

株式会社 菱化システム

Sygate Secure Enterprise で高度化する外部脅威からエンドポイントを保護
重要なセキュリティ基盤の構築を実現

Ryoka
Systems
Inc.

株式会社
菱化システム

三菱ケミカルホールディングスグループのITサービス会社である株式会社菱化システムは、高度化する外部からの攻撃の未然防止とセキュリティ基盤構築のために、シマンテックのエンドポイントセキュリティ製品 Sygate Secure Enterprise (SSE) を導入した。これにより、グループ全体で3万台以上に及ぶクライアントPCの通信を制御、不適切な通信をブロックすると共に、クライアントPCの健全性チェックとネットワーク検疫を行い、ネットワークインフラを高いセキュリティレベルで維持している。

高度化する攻撃の未然防止とセキュリティ基盤の構築が必要とされていた

株式会社菱化システムは三菱ケミカルホールディングスグループのIT関連業務全般を担う企業である。同グループは三菱化学と三菱ウェルファーマを中心に、グループ会社数371社、従業員数は33,000人に上り、グローバルに事業を展開している。菱化システムはグループ向けのOA環境の企画、運用や基幹システムの開発、運用だけでなく、化学業界を中心としたグループ外の顧客企業に向けたITコンサルからITソリューション事業、アウトソーシング事業、科学技術ソリューションの提供も行っており、今後はグループ外の事業比率を拡大していく計画だ。

その菱化システムがSygate Secure Enterprise (SSE) を導入したきっかけは、2004年頃からワーム等の攻撃方法の多様化、高度化が進み、それまでの対策方法では防御できない外部からの脅威の増大に対する危機感だった。また、情報漏えい事件が多発し、個人情報保護法などの法規制も強化される中で、クライアントPC内の情報を守るためのセキュリティ対策の強化も課題になっていた。インフラの企画と導入プロジェクトを担当した臼井 芳明氏(ソリューションサービス事業部インフラサービス部グループマネージャー)は「ワームやウイルス、OSの脆弱性への攻撃に対してはアンチウイルスソフトやWindowsアップデートで対策を行っていましたが、実際にパターンファイル更新やパッチの適用が最新状態になっているかどうかはユーザー任せであり、最新状態を維持するためには、新たに管理を強化する必要がありました。また、キーロガーやスパイウェア、Dos攻撃、ポートスキャン、不正アクセスなど、高度化する脅威に対する対策も早急に行う必要も感じていました」と振り返る。

Sygate Secure Enterprise で3万台を超えるクライアントPCのセキュリティポリシーの遵守徹底を実現

このような背景のもと、(1)セキュリティポリシーの強制適用ができること(2)セキュリティポリシーに反するPCの検疫ができること(3)接続形態によって、通信ルールが自動的に切り替わること(4)大規模及びグローバルでの導入実績があること、の4つを製品選定上の要件に上げ、いくつかの製品を比較検討した結果、Sygate Secure Enterprise (SSE) の導入を決定した。当時、製品の選定にあたった大黒 和夫氏(BN事業部 BN技術部 主席技師)は「SSEは管理者側でルールの管理、強制ができると共にエンドユーザーの操作制限ができました。また、PCの健全性チェックができ、ダイヤルアップやVPN、LANなどネットワークへの接続形態によって、通信ルールも自動的に切り替わります。それらの機能に加えて、大きく評価した点は、投資額が大きい上に展開に時間がかかるハードウェアによる検疫ネットワークに比べて、SSEはソフトウェアのためコストをかけずに短期間で導入が可能である、という点と、三菱ケミカルホールディングスグループよりユーザー数の多い企業でのグローバルでの導入実績でした」と選定理由を述べる。2004年12月から導入の検討を始めた菱化システムは、こうしてSSEの導入を決め、2005年3月から導入プロジェクトをスタートさせた。そして、サーバーインフラの運用や体制作り、具体的なルール作りを柱に設計を行い、システムの構築を進めていった。プロジェクトでサーバーの設計を担当した渋谷 正吉氏(BN事業部 データセンター)は「三菱ケミカルホールディングスのネットワークに接続するクライアントPCはグローバルで合計37,000台におよび、この中にはアフリカの駐在員や留学生など連絡が取りにくい社員のPCもあります。これらを全てカバーするために、アジア(35,000台)、アメリカ(1,300台)、ヨーロッパ(700台)の3拠点で管理することにしました。(裏面図)」と説明する。

企業情報

1970年に三菱化学とグループ14社によって設立されたITサービス会社。三菱ケミカルホールディングスグループ及びグループ外企業に対して、システムインテグレーションから運用までのサービス全般を提供している。

業種

ITサービス業

エンドースメント

高度化、多様化する攻撃の未然防御とセキュリティ対策強化のためにSSEを導入し、大きな効果を上げることができました。全世界で3万台を超えるクライアントPCを対象にしたセキュリティ基盤を構築することができ、Winnyを悪用したウイルスによる情報漏えいの未然防止の実現により、セキュリティ対策強化の効果が明確化されました。

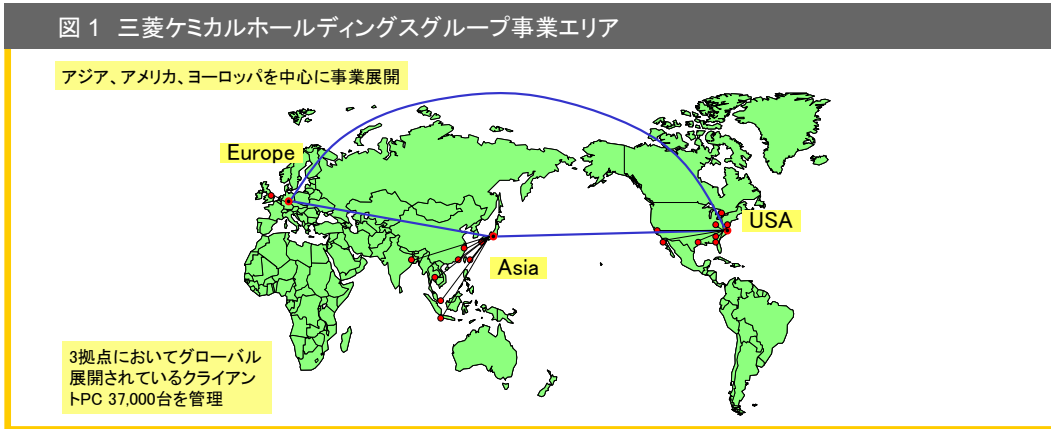


株式会社 菱化システム
ソリューションサービス事業部
インフラサービス部
グループマネージャー
臼井 芳明 氏



株式会社 菱化システム
BN事業部
BN技術部
主席技師
大黒 和夫 氏

図1 三菱ケミカルホールディングスグループ事業エリア



ルール設計では、通信を伴うアプリケーションに関して、アウトバウンドはブラックリスト制御で、スパイウェアなどが利用する通信ポート等を止め、情報漏えいを予防すると共に、トロイの木馬など気づかないうちに加害者になる可能性のある通信を禁止した。また、インバウンドは危険性が少ない、もしくはアプリケーションとの関係で利用せざるをえない通信ポートのみ許可するホワイトリスト制御を行うことにした。そして、各グループ企業や各部署ごとに通信を許可するアプリケーションのルールを決め、許可していない通信はブロックして、ポートスキャンや不正アクセスを防止することにした。

さらに、PCの健全性チェックでは、アンチウイルスソフトが常駐して、自動更新設定になっているかどうかをチェックすると共に、OSのパッチ適用に関しても自動更新設定になっているかどうかのチェックを行い、不適当な場合は通信を制限するようにした。加えて、通信ポートを利用するアプリケーションの仕様上、オープンにしているポートに対して、悪意のある通信パターンを自動検知してブロックするIPS/IDS機能も活用することにした。

Winnyを悪用したウイルスによる情報漏えい対策に大きな効果を発揮

こうして、グループ会社各社への導入を順次進め、2005年9月頃から、グループ全体で使い始めた。さらに、2006年春には、Sygate Enforcerによる検疫を開始し、会社資産のPCのVPNを利用した社内ネットワークへの接続を許可した。「以前は、セキュリティポリシー上ホテルや自宅などの社外からのネットワーク接続はPHSによる接続しか認めていませんでした。SSE導入後は、Sygate EnforcerがPC上のエージェントの有無、セキュリティポリシーの適合性をチェックして接続を制御してくれるため、エージェントが入っていない不適切な個人PCからの社内ネットワーク接続を不可として、ウイルス混入や情報漏洩を防止するとともに、会社PCでの一般webサイトへの直接接続を完全に抑止し、安全性を確保しながらブロードバンド接続による利便性の向上を図る事ができました。」(大黒氏)。

こうして、SSEによるセキュリティ基盤が構築され、現在順調に稼働しているが、導入効果として最も大きいのは、2006年春のWinnyを悪用したウイルスによる情報漏えい事件が多数報道される中でも、事前に対策を完了していたことにより同じ被害にあわずに済んだことである。SSEでIPTトンネルソフトやWinnyの起動を禁止し、外部から直接のインターネット接続を禁止することによりWinnyを悪用したウイルスからの情報漏えいを完全に阻止する。「SSEのエージェントが入っているPCであれば、情報漏えいの心配はなく、大丈夫だとグループ企業内に断言することができました。早く手を打ってよかったと、つくづく思いました」(臼井氏)。ちなみに、今回のプロジェクトは新たにセキュリティ基盤構築にチャレンジしたことでスケジュール通りに遂行できたことが評価されて、2005年度の菱化システムの社長表彰も受けるなど、社内でも高い評価を受けている。

SSE導入によりセキュリティ基盤構築を成功させた菱化システムでは、今後クライアントPCの管理精度の一層の向上に取り組んでいく方針で、ネットワークに接続された全クライアントPCのセキュリティを把握し、セキュリティ対策実施PCと未実施PCの管理方法を確立し、セキュリティ基盤をより一層強化していく考えだ。さらには、後継製品で管理サーバー台数の削減が見込めるSymantec Sygate Enterprise Protection 5.1への移行検討も視野に入れている。

*©2006 Symantec Corporation. All rights reserved. Symantec, Symantec ロゴは Symantec Corporation の登録商標です。その他の会社名、製品名は各社の登録商標または商標です。
*製品の仕様/価格は、都合により変更することがあります。本カタログの記載内容は 2006 年 10 月現在のものです。

ビジネス上の必要条件

- ・セキュリティポリシーの強制適用ができること
- ・セキュリティポリシーに反するPCの検疫ができること
- ・接続形態によって通信ルールが自動的に切り替わること
- ・PC3万台以上の規模に対応でき、グローバルでの導入実績とサポート体制があること

導入した製品

- ・Sygate Secure Enterprise 4.1(SSE)

製品導入による効果

Winny を悪用したウイルスによる情報漏えい事件が多数報道される前に、アプリケーションの通信制御対策をしていたため、対策効果が明確化した



株式会社 菱化システム
BN 事業部
データセンター
渋谷 正吉 氏

株式会社シマンテック

〒107-0052 東京都港区赤坂 1-11-44 赤坂インターシティ
www.symantec.com/jp

お問い合わせ先



マクニカネットワークス株式会社

本社 〒222-8562 横浜市港北区新横浜 1-5-5
TEL.045-476-1960 FAX.045-476-1970
大阪営業所 〒532-0003 大阪市淀川区宮原 3-4-30 ニッセイ新大阪ビル 17 階
TEL.06-6397-1055 FAX.06-6397-1056