Cisco IPS 4200 シリーズ
侵入検知/防御アプライアンス

増加する脆弱性攻撃からのネットワーク防御、機密情報漏えい防止、コンプライアンス強化を実現するセキュリティ アプライアンス

注目ポイント

未知の脅威の侵入、活動の封じ込め
組織のコンプライアンスを強化
多様な環境に適応するラインナップ
外部連携による自己防衛能力

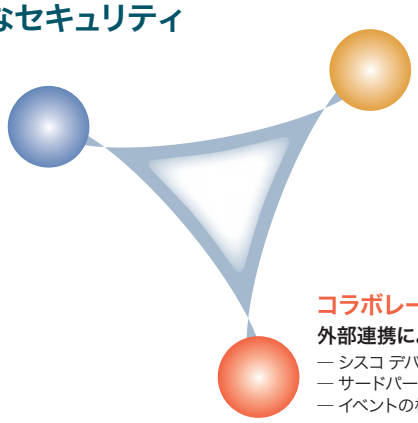
企業ネットワークに対する悪質な攻撃は、多様化とともに増加の一途をたどっています。

Cisco Intrusion Prevention System（IPS、侵入防御システム）は、ネットワークへの直接攻撃だけではなく、ワーム、ウイルス、スパイウェアといった不正なソフトウェアや、許可されていないP2P ソフトなどの悪意あるトラフィックを正確に識別、分類、停止することで、業務への影響を未然に防ぎます。

さらに、シスコの自己防衛型ネットワーク（SDN）の重要なコンポーネントである Cisco IPS ソリューションは、ネットワーク全体への統合、コラボレーション、適応型防御を実現することで、脅威に対して比類のない防御能力を発揮します。

綿密に連携した監視、防衛の網をネットワーク全体に広げることで、組織や企業にとって致命傷となる情報漏えいの防止、組織のコンプライアンスの強化を効果的に実現できます。

Cisco IPS が実現する高度なセキュリティ



適応型防御
急速に拡大、多様化する脅威にいち早く適応し、影響を最小化
— 既知、未知の攻撃の影響を効果的に軽減
— ふるまい、アノーマリ検知に対応
— リスクレートに応じた柔軟なポリシー設定

統合化
ネットワーク全体におよぶ監視と防御の標準化
— ネットワーク、サーバ、PC などのさまざまな脅威に対応
— ルータの IPS モジュールなどとの一元管理を実現
— ポリシーの仮想化による複数システムの収容

コラボレーション
外部連携による検知、防御能力の向上と迅速な対策
— シスコ デバイスおよびソフトとの連携による予防的防御
— サードパーティ製品との連携による検知率の向上
— イベントの相関分析と攻撃経路の識別による「みえる化」

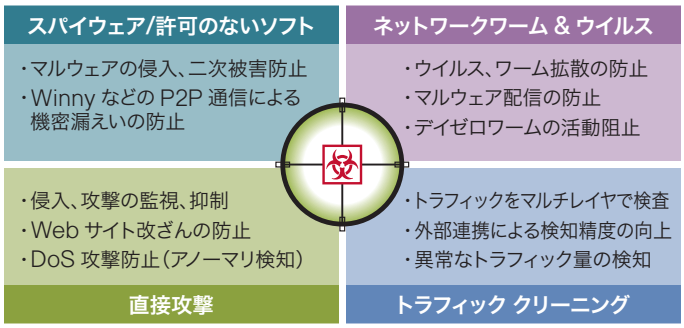
Cisco IPS 4200 シリーズ 侵入検知/防御アプライアンスについては→http://www.cisco.com/jp/go/ips/

Cisco IPS 4200 シリーズ 侵入検知/防御アプライアンス

マルチベクタの脅威検知

現在、ネットワークに接続した無防備のPCは、インターネット/イントラネットの区別なく、ほんの数分のうちにアタックによる被害を受けたり、不正なプログラムを仕掛けられたりするといわれています。Cisco IPS は、このようなネットワーク環境において、多面的な検知能力により、多種多様なネットワークへの攻撃とマルウェアが利用する通信を検知し、重要なビジネス上の資産を保護し、脅威に対抗することを可能にします。

Cisco.com 上の、Cisco Security Center では、ネットワークで起こりうる最新の脅威(インシデント)情報を集約。Cisco IPS での検知内容をもとに、より詳細な対策情報をインターネット上で即座に検索することができます。



Cisco IPS の特徴

スケーラブルなネットワーク監視

Cisco IPS 4200 シリーズにはサーバ数やセグメント数によるライセンス上の制約はありません。VLAN および VLAN トランクを流れる複数セグメントの通信を纏めて保護できます。さらに仮想化により、複数のシステムに対し異なる防御ポリシーの設定が可能です。

外部連携による効果

外部システムとの連携により、誤検知の低減、ネットワーク全体のポリシー変更など、IPS を中心にセキュリティの運用強化が可能です。
特にファイアウォール、ルータ、無線 LAN などとの連携では、シスコ自己防衛型ネットワーク(SDN)が真価を発揮します。

実測値ベースのパフォーマンス

Web 2.0 の展開に合わせ、多様化するメディアの特性に合わせたパフォーマンス値を採用。ビデオ配信など大容量データ向けの「メディアリッチ型」、音声や SQL など頻繁な少量データ向けの「トランザクション型」の値から、利用環境に合わせてシステムを設計することができます。

効果的なセキュリティ管理

デバイスの管理用 GUI に加え、Cisco Security Manager、Cisco Security MARS による統合管理に対応。IPS、ファイアウォールなど複数のデバイスの大量の情報を相関分析し、新たなポリシーに反映させる「みえる化」を実現します。

製品ラインアップ

製品モデル	Cisco IPS 4240	Cisco IPS 4255	Cisco IPS 4260	Cisco IPS 4270
筐体タイプ	ラックマウント(1U)	ラックマウント(1U)	ラックマウント(2U)	ラックマウント(4U)
スループット(メディアリッチ型)	250 Mbps	500 Mbps	2 Gbps	4 Gbps
スループット(トランザクション型)	250 Mbps	500 Mbps	1 Gbps	2 Gbps
検知機能	シグネチャによる検知(カスタムルール作成可能) トラフィック アノーマリ検知 DoS/DDoS 検知(しきい値学習、判定) Host-IDS(Cisco Security Agent:CSA)との連携、複合防御 脆弱性検査ソフトとの連携による、誤検知率低減			
遮断・防御機能	検知不正/異常パケットのドロップ、アラート、リセット ファイアウォールとの連携 スイッチ、ルータ、Wireless LAN コントローラとの連携など			
標準モニタリング インターフェイス	10/100/1000BASE-TX×4	10/100/1000BASE-TX×4	10/100/1000BASE-TX	なし
オプション モニタリング インターフェイス	非対応	非対応	10/100/1000BASE-TX×4(最大 9 ポート) 1000BASE-SX×2(最大 4 ポート)	10/100/1000BASE-TX×4 1000BASE-SX(光ファイバ)×2 合計最大 16 ポート
仮想 IPS(IPS ポリシー仮想化)	対応			

©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)
この資料の記載内容は 2008 年 2 月現在のものです。
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

お問い合せ先

0634-0802-01A-F