



デスクトップの
セキュリティ
侵入防御ソフトウェアをア
ップデートし、エンドポイントの
セキュリティを強化する



A Cisco on Cisco Case Study: Inside Cisco IT

概要

- 課題

 - 進化し続ける脅威から全世界 70,000 台のデスクトップを保護する

- ソリューション

 - Cisco Security Agent

- 成果

 - セキュリティを強化、必要な IT リソースを削減

- 次のステップ

 - 新しいデスクトップセキュリティポリシーを適用する

課題

進化し続ける脅威から全世界 70,000 台のデスクトップを保護する

- 脅威の主体の変化に対応する

2004 年: ウィルス、ワーム、トロイの木馬

2008 年: スパイウェア、ボットネット、ルートキット、スパイ型攻撃、ソーシャルネットワーキングサイト

2010 年: 未知

- 復旧と駆除にかかる高い負担を回避する:

1 件あたり 25 万ドル～ 250 万ドル

- 頻発する OS やアプリケーションの脆弱性に対するパッチあての回数を減らす

ソリューション

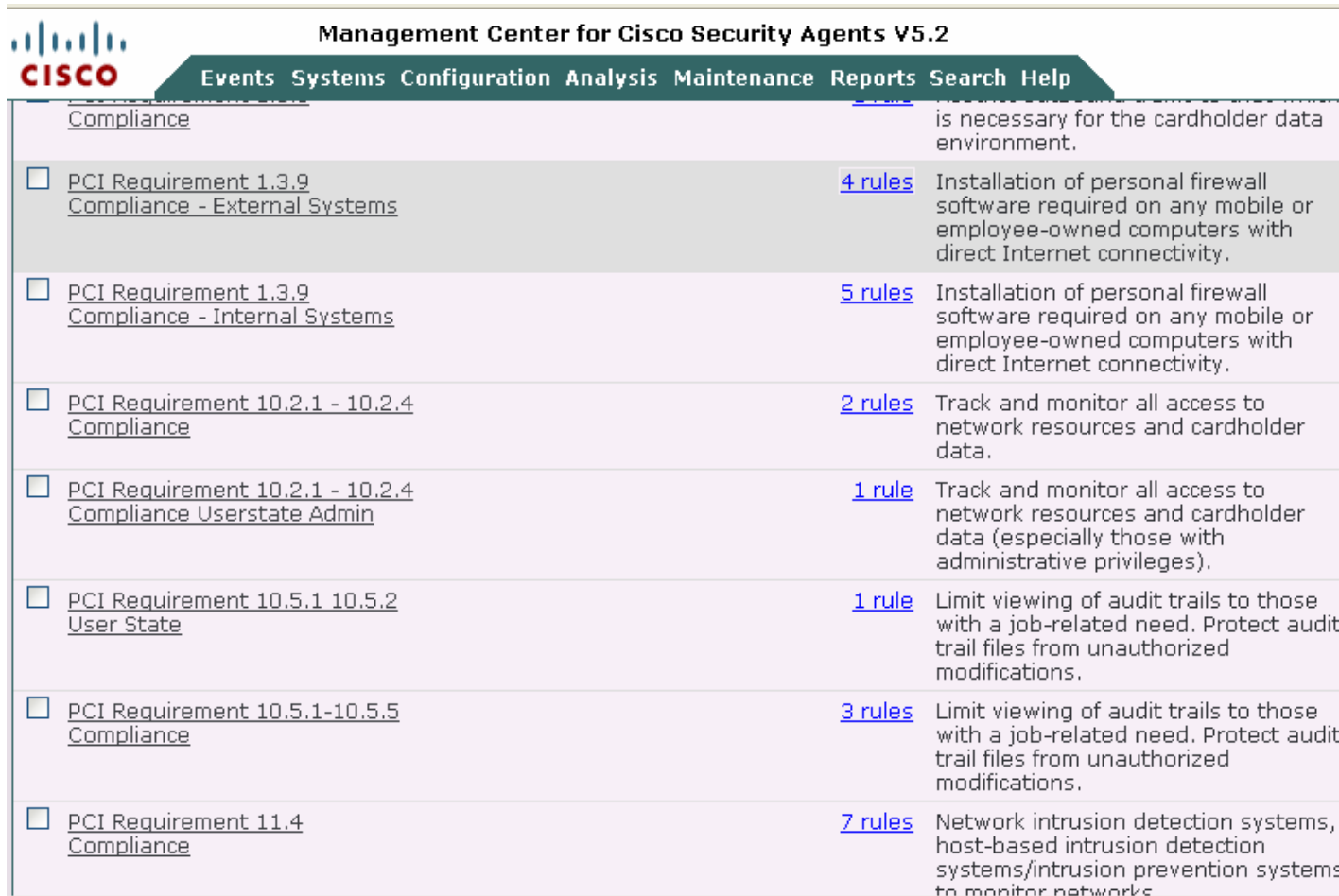
Cisco Security Agent

- 通常見られないようなアプリケーションの振る舞いを見つけ、ポリシーに基づいて対応：許可、拒否、ユーザによる選択



ソリューション

事前定義のポリシーとカスタムポリシー



The screenshot displays the Management Center for Cisco Security Agents V5.2 interface. The top navigation bar includes the Cisco logo and menu items: Events, Systems, Configuration, Analysis, Maintenance, Reports, Search, and Help. Below the navigation bar is a table listing various PCI compliance requirements and their associated rules.

Requirement	Rules	Description
Compliance		is necessary for the cardholder data environment.
<input type="checkbox"/> PCI Requirement 1.3.9 Compliance - External Systems	4 rules	Installation of personal firewall software required on any mobile or employee-owned computers with direct Internet connectivity.
<input type="checkbox"/> PCI Requirement 1.3.9 Compliance - Internal Systems	5 rules	Installation of personal firewall software required on any mobile or employee-owned computers with direct Internet connectivity.
<input type="checkbox"/> PCI Requirement 10.2.1 - 10.2.4 Compliance	2 rules	Track and monitor all access to network resources and cardholder data.
<input type="checkbox"/> PCI Requirement 10.2.1 - 10.2.4 Compliance Userstate Admin	1 rule	Track and monitor all access to network resources and cardholder data (especially those with administrative privileges).
<input type="checkbox"/> PCI Requirement 10.5.1 10.5.2 User State	1 rule	Limit viewing of audit trails to those with a job-related need. Protect audit trail files from unauthorized modifications.
<input type="checkbox"/> PCI Requirement 10.5.1-10.5.5 Compliance	3 rules	Limit viewing of audit trails to those with a job-related need. Protect audit trail files from unauthorized modifications.
<input type="checkbox"/> PCI Requirement 11.4 Compliance	7 rules	Network intrusion detection systems, host-based intrusion detection systems/intrusion prevention systems to monitor networks

ソリューション

展開

- 400 ユーザによるパイロット
- Cisco Security Agent によるアプリケーションの正常な振る舞いの学習 (5 種類の複雑なアプリケーションを利用)
 - シスコで利用されている 10,000 のアプリケーション全てでの学習は不要
- ユーザ側の負担が少なくなるように注意しながらのポリシー定義
- 全社展開
 - 全世界何万人もの従業員に 3 週間でプッシュ
- 1200 の試験場にある製造環境への展開
 - 感染拡大防止のため、試験場相互間の通信はせず、中央サーバとの通信に制限することをポリシーに明記

ソリューション

中央管理

- ブラウザベースの Management Center(管理ソフトウェア)でのソフトウェアの配布、セキュリティポリシーの作成、アラートの監視、レポートの生成
- 最初の展開には 2~3 週間の間、2 人のエンジニアのおよそ 65% の時間を拘束
- 現在では、新しいポリシーが必要なときに Cisco Security Agent の管理のため、シスコ IT の 2 人の従業員の 10% の時間のみ拘束

成果

セキュリティの強化

- 攻撃後の復旧にかかっていた 400 万ドルのコストを回避
- 必要な IT リソースを 12 人のフルタイム従業員から 1 人分以下に削減
- 頻繁に必要なだったパッチあて作業を削減
- 管理の厳しさに柔軟性を持たせることで、各部門のデスクトップセキュリティのニーズに対応

次のステップ

新しいセキュリティポリシーを適用する

- リムーバブルメディアの利用を管理する
- 各種のアプリケーショントラフィックを区別し、個別に対応を変える
- Windows Vista PC での IPv6 の使用を遮断し制限する
- 新しいセキュリティ戦術を立案するために、アプリケーションの振る舞いに関する情報をさらに収集する

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/ciscoitwork/index.html>



Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA

www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912

www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands

www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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.



©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSR, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0704R)