TrendMicro
Network VirusWall 1200
アーリーアダプタープログラム参加事例

EARLY ADAPTER CASE STUDY

TREND MICRO

古河インフォメーション・テクノロジー株式会社様

◆評価時期 2004年4月～6月

ネットワークサービス統括部
NS第2部
マネージャー
安本 昭夫 様

商　　号 ：古河インフォメーション・テクノロジー株式会社
設　　立 ：1987年2月
本　　社 ：東京都千代田区内神田2―16―8　古河電工ビル
代　　表 ：代表取締役　増田　一比古
資 本 金 ：7000万円
従業員数 ：323名
事　　業 ：ビジネスソリューションのご提供、FA分野を始め広域に亘る施設の管理システムのご提供、ネットワーク構築と運用サービス、そしてCADや科学技術計算を始めとする広範囲のCAE分野のサービスの4つのセグメントを事業範囲として、文字通り IT時代を支える応用分野全般に亘って、幅広くビジネスを展開
U R L ：http://www.fitec.co.jp

導入の背景

求められるネットワークウイルス対策

OSを含むソフトウェアのセキュリティーホールを狙い、ネットワーク経由で感染する「ネットワークウイルス」。2003年夏に猛威をふるったMSブラストもこのネットワークウイルスの一種であるが、夏休み中に発生したことがより大きな被害につながったことは記憶に新しい。「ちょうどお盆の休み明けで、初期対応を徹底させるのが困難でした」と語るのは、古河インフォメーション・テクノロジー（以下、FITEC）ネットワークサービス統括部NS第2部の安本昭夫マネージャーである。「あるお客様企業のネットワークがMSブラストに感染してしまったのです。あらかじめパッチの強制配信のための仕組みなどを準備していたにもかかわらず、対応が間に合わなかったという結果になってしまいました」

休み期間中にFITECの担当者がユーザー企業の本社に出向いて徹夜で対策作業を行ったが、各拠点や工場まではどうしても間に合わなかったという。そのため休み明けには、ユーザー企業の各拠点・工場の門前で社員にビラを配ったり、館内放送を流すなどしてPCの起動を制限。該当ポートを閉じてから復旧および脆弱性への対応を行ったが、その作業は内容、時間ともに厳しいものであった。「感染したPCは一台一台、ほぼ手作業で復旧作業を行いました。それだけで半月以上かかり、実際にポートを再び開けられたのはしばらくたってからのことでした。また、サーバへ感染させることは絶対にできませんから、この点はとくに慎重にならなければいけませんでした」と安本氏は振り返る。

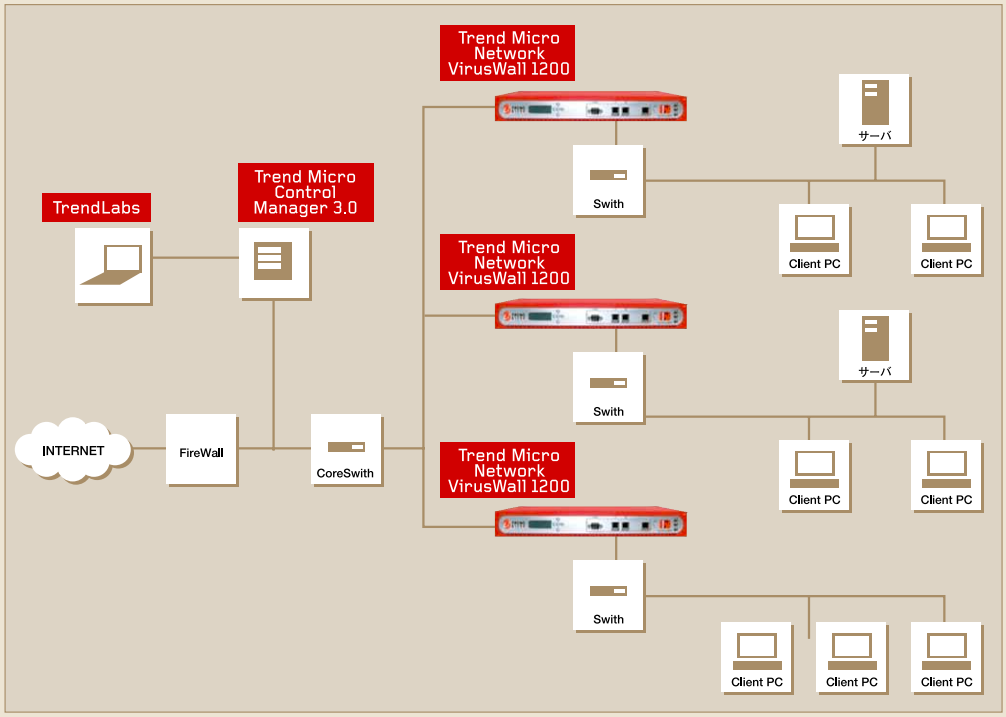
この問題からFITECが痛感したのは、ネットワークウイルスのゼロデイ・アタックに対応できること、そして複数の拠点を中央から集中管理できることの必要性である。「その点、Network　VirusWall 1200はまさに私たちが求めていた製品です。初めて製品情報を知ったときに『これだ』と思い、製品紹介セミナーに参加。そして今回のアーリーアダプタープログラムに参加しました」

導入決定のポイント

ネットワークウイルス検出と脆弱性の隔離がポイント

FITECでは、セキュリティ対策には以前から力を入れてきていた。「既存のウイルスバスターへのパターンファイル配信までの時間を短縮する取り組みや、URLフィルタリングの導入などに加え、社内組織の強化や情報セキュリティポリシー講座の開催など、さまざまな対策を行ってきました」と安本氏。しかし、昨今のネットワークウイルスの発生と蔓延の仕方には対応しきれなくなってきたのである。その状況について安本氏は次のように説明する。「ネットワークウイルスは次から次へと新種や亜種が量産され、もはやこれまでのパターンマッチングによる方式では対応しきれなくなっています。また、セキュリティホールの存在が確認されるのとほぼ同時に被害が拡大するゼロデイ・

ネットワークウイルスの対策にはパッチ適応以外のソリューションが必要と語る安本氏



各サブネットワークにNetwork VirusWallを配置することで、ネットワークウイルスへの効率的な対策が可能

アタックの危険性も増しています。パッチの適用だけでは、どうしても防御に限界があるのです。このような脆弱性をいかにつぶしていくか、あるいは脆弱性のある箇所をネットワークから隔離して安全を保つか、そうした視点からのセキュリティ対策が必要になってきていると言えます」

実際の運用状況

集中管理により設定や対策にかかる時間を短縮化

アーリーアダプタープログラムに参加してのNetwork VirusWall 1200に対する評価について、安本氏はこう語る。「まさに待ち望んでいた機能を備えた製品でした。既存のパターンにマッチするウイルスだけでなく、不明なファイルでも振る舞いを見て検知することができます。駆除や復旧を自動化していけるという点にも大きなメリットがありますね」

また、2003年夏のMSブラストの件と照らし合わせ、Network VirusWall 1200のハードウェア的運用が可能な点も評価している。「感染の過程について調査を進めたところ、お客様企業の管理資産となっていない外部のノートPCが原因のようでした。そうすると、モバイルユーザーの多い拠点がセキュリティ的に危険度が高いことになります。また、ネットワークウイルスにはIPアドレスの若い順に狙っていくものも多く、若いIPアドレスを使用している拠点ほど危険なことになります。Network VirusWall 1200はアプライアンス式の製品であるため、こうした拠点に対しネットワーク機器のような感覚で順次導入していくことができるのです。この『ハードウェア的な運用が可能』というのが重要で、工場をお持ちのお客様には重宝します。工場などだと最新のセキュリティソフトに対応していない古いOSを使用していることもありますし、そうした環境で確実にセキュリティ対策を行うためには必須の機能だと言えるでしょう」

実際の運用管理については、Trend Micro Control Manager 3.0（以下、Control Manager 3.0）の存在が大きいと安本氏は説明。「ポリシー設定などのさまざまなアクションをControl Manager 3.0で行えば、すべてのNetwork VirusWall 1200に即座に設定を反映させることができます。こうした一括管理が可能な点ももちろん大きな魅力ですが、それ以上に対応時間を短くできる点に意義があるのではないでしょうか。対応時間を短くできればそれだけセキュリティの危険性は低下しますし、費用面でのメリットも大きくなると言えます。実際、これまでルータなどの設定にかかっていた時間やコストは非常に高く、例えば、一万台程度のPC環境で数千万円程度の費用削減効果があるという結果になりました。Network VirusWall 1200によって安全性が高まるということに加え、Control Manager 3.0による簡単な設定で管理工数が削減できることも貢献していると言えます」

今後の展望

専業ベンダならではの安心感。今後は海外拠点のセキュリティも視野に

今回、アーリーアダプタープログラム参加の結果、FITECでは実際にNetwork VirusWall 1200の導入を決定した。その点について安本氏は、「コンセプトや機能、管理性などのメリットも大きいのですが、ウイルス対策ソフトのトレンドマイクロ社が提供しているという点にも大きな安心感があります。トレンドラボのウイルス解析と連動できますし、Control Manager 3.0との連携もトレンドマイクロという背景があるからこそ活きてくるのではないでしょうか」と、トレンドマイクロの優位性にも言及してくれた。

また、Network VirusWall 1200を利用した今後の展開、および要望などについても、「企業のネットワーク環境がグローバル化・ブロードバンド化が進んでいます。FITECとしては、Network VirusWall 1200を活用して海外においても同じセキュリティレベルのサービスを提供していきたいですね。ただ、OSとの組み合わせについてはさらに詳細に検証を重ねる必要があるでしょう。機能面でも、機器別のポリシー設定や運用など、さらに詳細な設定ができるようになるとありがたいですね」と、非常に前向きな意見を述べてくれた。

【お問い合わせ先】
トレンドマイクロ株式会社
東京本社
〒151-0053　東京都渋谷区代々木2-1-1　新宿マインズタワー
TEL 03-5334-3650（営業代表）FAX 03-5334-6324

◆ TrendMicro Network VirusWall 1200の詳細についてはこちらから
トレンドマイクロの製品情報サイト:http://www.trendmicro.co.jp

Copyright© 2004 Trend Micro Incorporated. All Rights Reserved.
TRENDMICRO、Trend Micro Control Manager、ウイルスバスターはトレンドマイクロ株式会社の登録商標です。各社の社名および製品名は、各社の商標または登録商標です。掲載内容は2004年6月記載現在のものです。内容は予告なく変更される場合があります。