

## CUSTOMER STORY

# 大手製紙パッケージ企業が 世界規模のセキュリティ・アーキテクチャに再投資

## FireEyeソリューションの導入により、複数の攻撃経路にわたる 統合カバレッジを実現

### 概要

### 業界



製造

### ソリューション

- FireEye ネットワーク・セキュリティ
- FireEye Eメール・セキュリティ - Cloudエディション
- Mandiant Managed Defense
- FireEye Security Orchestrator

### 利点

- 複数の攻撃経路にわたるフォレンジック情報をリアルタイムで収集することにより、攻撃に対して迅速で同期の取れた対応を実施
- 統合されたセキュリティ体制により、管理の簡略化とチームの効率化を実現
- ITおよび運用テクノロジーの環境をカバー

### 企業紹介

グローバル規模の紙およびパッケージ企業であり、消費者向けパッケージと段ボール梱包材の製造を専門としています。また、数多くのリサイクル施設も運営しています。



業界をリードする企業として、同社は常に紙およびパッケージ製品業界のパートナー企業のために、現実的で持続可能性のある成長を促進する革新的な方法を追求しています。飲料断熱パッケージのためのコスト効率の良いデザインを考案したり、リサイクルに適した、環境に優しい外食サービス用パッケージを生み出す活動を率いたりなど、同社の社員は世界中にある数百の施設で、協働、発明、戦略化に取り組んでいます。

一連の企業買収は、脅威の経路が大幅に増える原因にもなりました。同社の情報セキュリティ担当副社長は、グローバルなインフラを防御するための大量の多様なセキュリティ・テクノロジーを前任者から引き継ぎました。この副社長は次のように語っています。「当社は常に最高品質のセキュリティ対策機能を備えてきましたが、会社のロードマップを構築して今後の開発のための基礎を築くために私たちに必要なのは、次のレベルの防御にステップアップするような、洗練された統合型のセキュリティ体制への移行だということは明らかでした」

このメーカーが持っていた一連の従来型セキュリティ・ツールは、既知のマルウェアに対しては十分な防御力がありました。しかし、より連携した統合型のセキュリティ・アーキテクチャであれば、現代のさまざまなサイバー攻撃から企業を守れると、副社長は考えました。ここで重視したのは、ネットワーク・トラフィック、特にエンドポイント、サーバー、Eメールのネットワーク・トラフィックに対して、深い可視性を確立することでした。それによって、高度な脅威の検知と防御能力を強化しようと考えました。

## 「この市場で、業界をリードする専門家によりサポートされた統合セキュリティをお探しなら、FireEyeをお勧めします」

— 情報セキュリティ担当副社長、グローバル規模の紙およびパッケージ製造企業

副社長はさらに、脅威インテリジェンスの収集を一元化し、最高のソリューションを用いてログ・データを監視、解析することにより、セキュリティ業務の合理化とインシデント対応時間の改善を目指しました。

### 統合への道

副社長は、目的に合うソリューションを提供している企業はセキュリティ市場に何十社もあるものの、統一されたセキュリティ・エコシステムの一部として併用や運用ができるように設計されたものはごくわずかであることに気づきました。彼はこう述べています。「独立したソリューションを組み合わせる場合、攻撃を受けたときにベンダーの間で責任の押し付け合いが始まるかもしれないという危惧がありました。しかも、各コンポーネントを個別に購入した場合、単独のベンダーと1つの窓口で交渉する場合のコスト面での利点も失われてしまいます。FireEyeについて調べ始めた時、FireEyeのソリューション群は、連携した効率的なセキュリティ・アーキテクチャを形成するという当社の目標に適した設計になっていることがわかりました」

同社はFireEyeネットワーク・セキュリティ、FireEye Eメール・セキュリティ - Cloudエディション、Mandiant Managed Defense、FireEye Security Orchestratorについて、概念実証の評価(PoC)を徹底的に行いました。産業制御システム的环境における性能に加え、ソリューションを組み合わせた全体的な有効性も慎重に評価しました。

副社長は次のように語っています。「FireEyeのアプローチが当社の戦略に適していることは明白でした。すべてのソリューションが共通したルック・アンド・フィールをそなえていて、それが緊密に統合され、継続的に通信し合いながら、防御の協力体制を築いています。加えて、FireEyeのソリューションは実環境への影響がわずかです。これは、当社の事業運営上、非常に重要な点です」

### 業界の専門家に支えられた適応型防御

FireEyeのサポート・サービスでは、この企業に対してフルタイムのスタッフを割り当てています。そのため、同社のセキュリティ・チームは、同社の複雑なグローバル・インフラの事情に精通した専任担当者にいつでもオンデマンドでアクセス

できます。彼は次のように語っています。「担当者は当社の環境を把握し、当社のセキュリティ上の懸念を理解しており、リクエストに機敏に対応してくれます。ソリューションをさらに有効に活用する方法があれば、FireEyeの方から積極的に提案してくれます」

Mandiant Managed Defenseという、検知と対応の協調的なサービスを通じて、同社は信頼できるパートナーを獲得しました。最前線で活躍するMandiantのインシデント対応担当者からの専門知識を直接活用し、企業環境内に潜む脅威を24時間体制で監視できるようになったのです。「Mandiant Managed Defenseの専門家とやり取りするたびに、感銘を受けています。彼らは、世界中で侵害対策に当たっているコンサルタントからMandiantが継続的に得ているサイバー・セキュリティの専門知識をフル活用しています。レポートや推奨事項の質は非常に高く、業界最高の専門家がサポートしてくれていることは明白です。彼らのアドバイスに基づいて重要なセキュリティ判断を安心して行えるのは、非常に頼もしいことです」と、副社長は語ります。

FireEyeのソリューションは互いに協調し合いながらフォレンジック情報をリアルタイムで収集することにより、攻撃に対して迅速で同期した対応を実施できるように準備された環境を形成します。副社長はこう強調しています。「FireEyeのソリューションのいずれかが不正な活動の可能性のあるものを検知すると、脅威インテリジェンスの相関分析を行い、環境全体の防御を自動的に更新して、攻撃を防ぎます。単一の統合ソリューションを管理するのは、当社にとって非常に効率的であり、効果的でもあります」

### プロバイダーを越えてパートナーへ

副社長は次のように締めくくります。「FireEyeが提供してくれたのは、環境を形成するためのメカニズムです。ここでは脅威インテリジェンスが一元的にまとめて表示されるので、自社データと顧客データを予防的に保護できます。この市場で、業界をリードする専門家によりサポートされた統合セキュリティをお探しなら、FireEyeをお勧めします」。

FireEyeの詳細については、[www.FireEye.jp](http://www.FireEye.jp)をご覧ください。

### ファイア・アイ株式会社

〒101-0054 東京都千代田区神田錦町3-22  
テラススクエア8階 | 03-4577-4401 |  
Japan@fireeye.com

©2019 FireEye, Inc. All rights reserved.  
FireEyeはFireEye, Inc.の登録商標です。その他のブランド名、製品またはサービス名はそれぞれその所有者の商標またはサービスマークとして登録されている場合があります。F-EXT-CS-JA-JP-000359-01

### FireEyeについて

FireEyeは、インテリジェンス主導型のセキュリティ企業です。お客様は、FireEyeの革新的セキュリティ技術、国家レベルの脅威インテリジェンス、世界的に著名なMandiant®コンサルティングの知見が統合された単一プラットフォームを、自社のセキュリティ対策の一部としてシームレスに組み込むことができます。このアプローチにより、FireEyeは準備、防御、インシデントレスポンスといった、組織がサイバー攻撃対策をする上での課題となっていた複雑性や負担を解消します。

