deny Connection Inline は現在のパケットと TCP セッションをドロップします。Deny Packet Inline はパケットをドロップします。
14. Modify Packet Inline は、選択 ACK 許可オプションをパケットから除去します。Deny Connection Inline は現在のパケットと TCP セッションをドロップします。Deny Packet Inline はパケットをドロップします。
15. Modify Packet Inline は、タイムスタンプ オプションをパケットから除去します。Deny Connection Inline は現在のパケットと TCP セッションをドロップします。Deny Packet Inline はパケットをドロップします。
16. Modify Packet Inline は、ウィンドウ スケール オプションをパケットから除去します。Deny Connection Inline は現在のパケットと TCP セッションをドロップします。Deny Packet Inline はパケットをドロップします。
17. Modify Packet Inline は、このシグニチャに影響を与えません。Deny Connection Inline は現在のパケットと TCP 接続をドロップします。Deny Packet Inline はパケットをドロップします。
18. このシグニチャは、TTL を、セッションの各方向で単調に減少させるために使用します。たとえば、TTL 45 が、A から B に向かって検出される最も小さい TTL であり、Modify Packet Inline が設定されている場合、A から B 宛の将来のすべてのパケットの最大は 45 になります。それぞれの新しい小さい TTL は、そのセッション上のパケットの新しい最大値になります。
19. Modify Packet Inline は、IP TTL が単調に減少するようにします。Deny Connection Inline は現在のパケットと TCP セッションをドロップします。Deny Packet Inline はパケットをドロップします。
20. Modify Packet Inline は、予約されているすべての TCP フラグをクリアします。Deny Connection Inline は現在のパケットと TCP セッションをドロップします。Deny Packet Inline はパケットをドロップします。
21. このシグニチャは、シグニチャ 1300 のように、最後の 256 バイトに限定されません。
22. Modify Packet Inline は、このシグニチャに影響を与えません。Deny Connection Inline は現在のパケットと TCP 接続をドロップします。Deny Packet Inline はパケットをドロップします。
23. Modify Packet Inline は、このシグニチャに影響を与えません。Deny Connection Inline は現在のパケットと TCP 接続をドロップします。Deny Packet Inline はパケットをドロップします。
24. 2.4.21-15.EL.cisco.1 Modify Packet Inline は、MSS 値を TCP Min MSS に引き上げます。Deny Connection Inline は現在のパケットと TCP セッションをドロップします。Deny Packet Inline は、パケット 2.4.21-15.EL.cisco.1 をドロップします。
25. Modify Packet Inline は、MSS 値を TCP Max MSS に引き下げます。Deny Connection Inline は現在のパケットと TCP セッションをドロップします。Deny Packet Inline は、パケット 2.4.21-15.EL.cisco.1 をドロップします。
26. Modify Packet Inline は、このシグニチャに影響を与えません。Deny Connection Inline は現在のパケットと TCP セッションをドロップします。Deny Packet Inline はパケットをドロップします。
27. Modify Packet Inline、Deny Connection Inline、および Deny Packet Inline は、このシグニチャに影響を与えません。デフォルトでは、1330 シグニチャは、このシグニチャがアラートを送信するパケットをドロップします。
28. これらのサブシグニチャは、ノーマライザが TCP パケットをドロップする可能性がある理由を表します。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、IPS を通じてノーマライザ内のチェックに失敗したパケットを許可できます。ドロップ理由のエントリが、TCP 統計情報の中に作成されます。デフォルトでは、サブシグニチャはアラートを生成しません。

TCP ストリーム再構成モードの設定

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

（注）　パラメータ TCP Handshake Required および TCP Reassembly Mode は、インライン モードではなく、無差別モードでトラフィックを検査しているセンサーのみに影響します。インライン トラフィックを検査しているセンサーの非対称オプションを設定するには、Normalizer Mode パラメータを使用します。

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

ステップ 2　[Configuration] > *sensor_name* > [Policies] > [Signature Definitions] > [sig0] > [Active Signatures] > [Advanced] > [Miscellaneous] の順に選択します。

ステップ 3　[Stream Reassembly] の [TCP Handshake Required] フィールドで、[Yes] を選択します。[TCP Handshake Required] を選択すると、スリーウェイ ハンドシェイクが実行されたセッションだけを追跡するようセンサーに指定します。

ステップ 4　[TCP Reassembly Mode] フィールドで、ドロップダウン リストから、TCP セッションを再構成するためにセンサーが使用するモードを選択します。

- **[Asymmetric]**：センサーは状態をフローと同期し、双方向を必要としないエンジンの検査を継続します。
- **[Strict]**：何らかの理由でパケットが失われた場合、失われたパケット以降のすべてのパケットが処理されます。
- **[Loose]**：パケットがドロップされる可能性がある場合に使用します。

ヒント　選択を破棄して [Advanced] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 5　変更を適用し、変更後の設定を保存するには、[OK] をクリックし、[Apply] をクリックします。

ヒント　変更を破棄するには、[Reset] をクリックします。

詳細情報

インライン モードに設定されたセンサーの非対称検査オプションについては、「インライン TCP セッション トラッキング モード」（P.8-4）および「インライン TCP セッション トラッキング モード」（P.8-4）を参照してください。

TCP ストリーム再構成シグニチャの調整

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

注意　シグニチャ 3050 Half Open SYN Attack では、アクションとして Modify Packet Inline を選択した場合、保護がアクティブな間パフォーマンスが 20 ～ 30% 低下する場合があります。保護は、実際の SYN フラッドの間のみアクティブになります。

次の手順は、TCP ストリーム再構成シグニチャ（たとえばシグニチャ 1313 0 TCP MSS Exceeds Maximum）を調整する方法を示しています。

TCP ストリーム再構成シグニチャを調整するには、次の手順を実行します。

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

ステップ 2　[Configuration] > *sensor_name* > [Policies] > [Signature Definitions] > [sig0] > [Active Signatures] の順に選択します。

ステップ 3　[Filter] ドロップダウン リストから [Engine] を選択し、[Normalizer] を選択します。

ステップ 4　リスト中で設定する TCP フラグメント アセンブリ シグニチャを選択し（たとえば [Sig ID 1313 Subsig ID 0 TCP MSS Exceeds Maximum]）、[Edit] をクリックします。

ステップ 5　シグニチャ 1313 に対して設定可能な、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] フィールドで、デフォルトの 1460 から 1380 に設定を変更します。

（注）　このパラメータをデフォルトの 1460 から 1380 に変更することにより、VPN トンネルを通過するトラフィックのフラグメンテーションが禁止されます。

シグニチャ 1313 0 では、次のオプションのパラメータも変更できます。

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

ヒント　変更内容を破棄して [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。

ステップ 6　変更を適用し、変更後の設定を保存するには、[OK] をクリックし、[Apply] をクリックします。

ヒント　変更を破棄するには、[Reset] をクリックします。

IP ロギングの設定

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

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、指定された時間の間ログに記録されます。センサーがいずれかの IP ロギング条件を満たしている場合、IP ロギングが停止されます。

IP ロギング 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　管理者権限またはオペレータ権限を持つアカウントを使用して IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Policies] > [Signature Definitions] > [sig0] > [Active Signatures] > [Advanced] > [Miscellaneous] の順に選択します。

ステップ 3　[IP Log in the Max IP Log Packets] フィールドに、ログに記録するパケットの数を入力します。

ステップ 4　[IP Log Time] フィールドに、センサーでログに記録する期間を入力します。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] フィールドに、ログに記録する最大バイト数を入力します。

ヒント　選択を破棄して [Advanced] ダイアログボックスを閉じるには、[Cancel] をクリックします。

ステップ 6　変更を適用し、変更後の設定を保存するには、[OK] をクリックし、[Apply] をクリックします。

ヒント　変更を破棄するには、[Reset] をクリックします。