

Cisco Intrusion Prevention ソリューション

予防的な統合型、コラボレーション型、および適応型のネットワーク保護

Cisco® IPS (Intrusion Prevention System; 侵入防御システム) ソリューションは、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など、悪意のあるトラフィックを正確に識別、分類、および抑制することによって、業務への影響を未然に防ぎます。

ネットワークは複雑なアーキテクチャへと進化し、複数のセグメント、ブランチ、および入出力ポイントが含まれています。このような絶えず変化する環境においてネットワーク セキュリティに求められているのは、ネットワーク デバイス、サーバ、およびエンドポイントと連携して動作するソリューションです。

侵入防御は、セキュリティ ソリューションの成功をもたらす主要な要素ですが、単に標準的な脅威と判断したトラフィックを廃棄するだけでは十分とはいえません。

Cisco IPS ソリューションは、シスコ自己防衛型ネットワークの中心コンポーネントとして、攻撃や脅威の発生源または履歴に関係なく、包括的な脅威の防御を実現します。Cisco IPS ソリューションは、次の機能によって、先進的な脅威防御機能を提供します。

- **ネットワーク全体への統合** — 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 エンドポイントを含む、さまざまな媒体からの脅威を撃退します。専用のアプライアンスから、ルータおよびスイッチ用のサービス モジュールとして提供されるファイアウォールと IPS の統合型ソリューションにいたるまで、さまざまな製品が用意されています。ネットワーク全体にわたるレイヤ 2 ~ 7 のトラフィックを詳細に検査することで、ポリシー違反、脆弱性の悪用、および異常な動作からネットワークを保護します。さらに、展開を簡易化し、リスク評価値決定アルゴリズムによって状況に応じた分析を行って、最新のセキュリティ ポスチャ情報をユーザに提供します。
- **コラボレーションによる脅威の防御** — Cisco IPS ソリューションは、脅威を評価して対処する独自のセキュリティ システムをインフラストラクチャ全体に適用することで、優れたネットワーク スケーラビリティと耐障害性を提供します。このシステム全体を網羅するアプローチには、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、マルチベンダー 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、ホストベース (Cisco Security Agent) の IPS コラボレーション、ロードバランシング機能、暗号化トラフィックの把握などが含まれます。
- **ポスチャに対する予防的な対応** — Cisco IPS ソリューションは、ネットワーク脅威のポスチャが変化するのに合わせて、最新のセキュリティ環境を維持するように発展および適応することで、既知と未知の両方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、および脅威に対する迅速な対応により、時間とリソースを節約する以外に、最も重要な点として、組織の資産を保護し、生産性を向上させます。

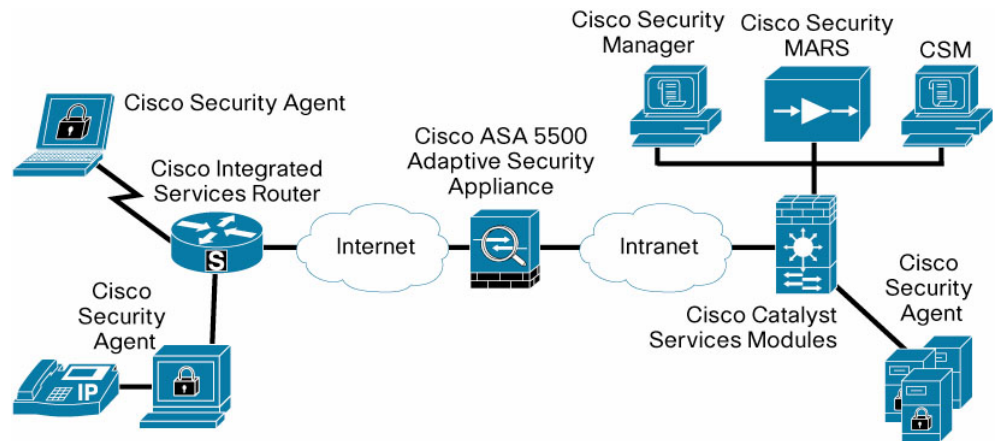
これにより、Day-Zero 攻撃からネットワークをエンドツーエンドで保護する、広範で包括的かつ予防的な脅威防御ソリューションが実現します。

主要ポイントでの統合された保護機能

Cisco IPS ソリューションは、ネットワーク内の主要ポイントで統合された、インライン型侵入防御機能を提供し、ネットワークの重要な資産とデータを保護できるようにします。図 1 に、ネットワーク

アーキテクチャ全体に IPS テクノロジーを戦略的に展開し、包括的な防御および保護を実現する方法を示します。

図 1 Cisco IPS ソリューションによるネットワーク全体の包括的な保護



ネットワーク インフラストラクチャ全体に、次のような幅広い保護機能が提供されます。

- **統合型の境界保護** — Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスは、統一された単一プラットフォームに統合型ファイアウォール、VPN、およびフル機能の IPS を備えており、ワームや悪意のある攻撃に対する最初の防御ラインとしてネットワークを保護します。
- **ブランチの保護** — シスコのサービス統合型ルータは、統合された IPS サービスを提供し、脅威がネットワークに侵入する前に防御します。脅威の識別は、着信 VPN トラフィックを復号化した直後、脅威がネットワークや重要な資産に被害をもたらす前に行われます。
- **統合されたデータ センターの保護** — Cisco® Catalyst 6500 シリーズ用の IDSM-2 (IDS Services Module 2) は、セキュリティ サービス ブレードを Catalyst スイッチのファブリックに統合することで、包括的な侵入防御を提供します。
- **Day-Zero 攻撃からのサーバ資産とホストの保護** — Cisco Security Agent を使用すると、ホストレベルとサーバレベルの両方で、エンドポイントの重要な資産を Day-Zero 攻撃から保護できます。
- **一括レポート** — CS-MARS (Cisco Security Monitoring, Analysis, and Response System) は、脅威の監視、相関分析、および緩和を行って、生産性を向上させ、法規制の順守を簡易化します。
- **集中管理** — Cisco Security Manager は、Cisco IPS、ファイアウォール、および VPN のデバイス構成やセキュリティ ポリシーに関するあらゆる面でのプロビジョニングを集中的に行える、強力で使いやすいソリューションを提供します。

上記の要素を組み合わせることで、悪意のあるさまざまなトラフィックを検出および抑制できる、包括的なインライン型侵入防御ソリューションが実現します。

ネットワーク全体への統合

Cisco IPS ソリューションはネットワークに統合され、優れた可視性、ネットワーク全体の脅威に対応するインテリジェンスを提供します。この可視性により、次の脅威からネットワークを保護できます。

- **ポリシー違反** — Cisco IPS ソリューションは、インスタント メッセージングおよびピアツーピア アプリケーションなどのトラフィック インспекション、厳密な HTTP の適用、ポート 80 インスペク

ション検査、MIME タイプと OS フィンガープリントに基づくトラフィック フィルタリングにより、アプリケーションの使用状況とポリシー適合性を厳密に制御します。ポリシー違反の管理は、状況に応じたユーザおよびエンドポイント情報の評価によっても可能です。

- **脆弱性の悪用** — Cisco IPS ソリューションは、さまざまなオペレーティング システム、ネットワーク サービス、アプリケーション、およびプロトコルにおける既知の脆弱性の悪用を阻止し、未知の脆弱性に対する新しいワームやウイルスからの保護も提供します。
- **異常な動作** — シスコの優れた異常検出機能は、ネットワークの「通常の」トラフィック パターンを学習し、異常な動作をスキャンすることで、ワームを検出します。急速に感染が広がるネットワーク ワームはネットワークをスキャンして、他のホストを感染させようとします。異常検出プログラムは、各プロトコルまたはサービスについて、通常のスキャン動作を調査し、しきい値ヒストグラムとスキャナの絶対しきい値にこの情報を蓄積します。スキャなしきい値によって絶対スキャンレートが指定され、この値を超えるソースは悪意があるとみなされます。
- **動作分析** — Cisco IPS ソリューションは、ネットワークの使用状況を動的に学習して、感染の特性を検出する機能を備えています。

多様な脅威の発見

Cisco IPS ソリューションは、さまざまな方法を使用してレイヤ 2 ~ 7 のトラフィックを検査および分析します。これにより、多様な脅威の識別が可能になり、不正利用が拡散する前に脆弱性に対するシグニチャを開発できる可能性が高くなります。脅威を発見する多様な方法としては、次のものがあります。

- **レート制限** — IPS デバイスでは、特定のタイプのトラフィックに対し、大量の帯域幅を使用できないよう制限することができます。この機能によって、外部デバイスへの信号送信が可能のため、Cisco IOS® ソフトウェア ベースのルータなどでも同様のレート制限を実行できます。
- **IPv6 検出** — IPv6 トラフィックの内容を詳細に表示し、悪意のあるトラフィックを容易に識別できます。
- **IP-in-IP の検出** — モバイル IP トラフィック内の悪意のあるトラフィックを識別します。
- **ステートフル パターンの認識** — すべてのプロトコルに関してマルチパケット検査を行い、脆弱性に基づく攻撃を識別して、データ ストリーム内に潜む攻撃を阻止します。
- **プロトコル分析** — Cisco IPS ソリューションは、ネットワーク トラフィックのプロトコル デコーディングおよび検証を行います。Cisco IPS センサー ソフトウェア バージョン 6.0 は、ICMP (IP、Internet Control Message Protocol)、TCP、および UDP などの主要なすべての TCP/IP トラフィックを監視します。また、アプリケーション レイヤ プロトコルのステートフルなデコーディングを実行でき、FTP、SMTP (Simple Mail Transfer Protocol)、HTTP、SMB、DNS (ドメイン ネーム システム)、RPC (Remote Procedure Call)、NetBIOS、NNTP (Network News Transfer Protocol)、GRE (Generic Routing Encapsulation)、Telnet などがサポートされます。
- **トラフィック異常の検出** — 通常のネットワーク トラフィック パターンの変化を識別する技術を使用して、複数のセッションおよび接続にわたった攻撃による異常を識別します (一定時間内の ICMP パケット数を事前に定義することで ICMP フラッドを検出するなど)。
- **プロトコル異常の検出** — RFC で規定された正常なプロトコルまたはサービスの動作について、適合性を監視することで攻撃を識別します (HTTP 要求に伴わない HTTP 応答など)。
- **レイヤ 2 検出** — スイッチド環境によく見られる、レイヤ 2 ARP (Address Resolution Protocol; アドレス解決プロトコル) 攻撃と man-in-the-middle 攻撃を識別します。

- **アプリケーション ポリシーの実施** — ピアツーピア、インスタント メッセージング、ポート 80 でトンネリングされたアプリケーションなど、さまざまなアプリケーションの詳細な分析と制御を行います。これにより、さまざまなトラフィック タイプと MIME (Multipurpose Internet Mail Extensions) タイプについてユーザがポリシーを定義し、悪意のあるトラフィックがネットワークを通過するのを防ぐことができます。
- **IPS 回避への対抗技術** — トラフィックの正常化、IP デフラグメンテーション、TCP ストリームの再構築、および難読化の解除により、IPS を回避しようとするハッカーに対する包括的な保護を実現します。
- **カスタマイズ可能なポリシー** — 革新的な TAME (Cisco Threat Analysis Micro Engine) ポリシー言語を使用すると、新しいポリシーの作成や既存のポリシーの変更を、ユーザ固有のセキュリティ要件に合わせて柔軟に実施できます。

リスク評価 (Risk Rating)

Cisco IPS ソリューションは状況に応じた優れたデータ分析を行って、脅威を特定し、フォールス ポジティブを排除します。このテクノロジーは、リスク評価と呼ばれます。リスク評価は、リスクバランスを考慮した脅威の分類を行うことにより、IPS のパケット廃棄処理の精度と信頼性を向上させます。この機能は、次のように、複数の条件を考慮した独自の多面的アルゴリズムを使用します。

- **イベントの重大度** — ユーザによる変更が可能な加重値で、疑わしいトラフィックによる被害の可能性を評価します。
- **シグニチャの信頼性** — ユーザによる変更が可能な加重値で、疑わしい動作を検出したシグニチャの信頼性を評価します。
- **資産価値** — ユーザが定義する値で、攻撃対象ホストの価値を表します。
- **攻撃の影響度** — 内部的な加重値で、IPS センサーがイベントの対象について把握している関連情報を評価します。

リスク評価による評価は整数値で表され、すべての IPS のシグニチャ、ポリシー、または異常検出アルゴリズムに対して動的に適用されます。この値が高いほど、関連するアラートの原因となったイベントのセキュリティ リスクは大きくなります。これによりユーザは、ネットワーク攻撃を抑制するためのポリシーの作成や、イベントをより適正に評価して詳細な調査の優先順位を決めることが可能になります。このため、ユーザはインライン型 IPS 処理に関するインテリジェントな判断が可能になり、正規のトラフィックを廃棄してしまう可能性はほとんどなくなります。

脅威評価 (Threat Rating)

脅威評価は、Cisco IPS センサー ソフトウェア バージョン 6.0 の新機能で、ネットワークの脅威に関する情報を一元化します。この機能では、脅威の評価値が高いイベントのみを表示するようにビューアをカスタマイズする機能により、アラームとイベントを最小限に抑えます。脅威評価値は次のように算出されます。

- 対応措置の成功に基づくイベントのリスク評価の動的な調整
- 対応措置が適用された場合、リスク評価は使用されない ($TR < RR$)
- 対応措置が適用されなかった場合、リスク評価は変更なし ($TR = RR$)

この結果、脅威のリスクを決定する単一の値が算出されます。これにより、アラームの管理とネットワーク上のリスクの判断が容易になります。

コラボレーションによる脅威の防御

ネットワークを保護するには、個別の攻撃を緩和するだけでなく、それ以上の機能を備えた IPS ソリューションが必要です。システム全体のセキュリティを提供するために、IPS はネットワークに配備された他のセキュリティ ポイントにも保護を拡大する必要があります。Cisco IPS ソリューションは、ネットワーク リソース情報を判断し、そのリソースと連携および通信する機能により、独自の優れた保護機能を提供します。Cisco IPS ソリューションは、次の機能を備えています。

- **IPS/Cisco Security Agent のコラボレーション** — 状況に応じた分析を行うためにエンドポイント情報を IPS に伝達することで、徹底した防御を実現します。さらに、Cisco Security Agent Watch List を使用して、IPS は疑わしいホストを検疫することもできます。その結果、エンドポイントによって悪意があると認識されたホストからネットワークを保護できます。
- **ソリューション間のフィードバックの連携** — アラームを伝えるネットワークトラフィックが他のネットワークセキュリティ デバイスおよびツールに送信されることで、単一セグメント上の攻撃からシステム全体を保護します。
- **パッシブ/アクティブ フィンガープリント** — パッシブ OS フィンガープリントまたは静的マッピングに基づいた、状況に応じたエンドポイント プロファイリングがリスク評価値決定アルゴリズム内の値に追加され、ブロック処理のしきい値を決定します。この自動化された、状況に応じた分析により、攻撃の妥当性を容易に判断し、フォールス ポジティブを軽減できます。
- **攻撃経路の識別** — IPS ソリューションの一部として CS-MARS を使用すると、攻撃を視覚的に表示し、ポリシーをリアルタイムで更新してネットワークを保護できます。
- **マルチベンダー イベント関連処理** — CS-MARS、Cisco IPS センサー、およびその他のセキュリティ デバイスとの連携により、ネットワーク全体を把握し、情報を関連付けることができます。

ポスチャに対する予防的な対応

ネットワークの脅威のポスチャが変化するのに合わせて、Cisco IPS ソリューションは、最新のセキュリティ環境を維持するように発展および適応し、既知と未知の両方の攻撃による脅威を軽減します。

- **異常の検出/動作分析** — Cisco IPS ソリューションを使用すると、悪意のあるワームや DoS 攻撃からネットワークを保護する機能を自動化できます。これは、ネットワークの動作を学習し、トラフィック パターンが決められた通常のパターンから外れたときにアラームを送信するセンサーの機能に基づいています。通常のトラフィックは静的に設定できますが、これらのインテリジェントなエンジンを使用して Day-Zero 攻撃からの保護を提供するセンサーにより、従来のポリシーベースのネットワークセキュリティを超えた、これまでにないレベルの保護を実現します。
- **デバイス上およびネットワーク イベントの関連処理** — Cisco MEG (Meta Event Generator) は、ワームを正確に分類する「On-Box」型の関連処理機能を提供します。Cisco IPS センサーソフトウェアには、センサーレベルの高度なイベント関連処理機能と知識ベースの異常検出機能が組み込まれているため、セキュリティ管理者は IPS センサーが検出する悪意のあるアクティビティを高い信頼性で自動的に分類できます。これにより、対応処理を実施し、ワームやウイルスの感染経路やワームの伝播をネットワーク全体で封じ込めることができます。

統合された構成オプション

シスコでは、さまざまなネットワーク IPS 構成ソリューションを提供しているため、お客様の固有の環境に最適な状態で侵入防御機能を実装できます。すべてのソリューションは、ハイ アベイラビリティかつ優れたカスタマー サポートが可能な設計になっています。また、45 Mbps から数 Gbps ま

での幅広いパフォーマンス レベルに対応しています。構成オプションには、専用アプライアンス、スイッチ モジュールとルータ モジュール、およびソフトウェアベースのソリューションなどがあります。

次のようなソリューションが用意されています。

- **Cisco IPS 4200 シリーズ センサー** — 専用の用途別デバイスを使用して侵入防御を行います。最大 8 つのインターフェイスを使用して複数のネットワーク セグメントを保護し、パッシブモードとインライン モードの両方で、2 つの処理を同時にサポートします。アプリケーション モデルは次のとおりです。
 - Cisco IDS 4215 センサー: 80 Mbps
 - Cisco IPS 4240 センサー: 250 Mbps
 - Cisco IPS 4255 センサー: 600 Mbps
 - Cisco IDS 4260 センサー: 1 Gbps

パフォーマンス値は、侵入検知テスト時のスループットです。

- **Cisco IDSM-2 (Cisco Catalyst 6500 シリーズ向け)** — 専用モジュールを使用して、完全な IPS 機能を Cisco Catalyst 6500 シリーズ スイッチに統合します。IDSM-2 バンドルでは、統合されたインライン型保護機能は 500 Mbps および 2 Gbps で動作します。
- **Cisco IDS ネットワーク モジュール (Cisco アクセス ルータ向け)** — Cisco IPS センサー ソフトウェア バージョン 6.0 を使用して、ルータに強化された侵入防御機能を統合します。これにより、検出、相関処理、および識別機能が向上し、最大 45 Mbps の速度で、脅威の軽減と隔離を効果的に行うことができます。
- **Cisco Advanced Inspection and Prevention Security Services Module (AIP-SSM) (Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス向け)** — Cisco ASA 5500 シリーズ多機能脅威抑制ソリューションの一部として、IPS 機能を提供します。
- **Cisco IOS IPS** — ルータ上の Cisco IOS ソフトウェアを使用して、主要な IPS 機能を提供します。

強力な管理、イベント相関処理、およびサービス

シスコでは、さまざまな管理ツールおよび相関処理ツールとサポート サービスを通じて、構成の規模や環境に関係なく、効率的かつ完全な IPS ソリューションを提供します。

管理ソリューション

- **CLI (Command Line Interface; コマンドライン インターフェイス)** — Cisco IOS ソフトウェアに似たフル機能の CLI により、SSH (Secure Shell) プロトコル接続を使ってデバイスを設定できます。
- **Cisco IPS Device Manager** — 1 つのデバイス マネージャから、セキュアなブラウザベースの GUI を利用した設定およびアラームの表示が可能です。Cisco IPS Device Manager は、使用しているオペレーティング システムに関係なく、デスクトップからでも簡単にアクセスできます。そのため、企業内のすべてのシステムから、データへの迅速なアクセスが可能です。使い慣れたブラウザ インターフェイスを利用するため操作性に優れ、SSL (Secure Sockets Layer) を使用することでデータのセキュリティが維持されます。
- **シスコのセキュリティ管理ソリューション** — Cisco IPS、ファイアウォール、および VPN に関するデバイスやセキュリティ ポリシーの設定を一元的に実行できる、強力で使いやすいソリューションです。Cisco Security Manager を利用することで、10 台未満のデバイスで構成される小規模なネットワークであっても、数千台のデバイスで構成される大規模なネットワークであっても、効

率的な管理が可能になります。インテリジェントなポリシーベースの管理手法によって、拡張性を備えたセキュリティ管理が実現します。

- **Cisco Router and Security Device Manager (SDM)** — Web ベースのデバイス マネージャにより、Cisco IOS IPS フィーチャ セットと Cisco IDS ネットワーク モジュールを搭載した Cisco アクセス ルータの構成および管理を容易かつ安全に行うことができます。

エンタープライズ IPS モニタリングとイベント関連処理ソリューション

- **CS-MARS** — アプライアンスベースのソリューションで、企業内のすべてのデータを相互に関連付けます。また、ネットワークおよびセキュリティへの投資を活用して、攻撃的な要素を識別および隔離し、確実に除去を行うよう通知します。CS-MARS を Cisco IPS センサー ソフトウェア バージョン 6.0 と組み合わせて使用すると、総合的なコラボレーティブ ソリューションが実現され、攻撃、ウイルス、ワーム、およびその他の悪意のあるトラフィックからネットワーク インフラストラクチャ全体を保護できます。

サービス

- **Cisco Services for IPS** — シスコのテクニカル サポート サービス ポートフォリオの一環として、Cisco Services for IPS では、Cisco SMARTnet[®] サービスと IPS シグニチャへのアクセス権限を組み合わせ、1 つの包括的なサービス プログラムとして提供します。主なサポート内容は、次のとおりです。
 - 標準の間隔でリリースされる、さまざまな脅威に対応する Cisco IPS シグニチャへのアクセス
 - Cisco IPS センサー ソフトウェア バージョン 6.x などのオペレーティング システム ソフトウェア アップデートへのアクセス
 - Cisco Technical Assistance Center (TAC) のアクセス (世界中から 24 時間利用可能)
 - Cisco.com とシスコ ナレッジ ベースへのアクセス
 - ハイレベルなハードウェア交換オプション (故障したハードウェアを交換するサービス担当者の派遣も可能)

IPS 対応の感染抑制デバイスに関し、シグニチャの更新処理を実行するには、このサービスが必要です。また、プレミアム サービスである Cisco Incident Control System (ICS) を利用するための前提条件にもなっています。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。

英語: http://www.cisco.com/en/US/products/ps6076/serv_group_home.html

日本語: <http://www.cisco.com/jp/services/portfolio/tss/ips.shtml>

その他の機能

- **自動および手動によるセンサーのバイパス構成** — Cisco IPS センサーでは、さまざまなメカニズムを使用して高いアベイラビリティを実現できます。また、独自のネットワーク コラボレーションを利用して耐障害性と冗長性を確保できます。たとえば、Cisco Catalyst スイッチで HSRP (Hot Standby Router Protocol; ホットスタンバイ ルータ プロトコル) 構成や Cisco EtherChannel[®]でのロード バランシングを使用して、プライマリ IPS デバイスに障害が発生した場合にトラフィックをセカンダリ デバイスに流します。また、Cisco IPS センサー ソフトウェア バージョン 6.0 は On-Box 型バイパス メカニズムを備えているため、特定のセンサー障害が発生した場合に、IPS センサーを自動的に Fail-Open に設定できます。このバイパス メカニズムは、手動で設定することもできます。手動で設定する場合、センサーをバイパス モードに切り替えて、Fail-Open の状態に設定する必要があります。これにより、IPS デバイスの信頼性が向上します。

- **SDEE (Security Device Event Exchange) のサポート** — SDEE は、ICSA の IDS コンソーシアムでシスコが開発した IPS 通信の標準プロトコルです。Cisco IPS センサー ソフトウェアバージョン 6.0 は SDEE を使用して、IPS センサーに柔軟性の高い標準化された API を提供しているため、Cisco IPS ソリューションとサードパーティ製の管理/モニタリング ソリューションを容易に統合できます。このため、ユーザはサードパーティ製ソリューションを使用して、Cisco IPS センサーが生成したイベントを監視できます。
- **SNMP トラップを使用したセンサー アラートの配信によるモニタリングおよび通知機能の向上** — Cisco IPS センサー ソフトウェア バージョン 6.0 は、既存のアラーム形式に加えて、SNMP (Simple Network Management Protocol; 簡易ネットワーク管理プロトコル) 形式のアラームを使用するモニタリング ツールにセンサーの IPS アラームを送信できます。また、SNMP を使用して IPS センサーの重大な診断およびステータス情報をポーリングし、ユーザにセンサーの状態を通知できます。

システム要件

インライン型 IPS サービスでは、Cisco IPS 4200 シリーズ センサーに複数のモニタリング インターフェイスが必要です。アップグレード オプションについては、<http://www.cisco.com/jp/product/hs/security/ids4200/> から Cisco IPS 4200 シリーズのデータシートを参照してください。

Cisco IPS センサー ソフトウェア バージョン 6.0 は、Cisco IDS 4215、4235、4240、4255、および 4260 センサーと、IDSM-2 (Cisco Catalyst 6500 シリーズ スイッチ向け)、および Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンス用 AIP-SSM でサポートされています。プロミスキャスベースの IDS モードは、Cisco IDS ネットワーク モジュールでのみサポートされています。

関連情報

Cisco IPS ソリューションの詳細については、<http://www.cisco.com/jp/product/hs/security/ids4200/> を参照してください。

リソース

Cisco IPS Alert Center: 脅威に関する具体的な情報(対策や関連する脆弱性などを含む)を素早く入手できます。詳細については、<http://www.cisco.com/go/ipsalert> を参照してください。

Cisco IPS ソリューションの詳細については、<http://www.cisco.com/jp/product/hs/security/ids4200/> を参照してください。

Cisco ASA 5500 シリーズ適応型セキュリティ アプライアンスの詳細については、<http://www.cisco.com/jp/product/hs/security/asa/> を参照してください。

CS-MARS の詳細については、<http://www.cisco.com/jp/product/hs/security/mars/> を参照してください。

Cisco Security Manager の詳細については、<http://www.cisco.com/go/csmanager> を参照してください。

Cisco IPS Event Viewer (IEV) を使用すると、最大 5 台の IPS センサーを監視できます。Cisco IEV をダウンロードするには、<http://www.cisco.com/pcgi-bin/tablebuild.pl/ids-ev> にアクセスしてください。この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。

Cisco IOS IPS の詳細については、<http://www.cisco.com/jp/product/hs/ios/security/ips/> を参照してください。

Cisco SDM の詳細については、<http://www.cisco.com/jp/product/hs/routers/crsdm/> を参照してください。

Cisco ICS の詳細については、<http://www.cisco.com/jp/product/hs/security/ics/> を参照してください。

©2007 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。(0701R)

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。



シスコシステムズ株式会社

〒107-0052 東京都港区赤坂2-14-27 国際新赤坂ビル東館

<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