目次

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[表記法](#)
[IPS ハードウェア/ソフトウェアの互換性](#)
[管理オプションと設定オプション](#)
[CiscoWorks Management Center for IPS Sensors（IPS MC）](#)
[CiscoWorks Monitoring Center for Security（SecMon）](#)
[Cisco Security Monitoring Analysis and Response System（MARS）](#)
[Cisco Threat Response（CTR）](#)
[IDS Event Viewer（IEV）](#)
[IDS Device Manager（IDM）](#)
[Cisco Secure Policy Manager（CSPM）](#)
[UNIX Director](#)
[関連情報](#)

概要

このドキュメントでは、Cisco Intrusion Prevention System（IPS）アプライアンス（4210、4215、4220、4230、4235、4240、4250、4255）、適応型セキュリティ アプライアンスのセキュリティ サービス モジュール（SSM）、ルータ モジュール、Catalyst 6000 Intrusion Detection System Module（IDSM-1、IDSM-2）のハードウェアとソフトウェアの互換性一覧を提供します。 このドキュメントでは、管理オプションの概要についても説明します。 各アプリケーションの簡単な概要とバージョン互換性の一覧が提供されます。 各互換性一覧に記載されているバージョンだけがサポートされているバージョンです。

Cisco Intrusion Prevention System は、以前は Cisco Intrusion Detection System（IDS）または NetRanger と呼ばれていました。 Cisco Intrusion Prevention System アプライアンスは、センサーとも呼ばれます。 詳細については、関連製品のマニュアルとリリース ノートを参照してください。

注このドキュメント内の表の「製品のステータス」列に注意してください。 この列は、関連するサポート終了（EOL）通知または販売終了（EoS）通知を示しています。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Intrusion Prevention System（IPS）アプライアンス（4210、4215、4220、4230、4235、4240、4250、4255）
- 適応型セキュリティ アプライアンス セキュリティ サービス モジュール（SSM）
- ルータ モジュール
- Catalyst 6000 侵入検知システム モジュール（IDSM-1、IDSM-2）

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

IPS ハードウェア/ソフトウェアの互換性

表 1?Appliances

アプライアンス	部品番号	ハードウェア	オプションのインターフェイス	使用可能なその他のハードウェア	互換性のあるソフトウェアバージョン	製品のステータス
IDS-4210	IDS-4210 IDS-4210-K9 IDS-4210-NFR	ソフトウェアのアップグレードとイメージの復元に使用可能な CD-ROM 付き IDE ハード ドライブ。		IDS-4210-MEM-U = SMARTnet のお客様がバージョン 4.1 以降にアップグレードするための追加 256 MB メモリ。お客様は、	3.1 ～最新 *	販売終了日：2003 年 12 月 8 日 サポート終了日：2008 年 12 月 8 日

				Product Upgrade Tool（登録ユーザ専用）経由でメモリを注文できます。		
IDS-4215	IDS-4215-K9 IDS-4215-4FE-K9	IDE ハード ドライブと Compact Flash。 ソフトウェアのアップグレードとイメージの復元に CD-ROM ドライブは使用できません。	IDS-4FE-INT=		4.1 ～最新 *	電流
IDS-4220	IDS-4220-E	ソフトウェアのアップグレードとイメージの復元に使用可能な CD-ROM 付き IDE ハード ドライブ。		IDS-4220-MEM-U = SMARTnet のお客様がバージョン 4.1 以降にアップグレードするための追加 256 MB メモリ。お客様は、Product Upgrade Tool（登録ユーザ専	3.1 ～ 4.1	**販売終了日：** 2002 年 7 月 31 日 **サポート終了日：** 2007 年 7 月 31 日

				用）経由でメモリを注文できます。		
IDS-4230	IDS-4230-FE	ソフトウェアのアップグレードとイメージの復元に使用可能な CD-ROM 付き IDE ハード ドライブ。			3.1 ~ 4.1	**販売終了日：** 2002 年 7 月 31 日 **サポート終了日：** 2007 年 7 月 31 日
IDS-4235	IDS-4235-K9	ソフトウェアのアップグレードとイメージの復元に使用可能な CD-ROM 付き SCSI ハードドライブ。	IDS-4FE-INT=	IDS-PWR= 予備の電源	3.1 ~ 最新 *	**販売終了日：** 2005 年 5 月 31 日 **サポート終了日：** 2010 年 5 月 31 日
IPS-4240	IPS-4240-K9 IPS-4240-DC-K9（DC 電源方式、NEBS 準拠のみ）	Compact Flash。 ソフトウェアのアップグレードとイメージの復元に使用可能な CD-ROM ドライブはありません。			4.1.4 ~ 最新 *	電流

IDS-4250	IDS-4250-TX-K9 IDS-4250-SX-K9 IDS-4250-XL-K9	ソフトウェアのアップグレードとイメージの復元に使用可能な CD-ROM 付き SCSI ハードドライブ。	IDS-4FE-INT= IDS-4250-SX-INT= IDS-XL-INT=	IDS-PWR=予備の電源 IDS-SCSI=予備の SCSI ハードドライブ	3.1 ～最新 *	**TX バージョンのみの販売終了日：** 2005 年 5 月 31 日 **TX のサポート終了日：** 2010 年 5 月 31 日 他の 2 つの IDS 4250 プラットフォームはこの EoL のお知らせの影響を受けません。
IPS-4255	IPS-4255-K9	Compact Flash。 ソフトウェアのアップグレードとイメージの復元に使用可能な CD-ROM ドライブはありません。			4.1.4 ～最新 *	電流

表 2?Modules

モジュール	部品番号	ハードウェア	オプションのインターフェイス	使用可能なその他のハードウェア	互換性のあるソフトウェアバージョン	製品のステータス

SSM	ASA-SSM-AIP-10-K9（ASA AIP Security Service Module-10）ASA-SSM-AIP-20-K9（ASA AIP Security Service Module-20）	Compact Flash。 ソフトウェアのアップグレードとイメージの復元に使用可能な CD-ROM ドライブはありません。			5.0 ～最新 *	電流
ルータモジュール	NM-CIDS-K9 NM-CIDS-K9=（RMA 部品番号のみ）	Compact Flash。 ソフトウェアのアップグレードとイメージの復元に使用可能な CD-ROM ドライブはありません。			電流へのCisco IOS® ソフトウェア リリース 12.2(15)ZJ またはそれ以降 Cisco IOS ソフトウェア リリース 12.3(4)T またはそれ以降 IDS 4.1 *	電流
ID	WS-X6381-	IDE ハード ディスク。 ソフ			2.5 ～	販売

SM-1	IDS WS-X6381-IDS= (RMA 部品番号のみ)	トウェアのアップグレードまたはイメージの復元に使用可能な CD-ROM ドライブはありません。			3.0	終了日：2003 年 4 月 20 日 サポート終了日：2008 年 4 月 20 日
IDSM-2	WS-SVC-IDS2-BUN-K9 WS-SVC-IDS2BUNK9= (RMA 部品番号のみ)	IDE ハード ドライブと Compact Flash。 ソフトウェアのアップグレードとイメージの復元に使用可能な CD-ROM ドライブはありません。			4.0 ～最新 *	電流

注 このドキュメントの発行時点で入手可能な最新バージョンのソフトウェアは 5.1 です。 5.1 より後のソフトウェア バージョンが必要な場合は、そのコードのバージョンのマニュアルをチェックして互換性を確認してください。

管理オプションと設定オプション

IPS センサーは、コマンドライン インターフェイスを使用して、またはこれらの項に記載された設定ツールまたは管理ツールのいずれかを使用して、管理および設定することができます。

CiscoWorks Management Center for IPS Sensors (IPS MC)

CiscoWorks Management Center for IPS Sensors は、Cisco Systems ネットワーク センサー、スイッチ IPS センサー、ルータ用の IPS ネットワーク モジュール、およびルータ内のインライン

侵入防御ソフトウェアの設定用のスケーラブルなアーキテクチャを使用したツールです。 CiscoWorks Management Center for IPS Sensors を使用すれば、管理者は、グループ プロファイルを使用して複数のセンサーを同時に設定することで、時間を節約できます。 加えて、考えられるネットワーク侵入の検知の精度と特性を高める強力な署名管理機能も提供します。

互換性については、「Management Center for IPS Sensors に対してサポートされているデバイスとソフトウェア バージョン」を参照してください。

CiscoWorks Monitoring Center for Security (SecMon)

CiscoWorks Monitoring Center for Security は、以下からセキュリティ イベントを収集、保存、表示、関連付け、および報告するためのツールです。

- Cisco Network IPS
- Cisco Network IDS
- Cisco Switch IDS
- インライン IPS 機能を備えた Cisco IOS ルータ
- ルータ用の Cisco IDS モジュール
- Cisco PIX ファイアウォール
- Cisco Catalyst 6500 シリーズ Firewall Services Modules (FWSM)
- CiscoWorks Management Center for Cisco Security Agents
- CiscoWorks Monitoring Center for Security サーバ

互換性については、「Monitoring Center for Security に対してサポートされているデバイスとソフトウェア バージョン」を参照してください。

Cisco Security Monitoring Analysis and Response System (MARS)

Cisco Security Monitoring Analysis and Response System (MARS) は、お客様によるより効率的なネットワーク デバイスとセキュリティ デバイスの使用を支援する、脅威の管理、モニタリング、および軽減のための高性能かつスケーラブルなアプライアンスのファミリです。 Cisco Security MARS は、従来のネットワーク インテリジェンスを使用したセキュリティ イベント モニタリング、コンテキスト相関、ベクトル解析、異常検出、ホットスポット識別、および自動軽減機能を統合します。 これらの機能を組み合わせることで、Cisco Security MARS は、企業がネットワーク コンプライアンスを維持しながら、ネットワーク攻撃を正確に識別して排除できるように支援します。

MARS のバージョン	サポートされているアプライアンス/センサー ソフトウェア
3.3.x	3.x および 4.x
3.4.x	3.x、4.x、5.x

詳細については、製品のリリース ノートを参照してください。

Cisco Threat Response (CTR)

Cisco Threat Response (CTR) は、Cisco IPS センサーと連動して効率的な侵入防止ソリューションを提供します。 Cisco Threat Response は、実質的に、誤報を排除し、本当の攻撃への対処を優先させ、損失の大きい侵入からの修復を支援します。

Cisco Threat Response は Cisco IPS バージョン 3.x 以降と互換性があります。 詳細については、製品のリリース ノートを参照してください。 また、Cisco Threat Response のサポート終了のお知らせを確認してください。

IDS Event Viewer (IEV)

IDS Event Viewer (IEV) は、最大 5 個のセンサーのアラームを表示および管理できる Java ベースのアプリケーションです。 IDS Event Viewer を使用すると、アラームをリアル タイムで、またはインポートされたログ ファイルとして接続および表示できます。 フィルタおよびビューを設定すると、アラームを管理したり、詳細分析の実行用にイベント データをインポートおよびエクスポートできるようになります。 また、IDS Event Viewer では、シクニチャ記述用の Network Security Database (NSDB; ネットワーク セキュリティ データベース) へのアクセスも提供しています。

IEV は IDS バージョン 3.1 ~ 4.x でサポートされます。 バージョン 5.x 以降はサポートされませんが、バージョン 5.x センサーのモニタには使用できます。 ただし、新しい 5.0 機能は IEV によって報告されません。 詳細については、「製品の設定例とテクニカル ノート」を参照してください。

IDS Device Manager (IDM)

IDS Device Manager (IDM) は、センサーの設定および管理を行うための Web ベースのアプリケーションです。 IDS Device Manager の Web サーバはセンサーに常駐します。 この Web サーバには、Netscape または Internet Explorer Web ブラウザでアクセスできます。

IDM は IDS バージョン 3.1 以降でサポートされます。 詳細については、「製品の設定例とテクニカル ノート」を参照してください。

Cisco Secure Policy Manager (CSPM)

Cisco Secure Policy Manager (CSPM) は、Cisco IDS Sensors、PIX ファイアウォール、および IPSec VPN ルータにポリシー ベースのセキュリティ管理を提供します。

注CSPM は EoL になっています。 「Cisco Secure Policy Manager 2.x および 3.x の EoS/EoL のお知らせ」を参照してください。

モデル	CSPM 2.2	CSPM 2.3i	CSPM 2.3.1i	CSPM 2.3.2i	CSPM 2.3.3i

UNIX Director

UNIX Director は、分散ネットワーク全体のセキュリティを管理するための一元化されたグラフィカル インターフェイスを提供します。 また、サードパーティ製ツール経由のデータ管理、NSDB へのアクセス、センサーと IDSM のリモート モニタリングと管理などのその他の重要な機能を実行し、セキュリティ イベントの発生時にセキュリティ担当者にページまたは電子メールを送信することができます。 Director インターフェイスは HP OpenView 上で動作します。

注Cisco IDS アプライアンス センサーのソフトウェア リリース 2.2.x は EoL になっています。 「Cisco IDS 2.2.x センサー ソフトウェアのサポート終了」を参照してください。

Director のバージョン	サポートされているアプライアンス/センサー ソフトウェア
2.1.1	2.1.1
2.2.0	2.2.0
2.2.1	2.2.1
2.2.2	2.2.2 と 2.5
2.2.3*	2.2.3、3.0、3.1

* 2.2.3 は IDS Director ソフトウェアの使用可能な最後のバージョンで、センサー ソフトウェア 3.1 以前をサポートします。

2.2.x Director は 2.2.x センサー バージョンと下位互換性がありますが、Director とセンサーの両方で少なくとも同じソフトウェアのバージョンが存在しない場合は、新しいセンサー機能が Director で使用できない可能性があります。 そのため、手動のコマンドライン設定が必要になります。 詳細については、製品マニュアルを参照してください。

関連情報

- Cisco Intrusion Prevention System
- セキュリティ製品に関する Field Notice (CiscoSecure Intrusion Detection を含む)
- テクニカルサポートとドキュメント - Cisco Systems