FortiMailとFortiSandboxの自動連携でメールセキュリティを強化

半導体製造装置や精密計測機器を製造・販売する株式会社 東京精密では、顧客である大手電機メーカーや自動車メーカーなどのミッションクリティカルな情報を取り扱うことから、社内ネットワークのセキュリティを強化、拡充を進めている。その第一弾としてメールセキュリティを強化。フォーティネットのFortiMailとFortiSandboxを連携させてメール経由の脅威の検知と防御を実現。さらに将来的にネットワークのコアもフォーティネット製品に統一することで、同一のユーザーインタフェースやFortiOSによる効率的な運用管理を可能にしている。

株式会社 東京精密

本　　社　東京都八王子市石川町2968-2
設　　立　1949年3月
資 本 金　104億6200万円
売 上 高　777億9200万円（連結）
従業員数　1784名（連結）
事 業 所　八王子工場、土浦工場
　　国内17営業所、海外拠点66カ所、
　　国内グループ会社5社など
　　（2017年3月31日現在）

半導体製造装置、精密測定機器を柱として、アジアを中心に欧米などグローバルな事業を展開。世界中の優れた技術・知恵・情報を融合して世界No.1の製品を創り出し、成長し続けることを目指している。
http://www.accretech.jp/

株式会社 東京精密
業務会社
情報システム室 IT戦略チーム
チームリーダ 上級職
宇野澤 宏夫氏

株式会社 東京精密
業務会社
情報システム室 IT戦略チーム
主任
宮野 寿幸氏

株式会社 トーセーシステムズ
開発部
ITサービス チーム
情報セキュリティスペシャリスト
戸塚 陽介氏

導入・構築のポイント

(1)FortiMailの導入で
メールセキュリティを刷新

(2)FortiMailとFortiSandboxの
システム連携による標的型攻撃対策

情報の取り扱いなど全社でセキュリティ対策を強化

東京精密は半導体製造装置と精密測定機器を2本柱にグローバルな事業を展開。半導体製造装置はスマートフォンや自動車、IoTなど、便利で快適な社会を構成する機器に不可欠であり、機器の小型化や高効率化といった機能改善や環境負荷の低減など社会的な要請に貢献しているという。

また、精密測定機器は自動車の製造ラインなど、様々な分野で必要とされる高精度の計測機能を提供し、ものづくりを支えてきた。例えば、真円度・円筒形状測定機器は、自動車エンジンのピストンなどの測定に利用されている。「当社の取引先は国内外の大手電機メーカーや自動車メーカーもあり、ミスは許されません。とくに近年は厳しいセキュリティ体制が取引先からも求められており、従業員に対して情報の取り扱いや安全管理を徹底するなど、全社でセキュリティ対策の強化に取り組んでいます」と東京精密 情報システム室 IT戦略チーム チームリーダの宇野澤宏夫氏は話す。

その取り組みの一つが、社内に設置された情報セキュリティ委員会だ。取締役が選任する委員長を最高責任者として知的財産権取得・管理、営業秘密管理、技術流出防止など情報セキュリティの強化を進めてきた。例えば、情報セキュリティの基本方針の策定、情報セキュリティポリシーに基づく各種規定の整備、その実

行の指導・監督を担う。また、「電子データのみならず、紙媒体などの情報も取り扱うことから、情報セキュリティ委員会の下にITセキュリティ部会、オフィースセキュリティ部会、監査・教育部会の3部会を設けています。私たちが活動するITセキュリティ部会では、IT関係のセキュリティ全般について企画推進しています」と、東京精密 情報システム室 IT戦略チーム 主任の宮野寿幸氏は説明する。東京精密では本社・工場・営業所などの国内拠点の通信はすべて東京・八王子の本社経由でやり取りされ、情報システム室が一元管理している。

FortiMailを導入しメールセキュリティを強化

標的型攻撃やランサムウェアなど、サイバー攻撃の脅威が増す中、東京精密では最新の脅威についてe-ラーニングなどを用いて定期的に研修を実施するほか、「従業員向けのポータルサイトに脅威の情報を掲載し、情報セキュリティ意識の向上に努めています。また、危険と判定されたWebサイトへのアクセス制御やスパムメールの配信制御を実施してきましたが、課題が持ち上がっていたのです」と宇野澤氏は話す。

従業員向けのセキュリティ教育として、スパムメールに注意する、送信元が怪しいメールの添付ファイルは開かないといった

訓練はしているものの、送信元を偽装する標的型メール攻撃などの脅威も伝えられており、よりきめ細かな対策がITセキュリティ部会で検討課題になっていたという。東京精密ではゲートウェイレベルでのメールセキュリティに加え、クライアントレベルでもメールセキュリティを行い、多層的なセキュリティ対策を講じてきた。

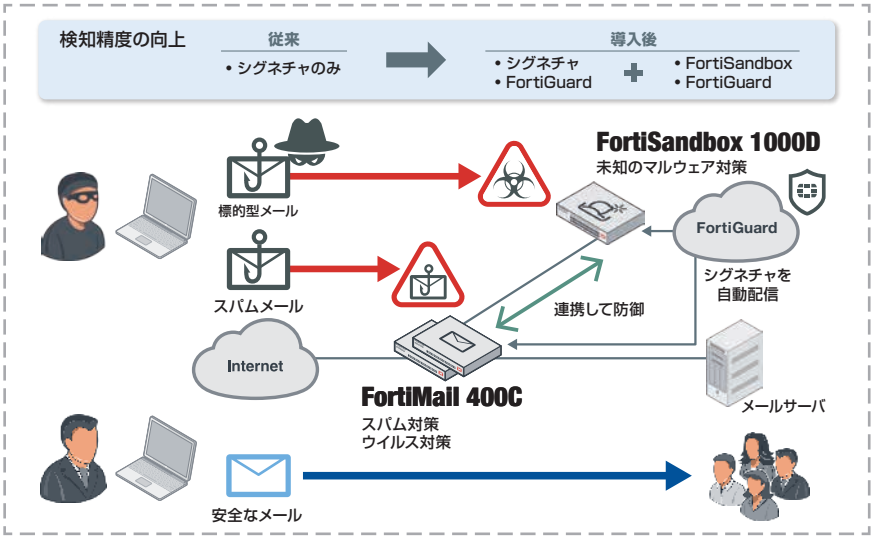
そして、従来から使用してきたメールセキュリティのゲートウェイ機器はリプレースの時期も控えており、「ゲートウェイをすり抜けるスパムメールが急増しており、メールセキュリティ機器の刷新が求められていました」(宮野氏)。ゲートウェイレベルで検知できないことでスパムメールのすり抜けが増え、時期によってはクライアントレベルのメールセキュリティでも相当数のスパムメールを検知していたと言う。

情報システム室ではいくつかの製品を検討した結果、セキュリティ機能に優れ、ユーザー数無制限ライセンスの統合セキュアメールアプライアンス「FortiMail」を導入。メールサーバーは既存システムを活用し、FortiMailはスパム対策やウイルス対策、フィルタリングなどセキュリティゲートウェイとして利用している。

FortiMailとFortiSandboxのシステム連携による標的型攻撃対策

東京精密では、メールセキュリティの強化に続いて、サンドボックスの検討に着手。「サイバー攻撃に対する入口・出口対策に加え、マルウェアの怪しい挙動を把握することにより、セキュリティリスクの低減が可能です」と宇野澤氏はサンドボックス導入の狙いを話す。そして、サンドボックスについても、いくつかの製品を検討した上で、FortiSandboxを導入している。「他の製品も検討しましたが、サンドボックス導入の目的は“検知”より“防御”です。情報システム室の限られた人員で効率的な運用が行えることがFortiSandbox導入の決め手になりました」と宮野氏は説明する。

東京精密様セキュリティ強化：FortiMail + FortiSandbox



例えば、FortiMailがメールに不審なファイルが添付されているのを検知した場合、そのメールの配信を保留にし、FortiMailと連携するFortiSandboxがメールを解析する。FortiSandboxが安全なメールであることを確認した場合、メールは配送されるが、未知のマルウェアと判断された場合はそのメールの配信を停止できる。

IT戦略チームのメンバーと一緒にFortiSandboxなどを運用しているトーセーシステムズ ITサービスチームの戸塚陽介氏は「FortiSandbox導入後は、ゲートウェイやクライアントのウイルス対策をすり抜けるマルウェアが大幅に減っており、確認作業の工数と時間の削減にも大きな効果があります」と、FortiMailとFortiSandboxのシステム連携による導入効果を話す。

FortiSandbox導入前は、マルウェア侵入の確認作業に毎日、約2.5時間の工数がかかっていたという。不審なファイルが見つかった場合、自前で作成した仮想環境でファイルの挙動を確認していたが、「現在は、FortiSandbox側で挙動を確認し、作業時間を短縮できます。その分、他の業務に時間を充てることができるようになりました」(戸塚氏)。

メールを介したランサムウェア感染が増える中、東京精密はFortiMailとFortiSandboxの導入により、システムで自動的に疑わしいメールの侵入を防いでおり、従業員端末におけるランサムウェアの被害は出ていない、と言う。メールによる脅威の侵入はもちろん、ネットワークを介した脅威の侵入リスクは消えないため「トータルで情報セキュリティの仕組みを構築できるフォーティネットを選びました」と宮野氏は話す。

東京精密では、さらに内部ネットワークのセキュリティ強化に向け、内部セグメンテーションファイアウォールの導入を進めている。その取り組みについては別途、詳しく紹介する。

FORTINET
フォーティネットジャパン株式会社

〒106-0032
東京都港区六本木 7-7-7
Tri-Seven Roppongi 9 階
www.fortinet.co.jp/contact

お問い合わせ