Cisco Intrusion Prevention System Manager Express コンフィギュレーション ガイド for IPS 7.1

Text Part Number: OL-19891-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、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。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

CONTENTS

はじめに

発行日：2011 年 3 月 31 日

内容

このドキュメントでは、IPS 7.1 に対応した Intrusion Prevention System Manager Express（IME）をインストール、設定、使用する方法について説明します。本書は Cisco Intrusion Prevention System（IPS; 侵入防御システム）7.1 のマニュアル セットの一部です。略語および関連のある IPS 用語を記載した用語集も含めてあります。このマニュアルは、「関連資料」（P.xxxiv）に記載されている資料と一緒に使用してください。ここでは、次のトピックを扱います。

対象読者

このマニュアルは、次の作業を実行する必要のある管理者を対象にしています。

- IME のインストールおよび設定。
- IPS センサーによるネットワークのセキュリティ保護。
- ネットワークへの侵入の防止とそれに続くアラームのモニタ。

マニュアルの構成

この文書は、次の項で構成されています。

項	タイトル	説明
1	「はじめに」	Cisco IPS とセンサーの使用を開始する方法について説明します。
2	「デバイス リストの設定」	IME でデバイスを追加して設定する方法について説明します。
3	「ダッシュボードの設定」	IME でダッシュボードを追加して設定する方法について説明します。
4	「RSS フィードの設定」	IME で Cisco RSS フィードに接続する方法について説明します。
5	「Startup Wizard の使用」	Startup Wizard を使用して、IME を使ってセンサーを設定する方法について説明します。
6	「センサーのセットアップ」	IME を使用して、センサーの基本的な設定を行う方法について説明します。
7	「インターフェイスの設定」	IME を使用して、センサーのインターフェイスを設定する方法について説明します。
8	「ポリシーの設定」	IME を使用して、センサーのポリシーを設定する方法について説明します。
9	「シグニチャの定義」	IME を使用して、センサーの IPS シグニチャを設定する方法について説明します。
10	「Custom Signature Wizard の使用」	Signature Wizard を使用して、IME を使ってシグニチャを設定する方法について説明します。
11	「イベント アクション規則の設定」	IME を使用して、センサーのイベント アクション規則のポリシーを設定する方法について説明します。
12	「異常検出の設定」	IME を使用して、センサーの AD ポリシーを設定する方法について説明します。
13	「グローバル相関の設定」	IME を使用して、センサーのグローバル相関を設定する方法について説明します。
14	「SSH および証明書の設定」	IME を使用して、センサーの SSH および TLS を設定する方法について説明します。
15	「Attack Response Controller でのブロッキングとレート制限の設定」	IME を使用して、センサーのブロック機能を設定する方法について説明します。
16	「SNMP の設定」	IME を使用して、センサーの SNMP を設定する方法について説明します。
17	「外部製品インターフェイスの設定」	IME を使用して、CSA MC への外部製品インターフェイスを設定する方法について説明します。
18	「センサーの管理」	IME を使用して、センサーを管理する方法について説明します。
19	「センサーのモニタリング」	IME を使用して、センサーのモニタリングを設定する方法について説明します。

項	タイトル	説明
20	「イベント モニタリングの設定」	IME を使用して、センサーのイベント モニタリングを設定する方法について説明します。
21	「レポートの設定と生成」	IME を使用して、レポートを設定および生成する方法について説明します。
22	「センサーへのログイン」	アプライアンスおよびモジュールにログインする方法について説明します。
23	「センサーの初期化」	センサーを初期化する方法について説明します。
24	「Cisco IPS ソフトウェアについて」	Cisco.com で最新の Cisco IPS ソフトウェアを特定してインストールする方法について説明します。
25	「システム イメージのアップグレード、ダウングレード、およびインストール」	センサーのシステム イメージについて、アップグレード、ダウングレード、新規システム イメージのインストールを行う方法について説明します。
A	「システム アーキテクチャの概要」	IPS 6.2 および 7.0 の基盤となるソフトウェア アーキテクチャについて説明します。
B	「シグニチャ エンジンについて」	IPS シグニチャ エンジンを、そのオプションとともに一覧を示します。
C	「トラブルシューティングのヒントと手順」	トラブルシューティング手順およびアドバイスの一覧を示します。
D	「Cisco IPS 7.1 で使用されるオープン ソース ライセンス ファイル」	Cisco IPS が使用するオープン ソース ライセンス ファイルの一覧を示します。
	「Glossary」	IPS 用語と略語の一覧を示します。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	用途
太字フォント	コマンド、キーワード、およびユーザが入力したテキストは、**太字**フォントで示しています。
*イタリック体*フォント	ドキュメント名、新規用語または強調する用語、値を指定するための引数は、*イタリック体*フォントで示しています。
[ ]	角カッコの中の要素は、省略可能です。
{ x | y | z }	必ずいずれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	いずれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
`courier` フォント	システムが表示するターミナル セッションおよび情報は、`courier` フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。

[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

（注） 「*注釈*」です。

ヒント 「*問題解決に役立つ情報*」です。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

ワンポイント アドバイス *時間を節約する*方法です。ここに紹介している方法で作業を行うと、時間を短縮できます。

警告 **「*警告*」の意味です。人為ミスを予防するための注意事項が記述されています。**

関連資料

Cisco IPS 7.1 ドキュメントと入手先に関する詳細な一覧については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/security/ips/7.0/roadmap/19889_01.html

Cisco ASA 5500 シリーズのドキュメントと入手先に関する詳細な一覧については、次の URL を参照してください。

http://www.cisco.com/en/US/docs/security/asa/roadmap/asaroadmap.html

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

CHAPTER 1

はじめに

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

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

この章では、IME およびその使用方法について説明します。内容は次のとおりです。

IME の導入

（注） IME 7.0.3 以降では、IME にアクセスするためのパスワードを作成する必要があります。

IME は、最大 10 のセンサーのレポートおよび設定に加え、システムの健全性、イベント、およびコラボレーション モニタリングを提供するネットワーク管理アプリケーションです。IME は、カスタマイズ可能なダッシュボードを使用してセンサーの健全性をモニタします。また、Cisco Security Center で RSS フィードが統合され、セキュリティ警告として提供されます。グローバル相関データはモニタさ

れ、イベントおよびレポートが表示されます。また、モニタされたイベントは、フィルタリング、グループ化、色付けにより、並べ替えて表示できます。IME では、ping、trace route、DNS ルックアップ、および whois ルックアップなどのツールがサポートされており、選択したイベントに使用できます。また、柔軟なレポート ネットワークが含まれています。さらに、IPS デバイスのモニタリングと設定のシームレスな統合を可能にする IDM コンフィギュレーション コンポーネントを内蔵しています。

IME では、センサーのセットアップ、ポリシーの設定、IPS イベントのモニタリング、およびレポートの作成を行うことができます。IME はシングル アプリケーション モードで動作します。すべてのアプリケーションは 1 つのシステムにインストールされ、そのシステムから全体を管理できます。

勧告

IME には、輸入、輸出、譲渡、使用を規制する米国またはその他の国の法律の対象となる暗号化機能が含まれています。シスコの暗号化製品を譲渡された第三者は、その暗号化技術の輸入、輸出、配布、および使用を許可されたわけではありません。輸入業者、輸出業者、販売業者、およびユーザは、米国および他の国での法律を 順守する責任があります。本製品を使用するにあたっては、関係法令の順守に同意する必要があります。米国および他の国の法律を順守できない場合は、本製品を至急送り返してください。

シスコの暗号化製品を管理する米国の法律の概要については、次の URL で参照できます。

http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

さらに詳しい情報が必要な場合は、export@cisco.com 宛てに電子メールでお問い合わせください。

SensorBase ネットワークへの参加

Cisco IPS には、セキュリティ機能である Cisco グローバル相関が実装されました。この機能では、シスコが長年にわたって蓄積してきた優れたセキュリティ インテリジェンスを駆使しています。Cisco IPS は定期的な間隔で Cisco SensorBase ネットワークから脅威の更新を受信します。これには、インターネット上の既知の脅威（常習的な攻撃者、Botnet ハーベスタ、悪意のあるソフトウェアの大発生、ダーク ネットなど）に関する詳細な情報が含まれています。重要な資産への攻撃の機会をつかまれる前に、IPS はこの情報を使用してフィルタリングによって悪質な攻撃者を除外します。そして、グローバルな脅威データをシステムに組み込み、早期に悪意のあるアクティビティを防止します。

SensorBase ネットワークへの参加に同意した場合は、IPS 宛てに送信されたトラフィックに関する集約された統計情報がシスコによって収集されます。この情報には、Cisco IPS ネットワーク トラフィック プロパティに関する要約データと、このトラフィックがシスコのアプライアンスでどのように処理されたかに関する情報が含まれます。トラフィックのデータ コンテンツおよびその他の企業秘密情報および個人情報の収集は行いません。すべてのデータは集約され、定期的な間隔でセキュリティ保護された HTTP によって Cisco SensorBase ネットワーク サーバに送信されます。シスコで共有されるすべてのデータは匿名とされ、機密情報として扱われます。

表 1-1 に、シスコでのデータの使用法を示します。

表 1-1　シスコによるネットワーク参加データの使用

参加レベル	データのタイプ	目的
Partial	プロトコル属性 (TCP 最大セグメント サイズおよびオプション ストリングなど)	潜在的脅威を追跡し、脅威による影響をシスコが理解するのに役立ちます
	攻撃タイプ (開始されたシグニチャおよびリスク レーティングなど)	現在の攻撃および攻撃の重大度を理解するために使用されます
	接続している IP アドレスおよびポート	攻撃元を特定します
	IPS パフォーマンスの概要 (CPU 使用率、メモリの使用状況、インライン モードと無差別モードなど)	製品の有効性を追跡します
Full	攻撃対象の IP アドレスおよびポート	脅威の動作パターンを検出します

部分的（[Partial]）または完全（[Full]）なネットワーク参加をイネーブルにすると、[Network Participation Disclaimer] が表示されます。参加するには、[Agree] をクリックします。ライセンスをインストールしていない場合は、センサーのライセンスが供与されるまでグローバル相関インスペクションとレピュテーション フィルタリングがディセーブルになることを知らせる警告が表示されます。ライセンスは http://www.cisco.com/go/license で取得できます。

詳細情報

- グローバル相関の詳細については、第 13 章「グローバル相関の設定」を参照してください。
- センサーのライセンシングの詳細については、「ライセンスの設定」（P.18-10）を参照してください。

IME の [Home] ペイン

IME の [Home] では、[Device List] ペインが開きます。ここでは IME のデバイスを設定できます。また、次のような機能もあります。

- ビデオ ヘルプ

  IME を起動すると、すべての機能を説明するビデオが再生されます。他に、手続き型ヘルプを含む 5 種類のビデオがあります。

  ペインごとに関連するビデオ ヘルプが再生されますが、[Help] > [Show Video Help] を選択すると、すべてのビデオ ヘルプにアクセスできます。

（注） IME のビデオ ヘルプの再生には、Adobe Flash Player の Internet Explorer プラグイン バージョン 8 以降が必要です。

- システムとセンサーのクロックの同期を確認。

  右上隅の、[Time] カラムの下にあるアイコンにより、センサーの時刻とローカル システムの時刻が同期しているかどうかが示されます。同期していない場合は、センサーの時刻を修正し、モニタリングとレポートのタイムスタンプが正確に行われるようにする必要があります。

- 1 秒間のイベント数

  [Home] ペインの右下隅に、IME が最近受信した EPS（1 秒間のイベント数）が表示されます。EPS のカウントは 5 秒ごとに更新されます。

IME では、メニュー機能により、さまざまな設定を行うことができます。

- [File] > [Export] : IME データベースから CSV ファイルにイベント データをエクスポートします。
- [File] > [Import] : IME の以前のバージョンまたは IEV 5.*x* からエクスポートされたイベント データをインポートします。
- [View] > [Reset Layout] : IME のペインをデフォルト表示にリセットします
- [Tools] > [Preferences] : イベント データの IME データベースへの保存方法の設定、電子メール通知のイネーブル化を行います。また、ネットワーク スニファ アプリケーションの場所、ビューごとのリアルタイム イベントの最大数、ビューごとの過去のイベントの最大数、イベントのポーリング インターバル、起動時にビデオ ヘルプで説明される機能の選択、などの設定も行います。さらに、キャッシュされた DNS 名の削除もできます。
- [Tools] > [Ping]、[Traceroute]、[Whois]、または [DNS Lookup]

  ping を使用すると、基本的なネットワーク接続を診断できます。ping により、センサーが応答するかどうかを簡単に確認できます。traceroute を使用すると、IP パケットが宛先に到達するまでのルートを表示できます。whois を使用すると、ドメイン名または IP アドレスの所有者を確認できます。DNS ルックアップを使用すると、電話帳を調べるように、ホスト名を IP アドレスに変換できます。

- [Tools] > [Change User Password] : [Change Password] ダイアログボックスで、既存のパスワードを変更できます。
- [Tools] > [IME Console Window] : IME Java コンソールを使用して、IME エラーのトラブルシューティングに役立つ、記録されたエントリをテキスト形式で表示およびコピーできます。仮想マシンのメモリ統計を表示するには、コンソールで `m` と入力します。ガーベージ コレクションを実行するには、コンソールで `g` と入力します。

詳細情報

- センサーの時刻の修正および設定の詳細については、「時刻の設定」（P.6-8）を参照してください。
- データ アーカイブの設定手順については、「データのアーカイブ」（P.1-11）を参照してください。
- 通知の設定手順については、「通知の設定」（P.1-12）を参照してください。
- 汎用オプションの詳細については、「汎用オプションの設定」（P.1-15）を参照してください。

システム要件

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

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

IME には、次の要件があります。

- 最小ハードウェア要件
  - IBM PC 互換の 2 GHz 以上のプロセッサ
  - 1024 × 768 以上の解像度を持つカラー モニタと 16 ビット色に対応したビデオ カード
  - 100 GB のハードディスク ドライブ
  - 2 GB のメモリ
- オペレーティング システム
  - Windows Vista Business および Ultimate（32 ビットのみ）
  - Windows XP Professional（32 ビットのみ）
  - Windows Server 2003
  - Windows 7（32 ビットおよび 64 ビット）
  - Windows Server 2008（32 ビットおよび 64 ビット）

（注）　IME は米国英語版および日本語版の Windows のみをサポートしています。

（注）　IME は Windows OS の仮想化はサポートしていません。

IME は、次の Cisco IPS ハードウェア プラットフォームをサポートしています。

- IPS 4240
- IPS 4255
- IPS 4260
- IPS 4270-20
- AIM IPS
- AIP SSC-5
- AIP SSM-10
- AIP SSM-20
- AIP SSM-40
- IDSM2
- IPS SSP-10
- IPS SSP-20
- IPS SSP-40
- IPS SSP-60
- NME IPS

（注）　IME は IDS-4210、IDS-4215、IDS-4235、IDS-4250、および NM-CIDS もサポートしていますが、これらのプラットフォームがサポートする IPS ソフトウェアは IPS 6.1 以前のものであり、いくつかの IME 機能はサポートされていません。

IME は、次の Cisco IPS のバージョンおよびその機能をサポートしています。

- Cisco IPS 7.1
  - IPv6
  - センサーの設定
  - センサー健全性ダッシュボード
  - イベント ダッシュボード
  - イベントのモニタリング
  - レポート
  - デバイスの最大数 10
  - EPS の最大数 100
- Cisco IPS 7.0
  - IPv6
  - センサーの設定
  - センサー健全性ダッシュボード
  - イベント ダッシュボード
  - イベントのモニタリング
  - レポート
  - デバイスの最大数 10
  - EPS の最大数 100
- Cisco IPS 6.2
  - IPv6
  - センサーの設定
  - センサー健全性ダッシュボード
  - イベント ダッシュボード
  - イベントのモニタリング
  - レポート
  - デバイスの最大数 10
  - EPS の最大数 100
- Cisco IPS 6.1
  - センサーの設定
  - センサー健全性ダッシュボード
  - イベント ダッシュボード
  - イベントのモニタリング
  - レポート

  - デバイスの最大数 10
  - EPS の最大数 100
- Cisco IPS 6.0
  - イベント ダッシュボード
  - イベントのモニタリング
  - レポート
  - デバイスの最大数 10
  - EPS の最大数 100
- Cisco IPS 5.1
  - イベント ダッシュボード
  - イベントのモニタリング
  - レポート
  - デバイスの最大数 10
  - EPS の最大数 100
- Cisco IOS IPS 12.3(14)T7 および 12.4(15)T2
  - イベント ダッシュボード
  - イベントのモニタリング
  - レポート
  - デバイスの最大数 10
  - EPS の最大数 100

IME のデモ モード

IME のデモ モードにより、デバイスに実際に接続せずに、センサーの設定とイベント モニタリング機能を確認することができます。デモ モードは、独立した IME デモ アイコンにより、デスクトップから起動できます。IME のデモ モードには、サンプル イベントと、健全性およびセキュリティのデータが含まれており、イベント モニタリング、センサーの健全性、およびセキュリティ状態のデモンストレーションに使用されます。

IME と IME のデモ モードは同時に実行することができます。ただし、デモ モードは一度に 1 つのインスタンスしか実行できません。デモ モードではデバイスの追加または削除はできません。ダッシュボードは仮想のデータで動作しますが、RSS フィードはインターネット接続に依存しているため、通常どおり動作します。イベント ビューの追加、編集、または削除もできます。ビューには仮想のイベントが表示されます。

IME のインストールまたはアップグレード、および IME へのデータの移行

ここでは、IME のインストールおよびアップグレード方法、および IEV または IME の以前のバージョンからデータを移行する方法について説明します。

Cisco IEV、Cisco IOS IPS、および CSM

Cisco IPS Event Viewer をインストールしている場合は、Install ウィザードで、IME をインストールする前にこれを削除するように求められます。

IME イベント モニタリングは、Cisco IPS 5.x/6.x のシグニチャ形式をサポートする IOS-IPS の各バージョンでもサポートされています。IOS IPS デバイスのモニタリングに IME を使用する場合は、IOS-IPS 12.4(15)T4 を推奨します。IME の新しい機能の中には、ヘルス モニタリングなど、サポートされていないものもあります。

注意　既存の CSM のインストールの上に IME をインストールしないでください。IME をインストールする前に、CSM をアンインストールする必要があります。また、IME の上に CSM をインストールしないでください。

インストール時の注意および警告

（注）　Windows 7 または Windows Server 2008 を使用している場合は、IME をアップグレードする前に、以前のバージョンの IME をアンインストールしてください。それ以外の場合は、現在使用中の IME のバージョンから IME 7.1.1 にアップグレードされます。

IME をインストールまたはアップグレードする場合は、次のことに注意してください。

- IME 7.1.1 は IME のすべてのバージョンに上書きインストールできますが、IEV には上書きインストールできません。警告データベースおよびユーザ設定はすべて保持されます。
- IME 7.1.1 は、IEV の以前のバージョンを検出します。その際、IME 7.1 をインストールする前に古いバージョンを手動で削除するか、別のシステムに IME をインストールするように求められます。インストール プログラムはストップします。
- IME 7.1.1 にアップグレードする前に、IME のすべてのインスタンスが閉じていることを確認してください。
- インストールを開始する前に、ウイルス対策プログラムやホストベースの侵入検知ソフトウェアをすべてディセーブル化し、開いているアプリケーションをすべて閉じます。インストーラにより、コマンド シェル アプリケーションが起動しますが、これによりホストベースの検出ソフトウェアが起動する可能性があり、インストールが失敗する原因になります。
- IME をインストールするには、管理者である必要があります。
- IME 7.1.1 は、MySQL データベースの他のインスタンスと共存できます。システムに MySQL データベースがインストールされている場合は、IME 7.1.1 をインストールする前にこれをアンインストールする必要はありません。

IME のインストールまたはアップグレード

IME をインストールするには、次の手順を実行します。

ステップ 1　Cisco.com の [Download Software] サイトから、IME の実行可能ファイルをコンピュータにダウンロードするか、ブラウザ ウィンドウで IDM を起動し、[Cisco IPS Manager Express] の下の [download] をクリックして IME の実行可能ファイルをダウンロードし、インストールします。IME の実行可能ファイルは、IME-7.1.1.exe などと表示されます。

ステップ 2　実行可能ファイルをダブルクリックすると、[Cisco IPS Manager Express - InstallShield Wizard] が表示されます。Cisco IPS Event Viewer の以前のバージョンがインストールされている場合は、警告が表示されます。その場合はインストールを中止し、IEV の古いバージョンを削除してから IME のインストールを再開します。

ステップ 3　[Next] をクリックして IME のインストールを開始します。

ステップ 4　使用許諾契約に同意して、[Next] をクリックします。

ステップ 5　インストール先のフォルダを選択して [Next] をクリックします。続いて [Install] をクリックして IME をインストールし、[Finish] をクリックしてウィザードを終了します。デスクトップに [Cisco IME] および [Cisco IME Demo] アイコンが表示されます。

（注）　IME を初めて起動すると、パスワードを設定するよう求められます。

IEV データの移行

IME に IEV 5.*x* のイベントを移行するには、インストールを終了し、IEV 5.*x* のエクスポート機能を使用して古いイベントを手動でエクスポートし、ローカル ファイルにデータを移動する必要があります。IME のインストール後に、これらのファイルを新しい IME のシステムにインポートできます。

（注）　IME は、IEV 4.*x* のインポートおよび移行機能はサポートしていません。

IEV 5.*x* からローカル ファイルにイベント データをエクスポートするには、次の手順を実行します。

ステップ 1　IEV 5.*x* で、[File] > [Database Administration] > [Export Database Tables] を選択します。

ステップ 2　ファイル名を入力し、テーブルを選択します。

ステップ 3　[OK] をクリックします。選択したテーブル内のイベントが、指定されたローカル ファイルにエクスポートされます。

IEV イベント データの IME へのインポート

イベント データを IME にインポートするには、次の手順を実行します。

ステップ 1　IME で、[File] > [Import] を選択します。

ステップ 2　IEV 5.*x* からエクスポートされたファイルを選択し、[Open] をクリックします。選択したファイルの内容が IME にインポートされます。

詳細情報

Cisco IPS ソフトウェアを入手する方法については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。

IME パスワードの作成および変更

（注）　IME 7.0.3 以降では、IME にアクセスするためのパスワードを作成する必要があります。

IME を初めて起動すると、[Password Policy] ダイアログボックスが表示されます。IME へのアクセスに使用するパスワードを入力します。確認のためにパスワードを再入力し、[OK] をクリックします。次回以降、IME にログインする場合は、[Enter IME] の [password] フィールドにパスワードを入力し、[OK] をクリックします。IME パスワードを変更するには、[Tools] > [Change User Password] を選択し、既存のパスワードと新しいパスワードを入力し、確認のために新しいパスワードを再入力します。IME をアンインストールして再インストールした場合は、新しいユーザ パスワードを作成する必要があります。パスワードの変更後に IME を再起動する必要はありません。

（注）　IME は、ユーザ ロールまたは複数のセッションをサポートしていないので、ユーザ名を設定する必要はありません。

パスワード要件

IME パスワードの要件として、次のものが挙げられます。

- 8 文字以上、80 文字以内である必要があります。
- 次の中から少なくとも 3 つのクラスの文字を含める必要があります。
  - 小文字
  - 大文字
  - 数字
  - 特殊文字（! @ $ % & *）
- ある文字が連続して 3 回以上繰り返さないようにしてください。
- すべて ASCII 文字を使用してください。

（注）　IME では、パスワードがセキュリティで保護されていることを確認するためにさまざまなチェックが行われます。パスワードが検証をパスしなかった場合は、エラー メッセージが表示されます。

詳細情報

ユーザの追加の詳細については、「認証およびユーザの設定」（P.6-18）を参照してください。

IME パスワードの復旧

IME パスワードを復旧するには、次の手順を実行します。

ステップ 1　IME クライアントを停止します。

ステップ 2　hosts.cfg ファイルを、インストールされたディレクトリから削除します。

例

```
C:¥Documents and Settings¥All Users¥Application Data¥Cisco Systems¥IME¥iev¥hosts.cfg
```

ステップ 3　IME クライアントを再起動します。

ステップ 4　新しいパスワードの作成を求められます。

イベントがデータベースから失われることはありません。hosts.cfg を削除して IME を再起動するまでの新しいイベントについても同様です。しかし、イベントのアカウント ユーザ名およびパスワードは、イベントと設定の両方に使用されます。イベントと設定にそれぞれ異なるユーザ名およびパスワードを設定していた場合は、各デバイスを編集して復元する必要があります。

データのアーカイブ

IME は、イベントの保存に MySQL データベースを使用します。IME の性能を維持するには、データベース テーブルを定期的にアーカイブする必要があります。[Tools] > [Preferences] > [Data Archive] ペインで、アーカイブ設定をカスタマイズできます。各イベント ファイルには、デフォルトで 1,000,000 のイベントが含まれます。IME は、最大 400 のイベント ファイルを保存できます。

サポートされているユーザ ロール

IME でデータ アーカイブを設定するには、管理者である必要があります。

フィールド定義

[Data Archive] ペインでは、次のフィールドが表示されます。

- [Maximum number of events in current event file]:現在のイベント ファイルごとのイベントの最大数を設定します。デフォルトは 1,000,000 です。指定できる範囲は 1000 ～ 1,000,000 です。
- [Maximum number of archived files] : 保持するアーカイブ ファイルの最大数を設定します。デフォルトは 100 です。指定できる範囲は 10 ～ 400 です。
- [Enable time schedule for archiving events] : 特定の時刻にイベント ファイルをアーカイブします。
- 次のタイム スケジュールが選択できます。
  - [Every] : スケジュールを分単位で設定します。デフォルトは 10 分です。
  - [Every] : スケジュールを 1 時間単位で設定します。デフォルトは 1 時間です。
  - [Every day at time] : 1 日の中で、イベント ファイルをアーカイブする時刻を指定します。

データ アーカイブの設定

データ アーカイブを設定するには、次の手順を実行します。

ステップ 1　IME で、[Tools] > [Preferences] > [Data Archive] を選択します。

ステップ 2　現在のイベント ファイル フィールドの [Maximum number of events] に、現在のイベント ファイルに含まれるイベントの最大数を入力します。デフォルトは 1,000,000 です。指定できる範囲は 1000 ～ 1,000,000 です。

ステップ 3　アーカイブ ファイル フィールドの [Maximum number] に、IME で保持されるアーカイブ ファイルの最大数を入力します。デフォルトは 100 です。指定できる範囲は 10 ～ 400 です。

ステップ 4　タイム スケジュールを使用してイベントをアーカイブする場合は、[Enable time schedule for archiving events] チェックボックスをオンにします。

ステップ 5　[Choose the following time schedule] の下に、使用するタイム スケジュールを入力します。分単位、1 時間単位で入力するか、または 1 日の中の特定の時刻を入力します。

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 6　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。

通知の設定

IME が特定の種類のイベントを受信したときに、電子メール通知が送信されるように設定できます。デフォルトでは、電子メール通知はディセーブルになっています。電子メール サーバ、送信者、および受信者が必要になります。

注意　IME の電子メール通知は、電子メール サーバの SSL 認証をサポートしていません。すべての電子メールは、指定された電子メール サーバのポート 25 に送信されます。多くの電子メール プロバイダーでは、認証されていない SMTP 電子メールがポート 25 に送信される場合、スパムメールと疑われ、受け入れられません。そのため、お客様の会社独自の電子メール サーバの使用を推奨します。

サポートされているユーザ ロール

電子メール通知を設定するには、管理者である必要があります。

フィールド定義

[Notification] ペインでは、次のフィールドが表示されます。

- [Enable email/epage notifications]：このチェックボックスをオンにすると、電子メール通知がイネーブルになります。
- [Mail Server (SMTP Host)]：お客様の会社の電子メール サーバを指定します。
- [From Address]：電子メール通知の送信先を指定します。
- [Recipient Address(es)]：電子メール通知を受信するセンサー管理者を指定します。
- [Send notifications for alerts]：確認するアラートのレベルを指定します。また、確認するアラートの種類とリスク レーティングを指定します。
- [Notification Interval]：通知インターバルを分単位で指定します。

  デフォルトは 10 分です。指定できる範囲は 1 ～ 1440 分です。
- [Notification Type]：要約された通知、詳細な通知、またはその両方を送信するように選択します。
- [Maximum number of detailed notifications per interval]：インターバルごとの詳細な通知の数を選択します。
- [Content contains]：詳細な通知に表示される内容を選択します。
  - イベント ID
  - 重大度
  - デバイス
  - アプリケーション名
  - 受信時刻
  - イベント時刻
  - センサーのローカル時刻
  - シグニチャ ID

- シグニチャ名
- シグニチャの詳細
- シグニチャのバージョン
- 攻撃者の IP アドレス
- 攻撃者の所在
- 攻撃対象者の IP アドレス
- 攻撃対象のポート
- 攻撃対象の OS
- 攻撃対象の所在地
- サマリー カウント
- 初期アラート ID
- 要約の種類
- 最終
- インターフェイス
- VLAN
- 仮想センサー
- コンテキスト
- 実行されたアクション
- アラートの詳細
- リスク レーティング
- 脅威レーティング
- レピュテーション
- レピュテーションの詳細
- プロトコル

電子メール通知の設定

IME の電子メール通知を設定するには、次の手順を実行します。

ステップ 1　IME で、[Tools] > [Preferences] > [Notification] を選択します。

ステップ 2　[Enable email/epage notifications] チェックボックスをオンにします。

ステップ 3　[Mail Server (SMTP Host)] フィールドに、電子メール サーバ名を入力します。お客様の会社独自の電子メール サーバを使用してください（例：smtp.mycompany.com）。

ステップ 4　[From Address] フィールドに、電子メール通知の送信先アドレスを入力します。

ステップ 5　[Recipient Address(es)] フィールドに、IME から電子メール通知を受信するユーザのアドレスを入力します。

ステップ 6　通知を受信するアラートの種類を選択します。続いて [Risk Rating Range] フィールドに、リスク レーティングの範囲を入力します。デフォルトは 80 ～ 100 です。これはリスク レーティングの「中」～「高」に相当します。

ステップ 7　[Notification Interval] フィールドに、インターバルを分単位で入力します。通知は、インターバルごとに、各センサーについての要約として送信されます。デフォルトは 1 ～ 100 分です。

ステップ 8　[Notification Type] の下に、受信する通知の種類（要約または詳細）を選択します。

ステップ 9　詳細な通知を選択する場合は、[Maximum number of detailed notifications per interval] の下に、要約ごとの詳細な通知の数、および要約の内容に含まれるフィールドの種類を入力します。

ステップ 10　[Apply] をクリックします。

ステップ 11　電子メール セットアップをテストするには、[Send a Test Mail] をクリックします。電子メール通知が正常にセットアップされた場合は、テスト用電子メールが送信され、受信したことを確認するように求めるダイアログボックスが表示されます。電子メール通知が正常にセットアップされていない場合は、SMTP ホストが不明であるというエラー メッセージが表示されます。

ステップ 12　[OK] をクリックして変更を保存します。

電子メール設定の例

```
Flag this message
high 2004-0 ICMP Echo Request (10.2.2.2)
Wednesday, March 10, 2010 3:13 PM
From abc@def.com Wed Mar 10 23:13:38 2010
Date:                    Wed, 10 Mar 2010 23:13:38 GMT
From:
abc@def.com
To:                         jsmith@cisco.com
To:                         jimsmith2010@yahoo.com
Subject:                                high 2004-0 ICMP Echo Request (10.2.2.2)

Jim
```

電子メール通知の例

次の例は、インターバルごとに各センサーの要約として送信された通知を示します。

```
low 9698-Signature Example "null" src_addr(*)/src_port(*) dest_addr(*)/dest_port(*) Total:
284
high 35786-Signature Example "null" src_addr(*)/src_port(*) dest_addr(*)/dest_port(*)
Total: 276
high 40971-Signature Example "null" src_addr(*)/src_port(*) dest_addr(*)/dest_port(*)
Total: 251
low 8813-Signature Example "null" src_addr(*)/src_port(*) dest_addr(*)/dest_port(*) Total:
565
high 21357-Signature Example "null" src_addr(*)/src_port(*) dest_addr(*)/dest_port(*)
Total: 279
high 41528-Signature Example "null" src_addr(*)/src_port(*) dest_addr(*)/dest_port(*)
Total: 554
```

次の例は、各イベントの詳細な情報を示します。

```
event_id=1186174940758000000
severity=high
device_name=shark
event_time=1186174940758000000
sig_id=21357
sig_name=Signature Example
```

詳細情報

- リスク カテゴリの設定手順については、「リスク カテゴリの設定」（P.11-33）を参照してください。

- リスク レーティングの計算の詳細については、「リスク レーティングの計算」（P.11-3）を参照してください。

汎用オプションの設定

[General] ペインでは、特定の汎用オプションを設定できます。たとえば、ネットワーク スニファ アプリケーション、含まれるリアルタイムまたは過去のイベントの最大数、イベント ポーリング インターバル、起動時に機能説明のビデオを再生するかどうか、キャッシュした DNS 名をクリアするかどうかが指定できます。

Wireshark などのネットワーク スニファ アプリケーションは、キャプチャされたイベントのデータ パケットを表示する際に役立ちます。Wireshark は、フリーの Unix および Windows 用ネットワーク プロトコル アナライザです。これを使用すると、稼動中のネットワークのデータ、またはディスク上のキャプチャ ファイルのデータを検査できます。対話的にキャプチャ データをブラウズし、各パケットの要約情報と詳細情報を表示できます。Wireshark には、機能豊富な表示フィルタ言語や TCP セッションの再構築されたストリームの表示機能など、いくつかの強力な機能があります。詳細については、http://www.wireshark.org を参照してください。

DNS を使用すると、人間が読める形式の名前を、ネットワーク パケットで必要とされる IP アドレスに変換できます。DNS 名は、速度を最適化するためにキャッシュされます。DNS ルックアップの結果はクリアすることができます。

サポートされているユーザ ロール

IME で一般的な設定を行うには、管理者である必要があります。

フィールド定義

[General] ペインには、次のフィールドが表示されます。

- [Network Sniffer Application Location] : ネットワーク スニファ アプリケーションへのパスを指定します。または、[Browse] をクリックしてパスを検索します。
- [Maximum Real-time Events Per View] : リアルタイム イベント ビューに含まれるイベントの最大数を指定します。ビューでは、イベントが最大数に達すると、古いイベントから削除されます。デフォルトは 2000 です。
- [Maximum Historical Events Per View] : 過去のイベント ビューに含まれるイベントの最大数を指定します。デフォルトは 50,000 です。
- [Event Polling Interval] : イベント ポーリングのインターバルごとの秒数を指定します。
- [Show feature presentation video at startup] : デフォルトでは、IME の起動時に毎回 IME の機能を説明するビデオが再生されます。必要ない場合は、ここでディセーブルにします。
- [Delete cached DNS names] : キャッシュされた DNS 名をクリアします。

一般的な設定

IME の一般的な設定を行うには、次の手順を実行します。

ステップ 1　IME で、[Tools] > [Preferences] > [General] を選択します。

ステップ 2　[Network Sniffer Application Location] フィールドに、ネットワーク スニファ アプリケーションの位置を入力します。または、[Browse] をクリックしてパスを検索します。

ステップ 3　[Maximum Real-time Events Per View] フィールドに、リアルタイム イベント ビューに含まれるイベントの最大数を入力します。

ステップ 4　[Maximum Historical Events Per View] フィールドに、過去のイベント ビューに含まれるイベントの最大数を入力します。

ステップ 5　[Event Polling Interval] フィールドに、イベント ポーリングのインターバルごとの秒数を入力します。

ステップ 6　[Show feature presentation video at startup] チェックボックスをオンにして機能説明のビデオをディセーブルにします。デフォルトはイネーブルです。

ステップ 7　キャッシュされた DNS 名を削除するには、[Delete cached DNS names] をクリックします。

CHAPTER 2

デバイス リストの設定

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

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

[Device List] ペインでデバイスを IME に追加し、各デバイスに関する重要な情報を表示できます。この章では、[Device List] ペインとデバイスの追加方法について説明します。内容は次のとおりです。

[Device List] ペイン

IME は、最大 10 台の Cisco IPS デバイスを管理します。[Device List] ペインの上半分には、各デバイスに関連する情報が表示されます。

ペインの右隅にある列ボタンをクリックして、[Choose Columns to Display] ダイアログボックスを表示し、表示する列や非表示にする列をカスタマイズできます。

このペインから、デバイス リストのセンサーを追加、編集、または削除できます。センサーに対するヘルスおよびイベント接続を開始および停止したり、センサーのステータスを表示したりすることができます。ping、trace route、whois、DNS ルックアップなどのツールを使用して、センサーに関する情報を取得することもできます。

[Device List] テーブルの [Add]、[Edit]、[Delete]、[Start]、[Stop]、[Status]、[Tools] ボタンを使用できます。テーブルでセンサーを選択して、右クリック メニューを使用することもできます。

[Device List] ペインの下半分には、IME ヘルス モニタリング センターにより、ペインの上半分で選択したセンサーに関する詳細が表示されます。ここに表示されるデータは、カスタマイズ可能なダッシュボード ガジェットの情報と一致します。

[Device Details] ペインには、選択されたセンサーに関する次の詳細が表示されます。

- [Sensor Health]：センサーおよびネットワーク セキュリティのヘルス情報がグラフ形式で表示されます。

  センサーのヘルスおよびネットワーク セキュリティのグラフの横にある [Details] をクリックすると、センサーよびネットワーク セキュリティのヘルス状態について固有の情報を取得できます。

  センサー ヘルス メトリックを変更する場合は、[Details] > [Configure Sensor Health Metrics] を選択します。[Configuration] > *sensor_name* > [Sensor Management] > [Sensor Health] へ移動し、ヘルス メトリックを再設定できます。

  脅威のしきい値を変更する場合は、[Details] > [Configure Thresholds] を選択します。[Configuration] > *sensor_name* > [Policies] > [IPS Policies] > [Risk Category] へ移動し、脅威のしきい値を設定できます。

  ネットワーク セキュリティ ヘルスをリセットする場合は、[Details] > [Reset Health Status] を選択します。[Configuration] > *sensor_name* > [Sensor Monitoring] > [Properties] > [Reset Network Security Health] へ移動し、ネットワーク セキュリティ ヘルスのステータスと計算をリセットできます。

- [Sensor Information]：ホスト名、IPS バージョン、センサーがインライン バイパスを使用しているかどうか、検知インターフェイスの合計、最後の設定更新、センサーの IP アドレス、デバイス タイプ、合計メモリ、合計データ ストレージが表示されます。

  [Analysis Engine Status] には、分析エンジンが動作しているかどうか、またはその状態を表示できます。

- [CPU, Memory, and & Load]：CPU、メモリ、センサー負荷の使用量、がグラフ形式で表示されます。

  検査負荷グラフの横にある [Details] をクリックすると、検査負荷の判断方法の詳細な説明が表示されます。

- [Licensing]：関連するライセンス、シグニチャ バージョン、およびシグニチャ エンジンのバージョン情報のすべてが表示されます。

- [Interface Status]：インターフェイス名、リンク ステータス、イネーブルかどうか、速度、モード、受信および転送されたパケットが表示されます。

- [Global Correlation Health]：グローバル相関の設定ステータスとネットワーク参加が表示されます。

（注） AIP SSC-5 は、グローバル相関機能をサポートしていません。

詳細情報

- センサーおよびネットワーク セキュリティ ヘルスを設定する手順については、「センサーのヘルスの設定」（P.18-14）を参照してください。
- 脅威のしきい値を変更する手順については、「リスク カテゴリの設定」（P.8-33）を参照してください。
- ネットワーク セキュリティ ヘルスを再設定する手順については、「ネットワーク セキュリティの稼動状態のリセット」（P.19-30）を参照してください。
- グローバル相関の詳細については、第 13 章「グローバル相関の設定」を参照してください。

[Device List] ペインのフィールド定義

[Device List] ペインには次のフィールドがあります。

- [Time]：ローカル システムと追加したセンサーの間に同期の問題がある場合、時刻フィールドにアイコンが表示されます。ローカル システムとセンサーが同期されている場合、フィールドは空白です。

（注）　センサーとローカル システムの間で時刻が同期されていないと、正確なモニタリングとレポートが行われません。

- [Device Name]：センサーに付けた名前が表示されます。
- [IP Address]：センサーの IP アドレスが表示されます。
- [Device Type]：IPS モデル名が表示されます。
- [Event Status]：IME がイベントを受け取るためにセンサーに接続されていることを示します。
- [Sensor Health]：センサーのヘルスが正常か、注意が必要かどうかを示します。
- [Global Correlation Status]：センサーのグローバル相関ステータスを示します。

（注）　AIP SSC-5 は、グローバル相関機能をサポートしていません。

- [Version]：インストールされている Cisco IPS ソフトウェア バージョンが表示されます。
- [License Expiration]：センサーのライセンスの有効期限が切れるまでの日数を示します。
- [Load]：負荷の割合が表示されます。
- [Memory]：メモリの使用率が表示されます。
- [CPU]：CPU の使用率が表示されます。
- [Signature Version]：現在のシグニチャのバージョンが表示されます。

詳細情報

- 時刻とセンサーについては、「時刻の設定」（P.6-8）を参照してください。
- センサー ヘルス メトリックの詳細については、「センサーのヘルスの設定」（P.18-14）を参照してください。
- グローバル相関の詳細については、第 13 章「グローバル相関の設定」を参照してください。
- センサーのライセンシングの詳細については、「ライセンスの設定」（P.18-10）を参照してください。
- 最新の IPS ソフトウェアの入手手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。

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

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

- [Sensor Name]：追加しているセンサーの名前。
- [Sensor IP Address]：追加しているセンサーの IP アドレス。
- [User Name]：このセンサーへのアクセスが許可されたユーザ アカウント名。
- [Password]：このセンサーへのアクセスが許可されたユーザ アカウントのパスワード。
- [Web Server Port]：Web サーバが使用する TCP ポート。HTTP または HTTPS の場合、デフォルトは 443 です。1 ～ 65535 以外の値を入力すると、エラー メッセージが表示されます。
- [Communication Protocol]：Web サーバで TLS と SSL をイネーブルにします。デフォルトは [Use encrypted connection (HTTPS)] です。暗号化された接続を使用することを強くお勧めします。
- [Event Start Time (UTC)]：最新のアラートを取得するか、取得するアラートの開始時刻を設定するかを選択できます。
- [Exclude alerts of the following severity level(s)]：取得する情報からセキュリティ レベルを除外するかどうかを選択できます。デフォルトでは、すべてのセキュリティ レベルが表示されます。

詳細情報

センサー パスワードの回復手順については、「パスワードの回復」（P.18-3）を参照してください。

デバイスの追加、編集、および削除

デバイスを追加、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　[Home] > [Devices] > [Device List] を選択し、[Add] をクリックします。

ステップ 2　[Add Device] ダイアログボックスの必須フィールドに入力します。

a. 追加しているセンサーのセンサー名とセンサーの IP アドレスを入力します。

b. このセンサーにアクセスできるユーザのユーザ名とパスワードを入力します。

c. デフォルトの Web サーバ ポートを変更するには、新しいポート番号を入力します。

d. 通信プロトコルを選択します。

（注）　暗号化された接続を使用することを強くお勧めします。

e. [Latest Alerts] チェックボックスをオンにするか、[Start Date] および [Start Time] フィールドに開始日時を入力して、イベントの開始時刻を選択します。

f. [Exclude alerts of the following severity level(s)] で、除外するレベルのチェックボックスをオンにします。デフォルトでは、すべてのレベルが表示されます。

g. [OK] をクリックして、IME システムにセンサーを追加します。

ステップ 3　[Yes] をクリックして、証明書を受け入れ、センサーとの HTTPS 接続を続行します。

（注）　[No] をクリックすると、証明書が拒否され、IME はセンサーにアクセスできません。

IME は、IME とセンサーの時刻設定をチェックし、正確であることを確認します。時刻が不正確で、センサーと IME システムの間に 5 分を超すずれがある場合、警告メッセージが表示されます。必ず、センサーとシステムを同期させてください。

注意　レポート、履歴イベント、およびトップ ガジェットの精度を維持するために、時刻が正確であることは非常に重要です。時刻の誤差が 5 分を超えている場合、[Device Lists] ペインでそのデバイスの横にアイコンが表示されます。

ステップ 4　デバイスを編集するには、リストでそのデバイスを選択し、[Edit] をクリックし、必要な変更を加えて [OK] をクリックします。

（注）　センサー名は IME データベースのキーなので、[Sensor Name] は変更できません。

ステップ 5　デバイスを削除するには、リストでそのデバイスを選択し、[Delete] をクリックします。[Device List] ペインにそのデバイスが表示されなくなります。

詳細情報

センサーの時刻を修正する方法については、「センサーの時刻の修正」（P.6-13）を参照してください。

デバイス、イベント、ヘルス、およびグローバル相関接続ステータスの開始、停止、および表示

[Start] > [Health Connection] を選択している限り、IME はセンサーに 10 秒おきにクエリーを実行して、ヘルス ステータス情報を取得します。[Start] > [Events Connection] を選択している限り、IME はセンサーからアラートを取得します。[Start] > [Global Correlation Connection] を選択している限り、IME はグローバル相関データを送受信します。

センサーでのイベントのポーリングを停止しなければならない場合があります。たとえば、別のセンサーのイベントを分析しているときに、リアルタイム イベントによる中断を避ける必要がある場合は、特定のセンサーからのイベントのポーリングを停止できます。ポーリングの完了後再開できます。また、10 秒単位の更新なしで、ステータスのスナップショットを表示する場合は、ヘルスとセキュリティのポーリングを停止できます。

イベント、ヘルス、およびグローバル相関の接続ステータスを開始、停止、および表示するには、次の手順を実行します。

ステップ 1　イベント、ヘルス、またはグローバル相関の接続ステータスを開始または停止するセンサーをデバイス リストで選択します。

ステップ 2　[Start] または [Stop] > [Health Connection] または [Events Connection] または [Global Correlation Connection] を選択します。列に [Connected] または [Not Connected] が表示されます。

ステップ 3　IME からセンサーへの接続ステータス、センサー バージョン、および統計情報を表示するには、リストでセンサーを選択し、[Status] をクリックします。[Device Status] ダイアログボックスに次の IPS コンポーネントの統計情報が表示されます。

- 分析エンジン
- 異常検出
- イベント ストア
- 外部製品インターフェイス
- グローバル相関
- Host
- Interface
- ネットワーク アクセス
- 通知
- OS 識別名
- SDEE サーバ
- トランザクション サーバ
- Virtual Sensor
- Web サーバ

ステップ 4　[Device Status] ダイアログボックスの内容を更新するには、[Refresh] をクリックします。

ステップ 5　センサーに関する詳細を表示するには、リストでそのセンサーを選択し、ペインの [Device Details] セクションに表示される情報を確認します。

[Device Details] ペインに表示するヘルス メトリックを変更するには、[Configuration] > *sensor_name* > [Sensor Management] > [Sensor Health] に進みます。[Device Details] ペインに表示するグローバル相関メトリックを変更するには、[Configuration] > *sensor_name* > [Sensor Management] > [Global Correlation] に進みます。

詳細情報

- センサー ヘルス メトリックの詳細については、「センサーのヘルスの設定」（P.18-14）を参照してください。
- グローバル相関の詳細については、第 13 章「グローバル相関の設定」を参照してください。

デバイスでのツールの使用

デバイスにツールを使用するには、次の手順を実行します。

ステップ 1　[Home] > [Devices] を選択します。

ステップ 2　センサーの ping 統計情報を取得するには、デバイス リスト テーブルでそのセンサーを選択し、[Tools] > [ping] をクリックします。そのセンサーの ping 統計情報を含む [Executing command - ping] ダイアログボックスが表示されます。

ステップ 3　IP パケットのルートを調べるには、リストでそのセンサーを選択し、[Tools] > [Traceroute] をクリックします。そのセンサーのルート統計情報を含む [Executing command - ping] ダイアログボックスが表示されます。

ステップ 4　whois 情報を調べるには、リストでそのセンサーを選択し、[Tools] > [WhoIs] をクリックします。そのセンサーの WHOIS 統計情報を含む [Executing command - ping] ダイアログボックスが表示されます。

ステップ 5　DNS 情報を調べるには、リストでそのセンサーを選択し、[Tools] > [DNS] をクリックします。そのセンサーの DNS ルックアップ統計情報を含む [Executing command - ping] ダイアログボックスが表示されます。

CHAPTER 3

ダッシュボードの設定

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

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

この章では、ダッシュボードとその追加および削除の方法について説明します。内容は次のとおりです。

ダッシュボードの概要

デフォルトでは、デフォルト ガジェットで構成されるヘルス ダッシュボードおよびトラフィック ダッシュボードが表示されます。すべてのダッシュボードをカスタマイズできます。ガジェットをリストから選択し、ドラッグ アンド ドロップによってデフォルト ダッシュボードに追加することもできれば、新しいダッシュボードを作成することも可能です。

ダッシュボードを追加するには、[Add Dashboard] をクリックします。ダッシュボードに追加できるガジェットを表示するには、[Add Gadgets] をクリックします。

ダッシュボードの追加および削除

（注）　IPS 6.1 および 6.2 は、グローバル相関機能をサポートしていません。

（注）　AIP SSC-5 は、グローバル相関機能をサポートしていません。

ダッシュボードやガジェットを追加または削除するには、次の手順を実行します。

ステップ 1　[Home] > [Dashboards] を選択し、[Add Dashboard] をクリックします。[Untitled] という名前のタブが表示されます。

ステップ 2　[Untitled] をダブルクリックし、タブ上にダッシュボード名を入力します。

ステップ 3　[Add Gadgets] をクリックします。

ステップ 4　追加するガジェットのアイコンをダッシュボードまでドラッグします。

ステップ 5　ガジェットをカスタマイズするには、右上の [Tool] アイコンをクリックします。設定ダイアログボックスが表示されます。

ステップ 6　ガジェットを折りたたむには、右上の [Double Arrows] アイコンをクリックします。

ステップ 7　ガジェットを削除するには、右上の [X] アイコンをクリックします。

ステップ 8　ダッシュボードを削除するには、タブ内の [X] をクリックします。

注意　[Delete Dashboard] ダイアログボックスが開き、ダッシュボードを削除するかどうかを確認するメッセージが表示されます。ダッシュボードを削除すると、そのダッシュボード内に作成したガジェットがすべて失われます。

IME ガジェット

ここでは、IME ガジェットについて説明します。内容は次のとおりです。

[Sensor Information] ガジェット

[Sensor Information] ガジェットには、次のようなセンサー情報が表示されます。

- [Host Name]：初期化中に設定されます。
- [IPS Version]：現在インストールされている IPS のバージョン。
- [In Bypass]：インターフェイスがバイパス モードで動作しているかどうか。

（注）　IPS SSP は、バイパス モードをサポートしていません。適応型セキュリティ アプライアンスは、適応型セキュリティ アプライアンスの設定と IPS SSP 上で行われているアクティビティのタイプによって、フェールオープン、フェールクローズ、またはフェールオーバーします。

- [Total Sensing Interfaces]：センサー プラットフォーム上のセンシング インターフェイスの数が表示されます。
- [Analysis Engine Status]：分析エンジンの実行ステータスが表示されます。分析エンジンが初期化中または再設定中である場合は、[Processing Transaction] と表示されます。それ以外の場合は、[Running Normally] と表示されます。
  - [Stage]：経過表示バーに分析エンジンのアップデートがどの段階にあるかが表示されます。
  - [Step]：経過表示バーに分析エンジンのアップデート中に実行される追加の処理が表示されます。
  - [Activity]：分析エンジンの動作が完了したことを通知します。

（注）　[Stage]、[Step]、[Activity] の各バーは、分析エンジンのアップデートが完了すると非表示になります。

- [IP Address]：初期化中に設定されます。
- [Device Type]：IPS センサー プラットフォームが表示されます。
- [Total Memory]：メモリの総容量が表示されます。
- [Total Data Storage]：データ ストレージの総容量が表示されます。

[Sensor Information] ガジェットの表示の変更

[Sensor Information] ガジェットのタイトルや表示する情報を取得するセンサーを変更するには、次の手順を実行します。

ステップ 1　ガジェットの右上にある [Tool] アイコンをクリックします。

ステップ 2　[Configure Settings] ウィンドウで次の値を変更できます。

- ガジェットのタイトル

- デバイス

ステップ 3　変更を保存するには、[Apply] をクリックします。変更を破棄する場合は、[Cancel] をクリックします。

詳細情報

- 分析エンジンの詳細については、「分析エンジンの概要」（P.8-2）を参照してください。
- センサーおよびバイパス モードの詳細については、「バイパス モードの設定」（P.7-29）を参照してください。

[Sensor Health] ガジェット

（注）　AIP SSC-5 は、グローバル相関機能をサポートしていません。

[Sensor Health] ガジェットには、センサーのヘルス情報とネットワーク セキュリティ情報が 2 つのカラー メーターとして表示されます。これらのメーターには、特定のメトリックの分析結果に応じて、[Normal]、[Needs Attention]、または [Critical] が表示されます。設定したメトリックの中で全体的なヘルス ステータスが最も高い重大度に設定されます。たとえば、センサーのヘルスを決定する 8 つのメトリックを設定し、そのうちの 7 つが緑で、1 つが赤である場合、全体的なセンサー ヘルスは赤で表示されます。

特定のセンサー ヘルス メトリックを表示するには、センサー ヘルス グラフの近くにある [i] アイコンをクリックします。センサー ヘルス メトリックは黄色と赤のしきい値レベルに従ってグループ化されています。

センサー ヘルス メトリックを変更するには、[Details] > [Configure Sensor Health Metrics] をクリックします。[Configuration] > *sensor_name* > [Sensor Management] > [Sensor Health] へ移動し、ヘルス メトリックを再設定したり、センサー ヘルス パラメータを有効または無効にしたりすることができます。

次のセンサー ヘルス メトリックとそのステータスが表示されます。

- 検査負荷
- 失われたパケット
- シグニチャ アップデート
- 残りのライセンス期間
- イベントの取得
- 失敗したアプリケーション
- バイパス モード状態

（注）　IPS SSP は、バイパス モードをサポートしていません。適応型セキュリティ アプライアンスは、適応型セキュリティ アプライアンスの設定と IPS SSP 上で行われているアクティビティのタイプによって、フェールオープン、フェールクローズ、またはフェールオーバーします。

- ダウンしているアクティブなインターフェイス
- グローバル相関

- ネットワーク参加

特定のネットワーク ヘルス メトリックとそのステータスを表示するには、ネットワーク セキュリティ ヘルス グラフの近くにある [i] アイコンをクリックします。色は、過去 5 分間に収集されたリスク レーティングおよび脅威レーティングを表します。これらのレーティングは、緑、黄、赤の 3 レベルに分類され、赤が最高のリスク レベルを表します。

脅威のしきい値を変更するには、[Details] > [Configure Thresholds] をクリックします。[Configuration] > *sensor_name* > [Policies] > [IPS Policies] > [Risk Category] へ移動し、脅威のしきい値を設定できます。

ネットワーク セキュリティ ヘルスをリセットするには、[Details] > [Reset Health Status] をクリックします。[Configuration] > *sensor_name* > [Sensor Monitoring] > [Properties] > [Reset Network Security Health] へ移動し、ネットワーク セキュリティ ヘルスのステータスと計算をリセットできます。

メーター内を右クリックすると、メニューが表示され、メーターのプロパティの変更、メーターに含まれる情報の印刷、およびセンサー ヘルスやネットワーク ヘルスの詳細の保存を実行できます。

[Sensor Health] ガジェットの表示の変更

[Sensor Health] ガジェットのタイトルや表示する情報を取得するセンサーを変更するには、次の手順を実行します。

ステップ 1　ガジェットの右上にある [Tool] アイコンをクリックします。

ステップ 2　[Configure Settings] ウィンドウで次の値を変更できます。

- ガジェットのタイトル
- デバイス

ステップ 3　変更を保存するには、[Apply] をクリックします。変更を破棄する場合は、[Cancel] をクリックします。

詳細情報

- 脅威のしきい値を変更する手順については、「リスク カテゴリの設定」（P.8-33）を参照してください。
- センサーおよびバイパス モードの詳細については、「バイパス モードの設定」（P.7-29）を参照してください。
- センサーおよびネットワーク セキュリティ ヘルスを設定する手順については、「センサーのヘルスの設定」（P.18-14）を参照してください。
- ネットワーク セキュリティ ヘルスを再設定する手順については、「ネットワーク セキュリティの稼動状態のリセット」（P.19-30）を参照してください。

[Licensing] ガジェット

[Licensing] ガジェットには、次のようなライセンス キーおよび他のソフトウェア アップデートのステータスに関する情報が表示されます。

- [License Status]：ライセンス キーがインストールされているかどうかと、その有効期限が表示されます。
- [Signature Version]：インストールされているシグニチャのバージョンが表示されます。
  - [Released On]：このシグニチャ バージョンがリリースされた日付。

  - [Applied On]：このシグニチャ バージョンが適用された日付。
  - [Auto Update Status]：自動アップデートが新しいバージョンをチェックしたかどうか。
- [Engine version]：インストールされているシグニチャ エンジンのバージョンが表示されます。
  - [Released On]：このシグニチャ エンジンがリリースされた日付。
  - [Applied On]：このシグニチャ エンジンが適用された日付。
  - [Auto Update Status]：自動アップデートが最後にアップデートをチェックした日時。

[Licensing] ガジェットの表示の変更

[Licensing] ガジェットのタイトルや表示する情報を取得するセンサーを変更するには、次の手順を実行します。

ステップ 1　ガジェットの右上にある [Tool] アイコンをクリックします。

ステップ 2　[Configure Settings] ウィンドウで次の値を変更できます。

- ガジェットのタイトル
- デバイス

ステップ 3　変更を保存するには、[Apply] をクリックします。変更を破棄する場合は、[Cancel] をクリックします。

詳細情報

ライセンス キーを取得してインストールする手順については、「ライセンスの設定」（P.18-10）を参照してください。

[Interface Status] ガジェット

[Interface Status] ガジェットには、次のような各インターフェイスに関する情報が表示されます。

- [Interface]：物理インターフェイスの名前（FastEthernet、GigabitEthernet、または PortChannel）。
- [Link]：インターフェイスがアップ状態かダウン状態か。
- [Enabled]：インターフェイスが無効であるか有効であるか。
- [Speed]：インターフェイスの速度が Auto、10 MB、100 MB、1000、10,000 MB のいずれであるか。
- [Mode]：インターフェイスが、無差別モード、インライン インターフェイス モード、インライン VLAN ペア モード、VLAN グループ モードのいずれであるか。
- [Received packets]：このインターフェイスで受信されたパケットの総数。
- [Transmitted packets]：このインターフェイスから送信されたパケットの総数。

[Interface Status] ガジェットの表示の変更

[Interface Status] ガジェットのタイトルや表示する情報を取得するデバイスを変更するには、次の手順を実行します。

ステップ 1　ガジェットの右上にある [Tool] アイコンをクリックします。

ステップ 2　[Configure Settings] ウィンドウで次の値を変更できます。

- ガジェットのタイトル
- デバイス

ステップ 3　変更を保存するには、[Apply] をクリックします。変更を破棄する場合は、[Cancel] をクリックします。

詳細情報

インターフェイスの詳細については、第 7 章「インターフェイスの設定」を参照してください。

[Global Correlation Reports] ガジェット

（注）　AIP SSC-5 は、グローバル相関機能をサポートしていません。

[Global Correlation Reports] ガジェットには、次のようなレピュテーションに関する情報が表示されます。

- [Packets Denied Due to Global Correlation]：検出された悪意のあるパケットのパーセンテージと、グローバル相関によってドロップされたパケットがあるかどうかが表示されます。
- [Total Packets Denied]：検出された悪意のあるパケットの総数と、グローバル相関基準によってドロップされたパケットが表示されます。

[Global Correlation Reports] ガジェットの表示の変更

[Global Correlation Reports] ガジェットのタイトルと情報の表示方法を変更するには、次の手順を実行します。

ステップ 1　ガジェットの右上にある [Tool] アイコンをクリックします。

ステップ 2　[Configure Settings] ウィンドウで次の値を変更できます。

- ガジェットのタイトル
- 表示メソッド（円グラフ、棒グラフ、または表）

ステップ 3　変更を保存するには、[Apply] をクリックします。変更を破棄する場合は、[Cancel] をクリックします。

詳細情報

- グローバル相関のレピュテーション機能の説明については、「レピュテーションについて」（P.13-3）を参照してください。

- ガジェットに表示されるセンサー ヘルス メトリックを設定する手順については、「センサーのヘルスの設定」（P.18-14）を参照してください。
- IME レポートの詳細については、第 21 章「レポートの設定と生成」を参照してください。

[Global Correlation Health] ガジェット

（注）　AIP SSC-5 は、グローバル相関機能をサポートしていません。

[Global Correlation Health] ガジェットには、次のようなグローバル相関に関する情報が表示されます。

- [Global Correlation Health]：グローバル相関のステータスが表示されます。
  - [Status of the Last Update Attempt]：グローバル相関がイネーブルであるかディセーブルであるかと、最後のアップデートが成功したか失敗したかを示します。ステータスの説明を表示するには、[i] アイコンをクリックします。

    （注）　ステータスが [Disabled] である場合は、グローバル相関がオフであるか、センサーのライセンスが取得されていません。

  - [Time Since Last Successful Update]：前回のアップデートからの時間を示します。
  - [Update Interval in Seconds]：アップデート間隔を秒数で示します。
  - [Update Server]：アップデートを実行するグローバル相関サーバの名前。
  - [Update Server Address]：アップデートを実行するグローバル相関サーバの IP アドレス。
- [Counters]：接続試行の回数が表示されます。
  - [Update Failures Since Last Success]：前回の成功したアップデート以降に発生した障害の数。
  - [Total Update Attempts]：センサーがグローバル相関をアップデートしようとした回数。
  - [Total Update Failures]：アップデートが失敗した回数。
- [Current Versions]：センサーがアップデートをチェックするコンポーネント（drop、rule、ip、config）のバージョンが表示されます。
- [Warnings]：グローバル相関に関する警告の数。
- [Network Participation]：ネットワーク参加のステータスが表示されます。
  - [Status]：接続状態が良好であるか、成功した最後の接続以降に発生した接続障害の回数が 1 ～ 5 回であるか、成功した最後の接続以降に発生した接続障害の回数が 5 回を超えるかを示します。ステータスの説明を表示するには、[i] アイコンをクリックします。
- [Counters]：接続試行の回数が表示されます。
  - [Total connection attempts]：接続試行の回数。
  - [Total connection failures]：接続障害が発生した回数。
  - [Connection failures since last success]：成功した最後の接続以降に発生した接続障害の数。
- [Connection History]：すべての接続試行とその結果（成功または失敗）が表示されます。接続試行のリストを表示するには、[i] アイコンをクリックします。

[Global Correlation Health] ガジェットの表示の変更

[Global Correlation Health] ガジェットの表示を変更するには、次の手順を実行します。

ステップ 1　ガジェットの右上にある [Tool] アイコンをクリックします。

ステップ 2　[Configure Settings] ウィンドウでガジェットのタイトルを変更します。

ステップ 3　変更を保存するには、[Apply] をクリックします。変更を破棄する場合は、[Cancel] をクリックします。

詳細情報

- グローバル相関のレピュテーション機能の説明については、「レピュテーションについて」（P.13-3）を参照してください。
- ガジェットに表示されるセンサー ヘルス メトリックを設定する手順については、「センサーのヘルスの設定」（P.18-14）を参照してください。
- ネットワーク参加の説明については、「ネットワーク参加について」（P.13-4）を参照してください。

[Network Security] ガジェット

[Network Security] ガジェットには、次のようなネットワーク セキュリティに関する情報が表示されます。

- Meta アラートとサマリー アラートを含むアラート数。
- 脅威レーティングおよびリスク レーティングの平均値。
- 脅威レーティングおよびリスク レーティングの指定期間内における最大値。

これらの値は、10 秒間隔でセンサーごとに集計され、緑、黄色、赤のいずれかに分類されます。緑が最高の安全性を表し、赤が最低の安全性を表します。全体的なネットワーク セキュリティ値は、すべての仮想センサーから取得されたセキュア値の中で最低の値を表します。

特定の仮想センサーの重大度レベルは、次のように計算されます。

- そのセンサーで過去 *n* 分以内に赤のイベントが 1 つ以上検出された場合、重大度は赤。*n* は設定された値で、デフォルトは 5 分です。
- そのセンサーで過去 *n* 分以内に黄のイベントが 1 つ以上検出され、赤のイベントが検出されなかった場合、重大度は黄。

  それ以外の場合、重大度は緑。

[Configuration] > *sensor_name* > [Policies] > [Event Action Rules] > [rules0] > [Risk Category] を選択し、リスク カテゴリを設定して、しきい値として緑、黄、赤のリスク レーティング値を指定します。

上のグラフは、合計、赤のイベント、黄のイベント、緑のイベントなどのカテゴリごとのイベント数を示します。下のグラフは、平均リスク レーティングと平均脅威レーティングの対比、または最大リスク レーティングと最大脅威レーティングの対比を示します。この情報は仮想センサーごとに分類されます。

[Network Security] ガジェットの表示の変更

[Network Security] ガジェットに表示されるネットワーク セキュリティ値を変更するには、次の手順を実行します。

ステップ 1　右上の [Tool] アイコンをクリックします。

ステップ 2　[Configure Settings] ウィンドウで次の値を変更できます。

- ガジェットのタイトル
- デバイスと仮想センサー
- イベント数グラフに表示するグラフを指定（すべて、赤、黄、緑）
- リスクと脅威の対比グラフに表示するグラフを指定（平均リスク レーティングと平均脅威レーティングの対比、または最大リスク レーティングと最大脅威レーティングの対比）

ステップ 3　[Apply] をクリックします。

詳細情報

脅威のしきい値を変更する手順については、「リスク カテゴリの設定」（P.8-33）を参照してください。

[Top Applications] ガジェット

[Top Applications] ガジェットには、センサーが検出した上位 10 のレイヤ 4 プロトコルが表示されます。

- TCP
- UDP
- ICMP
- IP

[Top Applications] ガジェットによって、センサー上の各種トラフィックの全体像を把握できます。

[Top Applications] ガジェットの表示の変更

[Top Applications] ガジェットに上位アプリケーションを表示する方法を変更するには、次の手順を実行します。

ステップ 1　ガジェットの右上にある [Tool] アイコンをクリックします。

ステップ 2　[Configure Settings] ウィンドウで次の値を変更できます。

- ガジェットのタイトル
- 情報を表示するデバイス
- 表示メソッド（円グラフ、棒グラフ、または表）
- 情報を表示するデバイス仮想センサー

ステップ 3　変更を保存するには、[Apply] をクリックします。変更を破棄する場合は、[Cancel] をクリックします。

[CPU, Memory, & Load] ガジェット

[CPU, Memory, & Load] ガジェットには、センサーの負荷、メモリ使用率、およびディスク使用量が表示されます。センサーに複数の CPU がある場合は、複数のメーターが表示されます。

- [Inspection Load]：トラフィック検査容量のうちセンサーの使用量を示します。

  0 はトラフィック バックアップが存在しないことを表し、100 はバッファが完全にバックアップされることを表します。検査負荷は、次の要因の影響を受けます。

  - 検査が必要なトラフィックの割合
  - 検査の対象となるトラフィックの種類
  - 検査の対象となるアクティブな接続の数
  - 1 秒あたりの新規接続の割合
  - 検出される攻撃の割合
  - センサーでアクティブとなっているシグニチャ
  - センサーに作成されたカスタム シグニチャ
- [CPU Usage]：センサーの CPU 使用量を示します。
- メモリ使用率：
  - [System]：設定およびイベントの保存に使用されているメモリの量。

    システム メモリはトラフィック検査には使用されません。システム メモリには、設定されている仮想センサーの数は影響しますが、トラフィック レートや攻撃レートの変化は影響しません。システム メモリは、センサーを設定しているとき以外は安定を保ちます。
  - [Analysis Engine]：SensorApp の一部である分析エンジンに割り当てられ、使用されているメモリの固定量。ここには、分析エンジンが現在使用しているメモリの量が表示されます。
- ディスク使用量：
  - [Boot]：OS ブート イメージとリカバリ イメージが含まれています。このパーティションは、センサーにシステム イメージをインストールするときに使用されます。
  - [Application Data]：設定データと IP ログ ファイルが含まれています。

各使用率の詳細を表示するには、[i] アイコンをクリックします。

[CPU, Memory, & Load] ガジェットの表示の変更

[CPU, Memory, & Load] ガジェットのタイトルや表示する情報を取得するセンサーを変更するには、次の手順を実行します。

ステップ 1　ガジェットの右上にある [Tool] アイコンをクリックします。

ステップ 2　[Configure Settings] ウィンドウで次の値を変更できます。

- ガジェットのタイトル
- デバイス

ステップ 3　変更を保存するには、[Apply] をクリックします。変更を破棄する場合は、[Cancel] をクリックします。

[RSS Feed] ガジェット

デフォルトでは、Cisco.com 上の Cisco Security Advisors サイトから直接 [RSS Feed] ガジェットに情報が取り込まれます。設定した RSS フィード チャネルを [RSS Feed] ガジェットに表示することもできます。モニタする RSS フィードごとにガジェットを作成できます。

[RSS Feed] ガジェットの表示の変更

[RSS Feed] ガジェットに RSS フィードを表示する方法を変更するには、次の手順を実行します。

ステップ 1　右上の [Tool] アイコンをクリックします。

ステップ 2　[Configure Settings] ウィンドウで次の値を変更できます。

- ガジェットのタイトル
- フィード チャネル URL

ステップ 3　[Apply] をクリックします。

詳細情報

RSS フィードのカスタマイズについては、「RSS フィードの設定」（P.4-2）を参照してください。

[Top Attackers] ガジェット

[Top Attackers] ガジェットには、指定した時間内における上位攻撃者の IP アドレスごとのイベント数が表示されます。グラフは制限時間に従って変更されます。また、さまざまな条件でフィルタ処理を行うことにより、必要な情報だけを表示できます。さらに、各 IP アドレスについて DNS 名前解決を使用することもできます。

[Top Attackers] ガジェットの表示の変更

[Top Attackers] ガジェットに上位攻撃者の統計情報を表示する方法を変更するには、次の手順を実行します。

ステップ 1　右上の [Tool] アイコンをクリックします。

ステップ 2　[Configure Settings] ウィンドウで次の値を変更できます。

- ガジェットのタイトル
- 表示フォーム（円グラフ、棒グラフ、または表）
- 一度に統計情報に表示する上位攻撃者数（10、20、または 30）
- 統計情報を収集する間隔（過去 1 時間、過去 8 時間、過去 1 日）
- このガジェットに関連するフィルター

ステップ 3　各 IP アドレスについて DNS 名前解決を使用する場合は、[Resolve addresses] チェックボックスをオンにします。

ステップ 4　[Apply] をクリックします。

詳細情報

フィルタの設定手順については、「フィルタの設定」（P.3-17）を参照してください。

[Top Victims] ガジェット

[Top Victims] ガジェットには、指定した時間内における上位攻撃対象の IP アドレスごとのイベント数が表示されます。グラフは制限時間に従って変更されます。また、さまざまな条件でフィルタ処理を行うことにより、必要な情報だけを表示できます。さらに、各 IP アドレスについて DNS 名前解決を使用することもできます。

[Top Victims] ガジェットの表示の変更

[Top Victims] ガジェットに上位攻撃対象の統計情報を表示する方法を変更するには、次の手順を実行します。

ステップ 1　右上の [Tool] アイコンをクリックします。

ステップ 2　[Configure Settings] ウィンドウで次の値を変更できます。

- ガジェットのタイトル
- 表示フォーム（円グラフ、棒グラフ、または表）
- 一度に統計情報に表示する上位攻撃対象者数（10、20、または 30）
- 統計情報を収集する間隔（過去 1 時間、過去 8 時間、過去 1 日）
- このガジェットに関連するフィルター

ステップ 3　各 IP アドレスについて DNS 名前解決を使用する場合は、[Resolve addresses] チェックボックスをオンにします。

ステップ 4　[Apply] をクリックします。

詳細情報

フィルタの設定手順については、「フィルタの設定」（P.3-17）を参照してください。

[Top Signatures] ガジェット

[Top Signatures] ガジェットには、指定した時間内における上位シグニチャが表示されます。グラフは制限時間に従って変更されます。また、さまざまな条件でフィルタ処理を行うことにより、必要な情報だけを表示できます。

[Top Signatures] ガジェットの表示の変更

[Top Signatures] ガジェットに上位シグニチャの統計情報を表示する方法を変更するには、次の手順を実行します。

ステップ 1　右上の [Tool] アイコンをクリックします。

ステップ 2　[Configure Settings] ウィンドウで次の値を変更できます。

- ガジェットのタイトル
- 表示フォーム（円グラフ、棒グラフ、または表）

- 一度に統計情報に表示する上位シグニチャ数（10、20、または 30）
- 統計情報を収集する間隔（過去 1 時間、過去 8 時間、過去 1 日）
- このガジェットに関連するフィルター

ステップ 3　[Apply] をクリックします。

詳細情報

フィルタの設定手順については、「フィルタの設定」（P.3-17）を参照してください。

[Attacks Over Time] ガジェット

[Attacks Over Time] ガジェットには、指定した時間内の攻撃数が表示されます。グラフは制限時間に従って変更されます。また、さまざまな条件でフィルタ処理を行うことにより、必要な情報だけを表示できます。

[Attacks Over Time] ガジェットの表示の変更

[Attacks Over Time] ガジェットに一定時間内の攻撃の統計情報を表示する方法を変更するには、次の手順を実行します。

ステップ 1　右上の [Tool] アイコンをクリックします。

ステップ 2　[Configure Settings] ウィンドウで次の値を変更できます。

- ガジェットのタイトル
- 統計情報を収集する間隔（過去 1 時間、過去 8 時間、過去 1 日）
- このガジェットに関連するフィルター

ステップ 3　[Apply] をクリックします。

詳細情報

フィルタの設定手順については、「フィルタの設定」（P.3-17）を参照してください。

個々の上位攻撃者および上位攻撃対象の IP アドレスに対する 1 つのイベントを調べる

上位攻撃者または上位攻撃対象の特定の IP アドレスに対する 1 つのイベントを調べるには、次の手順を実行します。

ステップ 1　[Home] > [Dashboards] > [Dashboardose] を選択し、個々の攻撃者または攻撃対象の IP アドレスを扱うダッシュボードのタブをクリックします。

ステップ 2　[Events for] ドロップダウン リストから攻撃者または攻撃対象の IP アドレス（例：**Attacker 51.66.166.10**）を選択します。データベースからデータが取得され、表示されます。このウィンドウでは、攻撃者または攻撃対象の設定を表示して変更を加えたり、イベントの詳細を表示したりできます。

ステップ 3　1 つのイベントを調べるには、リストでイベントを選択し、ツールバーの [Event] をクリックします。[Event] ドロップダウン リストから、次の情報を表示できます（これらの情報は、ウィンドウの下部にタブ形式で表示される [Event Details] セクションにも表示されます）。

- [Summary]：そのイベントに関する情報の要約が表示されます。
- [Explanation]：そのイベントに関連付けられたシグニチャの説明および関連シグニチャ情報が表示されます。
- [Related Threats]：関連する脅威と MySDN 内の詳細情報へのリンクが表示されます。
- [Trigger Packet]：イベントをトリガーしたパケットに関する情報が表示されます。
- [Context Data]：パケット コンテキスト情報が表示されます。
- [Actions Taken]：展開されたイベント アクションのリストが表示されます。
- [Notes]：イベントに名称（New、Assigned、Acknowledged、Closed、または Deleted）を割り当てることにより、イベントに対してアクションを実行できます。[Notes] フィールドに注釈を入力し、[Save Note] をクリックして保存します。

ステップ 4　このイベントの詳細を印刷するには、[Show All Details] をクリックして、イベントの詳細をプリンタ対応のウィンドウに表示します。

ステップ 5　選択したイベントから属性を追加するには、[Filter] ドロップダウン メニューから [Add to Filter] > [Attacker IP/Victim IP/Signature ID] を選択します。ウィンドウの上部に [Filter] タブが表示されます。

ステップ 6　このイベントからフィルタを作成するには、[Filter] ドロップダウン メニューから [Create a Filter] を選択します。

ステップ 7　このイベントに関連付けられたシグニチャを編集するには、[Edit Signature] をクリックします。[Configuration] > ***sensor_name*** > [Policies] > [Signature Definitions] > [sig0] > [Active Signatures] が表示され、シグニチャを編集できます。

ステップ 8　このイベントからイベント アクション規則フィルタを作成するには、[Create Rule] をクリックします。[Configuration] > ***sensor_name*** > [Policies] > [IPS Policies] > [Add Event Action Filter] へ移動し、イベント アクション規則フィルタを追加できます。

ステップ 9　攻撃者を阻止するには、[Stop Attacker] ドロップダウン メニューから次のオプションのいずれかを選択します。

- [Using Inline Deny]：このオプションを選択すると、[Configuration] > ***sensor_name*** > [Sensor Monitoring] > [Time-Based Actions] > [Denied Attackers] > [Add Denied Attacker] へ移動します。
- [Using Block on another device]：このオプションを選択すると、[Configuration] > ***sensor_name*** > [Sensor Monitoring] > [Time-Based Actions] > [Host Blocks] > [Add Host Block] へ移動します。

ステップ 10　このイベントに関係する IP アドレスに対して ping、traceroute、DNS、および whois を実行するには、これらのコマンドを [Tools] ドロップダウン メニューから選択します。

ping を使用すると、基本的なネットワーク接続を診断できます。ping により、センサーが応答するかどうかを簡単に確認できます。traceroute を使用すると、IP パケットが宛先に到達するまでのルートを表示できます。whois を使用すると、ドメイン名または IP アドレスの所有者を確認できます。DNS ルックアップを使用すると、電話帳を調べるように、ホスト名を IP アドレスに変換できます。

ステップ 11　イベントを保存、削除、またはコピーするには、[Other] ドロップダウン リストから実行するアクションを選択します。

ステップ 12　ビューに加えた変更を保存するには、[Apply] をクリックします。変更を破棄する場合は、[Reset] をクリックします。

詳細情報

- フィルタ規則を追加する手順については、「フィルタの設定」（P.3-17）を参照してください。
- イベント アクション規則フィルタを追加する手順については、「イベント アクション フィルタの設定」（P.11-16）を参照してください。
- 拒否攻撃者を追加する手順については、「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。
- ホスト ブロックを追加する手順については、「ホスト ブロックの設定」（P.19-6）を参照してください。
- ツールの使用の詳細については、「デバイスでのツールの使用」（P.2-6）を参照してください。

上位シグニチャに対する 1 つのイベントを調べる

特定のシグニチャ ID に対する 1 つのイベントを調べるには、次の手順を実行します。

ステップ 1　[Home] > [Dashboards] > [Dashboard] を選択し、特定のシグニチャについて特定のイベントを使用するセンサーのタブをクリックします。

ステップ 2　[Events for] ドロップダウン リストからシグニチャ ID（例：**SigID 3142**）を選択します。データベースからデータが取得され、表示されます。このウィンドウでは、設定を表示して変更を加えたり、イベントの詳細を表示したりできます。

ステップ 3　1 つのイベントを調べるには、リストでイベントを選択し、[Event] をクリックします。[Event] ドロップダウン リストから、次の情報を表示できます（これらの情報はウィンドウ下部の [Event Details] セクションに表示され、同じメニュー項目がタブ形式で表示されます）。

- [Summary]：そのイベントに関する情報の要約が表示されます。
- [Explanation]：そのイベントに関連付けられたシグニチャの説明および関連シグニチャ情報が表示されます。
- [Related Threats]：関連する脅威と MySDN 内の詳細情報へのリンクが表示されます。
- [Trigger Packet]：イベントをトリガーしたパケットに関する情報が表示されます。
- [Context Data]：パケット コンテキスト情報が表示されます。
- [Actions Taken]：展開されたイベント アクションのリストが表示されます。
- [Notes]：イベントに名称（New、Assigned、Acknowledged、Closed、または Deleted）を割り当てることにより、イベントに対してアクションを実行できます。[Notes] フィールドに注釈を入力し、[Save Note] をクリックして保存します。

ステップ 4　このイベントの詳細を印刷するには、[Show All Details] をクリックして、イベントの詳細をプリンタ対応のウィンドウに表示します。

ステップ 5　このイベントをフィルタに追加するには、[Filter] ドロップダウン メニューから [Add to Filter] > [Attacker IP/Victim IP/Signature ID] を選択します。ウィンドウの上部に [Filter] タブが表示されます。

ステップ 6　このイベントからフィルタを作成するには、[Filter] ドロップダウン メニューから [Create a Filter] を選択します。

ステップ 7　このイベントに関連付けられたシグニチャを編集するには、[Edit Signature] をクリックします。[Configuration] > ***sensor_name*** > [Policies] > [Signature Definitions] > [sig0] > [Active Signatures] へ移動し、シグニチャを編集できます。

ステップ 8　このイベントからイベント アクション規則フィルタを作成するには、[Create Rule] をクリックします。[Configuration] > ***sensor_name*** > [Policies] > [IPS Policies] > [Add Event Action Filter] へ移動し、イベント アクション規則フィルタを追加できます。

ステップ 9　攻撃者を阻止するには、[Stop Attacker] ドロップダウン メニューから次のオプションのいずれかを選択します。

- [Using Inline Deny]：このオプションを選択すると、[Configuration] > ***sensor_name*** > [Sensor Monitoring] > [Time-Based Actions] > [Denied Attackers] > [Add Denied Attacker] へ移動します。
- [Using Block on another device]：このオプションを選択すると、[Configuration] > ***sensor_name*** > [Sensor Monitoring] > [Time-Based Actions] > [Host Blocks] > [Add Host Block] へ移動します。

ステップ 10　このイベントに関係する IP アドレスに対して ping、traceroute、DNS、および whois を実行するには、これらのコマンドを [Tools] ドロップダウン メニューから選択します。

ping を使用すると、基本的なネットワーク接続を診断できます。ping により、センサーが応答するかどうかを簡単に確認できます。traceroute を使用すると、IP パケットが宛先に到達するまでのルートを表示できます。whois を使用すると、ドメイン名または IP アドレスの所有者を確認できます。DNS ルックアップを使用すると、電話帳を調べるように、ホスト名を IP アドレスに変換できます。

ステップ 11　イベントを保存、削除、またはコピーするには、[Other] ドロップダウン リストから実行するアクションを選択します。

詳細情報

- フィルタ規則を追加する手順については、「フィルタの設定」（P.3-17）を参照してください。
- イベント アクション規則フィルタを追加する手順については、「イベント アクション フィルタの設定」（P.11-16）を参照してください。
- 拒否攻撃者を追加する手順については、「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。
- ホスト ブロックを追加する手順については、「ホスト ブロックの設定」（P.19-6）を参照してください。
- ツールの使用の詳細については、「デバイスでのツールの使用」（P.2-6）を参照してください。

フィルタの設定

（注）　[Filter] タブと [Add Filter] ダイアログボックスのフィールドで IPv6 アドレスおよび IPv4 アドレスがサポートされるようになりました。

フィルタを設定するには、次の手順を実行します。

ステップ 1　[Home] > [Dashboards] を選択し、フィルタ規則を設定するダッシュボードのタブをクリックします。

ステップ 2　フィルタを適用するガジェット（例：[Top Attackers] ガジェット）を選択します。

フィルタ規則は、[Top Attackers]、[Top Victims]、および [Top Signatures] の各ガジェットに適用できます。

ステップ 3　[Events for] ドロップダウン メニューから、フィルタを追加する IP アドレスまたはシグニチャ ID を選択します。

ステップ 4　フィルタを適用するイベントを選択します。

ヒント　リストで複数の項目を選択するには、Ctrl キーを押します。

ステップ 5　[View Settings] > [Filter] をクリックします。

ステップ 6　[Filter Name] ドロップダウン メニューから、このフィルタのフィルタ名を選択するか、[Note] アイコンをクリックしてから [Add] をクリックし、新しいファイルを追加します。

a. [Filter Name] フィールドに、このフィルタの名前を入力します。

b. [Attacker IP] フィールドに攻撃者の IP アドレスを入力するか、[Note] アイコンをクリックして一意の IP アドレスまたは IP アドレスの範囲を追加し、[OK] をクリックします。

c. [Victim IP] フィールドに攻撃対象の IP アドレスを入力するか、[Note] アイコンをクリックして一意の IP アドレスまたは IP アドレスの範囲を追加し、[OK] をクリックします。

d. [Signature Name/ID] フィールドにシグニチャ名またはシグニチャ ID を入力するか、[Note] アイコンをクリックし、シグニチャ タイプを選択して、[OK] をクリックします。

e. [Victim Port] フィールドに攻撃対象ポートを入力するか、[Note] アイコンをクリックして必要な条件を満たす攻撃対象ポートを入力し、[OK] をクリックします。

f. このフィルタの重大度を選択します。

g. [Risk Rating] フィールドに、このフィルタのリスク レーティングを入力するか、[Note] アイコンをクリックして必要な条件を満たすリスク レーティングを入力し、[OK] をクリックします。

h. [Reputation] フィールドに、このフィルタのレピュテーション スコアを入力するか、[Note] アイコンをクリックして必要な条件を満たすレピュテーションを入力し、[OK] をクリックします。

i. [Threat Rating] フィールドに、このフィルタの脅威レーティングを入力するか、[Note] アイコンをクリックして必要な条件を満たす脅威レーティングを入力し、[OK] をクリックします。

j. [Actions Taken] フィールドに、このフィルタをトリガーするアクションを入力するか、[Note] アイコンをクリックして、このフィルタをトリガーするアクションのチェックボックスをオンにし、[OK] をクリックします。

k. [Sensor Name(s)] フィールドに、このフィルタの影響を受けるセンサーの名前を入力するか、[Note] アイコンをクリックして、このフィルタを適用するセンサーのチェックボックスをオンにし、[OK] をクリックします。

l. [Virtual Sensor] フィールドに、このフィルタを適用する仮想センサーを入力します。

m. [Status] ドロップダウン メニューから、フィルタ処理を行うステータスを選択します。

n. [Victim Locality] フィールドに、フィルタ処理の対象とする作成済みのイベント アクション規則変数の名前を入力します。

ステップ 7　グループを設定するには、[Group By] タブをクリックします。

a. [Group events based on the following criteria] チェックボックスをオンにし、ドロップダウン メニューからカテゴリを選択することにより、イベントをグループ化するための階層を構築します。

b. [Grouping Preferences] で、[Single Level]、[Show Group Columns]、[Show Count Columns] の各チェックボックスをオンにできます。[Show Group Columns] チェックボックスをオンにした場合は、カウント カラムのみを表示できます。

ステップ 8　色規則を追加するには、[Color Rules] タブをクリックしてから [Add] をクリックします。

a. [Filter Name] フィールドに、この色規則フィルタの名前を入力します。

b. [Enable] チェックボックスをオンにします。

（注）　[Enable] チェックボックスをオンにしなければ、色規則フィルタは有効になりません。

c. [Packet Parameters] では、この色規則フィルタを適用する IP アドレス、シグニチャ名、攻撃対象ポートを入力します。

d. [Rating and Action Parameters] では、この色規則フィルタを適用する重大度、リスク レーティング、脅威レーティング、およびアクションを入力します。

e. [Other Parameters] では、この色規則フィルタを適用するセンサー名、仮想センサー名、ステータス、攻撃対象の所在地を入力します。

f. [Color Parameters] では、この色規則フィルタの前景色、背景色、およびフォント タイプを選択し、[OK] をクリックします。

ヒント　これらのフィールドに入力する値の正しい形式を確認するために、[Note] アイコンをクリックしてください。

ステップ 9　フィールドとその順序を編集するには、[Fields] タブをクリックし、[Add >>]、[<< Remove]、[Move Up]、および [Move Down] をクリックして、表示するフィールドを選択し、希望する順序どおりにフィールドを並べ替えます。

ステップ 10　[General] タブをクリックし、[View Description] フィールドをクリックして、ビューの説明を入力します。

ステップ 11　[Save As] をクリックして新しいビューを作成し、[Name] フィールドにビューの名前を入力します。設定が新しいビューにコピーされます。

ステップ 12　[Save] をクリックして、ビューに加えた変更を保存します。フィルタが [Filter Name] ドロップダウン メニューに表示されます。

ステップ 13　ビューに加えた変更を保存するには、[Apply] をクリックします。変更を破棄する場合は、[Reset] をクリックします。

[Manage Filter Rules] ダイアログボックスのフィールド定義

[Manage Filter Rules] ダイアログボックスには次のフィールドがあります。

- [Basic Top Attacker Filter]：上位攻撃者イベントのすべての重大度（高、中、低、および情報）が表示されます。
- [Action Denied-Attacker]：拒否アクション イベントの拒否攻撃者アクション、新しいアラート ステータス、およびすべての重大度（高、中、低、および情報）が表示されます。
- [Basic Over Time Attack Filter]：経時的攻撃イベントのすべての重大度（高、中、低、および情報）が表示されます。
- [Basic Top Signature Filter]：上位シグニチャ イベントのすべての重大度（高、中、低、および情報）が表示されます。
- [Basic Top Victim Filter]：上位攻撃対象イベントのすべての重大度（高、中、低、および情報）が表示されます。

- [Related Events Filter]：関連イベントのすべての重大度（高、中、低、および情報）が表示されます。
- [Critical Threat]：重大なイベントの 75 ～ 100 のすべての脅威レーティング、新しいアラート ステータス、およびすべての重大度（高、中、低、および情報）が表示されます。
- [High Severity]：すべてのイベントについて、新しいアラート ステータスで重大度が高であるすべてのアラートが表示されます。
- [Basic View Filter]：すべてのイベントについて、すべての重大度（高、中、低、および情報）が表示されます。
- [Basic Filter]：すべてのイベントについて、新しいアラート ステータスとすべての重大度（高、中、低、および情報）が表示されます。

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

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

- [Filter Name]：このフィルタの名前を入力するか、デフォルトのフィルタ名から選択できます。
- [Attacker IP]：このフィルタに含める攻撃者の IP アドレス。有効な値は、*ip_address* および *ip_address_range* です（例：10.0.0.1、!10.0.0.1、!10.1.1.1）。

  （注） 感嘆符（!）は「除外する」ことを意味します。

- [Victim IP]：このフィルタに含める攻撃対象の IP アドレス。有効な値は、*ip_address* および *ip_address_range* です（例：10.0.0.1、!10.0.0.1、!10.1.1.1）。
- [Signature Name/ID]：このフィルタに含めるシグニチャの名前/ID。有効な値は、*signature_name*、*signature_id*、*signature_id/subsig_id*、または *signature_id_range* です。次に例を示します。
  - no_checkpoint
  - no_checkpoint, 3320
  - no_checkpoint, 3320/1
  - [3300-400 Victim Port]：このフィルタに含める攻撃対象ポート。

  有効な値は、*number* または *number_range* です（例：>=80、70-100、<90、!100）。
- [Severity]：このフィルタに含める重大度。
- [Risk Rating]：このフィルタに含めるリスク レーティング。有効な値は、*number* または *number_range* です（例：>=80、70-100、<90、!100）。
- [Reputation]：このフィルタに含めるレピュテーション スコア。有効値の範囲は、-10.0 ～ 10.0 です。
- [Threat Rating]：このフィルタに含める脅威レーティング。有効な値は、*number* または *number_range* です（例：>=80、70-100、<90、!100）。
- [Action(s) Taken]：フィルタがアラート内で検索するアクションを選択できます。アクションは文字列であり、選択することもできれば、自由形式で入力することも可能です。
- [Sensor Name(s)]：このフィルタに含めるセンサーを指定できます。

- [Virtual Sensor]：このフィルタに含める仮想センサーを指定できます。
- [Status]：このフィルタにステータス（All、New、Assigned、Closed、Detected、Acknowledged）を割り当てることができます。[Status] フィールドは、特定のイベントの分析結果を後で使用するために保存しておく場合などに役立ちます。注釈を追加し、ステータスを [Acknowledged] に変更することにより、ステータスでフィルタ処理を実行し、承認されたケースをすべて表示して、追加の分析を行うことができます。
- [Victim Locality]：フィルタ処理を行う参加/アドレス アラート内のアラート属性。この属性は、イベント アクション規則変数に定義されます。
- [Color Parameters]：イベントの色規則を設定できます（次のオプションは [Color Rules] タブでフィルタを追加する場合にのみ表示されます）。
  - [Foreground]：イベントの前景色が表示され、使用する色を選択できます。
  - [Background]：イベントの背景色が表示され、使用する色を選択できます。
  - [Font Type]：イベントのフォント タイプとして、太字、イタリック、またはその両方を選択できます。
  - [Preview Text]：イベントがビューにどのように表示されるかを確認できます。

CHAPTER 4

RSS フィードの設定

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

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

この章では、RSS フィードについて説明し、その設定についても取り上げます。内容は次のとおりです。

RSS フィードについて

これらの RSS フィード チャネルはデフォルトで、Cisco Intelligence Operations Web サイトから直接受信するように設定されます。ただし、必要な RSS フィードを特定し、それを受信するように IME を設定できます。この設定は、[Cisco Security Center] > [RSS Feeds] ペインで行います。[RSS Feed] ガジェットに特定の URL からのフィードを表示することも可能です。

RSS フィード形式は、頻繁に更新されるコンテンツ（セキュリティ情報、ニュース、ポッドキャスト、ブログなど）の公開に使用されます。IME を使用して、最新のセキュリティ問題やセキュリティ関連ニュースを入手できるように RSS フィードを設定できます。

IME は、次の RSS フィード形式をサポートします。

- RSS 0.9x
- RSS 1.0/RDF
- RSS 2.0
- Atom 0.3
- Atom 1.0

Informa のオープン ソース ライブラリを使用して、これらの RSS フィード形式に対応できます。

RSS フィードを設定して編成するには、[RRS Feeds] ペインのツールバーを使用します。右クリック メニューを使用して、同じ機能を実行することもできます。

RSS フィードの設定

RSS フィードのアイコンにはラベルがありませんが、マウス カーソルを合わせたときに表示されるヘルプを使用してアイコンを確認できます。RSS フィード チャネルを追加して、カテゴリにまとめることができます。また、RSS フィードの初期設定を設定することも可能です。

表 4-1 に、RSS のアイコンと、各アイコンが設定する内容を示します。

表 4-1　RSS アイコンの説明

アイコン	説明
	カテゴリの追加
	カテゴリの削除
	カテゴリの名前変更
	チャネルの追加
	チャネルの削除
	チャネルのリロード
	チャネルを別のカテゴリに移動
	チャネルの名前変更
	初期設定の変更

RSS フィードを設定するには、次の手順を実行します。

ステップ 1　追加したい RSS フィードを配信する Web サイトを特定します。

ステップ 2　RSS フィードの URL をコピーします。

ステップ 3　[Home] > [Cisco Security Center] > [RSS Feeds] を選択し、[RSS Feeds] ツールバーの [Add Channel] アイコンをクリックします。

ステップ 4　[Add Channel] ダイアログボックスで、RSS フィードを受信するチャネルの URL を入力します。左側ペインに RSS フィードのサイトが表示され、右側ペインにアイテムが表示されます。

ステップ 5　RSS フィード アイテムを表示するには、左側ペインでカテゴリを選択し、表示したいアイテムを右側ペインで選択します。右側ペインの下部に、アイテムの情報が表示されます。アイテムの詳細を参照するには、[Read more] をクリックします

ステップ 6　新しいカテゴリを作成するには、[Add Category] アイコンをクリックし、[Add Category] ダイアログボックスで新しいカテゴリ名を割り当てます。左側ペインのリストに、作成した新しいカテゴリが表示されます。

ステップ 7　チャネルを別のカテゴリに移動するには、右側ペインで [Move Channel] アイコンをクリックし、[Move Channel] ダイアログボックスで新しいカテゴリを選択して、[OK] をクリックします。

ステップ 8　カテゴリを別のカテゴリに移動するには、右側ペインでチャネルを選択し、[Move Channel] アイコンをクリックします。[Move Channel] ダイアログボックスで新しいカテゴリを選択して、[OK] をクリックします。

ステップ 9　カテゴリと、そのカテゴリ内にあるすべての RSS フィードを削除するには、左側ペインでカテゴリを選択し、[Delete Category] アイコンをクリックします。チャネルを削除するには、右側ペインの上部で対象チャネルを選択し、[Delete Channel] アイコンをクリックします。デフォルトの 3 つの Cisco RSS フィード カテゴリは削除できません。

ステップ 10　カテゴリの名前を変更するには、左側ペインで [Rename Category] アイコンをクリックし、[Rename Category] ダイアログボックスに新しい名前を入力します。チャネルの名前を変更するには、右側ペインの上部で対象チャネルを選択し、[Rename Channe] アイコンをクリックして、[Rename Channel] ダイアログボックスの [Site Name] フィールドに新しい名前を入力します。

ステップ 11　チャネルをリロードするには、左側ペインで対象チャネルを選択し、[Reload Channel] アイコンをクリックします。

ステップ 12　RSS フィードの初期設定を設定するには、[Change Preferences] アイコンをクリックします。

a. 重複チャネルを作成できるようにしたい場合は、[Allow duplicate channel creation] チェックボックスをオンにします。

b. ドロップダウン メニューから、キャッシュに残すニュース アイテムの数を選択します。10、30、50、100、300、または 1000 を選択できます。

c. [Refresh every minutes] フィールドで、RSS フィードを最新の情報に更新する頻度を選択します。

d. デフォルト ブラウザを変更するには、[Use following browser] オプション ボタンをクリックし、[Browser command line] フィールドにブラウザのコマンド ラインを入力して、[OK] をクリックします。

CHAPTER 5

Startup Wizard の使用

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

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

この章では、Startup Wizard、およびそれを使用してセンサー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。

[Startup Wizard Introduction] ウィンドウ

（注） Startup Wizard でセンサーの基本的な設定を行うには、管理者である必要があります。

注意 IME は設定されていないセンサーと通信できないため、センサーの CLI にログインし、**setup** コマンドを実行して通信パラメータを設定する必要があります。例外的に、AIP SSC-5 の場合は、ASDM から初期化できます。

Startup Wizard を使用すると、センサーのセットアップや、すでに設定されているセンサーの変更ができます。新しい未設定のセンサーの初期化には使用できません。この場合は、**setup** コマンドを使用する必要があります。**setup** コマンドでセンサーを初期化するまで、IME はセンサーと接続できません。

Startup Wizard では、センサーが検査、応答、およびトラフィックのレポートを行うように、必要に応じて段階的な設定を行います。これを使用して、センサーの基本的な設定、インターフェイスの設定、仮想センサーの作成、ポリシーの作成、仮想センサーへのポリシーおよびインターフェイスの割り当て

ができます。また、センサーが Cisco.com からシグニチャ アップデートおよびシグニチャ エンジン アップデートを自動的にダウンロードするように設定したり、センサーに変更を保存することもできます。

Startup Wizard は、すべての IPS プラットフォームで使用できます。ある機能が特定のプラットフォームで使用できない場合でも、設定ウィンドウを確認する必要はありません

（注） Startup Wizard では、VLAN グループはサポートされていません。

IPS モジュールは、次の機能をサポートしていません。

- AIM IPS および NME IPS：インライン インターフェイス ペア、VLAN グループ、仮想化、または時刻設定。
- AIP SSM および IPS SSP：インライン VLAN ペア、インライン インターフェイス ペア、VLAN グループ、時刻設定、またはインターフェイス設定（適応型セキュリティ アプライアンスでインターフェイスを設定する必要があります）。
- AIP SSC-5：インライン VLAN ペア、インライン インターフェイス ペア、VLAN グループ、仮想化、時刻設定、またはインターフェイス設定（適応型セキュリティ アプライアンスでインターフェイスを設定する必要があります）。
- IDSM2：インライン インターフェイス ペアの VLAN グループまたは時刻設定。

（注） IPS モジュールは、設置されているルータ、スイッチ、または適応型セキュリティ アプライアンスから時刻設定を取得します。

注意 IME がスタンドアロン モードで動作しているときは、IME の Startup Wizard を使用して ASA トラフィックを AIP SSM および IPS SSP に割り当てることはできません。ASDM から IME に接続できる場合は、IME を使用して ASA トラフィックを割り当てることができます。

注意 IPS SSP には、4 種類のポートがあります（コンソール、管理、GigabitEthernet、および 10GE）。コンソールおよび管理ポート（IPS SSP の前面パネル右側）は、IPS ソフトウェアによって設定および管理されます。GigabitEthernet および 10GE ポート（IPS SSP の前面パネル左側）は、IPS ソフトウェアではなく ASA ソフトウェアによって設定および管理されます。しかし、IPS SSP をリセットまたはシャットダウンすると、GigabitEthernet および 10GE ポートもリンク ダウンします。リンク ダウンによるポートへの影響を最小限に抑えるために、IPS SSP のリセットまたはシャットダウンは、スケジュールされたメンテナンス時間中に行う必要があります。

詳細情報

- センサーの高度な設定を行うには、先にセンサーを初期化する必要があります。その後、IME で [Configuration] > *sensor_name* > [Sensor Setup] を選択します。**setup** コマンドを使用してセンサーを初期化する手順については、「センサーの基本的なセットアップ」（P.23-5）を参照してください。
- ASA ソフトウェアについての詳細は、『ASA User Documentation』を参照してください。

センサーのセットアップ

ここでは、センサーのセットアップ方法について説明します。内容は次のとおりです。

[Sensor Setup] ウィンドウ

（注）　IPS 6.1 および 6.2 は、グローバル相関機能をサポートしていません。

（注）　AIP SSC-5 は、グローバル相関機能をサポートしていません。

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

[Sensor Setup] ウィンドウでは、センサーの基本動作を設定できます。初期化の際にすでに値が割り当てられているので、ほとんどのフィールドにはすでにデータが入力されていますが、このウィンドウで必要に応じて変更することができます。

フィールド定義

[Sensor Setup] ウィンドウには、次のフィールドが表示されます。

- [Network Settings]：センサーのネットワーク設定を設定します。
  - [Host Name]：センサーの名前。ホスト名は 1 ～ 64 文字の文字列で、^[A-Za-z0-9_/-]+$ に一致するパターンです。デフォルトは sensor です。ホスト名にスペースが含まれているか、または英数字が 64 文字を超えていると、エラー メッセージが表示されます。
  - [IP Address]：センサーの IP アドレス。デフォルトは 192.168.1.2 です。
  - [Subnet Mask]：IP アドレスに対応するマスク。デフォルトは 255.255.255.0 です。
  - [Gateway]：デフォルト ゲートウェイ アドレス デフォルトは 192.168.1.1 です。
  - [HTTP Proxy Server]：HTTP プロキシ サーバの IP アドレスを入力します。カスタマー ネットワークでプロキシが使用されている場合は、グローバル相関のアップデートをダウンロードするためのプロキシ サーバが必要になる場合があります。
  - [HTTP Proxy Port]：HTTP プロキシ サーバのポート番号を入力します。
  - [DNS Primary]：プライマリ DNS サーバの IP アドレスを入力します。

注意　グローバル相関が機能するには、DNS サーバまたは HTTP プロキシ サーバのいずれかが常に設定されている必要があります。

注意　DNS 解決は、グローバル相関のアップデート サーバにアクセスする場合にだけサポートされます。

- [Allowed hosts/networks that can access the sensor]：ACL を追加します。
  - [Network]：アクセス リストに追加するネットワークの IP アドレス。
  - [Mask]：アクセス リストに追加するネットワークのネットマスク。

  （注）　センサーの ACL エントリを変更すると、変更を適用する際に、IME によりセンサーへの接続が切断される場合があります。

- [Network Participation]：データ送信の際に SensorBase ネットワーク に参加するかどうか、および参加するレベルを選択します。
  - [Off]：どのデータも SensorBase ネットワークに提供されません。
  - [Partial]：データは SensorBase ネットワークに提供されますが、潜在的に機密性が高いと見なされるデータはフィルタリングによって除外され、送信されません。
  - [Full]：すべてのデータが SensorBase ネットワーク に提供されます。
- [Current Sensor Date and Time]：NTP サーバが設定されていないアプライアンスの時刻と日付を設定します
  - [Date]：センサーのローカルな日付。時刻と日付をアップデートしたら、[Apply Date/Time to Sensor] をクリックして変更を有効にします。
  - [Apply Date/Time to Sensor]：センサー上の時刻と日付をただちにアップデートします。

  （注）　Startup Wizard をキャンセルしても、時刻と日付の変更は保持されます。

- [Time Zone]：時間帯の名前および UTC オフセットを設定します。
  - [Zone Name]：サマータイムが実施されていない場合のローカル時間帯。デフォルトは UTC です。37 個の事前に定義された時間帯のセットから選択するか、または一意の名前（24 文字）を作成できます。名前に使用できる文字のパターンは、^[A-Za-z0-9()+:,_/-]+$ です。
  - [Offset]：ローカル時間帯のオフセット（分単位）。デフォルトは 0 です。事前に定義された時間帯を選択した場合、このフィールドには自動的に値が入力されます。

  （注）　時間帯のオフセットを変更するには、センサーをリブートする必要があります。

- [NTP Server]：センサーが NTP サーバを時刻源として使用するように設定します。
  - [IP Address]：NTP サーバを使用してセンサー上の時刻を設定する場合の、NTP サーバの IP アドレス。
  - [Authenticated NTP]：認証された NTP を使用します。キーおよびキー ID が必要です。
  - [Key]：NTP MD5 キー タイプ。
  - [Key ID]：NTP サーバ上で認証に使用されるキーの ID（1 ～ 65535）。キー ID が範囲外の場合は、エラー メッセージが表示されます。

  （注）　センサーの時刻源として NTP サーバを使用する方法を推奨します。

- [Summertime]
  - [Enable Summertime]：このチェックボックスをオンにすると、サマータイム モードがイネーブルになります。デフォルトはディセーブルです。
  - [Configure Summertime]：サマータイム設定を設定する場合は、これをクリックします。

[Add ACL Entry]/[Edit ACL Entry] ダイアログボックス

センサーへのアクセスを許可するホストまたはネットワークのリストを設定することができます。アクセス リストには、次のホストのエントリが存在する必要があります。

- センサーに Telnet で接続する必要のあるホスト。
- センサーに対して SSH を使用する必要のあるホスト。
- Web ブラウザからセンサーにアクセスする必要のある、IDM や ASDM などのホスト。
- センサーにアクセスする必要のある、CSM などの管理ステーション。
- 該当のセンサーがマスター ブロッキング センサーの場合、リストにはブロッキング転送センサーの IP アドレスのエントリが必要です。

フィールド定義

[Add ACL Entry]/[Edit ACL Entry] ダイアログボックスには、次のフィールドが表示されます。

- [IP Address]：センサーへのアクセスを許可するホストまたはネットワークの IP アドレス。
- [Network Mask]：センサーへのアクセスを許可するホストまたはネットワークのネットワーク マスク。単一のホストのネットマスクは 32 です。

[Configure Summertime] ダイアログボックス

[Configure Summertime] ダイアログボックスには、次のフィールドが表示されます。

- [Summer Zone Name]：サマータイム時間帯の名前。デフォルトは UTC です。37 個の事前に定義された時間帯のセットから選択するか、または一意の名前（24 文字）を作成できます。名前に使用できる文字のパターンは、^[A-Za-z0-9()+:,_/-]+$ です。
- [Offset]：サマータイム中に付加する時間数（分単位）。デフォルトは 60 です。事前に定義された時間帯を選択した場合、このフィールドには自動的に値が入力されます。

  （注）　時間帯のオフセットを変更するには、センサーをリブートする必要があります。

- [Start Time]：サマータイム開始時刻の設定。値は hh:mm 形式です。時間または分が範囲外の場合はエラー メッセージが表示されます。
- [End Time]：サマータイム終了時刻の設定。値は hh:mm 形式です。時間または分が範囲外の場合はエラー メッセージが表示されます。
- [Summertime Duration]：サマータイム期間が毎年実施されるか、1 回だけの日付かを設定します。
  - [Recurring]：サマータイム期間は recurring（毎年実施される）モードです。
  - [Date]：サマータイム期間は、nonrecurring（毎年実施されない）モードです。
  - [Start]：開始の週、日、月の設定。
  - [End]：終了の週、日、月の設定。

センサー設定の設定

（注）　IPS 6.1 および 6.2 は、グローバル相関機能をサポートしていません。

（注）　AIP SSC-5 は、グローバル相関機能をサポートしていません。

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

Startup Wizard でセンサー設定を設定するには、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* > [Sensor Setup] > [Startup Wizard] > [Launch Startup Wizard] を選択し、[Next] をクリックします。

ステップ 3　[Host Name] フィールドにセンサー名を入力します。

ステップ 4　[IP Address] フィールドにセンサーの IP アドレスを入力します。

ステップ 5　[Subnet Mask] フィールドにネットワーク マスク アドレスを入力します。

ステップ 6　[Gateway] フィールドにデフォルト ゲートウェイ アドレスを入力します。

（注）　センサーのネットワーク設定を変更すると、変更を適用する際に IME および ASDM によりセンサーへの接続が切断されます。

ステップ 7　グローバル相関をサポートするために、HTTP プロキシ サーバまたは DNS サーバを設定するには、[HTTP Proxy Server] フィールドに HTTP プロキシ サーバの IP アドレスを入力して [HTTP Proxy Port] フィールドにポート番号を入力するか、または [DNS Primary] フィールドに DNS サーバの IP アドレスを入力します。

注意　グローバル相関が機能するには、DNS サーバまたは HTTP プロキシ サーバのいずれかが常に設定されている必要があります。

注意　DNS 解決は、グローバル脅威の相関のアップデート サーバにアクセスする場合にだけサポートされます。

ステップ 8　センサーへのアクセスを許可するホストおよびネットワークを設定するには、[Add] をクリックします。

a.　[IP Address] フィールドに、センサーへのアクセスを許可するホストの IP アドレスを入力します。

b.　[Network Mask] フィールドに、センサーへのアクセスを許可するホストのネットワーク マスク アドレスを入力します。

c.　[OK] をクリックします。

ヒント 変更を破棄して [Add ACL Entry] 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　ネットワーク参加をイネーブルにするには、参加するネットワーク参加のレベルを選択します。

- [Off]：どのデータも SensorBase ネットワークに提供されません。
- [Partial]：データは SensorBase ネットワークに提供されますが、潜在的に機密性が高いと見なされるデータはフィルタリングによって除外され、送信されません。
- [Full]：すべてのデータが SensorBase ネットワーク に提供されます。

デフォルトはオフです。[Partial] または [Full] を選択した場合は、Network Participation Disclaimer に同意する必要があります。

ステップ 10　[Current Sensor Date and Time] で、ドロップダウン カレンダーから現在の日付と時刻を選択し、[OK] をクリックしてから、[Apply Date/Time to Sensor] をクリックします。ローカル ホスト上の日付と時刻が表示されます。

注意　誤った時刻を指定すると、保存されているイベントに誤ったタイムスタンプが設定されます。この場合は、イベントをクリアする必要があります。

（注）　Startup Wizard をキャンセルしても、時刻と日付の変更は保持されます。

（注）　IPS モジュール上では日付または時刻の変更はできません。また、NTP を設定している場合も日付または時刻の変更はできません。

ステップ 11　[Time Zone] で、時間帯およびオフセットを設定します。

a. [Zone Name] フィールドのドロップダウン リストから時間帯を選択するか、または作成済みの時間帯を入力します。これは、サマータイム時間が実施されていない場合に表示される時間帯です。

b. [Offset] フィールドに、UTC のオフセットを分単位で入力します。事前に定義された時間帯名を選択した場合、このフィールドには自動的に値が入力されます。

（注）　時間帯のオフセットを変更するには、センサーをリブートする必要があります。

ステップ 12　NTP 時刻同期を使用している場合は、[NTP Server] で次を入力します。

- [IP Address] フィールドに NTP サーバの IP アドレスを入力します。
- 認証された NTP を使用している場合は、[Authenticated NTP] チェックボックスをオンにしてから、[Key] フィールドに NTP サーバのキーを入力し、[Key ID] フィールドに NTP サーバのキー ID を入力します。

（注）　NTP サーバを定義すれば、センサーの時間はその NTP サーバによって設定されます。CLI で **clock set** コマンドを実行するとエラーが発生しますが、時間帯のパラメータおよびサマータイムのパラメータは有効です。

ステップ 13　サマータイムをイネーブルにするには、[Enable Summertime] チェックボックスをオンにし、[Configure Summertime] をクリックします。

ステップ 14　ドロップダウン リストから [Summer Zone Name] を選択するか、または作成済みのサマータイム名を入力します。これは、サマータイム時間が実施されている間に表示される時間帯名です。

ステップ 15　[Offset] フィールドに、サマータイム中に付加する時間数を分単位で入力します。事前に定義されたサマータイム時間帯名を選択した場合、このフィールドには自動的に値が入力されます。

ステップ 16　[Start Time] フィールドに、サマータイム設定に適用する時刻を入力します。

ステップ 17　[End Time] フィールドに、サマータイム設定から削除する時刻を入力します。

ステップ 18　[Summertime Duration] で、サマータイム設定が毎年指定された日付に発生する（recurring）か、または指定された日付で開始および終了する（date）かを選択します。

a. [Recurring]：ドロップダウン リストから開始時刻と終了時刻を選択します。デフォルトは 3 月の第 2 日曜日と 11 月の第 1 日曜日です。

b. [Date]：ドロップダウン リストから開始時刻と終了時刻を選択します。開始および終了時刻のデフォルトは 1 月 1 日です。

ステップ 19　[OK] をクリックします。

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 20　Startup Wizard を続行するには、[Next] をクリックします。

（注）　ネットワーク設定を変更すると、センサーへの接続が中断し、新しいアドレスでの再接続が必要になることがあります。

インターフェイスの設定

（注）　Startup Wizard は、AIM IPS、AIP SSC-5、AIP SSM、IPS SSP、または NME IPS のインターフェイスおよび仮想センサーの設定には使用できません。

ここでは、センサー インターフェイスの設定方法について説明します。内容は次のとおりです。

[Interface Summary] ウィンドウ

[Interface Summary] ウィンドウには、既存のインターフェイス コンフィギュレーションの設定が表示されます。仮想センサーにインターフェイスが割り当てられていない場合は、[Assigned Virtual Sensor] カラムに「Unassigned」と表示され、[Details] カラムには「Promiscuous」と表示されます。インターフェイスは、物理インターフェイスか論理インターフェイスのいずれかになります。物理インターフェイスは、論理インターフェイスの一部となる場合もあり、さらに細分化することもできます。

インターフェイス コンフィギュレーションは、次の 5 種類のいずれかに指定できます。

- 無差別
- 無差別 VLAN グループ（サブインターフェイス）
- インライン インターフェイス ペア
- インライン インターフェイス ペア VLAN グループ（サブインターフェイス）
- インライン VLAN ペア（サブインターフェイス）

（注） Startup Wizard では、VLAN グループはサポートされていません。

注意 無差別モード、インライン ペア モード、またはインライン VLAN ペア モードで動作するように、単一の物理インターフェイスを設定できますが、これらのモードを組み合わせてインターフェイスを設定することはできません。

（注） Startup Wizard セッションごとに 1 つの物理または論理インターフェイスを設定できます。複数のインターフェイスを設定するには、Startup Wizard を複数回実行します。

このウィンドウで [Finish] をクリックすると、Startup Wizard が終了し、変更をコミットできます。そうしない場合は、インターフェイスおよび仮想センサーの設定を続行できます。

フィールド定義

[Interface Summary] ウィンドウには、次のフィールドが表示されます。

- [Name] : インターフェイスの名前。値は、無差別インターフェイスの場合、FastEthernet または GigabitEthernet です。インライン インターフェイスの場合、この名前はペアに割り当てた名前になります。
- [Details] : インターフェイスが無差別またはインラインであるかどうかを示し、VLAN ペアの有無を示します。
- [Assigned Virtual Sensor] : インターフェイスまたはインターフェイス ペアが仮想センサーに割り当てられているかどうかを示します。
- [Enabled] : インターフェイスをイネーブルにするかどうかを指定します。
- [Description] : インターフェイスの説明。

[Restore Defaults to an Interface] ダイアログボックス

[Restore Default Interface] ダイアログボックスには、仮想センサーに設定された、または割り当てられたすべてのインターフェイスが表示されます。ここから復元を行うインターフェイスを選択します。選択したインターフェイスが仮想センサーに割り当てられている場合は、割り当てが取り消されます。インライン インターフェイス ペアを選択した場合は、両方の物理インターフェイスがデフォルトに復元され、論理インターフェイスは削除されます。インライン VLAN ペアまたは VLAN グループを選択してデフォルトに復元することはできません。

注意　デフォルトに復元できるのは、物理インターフェイスおよびインライン インターフェイス ペアだけです。

[Traffic Inspection Mode] ウィンドウ

[Traffic Inspection Mode] ウィンドウでは、センサー インターフェイスを、無差別、インライン インターフェイス、またはインライン VLAN ペア モードとして設定します。センサーに 1 つの物理インターフェイス（AIM-IPS など）だけがある場合、[Inline Interface Pair Mode] オプション ボタンはディセーブルになります。センサーがインライン VLAN ペア モードをサポートしていない場合も、オプション ボタンはディセーブルになります。

[Traffic Inspection Mode] ウィンドウには、次のオプション ボタンが表示されます。

- [Promiscuous Mode] : センサーは、検査されたパケットのデータ パス内にありません。センサーはパケットを変更またはドロップできません。
- [Inline Interface Pair Mode] : センサーは、検査されたパケットのデータ パス内にあります。センサーは検査されたパケットを変更またはドロップできます。インライン インターフェイス インスペクションを行うには、2 つの物理インターフェイスをペアにする必要があります。
- [Inline VLAN Pair Mode] : センサーは、検査されたパケットのデータ パス内にあります。センサーは検査されたパケットを変更またはドロップできます。インライン VLAN インスペクションを行うには、1 つの物理インターフェイスと偶数の VLAN が必要です。また、このインターフェイスはトランク ポートに接続される必要があります。

[Interface Selection] ウィンドウ

[Interface Selection] ウィンドウでは、設定するインターフェイスを選択できます。

（注）　Startup Wizard セッションごとに 1 つの物理または論理インターフェイスを設定できます。複数のインターフェイスを設定するには、Startup Wizard を複数回実行します。

[Inline Interface Pair] ウィンドウ

[Inline Interface Pair] ウィンドウでは、2 つの一意のインターフェイスにインターフェイス名を割り当てることができます。センサーがハードウェア バイパスをサポートしている場合は、そのことを示すアイコンが表示されます。ハードウェア バイパス インターフェイスとハードウェア バイパスをサポートしていないインターフェイスをペアにすると、ハードウェア バイパスが使用できないことを示す警告メッセージが表示されます。

（注）　停電が発生した場合でも、ハードウェア バイパス インターフェイスにより、パケット フローが続行されます。

フィールド定義

[Inline Interface Pair] ウィンドウには、次のフィールドが表示されます。

- [Inline Interface Name]：このインライン インターフェイス ペアに名前を割り当てます。
- [First Interface of Pair]：このペアの最初のインターフェイスを割り当てます。
- [Second Interface of Pair]：このペアの他のインターフェイスを割り当てます。

[Inline VLAN Pairs] ウィンドウ

[Interface Inspection Mode] ウィンドウで [Inline VLAN Pair Mode] オプション ボタンをオンにすると、[Inline VLAN Pairs] ウィンドウでインライン VLAN ペアを設定できます。設定済みの場合はインライン VLAN ペアがテーブルに表示され、編集または削除できます。

（注）　別のインターフェイスとペアになっているインターフェイスや無差別モードで仮想センサーに割り当てられているインターフェイスにはインライン VLAN ペアは作成できません。

無差別モードのインターフェイスにインライン VLAN ペアを作成するには、仮想センサーからインターフェイスを削除してからインライン VLAN ペアを作成する必要があります。ペアにできるのは使用可能なインターフェイスだけです。

（注）　使用しているセンサーが、インライン VLAN ペアをサポートしていない場合、[Inline VLAN Pairs] ウィンドウは表示されません。AIM IPS、AIP SSC-5、および NME IPS はインライン VLAN ペアをサポートしていません。

フィールド定義

[Inline VLAN Pairs] ウィンドウには、次のフィールドが表示されます。

- [Subinterface Number]：インライン VLAN ペアのサブインターフェイス番号。値は 1 ～ 255 です。
- [VLAN A]：最初の VLAN の VLAN 番号が表示されます。値は 1 ～ 4095 です。
- [VLAN B]：第 2 の VLAN の VLAN 番号が表示されます。値は 1 ～ 4095 です。
- [Interface]：インライン VLAN ペアの名前。
- [Virtual Sensor]：このインライン VLAN ペアの仮想センサーの名前。
- [Description]：インライン VLAN ペアの説明。

[Add Inline VLAN Pair Entry]/[Edit Inline VLAN Pair Entry] ダイアログボックス

（注）　VLAN をそれ自身とペアにすることはできません。

（注）　サブインターフェイス番号と VLAN 番号は、物理インターフェイスごとに一意である必要があります。

[Add Inline VLAN Pair Entry]/[Edit Inline VLAN Pair Entry] ダイアログボックスには、次のフィールドが表示されます。

- [Subinterface Number] : サブインターフェイス番号を割り当てることができます。1 ～ 255 の範囲の番号を割り当てることができます。
- [VLAN A] : このインライン VLAN ペアに最初の VLAN を割り当てることができます。1 ～ 4095 の任意の VLAN を割り当てることができます。
- [VLAN B] : このインライン VLAN ペアにもう一方の VLAN を割り当てることができます。1 ～ 4095 の任意の VLAN を割り当てることができます。
- [Description] : このインライン VLAN ペアの説明を追加できます。

インライン VLAN ペアの設定

Startup Wizard でインライン VLAN ペアを設定するには、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* > [Sensor Setup] > [Startup Wizard] > [Launch Startup Wizard] を選択し、[Traffic Inspection Mode] ウィンドウが表示されるまで [Next] をクリックします。

ステップ 3　[Inline VLAN Pair Mode] オプション ボタンをクリックしたら、[Next] をクリックして [Add] をクリックします。

ステップ 4　[Subinterface Number] フィールドに、インライン VLAN ペアのサブインターフェイス番号（1 ～ 255）を入力します。

ステップ 5　[VLAN 1] フィールドで、このインライン VLAN ペアの最初の VLAN（1 ～ 4095）を指定します。

ステップ 6　[VLAN 2] フィールドで、このインライン VLAN ペアのもう一方の VLAN（1 ～ 4095）を指定します。

ステップ 7　必要に応じて、[Description] フィールドにインライン VLAN ペアの説明を入力します。

ヒント　変更を破棄して [Add Inline VLAN Pair] 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] をクリックします。新しいインライン VLAN ペアが、[Inline VLAN Pairs] ウィンドウのリストに表示されます。

ステップ 9　インライン VLAN ペアを編集するには、そのペアを選択し、[Edit] をクリックします。

ステップ 10　サブインターフェイス番号と VLAN 番号の変更、説明の編集を行えます。

ヒント　変更を破棄して [Edit Inline VLAN Pair] 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 11　[OK] をクリックします。編集された VLAN ペアが [Inline VLAN Pairs] ウィンドウのリストに表示されます。

ステップ 12　VLAN ペアを削除するには、そのペアを選択して [Delete] をクリックします。その VLAN ペアは、[Inline VLAN Pairs] ウィンドウの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 13　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。

仮想センサーの設定

ここでは、仮想センサ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。

[Virtual Sensors] ウィンドウ

インターフェイスを設定したら、Startup Wizard の [Virtual Sensors] ウィンドウで、インターフェイスを仮想センサーに割り当てます。デフォルトでは、インターフェイスは仮想センサー vs0 に割り当てられます。インターフェイスは既存の仮想センサーに割り当てることができます。また、新しい仮想センサーを作成することもできます。仮想センサーを作成するには、[Create a Virtual Sensor] をクリックします。[Add Virtual Sensor] ダイアログボックスが表示され、仮想センサーを設定できるようになります。

（注）　AIM IPS、AIP SSM、AIP SSC-5、IPS SSP、および NME IPS には設定可能なインターフェイスがないため、デフォルトの仮想センサーを使用する必要があります。

フィールド定義

[Virtual Sensors] ウィンドウには、次のフィールドが表示されます。

- [Interface(s)]：仮想センサーに割り当てる 1 つまたは複数のインターフェイスがリストされます。
- [Assign Interface to Virtual Sensor]：使用できる仮想センサーがリストされます。デフォルトのセンサーは vs0 です。
- [Create a Virtual Sensor]：[Add Virtual Sensor] ダイアログで、新しいシグニチャ、イベント アクション規則、および異常検出ポリシーを使用する仮想センサーを作成できます。また、デフォルト ポリシーを使用することもできます。
- [IPS Policy Summary Information]：割り当てられたインターフェイスが、割り当てられたポリシーとともに表示されます。
- [Default Block Policy]: 拒否イベント アクション オーバーライドで使用されるデフォルトのリスク カテゴリ。リスク レーティングが 90 ～ 100 のアラートはデフォルトで拒否されます。

  デフォルトのリスク カテゴリを使用しない場合は、[HIGHRISK] リスク カテゴリを編集するか、[Configuration] > *sensor_name* > [Policies] > [IPS Policies] > [Event Action Rules] > [rules0] > [Risk Category] を選択して新しいリスク カテゴリを作成できます。

[Add Virtual Sensor] ダイアログボックス

[Add Virtual Sensor] ダイアログボックスでは、新しいシグニチャ 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を作成できますが、これらを設定することはできません。新しいポリシーを作成するには、デフォルトのポリシーをクローニングします。

新しいポリシーを設定するには、

- 新しいシグニチャ ポリシーの場合は、[Configuration] > *sensor_name* > [Policies] > [Signature Definitions] > [NewSigPolicy] > [All Signatures] を選択します。
- 新しいイベント アクション規則ポリシーの場合は、[Configuration] > *sensor_name* > [Policies] > [Event Action Rules] > [NewRulesPolicy] を選択します。
- 新しい異常検出ポリシーの場合は、[Configuration] > *sensor_name* > [Policies] > [Anomaly Detections] > [NewADPolicy] を選択します。

フィールド定義

[Add Virtual Sensor] ダイアログボックスには、次のフィールドが表示されます。

- [Virtual Sensor Name]：仮想センサーに名前を割り当てます。
- [Description]：仮想センサーの説明を入力します。
- [Assign a Signature Policy]
  - [Assign an Existing Signature Policy]：すでに作成済みのシグニチャ ポリシーを割り当てます。
  - [Create a New Signature Policy]：新しいシグニチャ ポリシーを作成します。
- [Assign an Event Action Rules Policy]
  - [Assign an Existing Event Action Rules Policy]：すでに作成済みのイベント アクション規則ポリシーを割り当てます。
  - [Create a New Event Action Rules Policy]：新しいイベント アクション規則ポリシーを作成します。
- [Assign an Anomaly Detection Policy]
  - [Assign an Existing Anomaly Detection Policy]：すでに作成済みの異常検出ポリシーを割り当てます。
  - [Create a New Anomaly Detection Policy]：新しい異常検出ポリシーを作成します。

仮想センサーの追加

Startup Wizard を使用して仮想センサーを追加するには、次の手順を実行します。

ステップ 1　管理者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* > [Sensor Setup] > [Startup Wizard] > [Launch Startup Wizard] を選択し、[Virtual Sensors] ウィンドウが表示されるまで [Next] をクリックします。

ステップ 3　[Create a Virtual Sensor] をクリックします。

ステップ 4　[Virtual Sensor Name] フィールドに仮想センサー名を入力します。

ステップ 5　[Description] フィールドに、この仮想センサーの識別に役立つ説明を入力します。

ステップ 6　次のいずれかの方法でシグニチャ ポリシーを割り当てます。

a. [Assign a Signature Policy] オプション ボタンをクリックし、ドロップダウン リストからシグニチャ ポリシーを選択します。

b. [Create a Signature Policy] オプション ボタンをクリックし、フィールドにシグニチャ ポリシーの名前を入力します。

（注）　新しいシグニチャ ポリシーを設定するには、[Configuration] > *sensor_name* > [Policies] > [IPS Policies] > [Signature Definitions] > [NewSigPolicy] > [All Signatures] を選択します。

ステップ 7　次のいずれかの方法でイベント アクション規則ポリシーを割り当てます。

a. [Assign an Event Action Rules Policy] オプション ボタンをクリックし、ドロップダウン リストからイベント アクション規則ポリシーを選択します。

b. [Create an Event Action Rules Policy] オプション ボタンをクリックし、フィールドにイベント アクション規則ポリシーの名前を入力します。

（注）　新しいイベント アクション規則ポリシーを設定するには、[Configuration] > *sensor_name* > [Policies] > [Event Action Rules] > [NewRulesPolicy] を選択します。

ステップ 8　次のいずれかの方法で異常検出ポリシーを割り当てます。

a. [Assign an Anomaly Detection Policy] オプション ボタンをクリックし、ドロップダウン リストから異常検出ポリシーを選択します。

b. [Create an Anomaly Detection Policy] オプション ボタンをクリックし、フィールドに異常検出ポリシーの名前を入力します。

（注）　新しい異常検出ポリシーを設定するには、[Configuration] > *sensor_name* > [Policies] > [IPS Policies] > [Anomaly Detections] > [NewADPolicy] を選択します。

ステップ 9　[Finish] をクリックし、[Confirm Configuration Changes] ダイアログボックスで [Yes] をクリックして変更を保存します。

自動アップデートの設定

シグニチャ アップデートとシグニチャ エンジン アップデートを、センサーが Cisco.com から自動的にダウンロードするように設定できます。自動アップデートをイネーブルにすると、センサーは Cisco.com にログインし、シグニチャ アップデートとシグニチャ エンジン アップデートをチェックします。アップデートが入手可能な場合、センサーはアップデートをダウンロードして、インストールします。Cisco.com から Cisco IPS シグニチャのアップデートおよびシグニチャ エンジンのアップデートをダウンロードするには、暗号化特権を持つ Cisco.com ユーザ アカウントが必要です。初めてシスコ ソフトウェアをダウンロードするときに、暗号化特権を持つアカウントを設定します。

注意　センサーは、非透過プロキシ サーバからの Cisco.com との通信をサポートしていません。

フィールド定義

Startup Wizard の [Auto Update] ウィンドウには、次のフィールドが表示されます。

- [Enable Signature and Engine Updates from Cisco.com] : センサーが Cisco.com にアクセスし、シグニチャ アップデートおよびシグニチャ エンジン アップデートをダウンロードしてセンサー上にインストールするようにします。

（注）　[Enable Signature and Engine Updates from Cisco.com] チェックボックスをオンにして、フィールドをイネーブルにする必要があります。

- [Cisco.com Access] : Cisco.com サーバのために次のオプションを指定します。
  - [Username] : Cisco.com 上のユーザ アカウントに対応するユーザ名を示します。
  - [Password] : Cisco.com 上のユーザ アカウントのパスワードを示します。
  - [Confirm Password] : Cisco.com のパスワードの再入力を強制することで、パスワードを確定します。
- [Schedule] : 毎日の開始時刻を指定します。
  - [Start Time] : アップデート プロセスを開始する時刻を 24 時間制で示します。これは、センサーが Cisco.com にアクセスして新しいアップデートをダウンロードする時刻です。

自動アップデートの設定

Cisco.com から自動アップデートを設定するには、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* > [Sensor Setup] > [Startup Wizard] > [Auto Update] を選択します。

ステップ 3　Cisco.com からのシグニチャ アップデートとシグニチャ エンジン アップデートをイネーブルにするには、[Enable Signature and Engine Updates from Cisco.com] チェックボックスをオンにします。

a. [Username] フィールドに、Cisco.com にログインするときに使用するユーザ名を入力します。ユーザ名の有効な値は、1 ～ 2047 文字です。

b. [Password] フィールドに、Cisco.com のユーザ名パスワードを入力します。パスワードの有効な値は、1 ～ 2047 文字です。

c. 確認のために [Confirm Password] フィールドにもう一度パスワードを入力します。

d. [Start Time] フィールドに、アップデートを開始する時刻を入力します。有効な値は hh:mm:ss（24 時間制）です。アップデートは毎日実行されます。

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 4　[Finish] をクリックして変更を保存します。

詳細情報

- ソフトウェアおよび暗号化特権を持つアカウントの取得手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。
- サポートされている FTP および HTTP サーバのリストについては、「サポートされる FTP および HTTP サーバ」（P.18-17）を参照してください。

- 自動アップデートをダウンロードするためにUNIX スタイルのディレクトリ リストを設定するには、「UNIX スタイルのディレクトリ リスト表示」（P.18-17）を参照してください。
- シグニチャ アップデートのインストールに要する時間の詳細については、「シグニチャのアップデートおよびインストール時間」（P.18-17）を参照してください。

CHAPTER 6

センサーのセットアップ

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

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

この章では、センサーのセットアップについて説明します。内容は次のとおりです。

初期化について

センサーをネットワークに設置したら、**setup** コマンドを使用してセンサーを初期化し、ネットワーク経由でセンサーが通信できるようにする必要があります。**setup** コマンドを使用してセンサーを初期化するまでは、IME の設定を行うことはできません。

setup コマンドを使用して、ホスト名、IP インターフェイス、アクセス コントロール リスト、グローバル相関サーバ、時間設定など、センサーの基本的な設定を行います。その後、続けて CLI の高度な設定を使用し、Telnet のイネーブル化、Web サーバの設定、仮想センサーとインターフェイスの割り当てとイネーブル化を実行できます。また、IME の Startup Wizard を使用することもできます。

センサーを初期化すると、[Sensor Setup] で他のネットワーク パラメータの必要な変更および設定ができます。

詳細情報

センサーの高度な設定を行うには、先にセンサーを初期化する必要があります。その後、IME で [Configuration] > *sensor_name* > [Sensor Setup] を選択します。**setup** コマンドを使用してセンサーを初期化する手順については、「センサーの基本的なセットアップ」（P.23-5）を参照してください。

ネットワークの設定

ここでは、ネットワークの設定の変更方法について説明します。内容は次のとおりです。

[Network] ペイン

（注）　ネットワークを設定するには、管理者である必要があります。

setup コマンドを使用してセンサーを初期化すると、[Network] ペインにネットワークおよび通信のパラメータ値が表示されます。これらのパラメータ値は、必要に応じて [Network] ペインで変更できます。

[Network] ペインのフィールド定義

（注）　AIP SSC-5 は、グローバル相関機能をサポートしていません。

（注）　IPS 6.1 および 6.2 は、グローバル相関機能をサポートしていません。

[Network] ペインには、次のフィールドが表示されます。

- [Network Settings]：センサーのネットワーク パラメータをイネーブルにします。
  - [Hostname]：センサーの名前。ホスト名は 1 ～ 64 文字の文字列で、^[A-Za-z0-9_/-]+$ に一致するパターンです。デフォルトは sensor です。ホスト名にスペースが含まれているか、または英数字が 64 文字を超えていると、エラー メッセージが表示されます。
  - [IP Address]：センサーの IP アドレス。デフォルトは 192.168.1.2 です。
  - [Network Mask]：IP アドレスに対応するマスク。デフォルトは 255.255.255.0 です。
  - [Default Route]：デフォルトのゲートウェイ アドレス。デフォルトは 192.168.1.1 です。
- [DNS/Proxy Settings]：グローバル相関をサポートするために、HTTP プロキシ サーバまたは DNS サーバのいずれかを設定します。
  - [HTTP Proxy Server]：プロキシ サーバの IP アドレスを入力します。ネットワークでプロキシを使用する場合、グローバル相関のアップデートをダウンロードするためのプロキシ サーバが必要になる場合があります。
  - [HTTP Proxy Port]：プロキシ サーバのポート番号を入力します。
  - [DNS Primary]：プライマリ DNS サーバの IP アドレスを入力します。
  - [DNS Secondary]：セカンダリ DNS サーバの IP アドレスを入力します。

– [DNS Tertiary]：ターシャリ DNS サーバの IP アドレスを入力します。

DNS サーバを使用している場合は、グローバル相関のアップデートに正常に到達できる DNS サーバを少なくとも 1 つ設定する必要があります。他の DNS サーバをバックアップ サーバとして設定することもできます。DNS クエリは、リストの先頭にあるサーバに送信されます。このサーバに到達できない場合、DNS クエリは次に設定されている DNS サーバに送信されます。

注意　グローバル相関が機能するには、DNS サーバまたは HTTP プロキシ サーバのいずれかが常に設定されている必要があります。

注意　DNS 解決は、グローバル相関のアップデート サーバにアクセスする場合にだけサポートされます。

- HTTP、FTP、Telnet、CLI、および他のオプション
  – [Web Server Port]：Web サーバが使用する TCP ポート。デフォルトは 443（HTTPS の場合）です。

  （注）　1 ～ 65535 以外の値を入力すると、エラー メッセージが表示されます。

  – [Enable TLS/SSL on HTTP]：Web サーバの TLS と SSL をイネーブルにします。デフォルトはイネーブルです。

  （注）　TLS と SSL はイネーブルにしておくことを強く推奨します。

  – [FTP Timeout]：センサーと FTP サーバの通信中にタイムアウトになるまで FTP クライアントが待機する時間（秒単位）を設定します。有効な値の範囲は 1 ～ 86400 秒です。デフォルト値は 300 秒です。
  – [Enable Telnet]：Telnet によるセンサーへのリモート アクセスをイネーブルまたはディセーブルにします。

  （注）　Telnet はセキュアなアクセス サービスではないため、デフォルトでは無効になっています。

  – [Allow Password Recovery]：パスワード リカバリをイネーブルにします。デフォルトはイネーブルです。

詳細情報

グローバル相関の詳細については、第 13 章「グローバル相関の設定」を参照してください。

ネットワークの設定

注意　グローバル相関機能が動作するには、有効なセンサーのライセンスが必要です。グローバル相関機能の統計情報については引き続き設定および表示できますが、グローバル相関データベースはクリアされ、更新は試行されなくなります。有効なライセンスをインストールすると、グローバル相関機能が再アクティブ化されます。

（注）　IPS 6.1 および 6.2 は、グローバル相関機能をサポートしていません。

（注）　AIP SSC-5 は、グローバル相関機能をサポートしていません。

ネットワークを設定するには、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* > [Sensor Setup] > [Network] を選択します。

ステップ 3　センサーのホスト名を編集するには、[Hostname] フィールドに新しい名前を入力します。

ステップ 4　センサーの IP アドレスを変更するには、[IP Address] フィールドに新しいアドレスを入力します。

ステップ 5　ネットワーク マスクを変更するには、[Network Mask] フィールドに新しいマスクを入力します。

ステップ 6　デフォルトのゲートウェイを変更するには、[Default Route] フィールドに新しいアドレスを入力します。

ステップ 7　グローバル相関をサポートするために、HTTP プロキシ サーバまたは少なくとも 1 つの DNS サーバを設定するには、[HTTP Proxy Server] フィールドに HTTP プロキシ サーバの IP アドレスを入力して [HTTP Proxy Port] フィールドにポート番号を入力するか、または [DNS Primary] フィールドに DNS サーバの IP アドレスを入力します。

DNS サーバを使用している場合は、グローバル相関のアップデートに正常に到達できる DNS サーバを少なくとも 1 つ設定する必要があります。他の DNS サーバをバックアップ サーバとして設定することもできます。DNS クエリは、リストの先頭にあるサーバに送信されます。このサーバに到達できない場合、DNS クエリは次に設定されている DNS サーバに送信されます。

注意　グローバル相関が機能するには、DNS サーバまたは HTTP プロキシ サーバのいずれかが常に設定されている必要があります。

注意　DNS 解決は、グローバル相関のアップデート サーバにアクセスする場合にだけサポートされます。

ステップ 8　Web サーバのポートを変更するには、[Web Server Port] フィールドに新しいポート番号を入力します。

（注）　Web サーバ ポートを変更した場合は、IME への接続時にブラウザの URL アドレスでそのポートを指定する必要があります。使用する形式は https://*sensor_ip_address*:*sensor_ip_address*（たとえば、https://10.1.9.201:1040）です。

ステップ 9　TLS/SSL をイネーブルまたはディセーブルにするには、[Enable TLS/SSL on HTTP] チェックボックスをオンまたはオフにします。

（注）　TLS/SSL は有効にしておくことを強くお勧めします。

（注）　TLS と SSL は、Web ブラウザと Web サーバ間の暗号化通信を可能にするプロトコルです。TLS/SSL をイネーブルにした場合、https://*sensor_ip_address* を使用して IME に接続します。TLS/SSL がディセーブルの場合は、http://*sensor_ip_address*:*port_number* を使用して、IME に接続します。

ステップ 10　FTP タイムアウトの時間を変更するには、[FTP Timeout] フィールドに新しい時間を入力します。デフォルト値は 300 秒です。

ステップ 11　リモート アクセスをイネーブルまたはディセーブルにするには、[Enable Telnet] チェックボックスをオンまたはオフにします。

（注）　Telnet はセキュアなアクセス サービスではないため、デフォルトでは無効になっています。ただし、センサー上でセキュアなサービスである SSH が常時実行されています。

ステップ 12　パスワード リカバリを許可するには、[Allow Password Recovery] チェックボックスをオンにします。

（注）　パスワード リカバリはイネーブルにしておくことを強く推奨します。パスワード リカバリをディセーブルにすると、パスワードに問題がある場合に、アクセスのためのセンサー イメージを再作成する必要があります。

ヒント　変更を元に戻すには、[Reset] をクリックします。

ステップ 13　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。

（注）　ネットワーク設定を変更すると、センサーへの接続が中断し、新しいアドレスでの再接続が必要になることがあります。

詳細情報

- グローバル相関の詳細については、第 13 章「グローバル相関の設定」を参照してください。
- さまざまなセンサーにおけるパスワード リカバリの手順については、「パスワードの回復」（P.18-3）を参照してください。

許可されたホストおよびネットワークの設定

ここでは、許可されたホストおよびネットワークをシステムに追加する方法について説明します。内容は次のとおりです。

[Allowed Hosts/Networks] ペイン

（注）　許可されたホストおよびネットワークを設定するには、管理者である必要があります。

setup コマンドを使用してセンサーを初期化すると、許可されたホストのパラメータ値が [Allowed Hosts/Networks] ペインに表示されます。これらのパラメータ値は、必要に応じて [Allowed Hosts/Networks] ペインで変更できます。[Allowed Hosts/Networks] ペインを使用して、センサーへのアクセスが許可されたホストまたはネットワークを指定します。デフォルトでは、リストには何もエントリがないため、ホストを追加するまで許可されたホストはありません。

（注）　許可されたホストのリストに、ASDM、IDM、IME、Cisco Security Manager などの管理ホスト、および Cisco Security MARS などのモニタリング ホストを追加する必要があります。追加しないと、センサーと通信できません。

注意　許可ホストを追加、編集、または削除するときは、センサーのリモート管理に使用する IP アドレスを削除しないように注意してください。

[Allowed Hosts/Network] ペインと、[Add Allowed Host] および [Edit Allowed Host] ダイアログボックスのフィールド定義

[Allowed Hosts/Network] ペインと、[Add Allowed Host] および [Edit Allowed Host] ダイアログボックスには、次のフィールドが表示されます。

- [IP Address]：センサーへのアクセスが許可されたホストの IP アドレス。
- [Network Mask]：ホストの IP アドレスに対応するマスク。

許可されたホストおよびネットワークの設定

センサーへのアクセスが許可されたホストとネットワークを指定するには、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* > [Sensor Setup] > [Allowed Hosts/Networks] を選択し、[Add] をクリックしてホストまたはネットワークをリストに追加します。許可されたホストは最大 512 台追加できます。

ステップ 3　[IP Address] フィールドに、ホストまたはネットワークの IP アドレスを入力します。入力した IP アドレスが既存のリストのエントリに含まれている場合、エラー メッセージが表示されます。

ステップ 4　ホストまたはネットワークのネットワーク マスクを [Network Mask] フィールドに入力するか、またはドロップダウン リストからネットワーク マスクを選択します。IME では、IP アドレスがホストであるかネットワークであるかに関係なく、必ずネットマスクを指定する必要があります。ネットマスクを指定しないと、「`Network Mask is not valid`」というエラーが表示されます。また、ネットワーク マスクが IP アドレスと一致しない場合も、エラー メッセージが表示されます。

ヒント　変更を破棄して [Add Allowed Host] 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　[OK] をクリックします。新しいホストまたはネットワークが、[Allowed Hosts/Networks] ペインにあるリストに表示されます。

ステップ 6　リストにある既存のエントリを編集するには、エントリを選択して [Edit] をクリックします。

ステップ 7　[IP Address] フィールドで、ホストまたはネットワークの IP アドレスを編集します。

ステップ 8　[Network Mask] フィールドで、ホストまたはネットワークのネットワーク マスクを編集します。

ヒント　変更を破棄して [Edit Allowed Host] 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。編集されたホストまたはネットワークが、[Allowed Hosts/Networks] ペインのリストに表示されます。

ステップ 10　リストからホストまたはネットワークを削除するには、そのホストまたはネットワークを選択し、[Delete] をクリックします。削除されたホストは、[Allowed Hosts/Networks] ペインのリストに表示されなくなります。

注意　ホストを削除すると、それ以降そのホストからのネットワーク接続はすべて拒否されます。

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 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。

時刻の設定

ここでは、時刻源とセンサーについて説明します。内容は次のとおりです。

[Time] ペイン

（注）　時刻を設定するには、管理者である必要があります。

[Time] ペインを使用して、センサーのローカルな日付、時刻、時間帯、サマータイム（DST）を設定し、センサーが時刻源に NTP サーバを使用するかどうかを設定します。

（注）　センサーの時刻源として NTP サーバを使用する方法を推奨します。

[Time] ペインのフィールド定義

[Time] ペインには、次のフィールドが表示されます。

- [Sensor Local Date]：センサー上の現在の日付。デフォルトは 1970 年 1 月 1 日です。日付の値が月の範囲外の場合、エラー メッセージが表示されます。
- [Sensor Local Time]：センサー上の現在の時刻（hh:mm:ss）。デフォルト値は 00:00:00 です。時間、分、または秒が範囲外の場合はエラー メッセージが表示されます。

  （注）　センサーが日付フィールドや時刻フィールドをサポートしていない場合、またはセンサー上で NTP を設定している場合、これらのフィールドはディセーブルになっています。

- [Standard Time Zone]：時間帯の名前と UTC オフセットを設定します。
  - [Zone Name]：サマータイムが実施されていない場合のローカル時間帯。デフォルトは UTC です。37 個の事前に定義された時間帯のセットから選択するか、または一意の名前（24 文字）を作成できます。名前に使用できる文字のパターンは、^[A-Za-z0-9()+:,_/-]+$ です。
  - [UTC Offset]：ローカル時間帯のオフセット（分単位）。デフォルトは 0 です。事前に定義された時間帯を選択した場合、このフィールドには自動的に値が入力されます。

（注）　時間帯のオフセットを変更するには、センサーをリブートする必要があります。

- [NTP Server]：センサーが NTP サーバを時刻源として使用するように設定します。
  - [IP Address]：NTP サーバを使用してセンサー上の時刻を設定する場合の、NTP サーバの IP アドレス。
  - [Authenticated NTP]：認証された NTP を使用します。キーおよびキー ID が必要です。
  - [Key]：NTP MD5 キー タイプ。
  - [Key ID]：NTP サーバ上で認証に使用されるキーの ID（1 ～ 65535）。キー ID が範囲外の場合は、エラー メッセージが表示されます。
  - [Unauthenticated NTP]：NTP を使用しますが、認証を必要としないため、キーおよびキー ID は必要ありません。
- [Summertime]：サマータイム設定をイネーブルにし、その設定をします。
  - [Enable Summertime]：ここをクリックすると、サマータイム モードがイネーブルになります。デフォルトはディセーブルです。

[Configure Summertime] ダイアログボックスのフィールド定義

[Configure Summertime] ダイアログボックスには、次のフィールドが表示されます。

- [Summer Zone Name]：サマータイム時間帯の名前。デフォルトは UTC です。37 個の事前に定義された時間帯のセットから選択するか、または一意の名前（24 文字）を作成できます。名前に使用できる文字のパターンは、^[A-Za-z0-9()+:,_/-]+$ です。
- [Offset]：サマータイム中に付加する時間数（分単位）。デフォルトは 60 です。事前に定義された時間帯を選択した場合、このフィールドには自動的に値が入力されます。

（注）　時間帯のオフセットを変更するには、センサーをリブートする必要があります。

- [Start Time]：サマータイム開始時刻の設定。値は hh:mm 形式です。時間または分が範囲外の場合はエラー メッセージが表示されます。
- [End Time]：サマータイム終了時刻の設定。値は hh:mm 形式です。時間または分が範囲外の場合はエラー メッセージが表示されます。
- [Summertime Duration]：サマータイム期間が毎年実施されるか、1 回だけの日付かを設定します。
  - [Recurring]：サマータイム期間は recurring（毎年実施される）モードです。
  - [Date]：サマータイム期間は、nonrecurring（毎年実施されない）モードです。
  - [Start]：開始の週、日、月の設定。
  - [End]：終了の週、日、月の設定。

センサー上の時刻の設定

センサー上の時刻を設定するには、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* > [Sensor Setup] > [Time] を選択します。

ステップ 3　[Sensor Local Date] で、ドロップダウン リストから現在の日付を選択します。日付とは、ローカル ホストの日付のことです。

ステップ 4　[Sensor Local Time] で、現在の時刻（hh:mm:ss）を入力します。時刻とは、ローカル ホストの時刻のことです。現在の時刻を表示する場合は、[Refresh] をクリックします。

注意　誤った時刻を指定すると、保存されているイベントに誤ったタイムスタンプが設定されます。この場合は、イベントをクリアする必要があります。

（注）　NTP を設定済みの場合、モジュール上の日付や時刻は変更できません。

ステップ 5　[Standard Time Zone] で、時間帯およびオフセットを設定します。

a. [Zone Name] フィールドのドロップダウン リストから時間帯を選択するか、または作成済みの時間帯を入力します。これは、サマータイム時間が実施されていない場合に表示される時間帯です。

b. [UTC Offset] フィールドに、UTC のオフセットを分単位で入力します。事前に定義された時間帯名を選択した場合、このフィールドには自動的に値が入力されます。

（注）　時間帯のオフセットを変更するには、センサーをリブートする必要があります。

ステップ 6　NTP 時刻同期を使用している場合は、[NTP Server] で次を入力します。

- [IP Address] フィールドに NTP サーバの IP アドレスを入力します。
- 認証された NTP を使用している場合は、[Authenticated NTP] チェックボックスをオンにしてから、[Key] フィールドに NTP サーバのキーを入力し、[Key ID] フィールドに NTP サーバのキー ID を入力します。
- 認証されていない NTP を使用している場合は、[Unauthenticated NTP] チェックボックスをオンにします。

（注）　NTP サーバを定義すれば、センサーの時間はその NTP サーバによって設定されます。CLI で **clock set** コマンドを実行するとエラーが発生しますが、時間帯のパラメータおよびサマータイムのパラメータは有効です。

（注）　センサーの時刻源として NTP サーバを使用する方法を推奨します。

ステップ 7　サマータイムをイネーブルにするには、[Enable Summertime] チェックボックスをオンにします。

ステップ 8　[Configure Summertime] をクリックします。

ステップ 9　ドロップダウン リストから [Summer Zone Name] を選択するか、または作成済みのサマータイム名を入力します。これは、サマータイム時間が実施されている間に表示される時間帯名です。

ステップ 10　[Offset] フィールドに、サマータイム中に付加する時間数を分単位で入力します。事前に定義されたサマータイム時間帯名を選択した場合、このフィールドには自動的に値が入力されます。

（注）　時間帯のオフセットを変更するには、センサーをリブートする必要があります。

ステップ 11　[Start Time] フィールドに、サマータイム設定に適用する時刻を入力します。

ステップ 12　[End Time] フィールドに、サマータイム設定から削除する時刻を入力します。

ステップ 13　[Summertime Duration] で、サマータイム設定が毎年指定された日付に発生する（recurring）か、または指定された日付で開始および終了する（date）かを選択します。

a.　[Recurring]：ドロップダウン リストから開始時刻と終了時刻を選択します。デフォルトは 3 月の第 2 日曜日と 11 月の第 1 日曜日です。

b.　[Date]：ドロップダウン リストから開始時刻と終了時刻を選択します。開始および終了時刻のデフォルトは、1 月 1 日です。

ヒント　変更を破棄して [Configure Summertime] 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 14　[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 15　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。

ステップ 16　時刻と日付の設定を変更した場合（ステップ 3 と 4）、[Apply Time to Sensor] をクリックして、変更した設定をセンサーに保存する必要があります。

時刻源とセンサー

センサーには、信頼できる時刻源が必要です。すべてのイベント（アラート）に、正しい UTC と現地時間のタイムスタンプが必要です。タイムスタンプがないと、攻撃の後でログを正しく分析できません。センサーを初期化するときに、時間帯とサマータイム設定をセットアップします。ここでは、センサーに時刻を設定するためのさまざまな方法を概説します。

（注）　NTP サーバを使用することを推奨します。認証された NTP または認証されていない NTP を使用できます。認証された NTP には、NTP サーバの IP アドレス、キー ID、およびキー値が必要です。NTP は初期化中にセットアップできます。また、CLI、IDM、IME、または ASDM を介して NTP を設定することもできます。

アプライアンス

- **clock set** コマンドを使用して、時刻を設定する。これがデフォルトです。
- アプライアンスは、NTP 同期時刻源から時刻を取得するように設定できます。

IDSM2

- IDSM2 は、自動的にそのクロックをスイッチ時刻と同期させることができる。これがデフォルトです。UTC 時刻は、スイッチと IDSM2 の間で同期が取られます。時間帯とサマータイム設定は、スイッチと IDSM2 の間で同期が取られません。

（注）　スイッチと IDSM2 の両方で時間帯とサマータイム設定が行われていることを確認し、UTC 時刻設定が正しいことを確認します。時間帯やサマータイム設定が IDSM2 とスイッチとで一致していないと、IDSM2 の現地時間が不正確になります。

- IDSM2 は、NTP 同期時刻源から時刻を取得するように設定できます。

AIM IPS および NME IPS

- AIM IPS および NME IPS は、自動的にそのクロックを取り付け先（親ルータ）のルータ シャーシのクロックと同期させることができる。これがデフォルトです。UTC 時刻は、親ルータと AIM IPS および NME IPS の間で同期が取られます。時間帯とサマータイム設定は、親ルータと AIM IPS および NME IPS の間で同期が取られません。

（注）　親ルータと AIM IPS および NME IPS の両方で時間帯とサマータイム設定が行われていることを確認し、UTC 時刻設定が正しいことを確認します。時間帯やサマータイムの設定が AIM IPS および NME IPS とルータとで一致していない場合、AIM IPS および NME IPS の現地時間は不正確になる可能性があります。

- AIM IPS および NME IPS は、時刻を NTP 同期時刻源（親ルータ以外の Cisco ルータなど）から取得するように設定できます。

ASA モジュール

- ASA モジュール（AIP SSM、AIP SSC-5、および IPS SSP）は、自動的にそのクロックを取り付け先の適応型セキュリティ アプライアンスのクロックと同期させることができる。これがデフォルトです。
- ASA モジュールは、時刻を NTP 同期時刻源（親ルータ以外の Cisco ルータなど）から取得するように設定できます。

詳細情報

- IPS モジュールと親シャーシの同期の詳細については、「IPS モジュールのシステム クロックと親デバイスのシステム クロックの同期」（P.6-12）を参照してください。
- NTP の設定の詳細については、「NTP の設定」（P.6-14）を参照してください。

IPS モジュールのシステム クロックと親デバイスのシステム クロックの同期

すべての IPS モジュール（AIM IPS、AIP SSM、AIP SSC-5、IDSM2、IPS SSP、および NME IPS）のシステム クロックは、モジュールの起動時に親シャーシのクロック（スイッチ、ルータ、またはセキュリティ アプライアンス）と同期します。また、親シャーシのクロックが設定された時間に同期します。モジュールのクロックと親シャーシのクロックは、時間の経過とともにずれが生じる傾向があります。誤差は、1 日で数秒になることがあります。この問題を回避するには、モジュールのクロックと親シャーシのクロックの両方が外部 NTP サーバと同期するようにします。モジュールまたは親シャーシのどちらかのクロックだけが NTP サーバと同期している場合、時間のずれが生じます。

センサーが NTP サーバと同期していることを確認する

Cisco IPS では、無効な NTP キー値または ID など、誤った NTP 設定をセンサーに適用することはできません。誤った設定を適用しようとすると、エラー メッセージが表示されます。NTP 設定を確認するには、**show statistics host** コマンドを使用してセンサーの統計情報を収集します。NTP 統計情報セクションには、NTP サーバとセンサーの同期に関するフィードバックを含む NTP 統計情報が表示されます。

NTP 設定を確認するには、次の手順を実行します。

ステップ 1　センサーにログインします。

ステップ 2　ホスト統計情報を生成します。

```
sensor# show statistics host
     ...
     NTP Statistics
             remote           refid      st t when poll reach   delay   offset  jitter
          11.22.33.44     CHU_AUDIO(1)     8 u   36   64    1    0.536    0.069   0.001
          LOCAL(0)        73.78.73.84      5 l   35   64    1    0.000    0.000   0.001
          ind assID status  conf reach auth condition  last_event cnt
            1 10372  f014   yes   yes   ok     reject   reachable  1
            2 10373  9014   yes   yes  none    reject   reachable  1
          status = Not Synchronized
     ...
```

ステップ 3　数分後に再びホスト統計情報を生成します。

```
sensor# show statistics host
     ...
     NTP Statistics
             remote           refid      st t when poll reach   delay   offset  jitter
          *11.22.33.44     CHU_AUDIO(1)     8 u   22   64  377    0.518   37.975  33.465
           LOCAL(0)        73.78.73.84      5 l   22   64  377    0.000    0.000   0.001
          ind assID status  conf reach auth condition  last_event cnt
            1 10372  f624   yes   yes   ok   sys.peer   reachable  2
            2 10373  9024   yes   yes  none    reject   reachable  2
          status = Synchronized
```

ステップ 4　ステータスが [Not Synchronized] のままの場合は、NTP サーバが正しく設定されていることを NTP サーバの管理者に確認してください。

センサーの時刻の修正

イベントには発生時の時刻がスタンプされるため、時刻を誤って設定した場合、保存されたイベントの時刻は不正確になります。イベント ストアのタイムスタンプは、常に UTC 時刻に基づいています。元のセンサーのセットアップ中に、時刻を 8:00 a.m. ではなく 8:00 p.m. に設定した場合、エラーを訂正すると、訂正された時刻がさかのぼって設定されます。そのため、新しいイベントに古いイベントの時刻よりも過去の時刻が記録される場合があります。

たとえば、初期セットアップ中にセンサーを中部時間に設定し、さらにサマータイムを有効にした場合、現地時間が 8:04 p.m. であれば、時刻は 20:04:37 CDT として表示され、UTC からのオフセットは -5 時間になります（翌日の 01:04:37 UTC）。1 週間後の 9:00 a.m. に、21:00:23 CDT と表示された時計を見て誤りに気づいたとします。この場合、時刻を 9:00 a.m. に変更すれば、時計は 09:01:33 CDT と表示されます。UTC からのオフセットは変更されていないため、UTC 時刻は 14:01:33 UTC になります。ここにタイムスタンプの問題が生じる原因があります。

イベント レコードのタイムスタンプの整合性を維持するには、**clear events** コマンドを使用して、古いイベントのイベント アーカイブを消去する必要があります。

（注）　イベントは、個別には削除できません。

詳細情報

イベント ストアからイベントをクリアする手順については、「イベントのクリア」（P.6-18）を参照してください。

NTP の設定

ここでは、Cisco ルータを NTP サーバとして設定する方法、および NTP サーバを時刻源として使用するようにセンサー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。

Cisco ルータを NTP サーバにする設定

センサーが NTP サーバを時刻源として使用するためには、センサーと NTP サーバの間に認証済みの接続が必要です。センサーがキーの暗号化のためにサポートしているのは、MD5 ハッシュ アルゴリズムのみです。Cisco ルータが NTP サーバとして動作するようにし、その内部クロックを時刻源として使用するには、次の手順を使用します。

注意　センサー NTP 機能は、NTP サーバとして動作する Cisco ルータと互換性があるように設計されています。センサーはその他の NTP サーバとともに動作しますが、テストやサポートはされていません。

（注）　NTP サーバのキー ID とキー値を手元に用意してください。NTP サーバを時刻源として使用するようにセンサーを設定する際に、NTP サーバの IP アドレスと共に必要になります。

Cisco ルータが NTP サーバとして動作するように設定するには、次の手順を実行します。

ステップ 1　ルータにログインします。

ステップ 2　コンフィギュレーション モードを開始します。

```
router# configure terminal
```

ステップ 3　キー ID とキー値を作成します。

```
router(config)# ntp authentication-key key_ID md5 key_value
```

キー ID は、1 から 65535 までの数値です。キー値はテキスト（数字または文字）です。この値は後で暗号化されます。

例

```
router(config)# ntp authentication-key 100 md5 attack
```

（注）　センサーがサポートするのは MD5 キーのみです。

（注）　すでにルータにキーが存在する場合もあります。他のキーを確認するには、**show running configuration** コマンドを使用します。これらの値は、信頼できるキーとしてステップ 4 で使用されます。

ステップ 4　ステップ 3 で作成したキーを信頼できるキーとして指定（または既存のキーを使用）します。

```
router(config)# ntp trusted-key key_ID
```

信頼できるキーの ID は、ステップ 3 のキー ID と同じ数値です。

例

```
router(config)# ntp trusted-key 100
```

ステップ 5　センサーが通信するルータ上のインターフェイスを指定します。

```
router(config)# ntp source interface_name
```

例

```
router(config)# ntp source FastEthernet 1/0
```

ステップ 6　センサーに割り当てる NTP マスター ストラタム番号を指定します。

```
router(config)# ntp master stratum_number
```

例

```
router(config)# ntp master 6
```

NTP マスター ストラタム番号は、NTP 階層におけるサーバの相対的な位置を示します。1 から 15 までの番号を選択できます。どの番号を選択するかは、センサーに対して重要ではありません。

センサーで NTP 時刻源を使用するための設定

センサーには、安定した時刻源が必要です。NTP サーバを使用することを推奨します。センサーが NTP サーバを時刻源として使用するように設定するには、次の手順を使用します。認証された NTP または認証されていない NTP を使用できます。

（注）　認証された NTP には、NTP サーバの IP アドレス、キー ID、およびキー値が必要です。

注意　センサー NTP 機能は、NTP サーバとして動作する Cisco ルータと互換性があるように設計されています。センサーはその他の NTP サーバとともに動作しますが、テストやサポートはされていません。

センサーが NTP サーバを時刻源として使用するように設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　コンフィギュレーション モードを開始します。

```
sensor# configure terminal
```

ステップ 3　サービス ホスト モードに入ります。

```
sensor(config)# service host
```

ステップ 4　認証されていない NTP を設定します。

a. NTP コンフィギュレーション モードを開始します。

```
sensor(config-hos)# ntp-option enabled-ntp-unauthenticated
```

b. NTP サーバの IP アドレスを指定します。

```
sensor(config-hos-ena)# ntp-server ip_address
```

c. 認証されていない NTP の設定を確認します。

```
sensor(config-hos-ena)# show settings
   enabled-ntp-unauthenticated
   -----------------------------------------------
      ntp-server: 10.89.147.45
   -----------------------------------------------
sensor(config-hos-ena)#
```

ステップ 5　認証された NTP を設定します。

a. NTP コンフィギュレーション モードを開始します。

```
sensor(config-hos)# ntp-option enable
```

b. NTP サーバの IP アドレスとキー ID を指定します。

```
sensor(config-hos-ena)# ntp-servers ip_address key-id key_ID
```

キー ID は、1 から 65535 までの数値です。これは、NTP サーバで設定済みのキー ID です。

例

```
sensor(config-hos-ena)# ntp-servers 10.16.0.0 key-id 100
```

c. NTP サーバのキー値を指定します。

```
sensor(config-hos-ena)# ntp-keys key_ID md5-key key_value
```

キー値はテキスト（数字または文字）です。これは、NTP サーバで設定済みのキー値です。

例

```
sensor(config-hos-ena)# ntp-keys 100 md5-key attack
```

d. NTP の設定を確認します。

```
sensor(config-hos-ena)# show settings
   enabled
   -----------------------------------------------
      ntp-keys (min: 1, max: 1, current: 1)
      -----------------------------------------------
         key-id: 100
         -----------------------------------------------
            md5-key: attack
```

```
            ------------------------------------------------
          ----------------------------------------------
          ntp-servers (min: 1, max: 1, current: 1)
          ----------------------------------------------
             ip-address: 10.16.0.0
             key-id: 100
          ----------------------------------------------
    ------------------------------------------------
    sensor(config-hos-ena)#
```

ステップ 6　NTP コンフィギュレーション モードを終了します。

```
sensor(config-hos-ena)# exit
sensor(config-hos)# exit
Apply Changes:?[yes]
```

ステップ 7　変更を適用する場合は Enter キーを押し、変更を廃棄する場合は **no** と入力します。

システム クロックの手動設定

（注）　センサーが NTP クロック ソースなど有効な外部の時刻メカニズムと同期している場合、システム クロックを設定する必要はありません。

アプライアンスのクロックを手動で設定するには、**clock set** *hh:mm [:ss] month day year* コマンドを使用します。他の時刻源を使用できない場合は、次のコマンドを使用してください。**clock set** コマンドは、次のプラットフォームには適用されません。

- AIM IPS
- AIP SSC-5
- AIP SSM
- IDSM2
- IPS SSP
- NME IPS

アプライアンスに手動でクロックを設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　クロックを手動で設定します。

```
sensor# clock set 13:21 Mar 29 2008
```

（注）　時刻形式は 24 時間です。

イベントのクリア

イベント ストアをクリアするには、**clear events** コマンドを使用します。

イベント ストアからイベントをクリアするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　イベント ストアをクリアします。

```
sensor# clear events
Warning: Executing this command will remove all events currently stored in the event
store.
Continue with clear? []:
```

ステップ 3　**yes** と入力してイベントをクリアします。

認証およびユーザの設定

ここでは、AAA RADIUS をサポートしているセンサーおよびサポートしていないセンサーのユーザ認証を設定する方法と、ユーザをシステムに追加する方法およびシステムから削除する方法について説明します。内容は次のとおりです。

AAA RADIUS をサポートしていないセンサーの [Authentication] ペイン

（注）　AAA RADIUS をサポートしているのは、IPS 7.0(4)E4 で動作するセンサーだけです。

IME では、一度に複数のユーザがログインできます。ローカル センサーでは、ユーザの作成および削除を行えます。一度に変更できるユーザ アカウントは 1 つだけです。各ユーザは、ユーザが何を変更でき何を変更できないかを制御するロールに関連付けられます。

（注）　ユーザを追加および編集するには、管理者である必要があります。

フィールド定義

[Authentication] ペインには、次のフィールドが表示されます。

- [Username]：ユーザ名は、^[A-Za-z0-9()+:,_/-]+$ の形式で入力します。ユーザ名は、文字または数字で始まり、A ～ Z（大文字または小文字）、0 ～ 9 の数字、「-」および「_」を含み、長さが 1 ～ 64 文字であることが必要です。
- [Role]：ユーザ ロール。値は、Administrator、Operator、Service、および Viewer です。デフォルトは Viewer です。

  （注）　サービス ロールが許可されるのは 1 ユーザだけです。

- [Status]：現在のユーザ アカウントのステータス（active、expired、または locked）を表示します。

AAA RADIUS をサポートしているセンサーの [Authentication] ペイン

（注）　IPS 7.0(4)E4 で動作するセンサーは AAA RADIUS をサポートしています。

[Authentication] ペインを使用して、センサーにログインできるユーザを設定します。一度に複数のユーザがログインできます。ローカル センサーでは、ユーザの作成および削除を行えます。一度に変更できるユーザ アカウントは 1 つだけです。各ユーザは、ユーザが何を変更でき何を変更できないかを制御するロールに関連付けられます。ユーザ パスワードに必要な要件は、[Passwords] ペインで設定します。

ローカル センサーでは、ユーザの作成および削除を行えます。一度に変更できるユーザ アカウントは 1 つだけです。各ユーザは、ユーザが何を変更でき何を変更できないかを制御するロールに関連付けられます。ユーザ パスワードに必要な要件は、**password** コマンドで設定します。

ユーザは、ローカルまたは RADIUS サーバ経由のいずれかで AAA によって認証されます。ローカル認証は、デフォルトでイネーブルになっています。RADIUS 認証は、アクティブにする前に設定する必要があります。

RADIUS によって認証されるユーザ ロールを指定する必要があります。RADIUS サーバでユーザ ロールを設定するか、[Authentication] ペインでデフォルト ユーザ ロールを指定します。ユーザ名およびパスワードは、設定された RADIUS サーバへの認証要求の中に送信されます。サーバは、ログインが認証されるかどうかを決定し、応答します。

（注）　センサーがデフォルト ユーザ ロールを使用するように設定されておらず、センサーのユーザ ロール情報が CiscoSecure ACS サーバの Accept Message にない場合、CiscoSecure ACS サーバがユーザ名とパスワードを受け入れても、センサーは RADIUS 認証を拒否します。

プライマリ RADIUS サーバとセカンダリ RADIUS サーバを設定できます。プライマリ RADIUS サーバが応答しない場合は、セカンダリ RADIUS サーバがユーザを認証および許可します。

いずれの RADIUS サーバも応答しない場合は、センサーがローカル認証（ローカル フォールバック）を使用するように設定できます。この場合、センサーはローカルに設定されたユーザ アカウントに対して認証を行います。センサーは RADIUS サーバが使用できない場合にだけローカル認証を使用します。ユーザの認証要求が RADIUS サーバで拒否された場合、ローカル認証は使用されません。

コンソール ポートを介して接続するユーザを認証する方法を設定することもできます。これには、ローカル ユーザ アカウントを使用する方法、最初に RADIUS を使用（応答しない場合はローカル ユーザ アカウントを使用）する方法、または RADIUS だけを使用する方法があります。ローカル フォールバックをイネーブルにしている場合は、SSH および Telnet セッションが、ローカル アカウントとして認証を試みます。ローカル フォールバックをディセーブルにしている場合、SSH および Telnet セッションは失敗します。

[Authentication] ペインで RADIUS サーバを設定するには、IP アドレス、ポート、および RADIUS サーバの共有秘密が必要です。さらに、RADIUS サーバの NAS-ID か、NAS-ID なしで（または cisco-ips のデフォルト IPS NAS-ID で）クライアントを認証するように設定された RADIUS サーバのいずれかが必要です。

フィールド定義

[Authentication] ペインには、次のフィールドが表示されます。

- [User Authentication]：ローカル認証または RADIUS サーバを使用する認証のいずれかを選択します。
- [Local Authentication]：このセンサーにアクセスするユーザを指定します。
  - [Username]：ユーザのユーザ名。ユーザ名は、^[A-Za-z0-9()+:,_/-]+$ の形式で入力します。ユーザ名は、文字または数字で始まり、A ～ Z（大文字または小文字）、0 ～ 9 の数字、「-」および「_」を含み、長さが 1 ～ 64 文字であることが必要です。
  - [Role]：ユーザのロール。値は、Administrator、Operator、Service、および Viewer です。デフォルトは Viewer です。

    （注） サービス ロールが許可されるのは 1 ユーザだけです。

  - [Status]：現在のユーザ アカウントのステータス（active、expired、または locked）を表示します。
- [RADIUS Authentication]：認証方式に RADIUS を指定します。
  - [Network Access ID]：認証を要求するサービスを識別します。値には、すでに RADIUS サーバで設定されている NAS-ID、cisco-ips、NAS-ID 以外を指定できます。デフォルトは cisco-ips です。
  - [Default User Role]：RADIUS ユーザが引き継ぐセンサー上のデフォルト ユーザ ロールを割り当てます。デフォルト ロールの値は、Administrator、Operator、Viewer、および Unspecified です。サービス ロールはデフォルト ロールになりません。デフォルトは Unspecified です。

    すべての RADIUS ユーザが引き継ぐセンサー上のデフォルト ユーザ ロールを設定しない場合は、ips-role=administrator、ips-role=operator、ips-role=viewer、ips-role=service、または ips-role=unspecified のいずれかのオプションを使用するグループまたはユーザのプロファイルで [Cisco IOS/PIX 6.x RADIUS Attributes] の [[009¥001] cisco-av-pair] を設定する必要があります。

    （注） センサーがデフォルト ユーザ ロールを使用するように設定されておらず、センサーのユーザ ロール情報が CiscoSecure ACS サーバの Accept Message にない場合、CiscoSecure ACS サーバがユーザ名とパスワードを受け入れても、センサーは RADIUS 認証を拒否します。

  - [Allow Local Authentication if all RADIUS Servers are Unresponsive]：このチェックボックスをオンにすると、RADIUS サーバが応答しない場合にローカル認証がデフォルトになります。デフォルトはイネーブルです。

- [Primary RADIUS Server]：メインの RADIUS サーバを設定します。
  - [Server IP Address]：RADIUS サーバの IP アドレス。
  - [Authentication Port]：RADIUS サーバのポート。指定しない場合は、デフォルトの RADIUS ポートが使用されます。
  - [Timeout (seconds)]：RADIUS サーバからの応答がないとセンサーが判断するまで、センサーがサーバからの応答を待機する時間を秒単位で指定します。
  - [Shared Secret]：RADIUS サーバ上で設定される秘密値。RADIUS サーバの秘密値を取得して [Shared Secret] フィールドに入力する必要があります。

    （注）　サーバがクライアントの要求を認証し、クライアントがサーバの応答を認証するには、RADIUS サーバと IPS センサーに同じ秘密値を設定する必要があります。

- [Secondary RADIUS Server (optional)]：セカンダリ RADIUS サーバを設定します（任意）。
  - [Enable a Secondary RADIUS Server]：バックアップ用の RADIUS サーバを設定します。
  - [Server IP Address]：RADIUS サーバの IP アドレス。
  - [Authentication Port]：RADIUS サーバのポート。指定しない場合は、デフォルトの RADIUS ポートが使用されます。
  - [Timeout (seconds)]：RADIUS サーバからの応答がないとセンサーが判断するまで、センサーがサーバからの応答を待機する時間を秒単位で指定します。
  - [Shared Secret]：RADIUS サーバ上で設定される秘密値。RADIUS サーバの秘密値を取得して [Shared Secret] フィールドに入力する必要があります。

    （注）　サーバがクライアントの要求を認証し、クライアントがサーバの応答を認証するには、RADIUS サーバと IPS センサーに同じ秘密値を設定する必要があります。

- [Console Authentication]：コンソール ポートを介して接続するユーザを認証する方法を選択します。
  - [Local]：コンソール ポートを介して接続するユーザは、ローカル ユーザ アカウントを使用して認証されます。
  - [Local and RADIUS]：コンソール ポートを介して接続するユーザは、最初に RADIUS を使用して認証されます。RADIUS が失敗した場合は、ローカル認証が試行されます。これがデフォルトです。
  - [RADIUS]：コンソール ポートを介して接続するユーザは、RADIUS によって認証されます。[Allow Local Authentication if all Radius Servers are Unresponsive] をイネーブルにしている場合、ユーザはローカル ユーザ アカウントによって認証されます。

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

[Add User] および [Edit User] ダイアログボックスには、次のフィールドが表示されます。

- [Username]：ユーザ名。ユーザ名は、^[A-Za-z0-9()+:,_/-]+$ の形式で入力します。ユーザ名は、文字または数字で始まり、A ～ Z（大文字または小文字）、0 ～ 9 の数字、「-」および「_」を含み、長さが 1 ～ 64 文字であることが必要です。
- [User Role]：ユーザ ロール。有効な値は、Administrator、Operator、Service、および Viewer です。デフォルトは Viewer です。

（注）　サービス ロールが許可されるのは 1 ユーザだけです。

- [Password]：ユーザのパスワード。パスワードは、センサー管理者が設定した要件に従っている必要があります。
- [Confirm Password]：確認のためにパスワードを再入力します。確認のために再入力したパスワードがユーザ パスワードと一致しない場合は、エラー メッセージが表示されます。
- [Change the password to access the sensor]：ユーザのパスワードを変更します。これは [Edit User] ダイアログボックスでのみ利用できます。

ユーザ ロールについて

ユーザ ロールには、次の 4 つがあります。

- ビューア（Viewer）：設定およびイベントを表示できますが、自分のユーザ パスワード以外の設定データは修正できません。
- オペレータ（Operator）：すべてのデータを表示できるほか、次のオプションを修正できます。
  - シグニチャ チューニング（優先順位、無効 / 有効）
  - 仮想センサーの定義
  - 管理対象ルータ
  - 自分のユーザ パスワード
- 管理者（Administrator）：すべてのデータを表示できるほか、オペレータが修正できるすべてのオプションに加えて、次のオプションを修正できます。
  - センサーのアドレス設定
  - 設定エージェントまたはビュー エージェントとして接続が許可されたホストのリスト
  - 物理的な検知インターフェイスの割り当て。
  - 物理インターフェイスの制御のイネーブル化またはディセーブル化。
  - ユーザとパスワードの追加および削除。
  - 新しい SSH ホスト キーとサーバ証明書の生成
- サービス（Service）：サービス権限を持つユーザはセンサーに 1 人だけ存在できます。サービス ユーザは、IDM または IMEIME にログインできません。サービス ユーザは、CLI ではなく bash シェルにログインします。

（注）　サービス ロールは、必要に応じて CLI をバイパスできる特殊なロールです。許可されるサービス アカウントは 1 つだけです。トラブルシューティング用には、サービス ロールのアカウントのみを作成してください。管理者権限を持つユーザだけが、サービス アカウントを編集できます。

サービス アカウントにログインすると、次の警告が表示されます。

```
************************ WARNING ****************************************************
UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
This account is intended to be used for support and troubleshooting purposes only.
Unauthorized modifications are not supported and will require this device to be
re-imaged to guarantee proper operation.
*******************************************************************************
```

注意　サービス アカウントを作成するかどうかは、慎重に検討する必要があります。サービス アカウントは、システムへのシェル アクセスを提供するため、システムが脆弱になります。ただし、管理者のパスワードが失われた場合は、サービス アカウントを使用してパスワードを作成できます。状況を分析して、システムにサービス アカウントを存在させるかどうかを決定してください。

サービス アカウントについて

トラブルシューティングの際に使用する TAC 用のサービス アカウントを作成できます。センサーには複数のユーザがアクセスできますが、センサーに対するサービス権限を持てるのは 1 人のユーザだけです。サービス アカウントは、サポートの目的のためにのみ使用します。

サービス アカウントが作成されると、root ユーザのパスワードはサービス アカウントのパスワードに同期化されます。root でアクセスするには、サービス アカウントでログインしてから **su - root** コマンドを使用してユーザ root に切り替える必要があります。

注意　TAC の指示に基づく場合を除き、サービス アカウントを使用してセンサーに変更を加えないでください。サービス アカウントを使用してセンサーを設定すると、その設定は TAC のサポート対象外になります。サービス アカウントを使用してオペレーティング システムにサービスを追加すると、他の IPS サービスの特定のパフォーマンスと機能に影響を及ぼします。TAC は、追加のサービスが加えられたセンサーをサポートしません。

注意　サービス アカウントを作成するかどうかは、慎重に検討する必要があります。サービス アカウントは、システムへのシェル アクセスを提供するため、システムが脆弱になります。ただし、管理者のパスワードが失われた場合は、サービス アカウントを使用してパスワードを作成できます。状況を分析して、システムにサービス アカウントを存在させるかどうかを決定してください。

サービス アカウントおよび RADIUS 認証

RADIUS 認証を使用し、サービス アカウントを作成および使用する場合は、センサー上と RADIUS サーバ上の両方にサービス アカウントを作成する必要があります。

センサー上のサービス アカウントにアクセスするには、ローカル認証を使用する必要があります。サービス アカウントは、ローカル アカウントとしてセンサー上に手動で作成する必要があります。その後、続けて RADIUS 認証を設定したら、ip-role=service に受諾メッセージを設定した RADIUS サーバ上でサービス アカウントを手動で設定する必要があります。

サービス アカウントにログインすると、センサーのアカウントと RADIUS サーバのアカウントの両方に対して認証されます。サービス アカウントには、シリアル コンソール ポートからアクセスするか、モニタおよびキーボード（センサーがサポートしている場合）から直接アクセスするか、または SSH や Telnet などのネットワーク接続からアクセスできますが、ログインにはローカル認証を使用する必要があります。

ユーザの追加、編集、削除と、AAA RADIUS をサポートしていないセンサーのアカウント作成

センサー上のユーザを設定するには、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* > [Sensor Setup] > [Authentication] を選択し、[Add] をクリックしてユーザを追加します。

ステップ 3　[Username] フィールドに、追加するユーザのユーザ名を入力します。

ステップ 4　[User Role] フィールドのドロップダウン リストから、次のいずれかのユーザ ロールを選択します。

- 管理者（Administrator）
- オペレータ（Operator）
- ビューア（Viewer）
- サービス（Service）

（注）　サービス ロールが許可されるのは 1 ユーザだけです。

ステップ 5　[Password] フィールドに、そのユーザの新しいパスワードを入力します。

ステップ 6　[Confirm Password] フィールドに、そのユーザの新しいパスワードを入力します。

ヒント　変更を破棄して [Add User] 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。新しいユーザが、[Users] ペインのユーザ リストに表示されます。

ステップ 8　ユーザを編集するには、ユーザ リストにあるユーザを選択し、[Edit] をクリックします。

ステップ 9　[Username] フィールド、[User Role] フィールド、および [Password] フィールドで、必要な変更を行います。

ヒント　変更を破棄して [Edit User] 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 10　[OK] をクリックします。編集されたユーザが、[Users] ペインのユーザ リストに表示されます。

ステップ 11　ユーザを削除するには、ユーザ リストにあるユーザを選択し、[Delete] をクリックします。削除されたユーザは、[Users] ペインのユーザ 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 12　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。

ユーザの追加、編集、削除と、AAA RADIUS をサポートしているセンサーのアカウント作成

注意　センサー上で RADIUS 認証を設定する前に、RADIUS サーバがすでに設定されていることを確認してください。IPS 7.0(4) は、CiscoSecure ACS 4.2 サーバでテスト済みです。RADIUS サーバのセットアップ方法については、RADIUS サーバのマニュアルを参照してください。

（注）　センサー上で RADIUS 認証をイネーブルにしても、すでに確立している接続は切断されません。RADIUS 認証は、センサーに新しく接続するときだけ必要になります。既存の CLI、IDM、および IME では、RADIUS 認証の設定に先立ってログイン クレデンシャルによる接続が確立しています。これらの接続を切断するには、RADIUS の設定後にセンサーをリセットする必要があります。

センサー上のユーザを設定するには、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* > [Sensor Setup] > [Authentication] を選択します。

ステップ 3　[User Authentication] の横にある [Local] または [RADIUS Server] オプション ボタンをクリックして、ユーザ認証のタイプを選択します。

ステップ 4　ローカル認証を設定するには、[Add] をクリックします。

ステップ 5　[Username] フィールドに、追加するユーザのユーザ名を入力します。

ステップ 6　[User Role] フィールドのドロップダウン リストから、次のいずれかのユーザ ロールを選択します。

- 管理者（Administrator）
- オペレータ（Operator）
- ビューア（Viewer）
- サービス（Service）

（注）　サービス ロールが許可されるのは 1 ユーザだけです。

ステップ 7　[Password] フィールドに、そのユーザの新しいパスワードを入力します。

ステップ 8　[Confirm Password] フィールドに、そのユーザの新しいパスワードを入力します。

ヒント 変更を破棄して [Add User] 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。新しいユーザが、[Authentication] ペインのユーザ リストに表示されます。

ステップ 10　ユーザを編集するには、ユーザ リストにあるユーザを選択し、[Edit] をクリックします。

ステップ 11　[Username] フィールド、[User Role] フィールド、および [Password] フィールドで、必要な変更を行います。

ヒント 変更を破棄して [Edit User] 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 12　[OK] をクリックします。編集されたユーザが、[Authentication] ペインのユーザ リストに表示されます。

ステップ 13　ユーザを削除するには、ユーザ リストにあるユーザを選択し、[Delete] をクリックします。削除されたユーザは、[Authentication] ペインのユーザ リストに表示されなくなります。

ステップ 14　RADIUS 認証を設定するには、

a. [Network Access ID] フィールドに、NAS-ID を入力します。

NAS-ID は、認証しようとしているサービスのタイプをサーバに伝えるためにクライアントが送信する ID です。値には、すでに RADIUS サーバで設定されている NAS-ID、cisco-ips、NAS-ID 以外を指定できます。デフォルトは cisco-ips です。

b. デフォルト ユーザ ロールを設定します。[Default User Role] ドロップダウン メニューから、このユーザのユーザ ロールを選択します。センサー上にデフォルト ユーザ ロールが割り当てられます。これは、すべての RADIUS ユーザが引き継ぎます。値は、Administrator、Operator、Viewer、または Unspecified です。デフォルトは Unspecified です。

（注） サービスはデフォルト ロールになりません。

すべての RADIUS ユーザが引き継ぐセンサー上のデフォルト ユーザ ロールを設定しない場合は、次のいずれかのオプションを使用するグループまたはユーザのプロファイルで [Cisco IOS/PIX 6.x RADIUS Attributes] の [[009¥001] cisco-av-pair] を設定する必要があります。

- ips-role=viewer
- ips-role=operator
- ips-role=administrator
- ips-role=service
- ips-role=unspecified

（注） センサーがデフォルト ユーザ ロールを使用するように設定されておらず、センサーのユーザ ロール情報が CiscoSecure ACS サーバの Accept Message にない場合、CiscoSecure ACS サーバがユーザ名とパスワードを受け入れても、センサーは RADIUS 認証を拒否します。

c. RADIUS サーバが応答不能になった場合にローカル認証に切り替えるには、[Allow Local Authentication if all RADIUS Servers are Unresponsive] チェックボックスをオンにします。

d. [Server IP Address] フィールドに RADIUS サーバの IP アドレスを入力します。

e. [Authentication port] フィールドに RADIUS サーバのポートを入力します。

f. [Timeout (seconds)] フィールドに、RADIUS サーバからの応答を待機する時間を秒単位で入力します。

g. [Shared Secret] フィールドに、RADIUS サーバから取得した秘密値を入力します。共有秘密とは、セキュアな通信に参加するパーティにだけ知らされる小さなデータのことです。

（注） サーバがクライアントの要求を認証し、クライアントがサーバの応答を認証するには、RADIUS サーバと IPS センサーに同じ秘密値を設定する必要があります。

h. （任意）プライマリ RADIUS サーバが応答しない場合にセカンダリ RADIUS サーバをイネーブルにして認証を実行させるには、[Enable a Secondary RADIUS Server] チェックボックスをオンにします。

i. [Server IP Address] フィールドに、セカンダリ RADIUS サーバの IP アドレスを入力します。

j. [Authentication Port] フィールドに RADIUS サーバのポートを入力します。

k. [Timeout (seconds)] フィールドに、RADIUS サーバからの応答を待機する時間を秒単位で入力します。

l. [Shared Secret] フィールドに、この RADIUS サーバのために取得した秘密値を入力します。

m. [Console Authentication] ドロップダウン リストから、コンソール認証のタイプを選択します。[Local]、[Local and RADIUS]、または [RADIUS] が選択できます。

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 15 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。

ユーザ アカウントのロック解除

（注） アカウント ロックを設定すると、ローカル認証だけでなく RADIUS 認証も影響を受けます。ローカルなログインまたは RADIUS アカウントへのログイン失敗が指定された試行回数に達すると、アカウントはセンサー上でローカルにロックされます。ローカル アカウントの場合は、パスワードをリセットするか、**unlock user** *username* コマンドを使用してアカウントのロックを解除します。RADIUS ユーザ アカウントの場合は、**unlock user** *username* コマンドを使用してアカウントのロックを解除する必要があります。

グローバル コンフィギュレーション モードで **unlock user** *username* コマンドを使用し、ログイン失敗が指定された試行回数に達してロックアウトされたユーザのアカウントのロックを解除します。

（注） **unlock** コマンドは IPS 7.0(4)E4 以降だけでサポートされています。これよりも前のバージョンの IPS ソフトウェアでは動作しません。

アカウントのロック解除を設定するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して次のようにセンサーにログインします。

ステップ 2　ロックされたアカウントを持つユーザを確認します。

```
sensor# show users all
    CLI ID   User       Privilege
*   1349     cisco      administrator
    5824     (jsmith)   viewer
    9802     tester     operator
```

jsmith というユーザ名がカッコで囲まれています。これはアカウントがロックされていることを示します。

ステップ 3　グローバル コンフィギュレーション モードを開始します。

```
sensor# configure terminal
sensor(config)#
```

ステップ 4　アカウントのロックを解除します。

```
sensor(config)# unlock user jsmith
```

ステップ 5　新しい設定を確認します。

```
sensor# show users all
    CLI ID   User       Privilege
*   1349     cisco      administrator
    5824     jsmith     viewer
    9802     tester     operator
```

ユーザ名 jsmith を囲んでいたカッコが外れています。これはアカウントのロックが解除されたことを示します。

CHAPTER 7

インターフェイスの設定

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

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

この章では、さまざまなインターフェイス モードとセンサーでのインターフェイスの設定方法について説明します。内容は次のとおりです。

センサーのインターフェイス

ここでは、センサー インターフェイスについて説明します。内容は次のとおりです。

インターフェイスについて

センサーのインターフェイスは、インターフェイスの最大速度および物理的な場所に従って名前が付けられています。物理的な場所は、ポート番号とスロット番号で構成されています。センサーのマザーボードに組み込まれたインターフェイスはすべてスロット 0 にあります。また、インターフェイス カード拡張スロットには、最下部スロットをスロット 1 として、下から上に向かって番号が付けられます（ポートの上から下に番号を付ける IPS 4270-20 は例外です）。特定のスロットを持つインターフェイスには、右のポートをポート 0 として、右から左に向かって大きくなるように番号が付けられます。たとえば、GigabitEthernet2/1 は、1 ギガビットの最大速度をサポートし、下から 2 番めの拡張スロットの右から 2 番めのインターフェイスです。IPS 4240、IPS 4255、IPS 4260、および IPS 4270-20 は、このルールの例外です。これらのセンサー上のコマンド/コントロール インターフェイスは、GigabitEthernet0/0 ではなく Management0/0 と呼ばれます。IPS 4270-20 には、Management0/1 と呼ばれる追加インターフェイスがあります。これは将来用に予約されています。

インターフェイスには、次の 3 つのロールがあります。

- コマンド/コントロール
- 検知
- 代替 TCP リセット

特定のインターフェイスに割り当てることができるロールには制約があります。また、複数のロールを担うインターフェイスもあります。検知インターフェイスを、他の検知インターフェイスに対する TCP リセット インターフェイスとして設定できます。TCP リセット インターフェイスは、同時に IDS（無差別）検知インターフェイスとしても機能します。次の制約事項が適用されます。

- AIM IPS、AIP SSC-5、AIP SSM、IPS SSP、および NME IPS には 1 つの検知インターフェイスしかないため、代替 TCP リセット インターフェイスを設定できません。
- Catalyst スイッチのハードウェアの制約により、どちらの IDSM2 検知インターフェイスも、System0/1 を TCP リセット インターフェイスとして使用するように永続的に設定されます。
- インライン インターフェイス モードまたはインライン VLAN ペア モードでは、TCP リセットは常に検知インターフェイス上で送信されるため、検知インターフェイスに割り当てられた TCP リセット インターフェイスは、これらのモードでは影響を与えません。

（注）　各物理インターフェイスは、VLAN グループ サブインターフェイスに分けることができます。各サブインターフェイスは、そのインターフェイスの VLAN のグループで構成されます。

コマンド/コントロール インターフェイス

コマンド/コントロール インターフェイスは、IP アドレスを持ち、センサーの設定に使用されます。このインターフェイスは、センサーからセキュリティ イベントとステータス イベントを受信し、センサーに統計情報を問い合わせます。

コマンド/コントロール インターフェイスは、常にイネーブルです。このインターフェイスは特定の物理インターフェイス（センサーのモデルによって異なる）に常時マッピングされています。コマンド/コントロール インターフェイスを検知インターフェイスや代替 TCP リセット インターフェイスとして使用することはできません。

表 7-1 に、各センサーのコマンド/コントロール インターフェイスを示します。

表 7-1　コマンド/コントロール インターフェイス

センサー	コマンド/コントロール インターフェイス
AIM IPS	Management0/0
AIP SSC	Management0/0
AIP SSM-10	GigabitEthernet0/0
AIP SSM-20	GigabitEthernet0/0
AIP SSM-40	GigabitEthernet0/0
IDSM2	GigabitEthernet0/2
IPS 4240	Management0/0
IPS 4255	Management0/0
IPS 4260	Management0/0
IPS 4270-20	Management0/0
IPS SSP-10	Management0/0
IPS SSP-20	Management0/0
IPS SSP-40	Management0/0
IPS SSP-60	Management0/0
NME IPS	Management0/1

センシング インターフェイス

検知インターフェイスは、セキュリティ違反に関してトラフィックを分析するために、センサーによって使用されます。センサーには、1 つ以上の検知インターフェイスがあり、その数はセンサーによって異なります。検知インターフェイスは、無差別モードで個別に動作させるか、またはペアにしてインライン インターフェイスを作成できます。

（注） アプライアンスでは、すべての検知インターフェイスがデフォルトでディセーブルになっています。これらのインターフェイスを使用するには、イネーブルにする必要があります。モジュールでは、検知インターフェイスは常にイネーブルです。

センサーに検知インターフェイスを追加するオプションのインターフェイス カードをサポートするアプライアンスもあります。これらのオプションのカードは、センサーの電源がオフのときに着脱する必要があります。センサーは、サポートされているインターフェイス カードの着脱を検出します。オプションのインターフェイス カードを取り外すと、速度、デュプレックス、記述文字列、インターフェイスのイネーブル/ディセーブル状態、インライン インターフェイス ペアの組み合わせなど、インターフェイスの設定の一部が削除されます。これらの設定は、カードを再挿入すると、デフォルト設定に復元されます。無差別およびインライン インターフェイスの分析エンジンへの割り当ては分析エンジンの設定から削除されませんが、これらのカードが再挿入され、もう一度インライン インターフェイスのペアを作成するまで無視されます。

詳細情報

- 各センサーで使用できる検知インターフェイスの数とタイプについては、「インターフェイス サポート」（P.7-4）を参照してください。
- インターフェイス モードの詳細については、「インターフェイス モードについて」（P.7-13）を参照してください。
- 仮想センサーの設定手順については、「仮想センサーの追加、編集、削除」（P.8-13）を参照してください。

インターフェイス サポート

表 7-2 では、Cisco IPS を実行するアプライアンスおよびモジュールのインターフェイス サポートについて説明します。

表 7-2　インターフェイス サポート

ベース シャーシ	追加されたインターフェイス カード	インライン VLAN ペア（検知ポート）をサポートするインターフェイス	インライン インターフェイス ペアをサポートする組み合わせ	インラインをサポートしないインターフェイス（指示制御ポート）
AIM IPS	—	VLAN ペアまたはインライン インターフェイス ペアではなく、ルータ設定の **ids-service-module** コマンドによる GigabitEthernet0/1	VLAN ペアまたはインライン インターフェイス ペアではなく、ルータ設定の **ids-service-module** コマンドによる GigabitEthernet0/1	Management0/0
AIP SSC-5	—	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる GigabitEthernet0/0	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる GigabitEthernet0/1	Management0/0
AIP SSM-10	—	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる GigabitEthernet0/1	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる GigabitEthernet0/1	GigabitEthernet0/0
AIP SSM-20	—	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる GigabitEthernet0/1	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる GigabitEthernet0/1	GigabitEthernet0/0
AIP SSM-40	—	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる GigabitEthernet0/1	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる GigabitEthernet0/1	GigabitEthernet0/0
IDSM2	—	GigabitEthernet0/7 GigabitEthernet0/8	0/7<->0/8	GigabitEthernet0/2

表 7-2　インターフェイス サポート（続き）

ベース シャーシ	追加されたインターフェイス カード	インライン VLAN ペア（検知ポート）をサポートするインターフェイス	インライン インターフェイス ペアをサポートする組み合わせ	インラインをサポートしないインターフェイス（指示制御ポート）
IPS 4240	—	GigabitEthernet0/0 GigabitEthernet0/1 GigabitEthernet0/2 GigabitEthernet0/3	0/0<->0/1 0/0<->0/2 0/0<->0/3 0/1<->0/2 0/1<->0/3 0/2<->0/3	Management0/0
IPS 4255	—	GigabitEthernet0/0 GigabitEthernet0/1 GigabitEthernet0/2 GigabitEthernet0/3	0/0<->0/1 0/0<->0/2 0/0<->0/3 0/1<->0/2 0/1<->0/3 0/2<->0/3	Management0/0
IPS 4260	—	GigabitEthernet0/1	該当なし	Management0/0
IPS 4260	4GE-BP スロット 1 スロット 2	GigabitEthernet0/1 GigabitEthernet2/0 GigabitEthernet2/1 GigabitEthernet2/2 GigabitEthernet2/3 GigabitEthernet3/0 GigabitEthernet3/1 GigabitEthernet3/2 GigabitEthernet3/3	 2/0<->2/1[1] 2/2<->2/3 3/0<->3/1 3/2<->3/3	Management0/0
IPS 4260	2SX スロット 1 スロット 2	GigabitEthernet0/1 GigabitEthernet2/0 GigabitEthernet2/1 GigabitEthernet3/0 GigabitEthernet3/1	すべての検知ポートをまとめてペアにすることが可能	Management0/0
IPS 4260	10GE スロット 1	GigabitEthernet0/1 TenGigabitEthernet2/0 TenGigabitEthernet2/1	 2/0<->2/1[2]	Management0/0
IPS 4270-20	—	—	該当なし	Management0/0 Management0/1[3]

表 7-2　インターフェイス サポート（続き）

ベース シャーシ	追加されたインターフェイス カード	インライン VLAN ペア（検知ポート）をサポートするインターフェイス	インライン インターフェイス ペアをサポートする組み合わせ	インラインをサポートしないインターフェイス（指示制御ポート）
IPS 4270-20	4GE-BP スロット 1 スロット 2	 GigabitEthernet3/0 GigabitEthernet3/1 GigabitEthernet3/2 GigabitEthernet3/3 GigabitEthernet4/0 GigabitEthernet4/1 GigabitEthernet4/2 GigabitEthernet4/3	 3/0<->3/1[4] 3/2<->3/3 4/0<->4/1 4/2<->4/3	Management0/0 Management0/1[5]
IPS 4270-20	2SX スロット 1 スロット 2	 GigabitEthernet3/0 GigabitEthernet3/1 GigabitEthernet4/0 GigabitEthernet4/1	すべての検知ポートをまとめてペアにすることが可能	Management0/0 Management0/1[6]
IPS 4270-20	10GE スロット 1 スロット 2	 TenGigabitEthernet5/0 TenGigabitEthernet5/1 TenGigabitEthernet7/0 TenGigabitEthernet7/1	すべての検知ポートをまとめてペアにすることが可能	Management0/0 Management0/1[7]
IPS SSP-10	—	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる PortChannel0/0	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる PortChannel0/0	Management0/0
IPS SSP-20	—	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる PortChannel0/0	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる PortChannel0/0	Management0/0
IPS SSP-40	—	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる PortChannel0/0	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる PortChannel0/0	Management0/0

表 7-2　インターフェイス サポート（続き）

ベース シャーシ	追加されたインターフェイス カード	インライン VLAN ペア（検知ポート）をサポートするインターフェイス	インライン インターフェイス ペアをサポートする組み合わせ	インラインをサポートしないインターフェイス（指示制御ポート）
IPS SSP-60	—	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる PortChannel0/0	VLAN ペアまたはインライン インターフェイス ペアではなく、セキュリティ コンテキストによる PortChannel0/0	Management0/0
NME IPS	—	VLAN ペアまたはインライン インターフェイス ペアではなく、ルータ設定の **ids-service-module** コマンドによる GigabitEthernet0/1	VLAN ペアまたはインライン インターフェイス ペアではなく、ルータ設定の **ids-service-module** コマンドによる GigabitEthernet0/1	Management0/1

1. ハードウェア バイパスをディセーブルにするには、他の組み合わせでインターフェイスのペアを作成します（2/0<->2/2、2/1<->2/3 など）。
2. ハードウェア バイパスをディセーブルにするには、他の組み合わせでインターフェイスのペアを作成します（2/0<->2/2、2/1<->2/3 など）。
3. 今後使用するために予約されています。
4. ハードウェア バイパスをディセーブルにするには、他の組み合わせでインターフェイスのペアを作成します（2/0<->2/2、2/1<->2/3 など）。
5. 今後使用するために予約されています。
6. 今後使用するために予約されています。
7. 今後使用するために予約されています。

（注）　IPS 4260 は、4GE-BP、2SX、および 10GE カードの組み合わせをサポートします。また、IPS 4270-20 では、4GE-BP、2SX、および 10GE カードを 6 枚まで、または合計 16 ポートになるまで（どちらか早く達した方）組み合わせることができますが、10GE カードは 2 枚までに制限されています。

TCP リセット インターフェイス

ここでは、TCP リセット インターフェイスとこれらを使用する必要がある場合について説明します。内容は次のとおりです。

代替 TCP リセット インターフェイスについて

攻撃者のホストと攻撃のターゲット ホストとの間のネットワーク接続をリセットするために、TCP リセット パケットを送信するようにセンサーを設定できます。一部のインストールでは、インターフェイスが無差別モードで動作している場合、攻撃が検出された検知インターフェイスと同じインターフェイスでセンサーが TCP リセット パケットを送信できないことがあります。このような場合は、検知イ

ンターフェイスを代替 TCP リセット インターフェイスに関連付けることができます。これにより、無差別モードで動作している場合に通常は検知インターフェイスで送信されるすべての TCP リセットを、関連付けた代替 TCP リセット インターフェイスで送信できます。

検知インターフェイスが代替 TCP リセット インターフェイスと関連付けられている場合、その関連付けは、センサーが無差別モードに設定されているときは適用されますが、検知インターフェイスがインライン モードに設定されている場合は無視されます。IDSM2 を除いて、すべての検知インターフェイスは、別の検知インターフェイスの代替 TCP リセット インターフェイスとなることができます。IDSM2 の代替 TCP リセット インターフェイスは、ハードウェアの制限があるために固定されています。

表 7-3 に代替 TCP リセット インターフェイスを示します。

（注） IPS モジュール上の検知インターフェイスは 1 つだけです（AIM IPS、AIP SSC-5、AIP SSM、IPS SSP、および NME IPS）。

表 7-3　代替 TCP リセット インターフェイス

センサー	代替 TCP リセット インターフェイス
AIM IPS	なし
AIP SSC-5	なし
AIP SSM-10	なし
AIP SSM-20	なし
AIP SSM-40	なし
IDSM2	System0/1[1]
IPS 4240	任意の検知インターフェイス
IPS 4255	任意の検知インターフェイス
IPS 4260	任意の検知インターフェイス
IPS 4270-20	任意の検知インターフェイス
IPS SSP-10	なし
IPS SSP-20	なし
IPS SSP-40	なし
IPS SSP-60	なし
NME IPS	なし

1. これは、Catalyst バックプレーン上の内部インターフェイスです。

代替 TCP リセット インターフェイスの指定

次の場合、代替 TCP リセット インターフェイスを指定する必要があります。

- スイッチが SPAN または VACL キャプチャでモニタされていて、スイッチがその SPAN または VACL ポートで着信パケットを受け入れない場合。
- 複数の VLAN でスイッチが SPAN または VACL キャプチャでモニタされていて、スイッチが 802.1q ヘッダー付きの着信パケットを受け入れない場合。

（注）　TCP リセットでは、リセットを送信する VLAN を判断するために 802.1q ヘッダーが必要です。

- 接続のモニタにネットワーク タップが使用されている場合。

（注）　タップは、センサーからの着信トラフィックを許可しません。

検知インターフェイスだけを代替 TCP リセット インターフェイスとして割り当てることができます。管理インターフェイスを代替 TCP リセット インターフェイスとして設定することはできません。

インターフェイス設定の制約事項

センサーでのインターフェイスの設定に適用される制約は次のとおりです。

- 物理インターフェイス
  - モジュール（AIM IPS、AIP SSC-5、AIP SSM、IDSM2、IPS SSP、およびNME IPS）上で、すべてのバックプレーン インターフェイスの速度、デュプレックス、および状態設定は固定されます。これらの設定は、すべてのバックプレーン インターフェイスのデフォルト設定で保護されます。
  - バックプレーン以外の FastEthernet インターフェイスでは、有効な速度設定は、10 Mbps、100 Mbps、および自動です。有効なデュプレックス設定は、全、半、および自動です。
  - ギガビットの銅インターフェイス（IPS 4240、IPS 4255、IPS 4260、および IPS 4270-20 上の 1000-TX）の場合、有効な速度設定は、10 Mbps、100 Mbps、1000 Mbps、および自動です。有効なデュプレックス設定は、全、半、および自動です。
  - ギガビット（銅またはファイバ）インターフェイスの場合、速度は 1000 Mbps に設定されている場合、有効なデュプレックス設定は自動だけです。
  - コマンド/コントロール インターフェイスを検知インターフェイスとして機能させることはできません。
- インライン インターフェイス ペア
  - インライン インターフェイス ペアには、物理インターフェイスのタイプ（銅またはファイバ）、インターフェイスの速度やデュプレックス設定に関係なく、任意の検知インターフェイスの組み合わせを含めることができます。ただし、異なるメディア タイプ、速度、デュプレックス設定のインターフェイスの組み合わせは十分にテストまたはサポートされていない場合があります。
  - コマンド/コントロール インターフェイスを、インライン インターフェイス ペアのメンバにすることはできません。
  - インライン インターフェイス ペアで物理インターフェイスをそれ自身とペアにすることはできません。
  - 物理インターフェイスは、1 つのインライン インターフェイス ペアのみのメンバにすることができます。
  - バイパス モードだけを設定でき、インライン モードをサポートするセンサー プラットフォームでのみインライン インターフェイス ペアを作成できます。
  - 物理インターフェイスのサブインターフェイス モードが **none** に設定されていない限り、物理インターフェイスをインライン インターフェイス ペアのメンバにすることはできません。

- インライン VLAN ペア
  - VLAN をそれ自身とペアにすることはできません。
  - インライン VLAN ペアでペアになっている VLAN のいずれかとして、デフォルト VLAN を使用することはできません。
  - 特定の検知インターフェイスについて、VLAN を 1 つのインライン VLAN ペアだけのメンバにすることができます。ただし、その VLAN は、複数の検知インターフェイスで 1 つのインライン VLAN ペアのメンバにできます。
  - インライン VLAN ペアで VLAN を指定する順序は重要ではありません。
  - インライン VLAN ペア モードの検知インターフェイスは、1 ～ 255 のインライン VLAN ペアを持つことができます。
- 代替 TCP リセット インターフェイス
  - 代替 TCP リセット インターフェイスは、検知インターフェイスにのみ割り当てることができます。コマンド/コントロール インターフェイスを代替 TCP リセット インターフェイスとして設定することはできません。代替 TCP リセット インターフェイス オプションはデフォルトで **none** に設定され、検知インターフェイス以外のすべてのインターフェイスに対して保護されています。
  - 複数の検知インターフェイスに対して同じ物理インターフェイスを代替 TCP リセット インターフェイスとして割り当てることができます。
  - 物理インターフェイスは、検知インターフェイスと代替 TCP リセット インターフェイスのどちらとしても機能します。
  - コマンド/コントロール インターフェイスを、検知インターフェイスの代替 TCP リセット インターフェイスとして機能させることはできません。
  - 検知インターフェイスを、自身の代替 TCP リセット インターフェイスとして機能させることはできません。
  - 代替 TCP リセット インターフェイスとして TCP リセット可能なインターフェイスのみを設定できます。

  （注） この制約の例外は IDSM2 です。両方の検知インターフェイスの代替 TCP リセット インターフェイス割り当ては System0/1（保護）です。

- VLAN グループ
  - 無差別モード、インライン インターフェイス ペア モード、またはインライン VLAN ペア モードに 1 つのインターフェイスを設定できますが、これらのモードを組み合わせることはできません。
  - 各インターフェイスの複数のグループに 1 つの VLAN を追加することはできません。
  - 複数の仮想センサーに 1 つの VLAN グループを追加することはできません。
  - 1 つのインターフェイスに追加できるユーザ定義 VLAN グループは最大 255 です。
  - 物理インターフェイスをペアにする場合、インターフェイスを分割することはできません。ペアは分割できます。
  - 複数のインターフェイスで 1 つの VLAN を使用できますが、この構成に対して警告を受け取ります。
  - 分割されているかどうかに関係なく、1 つ以上の物理インターフェイスとインライン VLAN ペアの任意の組み合わせに仮想センサーを割り当てることができます。
  - 物理インターフェイスと論理インターフェイスの両方を VLAN グループに分割できます。

- CLI、IDM、および IME は、ダングリング参照を削除するように求めます。ダングリング参照をそのままにして、設定の編集を続けることができます。
- CLI、IDM、および IME では、分析エンジンでインターフェイス設定と競合する設定変更を行うことはできません。
- CLI では、分析エンジン設定で競合の原因となる設定変更をインターフェイス設定で行うことができます。IDM と IME では、分析エンジン設定で競合の原因となるインターフェイス設定の変更を行うことは *できません*。

詳細情報

- インターフェイス ペアの組み合わせの詳細については、「インターフェイス サポート」（P.7-4）を参照してください。
- センサーおよびバイパス モードの詳細については、「バイパス モードの設定」（P.7-29）を参照してください。

ハードウェア バイパス モード

Cisco IPS ソフトウェア バイパスに加えて、IPS 4260 および IPS 4270-20 はハードウェア バイパスもサポートします。ここでは、ハードウェア バイパス カードとその設定上の制約事項について説明します。内容は次のとおりです。

ハードウェア バイパス カード

IPS 4260 と IPS 4270-20 がサポートするのは、ハードウェア バイパス機能を備えた 4 ポート GigabitEthernet カード（部品番号 IPS-4GE-BP-INT=）です。この 4GE バイパス インターフェイス カードは、ポート 0 と 1、およびポート 2 と 3 の間でのみハードウェア バイパスをサポートします。

（注）　ハードウェア バイパスをディセーブルにするには、他の組み合わせでインターフェイスのペアを作成します（2/0<->2/2、2/1<->2/3 など）。

ハードウェア バイパスは、Cisco IPS の既存のソフトウェア バイパス機能を補完します。ハードウェア バイパスとソフトウェア バイパスには、次の条件が適用されます。

- バイパスが OFF に設定されている場合、ソフトウェア バイパスはアクティブになりません。

  ハードウェア バイパスを使用できるインライン インターフェイスごとに、コンポーネント インターフェイスはフェールオープン機能をディセーブルにするように設定されます。SensorApp が失敗した場合、センサーの電源がオフになるかリセットされた場合、または、NIC インターフェイス ドライバが失敗するかアンロードされた場合、ペアのインターフェイスはフェールクローズ状態になります（トラフィックはインライン インターフェイスまたはインライン VLAN サブインターフェイスを通りません）。
- バイパスが ON に設定されている場合、ソフトウェア バイパスはアクティブになります。

  ソフトウェア バイパスは、各インライン インターフェイスのペアの物理インターフェイス間および各インライン VLAN サブインターフェイスのペアの VLAN 間でパケットを転送します。ハードウェア バイパスを使用できるインライン インターフェイスごとに、コンポーネント インターフェイスはスタンバイ モードに設定されます。センサーの電源がオフになるか、リセットされるか、

NIC インターフェイスが失敗するかアンロードされた場合、これらのペアのインターフェイスはハードウェアでフェールオープン状態になります（トラフィックはインライン インターフェイスを障害なく通過します）。他のインライン インターフェイスはフェールクローズ状態になります。

- バイパスが AUTO に設定されている場合（検査なしでトラフィックが通過）、ソフトウェア バイパスは SensorApp が失敗するとアクティブになります。

  ハードウェア バイパスを使用できるインライン インターフェイスごとに、コンポーネント インターフェイスはスタンバイ モードに設定されます。センサーの電源がオフになるか、リセットされるか、NIC インターフェイスが失敗するかアンロードされた場合、これらのペアのインターフェイスはハードウェアでフェールオープン状態になります。他のインライン インターフェイスはフェールクローズ状態になります。

（注）　フェールオーバーをテストするには、バイパス モードを ON または AUTO に設定して、1 つ以上のインライン インターフェイスを作成し、センサーの電源をオフにして、トラフィックがその後もインライン パスを通過することを確認します。

詳細情報

インライン バイパス モードの設定手順については、「バイパス モードの設定」（P.7-29）を参照してください。

ハードウェア バイパス設定の制約事項

4GE バイパス インターフェイス カードでハードウェア バイパス機能を使用するには、カードのハードウェア設計をサポートするインターフェイスをペアにする必要があります。ハードウェア バイパス対応インターフェイスと 1 つ以上のハードウェア バイパス設定の制約に違反するインターフェイスをペアにしたインライン インターフェイスを作成すると、ハードウェア バイパスはインライン インターフェイスで非アクティブとなり、次のような警告メッセージを受け取ります。

```
Hardware bypass functionality is not available on Inline-interface pair0.
Physical-interface GigabitEthernet2/0 is capable of performing hardware bypass only when
paired with GigabitEthernet2/1, and both interfaces are enabled and configured with the
same speed and duplex settings.
```

ハードウェア バイパスには、次の設定の制約事項が適用されます。

- 4 ポート バイパス カードは、IPS 4260 および IPS 4270-20 でのみサポートされます。
- フェールオープン ハードウェア バイパスは、インライン VLAN ペアではなく、インライン インターフェイス（インターフェイス ペア）でのみ機能します。
- フェールオープン ハードウェア バイパスは、次のすべての条件が満たされた場合にインライン インターフェイスで使用できます。
  - 両方の物理インターフェイスがハードウェア バイパスをサポートしている。
  - 両方の物理インターフェイスが同じインターフェイス カード上にある。
  - 2 つの物理インターフェイスが、ハードウェアでバイパス ペアとして関連付けられている。
  - 速度およびデュプレックス設定が、物理インターフェイス上で同じ。
  - 両方のインターフェイスが管理上イネーブルになっている。

- IPS 4260 および IPS 4270-20 に接続されている MDI/X スイッチ ポートで自動ネゴシエーションを設定する必要があります。

  ハードウェア バイパスを機能させるには、センサー ポートとスイッチ ポートの両方を自動ネゴシエーションに設定する必要があります。スイッチ ポートは、ケーブルの問題を解決するために、必要に応じて送信回線と受信回線を自動的に反転させる MDI/X をサポートしている必要があります。両方で同じ速度とデュプレックスが設定されている場合のみ、センサーは正しく動作することが保証されます。つまり、センサーも自動ネゴシエーションに設定する必要があります。

インターフェイス モードについて

ここでは、さまざまなインターフェイス モードについて説明します。内容は次のとおりです。

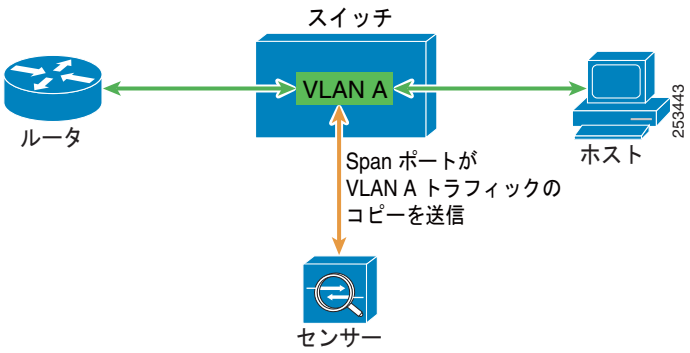
無差別モード

無差別モードでは、パケットはセンサーを通過しません。センサーは、実際に転送されるパケットではなく、モニタ対象のトラフィックのコピーを分析します。無差別モードで運用する利点は、転送されるトラフィックでパケットのフローにセンサーが影響を与えないことです。ただし、無差別モードで運用するときは、アトミック アタック（シングル パケット攻撃）などの特定のタイプの攻撃の場合に、悪意のあるトラフィックがターゲットに到達することをセンサーで阻止できないという短所があります。無差別モードのセンサー デバイスによって実行される応答アクションはイベント後の応答であるため、多くの場合、攻撃に対応するために、ルータやファイアウォールなど、他のネットワーキング デバイスによるサポートが必要となります。このような応答アクションは一部の攻撃を防ぐことはできますが、アトミック アタックでは、無差別モードベースのセンサーが管理対象デバイス（ファイアウォール、スイッチ、ルータなど）に ACL 修正を適用する前に、シングル パケットがターゲット システムに到達する可能性があります。

デフォルトでは、すべての検知インターフェイスは無差別モードです。インターフェイスをインライン インターフェイス モードから無差別モードに変更するには、変更対象のインターフェイスを含むすべてのインライン インターフェイスを削除し、インターフェイス設定からそのインターフェイスのすべてのインライン VLAN ペアのサブインターフェイスを削除します。

図 7-1 に無差別モードを示します。

図 7-1　無差別モード



IPv6、スイッチ、および VACL キャプチャなし

Catalyst スイッチの VACL は IPv6 をサポートしていません。トラフィックを無差別モードで設定されたセンサーにコピーする最も一般的な方法は、VACL キャプチャを使う方法です。IPv6 サポートが必要な場合は、SPAN ポートを使用できます。

ただし、次の設定を使用しない限り、スイッチでは最大 2 つのモニタ セッションしか設定できません。

- モニタ セッション
- 1 つ以上のセンサーに複数トランク
- トランク ポートごとに、1 つの IPS 内の複数の異なるセンサーまたは仮想センサーに対して多くの VLAN のモニタリングを実行できる VLAN を制限

次の設定では、1 つの SPAN セッションを使用して、指定された任意の VLAN 上のトラフィックすべてを指定されたすべてのポートに送信します。各ポート設定では、特定の 1 つの VLAN または複数の VLAN だけに通過を許可します。したがって、1 つの SPAN 設定行を使用して、異なる VLAN から異なるセンサーまたは仮想センサーすべてにデータを送信できます。

```
clear trunk 4/1-4 1-4094
set trunk 4/1 on dot1q 930
set trunk 4/2 on dot1q 932
set trunk 4/3 on dot1q 960
set trunk 4/4 on dot1q 962
set span 930, 932, 960, 962 4/1-4 both
```

（注）　VLAN ごとに異なる IPS ポリシーを割り当てる場合や 1 つのインターフェイスで処理できない大きな帯域幅をモニタする必要がある場合に SPAN/モニタ設定は役立ちます。

詳細情報

- 無差別モードの詳細については、「無差別モード」（P.7-13）を参照してください。
- スイッチでの SPAN/モニタ設定の詳細については、『*Catalyst 6500 Series Software Configuration Guide, 8.7*』の次の項を参照してください。
  - SPAN、RSPAN、およびミニ プロトコル アナライザの設定
  - スイッチ上での SPAN の設定

- イーサネット VLAN トランクの設定
- トランクでの許可 VLAN の定義

インライン インターフェイス モード

インライン インターフェイス ペア モードで運用する場合は、IPS が直接トラフィック フローに挿入され、パケット転送速度に影響を与えます。遅延が加わるため、パケット転送速度は遅くなります。その結果、センサーは、悪意のあるトラフィックがターゲットに到達する前にそのトラフィックをドロップして攻撃を阻止できるため、保護サービスが提供されます。インライン デバイスは、レイヤ 3 および 4 で情報を処理するだけでなく、より高度な埋め込み型攻撃のパケットの内容およびペイロードも分析します（レイヤ 3 ～ 7）。この詳細な分析では、通常は従来のファイアウォール デバイスを通過する攻撃をシステムが識別し、停止またはブロックするか、その両方を行うことができます。

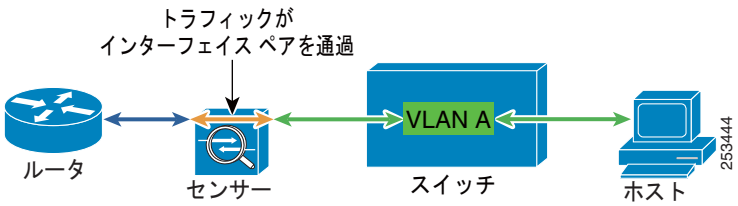
インライン インターフェイス ペア モードでは、パケットはセンサーのペアの 1 つめのインターフェイスを経由して入り、ペアの 2 つめのインターフェイスを経由して出ます。パケットは、シグニチャによって拒否または変更されないかぎり、ペアの 2 つめのインターフェイスに送信されます。

（注） 検知インターフェイスが 1 つだけの AIM IPS、AIP SSC-5、AIP SSM、IPS SSP、および NME IPS のモジュールでも、インラインで動作するように設定できます。

（注） ペアになっているインターフェイスが同じスイッチに接続されている場合は、それらのインターフェイスをスイッチ上で 2 つのアクセス ポートとして設定し、それぞれが異なる VLAN アクセスを持つようにする必要があります。このようにしないと、トラフィックはインライン インターフェイスを通過しません。

図 7-2 にインライン インターフェイス ペア モードを示します。

図 7-2　インライン インターフェイス ペア モード



インライン VLAN ペア モード

（注） AIM IPS、AIP SSC-5、AIP SSM、IPS SSP、および NME IPS はインライン VLAN ペアをサポートしません。

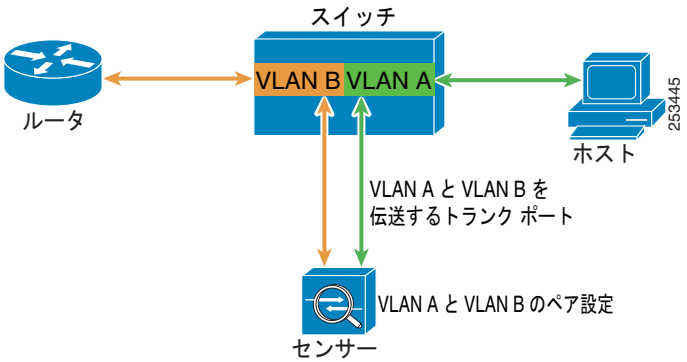
物理インターフェイス上で、VLAN をペアで関連付けることができます。これは、インライン VLAN ペア モードと呼ばれます。ペアの一方の VLAN で受信されたパケットは、分析後にペアのもう一方の VLAN に転送されます。

インライン VLAN ペア モードは、アクティブ検知モードです。このモードでは、検知インターフェイスが 802.1q トランク ポートとして動作し、センサーがトランク上の VLAN のペア間の VLAN ブリッジングを実行します。センサーは、ペアごとに各 VLAN 上で受信するトラフィックを検査し、そのパケットをペアのもう一方の VLAN に転送するか、または侵入の試行が検出された場合はそのパケットをドロップできます。IPS センサーは、各検知インターフェイス上で最大 255 個の VLAN ペアを同時にブリッジするように設定できます。センサーは、受信した各パケットの 802.1q ヘッダー内の VLAN ID フィールドを、センサーがパケットを転送する出力 VLAN の ID に置き換えます。センサーは、インライン VLAN ペアに割り当てられていないすべての VLAN で受信したすべてのパケットをドロップします。

（注）　インライン VLAN ペアでペアになっている VLAN のいずれかとして、デフォルト VLAN を使用することはできません。

図 7-3 にインライン VLAN ペア モードを示します。

図 7-3　　インライン VLAN ペア モード



VLAN グループ モード

各物理インターフェイスまたはインライン インターフェイスは、VLAN グループ サブインターフェイスに分けることができます。各サブインターフェイスは、そのインターフェイスの VLAN のグループで構成されます。分析エンジンは複数の仮想センサーをサポートします。各センサーはこれらの 1 つ以上のインターフェイスをモニタできます。これにより、複数のポリシーを同じセンサーに適用できます。この利点は、わずかなインターフェイスしかないセンサーを多くのインターフェイスがあるかのように使用できる点にあります。

（注）　インライン VLAN ペアに含まれている物理インターフェイスは、VLAN グループに分けることはできません。

VLAN グループ サブインターフェイスによって、物理インターフェイスまたはインライン インターフェイスと VLAN セットが関連付けられます。VLAN を複数の VLAN グループ サブインターフェイスのメンバにすることはできません。各 VLAN グループ サブインターフェイスは、1 ～ 255 の数値で識別されます。サブインターフェイス 0 は、仮想化されていない物理インターフェイスまたは論理インターフェイス全体を表すために使用される予約済みのサブインターフェイス番号です。サブインターフェイス 0 を作成、削除、または変更することはできません。また、サブインターフェイス 0 に関する統計情報は報告されません。

未割り当て VLAN グループは、別の VLAN グループに明示的に割り当てられていないすべての VLAN を含んでいる状態で維持されます。未割り当て VLAN グループ内の VLAN を直接指定することはできません。別の VLAN グループ サブインターフェイスに VLAN が追加されたり、または別の VLAN グループ サブインターフェイスから VLAN が削除されたりすると、未割り当て VLAN グループは更新されます。

通常、802.1q トランクのネイティブ VLAN 内のパケットには、そのパケットが属する VLAN 番号を示す 802.1q カプセル化ヘッダーがありません。各物理インターフェイスには、デフォルトの VLAN 変数が関連付けられており、この変数をネイティブ VLAN の VLAN 番号または 0 に設定する必要があります。値 0 は、ネイティブ VLAN が不明であるか、またはネイティブ VLAN の指定の有無は関係ないことを示しています。デフォルトの VLAN 設定が 0 の場合は、次の処理が行われます。

- 802.1q カプセル化のないパケットによってトリガーされたアラートには、VLAN 値 0 が報告されます。
- 802.1q カプセル化のないトラフィックは未割り当て VLAN グループに関連付けられ、ネイティブ VLAN として他の VLAN グループに割り当てることができません。

（注） スイッチのポートは、アクセス ポートまたはトランク ポートとして設定できます。アクセス ポートでは、すべてのトラフィックは、アクセス VLAN と呼ばれる 1 つの VLAN 内にあります。トランク ポートでは、ポートで複数の VLAN を伝送することができ、各パケットには VLAN ID を含む 802.1q ヘッダーと呼ばれる特別なヘッダーが付加されます。このヘッダーは、一般に VLAN タグと呼ばれます。ただし、トランク ポートには、ネイティブ VLAN と呼ばれる特別な VLAN があります。ネイティブ VLAN 内のパケットには、802.1q ヘッダーは付加されていません。IDSM2 は、ネイティブでないすべてのトラフィックの 802.1q ヘッダーを読み取り、そのパケットの VLAN ID を判断することができます。ただし、IDSM2 は、スイッチ設定内のポートのネイティブ VLAN としてどの VLAN が設定されているかはわからないため、ネイティブ パケットを受信する VLAN も認識できません。したがって、どの VLAN が該当のポートのネイティブ VLAN であるかを IDSM2 に通知する必要があります。IDSM2 は、タグが付いていないパケットを、ネイティブ VLAN ID のタグが付いたパケットとして処理します。

詳細情報

IDSM2 を VLAN グループ モードに設定する方法の詳細については、『Configuring the IDSM2』を参照してください。

インターフェイス設定のサマリー

[Summary] ペインには、検知インターフェイスをどのように設定したか（無差別モードに設定したインターフェイス、インライン ペアとして設定したインターフェイス、およびインライン VLAN ペアとして設定したインターフェイス）のサマリーが表示されます。このペインの内容は、インターフェイス設定を変更すると、変わります。

注意 無差別モード、インライン ペア モード、またはインライン VLAN ペア モードで動作するように、単一の物理インターフェイスを設定できますが、これらのモードを組み合わせてインターフェイスを設定することはできません。

フィールド定義

[Summary] ペインには次のフィールドがあります。

- [Name]：インターフェイスの名前。値は、無差別インターフェイスの場合、FastEthernet、GigabitEthernet、または PortChannel0/0 です。インライン インターフェイスの場合、この名前はペアに割り当てた名前になります。
- [Details]：インターフェイスが無差別、インライン、またはバックプレーンかどうか、および VLAN のペアがあるかどうかを示します。
- [Assigned Virtual Sensor]：インターフェイスまたはインターフェイス ペアが仮想センサーに割り当てられているかどうかを示します。
- [Description]：インターフェイスの説明。

インターフェイスの設定

ここでは、センサー上でのインターフェイスの設定方法について説明します。内容は次のとおりです。

[Interfaces] ペイン

（注）　センサーのインターフェイスのイネーブル化、ディセーブル化、および編集を行うには、管理者である必要があります。

[Interfaces] ペインには、センサー上の既存の物理インターフェイスとそれらに関連付けられている設定が一覧表示されます。センサーはインターフェイスを検出し、[Interfaces] ペインのインターフェイス リストに挿入します。

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、インターフェイスをイネーブルにする必要があります。**setup** コマンドを使用してセンサーを初期化したときにインターフェイスまたはインライン ペアを仮想センサーに割り当て、インターフェイスまたはインライン ペアをイネーブルにしました。インターフェイスの設定を変更する必要がある場合は、[Interfaces] ペインで変更できます。[Add Virtual Sensor] ダイアログボックスで仮想センサーを追加し、インターフェイスを割り当てるには、[Configuration] > *sensor_name* > [Policies] > [IPS Policies] > [Add Virtual Sensor] を選択します。

[Interfaces] ペインのフィールド定義

[Interfaces] ペインには次のフィールドがあります。

- [Interface Name]：インターフェイスの名前。値は、FastEthernet、GigabitEthernet、または PortChannel0/0 です。
- [Enabled]：インターフェイスがイネーブルかどうかを示します。

（注）　IPS SSP PortChannel0/0 インターフェイスは常にイネーブルです。

- [Media Type]：メディア タイプを示します。メディア タイプのオプションは次のとおりです。
  - [TX]：銅線メディア
  - [SX]：ファイバ メディア
  - [XL]：ネットワーク アクセラレータ カード
  - [Backplane interface]：モジュールを親シャーシのバックプレーンに接続する内部インターフェイス。
- [Duplex]：インターフェイスのデュプレックス設定を示します。デュプレックス タイプのオプションは次のとおりです。
  - [Auto]：インターフェイスを自動ネゴシエーション デュプレックスに設定します。
  - [Full]：インターフェイスを全二重に設定します。
  - [Half]：インターフェイスを半二重に設定します。
- [Speed]：インターフェイスの速度設定を示します。速度のオプションは、次のとおりです。
  - [Auto]：インターフェイスを自動ネゴシエーション速度に設定します。
  - [10 MB]：インターフェイスを 10 MB に設定します（TX インターフェイスの場合だけ）。
  - [100 MB]：インターフェイスを 100 MB に設定します（TX インターフェイスの場合だけ）。
  - [1000]：インターフェイスを 1 GB に設定します（ギガビット インターフェイスの場合だけ）。
  - [10000]：インターフェイスが 10 GB に設定されていることを示します（PortChannel0/0 のみ）。

（注）　このパラメータは保護されています。PortChannel0/0 インターフェイスの速度を変更することはできません。

- [Default VLAN]：インターフェイスが割り当てられている VLAN を示します。
- [Alternate TCP Reset Interface]：選択すると、このインターフェイスを無差別モニタリングに使用している場合、代替インターフェイス上で TCP リセットが送信され、シグニチャの起動によってリセット アクションがトリガーされます。
- [Description]：インターフェイスの説明を入力できます。

詳細情報

インターフェイス設定の制約事項の詳細については、「インターフェイス設定の制約事項」（P.7-9）を参照してください。

検知インターフェイスのイネーブル化とディセーブル化

（注）　IPS SSP PortChannel 0/0 インターフェイスは常にイネーブルです

インターフェイスをイネーブルまたはディセーブルにするには、次の手順を実行します。

ステップ 1　管理者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* > [Interfaces] > [Interfaces] を選択します。

ステップ 3　インターフェイスを選択し、[Enable] をクリックします。インターフェイスがイネーブルになります。インターフェイスでトラフィックをモニタするには、そのインターフェイスを仮想センサーに割り当てる必要があります。[Interfaces] ペインのリストの [Enabled] カラムが [Yes] になります。

ステップ 4　インターフェイスをディセーブルにするには、そのインターフェイスを選択し、[Disable] をクリックします。[Interfaces] ペインのリストの [Enabled] カラムが [No] になります。

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 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。

詳細情報

インターフェイス設定の制約事項の詳細については、「インターフェイス設定の制約事項」（P.7-9）を参照してください。

[Edit Interface] ダイアログボックスのフィールド定義

（注）　IPS SSP について編集できるインターフェイス フィールドは、[Description] フィールドだけです。

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

- [Interface Name]：インターフェイスの名前。値は、FastEthernet、GigabitEthernet、または PortChannel0/0 です。
- [Enabled]：インターフェイスがイネーブルかどうかを示します。

  （注）　IPS SSP PortChannel0/0 インターフェイスは常にイネーブルです。

- [Media Type]：メディア タイプを示します。メディア タイプのオプションは次のとおりです。
  - [TX]：銅線メディア
  - [SX]：ファイバ メディア
  - [XL]：ネットワーク アクセラレータ カード
  - [Backplane interface]：モジュールを親シャーシのバックプレーンに接続する内部インターフェイス。
- [Duplex]：インターフェイスのデュプレックス設定を示します。デュプレックス タイプのオプションは次のとおりです。
  - [Auto]：インターフェイスを自動ネゴシエーション デュプレックスに設定します。
  - [Full]：インターフェイスを全二重に設定します。
  - [Half]：インターフェイスを半二重に設定します。

- [Speed]：インターフェイスの速度設定を示します。速度のオプションは、次のとおりです。
  - [Auto]：インターフェイスを自動ネゴシエーション速度に設定します。
  - [10 MB]：インターフェイスを 10 MB に設定します（TX インターフェイスの場合だけ）。
  - [100 MB]：インターフェイスを 100 MB に設定します（TX インターフェイスの場合だけ）。
  - [1000]：インターフェイスを 1 GB に設定します（ギガビット インターフェイスの場合だけ）。
  - [10000]：インターフェイスを 1 GB に設定します（PortChannel0/0 のみ）。
- [Default VLAN]：インターフェイスが割り当てられている VLAN を示します。
- [Alternate TCP Reset Interface]：選択すると、このインターフェイスを無差別モニタリングに使用している場合、代替インターフェイス上で TCP リセットが送信され、シグニチャの起動によってリセット アクションがトリガーされます。
- [Description]：インターフェイスの説明を入力できます。

詳細情報

インターフェイス設定の制約事項の詳細については、「インターフェイス設定の制約事項」（P.7-9）を参照してください。

インターフェイスの編集

（注） IPS SSP について編集できるインターフェイス フィールドは、[Description] フィールドだけです。

インターフェイスの設定を編集するには、次の手順に従ってください。

ステップ 1　管理者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* > [Interfaces] > [Interfaces] を選択します。

ステップ 3　インターフェイスを選択して、[Edit] をクリックします。

（注） インターフェイスをダブルクリックして、[Edit Interface] ダイアログボックスを表示することもできます。

ステップ 4　[Description] フィールドの説明を変更するか、[No] または [Yes] チェックボックスをクリックして、状態をイネーブルからディセーブルに変更できます。[Use Alternative TCP Reset Interface] チェックボックスをオンにして、インターフェイスで代替 TCP リセット インターフェイスを使用できます。

ヒント 変更を破棄して [Edit Interface] 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　[OK] をクリックします。[Interfaces] ペインのリストに編集されたインターフェイスが表示されます。

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 6　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

インターフェイス設定の制約事項の詳細については、「インターフェイス設定の制約事項」（P.7-9）を参照してください。

インライン インターフェイス ペアの設定

ここでは、インライン インターフェイス ペアの設定方法について説明します。内容は次のとおりです。

[Interface Pairs] ペイン

（注）　インターフェイス ペアを設定するには、管理者である必要があります。

センサーでインライン モニタリングを実行できる場合は、センサーでインターフェイスのペアを設定できます。

（注）　AIM IPS、AIP SSC-5、AIP SSM、IPS SSP、および NME IPS では、モニタにインライン ペアは必要ありません。必要となるのは、物理インターフェイスを仮想センサーに追加することだけです。

詳細情報

- AIM IPS をインライン モードで設定する手順については、『Configuring the AIM IPS』を参照してください。
- AIP SSM をインライン モードで設定する手順については、『Configuring the AIP SSM』を参照してください。
- AIP SSC-5 をインライン モードで設定する手順については、『Configuring the AIP SSC-5』を参照してください。
- IPS SSP をインライン モードで設定する手順については、『Configuring the IPS SSP』を参照してください。
- NME IPS をインライン モードで設定する手順については、『Configuring the NME IPS』を参照してください。
- インターフェイス設定の制約事項の詳細については、「インターフェイス設定の制約事項」（P.7-9）を参照してください。

[Interface Pairs] ペインのフィールド定義

[Interface Pairs] ペインには次のフィールドがあります。

- [Interface Pair Name] インターフェイス ペアに付ける名前。
- [Paired Interfaces]：ペアにした 2 つのインターフェイス（GigabitEthernet0/0<->GigabitEthernet0/1 など）。
- [Description]：このインターフェイス ペアの説明を追加できます。

[Add Interface Pair]/[Edit Interface Pair] ダイアログボックスのフィールド定義

[Add Interface Pair]/[Edit Interface Pair] ダイアログボックスには次のフィールドがあります。

- [Interface Pair Name] インターフェイス ペアに付ける名前。
- [Select two interfaces]：リストからペアにする 2 つのインターフェイスを選択できます（GigabitEthernet0/0<->GigabitEthernet0/1 など）。
- [Description]：このインターフェイス ペアの説明を追加できます。

インライン インターフェイス ペアの設定

インライン インターフェイス ペアの設定を行うには、次の手順に従ってください。

ステップ 1　管理者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* > [Interfaces] > [Interface Pairs] を選択し、[Add] をクリックします。

ステップ 3　[Interface Pair Name] フィールドに名前を入力します。インライン インターフェイス名はユーザが作成する名前です。

ステップ 4　[Select two interfaces] フィールドでペアにする 2 つのインターフェイスを選択します。たとえば、GigabitEthernet0/0 と GigabitEthernet0/1 を選択します。

ステップ 5　必要に応じて、[Description] フィールドにインライン インターフェイス ペアの説明を入力できます。

ヒント　変更を破棄して [Add Interface pair] 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。[Interface Pairs] ペインのリストに新しいインライン インターフェイス ペアが表示されます。

ステップ 7　インライン インターフェイス ペアを編集するには、そのペアを選択し、[Edit] をクリックします。

ステップ 8　名前の変更、新しいインライン インターフェイス ペアの選択、説明の編集を行うことができます。

ヒント　変更を破棄して [Edit Interface Pair] 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。[Interface Pairs] ペインのリストに編集したインライン インターフェイス ペアが表示されます。

ステップ 10　インライン インターフェイス ペアを削除するには、そのペアを選択し、[Delete] をクリックします。そのインライン インターフェイス ペアは、[Interface Pairs] ペインの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。

詳細情報

インターフェイス設定の制約事項の詳細については、「インターフェイス設定の制約事項」（P.7-9）を参照してください。

インライン VLAN ペアの設定

ここでは、インライン VLAN ペアの設定方法について説明します。内容は次のとおりです。

[VLAN Pairs] ペイン

（注）　インライン VLAN ペアを設定するには、管理者である必要があります。

（注）　使用しているセンサーが、インライン VLAN ペアをサポートしていない場合、[VLAN Pairs] ペインは表示されません。AIM IPS、AIP SSC-5、AIP SSM、IPS SSP、および NME IPS は、インライン VLAN ペアをサポートしません。

[VLAN Pairs] ペインには、各物理インターフェイスの既存の VLAN ペアが表示されます。インライン VLAN ペアを作成するには、[Add] をクリックします。無差別モードのインターフェイスにインライン VLAN ペアを作成するには、仮想センサーからインターフェイスを削除してからインライン VLAN ペアを作成する必要があります。インターフェイスがすでにペアになっているか、無差別モードの場合、インライン VLAN ペアを作成しようとすると、エラー メッセージを受け取ります。

（注）　別のインターフェイスとペアになっているインターフェイスや無差別モードで仮想センサーに割り当てられているインターフェイスにはインライン VLAN ペアは作成できません。

（注）　インライン VLAN ペアでペアになっている VLAN のいずれかとして、デフォルト VLAN を使用することはできません。

詳細情報

インターフェイス設定の制約事項の詳細については、「インターフェイス設定の制約事項」（P.7-9）を参照してください。

[VLAN Pairs] ペインのフィールド定義

[VLAN Pairs] ペインには次のフィールドがあります。

- [Interface Name]：インライン VLAN ペアの名前。
- [Subinterface]：インライン VLAN ペアのサブインターフェイス番号。値は 1 ～ 255 です。
- [VLAN A]：最初の VLAN の VLAN 番号が表示されます。値は 1 ～ 4095 です。
- [VLAN B]：第 2 の VLAN の VLAN 番号が表示されます。値は 1 ～ 4095 です。
- [Description]：インライン VLAN ペアの説明。

[Add VLAN Pair]/[Edit VLAN Pair] ダイアログボックスのフィールド定義

[Add Inline VLAN Pair]/[Edit Inline VLAN Pair] ダイアログボックスには次のフィールドがあります。

- [Interface Name]：ペアにするインターフェイスの名前。
- [Subinterface Number]：サブインターフェイス番号を割り当てることができます。1 ～ 255 の範囲の番号を割り当てることができます。
- [VLAN A]：このインライン VLAN ペアに最初の VLAN を割り当てることができます。1 ～ 4095 の任意の VLAN を割り当てることができます。
- [VLAN B]：このインライン VLAN ペアにもう一方の VLAN を割り当てることができます。1 ～ 4095 の任意の VLAN を割り当てることができます。
- [Description]：このインライン VLAN ペアの説明を追加できます。

（注） VLAN をそれ自身とペアにすることはできません。

（注） サブインターフェイス番号と VLAN 番号は、物理インターフェイスごとに一意である必要があります。

詳細情報

インターフェイス設定の制約事項の詳細については、「インターフェイス設定の制約事項」（P.7-9）を参照してください。

インライン VLAN ペアの設定

インライン VLAN ペアの設定を行うには、次の手順に従ってください。

ステップ 1　管理者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* > [Interfaces] > [VLAN Pairs] を選択し、[Add] をクリックします。

ステップ 3　[Interface Name] リストからインターフェイスを選択します。

ステップ 4　[Subinterface Number] フィールドに、インライン VLAN ペアのサブインターフェイス番号（1 ～ 255）を入力します。

ステップ 5　[VLAN A] フィールドで、このインライン VLAN ペアの最初の VLAN（1 ～ 4095）を指定します。

ステップ 6　[VLAN B] フィールドで、このインライン VLAN ペアのもう一方の VLAN（1 ～ 4095）を指定します。

ステップ 7　必要に応じて、[Description] フィールドにインライン VLAN ペアの説明を入力します。

ヒント　変更を破棄して [Add VLAN Pair] 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] をクリックします。新しいインライン VLAN ペアが、[VLAN Pairs] ペインのリストに表示されます。

ステップ 9　インライン VLAN ペアを編集するには、そのペアを選択し、[Edit] をクリックします。

ステップ 10　サブインターフェイス番号と VLAN 番号の変更、説明の編集を行えます。

ヒント　変更を破棄して [Edit VLAN Pair] 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 11　[OK] をクリックします。編集された VLAN ペアが [VLAN Pairs] ペインのリストに表示されます。

ステップ 12　VLAN ペアを削除するには、そのペアを選択して [Delete] をクリックします。その VLAN ペアは、[VLAN Pairs] ペインの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 13　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

インターフェイス設定の制約事項の詳細については、「インターフェイス設定の制約事項」（P.7-9）を参照してください。

VLAN グループの設定

ここでは、VLAN グループの設定方法について説明します。内容は次のとおりです。

[VLAN Groups] ペイン

（注）　VLAN グループを設定するには、管理者である必要があります。

[VLAN Groups] ペインでは、センサー インターフェイスの設定で定義した VLAN グループの追加、編集、または削除を行うことができます。VLAN グループは、インターフェイスに存在する VLAN ID のグループで構成されています。各 VLAN グループは、少なくとも 1 つの VLAN ID で構成されています。インターフェイス（論理または物理）ごとに最大 255 の VLAN グループを設定できます。各グループには、任意の数の VLAN ID を含めることができます。その後、各 VLAN グループを仮想センサーに割り当てます（ただし、1 つのセンサーのみ）。同じセンサー上の異なる VLAN グループを異なる仮想センサーに割り当てることができます。

VLAN ID を VLAN グループに割り当てたあとに、その VLAN グループを仮想センサーに割り当てる必要があります。IME は、インターフェイスと仮想センサー設定間を相互検証します。一方のコンポーネントでの他方を無効化する可能性のある設定変更はブロックされます。

詳細情報

仮想センサーに VLAN グループを割り当てる手順については、「仮想センサーの追加、編集、削除」（P.8-13）を参照してください。

VLAN グループの展開

インライン ペアの VLAN グループは、VLAN ID を変換しません。したがって、論理インターフェイスで VLAN グループを使用するには、2 つのスイッチ間にインライン ペア インターフェイスが存在する必要があります。アプライアンスの場合、2 つのペアを同じスイッチに接続し、それらをアクセス ポートにして、2 つのポートに対して別々にアクセス VLAN を設定できます。この設定では、センサーは 2 つの VLAN 間を接続します。これは、2 つのポートはそれぞれアクセス モードであり、1 つの VLAN だけを伝送するためです。この場合、2 つのポートは異なる VLAN に存在する必要があります。センサーはこれら 2 つの VLAN をブリッジし、2 つの VLAN 間を流れるすべてのトラフィックをモニタします。IDSM2 の 2 つのデータ ポートは常に同じスイッチに接続されているため、IDSM2 はこの方法でも動作します。

2 つのスイッチ間にアプライアンスを接続することもできます。2 つの方法があります。第 1 の方法では、2 つのポートがアクセス ポートとして設定されるため、1 つの VLAN を伝送できます。この方法では、センサーは 2 つのスイッチ間で 1 つの VLAN をブリッジします。

第 2 の方法では、2 つのポートはトランク ポートとして設定されるため、複数の VLAN を伝送できます。この設定では、センサーは 2 つのスイッチ間で複数の VLAN をブリッジします。複数の VLAN がインライン インターフェイス ペアで伝送されるため、VLAN をグループに分けることができ、各グループを仮想センサーに割り当てることができます。第 2 の方法は、IDSM2 には適用されません。IDSM2 はこの方法では接続できないためです。

詳細情報

- VLAN グループで IDSM2 を設定する手順については、『Configuring the IDSM2』を参照してください。
- インターフェイス設定の制約事項の詳細については、「インターフェイス設定の制約事項」（P.7-9）を参照してください。

[VLAN Groups] ペインのフィールド定義

[VLAN Groups] ペインには次のフィールドがあります。

- [Interface Name]：VLAN グループの物理または論理インターフェイス名。
- [Subinterface]：VLAN グループのサブインターフェイス番号。値は 1 ～ 255 です。
- [VLAN Group]：VLAN グループの VLAN 番号を表示します。値は 1 ～ 4095 です。
- [Description]：VLAN グループの説明。

[Add VLAN Group]/[Edit VLAN Group] ダイアログボックスのフィールド定義

[Add VLAN Group]/[Edit VLAN Group] ダイアログボックスには次のフィールドがあります。

- [Interface Name]：VLAN グループの名前。
- [Subinterface Number]：VLAN グループのサブインターフェイス番号。値は 1 ～ 255 です。
- [VLAN Group]：VLAN グループの VLAN 番号を表示します。
  - [Unassigned VLANS]：VLAN グループに割り当てられていないすべての VLAN を選択できます。
  - [Specify VLAN Group]：この VLAN グループに割り当てる VLAN の ID を指定できます。

    "1, 5-8, 10-15" のように、1 ～ 4095 の値をカンマで区切って、個々の VLAN ID や範囲を指定します。
- [Description]：VLAN グループの説明。

VLAN グループの設定

VLAN グループを設定するには、次の手順に従ってください。

ステップ 1　管理者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* > [Interfaces] > [VLAN Groups] を選択し、[Add] をクリックします。

ステップ 3　[Interface Name] ドロップダウン リストから、インターフェイスを選択します。

ステップ 4　[Subinterface Number] フィールドに、VLAN グループのサブインターフェイス番号（1 ～ 255）を入力します。

ステップ 5　[VLAN Group] では、次のチェックボックスの 1 つをオンにして、このインターフェイスの VLAN グループを指定します。

a. [Unassigned VLANs]：サブインターフェイスに個別に割り当てられていないすべての VLAN を割り当てることができます。

b. [Specify VLAN Group]：このサブインターフェイスに割り当てる VLAN を指定できます。"1, 5-8, 10-15" のようなパターンで、複数の VLAN（1 ～ 4096）を割り当てることができます。このようにして、VLAN ID に基づいて異なるポリシーを設定できます。たとえば、VLAN 1 ～ 10 を 1 つの仮想センサー（VS0）に、VLAN 20 ～ 30 を別の仮想センサー（VS1）に向かうように設定できます。

（注）　[Specify VLAN Group] フィールドに入力するには、スイッチで設定されている VLAN ID が必要です。

ステップ 6　必要に応じて、[Description] フィールドに VLAN グループの説明を入力できます。

ヒント　変更を破棄して [Add VLAN Group] 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。新しい VLAN グループが [VLAN Groups] ペインのリストに表示されます。この VLAN グループを仮想センサーに割り当てる必要があります。

ステップ 8　VLAN グループを編集するには、グループを選択し、[Edit] をクリックします。

ステップ 9　サブインターフェイス番号と VLAN グループの変更、説明の編集を行えます。

ヒント　変更を破棄して [Edit VLAN Group] 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 10　[OK] をクリックします。編集された VLAN グループが [VLAN Groups] ペインのリストに表示されます。

ステップ 11　VLAN グループを削除するには、グループを選択し、[Delete] ボタンをクリックします。その VLAN グループは、[VLAN Groups] ペインの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 12　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。

バイパス モードの設定

ここでは、バイパス モードの設定方法について説明します。内容は次のとおりです。

[Bypass] ペイン

（注）　センサーでバイパス モードを設定するには、管理者である必要があります。

（注）　IPS SSP は、バイパス モードをサポートしていません。適応型セキュリティ アプライアンスは、適応型セキュリティ アプライアンスの設定と IPS SSP 上で行われているアクティビティのタイプによって、フェールオープン、フェールクローズ、またはフェールオーバーします。

インライン バイパスは、分析ツールとして、およびフェールオーバー保護メカニズムとして使用できます。通常は、センサーの分析エンジンがパケット分析を実行します。インライン バイパスがアクティブである場合、分析エンジンはバイパスされ、トラフィックは検査されることなく、インライン インターフェイスおよびインライン VLAN ペアを通過できます。インライン バイパスによって、センサー プロセスがアップグレードのために一時的に停止した場合や、センサー モニタリング プロセスが失敗した場合でも、パケットは引き続きセンサーを通過できます。オン、オフ、および自動という 3 つのモードがあります。デフォルトでは、バイパス モードは自動に設定されています。

インライン バイパス機能は、ソフトウェアで実行されるため、オペレーティング システムが稼動している場合にだけ動作します。センサーの電源がオフになっている場合、またはシャットダウンされている場合、インライン バイパスは動作しません。つまり、トラフィックはセンサーを通過しません。

注意　センサーをバイパス モードにすると、セキュリティ上の影響があります。バイパス モードをオンにすると、トラフィックはセンサーをバイパスし、検査されません。そのため、センサーは悪意のある攻撃を阻止できません。

注意　センサーが、シグニチャまたはグローバル相関の更新を適用すると、バイパスがトリガーされる場合があります。バイパスがトリガーされるかどうかは、センサーのトラフィック負荷とシグニチャまたはグローバル相関の更新のサイズによって決まります。バイパス モードをオフにすると、インライン センサーは更新の適用中にトラフィックの送信を停止します。

詳細情報

- AIP SSM、AIP SSC-5、およびバイパス モードの詳細については、「適応型セキュリティ アプライアンス、AIP SSM、AIP SSC-5、およびバイパス モード」（P.7-31）を参照してください。
- IPS SSP およびバイパス モードの詳細については、「適応型セキュリティ アプライアンス、IPS SSP、およびバイパス モード」（P.7-31）を参照してください。
- ASA ソフトウェアの詳細については、次の URL に掲載されている ASA ユーザ マニュアルを参照してください。

  http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html

[Bypass] ペインのフィールド定義

[Bypass] ペインには次のフィールドがあります。

- [Auto]：センサーのモニタリング プロセスがダウンしていない限り、トラフィックは検査のためにセンサーを通過します。

  センサーのモニタリング プロセスがダウンすると、センサーが再び動作するまで、トラフィックはセンサーをバイパスします。センサーは、動作を再開すると、トラフィックを検査します。Auto モードは、センサーのアップグレード時に役立ちます。センサーのアップグレード中でもトラフィック フローが確保されるからです。また、Auto モードによって、モニタリング プロセスが失敗した場合でも、トラフィックは引き続きセンサーを通過します。

- [Off] : バイパス モードをディセーブルにします。

  トラフィックは、検査のために、センサーを介して送信されます。センサーのモニタリング プロセスがダウンすると、トラフィックは通過しなくなります。これは、インライン トラフィックが常に検査されることを意味します。
- [On] : トラフィックは分析エンジンをバイパスし、検査されません。これは、インライン トラフィックが常に検査されないことを意味します。

適応型セキュリティ アプライアンス、AIP SSM、AIP SSC-5、およびバイパス モード

バイパス モード、適応型セキュリティ アプライアンス、AIP SSM、および AIP SSC-5 には次の条件が適用されます。

- [Bypass] が [Auto] または [Off] : AIP SSM および AIP SSC-5 がシャットダウンまたはリセットされると、適応型セキュリティ アプライアンスは、設定されているフェールオープンまたはフェールクローズ ルールに従ってトラフィックの通過を許可またはブロックします。
- [Bypass] が [Auto] : SensorApp が AIP SSM および AIP SSC-5 で停止した場合、AIP SSM および AIP SSC-5 NIC ドライバ（複数も可）は機能し続け、ハートビート パケットを通過させるので、設定されているフェールオープンまたはフェールクローズ ルールに関係なく、適応型セキュリティ アプライアンスはすべてのトラフィックを許可します。
- [Bypass] が [Off] : 設定されているフェールオープンまたはフェールクローズ ルールに関係なく、SensorApp が AIP SSM および AIP SSC-5 で停止すると、適応型セキュリティ アプライアンスはトラフィックの通過を停止します。

詳細情報

- IPS ソフトウェアのバイパス モードの詳細については、「バイパス モードの設定」（P.7-29）を参照してください。
- 適応型セキュリティ アプライアンスと AIP SSM の詳細については、『Configuring the AIP SSM』を参照してください。
- 適応型セキュリティ アプライアンスと AIP SSC-5 の詳細については、『Configuring the AIP SSC-5』を参照してください。
- ASA ソフトウェアの詳細については、次の URL に掲載されている ASA ユーザ マニュアルを参照してください。

  http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html

適応型セキュリティ アプライアンス、IPS SSP、およびバイパス モード

IPS SSP は、バイパス モードをサポートしていません。適応型セキュリティ アプライアンスは、適応型セキュリティ アプライアンスの設定と IPS SSP 上で行われているアクティビティのタイプによって、フェールオープン、フェールクローズ、またはフェールオーバーします。

IPS SSP を再設定するか、シグニチャまたはエンジンの更新を実行すると、適応型セキュリティ アプライアンスは、適応型セキュリティ アプライアンスで設定されているフェールオープンまたはフェールクローズ ポリシーに基づいてトラフィックを許可または停止し、フェールオーバーはトリガーしません。

IPS SSP をリセットまたはリロードするか、サービス パック更新、メジャー更新、またはマイナー更新を実行するか、IPS SSP でコントロール プレーンまたはデータ プレーンの障害が発生すると、フェールオーバーが設定されている場合、適応型セキュリティ アプライアンスはフェールオーバーします。フェールオーバーが設定されていない場合、または適応型セキュリティ アプライアンスがフェールオーバーできない場合、適応型セキュリティ アプライアンスはフェールオープンまたはフェールクローズ ポリシー設定に基づいて、トラフィックを許可または停止します。

詳細情報

- 適応型セキュリティ アプライアンスと IPS SSP の詳細については、『Configuring the IPS SSP』を参照してください。
- ASA ソフトウェアの詳細については、次の URL に掲載されている ASA ユーザ マニュアルを参照してください。

  http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html

トラフィック フロー通知の設定

ここでは、トラフィック フロー通知の設定方法について説明します。内容は次のとおりです。

[Traffic Flow Notifications] ペイン

（注）　トラフィック フロー通知を設定するには、管理者である必要があります。

インターフェイス上のパケットのフローをモニタし、そのフローが指定した間隔中に変更（開始および停止）された場合に通知を送信するようにセンサーを設定できます。特定の通知間隔内に失われたパケットのしきい値を設定でき、ステータス イベントがレポートされる前のインターフェイス アイドル遅延も設定できます。

[Traffic Notifications] ペインのフィールド定義

[Traffic Flow Notifications] ペインには、次のフィールドがあります。

- [Missed Packets Threshold]：通知が送信されるまでに、指定された時間中に失われる必要のあるパケットのパーセント。
- [Notification Interval]：センサーが失われたパケットの割合をチェックする間隔。
- [Interface Idle Threshold]：通知が送信されるまでに、インターフェイスがアイドル状態となってパケットを受信しない秒数。

トラフィック フロー通知の設定

トラフィック フロー通知を設定するには、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* > [Interfaces] > [Traffic Flow Notifications] を選択します。

ステップ 3　[Missed Packets Threshold] フィールドでは、通知を受け取るまでに失われる必要のあるパケットのパーセントを決定し、量を入力します。

ステップ 4　[Notification Interval] フィールドでは、失われたパケットのパーセントをチェックする秒数を決定し、数値を入力します。

ステップ 5　[Interface Idle Threshold] フィールドでは、通知を受けるまでにインターフェイスがアイドル状態となってパケットを受信しない秒数を決定し、入力します。

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 6　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。

CDP モードの設定

（注）　IPS SSP は、CDP モードをサポートしていません。

（注）　CDP モードを設定するには、管理者である必要があります。

CDP パケットの転送のイネーブルまたはディセーブルにするようにセンサーを設定できます。このアクションは、すべてのインターフェイスにグローバルに適用されます。

Cisco Discovery Protocol は、メディアおよびプロトコルに依存しないデバイス検出プロトコルであり、すべてのシスコ製装置（ルータ、アクセス サーバ、ブリッジ、スイッチなど）上で動作します。CDP を使用することにより、デバイスはその存在を他のデバイスにアドバタイズし、同じ LAN 上または WAN のリモート サイト上の他のデバイスに関する情報を受信できます。CDP は、SNAP をサポートするすべてのメディア（LAN、フレーム リレー、ATM メディアなど）で稼動します。

フィールド定義

[CDP Mode] ペインには次のフィールドがあります。

- [Drop CDP Packets]：センサーは CDP パケットを転送しません。
- [Forward CDP Packets]：センサーは CDP パケットを転送します。

CDP モードの設定

CDP モードを構成するには、次の手順に従ってください。

ステップ 1　管理者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* > [Interfaces] > [Interfaces] > [CDP Mode] を選択します。

ステップ 3　[CDP Mode] ドロップダウン リストから、[Drop CDP Packets]（デフォルト）または [Forward CDP Packets] を選択します。

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 4　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。

CHAPTER 8

ポリシーの設定

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

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

この章では、IPS ポリシーと、仮想センサー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。

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いてセキュリティ ポリシーを作成し、これらのカスタマイズしたポリシーを、VLAN または物理インターフェイスごとに適用できます。

IPS ポリシーのコンポーネント

ここでは、IPS ポリシーのさまざまなコンポーネントについて説明します。内容は次のとおりです。

分析エンジンの概要

分析エンジンは、パケット分析とアラート検出を実行します。指定したインターフェイスを流れるトラフィックをモニタします。

仮想センサーは分析エンジンで作成します。各仮想センサーには一意の名前が設定され、インターフェイスのリスト、インライン インターフェイス ペア、インライン VLAN ペア、および VLAN グループが関連付けられます。定義の順序付けに関する問題を避けるため、割り当てでは衝突や重なりは許可されません。インターフェイス、インライン インターフェイス ペア、インライン VLAN ペア、および VLAN グループを特定の仮想センサーに割り当て、パケットが複数の仮想センサーで処理されないようにします。各仮想センサーは、明確に名前が設定されたシグニチャ定義、イベント アクション規則、および異常検出設定にも関連付けられます。どの仮想センサーにも割り当てられていないインターフェイス、インライン インターフェイス ペア、インライン VLAN ペア、および VLAN グループからのパケットは、インライン バイパス設定に従って廃棄されます。

（注） Cisco IPS では、5 個以上の仮想センサーはサポートされません。デフォルトの仮想センサー vs0 は削除できません。

仮想センサーについて

センサーは 1 つまたは多数のモニタ対象データ ストリームからのデータ入力を受信できます。これらのモニタ対象データ ストリームは、物理インターフェイス ポートまたは仮想インターフェイス ポートのどちらでも構いません。たとえば、単一のセンサーでファイアウォールの前からのトラフィック、ファイアウォールの後ろからのトラフィック、またはファイアウォールの前後からのトラフィックを同時にモニタできます。単一のセンサーで 1 つ以上のデータ ストリームをモニタできます。この場合、単一のセンサー ポリシーまたは設定がすべてのモニタ対象データストリームに適用されます。

仮想センサーは、複数の設定ポリシーで定義されたデータを集めたものです。仮想センサーは、インターフェイス コンポーネントで定義されたパケットの集合に適用されます。

1 つの仮想センサーは複数のセグメントをモニタでき、1 つの物理センサーの中の仮想センサーごとに異なるポリシーまたは設定を適用できます。分析するモニタ対象セグメントごとに異なるポリシーを設定できます。また、同じポリシーインタンス（たとえば sig0、rules0、または ad0）を、異なる仮想センサーに適用することもできます。インターフェイス、インライン インターフェイス ペア、インライン VLAN ペア、および VLAN グループを仮想センサーに割り当てることができます。

（注） デフォルトの仮想センサーは vs0 です。デフォルトの仮想センサーは削除できません。インターフェイス リスト、異常検出動作モード、インライン TCP セッション トラッキング モード、および仮想センサーの記述は、デフォルトの仮想センサーについて変更できる唯一の設定です。シグニチャ定義、イベント アクション規則、異常検出ポリシーは変更できません。

（注） IPS SSP を搭載した Cisco ASA 5585-X は、インライン TCP セッション トラッキング モードをサポートしていません。

仮想化の利点および制約事項

（注） AIM IPS、AIP SSC-5、および NME IPS では仮想化がサポートされていません。

仮想化には次の利点があります。

- 個々のトラフィック セットにそれぞれ異なる設定を適用できます。
- IP スペースが重複している 2 つのネットワークを 1 つのセンサーでモニタできます。
- ファイアウォールまたは NAT デバイスの内側と外側の両方をモニタできます。

仮想化には次の制約事項があります。

- 非対称トラフィックの両側を同じ仮想センサーに割り当てる必要があります。
- VACL キャプチャまたは SPAN（無差別モニタリング）の使用は、VLAN タギングに関して矛盾しており、これによって VLAN グループの問題が発生します。
  - Cisco IOS ソフトウェアを使用している場合、VACL キャプチャ ポートまたは SPAN ターゲットは、トランキング用に設定されていても、常にタグ付きパケットを受信するわけではありません。
  - MSFC を使用している場合、学習したルートの高速パス スイッチングによって、VACL キャプチャおよび SPAN の動作が変わります。
- 固定ストアが制限されます。

仮想化には次のトラフィック キャプチャ要件があります。

- 仮想センサーで 802.1q ヘッダーを含むトラフィックを受信する必要があります（キャプチャ ポートのネイティブ VLAN 上のトラフィック以外）。
- センサーで、指定したセンサーの同じ仮想センサーに含まれる同じ VLAN グループの両方向のトラフィックをモニタする必要があります。

次のセンサーは仮想化をサポートしています。

- AIP SSM

- IPS 4240
- IPS 4255
- IPS 4260
- IPS 4270-20
- IPS SSP

IDSM2 では、インライン インターフェイス ペア上の VLAN グループを除き、仮想化がサポートされています。

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

インライン TCP セッション トラッキング モード

インラインでのパケット変更を選択している場合、ノーマライザ エンジンでは、ストリームからのパケットを 2 回認識すると、ストリームの状態を適切に追跡できません。このような場合は、ストリームが頻繁にドロップされます。この状況は、ストリームが、IPS によってモニタされている複数の VLAN またはインターフェイスを介してルーティングされている場合に、最もよく発生します。また、いずれかの方向のトラフィックがそれぞれ異なる VLAN またはインターフェイスから受信された場合に、ストリームを適切に追跡するために非対称トラフィックをマージできるようにする必要があり、これにより、状況がより複雑化します。

この状況を処理するために、ストリームが別々のインターフェイスまたは VLAN（または VLAN ペアのサブインターフェイス）で受信された場合には、これらを一意のストリームとして認識するように、モードを設定できます。

次のインライン TCP セッション トラッキング モードが適用されます。

- インターフェイスおよび VLAN：同じ VLAN（またはインライン VLAN ペア）内および同じインターフェイス上で同じセッション キー（AaBb）を持つすべてのパケットは、同じセッションに属しています。同じキーを持ち、VLAN が異なるパケットは、別々に追跡されます。
- VLAN だけ：同じ VLAN（またはインライン VLAN ペア）内で同じセッション キー（AaBb）を持つすべてのパケットは、インターフェイスにかかわらず同じセッションに属しています。同じキーを持ち、VLAN が異なるパケットは、別々に追跡されます。
- 仮想センサー：仮想センサー内で同じセッション キー（AaBb）を持つすべてのパケットは、同じセッションに属しています。これがデフォルトであり、ほとんどの場合、最良のオプションです。

（注）　IPS SSP を搭載した Cisco ASA 5585-X は、インライン TCP セッション トラッキング モードをサポートしていません。

ノーマライザ モードについて

ノーマライザ モードは、センサーがインライン モードで動作している場合にだけ適用されます。デフォルトは [Strict Evasion Protection] であり、これは、TCP ステートとシーケンスのトラッキングが完全に強制されることを意味します。ノーマライザによって、重複パケット、変更されたパケット、順序が正しくないパケットなどの検査が強制されます。このことは、攻撃者が IPS を回避することを阻止するのに役立ちます。

非対称モードでは、ノーマライザのチェックの大部分がディセーブルになります。非対称モードはストリーム全体を検査できない場合にだけ使用してください。この状況では、攻撃者が IPS を回避できるためです。

（注）　IPS SSP を搭載した Cisco ASA 5585-X は、ノーマライザ モードをサポートしていません。

イベント アクション オーバーライドの概要

イベント アクション オーバーライドを追加すると、イベントのリスク レーティングに基づいて、そのイベントに関連付けられているアクションを変更できます。イベント アクション オーバーライドは、各シグニチャを個別に設定しないで、グローバルにイベント アクションを追加する方法です。各イベント アクションには、関連付けられたリスク レーティング範囲があります。シグニチャ イベントが発生し、そのイベントのリスク レーティングがイベント アクションの範囲内に入っていた場合、そのアクションがイベントに追加されます。たとえば、リスク レーティングが 85 以上のイベントで SNMP トラップを生成させる場合、Request SNMP Trap のリスク レーティング範囲を 85 ～ 100 に設定します。アクション オーバーライドを使用しない場合は、イベント アクション オーバーライド コンポーネント全体をディセーブルにします。

（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。

リスク レーティングの計算

リスク レーティング（RR）は 0 ～ 100 の範囲の値であり、ネットワーク上の特定のイベントに関係するリスクの数値による定量化を表します。計算では、攻撃対象（たとえば特定のサーバ）のネットワーク資産の価値が考慮されるため、攻撃重大度レーティングとシグニチャ忠実度レーティングを使用してシグニチャごとに設定され、ターゲット価値レーティングを使用してサーバごとに設定されます。リスク レーティングは、いくつかのコンポーネントから計算され、そのうちの一部は設定、収集、計算で得られます。

（注）　リスク レーティングは、シグニチャではなくアラートに関連付けられます。

リスク レーティングを使用すると、注意が必要なアラートに優先順位を付けることができます。これらのリスク レーティング要因では、攻撃が成功した場合の重大度、シグニチャの忠実度、グローバル相関データから得た攻撃者の評判スコア、およびターゲット ホストの各自にとっての全体的な価値が考慮されます。リスク レーティングは evIdsAlert で報告されます。

特定のイベントのリスク レーティングを計算するために次の値が使用されます。

- シグニチャの忠実度評価（SFR）：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。シグニチャ忠実度レーティングはシグニチャごとに設定され、シグニチャが、それが表しているイベントまたは条件をどれだけ正確に検出するかを示します。

  シグニチャ忠実度レーティングは、シグニチャベースでシグニチャの作成者が計算します。シグニチャの作成者は、ターゲットに関する条件を絞り込んだ情報がない場合に、シグニチャの正確性についての基準となる信頼度ランキングを定義します。これは、分析対象パケットの配送を許可した

場合に、検出された動作がターゲット プラットフォームに対して意図した効果を生み出す信頼度を表します。たとえば、非常に具体的な規則（特定の正規表現）を使用して記述されたシグニチャは、汎用的な規則を使用して記述されたシグニチャよりもシグニチャ忠実度が高くなります。

（注）　シグニチャ忠実度レーティングは、検出されたイベントがどれだけ悪影響を及ぼすかを示すものではありません。

- 攻撃重大度レーティング（ASR）：脆弱性の悪用に成功した場合の重大度に関連付ける重み。

  攻撃重大度レーティングは、シグニチャのアラート重大度パラメータ（informational、low、medium、または high）から計算されます。攻撃重大度レーティングはシグニチャごとに設定され、検出されたイベントどれだけ危険かを示します。

（注）　攻撃重大度レーティングは、イベントがどれだけ正確に検出されるかを示すものではありません。

- ターゲットの価値レーティング（TVR）：ターゲットの考えられる価値に関連付けられる重み。

  ターゲットの価値レーティングはユーザ設定可能な値（zero、low、medium、high、または mission critical）であり、ネットワーク資産の IP アドレスを通じてその重要性を表します。価値の高い企業リソースにはより厳しく、あまり重要でないリソースにはより緩やかなセキュリティ ポリシーを開発できます。たとえば、デスクトップ ノードに割り当てるターゲットの価値レーティングよりも高いターゲットの価値レーティングを会社の Web サーバに割り当てることができます。この場合、会社の Web サーバに対する攻撃には、デスクトップ ノードに対する攻撃よりも高いリスク レーティングが付与されます。ターゲットの価値レーティングは、イベント アクション規則ポリシーで設定します。

- 攻撃関連性レーティング（ARR）：対象となるオペレーティング システムの関連性に関連付ける重み。

  攻撃関連性レーティングは、派生値（relevant、unknown、または not relevant）であり、アラート時に決定されます。関連するオペレーティング システムはシグニチャごとに設定します。

- 無差別デルタ（PD）：無差別デルタに関連付けられる重みであり、無差別モードの全体的なリスク レーティングから差し引くことができます。

  無差別デルタの範囲は 0 ～ 30 であり、シグニチャごとに設定します。

（注）　トリガー パケットがインラインでない場合、無差別デルタがレーティングから差し引かれます。

- ウォッチ リスト レーティング（WLR）：CSA MC ウォッチ リストに関連付けられる、範囲が 0 ～ 100 の重み（CSA MC での範囲は 0 ～ 35）。

  アラートの攻撃者がウォッチ リストに含まれている場合、その攻撃者のウォッチ リスト レーティングがレーティングに加算されます。

図 8-1 にリスク レーティングの式を示します。

図 8-1　　リスク レーティングの式

$$RR = \frac{ASR * TVR * SFR}{10000} + ARR - PD + WLR$$

191016

脅威レーティングの概要

脅威レーティングは、実行されたイベント アクションによって引き下げられたリスク レーティングです。非ロギング イベント アクションには脅威レーティングの調整があります。すべてのイベント アクションのうち最も大きな脅威レーティングがリスク レーティングから差し引かれます。

イベント アクションには次の脅威レーティングがあります。

- Deny attacker inline：45
- Deny attacker victim pair inline：40
- Deny attacker service pair inline：40
- Deny connection inline：35
- Deny packet inline：35
- Modify packet inline：35
- Request block host：20
- Request block connection：20
- Reset TCP connection：20
- Request rate limit：20

イベント アクションのサマライズ

サマライズを使用すると、基本集約機能として、複数のイベントを 1 つのアラートにまとめることにより、センサーから送信されたアラートの量が軽減されます。また、シグニチャごとに特別なパラメータを指定することにより、アラートの処理方法をさまざまに変更できます。各シグニチャは、優先される通常動作を反映したデフォルト値を使用して作成されます。ただし、各シグニチャの設定を修正することにより、エンジンのタイプごとに定められた制約の範囲内でこのデフォルトの処理方法を調整できます。

アラートを生成しないアクション（拒否、ブロック、TCP リセット）には、サマライズされない各シグニチャ イベントのフィルタが適用されます。アラートを生成するアクションは、これらの集約されたアラートに対しては実行されず、アクションが 1 つのサマライズされたアラートに適用された後、フィルタが適用されます。

アラートを生成する他のアクションのいずれかを選択し、フィルタで除外しない場合、[Product Alert] を選択しない場合であってもアラートが作成されます。アラートが作成されないようにするには、アラートを生成するすべてのアクションをフィルタで除外する必要があります。

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 アクションが処理されます。これにより、センサーは、一連のイベントにまたがって発生する疑わしいアクティビティを監視します。

イベント アクションの集約

基本的な集約には 2 つの動作モードがあります。簡易なモードでは、シグニチャに対し、アラートが送信される前に満たされる必要があるヒット数のしきい値を設定します。一方、高度なモードでは、各インターバルにおけるヒット数がカウントされます。このモードでは、センサーにより秒あたりのヒット数が追跡され、そのしきい値を超えた場合にのみアラートが送信されます。この例で、「ヒット」とはイベントを表すために使用した用語で、基本的にはアラートを指します。ただし、ヒット数がしきい値を超過するまでは、センサーからアラートとして送信されることはありません。

次のサマライズ オプションから選択できます。

- [Fire All]：シグニチャが起動されるたびにアラートが起動されます。サマライズにしきい値が設定されている場合、サマライズが発生するまで実行ごとにアラートが起動されます。サマライズが開始された後は、各アドレス セットについて、サマライズ間隔ごとに 1 つのアラートのみが起動されます。他のアドレス セットのアラートは、すべて発生するか、個別にサマライズされます。そのシグニチャのアラートが一定期間ないと、シグニチャはすべてを起動するモードに戻ります。
- [Summary]：初めてシグニチャがトリガーされたときにアラートが起動され、そのシグニチャの以降のアラートは、要約間隔の間サマライズされます。各アドレスセットについて、要約間隔ごとに 1 個のアラートのみが起動されます。グローバル要約しきい値に達した場合、シグニチャはグローバル サマライズ モードになります。
- [Global Summarization]：要約間隔ごとにアラートを起動します。シグニチャは、グローバル サマライズ用に事前設定できます。
- [Fire Once]：アドレス セットごとにアラートを起動します。このモードはグローバル サマライズ モードにアップグレードできます。

IPS ポリシーの設定

ここでは、IPS ポリシーと、仮想センサー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。

[IPS Policies] ペイン

[IPS Policies] ペインには、上半分に仮想センサーの一覧が表示されます。このペインの上半分では、仮想センサーを追加、編集、削除できます。

仮想センサーごとに、次の情報が表示されます。

- 仮想センサー名
- 割り当てられているインターフェイスまたはペア
- シグニチャ定義ポリシー
- イベント アクション規則オーバーライド ポリシー
  - リスク レーティング
  - 追加するアクション
  - イネーブルまたはディセーブル
- 異常検出ポリシー
- 仮想センサーの説明

（注）　デフォルトの仮想センサーは vs0 です。デフォルトの仮想センサーは削除できません。

ペインの下半分では、ペインの上半分で選択した各仮想センサーのイベント アクション規則を設定できます。イベント アクション規則は、[Configuration] > *sensor_name* > [Policies] > [Event Action rules] > [rules0] ペインでも設定できます。

ペインの [Event Action Rules] 部分には、次のタブが含まれています。

- [Event Action Filters] : イベントから指定を削除するか、イベント全体を廃棄してセンサーによる今後の処理を回避することができます。
- [IPv4 Target Value Rating] : IPv4 ターゲットの価値レーティングをネットワーク資産に割り当てることができます。ターゲットの価値レーティングは、各アラートのリスク レーティング値の計算に使用される要素の 1 つです。
- [IPv6 Target Value Rating] : IPv6 ターゲットの価値レーティングをネットワーク資産に割り当てることができます。ターゲットの価値レーティングは、各アラートのリスク レーティング値の計算に使用される要素の 1 つです。
- [OS Identifications] : IP アドレスを OS タイプに関連付けることができます。これは、センサーが攻撃関連性レーティングを計算するのに役立ちます。
- [Event Variables] : イベント アクション フィルタで使用するイベント変数を作成できます。同じ値を複数のフィルタで使用する場合は、イベント変数を使用できます。
- [Risk Category] : センサーとネットワークの稼動状態をモニタするために使用したり、イベント アクション オーバーライドで使用するための、リスク カテゴリを作成できます。
- [General] : イベント アクション規則に適用されるいくつかのグローバル設定を設定できます。

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。

[IPS Policies] ペインのフィールド定義

[IPS Policies] ペイン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。

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

（注） 仮想センサーを設定するには、管理者またはオペレータであることが必要です。

同じポリシー（たとえば sig0、rules0、および ad0）を、異なる仮想センサーに適用できます。[Add Virtual Sensor] ダイアログボックスには、この仮想センサーに割り当てることができるインターフェイスのみが表示されます。すでに他の仮想センサーに割り当てられているインターフェイスは、このダイアログボックスに表示されません。

また、イベント アクション オーバーライドを仮想センサーに割り当て、次のモードを設定することもできます。

- 異常検出動作モード

  （注） AIP SSC-5 は異常検出をサポートしていません。

- インライン TCP セッション トラッキング モード

  （注） IPS SSP を搭載した Cisco ASA 5585-X は、インライン TCP セッション トラッキング モードをサポートしていません。

- ノーマライザ モード

（注）　IPS SSP を搭載した Cisco ASA 5585-X は、ノーマライザ モードをサポートしていません。

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

- [Virtual Sensor Name]：この仮想センサーの名前。
- [Description]：この仮想センサーの説明。
- [Interfaces]：この仮想センサーのインターフェイスを割り当ておよび削除できます。
  - [Assigned]：インターフェイスまたはインターフェイス ペアが仮想センサーに割り当てられているかどうか。
  - [Name]：仮想センサーに割り当て可能なインターフェイスまたはインターフェイス ペアのリスト（GigabitEthernet または FastEthernet）。
  - [Details]：インライン ペアのインターフェイスのモードのリスト（インライン インターフェイスまたは無差別）。
- [Signature Definition Policy]：この仮想センサーに割り当てるシグニチャ定義ポリシーの名前。デフォルトは sig0 です。
- [Event Action Rules Policy]：この仮想センサーに割り当てるイベント アクション規則ポリシーの名前。デフォルトは rules0 です。
- [Use Event Action Overrides]：オンにした場合、[Add] をクリックして [Add Event Action Override] ダイアログボックスを開き、イベント アクション オーバーライドを設定できます。
  - [Risk Rating]：このオーバーライドのリスク レーティングのレベルを示します。
  - [Actions to Add]：このオーバーライドに追加するアクションを示します。
  - [Enabled]：このオーバーライドがイネーブルかディセーブルかを示します。
- [Anomaly Detection Policy]：この仮想センサーに割り当てる異常検出ポリシーの名前。デフォルトは ad0 です。
- [AD Operational Mode]：この仮想センサーについて、異常検出ポリシーが動作するモード。デフォルトは [Detect] です。
- [Inline TCP Session Tracking Mode]：同じストリームが複数回センサーを通過した場合に、同じストリームに対するビューを複数に分けるために使用されるモード。デフォルト モードは [Virtual Sensor] です。
  - インターフェイスおよび VLAN：同じ VLAN（またはインライン VLAN ペア）内および同じインターフェイス上で同じセッション キー（AaBb）を持つすべてのパケットは、同じセッションに属しています。同じキーを持ち、VLAN が異なるパケットは、別々に追跡されます。
  - VLAN だけ：同じ VLAN（またはインライン VLAN ペア）内で同じセッション キー（AaBb）を持つすべてのパケットは、インターフェイスにかかわらず同じセッションに属しています。同じキーを持ち、VLAN が異なるパケットは、別々に追跡されます。
  - 仮想センサー：仮想センサー内で同じセッション キー（AaBb）を持つすべてのパケットは、同じセッションに属しています。

（注）　IPS SSP を搭載した Cisco ASA 5585-X は、インライン TCP セッション トラッキング モードをサポートしていません。

- [Normalizer Mode]：トラフィックの検査で必要なノーマライザ モードの種類を選択できます。
  - [Strict Evasion Protection]：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。[Strict Evasion Protection] を指定すると、TCP ステートとシーケンスのトラッキングの完全な施行が提供されます。

  （注）　パケットの順序が正しくないか、またはパケットが失われていると、ノーマライザ エンジンのシグニチャ 1300 または 1330 が起動する場合があります。この処理によって状況の修正が試行されますが、結果として接続が拒否されることがあります。

  - [Asymmetric Mode Protection]：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。[Asymmetric Mode Protection] を指定すると、TCP レイヤでの回避防止が緩和されます。

  （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。

  （注）　IPS SSP を搭載した Cisco ASA 5585-X は、ノーマライザ モードをサポートしていません。

[Add Event Action Override] および [Edit Event Action Override] ダイアログボックスのフィールド定義

（注）　イベント アクション オーバーライドを追加または編集するためには、管理者またはオペレータであることが必要です。

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

- [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）を追加できます。設定したリスクに対応するリスク レーティングでイベントが発生した場合、イベント アクションがこのイベントに追加されます。追加モードでは、[Risk Rating] フィールドに入力することで数値範囲を作成できます。編集モードでは、作成したカテゴリを選択できます。
- [Available 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。
- [Assigned]：このオーバーライドにイベント アクションを割り当てることができます。
- [Enabled]：アクションをイネーブルにするにはチェックボックスをオンにします。

（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。

仮想センサーの追加、編集、削除

（注）　トラフィックをモニタする前に、すべてのインターフェイスを仮想センサーに割り当て、イネーブルにする必要があります。

仮想センサーを追加、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] > [IPS Policies] の順に選択し、[Add Virtual Sensor] をクリックします。

ステップ 3　[Virtual Sensor Name] フィールドに、仮想センサーの名前を入力します。

ステップ 4　[Description] フィールドに、この仮想センサーの説明を入力します。

ステップ 5　仮想センサーにインターフェイスを割り当てるには、目的のインターフェイスの横のチェックボックスをオンにし、[Assign] をクリックします。

（注）　[Interfaces] リストには、使用可能なインターフェイスのみが表示されます。他のインターフェイスが存在し、すでに仮想センサーに割り当てられている場合、このリストには現れません。

ステップ 6　ドロップダウン リストからシグニチャ定義ポリシーを選択します。デフォルトの sig0 を使用する場合を除き、[Configuration] > *sensor_name* > [Policies] > [Signature Definitions] > [Add] の順に選択してシグニチャ定義ポリシーを追加しておく必要があります。

ステップ 7　ドロップダウン リストからイベント アクション規則ポリシーを選択します。デフォルトの rules0 を使用する場合を除き、[Configuration] > *sensor_name* > [Policies] > [Event Action Rules] > [Add] の順に選択してイベント アクション規則ポリシーを追加しておく必要があります。

ステップ 8　この仮想センサーにイベント アクション オーバーライドを追加するには、[Use Event Action Overrides] チェックボックスをオンにし、[Add] をクリックします。

（注）　[Use Event Action Overrides] チェックボックスをオンにする必要があります。そうしないと、設定した値にかかわらず、イベント アクション オーバーライドがどれもイネーブルになりません。

a.　[Risk Rating] ドロップダウン リストからリスク レーティングを選択します。

b.　[Assigned] 列で、このイベント アクション オーバーライドに割り当てるアクションの横のチェックボックスをオンにします。

c.　[Enabled] 列で、イネーブルにするアクションの横のチェックボックスをオンにします。

（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。

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

d. [OK] をクリックします。

ステップ 9　ドロップダウン リストから異常検出ポリシーを選択します。デフォルトの ad0 を使用する場合を除き、[Configuration] > *sensor_name* > [Policies] > [Anomaly Detections] > [Add] の順に選択して異常検出ポリシーを追加しておく必要があります。

ステップ 10　ドロップダウン リストから異常検出モード（[Detect]、[Inactive]、[Learn]）を選択します。デフォルトは [Detect] です。

ステップ 11　[Double Arrow] アイコンを選択し、[Advanced Options] のデフォルト値を変更します。

a. センサーがインライン TCP セッションを追跡する方法を選択します（インターフェイスおよび VLAN ごと、VLAN のみ、または仮想センサー）。デフォルトは仮想センサーです。これはほぼ常に最適な選択肢となります。

b. ノーマライザ モードを選択します（厳格な回避保護または非同期モード保護）。

（注）　IPS SSP を搭載した Cisco ASA 5585-X は、ノーマライザ モードをサポートしていません。

ヒント　変更内容を破棄して [Add Virtual Sensor] 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 12　[OK] をクリックします。仮想センサーが [IPS Policies] ペインのリストに表示されます。

ステップ 13　仮想センサーを編集するには、リスト中の仮想センサーを選択し、[Edit] をクリックします。

ステップ 14　必要な変更を行い、[OK] をクリックします。編集後の仮想センサーが [IPS Policies] ペインの上半分にあるリストに表示されます。

ステップ 15　仮想センサーを削除するには、仮想センサーを選択し、[Delete] をクリックします。仮想センサーが [IPS Policies] ペインの上半分に表示されなくなります。

（注）　デフォルトの仮想センサー vs0 は削除できません。

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 16　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。

イベント アクション フィルタの設定

ここでは、イベント アクション フィルタの設定方法について説明します。内容は次のとおりです。

- 「イベント アクション フィルタの追加、編集、削除、イネーブル化、ディセーブル化、移動」（P.8-17）

イベント アクション フィルタの概要

イベント アクション フィルタは順序リストとして処理され、フィルタはリスト内で上下に移動できます。フィルタによって、センサーは、イベントに応答して特定のアクションを実行できます。すべてのアクションを実行したり、イベント全体を削除したりする必要はありません。フィルタは、イベントからアクションを削除することで機能します。1 つのイベントからすべてのアクションを削除するフィルタは、イベントを効率的に消費します。

注意　送信元および宛先 IP アドレスに基づくイベント アクション フィルタは Sweep エンジンでは機能しません。これは、これらのフィルタが、通常のシグニチャとしてフィルタしないためです。送信元および宛先 IP アドレスをスイープ アラートでフィルタするには、Sweep エンジン シグニチャの送信元および宛先 IP アドレス フィルタ パラメータを使用します。

（注）　スイープ シグニチャをフィルタリングする場合は、宛先アドレスをフィルタリングしないことを推奨します。複数の宛先アドレスがある場合、最後のアドレスだけがフィルタとの照合に使用されます。

[Event Action Filters] タブ

特定のアクションをイベントから削除するか、または、イベント全体を廃棄してセンサーによる今後の処理を回避するように、イベント アクション フィルタを設定できます。[Event Variables] ペインで定義した変数を使用して、フィルタに合わせてアドレスをグループ化できます。

（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（$）を付ける必要があります。「$」を付けないと、「`Bad source and destination`」エラーが生じます。

[Event Action Filters] タブのフィールド定義

[Event Action Filters] タブには次のフィールドがあります。

- [Name]：追加するフィルタに名前を付けることができます。フィルタをリスト中で移動したり、必要に応じて非アクティブ リストに移動できるように、フィルタに名前を付ける必要があります。
- [Enabled]：このフィルタがイネーブルかどうかを示します。
- [Sig 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。シグニチャの範囲を入力することもできます。
- [SubSig 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。SubSig 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。subSig ID の範囲を入力することもできます。
- [Attacker (IPv4/IPv6/port)]：攻撃パケットを送信したホストの IP アドレスまたはポートを示します。アドレスまたはポートの範囲を入力することもできます。
- [Victim (IPv4/IPv6/port)]：攻撃者のホストが使用している IP アドレスまたはポートを示します。アドレスまたはポートの範囲を入力することもできます。

- [Risk Rating]：このイベント アクション フィルタをトリガーするために使用されるリスク レーティング範囲を示します（0 ～ 100）。イベントが発生し、そのリスク レーティングがここで設定した最小 - 最大範囲に入っていた場合、イベントはこのイベント フィルタの規則と比較して処理されます。
- [Actions to Subtract]：イベントの条件がイベント アクション フィルタの基準を満たしている場合に、イベントから削除されるアクションを示します。

[Add Event Action Filter] および [Edit Event Action Filter] ダイアログ ボックスのフィールド定義

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

- [Name]：追加するフィルタに名前を付けることができます。フィルタをリスト中で移動したり、必要に応じて非アクティブ リストに移動できるように、フィルタに名前を付ける必要があります。
- [Enabled]：このフィルタをイネーブルにできます。
- [Signature ID]：このシグニチャに割り当てられた一意の数値を示します。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。シグニチャの範囲を入力することもできます。
- [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。サブシグニチャ ID の範囲を入力することもできます。
- [Attacker IPv4 Address]：攻撃パケットを送信したホストの IP アドレスを示します。アドレスの範囲を入力することもできます。
- [Attacker IPv6 Address]：攻撃パケットを送信したホストの攻撃者 IPv6 アドレスの範囲を次の形式で示します。

  <XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

  例：2001:0db8:1234:1234:1234:1234:1234:1234,2001:0db8:1234:1234:1234:1234:1234:8888。範囲の 2 番目の IPv6 アドレスは、最初の IPv6 アドレス以上である必要があります。

  （注）　IPv6 アドレスは、16 進数で表現された 128 ビットであり、コロンにより 8 個の 16 ビット グループに分かれています。先頭のゼロをスキップしたり、中間のゼロのグループを 2 個のコロン（::）で表現できます。アドレスは、プレフィクス 2001:db8 で始める必要があります。

- [Attacker Port]：攻撃者ホストによって使用されるポートを示します。これは、攻撃パケットの発信元のポートです。ポートの範囲を入力することもできます。
- [VictimIPv4 Address]：攻撃対象ホスト（攻撃パケットの受信者）の IP アドレスを示します。アドレスの範囲を入力することもできます。
- [VictimIPv6 Address]：攻撃対象になっているホスト（攻撃パケットの受信者）の攻撃対象 IPv6 アドレスの範囲を次の形式で示します。

  <XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

例：2001:0db8:1234:1234:1234:1234:1234:1234,2001:0db8:1234:1234:1234:1234:1234:8888。範囲の 2 番目の IPv6 アドレスは、最初の IPv6 アドレス以上である必要があります。

（注）　IPv6 アドレスは、16 進数で表現された 128 ビットであり、コロンにより 8 個の 16 ビット グループに分かれています。先頭のゼロをスキップしたり、中間のゼロのグループを 2 個のコロン（::）で表現できます。アドレスは、プレフィクス 2001:db8 で始める必要があります。

- [Victim Port]：攻撃パケットを受信したポートを示します。ポートの範囲を入力することもできます。
- [Risk Rating]：このイベント アクション フィルタをトリガーするために使用されるリスク レーティング範囲を示します（0 ～ 100）。イベントが発生し、そのリスク レーティングがここで設定した最小 - 最大範囲に入っていた場合、イベントはこのイベント フィルタの規則と比較して処理されます。
- [Actions to Subtract]：[Opens the Edit Actions] ダイアログボックスを開きます。このダイアログでは、イベントの条件がイベント アクション フィルタの基準を満たしている場合に、イベントから削除されるアクションを選択できます。
- More Options
  - [Active]：フィルタリング イベントに適用されるように、フィルタ リストにフィルタを追加できます。
  - [OS Relevance]：攻撃が攻撃対象オペレーティング システムに関係しないイベントをフィルタで除外します。
  - [Deny Percentage]：攻撃者拒否機能で拒否するパケットのパーセンテージを決定します。有効な範囲は 0 ～ 100 です。デフォルトは 100% です。
  - [Stop on Match]：このイベントをイベント アクション フィルタ リストの残りのフィルタに対して処理するかどうかを決定します。

    [No] に設定した場合、Stop フラグが見つかるまで残りのフィルタが照合のために処理されます。

    [Yes] の場合、以降の処理は行われません。このフィルタで指定されたアクションは削除され、残りのアクションが実行されます。
  - [Comments]：このフィルタに関連付けられているユーザ コメントを表示します。

イベント アクション フィルタの追加、編集、削除、イネーブル化、ディセーブル化、移動

（注）　グローバル相関インスペクションおよびレピュテーション フィルタリング拒否機能では、IPv6 アドレスがサポートされていません。グローバル相関インスペクションでは、センサーは IPv6 アドレスのレピュテーション データを受信または処理しません。IPv6 アドレスのリスク レーティングは、グローバル相関インスペクション用に変更されません。同様に、ネットワーク参加には、IPv6 アドレスからの攻撃に関するイベント データは含まれていません。また、IPv6 アドレスは拒否リストに表示されません。

（注）　レート制限およびブロッキングは、IPv6 トラフィックではサポートされていません。ブロック アクションまたはレート制限アクションが設定されているシグニチャが IPv6 トラフィックによってトリガーされると、アラートが生成されますが、アクションは実行されません。

イベント アクション フィルタを追加、編集、削除、イネーブル化、ディセーブル化、および移動するには、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] > [IPS Policies] の順に選択します。

ステップ 3　ペインの上半分で、イベント アクション フィルタを追加する仮想センサーをリストから選択します。

ステップ 4　ペインの [Event Action Rules] 部分で、[Event Action Filters] タブをクリックし、[Add] をクリックします。

ステップ 5　[Name] フィールドに、イベント アクション フィルタの名前を入力します。デフォルト名が設定されますが、より意味のある名前に変更できます。

ステップ 6　[Enabled] フィールドで [Yes] オプション ボタンをクリックし、フィルタをイネーブルにします。

ステップ 7　[Signature ID] フィールドに、このフィルタを適用するすべてのシグニチャのシグニチャ ID を入力します。リスト（2001,2004）または範囲（2001–2004）の他、[Event Variables] タブで定義したいずれかの SIG 変数を使用できます。変数の前には $ を付けます。

ステップ 8　[SubSignature ID] フィールドには、このフィルタを適用するシグニチャのサブシグニチャ ID を入力します。

ステップ 9　[Attacker IPv4 Address] フィールドに、送信元ホストの IP アドレスを入力します。[Event Variables] タブで定義した変数を使用できます。変数の前には $ を付けます。また、アドレスの範囲を入力することもできます（例：0.0.0.0-255.255.255.255）。

ステップ 10　Attacker IPv6 Address フィールドに、送信元ホストの攻撃者 IPv6 アドレスの範囲を次の形式で入力します。

<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

範囲の 2 番目の IPv6 アドレスは、最初の IPv6 アドレス以上である必要があります。

（注）　IPv6 アドレスは、16 進数で表現された 128 ビットであり、コロンにより 8 個の 16 ビット グループに分かれています。先頭のゼロをスキップしたり、中間のゼロのグループを 2 個のコロン（::）で表現できます。アドレスは、プレフィクス 2001:db8 で始める必要があります。

[Event Variables] タブで定義した変数を使用することもできます。変数の前には $ を付けます。

ステップ 11　[Attacker Port] フィールドに、攻撃者が攻撃パケットを送信するために使用するポート番号を入力します。

ステップ 12　[Victim IPv4 Address] フィールドに、受信者ホストの IP アドレスを入力します。[Event Variables] タブで変数を定義済みであれば、そのうちの 1 つを使用できます。変数の前には $ を付けます。また、アドレスの範囲を入力することもできます（例：0.0.0.0-255.255.255.255）。

ステップ 13　[Victim IPv6 Address] フィールドに、受信者ホストの IPv6 アドレスの範囲を次の形式で入力します。

<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

範囲の 2 番目の IPv6 アドレスは、最初の IPv6 アドレス以上である必要があります。

（注） IPv6 アドレスは、16 進数で表現された 128 ビットであり、コロンにより 8 個の 16 ビット グループに分かれています。先頭のゼロをスキップしたり、中間のゼロのグループを 2 個のコロン（::）で表現できます。アドレスは、プレフィクス 2001:db8 で始める必要があります。

[Event Variables] タブで定義した変数を使用できます。変数の前には $ を付けます。

ステップ 14 [Victim Port] フィールドに、攻撃対象ホストが攻撃パケットを受信するために使用するポート番号を入力します。

ステップ 15 [Risk Rating] フィールドに、このフィルタのリスク レーティング範囲を入力します。イベントのリスク レーティングが指定した範囲に収まる場合、イベントはこのフィルタの条件に照らして処理されます。

ステップ 16 [Actions to Subtract] フィールドで、メモ アイコンをクリックし、[Edit Actions] ダイアログボックスを開きます。このフィルタでイベントから削除するアクションのチェックボックスをオンにします。

ヒント リストで複数のイベント アクションを選択するには、Ctrl キーを押しながらクリックします。

ステップ 17 [Active] フィールドで、[Yes] オプション ボタンをクリックし、このフィルタをリストに追加して、フィルタリング イベントで有効にします。

ステップ 18 [OS Relevance] ドロップダウン リストで、攻撃対象について特定されたオペレーティング システムにアラートが関連するかどうかを知る必要があるかどうかを選択します。

ステップ 19 [Deny Percentage] フィールドに、拒否攻撃者機能で拒否するパケットのパーセンテージを入力します。デフォルトは 100% です。

ステップ 20 [Stop on Match] フィールドに、次のオプション ボタンのいずれかをクリックします。

a. [Yes]：この特定のフィルタのアクションが削除された後に、Event Action Filters コンポーネントで処理を停止するかどうか。残りのフィルタはすべて処理されないため、イベントから他のアクションを削除できません。

b. [No]：他のフィルタの処理を継続するかどうか。

ステップ 21 [Comments] フィールドに、このフィルタの目的や、このフィルタを特定の方法で設定した理由など、このフィルタとともに保存するコメントを入力します。

ヒント 変更内容を破棄して [Add Event Action Filter] 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 22 [OK] をクリックします。新しいイベント アクション フィルタが [Event Action Filters] タブのリストに表示されます。

ステップ 23 既存のイベント アクション フィルタを編集するには、リストで選択し、[Edit] をクリックします。

ステップ 24 必要な変更を加えます。

ヒント 変更内容を破棄して [Edit Event Action Filter] 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 25 [OK] をクリックします。編集後のイベント アクション フィルタが [Event Action Filters] タブのリストに表示されます。

ステップ 26　イベント アクション フィルタを削除するには、リストで選択し、[Delete] をクリックします。イベント アクション フィルタが [Event Action Filters] タブのリストに表示されなくなります。

ステップ 27　イベント アクション フィルタをリスト中で上下に移動するには、選択し、[Move Up] または [Move Down] 矢印アイコンをクリックします。

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 28　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。

IPv4 ターゲットの価値レーティングの設定

ここでは、IPv4 ターゲットの価値レーティング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。

[IPv4 Target Value Rating] タブ

（注）　ターゲットの価値レーティングを追加、編集、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。

ネットワーク資産にターゲットの価値レーティングを割り当てることができます。ターゲットの価値レーティングは、各アラートのリスク レーティング値の計算に使用される要素の 1 つです。異なるターゲットに異なるターゲットの価値レーティングを割り当てることができます。イベントのリスク レーティングが高いほど、より厳しいシグニチャ イベント アクションがトリガーされます。

[IPv4 Target Value Rating] タブのフィールド定義

[IPv4 Target Value Rating] タブには次のフィールドがあります。

- [Target Value Rating (TVR)]：このネットワーク資産に割り当てる価値を示します。値は、[High]、[Low]、[Medium]、[Mission Critical]、または [No Value] です。
- [Target IP Address]：ターゲットの価値レーティングを使用して優先順位を付けるネットワーク資産の IP アドレスを示します。

[Add Target Value Rating] および [Edit Target Value Rating] ダイアログボックスのフィールド定義

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

- [Target Value Rating (TVR)]：このネットワーク資産に価値を割り当てます。値は、[High]、[Low]、[Medium]、[Mission Critical]、または [No Value] です。
- [Target IPv4 Address(es)]：ターゲットの価値レーティングを使用して優先順位を付けるネットワーク資産の IP アドレスを示します。

IPv4 ターゲットの価値レーティングの追加、編集、および削除

ネットワーク資産の IPv4 ターゲットの価値レーティングを追加、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] > [IPS Policies] の順に選択します。

ステップ 3　[IPS Policies] ペインの上半分で、ターゲットの価値レーティングを設定する仮想センサーを選択します。

ステップ 4　ペインの [Event Action Rules] 部分で、[IPv4 Target Value Rating] タブをクリックし、[Add] をクリックします。

ステップ 5　ターゲットの価値レーティングを新しい資産グループに割り当てるには、次の手順を実行します。

a.　[Target Value Rating (TVR)] ドロップダウン リストからレーティングを選択します。値は [High]、[Low]、[Medium]、[Mission Critical]、または [No Value] です。

b.　[Target IPv4 Address(es)] フィールドに、ネットワーク資産の IP アドレスを入力します。IP アドレスの範囲を入力するには、その範囲の最も小さいアドレス、ハイフン、最も大きいアドレスの順に入力します。例：10.10.2.1-10.10.2.30。

ヒント　変更を破棄して [Add IPv4 Target Value Rating] 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。新しい資産の新しいターゲットの価値レーティングが [IPv4 Target Value Rating] タブのリストに表示されます。

ステップ 7　既存のターゲットの価値レーティングを編集するには、リストで選択し、[Edit] をクリックします。

ステップ 8　必要な変更を加えます。

ヒント　変更を破棄して [Edit IPv4 Target Value Rating] 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。編集したネットワーク資産が [IPv4 Target Value Rating] タブのリストに表示されます。

ステップ 10　ネットワーク資産を削除するには、リスト中で選択し、[Delete] をクリックします。ネットワーク資産が [Ipv4 Target Value Rating] タブの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。

IPv6 ターゲットの価値レーティングの設定

ここでは、IPv6 ターゲットの価値レーティング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。

[IPv6 Target Value Rating] タブ

（注）　ターゲットの価値レーティングを追加、編集、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。

ネットワーク資産にターゲットの価値レーティングを割り当てることができます。ターゲットの価値レーティングは、各アラートのリスク レーティング値の計算に使用される要素の 1 つです。異なるターゲットに異なるターゲットの価値レーティングを割り当てることができます。イベントのリスク レーティングが高いほど、より厳しいシグニチャ イベント アクションがトリガーされます。

[IPv6 Target Value Rating] タブのフィールド定義

[IPv6 Target Value Rating] タブには次のフィールドがあります。

- [Target Value Rating (TVR)]：このネットワーク資産に割り当てる価値を示します。値は、[High]、[Low]、[Medium]、[Mission Critical]、または [No Value] です。
- [Target IP Address]：ターゲットの価値レーティングを使用して優先順位を付けるネットワーク資産の IP アドレスを示します。

[Add Target Value Rating] および [Edit Target Value Rating] ダイアログボックスのフィールド定義

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

- [Target Value Rating (TVR)]：このネットワーク資産に価値を割り当てます。値は、[High]、[Low]、[Medium]、[Mission Critical]、または [No Value] です。
- [Target IPv6 Address(es)]：ターゲットの価値レーティングを使用して優先順位を付けるネットワーク資産の IPv6 アドレスを次の形式で示します。

  <XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

  例：2001:0db8:1234:1234:1234:1234:1234:1234,2001:0db8:1234:1234:1234:1234:1234:8888。範囲の 2 番目の IPv6 アドレスは、最初の IPv6 アドレス以上である必要があります。

（注） IPv6 アドレスは、16 進数で表現された 128 ビットであり、コロンにより 8 個の 16 ビットグループに分かれています。先頭のゼロをスキップしたり、中間のゼロのグループを 2 個のコロン（::）で表現できます。アドレスは、プレフィクス 2001:db8 で始める必要があります。

IPv6 ターゲットの価値レーティングの追加、編集、および削除

（注） グローバル相関インスペクションおよびレピュテーション フィルタリング拒否機能では、IPv6 アドレスがサポートされていません。グローバル相関インスペクションでは、センサーは IPv6 アドレスのレピュテーション データを受信または処理しません。IPv6 アドレスのリスク レーティングは、グローバル相関インスペクション用に変更されません。同様に、ネットワーク参加には、IPv6 アドレスからの攻撃に関するイベント データは含まれていません。また、IPv6 アドレスは拒否リストに表示されません。

（注） レート制限およびブロッキングは、IPv6 トラフィックではサポートされていません。ブロック アクションまたはレート制限アクションが設定されているシグニチャが IPv6 トラフィックによってトリガーされると、アラートが生成されますが、アクションは実行されません。

ネットワーク資産の IPv6 ターゲットの価値レーティングを追加、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] > [IPS Policies] の順に選択します。

ステップ 3　[IPS Policies] ペインの上半分で、ターゲットの価値レーティングを設定する仮想センサーを選択します。

ステップ 4　ペインの [Event Action Rules] 部分で、[IPv6 Target Value Rating] タブをクリックし、[Add] をクリックします。

ステップ 5　ターゲットの価値レーティングを新しい資産グループに割り当てるには、次の手順を実行します。

a. [Target Value Rating (TVR)] ドロップダウン リストからレーティングを選択します。値は [High]、[Low]、[Medium]、[Mission Critical]、または [No Value] です。

b. [Target IPv6 Address(es)] フィールドに、ネットワーク資産の IP アドレスを入力します。

<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

[Event Variables] タブで定義した変数を使用することもできます。変数の前には $ を付けます。範囲の 2 番目の IPv6 アドレスは、最初の IPv6 アドレス以上である必要があります。

（注） IPv6 アドレスは、16 進数で表現された 128 ビットであり、コロンにより 8 個の 16 ビット グループに分かれています。先頭のゼロをスキップしたり、中間のゼロのグループを 2 個のコロン（::）で表現できます。アドレスは、プレフィクス 2001:db8 で始める必要があります。

ヒント 変更を破棄して [Add IPv6 Target Value Rating] 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。新しい資産の新しいターゲットの価値レーティングが [IPv6 Target Value Rating] タブのリストに表示されます。

ステップ 7　既存のターゲットの価値レーティングを編集するには、リストで選択し、[Edit] をクリックします。

ステップ 8　必要な変更を加えます。

ヒント 変更を破棄して [Edit IPv6 Target Value Rating] 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。編集したネットワーク資産が [IPv6 Target Value Rating] タブのリストに表示されます。

ステップ 10　ネットワーク資産を削除するには、リスト中で選択し、[Delete] をクリックします。ネットワーク資産が [IPv6 Target Value Rating] タブの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。

OS ID の設定

ここでは、OS マップ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。

- 「[OS Identifications] タブのフィールド定義」（P.8-27）
- 「[Add Configured OS Map] および [Edit Configured OS Map] ダイアログボックスの定義」（P.8-27）
- 「設定された OS マップの追加、編集、削除、および移動」（P.8-28）

パッシブ OS フィンガープリントについて

パッシブ OS フィンガープリントにより、センサーはホストが稼動している OS を特定できます。センサーはホスト間のネットワーク トラフィックを分析して、これらのホストの OS をその IP アドレスとともに格納します。センサーはネットワーク上で交換される TCP SYN および SYNACK パケットを検査して、OS タイプを特定します。

次に、センサーはターゲット ホスト OS の OS を使用し、リスク レーティングの攻撃関連性レーティング コンポーネントを計算することによって、攻撃対象への攻撃の関連性を決定します。センサーは、攻撃の関連性に基づいて、攻撃に対するアラートのリスク レーティングを変更したり、攻撃のアラートをフィルタリングしたりする場合があります。ここで、リスク レーティングを使用すると、偽陽性アラートの数を減らしたり（IDS モードの利点）、疑わしいパケットを明確にドロップしたり（IPS モードの利点）できます。また、パッシブ OS フィンガープリントでは、攻撃対象 OS、OS ID のソース、および攻撃対象 OS との関連性をアラート内にレポートすることによって、アラート出力が拡張されます。

パッシブ OS フィンガープリントは、次の 3 つのコンポーネントで構成されます。

- Passive OS learning：パッシブ OS ラーニングは、センサーがネットワーク上のトラフィックを監視しているときに行われます。TCP SYN および SYNACK パケットの特性に基づいて、センサーは送信元 IP アドレスのホスト上で稼動している OS を特定します。
- User-configurable OS identification：学習した OS マップよりも優先される OS ホスト マップを設定できます
- Computation of attack relevance rating and risk rating：センサーは OS 情報を使用して攻撃シグニチャのターゲット ホストに対する関連性を決定します。攻撃の関連性は、攻撃アラートのリスク レーティング値を構成する攻撃関連性レーティング コンポーネントです。センサーは、CSA MC からのホスト ポスチャ情報で報告された OS タイプを使用して攻撃関連性レーティングを計算します。

OS 情報には 3 つのソースがあります。センサーは OS 情報のソースを次の順序でランク付けします。

1. 設定された OS マップ：ユーザが入力する OS マップ。

   設定された OS マップはイベント アクション規則ポリシーにあり、1 つ以上の仮想センサーに適用できます。

   （注）　同じ IP アドレスに対し複数のオペレーティング システムを指定できます。リスト中の最後のオペレーティング システムが照合されます。

2. インポートした OS マップ：外部データ ソースからインポートした OS マップ。

   インポートした OS マップはグローバルであり、すべての仮想センサーに適用されます。

   （注）　現在は CSA MC が唯一の外部データ ソースです。

3. 学習した OS マップ：SYN 制御ビットが設定されている TCP パケットのフィンガープリントを介して、センサーが検知した OS マップ。

学習した OS マップは、トラフィックを監視する仮想センサーに対してローカルです。

センサーは、ターゲット IP アドレスの OS を特定する必要がある場合に、設定した OS マップを調べます。ターゲット IP アドレスが設定した OS マップにない場合、センサーはインポートした OS マップを調べます。ターゲット IP アドレスがインポートした OS マップにない場合、センサーは学習した OS マップを調べます。そこでも見つからなかった場合、センサーはターゲット IP の OS を不明として処理します。

（注）　パッシブ OS フィンガープリントはデフォルトでイネーブルになっており、IPS にはシグニチャごとにデフォルトの脆弱な OS リストが含まれています。

パッシブ OS フィンガープリントの設定

パッシブ OS フィンガープリントを使用するために、設定を行う必要はありません。IPS には、各シグニチャについてデフォルトの脆弱な OS のリストが用意されており、パッシブ分析がデフォルトでイネーブルになっています。

パッシブ OS フィンガープリントについて次の側面を設定できます。

- OS マップの定義：OS マップを設定し、重要なシステムで動作している OS の ID を定義することをお勧めします。重要なシステムの OS および IP アドレスが変更される可能性が少ない場合は、OS マップを設定するのが適切です。
- 攻撃関連性レーティング計算を特定の IP アドレス範囲に限定：これにより、攻撃関連性レーティング計算が、保護されたネットワーク上の IP アドレスに限定されます。
- OS マップのインポート：OS マップのインポートは、パッシブ分析を通じて行われる OS ID の学習速度と忠実度を高めるためのメカニズムです。CSA MC などの外部製品インターフェイスがある場合は、そこから OS ID をインポートできます。
- ターゲットの OS 関連性の値を使用したイベント アクション規則フィルタの定義：これは、OS の関連性のみに対してアラートをフィルタするための方法を提供します。
- パッシブ分析のディセーブル化：センサーが新しい OS マップを学習するのを停止します。
- シグニチャ脆弱 OS リストの編集：脆弱 OS リストは、どの OS タイプが各シグニチャに対して脆弱かを指定したものです。デフォルトでは、[General OS] が、脆弱 OS リストを指定しないすべてのシグニチャに適用されます。

[OS Identifications] タブ

（注）　設定済みの OS マップを追加、編集、および削除するためには、管理者またはオペレータであることが必要です。

学習した OS マップよりも優先される OS ホスト マップを設定するには、[OS Identifications] タブを使用します。[OS Identifications] タブで、設定済みの OS マップの追加、編集、および削除を行うことができます。リスト内で OS マップを上下に移動すると、特定の IP アドレスと OS タイプの組み合わせに対する攻撃関連性レーティングおよびリスク レーティングの計算をセンサーが行う順序を変更できます。

また、リスト内で OS マップを上下に移動すると、特定の IP アドレスに関連付けられている OS をセンサーが解決する順序を変更できます。設定した OS マップでは、範囲を設定できます。そのため、ネットワーク 192.168.1.0/24 の場合、次のように定義できます（表 8-1）。

表 8-1　設定された OS マップの例

IP アドレス範囲の設定	OS
192.168.1.1	IOS
192.168.1.2-192.168.1.10、192.168.1.25	UNIX
192.168.1.1-192.168.1.255	Windows

より特定的なマップをリストの先頭に配置する必要があります。IP アドレス範囲設定では重複は許可されませんが、最もリストの先頭に近いエントリが優先されます。

[OS Identifications] タブのフィールド定義

[OS Identifications] タブには次のフィールドがあります。

- [Enable passive OS fingerprinting analysis] : オンにすると、センサーによりパッシブ OS 分析が実行されます。
- [Restrict Attack Relevance Ratings (ARR) to these IP addresses] : OS タイプから特定の IP アドレスへのマッピングを設定し、その IP アドレスの攻撃関連性レーティングをセンサーで計算します。
- [Configured OS Maps] : 設定されている OS マップの属性が表示されます。
  - [Name] : 設定されている OS マップに付けた名前が表示されます。
  - [Active] : この設定された OS マップがアクティブかどうか。
  - [IP Address] : この設定された OS マップの IP アドレス。
  - [OS Type] : この設定された OS マップの OS タイプ。

[Add Configured OS Map] および [Edit Configured OS Map] ダイアログボックスの定義

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

- [Name] : この設定された OS マップの名前。
- [Active] : 設定された OS マップをアクティブまたは非アクティブにします。
- [IP Address] : この設定された OS マップに関連付けられている IP アドレス。設定されている OS マップの IP アドレス（かつ設定されている OS マップのみ）は、IP アドレスのセットおよび IP アドレス範囲になります。次に示すのは、すべて設定された OS マップの有効な IP アドレス値です。
  - 10.1.1.1,10.1.1.2,10.1.1.15
  - 10.1.2.1
  - 10.1.1.1-10.2.1.1,10.3.1.1
  - 10.1.1.1-10.1.1.5
- [OS Type] : IP アドレスに関連付ける次の OS タイプのいずれかを選択できます。

- AIX
- BSD
- General OS
- HP UX
- IOS
- IRIX
- Linux
- Mac OS
- Netware
- その他
- Solaris
- UNIX
- Unknown OS
- Win NT
- Windows
- Windows NT/2K/XP

設定された OS マップの追加、編集、削除、および移動

設定された OS マップを追加、編集、削除、および移動するには、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] > [IPS Policies] の順に選択します。

ステップ 3　[IPS Policies] ペインの上半分で、OS ID を設定する仮想センサーを選択します。

ステップ 4　ペインの [Event Action Rules] 部分で、[OS Identifications] タブをクリックし、[Add] をクリックします。

ステップ 5　[Name] フィールドに設定される OS マップの名前を入力します。

ステップ 6　[Active] フィールドで、[Yes] オプション ボタンをクリックし、この設定される OS マップをリストに追加して有効にします。

ステップ 7　[IP Address] フィールドに、OS にマッピングするホストの IP アドレスを入力します。たとえば、10.10.5.5,10.10.2.1-10.10.2.30 という形式を使用します。

ステップ 8　[OS Type] ドロップダウン リストから、IP アドレスにマッピングする OS を選択します。

ヒント　変更を破棄して [Add Configured OS Map] 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。新たに設定された OS マップが [OS Identifications] タブのリストに表示されます。

ステップ 10　[Enable passive OS fingerprinting analysis] チェックボックスをオンにします。

（注）　[OS Identifications] タブで [Enable passive OS fingerprinting analysis] チェックボックスをオンにしないと、[Add Configured OS Map] ダイアログボックスで設定する値にかかわらず、設定される OS マップがイネーブルになりません。

ステップ 11　設定された OS マップを編集するには、リスト中で選択し、[Edit] をクリックします。

ステップ 12　必要な変更を加えます。

ヒント　変更を破棄して [Edit Configured OS Map] 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 13　[OK] をクリックします。編集後の設定された OS マップが [OS Identifications] タブのリストに表示されます。

ステップ 14　[Enable passive OS fingerprinting analysis] チェックボックスをオンにします。

（注）　[OS Identifications] タブで [Enable passive OS fingerprinting analysis] チェックボックスをオンにしないと、[Edit Configured OS Map] ダイアログボックスで設定する値にかかわらず、設定された OS マップがイネーブルになりません。

ステップ 15　設定された OS マップを削除するには、リスト中で選択し、[Delete] をクリックします。設定された OS マップが [OS Identifications] タブのリストに表示されなくなります。

ステップ 16　設定された OS マップをリスト中で上下に移動するには、移動対象を選択し、[Move Up] または [Move Down] 矢印をクリックします。

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 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。

イベント変数の設定

ここでは、イベント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。

[Event Variables] タブ

（注）　イベント変数を追加、編集、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。

イベント変数を作成し、イベント アクション フィルタでそれらの変数を使用できます。同じ値を複数のフィルタで使用する場合は、変数を使用します。変数の値を変更した場合、その変数を使用するフィルタが新しい値で更新されます。

（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。

IPv4 アドレス

IPv4 アドレスを設定する場合、完全な IP アドレス、範囲、複数の範囲を指定します。

- 10.89.10.10-10.89.10.23
- 10.90.1.1
- 192.56.10.1-192.56.10.255
- 10.1.1.1-10.2.255.255, 10.89.10.10-10.89.10.23

IPv6 アドレス

IPv6 アドレスを設定する場合は、次の形式を使用します。

<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

（注）　IPv6 アドレスは、16 進数で表現された 128 ビットであり、コロンにより 8 個の 16 ビット グループに分かれています。先頭のゼロをスキップしたり、中間のゼロのグループを 2 個のコロン（::）で表現できます。アドレスは、プレフィクス 2001:db8 で始める必要があります。

ワンポイントアドバイス　エンジニアリング グループに割り当てられる IP アドレス スペースがあり、そのグループに Windows システムが存在せず、そのグループに対する Windows 関連の攻撃を心配する必要がない場合、変数をそのエンジニアリング グループの IP アドレス スペースとして設定できます。次に、この変数を使用して、このグループに対するすべての Windows 関連の攻撃を無視するフィルタを設定できます。

[Event Variables] タブのフィールド定義

[Event Variables] タブには次のフィールドがあります。

- [Name]：この変数の名前を割り当てることができます。
- [Type]：変数をアドレスとして識別します。
- [Value]：この変数によって表される値を追加できます。

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

[Add Event Variable] および [Edit Event 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]：この変数の名前を割り当てることができます。
- [Type]：変数を IPv4 または IPv6 アドレスとして識別します。
  - [address]：IPv4 アドレスの場合は、完全な IP アドレス、範囲、複数の範囲を使用します。
  - [ipv6-address]：IPv6 アドレスの場合は次の形式を使用します。

    <XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

    （注）　IPv6 アドレスは、16 進数で表現された 128 ビットであり、コロンにより 8 個の 16 ビット グループに分かれています。先頭のゼロをスキップしたり、中間のゼロのグループを 2 個のコロン（::）で表現できます。アドレスは、プレフィクス 2001:db8 で始める必要があります。

  - [Value]：この変数によって表される値を追加できます。

イベント変数の追加、編集、削除

（注）　グローバル相関インスペクションおよびレピュテーション フィルタリング拒否機能では、IPv6 アドレスがサポートされていません。グローバル相関インスペクションでは、センサーは IPv6 アドレスのレピュテーション データを受信または処理しません。IPv6 アドレスのリスク レーティングは、グローバル相関インスペクション用に変更されません。同様に、ネットワーク参加には、IPv6 アドレスからの攻撃に関するイベント データは含まれていません。また、IPv6 アドレスは拒否リストに表示されません。

（注）　レート制限およびブロッキングは、IPv6 トラフィックではサポートされていません。ブロック アクションまたはレート制限アクションが設定されているシグニチャが IPv6 トラフィックによってトリガーされると、アラートが生成されますが、アクションは実行されません。

イベント変数を追加、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] > [IPS Policies] の順に選択します。

ステップ 3　[IPS Policies] ペインの上半分で、イベント変数を設定する仮想センサーを選択します。

ステップ 4　ペインの [Event Action Rules] 部分で、[Event Variables] タブをクリックし、[Add] をクリックします。

ステップ 5　[Name] フィールドにこの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 6　[Type] ドロップダウン リストから、IPv4 アドレスの場合は [address] を選択し、IPv6 のアドレスの場合は [ipv6-address] を選択します。

ステップ 7　[Value] フィールドにこの変数の値を入力します。

IPv4 アドレスの場合、完全な IP アドレス、範囲、複数の範囲を指定します。例：

- 10.89.10.10-10.89.10.23
- 10.90.1.1
- 192.56.10.1-192.56.10.255

（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。

IPv6 アドレスの場合は次の形式を使用します。

<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

（注）　IPv6 アドレスは、16 進数で表現された 128 ビットであり、コロンにより 8 個の 16 ビット グループに分かれています。先頭のゼロをスキップしたり、中間のゼロのグループを 2 個のコロン（::）で表現できます。アドレスは、プレフィクス 2001:db8 で始める必要があります。

ヒント　変更内容を破棄して [Add Event 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 8　[OK] をクリックします。新しい変数が [Event Variables] タブのリストに表示されます。

ステップ 9　既存の変数を編集するには、リストで選択し、[Edit] をクリックします。

ステップ 10　必要な変更を加えます。

ヒント　変更内容を破棄して [Edit Event 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 11　[OK] をクリックします。編集したイベント変数が [Event Variables] タブのリストに表示されます。

ステップ 12　イベント変数を削除するには、リストで選択し、[Delete] をクリックします。イベント変数が [Event Variables] タブの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 13　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。

リスク カテゴリの設定

ここでは、リスク カテゴリの設定方法について説明します。内容は次のとおりです。

[Risk Category] タブ

（注）　リスク レベルを追加および編集するには、管理者であることが必要です。

[Risk Category] タブで、定義済みのリスク カテゴリ（HIGHRISK、MEDIUMRISK、および LOWRISK）を使用するか、独自のラベルを定義できます。リスク カテゴリは、カテゴリ名を、リスク レーティングを定義する数値の範囲にリンクします。範囲を連続したものにするには、カテゴリに低いしきい値を指定します。上位のカテゴリは、次に高いカテゴリまたは 100 です。

その後、脅威を赤、黄、緑のカテゴリにグループ分けできます。これらの赤、黄、緑のしきい値統計情報は、イベント アクション オーバーライドで使用され、[Home] ページの [Network Security Gadget] にも表示されます。

（注）　定義済みのリスク カテゴリは削除できません。

赤、黄、緑のしきい値統計情報は、ネットワーク セキュリティの状態を表し、赤が最も重大です。しきい値を変更した場合、リスク カテゴリと同じ範囲のすべてのイベント アクション オーバーライドが、新しい範囲を反映するように変更されます。

新しいカテゴリは、そのしきい値に従って [Risk Category] リストに挿入され、その範囲をカバーするアクションが自動的に割り当てられます。

[Risk Category] タブのフィールド定義

[Risk Category] タブには次のフィールドがあります。

- [Risk Category Name]：このリスク レベルの名前。定義済みのカテゴリには次の値があります。

  - HIGHRISK：90（90 ～ 100）
  - MEDIUMRISK：70（70 ～ 89）
  - LOWRISK：1（1 ～ 69）
- [Risk Threshold]：このリスクのしきい値。値は 0 ～ 100 の数字です。
- [Risk Range]：このリスク カテゴリのリスク レーティング範囲。リスク レーティングとは、ネットワーク上の特定のイベントに関連付けられたリスクを数値化した、0 ～ 100 の範囲の値です。
- [Network Security Health Statistics]：赤、黄、緑のしきい値の数を一覧表示します。ネットワーク全体のセキュリティ値は、最も安全でない値（緑が最も安全で赤が最も安全でない）を表します。これらの色しきい値は、[Home] ペインの [Sensor Health] ガジェットを参照します。
  - Red Threat Threshold
  - Yellow Threat Threshold
  - Green Threat Threshold

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

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

- [Risk Name]：このリスク レベルの名前。
- [Risk Threshold]：このリスク レベルのリスクしきい値を割り当てることができます。リスク カテゴリが連続したものになるように、カテゴリの下限しきい値のみを指定または変更できます。上限しきい値は、次に高いカテゴリまたは 100 です。
- [Active]：このリスク レベルをアクティブにします。

リスク カテゴリの追加、編集、削除

リスク カテゴリを追加、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] > [IPS Policies] の順に選択します。

ステップ 3　[IPS Policies] ペインの上半分で、リスク カテゴリを設定する仮想センサーを選択します。

ステップ 4　ペインの [Event Action Rules] 部分で、[Risk Category] タブをクリックし、[Add] をクリックします。

ステップ 5　[Risk Name] フィールドに、このリスク カテゴリの名前を入力します。

ステップ 6　[Risk Threshold] フィールドに、リスクしきい値の数値（最小 0、最大 100）を入力します。この数値はリスクの下限を表します。範囲は [Risk Range] フィールドと、赤、黄、緑のしきい値フィールドに表示されます。

ステップ 7　このリスク カテゴリをアクティブにするには、[Yes] オプション ボタンをクリックします。

ヒント　変更内容を破棄して [Add Risk Category] 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] をクリックします。新しいリスク カテゴリが [Risk Category] タブのリストに表示されます。

ステップ 9　既存のリスク カテゴリを編集するには、リストで選択し、[Edit] をクリックします。

ステップ 10　必要な変更を加えます。

ヒント　変更内容を破棄して [EditRisk Category] 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 11　[OK] をクリックします。編集したリスク カテゴリが [Risk Category] タブのリストに表示されます。

ステップ 12　リスク カテゴリを削除するには、リスト中で選択し、[Delete] をクリックします。リスク カテゴリが [Risk Category] タブの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 13　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。

一般設定

ここでは、一般的な設定を行う方法について説明します。内容は次のとおりです。

[General] タブ

（注）　イベント アクション規則の一般的な設定を行うには、管理者またはオペレータであることが必要です。

Summarizer や Meta Event Generator を使用するかどうかなど、イベント アクション規則全体に適用される一般的な設定を行うことができます。Summarizer はイベントを単一アラートにグループ化するため、センサーが送信するアラートの数が減少します。Meta Event Generator はコンポーネント イベントを処理します。これによって、センサーは一連のイベントで疑わしいアクティビティが発生していないかどうかを監視できます。

注意　トラブルシューティング目的以外では、Summarizer または Meta Event Generator をディセーブルにしないでください。Summarizer をディセーブルにすると、すべてのシグニチャがサマライズなしの [Fire All] に設定されます。Meta Event Generator をディセーブルにすると、すべてのメタ エンジン シグニチャがディセーブルになります。

また、脅威レーティングの調整、イベント アクション フィルタの使用、一方向の TCP リセットのイネーブル化を行うこともできます。一方向の TCP リセットはインライン モードでだけ動作し、Deny Packet Inline アクションに自動追加されます。TCP リセットがアラートの攻撃対象に送信されるため、攻撃者に対してブラック ホールが作成され、攻撃対象の TCP リソースがクリアされます。

（注）　これにより、インライン センサーで、リスク レーティングが 90 以上のアラートのパケットを拒否されるようになります。また、リスク レーティングが 90 以上の TCP アラートで、一方向 TCP リセットを発行します。

攻撃者を拒否する期間、拒否攻撃者の最大数、ブロックの継続期間を設定できます。

[General] タブのフィールド定義

[General] タブには次のフィールドがあります。

- [Use Summarizer] : Summarizer コンポーネントをイネーブルにします。

  デフォルトでは、Summarizer はイネーブルになります。ディセーブルにすると、すべてのシグニチャがサマライズなしの [Fire All] に設定されます。サマライズするように個別のシグニチャを設定しても、この設定は Summarizer がイネーブルになっていない場合は無視されます。

- [Use Meta Event Generator] : Meta Event Generator をイネーブルにします。

  デフォルトでは、Meta Event Generator はイネーブルになります。Meta Event Generator をディセーブルにすると、すべてのメタ エンジン シグニチャがディセーブルになります。

- [Use Threat Rating Adjustment] : 脅威レーティングの調整がイネーブルになり、これによってリスク レーティングが調整されます。ディセーブルにすると、リスク レーティングは脅威レーティングと等しくなります。

- [Use Event Action Filters] : イベント アクション フィルタ コンポーネントをイネーブルにします。イネーブルになっているいずれかのフィルタを使用するには、このチェックボックスをオンにする必要があります。

- [Enable One Way TCP Reset] :（インラインのみ）TCP ベースのアラートで、拒否パケット インライン アクションの一方向の TCP リセットをイネーブルにします。TCP リセットがアラートの攻撃対象に送信されるため、攻撃対象の TCP リソースがクリアされます。

- [Deny Attacker Duration] : 攻撃者をインラインで拒否する秒数。有効な範囲は 0 ～ 518400 です。デフォルトは 3600 です。

- [Block Action Duration] : ホストまたは接続をブロックする時間（分単位）。有効な範囲は 0 ～ 10000000 です。デフォルトは 30 です。

- [Maximum Denied Attackers] : 一度にシステム内に許容できる拒否攻撃者の数を制限します。有効な範囲は 0 ～ 100000000 です。デフォルトは 10000 です。

一般的な設定

注意　一般設定オプションはグローバル レベルで動作するため、イネーブルにするとこれらの機能のすべてのセンサー処理に影響があります。

イベント アクション規則の一般的な設定を行うには、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] > [IPS Policies] の順に選択します。

ステップ 3　[IPS Policies] ペインの上半分で、一般的なカテゴリを設定する仮想センサーを選択します。

ステップ 4　ペインの [Event Action Rules] 部分で、[General] タブをクリックします。

ステップ 5　Summarizer の機能をイネーブルにするには、[Use Summarizer] チェックボックスをオンにします。

注意　Summarizer は、トラブルシューティング目的でのみディセーブルにします。それ以外の場合は、サマライズ用に設定したすべてのシグニチャが実際にサマライズされるように、Summarizer をイネーブルにしてください。

ステップ 6　Meta Event Generator をイネーブルにするには、[Use Meta Event Generator] チェックボックスをオンにします。

注意　Meta Event Generator は、トラブルシューティング目的でのみディセーブルにします。それ以外の場合は、すべての Meta エンジンのシグニチャが機能するように、Meta Event Generator をイネーブルにしてください。

ステップ 7　脅威レーティング調整をイネーブルにするには、[Use Threat Rating Adjustment] チェックボックスをオンにします。

ステップ 8　イベント アクション フィルタをイネーブルにするには、[Use Event Action Filters] チェックボックスをオンにします。

（注）　[Configuration] > se*nsor_name* > [Policies] > [IPS Policies] > [Event Action Filters] ペインで設定したイベント アクション フィルタがアクティブになるように、[General] ペインの [Use Event Action Filters] チェックボックスをオンにする必要があります。

ステップ 9　拒否パケット インライン アクションで一方向の TCP リセットをイネーブルにするには、[Enable One Way TCP Reset] チェックボックスをオンにします。

ステップ 10　[Deny Attacker Duration] フィールドに、攻撃者をインラインで拒否する秒数を入力します。

ステップ 11　[Block Action Duration] フィールドに、ホストまたは接続をブロックする期間を分単位で入力します。

ステップ 12　[Maximum Denied Attackers] フィールドに、同時に拒否する拒否攻撃者の最大数を入力します。

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 13　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。

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」（P.9-38）
- 「AIC エンジンのセンサーのパフォーマンス」（P.9-38）
- 「AIC 要求メソッドのシグニチャ」（P.9-39）

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。

CHAPTER 10

Custom Signature Wizard の使用

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

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

この章では、Custom Signature Wizard について、およびこのウィザードを使用してカスタム シグニチャを作成する方法について説明します。内容は次のとおりです。

Custom Signature Wizard について

（注） カスタム シグニチャを作成するには、管理者またはオペレータである必要があります。

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

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

詳細情報

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

シグニチャ エンジンの使用

次のシーケンスは、シグニチャ エンジンを使用してカスタム シグニチャを作成する場合に適用されます。

ステップ 1　シグニチャ エンジンを選択します。

- Atomic IP
- Atomic IP Advanced
- Service HTTP
- Service MSRPC
- Service RPC
- State（SMTP など）
- String ICMP
- String TCP
- String UDP
- Sweep

ステップ 2　シグニチャ識別パラメータを割り当てます。

- シグニチャ ID
- サブシグニチャ ID
- シグニチャ名
- アラート注釈（任意）
- ユーザ コメント（任意）

ステップ 3　エンジン固有のパラメータを割り当てます。

各エンジンに適用されるマスター パラメータのグループはありますが、パラメータはシグニチャ エンジンごとに異なります。

ステップ 4　アラート応答を割り当てます。

- シグニチャ忠実度レーティング
- アラートの重大度

ステップ 5　アラートの動作を割り当てます。デフォルトのアラートの動作を受け入れることができます。変更するには、[Advanced] をクリックします。Advanced Alert Behavior ウィザードが開きます。このウィザードを使用して、このシグニチャのアラートの処理方法を設定できます。

ステップ 6　[Finish] をクリックします。

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

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

- AIC FTP
- AIC HTTP
- Atomic ARP
- Atomic IP6
- Fixed ICMP
- Fixed TCP
- Fixed UDP
- Flood Host
- Flood Net
- Meta
- Multi String
- Normalizer
- Service DNS
- Service FTP
- Service Generic
- Service H225
- Service IDENT
- Service MSSQL
- Service NTP
- Service P2P
- Service SMB Advanced
- Service SNMP
- Service SSH
- Service TNS
- String XL ICMP
- String XL TCP
- String XL UDP
- Traffic ICMP
- Traffic Anomaly
- Trojan Bo2k
- Trojan Tfn2k
- Trojan UDP

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

詳細情報

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

シグニチャ エンジンを使用しない方法

次のシーケンスは、シグニチャ エンジンを使用せずにカスタム シグニチャを作成する場合に適用されます。

ステップ 1　使用するプロトコルを指定します。

- IP：ステップ 3 に進みます。
- ICMP：ステップ 2 に進みます。
- UDP：ステップ 2 に進みます。
- TCP：ステップ 2 に進みます。

ステップ 2　ICMP および UDP プロトコルの場合は、トラフィック タイプと検査データ タイプを選択します。TCP プロトコルの場合は、トラフィック タイプを選択します。

ステップ 3　シグニチャ識別パラメータを割り当てます。

- シグニチャ ID
- サブシグニチャ ID
- シグニチャ名
- アラート注釈（任意）
- ユーザ コメント（任意）

ステップ 4　エンジン固有のパラメータを割り当てます。各エンジンに適用されるマスター パラメータのグループはありますが、パラメータはシグニチャ エンジンごとに異なります。

ステップ 5　アラート応答を割り当てます。

- シグニチャ忠実度レーティング
- アラートの重大度

ステップ 6　アラートの動作を割り当てます。デフォルトのアラートの動作を受け入れることができます。変更するには、[Advanced] をクリックします。Advanced Alert Behavior ウィザードが開きます。このウィザードを使用して、このシグニチャのアラートの処理方法を設定できます。

ステップ 7　[Finish] をクリックします。

カスタム シグニチャの作成

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

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

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

Custom Signature Wizard は、カスタム シグニチャを設定する手順をステップバイステップで案内します。

Custom Signature Wizard を使用してカスタム シグニチャを作成するには、次の手順を実行します。

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

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

ステップ 3　新しいシグニチャの作成に使用するシグニチャ エンジンがわかっている場合は、[Yes] オプション ボタンをクリックし、[Select Engine] ドロップダウン リストからエンジンを選択して、[Next] をクリックします。手順 12 に進みます。使用するエンジンがわからない場合は、[No] オプション ボタンをクリックして、[Next] をクリックします。

ステップ 4　このシグニチャで検査するトラフィックのタイプと一致するオプション ボタンをクリックし、[Next] をクリックします。

- IP（IP の場合はステップ 12 に進みます）。
- ICMP（ICMP の場合はステップ 5 に進みます）。
- UDP（UDP の場合はステップ 6 に進みます）。
- TCP（TCP の場合はステップ 8 に進みます）。

ステップ 5　[ICMP Traffic Type] ウィンドウで、次のオプション ボタンの 1 つをクリックし、[Next] をクリックします。

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

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

- [Single Packet]：Atomic IP エンジン（ヘッダー データ用）または String UDP エンジンを使用して 1 つのパケットで攻撃を検査するシグニチャを作成しています。ステップ 11 に進みます。
- [Sweeps]：シグニチャに Sweep エンジンを使用してスイープ攻撃を検出するシグニチャを作成しています。ステップ 7 に進みます。

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

- [Host Sweep]：スイープを使用して、ホスト上の開いたポートを検索するシグニチャを作成しています。新しいシグニチャの作成に Sweep エンジンが使用され、ストレージ キーは Axxx に設定されます。ステップ 12 に進みます。
- [Port Sweep]：スイープを使用してネットワーク上のホストを検索するシグニチャを作成しています。新しいシグニチャの作成に Sweep エンジンが使用され、ストレージ キーは AxBx に設定されます。ステップ 12 に進みます。

ステップ 8　[TCP Traffic Type] ウィンドウで、次のオプション ボタンの 1 つをクリックし、[Next] をクリックします。

- [Single Packet]：1 つのパケットで攻撃を検査するシグニチャを作成しています。シグニチャの作成には Atomic IP エンジンが使用されます。ステップ 12 に進みます。
- [Single TCP Connection]：1 つの TCP 接続で攻撃を検出するシグニチャを作成しています。ステップ 9 に進みます。
- [Multiple Connections]：複数の接続で攻撃を検査するシグニチャを作成しています。ステップ 10 に進みます。

ステップ 9　[Service Type] ウィンドウで、次のオプション ボタンの 1 つをクリックして、[Next] をクリックし、ステップ 12 に進みます。

- [HTTP]：HTTP サービスを使用する攻撃を検出するシグニチャを作成しています。シグニチャの作成には Service HTTP エンジンが使用されます。
- [SMTP]：SMTP サービスを使用する攻撃を検出するシグニチャを作成しています。シグニチャの作成には SMTP エンジンが使用されます。
- [RPC]：RPC サービスを使用する攻撃を検出するシグニチャを作成しています。シグニチャの作成には Service RPC エンジンが使用されます。
- [MSRPC]：MSRPC サービスを使用する攻撃を検出するシグニチャを作成しています。シグニチャの作成には Service MSRPC エンジンが使用されます。
- [Other]：HTTP、SMTP、RPC 以外のサービスを使用する攻撃を検出するシグニチャを作成しています。シグニチャの作成には String TCP エンジンが使用されます。

ステップ 10　[TCP Sweep Type] ウィンドウで、次のオプション ボタンの 1 つをクリックして、[Next] をクリックし、ステップ 12 に進みます。

- [Host Sweep]：スイープを使用して、ホスト上の開いたポートを検索するシグニチャを作成しています。シグニチャの作成に Sweep エンジンが使用され、ストレージ キーは Axxx に設定されます。
- [Port Sweep]：スイープを使用してネットワーク上のホストを検索するシグニチャを作成しています。新しいシグニチャの作成に Sweep エンジンが使用され、ストレージ キーは AxBx に設定されます。

ステップ 11　1 つのパケットの場合は、[Inspect Data] ウィンドウで次のオプション ボタンの 1 つをクリックし、[Next] をクリックしてステップ 12 に進みます。

- [Header Data Only]：センサーで検査するパケットの部分としてヘッダーを指定します。
- [Payload Data Only]：センサーで検査するパケットの部分としてペイロードを指定します。

ステップ 12　[Signature Identification] ウィンドウで、このシグニチャを一意で識別する属性を指定し、[Next] をクリックします。

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

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

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

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

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

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

ステップ 13　エンジン固有のパラメータに値を割り当て、[Next] をクリックします。

ステップ 14　[Alert Response] ウィンドウで、次のアラート応答オプションを指定します。

a. [Signature Fidelity Rating] フィールドに値を入力します。シグニチャ忠実度レーティングの有効値は 0 ～ 100 で、シグニチャに対する信頼度を示します。100 が最も信頼度が高いことを示します。

b. [Severity of the Alert] ドロップダウン リストから、センサーがアラートを送信する際にイベント ビューアで報告する重大度を選択します。

- High
- Informational
- Low
- Medium

ステップ 15　デフォルトのアラートの動作を受け入れるには、[Finish] をクリックして、ステップ 22 に進みます。デフォルトのアラートの動作を変更するには、[Advanced] をクリックして、ステップ 16 に進みます。

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

ステップ 16　イベント カウント、キー、および間隔を設定します。

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

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

c. アラート率に基づいてイベントをカウントする場合は、[Use Event Interval] チェックボックスをオンにして、[Event Interval (seconds)] フィールドに、間隔として使用する秒数を入力します。

d. [Next] をクリックして続行します。[Alert Summarization] ウィンドウが表示されます。

ステップ 17　アラートの量を制御し、センサーでアラートをどのようにサマライズするかを設定するには、次のオプション ボタンの 1 つをクリックします。

- [Alert Every Time the Signature Fires] : シグニチャが悪意のあるトラフィックを検出するたびにセンサーからアラートを送信するように指定します。その後、アラートの量をダイナミックに調整できる追加しきい値を指定できます。ステップ 18 に進みます。
- [Alert the First Time the Signature Fires] : シグニチャが初めて悪意のあるトラフィックを検出したときにセンサーからアラートを送信するように指定します。その後、アラートの量をダイナミックに調整できる追加しきい値を指定できます。ステップ 19 に進みます。
- [Send Summary Alerts] : シグニチャが起動されるたびにアラートを送信せず、センサーからこのシグニチャのサマリー アラートのみを送信するように指定します。その後、アラートの量をダイナミックに調整できる追加しきい値を指定できます。ステップ 20 に進みます。
- [Send Global Summary Alerts] : 1 つのアドレス セットで初めてシグニチャが起動されたときにセンサーからアラートを送信し、その後、指定した時間間隔ですべてのアドレス セットに関するすべてのアラートのサマリーを含むグローバル サマリー アラートのみを送信するように指定します。ステップ 21 に進みます。

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

ステップ 18　[Alert Every Time the Signature Fires] オプションを設定します。

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

b. ダイナミック サマライズを使用するには、[Use Dynamic Summarization] チェックボックスをオンにします。ダイナミック サマライズでは、センサーは、設定したサマリー パラメータに基づいて送信するアラートの量をダイナミックに調整できます。

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

d. [Summary Interval (seconds)] フィールドに、時間間隔に使用する秒数を入力します。

e. センサーをグローバル サマライズ モードにするには、[Specify Global Summary Threshold] チェックボックスをオンにします。

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

ステップ 19　[Alert the First Time the Signature Fires] オプションを設定します。

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

b. センサーでダイナミック グローバル サマライズを使用するには、[Use Dynamic Global Summarization] チェックボックスをオンにします。

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

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

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

ステップ 20　[Send Summary Alerts] オプションを設定します。

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

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

c. センサーでダイナミック グローバル サマライズを使用するには、[Use Dynamic Global Summarization] チェックボックスをオンにします。

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

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

ステップ 21　[Global Summary Interval (seconds)] フィールドに、センサーがサマライズするイベントをカウントする秒数を入力します。

ステップ 22　[Finish] をクリックして、アラート動作の変更を保存します。

ステップ 23　[Finish] をクリックして、カスタム シグニチャを保存します。

ステップ 24　[Yes] をクリックして、カスタム シグニチャを作成します。作成したシグニチャがイネーブルになり、シグニチャのリストに追加されます。

ヒント　変更を破棄するには、[Cancel] をクリックします。

Custom Signature Wizard のフィールド定義

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

[Welcome] ウィンドウ

Custom Signature Wizard の [Welcome] ウィンドウには次のフィールドがあります。

- [Yes]：[Select Engine] フィールドがアクティブになり、シグニチャ エンジンのリストから選択できます。
- [Select Engine]：使用可能なシグニチャ エンジンのリストを表示します。シグニチャの作成に使用するシグニチャ エンジンがわかっている場合は [Yes] をクリックし、ドロップダウン リストからエンジンのタイプを選択します。
  - [Atomic IP]：Atomic IP シグニチャを作成できます。
  - [Service HTTP]：HTTP トラフィック用のシグニチャを作成できます。
  - [Service MSRPC]：MSRPC トラフィック用のシグニチャを作成できます。
  - [Service RPC]：RPC トラフィック用のシグニチャを作成できます。
  - [State SMTP]：SMTP トラフィック用のシグニチャを作成できます。
  - [String ICMP]：ICMP 文字列用のシグニチャを作成できます。
  - [String TCP]：TCP 文字列用のシグニチャを作成できます。
  - [String UDP]：UDP 文字列用のシグニチャを作成できます。
  - [Sweep]：スイープ用のシグニチャを作成できます。

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

[Protocol Type] ウィンドウ

特定のプロトコルで悪意のある動作を探すシグニチャを定義できます。シグニチャで次のプロトコルをデコードし、検査できます。

- IP
- ICMP
- UDP
- TCP

フィールド定義

Custom Signature Wizard の [Protocol Type] ウィンドウには次のフィールドがあります。

- [IP] : IP トラフィックをデコードおよび検査するシグニチャを作成します。
- [ICMP] : ICMP トラフィックをデコードおよび検査するシグニチャを作成します。
- [UDP] : UDP トラフィックをデコードおよび検査するシグニチャを作成します。
- [TCP] : TCP トラフィックをデコードおよび検査するシグニチャを作成します。

[Signature Identification] ウィンドウ

シグニチャ識別パラメータはシグニチャを説明しますが、シグニチャの動作には影響を与えません。シグニチャ ID、サブシグニチャ ID、およびシグニチャ名が必要です。その他のフィールドはオプションです。

フィールド定義

カスタム シグニチャ ウィンドウの [Signature Identification] ウィンドウには、次のフィールドがあります。

- [Signature ID] : このシグニチャに割り当てられた一意の数値を示します。シグニチャ ID により、センサーは特定のシグニチャを識別できます。アラートが生成されると、シグニチャ ID がイベント ビューアに報告されます。有効な範囲は、60000 ～ 65000 です。
- [SubSignature ID] : このサブシグニチャに割り当てられた一意の数値を示します。サブシグニチャ ID によって、広範なシグニチャのより詳細なバージョンが識別されます。有効な値は 0 ～ 255 です。アラートが生成されると、サブシグニチャがイベント ビューアに報告されます。
- [Signature Name] : このシグニチャに割り当てられた名前を示します。アラートが生成されると、イベント ビューアに報告されます。
- [Alert Notes] :（任意）このシグニチャが起動されたときに、アラートに関連付けられるテキストを指定します。アラートが生成されると、イベント ビューアに報告されます。
- [User Comments] :（任意）シグニチャ パラメータとともに格納する、このシグニチャに関するメモまたはその他のコメントを指定します。

[Service MSRPC Engine Parameters] ウィンドウ

Service MSRPC エンジンは、MSRPC パケットを処理します。MSRPC は、ネットワーク環境での複数のコンピュータ間の連携処理と、使用されるアプリケーション ソフトウェアに対応しています。MSRPC はトランザクションベースのプロトコルです。チャネルを確立し、処理要求および応答を受け渡す一連の通信が発生します。

MSRPC は、ISO レイヤ 5 および 6 のプロトコルで、UDP、TCP、SMB などの他のトランスポート プロトコルの上の階層となります。MSRPC エンジンには、MSRPC PDU のフラグメンテーションと再構成を処理する機能も含まれます。

この通信チャネルは、最近の Windows NT、Windows 2000、および Window XP のセキュリティ脆弱性の原因となっています。Service MSRPC エンジンは、最も一般的なトランザクション タイプについて DCE および RPC プロトコルをデコードするだけです。

フィールド定義

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

- [Event Action]：このシグニチャが検出されたときにセンサーで実行するアクションを指定します。デフォルトは [Produce Alert] です。

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

- [Specify Regex String]：（任意）最小および最大一致オフセット、正規表現文字列、最小一致長さを含む完全一致オフセットを指定できます。
- [Protocol]：プロトコルとして TCP または UDP を指定できます。
- [Specify Operation]：（任意）演算を指定できます。
- [Specify UUID]：（任意）UUID を指定できます。

詳細情報

- MSRPC エンジンの詳細については、「Service MSRPC エンジン」（P.B-50）を参照してください。
- シグニチャの正規表現構文を記載した表については、「正規表現の構文」（P.B-10）を参照してください。

[ICMP Traffic Type] ウィンドウ

Custom Signature Wizard の [ICMP Traffic Type] ウィンドウには次のフィールドがあります。

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

[Inspect Data] ウィンドウ

Custom Signature Wizard の [Inspect Data] ウィンドウには次のフィールドがあります。

- [Header Data Only]：センサーで検査するパケットの部分としてヘッダーを指定します。
- [Payload Data Only]：センサーで検査するパケットの部分としてペイロードを指定します。

[UDP Traffic Type] ウィンドウ

Custom Signature Wizard の [UDP Traffic Type] ウィンドウには次のフィールドがあります。

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

[UDP Sweep Type] ウィンドウ

Custom Signature Wizard の [UDP Sweep Type] ウィンドウには次のフィールドがあります。

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

[TCP Traffic Type] ウィンドウ

Custom Signature Wizard の [TCP Traffic Type] ウィンドウには次のフィールドがあります。

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

[Service Type] ウィンドウ

Custom Signature Wizard の [Service Type] ウィンドウには次のフィールドがあります。

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

[TCP Sweep Type] ウィンドウ

Custom Signature Wizard の [TCP Sweep Type] ウィンドウには次のフィールドがあります。

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

[Atomic IP Engine Parameters] ウィンドウ

Atomic IP エンジンでは、IP プロトコル ヘッダーおよび関連付けられたレイヤ 4 トランスポート プロトコル（TCP、UDP、および ICMP）とペイロードを検査するシグニチャを定義します。Atomic エンジンでは、複数のパケットにまたがる固定データは保存されません。その代わりに、1 つのパケットの解析を基にしてアラートを起動できます。

フィールド定義

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

- [Event Action]：このシグニチャが検出されたときにセンサーで実行するアクションを指定します。デフォルトは [Produce Alert] です。

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

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

  [Yes] を選択した場合は、次のプロトコルから選択できます。

  - [ICMP Protocol]：ICMP シーケンス、タイプ、コード、識別子、および合計長を指定できます。
  - [Other IP Protocols]：識別子を指定できます。
  - [TCP Protocol]：送信元と宛先について、TCP フラグ、ウィンドウ サイズ、マスク、ペイロード長、緊急ポインタ、ヘッダー長、予約属性、およびポート範囲を設定できます。
  - [UDP Protocol]：送信元と宛先について、有効な UDP 長、長さの不一致、およびポート範囲を指定できます。
- [Specify Payload Inspection]：（任意）次のペイロード検査オプションを指定できます。
- [Specify IP Payload Length]：（任意）ペイロード長を指定できます。
- [Specify IP Header Length]：（任意）ヘッダー長を指定できます。
- [Specify IP Type of Service]：（任意）タイプ オブ サービスを指定できます。
- [Specify IP Time-to-Live]：パケットの存続可能時間を指定できます。
- [Specify IP Version]：（任意）IP バージョンを指定できます。
- [Specify IP Identifier]：（任意）IP 識別子を指定できます。
- [Specify IP Total Length]：（任意）合計 IP 長を指定できます。
- [Specify IP Option Inspection]：（任意）次の IP 検査オプションを指定できます。
  - [IP Option]：照合する IP オプション コード。
  - [IP Option Abnormal Options]：オプションの不正リスト。
- [Specify IP Addr Options]：（任意）次の IP アドレス オプションを指定できます。
  - [Address with Localhost]：送信元または宛先としてローカル ホスト アドレスが使用されているトラフィックを識別します。

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

詳細情報

Atomic IP エンジンの詳細については、「Atomic IP エンジン」（P.B-27）を参照してください。

Atomic IP Advanced エンジンのシグニチャの例

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

ステップ 11　イベント カウンタを設定します。

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

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

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

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

ステップ 12　アラートの頻度を設定します。

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

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

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

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

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

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

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

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

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

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

ヒント　変更を破棄するには、[Reset] をクリックします。

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

詳細情報

Atomic IP Advanced エンジンの詳細については、「Atomic IP Advanced エンジン」（P.B-16）を参照してください。

[Service HTTP Engine Parameters] ウィンドウ

Service HTTP エンジンは、サービス固有文字列に基づくパターン照合インスペクション エンジンです。HTTP プロトコルは、今日のネットワークで最もよく使用されているプロトコルの 1 つです。また、最も長い前処理時間を必要とし、システムの全体的なパフォーマンスにとって必須の検査を必要とするシグニチャの数も最も多くあります。

Service HTTP エンジンでは、複数のパターンを 1 つのパターン マッチング テーブルにまとめることでデータ内の検索を一度に実行できる正規表現ライブラリが使用されます。このエンジンは、Web サービスのみに向けられたトラフィック、つまり HTTP 要求を検索します。このエンジンでリターン トラフィックを検査することはできません。このエンジンでは、各シグニチャが対象とする個別の Web ポートを指定できます。

HTTP 解読とは、符号化された文字を ASCII 対応文字に正規化することによって、HTTP メッセージをデコードするプロセスです。このプロセスは、ASCII 正規化と呼ばれることもあります。

HTTP パケットを検査するには、あらかじめそのデータを、ターゲット システムでのデータ処理時に表示されるものと同じデータ表現として解読または正規化しておく必要があります。また、ホスト ターゲット タイプごとにカスタマイズされたデコード方式を用意することが推奨されます。そのためには、ターゲット上で動作しているオペレーティング システムおよび Web サーバのバージョンを確認する必要があります。Service HTTP エンジンには、Microsoft IIS Web サーバ用のデフォルトの解読動作が用意されています。

フィールド定義

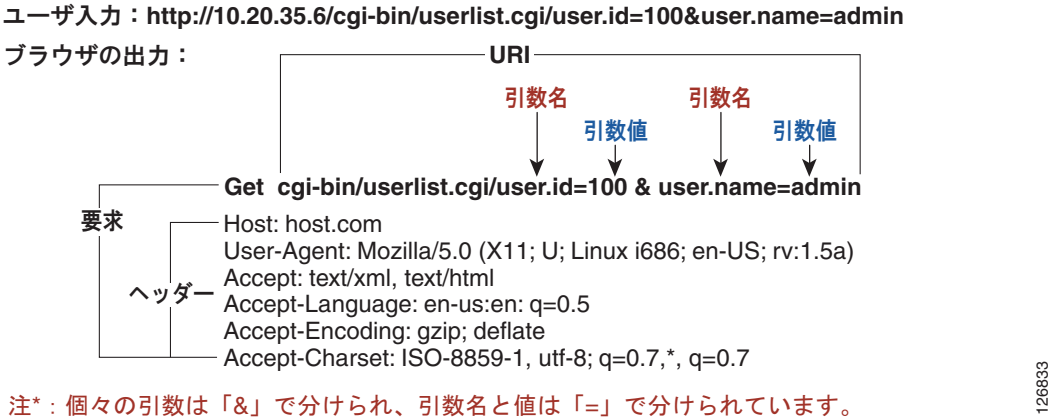
Custom Signature Wizard の [Service HTTP Engine Parameters] ウィンドウには、次のフィールドがあります。これらのオプションを使用して、非常に一般的なタイプのトラフィックや特定のタイプのトラフィックを検出するシグニチャを作成できます。

- [Event Action]：このシグニチャが検出されたときにセンサーで実行するアクションを指定します。デフォルトは [Produce Alert] です。

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

- [De Obfuscate]：検索の前に反回避 HTTP 解読を適用するかどうかを指定します。デフォルトは [Yes] です。
- [Max Field Sizes]：（任意）最大 URI、引数、ヘッダー、および要求フィールド長を指定できます。

  次の図は、最大フィールド サイズを示しています。



- [Regex]：URI、引数、ヘッダー、および要求正規表現の正規表現を指定できます。
- [Service Ports]：トラフィックで使用される特定のサービス ポートを示します。値はカンマ区切りのポートのリストです。
- [Swap Attacker Victim]：アラート メッセージで、および適用される任意のアクションについて、攻撃者と攻撃対象のアドレスとポート（送信元と宛先）を交換します。デフォルトは [No] です。

詳細情報

- Service HTTP エンジンの詳細については、「Service HTTP エンジン」（P.B-48）を参照してください。
- シグニチャの正規表現構文を記載した表については、「正規表現の構文」（P.B-10）を参照してください。

Service HTTP エンジンのシグニチャの例

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

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

Custom Signature Wizard を使用して、カスタム Service HTTP シグニチャを作成します。

カスタム Service HTTP シグニチャを作成するには、次の手順を実行します。

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

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

ステップ 3　[Yes] オプション ボタンをクリックして、[Select Engine] ドロップダウン リストから [Service HTTP] を選択し、[Next] をクリックします。

ステップ 4　このシグニチャを一意に識別する属性を指定するには、次の必須値を指定して、[Next] をクリックします。

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

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

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

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

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

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

ステップ 5　イベント アクションを割り当てます。

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

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

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

ステップ 7　（任意）[Max Field Sizes] で、次の最大フィールド サイズ パラメータを設定できます。

- [Specify Max URI Field Length]：最大 URI フィールド長をイネーブルにします。
- [Specify Max Arg Field Length]：最大引数フィールド長をイネーブルにします。
- [Specify Max Arg Field Length]：最大ヘッダー フィールド長をイネーブルにします。
- [Specify Max Arg Field Length]：最大要求フィールド長をイネーブルにします。

ステップ 8　[Regex] で、正規表現パラメータを設定します。

a. [Specify URI Regex] フィールドのドロップダウン リストから [Yes] を選択します。

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

c. 次のオプション パラメータに値を指定できます。

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

ステップ 9　[Service Ports] フィールドにポート番号を入力します。たとえば、Web ポート変数 $WEBPORTS を使用できます。値は、ターゲット サービスが常駐する、カンマ区切りのポートのリストまたはポート範囲です。

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

ステップ 11　[Next] をクリックします。

ステップ 12　（任意）次のデフォルトのアラート応答オプションを変更できます。

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

b. [Severity of the Alert] フィールドで、センサーがアラートを送信したときにイベント ビューアで報告する重大度を選択します。デフォルトは [Medium] です。

ステップ 13　[Next] をクリックします。

ステップ 14　デフォルトのアラート動作を変更するには、[Advanced] をクリックします。変更しない場合は、[Finish] をクリックします。カスタム シグニチャが作成されます。[Create Custom Signature] ダイアログボックスが表示され、このカスタム シグニチャを作成し、センサーに適用するかどうかを尋ねるメッセージが表示されます。

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

ヒント　変更を破棄するには、[Cancel] をクリックします。

詳細情報

- Service HTTP エンジンの詳細については、「Service HTTP エンジン」（P.B-48）を参照してください。
- シグニチャの正規表現構文を記載した表については、「正規表現の構文」（P.B-10）を参照してください。

[Service RPC Engine Parameters] ウィンドウ

Service RPC エンジンは、RPC プロトコル専用で、反回避戦略としてフル デコードを行います。これにより、フラグメント化されたメッセージ（複数パケット内の 1 つのメッセージ）およびバッチ メッセージ（1 つのパケット内の複数メッセージ）を処理できます。

RPC ポート マッパーは、ポート 111 上で動作します。通常の RPC メッセージは、550 より上位であれば任意のポートで送受信できます。RPC スイープは、TCP ポート スイープと似ていますが、有効な RPC メッセージが送信された場合に一意のポートだけをカウントするという点が異なります。RPC は UDP でも動作します。

フィールド定義

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

- [Event Action]：このシグニチャが検出されたときにセンサーで実行するアクションを指定します。デフォルトは [Produce Alert] です。

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

- [Direction]：センサーによる監視対象が、サービス ポートを宛先とするトラフィックか、送信元とするトラフィックかを指定します。デフォルトは [To Service] です。
- [Protocol]：プロトコルとして TCP または UDP を指定できます。
- [Service Ports]：ターゲット サービスが常駐するポートまたはポート範囲を示します。有効な値は、カンマで区切られたポートまたはポート範囲のリストです。
- [Specify Regex String]：検索する正規表現文字列を指定できます。
- [Specify Port Map Program]：このシグニチャが対象とするポート マッパーに送信するプログラム番号を示します。有効な範囲は 0 ～ 999999999 です。
- [Specify RPC Program]：このシグニチャが対象とする RPC プログラム番号を示します。有効な範囲は 0 ～ 1000000 です。
- [Specify Spoof Src]：送信元アドレスが 127.0.0.1 に設定された場合にアラートを起動します。
- [Specify RPC Max Length]：RPC メッセージ全体の最大許容長を示します。長さがこの値を超えるとアラームが生成されます。有効な範囲は 0 ～ 65535 です。
- [Specify RPC Procedure]：このシグニチャが対象とする RPC プロシージャ番号を示します。有効な範囲は 0 ～ 1000000 です。

詳細情報

- Service RPC エンジンの詳細については、「Service RPC エンジン」（P.B-53）を参照してください。
- シグニチャの正規表現構文を記載した表については、「正規表現の構文」（P.B-10）を参照してください。

[State Engine Parameters] ウィンドウ

State エンジンは、TCP ストリームのステートベースおよび正規表現ベースのパターン検査を行います。State エンジンは何かの状態を保存するデバイスで、入力があるたびに、その内容に基づいてある状態から別の状態に移行したり、処理や出力を行ったりできます。ステート マシンは、出力やアラートを発生させる特定のイベントを記述するために使用されます。State エンジンには、SMTP、シスコ ログイン、および LPR フォーマット ストリングの 3 つのステート マシンがあります。

フィールド定義

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

- [Event Action]：このシグニチャが検出されたときにセンサーで実行するアクションを指定します。デフォルトは [Produce Alert] です。

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

- [State Machine]：正規表現文字列の一致を制限する状態の名前を示します。

  オプションは、[Cisco Login]、[LPR Format String]、および [SMTP] です。
- [State Name]：状態の名前を識別します。オプションは、[Abort]、[Mail Body]、[Mail Header]、[SMTP Commands]、および [Start] です。
- [Specify Min Match Length]：一致の開始から終わりまでに正規表現文字列が一致している必要がある最小バイト数を示します。有効な範囲は 0 ～ 65535 です。
- [Regex String]：状態遷移をトリガーする正規表現の文字列を示します。
- [Direction]：遷移について検査するデータ ストリームの方向を示します。デフォルトは [To Service] です。
- [Service Ports]：ターゲット サービスが常駐するポートまたはポート範囲を示します。有効な値は、カンマで区切られたポートまたはポート範囲のリストです。
- [Swap Attacker Victim]：アラート メッセージで、および適用される任意のアクションについて、攻撃者と攻撃対象のアドレスとポート（送信元と宛先）を交換します。デフォルトは [No] です。
- [Specify Exact Match Offset]：正規表現の文字列が一致していることを報告するために必要な正確なストリーム オフセットをバイト数で示します。[Yes] を選択した場合、完全一致オフセットを設定できます。有効な範囲は 0 ～ 65535 です。[No] を選択した場合は、最小および最大一致オフセットを設定できます。

詳細情報

- State エンジンの詳細については、「State エンジン」（P.B-60）を参照してください。
- シグニチャの正規表現構文を記載した表については、「正規表現の構文」（P.B-10）を参照してください。

[String ICMP Engine Parameters] ウィンドウ

String エンジンは、ICMP、TCP、および UDP の各プロトコルを対象とした、汎用ベースのパターン マッチング インスペクション エンジンです。String エンジンでは、複数のパターンを 1 つのパターン マッチング テーブルにまとめることでデータ内の検索を一度に実行できる正規表現エンジンが使用されます。3 つの String エンジン、String ICMP、String TCP、および String UDP があります。

フィールド定義

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

- [Event Action]：このシグニチャが検出されたときにセンサーで実行するアクションを指定します。デフォルトは [Produce Alert] です。

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

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

- [Direction]：遷移について検査するデータ ストリームの方向を示します。デフォルトは [To Service] です。
- [ICMP Type]：ICMP ヘッダー TYPE 値。有効な範囲は 0 ～ 18 です。デフォルトは 0 ～ 18 です。
- [Swap Attacker Victim]：アラート メッセージで、および適用される任意のアクションについて、攻撃者と攻撃対象のアドレスとポート（送信元と宛先）を交換します。デフォルトは [No] です。
- [Specify Exact Match Offset]：正規表現の文字列が一致していることを報告するために必要な正確なストリーム オフセットをバイト数で示します。[Yes] を選択した場合、完全一致オフセットを設定できます。有効な範囲は 0 ～ 65535 です。[No] を選択した場合は、最小および最大一致オフセットを設定できます。

詳細情報

- String ICMP アーキテクチャの詳細については、「String エンジン」（P.B-62）を参照してください。
- シグニチャの正規表現構文を記載した表については、「正規表現の構文」（P.B-10）を参照してください。

[String TCP Engine Parameters] ウィンドウ

String エンジンは、ICMP、TCP、および UDP の各プロトコルを対象とした、汎用ベースのパターン マッチング インスペクション エンジンです。String エンジンでは、複数のパターンを 1 つのパターン マッチング テーブルにまとめることでデータ内の検索を一度に実行できる正規表現エンジンが使用されます。3 つの String エンジン、String ICMP、String TCP、および String UDP があります。

フィールド定義

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

- [Event Action]：このシグニチャが検出されたときにセンサーで実行するアクションを指定します。デフォルトは [Produce Alert] です。

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

- [Strip Telnet Options]：パターン検索の前に、データ ストリームから Telnet オプション制御文字を取り除きます。これは、主に、反回避ツールとして使用されます。デフォルトは [No] です。
- [Specify Min Match Length]：一致の開始から終わりまでに正規表現文字列が一致している必要がある最小バイト数を示します。有効な範囲は 0 ～ 65535 です。
- [Regex String]：1 つのパケットで検索する正規表現の文字列を示します。
- [Service Ports]：ターゲット サービスが常駐するポートまたはポート範囲を示します。有効な値は、カンマで区切られたポートまたはポート範囲のリストです。
- [Direction]：遷移について検査するデータ ストリームの方向を示します。デフォルトは [To Service] です。
- [Specify Exact Match Offset]：正規表現の文字列が一致していることを報告するために必要な正確なストリーム オフセットをバイト数で示します。[Yes] を選択した場合、完全一致オフセットを設定できます。有効な範囲は 0 ～ 65535 です。[No] を選択した場合は、最小および最大一致オフセットを設定できます。

- [Swap Attacker Victim]：アラート メッセージで、および適用される任意のアクションについて、攻撃者と攻撃対象のアドレスとポート（送信元と宛先）を交換します。デフォルトは [No] です。

詳細情報

- String ICMP アーキテクチャの詳細については、「String エンジン」（P.B-62）を参照してください。
- シグニチャの正規表現構文を記載した表については、「正規表現の構文」（P.B-10）を参照してください。

String TCP エンジンのシグニチャの例

（注） 次の手順は、カスタム String ICMP および UDP シグニチャの作成にも適用されます。

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

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

Custom Signature Wizard を使用して、カスタム String TCP シグニチャを作成します。

カスタム String TCP シグニチャを作成するには、次の手順を実行します。

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

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

ステップ 3　[Yes] オプション ボタンをクリックして、[Select Engine] ドロップダウン リストから [String TCP] を選択し、[Next] をクリックします。[Signature Identification] ウィンドウが表示されます。

ステップ 4　このシグニチャを一意に識別する属性を指定するには、次の必須値を指定して、[Next] をクリックします。

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

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

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

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

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

e. （任意）[User Comments] フィールドに、このシグニチャを説明するテキストを入力します。ここには、必要に応じてどのようなテキストを入力することもできます。このフィールドは、シグニチャやアラートには影響を与えません。デフォルトは [Sig Comment] です。[Next] をクリックします。[Engine Specific Parameters] ウィンドウが表示されます。

ステップ 5　イベント アクションを割り当てます。デフォルトは [Produce Alert] です。セキュリティ ポリシーに基づいて、拒否やブロックなどの複数のアクションを割り当てることができます。

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

ステップ 6　（任意）[Strip Telnet Options] フィールドで、ドロップダウン リストから [Yes] を選択し、パターンを検索する前にデータから Telnet オプション文字を除去します。

ステップ 7　（任意）最小一致長をイネーブルにするには、[Specify Min Match Length] フィールドのドロップダウン リストから [Yes] を選択し、[Min Match Length] フィールドに正規表現の文字列が一致する必要がある最小バイト数（0 ～ 65535）を入力します。

ステップ 8　[Regex String] フィールドに、このシグニチャが TCP パケットで検索する文字列を入力します。

ステップ 9　[Service Ports] フィールドに、23 などのポート番号を入力します。値は、ターゲット サービスが常駐する、カンマ区切りのポートのリストまたはポート範囲です。

ステップ 10　[Direction] ドロップダウン リストから、トラフィックの方向を選択します。

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

ステップ 11　（任意）完全一致オフセットをイネーブルにするには、[Specify Exact Match Offset] フィールドのドロップダウン リストから [Yes] を選択します。完全一致オフセットは、一致が有効であると認められるために正規表現の文字列が報告する必要がある正確なストリーム オフセットです（0 ～ 65535）。

a. [Specify Max Match Offset] フィールドに最大値を入力します。

b. [Specify Min Match Offset] フィールドに最小値を入力します。

ステップ 12　[Swap Attacker Victim] ドロップダウン リストから、[Yes] を選択し、アラート メッセージと実行するアクションにおいて、攻撃者と攻撃対象のアドレスとポート（宛先と送信元）を入れ替えます。

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

a. [Signature Fidelity Rating] フィールドに値を入力します。

SFR の有効値は 0 ～ 100 で、シグニチャに対する信頼度を示します。100 が最も信頼度が高いことを示します。デフォルトは 75 です。

b. [Severity of the Alert] フィールドで、センサーがアラートを送信したときにイベント ビューアで報告する重大度を選択します。デフォルトは [Medium] です。

ステップ 14　[Next] をクリックします。

ステップ 15　デフォルトのアラート動作を変更するには、[Advanced] をクリックします。変更しない場合は、[Finish] をクリックします。カスタム シグニチャが作成されます。[Create Custom Signature] ダイアログボックスが表示され、このカスタム シグニチャを作成し、センサーに適用するかどうかを尋ねるメッセージが表示されます。

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

ヒント　変更を破棄するには、[Cancel] をクリックします。

詳細情報

- String ICMP アーキテクチャの詳細については、「String エンジン」（P.B-62）を参照してください。
- シグニチャの正規表現構文を記載した表については、「正規表現の構文」（P.B-10）を参照してください。

[String UDP Engine Parameters] ウィンドウ

String エンジンは、ICMP、TCP、および UDP の各プロトコルを対象とした、汎用ベースのパターン マッチング インスペクション エンジンです。String エンジンでは、複数のパターンを 1 つのパターン マッチング テーブルにまとめることでデータ内の検索を一度に実行できる正規表現エンジンが使用されます。3 つの String エンジン、String ICMP、String TCP、および String UDP があります。

フィールド定義

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

- [Event Action]：このシグニチャが検出されたときにセンサーで実行するアクションを指定します。デフォルトは [Produce Alert] です。

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

- [Specify Min Match Length]：一致の開始から終わりまでに正規表現文字列が一致している必要がある最小バイト数を示します。有効な範囲は 0 ～ 65535 です。
- [Regex String]：1 つのパケットで検索する正規表現の文字列を示します。
- [Service Ports]：ターゲット サービスが常駐するポートまたはポート範囲を示します。有効な値は、カンマで区切られたポートまたはポート範囲のリストです。
- [Direction]：遷移について検査するデータ ストリームの方向を示します。
- [Swap Attacker Victim]：シグニチャの起動時に、アラートで報告される送信元アドレスと宛先アドレスを交換するかどうかを指定します。デフォルトは [No] です。
- [Specify Exact Match Offset]：正規表現の文字列が一致していることを報告するために必要な正確なストリーム オフセットをバイト数で示します。[Yes] を選択した場合、完全一致オフセットを設定できます。有効な範囲は 0 ～ 65535 です。[No] を選択した場合は、最小および最大一致オフセットを設定できます。

詳細情報

- String ICMP アーキテクチャの詳細については、「String エンジン」（P.B-62）を参照してください。
- シグニチャの正規表現構文を記載した表については、「正規表現の構文」（P.B-10）を参照してください。

[Sweep Engine Parameters] ウィンドウ

Sweep エンジンでは、2 つのホスト間または 1 つのホストから多数のホストへのトラフィックを分析します。既存のシグニチャを調整したり、カスタム シグニチャを作成したりすることができます。Sweep エンジンには、ICMP、UDP、および TCP のプロトコル固有パラメータがあります。

Sweep エンジンのアラート条件は、最終的に一意のパラメータのカウントに依存します。一意のパラメータは、スイープのタイプに応じた、個別ホストまたはポートの数のしきい値です。一意のパラメータは、期間内に一意のポート数またはホスト数がアドレス セット上に存在するとアラートをトリガーします。一意のポートおよびホストのトラッキング処理をカウンティングと言います。

Sweep エンジンのすべてのシグニチャに一意のパラメータを指定する必要があります。スイープでは、2 ～ 40（それぞれの値を含む）の制限値が強制されます。スイープの絶対最小値は 2 です。それ以外は（1 つのホストまたはポートの）スイープではありません。40 は、スイープによってメモリが過剰に消費されないように強制する必要がある場合の実際的な最大値です。一意の範囲の現実的な値は、5 ～ 15 です。

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

DataNode

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

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

フィールド定義

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

- [Event Action]：このシグニチャが検出されたときにセンサーで実行するアクションを指定します。デフォルトは [Produce Alert] です。

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

- [Unique]：一意のホスト接続の数のしきい値を示します。インターバル中にホスト接続数が [Unique] の値を超えると、アラートが送信されます。
- [Protocol]：プロトコルを示します。
  - [ICMP]：ICMP ストレージ タイプを指定し、ストレージ キー（攻撃者のアドレス、攻撃者のアドレスと攻撃対象のポート、または攻撃者と攻撃対象のアドレス）から 1 つを選択できます。
  - [TCP]：リバース抑制、反転スイープ、マスク、TCP フラグ、フラグメント ステータス、ストレージ キーを選択するか、ポート範囲を指定できます。
  - [UDP]：ストレージ キーを選択するか、ポート範囲を指定できます。
- [Src Addr Filter]：フィルタ値で定義された送信元 IP アドレス（または複数のアドレス）が含まれていないパケットを処理します。
- [Dst Addr Filter]：フィルタ値で定義された宛先 IP アドレス（または複数のアドレス）が含まれていないパケットを処理します。
- [Swap Attacker Victim]：シグニチャの起動時に、アラートで報告される送信元アドレスと宛先アドレスを交換するかどうかを指定します。デフォルトは [No] です。

詳細情報

Sweep エンジンの詳細については、「Sweep エンジン」（P.B-67）を参照してください。

[Alert Response] ウィンドウ

Custom Signature Wizard の [Alert Response] ウィンドウには次のフィールドがあります。

- [Signature Fidelity Rating]：ターゲットに関する具体的な情報がない場合に、このシグニチャをどの程度忠実に実行するかに関連付ける重みを示します。シグニチャ忠実度レーティングは、シグニチャベースでシグニチャの作成者が計算します。非常に具体的なルール（特定の正規表現）で作成されたシグニチャは、一般的なルールで作成されたシグニチャよりシグニチャ忠実度レーティングは高くなります。
- [Severity of the Alert]：アラートが報告される重大度。
  - [High]：最も深刻なセキュリティ アラート。
  - [Medium]：中程度のセキュリティ アラート。
  - [Low]：最も低いセキュリティ アラート。
  - [Information]：セキュリティ アラートではなく、ネットワーク アクティビティを示します。

[Alert Behavior] ウィンドウ

センサーの通常のアラート動作では、各アドレス セットに最初のアラートが送信され、次の 15 秒にわたって、このアドレス セットに対するすべてのアラートのサマリーを送信します。このアラート動作を変更するには、[Advanced] をクリックします。

[Event Count and Interval] ウィンドウ

Advanced Alert Behavior ウィザードの [Event Count and Interval] ウィンドウには次のフィールドがあります。

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

[Alert Summarization] ウィンドウ

Advanced Alert Behavior ウィザードの [Alert Summarization] ウィンドウには次のフィールドがあります。

- [Alert Every Time the Signature Fires]：シグニチャが悪意のあるトラフィックを検出するたびにセンサーからアラートを送信するように指定します。その後、センサーがアラートの量をダイナミックに調整できる追加しきい値を指定できます。
- [Alert the First Time the Signature Fires]：シグニチャが初めて悪意のあるトラフィックを検出したときにセンサーからアラートを送信するように指定します。その後、センサーがアラートの量をダイナミックに調整できる追加しきい値を指定できます。
- [Send Summary Alerts]：シグニチャが起動されるたびにアラートを送信せず、センサーからこのシグニチャのサマリー アラートのみを送信するように指定します。その後、センサーがアラートの量をダイナミックに調整できる追加しきい値を指定できます。
- [Send Global Summary Alerts]：1 つのアドレス セットで初めてシグニチャが起動されたときにセンサーからアラートを送信し、その後、指定した時間間隔ですべてのアドレス セットに関するすべてのアラートのサマリーを含むグローバル サマリー アラートのみを送信するように指定します。

[Alert Dynamic Response Fire All] ウィンドウ

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

- [Summary Key]：イベントのカウントに使用する属性を示します。たとえば、センサーでイベントが同じ攻撃者からかどうかに基づいてカウントする場合は、[Summary Key] として [Attacker Address] を選択します。
- [Use Dynamic Summarization]：センサーをダイナミックにサマライズ モードに設定できます。アラートの率が指定秒数内の指定された数のシグニチャを超えると、センサーはシグニチャごとにアラートを送信せず、アラートを 1 つのグローバル サマリーにまとめて送信します。指定間隔内にアラートの率がしきい値を下回ると、元のアラート動作に戻ります。グローバル サマリーでは、すべての攻撃者の IP アドレスとポート、およびすべての被害先 IP アドレスとポートに対してシグニチャが反応した件数がカウントされます。
  - [Summary Threshold]：サマリーを送信する前にセンサーが受信する必要がある最小ヒット数を示します。

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

[Alert Dynamic Response Fire Once] ウィンドウ

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

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

    アラート率が指定秒数内に指定された数のシグニチャを超えると、センサーはシグニチャが最初に起動されたときにアラートを送信せず、アラートを 1 つのグローバル サマリーにまとめて送信します。指定間隔内にアラートの率がしきい値を下回ると、元のアラート動作に戻ります。
  - [Global Summary Interval (seconds)]：センサーがサマリーを作成するためにイベントをカウントする間隔を示します。

[Alert Dynamic Response Summary] ウィンドウ

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

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

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

[Global Summarization] ウィンドウ

Advanced Alert Behavior ウィザードの [Global Summarization] ウィンドウには次のフィールドがあります。

- [Global Summary Interval (seconds)]：センサーがサマリーを作成するためにイベントをカウントする間隔を示します。

CHAPTER 11

イベント アクション規則の設定

（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。

（注） AIM IPS、AIP SSC-5、および NME IPS のイベント アクション規則ポリシーイベント アクション規則ポリシー

この章では、イベント アクション規則ポリシーを追加して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。

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。

イベント アクション規則のコンポーネント

（注）　[Event Action Rules] ペインで、イベント アクション規則ポリシーを作成して設定することができます。[Configuration] > *sensor_name* > [Policies] > [IPS Policies] を選択して、[IPS Policies] ペインの下部でイベント アクション規則を設定することもできます。

ここでは、イベント アクション規則の各種コンポーネントについて説明します。内容は次のとおりです。

イベント アクション規則の概要

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。

[Event Action Rules] ペインでは、イベント アクション規則ポリシーを追加、クローニング、または削除できます。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。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、[Event Action Rules] 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。

リスク レーティングの計算

リスク レーティング（RR）は 0 ～ 100 の範囲の値であり、ネットワーク上の特定のイベントに関係するリスクの数値による定量化を表します。計算では、攻撃対象（たとえば特定のサーバ）のネットワーク資産の価値が考慮されるため、攻撃重大度レーティングとシグニチャ忠実度レーティングを使用してシグニチャごとに設定され、ターゲット価値レーティングを使用してサーバごとに設定されます。リスク レーティングは、いくつかのコンポーネントから計算され、そのうちの一部は設定、収集、計算で得られます。

（注） リスク レーティングは、シグニチャではなくアラートに関連付けられます。

リスク レーティングを使用すると、注意が必要なアラートに優先順位を付けることができます。これらのリスク レーティング要因では、攻撃が成功した場合の重大度、シグニチャの忠実度、グローバル相関データから得た攻撃者の評判スコア、およびターゲット ホストの各自にとっての全体的な価値が考慮されます。リスク レーティングは evIdsAlert で報告されます。

特定のイベントのリスク レーティングを計算するために次の値が使用されます。

- シグニチャの忠実度評価（SFR）：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。シグニチャ忠実度レーティングはシグニチャごとに設定され、シグニチャが、それが表しているイベントまたは条件をどれだけ正確に検出するかを示します。

  シグニチャ忠実度レーティングは、シグニチャベースでシグニチャの作成者が計算します。シグニチャの作成者は、ターゲットに関する条件を絞り込んだ情報がない場合に、シグニチャの正確性についての基準となる信頼度ランキングを定義します。これは、分析対象パケットの配送を許可した場合に、検出された動作がターゲット プラットフォームに対して意図した効果を生み出す信頼度を表します。たとえば、非常に具体的な規則（特定の正規表現）を使用して記述されたシグニチャは、汎用的な規則を使用して記述されたシグニチャよりもシグニチャ忠実度が高くなります。

  （注） シグニチャ忠実度レーティングは、検出されたイベントがどれだけ悪影響を及ぼすかを示すものではありません。

- 攻撃重大度レーティング（ASR）：脆弱性の悪用に成功した場合の重大度に関連付ける重み。攻撃重大度レーティングは、シグニチャのアラート重大度パラメータ（informational、low、medium、または high）から計算されます。攻撃重大度レーティングはシグニチャごとに設定され、検出されたイベントどれだけ危険かを示します。

  （注） 攻撃重大度レーティングは、イベントがどれだけ正確に検出されるかを示すものではありません。

- ターゲットの価値レーティング（TVR）：ターゲットの考えられる価値に関連付けられる重み。

  ターゲットの価値レーティングはユーザ設定可能な値（zero、low、medium、high、または mission critical）であり、ネットワーク資産の IP アドレスを通じてその重要性を表します。価値の高い企業リソースにはより厳しく、あまり重要でないリソースにはより緩やかなセキュリティ ポリシーを開発できます。たとえば、デスクトップ ノードに割り当てるターゲットの価値レー

ティングよりも高いターゲットの価値レーティングを会社の Web サーバに割り当てることができます。この場合、会社の Web サーバに対する攻撃には、デスクトップ ノードに対する攻撃よりも高いリスク レーティングが付与されます。ターゲットの価値レーティングは、イベント アクション規則ポリシーで設定します。

- 攻撃関連性レーティング（ARR）：対象となるオペレーティング システムの関連性に関連付ける重み。攻撃関連性レーティングは、派生値（relevant、unknown、または not relevant）であり、アラート時に決定されます。関連するオペレーティング システムはシグニチャごとに設定します。
- 無差別デルタ（PD）：無差別デルタに関連付けられる重みであり、無差別モードの全体的なリスク レーティングから差し引くことができます。無差別デルタの範囲は 0 ～ 30 であり、シグニチャごとに設定します。

（注）　トリガー パケットがインラインでない場合、無差別デルタがレーティングから差し引かれます。

- ウォッチ リスト レーティング（WLR）：CSA MC ウォッチ リストに関連付けられる、範囲が 0 ～ 100 の重み（CSA MC での範囲は 0 ～ 35）。アラートの攻撃者がウォッチ リストに含まれている場合、その攻撃者のウォッチ リスト レーティングがレーティングに加算されます。

図 11-1 にリスク レーティングの式を示します。

図 11-1　　リスク レーティングの式

$$RR = \frac{ASR * TVR * SFR}{10000} + ARR - PD + WLR$$

191016

脅威レーティングの概要

脅威レーティングは、実行されたイベント アクションによって引き下げられたリスク レーティングです。非ロギング イベント アクションには脅威レーティングの調整があります。すべてのイベント アクションのうち最も大きな脅威レーティングがリスク レーティングから差し引かれます。

イベント アクションには次の脅威レーティングがあります。

- Deny attacker inline：45
- Deny attacker victim pair inline：40
- Deny attacker service pair inline：40
- Deny connection inline：35
- Deny packet inline：35
- Modify packet inline：35
- Request block host：20
- Request block connection：20
- Reset TCP connection：20
- Request rate limit：20

イベント アクション オーバーライドの概要

イベント アクション オーバーライドを追加すると、イベントのリスク レーティングに基づいて、そのイベントに関連付けられているアクションを変更できます。イベント アクション オーバーライドは、各シグニチャを個別に設定しないで、グローバルにイベント アクションを追加する方法です。各イベント アクションには、関連付けられたリスク レーティング範囲があります。シグニチャ イベントが発生し、そのイベントのリスク レーティングがイベント アクションの範囲内に入っていた場合、そのアクションがイベントに追加されます。たとえば、リスク レーティングが 85 以上のイベントで SNMP トラップを生成させる場合、Request SNMP Trap のリスク レーティング範囲を 85 ～ 100 に設定します。アクション オーバーライドを使用しない場合は、イベント アクション オーバーライド コンポーネント全体をディセーブルにします。

（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。

イベント アクション フィルタの概要

イベント アクション フィルタは順序リストとして処理され、フィルタはリスト内で上下に移動できます。フィルタによって、センサーは、イベントに応答して特定のアクションを実行できます。すべてのアクションを実行したり、イベント全体を削除したりする必要はありません。フィルタは、イベントからアクションを削除することで機能します。1 つのイベントからすべてのアクションを削除するフィルタは、イベントを効率的に消費します。

（注） スイープ シグニチャをフィルタリングする場合は、宛先アドレスをフィルタリングしないことを推奨します。複数の宛先アドレスがある場合、最後のアドレスだけがフィルタとの照合に使用されます。

イベント アクションのサマライズ

サマライズを使用すると、基本集約機能として、複数のイベントを 1 つのアラートにまとめることにより、センサーから送信されたアラートの量が軽減されます。また、シグニチャごとに特別なパラメータを指定することにより、アラートの処理方法をさまざまに変更できます。各シグニチャは、優先される通常動作を反映したデフォルト値を使用して作成されます。ただし、各シグニチャの設定を修正することにより、エンジンのタイプごとに定められた制約の範囲内でこのデフォルトの処理方法を調整できます。

アラートを生成しないアクション（拒否、ブロック、TCP リセット）には、サマライズされない各シグニチャ イベントのフィルタが適用されます。アラートを生成するアクションは、これらの集約されたアラートに対しては実行されず、アクションが 1 つのサマライズされたアラートに適用された後、フィルタが適用されます。

アラートを生成する他のアクションのいずれかを選択し、フィルタで除外しない場合、[Product Alert] を選択しない場合であってもアラートが作成されます。アラートが作成されないようにするには、アラートを生成するすべてのアクションをフィルタで除外する必要があります。

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 アクションが処理されます。これにより、センサーは、一連のイベントにまたがって発生する疑わしいアクティビティを監視します。

イベント アクションの集約

基本的な集約には 2 つの動作モードがあります。簡易なモードでは、シグニチャに対し、アラートが送信される前に満たされる必要があるヒット数のしきい値を設定します。一方、高度なモードでは、各インターバルにおけるヒット数がカウントされます。このモードでは、センサーにより秒あたりのヒット数が追跡され、そのしきい値を超えた場合にのみアラートが送信されます。この例で、「ヒット」とはイベントを表すために使用した用語で、基本的にはアラートを指します。ただし、ヒット数がしきい値を超過するまでは、センサーからアラートとして送信されることはありません。

次のサマライズ オプションから選択できます。

- [Fire All]：シグニチャが起動されるたびにアラートが起動されます。サマライズにしきい値が設定されている場合、サマライズが発生するまで実行ごとにアラートが起動されます。サマライズが開始された後は、各アドレス セットについて、サマライズ間隔ごとに 1 つのアラートのみが起動されます。他のアドレス セットのアラートは、すべて発生するか、個別にサマライズされます。そのシグニチャのアラートが一定期間ないと、シグニチャはすべてを起動するモードに戻ります。
- [Summary]：初めてシグニチャがトリガーされたときにアラートが起動され、そのシグニチャの以降のアラートは、要約間隔の間サマライズされます。各アドレスセットについて、要約間隔ごとに 1 個のアラートのみが起動されます。グローバル要約しきい値に達した場合、シグニチャはグローバル サマライズ モードになります。
- [Global Summarization]：要約間隔ごとにアラートを起動します。シグニチャは、グローバル サマライズ用に事前設定できます。
- [Fire Once]：アドレス セットごとにアラートを起動します。このモードはグローバル サマライズ モードにアップグレードできます。

シグニチャ イベント アクション プロセッサ

シグニチャ イベント アクション プロセッサは、シグニチャ イベント アクション オーバーライド、シグニチャ イベント アクション フィルタ、およびシグニチャ イベント アクション ハンドラを介して処理するように、アラーム チャネルのシグニチャ イベントから取得するデータ フローを調整します。次のコンポーネントで構成されます。

- アラーム チャネル：SensorApp インスペクション パスからのシグニチャ イベントを処理するために通信を行う領域を示すユニット。
- シグニチャ イベント アクション オーバーライド：リスク レーティング値に基づいてアクションを追加します。シグニチャ イベント アクション オーバーライドは、設定されたリスク レーティングしきい値の範囲に入るすべてのシグニチャに適用されます。各シグニチャ イベント アクション オーバーライドは独立し、アクション タイプごとに別々の設定値を持ちます。
- シグニチャ イベント アクション フィルタ：シグニチャ イベントのシグニチャ ID、アドレス、リスク レーティングに基づいてアクションを差し引きます。シグニチャ イベント アクション フィルタへの入力は、シグニチャ イベントアクション オーバーライドによって追加された可能性のあるアクションを含むグニチャ イベントです。

  （注） シグニチャ イベント アクション フィルタが実行できるのは、アクションを差し引くことだけです。新しいアクションを追加することはできません。

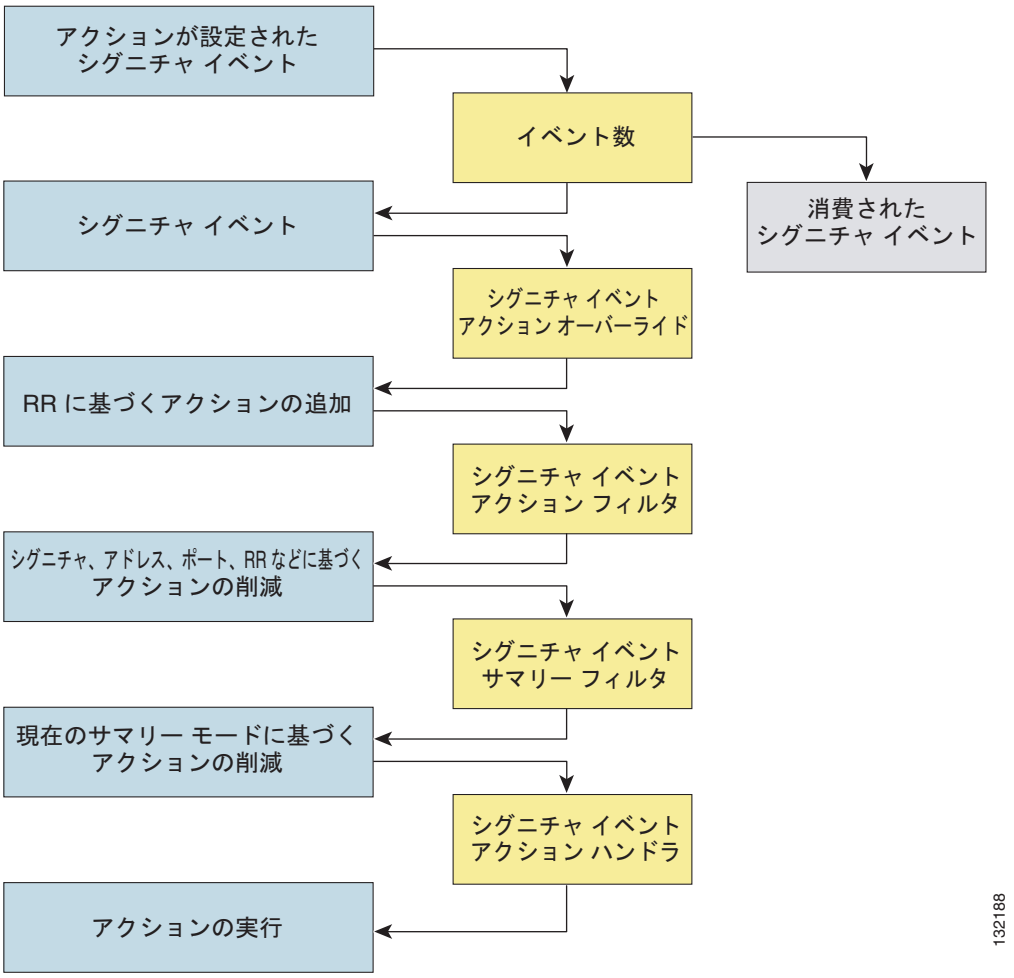
  シグニチャ イベント アクション フィルタには、次のパラメータが適用されます。

  - シグニチャ ID
  - サブシグニチャ ID

  - 攻撃者のアドレス
  - 攻撃者のポート
  - 攻撃対象のアドレス
  - 攻撃対象者のポート
  - リスク レーティングしきい値の範囲
  - 削除するアクション
  - シーケンス識別子（任意）
  - ストップ ビットまたは継続ビット
  - アクション フィルタ行をイネーブルにするビット
  - 攻撃対象 OS との関連性または OS との関連性
- シグニチャ イベント アクション ハンドラ：要求されたアクションを実行します。シグニチャ イベント アクション ハンドラからの出力は、実行されているアクションと、イベント ストアに書き込まれる evIdsAlert（ある場合）です。

図 11-2 に、シグニチャ イベント アクション プロセッサを通過するシグニチャ イベントの論理的な流れと、このイベントに対するアクションで実行される操作を示します。アラーム チャネルから受け取ったアクションが設定されているシグニチャ イベントから開始し、そのイベントは、上から下に向かってシグニチャ イベント アクション プロセッサの機能コンポーネントを通過します。

図 11-2　シグニチャ イベント アクション プロセッサを通過するシグニチャ イベント



イベント アクション

Cisco IPS は、次のイベント アクションを実行します。

- アラート アクションとログ アクション
  - [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。

- 拒否アクション
  - [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。

- その他のアクション

（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。

イベント アクション規則ポリシーの設定

ここでは、イベント アクション規則ポリシーを作成する方法について説明します。内容は次のとおりです。

[Event Action Rules] ペイン

（注） イベント アクション規則ポリシーを追加、クローニング、または削除するには、管理者またはオペレータであることが必要です。

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。

[Event Action Rules] ペインでは、イベント アクション規則ポリシーを追加、クローニング、または削除できます。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。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、[Event Action Rules] 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。

[Event Action Rules] ペインのフィールド定義

[Event Action Rules] ペインには、次のフィールドが表示されます。

- [Policy Name]：イベント アクション規則ポリシーの名前を指定します。
- [Assigned Virtual Sensor]：イベント アクション規則ポリシーが割り当てられている仮想センサーを指定します。

[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。

- [Policy Name]：新しいポリシーの一意の名前を作成できます。

イベント アクション規則ポリシーの追加、クローニング、削除

イベント アクション規則ポリシーを追加、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] > [Event Action Rules] 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、イベント アクション規則ポリシーの名前を入力します。

ヒント　変更を破棄して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。[Event Action Rules] ペインのリストにイベント アクション規則ポリシーが表示されます。

ステップ 5　既存のイベント アクション規則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、既存のイベント アクション規則ポリシー名の後に「_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　変更を破棄して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。[Event Action Rules] ペインのリストに、クローニングしたイベント アクション規則ポリシーが表示されます。

ステップ 8　イベント アクション規則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　デフォルトのイベント アクション規則ポリシー（rules0）は削除できません。

ステップ 9　[Yes] をクリックします。[Event Action Rules] ペインのリストにイベント アクション規則ポリシーが表示されなくなります。

[rules0] ペイン

[Event Action Rules (rules0)] ペインには、7 つのタブがあります。これらのタブを使用して、イベント アクション オーバーライド、イベント アクション フィルタ、ターゲットの価値レーティング、OS ID、イベント変数、リスク カテゴリ、[Configuration] > *sensor_name* > [Policies] > [Event Action Rules] ペインで追加したイベント アクション規則ポリシーの一般的な設定を設定できます。

[Configuration] > *sensor_name* > [Policies] > [IPS Policies] ペインの下部で、[IPS Policies] ペインの下部でイベント アクション規則を設定することもできます。

イベント アクション オーバーライドの設定

ここでは、イベント アクションの設定方法について説明します。内容は次のとおりです。

- 「[Event Action Overrides] タブ」（P.11-13）
- 「Deny Packet Inline について」（P.11-14）
- 「[Event Action Overrides] タブのフィールド定義」（P.11-14）
- 「[Add Event Action Override] および [Edit Event Action Override] ダイアログボックスのフィールド定義」（P.11-14）
- 「イベント アクション オーバーライドの追加、編集、削除、イネーブル化、ディセーブル化」（P.11-15）

[Event Action Overrides] タブ

（注）　イベント アクション オーバーライドを追加または編集するためには、管理者またはオペレータであることが必要です。

[Event Action Overrides] タブでは、イベント アクション オーバーライドを追加して、イベントの特定の詳細情報に基づいてイベントに関連付けられたアクションを変更できます。

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。

[Event Action Overrides] タブのフィールド定義

[Event Action Overrides] タブには次のフィールドがあります。

- [Use Event Action Overrides]：オンにすると、イネーブルになっているイベント アクション オーバーライドを使用できます。
- [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 レーティングを指定します。

  このレベルに一致するリスク レーティングでイベントが発生した場合、イベント アクションがこのイベントに追加されます。
- [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]：オーバーライドがイネーブルかどうかを示します。

[Add Event Action Override] および [Edit Event Action Override] ダイアログボックスのフィールド定義

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

- [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。設定したリスクに対応するリスク レーティングでイベントが発生した場合、イベント アクションがこのイベントに追加されます。
- [Available 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]：イベント アクション オーバーライドが起動されたときにアクションをイネーブルにするにはチェックボックスをオンにします。

イベント アクション オーバーライドの追加、編集、削除、イネーブル化、ディセーブル化

イベント アクション オーバーライドを追加、編集、削除、イネーブル化、およびディセーブル化するには、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] > [Event Action Rules] > [rules0] > [Event Action Overrides] を選択します。

ステップ 3　イベント アクション オーバーライドを作成するには、[Add] をクリックします。

ステップ 4　[Risk Rating] ドロップダウン メニューから、このネットワーク資産にリスク レーティング範囲を割り当てます。

ステップ 5　[Available Actions to Add] リストで、このイベント アクション オーバーライドが対応するイベント アクションをチェックします。

ステップ 6　オーバーライドでイネーブルにするアクションの [Enabled] チェックボックスをオンにします。

ヒント　変更内容を破棄して [Add Event Action Override] 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。新しいイベント アクション オーバーライドが [Event Action Overrides] タブのリストに表示されます。

ステップ 8　[Use Event Action Overrides] チェックボックスをオンにします。

（注）　[Event Action Overrides] タブで [Use Event Action Overrides] チェックボックスをオンにする必要があります。そうしないと、設定した値にかかわらず、イベント アクション オーバーライドがどれもイネーブルになりません。

ステップ 9　既存のイベント アクション オーバーライドを編集するには、リストで選択し、[Edit] をクリックします。必要な変更を加えます。

ヒント　変更内容を破棄して [Edit Event Action Override] 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 10　[OK] をクリックします。編集したイベント アクション オーバーライドが [Event Action Overrides] タブのリストに表示されます。

ステップ 11　[Use Event Action Overrides] チェックボックスをオンにします。

（注）　[Event Action Overrides] タブで [Use Event Action Overrides] チェックボックスをオンにする必要があります。そうしないと、設定した値にかかわらず、イベント アクション オーバーライドがどれもイネーブルになりません。

ステップ 12　イベント アクション オーバーライドを削除するには、リストで選択し、[Delete] をクリックします。イベント アクション オーバーライドが [Event Action Overrides] タブのリストに表示されなくなります。

ステップ 13　イベント アクション オーバーライドをイネーブルまたはディセーブルにするには、リストで選択し、[Edit] をクリックします。

ステップ 14　イベント アクション オーバーライドをディセーブルにするには、イベント アクション オーバーライドに割り当てたすべてのイベント アクションについて、[Enabled] チェックボックスをオフにします。イベント アクション オーバーライドをイネーブルにするには、イベント アクション オーバーライドに割り当てたすべてのイベント アクションについて、[Enabled] チェックボックスをオンにします。

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 15　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。

イベント アクション フィルタの設定

ここでは、イベント アクション フィルタの設定方法について説明します。内容は次のとおりです。

[Event Action Filters] タブ

（注）　イベント アクション フィルタを追加、編集、イネーブル化、ディセーブル化、または削除するには、管理者またはオペレータであることが必要です。

特定のアクションをイベントから削除するか、または、イベント全体を廃棄してセンサーによる今後の処理を回避するように、イベント アクション フィルタを設定できます。[Event Variables] ペインで定義した変数を使用して、フィルタに合わせてアドレスをグループ化できます。

注意　送信元および宛先 IP アドレスに基づくイベント アクション フィルタは Sweep エンジンでは機能しません。これは、これらのフィルタが、通常のシグニチャとしてフィルタしないためです。送信元および宛先 IP アドレスをスイープ アラートでフィルタするには、Sweep エンジン シグニチャの送信元および宛先 IP アドレス フィルタ パラメータを使用します。

（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（$）を付ける必要があります。「$」を付けないと、「`Bad source and destination`」エラーが生じます。

[Event Action Filters] タブのフィールド定義

[Event Action Filters] タブには次のフィールドがあります。

- [Name]：追加するフィルタに名前を付けることができます。フィルタをリスト中で移動したり、必要に応じて非アクティブ リストに移動できるように、フィルタに名前を付ける必要があります。
- [Enabled]：このフィルタがイネーブルかどうかを示します。
- [Sig 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。シグニチャの範囲を入力することもできます。
- [SubSig 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。SubSig 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。subSig ID の範囲を入力することもできます。
- [Attacker (IPv4/IPv6/port)]：攻撃パケットを送信したホストの IP アドレスまたはポートを示します。アドレスまたはポートの範囲を入力することもできます。
- [Victim (IPv4/IPv6/port)]：攻撃者のホストが使用している IP アドレスまたはポートを示します。アドレスまたはポートの範囲を入力することもできます。
- [Risk Rating]：このイベント アクション フィルタをトリガーするために使用されるリスク レーティング範囲を示します（0 ～ 100）。イベントが発生し、そのリスク レーティングがここで設定した最小 - 最大範囲に入っていた場合、イベントはこのイベント フィルタの規則と比較して処理されます。
- [Actions to Subtract]：イベントの条件がイベント アクション フィルタの基準を満たしている場合に、イベントから削除されるアクションを示します。

[Add Event Action Filter] および [Edit Event Action Filter] ダイアログ ボックスのフィールド定義

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

- [Name]：追加するフィルタに名前を付けることができます。フィルタをリスト中で移動したり、必要に応じて非アクティブ リストに移動できるように、フィルタに名前を付ける必要があります。
- [Enabled]：このフィルタをイネーブルにできます。
- [Signature ID]：このシグニチャに割り当てられた一意の数値を示します。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。シグニチャの範囲を入力することもできます。
- [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。サブシグニチャ ID の範囲を入力することもできます。
- [Attacker IPv4 Address]：攻撃パケットを送信したホストの IP アドレスを示します。アドレスの範囲を入力することもできます。
- [Attacker IPv6 Address]：攻撃パケットを送信したホストの攻撃者 IPv6 アドレスの範囲を次の形式で示します。

  <XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

  例：2001:0db8:1234:1234:1234:1234:1234:1234,2001:0db8:1234:1234:1234:1234:1234:8888。範囲の 2 番目の IPv6 アドレスは、最初の IPv6 アドレス以上である必要があります。

（注）　IPv6 アドレスは、16 進数で表現された 128 ビットであり、コロンにより 8 個の 16 ビット グループに分かれています。先頭のゼロをスキップしたり、中間のゼロのグループを 2 個のコロン（::）で表現できます。アドレスは、プレフィクス 2001:db8 で始める必要があります。

- [Attacker Port]：攻撃者ホストによって使用されるポートを示します。これは、攻撃パケットの発信元のポートです。ポートの範囲を入力することもできます。
- [VictimIPv4 Address]：攻撃対象ホスト（攻撃パケットの受信者）の IP アドレスを示します。アドレスの範囲を入力することもできます。
- [VictimIPv6 Address]：攻撃対象になっているホスト（攻撃パケットの受信者）の攻撃対象 IPv6 アドレスの範囲を次の形式で示します。

  <XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

  例：2001:0db8:1234:1234:1234:1234:1234:1234,2001:0db8:1234:1234:1234:1234:1234:8888。範囲の 2 番目の IPv6 アドレスは、最初の IPv6 アドレス以上である必要があります。

（注）　IPv6 アドレスは、16 進数で表現された 128 ビットであり、コロンにより 8 個の 16 ビット グループに分かれています。先頭のゼロをスキップしたり、中間のゼロのグループを 2 個のコロン（::）で表現できます。アドレスは、プレフィクス 2001:db8 で始める必要があります。

- [Victim Port]：攻撃パケットを受信したポートを示します。ポートの範囲を入力することもできます。
- [Risk Rating]：このイベント アクション フィルタをトリガーするために使用されるリスク レーティング範囲を示します（0 ～ 100）。イベントが発生し、そのリスク レーティングがここで設定した最小 - 最大範囲に入っていた場合、イベントはこのイベント フィルタの規則と比較して処理されます。
- [Actions to Subtract]：[Opens the Edit Actions] ダイアログボックスを開きます。このダイアログでは、イベントの条件がイベント アクション フィルタの基準を満たしている場合に、イベントから削除されるアクションを選択できます。
- More Options
  - [Active]：フィルタリング イベントに適用されるように、フィルタ リストにフィルタを追加できます。
  - [OS Relevance]：攻撃が攻撃対象オペレーティング システムに関係しないイベントをフィルタで除外します。
  - [Deny Percentage]：攻撃者拒否機能で拒否するパケットのパーセンテージを決定します。有効な範囲は 0 ～ 100 です。デフォルトは 100% です。
  - [Stop on Match]：このイベントをイベント アクション フィルタ リストの残りのフィルタに対して処理するかどうかを決定します。

    [No] に設定した場合、Stop フラグが見つかるまで残りのフィルタが照合のために処理されます。

    [Yes] の場合、以降の処理は行われません。このフィルタで指定されたアクションは削除され、残りのアクションが実行されます。

– [Comments]：このフィルタに関連付けられているユーザ コメントを表示します。

イベント アクション フィルタの追加、編集、削除、イネーブル化、ディセーブル化、移動

イベント アクション フィルタを追加、編集、削除、イネーブル化、ディセーブル化、および移動するには、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] > [Event Action Rules] > [rules0] > [Event Action Filters] を選択し、[Add] をクリックします。

ステップ 3　[Name] フィールドに、イベント アクション フィルタの名前を入力します。デフォルト名が設定されますが、より意味のある名前に変更できます。

ステップ 4　[Enabled] フィールドで [Yes] オプション ボタンをクリックし、フィルタをイネーブルにします。

ステップ 5　[Signature ID] フィールドに、このフィルタを適用するすべてのシグニチャのシグニチャ ID を入力します。リスト（2001,2004）または範囲（2001–2004）の他、[Event Variables] タブで定義したいずれかの SIG 変数を使用できます。変数の前には $ を付けます。

ステップ 6　[SubSignature ID] フィールドには、このフィルタを適用するシグニチャのサブシグニチャ ID を入力します。

ステップ 7　[Attacker IPv4 Address] フィールドに、送信元ホストの IP アドレスを入力します。[Event Variables] タブで定義した変数を使用できます。変数の前には $ を付けます。また、アドレスの範囲を入力することもできます（例：0.0.0.0-255.255.255.255）。

ステップ 8　Attacker IPv6 Address フィールドに、送信元ホストの攻撃者 IPv6 アドレスの範囲を次の形式で入力します。

<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

範囲の 2 番目の IPv6 アドレスは、最初の IPv6 アドレス以上である必要があります。

（注）　IPv6 アドレスは、16 進数で表現された 128 ビットであり、コロンにより 8 個の 16 ビット グループに分かれています。先頭のゼロをスキップしたり、中間のゼロのグループを 2 個のコロン（::）で表現できます。アドレスは、プレフィクス 2001:db8 で始める必要があります。

[Event Variables] タブで定義した変数を使用することもできます。変数の前には $ を付けます。

ステップ 9　[Attacker Port] フィールドに、攻撃者が攻撃パケットを送信するために使用するポート番号を入力します。

ステップ 10　[Victim IPv4 Address] フィールドに、受信者ホストの IP アドレスを入力します。

[Event Variables] タブで変数を定義済みであれば、そのうちの 1 つを使用できます。変数の前には $ を付けます。また、アドレスの範囲を入力することもできます（例：0.0.0.0-255.255.255.255）。

ステップ 11　[Victim IPv6 Address] フィールドに、受信者ホストの IPv6 アドレスの範囲を次の形式で入力します。

<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

範囲の 2 番目の IPv6 アドレスは、最初の IPv6 アドレス以上である必要があります。

（注）　IPv6 アドレスは、16 進数で表現された 128 ビットであり、コロンにより 8 個の 16 ビット グループに分かれています。先頭のゼロをスキップしたり、中間のゼロのグループを 2 個のコロン（::）で表現できます。アドレスは、プレフィクス 2001:db8 で始める必要があります。

[Event Variables] タブで定義した変数を使用できます。変数の前には $ を付けます。

ステップ 12　[Victim Port] フィールドに、攻撃対象ホストが攻撃パケットを受信するために使用するポート番号を入力します。

ステップ 13　[Risk Rating] フィールドに、このフィルタのリスク レーティング範囲を入力します。イベントのリスク レーティングが指定した範囲に収まる場合、イベントはこのフィルタの条件に照らして処理されます。

ステップ 14　[Actions to Subtract] フィールドで、メモ アイコンをクリックし、[Edit Actions] ダイアログボックスを開きます。このフィルタでイベントから削除するアクションのチェックボックスをオンにします。

ヒント　リストで複数のイベント アクションを選択するには、Ctrl キーを押しながらクリックします。

ステップ 15　[Active] フィールドで、[Yes] オプション ボタンをクリックし、このフィルタをリストに追加して、フィルタリング イベントで有効にします。

ステップ 16　[OS Relevance] ドロップダウン リストで、攻撃対象について特定されたオペレーティング システムにアラートが関連するかどうかを知る必要があるかどうかを選択します。

ステップ 17　[Deny Percentage] フィールドに、拒否攻撃者機能で拒否するパケットのパーセンテージを入力します。デフォルトは 100% です。

ステップ 18　[Stop on Match] フィールドに、次のオプション ボタンのいずれかをクリックします。

a.　[Yes]：この特定のフィルタのアクションが削除された後に、Event Action Filters コンポーネントで処理を停止するかどうか。残りのフィルタはすべて処理されないため、イベントから他のアクションを削除できません。

b.　[No]：他のフィルタの処理を継続するかどうか。

ステップ 19　[Comments] フィールドに、このフィルタの目的や、このフィルタを特定の方法で設定した理由など、このフィルタとともに保存するコメントを入力します。

ヒント　変更内容を破棄して [Add Event Action Filter] 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 20　[OK] をクリックします。新しいイベント アクション フィルタが [Event Action Filters] タブのリストに表示されます。

ステップ 21　既存のイベント アクション フィルタを編集するには、リストで選択し、[Edit] をクリックします。

ステップ 22　必要な変更を加えます。

ヒント　変更内容を破棄して [Edit Event Action Filter] 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 23　[OK] をクリックします。編集後のイベント アクション フィルタが [Event Action Filters] タブのリストに表示されます。

ステップ 24　イベント アクション フィルタを削除するには、リストで選択し、[Delete] をクリックします。イベント アクション フィルタが [Event Action Filters] タブのリストに表示されなくなります。

ステップ 25　イベント アクション フィルタをリスト中で上下に移動するには、選択し、[Move Up] または [Move Down] 矢印アイコンをクリックします。

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 26　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。

IPv4 ターゲットの価値レーティングの設定

ここでは、IPv4 ターゲットの価値レーティング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。

- 「[IPv4 Target Value Rating] タブ」（P.11-21）
- 「[IPv4 Target Value Rating] タブのフィールド定義」（P.11-21）
- 「[Add Target Value Rating] および [Edit Target Value Rating] ダイアログボックスのフィールド定義」（P.11-22）
- 「IPv4 ターゲットの価値レーティングの追加、編集、および削除」（P.11-22）

[IPv4 Target Value Rating] タブ

（注）　ターゲットの価値レーティングを追加、編集、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。

ネットワーク資産にターゲットの価値レーティングを割り当てることができます。ターゲットの価値レーティングは、各アラートのリスク レーティング値の計算に使用される要素の 1 つです。異なるターゲットに異なるターゲットの価値レーティングを割り当てることができます。イベントのリスク レーティングが高いほど、より厳しいシグニチャ イベント アクションがトリガーされます。

[IPv4 Target Value Rating] タブのフィールド定義

[IPv4 Target Value Rating] タブには次のフィールドがあります。

- [Target Value Rating (TVR)] : このネットワーク資産に割り当てる価値を示します。値は、[High]、[Low]、[Medium]、[Mission Critical]、または [No Value] です。
- [Target IP Address] : ターゲットの価値レーティングを使用して優先順位を付けるネットワーク資産の IP アドレスを示します。

[Add Target Value Rating] および [Edit Target Value Rating] ダイアログボックスのフィールド定義

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

- [Target Value Rating (TVR)] : このネットワーク資産に価値を割り当てます。値は、[High]、[Low]、[Medium]、[Mission Critical]、または [No Value] です。
- [Target IPv4 Address(es)] : ターゲットの価値レーティングを使用して優先順位を付けるネットワーク資産の IP アドレスを示します。

IPv4 ターゲットの価値レーティングの追加、編集、および削除

ネットワーク資産の IPv4 ターゲットの価値レーティングを追加、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] > [Event Action Rules] > [rules0] > [IPv4 Target Value Rating] を選択し、[Add] をクリックします。

ステップ 3　ターゲットの価値レーティングを新しい資産グループに割り当てるには、次の手順を実行します。

a. [Target Value Rating (TVR)] ドロップダウン リストからレーティングを選択します。値は [High]、[Low]、[Medium]、[Mission Critical]、または [No Value] です。

b. [Target IPv4 Address(es)] フィールドに、ネットワーク資産の IP アドレスを入力します。IP アドレスの範囲を入力するには、その範囲の最も小さいアドレス、ハイフン、最も大きいアドレスの順に入力します。例：10.10.2.1-10.10.2.30。

ヒント　変更を破棄して [Add IPv4 Target Value Rating] 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。新しい資産の新しいターゲットの価値レーティングが [IPv4 Target Value Rating] タブのリストに表示されます。

ステップ 5　既存のターゲットの価値レーティングを編集するには、リストで選択し、[Edit] をクリックします。

ステップ 6　必要な変更を加えます。

ヒント　変更を破棄して [Edit IPv4 Target Value Rating] 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。編集したネットワーク資産が [IPv4 Target Value Rating] タブのリストに表示されます。

ステップ 8　ネットワーク資産を削除するには、リスト中で選択し、[Delete] をクリックします。ネットワーク資産が [Ipv4 Target Value Rating] タブの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 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。

IPv6 ターゲットの価値レーティングの設定

ここでは、IPv6 ターゲットの価値レーティング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。

[IPv6 Target Value Rating] タブ

（注）　ターゲットの価値レーティングを追加、編集、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。

ネットワーク資産にターゲットの価値レーティングを割り当てることができます。ターゲットの価値レーティングは、各アラートのリスク レーティング値の計算に使用される要素の 1 つです。異なるターゲットに異なるターゲットの価値レーティングを割り当てることができます。イベントのリスク レーティングが高いほど、より厳しいシグニチャ イベント アクションがトリガーされます。

[IPv6 Target Value Rating] タブのフィールド定義

[IPv6 Target Value Rating] タブには次のフィールドがあります。

- [Target Value Rating (TVR)]：このネットワーク資産に割り当てる価値を示します。値は、[High]、[Low]、[Medium]、[Mission Critical]、または [No Value] です。
- [Target IP Address]：ターゲットの価値レーティングを使用して優先順位を付けるネットワーク資産の IP アドレスを示します。

[Add IPv6 Target Value Rating] および [Edit IPv6 Target Value Rating] ダイアログボックスのフィールド定義

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

- [Target Value Rating (TVR)]：このネットワーク資産に価値を割り当てます。値は、[High]、[Low]、[Medium]、[Mission Critical]、または [No Value] です。
- [Target IPv6 Address(es)]：ターゲットの価値レーティングを使用して優先順位を付けるネットワーク資産の IPv6 アドレスを次の形式で示します。

  <XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

  例：2001:0db8:1234:1234:1234:1234:1234:1234,2001:0db8:1234:1234:1234:1234:1234:8888。範囲の 2 番目の IPv6 アドレスは、最初の IPv6 アドレス以上である必要があります。

（注） IPv6 アドレスは、16 進数で表現された 128 ビットであり、コロンにより 8 個の 16 ビットグループに分かれています。先頭のゼロをスキップしたり、中間のゼロのグループを 2 個のコロン（::）で表現できます。アドレスは、プレフィクス 2001:db8 で始める必要があります。

IPv6 ターゲットの価値レーティングの追加、編集、および削除

ネットワーク資産の IPv6 ターゲットの価値レーティングを追加、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] > [Event Action Rules] > [rules0] > [IPv6 Target Value Rating] を選択し、[Add] をクリックします。

ステップ 3　ターゲットの価値レーティングを新しい資産グループに割り当てるには、次の手順を実行します。

a. [Target Value Rating (TVR)] ドロップダウン リストからレーティングを選択します。値は [High]、[Low]、[Medium]、[Mission Critical]、または [No Value] です。

b. [Target IPv6 Address(es)] フィールドに、ネットワーク資産の IP アドレスを入力します。

<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

[Event Variables] タブで定義した変数を使用することもできます。変数の前には $ を付けます。範囲の 2 番目の IPv6 アドレスは、最初の IPv6 アドレス以上である必要があります。

（注） IPv6 アドレスは、16 進数で表現された 128 ビットであり、コロンにより 8 個の 16 ビットグループに分かれています。先頭のゼロをスキップしたり、中間のゼロのグループを 2 個のコロン（::）で表現できます。アドレスは、プレフィクス 2001:db8 で始める必要があります。

ヒント　変更を破棄して [Add IPv6 Target Value Rating] 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。新しい資産の新しいターゲットの価値レーティングが [IPv6 Target Value Rating] タブのリストに表示されます。

ステップ 5　既存のターゲットの価値レーティングを編集するには、リストで選択し、[Edit] をクリックします。

ステップ 6　必要な変更を加えます。

ヒント　変更を破棄して [Edit IPv6 Target Value Rating] 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。編集したネットワーク資産が [IPv6 Target Value Rating] タブのリストに表示されます。

ステップ 8　ネットワーク資産を削除するには、リスト中で選択し、[Delete] をクリックします。ネットワーク資産が [IPv6 Target Value Rating] タブの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 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。

OS ID の設定

ここでは、OS ID 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。

[OS Identifications] タブ

（注）　設定済みの OS マップを追加、編集、および削除するためには、管理者またはオペレータであることが必要です。

学習した OS マップよりも優先される OS ホスト マップを設定するには、[OS Identifications] タブを使用します。[OS Identifications] タブで、設定済みの OS マップの追加、編集、および削除を行うことができます。リスト内で OS マップを上下に移動すると、特定の IP アドレスと OS タイプの組み合わせに対する攻撃関連性レーティングおよびリスク レーティングの計算をセンサーが行う順序を変更できます。

また、リスト内で OS マップを上下に移動すると、特定の IP アドレスに関連付けられている OS をセンサーが解決する順序を変更できます。設定した OS マップでは、範囲を設定できます。そのため、ネットワーク 192.168.1.0/24 の場合、次のように定義できます（表 11-1）。

表 11-1　設定された OS マップの例

IP アドレス範囲の設定	OS
192.168.1.1	IOS
192.168.1.2-192.168.1.10、192.168.1.25	UNIX
192.168.1.1-192.168.1.255	Windows

より特定的なマップをリストの先頭に配置する必要があります。IP アドレス範囲設定では重複は許可されませんが、最もリストの先頭に近いエントリが優先されます。

パッシブ OS フィンガープリントについて

パッシブ OS フィンガープリントにより、センサーはホストが稼動している OS を特定できます。センサーはホスト間のネットワーク トラフィックを分析して、これらのホストの OS をその IP アドレスとともに格納します。センサーはネットワーク上で交換される TCP SYN および SYNACK パケットを検査して、OS タイプを特定します。

次に、センサーはターゲット ホスト OS の OS を使用し、リスク レーティングの攻撃関連性レーティング コンポーネントを計算することによって、攻撃対象への攻撃の関連性を決定します。センサーは、攻撃の関連性に基づいて、攻撃に対するアラートのリスク レーティングを変更したり、攻撃のアラートをフィルタリングしたりする場合があります。ここで、リスク レーティングを使用すると、偽陽性アラートの数を減らしたり（IDS モードの利点）、疑わしいパケットを明確にドロップしたり（IPS モードの利点）できます。また、パッシブ OS フィンガープリントでは、攻撃対象 OS、OS ID のソース、および攻撃対象 OS との関連性をアラート内にレポートすることによって、アラート出力が拡張されます。

パッシブ OS フィンガープリントは、次の 3 つのコンポーネントで構成されます。

- Passive OS learning：パッシブ OS ラーニングは、センサーがネットワーク上のトラフィックを監視しているときに行われます。TCP SYN および SYNACK パケットの特性に基づいて、センサーは送信元 IP アドレスのホスト上で稼動している OS を特定します。
- User-configurable OS identification：学習した OS マップよりも優先される OS ホスト マップを設定できます
- Computation of attack relevance rating and risk rating：センサーは OS 情報を使用して攻撃シグニチャのターゲット ホストに対する関連性を決定します。攻撃の関連性は、攻撃アラートのリスク レーティング値を構成する攻撃関連性レーティング コンポーネントです。センサーは、CSA MC からのホスト ポスチャ情報で報告された OS タイプを使用して攻撃関連性レーティングを計算します。

OS 情報には 3 つのソースがあります。センサーは OS 情報のソースを次の順序でランク付けします。

1. 設定された OS マップ：ユーザが入力する OS マップ。設定された OS マップはイベント アクション規則ポリシーにあり、1 つ以上の仮想センサーに適用できます。

（注）　同じ IP アドレスに対し複数のオペレーティング システムを指定できます。リスト中の最後のオペレーティング システムが照合されます。

2. インポートした OS マップ：外部データ ソースからインポートした OS マップ。インポートした OS マップはグローバルであり、すべての仮想センサーに適用されます。

（注）　現在は CSA MC が唯一の外部データ ソースです。

3. 学習した OS マップ：SYN 制御ビットが設定されている TCP パケットのフィンガープリントを介して、センサーが検知した OS マップ。学習した OS マップは、トラフィックを監視する仮想センサーに対してローカルです。

センサーは、ターゲット IP アドレスの OS を特定する必要がある場合に、設定した OS マップを調べます。ターゲット IP アドレスが設定した OS マップにない場合、センサーはインポートした OS マップを調べます。ターゲット IP アドレスがインポートした OS マップにない場合、センサーは学習した OS マップを調べます。そこでも見つからなかった場合、センサーはターゲット IP の OS を不明として処理します。

（注）　パッシブ OS フィンガープリントはデフォルトでイネーブルになっており、IPS にはシグニチャごとにデフォルトの脆弱な OS リストが含まれています。

パッシブ OS フィンガープリントの設定

パッシブ OS フィンガープリントを使用するために、設定を行う必要はありません。IPS には、各シグニチャについてデフォルトの脆弱な OS のリストが用意されており、パッシブ分析がデフォルトでイネーブルになっています。

パッシブ OS フィンガープリントについて次の側面を設定できます。

- OS マップの定義：OS マップを設定し、重要なシステムで動作している OS の ID を定義することをお勧めします。重要なシステムの OS および IP アドレスが変更される可能性が少ない場合は、OS マップを設定するのが適切です。
- 攻撃関連性レーティング計算を特定の IP アドレス範囲に限定：これにより、攻撃関連性レーティング計算が、保護されたネットワーク上の IP アドレスに限定されます。
- OS マップのインポート：OS マップのインポートは、パッシブ分析を通じて行われる OS ID の学習速度と忠実度を高めるためのメカニズムです。CSA MC などの外部製品インターフェイスがある場合は、そこから OS ID をインポートできます。
- ターゲットの OS 関連性の値を使用したイベント アクション規則フィルタの定義：これは、OS の関連性のみに対してアラートをフィルタするための方法を提供します。
- パッシブ分析のディセーブル化：センサーが新しい OS マップを学習するのを停止します。
- シグニチャ脆弱 OS リストの編集：脆弱 OS リストは、どの OS タイプが各シグニチャに対して脆弱かを指定したものです。デフォルトでは、[General OS] が、脆弱 OS リストを指定しないすべてのシグニチャに適用されます。

[OS Identifications] タブのフィールド定義

[OS Identifications] タブには次のフィールドがあります。

- [Enable passive OS fingerprinting analysis] : オンにすると、センサーによりパッシブ OS 分析が実行されます。
- [Restrict Attack Relevance Ratings (ARR) to these IP addresses] : OS タイプから特定の IP アドレスへのマッピングを設定し、その IP アドレスの攻撃関連性レーティングをセンサーで計算します。
- [Configured OS Maps] : 設定されている OS マップの属性が表示されます。
  - [Name] : 設定されている OS マップに付けた名前が表示されます。
  - [Active] : この設定された OS マップがアクティブかどうか。
  - [IP Address] : この設定された OS マップの IP アドレス。
  - [OS Type] : この設定された OS マップの OS タイプ。

[Add Configured OS Map] および [Edit Configured OS Map] ダイアログボックスの定義

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

- [Name] : この設定された OS マップの名前。
- [Active] : 設定された OS マップをアクティブまたは非アクティブにします。
- [IP Address] : この設定された OS マップに関連付けられている IP アドレス。設定されている OS マップの IP アドレス（かつ設定されている OS マップのみ）は、IP アドレスのセットおよび IP アドレス範囲になります。次に示すのは、すべて設定された OS マップの有効な IP アドレス値です。
  - 10.1.1.1,10.1.1.2,10.1.1.15
  - 10.1.2.1
  - 10.1.1.1-10.2.1.1,10.3.1.1
  - 10.1.1.1-10.1.1.5
- [OS Type] : IP アドレスに関連付ける次の OS タイプのいずれかを選択できます。
  - AIX
  - BSD
  - General OS
  - HP UX
  - IOS
  - IRIX
  - Linux
  - Mac OS
  - Netware
  - その他
  - Solaris

- UNIX
- Unknown OS
- Win NT
- Windows
- Windows NT/2K/XP

設定された OS マップの追加、編集、削除、および移動

設定された OS マップを追加、編集、削除、および移動するには、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] > [Event Action Rules] > [rules0] > [OS Identifications] を選択し、[Add] をクリックします。

ステップ 3　[Name] フィールドに設定される OS マップの名前を入力します。

ステップ 4　[Active] フィールドで、[Yes] オプション ボタンをクリックし、この設定される OS マップをリストに追加して有効にします。

ステップ 5　[IP Address] フィールドに、OS にマッピングするホストの IP アドレスを入力します。たとえば、10.10.5.5,10.10.2.1-10.10.2.30 という形式を使用します。

ステップ 6　[OS Type] ドロップダウン リストから、IP アドレスにマッピングする OS を選択します。

ヒント　変更を破棄して [Add Configured OS Map] 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。新たに設定された OS マップが [OS Identifications] タブのリストに表示されます。

ステップ 8　[Enable passive OS fingerprinting analysis] チェックボックスをオンにします。

（注）　[OS Identifications] タブで [Enable passive OS fingerprinting analysis] チェックボックスをオンにしないと、[Add Configured OS Map] ダイアログボックスで設定する値にかかわらず、設定される OS マップがイネーブルになりません。

ステップ 9　設定された OS マップを編集するには、リスト中で選択し、[Edit] をクリックします。

ステップ 10　必要な変更を加えます。

ヒント　変更を破棄して [Edit Configured OS Map] 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 11　[OK] をクリックします。編集後の設定された OS マップが [OS Identifications] タブのリストに表示されます。

ステップ 12　[Enable passive OS fingerprinting analysis] チェックボックスをオンにします。

（注）　[OS Identifications] タブで [Enable passive OS fingerprinting analysis] チェックボックスをオンにしないと、[Edit Configured OS Map] ダイアログボックスで設定する値にかかわらず、設定された OS マップがイネーブルになりません。

ステップ 13　設定された OS マップを削除するには、リスト中で選択し、[Delete] をクリックします。設定された OS マップが [OS Identifications] タブのリストに表示されなくなります。

ステップ 14　設定された OS マップをリスト中で上下に移動するには、移動対象を選択し、[Move Up] または [Move Down] 矢印をクリックします。

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 15　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。

イベント変数の設定

ここでは、イベント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。

[Event Variables] タブ

（注）　イベント変数を追加、編集、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。

イベント変数を作成し、イベント アクション フィルタでそれらの変数を使用できます。同じ値を複数のフィルタで使用する場合は、変数を使用します。変数の値を変更した場合、その変数を使用するフィルタが新しい値で更新されます。

（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。

IPv4 アドレス

IPv4 アドレスを設定する場合、完全な IP アドレス、範囲、複数の範囲を指定します。

- 10.89.10.10-10.89.10.23
- 10.90.1.1
- 192.56.10.1-192.56.10.255
- 10.1.1.1-10.2.255.255, 10.89.10.10-10.89.10.23

IPv6 アドレス

IPv6 アドレスを設定する場合は、次の形式を使用します。

<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

（注） IPv6 アドレスは、16 進数で表現された 128 ビットであり、コロンにより 8 個の 16 ビット グループに分かれています。先頭のゼロをスキップしたり、中間のゼロのグループを 2 個のコロン（::）で表現できます。アドレスは、プレフィクス 2001:db8 で始める必要があります。

ワンポイントアドバイス エンジニアリング グループに割り当てられる IP アドレス スペースがあり、そのグループに Windows システムが存在せず、そのグループに対する Windows 関連の攻撃を心配する必要がない場合、変数をそのエンジニアリング グループの IP アドレス スペースとして設定できます。次に、この変数を使用して、このグループに対するすべての Windows 関連の攻撃を無視するフィルタを設定できます。

[Event Variables] タブのフィールド定義

[Event Variables] タブには次のフィールドがあります。

- [Name]：この変数の名前を割り当てることができます。
- [Type]：変数をアドレスとして識別します。
- [Value]：この変数によって表される値を追加できます。

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

[Add Event Variable] および [Edit Event 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]：この変数の名前を割り当てることができます。
- [Type]：変数を IPv4 または IPv6 アドレスとして識別します。
  - [address]：IPv4 アドレスの場合は、完全な IP アドレス、範囲、複数の範囲を使用します。
  - [ipv6-address]：IPv6 アドレスの場合は次の形式を使用します。

    <XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

（注）　IPv6 アドレスは、16 進数で表現された 128 ビットであり、コロンにより 8 個の 16 ビット グループに分かれています。先頭のゼロをスキップしたり、中間のゼロのグループを 2 個のコロン（::）で表現できます。アドレスは、プレフィクス 2001:db8 で始める必要があります。

– [Value]：この変数によって表される値を追加できます。

イベント変数の追加、編集、削除

イベント変数を追加、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] > [Event Action Rules] > [rules0] > [Event Variables] を選択し、[Add] をクリックします。

ステップ 3　[Name] フィールドにこの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 リストから、IPv4 アドレスの場合は [address] を選択し、IPv6 のアドレスの場合は [ipv6-address] を選択します。

ステップ 5　[Value] フィールドにこの変数の値を入力します。

IPv4 アドレスの場合、完全な IP アドレス、範囲、複数の範囲を指定します。例：

- 10.89.10.10-10.89.10.23
- 10.90.1.1
- 192.56.10.1-192.56.10.255

（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。

IPv6 アドレスの場合は次の形式を使用します。

<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>[,<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>-<XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX:XXXX>]

（注）　IPv6 アドレスは、16 進数で表現された 128 ビットであり、コロンにより 8 個の 16 ビット グループに分かれています。先頭のゼロをスキップしたり、中間のゼロのグループを 2 個のコロン（::）で表現できます。アドレスは、プレフィクス 2001:db8 で始める必要があります。

ヒント　変更内容を破棄して [Add Event 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 [Event Variables] タブの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、リストで選択し、[Edit] をクリックします。

ステップ 8　必要な変更を加えます。

ヒント　変更内容を破棄して [Edit Event 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。編集したイベント変数が [Event Variables] タブのリストに表示されます。

ステップ 10　イベント変数を削除するには、リストで選択し、[Delete] をクリックします。イベント変数が [Event Variables] タブの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。

リスク カテゴリの設定

ここでは、リスク カテゴリの設定方法について説明します。内容は次のとおりです。

[Risk Category] タブ

（注）　リスク レベルを追加および編集するには、管理者であることが必要です。

[Risk Category] タブで、定義済みのリスク カテゴリ（HIGHRISK、MEDIUMRISK、および LOWRISK）を使用するか、独自のラベルを定義できます。リスク カテゴリは、カテゴリ名を、リスク レーティングを定義する数値の範囲にリンクします。範囲を連続したものにするには、カテゴリに低いしきい値を指定します。上位のカテゴリは、次に高いカテゴリまたは 100 です。

その後、脅威を赤、黄、緑のカテゴリにグループ分けできます。これらの赤、黄、緑のしきい値統計情報は、イベント アクション オーバーライドで使用され、[Home] ページの [Network Security Gadget] にも表示されます。

（注）　定義済みのリスク カテゴリは削除できません。

赤、黄、緑のしきい値統計情報は、ネットワーク セキュリティの状態を表し、赤が最も重大です。しきい値を変更した場合、リスク カテゴリと同じ範囲のすべてのイベント アクション オーバーライドが、新しい範囲を反映するように変更されます。

新しいカテゴリは、そのしきい値に従って [Risk Category] リストに挿入され、その範囲をカバーするアクションが自動的に割り当てられます。

[Risk Category] タブのフィールド定義

[Risk Category] タブには次のフィールドがあります。

- [Risk Category Name]：このリスク レベルの名前。定義済みのカテゴリには次の値があります。
  - HIGHRISK：90（90 ～ 100）
  - MEDIUMRISK：70（70 ～ 89）
  - LOWRISK：1（1 ～ 69）
- [Risk Threshold]：このリスクのしきい値。値は 0 ～ 100 の数字です。
- [Risk Range]：このリスク カテゴリのリスク レーティング範囲。

  リスク レーティングとは、ネットワーク上の特定のイベントに関連付けられたリスクを数値化した、0 ～ 100 の範囲の値です。
- [Network Security Health Statistics]：赤、黄、緑のしきい値の数を一覧表示します。ネットワーク全体のセキュリティ値は、最も安全でない値（緑が最も安全で赤が最も安全でない）を表します。これらの色しきい値は、[Home] ペインの [Sensor Health] ガジェットを参照します。
  - Red Threat Threshold
  - Yellow Threat Threshold
  - Green Threat Threshold

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

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

- [Risk Name]：このリスク レベルの名前。
- [Risk Threshold]：このリスク レベルのリスクしきい値を割り当てることができます。

  リスク カテゴリが連続したものになるように、カテゴリの下限しきい値のみを指定または変更できます。上限しきい値は、次に高いカテゴリまたは 100 です。
- [Active]：このリスク レベルをアクティブにします。

リスク カテゴリの追加、編集、削除

リスク カテゴリを追加、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] > [Event Action Rules] > [rules0] > [Risk Category] を選択し、[Add] をクリックします。

ステップ 3　[Risk Name] フィールドに、このリスク カテゴリの名前を入力します。

ステップ 4　[Risk Threshold] フィールドに、リスクしきい値の数値（最小 0、最大 100）を入力します。この数値はリスクの下限を表します。範囲は [Risk Range] フィールドと、赤、黄、緑のしきい値フィールドに表示されます。

ステップ 5　このリスク カテゴリをアクティブにするには、[Yes] オプション ボタンをクリックします。

ヒント　変更内容を破棄して [Add Risk Category] 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。新しいリスク カテゴリが [Risk Category] タブのリストに表示されます。

ステップ 7　既存のリスク カテゴリを編集するには、リストで選択し、[Edit] をクリックします。

ステップ 8　必要な変更を加えます。

ヒント　変更内容を破棄して [EditRisk Category] 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。編集したリスク カテゴリが [Risk Category] タブのリストに表示されます。

ステップ 10　リスク カテゴリを削除するには、リスト中で選択し、[Delete] をクリックします。リスク カテゴリが [Risk Category] タブの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。

一般設定

ここでは、一般的な設定を行う方法について説明します。内容は次のとおりです。

- 「[General] タブ」（P.11-35）
- 「[General] タブのフィールド定義」（P.11-36）
- 「一般的な設定」（P.11-37）

[General] タブ

（注）　イベント アクション規則の一般的な設定を行うには、管理者またはオペレータであることが必要です。

Summarizer や Meta Event Generator を使用するかどうかなど、イベント アクション規則全体に適用される一般的な設定を行うことができます。Summarizer はイベントを単一アラートにグループ化するため、センサーが送信するアラートの数が減少します。Meta Event Generator はコンポーネント イベントを処理します。これによって、センサーは一連のイベントで疑わしいアクティビティが発生していないかどうかを監視できます。

注意　トラブルシューティング目的以外では、Summarizer または Meta Event Generator をディセーブルにしないでください。Summarizer をディセーブルにすると、すべてのシグニチャがサマライズなしの [Fire All] に設定されます。Meta Event Generator をディセーブルにすると、すべてのメタ エンジン シグニチャがディセーブルになります。

また、脅威レーティングの調整、イベント アクション フィルタの使用、一方向の TCP リセットのイネーブル化を行うこともできます。一方向の TCP リセットはインライン モードでだけ動作し、Deny Packet Inline アクションに自動追加されます。TCP リセットがアラートの攻撃対象に送信されるため、攻撃者に対してブラック ホールが作成され、攻撃対象の TCP リソースがクリアされます。

（注）　これにより、インライン センサーで、リスク レーティングが 90 以上のアラートのパケットを拒否されるようになります。また、リスク レーティングが 90 以上の TCP アラートで、一方向 TCP リセットを発行します。

攻撃者を拒否する期間、拒否攻撃者の最大数、ブロックの継続期間を設定できます。

[General] タブのフィールド定義

[General] タブには次のフィールドがあります。

- [Use Summarizer] : Summarizer コンポーネントをイネーブルにします。デフォルトでは、Summarizer はイネーブルになります。ディセーブルにすると、すべてのシグニチャがサマライズなしの [Fire All] に設定されます。サマライズするように個別のシグニチャを設定しても、この設定は Summarizer がイネーブルになっていない場合は無視されます。
- [Use Meta Event Generator] : Meta Event Generator をイネーブルにします。デフォルトでは、Meta Event Generator はイネーブルになります。Meta Event Generator をディセーブルにすると、すべてのメタ エンジン シグニチャがディセーブルになります。
- [Use Threat Rating Adjustment] : 脅威レーティングの調整がイネーブルになり、これによってリスク レーティングが調整されます。ディセーブルにすると、リスク レーティングは脅威レーティングと等しくなります。
- [Use Event Action Filters] : イベント アクション フィルタ コンポーネントをイネーブルにします。イネーブルになっているいずれかのフィルタを使用するには、このチェックボックスをオンにする必要があります。
- [Enable One Way TCP Reset] :（インラインのみ）TCP ベースのアラートで、拒否パケット インライン アクションの一方向の TCP リセットをイネーブルにします。TCP リセットがアラートの攻撃対象に送信されるため、攻撃対象の TCP リソースがクリアされます。
- [Deny Attacker Duration] : 攻撃者をインラインで拒否する秒数。有効な範囲は 0 ～ 518400 です。デフォルトは 3600 です。
- [Block Action Duration] : ホストまたは接続をブロックする時間（分単位）。有効な範囲は 0 ～ 10000000 です。デフォルトは 30 です。
- [Maximum Denied Attackers] : 一度にシステム内に許容できる拒否攻撃者の数を制限します。有効な範囲は 0 ～ 100000000 です。デフォルトは 10000 です。

一般的な設定

注意　一般設定オプションはグローバル レベルで動作するため、イネーブルにするとこれらの機能のすべてのセンサー処理に影響があります。

イベント アクション規則の一般的な設定を行うには、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] > [Event Action Rules] > [rules0] > [General] を選択します。

ステップ 3　Summarizer の機能をイネーブルにするには、[Use Summarizer] チェックボックスをオンにします。

注意　Summarizer は、トラブルシューティング目的でのみディセーブルにします。それ以外の場合は、サマライズ用に設定したすべてのシグニチャが実際にサマライズされるように、Summarizer をイネーブルにしてください。

ステップ 4　Meta Event Generator をイネーブルにするには、[Use Meta Event Generator] チェックボックスをオンにします。

注意　Meta Event Generator は、トラブルシューティング目的でのみディセーブルにします。それ以外の場合は、すべての Meta エンジンのシグニチャが機能するように、Meta Event Generator をイネーブルにしてください。

ステップ 5　脅威レーティング調整をイネーブルにするには、[Use Threat Rating Adjustment] チェックボックスをオンにします。

ステップ 6　イベント アクション フィルタをイネーブルにするには、[Use Event Action Filters] チェックボックスをオンにします。

（注）　[Configuration] > se*nsor_name* > [Policies] > [Event Action Rules] > [rules0] > [Event Action Filters] ペインで設定したイベント アクション フィルタがアクティブになるように、[General] ペインの [Use Event Action Filters] チェックボックスをオンにする必要があります。

ステップ 7　拒否パケット インライン アクションで一方向の TCP リセットをイネーブルにするには、[Enable One Way TCP Reset] チェックボックスをオンにします。

ステップ 8　[Deny Attacker Duration] フィールドに、攻撃者をインラインで拒否する秒数を入力します。

ステップ 9　[Block Action Duration] フィールドに、ホストまたは接続をブロックする期間を分単位で入力します。

ステップ 10　[Maximum Denied Attackers] フィールドに、同時に拒否する拒否攻撃者の最大数を入力します。

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 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。

CHAPTER 12

異常検出の設定

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

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

（注） AIP SSC-5 は異常検出をサポートしていません。

この章では、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。

異常検出コンポーネント

（注） AIP SSC-5 は異常検出をサポートしていません。

ここでは、異常検出の各種コンポーネントについて説明します。内容は次のとおりです。

異常検出について

注意 異常検出は、トラフィックが両方向から来ることを前提としています。センサーがトラフィックの一方向だけを参照するように設定されている場合は、異常検出をオフにする必要があります。そうしないと、異常検出が非対称環境で実行されている場合に、すべてのトラフィックに不完全な接続（スキャナ）があるものと識別され、すべてのトラフィック フローについてアラートが送信されます。

センサーの異常検出コンポーネントでは、ワームに感染したホストが検出されます。これによりセンサーでは、Code Red や SQL Slammer などのワームやスキャナからの保護に際してシグニチャ アップデートへの依存度が低くなります。異常検出コンポーネントでは、センサーが正常なアクティビティを学習し、正常な動作として学習した動作から逸脱する動作に対してアラートを送信するか、または動的応答アクションを実行します。

（注） 異常検出では、Nimda などの電子メール ベースのワームは検出されません。

異常検出では、次の 2 つの状況が検出されます。

- ワーム トラフィックによって輻輳し始めたパスでネットワークが起動した場合。
- ワームに感染した単一のソースがネットワークに入り、他の脆弱なホストのスキャンを開始した場合。

詳細情報

- ワームの動作の詳細については、「ワーム」（P.12-3）を参照してください。
- 異常検出をオフにする手順については、「異常検出のディセーブル化」（P.12-37）を参照してください。

ワーム

注意　異常検出は、トラフィックが両方向から来ることを前提としています。センサーがトラフィックの一方向だけを参照するように設定されている場合は、異常検出をオフにする必要があります。そうしないと、異常検出が非対称環境で実行されている場合に、すべてのトラフィックに不完全な接続（スキャナ）があるものと識別され、すべてのトラフィック フローについてアラートが送信されます。

ワームは、自身のコピーを作成してその拡散を促進する自動化された自己伝播型侵入エージェントです。ワームは脆弱なホストを攻撃して感染させ、そのホストをベースとして使用して他の脆弱なホストを攻撃します。ネットワーク インスペクションの 1 つの形式（通常はスキャン）を使用して他のホストを検索し、次のターゲットに伝播します。スキャニング ワームは、プローブする IP アドレスのリストを生成することによって脆弱なホストを特定し、ホストにアクセスします。Code Red ワーム、Sasser ワーム、Blaster ワーム、および Slammer ワームは、この方法で広がるワームの例です。

異常検出は、スキャナとして動作していることを手がかりとして、ワームに感染したホストを特定します。ワームは、拡散するために新しいホストを見つける必要があります。TCP や UDP などのプロトコルを使用してインターネットやネットワークをスキャンし、異なる宛先 IP アドレスへの、失敗するアクセス試行を生成することによってホストを見つけます。スキャナは、非常に多くの宛先 IP アドレスに対して（TCP および UDP で）同じ宛先ポートにイベントを生成する送信元 IP アドレスとして定義されます。

TCP プロトコルにとって重要なイベントは、一定時間内に SYN-ACK 応答のない SYN パケットなどの未確立の接続です。TCP プロトコルを使用してスキャンする、ワームに感染したホストは、同じ宛先ポートにおいて異常な数の IP アドレスに対する未確立接続を生成します。

UDP プロトコルにとって重要なイベントは、すべてのパケットが一方向だけに送信される単方向接続（UDP 接続など）です。ワームに感染したホストが UDP プロトコルを使用してスキャンを行う場合、タイムアウト期間内に同じクワッド上で複数の宛先 IP アドレスについて同じ宛先ポートで UDP パケットを生成しますが、受信はしません。

それ以外のプロトコル（ICMP など）にとって重要なイベントは、送信元 IP アドレスから多くの異なる宛先 IP アドレスに送信されるイベント、つまり一方向でのみ受信されるパケットです。

注意　感染の標的とする IP アドレスのリストがワームにあり、自己増殖のためにスキャンする必要がない場合（能動的なスキャンとは逆にネットワークをリッスンする受動的なマッピングなど）、異常検出ワーム ポリシーでは検出されません。感染したホスト内でファイルをプローブすることによってメーリング リストを受信し、そのリストにメールを送信するワームも検出されません。これは、レイヤ 3/ レイヤ 4 の異常が生成されからためです。

詳細情報

異常検出をオフにする手順については、「異常検出のディセーブル化」（P.12-37）を参照してください。

異常検出モード

異常検出は、最初に「正常時」学習プロセスを実行します。この処理の間にネットワークの正常な状態の大部分が異常検出に反映されます。次に、異常検出は正常なネットワークに最適な一連のポリシーしきい値を生成します。

異常検出には次のモードがあります。

- 学習受け入れモード

  異常検出はデフォルトで検出モードになっていますが、デフォルトで 24 時間、初期の学習受け入れモードを実行します。このフェーズ中は攻撃が行われないことを前提とします。異常検出は、ネットワーク トラフィックの初期ベースラインを作成します。これはナレッジ ベース（KB）と呼ばれます。定期スケジュールのデフォルトの間隔値は 24 時間で、デフォルトのアクションは循環です。これは、新しい KB が保存およびロードされ、24 時間後に初期 KB と置き換わることを意味します。

  （注）　異常検出は、空の初期 KB を処理するときには攻撃を検出しません。デフォルトの 24 時間が経過すると、KB が保存およびロードされ、異常検出も攻撃の検出を開始します。

  （注）　ネットワークの複雑さによっては、異常検出の学習受け入れモードをデフォルトの 24 時間よりも長くした方がよい場合もあります。

- 検出モード

  操作の進行中は、センサーを検出モードのままにする必要があります。これは 1 日 24 時間、週 7 日間実行します。KB が作成され、初期 KB と置き換えられると、異常検出はその KB に基づいて攻撃を検出します KB のしきい値に違反するネットワーク トラフィック フローを検知すると、アラートを送信します。異常検出は、異常を検出しながら、しきい値に違反しない段階的な変化を KB に記録して新しい KB を作成します。新しい KB が定期的に保存され、元の KB と置き換えられるため、KB は常に最新の状態に維持されます。

- 非アクティブ モード

  異常検出は、非アクティブ モードにすることでオフにできます。センサーが非対称環境で稼動している場合など、特定の状況では、異常検出を非アクティブ モードにする必要があります。異常検出では、トラフィックが両方向から来ることを前提とするため、センサーがトラフィックの一方向だけを参照するように設定されている場合は、異常検出によってすべてのトラフィックに不完全な接続（スキャナ）があるものと識別され、すべてのトラフィック フローについてアラートが送信されます。

次の例で、デフォルトの異常検出設定についてまとめます。仮想センサーを午後 11:00 に追加して、デフォルトの異常検出設定を変更しない場合、異常検出は初期 KB で動作を開始し、学習のみを実行します。これは検出モードですが、情報を 24 時間収集して初期 KB を置換するまで、攻撃を検出できません。最初の収集期間（デフォルトで 24 時間）が経過した後の最初の開始時刻（デフォルトでは午前 10:00）に、学習結果が新しい KB に保存され、この KB がロードされて初期 KB と置き換わります。異常検出はデフォルトで検出モードになっているため、新しい KB が用意できると、攻撃の検出を開始します。

詳細情報

- ワームの動作の詳細については、「ワーム」（P.12-3）を参照してください。
- センサーのモードを変更する手順については、「仮想センサーの追加、編集、削除」（P.8-13）を参照してください。

異常検出ゾーン

ネットワークをゾーンに分割することで、偽陰性の率を低下させることができます。ゾーンは、宛先 IP アドレスのセットです。ゾーンには、内部、不正、外部の 3 つがあり、それぞれに独自のしきい値があります。

外部ゾーンは、デフォルトのインターネット範囲（0.0.0.0 ～ 255.255.255.255）を持つデフォルトのゾーンです。デフォルトでは、内部ゾーンと不正ゾーンには IP アドレスは含まれません。内部ゾーンまたは不正ゾーンに含まれる IP アドレスのセットに一致しないパケットは、外部ゾーンで処理されます

内部ネットワークの IP アドレス範囲を使用して内部ゾーンを設定することを推奨します。このように設定すると、内部ゾーンには内部ネットワークの IP アドレス範囲に到着するすべてのトラフィックが含まれ、外部ゾーンにはインターネットに送信されるすべてのトラフィックが含まれます。

不正ゾーンには、割り当てられていない IP アドレスや、使用されていない内部 IP アドレス範囲に属する IP アドレスなど、正常なトラフィックに存在してはならない IP アドレスの範囲を設定できます。不正ゾーンには適正なトラフィックが到達しないと想定されるため、このゾーンは正確な検出に非常に役立ちます。これにより、非常に迅速なワーム ウイルス検出を可能にする非常に低いしきい値を設定できます。

詳細情報

ゾーンの設定の詳細については、「内部ゾーンの設定」（P.12-14）、「不正ゾーンの設定」（P.12-22）、および「不正ゾーンの設定」（P.12-22）を参照してください。

異常検出の設定手順

異常検出の検出部分を設定できます。しきい値のセットを設定し、学習によって KB に追加されたしきい値を上書きできます。ただし、異常検出は検出の設定に関係なく学習を継続します。KB をインポート、エクスポート、ロードできるほか、KB データを表示することもできます。

異常検出を設定するときには、次の手順に従ってください。

1. 仮想センサーに追加する異常検出ポリシーを作成します。デフォルトの異常検出ポリシー ad0 を使用することもできます。
2. 異常検出ポリシーを仮想センサーに追加します。
3. 異常検出ゾーンとプロトコルを設定します。
4. デフォルトでは、動作モードが検出に設定されていますが、最初の 24 時間は学習を実行し、KB のデータを作成します。初期 KB は空で、デフォルトの 24 時間の間に、異常検出が KB に取り込むデータを収集します。学習プロセスの時間をデフォルトの 24 時間よりも長くする場合は、モードを手動で学習受け入れモードに設定する必要があります。
5. センサーを最低でも 24 時間（デフォルト）、学習受け入れモードで動作させます。初期 KB 用にネットワークの正常な状態の情報を収集できるように、センサーを最低 24 時間、学習受け入れモードで動作させる必要があります。ただし、ネットワークの複雑さに応じて学習受け入れモードの時間を変更する必要があります。

（注）　最低 24 時間はセンサーを学習受け入れモードにしておくことを推奨しますが、それよりも長く（場合によっては 1 週間）学習受け入れモードで動作させると、さらによい結果が得られます。

この期間の後、センサーは初期 KB をネットワークの正常なアクティビティのベースラインとして保存します。

6. 異常検出を手動で学習受け入れモードに設定した場合は、検出モードに戻してください。
7. 異常検出パラメータを設定します。
   - ワームのタイムアウトと、異常検出がバイパスする送信元 IP アドレスおよび宛先 IP アドレスを設定します。このタイムアウトの後、スキャナしきい値は設定された値に戻ります。
   - 異常検出が検出モードのときに KB の自動更新をイネーブルにするかどうかを決定します。
   - デフォルトの Produce Alert 以外のイベント アクションも実行されるように、18 個の異常検出ワーム シグニチャを設定します。たとえば、Deny Attacker イベント アクションをシグニチャに設定します。

詳細情報

- 異常検出のモードを変更する手順については、「仮想センサーの追加、編集、削除」（P.8-13）を参照してください。
- 新しい異常検出ポリシーを設定する手順については、「異常検出ポリシーの設定」（P.12-8）を参照してください。
- ゾーンの設定の詳細については、「内部ゾーンの設定」（P.12-14）、「不正ゾーンの設定」（P.12-22）、および「不正ゾーンの設定」（P.12-22）を参照してください。
- 異常検出モードの詳細については、「異常検出モード」（P.12-4）を参照してください。
- 学習受け入れモードの設定の詳細については、「学習受け入れモードの設定」（P.12-11）を参照してください。
- 異常検出シグニチャの設定の詳細については、「異常検出シグニチャ」（P.12-6）を参照してください。
- Deny Attacker イベント アクションの詳細については、「イベント アクション」（P.11-8）を参照してください。

異常検出シグニチャ

トラフィック異常エンジンには、3 つのプロトコル（TCP、UDP、およびその他）をカバーする 9 つの異常検出シグニチャが含まれます。各シグニチャには 2 つのサブシグニチャがあります。一方はスキャナ用で、もう一方はワームに感染したホスト（またはワーム攻撃されているスキャナ）用です。異常検出は、異常を検出すると、これらのシグニチャのアラートをトリガーします。すべての異常検出シグニチャは、デフォルトでイネーブルになり、各シグニチャのアラート重大度は高く設定されます。

スキャナが検出されても、ヒストグラム異常が発生しない場合、スキャナ シグニチャはその攻撃者（スキャナ）の IP アドレスをファイルに保存します。ヒストグラム シグニチャがトリガーされた場合は、スキャンを行っている攻撃者のアドレスによってそれぞれ（スキャナ シグニチャではなく）ワーム シグニチャがトリガーされます。ヒストグラムがトリガーされているので、アラートの詳細には、ワーム検出に使用されたしきい値が表示されます。その時点から、すべてのスキャナがワーム感染ホストとして検出されます。アラートの重大度

次の異常検出イベント アクションが可能です。

- [Produce Alert]：イベントをイベント ストアに書き込みます。
- [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。

- [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 ロギングを開始します。
- [Deny Attacker Service Pair Inline]：送信元 IP アドレスと宛先ポートをブロックします。
- [SNMP Trap]：SNMP 通知の実行要求を NotificationApp に送信します。
- [Request Block Host]：このホスト（攻撃者）をブロックする要求を ARC に送信します。

表 12-1 に、異常検出ワーム シグニチャを示します。

表 12-1　異常検出ワーム シグニチャ

シグニチャ ID	サブシグニチャ ID	名前	説明
13000	0	Internal TCP Scanner	内部ゾーンで TCP プロトコル上に単一スキャナを識別しました。
13000	1	Internal TCP Scanner	内部ゾーンで TCP プロトコル上にワーム攻撃を識別しました。TCP ヒストグラムのしきい値を超え、TCP プロトコル上にスキャナが識別されました。
13001	0	Internal UDP Scanner	内部ゾーンで UDP プロトコル上に単一スキャナを識別しました。
13001	1	Internal UDP Scanner	内部ゾーンで UDP プロトコル上にワーム攻撃を識別しました。UDP ヒストグラムのしきい値を超え、UDP プロトコル上にスキャナが識別されました。
13002	0	Internal Other Scanner	内部ゾーンでその他のプロトコル上に単一スキャナを識別しました。
13002	1	Internal Other Scanner	内部ゾーンでその他のプロトコル上にワーム攻撃を識別しました。その他のヒストグラムのしきい値を超え、その他のプロトコル上にスキャナが識別されました。
13003	0	External TCP Scanner	外部ゾーンで TCP プロトコル上に単一スキャナを識別しました。
13003	1	External TCP Scanner	外部ゾーンで TCP プロトコル上にワーム攻撃を識別しました。TCP ヒストグラムのしきい値を超え、TCP プロトコル上にスキャナが識別されました。
13004	0	External UDP Scanner	外部ゾーンで UDP プロトコル上に単一スキャナを識別しました。
13004	1	External UDP Scanner	外部ゾーンで UDP プロトコル上にワーム攻撃を識別しました。UDP ヒストグラムのしきい値を超え、UDP プロトコル上にスキャナが識別されました。
13005	0	External Other Scanner	外部ゾーンでその他のプロトコル上に単一スキャナを識別しました。
13005	1	External Other Scanner	外部ゾーンでその他のプロトコル上にワーム攻撃を識別しました。その他のヒストグラムのしきい値を超え、その他のプロトコル上にスキャナが識別されました。

表 12-1　異常検出ワーム シグニチャ（続き）

シグニチャ ID	サブシグニチャ ID	名前	説明
13006	0	Illegal TCP Scanner	不正ゾーンで TCP プロトコル上に単一スキャナを識別しました。
13006	1	Illegal TCP Scanner	不正ゾーンで TCP プロトコル上にワーム攻撃を識別しました。TCP ヒストグラムのしきい値を超え、TCP プロトコル上にスキャナが識別されました。
13007	0	Illegal UDP Scanner	不正ゾーンで UDP プロトコル上に単一スキャナを識別しました。
13007	1	Illegal UDP Scanner	不正ゾーンで UDP プロトコル上にワーム攻撃を識別しました。UDP ヒストグラムのしきい値を超え、UDP プロトコル上にスキャナが識別されました。
13008	0	Illegal Other Scanner	不正ゾーンでその他のプロトコル上に単一スキャナを識別しました。
13008	1	Illegal Other Scanner	不正ゾーンでその他のプロトコル上にワーム攻撃を識別しました。その他のヒストグラムのしきい値を超え、その他のプロトコル上にスキャナが識別されました。

詳細情報

シグニチャにアクションを割り当てる手順については、「シグニチャへのアクションの割り当て」（P.9-19）を参照してください。

異常検出ポリシーの設定

ここでは、異常検出ポリシーを作成する方法について説明します。内容は次のとおりです。

[Anomaly Detections] ペイン

（注） 異常検出ポリシーを追加、クローニング、または削除するには、管理者またはオペレータであることが必要です。

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。

異常検出ポリシーを追加、クローニング、または削除するには、[Anomaly Detections] ペインを使用します。デフォルトの異常検出ポリシーは ad0 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、新しいポリシー インスタンスが作成されます。応答が成功すると、[Anomaly Detections] 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。

[Anomaly Detections] ペインのフィールド定義

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

- [Policy Name]：異常検出ポリシーの名前を示します。
- [Assigned Virtual Sensor]：この異常検出ポリシーが割り当てられた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。

- [Policy Name]：異常検出ポリシーの名前を示します。

異常検出ポリシーの追加、クローニング、削除

異常検出ポリシーを追加、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] > [Anomaly Detections] を選択し、[Add] をクリックします。

ステップ 3　[Policy Name] フィールドに、異常検出ポリシーの名前を入力します。

ヒント　変更を破棄して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。[Anomaly Detections] ペインのリストに異常検出ポリシーが表示されます。

ステップ 5　既存の異常検出ポリシーをクローニングするには、リストで異常検出ポリシーを選択し、[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ます。既存の異常検出ポリシー名に「_copy」が追加されています。

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　変更を破棄して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。クローニングされた異常検出ポリシーが [Anomaly Detections] ペインに表示されます。

ステップ 8　異常検出ポリシーを削除するには、そのポリシーを選択し、[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　デフォルトの異常検出ポリシーである ad0 は削除できません。

ステップ 9　[Yes] をクリックします。削除した異常検出ポリシーは、[Anomaly Detections] ペインのリストに表示されなくなります。

[ad0] ペイン

[ad0] ペイン（デフォルト）には、異常検出の設定ツールがあります。次の 5 つのタブがあります。

- [Operation Settings]：ワームのタイムアウトと、異常検出処理の実行中にセンサーが無視する送信元 IP アドレスおよび宛先 IP アドレスを設定できます。
- [Learning Accept Mode]：センサーによる学習 KB の自動受け入れと学習済み KB の受け入れスケジュールの設定をイネーブルにできます。
- [Internal Zone]：内部ゾーンの宛先 IP アドレスとしきい値を設定できます。
- [Illegal Zone]：不正ゾーンの宛先 IP アドレスとしきい値を設定できます。
- [External Zone]：外部ゾーンのしきい値を設定できます。

動作設定

ここでは、動作設定を行う方法について説明します。内容は次のとおりです。

- 「[Operation Settings] タブ」（P.12-10）
- 「[Operation Settings] タブのフィールド定義」（P.12-11）
- 「異常検出の動作設定」（P.12-11）

[Operation Settings] タブ

（注）　異常検出の動作設定を行うには、管理者またはオペレータであることが必要です。

[Operation Settings] タブでは、ワーム検出のタイムアウトを設定できます。このタイムアウトの後、スキャナしきい値は設定された値に戻ります。異常検出が KB の情報を収集するときにセンサーが無視する送信元 IP アドレスおよび宛先 IP アドレスも設定できます。異常検出は、これらの送信元 IP アドレスおよび宛先 IP アドレスを追跡せず、KB のしきい値はこれらの IP アドレスの影響を受けません。

[Operation Settings] タブのフィールド定義

[Operation Settings] タブには次のフィールドがあります。

- [Worm Timeout]：ワーム終了タイムアウトの時間を秒単位で設定できます。範囲は 120 ～ 10,000,000 秒です。デフォルトは 600 秒です。
- [Configure IP address ranges to ignore during anomaly detection processing]：異常検出の処理中に無視する IP アドレスを入力します。
  - [Enable ignored IP Addresses]：オンにすると、無視された IP アドレスのリストがイネーブルになります。
  - [Source IP Addresses]：異常検出で無視する送信元 IP アドレスを入力します。
  - [Destination IP Addresses]：異常検出で無視する宛先 IP アドレスを入力します。

異常検出の動作設定

異常検出の動作設定を行うには、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] > [Anomaly Detections] > [ad0] > [Operation Settings] を選択します。

ステップ 3　[Worm Timeout] フィールドに、ワーム検出がタイムアウトになるまでの時間を秒単位で入力します。範囲は 120 ～ 10,000,000 秒です。デフォルトは 600 秒です。

ステップ 4　無視された IP アドレスのリストをイネーブルにするには、[Enable ignored IP Addresses] チェックボックスをオンにします。

（注）　[Enable ignored IP Addresses] チェックボックスをオンにしなければ、入力した IP アドレスはすべて無視されません。

ステップ 5　[Source IP Addresses] フィールドに、異常検出で無視する送信元 IP アドレスまたはアドレスの範囲を入力します。有効な形式は 10.10.5.5,10.10.2.1-10.10.2.30 です。

ステップ 6　[Destination IP Addresses] フィールドに、異常検出で無視する宛先 IP アドレスまたはアドレスの範囲を入力します。

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 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。

学習受け入れモードの設定

ここでは、学習受け入れモードの設定方法について説明します。内容は次のとおりです。

- 「[Learning Accept Mode] タブ」（P.12-12）
- 「KB とヒストグラム」（P.12-12）

- 「[Learning Accept Mode] タブのフィールド定義」（P.12-13）
- 「[Add Start Time] および [Edit Start Time] ダイアログボックスのフィールド定義」（P.12-13）
- 「学習受け入れモードの設定」（P.12-13）

[Learning Accept Mode] タブ

（注）　学習受け入れモードを設定するには、管理者またはオペレータであることが必要です。

[Learning Accept Mode] タブでは、センサーが一定時間ごとに新しい KB を作成するかどうかを設定します。KB を作成し、ロード（[Rotate]）するか保存（[Save Only]）するかを設定できます。KB のロードまたは保存の頻度と時期を設定できます。生成されたファイルのデフォルト名は *YYYY-Mon-dd-hh_mm_ss* です。*Mon* は、当月の 3 文字の省略形です。

KB とヒストグラム

KB はツリー構造になっており、次の情報が含まれています。

- KB 名
- ゾーン名
- Protocol
- サービス

KB には、スキャナしきい値とヒストグラムがサービスごとに保存されます。学習受け入れモードを自動に設定し、アクションを [Rotate] に設定した場合、新しい KB は 24 時間ごとに作成され、作成後 24 時間にわたり使用されます。学習受け入れモードを自動に設定し、アクションを [Save Only] に設定すると、新しい KB は作成されますが、現在の KB が使用されます。学習受け入れモードを自動に設定しない場合、KB は作成されません。

（注）　学習受け入れモードでは、センサーのローカル時刻が使用されます。

スキャナしきい値は、1 つの送信元 IP アドレスがスキャンできるゾーン IP アドレスの最大数を定義します。ヒストグラムしきい値は、指定された数を超えるゾーン IP アドレスをスキャンできる送信元 IP アドレスの最大数を定義します。

異常検出は、攻撃が行われていない状態で学習したヒストグラムからの逸脱を発見した場合（つまり、定義されている数を超えるゾーン宛先 IP アドレスを同時にスキャンする送信元 IP アドレスの数が超過した場合）、ワーム攻撃と認識します。たとえば、ポート 445 に対するスキャンしきい値が 300 の場合、異常検出は、350 個のゾーン宛先 IP アドレスをスキャンするスキャナを検出すると、マス スキャナが検出されたことを示すアクションを生成します。ただし、このスキャナでは、ワーム攻撃が進行中かどうかはまだ確認されていません。表 12-2 で、この例について説明します。

表 12-2　ヒストグラムの例

送信元 IP アドレス数	10	5	2
宛先 IP アドレス数	5	20	100

異常検出は、ポート 445 で 50 を超えるゾーン宛先 IP アドレスを同時にスキャンする送信元 IP アドレスを 6 つ検出すると、ポート 445 でワーム攻撃が検出されたことを示す、送信元 IP アドレスの指定がないアクションを作成します。動的なフィルタしきい値の 50 が新しい内部スキャンしきい値となり、それにより異常検出はスキャナのしきい値定義を引き下げます。その結果、異常検出は、新しいスキャンしきい値（50）を超えてスキャンする送信元 IP アドレスごとに追加の動的フィルタを作成します。

KB が学習した内容を異常検出ポリシーまたはゾーンごとにオーバーライドできます。ネットワーク トラフィックの詳細が判明している場合は、偽陽性を制限するためにオーバーライドを使用する必要が生じることもあります。

[Learning Accept Mode] タブのフィールド定義

[Learning Accept Mode] タブには次のフィールドがあります。

- [Automatically accept learning knowledge base] : オンにすると、センサーが自動的に KB をアップデートします。オンにしない場合、異常検出は新しい KB を作成しません。
- [Action] : KB を循環させるか保存するかを指定できます。[Save Only] を選択すると、新しい KB が作成されます。作成された KB を調べ、異常検出にロードするかどうかを決定できます。[Rotate] を選択した場合は、定義したスケジュールに従って新しい KB が作成され、ロードされます。
- [Schedule] : [Calendar Schedule] または [Periodic Schedule] を選択できます。
  - [Periodic Schedule] : 最初の学習スナップショットの日時と、それ以降のスナップショットの間隔を設定できます。デフォルトは、24 時間形式での定期スケジュールです。
  - [Start Time] : 新しい KB を開始する時刻を入力します。有効な形式は hh:mm:ss です。
  - [Learning Interval] : 異常検出が新しい KB を作成する前にネットワークから学習する時間を入力します。
  - [Calendar Schedule] : KB を作成する日時を設定できます。
  - [Times of Day] : [Add] をクリックし、[Add Start Time] ダイアログボックスに日時を入力します。
  - [Days of the Week] : 設定する曜日のチェックボックスをオンにします。

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

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

- [Start Time] : 学習受け入れモードの開始時刻として、時、分、秒を入力します。有効な形式は、24 時間形式の hh:mm:ss です。

学習受け入れモードの設定

異常検出の学習受け入れ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] > [Anomaly Detections] > [ad0] > [Learning Accept Mode] を選択します。

ステップ 3　異常検出が KB を自動的にアップデートするように設定するには、[Automatically accept learning knowledge base] チェックボックスをオンにします。

ステップ 4　[Action] ドロップダウン リストから、次のいずれかのアクション タイプを選択します。

- [Rotate]：新しい KB が作成され、ロードされます。これがデフォルトです。
- [Save Only]：新しい KB が作成されますが、ロードされません。作成された KB を表示し、ロードするかどうかを決定できます。

ステップ 5　[Schedule] ドロップダウン リストから、次のいずれかのスケジュール タイプを選択します。

- [Calendar Schedule]：ステップ 6 に進みます。
- [Periodic Schedule]：ステップ 7 に進みます。

ステップ 6　次の手順でスケジュールを設定します。

a. [Add] をクリックして開始時刻を追加します。

b. 開始時刻の時、分、秒を 24 時間形式で入力します。

ヒント　変更を破棄して [Add Start Time] 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。

d. [Days of the Week] フィールドで、異常検出モジュールによって KB スナップショットをキャプチャする曜日のチェックボックスをオンにします。

ステップ 7　次の手順で定期スケジュール（デフォルト）を設定します。

a. [Start Time] フィールドに、開始時刻の時、分、秒を 24 時間形式で入力します。

b. [Learning Interval] フィールドに、以降の KB スナップショットの間隔を入力します。

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。

内部ゾーンの設定

ここでは、内部ゾーンの設定方法について説明します。内容は次のとおりです。

- 「[Add Protocol Number] および [Edit Protocol Number] ダイアログボックスのフィールド定義」（P.12-18）
- 「内部ゾーンの設定」（P.12-18）

[Internal Zone] タブ

（注）　内部ゾーンを設定するには、管理者またはオペレータであることが必要です。

[Internal Zone] タブには、次の 4 つのタブがあります。

- [General]：内部ゾーンをイネーブルにし、内部ゾーンに含めるサブネットを設定します。
- [TCP Protocol]：TCP プロトコルをイネーブルにし、独自のしきい値とヒストグラムを設定できます。
- [UDP Protocol]：UDP プロトコルをイネーブルにし、独自のしきい値とヒストグラムを設定できます。
- [Other Protocols]：その他のプロトコルをイネーブルにし、独自のしきい値とヒストグラムを設定できます。

内部ゾーンは、内部ネットワークを表している必要があります。また、内部ネットワークの IP アドレス範囲を宛先とするトラフィックをすべて受信する必要があります。

[General] タブ

[General] タブでは、ゾーンをイネーブルにします。ゾーンがディセーブルである場合、そのゾーンを宛先とするパケットは無視されます。ゾーンはデフォルトでイネーブルになります。

次に、このゾーンに属する IP アドレスを追加します。すべてのゾーンに IP アドレスを設定しなければ、すべてのパケットがデフォルト ゾーンである外部ゾーンに送信されます。

フィールド定義

[General] タブには次のフィールドがあります。

- [Enable the Internal Zone]：オンにすると、内部ゾーンがイネーブルになります。
- [Service Subnets]：内部ゾーンに適用するサブネットを入力します。有効な形式は 10.10.5.5,10.10.2.1-10.10.2.30 です。

[TCP Protocol] タブ

[TCP Protocol] タブでは、内部ゾーンの TCP プロトコルをイネーブルまたはディセーブルにします。TCP プロトコルの宛先ポートを設定できます。デフォルトのしきい値を使用することもできれば、スキャナ設定をオーバーライドし、独自のしきい値とヒストグラムを追加することもできます。

フィールド定義

[TCP Protocol] タブには次のフィールドがあります。

- [Enable the TCP Protocol]：オンにすると、TCP プロトコルがイネーブルになります。
- [Destination Port Map] タブ：TCP プロトコルに特定のポートを関連付けることができます。

  - [Port Number]：設定されているポート番号が表示されます。
  - [Service Enabled]：サービスがイネーブルであるかどうか。
  - [Scanner Overridden]：スキャナがオーバーライドされているかどうか。
  - [Overridden Scanner Settings]：設定されているスキャナ設定が表示されます。
  - [Threshold]：しきい値の設定が表示されます。
  - [Histogram]：設定されているヒストグラムが表示されます。
- [Default Thresholds] タブ：デフォルトのしきい値とヒストグラムが表示されます。デフォルトのしきい値は、KB に含まれず設定によってオーバーライドされていないサービスに使用されます。
  - [Scanner Threshold]：スキャナしきい値を変更できます。
  - [Threshold Histogram]：デフォルトのしきい値ヒストグラムが表示されます。
  - [Number of Destination IP Addresses]：低、中、高にグループ化された宛先 IP アドレスの数が表示されます。
  - [Number of Source IP Addresses]：宛先 IP アドレスの各グループに関連付けられた送信元 IP アドレスの数が表示されます。

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

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

- [Destination Port number]：宛先ポート番号を入力します。有効な範囲は 0 ～ 65535 です。
- [Enable the Service]：オンにすると、サービスがイネーブルになります。
- [Override Scanner Settings]：オンにすると、デフォルトのスキャナ設定がオーバーライドされ、すべてのヒストグラムを追加、編集、削除、および選択できます。
- [Scanner Threshold]：スキャナしきい値を設定できます。有効な範囲は 5 ～ 1000 です。デフォルトは 100 です。
- [Threshold Histogram]：追加したヒストグラムが表示されます。
  - [Number of Destination IP Addresses]：追加した宛先 IP アドレスの数が表示されます。
  - [Number of Source IP Addresses]：追加した送信元 IP アドレスの数が表示されます。

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

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

- [Number of Destination IP Addresses]：低、中、高の各グループの宛先 IP アドレス数を追加できます。宛先 IP アドレス数は、低が 5、中が 20、高が 100 です。
- [Number of Source IP Addresses]：送信元 IP アドレスの数を追加できます。有効な範囲は 0 ～ 4096 です。

[UDP Protocol] タブ

[UDP Protocol] タブでは、内部ゾーンの UDP プロトコルをイネーブルまたはディセーブルにします。UDP プロトコルの宛先ポートを設定できます。デフォルトのしきい値を使用することもできれば、スキャナ設定をオーバーライドし、独自のしきい値とヒストグラムを追加することもできます。

フィールド定義

[UDP Protocol] タブには次のフィールドがあります。

- [Enable the UDP Protocol]：オンにすると、UDP プロトコルがイネーブルになります。
- [Destination Port Map] タブ：UDP プロトコルに特定のポートを関連付けることができます。
  - [Port Number]：設定されているポート番号が表示されます。
  - [Service Enabled]：サービスがイネーブルであるかどうか。
  - [Scanner Overridden]：スキャナがオーバーライドされているかどうか。
  - [Overridden Scanner Settings]：設定されているスキャナ設定が表示されます。
  - [Threshold]：しきい値の設定が表示されます。
  - [Histogram]：設定されているヒストグラムが表示されます。
- [Default Thresholds] タブ：デフォルトのしきい値とヒストグラムが表示されます。
  - [Scanner Threshold]：スキャナしきい値を変更できます。
  - [Threshold Histogram]：デフォルトのしきい値ヒストグラムが表示されます。
  - [Number of Destination IP Addresses]：低、中、高にグループ化された宛先 IP アドレスの数が表示されます。
  - [Number of Source IP Addresses]：宛先 IP アドレスの各グループに関連付けられた送信元 IP アドレスの数が表示されます。

[Other Protocols] タブ

[Other Protocols] タブでは、内部ゾーンのその他のプロトコルをイネーブルまたはディセーブルにします。その他のプロトコルのプロトコル番号マップを設定できます。デフォルトのしきい値を使用することもできれば、スキャナ設定をオーバーライドし、独自のしきい値とヒストグラムを追加することもできます。

フィールドの説明

[Other Protocols] タブには次のフィールドがあります。

- [Enable Other Protocols]：オンにすると、その他のプロトコルがイネーブルになります。
- [Protocol Number Map] タブ：その他のプロトコルに特定のプロトコル番号を関連付けることができます。
  - [Protocol Number]：設定されているプロトコル番号が表示されます。
  - [Service Enabled]：サービスがイネーブルであるかどうか。
  - [Scanner Overridden]：スキャナがオーバーライドされているかどうか。
  - [Overridden Scanner Settings]：設定されているスキャナ設定が表示されます。
  - [Threshold]：しきい値の設定が表示されます。
  - [Histogram]：設定されているヒストグラムが表示されます。

- [Default Thresholds] タブ：デフォルトのしきい値とヒストグラムが表示されます。
  - [Scanner Threshold]：スキャナしきい値を変更できます。
  - [Threshold Histogram]：デフォルトのしきい値ヒストグラムが表示されます。
  - [Number of Destination IP Addresses]：低、中、高にグループ化された宛先 IP アドレスの数が表示されます。
  - [Number of Source IP Addresses]：宛先 IP アドレスの各グループに関連付けられた送信元 IP アドレスの数が表示されます。

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

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

- [Protocol number]：プロトコル番号を入力します。
- [Enable the Service]：サービスをイネーブルにできます。
- [Override Scanner Settings]：オンにすると、すべてのヒストグラムを追加、編集、削除、および選択できます。
- [Scanner Threshold]：スキャナしきい値を設定できます。有効な範囲は 5 ～ 1000 です。デフォルトは 100 です。
- [Threshold Histogram]：追加したヒストグラムが表示されます。
  - [Number of Destination IP Addresses]：追加した宛先 IP アドレスの数が表示されます。
  - [Number of Source IP Addresses]：追加した送信元 IP アドレスの数が表示されます。

内部ゾーンの設定

内部ゾーンを異常検出用に設定するには、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] > [Anomaly Detections] > [ad0] > [Internal Zone] を選択し、[General] タブをクリックします。

ステップ 3　内部ゾーンをイネーブルにするには、[Enable the Internal Zone] チェックボックスをオンにします。

（注）　[Enable the Internal Zone] チェックボックスをオンにしなければ、設定したプロトコルは無視されます。

ステップ 4　[Service Subnets] フィールドに、内部ゾーンを適用するサブネットを入力します。有効な形式は 10.10.5.5,10.10.2.1-10.10.2.30 です。

ステップ 5　TCP プロトコルを設定するには、[TCP Protocol] タブをクリックします。

ステップ 6　TCP プロトコルをイネーブルにするには、[Enable the TCP Protocol] チェックボックスをオンにします。

（注） [Enable the TCP Protocol] チェックボックスをオンにしなければ、TCP プロトコルの設定は無視されます。

ステップ 7　[Destination Port Map] タブをクリックし、[Add] をクリックして、宛先ポートを追加します。

ステップ 8　[Destination Port Number] フィールドに宛先ポート番号を入力します。有効な範囲は 0 ～ 65535 です。

ステップ 9　内部ゾーンをイネーブルにするには、[Enable the Service] チェックボックスをオンにします。

ステップ 10　そのポートのスキャナ値をオーバーライドするには、[Override Scanner Settings] チェックボックスをオンにします。デフォルトのスキャナ値を使用することもできれば、デフォルト値をオーバーライドし、独自のスキャナ値を設定することもできます。

ステップ 11　新しいスキャナ設定のヒストグラムを追加するには、[Add] をクリックします。

ステップ 12　[Number of Destination IP Addresses] ドロップダウン リストから値（[High]、[Medium]、または [Low]）を選択します。

ステップ 13　[Number of Source IP Addresses] フィールドに、このヒストグラムに関連付ける送信元 IP アドレスの数を入力します。有効な範囲は 0 ～ 4096 です。

ヒント　変更を破棄して [Add Histogram] 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 14　[OK] をクリックします。[Add Destination Port] ダイアログボックスのリストに新しいスキャナ設定が表示されます。

ヒント　変更を破棄して [Add Destination Port] 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 15　[OK] をクリックします。[Destination Port Map] タブのリストに新しい宛先ポート マップが表示されます。

ステップ 16　宛先ポート マップを編集するには、リストで宛先ポート マップを選択し、[Edit] をクリックします。

ステップ 17　フィールドに変更を加え、[OK] をクリックします。[Destination Port Map] タブのリストに編集済みの宛先ポート マップが表示されます。

ステップ 18　宛先ポート マップを削除するには、その宛先ポート マップを選択し、[Delete] をクリックします。その宛先ポート マップは、[Destination Port Map] タブのリストに表示されなくなります。

ステップ 19　デフォルトのしきい値を編集するには、[Default Thresholds] タブをクリックします。

ステップ 20　編集するしきい値ヒストグラムを選択し、[Edit] をクリックします。

ステップ 21　[Number of Destination IP Addresses] ドロップダウン リストから別の値（[High]、[Medium]、または [Low]）を選択します。

ステップ 22　[Number of Source IP Addresses] フィールドで、このヒストグラムに関連付ける送信元 IP アドレスの数を編集します。有効な範囲は 0 ～ 4096 です。[Default Thresholds] タブのリストに編集済みのしきい値ヒストグラムが表示されます。

ヒント　変更を破棄して [Edit Histogram] 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 23　UDP プロトコルを設定するには、[UDP Protocol] タブをクリックします。

ステップ 24　UDP プロトコルをイネーブルにするには、[Enable the UDP Protocol] チェックボックスをオンにします。

（注）　[Enable the UDP Protocol] チェックボックスをオンにしなければ、UDP プロトコルの設定は無視されます。

ステップ 25　[Destination Port Map] タブをクリックし、[Add] をクリックして、宛先ポートを追加します。

ステップ 26　[Destination Port Number] フィールドに宛先ポート番号を入力します。有効な範囲は 0 ～ 65535 です。

ステップ 27　内部ゾーンをイネーブルにするには、[Enable the Service] チェックボックスをオンにします。

ステップ 28　そのポートのスキャナ値をオーバーライドするには、[Override Scanner Settings] チェックボックスをオンにします。デフォルトのスキャナ値を使用することもできれば、デフォルト値をオーバーライドし、独自のスキャナ値を設定することもできます。

ステップ 29　新しいスキャナ設定のヒストグラムを追加するには、[Add] をクリックします。

ステップ 30　[Number of Destination IP Addresses] ドロップダウン リストから値（[High]、[Medium]、または [Low]）を選択します。

ステップ 31　[Number of Source IP Addresses] フィールドに、このヒストグラムに関連付ける送信元 IP アドレスの数を入力します。有効な範囲は 0 ～ 4096 です。

ヒント　変更を破棄して [Add Histogram] 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 32　[OK] をクリックします。[Add Destination Port] ダイアログボックスのリストに新しいスキャナ設定が表示されます。

ヒント　変更を破棄して [Add Destination Port] 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 33　[OK] をクリックします。[Destination Port Map] タブのリストに新しい宛先ポート マップが表示されます。

ステップ 34　宛先ポート マップを編集するには、リストで宛先ポート マップを選択し、[Edit] をクリックします。

ステップ 35　フィールドに変更を加え、[OK] をクリックします。[Destination Port Map] タブのリストに編集済みの宛先ポート マップが表示されます。

ステップ 36　宛先ポート マップを削除するには、その宛先ポート マップを選択し、[Delete] をクリックします。その宛先ポート マップは、[Destination Port Map] タブのリストに表示されなくなります。

ステップ 37　デフォルトのしきい値を編集するには、[Default Thresholds] タブをクリックし、編集するしきい値ヒストグラムを選択して、[Edit] をクリックします。

ステップ 38　[Number of Destination IP Addresses] ドロップダウン リストから別の値（[High]、[Medium]、または [Low]）を選択します。

ステップ 39　[Number of Source IP Addresses] フィールドで、このヒストグラムに関連付ける送信元 IP アドレスの数を編集します。有効な範囲は 0 ～ 4096 です。[Default Thresholds] タブのリストに編集済みのしきい値ヒストグラムが表示されます。

ヒント 変更を破棄して [Edit Histogram] 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 40 その他のプロトコルを設定するには、[Other Protocols] タブをクリックします。

ステップ 41 その他のプロトコルをイネーブルにするには、[Enable Other Protocols] チェックボックスをオンにします。

（注） [Enable Other Protocols] チェックボックスをオンにしなければ、その他のプロトコルの設定は無視されます。

ステップ 42 [Protocol Number Map] タブをクリックし、[Add] をクリックして、プロトコル番号を追加します。

ステップ 43 [Protocol Number] フィールドにプロトコル番号を入力します。有効な範囲は 0 ～ 255 です。

ステップ 44 そのプロトコルのサービスをイネーブルにするには、[Enable the Service] チェックボックスをオンにします。

ステップ 45 そのプロトコルのスキャナ値をオーバーライドするには、[Override Scanner Settings] チェックボックスをオンにします。デフォルトのスキャナ値を使用することもできれば、デフォルト値をオーバーライドし、独自のスキャナ値を設定することもできます。

ステップ 46 新しいスキャナ設定のヒストグラムを追加するには、[Add] をクリックします。

ステップ 47 [Number of Destination IP Addresses] ドロップダウン リストから値（[High]、[Medium]、または [Low]）を選択します。

ステップ 48 [Number of Source IP Addresses] フィールドに、このヒストグラムに関連付ける送信元 IP アドレスの数を入力します。有効な範囲は 0 ～ 4096 です。

ヒント 変更を破棄して [Add Histogram] 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 49 [OK] をクリックします。[Add Protocol Number] ダイアログボックスのリストに新しいスキャナ設定が表示されます。

ヒント 変更を破棄して [Add Protocol Number] 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 50 [OK] をクリックします。[Protocol Number Map] タブのリストに新しいプロトコル番号が表示されます。

ステップ 51 プロトコル番号マップを編集するには、リストでプロトコル番号マップを選択し、[Edit] をクリックします。

ステップ 52 フィールドに変更を加え、[OK] をクリックします。[Protocol Number Map] タブのリストに編集済みのプロトコル番号マップが表示されます。

ステップ 53 プロトコル番号マップを削除するには、そのプロトコル番号マップを選択し、[Delete] をクリックします。そのプロトコル番号マップは、[Protocol Number Map] タブのリストに表示されなくなります。

ステップ 54 デフォルトのしきい値を編集するには、[Default Thresholds] タブをクリックし、編集するしきい値ヒストグラムを選択して、[Edit] をクリックします。

ステップ 55　[Number of Destination IP Addresses] ドロップダウン リストから別の値（[High]、[Medium]、または [Low]）を選択します。

ステップ 56　[Number of Source IP Addresses] フィールドで、このヒストグラムに関連付ける送信元 IP アドレスの数を編集します。有効な範囲は 0 ～ 4096 です。[Default Thresholds] タブのリストに編集済みのしきい値ヒストグラムが表示されます。

ヒント　変更を破棄して [Edit Histogram] ダイアログボックスを閉じるには、[Cancel] 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 57　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。

不正ゾーンの設定

ここでは、不正ゾーンの設定方法について説明します。内容は次のとおりです。

[Illegal Zone] タブ

（注）　不正ゾーンを設定するには、管理者またはオペレータであることが必要です。

[Illegal Zone] タブには、次の 4 つのタブがあります。

- [General]：不正ゾーンをイネーブルにし、内部ゾーンに含めるサブネットを指定します。
- [TCP Protocol]：TCP プロトコルをイネーブルにし、独自のしきい値とヒストグラムを設定できます。
- [UDP Protocol]：UDP プロトコルをイネーブルにし、独自のしきい値とヒストグラムを設定できます。

- [Other Protocols]：その他のプロトコルをイネーブルにし、独自のしきい値とヒストグラムを設定できます。

不正ゾーンは、正常なトラフィックでは決して見られない IP アドレス範囲を表している必要があります。たとえば、割り当てられていない IP アドレスや、使用されていない内部 IP アドレス範囲に属する IP アドレスなどです。

[General] タブ

[General] タブでは、ゾーンをイネーブルにします。ゾーンがディセーブルである場合、そのゾーンを宛先とするパケットは無視されます。ゾーンはデフォルトでイネーブルになります。

次に、このゾーンに属する IP アドレスを追加します。すべてのゾーンに IP アドレスを設定しなければ、すべてのパケットがデフォルト ゾーンである外部ゾーンに送信されます。

フィールドの説明

[General] タブには次のフィールドがあります。

- [Enable the Internal Zone]：オンにすると、内部ゾーンがイネーブルになります。
- [Service Subnets]：内部ゾーンに適用するサブネットを入力します。有効な形式は 10.10.5.5,10.10.2.1-10.10.2.30 です。

[TCP Protocol] タブ

[TCP Protocol] タブでは、不正ゾーンの TCP プロトコルをイネーブルまたはディセーブルにします。TCP プロトコルの宛先ポートを設定できます。デフォルトのしきい値を使用することもできれば、スキャナ設定をオーバーライドし、独自のしきい値とヒストグラムを追加することもできます。

フィールドの説明

[TCP Protocol] タブには次のフィールドがあります。

- [Enable the TCP Protocol]：オンにすると、TCP プロトコルがイネーブルになります。
- [Destination Port Map] タブ：TCP プロトコルに特定のポートを関連付けることができます。
  - [Port Number]：設定されているポート番号が表示されます。
  - [Service Enabled]：サービスがイネーブルであるかどうか。
  - [Scanner Overridden]：スキャナがオーバーライドされているかどうか。
  - [Overridden Scanner Settings]：設定されているスキャナ設定が表示されます。
  - [Threshold]：しきい値の設定が表示されます。
  - [Histogram]：設定されているヒストグラムが表示されます。
- [Default Thresholds] タブ：デフォルトのしきい値とヒストグラムが表示されます。デフォルトのしきい値は、KB に含まれず設定によってオーバーライドされていないサービスに使用されます。
  - [Scanner Threshold]：スキャナしきい値を変更できます。
  - [Threshold Histogram]：デフォルトのしきい値ヒストグラムが表示されます。
  - [Number of Destination IP Addresses]：低、中、高にグループ化された宛先 IP アドレスの数が表示されます。
  - [Number of Source IP Addresses]：宛先 IP アドレスの各グループに関連付けられた送信元 IP アドレスの数が表示されます。

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

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

- [Destination Port number]：宛先ポート番号を入力します。有効な範囲は 0 ～ 65535 です。
- [Enable the Service]：オンにすると、サービスがイネーブルになります。
- [Override Scanner Settings]：オンにすると、デフォルトのスキャナ設定がオーバーライドされ、すべてのヒストグラムを追加、編集、削除、および選択できます。
- [Scanner Threshold]：スキャナしきい値を設定できます。有効な範囲は 5 ～ 1000 です。デフォルトは 100 です。
- [Threshold Histogram]：追加したヒストグラムが表示されます。
  - [Number of Destination IP Addresses]：追加した宛先 IP アドレスの数が表示されます。
  - [Number of Source IP Addresses]：追加した送信元 IP アドレスの数が表示されます。

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

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

- [Number of Destination IP Addresses]：低、中、高の各グループの宛先 IP アドレス数を追加できます。宛先 IP アドレス数は、低が 5、中が 20、高が 100 です。
- [Number of Source IP Addresses]：送信元 IP アドレスの数を追加できます。有効な範囲は 0 ～ 4096 です。

[UDP Protocol] タブ

[UDP Protocol] タブでは、不正ゾーンの UDP プロトコルをイネーブルまたはディセーブルにします。UDP プロトコルの宛先ポートを設定できます。デフォルトのしきい値を使用することもできれば、スキャナ設定をオーバーライドし、独自のしきい値とヒストグラムを追加することもできます。

フィールドの説明

[UDP Protocol] タブには次のフィールドがあります。

- [Enable the UDP Protocol]：オンにすると、UDP プロトコルがイネーブルになります。
- [Destination Port Map] タブ：UDP プロトコルに特定のポートを関連付けることができます。
  - [Port Number]：設定されているポート番号が表示されます。
  - [Service Enabled]：サービスがイネーブルであるかどうか。
  - [Scanner Overridden]：スキャナがオーバーライドされているかどうか。
  - [Overridden Scanner Settings]：設定されているスキャナ設定が表示されます。
  - [Threshold]：しきい値の設定が表示されます。
  - [Histogram]：設定されているヒストグラムが表示されます。

- [Default Thresholds] タブ：デフォルトのしきい値とヒストグラムが表示されます。
  - [Scanner Threshold]：スキャナしきい値を変更できます。
  - [Threshold Histogram]：デフォルトのしきい値ヒストグラムが表示されます。
  - [Number of Destination IP Addresses]：低、中、高にグループ化された宛先 IP アドレスの数が表示されます。
  - [Number of Source IP Addresses]：宛先 IP アドレスの各グループに関連付けられた送信元 IP アドレスの数が表示されます。

[Other Protocols] タブ

[Other Protocols] タブでは、不正ゾーンのその他のプロトコルをイネーブルまたはディセーブルにします。その他のプロトコルのプロトコル番号マップを設定できます。デフォルトのしきい値を使用することもできれば、スキャナ設定をオーバーライドし、独自のしきい値とヒストグラムを追加することもできます。

フィールドの説明

[Other Protocols] タブには次のフィールドがあります。

- [Enable Other Protocols]：オンにすると、その他のプロトコルがイネーブルになります。
- [Protocol Number Map] タブ：その他のプロトコルに特定のプロトコル番号を関連付けることができます。
  - [Protocol Number]：設定されているプロトコル番号が表示されます。
  - [Service Enabled]：サービスがイネーブルであるかどうか。
  - [Scanner Overridden]：スキャナがオーバーライドされているかどうか。
  - [Overridden Scanner Settings]：設定されているスキャナ設定が表示されます。
  - [Threshold]：しきい値の設定が表示されます。
  - [Histogram]：設定されているヒストグラムが表示されます。
- [Default Thresholds] タブ：デフォルトのしきい値とヒストグラムが表示されます。
  - [Scanner Threshold]：スキャナしきい値を変更できます。
  - [Threshold Histogram]：デフォルトのしきい値ヒストグラムが表示されます。
  - [Number of Destination IP Addresses]：低、中、高にグループ化された宛先 IP アドレスの数が表示されます。
  - [Number of Source IP Addresses]：宛先 IP アドレスの各グループに関連付けられた送信元 IP アドレスの数が表示されます。

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

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

- [Protocol number]：プロトコル番号を入力します。
- [Enable the Service]：サービスをイネーブルにできます。

- [Override Scanner Settings]：オンにすると、すべてのヒストグラムを追加、編集、削除、および選択できます。
- [Scanner Threshold]：スキャナしきい値を設定できます。有効な範囲は 5 ～ 1000 です。デフォルトは 100 です。
- [Threshold Histogram]：追加したヒストグラムが表示されます。
  - [Number of Destination IP Addresses]：追加した宛先 IP アドレスの数が表示されます。
  - [Number of Source IP Addresses]：追加した送信元 IP アドレスの数が表示されます。

不正ゾーンの設定

不正ゾーンを異常検出用に設定するには、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] > [Anomaly Detections] > [ad0] > [Illegal Zone] を選択します。

ステップ 3　[General] タブをクリックします。

ステップ 4　不正ゾーンをイネーブルにするには、[Enable the Illegal Zone] チェックボックスをオンにします。

（注）　[Enable the Illegal Zone] チェックボックスをオンにしなければ、設定したプロトコルは無視されます。

ステップ 5　[Service Subnets] フィールドに、不正ゾーンを適用するサブネットを入力します。有効な形式は 10.10.5.5,10.10.2.1-10.10.2.30 です。

ステップ 6　TCP プロトコルを設定するには、[TCP Protocol] タブをクリックします。

ステップ 7　TCP プロトコルをイネーブルにするには、[Enable the TCP Protocol] チェックボックスをオンにします。

（注）　[Enable the TCP Protocol] チェックボックスをオンにしなければ、TCP プロトコルの設定は無視されます。

ステップ 8　[Destination Port Map] タブをクリックし、[Add] をクリックして、宛先ポートを追加します。

ステップ 9　[Destination Port Number] フィールドに宛先ポート番号を入力します。有効な範囲は 0 ～ 65535 です。

ステップ 10　内部ゾーンをイネーブルにするには、[Enable the Service] チェックボックスをオンにします。

ステップ 11　そのポートのスキャナ値をオーバーライドするには、[Override Scanner Settings] チェックボックスをオンにします。デフォルトのスキャナ値を使用することもできれば、デフォルト値をオーバーライドし、独自のスキャナ値を設定することもできます。

ステップ 12　新しいスキャナ設定のヒストグラムを追加するには、[Add] をクリックします。

ステップ 13　[Number of Destination IP Addresses] ドロップダウン リストから値（[High]、[Medium]、または [Low]）を選択します。

ステップ 14　[Number of Source IP Addresses] フィールドに、このヒストグラムに関連付ける送信元 IP アドレスの数を入力します。有効な範囲は 0 ～ 4096 です。

ヒント 変更を破棄して [Add Histogram] 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 15 [OK] をクリックします。[Add Destination Port] ダイアログボックスのリストに新しいスキャナ設定が表示されます。

ヒント 変更を破棄して [Add Destination Port] 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。[Destination Port Map] タブのリストに新しい宛先ポート マップが表示されます。

ステップ 17 宛先ポート マップを編集するには、リストで宛先ポート マップを選択し、[Edit] をクリックします。

ステップ 18 フィールドに変更を加え、[OK] をクリックします。[Destination Port Map] タブのリストに編集済みの宛先ポート マップが表示されます。

ステップ 19 宛先ポート マップを削除するには、その宛先ポート マップを選択し、[Delete] をクリックします。その宛先ポート マップは、[Destination Port Map] タブのリストに表示されなくなります。

ステップ 20 デフォルトのしきい値を編集するには、[Default Thresholds] タブをクリックし、編集するしきい値ヒストグラムを選択して、[Edit] をクリックします。

ステップ 21 [Number of Destination IP Addresses] ドロップダウン リストから別の値（[High]、[Medium]、または [Low]）を選択します。

ステップ 22 [Number of Source IP Addresses] フィールドで、このヒストグラムに関連付ける送信元 IP アドレスの数を編集します。有効な範囲は 0 ～ 4096 です。[Default Thresholds] タブのリストに編集済みのしきい値ヒストグラムが表示されます。

ヒント 変更を破棄して [Edit Histogram] 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 23 UDP プロトコルを設定するには、[UDP Protocol] タブをクリックします。

ステップ 24 UDP プロトコルをイネーブルにするには、[Enable the UDP Protocol] チェックボックスをオンにします。

（注） [Enable the UDP Protocol] チェックボックスをオンにしなければ、UDP プロトコルの設定は無視されます。

ステップ 25 [Destination Port Map] タブをクリックし、[Add] をクリックして、宛先ポートを追加します。

ステップ 26 [Destination Port Number] フィールドに宛先ポート番号を入力します。有効な範囲は 0 ～ 65535 です。

ステップ 27 内部ゾーンをイネーブルにするには、[Enable the Service] チェックボックスをオンにします。

ステップ 28 そのポートのスキャナ値をオーバーライドするには、[Override Scanner Settings] チェックボックスをオンにします。デフォルトのスキャナ値を使用することもできれば、デフォルト値をオーバーライドし、独自のスキャナ値を設定することもできます。

ステップ 29 新しいスキャナ設定のヒストグラムを追加するには、[Add] をクリックします。

ステップ 30 [Number of Destination IP Addresses] ドロップダウン リストから値（[High]、[Medium]、または [Low]）を選択します。

ステップ 31　[Number of Source IP Addresses] フィールドに、このヒストグラムに関連付ける送信元 IP アドレスの数を入力します。有効な範囲は 0 ～ 4096 です。

ヒント　変更を破棄して [Add Histogram] 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 32　[OK] をクリックします。[Add Destination Port] ダイアログボックスのリストに新しいスキャナ設定が表示されます。

ヒント　変更を破棄して [Add Destination Port] 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 33　[OK] をクリックします。[Destination Port Map] タブのリストに新しい宛先ポート マップが表示されます。

ステップ 34　宛先ポート マップを編集するには、リストで宛先ポート マップを選択し、[Edit] をクリックします。

ステップ 35　フィールドに変更を加え、[OK] をクリックします。[Destination Port Map] タブのリストに編集済みの宛先ポート マップが表示されます。

ステップ 36　宛先ポート マップを削除するには、その宛先ポート マップを選択し、[Delete] をクリックします。その宛先ポート マップは、[Destination Port Map] タブのリストに表示されなくなります。

ステップ 37　デフォルトのしきい値を編集するには、[Default Thresholds] タブをクリックし、編集するしきい値ヒストグラムを選択して、[Edit] をクリックします。

ステップ 38　[Number of Destination IP Addresses] ドロップダウン リストから別の値（[High]、[Medium]、または [Low]）を選択します。

ステップ 39　[Number of Source IP Addresses] フィールドで、このヒストグラムに関連付ける送信元 IP アドレスの数を編集します。有効な範囲は 0 ～ 4096 です。[Default Thresholds] タブのリストに編集済みのしきい値ヒストグラムが表示されます。

ヒント　変更を破棄して [Edit Histogram] 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 40　その他のプロトコルを設定するには、[Other Protocols] タブをクリックします。

ステップ 41　その他のプロトコルをイネーブルにするには、[Enable Other Protocols] チェックボックスをオンにします。

（注）　[Enable Other Protocols] チェックボックスをオンにしなければ、その他のプロトコルの設定は無視されます。

ステップ 42　[Protocol Number Map] タブをクリックし、[Add] をクリックして、プロトコル番号を追加します。

ステップ 43　[Protocol Number] フィールドにプロトコル番号を入力します。有効な範囲は 0 ～ 255 です。

ステップ 44　そのプロトコルのサービスをイネーブルにするには、[Enable the Service] チェックボックスをオンにします。

ステップ 45　そのプロトコルのスキャナ値をオーバーライドするには、[Override Scanner Settings] チェックボックスをオンにします。デフォルトのスキャナ値を使用することもできれば、デフォルト値をオーバーライドし、独自のスキャナ値を設定することもできます。

ステップ 46　新しいスキャナ設定のヒストグラムを追加するには、[Add] をクリックします。

ステップ 47　[Number of Destination IP Addresses] ドロップダウン リストから値（[High]、[Medium]、または [Low]）を選択します。

ステップ 48　[Number of Source IP Addresses] フィールドに、このヒストグラムに関連付ける送信元 IP アドレスの数を入力します。有効な範囲は 0 ～ 4096 です。

ヒント　変更を破棄して [Add Histogram] 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 49　[OK] をクリックします。[Add Protocol Number] ダイアログボックスのリストに新しいスキャナ設定が表示されます。

ヒント　変更を破棄して [Add Protocol Number] 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 50　[OK] をクリックします。[Protocol Number Map] タブのリストに新しいプロトコル番号が表示されます。

ステップ 51　プロトコル番号マップを編集するには、リストでプロトコル番号マップを選択し、[Edit] をクリックします。

ステップ 52　フィールドに変更を加え、[OK] をクリックします。[Protocol Number Map] タブのリストに編集済みのプロトコル番号マップが表示されます。

ステップ 53　プロトコル番号マップを削除するには、そのプロトコル番号マップを選択し、[Delete] をクリックします。そのプロトコル番号マップは、[Protocol Number Map] タブのリストに表示されなくなります。

ステップ 54　デフォルトのしきい値を編集するには、[Default Thresholds] タブをクリックし、編集するしきい値ヒストグラムを選択して、[Edit] をクリックします。

ステップ 55　[Number of Destination IP Addresses] ドロップダウン リストから別の値（[High]、[Medium]、または [Low]）を選択します。

ステップ 56　[Number of Source IP Addresses] フィールドで、このヒストグラムに関連付ける送信元 IP アドレスの数を編集します。有効な範囲は 0 ～ 4096 です。[Default Thresholds] タブのリストに編集済みのしきい値ヒストグラムが表示されます。

ヒント　変更を破棄して [Edit Histogram] ダイアログボックスを閉じるには、[Cancel] 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 57　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。

外部ゾーンの設定

ここでは、外部ゾーンの設定方法について説明します。内容は次のとおりです。

[External Zone] タブ

（注）　外部ゾーンを設定するには、管理者またはオペレータであることが必要です。

[External Zone] タブには、次の 3 つのタブがあります。

- [TCP Protocol]：TCP プロトコルをイネーブルにし、独自のしきい値とヒストグラムを設定できます。
- [UDP Protocol]：UDP プロトコルをイネーブルにし、独自のしきい値とヒストグラムを設定できます。
- [Other Protocols]：その他のプロトコルをイネーブルにし、独自のしきい値とヒストグラムを設定できます。

外部ゾーンは、デフォルトのインターネット範囲（0.0.0.0 ～ 255.255.255.255）を持つデフォルトのゾーンです。デフォルトでは、内部ゾーンと不正ゾーンには IP アドレスは含まれません。内部ゾーンまたは不正ゾーンに含まれる IP アドレスのセットに一致しないパケットは、外部ゾーンで処理されます

[TCP Protocol] タブ

[TCP Protocol] タブでは、外部ゾーンの TCP プロトコルをイネーブルまたはディセーブルにします。TCP プロトコルの宛先ポートを設定できます。デフォルトのしきい値を使用することもできれば、スキャナ設定をオーバーライドし、独自のしきい値とヒストグラムを追加することもできます。

フィールド定義

[TCP Protocol] タブには次のフィールドがあります。

- [Enable the TCP Protocol]：オンにすると、TCP プロトコルがイネーブルになります。
- [Destination Port Map] タブ：TCP プロトコルに特定のポートを関連付けることができます。
  - [Port Number]：設定されているポート番号が表示されます。

  - [Service Enabled]：サービスがイネーブルであるかどうか。
  - [Scanner Overridden]：スキャナがオーバーライドされているかどうか。
  - [Overridden Scanner Settings]：設定されているスキャナ設定が表示されます。
  - [Threshold]：しきい値の設定が表示されます。
  - [Histogram]：設定されているヒストグラムが表示されます。
- [Default Thresholds] タブ：デフォルトのしきい値とヒストグラムが表示されます。デフォルトのしきい値は、KB に含まれず設定によってオーバーライドされていないサービスに使用されます。
  - [Scanner Threshold]：スキャナしきい値を変更できます。
  - [Threshold Histogram]：デフォルトのしきい値ヒストグラムが表示されます。
  - [Number of Destination IP Addresses]：低、中、高にグループ化された宛先 IP アドレスの数が表示されます。
  - [Number of Source IP Addresses]：宛先 IP アドレスの各グループに関連付けられた送信元 IP アドレスの数が表示されます。

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

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

- [Destination Port number]：宛先ポート番号を入力します。有効な範囲は 0 ～ 65535 です。
- [Enable the Service]：オンにすると、サービスがイネーブルになります。
- [Override Scanner Settings]：オンにすると、デフォルトのスキャナ設定がオーバーライドされ、すべてのヒストグラムを追加、編集、削除、および選択できます。
- [Scanner Threshold]：スキャナしきい値を設定できます。有効な範囲は 5 ～ 1000 です。デフォルトは 100 です。
- [Threshold Histogram]：追加したヒストグラムが表示されます。
  - [Number of Destination IP Addresses]：追加した宛先 IP アドレスの数が表示されます。
  - [Number of Source IP Addresses]：追加した送信元 IP アドレスの数が表示されます。

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

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

- [Number of Destination IP Addresses]：低、中、高の各グループの宛先 IP アドレス数を追加できます。宛先 IP アドレス数は、低が 5、中が 20、高が 100 です。
- [Number of Source IP Addresses]：送信元 IP アドレスの数を追加できます。有効な範囲は 0 ～ 4096 です。

[UDP Protocol] タブ

[UDP Protocol] タブでは、外部ゾーンの UDP プロトコルをイネーブルまたはディセーブルにします。UDP プロトコルの宛先ポートを設定できます。デフォルトのしきい値を使用することもできれば、スキャナ設定をオーバーライドし、独自のしきい値とヒストグラムを追加することもできます。

フィールドの説明

[UDP Protocol] タブには次のフィールドがあります。

- [Enable the UDP Protocol]：オンにすると、UDP プロトコルがイネーブルになります。
- [Destination Port Map] タブ：UDP プロトコルに特定のポートを関連付けることができます。
  - [Port Number]：設定されているポート番号が表示されます。
  - [Service Enabled]：サービスがイネーブルであるかどうか。
  - [Scanner Overridden]：スキャナがオーバーライドされているかどうか。
  - [Overridden Scanner Settings]：設定されているスキャナ設定が表示されます。
  - [Threshold]：しきい値の設定が表示されます。
  - [Histogram]：設定されているヒストグラムが表示されます。
- [Default Thresholds] タブ：デフォルトのしきい値とヒストグラムが表示されます。
  - [Scanner Threshold]：スキャナしきい値を変更できます。
  - [Threshold Histogram]：デフォルトのしきい値ヒストグラムが表示されます。
  - [Number of Destination IP Addresses]：低、中、高にグループ化された宛先 IP アドレスの数が表示されます。
  - Number of Source IP Addresses]:宛先 IP アドレスの各グループに関連付けられた送信元 IP アドレスの数が表示されます。

[Other Protocols] タブ

[Other Protocols] タブでは、外部ゾーンのその他のプロトコルをイネーブルまたはディセーブルにします。その他のプロトコルのプロトコル番号マップを設定できます。デフォルトのしきい値を使用することもできれば、スキャナ設定をオーバーライドし、独自のしきい値とヒストグラムを追加することもできます。

フィールドの説明

[Other Protocols] タブには次のフィールドがあります。

- [Enable Other Protocols]：オンにすると、その他のプロトコルがイネーブルになります。
- [Protocol Number Map] タブ：その他のプロトコルに特定のプロトコル番号を関連付けることができます。
  - [Protocol Number]：設定されているプロトコル番号が表示されます。
  - [Service Enabled]：サービスがイネーブルであるかどうか。
  - [Scanner Overridden]：スキャナがオーバーライドされているかどうか。
  - [Overridden Scanner Settings]：設定されているスキャナ設定が表示されます。
  - [Threshold]：しきい値の設定が表示されます。
  - [Histogram]：設定されているヒストグラムが表示されます。

- [Default Thresholds] タブ：デフォルトのしきい値とヒストグラムが表示されます。
  - [Scanner Threshold]：スキャナしきい値を変更できます。
  - [Threshold Histogram]：デフォルトのしきい値ヒストグラムが表示されます。
  - [Number of Destination IP Addresses]：低、中、高にグループ化された宛先 IP アドレスの数が表示されます。
  - [Number of Source IP Addresses]：宛先 IP アドレスの各グループに関連付けられた送信元 IP アドレスの数が表示されます。

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

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

- [Protocol number]：プロトコル番号を入力します。
- [Enable the Service]：サービスをイネーブルにできます。
- [Override Scanner Settings]：オンにすると、すべてのヒストグラムを追加、編集、削除、および選択できます。
- [Scanner Threshold]：スキャナしきい値を設定できます。有効な範囲は 5 ～ 1000 です。デフォルトは 100 です。
- [Threshold Histogram]：追加したヒストグラムが表示されます。
  - [Number of Destination IP Addresses]：追加した宛先 IP アドレスの数が表示されます。
  - [Number of Source IP Addresses]：追加した送信元 IP アドレスの数が表示されます。

外部ゾーンの設定

外部ゾーンを異常検出用に設定するには、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] > [Anomaly Detections] > [ad0] > [External Zone] を選択します。

ステップ 3　外部ゾーンをイネーブルにするには、[Enable the External Zone] チェックボックスをオンにします。

（注）　[Enable the External Zone] チェックボックスをオンにしなければ、設定したプロトコルは無視されます。

ステップ 4　TCP プロトコルを設定するには、[TCP Protocol] タブをクリックします。

ステップ 5　TCP プロトコルをイネーブルにするには、[Enable the TCP Protocol] チェックボックスをオンにします。

（注）　[Enable the TCP Protocol] チェックボックスをオンにしなければ、TCP プロトコルの設定は無視されます。

ステップ 6　[Destination Port Map] タブをクリックし、[Add] をクリックして、宛先ポートを追加します。

ステップ 7　[Destination Port Number] フィールドに宛先ポート番号を入力します。有効な範囲は 0 ～ 65535 です。

ステップ 8　内部ゾーンをイネーブルにするには、[Enable the Service] チェックボックスをオンにします。

ステップ 9　そのポートのスキャナ値をオーバーライドするには、[Override Scanner Settings] チェックボックスをオンにします。デフォルトのスキャナ値を使用することもできれば、デフォルト値をオーバーライドし、独自のスキャナ値を設定することもできます。

ステップ 10　新しいスキャナ設定のヒストグラムを追加するには、[Add] をクリックします。

ステップ 11　[Number of Destination IP Addresses] ドロップダウン リストから値（[High]、[Medium]、または [Low]）を選択します。

ステップ 12　[Number of Source IP Addresses] フィールドに、このヒストグラムに関連付ける送信元 IP アドレスの数を入力します。有効な範囲は 0 ～ 4096 です。

ヒント　変更を破棄して [Add Histogram] 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 13　[OK] をクリックします。[Add Destination Port] ダイアログボックスのリストに新しいスキャナ設定が表示されます。

ヒント　変更を破棄して [Add Destination Port] 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 14　[OK] をクリックします。[Destination Port Map] タブのリストに新しい宛先ポート マップが表示されます。

ステップ 15　宛先ポート マップを編集するには、リストで宛先ポート マップを選択し、[Edit] をクリックします。

ステップ 16　フィールドに変更を加え、[OK] をクリックします。[Destination Port Map] タブのリストに編集済みの宛先ポート マップが表示されます。

ステップ 17　宛先ポート マップを削除するには、その宛先ポート マップを選択し、[Delete] をクリックします。その宛先ポート マップは、[Destination Port Map] タブのリストに表示されなくなります。

ステップ 18　デフォルトのしきい値を編集するには、[Default Thresholds] タブをクリックし、編集するしきい値ヒストグラムを選択して、[Edit] をクリックします。

ステップ 19　[Number of Destination IP Addresses] ドロップダウン リストから別の値（[High]、[Medium]、または [Low]）を選択します。

ステップ 20　[Number of Source IP Addresses] フィールドで、このヒストグラムに関連付ける送信元 IP アドレスの数を編集します。有効な範囲は 0 ～ 4096 です。[Default Thresholds] タブのリストに編集済みのしきい値ヒストグラムが表示されます。

ヒント　変更を破棄して [Edit Histogram] 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 21　UDP プロトコルを設定するには、[UDP Protocol] タブをクリックします。

ステップ 22　UDP プロトコルをイネーブルにするには、[Enable the UDP Protocol] チェックボックスをオンにします。

（注）　[Enable the UDP Protocol] チェックボックスをオンにしなければ、UDP プロトコルの設定は無視されます。

ステップ 23　[Destination Port Map] タブをクリックし、[Add] をクリックして、宛先ポートを追加します。

ステップ 24　[Destination Port Number] フィールドに宛先ポート番号を入力します。有効な範囲は 0 ～ 65535 です。

ステップ 25　内部ゾーンをイネーブルにするには、[Enable the Service] チェックボックスをオンにします。

ステップ 26　そのポートのスキャナ値をオーバーライドするには、[Override Scanner Settings] チェックボックスをオンにします。デフォルトのスキャナ値を使用することもできれば、デフォルト値をオーバーライドし、独自のスキャナ値を設定することもできます。

ステップ 27　新しいスキャナ設定のヒストグラムを追加するには、[Add] をクリックします。

ステップ 28　[Number of Destination IP Addresses] ドロップダウン リストから値（[High]、[Medium]、または [Low]）を選択します。

ステップ 29　[Number of Source IP Addresses] フィールドに、このヒストグラムに関連付ける送信元 IP アドレスの数を入力します。有効な範囲は 0 ～ 4096 です。

ヒント　変更を破棄して [Add Histogram] 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 30　[OK] をクリックします。[Add Destination Port] ダイアログボックスのリストに新しいスキャナ設定が表示されます。

ヒント　変更を破棄して [Add Destination Port] 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 31　[OK] をクリックします。[Destination Port Map] タブのリストに新しい宛先ポート マップが表示されます。

ステップ 32　宛先ポート マップを編集するには、リストで宛先ポート マップを選択し、[Edit] をクリックします。

ステップ 33　フィールドに変更を加え、[OK] をクリックします。[Destination Port Map] タブのリストに編集済みの宛先ポート マップが表示されます。

ステップ 34　宛先ポート マップを削除するには、その宛先ポート マップを選択し、[Delete] をクリックします。その宛先ポート マップは、[Destination Port Map] タブのリストに表示されなくなります。

ステップ 35　デフォルトのしきい値を編集するには、[Default Thresholds] タブをクリックし、編集するしきい値ヒストグラムを選択して、[Edit] をクリックします。

ステップ 36　[Number of Destination IP Addresses] ドロップダウン リストから別の値（[High]、[Medium]、または [Low]）を選択します。

ステップ 37　[Number of Source IP Addresses] フィールドで、このヒストグラムに関連付ける送信元 IP アドレスの数を編集します。有効な範囲は 0 ～ 4096 です。[Default Thresholds] タブのリストに編集済みのしきい値ヒストグラムが表示されます。

ヒント　変更を破棄して [Edit Histogram] 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 38　その他のプロトコルを設定するには、[Other Protocols] タブをクリックします。

ステップ 39　その他のプロトコルをイネーブルにするには、[Enable Other Protocols] チェックボックスをオンにします。

（注）　[Enable Other Protocols] チェックボックスをオンにしなければ、その他のプロトコルの設定は無視されます。

ステップ 40　[Protocol Number Map] タブをクリックし、[Add] をクリックして、プロトコル番号を追加します。

ステップ 41　[Protocol Number] フィールドにプロトコル番号を入力します。有効な範囲は 0 ～ 255 です。

ステップ 42　そのプロトコルのサービスをイネーブルにするには、[Enable the Service] チェックボックスをオンにします。

ステップ 43　そのプロトコルのスキャナ値をオーバーライドするには、[Override Scanner Settings] チェックボックスをオンにします。デフォルトのスキャナ値を使用することもできれば、デフォルト値をオーバーライドし、独自のスキャナ値を設定することもできます。

ステップ 44　新しいスキャナ設定のヒストグラムを追加するには、[Add] をクリックします。

ステップ 45　[Number of Destination IP Addresses] ドロップダウン リストから値（[High]、[Medium]、または [Low]）を選択します。

ステップ 46　[Number of Source IP Addresses] フィールドに、このヒストグラムに関連付ける送信元 IP アドレスの数を入力します。有効な範囲は 0 ～ 4096 です。

ヒント　変更を破棄して [Add Histogram] 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 47　[OK] をクリックします。[Add Protocol Number] ダイアログボックスのリストに新しいスキャナ設定が表示されます。

ヒント　変更を破棄して [Add Protocol Number] 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 48　[OK] をクリックします。[Protocol Number Map] タブのリストに新しいプロトコル番号が表示されます。

ステップ 49　プロトコル番号マップを編集するには、リストでプロトコル番号マップを選択し、[Edit] をクリックします。

ステップ 50　フィールドに変更を加え、[OK] をクリックします。[Protocol Number Map] タブのリストに編集済みのプロトコル番号マップが表示されます。

ステップ 51　プロトコル番号マップを削除するには、そのプロトコル番号マップを選択し、[Delete] をクリックします。そのプロトコル番号マップは、[Protocol Number Map] タブのリストに表示されなくなります。

ステップ 52　デフォルトのしきい値を編集するには、[Default Thresholds] タブをクリックします。

ステップ 53　編集するしきい値ヒストグラムを選択し、[Edit] をクリックします。

ステップ 54　[Number of Destination IP Addresses] ドロップダウン リストから別の値（[High]、[Medium]、または [Low]）を選択します。

ステップ 55　[Number of Source IP Addresses] フィールドで、このヒストグラムに関連付ける送信元 IP アドレスの数を編集します。有効な範囲は 0 ～ 4096 です。[Default Thresholds] タブのリストに編集済みのしきい値ヒストグラムが表示されます。

ヒント 変更を破棄して [Edit Histogram] ダイアログボックスを閉じるには、[Cancel] 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 56 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。

異常検出のディセーブル化

センサーをトラフィックの一方向だけを参照するように設定している場合は、異常検出をディセーブルにする必要があります。そうしなければ、異常検出が非対称トラフィックをワーム スキャナと同じような不完全な接続と認識し、アラートを起動するため、大量のアラートが生成されます。

異常検出をディセーブルにするには、次の手順を実行します。

ステップ 1 管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2 分析エンジン サブモードを開始します。

```
sensor# configure terminal
sensor(config)# service analysis-engine
sensor(config-ana)#
```

ステップ 3 ディセーブルにする異常検出ポリシーが含まれる仮想センサー名を入力します。

```
sensor(config-ana)# virtual-sensor vs0
sensor(config-ana-vir)#
```

ステップ 4 異常検出動作モードをディセーブルにします。

```
sensor(config-ana-vir)# anomaly-detection
sensor(config-ana-vir-ano)# operational-mode inactive
sensor(config-ana-vir-ano)#
```

ステップ 5 分析エンジン サブモードを終了します。

```
sensor(config-ana-vir-ano)# exit
sensor(config-ana-vir)# exit
sensor(config-ana-)# exit
Apply Changes:?[yes]:
```

ステップ 6 変更を適用する場合は Enter を押します。変更を破棄する場合は「no」と入力します。

CHAPTER 13

グローバル相関の設定

（注） IPS 6.1 および 6.2 は、グローバル相関機能をサポートしていません。

（注） AIP SSC-5 は、グローバル相関機能をサポートしていません。

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

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

この章では、グローバル相関の設定について説明します。内容は次のとおりです。

グローバル相関について

センサーが悪意のあるアクティビティのレピュテーションを持つネットワーク デバイスを認識し、それらのアクティビティに対処できるようにグローバル相関を設定できます。シスコの中央脅威データベースである SensorBase ネットワーク に IPS デバイスを加えることにより、グローバル相関更新を受信して取り込むことができます。グローバル相関更新に含まれているレピュテーション データは、ネットワーク トラフィックの分析に組み込まれます。これにより、トラフィックが送信元 IP アドレスのレピュテーションに基づいて拒否または許可されるため、IPS の有効性が高まります。参加している IPS デバイスは、Cisco SensorBase ネットワークにデータを送信して戻します。これにより、最新かつグローバルな更新を維持するフィードバック ループがもたらされます。

センサーを、グローバル相関更新やテレメトリ データの送信に参加するように設定することもできますし、これらのサービスをオフにすることもできます。完全な参加を選択した場合、IBNP がリストを共有しておらず、SensorBase ネットワークへのデータ提供を継続しながらネットワークに関する機密情報を保護できるときには、特定の IP アドレスを除外できます。イベントのレピュテーション スコアを表示したり、攻撃者のレピュテーション スコアを参照したりできます。レピュテーション スコアに基づいてイベントをフィルタし、その結果を基にしてレポートを生成できます。

SensorBase ネットワークへの参加

Cisco IPS には、新しいセキュリティ機能である Cisco グローバル相関が実装されました。この機能では、シスコが長年にわたって蓄積してきた優れたセキュリティ インテリジェンスを駆使しています。Cisco IPS は定期的な間隔で Cisco SensorBase ネットワークから脅威の更新を受信します。これには、インターネット上の既知の脅威（常習的な攻撃者、Botnet ハーベスタ、悪意のあるソフトウェアの大発生、ダーク ネットなど）に関する詳細な情報が含まれています。重要な資産への攻撃の機会をつかまれる前に、IPS はこの情報を使用してフィルタリングによって悪質な攻撃者を除外します。そして、グローバルな脅威データをシステムに組み込み、早期に悪意のあるアクティビティを防止します。

SensorBase ネットワークへの参加に同意した場合は、IPS 宛てに送信されたトラフィックに関する集約された統計情報がシスコによって収集されます。この情報には、Cisco IPS ネットワーク トラフィック プロパティに関する要約データと、このトラフィックがシスコのアプライアンスでどのように処理されたかに関する情報が含まれます。トラフィックのデータ コンテンツおよびその他の企業秘密情報および個人情報の収集は行いません。すべてのデータは集約され、定期的な間隔でセキュリティ保護された HTTP によって Cisco SensorBase ネットワーク サーバに送信されます。シスコで共有されるすべてのデータは匿名とされ、機密情報として扱われます。

表 13-1 に、シスコでのデータの使用法を示します。

表 13-1　シスコによるネットワーク参加データの使用

参加レベル	データのタイプ	目的
Partial	プロトコル属性 （TCP 最大セグメント サイズおよびオプション ストリングなど）	潜在的脅威を追跡し、脅威による影響をシスコが理解するのに役立ちます
	攻撃タイプ （開始されたシグニチャおよびリスク レーティングなど）	現在の攻撃および攻撃の重大度を理解するために使用されます
	接続している IP アドレスおよびポート	攻撃元を特定します
	IPS パフォーマンスの概要 （CPU 使用率、メモリの使用状況、インライン モードと無差別モードなど）	製品の有効性を追跡します
Full	攻撃対象の IP アドレスおよびポート	脅威の動作パターンを検出します

部分的（[Partial]）または完全（[Full]）なネットワーク参加をイネーブルにすると、[Network Participation Disclaimer] が表示されます。参加するには、[Agree] をクリックします。ライセンスをインストールしていない場合は、センサーのライセンスが供与されるまでグローバル相関インスペクションとレピュテーション フィルタリングがディセーブルになることを知らせる警告が表示されます。ライセンスは http://www.cisco.com/go/license で取得できます。

詳細情報

センサー ライセンスを取得してインストールする方法については、「ライセンスの設定」（P.18-10）を参照してください。

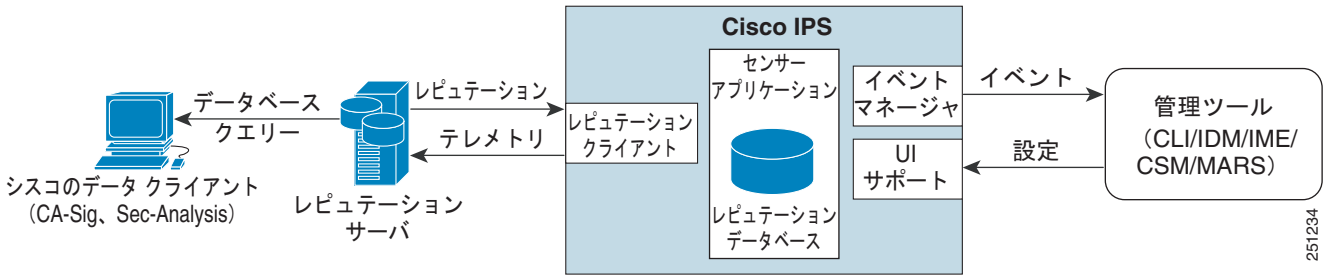
レピュテーションについて

レピュテーションとは、人間社会の場合と同様、インターネット上でのデバイスに関する評価のことです。レピュテーションを使用すると、インストール ベースの IPS センサーは、既存のネットワーク インフラストラクチャと協力してコラボレーションを行うことができるようになります。レピュテーションのあるネットワーク デバイスは、ほとんどが悪意のあるネットワーク デバイスまたは感染した可能性があるネットワーク デバイスです。レピュテーション情報と統計情報は IME で表示できます。

IPS センサーはグローバル相関サーバ（別名 レピュテーション サーバ）とのコラボレーションを行い、センサーの有効性を高めます。

図 13-1 に、センサーのロールとグローバル相関サーバを示します。

図 13-1　IPS 管理およびグローバル相関サーバとのやり取り



グローバル相関サーバは悪意のあるホストまたは感染したホストを特定できる可能性のある IP アドレスについて、センサーに情報を提供します。センサーはこの情報を使用して、実行するアクションを決定し（該当する場合）、既知のレピュテーションのあるホストから潜在的に有害なトラフィックを受け取るとそれを実行します。グローバル相関データベースは急速に変化するため、センサーはグローバル相関サーバから定期的にグローバル相関更新をダウンロードする必要があります。

注意　センサーが、シグニチャまたはグローバル相関の更新を適用すると、バイパスがトリガーされる場合があります。バイパスがトリガーされるかどうかは、センサーのトラフィック負荷とシグニチャまたはグローバル相関の更新のサイズによって決まります。バイパス モードをオフにすると、インライン センサーは更新の適用中にトラフィックの送信を停止します。

（注）　IPS SSP は、バイパス モードをサポートしていません。適応型セキュリティ アプライアンスは、適応型セキュリティ アプライアンスの設定と IPS SSP 上で行われているアクティビティのタイプによって、フェールオープン、フェールクローズ、またはフェールオーバーします。

詳細情報

- グローバル相関の統計情報表示の詳細については、「統計情報の表示」（P.19-31）を参照してください。
- センサーおよびバイパス モードの詳細については、「バイパス モードの設定」（P.7-29）を参照してください。

ネットワーク参加について

ネットワーク参加によって、ほぼリアルタイムのデータを世界中のセンターから収集できます。カスタマー サイトにインストールされているセンサーは、SensorBase ネットワークにデータを送信できます。これらのデータは、グローバル相関データベースに提供されるため、レピュテーションの忠実度が高まります。センサーと SensorBase ネットワーク間の通信には、TCP/IP を介した HTTPS 要求および応答が含まれます。

ネットワーク参加により、次のデータが収集されます。

- シグニチャ ID
- 攻撃者の IP アドレス
- 攻撃者のポート
- 最大セグメント サイズ

- 攻撃対象者の IP アドレス
- 攻撃対象者のポート
- シグニチャのバージョン
- TCP オプション ストリング
- レピュテーション スコア
- リスク レーティング

ネットワーク参加の統計情報には、警告のヒットとミス、レピュテーション アクション、拒否されたパケットのカウンタが示されます。

ネットワーク参加には、3 つのモードがあります。

- オフ：ネットワーク参加サーバは、データの収集、統計情報の追跡、または Cisco SensorBase ネットワークへの接続試行は行いません。
- 部分的な参加：ネットワーク参加サーバは、データを収集し、統計情報を追跡して、SensorBase ネットワークと通信します。潜在的に機密性が高いと見なされるデータは、フィルタリングによって除外され、送信されません。
- 完全参加：ネットワーク参加サーバは、データを収集し、統計情報を追跡して、SensorBase ネットワークと通信します。ネットワーク参加データから除外した IP アドレスを除き、収集されたすべてのデータが送信されます。

ネットワーク参加を行うには、インターネットへのネットワーク接続が必要です。

注意　センサーが、シグニチャまたはグローバル相関の更新を適用すると、バイパスがトリガーされる場合があります。バイパスがトリガーされるかどうかは、センサーのトラフィック負荷とシグニチャまたはグローバル相関の更新のサイズによって決まります。バイパス モードをオフにすると、インライン センサーは更新の適用中にトラフィックの送信を停止します。

（注）　IPS SSP は、バイパス モードをサポートしていません。適応型セキュリティ アプライアンスは、適応型セキュリティ アプライアンスの設定と IPS SSP 上で行われているアクティビティのタイプによって、フェールオープン、フェールクローズ、またはフェールオーバーします。

詳細情報

- グローバル相関の詳細については、「ネットワーク参加の設定」（P.13-11）を参照してください。
- センサーおよびバイパス モードの詳細については、「バイパス モードの設定」（P.7-29）を参照してください。

有効性について

IPS クライアントの参加により取得したデータと脅威に関する既知の資料を併用することで、IPS の有効性が高まります。シスコでは、次の使用に基づいて有効性を評価します。

- 実行可能なイベントの偽陽性（パーセンテージ）
- 実行可能なイベントにはならない脅威の偽陰性（パーセンテージ）
- すべてのイベントの実行可能なイベント（パーセンテージ）

IPS シグニチャ チームは、このデータを使用してシグニチャの忠実度を改善します。IPS エンジニアリング チームは、このデータを使用してさまざまなタイプのセンサーの配置について理解を深めます。

詳細情報

レピュテーションとリスク レーティングの詳細については、「レピュテーションとリスク レーティング」（P.13-6）を参照してください。

レピュテーションとリスク レーティング

リスク レーティングは、ネットワーク イベントに悪意があるかどうかの蓋然性の概念を示します。ネットワーク上で特定のイベントに関連するリスクの数値定量化を割り当てます。デフォルトでは、リスク レーティングが極端に高い警告が表示されると、トラフィックはシャットダウンされます。レピュテーションは、既知のアクティビティに基づいて、特定の攻撃者の IP アドレスから悪意のある動作が開始される可能性を示します。このレピュテーションについてのスコアがアラーム チャネルによって算出され、リスク レーティングに加算されます。このようにして、IPS の有効性が改善されていきます。悪いレピュテーション スコアを持つ攻撃者が認識されると、リスクがリスク レーティングに増分的に加算され、アグレッシブにされます。

アラーム チャネルは、データ パスからのシグニチャ イベントを処理します。このアラート処理装置は、各種集約技術、アクション オーバーライド、アクション フィルタ、攻撃者のレピュテーション、アクションごとのカスタム処理方法を備えています。ピュテーション参加クライアントから得た大量のレピュテーション データを使用して、アラーム チャネルで攻撃者のスコアを設定し、このスコアを使用してリスク レーティングとアラートのアクションを決定します。

詳細情報

- リスク レーティングの詳細については、「リスク レーティングの計算」（P.11-3）を参照してください。
- 脅威レーティングの詳細については、「脅威レーティングの概要」（P.11-4）を参照してください。
- イベント アクション フィルタの詳細については、「イベント アクション フィルタの概要」（P.11-5）を参照してください。
- アラーム チャネルの詳細については、「SensorApp について」（P.A-22）を参照してください。
- イベント アクション集約の詳細については、「イベント アクションの集約」（P.11-6）を参照してください。

グローバル相関機能と目的

グローバル相関には、次の 3 つの主要機能があります。

- グローバル相関インスペクション：攻撃者に関するグローバル相関レピュテーション ナレッジに基づいてアラート処理を変更します。また、センサー上で悪いスコアを持つ攻撃者が認識されると、その攻撃者によるアクションを拒否します。
- レピュテーション フィルタリング：悪意のある既知のサイトからのパケットに対して自動拒否アクションを適用します。
- ネットワーク レピュテーション：センサーはアラートおよび TCP フィンガープリント データを SensorBase ネットワークに送信します。

グローバル相関には、次の目的があります。

- アラートをインテリジェントに処理することにより、有効性を高める。

- 悪意のある既知のサイトに対する保護を強化する。
- テレメトリ データを SensorBase ネットワークと共有して、アラートおよびセンサー アクションの可視性をグローバル規模で向上する。
- 設定を簡素化する。
- 情報のアップロードおよびダウンロードを自動的に処理する。

グローバル相関の要件

グローバル相関には、次の要件があります。

- 有効なライセンス

  グローバル相関機能が動作するには、有効なセンサーのライセンスが必要です。グローバル相関機能の統計情報については引き続き設定および表示できますが、グローバル相関データベースはクリアされ、更新は試行されなくなります。有効なライセンスをインストールすると、グローバル相関機能が再アクティブ化されます。

- ネットワーク参加の免責事項への同意
- センサーおよび DNS サーバの外部接続

  Cisco IPS のグローバル相関機能では、センサーが Cisco SensorBase ネットワークに接続する必要があります。これらの機能が動作するには、ドメイン名解決も必要となります。DNS クライアントが稼動している HTTP プロキシ サーバを介して接続するようにセンサーを設定するか、またはセンサーの管理インターフェイスにルーティング可能なインターネット アドレスを割り当て、DNS サーバを使用するようにセンサーを設定できます。Cisco IPS では、HTTP プロキシと DNS サーバはグローバル相関機能でのみ使用されます。

  （注） slow コマンドと制御接続を使用して環境に配置されたセンサーは、グローバル相関更新のダウンロードが遅くなります。

- IPv6 アドレスはサポートされない

  グローバル相関インスペクションおよびレピュテーション フィルタリング拒否機能では、IPv6 アドレスがサポートされていません。グローバル相関インスペクションでは、センサーは IPv6 アドレスのレピュテーション データを受信または処理しません。IPv6 アドレスのリスク レーティングは、グローバル相関インスペクション用に変更されません。同様に、ネットワーク参加には、IPv6 アドレスからの攻撃に関するイベント データは含まれていません。また、IPv6 アドレスは拒否リストに表示されません。

- インライン モードのセンサー

  センサーは、インライン モードで動作する必要があります。これにより、グローバル相関機能でインライン拒否アクションを使用できるようになり、その有効性が高まります。

- グローバル相関機能をサポートするセンサー

  （注） AIP SSC-5 は、グローバル相関機能をサポートしていません。

- グローバル相関機能をサポートする IPS バージョン

  （注） IPS 6.1 および 6.2 は、グローバル相関機能をサポートしていません。

詳細情報

- センサー ライセンスを取得してインストールする方法については、「ライセンスの設定」（P.18-10）を参照してください。
- ネットワーク参加の免責事項の詳細については、「SensorBase ネットワークへの参加」（P.13-2）を参照してください。
- グローバル相関をサポートする DNS または HTTP プロキシ サーバ設定の詳細については、「ネットワークの設定」（P.6-2）を参照してください。
- グローバル相関のトラブルシューティングの詳細については、「グローバル相関のトラブルシューティング」（P.13-13）を参照してください。

グローバル相関のセンサー ヘルス状態メトリックについて

グローバル相関では、センサー ヘルス モニタに次のメトリックが追加されました。

- 緑色は、最後の更新が成功したことを示します。
- 黄色は、過去 86,400 秒以内に成功した更新はないことを示します。
- 赤色は、過去 3 日（259,200 秒）以内に成功した更新はないことを示します。

ネットワーク参加では、センサー ヘルス モニタに次のメトリックが追加されました。

- 緑色は、最後の接続が成功したことを示します。
- 黄色は、連続して失敗した接続（6 回未満）があることを示します。
- 赤色は、連続して失敗した接続（6 回超）があることを示します。

メトリックは、[Sensor Health] ガジェットと [Global Correlation Health] ガジェットで表示できます。

（注）　グローバル相関のヘルス状態ステータスはデフォルトで赤色に設定され、グローバル相関更新が成功すると緑色に変更されます。グローバル相関更新を成功させるには、DNS サーバまたは HTTP プロキシ サーバが必要です。DNS と HTTP プロキシ サーバの設定機能は IPS 7.0(1)E3 から実装されたため、7.0(1)E3 以降にアップグレードした場合は未設定の状態になっています。このため、グローバル相関ヘルス状態および全般的なセンサー ヘルス状態ステータスは、センサーで DNS または HTTP プロキシ サーバを設定するまで、赤色になります。DNS または HTTP プロキシ サーバを使用できない環境にセンサーが配置されている場合は、グローバル相関をディセーブルにし、グローバル相関ヘルス状態ステータスを含まないようにセンサー ヘルス状態ステータスを設定することで、赤色のグローバル相関ヘルス状態と全般的なセンサー ヘルス状態ステータスに対処できます。

詳細情報

- センサー ヘルス状態メトリックの詳細については、「センサーのヘルスの設定」（P.18-14）を参照してください。
- グローバル相関をディセーブルにする手順については、「グローバル相関のディセーブル化」（P.13-13）を参照してください。
- [Sensor Health] ガジェットおよび [Global Correlation Health] ガジェットの詳細については、「IME ガジェット」（P.3-2）を参照してください。

グローバル相関インスペクションおよびレピュテーションの設定

ここでは、グローバル相関インスペクションおよびレピュテーション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。

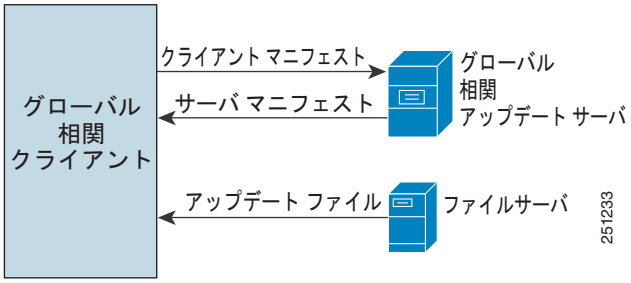
[Inspection/Reputation] ペイン

（注）　インスペクション / レピュテーションを設定するには、管理者権限またはオペレータ権限が必要です。

[Inspection/Reputation] ペインで、SensorBase ネットワークからの更新を使用してセンサーを設定し、リスク レーティングを調整できます。クライアントは、グローバル相関アップデート サーバおよびファイル サーバと通信することで、センサーに適用可能な利用できる更新を判断します。グローバル相関アップデート サーバは、センサーにサーバ マニフェスト ドキュメントを提供します。このドキュメントによって、使用可能な更新、およびファイル サーバからそれらを取得する方法が特定されます。センサーは、サーバ マニフェストの情報を使用して、ファイル サーバから更新ファイルをダウンロードします。

図 13-2 に、グローバル相関アップデート クライアントがファイルを取得する方法を示します。

図 13-2　　グローバル相関アップデート クライアント



注意　グローバル相関機能が動作するには、有効なセンサーのライセンスが必要です。グローバル相関機能の統計情報については引き続き設定および表示できますが、グローバル相関データベースはクリアされ、更新は試行されなくなります。有効なライセンスをインストールすると、グローバル相関機能が再アクティブ化されます。

グローバル相関を設定すると、更新は自動的に定期的な間隔で行われます。デフォルトの間隔は約 5 分ですが、この間隔はグローバル相関サーバで変更できます。センサーは、完全な更新を取得し、その後は定期的に差分更新を適用します。

HTTP プロキシまたは DNS サーバの設定は、[Network] ペインで行います。グローバル相関をオンにしている場合は、悪意のあるホストに対してどれだけ積極的に拒否アクションを実施するかを選択できます。次に、悪意のある既知のホストへのアクセスを拒否するために、レピュテーション フィルタリ

ングをイネーブルにします。発生する可能性があった内容に関するレポートだけが必要な場合は、[Test Global Correlation] をイネーブルにします。これにより、センサーは監査モードに設定され、センサーが実行したと想定されるアクションがイベント内に生成されます。

[Sensor Health] ガジェットでグローバル相関のステータスを表示するには、[Details] をクリックします。グローバル相関のステータスには、[Normal]、[Needs Attention]、または [Critical] が表示されます。

注意　センサーが、シグニチャまたはグローバル相関の更新を適用すると、バイパスがトリガーされる場合があります。バイパスがトリガーされるかどうかは、センサーのトラフィック負荷とシグニチャまたはグローバル相関の更新のサイズによって決まります。バイパス モードをオフにすると、インライン センサーは更新の適用中にトラフィックの送信を停止します。

（注）　IPS SSP は、バイパス モードをサポートしていません。適応型セキュリティ アプライアンスは、適応型セキュリティ アプライアンスの設定と IPS SSP 上で行われているアクティビティのタイプによって、フェールオープン、フェールクローズ、またはフェールオーバーします。

[Inspection/Reputation] ペインのフィールド定義

[Inspection/Reputation] ペインには次のフィールドがあります。

- [Global Correlation Inspection]：グローバル相関をオフまたはオンにします。オンの場合、センサーは、SensorBase ネットワークからの更新を使用して、リスク レーティングを調整します。デフォルトはオフです。センサーが拒否アクションを開始する場合にどれだけ積極的にグローバル相関情報を使用するかを指定する 3 つのモードがあります。
  - [Permissive]：拒否アクションに対する影響は最も少なくなります。
  - [Standard]：拒否アクションに対する影響は中程度です。
  - [Aggressive]：拒否アクションに対する影響は非常に大きくなります。
- [Reputation Filtering]：レピュテーション フィルタリングをオンまたはオフにできます。オンの場合、センサーは、グローバル相関データベースにリストされている悪意のあるホストへのアクセスを拒否します。デフォルトはオフです。
- [Test Global Correlation]：グローバル相関の影響を受ける拒否アクションのレポートをイネーブルにします。実際にホストを拒否することなく、グローバル相関機能をテストできます。

詳細情報

- センサー ライセンスを取得してインストールする方法については、「ライセンスの設定」（P.18-10）を参照してください。
- センサー ヘルス状態メトリックの詳細については、「センサーのヘルスの設定」（P.18-14）を参照してください。

グローバル相関インスペクションおよびレピュテーション フィルタリングの設定

グローバル相関インスペクションおよびレピュテーション フィルタリングを設定するには、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] > [Global Correlation] > [Inspection/Reputation] を選択します。

ステップ 3　グローバル相関インスペクションおよびレピュテーション フィルタリングをオンにするには、[On] オプション ボタンをクリックします。グローバル相関インスペクションおよびレピュテーション フィルタリングはデフォルトでオフになっています。

ステップ 4　ドロップダウン リストから、センサーが拒否アクションを開始する場合にグローバル相関情報を使用する程度を選択します。

- [Permissive]：拒否アクションに対する影響は最も少なくなります。
- [Standard]：拒否アクションに対する影響は中程度です。
- [Aggressive]：拒否アクションに対する影響は非常に大きくなります。

ステップ 5　レピュテーション フィルタリングをオンにするには、[On] オプション ボタンをクリックします。レピュテーション フィルタリングはデフォルトでオフになっています。

ステップ 6　トラフィックを拒否するかどうかについてグローバル相関に影響せずにグローバル相関のテストを実行するには、[Test Global Correlation] チェックボックスをオンにします。このように設定すると、グローバル相関インスペクションおよびレピュテーション フィルタリングがオンであるようにレポートが作成されます。

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。

ネットワーク参加の設定

ここでは、ネットワーク参加の設定方法について説明します。内容は次のとおりです。

[Network Participation] ペイン

（注）　ネットワーク参加を設定するには、管理者権限またはオペレータ権限が必要です。

[Network Participation] ペインでは、SensorBase ネットワークにデータを送信するようにセンサーを設定できます。完全な参加を行うようにセンサーを設定し、すべてのデータを SensorBase ネットワークに送信することができます。または、潜在的に機密性が高いと見なされるデータ（トリガー パケットの宛先 IP アドレスなど）は除いてデータを収集するようにセンサーを設定できます。

（注） センサーを部分的ネットワーク参加用に設定すると、第三者が、内部ネットワークに関する調査情報をグローバル相関データベースから抽出するときに制限が課されます。

完全な参加を選択すると、ネットワーク参加データから除外する IP アドレスを指定できます。除外された攻撃者 / 攻撃対象者の IP アドレスは、シスコには送信されません。

[Network Participation] ペインのフィールド定義

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

- [Off]：どのデータも SensorBase ネットワークに提供されません。
- [Partial]：データは SensorBase ネットワークに提供されますが、潜在的に機密性が高いと見なされるデータはフィルタリングによって除外され、送信されません。
- [Full]：除外された攻撃者 / 攻撃対象者の IP アドレスを除き、すべてのデータが SensorBase ネットワークに提供されます。

ネットワーク参加の設定

ネットワーク参加を設定するには、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] > [Global Correlation] > [Network Participation] を選択します。

ステップ 3　ネットワーク参加をオンにするには、[Partial] または [Full] オプション ボタンをクリックします。

- [Partial]：データは SensorBase ネットワークに提供されますが、潜在的に機密性が高いと見なされるデータはフィルタリングによって除外され、送信されません。
- [Full]：除外された攻撃者 / 攻撃対象者の IP アドレスを除き、すべてのデータが SensorBase ネットワークに提供されます。

注意　ネットワーク参加に参加するには、免責事項に同意する必要があります。

ステップ 4　ネットワーク参加データから除外する IP アドレスまたはアドレス範囲を指定するには、[Add] をクリックし、[IP Address] フィールドに IP アドレスまたはアドレス範囲を入力します。除外した IP アドレスは、[IP Addresses] テーブルに表示されます。

ステップ 5　除外した IP アドレスまたはアドレス範囲を削除するには、[IP Addresses] テーブルから該当の IP アドレスまたはアドレス範囲を選択し、[Delete] 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 6　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。

グローバル相関のトラブルシューティング

グローバル相関を設定するときに、次の点に注意してください。

- グローバル相関更新は、センサー管理インターフェイスを介して発生するため、ファイアウォールで、ポート 443 および 80 のトラフィックが許可されている必要があります。
- グローバル相関機能を動作させるには、HTTP プロキシ サーバまたは DNS サーバを設定する必要があります。
- グローバル相関機能を動作させるには、有効な IPS ライセンスが必要です。
- グローバル相関機能には、外部 IP アドレスだけが含まれているため、社内ラボにセンサーを配置した場合は、グローバル相関情報を受信できません。
- 使用しているセンサーが、グローバル相関機能をサポートしていることを確認します。

（注）　AIP SSC-5 は、グローバル相関機能をサポートしていません。

- 使用している IPS バージョンが、グローバル相関機能をサポートしていることを確認します。

（注）　IPS 6.1 および 6.2 は、グローバル相関機能をサポートしていません。

グローバル相関のディセーブル化

DNS サーバまたは HTTP プロキシ サーバを使用できない環境にセンサーが配置されている場合、グローバル相関をディセーブルにして、全般的なセンサー ヘルス状態でグローバル相関のヘルス状態が（問題があることを示す）赤色で表示されないようにすることができます。グローバル相関のステータスを除外するように、センサー ヘルス状態を設定することもできます。

グローバル相関インスペクション、レピュテーション フィルタリング、およびネットワーク参加をディセーブルにするには、次の手順を実行します。

ステップ 1　管理者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] > [Global Correlation] > [Inspection/Reputation] を選択します。

ステップ 3　グローバル相関インスペクションおよびレピュテーション フィルタリングをディセーブルにするには、[Off] オプション ボタンをクリックします。

ステップ 4　レピュテーション フィルタリングをディセーブルにするには、[Off] オプション ボタンをクリックします。

ステップ 5　[Configuration] > *sensor_name* > [Policies] > [Global Correlation] > [Network Participation] を選択します。

ステップ 6　ネットワーク参加をディセーブルにするには、[Off] オプション ボタンをクリックします。

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 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。

CHAPTER 14

SSH および証明書の設定

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

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

この章では、センサーの SSH と証明書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。

SSH について

SSH は、セキュリティで保護されていないチャネルでの強力な認証と安全な通信を提供します。SSH は、センサーへの接続を暗号化し、正しいセンサーに接続していることを検証するためのキーを提供します。また、ブロッキングを行うため、センサーが接続する他のデバイスに対する認証および暗号化されたアクセスも提供します。

SSH でホストやネットワークの認証を行うときには、次のいずれかまたは両方が使用されます。

- パスワード
- ユーザ RSA 公開キー

SSH は、以下に対する保護を提供します。

- IP スプーフィング：リモート ホストが、信頼できるホストから送信されたように装うパケットを送信します。

（注）　SSH は、外部へのルータであるようになりすますローカル ネットワーク上のスプーファからも保護します。

- IP ソース ルーティング：ホストが、他の信頼できるホストから送信された IP パケットを装います。
- DNS スプーフィング：攻撃者がネーム サーバ レコードを偽造します。
- 中間ホストによるクリア テキスト パスワードやデータの代行受信。
- 中間ホストを支配する攻撃者によるデータ操作。
- X 認証データをリッスンして X11 サーバにスプーフィング接続する攻撃。

（注）　SSH では、クリア テキストでのパスワードの送信は行われません。

認証キーの設定

ここでは、センサーの認証キー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。

[Authorized Keys] ペイン

（注）　認証キーを追加または編集するには、管理者である必要があります。オペレータ権限やビューア権限で許可キーの追加や編集を試みると、「Delivery Failed」メッセージが表示されます。

ローカル SSH サーバへのログインに RSA 認証を使用することを許可されたクライアントの公開キーを定義するには、[Authorized Keys] ペインを使用します。[Authorized Keys] ペインには、センサーへのアクセスが許可されたすべての SSH クライアントの公開キーが表示されます。参照できるのは自分のキーだけで、他のユーザのキーは参照できません。

センサーにログインできる各ユーザには、そのユーザがログインする際に使用する各クライアントにより収集された許可キーのリストが割り当てられています。SSH を使用してセンサーにログインするときは、パスワードの代わりに RSA 認証を使用できます。

公開キーの定義には、秘密キーを保存するクライアントで RSA キー生成ツールを使用します。生成された公開キーを 3 つの数字（係数の長さ、公開指数、公開係数）の組み合わせとして表示し、これらの数字を [Authorized Keys] ペインの下にあるフィールドに入力します。

[Authorized Keys] ペインのフィールド定義

[Authorized Keys] ペインには次のフィールドがあります。

- [ID]：キーを識別するための一意の文字列（1 ～ 256 文字）。ID にスペースが含まれているか、または英数字が 256 文字を超えていると、エラー メッセージが表示されます。
- [Modulus Length]：係数の有効ビット数（511 ～ 2048）。長さが範囲外の場合は、エラー メッセージが表示されます。
- [Public Exponent]：RSA アルゴリズムにより、データを暗号化するために使用されます。有効な範囲は 3 ～ 2147483647 です。指数が範囲外の場合は、エラー メッセージが表示されます。
- [Public Modulus]：RSA アルゴリズムにより、データを暗号化するために使用されます。公開係数は、1 ～ 2048 の数字の文字列です（係数は (2 ^ 長さ) < 係数 < (2 ^ (長さ + 1))）。係数が範囲外であるか、または数字以外の文字を使用すると、エラー メッセージが表示されます。数字は、「^[0-9][0-9]*$」のパターンに一致する必要があります。

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

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

- [ID]：キーを識別するための一意の文字列（1 ～ 256 文字）。ID にスペースが含まれているか、または英数字が 256 文字を超えていると、エラー メッセージが表示されます。
- [Modulus Length]：係数の有効ビット数（511 ～ 2048）。長さが範囲外の場合は、エラー メッセージが表示されます。
- [Public Exponent]：RSA アルゴリズムにより、データを暗号化するために使用されます。有効な範囲は 3 ～ 2147483647 です。指数が範囲外の場合は、エラー メッセージが表示されます。
- [Public Modulus]：RSA アルゴリズムにより、データを暗号化するために使用されます。公開係数は、1 ～ 2048 の数字の文字列です（係数は (2 ^ 長さ) < 係数 < (2 ^ (長さ + 1))）。係数が範囲外であるか、または数字以外の文字を使用すると、エラー メッセージが表示されます。数字は、「^[0-9][0-9]*$」のパターンに一致する必要があります。

許可キーの定義

公開キーを定義するには、次の手順を実行します。

ステップ 1　管理者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* > [Sensor Management] > [SSH] > [Authorized Keys] を選択し、[Add] をクリックして、リストに公開キーを追加します。最大 50 個の SSH 認証キーを追加できます。

ステップ 3　[ID] フィールドに、キーを識別するための一意の ID を入力します。

ステップ 4　[Modulus Length] フィールドに、整数を入力します。係数の長さは、係数の有効ビット数で表します。RSA キーの強度は、係数のサイズに依存します。係数のビット数が多いほど、キーは強力になります。

（注）　係数の長さ、公開指数、および公開係数がわからない場合は、秘密キーを保存するクライアントで RSA キー生成ツールを使用します。生成された公開キーを 3 つの数字（係数の長さ、公開指数、公開係数）として表示し、ステップ 4 ～ 6 でこれらの数字を入力します。

ステップ 5　[Public Exponent] フィールドに、整数を入力します。RSA アルゴリズムでは、公開指数を使用してデータが暗号化されます。公開指数の有効な値は、3 ～ 2147483647 の数字です。

ステップ 6　[Public Modulus] フィールドに、値を入力します。公開係数は、数字の文字列です（係数は (2 ^ 長さ) < 係数 < (2 ^ (長さ + 1))）。RSA アルゴリズムでは、公開係数を使用してデータが暗号化されます。

ヒント　変更を破棄して [Add Authorized Key] 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。[Authorized Keys] ペインの認証キー リストに新しいキーが表示されます。

ステップ 8　認証キー リストの既存のエントリを編集するには、そのエントリを選択し、[Edit] をクリックします。

ステップ 9　[Modulus Length]、[Public Exponent]、[Public Modulus] フィールドを編集します。

注意　エントリの作成後、[ID] フィールドを編集することはできません。

ヒント　変更を破棄して [Edit Authorized Key] 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 10　[OK] をクリックします。[Authorized Keys] ペインの認証キー リストに編集後のキーが表示されます。

ステップ 11　リストから公開キーを削除するには、そのキーを選択し、[Delete] をクリックします。[Authorized Keys] ペインの認証キー リストにキーが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 12　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。

既知のホスト キーの設定

ここでは既知のホスト キ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。

[Known Host Keys] ペイン

（注）　既知のホスト キーを追加または編集するには、管理者である必要があります。

センサーが管理するブロッキング デバイス、アップデートのダウンロードやファイルのコピーに使用する SSH（SCP）サーバの公開キーを定義するには、[Known Host Keys] ペインを使用します。[Known Host Keys] ページの設定に必要な情報を取得するには、各デバイスおよびサーバからその公開キーを入手することが必要です。公開キーを正しい形式で入手できない場合は、[Add Known Host Keys] ダイアログボックスで [Retrieve Host Key] をクリックします。

IME は、IP アドレスに指定されているホストから既知のホスト キーを取得しようとします。成功すると、IME により、[Add Known Host Key] ペインにキーが読み込まれます。

（注）　[Retrieve Host Key] は、[Add] ダイアログボックスでのみ使用できます。IP アドレスが無効であると、エラー メッセージが表示されます。

[Known Host Keys] ペインのフィールド定義

[Known Host Keys] ペインには次のフィールドがあります。

- [IP Address]：キーを追加しているホストの IP アドレス。
- [Modulus Length]：係数の有効ビット数（511 ～ 2048）。長さが範囲外の場合は、エラー メッセージが表示されます。
- [Public Exponent]：RSA アルゴリズムにより、データを暗号化するために使用されます。有効な範囲は 3 ～ 2147483647 です。指数が範囲外の場合は、エラー メッセージが表示されます。
- [Public Modulus]：RSA アルゴリズムにより、データを暗号化するために使用されます。公開係数は、1 ～ 2048 の数字の文字列です（係数は (2 ^ 長さ) < 係数 < (2 ^ (長さ + 1))）。係数が範囲外であるか、または数字以外の文字を使用すると、エラー メッセージが表示されます。数字は、「^[0-9][0-9]*$」のパターンに一致する必要があります。

[Add Known Host Key] および [Edit Known Host Key] ダイアログボックスのフィールド定義

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

センサーが管理するブロッキング デバイス、アップデートのダウンロードやファイルのコピーに使用する SSH（SCP）サーバの公開キーを定義するには、[Known Host Keys] ペインを使用します。[Known Host Keys] ページの設定に必要な情報を取得するには、各デバイスおよびサーバからその公開キーを入手することが必要です。公開キーを正しい形式で入手できない場合は、[Add Known Host Keys] ダイアログボックスで [Retrieve Host Key] をクリックします。

IME は、IP アドレスに指定されているホストから既知のホスト キーを取得しようとします。成功すると、IME により、[Add Known Host Key] ペインにキーが読み込まれます。

（注）　[Retrieve Host Key] は、[Add] ダイアログボックスでのみ使用できます。IP アドレスが無効であると、エラー メッセージが表示されます。

既知のホスト キーの定義

既知のホスト キーを設定するには、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* > [Sensor Management] > [SSH] > [Known Host Keys] を選択し、[Add] をクリックして、リストに既知のホスト キーを追加します。

ステップ 3　[IP Address] フィールドに、キーの追加対象となるホストの IP アドレスを入力します。

ステップ 4　[Retrieve Host Key] をクリックします。IME が、ステップ 3 で入力した IP アドレスにあるホストからキーを取得しようとします。成功した場合は、ステップ 8 に進みます。成功しなかった場合は、ステップ 5 ～ 7 を実行します。

注意　取得したキーがアドレスに対して正しいことを検証し、サーバ IP アドレスがスプーフィングされていないことを確認します。

ステップ 5　[Modulus Length] フィールドに、整数を入力します。係数の長さは、係数の有効ビット数で表します。RSA キーの強度は、係数のサイズに依存します。係数のビット数が多いほど、キーは強力になります。

ステップ 6　[Public Exponent] フィールドに、整数を入力します。RSA アルゴリズムでは、公開指数を使用してデータが暗号化されます。

ステップ 7　[Public Modulus] フィールドに、値を入力します。公開係数は、数字の文字列です（係数は (2 ^ 長さ) < 係数 < (2 ^ (長さ + 1))）。RSA アルゴリズムでは、公開係数を使用してデータが暗号化されます。

ヒント　変更を破棄して [Add Known Host Key] 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] をクリックします。[Known Host Keys] ペインの既知のホスト キー リストに新しいキーが表示されます。

ステップ 9　認証キー リストの既存のエントリを編集するには、そのエントリを選択し、[Edit] をクリックします。

ステップ 10　[Modulus Length]、[Public Exponent]、[Public Modulus] フィールドを編集します。

注意　エントリの作成後、[ID] フィールドを編集することはできません。

ヒント　変更を破棄して [Edit Known Host Key] 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 11　[OK] をクリックします。[Known Host Keys] ペインの既知のホスト キー リストに編集後のキーが表示されます。

ステップ 12　リストから公開キーを削除するには、そのキーを選択し、[Delete] をクリックします。[Known Host Keys] ペインの既知のホスト キー リストにキーが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 13　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。

センサー キーの生成

ここでは、センサー キーの取得方法について説明します。内容は次のとおりです。

[Sensor Key] ペイン

（注）　センサー SSH ホスト キーを生成するには、管理者である必要があります。

サーバでは、その身元を証明する手段として SSH ホスト キーが使用されます。クライアントは、既知のキーを見つけると、正しいサーバに接続したと認識します。センサーでは、初回起動時に SSH ホスト キーが生成されます。[Sensor Key] ペインに表示されます。キーを新しいキーに置換するには、[Generate Key] をクリックします。

フィールド定義

[Sensor Key] ペインには、センサー SSH ホスト キーが表示されます。新しいセンサー SSH ホスト キーを生成するには、[Generate Key] を押します。

センサー SSH ホスト キーの表示と生成

センサー SSH ホスト キーの表示や生成を行うには、次の手順を実行します。

ステップ 1　管理者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* > [Sensor Management] > [SSH] > [Sensor Key] を選択します。センサー SSH ホスト キーが表示されます。

ステップ 3　新しいセンサー SSH ホスト キーを生成するには、[Generate Key] をクリックします。ダイアログボックスに次の警告が表示されます。

```
Generating a new SSH host key requires you to update the known hosts tables on remote
systems with the new key so that future connections succeed. Do you want to continue?
```

注意　これ以降は、既存のキーの代わりに新しいキーが使用されるため、引き続き正常に接続するためには、リモート システム上にある既知ホストのテーブルを新しいホスト キーで更新する必要があります。

ステップ 4　[OK] をクリックして続行します。新しいホスト キーが生成され、古いホスト キーが削除されます。ステータス メッセージにより、キーが正常に更新されたことが通知されます。

証明書の概要

（注）　IME には、IDM コンフィギュレーション コンポーネントが組み込まれています。

Cisco IPS には、IDM を実行する Web サーバが含まれています。管理ステーションは、この Web サーバに接続します。ブロッキング転送センサーも、マスター ブロッキング センサーの Web サーバに接続します。セキュリティ機能を提供するため、この Web サーバは TLS という暗号化プロトコルを使用します。このプロトコルは、SSL プロトコルと密接な関係があります。Web ブラウザでは、`https://ip_address` で始まる URL が入力されると、それに対する応答として、TLS プロトコルまたは SSL プロトコルによりホストとの間で暗号化セッションのネゴシエーションが行われます。

注意　Web ブラウザでは、初めてのネゴシエーションが行われる際、この時点ではまだ Certification Authority（CA; 認証局）に対する信頼が確立されていないため、IDM から提示される証明書は拒否されます。

（注）　TLS および SSL を使用できるように、IDM はデフォルトでイネーブルになっています。TLS と SSL を使用することを強く推奨します。

TLS による暗号化セッションのネゴシエーション プロセスは、クライアントとサーバとが協調して何度もデータのやり取りを行うことから、「ハンドシェイク」と呼ばれます。サーバからクライアントへ証明書が送信されると、クライアントでは、この証明書に対して、次の 3 つのテストが実行されます。

1. 証明書に記載されている発行元は信頼できるか。

   各 Web ブラウザには、出荷される時点で、信頼されているサードパーティ CA のリストが組み込まれています。証明書に記載されている発行元が、ブラウザにより信頼されている CA のリストに含まれていれば、この最初のテストでは問題なしと判断されます。

2. その日の日付が、証明書の有効期間内にあるか。

   それぞれの証明書には、有効期間を表す 2 つの日付が記載された [Validity] フィールドがあります。その日の日付がこの期間内に該当すれば、この 2 番目のテストでは問題なしと判断されます。

3. 証明書に記載されているサブジェクトの共通名が、URL ホスト名と一致するか。

   URL ホスト名が、サブジェクトの共通名と比較されます。一致すれば、この 3 番目のテストでは問題なしと判断されます。

Web ブラウザから IDM に接続しようとすると、センサーは独自の証明書を発行しますが（センサーが自分自身の CA）、ブラウザにより信頼されている CA のリストにはセンサーが含まれていないため、返された証明書は無効と見なされます。

ブラウザにエラー メッセージが表示された場合の対処方法としては、次の 3 つの選択肢が考えられます。

- サイトへの接続を即座に解除する。
- その他の Web ブラウザ セッション用に証明書を受け入れる。
- 証明書に記載されている発行元を Web ブラウザの信頼 CA リストに追加して、有効期間が経過するまで証明書を信頼する。

最も簡単な方法は、発行元を永続的に信頼することです。ただし、発行元を追加する前に必ず、アウトオブバンド方式を使用して、証明書のフィンガープリントを検証します。これにより、センサーになりすました攻撃者による被害を回避できます。Web ブラウザに表示される証明書のフィンガープリントが、センサーのフィンガープリントと一致するかどうかを確認してください。

注意　センサーの組織名またはホスト名を変更した場合は、センサーの次回リブート時に新しい証明書が生成されます。Web ブラウザから IDM への次回接続時には、手動上書きダイアログボックスが表示されます。この場合は、Internet Explorer および Netscape で、証明書フィンガープリントの検証を再度実行する必要があります。

詳細情報

マスター ブロッキング センサーの詳細については、「マスター ブロッキング センサーの設定」（P.15-26）を参照してください。

信頼できるホストの設定

ここでは、信頼できるホストの設定方法について説明します。内容は次のとおりです。

[Trusted Hosts] ペイン

（注）　信頼できるホストを追加するには、管理者である必要があります。

マスター ブロッキング センサー、およびアップデートをダウンロードするためにセンサーが使用する TLS と SSL のサーバの証明書を追加するには、[Trusted Hosts] ペインを使用します。このペインを使用して、センサーが通信する外部製品インターフェイス（CSA MC など）の IP アドレスを追加することもできます。

[Trusted Hosts] ペインには、追加したすべての信頼できるホスト証明書がリストされます。証明書は、IP アドレスを入力することにより追加できます。IME では、追加された証明書が取得されると同時に、そのフィンガープリントが表示されます。フィンガープリントを受け入れると、証明書に対する信頼が確立されます。リストでは、エントリの追加や削除は行うことができますが、編集はできません。

[Trusted Hosts] ペインのフィールド定義

[Trusted Hosts] ペインには次のフィールドがあります。

- [IP Address]：信頼できるホストの IP アドレス。
- [MD5]：MD5（メッセージ ダイジェスト 5）暗号化。MD5 は、メッセージの 128 ビット ハッシュの計算に使用されるアルゴリズムです。

- [SHA1]：セキュリティで保護されたセキュア アルゴリズム。SHA1 は、暗号化メッセージ ダイジェスト アルゴリズムです。

[Add Trusted Host] ダイアログボックスのフィールド定義

[Add Trusted Host] ダイアログボックスには、次のフィールドが表示されます。

- [IP Address]：信頼できるホストの IP アドレス。
- [Port]：（任意）ホスト証明書を取得するポート番号を指定します。

信頼できるホストの追加

信頼できるホストを追加するには、次の手順を実行します。

ステップ 1　管理者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* > [Sensor Management] > [Certificates] > [Trusted Hosts] を選択し、[Add] をクリックして、リストに信頼できるホストを追加します。

ステップ 3　[IP Address] フィールドに、信頼できるホストの追加対象となるホストの IP アドレスを入力します。

ステップ 4　センサー が 443 以外のポートを使用する場合は、[Port] フィールドにポート番号を入力します。

ヒント　変更を破棄して [Add Trusted Host] 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　[OK] をクリックします。IME が、ステップ 3 で入力した IP アドレスにあるホストから証明書を取得します。[Trusted Hosts] ペインの信頼できるホストのリストに、新しく追加された信頼できるホストが表示されます。ダイアログボックスにより、IME がセンサーと通信していることが通知されます。

```
Communicating with the sensor, please wait ...
```

ダイアログボックスに、IME が信頼できるホストを正常に追加できたかどうかを知らせるステータスが表示されます。

```
The new host was added successfully.
```

ステップ 6　表示される値と、直接端末接続またはコンソールなどで安全に取得した値とを比較することにより、そのフィンガープリントが正しいかどうかを検証します。矛盾点が見つかった場合は、すぐに、その信頼できるホストを削除してください。

ステップ 7　信頼できるホストのリストに既存のエントリを表示するには、そのエントリを選択し、[View] をクリックします。[View Trusted Host] ダイアログボックスが表示されます。証明書のデータが表示されます。このダイアログボックスに表示されるデータは、読み取り専用です。

ステップ 8　[OK] をクリックします。リストから信頼できるホストを削除するには、そのキーを選択し、[Delete] をクリックします。[Trusted Hosts] ペインの信頼できるホストのリストに、信頼できるホストが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 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。

サーバ証明書の生成

ここでは、サーバ証明書の生成方法について説明します。内容は次のとおりです。

[Server Certificate] ペイン

（注）　サーバ証明書を生成するには、管理者である必要があります。

[Server Certificate] ペインには、センサー サーバ X.509 証明書が表示されます。このペインでは、新しいサーバによる自己署名 X.509 証明書を生成できます。証明書は、センサーの初回起動時に生成されます。新しいホスト証明書を生成するには、[Generate Certificate] をクリックします。

注意　証明書にはセンサーの IP アドレスが含まれます。センサーの IP アドレスを変更した場合は、新しい証明書を生成する必要があります。

フィールド定義

[Server Certificate] ペインには、センサー サーバ X.509 証明書が表示されます。新しいセンサー X.509 証明書を生成するには、[Generate Certificate] をクリックします。

サーバ証明書の表示と生成

センサー サーバ X.509 証明書の表示や生成を行うには、次の手順を実行します。

ステップ 1　管理者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* > [Sensor Setup] > [Certificate] > [Server Certificate] を選択します。センサー サーバ X.509 証明書が表示されます。

ステップ 3　新しいセンサー サーバ X.509 証明書を生成するには、[Generate Certificate] をクリックします。ダイアログボックスに次の警告が表示されます。

```
Generating a new server certificate requires you to verify the new fingerprint the next
time you connect or when you add the sensor as a trusted host. Do you want to continue?
```

注意　新しいフィンガープリントを書き込みます。接続時に Web ブラウザの表示内容を確認する場合や、センサーを信頼できるホストとして追加する場合には、このフィンガープリントが必要になります。センサーがマスター ブロッキング センサーである場合は、マスター ブロッキング センサーにブロックを送信するリモート センサー上で、信頼できるホストのテーブルを更新する必要があります。

ステップ 4　[OK] をクリックして続行します。新しいサーバ証明書が生成され、古いサーバ証明書が削除されます。

CHAPTER 15

Attack Response Controller でのブロッキングとレート制限の設定

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

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

（注） ARC は、以前は Network Access Controller と呼ばれていました。名前は変更されましたが、IME および CLI では、Network Access Controller、**nac**、および **network-access** という名前で呼ばれています。

この章では、センサー上でブロッキング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。

ARC のコンポーネント

ここでは、ARC の各種コンポーネントについて説明します。内容は次のとおりです。

- 「サポートされるデバイス数」（P.15-6）

ブロッキングについて

（注）　ARC は、以前は Network Access Controller と呼ばれていました。名前は変更されましたが、IME および CLI では、Network Access Controller、**nac**、および **network-access** という名前で呼ばれています。

ARC は、攻撃側のホストおよびネットワークからのアクセスをブロックすることにより、疑わしいイベントに対応し、ネットワーク デバイスを管理します。ARC は、管理しているデバイスの IP アドレスをブロックします。他のマスター ブロッキング センサーを含め、管理しているすべてのデバイスに同じブロックを送信します。ARC は、ブロックの時間をモニタし、時間の経過後にブロックを削除します。

ARC は、7 秒以内に新しいブロックのアクション応答を完了します。ほとんどの場合は、より短い時間でアクション応答を完了します。このパフォーマンス目標を達成するために、センサーでのブロックの実行レートが高すぎたり、管理するブロッキング デバイスおよびインターフェイスが多すぎたりしないように設定してください。最大ブロック数は 250 以下にし、最大ブロッキング項目数は 10 以下にすることを推奨します。ブロッキング項目の最大数を計算するために、セキュリティ アプライアンスはブロッキング コンテキストあたり 1 つのブロッキング項目としてカウントします。ルータは、ブロッキング インターフェイス / 方向あたり 1 つのブロッキング項目としてカウントします。Catalyst ソフトウェアを実行しているスイッチは、ブロッキング VLAN あたり 1 つのブロッキング項目としてカウントします。推奨される制限を超えた場合、ARC はブロックをタイミングよく適用しなかったり、ブロックをまったく適用できなかったりすることがあります。

注意　ブロッキングは、マルチ モード管理コンテキストの FWSM ではサポートされません。

マルチモードで設定されているセキュリティ アプライアンスでは、Cisco IPS はブロック要求に VLAN 情報を含めません。したがって、ブロックされる IP アドレスが各セキュリティ アプライアンスに対して正しいことを確認する必要があります。たとえば、センサーは、VLAN A に対して設定されているセキュリティ アプライアンス カスタマー コンテキストでパケットをモニタし、VLAN B に対して設定されている別のセキュリティ アプライアンス カスタマー コンテキストでブロッキングしている場合があります。VLAN A でブロックをトリガーするアドレスは、VLAN B 上の別のホストを指している可能性があります。

ブロックには次の 3 種類があります。

- ホスト ブロック：特定の IP アドレスからのすべてのトラフィックをブロックします。
- 接続ブロック：特定の送信元 IP アドレスから特定の宛先 IP アドレスおよび宛先ポートへのトラフィックをブロックします。同じ送信元 IP アドレスから異なる宛先 IP アドレスまたは宛先ポートへの複数の接続ブロックによって、接続ブロックからホスト ブロックにブロックが自動的に切り替えられます。
- ネットワーク ブロック：特定のネットワークからのトラフィックをすべてブロックします。ホスト ブロックと接続ブロックは、手動で開始するか、シグニチャがトリガーされたときに自動的に開始できます。ネットワーク ブロックは手動でだけ開始できます。

（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。

注意　ブロッキングとセンサーのパケット ドロップ機能を混同しないでください。センサーでは、インライン モードのセンサーに対してパケットのインライン拒否、接続のインライン拒否、および攻撃者のインライン拒否のアクションが設定されている場合にパケットをドロップできます。

自動ブロックの場合は、特定のシグニチャのイベント アクションとして [Request Block Host] チェックボックスまたは [Request Block Connection] チェックボックスをオンにし、そのアクションをすべての設定済みイベント アクション オーバーライドに追加する必要があります。これにより、SensorApp はそのシグニチャがトリガーされたときに ARC にブロック要求を送信することができます。ARC は、SensorApp からブロック要求を受信すると、ホストまたは接続をブロックするようにデバイス設定を更新します。

Cisco ルータおよび Catalyst 6500 シリーズ スイッチでは、ARC は ACL または VACL を適用してブロックを作成します。ACL および VACL は、インターフェイス方向または VLAN 上のデータ パケットの経路を許可または拒否します。各 ACL または VACL には、IP アドレスに適用される許可条件と拒否条件が含まれます。セキュリティ アプライアンスでは、ACL または VACL は使用されません。組み込みの **shun** および **no shun** コマンドが使用されます。

注意　ARC が作成する ACL が、ユーザやその他のシステムによって変更されることがあってはなりません。これらの ACL は一時的なものであり、新しい ACL がセンサーによって常に作成されています。Pre-Block ACL および Post-Block ACL に対してのみ、変更を加えることができます。

ARC がデバイスを管理するためには、次の情報が必要です。

- ログイン ユーザ ID（デバイスに AAA が設定されている場合）
- ログイン パスワード
- イネーブル パスワード（イネーブル特権のあるユーザは不要）
- 管理対象のインターフェイス（ethernet0 や vlan100 など）
- 作成される ACL または VACL で、最初に適用する任意の既存 ACL または VACL 情報（Pre-Block ACL または Pre-Block VACL）、または最後に適用する ACL または VACL 情報（Post-Block ACL または Post-Block VACL）これは、セキュリティ アプライアンスには該当しません。セキュリティ アプライアンスはブロックに ACL を使用しないためです。
- デバイスとの通信に Telnet と SSH のどちらを使用しているか
- ブロックしない IP アドレス（ホストまたはホストの範囲）
- ブロックの継続時間

ヒント　ARC のステータスを表示するには、IME で [Configuration] > *sensor_name* > [Sensor Monitoring] > [Support Information] > [Statistics] を選択します。

（注）　レート制限およびブロッキングは、IPv6 トラフィックではサポートされていません。ブロック アクションまたはレート制限アクションが設定されているシグニチャが IPv6 トラフィックによってトリガーされると、アラートが生成されますが、アクションは実行されません。

詳細情報

- シグニチャに Request Block Host または Request Block Connection イベント アクションを追加する手順については、「シグニチャへのアクションの割り当て」（P.9-19）を参照してください。
- 特定の RR のアラートに Request Block Host または Request Block Connection イベント アクションを追加するオーバーライドを設定する手順については、「イベント アクション オーバーライドの追加、編集、削除、イネーブル化、ディセーブル化」（P.11-15）を参照してください。
- Pre-Block ACL および Post-Block ACL の詳細については、「センサーによるデバイスの管理方法」（P.15-19）を参照してください。

レート制限について

ARC は、保護されているネットワーク内のトラフィックのレート制限を行います。レート制限により、センサーはネットワーク デバイス上の指定したトラフィック クラスのレートを制限できます。レート制限応答は、ホスト フラッド エンジンとネット フラッド エンジン、および TCP ハーフオープン SYN シグニチャに対してサポートされます。ARC では、Cisco IOS 12.3 以降を実行しているネットワーク デバイスにレート制限を設定できます。マスター ブロッキング センサーは、レート制限要求をブロッキング転送センサーに転送することもできます。

レート制限を追加するには、次の項目を指定します。

- レート制限のための送信元アドレスまたは宛先アドレス（あるいはその両方）
- TCP または UDP プロトコルを使用したレート制限のための送信元ポートまたは宛先ポート（あるいはその両方）

レート制限シグニチャを調整することもできます。また、アクションを [Request Rate Limit] に設定し、これらのシグニチャのパーセンテージを設定する必要があります。

（注）　レート制限およびブロッキングは、IPv6 トラフィックではサポートされていません。ブロック アクションまたはレート制限アクションが設定されているシグニチャが IPv6 トラフィックによってトリガーされると、アラートが生成されますが、アクションは実行されません。

表 15-1 に、サポートされているレート制限シグニチャとパラメータを示します。

表 15-1　レート制限シグニチャ

シグニチャ ID	シグニチャ名	プロトコル	許可される宛先 IP アドレス	データ
2152	ICMP Flood Host	ICMP	Yes	echo-request
2153	ICMP Smurf Attack	ICMP	Yes	echo-reply
4002	UDP Flood Host	UDP	Yes	なし
6901	Net Flood ICMP Reply	ICMP	No	echo-reply
6902	Net Flood ICMP Request	ICMP	No	echo-request
6903	Net Flood ICMP Any	ICMP	No	なし

表 15-1　レート制限シグニチャ（続き）

シグニチャ ID	シグニチャ名	プロトコル	許可される宛先 IP アドレス	データ
6910	Net Flood UDP	UDP	No	なし
6920	Net Flood TCP	TCP	No	なし
3050	TCP HalfOpenSyn	TCP	No	halfOpenSyn

ヒント　ARC のステータスを表示するには、IME で [Configuration] > *sensor_name* > [Sensor Monitoring] > [Support Information] > [Statistics] を選択します。

詳細情報

- ルータにレート制限を設定する手順については、「ルータ ブロッキング デバイスおよびレート制限デバイスのインターフェイスの設定」（P.15-21）を参照してください。
- センサーをマスター ブロッキング センサーとして設定する手順については、「マスター ブロッキング センサーの設定」（P.15-28）を参照してください。

レート制限でのサービス ポリシーについて

レート制限が設定されているインターフェイス/方向にサービス ポリシーを適用しないでください。適用した場合は、レート制限アクションが失敗します。レート制限を設定する前に、インターフェイス/方向にサービス ポリシーがないことを確認し、存在する場合には削除します。ARC では、ARC が以前に追加したものでないかぎり、既存のレート制限は削除されません。

レート制限では ACL が使用されますが、ブロックと同じ方法では使用されません。レート制限では、**ACL** および**クラス マップ** エントリを使用してトラフィックを識別し、**ポリシー マップ**および**サービス ポリシー** エントリを使用してトラフィックをポリシングします。

ARC を設定する前に

注意　2 つのセンサーが同じデバイスでブロッキングまたはレート制限を制御することはできません。この状況が必要な場合は、一方のセンサーをマスター ブロッキング センサーとして設定してデバイスを管理し、もう一方のセンサーでマスター ブロッキング センサーに要求を転送できます。

（注）　マスター ブロッキング センサーを追加する場合は、センサーあたりのブロッキング デバイス数を減らします。たとえば、それぞれ 1 つのブロッキング インターフェイス/方向を持つ 10 個のセキュリティ アプライアンスと 10 台のルータでブロックする場合は、センサーに 10 個を割り当て、マスター ブロッキング センサーに残りの 10 個を割り当てることができます。

ブロッキングやレート制限を実行するように ARC を設定する前に、必ず次の作業を行ってください。

- ネットワーク トポロジを分析し、どのデバイスをどのセンサーによってブロックしなければならないか、またブロックしてはならないのはどのアドレスかを確認します。

- 各デバイスにログインするために必要なユーザ名、デバイスのパスワード、イネーブル パスワード、および接続タイプ（Telnet または SSH）の情報を収集します。
- デバイス上のインターフェイスの名前を確認します。
- 必要に応じて、Pre-Block ACL または Pre-Block VACL、および Post-Block ACL または Post-Block VACL の名前を確認します。
- ブロックするインターフェイスとブロックしないインターフェイス、およびその方向（インかアウトか）を確認します。誤ってネットワーク全体をシャットダウンすることは避けなければなりません。

サポートされるデバイス数

注意　推奨される制限を超えた場合、ARC はブロックをタイミングよく適用しなかったり、ブロックをまったく適用できなかったりすることがあります。

デフォルトでは、ARC サービスは任意の組み合わせで 250 個までのデバイスをサポートします。ARC によるブロッキングがサポートされるデバイスは、次のとおりです。

- Cisco IOS 11.2 以降（ACL）を使用する Cisco シリーズ ルータ
  - Cisco 1600 シリーズ ルータ
  - Cisco 1700 シリーズ ルータ
  - Cisco 2500 シリーズ ルータ
  - Cisco 2600 シリーズ ルータ
  - Cisco 2800 シリーズ ルータ
  - Cisco 3600 シリーズ ルータ
  - Cisco 3800 シリーズ ルータ
  - Cisco 7200 シリーズ ルータ
  - Cisco 7500 シリーズ ルータ
- Catalyst 5000 スイッチ、RSM 搭載、IOS 11.2(9)P 以降（ACL）
- Catalyst 6500 スイッチおよび 7600 ルータ、IOS 12.1(13)E 以降（ACL）
- Catalyst 6500 スイッチ 7600 ルータ、Catalyst ソフトウェア バージョン 7.5(1) 以降（VACL）
  - Supervisor Engine 1A（PFC 搭載）
  - Supervisor Engine 1A（MSFC1 搭載）
  - Supervisor Engine 1A（MFSC2 搭載）
  - Supervisor Engine 2（MSFC2 搭載）
  - Supervisor Engine 720（MSFC3 搭載）

  （注）　Supervisor Engine での VACL ブロッキングと MSFC での ACL ブロッキングがサポートされます。
- PIX Firewall、バージョン 6.0 以降（**shun** コマンド）
  - 501

  - 506E
  - 515E
  - 525
  - 535
- ASA、バージョン 7.0 以降（**shun** コマンド）
  - ASA-5510
  - ASA-5520
  - ASA-5540
- FWSM 1.1 以降（**shun** コマンド）

ブロッキングを設定するには、ACL、VACLS、または **shun** コマンドのいずれかを使用します。すべてのファイアウォールおよび ASA モデルは **shun** コマンドをサポートします。

ARC によるレート制限がサポートされるデバイスは、次のとおりです。

- Cisco IOS 12.3 以降を使用する Cisco シリーズ ルータ
  - Cisco 1700 シリーズ ルータ
  - Cisco 2500 シリーズ ルータ
  - Cisco 2600 シリーズ ルータ
  - Cisco 2800 シリーズ ルータ
  - Cisco 3600 シリーズ ルータ
  - Cisco 3800 シリーズ ルータ
  - Cisco 7200 シリーズ ルータ
  - Cisco 7500 シリーズ ルータ

注意　ARC は、VIP を使用する 7500 ルータ上でレート制限を実行することはできません。ARC はエラーを報告しますが、レート制限は実行できません。

ブロッキング プロパティの設定

ここでは、センサーのブロッキング プロパティ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。

[Blocking Properties] ペイン

（注）　ブロッキングの対象としない IP アドレスを追加、編集、削除するには、管理者またはオペレータであることが必要です。

ブロッキングとレート制限をイネーブルにするために必要な基本的な設定を行うには、[Blocking Properties] ペインを使用します。

ブロッキング プロパティについて

ARC は、管理対象デバイス上のブロッキング アクションおよびレート制限アクションを制御します。手動であってもブロックされてはならないホストおよびネットワークを識別できるように、センサーを調整する必要があります。これは、信頼されたネットワーク デバイスの通常の動作が攻撃として扱われる可能性があるためです。そのようなデバイスは絶対にブロックしてはなりません。また、信頼できる内部のネットワークも絶対にブロックしてはなりません。シグニチャを適切にチューニングすることにより、偽陽性の数を減らし、ネットワークが正しく動作することを保証できます。シグニチャのチューニングとフィルタリングによって、アラームの生成を防止します。アラームが生成されない場合、それに関連付けられたブロックも実行されません。

（注）　[Never Block Address] はレート制限には適用されません。このオプションは、Request Block Host または Request Block Connection イベント アクションにのみ適用されます。このオプションは、Deny Attacker Inline、Deny Connection Inline、または Deny Packet Inline イベント アクションには適用されません。ブロック、拒否、またはドロップの対象から外すホストをフィルタ処理によって除外するには、イベント アクション規則を使用します。

ネットマスクを指定すると、それがブロックされないネットワークのネットマスクになります。ネットマスクを指定しないと、指定した IP アドレスだけがブロックされません。

注意　センサーがそれ自体をブロックすることを許可すると、ブロッキング デバイスとの通信ができなくなる可能性があるため、お勧めしません。センサーでそれ自体の IP アドレスをブロックするルールが作成されても、センサーからブロッキング デバイスへのアクセスが妨げられないことが確認された場合は、このオプションを設定できます。

デフォルトでは、センサーのブロッキングはイネーブルになっています。デバイスが ARC によって管理されていて、手動で何かを設定する必要があるときは、まずブロッキングをディセーブルにする必要があります。ユーザと ARC の両方が同じデバイスで同時に変更を加える状況を回避する必要があります。この状況が発生すると、デバイスまたは ARC でエラーが発生します。

デフォルトでは、Cisco IOS デバイスではブロッキングのみサポートされます。レート制限またはブロッキングとレート制限を選択することにより、ブロッキングのデフォルトをオーバーライドできます。

[Blocking Properties] ペインのフィールド定義

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

- [Enable blocking] : ホストのブロッキングをイネーブルにするかどうか。デフォルトはイネーブルです。[Enable blocking] がディセーブルであり、他のフィールドにデフォルト以外の値がある場合は、エラー メッセージが表示されます。

（注）　ブロッキングをイネーブルにする場合は、レート制限もイネーブルにします。ブロッキングをディセーブルにする場合は、レート制限もディセーブルにします。これは、ARC が新しいブロックまたはレート制限の追加や既存のブロックまたはレート制限の削除を行えないことを意味します。

（注）　ブロッキングをイネーブルにしない場合でも、他のすべてのブロッキング設定を指定できます。

- [Allow sensor IP address to be blocked] : センサーの IP アドレスのブロッキングを許可するかどうか。デフォルトはディセーブルです。
- [Log all block events and errors] : ブロックの開始から終了までのイベントと発生したエラー メッセージをログに記録するようにセンサーを設定します。ブロックがデバイスに追加されるかデバイスから削除されると、イベントがログに記録されます。これらすべてのイベントおよびエラーをログに記録する必要はない可能性があります。このオプションをディセーブルにすると、新しいイベントとエラーが抑止されます。デフォルトはイネーブルです。

（注）　すべてのブロック イベントとエラーの記録はレート制限にも適用されます。

- [Enable NVRAM write] : ARC の最初の接続時にルータが NVRAM への書き込みを実行するようにセンサーを設定します。イネーブルになっている場合は、ACL が更新されるたびに NVRAM が書き込まれます。デフォルトはディセーブルです。

（注）　NVRAM の書き込みをイネーブルにすると、ブロッキングとレート制限に対するすべての変更が NVRAM に必ず書き込まれます。ルータが再起動された場合でも、適切なブロックとレート制限がアクティブになります。NVRAM の書き込みがディセーブルになっている場合、ルータの再起動後にブロッキングまたはレート制限が行われない期間が短時間発生します。NVRAM 書き込みをイネーブルにしない場合、NVRAM の寿命が延び、新しいブロックとレート制限の設定にかかる時間が短縮されます。

- [Enable ACL Logging] : ACL または VACL のブロック エントリにログ パラメータを追加するように ARC を設定します。これにより、デバイスはパケットがフィルタ処理されるときに syslog イベントを生成します。このオプションは、ルータとスイッチだけに適用されます。デフォルトはディセーブルです。
- [Maximum Block Entries] : ブロックするエントリの最大数。値は 1 ～ 65535 です。デフォルトは 250 です。
- [Maximum Interfaces] : ブロックを実行するためのインターフェイスの最大数を設定します。

  たとえば、PIX 500 シリーズ セキュリティ アプライアンスは 1 つのインターフェイスとカウントされます。1 つのインターフェイスを持つルータは 1 つとしてカウントされますが、2 つのインターフェイスを持つルータは 2 つとしてカウントされます。インターフェイスの最大数はデバイスあたり 250 です。デフォルトは 250 です。

（注） [Maximum Interfaces] を使用して、ARC が管理できるデバイスおよびインターフェイスの最大数を設定します。ブロッキング デバイスの合計数（マスター ブロッキング センサーを含まない）がこの値を超えることはできません。ブロッキング項目の合計数もこの値を超えることはできません。ブロッキング項目は 1 つのセキュリティ アプライアンス コンテキスト、1 つのルータ ブロッキング インターフェイス/方向、または VLAN をブロッキングしている 1 つの Catalyst ソフトウェア スイッチです。

（注） また、デバイスあたり 250 個のインターフェイス、250 台のセキュリティ アプライアンス、250 台のルータ、250 台の Catalyst ソフトウェア スイッチ、および 100 台のマスター ブロッキング センサーは、固定の最大数であり、変更できません。

- [Maximum Rate Limit Entries]：レート制限エントリの最大数。レート制限エントリの最大数は、ブロッキング エントリの最大数以下である必要があります。ブロッキング エントリより多いレート制限エントリを設定すると、エラーが発生します。値は 1 ～ 32767 です。デフォルトは 250 です。
- [Never Block Addresses]：センサーによるブロッキングの対象外とする IP アドレスを設定します。

（注） [Never Block Address] はレート制限には適用されません。このオプションは、Request Block Host および Request Block Connection イベント アクションにのみ適用されます。このオプションは、Deny Attacker Inline、Deny Connection Inline、または Deny Packet Inline イベント アクションには適用されません。ブロック、拒否、またはドロップの対象から外すホストをフィルタ処理によって除外するには、イベント アクション規則を使用します。

  - [IP Address]：ブロックしない IP アドレス。
  - [Mask]：ブロックしない IP アドレスに対応するマスク。

ブロッキング プロパティの設定

ブロッキング プロパティを設定するには、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* > [Sensor Management] > [Blocking] > [Blocking Properties] を選択します。

ステップ 3　[Enable blocking] チェックボックスをオンにして、ブロッキングとレート制限をイネーブルにします。

（注） ブロッキングまたはレート制限が機能するためには、ブロッキングまたはレート制限を実行するようにデバイスを設定する必要があります。

ステップ 4　必要な場合以外は、[Allow the sensor IP address to be blocked] チェックボックスをオンにしないでください。

注意　センサーがそれ自体をブロックすることを許可すると、ブロッキング デバイスとの通信ができなくなる可能性があるため、お勧めしません。このオプションは、センサーが自分の IP アドレスをブロックする規則を作成した場合に、そのためにセンサーがブロックしている装置にアクセスできなくなることはないと保証されている場合にだけ選択します。

ステップ 5　ブロッキング イベントとエラーをログに記録する場合は、[Log all block events and errors] チェックボックスをオンにします。

ステップ 6　ARC の最初の接続時にルータが NVRAM への書き込みを実行するようにセンサーを設定する場合は、[Enable NVRAM write] チェックボックスをオンにします。

ステップ 7　ACL または VACL のブロック エントリにログ パラメータを追加するように ARC を設定する場合は、[Enable ACL logging] チェックボックスをオンにします。

ステップ 8　[Maximum Block Entries] フィールドには、同時に維持されるブロックの数を入力します（1 ～ 65535）。

（注）　最大ブロック エントリ数を 250 より大きな値に設定することは推奨しません。

（注）　ブロック数が最大ブロック エントリ数を超えることはありません。最大数に達すると、既存のブロックがタイムアウトするか削除されるまで新しいブロックは発生しません。

ステップ 9　ブロックを実行するインターフェイスの数を [Maximum Interfaces] フィールドに入力します。

ステップ 10　レート制限エントリの数（1 ～ 32767）を [Maximum Rate Limit Entries] フィールドに入力します。

注意　レート制限エントリの最大数は、ブロッキング エントリの最大数以下である必要があります。ブロッキング エントリより多いレート制限エントリを設定すると、エラーが発生します。

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 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。

[Add Never Block Address] および [Edit Never Block Address] ダイアログボックスのフィールド定義

[Add Never Block Address] および [Edit Never Block Address] ダイアログボックスには次のフィールドがあります。

- [IP Address]：ブロックしない IP アドレス。
- [Mask]：ブロックしない IP アドレスに対応するマスク。

ブロックしない IP アドレスの追加、編集、削除

ブロックしない IP アドレスを追加、編集、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* > [Sensor Management] > [Blocking] > [Blocking Properties] を選択し、[Add] をクリックして、ブロックしないアドレスのリストにホストまたはネットワークを追加します。

ステップ 3　[IP Address] フィールドに、ホストまたはネットワークの IP アドレスを入力します。

ステップ 4　[Network Mask] フィールドで、ホストまたはネットワークのネットワーク マスクを入力するか、リストからネットワーク マスクを選択します。

ヒント　変更内容を破棄して [Add Never Block Address] 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　[OK] をクリックします。エントリが同一である場合は、エラー メッセージが表示されます。新しいホストまたはネットワークが [Blocking Properties] ペインの [Never Block Addresses] リストに表示されます。

ステップ 6　[Never Block Addresses] リスト内の既存のエントリを編集するには、そのエントリを選択し、[Edit] をクリックします。

ステップ 7　[IP Address] フィールドで、ホストまたはネットワークの IP アドレスを編集します。

ステップ 8　[Network Mask] フィールドで、ホストまたはネットワークのネットワーク マスクを編集します。

ヒント　変更内容を破棄して [Edit Never Block Address] 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。編集したホストまたはネットワークが [Allowed Hosts] ペインの [Never Block Addresses] リストに表示されます。

ステップ 10　リストからホストまたはネットワークを削除するには、そのホストまたはネットワークを選択し、[Delete] をクリックします。そのホストは、[Blocking Properties] ペインの [Never Block Addresses] 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。

デバイス ログイン プロファイルの設定

ここでは、デバイス ログイン プロファイルの設定方法について説明します。内容は次のとおりです。

- 「[Add Device Login Profile] および [Edit Device Login Profile] ダイアログボックスのフィールド定義」（P.15-13）
- 「デバイス ログイン プロファイルの設定」（P.15-14）

[Device Login Profiles] ペイン

（注）　デバイス ログイン プロファイルを追加または編集するには、管理者またはオペレータであることが必要です。

センサーがブロッキング デバイスにログインするときに使用するプロファイルを設定するには、[Device Login Profiles] ペインを使用します。センサーが管理する他のハードウェアのデバイス ログイン プロファイルを設定する必要があります。デバイス ログイン プロファイルには、作成した名前の下に、ユーザ名、ログイン パスワード、およびイネーブル パスワードの情報が含まれます。たとえば、同じパスワードとユーザ名を共有するすべてのルータを 1 つのデバイス ログイン プロファイル名にまとめることができます。

（注）　ブロッキング デバイスを設定する前にデバイス ログイン プロファイルを作成する必要があります。

[Device Login Profiles] ペインのフィールド定義

[Device Login Profiles] ペインには次のフィールドがあります。

- [Profile Name]：プロファイルの名前。
- [Username]：ブロッキング デバイスへのログインに使用するユーザ名。
- [Login Password]：ブロッキング デバイスへのログインに使用するログイン パスワード。

  （注）　パスワードが存在する場合は、固定数のアスタリスクで表示されます。

- [Enable Password]：ブロッキング デバイスで使用されるイネーブル パスワード。

  （注）　パスワードが存在する場合は、固定数のアスタリスクで表示されます。

[Add Device Login Profile] および [Edit Device Login Profile] ダイアログボックスのフィールド定義

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

- [Profile Name]：プロファイルの名前。
- [Username]：ブロッキング デバイスへのログインに使用するユーザ名。
- [Login Password]：ブロッキング デバイスへのログインに使用するログイン パスワード。

（注）　パスワードが存在する場合は、固定数のアスタリスクで表示されます。

- [Enable Password]：ブロッキング デバイスで使用されるイネーブル パスワード。

（注）　パスワードが存在する場合は、固定数のアスタリスクで表示されます。

デバイス ログイン プロファイルの設定

デバイス ログイン プロファイルを設定するには、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* > [Sensor Management] > [Blocking] > [Device Login Profiles] を選択し、[Add] をクリックして、プロファイルを追加します。

ステップ 3　[Profile Name] フィールドにプロファイル名を入力します。

ステップ 4　（任意）[Username] フィールドに、ブロッキング デバイスへのログインに使用するユーザ名を入力します。

ステップ 5　（任意）[New Password] フィールドにログイン パスワードを入力します。

ステップ 6　（任意）確認のために [Confirm New Password] フィールドにもう一度ログイン パスワードを入力します。

ステップ 7　（任意）[New Password] フィールドにイネーブル パスワードを入力します。

ステップ 8　（任意）確認のために [Confirm New Password] フィールドにもう一度イネーブル パスワードを入力します。

ヒント　変更を破棄して [Add Device Login Profile] 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。すでに存在するプロファイル名を入力すると、エラー メッセージが表示されます。新しいデバイス ログイン プロファイルが [Device Login Profile] ペインのリストに表示されます。

ステップ 10　デバイス ログイン プロファイル リストの既存のエントリを編集するには、そのエントリを選択し、[Edit] をクリックします。

ステップ 11　[Username] フィールドで、ブロッキング デバイスへのログインに使用するユーザ名を編集します。

ステップ 12　ログイン パスワードを変更するには、[Change the login password] チェックボックスをオンにします。

ステップ 13　[New Password] フィールドに新しいログイン パスワードを入力します。

ステップ 14　確認のために [Confirm New Password] フィールドに新しいログイン パスワードをもう一度入力します。

ステップ 15　イネーブル パスワードを変更するには、[Change the enable password] チェックボックスをオンにします。

ステップ 16　[New Password] フィールドに新しいイネーブル パスワードを入力します。

ステップ 17　確認のために [Confirm New Password] フィールドにもう一度イネーブル パスワードを入力します。

ヒント　変更を破棄して [Edit Device Login Profile] 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 18　[OK] をクリックします。編集したデバイス ログイン プロファイルが、[Device Login Profile] ペインのリストに表示されます。

ステップ 19　リストからデバイス ログイン プロファイルを削除するには、そのプロファイルを選択し、[Delete] をクリックします。そのデバイス ログイン プロファイルは、[Device Login Profile] ペインの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 20　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。

ブロッキング デバイスの設定

ここでは、ブロッキング デバイスの設定方法について説明します。内容は次のとおりです。

[Blocking Device] ペイン

（注）　ブロッキング デバイスを設定するには、管理者またはオペレータであることが必要です。

センサーがブロッキングとレート制限を実行するために使用するデバイスを設定するには、[Blocking Device] ペインを使用します。Cisco IOS ルータまたは Catalyst 6500 スイッチに配置する ACL 規則を生成するか、またはセキュリティ アプライアンス上に排除規則を生成することによって攻撃をブロックするようにセンサーを設定できます。このようなルータ、スイッチ、ファイアウォールは、ブロッキング デバイスと呼ばれます。

レート制限では ACL が使用されますが、ブロックと同じ方法では使用されません。レート制限では、ACL およびクラス マップ エントリを使用してトラフィックを識別し、ポリシー マップおよびサービス ポリシー エントリを使用してトラフィックをポリシングします。

注意　1 つのセンサーで複数のデバイスを管理できますが、1 つのデバイスに対して複数のセンサーは使用できません。そのような目的には、マスター ブロッキング センサーを使用する必要があります。

[Blocking Devices] ペインでデバイスを設定するためには、まずセンサーが管理する各デバイスにデバイス ログイン プロファイルを指定する必要があります。

[Blocking Devices] ペインのフィールド定義

[Blocking Devices] ペインには次のフィールドがあります。

- [IP Address]：ブロッキング デバイスの IP アドレス。
- [Sensor's NAT Address]：センサーの NAT アドレス。
- [Device Login Profile]：ブロッキング デバイスへのログインに使用するデバイス ログイン プロファイル。
- [Device Type]：デバイスのタイプ（[Cisco Router]、[Cat 6K]、[PIX/ASA]）。デフォルトは [Cisco Router] です。
- [Response Capabilities]：デバイスが、ブロッキング、レート制限、またはその両方を使用するかどうかを示します。
- [Communication]：ブロッキング デバイスへのログインに使用する通信メカニズム（[SSH 3DES] および [Telnet]）を示します。デフォルトは [SSH 3DES] です。

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

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

- [IP Address]：ブロッキング デバイスの IP アドレス。
- [Sensor's NAT Address]：センサーの NAT アドレス。
- [Device Login Profile]：ブロッキング デバイスへのログインに使用するデバイス ログイン プロファイル。
- [Device Type]：デバイスのタイプ（[Cisco Router]、[Cat 6K]、[PIX/ASA]）。デフォルトは [Cisco Router] です。
- [Response Capabilities]：デバイスが、ブロッキング、レート制限、またはその両方を使用するかどうかを示します。
- [Communication]：ブロッキング デバイスへのログインに使用する通信メカニズム（[SSH 3DES] および [Telnet]）を示します。デフォルトは [SSH 3DES] です。

ブロッキング デバイスおよびレート制限デバイスの追加、編集、削除

ブロッキング デバイスおよびレート制限デバイスを追加、編集、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* > [Blocking] > [Blocking Devices] を選択し、[Add] をクリックして、ブロッキング デバイスを追加します。デバイス ログイン プロファイルを設定していない場合は、エラー メッセージが表示されます。

ステップ 3　[IP Address] フィールドには、ブロッキング デバイスの IP アドレスを入力します。

ステップ 4　（任意）[Sensor's NAT Address] フィールドにセンサーの NAT アドレスを入力します。

ステップ 5　[Device Login Profile] ドロップダウン リストからデバイス ログイン プロファイルを選択します。

ステップ 6　[Device Type] ドロップダウン リストからデバイス タイプを選択します。

ステップ 7　[Response Capabilities] フィールドで、[Block] チェックボックスまたは [Rate Limit] チェックボックス（あるいは両方）をオンにし、デバイスがブロッキングとレート制限のどちらを実行するか、または両方を実行するかを指定します。

（注）　シグニチャがトリガーされたときに SensorApp がブロック要求またはレート制限要求を ARC に送信するように、特定のシグニチャに対してブロッキング アクションとレート制限アクションを選択する必要があります。

ステップ 8　[Communication] ドロップダウン リストから、次のいずれかの通信タイプを選択します。[SSH 3DES] を選択した場合は、ステップ 11 に進んでください。

ヒント　変更内容を破棄して [Add Blocking Device] 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。IP アドレスがすでに追加されている場合は、エラー メッセージが表示されます。新しいデバイスが [Blocking Devices] ペインのリストに表示されます。

ステップ 10　[SSH 3DES] を選択した場合は、デバイスを既知のホスト リストに追加する必要があります。

（注）　[SSH 3DES] を選択する場合は、ブロッキング デバイスが 3DES 暗号化をサポートする機能セットまたはライセンスを備えている必要があります。

（注）　[Configuration] > *sensor_name* > [Sensor Management] > [SSH] > [Known Host Keys] > [Add Known Host Key] を選択して、デバイスを既知のホスト リストに追加することもできます。

a.　センサーに Telnet 接続し、CLI にログインします。

b.　グローバル コンフィギュレーション モードを開始します。

```
sensor# configure terminal
```

c.　公開キーを入手します。

```
sensor(config)# ssh host-key blocking_device_ip_address
```

d.　公開キーを既知のホストのリストに追加することを確認するように求めるメッセージが表示されます。

```
Would you like to add this to the trusted certificate table for this host?[yes]:
```

e.　**yes** と入力します。

f.　グローバル コンフィギュレーション モードと CLI を終了します。

```
sensor(config)# exit
sensor# exit
```

ステップ 11　ブロッキング デバイス リストの既存のエントリを編集するには、そのエントリを選択し、[Edit] をクリックします。

ステップ 12　必要に応じて、センサーの NAT アドレスを編集します。

ステップ 13　必要に応じて、デバイス ログイン プロファイルを変更します。

ステップ 14　必要に応じて、デバイス タイプを変更します。

ステップ 15　必要に応じて、デバイスがブロッキングとレート制限のどちらを実行するかの設定を変更します。

ステップ 16　必要に応じて、通信タイプを変更します。

ヒント　変更内容を破棄して [Edit Blocking Device] 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。編集したブロッキング デバイスが [Blocking Device] ペインのリストに表示されます。

ステップ 18　リストからブロッキング デバイスを削除するには、そのデバイスを選択し、[Delete] をクリックします。そのデバイスは、[Blocking Device] ペインの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 19　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。

Router Blocking Device Interfaces の設定

ここでは、ルータ ブロッキング デバイス インターフェイスの設定方法について説明します。内容は次のとおりです。

[Router Blocking Device Interfaces] ペイン

（注）　ルータ ブロッキング デバイス インターフェイスを設定するには、管理者またはオペレータであることが必要です。

[Router Blocking Device Interfaces] ペインで、ルータにブロッキング インターフェイスまたはレート制限インターフェイスを設定し、ブロッキングまたはレート制限の対象とするトラフィックの方向を指定する必要があります。

ルータ ブロッキング デバイス インターフェイスの概要

（注）　Pre-Block ACL および Post-Block ACL はレート制限には適用されません。

Pre-Block ACL と Post-Block ACL は、ルータのコンフィギュレーション内に作成し、保存します。これらの ACL は名前付きまたは番号付きの拡張 IP ACL にする必要があります。ACL の作成の詳細については、ルータのマニュアルを参照してください。[Pre-Block ACL] と [Post-Block ACL] の各フィールドに、ルータにすでに設定されている ACL の名前を入力します。

Pre-Block ACL は、主にブロック対象外のものを許可するために使用されます。この ACL を使用してパケットがチェックされるとき、最初に一致する行によってアクションが決まります。最初に一致する行が Pre-Block ACL の許可の行である場合、ACL の後の方に（自動ブロックの）拒否の行があっても、そのパケットは許可されます。Pre-Block ACL は、ブロックによって生じる拒否の行よりも優先されます。

Post-Block ACL は、同じインターフェイスまたは方向に対して、追加的にブロッキングまたは許可を行う場合に最適です。センサーが管理するインターフェイスまたは方向に既存の ACL がある場合、その ACL を Post-Block ACL として使用できます。Post-Block ACL がない場合、センサーは新しい ACL の最後に **permit ip any any** を挿入します。

センサーが起動すると、2 つの ACL の内容が読み込まれます。そして、次のエントリを持った 3 つ目の ACL が作成されます。

- センサーの IP アドレスに対する **permit** 行
- Pre-Block ACL のすべての設定行のコピー
- センサーによってブロックされている各アドレスの **deny** 行
- Post-Block ACL のすべての設定行のコピー

センサーは新しい ACL を、指定したインターフェイスと方向に適用します。

（注）　新しい ACL がルータのインターフェイスまたは方向に適用されると、そのインターフェイスまたは方向に対する他の ACL が適用されなくなります。

センサーによるデバイスの管理方法

（注）　ACL はレート制限デバイスには適用されません。

ARC は、Cisco のルータやスイッチを管理する場合、それらのデバイス上の ACL を使用します。ACL は、次のように作成されます。

1. センサー IP アドレス、またはセンサーの NAT アドレス（指定されている場合）がある **permit** 行

   （注）　センサーのブロックを許可している場合、この行は ACL に含まれません。

2. Pre-Block ACL（指定されている場合）

   この ACL は、すでにデバイスに存在している必要があります。

（注）　ARC は、この ACL の行を読み取り、その行を ACL の先頭にコピーします。

3. アクティブなブロックがある場合、そのブロック
4. 次のいずれか
   - Post-Block ACL（指定されている場合）

     この ACL は、すでにデバイスに存在している必要があります。

     （注）　ARC は、この ACL の行を読み取り、その行を ACL の末尾にコピーします。

     （注）　一致しなかったすべてのパケットを許可する場合は、ACL の最後の行を必ず **permit ip any any** にしてください。

   - **permit ip any any**（Post-Block ACL を指定した場合は使用されません）

ARC は、デバイスの管理に 2 つの ACL を使用します。アクティブな ACL は一度に 1 つだけです。オフラインの ACL 名を使用して新しい ACL が作成され、それがインターフェイスに適用されます。次に、ARC は次のサイクルで逆のプロセスを実行します。

注意　ARC が作成する ACL が、ユーザやその他のシステムによって変更されることがあってはなりません。これらの ACL は一時的なものであり、新しい ACL がセンサーによって常に作成されています。Pre-Block ACL および Post-Block ACL に対してのみ、変更を加えることができます。

Pre-Block ACL または Post-Block ACL を修正する必要がある場合は、次の手順を実行します。

1. センサーでブロッキングをディセーブルにします。
2. デバイスの設定に変更を加えます。
3. センサーでブロッキングを再びイネーブルにします。

ブロッキングが再度イネーブルになると、センサーは新しいデバイス設定を読み取ります。

注意　1 つのセンサーで複数のデバイスを管理できますが、1 つのデバイスに対して複数のセンサーは使用できません。その場合は、マスター ブロッキング センサーを使用してください。

詳細情報

- ブロッキングをイネーブルにする手順については、「ブロッキング プロパティの設定」（P.15-10）を参照してください。
- センサーをマスター ブロッキング センサーとして設定する手順については、「マスター ブロッキング センサーの設定」（P.15-28）を参照してください。

[Router Blocking Device Interfaces] ペインのフィールド定義

[Router Blocking Device Interfaces] ペインには次のフィールドがあります。

- [Router Blocking Device]：ルータ ブロッキング デバイスまたはレート制限デバイスの IP アドレス。

- [Blocking Interface]：ルータ ブロッキング デバイスまたはレート制限デバイス上で使用するインターフェイス。有効な値は、a ～ z、A ～ Z、0 ～ 9、特殊文字の "." および "/" で構成される 1 ～ 64 文字の文字列です。
- [Direction]：ブロッキング ACL を適用する方向。有効な値は、[In] または [Out] です。
- [Pre-Block ACL]：ブロッキング ACL の前に適用する ACL。有効な値は 0 ～ 64 文字です。このフィールドはレート制限には適用されません。
- [Post-Block ACL]：ブロッキング ACL の後に適用する ACL。有効な値は 0 ～ 64 文字です。このフィールドはレート制限には適用されません。

（注）　Post-Block ACL を Pre-Block ACL と同じものにすることはできません。

[Add Router Blocking Device Interface] および [Edit Router Blocking Device Interface] ダイアログボックスのフィールド定義

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

- [Router Blocking Device]：ルータ ブロッキング デバイスまたはレート制限デバイスの IP アドレス。
- [Blocking Interface]：ルータ ブロッキング デバイスまたはレート制限デバイス上で使用するインターフェイス。有効な値は、a ～ z、A ～ Z、0 ～ 9、特殊文字の "." および "/" で構成される 1 ～ 64 文字の文字列です。
- [Direction]：ブロッキング ACL を適用する方向。有効な値は、[In] または [Out] です。
- [Pre-Block ACL]：ブロッキング ACL の前に適用する ACL。有効な値は 0 ～ 64 文字です。このフィールドはレート制限には適用されません。
- [Post-Block ACL]：ブロッキング ACL の後に適用する ACL。有効な値は 0 ～ 64 文字です。このフィールドはレート制限には適用されません。

（注）　Post-Block ACL を Pre-Block ACL と同じものにすることはできません。

ルータ ブロッキング デバイスおよびレート制限デバイスのインターフェイスの設定

ルータ ブロッキング デバイスおよびレート制限デバイスのインターフェイスを設定するには、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* > [Sensor Management] > [Blocking] > [Router Blocking Device Interfaces] を選択し、[Add] をクリックして、ルータ ブロッキング デバイスまたはレート制限デバイスのインターフェイスを追加します。

ステップ 3　[Router Blocking Device] ドロップダウン リストから、ルータ ブロッキング デバイスまたはレート制限デバイスの IP アドレスを選択します。

ステップ 4　[Blocking Interface] フィールドにブロッキング インターフェイスまたはレート制限インターフェイスの名前を入力します。

ステップ 5　[Direction] ドロップダウン リストから方向（[In] または [Out]）を選択します。

ステップ 6　（任意）[Pre-Block ACL] フィールドに Pre-Block ACL の名前を入力します。

（注）　この手順はレート制限デバイスには適用されません。

ステップ 7　（任意）[Post-Block ACL] フィールドに Post-Block ACL の名前を入力します。

（注）　この手順はレート制限デバイスには適用されません。

ヒント　変更を破棄して [Add Router Blocking Device Interface] 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] をクリックします。IP アドレス、インターフェイス、方向の組み合わせがすでに存在する場合は、エラー メッセージが表示されます。新しいインターフェイスが [Router Blocking Device Interfaces] ペインのリストに表示されます。

ステップ 9　ルータ ブロッキング デバイス インターフェイス リスト内の既存のエントリを編集するには、そのエントリを選択し、[Edit] をクリックします。

ステップ 10　必要に応じて、ブロッキング インターフェイスまたはレート制限インターフェイスの名前を編集します。

ステップ 11　必要に応じて、方向を変更します。

ステップ 12　必要に応じて、Pre-Block ACL の名前を編集します。

ステップ 13　必要に応じて、Post-Block ACL の名前を編集します。

ヒント　変更を破棄して [Edit Router Blocking Device Interface] 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 14　[OK] をクリックします。編集したブロッキング デバイス インターフェイスまたはレート制限デバイス インターフェイスは、[Router Blocking Device Interfaces] ペインのリストに表示されなくなります。

ステップ 15　リストからルータ ブロッキング デバイス インターフェイスまたはレート制限デバイス インターフェイスを削除するには、そのインターフェイスを選択し、[Delete] をクリックします。そのルータ ブロッキング デバイス インターフェイスまたはレート制限デバイス インターフェイスは、[Router Blocking Device Interfaces] ペインの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 16　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。

Cat 6K のブロッキング デバイス インターフェイスの設定

ここでは、Catalyst 6500 Series シリーズ インターフェイスの設定方法について説明します。内容は次のとおりです。

[Cat 6K Blocking Device Interfaces] ペイン

（注）　Catalyst 6500 シリーズ スイッチのブロッキング デバイス インターフェイスを設定するには、管理者またはオペレータであることが必要です。

[Cat 6K Blocking Device Interfaces] ペインで、ブロッキング Catalyst 6500 シリーズ スイッチの VLAN ID および VACL を指定します。

Cat 6K ブロッキング デバイス インターフェイスの概要

Cisco Catalyst ソフトウェアを実行している場合にはスイッチ自体にある VACL を使用し、Cisco IOS ソフトウェアを実行している場合には MSFC 上またはスイッチ自体にあるルータの ACL を使用して、ARC のブロッキングを設定できます。ここでは、VACL を使用したブロッキングについて説明します。VACL を使用するスイッチでレート制限を実行するように設定することはできません。Catalyst 6500 シリーズ スイッチ上でブロッキング インターフェイスを設定し、ブロックするトラフィックの VLAN を指定する必要があります。

Pre-Block VACL と Post-Block VACL は、スイッチ設定内に作成し、保存します。これらの VACL は名前付きまたは番号付きの拡張 IP VACL にする必要があります。VACL の作成の詳細については、スイッチのマニュアルを参照してください。[Pre-Block VACL] と [Post-Block VACL] の各フィールドに、スイッチにすでに設定されている VACL の名前を入力します。

Pre-Block VACL は、主としてセンサーによってブロックしない対象を許可する場合に使用します。パケットが VACL に対してチェックされると、最初に一致した行によってアクションが決定されます。最初の行が Pre-Block VACL の permit 行と一致する場合、VACL の後の方に（自動ブロックからの）deny 行がある場合でも、パケットは許可されます。Pre-Block VACL では、ブロックの結果の deny 行をオーバーライドできます。

Post-Block VACL は、同じ VACL に対して追加的にブロッキングまたは許可を行う場合に最適です。センサーが管理する VLAN に既存の VACL がある場合、その VACL を Post-Block VACL として使用できます。Post-Block V ACL がない場合、センサーは新しい VACL の最後に **permit ip any any** を挿入します。

（注）　IDSM-2 は新しい VACL の末尾に **permit ip any any capture** を挿入します。

センサーが起動すると、2 つの VACL の内容を読み取ります。センサーは次のエントリから成る 3 つ目の VACL を作成します。

- センサーの IP アドレスに対する **permit** 行
- Pre-Block VACL のすべての設定行のコピー
- センサーによってブロックされている各アドレスの **deny** 行
- Post-Block VACL のすべての設定行のコピー

センサーは新しい VACL を指定された VLAN に適用します。

（注）　新しい VACL がスイッチの VLAN に適用されると、その VLAN に対する他の VACL の適用は無効になります。

詳細情報

ルータ ACL を使用したブロッキングについては、「ルータ ブロッキング デバイスおよびレート制限デバイスのインターフェイスの設定」（P.15-21）を参照してください。

[Cat 6K Blocking Device Interfaces] ペインのフィールド定義

[Cat 6K Blocking Device Interfaces] ペインには次のフィールドがあります。

- [Cat 6K Blocking Device] : Catalyst 6500 シリーズ スイッチ ブロッキング デバイスの IP アドレス。
- [VLAN ID] : Catalyst 6500 シリーズ スイッチ ブロッキング デバイスで使用する VLAN ID。値は 1 ～ 4094 です。
- [Pre-Block VACL] : ブロッキング VACL の前に適用する VACL。値は 0 ～ 64 文字です。
- [Post-Block VACL] : ブロッキング VACL の後に適用する VACL。値は 0 ～ 64 文字です。

（注）　Post-Block VACL を Pre-Block VACL と同じものにすることはできません。

[Add Cat 6K Blocking Device Interface] および [Edit Cat 6K Blocking Device Interface] ダイアログボックスのフィールド定義

[Add Cat 6K Blocking Device Interface] および [Edit Cat 6K Blocking Device Interface] ダイアログボックスには次のフィールドがあります。

- [Cat 6K Blocking Device] : Catalyst 6500 シリーズ スイッチ ブロッキング デバイスの IP アドレス。
- [VLAN ID] : Catalyst 6500 シリーズ スイッチ ブロッキング デバイスで使用する VLAN ID。値は 1 ～ 4094 です。
- [Pre-Block VACL] : ブロッキング VACL の前に適用する VACL。値は 0 ～ 64 文字です。
- [Post-Block VACL] : ブロッキング VACL の後に適用する VACL。値は 0 ～ 64 文字です。

（注）　Post-Block VACL を Pre-Block VACL と同じものにすることはできません。

Cat 6K のブロッキング デバイス インターフェイスの設定

Catalyst 6500 シリーズ スイッチ ブロッキング デバイス インターフェイスを設定するには、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* > [Sensor Management] > [Blocking] > [Cat 6K Blocking Device Interfaces] を選択し、[Add] をクリックして、Catalyst 6500 シリーズ スイッチ ブロッキング デバイス インターフェイスを追加します。

ステップ 3　[Cat 6K Blocking Device] ドロップダウン リストから、Catalyst 6500 シリーズ スイッチの IP アドレスを選択します。

ステップ 4　[VLAN ID] フィールドに VLAN ID を入力します。

ステップ 5　（任意）[Pre-Block VACL] フィールドに Pre-Block VACL の名前を入力します。

ステップ 6　（任意）[Post-Block VACL] フィールドに Post-Block VACL の名前を入力します。

ヒント　変更を破棄して [Add Cat 6K Blocking Device Interface] 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。IP アドレスと VLAN の組み合わせがすでに存在している場合は、エラー メッセージが表示されます。新しいインターフェイスが [Cat 6K Blocking Device Interfaces] ペインのリストに表示されます。

ステップ 8　Catalyst 6500 シリーズ スイッチ ブロッキング デバイス インターフェイス リストの既存のエントリを編集するには、そのエントリを選択し、[Edit] をクリックします。

ステップ 9　必要に応じて、VLAN ID を編集します。

ステップ 10　必要に応じて、Pre-Block VACL の名前を編集します。

ステップ 11　必要に応じて、Post-Block VACL の名前を編集します。

ヒント　変更を破棄して [Edit Cat 6K Blocking Device Interface] 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 12　[OK] をクリックします。編集した Catalyst 6500 シリーズ スイッチ ブロッキング デバイス インターフェイスが [Cat 6K Blocking Device Interfaces] ペインのリストに表示されます。

ステップ 13　リストから Catalyst 6500 シリーズ スイッチ ブロッキング デバイス インターフェイスを削除するには、そのインターフェイスを選択し、[Delete] をクリックします。その Catalyst 6500 シリーズ スイッチ ブロッキング デバイス インターフェイスは、[Cat 6K Blocking Device Interfaces] ペインの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 14　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。

マスター ブロッキング センサーの設定

ここでは、マスター ブロッキング センサ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。

[Master Blocking Sensor] ペイン

（注）　マスター ブロッキング センサーを設定するには、管理者またはオペレータであることが必要です。

[Master Blocking Sensor] ペインで、ブロッキング デバイスの設定に使用するマスター ブロッキング センサーを指定します。

マスター ブロッキング センサーについて

複数のセンサー（ブロッキング転送センサー）が、1 つ以上のデバイスを制御する、指定したマスター ブロッキング センサーに、ブロッキング要求を転送できます。マスター ブロッキング センサーは、他の 1 つ以上のセンサーに代わって 1 つ以上のデバイスでブロッキングを制御するセンサーで実行されている ARC です。マスター ブロッキング センサー上の ARC は、他のセンサーで実行されている ARC の要求に応じて、デバイスのブロッキングを制御します。マスター ブロッキング センサーは、レート制限を転送することもできます。

注意　2 つのセンサーが同じデバイスでブロッキングまたはレート制限を制御することはできません。この状況が必要な場合は、一方のセンサーをマスター ブロッキング センサーとして設定してデバイスを管理し、もう一方のセンサーでマスター ブロッキング センサーに要求を転送できます。

マスター ブロッキング センサーを追加する場合は、センサーあたりのブロッキング デバイス数を減らします。たとえば、それぞれ 1 つのブロッキング インターフェイス / 方向を持つ 10 個のファイア ウォールと 10 台のルータでブロックする場合は、センサーに 10 個を割り当て、マスター ブロッキング センサーに残りの 10 個を割り当てることができます。

ブロッキング転送センサーで、マスター ブロッキング センサーとして機能するリモート ホストを識別します。マスター ブロッキング センサーでは、ブロッキング転送センサーをアクセス リストに追加する必要があります。

マスター ブロッキング センサーが Web 接続に TLS を必要とする場合は、マスター ブロッキング センサー リモート ホストの X.509 証明書を受け入れるようにブロッキング転送センサーの ARC を設定する必要があります。センサーでは TLS がデフォルトでイネーブルになりますが、このオプションは変更できます。

（注）　通常、マスター ブロッキング センサーはネットワーク デバイスを管理するように設定します。ブロッキング転送センサーは、通常は他のネットワーク デバイスを管理するようには設定されていませんが、これを行うことは可能です。

ブロッキングやレート制限用に設定されたデバイスが存在しない場合でも、ブロッキングまたはレート制限を実行するように設定されたセンサーは、ブロッキング要求またはレート制限要求をマスター ブロッキング センサーに転送できます。ブロッキングまたはレート制限要求がイベント アクションとして設定されているシグニチャが起動した場合、センサーはブロック要求またはレート制限要求をマスター ブロッキング センサーに転送し、そのセンサーがブロックまたはレート制限を実行します。

注意　1 つのセンサーだけがデバイス上のすべてのブロッキング インターフェイスを制御する必要があります。

[Master Blocking Sensor] ペインのフィールド定義

[Master Blocking Sensor] ペインには次のフィールドがあります。

- [IP Address] : マスター ブロッキング センサーの IP アドレス。
- [Port] : マスター ブロッキング センサーへの接続に使用するポート。デフォルトは 443 です。
- [Username] : マスター ブロッキング センサーへのログインに使用するユーザ名。ユーザ名は、^[A-Za-z0-9()+:,_/-]+$ の形式で入力します。ユーザ名は、文字または数字で始まり、A ～ Z（大文字または小文字）、0 ～ 9 の数字、「-」および「_」を含み、長さが 1 ～ 64 文字であることが必要です。
- [TLS Used] : TLS を使用するかどうか。

[Add Master Blocking Sensor] および [Edit Master Blocking Sensor] ダイアログボックスのフィールド定義

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

- [IP Address] : マスター ブロッキング センサーの IP アドレス。すでに存在する IP アドレスを入力すると、警告が表示されます。
- [Port (optional)] : マスター ブロッキング センサーへの接続に使用するポート。デフォルトは 443 です。
- [Username] : マスター ブロッキング センサーへのログインに使用するユーザ名。ユーザ名は、^[A-Za-z0-9()+:,_/-]+$ の形式で入力します。ユーザ名は、文字または数字で始まり、A ～ Z（大文字または小文字）、0 ～ 9 の数字、「-」および「_」を含み、長さが 1 ～ 64 文字であることが必要です。
- [Change the password] : パスワードを変更するかどうか。
- [New Password] : マスター ブロッキング センサーへのログインに使用するログイン パスワード。
- [Confirm Password] : 確認のためにログイン パスワードを再入力します。
- [Use TLS] : TLS を使用するかどうか。

マスター ブロッキング センサーの設定

マスター ブロッキング センサーを設定するには、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* > [Sensor Management] > [Blocking] > [Master Blocking Sensor] を選択し、[Add] をクリックして、マスター ブロッキング センサーを追加します。

ステップ 3　[IP Address] フィールドには、マスター ブロッキング センサーの IP アドレスを入力します。

ステップ 4　（任意）[Port] フィールドにポート番号を入力します。デフォルトは 443 です。

ステップ 5　[Username] フィールドにユーザ名を入力します。

ステップ 6　[New Password] フィールドに、ユーザのパスワードを入力します。

ステップ 7　確認のために [Confirm New Password] フィールドにもう一度パスワードを入力します。

ステップ 8　[TLS] チェックボックスをオンにします。

ヒント　変更内容を破棄して [Add Master Blocking Sensor] 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。IP アドレスがすでに追加されている場合は、エラー メッセージが表示されます。新しいマスター ブロッキング センサーが [Master Blocking Sensor] ペインのリストに表示されます。

ステップ 10　TLS を選択した場合は、マスター ブロッキング センサー リモート ホストの TLS/SSL X.509 証明書を受け入れるようにブロッキング転送センサーの ARC を設定する必要があります。

（注）　[Configuration] > *sensor_name* > [Sensor Management] > [Certificates] > [Trusted Hosts] > [Add Trusted Host] を選択して、X.509 証明書を受け入れるようにブロッキング転送センサーを設定することもできます。

a.　管理者権限を持つアカウントを使用してブロッキング転送センサーの CLI にログインします。

b.　グローバル コンフィギュレーション モードを開始します。

```
sensor# configure terminal
```

c.　信頼できるホストを追加します。

```
sensor(config)# tls trusted-host ip-address master_blocking_sensor_ip_address
```

信頼できるホストの追加を確認するように求めるメッセージが表示されます。

```
Would you like to add this to the trusted certificate table for this host?[yes]:
```

d.　**yes** と入力してホストを追加します。

e.　グローバル コンフィギュレーション モードと CLI を終了します。

```
sensor(config)# exit
sensor# exit
```

（注） 証明書のフィンガープリントに基づいて証明書を受け入れるように要求されます。センサーが提供するのは、自己署名証明書（認識された認証局の署名がある証明書ではなく）だけです。ホスト センサーにログインし、**show tls fingerprint** コマンドを入力して、ホスト証明書のフィンガープリントが一致することを確認することによって、マスター ブロッキング センサーのホスト センサー証明書を検証できます。

ステップ 11　マスター ブロッキング センサー リストの既存のエントリを編集するには、そのエントリを選択し、[Edit] をクリックします。

ステップ 12　（任意）ポートを編集します。

ステップ 13　必要に応じて、ユーザ名を編集します。

ステップ 14　このユーザのパスワードを変更するには、[Change the password] チェックボックスをオンにします。

a.　[New Password] フィールドに新しいパスワードを入力します。

b.　確認のために [Confirm New Password] フィールドに新しいパスワードをもう一度入力します。

ステップ 15　必要に応じて、[TLS] チェックボックスをオンまたはオフにします。

ヒント　変更内容を破棄して [Edit Master Blocking Sensor] 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。編集したマスター ブロッキング センサーが [Master Blocking Sensor] ペインのリストに表示されます。

ステップ 17　リストからマスター ブロッキング センサーを削除するには、そのマスター ブロッキング センサーを選択し、[Delete] をクリックします。そのマスター ブロッキング センサーは、[Master Blocking Sensor] ペインの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 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。

CHAPTER 16

SNMP の設定

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

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

この章では、センサーが SNMP および SNMP トラップを使用するように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。

SNMP の概要

注意 センサーが SNMP トラップを送信するようにするには、シグニチャの設定時にイベント アクションとして [Request SNMP Trap] も選択する必要があります。

SNMP は、ネットワーク デバイス間での管理情報の交換を容易にするアプリケーション層プロトコルです。SNMP を使用すると、ネットワーク管理者は、ネットワークのパフォーマンスを管理し、ネットワークの問題を検出および解決し、ネットワークの拡大に対する計画を策定できます。

SNMP は単純な要求/応答プロトコルです。ネットワーク管理システムが要求を発行し、管理対象デバイスが応答を返します。この動作は、Get、GetNext、Set、および Trap の 4 つのプロトコル操作のいずれかを使用することによって実装されます。

SNMP によるモニタリングのためにセンサーを設定することができます。SNMP は、ネットワーク管理ステーションがスイッチ、ルータ、センサーなどの多くのタイプのデバイスのヘルスとステータスをモニタするための標準的な方法を定義します。

SNMP トラップを送信するようにセンサーを設定できます。SNMP トラップを使用すると、エージェントは非送信請求 SNMP メッセージを使用して管理ステーションに重要なイベントを通知できます。

トラップで指示される通知には次の利点があります。マネージャが多数のデバイスを管理する必要があり、各デバイスに多数のオブジェクトがある場合に、すべてのデバイスのすべてのオブジェクトに情報をポーリングまたは要求することは非現実的です。ソリューションは、送信要求を行わずに、管理対象デバイス上のエージェントごとにマネージャに通知することです。イベントのトラップと呼ばれるメッセージを送信することで、この処理を行います。

イベントの受信後、マネージャはイベントを表示し、イベントに基づいてアクションを実行できます。たとえば、マネージャは、エージェントを直接ポーリングするか、他の関連デバイス エージェントをポーリングしてイベントの詳細情報を取得できます。

（注）　トラップで指示された通知は、重要でない SNMP 要求を排除することによって、ネットワークおよびエージェントのリソースを実質的に節約できます。ただし、SNMP ポーリングを完全には排除できません。SNMP 要求は、検出とトポロジ変更に必要です。また、管理対象デバイス エージェントは、デバイスに致命的な停止が生じた場合にはトラップを送信できません。

詳細情報

センサーに SNMP トラップを送信させる手順については、「シグニチャへのアクションの割り当て」（P.9-19）を参照してください。

SNMP の一般設定の設定

ここでは、SNMP の設定方法について説明します。内容は次のとおりです。

[SNMP General Configuration] ペイン

（注）　SNMP を使用するようにセンサーを設定するには、管理者である必要があります。

SNMP を使用するようにセンサーを設定するには、[General Configuration] ペインを使用します。

[SNMP General Configuration] ペインのフィールド定義

[SNMP General Configuration] ペインには、次のフィールドが表示されます。

- [Enable SNMP Gets/Sets]：このフィールドがオンの場合、SNMP get および SNMP set が許可されます。
- [SNMP Agent Parameters]：SNMP エージェントのパラメータを設定します。
  - [Read-Only Community String]：読み取り専用アクセスのコミュニティ ストリングを示します。
  - [Read-Write Community String]：読み取りと書き込みアクセスのコミュニティ ストリングを示します。
  - [Sensor Contact]：センサーの問い合せ先担当者、問い合せ先、またはその両方を示します。

- [Sensor Location]：センサーの場所を示します。
- [Sensor Agent Port]：センサーの IP ポートを示します。デフォルトは 161 です。
- [Sensor Agent Protocol]：センサーの IP プロトコルを示します。デフォルトは UDP です。

SNMP の一般パラメータの設定

一般的な SNMP 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* > [Sensor Management] > [SNMP] > [General Configuration] を選択します。

ステップ 3　SNMP 管理ワークステーションがセンサー SNMP エージェントに要求を発行できるように、[Enable SNMP Gets/Sets] チェックボックスをオンにして SNMP をイネーブルにします。

ステップ 4　SNMP エージェント パラメータを設定します。SNMP 管理ワークステーションがセンサー SNMP エージェントに対して要求できる値があります。

a. [Read-Only Community String] フィールドに、読み取り専用コミュニティ ストリングを入力します。読み取り専用コミュニティ ストリングは、センサー SNMP エージェントの識別に役立ちます。

b. [Read-Write Community String] フィールドに、読み取り / 書き込みコミュニティ ストリングを入力します。読み取り / 書き込みコミュニティ ストリングは、センサー SNMP エージェントの識別に役立ちます。

（注） 管理ワークステーションは SNMP 要求を、センサーに常駐するセンサー SNMP エージェントに送信します。管理ワークステーションから発行された要求において、コミュニティ ストリングがセンサー上の内容と一致しない場合、センサーによって要求が拒否されます。

c. [Sensor Contact] フィールドにセンサーの問い合せ先のユーザ ID を入力します。

d. [Sensor Location] フィールドにセンサーの場所を入力します。

e. [Sensor Agent Port] フィールドにセンサー SNMP エージェントのポートを入力します デフォルトの SNMP ポート番号は 161 です。

f. [Sensor Agent Protocol] ドロップダウン リストから、センサー SNMP エージェントが使用するプロトコルを選択します。デフォルト プロトコルは UDP です。

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。

SNMP トラップの設定

ここでは、SNMP トラップの設定方法について説明します。内容は次のとおりです。

- 「[Add SNMP Trap Destination]/[Edit SNMP Trap Destination] ダイアログボックスのフィールド定義」（P.16-4）
- 「SNMP トラップの設定」（P.16-5）

[Traps Configuration] ペイン

（注）　センサー上に SNMP トラップを設定するには、管理者である必要があります。

SNMP トラップとセンサーのトラップ宛先をセットアップするには、[Traps Configuration] ペインを使用します。SNMP トラップは通知です。イベントが fatal、error、または warning のいずれかであるかに基づいて、センサーがトラップを送信するように設定します。

[SNMP Traps Configuration] ペインのフィールド定義

[SNMP Traps Configuration] ペインには、次のフィールドが表示されます。

- [Enable SNMP Traps]：このフィールドがオンの場合、プル アップデートを使用するようにリモート サーバに指示します。
- [SNMP Traps]：SNMP を使用して通知するエラー イベントを選択します。
  - [Fatal]：すべての fatal エラー イベントについてトラップを生成します。
  - [Error]：すべての error エラー イベントについてトラップを生成します。
  - [Warning]：すべての warning エラー イベントについてトラップを生成します。
- [Enable detailed traps for alerts]：このフィールドがオンの場合、トラップにアラートの全テキストが含まれます。選択しない場合は、スパース モードが使用されます。スパース モードでは、484 バイト未満のアラートのテキストが含まれます。
- [Default Trap Community String]：トラップに特定のストリングが設定されていない場合に使用するコミュニティ ストリング。
- [SNMP Trap Destinations]：トラップの宛先を示します。宛先について次の情報を指定する必要があります。
  - [IP Address]：トラップ宛先の IP アドレス。
  - [UDP Port]：トラップ宛先の UDP ポート。
  - [Trap Community String]：トラップ コミュニティ ストリング。

[Add SNMP Trap Destination]/[Edit SNMP Trap Destination] ダイアログボックスのフィールド定義

[Add SNMP Trap Destination]/[Edit SNMP Trap Destination] ダイアログボックスには、次のフィールドが表示されます。

- [IP Address]：トラップ宛先の IP アドレス。
- [UDP Port]：トラップ宛先の UDP ポート。デフォルトはポート 162 です。
- [Trap Community String]：トラップ コミュニティ ストリング。

SNMP トラップの設定

SNMP トラップを設定するには、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* > [Sensor Management] > [SNMP] > [Traps Configuration] を選択します。

ステップ 3　[Enable SNMP Traps] チェックボックスをオンにして、SNMP トラップをイネーブルにします。

ステップ 4　SNMP トラップのパラメータを設定します。

a. SNMP トラップを使用して通知するエラー イベントを選択します。センサーが、fatal、error、warning のエラー イベントのいずれかに基づいて SNMP トラップを送信するか、またはすべてに基づいて SNMP トラップを送信するかを選択できます。

b. 詳細な SNMP トラップが必要な場合は、[Enable detailed traps for alerts] チェックボックスをオンにします。

c. [Default Trap Community String] フィールドに、詳細なトラップに含めるコミュニティ ストリングを入力します。

ステップ 5　どの管理ワークステーションに送信するかをセンサーに知らせるため、SNMP トラップ宛先のパラメータを設定します。

a. [Add] をクリックします。

b. [IP Address] フィールドに SNMP 管理ステーションの IP アドレスを入力します。

c. [UDP Port] フィールドに SNMP 管理ステーションの UDP ポートを入力します。

d. [Trap Community String] フィールドにトラップ コミュニティ ストリングを入力します。

（注）　コミュニティ ストリングがトラップに表示されます。これは、複数のエージェントから複数のタイプのトラップを受信する場合に役立ちます。たとえば、ルータまたはセンサーがトラップを送信する場合に、具体的にルータまたはセンサーを識別する何かをコミュニティ ストリングに入力すると、コミュニティ ストリングに基づいてトラップをフィルタリングすることができます。

ヒント　変更を破棄して [Add SNMP Trap Destination] 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。[Traps Configuration] ペインのリストに新しい SNMP トラップ宛先が表示されます。

ステップ 7　SNMP トラップ宛先を編集するには、その SNMP トラップ宛先を選択して [Edit] をクリックします。

ステップ 8　必要に応じて [UDP Port] フィールドおよび [Trap Community String] フィールドを編集します。

ヒント　変更を破棄して [Edit SNMP Trap Destination] 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。[Traps Configuration] ペインのリストに編集した SNMP トラップ宛先が表示されます。

ステップ 10　SNMP トラップ宛先を削除するには、その SNMP トラップ宛先を選択して [Delete] をクリックします。削除された SNMP トラップ宛先は、[Traps Configuration] ペインの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。

サポート対象 MIB

センサーでは次の専用 MIB がサポートされています。

- CISCO-CIDS-MIB
- CISCO-PROCESS-MIB
- CISCO-ENHANCED-MEMPOOL-MIB
- CISCO-ENTITY-ALARM-MIB

（注）　MIB II はセンサーで使用できますが、サポート対象外です。一部の要素が正しくないことが認識されています（検知インターフェイスでの IF MIB からのパケット カウントなど）。MIB II の要素を使用することはできますが、これらすべてが正確な情報を提供することは保証できません。他に掲載されている MIB は完全にサポートされ、出力も正確です。

これらのシスコの専用 MIB は、次の URL から SNMP v2 の見出しの下で取得できます。

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

CHAPTER 17

外部製品インターフェイスの設定

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

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

この章では、外部製品インターフェイスの設定方法について説明します。内容は次のとおりです。

外部製品インターフェイスについて

外部製品インターフェイスは、外部のセキュリティおよび管理製品から情報を受信して処理することを目的としています。これらの外部セキュリティおよび管理製品は、センサー設定情報を自動的に拡張するために使用できる情報を収集します。外部製品から受信できる情報の種類には、ホスト プロファイル（ホスト OS 設定、アプリケーション設定、およびセキュリティ態勢）、悪意のあるネットワーク アクティビティの原因であると認識された IP アドレスなどがあります。

（注） Cisco IPS で追加できるのは、CSA MC のインターフェイスだけです。

CSA MC について

CSA MC は、ネットワーク ホストにセキュリティ ポリシーを適用します。これには 2 つのコンポーネントがあります。

- ネットワーク ホスト上に存在し、そのホストを保護するエージェント。

- 管理コンソール（MC）：エージェントを管理するアプリケーション。セキュリティ ポリシーの更新をエージェントにダウンロードし、エージェントから操作情報をアップロードします。

CSA MC は、管理する CSA エージェントからホスト ポスチャ情報を受信します。また、ネットワークから隔離する必要があると判断した IP アドレスのウォッチ リストも維持します。CSA MC は、ホスト ポスチャ イベントと隔離 IP アドレス イベントという 2 種類のイベントをセンサーに送信します。

ホスト ポスチャ イベント（IPS ではインポートされた OS 識別名と呼ばれる）には、次の情報が含まれます。

- CSA MC によって割り当てられた一意のホスト ID
- CSA エージェント ステータス
- ホスト システムのホスト名
- ホスト上でイネーブルになっている IP アドレスのセット
- CSA ソフトウェア バージョン
- CSA ポーリング ステータス
- CSA テスト モード ステータス
- NAC ポスチャ

たとえば、OS 固有のシグニチャが起動し、ターゲットがその OS を実行している場合、攻撃の関連性は高く、応答の重大度が増します。ターゲットの OS が異なる場合、攻撃の関連性は低く、応答の重大度は低下する可能性があります。OS が異なるホストのシグニチャ攻撃関連性レーティングは、調整されます。

隔離ホスト イベント（IPS ではウォッチ リストと呼ばれる）には、次の情報が含まれます。

- IP アドレス
- 隔離の理由
- 規則違反に関連付けられたプロトコル（TCP、UDP、または ICMP）
- 規則違反が、確立されたセッションと UDP パケットのどちらに関連付けられているかを示すインジケータ

たとえば、ホストのいずれかを攻撃者として表示するシグニチャが起動された場合は、きわめて重大であると見なされます。このホストでは、リスク レーティングが高くなります。レーティング上昇の度合いは、ホストが隔離対象となった理由によって異なります。

センサーは、これらのイベントからの情報を使用し、イベントの情報とホスト ポスチャおよび隔離 IP アドレスのリスク レーティング設定に基づいてリスク レーティングをどこまで引き上げるかを決定します。

（注） ホスト ポスチャとウォッチ リスト IP アドレス情報は、仮想センサーには関連付けられず、グローバル情報として扱われます。

CSA MC と IPS センサー間の安全な通信は SSL/TLS によって維持されます。センサーは、CSA MC を使用して SSL/TLS 通信を開始します。この通信は相互に認証されます。CSA MC は、認証のために X.509 証明書を提供します。センサーは、ユーザ名 / パスワード認証を使用します。

（注） イネーブルにできるのは 2 つの CSA MC インターフェイスだけです。

注意　センサーとの通信が可能となるように、CSA MC を信頼できるホストとして追加する必要があります。CSA MC を信頼できるホストとして追加するには、[Configuration] > *sensor_name* > [Sensor Management] > [Certificates] > [Trusted Hosts] > [Add] を選択します。

詳細情報

信頼できるホストを追加する手順については、「信頼できるホストの追加」（P.14-10）を参照してください。

外部製品インターフェイスの問題

外部製品インターフェイスがホスト ポスチャと隔離イベントを受信すると、次の問題が発生することがあります。

- センサーは、特定の数のホスト レコードしか格納できません。
  - レコード数が 10,000 を超えると、その後のレコードはドロップされます。
  - 10,000 の上限に達すると、9900 を下回るまでドロップされ、新しいレコードがドロップされなくなります。
- ホストは IP アドレスを変更できるか、別のホスト IP アドレスを使用しているように見えます。これは、DHCP のリース有効期限切れやワイヤレス ネットワークでの移動によって発生します。IP アドレスが競合する場合、センサーは最新のホスト ポスチャ イベントを最も正確であると見なします。
- ネットワークには、異なる VLAN のオーバーラップする IP アドレス範囲が含まれていることがありますが、ホスト ポスチャには VLAN ID 情報は含まれません。特定のアドレス範囲を無視するようにセンサーを設定できます。
- CSA MC はファイアウォールの内側にあるため、ホストに到達不能となることがあります。到達不能のホストは除外できます。
- CSA MC イベント サーバでは、デフォルトで開いたサブスクリプションを最大 10 まで使用できます。この値を変更できます。サブスクリプションを開くには、管理者アカウントとパスワードが必要です。
- CSA データは仮想化されません。センサーによってグローバルに処理されます。
- ホスト ポスチャ OS と IP アドレスは、パッシブ OS フィンガープリント ストレージに統合されます。これらは、インポートされた OS プロファイルとして表示できます。
- 隔離されたホストは表示できません。
- センサーは、各 CSA MC ホスト X.509 証明書を認識する必要があります。これらを信頼できるホストとして追加する必要があります。
- 最大 2 つの外部製品デバイスを設定できます。

詳細情報

- OS マップおよび識別の操作の詳細については、「設定された OS マップの追加、編集、削除、および移動」（P.11-29）と「OS ID の設定」（P.19-26）を参照してください。
- 信頼できるホストの追加手順については、「信頼できるホストの追加」（P.14-10）を参照してください。

CSA MC での IPS インターフェイス サポートの設定

（注）　ホスト ポスチャ イベントと隔離 IP アドレス イベントの詳細については、『*Using Management Center for Cisco Security Agents 5.1*』を参照してください。

ホスト ポスチャ イベントと隔離 IP アドレス イベントをセンサーに送信するように CSA MC を設定する必要があります。

IPS インターフェイスをサポートするように CSA MC を設定するには、次の手順を実行します。

ステップ 1　[Events] > [Status Summary] を選択します。

ステップ 2　[Network Status] セクションで、[Host history collection enabled] の横にある [No] をクリックし、ポップアップ ウィンドウで [Enable] をクリックします。

（注）　ホスト履歴収集がシステムでグローバルにイネーブルになります。この機能をオンにすると MC ログ ファイルがすぐに一杯になる可能性があるため、デフォルトではディセーブルになっています。

ステップ 3　[Systems] > [Groups] を選択し、次に作成する管理者アカウントとともに使用する新しいグループ（ホストなし）を作成します。

ステップ 4　[Maintenance] > [Administrators] > [Account Management] を選択して、MC システムへの IPS アクセスを提供する新しい CSA MC 管理者アカウントを作成します。

ステップ 5　ロールが **Monitor** である新しい管理者アカウントを作成します。この新しいアカウントに設定特権を許可しないことにより、MC のセキュリティを維持できます。センサーに外部製品インターフェイスを設定するときに必要になるため、この管理者アカウントのユーザ名とパスワードを記録しておいてください。

ステップ 6　この管理者アカウントをさらに制限するには、[Maintenance] > [Administrators] > [Access Control] を選択します。

ステップ 7　[Access Control] ウィンドウで、先ほど作成した管理者とグループを選択します。

（注）　この設定を保存すると、この新しい管理者アカウントの MC アクセスがさらに制限され、CSA MC のセキュリティが維持されます。

外部製品インターフェイスの設定

ここでは、[External Product Interfaces] ペインについて説明します。内容は次のとおりです。

[External Product Interfaces] ペイン

（注） 外部製品インターフェイスおよびポスチャ ACL を追加、編集、および削除するためには、管理者であることが必要です。

CSA MC のインターフェイスを追加し、センサーが CSA MC から情報を受信して処理できるようにするには、[External Product Interfaces] ペインを使用します。

注意 センサーとの通信が可能となるように、外部製品を信頼できるホストとして追加する必要があります。信頼できるホストを追加するには、[Configuration] > *sensor_name* > [Sensor Management] > [Certificates] > [Trusted Hosts] > [Add] を選択します。

[External Product Interfaces] ペインのフィールド定義

[External Product Interfaces] ペインには次のフィールドがあります。

- [IP Address]：外部製品の IP アドレス。
- [Enabled]：外部製品がイネーブルかどうかを示します。
- [Port]：通信に使用されるポートを指定します。
- [TLS Used]：安全な通信が使用されるかどうかを示します。
- [Username]：CSA MC に接続するユーザ ログイン名を示します。
- [Host Posture Settings]：CSA MC から受信したホスト ポスチャの処理方法を示します。
  - [Enabled]：ホスト ポスチャの受信がイネーブルになっていることを示します。ディセーブルである場合、CSA MC から受信したホスト ポスチャ情報は削除されます。
  - [Allow Unreachable]：CSA MC から到達不能なホストのホスト ポスチャ情報の受信を許可/拒否します。

    CSA MC がホスト ポスチャに含まれるどの IP アドレスを使用してもホストとの接続を確立できない場合、そのホストは到達不能です。このオプションは、IPS が認識できない可能性のある IP アドレスやネットワーク内で重複している可能性のある IP アドレスを持つポスチャのフィルタリングに役立ちます。このフィルタは、CSA MC から到達不能なホストに IPS からも到達できないようなネットワーク トポロジに最も適しています。たとえば、IPS と CSA MC が同じネットワーク セグメントにある場合などです。

  - [Posture ACLs]：ホスト ポスチャを許可または拒否するネットワーク アドレス範囲を指定します。このオプションによって、IPS が認識できない可能性のある IP アドレスやネットワーク内で重複している可能性のある IP アドレスを持つポスチャをフィルタリングできます。
- [Watch List Settings]：CSA MC から受信したウォッチ リスト設定の処理方法を示します。
  - [Enabled]：ウォッチ リストの受信がイネーブルになっていることを示します。ディセーブルである場合、CSA MC から受信したウォッチ リスト情報は削除されます。
  - [Manual RR Increase]：手動ウォッチ リストのリスク レーティングの加算率を示します。
  - [Session RR Increase]：セッションベース ウォッチ リストのリスク レーティングの加算率を示します。
  - [Packet RR Increase]：パケットベース ウォッチ リストのリスク レーティングの加算率を示します。
- [SDEE URL]：IPS が SDEE 通信を使用して情報を取得するために使用する CSA MC 上の URL。この URL は、IPS が通信する CSA MC のソフトウェア バージョンに基づいて設定する必要があります。CSA MC バージョン 5.0 の場合は /csamc50/sdee-server、CSA MC バージョン 5.1 の場合は /csamc51/sdee-server、CSA MC バージョン 5.2 以降の場合は /csamc/sdee-server（これがデフォルト値）となります。

[Add External Product Interface] および [Edit External Product Interface] ダイアログボックスのフィールド定義

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

- [External Product's IP Address]：外部製品の IP アドレス。
- [Enable receipt of information]：センサーによる外部製品インターフェイスからの情報受信をイネーブルにします。

（注） このオプションをオンにしない場合、このデバイスから受信したホスト ポスチャおよび隔離の情報はすべてセンサーから削除されます。

- [Communication Settings]：SDEE URL および TLS を表示し、ポートを変更できます。
  - [SDEE URL]：IPS が SDEE 通信を使用して情報を取得するために使用する CSA MC 上の URL。この URL は、IPS が通信する CSA MC のソフトウェア バージョンに基づいて設定する必要があります。CSA MC バージョン 5.0 の場合は /csamc50/sdee-server、CSA MC バージョン 5.1 の場合は /csamc51/sdee-server、CSA MC バージョン 5.2 以降の場合は /csamc/sdee-server（これがデフォルト値）となります。
  - [Port]：通信に使用されるポートを指定します。
  - [Use TLS]：安全な通信が使用されることを示します。この値は変更できません。
- [Login Settings]：CSA MC へのログインに必要なクレデンシャルを指定できます。
  - [Username]：CSA MC へのログインに使用するユーザ名を入力します。
  - [Password]：そのユーザにパスワードを割り当てます。
  - [Confirm Password]：確認のためにパスワードを再入力します。
- [Watch List Settings]：CSA MC から受信したウォッチ リスト設定の処理方法を設定できます。

  - [Enable receipt of watch list] : ウォッチ リスト情報の受信をイネーブル/ディセーブルにします。ディセーブルにした場合、CSA MC から受信したウォッチ リスト情報は削除されます。
  - [Manual Watch List RR Increase] : 手動ウォッチ リストのリスク レーティングの加算率を拡大できます。
  - [Session-based Watch List RR Increase] : セッションベース ウォッチ リストのリスク レーティングの加算率を拡大できます。
  - [Packet-based Watch List RR Increase] : パケットベース ウォッチ リストのリスク レーティングの加算率を拡大できます。
- [Host Posture Settings] : CSA MC から受信したホスト ポスチャの処理方法を示します。
  - [Enable receipt of host postures] : ホスト ポスチャ情報の受信をイネーブル/ディセーブルにします。ディセーブルにした場合、CSA MC から受信したホスト ポスチャ情報は削除されます。
  - [Allow unreachable hosts' postures] : CSA MC から到達不能なホストのホスト ポスチャ情報の受信を許可/拒否します。

    CSA MC がホスト ポスチャに含まれるどの IP アドレスを使用してもホストとの接続を確立できない場合、そのホストは到達不能です。このオプションは、IPS が認識できない可能性のある IP アドレスやネットワーク内で重複している可能性のある IP アドレスを持つポスチャのフィルタリングに役立ちます。このフィルタは、CSA MC から到達不能なホストに IPS からも到達できないようなネットワーク トポロジに最も適しています。たとえば、IPS と CSA MC が同じネットワーク セグメントにある場合などです。
- [Permitted and Denied Host Posture Addresses] : 許可または拒否する ACL ホスト ポスチャを追加できます。
  - [Name] : ポスチャ ACL の名前。
  - [Active] : このポスチャ ACL がアクティブかどうかを示します。
  - [IP Address] : ポスチャ ACL の IP アドレス。
  - [Network Mask] : ポスチャ ACL のネットワーク マスク。
  - [Action] : ポスチャ ACL が実行するアクション（拒否または許可）。

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

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

- [Name] : ポスチャ ACL の名前。
- [Active] : このポスチャ ACL がアクティブかどうかを示します。
- [IP Address] : ポスチャ ACL の IP アドレス。
- [Network Mask] : ポスチャ ACL のネットワーク マスク。
- [Action] : ポスチャ ACL が実行するアクション（拒否または許可）。

外部製品インターフェイスおよびポスチャ ACL の追加、編集、削除

注意　Cisco IPS で追加できる外部製品インターフェイスは CSA MC インターフェイスだけです。Cisco IPS は、2 つの CSA MC インターフェイスをサポートしています。

（注）　センサーとの通信が可能となるように、外部製品を信頼できるホストとして追加してください。信頼できるホストを追加するには、[Configuration] > *sensor_name* > [Sensor Management] > [Certificates] > [Trusted Hosts] > [Add] を選択します。

外部製品インターフェイスを追加するには、次の手順を実行します。

ステップ 1　管理者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* > [Sensor Management] > [External Product Interfaces] を選択し、[Add] をクリックして、外部製品インターフェイスを追加します。

ステップ 3　[External Product's IP Address] フィールドに外部製品の IP アドレスを入力します。

ステップ 4　外部製品からセンサーに情報が渡されるようにするには、[Enable receipt of information] チェックボックスをオンにします。

ステップ 5　必要に応じて、[Port] フィールドでデフォルト ポート 443 を変更します。

（注）　[Communication Settings] では、ポート値のみ変更できます。

ステップ 6　ログイン設定を指定します。

a. [Username] フィールドに、外部製品にログインできるユーザのユーザ名を入力します。

b. [Password] フィールドに、そのユーザが使用するパスワードを入力します。

c. [Confirm Password] フィールドにパスワードを再入力します。

（注）　ステップ 7 ～ 15 は任意です。ステップ 7 ～ 15 を実行しない場合、CSA MC 情報の受信にはデフォルト値が使用され、フィルタが適用されずにすべての情報が受信されます。

ステップ 7　（任意）ウォッチ リスト設定を指定します。

a. 外部製品からセンサーにウォッチ リスト情報が渡されるようにするには、[Enable receipt of watch list] チェックボックスをオンにします。

（注）　[Enable receipt of watch list] チェックボックスをオンにしない場合、CSA MC から受信したウォッチ リスト情報は削除されます。

b. [Manual Watch List RR Increase] フィールドでは、リスク レーティングの加算率をデフォルトの 25 から別の値に変更できます。有効な値の範囲は 0 ～ 35 です。

c. [Session-based Watch List RR Increase] フィールドでは、リスク レーティングの加算率をデフォルトの 25 から別の値に変更できます。有効な値の範囲は 0 ～ 35 です。

d. [Packet-based Watch List RR Increase] フィールドでは、リスク レーティングの加算率をデフォルトの 10 から別の値に変更できます。有効な値の範囲は 0 ～ 35 です。

ステップ 8　（任意）外部製品からセンサーにホスト ポスチャ情報が渡されるようにするには、[Enable receipt of host postures] チェックボックスをオンにします。

（注）　[Enable receipt of host postures] チェックボックスをオンにしない場合、CSA MC から受信したホスト ポスチャ情報は削除されます。

ステップ 9　（任意）到達不能ホストからのホスト ポスチャ情報が外部製品からセンサーに渡されるようにするには、[Allow unreachable hosts' postures] チェックボックスをオンにします。

（注）　CSA MC がホスト ポスチャに含まれるどの IP アドレスを使用してもホストとの接続を確立できない場合、そのホストは到達不能です。このオプションは、IPS が認識できない可能性のある IP アドレスやネットワーク内で重複している可能性のある IP アドレスを持つポスチャのフィルタリングに役立ちます。このフィルタは、CSA MC から到達不能なホストに IPS からも到達できないようなネットワーク トポロジに最も適しています。たとえば、IPS と CSA MC が同じネットワーク セグメントにある場合などです。

ステップ 10　（任意）ポスチャ ACL を追加するには、[Add] をクリックします。

（注）　ポスチャ ACL は、ホスト ポスチャの許可または拒否の対象となるネットワーク アドレスの範囲です。ポスチャ ACL を使用して、IPS が認識できない可能性のある IP アドレスやネットワーク内で重複している可能性のある IP アドレスを持つポスチャをフィルタリングできます。

ステップ 11　（任意）[Name] フィールドにポスチャ ACL の名前を入力します。

ステップ 12　（任意）[Active] フィールドで、[Yes] オプション ボタンをクリックしてポスチャ ACL をアクティブにします。

ステップ 13　（任意）[IP Address] フィールドにポスチャ ACL が使用する IP アドレスを入力します。

ステップ 14　（任意）[Network Mask] フィールドにポスチャ ACL が使用するネットワーク マスクを編集します。

ステップ 15　（任意）[Action] ドロップダウン リストで、ポスチャ ACL が実行するアクション（[Deny] または [Permit]）を選択します。

ヒント　変更内容を元に戻して [Add Posture ACL] 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　（任意）[OK] をクリックします。[Add External Product Interface] ダイアログボックスの [Host Posture Setting] リストに新しいポスチャ ACL が表示されます。[Move Up] ボタンおよび [Move Down] ボタンを使用して、作成したポスチャ ACL の順序を変更できます。

ステップ 17　既存のポスチャ ACL を編集するには、ポスチャ ACL を選択して [Edit] をクリックします。

ステップ 18　[IP Address]、[Network Mask]、[Action] の各フィールドを編集するか、[No] オプション ボタンをクリックしてアクティブ状態を非アクティブに変更します。

ヒント　変更を破棄して [Edit Posture ACL] 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 19　[OK] をクリックします。編集したポスチャ ACL が [Add External Product Interface] ダイアログボックスの [Host Posture Setting] リストに表示されます。

ステップ 20　リストからポスチャ ACL を削除するには、そのポスチャ ACL を選択し、[Delete] をクリックします。そのポスチャ ACL は、[Add External Product Interface] ダイアログボックスの [Host Posture Setting] リストに表示されなくなります。

ステップ 21　[OK] をクリックします。外部製品インターフェイスが [External Product Interfaces] ペインの [Center for Cisco Security Agents] リストに表示されます。

ヒント 変更を破棄して [Add External Product Interface] 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 22 外部製品インターフェイスを編集するには、そのインターフェイスを選択し、[Edit] をクリックします。

ステップ 23 ダイアログボックスのフィールドに必要な変更を加えます。

ヒント 変更を破棄して [Edit External Product Interface] 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 24 [OK] をクリックします。編集した外部製品インターフェイスが [External Product Interfaces] ペインの [Management Center for Cisco Security Agents] リストに表示されます。

ステップ 25 外部製品インターフェイスを削除するには、そのインターフェイスを選択し、[Delete] ボタンをクリックします。その外部製品インターフェイスは、[External Product Interfaces] ペインの [Management Center for Cisco Security Agents] 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 26 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。

外部製品インターフェイスのトラブルシューティング

外部製品のインターフェイスのトラブルシューティングを行う場合は、次のことをチェックしてください。

- CLI で **show statistics external-product-interface** コマンドからの出力をチェックするか、IME で [Configuration] > *sensor_name* > [Sensor Monitoring] > [Support Information] > [Statistics] を選択して、応答の [Interface] の状態行をチェックして、インターフェイスがアクティブであることを確認します。
- 信頼できるホストに CSA MC IP アドレスを追加したことを確認します。追加するのを忘れた場合は、追加し、数分待ってから、もう一度チェックします。
- ブラウザを使用して CSA MC でサブスクリプションを開いてから閉じて、サブスクリプション ログイン情報を確認します。
- イベント ストアで CSA MC のサブスクリプション エラーをチェックします。

詳細情報

- 信頼できるホストの追加手順については、「信頼できるホストの追加」（P.14-10）を参照してください。
- イベントを表示する手順については、「イベントのモニタリング」（P.19-1）を参照してください。

CHAPTER 18

センサーの管理

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

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

この章では、パスワードの設定、ライセンス キーの取得とインストール、IP ロギング変数の設定、最新ソフトウェアによるセンサーのアップデート、センサー デフォルトの復元、センサーのリブート、センサーのシャットダウンなど、センサーの管理方法について説明します。この章は、次の内容で構成されています。

パスワードの設定

ここでは、センサーのユーザのパスワード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。

[Passwords] ペイン

センサーの管理者は、[Passwords] ペインでパスワードの作成方法を設定できます。ユーザが作成するパスワードはすべて、[Passwords] ペインで設定されたポリシーに従う必要があります。

注意　パスワード ポリシーに、大文字や数字などの文字セットの最小文字数を含める場合、必須文字セットの最小文字数の合計は最小パスワード サイズを超えることはできません。たとえば、最小パスワード サイズを 8 文字に設定し、パスワードに 5 文字以上の小文字と 5 文字以上の大文字を含めるように要求することはできません。

[Passwords] ペインのフィールド定義

[Passwords] ペインには次のフィールドがあります。

- [Attempt Limit]：ユーザがある回数ログインに失敗したら、それ以上続けられないようにアカウントをロックできます。デフォルトは 0 です。これは無制限の認証試行を示します。セキュリティのために、この数値を変更する必要があります。
- [Size Range]：パスワードに許容される最小サイズと最大サイズに指定する範囲。有効な範囲は 6 ～ 64 文字です。
- [Minimum Digit Characters]：ユーザが指定するパスワードには、この数以上の数字が含まれている必要があります。
- [Minimum Upper Case Characters]：ユーザが指定するパスワードに含むことができる大文字のアルファベットの数の上限です。
- [Minimum Lower Case Characters]：ユーザが指定するパスワードには、この数以上の小文字のアルファベット文字が含まれている必要があります。
- [Minimum Other Characters]：ユーザが指定するパスワードには、この数以上のアルファベット以外の印刷可能文字が含まれている必要があります。
- [Number of Historical Passwords]：アカウントごとにセンサーで記憶させる履歴パスワードの数。新しいパスワードが記憶されているいずれかのパスワードと一致した場合は、アカウントのパスワードの変更試行に失敗します。この値が 0 の場合、以前のパスワードは記憶されません。

詳細情報

さまざまなセンサーでパスワードを回復する手順については、「パスワードの回復」（P.18-3）を参照してください。

パスワード要件の設定

パスワード要件を設定するには、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* > [Sensor Management] > [Passwords] を選択します。

ステップ 3　[Attempt Limit] フィールドに、ユーザが正しいパスワードを入力するまで試行できる回数を入力します。デフォルトは 0 です。これは無制限の認証試行を示します。セキュリティのために、この数値を変更する必要があります。

ステップ 4　[Size Range] フィールドに、パスワードに許容される長さを入力します。有効な範囲は 6 ～ 64 です。

ステップ 5　[Minimum Digit Characters] フィールドに、パスワードに入力できる数字の数の最小値を入力します。

ステップ 6　[Minimum Upper Case Characters] フィールドに、パスワードに入力できる大文字の数の最小値を入力します。

ステップ 7　[Minimum Lower Case Characters] フィールドに、パスワードに入力できる小文字の数の最小値を入力します。

注意　パスワード ポリシーに、大文字や数字などの文字セットの最小文字数を含める場合、必須文字セットの最小文字数の合計は最小パスワード サイズを超えることはできません。たとえば、最小パスワード サイズを 8 文字に設定し、パスワードに 5 文字以上の小文字と 5 文字以上の大文字を含めるように要求することはできません。

ステップ 8　[Minimum Other Characters] フィールドに、パスワードに入力できるその他の文字数の最小値を入力します。

ステップ 9　[Number of Historical Passwords] フィールドに、アカウントごとにセンサーで記憶させる履歴パスワードの数を入力します。

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 10　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。

パスワードの回復

ほとんどの IPS プラットフォームでは、サービス アカウントを使用したり、センサーのイメージを再作成したりせずに、センサー上でパスワードを回復できるようになりました。ここでは、さまざまなプラットフォームでパスワードを回復する方法について説明します。内容は次のとおりです。

パスワードの回復について

パスワード回復の実装は、IPS プラットフォームの要件によって異なります。パスワードの回復は、cisco 管理者アカウントに対してのみ実装され、デフォルトでイネーブルになっています。IPS 管理者は、その後 CLI を使用して他のアカウントのユーザ パスワードを回復できます。シスコのユーザ パスワードは **cisco** に戻るため、次回ログイン後に変更する必要があります。

（注）　管理者は、セキュリティ上の理由から、パスワードの回復機能をディセーブルにしなければならない場合があります。

表 18-1 に、プラットフォーム別のパスワード回復方法を示します。

表 18-1　プラットフォーム別のパスワード回復方法

プラットフォーム	説明	回復方法
4200 シリーズ センサー	スタンドアロン IPS アプライアンス	GRUB プロンプトまたは ROMMON
AIM IPS NME IPS	ルータ IPS モジュール	ブートローダ コマンド
AIP SSM AIP SSC-5 IPS SSP	ASA 5500 シリーズ適応型セキュリティ アプライアンス モジュール	適応型セキュリティ アプライアンス の CLI コマンド
IDSM2	スイッチ IPS モジュール	メンテナンス パーティションからイメージをダウンロード

詳細情報

パスワード回復をディセーブルにする手順については、「パスワード回復のディセーブル化」（P.18-9）を参照してください。

アプライアンスのパスワードの回復

アプライアンスのパスワードを回復するには、GRUB メニューを使用する方法と ROMMON を使用する方法があります。ここでは、アプライアンスでパスワードを回復する方法について説明します。内容は次のとおりです。

- 「GRUB メニューの使用」（P.18-4）
- 「ROMMON の使用」（P.18-5）

GRUB メニューの使用

4200 シリーズのアプライアンスでは、パスワードの回復には、ブートアップ中に表示される GRUB メニューを使用します。GRUB メニューが表示されたら、任意のキーを押してブート プロセスを停止します。

（注）　GRUB メニューを使用してパスワードを回復するには、ターミナル サーバを使用するか、アプライアンスとの直接シリアル接続が必要です。

アプライアンスでパスワードを回復するには、次の手順を実行します。

ステップ 1　アプライアンスをリブートして、GRUB メニューを表示します。

```
GNU GRUB version 0.94 (632K lower / 523264K upper memory)
----------------------------------------
0: Cisco IPS
1: Cisco IPS Recovery
```

```
2: Cisco IPS Clear Password (cisco)
-----------------------------------------

    Use the ^ and v keys to select which entry is highlighted.
    Press enter to boot the selected OS, 'e' to edit the
    Commands before booting, or 'c' for a command-line.

    Highlighted entry is 0:
```

ステップ 2　任意のキーを押して、ブート プロセスを停止します。

ステップ 3　[2: Cisco IPS Clear Password (cisco)] を選択します。

パスワードが **cisco** にリセットされます。次に CLI にログインするときにパスワードを変更できます。

詳細情報

アプライアンスをターミナル サーバに接続する手順については、「ターミナル サーバへの接続」（P.C-23）を参照してください。

ROMMON の使用

IPS 4240 と IPS 4255 については、ROMMON を使用してパスワードを回復できます。ROMMON CLI にアクセスするには、ターミナル サーバまたは直接接続からセンサーをリブートして、ブート プロセスを中断します。

ROMMON CLI を使用してパスワードを回復するには、次の手順を実行します。

ステップ 1　アプライアンスをリブートします。

ステップ 2　ブート プロセスを中断するには、**ESC** または **Control-R**（ターミナル サーバ）を押すか、**BREAK** コマンドを送信します（直接接続）。

ブート コードによって 10 秒間停止するか、次のようなメッセージが表示されます。

- `Evaluating boot options`
- `Use BREAK or ESC to interrupt boot`

ステップ 3　次のコマンドを入力してパスワードをリセットします。

```
confreg 0x7
boot
```

サンプル ROMMON セッション：

```
Booting system, please wait...
CISCO SYSTEMS
Embedded BIOS Version 1.0(11)2 01/25/06 13:21:26.17
...
Evaluating BIOS Options...
Launch BIOS Extension to setup ROMMON
Cisco Systems ROMMON Version (1.0(11)2) #0: Thu Jan 26 10:43:08 PST 2006
Platform IPS-4240-K9
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.
Management0/0
Link is UP
MAC Address:000b.fcfa.d155
Use ? for help.
rommon #0> confreg 0x7
```

```
Update Config Register (0x7) in NVRAM...
rommon #1> boot
```

詳細情報

アプライアンスをターミナル サーバに接続する手順については、「ターミナル サーバへの接続」（P.C-23）を参照してください。

AIM IPS パスワードの回復

AIM IPS のパスワードを回復するには、**clear password** コマンドを使用します。AIM IPS へのコンソール アクセスとルータへの管理者アクセス権が必要です。

AIM IPS のパスワードを回復するには、次の手順を実行します。

ステップ 1　ルータにログインします。

ステップ 2　ルータで特権 EXEC モードを開始します。

```
router> enable
```

ステップ 3　ルータのモジュール スロット番号を確認します。

```
router# show run | include ids-sensor
interface IDS-Sensor0/0
router#
```

ステップ 4　AIM IPS との間にセッションを確立します。

```
router# service-module ids-sensor slot/port session
```

例

```
router# service-module ids-sensor 0/0 session
```

ステップ 5　**Control-shift-6** のあとで **x** を押して、ルータ CLI に移動します。

ステップ 6　ルータ コンソールから AIM-IPS をリセットします。

```
router# service-module ids-sensor 0/0 reset
```

ステップ 7　**Enter** を押して、ルータ コンソールに戻ります。

ステップ 8　ブート オプションのプロンプトが表示されたら、素早く ******* を入力します。ブートローダが起動されます。

ステップ 9　パスワードをクリアします。

```
ServicesEngine boot-loader# clear password
```

AIM IPS がリブートします。パスワードが **cisco** にリセットされます。ユーザ名 **cisco** とパスワード **cisco** を使用して CLI にログインします。これで、パスワードを変更できます。

ASA モジュールのパスワードの回復

CLI または ASDM を使用して AIP SSM、AIP SSC-5、および IPS SSP のパスワードをデフォルト（**cisco**）にリセットできます。パスワードをリセットすると、ASA モジュールはリブートされます。リブート中、IPS サービスは利用できません。

（注）　AIP SSM のパスワードをリセットするには、ASA 7.2.(2) 以降が必要です。AIP SSC-5 のパスワードをリセットするには、ASA 8.2.(1) 以降が必要です。IPS SSP のパスワードをリセットするには、ASA 8.2(4.4) 以降および ASA 8.4(2) 以降が必要です。ASA 8.3(*x*) ではサポートされていません。

hw-module module *slot_number* **password-reset** コマンドを使用して、パスワードをデフォルトの **cisco** にリセットします。ASA 5500 シリーズの適応型セキュリティ アプライアンスは、ROMMON の confreg ビットを 0x7 に設定し、モジュールをリブートします。ROMMON ビットによって、GRUB メニューのデフォルトがオプション 2（[reset password]）に設定されます。

指定されたスロットのモジュールにパスワードの回復をサポートしない IPS バージョンがある場合、次のエラー メッセージが表示されます。

```
ERROR: the module in slot <n> does not support password recovery.
```

ASDM の使用

ASDM でパスワードをリセットするには、次の手順を実行します。

ステップ 1　ASDM メニュー バーで、[Tools] > [IPS Password Reset] を選択します。

（注）　IPS モジュールがインストールされていない場合、このオプションはメニューに表示されません。

ステップ 2　[IPS Password Reset] 確認ダイアログボックスで [OK] をクリックして、パスワードをデフォルト（**cisco**）にリセットします。

ダイアログボックスに、パスワードのリセットが正常に完了したか、失敗したかが表示されます。リセットが失敗した場合は、ソフトウェア バージョンが正しいことを確認してください。

ステップ 3　[Close] をクリックして、ダイアログボックスを閉じます。ASA モジュールがリブートされます。

IDSM2 パスワードの回復

IDSM2 のパスワードを回復するには、特別なパスワード回復イメージ ファイルをインストールする必要があります。このインストールでは、パスワードだけがリセットされ、他のすべての情報は影響を受けません。パスワード回復イメージはバージョンに依存し、Cisco Download Software サイトから入手できます。IPS 6.*x* の場合は、WS-SVC-IDSM2-K9-a-6.0-password-recovery.bin.gz をダウンロードします。IPS 7.*x* の場合は、WS-SVC-IDSM2-K9-a-7.0-password-recovery.bin.gz をダウンロードします。

イメージのインストールにサポートされているプロトコルは FTP だけなので、必ずスイッチがアクセスできる FTP サーバにパスワード回復イメージを置いてください。IDSM2 でパスワードを回復するには、Cisco 6500 シリーズ スイッチへの管理者アクセス権が必要です。

パスワード回復イメージのインストール中に次のメッセージが表示されます。

```
Upgrading will wipe out the contents on the hard disk.
Do you want to proceed installing it [y|n]:
```

このメッセージはエラーです。パスワード回復イメージをインストールしても設定は削除されません。ログイン アカウントがリセットされるだけです。

パスワード回復イメージ ファイルをダウンロードしたら、システム イメージ ファイルのインストール手順を実行します。ただし、システム イメージ ファイルの代わりにパスワード回復イメージ ファイルを使用します。イメージ回復ファイルのインストール後、IDSM2 はプライマリ パーティションにリブートされます。そのようにリブートされない場合は、スイッチから次のコマンドを入力します。

```
hw-module module module_number reset hdd:1
```

（注）　パスワードが **cisco** にリセットされます。ユーザ名 **cisco** とパスワード **cisco** を使用して CLI にログインします。これで、パスワードを変更できます。

詳細情報

システム イメージ ファイルのインストール手順を使用して IDSM2 パスワード回復ファイルをインストールする手順については、「IDSM2 システム イメージのインストール」（P.25-29）を参照してください。

NME IPS パスワードの回復

NME IPS のパスワードを回復するには、**clear password** コマンドを使用します。NME IPS へのコンソール アクセスとルータへの管理者アクセス権が必要です。

NME IPS のパスワードを回復するには、次の手順を実行します。

ステップ 1　ルータにログインします。

ステップ 2　ルータで特権 EXEC モードを開始します。

```
router> enable
```

ステップ 3　ルータのモジュール スロット番号を確認します。

```
router# show run | include ids-sensor
interface IDS-Sensor1/0
router#
```

ステップ 4　NME IPS との間にセッションを確立します。

```
router# service-module ids-sensor slot/port session
```

例

```
router# service-module ids-sensor 1/0 session
```

ステップ 5　**Control-shift-6** のあとで **x** を押して、ルータ CLI に移動します。

ステップ 6　ルータ コンソールから NME IPS をリセットします。

```
router# service-module ids-sensor 1/0 reset
```

ステップ 7　**Enter** を押して、ルータ コンソールに戻ります。

ステップ 8　ブート オプションのプロンプトが表示されたら、素早く ******* を入力します。ブートローダが起動されます。

ステップ 9　パスワードをクリアします。

```
ServicesEngine boot-loader# clear password
```

NME IPS がリブートします。パスワードが **cisco** にリセットされます。ユーザ名 **cisco** とパスワード **cisco** を使用して CLI にログインします。これで、パスワードを変更できます。

パスワード回復のディセーブル化

注意　パスワード回復がディセーブルになっているセンサーでパスワードを回復しようとすると、エラーや警告が表示されずにプロセスは進みますが、パスワードはリセットされません。パスワードを忘れたためにセンサーにログインできないときに、パスワード回復がディセーブルに設定されている場合は、センサーのイメージを再作成する必要があります。

パスワードの回復は、デフォルトでイネーブルです。パスワード回復は、CLI または MIE からディセーブルにすることができます。

CLI でパスワード回復をディセーブルにするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　グローバル コンフィギュレーション モードを開始します。

```
sensor# configure terminal
```

ステップ 3　ホスト モードを開始します。

```
sensor(config)# service host
```

ステップ 4　パスワード回復をディセーブルにします。

```
sensor(config-hos)# password-recovery disallowed
```

IME でパスワード回復をディセーブルにするには、次の手順を実行します。

ステップ 1　管理者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* > [Sensor Setup] > [Network] を選択します。

ステップ 3　パスワード回復をディセーブルにするには、[Allow Password Recovery] チェックボックスをオフにします。

パスワード回復のトラブルシューティング

パスワード回復のトラブルシューティングを行う場合は、次の点に注意してください。

- ROMMON プロンプト、GRUB メニュー、スイッチの CLI、ルータの CLI からは、パスワード回復がセンサーの設定でディセーブルになっているかどうかを確認できません。パスワード回復を試みると、常に成功したように見えます。ディセーブルになっている場合、パスワードは **cisco** にリセットされません。唯一のオプションはセンサーのイメージの再作成です。
- パスワード回復は、ホストの設定でディセーブルにすることができます。AIM IPS や NME IPS ブートローダ、ROMMON、IDSM2 のメンテナンス パーティションなどの外部メカニズムを使用しているプラットフォームの場合、パスワードをクリアするコマンドを実行できますが、IPS でパスワード回復がディセーブルになっている場合、IPS はパスワード回復が許可されていないことを検出し、外部要求を拒否します。
- パスワード回復の状態をチェックするには、**show settings | include password** コマンドを使用します。
- IDSM2 でパスワード回復を実行すると、「`Upgrading will wipe out the contents on the storage media.`」というメッセージが表示されます。このメッセージは無視できます。指定されたパスワード回復イメージを使用すると、パスワードだけがリセットされます。

パスワード回復の状態の確認

パスワード回復がイネーブルになっているかどうかを確認するには、**show settings** | **include password** コマンドを使用します。

パスワード回復がイネーブルになっているかどうかを確認するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　サービス ホスト サブモードを開始します。

```
sensor# configure terminal
sensor (config)# service host
sensor (config-hos)#
```

ステップ 3　**include** キーワードを使用して、フィルタ処理された出力で設定を表示し、パスワード回復の状態を確認します。

```
sensor(config-hos)# show settings | include password
   password-recovery: allowed <defaulted>
sensor(config-hos)#
```

ライセンスの設定

ここでは、ライセンス キーの取得およびインストール方法について説明します。内容は次のとおりです。

- 「[Licensing] ペインのフィールド定義」（P.18-12）
- 「ライセンス キーの取得とインストール」（P.18-13）

[Licensing] ペイン

（注）　[Licensing] ペインにライセンス情報を表示し、センサーのライセンス キーをインストールするには、管理者である必要があります。

[Licensing] ペインで、センサーのライセンス キーを取得し、インストールできます。[Licensing] ペインには、現在のライセンスのステータスが表示されます。

ライセンスについて

（注）　AIP SSC-5 は、グローバル相関機能をサポートしていません。

ライセンス キーがなくてもセンサーは機能しますが、シグニチャのアップデートを取得する場合とグローバル相関機能を使用する場合はライセンス キーが必要です。ライセンス キーを取得するには、次のものが必要です。

- Cisco Service for IPS サービス契約：代理店、シスコ サービスまたは製品のセールスにお問い合わせの上、契約を購入してください。
- IPS デバイスのシリアル番号：IME で IPS デバイスのシリアル番号を確認するには、[Configuration] > *sensor_name* > [Sensor Management] > [Licensing] を選択します。または、CLI で **show version** コマンドを使用します。
- 有効な Cisco.com ユーザ名およびパスワード

トライアル ライセンス キーも使用できます。契約上の問題によってセンサーのライセンスを取得できない場合は、ライセンスが必要なシグニチャのアップデートをサポートする 60 日間のトライアル ライセンスを取得できます。

Cisco.com ライセンス サーバからライセンス キーを取得できます。キーはその後センサーに配信されます。または、ローカル ファイルで提供されたライセンス キーからライセンス キーを更新できます。http://www.cisco.com/go/license にアクセスし、[IPS Signature Subscription Service] をクリックして、ライセンス キーを申し込みます。

次の場所で、ライセンス キーのステータスを表示できます。

- IME ホームページの [Licensing] タブの [Device Details] セクション
- CLI ログインのライセンスのお知らせ

IME または CLI を起動すると、トライアル、無効、有効期限切れなど、ライセンス キーのステータスが通知されます。ライセンス キーがない場合、ライセンス キーが無効または有効期限切れの場合、IME および CLI は引き続き使用できますが、シグニチャのアップデートをダウンロードすることはできません。

センサーに有効なライセンスがある場合は、[License] ペインの [Download] をクリックして、IME が動作しているコンピュータにライセンス キーのコピーをダウンロードして、ローカル ファイルに保存できます。その後、紛失したライセンスまたは破損したライセンスを置き換えるか、センサーのイメージの再作成後にライセンスを再インストールできます。

IPS 製品のサービス プログラム

ライセンス キーをダウンロードし、最新の IPS シグニチャのアップデートを取得するには、IPS 製品の Cisco Services for IPS サービス契約が必要です。シスコと直接取引がある場合は、アカウント マネージャまたはサービス アカウント マネージャにお問い合わせのうえ、Cisco Services for IPS サービス契約を購入してください。シスコと直接取引がない場合は、第 1 層または第 2 層パートナーからサービス アカウントを購入できます。

次の IPS 製品を購入する場合は、Cisco Services for IPS サービス契約も購入する必要があります。

- IPS 4240
- IPS 4255
- IPS 4260
- IPS 4270-20
- AIM IPS
- IDSM2
- NME IPS

IPS を搭載していない ASA 5500 シリーズの適応型セキュリティ アプライアンス製品を購入する場合は、SMARTnet 契約を購入する必要があります。

（注） SMARTnet は、オペレーティング システムのアップデート、Cisco.com へのアクセス、TAC へのアクセス、サイトでのハードウェア交換 NBD を提供します。

AIP SSM、IPS SSP、または AIP SSC-5 がインストールされた ASA 5500 シリーズの適応型セキュリティ アプライアンス製品を購入した場合、または ASA 5500 シリーズの適応型セキュリティ アプライアンス製品に追加するようにこれらを購入した場合、Cisco Services for IPS サービス契約を購入する必要があります。

（注） Cisco Services for IPS は、IPS シグニチャのアップデート、オペレーティング システムのアップデート、Cisco.com へのアクセス、TAC へのアクセス、サイトでのハードウェア交換 NBD を提供します。

たとえば、ASA 5585-X を購入し、その後 IPS が必要となり ASA-IPS10-K9 を購入した場合、Cisco Services for IPS サービス契約を購入する必要があります。Cisco Services for IPS サービス契約の購入後、ライセンス キーを申請するための製品シリアル番号も必要になります。

注意 製品を RMA のために送付した場合、シリアル番号が変わります。そのときは、新しいシリアル番号用に新しいライセンス キーを取得する必要があります。

[Licensing] ペインのフィールド定義

[Licensing] ペインには次のフィールドがあります。

- [Current License]：現在のライセンスのステータスを提供します。
  - [License Status]：センサーの現在のライセンス ステータス。

  - [Expiration Date]：ライセンス キーの有効期限が切れる（または切れた）日付。キーが無効の場合、日付は表示されません。
  - [Serial Number]：センサーのシリアル番号。
  - [Product ID]：センサーの製品 ID。
- [Update License]：新しいライセンス キーの入手先を指定します。
  - [Cisco.com]：Cisco.com のライセンス サーバにライセンス キーを問い合わせます。
  - [License File]：ライセンス ファイルを使用するように指定します。
  - [Local File Path]：ライセンス キーを含むローカル ファイルの場所を示します。

ライセンス キーの取得とインストール

（注） 有効な Cisco.com ユーザ名とパスワードのほかに、ライセンス キーを申請するには、その前に Cisco Services for IPS サービス契約を購入する必要があります。

ライセンス キーを取得およびインストールするには、次の手順に従ってください。

ステップ 1　管理者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* > [Sensor Management] > [Licensing] を選択します。[Licensing] ペインには、現在のライセンスのステータスが表示されます。ライセンスをすでにインストールした場合は、必要に応じて、[Download] をクリックして保存できます。

ステップ 3　次のいずれかの方法でライセンス キーを取得します。

- [Cisco.com] オプション ボタンをクリックして、Cisco.com からライセンスを取得します。IME が Cisco.com のライセンス サーバにアクセスし、サーバにシリアル番号を送信して、ライセンス キーを取得します。これがデフォルトの方法です。ステップ 4 に進みます。
- [License File] オプション ボタンをクリックして、ライセンス ファイルを使用します。このオプションを使用するには、URL www.cisco.com/go/license にアクセスして、ライセンス キーを申請する必要があります。ライセンス キーが電子メールで送信されます。そのメールを IME がアクセスできるドライブに保存します。このオプションは、コンピュータから Cisco.com にアクセスできない場合に便利です。ステップ 7 に進みます。

ステップ 4　[Update License] をクリックし、[Licensing] ダイアログボックスで [Yes] をクリックして、続行します。[Status] ダイアログボックスに、センサーが Cisco.com に接続しようとしていることを伝えるメッセージが表示されます。情報ダイアログボックスにライセンス キーが更新されたことを伝えるメッセージが表示されます。

ステップ 5　[OK] をクリックします。

ステップ 6　www.cisco.com/go/license にアクセスします。

ステップ 7　必須フィールドに入力します。ライセンス キーが、指定された電子メール アドレスに送信されます。

注意　ライセンス キーは指定されたシリアル番号のデバイスでのみ機能するので、IPS デバイスの正しいシリアル番号が必要です。

ステップ 8　ライセンス キーを、ハードディスク ドライブまたは IME を実行するクライアントがアクセスできるネットワーク ドライブに保存します。

ステップ 9　IME にログインします。

ステップ 10　[Configuration] > *sensor_name* > [Sensor Management] > [Licensing] を選択します。

ステップ 11　[Update License] で [License File] オプション ボタンをクリックします。

ステップ 12　[Local File Path] フィールドでライセンス ファイルへのパスを指定するか、[Browse Local] をクリックして、ファイルを検索します。

ステップ 13　ライセンス ファイルを検索し、[Open] をクリックします。

ステップ 14　[Update License] をクリックします。

センサーのヘルスの設定

ここでは、センサーのヘルスのメトリックの設定方法について説明します。内容は次のとおりです。

[Sensor Health] ペイン

（注）　センサーのヘルスのメトリックを設定するには、管理者である必要があります。

[Sensor Health] ペインで、IPS のヘルスとネットワーク セキュリティのステータスを判断するために使用されるメトリックを設定できます。さまざまなガジェットの [Home] ペインに結果が表示されます。

チェックボックスをオンにせずにメトリックを選択しない場合、ヘルスとネットワーク セキュリティ ステータスの結果に表示されません。デフォルト設定を受け入れるか、値を編集できます。

全体的なヘルスは、メトリックの中で最も重大な設定値に設定されます。たとえば、選択されたすメトリックで、赤いメトリックが 1 つある以外はすべて緑の場合、全体的なヘルスは赤になります。IPS は、IPS の全体的なヘルス ステータスが変化すると、ヘルスおよびセキュリティ ステータス イベントを生成します。

センサーのセキュリティ ステータスは、仮想センサーによって検出されたイベントの脅威レーティングを使用して、仮想センサーごとに決定されます。仮想センサーのセキュリティ ステータスは、仮想センサーがそのセンサーのしきい値を超える脅威レーティングのイベントを検出すると発生します。しきい値を超えると、セキュリティ ステータスは、設定された時間内に、それ以上のイベントが高いレベルで検出されなくなるまで、重大レベルのままです。

[Sensor Health] ペインのフィールド定義

（注）　AIP SSC-5 は、グローバル相関機能をサポートしていません。

[Sensor Health] ペインには次のフィールドがあります。

- [Inspection Load]：検査負荷のしきい値と、このメトリックをセンサーの全体的なヘルス レーティングに適用するかどうかを設定できます。
- [Missed Packet]：失われたパケットのしきい値のパーセントと、このメトリックをセンサーの全体的なヘルス レーティングに適用するかどうかを設定できます。
- [Memory Usage]：メモリ使用量のしきい値のパーセントと、このメトリックがセンサーの全体的なヘルス レーティングに適用されるかどうかを設定できます。
- [Signature Update]：最後のシグニチャのアップデートが適用された時間のしきい値と、このメトリックをセンサーの全体的なヘルス レーティングに適用するかどうかを設定できます。
- [License Expiration]：ライセンスの有効期限のしきい値と、このメトリックをセンサーの全体的なヘルス レーティングに適用するかどうかを設定できます。
- [Event Retrieval]：最後にイベントが取得された時間のしきい値と、このメトリックをセンサーの全体的なヘルス レーティングに適用するかどうかを設定できます。

（注）　イベント取得メトリックでは、IME などの外部モニタリング アプリケーションによって最後のイベントが取得された時間が記録されます。外部イベント モニタリングを行っていない場合は、[Event Retrieval] をディセーブルにしてください。

- [Network Participation]：ネットワーク参加ヘルス メトリックをセンサーの全体的なヘルス レーティングに適用するかどうかを選択できます。
- [Global Correlation]：グローバル相関ヘルス メトリックをセンサーの全体的なヘルス レーティングに適用するかどうかを選択できます。
- [Application Failure]：アプリケーション障害をセンサーの全体的なヘルス レーティングに適用するかどうかを選択できます。
- [IPS in Bypass Mode]：バイパス モードがアクティブかどうかを認識し、それをセンサーの全体的なヘルス レーティングに適用するかどうかを選択できます。

（注）　IPS SSP は、バイパス モードをサポートしていません。適応型セキュリティ アプライアンスは、適応型セキュリティ アプライアンスの設定と IPS SSP 上で行われているアクティビティのタイプによって、フェールオープン、フェールクローズ、またはフェールオーバーします。

- [One or More Active Interfaces Down]：1 つ以上のインターフェイスがダウンしているかどうかを認識し、それをセンサーの全体的なヘルス レーティングに適用するかどうかを選択できます。
- [Yellow Threshold]：黄色の最も低いしきい値をパーセント、日、秒、または失敗数で設定できます。
- [Red Threshold]：赤の最も低いしきい値をパーセント、日、秒、または失敗数で設定できます。

詳細情報

- IME ガジェットの詳細については、「IME ガジェット」（P.3-2）を参照してください。
- IME の [Home] ペインの説明については、「IME の [Home] ペイン」（P.1-3）を参照してください。
- センサーおよびバイパス モードの詳細については、「バイパス モードの設定」を参照してください。

IP ロギング変数の設定

（注）　IP ロギング変数を設定するには、管理者である必要があります。

IP ロギング変数の Maximum Open IP Log Files を設定できます。これは、センサーの一般的な操作に適用されます。

フィールド定義

[Global Variables] ペインには、次のフィールドがあります。

- [Maximum Open IP Log Files] : 同時に開いている IP ログ ファイルの最大数。有効な範囲は 20 ～ 100 です。デフォルトは 20 です。

自動アップデートの設定

ここでは、ソフトウェアの自動アップデートを行うようにセンサー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。

[Auto/Cisco.com Update] ペイン

（注）　[Auto Update] ペインを表示して、自動アップデートを設定するには、管理者である必要があります。

注意　自動アップデートは、DOS スタイルのパスで設定された Windows FTP サーバでは動作しません。サーバが DOS スタイルのパスではなく、UNIX スタイルのパス オプションで設定されていることを確認してください。

Cisco.com およびローカル サーバからシグニチャのアップデートとシグニチャ エンジンのアップデートを自動的にダウンロードするようにセンサーを設定できます。自動アップデートをイネーブルにすると、センサーは Cisco.com にログインし、シグニチャ アップデートとシグニチャ エンジン アップデートをチェックします。アップデートが入手可能な場合、センサーはアップデートをダウンロードして、インストールします。Cisco.com から Cisco IPS シグニチャのアップデートおよびシグニチャ エンジンのアップデートをダウンロードするには、暗号化特権を持つ Cisco.com ユーザ アカウントが必要です。初めてシスコ ソフトウェアをダウンロードするときに、暗号化特権を持つアカウントを設定します。

注意　センサーは、非透過プロキシ サーバからの Cisco.com との通信をサポートしていません。

詳細情報

ソフトウェアおよび暗号化特権を持つアカウントの取得手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。

サポートされる FTP および HTTP サーバ

IPS ソフトウェアのアップデートについてサポートされている FTP サーバは次のとおりです。

- WU-FTPD 2.6.2（Linux）
- Solaris 2.8
- Sambar 6.0（Windows 2000）
- Serv-U 5.0（Windows 2000）
- MS IIS 5.0（Windows 2000）

IPS ソフトウェアのアップデートについてサポートされている HTTP/HTTPS サーバは次のとおりです。

- CSM - Apache Server（Tomcat）
- CSM - Apache Server（JRun）

UNIX スタイルのディレクトリ リスト表示

FTP サーバを使用して自動アップデートを設定するには、FTP サーバは UNIX スタイルのディレクトリ リスト表示応答を提供する必要があります。MS-DOS スタイルのディレクトリ リスト表示は、センサーの自動アップデート機能ではサポートされていません。

（注） サーバが MS-DOS スタイルのディレクトリ リスト表示を提供している場合、センサーはディレクトリ リスト表示を解析できず、入手可能な新しいアップデートがあるかどうかを判断できません。

Microsoft IIS で UNIX スタイルのディレクトリ リスト表示を使用するには、次の手順を使用します。

ステップ 1　[Start] > [Program Files] > [Administrative Tools] を選択します。

ステップ 2　[Home Directory] タブをクリックします。

ステップ 3　[UNIX directory listings style] オプション ボタンをクリックします。

シグニチャのアップデートおよびインストール時間

シグニチャのアップデートの実行中、短時間トラフィックが検査されない時間があります。ただし、バイパスをイネーブルにしている場合、トラフィックは引き続き通過します。

シグニチャのアップデートによって正規表現を含むシグニチャが追加または変更される場合、SensorApp で使用される正規表現キャッシュ テーブルを再コンパイルする必要があります。再コンパイル時間はプラットフォーム、変更または追加されたシグニチャの数、および変更または追加されたシグニチャのタイプによって異なります。

シグニチャのアップデートで、IPS 4255 や IPS 4260 などのハイエンド プラットフォームで 1 つまたは 2 つの新しいシグニチャが追加されただけの場合、再コンパイルはほんの数秒で終了します。

次の条件では、再コンパイルに数分、最大で 30 分かかります。

- 大量のシグニチャを追加する場合。たとえば、シグニチャのアップデートで、S240 の上に S258 をインストールするなど、複数のシグニチャ レベルをスキップして新しいシグニチャをインストールする場合。
- 大量のシグニチャを変更する場合。たとえば、シグニチャのアップデートで、大量の古いシグニチャをディセーブルまたは非アクティブにする場合。

再コンパイル中、SensorApp はパケットのモニタリングを停止します。パケット バッファが SensorApp への途中で蓄積し始めると、インターフェイス ドライバはそれを検出し、SensorApp からのパケットの受信を停止します。センサーがインライン モードで、バイパス オプションが [Auto] に設定されている場合、ドライバはバイパスをオンにします。バイパスが [Off] に設定されている場合、ドライバはインターフェイス リンクを切断します。

（注）　バイパス設定が動作し始める前に、一部のパケットがドロップされる可能性があります。SensorApp は、正規表現キャッシュ ファイルの再コンパイルを完了すると、ドライバと再接続し、モニタリングを再開します。ドライバは解析のために SensorApp にパケットの受け渡しを開始し、必要に応じて、インターフェイス リンクをアップさせます。

詳細情報

バイパス モードの詳細については、「バイパス モードの設定」（P.7-29）を参照してください。

[Auto/Cisco.com Update] ペインのフィールド定義

[Auto/Cisco.com Update] ペインには次のフィールドがあります。

- [Enable Auto Update From a Remote Server]：センサーはリモート サーバに格納されたアップデートをインストールできます。

  （注）　[Enable Auto Update From a Remote Server] がオフの場合、すべてのフィールドはディセーブルとなり、クリアされます。このオンとオフを切り替えると、他のすべての設定が失われます。

- [Remote Server Settings]：リモート サーバ用に次のオプションを指定できます。
  - [IP Address]：リモート サーバの IP アドレスを示します。
  - [File Copy Protocol]：FTP または SCP のどちらを使用するかを指定します。
  - [Directory]：リモート サーバ上のアップデートへのパスを示します。
  - [Username]：リモート サーバのユーザ アカウントに対応するユーザ名を示します。
  - [Password]：リモート サーバのユーザ アカウントのパスワードを示します。
  - [Confirm Password]：リモート サーバのパスワードの再入力を強制することで、パスワードを確定します。
- [Enable Signature and Engine Updates from Cisco.com]：センサーが Cisco.com にアクセスして、シグニチャのアップデートとエンジンのアップデートをダウンロードできるようにします。
- [Cisco.com Server Settings]：Cisco.com サーバ用の次のオプションを指定できます。

  - [Username]：Cisco.com 上のユーザ アカウントに対応するユーザ名を示します。
  - [Cisco.com URL]：[Enable Signature and Engine Updates from Cisco.com] チェックボックスをオンにした場合、正しい URL が自動的に入力されます。
  - [Password]：Cisco.com 上のユーザ アカウントのパスワードを示します。
  - [Confirm Password]：Cisco.com のパスワードの再入力を強制することで、パスワードを確定します。
- [Schedule]：次のスケジュール オプションを指定できます。
  - [Start Time]：アップデート プロセスの開始時間を示します。これは、センサーがリモート サーバにアクセスし、使用可能なアップデートを検索する時間です。
  - [Frequency]：時間または週単位のどちらでアップデートを実行するかを指定します。

    [Hourly]：n 時間ごとにアップデートをチェックするように指定します。

    [Daily]：アップデートを実行する曜日を指定します。

Auto Update の設定

リモート サーバまたは Cisco.com から自動アップデートを設定するには、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* > [Sensor Management] > [Auto/Cisco.com Update] を選択します。

ステップ 3　リモート サーバからの自動アップデートをイネーブルにするには、[Enable Auto Update from a Remote Server] チェックボックスをオンにします。

a. [IP Address] フィールドに、アップデートをダウンロードして格納したリモート サーバの IP アドレスを入力します。

b. リモート サーバへの接続に使用するプロトコルを指定するには、[File Copy Protocol] ドロップダウン リストから FTP または SCP を選択します。

c. [Directory] フィールドに、アップデートが置かれるリモート サーバ上のディレクトリへのパスを入力します。パスの有効な値は、1 ～ 128 文字です。

d. [Username] フィールドに、リモート サーバにログインする際に使用するユーザ名を入力します。ユーザ名の有効な値は、1 ～ 2047 文字です。

e. [Password] フィールドに、リモート サーバのユーザ名のパスワードを入力します。パスワードの有効な値は、1 ～ 2047 文字です。

f. 確認のために [Confirm Password] フィールドにもう一度パスワードを入力します。

g. 時間単位のアップデートの場合は、[Hourly] チェックボックスをオンにして、次の手順を実行します。

- [Start Time] フィールドに、アップデートを開始する時刻を入力します。有効な値は、hh:mm:ss です。
- [Every_hours] フィールドに、各アップデートが行われる時間間隔を入力します。有効な値は 1 ～ 8760 です。

  たとえば、5 と入力すると、センサーは 5 時間ごとにサーバ上のファイルのディレクトリを確認します。更新があれば、ダウンロードし、インストールします。更新可能なものが複数ある場合でも、1 回にインストールされる更新は 1 つだけです。センサーはインストール可能な最新のアップデートを特定し、そのファイルをインストールします。

h. 週単位のアップデートの場合は、[Daily] チェックボックスをオンにして、次の手順を実行します。

- [Start Time] フィールドに、アップデートを開始する時刻を入力します。有効な値は、hh:mm:ss です。
- [Days] フィールドで、センサーが使用可能なアップデートをチェックしてダウンロードする曜日をオンにします。

ステップ 4　Cisco.com からのシグニチャ アップデートとシグニチャ エンジン アップデートをイネーブルにするには、[Enable Signature and Engine Updates from Cisco.com] チェックボックスをオンにします。

a. [Username] フィールドに、Cisco.com にログインするときに使用するユーザ名を入力します。ユーザ名の有効な値は、1 ～ 2047 文字です。

b. [Password] フィールドに、Cisco.com のユーザ名パスワードを入力します。パスワードの有効な値は、1 ～ 2047 文字です。

c. 確認のために [Confirm Password] フィールドにもう一度パスワードを入力します。

d. 時間単位のアップデートの場合は、[Hourly] チェックボックスをオンにして、次の手順を実行します。

- [Start Time] フィールドに、アップデートを開始する時刻を入力します。有効な値は、hh:mm:ss です。
- [Every_hours] フィールドに、各アップデートが行われる時間間隔を入力します。有効な値は 1 ～ 8760 です。

  たとえば、5 と入力すると、センサーは 5 時間ごとにサーバ上のファイルのディレクトリを確認します。更新があれば、ダウンロードし、インストールします。更新可能なものが複数ある場合でも、1 回にインストールされる更新は 1 つだけです。センサーはインストール可能な最新のアップデートを特定し、そのファイルをインストールします。

e. 週単位のアップデートの場合は、[Daily] チェックボックスをオンにして、次の手順を実行します。

- [Start Time] フィールドに、アップデートを開始する時刻を入力します。有効な値は、hh:mm:ss です。
- [Days] フィールドで、センサーが使用可能なアップデートをチェックしてダウンロードする曜日をオンにします。

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　[Apply] をクリックして変更内容を保存します。

センサーの手動アップデート

ここでは、センサーの手動アップデート方法について説明します。内容は次のとおりです。

- 「[Update Sensor] ペイン」（P.18-21）
- 「[Update Sensor] ペインのフィールド定義」（P.18-21）
- 「センサーのアップデート」（P.18-21）

[Update Sensor] ペイン

（注）　[Update Sensor] ペインを表示して、サービス パックとシグニチャのアップデートでセンサーを更新するには、管理者である必要があります。

[Update Sensor] ペインでは、サービス パックとシグニチャのアップデートを即座に適用できます。センサーを手動で更新するには、サービス パックとシグニチャのアップデートを Cisco.com から FTP サーバにダウンロードし、それらを FTP サーバからセンサーにダウンロードするように設定する必要があります。

詳細情報

- シグニチャのアップデートおよびそれらのインストールに要する時間については、「シグニチャのアップデートおよびインストール時間」（P.18-17）を参照してください。
- Cisco.com でソフトウェア ファイルを取得する手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。

[Update Sensor] ペインのフィールド定義

[Update Sensor] ペインには次のフィールドがあります。

- [Update is located on a remote server and is accessible by the sensor]：次のオプションを指定できます。
  - [URL]：アップデートが置かれているサーバのタイプを示します。FTP、HTTP、HTTPS、または SCP のどれを使用するかを指定します。
  - [://]：リモート サーバ上のアップデートへのパスを示します。
  - [Username]：リモート サーバのユーザ アカウントに対応するユーザ名を示します。
  - [Password]：リモート サーバのユーザ アカウントのパスワードを示します。
- [Update is located on this client]：次のオプションを指定できます。
  - [Local File Path]：このローカル クライアントでのアップデート ファイルへのパスを示します。
  - [Browse Local]：このローカル クライアントのファイル システムの [Browse] ダイアログボックスを開きます。このダイアログボックスから、アップデート ファイルに移動できます。

センサーのアップデート

（注）　センサーを手動で更新するには、サービス パックとシグニチャのアップデートを Cisco.com から FTP サーバにダウンロードし、それらを FTP サーバからセンサーにダウンロードするように設定する必要があります。

サービス パックとシグニチャのアップデートをすぐに適用するには、次の手順を実行します。

ステップ 1　管理者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* > [Sensor Management] > [Update Sensor] を選択します。

ステップ 3　リモート サーバからアップデートを取得して、センサーにインストールするには、次の手順を実行します。

a. [Update is located on a remote server and is accessible by the sensor] チェックボックスをオンにします。

b. [URL] フィールドには、アップデートのある URL を入力します。

次の URL タイプがサポートされています。

- [FTP:] : FTP ネットワーク サーバのソース URL。
  このプレフィクスの構文は次のとおりです。
  `ftp://location/relative_directory/filename`

  または
  `ftp://location//absolute_directory/filename`

- [HTTPS:] : ウェブ サーバのソース URL。
  このプレフィクスの構文は次のとおりです。
  `https://location/directory/filename`

  （注）　HTTPS プロトコルを使用し始める前に、TLS の信頼できるホストを設定します。

- [SCP:] : SCP ネットワーク サーバのソース URL。
  このプレフィクスの構文は次のとおりです。
  `scp://location/relative_directory/filename`

  または
  `scp://location/absolute_directory/filename`

- [HTTP:] : Web サーバのソース URL です。
  このプレフィクスの構文は次のとおりです。
  `http://location/directory/filename`

  次の例は、FTP プロトコルを示しています。
  `ftp://user@ip_address/UPDATES/file_name.rpm.pkg`

  （注）　アップデートをあらかじめ Cisco.com からダウンロードし、FTP サーバに保存しておく必要があります。

c. [Username] フィールドに、リモート サーバのアカウントのユーザ名を入力します。

d. [Password] フィールドに、リモート サーバのこのアカウントに関連付けられているパスワードを入力します。

ステップ 4　ローカル クライアントからプッシュして、センサーにインストールするには、次の手順を実行します。

a. [Update is located on this client] チェックボックスをオンにします。

b. ローカル クライアントのアップデート ファイルへのパスを指定するか、[Browse Local] をクリックして、ローカル クライアントのファイルを検索します。

ステップ 5　[Update Sensor] をクリックします。[Update Sensor] ダイアログボックスに、更新すると、センサーとの接続が失われ、再ログインが必要になることを伝えるメッセージが表示されます。

ステップ 6　[OK] をクリックして、センサーを更新します。

（注）　サービス パック、マイナー、メジャー、およびエンジニアリング パッチのアップデート中は、IME および CLI 接続が失われます。これらのアップデートの 1 つを適用している場合、インストーラにより IPS アプリケーションが再起動されます。センサーをリブートできます。シグニチャのアップデートの場合、接続は失われないので、システムをリブートする必要はありません。

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

詳細情報

Cisco.com でソフトウェア ファイルを取得する手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。

デフォルトの復元

（注）　[Restore Defaults] ペインを表示して、センサーのデフォルトを復元するには、管理者である必要があります。

[Restore Defaults] ペインでは、センサーにいつでもデフォルトの設定を復元できます。

警告　**デフォルトを復元すると、現在のアプリケーションの設定が削除され、デフォルト設定が復元されます。ネットワーク設定もデフォルトに戻り、センサーとの接続もただちに失われます。**

デフォルトの設定を復元するには、次の手順を実行します。

ステップ 1　管理者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* > [Sensor Management] > [Restore Defaults] を選択します。

ステップ 3　デフォルト設定を復元するには、[Restore Defaults] をクリックします。

ステップ 4　[Restore Defaults] ダイアログボックスで [OK] をクリックします。

（注）　デフォルトを復元すると、IP アドレス、ネットマスク、デフォルト ゲートウェイ、およびアクセス リストがリセットされます。パスワードと時間はリセットされません。手動および自動ブロックも有効なままになります。手動でセンサーをリブートする必要があります。

センサーのリブート

（注）　[Reboot Sensor] ペインを表示して、センサーをリブートするには、管理者である必要があります。

[Reboot Sensor] ペインからセンサーのシャットダウンと再起動を行うことができます。

センサーをリブートするには、次の手順を実行します。

ステップ 1　管理者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 Management] > [Reboot Sensor] を選択し、[Reboot Sensor] をクリックします。

ステップ 3　センサーをシャットダウンして再起動するには、[OK] をクリックします。センサー アプリケーションがシャットダウンされ、センサーがリブートされます。リブート後に、再ログインする必要があります。

（注）　CLI にログインしているユーザに対して、センサー アプリケーションがシャットダウンされることを伝えるメッセージが表示されてから、30 秒後にシャットダウンされます。

センサーのシャットダウン

（注）　[Shut Down Sensor] ペインを表示し、センサーをシャットダウンするには、管理者である必要があります。

センサーは、IPS アプリケーションをシャットダウンしたあとに安全に電源を切断できる状態になります。

センサーをシャットダウンするには、次の手順を実行します。

ステップ 1　管理者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* > [Sensor Management] > [Shut Down Sensor] を選択し、[Shut Down Sensor] をクリックします。

ステップ 3　[Shut Down Sensor] ダイアログボックスで [OK] をクリックします。センサー アプリケーションがシャットダウンされ、センサーに開かれている接続が閉じます。

（注）　CLI にログインしているユーザに対して、センサー アプリケーションがシャットダウンされることを伝えるメッセージが表示されてから、30 秒後にシャットダウンされます。

CHAPTER 19

センサーのモニタリング

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

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

IME を使用すると、パフォーマンス、統計情報、接続を含む、センサーのすべての側面をモニタできます。また、拒否攻撃者やイベントの一覧を表示することもできます。IP ロギングの設定、ホストとネットワーク ブロックの設定、レート制限の設定と管理を行うことができます。OS ID と異常検出をモニタできます。ここでは、センサーのモニタ方法について説明します。内容は次のとおりです。

イベントのモニタリング

ここでは、センサー上のイベント データのフィルタおよび表示方法について説明します。内容は次のとおりです。

[Events] ペイン

[Events] ペインでは、イベント データをフィルタおよび表示できます。イベント、時間、またはその両方に基づいて、イベントをフィルタリングできます。デフォルトでは、過去 1 時間のすべてのアラートとエラー イベントが表示されます。これらのイベントにアクセスするには、[View] をクリックします。

[View] をクリックすると、まだ時間範囲を設定していない場合、IME によりイベントの時間範囲が定義されます。範囲の終了時間を指定しないと、[View] をクリックした時間に定義されます。

多数のイベントをセンサーから取得するときのシステム エラーを防ぐため、IME では、一度に表示できるイベントの数が制限されています（ページあたりの最大行数は 500 です）。他のイベントを表示するには [Back] および [Next] をクリックします。

[Events] ペインのフィールド定義

[Events] ペインには次のフィールドがあります。

- [Show Alert Events]：表示するアラートのレベルを設定できます。
  - [Informational]
  - [Low]
  - [Medium]
  - [High]

  デフォルトでは、すべてのレベルがイネーブルになっています。
- [Threat Rating (0-100)]：脅威レーティングの値の範囲（最小および最大レベル）を変更できます。
- [Show Error Events]：表示するエラーの種類を設定できます。
  - [Warning]
  - [Error]
  - [Fatal]

  デフォルトでは、すべてのレベルがイネーブルになっています。
- [Show Attack Response Controller events]：ARC（旧称 Network Access Controller）イベントを表示します。デフォルトはディセーブルです。

  （注）　NAC は ARC と呼ばれていますが、Cisco IPS では、IME と CLI 全体での名称変更が完了していません。
- [Show status events]：ステータス イベントを表示します。デフォルトはディセーブルです。
- [Select the number of the rows per page]：ページあたりに表示する行数を指定できます。有効な範囲は 100 ～ 500 です。デフォルトは 100 です。

- [Show all events currently stored on the sensor]：センサーに格納されているすべてのイベントを取得します。
- [Show past events]：指定した時間または分だけ戻って以前のイベントを表示します。
- [Show events from the following time range]：指定した時間範囲のイベントを取得します。

詳細情報

脅威レーティングの詳細については、「脅威レーティングの概要」（P.11-4）を参照してください。

[Event Viewer] ペインのフィールド定義

[Event Viewer] ペインには次のフィールドがあります。

- [#]: 結果クエリー内のイベントの順序番号を示します。
- [Type]：イベントの種類（Error、NAC、Status、Alert）を示します。
- [Sensor UTC Time]：イベントが発生した日時を示します。
- [Sensor Local Time]：センサーのローカル時刻。
- [Event ID]：センサーによりイベントに割り当てられた数値 ID。
- [Events]：イベントの簡単な説明。
- [Sig ID]：アラート イベントを発生しその原因となったシグニチャを示します。
- [Performed Actions]：センサーが実行したアクション。

イベント表示の設定

イベントの表示方法を設定するには、次の手順を実行します。

ステップ 1　IME にログインします。

ステップ 2　[Configuration] > *sensor_name* > [Sensor Monitoring] > [Events] の順に選択します。

ステップ 3　[Show Alert Events] で、表示するアラートのレベルのチェックボックスをオンにします。

ステップ 4　[Threat Rating] フィールドに、脅威レーティングの最小および最大範囲を入力します。

ステップ 5　[Show Error Events] で、表示するエラーの種類のチェックボックスをオンにします。

ステップ 6　ARC（旧称 Network Access Controller）イベントを表示するには、[Show Attack Response Controller events] チェックボックスをオンにします。

ステップ 7　ステータス イベントを表示するには、[Show status events] チェックボックスをオンにします。

ステップ 8　[Select the number of the rows per page] フィールドに、ページあたりに表示する行の数を入力します。デフォルトは 100 です。値は 100、200、300、400、または 500 です。

ステップ 9　表示するイベントの時刻を設定するには、次のいずれかのオプション ボタンをクリックします。

- **[Show all events currently stored on the sensor]**
- **[Show past events]**：以前のイベントを表示するために戻る時間と分を入力します。
- **[Show events from the following time range]**：開始時刻と終了時刻を入力します。

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 10　[View] をクリックして設定したイベントを表示します。

ステップ 11　列内で上下にソートするには、右側をクリックして上下の矢印を表示します。

ステップ 12　100 個ずつページを移動するには [Next] または [Back] をクリックします。

ステップ 13　イベントの詳細を表示するには、[Details] をクリックします。イベントの詳細が別のダイアログボックスに表示されます。ダイアログボックスのタイトルはイベント ID になります。

イベント ストアのクリア

イベント ストアをクリアするには、**clear events** コマンドを使用します。

イベント ストアからイベントをクリアするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　イベント ストアをクリアします。

```
sensor# clear events
Warning: Executing this command will remove all events currently stored in the event
store.
Continue with clear? []:
```

ステップ 3　**yes** と入力してイベントをクリアします。

拒否攻撃者の設定とモニタリング

ここでは、拒否攻撃者リストをモニタする方法について説明します。内容は次のとおりです。

- 「[Denied Attackers] ペイン」（P.19-4）
- 「[Denied Attackers] ペインのフィールド定義」（P.19-5）
- 「拒否攻撃者リストのモニタリングと拒否攻撃者の追加」（P.19-5）

[Denied Attackers] ペイン

（注）　拒否攻撃者リストをモニタおよびクリアするには、管理者である必要があります。

[Denied Attackers] ペインには、拒否攻撃者のすべての IP アドレスとヒット カウントが表示されます。すべての IP アドレスのヒット カウントをリセットするか、拒否攻撃者のリストをクリアできます。また、モニタ対象の拒否攻撃者を設定することもできます。

（注）　リセットとクリアはテーブル中のすべての項目に適用されます。

[Denied Attackers] ペインのフィールド定義

[Denied Attackers] ペインには次のフィールドがあります。

- [Virtual Sensor]：攻撃者を拒否している仮想センサー。

（注）　AIM IPS、AIP SSC-5、および NME IPS では仮想化がサポートされていません。

- [Attacker IP]：センサーが拒否している攻撃者の IP アドレス。
- [Victim IP]：センサーが拒否している攻撃対象の IP アドレス。
- [Port]：センサーが拒否しているホストのポート。
- [Protocol]：攻撃者が使用しているプロトコル。
- [Requested Percentage]：インライン モードのセンサーによって拒否するよう設定したトラフィックのパーセンテージ。
- [Actual Percentage]：センサーが実際に拒否しているインライン モードのトラフィックのパーセンテージ。

（注）　センサーは要求されたパーセンテージに正確に一致するように拒否しようとしますが、パーセンテージの小数部のため、要求されたしきい値を下回ることがあります。

- [Hit Count]：その拒否攻撃者のヒット カウントを表示します。

拒否攻撃者リストのモニタリングと拒否攻撃者の追加

拒否攻撃者のリストおよびそのヒットカウントの表示、拒否攻撃者の追加と削除、拒否攻撃者リストのクリア、ヒット カウントのリセットを行うには、次の手順を実行します。

ステップ 1　管理者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* > [Sensor Monitoring] > [Time-Based Actions] > [Denied Attackers] の順に選択します。

ステップ 3　リストを更新するには、[Refresh] をクリックします。

ステップ 4　拒否攻撃者のリスト全体をクリアするには、[Clear List] をクリックします。

ステップ 5　すべての拒否攻撃者についてヒット カウントを最初からやり直すには、[Reset All Hit Counts] をクリックします。

ステップ 6　拒否攻撃者をモニタ対象リストに追加するには [Add] をクリックします。

ステップ 7　[Attacker IP] フィールドに、攻撃者の IP アドレスを入力します。

（注）　IPv4 および IPv6 IP アドレスを入力できます。

ステップ 8　[Specify Victim Address or Port] チェックボックスをオンにし、IP アドレスとポート番号を入力します。

ステップ 9　[Specify Virtual Sensor] チェックボックスをオンにし、ドロップダウン リストから仮想センサーを選択します。

ヒント　変更内容を破棄して [Denied Attackers] ペインに戻るには、[Cancel] をクリックします。

ステップ 10　[OK] をクリックして変更を保存します。拒否攻撃者が [Denied Attacker] リストに表示されます。

ステップ 11　リストから拒否攻撃者を削除するには、そのエントリを選択し、次に [Delete] をクリックします。

ホスト ブロックの設定

ここではホスト ブロックの設定方法について説明します。内容は次のとおりです。

[Host Blocks] ペイン

（注）　アクティブ ホスト ブロックを設定するには、管理者またはオペレータであることが必要です。

ホストのブロックを設定および管理するには、[Host Blocks] ペインを使用します。ホスト ブロックは、特定のホストからのトラフィックを永続的（ブロックを削除するまで）または指定した期間拒否します。接続に対するブロックは、宛先 IP アドレス、宛先プロトコル、ポートで指定できます。ホスト ブロックはその送信元 IP アドレスで定義します。既存のブロックと同じ送信元 IP アドレスのブロックを追加した場合、新しいブロックで古いブロックが上書きされます。

ブロックの期間を指定する場合、値の範囲は 1 ～ 70560 分（49 日間）です。期間を指定しない場合、ホスト ブロックは、センサーを再起動するかブロックを削除するまで有効なままになります。

（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。

[Host Block] ペインのフィールド定義

[Host Blocks] ペインには次のフィールドがあります。

- [Source IP]：ブロックの送信元 IP アドレス。
- [Destination IP]：ブロックの宛先 IP アドレス。
- [Destination Port]：ブロックの宛先ポート。
- [Protocol]：プロトコルの種類（TCP、UDP、または ANY）。デフォルトは ANY です。
- [Minutes Remaining]：ブロックの残り時間（分単位）。

- [Timeout (minutes)]：ブロックの元のタイムアウト値（分単位）。有効な値の範囲は 1 ～ 70560 分（49 日間）です。
- [VLAN]：シグニチャを発生したデータを伝送した VLAN を示します。

（注）　ブロック要求に VLAN ID が含まれていますが、セキュリティ アプライアンスには渡されません。管理コンテキストにログインしている場合、センサーは FWSM 2.1 以降をブロックできません。

- [Connection Block Enabled]：ホストの接続をブロックするかどうか。

（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。

[Add Host Block] ダイアログボックスのフィールド定義

[Add Active Host Block] ダイアログボックスには次のフィールドがあります。

- [Source IP]：ブロックの送信元 IP アドレス。
- [Enable connection blocking]：ホストの接続をブロックするかどうか。
- [Connection Blocking]：接続ブロックのパラメータを設定できます。
  - [Destination IP]：ブロックの宛先 IP アドレス。
  - [Destination Port (optional)]：ブロックの宛先ポート。
  - [Protocol (optional)]：プロトコルの種類（TCP、UDP、または ANY）。デフォルトは ANY です。

（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。

- [VLAN (optional)]：シグニチャを発生したデータを伝送した VLAN を示します。

（注）　ブロック要求に VLAN ID が含まれていますが、セキュリティ アプライアンスには渡されません。管理コンテキストにログインしている場合、センサーは FWSM 2.1 以降をブロックできません。

- [Enable Timeout]：ブロックのタイムアウト値を分単位で設定できます。
- [Timeout]：ブロックを継続する時間（分単位）。有効な値の範囲は 1 ～ 70560 分（49 日間）です。
- [No Timeout]：ブロックのタイムアウトを設定しないことを選択できます。

ホスト ブロックの追加、削除、管理

ホスト ブロックを追加、削除、および管理するには、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* > [Sensor Monitoring] > [Time-Based Actions] > [Host Blocks] の順に選択し、[Add] をクリックしてホスト ブロックを追加します。

ステップ 3　[Source IP] フィールドに、ブロックするホストの送信元 IP アドレスを入力します。

ステップ 4　接続ベースのブロックを行うには、[Enable Connection Blocking] チェックボックスをオンにします。

（注）　接続ブロックは、特定の送信元 IP アドレスから特定の宛先 IP アドレスおよび宛先ポートへのトラフィックをブロックします。

（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。

a.　[Destination IP] フィールドに、宛先 IP アドレスを入力します。

b.　（任意）[Destination Port] フィールドに宛先ポートを入力します。

c.　（任意）[Protocol] ドロップダウン リストからプロトコルを選択します。

ステップ 5　（任意）[VLAN] フィールドに接続ブロックの VLAN を入力します。

ステップ 6　次のようにしてタイムアウトを設定します。

- 指定した期間についてブロックを設定するには、[Enable Timeout] オプション ボタンをクリックし、[Timeout] フィールドに時間を分単位で入力します。
- ブロックの期間を指定しない場合は、[No Timeout] オプション ボタンをクリックします。

ヒント　変更内容を破棄して [Add Host Block] 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　[Apply] をクリックします。新しいホスト ブロックが [Host Blocks] ペインのリストに表示されます。

ステップ 8　[Refresh] をクリックしてホスト ブロック リストの内容を更新します。

ステップ 9　ブロックを削除するには、リスト中でホスト ブロックを選択し、[Delete] をクリックします。[Delete Host Block] ダイアログボックスが開き、このブロックを削除してよいかどうかを確認するメッセージが表示されます。

ヒント　変更内容を破棄して [Delete Host Block] 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 10　ブロックを削除するには [Yes] をクリックします。ホスト ブロックが [Host Blocks] ペインのリストに表示されなくなります。

ネットワーク ブロックの設定

ここではネットワーク ブロックの設定方法について説明します。内容は次のとおりです。

[Network Blocks] ペイン

（注）　ネットワーク ブロックを設定するには、管理者またはオペレータであることが必要です。

ネットワークのブロックを設定および管理するには、[Network Blocks] ペインを使用します。ネットワーク ブロックは、特定のネットワークからのトラフィックを永続的（ブロックを削除するまで）または指定した期間拒否します。ネットワーク ブロックは、その送信元 IP アドレスとネットマスクで定義します。ネットマスクはブロックされるサブネットを定義します。ホスト サブネット マスクも指定できます。

ブロックの期間を指定する場合、値の範囲は 1 ～ 70560 分（49 日間）です。期間を指定しない場合、ブロックは、センサーを再起動するかブロックを削除するまで有効なままになります。

（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。

[Network Blocks] ペインのフィールド定義

[Network Blocks] ペインには次のフィールドがあります。

- [IP Address]：ブロックの IP アドレス。
- [Mask]：ブロックのネットワーク マスク。
- [Minutes Remaining]：ブロックの残り時間（分単位）。
- [Timeout (minutes)]：ブロックの元のタイムアウト値（分単位）。有効な値の範囲は 1 ～ 70560 分（49 日間）です。

[Add Network Block] ダイアログボックスのフィールド定義

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

- [Source IP]：ブロックの IP アドレス。
- [Netmask]：ブロックのネットワーク マスク。
- [Enable Timeout]：ブロックのタイムアウト値を分単位で指定します。

- [Timeout]：ブロック期間を分単位で指定します。有効な値の範囲は 1 ～ 70560 分（49 日間）です。
- [No Timeout]：ブロックのタイムアウトを設定しないことを選択できます。

ネットワーク ブロックの追加、削除、管理

（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。

ネットワーク ブロックを追加、削除、および管理するには、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* > [Sensor Monitoring] > [Time-Based Actions] > [NetworkBlocks] の順に選択し、[Add] をクリックしてネットワーク ブロックを追加します。

ステップ 3　[Source IP] フィールドに、ブロックするネットワークの送信元 IP アドレスを入力します。

ステップ 4　[Netmask] ドロップダウン リストから、ネットマスクを選択します。

ステップ 5　次のようにしてタイムアウトを設定します。

- 指定した期間についてブロックを設定するには、[Enable Timeout] オプション ボタンをクリックし、[Timeout] フィールドに時間を分単位で入力します。
- ブロックの期間を指定しない場合は、[No Timeout] オプション ボタンをクリックします。

ヒント　変更内容を元に戻して [Add Network Block] 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　[Apply] をクリックします。ブロックがすでに追加されている場合、エラー メッセージが表示されます。新しいネットワーク ブロックが [Network Blocks] ペインのリストに表示されます。

ステップ 7　[Refresh] をクリックしてネットワーク ブロック リストの内容を更新します。

ステップ 8　リスト中でネットワーク ブロックを選択し、[Delete] をクリックしてそのブロックを削除します。[Delete Network Block] ダイアログボックスで、このブロックを削除してよいかどうかを質問されます。

ステップ 9　ブロックを削除するには [Yes] をクリックします。ネットワーク ブロックが [Network Blocks] ペインのリストに表示されなくなります。

レート制限の設定

ここでは、レート制限の設定および管理方法について説明します。内容は次のとおりです。

- 「[Add Rate Limit] ダイアログボックスのフィールド定義」（P.19-11）
- 「レート制限の追加、削除、管理」（P.19-12）

[Rate Limits] ペイン

（注）　レート制限を追加するには、管理者であることが必要です。

レート制限を設定および管理するには [Rate Limits] ペインを使用します。レート制限は、ネットワーク デバイス インターフェイス上で許可される、指定した種類のトラフィックの量を、最大帯域幅キャパシティの特定のパーセンテージに制限します。このパーセンテージを超えるトラフィックは、ネットワーク デバイスによってドロップされます。レート制限は、指定したターゲット ホストへのトラフィックや、設定したインターフェイスまたは方向に通過するすべてのトラフィックを制限できます。レート制限は、永続的に使用するか、指定した期間使用できます。レート制限は、プロトコル、オプションの宛先アドレス、オプションのデータ値で識別されます。

レート制限はパーセンテージで指定されるため、帯域幅容量が異なるインターフェイス上では、実際に異なる制限に変換されます。レート制限パーセント値は、1 ～ 100 の間の整数であることが必要です。

[Rate Limits] ペインのフィールド定義

[Rate Limits] ペインには次のフィールドがあります。

- [Protocol]：レート制限されるトラフィックのプロトコル。
- [Rate]：レート制限されるトラフィックに許可される最大帯域幅のパーセンテージ。この制限を超える一致トラフィックはドロップされます。
- [Source IP]：レート制限されるトラフィックの、送信元ホストの IP アドレス。
- [Source Port]：レート制限されるトラフィックの送信元ホスト ポート。
- [Destination IP]：レート制限されるトラフィックの、宛先ホストの IP アドレス。
- [Destination Port]：レート制限されるトラフィックの宛先ホスト ポート。
- [Data]：指定したプロトコルについて、より正確にトラフィックを限定するための、追加の識別情報。たとえば、echo-request は、ICMP プロトコル トラフィックをレート制限された ping に絞り込みます。
- [Minutes Remaining]：レート制限が有効な残り時間（分単位）。
- [Timeout (minutes)]：このレート制限の合計時間（分単位）。

[Add Rate Limit] ダイアログボックスのフィールド定義

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

- [Protocol]：レート制限されるトラフィックのプロトコル（ICMP、TCP、または UDP）。
- [Rate]（1-100）：レート制限されるトラフィックに許可される最大帯域幅のパーセンテージ。
- [Source IP]（任意）：レート制限されるトラフィックの、送信元ホストの IP アドレス。
- [Source Port]（任意）：レート制限されるトラフィックの、送信元ホストのポート。
- [Destination IP]（任意）：レート制限されるトラフィックの、宛先ホストの IP アドレス。

- [Destination Port]（任意）：レート制限されるトラフィックの、宛先ホストのポート。
- [Use Additional Data]：echo-reply、echo-request、halfOpenSyn などの追加データを指定するかどうかを選択できます。
- [Timeout]：タイムアウトをイネーブルにするかどうかを選択できます。
  - [No Timeout]：タイムアウトはイネーブルになっていません。
  - [Enable Timeout]：タイムアウトを分単位で指定できます（1 ～ 70560）。

レート制限の追加、削除、管理

レート制限を追加、削除、および管理するには、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* > [Sensor Monitoring] > [Time-Based Actions] > [Rate Limits] の順に選択し、[Add] をクリックしてレート制限を追加します。

ステップ 3　[Protocol] ドロップダウン リストから、レート制限するプロトコル（ICMP、TCP、または UDP）を選択します。

ステップ 4　[Rate] フィールドに、レート制限のパーセンテージ（1 ～ 100）を入力します。

ステップ 5　（任意）[Source IP] フィールドに、送信元 IP アドレスを入力します。

ステップ 6　（任意）[Source Port] フィールドに、送信元ポートを入力します。

ステップ 7　（任意）[Destination IP] フィールドに、宛先 IP アドレスを入力します。

ステップ 8　（任意）[Destination Port] フィールドに宛先ポートを入力します。

ステップ 9　（任意）追加のデータを使用するようにレート制限を設定するには、[Use Additional Data] チェックボックスをオンにします。

ステップ 10　[Select Data] ドロップダウン リストから、追加データ（echo-reply、echo-request、または halfOpenSyn）を選択します。

ステップ 11　次のようにしてタイムアウトを設定します。

- レート制限の期間を指定しない場合は、[No Timeout] オプション ボタンをクリックします。
- タイムアウトを分単位で指定するには、[Enable Timeout] オプション ボタンをクリックし、[Timeout] フィールドに期間（分単位で 1 ～ 70560）を入力します。

ヒント　変更内容を破棄して [Add Rate Limit] 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 12　[Apply] をクリックします。新しいレート制限が [Rate Limits] ペインのリストに表示されます。

ステップ 13　[Refresh] をクリックして [Rate Limits] リストの内容を更新します。

ステップ 14　レート制限を削除するには、リストからレート制限を選択し、[Delete] をクリックします。[Delete Rate Limit] ダイアログボックスで、このレート制限を削除してよいかどうかを質問されます。

ヒント　[Delete Rate Limit] ダイアログボックスを閉じるには、[No] をクリックします。

ステップ 15　レート制限を削除するには [Yes] をクリックします。レート制限はレート制限リストに表示されなくなります。

詳細情報

シグニチャにアクションを割り当てる手順については、「シグニチャへのアクションの割り当て」（P.9-19）を参照してください。

IP ロギングの設定

ここでは、IP ロギング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。

IP ロギングについて

注意　IP ロギングを有効にすると、システムのパフォーマンスが低下します。

最も単純な IP ロギングは IP アドレスで構成されます。IP アドレスで指定したホストに関連するすべての IP トラフィックをキャプチャするように、センサーを設定できます。センサーは、この IP アドレスを含まれている最初のパケットを検出するとすぐに収集を開始し、設定したパラメータに従って収集を続けます。その IP アドレスで IP トラフィックをログに記録する時間（分単位）、パケットの数、バイト数などを指定できます。指定したパラメータが 1 つでも該当した時点で、センサーは IP トラフィックのロギングを停止します。

ログ ファイルは、次の 3 つの状態のいずれかになります。

- [Added] : IP ロギングが追加されている場合
- [Started] : センサーが最初のパケットを検出すると、ログ ファイルがオープンされ Started 状態になります。
- [Completed] : IP ロギングの制限に達した場合。

3 つの状態すべてのファイルの数は 20 に制限されます。IP ログは、循環バッファに格納されます。循環バッファは、新しい IP ログによって古いログが上書きされるので、いっぱいになることがありません。

（注）　ログは、センサーによって再利用されるまでセンサー上に保持されます。センサー上の IP ログ ファイルを管理することはできません。

IP ログ ファイルを WireShark や TCPDUMP などのスニフィング ツールで表示するために、FTP または SCP サーバにコピーすることができます。ファイルは、PCAP バイナリ形式で、pcap ファイル拡張子付きで保存されます。

[IP Logging] ペイン

（注）　IP ロギングを設定するには、管理者であることが必要です。

[IP Logging] ペインには、システム上でダウンロード可能なすべての IP ログが表示されます。IP ログは、2 通りの方法で生成されます。

- [Add IP Logging] ダイアログボックスで IP ログを追加した場合
- シグニチャのイベント アクションとして次のいずれかを選択した場合
  - Log Attacker Packets
  - Log Pair Packets
  - Log Victim Packets

  このシグニチャに基づく攻撃をセンサーが検出したときに、IP ログが作成されます。IP ログをトリガーしたイベント アラートが IP ロギング テーブルに表示されます。

[IP Logging] ペインのフィールド定義

[IP Logging] ペインには次のフィールドがあります。

- [Log ID]：IP ログの ID。
- [Virtual Sensor]：IP ログが関連付けられている仮想センサー。

  （注）　AIM IPS、AIP SSC-5、および NME IPS では仮想化がサポートされていません。

- [IP Address]：ログがキャプチャされているホストの IP アドレス。
- [Status]：IP ログのステータス。有効な値は、added、started、または completed です。
- [Start Time]：最初にキャプチャされたパケットのタイムスタンプ。
- [Current End Time]：最後にキャプチャされたパケットのタイムスタンプ。キャプチャが完了していない場合、タイムスタンプはありません。
- [Alert ID]：IP ログをトリガーしたイベント アラートが存在する場合、その ID。
- [Packets Captured]：現在キャプチャされたパケット数。
- [Bytes Captured]：現在キャプチャされたバイト数。

[Add IP Logging] および [Edit IP Logging] ダイアログボックスの定義

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

- [Virtual Sensor]：IP ログをキャプチャする仮想センサーを選択できます。

  （注）　AIM IPS、AIP SSC-5、および NME IPS では仮想化がサポートされていません。

- [IP Address]：ログがキャプチャされているホストの IP アドレス。

  （注）　IPv4 および IPv6 IP アドレスを入力できます。

- [Maximum Values]：IP ロギングの値を設定できます。
  - [Duration]：パケットをキャプチャする最大期間。指定できる範囲は 1 ～ 60 分です。デフォルトは 10 分です。

    （注）　[Edit IP Logging] ダイアログボックスの場合、[Duration] フィールドは、編集内容を IP ロギングに適用した後で延長される時間です。

  - [Packets]（任意）：キャプチャする最大パケット数。範囲は 0 ～ 4294967295 パケットです。
  - [Bytes]（任意）：キャプチャする最大バイト数。有効な範囲は 0 ～ 4294967295 バイトです。

IP ロギングの設定

特定のホストの IP トラフィックを記録するには、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* > [Sensor Monitoring] > [Time-Based Actions] > [IP Logging] の順に選択し、[Add] をクリックします。

ステップ 3　[Virtual Sensor] ドロップダウン リストから、IP ロギングを有効にする仮想センサーを選択します。

ステップ 4　[IP Address] フィールドに、IP ログのキャプチャ元ホストの IP アドレスを入力します。すでに存在し Added または Started 状態のキャプチャを追加しようとすると、エラー メッセージが表示されます。

（注）　IPv4 および IPv6 IP アドレスを入力できます。

ステップ 5　[Duration] フィールドに、IP ログをキャプチャする時間（分単位）を入力します。指定できる範囲は 1 ～ 60 分です。デフォルトは 10 分です。

ステップ 6　（任意）[Packets] フィールドに、キャプチャするパケット数を入力します。範囲は 0 ～ 4294967295 パケットです。

ステップ 7　（任意）[Bytes] フィールドに、キャプチャするバイト数を入力します。範囲は 0 ～ 4294967295 パケットです。

ヒント　変更内容を破棄して [Add IP Log] 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　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。IP ログが、ログ ID とともに [IP Logging] ペインのリストに表示されます。

ステップ 9　リスト中の既存のログ エントリを編集するには、エントリを選択して [Edit] をクリックします。

ステップ 10　[Duration] フィールドで、パケットをキャプチャする時間（分単位）を編集します。

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。編集した IP ログが、[IP Logging] ペインのリストに表示されます。

ステップ 12　IP ロギングを停止するには、停止するログのログ ID を選択し、[Stop] をクリックします。

ステップ 13　[OK] をクリックしてそのログの IP ロギングを停止します。

ステップ 14　IP ログをダウンロードするには、ログ ID を選択し、[Download] をクリックします。

ステップ 15　ログをローカル マシンに保存します。WireShark を使用してログを表示できます。

異常検出 KB のモニタリング

（注）　AIP SSC-5 は異常検出をサポートしていません。

ここでは、異常検出 KB の使用方法について説明します。内容は次のとおりです。

[Anomaly Detection] ペイン

（注）　AIP SSC-5 は異常検出をサポートしていません。

（注）　異常検出 KB をモニタするためには、管理者であることが必要です。

[Anomaly Detection] ペインには、すべての仮想センサーの KB が表示されます。[Anomaly Detection] ペインで、次のアクションを実行できます。

- 特定の KB のしきい値の表示
- KB の比較
- KB のロード
- KB を現在の KB にする
- KB の名前変更
- KB のダウンロード
- KB のアップロード

- 特定の KB またはすべての KB の削除

（注）　[Anomaly Detection] ボタンは、リスト中の 1 つの行のみが選択されている場合にアクティブになります。例外は、2 つの行を選択できる [Compare KBs] の場合です。それ以外の数の行が選択されている場合、どのボタンもアクティブになりません。

KB について

KB はツリー構造になっており、次の情報が含まれています。

- KB 名
- ゾーン名
- Protocol
- サービス

KB には、スキャナしきい値とヒストグラムがサービスごとに保存されます。学習受け入れモードを自動に設定し、アクションを [Rotate] に設定した場合、新しい KB は 24 時間ごとに作成され、作成後 24 時間にわたり使用されます。学習受け入れモードを自動に設定し、アクションを [Save Only] に設定すると、新しい KB は作成されますが、現在の KB が使用されます。学習受け入れモードを自動に設定しない場合、KB は作成されません。

（注）　学習受け入れモードでは、センサーのローカル時刻が使用されます。

スキャナしきい値は、1 つの送信元 IP アドレスがスキャンできるゾーン IP アドレスの最大数を定義します。ヒストグラムしきい値は、指定された数を超えるゾーン IP アドレスをスキャンできる送信元 IP アドレスの最大数を定義します。

異常検出は、攻撃が行われていない状態で学習したヒストグラムからの逸脱を発見した場合（つまり、定義されている数を超えるゾーン宛先 IP アドレスを同時にスキャンする送信元 IP アドレスの数が超過した場合）、ワーム攻撃と認識します。たとえば、ポート 445 に対するスキャンしきい値が 300 の場合、異常検出は、350 個のゾーン宛先 IP アドレスをスキャンするスキャナを検出すると、マス スキャナが検出されたことを示すアクションを生成します。ただし、このスキャナでは、ワーム攻撃が進行中かどうかはまだ確認されていません。表 19-1 で、この例について説明します。

表 19-1　ヒストグラムの例

送信元 IP アドレス数	10	5	2
宛先 IP アドレス数	5	20	100

異常検出は、ポート 445 で 50 を超えるゾーン宛先 IP アドレスを同時にスキャンする送信元 IP アドレスを 6 つ検出すると、ポート 445 でワーム攻撃が検出されたことを示す、送信元 IP アドレスの指定がないアクションを作成します。動的なフィルタしきい値の 50 が新しい内部スキャンしきい値となり、それにより異常検出はスキャナのしきい値定義を引き下げます。その結果、異常検出は、新しいスキャンしきい値（50）を超えてスキャンする送信元 IP アドレスごとに追加の動的フィルタを作成します。

KB が学習した内容を異常検出ポリシーまたはゾーンごとにオーバーライドできます。ネットワーク トラフィックの詳細が判明している場合は、偽陽性を制限するためにオーバーライドを使用する必要が生じることもあります。

[Anomaly Detection] ペインのフィールド定義

[Anomaly Detection] ペインには次のフィールドとボタンがあります。

- [Virtual Sensor]：KB が属する仮想センサー。
- [Knowledge Base Name]：KB の名前。

（注）　デフォルトでは、KB は日付に応じて名前が設定されます。デフォルトの名前は日付と時刻です（year-month-day-hour_minutes_seconds）。初期 KB は、デフォルトのしきい値を持つ最初の KB です。

- [Current]：[Yes] は、現在ロードされている KB を示します。
- [Size]：KB のサイズ（キロバイト単位）。通常の範囲は、1 KB から、500 ～ 700 KB です。
- [Created]：KB が作成された日付。

ボタンの機能

- [Show Thresholds]：選択した KB の [Thresholds] ウィンドウを表示します。このウィンドウでは、選択した KB のスキャナしきい値とヒストグラムを表示できます。
- [Compare KBs]：[Compare Knowledge Bases] ダイアログボックスを表示します。このダイアログボックスでは、選択されている KB と比較する KB を選択できます。[Differences between knowledge bases *KB name and KB name*] ウィンドウが表示されます。
- [Load]：選択した KB をロードし、現在使用されている KB にします。
- [Save Current]：[Save Knowledge Base] ダイアログボックスを表示します。このダイアログボックスでは、選択した KB のコピーを保存できます。
- [Rename]：[Rename Knowledge Base] ダイアログボックスを表示します。このダイアログボックスでは、選択した KB の名前を変更できます。
- [Download]：[Download Knowledge Base From Sensor] ダイアログボックスを表示します。このダイアログボックスでは、リモート センサーから KB をダウンロードできます。
- [Upload]：[Upload Knowledge Base to Sensor] ダイアログボックスを表示します。このダイアログボックスでは、KB をリモート センサーにアップロードできます。
- [Delete]：選択した KB を削除します。
- [Delete All]：すべての KB を削除します。
- [Refresh]：[Anomaly Detection] ペインを更新します。

しきい値の表示

ここでは、KB しきい値情報の表示方法について説明します。内容は次のとおりです。

- 「[Threshold for KB_Name] ウィンドウ」（P.19-19）
- 「[Thresholds for KB_Name] ウィンドウのフィールド定義」（P.19-19）
- 「KB しきい値のモニタリング」（P.19-19）

[Threshold for KB_Name] ウィンドウ

[Thresholds for *KB_Name*] ウィンドウには、選択した KB の次のしきい値情報が表示されます。

- ゾーン名
- プロトコル
- 学習したスキャナしきい値
- ユーザ スキャナしきい値
- 学習したヒストグラム
- ユーザ ヒストグラム

しきい値情報は、ゾーン、プロトコル、ポートでフィルタできます。ゾーンとプロトコルの各組み合わせに対し、学習（デフォルト）モードまたはユーザ設定可能モードのいずれかについて、スキャナしきい値とヒストグラムしきい値の 2 つのしきい値が表示されます。

[Thresholds for *KB_Name*] ウィンドウのフィールド定義

[Thresholds for *KB_Name*] ウィンドウには次のフィールドがあります。

- [Filters]：ゾーンまたはプロトコルでしきい値情報をフィルタできます。
  - [Zones]：全ゾーン、外部のみ、不正のみ、または内部のみでフィルタします。
  - [Protocols]：全プロトコル、TCP のみ、UDP のみ、その他のみでフィルタします。

  （注）　特定のプロトコルを選択した場合、すべてのポートまたは単一のポート（TCP および UDP）、すべてのプロトコル、単一のプロトコル（その他）に対してフィルタすることもできます。

- [Zone]：ゾーン名（external、internal、illegal）を一覧表示します。
- [Protocol]：プロトコル（TCP、UDP、または Other）を一覧表示します。
- [Scanner Threshold (Learned)]：スキャナしきい値の学習した値を一覧表示します。
- [Scanner Threshold (User)]：スキャナしきい値のユーザ設定値を一覧表示します。
- [Histogram (Learned)]：ヒストグラムしきい値の学習した値を一覧表示します。
- [Histogram (User)]：ヒストグラムしきい値のユーザ設定値を一覧表示します。

KB しきい値のモニタリング

KB しきい値をモニタするには、次の手順に従います。

ステップ 1　管理者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* > [Sensor Monitoring] > [Dynamic Data] > [Anomaly Detection] の順に選択します。

ステップ 3　[Anomaly Detection] ペインを更新し最新の KB 情報を表示するには、[Refresh] をクリックします。

ステップ 4　KB のしきい値を表示するには、リスト中の KB を選択し、[Show Thresholds] をクリックします。[Thresholds for *KB_Name*] ウィンドウが表示されます。デフォルト表示には、すべてのゾーンとすべてのプロトコルが表示されます。

ステップ 5　1 つのゾーンのみを表示するように表示をフィルタするには、[Zones] ドロップダウン リストからゾーンを選択します。

ステップ 6　1 つのプロトコルのみを表示するように表示をフィルタするには、[Protocols] ドロップダウン リストからプロトコルを選択します。デフォルトの表示には、TCP または UDP プロトコルの場合はポートが表示され、その他のプロトコルの場合はすべてのプロトコルが表示されます。

ステップ 7　TCP または UDP の単一のポートを表示するように表示をフィルタするには、[Single Port] オプション ボタンをクリックし、[Port] フィールドにポート番号を入力します。

ステップ 8　その他のプロトコルで単一のポートを表示するように表示をフィルタするには、[Single Protocol] オプション ボタンをクリックし、[Protocol] フィールドにプロトコル番号を入力します。

ステップ 9　ウィンドウを最新のしきい値情報で更新するには、[Refresh] をクリックします。

KB の比較

ここでは、KB の比較方法について説明します。内容は次のとおりです。

[Compare Knowledge Base] ダイアログボックス

2 つの KB を比較し、その間の違いを表示できます。また、しきい値の差が指定したパーセンテージを超えているサービスを表示することもできます。[Details of Difference] 列には、特定のポートまたはプロトコルが現れる KB か、しきい値パーセンテージの違いが表示されます。

フィールド定義

[Compare Knowledge Bases] ダイアログボックスには次のフィールドがあります。

- すべての KB が含まれるドロップダウン リスト

[Differences between knowledge bases *KB_Name* and *KB_Name*] ウィンドウ

[Differences between knowledge base *KB_Name* and *KB_Name*] ウィンドウには、次の種類の情報が表示されます。

- ゾーン
- プロトコル
- 差異の詳細

表示する差異のパーセンテージを指定できます。デフォルトは 10% です。

フィールド定義

[Differences between knowledge bases *KB_Name* and *KB_Name*] ウィンドウには次のフィールドがあります。

- [Specify Percentage of Difference]：デフォルトを 10% から変更し、異なる差異パーセンテージを表示できます。
- [Zone]：KB の差異のゾーンを表示します（internal、illegal、または external）。
- [Protocol]：KB の差異のプロトコルを表示します（TCP、UDP、または Other）。
- [Details of Difference]：第 2 の KB の差異の詳細を表示します。

[Difference Thresholds between knowledge bases *KB_Name* and *KB_Name*] ウィンドウ

[Differences Thresholds between knowledge base *KB_Name* and *KB_Name*] ウィンドウには、次の種類の情報が表示されます。

- ナレッジ ベース名
- ゾーン名
- プロトコル
- スキャナしきい値（学習およびユーザ設定）
- ヒストグラム（学習およびユーザ設定）

フィールド定義

[Differences Thresholds between knowledge base *KB_Name* and *KB_Name*] ウィンドウには、次の種類の情報が表示されます。

- [Knowledge Base]：KB 名が表示されます。
- [Zone]：ゾーン名が表示されます（internal、illegal、または external）。
- [Protocol]：プロトコルが表示されます（TCP、UDP、または Other）。
- [Scanner Threshold (Learned)]：スキャナしきい値の学習した値を一覧表示します。
- [Scanner Threshold (User)]：スキャナしきい値のユーザ設定値を一覧表示します。
- [Histogram (Learned)]：ヒストグラムしきい値の学習した値を一覧表示します。
- [Histogram (User)]：ヒストグラムしきい値のユーザ設定値を一覧表示します。

KB の比較

2 つの KB を比較するには、次の手順を実行します。

ステップ 1　管理者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* > [Sensor Monitoring] > [Dynamic Data] > [Anomaly Detection] の順に選択します。

ステップ 3　[Anomaly Detection] ペインを最新の KB 情報で更新するには、[Refresh] をクリックします。

ステップ 4　リスト中で比較する KB を選択し、[Compare KBs] をクリックします。

ステップ 5　ドロップダウン リストから、比較で使用する他の KB を選択します。

（注）　また、**Ctrl** キーを押しながら 2 つの KB を選択することもできます。

ステップ 6　[OK] をクリックします。[Differences between knowledge bases *KB_Name* and *KB_Name*] ウィンドウが表示されます。

（注）　2 つの KB に違いがない場合、リストは空になります。

ステップ 7　差異のパーセンテージを 10% から変更するには、[Specify Percentage of Difference] フィールドに新しい値を入力します。

ステップ 8　差異の詳細を表示するには、行を選択して [Details] をクリックします。[Difference Thresholds between knowledge bases *KB_Name* and *KB_Name*] ウィンドウに詳細が表示されます。

現在の KB の保存

ここでは、現在の KB の保存、ロード、削除方法について説明します。内容は次のとおりです。

[Save Knowledge Base] ダイアログボックス

KB を異なる名前で保存できます。KB を保存しようとしたときに異常検出がアクティブでない場合、エラーが生成されます。KB 名がすでに存在する場合は、新しい名前を選択するか、デフォルトを使用して古い KB を上書きします。また、KB ファイルのサイズが制限されているため、新しい KB が生成されて制限に達すると、最も古い KB が削除されます（現在の KB または初期 KB でない限り）。

（注）　初期 KB は上書きできません。

フィールド定義

[Save Knowledge Base] ダイアログボックスには次のフィールドがあります。

- [Virtual Sensor]：保存した KB の仮想センサーを選択できます。
- [Save As]：デフォルトの名前をそのまま使用するか、保存する KB の新しい名前を入力します。

KB のロード

（注）　KB をロードすると現在の KB に設定されます。

KB をロードするには、次の手順を実行します。

ステップ 1　管理者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* > [Sensor Monitoring] > [Dynamic Data] > [Anomaly Detection] の順に選択します。

ステップ 3　リスト中でロードする KB を選択し、[Load] をクリックします。[Load Knowledge Base] ダイアログボックスが開き、ナレッジ ベースをロードしてよいかどうかを確認するメッセージが表示されます。

ステップ 4　[Yes] をクリックします。この KB の [Current] 列が [Yes] になります。

KB の保存

KB を新しい KB および仮想センサーとともに保存するには、次の手順を実行します。

ステップ 1　管理者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* > [Sensor Monitoring] > [Dynamic Data] > [Anomaly Detection] の順に選択します。

ステップ 3　リスト中で新しい KB として保存する KB を選択し、[Save Current] をクリックします。

ステップ 4　[Virtual Sensor] ドロップダウン リストから、この KB を適用する仮想センサーを選択します。

ステップ 5　[Save As] フィールドで、デフォルトの名前をそのまま使用するか、KB の新しい名前を入力します。

ヒント　変更内容を破棄して [Save Knowledge Base] 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　[Apply] をクリックします。KB が新しい名前で [Anomaly Detection] ペインのリストに表示されます。

KB の削除

（注）　現在の KB としてロードされている KB や初期 KB は削除できません。

KB を削除するには、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* > [Sensor Monitoring] > [Dynamic Data] > [Anomaly Detection] の順に選択します。

ステップ 3　リスト中で削除する KB を選択し、[Delete] をクリックします。[Delete Knowledge Base] ダイアログボックスが開き、ナレッジ ベースを削除してよいかどうかを確認するメッセージが表示されます。

ステップ 4　[Yes] をクリックします。KB が [Anomaly Detection] ペインのリストに表示されなくなります。

KB の名前変更

（注）　初期 KB の名前は変更できません。

KB の名前を変更するには、次の手順を実行します。

ステップ 1　管理者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* > [Sensor Monitoring] > [Dynamic Data] > [Anomaly Detection] の順に選択します。

ステップ 3　リスト中で名前を変更する KB を選択し、[Rename] をクリックします。

ステップ 4　[New Name] フィールドに KB の新しい名前を入力します。

ステップ 5　[Apply] をクリックします。新しい名前の KB が [Anomaly Detection] ペインのリストに表示されます。

KB のダウンロード

FTP または SCP プロトコルを使用して、KB を離れた場所にダウンロードできます。リモート URL、ユーザ名、パスワードを知っている必要があります。

フィールド定義

[Download Knowledge Base From Sensor] ダイアログボックスには次のフィールドがあります。

- [File Transfer Protocol]：ファイル転送プロトコルとして SCP または FTP を選択できます。
- [IP address]：KB のダウンロード元のリモート センサーの IP アドレス。
- [Directory]：リモート センサー上の KB が存在するパス。
- [File Name]：KB のファイル名。
- [Username]：リモート センサー上のユーザ アカウントに対応するユーザ名。
- [Password]：リモート センサー上のユーザ アカウントのパスワード。

KB のダウンロード

センサーから KB をダウンロードするには、次の手順を実行します。

ステップ 1　管理者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* > [Sensor Monitoring] > [Dynamic Data] > [Anomaly Detection] の順に選択します。

ステップ 3　センサーから KB をダウンロードするには、[Download] をクリックします。

ステップ 4　[File Transfer Protocol] ドロップダウン リストから、使用するプロトコル（SCP または FTP）を選択します。

ステップ 5　[IP address] フィールドに、KB のダウンロード元のセンサーの IP アドレスを入力します。

ステップ 6　[Directory] フィールドに、センサー上の KB が存在するパスを入力します。

ステップ 7　[File Name] フィールドに、KB のファイル名を入力します。

ステップ 8　[Username] フィールドに、センサー上のユーザ アカウントに対応するユーザ名を入力します。

ステップ 9　[Password] フィールドに、センサー上のユーザ アカウントのパスワードを入力します。

ヒント　変更を破棄して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 10　[Apply] をクリックします。新しい KB が [Anomaly Detection] ペインのリストに表示されます。

KB のアップロード

FTP または SCP プロトコルを使用して、KB を離れた場所からアップロードできます。リモート URL、ユーザ名、パスワードを知っている必要があります。

フィールド定義

[Upload Knowledge Base to Sensor] ダイアログボックスには次のフィールドがあります。

- [File Transfer Protocol]：ファイル転送プロトコルとして SCP または FTP を選択できます。
- [IP address]：KB のアップロード先のリモート センサーの IP アドレス。
- [Directory]：センサー上の KB が存在するパス。
- [File Name]：KB のファイル名。
- [Virtual Sensor]：この KB を関連付ける仮想センサー。
- [Save As]：KB を新しいファイル名で保存できます。
- [Username]：センサー上のユーザ アカウントに対応するユーザ名。
- [Password]：センサー上のユーザ アカウントのパスワード。

KB のアップロード

センサーに KB をアップロードするには、次の手順を実行します。

ステップ 1　管理者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* > [Sensor Monitoring] > [Dynamic Data] > [Anomaly Detection] の順に選択します。

ステップ 3　センサーに KB をアップロードするには、[Upload] をクリックします。

ステップ 4　[File Transfer Protocol] ドロップダウン リストから、使用するプロトコル（SCP または FTP）を選択します。

ステップ 5　[IP address] フィールドに、KB のダウンロード先センサーの IP アドレスを入力します。

ステップ 6　[Directory] フィールドに、センサー上の KB が存在するパスを入力します。

ステップ 7　[File Name] フィールドに、KB のファイル名を入力します。

ステップ 8　[Virtual Sensor] ドロップダウン リストから、この KB を適用する仮想センサーを選択します。

ステップ 9　[Save As] フィールドに、新しい KB の名前を入力します。

ステップ 10　[Username] フィールドに、センサー上のユーザ アカウントに対応するユーザ名を入力します。

ステップ 11　[Password] フィールドに、センサー上のユーザ アカウントのパスワードを入力します。

ヒント　変更を破棄して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 12　[Apply] をクリックします。新しい KB が [Anomaly Detection] ペインのリストに表示されます。

OS ID の設定

ここでは、センサーの学習した OS およびインポートした OS マップを表示する方法について説明します。内容は次のとおりです。

- 「学習したオペレーティング システムの設定」（P.19-26）
- 「インポートしたオペレーティング システムの設定」（P.19-27）

学習したオペレーティング システムの設定

（注）　[Learned OS] ペインのリストのクリアまたはエントリの削除を行うには、管理者またはオペレータであることが必要です。

[Learned OS] ペインには、ネットワーク上のトラフィックを観察することでセンサーが学習した OS マップが表示されます。センサーは、TCP セッションのネゴシエーションを調べて、各ホストで動作している OS を判定します。

リストのクリアまたは 1 つのエントリの削除を行うには、行を選択して [Delete] をクリックします。[Refresh] をクリックしてリストを更新します。現在表示されている、テーブル内の学習した OS 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するには、[Export] をクリックします。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。

（注）　パッシブ OS フィンガープリントがイネーブルなままで、ホストがまだネットワーク上で通信している場合、学習した OS マップにはすぐに情報が設定されます。

フィールド定義

[Learned OS] ペインには次のフィールドがあります。

- [Virtual Sensor] : OS の値が関連付けられている仮想センサー。

  （注）　AIM IPS、AIP SSC-5、および NME IPS では仮想化がサポートされていません。

- [Host IP Address] : OS 値がマッピングされている IP アドレス。

- [OS Type]：IP アドレスに関連付けられている OS の種類。

値の削除と学習した OS リストのクリア

学習した OS 値の削除またはリスト全体のクリアを行うには、次の手順を実行します。

ステップ 1　管理者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* > [Sensor Monitoring] > [Dynamic Data] > [OS Identifications] > [Learned OS] の順に選択します。

ステップ 3　リスト中の 1 つのエントリを削除するには、そのエントリを選択し、[Delete] をクリックします。学習した OS の値が [Learned OS] ペインのリストに表示されなくなります。

ステップ 4　学習した OS の値の最新のリストを取得するには、[Refresh] をクリックします。学習した OS のリストが更新されます。

ステップ 5　学習した OS の値をすべてクリアするには、[Clear List] をクリックします。学習した OS のリストが空になります。

ステップ 6　学習した OS のリストを CSV および HTML 形式で保存するには、[Export] をクリックします。また、**Ctrl-C** を使用して [Learned OS] ペインの内容をコピーし、**Ctrl-V** を使用してメモ帳や Word に内容をコピーすることもできます。

詳細情報

設定された OS マップの追加、編集、削除、移動の詳細については、「OS ID の設定」（P.11-25）を参照してください。

インポートしたオペレーティング システムの設定

（注）　[Imported OS] ペインのリストのクリアまたはエントリの削除を行うには、管理者またはオペレータであることが必要です。

CSA MC が外部インターフェイス製品として設定されている場合、[Imported OS] ペインには、センサーが CSA MC からインポートした OS マップが表示されます。外部製品インターフェイスを追加するには、[Configuration] > [External Product Interfaces] を選択します。リストのクリアまたは 1 つのエントリの削除を行うには、行を選択して [Delete] をクリックします。

フィールド定義

[Imported OS] ペインには次のフィールドがあります。

- [Host IP Address]：OS 値がマッピングされている IP アドレス。
- [OS Type]：IP アドレスに関連付けられている OS の種類。

値の削除とインポートした OS リストのクリア

インポートした OS 値の削除またはリスト全体のクリアを行うには、次の手順を実行します。

ステップ 1　管理者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* > [Sensor Monitoring] > [Dynamic Data] > [OS Identifications] > [Imported OS] の順に選択します。

ステップ 3　リスト中の 1 つのエントリを削除するには、そのエントリを選択し、[Delete] をクリックします。インポートした OS の値が [Imported OS] ペインのリストに表示されなくなります。

ステップ 4　インポートした OS の値をすべてクリアするには、[Clear List] をクリックします。インポートした OS のリストが空になります。

ステップ 5　最新のインポートされた OS の値でペインを更新するには、[Refresh] をクリックします。

詳細情報

外部製品インターフェイスの詳細については、第 17 章「外部製品インターフェイスの設定」を参照してください。

フロー状態のクリア

ここでは、センサー データベースのクリア方法について説明します。内容は次のとおりです。

[Clear Flow States] ペイン

注意　アラート データベースをクリアすると、進行中のすべてのサマリー アラートが削除され、最終的なサマリー アラートが生成されなくなります。アラート データベースは、トラブルシューティング目的でのみクリアすることをお勧めします。

[Clear Flow States] ペインでは、ノード、アラート、インスペクタ データベースなど、データベースの内容の一部または全部をクリアできます。仮想センサー名を指定しない場合、すべての仮想センサー データベースがクリアされます。

（注）　AIM IPS、AIP SSC-5、および NME IPS では仮想化がサポートされていません。

データベース中のノードをクリアすると、再起動したかのようにセンサーが最初から開始されます。オープンされているすべての TCP ストリームの情報が削除され、新しいパケットが受信されるのに従って、新しい TCP ストリーム ノードが作成されます。

インスペクタ データベースをクリアすると、TCP および状態情報は保持されますが、将来アラートにつながる可能性があるすべての検査レコードは削除されます。新しいパケットの取得に従い、新しい検査レコードが作成されます。

アラート データベースをクリアすると、アラート データベースは完全にクリアされます。

[Clear Flow States] ペインのフィールド定義

[Clear Flow States] ペインには次のフィールドがあります。

- [Clear Nodes]：パケット ノード、TCP セッション情報、インスペクタ リストを含め、パケット データベース要素全体をクリアします。
- [Clear Inspectors]：ノード中に格納されているインスペクタ リストをクリアします。TCP セッション情報やノードはクリアされません。インスペクタ リストは、センサーの動作中に収集されたパケット作業と観察を表します。
- [Clear Alerts]（非推奨）：アラート ノード、メタ インスペクタ情報、サマリー状態、イベント カウント構造を含む、アラート データベースをクリアします。

注意　アラート データベースをクリアすると、進行中のすべてのサマリー アラートが削除され、最終的なサマリー アラートが生成されなくなります。アラート データベースは、トラブルシューティング目的でのみクリアすることをお勧めします。

- [Clear All]：すべての仮想センサー データベースをクリアします。
- [Specify a Single Virtual Sensor (otherwise all virtual sensors will be cleared)]：特定の仮想センサーのデータベースをクリアできます。

フロー状態のクリア

フロー状態をクリアするには、次の手順を実行します。

ステップ 1　管理者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* > [Sensor Monitoring] > [Properties] > [Clear Flow States] の順に選択します。

ステップ 3　クリアする値のオプション ボタンをクリックします。

- [Clear Nodes]
- [Clear Inspectors]
- [Clear Alerts]（非推奨）
- [Clear All]

注意　アラート データベースをクリアすると、進行中のすべてのサマリー アラートが削除され、最終的なサマリー アラートが生成されなくなります。アラート データベースは、トラブルシューティング目的でのみクリアすることをお勧めします。

ステップ 4　1 つの仮想センサーのフロー状態をクリアするには、[Specify a Single Virtual Sensor (otherwise all virtual sensors will be cleared)] チェックボックスをオンにします。すべての仮想センサーのフロー状態をクリアするには、手順 6 に進みます。

ステップ 5　ドロップダウン リストから、フロー状態をクリアする仮想センサーを選択します。

ステップ 6　[Clear Flow State Now] をクリックします。

ネットワーク セキュリティの稼動状態のリセット

（注）　ネットワーク セキュリティの稼動状態をリセットするには、管理者であることが必要です。

（注）　AIM IPS、AIP SSC-5、および NME IPS では仮想化がサポートされていません。

[Reset Network Security Health] ペインでは、ネットワーク セキュリティの稼動状態のステータスと計算をリセットできます。これにより、[Home] ページの [Network Security Health] ガジェットがクリアされます。仮想センサー名を指定しない場合、すべての仮想センサーのネットワーク セキュリティ稼動状態情報がクリアされます。

フィールド定義

[Reset Network Security Health] ペインには次のフィールドがあります。

- [Specify a Single Virtual Sensor (otherwise network security for all virtual sensors will be reset)] : 特定の仮想センサーのネットワーク セキュリティ データをクリアできます。

ネットワーク セキュリティの稼動状態データのリセット

ネットワーク セキュリティの稼動状態データをリセットするには、次の手順を実行します。

ステップ 1　管理者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* > [Sensor Monitoring] > [Properties] > [Reset Network Security Health] の順に選択します。

ステップ 3　1 つの仮想センサーのネットワーク セキュリティ稼動状態をリセットするには、[Specify a Single Virtual Sensor (otherwise network security for all virtual sensors will be reset)] チェックボックスをオンにします。すべての仮想センサーのデータをリセットするには、ステップ 5 に進みます。

ステップ 4　ドロップダウン リストから、ネットワーク セキュリティ稼動状態データをクリアする仮想センサーを選択します。

ステップ 5　[Reset Network Security Health Now] をクリックします。[Home] ページの [Network Security Health] ガジェットのデータがクリアされます。

（注）　[Network Security] ガジェットに表示される脅威しきい値を変更するには、[Configuration] > *sensor_name* > [Event Action Rules] > [rules0] > [Risk Category] の順に選択します。

詳細情報

- ネットワーク セキュリティ データが含まれる [Sensor Health] ガジェットの詳細については、「[Sensor Health] ガジェット」（P.3-4）を参照してください。
- センサーの稼動状態を設定するための手順については、「センサーのヘルスの設定」（P.18-14）を参照してください。
- リスク カテゴリを設定するための手順については、「リスク カテゴリの設定」（P.11-33）を参照してください。

診断レポートの生成

（注）　診断を実行するには、管理者であることが必要です。

（注）　診断レポートの生成には数分かかります。

トラブルシューティング用に、センサーの診断情報を取得できます。診断レポートには、ログ、ステータス、設定など、TAC がセンサーをトラブルシューティングするときに使用するための、システム内部の情報が含まれています。[Diagnostics Report] ペインでレポートを表示するか、[Save] をクリックしてハードディスク ドライブにレポートを保存できます。

ボタンの定義

[Diagnostics Report] ペインには次のボタンがあります。

- [Save] : [Save As] ダイアログを開きます。このダイアログでは、診断レポートのコピーをハードディスク ドライブに保存できます。
- [Generate Report] : 診断処理を開始します。

  この処理が完了するまでに数分の時間がかかることがあります。処理が完了した後、レポートが生成され、更新後のレポートで表示が更新されます。

診断レポートの生成

注意　診断処理を開始した後は、IME の他のオプションをクリックしたり [Diagnostics] ペインを閉じたりしないでください。センサーに対する他の作業は、この処理が完了してから実行する必要があります。

診断を実行するには、次の手順を実行します。

ステップ 1　管理者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* > [Sensor Monitoring] > [Support Information] > [Diagnostics Report] の順に選択し、[Generate Report] をクリックします。

（注）　診断処理は、完了までに数分かかります。処理が完了したら、更新後の結果で表示が更新されます。

ステップ 3　このレポートをファイルとして保存するには、[Save] をクリックします。[Save As] ダイアログボックスが開きます。このダイアログでは、レポートをハードディスク ドライブに保存できます。

統計情報の表示

[Statistics] ペインには、次のカテゴリの統計情報が表示されます。

- 分析エンジン

[Analysis Engine] セクションにはグローバル相関統計情報も含まれています。

- Anomaly Detection
- Event Store
- External Product Interface
- Host
- Interface Configuration
- Logger
- Network Access（Attack Response Controller と呼ばれるようになりました）
- Notification
- OS Identification
- Transaction Server
- Virtual Sensor
- Web Server

ボタンの定義

[Statistics] ペインには次のボタンがあります。

- [Refresh]：センサー アプリケーションに関する最新情報を表示します。これには、Web Server、Transaction Source、Transaction Server、Network Access Controller、Logger、Host、Event Store、Analysis Engine、Interface Configuration、および Authentication が含まれています。

（注）　Network Access Controller（Cisco IPS 5.1 からは Attack Response Controller と呼ばれるようになりました）は、統計情報出力に引き続き Network Access Controller として表示されます。

統計情報の表示

センサーの統計情報を表示するには、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* > [Sensor Monitoring] > [Support Information] > [Statistics] の順に選択します。

ステップ 3　統計情報が変化したときに更新するには、[Refresh] をクリックします。

システム情報の表示

[System Information] ペインには、次の情報が表示されます。

- TAC 連絡先情報
- プラットフォーム情報
- ブートしたパーティション
- ソフトウェア バージョン

- アプリケーションのステータス（MainApp、Analysis Engine、および CollaborationApp）
- インストール済みアップグレード
- PEP 情報
- メモリ使用量
- ディスク使用量

ボタンの定義

[System Information] ペインには次のボタンがあります。

- [Refresh]：ソフトウェア バージョンや PEP 情報など、センサーに関する最新情報を表示します。

システム情報の表示

システム情報を表示するには、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* > [Sensor Monitoring] > [Support Information] > [System Information] の順に選択します。[System Information] ペインに、システムに関する情報が表示されます。

ステップ 3　[Refresh] をクリックします。ペインが更新され、新しい情報が表示されます。

CHAPTER 20

イベント モニタリングの設定

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

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

この章では、IME イベント モニタリングとおよびその設定方法について説明します。内容は次のとおりです。

イベント モニタリングについて

[Event Monitoring] ペインにはイベントのビューがあります。ビューには、リアルタイム イベントまたは履歴イベント（データベースに格納されたイベント）が表示されます。IME には事前定義されたビューがあります。ユーザ独自のビューを作成することもできます。事前定義されたビューについて、削除や変更の保存を行うことはできません。[Event Monitoring] ペインの左側にビュー ツリーが表示され、右側でビューの設定や表示を行います。

[Event Monitoring] ペインの右側は 3 つの部分で構成されます。

- [View Settings]：5 つのタブがあります。これらのタブを使用して、表示するイベントや表示方法を指定します。イベントは、フィルタ、グループ、色、フィールド、およびビューの種類別に表示できます。

フィルタを使用して、ビューを詳細にリストアップできます。グループを使用して、ビュー内でデータを並べ替えることができます。色を使って、特定のデータを目立たせることができます。たとえば、特定の攻撃者 IP アドレスからのイベントを検索する場合、重大度が「高」であるイベントを強調表示して、それらのイベントに特定の色を適用できます。表示するフィールドを選択し、その順序（昇順/降順）を指定できます。

- [Events table]：ビューにイベントを表示します。ツールバーを使用するか、またはメニューを右クリックして行を選択し、さまざまなアクションを実行することで、イベントを操作できます。
- [Event Details]：[Events table] で 1 つの行を選択すると、ペインの [Event Details] セクションにそのイベントの詳細が表示されます。

[Group By]、[Color Rules]、[Fields]、および [General] タブ

[Group By] タブでは、イベントの属性に基づいてイベントをグループ化できます。グループ レベルは、最大 4 つまでネストできます。たとえば、まず重大度に基づいてグループ化し、次に攻撃者 IP アドレスに基づいてグループ化することなどができます。選択基準は、フィルタを作成する場合と同様です。

[Color Rules] タブでは、特定の基準に基づいてイベントを選択し、選択したイベントにさまざまな背景色や前景色を適用できます。選択基準は、フィルタを作成する場合と同様です。色は上から下に向かって適用する必要があります。最初の一致で、色規則が適用されます。

[Fields] タブでは、イベント データを参照したいフィールドの追加や削除を行うことができます。また、それらのフィールドをリスト内で上下に移動させて、表示する順序を設定できます。選択基準は、フィルタを作成する場合と同様です。

[General] タブでは、ビューを選択して説明を加えることができます。事前定義されたビューと作成したビューを利用できます。これらのビューは、[Event Monitoring] ペインの左側の [Event Views] ツリーに表示されます。

フィルタについて

（注） [Filter] タブと [Add Filter] ダイアログボックスのフィールドで IPv6 アドレスおよび IPv4 アドレスがサポートされるようになりました。

IME では特定のビューのフィルタリング プロパティを設定できるため、参照したいイベントだけを表示することが可能です。イベントにフィルタを適用しないと、すべてのイベントが表示されます。フィルタを適用すると、フィルタに指定した基準に一致するイベントだけが表示されます。

参照したい情報だけをビューに表示するように、さまざまな基準を使用してフィルタを作成できます。イベントは、1 つのレベルまたは列を使ってグループ化できます。また、次の基準を使ってグループ化することも可能です。

- 重大度
- 日付
- 時刻
- デバイス
- シグニチャ名

- シグニチャ ID
- 攻撃者の IP アドレス
- 攻撃対象者の IP アドレス
- 実行されたアクション
- 攻撃対象者のポート
- 脅威レーティング
- リスク レーティング
- レピュテーション

ワンポイント アドバイス　たとえば、重大度が「高」のすべてのイベントに関心がある場合、フィルタの [Severity] セクションで [High] チェックボックスをオンにしてフィルタを作成します。このフィルタを適用すると、重大度が「高」のイベントだけが表示されます。

事前定義されたフィルタを使用するか、または新しいフィルタを追加することができます。事前定義されたフィルタの編集や削除を行うことはできません。各フィールドには、カンマ区切りの値を入力します。フィールドでは、1 つのエントリ、範囲、および NOT 演算子がサポートされます。たとえば、[attacker IP address] では、次の形式がサポートされます。

- 10.1.1.1,10.1.1.5
- 10.1.1.1-10.1.1.15
- !10.1.1.1

（注）　感嘆符（!）は「除外する」ことを意味します。

フィルタを使用して、次のようなクエリを実行できます。

- Attacker IP address（攻撃者 IP アドレス）が 10.1.1.1 または 10.1.1.5 で、Signature ID（シグニチャ ID）が ID 5042 のイベントを表示する
- Risk rating（リスク レーティング）が 75-100 で、Attacker IP address（攻撃者 IP アドレス）が 192.2.3.3 のイベントを表示する

これらのフィルタ定義は、[Manage Filter Rules] ダイアログボックスに表示されます。[Risk Rating]、[Threat Rating]、[Destination Port] の各フィールドでは、次の形式がサポートされます。

- =
- !=
- >
- >=
- <
- <=
- 範囲内
- 範囲外

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

[Filter] タブおよび [Add Filter] ダイアログボックスには、次のフィールドが表示されます。

- [Filter Name]：このフィルタの名前を入力するか、デフォルトのフィルタ名から選択できます。
- [Attacker IP]：このフィルタに含める攻撃者の IP アドレス。有効な値は、*ip_address* および *ip_address_range* です（例：10.0.0.1、!10.0.0.1、!10.1.1.1）。

  （注）　感嘆符（!）は「除外する」ことを意味します。

- [Victim IP]：このフィルタに含める攻撃対象の IP アドレス。有効な値は、*ip_address* および *ip_address_range* です（例：10.0.0.1、!10.0.0.1、!10.1.1.1）。
- [Signature Name/ID]：このフィルタに含めるシグニチャの名前/ID。有効な値は、*signature_name*、*signature_id*、*signature_id/subsig_id*、または *signature_id_range* です。次に例を示します。
  - no_checkpoint
  - no_checkpoint, 3320
  - no_checkpoint, 3320/1
  - 3300-400
- [Victim Port]：このフィルタに含める攻撃対象ポート。有効な値は、*number* または *number_range* です（例：>=80、70-100、<90、!100）。
- [Severity]：このフィルタに含める重大度。
- [Risk Rating]：このフィルタに含めるリスク レーティング。有効な値は、*number* または *number_range* です（例：>=80、70-100、<90、!100）。
- [Reputation]：このフィルタに含めるレピュテーション スコア。有効値の範囲は、-10.0 ～ 10.0 です。
- [Threat Rating]：このフィルタに含める脅威レーティング。有効な値は、*number* または *number_range* です（例：>=80、70-100、<90、!100）。
- [Action(s) Taken]：フィルタがアラート内で検索するアクションを選択できます。アクションは文字列であり、選択することもできれば、自由形式で入力することも可能です。
- [Sensor Name(s)]：このフィルタに含めるセンサーを指定できます。
- [Virtual Sensor]：このフィルタに含める仮想センサーを指定できます。
- [Status]：このフィルタにステータス（[All]、[New]、[Assigned]、[Closed]、[Detected]、[Acknowledged]）を割り当てることができます。

  [Status] フィールドは、特定のイベントの分析結果を後で使用するために保存しておく場合などに役立ちます。注釈を追加し、ステータスを [Acknowledged] に変更することにより、ステータスでフィルタ処理を実行し、承認されたケースをすべて表示して、追加の分析を行うことができます。
- [Victim Locality]：フィルタ処理を行う参加/アドレス アラート内のアラート属性。この属性は、イベント アクション規則変数に定義されます。
- [Color Parameters]：イベントの色規則を設定できます（次のオプションは [Color Rules] タブでフィルタを追加する場合にのみ表示されます）。
  - [Foreground]：イベントの前景色が表示され、使用する色を選択できます。

- [Background]：イベントの背景色が表示され、使用する色を選択できます。
- [Font Type]：イベントのフォント タイプとして、太字、イタリック、またはその両方を選択できます。
- [Preview Text]：イベントがビューにどのように表示されるかを確認できます。

イベント ビューの操作

イベント ビューを操作するには、次の手順を実行します。

ステップ 1　[Event Monitoring] > [Event Monitoring] > [Event Views] を選択します。

[Event Monitoring] ペインの左側に、事前定義されたビューが 5 つ表示されます（[Basic View]、[Blocked Attacks View]、[Dropped Attacks View]、[Grouped Severity View]、and [Real-Time Colored View]）。イベントは、[View] ペインの下部に表示されます。

ステップ 2　ビューを作成するには、[New] をクリックします。

ステップ 3　[New View] ダイアログボックスの [Name] フィールドにビューの名前を入力し、[OK] をクリックします。マイ ビューの下にあるペインの左側に、新しいビューが表示されます。1 つのイベントに対して、フィルタを作成して適用できます。

詳細情報

- 1 つのイベントを調べる手順については、「1 つのイベントを調べる」（P.20-5）を参照してください。
- フィルタを作成して適用する手順については、「イベント ビューのフィルタの設定」（P.20-7）を参照してください。

1 つのイベントを調べる

1 つのイベントを調べるには、次の手順を実行します。

ステップ 1　[Event Monitoring] > [Event Monitoring] > [Event Views] > [Basic View] を選択します。

ステップ 2　イベントを収集する期間を設定します。

ステップ 3　1 つのイベントを調べるには、リストでイベントを選択し、ツールバーの [Event] をクリックします。[Event] ドロップダウン リストから、次の情報を表示できます（これらの情報は、ウィンドウの下部にタブ形式で表示される [Event Details] セクションにも表示されます）。

- [Summary]：そのイベントに関する情報の要約が表示されます。
- [Explanation]：そのイベントに関連付けられたシグニチャの説明および関連シグニチャ情報が表示されます。
- [Related Threats]：関連する脅威と MySDN 内の詳細情報へのリンクが表示されます。
- [Trigger Packet]：イベントをトリガーしたパケットに関する情報が表示されます。
- [Context Data]：パケット コンテキスト情報が表示されます。
- [Actions Taken]：展開されたイベント アクションのリストが表示されます。

- [Notes]：イベントに名称（New、Assigned、Acknowledged、Closed、または Deleted）を割り当てることにより、イベントに対してアクションを実行できます。[Notes] フィールドに注釈を入力し、[Save Note] をクリックして保存します。

ステップ 4　このイベントの詳細を印刷するには、[Show All Details] をクリックして、イベントの詳細をプリンタ対応のウィンドウに表示します。

ステップ 5　選択したイベントから属性を追加するには、[Filter] ドロップダウン メニューから [Add to Filter] > [Attacker IP/Victim IP/Signature ID] を選択します。ウィンドウの上部に [Filter] タブが表示されます。

ステップ 6　このイベントからフィルタを作成するには、[Filter] ドロップダウン メニューから [Create a Filter] を選択します。

ステップ 7　このイベントに関連付けられたシグニチャを編集するには、[Edit Signature] をクリックします。[Configuration] > *sensor_name* > [Policies] > [Signature Definitions] > [sig0] > [Active Signatures] へ移動し、シグニチャを編集できます。

ステップ 8　このイベントからイベント アクション規則フィルタを作成するには、[Create Rule] をクリックします。[Configuration] > *sensor_name* > [Policies] > [IPS Policies] > [Add Event Action Filter] へ移動し、イベント アクション規則フィルタを追加できます。

ステップ 9　攻撃者を阻止するには、[Stop Attacker] ドロップダウン メニューから次のオプションのいずれかを選択します。

- [Using Inline Deny]：このオプションを選択すると、[Configuration] > *sensor_name* > [Sensor Monitoring] > [Time-Based Actions] > [Denied Attackers] > [Add Denied Attacker] へ移動します。
- [Using Block on another device]：このオプションを選択すると、[Configuration] > *sensor_name* > [Sensor Monitoring] > [Time-Based Actions] > [Host Blocks] > [Add Host Block] へ移動します。

ステップ 10　このイベントに関係する IP アドレスに対して ping、traceroute、DNS、および whois を実行するには、これらのコマンドを [Tools] ドロップダウン メニューから選択します。

ping を使用すると、基本的なネットワーク接続を診断できます。ping により、センサーが応答するかどうかを簡単に確認できます。traceroute を使用すると、IP パケットが宛先に到達するまでのルートを表示できます。whois を使用すると、ドメイン名または IP アドレスの所有者を確認できます。DNS ルックアップを使用すると、電話帳を調べるように、ホスト名を IP アドレスに変換できます。

ステップ 11　イベントを保存、削除、またはコピーするには、[Other] ドロップダウン リストから実行するアクションを選択します。

ステップ 12　ビューに加えた変更を保存するには、[Apply] をクリックします。変更を破棄する場合は、[Reset] をクリックします。

詳細情報

- フィルタを追加する手順については、「イベント ビューのフィルタの設定」（P.20-7）を参照してください。
- イベント アクション規則フィルタを追加する手順については、「イベント アクション フィルタの設定」（P.11-16）を参照してください。
- 拒否攻撃者を追加する手順については、「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。
- ホスト ブロックを追加する手順については、「ホスト ブロックの追加、削除、管理」（P.19-8）を参照してください。
- ツールの詳細については、「デバイスでのツールの使用」（P.2-6）を参照してください。

イベント ビューのフィルタの設定

（注）　[Filter] タブと [Add Filter] ダイアログボックスのフィールドで IPv6 アドレスおよび IPv4 アドレスがサポートされるようになりました。

フィルタを設定するには、次の手順を実行します。

ステップ 1　[Event Monitoring] を選択し、[New] をクリックします。

ヒント　リストで複数の項目を選択するには、**Ctrl** キーを押しながらクリックします。

ステップ 2　[New View] ダイアログボックスで、新しいビューの名前を入力します。ビュー ツリーのマイ ビューの下に、新しいビューが表示されます。

ステップ 3　[View Settings] > [Filter] をクリックします。

ステップ 4　[Filter Name] ドロップダウン メニューから、このフィルタのフィルタ名を選択するか、[Note] アイコンをクリックしてから [Add] をクリックし、新しいファイルを追加します。

a. [Filter Name] フィールドに、このフィルタの名前を入力します。

b. [Attacker IP] フィールドに攻撃者の IP アドレスを入力するか、[Note] アイコンをクリックして一意の IP アドレスまたは IP アドレスの範囲を追加し、[OK] をクリックします。

c. [Victim IP] フィールドに攻撃対象の IP アドレスを入力するか、[Note] アイコンをクリックして一意の IP アドレスまたは IP アドレスの範囲を追加し、[OK] をクリックします。

d. [Signature Name/ID] フィールドにシグニチャ名またはシグニチャ ID を入力するか、[Note] アイコンをクリックし、シグニチャ タイプを選択して、[OK] をクリックします。

e. [Victim Port] フィールドに攻撃対象ポートを入力するか、[Note] アイコンをクリックして必要な条件を満たす攻撃対象ポートを入力し、[OK] をクリックします。

f. このフィルタの重大度を選択します。

g. [Risk Rating] フィールドに、このフィルタのリスク レーティングを入力するか、[Note] アイコンをクリックして必要な条件を満たすリスク レーティングを入力し、[OK] をクリックします。

h. [Reputation] フィールドに、このフィルタのレピュテーション スコアを入力するか、[Note] アイコンをクリックして必要な条件を満たすレピュテーションを入力し、[OK] をクリックします。

i. [Threat Rating] フィールドに、このフィルタの脅威レーティングを入力するか、[Note] アイコンをクリックして必要な条件を満たす脅威レーティングを入力し、[OK] をクリックします。

j. [Actions Taken] フィールドに、このフィルタをトリガーするアクションを入力するか、[Note] アイコンをクリックして、このフィルタをトリガーするアクションのチェックボックスをオンにし、[OK] をクリックします。

k. [Sensor Name(s)] フィールドに、このフィルタの影響を受けるセンサーの名前を入力するか、[Note] アイコンをクリックして、このフィルタを適用するセンサーのチェックボックスをオンにし、[OK] をクリックします。

l. [Virtual Sensor] フィールドに、このフィルタを適用する仮想センサーを入力します。

m. [Status] ドロップダウン メニューから、フィルタ処理を行うステータスを選択します。

n. [Victim Locality] フィールドに、フィルタ処理の対象とする作成済みのイベント アクション規則変数の名前を入力します。

ステップ 5　グループを設定するには、[Group By] タブをクリックします。

a. [Group events based on the following criteria] チェックボックスをオンにし、ドロップダウン メニューからカテゴリを選択することにより、イベントをグループ化するための階層を構築します。

b. [Grouping Preferences] で、[Single Level]、[Show Group Columns]、[Show Count Columns] の各チェックボックスをオンにできます。[Show Group Columns] チェックボックスをオンにした場合は、カウント カラムのみを表示できます。

ステップ 6　色規則を追加するには、[Color Rules] タブをクリックしてから [Add] をクリックします。

a. [Filter Name] フィールドに、この色規則フィルタの名前を入力します。

b. [Enable] チェックボックスをオンにします。

（注） [Enable] チェックボックスをオンにしなければ、色規則フィルタは有効になりません。

c. [Packet Parameters] では、この色規則フィルタを適用する IP アドレス、シグニチャ名、攻撃対象ポートを入力します。

d. [Rating and Action Parameters] では、この色規則フィルタを適用する重大度、リスク レーティング、脅威レーティング、およびアクションを入力します。

e. [Other Parameters] では、この色規則フィルタを適用するセンサー名、仮想センサー名、ステータス、攻撃対象の所在地を入力します。

f. [Color Parameters] では、この色規則フィルタの前景色、背景色、およびフォント タイプを選択し、[OK] をクリックします。

ヒント これらのフィールドに入力する値の正しい形式を確認するために、[Note] アイコンをクリックしてください。

ステップ 7　フィールドとその順序を編集するには、[Fields] タブをクリックし、[Add >>]、[<< Remove]、[Move Up]、および [Move Down] をクリックして、表示するフィールドを選択し、希望する順序どおりにフィールドを並べ替えます。

ステップ 8　[General] タブをクリックし、[View Description] フィールドをクリックして、ビューの説明を入力します。

ステップ 9　[Save As] をクリックして新しいビューを作成し、[Name] フィールドにビューの名前を入力します。設定が新しいビューにコピーされます。

ステップ 10　[Save] をクリックして、ビューに加えた変更を保存します。フィルタが [Filter Name] ドロップダウン メニューに表示されます。

ステップ 11　ビューに加えた変更を保存するには、[Apply] をクリックします。変更を破棄する場合は、[Reset] をクリックします。

CHAPTER 21

レポートの設定と生成

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

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

この章では、IME レポートについて説明し、その設定と生成についても取り上げます。内容は次のとおりです。

IME レポートについて

IME では、さまざまなフィルタを使用してカスタマイズ可能な各種レポートを作成できます。レポートは、棒グラフまたは円グラフを示すウィンドウで構成されます。ウィンドウにはグラフの作成に使用された表形式のデータも表示されます。

IME レポートには、次の 6 種類があります。

- 上位攻撃者（Top Attacker）レポート：一定の時間における上位攻撃者の IP アドレスを示します。上位何番目までの攻撃者の IP アドレスを表示するかを指定できます。上位攻撃者（Top Attacker）レポートには、事前定義されたレポートが 4 つあります。
  - 上位攻撃者（基本）（Basic Top Attacker）
  - 上位 10 攻撃者（直前の 1 時間）（Top 10 Attackers Last 1 Hour）
  - 上位 10 攻撃者（直前の 8 時間、重大度高）（Top 10 Attackers Last 8 Hours with High Severity）
  - 上位 20 主要攻撃者（直前の 24 時間）（Top 20 Critical Attackers Last 24 Hours）
- 上位攻撃対象（Top Victim）レポート：一定の時間における上位攻撃対象者の IP アドレスを示します。上位何番目までの攻撃対象者の IP アドレスを表示するかを指定できます。上位攻撃対象（Top Victim）レポートには、事前定義されたレポートが 4 つあります。
  - 上位攻撃対象者（基本）（Basic Top Victim）
  - 上位 10 攻撃対象者（直前の 1 時間）（Top 10 Victims Last 1 Hour）

  - 上位 10 攻撃対象者（直前の 8 時間、重大度高）（Top 10 Victims Last 8 Hours with High Severity）
  - 上位 20 攻撃対象者（アクションが拒否された攻撃者情報あり）（Top 20 Victims with Action Denied Attacker）
- 上位シグニチャ（Top Signature）レポート：一定の時間において開始された上位シグニチャを示します。上位何番目までのシグニチャを表示するかを指定できます。上位シグニチャ（Top Signature）レポートには、事前定義されたレポートが 4 つあります。
  - 上位シグニチャ（基本）（Basic Top Signature）
  - 上位 10 シグニチャ（直前の 1 時間）（Top 10 Signatures Last 1 Hour）
  - 上位 10 シグニチャ（直前の 8 時間、重大度高）（Top 10 Signatures Last 8 Hours with High Severity）
  - 上位 20 シグニチャ（直前の 24 時間）（Top 20 Critical Signatures Last 24 Hours）
- 攻撃（Attacks Over Time）レポート：一定の時間における攻撃を示します。事前定義されたレポートが 5 つあります。
  - 攻撃（基本）（Basic Over Time Attack）
  - ブロックされた攻撃（直前の 24 時間）（Attacks Blocked in Last 24 Hours）
  - ドロップされた攻撃（直前の 24 時間）（Attacks Dropped in Last 24 Hours）
  - 攻撃（直前の 1 時間）（Attacks Over Time Last 1 Hour）
  - 重大な攻撃（直前の 24 時間）（Critical Attacks Over Last 24 Hours）
- フィルタ処理されたイベントとすべてのイベント（Filtered Events vs All Events）レポート：一定期間における、全イベントに対する一連のイベントを表示します。事前定義されたレポートが 1 つあります。
  - ネガティブ レピュテーション イベント（Negative Reputation Events）
- グローバル相関レポート：センサーの実行が開始された後のグローバル相関レポートを表示します。グローバル相関レポートには、事前定義されたレポートが 2 つあります。
  - レピュテーション フィルタ（Reputation Filter）
  - グローバル相関

ユーザ定義のレポートとデモ レポート（事前定義されたレポートのサンプル）もあります。

[Reports] ウィンドウは、2 つの部分に分かれています。左側ペインの [Report] ツリーには、レポートリストがツリー形式で表示されます。右側ペインの [Report Settings] ペインには、レポートが表示されます。[Report] ツリーには、事前定義された一連のレポート（上位攻撃者（基本）（Basic Top Attacker）など）や、[My Reports] ノード下にユーザ定義レポートを保存する場所が含まれます。リストからレポートを選択し、[Generate Report] をクリックすると、[Report Settings] ペインの下半分に、対応するレポートがグラフや表とともに表示されます。[Reports Setting] ペインには [General] と [Filter] という 2 つのタブがあり、これらのタブを使用してレポートをカスタマイズできます。

IME では、レポートを PDF または RTF ファイルとして保存したり、印刷したりすることもできます。

（注）　[Filter] タブと [Add Filter] ダイアログボックスのフィールドで IPv6 アドレスおよび IPv4 アドレスがサポートされるようになりました。

レポートの設定と生成

（注）　[Filter] タブと [Add Filter] ダイアログボックスのフィールドで IPv6 アドレスおよび IPv4 アドレスがサポートされるようになりました。

レポートに含める項目数と時間間隔を設定して、レポートをカスタマイズできます。IP アドレスの解決には、DNS を使用することもできます。フィルタを使用して、レポートに含める情報の種類をさらに絞り込むこともできます。

レポートの設定および生成を行うには、次の手順を実行します。

ステップ 1　[Report] ツリーで [New] をクリックして表示される [New Report] ダイアログボックスに、新しいレポートの名前を入力し、ドロップダウン リストからレポートの種類を選択して、[OK] をクリックします。[Report] ツリーの [My Reports] に、新しいレポートが表示されます。

ステップ 2　レポートを選択し、[General] タブでレポートを設定します。

a. [Report Description] フィールドに、このレポートの説明を入力します。

b. [Top] フィールドに、このレポートに上位何番目までのイベントを表示するかを入力します。

c. DNS アドレス解決を使用する場合は、[Resolve Addresses Using DNS] チェックボックスをオンにします。

d. 期間を入力するか、カスタム時間を入力して、このレポートの時間間隔を設定します。

ステップ 3　[Filter] タブの [Filter Name] ドロップダウン メニューからフィルタ名を選択するか、またはフィルタを追加して、[Note] アイコンをクリックします。

ステップ 4　[Manage Filter Rules] ダイアログボックスで、レポートのフィルタ フィールドを設定します。

ステップ 5　[Generate Report] をクリックします。統計情報（グラフ形式と表形式）とともに、レポートが [Report Settings] ペインの下半分に表示されます。

ステップ 6　表示をカスタマイズするには、[Display Type] ドロップダウン メニューで [Bar] または [Pie Chart] を選択します。

ステップ 7　[Print] をクリックしてレポートを印刷するか、または [Save] をクリックしてレポートを PDF 形式か RFT 形式でハードディスク ドライブに保存します。

ステップ 8　1 つの IP アドレスに関するイベントを表示するには、[Events for] ドロップダウン リストから IP アドレスを選択します。

詳細情報

- フィルタを作成する手順については、「フィルタの設定」（P.3-17）を参照してください。
- 1 つの IP アドレスに関するイベントを設定する手順については、「個々の上位攻撃者および上位攻撃対象の IP アドレスに対する 1 つのイベントを調べる」（P.3-14）を参照してください。
- 1 つのシグニチャに関するイベントを設定する手順については、「上位シグニチャに対する 1 つのイベントを調べる」（P.3-16）を参照してください。

CHAPTER 22

センサーへのログイン

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

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

（注） IPS プラットフォームでは、10 個の CLI セッションを同時に確立することができます。

この章では、さまざまな Cisco IPS プラットフォームにログインする方法について説明します。内容は次のとおりです。

サポートされるユーザ ロール

次のユーザ権限を使用してログインできます。

- 管理者（Administrator）
- オペレータ（Operator）
- ビューア（Viewer）
- サービス（Service）

サービス ロールでは、CLI に直接アクセスできません。サービス アカウント ユーザは、bash シェルに直接ログインします。このアカウントは、サポートおよびトラブルシューティング目的でのみ使用します。無許可の変更はサポートされず、正しく動作することを保証するには、センサーでイメージを再作成することが必要になります。サービス ロールでは、1 ユーザのみ作成できます。

サービス アカウントにログインすると、次の警告が表示されます。

```
******************************** WARNING ****************************************
UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
This account is intended to be used for support and troubleshooting purposes only.
Unauthorized modifications are not supported and will require this device to be re-imaged
to guarantee proper operation.
*********************************************************************************
```

（注） サービス ロールは、必要に応じて CLI をバイパスできる特殊なロールです。管理者権限を持つユーザだけが、サービス アカウントを編集できます。

詳細情報

- サービス アカウントの詳細については、「サービス アカウントについて」（P.6-23）を参照してください。
- ユーザの追加および削除を行う手順については、「認証およびユーザの設定」（P.6-18）を参照してください。

アプライアンスへのログイン

（注） コンソールからアプライアンスを初期化（**setup** コマンドを実行）する必要があります。ネットワークを設定すると、SSH および Telnet が有効になります。

アプライアンスには、コンソール ポートからログインできます。

アプライアンスにログインするには、次の手順を実行します。

ステップ 1　アプライアンスにログインするため、コンソール ポートをセンサーに接続します。

ステップ 2　ログイン プロンプトに対してユーザ名とパスワードを入力します。

（注） デフォルトのユーザ名とパスワードはどちらも **cisco** です。初めてアプライアンスにログインするとき、このユーザ名とパスワードを変更するように求めるメッセージが表示されます。最初に、UNIX パスワード（**cisco**）を入力してください。次に、新しいパスワードを 2 回入力します。

```
login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable laws and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.
```

```
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license to obtain a new license or install a license.
ips-4240#
```

詳細情報

- アプライアンスをターミナル サーバに接続する手順については、「ターミナル サーバの設定」（P.22-3）を参照してください。
- **setup** コマンドを使用してアプライアンスを初期化する手順については、「センサーの基本的なセットアップ」（P.23-5）を参照してください。

ターミナル サーバの設定

ターミナル サーバは複数の低速非同期ポートを持つルータです。この複数のポートは、他のシリアル デバイスに接続されています。ターミナル サーバを使用して、アプライアンスを含むネットワーク機器をリモートで管理することができます。

RJ-45 接続またはヒドラ ケーブル アセンブリ接続を使用して Cisco ターミナル サーバをセットアップするには、次の手順を実行します。

ステップ 1　次のいずれかの方法で、ターミナル サーバに接続します。

- RJ-45 接続を行うターミナル サーバの場合、180 ロールオーバー ケーブルをアプライアンスのコンソール ポートからターミナル サーバのポートに接続します。
- ヒドラ ケーブル アセンブリの場合、ストレート パッチ ケーブルをアプライアンスのコンソール ポートからターミナル サーバのポートに接続します。

ステップ 2　ターミナル サーバで、ラインとポートを設定します。イネーブル モードで次の設定を入力します。ここで、# は設定するポートの回線番号です。

```
config t
line #
login
transport input all
stopbits 1
flowcontrol hardware
speed 9600
exit
exit
wr mem
```

ステップ 3　アプライアンスへの不正アクセスを防ぐため、ターミナル セッションは確実に正しく終了してください。

ターミナル セッションが正しく終了されていない場合、つまり、セッションを開始したアプリケーションから exit(0) 信号が受信されていない場合、ターミナル セッションは開いたままです。ターミナル セッションが正しく終了していない場合、そのシリアル ポート上で開かれる次のセッションでは、認証が実行されません。

注意　接続を確立するために使用したアプリケーションを終了する前に、必ずセッションを終了してログイン プロンプトに戻ってください。

注意　誤って接続が切断されたり終了した場合は、接続を再確立し、正しく終了して、アプライアンスに対する不正なアクセスを防ぎます。

AIM IPS へのログイン

ここでは、AIM IPS へのセッションを確立する方法について説明します。内容は次のとおりです。

AIM IPS およびセッション コマンド

ルータ コンソールから AIM IPS へのセッションを確立します。AIM IPS は外部コンソール ポートを備えていないため、AIM IPS へのコンソール アクセスは、ルータで **service-module ids-sensor** *slot*/*port* **session** コマンドを発行したとき、または AIM IPS ポート番号に対応するスロット番号を使用してルータへの Telnet 接続を開始したときにイネーブルになります。外部コンソール ポートがないことは、初期ブート設定がルータを通じてのみ可能であることを意味します。

service-module ids-sensor *slot*/*port* **session** コマンドを発行すると、v との間にコンソール セッションが作成されます。このセッションで任意の IPS コンフィギュレーション コマンドを発行できます。セッションでの作業を完了し、IPS CLI を終了すると、Cisco IOS CLI に戻ります。

session コマンドを使用すると、IDS-Senso インターフェイスの IP アドレスを使用して逆方向の Telnet 接続が開始されます。IDS-Sensor インターフェイスは、AIM IPS とルータの間のインターフェイスです。**session** コマンドを起動する前に、IDS-Sensor インターフェイスに IP アドレスを割り当てる必要があります。ルーティング可能な IP アドレスを割り当てると、IDS-Sensor インターフェイス自体が攻撃に対して脆弱になります。これは、ルーティング可能な IP アドレスを通して、ネットワーク上で AIM IPS を確認できるようになるためです。つまり、ルータ外部にある AIM IPS と通信できるようになるためです。この脆弱性に対処するため、IDS-Sensor インターフェイスにアンナンバード IP アドレスを割り当てます。こうすると、AIM IPS IP アドレスはルータと AIM IPS 間でローカルにのみ使用されるようになり、AIM IPS との間にセッションを確立しようとする試みから隔離されます。

（注）　アプリケーション ソフトウェアのインストールまたはモジュール イメージの再作成を行う前にセッションを開始すると、ブートローダが起動します。ソフトウェアのインストール後、アプリケーションを始動するセッションを開始します。

注意　モジュールへのセッションを確立してコンソールから大規模な転送処理を実行する場合、ホスト コンソールのインターフェイス速度を 115200/bps 以上に設定しないと、文字のトラフィックが失われることがあります。速度が 115200/bps に設定されていることを確認するには、**show running config** コマンドを使用します。

詳細情報

アンナンバード IP アドレスを設定する手順については、「Using an Unnumbered IP Address Interface」を参照してください。

AIM IPS へのセッション接続

（注） ルータから AIM IPS を初期化（**setup** コマンドを実行）する必要があります。ネットワークを設定すると、SSH および Telnet が有効になります。

AIM IPS からルータへのセッションを確立するには、**service-module ids-sensor** *slot*/*port* **session** コマンドを使用します。セッション プロンプトをルータ プロンプトに戻すには（AIM IPS プロンプトからルータ プロンプトに戻るには）、**Ctrl キーと Shift キーを押した状態で 6 キー**を押し、続いて **x** を押します。セッション プロンプト（ルータ プロンプト）に戻るには、空白行で **Enter** を押します。ルータ コマンドを実行した後でこのセッションに戻る場合は、ルータに対するセッションを一時停止する必要があります。AIM IPS セッションに戻る予定のない場合は、セッションを一時停止するのではなく閉じてください。

セッションを閉じると、AIM IPS CLI から完全にログアウトします。ログインするには、新しいセッション接続を確立するためにユーザ名とパスワードを入力する必要があります。セッションを一時停止した場合は、CLI にログインしたまま残ります。**session** コマンドを使用して接続した場合は、ユーザ名とパスワードを入力せずに同じ CLI に戻ることができます。

（注） Telnet クライアントには多くの種類があります。クライアントによっては、**Ctrl キーを押した状態で 6 キーを押してから x キー**を押す必要があります。制御文字は、^^、Ctrl-^、または ASCII 値 30（16 進数では 1E）で表されます。

注意 **disconnect** コマンドを使用してセッションを終了しても、そのセッションは残ります。この開いている状態のセッションは、残った接続を利用しようとしている人間に悪用されるおそれがあります。

AIM IPS へのセッションを開始または終了するには、次の手順を実行します。

ステップ 1　ルータにログインします。

ステップ 2　AIM IPS のステータスをチェックし、実行中であることを確認します。

```
router# service-module ids-sensor 0/1 status
Service Module is Cisco IDS-Sensor0/1
Service Module supports session via TTY line 322
Service Module is in Steady state
Getting status from the Service Module, please wait..
Cisco Systems Intrusion Prevention System Network Module
  Software version:  6.2(1)E3
  Model:             AIM IPS
  Memory:            443508 KB
  Mgmt IP addr:      10.89.148.196
  Mgmt web ports:    443
  Mgmt TLS enabled:  true


router#
```

ステップ 3　ルータから AIM IPS へのセッションを開始します。

```
router# service-module ids-sensor 0/1 session
Trying 10.89.148.196, 2322 ... Open
```

ステップ 4　モジュール セッションを終了するか、または一時停止して終了します。

- `sensor# exit`

（注）　IPS CLI のサブモードにいる場合は、すべてのサブモードを終了する必要があります。センサーのログイン プロンプトが表示されるまで、**exit** と入力します。

注意　セッションを適切に終了しないと、残っているセッションを別のユーザが乗っ取ることが可能になります。Cisco IOS セッションを完全に終了するため、必ず `router#` プロンプトで **exit** と入力してください。

- AIM IPS へのセッションを一時停止して終了するには、**Ctrl キーを押した状態で Shift キー**を押し、**6** を押します。すべてのキーから指を放してから、**x** を押します。

（注）　セッションでの作業が終了したら、ルータに戻ってセッション（IPS アプリケーション）とモニタ対象のルータ インターフェイスの間の関連付けを確立する必要があります。

ステップ 5　ルータから接続解除します。

```
router# disconnect
```

ステップ 6　**Enter** キーを押して接続解除を確認します。

```
router# Closing connection to 10.89.148.196 [confirm] <Enter>
```

詳細情報

AIM IPS を初期化する手順については、「センサーの基本的なセットアップ」（P.23-5）を参照してください。

AIP SSM、AIP SSC-5、および IPS SSP へのログイン

（注）　ASA モジュール（AIP SSM、AIP SSC-5、および IPS SSP）を初期化すると、SSH と Telnet が有効になります。

適応型セキュリティ アプライアンスから ASA モジュールにログインします。

適応型セキュリティ アプライアンスから ASA モジュールへのセッションを確立するには、次の手順を実行します。

ステップ 1　適応型セキュリティ アプライアンスにログインします。

（注）　適応型セキュリティ アプライアンスがマルチモードで動作している場合は、続行する前に **change system** コマンドを使用して、システム レベルのプロンプトを表示させます。

ステップ 2　ASA モジュールとの間にセッションを確立します。

```
asa# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

ログインするためのセッション タイムアウトは 60 秒です。

ステップ 3　ログイン プロンプトに対してユーザ名とパスワードを入力します。

（注）　デフォルトのユーザ名とパスワードはどちらも **cisco** です。初めてモジュールにログインするとき、このユーザ名とパスワードを変更するように求めるメッセージが表示されます。最初に、UNIX パスワード（**cisco**）を入力してください。次に、新しいパスワードを 2 回入力します。

```
login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable laws and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license to obtain a new license or install a license.
aip-ssm#
```

ステップ 4　セッションからエスケープして適応型セキュリティ アプライアンス プロンプトに戻るには、次のいずれかの手順を実行します。

- **exit** と入力します。
- **Ctrl キーと Shift キーを押した状態で 6 キーを押し、続いて x** を押します（**CTRL^X** と表されます）。

詳細情報

- **setup** コマンドを使用して AIP SSM を初期化する手順については、「センサーの基本的なセットアップ」（P.23-5）を参照してください。

- **setup** コマンドを使用して IPS SSP を初期化する手順については、「IPS SSP の高度なセットアップ」（P.23-26）を参照してください。
- ASDM を使用して AIP SSC-5 を初期化する手順については、「ASDM での AIP SSC-5 のセットアップ」（P.23-8）を参照してください。

IDSM2 へのログイン

（注） スイッチから IDSM2 を初期化（**setup** コマンドを実行）する必要があります。ネットワークを設定すると、SSH および Telnet が有効になります。

スイッチから IDSM2 にログインします。

IDSM2 へのセッションを確立するには、次の手順を実行します。

ステップ 1　スイッチから IDSM2 へのセッションを確立します。

- Catalyst ソフトウェアの場合

```
console> (enable) session slot_number
```

- Cisco IOS ソフトウェアの場合

```
router# session slot_number processor 1
```

ステップ 2　ログイン プロンプトに対してユーザ名とパスワードを入力します。

（注） デフォルトのユーザ名とパスワードはどちらも **cisco** です。初めて IDSM2 にログインするとき、このユーザ名とパスワードを変更するように求めるメッセージが表示されます。最初に、UNIX パスワード（**cisco**）を入力してください。次に、新しいパスワードを 2 回入力します。

```
login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable laws and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license to obtain a new license or install a license.
idsm-2#
```

詳細情報

setup コマンドを使用して IDSM2 を初期化する手順については、「センサーの基本的なセットアップ」（P.23-5）を参照してください。

NME IPS へのログイン

ここでは、NME IPS へのセッションを確立する方法について説明します。内容は次のとおりです。

NME IPS およびセッション コマンド

ルータ コンソールから NME IPS へのセッションを確立します。NME IPS は外部コンソール ポートを備えていないため、NME IPS へのコンソール アクセスは、ルータで **service-module ids-sensor** *slot*/*port* **session** コマンドを発行したとき、または NME IPS ポート番号に対応するスロット番号を使用してルータへの Telnet 接続を開始したときにイネーブルになります。外部コンソール ポートがないことは、初期ブート設定がルータを通じてのみ可能であることを意味します。

service-module ids-sensor *slot*/*port* **session** コマンドを発行すると、NME IPS との間にコンソール セッションが作成されます。このセッションで任意の IPS コンフィギュレーション コマンドを発行できます。セッションでの作業を完了し、IPS CLI を終了すると、Cisco IOS CLI に戻ります。

session コマンドを使用すると、IDS-Senso インターフェイスの IP アドレスを使用して逆方向の Telnet 接続が開始されます。IDS-Sensor インターフェイスは、NME IPS とルータの間のインターフェイスです。**session** コマンドを起動する前に、IDS-Sensor インターフェイスに IP アドレスを割り当てる必要があります。ルーティング可能な IP アドレスを割り当てると、IDS-Sensor インターフェイス自体が攻撃に対して脆弱になります。これは、ルーティング可能な IP アドレスを通して、ネットワーク上で NME IPS を確認できるようになるためです。つまり、ルータ外部にある NME IPS と通信できるようになるためです。この脆弱性に対処するため、IDS-Sensor インターフェイスにアンナンバード IP アドレスを割り当てます。こうすると、NME IPS IP アドレスはルータと NME IPS 間でローカルにのみ使用されるようになり、NME IPS との間にセッションを確立しようとする試みから隔離されます。

（注） アプリケーション ソフトウェアのインストールまたはモジュール イメージの再作成を行う前にセッションを開始すると、ブートローダが起動します。ソフトウェアのインストール後、アプリケーションを始動するセッションを開始します。

注意 モジュールへのセッションを確立してコンソールから大規模な転送処理を実行する場合、ホスト コンソールのインターフェイス速度を 115200/bps 以上に設定しないと、文字のトラフィックが失われることがあります。速度が 115200/bps に設定されていることを確認するには、**show running config** コマンドを使用します。

詳細情報

アンナンバード IP アドレスを設定する手順については、「Setting Up Interfaces on NME IPS and the Router」を参照してください。

NME IPS へのセッション接続

（注） ルータから NME IPS を初期化（**setup** コマンドを実行）する必要があります。ネットワークを設定すると、SSH および Telnet が有効になります。

NME IPS からモジュールへのセッションを確立するには、**service-module ids-sensor** *slot*/*port* **session** コマンドを使用します。セッション プロンプトをルータ プロンプトに戻すには（NME IPS プロンプトからルータ プロンプトに戻るには）、**Ctrl キーと Shift キーを押した状態で 6 キー**を押し、続いて **x** を押します。セッション プロンプト（ルータ プロンプト）に戻るには、空白行で **Enter** を押します。ルータ コマンドを実行した後でこのセッションに戻る場合は、ルータに対するセッションを一時停止する必要があります。NME IPS セッションに戻る予定のない場合は、セッションを一時停止するのではなく閉じてください。

セッションを閉じると、NME IPS CLI から完全にログアウトします。ログインするには、新しいセッション接続を確立するためにユーザ名とパスワードを入力する必要があります。セッションを一時停止した場合は、CLI にログインしたまま残ります。**session** コマンドを使用して接続した場合は、ユーザ名とパスワードを入力せずに同じ CLI に戻ることができます。

（注） Telnet クライアントには多くの種類があります。クライアントによっては、**Ctrl キーを押した状態で 6 キーを押してから x キー**を押す必要があります。制御文字は、^^、Ctrl-^、または ASCII 値 30（16 進数では 1E）で表されます。

注意 **disconnect** コマンドを使用してセッションを終了しても、そのセッションは残ります。この開いている状態のセッションは、残った接続を利用しようとしている人間に悪用されるおそれがあります。

NME IPS へのセッションを開始または終了するには、次の手順を実行します。

ステップ 1　ルータにログインします。

ステップ 2　NME IPS のステータスをチェックし、実行中であることを確認します。

```
router# service-module ids-sensor 1/0 status
Service Module is Cisco IDS-Sensor1/0
Service Module supports session via TTY line 130
Service Module is in Steady state
Service Module heartbeat-reset is disabled
Getting status from the Service Module, please wait..

Cisco Systems Intrusion Prevention System Network Module
  Software version:  6.2(1)E3
  Model:             NME IPS
  Memory:            443508 KB
  Mgmt IP addr:      10.89.148.195
  Mgmt web ports:    443
  Mgmt TLS enabled:  true


router#
```

ステップ 3　ルータから NME IPS へのセッションを開始します。

```
router# service-module ids-sensor 1/0 session
Trying 10.89.148.195, 2322 ... Open
```

ステップ 4　モジュール セッションを終了するか、または一時停止して終了します。

- `sensor# exit`

（注）　IPS CLI のサブモードにいる場合は、すべてのサブモードを終了する必要があります。センサーのログイン プロンプトが表示されるまで、**exit** と入力します。

注意　セッションを適切に終了しないと、残っているセッションを別のユーザが乗っ取ることが可能になります。Cisco IOS セッションを完全に終了するため、必ず `router#` プロンプトで **exit** と入力してください。

- NME IPS へのセッションを一時停止して終了するには、**Ctrl キーを押した状態で Shift キー**を押し、**6** を押します。すべてのキーから指を放してから、**x** を押します。

（注）　セッションでの作業が終了したら、ルータに戻ってセッション（IPS アプリケーション）とモニタ対象のルータ インターフェイスの間の関連付けを確立する必要があります。

ステップ 5　ルータから接続解除します。

```
router# disconnect
```

ステップ 6　**Enter** キーを押して接続解除を確認します。

```
router# Closing connection to 10.89.148.196 [confirm] <Enter>
```

詳細情報

NME IPS を初期化する手順については、「センサーの基本的なセットアップ」（P.23-5）を参照してください。

センサーへのログイン

（注）　**setup** コマンドを使用してセンサーを初期化し、Telnet をイネーブルにすると、SSH または Telnet を使用してセンサーにログインできます。

センサーにログインするには、次の手順を実行します。

ステップ 1　SSH または Telnet を使用して、ネットワーク経由でセンサーにログインします。

```
ssh sensor_ip_address
telnet sensor_ip_address
```

ステップ 2　ログイン プロンプトに対してユーザ名とパスワードを入力します。

```
login: ******
Password: ******
***NOTICE***
```

```
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable law s and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license to obtain a new license or install a license.
sensor#
```

詳細情報

センサーを初期化する手順については、「センサーの基本的なセットアップ」（P.23-5）を参照してください。

CHAPTER 23

センサーの初期化

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

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

この章では、**setup** コマンドを使用してセンサーを初期化する方法について説明します。この章は、次の項で構成されています。

初期化について

（注） **setup** コマンドを使用するには、管理者である必要があります。

センサーをネットワークに設置したら、**setup** コマンドを使用してセンサーを初期化し、ネットワーク経由でセンサーが通信できるようにする必要があります。**setup** コマンドを使用してセンサーを初期化するまでは、IME の設定を行うことはできません。

setup コマンドを使用して、ホスト名、IP インターフェイス、アクセス コントロール リスト、グローバル相関サーバ、時間設定など、センサーの基本的な設定を行います。その後、続けて CLI の高度な設定を使用し、Telnet のイネーブル化、Web サーバの設定、仮想センサーとインターフェイスの割り当てとイネーブル化を実行できます。また、IME の Startup Wizard を使用することもできます。

（注）　AIP SSC-5 を初期化するために **setup** コマンドを実行する必要はありません。この場合は、ASDM を使用して初期化します。

注意　グローバル相関機能が動作するには、有効なセンサーのライセンスが必要です。グローバル相関機能の統計情報については引き続き設定および表示できますが、グローバル相関データベースはクリアされ、更新は試行されなくなります。有効なライセンスをインストールすると、グローバル相関機能が再アクティブ化されます。

（注）　AIP SSC-5 は、グローバル相関機能をサポートしていません。

詳細情報

- **setup** コマンドを使用して AIP SSM を初期化する手順については、「AIP SSM の高度なセットアップ」（P.23-17）を参照してください。
- **setup** コマンドを使用して IPS SSP を初期化する手順については、「IPS SSP の高度なセットアップ」（P.23-26）を参照してください。
- ASDM を使用して AIP SSC-5 を初期化する手順については、「ASDM での AIP SSC-5 のセットアップ」（P.23-8）を参照してください。
- **setup** コマンドを使用して AIM IPS を初期化する手順については、「AIM PS の高度なセットアップ」（P.23-15）を参照してください。
- **setup** コマンドを使用して NME IPS を初期化する手順については、「NME IPS の高度なセットアップ」（P.23-30）を参照してください。
- **setup** コマンドを使用して IDSM2 を初期化する手順については、「IDSM2 の高度なセットアップ」（P.23-21）を参照してください。

簡易セットアップ モード

コンソール ケーブルを使用してセンサーに接続すると、センサーが自動的に **setup** コマンドを呼び出します。この時点では、センサーの基本的なネットワーク設定はまだ行われていません。次の条件下では、センサーは自動セットアップの呼び出しを行いません。

- 初期化がすでに正常に完了している場合。
- センサーの回復またはダウングレードを行った場合。
- 自動セットアップを使用してセンサーを正常に設定した後、ホスト コンフィギュレーションをデフォルトにした場合。

setup コマンドを入力すると、システムのコンソール画面に [System Configuration Dialog] と呼ばれる対話形式のダイアログが表示されます。[System Configuration Dialog] に従って設定プロセスを進めます。前回設定されたデフォルト値は、各プロンプトの横のカッコ内に表示されます。

システム設定ダイアログ

（注）　IPS 6.1 および 6.2 は、グローバル相関機能をサポートしていません。

（注）　AIP SSC-5 は、グローバル相関機能をサポートしていません。

（注）　AIP SSC-5 を初期化するために **setup** コマンドを実行する必要はありません。この場合は、ASDM を使用して初期化します。

setup コマンドを入力すると、システムのコンソール画面に [System Configuration Dialog] と呼ばれる対話形式のダイアログが表示されます。[System Configuration Dialog] に従って設定プロセスを進めます。現在の値は、各プロンプトの横のカッコ内に表示されます。

変更するオプションに到達するまで [System Configuration Dialog] 全体を実行する必要があります。変更しない項目のデフォルト設定を使用するには、Enter キーを押します。

変更を中断し、[System Configuration Dialog] を最後まで実行せずに [EXEC] プロンプトに戻るには、Ctrl+C を押します。

[System Configuration Dialog] では、各プロンプトのヘルプ テキストを表示できます。ヘルプ テキストを表示するには、プロンプトで疑問符（**?**）を入力します。

変更が完了したら、セットアップ セッション中に作成した設定が [System Configuration Dialog] に表示されます。また、この設定を使用するかどうかを問い合わせてきます。**yes** を入力すると、その設定が保存されます。**no** を入力すると、設定は保存されずにプロセスが再開されます。このプロンプトにはデフォルトがありません。**yes** または **no** を入力する必要があります。

サマータイムは、[recurring] モードまたは [date] モードのいずれかで設定できます。[recurring] モードを選択すると、開始日および終了日は、週、日、月、および時間がベースになります。[date] モードを選択すると、開始日および終了日は、月、日、年、および時間がベースになります。[disable] を選択すると、サマータイムがオフになります。

（注）　システムがアプライアンスで NTP を使用していない場合は、[System Configuration Dialog] で日付と時間を設定するだけで済みます。

（注）　System Configuration Dialog は対話型のダイアログです。デフォルトの設定が表示されています。

例 23-1 に、[System Configuration Dialog] の例を示します。

例 23-1　[System Configuration Dialog] の例

```
    --- Basic Setup ---

    --- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.
```

```
Current time: Wed Nov 11 21:19:51 2009

Setup Configuration last modified:

Enter host name[sensor]:
Enter IP interface[192.168.1.2/24,192.168.1.1]:
Modify current access list?[no]:
Current access list entries:
  [1] 0.0.0.0/0
Delete:
Permit:
Use DNS server for Global Correlation?[no]:
DNS server IP address[171.68.226.120]:
Use HTTP proxy server for Global Correlation?[no]:
HTTP proxy server IP address[128.107.241.169]:
HTTP proxy server Port number[8080]:
Modify system clock settings?[no]:
  Modify summer time settings?[no]:
    Use USA SummerTime Defaults?[yes]:
    Recurring, Date or Disable?[Recurring]:
    Start Month[march]:
    Start Week[second]:
    Start Day[sunday]:
    Start Time[02:00:00]:
    End Month[november]:
    End Week[first]:
    End Day[sunday]:
    End Time[02:00:00]:
    DST Zone[]:
    Offset[60]:
  Modify system timezone?[no]:
    Timezone[UTC]:
    UTC Offset[0]:
  Use NTP?[no]: yes
    NTP Server IP Address[]:
    Use NTP Authentication?[no]: yes
      NTP Key ID[]: 1
      NTP Key Value[]: 8675309
Participation in the SensorBase Network allows Cisco to collect aggregated statistics
about traffic sent to your IPS.
SensorBase Network Participation level?[off]: full

If you agree to participate in the SensorBase Network, Cisco will collect aggregated
statistics about traffic sent to your IPS.
This includes summary data on the Cisco IPS network traffic properties and how this
traffic was handled by the Cisco appliances.We do not collect the data content of traffic
or other sensitive business or personal information.All data is aggregated and sent via
secure HTTP to the Cisco SensorBase Network servers in periodic intervals.All data shared
with Cisco will be anonymous and treated as strictly confidential.
The table below describes how the data will be used by Cisco.
Participation Level = "Partial":
* Type of Data: Protocol Attributes (e.g. TCP max segment size and
    options string)
    Purpose: Track potential threats and understand threat exposure
  * Type of Data: Attack Type (e.g. Signature Fired and Risk Rating)
    Purpose: Used to understand current attacks and attack severity
  * Type of Data: Connecting IP Address and port
    Purpose: Identifies attack source
  * Type of Data: Summary IPS performance (CPU utilization memory usage,
    inline vs.promiscuous, etc)
    Purpose: Tracks product efficacy
Participation Level = "Full" additionally includes:
```

```
* Type of Data: Victim IP Address and port
    Purpose: Detect threat behavioral patterns

Do you agree to participate in the SensorBase Network?[no]:
```

センサーの基本的なセットアップ

（注）　IPS 6.1 および 6.2 は、グローバル相関機能をサポートしていません。

（注）　AIP SSC-5 は、グローバル相関機能をサポートしていません。

（注）　AIP SSC-5 を初期化するために **setup** コマンドを実行する必要はありません。この場合は、ASDM を使用して初期化します。

setup コマンドを使用して、センサーの基本的なセットアップを行うことができます。その後、続けて CLI、IDM、または IME を使用してセンサーのセットアップを完了させることができます。

setup コマンドを使用してセンサーの基本的なセットアップを行うには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して次のようにセンサーにログインします。

（注）　デフォルトのユーザ名とパスワードはどちらも **cisco** です。

ステップ 2　センサーへの初回ログインでは、デフォルト パスワードの変更を求められます。パスワードは最低 8 文字で、強力なパスワードにする必要があります。辞書にある単語は使用しないでください。パスワードを変更すると、基本的なセットアップが開始します。

ステップ 3　`setup` コマンドを入力します。System Configuration Dialog が表示されます。

ステップ 4　ホスト名を指定します。ホスト名は 64 文字までの文字列で、大文字と小文字が区別されます。数字、「_」、および「-」は使用できますが、スペースは受け付けられません。デフォルトは sensor です。

ステップ 5　IP インターフェイスを指定します。IP インターフェイスは、IP アドレス / ネットマスク , ゲートウェイ（*X.X.X.X/nn,Y.Y.Y.Y*）の形式で指定します。ここで、*X.X.X.X* は、32 ビット アドレスのセンサーの IP アドレスで、ピリオドで区切った 4 つのオクテットで記述されています。*nn* はネットマスクのビット数です。*Y.Y.Y.Y* は、32 ビット アドレスのデフォルト ゲートウェイで、ピリオドで区切った 4 つのオクテットで記述されています。

ステップ 6　`yes` と入力してネットワーク アクセス リストを修正します。

a. エントリを削除する場合は、エントリの番号を入力して Enter キーを押すか、または Enter キーを押して Permit 行に進みます

b. アクセス リストに追加するネットワークの IP アドレスおよびネットマスクを指定します。

たとえば、10.0.0.0/8 は 10.0.0.0 ネットワーク上のすべての IP アドレス（10.0.0.0 ～ 10.255.255.255）を許可し、10.1.1.0/24 は 10.1.1.0 サブネット上の IP アドレスだけ（10.1.1.0 ～ 10.1.1.255）を許可します。ネットワーク全体ではなく単一の IP アドレスへのアクセスを許可する場合は、32 ビット ネットマスクを使用します。たとえば、10.1.1.1/32 は 10.1.1.1 のアドレスだけを許可します。

c. アクセス リストに追加するネットワークをすべて入力し終わるまで、ステップ b を繰り返します。終わったら、空白の Permit 行で Enter キーを押して、次の手順に進みます。

ステップ 7　グローバル相関が動作するように DNS サーバまたは HTTP プロキシ サーバを設定する必要があります。

a. **yes** を入力すると、DNS サーバが追加されます。その後、続けて DNS サーバの IP アドレスを入力します。

b. **yes** を入力すると、HTTP プロキシ サーバが追加されます。その後、続けて HTTP プロキシ サーバの IP アドレスおよびポート番号を入力します。

注意　グローバル相関機能が動作するには、有効なセンサーのライセンスが必要です。グローバル相関機能の統計情報については引き続き設定および表示できますが、グローバル相関データベースはクリアされ、更新は試行されなくなります。有効なライセンスをインストールすると、グローバル相関機能が再アクティブ化されます。

ステップ 8　システム クロックの設定値を修正するには、**yes** と入力します。

a. サマータイム設定を修正するには、**yes** と入力します。

（注）　サマータイムは DST とも呼びます。サマータイムを採用していない地域の場合は、ステップ m に進みます。

b. 米国のサマータイムのデフォルトを選択するには、**yes** と入力します。または、サマータイムの設定方法を指定するには、**no** と入力して [recurring]、[date]、または [disable] を選択します。デフォルトは [recurring] です。

c. [recurring] を選択した場合は、サマータイム設定の開始月を入力します。

有効な値は、january、february、march、april、may、june、july、august、september、october、november および december です。デフォルト値は march です。

d. サマータイム設定の開始週を指定します。有効な値は first、second、third、fourth、fifth、および last です。デフォルトは値 second です。

e. サマータイム設定の開始曜日を指定します。有効な値は、sunday、monday、tuesday、wednesday、thursday、friday、および saturday です。デフォルト値は sunday です。

f. サマータイム設定の開始時刻を指定します。デフォルト値は 02:00:00 です。

（注）　デフォルトの定期的なサマータイム パラメータはアメリカ合衆国の時間帯用です。デフォルト値は、開始時刻が 3 月の第 2 日曜日午前 2 時、終了時刻が 11 月の第 1 日曜日午前 2 時と指定します。デフォルトのサマータイム オフセットは 60 分です。

g. サマータイム設定の終了月を指定します。有効な値は、january、february、march、april、may、june、july、august、september、october、november および december です。デフォルト値は november です。

h. サマータイム設定の終了週を指定します。有効な値は first、second、third、fourth、fifth、および last です。デフォルトは first です。

i. サマータイム設定の終了曜日を指定します。有効な値は、sunday、monday、tuesday、wednesday、thursday、friday、および saturday です。デフォルト値は sunday です。

j. サマータイム設定の終了時刻を指定します。デフォルト値は 02:00:00 です。

k. DST ゾーンを指定します。ゾーン名は、最長で 24 文字の文字列で、[A-Za-z0-9()+:,_/-]+$ を使用できます。

l. サマータイム オフセットを指定します。協定世界時（UTC）からのサマータイム オフセットを分単位で指定します（負数は、グリニッジ子午線より西側の時間帯を示します）。デフォルトは 60 です。

m. システムの時間帯を修正するには、**yes** と入力します。

n. 標準時の時間帯名を指定します。ゾーン名には 24 文字までの文字列を使用できます。

o. 標準時の時間帯のオフセットを指定します。

UTC からの標準時間帯のオフセットを分単位で指定します（負数は、グリニッジ子午線より西側の時間帯を示します）デフォルトは 0 です。

p. NTP を使用する場合は **yes** と入力します。認証された NTP を使用するには、NTP サーバの IP アドレス、NTP キー ID、および NTP キー値が必要です。これらがこの時点で存在しない場合は、後で NTP を設定できます。または、認証されていない NTP を選択できます。

ステップ 9　SensorBase Network Participation に参加するには、**off**、**partial**、または **full** と入力します。

- Off : どのデータも SensorBase ネットワークに提供されません。
- Partial : データは SensorBase ネットワークに提供されますが、潜在的に機密性が高いと見なされるデータはフィルタリングによって除外され、送信されません。
- Full : 除外された攻撃者 / 攻撃対象者の IP アドレスを除き、すべてのデータが SensorBase ネットワークに提供されます。

SensorBase Network Participation の免責事項が表示されます。ここでは、SensorBase Network に参加する際に必要なものが示されます。

ステップ 10　**yes** と入力して SensorBase Network に参加します。

```
The following configuration was entered.
service host
network-settings
host-ip 10.89.143.126/24,10.89.143.254
host-name sensor126
telnet-option disabled
access-list 10.0.0.0/8
ftp-timeout 300
no login-banner-text
dns-primary-server enabled
address 171.68.226.120
exit
dns-secondary-server disabled
dns-tertiary-server disabled
http-proxy proxy-server
address 128.107.241.170
port 8080
exit
time-zone-settings
offset -360
standard-time-zone-name CST
exit
summertime-option recurring
offset 60
summertime-zone-name CDT
start-summertime
month march
week-of-month second
day-of-week sunday
time-of-day 02:00:00
exit
```

```
end-summertime
month november
week-of-month first
day-of-week sunday
time-of-day 02:00:00
exit
exit
ntp-option enabled
ntp-keys 1 md5-key 8675309
ntp-servers 10.89.143.92 key-id 1
exit
service global-correlation
network-participation full
exit


[0] Go to the command prompt without saving this config.
[1] Return to setup without saving this config.
[2] Save this configuration and exit setup.
[3] Continue to Advanced setup.
```

ステップ 11　設定を保存するには、**2** と入力します（または、**3** と入力して、CLI、IDM、または IME を使用した高度なセットアップに進みます）。

```
Enter your selection[2]: 2
Configuration Saved.
```

ステップ 12　センサーをリブートするには、**yes** と入力します。

ステップ 13　リブート後、センサーにログインし、自己署名 X.509 証明書を表示します（TLS で必要です）。

```
sensor# show tls fingerprint
MD5: C4:BC:F2:92:C2:E2:4D:EB:92:0F:E4:86:53:6A:C6:01
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
```

ステップ 14　証明書のフィンガープリントを書き留めます。このフィンガープリントは、Web ブラウザでこのアプライアンスに HTTPS を使用して接続したときに、証明書の信頼性を確認するために必要になります。

ステップ 15　最新のサービス パックおよびシグニチャ アップデートを適用します。これでセンサーの侵入防御設定を行う準備ができました。

詳細情報

- 最新のサービス パックおよびシグニチャ アップデートの取得手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。
- AIP SSC-5 を初期化する手順については、「ASDM での AIP SSC-5 のセットアップ」（P.23-8）を参照してください。

ASDM での AIP SSC-5 のセットアップ

AIP SSC-5 の初期化では、他のセンサーのように IPS CLI で **setup** コマンドを実行する必要はありません。AIP SSC-5 は、ASDM から初期化できます。ASDM を起動すると、AIP SSC-5 の管理インターフェイスに接続され、次のデフォルト ネットワーク パラメータが設定されます。

- 管理 VLAN：VLAN 1
- 管理 IP アドレス：192.168.1.1/24

（注）　適応型セキュリティ アプライアンスのデフォルトの管理 IP アドレスは 192.168.1.1/24 です。

- ゲートウェイ：192.168.1.1
- ユーザ名およびパスワード：**cisco**

ASDM でデフォルト パラメータを変更するには、[Configuration] > [Device Setup] > [SSC Setup] を選択します。AIP SSC-5 で IPS のより高度な設定を行うには、[IPS] タブをクリックして IDM を起動するか、IPS CLI にログインします。

詳細情報

- ASDM の使用方法の詳細については、ASDM のマニュアルを参照してください。
- 最新のサービス パックおよびシグニチャ アップデートの取得手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。

高度なセットアップ

この項では、基本的なセットアップに続けて CLI の Advanced Setup を使用し、さまざまな Cisco IPS プラットフォームの高度なセットアップを行う方法について説明します。内容は次のとおりです。

アプライアンスの高度なセットアップ

（注）　現在サポートされている Cisco IPS アプライアンスは、IPS 4240、IPS 4255、IPS 4260、および IPS 4270-20 です。

新しいサブインターフェイスの追加は、2 つのステップからなるプロセスです。まず、仮想センサーの設定を編集するときにインターフェイスを分類します。次に、どのインターフェイスとサブインターフェイスをどの仮想センサーに割り当てるかを選択します。インターフェイスはアプライアンスのモデルによって異なりますが、プロンプトはすべてのモデルで同じです。

続けてアプライアンスの高度なセットアップを行うには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用してアプライアンスにログインします。

ステップ 2　`setup` コマンドを入力します。System Configuration Dialog が表示されます。

ステップ 3　高度なセットアップにアクセスするには、`3` と入力します。

ステップ 4　Telnet サーバのステータスを指定します。デフォルトはディセーブルです。

ステップ 5　Web サーバ ポートを指定します。Web サーバ ポートは Web サーバが使用する TCP ポートです（1 ～ 65535）。デフォルトは 443 です。

（注）　デフォルトでは、Web サーバは TLS および SSL の暗号化を使用するように設定されています。ポートを 80 に設定しても、暗号化はディセーブルになりません。

ステップ 6　**yes** と入力して、インターフェイスと仮想センサーの設定を修正します。現在のインターフェイス設定が表示されます

```
Current interface configuration
 Command control: Management0/0
 Unassigned:
  Promiscuous:
   GigabitEthernet0/0
   GigabitEthernet0/1
   GigabitEthernet0/2
   GigabitEthernet0/3

 Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

 Virtual Sensor: vs1
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

 Virtual Sensor: vs2
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

ステップ 7　インターフェイス設定を編集するには、**1** と入力します。

（注）　次のオプションを使用して、インターフェイスを作成および削除できます。インターフェイスを仮想センサーの設定に含まれる仮想センサーに割り当てます。インターフェイスに無差別モードを使用していて、インターフェイスを VLAN で分割していない場合、追加の設定は必要ありません。

```
[1] Remove interface configurations.
  [2] Add/Modify Inline Vlan Pairs.
  [3] Add/Modify Promiscuous Vlan Groups.
  [4] Add/Modify Inline Interface Pairs.
  [5] Add/Modify Inline Interface Pair Vlan Groups.
  [6] Modify interface default-vlan.
Option:
```

ステップ 8　インライン VLAN ペアを追加するには、**2** と入力します。使用可能なインターフェイスのリストが表示されます。

注意　新しい VLAN ペアが仮想センサーに自動的に追加されることはありません。

```
Available Interfaces
  [1] GigabitEthernet0/0
  [2] GigabitEthernet0/1
  [3] GigabitEthernet0/2
  [4] GigabitEthernet0/3
Option:
```

ステップ 9　インライン VLAN ペアを GigabitEthernet0/0 に追加するには、**1** と入力します。たとえば、次のようになります。

```
Inline Vlan Pairs for GigabitEthernet0/0
   None
```

ステップ 10　サブインターフェイス番号と説明を入力します。

```
Subinterface Number:
Description[Created via setup by user asmith]:
```

ステップ 11　VLAN 1 および VLAN 2 の数を入力します。

```
Vlan1[]: 200
Vlan2[]: 300
```

ステップ 12　Enter キーを押して使用可能なインターフェイスのメニューに戻ります。

（注）　プロンプトに値を入れずに改行すると、前のメニューに戻ります。

```
  [1] GigabitEthernet0/0
  [2] GigabitEthernet0/1
  [3] GigabitEthernet0/2
  [4] GigabitEthernet0/3
Option:
```

（注）　この時点で、インライン VLAN ペアのもう 1 つのインターフェイス（GigabitEthernet0/1 など）を設定できます。

ステップ 13　Enter キーを押して、最上位レベルのインターフェイス編集メニューに戻ります。

```
[1] Remove interface configurations.
  [2] Add/Modify Inline Vlan Pairs.
  [3] Add/Modify Promiscuous Vlan Groups.
  [4] Add/Modify Inline Interface Pairs.
  [5] Add/Modify Inline Interface Pair Vlan Groups.
  [6] Modify interface default-vlan.
Option:
```

ステップ 14　インライン インターフェイス ペアを追加するには、**4** と入力します。次のオプションが表示されます。

```
Available Interfaces
   GigabitEthernet0/1
   GigabitEthernet0/2
   GigabitEthernet0/3
```

ステップ 15　ペア名、説明、およびペアにするインターフェイスを入力します。

```
Pair name: newPair
```

```
Description[Created via setup by user asmith:
Interface1[]: GigabitEthernet0/1
Interface2[]: GigabitEthernet0/2
Pair name:
```

ステップ 16　Enter キーを押して、最上位レベルのインターフェイス編集メニューに戻ります。

```
  [1] Remove interface configurations.
  [2] Add/Modify Inline Vlan Pairs.
  [3] Add/Modify Promiscuous Vlan Groups.
  [4] Add/Modify Inline Interface Pairs.
  [5] Add/Modify Inline Interface Pair Vlan Groups.
  [6] Modify interface default-vlan.
Option:
```

ステップ 17　Enter キーを押して、最上位レベルの編集メニューに戻ります。

```
  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

ステップ 18　仮想センサーの設定を編集するには、**2** と入力します。

```
  [1] Remove virtual sensor.
  [2] Modify "vs0" virtual sensor configuration.
  [3] Create new virtual sensor.
Option:
```

ステップ 19　仮想センサーの設定 vs0 を修正するには、**2** と入力します。

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

No Interfaces to remove.

 Unassigned:
  Promiscuous:
   [1] GigabitEthernet0/3
   [2] GigabitEthernet0/0
  Inline Vlan Pair:
   [3] GigabitEthernet0/0:1  (Vlans: 200, 300)
  Inline Interface Pair:
   [4] newPair (GigabitEthernet0/1, GigabitEthernet0/2)
Add Interface:
```

ステップ 20　インライン VLAN ペア GigabitEthernet0/0:1 を追加するには、**3** と入力します。

ステップ 21　インライン インターフェイス ペア NewPair を追加するには、**4** と入力します。

ステップ 22　Enter キーを押して、最上位レベルの仮想センサー メニューに戻ります。

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0
  Inline Vlan Pair:
   GigabitEthernet0/0:1  (Vlans: 200, 300)
  Inline Interface Pair:
   newPair (GigabitEthernet0/1, GigabitEthernet0/2)

  [1] Remove virtual sensor.
  [2] Modify "vs0" virtual sensor configuration.
  [3] Create new virtual sensor.
```

```
Option: GigabitEthernet0/1, GigabitEthernet0/2)
Add Interface:
```

ステップ 23　Enter キーを押して、最上位レベルのインターフェイスおよび仮想センサー設定メニューに戻ります。

```
  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

ステップ 24　デフォルトの脅威防御設定を修正する場合は、**yes** と入力します。

（注）　センサーには、パケットの拒否イベント アクションを高リスク評価のアラートに追加するためのオーバーライドが組み込まれています。この保護が不要な場合は、自動脅威防御をディセーブルにします。

```
Virtual sensor newVs is configured to prevent high risk threats in inline mode. (Risk
Rating 90-100)
Virtual sensor vs0 is configured to prevent high risk threats in inline mode.(Risk Rating
90-100)
Do you want to disable automatic threat prevention on all virtual sensors?[no]:
```

ステップ 25　すべての仮想センサーで自動脅威防御をディセーブルにするには、**yes** と入力します。

ステップ 26　Enter キーを押して、インターフェイスと仮想センサーの設定を終了します。

```
The following configuration was entered.
service host
network-settings
host-ip 192.168.1.2/24,192.168.1.1
host-name sensor
telnet-option disabled
ftp-timeout 300
no login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service web-server
port 342
exit
service interface
physical-interfaces GigabitEthernet0/0
admin-state enabled
subinterface-type inline-vlan-pair
subinterface 1
description Created via setup by user asmith
vlan1 200
vlan2 300
exit
exit
exit
physical-interfaces GigabitEthernet0/1
admin-state enabled
exit
physical-interfaces GigabitEthernet0/2
admin-state enabled
exit
```

```
physical-interfaces GigabitEthernet0/0
admin-state enabled
exit
inline-interfaces newPair
description Created via setup by user asmith
interface1 GigabitEthernet0/1
interface2 GigabitEthernet0/2
exit
exit
service analysis-engine
virtual-sensor newVs
description Created via setup by user cisco
signature-definition newSig
event-action-rules rules0
anomaly-detection
anomaly-detection-name ad0
operational-mode inactive
exit
physical-interface GigabitEthernet0/0
exit
virtual-sensor vs0
physical-interface GigabitEthernet0/0 subinterface-number 1
logical-interface newPair
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Disabled
risk-rating-range 90-100
exit
exit

[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.
```

ステップ 27　設定を保存するには、**2** と入力します。

```
Enter your selection[2]: 2
Configuration Saved.
```

ステップ 28　アプライアンスをリブートします。

```
sensor# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? []:
```

ステップ 29　リブートを続行するには、**yes** と入力します。

ステップ 30　最新のサービス パックおよびシグニチャ アップデートを適用します。

これでアプライアンスの侵入防御設定を行う準備ができました。

詳細情報

最新のサービス パックおよびシグニチャ アップデートの取得手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。

AIM PS の高度なセットアップ

続けて AIM IPS の高度なセットアップを行うには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して AIM IPS のセッションを開始します。

```
router# service-module ids-sensor 0/0 session
Trying 10.1.9.1, 2322 ... Open


sensor login: cisco
Password: ********
```

ステップ 2　**setup** コマンドを入力します。System Configuration Dialog が表示されます。

ステップ 3　高度なセットアップにアクセスするには、**3** と入力します。

ステップ 4　Telnet サーバのステータスを指定します。Telnet サービスをディセーブルまたはイネーブルにできます。デフォルトはディセーブルです。

ステップ 5　Web サーバ ポートを指定します。

Web サーバ ポートは Web サーバが使用する TCP ポートです（1 ～ 65535）。デフォルトは 443 です。

（注）　デフォルトでは、Web サーバは TLS および SSL の暗号化を使用するように設定されています。ポートを 80 に設定しても、暗号化はディセーブルになりません。

ステップ 6　**yes** と入力して、インターフェイスと仮想センサーの設定を修正します。

分析エンジンが初期化中で、現在仮想センサーの設定を修正できないという警告が表示される場合があります。Space キーを押して、次のメニューを表示します。

```
[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.

Enter your selection[2]:
```

分析エンジンが初期化中という警告が表示された場合は、**2** と入力してここまでの設定を保存し、セットアップを終了します。その後、セットアップを再開し、インターフェイスおよび仮想センサー設定メニューに戻るまで Enter キーを押します。

ステップ 7　仮想センサーの設定を修正するには、**2** と入力します。

```
Modify interface/virtual sensor configuration?[no]: yes
Current interface configuration
 Command control: Management0/0
 Unassigned:
  Monitored:
   GigabitEthernet0/1

 Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

ステップ 8　仮想センサー vs0 の設定を編集するには、**2** と入力します。

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

No Interfaces to remove.

Unassigned:
  Monitored:
   [1] GigabitEthernet0/1
Add Interface:
```

ステップ 9　仮想センサー vs0 に GigabitEthernet0/1 を追加するには、**1** と入力します。

```
Add Interface: 1

 Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0
  Monitored:
   GigabitEthernet0/1

  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

ステップ 10　Enter キーを押して、インターフェイスおよび仮想センサー設定メニューを終了します。

```
Modify default threat prevention settings?[no]:
```

ステップ 11　デフォルトの脅威防御設定を修正する場合は、**yes** と入力します。

（注）　センサーには、パケットの拒否イベント アクションを高リスク評価のアラートに追加するためのオーバーライドが組み込まれています。この保護が不要な場合は、自動脅威防御をディセーブルにします。

```
Virtual sensor newVs is configured to prevent high risk threats in inline mode. (Risk
Rating 90-100)
Virtual sensor vs0 is configured to prevent high risk threats in inline mode.(Risk Rating
90-100)
Do you want to disable automatic threat prevention on all virtual sensors?[no]:
```

ステップ 12　すべての仮想センサーで自動脅威防御をディセーブルにするには、**yes** と入力します。

```
The following configuration was entered.

service host
network-settings
host-ip 10.1.9.201/24,10.1.9.1
host-name aim-ips
telnet-option disabled
access-list 10.0.0.0/8
access-list 64.0.0.0/8
ftp-timeout 300
no login-banner-text
exit
time-zone-settings
offset 0
```

```
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service web-server
port 443
exit
service analysis-engine
virtual-sensor vs0
physical-interface GigabitEthernet0/1
exit
exit
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Disabled
risk-rating-range 90-100
exit
exit

[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.
```

ステップ 13　設定を保存するには、**2** と入力します。

```
Enter your selection[2]: 2
Configuration Saved.
```

ステップ 14　AIM IPS をリブートします。

```
aim-ips# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? []:
```

ステップ 15　リブートを続行するには、**yes** と入力します。

ステップ 16　最新のサービス パックおよびシグニチャ アップデートを適用します。これで、AIM IPS に侵入防御を設定する準備ができました。

詳細情報

最新のサービス パックおよびシグニチャ アップデートの取得手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。

AIP SSM の高度なセットアップ

続けて AIP SSM の高度なセットアップを行うには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して AIP SSM のセッションを開始します。

```
asa# session 1
```

ステップ 2　**setup** コマンドを入力します。System Configuration Dialog が表示されます。

ステップ 3　高度なセットアップにアクセスするには、**3** と入力します。

ステップ 4　Telnet サーバのステータスを指定します。Telnet サービスをディセーブルまたはイネーブルにできます。デフォルトはディセーブルです。

ステップ 5　Web サーバ ポートを指定します。Web サーバ ポートは Web サーバが使用する TCP ポートです（1 ～ 65535）。デフォルトは 443 です。

（注）　デフォルトでは、Web サーバは TLS および SSL の暗号化を使用するように設定されています。ポートを 80 に設定しても、暗号化はディセーブルになりません。

ステップ 6　**yes** と入力して、インターフェイスと仮想センサーの設定を修正します。

```
Current interface configuration
 Command control: GigabitEthernet0/0
 Unassigned:
  Monitored:
   GigabitEthernet0/1

 Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

ステップ 7　インターフェイス設定を編集するには、**1** と入力します。

（注）　AIP SSM にはインターフェイスを設定する必要はありません。Modify interface default-vlan 設定は無視する必要があります。仮想センサー間でトラフィックを分離する場合は、他のセンサーとは別に AIP SSM を設定します。

```
  [1] Modify interface default-vlan.
Option:
```

ステップ 8　Enter キーを押して、最上位レベルのインターフェイスおよび仮想センサー設定メニューに戻ります。

```
  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

ステップ 9　仮想センサーの設定を編集するには、**2** と入力します。

```
  [1] Remove virtual sensor.
  [2] Modify "vs0" virtual sensor configuration.
  [3] Create new virtual sensor.
Option:
```

ステップ 10　仮想センサー vs0 の設定を修正するには、**2** と入力します。

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

No Interfaces to remove.

 Unassigned:
  Monitored:
   [1] GigabitEthernet0/1
Add Interface:
```

ステップ 11　仮想センサー vs0 に GigabitEthernet0/1 を追加するには、**1** と入力します。

（注）　ASA 7.2 以前では、1 つの仮想センサーがサポートされています。適応型セキュリティ アプライアンスから着信するパケットのモニタリングには、GigabitEthernet0/1 が割り当てられた仮想センサーが使用されます。GigabitEthernet0/1 は vs0 に割り当てることを推奨しますが、必要ならば別の仮想センサーに割り当ててもかまいません。

（注）　IPS 6.0 以降を実行する ASA 7.2.3 以降では、複数の仮想センサーがサポートされています。ASA 7.2.3 では、パケットを特定の仮想センサーのモニタリング対象にすることも、デフォルトの仮想センサーのモニタリング対象とすることもできます。デフォルトの仮想センサーは、GigabitEthernet0/1 が割り当てられている仮想センサーです。GigabitEthernet0/1 は vs0 に割り当てることを推奨しますが、必要ならば別の仮想センサーに割り当ててもかまいません。

ステップ 12　Enter キーを押して、メインの仮想センサー メニューに戻ります。

ステップ 13　仮想センサーを作成するには、**3** と入力します。

```
Name[]:
```

ステップ 14　仮想センサーの名前と説明を入力します。

```
Name[]: newVs
Description[Created via setup by user cisco]: New Sensor
Anomaly Detection Configuration
  [1] ad0
  [2] Create a new anomaly detection configuration
Option[2]:
```

ステップ 15　既存の異常検出の設定 ad0 を使用するには、**1** と入力します。

```
Signature Definition Configuration
  [1] sig0
  [2] Create a new signature definition configuration
Option[2]:
```

ステップ 16　シグニチャ定義のコンフィギュレーション ファイルを作成するには、**2** と入力します。

ステップ 17　シグニチャ定義の設定名 **newSig** を入力します。

```
Event Action Rules Configuration
  [1] rules0
  [2] Create a new event action rules configuration
Option[2]:
```

ステップ 18　既存のイベント アクション規則の設定 rules0 を使用するには、**1** と入力します。

（注）　GigabitEthernet0/1 が vs0 に割り当てられていない場合、新しい仮想センサーに割り当てるようにプロンプトが表示されます。

（注）　ASA 7.2 以前では、1 つの仮想センサーがサポートされています。適応型セキュリティ アプライアンスから着信するパケットのモニタリングには、GigabitEthernet0/1 が割り当てられた仮想センサーが使用されます。GigabitEthernet0/1 は vs0 に割り当てることを推奨しますが、必要ならば別の仮想センサーに割り当ててもかまいません。

（注）　IPS 6.0 を実行する ASA 7.2.3 以降では、複数の仮想センサーがサポートされています。ASA 7.2.3 では、パケットを特定の仮想センサーのモニタリング対象にすることも、デフォルトの仮想センサーのモニタリング対象とすることもできます。デフォルトの仮想センサーは、GigabitEthernet0/1 が割り当てられている仮想センサーです。GigabitEthernet0/1 は vs0 に割り当てることを推奨しますが、必要ならば別の仮想センサーに割り当ててもかまいません。

```
Virtual Sensor: newVs
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: newSig
  Monitored:
   GigabitEthernet0/1

  [1] Remove virtual sensor.
  [2] Modify "newVs" virtual sensor configuration.
  [3] Modify "vs0" virtual sensor configuration.
  [4] Create new virtual sensor.
Option:
```

ステップ 19　Enter キーを押して、インターフェイスおよび仮想センサー設定メニューを終了します。

```
Modify default threat prevention settings?[no]:
```

ステップ 20　デフォルトの脅威防御設定を修正する場合は、**yes** と入力します。

（注）　センサーには、パケットの拒否イベント アクションを高リスク評価のアラートに追加するためのオーバーライドが組み込まれています。この保護が不要な場合は、自動脅威防御をディセーブルにします。

```
Virtual sensor newVs is configured to prevent high risk threats in inline mode. (Risk
Rating 90-100)
Virtual sensor vs0 is configured to prevent high risk threats in inline mode.(Risk Rating
90-100)
Do you want to disable automatic threat prevention on all virtual sensors?[no]:
```

ステップ 21　すべての仮想センサーで自動脅威防御をディセーブルにするには、**yes** と入力します。

```
The following configuration was entered.

service host
network-settings
host-ip 10.1.9.201/24,10.1.9.1
host-name aip-ssm
telnet-option disabled
access-list 10.0.0.0/8
access-list 64.0.0.0/8
ftp-timeout 300
no login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service web-server
port 342
exit
```

```
service analysis-engine
virtual-sensor newVs
description New Sensor
signature-definition newSig
event-action-rules rules0
anomaly-detection
anomaly-detection-name ad0
exit
physical-interfaces GigabitEthernet0/1
exit
exit
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Disabled
risk-rating-range 90-100
exit
exit

[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.
```

ステップ 22　設定を保存するには、**2** と入力します。

```
Enter your selection[2]: 2
Configuration Saved.
```

ステップ 23　AIP SSM をリブートします。

```
aip-ssm# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? []:
```

ステップ 24　リブートを続行するには、**yes** と入力します。

ステップ 25　最新のサービス パックおよびシグニチャ アップデートを適用します。これで AIP SSM の侵入防御設定を行う準備ができました。

詳細情報

最新のサービス パックおよびシグニチャ アップデートの取得手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。

IDSM2 の高度なセットアップ

続けて IDSM2 の高度なセットアップを行うには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して IDSM2 のセッションを開始します。

- Catalyst ソフトウェア

  ```
  console> enable
  console> (enable) session module_number
  ```

- Cisco IOS ソフトウェア

  ```
  router# session slot slot_number processor 1
  ```

ステップ 2　**setup** コマンドを入力します。System Configuration Dialog が表示されます。

ステップ 3　高度なセットアップにアクセスするには、**3** と入力します。

ステップ 4　Telnet サーバのステータスを指定します。Telnet サービスをディセーブルまたはイネーブルにできます。デフォルトはディセーブルです。

ステップ 5　Web サーバ ポートを指定します。Web サーバ ポートは Web サーバが使用する TCP ポートです（1 ～ 65535）。デフォルトは 443 です。

（注）　デフォルトでは、Web サーバは TLS および SSL の暗号化を使用するように設定されています。ポートを 80 に設定しても、暗号化はディセーブルになりません。

ステップ 6　**yes** と入力して、インターフェイスと仮想センサーの設定を修正します。

```
Current interface configuration
 Command control: GigabitEthernet0/2
 Unassigned:
  Promiscuous:
   GigabitEthernet0/7
   GigabitEthernet0/8

 Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

ステップ 7　インターフェイス設定を編集するには、**1** と入力します。

（注）　次のオプションを使用して、インターフェイスを作成および削除できます。インターフェイスを仮想センサーの設定に含まれる仮想センサーに割り当てます。インターフェイスに無差別モードを使用していて、インターフェイスを VLAN で分割していない場合、追加の設定は必要ありません。

（注）　IDSM2 は、Add/Modify Inline Interface Pair Vlan Groups オプションをサポートしていません。インライン インターフェイス ペアを実行する場合、2 つの IDSM2 データ ポートが、ネイティブ VLAN だけを伝送するアクセス ポートまたはトランク ポートとして設定されます。パケットには 802.1q ヘッダーがなく、VLAN で分割できません。複数の VLAN をインラインでモニタするには、インライン VLAN ペアを使用してください。

```
  [1] Remove interface configurations.
  [2] Add/Modify Inline Vlan Pairs.
  [3] Add/Modify Promiscuous Vlan Groups.
  [4] Add/Modify Inline Interface Pairs.
  [5] Modify interface default-vlan.
Option:
```

ステップ 8　無差別 VLAN グループを追加するには、**3** と入力します。

```
Available Interfaces
  [1] GigabitEthernet0/7
  [2] GigabitEthernet0/8
Option:
```

ステップ 9　VLAN グループを GigabitEthernet0/8 に追加するには、**2** と入力します。

```
Promiscuous Vlan Groups for GigabitEthernet0/8
   None
Subinterface Number:
```

a. サブインターフェイス 10 を追加するには、**10** と入力します。

```
Subinterface Number: 10
Description[Created via setup by user asmith]:
Select vlans:
  [1] All unassigned vlans.
  [2] Enter vlans range.
Option:
```

b. 未割り当ての VLAN すべてをサブインターフェイス 10 に割り当てるには、**1** と入力します。

```
Subinterface Number:
```

c. サブインターフェイス 9 を追加するには、**9** と入力します。

```
Subinterface Number: 9
Description[Created via setup by user asmith]:
Vlans[]:
```

d. VLAN 1-100 をサブインターフェイス 9 に割り当てるには、**1-100** と入力します。

（注） この操作により、サブインターフェイス 10 に含まれている未割り当て VLAN から VLAN 1-100 が削除されます。

e. すべての VLAN グループを追加し終わるまで、ステップ c と d を繰り返します。

f. 空白の subinterface 行で Enter キーを押して、VLAN グループに使用できるインターフェイスのリストに戻ります。

```
  [1] GigabitEthernet0/7
  [2] GigabitEthernet0/8
Option:
```

ステップ 10　Enter キーを押して、最上位レベルのインターフェイス設定メニューに戻ります。

```
  [1] Remove interface configurations.
  [2] Add/Modify Inline Vlan Pairs.
  [3] Add/Modify Promiscuous Vlan Groups.
  [4] Add/Modify Inline Interface Pairs.
  [5] Modify interface default-vlan.
Option:
```

ステップ 11　Enter キーを押して、最上位レベルのメニューに戻ります。

```
  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

ステップ 12　仮想センサーの設定を編集するには、**2** と入力します。

```
  [1] Remove vs
  [2] Modify "vs0"
  [3] Create new vs
Option:
```

ステップ 13　仮想センサー vs0 の設定を修正するには、**2** と入力します。

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

No Interfaces to remove.

Unassigned:
  Promiscuous:
   [1] GigabitEthernet0/7
```

ステップ 14　VLAN グループ GigabitEthernet0/8:10 を仮想センサー vs0 に追加するには、**2** と入力します。

```
Promiscuous Vlan Groups:
   [2] GigabitEthernet0/8:10  (Vlans: unassigned)
   [3] GigabitEthernet0/8:9  (Vlans: 1-100)
Add Interface:
```

ステップ 15　Enter キーを押して、最上位レベルの仮想センサー設定メニューに戻ります。

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0
  Promiscuous Vlan Groups:
   GigabitEthernet0/8:10  (Vlans: unassigned)
   GigabitEthernet0/8:9  (Vlans: 1-100)

  [1] Remove vs
  [2] Modify "vs0"
  [3] Create new vs
Option:
```

ステップ 16　Enter キーを押して、最上位レベルのインターフェイスおよび仮想センサー設定メニューに戻ります。

```
  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

ステップ 17　Enter キーを押して、インターフェイスおよび仮想センサー設定メニューを終了します。

ステップ 18　デフォルトの脅威防御設定を修正する場合は、**yes** と入力します。

（注）　センサーには、パケットの拒否イベント アクションを高リスク評価のアラートに追加するためのオーバーライドが組み込まれています。この保護が不要な場合は、自動脅威防御をディセーブルにします。

```
Virtual sensor vs0 is configured to prevent high risk threats in inline mode.(Risk Rating
90-100)
Do you want to disable automatic threat prevention on all virtual sensors?[no]:
```

ステップ 19　すべての仮想センサーで自動脅威防御をディセーブルにするには、**yes** と入力します。

```
The following configuration was entered.
service host
network-settings
host-ip 10.1.9.201/24,10.1.9.1
host-name idsm-2
telnet-option disabled
ftp-timeout 300
no login-banner-text
exit
```

```
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service web-server
port 342
exit
service interface
physical-interfaces GigabitEthernet0/8
admin-state enabled
subinterface-type vlan-group
subinterface 9
description Created via setup by user asmith
vlans range 1-100
exit
subinterface 10
description Created via setup by user asmith
vlans unassigned
exit
exit
exit
exit
service analysis-engine
virtual-sensor vs0
description Created via setup by user cisco
signature-definition sig0
event-action-rules rules0
anomaly-detection
anomaly-detection-name ad0
operational-mode inactive
exit
physical-interface GigabitEthernet0/8 subinterface-number 9
physical-interface GigabitEthernet0/8 subinterface-number 10
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Disabled
risk-rating-range 90-100
exit

[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.
```

ステップ 20　設定を保存するには、**2** と入力します。

```
Enter your selection[2]: 2
Configuration Saved.
```

ステップ 21　IDSM2 をリブートします。

```
idsm-2# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? []:
```

ステップ 22　リブートを続行するには、**yes** と入力します。

ステップ 23　最新のサービス パックおよびシグニチャ アップデートを適用します。これで、IDSM2 に侵入防御を設定する準備ができました。

詳細情報

最新のサービス パックおよびシグニチャ アップデートの取得手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。

IPS SSP の高度なセットアップ

注意　IPS SSP のコンソールおよび管理ポートは、IPS ソフトウェアによって設定および制御されます。また、ASA 5585-X GigabitEthernet および 10 GE ポートは、ASA ソフトウェアによって設定、制御および管理されます。ただし、IPS SSP をシャット ダウンまたはリセットした場合、ASA 5585-X ポートもリンク ダウンします。

続けて IPS SSP の高度なセットアップを行うには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して IPS SSP のセッションを開始します。

```
asa# session 1
Opening command session with slot 1.
Connected to slot 1.Escape character sequence is 'CTRL-^X'.


login: cisco
Password:
Last login: Fri Jan 14 04:14:54 from 10.77.25.187
***NOTICE***
This product contains cryptographic features and is subject to United States
and local country laws governing import, export, transfer and use.Delivery
of Cisco cryptographic products does not imply third-party authority to import,
export, distribute or use encryption.Importers, exporters, distributors and
users are responsible for compliance with U.S.and local country laws.By using
this product you agree to comply with applicable laws and regulations.If you
are unable to comply with U.S.and local laws, return this product immediately.

A summary of U.S.laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.
asa#
```

ステップ 2　**setup** コマンドを入力します。System Configuration Dialog が表示されます。

ステップ 3　高度なセットアップにアクセスするには、**3** と入力します。

ステップ 4　Telnet サーバのステータスを指定します。Telnet サービスをディセーブルまたはイネーブルにできます。デフォルトはディセーブルです。

ステップ 5　Web サーバ ポートを指定します。Web サーバ ポートは Web サーバが使用する TCP ポートです（1 ～ 65535）。デフォルトは 443 です。

（注）　デフォルトでは、Web サーバは TLS および SSL の暗号化を使用するように設定されています。ポートを 80 に設定しても、暗号化はディセーブルになりません。

ステップ 6　**yes** と入力して、インターフェイスと仮想センサーの設定を修正します。

```
Current interface configuration
```

```
 Command control: Management0/0
 Unassigned:
  Monitored:
   PortChannel 0/0

 Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

ステップ 7　インターフェイス設定を編集するには、**1** と入力します。

（注）　IPS SSP にはインターフェイスを設定する必要はありません。Modify interface default-vlan 設定は無視する必要があります。仮想センサー間でトラフィックを分離する場合は、他のセンサーとは別に IPS SSP を設定します。

```
  [1] Modify interface default-vlan.
Option:
```

ステップ 8　Enter キーを押して、最上位レベルのインターフェイスおよび仮想センサー設定メニューに戻ります。

```
  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

ステップ 9　仮想センサーの設定を編集するには、**2** と入力します。

```
  [1] Remove virtual sensor.
  [2] Modify "vs0" virtual sensor configuration.
  [3] Create new virtual sensor.
Option:
```

ステップ 10　仮想センサー vs0 の設定を修正するには、**2** と入力します。

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

No Interfaces to remove.

 Unassigned:
  Monitored:
   [1] PortChannel 0/0
Add Interface:
```

ステップ 11　PortChannel0/0 を仮想センサー vs0 に追加するには、**1** と入力します。

（注）　複数の仮想センサーがサポートされています。適応型セキュリティ アプライアンスでは、パケットを特定の仮想センサーのモニタリング対象にすることも、デフォルトの仮想センサーのモニタリング対象とすることもできます。デフォルトの仮想センサーは、PortChannel0/0 が割り当てられている仮想センサーです。PortChannel0/0 は vs0 に割り当てることを推奨しますが、必要ならば別の仮想センサーに割り当ててもかまいません。

ステップ 12　Enter キーを押して、メインの仮想センサー メニューに戻ります。

ステップ 13　仮想センサーを作成するには、**3** と入力します。

```
Name[]:
```

ステップ 14　（任意）仮想センサーの名前と説明を入力します。

（注）　ステップ 14 ～ 18 は任意です。複数の仮想センサーを使用する場合にだけ必要です。

```
Name[]: newVs
Description[Created via setup by user cisco]: New Sensor
Anomaly Detection Configuration
  [1] ad0
  [2] Create a new anomaly detection configuration
Option[2]:
```

ステップ 15　（任意）既存の異常検出の設定 ad0 を使用するには、**1** と入力します。

```
Signature Definition Configuration
  [1] sig0
  [2] Create a new signature definition configuration
Option[2]:
```

ステップ 16　（任意）シグニチャ定義のコンフィギュレーション ファイルを作成するには、**2** と入力します。

ステップ 17　（任意）シグニチャ定義の設定名 **newSig** を入力します。

```
Event Action Rules Configuration
  [1] rules0
  [2] Create a new event action rules configuration
Option[2]:
```

ステップ 18　（任意）既存のイベント アクション規則の設定 rules0 を使用するには、**1** と入力します。

（注）　PortChannel0/0 が vs0 に割り当てられていない場合、新しい仮想センサーに割り当てるようにプロンプトが表示されます。

```
Virtual Sensor: newVs
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: newSig
  Monitored:
   PortChannel0/0

  [1] Remove virtual sensor.
  [2] Modify "newVs" virtual sensor configuration.
  [3] Modify "vs0" virtual sensor configuration.
  [4] Create new virtual sensor.
Option:
```

ステップ 19　Enter キーを押して、インターフェイスおよび仮想センサー設定メニューを終了します。

```
Modify default threat prevention settings?[no]:
```

ステップ 20　デフォルトの脅威防御設定を修正する場合は、**yes** と入力します。

（注）　センサーには、パケットの拒否イベント アクションを高リスク評価のアラートに追加するためのオーバーライドが組み込まれています。この保護が不要な場合は、自動脅威防御をディセーブルにします。

```
Virtual sensor newVs is configured to prevent high risk threats in inline mode. (Risk
Rating 90-100)
Virtual sensor vs0 is configured to prevent high risk threats in inline mode.(Risk Rating
90-100)
Do you want to disable automatic threat prevention on all virtual sensors?[no]:
```

ステップ 21　すべての仮想センサーで自動脅威防御をディセーブルにするには、**yes** と入力します。

```
The following configuration was entered.

service host
network-settings
host-ip 10.1.9.201/24,10.1.9.1
host-name ips-ssp
telnet-option disabled
access-list 10.0.0.0/8
access-list 64.0.0.0/8
ftp-timeout 300
no login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service web-server
port 342
exit
service analysis-engine
virtual-sensor newVs
description New Sensor
signature-definition newSig
event-action-rules rules0
anomaly-detection
anomaly-detection-name ad0
exit
physical-interfaces PortChannel0/0
exit
exit
service event-action-rules rules0
overrides deny-packet-inline
override-item-status Disabled
risk-rating-range 90-100
exit
exit

[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.
```

ステップ 22　設定を保存するには、**2** と入力します。

```
Enter your selection[2]: 2
Configuration Saved.
```

ステップ 23　IPS SSP をリブートします。

```
ips-ssp# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? []:
```

ステップ 24　リブートを続行するには、**yes** と入力します。

ステップ 25　リブート後、IPS SSP にログインし、自己署名 X.509 証明書を表示します（TLS で必要です）。

```
ips-ssp# show tls fingerprint
MD5: C4:BC:F2:92:C2:E2:4D:EB:92:0F:E4:86:53:6A:C6:01
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
```

ステップ 26　証明書のフィンガープリントを書き留めます。フィンガープリントは、HTTPS を使用して Web ブラウザでこの IPS SSP に接続した際に証明書の信頼性を確認するために必要になります。

ステップ 27　最新のサービス パックおよびシグニチャ アップデートを適用します。これで IPS SSP の侵入防御設定を行う準備ができました。

詳細情報

最新のサービス パックおよびシグニチャ アップデートの取得手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。

NME IPS の高度なセットアップ

続けて NME IPS の高度なセットアップを行うには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して NME IPS のセッションを開始します。

```
router# service-module ids-sensor 1/0 session
Trying 10.1.9.1, 2322 ... Open


sensor login: cisco
Password: ********
```

ステップ 2　**setup** コマンドを入力します。System Configuration Dialog が表示されます。

ステップ 3　高度なセットアップにアクセスするには、**3** と入力します。

ステップ 4　Telnet サーバのステータスを指定します。Telnet サービスをディセーブルまたはイネーブルにできます。デフォルトはディセーブルです。

ステップ 5　Web サーバ ポートを指定します。

Web サーバ ポートは Web サーバが使用する TCP ポートです（1 ～ 65535）。デフォルトは 443 です。

（注）　デフォルトでは、Web サーバは TLS および SSL の暗号化を使用するように設定されています。ポートを 80 に設定しても、暗号化はディセーブルになりません。

ステップ 6　**yes** と入力して、インターフェイスと仮想センサーの設定を修正します。分析エンジンが初期化中で、現在仮想センサーの設定を修正できないという警告が表示される場合があります。Space キーを押して、次のメニューを表示します。

```
[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
```

```
[2] Save this configuration and exit setup.

Enter your selection[2]:
```

分析エンジンが初期化中という警告が表示された場合は、**2** と入力してここまでの設定を保存し、セットアップを終了します。その後、セットアップを再開し、インターフェイスおよび仮想センサー設定メニューに戻るまで Enter キーを押します。

ステップ 7　仮想センサーの設定を修正するには、**2** と入力します。

```
Modify interface/virtual sensor configuration?[no]: yes
Current interface configuration
 Command control: Management0/1
 Unassigned:
  Monitored:
   GigabitEthernet0/1

 Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

ステップ 8　仮想センサー vs0 の設定を編集するには、**2** と入力します。

```
Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0

No Interfaces to remove.

Unassigned:
  Monitored:
   [1] GigabitEthernet0/1
Add Interface:
```

ステップ 9　仮想センサー vs0 に GigabitEthernet0/1 を追加するには、**1** と入力します。

```
Add Interface: 1

 Virtual Sensor: vs0
  Anomaly Detection: ad0
  Event Action Rules: rules0
  Signature Definitions: sig0
  Monitored:
   GigabitEthernet0/1

  [1] Edit Interface Configuration
  [2] Edit Virtual Sensor Configuration
  [3] Display configuration
Option:
```

ステップ 10　Enter キーを押して、インターフェイスおよび仮想センサー設定メニューを終了します。

```
Modify default threat prevention settings?[no]:
```

ステップ 11　デフォルトの脅威防御設定を修正する場合は、**yes** と入力します。

（注）　センサーには、パケットの拒否イベント アクションを高リスク評価のアラートに追加するためのオーバーライドが組み込まれています。この保護が不要な場合は、自動脅威防御をディセーブルにします。

```
Virtual sensor vs0 is configured to prevent high risk threats in inline mode.(Risk Rating
90-100)
Do you want to disable automatic threat prevention on all virtual sensors?[no]:
```

ステップ 12　すべての仮想センサーで自動脅威防御をディセーブルにするには、**yes** と入力します。または、Enter キーを押してデフォルトの no を受け入れます。

```
The following configuration was entered.

service host
network-settings
host-ip 192.168.1.2/24,192.168.1.1
host-name nme-ips
telnet-option enabled
access-list 10.0.0.0/8
access-list 64.0.0.0/8
ftp-timeout 300
no login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service web-server
port 443
exit
service analysis-engine
virtual-sensor vs0
physical-interface GigabitEthernet0/1
exit
exit
service event-action-rules rules0
overrides
override-item-status Enabled
risk-rating-range 90-100
exit
exit

[0] Go to the command prompt without saving this config.
[1] Return to Advanced setup without saving this config.
[2] Save this configuration and exit setup.
```

ステップ 13　設定を保存するには、**2** と入力します。

```
Enter your selection[2]: 2
Configuration Saved.
```

ステップ 14　NME IPS をリブートします。

```
nme-ips# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? []:
```

ステップ 15　リブートを続行するには、**yes** と入力します。

ステップ 16　最新のサービス パックおよびシグニチャ アップデートを適用します。これで、NME IPS に侵入防御を設定する準備ができました。

詳細情報

最新のサービス パックおよびシグニチャ アップデートの取得手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。

初期化の確認

（注）　AIP SSC-5 は、グローバル相関機能をサポートしていません。

センサーが初期化されていることを確認するには、次の手順を実行します。

ステップ 1　センサーにログインします。

ステップ 2　設定を表示します。

```
sensor# show configuration
! ------------------------------
! Current configuration last modified Mon Nov 09 12:03:44 2009
! ------------------------------
! ! Version 7.1(1)E4
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S369.0   2009-09-29
! ------------------------------
service interface
exit
! ------------------------------
service authentication
password-strength
size 6
exit
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 172.23.204.84/24,172.23.204.1
host-name sensor
telnet-option enabled
access-list 0.0.0.0/0
dns-primary-server enabled
address 1.1.1.1
exit
dns-secondary-server enabled
address 2.2.2.2
exit
http-proxy proxy-server
address 1.1.1.1
port 1
exit
```

```
exit
time-zone-settings
offset -480
standard-time-zone-name PST
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
signatures 1000 0
status
retired med-mem-retired
exit
exit
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
!------------------------------
service global-correlation
exit
! ------------------------------
service analysis-engine
exit
sensor#
```

（注） また、**more current-config** コマンドを使用して設定を表示することもできます。

ステップ 3　自己署名 X.509 証明書を表示します（TLS で必要です）。

```
sensor# show tls fingerprint
MD5: C4:BC:F2:92:C2:E2:4D:EB:92:0F:E4:86:53:6A:C6:01
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
```

ステップ 4　証明書のフィンガープリントを書き留めます。フィンガープリントは、Web ブラウザでこのセンサーに接続した際に証明書の信頼性を確認するために必要になります。

詳細情報

センサーにログインする手順については、第 22 章「センサーへのログイン」を参照してください。

CHAPTER 24

Cisco IPS ソフトウェアについて

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

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

この章では、Cisco IPS ソフトウェアとその入手およびインストール方法について説明します。内容は次のとおりです。

注意 Cisco IPS センサーの BIOS は Cisco IPS センサーに固有のものです。シスコ Web サイトから入手できる BIOS ファイルを使用し、シスコの手順に基づいてアップグレードする必要があります。シスコ以外またはサードパーティの BIOS を Cisco IPS センサーにインストールする場合は、保証の対象外となります。

IPS 7.1(1)E4 のファイル リスト

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

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

次のファイルは Cisco IPS 7.1(1)E4 の一部です。

- Readme
  - IPS-7-1-1-E4.readme.txt
- システム イメージ ファイル
  - IPS-SSP_10-K9-sys-1.1-a-7.1-1-E4.img
  - IPS-SSP_20-K9-sys-1.1-a-7.1-1-E4.img
  - IPS-SSP_40-K9-sys-1.1-a-7.1-1-E4.img
  - IPS-SSP_60-K9-sys-1.1-a-7.1-1-E4.img
- リカバリ イメージ ファイル
  - IPS-SSP_10-K9-r-1.1-a-7.1-1-E4.pkg
  - IPS-SSP_20-K9-r-1.1-a-7.1-1-E4.pkg
  - IPS-SSP_40-K9-r-1.1-a-7.1-1-E4.pkg
  - IPS-SSP_60-K9-r-1.1-a-7.1-1-E4.pkg

Cisco IPS ソフトウェアの入手方法

メジャー アップデート、マイナー アップデート、サービス パック、シグニチャ アップデート、シグニチャ エンジン アップデート、システム ファイル、リカバリ ファイル、ファームウェア アップグレード、および Readme は、Cisco.com のソフトウェア ダウンロード サイトにあります。シグニチャ アップデートは、約 1 週間ごとに Cisco.com に掲示されますが、必要な場合は、さらに頻繁にアップデートされます。サービス パックは必要に応じて Cisco.com に掲示されます。メジャー アップデートおよびマイナー アップデートも定期的に掲示されます。最新の IPS ソフトウェアがないかどうか、定期的に Cisco.com を確認してください。

ソフトウェアをダウンロードするには、暗号化アクセス用のアカウントが必要です。このアカウントは、ソフトウェア ダウンロード サイトから IPS ソフトウェアを初めてダウンロードする際にセットアップします。また、IPS Alert Bulletins にサインアップしてソフトウェア リリースの最新情報を入手することができます

（注） ソフトウェアをダウンロードするには、Cisco.com にログインする必要があります。ダウンロードには、有効な IPS メンテナンス契約と Cisco.com のパスワードが必要です。シグニチャ アップデートを適用するにはセンサー ライセンスが必要です。

IPS ソフトウェアのダウンロード

Cisco.com のソフトウェアをダウンロードするには、次の手順を実行します。

ステップ 1　Cisco.com にログインします。

ステップ 2　[Support] ドロップダウン メニューから、[Download Software] を選択します。

ステップ 3　[Select a Software Product Category] で、[Security Software] を選択します。

ステップ 4　[Intrusion Prevention System (IPS)] を選択します。

ステップ 5　ユーザ名とパスワードを入力します。

ステップ 6　[Download Software] ウィンドウで、[IPS Appliances] > [Cisco Intrusion Prevention System] を選択し、ダウンロードするバージョンをクリックします。

（注）　ソフトウェアをダウンロードするには、IPS 登録サービス ライセンスが必要です。

ステップ 7　必要なソフトウェア ファイルのタイプをクリックします。利用可能なファイルがウィンドウの右側のリストに表示されます。これは、ファイル名、ファイル サイズ、メモリ、およびリリース日でソートすることができます。リリース ノートやその他の製品マニュアルにアクセスすることもできます。

ステップ 8　ダウンロードするファイルをクリックします。ファイルの詳細が表示されます。

ステップ 9　ファイルが正しいことを確認し、[Download] をクリックします。

ステップ 10　[Agree] をクリックして、ソフトウェア ダウンロード規約に同意します。Cisco.com から初めてファイルをダウンロードする場合は、先に [Encryption Software Export Distribution Authorization] フォームに必要事項を入力する必要があります。

- フォームに入力し、[Submit] をクリックします。

  Cisco Systems Inc., Encryption Software Usage Handling and Distribution Policy が表示されます。
- ポリシーを読み、[I Accept] をクリックします。

  [Encryption Software Export/Distribution] フォームが表示されます。

すでに [Encryption Software Export Distribution Authorization] フォームに記入し、Cisco Systems Inc., Encryption Software Usage Handling and Distribution Policy を読んで承諾した場合、これらのフォームは表示されません。[File Download] ダイアログボックスが表示されます。

ステップ 11　ファイルを開くか、コンピュータに保存します。

ステップ 12　Readme に記載されている説明に従ってアップデートをインストールします。

（注）　メジャー アップデート、マイナー アップデート、サービス パック、リカバリ ファイル、シグニチャ アップデート、シグニチャ エンジン アップデートは、すべてのセンサーで同一です。システム イメージ ファイルは、プラットフォームごとに用意されます。

詳細情報

- IPS メンテナンス契約の詳細については、「IPS 製品のサービス プログラム」（P.18-12）を参照してください。
- センサー ライセンスの詳細については、「ライセンスの設定」（P.18-10）を参照してください。

IPS ソフトウェアのバージョン管理

Cisco.com から IPS ソフトウェア イメージをダウンロードするときは、そのバージョン管理方式を理解して、ファイルがそれぞれ、ベース ファイル、累積ファイル、あるいは差分ファイルのどれであるかを知っておく必要があります。

（注）　センサーにインストールされているソフトウェアのバージョンは、IME の [Device List] ペインにある [Sensor Information] タブに一覧表示されます。

メジャー アップデート

メジャー アップデートには、製品の新しい機能やアーキテクチャの変更などが含まれます。たとえば、Cisco IPS 7.0 ベース バージョンでは、前回のメジャー リリース以降の内容（マイナー アップデートの機能、サービス パックのフィックス、およびシグニチャ アップデート）すべて（廃止予定の機能は除く）に加えて、新しい変更が組み込まれます。メジャー アップデート 7.0(1) には、5.1(6) 以降が必要です。各メジャー アップデートには、対応するシステム パッケージおよびリカバリ パッケージがあります。

（注）　7.0(1) メジャー アップデートは、5.1(6) 以降のセンサーを 7.0(1) にアップグレードする場合に使用します。7.0(1) がすでにインストールされているセンサーに 7.0(1) を再インストールする場合は、メジャー アップデートではなくシステム イメージまたはリカバリ手順を使用します。

マイナー アップデート

マイナー アップデートは、メジャー バージョンに対する差分です。マイナー アップデートは、サービス パックのベース バージョンでもあります。7.0 の最初のマイナー アップデートは、7.1(1) です。マイナー アップデートは、製品のマイナーな拡張を行うためにリリースされます。マイナー アップデートには、前回のメジャー バージョン以降に発生したすべてのマイナー機能（廃止予定の機能は除く）、サービス パックのフィックス、およびシグニチャ アップデートに加えて、新しいマイナー機能のリリースが組み込まれます。マイナー アップデートを前回のメジャー バージョンまたはマイナー バージョンにインストールすることができます（通常、それよりも前のバージョンにもインストールすることができます）。最新のマイナー バージョンにアップグレードするために最低限必要なバージョンは、マイナー アップデートに付属している Readme に記載されています。各マイナー アップデートには、対応するシステム パッケージおよびリカバリ パッケージがあります。

サービス パック

サービス パックは、ベース バージョンのリリース（マイナーまたはメジャー）の後で、複数のプログラムが累積した形で提供されるものです。サービス パックは、障害フィックスのリリースとして使用され、新しい機能強化は行われません。サービス パックには、前回のベース バージョン（マイナーまたはメジャー）以降に発生したすべてのサービス パックのフィックスに加えて、新しい障害フィックスのリリースが組み込まれます。サービス パックを適用するには、マイナー バージョンが必要です。最新のサービス パックにアップグレードするために最低限必要なバージョンは、サービス パックに付属している Readme に記載されています。サービス パックには、最新のエンジン アップデートも含まれています。たとえば、サービス パック 7.1(3) がリリースされるときに、最新のエンジン レベルが E4 の場合、サービス パックは 7.1(3)E4 としてリリースされます。

パッチ リリース

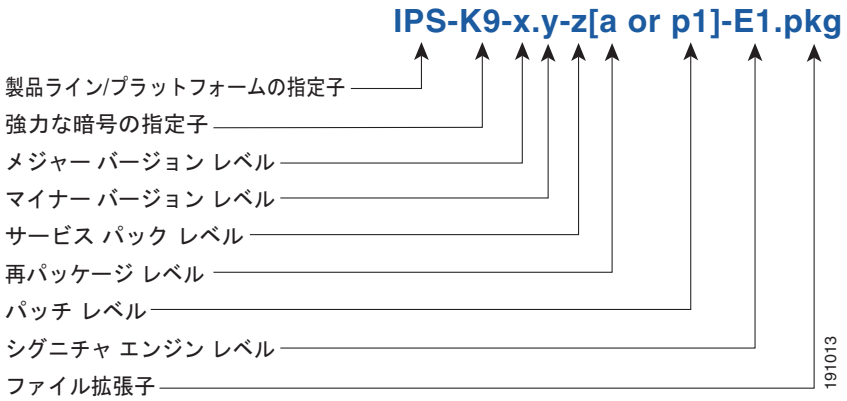
パッチ リリースは、ソフトウェアのリリース後にアップグレード バイナリで見つかった不具合をフィックスするために使用されます。次のメジャー アップデート、マイナー アップデート、またはサービス パックでこれらの不具合がフィックスされるまでの間に、パッチが公開されます。パッチには、関連するサービス パック レベルにある以前のパッチ リリースがすべて含まれます。各パッチは、次の公式のメジャー アップデート、マイナー アップデート、またはサービス パックで集約されます。

パッチ リリースをインストールする前に、最新のメジャー アップデート、マイナー アップデート、またはサービス パックをインストールしておく必要があります。たとえば、パッチ リリース 7.1(1p1) には、7.1(1) が必要です。

（注）　新しいパッチへのアップグレード時に、古いパッチをアンインストールする必要はありません。たとえば、7.1(1p1) を 7.1(1p2) にアップグレードする前に、7.1(1p1) をアンインストールする必要はありません。

図 24-1 は、メジャー アップデート、マイナー アップデート、サービス パック、およびパッチ リリースで、IPS ソフトウェアのファイル名の各部分が何を表すかを示しています。

図 24-1　メジャー アップデート、マイナー アップデート、サービス パックおよびパッチ リリース用の IPS ソフトウェアのファイル名

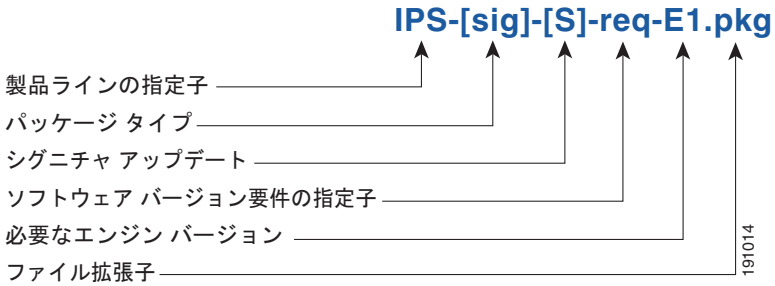


シグニチャ アップデート

シグニチャ アップデートは、悪意のあるネットワーク アクティビティを認識するように設計されたルール セットが含まれているパッケージ ファイルです。シグニチャ アップデートは、他のソフトウェア アップデートとは別個にリリースされます。メジャー アップデートまたはマイナー アップデートがリリースされるたびに、少なくとも 6 ヵ月間はシグニチャ アップデートを新しいバージョンおよび次に古いバージョンにインストールできます。シグニチャ アップデートは、必要なシグニチャ エンジンのバージョンによって決まります。このため、*req* 指示子で、特定のシグニチャ アップデートのサポートに必要なシグニチャ エンジンが示されています。

図 24-2 は、シグニチャ アップデートで、IPS ソフトウェアのファイル名の各部分が何を表すかを示しています。

図 24-2　シグニチャ アップデート用の IPS ソフトウェアのファイル名

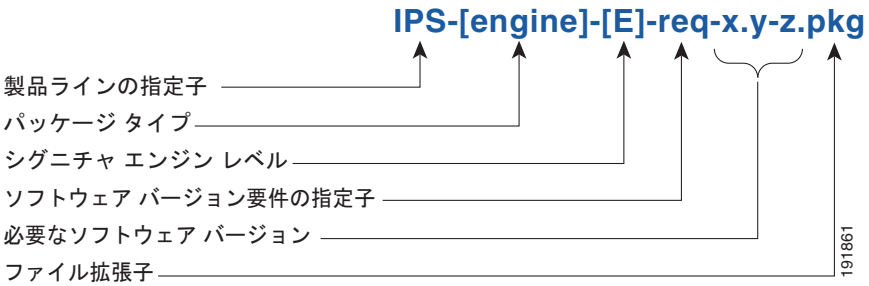


シグニチャ エンジンのアップデート

シグニチャ エンジンのアップデートは、新しいシグニチャ アップデートをサポートするためのバイナリ コードが含まれている実行可能ファイルです。シグニチャ エンジン ファイルには、特定のサービス パックが必要です。これは *req* 指示子でも識別できます。

図 24-3 は、シグニチャ エンジン アップデートで、IPS ソフトウェアのファイル名の各部分が何を表すかを示しています。

図 24-3　シグニチャ エンジン アップデート用の IPS ソフトウェアのファイル名



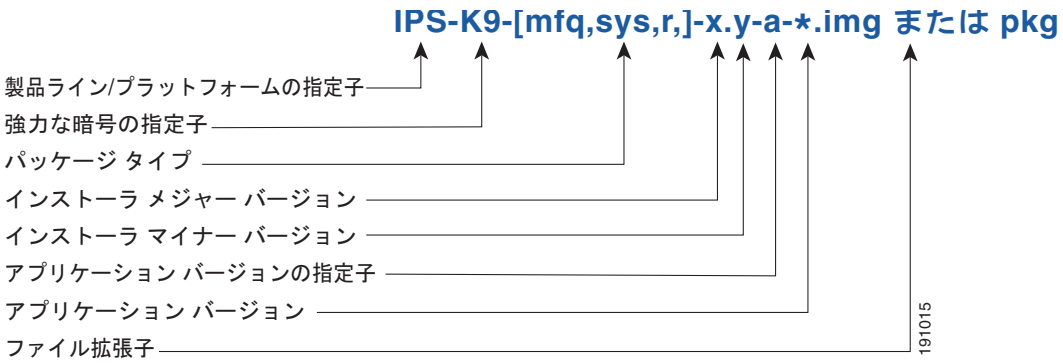
リカバリ イメージ ファイルおよびシステム イメージ ファイル

リカバリ イメージ ファイルおよびシステム イメージ ファイルには、インストーラのバージョンと基盤アプリケーションのバージョンが個別に含まれています。インストーラのバージョンには、メジャー バージョンのフィールドとマイナー バージョンのフィールドがあります。メジャー バージョンは、イメージ インストーラに大きな変更があるたびに増加されます。たとえば、.tar から .rpm への切り替えや、カーネルの変更などが挙げられます。マイナー バージョンは次のいずれかの場合に増加します。

- ユーザ プロンプトの追加など、インストーラに小さな変更があった場合。
- インストーラの不具合や問題をフィックスするためにイメージ ファイルを再パッケージングする必要がある場合。この場合、パッケージでは、インストーラのマイナー バージョンを 1 つ増加させる必要があります。

図 24-4 は、リカバリ イメージ ファイルおよびシステム イメージ ファイルで、IPS ソフトウェアのファイル名の各部分が何を表すかを示しています。

図 24-4　リカバリ イメージ ファイルおよびシステム イメージ ファイルに対応する IPS ソフトウェアのファイル名



ソフトウェア リリースの例

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

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

表 24-1 に、プラットフォームに依存しない Cisco IPS 7.*x* ソフトウェア リリースの例を示します。

表 24-1　プラットフォームに依存しないリリースの例

リリース	目標頻度	識別子	バージョンの例	ファイル名の例
シグニチャ アップデート[1]	週に 1 回	sig	S369	IPS-sig-S369-req-E4.pkg
シグニチャ エンジンのアップデート[2]	必要に応じて	engine	E4	IPS-engine-E4-req-7.1-1.pkg
サービス パック[3]	半年ごと または必要に応じて	—	7.1(3)	IPS-K9-7.1-3-E4.pkg
マイナー バージョン アップデート[4]	年に 1 回	—	7.2(1)	IPS-K9-7.2-1-E4.pkg （注）　IPS-AIM-K9-7.2-1-E4.pkg は、AIM-IPS のマイナー バージョン アップデートです。IPS-NME-K-9-7.2-1-E4.pkg は、NME-IPS のマイナー バージョン アップデートです。
メジャー バージョン アップデート[5]	年に 1 回	—	8.0(1)	IPS-K9-8.0-1-E4.pkg
パッチ リリース[6]	必要に応じて	patch	7.1(1p1)	IPS-K9-patch-7.1-1pl-E4.pkg
リカバリ パッケージ[7]	年に 1 回または必要に応じて	r	1.1-7.1(1)	IPS-K9-r-1.1-a-7.1-1-E4.pkg

1. シグニチャ アップデートには、最新の累積 IPS シグニチャが含まれます。
2. シグニチャ エンジンのアップデートは、最新のシグニチャ アップデートの新しいシグニチャによって使用される新しいエンジンやエンジンのパラメータを追加します。
3. サービス パックには、障害のフィックスが含まれます。
4. マイナー バージョンには、マイナー バージョンの新しい特性や機能が含まれます。
5. メジャー バージョンには、メジャー バージョンの新しい機能やアーキテクチャが含まれます。
6. パッチ リリースは暫定的なフィックスです。
7. 同じ基盤アプリケーション イメージを含む新しいリカバリ パッケージをリリースする必要がある場合は、r 1.1 を r 1.2 に変更できます。たとえば、インストーラの障害フィックスがある場合、基盤アプリケーション バージョンがまだ 7.1(1) であっても、リカバリ パーティション イメージは r 1.2 になります。

表 24-2 に、プラットフォームに依存するソフトウェア リリースの例を示します。

表 24-2　プラットフォームに依存するリリースの例

リリース	目標頻度	識別子	サポートされているプラットフォーム	ファイル名の例
システム イメージ[1]	年に 1 回	sys	センサー プラットフォームごとに個別のファイル	IPS-SSP_10-K9-sys-1.1-a-7.1-1-E4.img
メンテナンス パーティション イメージ[2]	年に 1 回	mp	IDSM2	c6svc-mp.2-1-2.bin.gz
ブートローダ	必要に応じて	bl	AIM-IPS NME-IPS	pse_aim_x.y.z.bin pse_nm_x.y.z.bin （x、y、z はリリース番号）
ミニカーネル	必要に応じて	mini-kernel	AIM-IPS NME-IPS	pse_mini_kernel_1.1.10.64.bz2

1. システム イメージには、センサー全体のイメージの再作成に使用される、リカバリとアプリケーションを組み合わせたイメージが含まれます。
2. メンテナンス パーティション イメージには、IDSM2 メンテナンス パーティションの完全なイメージが含まれます。このファイルは、IDSM2 アプリケーション パーティションからインストールされますが、IDSM2 アプリケーション パーティションには影響はありません。

表 24-3 に、プラットフォーム固有の名前に使用するプラットフォーム識別子を示します。

表 24-3　プラットフォーム識別子

センサー ファミリ	識別子
IPS-4240 シリーズ	4240
IPS-4255 シリーズ	4255
IPS-4260 シリーズ	4260
IPS 4270-20 シリーズ	4270_20
Catalyst 6K の IDS モジュール	IDSM2
IPS ネットワーク モジュール	AIM NME
適応型セキュリティ アプライアンス モジュール	SSC_5 SSM_10 SSM_20 SSM_40

詳細情報

IPS ソフトウェア ファイルをインストールする方法の詳細については、第 25 章「システム イメージのアップグレード、ダウングレード、およびインストール」を参照してください。

IPS のマニュアルへのアクセス

次の URL には、IPS のマニュアルが用意されています。

http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/tsd_products_support_series_home.html

また、Cisco.com から IPS のマニュアルにアクセスするには、次の手順を実行します。

ステップ 1　Cisco.com にログインします。

ステップ 2　[Support] をクリックします。

ステップ 3　[Support and Documentation] で、[Security] をクリックします。

ステップ 4　[Products] > [Security] > [Intrusion Prevention System (IPS)] > [IPS Appliances] > [Cisco IPS 4200 Series Sensors] の順にクリックします。[Cisco IPS 4200 Series Sensors] ウィンドウが表示されます。

ステップ 5　次のいずれかのカテゴリをクリックし、Cisco IPS のマニュアルにアクセスします。

- [Download Software]：ソフトウェア ダウンロード サイトに移動します。

  （注）　ソフトウェア ダウンロード サイトにアクセスするには、Cisco.com にログインする必要があります。

- [Release and General Information]：マニュアルのロードマップおよびリリース ノートが表示されます。
- [Reference Guides]：コマンド リファレンスおよびテクニカル リファレンスが表示されます。
- [Design]：設計ガイドおよび設計テクニカル ノートが表示されます。
- [Install and Upgrade]：ハードウェアの設置と規制に関するガイドが表示されます。
- [Configure]：IPS CLI、IDM、および IME のコンフィギュレーション ガイドが表示されます。
- [Troubleshoot and Alerts]：TAC テクニカル ノートおよびフィールド ノーティスが表示されます。

Cisco Security Intelligence Operations

Cisco.com の Cisco Security Intelligence Operations サイトは、現在の脆弱性およびセキュリティ上の脅威に関するインテリジェンス レポートを提供します。また、組織のリスクを減らすために、ネットワークを保護し、セキュリティ システムを展開するのに役立つその他のセキュリティ項目に関するレポートも提供します。

最新のセキュリティ上の脅威を確認しておくことで、最も効果的にネットワークを保護、管理できます。Cisco Security Intelligence Operations には、日付、重大度、緊急性、および脅威に対処可能な新しいシグニチャがあるかどうかをトップ 10 形式で一覧表示するインテリジェンス レポートが含まれます。

Cisco Security Intelligence Operations には、該当するセキュリティ上の記事を一覧表示する Security News のセクションが含まれます。セキュリティ関連のツールやリンクもあります。

Cisco Security Intelligence Operations には、次の URL からアクセスできます。

http://tools.cisco.com/security/center/home.x

Cisco Security Intelligence Operations はまた、シグニチャ ID、タイプ、構造、および説明を含む、個別のシグニチャ情報のリポジトリでもあります。

セキュリティ警告およびシグニチャは、次の URL で検索できます。

http://tools.cisco.com/security/center/search.x

CHAPTER 25

システム イメージのアップグレード、ダウングレード、およびインストール

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

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

この章では、システム イメージをアップグレード、ダウングレード、およびインストールする方法について説明します。内容は次のとおりです。

アップグレード、ダウングレード、およびシステム イメージ

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

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

センサーのソフトウェアをアップグレードおよびダウングレードできます。アップグレードでは、サービス パック、シグニチャ アップデート、シグニチャ エンジン アップデート、マイナー バージョン、メジャー バージョン、またはリカバリ パーティション ファイルが適用されます。ダウングレードでは、最後に適用されたサービス パックまたはシグニチャ アップデートがセンサーから削除されます。

注意　**downgrade** コマンドを使用して、Cisco IPS 7.1 から 7.0 へなど、以前のメジャー バージョンまたはマイナー バージョンに戻すことはできません。**downgrade** コマンドでは、最新のシグニチャ アップデートまたはシグニチャ エンジン アップデートからのダウングレードのみ可能です。7.0 に戻すには、センサーのイメージを再作成する必要があります。

センサーのアプリケーション パーティション イメージが使用できなくなった場合は、復旧することができます。**recover** コマンドを使用と、ホスト設定を保持したまま他の設定を出荷時の初期状態に戻すことができます。

センサーに新しいシステム イメージをインストールするには、使用しているプラットフォームに応じて、ROMMON、ブートローダ ファイル、またはメンテナンス パーティションを使用します。

センサーに新しいシステム イメージをインストールすると、すべてのアカウントが削除され、デフォルトの cisco アカウントはデフォルトのパスワード **cisco** を使用するようにリセットされます。システム イメージをインストールした後で、センサーを再度初期化する必要があります。

センサーのイメージを再作成し、初期化を行った後で、最新のサービス パック、シグニチャ アップデート、シグニチャ エンジン アップデート、マイナー アップデート、メジャー アップデート、およびリカバリ パーティション ファイルでセンサーをアップグレードする必要があります。

詳細情報

- センサーを初期化する手順については、第 23 章「センサーの初期化」を参照してください。
- Cisco.com でソフトウェアを検索する手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。
- さまざまなセンサーのイメージを再作成手順については、「システム イメージのインストール」（P.25-13）を参照してください。

サポートされる FTP サーバおよび HTTP/HTTPS サーバ

IPS ソフトウェアのアップデートについてサポートされている FTP サーバは次のとおりです。

- WU-FTPD 2.6.2（Linux）
- Solaris 2.8
- Sambar 6.0（Windows 2000）
- Serv-U 5.0（Windows 2000）
- MS IIS 5.0（Windows 2000）

IPS ソフトウェアのアップデートについてサポートされている HTTP/HTTPS サーバは次のとおりです。

- CMS - Apache Server（Tomcat）
- CMS - Apache Server（JRun）

詳細情報

- Cisco.com から IPS ソフトウェア アップデートをダウンロードする手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。
- 自動アップデートを設定する手順については、「自動アップグレードの設定」（P.25-6）を参照してください。

センサーのアップグレード

サービス パック、シグニチャ アップデート、エンジン アップデート、マイナー バージョン、メジャー バージョン、またはリカバリ パーティション ファイルのアップグレードを適用するには、**upgrade** *source-url* コマンドを使用します。

オプション

次のオプションが適用されます。

- *source-url*：コピー元のファイルの場所。
  - ftp:：FTP ネットワーク サーバのコピー元 URL。このプレフィクスの構文は、次のとおりです。

    ftp:[//[username@] location]/relativeDirectory]/filename

    ftp:[//[username@]location]//absoluteDirectory]/filename

    （注）　パスワードを入力するように求められます。

  - scp:：SCP ネットワーク サーバのコピー元 URL。このプレフィクスの構文は、次のとおりです。

    scp:[//[username@] location]/relativeDirectory]/filename

    scp:[//[username@] location]//absoluteDirectory]/filename

    （注）　パスワードを入力するように求められます。

  - http:：Web サーバのコピー元 URL。このプレフィクスの構文は、次のとおりです。

    http:[[//username@] location]/directory] filename

    （注）　ディレクトリは、目的のファイルの絶対パスで指定する必要があります。

  - https:：Web サーバのコピー元 URL。このプレフィクスの構文は、次のとおりです。

    https:[[//username@] location]/directory] filename

    （注）　ディレクトリは、目的のファイルの絶対パスで指定する必要があります。

センサーのアップグレード

センサーをアップグレードするには、次の手順を実行します。

ステップ 1　アップグレード用のファイルをセンサーからアクセスできる FTP、SCP、HTTP、または HTTPS サーバにダウンロードします。

ステップ 2　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 3　コンフィギュレーション モードを開始します。

```
sensor# configure terminal
```

ステップ 4　センサーをアップグレードします。

```
sensor(config)# upgrade url/IPS-K9-7.0-1-E4.pkg
```

この URL は、アップデート ファイルがある場所を指します。たとえば、FTP を使用してアップデートを取得する場合は、次のように入力します。

```
sensor(config)# upgrade ftp://username@ip_address//directory/IPS-K9-7.0-1-E4.pkg
```

ステップ 5　プロンプトが表示されたら、パスワードを入力します。

```
Enter password: ********
```

ステップ 6　**yes** と入力してアップグレードを完了します。

（注）　メジャー アップデート、マイナー アップデート、およびサービス パックによって、IPS プロセスが強制的に再起動されることがあります。また、インストールを完了するためにセンサーが強制的にリブートされることもあります。

（注）　オペレーティング システムのイメージが再作成され、サービス アカウントを使用してセンサーに配置されたすべてのファイルが削除されます。

詳細情報

- サポートされる FTP サーバおよび HTTP/HTTPS サーバのリストについては、「サポートされる FTP サーバおよび HTTP/HTTPS サーバ」（P.25-2）を参照してください。
- Cisco.com でソフトウェアを検索する手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。
- AIM IPS でハートビートのリセットをディセーブルにする手順については、「Enabling and Disabling Heartbeat Reset」を参照してください。NME IPS については、「Enabling and Disabling Heartbeat Reset」を参照してください。

リカバリ パーティションのアップグレード

リカバリ パーティションを最新バージョンでアップグレードして、センサー上のアプリケーション パーティションを復旧する場合に備えておくことには、**upgrade** コマンドを使用します。

（注）　リカバリ パーティション イメージはメジャー アップデートおよびマイナー アップデートのために生成されます。サービス パックやシグニチャ アップデートのために生成されることはごくまれにしかありません。

（注）　AIM IPS および NME IPS には、IPS 7.0 のリカバリ パーティションをアップグレードするときに使用する必要のある固有のリカバリ イメージがあります。AIM IPS では、IPS-AIM-K9-r-1.1-a-7.0-1-E4.pkg を使用します。NME IPS では、IPS-NME-K9-r-1.1-a-7.0-1-E4.pkg を使用します。

リカバリ パーティションのアップグレード

センサーのリカバリ パーティションをアップグレードするには、次の手順を実行します。

ステップ 1　リカバリ パーティション イメージ ファイル（IPS-K9-r-1.1-a-7.0-1-E4.pkg など）を、センサーからアクセスできる FTP、SCP、HTTP、または HTTPS サーバにダウンロードします。

注意　ブラウザによっては、ファイル名に拡張子が付加されます。保存されたファイルのファイル名は、ダウンロード ページに表示されているファイル名と一致する必要があります。一致していなければ、そのファイルはリカバリ パーティションのアップグレードに使用できません。

ステップ 2　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 3　コンフィギュレーション モードを開始します。

```
sensor# configure terminal
```

ステップ 4　リカバリ パーティションをアップグレードします。

```
sensor(config)#
upgrade scp://user@server_ipaddress//upgrade_path/IPS-K9-r-1.1-a-7.0-1-E4.pkg

sensor(config)#
upgrade ftp://user@server_ipaddress//upgrade_path/IPS-K9-r-1.1-a-7.0-1-E4.pkg
```

ステップ 5　サーバ パスワードを入力します。アップグレード プロセスが開始されます。

（注）　この手順では、リカバリ パーティションのイメージを再作成するだけです。アプリケーション パーティションは、このアップグレードでは変更されません。リカバリ パーティションの後にアプリケーション パーティションのイメージを再作成するには、**recover application-partition** コマンドを使用します。

詳細情報

- サポートされる FTP サーバおよび HTTP/HTTPS サーバのリストについては、「サポートされる FTP サーバおよび HTTP/HTTPS サーバ」（P.25-2）を参照してください。
- Cisco.com でソフトウェアを検索する手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。

- **recover** コマンドの使用手順については、「アプリケーション パーティションの復旧」（P.25-12）を参照してください。

自動アップグレードの設定

ここでは、アップグレード ディレクトリにあるアップグレード ファイルを自動的に検索するようにセンサー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。

自動アップグレードについて

アップグレード ディレクトリにある新しいアップグレード ファイルを自動的に検索するようにセンサーを設定することができます。たとえば、複数のセンサーが、異なるアップデート スケジュール（24 時間ごと、月曜日、水曜日、および金曜日の午後 11 時など）で同じリモート FTP サーバ ディレクトリを参照できます。

自動アップグレードのスケジュールを設定するには、次の情報を指定します。

- サーバの IP アドレス
- センサーがアップグレード ファイルをチェックするファイル サーバ上のディレクトリのパス
- ファイル コピー プロトコル（SCP または FTP）
- ユーザ名とパスワード
- アップグレード スケジュール

センサーが自動アップグレード ファイルをポーリングするためには、ソフトウェア アップグレードを Cisco.com からダウンロードし、アップグレード ディレクトリにコピーしておく必要があります。

（注）　自動アップデートの設定中に不正アクセスを示すエラー メッセージが表示された場合は、センサーと Cisco.com の間のファイアウォール上で正しいポートが開いていることを確認してください。たとえば、www.cisco.com への最初の自動アップデート接続には、198.133.219.25 ポート 443 が必要であり、選択したパッケージを Cisco ファイル サーバからダウンロードするには、198.133.219.243 ポート 80 が必要です。Cisco ファイル サーバの IP アドレスは変更されることがありますが、**show statistics host** コマンドの出力の lastDownloadAttempt セクションで確認できます。

（注）　前回の自動アップデートまたは予定されている次回の自動アップデートのステータスをチェックするには、**show statistics host** コマンドを実行し、Auto Update Statistics セクションを確認します。

詳細情報

Cisco.com でソフトウェアを検索する手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。

自動アップグレードの設定

自動アップグレードを設定するには、サービス ホスト サブモードで **auto-upgrade-option enabled** コマンドを使用します。

オプション

次のオプションが適用されます。

- **cisco-server**：シグニチャおよびシグニチャ エンジンの Cisco.com からの自動アップデートをイネーブルにします。
- **cisco-url**：Cisco サーバ ロケータ サービス。**www.cisco.com の IP アドレスが変更された場合を除き、このオプションを変更する必要はありません。**
- **default**：値をシステムのデフォルト設定に戻します。
- **directory**：アップグレード ファイルが置かれているファイル サーバ上のディレクトリ。先頭の「/」は、絶対パスであることを示します。
- **file-copy-protocol**：ファイル サーバからのファイルのダウンロードに使用されるファイル コピー プロトコル。有効な値は、**ftp** または **scp** です。

  （注）　SCP を使用する場合は、センサーが SSH を介してサーバと通信できるように、**ssh host-key** コマンドを使用してサーバを SSH の既知ホスト リストに追加する必要があります。

- **ip-address**：ファイル サーバの IP アドレス。
- **password**：Cisco サーバの認証用のユーザ パスワード。
- **schedule-option**：Cisco サーバによる自動アップグレードのスケジュールを設定します。カレンダー スケジューリングでは、特定の曜日の特定の時刻にアップグレードが開始されます。定期スケジューリングでは、特定の間隔でアップグレードが開始されます。
  - **calendar-schedule**：自動アップグレードを実行する曜日と時刻を設定します。
  - **days-of-week**：自動アップグレードを実行する曜日。複数の曜日を選択できます。*sunday* から *saturday* までが有効な値です。
  - **no**：エントリまたは選択設定を削除します。
  - **times-of-day**：自動アップグレードを開始する時刻。複数の時刻を選択できます。有効な値は *hh:mm[:ss]* です。
  - **periodic-schedule**：最初の自動アップグレードを実行する時刻と自動アップグレードの間隔を設定します。
  - **interval**：自動アップグレードの間隔（時間単位）。有効な値は 0 ～ 8760 です。
  - **start-time**：最初の自動アップグレードを開始する時刻。有効な値は *hh:mm[:ss]* です。
- **user-name**：サーバ認証用のユーザ名。
- **user-server**：ユーザ定義のサーバからの自動アップグレードをイネーブルにします。

自動アップグレードのスケジューリング

自動アップグレードをスケジューリングするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　自動アップグレード サブモードを開始します。

```
sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# auto-upgrade
sensor(config-hos-aut)#
```

ステップ 3　Cisco.com またはファイル サーバで新しいアップグレードを自動的に検索するようにセンサーを設定します。

a. Cisco.com で次の操作を行います。ステップ 4 に進みます。

```
sensor(config-hos-aut)# cisco-server enabled
```

b. サーバから次の操作を行います。

```
sensor(config-hos-aut)# user-server enabled
```

c. ファイル サーバの IP アドレスを指定します。

```
sensor(config-hos-ena)# ip-address 10.1.1.1
```

d. アップグレード ファイルが置かれているファイル サーバ上のディレクトリを指定します。

```
sensor(config-hos-ena)# directory /tftpboot/sensor_updates
```

e. ファイル サーバ プロトコルを指定します。

```
sensor(config-hos-ena)# file-copy-protocol ftp
```

（注） SCP を使用する場合は、センサーが SSH を介してサーバと通信できるように、**ssh host-key** コマンドを使用してサーバを SSH の既知ホスト リストに追加する必要があります。

ステップ 4　認証用のユーザ名を指定します。

```
sensor(config-hos-ena)# user-name tester
```

ステップ 5　このユーザのパスワードを指定します。

```
sensor(config-hos-ena)# password
Enter password[]: ******
Re-enter password: ******
```

ステップ 6　スケジューリングを指定します。

a. 特定の曜日の特定の時刻にアップグレードが開始されるカレンダー スケジューリングは、次のように指定します。

```
sensor(config-hos-ena)# schedule-option calendar-schedule
sensor(config-hos-ena-cal)# days-of-week sunday
sensor(config-hos-ena-cal)# times-of-day 12:00:00
```

b. 特定の間隔でアップグレードが開始される定期スケジューリングは、次のように指定します。

```
sensor(config-hos-ena)# schedule-option periodic-schedule
sensor(config-hos-ena-per)# interval 24
```

```
sensor(config-hos-ena-per)# start-time 13:00:00
```

ステップ 7　設定を確認できます。

```
sensor(config-hos-ena)# show settings
   enabled
   -----------------------------------------------
      schedule-option
      -----------------------------------------------
         periodic-schedule
         -----------------------------------------------
            start-time: 13:00:00
            interval: 24 hours
         -----------------------------------------------
      -----------------------------------------------
      ip-address: 10.1.1.1
      directory: /tftpboot/update/6.1_dummy_updates
      user-name: tester
      password: <hidden>
      file-copy-protocol: ftp default: scp
   -----------------------------------------------
sensor(config-hos-ena)#
```

ステップ 8　自動アップグレード サブモードを終了します。

```
sensor(config-hos-ena)# exit
sensor(config-hos)# exit
Apply Changes:?[yes]:
```

ステップ 9　**Enter** を押して変更内容を確定するか、**no** を入力して、これらを破棄します。

詳細情報

- サポートされる FTP サーバおよび HTTP/HTTPS サーバのリストについては、「サポートされる FTP サーバおよび HTTP/HTTPS サーバ」（P.25-2）を参照してください。
- SCP サーバを SSH の既知ホスト リストに追加する手順については、「既知のホスト キーの設定」（P.14-4）を参照してください。

自動アップグレードの例

表 25-1 に自動アップグレードの例を示します。これらの例では、アップグレードが 1:00 に開始され、以後 1 時間ごとに実行されるように設定されています。たとえば、サイクル 1 は 1:00、サイクル 2 は 2:00、サイクル 3 は 3:00 にそれぞれ開始されます。

表 25-1　自動アップグレード事例

ケース / 現在のバージョン	リモート ディレクトリ内のファイル	自動アップデートのサイクル / 新バージョン
ケース 0 5.1(4) E0 S250	• IPS-sig-S260-minreq-5.0-6.pkg • IPS-engine-E2-req-5.1-4.pkg • IPS-sig-S262-req-E2.pkg • IPS-sig-S263-req-E2.pkg • IPS-engine-E3-req-5.1-4.pkg • IPS-sig-S264-req-E3.pkg	• サイクル 1 で IPS-engine-E3-req-5.1-4.pkg をインストールします。 新バージョンは 5.1(4) E2 S250 です。 • サイクル 2 で IPS-sig-S264-req-E3.pkg をインストールします。 新バージョンは 5.1(4) E2 S264 です。
ケース 1 5.1(4) E0 S250	• IPS-K9-sp-5.1-5.pkg • IPS-sig-S260-minreq-5.0-6.pkg • IPS-K9-5.1-6-E1.pkg • IPS-engine-E2-req-5.1-6.pkg • IPS-sig-S262-req-E2.pkg • IPS-sig-S263-req-E2.pkg	• サイクル 1 で IPS-K9-5.1-6-E1.pkg をインストールします。 新バージョンは 5.1(6) E1 S260 です。 • サイクル 2 で IPS-engine-E2-req-5.1-6.pkg をインストールします。 新バージョンは 5.1(6) E2 S260 です。 • サイクル 3 で IPS-sig-S263-req-E2.pkg をインストールします。 新バージョンは 5.1(6) E2 S263 です。
ケース 2 5.1(6) E5 S300	• IPS-K9-6.0-1-E7.pkg • IPS-K9-6.0-2-E9.pkg • IPS-K9-6.0-3-E11.pkg • IPS-engine-E10-req-6.0-2.pkg • IPS-engine-E12-req-6.0-3.pkg • IPS-sig-S305-req-E12.pkg • IPS-sig-S307-req-E12.pkg	• サイクル 1 で IPS-K9-6.0-3-E11.pkg をインストールします。 新バージョンは 6.0(3) E11 S300 です。 • サイクル 2 で IPS-engine-E12-req-6.0-3.pkg をインストールします。 新バージョンは 6.0(3) E12 S300 です。 • サイクル 3 で IPS-sig-S307-req-E12.pkg をインストールします。 新バージョンは 6.0(3) E12 S307 です。
ケース 3 5.1(6) E10 S300	• IPS-K9-6.0-1-E9.pkg • IPS-engine-E11-req-6.0-1.pkg • IPS-sig-S305-req-E11.pkg • IPS-sig-S307-req-E11.pkg	• E9 は E10 よりも小さいため、サイクル 1 では何もインストールされません。
ケース 4 5.1(6) E10 S300	• IPS-engine-E11-req-5.1-6.pkg • IPS-sig-S301-req-E10.pkg	• サイクル 1 で IPS-engine-E11-req-5.1-6.pkg をインストールします。 新バージョンは 5.1(6) E11 S300 です。

表 25-1　自動アップグレード事例（続き）

ケース / 現在のバージョン	リモート ディレクトリ内のファイル	自動アップデートのサイクル / 新バージョン
ケース 5 5.1(6) E10 S300	• IPS-sig-S301-req-E10.pkg • IPS-sig-S302-req-E11.pkg • IPS-sig-S303-req-E12.pkg • IPS-engine-E11-req-5.1-6.pkg	• サイクル 1 で IPS-engine-E11-req-5.1-6.pkg をインストールします。 新バージョンは 5.1(6) E11 S300 です。 • サイクル 2 で IPS-sig-S302-req-E11.pkg をインストールします。 新バージョンは 5.1(6) E11 S302 です。
ケース 6 6.0(3)E1 S300 (IPS 4270-20)	• IPS-K9-6.0-4-E1.pkg • IPS-4270_20-K9-6.0-4-E1.pkg	• サイクル 1 で IPS-4270_20-K9-6.0-4-E1.pkg をインストールします。 新バージョンは 6.0(4)E1 S310 です。
ケース 7 6.0(4)E3 S330 (AIM IPS)	• IPS-K9-6.0-5-E3.pkg • IPS-AIM-K9-6.0-5-E3.pkg	• サイクル 1 で IPS-AIM-K9-6.0-5-E3.pkg をインストールします。 新バージョンは 6.0(5)E3 S335 です。
ケース 8 6.0(5)E5 S330 (AIM IPS)	• IPS-K9-7.0-1-E5.pkg • IPS-AIM-K9-7.0-1-E5.pkg	• サイクル 1 で IPS-K9-7.0-1-E5.pkg をインストールします。 新バージョンは 7.0(1)E5 S377 です。

センサーのダウングレード

最後に適用されたシグニチャ アップグレードまたはシグニチャ エンジン アップグレードをセンサーから削除するには、**downgrade** コマンドを使用します。

注意　**downgrade** コマンドを使用して、Cisco IPS 7.1 から 7.0 へなど、以前のメジャー バージョンまたはマイナー バージョンに戻すことはできません。**downgrade** コマンドでは、最新のシグニチャ アップデートまたはシグニチャ エンジン アップデートからのダウングレードのみ可能です。7.0 に戻すには、センサーのイメージを再作成する必要があります。

最後に適用されたシグニチャ アップデートまたはシグニチャ エンジン アップデートをセンサーから削除するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して次のようにセンサーにログインします。

ステップ 2　グローバル コンフィギュレーション モードを開始します。

```
sensor# configure terminal
```

ステップ 3　最近適用されたサービス パックまたはシグニチャ アップデートがない場合、**downgrade** コマンドは使用できません。

```
sensor(config)# downgrade
No downgrade available.
sensor(config)#
```

アプリケーション パーティションの復旧

ここでは、アプリケーション パーティションを復旧する方法について説明します。内容は次のとおりです。

アプリケーション パーティションについて

センサーのアプリケーション パーティション イメージが使用できなくなった場合は、復旧することができます。この方法を使用したときには、一部のネットワーク設定情報が保持されるため、復旧を実行した後もネットワークにアクセスできます。

recover application-partition コマンドを使用してリカバリ パーティションをブートすると、センサー上のアプリケーション パーティションが自動的に復旧されます。

（注）　アプリケーション パーティション イメージを復旧する前にリカバリ パーティションを最新のバージョンにアップグレードしてある場合は、その最新のソフトウェア イメージをインストールできます。

recover application-partition コマンドは、Telnet 接続または SSH 接続を使用して実行できるため、リモート ロケーションにインストールされているセンサーを復旧する場合に使用することを推奨します。

（注）　復旧後にセンサーに再接続する場合は、デフォルトのユーザ名とパスワード **cisco** を使用してログインする必要があります。

詳細情報

リカバリ パーティションを最新バージョンにアップグレードする手順については、「リカバリ パーティションのアップグレード」（P.25-4）を参照してください。

センサーのアプリケーション パーティション イメージの復旧

アプリケーション パーティション イメージを復旧するには、次の手順を実行します。

ステップ 1　リカバリ パーティション イメージ ファイル（IPS-K9-r-1.1-a-7.0-1-E4.pkg）をセンサーからアクセスできる FTP、HTTP、または HTTPS サーバにダウンロードします。

ステップ 2　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 3　コンフィギュレーション モードを開始します。

```
sensor# configure terminal
```

（注）　リカバリ パーティションをアップグレードするには、センサーで IPS 7.0(1) 以上がすでに実行されている必要があります。

ステップ 4　アプリケーション パーティション イメージを復旧します。

```
sensor(config)# recover application-partition
Warning: Executing this command will stop all applications and re-image the node to
version 6.2(1)E3. All configuration changes except for network settings will be reset to
default.
Continue with recovery? []:
```

ステップ 5　**yes** と入力して続行します。

recover コマンドを実行すると、即座にシャットダウンが開始されます。シャットダウンには少し時間がかかることがあり、この間に CLI にアクセスできますが、アクセスは警告なしに終了します。

アプリケーション パーティションのイメージは、リカバリ パーティションに保存されているイメージを使用して再作成されます。ここで、**setup** コマンドを使用してアプライアンスを初期化する必要があります。IP アドレス、ネットマスク、アクセス リスト、時間帯、およびオフセットは、保存されてから、イメージが再作成されたアプリケーション パーティションに適用されます。**recover application-partition** コマンドをリモートで実行した場合は、デフォルトのユーザ名とパスワード（**cisco**/**cisco**）を使用してセンサーに SSH 接続し、**setup** コマンドで再度センサーを初期化できます。Telnet は、デフォルトでディセーブルになっているため、センサーを初期化してからでなければ使用できません。

詳細情報

- TFTP サーバの詳細については、「TFTP サーバ」（P.25-14）を参照してください。
- Cisco.com でソフトウェアを検索する手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。
- **setup** コマンドの使用手順については、第 23 章「センサーの初期化」を参照してください。

システム イメージのインストール

ここでは、システム イメージをアプライアンスおよびモジュールにインストールする手順について説明します。内容は次のとおりです。

注意　システム イメージをインストールすると、すべてのユーザ設定が失われます。システム イメージのインストールによるセンサーの復旧を試みる前に、**recover application-partition** コマンドを使用するか、またはセンサーの起動時にリカバリ パーティションを選択する方法による復旧を試みてください。

ROMMON

Cisco のセンサーには、ROMMON と呼ばれるプリブート CLI が含まれているものがあります。ROMMON を使用すると、プライマリ デバイス上のイメージの欠落や破損などが原因で標準のアプリケーションをブートできない場合に、センサー上のイメージをブートすることができます。ROMMON は、特にリモート センサーの復旧に役立ちます（シリアル コンソール ポートが利用可能な場合）。

ROMMON へのアクセスは、センサー シャーシの RJ-45F コネクタで利用可能な Cisco 標準の非同期 RS-232C DTE であるシリアル コンソール ポートを介してのみ可能です。シリアル ポートは、9600 ボー、8 データ ビット、1 ストップ ビット、パリティなし、フロー制御なしに設定されています。

詳細情報

ターミナル サーバの使用手順については、「ターミナル サーバの設定」（P.25-14）を参照してください。

TFTP サーバ

ROMMON は TFTP を使用して、イメージをダウンロードして起動します。TFTP は、遅延やエラーリカバリなどのネットワークの問題は処理しません。TFTP は限定的なパケットの整合性チェックを実装するので、正しい整合性値を持つパケットが順に到着し、エラーが発生する可能性はきわめて低くなります。ただし、TFTP はパイプラインを提供しないので、転送の合計時間は、転送するパケットの数にネットワークの平均値 RTT を掛けた値と等しくなります。この制限があるため、TFTP サーバはセンサーと同じ LAN セグメントに配置することをお勧めします。RTT が 100 ミリ秒未満のネットワークは、信頼性の高いイメージ配信を提供する必要があります。TFTP サーバによっては、転送可能なファイルの最大サイズが 32 MB に制限されている場合があります。

ターミナル サーバの設定

ターミナル サーバは複数の低速非同期ポートを持つルータです。この複数のポートは、他のシリアル デバイスに接続されています。ターミナル サーバを使用して、アプライアンスを含むネットワーク機器をリモートで管理することができます。

RJ-45 接続またはヒドラ ケーブル アセンブリ接続を使用して Cisco ターミナル サーバをセットアップするには、次の手順を実行します。

ステップ 1　次のいずれかの方法で、ターミナル サーバに接続します。

- RJ-45 接続を行うターミナル サーバの場合、180 ロールオーバー ケーブルをアプライアンスのコンソール ポートからターミナル サーバのポートに接続します。
- ヒドラ ケーブル アセンブリの場合、ストレート パッチ ケーブルをアプライアンスのコンソール ポートからターミナル サーバのポートに接続します。

ステップ 2　ターミナル サーバで、ラインとポートを設定します。イネーブル モードで次の設定を入力します。ここで、# は設定するポートの回線番号です。

```
config t
line #
login
transport input all
stopbits 1
flowcontrol hardware
speed 9600
exit
exit
wr mem
```

ステップ 3　アプライアンスへの不正アクセスを防ぐため、ターミナル セッションは確実に正しく終了してください。

ターミナル セッションが正しく終了されていない場合、つまり、セッションを開始したアプリケーションから exit(0) 信号が受信されていない場合、ターミナル セッションは開いたままです。ターミナル セッションが正しく終了していない場合、そのシリアル ポート上で開かれる次のセッションでは、認証が実行されません。

注意　接続を確立するために使用したアプリケーションを終了する前に、必ずセッションを終了してログイン プロンプトに戻ってください。

注意　誤って接続が切断されたり終了した場合は、接続を再確立し、正しく終了して、アプライアンスに対する不正なアクセスを防ぎます。

IPS 4240 および IPS 4255 システム イメージのインストール

注意　システム イメージをインストールすると、すべてのユーザ設定が失われます。システム イメージのインストールによるセンサーの復旧を試みる前に、**recover application-partition** コマンドを使用するか、またはセンサーの起動時にリカバリ パーティションを選択する方法による復旧を試みてください。

アプライアンスで ROMMON を使用してシステム イメージをコンパクト フラッシュ デバイスに TFTP 転送することにより、IPS 4240 および IPS 4255 システム イメージをインストールできます。

（注）　この手順は IPS-4240 を対象としていますが、IPS 4255 にも有効です。IPS 4255 用のシステム イメージには、ファイル名に「4255」が付いています。

IPS 4240 および IPS 4255 システム イメージをインストールするには、次の手順を実行します。

ステップ 1　IPS 4240 システム イメージ ファイル（IPS-4240-K9-sys-1.1-a-7.0-1-E4.img）を IPS 4240 からアクセスできる TFTP サーバの tftp ルート ディレクトリにダウンロードします。

（注）　IPS 4240 のイーサネット ポートに接続されているネットワークから TFTP サーバの場所にアクセスできることを確認します。

ステップ 2　IPS 4240 をブートします。

```
Booting system, please wait...

CISCO SYSTEMS
Embedded BIOS Version 1.0(5)0 09/14/04 12:23:35.90

Low Memory: 631 KB
High Memory: 2048 MB
PCI Device Table.
Bus Dev Func VendID DevID Class              Irq
00  00  00   8086   2578  Host Bridge
00  01  00   8086   2579  PCI-to-PCI Bridge
00  03  00   8086   257B  PCI-to-PCI Bridge
00  1C  00   8086   25AE  PCI-to-PCI Bridge
00  1D  00   8086   25A9  Serial Bus         11
00  1D  01   8086   25AA  Serial Bus         10
00  1D  04   8086   25AB  System
00  1D  05   8086   25AC  IRQ Controller
00  1D  07   8086   25AD  Serial Bus         9
00  1E  00   8086   244E  PCI-to-PCI Bridge
00  1F  00   8086   25A1  ISA Bridge
00  1F  02   8086   25A3  IDE Controller     11
00  1F  03   8086   25A4  Serial Bus         5
00  1F  05   8086   25A6  Audio              5
02  01  00   8086   1075  Ethernet           11
03  01  00   177D   0003  Encrypt/Decrypt    9
03  02  00   8086   1079  Ethernet           9
03  02  01   8086   1079  Ethernet           9
03  03  00   8086   1079  Ethernet           9
03  03  01   8086   1079  Ethernet           9
04  02  00   8086   1209  Ethernet           11
04  03  00   8086   1209  Ethernet           5

Evaluating BIOS Options ...
Launch BIOS Extension to setup ROMMON

Cisco Systems ROMMON Version (1.0(5)0) #1: Tue Sep 14 12:20:30 PDT 2004

Platform IPS-4240-K9
Management0/0

MAC Address: 0000.c0ff.ee01
```

ステップ 3　システムの起動中に、次のプロンプトで Break または Esc を押して、ブートを中断します。ブートを即座に開始するには、スペースバーを押します。

（注）　Break または Esc は 10 秒以内に押してください。

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
```

システムが ROMMON モードに入ります。`rommon>` プロンプトが表示されます。

ステップ 4　現在のネットワーク設定を確認します。

```
rommon> set

ROMMON Variable Settings:
      ADDRESS=0.0.0.0
      SERVER=0.0.0.0
      GATEWAY=0.0.0.0
```

```
PORT=Management0/0
VLAN=untagged
IMAGE=
CONFIG=
```

変数の定義は次のとおりです。

- Address：IPS 4240 のローカル IP アドレス
- Server：アプリケーション イメージが格納されている TFTP サーバの IP アドレス
- Gateway：IPS 4240 によって使用されるゲートウェイ IP アドレス
- Port：IPS 4240 の管理に使用されるイーサネット インターフェイス
- VLAN：VLAN ID 番号（タグなしのまま）
- Image：システム イメージ ファイル パスとファイル名
- Config：これらのプラットフォームでは未使用

（注） ネットワーク接続を確立するために、すべての値が必要なわけではありません。address、server、gateway、および image の値は必要です。ローカル環境を設定するために必要な設定がわからない場合は、システム管理者に連絡してください。

ステップ 5　必要に応じて、TFTP ダウンロードに使用するインターフェイスを変更します。

（注） TFTP ダウンロードに使用されるデフォルトのインターフェイスは Management0/0 です。これは、IPS 4240 の MGMT インターフェイスに対応します。

```
rommon> PORT=interface_name
```

ステップ 6　必要に応じて、IPS 4240 上のローカル ポートの IP アドレスを割り当てます。

```
rommon> ADDRESS=ip_address
```

（注） IPS 4240 に割り当てられているものと同じ IP アドレスを使用します。

ステップ 7　必要に応じて、TFTP サーバの IP アドレスを割り当てます。

```
rommon> SERVER=ip_address
```

ステップ 8　必要に応じて、ゲートウェイの IP アドレスを割り当てます。

```
rommon> GATEWAY=ip_address
```

ステップ 9　次のいずれかのコマンドを使用して、ローカル イーサネット ポートから ping を実行することにより、TFTP サーバにアクセスできることを確認します。

```
rommon> ping server_ip_address
rommon> ping server
```

ステップ 10　必要に応じて、イメージのダウンロード元である TFTP ファイル サーバ上のパスおよびファイル名を定義します。

```
rommon> IMAGE=path/file_name
```

注意　**IMAGE** コマンドは、必ずすべて大文字で入力してください。他の ROMMON コマンドは小文字と大文字のどちらでも入力できますが、**IMAGE** コマンドはすべて大文字で入力する必要があります。

UNIX の例

```
rommon> IMAGE=/system_images/IPS-4240-K9-sys-1.1-a-7.0-1-E4.img
```

（注）　このパスは、UNIX TFTP サーバのデフォルト tftpboot ディレクトリからの相対パスです。デフォルトの tftpboot ディレクトリに置かれているイメージの IMAGE 指定には、ディレクトリ名もスラッシュも含まれていません。

Windows の例

```
rommon> IMAGE=¥system_images¥IPS-4240-K9-sys-1.1-a-7.0-1-E4.img
```

ステップ 11　**set** と入力し、Enter を押して、ネットワーク設定を確認します。

（注）　**sync** コマンドを使用すると、これらの設定をブート後も維持されるように NVRAM に保存できます。保存しない場合は、ROMMON からイメージをブートするときに毎回この情報を入力する必要があります。

ステップ 12　システム イメージをダウンロードしてインストールします。

```
rommon> tftp
```

注意　システム イメージの破損を避けるために、システム イメージのインストール中は IPS 4240 の電源を切らないでください。

（注）　ネットワーク設定が正しい場合、指定したイメージが IPS 4240 にダウンロードされ、ブートされます。必ず IPS 4240 イメージを使用してください。

詳細情報

- TFTP サーバの詳細については、「TFTP サーバ」（P.25-14）を参照してください。
- Cisco.com でソフトウェアを検索する手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。
- アプリケーション パーティションを復旧する手順については、「アプリケーション パーティションの復旧」（P.25-12）を参照してください。

IPS 4260 システム イメージのインストール

注意　システム イメージをインストールすると、すべてのユーザ設定が失われます。システム イメージのインストールによるセンサーの復旧を試みる前に、**recover application-partition** コマンドを使用するか、またはセンサーの起動時にリカバリ パーティションを選択する方法による復旧を試みてください。

アプライアンスで ROMMON を使用してシステム イメージをフラッシュ デバイスに TFTP 転送することにより IPS 4260 システム イメージをインストールできます。

IPS 4260 システム イメージをインストールするには、次の手順を実行します。

ステップ 1　IPS 4260 システム イメージ ファイル（IPS-4260-K9-sys-1.1-a-7.0-1-E4.img）を IPS 4260 からアクセスできる TFTP サーバの tftp ルート ディレクトリにダウンロードします。

IPS 4260 のイーサネット ポートに接続されているネットワークから TFTP サーバの場所にアクセスできることを確認します。

ステップ 2　IPS 4260 をブートします。

ステップ 3　システムの起動中に、次のプロンプトに対して Ctrl を押した状態で R を押します。

```
Evaluating Run Options...
```

（注）　Ctrl を押した状態で R を押す操作は 5 秒以内に行ってください。

```
Assuming IPS-4260-K9 Platform
 2 Ethernet Interfaces detected

Cisco Systems ROMMON Version (1.0(11)1c) #26: Mon Mar 13 18:05:54 CST 2006

Platform IPS-4260-K9
Management0/0
Link is UP
MAC Address: 0004.23cc.6047


Use ? for help.
rommon #0>
```

ステップ 4　必要に応じて、TFTP ダウンロードに使用するポートを変更します。

```
rommon #1> interface name
```

使用中のポートは、プラットフォーム ID のすぐ後にリスト表示されます。この例では、ポート Management0/0 は使用されています。

（注）　TFTP ダウンロードに使用されるデフォルトのポートは、Management0/0 です。これは、IPS 4260 のコマンド/コントロール（MGMT）インターフェイスに対応します。

（注）　ポート Management0/0（MGMT）および GigabitEthernet0/1（GE 0/1）は、シャーシ背面のラベルに記載されています。

ステップ 5　IPS 4260 上のローカル ポートの IP アドレスを指定します。

```
rommon> address ip_address
```

（注）　IPS 4260 に割り当てられているものと同じ IP アドレスを使用します。

ステップ 6　TFTP サーバの IP アドレスを指定します。

```
rommon> server ip_address
```

ステップ 7　ゲートウェイの IP アドレスを指定します。

```
rommon> gateway ip_address
```

ステップ 8　ローカル イーサネット ポートから ping を実行することにより、TFTP サーバにアクセスできることを確認します。

```
rommon> ping server_ip_address
rommon> ping server
```

ステップ 9　イメージのダウンロード元である TFTP ファイル サーバ上のパスとファイル名を指定します。

```
rommon> file path/filename
```

UNIX の例

```
rommon> file /system_images/IPS-4260-K9-sys-1.1-a-7.0-1-E4.img
```

（注）　このパスは、UNIX TFTP サーバのデフォルト tftpboot ディレクトリからの相対パスです。デフォルトの tftpboot ディレクトリに置かれているイメージのファイルの場所には、ディレクトリ名もスラッシュも含まれていません。

Windows の例

```
rommon> file <tftpboot_directory>IPS-4260-K9-sys-1.1-a-7.0-1-E4.img
```

ステップ 10　システム イメージをダウンロードしてインストールします。

```
rommon> tftp
```

（注）　IPS 4260 は、イメージの再作成処理中に、一度リブートします。アップデート プロセスの間は IPS 4260 の電源を切らないでください。電源を切ると、アップグレードが破損することがあります。

詳細情報

- TFTP サーバの詳細については、「TFTP サーバ」（P.25-14）を参照してください。
- Cisco.com でソフトウェアを検索する手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。
- アプリケーション パーティションを復旧する手順については、「アプリケーション パーティションの復旧」（P.25-12）を参照してください。

IPS 4270-20 システム イメージのインストール

注意　システム イメージをインストールすると、すべてのユーザ設定が失われます。システム イメージのインストールによるセンサーの復旧を試みる前に、**recover application-partition** コマンドを使用するか、またはセンサーの起動時にリカバリ パーティションを選択する方法による復旧を試みてください。

アプライアンスで ROMMON を使用してシステム イメージをコンパクト フラッシュ デバイスに TFTP 転送することにより、IPS 4270-20 システム イメージをインストールできます。

IPS 4270-20 システム イメージをインストールするには、次の手順を実行します。

ステップ 1　IPS 4270-20 システム イメージ ファイル（IPS-4270_20-K9-sys-1.1-a-7.0-1-E4.img）を IPS 4270-20 からアクセスできる TFTP サーバの tftp ルート ディレクトリにダウンロードします。

（注）　IPS 4270-20 のイーサネット ポートに接続されているネットワークから TFTP サーバの場所にアクセスできることを確認します。

ステップ 2　IPS 4270-20 をブートします。

```
Booting system, please wait...
Cisco Systems ROMMON Version (1.0(12)10) #7: Thu Jun 21 13:50:04 CDT 2007

ft_id_update: Invalid ID-PROM Controller Type (0x5df)

ft_id_update: Defaulting to Controller Type (0x5c2)
```

（注）　コントローラ タイプに関するエラーは既知の問題であり、無視してかまいません。

ステップ 3　システムの起動中に、次のプロンプトで Break または Esc を押して、ブートを中断します。ブートを即座に開始するには、スペースバーを押します。

（注）　Break または Esc は 10 秒以内に押してください。

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
```

システムが ROMMON モードに入ります。rommon> プロンプトが表示されます。

ステップ 4　現在のネットワーク設定を確認します。

```
rommon> set

ROMMON Variable Settings:
  ADDRESS=0.0.0.0
  SERVER=0.0.0.0
  GATEWAY=0.0.0.0
  PORT=Management0/0
  VLAN=untagged
  IMAGE=
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=2
```

```
RETRY=20
```

変数の定義は次のとおりです。

- Address：IPS 4270-20 のローカル IP アドレス
- Server：アプリケーション イメージが格納されている TFTP サーバの IP アドレス
- Gateway：IPS 4270-20 によって使用されるゲートウェイ IP アドレス
- Port：IPS 4270-20 の管理に使用されるイーサネット インターフェイス
- VLAN：VLAN ID 番号（タグなしのまま）
- Image：システム イメージ ファイル パスとファイル名
- Config：これらのプラットフォームでは未使用

（注） ネットワーク接続を確立するために、すべての値が必要なわけではありません。address、server、gateway、および image の値は必要です。ローカル環境を設定するために必要な設定がわからない場合は、システム管理者に連絡してください。

ステップ 5　必要に応じて、IPS 4270-20 上のローカル ポートの IP アドレスを割り当てます。

```
rommon> ADDRESS=ip_address
```

（注） IPS 4270-20 に割り当てられているものと同じ IP アドレスを使用します。

ステップ 6　必要に応じて、TFTP サーバの IP アドレスを割り当てます。

```
rommon> SERVER=ip_address
```

ステップ 7　必要に応じて、ゲートウェイの IP アドレスを割り当てます。

```
rommon> GATEWAY=ip_address
```

ステップ 8　次のいずれかのコマンドを使用して、ローカル イーサネット ポートから ping を実行することにより、TFTP サーバにアクセスできることを確認します。

```
rommon> ping server_ip_address
rommon> ping server
```

ステップ 9　必要に応じて、イメージのダウンロード元である TFTP ファイル サーバ上のパスおよびファイル名を定義します。

```
rommon> IMAGE=path/file_name
```

UNIX の例

```
rommon> IMAGE=/system_images/IPS-4270_20-K9-sys-1.1-a-7.0-1-E4.img
```

（注） このパスは、UNIX TFTP サーバのデフォルト tftpboot ディレクトリからの相対パスです。デフォルトの tftpboot ディレクトリに置かれているイメージの IMAGE 指定には、ディレクトリ名もスラッシュも含まれていません。

Windows の例

```
rommon> IMAGE=¥system_images¥IPS-4270_20-K9-sys-1.1-a-7.0-1-E4.img
```

ステップ 10　**set** と入力し、Enter を押して、ネットワーク設定を確認します。

（注）　**sync** コマンドを使用すると、これらの設定をブート後も維持されるように NVRAM に保存できます。保存しない場合は、ROMMON からイメージをブートするときに毎回この情報を入力する必要があります。

ステップ 11　システム イメージをダウンロードしてインストールします。

```
rommon> tftp
```

注意　システム イメージの破損を避けるために、システム イメージのインストール中は IPS 4270-20 の電源を切らないでください。

（注）　ネットワーク設定が正しい場合、指定したイメージが IPS 4270-20 にダウンロードされ、ブートされます。必ず IPS 4270-20 イメージを使用してください。

詳細情報

- TFTP サーバの詳細については、「TFTP サーバ」（P.25-14）を参照してください。
- Cisco.com でソフトウェアを検索する手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。
- アプリケーション パーティションを復旧する手順については、「アプリケーション パーティションの復旧」（P.25-12）を参照してください。

AIM IPS システム イメージのインストール

注意　システム イメージをインストールすると、すべてのユーザ設定が失われます。システム イメージのインストールによるセンサーの復旧を試みる前に、**recover application-partition** コマンドを使用するか、またはセンサーの起動時にリカバリ パーティションを選択する方法による復旧を試みてください。

AIM IPS システム イメージをインストールするには、次の手順を実行します。

ステップ 1　AIM IPS システム イメージ ファイル（IPS-AIM-K9-sys-1.1-7.0-1-E4.img）をダウンロードし、TFTP サーバの tftp ルート ディレクトリに配置します。

（注）　AIM IPS が TFTP サーバにアクセスできるようにネットワークが設定されていることを確認します。

利用可能な TFTP サーバがない場合は、ルータを TFTP サーバとして設定できます。

```
router# copy tftp: flash:
router# configure terminal
router(config)# tftp-server flash:IPS-AIM-K9-sys-1.1-7.0-1-E4.img
router(config)# exit
router#
```

ステップ 2　ハートビートのリセットをディセーブルにします。

```
router# service-module IDS-Sensor 0/slot_number heartbeat-reset disable
```

（注）　ハートビートのリセットをディセーブルにすると、システム イメージのインストール プロセスに時間がかかりすぎる場合でも、モジュールがリセットされなくなります。

ステップ 3　AIM IPS との間にセッションを確立します。

```
router# service-module IDS-Sensor 0/slot_number session
```

（注）　AIM IPS スロット番号を確認するには、**show configuration | include interface IDS-Sensor** コマンドを使用します。

ステップ 4　Shift と Ctrl を押した状態で 6 を押してから X を押してセッションを中断します。

`router#` プロンプトが表示されます。このプロンプトが表示されない場合は、Ctrl を押した状態で 6 を押してから、X を押してみてください。

ステップ 5　AIM IPS をリセットします。**reset** コマンドを確認するように要求されます。

```
router# service-module IDS-Sensor 0/slot_number reset
```

ステップ 6　**Enter** キーを押して確認します。Enter を押して、中断したセッションを再開します。

ブートローダのバージョンが表示された後、次のプロンプトが 15 秒間表示されます。

```
Please enter '***' to change boot configuration:
```

ステップ 7　この 15 秒の間に ******* と入力します。ブートローダ プロンプトが表示されます。

ステップ 8　Enter を押して AIM IPS とのセッションに戻ります。

ステップ 9　ブートローダを設定します。

```
ServicesEngine bootloader> config

IP Address [10.89.148.188]>
Subnet mask [255.255.255.0]>
TFTP server [10.89.150.74]>
Gateway [10.89.148.254]>
Default boot [disk]>
Number cores [2]>
ServicesEngine boot-loader >
```

各プロンプトで、値を入力するか、Enter を押して角括弧で囲まれた保存済みの値をそのまま適用します。

（注）　ゲートウェイの IP アドレスは、IDS-Sensor *スロット/ポート* インターフェイスの IP アドレスと一致している必要があります。

（注）　**unnumbered** コマンドを使用してモジュール インターフェイスをセットアップする場合、ゲートウェイの IP アドレスは、unnumbered コマンドの一部として使用されている他のルータ インターフェイスの IP アドレスとする必要があります。

注意　AIM IPS イメージのパス名はフル パスですが、tftp サーバのルート ディレクトリからの相対パスです（通常は、/tftpboot）。

ステップ 10　ブートローダを起動します。

```
ServicesEngine bootloader> upgrade
```

ステップ 11　ブートローダの指示に従ってソフトウェアをインストールします（オプション 1 を選択して、ウィザードの指示に従います）。

（注）　次の例では、AIM IPS IP の IP アドレスは 10.1.9.201 です。イメージ処理では、IP アドレス 10.1.9.1 のルータ TFTP サーバから AIM IPS イメージにアクセスします。

例

```
Booting from flash...please wait.
Please enter '***' to change boot configuration:
11 ***
ServicesEngine boot-loader Version : 1.1.0
ServicesEngine boot-loader > config

IP Address [10.1.9.201]>
Subnet mask [255.255.255.0]>
TFTP server [10.1.9.1]>
Gateway [10.1.9.1]>
Default boot [disk]>
Number cores [2]>
ServicesEngine boot-loader > upgrade

Cisco Systems, Inc.
Services engine upgrade utility for AIM-IPS
-----
Main menu
1 - Download application image and write to USB Drive
2 - Download bootloader and write to flash
3 - Download minikernel and write to flash
r - Exit and reset card
x - Exit
Selection [123rx]
Download recovery image via tftp and install on USB Drive
TFTP server [10.1.9.1]>
full pathname of recovery image []:IPS-AIM-K9-sys-1.1-7.0-1-E4.img
Ready to begin
Are you sure [Y/N]
Returning TRUE
Press <CTRL-C> to abort.
octeth1:        Up     1Gbs Full duplex, (port  1)
octeth0:        Down  10Mbs Half duplex, (port  0)
Using octeth1 device
TFTP from server 10.1.9.1; our IP address is 10.1.9.201
Filename 'IPS-AIM-K9-sys-1.1-7.0-1-E4.img'.
Load address: 0x21000000
Loading: ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
         ###################################################################
```

```
                ################################################################
                ################################################################
                ################################################################
                ######
                32 MB received
                ################################################################
                ########################
done
```

ステップ 12　Shift と Ctrl を押した状態で 6 を押してから X を押してセッションを中断します。`router#` プロンプトが表示されます。このプロンプトが表示されない場合は、Ctrl を押した状態で 6 を押してから、X を押してみてください。

ステップ 13　ルータの CLI 側で、セッションをクリアします。

```
router# service-module interface ids-sensor 0/slot_number session clear
```

ステップ 14　ハートビートのリセットをイネーブルにします。

```
router# service-module IDS-sensor 0/slot_number heartbeat-reset enable
```

詳細情報

- TFTP サーバの詳細については、「TFTP サーバ」（P.25-14）を参照してください。
- アンナンバード IP アドレスを設定する手順については、「Using an Unnumbered IP Address Interface」を参照してください。
- アプリケーション パーティションを復旧する手順については、「アプリケーション パーティションの復旧」（P.25-12）を参照してください。
- Cisco.com でソフトウェアを検索する手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。

AIP SSM および AIP SSC-5 システム イメージのインストール

注意　システム イメージをインストールすると、すべてのユーザ設定が失われます。システム イメージのインストールによるセンサーの復旧を試みる前に、**recover application-partition** コマンドを使用するか、またはセンサーの起動時にリカバリ パーティションを選択する方法による復旧を試みてください。

ここでは、AIP SSM および AIP SSC-5 システム イメージをインストールする方法について説明します。内容は次のとおりです。

- 「AIP SSM または AIM-SSC-5 イメージの再作成」（P.25-26）
- 「recover configure/boot コマンドを使用した AIP SSM または AIP SSC-5 イメージの再作成」（P.25-27）

AIP SSM または AIM-SSC-5 イメージの再作成

AIP SSM および AIP SSC-5 のイメージは、次のいずれかの方法で再作成できます。

- 適応型セキュリティ アプライアンスから **hw-module module 1 recover configure/boot** コマンドを使用します。

- **recover application-partition** コマンドを使用して、センサーの CLI からアプリケーション イメージを復旧します。
- **upgrade** コマンドを使用して、センサーの CLI からリカバリ イメージをアップグレードします。

詳細情報

- **hw-module module 1 recover configure/boot** コマンドの使用手順については、「recover configure/boot コマンドを使用した AIP SSM または AIP SSC-5 イメージの再作成」（P.25-27）を参照してください。
- アプリケーション パーティションを復旧する手順については、「アプリケーション パーティションの復旧」（P.25-12）を参照してください。
- リカバリ イメージをアップグレードする手順については、「リカバリ パーティションのアップグレード」（P.25-4）を参照してください。

recover configure/boot コマンドを使用した AIP SSM または AIP SSC-5 イメージの再作成

AIP SSM または AIP SSC-5 で障害が発生し、モジュール アプリケーション イメージを実行できない場合は、適応型セキュリティ アプライアンス CLI を使用して、アプリケーション イメージを TFTP サーバからモジュールに転送できます。適応型セキュリティ アプライアンスはモジュール ROMMON アプリケーションと通信し、イメージを転送できます。

（注） 指定する TFTP サーバが、最大 60 MB のサイズのファイルを転送できることを確認してください。

（注） ネットワークとイメージのサイズに応じて、このプロセスは完了までに約 15 分間かかることがあります。

AIP SSM および AIP SSC-5 システム イメージをインストールするには、次の手順を実行します。

ステップ 1　適応型セキュリティ アプライアンスにログインします。

ステップ 2　イネーブル モードを開始します。

```
asa# enable
```

ステップ 3　AIP SSM および AIP SSC-5 用のリカバリ設定を指定します。

```
asa (enable)# hw-module module 1 recover configure
```

（注） リカバリ設定に誤りがあった場合は、**hw-module module 1 recover stop** コマンドを使用してシステム イメージの再作成を停止してから、設定を修正できます。

ステップ 4　システム イメージの TFTP URL を指定します。

```
Image URL [tftp://0.0.0.0/]:
```

例

```
Image URL [tftp://0.0.0.0/]: tftp://10.89.146.1/IPS-SSM-K9-sys-1.1-a-7.0-1-E4.img
```

ステップ 5　AIP SSM または AIP SSC-5 のコマンド/コントロール インターフェイスを指定します。

（注）　ポート IP アドレスは、AIP SSM および AIP SSC-5 の管理 IP アドレスです。

```
Port IP Address [0.0.0.0]:
```

例

```
Port IP Address [0.0.0.0]: 10.89.149.231
```

ステップ 6　VLAN ID を 0 のままにします。

```
VLAN ID [0]:
```

ステップ 7　AIP SSM または AIP SSC-5 のデフォルト ゲートウェイを指定します。

```
Gateway IP Address [0.0.0.0]:
```

例

```
Gateway IP Address [0.0.0.0]: 10.89.149.254
```

ステップ 8　リカバリを実行します。イメージが TFTP サーバから AIP SSM または AIP SSC-5 に転送され、AIP SSM または AIP SSC-5 が再起動されます。

```
asa# hw-module module 1 recover boot
```

ステップ 9　完了するまでリカバリを定期的にチェックします。

（注）　ステータスは、リカバリ中は [Recovery] となり、イメージの再作成が完了すると [Up] になります。

```
asa# show module 1

Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5540 Adaptive Security Appliance         ASA5540            P2B00000019
  1 ASA 5500 Series Security Services Module-20  ASA-SSM-20         P1D000004F4

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 000b.fcf8.7b1c to 000b.fcf8.7b20  0.2          1.0(7)2      7.1(1)82
  1 000b.fcf8.011e to 000b.fcf8.011e  0.1          1.0(7)2      5.0(0.22)S129.0

Mod Status
--- ------------------
  0 Up Sys
  1 Up
asa#

asa# show module 1
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5505 Adaptive Security Appliance         ASA5505            JAB11370240
  1 ASA 5500 Series Security Services Card-5     ASA-SSC-AIP-5      JAF12380MDH

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- --------------------------
  1 SSC SSM                        Down 7.0.(1)E4
```

（注）　出力の [Status] フィールドは、AIP SSM または AIP SSC-5 の動作ステータスを示します。AIP SSM または AIP SSC-5 の動作ステータスは、通常は [Up] となります。適応型セキュリティ アプライアンスが AIP SSM または AIP SSC-5 にアプリケーション イメージを転送している間は、出力の [Status] フィールドは [Recover] となります。適応型セキュリティ アプライアンスによるイメージの転送が完了し、AIP SSM または AIP SSC-5 が再起動されると、新たに転送されたイメージが実行されます。

（注）　リカバリ処理中にエラーが発生した場合、デバッグを実行するには、**debug module-boot** コマンドを使用して、システム イメージの再作成処理のデバッグをイネーブルにします。

ステップ 10　AIP SSM または AIP SSC-5 との間にセッションを確立し、**setup** コマンドで AIP SSM または AIP SSC-5 を初期化します。

（注）　AIP SSC-5 を初期化するために **setup** コマンドを実行する必要はありません。この場合は、ASDM を使用して初期化します。

詳細情報

- TFTP サーバの詳細については、「TFTP サーバ」（P.25-14）を参照してください。
- **setup** コマンドを使用して AIP SSM を初期化する手順については、第 23 章「センサーの初期化」を参照してください。
- ASDM を使用して AIP SSC-5 を初期化する手順については、「ASDM での AIP SSC-5 のセットアップ」（P.23-8）を参照してください。
- Cisco.com でソフトウェアを検索する手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。

IDSM2 システム イメージのインストール

ここでは、IDSM2 システム イメージのインストール方法について説明します。内容は次のとおりです。

IDSM2 システム イメージについて

IDSM2 アプリケーション パーティションが使用できなくなった場合は、メンテナンス パーティションからイメージを再作成できます。IDSM2 のアプリケーション パーティションのイメージを再作成したら、**setup** コマンドを使用して IDSM2 を初期化する必要があります。

新しいメンテナンス パーティション イメージ ファイルがある場合は、アプリケーション パーティションからメンテナンス パーティションのイメージを再作成できます。

詳細情報

setup コマンドを使用して IDSM2 を初期化する手順については、第 23 章「センサーの初期化」を参照してください。

Catalyst ソフトウェアの IDSM2 システム イメージのインストール

システム イメージをインストールするには、次の手順を実行します。

ステップ 1　IDSM2 システム イメージ ファイル（IPS-IDSM2-K9-sys-1.1-a-7.0-1-E4.bin.gz）を IDSM2 からアクセスできる FTP サーバの FTP ルート ディレクトリにダウンロードします。

ステップ 2　スイッチの CLI にログインします。

ステップ 3　IDSM2 をメンテナンス パーティションにブートします。

```
console> (enable) reset module_number cf:1
```

ステップ 4　メンテナンス パーティション CLI にログインします。

```
login: guest
Password: cisco
```

（注）　IDSM2 にメンテナンス パーティションを設定する必要があります。

ステップ 5　システム イメージをインストールします。

```
guest@hostname.localdomain# upgrade ftp://user@ftp server IP/directory
path/IPS-IDSM2-K9-sys-1.1-a-7.0-1-E4.bin.gz
```

ステップ 6　FTP サーバのパスワードを指定します。アプリケーション パーティション ファイルのダウンロードが完了すると、次に進むかどうか尋ねられます。

```
Upgrading will wipe out the contents on the hard disk. Do you want to proceed installing
it [y|n]:
```

ステップ 7　**y** と入力して続行します。アプリケーション パーティション ファイルのインストールが完了すると、メンテナンス パーティションの CLI に戻ります。

ステップ 8　メンテナンス パーティションの CLI を終了して、スイッチの CLI に戻ります。

ステップ 9　IDSM2 をアプリケーション パーティションにリブートします。

```
console> (enable) reset module_number hdd:1
```

ステップ 10　IDSM2 のリブートが完了したら、ソフトウェアのバージョンをチェックします。

ステップ 11　アプリケーション パーティション CLI にログインし、**setup** コマンドを使用して IDSM2 を初期化します。

詳細情報

- サポートされる FTP サーバおよび HTTP/HTTPS サーバのリストについては、「サポートされる FTP サーバおよび HTTP/HTTPS サーバ」（P.25-2）を参照してください。
- IDSM2 にメンテナンス パーティションを設定する手順については、「Catalyst ソフトウェアの IDSM2 メンテナンス パーティションの設定」（P.25-32）および 「Cisco IOS ソフトウェアの IDSM2 メンテナンス パーティションの設定」（P.25-36）を参照してください。
- Cisco.com でソフトウェアを検索する手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。
- IDSM2 を初期化する手順については、第 23 章「センサーの初期化」を参照してください。

Cisco IOS ソフトウェアの IDSM2 システム イメージのインストール

システム イメージをインストールするには、次の手順を実行します。

ステップ 1　IDSM2 システム イメージ ファイル（IPS-IDSM2-K9-sys-1.1-a-7.0-1-E4.bin.gz）を IDSM2 からアクセスできる FTP サーバの FTP ルート ディレクトリにダウンロードします。

ステップ 2　スイッチの CLI にログインします。

ステップ 3　IDSM2 をメンテナンス パーティションにブートします。

```
router# hw-module module module_number reset cf:1
```

ステップ 4　メンテナンス パーティション CLI との間にセッションを確立します。

```
router# session slot slot_number processor 1
```

ステップ 5　メンテナンス パーティション CLI にログインします。

```
login: guest
Password: cisco
```

ステップ 6　メンテナンス パーティション インターフェイスの IP アドレスを設定します。

```
guest@localhost.localdomain# ip address ip_address netmask
```

（注）　スイッチ設定に基づき、IDSM2 管理インターフェイスがある VLAN に適したアドレスを選択します。

ステップ 7　メンテナンス パーティションのデフォルト ゲートウェイのアドレスを設定します。

```
guest@localhost.localdomain# ip gateway gateway_address
```

ステップ 8　システム イメージをインストールします。

```
guest@hostname.localdomain# upgrade
ftp://user@ftp_server_ip_address/directory_path/IPS-IDSM2-K9-sys-1.1-a-7.0-1-E4.bin.gz
-install
```

ステップ 9　FTP サーバのパスワードを指定します。

アプリケーション パーティション ファイルのダウンロードが完了すると、次に進むかどうか尋ねられます。

```
Upgrading will wipe out the contents on the hard disk.
Do you want to proceed installing it [y|n]:
```

ステップ 10　**y** と入力して続行します。アプリケーション パーティション ファイルのインストールが完了すると、メンテナンス パーティションの CLI に戻ります。

ステップ 11　メンテナンス パーティションの CLI を終了して、スイッチの CLI に戻ります。

ステップ 12　IDSM2 をアプリケーション パーティションにリブートします。

```
router# hw-module module module_number reset hdd:1
```

ステップ 13　IDSM2 がオンラインであり、ソフトウェアのバージョンが正しいことと、ステータスが [ok] であることを確認します。

```
router# show module module_number
```

ステップ 14　IDSM2 アプリケーション パーティション CLI との間にセッションを確立します。

```
router# session slot slot_number processor 1
```

ステップ 15　**setup** コマンドを使用して IDSM2 を初期化します。

詳細情報

- サポートされる FTP サーバおよび HTTP/HTTPS サーバのリストについては、「サポートされる FTP サーバおよび HTTP/HTTPS サーバ」（P.25-2）を参照してください。
- IDSM2 にメンテナンス パーティションを設定する手順については、「Catalyst ソフトウェアの IDSM2 メンテナンス パーティションの設定」（P.25-32）および「Cisco IOS ソフトウェアの IDSM2 メンテナンス パーティションの設定」（P.25-36）を参照してください。
- Cisco.com でソフトウェアを検索する手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。
- IDSM2 を初期化する手順については、第 23 章「センサーの初期化」を参照してください。

Catalyst ソフトウェアの IDSM2 メンテナンス パーティションの設定

IDSM2 メンテナンス パーティションを設定するには、次の手順を実行します。

ステップ 1　スイッチの CLI にログインします。

ステップ 2　特権モードに入ります。

```
console# enable
console(enable)#
```

ステップ 3　IDSM2 をリロードします。

```
console> (enable) reset module_number cf:1
```

ステップ 4　IDSM2 との間にセッションを確立します。

```
console# session 9
Trying IDS-9...
Connected to IDS-9.
Escape character is '^]'.

Cisco Maintenance image
```

（注）　IDSM2 メンテナンス パーティションに Telnet または SSH で接続することはできません。IDSM2 とのセッションはスイッチ CLI から確立する必要があります。

ステップ 5　ユーザ **guest** とパスワード **cisco** でログインします。

（注）　ゲスト パスワードの変更は可能ですが、推奨できません。メンテナンス パーティションのゲスト パスワードを忘れ、何らかの理由で IDSM2 アプリケーション パーティションにログインできない場合は、IDSM2 の RMA が必要です。

```
login: guest
Password: cisco

Maintenance image version: 2.1(2)

guest@idsm2.localdomain#
```

ステップ 6　IDSM2 メンテナンス パーティションのホスト設定を表示します。

```
guest@idsm2.localdomain# show ip

IP address      : 10.89.149.74
Subnet Mask     : 255.255.255.128
IP Broadcast    : 10.255.255.255
DNS Name        : idsm2.localdomain
Default Gateway : 10.89.149.126
Nameserver(s)   :

guest@idsm2.localdomain#
```

ステップ 7　IDSM2 メンテナンス パーティションのホスト設定（IP アドレス、ゲートウェイ、ホスト名）をクリアします。

```
guest@idsm2.localdomain# clear ip
guest@localhost.localdomain# show ip

IP address      : 0.0.0.0
Subnet Mask     : 0.0.0.0
IP Broadcast    : 0.0.0.0
DNS Name        : localhost.localdomain
Default Gateway : 0.0.0.0
Nameserver(s)   :

guest@localhost.localdomain#
```

ステップ 8　メンテナンス パーティションのホスト設定を指定します。

a.　IP アドレスを指定します。

```
guest@localhost.localdomain# ip address ip_address netmask
```

b.　デフォルト ゲートウェイを指定します。

```
guest@localhost.localdomain# ip gateway gateway_ip_address
```

c.　ホスト名を指定します。

```
guest@localhost.localdomain# ip host hostname
```

ステップ 9　メンテナンス パーティションのホスト設定を表示します。

```
guest@idsm2.localdomain# show ip

IP address      : 10.89.149.74
Subnet Mask     : 255.255.255.128
IP Broadcast    : 10.255.255.255
DNS Name        : idsm2.localdomain
Default Gateway : 10.89.149.126
Nameserver(s)   :

guest@idsm2.localdomain#
```

ステップ 10　アプリケーション パーティションにインストールされているイメージを確認します。

```
guest@idsm2.localdomain# show images
Device name             Partition#              Image name
-----------             ----------              ----------
Hard disk(hdd)          1                       7.0(1)
guest@idsm2.localdomain#
```

ステップ 11　メンテナンス パーティションのバージョン（BIOS バージョンを含む）を確認します。

```
guest@idsm2.localdomain# show version

Maintenance image version: 2.1(2)
mp.2-1-2.bin : Thu Nov 18 11:41:36 PST 2004 :
integ@kplus-build-lx.cisco.com

Line Card Number :WS-SVC-IDSM2-XL
Number of Pentium-class Processors : 2
BIOS Vendor: Phoenix Technologies Ltd.
BIOS Version: 4.0-Rel 6.0.9

Total available memory: 2012 MB
Size of compact flash: 61 MB
Size of hard disk: 19077 MB
Daughter Card Info: Falcon rev 3, FW ver 2.0.3.0 (IDS), SRAM  8 MB, SDRAM  256 MB

guest@idsm2.localdomain#
```

ステップ 12　アプリケーション パーティションをアップグレードします。

```
guest@idsm2.localdomain# upgrade
ftp://jsmith@10.89.146.11//RELEASES/Latest/7.0-1/WS-SVC-IDSM2-K9-sys-1.1-a-7.0-1-E4.bin.
gz
Downloading the image. This may take several minutes...
Password for jsmith@10.89.146.114:

ftp://jsmith@10.89.146.11//RELEASES/Latest/7.0-1/WS-SVC-IDSM2-K9-sys-1.1-a-7.0-1-E4.bin.gz
(unknown size)
/tmp/upgrade.gz           [|]   28616K
29303086 bytes transferred in 5.34 sec (5359.02k/sec)

Upgrade file
ftp://jsmith@10.89.146.114//RELEASES/Latest/7.0-1/WS-SVC-IDSM2-K9-sys-1.1-a-7.0-1-E4.bin.g
z is downloaded.
Upgrading will wipe out the contents on the storage media.
Do you want to proceed installing it [y|N]:
```

ステップ 13　**y** と入力してアップグレードを続行します。

```
Proceeding with upgrade. Please do not interrupt.
If the upgrade is interrupted or fails, boot into maintenance image again and restart
upgrade.

Creating IDS application image file...
```

```
Initializing the hard disk...
Applying the image, this process may take several minutes...
Performing post install, please wait...
Application image upgrade complete. You can boot the image now.
guest@idsm3.localdomain#
```

ステップ 14　アップグレード ログを表示します。

```
guest@idsm3.localdomain# show log upgrade

Upgrading the line card on Fri Mar 11 21:21:53 UTC 2005
Downloaded upgrade image
ftp://jsmith@10.89.146.114//RELEASES/Latest/7.0-1/WS-SVC-IDSM2-K9-sys-1.1-a-7.0-1-E4.bin.g
z
Extracted the downloaded file
Proceeding with image upgrade.
Fri Mar 11 21:22:06 2005 : argv1 = 0, argv2 = 0, argv3 = 3, argv4 = 1
Fri Mar 11 21:22:06 2005 : Creating IDS application image file...
Fri Mar 11 21:22:06 2005 : footer: XXXXXXXXXXXXXXXX
Fri Mar 11 21:22:06 2005 : exeoff: 0000000000031729
Fri Mar 11 21:22:06 2005 : image: 0000000029323770
Fri Mar 11 21:22:06 2005 : T: 29323818, E: 31729, I: 29323770
Fri Mar 11 21:22:07 2005 : partition: /dev/hdc1
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Image: /tmp/cdisk.gz
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Device: /dev/hdc1
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Install type: 1
Fri Mar 11 21:22:07 2005 : Initializing the hard disk...
Fri Mar 11 21:22:07 2005 : Required disk size: 524288 Kb (blocks)
Fri Mar 11 21:22:07 2005 : Available disk size: 19535040 Kb (blocks)
Fri Mar 11 21:22:13 2005 : Partitions created on '/dev/hdc'.
Fri Mar 11 21:22:13 2005 : Device '/dev/hdc' verified for OK.
Fri Mar 11 21:22:19 2005 : Created ext2 fileSystem on '/dev/hdc1'.
Fri Mar 11 21:22:19 2005 : Directory '/mnt/hd/' created.
Fri Mar 11 21:22:19 2005 : Partition '/dev/hdc1' mounted.
Fri Mar 11 21:22:19 2005 : Finished initializing the hard disk.
Fri Mar 11 21:22:19 2005 : Applying the image, this process may take several minutes...
Fri Mar 11 21:22:19 2005 : Directory changed to '/mnt/hd'.
Fri Mar 11 21:22:20 2005 : Performing post install, please wait...
Fri Mar 11 21:22:20 2005 : File /mnt/hd/post-install copied to /tmp/post-install.
Fri Mar 11 21:22:20 2005 : Directory changed to '/tmp'.
Fri Mar 11 21:22:28 2005 : Partition '/dev/hdc1' unmounted.
Fri Mar 11 21:22:28 2005 : Directory changed to '/tmp'.
Application image upgrade complete. You can boot the image now.
Partition upgraded successfully
guest@idsm2.localdomain#
```

ステップ 15　アップグレード ログをクリアします。

```
guest@idsm2.localdomain# clear log upgrade
Cleared log file successfully
```

ステップ 16　アップグレード ログを表示します。

```
guest@idsm2.localdomain# show log upgrade
guest@idsm2.localdomain#
```

ステップ 17　別のコンピュータに対して ping を実行します。

```
guest@idsm2.localdomain# ping 10.89.146.114
PING 10.89.146.114 (10.89.146.114) from 10.89.149.74 : 56(84) bytes of data.
64 bytes from 10.89.146.114: icmp_seq=0 ttl=254 time=381 usec
64 bytes from 10.89.146.114: icmp_seq=1 ttl=254 time=133 usec
64 bytes from 10.89.146.114: icmp_seq=2 ttl=254 time=129 usec
64 bytes from 10.89.146.114: icmp_seq=3 ttl=254 time=141 usec
```

```
64 bytes from 10.89.146.114: icmp_seq=4 ttl=254 time=127 usec

--- 10.89.146.114 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0.127/0.182/0.381/0.099 ms
guest@idsm2.localdomain#
```

ステップ 18　IDSM2 をリセットします。

（注）　メンテナンス パーティションから **reset** コマンドを発行するときにパーティションを指定することはできません。IDSM2 は、ブート デバイス変数で指定されたパーティションにブートされます。ブート デバイス変数が設定されていない場合、IDSM2 はアプリケーション パーティションにブートされます。

```
guest@idsm2.localdomain# reset
guest@idsm2.localdomain#
2005 Mar 11 21:55:46 CST -06:00 %SYS-4-MOD_SHUTDOWNSTART:Module 9 shutdown in progress. Do
not remove module until shutdown completes

Broadcast message from root Fri Mar 11 21:55:47 2005...

The system is going down for system halt NOW !!
console> (enable)#
```

詳細情報

サポートされる FTP サーバおよび HTTP/HTTPS サーバのリストについては、「サポートされる FTP サーバおよび HTTP/HTTPS サーバ」（P.25-2）を参照してください。

Cisco IOS ソフトウェアの IDSM2 メンテナンス パーティションの設定

IDSM2 メンテナンス パーティションを設定するには、次の手順を実行します。

ステップ 1　スイッチの CLI にログインします。

ステップ 2　IDSM2 との間にセッションを確立します。

```
router# session slot 11 processor 1
The default escape character is Ctrl-^, then x.
You can also type 'exit' at the remote prompt to end the session
Trying 127.0.0.111 ... Open

Cisco Maintenance image
```

（注）　IDSM2 メンテナンス パーティションに Telnet または SSH で接続することはできません。IDSM2 とのセッションはスイッチ CLI から確立する必要があります。

ステップ 3　ユーザ **guest** とパスワード **cisco** でログインします。

（注）　ゲスト パスワードの変更は可能ですが、推奨できません。メンテナンス パーティションのゲスト パスワードを忘れ、何らかの理由で IDSM2 アプリケーション パーティションにログインできない場合は、IDSM2 の RMA が必要です。

```
login: guest
password: cisco

Maintenance image version: 2.1(2)

guest@idsm2.localdomain#
```

ステップ 4　メンテナンス パーティションのホスト設定を表示します。

```
guest@idsm2.localdomain# show ip

IP address      : 10.89.149.74
Subnet Mask     : 255.255.255.128
IP Broadcast    : 10.255.255.255
DNS Name        : idsm2.localdomain
Default Gateway : 10.89.149.126
Nameserver(s)   :

guest@idsm2.localdomain#
```

ステップ 5　メンテナンス パーティションのホスト設定（IP アドレス、ゲートウェイ、ホスト名）をクリアします。

```
guest@idsm2.localdomain# clear ip
guest@localhost.localdomain# show ip

IP address      : 0.0.0.0
Subnet Mask     : 0.0.0.0
IP Broadcast    : 0.0.0.0
DNS Name        : localhost.localdomain
Default Gateway : 0.0.0.0
Nameserver(s)   :

guest@localhost.localdomain#
```

ステップ 6　メンテナンス パーティションのホスト設定を指定します。

a.　IP アドレスを指定します。

```
guest@localhost.localdomain# ip address ip_address netmask
```

b.　デフォルト ゲートウェイを指定します。

```
guest@localhost.localdomain# ip gateway gateway_ip_address
```

c.　ホスト名を指定します。

```
guest@localhost.localdomain# ip host hostname
```

ステップ 7　メンテナンス パーティションのホスト設定を表示します。

```
guest@idsm2.localdomain# show ip

IP address      : 10.89.149.74
Subnet Mask     : 255.255.255.128
IP Broadcast    : 10.255.255.255
DNS Name        : idsm2.localdomain
Default Gateway : 10.89.149.126
Nameserver(s)   :

guest@idsm2.localdomain#
```

ステップ 8　アプリケーション パーティションにインストールされているイメージを確認します。

```
guest@idsm2.localdomain# show images
Device name             Partition#              Image name
-----------             ----------              ----------
```

```
Hard disk(hdd)          1                       7.0(1)
guest@idsm2.localdomain
#
```

ステップ 9　メンテナンス パーティションのバージョン（BIOS バージョンを含む）を確認します。

```
guest@idsm2.localdomain# show version

Maintenance image version: 2.1(2)
mp.2-1-2.bin : Thu Nov 18 11:41:36 PST 2004 :
integ@kplus-build-lx.cisco.com

Line Card Number :WS-SVC-IDSM2-XL
Number of Pentium-class Processors : 2
BIOS Vendor: Phoenix Technologies Ltd.
BIOS Version: 4.0-Rel 6.0.9

Total available memory: 2012 MB
Size of compact flash: 61 MB
Size of hard disk: 19077 MB
Daughter Card Info: Falcon rev 3, FW ver 2.0.3.0 (IDS), SRAM  8 MB, SDRAM  256 MB

guest@idsm2.localdomain#
```

ステップ 10　アプリケーション パーティションをアップグレードします。

```
guest@idsm2.localdomain# upgrade
ftp://jsmith@10.89.146.11//RELEASES/Latest/7.0-1/IPS-IDSM2-K9-sys-1.1-a-7.0-1-E4.img
Downloading the image. This may take several minutes...
Password for jsmith@10.89.146.114:
500 'SIZE IPS-IDSM2-K9-sys-1.1-a-6.2-1.bin.gz': command not understood.

ftp://jsmith@10.89.146.11//RELEASES/Latest/7.0-1/IPS-IDSM2-K9-sys-1.1-a-7.0-1-E4.img
(unknown size)
/tmp/upgrade.gz            [|]   28616K
29303086 bytes transferred in 5.34 sec (5359.02k/sec)

Upgrade file
ftp://jsmith@10.89.146.114//RELEASES/Latest/7.0-1/IPS-IDSM2-K9-sys-1.1-a-7.0-1-E4.img is
downloaded.
Upgrading will wipe out the contents on the storage media.
Do you want to proceed installing it [y|N]:
```

ステップ 11　**y** と入力してアップグレードを続行します。

```
Proceeding with upgrade. Please do not interrupt.
If the upgrade is interrupted or fails, boot into maintenance image again and restart
upgrade.

Creating IDS application image file...

Initializing the hard disk...
Applying the image, this process may take several minutes...
Performing post install, please wait...
Application image upgrade complete. You can boot the image now.
guest@idsm3.localdomain#
```

ステップ 12　アップグレード ログを表示します。

```
guest@idsm3.localdomain# show log upgrade

Upgrading the line card on Fri Mar 11 21:21:53 UTC 2005
Downloaded upgrade image
ftp://jsmith@10.89.146.114//RELEASES/Latest/7.0-1/IPS-IDSM2-K9-sys-1.1-a-7.0-1-E4.img
Extracted the downloaded file
```

```
Proceeding with image upgrade.
Fri Mar 11 21:22:06 2005 : argv1 = 0, argv2 = 0, argv3 = 3, argv4 = 1
Fri Mar 11 21:22:06 2005 : Creating IDS application image file...
Fri Mar 11 21:22:06 2005 : footer: XXXXXXXXXXXXXXXX
Fri Mar 11 21:22:06 2005 : exeoff: 0000000000031729
Fri Mar 11 21:22:06 2005 : image: 0000000029323770
Fri Mar 11 21:22:06 2005 : T: 29323818, E: 31729, I: 29323770
Fri Mar 11 21:22:07 2005 : partition: /dev/hdc1
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Image: /tmp/cdisk.gz
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Device: /dev/hdc1
Fri Mar 11 21:22:07 2005 : startIDSAppUpgrade:Install type: 1
Fri Mar 11 21:22:07 2005 : Initializing the hard disk...
Fri Mar 11 21:22:07 2005 : Required disk size: 524288 Kb (blocks)
Fri Mar 11 21:22:07 2005 : Available disk size: 19535040 Kb (blocks)
Fri Mar 11 21:22:13 2005 : Partitions created on '/dev/hdc'.
Fri Mar 11 21:22:13 2005 : Device '/dev/hdc' verified for OK.
Fri Mar 11 21:22:19 2005 : Created ext2 fileSystem on '/dev/hdc1'.
Fri Mar 11 21:22:19 2005 : Directory '/mnt/hd/' created.
Fri Mar 11 21:22:19 2005 : Partition '/dev/hdc1' mounted.
Fri Mar 11 21:22:19 2005 : Finished initializing the hard disk.
Fri Mar 11 21:22:19 2005 : Applying the image, this process may take several minutes...
Fri Mar 11 21:22:19 2005 : Directory changed to '/mnt/hd'.
Fri Mar 11 21:22:20 2005 : Performing post install, please wait...
Fri Mar 11 21:22:20 2005 : File /mnt/hd/post-install copied to /tmp/post-install.
Fri Mar 11 21:22:20 2005 : Directory changed to '/tmp'.
Fri Mar 11 21:22:28 2005 : Partition '/dev/hdc1' unmounted.
Fri Mar 11 21:22:28 2005 : Directory changed to '/tmp'.
Application image upgrade complete. You can boot the image now.
Partition upgraded successfully
guest@idsm2.localdomain#
```

ステップ 13　アップグレード ログをクリアします。

```
guest@idsm2.localdomain# clear log upgrade
Cleared log file successfully
```

ステップ 14　アップグレード ログを表示します。

```
guest@idsm2.localdomain# show log upgrade
guest@idsm2.localdomain#
```

ステップ 15　別のコンピュータに対して ping を実行します。

```
guest@idsm2.localdomain# ping 10.89.146.114
PING 10.89.146.114 (10.89.146.114) from 10.89.149.74 : 56(84) bytes of data.
64 bytes from 10.89.146.114: icmp_seq=0 ttl=254 time=381 usec
64 bytes from 10.89.146.114: icmp_seq=1 ttl=254 time=133 usec
64 bytes from 10.89.146.114: icmp_seq=2 ttl=254 time=129 usec
64 bytes from 10.89.146.114: icmp_seq=3 ttl=254 time=141 usec
64 bytes from 10.89.146.114: icmp_seq=4 ttl=254 time=127 usec

--- 10.89.146.114 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max/mdev = 0.127/0.182/0.381/0.099 ms
guest@idsm2.localdomain#
```

ステップ 16　IDSM2 をリセットします。

（注）　メンテナンス パーティションから **reset** コマンドを発行するときにパーティションを指定することはできません。IDSM2 は、ブート デバイス変数で指定されたパーティションにブートされます。ブート デバイス変数が設定されていない場合、IDSM2 はアプリケーション パーティションにブートされます。

```
guest@idsm2.localdomain# reset
guest@idsm2.localdomain#
Broadcast message from root Fri Mar 11 22:04:53 2005...

The system is going down for system halt NOW !!

[Connection to 127.0.0.111 closed by foreign host]
router#
```

詳細情報

サポートされる FTP サーバおよび HTTP/HTTPS サーバのリストについては、「サポートされる FTP サーバおよび HTTP/HTTPS サーバ」（P.25-2）を参照してください。

Catalyst ソフトウェアの IDSM2 メンテナンス パーティションのアップグレード

メンテナンス パーティションをアップグレードするには、次の手順を実行します。

ステップ 1　IDSM2 メンテナンス パーティション ファイル（c6svc-mp.2-1-2.bin.gz）を IDSM2 からアクセスできる FTP サーバの FTP ルート ディレクトリにダウンロードします。

ステップ 2　スイッチから IDSM2 との間にセッションを確立します。

```
console>(enable) session slot_number
```

ステップ 3　IDSM2 の CLI にログインします。

ステップ 4　コンフィギュレーション モードを開始します。

```
idsm2# configure terminal
```

ステップ 5　メンテナンス パーティションをアップグレードします。

```
idsm2(config)# upgrade
ftp://user@ftp_server_IP_address/directory_path/c6svc-mp.2-1-2.bin.gz
```

続行するかどうか尋ねられます。

ステップ 6　FTP サーバのパスワードを入力します。

ステップ 7　**y** と入力して続行します。

メンテナンス パーティション ファイルがアップグレードされます。

詳細情報

- サポートされる FTP サーバおよび HTTP/HTTPS サーバのリストについては、「サポートされる FTP サーバおよび HTTP/HTTPS サーバ」（P.25-2）を参照してください。
- Cisco.com でソフトウェアを検索する手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。

Cisco IOS ソフトウェアの IDSM2 メンテナンス パーティションのアップグレード

メンテナンス パーティションをアップグレードするには、次の手順を実行します。

ステップ 1　IDSM2 メンテナンス パーティション ファイル（c6svc-mp.2-1-2.bin.gz）を IDSM2 からアクセスできる FTP サーバの FTP ルート ディレクトリにダウンロードします。

ステップ 2　スイッチの CLI にログインします。

ステップ 3　アプリケーション パーティション CLI との間にセッションを確立します。

```
router# session slot slot_number processor 1
```

ステップ 4　IDSM2 にログインします。

ステップ 5　コンフィギュレーション モードを開始します。

```
idsm2# configure terminal
```

ステップ 6　メンテナンス パーティションをアップグレードします。

```
idsm2(config)# upgrade
ftp://user@ftp_server_IP_address/directory_path/c6svc-mp.2-1-2.bin.gz
```

ステップ 7　FTP サーバのパスワードを指定します。

```
Password: ********
```

続行するかどうかの確認を求められます。

```
Continue with upgrade?:
```

ステップ 8　**yes** と入力して続行します。

詳細情報

- サポートされる FTP サーバおよび HTTP/HTTPS サーバのリストについては、「サポートされる FTP サーバおよび HTTP/HTTPS サーバ」（P.25-2）を参照してください。
- Cisco.com でソフトウェアを検索する手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。

IPS SSP システム イメージのインストール

注意　システム イメージをインストールすると、すべてのユーザ設定が失われます。システム イメージのインストールによるセンサーの復旧を試みる前に、**recover application-partition** コマンドを使用するか、またはセンサーの起動時にリカバリ パーティションを選択する方法による復旧を試みてください。

ここでは、**hw-module** コマンドまたは ROMMON を使用して IPS SSP システム イメージをインストールする方法について説明します。内容は次のとおりです。

- 「hw-module コマンドを使用したシステム イメージのインストール」（P.25-42）
- 「ROMMON を使用したシステム イメージのインストール」（P.25-44）

hw-module コマンドを使用したシステム イメージのインストール

システム イメージをインストールするには、適応型セキュリティ アプライアンス CLI を使用して TFTP サーバから IPS SSP へソフトウェア イメージを転送します。適応型セキュリティ アプライアンスは、IPS SSP の ROMMON アプリケーションとの通信によってイメージを転送できます。

（注） 指定する TFTP サーバが、最大 60 MB のサイズのファイルを転送できることを確認してください。

（注） ネットワークとイメージのサイズに応じて、このプロセスは完了までに約 15 分間かかることがあります。

IPS SSP ソフトウェア イメージをインストールするには、次の手順を実行します。

ステップ 1　適応型セキュリティ アプライアンスにログインします。

ステップ 2　イネーブル モードを開始します。

```
asa# enable
```

ステップ 3　IPS SSP のリカバリ設定を指定します。

```
asa (enable)# hw-module module 1 recover configure
```

（注） リカバリ設定に誤りがあった場合は、**hw-module module 1 recover stop** コマンドを使用してシステム イメージの再作成を停止してから、設定を修正できます。

ステップ 4　ソフトウェア イメージの TFTP URL を指定します。

```
Image URL [tftp://0.0.0.0/]:
```

例

```
Image URL [tftp://0.0.0.0/]: tftp://10.89.146.1/IPS-SSP_10-K9-sys-1.1-a-7.1-1-E4.img
```

ステップ 5　IPS SSP のコマンド/コントロール インターフェイスを指定します。

（注） ポート IP アドレスは、IPS SSP の管理 IP アドレスです。

```
Port IP Address [0.0.0.0]:
```

例

```
Port IP Address [0.0.0.0]: 10.89.149.231
```

ステップ 6　VLAN ID を 0 のままにします。

```
VLAN ID [0]:
```

ステップ 7　IPS SSP のデフォルト ゲートウェイを指定します。

```
Gateway IP Address [0.0.0.0]:
```

例

```
Gateway IP Address [0.0.0.0]: 10.89.149.254
```

ステップ 8　リカバリを実行します。

```
asa# hw-module module 1 recover boot
```

ソフトウェア イメージが TFTP サーバから IPS SSP に転送され、IPS SSP が再起動されます。

ステップ 9　完了するまでリカバリを定期的にチェックします。

（注）　ステータスは、リカバリ中は [Recovery] となり、インストールが完了すると [Up] になります。

```
asa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5585-X IPS Security Services Processor-10 with 8GE
Model:              ASA5585-SSP-IPS10
Hardware version:   1.0
Serial Number:      JAF1350ABSL
Firmware version:   2.0(1)3
Software version:   7.1(0.326)E4
MAC Address Range:  8843.e12f.5414 to 8843.e12f.541f
App. name:          IPS
App. Status:        Up
App. Status Desc:   Normal Operation
App. version:       7.1(1)E4
Data plane Status:  Up
Status:             Up
Mgmt IP addr:       10.89.148.11
Mgmt Network mask:  255.255.255.0
Mgmt Gateway:       10.89.148.254
Mgmt Access List:   10.0.0.0/8
Mgmt Access List:   64.0.0.0/8
Mgmt web ports:     443
Mgmt TLS enabled    true
asa#
```

（注）　出力の [Status] フィールドは IPS SSP の動作ステータスを示します。IPS SSP の動作ステータスは、通常は [Up] となります。適応型セキュリティ アプライアンスが IPS SSP にソフトウェア イメージを転送している間は、出力の [Status] フィールドは [Recover] となります。適応型セキュリティ アプライアンスによるイメージの転送が完了し、IPS SSP が再起動されると、新たに転送されたイメージが実行されます。

（注）　このプロセス中にエラーが発生した場合、デバッグを実行するには、**debug module-boot** コマンドを使用して、ソフトウェア インストール プロセスのデバッグをイネーブルにします。

ステップ 10　IPS SSP との間にセッションを確立します。

ステップ 11　**cisco** を 3 回入力し、新しいパスワードを 2 回入力します。

ステップ 12　**setup** コマンドを使用して IPS SSP を初期化します。

詳細情報

- アプリケーション パーティションを復旧する手順については、「アプリケーション パーティションの復旧」（P.25-12）を参照してください。
- Cisco.com でソフトウェアを検索する手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。

ROMMON を使用したシステム イメージのインストール

適応型セキュリティ アプライアンスで ROMMON を使用してシステム イメージを IPS SSP に TFTP 転送することにより、IPS SSP システム イメージをインストールできます。

IPS SSP システム イメージをインストールするには、次の手順を実行します。

ステップ 1　IPS SSP システム イメージ ファイル（IPS-SSP_10-K9-sys-1.1-a-7.1-1-E4.img など）を適応型セキュリティ アプライアンスからアクセスできる TFTP サーバの tftp ルート ディレクトリにダウンロードします。

（注）　適応型セキュリティ アプライアンスのイーサネット ポートに接続されているネットワークから TFTP サーバの場所にアクセスできることを確認します。

ステップ 2　IPS SSP をブートします。

```
Booting system, please wait...

CISCO SYSTEMS
Embedded BIOS Version 0.0(2)10 11:16:38 04/15/10
Com KbdBuf SMM UsbHid Msg0 Prompt Pmrt Cache1 LowM ExtM HugeM Cache2 Flg Siz0 Amrt PMM
PnpDsp Smbios Lpt0 Npx1 Apm Lp1 Acpi Typ Dbg Enb Mp MemReduce MemSync1 CallRoms MemSync2
DriveInit


Total memory : 12 GB
Total number of CPU cores : 8
Com Lp1 Admgr2 Brd10 Plx2 OEM0=7EFF5C74
Cisco Systems ROMMON Version (1.0(12)10) #0: Thu Apr  8 00:12:33 CDT 2010

Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.

Management0/0
Link is UP
MAC Address: 5475.d029.7fa9
```

ステップ 3　システムの起動中に、次のプロンプトで Break または Esc を押して、ブートを中断します。ブートを即座に開始するには、スペースバーを押します。

（注）　Break または Esc は 10 秒以内に押してください。

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
```

システムが ROMMON モードに入ります。`rommon>` プロンプトが表示されます。

ステップ 4　現在のネットワーク設定を確認します。

```
rommon #0> set
ROMMON Variable Settings:
  ADDRESS=0.0.0.0
  SERVER=0.0.0.0
  GATEWAY=0.0.0.0
  PORT=Management0/0
  VLAN=untagged
  IMAGE=
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20
```

変数の定義は次のとおりです。

- Address：IPS SSP のローカル IP アドレス
- Server：アプリケーション イメージが格納されている TFTP サーバの IP アドレス
- Gateway：IPS SSP が使用するゲートウェイの IP アドレス
- Port：IPS SSP の管理に使用されるイーサネット インターフェイス
- VLAN：VLAN ID 番号（タグなしのまま）
- Image：システム イメージ ファイル パスとファイル名
- Config：これらのプラットフォームでは未使用

（注） ネットワーク接続を確立するために、すべての値が必要なわけではありません。address、server、gateway、および image の値は必要です。ローカル環境を設定するために必要な設定がわからない場合は、システム管理者に連絡してください。

ステップ 5　必要に応じて、TFTP ダウンロードに使用するインターフェイスを変更します。

（注） TFTP ダウンロードに使用されるデフォルトのインターフェイスは Management0/0 です。これは、IPS SSP の管理インターフェイスに対応します。

```
rommon> PORT=interface_name
```

ステップ 6　必要に応じて、IPS SSP 上のローカル ポートの IP アドレスを割り当てます。

```
rommon> ADDRESS=ip_address
```

（注） IPS SSP に割り当てられているものと同じ IP アドレスを使用します。

ステップ 7　必要に応じて、TFTP サーバの IP アドレスを割り当てます。

```
rommon> SERVER=ip_address
```

ステップ 8　必要に応じて、ゲートウェイの IP アドレスを割り当てます。

```
rommon> GATEWAY=ip_address
```

ステップ 9　次のいずれかのコマンドを使用して、ローカル イーサネット ポートから ping を実行することにより、TFTP サーバにアクセスできることを確認します。

```
rommon> ping server_ip_address
rommon> ping server
```

ステップ 10　必要に応じて、イメージのダウンロード元である TFTP ファイル サーバ上のパスおよびファイル名を定義します。

```
rommon> IMAGE=path/file_name
```

注意　**IMAGE** コマンドは、必ずすべて大文字で入力してください。他の ROMMON コマンドは小文字と大文字のどちらでも入力できますが、**IMAGE** コマンドはすべて大文字で入力する必要があります。

UNIX の例

```
rommon> IMAGE=/system_images/IPS-SSP_10-K9-sys-1.1-a-7.1-1-E4.img
```

（注）　このパスは、UNIX TFTP サーバのデフォルト tftpboot ディレクトリからの相対パスです。デフォルトの tftpboot ディレクトリに置かれているイメージの IMAGE 指定には、ディレクトリ名もスラッシュも含まれていません。

Windows の例

```
rommon> IMAGE=¥system_images¥IPS-SSP_10-K9-sys-1.1-a-7.1-1-E4.img
```

ステップ 11　**set** と入力し、Enter を押して、ネットワーク設定を確認します。

（注）　**sync** コマンドを使用すると、これらの設定をブート後も維持されるように NVRAM に保存できます。保存しない場合は、ROMMON からイメージをブートするときに毎回この情報を入力する必要があります。

ステップ 12　システム イメージをダウンロードしてインストールします。

```
rommon> tftp
```

注意　システム イメージの破損を避けるために、システム イメージのインストール中は IPS SSP の電源を切らないでください。

（注）　ネットワーク設定が正しい場合、指定したイメージが IPS SSP にダウンロードされ、ブートされます。必ず IPS SSP イメージを使用してください。

詳細情報

- IPS SSP アプリケーション パーティションを復旧する手順については、「アプリケーション パーティションの復旧」（P.25-12）を参照してください。
- Cisco.com でソフトウェアを検索する手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。

NME IPS システム イメージのインストール

（注）　NME IPS スロット番号を確認するには、**show configuration | include interface ids-sensor** コマンドを使用します。

NME IPS システム イメージをインストールするには、次の手順を実行します。

ステップ 1　NME IPS システム イメージ ファイル（IPS-NME-K9-sys-1.1-7.0-1-E4.img）をダウンロードし、TFTP サーバの tftp ルート ディレクトリに配置します。

（注）　NME IPS が TFTP サーバにアクセスできるようにネットワークが設定されていることを確認します。

利用可能な TFTP サーバがない場合は、ルータを TFTP サーバとして設定できます。

```
router# copy tftp: flash:
router# configure terminal
router(config)# tftp-server flash:IPS-NME-K9-sys-1.1-7.0-1-E4img
router(config)# exit
router#
```

ステップ 2　ハートビートのリセットをディセーブルにします。

```
router# service-module ids-sensor 1/0 heartbeat-reset disable
```

（注）　ハートビートのリセットをディセーブルにすると、システム イメージのインストール プロセスに時間がかかりすぎる場合でも、モジュールがリセットされなくなります。

ステップ 3　NME IPS との間にセッションを確立します。

```
router# service-module ids-sensor 1/0 session
```

ステップ 4　Shift と Ctrl を押した状態で 6 を押してから X を押してセッションを中断します。`router#` プロンプトが表示されます。このプロンプトが表示されない場合は、Ctrl を押した状態で 6 を押してから、X を押してみてください。

ステップ 5　NME IPS をリセットします。**reset** コマンドを確認するように要求されます。

```
router# service-module ids-sensor 1/0 reset
```

ステップ 6　**Enter** キーを押して確認します。

ステップ 7　Enter を押して、中断したセッションを再開します。ブートローダのバージョンが表示された後、次のプロンプトが 15 秒間表示されます。

```
Please enter '***' to change boot configuration:
```

ステップ 8　この 15 秒の間に ******* と入力します。

ブートローダ プロンプトが表示されます。

ステップ 9　Enter を押して NME IPS とのセッションに戻ります。

ステップ 10　ブートローダを設定します。

```
ServicesEngine bootloader> config
```

```
IP Address [10.89.148.195]>
Subnet mask [255.255.255.0]>
TFTP server [10.89.150.74]>
Gateway [10.89.148.254]>
Default boot [disk]>
Number cores [2]>
ServicesEngine boot-loader >
```

各プロンプトで、値を入力するか、Enter を押して角括弧で囲まれた保存済みの値をそのまま適用します。

注意　NME IPS イメージのパス名はフル パスですが、tftp サーバのルート ディレクトリからの相対パスです（通常は、/tftpboot）。

ステップ 11　ブートローダを起動します。

```
ServicesEngine bootloader> upgrade
```

ステップ 12　ブートローダの指示に従ってソフトウェアをインストールします（オプション 1 を選択して、ウィザードの指示に従います）。

例

```
Booting from flash...please wait.
Please enter '***' to change boot configuration:
12 ***
ServicesEngine boot-loader Version : 1.2.0
ServicesEngine boot-loader > config

IP Address [10.89.148.195]>
Subnet mask [255.255.255.0]>
TFTP server [10.89.150.74]>
Gateway [10.89.148.254]>
Default boot [disk]>
Number cores [2]>
ServicesEngine boot-loader > upgrade

Cisco Systems, Inc.
Services engine upgrade utility for NM-IPS
-----
Main menu
1 - Download application image and write to USB Drive
2 - Download bootloader and write to flash
3 - Download minikernel and write to flash
r - Exit and reset card
x - Exit
Selection [123rx]
Download recovery image via tftp and install on USB Drive
TFTP server [10.89.150.74]>
full pathname of recovery image
[]:test/sensor/7.1-1-E4/IPS-NME-K9-sys-1.1-a-7.1-1-E4.img
Ready to begin
Are you sure [Y/N]
Press <CTRL-C> to abort.
octeth0:        Up     1Gbs Full duplex, (port 0)
octeth1:        Up     1Gbs Full duplex, (port 1)
Using octeth0 device
TFTP from server 10.89.150.74; our IP address is 10.89.148.195; sending through gateway
10.89.148.254
Filename 'test/sensor/7.1-1-E4/IPS-NME-K9-sys-1.1-a-7.1-1-E4.img'.
Load address: 0x21000000
Loading: octeth0: Down   1Gbs Half duplex, (port 0)
```

```
octeth0: Down   1Gbs Full duplex, (port 0)
octeth0: Up     1Gbs Full duplex, (port 0)
T T T T T T T T T ##################################################################
          ##################################################################
          ##################################################################
          ##################################################################
          ##################################################################
          ##################################################################
          ##################################################################
          ##################################################################
          ##################################################################
          ##################################################################
          ######
          32 MB received
          ##################################################################
          ##################################################################
          ###################
done
```

ステップ 13　Shift と Ctrl を押した状態で 6 を押してから X を押してセッションを中断します。`router#` プロンプトが表示されます。このプロンプトが表示されない場合は、Ctrl を押した状態で 6 を押してから、X を押してみてください。

ステップ 14　ルータの CLI 側で、セッションをクリアします。

```
router# service-module interface ids-sensor 1/0 session clear
```

ステップ 15　ハートビートのリセットをイネーブルにします。

```
router# service-module IDS-sensor 1/0 heartbeat-reset enable
```

詳細情報

- TFTP サーバの詳細については、「TFTP サーバ」（P.25-14）を参照してください。
- アンナンバード IP アドレスを設定する手順については、「Setting Up Interfaces on NME IPS and the Router」を参照してください。
- Cisco.com でソフトウェアを検索する手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。

APPENDIX A

システム アーキテクチャの概要

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

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

この付録では、Cisco IPS システム アーキテクチャについて説明します。内容は次のとおりです。

Cisco IPS の目的

Cisco IPS の目的は、悪意のあるネットワーク アクティビティを検出および防止することです。Cisco IPS ソフトウェアは、アプライアンスとモジュールの 2 つのプラットフォームにインストールできます。Cisco IPS には、管理アプリケーションとモニタリング アプリケーションが含まれています。IDM は IPS の管理およびモニタに使用できるネットワーク管理 JAVA アプリケーションです。IME は IPS イベントの表示に使用できる IPS ネットワーク モニタリング JAVA アプリケーションです。IME には、IDM コンフィギュレーション コンポーネントも含まれます。IDM と IME は、コンピュータでホストされる HTTP または HTTPS を使用して IPS と通信します。

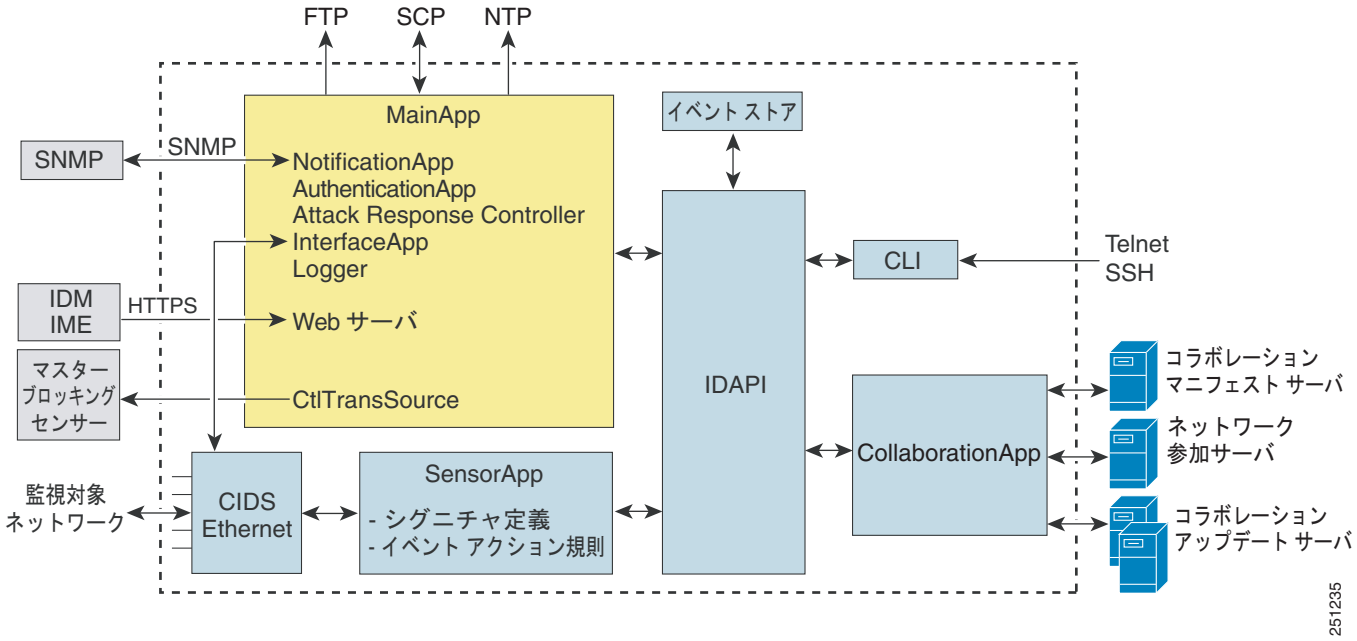
システム設計

（注）　AIP SSC-5 は、グローバル相関機能をサポートしていません。

Cisco IPS ソフトウェアは、Linux オペレーティング システム上で動作します。Linux OS を強化するために、不要なパッケージの削除、使用しないサービスの無効化、ネットワーク アクセスの制限、およびシェルへのアクセスの停止を行いました。

図 A-1 に、IPS ソフトウェアのシステム設計を示します。

図 A-1　システム設計



詳細情報

- MainApp の詳細については、「MainApp」（P.A-5）を参照してください。
- SensorApp の詳細については、「SensorApp」（P.A-22）を参照してください。
- CollaborationApp の詳細については、「CollaborationApp」（P.A-28）を参照してください。
- CLI の詳細については、「CLI」（P.A-30）を参照してください。

システム アプリケーション

（注）　各アプリケーションには、それぞれ独自の XML 形式の構成ファイルがあります。

Cisco IPS ソフトウェアには、次のアプリケーションが含まれています。

- MainApp：システムの初期化、他のアプリケーションの起動および停止、OS の構成、およびプラットフォームのアップデートを行います。次のコンポーネントが含まれます。
  - CtlTransSource（Control Transaction Server）：センサーによる制御トランザクションの送信を許可します。Attack Response Controller（旧称 Network Access Controller）のマスター ブロッキング センサー機能をイネーブルにするために使用されます。
  - Event Store：IPS イベント（エラー、ステータス、アラートの各システム メッセージ）を格納するために使用され、CLI、IDM、IME、ASDM、または SDEE からアクセスできるインデックス付きストアです。
  - InterfaceApp：バイパスおよび物理設定を処理し、ペアにするインターフェイスを定義します。物理設定は、速度、デュプレックス、および管理状態です。
  - Logger：アプリケーションのすべてのログ メッセージをログ ファイルに書き込み、アプリケーションのエラー メッセージを Event Store に書き込みます。
  - Attack Response Controller（旧称 Network Access Controller）：リモート ネットワーク デバイス（ファイアウォール、ルータ、スイッチ）を管理し、アラート イベントの発生時にブロッキング機能を提供します。ARC は、ACL を作成して制御対象ネットワーク デバイスに適用するか、または、**shun** コマンド（ファイアウォール）を使用します。
  - NotificationApp：アラート、ステータス、およびエラー イベントによってトリガーされたときに SNMP トラップを送信します。NotificationApp は、パブリック ドメイン SNMP エージェントを使用します。SNMP GET は、センサーの全般的な状態に関する情報を提供します。
  - Web Server（HTTP SDEE サーバ）：SDEE プロトコルを使用して、他の IPS デバイスとの Web インターフェイスおよび通信を提供します。IPS サービスの提供には、サーブレットが使用されます。
  - AuthenticationApp：CLI、IDM、IME、ASDM、または SDEE アクションの実行についてユーザが認証されていることを確認します。
- SensorApp（分析エンジン）：パケットのキャプチャと分析を行います。
- CollaborationApp：IDAPI 制御トランザクション、セマフォ、共有メモリ、ファイル交換など、さまざまなプロセス間通信テクノロジーを使用して、MainApp や SensorApp との間に構築されるインターフェイスです。
- CLI：Telnet または SSH を通じてセンサーに正しくログインすると実行されるインターフェイスです。CLI で作成されたすべてのアカウントは、CLI をアカウントのシェルとして使用します（サービス アカウントは例外。許可されるサービス アカウントは 1 つだけです）。使用できる CLI コマンドは、ユーザの権限に依存します。

すべての Cisco IPS アプリケーションは、共通 API（IDAPI）を通じて相互に通信します。リモート アプリケーション（他のセンサー、管理アプリケーション、サードパーティ製ソフトウェア）は、SDEE プロトコルでセンサーと通信します。

センサーには、次のパーティションがあります。

- アプリケーション パーティション：フル IPS システム イメージ。
- メンテナンス パーティション：IDSM2 のアプリケーション パーティションのイメージを再作成するために使用される、特殊な目的の IPS イメージ。メンテナンス パーティションのイメージを再作成すると、すべての設定が失われます。
- リカバリ パーティション：センサーのリカバリに使用される、特殊な目的のイメージ。リカバリ パーティションで起動すると、アプリケーション パーティションを完全に再作成することができます。ネットワーク設定は保存されますが、それ以外のすべての設定は失われます。

ユーザ対話

Cisco IPS とは、次の方法で対話します。

- デバイス パラメータの設定

  システムおよびその機能の初期設定を生成します。これは頻度の低いタスクで、通常は 1 回だけ行います。システムには、必要な変更を最小限にするように、妥当なデフォルト値が設定されています。Cisco IPS の設定は、CLI、IDM、IME、CSM、ASDM を通して、または SDEE を使用する別のアプリケーションから行うことができます。

- 調整

  主にネットワーク トラフィックをモニタするアプリケーションの一部である分析エンジンの設定に、微調整を加えることができます。システムをネットワークに最初にインストールした後、システムが効率的に動作し、有用な情報が生成されるようになるまで、何度でもシステムを調整できます。カスタム シグニチャの作成、機能のイネーブル化、サービス パックまたはシグニチャ アップデートの適用などを行えます。Cisco IPS の調整は、CLI、IDM、IME、CSM、ASDM を通して、または SDEE を使用する別のアプリケーションから行うことができます。

- アップデート

  自動アップデートをスケジュールすることも、アプリケーションおよびシグニチャ データ ファイルに今すぐアップデートを適用するように要求することもできます。Cisco IPS のアップデートは、CLI、IDM、IME、CSM、ASDM を通して、または SDEE を使用する別のアプリケーションから行うことができます。

- 情報の取得

  CLI、IDM、IME、CSM、ASDM、CS MARS 経由でシステムから、または SDEE を使用する別のアプリケーションから、データ（ステータス メッセージ、エラー、アラート）を取得できます。

セキュリティ機能

Cisco IPS には、次のセキュリティ機能を搭載しています。

- ネットワーク アクセスは、特別にアクセスを許可されたホストに制限されます。
- Web Server、SSH と SCP、または Telnet 経由で接続を試みるリモート ホストはすべて認証されます。
- デフォルトでは、Telnet アクセスはディセーブルです。Telnet をイネーブルにするように選択できます。
- デフォルトでは、SSH アクセスはイネーブルです。
- FTP サーバは、センサー上では実行されません。SCP を使用して、リモートでファイルをコピーできます。
- デフォルトでは、Web Server は TLS または SSL を使用します。TLS と SSL をディセーブルにするように選択できます。
- 不要なサービスはディセーブルにされます。
- CISCO-CIDS-MIB 内では、Cisco MIB ポリシングが必要とする SNMP セットのみが許可されます。パブリック ドメイン SNMP エージェントが実装する OID は、MIB によって指定されたときに書き込み可能になります。

MainApp

ここでは MainApp について説明します。内容は次のとおりです。

MainApp について

MainApp には、SensorApp と CLI を除くすべての IPS コンポーネントが含まれます。起動時にオペレーティング システムによってロードされ、SensorApp をロードします。その後、MainApp は次のサブシステム コンポーネントを起動します。

- Authentication
- Logger
- ARC
- Web Server
- Notification（SNMP）
- External Product Interface
- Interface manager
- Event Store
- Health and security monitoring

MainApp の役割

MainApp には、次の役割があります。

- シスコがサポートするハードウェア プラットフォームの検証
- ソフトウェア バージョンと PEP 情報の報告
- IPS コンポーネントの起動、停止、バージョンの報告
- ホスト システムの設定
- システム クロックの管理
- Event Store の管理
- ソフトウェア アップグレードのインストールとアンインストール

（注）　Cisco IPS では、MainApp は Cisco.com からシグニチャとシグニチャ エンジンのアップデートを自動的にダウンロードできます。

- オペレーティング システムのシャットダウンまたはリブート

MainApp は、**show version** コマンドへの応答として次の情報を表示します。

- センサーのビルド バージョン
- MainApp のバージョン
- 実行中の各アプリケーションのバージョン
- インストールされている各アップグレードのバージョンおよびタイムスタンプ
- インストールされている各アップグレードの次のダウングレード バージョン
- プラットフォームのバージョン
- 他のパーティションにあるセンサーのビルドのバージョン

MainApp は、ホストの統計情報の収集、ヘルス状態およびセキュリティのモニタリング ステータスの報告も行います。

Event Store

ここでは、Event Store について説明します。内容は次のとおりです。

Event Store について

各 IPS イベントは、タイムスタンプ、および一意で単純な昇順の ID と共に Event Store に格納されます。このタイムスタンプを主キーとして使用することにより、固定サイズのインデックス化された Event Store にイベントをインデックス付けします。循環式の Event Store が設定済みサイズに達すると、最も古いイベントを上書きして新しいイベントが格納されます。Event Store にアラート イベントを書き込むアプリケーションは SensorApp だけです。ログ、ステータス、エラー イベントは、すべてのアプリケーションが Event Store に書き込みます。

固定サイズのインデックス化された Event Store では、時刻、タイプ、プライオリティ、および限られた数のユーザ定義属性に基づいて、シンプルなイベントのクエリーを実行できます。侵入イベントのそれぞれに low、medium、または high のプライオリティを割り当てると、1 回のイベント クエリーで目的のイベント タイプ、侵入イベントのプライオリティ、および時間範囲のリストを指定できます。

表 A-1 に、いくつかの例を示します。

表 A-1　IPS イベントの例

IPS イベント タイプ	侵入イベントのプライオリティ	開始タイムスタンプ値	停止タイムスタンプ値	意味
status	—	0	最大値	格納されているすべての status イベントを取得します。
error status	—	0	65743	時刻 65743 よりも前に格納されたすべての error および status イベントを取得します。
status	—	65743	最大値	時刻 65743 以降に格納された status イベントを取得します。
intrusion attack response	low	0	最大値	プライオリティが low で格納されているすべての intrusion および network access イベントを取得します。
attack response error status intrusion	medium high	4123000000	4123987256	時刻が 4123000000 から 4123987256 の間に格納された、プライオリティが medium または high の attack response、error、status、および intrusion イベントを取得します。

Event Store のサイズは、センサーが IPS イベント コンシューマに接続されていないときに IPS イベントをバッファリングするのに十分な大きさです。バッファリングが十分であるかどうかは、ユーザの要件と、使用するノードの能力に依存します。循環バッファ内の最も古いイベントは、最新のイベントによって置き換えられます。

イベント データ構造

さまざまな機能ユニットが、次の 7 種類のデータをやり取りします。

- intrusion イベント：SensorApp によって生成されます。intrusion イベントはセンサーが検出します。
- error イベント：ハードウェアまたはソフトウェアの不具合によって発生します。
- status イベント：設定が更新されたなどの、アプリケーションのステータスの変更を報告します。
- control transaction log イベント：センサーが制御トランザクションの結果を記録します。
- network access イベント：ブロック要求などの ARC 向けアクション。
- debug イベント：アプリケーションのステータスの変更に関するきわめて詳細なレポートで、デバッグに使用されます。
- 制御トランザクション データ：制御トランザクションに関連するデータ。たとえば、アプリケーションの診断データ、セッション ログ、およびアプリケーションとやり取りされる設定データ。

これら 7 種類のデータを *IPS データ*と総称します。6 つのイベント タイプ（intrusion、error、status、control transaction log、network access、debug）は特徴が似ており、*IPS イベント*と総称されます。IPS イベントは、IPS を構成する数種類のアプリケーションによって生成され、他の IPS アプリケーションに受信されます。IPS イベントには、次のような特徴があります。

- IDS イベントを生成するように設定されているアプリケーション インスタンスによって、自然発生的に生成されます。特定のイベントを生成するように他のアプリケーション インスタンスから要求されることはありません。
- 特定の宛先はありません。1 つまたは複数のアプリケーションによって格納され、その後、取得されます。

制御トランザクションは、次のタイプの要求に関係します。

- アプリケーション インスタンスの設定データを更新する要求
- アプリケーション インスタンスの診断データの要求
- アプリケーション インスタンスの診断データをリセットする要求
- アプリケーション インスタンスを再起動する要求
- ブロック要求などの ARC 向け要求

制御トランザクションには、次のような特徴があります。

- 常に、1 つの応答を伴う 1 つの要求によって構成されます。

  要求と応答には、任意の量のデータが関連付けられる可能性があります。すべての応答には、少なくとも肯定応答または否定応答が含まれます。
- ポイントツーポイントのトランザクションです。

  制御トランザクションは、1 つのアプリケーション インスタンス（発信側）からもう 1 つのアプリケーション インスタンス（応答側）に送信されます。

IPS データは、XML 形式で XML ドキュメントとして表されます。システムには、ユーザ設定可能なパラメータがいくつかの XML ファイルで格納されます。

IPS イベント

IPS アプリケーションは、ある種のできごとが発生したことを報告するために IPS イベントを生成します。イベントは、SensorApp が生成するアラートやアプリケーションが生成するエラーなどのデータです。イベントは、Event Store というローカル データベースに格納されます。

5 種類のイベントがあります。

- evAlert：ネットワーク アクティビティによってシグニチャがトリガーされたことを報告する alert イベント メッセージ
- evStatus：IPS アプリケーションのステータスとアクションを報告する status イベント メッセージ
- evError：応答アクションの試行中に発生したエラーを報告する error イベント メッセージ
- evLogTransaction：各センサー アプリケーションによって生成された制御トランザクションを報告する log transaction メッセージ
- evShunRqst：ARC がいつ block 要求を発行したかを報告する block 要求メッセージ

status メッセージおよび error メッセージは、CLI、IME、および ASDM を使用して表示できます。

SensorApp および ARC は、応答アクション（TCP リセット、IP ロギングの開始と停止、ブロッキングの開始と停止、トリガー パケット）をステータス メッセージとしてログに記録します。

NotificationApp

NotificationApp は、センサーが SNMP トラップとしてアラートとシステム エラー メッセージを送信することを許可します。Event Store にあるイベントにサブスクライブし、SNMP MIB に変換して、パブリック ドメイン SNMP エージェントを介して宛先に送信します。NotificationApp は、set と get の送信をサポートします。SNMP GET は、センサーのヘルス状態に関する基本的な情報を提供します。

NotificationApp は、スパース モードで evAlert イベントから次の情報を送信します。

- 発信元情報
- イベント ID
- イベントの重大度
- 時刻（UTC および現地時間）
- シグニチャ名
- シグニチャ ID
- サブシグニチャ ID
- 参加者情報
- アラームの特性

NotificationApp は、詳細モードで evAlert イベントから次の情報を送信します。

- 発信元情報
- イベント ID
- イベントの重大度
- 時刻（UTC および現地時間）
- シグニチャ名
- シグニチャ ID
- サブシグニチャ ID
- バージョン
- サマリー
- インターフェイス グループ
- VLAN
- 参加者情報
- アクション
- アラームの特性
- シグニチャ
- IP ログ ID

NotificationApp ユーザが定義したフィルタに基づいて、トラップとして送信する evError イベントを決定します。エラーの重大度（error、fatal、warning）に基づいてフィルタできます。NotificationApp は、evError イベントから次の情報を送信します。

- 発信元情報
- イベント ID
- イベントの重大度

- 時刻（UTC および現地時間）
- エラー メッセージ

NotificationApp は、センサーからの次のような一般的なヘルス状態およびシステム情報の取得（GET）をサポートします。

- パケット損失
- パケット拒否
- 生成されたアラーム
- FRP のフラグメント
- FRP のデータグラム
- 初期接続状態での TCP ストリーム
- 接続確立状態での TCP ストリーム
- 接続終了状態での TCP ストリーム
- システムでの TCP ストリーム
- 再構成のためにキューに格納された TCP パケット
- アクティブなノードの総数
- 両方の IP アドレスと両方のポートをキーとする TCP ノード
- 両方の IP アドレスと両方のポートをキーとする UDP ノード
- 両方の IP アドレスをキーとする IP ノード
- センサー メモリの重大な段階
- インターフェイス ステータス
- コマンドおよび制御パケットの統計情報
- フェールオーバー状態
- システムの動作期間
- CPU 使用率
- システムのメモリ使用率
- PEP

（注） すべての IPS プラットフォームが PEP をサポートするわけではありません。

NotificationApp は次の統計情報を提供します。

- エラー トラップ数
- イベント アクション トラップ数
- SNMP GET 要求の数
- SNMP SET 要求の数

CtlTransSource

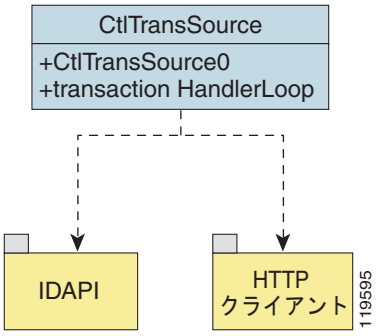
CtlTransSource は、ローカルで開始されたリモート制御トランザクションを HTTP プロトコルを使用してリモートの宛先に転送するアプリケーションです。CtlTransSource は、TLS または非 TLS 接続を開始し、その接続を使用してリモート制御トランザクションを HTTP サーバに伝えます。

CtlTransSource は、リモート HTTP サーバでリモート制御トランザクションを実行するために必要なクレデンシャルを確立する必要があります。CtlTransSource は、リモート ノード上の HTTP サーバにユーザ名 / パスワードの形式で ID を提示することによってクレデンシャルを確立します（基本認証）。認証に成功すると、ユーザ認証を含む Cookie が割り当てられます。この接続に関するすべての要求では、この Cookie を提示する必要があります。

CtlTransSource サーバ内の transactionHandlerLoop メソッドは、リモート制御トランザクションに対するプロキシとして機能します。ローカル アプリケーションがリモート制御トランザクションを起動すると、IDAPI は最初にトランザクションを CtlTransSource に送信します。transactionHandlerLoop メソッドは、CtlTransSource に送信されたリモート制御トランザクションを待機するループです。

図 A-2 に、CtlTransSource 内の transactionHandlerLoop メソッドを示します。

図 A-2　　CtlTransSource



transactionHandlerLoop は、リモート アドレッシングされたトランザクションを受信すると、そのリモート制御トランザクションをリモートの宛先に転送するように試みます。transactionHandlerLoop は、トランザクションを RDEP 制御トランザクション メッセージの形式にします。transactionHandlerLoop は、HttpClient クラスを使用して、リモート ノード上の HTTP サーバに対する制御トランザクション要求を発行します。リモート HTTP サーバは、リモート制御トランザクションを処理し、適切な応答メッセージを HTTP 応答として返します。リモート HTTP サーバが IPS Web サーバである場合、Web サーバは CtlTransSource サーブレットを使用してリモート制御トランザクションを処理します。

transactionHandlerLoop は、リモート制御トランザクションの発信側に対する制御トランザクションの応答として、応答または失敗応答を返します。HTTP サーバが非認証ステータス応答（HTTP クライアントが HTTP サーバに対する十分なクレデンシャルを持っていないことを示す）を返す場合、transactionHandlerLoop は CtlTransSource 専用のユーザ名とパスワードを使用してリクエスタの ID を認証して、トランザクション要求を再発行します。transactionHandlerLoop は、終了を指示する制御トランザクションを受信するか終了イベントが発生するまでループします。

Attack Response Controller

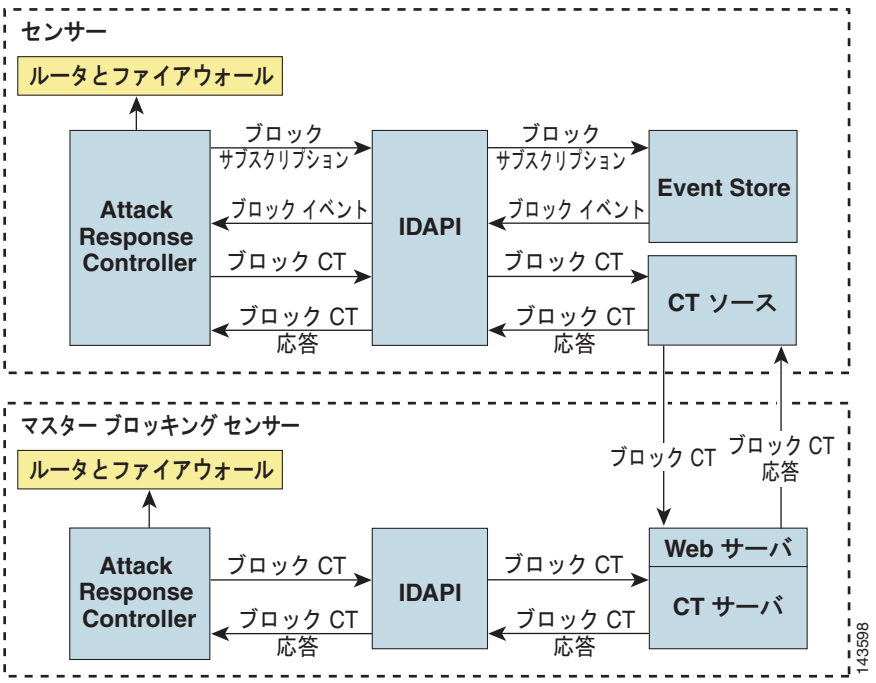
ここでは ARC について説明します。内容は次のとおりです。

ARC について

ARC の主な役割は、イベントをブロックすることです。NAC アプリケーションはブロックに対応するとき、管理対象のデバイスと直接対話してブロックを有効化するか、Control Transaction Server を通じてマスター ブロッキング センサーにブロック要求を送信します。マスター ブロッキング センサー上の Web Server は、制御トランザクションを受け取るとそれを Control Transaction Server に渡し、Control Transaction Server は ARC に渡します。次に、マスター ブロッキング センサー上の ARC は、管理対象のデバイスと対話してブロックを有効化します。

図 A-3 は ARC を図示したものです。

図 A-3　　ARC



（注） ARC のインスタンスは、ネットワーク デバイスを制御できない場合、1 つだけ制御できる場合、多数を制御できる場合があります。ARC は、他の ARC アプリケーション、IPS 管理ソフトウェア、他のネットワーク管理ソフトウェア、システム管理者との間でネットワーク デバイスの制御を一切共有しません。1 つのセンサーについて実行できる ARC アプリケーションのインスタンスは 1 つだけです。

ARC は、次のいずれかに対応してブロックを開始します。

- ブロック アクションが設定されたシグニチャから生成された alert イベント
- CLI、IDM、IME、または ASDM から手動で設定されたブロック
- ホストまたはネットワーク アドレスに対して永続的に設定されたブロック

ARC がデバイスをブロックするように設定すると、そのデバイスとの間で Telnet または SSH 接続を開始します。ARC は、デバイスごとに接続を維持します。ブロックが開始されると、ARC は制御対象の各デバイスに新しい設定または ACL のセットを（インターフェイス方向ごとに 1 つずつ）プッシュします。ブロックが完了すると、すべての設定または ACL はブロックを削除するようにアップデートされます。

ARC の機能

ARC には、次の機能があります。

- 3DES（デフォルト）または DES 暗号化を使用する Telnet および SSH 1.5。

  そのデバイスの ARC 設定で指定されたプロトコルのみが試行されます。何らかの理由で接続が失われると、ARC は再確立を試みます。

- ルータ上の既存 ACL およびスイッチ上の既存 VACL。

  既存 ACL が、ARC によって制御されるルータのインターフェイス / 方向に存在する場合は、この ACL を ARC によって生成される設定にマージするように指定できます。これは、preblock ACL を指定するとすべてのブロックの前に、postblock ACL を指定するとブロックの後に行われます。Catalyst 6000 VACL デバイス タイプには、ARC が制御するインターフェイスごとに preblock および postblock VACL を指定できます。ファイアウォール デバイス タイプでは、ブロックを実行するために別の API が使用され、ARC はファイアウォール上の既存 ACL には影響を与えません。

  （注） Catalyst 5000 RSM および Catalyst 6000 MSFC2 ネットワーク デバイスは、Cisco ルータとして同じようにサポートされます。

- リモート センサーのリストに対するブロックの転送

  ARC は、リモート センサーのリストにブロックを転送できます。そのため、複数のセンサーが実質的に集団となって 1 つのネットワーク デバイスを制御することができます。このようなリモート センサーをマスター ブロッキング センサーと言います。

- ネットワーク デバイスのインターフェイスに対するブロッキングの指定

  ルータの ARC 設定で、ブロッキングが実行されるインターフェイス / 方向を指定できます。VACL 設定では、ブロッキングが実行されるインターフェイスを指定できます。

  （注） シスコのファイアウォールは、インターフェイスまたは方向に基づくブロックは行いません。したがって、この設定がファイアウォールで指定されることはありません。

  ARC は、同時に 250 までのインターフェイスを制御できます。

- ホストまたはネットワークに対する指定された時間のブロッキング

  ARC は、分単位で指定された時間だけ、または永続的にホストまたはネットワークをブロックできます。ARC は、ブロックの期限がいつ切れたかを判断し、期限切れになるとホストまたはネットワークのブロックを解除します。

- 重要なイベントのロギング

  ARC は、ブロックまたはブロック解除アクションが正常に完了するか何らかのエラーが発生すると、確認イベントを書き込みます。また、ARC は、ネットワーク デバイスの通信セッションの切断と回復、コンフィギュレーション エラー、ネットワーク デバイスから報告されるエラーなどの重要なイベントも記録します。

- ARC 再起動時におけるブロッキング状態の維持

  シャットダウン/再起動が発生したとき、ARC は期限が切れていないブロックを再適用します。シャットダウン中に期限が切れたブロックは削除されます。

  （注） ARC がブロッキング状態を正しく維持するためには、アプリケーションのシャットダウン中にシステムの時刻が変更されないことが条件です。

- ネットワーク デバイス再起動時におけるブロッキング状態の維持

  ネットワーク デバイスがシャットダウンされ、再起動されると、ARC は必要に応じてブロックを再適用したり、期限が切れたブロックを削除します。ARC は、ARC のシャットダウンおよび再起動が同時に、または重複して発生しても影響を受けません。

- 認証と認可

  ARC は、リモート TACACS+ サーバの使用を含め、AAA 認証および認可を使用するネットワーク デバイスとの間で通信セッションを確立できます。

- 2 種類のブロッキング

  ARC は、ホスト ブロックとネットワーク ブロックをサポートしています。ホスト ブロックは、接続ベースまたは無条件です。ネットワーク ブロックは、常に無条件です。

- NAT アドレス指定

  ARC は、センサーに対して NAT アドレスを使用するネットワーク デバイスを制御できます。ネットワーク デバイスを設定する際に NAT アドレスを指定すると、そのデバイスに対するブロックからセンサーのアドレスがフィルタ処理されるときに、ローカル IP アドレスの代わりにそのアドレスが使用されます。

- シングル ポイント制御

  ARC はネットワーク デバイスの制御を管理者や他のソフトウェアとの間で共有しません。設定を更新する必要がある場合は、変更が完了するまで ARC をシャットダウンしておきます。CLI または Cisco IPS マネージャを通して、ARC をイネーブルまたはディセーブルに設定できます。ARC は、再イネーブルされると、自身を完全に初期化し直します。これには、制御対象のネットワーク デバイスごとに現在の設定の再読み込みすることも含まれます。

  （注） ファイアウォールを含むすべてのネットワーク デバイスを設定する際は、ARC によるブロッキングを無効にすることを推奨します。

- 常に最大 250 のアクティブなブロック

  ARC は、同時に 250 までのアクティブなブロックを維持できます。ARC は 65535 までのブロックをサポートしていますが、設定は 250 までにすることを推奨します。

（注）　ブロックの数は、インターフェイス/方向の数とは異なります。

サポートされているブロッキング デバイス

ARC は、次のデバイスを制御できます。

- Cisco IOS 11.2 以降を実行する Cisco ルータ

（注）　レート制限を実行するには、ルータで Cisco IOS 12.3 以降を実行している必要があります。

- スーパーバイザ エンジン上で実行される Supervisor Engine ソフトウェア 5.3(1) 以降、および RSM 上で実行される IOS 11.2(9)P 以降を使用する Catalyst 5000 シリーズ スイッチ

（注）　ブロッキングは RSM 上で実行されるため、RSM が必要です。

- PFC がインストールされ、Catalyst ソフトウェア 5.3 以降が実行される Catalyst 6000 シリーズ スイッチ
- Catalyst ソフトウェア 5.4(3) 以降、および MSFC2 上の Cisco IOS 12.1(2)E 以降を使用する Catalyst 6000 MSFC2
- Cisco ASA 500 シリーズ モデル ; ASA 5510、ASA 5520、ASA 5540
- FWSM

（注）　FWSM はマルチ モード管理コンテキストをブロックできません。

ACL と VACL

ARC が制御するインターフェイス/方向のパケットをフィルタ処理する場合は、すべてのブロックの前に ACL を適用したり（preblock ACL）、すべてのブロックの後に ACL を適用する（postblock ACL）ように ARC を設定できます。これらの ACL は、ネットワーク デバイス上で非アクティブな ACL として設定されます。preblock および postblock ACL は、インターフェイスおよび方向ごとに定義できます。ARC は、ネットワーク デバイス上のアクティブな ACL を更新する際、リストを取得してキャッシュしてから、ブロッキング ACE にマージします。ほとんどの場合は、ブロックの効果を妨げないように、既存 ACL を postblock ACL として指定します。ACL はパケットを、最初に検索された ACE と照合することにより機能します。最初の ACE でパケットが許可された場合、その後の拒否エントリは検索されません。

インターフェイス/方向ごとに異なる preblock および postblock ACL を指定することも、同じ ACL を複数のインターフェイス/方向に再利用することもできます。preblock リストを適用しない場合は、ホストやネットワークに対して never block オプションを使用したり、既存の設定ステートメントを使用して常にブロックしたりすることができます。forever block は、normal block でタイムアウト値を -1 にした場合と同じです。

ARC は、所有する ACL のみを変更します。ユーザによって定義された ACL は変更しません。ARC が維持する ACL は、ユーザ定義の ACL では使用が禁じられている特殊な形式になっています。命名規則は、**IPS_**<interface_name>**_[in | out]_[0 | 1]** です。<interface_name> は、ブロッキング インターフェイスに対して ARC 設定で指定された名前に対応します。

Catalyst スイッチでは、これは、ブロッキング インターフェイスの VLAN 番号です。これらの名前は、preblock および postblock ACL では使用しないでください。

Catalyst 6000 VACL では、preblock および postblock VACL を指定できます。また、インターフェイスのみが指定可能です（VLAN では方向は使用されません）。

ファイアウォールでは、ブロッキングに異なる API が使用されるため、preblock または postblock ACL は使用できません。代わりに、ファイアウォールでは ACL を直接作成する必要があります。

再起動時の状態の維持

センサーがシャットダウンされると、ARC が維持しているローカル ファイル（nac.shun.txt）にすべてのブロッキングとレート制限（および開始時のタイムスタンプ）が書き込まれます。ARC が起動すると、このファイルを使用して、制御対象のネットワーク デバイスにブロックのアップデートが必要かどうかが判断されます。ファイル内に期限が切れていないブロックが見つかると、ネットワーク デバイスの起動時に適用されます。ARC がシャットダウンするときは、有効なブロックが存在していても ACL に対して特別なアクションは行われません。nac.shun.txt ファイルが正確であるためには、ARC が実行されていない間にシステムの時刻が変更されないことが必要です。

注意　nac.shun.txt ファイルには手動による変更を加えないでください。

次のシナリオに、ARC が再起動時にどのように状態を維持するかを示します。

シナリオ 1

ARC が停止したときには 2 つのブロックが有効で、そのうちの 1 つは ARC が再起動する前に期限が切れます。再起動した ARC は、最初に nac.shun.txt ファイルを読み取ります。次に、preblock および postblock ACL または VACL を読み取ります。アクティブな ACL または VACL は、次の順序で構築されます。

1. **allow** *sensor_ ip_address* コマンド（**allow sensor shun** コマンドが設定されていない場合）
2. preblock ACL
3. 設定にある **always block** コマンドのエントリ
4. nac.shun.txt にある期限が切れていないブロック
5. postblock ACL

ARC 設定でホストが never block と指定されている場合、ACL の permit ステートメントには変換されません。代わりに、ARC にキャッシュされて、受信 addShunEvent イベントおよび addShunEntry 制御トランザクションをフィルタ処理するために使用されます。

シナリオ 2

preblock ACL および postblock ACL は指定されていませんが、アクティブな ACL が存在しています。新しい ACL は、次の順序で構築されます。

1. **allow** *sensor_ ip_address* コマンド（**allow sensor shun** コマンドが設定されていない場合）
2. 設定にある **always block** コマンドのエントリ
3. nac.shun.txt にある期限が切れていないブロック
4. **permit IP any any** コマンド

接続ベースおよび無条件のブロッキング

ARC は、ホストに関しては 2 種類、ネットワークに関しては 1 種類のブロッキングをサポートしています。ホスト ブロックは、接続ベースまたは無条件です。ネットワーク ブロックは、常に無条件です。

ARC は、ホスト ブロックを受信すると、その connectionShun 属性を調べます。connectionShun が true に設定されていると、ARC は接続ブロッキングを実行します。すべてのホスト ブロックは、宛先 IP アドレス、ソース ポート、宛先ポート、プロトコルといったオプションのパラメータを含むことができます。接続ブロックが実行されるためには、少なくともソース IP アドレスと宛先 IP アドレスが存在している必要があります。ソース ポートが接続ブロックに存在しても、これは無視されてブロックには含まれません。

次の条件のとき、ARC は必要に応じて接続タイプからブロックを変換して、ブロックを無条件にします。

- 指定されたソース IP アドレスに対して、いずれかのタイプのブロックがアクティブである。
- そのソース IP アドレスに対して、いずれかのタイプの新しいブロックが受信された。
- 新しいブロックのいずれかのオプション パラメータ（ソース ポートを除く）が以前のブロックと異なる。

ブロックがアップデートされると（既存のブロックがすでに有効になっているソース IP アドレスやネットワークに関して新しいブロックが受信された場合など）、既存のブロックの残り時間（分）が決定されます。新しいブロックの時間がこの残り時間以下の場合、アクションは何も発生しません。そうでない場合は、新しいブロックのタイムアウトによって既存のブロックのタイムアウトが置き換えられます。

注意　Cisco ファイアウォールは、ホストの接続ブロッキングをサポートしません。接続ブロックが適用されると、ファイアウォールは接続ブロックを無条件ブロックのように扱います。Cisco ファイアウォールは、ネットワーク ブロッキングもサポートしません。ARC が Cisco ファイアウォールに対してネットワーク ブロックの適用を試みることはありません。

Cisco ファイアウォールによるブロッキング

ARC は、**shun** コマンドを使用することにより、ファイアウォールに対してブロックを実行します。**shun** コマンドの形式は次のとおりです。

- IP アドレスをブロックする。

  shun srcip [*destination_ip_address source_port destination_port* [*port*]]

- IP アドレスのブロックを解除する。

  no shun ip

- すべてのブロックをクリアする。

  clear shun

- アクティブなブロック、または実際にブロックされているグローバル アドレスを表示する。

  show shun [*ip_address*]

ARC は、**show shun** コマンドに対する応答を使用して、ブロックが実行されたかどうかを判断します。

shun コマンドは既存の ACL、条件、アウトバウンド コマンドを置き換えるものではないので、既存のファイアウォール設定をキャッシュしたり、ブロックをファイアウォール設定にマージする必要はありません。

注意　ARC の実行中は、手動でブロックを実行したり既存のファイアウォール設定を変更したりしないでください。

block コマンドでソース IP アドレスのみを指定すると、既存のアクティブな TCP 接続は維持されますが、ブロックされたホストからの着信パケットはすべてドロップされます。

ARC が最初に起動したとき、ファイアウォールでアクティブなブロックが内部のブロッキング リストと比較されます。内部のリストに対応するエントリがないブロックは削除されます。

ARC は、ファイアウォールでの認証をサポートするためにローカル ユーザ名または TACACS+ サーバを使用します。ファイアウォールで認証に AAA を使用して TACACS+ サーバは使用しないように設定すると、ARC はファイアウォールとの通信に予約済みのユーザ名 *pix* を使用します。

ファイアウォールで認証に TACACS+ サーバを使用する場合は、TACACS+ ユーザ名を使用します。AAA ログインを使用する一部のファイアウォール設定では、3 つのパスワード プロンプトが表示されます。初期ファイアウォール パスワード、AAA パスワード、イネーブル パスワードです。ARC では、初期 AAA ファイアウォール パスワードと AAA パスワードを同じにすることが要求されます。

NAT または PAT を使用するようにファイアウォールを設定し、ネットワーク外にあるファイアウォール上のパケットをセンサーがチェックする場合、ネットワーク内のファイアウォールから開始されたホスト攻撃が検出されると、センサーはファイアウォールから提供された変換アドレスのブロックを試みます。ダイナミック NAT アドレッシングを使用している場合は、ブロックが効果を発揮しなかったり、無害なホストがブロックされることがあります。PAT アドレッシングを使用している場合は、ファイアウォールが内部ネットワーク全体をブロックする可能性があります。これらの状況を回避するには、センサーを内部インターフェイスに配置するか、センサーがブロックを行わないように設定します。

Catalyst スイッチによるブロッキング

Catalyst スイッチには、VACL を使用する PFC フィルタ パケットが搭載されています。VACL は、VLAN 間および VLAN 内のすべてのパケットをフィルタ処理します。

WAN カードが取り付けられている場合は MSFC ルータ ACL がサポートされ、MSFC2 を通じてセンサーがインターフェイスを制御するようにすることができます。

（注）　MSFC2 カードは、VACL によるブロッキングを行うための Catalyst スイッチ設定の一部として必要なわけではありません。

注意　Catalyst スイッチで ARC を設定する場合は、制御インターフェイスで方向を指定しないでください。インターフェイス名は VLAN 番号です。preblock および postblock のリストは、VACL である必要があります。

Catalyst VACL に対しては、次のコマンドを使用できます。

- 既存の VACL を表示する。
  show security acl info *acl_name*
- アドレスをブロックする（*address_spec* は、ルータの ACL で使用されるものと同じです）。
  set security acl ip *acl_name* **deny** *address_spec*

- リストの構築後に VACL をアクティブにする。

  commit security acl all

- 1 つの VACL をクリアする。

  clear security acl map *acl_name*

- すべての VACL をクリアする。

  clear security acl map all

- VACL を VLAN にマップする。

  set sec acl *acl_name vlans*

Logger

センサーは、すべてのイベント（alert、error、status、debug の各メッセージ）を永続的な循環バッファに記録します。また、センサーは IP ログも生成します。このメッセージと IP ログには、CLI、IDM、ASDM、および SDEE クライアントからアクセスできます。

IPS アプリケーションは、Logger を使用してメッセージを記録します。Logger は、ログ メッセージを debug、timing、warning、error、fatal の 5 段階の重大度のいずれかで送信します。Logger は、ログ メッセージを、循環式のテキスト ファイルである /usr/cids/idsRoot/log/main.log に書き込みます。ファイルがサイズの上限に達すると、古いメッセージは新しいメッセージによって上書きされます。したがって、main.log では、最後に書き込まれたメッセージが末尾にあるとは限りません。main.log に書き込まれた最新の行を見つけるには、「= END OF FILE =」を検索してください。

main.log は、**show tech-support** コマンドの出力に含まれます。メッセージが warning またはそれよりも上（error または fatal）のレベルで記録されると、Logger はメッセージを evError イベントに変換して（対応するエラーの重大度で）、Event Store に挿入します。

Logger は、informational 以上のレベルで cron メッセージ以外のすべての sys ログ メッセージ（*.info;cron.none）を受信し、エラーの重大度を warning に設定してから evErrors として Event Store に挿入します。Logger およびアプリケーションのロギングは、service logger コマンドによって制御されます。

Logger は、さまざまなロギング ゾーンのロギング重大度を制御することにより、各アプリケーションが生成するログ メッセージを制御できます。ユーザは、TAC のエンジニアまたは開発者の依頼および指示の下で、ロガー サービスの individual-zone-control にのみアクセスします。トラブルシューティングのために、TAC はデバッグ ロギングを依頼することがあります。

AuthenticationApp

ここでは AuthenticationApp について説明します。内容は次のとおりです。

AuthenticationApp について

AuthenticationApp には、次の役割があります。

- ユーザの ID を認証する。
- ユーザのアカウント、権限、キー、証明書を管理する。
- AuthenticationApp、およびセンサー上の他のアクセス サービスで使用する認証方法を設定する。

ユーザの認証

ユーザ アクセスに適切なセキュリティを確立するために、センサーで認証を設定する必要があります。センサーをインストールすると、初期アカウントとして、パスワードの期限が切れている cisco というアカウントが作成されます。センサーに対する管理アクセス権を持ったユーザは、デフォルトの管理アカウント（cisco）を使用してセンサーにログインすることにより、IDM や ASDM などの CLI または IPS マネージャを通じてセンサーにアクセスします。CLI で、管理者はパスワードの変更を要求されます。IPS マネージャは setEnableAuthenticationTokenStatus 制御トランザクションを開始して、アカウントのパスワードを変更します。

CLI または IPS マネージャを通じて、管理者は、ユーザ名とパスワード、SSH 認証キーなどの使用する認証方法を設定します。管理者用のアプリケーションは、認証設定を確立するために setAuthenticationConfig 制御トランザクションを起動します。

認証設定には、アカウント ロッキングの処理方法を指定するログイン試行の上限値が含まれています。アカウント ロッキングは、ログインの試みが連続して失敗した回数が、指定されたログイン試行の上限値を超えると起動されます。アカウントがロックされると、その後のログインの試行はすべて拒否されます。アカウントのロックを解除するには、setEnableAuthenticationTokenStatus 制御トランザクションを使用してアカウントの認証トークンをリセットします。アカウント ロッキング機能は、ログイン試行の上限値を 0 に設定すると無効になります。

管理者は、CLI または IPS マネージャから新しいユーザ アカウントを追加できます。

センサーにおける認証の設定

ユーザが Web Server や CLI などのサービスを通じてセンサーにアクセスしようとするときは、ユーザの ID を認証し、ユーザの権限を確立する必要があります。ユーザにアクセスを提供するサービスは、ユーザの ID を認証するために、AuthenticationApp に対して execAuthenticateUser 制御トランザクション要求を開始します。通常、制御トランザクション要求にはユーザ名とパスワードが含まれています。または、SSH によって確認されたキーによってユーザの ID を認証できます。

AuthenticationApp は、execAuthenticateUser 制御トランザクション要求に対して、ユーザの ID の認証を試みることによって応答します。AuthenticationApp は、ユーザの認証ステータスおよび権限を含む制御トランザクション応答を返します。ユーザの ID を認証できない場合、AuthenticationApp は、非認証ステータスと匿名ユーザ権限を制御トランザクション応答として返します。制御トランザクション応答は、アカウントのパスワードが期限切れであるかどうかも示します。execAuthenticateUser 制御トランザクションを開始することによってユーザを認証するユーザ インターフェイス アプリケーションは、ユーザにパスワードの変更を要求します。

AuthenticationApp は、基盤となるオペレーティング システムを使用してユーザの ID の認証を確認します。すべての IPS アプリケーションは、AuthenticationApp に制御トランザクションを送信します。AuthenticationApp は、オペレーティング システムを使用してその応答を作成します。

リモート シェル サービスである Telnet と SSH は、IPS アプリケーションではありません。これらは、オペレーティング システムを直接呼び出します。ユーザが認証されていれば、オペレーティング システムは IPS CLI を起動します。この場合、CLI は特殊な形式の execAuthenticateUser 制御トランザクションを送信することにより、ログイン ユーザの権限レベルを判断します。次に CLI は、この権限レベルに応じて、使用可能にするコマンドを用意します。

TLS および SSH 信頼関係の管理

IP ネットワーク上の暗号化通信は、パケット内のデータを復号化するために必要な秘密キーを、交換されるパケットだけから受動的攻撃者が発見できないようにすることで、データ プライバシーを実現します。

しかし、同じような危険性を持つ攻撃ベクトルとして、接続のサーバ側であるように装う詐称があります。すべての暗号化プロトコルには、クライアントがこの種の攻撃から身を守るための手段が用意されています。IPS は、SSH と TLS という 2 つの暗号化プロトコルをサポートしています。また、AuthenticationApp は、センサーが暗号化通信のクライアントまたはサーバになる場合の信頼を管理するのに役立ちます。

IPS Web Server および SSH サーバは、暗号化通信のサーバ エンドポイントです。これらは、秘密キーによって ID を保護し、接続してくるクライアントに公開キーを提供します。TLS では、この公開キーは X.509 証明書の中に含まれています。X.509 証明書には他の情報も格納されています。センサーに接続するリモート システムは、接続確立時に受け取った公開キーが、目的のものであることを確認する必要があります。

クライアントは、中間者攻撃を防御するため、信頼できる公開キーのリストを維持する必要があります。この信頼性を確立するための詳細な手順は、プロトコルおよびクライアント ソフトウェアによって異なります。一般的に、クライアントは 16 ～ 20 バイトのフィンガープリントを表示します。クライアントが信頼を確立するように設定する人間のオペレータは、信頼の確立を試行する前に、アウトオブバンド方式を使用してサーバのキー フィンガープリントを取得する必要があります。フィンガープリントが一致すると信頼関係が確立され、その後、クライアントは自動的にそのサーバに接続でき、リモート サーバが詐称者でないことを確信できます。

show ssh server-key および **show tls fingerprint** を使用して、センサーのキー フィンガープリントを表示できます。センサー コンソールに直接接続したときにこれらのコマンドの出力を記録しておくと、後から信頼関係を確立する際、その情報を使用することにより、ネットワークを通じてセンサーの ID を確認できます。

たとえば、最初に Microsoft Internet Explorer Web ブラウザを通じてセンサーに接続したときには、証明書が信頼されていないというセキュリティ警告のダイアログボックスが表示されます。Internet Explorer のユーザ インターフェイスを使用して証明書のサムプリントを調べます。この値は、**show tls fingerprint** コマンドによって表示される SHA1 フィンガープリントに正確に一致する必要があります。確認が終わったら、この証明書をブラウザの信頼済み CA のリストに追加して、永続的な信頼を確立します。

この信頼性を確立するための手順は、TLS クライアントごとに異なります。センサー自体に TLS クライアントが含まれており、制御トランザクションを他のセンサーに送信したり、アップグレードおよびコンフィギュレーション ファイルを TLS Web サーバからダウンロードするために使用されます。センサーの通信相手となる TLS サーバの信頼性を確立するには、**tls trusted-host** コマンドを使用します。

同様に、センサーには SSH クライアントが含まれており、管理対象ネットワーク デバイスとの通信、アップグレードのダウンロード、リモート ホストへのコンフィギュレーション ファイルおよびサポート ファイルのコピーに使用されます。センサーが接続する SSH サーバとの信頼関係を確立するには、**ssh host-key** コマンドを使用します。

TLS trusted certificate および SSH 既知ホストのリストは、**service trusted-certificates** コマンドおよび **service ssh-known-hosts** コマンドで管理できます。

X.509 証明書には、信頼関係のセキュリティを向上させる追加情報が含まれていますが、これは混乱を招く場合があります。たとえば、X.509 証明書には、その証明書を信頼できる有効期間が含まれています。通常、これは証明書が作成された瞬間から始まる数年の期間です。使用時点で X.509 証明書が有効であることを厳密に確認するには、クライアント システムで正確なクロックを維持する必要があります。

また、X.509 証明書は、特定のネットワーク アドレスと結び付けられています。センサーはこのフィールドに、センサーのコマンドおよびコントロール インターフェイスの IP アドレスを挿入します。そのため、センサーのコマンドおよびコントロール IP アドレスを変更すると、サーバの X.509 証明書は再生成されます。新しい IP アドレスでこのセンサーを見つけ、新しい証明書を信頼するには、以前の証明書を信頼していた、ネットワーク上のすべてのクライアントを再設定しなければなりません。

AuthenticationApp の SSH 既知ホストおよび TLS 信頼済み証明書サービスを使用することにより、センサーを高いセキュリティ レベルで運用することができます。

Web Server

Web Server は SDEE サポートを提供します。これによってセンサーは、セキュリティ イベントの報告、IDIOM トランザクションの受信、および IP ログの提供が可能になります。

Web Server は HTTP 1.0 と 1.1 をサポートします。Web Server との通信には、パスワードなどの機密情報が関係することがよくあります。これらを攻撃者が盗聴することが可能になると、システムの安全性が大きく損なわれます。そのため、センサーは TLS がイネーブルな状態で出荷されます。TLS プロトコルは、SSL と互換性のある暗号化プロトコルです。

（注） RDEP イベント サーバ サービスは IPS 6.1 で廃止され、現在の IPS システム アーキテクチャから削除されています。現在、Web Server は SDEE イベント サーバを使用しています。

SensorApp

ここでは SensorApp について説明します。内容は次のとおりです。

SensorApp について

SensorApp はパケットの取り込みと分析を実行します。SensorApp のシグニチャを通してポリシー違反が検出され、違反に関する情報が alert の形式で Event Store に転送されます。

パケットは、センサー上のネットワーク インターフェイスからパケットを収集するように設計されたプロデューサによって供給されたプロセッサのパイプラインを通ります。

SensorApp は次のプロセッサをサポートします。

- 時間プロセッサ

  このプロセッサがタイムスライス カレンダーに格納されたイベントを処理します。主なタスクは、古いデータベース エントリを有効期限切れにすることと時間に依存する統計情報を計算することです。

- 拒否フィルタ プロセッサ

  このプロセッサが攻撃者拒否機能を処理します。拒否されたソース IP アドレスのリストを維持します。リストの各エントリは、グローバル拒否タイマー（仮想センサー設定で設定可能）に基づいて有効期限が切れます。

- シグニチャ イベント アクション プロセッサ

  イベント アクションを処理します。次のイベント アクションをサポートします。

  - TCP フローのリセット
  - IP ログ
  - パケットの拒否
  - フローの拒否
  - 攻撃者の拒否
  - アラート
  - ホストのブロック
  - 接続のブロック
  - SNMP トラップの生成
  - トリガー パケットのキャプチャ

  イベント アクションは、イベント リスク レーティングのしきい値と関連付けることができます。アクションが発生するには、この値を上回る必要があります。

- 統計プロセッサ

  このプロセッサがパケット数やパケット到着レートなどのシステム統計情報を記録します。

- レイヤ 2 プロセッサ

  このプロセッサがレイヤ 2 関連イベントを処理します。また、不正な形式のパケットを識別し、処理パスから取り除きます。alert、capture packet、deny packet など、不正な形式のパケットを検出するための実行可能なイベントを設定します。レイヤ 2 プロセッサは、設定したポリシーで拒否されたパケットに関する統計情報を更新します。

- データベース プロセッサ

  このプロセッサがシグニチャの状態とフロー データベースを管理します。

- フラグメント再構成プロセッサ

  フラグメント化された IP データグラムをこのプロセッサが再構成します。センサーがインライン モードの場合、IP フラグメントの正規化も行います。

- ストリーム再構成プロセッサ

  さまざまなストリームベース インスペクタでのパケットが正しい順序で到着するように TCP ストリームの順序をこのプロセッサが変更します。TCP ストリームの正規化も行います。Normalizer エンジンでは、アラート アクションと拒否アクションをイネーブルまたはディセーブルにできます。

TCP ストリーム再構成プロセッサのノーマライザには、再設定イベントの後にストリームの状態を再構築できるホールドダウン タイマーがあります。このタイマーは設定できません。ホールドダウン期間中、システムは、通過するストリームの最初のパケットでストリームの状態を同期します。ホールドダウンの有効期限が切れると、SensorApp は設定されたポリシーを強制します。このポリシーが、スリーウェイ ハンドシェイクで開かれなかったストリーム拒否のコールを発信する場合、確立されたストリームの中でホールドダウン期間に休止されていたストリームは転送されず、タイムアウトが許可されます。ホールドダウン期間に同期されたストリームは続行可能となります。

- シグニチャ分析プロセッサ

  処理中のパケットを対象とするように設定された、ストリームベースではないインスペクタにパケットをこのプロセッサが発送します。

- スレーブ ディスパッチ プロセッサ

  デュアル CPU システムで見られるプロセス。

一部のプロセッサはインスペクタをコールしてシグニチャ分析を実行します。インスペクタはすべて、必要に応じてアラーム チャネルをコールしてアラートを生成できます。

SensorApp は次のユニットもサポートします。

- 分析エンジン

  センサー設定を処理します。インターフェイスとシグニチャおよびアラーム チャネル ポリシーを設定済みのインターフェイスにマッピングします。

- アラーム チャネル

  インスペクタによって生成されたすべてのシグニチャ イベントを処理します。主な機能は、渡された各イベントに対するアラートの生成です。

インライン、正規化、イベント リスク レーティング機能

（注） IPS SSP を搭載した Cisco ASA 5585-X では、正規化がサポートされていません。

SensorApp には、次のインライン、正規化、イベント リスク レーティング機能があります。

- パケットのインライン処理

  センサーがデータ パスでパケットを処理するとき、ポリシー設定で明示的に拒否されている場合を除き、すべてのパケットは変更が加えられることなく転送されます。TCP 正規化により、適切なカバレッジを確保するため一部のパケットが遅延することがあります。ポリシー違反が検出されると、SensorApp はアクションの設定を許可します。インライン モードでは、パケットの拒否、フローの拒否、攻撃者の拒否など、追加のアクションを実行できます。

  IPS に対して不明または存在しないパケットはすべて、ペアにされたインターフェイスに転送されます。このとき、分析は行われません。ポリシー違反が原因で拒否されるおそれのあるものを除き、すべてのブリッジング プロトコルとルーティング プロトコルが転送されます。インライン（または無差別）データ処理に使用するインターフェイスに関連付けられる IP スタックはありません。無差別モードでの 802.1q パケットの現在のサポートは、インライン モードに拡張されています。

- IP の正規化

  IP データグラムの意図的または意図しないフラグメンテーションにより、悪用が隠れてしまい、検出が困難になったり不可能になったりすることがあります。フラグメンテーションは、ファイアウォールやルータで実行されるアクセス コントロール ポリシーを回避するために使用されること

もあります。オペレーティング システムごとに、異なる方法を使用してフラグメント化されたデータグラムをキューに格納してディスパッチします。エンド ホストがデータグラムを再構築できる、考えられるすべての方法をセンサーで確認する必要がある場合、センサーは DoS 攻撃に脆弱になります。フラグメント化されたすべてのデータグラムをインラインで再構築し、完成したパケットのみを転送し、必要に応じてデータグラムを再度フラグメント化することで、これを避けることができます。IP Fragmentation Normalization ユニットはこの機能を実行します。

- TCP の正規化

  意図的または自然の TCP セッションのセグメント化を通じて、一部の攻撃クラスが隠れることがあります。ポリシーの強制が、偽陽性または偽陰性なく行われるようにするため、2 つの TCP エンドポイントの状態を追跡し、実際のホスト エンドポイントで実際に処理されるデータのみを通過させる必要があります。TCP ストリームの重なりが起きる可能性がありますが、TCP セグメントの再送以外では非常にまれです。TCP セッションの上書きが起こらないことが必要です。上書きが起きる場合、誰かが意図的にセキュリティ ポリシーを回避しようとしているか、TCP スタックの実装が壊れています。両方のエンドポイントの状態に関する完全な情報を維持することは、センサーが TCP プロキシとして動作しない限り不可能です。センサーが TCP プロキシとして動作する代わりに、セグメントが適切に順序付けされ、ノーマライザは回避や攻撃に関連する異常なパケットを探します。

- イベント リスク レーティング

  イベント リスク レーティングには、潜在的に悪意のあるアクションの検出に加え、次の追加情報が組み込まれます。

  - 攻撃が成功した場合の重大度
  - シグニチャの忠実度
  - ターゲット ホストに対する関連性
  - ターゲット ホストの各自にとっての全体的な価値

  イベント リスク レーティングはシステムの偽陽性の抑制に役立ち、アラートの原因についてより精度の高い制御が可能になります。

SensorApp の新機能

SensorApp の新機能は次のとおりです。

- ポリシー テーブル：リスク カテゴリの設定（高、中、低）を提供します。
- 回避保護：ノーマライザについて、インライン インターフェイス モード センサーを厳格なモードから非同期モードに切り替えることができます。
- センサー ヘルス状態メーター：センサー全体のヘルス状態の統計情報を提供します。
- トップレベル サービス：TCP、UDP、ICMP、IP プロトコルの上位 10 のインスタンスを提供します。
- セキュリティ メーター：アラートを脅威のカテゴリに分類し、この情報を赤、黄、緑のバケットに報告します。これらのバケットのトランジション ポイントを設定できます。
- フロー状態のクリア：データベースをクリアして、再起動したかのようにセンサーを最初から開始できます。
- 再起動ステータス：センサーの現在の開始段階と再起動段階を定期的に報告します。

パケット フロー

パケットは NIC で受信され、IPS 共有ドライバによってカーネル ユーザにマップされたメモリ領域に配置されます。パケットは IPS ヘッダーに付加されます。各パケットには、シグニチャ イベント アクション プロセッサに到達したパケットを許可するか拒否するかを指定するフィールドもあります。

プロデューサは、共有カーネル ユーザにマップされたパケット バッファからパケットをプルし、センサー モデルに適切なプロセッサを実装する処理機能をコールします。次の順序で実行されます。

- シングル プロセッサ実行

  時間プロセッサ --> レイヤ 2 プロセッサ --> 拒否フィルタ プロセッサ --> フラグメント再構成プロセッサ --> 統計プロセッサ --> データベース プロセッサ --> シグニチャ分析プロセッサ --> ストリーム再構成プロセッサ --> シグニチャ イベント アクション プロセッサ

- デュアル プロセッサ実行

  実行スレッド 1 時間プロセッサ --> レイヤ 2 プロセッサ --> 拒否フィルタ プロセッサ --> フラグメント再構成プロセッサ --> 統計プロセッサ --> データベース プロセッサ --> シグニチャ分析プロセッサ --> スレーブ ディスパッチ プロセッサ --> | 実行スレッド 2 データベース プロセッサ --> ストリーム再構成プロセッサ --> シグニチャ イベント アクション プロセッサ

シグニチャ イベント アクション プロセッサ

シグニチャ イベント アクション プロセッサは、シグニチャ イベント アクション オーバーライド、シグニチャ イベント アクション フィルタ、およびシグニチャ イベント アクション ハンドラを介して処理するように、アラーム チャネルのシグニチャ イベントから取得するデータ フローを調整します。次のコンポーネントで構成されます。

- アラーム チャネル

  SensorApp インスペクション パスからのシグニチャ イベントを処理するために通信を行う領域を示すユニット。

- シグニチャ イベント アクション オーバーライド

  リスク レーティング値に基づいてアクションを追加します。シグニチャ イベント アクション オーバーライドは、設定されたリスク レーティングしきい値の範囲に入るすべてのシグニチャに適用されます。各シグニチャ イベント アクション オーバーライドは独立し、アクション タイプごとに別々の設定値を持ちます。

- シグニチャ イベント アクション フィルタ

  シグニチャ イベントのシグニチャ ID、アドレス、リスク レーティングに基づいてアクションを差し引きます。シグニチャ イベント アクション フィルタへの入力は、シグニチャ イベントアクション オーバーライドによって追加された可能性のあるアクションを含むグニチャ イベントです。

  （注） シグニチャ イベント アクション フィルタが実行できるのは、アクションを差し引くことだけです。新しいアクションを追加することはできません。

  シグニチャ イベント アクション フィルタには、次のパラメータが適用されます。

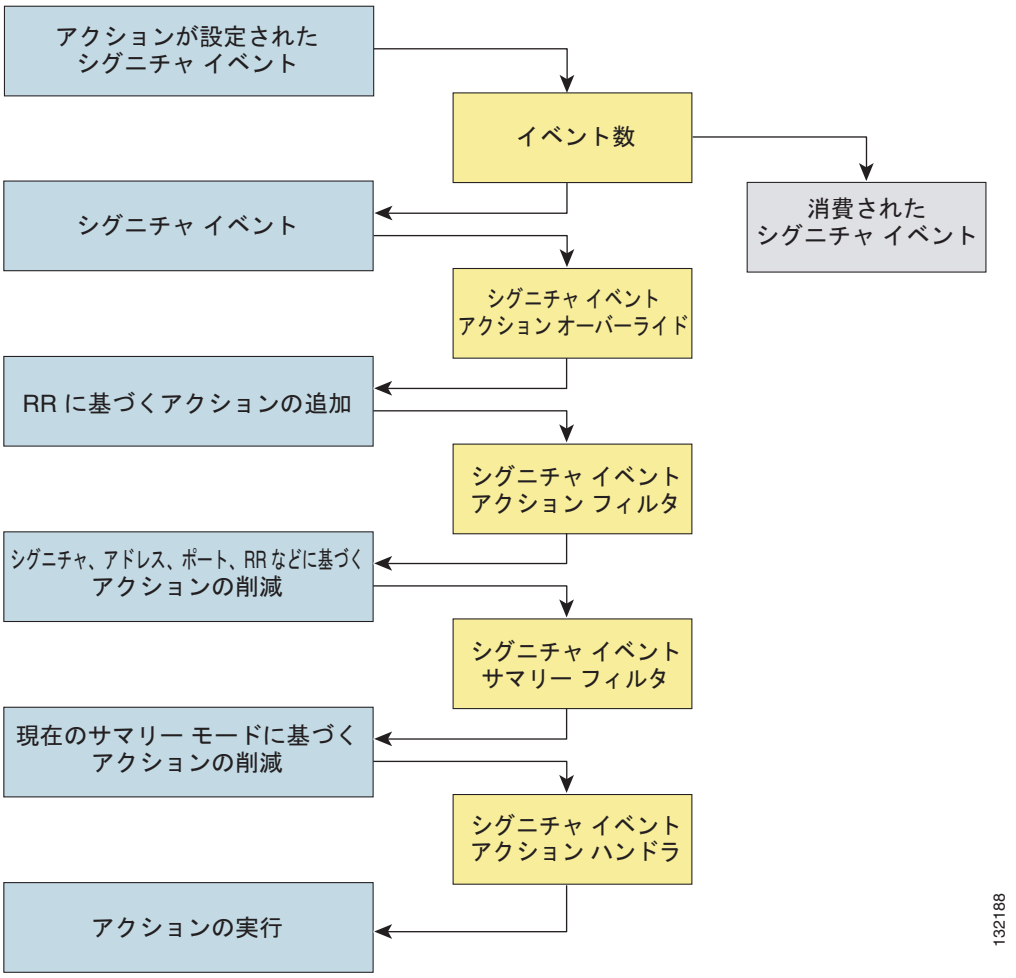
  - シグニチャ ID
  - サブシグニチャ ID
  - 攻撃者のアドレス
  - 攻撃者のポート

  - 攻撃対象のアドレス
  - 攻撃対象者のポート
  - リスク レーティングしきい値の範囲
  - 削除するアクション
  - シーケンス識別子（任意）
  - ストップ ビットまたは継続ビット
  - アクション フィルタ行をイネーブルにするビット
  - 攻撃対象 OS との関連性または OS との関連性
- シグニチャ イベント アクション ハンドラ

  要求されたアクションを実行します。シグニチャ イベント アクション ハンドラからの出力は、実行されているアクションと、イベント ストアに書き込まれる evIdsAlert（ある場合）です。

図 A-4 に、シグニチャ イベント アクション プロセッサを通過するシグニチャ イベントの論理的な流れと、このイベントに対するアクションで実行される操作を示します。アラーム チャネルから受け取ったアクションが設定されているシグニチャ イベントから開始し、そのイベントは、上から下に向かってシグニチャ イベント アクション プロセッサの機能コンポーネントを通過します。

図 A-4　シグニチャ イベント アクション プロセッサを通過するシグニチャ イベント



CollaborationApp

（注）　IPS 6.1 および 6.2 は、グローバル相関機能をサポートしていません。

（注）　AIP SSC-5 は、グローバル相関機能をサポートしていません。

ここでは CollaborationApp について説明します。内容は次のとおりです。

CollaborationApp について

CollaborationApp は、MainApp と SensorApp のピアです。IDAPI 制御トランザクション、セマフォ、共有メモリ、ファイル交換など、さまざまなプロセス間通信テクノロジーを使用してインターフェイスを構築します。

レピュテーション アップデートが、グローバル相関サーバと CollaborationApp の間で交換されます。CollaborationApp は 4 つのアップデート コンポーネントを使用してセンサーとの通信を行います。

- 規則スコアの重み付け値のセット
- IP アドレスとアドレス範囲のセット。規則とアラートとともに、レピュテーション スコアの計算に必要な情報を提供します。
- IP アドレスとアドレス範囲のリスト。トラフィックは常に拒否されます。
- ネットワーク参加設定。センサーがテレメトリ データをサーバに送信する速度を、サーバ側で制御できるようになります。

センサーはネットワーク参加サーバにコラボレーション情報を送信します。センサーは、グローバル相関サーバにクエリを実行し、コラボレーション アップデートの利用可能なリストと、アップデート ファイルをダウンロードできるグローバル相関サーバを照会します。

（注）　SensorApp は CollaborationApp より前に起動しますが、初期化は非同期に実行されます。このため、レピュテーション アップデート サーバは、SensorApp でアップデートを受け入れる準備が整う前に、グローバル相関の更新をダウンロードして適用を試みることができます。アップデート サーバは、アップデートをダウンロードして部分的に処理することはできますが、アップデートをコミットするには、SensorApp is の準備が整うまで待機する必要があります。

詳細情報

グローバル相関の詳細および設定方法については、第 13 章「グローバル相関の設定」を参照してください。

コンポーネントのアップデート

グローバル相関アップデート クライアントは、グローバル相関アップデート サーバとマニフェストを交換します。サーバ マニフェストを解析してダウンロード可能な新しいアップデートがあるかどうかを確認し、存在する場合には、インストールするアップデートのリストを作成します。すべてのアップデートが正常に適用されると、グローバル相関アップデート クライアントは各コンポーネントについてアップデートを適用し、SensorApp に新しいアップデートが利用できることを通知します。そして、クライアント マニフェストを更新し、各コンポーネントに最後にコミットしたアップデートを反映します。

クライアント マニフェストには、センサーの UDI が含まれます。ここには、センサーのシリアル番号と、暗号化された共有秘密（サーバが、センサーが真正な Cisco IPS センサーであることを確認するために使用する）が含まれています。サーバ マニフェストには、各コンポーネントで利用可能なアップデート ファイルのリストが含まれています。リスト内の各アップデート ファイルでは、サーバ マニフェストにアップデートのバージョン、種類、順序、場所、ファイル転送プロトコルなどのデータが含まれています。

アップデート ファイルには、完全なアップデート ファイルと差分アップデート ファイルの 2 種類があります。完全なアップデート ファイルを使用すると、コンポーネントのデータベースに既存のデータはすべて置換されます。差分アップデート ファイルを使用すると、情報の追加、削除、置換を行って既存のレピュテーション データが変更されます。すべてのコンポーネントにすべてのアップデート ファイルが適用されると、作業データベースを置換して、一時データベースをコミットします。

秘密暗号化メカニズムと復号化キー管理によって認証と認可が実現されます。グローバル相関アップデート サーバは、クライアント マニフェストに含まれる共有秘密暗号化メカニズムを使用して、センサーを認証します。グローバル相関アップデート クライアントは、復号化キー管理を使用してセンサーを認証します。グローバル相関アップデート サーバで認証されたセンサーに、サーバ マニフェストに含まれる有効なキーが送信されます。これにより、アップデート ファイルを復号化できるようになります。

注意　グローバル相関をイネーブルに設定し、DNS または HTTP プロキシ サーバを設定していないと、警告メッセージが表示されます。警告では、グローバル相関をディセーブルにするか、DNS または HTTP プロキシ サーバを追加するように通知されます。

詳細情報

グローバル相関をサポートする DNS または HTTP プロキシ サーバを追加する手順については、「ネットワークの設定」（P.6-2）を参照してください。

error イベント

グローバル相関のアップデートに失敗すると、evError イベントが生成されます。エラー メッセージは、センサーの統計情報に含まれます。次の条件に該当する場合、重大度レベルが Error のステータス メッセージが発生します。

- センサーのライセンスが取得されていない
- DNS または HTTP プロキシ サーバが設定されていない
- マニフェスト交換に失敗した
- アップデート ファイルのダウンロードに失敗した
- アップデートの適用またはコミットに失敗した

グローバル相関をイネーブルにするようにホストまたはグローバル相関の設定を保存したときに、DNS または HTTP プロキシ サーバが設定されていないと、重大度レベルが Warning の evError イベントが発生します。

詳細情報

センサーの統計情報を表示するための手順については、「統計情報の表示」（P.19-31）を参照してください。

CLI

ここでは、Cisco IPS CLI について説明します。内容は次のとおりです。

CLI の概要

CLI は、Telnet、SSH、シリアル インターフェイスなどのすべての直接ノード アクセスについて、センサーのユーザ インターフェイスを提供します。センサー アプリケーションは CLI で設定します。基盤となる OS への直接接続は、サービス ロールを通じて許可されます。

ユーザ ロール

ユーザ ロールには、次の 4 つがあります。

- ビューア（Viewer）：設定およびイベントを表示できますが、自分のユーザ パスワード以外の設定データは修正できません。
- オペレータ（Operator）：すべてのデータを表示できるほか、次のオプションを修正できます。
  - シグニチャ チューニング（優先順位、無効 / 有効）
  - 仮想センサーの定義
  - 管理対象ルータ
  - 自分のユーザ パスワード
- 管理者（Administrator）：すべてのデータを表示できるほか、オペレータが修正できるすべてのオプションに加えて、次のオプションを修正できます。
  - センサーのアドレス設定
  - 設定エージェントまたはビュー エージェントとして接続が許可されたホストのリスト
  - 物理的な検知インターフェイスの割り当て。
  - 物理インターフェイスの制御のイネーブル化またはディセーブル化。
  - ユーザとパスワードの追加および削除。
  - 新しい SSH ホスト キーとサーバ証明書の生成
- サービス（Service）：サービス権限を持つユーザはセンサーに 1 人だけ存在できます。サービス ユーザは、IME にログインできません。サービス ユーザは、CLI ではなく bash シェルにログインします。

（注） サービス ロールは、必要に応じて CLI をバイパスできる特殊なロールです。許可されるサービス アカウントは 1 つだけです。トラブルシューティング用には、サービス ロールのアカウントのみを作成してください。管理者権限を持つユーザだけが、サービス アカウントを編集できます。

サービス アカウントにログインすると、次の警告が表示されます。

```
************************ WARNING ****************************************************
UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
This account is intended to be used for support and troubleshooting purposes only.
Unauthorized modifications are not supported and will require this device to be
re-imaged to guarantee proper operation.
*************************************************************************************
```

注意　サービス アカウントを作成するかどうかは、慎重に検討する必要があります。サービス アカウントは、システムへのシェル アクセスを提供するため、システムが脆弱になります。ただし、管理者のパスワードが失われた場合は、サービス アカウントを使用してパスワードを作成できます。状況を分析して、システムにサービス アカウントを存在させるかどうかを決定してください。

サービス アカウント

サービス アカウントは、サポートとトラブルシューティングのツールです。これによって TAC は、CLI シェルではなくネイティブ オペレーティング システムのシェルにログインすることができます。これは、デフォルトではセンサーには存在しません。センサーのトラブルシューティングのために TAC がこれを使用できるようにするためには、ユーザが作成する必要があります。

1 つのセンサーで使用できるサービス アカウントは 1 つだけです。また、1 つのサービス ロールで使用できるアカウントも 1 つだけです。サービス アカウントのパスワードが設定またはリセットされると、root アカウントのパスワードが同じパスワードに設定されます。そのため、サービス アカウントのユーザはこの同じパスワードを使用して、root に su できます。サービス アカウントが削除されると、root アカウントのパスワードはロックされます。

サービス アカウントは、設定の目的で使用されることを想定していません。TAC の指示に基づき、サービス アカウントからセンサーに対して加えられた変更だけがサポートされます。サービス アカウントからオペレーティング システムに追加のサービスを加えること、およびそれを実行することは、他の IPS サービスの適切な実行に影響するため、シスコはこれをサポートしません。TAC は、追加のサービスが加えられたセンサーをサポートしません。

サービス アカウントへのログインは、ログ ファイル /var/log/.tac を確認することによって追跡できます。このファイルは、サービス アカウントによるログインの記録でアップデートされます。

（注）　Cisco IPS には、CLI、IDM、または IME を通して利用可能なトラブルシューティング機能が組み込まれています。大部分のトラブルシューティングでは、サービス アカウントは必要ではありません。特異な問題のトラブルシューティングを行うため、TAC の指示により、サービス アカウントの作成が必要になることがあります。サービス アカウントを使用すると、CLI に組み込まれている保護をバイパスし、（通常はディセーブルになっている）センサーへの root 権限アクセスが許可されます。特別な理由により必要となる場合を除き、サービス アカウントを作成しないことをお勧めします。不要になったサービス アカウントは、必ず削除してください。

通信

ここでは、Cisco IPS が使用する通信プロトコルについて説明します。内容は次のとおりです。

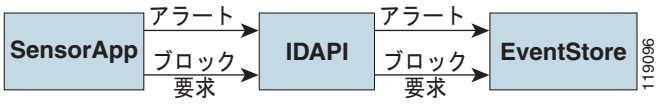
IDAPI

IPS アプリケーションは、内部通信の処理にプロセス間通信 API（IDAPI）を使用します。IDAPI はイベント データを読み書きし、制御トランザクションのメカニズムを提供します。IDAPI は、すべてのアプリケーションが通信の際に使用するインターフェイスです。

SensorApp は、そのインターフェイス上のネットワーク トラフィックをキャプチャし、分析します。シグニチャが一致すると、SensorApp はアラートを生成します。このアラートは Event Store に格納されます。シグニチャがブロッキング応答アクションを実行するように設定されていると、SensorApp はブロック イベントを生成します。このイベントも Event Store に格納されます。

図 A-5 に、IDAPI インターフェイスを示します。

図 A-5　　IDAPI



各アプリケーションは、イベントおよび制御トランザクションを送受信するように IDAPI に登録します。IDAPI は次のサービスを提供します。

- 制御トランザクション
  - 制御トランザクションを開始する。
  - インバウンド制御トランザクションを待機する。
  - 制御トランザクションに応答する。
- IPS イベント
  - リモート IPS イベントをサブスクライブする。受信したリモート IDS イベントは、Event Store に格納されます。
  - Event Store から IPS イベントを読み取ります。
  - Event Store に IPS イベントを書き込みます。

IDAPI は、アトミックなデータ アクセスを実現するために必要な同期メカニズムを備えています。

IDIOM

IDIOM は、IPS によって報告されるイベント メッセージ、および侵入検知システムの設定と制御に使用される操作メッセージを定義するデータ形式の標準です。これらのメッセージは、IDIOM XML スキーマに準拠した XML ドキュメントによって構成されています。

IDIOM は、イベントと制御トランザクションという 2 種類のインタラクションをサポートしています。イベント インタラクションは、alerts などの IPS イベントを交換するために使用されます。IDIOM は、イベント インタラクションにイベント メッセージとエラー メッセージという 2 種類のメッセージを使用します。制御トランザクションは、ホストが別のホストでアクションを開始したり、別のホストの状態を変更または読み取るための手段です。制御トランザクションでは、要求、応答、設定、エラーの 4 種類の IDIOM メッセージが使用されます。1 つのホスト内のアプリケーション インスタンス間で通信されるイベントおよび制御トランザクションは、ローカル イベントまたはローカル制御トランザクションと呼ばれ、ローカル IDIOM メッセージと総称されます。異なるホスト間で通信されるイベントおよび制御トランザクションは、リモート イベントおよびリモート制御トランザクションと呼ばれ、リモート IDIOM メッセージと総称されます。

（注）　大部分の IDIOM は、IDCONF、SDEE、および CIDEE で置き換えられています。

IDCONF

Cisco IPS は、XML ドキュメントを使用して設定を管理しています。IDCONF は、Cisco IPS 制御トランザクションなどの XML スキーマを指定します。IDCONF スキーマは設定ドキュメントの内容は指定しませんが、設定ドキュメントに基づいてフレームワークとビルディング ブロックが開発されます。これにより、サポートされる機能の属性を通して、IPS マネージャと CLI が特定のプラットフォームや機能で設定不可能な機能を無視できるメカニズムが提供されます。

IDCONF メッセージは、IDIOM 要求内部と応答メッセージにラップされます。

次に、IDCONF の例を示します。

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<request xmlns="http://www.cisco.com/cids/idiom" schemaVersion="2.00">
  <editConfigDelta xmlns="http://www.cisco.com/cids/idconf">
    <component name="userAccount">
      <config typedefsVersion="2004-03-01" xmlns="http://www.cisco.com/cids/idconf">
        <struct>
           <map name="user-accounts‟ editOp=‟merge”>
            <mapEntry>
              <key>
               <var name="name">cisco</var>
             </key>
              <struct>
               <struct name="credentials">
                 <var name="role">administrator</var>
               </struct>
              </struct>
           </mapEntry>
         </map>
        </struct>
      </config>
    </component>
  </editDefaultConfig>
</request>
```

SDEE

IPS は、侵入アラート イベントやステータス イベントなど各種イベントを生成します。IPS は、独自の IPS 業界最高レベルのプロトコル SDEE（セキュリティ デバイスのイベントを伝える、製品に依存しない標準）を使用して、管理アプリケーションなどのクライアントにイベントを伝達します。SDEE は、さまざまなタイプのセキュリティ デバイスによって生成されるイベントを伝えるために必要な拡張性機能を追加します。

クライアントにイベントを伝達するために SDEE を使用するシステムは、SDEE プロバイダーと呼ばれます。SDEE は、HTTP または HTTP over SSL と TLS プロトコルを使用してイベントを送信できることを指定します。HTTP または HTTPS を使用する場合、SDEE クライアントは HTTP 要求の発信側となり、SDEE プロバイダーは HTTP サーバとして動作します。

IPS には、HTTP または HTTPS 要求を処理する Web Server が含まれます。Web Server はロード可能なランタイム サーブレットを使用して、さまざまな種類の HTTP 要求を処理します。各サーブレットは、サーブレットに関連付けられた URL に向けられた HTTP 要求を処理します。SDEE サーバは、Web サーバ サーブレットとして実装されます。

SDEE サーバは、認証された要求のみを処理します。要求は、発信元が Web サーバあり、クライアントの身元を認証でき、かつクライアントの権限レベルを特定できる場合に認証されます。

CIDEE

CIDEE は、Cisco IPS で使用される SDEE への拡張子を指定します。CIDEE 標準では、Cisco IPS でサポートされる使用可能なすべての拡張子が指定されています。一部のシステムでは、CIDEE 拡張子のサブセットを実装できます。ただし、必須として指定されている拡張子は、すべてのシステムでサポートされる必要があります。

CIDEE は SDEE evIdsAlert 要素に対し、Cisco IPS 固有のセキュリティ デバイス イベントと IPS 拡張子を指定します。

CIDEE は次のイベントをサポートします。

- evError：エラー イベント

  プロバイダーがエラーまたは警告の条件を検出したときに、CIDEE プロバイダーによって生成されます。evError イベントには、エラー コードとテキストによるエラーの説明が含まれます。

- evStatus：ステータス メッセージ イベント

  ホストに注意すべき事項が発生したことを知らせるときに、CIDEE プロバイダーによって生成されます。ステータス イベントには、さまざまな種類のステータス メッセージが報告されます。1 つのイベントにつき、1 つのメッセージが報告されます。各種ステータス メッセージには、ステータス メッセージが説明している事項に固有のデータ要素のセットが含まれます。ステータス メッセージの多くに含まれる情報は、監査の面で有益な情報です。エラーと警告は状態情報とは見なされず、evStatus ではなく evError を使用して報告されます。

- evShunRqst：ブロック要求イベント

  ネットワーク ブロッキングを処理するサービスによってブロック アクションを開始する必要があることを知らせるために生成されます。

次に、CDIEE 拡張イベントの例を示します。

```
<sd:events xmlns:cid="http://www.cisco.com/cids/2004/04/cidee"
xmlns:sd="‟http://example.org/2003/08/sdee”">
 <sd:evIdsAlert eventId="1042648730045587005" vendor="Cisco‟ severity="medium">
  <sd:originator>
    <sd:hostId>Beta4Sensor1</sd:hostId>
    <cid:appName>sensorApp</cid:appName>
    <cid:appInstanceId>8971</cid:appInstanceId>
  </sd:originator>
  <sd:time offset="0" timeZone="UTC">1043238671706378000</sd:time>
  <sd:signature description="IOS Udp Bomb" id="4600" cid:version="S37">
    <cid:subsigId>0</cid:subsigId>
  </sd:signature> …
```

Cisco IPS ファイル構造

Cisco IPS のディレクトリ構造は次のとおりです。

- /usr/cids/idsRoot：メインのインストール ディレクトリ。
- /usr/cids/idsRoot/shared：システムの回復中に使用されるファイルが格納されます。
- /usr/cids/idsRoot/var：センサーの実行中に動的に作成されるファイルが格納されます。

- /usr/cids/idsRoot/var/updates：アップデート インストレーション用のファイルとログが格納されます。
- /usr/cids/idsRoot/var/virtualSensor：SensorApp が正規表現を分析するために使用するファイルが格納されます。
- /usr/cids/idsRoot/var/eventStore：Event Store アプリケーションが含まれます。
- /usr/cids/idsRoot/var/core：システムのクラッシュ時に作成される重要なファイルが格納されます。
- /usr/cids/idsRoot/var/iplogs：iplog ファイルのデータが格納されます。
- /usr/cids/idsRoot/bin：バイナリ実行可能ファイルが含まれます。
- /usr/cids/idsRoot/bin/authentication：認証アプリケーションが含まれます。
- /usr/cids/idsRoot/bin/cidDump：技術サポート向けのデータを収集するスクリプトが含まれます。
- /usr/cids/idsRoot/bin/cidwebserver：Web Server アプリケーションが含まれます。
- /usr/cids/idsRoot/bin/cidcli：CLI アプリケーションが含まれます。
- /usr/cids/idsRoot/bin/nac：ARC アプリケーションが含まれます。
- /usr/cids/idsRoot/bin/logApp：ロガー アプリケーションが含まれます。
- /usr/cids/idsRoot/bin/mainApp：メイン アプリケーションが含まれます。
- /usr/cids/idsRoot/bin/sensorApp：センサー アプリケーションが含まれます。
- /usr/cids/idsRoot/bin/collaborationApp：コラボレーション アプリケーションが含まれます。
- /usr/cids/idsRoot/bin/falcondump：IDSM2 のセンシング ポートでパケット ダンプを取得するアプリケーションが含まれます。
- /usr/cids/idsRoot/etc：センサーのコンフィギュレーション ファイルが含まれます。
- /usr/cids/idsRoot/htdocs：Web Server の IDM ファイルが含まれます。
- /usr/cids/idsRoot/lib：センサー アプリケーションのライブラリ ファイルが含まれます。
- /usr/cids/idsRoot/log：デバッグ用のログ ファイルが含まれます。
- /usr/cids/idsRoot/tmp：センサーの実行中に作成される一時ファイルが格納されます。

Cisco IPS アプリケーションの概要

表 A-2 に、IPS を構成するアプリケーションの概要を示します。

表 A-2　アプリケーションの概要

アプリケーション	説明
AuthenticationApp	IP アドレス、パスワード、デジタル証明書に基づいてユーザを許可および認証します。
Attack Response Controller	ARC は、各センサー上で実行されます。各 ARC は、ローカル Event Store の network access イベントをサブスクライブします。ARC の設定には、そのローカル ARC が制御するセンサーおよびネットワーク アクセス デバイスのリストが含まれます。network access イベントをマスター ブロッキング センサーに送信するように設定されている ARC は、デバイスを制御するリモート ARC にネットワーク アクセス コントロール トランザクションを送信します。これらのネットワーク アクセス アクション制御トランザクションは、IPS マネージャがネットワーク アクセス アクションを発行するときにも使用されます。
CLI	コマンドライン入力を受け付け、IDAPI を使用してローカル設定を変更します。
CollaborationApp	グローバル相関データベースを通して他のデバイスと情報を共有し、すべてのデバイスの総合的な有効性を高めます。
Control Transaction Server[1]	リモート クライアントからの制御トランザクションを受け付け、ローカル制御トランザクションを開始して、リモート クライアントに応答を返します。
Control Transaction Source[2]	リモート アプリケーションに向けられた制御トランザクションを待機し、制御トランザクションをリモート ノードに転送し、応答を発信側に返します。
IDM	HTML IPS 管理インターフェイスを提供する Java アプレットです。
IME	イベントの表示やアーカイブを行うためのインターフェイスを提供する Java アプレットです。
InterfaceApp	バイパスおよび物理設定を処理し、ペアにするインターフェイスを定義します。物理設定は、速度、デュプレックス、および管理状態です。
Logger	アプリケーションのすべてのログ メッセージをログ ファイルに書き込み、アプリケーションのエラー メッセージをイベント ストアに書き込みます。
MainApp	設定を読み取ってアプリケーションを起動し、アプリケーションの開始および終了とノードの再起動を扱い、ソフトウェアのアップグレードを処理します。
NotificationApp	アラート、ステータス、およびエラー イベントによってトリガーされたときに SNMP トラップを送信します。NotificationApp は、パブリック ドメイン SNMP エージェントを使用します。SNMP GET は、センサーの全般的な状態に関する情報を提供します。
SDEE Server[3]	リモート クライアントからのイベントの要求を受け入れます。

表 A-2　アプリケーションの概要（続き）

アプリケーション	説明
SensorApp	モニタされているネットワーク上のトラフィックをキャプチャして分析し、intrusion および network access イベントを生成します。ロギングをオン / オフする IP ロギング制御トランザクション、および IP ログ ファイルを送信および削除する IP ロギング制御トランザクションに応答します。
Web Server	リモート HTTP クライアント要求を待機し、適切なサーブレット アプリケーションを呼び出します。

1. これは Web サーバ サーブレットです。
2. これは、リモート制御トランザクション プロキシです。
3. これは Web サーバ サーブレットです。

APPENDIX B

シグニチャ エンジンについて

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

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

この付録では、IPS シグニチャ エンジンについて説明します。内容は次のとおりです。

シグニチャ エンジンについて

シグニチャ エンジンは、Cisco IPS のコンポーネントの 1 つで、特定のカテゴリに属する数多くのシグニチャをサポートするように設計されています。エンジンは、パーサーとインスペクタで構成されています。各エンジンには複数のパラメータがあり、許可される範囲や値が設定されます。

（注）　Cisco IPS エンジンで、標準化された正規表現がサポートされています。

Cisco IPS には次のシグニチャ エンジンが含まれています。

- AIC：Web トラフィックの包括的な分析を行います。AIC エンジンは、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。インスタント メッセージングや GotoMyPC など、指定したポート上でトンネリングを行おうとするアプリケーションに対する管理制御も可能です。また、AIC を使用して FTP トラフィックを調査し、実行中のコマンドを制御することもできます。AIC エンジンには、AIC FTP と AIC HTTP の 2 つがあります。
- Atomic：Atomic エンジンは、複数レベルの選択を使用して 4 つのエンジンに結合されます。1 つのシグニチャの中で、IP + TCP のように、レイヤ 3 とレイヤ 4 の属性を組み合わせることができます。Atomic エンジンでは、標準化された正規表現がサポートされています。Atomic エンジンは次の種類で構成されます。
  - Atomic ARP：レイヤ 2 ARP プロトコルを検査します。大半のエンジンはレイヤ 3 IP プロトコルに基づいているため、Atomic ARP エンジンはこの点で異なります。
  - Atomic IP Advanced：IPv6 レイヤ 3 および ICMPv6 レイヤ 4 トラフィックを検査します。
  - 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。

    このエンジンでは、IP ヘッダーおよびレイヤ 4 ヘッダーのフィールドに一致する値を指定でき、正規表現を使用してレイヤ 4 のペイロードを検査できます。

    （注）　すべての IP パケットは Atomic IP エンジンによって検査されます。このエンジンは、4.x Atomic ICMP、Atomic IP Options、Atomic L3 IP、Atomic TCP、および Atomic UDP エンジンに置き換わります。

  - 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 の 2 つの脆弱性を検出します。
- Fixed：固定の深さまで並行して正規表現一致を実行し、1 つの正規表現テーブルを使用して検査を停止します。Fixed エンジンには、CMP、TCP、および UDP の 3 つの種類があります。
- Flood：ホストおよびネットワークに向けられた ICMP および UDP フラッドを検出します。Flood エンジンには、Flood Host と Flood Net の 2 つの種類があります。
- 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 つのシグニチャに対して複数の文字列を照合することで、レイヤ 4 トランスポート プロトコルとペイロードを検査します。このエンジンは、ストリームベースの TCP と、単一の UDP および ICMP パケットを検査します。
- Normalizer：IP および TCP Normalizer が機能する方法を設定し、IP および TCP Normalizer 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：特定のプロトコルを扱います。Service エンジンは次のプロトコル タイプに分かれています。

- DNS：DNS（TCP および UDP）トラフィックを検査します。
- FTP：FTP トラフィックを検査します。
- FTP V2：IOS IPS をサポートします。

  このシグニチャ エンジンには、IOS IPS 用に調整されたプロトコル デコード エンジンが備わっています。このエンジンを使用しようとすると、エラー メッセージが表示されます。
- Generic：カスタム サービスおよびペイロードをデコードし、ネットワーク プロトコルを汎用的に分析します。
- H225：VoIP トラフィックを検査します。ネットワーク管理者が、VoIP ネットワーク宛の SETUP メッセージが有効であり、ポリシーで指定されている範囲内にあることを確認するために役立ちます。また、url-ids、email-ids、および表示情報などのアドレスおよび Q.931 文字列フィールドが特定の長さに準拠し、潜在的な攻撃パターンが含まれていないことを確認するためにも役立ちます。
- 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。
- HTTP V2：IOS IPS をサポートします。

  このシグニチャ エンジンには、IOS IPS 用に調整されたプロトコル デコード エンジンが備わっています。このエンジンを使用しようとすると、エラー メッセージが表示されます。
- 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。
- MSRPC：MSRPC トラフィックを検査します。
- MSSQL：Microsoft SQL トラフィックを検査します。
- NTP：NTP トラフィックを検査します。
- P2P：P2P トラフィックを検査します。
- RPC：RPC トラフィックを検査します。
- SMB Advanced：Microsoft SMB パケットと Microsoft DCE/RPC（MSRPC）over SMB パケットを処理します。

  （注） SMB エンジンは、SMB Advanced エンジンで置き換えられました。SMB エンジンが IDM、IME、CLI で表示される場合でも、そのシグニチャは廃止されています。つまり、新しいシグニチャには、対応する古いシグニチャの ID を使用して設定された古いパラメータがあります。SMB エンジンで使用していたカスタム シグニチャは、新しい SMB Advanced エンジンを使用して書き直してください。
- SMPT V1：IOS IPS をサポートします。

  このシグニチャ エンジンには、IOS IPS 用に調整されたプロトコル デコード エンジンが備わっています。このエンジンを使用しようとすると、エラー メッセージが表示されます。
- SNMP：SNMP トラフィックを検査します。
- SSH：SSH トラフィックを検査します。
- 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のステートフル検索を実行します。State エンジンには、状態遷移を定義するために使用される隠れたコンフィギュレーション ファイルがあるため、シグニチャの更新で新しい状態定義を提供できます。
- String：ICMP、TCP、または UDP プロトコルに基づいて、正規表現文字列を検索します。3 つの String エンジン、String ICMP、String TCP、および String UDP があります。

- String XL：ICMP、TCP、または UDP プロトコルに基づいて、正規表現文字列を検索します。String XL エンジンでは、正規表現アクセラレータ カード向けの最適化された操作が可能です。String エンジンには、String ICMP XL、String TCP XL、String UDP XL の 3 つの種類があります。

（注）　現時点で String XL エンジンと正規表現アクセラレータ カードをサポートしているのは、Cisco ASA 5585-X のみです。

（注）　正規表現アクセラレータ カードは、標準の String エンジンと新しい String XL エンジンの両方で使用されます。ほとんどの標準の String エンジンのシグニチャは、変更することなく、正規表現アクセラレータ カードでコンパイルおよび解析できます。ただし、標準の String エンジンのシグニチャを正規表現アクセラレータ カード向けにコンパイルできない特殊な状況があります。そのような状況では、新しいシグニチャは、正規表現アクセラレータ カードでコンパイルできない String XL エンジンの特定のパラメータを使用して、String XL エンジンで記述されます。String XL エンジンの新しいシグニチャにより、標準の String エンジンの元のシグニチャが廃止されます。

- 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スイープを分析します。Sweep エンジンには Sweep と Sweep Other TCP の 2 つの種類があります。
- Traffic Anomaly：TCP、UDP、およびその他のトラフィックのワームを検査します。
- 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。
- Trojan：BO2K や TFN2K などの標準的でないプロトコルのトラフィックを分析します。Trojan エンジンには、Bo2k、Tfn2k、および UDP の 3 つの種類があります。これらのエンジンには、ユーザが設定できるパラメータはありません。

Master エンジン

Master エンジンは、他のエンジンに対して構造体とメソッドを提供し、設定からの入力とアラート出力を処理します。ここでは、Master エンジンについて説明します。内容は次のとおりです。

一般的なパラメータ

次のパラメータは、Master エンジンの一部であり、すべてのシグニチャに適用されます（そのシグニチャ エンジンで意味を持つ場合）。

表 B-1 に、Master エンジンの一般的なパラメータの一覧を示します。

表 B-1　Master エンジンのパラメータ

パラメータ	説明	値
Signature ID	このシグニチャの ID を指定します。	*数値*
Sub Signature ID	このシグニチャのサブ ID を指定します。	*数値*
Alert Severity	アラートの重大度を指定します。 • 危険なアラート • 中レベルのアラート • 低レベルのアラート • 情報アラート	• High • Medium • Low • Informational（デフォルト）
Sig Fidelity Rating	このシグニチャの忠実度評価を指定します。	0 ～ 100 （デフォルト = 100）
Promiscuous Delta	アラートの重大度を決定するために使用されるデルタ値を指定します。	0 ～ 30 （デフォルト = 5）
Signature Name	シグニチャの名前を指定します。	*sig-name*
Alert Notes	アラート メッセージに含まれる、このシグニチャに関する追加情報を指定します。	*アラートの注記*
User Comments	このシグニチャに関するコメントを指定します。	*コメント*
Alert Traits	このシグニチャについて文書化する特性を指定します。	0 ～ 65335
Release	シグニチャが最後に更新されたリリースを指定します。	*リリース*
Signature Creation Date	シグニチャが作成された日付を指定します。	—
Signature Type	シグニチャのカテゴリを指定します。	• Anomaly • Component • Exploit • Other
Engine	シグニチャが属するエンジンを指定します。 **（注）** エンジン固有のパラメータは、Engine カテゴリの下に表示されます。	—
Event Count	アラートを生成するまでのイベントの発生回数を指定します。	1 ～ 65535 （デフォルト = 1）

表 B-1　Master エンジンのパラメータ（続き）

パラメータ	説明	値
Event Count Key	このシグニチャに関するイベントをカウントするストレージ タイプを指定します。 • 攻撃者のアドレス • 攻撃者と攻撃対象のアドレス • 攻撃者のアドレスと攻撃対象のポート • 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	• Axxx • AxBx • Axxb • xxBx • AaBb
Specify Alert Interval {Yes | No}	アラート間隔をイネーブルにします。 • 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。	2 ～ 1000
Status	シグニチャが、イネーブルとディセーブルのどちらであるか、アクティブと廃棄のどちらであるかを指定します。	Enabled | Retired {Yes | No}
Obsoletes	新しいシグニチャにより古いシグニチャがディセーブルになったことを示します。	—
Vulnerable OS List	パッシブ OS フィンガープリントと組み合わせることにより、IPS は、指定された攻撃がターゲット システムに該当する可能性が高いかどうかを判定します。	AIX BSD General OS HP-UX IOS IRIX Linux Mac OS Netware Other Solaris UNIX Windows Windows NT Windows NT/2K/XP
Mars Category {Yes | No}	シグニチャを MARS 攻撃カテゴリにマッピングします。[1]	—

1. 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。詳細は MARS のドキュメントを参照してください。

Promiscuous Delta

無差別モードの特定のアラートのリスク レーティングは、無差別デルタによって引き下げられます。センサーはターゲット システムの属性を認識せず、無差別モードではパケットを拒否できないため、無差別アラートの優先順位を下げ（低いリスク レーティングに基づきます）、よりリスク レーティングが高いアラートに管理者が注目できるようにすることは有用です。インライン モードでは、センサーで攻撃パケットを拒否し、ターゲット ホストに攻撃パケットが到達しないようにできるため、ターゲットに脆弱性があるかどうかは問題になりません。攻撃はネットワーク上で許可されなかったため、IPS によりリスク レーティングから差し引かれません。サービス、OS、またはアプリケーション固有

でないシグニチャの無差別デルタは 0 になります。シグニチャが OS、サービス、またはアプリケーション固有である場合、無差別デルタは、各カテゴリの 5 ポイントから計算された 5、10、または 15 になります。

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。

Obsoletes

シスコのシグニチャ チームは、obsoletes フィールドを使用して、新しくより適切なシグニチャで置き換えられた、廃止された古いシグニチャを示したり、エンジンのより優れたインスタンスが利用可能になったときに、エンジン内のディセーブルになったシグニチャを示します。たとえば、一部の String XL ハードウェア アクセラレーション シグニチャにより、String エンジンで定義されていた相当するシグニチャが置き換えられています。

Vulnerable OS List

シグニチャの脆弱 OS 設定とパッシブ OS フィンガープリントを組み合わせることで、IPS により特定の攻撃がターゲット システムに該当するかどうかを判定できます。攻撃が該当することがわかった場合、得られたアラートのリスク レーティング値が引き上げられます。一般にパッシブ OS フィンガープリント リストにエントリがないことが原因で、該当するかどうかが不明な場合、リスク レーティングは変更されません。パッシブ OS フィンガープリント エントリがあり、シグニチャの脆弱 OS 設定に一致しない場合、リスク レーティング値は引き下げられます。リスク レーティングの引き上げまたは引き下げ幅のデフォルト値は、+/- 10 ポイントです。

詳細情報

- 無差別モードの詳細については、「無差別モード」（P.7-13）を参照してください。
- パッシブ OS フィンガープリントの詳細については、「OS ID の設定」（P.11-25）を参照してください。

アラート頻度

アラート頻度パラメータの目的は、stick などの IDS DoS ツールに対抗するために、イベント ストアに書き込まれるアラートの量を削減することです。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。

表 B-2 にアラート頻度パラメータの一覧を示します。

表 B-2　Master エンジンのアラート頻度のパラメータ

パラメータ	説明	値
Alert Frequency	アラートをグループ化するためのサマリー オプション。	—
Summary Mode	サマライズで使用するモード。	—
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。	—
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。	—
Summarize	アラートをサマライズします。	—

表 B-2　Master エンジンのアラート頻度のパラメータ（続き）

パラメータ	説明	値
Summary Threshold	アラート数のしきい値。この値を超えるとシグニチャはサマリー モードに送られます。	0 ～ 65535
Global Summary Threshold	イベント数のしきい値。この値を超えるとアラートはグローバル サマリーにサマライズされます。	1 ～ 65535
Summary Interval	各サマリー アラートで使用される時間（秒数）。	1 ～ 1000
Summary Key	シグニチャをサマライズするストレージ タイプ：	Axxx
	• 攻撃者のアドレス	AxBx
	• 攻撃者と攻撃対象のアドレス	Axxb
	• 攻撃者のアドレスと攻撃対象のポート	xxBx
	• 攻撃対象のアドレス	AaBb
	• 攻撃者と攻撃対象のアドレスおよびポート	

イベント アクション

（注）　以下のイベント アクションのほとんどは、特定のエンジンに適していない場合を除き、各シグニチャ エンジンに属します。

以下のイベント アクション パラメータは、各シグニチャ エンジンに属します（そのシグニチャ エンジンにとって意味がある場合）。

- アラート アクションとログ アクション
  - Product Alert：アラートをイベント ストアに書き込みます。
  - Produce Verbose Alert：エンコード ダンプ（切り捨てられている可能性あり）を、アラートに含めます。
  - Log Attacker Packets：攻撃者のアドレスが格納されたパケットの IP ロギングを開始し、アラートを送信します。
  - Log Victim Packets：攻撃対象のアドレスが格納されたパケットの IP ロギングを開始し、アラートを送信します。
  - Log Attacker/Victim Pair Packets：（インライン モードのみ）攻撃者と攻撃対象のアドレス ペアが格納されたパケットの IP ロギングを開始します。
  - Request SNMP Trap：NotificationApp に、SNMP 通知を実行するための要求を送信します。
- 拒否アクション
  - Deny Packet Inline：（インライン モードのみ）このパケットを送信しません。

    （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 モードのみ）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 モードのみ）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 モードのみ）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 モードのみ）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送信しません。

（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。各拒否アドレスは、拒否が開始される原因となった最初のイベントから *X* 秒間でタイムアウトします。X は管理者が設定した秒数です。すべての拒否攻撃者エントリをクリアするには、[Monitoring] > [Properties] > [Denied Attackers] > [Clear List] の順に選択します。これにより、そのアドレスがネットワーク上で元のとおり許可されます。

- Modify Packet Inline :（インライン モードのみ）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、Normalizer Engine の一部です。これは、パケットをスクラブし、不正チェックサム、範囲外の値、その他の RFC 違反など、不規則な問題を修正します。

- その他のアクション

（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] : ARC に対してこの接続をブロックするよう要求します。
- [Request Block Host] : ARC に対してこの攻撃者ホストをブロックするよう要求します。
- [Request Rate Limit] : ARC に対してレート制限を実行するよう要求します。
- [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。

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。

正規表現の構文

正規表現（Regex）は、テキストを記述する手段として、強力で柔軟性のある表記言語です。パターンマッチングでは、正規表現によりあらゆる任意のパターンを簡潔に表記できます。

表 B-3 に、IPS シグニチャの正規表現構文の一覧を示します。

表 B-3　シグニチャの正規表現構文

メタ文字	名前	説明
?	疑問符	0 回または 1 回の繰り返し。
*	星印（アスタリスク）	0 回以上の繰り返し。
+	プラス	1 回以上の繰り返し。
{x}	量指定子	ちょうど *X* 回の繰り返し。
{x,}	最小量指定子	少なくとも *X* 回の繰り返し。
.	ドット	改行（0x0A）以外の任意の 1 文字。
[abc]	文字クラス	リスト内の任意の 1 文字。
[^abc]	否定文字クラス	リストにない任意の 1 文字。
[a-z]	文字範囲クラス	範囲内（両端も含む）の任意の 1 文字。
( )	カッコ	他のメタ文字の適用範囲を制限する際に使用する。
|	論理和（OR）	このメタ文字によって区切られている複数の表現のいずれかと一致します。
^	キャレット	行の先頭。
¥*char*	エスケープ文字。	*char* がメタ文字である場合も含めて、*char* そのものと一致する。
char	文字	char がメタ文字でない場合は、char そのものと一致する。
¥r	復帰	復帰文字（0x0D）と一致する。
¥n	改行	改行文字（0x0A）と一致する。
¥t	Tab	タブ文字（0x09）と一致する。
¥f	フォーム フィード	フォーム フィード文字（0x0C）と一致する。

表 B-3　シグニチャの正規表現構文（続き）

メタ文字	名前	説明
¥xNN	エスケープされた 16 進数文字	16 進コード 0xNN（0<=N<=F）を持つ文字と一致する。
¥NNN	エスケープされた 8 進数文字	8 進コード NNN（0<=N<=8）を持つ文字と一致する。

繰り返し演算子ではいずれの場合も、該当する文字列のうち最も短いものが一致対象となります。一方、それ以外の演算子では、その適用範囲に最大限多くの文字が取り込まれるため、該当する文字列のうち最も長いものが一致対象となります。

表 B-4 は、正規表現のパターンの例を示したものです。

表 B-4　正規表現のパターン

一致対象	正規表現
Hacker	Hacker
Hacker または hacker	[Hh]acker
bananas、banananas、bananananananas など、一定の規則で構成されたすべての文字列	ba(na)+s
同じ行の中にある foo と bar の間に改行以外の文字が 0 個以上ある文字列	foo.*bar
foo または bar	foo|bar
moon または soon	(m|s)oon

特殊文字

表 B-5 に、正規表現アクセラレータ カードの特殊文字とその 16 進表現の一覧を示します。リテラル文字は正規表現のメタ文字です。これらの文字を検査対象のトラフィックと照合するためには、文字の 16 進表現を使用します。

表 B-5　特殊文字

リテラル文字	16 進表現
.	¥x2e
[	¥x5b
]	¥x5d
-	¥x2d
^	¥x5e
¥	¥x5c
/	¥x2f
*	¥x2a
+	¥x2b
?	¥x3f
{	¥x7b

表 B-5　特殊文字（続き）

リテラル文字	16 進表現
}	¥x7d
“	¥x22
(	¥x28
)	¥x29

詳細情報

これらの特殊文字を使用する 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。

AIC エンジン

Application Inspection and Control（AIC）エンジンは、HTTP Web トラフィックを検査し、FTP コマンドを強制します。ここでは、AIC エンジンとそのパラメータについて説明します。内容は次のとおりです。

AIC エンジンについて

AIC は、Web トラフィックの包括的な分析を行います。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。インスタント メッセージングや GotoMyPC など、指定したポート上でトンネリングを行おうとするアプリケーションに対する管理制御も可能です。P2P やインスタント メッセージの検査とポリシー チェックは、これらのアプリケーションが HTTP 上で動作している場合に可能です。また、AIC は、FTP トラフィックを調査し、実行中のコマンドを制御するための手段も備えています。定義済みのシグニチャをイネーブルまたはディセーブルにしたり、カスタム シグニチャを通じてポリシーを作成できます。

（注）　AIC エンジンは、AIC Web ポートで HTTP トラフィックを受信したときに実行されます。トラフィックが Web トラフィックであるものの、AIC Web ポートで受信されなかった場合は、Service HTTP エンジンが実行されます。AIC の検査は、ポートが AIC Web ポートとして設定されており、検査対象のトラフィックが HTTP トラフィックであれば、任意のポートで実行できます。

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。

AIC エンジンのパラメータ

AIC エンジンでは、Web トラフィックを詳細に検査するためのシグニチャが定義されています。また、FTP コマンドを認証および強制するためのシグニチャも定義されています。AIC エンジンには、AIC HTTP と AIC FTP の 2 つがあります。

AIC エンジンには、次の機能が搭載されています。

- Web トラフィック
  - RFC 準拠強制
  - HTTP 要求方法の認証と強制
  - 応答メッセージの検証
  - MIME タイプの適用
  - 転送符号化タイプの検証
  - メッセージ コンテンツと転送データの種類に基づくコンテンツ制御
  - URI 長さ強制
  - 設定されたポリシーとヘッダーに従ったメッセージ サイズ強制
  - トンネリング、P2P、およびインスタント メッセージ強制。

    この強制は、正規表現を通じて実行されます。定義済みのシグニチャがありますが、ユーザがリストを拡張できます。
- FTP トラフィック
  - FTP コマンドの承認と強制

表 B-6 に、AIC HTTP エンジンに固有のパラメータを示します。

表 B-6　AIC HTTP エンジンのパラメータ

パラメータ	説明
Signature Type	AIC デバイスの種類。
Content Types	MIME タイプを扱う AIC シグニチャ。 • [Define Content Type] : 特定の MIME タイプ（image/gif）の拒否、メッセージサイズ違反の定義、ヘッダーと本文で宣言されている MIME タイプの不一致の判定などのアクションを関連付けます。 • [Define Recognized Content Types] : センサーによって認識されたコンテンツ タイプを一覧表示します。
Define Web Traffic Policy	非準拠の HTTP トラフィックを認識した場合に実行するアクションを指定します。[Alert on Non-HTTP Traffic Yes | No] はシグニチャをイネーブルにします。このシグニチャは、デフォルトではディセーブルになっています。

表 B-6　AIC HTTP エンジンのパラメータ（続き）

パラメータ	説明
Max Outstanding Requests Overrun	接続あたりに許可される最大 HTTP 要求（1 ～ 16）。
Msg Body Pattern	メッセージ本文の中の特定のパターンを探すシグニチャを定義するには、正規表現を使用します。
Request Methods	HTTP 要求方法にアクションを関連付けることができる AIC シグニチャ。 • [Define Request Method]：get、put など。 • [Recognized Request Methods]：センサーによって認識される方法の一覧を表示します。
Transfer Encoding	AIC 転送符号化を扱うシグニチャ。 • [Define Transfer Encoding]：compress、chunked などのアクションを各方法に関連付けます。 • [Recognized Transfer Encodings]：センサーによって認識される方法の一覧を表示します。 • [Chunked Transfer Encoding]：エラーは、チャンク エンコーディング エラーが認識された場合に実行するアクションを指定します。

表 B-7 に、AIC FTP エンジンに固有のパラメータを示します。

表 B-7　AIC FTP エンジンのパラメータ

パラメータ	説明
Signature Type	AIC シグニチャのタイプを指定します。
FTP Commands	アクションを FTP コマンドに関連付けます。 • [FTP Command]：検査する FTP コマンドを選択できます。
Unrecognized FTP Command	認識されない FTP コマンドを検査します。

詳細情報

- AIC エンジンのシグニチャの設定手順については、「Application Policy シグニチャの設定」（P.9-37）を参照してください。
- カスタム AIC シグニチャの例については、「AIC シグニチャの調整」（P.9-45）を参照してください。
- すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。
- シグニチャの正規表現構文の一覧については、「正規表現の構文」（P.B-10）を参照してください。

Atomic エンジン

Atomic エンジンには、アラートを発生する、単純な単一 パケット条件のシグニチャが含まれています。ここでは、Atomic エンジンについて説明します。内容は次のとおりです。

- 「Atomic IP Advanced エンジン」（P.B-16）
- 「Atomic IP エンジン」（P.B-27）
- 「Atomic IPv6 エンジン」（P.B-30）

Atomic ARP エンジン

Atomic ARP エンジンは、レイヤ 2 の基本的な ARP シグニチャを定義し、ARP スプーフィング ツールである dsniff と ettercap に対して高度な検出を実行します。

表 B-8 に、Atomic ARP エンジンに固有のパラメータを示します。

表 B-8　Atomic ARP エンジンのパラメータ

パラメータ	説明	値
Specify ARP Operation	（任意）ARP 動作をイネーブルにします。 • [ARP Operation]：検査する ARP 動作の種類。	0 ～ 65535
Specify Mac Flip Times	（任意）MAC アドレス フリップ回数をイネーブルにします。 • [Mac Flip Times]：アラート中で何度 MAC アドレスを反転させるかを指定します。	0 ～ 65535
Specify Request Inbalance	（任意）要求のアンバランスをイネーブルにします。 • [Request Inbalance]：特定の IP アドレスに対して、応答よりも要求の方が指定した数より多い場合に、アラートを起動します。	0 ～ 65535

表 B-8　Atomic ARP エンジンのパラメータ（続き）

パラメータ	説明	値
Specify Type of ARP Sig	（任意）ARP シグニチャのタイプをイネーブルにします。 • [Type of ARP Sig]：発行する ARP シグニチャのタイプを指定します。 – [Destination Broadcast]：255.255.255.255 の ARP 宛先アドレスを検出した場合に、このシグニチャのアラートを起動します。 – [Same Source and Destination]：送信元と宛先の MAC アドレスが同じである ARP 宛先アドレスを検出した場合に、このシグニチャのアラートを起動します。 – [Source Broadcast]（デフォルト）：255.255.255.255 の ARP 送信元アドレスを検出した場合に、このシグニチャのアラートを起動します。 – [Source Multicast]：ARP 送信元 MAC アドレス 01:00:5e:（00-7f）を検出した場合に、このシグニチャのアラートを起動します。	Dst Broadcast Same Src and Dst Src Broadcast Src Multicast
Storage Key	固定データを保存するために使用するアドレス キーのタイプ。 • 攻撃者のアドレス • 攻撃者と攻撃対象のアドレス • 攻撃対象のアドレス • グローバル	Axxx AxBx xxBx xxxx

詳細情報

すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Atomic IP Advanced エンジン

ここでは、Atomic IP Advanced エンジンについて説明します。内容は次のとおりです。

Atomic IP Advanced エンジンについて

Atomic IP Advanced エンジンは、IPv6 ヘッダーとその拡張、IPv4 ヘッダーとそのオプション、ICMP、ICMPv6、TCP、および UDP を解析および解釈し、通常でないアクティビティを示す異常を探します。

Atomic IP Advanced エンジンのシグニチャは次のことを実行します。

- 偽造された IP アドレスなど、IP アドレスの異常を検査します
- パケットの長さフィールドの不正な情報の検査
- パケットに関する情報アラートの起動
- 限定的な既知の脆弱性についての重大度が高いアラートの起動
- Engine Atomic IP における、IPv6 にも適用可能な IPv6 固有のシグニチャの複製
- IP アドレス、ポート、プロトコル、パケット データからの限定的なデータに基づく、トンネリングされたトラフィックを識別するためのデフォルト シグニチャの提供

最も外側の IP トンネルのみが認識されます。IPv4 トンネルの内部に IPv6 トンネルまたは IPv6 トラフィックが検出された場合、シグニチャによりアラートが起動されます。埋め込みトンネルの中の他のすべての IPv6 トラフィックは検査されません。次のトンネリング方法がサポートされていますが、個別には検出されません。たとえば、ISATAP、6to4、および手動 IPv6 RFC 4213 トンネルは、すべて IPv4 の中の IPv6 として認識され、シグニチャ 1007 によって検出されます。

- ISATAP
- 6to4（RFC 3056）
- 手動で設定されたトンネル（RFC 4213）
- IPv6 over GRE
- UDP の中の Teredo（IPv6）
- MPLS（暗号化なし）
- IPv6 over IPv6

IPv6 は次の機能をサポートしています。

- 送信元 IP アドレス、宛先 IP アドレス、または IP アドレスのペアによる拒否
- アラート
- TCP 接続のリセット
- ロギング

詳細情報

- カスタム Atomic IP Advanced シグニチャの例については、「Atomic IP Advanced エンジンのシグニチャの例」（P.9-26）を参照してください。
- Atomic IP Advanced エンジンの制限事項の一覧については、「Atomic IP Advanced エンジンの制限事項」（P.B-18）を参照してください。
- Atomic IP Advanced エンジンのパラメータの一覧については、「Atomic IP Advanced エンジンのパラメータ」（P.B-18）を参照してください。
- すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Atomic IP Advanced エンジンの制限事項

Atomic IP Advanced エンジンには次の制限があります。

- パケットがフラグメント化されており、レイヤ 4 ID が最初のパケットに現れない場合、パケットのレイヤ 4 フィールドを検出できません。
- フラグメントの組み立てがないため、IPv6 によってフラグメント化されたパケットを使用したフロー中のレイヤ 4 攻撃を検出できません。
- トンネリングされたフローを使用した攻撃を検出できません。
- フラグメンテーション ヘッダーについては限定的なチェックが行われます。
- AIM IPS および NME IPS では、IPv6 の機能がサポートされていません。これは、それらがインストールされているルータにより IPv6 データが送信されないためです。IPv6 検査は、IDSM2 上で動作する可能性がありますが、正式にはサポートされていません。管理（コマンドおよび制御）インターフェイス上では IPv6 がサポートされていません。ASA 8.2(1) では、AIP SSM および AIP SSC-5 で IPv6 の機能がサポートされています。ASA 8.2(4) では、IPS SSP により IPv6 の機能がサポートされています。
- 不正な重複ヘッダーがある場合、シグニチャが起動されますが、個々のヘッダーは個別に検査されません。
- 異常検出では IPv6 トラフィックがサポートされておらず、IPv4 トラフィックのみが異常検出プロセッサに渡されます。
- レート制限およびブロッキングは、IPv6 トラフィックではサポートされていません。ブロック アクションまたはレート制限アクションが設定されているシグニチャが IPv6 トラフィックによってトリガーされると、アラートが生成されますが、アクションは実行されません。

詳細情報

- カスタム Atomic IP Advanced シグニチャの例については、「Atomic IP Advanced エンジンのシグニチャの例」（P.9-26）を参照してください。
- Atomic IP Advanced エンジンのパラメータの一覧については、「Atomic IP Advanced エンジンのパラメータ」（P.B-18）を参照してください。
- すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Atomic IP Advanced エンジンのパラメータ

（注）　各範囲の 2 番目の数は、最初の数と同じかそれより大きいことが必要です。

表 B-9 に、Atomic IP Advanced エンジン固有のパラメータを示します。

表 B-9　Atomic IP Advanced エンジンのパラメータ

パラメータ	説明	値
Global		
Fragment Status	フラグメントが必要かどうかを指定します。	Any | No Fragments | Want Fragments

表 B-9　Atomic IP Advanced エンジンのパラメータ（続き）

パラメータ	説明	値
Specify Encapsulation	（任意）パケットの L3 の開始前にカプセル化を指定します。[1] • [Encapsulation]：検査するカプセル化の種類。	None | MPLS | GRE | Ipv4 in IPv6 | IP IP | Any
Specify IP Version	（任意）IP プロトコル バージョンを指定します。 • [IP Version]：IPv4 または IPv6。	IPv4| IPv6
Swap Attacker Victim	攻撃者と攻撃対象のアドレスとポート（送信元および宛先）を、アラート メッセージとアクションで入れ替える場合は [Yes]。入れ替えない場合は [No]（デフォルト）。	[Yes] | [No]
Regex		
Specify Regex Inspection	（任意）正規表現検査をイネーブルにします。	[Yes] | [No]
Regex Scope	検索の開始および終了場所を指定します。	• ipv6-doh-only • ipv6-doh-plus • ipv6-hoh-only • ipv6-hoh-plus • ipv6-rh-only • ipv6-rh-plus • layer3-only • layer3-plus • layer4
Regex String	単一の TCP パケット内で検索する正規表現を指定します。	string
Specify Exact Match Offset	完全一致オフセットをイネーブルにします。 • [Exact Match Offset]：一致が有効であるために、[Regex String] が報告する必要がある正確なストリーム オフセット。	0 ～ 65535
Specify Minimum Match Length	最小一致長をイネーブルにします。 • [Minimum Match Length]：[Regex String] が一致する必要がある最小バイト数を指定します。	0 ～ 65535
Specify Minimum Match Offset	最小一致オフセットをイネーブルにします。 • [Minimum Match Offset]：一致が有効であるために [Regex String] が報告する必要がある、最小ストリーム オフセットを指定します。	0 ～ 65535
Specify Maximum Match Offset	最大一致オフセットをイネーブルにします。 • [Maximum Match Offset]：一致が有効であるために [Regex String] が報告する必要がある、最大ストリーム オフセットを指定します。	0 ～ 65535

表 B-9　Atomic IP Advanced エンジンのパラメータ（続き）

パラメータ	説明	値
IPv6		
Specify Authentication Header	（任意）認証ヘッダーの検査をイネーブルにします。 • [AH Present]：認証ヘッダーが存在することを指定します。 – [AH Length]：認証ヘッダーの長さを指定します。 – [AH Next Header]：認証ヘッダーの値を指定します。	Have AH | No AH 0 ～ 1028 0 ～ 255
Specify Destination Options Header	（任意）宛先オプション ヘッダーの検査をイネーブルにします。 • [DOH Present]：宛先オプション ヘッダーが存在することを指定します。 – [DOH Count]：検査する宛先オプション ヘッダーの数を指定します。 – [DOH Length]：検査する宛先オプション ヘッダーの長さを指定します。 – [DOH Next Header]：検査する次の宛先オプション ヘッダーの数を指定します。 – [DOH Option Type]：検査する宛先オプション ヘッダーのタイプを指定します。 – [DOH Option Length]：検査する宛先オプション ヘッダーの長さを指定します。	Have DOH | No DOH 0 ～ 2 8 ～ 2048 0 ～ 255 0 ～ 255 0 ～ 255
Specify ESP Header	（任意）ESP ヘッダーの検査をイネーブルにします。 • [ESP Present]：ESP ヘッダーが存在することを指定します。	Have ESP | No ESP
Specify First Next Header	（任意）最初の次ヘッダーの検査をイネーブルにします。 • [First Next Header]：検査する最初の次ヘッダーの値を指定します。	0 ～ 255
Specify Flow Label	（任意）フロー ラベルの検査をイネーブルにします。 • [Flow Label]：検査するフロー ラベルの値を指定します。	0 ～ 1048575
Specify Headers Out of Order	（任意）順序が不正なヘッダーの検査をイネーブルにします。 • [Headers Out of Order]：検査するヘッダーの順序を指定します。	[Yes] | [No]

表 B-9　Atomic IP Advanced エンジンのパラメータ（続き）

パラメータ	説明	値
Specify Headers Repeated	（任意）繰り返しヘッダーの検査をイネーブルにします。 • [Headers Repeated]：検査するヘッダーの繰り返しを指定します。	[Yes] | [No]
Specify Hop Limit	（任意）ホップ制限をイネーブルにします。 • [Hop Limit]：検査するホップ制限の値を指定します。	0 ～ 255
Specify Hop Options Header	（任意）ホップバイホップ オプション ヘッダーの検査をイネーブルにします。 • [HOH Present]：ホップバイホップ オプション ヘッダーが存在することを指定します。	Have HOH | No HOH
Specify IPv6 Address Options	（任意）IPv6 アドレス オプションをイネーブルにします。 • [IPv6 Address Options]：IPv6 アドレス オプションを指定します。 – [Address With Localhost]：::1 の IP アドレス。 – [Documentation Address]：プレフィクスが 2001:db8::/32 の IP アドレス。 – [IPv6 Address]：IP アドレス。 – [Link Local Address]：IPv6 リンクローカル アドレスを検査します。 – [Multicast Destination]：宛先マルチキャスト アドレスを検査します。 – [Multicast Source]：送信元マルチキャスト アドレスを検査します。 – [Not Link Local Address]：リンクローカルでないアドレスを検査します。 – [Not Valid Address]：リンクローカル、グローバル、またはマルチキャスト用に予約されていないアドレスを検査します。 – [Source IP Equals Destination IP]：送信元アドレスと宛先アドレスは同じです。	
Specify IPv6 Data Length	（任意）IPv6 データ長の検査をイネーブルにします。 • [IPv6 Data Length]：検査する IPv6 データ長を指定します。	0 ～ 65535

表 B-9　Atomic IP Advanced エンジンのパラメータ（続き）

パラメータ	説明	値
Specify IPv6 Header Length	（任意）IPv6 ヘッダー長の検査をイネーブルにします。 • [Pv6 Header Length]：検査する IPv6 ヘッダーの長さを指定します。	0 ～ 65535
Specify IPv6 Total Length	（任意）IPv6 合計長の検査をイネーブルにします。 • [IPv6 Total Length]：検査する IPv6 合計長を指定します。	0 ～ 65535
Specify IPv6 Payload Length	（任意）IPv6 ペイロード長の検査をイネーブルにします。 • [IPv6 Payload Length]：検査する IPv6 ペイロード長を指定します。	0 ～ 65535
Specify Routing Header	（任意）ルーティング ヘッダーの検査をイネーブルにします。 • [RH Present]：ルーティング ヘッダーが存在することを指定します。	Have RH | No RH
Specify Traffic Class	（任意）トラフィック クラスの検査をイネーブルにします。 • [Traffic Class]：検査するトラフィック クラスの値を指定します。	0 ～ 255
IPV4		
Specify IP Addr Options	（任意）IP アドレス オプションをイネーブルにします。 • [IP Addr Options]：IP アドレス オプションを指定します。	Address With Localhost IP Address RFC 1918 Address Src IP Eq Dst IP
Specify IP Header Length	（任意）IP ヘッダー長の検査をイネーブルにします。 • [IP Header Length]：検査する IP ヘッダーの長さを指定します。	0 ～ 16
Specify IP Identifier	（任意）IP ID の検査をイネーブルにします。 • [IP Identifier]：検査する IP ID を指定します。	0 ～ 255

表 B-9　Atomic IP Advanced エンジンのパラメータ（続き）

パラメータ	説明	値
Specify IP Option Inspection	（任意）IP オプションの検査をイネーブルにします。 • [IP Option Inspection]：IP オプションの値を指定します。 – [IP Option]：照合する IP オプション コード。 – [IP Option Abnormal Options]：不正なオプションのリスト。	0 ～ 65535 [Yes] | [No]
Specify IP Payload Length	（任意）IP ペイロード長の検査をイネーブルにします。 • [IP Payload Length]：検査する IP ペイロードの長さを指定します。	0 ～ 65535
Specify IP Type of Service	（任意）IP タイプ オブ サービスを指定します。 • [IP Type of Service]：検査する IP タイプ オブ サービスを指定します。	0 ～ 255
Specify IP Total Length	（任意）IP 合計長の検査をイネーブルにします。 • [IP Total Length]：検査する IP パケットの合計長を指定します。	0 ～ 65535
Specify IP Time-to-Live	（任意）IP 存続可能時間の検査をイネーブルにします。 • [IP Time-to-Live]：IP TTL の検査を指定します。	0 ～ 255
Specify IP Version	（任意）IP バージョンの検査をイネーブルにします。 • [IP Version]：検査する IP バージョンを指定します。	0 ～ 16
L4 Protocol		
Specify L4 Protocol	（任意）L4 プロトコルの検査をイネーブルにします。 • [L4 Protocol]：検査する L4 プロトコルを指定します。	ICMP Protocol ICMPv6 Protocol TCP Protocol UDP Protocol Other IP Protocols
L4 Protocol Other		
Other IP Protocol ID	（任意）他の L4 プロトコルの検査をイネーブルにします。 • [Other IP Protocol ID]：アラートを送信する単一の IP プロトコル番号を指定します。	0 ～ 256
L4 Protocol ICMP		

表 B-9　Atomic IP Advanced エンジンのパラメータ（続き）

パラメータ	説明	値
Specify ICMP Code	（任意）L4 ICMP コードの検査をイネーブルにします。 • [ICMP Code] : ICMP ヘッダーの CODE 値を指定します。	0 ～ 65535
Specify ICMP ID	（任意）L4 ICMP ID の検査をイネーブルにします。 • [ICMP ID] : ICMP ヘッダーの IDENTIFIER 値を指定します。	0 ～ 65535
Specify ICMP Sequence	（任意）L4 ICMP シーケンスの検査をイネーブルにします。 • [ICMP Sequence] : 検査する ICMP シーケンスを指定します。	0 ～ 65535
Specify ICMP Type	（任意）ICMP ヘッダー タイプの検査をイネーブルにします。 • [ICMP Type] : ICMP ヘッダーの TYPE 値を指定します。	0 ～ 65535
L4 Protocol ICMPv6		
Specify ICMPv6 Code	（任意）L4 ICMPv6 コードの検査をイネーブルにします。 • [ICMPv6 Code] : ICMPv6 ヘッダーの CODE 値を指定します。	0 ～ 255
Specify ICMPv6 ID	（任意）L4 ICMPv6 ID の検査をイネーブルにします。 • [ICMPv6 ID] : ICMPv6 ヘッダーの IDENTIFIER 値を指定します。	0 ～ 65535
Specify ICMPv6 Length	（任意）L4 ICMPv6 の長さの検査をイネーブルにします。 • [ICMPv6 Length] : ICMPv6 ヘッダーの LENGTH 値。	0 ～ 65535
Specify ICMPv6 MTU Field	（任意）L4 ICMPv6 の MTU フィールドの検査をイネーブルにします。 • [ICMPv6 MTU Field] : ICMPv6 ヘッダーの MTU フィールドの値。	4,294,967,295
Specify ICMPv6 Option Type	（任意）L4 ICMPv6 タイプの検査をイネーブルにします。 • [ICMPv6 Option Type] : 検査する ICMPv6 オプション タイプを指定します。	0 ～ 255
Specify ICMPv6 Option Length	（任意）L4 ICMPv6 オプション タイプの検査をイネーブルにします。 • [ICMPv6 Option Length] : 検査する ICMPv6 オプション タイプを指定します。	0 ～ 255

表 B-9　Atomic IP Advanced エンジンのパラメータ（続き）

パラメータ	説明	値
Specify ICMPv6 Sequence	（任意）L4 ICMPv6 シーケンスの検査をイネーブルにします。 • [ICMPv6 Sequence]：ICMPv6 ヘッダーの SEQUENCE 値。	0 ～ 65535
Specify ICMPv6 Type	（任意）L4 ICMPv6 タイプの検査をイネーブルにします。 • [ICMPv6 Type]：ICMPv6 ヘッダーの TYPE 値。	0 ～ 255
L4 Protocol TCP and UDP		
Specify Destination Port	（任意）宛先ポートの使用を指定します。 • [Destination Port]：このシグニチャが対象にする宛先ポート。	0 ～ 65535
Specify Source Port	（任意）送信元ポートの使用を指定します。 • [Source Port]：このシグニチャが対象にする送信元ポート。	0 ～ 65535
Specify TCP Mask	（任意）TCP マスクの使用を指定します。 • [TCP Mask]：TCP フラグの比較で使用するマスク。 – URG ビット – ACK ビット – PSH ビット – RST ビット – SYN ビット – FIN ビット	• URG • ACK • PSH • RST • SYN • FIN
Specify TCP Flags	（任意）TCP フラグの使用をイネーブルにします。 • [TCP Flags]：マスクによってマスクされた場合に照合する TCP フラグ。 – URG ビット – ACK ビット – PSH ビット – RST ビット – SYN ビット – FIN ビット	• URG • ACK • PSH • RST • SYN • FIN
Specify TCP Reserved	（任意）TCP 予約の使用をイネーブルにします。 • [TCP Reserved]：TCP 予約。	0 ～ 63

表 B-9　Atomic IP Advanced エンジンのパラメータ（続き）

パラメータ	説明	値
Specify TCP Header Length	（任意）L4 TCP ヘッダー長の検査をイネーブルにします。 • [TCP Header Length]：検査で使用する TCP ヘッダーの長さを指定します。	0 ～ 60
Specify TCP Payload Length	（任意）L4 TCP ペイロード長の検査をイネーブルにします。 • [TCP Payload Length]：TCP ペイロードの長さを指定します。	0 ～ 65535
Specify TCP URG Pointer	（任意）L4 TCP の URG ポインタの検査をイネーブルにします。 • [TCP URG Pointer]：TCP URG フラグの検査を指定します。	0 ～ 65535
Specify TCP Window Size	（任意）L4 TCP ウィンドウ サイズの検査をイネーブルにします。 • [TCP Window Size]：TCP パケットのウィンドウ サイズを指定します。	0 ～ 65535
Specify UDP Valid Length	（任意）L4 UDP の有効長の検査をイネーブルにします。 • [UDP Valid Length]：有効であると見なし検査しない UDP パケット長を指定します。	0 ～ 65535
Specify UDP Length Mismatch	（任意）L4 UDP の長さの不一致の検査をイネーブルにします。 • [UDP Length Mismatch]：IP データ長が UDP ヘッダー長よりも小さい場合にアラートを起動します。	[Yes] | [No]

1. パケットが GRE、IPIP、IPv4inIPv6、または MPL である場合、センサーは L3 カプセル化ヘッダーとカプセル化ヘッダーをスキップし、すべての検査は 2 番目の L3 から開始されます。カプセル化列挙機能により、エンジンは前の情報を参照し、問題の L3 の前にカプセル化ヘッダーがあるかどうかを確認します。

詳細情報

- カスタム Atomic IP Advanced シグニチャの例については、「Atomic IP Advanced エンジンのシグニチャの例」（P.9-26）を参照してください。
- Atomic IP Advanced エンジンの制限事項の一覧については、「Atomic IP Advanced エンジンの制限事項」（P.B-18）を参照してください。
- すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。
- シグニチャの正規表現構文の一覧については、「正規表現の構文」（P.B-10）を参照してください。

Atomic IP エンジン

Atomic IP エンジンでは、IP プロトコル ヘッダーおよび関連付けられたレイヤ 4 トランスポート プロトコル（TCP、UDP、および ICMP）とペイロードを検査するシグニチャを定義します。Atomic エンジンでは、複数のパケットにまたがる固定データは保存されません。その代わりに、1 つのパケットの解析を基にしてアラートを起動できます。

表 B-10 に、Atomic IP エンジンに固有のパラメータを示します。

表 B-10　Atomic IP エンジンのパラメータ

パラメータ	説明	値
Specify IP Addr Options	（任意）IP アドレス オプションをイネーブルにします。 • [IP Addr Options] : IP アドレス オプションを指定します。	Address With Localhost IP Address RFC 1918 Address Src IP Eq Dst IP
Specify IP Header Length	（任意）IP ヘッダー長の検査をイネーブルにします。 • [IP Header Length] : 検査する IP ヘッダーの長さを指定します。	0 ～ 16
Specify IP Identifier	（任意）IP ID の検査をイネーブルにします。 • [IP Identifier] : 検査する IP ID を指定します。	0 ～ 255
Specify IP Option Inspection	（任意）IP オプションの検査をイネーブルにします。 • [IP Option Inspection] : IP オプションの値を指定します。 – [IP Option] : 照合する IP オプション コード。 – [IP Option Abnormal Options] : 不正なオプションのリスト。	0 ～ 65535 [Yes] | [No]
Specify IP Payload Length	（任意）IP ペイロード長の検査をイネーブルにします。 • [IP Payload Length] : 検査する IP ペイロードの長さを指定します。	0 ～ 65535
Specify IP Type of Service	（任意）IP タイプ オブ サービスを指定します。 • [IP Type of Service] : 検査する IP タイプ オブ サービスを指定します。	0 ～ 6255

表 B-10　Atomic IP エンジンのパラメータ（続き）

パラメータ	説明	値
Specify IP Total Length	（任意）IP 合計長の検査をイネーブルにします。 • [IP Total Length]：検査する IP パケットの合計長を指定します。	0 ～ 65535
Specify IP Time-to-Live	（任意）IP 存続可能時間の検査をイネーブルにします。 • [IP Time-to-Live]：IP TTL の検査を指定します。	0 ～ 255
Specify IP Version	（任意）IP バージョンの検査をイネーブルにします。 • [IP Version]：検査する IP バージョンを指定します。	0 ～ 16
Specify L4 Protocol	（任意）L4 プロトコルの検査をイネーブルにします。 • [L4 Protocol]：検査する L4 プロトコルを指定します。	ICMP Protocol TCP Protocol UDP Protocol Other IP Protocols
Specify ICMP Code	（任意）L4 ICMP コードの検査をイネーブルにします。 • [ICMP Code]：ICMP ヘッダーの CODE 値を指定します。	0 ～ 65535
Specify ICMP ID	（任意）L4 ICMP ID の検査をイネーブルにします。 • [ICMP ID]：ICMP ヘッダーの IDENTIFIER 値を指定します。	0 ～ 65535
Specify ICMP Sequence	（任意）L4 ICMP シーケンスの検査をイネーブルにします。 • [ICMP Sequence]：検査する ICMP シーケンスを指定します。	0 ～ 65535
Specify ICMP Type	（任意）ICMP ヘッダー タイプの検査をイネーブルにします。 • [ICMP Type]：ICMP ヘッダーの TYPE 値を指定します。	0 ～ 65535
Specify ICMP Total Length	（任意）L4 ICMP 合計ヘッダー長の検査をイネーブルにします。 • [ICMP Total Length]：検査する ICMP 合計長の値を指定します。	0 ～ 65535
Other IP Protocol ID	（任意）他の L4 プロトコルの検査をイネーブルにします。 • [Other IP Protocol ID]：アラートを送信する単一の IP プロトコル番号を指定します。	0 ～ 256

表 B-10　Atomic IP エンジンのパラメータ（続き）

パラメータ	説明	値
Specify Destination Port	（任意）宛先ポートの使用を指定します。 • [Destination Port]：このシグニチャが対象にする宛先ポート。	0 ～ 65535
Specify Source Port	（任意）送信元ポートの使用を指定します。 • [Source Port]：このシグニチャが対象にする送信元ポート。	0 ～ 65535
Specify TCP Mask	（任意）TCP マスクの使用を指定します。 • [TCP Mask]：TCP フラグの比較で使用するマスク。 – URG ビット – ACK ビット – PSH ビット – RST ビット – SYN ビット – FIN ビット	• URG • ACK • PSH • RST • SYN • FIN
Specify TCP Flags	（任意）TCP フラグの使用をイネーブルにします。 • [TCP Flags]：マスクによってマスクされた場合に照合する TCP フラグ。 – URG ビット – ACK ビット – PSH ビット – RST ビット – SYN ビット – FIN ビット	• URG • ACK • PSH • RST • SYN • FIN
Specify TCP Reserved	（任意）TCP 予約の使用をイネーブルにします。 • [TCP Reserved]：TCP 予約。	0 ～ 63
Specify TCP Header Length	（任意）L4 TCP ヘッダー長の検査をイネーブルにします。 • [TCP Header Length]：検査で使用する TCP ヘッダーの長さを指定します。	0 ～ 60

表 B-10　Atomic IP エンジンのパラメータ（続き）

パラメータ	説明	値
Specify TCP Payload Length	（任意）L4 TCP ペイロード長の検査をイネーブルにします。 • [TCP Payload Length]：TCP ペイロードの長さを指定します。	0 ～ 65535
Specify TCP URG Pointer	（任意）L4 TCP の URG ポインタの検査をイネーブルにします。 • [TCP URG Pointer]：TCP URG フラグの検査を指定します。	0 ～ 65535
Specify TCP Window Size	（任意）L4 TCP ウィンドウ サイズの検査をイネーブルにします。 • [TCP Window Size]：TCP パケットのウィンドウ サイズを指定します。	0 ～ 65535
Specify UDP Length	（任意）L4 UDP の長さの検査をイネーブルにします。 • [UDP Length]：IP データ長が UDP ヘッダー長よりも小さい場合にアラートを起動します。	0 ～ 65535
Specify UDP Valid Length	（任意）L4 UDP の有効長の検査をイネーブルにします。 • [UDP Valid Length]：有効であると見なし検査しない UDP パケット長を指定します。	0 ～ 65535
Specify UDP Length Mismatch	（任意）L4 UDP の長さの不一致の検査をイネーブルにします。 • [UDP Length Mismatch]：IP データ長が UDP ヘッダー長よりも小さい場合にアラートを起動します。	[Yes] | [No]

詳細情報

すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Atomic IPv6 エンジン

Atomic IPv6 エンジンは、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 の 2 つの脆弱性を検出します。これらの脆弱性は、ルータのクラッシュやその他のセキュリティ上の問題につながることがあります。IOS の脆弱性の 1 つは、複数の先頭フラグメントを処理し、バッファ オーバーフローを引き起こします。もう 1 つの脆弱性は、不正な ICMPv6 ネイバー探索オプションを処理し、これもバッファ オーバーフローを引き起こします。

（注）　IPv6 では、IP アドレスのサイズが 32 ビットから 128 ビットに拡大されました。これにより、サポートされるアドレッシング階層が増大し、より多くのノードにアドレスを割り当てることができ、アドレスの自動設定が可能になりました。

8 個の Atomic IPv6 シグニチャがあります。Atomic IPv6 は、次の種類の ネイバー探索プロトコルを検査します。

- タイプ 133：ルータ送信要求
- タイプ 134：ルータ アドバタイズメント
- タイプ 135：ネイバー送信要求
- タイプ 136：ネイバー アドバタイズメント
- タイプ 137：リダイレクト

（注）　ホストとルータは、ネイバー探索を使用して、アタッチされたリンクに常駐することがわかっているネイバーのリンク層アドレスを判断し、無効になったキャッシュ値をすばやくパージします。また、ホストはネイバー探索を使用して、ホストに代わってパケットを転送する隣接ルータを検出します。

各ネイバー探索タイプには、1 つ以上の Neighborhood Discovery オプションを設定できます。Atomic IPv6 エンジンは、各オプションの長さが、RFC 2461 で規定されている正規の値に準拠しているかどうかを検査します。オプション結果の長さの違反がある場合、異常な長さが見つかったオプション タイプに対応するアラートが発生します（シグニチャ 1601 ～ 1605）。

（注）　Atomic IPv6 シグニチャには、設定すべき固有のパラメータがありません。

表 B-11 に Atomic IPv6 のシグニチャの一覧を示します。

表 B-11　Atomic IPv6 のシグニチャ

シグニチャ ID	サブシグニチャ ID	名前	説明
1600	0	ICMPv6 長さゼロ オプション	長さが ZERO と指定されたすべてのオプション タイプ
1601	0	ICMPv6 オプション タイプ 1 違反	有効な長さである 8 または 16 バイトの違反。
1602	0	ICMPv6 オプション タイプ 2 違反	有効な長さである 8 または 16 バイトの違反。
1603	0	ICMPv6 オプション タイプ 3 違反	有効な長さである 32 バイトの違反。
1604	0	ICMPv6 オプション タイプ 4 違反	有効な長さである 80 バイトの違反。
1605	0	ICMPv6 オプション タイプ 5 違反	有効な長さである 8 バイトの違反。

表 B-11　Atomic IPv6 のシグニチャ（続き）

シグニチャ ID	サブシグニチャ ID	名前	説明
1606	0	ICMPv6 の短いオプション データ	不十分なデータのシグニチャ（実際のパケットにあるよりも多くのオプションのデータがあるとパケットに指定されている場合）
1607	0	IPv6 の複数の巧妙に細工されたフラグメント パケット	30 秒間の間に複数の先頭フラグメントが検出された場合にアラートを生成します。

詳細情報

すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Fixed エンジン

Fixed エンジンでは、複数の正規表現パターンを 1 つのパターン マッチング テーブルに組み合わせ、データ全体で単一の検索が可能です。ICMP、TCP、および UDP プロトコルがサポートされています。最低検査深度に達した場合（1 ～ 100 バイト）、検査が停止します。Fixed エンジンには、Fixed ICMP、Fixed TCP、および Fixed UDP の 3 つの種類があります。

（注）　Fixed TCP と Fixed UDP では、Service Ports パラメータが除外ポートとして使用されます。Fixed ICMP では Service Ports パラメータが除外 ICMP タイプとして使用されます。

表 B-12 に、Fixed ICMP エンジンに固有のパラメータを示します。

表 B-12　Fixed ICMP エンジンのパラメータ

パラメータ	説明	値
Direction	トラフィックの方向。 • 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。 • 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。	From Service To Service
Max Payload Inspect Length	シグニチャの最大検査深度を指定します。	1 ～ 250
Regex String	単一のパケット内で検索する正規表現を指定します。	string
Specify Exact Match Offset	（任意）完全一致オフセットをイネーブルにします。 • [Exact Match Offset]：一致が有効であるために、[Regex String] が報告する必要がある正確なストリーム オフセット。	0 ～ 65535

表 B-12　Fixed ICMP エンジンのパラメータ（続き）

パラメータ	説明	値
Specify Minimum Match Length	（任意）最小一致長をイネーブルにします。 • [Minimum Match Length]：[Regex String] が一致する必要がある最小バイト数を指定します。	0 ～ 65535
Specify ICMP Type	（任意）ICMP ヘッダー タイプの検査をイネーブルにします。 • [ICMP Type]：ICMP ヘッダーの TYPE 値を指定します。	0 ～ 65535
Swap Attacker Victim	攻撃者と攻撃対象のアドレスとポート（送信元および宛先）を、アラート メッセージとアクションで入れ替える場合は [Yes]。入れ替えない場合は [No]（デフォルト）。	[Yes] | [No]

表 B-13 に、Fixed TCP エンジンに固有のパラメータを示します。

表 B-13　Fixed TCP エンジンのパラメータ

パラメータ	説明	値
Direction	トラフィックの方向。 • 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。 • 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。	From Service To Service
Max Payload Inspect Length	シグニチャの最大検査深度を指定します。	1 ～ 250
Regex String	単一のパケット内で検索する正規表現を指定します。	string
Specify Exact Match Offset	（任意）完全一致オフセットをイネーブルにします。 • [Exact Match Offset]：一致が有効であるために、[Regex String] が報告する必要がある正確なストリーム オフセット。	0 ～ 65535
Specify Minimum Match Length	（任意）最小一致長をイネーブルにします。 • [Minimum Match Length]：[Regex String] が一致する必要がある最小バイト数を指定します。	0 ～ 65535

表 B-13　Fixed TCP エンジンのパラメータ（続き）

パラメータ	説明	値
Specify Service Ports	サービス ポートの使用をイネーブルにします。 • [Service Ports] : 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。	0 ～ 65535[1] a-b[,c-d]
Swap Attacker Victim	攻撃者と攻撃対象のアドレスとポート（送信元および宛先）を、アラート メッセージとアクションで入れ替える場合は [Yes]。入れ替えない場合は [No]（デフォルト）。	[Yes] | [No]

1. 範囲の 2 番目の数は、最初の数以上である必要があります。

表 B-14 に、Fixed UDP エンジンに固有のパラメータを示します。

表 B-14　Fixed UDP エンジンのパラメータ

パラメータ	説明	値
Direction	トラフィックの方向。 • 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。 • 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。	From Service To Service
Max Payload Inspect Length	シグニチャの最大検査深度を指定します。	1 ～ 250
Regex String	単一のパケット内で検索する正規表現を指定します。	string
Specify Exact Match Offset	（任意）完全一致オフセットをイネーブルにします。 • [Exact Match Offset] : 一致が有効であるために、[Regex String] が報告する必要がある正確なストリーム オフセット。	0 ～ 65535
Specify Minimum Match Length	（任意）最小一致長をイネーブルにします。 • [Minimum Match Length] : [Regex String] が一致する必要がある最小バイト数を指定します。	0 ～ 65535
Specify Service Ports	サービス ポートの使用をイネーブルにします。 • [Service Ports] : 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。	0 ～ 65535[1] a-b[,c-d]
Swap Attacker Victim	攻撃者と攻撃対象のアドレスとポート（送信元および宛先）を、アラート メッセージとアクションで入れ替える場合は [Yes]。入れ替えない場合は [No]（デフォルト）。	[Yes] | [No]

1. 範囲の 2 番目の数は、最初の数以上である必要があります。

詳細情報

- シグニチャの正規表現構文の一覧については、「正規表現の構文」（P.B-10）を参照してください。
- すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Flood エンジン

Flood エンジンは、複数のパケットを単一のホストまたはネットワークに送信しているホストまたはネットワークをモニタするシグニチャを定義します。たとえば、攻撃対象ホスト宛に、秒あたり 150 個以上のパケット（特定の種類）が検出された場合にアラートを起動するシグニチャを作成できます。Flood エンジンには、Flood Host と Flood Net の 2 つの種類があります。

表 B-15 に、Flood Host エンジンに固有のパラメータを示します。

表 B-15　Flood Host エンジンのパラメータ

パラメータ	説明	値
Protocol	検査するトラフィックの種類。	ICMP UDP
Rate	1 秒あたりのパケットのしきい値。	0 ～ 65535[1]
ICMP Type	ICMP ヘッダー タイプの値を指定します。	0 ～ 65535
Dst Ports	UDP プロトコルを選択した場合の宛先ポートを指定します。	0 ～ 65535[2] a-b[,c-d]
Src Ports	UDP プロトコルを選択した場合の送信元ポートを指定します。	0 ～ 65535[3] a-b[,c-d]

1. レートがこの数値（パケット/秒）よりも大きい場合にアラートが起動されます。
2. 範囲の 2 番目の数は、最初の数以上である必要があります。
3. 範囲の 2 番目の数は、最初の数以上である必要があります。

表 B-16 に、Flood Net エンジンに固有のパラメータを示します。

表 B-16　Flood Net エンジンのパラメータ

パラメータ	説明	値
Gap	フラッディング シグニチャに許容される時間の間隔（秒単位）。	0 ～ 65535
Peaks	フラッディング トラフィックの許容されるピークの数。	0 ～ 65535
Protocol	検査するトラフィックの種類。	ICMP TCP UDP
Rate	1 秒あたりのパケットのしきい値。	0 ～ 65535[1]
Sampling Interval	トラフィックをサンプリングする間隔。	1 ～ 3600
ICMP Type	ICMP ヘッダー タイプの値を指定します。	0 ～ 65535

1. レートがこの数値（パケット/秒）よりも大きい場合にアラートが起動されます。

詳細情報

すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Meta エンジン

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。

表 B-17 に、Meta エンジンに固有のパラメータを示します。

表 B-17　Meta エンジンのパラメータ

パラメータ	説明	値
Swap Attacker Victim	攻撃者と攻撃対象のアドレスとポート（送信元および宛先）を、アラート メッセージとアクションで入れ替える場合は [Yes]。入れ替えない場合は [No]（デフォルト）。	[Yes] | [No]
Meta Reset Interval	Meta シグニチャをリセットする時間（秒単位）。	0 ～ 3600
Component List	Meta コンポーネントのリスト。 • [edit]：既存のエントリを編集します。 • [insert]：新しいエントリをリストに挿入します。 – [begin]：エントリをアクティブなリストの先頭に配置します。 – [end]：エントリをアクティブなリストの末尾に配置します。 – [inactive]：エントリを非アクティブなリストに配置します。 – [before]：エントリを指定したエントリの前に配置します。 – [after]：エントリを指定したエントリの後に配置します。 • [move]：リスト内のエントリを移動します。	*name1*

表 B-17　Meta エンジンのパラメータ（続き）

パラメータ	説明	値
Meta Key	Meta シグニチャのストレージ タイプ。 • 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	AaBb AxBx Axxx xxBx
Unique Victims	Meta シグニチャごとに一意の必須攻撃対象ポートの番号。	1 ～ 256
Component List In Order	コンポーネント リストを順番に起動するかどうか。	[Yes] | [No]

詳細情報

- カスタム Meta エンジンのシグニチャの例については、「Meta エンジンのシグニチャの例」（P.9-23）を参照してください。
- すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Multi String エンジン

注意　Multi String エンジンは、メモリの使用状況に大きく影響することがあります。

Multi String エンジンでは、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。この検査は、1 つのシグニチャに対して複数の文字列を照合して行います。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。たとえば、UDP サービスで regex 1 とそれに続く regex 2 を検索するシグニチャを定義できます。UDP および TCP の場合は、ポート番号と方向を指定できます。1 つの送信元ポート、1 つの宛先ポート、または両方のポートを指定できます。文字列の照合は両方向で実行されます。

Multi String エンジンは、複数の正規表現パターンを指定する必要がある場合に使用します。それ以外の場合は、String ICMP、String TCP、または String UDP エンジンを使用して、これらのプロトコルのいずれかに対応した単一の正規表現パターンを指定できます。

表 B-18 に、Multi String エンジンに固有のパラメータを示します。

表 B-18　Multi String エンジンのパラメータ

パラメータ	説明	値
Inspect Length	起動するシグニチャに対して違反するすべての文字列を含める必要があるストリームまたはパケットの長さ。	0 ～ 4294967295
Protocol	Layer 4 プロトコル選択。	ICMP TCP UDP

表 B-18　Multi String エンジンのパラメータ（続き）

パラメータ	説明	値
Regex Component	正規表現コンポーネントのリスト。 • [Regex String]：検索する文字列。 • [Spacing Type]：直前の一致から、またはストリームやパケットの先頭から（リスト内の最初のエントリである場合）の、必要なスペースのタイプ。	list（1 ～ 16 項目） exact minimum
Port Selection	検査する TCP または UDP ポートのタイプ。 • [Both Ports]：送信元ポートと宛先ポートの両方を指定します。 • [Destination]：宛先ポートの範囲を指定します。 • [Source]：送信元ポートの範囲を指定します。[1]	0 ～ 65535 [2]
Extra Spacing	この正規表現文字列と直前の正規表現文字列との間、またはストリームやパケットの先頭から（リスト内の最初のエントリである場合）、空ける必要のあるバイト数。	0 ～ 4294967296
Minimum Spacing	この正規表現文字列と直前の正規表現文字列との間、またはストリームやパケットの先頭から（リスト内の最初のエントリである場合）、空ける必要のある最小バイト数。	0 ～ 4294967296
Swap Attacker Victim	攻撃者と攻撃対象のアドレスとポート（送信元および宛先）を、アラート メッセージとアクションで入れ替える場合は [Yes]。入れ替えない場合は [No]（デフォルト）。	[Yes] | [No]

1. ポート マッチングは、クライアントからサーバとサーバからクライアントへの両方のトラフィック フロー方向に対して双方向で実行されます。たとえば、送信元ポートの値が 80 で、クライアントからサーバへのトラフィック フロー方向の場合、クライアント ポートが 80 の場合に検査が行われます。サーバからクライアントへのトラフィック フロー方向では、サーバ ポートが 80 の場合に検査が行われます。
2. 有効な値は 0 ～ 65535 の範囲の、a-b[,c-d] 形式による整数範囲のカンマ区切りのリストです。範囲の 2 番目の数は、最初の数以上である必要があります。

詳細情報

- シグニチャの正規表現構文の一覧については、「正規表現の構文」（P.B-10）を参照してください。
- すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Normalizer エンジン

Normalizer エンジンは、IP フラグメンテーションと TCP 正規化を扱います。ここでは、Normalizer エンジンについて説明します。内容は次のとおりです。

Normalizer エンジンについて

（注）　IPS SSP を搭載した Cisco ASA 5585-X では、正規化がサポートされていません。

（注）　Normalizer エンジンには、カスタム シグニチャを追加できません。既存のシグニチャを調整することはできます。

Normalizer エンジンは IP フラグメントの再構築と TCP ストリームの再構築を扱います。Normalizer エンジンを使用すると、センサーが同時に追跡を試みるフラグメントの最大数など、システム リソースの使用量について制限を設定できます。無差別モードのセンサーは、違反時にアラートを報告します。インライン モードのセンサーは、Produce Alert、Deny Packet Inline、および Modify Packet Inline など、イベント アクション パラメータで指定されたアクションを実行します。

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。

IP フラグメンテーションの正規化

IP データグラムの意図的または意図しないフラグメンテーションにより、悪用が隠れてしまい、検出が困難になったり不可能になったりすることがあります。フラグメンテーションは、ファイアウォールやルータで実行されるアクセス コントロール ポリシーを回避するために使用されることもあります。オペレーティング システムごとに、異なる方法を使用してフラグメント化されたデータグラムをキューに格納してディスパッチします。エンド ホストがデータグラムを再構築できる、考えられるすべての方法をセンサーで確認する必要がある場合、センサーは DoS 攻撃に脆弱になります。フラグメント化されたすべてのデータグラムをインラインで再構築し、完成したパケットのみを転送し、必要に応じてデータグラムを再度フラグメント化することで、これを避けることができます。IP Fragmentation Normalization ユニットはこの機能を実行します。

TCP 正規化

意図的または自然の TCP セッションのセグメント化を通じて、一部の攻撃クラスが隠れることがあります。ポリシーの強制が、偽陽性または偽陰性なく行われるようにするため、2 つの TCP エンドポイントの状態を追跡し、実際のホスト エンドポイントで実際に処理されるデータのみを通過させる必要があります。TCP ストリームの重なりが起きる可能性がありますが、TCP セグメントの再送以外では非常にまれです。TCP セッションの上書きが起こらないことが必要です。上書きが起きる場合、誰かが意図的にセキュリティ ポリシーを回避しようとしているか、TCP スタックの実装が壊れています。両方のエンドポイントの状態に関する完全な情報を維持することは、センサーが TCP プロキシとして動作しない限り不可能です。センサーが TCP プロキシとして動作する代わりに、セグメントが適切に順序付けされ、Normalizer エンジンは回避や攻撃に関連する異常なパケットを探します。

IPv6 フラグメント

Normalizer エンジンは、IPv6 フラグメントを再構築し、他のエンジンやプロセッサでの検査やアクション用に、再構築したバッファを転送することができます。IPv4 と IPv6 では次の違いがあります。

- Normalizer エンジンのシグニチャの Modify Packet Inline は、IPv6 データグラムに対しては適用されません。

- シグニチャ 1206（IP Fragment Too Small）は、IPv6 データグラムに対しては起動されません。Atomic IP Advanced エンジンのシグニチャ 1741 は、小さすぎる IPv6 フラグメントに対して起動されます。
- シグニチャ 1202 は、IPv6 で、Maximum Datagram Size を超えた追加の 48 バイトを許可します。これは、IPv6 ヘッダー フィールドが長いためです。

詳細情報

Normalizer エンジンのシグニチャの設定手順については、「IP フラグメント再構成のシグニチャの設定」（P.9-46）および「TCP ストリーム再構成シグニチャの設定」（P.9-49）を参照してください。

Normalizer エンジンのパラメータ

表 B-19 に、Normalizer エンジンに固有のパラメータを示します。

表 B-19　Normalizer エンジンのパラメータ

パラメータ	説明
Edit Defaults	編集可能なシグニチャ。
Specify Fragment Reassembly Timeout	（任意）フラグメント再構築タイムアウトをイネーブルにします。
Specify Hijack Max Old Ack	（任意）hijack-max-old-ack をイネーブルにします。
Specify Max Datagram Size	（任意）最大データグラム サイズをイネーブルにします。
Specify Max Fragments	（任意）最大フラグメントをイネーブルにします。
Specify Max Fragments per Datagram	（任意）データグラムあたりの最大フラグメントをイネーブルにします。
Specify Max Last Fragments	（任意）直前の最大フラグメントをイネーブルにします。
Specify Max Partial Datagrams	（任意）最大部分データグラムをイネーブルにします。
Specify Max Small Frags	（任意）最大スモール フラグメントをイネーブルにします。
Specify Min Fragment Size	（任意）最小フラグメント サイズをイネーブルにします。
Specify Service Ports	（任意）サービス ポートをイネーブルにします。
Specify SYN Flood Max Embryonic	（任意）SYN フラッドの最大初期接続をイネーブルにします。
Specify TCP Closed Timeout	（任意）TCP クローズド タイムアウトをイネーブルにします。
Specify TCP Embryonic Timeout	（任意）TCP 初期接続タイムアウトをイネーブルにします。
Specify TCP Idle Timeout	（任意）TCP アイドル タイムアウトをイネーブルにします。
Specify TCP Max MSS	（任意）TCP 最大 mss（最大セグメント サイズ）をイネーブルにします。
Specify TCP Max Queue	（任意）TCP 最大キューをイネーブルにします。
Specify TCP Min MSS	（任意）TCP 最小 mss をイネーブルにします。
Specify TCP Option Number	（任意）TCP オプション番号をイネーブルにします。

詳細情報

すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Service エンジン

ここでは、Service エンジンについて説明します。内容は次のとおりです。

Service エンジンについて

Service エンジンでは、2 つのホスト間のレイヤ 5+ トラフィックの解析が行われます。永続的データを追跡する 1 対 1 のシグニチャがあります。エンジンは、ライブ サービスと類似の方法でレイヤ 5+ ペイロードを解析します。

各 Service エンジンには共通した特性がある一方、個々のエンジンには検査対象のサービスに関する固有の情報が保持されます。String エンジンの使用が不適切であるか望ましくない場合には、Service エンジンによって、アルゴリズムに特化した汎用文字列エンジンの機能が補完されます。

Service DNS エンジン

Service DNS エンジンは、高度な DNS デコードを行います。これには、反回避技術（複数のジャンプの追跡など）が含まれます。長さ、命令コード、文字列などの多数のパラメータがあります。Service DNS エンジンは、2 つのプロトコルに対応するインスペクタであり、TCP ポート 53 と UDP ポート 53 の両方で稼動します。TCP の場合はストリームを使用し、UDP の場合はクワッドを使用します。

表 B-20 に、Service DNS エンジンに固有のパラメータを示します。

表 B-20　Service DNS エンジンのパラメータ

パラメータ	説明	値
Protocol	このインスペクタの該当プロトコル。	TCP UDP
Specify Query Chaos String	（任意）DNS クエリー クラスのカオス文字列をイネーブルにします。	*query-chaos-string*
Specify Query Class	（任意）クエリー クラスをイネーブルにします。 • [Query Class]：DNS クエリー クラス 2 バイト値	0 ～ 65535
Specify Query Invalid Domain Name	（任意）無効なドメイン名のクエリーをイネーブルにします。 • [Query Invalid Domain Name]：255 を超える DNS クエリー長	[Yes] | [No]
Specify Query Jump Count Exceeded	（任意）クエリー ジャンプ カウント超過をイネーブルにします。 • [Query Jump Count Exceeded]：DNS 圧縮カウンタ	[Yes] | [No]
Specify Query Opcode	（任意）クエリー命令コードをイネーブルにします。 • [Query Opcode]：DNS クエリー命令コードの 1 バイト値	0 ～ 65535
Specify Query Record Data Invalid	（任意）無効なレコード データのクエリーをイネーブルにします。 • [Query Record Data Invalid]：不完全な DNS レコード データ	[Yes] | [No]
Specify Query Record Data Length	（任意）クエリー レコード データ長をイネーブルにします。 • [Query Record Data Length]：DNS 応答レコード データ長	0 ～ 65535
Specify Query Src Port 53	（任意）クエリー送信元ポート 53 をイネーブルにします。 • [Query Src Port 53]：DNS パケットの送信元ポート 53	[Yes] | [No]
Specify Query Stream Length	（任意）クエリー ストリーム長をイネーブルにします。 • [Query Record Data Length]：DNS パケット長	0 ～ 65535

表 B-20　Service DNS エンジンのパラメータ（続き）

パラメータ	説明	値
Specify Query Type	（任意）クエリー タイプをイネーブルにします。 • [Query Type]：DNS クエリー タイプの 2 バイト値	0 ～ 65535
Specify Query Value	（任意）クエリー値をイネーブルにします。 • [Query Value]：クエリー 0、応答 1	[Yes] | [No]

詳細情報

すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Service FTP エンジン

Service FTP エンジンは、FTP の port コマンドのデコードに特化しており、無効な **port** コマンドと PASV ポートのスプーフィングを捕捉します。このエンジンは、String エンジンが検出に適していない場合のギャップを埋めます。パラメータはいずれも Boolean 型で、**port** コマンドのデコードおけるさまざまなエラー トラップ条件へのマッピングに使用します。Service FTP エンジンは、TCP ポート 20 および 21 で稼動します。ポート 20 はデータ用であり、Service FTP エンジンはこのポートに対して検査を行いません。Service FTP エンジンは、ポート 21 の制御トランザクションを検査します。

表 B-21 に、Service FTP エンジンに固有のパラメータを示します。

表 B-21　Service FTP エンジンのパラメータ

パラメータ	説明	値
Direction	トラフィックの方向。 • 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。 • 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。	From Service To Service
FTP Inspection Type	実行する検査のタイプ： • FTP port コマンド内の無効なアドレスを検索します。 • FTP port コマンド内の無効なポートを検索します。 • PASV ポート スプーフィングを検索します。	Invalid Address in PORT Command Invalid Port in PORT Command PASV Port Spoof
Service Ports	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。	0 ～ 65535[1] a-b[,c-d]
Swap Attacker Victim	攻撃者と攻撃対象のアドレスとポート（送信元および宛先）を、アラート メッセージとアクションで入れ替える場合は [Yes]。入れ替えない場合は [No]（デフォルト）。	[Yes] | [No]

1. 範囲の 2 番目の数は、最初の数以上である必要があります。

詳細情報

すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Service Generic エンジン

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、設定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。

新機能により、Service Generic エンジンと拡張命令に正規表現パラメータが追加されます。Service Generic エンジンでは、パケットを解析するために作成されたミニプログラムに基づいてトラフィックを解析できます。これらのミニプログラムは、パケットを分析し特定の条件を探すコマンドで構成されます。

（注） 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。

注意 複雑な言語特有の性質上、重大度とイベント アクション以外の 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お勧めしません。

表 B-22 に、Service Generic エンジンに固有のパラメータを示します。

表 B-22　Service Generic エンジンのパラメータ

パラメータ	説明	値
Specify Dst Port	（任意）宛先ポートをイネーブルにします。 • [Dst Port]：シグニチャの該当宛先ポート。	0 ～ 65535
Specify IP Protocol	（任意）IP プロトコルをイネーブルにします。 • [IP Protocol]：インスペクタが検査する IP プロトコル。	0 ～ 255
Specify Payload Source	（任意）ペイロード送信元の検査をイネーブルにします。 • [Payload Source]：次のタイプのペイロード送信元検査 – ICMP データの検査 – レイヤ 2 ヘッダーの検査 – レイヤ 3 ヘッダーの検査 – レイヤ 4 ヘッダーの検査 – TCP データの検査 – UDP データの検査	ICMP Data 12 Header 13 Header 14 Header TCP Data UDP Data
Specify Src Port	（任意）送信元ポートをイネーブルにします。 • [Src Port]：シグニチャの該当送信元ポート。	0 ～ 65535

表 B-22　Service Generic エンジンのパラメータ（続き）

パラメータ	説明	値
Specify Regex String	ポリシー タイプが [regex] の場合に検索する正規表現。 • 単独の TCP パケット内での検索に使用する正規表現。 • （任意）使用する最小一致長をイネーブルにします。 一致と見なされるために必要な正規表現の最小一致長です。	Regex String Specify Min Match Length
Swap Attacker Victim	攻撃者と攻撃対象のアドレスとポート（送信元および宛先）を、アラート メッセージとアクションで入れ替える場合は [Yes]。入れ替えない場合は [No]（デフォルト）。	[Yes] | [No]

詳細情報

- シグニチャの正規表現構文の一覧については、「正規表現の構文」（P.B-10）を参照してください。
- すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Service H225 エンジン

Service H225 エンジンは、多数のサブプロトコルで構成され H.323 スイートに含まれている H225.0 プロトコルを分析します。H.323 はプロトコルと他の標準を集めたものであり、パケットベース ネットワーク上での会議が可能になります。

H.225.0 コール シグナリングおよびステータス メッセージは H.323 コール セットアップの一部です。ゲートキーパーやエンドポイント ターミナルなど、ネットワーク内のさまざまな H.323 エンティティが H.225.0 プロトコル スタックの実装を実行します。Service H225 エンジンは H225.0 プロトコルを分析し、複数の H.323 ゲートキーパー、VoIP ゲートウェイ、およびエンドポイント ターミナルに対する攻撃を検査します。また、TCP PDU 上で交換されるコール シグナリング メッセージのディープ パケット インスペクション機能が提供されます。Service H225 エンジンは、H.225.0 プロトコルを分析し、無効な H.255.0 メッセージや、これらのメッセージ内のさまざまなプロトコルフ ィールド上の悪用およびオーバーフロー攻撃を検査します。

H.225.0 コール シグナリング メッセージは Q.931 プロトコルを基にしています。コール元エンドポイントは、コール先のエンドポイントに Q.931 セットアップ メッセージを送信します。そのアドレスは、アドミッション手順や何らかの検索手段で取得されます。コール先エンドポイントは、Q.931 接続メッセージを送信して接続を受け付けるか、接続を拒否します。H.225.0 の接続が確立されると、コール元またはコール先のエンドポイントが H.245 アドレスを渡します。このアドレスは、制御プロトコル（H.245）チャネルを確立するために使用されます。

特に重要なのは、SETUP コール シグナリング メッセージです。これは、このメッセージがコール セットアップの中で H.323 エンティティ間で交換される最初のメッセージであるためです。SETUP メッセージは、コール シグナリング メッセージの一般的なフィールドの多くを使用しており、確度の高い攻撃にさらされた実装は、ほとんど SETUP メッセージのセキュリティ チェックに失敗します。そのため、H.225.0 SETUP メッセージの正当性をチェックし、ネットワークの境界でチェックを強制することはきわめて重要です。

Service H225 エンジンには、H225 SETUP セットアップ メッセージの TPKT の検証、Q.931 プロトコルの検証、および ASN.1PER 検証のための組み込みシグニチャがあります。ASN.1 はデータ構造を記述するための表記法です。PER では異なるスタイルの符号化が使用されます。PER は、データ タイプに基づく符号化に特化して、はるかにコンパクトな表現を生成します。

Q.931 および TPKT の長さシグニチャの調整、H.225 プロトコル フィールドに対するより詳細なシグニチャの追加と適用、Q.931 または H.225 プロトコルの単一のフィールドの複数パターン検索シグニチャの適用を行うことができます。

Service H225 エンジンでは次の機能がサポートされています。

- TPKT 検証と長さチェック
- Q.931 情報要素検証
- Q.931 情報要素におけるテキスト フィールドの正規表現シグニチャ
- Q.931 情報要素に対する長さチェック
- SETUP メッセージの検証
- ASN.1 PER 符号化エラー チェック
- 正規表現と長さの両方について、ULR-ID、E-mail-ID、h323-id などの設定シグニチャ。

TPKT シグニチャと ASN.1 シグニチャの数は固定です。これらのタイプについてはカスタム シグニチャを作成できません。TPKT シグニチャでは、長さシグニチャの値の範囲のみを変更します。ASN.1 のパラメータは変更できません。Q.931 シグニチャでは、テキスト フィールドに対する新しい正規表現を追加できます。SETUP シグニチャでは、SETUP メッセージのさまざまなフィールドに対する長さおよび正規表現チェックのシグニチャを追加できます。

表 B-23 に、Service H225 エンジンに固有のパラメータを示します。

表 B-23　Service H.225 エンジンのパラメータ

パラメータ	説明	値
Message Type	シグニチャを適用する H225 メッセージのタイプ。 • SETUP • ASN.1-PER • Q.931 • TPKT	asn.1-per q.931 setup tpkt
Policy Type	シグニチャを適用する H225 ポリシーのタイプ： • フィールド長を検査する。 • 存在を検査する。 特定のフィールドがメッセージ内に存在する場合は、アラートが送信されます。 • 正規表現を検査する。 • フィールドの妥当性を検査する。 • 値を検査する。 TPKT シグニチャの場合、[regex] と [presence] は有効な値ではありません。	length presence regex validate value

表 B-23　Service H.225 エンジンのパラメータ（続き）

パラメータ	説明	値
Specify Field Name	（任意）フィールド名の使用をイネーブルにします。SETUP および Q.931 メッセージ タイプのみで有効です。このシグニチャを適用するフィールド名のドット付き表記を指定します。 • [Field Name]：検査するフィールドの名前。	1 ～ 512
Specify Invalid Packet Index	（任意）ASN と TPKT 固有のエラー、および固定マッピングを持つその他のエラーで使用する無効なパケット インデックスをイネーブルにします。 • [Invalid Packet Index]：無効なパケット インデックスを検査します。	0 ～ 255
Value Range Regex String	ポリシー タイプが [regex] の場合に検索する正規表現。TPKT シグニチャには設定しないでください。 • 単独の TCP パケット内での検索に使用する正規表現。 • （任意）使用する最小一致長をイネーブルにします。 一致と見なされるために必要な正規表現の最小一致長です。TPKT シグニチャには設定しないでください。	Regex String Specify Min Match Length
Specify Value Range	長さまたは値ポリシー タイプ（0x00 ～ 6535）で有効です。その他のポリシー タイプの場合は無効です。 • [Value Range]：値の範囲。	0 ～ 65535[1] a-b
Swap Attacker Victim	攻撃者と攻撃対象のアドレスとポート（送信元および宛先）を、アラート メッセージとアクションで入れ替える場合は [Yes]。入れ替えない場合は [No]（デフォルト）。	[Yes] | [No]

1. 範囲の 2 番目の数は、最初の数以上である必要があります。

詳細情報

- シグニチャの正規表現構文の一覧については、「正規表現の構文」（P.B-10）を参照してください。
- すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Service HTTP エンジン

Service HTTP エンジンは、サービス固有文字列に基づくパターン照合インスペクション エンジンです。HTTP プロトコルは、今日のネットワークで最もよく使用されているプロトコルの 1 つです。また、最も長い前処理時間を必要とし、システムの全体的なパフォーマンスにとって必須の検査を必要とするシグニチャの数も最も多くあります。

Service HTTP エンジンでは、複数のパターンを 1 つのパターン マッチング テーブルにまとめることでデータ内の検索を一度に実行できる正規表現ライブラリが使用されます。このエンジンは、Web サービスのみに向けられたトラフィック、つまり HTTP 要求を検索します。このエンジンでリターン トラフィックを検査することはできません。このエンジンでは、各シグニチャが対象とする個別の Web ポートを指定できます。

HTTP 解読とは、符号化された文字を ASCII 対応文字に正規化することによって、HTTP メッセージをデコードするプロセスです。このプロセスは、ASCII 正規化と呼ばれることもあります。

HTTP パケットを検査するには、あらかじめそのデータを、ターゲット システムでのデータ処理時に表示されるものと同じデータ表現として解読または正規化しておく必要があります。また、ホスト ターゲット タイプごとにカスタマイズされたデコード方式を用意することが推奨されます。そのためには、ターゲット上で動作しているオペレーティング システムおよび Web サーバのバージョンを確認する必要があります。Service HTTP エンジンには、Microsoft IIS Web サーバ用のデフォルトの解読動作が用意されています。

表 B-24 に、Service HTTP エンジンに固有のパラメータを示します。

表 B-24　Service HTTP エンジンのパラメータ

パラメータ	説明	値
De Obfuscate	検索の前に反回避解読を適用します。	[Yes] | [No]
Max Field Sizes	最大フィールド サイズ グループ。	—
Specify Max Arg Field Length	（任意）引数フィールドの最大長をイネーブルにします。 • [Max Arg Field Length]：引数フィールドの最大長。	0 ～ 65535
Specify Max Header Field Length	（任意）ヘッダー フィールドの最大長をイネーブルにします。 • [Max Header Field Length]：ヘッダー フィールドの最大長。	0 ～ 65535
Specify Max Request Field Length	（任意）要求フィールドの最大長をイネーブルにします。 • [Max Request Field Length]：要求フィールドの最大長。	0 ～ 65535
Specify Max URI Field Length	（任意）[URI] フィールドの最大長をイネーブルにします。 • [Max URI Field Length]：[URI] フィールドの最大長。	0 ～ 65535
Regex	正規表現グループ。	—

表 B-24　Service HTTP エンジンのパラメータ（続き）

パラメータ	説明	値
Specify Arg Name Regex	（任意）特定の正規表現の [Arguments] フィールドの検索をイネーブルにします。 • [Arg Name Regex]：[HTTP Arguments] フィールドで検索する正規表現（? の後およびコンテンツ長で定義されているエンティティ本体の中）。	—
Specify Header Regex	（任意）特定の正規表現の [Header] フィールドの検索をイネーブルにします。 • [Header Regex]：[HTTP Header] フィールドで検索する正規表現。 ヘッダーは、最初の CRLF の後ろから定義され、CRLFCRLF まで続きます。	—
Specify Request Regex	（任意）特定の正規表現の [Request] フィールドの検索をイネーブルにします。 • [Request Regex]：[HTTP URI] フィールドと [HTTP Argument] フィールドの両方で検索する正規表現。 • [Specify Min Request Match Length]：要求の最小一致長の設定をイネーブルにします。	0 ～ 65535
Specify URI Regex	（任意）[HTTP URI] フィールドで検索する正規表現。[URI] フィールドは、HTTP メソッド（たとえば、GET）の後ろで、最初の CRLF の前まで定義されます。正規表現は保護されています。つまり、値は変更できません。	[/¥¥][a-zA-Z][a-zA-Z][a-zA-Z][a-zA-Z][a-zA-Z][a-zA-Z][a-zA-Z][.]jpeg
Service Ports	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。	0 ～ 65535[1] a-b[,c-d]
Swap Attacker Victim	攻撃者と攻撃対象のアドレスとポート（送信元および宛先）を、アラート メッセージとアクションで入れ替える場合は [Yes]。入れ替えない場合は [No]（デフォルト）。	[Yes] | [No]

1. 範囲の 2 番目の数は、最初の数以上である必要があります。

詳細情報

- Service HTTP のカスタム シグニチャの例については、「Service HTTP エンジンのシグニチャの例」（P.10-18）を参照してください。
- すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。
- シグニチャの正規表現構文の一覧については、「正規表現の構文」（P.B-10）を参照してください。

Service IDENT エンジン

Service IDENT エンジンでは、TCP ポート 113 のトラフィックの検査が行われます。このエンジンは、基本的なデコードを実行できるほか、データ長のオーバーフローを指定するためのパラメータを備えています。たとえば、コンピュータ A のユーザまたはプログラムがコンピュータ B のアイデンティティ要求を実行する場合、A と B の間の接続のユーザのアイデンティティのみを問い合わせることができます。B 上の ident サーバは、TCP ポート 113 上で接続をリッスンします。A 上のクライアントは接続を確立し、接続で使用されている A および B 上のポート番号を送信することで、識別情報が必要な接続を指定します。B 上のサーバはその接続を使用しているユーザを特定し、そのユーザの名前を示す文字列を A に応答します。Service IDENT エンジンでは、TCP ポート 113 で ident の悪用が検査されます。

表 B-25 に、Service IDENT エンジンに固有のパラメータを示します。

表 B-25　Service IDENT エンジンのパラメータ

パラメータ	説明	値
Inspection Type	実行する検査のタイプ： • [Has Newline]：ペイロードの終端しない改行を検査します。 • [Has Bad Port]：ペイロードの不正なポートを検査します。 • [Payload Size]：このサイズよりも長いペイロード長を検査します。	—
Service Ports	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。	0 ～ 65535[1] a-b[,c-d]
Direction	トラフィックの方向： • 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。 • 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。	From Service To Service

1. 範囲の 2 番目の数は、最初の数以上である必要があります。

詳細情報

すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Service MSRPC エンジン

Service MSRPC エンジンは、MSRPC パケットを処理します。MSRPC は、ネットワーク環境での複数のコンピュータ間の連携処理と、使用されるアプリケーション ソフトウェアに対応しています。MSRPC はトランザクションベースのプロトコルです。チャネルを確立し、処理要求および応答を受け渡す一連の通信が発生します。

MSRPC は、ISO レイヤ 5 および 6 のプロトコルで、UDP、TCP、SMB などの他のトランスポート プロトコルの上の階層となります。MSRPC エンジンには、MSRPC PDU のフラグメンテーションと再構成を処理する機能も含まれます。

この通信チャネルは、最近の Windows NT、Windows 2000、および Window XP のセキュリティ脆弱性の原因となっています。Service MSRPC エンジンは、最も一般的なトランザクション タイプについて DCE および RPC プロトコルをデコードするだけです。

表 B-26 に、Service MSRPC エンジンに固有のパラメータを示します。

表 B-26　Service MSRPC エンジンのパラメータ

パラメータ	説明	値
Protocol	このインスペクタの該当プロトコル。 • [Type]：UDP または TCP	TCP UDP
Specify Flags	設定するフラグ • MSRPC TCP フラグ • MSRPC TCP フラグ マスク	Concurrent Execution Did Not Execute First Fragment Last Fragment Maybe Semantics Object UUID Pending Cancel Reserved
Specify Operation	（任意）MSRPC 動作の使用をイネーブルにします。 • [Operation]：要求する MSRPC 動作。 SMB_COM_TRANSACTION コマンドに必要です。完全一致。	0 ～ 65535
Swap Attacker Victim	攻撃者と攻撃対象のアドレスとポート（送信元および宛先）を、アラート メッセージとアクションで入れ替える場合は [Yes]。入れ替えない場合は [No]（デフォルト）。	[Yes] | [No]
Specify Regex String	（任意）正規表現文字列の使用をイネーブルにします。 • [Specify Exact Match Offset]：完全一致オフセットをイネーブルにします。 – [Exact Match Offset]：一致を有効にするために正規表現文字列がレポートする必要がある正確なストリーム オフセット。 • [Specify Min Match Length]：最小一致長をイネーブルにします。 – [Min Match Length]：正規表現文字列が一致する必要があるバイトの最小数。	0 ～ 65535
Specify UUID	（任意）UUID をイネーブルにします。 • [UUID]：[MSRPC UUID] フィールド	000001a000000000c0000 00000000046

詳細情報

- シグニチャの正規表現構文の一覧については、「正規表現の構文」（P.B-10）を参照してください。
- すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Service MSSQL エンジン

Service MSSQL エンジンは、Microsoft SQL サーバによって使用されるプロトコルを検査します。このエンジンには 1 つの MSSQL シグニチャが含まれています。MSSQL サーバへのデフォルトの sa アカウントでのログインの試みを検出した場合にアラートを起動します。ログイン ユーザ名や、パスワードが使用されたかどうかなど、MSSQL プロトコル値に基づいてカスタム シグニチャを追加できます。

表 B-27 に、Service MSSQL エンジンに固有のパラメータを示します。

表 B-27　Service MSSQL エンジンのパラメータ

パラメータ	説明	値
Password Present	MS SQL ログインでパスワードが使用されたかどうか。	[Yes] | [No]
Specify SQL Username	（任意）SQL ユーザ名の使用をイネーブルにします。 • [SQL Username]：MS SQL サービスにログインするユーザのユーザ名（完全一致）。	sa

詳細情報

すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Service NTP エンジン

Service NTP エンジンは、NTP プロトコルを検査します。このエンジンには、1 つの NTP シグニチャ（NTP readvar オーバーフロー シグニチャ）が含まれます。このシグニチャは、サイズが大きいため NTP サービスでキャプチャできない NTP データが、readvar コマンドに指定されていることを検出した場合に、アラートを起動します。NTP プロトコルの値（モードや制御パケットのサイズなど）に基づいて、シグニチャを調整したり、カスタム シグニチャを作成したりできます。

表 B-28 に、Service NTP エンジンに固有のパラメータを示します。

表 B-28　Service NTP エンジンのパラメータ

パラメータ	説明	値
Inspection Type	実行する検査のタイプ。	
Inspect NTP Packets	NTP パケットを検査します。 • [Control Opcode]：RFC1305 の付録 B に基づく NTP 制御パケットの命令コード番号。 • [Max Control Data Size]：制御パケットで送信されるデータの最大許容量。 • [Operation Mode]：RFC 1305 に基づく NTP パケットの動作モード。	0 ～ 65535
IS Invalid Data Packet	無効な NTP データ パケットを検索します。NTP データ パケットの構造を調べ、サイズが正しいことを確認します。	[Yes] | [No]
Is Non NTP Traffic	NTP ポートの非 NTP パケットをチェックします。	[Yes] | [No]

詳細情報

すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Service P2P

P2P ネットワークでは、ファイル共有の目的で、同時にクライアントとサーバの両方の機能を果たすノードが使用されます。P2P ネットワークには、著作権が設定された資料が含まれることが多く、企業で使用することは企業ポリシーに違反する場合があります。Service P2P エンジンはそのようなネットワークをモニタし、最適化された TCP および UDP P2P プロトコル識別機能を提供します。Service P2P エンジンには次の特性があります。

- すべての TCP および UDP ポートでリッスンする
- 正規表現ではなくハードコーディングされたシグニチャを通じた高いパフォーマンス
- P2P プロトコルが認識されるか、P2P プロトコルが認識されずに 10 個のパケットが検出された後はトラフィックを無視

P2P シグニチャはハードコーディングされているため、編集可能な唯一のパラメータは Master エンジン パラメータです。

詳細情報

すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Service RPC エンジン

Service RPC エンジンは、RPC プロトコル専用で、反回避戦略としてフル デコードを行います。これにより、フラグメント化されたメッセージ（複数パケット内の 1 つのメッセージ）およびバッチ メッセージ（1 つのパケット内の複数メッセージ）を処理できます。

RPC ポート マッパーは、ポート 111 上で動作します。通常の RPC メッセージは、550 より上位であれば任意のポートで送受信できます。RPC スイープは、TCP ポート スイープと似ていますが、有効な RPC メッセージが送信された場合に一意のポートだけをカウントするという点が異なります。RPC は UDP でも動作します。

表 B-29 に、Service RPC エンジンに固有のパラメータを示します。

表 B-29　Service RPC エンジンのパラメータ

パラメータ	説明	値
Direction	トラフィックの方向。 • 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。 • 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。	From Service To Service
Protocol	該当プロトコル。	TCP UDP
Service Ports	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。	0 ～ 65535[1] a-b[,c-d]

表 B-29　Service RPC エンジンのパラメータ（続き）

パラメータ	説明	値
Specify Regex String	（任意）正規表現文字列の使用をイネーブルにします。 • [Specify Exact Match Offset]：完全一致オフセットをイネーブルにします。 – [Exact Match Offset]：一致を有効にするために正規表現文字列がレポートする必要がある正確なストリーム オフセット。 • [Specify Min Match Length]：最小一致長をイネーブルにします。 – [Min Match Length]：正規表現文字列が一致する必要があるバイトの最小数。	0 ～ 65535
Specify Spoof Src	（任意）スプーフィングの送信元アドレスをイネーブルにします。 • [Is Spoof Src]：送信元アドレスが 127.0.0.1 の場合にアラートを起動します。	[Yes] | [No]
Specify Port Map Program	（任意）ポートマッパー プログラムをイネーブルにします。 • [Port Map Program]：シグニチャのポートマッパーに送信されたプログラム番号。	0 ～ 9999999999
Specify RPC Max Length	（任意）RPC 最大長をイネーブルにします。 • [RPC Max Length]：RPC メッセージ全体の最大許容長。長さが指定した値より長いとアラートを起動します。	0 ～ 65535
Specify RPC Procedure	（任意）RPC プロシージャをイネーブルにします。 • [RPC Procedure]：シグニチャの RPC プロシージャ番号。	0 ～ 1000000
Specify RPC Program	（任意）RPC プログラムをイネーブルにします。 • [RPC Program]：シグニチャの RPC プログラム番号。	0 ～ 1000000
Swap Attacker Victim	攻撃者と攻撃対象のアドレスとポート（送信元および宛先）を、アラート メッセージとアクションで入れ替える場合は [Yes]。入れ替えない場合は [No]（デフォルト）。	[Yes] | [No]

1. 範囲の 2 番目の数は、最初の数以上である必要があります。

詳細情報

- シグニチャの正規表現構文の一覧については、「正規表現の構文」（P.B-10）を参照してください。
- すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Service SMB Advanced エンジン

（注） SMB エンジンは、SMB Advanced エンジンで置き換えられました。SMB エンジンが IDM、IME、CLI で表示される場合でも、そのシグニチャは廃止されています。つまり、新しいシグニチャには、対応する古いシグニチャの ID を使用して設定された古いパラメータがあります。SMB エンジンで使用していたカスタム シグニチャは、新しい SMB Advanced エンジンを使用して書き直してください。

Service SMB Advanced エンジンは、Microsoft SMB パケットと Microsoft RPC over SMB パケットを処理します。Service SMB Advanced エンジンは、コネクション型の MSRPC に対し、MSRPC エンジンと同じデコード方法を使用します。ただし、MSRPC パケットは SMB プロトコル上でやりとりされる必要があります。Service SMB Advanced エンジンは、TCP ポート 139 および 445 上での MSRPC over SMB をサポートしています。MSRPC エンジンの、コネクション型 DCS/RPC コードのコピーを使用しています。

表 B-30 に、Service SMB Advanced エンジンに固有のパラメータを示します。

表 B-30　Service SMB Advanced エンジンのパラメータ

パラメータ	説明	値
Service Ports	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。	0 ～ 65535 a-b[,c-d] [1]
Specify Command	（任意）SMB コマンドをイネーブルにします。 • [Command]：SMB コマンドの値。完全に一致する必要があります。SMB パケットのタイプを定義します。[2]	0 ～ 255
Specify Direction	（任意）トラフィック方向をイネーブルにします。 • [Direction]：トラフィックの方向を指定できます。 – [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。	from service to service
Specify Operation	（任意）MSRPC over SMB をイネーブルにします。 • [MSRPC Over SMB Operation]：SMB_COM_TRANSACTION コマンドに使用します。完全に一致する必要があります。	0 ～ 65535
Specify Regex String	（任意）正規表現文字列の検索をイネーブルにします。 • [Regex String]：単一の TCP パケット内で検索する正規表現。	

表 B-30　Service SMB Advanced エンジンのパラメータ（続き）

パラメータ	説明	値
Specify Exact Match Offset	（任意）完全一致オフセットをイネーブルにします。 • [Exact Match Offset]：一致を有効にするために正規表現文字列が報告する必要がある正確なストリーム オフセット。	
Specify Min Match Length	（任意）最小一致長をイネーブルにします。 • [Min Match Length]：正規表現文字列が一致する必要がある最小バイト数。	
Specify Payload Source	（任意）ペイロード送信元をイネーブルにします。 • [Payload Source]：ペイロード送信元の検査。[3]	
Specify Scan Interval	（任意）スキャン間隔をイネーブルにします。 • [Scan Interval]：アラート率の計算に使用される間隔（秒数）。	1 ～ 131071
Specify TCP Flags	（任意）TCP フラグをイネーブルにします。 • MSRPC TCP フラグ • MSRPC TCP フラグ マスク	• concurrent execution • did not execute • first fragment • last fragment • maybe • object UUID • pending cancel • reserved
Specify Type	（任意）MSRPC over SMB パケットのタイプをイネーブルにします。 • [Type]：MSRPC over SMB パケットの [Type] フィールド。	• [0] = 要求 • [2] = 応答 • [11] = バインド • [12] = バインド応答
Specify UUID	（任意）UUID を経由した MSRPC をイネーブルにします。 • [UUID]：[MSRPC UUID] フィールド。	16 進数の 0 ～ 9、a ～ f、A ～ F で構成される 32 文字の文字列。

表 B-30　Service SMB Advanced エンジンのパラメータ（続き）

パラメータ	説明	値
Specify Hit Count	（任意）ヒット カウントをイネーブルにします。 • [Hit Count]：scan-interval 内の発生回数のしきい値。この値を超えるとアラートが起動されます。	1 ～ 65535
Swap Attacker Victim	攻撃者と攻撃対象のアドレスとポート（送信元および宛先）を、アラート メッセージとアクションで入れ替える場合は [Yes]。入れ替えない場合は [No]（デフォルト）。	[Yes] | [No]

1. 範囲の 2 番目の数は、最初の数以上である必要があります。
2. 現在 37（0x25）SMB_COM_TRANSACTION コマンドと 162（0xA2）SMB_COM_NT_CREATE_ANDX コマンドがサポートされています。
3. TCP_Data ではパケット全体に正規表現が実行されし、SMB_Data では SMB ペイロードのみに正規表現が実行され、Resource_DATA では SMB_Resource に対して正規表現が実行されます。

詳細情報

- シグニチャの正規表現構文の一覧については、「正規表現の構文」（P.B-10）を参照してください。
- すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Service SNMP エンジン

Service SNMP エンジンは、ポート 161 宛のすべての SNMP パケットを検査します。特定のコミュニティ名とオブジェクト ID に基づいて、SNMP シグニチャを調整したり、カスタム SNMP シグニチャを作成したりできます。

コミュニティ名とオブジェクト ID を照合するために、文字列比較や正規表現演算を使用する代わりに、整数を使用してすべての比較を実行し、プロトコル デコードを高速化しストレージ要件を削減します。

表 B-31 に、Service SNMP エンジンに固有のパラメータを示します。

表 B-31　Service SNMP エンジンのパラメータ

パラメータ	説明	値
Inspection Type	実行する検査のタイプ。	—
Brute Force Inspection	総当たり攻撃の試行を検査します。 • [Bruce Force Count]：総当たり攻撃と見なされる一意の SNMP コミュニティ名の数。	0 ～ 65535
Invalid Packet Inspection	SNMP プロトコル違反を検査します。	—

表 B-31　Service SNMP エンジンのパラメータ（続き）

パラメータ	説明	値
Non SNMP Traffic Inspection	UDP ポート 161 宛の非 SNMP トラフィックを検査します。	—
SNMP Inspection	SNMP トラフィックを検査します。 • [Specify Community Name] [yes | no]: – [Community Name]：SNMP コミュニティ名（SNMP パスワード）を検索します。 • [Specify Object ID] [yes | no]: – [Object ID]：SNMP オブジェクト ID を検索します。	*community-name* *object-id*

詳細情報

すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Service SSH エンジン

Service SSH エンジンは、ポート 22 の SSH トラフィックに対して使用します。SSH セッションのセットアップを除いてすべてが暗号化されるため、Service SSH エンジンではセットアップのフィールドだけがモニタされます。SSH には 2 つのデフォルト シグニチャがあります。これらのシグニチャを調整することはできますが、カスタム シグニチャは作成できません。

表 B-32 に、Service SSH エンジンに固有のパラメータを示します。

表 B-32　Service SSH エンジンのパラメータ

パラメータ	説明	値
Length Type	次の SSH 長さタイプのいずれかを検査します。 • [Key Length]：検査対象の SSH キーの長さ。 – [Length]：キーがこれより長い場合は、RSAREF オーバーフローが発生します。 • [User Length]：ユーザ長の SSH 検査。 – [Length]：キーがこれより長い場合は、RSAREF オーバーフローが発生します。	0 ～ 65535
Service Ports	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。	0 ～ 65535[1] a-b[,c-d]
Specify Packet Depth	（任意）パケット数をイネーブルにします。 • [Packet Depth]：セッション キーが失われたと判断するまでにモニタするパケット数。	0 ～ 65535

1. 範囲の 2 番目の数は、最初の数以上である必要があります。

詳細情報

すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Service TNS エンジン

Service TNS エンジンでは、TNS プロトコルが検査されます。TNS では、データベース アプリケーションに対し、すべての業界標準ネットワーク プロトコルに対する単一かつ共通のインターフェイスが提供されます。TNS により、アプリケーションは、異なるプロトコルを使用して他のデータベース アプリケーションにネットワークから接続できます。デフォルトの TNS リスナー ポートは TCP 1521 です。TNS では、クライアントを別のホストまたは別の TCP ポートにリダイレクトするための REDIRECT フレームもサポートされています。REDIRECT パケットをサポートするため、TNS エンジンはすべての TCP ポート上でリッスンを行い、高速な TNS フレーム ヘッダー検証ルーチンを使用して非 TNS ストリームを無視します。

表 B-33 に、Service TNS エンジンに固有のパラメータを示します。

表 B-33　Service TNS エンジンのパラメータ

パラメータ	説明	値
Direction	トラフィックの方向。 • 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。 • 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。	From Service To Service
Type Frame Type	TNS フレーム値のタイプを指定します。 • [1]：接続 • [2]：受け入れ • [4]：拒否 • [5]：リダイレクト • [6]：データ • [11]：再送信 • [12]：マーカー	1 2 4 5 6 11 12

表 B-33　Service TNS エンジンのパラメータ（続き）

パラメータ	説明	値
Specify Regex String	（任意）正規表現文字列の使用をイネーブルにします。 • [Specify Exact Match Offset]：完全一致オフセットをイネーブルにします。 – [Exact Match Offset]：一致を有効にするために正規表現文字列がレポートする必要がある正確なストリーム オフセット。 • [Specify Min Match Length]：最小一致長をイネーブルにします。 – [Min Match Length]：正規表現文字列が一致する必要があるバイトの最小数。	0 ～ 65535
Specify Regex Payload Source	検査するプロトコルを指定します。 • [Payload Source] – [TCP Data]：TCP パケットのデータ部分に対して正規表現を実行します。 – [TNS Data]：すべての空白が削除されている TNS データに対してのみ正規表現を実行します。	TCP TNS

詳細情報

- シグニチャの正規表現構文の一覧については、「正規表現の構文」（P.B-10）を参照してください。
- すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

State エンジン

State エンジンは、TCP ストリームのステートベースおよび正規表現ベースのパターン検査を行います。State エンジンは何かの状態を保存するデバイスで、入力があるたびに、その内容に基づいてある状態から別の状態に移行したり、処理や出力を行ったりできます。ステート マシンは、出力やアラートを発生させる特定のイベントを記述するために使用されます。State エンジンには、SMTP、シスコ ログイン、および LPR フォーマット ストリングの 3 つのステート マシンがあります。

表 B-34 に、State エンジンに固有のパラメータを示します。

表 B-34　State エンジンのパラメータ

パラメータ	説明	値
State Machine	ステート マシン グループ。	• SMPT • LPR Format String • Cisco Login
Cisco Login	Cisco ログインのステート マシンを指定します。 • [State Name]：状態の名前。この状態になると、シグニチャによりアラートが起動されます。 – シスコ デバイスの状態 – Control-C 状態 – パスワード プロンプト状態 – 開始状態	• Cisco Device • Control C • Pass Prompt • Start Cisco
LPR Format String	LPR フォーマット ストリングの脆弱性を検査するステート マシンを指定します。 • [State Name]：状態の名前。この状態になると、シグニチャによりアラートが起動されます。 – LPR フォーマット ストリング検査を終了する中断状態 – フォーマット文字の状態 – 開始状態	• Abort • Format Char • Start
State Name	SMTP プロトコルのステート マシンを指定します。 • [State Name]：状態の名前。この状態になると、シグニチャによりアラートが起動されます。 – LPR フォーマット ストリング検査を終了する中断状態 – メール本文の状態 – メール ヘッダーの状態 – SMTP コマンドの状態 – 開始状態	• Abort • Mail Body • Mail Header • SMPT Commands • Start Abort
Direction	トラフィックの方向： • 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。 • 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。	From Service To Service
Service Ports	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。	0 ～ 65535[1] a-b[,c-d]

表 B-34　State エンジンのパラメータ（続き）

パラメータ	説明	値
Specify Exact Match Offset	（任意）完全一致オフセットをイネーブルにします。 • [Exact Match Offset]：一致を有効にするために正規表現文字列がレポートする必要がある正確なストリーム オフセット。	0 ～ 65535
Specify Max Match Offset	（任意）最大一致オフセットをイネーブルにします。 • [Max Match Offset]：一致を有効にするために正規表現文字列がレポートする必要がある最大ストリーム オフセット。	0 ～ 65535
Specify Min Match Offset	（任意）最小一致オフセットをイネーブルにします。 • Min Match Offset：一致を有効にするために正規表現文字列がレポートする必要がある最小ストリーム オフセット。	0 ～ 65535
Specify Min Match Length	（任意）最小一致長をイネーブルにします。 • [Min Match Length]：正規表現文字列が一致する必要があるバイトの最小数。	0 ～ 65535
Swap Attacker Victim	攻撃者と攻撃対象のアドレスとポート（送信元および宛先）を、アラート メッセージとアクションで入れ替える場合は [Yes]。入れ替えない場合は [No]（デフォルト）。	[Yes] | [No]

1. 範囲の 2 番目の数は、最初の数以上である必要があります。

詳細情報

すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

String エンジン

String エンジンは、ICMP、TCP、および UDP の各プロトコルを対象とした、汎用ベースのパターン マッチング インスペクション エンジンです。String エンジンでは、複数のパターンを 1 つのパターン マッチング テーブルにまとめることでデータ内の検索を一度に実行できる正規表現エンジンが使用されます。3 つの String エンジン、String ICMP、String TCP、および String UDP があります。

表 B-35 に、String ICMP エンジンに固有のパラメータを示します。

表 B-35　String ICMP エンジンのパラメータ

パラメータ	説明	値
Direction	トラフィックの方向： • 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。 • 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。	From Service To Service
ICMP Type	ICMP ヘッダーの TYPE 値。	0 ～ 18[1] a-b[,c-d]

表 B-35　String ICMP エンジンのパラメータ（続き）

パラメータ	説明	値
Specify Exact Match Offset	（任意）完全一致オフセットをイネーブルにします。 • [Exact Match Offset]：一致を有効にするために正規表現文字列がレポートする必要がある正確なストリーム オフセット。	0 ～ 65535
Specify Min Match Length	（任意）最小一致長をイネーブルにします。 • [Min Match Length]：正規表現文字列が一致する必要があるバイトの最小数。	0 ～ 65535
Swap Attacker Victim	攻撃者と攻撃対象のアドレスとポート（送信元および宛先）を、アラート メッセージとアクションで入れ替える場合は [Yes]。入れ替えない場合は [No]（デフォルト）。	[Yes] | [No]

1. 範囲の 2 番目の数は、最初の数以上である必要があります。

表 B-36 に、String TCP エンジンに固有のパラメータを示します。

表 B-36　String TCP エンジン

パラメータ	説明	値
Direction	トラフィックの方向： • 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。 • 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。	From Service To Service
Service Ports	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。	0 ～ 65535[1] a-b[,c-d]
Specify Exact Match Offset	（任意）完全一致オフセットをイネーブルにします。 • [Exact Match Offset]：一致を有効にするために正規表現文字列がレポートする必要がある正確なストリーム オフセット。	0 ～ 65535
Specify Min Match Length	（任意）最小一致長をイネーブルにします。 • [Min Match Length]：正規表現文字列が一致する必要があるバイトの最小数。	0 ～ 65535
Strip Telnet Options	パターンを検索する前に、データから Telnet オプション文字を削除します。[2]	[Yes] | [No]
Swap Attacker Victim	攻撃者と攻撃対象のアドレスとポート（送信元および宛先）を、アラート メッセージとアクションで入れ替える場合は [Yes]。入れ替えない場合は [No]（デフォルト）。	[Yes] | [No]

1. 範囲の 2 番目の数は、最初の数以上である必要があります。
2. このパラメータは、主に、IPS 反回避ツールとして使用します。

表 B-37 に、String UDP エンジンに固有のパラメータを示します。

表 B-37　String UDP エンジン

パラメータ	説明	値
Direction	トラフィックの方向： • 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。 • 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。	From Service To Service
Service Ports	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。	0 ～ 65535[1] a-b[,c-d]
Specify Exact Match Offset	（任意）完全一致オフセットをイネーブルにします。 • [Exact Match Offset]：一致を有効にするために正規表現文字列がレポートする必要がある正確なストリーム オフセット。	0 ～ 65535
Specify Min Match Length	（任意）最小一致長をイネーブルにします。 • [Min Match Length]：正規表現文字列が一致する必要があるバイトの最小数。	0 ～ 65535
Swap Attacker Victim	攻撃者と攻撃対象のアドレスとポート（送信元および宛先）を、アラート メッセージとアクションで入れ替える場合は [Yes]。入れ替えない場合は [No]（デフォルト）。	[Yes] | [No]

1. 範囲の 2 番目の数は、最初の数以上である必要があります。

詳細情報

- カスタム String エンジン シグニチャの例については、「String TCP エンジンのシグニチャの例」（P.10-24）を参照してください。
- すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

String XL エンジン

String XL エンジンは、他の String エンジンと同様に、シグニチャあたり 1 つの文字列のマッチング機能を備えていますが、異なる正規表現構文が使用されます。String TCP XL エンジンはストリームベースであり、クロスパケット インスペクション（XPI）が使用されます。パケットは適切な順番に並んでいる必要があります。UDP と ICMP はどちらもステートレスであるため、String UDP XL および String ICMP XL シグニチャ エンジンはセッション状態を割り当てる必要がなく、各パケットは個別に検索されます。

正規表現アクセラレータ カードは、標準の String エンジンと新しい String XL エンジンの両方で使用されます。ほとんどの標準の String エンジンのシグニチャは、変更することなく、正規表現アクセラレータ カードでコンパイルおよび解析できます。ただし、標準の String エンジンのシグニチャを正規表現アクセラレータ カード向けにコンパイルできない特殊な状況があります。そのような状況では、新しいシグニチャは、正規表現アクセラレータ カードでコンパイルできない String XL エンジンの特定のパラメータを使用して、String XL エンジンで記述されます。String XL エンジンの新しいシグニチャにより、標準の String エンジンの元のシグニチャが廃止されます。

正規表現構文または raw 表現構文を使用できますが、raw 表現構文はエキスパート ユーザ専用です。String XL シグニチャを設定するときは、raw 表現構文を使用するのでない限り、[Regex String] パラメータが必要です。

（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。

表 B-38 に、String XL エンジン（TCP、ICMP、および UDP）に固有のパラメータを示します。

表 B-38　String XL エンジンのパラメータ

パラメータ	説明	値
Direction	（必須）検査するトラフィックの方向。 • 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。 • 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。	From Service To Service
Dot All	[Yes] に設定すると、¥n を含む [¥x00-¥xFF] をマッチングされます。[No] に設定すると、¥n を除く範囲 [¥x00-¥xFF] のすべてにマッチングされます。	Yes | No（デフォルト）
End Optional	パケットの最後で他のすべての条件が満たされているものの、パケットの最後が見つからない場合、最小を超えた場合に一致が報告されます。	Yes | No（デフォルト）
ICMP Type	ICMP メッセージ タイプ。シグニチャ エンジンが String ICMP の場合に必要です。	0 ～ 18[1] a-b[,c-d]
No Case	式の中のすべてのアルファベット文字を、大文字と小文字を区別せずに扱います。	Yes | No（デフォルト）
Raw Regex	[Yes] に設定された場合、Min Match Length、Max Match Length、Min Whole Length、Max Whole Length、Dot All、UTF8、No Case、Stingy、および End Optional は、正規表現文字列を再フォーマットするために使用されません。 （注） [Raw Regex] を使用すると、raw 構文で正規表現文字列を入力でき、変換されることはありません。	Yes | No（デフォルト）
Regex String	（必須）検索で使用する正規表現パターン。 （注） このパラメータは、[Max Stream Length] が設定されている場合は必須です。[Max Stream Length] が設定されている場合は、[Regex String] を設定しないでください。	string

表 B-38　String XL エンジンのパラメータ（続き）

パラメータ	説明	値
Service Ports	（必須）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。 （注）　このパラメータは、String XL TCP および String XL UDP シグニチャ エンジンでは必須です。String XL ICMP シグニチャ エンジンでは使用できません。	0 ～ 65535[2] a-b[,c-d]
Specify Exact Match Offset	完全一致オフセットをイネーブルにします。 • [Exact Match Offset]：一致を有効にするために正規表現文字列がレポートする必要がある正確なストリーム オフセット（バイト単位）。	[Yes] | [No] 0 ～ 65535
Specify Maximum Match Offset	最大一致オフセットをイネーブルにします。 • [Maximum Match Offset]：一致を有効にするために正規表現文字列が報告する必要がある最大ストリーム オフセット（バイト単位）。	[Yes] | [No] 0 ～ 65535
Specify Min Match Offset	最小一致オフセットをイネーブルにします。 • [Min Match Offset]：一致を有効にするために正規表現文字列が報告する必要がある最小ストリーム オフセット（バイト単位）。	[Yes] | [No] 0 ～ 65535
Specify Max Match Length	最大一致長をイネーブルにします。 • [Max Match Length]：パターンが一致したと見なされるために正規表現文字列が一致する必要がある最大バイト数。	[Yes] | [No] 0 ～ 65535
Specify Min Match Length	最小一致長をイネーブルにします。 • [Min Match Length]：パターンが一致したと見なされるために正規表現文字列が一致する必要がある最小バイト数。	[Yes] | [No] 0 ～ 65535
Specify Max Stream Length	最大ストリーム長をイネーブルにします。 • [Max Stream Length]：設定された先頭数バイトに検索を制限します。ストリームの長さはこの値に対してチェックされます。ストリームにこの値よりも多くのバイトが含まれている場合、アラートが起動されます。 （注）　このパラメータを指定した場合、[Raw Regex] と [Regex String] は設定できません。	[Yes] | [No] 0 ～ 65535
Specify Max Whole Length	最大全体長をイネーブルにします。 • [Max Whole Length]：フラグメント化されないパターンの最大長。	[Yes] | [No] 0 ～ 65535
Specify Min Whole Length	最小全体長をイネーブルにします。 • [Min Whole Length]：フラグメント化されないパターンの最小長。	[Yes] | [No] 0 ～ 65535

表 B-38　String XL エンジンのパラメータ（続き）

パラメータ	説明	値
Stingy	最初に完了した一致の後、より大きな一致の検索を行いません。 （注）　[Stingy] は必ず [Min Match Length] と組み合わせて使用します。単独で使用した場合は無視されます。	Yes | No（デフォルト）
Strip Telnet Options	パターンを検索する前に、データから Telnet オプション文字を削除します。[3]	Yes | No（デフォルト）
Swap Attacker Victim	攻撃者と攻撃対象のアドレスとポート（送信元および宛先）を、アラート メッセージとアクションで入れ替える場合は [Yes]。入れ替えない場合は [No]（デフォルト）。	Yes | No（デフォルト）
UTF8	式の中のすべての適正な UTF-8 バイト シーケンスを 1 個の文字として扱います。	Yes | No（デフォルト）

1. 範囲の 2 番目の数は、最初の数以上である必要があります。
2. 範囲の 2 番目の数は、最初の数以上である必要があります。
3. このパラメータは、主に、IPS 反回避ツールとして使用します。

サポートされないパラメータ

String XL エンジンには [End Optional] および [Specify Max Stream Length] パラメータがありますが、IPS 7.1(1)E4 ではディセーブルになっています。これらのパラメータを設定しようとするとエラー メッセージが表示されます。たとえば、[Specify Max Stream Length] を使用してシグニチャを作成し、保存しようとすると、次のエラー メッセージが表示されます。

```
Apply Changes?[yes]: yes
Error: string-xl-tcp 60003.0 : Maximum Stream Length is currently not supported.
Please don't use this option.

The configuration changes failed validation, no changes were applied.
Would you like to return to edit mode to correct the errors? [yes]:
```

詳細情報

- シグニチャの正規表現構文の一覧については、「正規表現の構文」（P.B-10）を参照してください。
- すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。
- String XL エンジンの一致オフセット シグニチャの例については、「String XL エンジンの Match Offset シグニチャの例」（P.9-28）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については、「String XL エンジンの最小一致長シグニチャの例」（P.9-31）を参照してください。

Sweep エンジン

ここでは、Sweep エンジンについて説明します。内容は次のとおりです。

Sweep エンジン

Sweep エンジンでは、2 つのホスト間または 1 つのホストから多数のホストへのトラフィックを分析します。既存のシグニチャを調整したり、カスタム シグニチャを作成したりすることができます。Sweep エンジンには、ICMP、UDP、および TCP のプロトコル固有パラメータがあります。

Sweep エンジンのアラート条件は、最終的に一意のパラメータのカウントに依存します。一意のパラメータは、スイープのタイプに応じた、個別ホストまたはポートの数のしきい値です。一意のパラメータは、期間内に一意のポート数またはホスト数がアドレス セット上に存在するとアラートをトリガーします。一意のポートおよびホストのトラッキング処理をカウンティングと言います。

注意　送信元および宛先 IP アドレスに基づくイベント アクション フィルタは Sweep エンジンでは機能しません。これは、これらのフィルタが、通常のシグニチャとしてフィルタしないためです。送信元および宛先 IP アドレスをスイープ アラートでフィルタするには、Sweep エンジン シグニチャの送信元および宛先 IP アドレス フィルタ パラメータを使用します。

Sweep エンジンのすべてのシグニチャに一意のパラメータを指定する必要があります。スイープでは、2 ～ 40（それぞれの値を含む）の制限値が強制されます。スイープの絶対最小値は 2 です。それ以外は（1 つのホストまたはポートの）スイープではありません。40 は、スイープによってメモリが過剰に消費されないように強制する必要がある場合の実際的な最大値です。一意の範囲の現実的な値は、5 ～ 15 です。

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

DataNode

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

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

表 B-39 に、Sweep エンジンに固有のパラメータを示します。

表 B-39　Sweep エンジンのパラメータ

パラメータ	説明	値
Destination Address Filter	スイープ カウント アルゴリズムから除外する宛先 IP アドレス。	<A.B.C.D>-<A.B.C.D> [,<A.B.C.D>-<A.B.C.D>]
Source Address Filter	スイープ カウント アルゴリズムから除外する送信元 IP アドレス。	<A.B.C.D>-<A.B.C.D> [,<A.B.C.D>-<A.B.C.D>]

表 B-39　Sweep エンジンのパラメータ（続き）

パラメータ	説明	値
Protocol	このインスペクタの該当プロトコル。	• ICMP • UDP • TCP
Specify ICMP Type	（任意）ICMP ヘッダー タイプの検査をイネーブルにします。 • [ICMP Type]：ICMP ヘッダーの TYPE 値を指定します。	0 ～ 255
Specify Port Range	（任意）検査でのポート範囲の使用をイネーブルにします。 • [Port Range]：検査で使用する UDP ポート範囲。	0 ～ 65535 a-b[,c-d]
Fragment Status	フラグメントが必要かどうかを指定します。 • 任意のフラグメント ステータス • フラグメントを検査しない • フラグメントを検査する	• Any • No Fragment • Want Fragment
Inverted Sweep	一意のカウントの対象として宛先ポートではなく送信元ポートを使用します。	[Yes] | [No]
Mask	TCP フラグの比較に使用するマスク： • URG ビット • ACK ビット • PSH ビット • RST ビット • SYN ビット • FIN ビット	• URG • ACK • PSH • RST • SYN • FIN
Storage Key	固定データを保存するために使用するアドレス キーのタイプ。 • 攻撃者のアドレス • 攻撃者と攻撃対象のアドレス • 攻撃者のアドレスと攻撃対象のポート	Axxx AxBx Axxb
Suppress Reverse	このアドレス セットで反対方向にスイープが実行されている場合、アラートを起動しません。	[Yes] | [No]
Swap Attacker Victim	攻撃者と攻撃対象のアドレスとポート（送信元および宛先）を、アラート メッセージとアクションで入れ替える場合は [Yes]。入れ替えない場合は [No]（デフォルト）。	[Yes] | [No]

表 B-39　Sweep エンジンのパラメータ（続き）

パラメータ	説明	値
TCP Flags	マスクによってマスクされた場合に照合する TCP フラグ。 • URG ビット • ACK ビット • PSH ビット • RST ビット • SYN ビット • FIN ビット	• URG • ACK • PSH • RST • SYN • FIN
Unique	2 つのホスト間の一意のポート接続数のしきい値。	0 ～ 65535

詳細情報

すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Sweep Other TCP エンジン

Sweep Other TCP エンジンは、2 台のホスト間のトラフィックを分析し、一般に攻撃対象を特定するために使用する異常なパケットを探します。既存のシグニチャを調整したり、カスタム シグニチャを作成したりすることができます。

TCP スイープには、TCP フラグとマスクが指定されている必要があります。TCP フラグのセット中で、複数のエントリを指定できます。また、特定のパケットを除外するためのポート範囲を必要に応じて指定できます。

表 B-40 に、Sweep Other TCP エンジンに固有のパラメータを示します。

表 B-40　Sweep Other TCP エンジンのパラメータ

パラメータ	説明	値
Specify Port Range	（任意）検査でのポート範囲の使用をイネーブルにします。 • [Port Range]：検査で使用する UDP ポート範囲。	0 ～ 65535 a-b[,c-d]
Set TCP Flags	照合する TCP フラグを設定します。 • [TCP Flags]：検査で使用される TCP フラグ。 – URG ビット – ACK ビット – PSH ビット – RST ビット – SYN ビット – FIN ビット	• URG • ACK • PSH • RST • SYN • FIN

詳細情報

すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Traffic Anomaly エンジン

（注）　異常検出シグニチャを編集または調整できますが、カスタム異常検出シグニチャは作成できません。

Traffic Anomaly エンジンには、3 つのプロトコル（TCP、UDP、およびその他）をカバーする 9 つの異常検出シグニチャが含まれます。各シグニチャには 2 つのサブシグニチャがあります。一方はスキャナ用で、もう一方はワームに感染したホスト（またはワーム攻撃されているスキャナ）用です。異常検出は、異常を検出すると、これらのシグニチャのアラートをトリガーします。すべての異常検出シグニチャは、デフォルトでイネーブルになり、各シグニチャのアラート重大度は高く設定されます。

スキャナが検出されても、ヒストグラム異常が発生しない場合、スキャナ シグニチャはその攻撃者（スキャナ）の IP アドレスをファイルに保存します。ヒストグラム シグニチャがトリガーされた場合は、スキャンを行っている攻撃者のアドレスによってそれぞれ（スキャナ シグニチャではなく）ワーム シグニチャがトリガーされます。ヒストグラムがトリガーされているので、アラートの詳細には、ワーム検出に使用されたしきい値が表示されます。その時点から、すべてのスキャナがワーム感染ホストとして検出されます。

次の異常検出イベント アクションが可能です。

- [Product Alert]：イベント ストアにイベントを書き込みます。
- [Deny Attacker Inline]：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。
- [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 ロギングを開始します。
- [Log Attacker/Victim Pair Packets]：攻撃者と攻撃対象のアドレス 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。
- [Deny Attacker Service Pair Inline]：送信元 IP アドレスと宛先ポートをブロックします。
- [Request SNMP Trap]：NotificationApp に、SNMP 通知を実行するための要求を送信します。
- [Request Block Host]：このホスト（攻撃者）をブロックする要求を ARC に送信します。

表 41 に、異常検出ワーム シグニチャを示します。

表 41　異常検出ワーム シグニチャ

シグニチャ ID	サブシグニチャ ID	名前	説明
13000	0	Internal TCP Scanner	内部ゾーンで TCP プロトコル上に単一スキャナを識別しました。
13000	1	Internal TCP Scanner	内部ゾーンで TCP プロトコル上にワーム攻撃を識別しました。TCP ヒストグラムのしきい値を超え、TCP プロトコル上にスキャナが識別されました。
13001	0	Internal UDP Scanner	内部ゾーンで UDP プロトコル上に単一スキャナを識別しました。
13001	1	Internal UDP Scanner	内部ゾーンで UDP プロトコル上にワーム攻撃を識別しました。UDP ヒストグラムのしきい値を超え、UDP プロトコル上にスキャナが識別されました。

表 41　異常検出ワーム シグニチャ（続き）

シグニチャ ID	サブシグニチャ ID	名前	説明
13002	0	Internal Other Scanner	内部ゾーンでその他のプロトコル上に単一スキャナを識別しました。
13002	1	Internal Other Scanner	内部ゾーンでその他のプロトコル上にワーム攻撃を識別しました。その他のヒストグラムのしきい値を超え、その他のプロトコル上にスキャナが識別されました。
13003	0	External TCP Scanner	外部ゾーンで TCP プロトコル上に単一スキャナを識別しました。
13003	1	External TCP Scanner	外部ゾーンで TCP プロトコル上にワーム攻撃を識別しました。TCP ヒストグラムのしきい値を超え、TCP プロトコル上にスキャナが識別されました。
13004	0	External UDP Scanner	外部ゾーンで UDP プロトコル上に単一スキャナを識別しました。
13004	1	External UDP Scanner	外部ゾーンで UDP プロトコル上にワーム攻撃を識別しました。UDP ヒストグラムのしきい値を超え、UDP プロトコル上にスキャナが識別されました。
13005	0	External Other Scanner	外部ゾーンでその他のプロトコル上に単一スキャナを識別しました。
13005	1	External Other Scanner	外部ゾーンでその他のプロトコル上にワーム攻撃を識別しました。その他のヒストグラムのしきい値を超え、その他のプロトコル上にスキャナが識別されました。
13006	0	Illegal TCP Scanner	不正ゾーンで TCP プロトコル上に単一スキャナを識別しました。
13006	1	Illegal TCP Scanner	不正ゾーンで TCP プロトコル上にワーム攻撃を識別しました。TCP ヒストグラムのしきい値を超え、TCP プロトコル上にスキャナが識別されました。
13007	0	Illegal UDP Scanner	不正ゾーンで UDP プロトコル上に単一スキャナを識別しました。
13007	1	Illegal UDP Scanner	不正ゾーンで UDP プロトコル上にワーム攻撃を識別しました。UDP ヒストグラムのしきい値を超え、UDP プロトコル上にスキャナが識別されました。
13008	0	Illegal Other Scanner	不正ゾーンでその他のプロトコル上に単一スキャナを識別しました。
13008	1	Illegal Other Scanner	不正ゾーンでその他のプロトコル上にワーム攻撃を識別しました。その他のヒストグラムのしきい値を超え、その他のプロトコル上にスキャナが識別されました。

詳細情報

すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Traffic ICMP エンジン

Traffic ICMP エンジンは、TFN2K、LOKI、DDoS などの非標準プロトコルを分析します。このエンジンには、ユーザが設定可能なパラメータを持つ 2 つのシグニチャ（LOKI プロトコルに基づく）だけが含まれます。

TFN2K は、TFN の新しいバージョンです。TFN2K は DDoS エージェントの一種であり、感染した複数のコンピュータ（ゾンビ）による協調した攻撃（何百または何千もの未知の攻撃ホストから 1 つのコンピュータまたはドメインに向けて偽のトラフィック フラッドを送信する攻撃）を制御します。TFN2K はランダムに抽出されたパケット ヘッダー情報を送信しますが、それにはシグニチャの定義に使用できる 2 つの識別子が付いています。1 つは L3 チェックサムが不正かどうかを示し、もう 1 つはペイロードの末尾に文字 64「A」が検出されたかどうかを示します。TFN2K は、任意のポートで実行可能であり、ICMP、TCP、UDP、またはこれらのプロトコルの組み合わせを使用して通信できます。

LOKI は、バック ドア型トロイの木馬タイプです コンピュータが感染すると、悪意のあるコードにより ICMP トンネルが作成されます。この ICMP トンネルは、ICMP 応答内での小さなペイロードの送信に使用されるおそれがあります（ICMP をブロックするように設定していないと、ICMP 応答はファイアウォールを通過することがあります）。LOKI シグニチャは、ICMP エコーの要求と応答のアンバランス、簡易 ICMP コード、およびペイロード識別子をモニタします。

（TFN2K を除く）DDOS カテゴリは、ICMP ベースの DDOS エージェントを対象とします。ここで使用する主なツールは、TFN と Stacheldraht です。これらは TFN2K と同様に動作しますが、ICMP だけに依存し、固定コマンド（整数および文字列）を備えています。

表 B-42 に、Traffic ICMP エンジンに固有のパラメータを示します。

表 B-42　Traffic ICMP エンジンのパラメータ

パラメータ	説明	値
Parameter Tunable Sig	設定可能なパラメータがシグニチャに存在するかどうか。	[Yes] | [No]
Inspection Type	実行する検査のタイプ： • 最初の LOKI トラフィックを検査する • 変更された LOKI トラフィックを検査する	Is Loki Is Mod Loki
Reply Ratio	要求と応答のアンバランス。要求と比べて、応答が指定した数より多い場合に、アラートを起動します。	0 ～ 65535
Want Request	アラートを起動する前に、ECHO REQUEST の検出が必要となります。	[Yes] | [No]

詳細情報

すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

Trojan エンジン

Trojan エンジンは、BO2K や TFN2K などの非標準プロトコルを分析します。Trojan エンジンには、Trojan BO2K、TrojanTFN2K、および Trojan UDP の 3 つの種類があります。

BO は、Windows を標的とした最初のバック ドア型トロイの木馬です。この BO は UDP 上でのみ実行されます。BO は、まもなく BO2K で置き換えられました。BO2K は、基本的な XOR 暗号を利用する UDP と TCP のどちらにも対応していました。特定のクロスパケット特性を持つプレーン BO ヘッダーが使用されています。

BO2K には、BO ヘッダーを暗号化し、クロスパケット パターンをほぼ認識不能にする、隠蔽用の TCP モジュールも含まれています。BO と BO2K の UDP モードは、Trojan UDP エンジンによって処理されます。TCP モードは Trojan BO2K エンジンによって処理されます。

（注）　Trojan エンジンには、Trojan UDP エンジンの [Swap Attacker Victim] を除き、固有のパラメータはありません。

詳細情報

すべてのシグニチャ エンジンに共通のパラメータの詳細については、「Master エンジン」（P.B-4）を参照してください。

APPENDIX C

トラブルシューティングのヒントと手順

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

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

この付録にはトラブルシューティングに関するヒントと、センサーおよびソフトウェアに関する手順が含まれています。内容は次のとおりです。

Bug Toolkit

Bug Toolkit を使用して、ソフトウェア バージョン、フィーチャ セット、およびキーワードに基づいて既知のバグを検索します。結果の表に、各バグがいつ統合されたか、該当する場合は、いつ修正されたかが表示されます。また、検索結果をバグ グループに保存し、それらのグループに新しい不具合アラートを提供できる永続的アラート エージェントを作成できます。

（注）　Bug Toolkit にアクセスするには、Cisco.com にログインする必要があります。

Bug Toolkit にアクセスするには、次の URL を使用してください。

http://tools.cisco.com/Support/BugToolKit/action.do?hdnAction=searchBugs

予防保守

ここでは、センサーの予防保守を実行する方法について説明します。内容は次のとおりです。

予防保守について

次の処理は、センサーの維持に役立ちます。

- 適切な設定をバックアップします。現在の設定が使用不可能になっても、それをバックアップ バージョンと交換することができます。
- バックアップ設定をリモート システムに保存します。
- 手動アップグレードは、必ず設定をバックアップしてから行ってください。自動アップグレードが設定されている場合は、定期バックアップを必ず実施してください。
- サービス アカウントを作成します。サービス アカウントは、TAC の指示による特別なデバッグを行う状況で必要になります。

注意　サービス アカウントを作成するかどうかは、慎重に検討する必要があります。サービス アカウントは、システムへのシェル アクセスを提供するため、システムが脆弱になります。状況を分析して、システムにサービス アカウントを存在させるかどうかを決定してください。

詳細情報

- コンフィギュレーション ファイルのバックアップ手順については、「バックアップ コンフィギュレーション ファイルの作成と使用」（P.C-3）を参照してください。
- リモート サーバを使用して、コンフィギュレーション ファイルをコピーおよび復元する手順については、「リモート サーバを使用したコンフィギュレーション ファイルのバックアップと復元」（P.C-3）を参照してください。

- サービス アカウントの詳細については、「サービス アカウントの作成」（P.C-5）を参照してください。

バックアップ コンフィギュレーション ファイルの作成と使用

設定を保護するために、現在の設定のバックアップを作成し、表示することによってそれが保存したい設定であることを確認できます。この設定を復元する必要があるときは、バックアップ コンフィギュレーション ファイルを現在の設定とマージするか、現在のコンフィギュレーション ファイルにバックアップ コンフィギュレーション ファイルを上書きします。

現在の設定をバックアップするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　現在の設定を保存します。現在の設定がバックアップ ファイルに保存されます。

```
sensor# copy current-config backup-config
```

ステップ 3　バックアップ コンフィギュレーション ファイルを表示します。バックアップ コンフィギュレーション ファイルが表示されます。

```
sensor# more backup-config
```

ステップ 4　バックアップの設定を現在の設定とマージすることも、現在の設定を上書きすることもできます。

- バックアップの設定を現在の設定とマージします。

  ```
  sensor# copy backup-config current-config
  ```

- バックアップの設定で現在の設定を上書きします。

  ```
  sensor# copy /erase backup-config current-config
  ```

リモート サーバを使用したコンフィギュレーション ファイルのバックアップと復元

（注）　アップグレードの前に、リモート サーバに現在のコンフィギュレーション ファイルをコピーすることをお勧めします。

copy [**/erase**] *source_url destination_url keyword* コマンドを使用して、コンフィギュレーション ファイルをリモート サーバにコピーします。その後、リモート サーバから現在の設定を復元できます。まず、現在の設定をバックアップするように求めるメッセージが表示されます。

オプション

次のオプションが適用されます。

- **/erase**：コピーの前にコピー先のファイルを消去します。

  このキーワードは、current-config のみに適用されます。backup-config は常に上書きされます。このキーワードがコピー先の current-config に対して指定されている場合、コピー元の設定がシステムのデフォルト設定に適用されます。コピー先の current-config に対して指定されていない場合、コピー元の設定が current-config とマージされます。

- *source_url*：コピーするコピー元ファイルの場所。URL またはキーワードです。
- *destination_url*：コピーするコピー先のファイルの場所。URL またはキーワードです。
- **current-config**：現在実行されている設定。コマンドが入力されると設定は永続的になります。
- **backup-config**：設定のバックアップのストレージの場所。

コピー元およびコピー先の URL の形式は、ファイルによって変わります。次に有効なタイプを示します。

- ftp:：FTP ネットワーク サーバのコピー元またはコピー先の URL。このプレフィクスの構文は、次のとおりです。

  ftp:[//[username@] location]/relativeDirectory]/filename

  ftp:[//[username@]location]//absoluteDirectory]/filename

- scp:：SCP ネットワーク サーバのコピー元またはコピー先の URL。このプレフィクスの構文は、次のとおりです。

  scp:[//[username@] location]/relativeDirectory]/filename

  scp:[//[username@] location]//absoluteDirectory]/filename

（注） FTP または SCP プロトコルを使用する場合、パスワードの入力を求められます。SCP プロトコルを使用する場合は、SSH の既知ホスト リストにリモート ホストを追加する必要があります。

- http:：Web サーバのコピー元 URL。このプレフィクスの構文は、次のとおりです。

  http:[[/[username@]location]/directory]/filename

- https:：Web サーバのコピー元 URL。このプレフィクスの構文は、次のとおりです。

  https:[[/[username@]location]/directory]/filename

（注） Web サイトにアクセスするためにユーザ名が必要な場合は、HTTP および HTTPS ではパスワードの入力が求められます。HTTPS プロトコルを使用する場合、リモート ホストは TLS の信頼できるホストである必要があります。

注意 検知インターフェイスと仮想センサーが同じ設定ではない場合、別のセンサーからコンフィギュレーション ファイルをコピーすると、エラーが発生する可能性があります。

リモート サーバへの現在の設定のバックアップ

現在の設定をリモート サーバにバックアップするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　現在の設定をリモート サーバにバックアップします。

```
sensor# copy current-config scp://user@192.0.2.0//configuration/cfg current-config
Password: ********
Warning: Copying over the current configuration may leave the box in an unstable state.
Would you like to copy current-config to backup-config before proceeding? [yes]:
```

ステップ 3　**yes** と入力して、現在の設定をバックアップ設定にコピーします。

```
cfg            100% |*********************************************| 36124       00:00
```

バックアップ ファイルからの現在の設定の復元

バックアップ ファイルから現在の設定を復元するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　現在の設定をリモート サーバにバックアップします。

```
sensor# copy scp://user@192.0.2.0//configuration/cfg current-config
Password: ********
Warning: Copying over the current configuration may leave the box in an unstable state.
Would you like to copy current-config to backup-config before proceeding? [yes]:
```

ステップ 3　**yes** と入力して、現在の設定をバックアップ設定にコピーします。

```
cfg            100% |*********************************************| 36124       00:00

Warning: Replacing existing network-settings may leave the box in an unstable state.
Would you like to replace existing network settings
(host-ipaddress/netmask/gateway/access-list) on sensor before proceeding? [no]:
sensor#
```

ステップ 4　現在設定されているホスト名、IP アドレス、サブネット マスク、管理インターフェイス、およびアクセス リストを保持する場合は、**no** を入力します。他の設定の復元後もセンサーへのアクセスを維持するために、この情報を保持することをお勧めします。

詳細情報

サポートされている HTTP/HTTPS サーバのリストについては、「サポートされる FTP サーバおよび HTTP/HTTPS サーバ」（P.25-2）を参照してください。

サービス アカウントの作成

トラブルシューティングの際に使用する TAC 用のサービス アカウントを作成できます。センサーには複数のユーザがアクセスできますが、センサーに対するサービス権限を持てるのは 1 人のユーザだけです。サービス アカウントは、サポートの目的のためにのみ使用します。

サービス アカウントが作成されると、root ユーザのパスワードはサービス アカウントのパスワードに同期化されます。root でアクセスするには、サービス アカウントでログインしてから **su - root** コマンドを使用してユーザ root に切り替える必要があります。

注意　TAC の指示に基づく場合を除き、サービス アカウントを使用してセンサーに変更を加えないでください。サービス アカウントを使用してセンサーを設定すると、その設定は TAC のサポート対象外になります。サービス アカウントを使用してオペレーティング システムにサービスを追加すると、他の IPS サービスの特定のパフォーマンスと機能に影響を及ぼします。TAC は、追加のサービスが加えられたセンサーをサポートしません。

注意　サービス アカウントを作成するかどうかは、慎重に検討する必要があります。サービス アカウントは、システムへのシェル アクセスを提供するため、システムが脆弱になります。ただし、管理者のパスワードが失われた場合は、サービス アカウントを使用してパスワードを作成できます。状況を分析して、システムにサービス アカウントを存在させるかどうかを決定してください。

サービス アカウントを追加するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　コンフィギュレーション モードを開始します。

```
sensor# configure terminal
```

ステップ 3　サービス アカウントのパラメータを指定します。ユーザ名は、^[A-Za-z0-9()+:,_/-]+$ の形式で入力します。ユーザ名は、文字または数字で始まり、A ～ Z（大文字または小文字）、0 ～ 9 の数字、「-」および「_」を含み、長さが 1 ～ 64 文字であることが必要です。

```
sensor(config)# user username privilege service
```

ステップ 4　入力を要求されたらパスワードを指定します。パスワードは、センサー管理者が設定した要件に従っている必要があります。このセンサーに対してサービス アカウントがすでに存在する場合は、次のエラー メッセージが表示され、サービス アカウントは作成されません。

```
Error: Only one service account allowed in UserAccount document
```

ステップ 5　コンフィギュレーション モードを終了します。

```
sensor(config)# exit
sensor#
```

サービス アカウントを使用して CLI にログインすると、次の警告が表示されます。

```
************************ WARNING ****************************************************
UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. This account is intended to be
used for support and troubleshooting purposes only. Unauthorized modifications are not
supported and will require this device to be reimaged to guarantee proper operation.
*****************************************************************************************
```

ディザスタ リカバリ

ここでは、推奨事項と、障害発生後にセンサーの復旧が必要な場合に実行する手順について説明します。

次に示す推奨事項に従い、障害に備えてください。

- 設定に CLI、IDM、または IME を使用している場合は、変更を加えるたびに現在の設定をセンサーから FTP または SCP サーバにコピーします。
- その設定に対する特定のソフトウェア バージョンをメモします。コピーされた設定は、同じバージョンのセンサーにしか適用できません。
- また、そのセンサー上で使用されているユーザ ID のリストも必要です。ユーザ ID およびパスワードのリストは、設定内に保存されません。

障害が発生したときにセンサーの復旧が必要な場合は、次の作業を行ってみてください。

1. センサーのイメージを再作成します。
2. デフォルトのユーザ ID とパスワード（**cisco**）を使用してセンサーにログインします。

（注）　パスワード **cisco** の変更を求めるプロンプトが表示されます。

3. センサーを初期化します。
4. センサーのアップグレードを行い、最後に設定が保存およびコピーされたときにセンサーに搭載されていた IPS ソフトウェア バージョンにします。

警告　**センサーを障害発生前にセンサーに搭載されていた IPS ソフトウェア バージョンに戻さずに、保存された設定のコピーを試みると、設定エラーを引き起こす場合があります。**

5. 最後に保存された設定をセンサーにコピーします。
6. クライアントを更新して、センサーの新しいキーと証明書を使用します。

   イメージを再作成すると、センサーの SSH キーと HTTPS 証明書が変更されるので、ホストを SSN の既知のホスト リストに追加し直す必要があります。
7. 前のユーザを作成します。

詳細情報

- コンフィギュレーション ファイルのバックアップ手順については、「バックアップ コンフィギュレーション ファイルの作成と使用」（P.C-3）を参照してください。
- センサー上の現在のユーザのリストを取得する手順については、「認証およびユーザの設定」（P.6-18）を参照してください。
- センサーのイメージを再作成する手順については、第 25 章「システム イメージのアップグレード、ダウングレード、およびインストール」を参照してください。
- **setup** コマンドを使用してセンサーを初期化する手順については、第 23 章「センサーの初期化」を参照してください。
- IPS ソフトウェアを入手し、インストールする方法については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。
- リモート サーバを使用して、コンフィギュレーション ファイルをコピーおよび復元する手順については、「リモート サーバを使用したコンフィギュレーション ファイルのバックアップと復元」（P.C-3）を参照してください。
- ホストを SSH の既知のホスト リストに追加する手順については、「既知のホスト キーの定義」（P.14-6）を参照してください。
- ユーザの追加手順については、「認証およびユーザの設定」（P.6-18）を参照してください。

パスワードの回復

ほとんどの IPS プラットフォームでは、サービス アカウントを使用したり、センサーのイメージを再作成したりせずに、センサー上でパスワードを回復できるようになりました。ここでは、各種 IPS プラットフォームのパスワードの回復方法について説明します。内容は次のとおりです。

- 「パスワードの回復について」（P.C-8）

パスワードの回復について

パスワード回復の実装は、IPS プラットフォームの要件によって異なります。パスワードの回復は、cisco 管理者アカウントに対してのみ実装され、デフォルトでイネーブルになっています。IPS 管理者は、その後 CLI を使用して他のアカウントのユーザ パスワードを回復できます。シスコのユーザ パスワードは **cisco** に戻るため、次回ログイン後に変更する必要があります。

（注） 管理者は、セキュリティ上の理由から、パスワードの回復機能をディセーブルにしなければならない場合があります。

表 C-1 に、プラットフォーム別のパスワード回復方法を示します。

表 C-1　プラットフォーム別のパスワード回復方法

プラットフォーム	説明	回復方法
4200 シリーズ センサー	スタンドアロン IPS アプライアンス	GRUB プロンプトまたは ROMMON
AIM IPS NME IPS	ルータ IPS モジュール	ブートローダ コマンド
AIP SSM AIP SSC-5 IPS SSP	ASA 5500 シリーズ適応型セキュリティ アプライアンス モジュール	適応型セキュリティ アプライアンス の CLI コマンド
IDSM2	スイッチ IPS モジュール	メンテナンス パーティションからイメージをダウンロード

アプライアンスのパスワードの回復

ここでは、アプライアンスのパスワードを回復する 2 つの方法について説明します。内容は次のとおりです。

GRUB メニューの使用

4200 シリーズのアプライアンスでは、パスワードの回復には、ブートアップ中に表示される GRUB メニューを使用します。GRUB メニューが表示されたら、任意のキーを押してブート プロセスを停止します。

（注）　GRUB メニューを使用してパスワードを回復するには、ターミナル サーバを使用するか、アプライアンスとの直接シリアル接続が必要です。

アプライアンスでパスワードを回復するには、次の手順を実行します。

ステップ 1　アプライアンスをリブートして、GRUB メニューを表示します。

```
GNU GRUB version 0.94 (632K lower / 523264K upper memory)
------------------------------------------
0: Cisco IPS
1: Cisco IPS Recovery
2: Cisco IPS Clear Password (cisco)
------------------------------------------

    Use the ^ and v keys to select which entry is highlighted.
    Press enter to boot the selected OS, 'e' to edit the
    Commands before booting, or 'c' for a command-line.

    Highlighted entry is 0:
```

ステップ 2　任意のキーを押して、ブート プロセスを停止します。

ステップ 3　**2: Cisco IPS Recovery** を選択します。

パスワードが **cisco** にリセットされます。次に CLI にログインするときにパスワードを変更できます。

ROMMON の使用

IPS 4240 と IPS 4255 では、ROMMON を使用して、パスワードを回復できます。ROMMON CLI にアクセスするには、ターミナル サーバまたは直接接続からセンサーをリブートして、ブート プロセスを中断します。

ROMMON CLI を使用してパスワードを回復するには、次の手順を実行します。

ステップ 1　アプライアンスをリブートします。

ステップ 2　ブート プロセスを中断するには、**ESC** または **Control-R**（ターミナル サーバ）を押すか、**BREAK** コマンドを送信します（直接接続）。

ブート コードによって 10 秒間停止するか、次のようなメッセージが表示されます。

- `Evaluating boot options`
- `Use BREAK or ESC to interrupt boot`

ステップ 3　次のコマンドを入力してパスワードをリセットします。

```
confreg=0x7
boot
```

サンプル ROMMON セッション：

```
Booting system, please wait...
CISCO SYSTEMS
Embedded BIOS Version 1.0(11)2 01/25/06 13:21:26.17
...
Evaluating BIOS Options...
Launch BIOS Extension to setup ROMMON
Cisco Systems ROMMON Version (1.0(11)2) #0: Thu Jan 26 10:43:08 PST 2006
Platform IPS 4240-K9
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.
Management0/0
Link is UP
MAC Address:000b.fcfa.d155
Use ? for help.
rommon #0> confreg 0x7
Update Config Register (0x7) in NVRAM...
rommon #1> boot
```

AIM IPS パスワードの回復

AIM IPS のパスワードを回復するには、**clear password** コマンドを使用します。AIM IPS へのコンソール アクセスとルータへの管理者アクセス権が必要です。

AIM IPS のパスワードを回復するには、次の手順を実行します。

ステップ 1　ルータにログインします。

ステップ 2　ルータで特権 EXEC モードを開始します。

```
router> enable
```

ステップ 3　ルータのモジュール スロット番号を確認します。

```
router# show run | include ids-sensor
interface IDS-Sensor0/0
router#
```

ステップ 4　AIM IPS との間にセッションを確立します。

```
router# service-module ids-sensor slot/port session
```

例：

```
router# service-module ids-sensor 0/0 session
```

ステップ 5　**Control-shift-6** のあとで **x** を押して、ルータ CLI に移動します。

ステップ 6　ルータ コンソールから AIM IPS をリセットします。

```
router# service-module ids-sensor 0/0 reset
```

ステップ 7　**Enter** を押して、ルータ コンソールに戻ります。

ステップ 8　ブート オプションのプロンプトが表示されたら、素早く ******* を入力します。ブートローダが起動されます。

ステップ 9　パスワードをクリアします。

```
ServicesEngine boot-loader# clear password
```

AIM IPS がリブートされます。パスワードが **cisco** にリセットされます。ユーザ名 **cisco** とパスワード **cisco** を使用して CLI にログインします。これで、パスワードを変更できます。

AIP SSM、AIP SSC-5、および IPS SSP のパスワードの回復

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

CLI または ASDM を使用して AIP SSM、AIP SSC-5、および IPS SSP のパスワードをデフォルト（**cisco**）にリセットできます。パスワードをリセットすると、AIP SSM、AIP SSC-5、および IPS SSP がリブートされます。リブート中、IPS サービスは利用できません。

（注） AIP SSM のパスワードをリセットするには、ASA 7.2.(2) 以降が必要です。AIP SSC-5 のパスワードをリセットするには、ASA 8.2.(1) 以降が必要です。IPS SSP のパスワードをリセットするには、ASA 8.2(4.4) 以降および ASA 8.4(2) 以降が必要です。ASA 8.3(*x*) ではサポートされていません。

hw-module module *slot_number* **password-reset** コマンドを使用して、パスワードをデフォルトの **cisco** にリセットします。ASA 5500 シリーズの適応型セキュリティ アプライアンスは、ROMMON の confreg ビットを 0x7 に設定し、センサーをリブートします。ROMMON ビットによって、GRUB メニューのデフォルトがオプション 2（[reset password]）に設定されます。

指定されたスロットのモジュールにパスワードの回復をサポートしない IPS バージョンがある場合、次のエラー メッセージが表示されます。

```
ERROR: the module in slot <n> does not support password recovery.
```

ASDM の使用

ASDM でパスワードをリセットするには、次の手順を実行します。

ステップ 1　ASDM メニュー バーで、[Tools] > [IPS Password Reset] を選択します。

（注） IPS モジュールがインストールされていない場合、このオプションはメニューに表示されません。

ステップ 2　[IPS Password Reset] 確認ダイアログボックスで [OK] をクリックして、パスワードをデフォルト（**cisco**）にリセットします。ダイアログボックスに、パスワードのリセットが正常に完了したか、失敗したかが表示されます。リセットが失敗した場合は、ソフトウェア バージョンが正しいことを確認してください。

ステップ 3　[Close] をクリックして、ダイアログボックスを閉じます。AIP SSM、AIP SSC-5、および IPS SSP がリブートされます。

IDSM2 パスワードの回復

IDSM2 のパスワードを回復するには、特別なパスワード回復イメージ ファイルをインストールする必要があります。このインストールでは、パスワードだけがリセットされ、他のすべての情報は影響を受けません。パスワード回復イメージはバージョンに依存し、Cisco Download Software サイトから入手できます。IPS 6.*x* の場合は、WS-SVC-IDSM2-K9-a-6.0-password-recovery.bin.gz をダウンロードします。IPS 7.*x* の場合は、WS-SVC-IDSM2-K9-a-7.0-password-recovery.bin.gz をダウンロードします。

イメージのインストールにサポートされているプロトコルは FTP だけなので、必ずスイッチがアクセスできる FTP サーバにパスワード回復イメージを置いてください。IDSM2 でパスワードを回復するには、Cisco 6500 シリーズ スイッチへの管理者アクセス権が必要です。

パスワード回復イメージのインストール中に次のメッセージが表示されます。

```
Upgrading will wipe out the contents on the hard disk.
Do you want to proceed installing it [y|n]:
```

このメッセージはエラーです。パスワード回復イメージをインストールしても設定は削除されません。ログイン アカウントがリセットされるだけです。

パスワード回復イメージ ファイルをダウンロードしたら、システム イメージ ファイルのインストール手順を実行します。ただし、システム イメージ ファイルの代わりにパスワード回復イメージ ファイルを使用します。イメージ回復ファイルのインストール後、IDSM2 はプライマリ パーティションにリブートされます。そのようにリブートされない場合は、スイッチから次のコマンドを入力します。

```
hw-module module module_number reset hdd:1
```

（注）　パスワードが **cisco** にリセットされます。ユーザ名 **cisco** とパスワード **cisco** を使用して CLI にログインします。これで、パスワードを変更できます。

詳細情報

システム イメージ ファイルのインストール手順を使用して IDSM2 パスワード回復ファイルをインストールする手順については、「IDSM2 システム イメージのインストール」（P.25-29）を参照してください。

NME IPS パスワードの回復

NME IPS のパスワードを回復するには、**clear password** コマンドを使用します。NME IPS へのコンソール アクセスとルータへの管理者アクセス権が必要です。

NME IPS のパスワードを回復するには、次の手順を実行します。

ステップ 1　ルータにログインします。

ステップ 2　ルータで特権 EXEC モードを開始します。

```
router> enable
```

ステップ 3　ルータのモジュール スロット番号を確認します。

```
router# show run | include ids-sensor
interface IDS-Sensor1/0
router#
```

ステップ 4　NME IPS との間にセッションを確立します。

```
router# service-module ids-sensor slot/port session
```

例

```
router# service-module ids-sensor 1/0 session
```

ステップ 5　**Control-shift-6** のあとで **x** を押して、ルータ CLI に移動します。

ステップ 6　ルータ コンソールから NME IPS をリセットします。

```
router# service-module ids-sensor 1/0 reset
```

ステップ 7　**Enter** を押して、ルータ コンソールに戻ります。

ステップ 8　ブート オプションのプロンプトが表示されたら、素早く ******* を入力します。ブートローダが起動されます。

ステップ 9　パスワードをクリアします。

```
ServicesEngine boot-loader# clear password
```

NME IPS がリブートされます。パスワードが **cisco** にリセットされます。ユーザ名 **cisco** とパスワード **cisco** を使用して CLI にログインします。これで、パスワードを変更できます。

パスワード回復のディセーブル化

注意　パスワード回復がディセーブルになっているセンサーでパスワードを回復しようとすると、エラーや警告が表示されずにプロセスは進みますが、パスワードはリセットされません。パスワードを忘れたためにセンサーにログインできないときに、パスワード回復がディセーブルに設定されている場合は、センサーのイメージを再作成する必要があります。

パスワードの回復は、デフォルトでイネーブルです。パスワード回復は、CLI または MIE からディセーブルにすることができます。

CLI でパスワード回復をディセーブルにするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　グローバル コンフィギュレーション モードを開始します。

```
sensor# configure terminal
```

ステップ 3　ホスト モードを開始します。

```
sensor(config)# service host
```

ステップ 4　パスワード回復をディセーブルにします。

```
sensor(config-hos)# password-recovery disallowed
```

IME でパスワード回復をディセーブルにするには、次の手順を実行します。

ステップ 1　管理者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* > [Sensor Setup] > [Network] を選択します。

ステップ 3　パスワード回復をディセーブルにするには、[Allow Password Recovery] チェックボックスをオフにします。

パスワード回復の状態の確認

パスワード回復がイネーブルになっているかどうかを確認するには、**show settings | include password** コマンドを使用します。

パスワード回復がイネーブルになっているかどうかを確認するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　サービス ホスト サブモードを開始します。

```
sensor# configure terminal
sensor (config)# service host
sensor (config-hos)#
```

ステップ 3　**include** キーワードを使用して、フィルタ処理された出力で設定を表示し、パスワード回復の状態を確認します。

```
sensor(config-hos)# show settings | include password
   password-recovery: allowed <defaulted>
sensor(config-hos)#
```

パスワード回復のトラブルシューティング

パスワード回復のトラブルシューティングを行う場合は、次の点に注意してください。

- ROMMON プロンプト、GRUB メニュー、スイッチの CLI、ルータの CLI からは、パスワード回復がセンサーの設定でディセーブルになっているかどうかを確認できません。パスワード回復を試みると、常に成功したように見えます。ディセーブルになっている場合、パスワードは **cisco** にリセットされません。唯一のオプションはセンサーのイメージの再作成です。
- パスワード回復は、ホストの設定でディセーブルにすることができます。AIM IPS や NME IPS ブートローダ、ROMMON、IDSM2 のメンテナンス パーティションなどの外部メカニズムを使用しているプラットフォームの場合、パスワードをクリアするコマンドを実行できますが、IPS でパスワード回復がディセーブルになっている場合、IPS はパスワード回復が許可されていないことを検出し、外部要求を拒否します。

  パスワード回復の状態をチェックするには、**show settings | include password** コマンドを使用します。
- IDSM2 でパスワード回復を実行すると、「`Upgrading will wipe out the contents on the storage media.`」というメッセージが表示されます。このメッセージは無視できます。指定されたパスワード回復イメージを使用すると、パスワードだけがリセットされます。

時刻とセンサー

ここでは、センサー上で正確な時刻を維持する方法について説明します。内容は次のとおりです。

時刻源とセンサー

センサーには、信頼できる時刻源が必要です。すべてのイベント（アラート）に、正しい UTC と現地時間のタイムスタンプが必要です。タイムスタンプがないと、攻撃の後でログを正しく分析できません。センサーを初期化するときに、時間帯とサマータイム設定をセットアップします。ここでは、センサーに時刻を設定するためのさまざまな方法を概説します。

（注）　NTP サーバを使用することを推奨します。認証された NTP または認証されていない NTP を使用できます。認証された NTP には、NTP サーバの IP アドレス、キー ID、およびキー値が必要です。NTP は初期化中にセットアップできます。また、CLI、IDM、IME、または ASDM を介して NTP を設定することもできます。

アプライアンス

- **clock set** コマンドを使用して、時刻を設定する。これがデフォルトです。
- アプライアンスは、NTP 同期時刻源から時刻を取得するように設定できます。

IDSM2

- IDSM2 は、自動的にそのクロックをスイッチ時刻と同期させることができます。これがデフォルトです。UTC 時刻は、親ルータと IDSM2 の間で同期が取られます。時間帯とサマータイム設定は、スイッチと IDSM2 の間で同期が取られません。

  （注）　スイッチと IDSM2 の両方で時間帯とサマータイム設定が行われていることを確認し、UTC 時刻設定が正しいことを確認します。時間帯またはサマータイム設定、あるいはその両方が IDSM2 とスイッチの間で一致していない場合、IDSM2 のローカル時刻が不正確になることがあります。

- IDSM2 は、時刻を NTP 同期時刻源から取得するように設定できます。

AIM IPS と NME IPS

- AIM IPS と NME IPS は、インストール先のルータ シャーシ（親ルータ）のクロックと自動的にクロックを同期させることができます。これがデフォルトです。UTC 時刻は、親ルータと AIM IPS および NME IPS の間で同期が取られます。時間帯とサマータイム設定は、親ルータと AIM IPS および NME IPS の間で同期が取られません。

（注）　親ルータと AIM IPS および NME IPS の両方で時間帯とサマータイムを設定し、UTC 時刻設定が正しいことを確認してください。AIM IPS および NME IPS とルータ間で時間帯またはサマータイムの設定、あるいはその両方の設定が一致していない場合、AIM IPS と NME IPS のローカル時刻が不正確になることがあります。

- AIM IPS と NME IPS は、時刻を親ルータ以外の Cisco ルータなどの NTP 同期時刻源から取得するように設定できます。

ASA モジュール

- ASA モジュール（AIP SSM、AIP SSC-5、および IPS SSP）は、インストール先の適応型セキュリティ アプライアンスのクロックと自動的にクロックを同期させます。これがデフォルトです。
- ASA モジュールは、時刻を NTP 同期時刻源（親ルータ以外の Cisco ルータなど）から取得するように設定できます。

詳細情報

NTP の設定手順については、「NTP の設定」（P.6-14）を参照してください。

IPS モジュールのクロックと親デバイスのクロックの同期

すべての IPS モジュール（AIM IPS、AIP SSM、AIP SSC-5、IDSM2、IPS SSP、および NME IPS）は、モジュールがブートアップするたび、および親シャーシのクロックが設定されるたびに、親シャーシのクロック（スイッチ、ルータまたはセキュリティ アプライアンス）にシステム クロックを同期させます。モジュールのクロックと親シャーシのクロックは、時間の経過とともにずれが生じる傾向があります。誤差は、1 日で数秒になることがあります。この問題を回避するには、モジュールのクロックと親のクロックが両方とも外部 NTP サーバと同期していることを確認してください。モジュールまたは親シャーシのどちらかのクロックだけが NTP サーバと同期している場合、時間のずれが生じます。

センサーと NTP サーバの同期の確認

IPS では、無効な NTP キー値や ID などの誤った NTP 設定をセンサーに適用できません。誤った設定を適用しようとすると、エラー メッセージが表示されます。NTP 設定を確認するには、**show statistics host** コマンドを使用してセンサーの統計情報を収集します。NTP 統計情報セクションには、NTP サーバとセンサーの同期に関するフィードバックを含む NTP 統計情報が表示されます。

NTP 設定を確認するには、次の手順を実行します。

ステップ 1　センサーにログインします。

ステップ 2　ホストの統計情報を生成します。

```
sensor# show statistics host
     ...
     NTP Statistics
             remote           refid      st t when poll reach   delay   offset  jitter
         11.22.33.44     CHU_AUDIO(1)     8 u   36   64    1    0.536    0.069   0.001
         LOCAL(0)        73.78.73.84      5 l   35   64    1    0.000    0.000   0.001
        ind assID status  conf reach auth condition  last_event cnt
          1 10372  f014   yes   yes   ok     reject    reachable  1
          2 10373  9014   yes   yes  none    reject    reachable  1
        status = Not Synchronized
     ...
```

ステップ 3　数分後にもう一度、ホストの統計情報を収集します。

```
sensor# show statistics host
   ...
   NTP Statistics
           remote           refid      st t when poll reach   delay   offset  jitter
      *11.22.33.44     CHU_AUDIO(1)     8 u   22   64  377    0.518   37.975  33.465
       LOCAL(0)        73.78.73.84      5 l   22   64  377    0.000    0.000   0.001
      ind assID status  conf reach auth condition  last_event cnt
        1 10372  f624   yes   yes   ok   sys.peer   reachable  2
        2 10373  9024   yes   yes  none    reject   reachable  2
      status = Synchronized
```

ステップ 4　ステータスが [Not Synchronized] のままの場合は、NTP サーバが正しく設定されていることを NTP サーバの管理者に確認してください。

センサーの時刻の修正

イベントには発生時の時刻がスタンプされるため、時刻を誤って設定した場合、保存されたイベントの時刻は不正確になります。イベント ストアのタイムスタンプは、常に UTC 時刻に基づいています。元のセンサーのセットアップ中に、時刻を 8:00 a.m. ではなく 8:00 p.m. に設定した場合、エラーを訂正すると、訂正された時刻がさかのぼって設定されます。そのため、新しいイベントに古いイベントの時刻よりも過去の時刻が記録される場合があります。

たとえば、初期セットアップ中にセンサーを中部時間に設定し、さらにサマータイムを有効にした場合、現地時間が 8:04 p.m. であれば、時刻は 20:04:37 CDT として表示され、UTC からのオフセットは -5 時間になります（翌日の 01:04:37 UTC）。1 週間後の 9:00 a.m. に、21:00:23 CDT と表示された時計を見て誤りに気づいたとします。それから時刻を 9:00 a.m. に変更します。時計は現在 09:01:33 CDT と表示されています。UTC からのオフセットは変更されていないため、UTC 時刻は 14:01:33 UTC になります。ここにタイムスタンプの問題が生じる原因があります。

イベント レコードのタイムスタンプの整合性を維持するには、**clear events** コマンドを使用して、古いイベントのイベント アーカイブを消去する必要があります。

（注）　イベントは、個別には削除できません。

詳細情報

イベントを消去する手順については、「イベントのクリア」（P.C-96）を参照してください。

仮想化の利点および制約事項

センサーで設定の問題が発生しないように、センサーで仮想化を行う利点と制約事項を理解してください。

（注）　AIM IPS、AIP SSC-5、および NME IPS では仮想化がサポートされていません。

仮想化には次の利点があります。

- 個々のトラフィック セットにそれぞれ異なる設定を適用できます。
- IP スペースが重複している 2 つのネットワークを 1 つのセンサーでモニタできます。

- ファイアウォールまたは NAT デバイスの内側と外側の両方をモニタできます。

仮想化には次の制約事項があります。

- 非対称トラフィックの両側を同じ仮想センサーに割り当てる必要があります。
- VACL キャプチャまたは SPAN（無差別モニタリング）の使用は、VLAN タギングに関して矛盾しており、これによって VLAN グループの問題が発生します。
  - Cisco IOS ソフトウェアを使用している場合、VACL キャプチャ ポートまたは SPAN ターゲットは、トランキング用に設定されていても、常にタグ付きパケットを受信するわけではありません。
  - MSFC を使用している場合、学習したルートの高速パス スイッチングによって、VACL キャプチャおよび SPAN の動作が変わります。
- 固定ストアが制限されます。

仮想化には次のトラフィック キャプチャ要件があります。

- 仮想センサーで 802.1q ヘッダーを含むトラフィックを受信する必要があります（キャプチャ ポートのネイティブ VLAN 上のトラフィック以外）。
- センサーで、指定したセンサーの同じ仮想センサーに含まれる同じ VLAN グループの両方向のトラフィックをモニタする必要があります。

次のセンサーは仮想化をサポートしています。

- IDSM2（インライン インターフェイス ペアの VLAN グループを除く）
- IPS 4240
- IPS 4255
- IPS 4260
- IPS 4270-20
- AIP SSM
- IPS SSP

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

サポート対象 MIB

SNMP の設定の問題が発生しないように、センサーでサポートされている MIB を確認してください。

センサーでは次の専用 MIB がサポートされています。

- CISCO-CIDS-MIB
- CISCO-PROCESS-MIB
- CISCO-ENHANCED-MEMPOOL-MIB
- CISCO-ENTITY-ALARM-MIB

（注） MIB II はセンサーで使用できますが、サポート対象外です。一部の要素が正しくないことが認識されています（検知インターフェイスでの IF MIB からのパケット カウントなど）。MIB II の要素を使用することはできますが、これらすべてが正確な情報を提供することは保証できません。他に掲載されている MIB は完全にサポートされ、出力も正確です。

これらのシスコの専用 MIB は、次の URL から SNMP v2 の見出しの下で取得できます。

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

異常検出をディセーブルにする場合

センサーをトラフィックの一方向だけを参照するように設定している場合は、異常検出をディセーブルにする必要があります。そうしなければ、異常検出が非対称トラフィックをワーム スキャナと同じような不完全な接続と認識し、アラートを起動するため、大量のアラートが生成されます。

異常検出をディセーブルにするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　分析エンジン サブモードを開始します。

```
sensor# configure terminal
sensor(config)# service analysis-engine
sensor(config-ana)#
```

ステップ 3　ディセーブルにする異常検出ポリシーが含まれる仮想センサー名を入力します。

```
sensor(config-ana)# virtual-sensor vs0
sensor(config-ana-vir)#
```

ステップ 4　異常検出動作モードをディセーブルにします。

```
sensor(config-ana-vir)# anomaly-detection
sensor(config-ana-vir-ano)# operational-mode inactive
sensor(config-ana-vir-ano)#
```

ステップ 5　分析エンジン サブモードを終了します。

```
sensor(config-ana-vir-ano)# exit
sensor(config-ana-vir)# exit
sensor(config-ana-)# exit
Apply Changes:?[yes]:
```

ステップ 6　変更を適用する場合は Enter を押します。変更を破棄する場合は「no」と入力します。

詳細情報

ワームの詳細については、「ワーム」（P.12-3）を参照してください。

分析エンジンが応答しない場合

エラー メッセージ　Output from show statistics analysis-engine
Error: getAnalysisEngineStatistics : ct-sensorApp.424 not responding, please check system processes - The connect to the specified Io::ClientPipe failed.

エラー メッセージ　Output from show statistics anomaly-detection
Error: getAnomalyDetectionStatistics : ct-sensorApp.424 not responding, please check system processes - The connect to the specified Io::ClientPipe failed.

エラー メッセージ　Output from show statistics denied-attackers
Error: getDeniedAttackersStatistics : ct-sensorApp.424 not responding, please check system processes - The connect to the specified Io::ClientPipe failed.

考えられる原因　これらのエラー メッセージは、**show tech support** コマンドの実行時に、分析エンジンが動作していない場合に表示されます。

推奨処置　分析エンジンが動作していることを確認し、問題が解決されるかどうかをモニタしてください。

分析エンジンが動作していることを確認し、問題をモニタするには、次の手順を実行します。

ステップ 1　センサーにログインします。

ステップ 2　分析エンジンが動作していないことを確認します。

```
sensor# show version

-----
MainApp N-2007_JUN_19_16_45 (Release) 2007-06-19T17:10:20-0500 Running
AnalysisEngine N-2007_JUN_19_16_45 (Release) 2007-06-19T17:10:20-0500 Not Running
CLI N-2007_JUN_19_16_45 (Release) 2007-06-19T17:10:20-0500
```

分析エンジンが `Not Running` となっているかどうかをチェックします。

ステップ 3　**show tech-support** と入力し、出力を保存します。

ステップ 4　センサーをリブートします。

ステップ 5　センサーが安定化したら、**show version** と入力して、問題が解決されたかどうかを確認します。

ステップ 6　分析エンジンがまだ `Not Running` となっている場合は、**show tech support** コマンドの出力を用意して、TAC にお問い合わせください。

グローバル相関のトラブルシューティング

グローバル相関を設定するときに、次の点に注意してください。

- グローバル相関更新は、センサー管理インターフェイスを介して発生するため、ファイアウォールで、ポート 443 および 80 のトラフィックが許可されている必要があります。

- グローバル相関機能を動作させるには、HTTP プロキシ サーバまたは DNS サーバを設定する必要があります。
- グローバル相関機能を動作させるには、有効な IPS ライセンスが必要です。
- グローバル相関機能には、外部 IP アドレスだけが含まれているため、社内ラボにセンサーを配置した場合は、グローバル相関情報を受信できません。
- 使用しているセンサーが、グローバル相関機能をサポートしていることを確認します。

（注）　AIP SSC-5 は、グローバル相関機能をサポートしていません。

- 使用している IPS バージョンが、グローバル相関機能をサポートしていることを確認します。

（注）　IPS 6.1 および 6.2 は、グローバル相関機能をサポートしていません。

詳細情報

グローバル相関機能と、それらの設定方法の詳細については、第 13 章「グローバル相関の設定」を参照してください。

外部製品インターフェイスのトラブルシューティング

ここでは、外部製品インターフェイスで発生する可能性のある問題とトラブルシューティングのヒントを紹介します。内容は次のとおりです。

外部製品インターフェイスの問題

外部製品インターフェイスがホスト ポスチャと隔離イベントを受信すると、次の問題が発生することがあります。

- センサーは、特定の数のホスト レコードしか格納できません。
  - レコード数が 10,000 を超えると、その後のレコードはドロップされます。
  - 10,000 の上限に達すると、9900 を下回るまでドロップされ、新しいレコードがドロップされなくなります。
- ホストは IP アドレスを変更できるか、別のホスト IP アドレスを使用しているように見えます。これは、DHCP のリース有効期限切れやワイヤレス ネットワークでの移動によって発生します。

  IP アドレスが競合する場合、センサーは最新のホスト ポスチャ イベントを最も正確であると見なします。
- ネットワークには、異なる VLAN のオーバーラップする IP アドレス範囲が含まれていることがありますが、ホスト ポスチャには VLAN ID 情報は含まれません。特定のアドレス範囲を無視するようにセンサーを設定できます。
- CSA MC はファイアウォールの内側にあるため、ホストに到達不能となることがあります。到達不能のホストは除外できます。

- CSA MC イベント サーバでは、デフォルトで開いたサブスクリプションを最大 10 まで使用できます。この値を変更できます。サブスクリプションを開くには、管理者アカウントとパスワードが必要です。
- CSA データは仮想化されません。センサーによってグローバルに処理されます。
- ホスト ポスチャ OS と IP アドレスは、パッシブ OS フィンガープリント ストレージに統合されます。これらは、インポートされた OS プロファイルとして表示できます。
- 隔離されたホストは表示できません。
- センサーは、各 CSA MC ホスト X.509 証明書を認識する必要があります。これらを信頼できるホストとして追加する必要があります。
- 最大 2 つの外部製品デバイスを設定できます。

詳細情報

- 外部製品インターフェイスの詳細については、第 17 章「外部製品インターフェイスの設定」を参照してください。
- OS マップおよび識別の操作の詳細については、「設定された OS マップの追加、編集、削除、および移動」（P.11-29）と「OS ID の設定」（P.19-26）を参照してください。
- 信頼できるホストの追加手順については、「信頼できるホストの追加」（P.14-10）を参照してください。

外部製品インターフェイスのトラブルシューティングのヒント

外部製品のインターフェイスのトラブルシューティングを行う場合は、次のことをチェックしてください。

- CLI で **show statistics external-product-interface** コマンドからの出力をチェックするか、IME で [Configuration] > *sensor_name* > [Sensor Monitoring] > [Support Information] > [Statistics] を選択して、応答の [Interface] の状態行をチェックして、インターフェイスがアクティブであることを確認します。
- 信頼できるホストに CSA MC IP アドレスを追加したことを確認します。追加するのを忘れた場合は、追加し、数分待ってから、もう一度チェックします。
- ブラウザを使用して CSA MC でサブスクリプションを開いてから閉じて、サブスクリプション ログイン情報を確認します。
- イベント ストアで CSA MC のサブスクリプション エラーをチェックします。

詳細情報

- 信頼できるホストの追加手順については、「信頼できるホストの追加」（P.14-10）を参照してください。
- イベントを表示する手順については、「イベントの表示」（P.C-93）を参照してください。

4200 シリーズ アプライアンスのトラブルシューティング

ここでは、4200 シリーズのアプライアンスのトラブルシューティングについて説明します。内容は次のとおりです。

- 「ターミナル サーバへの接続」（P.C-23）
- 「接続のゆるみのトラブルシューティング」（P.C-24）

ターミナル サーバへの接続

ターミナル サーバは複数の低速非同期ポートを持つルータです。この複数のポートは、他のシリアル デバイスに接続されています。ターミナル サーバを使用して、アプライアンスを含むネットワーク機器をリモートで管理することができます。

RJ-45 接続またはヒドラ ケーブル アセンブリ接続を使用して Cisco ターミナル サーバをセットアップするには、次の手順を実行します。

ステップ 1　次のいずれかの方法で、ターミナル サーバに接続します。

- RJ-45 接続を行うターミナル サーバの場合、180 ロールオーバー ケーブルをアプライアンスのコンソール ポートからターミナル サーバのポートに接続します。
- ヒドラ ケーブル アセンブリの場合、ストレート パッチ ケーブルをアプライアンスのコンソール ポートからターミナル サーバのポートに接続します。

ステップ 2　ターミナル サーバで、ラインとポートを設定します。イネーブル モードで次の設定を入力します。ここで、# は設定するポートの回線番号です。

```
config t
line #
login
transport input all
stopbits 1
flowcontrol hardware
speed 9600
exit
exit
wr mem
```

ステップ 3　アプライアンスへの不正アクセスを防ぐため、ターミナル セッションは確実に正しく終了してください。ターミナル セッションが正しく終了されていない場合、つまり、セッションを開始したアプリケーションから exit(0) 信号が受信されていない場合、ターミナル セッションは開いたままです。ターミナル セッションが正しく終了していない場合、そのシリアル ポート上で開かれる次のセッションでは、認証が実行されません。

注意　接続を確立するために使用したアプリケーションを終了する前に、必ずセッションを終了してログイン プロンプトに戻ってください。

注意　誤って接続が切断されたり終了した場合は、接続を再確立し、正しく終了して、アプライアンスに対する不正なアクセスを防ぎます。

接続のゆるみのトラブルシューティング

センサーまたは適応型セキュリティ アプライアンスの接続のゆるみの問題を解決するには、次の手順を実行します。

- すべての電源コードがしっかりと接続されていることを確認します。
- すべてのケーブルが適切に配線され、すべての外部および内部コンポーネントにしっかりと接続されていることを確認します。
- すべてのデータ コードと電源コードを取り外し、損傷がないかどうかをチェックします。ケーブルのピンが折れ曲がったり、コネクタが損傷したりしていないかを確認します。
- 各デバイスが正しく設置されていることを確認します。
- デバイスにラッチがある場合は、完全に閉じ、ロックされていることを確認します。
- インターロックまたは相互接続インジケータが、コンポーネントが適切に接続されていないことを示していないかどうかをチェックします。
- 問題が解決されない場合は、各デバイスを取り外し、コネクタやソケットのピンの曲がりやその他の損傷がないかどうかをチェックしながら、もう一度取り付けてください。

分析エンジンがビジー状態

センサーのイメージを再作成すると、分析エンジンは正規表現テーブルの再構築でビジー状態となり、新しい設定に応答しません。**show statistics virtual-sensor** コマンドを使用して、分析エンジンがビジー状態かどうかをチェックできます。分析エンジンがビジー状態の場合、次のエラー メッセージが表示されます。

```
sensor# show statistics virtual-sensor
Error: getVirtualSensorStatistics : Analysis Engine is busy rebuilding regex tables. This
may take a while.
sensor#
```

分析エンジンが正規表現テーブルの再構築でビジー状態ときに、シグニチャのイネーブル化や非アクティブ化などの設定の更新を行おうとすると、エラーメッセージが表示されます。

```
sensor# configure terminal
sensor(config)# service sig sig0
sensor(config-sig)# sig 2000 0
sensor(config-sig-sig)# status enabled
sensor(config-sig-sig)# status
sensor(config-sig-sig-sta)# enabled true
sensor(config-sig-sig-sta)# retired false
sensor(config-sig-sig-sta)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes?[yes]:
Error: editConfigDeltaSignatureDefinition : Analysis Engine is busy rebuilding regex
tables. This may take a while.
The configuration changes failed validation, no changes were applied.
```

```
Would you like to return to edit mode to correct the errors? [yes]: no
No changes were made to the configuration.
sensor(config)#
```

センサーのブート直後に仮想センサーの統計情報を取得しようとすると、エラー メッセージが表示されます。キャッシュ ファイルは再構築されていますが、仮想センサーの初期化は完了していません。

```
sensor# show statistics virtual-sensor
Error: getVirtualSensorStatistics : Analysis Engine is busy.
sensor#
```

分析エンジンがビジー状態であるというエラーを受け取った場合は、しばらく時間をおいてから設定の変更を行ってください。**show statistics virtual-sensor** コマンドを使用して、いつ分析エンジンがもう一度使用可能になるかを確認してください。

Cisco 7200 シリーズ ルータへの IPS 4240 の接続

IPS 4240 が直接 7200 シリーズのルータに接続され、IPS 4240 とルータの両方のインターフェイスで、デュプレックスが全二重、速度が 100 にハードコード化されている場合、接続は機能しません。速度とデュプレックスを自動にして IPS 4240 を設定した場合、ルータに接続しますが、速度は 100、デュプレックスは半二重です。

速度が 100、デュプレックスが全二重の状態で正しく接続するには、IPS 4240 とルータの両方のインターフェイスで、速度とデュプレックスを自動に設定します。また、どちらかのインターフェイスがハードコード化されている場合は、クロス ケーブルを使用して接続する必要があります。

通信の問題

ここでは、4200 シリーズ センサーの通信に関する問題のトラブルシューティングに役立つ情報を説明します。内容は次のとおりです。

- 「Telnet または SSH からセンサーの CLI にアクセスできない」（P.C-25）
- 「設定が誤っているアクセス リストの修正」（P.C-28）
- 「IP アドレスの重複が原因でインターフェイスがシャットダウンする」（P.C-28）

Telnet または SSH からセンサーの CLI にアクセスできない

Telnet（すでにイネーブルにしてある場合）または SSH を使用してセンサーの CLI にアクセスできない場合は、次の手順を実行します。

ステップ 1　コンソール、ターミナルまたはモジュール セッションからセンサーの CLI にログインします。

ステップ 2　センサー管理インターフェイスがイネーブルになっていることを確認します。

```
sensor# show interfaces
Interface Statistics
   Total Packets Received = 0
   Total Bytes Received = 0
   Missed Packet Percentage = 0
   Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
```

```
   Link Status = Up
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface GigabitEthernet0/0
   Media Type = TX
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 944333
   Total Bytes Received = 83118358
   Total Multicast Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 397633
   Total Bytes Transmitted = 435730956
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
sensor#
```

管理インターフェイスは、リストのステータス行が `Media Type = TX` となっているインターフェイスです。[Link Status] が `Down` の場合は、ステップ 3 に進みます。[Link Status] が `Up` の場合は、ステップ 5 に進みます。

ステップ 3　センサー IP アドレスが一意であることを確認します。

```
sensor# setup
--- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Current Configuration:


service host
network-settings
host-ip 10.89.130.108/23,10.89.130.1
host-name sensor
telnet-option enabled
access-list 0.0.0.0/0
ftp-timeout 300
no login-banner-text
exit
--MORE--
```

管理インターフェイスによって、ネットワーク上の別のデバイスに同じ IP アドレスが指定されていることが検出されると、インターフェイスは表示されません。

ステップ 4　管理ポートがアクティブなネットワーク接続に接続されていることを確認します。管理ポートがアクティブなネットワーク接続に接続されていない場合、管理インターフェイスは表示されません。

ステップ 5　センサーに接続を試みているワークステーションの IP アドレスが、センサーのアクセス リストで許可されていることを確認します。

```
sensor# setup
--- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Current Configuration:


service host
network-settings
host-ip 10.89.130.108/23,10.89.130.1
host-name sensor
telnet-option enabled
access-list 0.0.0.0/0
ftp-timeout 300
no login-banner-text
exit
--MORE--
```

ワークステーションのネットワーク アドレスがセンサーのアクセス リストで許可されている場合は、ステップ 6 に進みます。

ステップ 6　ワークステーションのネットワーク アドレスに許可エントリを追加し、設定を保存して、再度接続を試みます。

ステップ 7　ネットワーク設定で、ワークステーションがセンサーに接続できるようになっていることを確認します。

センサーがファイアウォールで保護され、ワークステーションがファイアウォールの前にある場合は、ワークステーションにセンサーへのアクセスを許可するようにファイアウォールが設定されていることを確認します。または、ワークステーションがワークステーションの IP アドレスでネットワーク アドレス変換を実行するファイアウォールの内側に置かれ、センサーがファイアウォールの前にある場合、センサーのアクセス リストにワークステーションの変換後のアドレスに対する許可エントリが含まれていることを確認します。

詳細情報

- IP アドレスの変更、アクセス リストの変更、Telnet のイネーブル化およびディセーブル化の手順については、「ネットワークの設定」（P.6-2）を参照してください。
- センサーで直接 CLI セッションを開くさまざまな方法については、第 22 章「センサーへのログイン」を参照してください。

設定が誤っているアクセス リストの修正

設定が誤っているアクセス リストを修正するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　設定を表示して、アクセス リストを確認します。

```
sensor# show configuration | include access-list
access-list 10.0.0.0/8
access-list 64.0.0.0/8
sensor#
```

ステップ 3　クライアント IP アドレスが許可されたネットワーク内にリストされているかどうか確認します。表示されていない場合は、次のように追加します。

```
sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# network-settings
sensor(config-hos-net)# access-list 171.69.70.0/24
```

ステップ 4　設定を確認できます。

```
sensor(config-hos-net)# show settings
   network-settings
   -----------------------------------------------
      host-ip: 10.89.149.238/25,10.89.149.254 default: 10.1.9.201/24,10.1.9.1
      host-name: sensor-238 default: sensor
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 3)
      -----------------------------------------------
         network-address: 10.0.0.0/8
         -----------------------------------------------
         network-address: 64.0.0.0/8
         -----------------------------------------------
         network-address: 171.69.70.0/24
         -----------------------------------------------
      -----------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text: <defaulted>
   -----------------------------------------------
sensor(config-hos-net)#
```

IP アドレスの重複が原因でインターフェイスがシャットダウンする

同じ IP アドレスを持つ 2 台のセンサーが新たにイメージ化され、同じネットワーク上で同時にアップ状態になると、インターフェイスはシャットダウンします。Linux では、他のホストとのアドレスの競合を検出した場合、コマンド/コントロール インターフェイスがアクティブになることが防止されます。

問題のセンサーが、ネットワーク上の別のホストと競合する IP アドレスを持っていないことを確認するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　インターフェイスがアップ状態かどうかを判断します。

```
sensor# show interfaces
Interface Statistics
```

```
   Total Packets Received = 0
   Total Bytes Received = 0
   Missed Packet Percentage = 0
   Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface GigabitEthernet0/0
   Media Type = TX
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 1822323
   Total Bytes Received = 131098876
   Total Multicast Packets Received = 20
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 219260
   Total Bytes Transmitted = 103668610
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
sensor#
```

出力で、コマンド/コントロール インターフェイス リンクがダウンしていることが示されている場合、ハードウェアに問題があるか IP アドレスが競合しています。

ステップ 3　センサーのケーブル接続が正しいことを確認します。

ステップ 4　IP アドレスが正しいことを確認します。

詳細情報

- センサーのケーブル接続が正しいことを確認するには、『*Installing Cisco Intrusion Prevention System Appliances and Module 7.0*』または『*Installing the Cisco Intrusion Prevention System Security Services Processor 7.1*』で、使用しているセンサーの章を参照してください。
- IP アドレスが正しいことを確認する手順については、「ネットワークの設定」（P.6-2）を参照してください。

SensorApp とアラート

ここでは、SensorApp とアラートに関する問題のトラブルシューティングに役立つ情報を提供します。内容は次のとおりです。

SensorApp が実行されていない

センシング プロセス（SensorApp）は、常に動作している必要があります。常に動作していないと、アラートを受信できません。SensorApp は分析エンジンの一部なので、分析エンジンが動作していることを確認する必要があります。

分析エンジンが動作していることを確認するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　分析エンジン サービスのステータスを特定します。

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.1(1)E4

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S518.0              2010-10-04
OS Version:             2.6.29.1
Platform:               ASA5585-SSP-IPS20
Serial Number:          JAF1350ABSF
Licensed, expires:      04-Oct-2011 UTC
Sensor up-time is 4:32.
Using 10378M out of 11899M bytes of available memory (87% usage)
system is using 25.1M out of 160.0M bytes of available disk space (16% usage)
application-data is using 65.4M out of 171.4M bytes of available disk space (40%
 usage)
boot is using 56.1M out of 71.7M bytes of available disk space (83% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96%
 usage)


MainApp            S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500   Running
AnalysisEngine     S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500   NotRunning
CollaborationApp   S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500   Running
CLI                S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500

Upgrade History:

  IPS-K9-7.1-1-E4   00:42:07 UTC Thu Oct 21 2010
```

```
Recovery Partition Version 1.1 - 7.1(1)E4

Host Certificate Valid from: 21-Oct-2010 to 21-Oct-2012

sensor#
```

ステップ 3　分析エンジンが動作していない場合は、それに関係するエラーが発生していないか調べます。

```
sensor# show events error fatal past 13:00:00 | include AnalysisEngine
evError: eventId=1077219258696330005 severity=warning

originator:
hostId: sensor
appName: sensorApp
appInstanceId: 1045
time: 2004/02/19 19:34:20 2004/02/19 19:34:20 UTC
errorMessage: name=errUnclassified Generating new Analysis Engine configuration file.
```

（注）　最後の再起動の日時が表示されます。この例では、最後の再起動は 2004 年 2 月 19 日の 7 時 34 分でした。

ステップ 4　ソフトウェアの更新が最新のものであることを確認します。

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.1(1)E4

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S518.0              2010-10-04
OS Version:             2.6.29.1
Platform:               ASA5585-SSP-IPS20
Serial Number:          JAF1350ABSF
Licensed, expires:      04-Oct-2011 UTC
Sensor up-time is 4:32.
Using 10378M out of 11899M bytes of available memory (87% usage)
system is using 25.1M out of 160.0M bytes of available disk space (16% usage)
application-data is using 65.4M out of 171.4M bytes of available disk space (40%
 usage)
boot is using 56.1M out of 71.7M bytes of available disk space (83% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96%
 usage)


MainApp            S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500   Running
AnalysisEngine     S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500   NotRunning
CollaborationApp   S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500   Running
CLI                S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500

Upgrade History:

  IPS-K9-7.1-1-E4   00:42:07 UTC Thu Oct 21 2010

Recovery Partition Version 1.1 - 7.1(1)E4
```

```
Host Certificate Valid from: 21-Oct-2010 to 21-Oct-2012

sensor#
```

ステップ 5　最新のものではない場合は、Cisco.com からダウンロードします。

詳細情報

- IPS システム アーキテクチャの詳細については、付録 A「システム アーキテクチャの概要」を参照してください。
- 最新の Cisco IPS ソフトウェアの入手手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。

物理的な接続性、SPAN、または VACL ポートの問題

センサーが正しく接続されていないと、アラートを受信しません。

センサーが正しく接続されていることを確認するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　インターフェイスがアップ状態にあり、パケット カウントが増加していることを確認します。

```
sensor# show interfaces
Interface Statistics
   Total Packets Received = 0
   Total Bytes Received = 0
   Missed Packet Percentage = 0
   Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface GigabitEthernet0/0
   Media Type = TX
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 1830137
```

```
   Total Bytes Received = 131624465
   Total Multicast Packets Received = 20
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 220052
   Total Bytes Transmitted = 103796666
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
sensor#
```

ステップ 3　インターフェイスがダウンしている場合は、センシング ポートが適切に接続されているか確認します。

a. アプライアンス上でセンシング ポートが適切に接続されていることを確認します。

b. センシング ポートが IDSM2 上の正しい SPAN または VACL キャプチャ ポートに接続されていることを確認します。

ステップ 4　インターフェイスの設定を確認します。

a. インターフェイスが正しく設定されていることを確認します。

b. Cisco スイッチ上で SPAN および VACL キャプチャ ポート設定を確認します。手順については、スイッチのマニュアルを参照してください。

ステップ 5　インターフェイスがアップ状態であり、パケット カウントが増加していることを再び確認します。

```
sensor# show interfaces
```

詳細情報

- センサーに検知インターフェイスを正しくインストールする手順については、『*Installing Cisco Intrusion Prevention System Appliances and Module 7.0*』または『*Installing the Cisco Intrusion Prevention System Security Services Processor 7.1*』の該当するアプライアンスの章を参照してください。
- IDSM2 で SPAN または VACL キャプチャ ポートを接続する手順については、『Configuring the IDSM2』を参照してください。
- センサーでのインターフェイスの設定手順については、第 7 章「インターフェイスの設定」を参照してください。

アラートを表示できない

アラートが表示されない場合は、次のことを確認します。

- シグニチャがイネーブルになっている
- シグニチャが非アクティブになっていない
- [Produce Alert] がアクションとして設定されている

（注） [Produce Alert] の選択後、設定に戻り、別のイベント アクションを追加し、[Produce Alert] を新しい設定に追加しなかった場合、アラートはイベント ストアに送信されません。シグニチャを設定するたびに、新しい設定によって古い設定は上書きされます。シグニチャごとに必要なすべてのイベント アクションを設定したことを確認してください。

- センサーがパケットを監視している

- アラートが生成されている
- 検知インターフェイスが仮想センサーに存在する

アラートが表示されることを確認するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　シグニチャが有効であることを確認します。

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 1300 0
sensor(config-sig-sig)# status
sensor(config-sig-sig-sta)# show settings
   status
   -----------------------------------------------
      enabled: true <defaulted>
      retired: false <defaulted>
   -----------------------------------------------
sensor(config-sig-sig-sta)#
```

ステップ 3　[Produce Alert] を設定したことを確認します。

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 1300 0
sensor(config-sig-sig)# engine ?
normalizer     Signature engine
sensor(config-sig-sig)# engine normalizer
sensor(config-sig-sig-nor)# event-action produce-alert
sensor(config-sig-sig-nor)# show settings
   normalizer
   -----------------------------------------------
      event-action: produce-alert default: produce-alert|deny-connection-inline
      edit-default-sigs-only
      -----------------------------------------------
sensor#
```

ステップ 4　センサーがパケットを監視していることを確認します。

```
sensor# show interfaces FastEthernet0/1
MAC statistics from interface FastEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 267581
   Total Bytes Received = 24886471
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 57301
   Total Bytes Transmitted = 3441000
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
```

```
   Total Transmit Errors = 1
   Total Transmit FIFO Overruns = 0
sensor#
```

ステップ 5　アラートが表示されるかどうかを確認します。

```
sensor# show statistics virtual-sensor
SigEvent Preliminary Stage Statistics
    Number of Alerts received = 0
    Number of Alerts Consumed by AlertInterval = 0
    Number of Alerts Consumed by Event Count = 0
    Number of FireOnce First Alerts = 0
    Number of FireOnce Intermediate Alerts = 0
    Number of Summary First Alerts  = 0
    Number of Summary Intermediate Alerts  = 0
    Number of Regular Summary Final Alerts  = 0
    Number of Global Summary Final Alerts  = 0
    Number of Alerts Output for further processing = 0alertDetails: Traffic Source: int0 ;
```

センサーがパケットを監視しない

センサーがネットワーク上のパケットを監視していない場合、インターフェイスの設定が正しくないことが考えられます。

センサーがパケットを監視していない場合は、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　インターフェイスがアップ状態であり、パケットを受信していることを確認します。

```
sensor# show interfaces GigabitEthernet0/1
MAC statistics from interface GigabitEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Down
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
sensor#
```

ステップ 3　インターフェイスがアップ状態でない場合は、次の手順を実行します。

- ケーブル配線を調べます。
- インターフェイスをイネーブルにします。

```
sensor# configure terminal
sensor(config)# service interface
sensor(config-int)# physical-interfaces GigabitEthernet0/1
sensor(config-int-phy)# admin-state enabled
sensor(config-int-phy)# show settings
   <protected entry>
   name: GigabitEthernet0/1
   -----------------------------------------------
      media-type: tx <protected>
      description: <defaulted>
      admin-state: enabled default: disabled
      duplex: auto <defaulted>
      speed: auto <defaulted>
      alt-tcp-reset-interface
      -------------------------------------------------
         none
         -------------------------------------------------
         -------------------------------------------------
      -------------------------------------------------
   -----------------------------------------------
sensor(config-int-phy)#
```

ステップ 4　インターフェイスが動作し、パケットを受信しているかどうかをチェックします。

```
sensor# show interfaces
MAC statistics from interface GigabitEthernet0/1
   Media Type = TX
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 3
   Total Bytes Received = 900
   Total Multicast Packets Received = 3
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0 ...
```

詳細情報

センサーを正しくインストールする手順については、『*Installing Cisco Intrusion Prevention System Appliances and Module 7.0*』または『*Installing the Cisco Intrusion Prevention System Security Services Processor 7.1*』の該当するセンサーの章を参照してください。

破損した SensorApp 設定のクリーンアップ

SensorApp 設定が破損状態となり SensorApp が動作しない場合は、SensorApp を完全に削除して SensorApp を再起動する必要があります。

SensorApp 設定を削除するには、次の手順を実行します。

ステップ 1　サーバ アカウントにログインします。

ステップ 2　root に su します。

ステップ 3　IPS アプリケーションを停止します。

```
/etc/init.d/cids stop
```

ステップ 4　仮想センサー ファイルを交換します。

```
cp /usr/cids/idsRoot/etc/defVirtualSensorConfig.xml
/usr/cids/idsRoot/etc/VS-Config/virtualSensor.xml
```

ステップ 5　キャッシュ ファイルを削除します。

```
rm /usr/cids/idsRoot/var/virtualSensor/*.pmz
```

ステップ 6　サービス アカウントを終了します。

ステップ 7　センサー CLI にログインします。

ステップ 8　IPS サービスを開始します。

```
sensor# cids start
```

ステップ 9　管理者権限でアカウントにログインします。

ステップ 10　センサーをリブートします。

```
sensor# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? [yes]:yes
Request Succeeded.
sensor#
```

詳細情報

IPS システム アーキテクチャの詳細については、付録 A「システム アーキテクチャの概要」を参照してください。

ブロッキング

ここでは、ブロッキングおよび ARC サービスをトラブルシューティングするうえで役立つ情報を提供します。内容は次のとおりです。

- 「ネットワーク デバイスへの SSH 接続を有効にする」（P.C-44）
- 「シグニチャに対してブロッキングが発生していない」（P.C-45）
- 「マスター ブロッキング センサーの設定を確認する」（P.C-46）

ブロッキングのトラブルシューティング

ARC の設定の終了後、**show version** マンドを使用して ARC が正しく動作しているかどうかを確認できます。ネットワーク デバイスに ARC が接続されていることを確認するには、**show statistics networkAccess** コマンドを使用します。

（注）　ARC は、以前は Network Access Controller と呼ばれていました。IPS 5.1 以降、名前は変更されていますが、IDM、IME、および CLI には、Network Access Controller、**nac**、および **network-access** として表示されます。

ARC をトラブルシュートするには、次の手順を実行します。

1. ARC が動作していることを確認します。
2. ARC がネットワーク デバイスに接続されていることを確認します。
3. 特定のシグニチャについてイベント アクションが [Block Host] に設定されていることを確認します。
4. マスター ブロッキング センサーが正しく設定されていることを確認します。

詳細情報

- ARC が動作していることを確認する手順については、「ARC が動作中であることを確認する」（P.C-38）を参照してください。
- ARC が接続されていることを確認する手順については、「ARC 接続がアクティブであることを確認する」（P.C-39）を参照してください。
- イベント アクションが [Block Host] に設定されていることを確認する手順については、「シグニチャに対してブロッキングが発生していない」（P.C-45）を参照してください。
- マスター ブロッキング センサーが適切に設定されていることを確認する手順については、「マスター ブロッキング センサーの設定を確認する」（P.C-46）を参照してください。
- ARC アークテクチャの説明については、「Attack Response Controller」（P.A-12）を参照してください。

ARC が動作中であることを確認する

ARC が動作していることを確認するには、**show version** コマンドを使用します。MainApp が動作していない場合、ARC は実行できません。ARC は MainApp の一部です。

ARC が動作していることを確認するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　MainApp が動作していることを確認します。

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.1(1)E4
```

```
Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S518.0              2010-10-04
OS Version:             2.6.29.1
Platform:               ASA5585-SSP-IPS20
Serial Number:          JAF1350ABSF
Licensed, expires:      04-Oct-2011 UTC
Sensor up-time is 4:32.
Using 10378M out of 11899M bytes of available memory (87% usage)
system is using 25.1M out of 160.0M bytes of available disk space (16% usage)
application-data is using 65.4M out of 171.4M bytes of available disk space (40%
 usage)
boot is using 56.1M out of 71.7M bytes of available disk space (83% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96%
 usage)


MainApp            S-SPYKER_2010_OCT_21_00_27_7_1_1    (Release)    2010-10-21
T00:29:47-0500    Running
AnalysisEngine     S-SPYKER_2010_OCT_21_00_27_7_1_1    (Release)    2010-10-21
T00:29:47-0500    Running
CollaborationApp   S-SPYKER_2010_OCT_21_00_27_7_1_1    (Release)    2010-10-21
T00:29:47-0500    Running
CLI                S-SPYKER_2010_OCT_21_00_27_7_1_1    (Release)    2010-10-21
T00:29:47-0500

Upgrade History:

  IPS-K9-7.1-1-E4   00:42:07 UTC Thu Oct 21 2010

Recovery Partition Version 1.1 - 7.1(1)E4

Host Certificate Valid from: 21-Oct-2010 to 21-Oct-2012

sensor
```

ステップ 3　MainApp の表示が `Not Running` である場合、ARC は故障しています。TAC にお問い合わせください。

詳細情報

IPS システム アーキテクチャの詳細については、付録 A「システム アーキテクチャの概要」を参照してください。

ARC 接続がアクティブであることを確認する

ARC 統計情報の State が `Active` ではない場合、問題があります。

統計情報の State が Active かどうか確認するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　ARC が接続状態にあることを確認します。出力の State セクションを調べて、すべてのデバイスが接続状態にあることを確認します。

```
sensor# show statistics network-access
Current Configuration
   LogAllBlockEventsAndSensors = true
   EnableNvramWrite = false
```

```
   EnableAclLogging = false
   AllowSensorBlock = false
   BlockMaxEntries = 250
   MaxDeviceInterfaces = 250
   NetDevice
      Type = Cisco
      IP = 10.89.147.54
      NATAddr = 0.0.0.0
      Communications = telnet
      BlockInterface
         InterfaceName = fa0/0
         InterfaceDirection = in
State
   BlockEnable = true
   NetDevice
      IP = 10.89.147.54
      AclSupport = uses Named ACLs
      Version = 12.2
      State = Active
sensor#
```

ステップ 3　ARC が接続状態にない場合は、繰り返し発生しているエラーを探します。

```
sensor# show events error hh:mm:ss month day year | include : nac
```

例

```
sensor# show events error 00:00:00 Apr 01 2007 | include : nac
```

ステップ 4　ソフトウェアの更新が最新のものであることを確認します。

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.1(1)E4

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S518.0              2010-10-04
OS Version:             2.6.29.1
Platform:               ASA5585-SSP-IPS20
Serial Number:          JAF1350ABSF
Licensed, expires:      04-Oct-2011 UTC
Sensor up-time is 4:32.
Using 10378M out of 11899M bytes of available memory (87% usage)
system is using 25.1M out of 160.0M bytes of available disk space (16% usage)
application-data is using 65.4M out of 171.4M bytes of available disk space (40%
 usage)
boot is using 56.1M out of 71.7M bytes of available disk space (83% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96%
 usage)


MainApp            S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500   Running
AnalysisEngine     S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500   Running
CollaborationApp   S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500   Running
CLI                S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500

Upgrade History:
```

```
  IPS-K9-7.1-1-E4   00:42:07 UTC Thu Oct 21 2010

Recovery Partition Version 1.1 - 7.1(1)E4

Host Certificate Valid from: 21-Oct-2010 to 21-Oct-2012

sensor
```

（注）　最新のものではない場合は、Cisco.com からダウンロードします。

ステップ 5　ARC の既知の DDTS については、ソフトウェア アップグレードに添付の Readme を参照してください。

ステップ 6　デバイスごとに設定（ユーザ名、パスワード、IP アドレス）が正しいことを確認します。

ステップ 7　ネットワーク デバイスごとにインターフェイスと方向が正しいことを確認します。

ステップ 8　ネットワーク デバイスで SSH-3DES が使用されている場合は、デバイスへの SSH 接続をすでに有効にしていることを確認します。

ステップ 9　制御対象の各デバイスで各インターフェイスと方向が正しいことを確認します。

詳細情報

- 最新の Cisco IPS ソフトウェアの入手手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。
- デバイスの設定の詳細については、「デバイスのアクセスに関する問題点」（P.C-41）を参照してください。
- 各ネットワーク デバイスのインターフェイスと方向を確認する手順については、「ネットワーク デバイス上のインターフェイスと方向を確認する」（P.C-43）を参照してください。
- SSH をイネーブルにする手順については、「ネットワーク デバイスへの SSH 接続を有効にする」（P.C-44）を参照してください。

デバイスのアクセスに関する問題点

ARC は、管理しているデバイスにアクセスできない場合があります。管理対象のデバイスの IP アドレス、ユーザ名、およびパスワードが正しいこと、インターフェイスと方向が正しく設定されていることを確認します。

（注）　SSH デバイスは、SSH 1.5 をサポートしている必要があります。センサーは SSH 2.0 をサポートしていません。

デバイスへのアクセスの問題についてトラブルシューティングを行うには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　管理対象デバイスの IP アドレスを確認します。

```
sensor# configure terminal
sensor (config)# service network-access
sensor(config-net)# show settings
   general
   ------------------------------------------------
```

```
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      never-block-networks (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
      block-networks (min: 0, max: 250, current: 0)
      ------------------------------------------------
      ------------------------------------------------
   ---------------------------------------------
   user-profiles (min: 0, max: 250, current: 1)
   ---------------------------------------------
      profile-name: r7200
      ------------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username: netrangr default:
      ------------------------------------------------
   ---------------------------------------------
   cat6k-devices (min: 0, max: 250, current: 0)
   ---------------------------------------------
   ---------------------------------------------
   router-devices (min: 0, max: 250, current: 1)
   ---------------------------------------------
      ip-address: 10.89.147.54
      ------------------------------------------------
         communication: telnet default: ssh-3des
         nat-address: 0.0.0.0 <defaulted>
         profile-name: r7200
         block-interfaces (min: 0, max: 100, current: 1)
         ------------------------------------------------
            interface-name: fa0/0
            direction: in
            ------------------------------------------------
               pre-acl-name: <defaulted>
               post-acl-name: <defaulted>
            ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
   ---------------------------------------------
   firewall-devices (min: 0, max: 250, current: 0)
   ---------------------------------------------
   ---------------------------------------------
sensor(config-net)#
```

ステップ 3　デバイスに手動で接続して、正しいユーザ名、正しいパスワード、および有効なパスワードを使用していること、さらにセンサーからデバイスに到達可能であることを確認します。

a.　サーバ アカウントにログインします。

b.　Telnet または SSH を使用してネットワーク デバイスに接続し、設定を確認します。

c. デバイスに到達できることを確認します。

d. ユーザ名とパスワードを確認します。

ステップ 4　各ネットワーク デバイスの各インターフェイスと方向が正しいことを確認します。

詳細情報

各ネットワーク デバイスのインターフェイスと方向を確認する手順については、「ネットワーク デバイス上のインターフェイスと方向を確認する」（P.C-43）を参照してください。

ネットワーク デバイス上のインターフェイスと方向を確認する

制御対象の各デバイス上で各インターフェイスと方向が正しいことを確認するには、手動ブロックを偽のホストに送信し、ルータの ACL 内のブロックされているアドレスについて拒否エントリが存在するかどうかを確認できます。

（注）　手動ブロックを実行するには、[Configuration] > ***sensor_name*** > [Sensor Monitoring] > [Time-Based Actions] > [Host Blocks] を選択します。

不正なホストに対する手動ブロックを開始するには、次の手順を実行します。

ステップ 1　ARC 一般サブモードを開始します。

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)# general
```

ステップ 2　偽のホストの IP アドレスの手動ブロックを開始します。

```
sensor(config-net-gen)# block-hosts 10.16.0.0
```

ステップ 3　一般サブモードを終了します。

```
sensor(config-net-gen)# exit
sensor(config-net)# exit
Apply Changes:? [yes]:
```

ステップ 4　**Enter** を押して変更内容を確定するか、**no** を入力して、これらを破棄します。

ステップ 5　ルータに Telnet 接続して、ブロックされたアドレスの拒否エントリがルータの ACL 内に存在することを確認します。手順については、ルータのマニュアルを参照してください。

ステップ 6　手動ブロックを削除するにはステップ 1 ～ 4 を繰り返します。ただし、ステップ 2 では、コマンドの前に **no** を配置します。

```
sensor(config-net-gen)# no block-hosts 10.16.0.0
```

ネットワーク デバイスへの SSH 接続を有効にする

ネットワーク デバイスの通信プロトコルとして SSH-3DES を使用している場合は、デバイス上で該当するプロトコルを必ず有効にしておく必要があります。

ネットワーク デバイスへの SSH 接続を有効にするには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　コンフィギュレーション モードに入ります。

```
sensor# configure terminal
```

ステップ 3　SSH を有効にします。

```
sensor(config)# ssh host blocking_device_ip_address
```

ステップ 4　デバイスを受け入れるよう指示するメッセージが表示されたら、**yes** と入力します。

シグニチャに対してブロッキングが発生していない

特定のシグニチャに対してブロッキングが発生していない場合は、イベント アクションがホストをブロックするように設定されているかどうかチェックします。

特定のシグニチャに対してブロッキングが発生していることを確認するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　シグニチャ定義サブモードを開始します。

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)#
```

ステップ 3　イベント アクションが、ホストをブロックするように設定されていることを確認します。

（注）　アラートを受け取る場合は、イベント アクションを設定するときに、常に **produce-alert** を追加する必要があります。

```
sensor(config-sig)# signatures 1300 0
sensor(config-sig-sig)# engine normalizer
sensor(config-sig-sig-nor)# event-action produce-alert|request-block-host
sensor(config-sig-sig-nor)# show settings
   normalizer
   -----------------------------------------------
      event-action: produce-alert|request-block-host default: produce-alert|deny
-connection-inline
      edit-default-sigs-only
      -----------------------------------------------
         default-signatures-only
         -----------------------------------------------
            specify-service-ports
            -----------------------------------------------
               no
               -----------------------------------------------
               -----------------------------------------------
            -----------------------------------------------
            specify-tcp-max-mss
            -----------------------------------------------
               no
               -----------------------------------------------
               -----------------------------------------------
            -----------------------------------------------
            specify-tcp-min-mss
            -----------------------------------------------
               no
               -----------------------------------------------
               -----------------------------------------------
--MORE--
```

ステップ 4　シグニチャ定義サブモードを終了します。

```
sensor(config-sig-sig-nor)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 5　**Enter** を押して変更内容を確定するか、**no** を入力して、これらを破棄します。

マスター ブロッキング センサーの設定を確認する

マスター ブロッキング センサーが適切に設定されていることを確認するか、適切に設定されていないマスター ブロッキング センサーのトラブルシューティングを行うには、**show statistics network-access** コマンドを使用できます。リモート マスター ブロッキング センサーが TLS を使用して Web アクセスを行っている場合は、転送センサーが TLS の信頼できるホストとして設定されていることを確認します。

マスター ブロッキング センサーの設定を確認するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　ARC の統計情報を表示し、マスター ブロッキング センサーのエントリが統計情報にあることを確認します。

```
sensor# show statistics network-access
Current Configuration
   AllowSensorShun = false
   ShunMaxEntries = 250
   MasterBlockingSensor
      SensorIp = 10.89.149.46
      SensorPort = 443
      UseTls = 1
State
   ShunEnable = true
   ShunnedAddr
      Host
         IP = 122.122.122.44
         ShunMinutes = 60
         MinutesRemaining = 59
```

ステップ 3　統計情報にマスター ブロッキング センサーが表示されていない場合は、追加する必要があります。

ステップ 4　偽のホスト IP アドレスへの手動ブロックを開始し、マスター ブロッキング センサーがブロックを開始していることを確認します。

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)# general
sensor(config-net-gen)# block-hosts 10.16.0.0
```

ステップ 5　ネットワーク アクセス一般サブモードを終了します。

```
sensor(config-net-gen)# exit
sensor(config-net)# exit
Apply Changes:? [yes]:
```

ステップ 6　**Enter** を押して変更内容を確定するか、**no** を入力して、これらを破棄します。

ステップ 7　ARC の統計情報にブロックが表示されていることを確認します。

```
sensor# show statistics network-access
Current Configuration
   AllowSensorShun = false
   ShunMaxEntries = 100
State
   ShunEnable = true
   ShunnedAddr
      Host
         IP = 10.16.0.0
         ShunMinutes =
```

ステップ 8　マスター ブロッキング センサー ホストの CLI にログインし、**show statistics network-access** コマンドを使用して、ブロックがマスター ブロッキング センサー ARC 統計情報にも表示されることを確認します。

```
sensor# show statistics network-access
Current Configuration
   AllowSensorShun = false
   ShunMaxEntries = 250
   MasterBlockingSensor
      SensorIp = 10.89.149.46
      SensorPort = 443
      UseTls = 1
State
   ShunEnable = true
   ShunnedAddr
      Host
         IP = 10.16.0.0
         ShunMinutes = 60
         MinutesRemaining = 59
```

ステップ 9　リモート マスター ブロッキング センサーが TLS を使用して Web アクセスを行っている場合は、転送センサーが TLS ホストとして設定されていることを確認します。

```
sensor# configure terminal
sensor(config)# tls trust ip master_blocking_sensor_ip_address
```

詳細情報

センサーをマスター ブロッキング センサーとして設定する手順については、「マスター ブロッキング センサーの設定」（P.15-28）を参照してください。

ロギング

ここでは、デバッグ ロギングについて説明します。内容は次のとおりです。

デバッグ ロギングについて

TAC では、トラブルシューティングのためにデバッグ ロギングをオンにすることを推奨する場合もあります。ロガーでは、さまざまなロギング ゾーンのロギングの重大度を制御することにより、各アプリケーションが生成するログ メッセージの種類を制御します。デフォルトでは、デバッグ ロギングはオンではありません。

個別ゾーン制御を有効にすると、各ゾーンでは設定されたロギング レベルを使用します。個別ゾーン制御を有効にしなければ、すべてのゾーンで同じロギング レベルが使用されます。

デバッグ ロギングをイネーブルにする

注意　デバッグ ロギングをイネーブルにすることは、パフォーマンスに重大な影響を与えるので、TAC によって指示された場合にのみ使用する必要があります。

デバッグ ロギングをイネーブルにするには、次の手順を実行できます。

ステップ 1　サーバ アカウントにログインします。

ステップ 2　log.conf ファイルを編集し、追加のログ ステートメントに対応できるようにログのサイズを増やします。

```
vi /usr/cids/idsRoot/etc/log.conf
```

ステップ 3　`fileMaxSizeInK=500` を `fileMaxSizeInK=5000` に変更します。

ステップ 4　ファイルのゾーンおよび CID セクションの位置を特定し、重大度をデバッグに設定します。

```
severity=debug
```

ステップ 5　ファイルを保存し、vi エディタを終了し、サービス アカウントを終了します。

ステップ 6　CLI に管理者としてログインします。

ステップ 7　マスター制御サブモードを開始します。

```
sensor# configure terminal
sensor(config)# service logger
sensor(config-log)# master-control
```

ステップ 8　すべてのゾーンのデバッグ ロギングをイネーブルにするには、次のように設定します。

```
sensor(config-log-mas)# enable-debug true
sensor(config-log-mas)# show settings
   master-control
   -----------------------------------------------
      enable-debug: true default: false
      individual-zone-control: false <defaulted>
   -----------------------------------------------
sensor(config-log-mas)#
```

ステップ 9　個々のゾーン制御をオンにするには、次のように設定します。

```
sensor(config-log-mas)# individual-zone-control true
sensor(config-log-mas)# show settings
   master-control
   -----------------------------------------------
      enable-debug: true default: false
      individual-zone-control: true default: false
   -----------------------------------------------
sensor(config-log-mas)#
```

ステップ 10　マスター ゾーン制御を終了します。

```
sensor(config-log-mas)# exit
```

ステップ 11　ゾーン名を表示します。

```
sensor(config-log)# show settings
   master-control
   -----------------------------------------------
      enable-debug: false <defaulted>
      individual-zone-control: true default: false
```

```
   ------------------------------------------------
   zone-control (min: 0, max: 999999999, current: 14)
   ------------------------------------------------
      <protected entry>
      zone-name: AuthenticationApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: Cid
      severity: debug <defaulted>
      <protected entry>
      zone-name: Cli
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdapiCtlTrans
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdsEventStore
      severity: warning <defaulted>
      <protected entry>
      zone-name: MpInstaller
      severity: warning <defaulted>
      <protected entry>
      zone-name: cmgr
      severity: warning <defaulted>
      <protected entry>
      zone-name: cplane
      severity: warning <defaulted>
      <protected entry>
      zone-name: csi
      severity: warning <defaulted>
      <protected entry>
      zone-name: ctlTransSource
      severity: warning <defaulted>
      <protected entry>
      zone-name: intfc
      severity: warning <defaulted>
      <protected entry>
      zone-name: nac
      severity: warning <defaulted>
      <protected entry>
      zone-name: sensorApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: tls
      severity: warning <defaulted>
   ------------------------------------------------
sensor(config-log)#
```

ステップ 12　特定のゾーンの重大度レベル（デバッグ、タイミング、警告、またはエラー）を変更します。

```
sensor(config-log)# zone-control IdsEventStore severity error
sensor(config-log)# show settings
   master-control
   ------------------------------------------------
      enable-debug: true default: false
      individual-zone-control: true default: false
   ------------------------------------------------
   zone-control (min: 0, max: 999999999, current: 14)
   ------------------------------------------------
      <protected entry>
      zone-name: AuthenticationApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: Cid
```

```
      severity: debug <defaulted>
      <protected entry>
      zone-name: Cli
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdapiCtlTrans
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdsEventStore
      severity: error default: warning
      <protected entry>
      zone-name: MpInstaller
      severity: warning <defaulted>
      <protected entry>
      zone-name: cmgr
      severity: warning <defaulted>
      <protected entry>
      zone-name: cplane
      severity: warning <defaulted>
      <protected entry>
      zone-name: csi
      severity: warning <defaulted>
      <protected entry>
      zone-name: ctlTransSource
      severity: warning <defaulted>
      <protected entry>
      zone-name: intfc
      severity: warning <defaulted>
      <protected entry>
      zone-name: nac
      severity: warning <defaulted>
      <protected entry>
      zone-name: sensorApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: tls
      severity: warning <defaulted>
   ------------------------------------------------
sensor(config-log)#
```

ステップ 13　特定のゾーンのデバッグをオンにします。

```
sensor(config-log)# zone-control nac severity debug
sensor(config-log)# show settings
   master-control
   ------------------------------------------------
      enable-debug: true default: false
      individual-zone-control: true default: false
   ------------------------------------------------
   zone-control (min: 0, max: 999999999, current: 14)
   ------------------------------------------------
      <protected entry>
      zone-name: AuthenticationApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: Cid
      severity: debug <defaulted>
      <protected entry>
      zone-name: Cli
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdapiCtlTrans
      severity: warning <defaulted>
      <protected entry>
```

```
      zone-name: IdsEventStore
      severity: error default: warning
      <protected entry>
      zone-name: MpInstaller
      severity: warning <defaulted>
      <protected entry>
      zone-name: cmgr
      severity: warning <defaulted>
      <protected entry>
      zone-name: cplane
      severity: warning <defaulted>
      <protected entry>
      zone-name: csi
      severity: warning <defaulted>
      <protected entry>
      zone-name: ctlTransSource
      severity: warning <defaulted>
      <protected entry>
      zone-name: intfc
      severity: warning <defaulted>
      <protected entry>
      zone-name: nac
      severity: debug default: warning
      <protected entry>
      zone-name: sensorApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: tls
      severity: warning <defaulted>
   ------------------------------------------------
sensor(config-log)#
```

ステップ 14　ロガー サブモードを終了します。

```
sensor(config-log)# exit
Apply Changes:?[yes]:
```

ステップ 15　**Enter** を押して変更内容を確定するか、**no** を入力して、これらを破棄します。

詳細情報

それぞれのゾーン名が示す内容に関するリストについては、「ゾーン名」（P.C-51）を参照してください。

ゾーン名

表 C-2 デバッグ ロガー ゾーン名をリストします。

表 C-2　デバッグ ロガー ゾーン名

ゾーン名	説明
AD	異常検出ゾーン
AuthenticationApp	認証ゾーン
Cid	一般的なロギング ゾーン
Cli	CLI ゾーン
IdapiCtlTrans	すべての制御トランザクション ゾーン

表 C-2　デバッグ ロガー ゾーン名（続き）

ゾーン名	説明
IdsEventStore	イベント ストア ゾーン
MpInstaller	IDSM2 マスター パーティション インストーラ ゾーン
cmgr	カード マネージャ サービス ゾーン[1]
cplane	コントロール プレーン ゾーン[2]
csi	CIDS サーブレット インターフェイス[3]
ctlTransSource	発信制御トランザクション ゾーン
intfc	インターフェイス ゾーン
nac	ARC ゾーン
rep	レピュテーション ゾーン
sched	自動更新スケジューラ ゾーン
sensorApp	AnalysisEngine ゾーン
tls	SSL および TLS ゾーン

1. カード マネージャ サービスは、シャーシ内のモジュール間で制御および状態情報を交換するために、AIP SSM 上で使用されます。
2. コントロール プレーンは、AIP SSM 上のカード マネージャが使用するトランスポート通信層です。
3. CIDS サーブレット インターフェイスは、CIDS Web サーバとサーブレット間のインターフェイス層です。

詳細情報

IPS ロガー サービスの詳細については、「Logger」（P.A-19）を参照してください。

SysLog に cidLog メッセージを転送する

cidLog メッセージを syslog に転送することが有用な場合があります。

cidLog メッセージを syslog に転送するには、次の手順を実行します。

ステップ 1　idsRoot/etc/log.conf ファイルに進みます。

ステップ 2　次の変更を加えます。

a. [logApp] `enabled=false` を設定します。

`enabled=true` はコメント化されます。これは `enabled=false` がデフォルトであるためです。

b. [drain/main] `type=syslog` を設定します。

次の例に、ロギング設定ファイルを示します。

```
timemode=local
;timemode=utc

[logApp]
;enabled=true
;-------- FIFO parameters --------
fifoName=logAppFifo
fifoSizeInK=240
;-------- logApp zone and drain parameters --------
zoneAndDrainName=logApp
```

```
fileName=main.log
fileMaxSizeInK=500

[zone/Cid]
severity=warning
drain=main

[zone/IdsEventStore]
severity=debug
drain=main

[drain/main]
type=syslog
```

syslog の出力が syslog ファシリティ local6 に送信され、syslog メッセージ プロパティとは次の対応関係があります。

```
LOG_DEBUG,        //   debug
LOG_INFO,           //   timing
LOG_WARNING,   //    warning
LOG_ERR,           //   error
LOG_CRIT           //    fatal
```

（注） /etc/syslog.conf の該当するファシリティが適切な優先順位で有効になっていることを確認します。

注意 syslog は logApp よりかなり時間がかかります（1 秒あたり 50 メッセージ程度。logApp は 1 秒あたり 1000 メッセージ程度）。デバッグの重大度は、一度に 1 つのゾーンでのみイネーブルにすることを推奨します。

シグニチャに対して TCP リセットが発生しない

イベント アクションがリセットするよう設定されていない場合、特定のシグニチャに対して TCP リセットが発生しません。

（注） TCP リセットは、MPLS リンクおよび GRE、IPv4 の中の IPv4、IPv4 の中の IPv6、IPv6 の中の IPv4 のトンネルではサポートされていません。

特定のシグニチャに対してリセットが発生しないという問題のトラブルシューティングを行うには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　イベント アクションが TCP リセットに設定されていることを確認します。

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 1000 0
sensor(config-sig-sig)# engine atomic-ip
sensor(config-sig-sig-ato)# event-action reset-tcp-connection|produc-alert
sensor(config-sig-sig-ato)# show settings
   atomic-ip
```

```
   ------------------------------------------------
      event-action: produce-alert|reset-tcp-connection default: produce-alert
      fragment-status: any <defaulted>
      specify-l4-protocol
      ------------------------------------------------
         no
         ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
      specify-ip-payload-length
      ------------------------------------------------
         no
         ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
      specify-ip-header-length
      ------------------------------------------------
         no
         ------------------------------------------------
         ------------------------------------------------
      ------------------------------------------------
      specify-ip-tos
      ------------------------------------------------
--MORE--
```

ステップ 3　シグニチャ定義サブモードを終了します。

```
sensor(config-sig-sig-ato)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 4　**Enter** を押して変更内容を確定するか、**no** を入力して、これらを破棄します。

ステップ 5　正しいアラートが生成されていることを確認します。

```
sensor# show events alert
evAlert: eventId=1047575239898467370 severity=medium
originator:
hostId: sj_4250_40
appName: sensorApp
appInstanceId: 1004
signature: sigId=20000 sigName=STRING.TCP subSigId=0 version=Unknown
addr: locality=OUT 172.16.171.19
port: 32771
victim:
addr: locality=OUT 172.16.171.13 port: 23
actions:
tcpResetSent: true
```

ステップ 6　センサーからの着信 TCP リセット パケットを、スイッチが許容していることを確認します。詳細については、スイッチのマニュアルを参照してください。

ステップ 7　リセットが送信されていることを確認します。

```
root# ./tcpdump -i eth0 src host 172.16.171.19
tcpdump: WARNING: eth0: no IPv4 address assigned
tcpdump: listening on eth0
13:58:03.823929 172.16.171.19.32770 > 172.16.171.13.telnet: R 79:79(0) ack 62 win 0
13:58:03.823930 172.16.171.19.32770 > 172.16.171.13.telnet: R 80:80(0) ack 62 win 0
13:58:03.823930 172.16.171.19.32770 > 172.16.171.13.telnet: R 80:80(0) ack 62 win 0
13:58:03.823930 172.16.171.19.32770 > 172.16.171.13.telnet: R 80:80(0) ack 62 win 0
```

ソフトウェアのアップグレード

ここでは、ソフトウェア アップグレードのトラブルシューティングに役立つ情報を提供します。内容は次のとおりです。

アップグレード

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

IPS センサーをアップグレードする際に分析エンジンが動作していないと、次のエラーを受け取ります。

```
sensor# upgrade scp://user@10.1.1.1/upgrades/IPS-K9-7.1-1-E4.pkg
Password: ********
Warning: Executing this command will apply a major version upgrade to the application
partition.The system may be rebooted to complete the upgrade.
Continue with upgrade?: yes
Error: AnalysisEngine is not running.Please reset box and attempt upgrade again.
```

このエラーを受け取った場合、もう一度アップグレードを試みる前に、分析エンジンを実行させる必要があります。このエラーは、多くの場合、現在実行しているバージョンの不具合によって発生します。センサーをリブートしてみてください。リブート後、**setup** コマンドを実行し、仮想センサー vs0 からインターフェイスを削除します。センサーがトラフィックをモニタしていない場合、分析エンジンは通常そのままアップ状態で実行されます。今度はアップグレードできます。アップグレード後、**setup** コマンドを使用して、インターフェイスを仮想センサー vs0 に追加し直します。

または、システム イメージ ファイルを使用して、センサーのイメージを必要なバージョンに直接再作成できます。イメージの再作成プロセスでは分析エンジンが動作しているかどうかはチェックされないので、エラーを回避しながら、センサーのイメージを再作成できます

注意　システム イメージ ファイルを使用したイメージの再作成では、すべての設定でデフォルト値が復元されます。

詳細情報

- **setup** コマンドの実行の詳細については、第 23 章「センサーの初期化」を参照してください。
- センサーのイメージの再作成の詳細については、第 25 章「システム イメージのアップグレード、ダウングレード、およびインストール」を参照してください。

適用する更新とその前提条件

ソフトウェアのサービス パックのバージョンとマイナーおよびメジャー バージョンは正しいものを使用する必要があります。新しいソフトウェアの適用に関して問題が発生している場合は、適切な前提条件を満たした適切な更新を適用しているかどうかを確認します。

- シグニチャの更新には、ファイル名に示されている最小バージョンとエンジン バージョンが必要です。
- エンジンの更新では、エンジン更新ファイル名のメジャーまたはマイナー バージョンが必要です。サービス パックを適用するには、正しいマイナー バージョンが必要です。
- マイナー バージョンを適用するには、正しいメジャー バージョンが必要です。
- メジャー バージョンを適用するには、前のメジャー バージョンが必要です。

詳細情報

IPS ソフトウェアのファイル名の意味については、「IPS ソフトウェアのバージョン管理」（P.24-3）を参照してください。

自動アップデートに関する問題

次のリストに、自動更新のトラブルシューティングに役立つ情報を示します。

- TCPDUMP を実行します。
  - サービス アカウントを作成します。root に **su** し、さらにコマンド/コントロール インターフェイスで TCPDUMP を実行して、センサーと FTP サーバとの間のパケットをキャプチャします。
  - **upgrade** コマンドを使用して、センサーを手動でアップグレードします。
  - FTP サーバから返されるエラーの TCPDUMP 出力を調べます。
- センサーが正しいディレクトリ内にあることを確認します。

  ディレクトリを正しく指定する必要があります。これが、Windows FTP サーバにおける問題の原因です。場合によっては、ディレクトリ名の前に余分に「/」を 1 つ、または 2 つ付ける必要があります。

  これを確認するには、固有の FTP 接続を介して送信された TCPDUMP 出力に示されているのと同じ FTP コマンドを使用します。
- MS-DOS ファイル構造体ではなく UNIX ファイル構造体をエミュレートするには、Windows FTP サーバ セットアップ オプションを使用する必要があります。
- SCP を使用する場合は、SSH ホスト キーを既知のホスト リストに必ず追加しておきます。

手動による **upgrade** コマンドを試してから、自動アップデートを試みます。**upgrade** コマンドでは動作するが、自動アップデートでは動作しない場合は、次の手順を実行します。

- センサーが使用している IPS ソフトウェア バージョンを確認します。
- 自動更新には、必ずパスワードを設定します。自動アップデートのパスワードは、手動アップデートで使用されるパスワードと一致する必要があります。
- FTP サーバ内のファイル名が、Cisco.com の [Downloads] に表示されるものと同じであることを確認します。これには大文字の使用も含まれます。

  一部の Windows FTP サーバは大文字化されていないファイルへのアクセスを許可しますが、名前が変更されているのでセンサーは最終的にファイルを拒否します。

- 必要であれば、自動更新で TCPDUMP を実行します。正常な手動アップデートを異常な自動アップデートと比較し、そこからトラブルシューティングを行うことができます。

詳細情報

- サービス アカウントの作成手順については、「サービス アカウントの作成」（P.C-5）を参照してください。
- センサーのイメージの再作成手順については、第 25 章「システム イメージのアップグレード、ダウングレード、およびインストール」を参照してください。
- ホストを SSH の既知のホスト リストに追加する手順については、「既知のホスト キーの定義」（P.14-6）を参照してください。
- ソフトウェア バージョンを確認する手順については、「バージョン情報の表示」（P.C-78）を参照してください。

センサーに格納されたアップデートを使用してセンサーを更新する

アップデート パッケージをセンサー上の /var ディレクトリに格納し、必要に応じて、そこからセンサーを更新することができます。

センサーに格納されたアップデートを使用してセンサーを更新するには、次の手順を実行します。

ステップ 1　サーバ アカウントにログインします。

ステップ 2　Cisco.com からアップデート パッケージファイルを取得します。

ステップ 3　FTP または SCP を使用して、更新ファイルをセンサーの /usr/cids/idsRoot/var ディレクトリに送信します。

ステップ 4　ファイルの権限を設定します。

```
chmod 644 ips_package_file_name
```

ステップ 5　サービス アカウントを終了します。

ステップ 6　管理者権限を持つアカウントを使用して次のようにセンサーにログインします。

ステップ 7　センサーのホスト キーを格納します。

```
sensor# configure terminal
sensor(config)# service ssh
sensor(config-ssh)# rsa1-keys sensor_ip_address
```

ステップ 8　センサーをアップグレードします。

```
sensor(config)# upgrade scp://service@Sensor_ip_address/upgrade/ips_package_file_name
Enter password: *****
Re-enter password: *****
```

詳細情報

Cisco IPS ソフトウェアの入手手順については、「Cisco IPS ソフトウェアの入手方法」（P.24-2）を参照してください。

IDM のトラブルシューティング

（注）　次の手順は、ASDM の IPS セクションにも適用されます。

ここでは、IDM のトラブルシューティング手順について説明します。内容は次のとおりです。

IDM を起動できない：Java アプレットのロードに失敗する

症状　ブラウザに「Loading Cisco IDM.Please wait ...」と表示され、ウィンドウの左下に「Loading Java Applet Failed」と表示されます。

考えられる原因　この状態は、IDM を起動しているマシンに複数の Java プラグインがインストールされている場合に発生することがあります。

推奨処置　Java のキャッシュを消去し、temp ファイルを削除して、使用しているブラウザの履歴を消去してください。これで、これらのプラグインがデフォルトで使用されなくなり、各アプレットで適切なプラグインが使用されます。

キャッシュを消去するには、次の手順を実行します。

ステップ 1　すべてのブラウザ ウィンドウを閉じます。

ステップ 2　Java プラグイン 1.3.*x* がインストールされている場合は、次の手順を実行します。

a. [Start] > [Settings] > [Control Panel] > [Java Plug-in 1.3.x] をクリックします。
b. [Advanced] タブをクリックします。
c. [Java Runtime Environment] のドロップダウン メニューから [JRE 1.3.x] を選択します。
d. [Cache] タブをクリックします。
e. [Clear] をクリックします。

ステップ 3　Java プラグイン 1.4.*x* がインストールされている場合は、次の手順を実行します。

a. [Start] > [Settings] > [Control Panel] > [Java Plug-in 1.4.x] をクリックします。
b. [Advanced] タブをクリックします。
c. [Java Runtime Environment] のドロップダウン メニューから [JRE 1.3.x] を選択します。
d. [Cache] タブをクリックします。
e. [Browser] タブをクリックします。
f. ブラウザのすべてのチェックボックスをオフにします。
g. [Clear Cache] をクリックします。

ステップ 4　temp ファイルを削除し、ブラウザの履歴を消去します。

IDM が起動できない：分析エンジンがビジー状態

エラー メッセージ　Error connecting to sensor. Failed to load sensor-errNotAvailable-Analysis Engine is busy. Exiting IDM.

考えられる原因　この状態は、センサーの分析エンジンがタスクの実行でビジー状態となり、IDM に応答しない場合に発生することがあります。

推奨処置　しばらく時間をおいてから、再接続を試みてください。

IDM、リモート マネージャ、または検知インターフェイスがセンサーにアクセスできない

IDM、リモート マネージャ、または検知インターフェイスがセンサーにアクセスできないけれども、SSH または Telnet（イネーブルの場合）を使用してセンサーの CLI にアクセスできる場合は、次の手順を実行します。

ステップ 1　ネットワーク設定で、センサーで設定されている Web サーバ ポートへのアクセスが許可されていることを確認します。

```
sensor# setup


    --- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.


Current Configuration:


service host
network-settings
host-ip 10.89.130.108/23,10.89.130.1
host-name sensor
telnet-option enabled
access-list 0.0.0.0/0
ftp-timeout 300
no login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service web-server
port 443
```

```
exit
```

ステップ 2　ルータ、スイッチ、またはファイアウォールなどのネットワーク デバイスがセンサーとワークステーションの間にある場合、これらのデバイスで、ワークステーションがセンサーの Web サーバ ポートにアクセスできるように設定されていることを確認します。すべてのリモート管理通信は、センサーの Web サーバによって実行されます。

詳細情報

センサー上で Telnet をイネーブルまたはディセーブルにする手順および Web サーバを設定する手順については、「ネットワークの設定」（P.6-2）を参照してください。

シグニチャがアラートを生成しない

注意　イベント アクションを設定するたびに、他のアクションを追加することはできません。イベント アクションを設定するたびに、実際にはそのリストが置き換えられます。したがって、イベント アクションを設定するときは、常に [Produce Alert] を選択してください。

シグニチャが起動されてもアラートが表示されない場合は、イベント アクションとして [Produce Alert] が設定されていることを確認してください。たとえば、[Produce Alert] の選択後に別のイベント アクションを追加し、[Produce Alert] を新しい設定に追加しなかった場合、アラートはイベント ストアに送信されません。アラートを受け取っていることを確認するには、仮想センサーとイベント ストアの統計情報をチェックしてください。

詳細情報

- イベント アクションの詳細については、「イベント アクション」（P.11-8）を参照してください。
- イベント アクションの設定手順については、「シグニチャへのアクションの割り当て」（P.9-19）を参照してください。
- 仮想センサーとイベント ストアに関する統計情報の取得手順については、「統計情報の表示」（P.19-31）を参照してください。

IME のトラブルシューティング

ここでは、IME のトラブルシューティング ツールについて説明します。内容は次のとおりです。

IME とセンサーの時刻の同期

症状　IME の [Events] ダッシュボードに、「No Data Available」と表示されます。履歴クエリーがイベントを返しません。ただし、イベントは IME に報告され、リアルタイム イベント ビューアに表示されます。

考えられる原因　センサーと IME ローカル サーバが同期されていません。IME ダッシュボードは、IME ローカル時刻を基準にした時刻を使用します。これらの時刻が同期されていないと、クエリーから結果が返されません。IME にセンサーを追加すると、時刻の同期がチェックされ、誤っている場合は訂正するよう求める警告が表示されます。[Home] > [Devices] > [Device List] を選択すると、同期に問題があることを示すクロックに関する警告が表示されます。

推奨処置　センサーまたは IME ローカル サーバで時刻の設定を変更します。ほとんどの場合、センサーの時刻は誤って設定されているかデフォルトの時刻に設定されているので、センサーの時刻を変更する必要があります。

詳細情報

- 時刻とセンサーの詳細については、「時刻源とセンサー」（P.C-15）を参照してください。
- センサー上の時刻を変更する手順については、「センサーの時刻の修正」（P.C-17）を参照してください。

「Not Supported」エラー メッセージ

症状　IME のデバイス リスト テーブルおよび一部のガジェットに「Not Supported」と表示され、データが含まれません。

考えられる原因　[Details] をクリックして、このメッセージの説明を表示します。IME で特定の情報を取得するには、IPS 6.1 以降が必要です。IME は、IPS 5.0 以降および特定の IOS IPS バージョンでもイベント モニタリングと報告を行いますが、ヘルス情報や統合された設定などの一部の機能は利用できません。

推奨処置　IPS 6.1 以降にアップグレードしてください。

IDSM2 のトラブルシューティング

（注）　IDSM2 のソフトウェアのアーキテクチャは、4200 シリーズ センサーと同じです。「4200 シリーズ アプライアンスのトラブルシューティング」（P.C-22）に記載されたトラブルシューティング ツールと同じものを使用できます。

ここでは、特に IDSM2 のトラブルシューティングについて説明します。内容は次のとおりです。

- 「ステータス LED は点灯しているが、IDSM2 がオンラインにならない」（P.C-66）
- 「IDSM2 コマンド/コントロール ポートと通信できない」（P.C-66）
- 「TCP リセット インターフェイスの使用方法」（P.C-68）
- 「IDSM2 へのシリアル ケーブルの接続」（P.C-68）

IDSM2 の問題の診断

次のリストに示した内容に基づいて、IDSM2 の問題を診断します。

- IDSM2 とマザーボードとの間のリボン ケーブルが緩んでいます。

  モジュールを物理的に取り扱った際に、ベース カードからコネクタが外れ、ドーター カードとベース カードの接続が失われています。リボン ケーブル コネクタが外れると、ポート 7 および 8 にオンライン診断エラーが発生します。このような状態が生じている場合、モジュールは動作しません。詳細については、Partner Field Notice 29877 を参照してください。

- 不具合の DIMM を搭載して出荷された IDMS2 があります。IDMS2 でメモリの不具合をチェックする手順については、Field Notice 29837 を参照してください。

- ハードディスク ドライブで読み書きができません。

  ハードディスク ドライブが長期間（2 週間以上）、常時使用状態になっていると、次に示すような複数の症状が発生する可能性があります。

  - ログインできない
  - 読み/書き動作を行う際のコンソールに対する I/O エラー（**ls** コマンド）
  - コマンドが正常に実行されない（実行ファイルへのパスを検出できない）

  スイッチからのレポートでモジュールは ok であると示されていても、サービス アカウントにログインするか、コマンドの実行を試みると、問題があることがわかります。4.1(4) サービス パックによってこの問題は多少解決されていますが、4.1(4) アプリケーション パーティション イメージで IDSM2 のイメージを再作成する場合は、4.1(4b) パッチを適用する必要があります。詳細については、toCSCef12198 を参照してください。

- ストリームベースのシグニチャに対して IP ロギングを有効にすると、SensorApp によって CPU がクラッシュしたり CPU が 99% 占有されてしまいます（1300 シリーズ）。回避方法については CSCed32093 を参照してください。

- IDSM2 がロックされ、リモート アクセスが禁止されているように見えます（SSH、Telnet、IDM、Event Server、Control Transaction Server、および IP ログ サーバ）。この不具合は SWAP の使用に関連しています。IDSM2 は ping に応答します。4.1(4) サービス パックを適用して、この問題を解決します。詳細については、CSCed54146 を参照してください。

- IDSM2 をアップグレードして間もなく、または VMS でシグニチャを調整して間もなくすると、IDSM2 は応答しなくなり、多くの場合 SensorApp コア ファイルが生成されます。この問題には、4.1(4b) パッチを適用します。

- IDSM2 の設定がサポートされていることを確認します。

IDSM2 で上に記載された問題がないにもかかわらず、SSH や Telnet からログインできない、スイッチとのセッションを開始できないなど、反応がない場合は、IDSM2 が ping に応答するかどうか、およびサービス アカウントからログインできるかどうかを確認してください。ログインが可能な場合は、cidDump とコア ファイルを取得し、TAC に連絡してください。

詳細情報

サポートされている IDSM2 設定を示す表については、「サポートされている IDSM2 の設定」（P.C-63）を参照してください。

サポートされている IDSM2 の設定

（注）　次の表は特定のバージョンを推奨するものではなく、サポートされている最も初期のバージョンを示しています。

表 C-3 に、サポートされている IDSM2 の最小設定を示します。

表 C-3　IDSM2 機能をサポートする最小 Catalyst 6500 ソフトウェア バージョン

Catalyst/IDSM2 機能	Catalyst ソフトウェア				Cisco IOS ソフトウェア			
	Sup1	Sup2	Sup32	Sup720	Sup1	Sup2	Sup32	Sup720
SPAN	7.5(1)	7.5(1)	8.4(1)	8.1(1)	12.1(19)E1	12.1(19)E1 12.2(18)SXF1	12.2(18)SXF1	12.2(14)SX1
VACL キャプチャ[1]	7.5(1)	7.5(1)	8.4(1)	8.1(1)	12.1(19)E1	12.1(19)E1 12.2(18)SXF1	12.2(18)SXF1	12.2(14)SX1
VACL キャプチャ搭載の ECLB[2]	8.5(1)	8.5(1)	8.5(1)	8.5(1)	該当なし	12.2(18)SXF4	12.2(18)SXF1	12.2(18)SXE1
インライン インターフェイス ペア	8.4(1)	8.4(1)	8.4(1)	8.4(1)	該当なし	12.2(18)SXF4	12.2(18)SXF4	12.2(18)SXE1
インライン インターフェイス ペアを持つ ECLB	8.5(1)	8.5(1)	8.5(1)	8.5(1)	該当なし	12.2(18)SXF4	12.2(18)SXF4	12.2(18)SXF4
インライン VLAN ペア	8.4(1)	8.4(1)	8.4(1)	8.4(1)	該当なし	12.2(18)SXF4	12.2(18)SXF4	12.2(18)SXF4
インライン VLAN ペアを持つ ECLB	8.5(1)	8.5(1)	8.5(1)	8.5(1)	該当なし	12.2(18)SXF4	12.2(18)SXF4	12.2(18)SXF4

1. PFC2/3 または MSFC2/3 が必要。
2. PFC2/3 または MSFC2/3 が必要。

トラブルシューティング用のスイッチ コマンド

次のスイッチ コマンドは、IDSM2 のトラブルシューティングに役立ちます。

- **show module**（Catalyst ソフトウェアおよび Cisco IOS ソフトウェア）
- **show version**（Catalyst ソフトウェアおよび Cisco IOS ソフトウェア）
- **show port**（Catalyst ソフトウェア）
- **show trunk**（Catalyst ソフトウェア）
- **show span**（Catalyst ソフトウェア）
- **show security acl**（Catalyst ソフトウェア）
- **show intrusion-detection module**（Cisco IOS ソフトウェア）

- **show monitor**（Cisco IOS ソフトウェア）
- **show vlan access-map**（Cisco IOS ソフトウェア）
- **show vlan filter**（Cisco IOS ソフトウェア）

ステータス LED が点灯しない

IDSM2 でステータス インジケータが点灯していない場合は、IDSM2 への電源をオンにする必要があります。

（注） IDSM2 を初めて取り付けたときに、ステータスが other を示すのは正常な動作です。IDSM2 が診断ルーチンを完了し、オンラインになると、ステータスは ok となります。IDSM2 がオンラインになるまで 5 分程度かかります。

IDSM2, のステータスを確認するには、次の手順を実行します。

ステップ 1　コンソールにログインします。

ステップ 2　IDSM2 がオンラインであることを確認します。

- Catalyst ソフトウェア

```
console> enable

Enter password:
console> (enable) show module
Mod Slot Ports Module-Type                Model               Sub Status
--- ---- ----- ------------------------- ------------------- --- --------
1   1    2     1000BaseX Supervisor      WS-X6K-SUP1A-2GE    yes ok
15  1    1     Multilayer Switch Feature WS-F6K-MSFC         no  ok
2   2    48    10/100BaseTX Ethernet     WS-X6248-RJ-45      no  ok
3   3    48    10/100/1000BaseT Ethernet WS-X6548-GE-TX      no  ok
4   4    16    1000BaseX Ethernet        WS-X6516A-GBIC      no  ok
6   6    8     Intrusion Detection Mod   WS-SVC-IDSM2        yes ok

Mod Module-Name          Serial-Num
--- -------------------- -----------
1                        SAD041308AN
15                       SAD04120BRB
2                        SAD03475400
3                        SAD073906RC
4                        SAL0751QYN0
6                        SAD062004LV

Mod MAC-Address(es)                         Hw     Fw          Sw
--- --------------------------------------- ------ ----------- ------------------
1   00-d0-c0-cc-0e-d2 to 00-d0-c0-cc-0e-d3 3.1    5.3.1       8.4(1)
    00-d0-c0-cc-0e-d0 to 00-d0-c0-cc-0e-d1
    00-30-71-34-10-00 to 00-30-71-34-13-ff
15  00-30-7b-91-77-b0 to 00-30-7b-91-77-ef 1.4    12.1(23)E2 12.1(23)E2
2   00-30-96-2b-c7-2c to 00-30-96-2b-c7-5b 1.1    4.2(0.24)V 8.4(1)
3   00-0d-29-f6-01-98 to 00-0d-29-f6-01-c7 5.0    7.2(1)     8.4(1)
4   00-0e-83-af-15-48 to 00-0e-83-af-15-57 1.0    7.2(1)     8.4(1)
6   00-e0-b0-ff-3b-80 to 00-e0-b0-ff-3b-87 0.102  7.2(0.67)  5.0(0.30)

Mod Sub-Type                Sub-Model           Sub-Serial  Sub-Hw Sub-Sw
--- ----------------------- ------------------- ----------- ------ ------
1   L3 Switching Engine     WS-F6K-PFC          SAD041303G6 1.1
```

```
6   IDS 2 accelerator board WS-SVC-IDSUPG       .           2.0
console> (enable)
```

- Cisco IOS ソフトウェア

```
router# show module
Mod Ports Card Type                                   Model              Serial No.
--- ----- ------------------------------------- ------------------ -----------
  1   48  48 port 10/100 mb RJ-45 ethernet       WS-X6248-RJ-45     SAD04010l2S
  2   48  48 port 10/100 mb RJ45                 WS-X6348-RJ-45     SAL04483QBL
  3   48  SFM-capable 48 port 10/100/1000mb RJ45 WS-X6548-GE-TX     SAD073906GH
  5    8  Intrusion Detection System             WS-SVC-IDSM2      SAD0751059U
  6   16  SFM-capable 16 port 1000mb GBIC        WS-X6516A-GBIC     SAL0740MMYJ
  7    2  Supervisor Engine 720 (Active)         WS-SUP720-3BXL     SAD08320L2T
  9    1  1 port 10-Gigabit Ethernet Module      WS-X6502-10GE      SAD071903BT
 11    8  Intrusion Detection System             WS-SVC-IDSM2       SAD05380608
 13    8  Intrusion Detection System             WS-SVC-IDSM2      SAD072405D8

Mod MAC addresses                       Hw     Fw           Sw           Status
--- ----------------------------------- ------ ------------ ------------ -------
  1  00d0.d328.e2ac to 00d0.d328.e2db   1.1    4.2(0.24)VAI 8.5(0.46)ROC Ok
  2  0003.6c14.e1d0 to 0003.6c14.e1ff   1.4    5.4(2)       8.5(0.46)ROC Ok
  3  000d.29f6.7a80 to 000d.29f6.7aaf   5.0    7.2(1)       8.5(0.46)ROC Ok
  5  0003.fead.651a to 0003.fead.6521   4.0    7.2(1)       5.0(1.1)     Ok
  6  000d.ed23.1658 to 000d.ed23.1667   1.0    7.2(1)       8.5(0.46)ROC Ok
  7  0011.21a1.1398 to 0011.21a1.139b   4.0    8.1(3)       12.2(PIKESPE Ok
  9  000d.29c1.41bc to 000d.29c1.41bc   1.3    Unknown      Unknown      PwrDown
 11  00e0.b0ff.3340 to 00e0.b0ff.3347   0.102  7.2(0.67)    5.0(1.1)     Ok
 13  0003.feab.c850 to 0003.feab.c857   4.0    7.2(1)       5.0(1)       Ok

Mod Sub-Module                  Model              Serial        Hw     Status
--- --------------------------- ------------------ ------------ ------- -------
  5 IDS 2 accelerator board     WS-SVC-IDSUPG      07E91E508A    2.0    Ok
  7 Policy Feature Card 3       WS-F6K-PFC3BXL     SAD083305A1   1.3    Ok
  7 MSFC3 Daughterboard         WS-SUP720          SAD083206JX   2.1    Ok
 11 IDS 2 accelerator board     WS-SVC-IDSUPG      .             2.0    Ok
 13 IDS 2 accelerator board     WS-SVC-IDSUPG      0347331976    2.0    Ok

Mod Online Diag Status
--- -------------------
  1 Pass
  2 Pass
  3 Pass
  5 Pass
  6 Pass
  7 Pass
  9 Unknown
 11 Pass
 13 Pass
router#
```

ステップ 3　ステータスが ok にならないときは、モジュールをオンにします。

```
router# set module power up module_number
```

ステータス LED は点灯しているが、IDSM2 がオンラインにならない

ステータス インジケータは点灯しているけれども、IDSM2 がオンラインにならない場合は、次のトラブルシューティングを実行してください。

- IDSM2 をリセットします。
- IDSM2 がスイッチに適切に取り付けられていることを確認します。
- ハードディスク ドライブのステータスに問題がある場合は、アプリケーション パーティションのイメージを再度作成します。

IDSM2 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　コンソールにログインします。

ステップ 2　IDSM2 がイネーブルになっていることを確認します。

```
router# show module
```

ステップ 3　ステータスが ok を示していない場合は、IDSM2 をイネーブルにします。

```
router# set module enable module_number
```

ステップ 4　それでも IDSM2 がオンラインにならない場合は、リセットします。

```
router# reset module_number
```

IDSM2 がオンラインになるまで、5 分程度かかります。

ステップ 5　それでも IDSM2 がオンラインにならない場合は、ハードウェアとオペレーティング システムが ok であるかどうか確認します。

```
router# show test module_number
```

ステップ 6　port のステータスが fail を示している場合は、IDSM2 がスイッチにしっかりと接続されているか確認します。

ステップ 7　hdd ステータスが fail を示している場合は、アプリケーション パーティションのイメージを再作成する必要があります。

詳細情報

アプリケーション パーティション イメージの再作成手順については、第 25 章「システム イメージのアップグレード、ダウングレード、およびインストール」を参照してください。

IDSM2 コマンド/コントロール ポートと通信できない

IDSM2 のコマンド/コントロール ポートと通信できない場合は、コマンド/コントロール ポートが正しい VLAN に置かれていない場合があります。

IDSM2 のコマンド/コントロール ポートと通信するには、次の手順を実行します。

ステップ 1　コンソールにログインします。

ステップ 2　ping を使用して他のシステムからコマンド ポートに接続できることを確認します。

ステップ 3　IP アドレス、マスク、およびゲートウェイ設定が正しいことを確認します。

```
router# show configuration
```

ステップ 4　コマンド/コントロール ポートが正しい VLAN 内にあることを確認します。

- Catalyst ソフトウェア

```
console> (enable) show port 6/8
* = Configured MAC Address

# = 802.1X Authenticated Port Name.

Port  Name                 Status     Vlan       Duplex Speed       Type
----- -------------------- ---------- ---------- ------ ----------- ------------
 6/8                       connected  trunk        full        1000 IDS


Port  Status      ErrDisable Reason    Port ErrDisableTimeout  Action on Timeout
----  ----------  -------------------  ----------------------  -----------------
 6/8  connected                     -  Enable                  No Change

Port  Align-Err  FCS-Err    Xmit-Err   Rcv-Err    UnderSize
----- ---------- ---------- ---------- ---------- ---------
 6/8           0          0          0          0         0

Port  Single-Col Multi-Coll Late-Coll  Excess-Col Carri-Sen Runts     Giants
----- ---------- ---------- ---------- ---------- --------- --------- ---------
 6/8           0          0          0          0         0         0         -

Port  Last-Time-Cleared
----- --------------------------
 6/8  Wed Mar 2 2005, 15:29:49

Idle Detection
--------------
   --
console> (enable)
```

- Cisco IOS ソフトウェア

```
router#show intrusion-detection module 5 management-port state
Intrusion-detection module 5 management-port:

Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Vlans allowed on trunk:1
Vlans allowed and active in management domain: 1
Vlans in spanning tree forwarding state and not pruned:
   1
Access Vlan = 1


router#
```

ステップ 5　コマンド/コントロール ポートが正しい VLAN に存在しない場合は、正しい VLAN に配置してください。

詳細情報

スイッチを IDSM2 へのコマンドおよび制御アクセス用に設定する手順については、『Configuring the Catalyst 6500 Series Switch for Command and Control Access to IDSM2』を参照してください。

TCP リセット インターフェイスの使用方法

IDSM2 には、TCP リセット インターフェイス（ポート 1）があります。IDSM2 は、センシング ポートで TCP リセットを送信できないので、専用の TCP リセット インターフェイスが用意されています。IDSM2 においてリセット上の問題が発生した場合は、次の手順を試してください。

- センシング ポートがアクセス ポート（1 つの VLAN）である場合、リセット ポートが同じ VLAN に存在するように設定する必要があります。
- センシング ポートが dot1q トランク ポート（マルチ VLAN）である場合、このセンシング ポートとリセット ポートはすべて同じネイティブ VLAN を持つ必要があり、リセット ポートは両方のセンシング ポートによってトランク接続されている VLAN すべてにトランク接続されている必要があります。

詳細情報

TCP リセット インターフェイスの使用の詳細については、『Configuring the IDSM2』を参照してください。

IDSM2 へのシリアル ケーブルの接続

IDSM2 上のシリアル コンソール ポートにシリアル ケーブルを直接接続することができます。これにより、スイッチおよびモジュールのネットワーク インターフェイスをバイパスできます。

シリアル ケーブルを IDSM2 に接続するには、次の手順を実行します。

ステップ 1　IDSM2 で 2 つの RJ-45 ポートの位置を探します。マザーボードのほぼ中心にあります。モジュールの前面プレートと向き合っている場合は、右側にある RJ-45 ポートがシリアル コンソール ポートです。

ステップ 2　ストレート型ケーブルを IDSM2 の右側のポートに接続し、ケーブルの他端をターミナル サーバ ポートに接続します。

ステップ 3　ターミナル サーバ ポートを 19200 ボー、8 ビット、パリティなしに設定します。これで IDSM2 に直接ログインできるようになります。

（注）　シリアル ケーブルはシャーシの前方から引き出す必要があるため、IDSM2 へのシリアル ケーブルの接続は、スイッチ シャーシ内で IDSM2 の上にモジュールが配置されていない場合にのみ可能です。

AIP SSM、AIP SSC-5、および IPS SSP のトラブルシューティング

（注） AIP SSM、AIP SSC-5、および IPS SSP は、4200 シリーズ センサーとして同じソフトウェア アーキテクチャを共有しています。「4200 シリーズ アプライアンスのトラブルシューティング」（P.C-22）に記載されたトラブルシューティング ツールと同じものを使用できます。

ここでは、AIP SSM、AIP SSC-5、および IPS SSP のトラブルシューティングについて説明します。内容は次のとおりです。

ヘルスおよびステータス情報

（注） 次の例は AIP SSM の情報を示していますが、手順は AIP-SSC-5 と IPS SSP でも使用できます。

ASA モジュールの一般的なヘルス状態を表示するには、**show module 1 details** コマンドを使用します。

```
asa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model:              ASA-SSM-20
Hardware version:   0.2
Serial Number:      P2B000005D0
Firmware version:   1.0(10)0
Software version:   5.1(0.1)S153.0
Status:             Up
Mgmt IP addr:       10.89.149.219
Mgmt web ports:     443
Mgmt TLS enabled:   true
asa#
```

出力は ASA モジュールがアップ状態であることを示しています。ステータスが Down の場合、**hw-module module 1 reset** コマンドを使用して、ASA モジュールをリセットできます。

```
asa# hw-module module 1 reset
The module in slot 1 should be shut down before
resetting it or loss of configuration may occur.
Reset module in slot 1? [confirm]
Reset issued for module in slot 1
asa(config)# show module

Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5520 Adaptive Security Appliance         ASA5520            P2A00000014
  1 ASA 5500 Series Security Services Module-10  ASA-SSM-10         P2A0000067U

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
```

```
--- -------------------------------- ------------ ------------ ---------------
  0 000b.fcf8.7bdc to 000b.fcf8.7be0  0.2          1.0(10)0     7.0(1)
  1 000b.fcf8.0176 to 000b.fcf8.0176  0.2          1.0(10)0     5.1(0.1)S153.0

Mod Status
--- ------------------
  0 Up Sys
  1 Shutting Down
**************************************************
asa(config)# show module

Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5520 Adaptive Security Appliance         ASA5520            P2A00000014
  1 ASA 5500 Series Security Services Module-10  ASA-SSM-10         P2A0000067U

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- -------------------------------- ------------ ------------ ---------------
  0 000b.fcf8.7bdc to 000b.fcf8.7be0  0.2          1.0(10)0     7.0(1)
  1 000b.fcf8.0176 to 000b.fcf8.0176  0.2          1.0(10)0     5.1(0.1)S153.0

Mod Status
--- ------------------
  0 Up Sys
  1 Up
asa(config)#
```

ASA モジュールの回復時に問題が発生した場合は、**debug module-boot** コマンドを使用して、ASA モジュールのブート時の出力を確認します。TFTP サーバの IP アドレスとファイルが正しいことを確認します。次に、もう一度 **hw-module module 1 recover** コマンドを使用して、モジュールを回復します。

```
asa(config)# hw-module module 1 recover configure
Image URL [tftp://0.0.0.0/]: tftp://10.89.146.1/IPS-SSM-K9-sys-1.1-a-5.1-0.1.i$
Port IP Address [0.0.0.0]: 10.89.150.227
VLAN ID [0]:
Gateway IP Address [0.0.0.0]: 10.89.149.254
asa(config)# debug module-boot
debug module-boot enabled at level 1
asa(config)# hw-module module 1 recover boot
The module in slot 1 will be recovered. This may erase all configuration and all data on
that device and attempt to download a new image for it.
Recover module in slot 1? [confirm]
Recover issued for module in slot 1
asa(config)# Slot-1 140> Cisco Systems ROMMON Version (1.0(10)0) #0: Fri Mar 25 23:02:10
PST 2005
Slot-1 141> Platform ASA-SSM-10
Slot-1 142> GigabitEthernet0/0
Slot-1 143> Link is UP
Slot-1 144> MAC Address: 000b.fcf8.0176
Slot-1 145> ROMMON Variable Settings:
Slot-1 146>   ADDRESS=10.89.150.227
Slot-1 147>   SERVER=10.89.146.1
Slot-1 148>   GATEWAY=10.89.149.254
Slot-1 149>   PORT=GigabitEthernet0/0
Slot-1 150>   VLAN=untagged
Slot-1 151>   IMAGE=IPS-SSM-K9-sys-1.1-a-5.1-0.1.img
Slot-1 152>   CONFIG=
Slot-1 153>   LINKTIMEOUT=20
Slot-1 154>   PKTTIMEOUT=4
Slot-1 155>   RETRY=20
Slot-1 156> tftp IPS-SSM-K9-sys-1.1-a-5.1-0.1.img@10.89.146.1 via 10.89.149.254
Slot-1 157> TFTP failure: Packet verify failed after 20 retries
```

```
Slot-1 158> Rebooting due to Autoboot error ...
Slot-1 159> Rebooting....
Slot-1 160> Cisco Systems ROMMON Version (1.0(10)0) #0: Fri Mar 25 23:02:10 PST 2005
Slot-1 161> Platform ASA-SSM-10
Slot-1 162> GigabitEthernet0/0
Slot-1 163> Link is UP
Slot-1 164> MAC Address: 000b.fcf8.0176
Slot-1 165> ROMMON Variable Settings:
Slot-1 166>   ADDRESS=10.89.150.227
Slot-1 167>   SERVER=10.89.146.1
Slot-1 168>   GATEWAY=10.89.149.254
Slot-1 169>   PORT=GigabitEthernet0/0
Slot-1 170>   VLAN=untagged
Slot-1 171>   IMAGE=IPS-SSM-K9-sys-1.1-a-5.1-0.1.img
Slot-1 172>   CONFIG=
Slot-1 173>   LINKTIMEOUT=20
Slot-1 174>   PKTTIMEOUT=4
Slot-1 175>   RETRY=20
Slot-1 176> tftp IPS-SSM-K9-sys-1.1-a-5.1-0.1.img@10.89.146.1 via 10.89.149.254
```

IPS スイッチボードのフェールオープン ポリシーでトラフィック フローが停止する

問題　IPS SSP がリセットまたはシャットダウンされると、IPS SSP（1/x）に置かれているポートでトラフィックが通過しなくなります。この問題は、トラフィックが IPS によってモニタされているかどうかに関係なく、これらのポートを通過するすべてのトラフィックに影響を与えます。IPS SSP がリセットまたはシャットダウンされると、ポート上のリンクがリンク ダウンします。

考えられる原因　IPS SSP（1/x）に置かれているポートを使用して、任意のメカニズムからリセットまたはシャットダウンします。

ソリューション　適応型セキュリティ アプライアンス（0/x）上のポートは、IPS SSP がリセットまたはシャットダウンされてもリンクは失われないので、これらのポートを使用します。

フェールオーバー シナリオ

次のフェールオーバー シナリオは、IPS SSP での設定変更、シグニチャおよびシグニチャ エンジンの更新、サービス パック、および SensorApp クラッシュ時に ASA 5585-X に適用されます。

フェールオープン モードの 1 台の ASA 5585-X

- ASA が IPS SSP に対してフェールオープン モードに設定され、IPS SSP で設定変更またはシグニチャ / シグニチャ エンジンの更新が行われた場合、トラフィックは検査を受けずに ASA を通過します。
- ASA が IPS SSP に対してフェールオープン モードに設定され、IPS SSP で SensorApp のクラッシュまたはサービス パックのアップグレードが発生した場合、トラフィックは検査を受けずに ASA を通過します。

フェールクローズ モードの 1 台の ASA 5585-X

- ASA が IPS SSP に対してフェールクローズ モードに設定され、IPS SSP で設定変更またはシグニチャ / シグニチャ エンジンの更新が行われた場合、ASA 経由のトラフィックは停止します。

- ASA が IPS SSP に対してフェールクローズ モードに設定され、IPS SSP で SensorApp クラッシュまたはサービス パックのアップグレードが発生した場合、ASA 経由のトラフィックは停止します。

フェールオープン モードの 2 台の ASA 5585-X

- 2 台の ASA がフェールオープン モードに設定され、アクティブな ASA 上の IPS SSP で設定変更やシグニチャ / シグニチャ エンジンの更新が行われた場合、トラフィックは検査を受けずにアクティブな ASA をそのまま通過します。フェールオーバーはトリガーされません。
- 2 台の ASA がフェールオープン モードに設定され、アクティブな ASA 上の IPS SSP で SensorApp のクラッシュまたはサービス パックのアップグレードが発生した場合、フェールオーバーがトリガーされ、トラフィックは前にスタンバイ IPS SSP だった IPS SSP を通過します。

フェールクローズ モードの 2 台の ASA 5585-X

- 2 台の ASA がフェールクローズ モードに設定され、アクティブな ASA 上の IPS SSP で設定変更またはシグニチャ / シグニチャ エンジンの更新が行われた場合、アクティブな ASA 経由のトラフィックは停止します。フェールオーバーはトリガーされません。
- 2 台の ASA がフェールクローズ モードに設定され、アクティブな ASA 上の IPS SSP で SensorApp のクラッシュまたはサービス パックのアップグレードが発生した場合、フェールオーバーがトリガーされ、トラフィックは前にスタンバイ IPS SSP だった IPS SSP を通過します。

設定例

プライマリ ASA には次の設定を使用します。

```
interface GigabitEthernet0/7
 description LAN Failover Interface

failover
failover lan unit primary
failover lan interface folink GigabitEthernet0/7
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```

セカンダリ ASA には次の設定を使用します。

```
interface GigabitEthernet0/7
 description LAN Failover Interface

failover
failover lan unit secondary
failover lan interface folink GigabitEthernet0/7
failover interface ip folink 172.27.48.1 255.255.255.0 standby 172.27.48.2
```

AIP SSM およびデータ プレーン

症状　AIP SSM データ プレーンは、シグニチャの更新の適用中もアップ状態が維持されます。AIP SSM データ プレーンのステータスをチェックするには、シグニチャの更新中に **show module** コマンドを使用します。

考えられる原因　バイパス モードがオフに設定されています。この問題は、シグニチャの更新中、および CSM または IDM を使用してシグニチャの更新を適用するときに発生します。この問題は、IPS システム ソフトウェアのアップグレード中は発生しません。

AIM IPS および NME IPS のトラブルシューティング

（注） AIM IPS と NME IPS は 4200 シリーズ センサーとして同じソフトウェア アーキテクチャを共有しています。「4200 シリーズ アプライアンスのトラブルシューティング」（P.C-22）に記載されたトラブルシューティング ツールと同じものを使用できます。

ここでは、IPS ネットワーク モジュールの AIM IPS と NME IPS のトラブルシューティングについて説明します。内容は次のとおりです。

他の IPS ネットワーク モジュールとの相互運用性

Cisco アクセス ルータは、ルータごとに 1 つの IDS/IPS モジュールのみをサポートします。複数の IDS/IPS モジュールがインストールされている場合、最も高度な機能を持つカードがイネーブルになります。高度な機能の階層は次のとおりです。

1. NME IPS
2. AIM IPS
3. NM CIDS

たとえば、すべてのモジュールがインストールされている場合、NME IPS によって他のすべてのモジュールがディセーブルになることを意味します。AIM IPS によって、すべての NM CID をディセーブルにします。同じ機能レベルのモジュールが複数インストールされている場合、最初に検出されたモジュールがイネーブルになり、他のすべてのカードはディセーブルになります。

ディセーブルのモジュールを起動、イネーブル化、および設定することはできません。機能性の低いモジュールを起動するには、高機能モジュールをルータから削除し、リブートする必要があります。ディセーブルのモジュールは、**show diag** コマンド出力に表示されます。モジュールの状態は、存在するけれどもディセーブル状態であると報告されます。

最も高機能のモジュールのスロットおよびポートが **interface ids slot/port** コンフィギュレーション コマンドと一致しない場合、次の警告が表示され、そのモジュールはディセーブルになります。

```
The module in slot x will be disabled and configuration ignored.
```

正しいスロット/ポート番号が表示されるので、設定を変更できます。

注意　NM CIDS を NME IPS にアップグレードすることはできません。NM CIDS の詳細については、『Introducing NM CIDS』と『Installing NM CIDS』を参照してください。

情報の収集

次に示す CLI コマンドおよびスクリプトを使用すれば、問題が発生した際にセンサーに関する情報を収集し、センサーの状態を診断することができます。**show tech-support** コマンドを使用してセンサーのすべての情報を収集することも、ここで示す他の個々のコマンドを使用して特定の情報を収集することもできます。

ここでは、次の項目について説明します。

ヘルスおよびネットワーク セキュリティ情報

特権 EXEC モードで **show health** コマンドを使用して、センサーの全体的なヘルス ステータス情報を表示します。ヘルス ステータス カテゴリは赤と緑でランク付けされ、赤が重大です。

注意　センサーが初めて起動するとき、完全なアップ状態となって動作するまで、一部のヘルス メトリックのステータスが赤になるのは正常な動作です。

センサーの全体的なヘルス ステータスを表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　センサーのヘルスおよびセキュリティ ステータスを表示します。

```
sensor# show health
Overall Health Status                                 Red
Health Status for Failed Applications                 Green
Health Status for Signature Updates                   Green
Health Status for License Key Expiration              Red
Health Status for Running in Bypass Mode              Green
Health Status for Interfaces Being Down               Red
Health Status for the Inspection Load                 Green
Health Status for the Time Since Last Event Retrieval Green
Health Status for the Number of Missed Packets        Green
Health Status for the Memory Usage                    Not Enabled
Health Status for Global Correlation                  Red
```

```
Health Status for Network Participation                Not Enabled

Security Status for Virtual Sensor vs0   Green
sensor#
```

テクニカル サポート情報

show tech-support コマンドは、センサーのすべてのステータスおよび設定情報をキャプチャするのに役立ちます。ここでは、**show tech-support** コマンドについて説明します。内容は次のとおりです。

- 「show tech-support コマンドについて」（P.C-75）
- 「技術サポート情報の表示」（P.C-75）
- 「テクニカル サポート コマンド出力」（P.C-76）

show tech-support コマンドについて

show tech-support コマンドはセンサーにおけるすべてのステータスと情報をキャプチャし、現在の設定、バージョン情報、cidDump 情報などが含まれます。出力は、大きくなり 1 MB を超えることもあります。出力はリモート システムに転送できます。リモート システムに出力をコピーする手順については、「技術サポート情報の表示」（P.C-75）を参照してください。

同じ情報を IME から取得するには、[Configuration] > *sensor_name* > [Sensor Monitoring] > [Support Information] > [System Information] を選択します。

（注）　TAC に連絡する前に **show tech-support** コマンドを必ず実行してください。

技術サポート情報の表示

show tech-support [**page**] [**destination-url** *destination_url*] コマンドを使用して、画面にシステム情報を表示するか、特定の URL に送信します。その情報を TAC のトラブルシューティング情報として使用できます。

次のパラメータはオプションです。

- **page**：一度に 1 ページの情報として出力を表示します。**Enter** を押して、出力の次の行を表示するか、スペースバーを使用して、次の情報ページを表示します。
- **destination-url**：情報を HTML としてフォーマットし、このコマンドに続く宛先に送信する必要があることを示します。このキーワードを使用すると、出力は画面に表示されません。
- *destination-url*：情報を HTML としてフォーマットする必要があることを示します。URL は、情報を送信する宛先を示します。このキーワードを使用しない場合、情報は画面に表示されます。

技術サポート情報を表示するには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　画面上に出力を表示します。

```
sensor# show tech-support page
```

システム情報が画面上に一度に 1 ページずつ表示されます。次のページを表示するにはスペースバーを押します。プロンプトに戻るには、**Ctrl+C** を押します。

ステップ 3　出力（HTML フォーマット）をファイルに送信するには、次の手順を実行します。

a. 次のコマンドを入力し、その後ろに有効な宛先を指定します。

```
sensor# show tech-support destination-url destination_url
```

次に示す種類の宛先を指定できます。

- **ftp:** : FTP ネットワーク サーバの宛先 URL。このプレフィクスの構文は、`ftp:[[//username@location]/relativeDirectory]/filename` または `ftp:[[//username@location]//absoluteDirectory]/filename` です。
- **scp:** : SCP ネットワーク サーバの宛先 URL。このプレフィクスの構文は、`scp:[[//username@]location]/relativeDirectory]/filename` または `scp:[[//username@]location]//absoluteDirectory]/filename` です。

たとえば、テクニカル サポート出力をファイル `/absolute/reports/sensor1Report.html` に送信するには、次のコマンドを入力します。

```
sensor# show tech support dest
ftp://csidsuser@10.2.1.2//absolute/reports/sensor1Report.html
```

`password:` プロンプトが表示されます。

b. このユーザ アカウントのパスワードを入力します。`Generating report:` メッセージが表示されます。

テクニカル サポート コマンド出力

show tech-support コマンド出力の例を次に示します。

（注） この出力例では、コマンドの先頭部分を示すとともに、インターフェイス、ARC、および cidDump サービスに関する情報を一覧表示します。

```
sensor# show tech-support page
System Status Report
This Report was generated on Wed Apr 8 21:42:39 2009.
Output from show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.1(1)E4

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S383.0                  2009-02-20
    Virus Update        V1.4                    2007-03-02
OS Version:             2.4.30-IDS-smp-bigphys
Platform:               IPS 4240-K9
Serial Number:          JMX1013K020
No license present
Sensor up-time is 1 day.
Using 1421914112 out of 1984552960 bytes of available memory (71% usage)
system is using 16.5M out of 38.5M bytes of available disk space (43% usage)
application-data is using 43.5M out of 166.8M bytes of available disk space (27%
 usage)
```

```
boot is using 40.5M out of 68.6M bytes of available disk space (62% usage)
application-log is using 123.5M out of 513.0M bytes of available disk space (24%
 usage)


MainApp            B-BEAU_2009_APR_07_08_00_7_0_0_118   (Release)   2009-04-07T0
8:05:05-0500   Running
AnalysisEngine     B-BEAU_2009_APR_07_08_00_7_0_0_118   (Release)   2009-04-07T0
8:05:05-0500   Running
CollaborationApp   B-BEAU_2009_APR_07_08_00_7_0_0_118   (Release)   2009-04-07T0
8:05:05-0500   Running
CLI                B-BEAU_2009_APR_07_08_00_7_0_0_118   (Release)   2009-04-07T0
8:05:05-0500

Upgrade History:

  IPS-K9-7.1-1-E4 21:41:28 UTC Mon Feb 22 2010

Recovery Partition Version 1.1 - 7.1(1)E4

Host Certificate Valid from: 08-Apr-2009 to 09-Apr-2011


Output from show interfaces
Interface Statistics
   Total Packets Received = 0
   Total Bytes Received = 0
   Missed Packet Percentage = 0
   Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/0
   Interface function = Sensing interface
   Description =
   Media Type = TX
   Default Vlan = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Hardware Bypass Capable = No
   Hardware Bypass Paired = N/A
   Link Status = Down
   Admin Enabled Status = Disabled
   Link Speed = N/A
   Link Duplex = N/A
   Missed Packet Percentage = 0
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface Management0/0
   Interface function = Command-control interface
--MORE--
```

バージョン情報

show version コマンドは、センサー情報の取得に役立ちます。ここでは、**show version** コマンドについて説明します。内容は次のとおりです。

show version コマンドについて

show version コマンドは、基本的なセンサー情報を示します。さらに、障害が発生している場所を示すことができます。次のような情報が提供されます。

- 実行中のアプリケーション
- アプリケーションのバージョン
- ディスクおよびメモリの用途
- アプリケーションのアップグレード履歴

（注） 同じ情報を IME から取得するには、[Configuration] > *sensor_name* > [Sensor Monitoring] > [Support Information] > [Diagnostics Report] を選択します。

バージョン情報の表示

インストールされているすべてのオペレーティング システム パッケージ、シグニチャ パッケージ、およびシステムで実行中の IPS プロセスのバージョン情報を表示するには、**show version** コマンドを使用します。システム全体の設定を表示するには、**more current-config** コマンドを使用します。

バージョンおよび設定を表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　バージョン情報を表示します。

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.1(1)E4

Host:
    Realm Keys          key1.0
Signature Definition:
    Signature Update    S518.0              2010-10-04
OS Version:             2.6.29.1
Platform:               ASA5585-SSP-IPS20
Serial Number:          JAF1350ABSF
Licensed, expires:      04-Oct-2011 UTC
Sensor up-time is 4:32.
Using 10378M out of 11899M bytes of available memory (87% usage)
system is using 25.1M out of 160.0M bytes of available disk space (16% usage)
application-data is using 65.4M out of 171.4M bytes of available disk space (40%
 usage)
boot is using 56.1M out of 71.7M bytes of available disk space (83% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96%
 usage)
```

```
MainApp            S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500   Running
AnalysisEngine     S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500   Running
CollaborationApp   S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500   Running
CLI                S-SPYKER_2010_OCT_21_00_27_7_1_1   (Release)   2010-10-21
T00:29:47-0500

Upgrade History:

  IPS-K9-7.1-1-E4   00:42:07 UTC Thu Oct 21 2010

Recovery Partition Version 1.1 - 7.1(1)E4

Host Certificate Valid from: 21-Oct-2010 to 21-Oct-2012

sensor#
```

（注） --MORE-- というプロンプトが表示された場合、スペースバーを押すと詳細な情報が表示され、**Ctrl+C** キーを押すと出力がキャンセルされ CLI プロンプトに戻ります。

ステップ 3　設定情報を表示します。

（注） **more current-config** または **show configuration** コマンドを使用できます。

```
sensor# more current-config
! ------------------------------
! Current configuration last modified Fri Apr 10 13:29:06 2009
! ------------------------------
! Version 7.1(1)
! Host:
!     Realm Keys          key1.0
! Signature Definition:
!     Signature Update    S383.0   2009-02-20
!     Virus Update        V1.4     2007-03-02
! ------------------------------
service interface
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 10.89.147.24/25,10.89.147.126
telnet-option enabled
access-list 0.0.0.0/0
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
```

```
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
exit
! ------------------------------
service web-server
exit
! ------------------------------
service anomaly-detection ad0
exit
! ------------------------------
service external-product-interface
exit
! ------------------------------
service health-monitor
exit
! ------------------------------
service global-correlation
exit
! ------------------------------
service analysis-engine
exit
sensor#
```

統計情報

show statistics コマンドは、センサーのサービスの状態を調べる際に役立ちます。ここでは、**show statistics** コマンドについて説明します。内容は次のとおりです。

- 「show statistics コマンドについて」（P.C-80）
- 「統計情報の表示」（P.C-81）

show statistics コマンドについて

センサーのサービスの状態のスナップショットを表示するには、**show statistics** コマンドを使用します。次のサービスは統計情報を提供します。

- 分析エンジン
- 認証
- 拒否攻撃者
- イベント サーバ
- イベント ストア
- ホスト
- Logger

- 攻撃応答（旧ネットワーク アクセス）
- 通知
- SDEE サーバ
- トランザクション サーバ
- トランザクション ソース
- 仮想センサー
- Web サーバ

（注）　同じ情報を IME から取得するには、[Configuration] > *sensor_name* > [Sensor Monitoring] > [Support Information] > [Statistics] を選択します。

統計情報の表示

各センサー アプリケーションの統計情報を表示するには、**show statistics [analysis-engine** | **anomaly-detection** | **authentication** | **denied-attackers** | **event-server** | **event-store** | **external-product-interface** | **global-correlation** | **host** | **logger** | **network-access** | **notification** | **os-identification** | **sdee-server** | **transaction-server** | **virtual-sensor** | **web-server] [clear]** コマンドを使用します。

すべての仮想センサーについてこれらのコンポーネントの統計情報を表示するには、**show statistics** {**anomaly-detection** | **denied-attackers** | **os-identification** | **virtual-sensor**} [***name*** | **clear**] コマンドを使用します。仮想センサー名を指定すると、その仮想センサーの統計情報だけが表示されます。

（注）　**clear** オプションは、分析エンジン、異常検出、ホスト、ネットワーク アクセス、または OS 識別アプリケーションには使用できません。

センサーの統計情報を表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　分析エンジンの統計情報を表示します。

```
sensor# show statistics analysis-engine
Analysis Engine Statistics
   Number of seconds since service started = 1421127
   Measure of the level of current resource utilization = 0
   Measure of the level of maximum resource utilization = 0
   The rate of TCP connections tracked per second = 0
   The rate of packets per second = 0
   The rate of bytes per second = 0
   Receiver Statistics
      Total number of packets processed since reset = 0
      Total number of IP packets processed since reset = 0
   Transmitter Statistics
      Total number of packets transmitted = 0
      Total number of packets denied = 0
      Total number of packets reset = 0
   Fragment Reassembly Unit Statistics
      Number of fragments currently in FRU = 0
      Number of datagrams currently in FRU = 0
   TCP Stream Reassembly Unit Statistics
      TCP streams currently in the embryonic state = 0
```

```
      TCP streams currently in the established state = 0
      TCP streams currently in the closing state = 0
      TCP streams currently in the system = 0
      TCP Packets currently queued for reassembly = 0
   The Signature Database Statistics.
      Total nodes active = 0
      TCP nodes keyed on both IP addresses and both ports = 0
      UDP nodes keyed on both IP addresses and both ports = 0
      IP nodes keyed on both IP addresses = 0
   Statistics for Signature Events
      Number of SigEvents since reset = 0
   Statistics for Actions executed on a SigEvent
      Number of Alerts written to the IdsEventStore = 0
sensor#
```

ステップ 3　AD の統計情報を表示します。

```
sensor# show statistics anomaly-detection
Statistics for Virtual Sensor vs0
   No attack
   Detection - ON
   Learning - ON
   Next KB rotation at 10:00:01 UTC Sat Jan 18 2008
   Internal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   External Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   Illegal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
Statistics for Virtual Sensor vs1
   No attack
   Detection - ON
   Learning - ON
   Next KB rotation at 10:00:00 UTC Sat Jan 18 2008
   Internal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   External Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
   Illegal Zone
      TCP Protocol
      UDP Protocol
      Other Protocol
sensor-4240#
```

ステップ 4　認証の統計情報を表示します。

```
sensor# show statistics authentication
General
   totalAuthenticationAttempts = 128
   failedAuthenticationAttempts = 0
sensor#
```

ステップ 5　システムの拒否攻撃者の統計情報を表示します。

```
sensor# show statistics denied-attackers
```

```
Denied Attackers and hit count for each.
Denied Attackers and hit count for each.
Statistics for Virtual Sensor vs0
   Denied Attackers with percent denied and hit count for each.


   Denied Attackers with percent denied and hit count for each.


Statistics for Virtual Sensor vs1
   Denied Attackers with percent denied and hit count for each.


   Denied Attackers with percent denied and hit count for each.


sensor#
```

ステップ 6　イベント サーバの統計情報を表示します。

```
sensor# show statistics event-server
General
   openSubscriptions = 0
   blockedSubscriptions = 0
Subscriptions
sensor#
```

ステップ 7　イベント ストアの統計情報を表示します。

```
sensor# show statistics event-store
Event store statistics
   General information about the event store
      The current number of open subscriptions = 2
      The number of events lost by subscriptions and queries = 0
      The number of queries issued = 0
      The number of times the event store circular buffer has wrapped = 0
   Number of events of each type currently stored
      Debug events = 0
      Status events = 9904
      Log transaction events = 0
      Shun request events = 61
      Error events, warning = 67
      Error events, error = 83
      Error events, fatal = 0
      Alert events, informational = 60
      Alert events, low = 1
      Alert events, medium = 60
      Alert events, high = 0
sensor#
```

ステップ 8　グローバル相関の統計情報を表示します。

```
sensor# show statistics global-correlation
Network Participation:
   Counters:
      Total Connection Attempts = 0
      Total Connection Failures = 0
      Connection Failures Since Last Success = 0
   Connection History:
Updates:
   Status Of Last Update Attempt = Disabled
   Time Since Last Successful Update = never
   Counters:
      Update Failures Since Last Success = 0
      Total Update Attempts = 0
```

```
      Total Update Failures = 0
   Update Interval In Seconds = 300
   Update Server = update-manifests.ironport.com
   Update Server Address = Unknown
   Current Versions:
Warnings:
   Unlicensed = Global correlation inspection and reputation filtering have been
 disabled because the sensor is unlicensed.
   Action Required = Obtain a new license from http://www.cisco.com/go/license.
sensor#
```

ステップ 9　ホストの統計情報を表示します。

```
sensor# show statistics host
General Statistics
   Last Change To Host Config (UTC) = 16:11:05 Thu Feb 10 2008
   Command Control Port Device = FastEthernet0/0
Network Statistics
   fe0_0     Link encap:Ethernet HWaddr 00:0B:46:53:06:AA
             inet addr:10.89.149.185 Bcast:10.89.149.255 Mask:255.255.255.128
             UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
             RX packets:1001522 errors:0 dropped:0 overruns:0 frame:0
             TX packets:469569 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:57547021 (54.8 Mib) TX bytes:63832557 (60.8 MiB)
             Interrupt:9 Base address:0xf400 Memory:c0000000-c0000038
NTP Statistics
   status = Not applicable
Memory Usage
   usedBytes = 500592640
   freeBytes = 8855552
   totalBytes = 509448192
Swap Usage
   Used Bytes = 77824
   Free Bytes = 600649728

   Total Bytes = 600727552
CPU Statistics
   Usage over last 5 seconds = 0
   Usage over last minute = 1
   Usage over last 5 minutes = 1
Memory Statistics
   Memory usage (bytes) = 500498432
   Memory free (bytes) = 894976032
Auto Update Statistics
   lastDirectoryReadAttempt = 15:26:33 CDT Tue Jun 17 2008
    =   Read directory: http://tester@198.133.219.243//cisco/ciscosecure/ips/6.x/sigup/
    =   Success
   lastDownloadAttempt = 15:26:33 CDT Tue Jun 17 2008
    =   Download: http://bmarquardt@198.133.219.243//cisco/ciscosecure/ips/6.x/sigup/IPS-
sig-S338-req-E1.pkg
    =   Error: httpResponse status returned:  Unauthorized
   lastInstallAttempt = N/A
   nextAttempt = 16:26:30 CDT Tue Jun 17 2008

sensor#
```

ステップ 10　ロギング アプリケーションの統計情報を表示します。

```
sensor# show statistics logger
The number of Log interprocessor FIFO overruns = 0
The number of syslog messages received = 11
The number of <evError> events written to the event store by severity
   Fatal Severity = 0
```

```
   Error Severity = 64
   Warning Severity = 35
   TOTAL = 99
The number of log messages written to the message log by severity
   Fatal Severity = 0
   Error Severity = 64
   Warning Severity = 24
   Timing Severity = 311
   Debug Severity = 31522
   Unknown Severity = 7
   TOTAL = 31928
sensor#
```

ステップ 11　ARC の統計情報を表示します。

```
sensor# show statistics network-access
Current Configuration
   LogAllBlockEventsAndSensors = true
   EnableNvramWrite = false
   EnableAclLogging = false
   AllowSensorBlock = false
   BlockMaxEntries = 11
   MaxDeviceInterfaces = 250
   NetDevice
      Type = PIX
      IP = 10.89.150.171
      NATAddr = 0.0.0.0
      Communications = ssh-3des
   NetDevice
      Type = PIX
      IP = 10.89.150.219
      NATAddr = 0.0.0.0
      Communications = ssh-3des
   NetDevice
      Type = PIX
      IP = 10.89.150.250
      NATAddr = 0.0.0.0
      Communications = telnet
   NetDevice
      Type = Cisco
      IP = 10.89.150.158
      NATAddr = 0.0.0.0
      Communications = telnet
      BlockInterface
         InterfaceName = ethernet0/1
         InterfaceDirection = out
         InterfacePostBlock = Post_Acl_Test
      BlockInterface
         InterfaceName = ethernet0/1
         InterfaceDirection = in
         InterfacePreBlock = Pre_Acl_Test
         InterfacePostBlock = Post_Acl_Test
   NetDevice
      Type = CAT6000_VACL
      IP = 10.89.150.138
      NATAddr = 0.0.0.0
      Communications = telnet
      BlockInterface
         InterfaceName = 502
         InterfacePreBlock = Pre_Acl_Test
      BlockInterface
         InterfaceName = 507
         InterfacePostBlock = Post_Acl_Test
State
```

```
   BlockEnable = true
   NetDevice
      IP = 10.89.150.171
      AclSupport = Does not use ACLs
      Version = 6.3
      State = Active
      Firewall-type = PIX
   NetDevice
      IP = 10.89.150.219
      AclSupport = Does not use ACLs
      Version = 7.0
      State = Active
      Firewall-type = ASA
   NetDevice
      IP = 10.89.150.250
      AclSupport = Does not use ACLs
      Version = 2.2
      State = Active
      Firewall-type = FWSM
   NetDevice
      IP = 10.89.150.158
      AclSupport = uses Named ACLs
      Version = 12.2
      State = Active
   NetDevice
      IP = 10.89.150.138
      AclSupport = Uses VACLs
      Version = 8.4
      State = Active
   BlockedAddr
      Host
         IP = 22.33.4.5
         Vlan =
         ActualIp =
         BlockMinutes =
      Host
         IP = 21.21.12.12
         Vlan =
         ActualIp =
         BlockMinutes =
      Host
         IP = 122.122.33.4
         Vlan =
         ActualIp =
         BlockMinutes = 60
         MinutesRemaining = 24
      Network
         IP = 111.22.0.0
         Mask = 255.255.0.0
         BlockMinutes =
sensor#
```

ステップ 12　通知アプリケーションの統計情報を表示します。

```
sensor# show statistics notification
General
   Number of SNMP set requests = 0
   Number of SNMP get requests = 0
   Number of error traps sent = 0
   Number of alert traps sent = 0
sensor#
```

ステップ 13　OS 識別の統計情報を表示します。

```
sensor# show statistics os-identification
Statistics for Virtual Sensor vs0
   OS Identification
      Configured
      Imported
      Learned
sensor#
```

ステップ 14　SDEE サーバの統計情報を表示します。

```
sensor# show statistics sdee-server
General
   Open Subscriptions = 0
   Blocked Subscriptions = 0
   Maximum Available Subscriptions = 5
   Maximum Events Per Retrieval = 500
Subscriptions
sensor#
```

ステップ 15　トランザクション サーバの統計情報を表示します。

```
sensor# show statistics transaction-server
General
   totalControlTransactions = 35
   failedControlTransactions = 0
sensor#
```

ステップ 16　仮想センサーの統計情報を表示します。

```
sensor# show statistics virtual-sensor vs0
   Statistics for Virtual Sensor vs0
      Name of current Signature-Definition instance = sig0
      Name of current Event-Action-Rules instance = rules0
      List of interfaces monitored by this virtual sensor =
      General Statistics for this Virtual Sensor
         Number of seconds since a reset of the statistics = 1421711
         Measure of the level of resource utilization = 0
         Total packets processed since reset = 0
         Total IP packets processed since reset = 0
         Total packets that were not IP processed since reset = 0
         Total TCP packets processed since reset = 0
         Total UDP packets processed since reset = 0
         Total ICMP packets processed since reset = 0
         Total packets that were not TCP, UDP, or ICMP processed since reset =
         Total ARP packets processed since reset = 0
         Total ISL encapsulated packets processed since reset = 0
         Total 802.1q encapsulated packets processed since reset = 0
         Total packets with bad IP checksums processed since reset = 0
         Total packets with bad layer 4 checksums processed since reset = 0
         Total number of bytes processed since reset = 0
         The rate of packets per second since reset = 0
         The rate of bytes per second since reset = 0
         The average bytes per packet since reset = 0
      Denied Address Information
         Number of Active Denied Attackers = 0
         Number of Denied Attackers Inserted = 0
         Number of Denied Attacker Victim Pairs Inserted = 0
         Number of Denied Attacker Service Pairs Inserted = 0
         Number of Denied Attackers Total Hits = 0
         Number of times max-denied-attackers limited creation of new entry = 0
         Number of exec Clear commands during uptime = 0
      Denied Attackers and hit count for each.
      Denied Attackers with percent denied and hit count for each.
```

```
      The Signature Database Statistics.
         The Number of each type of node active in the system (can not be reset
            Total nodes active = 0
            TCP nodes keyed on both IP addresses and both ports = 0
            UDP nodes keyed on both IP addresses and both ports = 0
            IP nodes keyed on both IP addresses = 0
         The number of each type of node inserted since reset
            Total nodes inserted = 0
            TCP nodes keyed on both IP addresses and both ports = 0
            UDP nodes keyed on both IP addresses and both ports = 0
            IP nodes keyed on both IP addresses = 0
         The rate of nodes per second for each time since reset
            Nodes per second = 0
            TCP nodes keyed on both IP addresses and both ports per second = 0
            UDP nodes keyed on both IP addresses and both ports per second = 0
            IP nodes keyed on both IP addresses per second = 0
         The number of root nodes forced to expire because of memory constraint
            TCP nodes keyed on both IP addresses and both ports = 0
         Packets dropped because they would exceed Database insertion rate limit
s = 0
      Fragment Reassembly Unit Statistics for this Virtual Sensor
         Number of fragments currently in FRU = 0
         Number of datagrams currently in FRU = 0
         Number of fragments received since reset = 0
         Number of fragments forwarded since reset = 0
         Number of fragments dropped since last reset = 0
         Number of fragments modified since last reset = 0
         Number of complete datagrams reassembled since last reset = 0
         Fragments hitting too many fragments condition since last reset = 0
         Number of overlapping fragments since last reset = 0
         Number of Datagrams too big since last reset = 0
         Number of overwriting fragments since last reset = 0
         Number of Initial fragment missing since last reset = 0
         Fragments hitting the max partial dgrams limit since last reset = 0
         Fragments too small since last reset = 0
         Too many fragments per dgram limit since last reset = 0
         Number of datagram reassembly timeout since last reset = 0
         Too many fragments claiming to be the last since last reset = 0
         Fragments with bad fragment flags since last reset = 0
      TCP Normalizer stage statistics
         Packets Input = 0
         Packets Modified = 0
         Dropped packets from queue = 0
         Dropped packets due to deny-connection = 0
         Current Streams = 0
         Current Streams Closed = 0
         Current Streams Closing = 0
         Current Streams Embryonic = 0
         Current Streams Established = 0
         Current Streams Denied = 0
      Statistics for the TCP Stream Reassembly Unit
         Current Statistics for the TCP Stream Reassembly Unit
            TCP streams currently in the embryonic state = 0
            TCP streams currently in the established state = 0
            TCP streams currently in the closing state = 0
            TCP streams currently in the system = 0
            TCP Packets currently queued for reassembly = 0
         Cumulative Statistics for the TCP Stream Reassembly Unit since reset
            TCP streams that have been tracked since last reset = 0
            TCP streams that had a gap in the sequence jumped = 0
            TCP streams that was abandoned due to a gap in the sequence = 0
            TCP packets that arrived out of sequence order for their stream = 0
            TCP packets that arrived out of state order for their stream = 0
            The rate of TCP connections tracked per second since reset = 0
```

```
SigEvent Preliminary Stage Statistics
   Number of Alerts received = 0
   Number of Alerts Consumed by AlertInterval = 0
   Number of Alerts Consumed by Event Count = 0
   Number of FireOnce First Alerts = 0
   Number of FireOnce Intermediate Alerts = 0
   Number of Summary First Alerts = 0
   Number of Summary Intermediate Alerts = 0
   Number of Regular Summary Final Alerts = 0
   Number of Global Summary Final Alerts = 0
   Number of Active SigEventDataNodes = 0
   Number of Alerts Output for further processing = 0
SigEvent Action Override Stage Statistics
   Number of Alerts received to Action Override Processor = 0
   Number of Alerts where an override was applied = 0
   Actions Added
      deny-attacker-inline = 0
      deny-attacker-victim-pair-inline = 0
      deny-attacker-service-pair-inline = 0
      deny-connection-inline = 0
      deny-packet-inline = 0
      modify-packet-inline = 0
      log-attacker-packets = 0
      log-pair-packets = 0
      log-victim-packets = 0
      produce-alert = 0
      produce-verbose-alert = 0
      request-block-connection = 0
      request-block-host = 0
      request-snmp-trap = 0
      reset-tcp-connection = 0
      request-rate-limit = 0
SigEvent Action Filter Stage Statistics
   Number of Alerts received to Action Filter Processor = 0
   Number of Alerts where an action was filtered = 0
   Number of Filter Line matches = 0
   Number of Filter Line matches causing decreased DenyPercentage = 0
   Actions Filtered
      deny-attacker-inline = 0
      deny-attacker-victim-pair-inline = 0
      deny-attacker-service-pair-inline = 0
      deny-connection-inline = 0
      deny-packet-inline = 0
      modify-packet-inline = 0
      log-attacker-packets = 0
      log-pair-packets = 0
      log-victim-packets = 0
      produce-alert = 0
      produce-verbose-alert = 0
      request-block-connection = 0
      request-block-host = 0
      request-snmp-trap = 0
      reset-tcp-connection = 0
      request-rate-limit = 0
SigEvent Action Handling Stage Statistics.
   Number of Alerts received to Action Handling Processor = 0
   Number of Alerts where produceAlert was forced = 0
   Number of Alerts where produceAlert was off = 0
   Actions Performed
      deny-attacker-inline = 0
      deny-attacker-victim-pair-inline = 0
      deny-attacker-service-pair-inline = 0
      deny-connection-inline = 0
      deny-packet-inline = 0
```

```
            modify-packet-inline = 0
            log-attacker-packets = 0
            log-pair-packets = 0
            log-victim-packets = 0
            produce-alert = 0
            produce-verbose-alert = 0
--MORE--
```

ステップ 17　Web サーバの統計情報を表示します。

```
sensor# show statistics web-server
listener-443
   number of server session requests handled = 61
   number of server session requests rejected = 0
   total HTTP requests handled = 35
   maximum number of session objects allowed = 40
   number of idle allocated session objects = 10
   number of busy allocated session objects = 0
crypto library version = 6.0.3
sensor#
```

ステップ 18　アプリケーション、たとえば、ロギング アプリケーションの統計情報を消去します。

```
sensor# show statistics logger clear
The number of Log interprocessor FIFO overruns = 0
The number of syslog messages received = 141
The number of <evError> events written to the event store by severity
   Fatal Severity = 0
   Error Severity = 14
   Warning Severity = 142
   TOTAL = 156
The number of log messages written to the message log by severity
   Fatal Severity = 0
   Error Severity = 14
   Warning Severity = 1
   Timing Severity = 0
   Debug Severity = 0
   Unknown Severity = 28
   TOTAL = 43
```

統計情報が取得され、消去されます。

ステップ 19　統計情報が消去されたことを確認します。

```
sensor# show statistics logger
The number of Log interprocessor FIFO overruns = 0
The number of syslog messages received = 0
The number of <evError> events written to the event store by severity
   Fatal Severity = 0
   Error Severity = 0
   Warning Severity = 0
   TOTAL = 0
The number of log messages written to the message log by severity
   Fatal Severity = 0
   Error Severity = 0
   Warning Severity = 0
   Timing Severity = 0
   Debug Severity = 0
   Unknown Severity = 0
   TOTAL = 0
sensor#
```

統計情報はすべて 0 から始まります。

インターフェイス情報

show interfaces コマンドは、センシング インターフェイスおよびコマンド/コントロール インターフェイスに関する情報を収集するために有用です。ここでは、**show interfaces** コマンドについて説明します。内容は次のとおりです。

show interfaces コマンドについて

show interfaces コマンドにより次の情報を把握することができます。

- インターフェイスがアップ状態かダウン状態かどうか
- パケットが監視されているかどうか、どのインターフェイスでそれが行われるかどうか
- SensorApp によってパケットがドロップされているかどうか
- パケット ドロップを生じるようなエラーがインターフェイスによってレポートされているかどうか

show interfaces コマンドは、すべてのシステム インターフェイスの統計情報を表示します。または、個々のコマンドを使用して、コマンド/コントロール インターフェイス（**show interfaces** *command_control_interface_name*）や検知インターフェイス（**show interfaces** *interface_name*）の統計情報を表示できます。

interfaces コマンドの出力

次に、**show interfaces** コマンドの出力例を示します。

```
sensor# show interfaces
Interface Statistics
   Total Packets Received = 0
   Total Bytes Received = 0
   Missed Packet Percentage = 0
   Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
```

```
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface GigabitEthernet0/0
   Media Type = TX
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 2211296
   Total Bytes Received = 157577635
   Total Multicast Packets Received = 20
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 239723
   Total Bytes Transmitted = 107213390
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
sensor#
```

イベント情報

show events コマンドを使用すれば、SensorApp によって生成されたアラートおよびアプリケーションによって生成されたエラーを表示できます。ここでは、**show events** コマンドについて説明します。内容は次のとおりです。

センサーのイベント

5 種類のイベントがあります。

- evAlert：侵入検知アラート
- evError：アプリケーション エラー
- evStatus：ステータスの変更（IP ログの作成など）
- evLogTransaction：各センサー アプリケーションによって処理されるコントロール トランザクションのレコード
- evShunRqst：ブロックの要求

イベントは、新しいイベントによって上書きされるまでイベント ストアに残ります。

show events コマンドについて

show events コマンドは、イベント ビューアまたは Security Monitor でイベントを確認できないといった、イベント キャプチャの問題をトラブルシューティングする際に役立ちます。**show events** コマンドを使用すれば、イベントが生成されていることを確認するためにセンサー上でどのイベントが生成されているかを特定し、モニタ側に障害があるかどうかを判定することができます。

イベント ストアからすべてのイベントをクリアするには、**clear events** コマンドを使用します。

ここで、**show events** コマンドのパラメータを示します。

```
sensor# show events
<cr>
alert          Display local system alerts.
error          Display error events.
hh:mm[:ss]     Display start time.
log            Display log events.
nac            Display NAC shun events.
past           Display events starting in the past specified time.
status         Display status events.
|              Output modifiers.
```

イベントの表示

イベント ストアからイベントを表示するには、**show events** [{**alert** [informational] [low] [medium] [high] [**include-traits** ***traits***] [**exclude-traits** ***traits***] [**min-threat-rating** *min-rr*] [**max-threat-rating** *max-rr*] | **error** [warning] [error] [fatal] | **NAC** | **status**}] [*hh:mm:ss* [*month day* [*year*]] | **past** *hh:mm:ss*] コマンドを使用します。

イベントは、開始時刻からのイベントが表示されます。開始時刻を指定しない場合、イベントは現在の時刻から表示されます。イベント タイプを指定しない場合、すべてのイベントが表示されます。

（注） イベントは、ライブ フィードとして表示されます。要求をキャンセルするには、Ctrl キーを押した状態で C キーを押します。

次のオプションが適用されます。

- **alert**：アラートを表示します。侵入攻撃が進行中であるか試みられたことを示す可能性がある、ある種の疑わしいアクティビティを通知します。アラート イベントは、ネットワーク アクティビティによってシグニチャがトリガーされるたびに、分析エンジンによって生成されます。レベルが選択されていない場合（情報、低、中、または高）、すべてのアラート イベントが表示されます。
- **include-traits**: 指定された特性を持つアラートを表示します。
- **exclude-traits**：指定された特性を持つアラートを表示しません。
- **traits**：十進数で表される trait ビットの位置（0 ～ 15）。
- **min-threat-rating**：この値以上の脅威レーティングを持つイベントを表示します。デフォルトは 0 です。有効な範囲は 0 ～ 100 です。
- **max-threat-rating**：この値以下の脅威レーティングを持つイベントを表示します。デフォルトは 100 です。有効な範囲は 0 ～ 100 です。
- **error**：エラー イベントを表示します。エラー イベントは、エラー状態が検出されたときに、サービスによって生成されます。レベルが選択されていない場合（警告、エラー、または重大）、すべてのエラー イベントが表示されます。
- **NAC**：ARC（ブロック）要求を表示します。

  （注） ARC は、NAC と呼ばれていました。この名前変更は、Cisco IPS 7.0 の IDM、IME、および CLI を通して完全に実装されていません。

- **status**：ステータス イベントを表示します。

- **past**：指定された過去の時間、分、および秒から始まったイベントを表示します。
- *hh:mm:ss*：表示を開始する過去の時間、分、および秒。

（注）　**show events** コマンドは、指定されたイベントが取得可能になるまで、イベントを表示し続けます。終了するには、Ctrl キーを押した状態で C キーを押します。

イベント ストアからイベントを表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　今から始まるすべてのイベントを表示します。

```
sensor#@ show events
evError: eventId=1041472274774840147 severity=warning vendor=Cisco
  originator:
    hostId: sensor2
    appName: cidwebserver
    appInstanceId: 12075
  time: 2008/01/07 04:41:45 2008/01/07 04:41:45 UTC
  errorMessage: name=errWarning received fatal alert: certificate_unknown

evError: eventId=1041472274774840148 severity=error vendor=Cisco
  originator:
    hostId: sensor2
    appName: cidwebserver
    appInstanceId: 351
  time: 2008/01/07 04:41:45 2008/01/07 04:41:45 UTC
  errorMessage: name=errTransport WebSession::sessionTask(6) TLS connection exce
ption: handshake incomplete.
```

Ctrl キーを押した状態で C キーを押すまで、すべてのイベントが表示され続けます。

ステップ 3　2008 年 2 月 9 日の 10:00 a.m. から始まるブロック要求を表示します。

```
sensor# show events NAC 10:00:00 Feb 9 2008
evShunRqst: eventId=1106837332219222281 vendor=Cisco
  originator:
    deviceName: Sensor1
    appName: NetworkAccessControllerApp
    appInstance: 654
  time: 2008/02/09 10:33:31 2008/08/09 13:13:31
  shunInfo:
    host: connectionShun=false
      srcAddr: 11.0.0.1
      destAddr:
      srcPort:
      destPort:
      protocol: numericType=0 other
    timeoutMinutes: 40
  evAlertRef: hostId=esendHost 123456789012345678
sensor#
```

ステップ 4　2008 年 2 月 9 日の 10:00 a.m. から始まる警告レベルのエラーを表示します。

```
sensor# show events error warning 10:00:00 Feb 9 2008
evError: eventId=1041472274774840197 severity=warning vendor=Cisco
  originator:
    hostId: sensor
    appName: cidwebserver
    appInstanceId: 12160
  time: 2008/01/07 04:49:25 2008/01/07 04:49:25 UTC
```

```
  errorMessage: name=errWarning received fatal alert: certificate_unknown
```

ステップ 5　45 秒前からのアラートを表示します。

```
sensor# show events alert past 00:00:45

evIdsAlert: eventId=1109695939102805307 severity=medium vendor=Cisco
  originator:
    hostId: sensor
    appName: sensorApp
    appInstanceId: 367
  time: 2008/03/02 14:15:59 2008/03/02 14:15:59 UTC
  signature: description=Nachi Worm ICMP Echo Request id=2156 version=S54
    subsigId: 0
    sigDetails: Nachi ICMP
  interfaceGroup:
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 10.89.228.202
    target:
      addr: locality=OUT 10.89.150.185
  riskRatingValue: 70
  interface: fe0_1
  protocol: icmp


evIdsAlert: eventId=1109695939102805308 severity=medium vendor=Cisco
  originator:
--MORE--
```

ステップ 6　30 秒前に始まったイベントを表示します。

```
sensor# show events past 00:00:30
evStatus: eventId=1041526834774829055 vendor=Cisco
  originator:
    hostId: sensor
    appName: mainApp
    appInstanceId: 2215
  time: 2008/01/08 02:41:00 2008/01/08 02:41:00 UTC
  controlTransaction: command=getVersion successful=true
    description: Control transaction response.
    requestor:
      user: cids
      application:
        hostId: 64.101.182.101
        appName: -cidcli
        appInstanceId: 2316


evStatus: eventId=1041526834774829056 vendor=Cisco
  originator:
    hostId: sensor
    appName: login(pam_unix)
    appInstanceId: 2315
  time: 2008/01/08 02:41:00 2008/01/08 02:41:00 UTC
  syslogMessage:
    description: session opened for user cisco by cisco(uid=0)
```

イベントのクリア

イベント ストアをクリアするには、**clear events** コマンドを使用します。

イベント ストアからイベントをクリアするには、次の手順を実行します。

ステップ 1　管理者権限を持つアカウントを使用して CLI にログインします。

ステップ 2　イベント ストアをクリアします。

```
sensor# clear events
Warning: Executing this command will remove all events currently stored in the event
store.
Continue with clear? []:
```

ステップ 3　**yes** と入力してイベントをクリアします。

cidDump スクリプト

IDM、IME または CLI へのアクセス権がない場合も、root としてログインし、/usr/cids/idsRoot/bin/cidDump を実行することにより、サービス アカウントから基本的なスクリプトである cidDump を実行できます。cidDump ファイルのパスは、/usr/cids/idsRoot/htdocs/private/cidDump.html です。

cidDump は大量の情報を取り込むためのスクリプトです。この情報には、IPS プロセス リスト、ログ ファイル、OS 情報、ディレクトリ リスト、パッケージ情報、コンフィギュレーション ファイルなどがあります。

cidDump スクリプトを実行するには、次の手順を実行します。

ステップ 1　センサーのサービス アカウントにログインします。

ステップ 2　サービス アカウント パスワードを使用して **root** に **su** します。

ステップ 3　次のコマンドを入力します。

```
/usr/cids/idsRoot/bin/cidDump
```

ステップ 4　次のコマンドを入力して、生成される /usr/cids/idsRoot/log/cidDump.html ファイルを圧縮します。

```
gzip /usr/cids/idsRoot/log/cidDump.html
```

ステップ 5　問題がある場合は、生成された HTML ファイルを TAC または IPS の開発者に送信します。

詳細情報

ファイルを Cisco FTP サイトに置く手順については、「Cisco FTP サイトへのファイルのアップロードおよびそのサイト上のファイルへのアクセス」（P.C-97）を参照してください。

Cisco FTP サイトへのファイルのアップロードおよびそのサイト上のファイルへのアクセス

大きなファイル（たとえば、cidDump.html、**show tech-support** コマンドの出力、コア ファイル）を ftp-sj サーバにアップロードできます。

Cisco FTP サイトへのファイルのアップロードおよび Cisco FTP サイトのファイルへのアクセスを行うには、次の手順に従います。

ステップ 1　ftp-sj.cisco.com に匿名でログインします。

ステップ 2　/incoming というディレクトリに変更します。

ステップ 3　**put** コマンドを使用してファイルをアップロードします。必ずバイナリ転送タイプを使用します。

ステップ 4　アップロードされたファイルにアクセスするには、ECS でサポートされたホストにログインします。

ステップ 5　/auto/ftp/incoming ディレクトリに変更します。

APPENDIX D

Cisco IPS 7.1 で使用されるオープン ソース ライセンス ファイル

発行日：2010 年 11 月 12 日

このドキュメントには、Cisco IPS 7.1 で使用されるオープン ソース ソフトウェアのライセンスおよび通知を記載します。このドキュメントに記載される無料/オープン ソース ソフトウェア（GNU Lesser/General Public License など、適切な無料/オープン ソース ライセンスに基づいて認められるソフトウェア）について質問がある場合やソース コードのコピーを入手したい場合には、external-opensource-requests@cisco.com 宛てにお問い合わせください。

内容

この付録には、Cisco IPS 7.1 で使用されるオープン ソース ソフトウェアの一覧を示します。構成は次のとおりです。

bash 3.2

Available under license:

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The “Program”, below, refers to any such program or work, and a “work based on the Program” means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term “modification”.) Each licensee is addressed as “you”.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the

user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO

THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than 'show w' and 'show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a “copyright disclaimer” for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

'Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

busybox 1.13.1

Available under license:

A note on GPL versions

BusyBox is distributed under version 2 of the General Public License (included in its entirety, below). Version 2 is the only version of this license which this version of BusyBox (or modified versions derived from this one) may be distributed under.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for

this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights.

These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software. Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any

associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is

void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

<one line to give the program’s name and a brief idea of what it does. Copyright (C) <year

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type ‘show w’.

This is free software, and you are welcome to redistribute it under certain conditions; type ‘show c’ for details.

The hypothetical commands ‘show w’ and ‘show c’ should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than ‘show w’ and ‘show c’; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a “copyright disclaimer” for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program ‘Gnomovision’ (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

The code and graphics on this website (and it’s mirror sites, if any) are

Copyright (c) 1999-2004 by Erik Andersen. All rights reserved.

Copyright (c) 2005-2006 Rob Landley.

Documents on this Web site including their graphical elements, design, and layout are protected by trade dress and other laws and MAY BE COPIED OR IMITATED IN WHOLE OR IN PART. THIS WEBSITE IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE WEBSITE TO THE EXTENT PERMITTED BY APPLICABLE LAW.

SHOULD THIS WEBSITE PROVE DEFECTIVE, YOU MAY ASSUME THAT SOMEONE MIGHT GET AROUND TO SERVICING, REPAIRING OR CORRECTING IT SOMETIME WHEN THEY HAVE NOTHING BETTER TO DO. REGARDLESS, YOU GET TO KEEP BOTH PIECES.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THIS WEBSITE AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THIS WEBSITE (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR LOSS OF HAIR, LOSS OF LIFE, LOSS OF MEMORY, LOSS OF YOUR CARKEYS, MISPLACEMENT OF YOUR PAYCHECK, OR COMMANDER DATA BEING RENDERED UNABLE TO ASSIST THE STARFLEET OFFICERS ABORD THE STARSHIP ENTERPRISE TO RECALIBRATE THE MAIN DEFLECTOR ARRAY, LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE WEBSITE TO OPERATE WITH YOUR WEBBROWSER), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

You have been warned.

You can contact the webmaster at <rob@landley.net of problem with this.

bzip2 applet in busybox is based on lightly-modified source of bzip2 version 1.0.4. bzip2 source is distributed under the following conditions (copied verbatim from LICENSE file).

This program, “bzip2”, the associated library “libbzip2”, and all documentation, are copyright (C) 1996-2006 Julian R Seward. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

3. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

4. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR “AS IS” AND ANY EXPRESSOR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Julian Seward, Cambridge, UK.

jseward@bzip.org

bzip2/libbzip2 version 1.0.4 of 20 December 2006

cracklib 2.8.12

Available under license:

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program

is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program).

Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

<one line to give the program’s name and a brief idea of what it does. Copyright (C) <year

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type ‘show w’.

This is free software, and you are welcome to redistribute it under certain conditions; type ‘show c’ for details.

The hypothetical commands ‘show w’ and ‘show c’ should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than ‘show w’ and ‘show c’; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a “copyright disclaimer” for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

‘Gnomovision’ (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

curl 7.18.2 1

Available under license:

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2008, Daniel Stenberg, <daniel@haxx.se

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

Copyright (c) 1995, 1996, 1997, 1998, 1999 Kungliga Tekniska Hogskolan

(Royal Institute of Technology, Stockholm, Sweden).

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the Institute nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE INSTITUTE AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE INSTITUTE OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

diffutils 2.8.1

Available under license:

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation’s software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO

THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

<one line to give the program’s name and a brief idea of what it does.

Copyright (C) <year

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type ‘show w’.

This is free software, and you are welcome to redistribute it under certain conditions; type ‘show c’ for details.

The hypothetical commands ‘show w’ and ‘show c’ should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than ‘show w’ and ‘show c’; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a “copyright disclaimer” for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

‘Gnomovision’ (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

e2fsprogs 1.39

Available under license:

This package, the EXT2 filesystem utilities, are made available under the GNU Public License, with the exception of the lib/uuid directory which is made available under a BSD-style license. Please seelib/uuid/COPYING for more details for the license for the files comprising the libuuid library.

However, I request that if the version string in the file version.h contains the string “pre-”, or “WIP” that this version of e2fsprogs be distributed in source form only. Please feel free to give a copy of the e2fsck binary to help a friend recover his or her filesystem, as the need arises. However, “pre” or “WIP” indicates that this release is under development, and available for ALPHA testing. So for your protection as much as mine, I’d prefer that it not appear in a some distribution --- especially not a CD-ROM distribution!

The most recent officially distributed version can be found at http://e2fsprogs.sourceforge.net. If you need to make a distribution, that’s the one you should use. If there is some reason why you’d like a more recent version that is still in ALPHA testing for your distribution, please contact me (tytso@mit.edu), and we will very likely be able to work out something that will work for all concerned.

The release schedules for this package are flexible, if you give me enough lead time.

Theodore Ts’o

15-Mar-2003

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation’s software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License.

However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO

THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

<one line to give the program’s name and a brief idea of what it does.

Copyright (C) <year

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type ‘show w’.

This is free software, and you are welcome to redistribute it under certain conditions; type ‘show c’ for details.

The hypothetical commands ‘show w’ and ‘show c’ should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than ‘show w’ and ‘show c’; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a “copyright disclaimer” for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

‘Gnomovision’ (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

Expat XML parser 2.0.1

Available under license:

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

expect 5.4.3

Available under license:

Written by: Don Libes, NIST, 2/6/90

Design and implementation of this program was paid for by U.S. tax dollars. Therefore it is public domain. However, the author and NIST would appreciate credit if this program or parts of it are used.

glibc 2.9

Available under license:

GNU GENERAL PUBLIC LICENSE

This file contains the copying permission notices for various files in the GNU C Library distribution that have copyright owners other than the Free Software Foundation. These notices all require that a copy of the notice be included in the accompanying documentation and be distributed with binary distributions of the code, so be sure to include this file along with any binary distributions derived from the GNU C Library.

All code incorporated from 4.4 BSD is distributed under the following license:

Copyright (C) 1991 Regents of the University of California.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. [This condition was removed.]

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The DNS resolver code, taken from BIND 4.9.5, is copyrighted both by UC Berkeley and by Digital Equipment Corporation. The DEC portions are under the following license:

Portions Copyright (C) 1993 by Digital Equipment Corporation.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies, and that the name of Digital Equipment Corporation not be used in advertising or publicity pertaining to distribution of the document or software without specific, written prior permission.

THE SOFTWARE IS PROVIDED “AS IS” AND DIGITAL EQUIPMENT CORP. DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL DIGITAL EQUIPMENT CORPORATION BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

The Sun RPC support (from rpcsrc-4.0) is covered by the following license:

Copyright (C) 1984, Sun Microsystems, Inc.

Sun RPC is a product of Sun Microsystems, Inc. and is provided for unrestricted use provided that this legend is included on all tape media and as a part of the software program in whole or part. Users may copy or modify Sun RPC without charge, but are not authorized to license or distribute it to anyone else except as part of a product or program developed by the user.

SUN RPC IS PROVIDED AS IS WITH NO WARRANTIES OF ANY KIND INCLUDING THE WARRANTIES OF DESIGN, MERCHANTIBILITY AND FITNESS FOR A PARTICULAR PURPOSE, OR ARISING FROM A COURSE OF DEALING, USAGE OR TRADE PRACTICE.

Sun RPC is provided with no support and without any obligation on the part of Sun Microsystems, Inc. to assist in its use, correction, modification or enhancement.

SUN MICROSYSTEMS, INC. SHALL HAVE NO LIABILITY WITH RESPECT TO THE INFRINGEMENT OF COPYRIGHTS, TRADE SECRETS OR ANY PATENTS BY SUN RPC OR ANY PART THEREOF.

In no event will Sun Microsystems, Inc. be liable for any lost revenue or profits or other special, indirect and consequential damages, even if Sun has been advised of the possibility of such damages.

The following CMU license covers some of the support code for Mach, derived from Mach 3.0:

Mach Operating System

Copyright (C) 1991,1990,1989 Carnegie Mellon University

All Rights Reserved.

Permission to use, copy, modify and distribute this software and its documentation is hereby granted, provided that both the copyright notice and this permission notice appear in all copies of the software, derivative works or modified versions, and any portions thereof, and that both notices appear in supporting documentation.

CARNEGIE MELLON ALLOWS FREE USE OF THIS SOFTWARE IN ITS “AS IS” CONDITION. CARNEGIE MELLON DISCLAIMS ANY LIABILITY OF ANY KIND FOR ANY DAMAGES WHATSOEVER RESULTING FROM THE USE OF THIS SOFTWARE.

Carnegie Mellon requests users of this software to return to

Software Distribution Coordinator

School of Computer Science

Carnegie Mellon University

Pittsburgh PA 15213-3890

or Software.Distribution@CS.CMU.EDU any improvements or extensions that they make and grant Carnegie Mellon the rights to redistribute these changes.

The file if_ppp.h is under the following CMU license:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY CARNEGIE MELLON UNIVERSITY AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE UNIVERSITY OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The following license covers the files from Intel’s “Highly Optimized Mathematical Functions for Itanium” collection:

Intel License Agreement

Copyright (c) 2000, Intel Corporation

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- The name of Intel Corporation may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL INTEL OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The files inet/getnameinfo.c and sysdeps/posix/getaddrinfo.c are copyright (C) by Craig Metz and are distributed under the following license:

The Inner Net License, Version 2.00

The author(s) grant permission for redistribution and use in source and binary forms, with or without modification, of the software and documentation provided that the following conditions are met:

0. If you receive a version of the software that is specifically labelled as not being for redistribution (check the version message and/or README), you are not permitted to redistribute that version of the software in any way or form.

1. All terms of the all other applicable copyrights and licenses must be followed.

2. Redistributions of source code must retain the authors’ copyright notice(s), this list of conditions, and the following disclaimer.

3. Redistributions in binary form must reproduce the authors’ copyright notice(s), this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

4. [The copyright holder has authorized the removal of this clause.]

5. Neither the name(s) of the author(s) nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY ITS AUTHORS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT

LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

If these license terms cause you a real problem, contact the author. /

GNU LESSER GENERAL PUBLIC LICENSE

Copyright 1992, 1993, 1994, 1997 Henry Spencer. All rights reserved.

gnupg 1.4.5

Available under license:

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin St., Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights.

These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The “Program”, below, refers to any such program or work, and a “work based on the Program” means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term “modification”.) Each licensee is addressed as “you”.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program’s source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License.

However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

<one line to give the program’s name and a brief idea of what it does.

Copyright (C) <year

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin St., Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type ‘show w’.

This is free software, and you are welcome to redistribute it under certain conditions; type ‘show c’ for details.

The hypothetical commands ‘show w’ and ‘show c’ should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than ‘show w’ and ‘show c’; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a “copyright disclaimer” for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

‘Gnomovision’ (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

hotplug 2004_03_29

Available under license:

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The “Program”, below, refers to any such program or work, and a “work based on the Program” means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term “modification”.) Each licensee is addressed as “you”.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least

the “copyright” line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type 'show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type 'show c' for details.

The hypothetical commands 'show w' and 'show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than 'show w' and 'show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a “copyright disclaimer” for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program 'Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

i2c-tools 3.0.2

Available under license:

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation’s software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all. The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License.

However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

<one line to give the program’s name and a brief idea of what it does.

Copyright (C) <year

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type ‘show w’.

This is free software, and you are welcome to redistribute it under certain conditions; type ‘show c’ for details.

The hypothetical commands ‘show w’ and ‘show c’ should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than ‘show w’ and ‘show c’; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a “copyright disclaimer” for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

‘Gnomovision’ (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

ipmiutil 2.3.3

Available under license:

The BSD 2.0 License

Copyright (c) 2002-2008, Intel Corporation

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

a. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

b. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

c. Neither the name of Intel Corporation nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

iptables 1.4.1

Available under license:

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

675 Mass Ave, Cambridge, MA 02139, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License.

However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances. It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the

integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Appendix: How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

<one line to give the program’s name and a brief idea of what it does.

Copyright (C) 19yy <name of author

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19yy name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type ‘show w’.

This is free software, and you are welcome to redistribute it under certain conditions; type ‘show c’ for details.

The hypothetical commands ‘show w’ and ‘show c’ should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than ‘show w’ and ‘show c’; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a “copyright disclaimer” for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

‘Gnomovision’ (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

kernel 2.6.29.1

Available under license:

NOTE! This copyright does *not* cover user programs that use kernel services by normal system calls - this is merely considered normal use of the kernel, and does *not* fall under the heading of “derived work”. Also note that the GPL below is copyrighted by the Free Software Foundation, but the instance of code that it refers to (the Linux kernel) is copyrighted by me and others who actually wrote it.

Also note that the only valid version of the GPL as far as the kernel is concerned is _this_ particular version of the license (i.e. v2, not v2.2 or v3.x or whatever), unless explicitly otherwise stated.

Linus Torvalds

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most

of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License.

However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

<one line to give the program’s name and a brief idea of what it does.

Copyright (C) <year

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type ‘show w’.

This is free software, and you are welcome to redistribute it under certain conditions; type ‘show c’ for details.

The hypothetical commands ‘show w’ and ‘show c’ should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than ‘show w’ and ‘show c’; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a “copyright disclaimer” for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

‘Gnomovision’ (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

Copyright (c) 2003-2006 QLogic Corporation

QLogic Linux Networking HBA Driver

This program includes a device driver for Linux 2.6 that may be distributed with QLogic hardware specific firmware binary file.

You may modify and redistribute the device driver code under the GNU General Public License as published by the Free Software Foundation (version 2 or a later version).

You may redistribute the hardware specific firmware binary file under the following terms:

1. Redistribution of source code (only if applicable), must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistribution in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of QLogic Corporation may not be used to endorse or promote products derived from this software without specific prior written permission

REGARDLESS OF WHAT LICENSING MECHANISM IS USED OR APPLICABLE, THIS PROGRAM IS PROVIDED BY QLOGIC CORPORATION “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

USER ACKNOWLEDGES AND AGREES THAT USE OF THIS PROGRAM WILL NOT CREATE OR GIVE GROUNDS FOR A LICENSE BY IMPLICATION, ESTOPPEL, OR OTHERWISE IN ANY INTELLECTUAL PROPERTY RIGHTS (PATENT, COPYRIGHT, TRADE SECRET, MASK WORK, OR OTHER PROPRIETARY RIGHT) EMBODIED IN ANY OTHER QLOGIC HARDWARE OR SOFTWARE EITHER SOLELY OR IN COMBINATION WITH THIS PROGRAM.

Copyright (c) 2003-2008 QLogic Corporation

QLogic Linux Networking HBA Driver

This program includes a device driver for Linux 2.6 that may be distributed with QLogic hardware specific firmware binary file.

You may modify and redistribute the device driver code under the GNU General Public License as published by the Free Software Foundation (version 2 or a later version).

You may redistribute the hardware specific firmware binary file under the following terms:

1. Redistribution of source code (only if applicable), must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistribution in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of QLogic Corporation may not be used to endorse or promote products derived from this software without specific prior written permission

REGARDLESS OF WHAT LICENSING MECHANISM IS USED OR APPLICABLE, THIS PROGRAM IS PROVIDED BY QLOGIC CORPORATION “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

USER ACKNOWLEDGES AND AGREES THAT USE OF THIS PROGRAM WILL NOT CREATE OR GIVE GROUNDS FOR A LICENSE BY IMPLICATION, ESTOPPEL, OR OTHERWISE IN ANY INTELLECTUAL PROPERTY RIGHTS (PATENT, COPYRIGHT, TRADE SECRET, MASK WORK, OR OTHER PROPRIETARY RIGHT) EMBODIED IN ANY OTHER QLOGIC HARDWARE OR SOFTWARE EITHER SOLELY OR IN COMBINATION WITH THIS PROGRAM.

FlashPoint Driver Developer’s Kit

Version 1.0

Copyright 1995-1996 by Mylex Corporation

All Rights Reserved

This program is free software; you may redistribute and/or modify it under the terms of either:

a) the GNU General Public License as published by the Free Software Foundation; either version 2, or (at your option) any later version,

or

b) the “BSD-style License” included below.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY, without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See either the GNU General Public License or the BSD-style License below for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

The BSD-style License is as follows:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain this LICENSE.FlashPoint file, without modification, this list of conditions, and the following disclaimer. The following copyright notice must appear immediately at the beginning of all source files:

Copyright 1995-1996 by Mylex Corporation. All Rights Reserved

This file is available under both the GNU General Public License and a BSD-style copyright; see LICENSE.FlashPoint for details.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of Mylex Corporation may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY MYLEX CORP. “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 2003-2005 QLogic Corporation

QLogic Linux Fibre Channel HBA Driver

This program includes a device driver for Linux 2.6 that may be distributed with QLogic hardware specific firmware binary file.

You may modify and redistribute the device driver code under the GNU General Public License as published by the Free Software Foundation (version 2 or a later version).

You may redistribute the hardware specific firmware binary file under the following terms:

1. Redistribution of source code (only if applicable), must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistribution in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of QLogic Corporation may not be used to endorse or promote products derived from this software without specific prior written permission

REGARDLESS OF WHAT LICENSING MECHANISM IS USED OR APPLICABLE, THIS PROGRAM IS PROVIDED BY QLOGIC CORPORATION “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

USER ACKNOWLEDGES AND AGREES THAT USE OF THIS PROGRAM WILL NOT CREATE OR GIVE GROUNDS FOR A LICENSE BY IMPLICATION, ESTOPPEL, OR OTHERWISE IN ANY INTELLECTUAL PROPERTY RIGHTS (PATENT, COPYRIGHT, TRADE SECRET, MASK WORK, OR OTHER PROPRIETARY RIGHT) EMBODIED IN ANY OTHER QLOGIC HARDWARE OR SOFTWARE EITHER SOLELY OR IN COMBINATION WITH THIS PROGRAM.

GNU LIBRARY GENERAL PUBLIC LICENSE

nicstar.c v0.22 Jawaid Bazyar (bazyar@hypermall.com)

nicstar.c, M. Welsh (matt.welsh@cl.cam.ac.uk)

Hacked October, 1997 by Jawaid Bazyar, Interlink Advertising Services Inc.

http://www.hypermall.com/

10/1/97 - commented out CFG_PHYIE bit - we don’t care when the PHY interrupts us (except possibly for removal/insertion of the cable?)

10/4/97 - began heavy inline documentation of the code. Corrected typos and spelling mistakes.

10/5/97 - added code to handle PHY interrupts, disable PHY on loss of link, and correctly re-enable PHY when link is re-established. (put back CFG_PHYIE)

Modified to work with the IDT7721 nicstar -- AAL5 (tested) only.

R. D. Rechenmacher <ron@fnal.gov

Linux driver for the IDT77201 NICStAR PCI ATM controller.

PHY component is expected to be 155 Mbps S/UNI-Lite or IDT 77155; see init_nicstar() for PHY initialization to change this. This driver expects the Linux ATM stack to support scatter-gather lists (skb-Implementing minimal-copy of received data:

IDT always receives data into a small buffer, then large buffers as needed. This means that data must always be copied to create the linear buffer needed by most non-ATM protocol stacks (e.g. IP)

Fix is simple: make large buffers large enough to hold entire SDU, and leave <small_buffer_data copy small buffer contents to head of large buffer.

Trick is to avoid fragmenting Linux, due to need for a lot of large buffers. This is done by 2 things:

1) skb-combined, allow nicstar_free_rx_skb to be called to recycle large data buffers

2) skb_clone of received buffers

See nicstar_free_rx_skb and linearize_buffer for implementation details.

Copyright (c) 1996 University of Cambridge Computer Laboratory

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA. M. Welsh, 6 July 1996

linux-2.6.29.1/drivers/net/LICENSE.SRC

Code in this directory written at the IDA Supercomputing Research Center carries the following copyright and license.

Copyright 1993 United States Government as represented by the Director, National Security Agency. This software may be used and distributed according to the terms of the GNU General Public License, incorporated herein by reference.

In addition to the disclaimers in the GPL, SRC expressly disclaims any and all warranties, expressed or implied, concerning the enclosed software.

This software was developed at SRC for use in internal research, and the intent in sharing this software is to promote the productive interchange of ideas throughout the research community. All software is furnished on an “as-is” basis. No further updates to this software should be expected. Although updates may occur, no commitment exists.

linux-2.6.29.1/drivers/net/wireless/libertas/LICENSE

Copyright (c) 2003-2006, Marvell International Ltd.

All Rights Reserved

This program is free software; you can redistribute it and/or modify it under the terms of version 2 of the GNU General Public License as published by the Free Software Foundation.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA.

The files in this directory and elsewhere which refer to this LICENCE file are part of JFFS2, the Journalling Flash File System v2.

Copyright © 2001-2007 Red Hat, Inc. and others

JFFS2 is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 or (at your option) any later version.

JFFS2 is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with JFFS2; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA.

As a special exception, if other files instantiate templates or use macros or inline functions from these files, or you compile these files and link them with other works to produce a work based on these files, these files do not by themselves cause the resulting work to be covered by the GNU General Public License. However the source code for these files must still be made available in accordance with section (3) of the GNU General Public License.

This exception does not invalidate any other reasons why a work based on this file might be covered by the GNU General Public License.

libpcap 0.9.8

Available under license:

License: BSD

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

libtecla 1.4.1

Available under license:

Copyright (c) 2000, 2001 by Martin C. Shepherd.

All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

Linux-Pam 1.0.1

Available under license:

Unless otherwise *explicitly* stated the following text describes the licensed conditions under which the contents of this libpamc release may be distributed:

Redistribution and use in source and binary forms of libpamc, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain any existing copyright notice, and this entire permission notice in its entirety, including the disclaimer of warranties.

2. Redistributions in binary form must reproduce all prior and current copyright notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The name of any author may not be used to endorse or promote products derived from this software without their specific prior written permission.

ALTERNATIVELY, this product may be distributed under the terms of the GNU Library General Public License (LGPL), in which case the provisions of the GNU LGPL are required INSTEAD OF the above restrictions. (This clause is necessary due to a potential conflict between the GNU LGPL and the restrictions contained in a BSD-style copyright.)

THIS SOFTWARE IS PROVIDED '"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR(S) BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

lm_sensors 3.0.2

Available under license:

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.,

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as

separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License.

However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

<one line to give the program’s name and a brief idea of what it does.

Copyright (C) <year

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type ‘show w’.

This is free software, and you are welcome to redistribute it under certain conditions; type ‘show c’ for details.

The hypothetical commands ‘show w’ and ‘show c’ should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than ‘show w’ and ‘show c’; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a “copyright disclaimer” for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

‘Gnomovision’ (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

module-init-tools 3.2.2 1.0.0.0900084

Available under license:

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights.

These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The “Program”, below, refers to any such program or work, and a “work based on the Program” means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term “modification”.) Each licensee is addressed as “you”.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program’s source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License.

However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

<one line to give the program’s name and a brief idea of what it does.

Copyright (C) <year

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w’.

This is free software, and you are welcome to redistribute it under certain conditions; type `show c’ for details.

The hypothetical commands `show w’ and `show c’ should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w’ and `show c’; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a “copyright disclaimer” for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

‘Gnomovision’ (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

Ncurses 5.6

Available under license:

Copyright (c) 1998-2004,2006 Free Software Foundation, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, distribute with modifications, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name(s) of the above copyright holders shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization.

net-snmp 5.4.1

Available under license:

Various copyrights apply to this package, listed in various separate parts below. Please make sure that you read all the parts.

Part 1: CMU/UCD copyright notice: (BSD like)

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Part 2: Networks Associates Technology, Inc. copyright notice (BSD)

Copyright (c) 2001-2003, Networks Associates Technology, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Networks Associates Technology, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 3: Cambridge Broadband Ltd. copyright notice (BSD)

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 4: Sun Microsystems, Inc. copyright notice (BSD)

Copyright 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 5: Sparta, Inc. copyright notice (BSD)

Copyright (c) 2003-2006, Sparta, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Sparta, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 6: Cisco/BUPTNIC copyright notice (BSD)

Copyright (c) 2004, Cisco, Inc. and Information Network

Center of Beijing University of Posts and Telecommunications.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Cisco, Inc., Beijing University of Posts and Telecommunications, nor the names of their contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Part 7: Fabasoft R&D Software GmbH & Co KG copyright notice (BSD)

Copyright (c) Fabasoft R&D Software GmbH & Co KG, 2003

oss@fabasoft.com

Author: Bernhard Penz <bernhard.penz@fabasoft.com

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- The name of Fabasoft R&D Software GmbH & Co KG or any of its subsidiaries, brand or product names may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NTP 4.2.4p5

Available under license:

This file is automatically generated from html/copyright.html

Copyright Notice

jpg “Clone me,” says Dolly sheepishly

Last update: 20:31 UTC Saturday, January 06, 2007

The following copyright notice applies to all files collectively called the Network Time Protocol Version 4 Distribution. Unless specifically declared otherwise in an individual file, this notice applies as if the text was explicitly included in the file.

Copyright (c) David L. Mills 1992-2008

Permission to use, copy, modify, and distribute this software and its documentation for any purpose with or without fee is hereby granted, provided that the above copyright notice appears in all copies and that both the copyright notice and this permission notice appear in supporting documentation, and that the name University of Delaware not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission. The University of Delaware makes no representations about the suitability this software for any purpose. It is provided “as is” without express or implied warranty.

The following individuals contributed in part to the Network Time Protocol Distribution Version 4 and are acknowledged as authors of this work.

1. Mark Andrews <mark_andrews@isc.org controller

2. Bernd Altmeier <altmeier@atlsoft.de line and PCI-bus devices

3. Viraj Bais <vbais@mailman1.intel.com <kirkwood@striderfm.intel.com

4. Michael Barone <michael,barone@lmco.com

5. Jean-Francois Boudreault <Jean-Francois.Boudreault@viagenie.qc.ca

6. Karl Berry <karl@owl.HQ.ileaf.com

7. Greg Brackley <greg.brackley@bigfoot.com Clean up recvbuf and iosignal code into separate modules.

8. Marc Brett <Marc.Brett@westgeo.com

9. Piete Brooks <Piete.Brooks@cl.cam.ac.uk Trimble PARSE support

10. Reg Clemens <reg@dwf.com

11. Steve Clift <clift@ml.csiro.au

12. Casey Crellin <casey@csc.co.za help with target configuration

13. Sven Dietrich <sven_dietrich@trimble.com clock driver, NT adj. residuals, integrated Greg’s Winnt port.

14. John A. Dundas III <dundas@salt.jpl.nasa.gov

15. Torsten Duwe <duwe@immd4.informatik.uni-erlangen.de port

16. Dennis Ferguson <dennis@mrbill.canet.ca NTP Version 2 as specified in RFC-1119

17. John Hay <jhay@@icomtek.csir.co.za

18. Glenn Hollinger <glenn@herald.usask.ca

19. Mike Iglesias <iglesias@uci.edu

20. Jim Jagielski <jim@jagubox.gsfc.nasa.gov

21. Jeff Johnson <jbj@chatham.usdesign.com overhaul

22. Hans Lambermont <Hans.Lambermont@nl.origin-it.com <H.Lambermont@chello.nl

23. Poul-Henning Kamp <phk@FreeBSD.ORG author)

24. Frank Kardel [27]<kardel (at) ntp (dot) org driver (scripts, syslog cleanup, dynamic interface handling

25. William L. Jones <jones@hermes.chpc.utexas.edu modifications, HPUX modifications

26. Dave Katz <dkatz@cisco.com

27. Craig Leres <leres@ee.lbl.gov GPS clock driver

28. George Lindholm <lindholm@ucs.ubc.ca

29. Louis A. Mamakos <louie@ni.umd.edu

30. Lars H. Mathiesen <thorinn@diku.dk code for Version 3 as specified in RFC-1305

31. Danny Mayer <mayer@ntp.org Maintenance

32. David L. Mills <mills@udel.edu discipline, authentication, precision kernel; clock drivers: Spectracom, Austron, Arbiter, Heath, ATOM, ACTS, KSI/Odetics; audio clock drivers: CHU, WWV/H, IRIG

33. Wolfgang Moeller <moeller@gwdgv1.dnet.gwdg.de

34. Jeffrey Mogul <mogul@pa.dec.com

35. Tom Moore <tmoore@fievel.daytonoh.ncr.com

36. Kamal A Mostafa <kamal@whence.com

37. Derek Mulcahy <derek@toybox.demon.co.uk Hart-Davis <d@hd.org

38. Rainer Pruy <Rainer.Pruy@informatik.uni-erlangen.de monitoring/trap scripts, statistics file handling

39. Dirce Richards <dirce@zk3.dec.com

40. Wilfredo Sanchez <wsanchez@apple.com NetInfo

41. Nick Sayer <mrapple@quack.kfu.com

42. Jack Sasportas <jack@innovativeinternet.com space on the stuff in the html/pic/ subdirectory

43. Ray Schnitzler <schnitz@unipress.com

44. Michael Shields <shields@tembel.org

45. Jeff Steinman <jss@pebbles.jpl.nasa.gov driver

46. Harlan Stenn <harlan@pfcs.com makeover, various other bits (see the ChangeLog)

47. Kenneth Stone <ken@sdd.hp.com

48. Ajit Thyagarajan <ajit@ee.udel.edu support

49. Tomoaki TSURUOKA <tsuruoka@nc.fukuoka-u.ac.jp driver

50. Paul A Vixie <vixie@vix.com TrueTime clock driver

51. Ulrich Windl <Ulrich.Windl@rz.uni-regensburg.de validated HTML documents according to the HTML DTD

References

1. mailto:mark_andrews@isc.org

2. mailto:altmeier@atlsoft.de
3. mailto:vbais@mailman1.intel.co
4. mailto:kirkwood@striderfm.intel.com
5. mailto:michael.barone@lmco.com
6. mailto:Jean-Francois.Boudreault@viagenie.qc.ca
7. mailto:karl@owl.HQ.ileaf.com
8. mailto:greg.brackley@bigfoot.com
9. mailto:Marc.Brett@westgeo.com
10. mailto:Piete.Brooks@cl.cam.ac.uk
11. mailto:reg@dwf.com
12. mailto:clift@ml.csiro.au
13. mailto:casey@csc.co.za
14. mailto:Sven_Dietrich@trimble.COM
15. mailto:dundas@salt.jpl.nasa.gov
16. mailto:duwe@immd4.informatik.uni-erlangen.de
17. mailto:dennis@mrbill.canet.ca
18. mailto:jhay@icomtek.csir.co.za
19. mailto:glenn@herald.usask.ca
20. mailto:iglesias@uci.edu
21. mailto:jagubox.gsfc.nasa.gov
22. mailto:jbj@chatham.usdesign.com
23. mailto:Hans.Lambermont@nl.origin-it.com
24. mailto:H.Lambermont@chello.nl
25. mailto:phk@FreeBSD.ORG
26. http://www4.informatik.uni-erlangen.de/%7ekardel
27. mailto:kardel(at)ntp(dot)org
28. mailto:jones@hermes.chpc.utexas.edu
29. mailto:dkatz@cisco.com
30. mailto:leres@ee.lbl.gov
31. mailto:lindholm@ucs.ubc.ca
32. mailto:louie@ni.umd.edu
33. mailto:thorinn@diku.dk
34. mailto:mayer@ntp.org
35. mailto:mills@udel.edu
36. mailto:moeller@gwdgv1.dnet.gwdg.de
37. mailto:mogul@pa.dec.com
38. mailto:tmoore@fievel.daytonoh.ncr.com
39. mailto:kamal@whence.com

40. mailto:derek@toybox.demon.co.uk
41. mailto:d@hd.org
42. mailto:Rainer.Pruy@informatik.uni-erlangen.de
43. mailto:dirce@zk3.dec.com
44. mailto:wsanchez@apple.com
45. mailto:mrapple@quack.kfu.com
46. mailto:jack@innovativeinternet.com
47. mailto:schnitz@unipress.com
48. mailto:shields@tembel.org
49. mailto:pebbles.jpl.nasa.gov
50. mailto:harlan@pfcs.com
51. mailto:ken@sdd.hp.com
52. mailto:ajit@ee.udel.edu
53. mailto:tsuruoka@nc.fukuoka-u.ac.jp
54. mailto:vixie@vix.com
55. mailto:Ulrich.Windl@rz.uni-regensburg.de

GNU LESSER GENERAL PUBLIC LICENSE

Redistribution and use in source and binary forms, with or without

GNU GENERAL PUBLIC LICENSE

General Public Licence for the software known as MSNTP

openssh 5.1p1

Available under license:

This file is part of the OpenSSH software.

The licences which components of this software fall under are as follows. First, we will summarize and say that all components are under a BSD licence, or a licence more free than that.

1)

OpenSSH contains no GPL code.

Copyright (c) 1995 Tatu Ylonen <ylo@cs.hut.fi

All rights reserved

As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than “ssh” or “Secure Shell”.

[Tatu continues]

However, I am not implying to give any licenses to any patents or copyrights held by third parties, and the software includes parts that are not under my direct control. As far as I know, all included source code is used in accordance with the relevant license agreements and can be used freely for any purpose (the GNU license being the most restrictive); see below for details.

[However, none of that term is relevant at this point in time. All of these restrictively licensed software components which he talks about have been removed from OpenSSH, i.e.,

- RSA is no longer included, found in the OpenSSL library
- IDEA is no longer included, its use is deprecated
- DES is now external, in the OpenSSL library
- GMP is no longer used, and instead we call BN code from OpenSSL
- Zlib is now external, in a library
- The make-ssh-known-hosts script is no longer included
- TSS has been removed
- MD5 is now external, in the OpenSSL library
- RC4 support has been replaced with ARC4 support from OpenSSL
- Blowfish is now external, in the OpenSSL library

[The licence continues]

Note that any information and cryptographic algorithms used in this software are publicly available on the Internet and at any major bookstore, scientific library, and patent office worldwide. More information can be found e.g. at “http://www.cs.hut.fi/crypto”.

The legal status of this program is some combination of all these permissions and restrictions. Use only at your own responsibility.

You will be responsible for any legal consequences yourself; I am not making any claims whether possessing or using this is legal or not in your country, and I am not taking any responsibility on your behalf.

NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

2)

The 32-bit CRC compensation attack detector in deattack.c was contributed by CORE SDI S.A. under a BSD-style license.

Cryptographic attack detector for ssh - source code

Copyright (c) 1998 CORE SDI S.A., Buenos Aires, Argentina.

All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that this copyright notice is retained.

THIS SOFTWARE IS PROVIDED “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES ARE DISCLAIMED. IN NO EVENT SHALL CORE SDI S.A. BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OR MISUSE OF THIS SOFTWARE.

Ariel Futoransky <futo@core-sdi.com

<http://www.core-sdi.com

3)

ssh-keyscan was contributed by David Mazieres under a BSD-style license.

Copyright 1995, 1996 by David Mazieres <dm@lcs.mit.edu

Modification and redistribution in source and binary forms is permitted provided that due credit is given to the author and the OpenBSD project by leaving this copyright notice intact.

4)

The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers and Paulo Barreto is in the public domain and distributed with the following license:

version 3.0 (December 2000)

Optimised ANSI C code for the Rijndael cipher (now AES)

author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be

author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be

author Paulo Barreto <paulo.barreto@terra.com.br

This code is hereby placed in the public domain.

THIS SOFTWARE IS PROVIDED BY THE AUTHORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

5)

One component of the ssh source code is under a 3-clause BSD license, held by the University of California, since we pulled these parts from original Berkeley code.

Copyright (c) 1983, 1990, 1992, 1993, 1995

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

6)

Remaining components of the software are provided under a standard 2-term BSD licence with the following names as copyright holders:

Markus Friedl

Theo de Raadt

Niels Provos

Dug Song

Aaron Campbell

Damien Miller

Kevin Steves

Daniel Kouril

Wesley Griffin

Per Allansson

Nils Nordman

Simon Wilkinson

Portable OpenSSH additionally includes code from the following copyright holders, also under the 2-term BSD license:

Ben Lindstrom

Tim Rice

Andre Lucas

Chris Adams

Corinna Vinschen

Cray Inc.

Denis Parker

Gert Doering

Jakob Schlyter

Jason Downs

Juha Yrj?l?

Michael Stone

Networks Associates Technology, Inc.

Solar Designer

Todd C. Miller

Wayne Schroeder

William Jones

Darren Tucker

Sun Microsystems

The SCO Group

Daniel Walsh

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

8)

Portable OpenSSH contains the following additional licenses:

a) md5crypt.c, md5crypt.h

“THE BEER-WARE LICENSE” (Revision 42):

<phk@login.dknet.dk

notice you can do whatever you want with this stuff. If we meet some day, and you think this stuff is worth it, you can buy me a beer in return. Poul-Henning Kamp

b) snprintf replacement

Copyright Patrick Powell 1995

his code is based on code written by Patrick Powell

papowell@astart.com) It may be used for any purpose as long as this notice remains intact on all source code distributions

c) Compatibility code (openbsd-compat)

Apart from the previously mentioned licenses, various pieces of code in the openbsd-compat/ subdirectory are licensed as follows:

Some code is licensed under a 3-term BSD license, to the following copyright holders:

Todd C. Miller

Theo de Raadt

Damien Miller

Eric P. Allman

The Regents of the University of California

Constantin S. Svintsoff

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Some code is licensed under an ISC-style license, to the following copyright holders:

Internet Software Consortium.

Todd C. Miller

Reyk Floeter

Chad Mynhier

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED “AS IS” AND TODD C. MILLER DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL TODD C. MILLER BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

Some code is licensed under a MIT-style license to the following copyright holders:

Free Software Foundation, Inc.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, distribute with modifications, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED “AS IS”, WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name(s) of the above copyright holders shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization.

openssl 0.9.8j

Notifications:

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Available under license:

LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit.

See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)”

4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

“This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: “This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”

The word ‘cryptographic’ can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publicly available version or derivative of this code cannot be changed, i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

Copyright (C) 1995-1997 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an Blowfish implementation written by Eric Young (eay@cryptsoft.com).

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution.

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by Eric Young (eay@cryptsoft.com).

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed, i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

The reason behind this being stated in this direct manner is past experience in code simply being copied and the attribution removed from it and then being distributed as part of other packages. This implementation was a non-trivial and unpaid effort.

Copyright (C) 1995-1997 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an DES implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with MIT's libdes.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution.

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of that the SSL library. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by Eric Young (eay@cryptsoft.com)

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed, i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

The reason behind this being stated in this direct manner is past experience in code simply being copied and the attribution removed from it and then being distributed as part of other packages. This implementation was a non-trivial and unpaid effort.

pciutils 3.0.1

Available under license:

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

<one line to give the program’s name and a brief idea of what it does.

Copyright (C) <year

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type ‘show w’.

This is free software, and you are welcome to redistribute it under certain conditions; type ‘show c’ for details.

The hypothetical commands ‘show w’ and ‘show c’ should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than ‘show w’ and ‘show c’; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a “copyright disclaimer” for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

‘Gnomovision’ (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.

Copyright (c) 1997--2008 Martin Mares <mj@ucw.cz

All files in this package can be freely distributed and used according to the terms of the GNU General Public License, either version 2 or (at your opinion) any newer version. See http://www.gnu.org/ for details.

List of PCI ID’s

Maintained by Martin Mares <mj@ucw.cz

Linux PCI ID’s Project at http://pciids.sf.net/.

New data are always welcome, especially if accurate. If you have anything to contribute, please follow the instructions at the web site or send a diff -u against the most recent pci.ids to pci-ids@ucw.cz.

This file can be distributed under either the GNU General Public License (version 2 or higher) or the 3-clause BSD License.

Daily snapshot on Thu 2008-09-11 01:05:01

License: BSD

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

procps 3.2.7

Available under license:

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

<one line to give the program’s name and a brief idea of what it does.

Copyright (C) <year

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type ‘show w’.

This is free software, and you are welcome to redistribute it under certain conditions; type ‘show c’ for details.

The hypothetical commands ‘show w’ and ‘show c’ should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than ‘show w’ and ‘show c’; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a “copyright disclaimer” for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

‘Gnomovision’ (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

sysfsutils 2.1.0

Available under license:

The commands and utilities under the “test” directory are licensed under the GNU General Public License (GPL) Version 2, June 1991. The full text of the GPL is located at:

sysfsutils/cmd/GPL

The sysfs library is licensed under the GNU Lesser Public License (LGPL) Version 2.1, February 1999. The full text of the LGPL is located at:

sysfsutils/lib/LGPL

The GNU General Public License (GPL)

GNU Lesser Public License

sysstat 8.1.3

Available under license:

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

675 Mass Ave, Cambridge, MA 02139, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

Appendix: How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the “copyright” line and a pointer to where the full notice is found.

<one line to give the program’s name and a brief idea of what it does.

Copyright (C) 19yy <name of author

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 675 Mass Ave, Cambridge, MA 02139, USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) 19yy name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type ‘show w’.

This is free software, and you are welcome to redistribute it under certain conditions; type ‘show c’ for details.

The hypothetical commands ‘show w’ and ‘show c’ should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than ‘show w’ and ‘show c’; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a “copyright disclaimer” for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program

‘Gnomovision’ (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

tcl 8.4.9

Available under license:

This software is copyrighted by the Regents of the University of California, Sun Microsystems, Inc., Scriptics Corporation, ActiveState Corporation and other parties. The following terms apply to all files associated with the software unless explicitly disclaimed in individual files.

The authors hereby grant permission to use, copy, modify, distribute, and license this software and its documentation for any purpose, provided that existing copyright notices are retained in all copies and that this notice is included verbatim in any distributions. No written agreement, license, or royalty fee is required for any of the authorized uses.

Modifications to this software may be copyrighted by their authors and need not follow the licensing terms described here, provided that the new terms are clearly indicated on the first page of each file where they apply.

IN NO EVENT SHALL THE AUTHORS OR DISTRIBUTORS BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF THIS SOFTWARE, ITS DOCUMENTATION, OR ANY DERIVATIVES THEREOF, EVEN IF THE AUTHORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THE AUTHORS AND DISTRIBUTORS SPECIFICALLY DISCLAIM ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. THIS SOFTWARE IS PROVIDED ON AN “AS IS” BASIS, AND THE AUTHORS AND DISTRIBUTORS HAVE NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

GOVERNMENT USE: If you are acquiring this software on behalf of the U.S. government, the Government shall have only “Restricted Rights” in the software and related documentation as defined in the Federal Acquisition Regulations (FARs) in Clause 52.227.19 (c) (2). If you are acquiring the software on behalf of the Department of Defense, the software shall be classified as “Commercial Computer Software” and the Government shall have only “Restricted Rights” as defined in Clause 252.227-7013 (c) (1) of DFARs. Notwithstanding the foregoing, the authors grant the U.S. Government and others acting in its behalf permission to use and distribute the software in accordance with the terms specified in this license.

tcpdump 3.9.8 1.0.1.0801182

Available under license:

License: BSD

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

tipc 1.7.6-bundle

Available under license:

net/tipc/tipc_user_reg.c: TIPC user registry code

Copyright (c) 2000-2006, Ericsson AB

Copyright (c) 2004-2006, Wind River Systems

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. Neither the names of the copyright holders nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

* Alternatively, this software may be distributed under the terms of the GNU General Public License (“GPL”) version 2 as published by the Free Software Foundation.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

client_tipc.c

Short description: TIPC benchmark demo (client side)

Copyright (c) 2001-2005, Ericsson Research Canada

Copyright (c) 2004-2006, Wind River Systems

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the names of the copyright holders nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

util-linux 2.12r

Available under license:

GNU GENERAL PUBLIC LICENSE

Copyright (c) 1989 The Regents of the University of California.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

This product includes software developed by the University of California, Berkeley and its contributors.

4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright (c) 2000-2001 Gunnar Ritter. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. [deleted]

4. Neither the name of Gunnar Ritter nor the names of his contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY GUNNAR RITTER AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL GUNNAR RITTER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS

INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

zlib 1.2.3

Available under license:

License attached

zlib.h -- interface of the ‘zlib’ general purpose compression library version 1.2.3, July 18th, 2005

Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler

This software is provided ‘as-is’, without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Jean-loup Gailly　　Mark Adler

jloup@gzip.org　　madler@alumni.caltech.edu

The data format used by the zlib library is described by RFCs (Request for Comments) 1950 to 1952 in the files http://www.ietf.org/rfc/rfc1950.txt (zlib format), rfc1951.txt (deflate format) and rfc1952.txt (gzip format).

■ zlib 1.2.3

GLOSSARY

数字

3DES トリプル DES（Data Encryption Standard）。DES をより強力にしたバージョンで、SSH バージョン 1.5 のデフォルトの暗号化方式。センサーと SSH セッションを確立するときに使用されます。センサーでデバイスを管理しているときに使用できます。

802.x LAN プロトコルの定義に関する IEEE 標準のセット。

A

AAA 認証、許可、アカウンティング。「トリプル A」と読みます。シスコ デバイスの主要な推奨アクセス コントロール方法です。

ACE Access Control Entry（アクセス コントロール エントリ）。ACL 内のエントリで、指定されたアドレスまたはプロトコルに関して実行するアクションを記述します。センサーは、ACE を追加または削除してホストをブロックします。

ACK 確認応答。1 台のネットワーク デバイスからもう 1 台のネットワーク デバイスに送信される、イベントが発生したこと（メッセージの受信など）を確認する通知。

ACL Access Control List（アクセス コントロール リスト）。ルータを経由するデータの流れを制御する ACE のリストです。ルータ インターフェイスごとに、受信データ用と送信データ用の 2 つの ACL があります。1 つの方向で同時にアクティブにできる ACL は 1 つだけです。ACL は、番号または名前で識別されます。ACL は、標準、強化、拡張のいずれかになります。センサーで ACL を管理するように設定できます。

ACS サーバ Cisco Access Control Server。ネットワーク ユーザ、ネットワーク管理者、ネットワーク インフラストラクチャ リソースの集中管理ポイントとなる RADIUS セキュリティ サーバ。

AIC エンジン Application Inspection および Control エンジン。Web トラフィックを詳細に分析します。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。インスタント メッセージングなど、指定されたポートを介してトンネリングを試みるアプリケーションや gotomypc などのトンネリング アプリケーションを管理制御できます。また、FTP トラフィックを検査し、発行されるコマンドを制御できます。

AIM IPS Advanced Integration Module。Cisco ルータにインストールされている IPS ネットワーク モジュールの一種。

AIP SSM Advanced Inspection and Prevention Security Services Module。Cisco ASA 5500 シリーズの適応型セキュリティ アプライアンスの IPS プラグイン モジュール。AIP SSM は、多数の埋め込み型シグニチャ ライブラリに基づいて異常や悪用を探索することでネットワーク トラフィックのモニタおよびリアルタイム分析を行う IPS モジュールです。不正なアクティビティを検出すると、AIP SSM は、該当する接続を終了して攻撃元のホストを永続的にブロックし、この事象をログに記録し、さらにアラートを Device Manager に送信します。適応型セキュリティ アプライアンスも参照してください。

API アプリケーション プログラミング インターフェイス。アプリケーション プログラムが通信ソフトウェアと対話する手段。標準化された API では、基礎となる通信手段とは関係なく、アプリケーション プログラムを開発できます。コンピュータ アプリケーション プログラムは、一式の標準ソフトウェア割り込み、呼び出し、およびデータ フォーマットを実行して、他のデバイスとの接続を開始します（ネットワーク サービス、メインフレーム通信プログラム、その他のプログラム間通信）。通常、API を使用すると、ソフトウェア開発者はアプリケーションがオペレーティング システムやネットワークと通信するために必要なリンクを簡単に作成できます。

ARC Attack Response Controller。以前は Network Access Controller（NAC）と呼ばれていました。IPS のコンポーネントの 1 つ。適用可能な場合にブロックおよびブロック解除の機能を提供するソフトウェア モジュール。

ARP アドレス解決プロトコル。IP アドレスを MAC アドレスにマッピングする際に使用されるインターネット プロトコル。RFC 826 で定義されています。

ASDM Adaptive Security Device Manager。適応型セキュリティ デバイスの設定と管理が可能な Web ベースのアプリケーション。

ASN.1 抽象構文記法 1。データ プレゼンテーションの標準。

Atomic エンジン 2 つの Atomic エンジンがあります。アトミック IP は IP プロトコル パケットとそれに関連付けられたレイヤ 4 トラスポート プロトコルを検査します。アトミック ARP はレイヤ 2 ARP プロトコルを検査します。

AuthenticationApp IPS のコンポーネントの 1 つ。IP アドレス、パスワード、デジタル証明書に基づいてユーザを許可および認証します。

AV アンチウィルス。

B

BIOS Basic Input/Output System。センサーを起動し、センサー内のデバイスとシステム間の通信を行うプログラム。

BO BackOrifice。UDP 上だけで実行された Windows を標的とした最初のバック ドア型トロイの木馬。

BO2K BackOrifice 2000。TCP と UDP 上で実行される Windows を標的とするバック ドア型トロイの木馬。

Bpdu Bridge Protocol Data Unit（ブリッジ プロトコル データ ユニット）。ネットワーク内のブリッジ間で情報を交換するために設定可能な間隔で送出される、スパニングツリー プロトコルの hello パケット。

C

CA 認証局（certification authority）。デジタル証明書（特に X.509 証明書）を発行し、証明書内のデータ項目間のバインディングを保証するエンティティです。センサーは、自己署名証明書を使用します。

CA 証明書 別の CA によって発行された、CA の証明書。

CEF シスコ エクスプレス フォワーディング。CEF は、高度なレイヤ 3 IP スイッチング テクノロジーです。CEF によって、インターネットや、Web ベースのアプリケーションまたは対話型セッションが集中的に使用されるネットワークなどの、大規模でダイナミックなトラフィック パターンを持つネットワークのパフォーマンスおよびスケーラビリティが最適化されます。

cidDump 大量の情報を取り込むためのスクリプト。この情報には、IPS プロセス リスト、ログ ファイル、OS 情報、ディレクトリ リスト、パッケージ情報、コンフィギュレーション ファイルなどがあります。

CIDEE Cisco Intrusion Detection Event Exchange。Cisco IPS システムで使用される SDEE への拡張子を指定します。CIDEE 標準では、Cisco IPS システムでサポートされる使用可能なすべての拡張子が指定されています。

CIDS ヘッダー IPS システムの各パケットに追加されるヘッダー。パケットの分類、長さ、チェックサムの結果、タイムスタンプ、受信インターフェイスが含まれます。

Cisco IOS CiscoFusion アーキテクチャの下で全製品に共通の機能、拡張性、セキュリティを提供するシスコ ソフトウェア。Cisco IOS では、広範なプロトコル、メディア、サービス、およびプラットフォームをサポートしながら、インターネットワークのインストールと管理を一元化、統合、および自動化できます。

CLI コマンドライン インターフェイス。センサー アプリケーションの設定と制御に使用される、センサーに付属のシェル。

CollaborationApp IPS のコンポーネントの 1 つ。グローバル相関データベースを通して他のデバイスと情報を共有し、すべてのデバイスの総合的な有効性を高めます。

Control Transaction Server IPS のコンポーネントの 1 つ。リモート クライアントからの制御トランザクションを受け付け、ローカル制御トランザクションを開始して、リモート クライアントに応答を返します。

Control Transaction Source IPS のコンポーネントの 1 つ。リモート アプリケーションに向けられた制御トランザクションを待機し、制御トランザクションをリモート ノードに転送し、応答を発信側に返します。

Cookie Web サーバから Web ブラウザに送信される情報。ブラウザはこれを保存し、Web サーバに追加要求を行うたびに Web サーバに送り返します。

CSA MC Cisco Security Agent Management Center。CSA MC は、管理する CSA エージェントからホスト ポスチャ情報を受信します。また、ネットワークから隔離する必要があると判断した IP アドレスのウォッチ リストも維持します。

CSM Cisco Security Manager。Cisco Self-Defending Network ソリューションのプロビジョニング コンポーネントです。CS-Manager は CS-MARS と完全に統合されています。

CS-MARS Cisco Security Monitoring, Analysis, and Response System。Cisco Self-Defending Network ソリューションのモニタリング コンポーネント。CS-MARS は CS-Manager と完全に統合されています。

CVE Common Vulnerabilities and Exposures。http://cve.mitre.org/ で管理されている脆弱性および他の情報セキュリティの危険に関する標準化された名前のリスト。

D

DCE データ回線終端装置（ITU-T の拡張）。ユーザとネットワークを結ぶインターフェイスのネットワーク側を構成する通信ネットワークのデバイスおよび接続。DCE は、ネットワークへの物理的接続を提供し、トラフィックの転送を行い、DCE と DTE デバイス間のデータ転送を同期化するためのクロッキング信号を提供します。DCE の例として、モデルとインターフェイス カードがあります。

DCOM 分散コンポーネント オブジェクト モデル。ソフトウェア コンポーネントどうしがネットワーク上で直接通信できるようにするプロトコル。Microsoft が開発し、以前はネットワーク OLE と呼ばれた DCOM は、HTTP などのインターネット プロトコルを含む複数のネットワーク転送で使用されるように設計されています。

DDoS 分散型サービス拒否攻撃。多数の侵害されたシステムが 1 つのターゲットを攻撃することで、対象のシステムユーザにサービス拒否を発生させる攻撃。ターゲット システムにメッセージが大量に送信されると、基本的にそのシステムが強制的にシャット ダウンされ、システムの正規ユーザへのサービスが拒否されます。

DES データ暗号規格。アルゴリズムではなく 56 ビット キーを基盤とする、強力な暗号化方式。

DIMM Dual In-line Memory Module（デュアル インライン メモリ モジュール）。

DMZ 非武装地帯。プライベート（内部）ネットワークとパブリック（外部）ネットワークとの間の中立地帯に位置する単独のネットワークです。

DNS ドメイン ネーム システム（Domain Name System）。インターネット全体にわたるホスト名と IP アドレスのマッピングです。DNS を使用すると、人間が読める形式の名前を、ネットワーク パケットで必要とされる IP アドレスに変換できます。

DoS Denial of Service（サービス拒絶）。特定のシステムまたはネットワークの操作を混乱させることを目的とする攻撃です。

DRAM ダイナミック RAM。定期的な更新が必要なコンデンサ内に情報を格納する RAM。内容の更新中、プロセッサが DRAM にアクセスできなくなるため、遅延が発生することがあります。ただし、DRAM は SRAM ほど複雑ではなく、大容量です。

DTE データ端末機器。RS-232C 接続上のデバイスのロールを指します。DTE はデータを送信回線に書き込み、受信回線からデータを読み取ります。

DTP ダイナミック トランキング プロトコル。2 台のデバイスを結ぶリンクでのトランキングや使用するトランキング カプセル化のタイプ（ISL または 802.1q）のネゴシエーションに使用される、VLAN グループのシスコ独自のプロトコル。

E

ECLB イーサネット チャネル ロード バランシング。Catalyst スイッチが、異なる物理パスでトラフィック フローを分岐できるようにします。

ESD 静電放電。静電放電は、1 つの物体から別の物体への急速な電荷の移動により、数千ボルトの電荷が発生することを指します。電気的コンポーネントやサーキット カード アセンブリ全体に重大なダメージを引き起こす場合があります。

evIdsAlert イベント ストアに書き込まれる、アラートを表す XML エンティティ。

F

Fast Flux
Fast Flux はボットネットで使用される DNS 手法の 1 つで、フィッシング サイトやマルウェア配信サイトを、プロキシとして動作する絶えず変化する侵害されたホスト ネットワークの後ろに隠します。マルウェア ネットワークの検出や対策を困難にするためにピアツーピア ネットワーキング、分散指示管理、Web ベース ロード バランシング、プロキシ リダイレクションを組み合わせる手法を指すこともあります。Storm Worm は、この手法を利用した最新のマルウェアのバリアントの 1 つです。

Flood エンジン
ホストおよびネットワーク宛の ICPM および UDP フラッドを検出します。

FQDN
完全修飾名。DNS のツリー階層で正確な場所を指定するドメイン名。ルート ドメインを基準に、トップレベル ドメインを含むすべてのドメイン レベルを指定します。完全修飾ドメイン名は、ネームスペースでこの正確さによって識別されます。

FTP
File Transfer Protocol（ファイル転送プロトコル）。ネットワーク ノード間でファイルを転送するために使用され、TCP/IP プロトコル スタックの一部であるアプリケーション プロトコル。FTP は、RFC 959 で定義されています。

FTP サーバ
ファイル転送プロトコル（File Transfer Protocol）サーバ。ネットワーク ノード間のファイルの転送に FTP プロトコルを使用するサーバ。

FWSM
ファイアウォール セキュリティ モジュール。Catalyst 6500 シリーズ スイッチにインストールできるモジュール。ブロックに **shun** コマンドを使用します。FWSM は、シングル モードでもマルチモードでも設定できます。

G

GBIC
ギガビット インターフェイス コンバータ。多くの場合、光ケーブルをファイバ インターフェイスに適応させる光ファイバ トランシーバを指します。ファイバ対応スイッチと NIC は、一般に GBIC スロットと SFP スロット、またはそのどちらかを提供します。詳細については、『*Catalyst Switch Cable, Connector, and AC Power Cord Guide*』を参照してください。

Gigabit Ethernet
1996 年に IEEE（電気電子学会）802.3z 規格委員会によって承認された、高速イーサネットの規格。

GMT
Greenwich Mean Time（グリニッジ標準時）。経度が 0 度のタイムゾーン。現在は、協定世界時（UTC）と呼ばれます。

GRUB
Grand Unified Bootloader。ブート ローダーは、コンピュータを起動すると最初に実行されるソフトウェア プログラムです。オペレーティング システム カーネル ソフトウェアをロードし、制御を渡す役割を果たします。その後、カーネルがオペレーティング システムの残りを初期化します。

H

H.225.0
H.225.0 セッションの確立とパケット化を規定する ITU 標準。H.225.0 では、実際には、RAS、Q.931 の使用、RTP の使用など、いくつかの異なるプロトコルが定められています。

H.245
H.245 エンドポイントの制御を規定する ITU 標準。

H.323
異種の通信デバイスが、標準化された通信プロトコルを使用して、相互に通信できます。H.323 は、CODEC の共通セット、コール セットアップとネゴシエーションの手順、および基本的なデータ転送方法を定義しています。

HTTP ハイパーテキスト転送プロトコル。IPS アーキテクチャでリモート データ交換に使用される、ステートレスな要求 / 応答メディア転送プロトコルです。

HTTPS 標準 HTTP プロトコルを拡張したもので、Web サイトからのトラフィックを暗号化することによって機密保持を可能にします。デフォルトでは、このプロトコルは TCP ポート 443 を使用します。

I

ICMP Internet Control Message Protocol（インターネット制御メッセージ プロトコル）。エラーを報告し、IP パケット処理に関連するその他の情報を提供するネットワーク層のインターネット プロトコル。RFC 792 に規定されています。

ICMP フラッド プロトコル実装で処理可能な数よりも多いエコー要求（"ping"）パケットをホストに送信する DoS 攻撃。

IDAPI Intrusion Detection Application Programming Interface。IPS アーキテクチャ アプリケーション間に単純なインターフェイスを提供します。IDAPI はイベント データを読み書きし、制御トランザクションのメカニズムを提供します。

IDCONF 侵入検知設定。侵入検知と予防システムの設定に使用される操作メッセージを定義するデータ形式の標準です。

IDENT RFC 1413 で指定された Ident プロトコルは、特定の TCP 接続のユーザの識別に役立つインターネット プロトコルです。

IDIOM Intrusion Detection Interchange and Operations Messages。侵入検知システムによって報告されるイベント メッセージ、および侵入検知システムの設定と制御に使用される操作メッセージを定義するデータ形式の標準です。

IDM IPS Device Manager。センサーの設定と管理が可能な Web ベースのアプリケーションです。IDM の Web サーバはセンサーに常駐します。この Web サーバには、Internet Explorer や Firefox などの Web ブラウザでアクセスできます。

IDMEF Intrusion Detection Message Exchange Format。IETF Intrusion Detection Working Group による標準草案です。

IDS MC Management Center for IDS Sensors。Web ベースの IDS マネージャで、最大 300 台のセンサーの設定を管理できます。

IDSM-2 Intrusion Detection System Module。Catalyst 6500 シリーズ スイッチで侵入検知を実行するスイッチング モジュールです。

IME IPS Manager Express。システムのヘルス モニタリング、イベント モニタリング、レポートおよび最大 10 のセンサーの設定を行うことができるネットワーク管理アプリケーション。

InterfaceApp IPS のコンポーネントの 1 つ。バイパスおよび物理設定を処理し、ペアにするインターフェイスを定義します。物理設定は、速度、デュプレックス、および管理状態です。

IP アドレス TCP/IP を使用するホストに割り当てられる 32 ビット アドレス。IP アドレスは、5 つのクラス（A、B、C、D、または E）のいずれかに属し、ピリオドで区切られた 4 つのオクテット（ドット付き 10 進形式）で記述されます。各アドレスはネットワーク番号、オプションのサブネットワーク番号、およびホスト番号で構成されます。ルーティングにはネットワーク番号とサブネットワーク番号を組み合わせて使用し、ネットワーク内またはサブネットワーク内の個別のホストのアドレス指定にはホスト番号を使用します。IP アドレスからのネットワーク情報とサブネットワーク情報の抽出には、サブネット マスクを使用します。

IP スプーフィング IP スプーフィング攻撃は、ネットワーク外の攻撃者が信頼されたユーザになりすますことによって発生します。攻撃者は、ネットワークの IP アドレス範囲内の IP アドレスを使用するか、信頼され、ネットワーク上の指定されたリソースへのアクセスが可能な、許可された外部 IP アドレスを使用して、このなりすましを行います。攻撃者が IPSec セキュリティ パラメータにアクセスした場合は、その攻撃者が企業ネットワークへのアクセスを許可されたリモート ユーザを偽装する可能性があります。

iplog 指定されたアドレスとの間でやり取りされるバイナリ パケットのログ。iplog は、シグニチャに log イベント アクションが選択されている場合に作成されます。iplog は、WireShark および TCPDUMP で読み取り可能な libpcap 形式で格納されます。

IPS 侵入防御システム。ネットワーク トラフィックの分析技術を使用して、ネットワークへの侵入の存在をユーザに警告するシステムです。

IPS SSP 侵入防御システム セキュリティ サービス プロセッサ。Cisco ASA 5585-X 適応型セキュリティ アプライアンスの IPS プラグイン モジュール。IPS SSP は、多数の埋め込み型シグニチャ ライブラリに基づいて異常や悪用を探索することでネットワーク トラフィックのモニタおよびリアルタイム分析を行う IPS サービス プロセッサです。不正なアクティビティを検出すると、IPS SSP は、該当する接続を終了して攻撃元のホストを永続的にブロックし、この事象をログに記録し、さらにアラートを Device Manager に送信します。適応型セキュリティ アプライアンスも参照してください。

IPS データまたはメッセージ IPS アプリケーション間でコマンド / コントロール インターフェイスを介して転送されるメッセージ。

IPv6 IP バージョン 6。IP の現在のバージョン（バージョン 4）に代わるバージョン。IPv6 ではパケット ヘッダーのフロー ID がサポートされており、フローの識別が可能です。以前は IPng（next generation（次世代））と呼ばれていました。

ISL スイッチ間リンク スイッチとルータの間のトラフィック フローとして VLAN 情報を維持するシスコ独自のプロトコル。

J

Java Web Start Java Web Start は、プラットフォームに依存しない、安全で堅牢な展開テクノロジーです。開発者は、アプリケーションを標準 Web サーバで利用可能にすることで、すべての機能を備えたアプリケーションをユーザに展開できます。ユーザは任意の Web ブラウザを使用してアプリケーションを起動し、常に最新バージョンを使用できます。

JNLP Java Network Launching Protocol。XML ファイル形式で定義され、Java Web Start アプリケーションの起動方法を指定しています。JNLP は、起動メカニズムを正しく実装する方法を定義したルールのセットで構成されています。

K

KB ナレッジ ベース。異常検出で学習され、ワーム ウィルス検出に使用されるしきい値のセット。

L

LACP リンク集約制御プロトコル。LACP は、LAN ポート間で LACP パケットを交換することで、EtherChannel リンクの自動作成を支援します。このプロトコルは、IEEE 802.3ad で定義されています。

LAN ローカルエリア ネットワーク。特定のホストのローカルとなっているレイヤ 2 ネットワーク ドメインを指します。同じ LAN 上の 2 つのホストで交換されるパケットは、レイヤ 3 ルーティングを必要としません。

Logger IPS のコンポーネントの 1 つ。アプリケーションのすべてのログ メッセージをログ ファイルに書き込み、アプリケーションのエラー メッセージをイベント ストアに書き込みます。

LOKI リモート アクセス、バック ドア トロイの木馬、ICMP トンネリング ソフトウェア。コンピュータが感染すると、悪意のあるコードによってペイロード サイズの小さい ICMP 応答の送信に使用できる ICMP トンネルが作成されます。

M

MainApp IPS のメイン アプリケーション。オペレーティング システムのブート後、センサーで最初に起動するアプリケーションです。設定を読み取ってアプリケーションを起動し、アプリケーションの開始および終了とノードの再起動を扱い、ソフトウェアのアップグレードを処理します。

MD5 Message Digest 5。128 ビット ハッシュを作成する単方向のハッシュ アルゴリズム。MD5 とセキュア ハッシュ アルゴリズム（SHA）は両方とも MD4 のバリエーションであり、MD4 のハッシュ アルゴリズムのセキュリティを強化するように設計されています。シスコは、IPSec フレームワーク内での認証にハッシュを使用します。また、SNMP v.2 のメッセージ認証にも使用します。MD5 は、通信の整合性を検証し、発信元を認証し、適時性をチェックします。

Meta エンジン 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。

MIB 管理情報ベース。SNMP や CMIP などのネットワーク管理プロトコルにより使用および管理されるネットワーク管理情報のデータベース。MIB オブジェクトの値は、SNMP コマンドまたは CMIP コマンドを使用して変更および取得できます。これらのコマンドは通常、GUI のネットワーク管理システムから実行します。MIB オブジェクトはツリー構造であり、ツリーにはパブリック（標準）ブランチとプライベート（独自）ブランチを含みます。

MIME Multipurpose Internet Mail Extension。電子メールで、テキスト以外のデータ（つまり、プレーン ASCII コードでは表現できないデータ）を転送するための規格。たとえば、バイナリ、外国語テキスト（ロシア語や中国語など）、オーディオ、ビデオなどのデータです。MIME は RFC 2045 で定義されています。

MPF モジュラ ポリシー フレームワーク。Cisco IOS ソフトウェアのモジュラ QoS CLI と同様の方法でセキュリティ アプライアンスの機能を設定するための手段です。

MSFC、MSFC2 マルチレイヤ スイッチ フィーチャ カード。Catalyst 6000 スーパーバイザ エンジンのオプション カードで、スイッチの L3 ルーティングを実行します。

MSRPC Microsoft Remote Procedure Call。MSRPC は、Microsoft による DCE RPC メカニズムの実装です。Microsoft は、Unicode 文字列、暗黙ハンドル、インターフェイスの継承（DCOM で広く使用される）、および DCE/RPC にすでに存在する可変文字列や構造パラダイムでの複雑な計算のサポートを追加しました。

MySDN My Self-Defending Network。IDM および IME のシグニチャ定義セクションの一部。シグニチャに関する詳細情報を提供します。

N

NAC Network Access Controller。「ARC」を参照してください。

NAS-ID ネットワーク アクセス ID。クライアントが、認証を試みているサービスのタイプを伝えるためにサーバに送信する識別子。

NAT Native Address Translation。ネットワーク デバイスが外部ネットワークに対してホストの実際の IP アドレスとは異なる IP アドレスを提示できるしくみ。

NBD 次の営業日。シスコ サービス契約による交換ハードウェアの到着。

never block アドレス ブロックされることのないように指定したホストおよびネットワーク。

never shun アドレス 「never block アドレス」を参照。

NIC ネットワーク インターフェイス カード。コンピュータ システムとのネットワーク通信機能を提供するボード。

NME IPS Network Module Enhanced。Cisco 2800 および 3800 シリーズのサービス統合型ルータの任意のネットワーク モジュール スロットにインストールできる IPS モジュール。

NMS Network Management System（ネットワーク管理システム）。ネットワークの少なくとも一部分の管理に責任を負うシステム。NMS は、一般的に適度にパワーのある装備の整ったコンピュータで、エンジニアリング ワークステーションなどです。NMS はエージェントと通信して、ネットワークの統計やリソースを追跡し続けるのに役立ちます。

Normalizer エンジン 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。

NOS ネットワーク OS。分散ファイル システムを指すときに使用される総称的な用語。LAN Manager、NetWare、NFS、VINES などが含まれます。

NotificationApp IPS のコンポーネントの 1 つ。アラート、ステータス、およびエラー イベントによってトリガーされたときに SNMP トラップを送信します。NotificationApp は、パブリック ドメイン SNMP エージェントを使用します。SNMP GET は、センサーの全般的な状態に関する情報を提供します。

NTP ネットワーク タイム プロトコル。インターネット内に置かれているラジオ クロックおよびアトミック クロックを参照することにより、正確な現地時間を維持する TCP 上に構築されたプロトコル。このプロトコルでは、分散されたクロックを長期にわたりミリ秒以内のレベルで同期させることができます。

NTP サーバ ネットワーク タイム プロトコル（Network Timing Protocol）サーバ。NTP を使用するサーバ。NTP は、TCP 上に構築されたプロトコルで、インターネット上にあるラジオおよびアトミック クロックを参照して正確なローカル タイムを維持します。このプロトコルでは、分散されたクロックを長期にわたりミリ秒以内のレベルで同期させることができます。

NVRAM 不揮発性読み取り / 書き込みメモリ。ユニットの電源オフ時に内容を保持する RAM。

O

OIR 活性挿抜 システム電源のオフ、コンソール コマンドの入力、他のソフトウェアやインターフェイスのシャットダウンを伴わずにカードの追加、交換、取り外しを行うことができる機能。

OPS Outbreak Prevention Service。

P

PAgP Port Aggregation Control Protocol。PAgP は、LAN ポート間で PAgP パケットを交換することで、EtherChannel リンクの自動作成を支援します。シスコ独自のプロトコルです。

PAM アプリケーションに AAA 機能を提供するソフトウェア モジュール。

PAP パスワード認証プロトコル。最もよく使用される RADIUS メッセージング プロトコル。

PASV ポート スプーフィング 保護された FTP サーバから非 FTP ポートへの接続をファイアウォール経由で開こうとする試み。ファイアウォールが不正接続を開くことによって、FTP 227 **passive** コマンドを誤って解釈したときに発生します。

PAT ポート アドレス変換。NAT より制限された変換方式で、1 つの IP アドレスと複数の異なるポートを使用してネットワークのホストを表します。

PAWS Protection Against Wrapped Sequence。ハイ パフォーマンス TCP ネットワークでのシーケンス番号のラップに対する保護。RFC 1323 を参照してください。

PCI Peripheral Component Interface。Intel ベースのコンピュータで使用される最も一般的な周辺装置拡張バス。

PDU プロトコル データ ユニット。パケットの OSI 用語。「BPDU」と「パケット」も参照してください。

PEP Cisco Product Evolution Program。PEP は、センサーの PID、VID、および SN で構成される UDI 情報です。PEP は、電子クエリー、製品ラベル、出荷品目を通して、ハードウェア バージョンとシリアル番号を提供します。

PER パック済みエンコーディング ルール。PER では、すべてのタイプを同じようにエンコードする一般的なエンコード スタイルを使用せずに、日付タイプに基づいてエンコードを特化して、よりコンパクトな表現を生成します。

PFC ポリシー フィーチャ カード（Policy Feature Card）。Catalyst 6000 スーパーバイザ エンジンのオプション カードで、VACL パケットのフィルタ処理をサポートします。

PID 製品 ID。UDI の 3 つのパートの 1 つを構成する注文可能製品識別子です。UDI は PEP ポリシーの一部です。

ping Packet Internet Groper。ネットワーク デバイスへの到達可能性をテストするために、IP ネットワークでよく使用されます。ターゲット ホストに ICMP エコー要求パケットを送信し、エコー応答返信をリッスンします。

PIX ファイアウォール Private Internet Exchange Firewall。シスコのネットワーク セキュリティ デバイスで、プログラミングによってネットワーク間でアドレスとポートをブロックしたり使用可能にしたりできます。

PKI 公開キー インフラストラクチャ（Public Key Infrastructure）。クライアントの X.509 証明書を使用した HTTP クライアントの認証です。

Point-to-Point（P2P; ポイントツーポイント） ピアツーピア。P2P ネットワークでは、ファイル共有の目的で、同時にクライアントとサーバの両方の機能を果たすノードが使用されます。

POST 電源投入時自己診断テスト。ハードウェア デバイスの電源を入れると、そのデバイスで実行されるハードウェア診断のセット。

Post-ACL ARC が ACL エントリを読み取り、ブロックされているアドレスのすべての拒否エントリの後ろにエントリを入れる ACL を指定します。

Pre-ACL ARC が ACL エントリを読み取り、ブロックされているアドレスのすべての拒否エントリの前にエントリを入れる ACL を指定します。

Q

Q.931 ISDN ネットワーク接続の確立、維持、およびクリアする信号送信に関する ITU-T 仕様。

QoS Quality of Service。伝送システムのパフォーマンスを基に、その伝送品質とサービスのアベイラビリティを表します。

R

RADIUS システムに対して、ネットワーク サービスに接続し、使用するための一元化された AAA 機能を提供するネットワーキング プロトコル。

RAM ランダムアクセス メモリ。マイクロプロセッサによる読み書きが可能な揮発性メモリ。

RAS Registration, Admission, and Status Protocol。管理機能を実行するためにエンドポイントとゲートキーパー間で使用されるプロトコル。RAS シグナリング機能は、VoIP ゲートウェイとゲートキーパー間で、登録、許可、帯域幅変更、ステータス、および解放手順を実行します。

RBCP ルータ ブレード制御プロトコル。RBCP は SCP に基づいていますが、ルータ アプリケーション専用に変更されています。イーサネット インターフェイスで動作し、メッセージに 802.2 SNAP カプセル化を使用するように設計されています。

regex 「正規表現」を参照。

Remote Authentication Dial In User Service 「RADIUS」を参照してください。

RMA 返品許可。不具合のあるハードウェアを返却し、交換品を受け取るシスコ プログラム。

ROMMON ROM モニタ（Read-Only-Memory Monitor）。ROMMON は、復旧のためにシステム イメージをセンサーに TFTP 転送できます。

RPC リモート プロシージャ コール。クライアント / サーバ コンピューティングの技術的な基礎。RPC は、クライアントで作成または指定されるプロシージャ コールで、サーバで実行され、結果はネットワーク経由でクライアントに返されます。

RSM Router Switch Module。Catalyst 5000 スイッチにインストールされているルータ モジュール。スタンドアロン ルータとまったく同様に機能します。

RTP Real-Time Transport Protocol（リアルタイム転送プロトコル）。一般に、IP ネットワークで使用されます。RTP は、音声、ビデオ、シミュレーション データなどのリアルタイム データをマルチキャストまたはユニキャストのネットワーク サービスとして、アプリケーションがリアルタイムにデータを転送できるように、エンドツーエンドのネットワーク転送機能を提供するように設計されています。RTP は、ペイロード タイプの識別、シーケンス番号付け、タイムスタンプ処理、配信のモニタリングなどのサービスをリアルタイム アプリケーションに提供します。

RTT ラウンドトリップ時間。ネットワークによってホストに課されるパケットを送信してから受信確認を受け取るまでの遅延時間の測定値。

RU ラック ユニット。ラックは、ラック ユニットで測定されます。1 RU は、44 mm つまり 1.75 インチです。

S

SCEP Simple Certificate Enrollment Protocol。PKCS#7 および PKCS#10 の使用によって既存のテクノロジーを活用した、シスコの PKI 通信プロトコルです。SCEP は進化した登録プロトコルです。

SCP Switch Configuration Protocol。イーサネット上で直接実行されるシスコの制御プロトコル。

SDEE Security Device Event Exchange。セキュリティ デバイスのイベントを伝える、製品に依存しない標準。さまざまなタイプのセキュリティ デバイスによって生成されるイベントを伝えるために必要な拡張性機能を追加します。

SDEE サーバ リモート クライアントからのイベントの要求を受け入れます。

Security Monitor Monitoring Center for Security。ネットワーク デバイスに、イベントの収集、表示、および報告の機能を提供します。IDS MC とともに使用されます。

SensorApp IPS のコンポーネントの 1 つ。パケットの取り込みと分析を実行します。SensorApp は、ネットワーク トラフィックで悪意のあるコンテンツを分析します。パケットは、センサー上のネットワーク インターフェイスからパケットを収集するように設計されたプロデューサによって供給されたプロセッサのパイプラインを通ります。SensorApp は分析エンジンを実行するスタンドアロンの実行可能ファイルです。

Service エンジン DNS、FTP、H255、HTTP、IDENT、MS RPC、MS SQL、NTP、P2P、RPC、SMB、SNMP、SSH、TNS などの特定のプロトコルを処理します。

session コマンド ルータとスイッチに対して使用されるコマンドで、ルータまたはスイッチ内のモジュールに対して Telnet またはコンソールのいずれかによるアクセスを提供します。

SFP 小型フォーム ファクタ。多くの場合、光ケーブルをファイバ インターフェイスに適応させる光ファイバ トランシーバを指します。詳細については、GBIC を参照してください。

shun コマンド 新規接続を抑制し、既存のすべての接続からのパケットを不許可にすることにより、攻撃元ホストへのダイナミック応答をイネーブルにします。PIX ファイアウォールでブロックしているときに、ARC によって使用されます。

SMB サーバ メッセージ ブロック。LAN マネージャおよび同様の NOS で、データをパッケージ化し、他のシステムと情報を交換するために使用されるファイルシステム プロトコル。

SMTP Simple Mail Transfer Protocol（シンプル メール転送プロトコル）。電子メール サービスを提供するインターネット プロトコル。

SN Serial Number（シリアル番号）。UDI に含まれます。SN はシスコ製品のシリアル番号です。

SNAP サブネットワーク アクセス プロトコル。サブネットワーク内のネットワーク エンティティとエンドシステム内のネットワーク エンティティ間で動作するインターネット プロトコル。SNAP は、IEEE ネットワーク上で IP データグラムと ARP メッセージをカプセル化する標準方式を指定します。エンド システム内の SNAP エンティティは、サブネットワークのサービスを利用して、3 つの重要な機能（データ転送、接続管理、および QoS 選択）を実行します。

SNMP 簡易ネットワーク管理プロトコル。TCP/IP ネットワークでほぼ独占的に使用されているネットワーク管理プロトコル。SNMP を使用すると、ネットワーク デバイスのモニタリングと制御、および設定、統計情報収集、パフォーマンス、セキュリティの管理が可能になります。

SNMP2 SNMP Version 2。ネットワーク管理プロトコルのバージョン 2。SNMP2 では、集中型および分散型のネットワーク管理方式がサポートされ、SMI、プロトコル動作、管理アーキテクチャ、およびセキュリティが改善されています。

SPAN スイッチド ポート アナライザ。Catalyst 5000 スイッチの機能。既存のネットワーク アナライザのモニタリング機能をスイッチ型イーサネット環境に拡張します。SPAN は、1 つのスイッチド セグメントのトラフィックを事前定義済みの SPAN ポートにミラーリングします。SPAN ポートに接続されたネットワーク アナライザで、その他の任意の Catalyst スイッチド ポートからのトラフィックをモニタできます。

SQL 構造化照会言語。リレーショナル データベースの定義およびアクセスに使用される国際的な標準言語。

SRAM 電源が供給される限り内容を保持する RAM のタイプ。SRAM は、DRAM のように継続的な更新は必要ありません。

SSH Secure Shell（セキュア シェル）。強力な認証と安全な通信を使用してネットワーク上の別のコンピュータにログインするユーティリティ。

SSL Secure Socket Layer。e- コマースにおけるクレジットカード番号の転送など、安全なトランザクションを提供するために使用されるインターネット用暗号化テクノロジー。

Stacheldraht ICMP プロトコルに依存する DDoS ツール。

State エンジン HTTP 文字列のステートフル検索。

String エンジン シグニチャ エンジンの 1 つ。正規表現ベースのパターン検査、および、TCP、UDP、ICMP などの複数の転送プロトコルのアラート機能を提供します。

SYN フラッド プロトコルの実装で処理可能な数を超える多数の TCP SYN パケット（接続開始時に使用されるシーケンス番号の同期化要求）をホストに送信する DoS 攻撃。

T

TAC Cisco Technical Assistance Center。世界には、4 つの TAC があります。

TACACS+ Terminal Access Controller Access Control System Plus（ターミナル アクセス コントローラ アクセス コントロール システム プラス）。シスコが強化した専用の Terminal Access Controller Access Control System（TACACS）。認証、許可、アカウンティングに追加サポートを提供します。

TCP 伝送制御プロトコル。信頼性の高い全二重データ伝送を可能にする、コネクション型トランスポート層プロトコル。TCP は TCP/IP プロトコル スタックの一部です。

TCP リセット インターフェイス TCP リセットを送信できる IDSM-2 上のインターフェイス。ほとんどのセンサーでは、パケットがモニタされている検知インターフェイスで TCP リセットが送信されますが、IDSM-2 では、検知インターフェイスを TCP リセットの送信に使用することができません。IDSM-2 の場合、TCP リセット インターフェイスは、Catalyst ソフトウェアでポート 1 として指定され、Cisco IOS ソフトウェアのユーザには表示されません。TCP リセット アクションは、TCP ベースのサービスに関連するシグニチャ上のアクションとして選択したときだけ有効なアクションとなります。

TCPDUMP TCPDUMP ユーティリティは、フリーの UNIX および Windows 用ネットワーク プロトコル アナライザです。これを使用すると、稼動中のネットワークのデータ、またはディスク上のキャプチャ ファイルのデータを検査できます。さまざまなオプションを使用して、各パケットの要約情報と詳細情報を表示できます。詳細については、http://www.tcpdump.org/ を参照してください。

Telnet TCP/IP プロトコル スタックにおける標準の端末エミュレーション プロトコル。Telnet はリモート端末接続に使用され、ユーザはこれを使用してリモート システムにログインし、そのリソースを、ローカル システムに接続されているかのように使用することができます。Telnet は RFC 854 で定義されています。

TFN Tribe Flood Network。偽装の送信元 IP アドレスやすぐに変更される送信元 IP アドレスを使用して、攻撃を突き止めたりフィルタリングしたりする手段を妨げることができる一般的な DoS 攻撃。

TFN2K Tribe Flood Network 2000。偽装の送信元 IP アドレスやすぐに変更される送信元 IP アドレスを使用して、攻撃を突き止めたりフィルタリングしたりする手段を妨げることができる一般的な DoS 攻撃。

TFTP 簡易ファイル転送プロトコル。FTP の単純なバージョンで、1 つのコンピュータから別のコンピュータに、通常はクライアント認証（ユーザ名とパスワードなど）を使用せずにネットワークを介してファイルを転送できます。

TLS Transport Layer Security。ピアの ID をネゴシエートし、暗号化通信を確立するために、ストリーム転送で使用されるプロトコル。

TNS Transparent Network Substrate。データベース アプリケーションに、すべての業界標準ネットワーク プロトコルに対する 1 つの共通インターフェイスを提供します。TNS により、データベース アプリケーションは、異なるプロトコルを使用して他のデータベース アプリケーションにネットワークから接続できます。

TPKT トランスポート パケット。RFC 1006 で定義された、パケット内のメッセージの境界を区切る方法。プロトコルでは、TCP の上で ISO トランスポート サービスを使用します。

traceroute 多くのシステム上で使用できる、パケットが宛先まで通るパスを追跡するプログラム。ほとんどの場合、ホスト間のルーティングの問題のデバッグに使用されます。traceroute プロトコルは RFC 1393 でも定義されています。

Traffic ICMP エンジン TFN2K、LOKI、DDOS などの非標準プロトコルを分析します。

Trojan エンジン BO2K や TFN2K などの非標準プロトコルからのトラフィックを分析します。

U

UDI Unique Device Identifier。すべてのシスコ製品に一意の ID を提供します。UDI は、PID、VID、および SN で構成されています。UDI は、Cisco IPS ID PROM に格納されます。

UDLD 単一方向リンク検出。LAN ポートに接続された光ファイバまたは銅製イーサネット ケーブルを使用して接続されたデバイスで、ケーブルの物理構成をモニタし、単一方向リンクの存在を検出することができるシスコ独自のプロトコルです。単一方向のリンクはスパニング ツリー トポロジ ループなど、さまざまな問題の原因となる可能性があるため、単一方向のリンクが検出された場合、UDLD は影響を受けた LAN ポートをシャットダウンしてアラートを送信します。

UDP ユーザ データグラム プロトコル。TCP/IP プロトコル スタックのコネクションレス型トランスポート層プロトコルです。UDP は、確認応答や配信保証なしでデータグラムを交換する単純なプロトコルです。エラー処理と再送信は、他のプロトコルで処理する必要があります。UDP は RFC 768 で定義されています。

UPS 無停電電源装置。

UTC Coordinated Universal Time（協定世界時）。経度が 0 度のタイムゾーン。旧名称はグリニッジ標準時（GMT）およびズールー時。

UTF-8 8 ビットの Unicode Transformation Format。Unicode の可変長文字エンコーディング。UTF-8 は、Unicode 文字セットのすべての文字を表すことができ、ASCII と下位互換性があります。

V

VACL VLAN ACL。スイッチを経由して渡されるすべてのパケット（VLAN 内および VLAN 間）をフィルタする ACL。セキュリティ ACL とも言います。

VID バージョン ID。UDI に含まれます。

VIP Versatile Interface Processor。Cisco 7000 および Cisco 7500 シリーズ ルータで使用されるインターフェイス カード。VIP は、マルチレイヤ スイッチングを行い、Cisco IOS を実行します。VIP の最新バージョンは VIP2 です。

VLAN バーチャル LAN（Virtual Local Area Network）。（管理ソフトウェアを使用して）設定された 1 つ以上の LAN 上のデバイス グループ。実際には多数の異なる LAN セグメントに配置されている場合でも、同じケーブルに接続されているかのように通信できます。VLAN は物理接続ではなく論理接続に基づいているため、柔軟性がとても高い機能です。

VMS CiscoWorks VPN/Security Management Solution。さまざまな Web ベース ツールを組み合わせた、ネットワーク セキュリティ アプリケーション スイート。これらのツールは、エンタープライズ VPN、ファイアウォール、ネットワーク侵入検知システム、およびホストベースの侵入防御システムを構成、管理、およびトラブルシューティングするために使用できます。

VoIP Voice over IP。POTS のような機能、信頼性、および音声品質を備えながら、IP ベースのインターネット上で通常のテレフォニー スタイルの音声を伝送する機能。VoIP を使用すれば、ルータから IP ネットワーク上で音声トラフィック（通話や FAX など）を伝送できます。VoIP では、DSP が音声信号をフレームに分割します。その後、フレームは、2 つずつ連結され、音声パケットに保存されます。これらの音声パケットは、ITU-T 仕様の H.323 に従って、IP を使用して送信されます。

VPN バーチャル プライベート ネットワーク（ネットワーキング）ネットワーク間のトラフィックをすべて暗号化することにより、パブリック TCP/IP ネットワーク経由でも IP トラフィックをセキュアに転送できます。VPN では、「トンネリング」が使用され、すべての情報が IP レベルで暗号化されます。

VTP VLAN トランキング プロトコル。ネットワーク全体で VLAN の追加、削除、および名前の変更を管理するシスコのレイヤ 2 メッセージング プロトコル。

VTP VLAN トランキング プロトコル。ネットワーク全体で VLAN の追加、削除、および名前の変更を管理するシスコのレイヤ 2 メッセージング プロトコル。

W

WAN Wide-Area Network（ワイドエリア ネットワーク）。広範な地理的領域に分散するユーザにサービスを提供し、多くの場合、共通の通信事業者が提供する送信デバイスを使用するデータ通信ネットワークです。フレームリレー、SMDS、および X.25 が WAN の代表例です。

Web サーバ IPS のコンポーネントの 1 つ。リモート HTTP クライアント要求を待機し、適切なサーブレット アプリケーションを呼び出します。

WHOIS ドメイン名または IP アドレスの所有者を特定する公式データベースへのクエリーに使用される TCP ベースのクエリー / 応答プロトコル。

Wireshark Wireshark は、フリーの Unix および Windows 用ネットワーク プロトコル アナライザです。これを使用すると、稼動中のネットワークのデータ、またはディスク上のキャプチャ ファイルのデータを検査できます。対話的にキャプチャ データをブラウズし、各パケットの要約情報と詳細情報を表示できます。Wireshark には、機能豊富な表示フィルタ言語や TCP セッションの再構築されたストリームの表示機能など、いくつかの強力な機能があります。詳細については、http://www.wireshark.org を参照してください。

X

X.509 証明書に含まれる情報を定義する標準。

XML eXtensible Markup Language。異種ホスト間のデータ交換に使用されるテキスト ファイル形式。

XPI クロス パケット インスペクション。複数のパケットにわたって検索し、パケットおよびペイロードの再構成を行える、TCP で使用されているテクノロジー。

あ

アーキテクチャ コンピュータまたは通信システムの全体的な構造。アーキテクチャはシステムの機能と制限に影響を与えます。

アクション イベントに対するセンサーの応答。アクションは、イベントがフィルタ処理されない場合にだけ発生します。TCP リセット、ホストのブロック、接続のブロック、IP ログ収集、アラート トリガー パケットのキャプチャなどがあります。

アクティブ ACL ARC によって作成、管理される ACL。ルータのブロック インターフェイスに適用されます。

アスペクト バージョン IDIOM のデフォルト コンフィギュレーション設定と関連付けられたバージョン情報。たとえば、シスコは攻撃シグニチャの標準セットを、S アスペクトのデフォルト設定の集合として公開しています。S アスペクトのバージョン番号は、シグニチャ更新パッケージ ファイル名では S の後ろに表示されます。その他のアスペクトとしては、ウィルス シグニチャ定義を含む V アスペクト、IDIOM 署名キーを含むキーアスペクトがあります。

宛先アドレス データを受信するネットワーク デバイスのアドレス。

アトミック アタック 1 つのパケット内に含まれる悪用を表します。たとえば、"ping of death" 攻撃は、単一の異常に大きな ICMP パケットです。

アプリケーション Cisco IPS 環境で動作するように設計された任意のプログラム（プロセス）。

アプリケーション イメージ センサーの操作に使用される永続的なストレージ デバイスに格納される完全な IPS イメージ。

アプリケーション インスタンス IPS 環境の特定のハードウェアで動作する特定のアプリケーション。アプリケーション インスタンスには、その名前と、ホスト コンピュータの IP アドレスによってアドレス可能です。

アプリケーション パーティション IPS ソフトウェア イメージを含むブート可能ディスクまたはコンパクトフラッシュ パーティション。

アラート 厳密には IPS のイベント タイプの 1 つを指し、evAlert としてイベント ストアに書き込まれます。一般に、アラートは、ネットワークの不正使用が進行中であるか、潜在的なセキュリティの問題が発生していることを示す IPS メッセージです。アラームとも言います。

アラーム チャネル インスペクタによって生成されたすべてのシグニチャ イベントを処理する IPS ソフトウェア モジュール。主な機能は、受信した各イベントに対するアラートの生成です。

暗号化 データに特殊なアルゴリズムを適用してそのデータの外見を変更し、その情報を読む許可を与えられていないユーザには理解できないようにすること。

暗号キー クリア テキストと暗号文の間の変換に使用されるシークレット バイナリ データ。暗号化と復号化に同じ暗号キーが使用される場合を対称と言います。暗号キーが暗号化と復号化のいずれかに使用される（両方ではない）場合を非対称と言います。

い

異常検出 AD。正常なネットワーク トラフィックのベースラインを作成し、そのベースラインを使用してワームに感染したホストを検出するセンサー コンポーネント。

イベント アラート、ブロック要求、ステータス メッセージ、またはエラー メッセージを含む IPS メッセージ。

イベント ストア IPS のコンポーネントの 1 つ。IPS イベントの格納に使用される、固定サイズのインデックス付きストア。

インライン インターフェイス センサーが 1 つのインターフェイスで受け取ったすべてのトラフィックをペアの他方のインターフェイスに転送するように設定された物理インターフェイスのペア。

インライン モード ネットワークに出入りするすべてのパケットがセンサーを通過する必要があります。

う

ウィルス コンピュータ ソフトウェアの隠された、自己複製セクション。通常、感染によって伝播する悪意のあるロジックです。自分自身のコピーを別のプログラムに挿入し、その一部となります。ウィルスは自力では実行できません。ウィルスをアクティブにするには、ホスト プログラムを実行する必要があります。

ウィルス更新 特にウィルスに対応したシグニチャ更新。

ウォッチ リスト レーティング WLR。0 ～ 100 の範囲で CSA MC ウォッチ リストに関連付けられる重み（CSA MC は 0 ～ 35 の範囲のみを使用します）。

え

エスケープ表現 正規表現で使用されます。各文字は、それぞれに対応する 16 進数値で表現できます。たとえば、¥x61 は「a」に対応しているので、文字列「a」を表すエスケープ表現は ¥x61 になります。

エンジン センサーのコンポーネントの 1 つ。特定の 1 つのカテゴリで多数のシグニチャをサポートするように設計されています。各エンジンには、シグニチャの作成や既存のシグニチャの調整に使用できるパラメータがあります。

エンタープライズ ネットワーク 企業などの組織内で大部分の主要ポイントを接続する、大規模で多様なネットワーク。私的に所有され、保守される点で WAN とは異なります。

か

仮想化された検知インターフェイス 仮想化されたインターフェイスはサブインターフェイスに分割され、各サブインターフェイスは VLAN のグループで構成されます。1 つ以上のサブインターフェイスに 1 つの仮想センサーを関連付け、それらのサブインターフェイスに異なる侵入防止ポリシーを割り当てることができます。物理インターフェイスとインライン インターフェイスの両方を仮想化できます。

仮想化されていない検知インターフェイス 仮想化されていない検知インターフェイスは、サブインターフェイスに分割されず、インターフェイス全体を 1 つの仮想センサーだけに関連付けることができます。

仮想センサー シグニチャ エンジンのセンシング インターフェイスと設定ポリシー、およびシグニチャ エンジンに適用するアラーム フィルタの論理グループ。つまり、それぞれが異なるシグニチャの動作とトラフィック供給で設定された、同一アプライアンス上で動作する複数の仮想センサーです。

カットスルー アーキテクチャ カットスルー アーキテクチャとは、パケットスイッチング システムの設計方法の 1 つです。パケットがスイッチに到達すると、パケット内の最初の数バイトのみを読み取って宛先アドレスを確認し、ほぼ瞬時にパケットの転送を開始します。この手法はパフォーマンスを向上させます。

き

偽陰性 不正なトラフィックが検出されたときにシグニチャが起動されない状態。

偽陽性 正常なトラフィックまたは良好なアクションによってシグニチャが起動される状態。

脅威レーティング TR。脅威レーティングは、モニタ対象のネットワークでアラートの脅威を示す応答アクションに基づいて、攻撃のリスク レーティングの数値的な減少を表す 0 ～ 100 の値です。

共有秘密情報 セキュア通信に関わる当事者のみが知っているデータ。共有秘密には、パスワード、パスフレーズ、大きな数、ランダムに選択したバイトの配列などがあります。

拒否フィルタ プロセッサ IPS のプロセッサ。攻撃者拒否機能を処理します。拒否されたソース IP アドレスのリストを維持します。

く

グローバル相関 IPS センサーは、グローバル相関データベースを通して他のデバイスと情報を共有し、すべてのデバイスの有効性を総合的に向上させます。

グローバル相関クライアント 更新を取得し、ローカル グローバル相関データベースにインストールする CollaborationApp のソフトウェア コンポーネント。

グローバル相関データベース IPS センサーなどのコラボレーション デバイスから取得され、これらの間で共有される情報の集合。

こ

攻撃 知的脅威から発生するシステム セキュリティへの攻撃。セキュリティ サービスを回避してシステムのセキュリティ ポリシーを妨害するために、（特に方法や技術に関して）用意周到に計画したうえで試みられた知的行為を意味します。

攻撃関連性レーティング ARR。ターゲット OS の関連性に関連付けられた重み。攻撃関連性レーティングは取得値（関連性あり、不明、関連性なし）で、アラート時に決定されます。関連する OS はシグニチャごとに設定されます。

攻撃重大度レーティング ASR。脆弱性の悪用が成功した場合の重大度に関連付けられた重み。攻撃重大度レーティングは、シグニチャのアラート重大度パラメータ（informational、low、medium、または high）から計算されます。攻撃重大度レーティングはシグニチャごとに設定され、検出されたイベントどれだけ危険かを示します。

コマンド / コントロール インターフェイス IPS マネージャなどのネットワーク デバイスと通信する、センサー上のインターフェイス。このインターフェイスには IP アドレスが割り当てられています。

コミュニティ SNMP における、同じ管理ドメイン内の管理対象デバイスと NMS の論理グループ。

混合モード ネットワーク セグメントのパケットをモニタするパッシブ インターフェイス。検知インターフェイスには IP アドレスが割り当てられず、攻撃者に見えません。

コンソール センサーのモニタと制御に使用される端末またはラップトップ コンピュータ。

コンソール ポート センサーでコンソール デバイスへの接続に使用される、RJ45 シリアル ポートまたは DB9 シリアル ポート。

さ

サービス パック 不具合の修正のリリースおよび新しいシグニチャ エンジンのサポートに使用されます。サービス パックには、最後のベース バージョン（マイナーまたはメジャー）以降のすべての不具合の修正と新しい不具合の修正が含まれます。

再構成 ソースまたは中間ノードでフラグメント化された IP データグラムを宛先で元に戻すこと。

再パッケージ リリース パッケージングまたはインストーラの不具合に対処したリリース。

サブシグニチャ 一般のシグニチャより細分化されたシグニチャ。通常は、より広い範囲のシグニチャをさらに定義します。

し

時間プロセッサ IPS のプロセッサ。タイムスライス カレンダーに格納されたイベントを処理します。主なタスクは、古いデータベース エントリを有効期限切れにすることと時間に依存する統計情報を計算することです。

しきい値 アラームが送信されるまでに許容される最大 / 最小の条件を定義する、上限または下限の値。

シグニチャ シグニチャはネットワーク情報を抽出し、典型的な侵入アクティビティを示すルール セットと比較します。

シグニチャ アップデート ワーム、DDOS、ウィルスなどの悪意のあるネットワーク アクティビティを認識するためのルール セットを含む実行可能ファイル。シグニチャ更新は独立してリリースされ、必要なシグニチャ エンジン バージョンに依存し、独自のバージョニング スキームを持ちます。

シグニチャ イベント アクション オーバーライド リスク レーティング値に基づいてアクションを追加します。シグニチャ イベント アクション オーバーライドは、設定されたリスク レーティングしきい値の範囲に入るすべてのシグニチャに適用されます。各シグニチャ イベント アクション オーバーライドは独立し、アクション タイプごとに別々の設定値を持ちます。

シグニチャ イベント アクション ハンドラ 要求されたアクションを実行します。シグニチャ イベント アクション ハンドラからの出力は、実行されているアクションと、イベント ストアに書き込まれる evIdsAlert（ある場合）です。

シグニチャ イベント アクション フィルタ シグニチャ イベントのシグニチャ ID、アドレス、リスク レーティングに基づいてアクションを差し引きます。シグニチャ イベント アクション フィルタへの入力は、シグニチャ イベントアクション オーバーライドによって追加された可能性のあるアクションを含むグニチャ イベントです。

シグニチャ イベント アクション プロセッサ イベント アクションを処理します。イベント アクションは、イベント リスク レーティングのしきい値と関連付けることができます。アクションが発生するには、この値を上回る必要があります。

シグニチャ エンジン センサーのコンポーネントの 1 つ。特定のカテゴリで多数のシグニチャをサポートします。エンジンは、パーサーとインスペクタで構成されています。各エンジンには規定のパラメータのセットがあり、パラメータには使用可能な範囲や値のセットがあります。

シグニチャ エンジンのアップデート 新しいシグニチャ アップデートをサポートするバイナリ コードを含む、独自のバージョニング スキームを持つ実行可能ファイル。

シグニチャ忠実度レーティング SFR。ターゲットに関する具体的な情報がない場合に、シグニチャをどの程度忠実に実行するかに関連付ける重みを示します。シグニチャ忠実度レーティングはシグニチャごとに設定され、シグニチャが、それが表しているイベントまたは条件をどれだけ正確に検出するかを示します。

シグニチャ分析プロセッサ IPS のプロセッサ。処理中のパケットを対象とするように設定された、ストリームベースではないインスペクタにパケットを発送します。

システム イメージ センサー全体のイメージの再作成に使用される、IPS アプリケーションとリカバリの完全なイメージ。

自動ステート 通常自動ステート モードでは、VLAN 上のポートが少なくとも 1 つアップしていると、レイヤ 3 インターフェイスはアップしたままになります。VLAN 上のポートにロード バランサやファイアウォール サーバなどのアプライアンスが接続されている場合、これらのポートを自動ステート機能から除外するように設定して、これらのポートが非アクティブの場合でも転送 SVI がダウンしないようにすることができます。

出力 ネットワークを離れるトラフィック。

証明書 公開キーなどのユーザまたはデバイス属性のデジタル表現であり、信頼できる秘密キーで署名されています。

侵入検知システム IDS。不正な方法によるシステム リソースへのアクセスの試みを発見し、リアルタイムまたはそれに近い形で警告を与えることを目的として、システム イベントのモニタと分析を行うセキュリティ サービス。

信頼できるキー ユーザが信頼する公開キー。特に、認証パスで最初の公開キーとして使用される公開キーです。

信頼できる証明書 証明書のユーザが検証テストなしで有効であると信頼する証明書。特に、認証パスで最初の公開キーの提供に使用される公開キー証明書です。

す

スイッチ 各フレームの宛先アドレスに基づいて、フレームのフィルタリング、転送、およびフラッディングを行うネットワーク デバイス。スイッチは、OSI モデルのデータリンク層で動作します。

据え置き 平らな面に設置する場合にセンサー底部にゴム脚を取り付けます。ゴム脚を使用すると、センサーの周りに適正なエアーフローが確保され、振動を吸収するので、ハードディスク ドライブへの衝撃が軽減されます。

ストリーム再構成プロセッサ IPS のプロセッサ。さまざまなストリームベース インスペクタでのパケットが正しい順序で到着するように TCP ストリームの順序を変更します。TCP ストリームの正規化も行います。Normalizer エンジンでは、アラート アクションと拒否アクションをイネーブルまたはディセーブルにできます。

スニファ インターフェイス 「センシング インターフェイス」を参照。

スパニング ツリー ネットワーク トポロジのループのないサブセット。

スリーウェイ ハンドシェイク 2 つのプロトコル エンティティが接続の確立中に同期するプロセス。

スレーブ ディスパッチ プロセッサ IPS のプロセッサ。デュアル CPU システムで見られるプロセス。

せ

正規表現 データ ストリームまたはファイル内で指定された文字シーケンスを検索する方法を定義できるメカニズム。正規表現は高機能かつ柔軟な表記法で、テキストを表現するためのミニ プログラミング言語のようなものです。パターン マッチングでは、正規表現によりあらゆる任意のパターンを簡潔に表記できます。

制御インターフェイス ARC では、ネットワーク デバイスと Telnet セッションまたは SSH セッションを開くときに、そのデバイスのルーティング インターフェイスの 1 つがリモート IP アドレスとして使用されます。これが制御インターフェイスです。

制御トランザクション CT。特定のアプリケーション インスタンスに対して出されたコマンドを含む IPS メッセージ。制御トランザクションは、管理アプリケーションと IPS センサー間、または同じ IPS センサー上のアプリケーション間で送信できます。制御トランザクションには、*start*、*stop*、*getConfig* などがあります。

脆弱性 コンピュータやネットワークの悪用パターンが開始されやすい状況を許す、当該コンピュータやネットワークの 1 つ以上の属性。

製造イメージ 製造によってイメージ センサーに使用される完全な IPS システム イメージ。

セキュア シェル プロトコル 伝送制御プロトコル（TCP）アプリケーションを介して、ルータへのセキュア リモート接続を提供するプロトコルです。

セキュリティ コンテキスト 1 つの適応型セキュリティ アプライアンスは複数の仮想デバイスに分割できます。これをセキュリティ コンテキストと呼びます。各コンテキストは、独自のセキュリティ ポリシー、インターフェイス、および管理者を持つ独立したデバイスです。マルチコンテキストは、複数のスタンドアロン デバイスを使用することに似ています。マルチコンテキスト モードでは、ルーティング テーブル、ファイアウォール機能、IPS、管理など、多くの機能がサポートされます。

接続ブロック 特定の送信元 IP アドレスから特定の宛先 IP アドレスおよび宛先ポートへのトラフィックをブロックします。

センサー 侵入検知エンジンのことです。不正行為の兆候を探してネットワーク トラフィックを分析します。

センシング インターフェイス 目的のネットワーク セグメントをモニタする、センサー上のインターフェイス。センシング インターフェイスは、混合モードです。つまり、IP アドレスを持たず、モニタしたセグメント上では見えません。

全二重 送信ステーションと受信ステーション間でデータを同時伝送する機能。

そ

送信元アドレス データを送信するネットワーク デバイスのアドレス。

ゾーン 異常検出で使用される、内部、不正、または外部ゾーンにソートされる宛先 IP アドレスのセット。

ソフトウェア バイパス 検査なしでトラフィックを IPS システム経由で通過させます。

た

ダークネット ユーザが信頼する人々とのみ接続する仮想プライベート ネットワーク。一般に、ダークネットは通信する人々の閉じた、プライベートな任意のタイプのグループを意味しますが、多くの場合、特にファイル共有ネットワークに使用されます。すべての秘密の通信ネットワークに対して集合的に使用されることもあります。

ターゲットの価値レーティング TVR。ターゲットの認識値に関連付けられた重み。ターゲットの価値レーティングはユーザ設定可能な値（zero、low、medium、high、または mission critical）であり、ネットワーク資産の IP アドレスを通じてその重要性を表します。

ターミナル サーバ 他のシリアル デバイスに接続された複数の低速な非同期ポートを搭載したルータ。ターミナル サーバは、センサーを含むネットワーク機器をリモートで管理する場合に利用できます。

単一方向リンク検出 「UDLD」を参照してください。

ち

チューニング シグニチャ パラメータを調整して既存のシグニチャを変更すること。

て

データグラム 事前に仮想回線を確立することなく、伝送媒体上のネットワーク層ユニットとして送信される情報の論理的なグループ化。IP データグラムは、インターネットにおける主な情報単位です。セル、フレーム、メッセージ、パケット、セグメントという用語も、OSI 参照モデルのさまざまなレイヤとさまざまなテクノロジー領域で、情報の論理的なグループ化を表すために使用されます。

データベース プロセッサ IPS のプロセッサ。シグニチャの状態とフロー データベースを管理します。

適応型セキュリティ アプライアンス ASA。ファイアウォール、VPN コンセントレータ、および侵入防御ソフトウェア機能が 1 つのソフトウェア イメージに結合されています。適応型セキュリティ アプライアンスは、シングル モードまたはマルチモードで設定できます。

と

統計プロセッサ IPS のプロセッサ。パケット数やパケット到着レートなどのシステム統計情報を記録します。

トポロジ 企業ネットワーキング構造内のネットワーク ノードおよびメディアの物理的な配置。

トラップ 特別に定義された状況やしきい値の到達などの重要なイベントの発生を知らせるために、SNMP エージェントから NMS、コンソールまたは端末に送信されるメッセージ。

トラフィック分析 データが暗号化されている場合、または直接使用可能でない場合にも、データ フローの観測可能な特徴から情報を推理すること。このような特徴には、発信元と宛先（複数の場合もある）の ID と場所や、事象の存在、回数、頻度、期間などがあります。

トランク ネットワーク トラフィックが移動する 2 つのスイッチ間の物理および論理接続。バックボーンは多数のトランクで構成されています。

な

ナレッジ ベース 「KB」を参照してください。

に

認証 ユーザがシステムを使用する権限を持っていることを確認する処理。通常はパスワード キーまたは証明書によって行われます。

ね

ネイバー検索 IPv6 のプロトコル。同じリンク上の IPv6 ノードは、ネイバー検索を使用して相手の存在の検出、相手のリンク層アドレスの特定、ルータの検索、アクティブ ネイバーへのパスに関する到達可能性情報の維持を行います。

ネットワーク アクセス ID 「NAS-ID」を参照してください。

ネットワーク参加 グローバル相関データベースに学習した情報を提供するネットワーク。

ネットワーク参加クライアント SensorBase ネットワークにデータを送信する CollaborationApp のソフトウェア コンポーネント。

ネットワーク デバイス ネットワーク上の IP トラフィックを制御し、攻撃元ホストをブロックできるデバイス。ネットワーク デバイスには、Cisco ルータや PIX Firewall などがあります。

の

ノード コマンド / コントロール ネットワーク上の物理的な通信要素。たとえば、アプライアンス、IDSM-2、またはルータを指します。

は

ハードウェア バイパス 物理インターフェイスをペアにする特殊なインターフェイス カード。ソフトウェア エラーが検出されると、物理インターフェイスを直接接続し、トラフィックがペアを通過できるようにするバイパス メカニズムを起動します。ハードウェア バイパスは、ネットワーク インターフェイスでトラフィックを通過させますが、IPS システムへは渡しません。

バイパス モード センサーが失敗した場合でも、引き続きセンサーからパケットを通過させるモード。バイパス モードは、インラインペア インターフェイスにのみ適用されます。

パケット 情報を論理的にグループ化したもの。制御情報が格納されたヘッダーと、（通常は）ユーザ データが含まれています。パケットは、ほとんどの場合ネットワーク層のデータの単位を表します。データグラム、フレーム、メッセージ、セグメントという用語も、OSI 参照モデルのさまざまなレイヤとさまざまなテクノロジー領域で、情報の論理的なグループ化を表すために使用されます。

バックプレーン シャーシ内でのインターフェイス プロセッサまたはカードとデータ バスおよび配電バス間の物理接続。

パッシブ OS フィンガープリント センサーは、ネットワークで交換されるパケットの特性を検査することで、ホストのオペレーティング システムを特定します。

パッシブ フィンガープリント システムで使用できる OS やサービスをネットワーク対話のパッシブな観察から決定すること。

パッチ リリース ソフトウェア リリース（サービス パック、マイナー、またはメジャー更新）のリリース後に更新（マイナー、メジャー、またはサービス パック）バイナリで特定された不具合を解決するリリース。

ハンドシェイク 複数のネットワーク デバイス間で、伝送の同期を確認するために交換される一連のメッセージ。

半二重 送信ステーションと受信ステーション間で、一度に 1 方向にのみデータ転送できる機能。BSC は、半二重プロトコルの一例です。

ふ

ブートローダ システムの電源投入時に読み込まれるソフトウェアの小セット。（ディスク、ネットワーク、外部のコンパクト フラッシュや外部の USB フラッシュ メモリから）オペレーティング システムをロードし、そのオペレーティング システムが IPS アプリケーションをロード、実行します。AIM-IPS の場合、モジュールをネットワークから起動し、モジュールがソフトウェアにアクセスできないときに、ソフトウェアのインストールとアップグレード、ディザスタ リカバリ、その他の動作を補助します。

ファイアウォール 接続されている任意のパブリック ネットワークおよびプライベート ネットワーク間でバッファとして設計された、1 つのルータまたはアクセス サーバ、または複数のルータまたはアクセス サーバ。ファイアウォール ルータは、アクセス リストや他の方法を使用して、プライベート ネットワークのセキュリティを確保します。

ファスト イーサネット 各種 100 Mbps イーサネット仕様のいずれか。ファスト イーサネットは、10BASE-T イーサネット仕様の 10 倍の速度を実現し、フレーム フォーマット、MAC メカニズム、MTU などの品質を維持します。その類似性により、ファスト イーサネット ネットワーク上で既存の 10BaseT アプリケーションおよびネットワーク管理ツールを使用できます。IEEE 802.3 仕様の拡張に基づいています。

フェール オープン ハードウェア障害後にデバイスからトラフィックを通過させます。

フェール クローズ ハードウェア障害後にデバイスでのトラフィックをブロックします。

フォワーディング インターネットワーキング デバイス経由でフレームを最終宛先に送信するプロセス。

複合攻撃 1 つのセッションの複数のパケットにわたって影響します。FTP、Telnet などのほとんどのカンバセーション攻撃とほとんどの正規表現ベースの攻撃が含まれます。

プラグイン可能な認証モジュール 「PAM」を参照してください。

フラグメンテーション 元のパケット サイズをサポートできないネットワーク メディアを介してパケットを送信するときに、パケットを小さい単位に分割するプロセス。

フラグメント 小さな単位に分割された大きなパケットの一部。

フラグメント再構成プロセッサ IPS のプロセッサ。フラグメント化された IP データグラムを再構成します。センサーがインライン モードの場合、IP フラグメントの正規化も行います。

ブラックホール ネットワークの一部分の悪条件またはシステム設定の不備により、パケットが入っても現れないインターネットワークの領域を表すルーティング用語。

フラッディング スイッチおよびブリッジにより使用されるトラフィック通過手法。インターフェイス上で受信されたトラフィックは、最初に情報を受信したインターフェイスを除き、そのデバイスのすべてのインターフェイスから送信されます。

ブロック 指定されたネットワーク ホストまたはネットワークから入ってくるすべてのパケットをネットワーク デバイスが拒否するように指定するセンサーの機能。

ブロック インターフェイス センサーが管理する、ネットワーク デバイス上のインターフェイス。

ブロック解除 それまで適用されていたブロックを削除するようにルータに指示すること。

分析エンジン センサー設定を処理する IPS ソフトウェア モジュール。インターフェイスとシグニチャおよびアラーム チャネル ポリシーを設定済みのインターフェイスにマッピングします。パケット分析とアラート検出を実行します。分析エンジン機能は、SensorApp プロセスによって提供されます。

へ

ベース バージョン サービス パックやシグニチャ更新などのフォローアップ リリースをインストールする前にインストールする必要があるソフトウェア リリース。メジャーおよびマイナー更新はベース バージョン リリースです。

ほ

ホスト ブロック ARC は、特定の IP アドレスからのすべてのトラフィックをブロックします。

ボットネット 自立的および自動的に実行されるソフトウェア ロボット、つまりボットの集合。多くの場合、悪意のあるソフトウェアを表す場合に使用される用語ですが、配布されたコンピューティング ソフトウェアを使用するコンピュータのネットワークを指すこともあります。ボットネットという用語は、一般的な指示管理インフラストラクチャで、通常、ワーム、トロイの木馬、バック ドアを通してインストールされたソフトウェアを実行する侵害されたコンピュータ（ゾンビ コンピュータと呼ばれる）の集合を指すときに使用されます。

ま

マイナー アップデート 製品ラインへの小規模な機能強化を含むマイナー バージョン。マイナー アップデートはメジャー バージョンに対する差分であり、サービス パックのベース バージョンです。

マスター ブロッキング センサー 1 つ以上のデバイスを制御するリモート センサーです。ブロッキング転送センサーがブロッキング要求をマスター ブロッキング センサーに送信し、マスター ブロッキング センサーがブロッキング要求を実行します。

マルウェア 不明なホストにインストールされている悪意のあるソフトウェアです。

む

無差別デルタ PD。シグニチャごとに設定される 0 ～ 30 の重み。無差別モードでは、全体的なリスク レーティングからこの値を差し引くことができます。

め

メジャー アップデート 製品の主要な新機能または大きなアーキテクチャ上の変更を含むベース バージョン。

メンテナンス パーティション IDSM2 上のブート可能ディスク パーティション。ここから、アプリケーション パーティションに IPS イメージをインストールできます。IDSM2 がメンテナンス パーティションにブートされている間、IPS 機能は使用できません。

メンテナンス パーティション イメージ IDSM2 上のメンテナンス パーティションにインストールされたブート可能ソフトウェア イメージ。メンテナンス パーティション イメージは、アプリケーション パーティションへのブート中にのみインストールできます。

も

モジュール スイッチ、ルータ、またはセキュリティ アプライアンス シャーシのリムーバブル カード。AIM IPS、AIP SSM、IDSM2、および NME IPS は IPS モジュールです。

モニタリング インターフェイス 「センシング インターフェイス」を参照。

ら

ラウンドトリップ時間 「RTT」を参照してください。

ラックマウント センサーを装置ラックに搭載すること。

り

リカバリ パッケージ アプリケーションの完全なイメージとインストーラを含む IPS パッケージ ファイル。センサーで復旧に使用されます。

リスク レーティング RR。リスク レーティングとは、ネットワーク上の特定イベントと関連付けられたリスクを数値化した 0 ～ 100 の値です。攻撃のリスクは、攻撃の重大度、忠実度、関連性、および資産価値を表し、応答または軽減アクションではありません。このリスクは、ネットワークに対する障害が大きくなるほど高くなります。

良性トリガー シグニチャは正しく起動されたけれどもトラフィックのソースに悪意がない状態。

れ

レイヤ 2 プロセッサ IPS のプロセッサ。レイヤ 2 関連イベントを処理します。また、不正な形式のパケットを識別し、処理パスから取り除きます。

レピュテーション レピュテーションとは、人間社会の場合と同様、インターネット上でのデバイスに関する評価のことです。レピュテーションを使用すると、インストール ベースの IPS センサーは、既存のネットワーク インフラストラクチャと協力してコラボレーションを行うことができるようになります。レピュテーションのあるネットワーク デバイスは、ほとんどが悪意のあるネットワーク デバイスまたは感染した可能性があるネットワーク デバイスです。

ロギング ログ ファイルに発生したアクションを収集します。セキュリティ情報のロギングは、イベント（IPS のコマンド、エラー、およびアラート）のロギングと、個々の IP セッション情報のロギングという 2 つのレベルで実行されます。

ろ

ロギング ログ ファイルに発生したアクションを収集します。セキュリティ情報のロギングは、イベント（IPS のコマンド、エラー、およびアラート）のロギングと、個々の IP セッション情報のロギングという 2 つのレベルで実行されます。

わ

ワーム 独立して実行され、自身の完全な動作バージョンをネットワーク上の他のホストに伝播させて、コンピュータ リソースを破壊的に消費することができるコンピュータ プログラム。

INDEX

数字

A

B

C

D

E

F

G

H

I

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

あ

い

う

え

か

き

く

け

こ

さ

し

す

せ

そ

た

ち

つ

て

と

な

に

ね

の

は

ひ

ふ

へ

ほ

ま

み

む

め

も

ゆ

ら

り

れ

ろ

わ