

侵入防御システムをシスコ ROS に外部委託する Scientific Atlanta

24 時間の監視体制に加え、詳しい説明と推奨対応措置の提供によりセキュリティの脅威への素早い対応が可能になります。

ビジネス上の利点

- セキュリティイベントの早期認識
- 誤検知数の削減
- セキュリティイベントとネットワークパフォーマンスに対する可視性
- 熟練のネットワークセキュリティスタッフへの容易なアクセス

2006 年にシスコの一部となった Scientific Atlanta では、侵入防御システム (IPS) の管理を外部委託しています。同社には、ネットワークセキュリティインシデントを 24 時間監視したり、IPS のセンサーのシグネチャを定期的に新しいものに更新したり、誤検知を減らすようにセンサーを調整したりするスタッフがいません。

そこで、Scientific Atlanta の IT グループではセキュリティ管理業務を外部委託することにし、委託先にシスコ ROS を選択しました。シスコ® ROS は、タイムリーで確実な情報提供や対応時間の

SLA、シスコの IPS センサーに対する深い理解を売りにしていることが選択基準になりました。

IPS 管理の外部委託にあたり、シスコ ROS と、Scientific Atlanta のネットワークセキュリティチームはビジネス要件と技術要件について話し合いました。話し合った要件は、通知が必要な攻撃のタイプをはじめ、ネットワーク内で監視が必要な箇所、資産の価値、連絡方法、必要なセンサーのタイプなどでした。監視機器導入の第 1 段階で、Scientific Atlanta はネットワークの境界にあったセンサーを Cisco IPS 4200 シリーズセンサーに置き換えました。次の段階では、シスコ ROS のアドバイスを元に社内ネットワークに IPS センサーを導入しました。

人の目によって脅威に該当するパターンのネットワークトラフィックがないかどうかを監視する専門のチームを持つことで、Scientific Atlanta では潜在的なセキュリティの脅威を早期に認識することが可能になりました。また、Scientific Atlanta がシスコ ROS に提供した資産価値やオペレーティングシステムなどの情報は誤報を減らすのに役立ちました。さらに、Scientific Atlanta ではオンラインポータルを利用して 24 時間いつでもセンサーの動きを見ることができるようになっています。

“シスコ ROS が管理するセキュリティサービスで最も重要なのはセンサーが収集した生のデータを対応可能な情報に変換することです。トラブルチケットにはセンサーが収集したデータの重要性が説明され、推奨される対応措置が記されているのでセキュリティチームの対応の効率は向上し、それにかかずに時間は短縮されています”

Scott Stanton, Information Security Architect, Scientific Atlanta

シスコ ROS が管理するセキュリティサービスはセンサーが収集した生のデータを対応可能な情報に変換します。トラブルチケットにはセンサーが収集したデータの重要性が説明され、推奨される対応措置が記されているのでセキュリティチームの対応の効率性は向上し、対応に要する時間は短縮されています。

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/ciscoitwork/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