

## Cisco IPS Manager Express

### 製品概要

Intrusion Prevention System (IPS; 侵入防御システム) は、ワーム、トロイの木馬や、その他の悪意のある攻撃からネットワークと資産を保護します。Cisco® IPS Manager Express (IME) は、中堅・中小企業のニーズを満たすように設計された、強力なオールインワン型の IPS 管理アプリケーションです。1つのアプリケーションで、5台の Cisco IPS センサーに対してプロビジョニング、監視、トラブルシューティング、およびレポート生成を行うことができます。Cisco IPS Manager Express は Cisco IPS ソリューションの主要なパーツで、ネットワークと資産の直感的、強力、かつ安全な保護を実現します。

- 直感的：使いやすいインターフェイスが導入と管理を簡素化します。
- 強力：ハイパフォーマンスと高度な機能が強力なセキュリティ保護を実現し、分析時間を短縮します。
- 安全：24時間体制のグローバルなセキュリティ インテリジェンス チームによって提供されるセキュリティ更新が安心をもたらします。

### 機能と利点

#### 直感的でカスタマイズ可能なダッシュボード

Cisco IPS Manager Express のダッシュボード (図 1) は、使いやすく作られています。1つのダッシュボードで、IPS センサーの健全性とネットワーク セキュリティの健全性の両方を調査できます。10 を超えるドラッグアンドドロップ ガジェットで、ダッシュボードをカスタマイズできます。ダッシュボードには設定が保存されるため、Cisco IPS Manager Express の次回起動時に同じ設定を復元できます。Live RSS (Really Simple Syndication) フィードにより、最新のセキュリティの脅威に関する情報が提供されます。

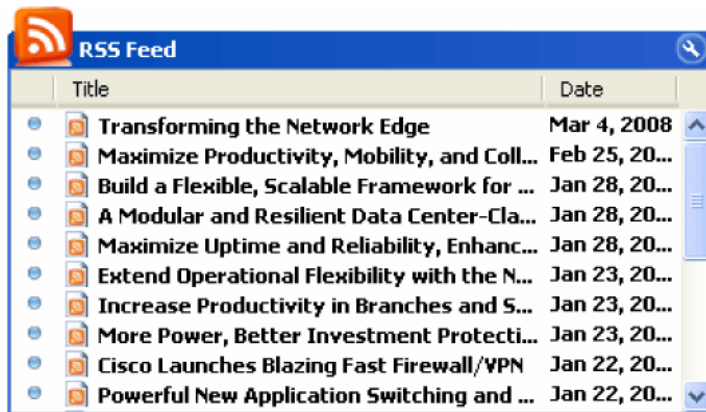
図 1 カスタマイズ可能なダッシュボード



## Live RSS フィード

Live RSS フィード（図 2）により、ネットワーク上の最新のセキュリティの脅威に関する情報が提供されます。RSS フィードは、ニーズに合わせてパーソナライズでき、また、ネットワークを保護するための推奨内容を提供できます。

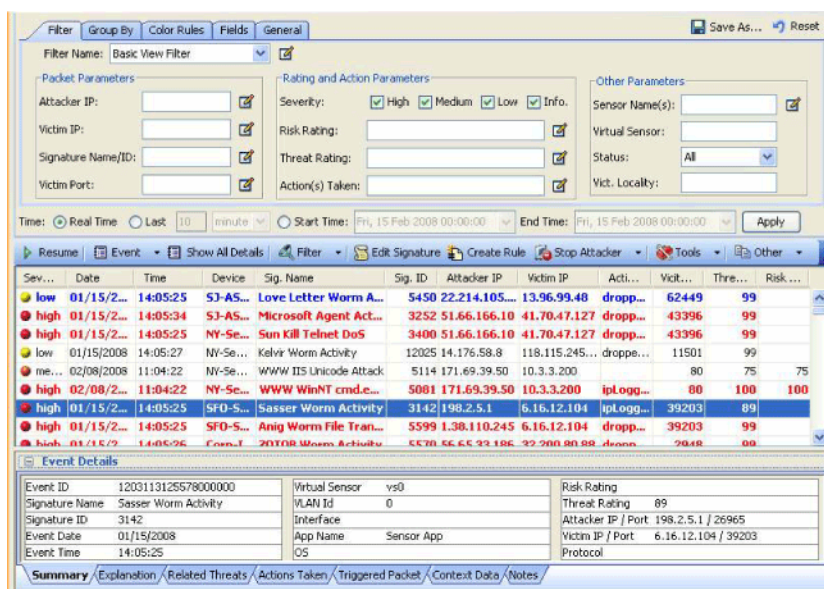
図 2 Live RSS フィード ガジェット



## Cisco IPS Manager Express Event Viewer を使用したリアルタイムおよび過去のイベントの強力な監視

Cisco IPS Manager Express は、分析とトラブルシューティングの時間を短縮するために、多くの高度なイベント監視機能を備えています。Cisco IPS Manager Express Event Viewer（図 3）を使用すると、1つのビューでリアルタイム イベントとイベントの履歴を監視できます。分析に役立つように、Cisco IPS Manager Express Event Viewer にはフィルタリング、色分け、およびグループ化の機能があります。10 を超えるパラメータを使用して、イベントを色分けまたはフィルタリングすることができます。マルチレベルのグループ化により、4レベルの階層グループ化が可能です。イベントをより深く理解できるように Event Details でイベントとシグニチャに関する情報を提供します。

図 3 Cisco IPS Manager Express Event Viewer



### 柔軟性の高いレポート作成ツール

Cisco IPS Manager Express のレポート作成ツールを使用すると、数秒でカスタム レポートや準拠レポートを生成できます。10 を超える定義済みのテンプレートから選択したり、使いやすいフィルタを使用して独自のレポートを作成することができます。レポート作成ツールを使用して、円グラフまたは棒グラフを選択できます。選択した期間に合わせてレポートをカスタマイズできます。また、IP アドレスを含むレポートを表示できます。読みやすくするために、組み込まれた DNS 解決を使用して IP アドレスを DNS 名に変換できます。すべてのレポートは、共有したり後から表示するために、印刷したり PDF または RTF 形式で保存することができます。

### 高度なポリシー プロビジョニング

Cisco IPS ポリシー プロビジョニング テーブルを使用すると、各イベントのリスク レベルを数量化するシスコの革新的な機能である Risk Rating に基づいて、ネットワーク セキュリティ ポリシーをすばやく簡単に定義することができます。Risk Rating のレンジに応じて、それぞれ異なるポリシー アクションを割り当てることができます。Risk Ratings が高いイベントからはパケットをドロップさせ、Risk Ratings が中程度であるイベントについてはユーザに警告させるように、IPS を設定することができます。また、ポリシー例外テーブルを使用すると、ポリシーに対する例外を作成することもできます。

### アプリケーション機能との緊密な統合

Cisco IPS Manager Express 内部の各アプリケーション機能が緊密に統合されることで、脅威への応答時間が短縮されます。ワンクリックで、イベントごとにイベント ビューアからポリシー テーブルまたはシグニチャ テーブルにリンクすることができます。イベント ビューアからポリシー テーブルにリンクすると、事前に蓄積されているイベント情報が表示されます。この強力なリンクにより、ポリシー プロビジョニングが簡素化され、誤操作の可能性が低くなります。ワンクリック ブロックにより、イベント ビューアから攻撃を直接停止できます。

### 直感的な Startup Wizard

Cisco IPS Manager Express Startup Wizard は、IPS センサーのセットアップを簡素化し、導入時間を短縮します。このウィザードでは、センサーが Cisco IPS 4200 シリーズ アプライアンスであっても Cisco ASA 5500 シリーズ アプライアンスの IPS モジュールであっても、IPS センサーの設定方法がステップ バイ ステップで説明されます。Cisco IPS Manager Express Startup Wizard を使用すると、IPS センサーが完全に機能するように数分間で設定できます。

### 機能の仕様

サポートされている機能を表 1 で、最小システム要件を表 2 で、サポートされている IPS センサーと IPS センサー ソフトウェアを表 3 でそれぞれ説明します。

表 1. サポートされている機能

機能	機能の説明	IPS センサー*	Cisco IOS IPS
ホームページ			
5 センサー ダッシュボード ビュー	CPU 利用率、メモリ利用率、IP アドレス、センサー健全性状態、およびライセンス有効期限を含む、主なセンサーの統計情報が一目で簡単にわかる、5 センサー ダッシュボード ビュー。	可	非対応

機能	機能の説明	IPS センサー*	Cisco IOS IPS
<b>センサー健全性メーター</b>	センサー健全性を示す直感的な3つのレベル（赤、黄、緑）のメーターにより、各センサーの健全性が一目でわかります。カスタマイズ可能な6つのパラメータのそれぞれについてしきい値を調整できるため、ユーザは組織のニーズに合わせてメーターをカスタマイズできます。	可	非対応
<b>セキュリティ健全性メーター</b>	ネットワークセキュリティ健全性ベースの Threat Rating を示す直感的な3つのレベル（赤、黄、緑）のメーター。調整可能なしきい値により、ユーザは組織のニーズに合わせてメーターをカスタマイズできます。	可	非対応
<b>カスタマイズ可能なダッシュボード</b>			
<b>健全性ガジェットおよびリアルタイムトラフィックガジェット</b>	センサー健全性統計情報およびリアルタイムトラフィック統計情報を一目でわかるようにするためのドラッグアンドドロップガジェット。 <ul style="list-style-type: none"> <li>センサー情報： <ul style="list-style-type: none"> <li>センサー健全性</li> <li>センサー情報</li> <li>CPU、メモリ、ディスク、およびセンサー負荷</li> <li>ライセンス情報</li> <li>インターフェイスの状態</li> </ul> </li> <li>リアルタイムのトラフィック統計情報： <ul style="list-style-type: none"> <li>上位アプリケーション</li> <li>ネットワークセキュリティ</li> </ul> </li> </ul>	可	非対応
<b>イベント統計情報およびセキュリティニュースガジェット</b>	イベント統計情報およびセキュリティニュースを一目でわかるようにするためのドラッグアンドドロップガジェット。 <ul style="list-style-type: none"> <li>イベント統計情報： <ul style="list-style-type: none"> <li>上位の攻撃者</li> <li>上位の被害者</li> <li>上位のシグニチャ</li> <li>一定時間内の攻撃</li> </ul> </li> <li>セキュリティニュース： <ul style="list-style-type: none"> <li>RSS フィード</li> </ul> </li> </ul>	可	可
<b>カスタマイズ可能なガジェット</b>	パーソナライズのため、およびトラブルシューティングを容易にするためのグラフ（円グラフ、棒グラフ、表）と時間間隔のカスタマイズ。	可	可
<b>ガジェットの最小化</b>	ダッシュボードのスペースを節約するためにガジェットを最小化できます。	可	可
<b>複数のダッシュボードビュー</b>	カスタマイズと柔軟性の高い表示のための複数のダッシュボードビュー。	可	可
<b>ダッシュボードビューの保存</b>	保存されたダッシュボードビューにより、Cisco IPS Manager Express の次回起動時に同じビューを表示することができます。	可	可
<b>イベントビューア</b>			
<b>リアルタイムイベントビューア</b>	リアルタイムイベント監視用のリアルタイムイベントビューア。	可	可
<b>リアルタイムイベントビューアの一時停止</b>	分析やトラブルシューティングを行うために、一時停止して前後にスクロールできます。	可	可
<b>履歴イベントビューア</b>	分析とトラブルシューティングを行うために、指定した時間間隔（日付と時刻）のイベントを表示できます。	可	可

機能	機能の説明	IPS センサー*	Cisco IOS IPS
イベントの色分け	分析とトラブルシューティングを改善するための強力なイベントの色分け（基準はシグニチャ、重大度、攻撃者/被害者の IP アドレス、被害者のポート、Risk Rating、Threat Rating、仮想センサー、センサー）。	可	可
イベントフィルタリング	分析とトラブルシューティングを簡素化するための強力なイベントのフィルタリング（基準はシグニチャ、重大度、攻撃者/被害者の IP アドレス、被害者のポート、Risk Rating、Threat Rating、仮想センサー、センサー）。	可	可
マルチレベルイベントグループ化	分析とトラブルシューティングを簡素化するための強力なマルチレベル イベントグループ化（基準はシグニチャ、重大度、攻撃者/被害者の IP アドレス、Risk Rating、Threat Rating、センサー）。	可	可
ドラッグアンドドロップ カラム	ドラッグアンドドロップ カラムにより、カラムの順序を簡単に変更したり、ビューをカスタマイズできます。	可	可
マルチカラムソート	複数のカラムを確認しやすくするために、カラムをアルファベットと数字の順番にソートできます。	可	可
カスタマイズ可能なビュー	ユーザは、分析とトラブルシューティングを簡素化するために、カスタマイズされたイベントビュー（フィルタ、色、グループ設定、およびカラム配置を含む）を作成し、保存できます。	可	可
インラインパケットデコード	Event Details で、トラブルシューティングとフォレンジック（調査）のためにインライン パケット デコードを表示できます。	可	可
Ethereal 統合サポート	Cisco IPS Manager Express は、高度なトラブルシューティングとフォレンジックを行うために、Wireshark Ethereal を統合できます。	可	可
Cisco Security Center への動的なリンク	Event Details では、Cisco Security Center からのデータに基づくイベント情報を表示して、分析とトラブルシューティングを簡素化することができます。	可	可
ポリシー テーブルへの動的なイベントリンク	ポリシー テーブルへの動的なイベント リンクにより、ポリシー例外を簡単に作成し、プロビジョニングを簡素化することができます。	可	非対応
シグニチャ テーブルへの動的なリンク	シグニチャ テーブルへの動的なイベント リンクは、シグニチャのチューニングを簡素化します。	可	非対応
ワンクリックブロック/拒否	ユーザは、イベント ビューアのボタン クリックで、攻撃者のパケットをブロックまたは拒否して、ただちに脅威を防止することができます。	可	非対応
統合されたネットワーク ツール	分析とトラブルシューティングを簡素化するために、ping、trace-route、DNS lookup、whois などのネットワーク ツールがイベント ビューアに統合されています。	可	可
イベント インシデント処理	イベント インシデント処理設定は、インシデント処理プロセスの簡素化に役立ちます。インシデント処理設定（割り当て、確認応答、クローズ）をイベントに割り当て、これらの設定に基づいてイベントをフィルタリングし、各イベントのノートを作成することができます。	可	可
イベントの保存とエクスポート	将来の分析や記録保持のために、すべてのイベントや選択したイベントを HTML または CSV に保存します。イベントを Cisco IPS Manager Express からエクスポートして、共有や記録保持に使用できます。	可	可

機能	機能の説明	IPS センサー*	Cisco IOS IPS
Events per Second (EPS) メーター	EPS は、Cisco IPS Manager Express が 1 秒間に処理するイベントの数を示します。EPS は、センサーごとに表示することもできます。	可	可
電子メール通知	電子メール通知により、離れた場所においても脅威に関する情報を知ることができます。電子メール通知の間隔、および受信するイベントを指定できます。イベントは、重大度と Risk Rating に基づいてフィルタリングできます。	可	可
データアーカイブ	カスタマイズ可能なアーカイブ スケジュールによるオンボックス データ アーカイブにより、すばやいデータ分析が可能になります。	可	可
<b>構成</b>			
ポリシープロビジョニング	Risk Rating に基づいて、ポリシーをプロビジョニングします。さまざまな Risk Rating 範囲に IPS アクションが割り当てられます。	可	非対応
ポリシー例外	Risk Rating、攻撃者の IP アドレス/ポート、被害者の IP アドレス/ポート、およびシグニチャに基づいて、ポリシー例外を定義します。	可	非対応
異常検出のプロビジョニング	異常なネットワーク動作に対してアラートを送信するようにセンサーを設定できます。Cisco Anomaly Detection は、デイゼロ攻撃に対する保護を実現します。	可	非対応
<b>シグニチャ プロビジョニング</b>			
シグニチャ アクション割り当て	シグニチャに割り当てる 14 のアクションを選択できます。これらのアクションには、パケットの拒否やアラートが含まれます。	可	非対応
シグニチャの有効化と無効化	要件に基づいてシグニチャを有効または無効にすることができます。	可	非対応
自動シグニチャ更新	セキュリティを高めたり、導入を容易にするために、センサーによってユーザ指定の時間に自動的に新しいシグニチャ更新を受信し、適用します。	可	非対応
シグニチャ ウィザード	シグニチャ ウィザードは、独自のシグニチャを作成する段階的なガイドです。	可	非対応
シグニチャ フィルタリング	シグニチャ プロビジョニングを簡素化するための (シグニチャ、重大度、忠実度、Risk Rating、およびアクションによる) 直感的なシグニチャ フィルタリング。	可	非対応
カラムのドラッグアンドドロップ	カラムのドラッグアンドドロップにより、カラムの順序を簡単に変更し、カスタマイズしたビューを使用できます。	可	非対応
カラム ソート	簡単に表示するために、カラムをアルファベットと数字の順序に基づいてソートできます。	可	非対応
シグニチャ エクスポート	シグニチャ エクスポートにより、シグニチャ テーブルを CSV (comma-separated value; カンマ区切り形式) または HTML にエクスポートできます。	可	非対応
<b>レポート機能</b>			
定義済みのレポート テンプレート	簡単にレポートを生成できる 10 を超える定義済みのレポート テンプレート。定義済みのレポート テンプレートには、過去 1 時間での上位 10 位の攻撃者、過去 1 時間での上位 10 位の被害者、および過去 1 時間での攻撃が含まれます。	可	可

機能	機能の説明	IPS センサー*	Cisco IOS IPS
カスタマイズ可能なレポート	ユーザは、指定した時間フレーム、および攻撃者の IP アドレス、被害者の IP アドレス、被害者のポート、シグニチャ、Risk Rating、Threat Rating、および行われたアクションなどのフィルタ基準に基づいて、カスタマイズされたレポートを作成できます。	可	可
カスタマイズ可能なグラフ	ユーザは、パーソナライズされたレポート用に、グラフの種類（円グラフまたは棒グラフ）を指定できます。	可	可
レポートの保存	ユーザは、準拠レポートや記録のために、レポートを PDF または RTF 形式で保存できます。	可	可
<b>セットアップとヘルプ</b>			
Startup Wizard	直感的な Startup Wizard がネットワーク設定、時間設定、およびインターフェイス構成を含む IPS の設定に関する段階的な手順を説明します。	可	非対応
管理者パスワードの必要条件	試行回数、最小文字数、最小文字種類、履歴パスワード数を含む、管理者パスワードの最低限の必要条件を指定できます。	可	非対応
ビデオ ヘルプ	ビデオ ヘルプは、Cisco IPS Manager Express の主な機能の使用法に関する段階的なビジュアルガイドです。	可	可

\*表 3 に示されている IPS センサーのみでサポートされます。

表 2. 最小システム要件

コンポーネント	最小要件
システム ハードウェア	<ul style="list-style-type: none"> <li>IBM PC 互換コンピュータ (2 GHz 以上のプロセッサ)</li> <li>1024 x 768 以上の解像度のカラー モニタ、および 16 ビット カラーが表示可能なビデオ カード</li> </ul>
ハード ドライブ	<ul style="list-style-type: none"> <li>100 GB</li> </ul>
メモリ (RAM)	<ul style="list-style-type: none"> <li>2 GB</li> </ul>
サポートされているオペレーティングシステム	<ul style="list-style-type: none"> <li>Windows Vista Business および Ultimate (32 ビットのみ)</li> <li>Windows XP Professional (32 ビットのみ)</li> <li>Windows 2003 Server</li> </ul> <p><b>メモ :</b> Cisco IPS Manager Express は、32 ビット米国英語版および日本語版の Windows をサポートします。</p>

表 3. サポートされている IPS センサーおよび IPS センサー ソフトウェア

IPS センサー	IPS センサー ソフトウェア	IPS Manager Express (IME)
<ul style="list-style-type: none"> <li>Cisco IPS 4240、4255、4260、4270</li> <li>Security Services Module 10、20、および 40 (AIP-SSM-10、AIP-SSM-20、および AIP-SSM-40)</li> <li>Cisco IPS Advanced Integration Module (AIM)</li> <li>Cisco Catalyst® 6500 シリーズ侵入検知システム (IDSM-2) サービス モジュール</li> </ul>	IPS ソフトウェアバージョン 6.1	<ul style="list-style-type: none"> <li>センサー構成</li> <li>センサー健全性ダッシュボード</li> <li>イベント ダッシュボード</li> <li>イベント監視</li> <li>レポート機能</li> <li>最大 5 デバイス</li> <li>最大 75 イベント/秒 (Events per Second[EPS])</li> </ul>
<ul style="list-style-type: none"> <li>Cisco IPS 4215、4235、4240、4250、4255、4260、4270</li> <li>Security Services Module 10、20、および 40 (AIP-SSM-10、AIP-SSM-20、および AIP-SSM-40)</li> <li>Cisco IPS Advanced Integration Module (AIM)</li> <li>Cisco Catalyst® 6500 シリーズ侵入検知システム (IDSM-2) サービス モジュール</li> <li>Cisco ネットワーク モジュール - Cisco 侵入検知システム (NM-CIDS)</li> </ul>	IPS ソフトウェアバージョン 6.0	<ul style="list-style-type: none"> <li>イベント ダッシュボード</li> <li>イベント監視</li> <li>レポート機能</li> <li>最大 5 デバイス</li> <li>最大 75 イベント/秒 (Events per Second[EPS])</li> </ul>

IPS センサー	IPS センサー ソフトウェア	IPS Manager Express (IME)
<ul style="list-style-type: none"> <li>• Cisco IPS 4210、4215、4235、4240、4250、4255、4260</li> <li>• セキュリティ サービス モジュール 10 および 20 (AIP-SSM-10 および AIP-SSM-20)</li> <li>• Cisco Catalyst® 6500 シリーズ侵入検知システム (IDSM-2) サービス モジュール</li> <li>• Cisco ネットワーク モジュール - Cisco 侵入検知システム (NM-CIDS)</li> </ul>	IPS ソフトウェアバージョン 5.1	<ul style="list-style-type: none"> <li>• イベント ダッシュボード</li> <li>• イベント監視</li> <li>• レポート機能</li> <li>• 最大 5 デバイス</li> <li>• 最大 75 イベント/秒 (Events per Second[EPS])</li> </ul>
<ul style="list-style-type: none"> <li>• Cisco IOS® IPS (サービス統合型ルータ上)</li> </ul>	12.3(14)T7、12.4(15)T2	<ul style="list-style-type: none"> <li>• イベント ダッシュボード</li> <li>• イベント監視</li> <li>• レポート機能</li> <li>• 最大 5 デバイス</li> <li>• 最大 75 イベント/秒 (Events per Second[EPS])</li> </ul>

### 発注情報

この製品には Cisco IPS ソフトウェアが同梱されています。ソフトウェアをダウンロードするには Cisco Software Center にアクセスしてください。

### 関連情報

Cisco IPS Manager Express の詳細については、<http://www.cisco.com/jp/go/ime/> にアクセスしてください。

©2008 Cisco Systems, Inc. All rights reserved.

Cisco、Cisco Systems、および Cisco Systems ロゴは、Cisco Systems, Inc. またはその関連会社の米国およびその他の一定の国における登録商標または商標です。本書類またはウェブサイトに掲載されているその他の商標はそれぞれの権利者の財産です。

「パートナー」または「partner」という用語の使用は Cisco と他社との間のパートナーシップ関係を意味するものではありません。(0704R)

この資料に記載された仕様は予告なく変更する場合があります。



シスコシステムズ合同会社

〒107-6227 東京都港区赤坂 9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先 (シスコ コンタクト センター)

<http://www.cisco.com/jp/go/contactcenter>

0120-933-122 (通話料無料), 03-6670-2992 (携帯電話, PHS)

電話受付時間: 平日 10:00 ~ 12:00, 13:00 ~ 17:00

お問い合わせ先