



# 侵入防御システム管理の 外部委託

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



## A Cisco on Cisco Case Study: Inside Cisco IT

# 概要

- 課題

  - IPS センサーを監視し管理する

- ソリューション

  - シスコ ROS の IPS 管理サービス

- 成果

  - セキュリティイベントの早期認識

- 次のステップ

  - ルータやファイアウォール上でのトラフィック遮断による能動的防御

# 課題

## IPS センサーを監視し管理する

- Scientific Atlanta にいなかった IT スタッフ

  - センサーが収集したデータの 24 時間監視業務の担当者

  - シグネチャの定期的な更新作業の担当者

  - 誤検知を減らすために行うセンサーの継続的調整作業の担当者

- 管理サービスプロバイダーの選定条件

  - 確実な情報提供

  - 対応時間の SLA

  - シスコの IPS センサーに対する深い理解

# ソリューション

## シスコ ROS の IPS 管理サービス

- 事前の話し合い(要件定義)

  - 通知が必要な攻撃のタイプ

  - 監視が必要なネットワークの場所

  - 資産価値

  - 連絡方法

  - 推奨センサーモデル

- センサーの2段階の導入

  - ネットワーク境界へ

  - 社内ネットワークへ

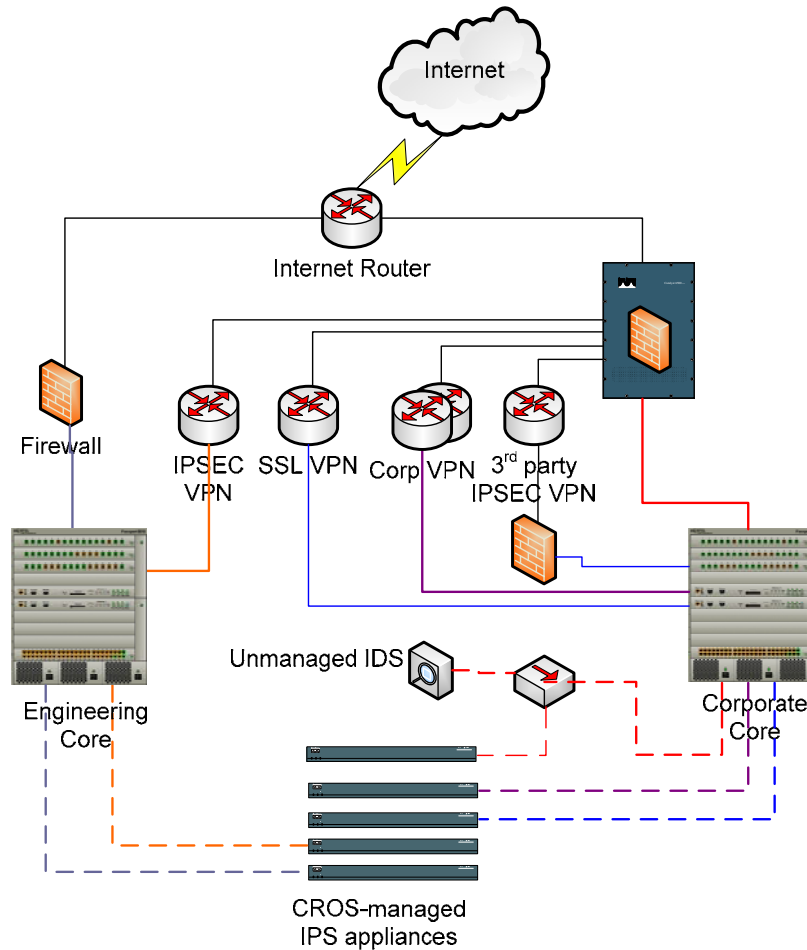
- 24 時間の監視体制

- E メール、または電話による通知

  - Scientific Atlanta は、Eメールのトラブルチケットで報告されている脅威に関する詳しい情報をオンラインポータルから閲覧可能

# ソリューション

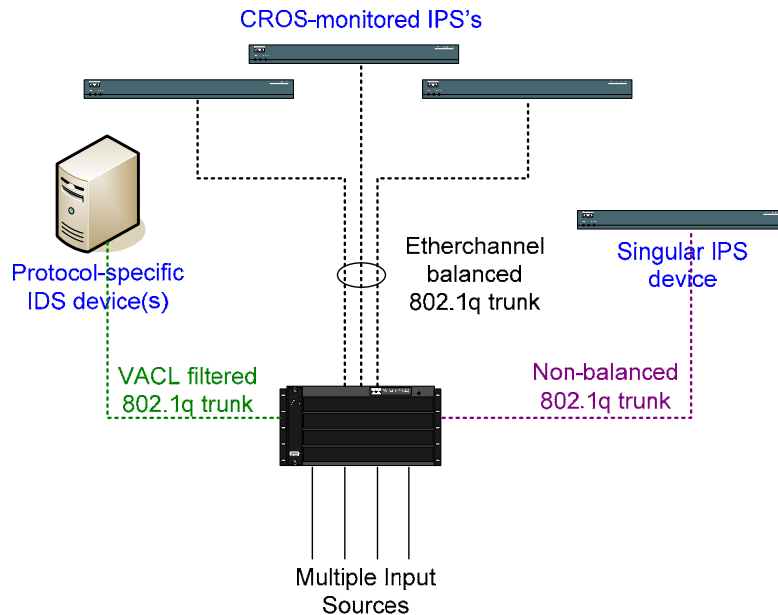
## ネットワーク境界への IPS の導入



Dotted lines indicate SPAN or Monitor outputs to IPS appliances. In some cases, a single IPS will receive multiple SPAN inputs.

# ソリューション

## 社内ネットワークへの IPS の導入



6504 configuration uses RSPAN to mirror inputs to a target VLAN. This VLAN is trunked via 802.1q to the IPS devices. VACLs may be used to filter IP's or src/dst ports.

# 成果

## セキュリティイベントの早期認識

- 誤検知数の削減
- オンラインポータルを利用することによるセキュリティイベントやネットワークパフォーマンスに対する可視性
- 熟練スタッフへの容易なアクセス

「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ます」

Scott Stanton  
Information Security Architect  
Scientific Atlanta, a Cisco Company

# 次のステップ

## 能動的防衛

- 将来的にシスコ ROS はシスコのルータやファイアウォール上で悪意あるトラフィックを遮断

本物の脅威かどうかは Scientific Atlanta が事前に判断

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、  
Cisco on Cisco ウェブサイトからご覧ください。

<http://www.cisco.com/web/JP/ciscoitnetwork/index.html>



**Americas Headquarters**  
Cisco Systems, Inc.  
San Jose, CA

**Asia Pacific Headquarters**  
Cisco Systems (USA) Pte. Ltd.  
Singapore

**Europe Headquarters**  
Cisco Systems International BV  
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks.; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, FastStep, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, IQ Expertise, the IQ logo, IQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0801R)