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。