

[ 導入事例 ]

## 自己防衛型ネットワークでセキュリティを強化 利便性を損なうことなく情報の安全性を高める

### セコムトラストネット株式会社



「トラステッド・サービス・プロバイダー」というコンセプトを打ち立て、多岐にわたるセキュリティサービスを提供するセコムトラストネット。ここでは社内のセキュリティをさらに強化するために、シスコの自己防衛型ネットワークが導入されている。利便性と安全性を両立できるメカニズムを活用によって、これからの企業が目指すべき“セキュリティモデル”を確立。今後はこのネットワークをセコムグループ全体のショーケースとして活かすことで、セコムのブランド構築に役立てていくことも視野に入っているという。インテグレーションはシスコと強い協業関係にある日本アイ・ビー・エム(IBM)が担当。自己防衛型ネットワークはIBMが提唱する“オートノミック・コンピューティング”を実現する上でも、重要な役割を果たすと評価されている。

#### 導入の背景 / 課題

- ・情報セキュリティのトップ企業として、社内の情報セキュリティにも積極的に取り組んできたが、2004年11月にはそれをさらに強化するためのプロジェクトを発足した。
- ・自己防衛型ネットワークに関してはそれ以前から注目しており、今回のプロジェクト発足に伴い導入が決定した。

#### 導入ソリューション

- ・シスコ自己防衛型ネットワーク
  - Cisco Security Agent( CSA )
  - Network Admission Control( NAC )
- ・シスコネットワークングソリューション
  - Cisco Catalyst 6503
  - Cisco Catalyst 2950
  - Cisco Aironet

#### 導入効果(期待される導入効果)

- ・利便性を損なわずにセキュリティを強化可能。セキュリティレベルを満たさないPCがネットワークに接続できなくなるため、管理に膨大な手間をかけることなくネットワーク全体のセキュリティレベルを維持できる。
- ・ゼロデイアタックへの対応が可能。CSAによってPCの挙動を監視することで、対応策が公表されていないウイルス/ワームの被害を回避できる。
- ・過失によって発生するセキュリティ問題の回避が可能。ユーザーの挙動もCSAによって監視・ログ取得することが可能になるので、問題のある行為を防止できる。
- ・情報漏えいの防止。上記の効果の結果として、情報漏えいの防止が容易になる。

### 情報セキュリティのリーディング企業が 自己防衛型ネットワークを社内に導入

情報セキュリティをいかにして確立するか。これはいまや全ての企業にとって、最も重要な経営課題のひとつになっている。その背景としては、企業からの個人情報漏えい事件が相次いで発生したことや、2005年4月から「個人情報保護法」が全面施行されたことなどが挙げられる。個人情報の保護は法的に“企業責任”とみなされるようになっており、適切な情報セキュリティを確立できない企業は、法的リスクにさらされることになるのだ。

情報セキュリティを確立するには、セキュリティポリシーの策定や運用ルールの明確化、社員教育などの組織的・人的な対応が欠かせないことはいままでもない。しかし人間は常に“過失する可能性のある存在”であるため、適切な運用を徹底させるには、システムそのものにセキュリティ機能を組み込むことも求められる。これは決して簡単なことではない。セキュリティレベルの低いPCがたった1台だけでもネットワークに接続されれば、ネットワークシステム全体のセキュリティが脅かされることになるからである。

このような観点からシスコは“自己防衛型ネットワーク”を提唱し、その実現に向けた取り組みを進めてきた。自己防衛型ネットワークとは、ネットワーク自身がネットワークに接続されるPCのセキュリティレベルをチェックし、必要な対応を行うというメカニズム。十分なセキュリティレベルに達していないPCが接続された場合には、そのPCを正規ネットワークに接続できないようにしたり、セキュリティ確保に必要なソフトウェアのインストール等を行った上で正規ネットワークに接続するといった対応を、自動的に行えるのである。これによってセキュリティレベルの低いPCがネットワークに紛れ込むことを防ぎ、コンピューターウイルス/ワームの被害や情報漏えい等を回避可能。このメカニズムは「Network Admission Control (NAC)」に対応したネットワーク機器や管理サーバー、クライアントエージェントを導入することで実現でき、さらに各PCに「Cisco Security Agent (CSA)」を導入しておけば、PC上で稼働するソフトウェアの挙動を自動的にチェックし、許可されない動きを防止することも可能なのだ。

このソリューションの可能性にいち早く着目し、すでに導入を完了しているのがセコムトラストネットである。同社は情報セキュリティ市場におけるリーディングカンパニーであり、インターネット時代に“安心”と“信頼”をもたらす「トラステッド・サービス・プロバイダー」というコンセプトを打ち立てた企業として知られている。このコンセプトに基づき、世界最高水準の堅牢性を誇るセキュアデータセンターを“サイバーセキュリティサービス”の戦略拠点として、顧客のサーバーやデータを安全に利用してもらうために必須となる

自己防衛型ネットワークでセキュリティを強化  
利便性を損なうことなく情報の安全性を高める  
セコムトラストネット株式会社

監視サービスや認証サービス等を展開、刻々と進化していくネット犯罪にも最新テクノロジーを駆使した万全の体制で、最高の安全と安心を提供している。

もちろん社内のセキュリティへの取り組みにも積極的に取り組んでおり、自社のデータセンターサービスが提供するIDS（侵入検知システム）やウイルスゲートウェイの活用、セキュリティパッチの迅速な適用などを進めてきた。そして2004年11月には社内の情報セキュリティをさらに強化するための、全社的なプロジェクトに着手。この一環として自己防衛型ネットワークの導入が決定されたのである。2005年4月には全社展開を開始、その翌月に約300台のクライアントPCと約50台のサーバーを対象にした自己防衛型ネットワークを完成させているのだ。



社員証を兼ねたICカードで、ユーザ認証を行う。



「自己防衛型はセキュリティと利便性の両立が可能です。  
今回の取り組みは企業の“セキュリティモデル”確立に向けた  
チャレンジであり、セコムのブランド構築の一環でもあります」

セコムトラストネット株式会社  
ネットワークエンジニアリング部  
部長  
小笠原 寛 氏

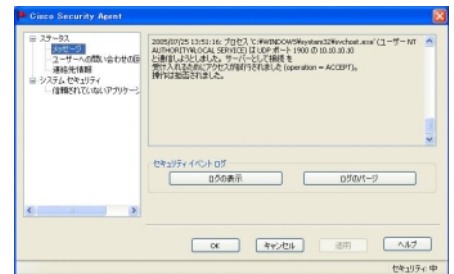
最大の目的はセキュリティと利便性の両立  
ゼロデイアタックへの対応にも大きな期待

「自己防衛型ネットワーク導入の最大の目的は、高レベルのセキュリティ維持と利便性を両立することにあります」と説明するのは、セコムトラストネット ネットワークエンジニアリング部で部長を務める小笠原氏。一般にセキュリティ強化に向けた対策は利便性を損なう傾向があり、ユーザーにより多くの作業負担を強いケースが珍しくないが、自己防衛型ネットワークであればユーザーや管理者の負担を増大させることなく、適切なセキュリティレベルを維持できるという。たとえばウイルスやワームの被害を回避するには、ウイルス対策ソフトウェアのパターンファイルを常に最新のものに更新する作業や、Windows Updateによるセキュリティパッチの適用が欠かせない。しかしパターンファイルの更新は自動化が容易だが、パッチ適用の管理はユーザーや管理者に大きな負担を強いることになる。これに対して自己防衛型ネットワークであれば、十分なパッチを適用していないPCを自動検出し、ネットワークへの接続を拒否したり、必要なパッチを導入した上で再接続させるといったことを自動的に行えるのだ。「ひとつの完結したソリューションとしてここまで実現できるのは、シスコの自己防衛型ネットワーク以外にはありません」

その一方で「自己防衛型ネットワークの導入はゼロデイアタックへの対応にも有効」というのは、セコムトラストネット ネットワークエンジニアリング部の片山氏だ。ゼロデイアタックとは、セキュリティホールが発見されたときに、パターンファイルやパッチ等の対応策が公開される前に行われる攻撃のこと。攻撃を受ける側のシステムが十分な対応を行えないため、被害が拡大しやすいという特徴がある。しかしすべてのPCにCSAが導入されていれば、パターンファイルや最新パッチが適用されていなくても、システムに被害をもたらす動きを阻止できるのである。「CSAがどれだけの効果を発揮するのは設定内容にも依存しますが、デフォルトのままでもかなり高いセキュリティレベルを確保できます」と片山氏。セコムトラストネットではさらに、レジストリ変更への対応や特定ファイルへのアクセス拒否等のカスタマイズされた設定を行うことで、より高いレベルのセキュリティを実現しているという。

小笠原氏も「CSAは非常に有力なソリューション」だと指摘。2004年11月に始まったセキュリティ強化プロジェクトでは、セキュリティの現状把握から組織や体制の見直し、システム面での問題の洗い出しなどが徹底して行われたが、目標となるセキュリティと現状とのギャップを埋める手段として、CSAが果たした役割は大きいと説明する。「従来のシステムではユーザーの過失で発生する情報漏えいを防ぐことは困難でした。しかしCSAならこれも防止することが可能です」

Cisco Security Agent( CSA )のエラー画面



ネットワークで不正な通信があった



インターネットエクスプローラで不正な動作があった



許可なくソフトウェアをインストールした



「自己防衛型ネットワークの導入はゼロデイアタックへの対応にも有効。デフォルトのままでも十分ですが、設定のカスタマイズでさらに高いレベルのセキュリティを実現できます」

セコムトラストネット株式会社  
 ネットワークエンジニアリング部  
 片山 光太郎 氏

## インテグレーションは日本IBMが担当 活用効果をIBM基礎研究所で徹底検証

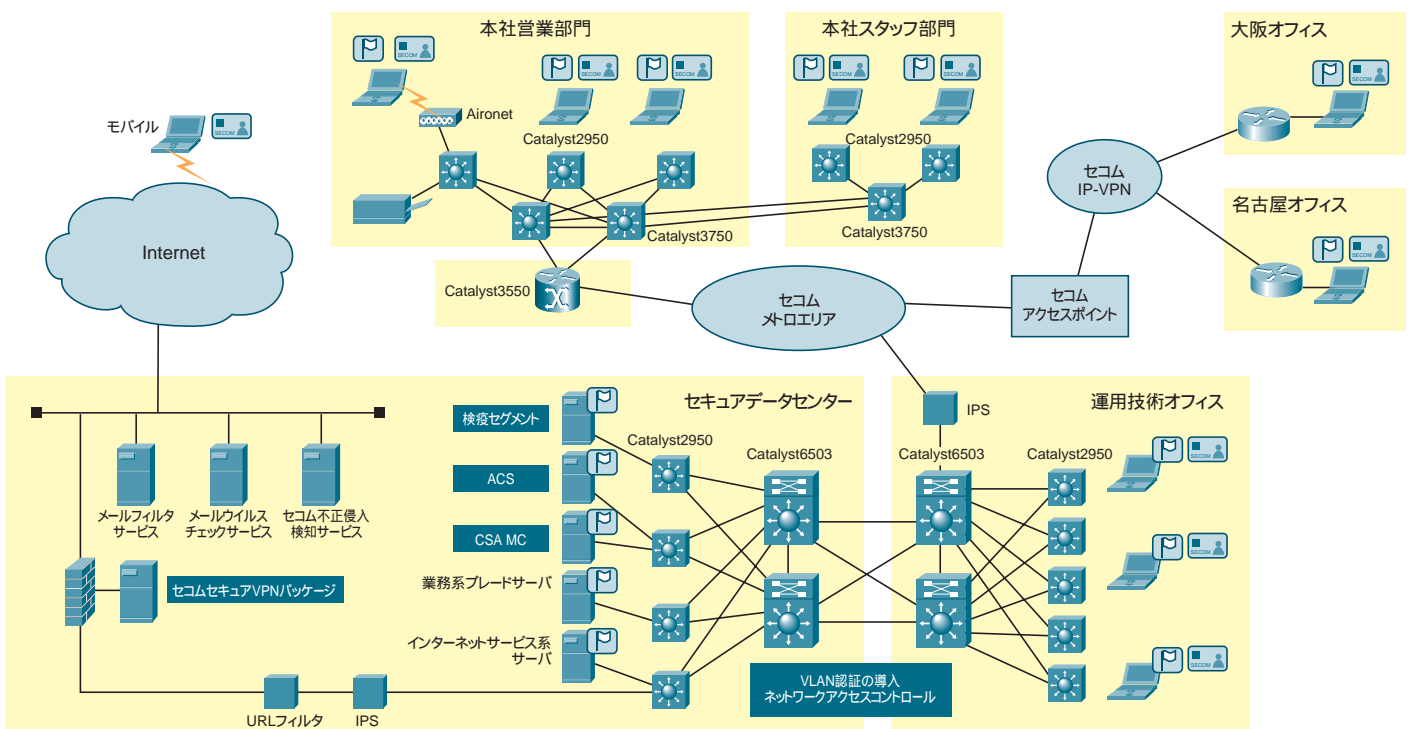
セコムトラストネットでは、自己防衛型ネットワークの導入に伴い、社内ネットワークの再構築も行われている。今回構築されたネットワークの構成は図に示すとおりだ。

まずネットワークのコア部分は「Cisco Catalyst6503」を採用。ディストリビューションには「Cisco Catalyst 2950」が導入されている。一部の事業所では無線LANアクセスポイントとして「Cisco Aironet」が設置されており、クライアントPCを無線LANで接続可能。ユーザー認証はドメインレベルだけではなく、認証VLANによるネットワーク認証も行われることになっている。

このネットワークに接続されるすべてのクライアントやサーバーには、NACの構成要素となる「Cisco Trust Agent」とCSAが導入されている。「Cisco Trust Agent」はクライアントやサーバーのソフトウェア構成やセキュリティパッチ導入状況をチェックし、不適切なコンピューターのネットワーク接続を防止する。CSAは前述のようにコンピューター内部の挙動を監視、ウイルスやワーム、スパイウェアからコンピューターやネットワークを保護する。

自己防衛型ネットワークのインテグレーションは日本アイ・ビー・エム（IBM）が担当した。「IBMはシスコと強い協業関係にあり、自己防衛型ネットワークに関してもかなり深いレベルの検証を行っています」と片山氏。このソリューションに関して最も高い能力のあるインテグレーターだと評価しているという。

セコムトラストネット 社内セキュリティ強化プロジェクトネットワーク全体構成





## 「シスコの自己防衛型ネットワークはIBMにとっても魅力的なソリューション。 セキュリティのオートノミック化を実現する上で 重要な役割を果たすと考えています」

日本アイ・ビー・エム株式会社  
TS&NWサービス事業 NW & Siteインテグレーション・サービス コンピテンシー  
部長  
前田 浩 氏

「シスコの自己防衛型ネットワークはIBMにとっても魅力的なソリューション」というのは、日本アイ・ビー・エム ネットワーク・サービス事業部で部長を務める前田氏だ。IBMはオートノミックコンピューティングを提唱し、環境変化に対して自律的に対応できるシステムの実現に向けた取り組みを積極的に進めてきた。すでにリソースの仮想化や動的な割り当て、障害の自動修復などを可能にするテクノロジーや製品、ソリューションを提供しているが、エンドユーザーまで行き届いたセキュリティをオートノミックに実現する上で、自己防衛型ネットワークは重要な役割を果たすという。「特にCSAに関しては、米国シスコの開発者に協力していただきながら、IBMの東京基礎研究所で徹底的な検証を行いました。CSAならPCの挙動をプリミティブなレベルで監視し、アノマリー(変則的な挙動)をアーキテクチャーとして防止できます。PC全体の動きをポリシーベースで管理できる、優れたソリューションだと評価しています」

### セコムグループのブランド構築の一環として 目指すべき“セキュリティモデル”を提示

セコムトラストネットは、今後は自己防衛型ネットワークの機能活用を、さらに拡大していく計画だという。そのひとつとして挙げられているのが、PC上で行われたファイルコピー等の操作ログの取得である。この機能はCSAによって実現可能だ。

また社外からの接続にも、自己防衛型ネットワークの機能を適用していく計画だ。セコムトラストネットではデスクトップに固定されたPCだけではなく、持ち歩いて利用するモバイル型のPCも活用されており、社外からのモバイル接続(インターネットVPN)も2003年に「Cisco VPN 3000コンセントレータ」を導入することで可能になっている。最新の「Cisco VPN 3000コンセントレータ」はNACに対応しているが、すでに導入されているものをアップグレードすることで、VPN接続でも自己防衛機能を利用する予定だという。

「利便性とトレードオフの関係にあるセキュリティ対策は、すでに過去のものだけといえます」と小笠原氏。これからのセキュリティ対策は利便性と両立すべきであり、今回の取り組みはこのコンセプトを具現化するための、重要なチャレンジなのだという。これによってこれからの企業が目指すべき“セキュリティモデル”を提示することが可能になり、情報セキュリティのトップ企業としても大きな貢献を果たせるからだ。「今後はこのネットワークを、セコムグループ全体のショーケースとして活かすことも考えています。自己防衛型ネットワークの導入は単なるセキュリティ対策ではなく、セコムのブランド構築の一環でもあるのです」

#### Profile

### セコムトラストネット株式会社

本 社: 東京都渋谷区神宮前 1-5-1  
セコム本社ビル 4F  
設 立: 1985年8月  
資本金: 14億6880万円

インターネット時代に“安心”と“信頼”をもたらす「トラステッド・サービス・プロバイダー」というコンセプトを打ち立てた、情報セキュリティ市場におけるリーディングカンパニー。1985年に設立されたセコムネット株式会社を前身に、2000年4月にセコムグループにおけるサイバーセキュリティ事業の中核企業として「セコムトラストネット」と社名変更した。世界最高水準の堅牢性を誇るセキュアデータセンターを戦略拠点とし、データセンターサービスや監視系サービス、認証系サービス等を展開、安全・安心してインターネットを利用するための各種セキュリティサービスを提供している

<http://www.secomtrust.net/>

©2005 Cisco Systems, Inc. All rights reserved.

Cisco, Cisco Systems, および Cisco ロゴは米国およびその他の国における Cisco Systems, Inc. の商標または登録商標です。

その他、記載されている会社名、製品名は各社の商標、登録商標または登録サービスマークです。

この資料の記載内容は2005年8月現在のものです。

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。



シスコシステムズ株式会社

URL: <http://www.cisco.com/jp/>

問合せURL: <http://www.cisco.com/jp/go/contactcenter>

〒107-0052 東京都港区赤坂2-14-27 国際新赤坂ビル東館

TEL: 03-6670-2992

電話でのお問合せは、以下の時間帯で受付けております。

平日 10:00 ~ 12:00 および 13:00 ~ 17:00

お問い合わせ先