

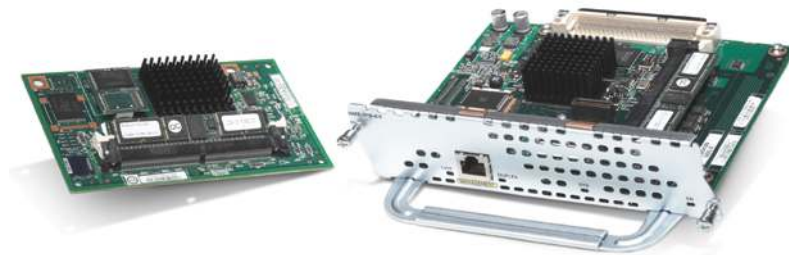
## Cisco ISR 1841、ISR 2800 および ISR 3800 シリーズ用 Cisco IPS モジュール

Cisco® Intrusion Prevention System (IPS; 侵入防御システム) Advanced Integration Module (AIM) および Network Module Enhanced (NME) は、企業のブランチ オフィスに統合型の侵入防御機能を提供し、セキュリティをネットワーク エッジまで拡張します。

Cisco ISR 1841、ISR 2800 および ISR 3800 サービス統合型ルータ シリーズ用 Cisco IPS AIM および IPS NME は、ブランチ オフィスや中小企業に Cisco IPS 機能を提供します(図 1)。Cisco IPS は、シスコの自己防衛型ネットワークの重要なコンポーネントであり、進化するセキュリティ環境に合わせて設計されたアーキテクチャに基づくソリューションです。企業のお客様は、Cisco IPS であらゆる場所をセキュリティ保護し、ライフサイクル サービス アプローチを活用することにより、ネットワークへの攻撃や業務の中断から重要なビジネス プロセスとプライバシーを保護しながらポリシーと法規制への準拠に対応するネットワーク プラットフォームを設計、実装、運用、および最適化できます。

セキュリティに対する脅威がますます複雑化かつ高度化するにつれて、ネットワーク内のあらゆる場所が危険にさらされる可能性が高まっています。Cisco IPS はワーム、スパイウェア、アドウェア、ネットワーク ウイルス、アプリケーションの不正利用といった悪意のあるトラフィックを正確に特定、分類、および抑制します。このような適切な防御システムを導入することで、業務の継続性を保証しながら、侵入によって発生する損失を最小限に抑えることが可能です。

図 1 Cisco ISR 用 Cisco IPS AIM および IPS NME



シスコでは、さまざまな IPS ソリューションを提供しています。Cisco IPS AIM は中堅・中小企業および小規模ブランチ オフィスに適しており、Cisco IPS NME は小規模企業および大規模ブランチ オフィスに適しています。Cisco IPS AIM および IPS NME 上で稼働する Cisco IPS センサー ソフトウェアは、エンタープライズ クラスの高度な IPS 機能を提供しており、増え続けるブランチ オフィスのセキュリティ ニーズに対応します。また、Cisco IPS AIM および IPS NME のパフォーマンスは、現在および将来のブランチ オフィスの WAN 帯域幅要件に合わせて拡張できます。IPS と Cisco ISR を統合すれば、ソリューション コストを低く抑えながら、あらゆる規模のビジネスに最適な状態を保つことができます。

Cisco IPS ソリューションでは、さまざまなデバイス設定とイベント表示オプションを用意することで、展開および監視を容易にしています。たとえば、単一のデバイスを管理する Cisco IPS Device Manager (IDM)、イベントを監視する Cisco IPS Manager Express (IME)、ネットワーク全体のデバ

イス設定とポリシー展開を行う Cisco Security Manager、イベントの監視と相関分析を行う Cisco Security Monitoring, Analysis and Response System (CS-MARS) などがあります。

### Cisco ISR 1841、ISR 2800 および ISR 3800 シリーズ ルータ用 Cisco IPS AIM および IPS NME — フルサービス ブランチ ソリューションへの IPS の統合

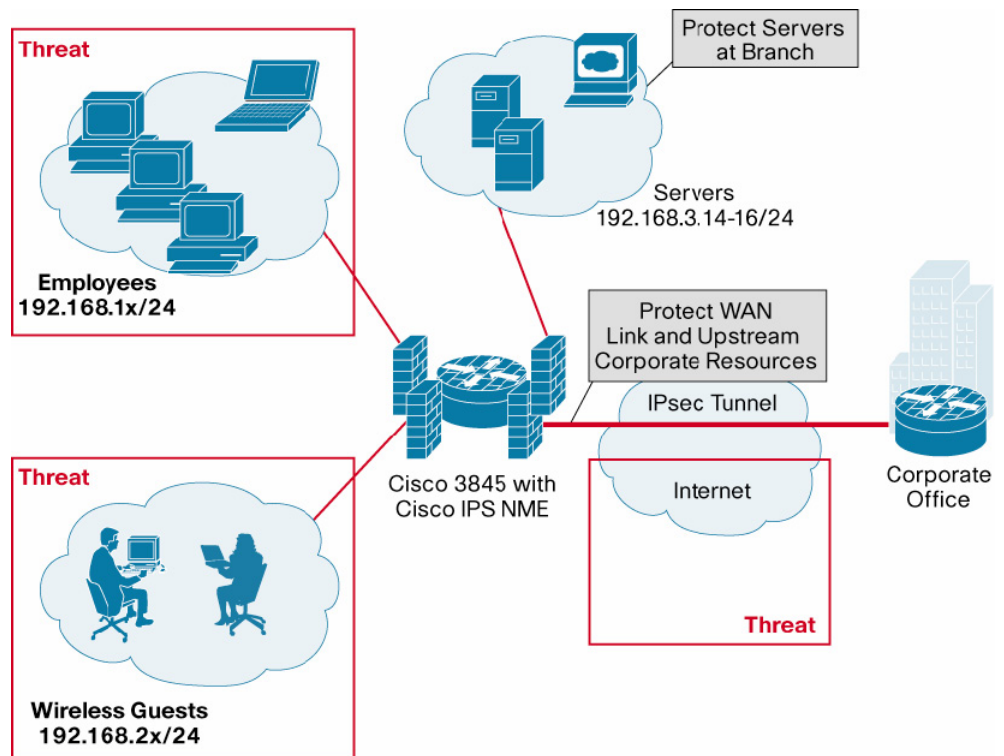
Cisco ISR では、IPS とブランチ オフィスのルーティングを統合することにより、インターネットで発生する脅威からリモート ブランチ オフィスのネットワークを保護し、ブランチ オフィス内の感染ホストにおける WAN リンクの過負荷を軽減することができます。IPS をブランチ オフィス ルータに統合することにより、お客様にはさまざまな利点がもたらされます。

- **専用プロセッサによるパフォーマンスの最大化** — IPS AIM および IPS NME には、IPS のすべての機能用に独自の CPU と DRAM が搭載されています。これにより、ホスト ルータからのディープ パケット インスペクションなど、プロセッサに負荷が集中するタスクからルータの CPU を解放できます。
- **パフォーマンス** — Cisco IPS AIM は最大で 45 Mbps、IPS NME は最大で 75 Mbps のトラフィックを監視できるため、T1/E1 および T3 までの環境に最適です。
- **インライン モードおよびプロミスキャス モード** — インライン モードおよびプロミスキャス モードでの IPS インスペクションがサポートされています。インライン モードでは、IPS モジュールをパケット パスの途中に配置し、違反したパケットを廃棄するように設定できます。
- **Cisco IPS ソリューション用の共通の管理ツール** — Cisco IPS AIM および IPS NME では、Cisco Security Manager をサポートしています。これは、Cisco IPS 4200 シリーズ センサーでサポートされているのと同じ管理ツールであるため、アプライアンスとルータ センサーの両方に集中管理システムを提供できます。
- **監視インターフェイスの柔軟性** — Cisco IPS AIM および IPS NME は ルータのバックプレーンに直接接続することで、T1、T3、DSL、ATM、ファスト イーサネット、ギガビット イーサネットなど、すべてのルータ インターフェイスに入出力するパケットを監視できます。
- **インバンド管理(AIM のみ)** — モジュールに搭載されたギガビット イーサネット ポートは、Cisco IPS AIM CLI(コマンドライン インターフェイス)のインバンド管理、および Web ベースの管理アプリケーションである Cisco IPS Device Manager 用として使用できます。IPS AIM には、ルータのコンソール ポートまたはレイヤ 3 インターフェイス向けの Secure Shell (SSH; セキュア シェル) プロトコルを使用してアクセスします。物理的な管理ポートは不要です。
- **アウトバンド管理(NME のみ)** — デバイス管理に個別のネットワークが必要な場合、Cisco IPS NME には、コンソールおよび Web ベースのデバイス マネージャ アクセス専用の外部ギガビット イーサネット ポートが用意されています。
- **物理的なスペースの節約** — Cisco IPS AIM および IPS NME は Cisco ISR に装着されるため、ワイヤリング クローゼット内の貴重なスペースを節約できます。
- **ダウンタイムの短縮(NME のみ)** — モジュラ型の Cisco ISR 上の NME スロットは外部からアクセス可能なため、現場での取り付けや交換は非常に簡単です。また、Cisco ISR 3845 は Online Insertion and Removal (OIR; 活性挿抜) をサポートしています。これにより、電源スイッチを再投入しなくても同種のモジュールを簡単に交換できるため、平均修復時間が最小限に短縮され、ルータ全体のアベイラビリティが向上します。
- **電源およびケーブルの容易な管理** — Cisco IPS AIM および IPS NME は、DC 電源や冗長電源といったルータの電源オプションを使用できるという利点があります。

- **精密なセキュリティ** — Cisco IPS AIM および IPS NME は、一般的なすべての Cisco IOS<sup>®</sup> ソフトウェア機能のほか、VPN、ファイアウォール、Network Address Translation (NAT; ネットワークアドレス変換)、Web Cache Control Protocol (WCCP)、Cisco Wide Area Application Service (WAAS) などのセキュリティ機能および WAN 最適化機能と相互運用できます。

図 2 に、Cisco IPS NME を使用したブランチ オフィスの展開例を示します。

図 2 Cisco IPS NME を使用したブランチ オフィスの展開例



### Cisco IPS の利点

Cisco IPS AIM および IPS NME で稼働する Cisco IPS センサー ソフトウェアには、多様な脅威からネットワークを確実に防御する革新的なセキュリティ技術が実装されています。相関管理ツールや検証ツールを含むこれらの技術を活用すれば、正規のトラフィックを廃棄してしまうリスクを大幅に軽減できます。

### ネットワーク全体にわたる統合

Cisco IPS ソリューションは、ネットワーク、サーバ、デスクトップ エンドポイントなど、さまざまな媒体からの脅威を抑制します。また、専用アプライアンス、統合型のファイアウォールおよび IPS デバイスからルータやスイッチ用のサービス モジュールにいたるまで、さまざまなシスコ プラットフォーム上に展開できます。Cisco IPS ソリューションでは、ネットワーク レイヤ 2 ~ 7 のトラフィックについて詳細な検査を行うことにより、ポリシー違反、脆弱性の悪用、および異常な動作などからネットワークを保護します。

### コラボレーションによる脅威の防御

Cisco IPS は、脅威に対して連携動作を行い、脅威を評価したうえで対処する独自のセキュリティエコシステムをシステム全体にわたって採用することで、優れたネットワークのスケラビリティと復

元力を提供します。このようなユビキタスなアプローチには、ソリューション間のフィードバックの連携、共通のポリシー管理、ベンダー間のイベント相関処理、攻撃経路の識別、パッシブ/アクティブフィンガープリント、Cisco Security Agent および IPS 間のホストベースのコラボレーションなどが含まれます。

### プロアクティブなポストチャ対応

Cisco IPS は、ネットワークの脅威に対するセキュリティ ポストチャの変更に合わせて最新のセキュリティ体制を維持するように進化することで、既知および未知の攻撃による脅威を軽減します。幅広い動作分析、異常検出、ポリシー調整、および脅威への迅速な対応を行うことにより、時間とリソースを節約し、さらに組織の資産保護や生産性向上を可能にします。

### 容易な管理

Cisco IPS AIM および IPS NME のインストールは、ルータでカードを認識するように設定するのと同じくらい簡単です。IPS AIM および NME を初期化して実行したあと、設定を変更し、任意の管理コンソールからモジュールにプッシュします。

### 主な管理機能

主な管理機能は次のとおりです。

- **Cisco IPS Device Manager** — ネットワークおよびスイッチの IPS センサーを設定します。グループ プロファイルにより、複数のセンサーを同時に設定するためのスケーラブルな基盤を提供します。
- **Cisco IPS Manager Express** — 最大 5 つの IPS デバイスで生成される IPS イベントを監視します。
- **Cisco Security Manager** — 統合型の監視機能を使用して、ネットワーク IPS、スイッチ IPS、ホスト IPS、ファイアウォール、およびルータからイベントをキャプチャし、保存、表示、相関分析したうえでレポートします。
- **CS-MARS** — 高性能でスケーラブルなアプライアンス ファミリーを提供し、脅威を管理、監視、および軽減します。

## Cisco IPS AIM の製品概要

### 製品番号

表 1 に、Cisco IPS AIM および IPS NME の製品番号と説明を示します。

表 1 Cisco IPS AIM および IPS NME の製品番号

製品番号	説明
AIM-IPS-K9	Cisco ISR 1841、ISR 2800 および ISR 3800 シリーズ用 Cisco IPS AIM
NME-IPS-K9	Cisco ISR 2811、ISR 2821、ISR 2851 および ISR 3800 シリーズ用 Cisco IPS NME

### サポート対象プラットフォーム

シスコのサービス統合型ルータごとに、1 台の Cisco IPS AIM または IPS NME がサポートされます。表 2 に、サポート対象のルータ プラットフォームを示します。

表 2 サポートされているルータ プラットフォーム

ルータ	Cisco IPS AIM	Cisco IPS NME
Cisco ISR 1841 および ISR 2801	○(プラットフォームあたり最大 1 枚)	×
Cisco ISR 2811、2821、および 2851	○(プラットフォームあたり最大 1 枚)	
Cisco ISR 3825 および 3845	○(プラットフォームあたり最大 1 枚)	

### Cisco IOS ソフトウェア フィーチャ セットおよびリリース

表 3 に Cisco IPS AIM および IPS NME に必要な Cisco IOS フィーチャ セットおよびリリース、表 4 にサポート対象の Cisco IOS ソフトウェア リリースを示します。

表 3 Cisco IPS AIM および IPS NME でサポートされる Cisco IOS ソフトウェア フィーチャ セット

Cisco IOS ソフトウェア フィーチャ セット
Cisco IOS Advanced Security
Cisco IOS Advanced IP Services
Cisco IOS Advanced Enterprise Services

表 4 Cisco IPS AIM および IPS NME でサポートされる Cisco IOS ソフトウェア リリース

製品番号	最小限必要な Cisco IOS ソフトウェア リリース
AIM-IPS-K9	12.4(15)XY または 12.4(20)T
NME-IPS-K9	12.4(20)YA

### Cisco IPS センサー ソフトウェアおよびシグニチャ ライセンス

Cisco IPS AIM および IPS NME は、Cisco IPS センサー ソフトウェアで動作します。表 5 に最小限必要なリリースを示します。

表 5 Cisco IPS AIM および IPS NME でサポートされる Cisco IPS センサー ソフトウェア リリース

製品番号	最小限必要な Cisco IPS ソフトウェア リリース
AIM-IPS-K9	6.0(3)
NME-IPS-K9	6.1(1)

最新の Cisco IPS センサー ソフトウェアへのアップグレードについては、Software Center から Cisco Secure Software (<http://www.cisco.com/kobayashi/sw-center/ciscosecure/ids/crypto/>) にアクセスしてください。

Cisco IPS AIM および IPS NME でシグニチャ アップデートを実施するには、センサーごとに有効な Cisco Services for IPS サービス契約が必要です。IPS アプリケーション ソフトウェアにはライセンス要件が適用されているため、有効な Cisco Services for IPS サポート契約のあるセンサーでのみシグニチャ アップデートを実施できます。

### Cisco Services for IPS

Cisco Services for IPS は、Cisco IPS ソリューションで最新の脆弱性と脅威を正確に識別、分類、および抑止できるようにするためのセキュリティ上のインテリジェンスとシグニチャ ファイル アップデートをタイムリーに提供する、包括的なサポート プログラムであり、次の機能を備えています (表 6 および 7 を参照)。

- Cisco IPS AIM などの IPS ソリューションでシグニチャ アップデートを実施する権限
- ネットワークを最新のビジネス ニーズに対応させ、ハードウェアの Return On Investment (ROI; 投資利益率)を向上させる、継続的な IPS システム ソフトウェア アップデート
- シグニチャのリリースと関連情報に関するタイムリーなアラート
- 問題を迅速に解決するための Cisco Technical Assistance Center (TAC) へのグローバル アクセス (24 時間 365 日アクセス可能)
- 強力なオンライン ツールと情報が用意された Cisco.com へのアクセス登録
- ハードウェア交換オプション (2 時間以内～翌営業日 [NBD])
- Cisco IntelliShield Alert Manager へのリンク

表 6 Cisco IPS AIM 用の Cisco Services for IPS

Cisco Services for IPS の製品番号	説明
<b>企業向け</b>	
CON-SU1-AIMIPSK9	IPS SVC、AR NBD AIM-IPS-K9
CON-SU2-AIMIPSK9	IPS SVC、AR 8X5X4 AIM-IPS-K9
CON-SU3-AIMIPSK9	IPS SVC、AR 24X7X4 AIM-IPS-K9
CON-SU4-AIMIPSK9	IPS SVC、AR 24X7X2 AIM-IPS-K9
CON-SUO1-AIMIPSK9	IPS SVC、ONSITE NBD AIM-IPS-K9
CON-SUO2-AIMIPSK9	IPS SVC、ONSITE 8X5X4 AIM-IPS-K9
CON-SUO3-AIMIPSK9	IPS SVC、ONSITE24X7X4 AIM-IPS-K9
CON-SUO4-AIMIPSK9	IPS SVC、ONSITE24X7X2 AIM-IPS-K9
<b>サービスプロバイダー向け</b>	
SP-SFA1-AIMIPSK9	IPS-SP SVC、AR NBD AIM-IPS-K9
SP-SFA2-AIMIPSK9	IPS-SP SVC、AR 8X5X4 AIM-IPS-K9
SP-SFA3-AIMIPSK9	IPS-SP SVC、AR 24X7X4 AIM-IPS-K9
SP-SFA4-AIMIPSK9	IPS-SP SVC、AR 24X7X2 AIM-IPS-K9
SP-SFC1-AIMIPSK9	IPS-SP SVC、ONSITE NBD AIM-IPS-K9
SP-SFC2-AIMIPSK9	IPS-SP SVC、ONSITE 8X5X4 AIM-IPS-K9
SP-SFC3-AIMIPSK9	IPS-SP SVC、ONSITE24X7X4 AIM-IPS-K9
SP-SFC4-AIMIPSK9	IPS-SP SVC、ONSITE24X7X2 AIM-IPS-K9

表 7 Cisco IPS NME 用の Cisco Services for IPS

Cisco Services for IPS の製品番号	説明
<b>企業向け</b>	
CON-SU1-NMEIPSK9	IPS SVC、AR NBD NME-IPS-K9
CON-SU2-NMEIPSK9	IPS SVC、AR 8X5X4 NME-IPS-K9
CON-SU3-NMEIPSK9	IPS SVC、AR 24X7X4 NME-IPS-K9
CON-SU4-NMEIPSK9	IPS SVC、AR 24X7X2 NME-IPS-K9
CON-SUO1-NMEIPSK9	IPS SVC、ONSITE NBD NME-IPS-K9
CON-SUO2-NMEIPSK9	IPS SVC、ONSITE 8X5X4 NME-IPS-K9
CON-SUO3-NMEIPSK9	IPS SVC、ONSITE24X7X4 NME-IPS-K9
CON-SUO4-NMEIPSK9	IPS SVC、ONSITE24X7X2 NME-IPS-K9
<b>サービスプロバイダー向け</b>	
SP-SFA1-NMEIPSK9	IPS-SP SVC、AR NBD NME-IPS-K9

Cisco Services for IPS の製品番号	説明
SP-SFA2-NMEIPSK9	IPS-SP SVC, AR 8X5X4 NME-IPS-K9
SP-SFA3-NMEIPSK9	IPS-SP SVC, AR 24X7X4 NME-IPS-K9
SP-SFA4-NMEIPSK9	IPS-SP SVC, AR 24X7X2 NME-IPS-K9
SP-SFC1-NMEIPSK9	IPS-SP SVC, ONSITE NBD NME-IPS-K9
SP-SFC2-NMEIPSK9	IPS-SP SVC, ONSITE 8X5X4 NME-IPS-K9
SP-SFC3-NMEIPSK9	IPS-SP SVC, ONSITE24X7X4 NME-IPS-K9
SP-SFC4-NMEIPSK9	IPS-SP SVC, ONSITE24X7X2 NME-IPS-K9

**注:** Cisco IPS AIM または IPS NME 用の Cisco Services for IPS は、Cisco ISR 1841、Cisco ISR 2800 および ISR 3800 シリーズの Cisco SMARTnet<sup>®</sup> サポートを補完するものであり、プラットフォームの Cisco SMARTnet サポートに追加して購入する必要があります。

Cisco Services for IPS の詳細については、以下の URL を参照してください。

<http://www.cisco.com/jp/services/portfolio/tss/ips.html>

## ハードウェア仕様

表 8 に、Cisco IPS AIM および IPS NME のハードウェア仕様を示します。

表 8 Cisco IPS AIM および IPS NME のハードウェア仕様

機能	Cisco IPS AIM	Cisco IPS NME
<b>ハードウェア機能</b>		
監視ポートおよび管理ポート	ギガビットイーサネットポート × 1	外部ギガビットイーサネットポート × 1
<b>物理仕様</b>		
寸法 (幅 × 高さ × 奥行)	<ul style="list-style-type: none"> <li>5.25 × 0.95 × 3.25 インチ</li> <li>13.3 × 2.41 × 8.26 cm</li> </ul>	<ul style="list-style-type: none"> <li>7.12 × 6.50 × 1.62 インチ</li> <li>18.1 × 16.5 × 4.1 cm</li> </ul>
重量	0.27 kg (0.6 ポンド)	0.45 kg (1.0 ポンド)
動作湿度	5 ~ 95% (結露しないこと)	
動作温度	<ul style="list-style-type: none"> <li>32 ~ 104°F</li> <li>0 ~ 40°C</li> </ul>	
非動作温度	<ul style="list-style-type: none"> <li>-40 ~ 185°F</li> <li>-40 ~ 85°C</li> </ul>	
動作高度	<ul style="list-style-type: none"> <li>0 ~ 10,000 フィート</li> <li>0 ~ 3,000 m</li> </ul>	

## 適合規格、安全性、EMC、電気通信、ネットワーク認定

IPS AIM および IPS NME を Cisco ISR 1841、ISR 2800、または ISR 3800 シリーズ ルータに搭載した場合でも、ルータ自体の標準規格 (適合規格、安全性、EMC、電気通信、ネットワーク認定) に変更はありません。Cisco ISR 1841、ISR 2800、および ISR 3800 シリーズ ルータのデータシートを参照してください。

## パフォーマンス仕様

Cisco IPS AIM は最大 45 Mbps、IPS NME は最大 75 Mbps で稼働します。パフォーマンスは、テスト用のプラットフォーム、トラフィック プロファイル、およびプラットフォームで同時に稼働しているサービスによって異なります。

## 機能仕様

表 9 に、Cisco IPS AIM および IPS NME の機能仕様を示します。

表 9 Cisco IPS AIM および IPS NME の機能仕様

機能	Cisco IPS AIM および IPS NME
標準の監視インターフェイス	ルータの内部バス
標準コマンドおよびコントロール インターフェイス	<ul style="list-style-type: none"> <li>• AIM: インバンド管理用の内部ギガビット イーサネット ポート</li> <li>• NME: アウトオブバンド管理用の外部ギガビット イーサネット ポート</li> </ul>
オプションのインターフェイス	×
ステートフル パターンの認識	○
学習的検出	○
異常検出	○
スニープまたはフラッド	○
DoS 攻撃の軽減	○
ワームまたはウイルス	○
Common Gateway Interface (CGI) または Web 攻撃	○
バッファ オーバーフロー保護	○
Remote Procedure Call (RPC) 攻撃検出	○
IP フラグメンテーション攻撃	○
Internet Control Message Protocol (ICMP) 攻撃	○
Simple Mail Transfer Protocol (SMTP)、Send Mail、Internet Message Access Protocol (IMAP) または Post Office Protocol (POP) 攻撃	○
FTP、SSH、Telnet、および Rlogin 攻撃	○
Domain Name System (DNS) 攻撃	○
TCP ハイジャック	○
Windows または NetBIOS 攻撃	○
TCP アプリケーション保護	○
Network Time Protocol (NTP) 攻撃	○
シグニチャ マイクロエンジン テクノロジーを使用したカスタマイズ可能なシグニチャ	○
自動シグニチャ アップデート	○
アラームのサマライズ	○
802.1q トラフィックのサポート	○
センサーおよび管理コンソール間の IPSec または Secure Socket Layer (SSL)	○
暗号化されたシグニチャ パッケージ	○
リモート管理用 SSH	○
セキュアなファイル転送のための Serial Control Protocol (SCP) サポート	○
IP フラグメンテーションの再構成	○
TCP ストリームの再構成	○
Unicode の難読化解除	○
ルータ ACL の変更	○

機能	Cisco IPS AIM および IPS NME
ファイアウォールのポリシー変更	○
スイッチ ACL の変更	○
TCP のリセットによるセッション終了	○
IP セッションのロギングまたはセッション リプレイ	○
アラーム表示	○
E メールによるアラート	○
ポケットベルによるアラート	○
カスタマイズ可能なスクリプト実行	○
複数のアラーム宛先	○
サードパーティ製ツールの統合	○
IPS アクティブ アップデートの通知	○
Web ユーザ インターフェイス (HTTPS)	○
Command-line interface (CLI; コマンドライン インターフェイス) (コンソール)	○
CLI (Telnet または SSH)	○
CiscoWorks VPN Security Management Solution のサポート	○
冗長電源装置	○ (Cisco ISR 3845 のみ)
リンク障害検出のモニタリング	○
通信障害の検出	○
サービス障害の検出	○
デバイス障害の検出	○

©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。(0805R) 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>

0120-092-255 (通話料無料)

電話受付時間：平日 10:00～12:00、13:00～17:00

お問い合わせ先