IPS シグニチャの定義

（注） 4.17 以降、Cisco Security Manager は引き続き IPS の機能をサポートしますが、IPS はサポートが終了しているため、IPS の拡張機能はサポートされません。詳細については、EOL 通知を参照してください。

Security Manager を使用すると、専用の IPS アプライアンスやサービス モジュール、または Cisco IOS IPS デバイスに IPS シグニチャを設定できます。Cisco IOS IPS のシグニチャを設定する場合、ルータでは、専用のアプライアンスやサービス モジュールほどは多くのシグニチャを使用できないことに注意してください。

この章は次のトピックで構成されています。

- シグニチャについて （1 ページ）
- シグニチャの設定 （5 ページ）
- シグニチャの設定値の設定 （42 ページ）

シグニチャについて

ネットワークへの侵入とは、ネットワーク リソースへの攻撃、またはネットワーク リソースの不正使用を指しています。Cisco IPS センサーおよび Cisco IOS IPS デバイスでは、シグニチャベースのテクノロジーを使用して、ネットワーク侵入を検出します。シグニチャによって、センサーが検出およびレポートするネットワーク侵入のタイプを指定します。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、シグニチャを使用して、Denial of Service（DoS; サービス拒絶）攻撃などの既知のタイプの攻撃を検出し、定義したアクションに従って対応します。

基本的なレベルでは、シグニチャベースの侵入検知テクノロジーは、ウイルス チェック プログラムにたとえることができます。Cisco IPS には、センサーがネットワーク アクティビティと照合するシグニチャのセットが含まれています。一致が見つかると、センサーは、イベントのロギングや、Security Manager Event Viewer へのアラームの送信などのアクションを実行します。

シグニチャによって false positive が生成される場合もあります。通常のネットワーク アクティビティであっても、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 パラメータを編集（シグニチャを調整）することにより、false positive 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。アラートは他のイベントと同様、Event Viewer などの Web ベースのクライアントによって、イベント ストアから取得される場合があります。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ネ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。

シグニチャの詳細については、以下を参照してください。

- シグネチャの詳細情報の取得　（3 ページ）
- シグニチャ継承について　（4 ページ）

関連項目

- シグニチャの設定 （5 ページ）
- グローバル相関の設定

シグネチャの詳細情報の取得

Cisco Security Intelligence Operations Web サイトで、各シグネチャの詳細情報を表示できます。Web サイトには、ネットワーク セキュリティに関する豊富な情報とベスト プラクティスの推奨事項が含まれており、IntelliShield アラートを設定できます。また、Web サイトでは、ネットワークを保護し、修復に優先順位を付け、組織のリスクを減らすようにシステムを構築するために役立つ高度なセキュリティ項目に関する情報も提供しています。

Security Manager の Signatures ポリシーを編集する際（ [Signatures] ページ （5 ページ）を参照）、シグネチャ ID は IPS シグネチャの Cisco Security Intelligence Operations データベースに直接リンクされています。シグネチャ ID をクリックすると、シグネチャに関する情報（説明、シグネチャが基づく脆弱性、シグネチャが作成された日時など）を含むページが開きます。このデータベースは、http://tools.cisco.com/security/center/search.x?search=Signature でユーザー自身が検索できます（データベースは以前、Cisco Network Security Database または NSDB と呼ばれていました）。

Cisco.com にアクセスできない場合、シグニチャ ID はシグネチャ データベース情報のローカル コピーにリンクされています。Security Manager によって、Cisco.com にアクセスできるかどうかが検出され、適切なリンクが作成されるため、ユーザはプリファレンスを設定する必要がありません。

データベースには、デフォルトの組み込みシグネチャの情報のみが含まれます。カスタム シグネチャ（ユーザが定義したシグネチャ）の情報は表示できません。

Security Manager 4.4 以降、[シグネチャ（Signatures）] ページ（[IPS] > [シグネチャ（Signatures）] > [シグネチャ（Signatures）]）には、各シグネチャの [説明（Explanation）] タブと [関連する脅威（Related Threats）] タブが含まれています。別のウィンドウの [シグネチャ（Signatures）] ページで、これらのタブに詳細情報が表示されます。たとえば、[説明（Explanation）] タブには、説明、シグネチャ ID などが表示されます。[関連する脅威（Related Threats）] タブには、使用している可能性のある他のソフトウェアの脆弱性などが表示されます。

ヒント このウィンドウが表示されていない場合は、[シグネチャ（Signatures）] ページの左下隅にある上矢印ボタンを使用してウィンドウを展開します。このウィンドウを非表示にするには、[シグネチャ（Signatures）] ページの左下隅にある、対応する下矢印を使用してウィンドウを折りたたみます。このウィンドウのサイズは、標準のコントロールで変更できます。

シグニチャ継承について

IPS デバイスのシグニチャ継承は、他のどの Security Manager のルール ベースのポリシーの場合とも異なります。継承とは、最初に一致したルールベースのポリシーの階層リスト（アクセス ルールなど）を適用する、Security Manager の機能のことです。シグニチャ継承での相違点は、IPS デバイスの場合、Security Manager によってシグニチャ単位の継承が可能になる点です。

次の例は、シグニチャ単位の継承がどのように行われるかを示しています。

ステップ 1 ポリシービューで、[IPS] > [シグネチャ（Signatures）] > [シグネチャ（Signatures）] を選択します。

ステップ 2 test1 という名前のポリシーを作成します。

ステップ 3 test2 という名前の別のポリシーを作成します。

ステップ 4 [test 2] を右クリックし、[シグニチャの継承（Inherit Signatures）] を選択します。[Inherit Rules - test 2] ダイアログボックスが表示されます。

ステップ 5 [test1] を選択し、[OK] ボタンをクリックします。

ステップ 6 [test1] を選択し、シグニチャを編集します。編集した内容をメモし、変更内容を保存します。

ステップ 7 [test2] を選択し、編集したシグニチャを選択します。test2 が、test1 に対して行った編集内容を継承していることを確認します。

IPS シグネチャの削除

Security Manager 4.1 から、（導入されている一番低いシグネチャ レベルより古いシグネチャとして定義される）古いシグネチャ バージョンは、データベースの最適化を目的とする定期的な削除操作によって削除されます。

（注） 削除操作の結果、一部の未使用のチューニング コンテキストが削除されることに注意してください。

削除されたシグネチャの一部は、Cisco.com から IPS シグネチャ パッケージを次回ダウンロードする際に復元できる可能性があります。

デフォルトでは、IPS シグネチャの削除はディセーブルになっています。IPS シグネチャの削除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 Cisco Security Manager Daemon Manager を停止します。コマンドプロンプトで、**net stop crmdmgtd** と入力します。

ステップ 2 *NMSROOT* \MDC\ips\etc\sensorupdate.properties ファイルに移動します（*NMSROOT* は Security Manager インストールディレクトリへのパスを表します）。デフォルトは C:\Program Files\CSCOpx です。

ステップ 3 sensorupdate.properties で、purgeUnusedSignautesEntriesinDB:false を purgeUnusedSignautesEntriesinDB:true に変更します。

ステップ 4 Cisco Security Manager Daemon Manager を再起動します。コマンドプロンプトで、**net start crmdmgtd** と入力します。

これで、IPS シグネチャの削除が毎日 0 時に実行されます。

シグニチャの設定

Signatures ポリシーで、Cisco IPS センサーと Cisco IOS IPS デバイスのシグニチャを設定します。

ここでは、次の内容について説明します。

- [Signatures] ページ （5 ページ）
- シグネチャ更新レベルの表示 （18 ページ）
- シグニチャのイネーブル化とディセーブル化 （20 ページ）
- カスタム シグニチャの追加 （26 ページ）
- シグニチャのクローニング （30 ページ）
- カスタム署名の正規表現 （30 ページ）
- シグニチャ パラメータの編集（シグニチャの調整） （31 ページ）
- シグネチャの編集 （20 ページ）

[Signatures] ページ

[Signatures] ページを使用して、IPS シグニチャの追加、編集および削除を実行できる、シグニチャ サマリー テーブルを表示します。このページで、シグニチャをイネーブルまたはディセーブルにして、ポリシー内のアクティブなシグニチャ セットを調整できます。このページを使用して、エンジンからシグニチャをアンロードすることもできます。

IPS デバイス バージョン 7.3(1) 以降では、Security Manager バージョン 4.6 以降で、1 つ以上のシグニチャ ポリシーにシグニチャ脅威プロファイルを適用できます。シグニチャ脅威プロファイルは、カスタマイズされた調整を含む定義済みのシグニチャ テンプレートです。これらの調整により、シグネチャ カバレッジおよび応答アクションが調整され、センサーがさまざまな展開および脅威シナリオでより適切な選択を行えるようになります。この [シグネチャ（Signatures）] ページには、ポリシーに適用されている脅威プロファイルとそのバージョンが表示されます。[変更の手順（To Change）] ボタンをクリックし、ポリシーに適用する脅威プロファイルを選択します。詳細については、 シグネチャ脅威プロファイルの適用 （13 ページ）を参照してください。脅威プロファイルに属しているシグネチャを確認するには、「**Threat**

Profile」というテキストによって [ソース（Source）] 列をフィルタ処理します。テーブルをフィルタ処理する方法については、テーブルのフィルタリングを参照してください。

共有シグネチャポリシーで作成済みの脅威プロファイルが 1 つ以上含まれていない特定のシグネチャパッケージをダウンロードすると、Security Manager では、共有シグニチャのポリシービューに「現在適用されている脅威プロファイルは、このシグネチャバージョンには適用されません（Currently applied threat profile is not applicable to this signature version）」という警告メッセージが表示されます。同様に、Security Manager のデバイスビューでは、サポートされていないデバイスに共有シグネチャポリシーを適用しようとすると、同じ警告メッセージが表示されます。

脅威プロファイルの更新は個別に実行できないため、脅威プロファイルのバージョンを更新する場合は、デバイスの現在のシグネチャバージョンを更新する必要があります。脅威プロファイルのバージョンを更新すると、脅威プロファイルに関連付けられたシグネチャが変更されますが、ユーザーがすでに実行したユーザー定義シグネチャの調整は保持されることに注意してください。

（注） 脅威プロファイルは、IOS-IPS ではサポートされていません。

ヒント

- 有効になっているシグネチャと無効になっているシグネチャは、特定のシグネチャの [有効（Enabled）] チェックボックスによって示されます。Security Manager の以前のリリースでは、無効になっている署名は、テーブルの行を覆うハッシュマークによって示されていました。設定を展開すると、ディセーブルなシグネチャはデバイスから削除されます。詳細については、シグニチャのイネーブル化とディセーブル化 （20 ページ）を参照してください。
- 多くのカラムでは、カラムを右クリックして直接プロパティを編集できます。編集した内容は、選択したすべての行に適用されます。複数の行を選択した場合、選択できるオプションは選択したすべての行に有効なものに限られます。右クリックメニューの内容は、右クリックしたセルに基づいて異なります。使用可能なコマンドの詳細については、シグネチャのショートカット メニュー （15 ページ）を参照してください。
- 列を表示または非表示にするには、シグネチャサマリーテーブルのテーブル見出し行を右クリックし、[列の表示（Show Columns）] をクリックします。デフォルトでは、すべての列が表示されます。

（注） Security Manager のバージョン 4.5 以降には、シグネチャごとに [メモ（Notes）] 列があります。この機能によりメモを追加でき、後で特定のシグネチャに戻って、自分や他のユーザーがシグネチャやイベントに追加した内容を確認できます。この機能は、ネットワーク管理者が、ノイズの多いシグネチャや特に注意が必要なシグネチャを監視するために役立ちます。ただし、Security Manager データベースを復元すると、デフォルトでは [メモ（Notes）] 列が表示されない場合があります。[メモ（Notes）] 列を表示するには、シグネチャサマリーテーブルでテーブル見出し行を右クリックし、[列の表示（Show Columns）] をクリックして、最後に [メモ（Notes）] をクリックします。Security Manager のインストール時にデータベースをバックアップして復元すると、この状況が発生する場合があります。ただし、この状況は、インラインアップグレード時には発生しません。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから **[IPS] > [シグネチャ（Signatures）] > [シグネチャ（Signatures）]** を選択します。
- （ポリシービュー、IPS アプライアンスおよびサービスモジュール）**[IPS] > [シグネチャ（Signatures）] > [シグネチャ（Signatures）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。
- （ポリシービュー、Cisco IOS IPS デバイス）**[IPS（ルータ）（IPS (Router)）] > [シグネチャ（Signatures）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。

関連項目

- テーブルのフィルタリング
- テーブル カラムおよびカラム見出しの機能
- シグニチャ継承について （4 ページ）
- シグニチャのイネーブル化とディセーブル化 （20 ページ）
- シグニチャのクローニング （30 ページ）
- イベント アクション フィルタの設定
- イベント アクション ルールの設定

フィールド リファレンス

表 *1 : Signature Policy*

要素	説明
ID	シグネチャ 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。ID 番号をクリックすると、 シグネチャの詳細情報の取得 （3 ページ）で説明したように、Web ブラウザでシグネチャの詳細情報が表示されたページが開きます。
Sub	サブシグネチャ 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。
名前	証明書に割り当てられる名前を示します。
[有効（Enabled）]	このポリシーでシグネチャが有効か無効かを示すチェックボックス。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。
重大度	シグニチャによってレポートされる重大度レベル（[High]、[Medium]、[Low]、または [Informational]）を示します。
Fidelity	ターゲットに関する具体的な情報がない場合に、このシグニチャをどの程度忠実に実行するかに関連付ける重みを示します。

要素	説明
注記	

要素	説明
	メモを追加して、後で特定のシグネチャに戻って、自分や他のユーザーがシグネチャやイベントに追加した内容を確認できるようにします。この機能は、ネットワーク管理者が、ノイズの多いシグネチャや特に注意が必要なシグネチャを監視するために役立ちます。 デバイスへの展開時には、メモはデバイスに保存されません。ここで説明する [メモ（Notes）] は、Security Manager の GUI のみの機能であり、Security Manager の IPS ポリシーの一部ではないため、デバイスへの展開時には無視されます。 [メモ（Notes）] は IPS ポリシーの一部ではないため、共有署名ポリシーの割り当てまたは継承は [メモ（Notes）] には影響しません。 シグネチャを右クリックしてメモを追加しても、アクティビティ/チケットの作成は求められません。ただし、シグネチャをダブルクリックするか [編集（Edit）] ボタンをクリックしてメモを追加すると、シグネチャポリシーの変更をともなうため、アクティビティ/チケットの作成を求められます。 シグネチャ更新操作の一部としてシグネチャにメモを追加することはできません。ただし、他のパラメータは編集できます。 メモは、グローバル検索機能では検索できません。 [メモ（Notes）] 列には、メモのテキストは表示されません。アイコンのみが表示されます。メモのテキストを表示するには、アイコンをダブルクリックする必要があります。 [ファイルにエクスポート（Export to File）] ボタンを使用すると、result.csv ファイルの [メモ（Notes）] 列には「Y」または「N」のみが表示されます。これは、それらのシグネチャにメモが付けられているかどうかを示します。実際のテキストはエクスポートされません。 メモは編集できません。追加されたすべてのメモは、新しいメモエントリとして既存のメモに付加されます。もちろん、メモを削除して、更新されたメモを新たに追加することもできます。 メモを追加するには、特定のシグネチャの行を右クリックし、[メモの追加（Add Note）] をクリックします。メモを追加したら、[保存（Save）] をクリックして [メモ（Notes）] ダイアログボックスを閉じます。[メモ（Notes）] ダイアログボックスを閉じると、特定のシグネチャの行に「メモ」アイコンが表示されます。 複数の署名にメモを追加するには、目的のシグネチャを選択し（Windows では Shift キーまたは Ctrl キーを押しながらクリック）、1 つの特定シグネチャの場合と同じ手順を続行します。 メモには、ローカルメモと共有メモがあります。ローカルポリシーのみを持つデバイスにメモを追加する場合は、ローカルメモのみを追加、編集、および削除できます。共有ポリシーが割り当てられたデバイスにメモを追加する場合は、ローカルメモと共有メモ（[このメモを共有（Share this Note）] オプショ

要素	説明
	ンをオンにする）の両方を追加、編集、および削除できます。ただし、共有ポリシーが割り当てられている場合でも、その特定のデバイスのみにメモを追加（つまり、メモのローカルオーバーライド）できます。 **ヒント** デバイスに共有ポリシーが割り当てられている場合、共有ポリシーに影響を与えずに特定のシグネチャについてそのデバイスにのみメモを追加するには、デバイスビューで [このメモを共有（Share this Note）] オプションをオンにせずにメモを追加する必要があります。 **ヒント** [シグネチャの編集（Edit Signature）] ダイアログボックスでメモを操作することもできます。この表で後述する「[編集（Edit）] ボタン」を参照してください。
[基本 RR（Base RR）]	シグニチャの基本リスク レーティング値を示します。
アクション（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。
ソース	シグニチャの設定を上書きする、継承階層内の一番低いポリシーを示します。値は次のとおりです。 • [Default]：シグネチャはデフォルトのシスコ定義の設定を使用します。 • [Local]：シグネチャは選択したデバイス向けに特別に定義されています（デバイス ビューのみ）。 • [Policy name]：継承階層内の一番低い共有ポリシーを示します。ポリシー名はポリシー ビューで表示するか、またはデバイスに共有シグネチャ ポリシーを割り当てる場合はデバイス ビューで表示できます。

要素	説明
Retired	シグネチャが廃棄される条件（条件が存在する場合）。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。 **ワンポイントアドバイス**）[廃棄（Retired）] フィールドを使用して、IOS-IPS デバイス上のディセーブルにしたシグニチャをアンロードし、そのデバイスのメモリ使用量を最適な量にします。 シグニチャ ポリシーのエンジン レベルが E-4 未満の場合、[Retired] フィールドの値は [false] と [true] のどちらかになります。[false] の場合、シグニチャは廃棄されません。[true] の場合、シグニチャは廃棄されます。 シグニチャ ポリシーのエンジン レベルが E-4 である場合、[Retired] フィールドの値は次の 4 つのいずれかになります。 • [偽（false）]：シグネチャは廃棄されません。 • [低メモリ廃棄（low-mem-retired）]：シグネチャは、メモリ容量が少ないプラットフォームで廃棄されます。メモリ容量が少ないデバイスとは、メモリが 2 GB 以下のものを指します。 • [中メモリ廃棄（med-mem-retired）]：シグニチャは、メモリ容量が中程度のプラットフォームで廃棄されます。メモリ容量が中程度のデバイスとは、メモリが 2 GB より大きく 4 GB 以下のものを指します（メモリが 4 GB を超えるデバイスは、メモリ容量が多いプラットフォームと見なされます）。 • [真（true）]：シグネチャはすべてのプラットフォームで廃棄されます。 [low-mem-retired] または [med-mem-retired] を選択すると、Security Manager はデバイスに対して、それらの条件を持ったシグネチャを設定します。デバイスでシグネチャが実際に廃棄されるかどうかはデバイスに取り付けられているメモリの容量によって異なります。デバイスによって実際に廃棄されるシグネチャが判断されます。 **ヒント**　ここで使用されているエンジンレベルという用語は、上の行で使用されているエンジンという用語とは異なります。
エンジン	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。
[View Update Level] ボタン （デバイス ビューだけ）	このデバイスのシグネチャ更新レベルを表示するには、このボタンをクリックします。詳細については、シグネチャ更新レベルの表示 （18 ページ）を参照してください。

要素	説明
[Export to File] ボタン	このボタンをクリックして、現在のデバイスのシグニチャ サマリーを Comma Separated Value（CSV; カンマ区切り値）ファイルにエクスポートします。Security Manager サーバ上のフォルダを選択し、ファイル名を指定するように要求されます。
[追加（Add）] ボタン	カスタム シグネチャを追加するには、このボタンをクリックします。詳細は、次のトピックを参照してください。 • カスタム シグニチャの追加 （26 ページ） • [Edit Signature] ダイアログボックス、[Add Custom Signature] ダイアログボックス （22 ページ）
[編集（Edit）] ボタン	選択したシグネチャを編集するには、このボタンをクリックします。一度に編集できるシグニチャは1つです。詳細は、次のトピックを参照してください。 • シグネチャの編集 （20 ページ） • [Edit Signature] ダイアログボックス、[Add Custom Signature] ダイアログボックス （22 ページ）
[削除（Delete）] ボタン	選択したカスタムシグネチャを削除するには、このボタンをクリックします。 シスコ定義のシグネチャは削除できません。シスコ定義のシグネチャを展開しない場合は、シグネチャを廃棄またはディセーブルにできます。

シグネチャ脅威プロファイルの適用

[脅威プロファイルの適用（Apply Threat Profile）] ダイアログボックスを使用して、利用可能なプロファイルからシグネチャ脅威プロファイルを選択し、ポリシーに適用します。脅威プロファイルを適用すると、 [Signatures] ページ （5 ページ）上の [有効化（Enabled）] および [廃止（Retired）] フィールドのみが変更されます。特定の脅威プロファイルをポリシーに適用すると、対応するシグネチャチューニングが [シグネチャ（Signature）] ページの既存のシグネチャとマージされます。脅威プロファイルに属するシグニチャを表示するには、[シグニチャ（Signature）] ページで、テキスト **Threat Profile** が含まれるように [ソース（Source）] 列をフィルタリングします。テーブルをフィルタ処理する方法については、テーブルのフィルタリングを参照してください。

現在シスコが提供している次の脅威プロファイルのいずれかを選択します。

- SCADA：主に産業用制御システムを保護するために Cisco IPS デバイスを使用している場合は、この脅威プロファイルテンプレートを選択します。SCADA 署名テンプレートには、デフォルトセットの署名に加えて、一般的な SCADA プロトコル検出用の特殊な署名と、ほとんどのデバイス制御環境で共通するツールや環境に対応する特定の識別子が含まれています。

- Edge：主にインターネット接続を保護するために Cisco IPS デバイスを使用している場合は、この脅威プロファイルテンプレートを選択します。Edge 署名テンプレートには、デフォルトセットの署名に加えて、デスクトップ オペレーティング システム、Web ブラウザ、Web テクノロジ、および一般的なデスクトップ アプリケーションに対してより広範な保護を提供する追加の署名が含まれています。
- Web_Applications：主に Web サーバーファームを保護するために Cisco IPS デバイスを使用している場合は、この脅威プロファイルテンプレートを選択します。Web_Applications 署名テンプレートには、デフォルトセットの署名に加えて、Web サーバー、Web 開発ツールとフレームワーク、コンテンツ管理システム、ロードバランサ、およびデータベースに幅広い保護を提供する追加の署名が含まれています。
- Data Center：主にデータセンターを保護するために Cisco IPS デバイスを使用している場合は、この脅威プロファイルテンプレートを選択します。Data Center 署名テンプレートには、デフォルトセットの署名に加えて、サーバー オペレーティング システム、Web サーバー、アプリケーションサーバー、データベース、コンテンツ管理システム、メッセージングサーバー、および仮想化システムに対してより広範な保護を提供する追加の署名が含まれています。

（注） ローカル署名（選択したデバイスに対して定義され、ソースポリシーがローカルである署名）でユーザーが実行したシグネチャチューニングは、脅威プロファイル上で保持されます。デフォルト署名の場合、脅威プロファイルのチューニングは保持されます。

ナビゲーション パス

- （デバイスビュー）ポリシーセレクタから **[IPS] > [シグネチャ（Signatures）] > [シグネチャ（Signatures）]** を選択します。
- （ポリシービュー、IPS デバイス）**[IPS] > [シグネチャ（Signatures）] > [シグネチャ（Signatures）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。

フィールド リファレンス

表 *2:* 脅威プロファイルの詳細

要素	説明
署名 ID	シグネチャ 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。
Sub Signature ID	サブシグネチャ 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。

要素	説明
[有効（Enabled）]	この脅威プロファイルでシグネチャが有効か無効かを示します。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。
Retired	シグネチャがこの脅威プロファイルで廃止されているか、アクティブであるかを示します。
[競合あり（Has Conflict）]	適用された脅威プロファイルからのチューニングを含むシグネチャに、ユーザーによって実行されたチューニングも含まれているかどうかを示します。ユーザーおよび適用された脅威プロファイルによってチューニングされたシグネチャでは、[競合あり（Has Conflict）] 列に True のフラグが付けられます。適用された脅威プロファイルとユーザーによるシグネチャのチューニングの間に競合がない場合、そのシグネチャの [競合あり（Has Conflict）] 列に False と表示されます。 （注） ローカル署名（選択したデバイスに対して定義され、ソースポリシーがローカルである署名）でユーザーが実行したシグネチャチューニングは、脅威プロファイル上で保持されます。デフォルト署名の場合、脅威プロファイルのチューニングは保持されます。

シグネチャのショートカット メニュー

シグネチャ ポリシーのシグネチャ サマリー テーブル内を右クリックすると、選択したシグネチャに対してさまざまな機能を実行するためのショートカット メニューが表示されます。コマンドには、単一のシグネチャを選択した場合のみに表示されるものもあれば、複数のシグネチャに対して同時に使用でき、変更内容が選択したすべてのシグネチャに適用されるものもあります。シグネチャ ポリシーの詳細については、[Signatures] ページ （5 ページ）を参照してください。

また、使用可能なコマンドは右クリックしたセルによって異なります。コマンドには、どのセルを右クリックしても使用できるものもあれば、単一のセルだけで使用できるものもあります。

ヒント 右クリック コマンドを使用してデフォルト シグネチャのセルの値を変更するときには、シグネチャはデバイス ビューでローカル シグネチャに変換されるか、ポリシー ビューで共有ポリシー固有のシグネチャに変換されます。

次の表に、使用可能なコマンドの説明を示します。

表 *3:* シグネチャのショートカット メニュー

メニュー コマンド	説明
すべてのセルに使用できるコマンド	
行を追加（Add Row）	カスタム シグネチャを追加します。詳細は、次のトピックを参照してください。 • カスタム シグニチャの追加 （26 ページ） • [Edit Signature] ダイアログボックス、[Add Custom Signature] ダイアログボックス （22 ページ）
Edit Row	選択したシグネチャを編集します。一度に編集できるシグニチャは 1 つです。詳細は、次のトピックを参照してください。 • シグネチャの編集 （20 ページ） • [Edit Signature] ダイアログボックス、[Add Custom Signature] ダイアログボックス （22 ページ）
Delete Row	選択したカスタム シグネチャを削除します。 シスコ定義のシグネチャは削除できません。シスコ定義のシグネチャを展開しない場合は、シグネチャを廃棄またはディセーブルにできます。
複製（Clone）	選択したシグネチャと同一のプロパティを持つ新規カスタム シグネチャを作成します。詳細については、 シグニチャのクローニング （30 ページ）を参照してください。
Enable、Disable	シグニチャをイネーブルまたはディセーブルな状態にします。ディセーブルなシグニチャは、網掛けされて表示されます。詳細については、 シグニチャのイネーブル化とディセーブル化 （20 ページ）を参照してください。
Show Events Show MARS Events	イベントビューアまたは Cisco Security MARS アプリケーションへの移動を有効にして、選択したシグニチャによって検出されたリアルタイムのイベントまたは過去のイベントを表示できるようにします。詳細については、IPS シグニチャのイベントの表示およびIPS シグニチャの CS-MARS イベントの表示を参照してください。
[Action] セルのコマンド	
Add to Actions	選択したシグニチャの現在のアクション リストにアクションを追加します。
Delete from Actions	選択したシグニチャの現在のアクション リストからアクションを削除します。

メニュー コマンド	説明
Replace Actions With	選択したシグニチャの現在のアクションセットを、選択した単一のアクションに置き換えます。複数のアクションを選択する場合、サブメニューから [その他（More）] を選択し、次に Ctrl キーを押した状態で目的のアクションをクリックして選択します。
Edit Actions	[Edit Actions] ダイアログボックスが開きます。このダイアログボックスで、シグネチャに対して実行するアクションを選択できます。選択したアクションで、シグニチャの現在のアクションリストを置き換えます。詳細については、[Edit Action]、[Add Action]、[Replace Action] ダイアログボックス （17 ページ）を参照してください。
[Severity] セルのコマンド	
• 高い • 中規模 • 低い • 情報（Informational）	シグネチャの重大度レベルを、選択したレベルに変更します。
[Fidelity] セルのコマンド	
Edit Fidelity	シグニチャの忠実度評価を変更します。忠実度評価は、ターゲットに関する具体的な情報がない場合に、このシグニチャをどの程度忠実に実行するかに関連付ける重みを示します。
[Retired] セルのコマンド	
• 廃止（Retire） • アクティブ化 • Retire on Low Memory • Retire on Medium Memory	シグネチャの廃棄ステータスを、選択したステータスに変更します。廃棄ステータス カテゴリの詳細については、[Edit Signature] ダイアログボックス、[Add Custom Signature] ダイアログボックス （22 ページ）を参照してください。

[Edit Action]、[Add Action]、[Replace Action] ダイアログボックス

シグネチャに定義されているアクションを変更するには、[Edit Action]、[Add Action]、または [Replace Action] ダイアログボックスを使用します。これらのダイアログボックスは、シグネチャのショートカット メニュー （15 ページ）で説明したように、右クリック メニューを使用して [Action] セルを編集するときにのみ使用できます。動作はダイアログボックス名によって異なります。

- [Add Actions]：選択したアクションは、シグネチャですでに定義されているアクションに追加されます。このダイアログボックスを開くには、シグネチャの[アクション（Actions）] セルを右クリックし、[アクションに追加（Add to Actions）] > [さらに追加（More）] を選択します。
- [Replace Actions]：選択したアクションは、シグネチャで定義されているアクションをすべて置き換えます。このダイアログボックスを開くには、シグネチャの [アクション（Actions）] セルを右クリックし、[アクションを置換（Replace Actions With）] > [さらに追加（More）] を選択します。
- [Edit Actions]：選択したアクションは、シグネチャで定義されているアクションをすべて置き換えます。このダイアログボックスを開くには、シグネチャの[アクション（Actions）] セルを右クリックし、[アクションの編集（Edit Actions）] を選択します。

使用可能なアクションの説明については、IPS イベント アクションについてを参照してください。Ctrl キーを押した状態でクリックすることで、複数のアクションを選択できます。

（注） ダイアログボックスを開いたときに表示されるアクションのリストは、状況に応じて変わります。アクションのリストは、[Actions] カラムで 1 つのシグニチャ行だけを右クリックしたか、[Actions] カラムで右クリックする前に複数のシグニチャ行を選択したか、によって変わります。[Actions] カラムで 1 つのシグニチャ行だけを右クリックした場合、アクションのリストは、そのシグニチャのエンジンのリストになります。[Actions] カラムで右クリックする前に複数のシグニチャ行を選択した場合、アクションのリストは、影響を受ける各エンジンで使用できるリストになります（リストには、共通のアクションが含まれます。選択したシグニチャのすべてのアクションが含まれるわけではありません）。

[Edit Fidelity] ダイアログボックス

[Edit Fidelity] ダイアログボックスを使用して、特定のシグニチャの [Fidelity Rating] で変更を行います。忠実度評価、または Signature Fidelity Rating（SFR; シグニチャの忠実度評価）は、ターゲットに関する具体的な情報がない場合に、このシグニチャをどの程度忠実に実行するかに関連付ける重みを示します。この評価には、0 ～ 100 の任意の数字を指定できます。100 は、シグニチャの信頼性が最も高いことを意味します。

ナビゲーション パス

シグネチャ ポリシーで、シグネチャの [Fidelity] セルを右クリックし、[Edit Fidelity] を選択します。シグネチャ ポリシーを開く方法については、[Signatures] ページ （5 ページ）を参照してください。シグネチャのショートカット メニューの詳細については、シグネチャのショートカット メニュー （15 ページ）を参照してください。

シグネチャ更新レベルの表示

デバイス ビューで、Security Manager のデバイスに適用されている現在のシグネチャ更新パッケージを判定し、デバイスに展開されているパッケージと比較できます。

適用された更新レベルと展開された更新レベルとの間の相違は、次の場合に発生する可能性があります。

- デバイスが、Security Manager の外部で更新された。
- Security Manager で更新はポリシーに適用されたが、デバイスにまだパブリッシュされていない。
- Security Manager の初回の展開時に、デバイスがまだ Security Manager の制御下にない。

シグネチャ更新レベルを表示するには、デバイスビューで IPS デバイスに対して、[IPS] > [シグネチャ（Signatures）]>[シグネチャ（Signatures）] ポリシーを選択します。次に、[更新レベルの表示（View Update Level）] ボタンをクリックして [更新レベル（Update Level）] ダイアログボックスを開きます。

次の表に、ダイアログボックスに表示される情報を示します。

表 *4 : [Update Level]* ダイアログボックス

要素	説明
Applied Level	このカラムには、Security Manager でこのデバイスに適用されるパッチ レベルが表示されます。
Deployed Level	このカラムには、選択したデバイスで現在実行されているパッチ レベルが表示されます。
メジャー アップデート	メジャー更新レベルを示します。
マイナー アップデート	マイナー更新レベルを示します。
サービス パック	サービス パック レベルを示します。
パッチ	パッチ レベルを示します。
エンジン	エンジン レベルを示します。
シグニチャ アップデート	シグニチャ更新レベルを示します。 （注） このフィールドは、このページにおいて、IOS IPS デバイスに適用される唯一のフィールドです。その他のフィールドはすべて、IPS デバイス専用です。
[Revert] ボタン	誤って [適用レベル（Applied Level）] を変更した場合は、新しい [適用レベル（Applied Level）] を廃棄できます。[復元（Revert）] をクリックすると、[適用レベル（Applied Level）] が [展開レベル（Deployed Level）] に同期されます。 ヒント 復元が実行される前に、警告ダイアログが表示されます。アクティビティを送信するかどうかを確認する警告ダイアログも表示されます。

シグニチャのイネーブル化とディセーブル化

個別のシグネチャをイネーブルまたはディセーブルにできます。変更は、設定をデバイスに再展開すると有効になります。

シグネチャがディセーブルになっている場合、テーブルでそのルールにハッシュ マークが重なって表示されます。設定を展開すると、ディセーブルなシグネチャはデバイスから削除されます。

シグネチャのディセーブル化は、デバイスで使用するシグネチャの数を減らす場合や、カスタム シグネチャを削除せずにその使用を一時的に停止する場合に役立ちます。あとでディセーブルにしたシグネチャを再びイネーブルにできます。

（注） 廃棄されたシグニチャをイネーブルにできますが、廃棄されたシグニチャはシグニチャ マイクロ エンジンに含まれていないため、トラフィックのスキャンには使用されません。特定のシグニチャに関してネットワーク トラフィックをセンサーでスキャンする場合は、そのシグニチャをイネーブルにし、廃棄はしないでください。AIP-SSC-5 では、廃棄されたシグニチャをイネーブルにできません。

ステップ 1 次のいずれかを実行します。

- （デバイス ビュー）ポリシー セレクタから **[IPS] > [シグネチャ（Signatures）] > [シグネチャ（Signatures）]** を選択します。
- （ポリシー ビュー、IPS アプライアンスおよびサービス モジュール）**[IPS] > [シグネチャ（Signatures）] > [シグネチャ（Signatures）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。
- （ポリシー ビュー、Cisco IOS IPS デバイス）**[IPS（ルータ）（IPS (Router)）] > [シグネチャ（Signatures）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。

[Signature] ページが表示されます（[Signatures] ページ （5 ページ）を参照）。

ステップ 2 イネーブル ステータスを変更するシグネチャを右クリックして、適宜 [イネーブル（Enable）] または [ディセーブル（Disable）] を選択します。

シグネチャの編集

シグネチャを編集して、その動作を変更できます。たとえば、シグネチャが起動するときに実行するアクションや、シグネチャのリスク評価の計算に使用される重大度および忠実度評価を変更できます。

一部のシグニチャには、次に示す特別な要件があります。たとえば、ACL 違反シグニチャを検出するようにセンサーを設定するには、ACL 違反を記録するように 1 つ以上の Cisco IOS ルー

タを最初に設定する必要があります。次に、センサーと通信するようにそれらのルータを設定する必要があります。最後に、これらのルータからsyslogトラフィックを受信するようにセンサーを設定する必要があります。

ヒント　この手順では、シグネチャ全体を編集する方法について説明します。シグネチャ ポリシーの右クリック メニューを使用することで、シグネチャの個別のプロパティを選択して編集することもできます。使用可能なコマンドの詳細については、シグネチャのショートカット メニュー（15 ページ）を参照してください。

関連項目

- シグニチャについて （1 ページ）
- IPS イベント アクションについて
- シグニチャのイネーブル化とディセーブル化 （20 ページ）
- シグニチャのクローニング （30 ページ）
- イベント アクション フィルタの設定
- イベント アクション ルールの設定

ステップ 1　次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[IPS] > [シグネチャ（Signatures）] > [シグネチャ（Signatures）]** を選択します。
- （ポリシービュー、IPSアプライアンスおよびサービスモジュール）**[IPS] > [シグネチャ（Signatures）] > [シグネチャ（Signatures）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。
- （ポリシービュー、Cisco IOS IPS デバイス）**[IPS（ルータ）（IPS (Router)）] > [シグネチャ（Signatures）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。

[Signature] ページが表示されます（[Signatures] ページ （5 ページ）を参照）。

ステップ 2　編集するシグネチャを右クリックし、[行の編集（Edit Row）] を選択します。シグネチャを選択して、シグネチャ テーブルの下にある [Edit Row]（鉛筆）ボタンをクリックすることもできます。[Edit Signature] ダイアログボックスが開きます。

ヒント　テーブルの上にある [Filter] フィールドを使用すると、目的のシグネチャを検索しやすくなります。テーブルのフィルタリングの詳細については、テーブルのフィルタリングを参照してください。

ステップ 3　シグネチャに目的の変更を加えます。各オプションの具体的な詳細については、[Edit Signature] ダイアログボックス、[Add Custom Signature] ダイアログボックス （22 ページ）を参照してください。

シグネチャを編集するときは、次の点を考慮してください。

- デフォルトシグネチャは編集できません。デフォルトシグネチャは、シスコ定義バージョンのシグネチャです。デフォルトシグネチャを編集する前に、デフォルトシグネチャをローカルシグネチャ（選択したデバイスに定義されているシグネチャ）または共有ポリシー固有のシグネチャ（共有ポリシーで定義されているシグネチャ）のいずれかに変換する必要があります。[Edit Signature] ダイアログボックスのフィールドを変更する前に、[Source Policy] フィールドから [Local] または共有ポリシー名を選択する必要があります。
- シグネチャのすべての特性を変更できるわけではありません。たとえば、シグネチャ ID またはサブシグネチャ ID は変更できません。このフィールドは読み取り専用です。
- シグネチャの詳細パラメータを変更する場合は、シグニチャ パラメータの編集（シグニチャの調整）（31 ページ）で説明する手順に従ってください。

ステップ 4 [OK] をクリックして変更を保存します。

[Edit Signature] ダイアログボックス、[Add Custom Signature] ダイアログボックス

[Edit Signature] ダイアログボックスと [Add Custom Signature] ダイアログボックスは基本的には同じです。ほとんどのフィールドは同一ですが、レイアウトが多少異なります。このダイアログボックスは、次のように使用します。

- [Edit Signature] ダイアログボックスを使用して、デフォルト以外のシグネチャの特性を編集します（読み取り専用モードでは、デフォルト シグネチャの特性の表示のみが可能です）。

デフォルトシグネチャは編集できません。シグネチャに変更を加えるには、ダイアログボックスの一番上にある [Source Policy] フィールドで [Default] 以外のシグネチャを選択する必要があります。

- [Add Custom Signature] ダイアログボックスを使用して、カスタム シグニチャを作成します。[Add Custom Signature] ダイアログボックスで、名前を入力してから、ドロップダウンリストから既存のエンジンを選択します。シグニチャ ID とサブシグニチャ ID は、Security Manager によって割り当てられます。残りのパラメータの選択を終了すると、新しいシグニチャは、[Signatures] ページの適切な数値位置に追加され、選択された状態になります。

（注） Security Manager 4.4 以降では、カスタムシグニチャを追加するときに、シグニチャ ID とサブシグニチャ ID を指定できます。既に存在する シグネチャ ID/サブシグニチャ ID の組み合わせを指定すると、エラーメッセージが表示されます。

ナビゲーション パス

[Signatures] ページから、次の作業ができます。

- シグネチャを編集するには、編集するポリシーを右クリックし、[行の編集（Edit Row）] を選択します。

- カスタムシグネチャを追加するには、テーブルの下にある [行の追加（Add Row）]（+）ボタンをクリックするか、任意の行を右クリックし、[行の追加（Add Row）] を選択します。

[Signature] ページを開く方法については、[Signatures] ページ （5 ページ）を参照してください。

関連項目

- [Edit Action]、[Add Action]、[Replace Action] ダイアログボックス （17 ページ）
- [Edit Signature Parameters] ダイアログボックス （33 ページ）
- エンジンのオプション （27 ページ）

フィールド リファレンス

表 5 : [Edit Signature] ダイアログボックス、[Add Custom Signature] ダイアログボックス

要素	説明
Source Policy （[Edit signature] のみ）	シグネチャの編集におけるポリシーは、次のとおりです。 • [Default]：デフォルトのシスコ定義のシグネチャ。このシグネチャは編集できません。シグネチャを編集するには、[Default] 以外のシグネチャを選択する必要があります。 • [Local]：選択したデバイス向けに特別に定義されているローカルシグネチャです。このオプションはポリシー ビューでは使用できません。 • [Policy name]（変数）：共有ポリシーの名前。デバイス ビューでは、デバイスに共有ポリシーを割り当てた場合のみ、ポリシー名を使用できます。ポリシー ビューでは、編集しているポリシー名を指します。ポリシー名を選択して、シグネチャを編集し、編集した内容を共有ポリシーが割り当てられているすべてのデバイスに反映します。
名前 （[Add] のみ）	シグネチャの名前。 いったん作成したシグネチャの名前は変更できません。名前を変更する場合、シグネチャの複製を作成する必要があります。
[SigID] （[Add] のみ）	カスタムシグネチャを追加するときに指定するシグネチャ ID。 値の許容範囲は 60000 ～ 65000 です。
[SubSigID] （[Add] のみ）	カスタムシグネチャを追加するときに指定するサブシグネチャ ID。 値の許容範囲は 0 ～ 255 です。

要素	説明
Inheritance Mandatory （[Edit signature] のみ）	選択すると、このポリシーから継承されるすべてのポリシーで、定義されたシグニチャ設定が使用されるようになります。
[有効（Enabled）]	シグニチャがイネーブルかどうかを示します。
重大度	シグニチャによってレポートされる重大度レベル（[High]、[Medium]、[Low]、または [Informational]）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、このシグニチャをどの程度忠実に実行するかに関連付ける重みを示します。
アクション（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。アクションの一覧については、IPS イベント アクションについてを参照してください。 Ctrl キーを押した状態でクリックすることで、複数のアクションを選択できます。
Base Risk Rating Risk Rating （シグネチャの追加または編集で、フィールドの名前は若干異なります）	シグネチャの基本リスク レーティング値。この値は、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 x 重大度係数 /100）計算されます。この値は読み取り専用です。直接変更できません。値を変更するには、[Severity] フィールドと [Fidelity] フィールドを変更します。 重大度係数は、[Severity] フィールドでの選択内容に応じて、次の値をとります。 • High = 100 • Medium = 75 • Low = 50 • Informational = 25
エンジン （編集時は読み取り専用。カスタム シグネチャの追加時は読み書き可能）	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。エンジンの詳細については、エンジンのオプション （27 ページ）を参照してください。 カスタム シグネチャを追加するときは、適切なエンジンを選択する必要があります。各エンジンに関する詳細情報と使用可能なパラメータについては、ご使用の IPS ソフトウェア リリースに対応したCisco Intrusion Prevention System Device Manager のインストールおよび使用法ガイド [英語] の「Signature Engines」セクションを参照してください。 **ヒント** ここで使用されているエンジンという用語は、下の行で使用されるエンジンレベルという用語とは異なります。

要素	説明
Retired	シグネチャが廃棄される条件（条件が存在する場合）。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。 **ワンポイントアドバイス**：[廃棄（Retired）] フィールドを使用して、IOS-IPS デバイス上のディセーブルにしたシグニチャをアンロードし、そのデバイスのメモリ使用量を最適な量にします。 シグニチャ ポリシーのエンジン レベルが E-4 未満の場合、[Retired] フィールドの値は [false] と [true] のどちらかになります。[false] の場合、シグニチャは廃棄されません。[true] の場合、シグニチャは廃棄されます。 シグニチャ ポリシーのエンジン レベルが E-4 である場合、[Retired] フィールドの値は次の 4 つのいずれかになります。 • [偽（false）]：シグネチャは廃棄されません。 • [低メモリ廃棄（low-mem-retired）]：シグネチャは、メモリ容量が少ないプラットフォームで廃棄されます。メモリ容量が少ないデバイスとは、メモリが 2 MB 以下のものを指します。 • [中メモリ廃棄（med-mem-retired）]：シグニチャは、メモリ容量が中程度のプラットフォームで廃棄されます。メモリ容量が中程度のデバイスとは、メモリが 2 MB より大きく 4 MB 以下のものを指します（メモリが 4 MB を超えるデバイスは、メモリ容量が多いプラットフォームと見なされます）。 • [真（true）]：シグネチャはすべてのプラットフォームで廃棄されます。 [low-mem-retired] または [med-mem-retired] を選択すると、Security Manager はデバイスに対して、それらの条件を持ったシグネチャを設定します。デバイスでシグネチャが実際に廃棄されるかどうかはデバイスに取り付けられているメモリの容量によって異なります。デバイスによって実際に廃棄されるシグネチャが判断されます。 **ヒント**　ここで使用されているエンジンレベルという用語は、上の行で使用されているエンジンという用語とは異なります。
Obsolete （[Edit signature] のみ）	シグニチャが古いかどうかを示します。古いシグニチャは、シグニチャエンジンから削除されます。再度アクティブにすることはできません。

要素	説明
[Restore Defaults] ボタン （カスタム以外のシグネチャのみ。[Edit signature] のみ）	このボタンをクリックして、このシグネチャをシスコ定義のデフォルト値に戻します。
[Edit Parameters] ボタン	このボタンをクリックして、[Edit Signature Parameters] ダイアログボックスを使用し、このシグネチャの詳細パラメータを編集します。詳細は、次のトピックを参照してください。 • [Edit Signature Parameters] ダイアログボックス （33 ページ） • シグニチャ パラメータの編集（シグニチャの調整） （31 ページ）

カスタム シグニチャの追加

組み込みシグネチャで指定されていないトラフィック パターンが必要な場合、独自のカスタム シグネチャを作成してトラフィック パターンを定義できます。

組み込みシグネチャがトラフィック パターンを網羅している場合でも、デフォルト シグネチャを変更せずに、カスタム シグネチャを作成し、詳細シグネチャ パラメータを編集できます。既存のシグネチャと同様のカスタム シグネチャを作成する場合は、 シグニチャのクローニング （30 ページ）で説明するように、シグネチャを複製するのが最も簡単な方法です。

一部の IPS デバイスにカスタムシグニチャを追加する場合、正規表現を使用できます。正規表現を使用する際の適切な構文の重要性について詳しくは、 カスタム署名の正規表現 （30 ページ）を参照してください。

（注） AIP-SSC-5 では、カスタム シグニチャはサポートされていません。

ステップ 1 次のいずれかを実行します。

- （デバイス ビュー）ポリシー セレクタから **[IPS] > [シグネチャ（Signatures）] > [シグネチャ（Signatures）]** を選択します。
- （ポリシー ビュー、IPS アプライアンスおよびサービス モジュール）**[IPS] > [シグネチャ（Signatures）] > [シグネチャ（Signatures）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。
- （ポリシー ビュー、Cisco IOS IPS デバイス）**[IPS（ルータ）（IPS (Router)）] > [シグネチャ（Signatures）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。

[Signature] ページが表示されます（ [Signatures] ページ （5 ページ）を参照）。

ステップ 2 シグネチャテーブルの下にある [行の追加（+）（Add Row (+)）] ボタンをクリックし、[カスタムシグネチャの追加（Add Custom Signature）] ダイアログボックスを開きます。

ステップ 3 必要な設定を行います。各オプションの具体的な詳細については、[Edit Signature] ダイアログボックス、[Add Custom Signature] ダイアログボックス （22 ページ）を参照してください。

シグネチャを作成するときは、次の点を考慮してください。

- いったん定義したシグネチャの名前は変更できません。あとで名前を変更する場合、シグネチャを複製し、複製を作成する際に名前を変更する必要があります。
- シグネチャに適したシグネチャ エンジンを選択します。シグネチャ エンジンの詳細については、 エンジンのオプション （27 ページ）を参照してください。いったんシグネチャを作成すると、エンジンは変更できません。誤ったエンジンを選択した状態で [OK] をクリックしシグネチャを保存した場合、最初からやり直して、完全に新しいシグネチャを作成する必要があります。
- デフォルトでは、イネーブルのシグネチャが作成されます。ただし、[Enabled] チェックボックスの選択を解除して、最初からディセーブルのシグネチャを作成できます。これで、パラメータの編集が終っていない場合に、シグネチャをディセーブルにできます。
- シグニチャ パラメータの編集（シグニチャの調整） （31 ページ）で説明する手順に従って、シグネチャの詳細パラメータを定義します。多くのパラメータがシグネチャ エンジンによって決まるため、パラメータを編集する前に目的のエンジンを選択する必要があります。

パラメータを設定する前にシグネチャを保存できるかどうかは、選択したエンジンによって異なります。シグネチャの定義を保存するには、少なくとも、[パラメータの編集（Edit Parameters）] をクリックして [シグネチャパラメータの編集（Edit Signature Parameters）] ダイアログボックスを開いてから、[シグネチャパラメータの編集（Edit Signature Parameters）] ダイアログボックスで [OK] をクリックする必要があります。ただし、有効なシグネチャを作成するには、パラメータを設定して目的のトラフィック パターンを指定する必要があります。

ステップ 4 [OK] をクリックして変更を保存します。

カスタム シグネチャはテーブルの最後に追加され、60000 から始まるシグネチャ ID のうち、次に使用可能なシグネチャ ID が設定されます。

（注） Security Manager 4.4 以降では、カスタムシグニチャを追加するときに、シグニチャ ID とサブシグニチャ ID を指定できます。既に存在する シグネチャ ID/サブシグニチャ ID の組み合わせを指定すると、エラーメッセージが表示されます。

エンジンのオプション

次のリストに、[Edit Signature Parameters] ダイアログボックスの [Engine] フィールドで指定できるオプションを示します。各エンジンに関する詳細情報と使用可能なパラメータについては、ご使用の IPS ソフトウェアリリースに対応したCisco Intrusion Prevention System Device Manager のインストールおよび使用法ガイド [英語] の「Signature Engines」セクションを参照してください。

- [AIC FTP]：FTP トラフィックを検査し、発行するコマンドを制御できるようにします。
- [AIC HTTP]：HTTP セッションに対してより細かな制御を実行して、HTTP プロトコルの悪用を防ぎます。
- [Atomic ARP]：レイヤ 2 ARP プロトコルを検査します。Atomic ARP エンジンが異なるのは、大半のエンジンはレイヤ 3 IP に基づいているためです。
- [atomic-ip]：IP プロトコル パケット、および関連付けられているレイヤ 4 トランスポート プロトコルを検査します。
- [Atomic IPv6]：不正な形式の IPv6 トラフィックによって引き起こされる IOS 脆弱性を検出します。
- [Flood Host]：ホストに向けられた ICMP フラッドと UDP フラッドを検出します。
- [Flood Net]：ネットワークに向けられた ICMP フラッドと UDP フラッドを検出します。
- Meta：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。
- [multi-string]：1 つのシグニチャに一致する複数のストリングを使用して、レイヤ 4 トランスポート 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。シグニチャを起動するために一致する必要が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 ノーマライザが機能する方法を設定し、IP および TCP ノーマライザに関連するシグニチャ イベントに設定を提供します。RFC 準拠を強制できます。
- [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 サービスおよびペイロードをデコードします。

Service Generic エンジンを使用すると、設定ファイルでシグニチャを更新するだけで、プログラム シグニチャを発行できます。このエンジンには、コンフィギュレーション ファイルで定義されている簡易マシンおよびアセンブリ言語が含まれています。このエンジンは、仮想マシンを介して（アセンブリ言語から導出された）マシン コードを実行します。仮想マシンは、命令を処理し、パケットから重要な情報を引き出して、マシン コードに指定されている比較および演算を実行します。このエンジンは、String エンジンと State エンジンを補足する迅速なシグニチャ応答エンジンとして設計されています。

Service Generic エンジンを使用してカスタム シグニチャを作成することはできません。

（注） 複雑な言語特有の性質上、Service Generic エンジンのシグニチャ パラメータを編集することは推奨しません。シグネチャの重大度とイベント アクションのみを変更してください。

- [Service Generic Advanced]：ネットワーク プロトコルの一般的な分析を行います。

- [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 変数では、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 SMB Advanced]：Microsoft SMB パケットと Microsoft RPC over SMB パケットを処理します。
- [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。
- [Service TNS]：TNS 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 と TCP）、宛先ポート（TCP と 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の、TCP フラグの組み合わせを分析します。シグネチャはフラグ A、B、および C を探します。3 つすべてが検出されると、アラートが発生します。
- Traffic ICMP：TFN2K、LOKI、DDOS などの非標準プロトコルを分析します。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。
- [Traffic Anomaly]：ワームに感染したホストの TCP、UDP、およびその他のトラフィックを分析します。
- [Trojan Bo2k]：非標準プロトコル BO2K からのトラフィックを分析します。このエンジンには、ユーザが設定できるパラメータはありません。
- [Trojan Tfn2k]：非標準プロトコル TFN2K からのトラフィックを分析します。このエンジンには、ユーザが設定できる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分析します。このエンジンには、ユーザが設定できるパラメータはありません。

シグニチャのクローニング

既存のシグネチャと同様のカスタム シグネチャを作成する場合、シグネチャの複製、つまりコピーを作成できます。次に、複製が要件に応じて実行されるように、パラメータを編集できます。

たとえば、シスコ定義のシグネチャの複製を作成し、ニーズに合わせてカスタマイズできます。シスコのシグネチャをローカル シグネチャまたは共有ポリシー シグネチャに変換して直接パラメータを編集するよりも、実行しやすい場合があります。

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 次のいずれかを実行します。

- （デバイス ビュー）ポリシー セレクタから **[IPS] > [シグネチャ（Signatures）] > [シグネチャ（Signatures）]** を選択します。
- （ポリシー ビュー、IPS アプライアンスおよびサービス モジュール）**[IPS] > [シグネチャ（Signatures）] > [シグネチャ（Signatures）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。
- （ポリシー ビュー、Cisco IOS IPS デバイス）**[IPS（ルータ）（IPS (Router)）] > [シグネチャ（Signatures）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。

[Signature] ページが表示されます（[Signatures] ページ （5 ページ）を参照）。

ステップ 2 複製するシグネチャを右クリックし、[複製（Clone）] を選択します。

Security Manager によるコピーの作成には、時間がかかることがあります。一部の属性は読み取り専用でコピーできない旨の警告が表示される場合があります。警告が表示されたら、[OK] をクリックします。次に、[Add Custom Signature] ダイアログボックスが表示されます。

ステップ 3 カスタム シグニチャの追加 （26 ページ）の説明に従って、複製したシグネチャのプロパティを編集します。

ステップ 4 [OK] をクリック複製したシグニチャは、[Signatures] ページのサマリー テーブルに最後のシグネチャとして表示されます。

複製したシグニチャは、デフォルトでイネーブルおよびアクティブになります。

カスタム署名の正規表現

一部の IPS デバイスにカスタム署名を追加する際、正規表現を使用できます。

IPS デバイスのタイプやカスタム署名の特定の特性に関係なく、正規表現のシンタックスが正しくないと、カスタム署名の追加後にデバイスの展開が失敗します。

正規表現には、多くの制御文字や正規表現パターン自体を記述するための正規表現表記を含む場合があります。正規表現自体でそれらをリテラル文字として使用する場合は、「\」エスケープ文字でエスケープする必要があります。一方、それらを本来の意味で使用する場合は、適切な正規表現シンタックスに準拠するよう注意する必要があります。

展開の失敗の原因となる正規表現の例：!@#$%^&*()_+{}|:"<>?

正常に展開される正規表現の例：!@#$%\^&*\(\)_+\{\}|:\"<>\?

この例では、カスタム 署名での正規表現の使用について説明します。

ステップ 1 Cisco ASA 5500 シリーズ IPS セキュリティ サービス プロセッサ（5525-X など）を追加します。

ステップ 2 string-XL エンジン（string-xl-tcp など）を使用して、カスタム署名を IPS デバイスに追加します。

ステップ 3 [パラメータの編集（Edit Parameter）] をクリックして、カスタム署名の正規表現を作成します。

ステップ 4 IPS デバイスを展開します。

ステップ 5 正規表現で使用されたシンタックスが正しくないと展開は失敗しますが、正しいシンタックスを使用すると展開は成功します。

シグニチャ パラメータの編集（シグニチャの調整）

イベント アクション フィルタおよびオーバーライド ポリシーを使用するか、またはシグネチャに関連したアクションを変更して、ニーズに合うようにシグネチャの動作を変更できない場合、シグネチャ パラメータの微調整が必要になる場合があります。ただし、これらのパラメータは複雑で、パケットの特性に対する深い理解がしばしば必要になる場合があるため、パラメータの編集は最後のオプションとして検討してください。

パラメータを編集する理由は、false positive と false negative を減らすためです。

- false positive は、ウイルススキャンなどの正当なネットワーク アクティビティが攻撃として解釈およびレポートされた場合に発生します。これは、攻撃が行われる前に、攻撃を識別するために指定されている基準をネットワーク アクティビティが満たした場合に発生します。センサーの設定を調整することにより、false positive の数を減らすことができます。
- false negative は、攻撃が検出されなかった場合に発生します。センサーの設定を調整することにより、false negative の数を減らすことができます。

ヒント デフォルト シグネチャのパラメータは編集できません。デフォルト シグネチャのパラメータを編集する前に、シグネチャをローカル シグネチャまたは共有ポリシー シグネチャに変換する必要があります。正規表現の編集など、シグネチャを複製し、カスタム シグネチャに変換する必要がある場合があります。

この手順では、シグニチャ パラメータを編集してシグニチャを調整する方法について説明します。

関連項目

- シグネチャの編集 （20 ページ）
- シグニチャについて （1 ページ）
- イベント アクション フィルタの設定
- イベント アクション オーバーライドの設定

ステップ 1 次のいずれかを実行します。

- （デバイス ビュー）ポリシー セレクタから **[IPS] > [シグネチャ（Signatures）] > [シグネチャ（Signatures）]** を選択します。
- （ポリシー ビュー、IPS アプライアンスおよびサービス モジュール）**[IPS] > [シグネチャ（Signatures）] > [シグネチャ（Signatures）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。
- （ポリシー ビュー、Cisco IOS IPS デバイス）**[IPS（ルータ）（IPS (Router)）] > [シグネチャ（Signatures）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。

[Signature] ページが表示されます（ [Signatures] ページ （5 ページ）を参照）。

ステップ 2 パラメータを編集するシグネチャを右クリックし、[行の編集（Edit Row）] を選択します。[Edit Signature] ダイアログボックスが表示されます（ [Edit Signature] ダイアログボックス、[Add Custom Signature] ダイアログボックス （22 ページ）を参照）。

ステップ 3 [Source Policy] フィールドに [Default] が表示されている場合、パラメータを編集できるようにするには、[Source Policy] を [Local] または共有ポリシーの名前に変更する必要があります。[Local] オプションはデバイス ビューのみで使用可能です。このオプションでは、変更内容を編集中のデバイスに適用し、その他のデバイスには適用しません。共有ポリシーの名前を選択した場合、変更内容はポリシーが割り当てられているすべてのデバイスに適用されます。

ステップ 4 [パラメータの編集（Edit Parameters）] をクリックします。[Edit Signature Parameters] ダイアログボックスが表示されます。

[Edit Signature Parameters] ダイアログボックスは、フォルダ ツリー構造を保持しています。左側のツリーにはパラメータ名が表示され、右側にはパラメータの値が表示されます。

変更できる値には、名前の部分に小さなボックスがあります。これはチェックボックスです。チェックボックスが空の場合、パラメータのデフォルト値が使用されていることを示します。チェックボックスをオンにして、パラメータを設定します。値のフィールドをクリックして、パラメータを変更します。緑色のチェックは、ユーザが定義した値が使用されていることを示します。緑色のチェックをクリックして、値をデフォルトに戻します。（フィールドを編集すると、通常ボックスにチェック マークが追加されます）。

パラメータを変更するには、右側の対象フィールドをクリックします。パラメータをクリックした場合の動作は、パラメータ タイプによって異なります。

- 読み取り専用のパラメータ：多くのパラメータは読み取り専用で変更できません（シグネチャ ID など）。これらのパラメータをクリックしても通常無効になります。ただし、パラメータ リストでは、ダイアログボックスが開きます（[Obsoletes] リストなど）。
- テキストまたは数値のパラメータ：英数字または数字の値を入力する必要があるパラメータをクリックすると、フィールドは編集ボックスになります。目的の値を入力し、Enter キーを押すか、または編集ボックスの外側をクリックします。
- 事前に定義された値のパラメータ：多くのパラメータには、数個の選択できる値があります（[Yes]/[No] など）。これらのパラメータをクリックすると、ドロップダウン リストがアクティブになります。目的のオプションを選択し、フィールドの外側をクリックします。
- リストのパラメータ：項目のリストを保持しているパラメータもあります。これらのパラメータでは、パラメータ値に [Set] または [List] などの単語と鉛筆アイコンが表示されます。フィールド内をクリックすると、ダイアログボックスが開き、項目に関連するリストを設定できます。例としては、Meta エンジン コンポーネントのリストがあります。詳細については、Meta エンジン シグネチャのコンポーネント リストの編集 （40 ページ）を参照してください。
- 変数パラメータ：ポリシー オブジェクトを選択して、パラメータの内容を指定できるパラメータもあります。たとえば、一部のシグネチャ エンジンでは、ポート リスト オブジェクトを選択して、ポートを指定できます。これらのパラメータをクリックすると、[Select] ボタンのついた編集ボックスが表示されます。編集ボックスにポリシーオブジェクトの名前を含む項目を直接入力するか、[選択（Select）] をクリックしてリストからポリシーオブジェクトを選択するか、新しいオブジェクトを作成できます。

[Edit Signature Parameters] ダイアログボックスの詳細については、[Edit Signature Parameters] ダイアログボックス （33 ページ）を参照してください。

ステップ 5 必要に応じて設定を変更してから、[OK] をクリックし変更を保存します。[Edit Signature] ダイアログボックスに戻ります。

ステップ 6 [シグネチャの編集（Edit Signature）] ダイアログボックスで、[OK] をクリックしてシグネチャへの変更を保存します。

ヒント 編集内容で望ましい効果が得られなかった場合、または編集を誤った可能性がある場合は、[シグネチャの編集（Edit Signature）] ダイアログボックスで [デフォルトの復元（Restore Defaults）] ボタンをクリックして、変更内容を消去できます。その後、もう一度やり直すことができます。

[Edit Signature Parameters] ダイアログボックス

[Edit Signature Parameters] ダイアログボックスを使用して、特定のシグニチャの組み込みマイクロエンジン パラメータを編集（調整とも呼びます）します。エンジンが異なると、そのパラメータも異なるため、[Edit Signature Parameters] ダイアログボックスの表示は変化します。シグネチャ パラメータの編集の詳細については、シグニチャ パラメータの編集（シグニチャの調整） （31 ページ）を参照してください。

[Edit Signature Parameters] ダイアログボックスは、フォルダ ツリー構造を保持しています。左側のツリーにはパラメータ名が表示され、右側にはパラメータの値が表示されます。

変更できる値には、名前の部分に小さなボックスがあります。これはチェックボックスです。チェックボックスが空の場合、パラメータのデフォルト値が使用されていることを示します。チェックボックスをオンにして、パラメータを設定します。値のフィールドをクリックして、パラメータを変更します。緑色のチェックは、ユーザが定義した値が使用されていることを示します。緑色のチェックをクリックして、値をデフォルトに戻します。（フィールドを編集すると、通常ボックスにチェック マークが追加されます）。

パラメータを変更するには、右側の対象フィールドをクリックします。パラメータをクリックした場合の動作は、パラメータ タイプによって異なります。

- 読み取り専用のパラメータ：多くのパラメータは読み取り専用で変更できません（シグネチャ ID など）。これらのパラメータをクリックしても通常無効になります。ただし、パラメータ リストでは、ダイアログボックスが開きます（[Obsoletes] リストなど）。
- テキストまたは数値のパラメータ：英数字または数字の値を入力する必要があるパラメータをクリックすると、フィールドは編集ボックスになります。目的の値を入力し、Enter キーを押すか、または編集ボックスの外側をクリックします。
- 事前に定義された値のパラメータ：多くのパラメータには、数個の選択できる値があります（[Yes]/[No] など）。これらのパラメータをクリックすると、ドロップダウン リストがアクティブになります。目的のオプションを選択し、フィールドの外側をクリックします。
- リストのパラメータ：項目のリストを保持しているパラメータもあります。これらのパラメータでは、パラメータ値に [Set] または [List] などの単語と鉛筆アイコンが表示されます。フィールド内をクリックすると、ダイアログボックスが開き、項目に関連するリストを設定できます。例としては、Meta エンジン コンポーネントのリストがあります。詳細については、Meta エンジン シグネチャのコンポーネント リストの編集 （40 ページ）を参照してください。
- 変数パラメータ：ポリシーオブジェクトを選択して、パラメータの内容を指定できるパラメータもあります。たとえば、一部のシグネチャ エンジンでは、ポート リスト オブジェクトを選択して、ポートを指定できます。これらのパラメータをクリックすると、[Select] ボタンのついた編集ボックスが表示されます。編集ボックスにポリシーオブジェクトの名前を含む項目を直接入力するか、[選択（Select）] をクリックしてリストからポリシーオブジェクトを選択するか、新しいオブジェクトを作成できます。

ナビゲーション パス

[シグネチャの編集（Edit Signature）] ダイアログボックスまたは [カスタムシグネチャの追加（Add Custom Signature）] ダイアログボックスから、[パラメータの編集（Edit Parameters）] ボタンをクリックします。これらのダイアログボックスを開く方法については、[Edit Signature] ダイアログボックス、[Add Custom Signature] ダイアログボックス （22 ページ）を参照してください。

ヒント　ボタンがアクティブでない場合、最初に [Source Policy] フィールドから [Local] または共有ポリシーの名前を選択するか、シグネチャを複製しカスタムポリシーを作成する必要があります。[Local] オプションはデバイス ビューのみで使用可能です。このオプションでは、変更内容を編集中のデバイスに適用し、その他のデバイスには適用しません。共有ポリシーの名前を選択した場合、変更内容はポリシーが割り当てられているすべてのデバイスに適用されます。

フィールド リファレンス

表 *6 : [Edit Signature Parameters]* ダイアログボックス

要素	説明
Tuning Context （ポリシー ビューだけ）	特定のシグニチャ ポリシーのシグニチャ パラメータが編集された（調整された）方法を一意に示すために、Security Manager が必要とする情報を表示します。[Tuning Context] フィールドは、次の項目が含まれている文字列です。 • [コンテキスト（Context）]：マイクロエンジンを一意に定義するために、Security Manager サーバーによって提供される識別情報。 • [SigLevel]（IPS）または [バージョン（Version）]（IOS IPS）：IPS ポリシーの場合、シグニチャマイクロエンジンの定義が適用されるシグニチャ更新レベルの範囲を示します。IOS IPS の場合、IOS IPS バージョンを示します。 • [エンジン（Engine）]：IPS エンジンの名前。 **ヒント** 例として、[Tuning Context] フィールドには、Context:9、SigLevel:302-449、Engine:atomic-ip の文字ストリングを含めることができます。 [Tuning Context] フィールドには、すべてのシグネチャ ポリシーに対して、それぞれ 1 つ以上のチューニング コンテキストを含めることができます。 • 最も高いシグネチャレベルのチューニングコンテキストには、「Reference context」が先頭に追加されます。 • 「Reference context」が先頭に追加された共有ポリシーを変更する場合、Security Manager から、ポリシーを他の適用可能なコンテキストにコピーするかどうかを尋ねられる場合があります（特定のデバイスが、複数のコンテキストで表示される場合があります）。 • ポリシーを他の適用可能なコンテキストにコピーすることを選択した場合、コピーできないパラメータがある場合はエラー メッセージが表示されます。 **（注）** Security Manager 4.1 から、（導入されている一番低いシグネチャ レベルより古いシグネチャとして定義される）古いシグネチャバージョンは、データベースの最適化を目的とする定期的な削除操作によって削除されます。結果として、一部の未使用のチューニング コンテキストが削除されることに注意してください。

要素	説明
シグネチャ ID	このシグニチャに割り当てられた一意の数値。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。
サブシグニチャ ID	このサブシグニチャに割り当てられた一意の数値。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。
Promiscuous Delta	無差別モードでの動作時におけるアラートの重大度を変更します。値は、アラートの全体的なリスクレーティングから除外されます。インラインモードでの動作時は、[Promiscuous Delta] は無視されます。指定できる値の範囲は、0 ～ 30 です。
Sig Description	シグネチャを他のシグネチャとシグネチャを識別するために役立つシグネチャの説明。 • [Alert Notes]：アラート メッセージに含まれる、シグニチャに関する追加情報。 • [User Comments]：シグニチャに関するコメント。 • [Alarm Traits]：このシグニチャについて文書化する特性。値は 0 ～ 65535 です。デフォルトは 0 です。 • [Release]：シグニチャが最後に更新されたリリース。 • [Signature Creation Date]：シグネチャが作成された日付。 • [Signature Type]：シグネチャのタイプ（[Anomaly]、[Component]、[Exploit]、[Vulnerability] または [Other]）。
エンジン	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。エンジンは、Engines フォルダで使用可能なパラメータを決定します。エンジンの詳細については、エンジンのオプション（27 ページ）を参照してください。 各エンジンに関する詳細情報と使用可能なパラメータについては、ご使用の IPS ソフトウェアリリースに対応した Cisco Intrusion Prevention System Device Manager のインストールおよび使用法ガイド [英語] の「Signature Engines」セクションを参照してください。 **ヒント** 多くのエンジンには、[Fragment Status] パラメータが含まれています。このパラメータによって、パケット フラグメントを検査する必要があるかどうかを指定できます。フラグメントを検査するかしないか、またはシグネチャをすべてのパケット ステータスに適用するかを選択できます。

要素	説明
Event Counter	センサーがイベントをカウントする方法。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。次の値を設定します。 • [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。 • [アラート間隔の指定（Specify Alert Interval）]：イベントカウントをリセットするアラート間の時間を指定するかどうかを示します（[はい（Yes）] または [いいえ（No）]）。[はい（Yes）] を選択した場合は、時間を秒単位で入力します（2 ～ 1000）。
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。シグニチャに対して次のパラメータを指定します。以下に、パラメータの説明を記載します。 • Summary Mode • Summary Interval • Summary Key • Specify Global Summary Threshold

要素	説明
Summary Mode （[Alert Frequency] グループ）	アラートのサマライズのモード。Fire All、Fire Once、Summarize、および Global Summarize という 4 つのモードがあります。サマリー モードは、現在のアラート量に応じて動的に変わります。たとえば、シグニチャを Fire All に設定できますが、一定のしきい値に達するとサマライズが開始されます。選択したサマリーモードによって、[Summary Mode] グループで使用可能な他のパラメータの種類を制御します。 • [Fire All]：すべてのイベントについてアラートを起動します。 • [Fire Once]：1 回だけアラートを起動します。 • [Summarize]：アラートをサマライズします。 • [Global Summarize]：攻撃者や攻撃対象の数に関係なく 1 回だけアラートが起動されるようにアラートをサマライズします。 （注） ASA デバイ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。
Specify Summary Threshold （[Summary Mode] グループ）	[Fire All] を選択すると、デバイスがサマリー モードに動的に変化した場合に使用されるサマリーのしきい値の設定値を設定するかどうかを選択できます。[Yes] を選択した場合、サマリー間隔、サマリー キー、またはグローバルなサマリーのしきい値を設定できます。
Summary Interval （[Summary Mode] グループ）	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 （[Summary Mode] グループ）	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 （[Summary Mode] グループ）	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、イベントのしきい値を指定するかどうかを示します（[はい（Yes）] または [いいえ（No）]）。[はい（Yes）] を選択した場合は、イベントのしきい値を入力します（1 ～ 65535）。デフォルトは 240 です。

要素	説明
ステータス	シグネチャの状態。 [Obsoletes] リストでは、このシグネチャで使用されていないシグネチャが表示されます。鉛筆アイコンをクリックして、リストを開きます。ほとんどの場合、この情報は読み取り専用です。リストを変更できる場合は、パラメータ フィールド内の [Set] をクリックして、リストを開きます。このリストでは、使用されていないシグネチャ ID を追加できます。
Vulnerable OS List	攻撃者がターゲットとしているオペレーティング システムのリスト。
MARS Category	シグニチャが属している、Cisco Security MARS でのカテゴリ。このメタデータを使用して、MARS が学習したイベント カテゴリに関連するシグニチャを処理するために必要なデータを MARS に提供するように生成されたイベントを特徴付けます。
[すべてを展開（Expand All）] ボタン	すべてのカテゴリおよびサブカテゴリを展開します。
[すべて折りたたみ（Collapse All）] ボタン	このカテゴリのすべてのフィールドを折りたたみます。

Meta エンジン シグネチャのコンポーネント リストの編集

[Edit Signature Parameter - Component List] ダイアログボックスを使用して、Meta エンジン シグネチャのコンポーネント リストを編集します。

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。

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。このため、Meta エンジン シグネチャでは、Meta シグネチャの検索対象となるシグネチャを指定する必要があります。このシグネチャのリストは、[Component List] に含まれています。

[Component List] は、シグネチャ パラメータの一部です。パラメータを編集するには、シグニチャ パラメータの編集（シグニチャの調整） （31 ページ）で説明した手順に従ってください。Meta エンジンを使用するシグネチャの [シグニチャパラメータの編集（Edit Signature

Parameters）] ダイアログボックスを開いて、**[エンジン（Engine）] > [コンポーネントリスト（Component List）]** パラメータを確認してください。パラメータ値には、鉛筆アイコンと単語 [List] が含まれています。[リスト（List）] をクリックして、[シグネチャパラメータの編集 - コンポーネントリスト（Edit Signature Parameter - Component List）] ダイアログボックスを開きます。

ダイアログボックスは、非アクティブ リスト（左側）とアクティブ リスト（右側）の 2 つのリストに分けられます。アクティブ リストは、Meta エンジン シグネチャが検索するシグネチャを定義します。

コンポーネント リストを変更するには、次の手順を実行します。

- 新しいコンポーネントの追加：非アクティブリストの左側にある [エントリの追加（Add Entry）]（+）ボタンをクリックします。[Add Signature Parameter -List Entry] ダイアログボックスが開きます。次の値を設定します。
  - [エントリキー（Entry Key）]：コンポーネントの名前。
  - [コンポーネントのシグネチャID（Component Sig ID）]：検索するシグネチャのシグネチャ ID。
  - [コンポーネントのサブシグネチャID（Component SubSig ID）]：サブシグネチャ ID。サブシグネチャが存在しない場合は、0 を入力します。
  - [コンポーネントカウント（Component Count）]：Meta シグネチャがトリガーされるまでにシグネチャが起動する回数。
  - [コンポーネントではない（Is a Not Component）]：このフィールドでは、ネガティブ エントリを作成できます。これにより、起動させるシグネチャと起動させないシグネチャのリストを指定できます。起動させるシグネチャには[いいえ（No）]を選択し、起動させないシグネチャには [はい（Yes）] を選択します。

[シグネチャパラメータの追加 - エントリのリスト（Add Signature Parameter - List Entry）] ダイアログボックスで [OK] をクリックすると、新しいコンポーネントが非アクティブリストに追加されます。新しいコンポーネントを選択し、[>>] ボタンをクリックしてアクティブ リストに移動します。次に、上下の矢印ボタンを使用して、アクティブ コンポーネント リストでのコンポーネントの位置を移動します。3 つめのボタンを使用して、コンポーネントの順番を前回保存した順番にリセットできます。

- 既存のコンポーネントの編集：（いずれかのリストで）コンポーネントを選択して、リストの間にある [エントリの編集（Edit Entry）]（鉛筆）ボタンをクリックします。[Edit Signature Parameter - List Entry] ダイアログボックスが開きます。コンポーネント名を変更できないこと以外は、パラメータは新しいエントリの追加と同様です。
- コンポーネントの削除：非アクティブリストのコンポーネントを選択し、非アクティブリストの左側にある [エントリの削除（Delete Entry）]（ゴミ箱）ボタンをクリックします。アクティブ コンポーネントを削除する場合、最初にアクティブ リストでアクティブ コンポーネントを選択し、[<<] ボタンをクリックして、非アクティブ リストに移動します。

- デフォルトの復元：コンポーネントのデフォルト値を復元する場合、コンポーネントを選択し、[復元（Restore）] をクリックします。

[Obsoletes] ダイアログボックス

[Obsoletes] ダイアログボックスを使用して、特定のシグニチャに関連付けられている古いシグニチャを識別します。ほとんどの場合、この情報は読み取り専用です。場合によっては、読み書き可能になります。たとえば、ローカルシグネチャまたは共有ポリシー固有のシグネチャにおける IOS IPS シグネチャ ポリシーのリストを編集できます。

リストを編集できる場合は、次の作業が実行できます。

- [エントリの追加（+）（Add Entry (+)）] ボタンをクリックして、編集中のシグネチャで使用されていないシグネチャのシグネチャ ID およびサブシグネチャ ID を追加します。
- エントリを選択し、[エントリの削除（ゴミ箱）（Delete Entry (trash can)）] ボタンをクリックして、使用されていないシグネチャのリストからエントリを削除します。

ナビゲーション パス

[Obsoletes] リストは、シグネチャ パラメータの一部です。パラメータを編集するには、シグニチャ パラメータの編集（シグニチャの調整） （31 ページ）で説明した手順に従ってください。[シグネチャパラメータの編集（Edit Signature Parameters）] ダイアログボックスを開いて、[ステータス（Status）]>[廃止（Obsoletes）] パラメータを確認してください。パラメータ値には、鉛筆アイコンと単語 [Set] が含まれています（パラメータが読み取り専用でない場合）。鉛筆アイコンまたは単語をクリックして、[Obsoletes] ダイアログボックスを開きます。

シグニチャの設定値の設定

[Signature Settings] ページを使用して、IPS アプライアンスとサービス モジュール（Cisco IOS IPS デバイスを除く）の設定値を定義します。これらの設定値では、次のポリシーを定義します。

- **アプリケーション ポリシー**：HTTP をイネーブルまたはディセーブルにし、HTTP 要求の最大数を決定および指定し、AIC Web ポートを指定して、FTP をイネーブルまたはディセーブルにします。
- **フラグメント再構築ポリシー**：IP 再構築モードを選択して、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築するように、センサーを設定します。
- **ストリーム再構築ポリシー**：TCP ハンドシェイクを必須とするかどうかを指定し、TCP 再構築モードを選択して、完全なスリー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ーするように、センサーを設定します。
- **IP ロギングポリシー**：許可される最大ログパケット数、IP ログ時間、および許可される最大 IP ログサイズを決定および選択して、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、センサーを設定します。

ヒント　これらのすべての設定には、デフォルト値が存在します。このため、デフォルト以外の値を使用する必要がある場合のみ、このポリシーを設定してください。

Signature Settings ポリシーを設定するには、次のいずれかを実行します。

- （デバイスビュー）ポリシーセレクタから **[IPS] > [シグネチャ（Signatures）] > [設定（Settings）]** を選択します。
- （ポリシービュー）**[IPS] > [シグネチャ（Signatures）] > [設定（Settings）]** を選択し、既存のポリシーを選択するか、または新しいポリシーを作成します。

その後、次の表で説明するオプションを設定できます。

表 *7 : [Signature Settings]* ページ

要素	説明
HTTP の有効化	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、[はい（Yes）] を選択します。
Max HTTP Requests	各接続の未処理の HTTP 要求の最大数。
AIC Web Ports	AIC トラフィックを検索するポート。ポート番号またはポートを定義するポート リスト オブジェクトのカンマ区切りのリストを入力します。[選択（Select）] をクリックしてリストからポートリストオブジェクトを選択するか、新しいオブジェクトを作成できます。
Enable FTP	FTP 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、[はい（Yes）] を選択します。
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築に使用する方式。
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かどうかを示します。

要素	説明
TCP Reassembly Mode	センサーが、次のオプションを使用する TCP セッションの再構築に使用するモード。 • [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します。 （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。 • [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。 • [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。
Max IP Log Packets	記録するパケットの数。
IP Log Time	センサーが記録する期間（1 ～ 60 分）。デフォルトは 30 分です。
Max IP Log Bytes	記録する最大バイト数。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。