



Cisco IT@Work 事例研究:
**Cisco Security Agent の
Windows PC への展開**

Cisco Information Technology

May 4, 2004

概要

Cisco.com

- 課題

PC や携帯端末など、個々の資産をデスクトップレベルで保護し、ウィルスの駆除や、それに付随する生産性の喪失に伴うコストを削減する

- ソリューション

37,000 台の Windows PC への Cisco Security Agent の展開

- 成果

2004 年 4 月、bagle.aa ウィルスが猛威をふるった際に、CSA によって保護されたコンピュータの 99.86 % が感染を免れたことで、その効果を実証

- 次のステップ

より厳格なポリシーの作成と、社内および顧客向けの Windows 2000 サーバへの適用

課題: 資産を保護し、コストを削減する

Cisco.com

- 増え続けるウィルスやワームの駆除にかかる時間と費用の削減

ウィルス駆除とそれに付随した生産性喪失に伴うコストは 2003 年には 280 億ドルだったが、2007 年には 750 億ドルに増加する見込み (出典: Radicati Group, 2003)

- PC や携帯端末など、個々の資産に対するデスクトップレベルでの保護

Cisco PIX® Firewalls や Cisco NIDS、アンチウィルスソフトなどは、デスクトップ向けに特化したソリューションではない

- 通常業務を妨げないことを確実にするソリューションにより、従業員の生産性を保護

ソリューション: 動作に基づく保護機能を展開

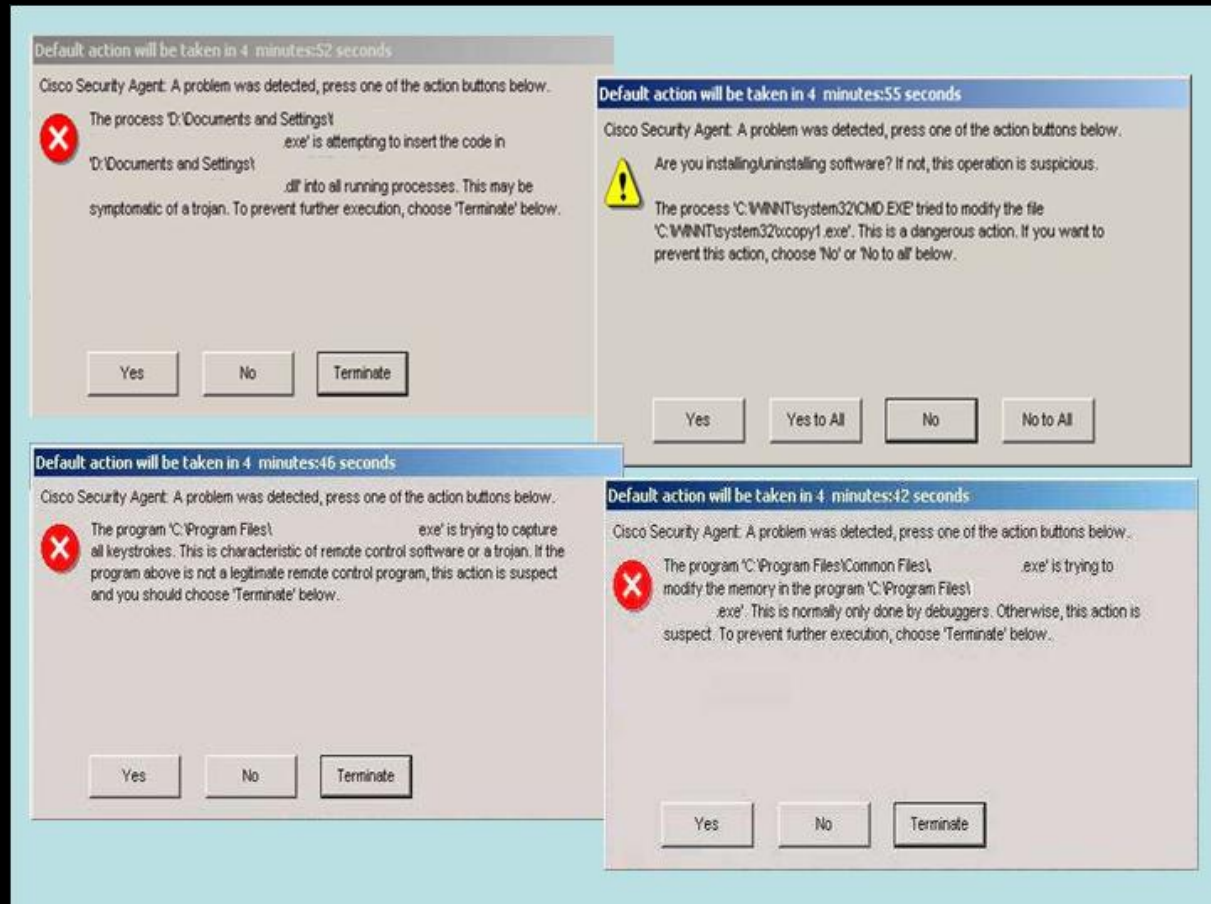
Cisco.com

- 従業員の PC へ Cisco Security Agent を展開

「シグニチャ」ではなく、「動作」に基づいた保護機能

- アプリケーションの動作を規定するポリシーを作成

アプリケーションの動作が規定の範囲を超えた場合、それを許可するか拒否するか、またはユーザに問い合わせるかを判断



ソリューション: ポリシーを定義し、全世界に展開

Cisco.com

- 500 ユーザによる試験運用を行いポリシーを調整

PC の保護と従業員の利便性との絶妙なバランス; アプリケーション動作の許否を問うポップアップの表示を最小限にする

- 全世界の従業員にソフトウェアを配信
- ユーザに対し、デスクトップセキュリティ、および Cisco Security Agent の効果的な利用法に関する教育を実施

The screenshot displays the Management Center for Cisco Security Agents interface. A rule is being configured with the following details:

- Action:** Query User (Default Deny). The text used to query the user is "Are you installing/uninstalling software? If not, this op".
- When:** Applications in any of the selected classes: <All Applications>, <Network Applications>, <Processes created by Network Applications>, <Processes created by Servers (TCP and UDP)>, <Processes executing downloaded content>.
- Operations:** Attempt the following operations: Read, Write.
- Files:** On any of these files: %system executable files, %system libs and drivers.

Annotations in red text and arrows point to these specific configuration elements:

- "Log all suspicious activity." points to the top of the rule configuration area.
- "Query the user (default deny) ..." points to the "Query User (Default Deny)" action.
- "... when any application ..." points to the "Applications in any of the selected classes" list.
- "... tries to write ..." points to the "Attempt the following operations" section.
- "... system executables, libraries, or drivers." points to the "On any of these files" list.

成果: セキュリティを強化、コストを削減

Cisco.com

- ウィルスやワームの駆除とそれに付随するコストを大幅に削減
- ウィルスの進行が抑えられ、従業員の生産性が向上
展開したポリシーがあまり厳格ではなくても有効
- ソリューションの展開以前に感染していたシステムを検知

成果: bagle.aa ウィルスを抑え込む

Cisco.com

- 2004 年 4 月、ウィルスが蔓延
- パッチ適用や .DAT ファイルの更新が間に合わない
- Cisco Security Agent を導入している 38,370 台のデスクトップのうち感染の危機に直面したのは 600 台以上 – 620 人のユーザが、感染しているファイルを開封
- Cisco Security Agent は、不審な動作(レジストリファイルの書き換え)を警告することで、54 人を除く全てで、ウィルスの感染を阻止
 - ウィルスに感染したユーザは、不審なアプリケーションが E メールリソースにアクセスしようとしていると警告された際、「はい」をクリックしていた
- 感染拡大を 90% 抑えたことで、駆除を容易に、少ないコストで実施
 - ユーザがこうしたファイルを開いてしまう可能性を減らすためのポリシー改善というステップにもつながる

次のステップ: 概要

Cisco.com

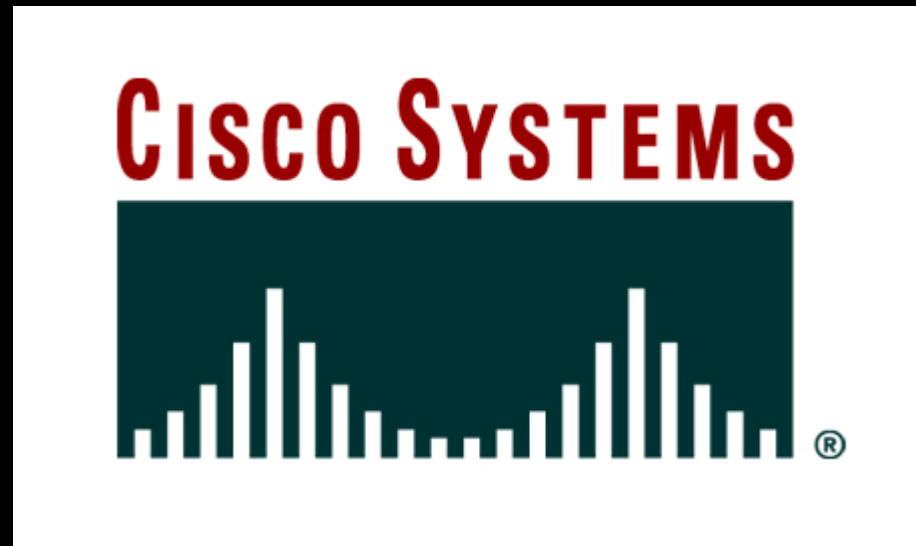
- より厳格なポリシーの作成
- ネットワーク アドミッション コントロール(NAC)を使い、ネットワークへのアクセスを Cisco Security Agent がインストールされた従業員のみに制限
- 社内および顧客向けの Windows 2000 サーバに Cisco Security Agent をインストール
 - Cisco CallManager や Cisco Unity software などを含む
- Cisco Security Agent およびネットワーク侵入検知システム(NIDS)から CiscoWorks VMS/SecMon や Cisco セキュリティ情報管理システムへ送られる情報を組み合わせることによる、ネットワークの全般的な健康状態を管理する包括的な視点の構築

教訓: 概要

Cisco.com

- ポリシーの調整に時間をかけること
- 幅広いユーザ層やアプリケーションを使って試験運用を行うこと
- アプリケーションの許否を判断する必要も出てくるため、ユーザを教育すること

その他、各ビジネスソリューションに対する Cisco IT の事例研究は、
Cisco IT @ Work をご覧ください
<http://www.cisco.com/jp> (シスコシステムズ→ Cisco IT @ Work)



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。