

## ネットワークベースの侵入防御でデータセンターの資産を保護する

シスコはデータの喪失やサービスの中断が起こる前にネットワークの脅威を検知し緩和します

### ビジネス上の利点

- データセンター資産の保護
- 実害発生前のセキュリティ事象の検知
- 早期の検知と修復の実現
- データ喪失とサービス中断発生防止に貢献

ネットワークの可用性を保証し知的所有権を保護するため、シスコはネットワークが各種の脅威にさらされていないかどうかを常に監視しています。ネットワークの脅威には内部からの脅威やデータセンター資産への不正アクセスも含まれます。悪意ある行為はファイアーウォールの内外を問わず、通常、ウィルスに感染したホストやセキュリティ侵害を受けたホストが発生源になります。

データセンターには会社のもっとも貴重な資産が保管されているにもかかわらず、境界ベースの侵入防御システム (IPS) ではデー

タセンター内で発生したセキュリティ事象に対して可視性を得ることができていませんでした。境界ベースの IPS では、社内に流入、または社内から流出するトラフィックに含まれている脅威しか検知することができません。そのため、Cisco Computer Security Incident Response Team (CSIRT) は好ましくないネットワークトラフィックがあっても、支店から本店への WAN リンクのパフォーマンスの低下などの問題が発生するまで気づくことができませんでした。

しかし現在、CSIRT ではネットワークベースの IPS を利用して、ユーザが二次的な影響を受ける前に社内で発生するセキュリティ事象の検知と緩和ができるようになっていました。2007 年には、CSIRT チームは 97 % のセキュリティ事象を誰よりも早く見つけ出しています。これに対し、新しい IPS 展開前の 2004 年にはわずか 8 % しか察知できていませんでした。

ネットワークベースの IPS は Rinbot ウィルスを、その存在が知られる前に検知しました。CSIRT はシグネチャを作成し、IPS のセンサーにプッシュしたため、センサーは影響を受ける数百のラボシステムを特定することができました。早い段階での検知と修復により、被害の拡大が防止されました。

**“ネットワークベースの IPS を利用することで、内部のセキュリティ事象に対しても、サービスの中断や知的所有権の喪失、ウィルス感染などといった二次的被害をユーザが受ける前に検知し緩和することができるようになりました”**

Gavin Reid, Manager of Computer Security Incident Response Team, Cisco

CSIRT はネットワークの脅威に対し、データ喪失やサービスの中断を引き起こす前に先手を打って対処できるようになりました。2007 年の 3 月から 6 月にかけて、シスコは社内のシステムを遠隔制御するコマンド & コントロールサーバを毎週、複数見つけ排除していました。

### 詳しい情報はこちら

その他のビジネスソリューションに対するシスコ IT の事例研究は、シスコ IT 内の Cisco on Cisco ウェブサイトからご覧になれます。<http://www.cisco.com/web/JP/ciscoitnetwork/index.html>

## 付記

この文書に記載されている事例は、シスコが自社製品の展開によって得たものであり、この結果には様々な要因が関連していると考えられるため、同様の結果を別の事例で得られることを保証するものではありません。

この文書は、明示、黙示に関わらず、商品性の保証や特定用途への適合性を含む、いかなる保証をも与えるものではありません。

司法権によっては、明示、黙示に関わらず上記免責を認めない場合があります。その場合、この免責事項は適用されないことがあります。

©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