

導入事例

東海澱粉 株式会社 様

導入サービス ■ FireEye ETP

お客様プロフィール

世界の、食の、総合会社。


東海澱粉 株式会社
 TOKAI DENPUN CO.,LTD

所在地	静岡県静岡市葵区伝馬町24-15
設立	1947年8月11日
従業員数	656名
事業概要	澱粉、農産物、水産物、畜産物、調味料、油脂、食品添加物、醸造用原材料、飼肥料、医薬工業薬品、化学製品類、包材、食品機械等の販売、輸出、輸入ならびに加工又は製造
URL	http://www.tdc-net.co.jp/



東海澱粉株式会社
経営企画部 システム課
課長 八木 浩義氏



東海澱粉株式会社
経営企画部 システム課
山崎 俊良氏

「高性能かつ実績豊富な標的型メール対策をクラウドで導入したい。ソフトバンク・テクノロジーは、当社にとって理想的なソリューションを提案してくれました。」



導入のポイント

- 機能と導入実績が豊富なFireEyeをクラウドで活用
- クラウドで、導入コストと構築・導入・運用の負荷を圧縮
- 従来の対策では把握が難しかった標的型メール攻撃の実態を把握

抱えていた課題、解決したかったこと

自社にとっての最適解を模索していた標的型メール攻撃対策

1947年設立。澱粉の売買からスタートし、現在では業界屈指の食品総合会社として存在感を放っている東海澱粉。水産、畜産、農産を網羅する商社事業だけでなく、食品メーカー事業も順調に業績を伸ばしている。

情報漏えい対策などに積極的に取り組んでいる同社では、2015年9月、従来のウイルスメール対策やスパムメール対策だけでは検知・防御が難しいとされる標的型メール攻撃への対策を強化するためFireEye ETPを導入した。

その背景には、中間流通業者として顧客の重要な機密情報を取り扱うことが多いこと。海外との取引も多いため、メールの利用を制限することは難しく多言語のメールが行き交うため、「怪しいメールはクリックしない」というような運用ルールだけでは、マルウェアなどへの対策が不十分だという認識があった。

また、既存のメールセキュリティに加えて、さらに標的型攻撃対策をどこまで実施すればいいのか。進化のスピードが速く、専門家でも実態を把握するのが難しいとされる標的型攻撃に対して、どのような製品やサービスを選ばいいのか。社内のコンセンサスが得られるのか、といった点に関しても見極めが難しかったという。

- 従来の対策だけではカバーできないマルウェアなどへの対策は必須
- 導入する製品やサービスの見極めが困難
- 標的型攻撃に対する社内コンセンサスも課題

導入の要件

理想は機能・コスト・運用負荷のバランスが整ったクラウドソリューション

「導入するのであればFireEyeしかない」という思いは検討の初期段階からあった。仮に、安価で機能の不十分な製品を採用してインシデントが発生すれば、情報システム部門の判断能力に疑問を持たれてしまうからだ。

情報セキュリティ対策に関しては全面的に任されているため、その分、責任も重く、インシデントは発生しない状態が当たり前と思われている。当然、国内外の大手企業が数多く採用しており、機能も充実しているFireEyeは第一候補だったという。

- 実績豊富で機能も充実しているFireEyeは第一候補
- クラウドで利用できる標的型攻撃対策が要件

しかしながら、闇雲に高価な製品やサービスを導入するわけにもいかない。導入の期間かつコストを抑え、既存のメールシステムに変更や修正を加えることなく利用できるクラウドソリューションであることが、もう1つの要件だった。

すでにスパムメール対策において、クラウドは大きな成果を上げていた。標的型メール対策においても同じ手法を採用することで、初期費用と構築・導入・保守・運用にかかる手間を抑え、大きな成果を上げたい。また、社内のコンセンサスも得やすいと考えていた。

ソフトバンク・テクノロジーを選んだ理由

経験と知識の豊富なベンダーのサポートは必須

数社からの提案の中で、ソフトバンク・テクノロジーは、FireEyeをクラウドで利用できるソリューション（FireEye ETP）を提案した。FireEye ETPの機能や性能に関しては、実際に1か月間、同社が受信するメールを分析する評価試験において確認し導入を決めたという。

これまで認識できなかったマルウェアを含んだメールを確認することができ、誤検知は1件もなかったという。改めて標的型攻撃に特

化したFireEyeのメカニズムに感心した、と当時の様子を振り返る。

一方、日々巧妙化するマルウェアなどの詳細な分析に関しては、専門的な経験や知識も必要な場面も少なくないことから、経験と知識の豊富なベンダーのサポートが受けられること、そしてサービスの保守運用体制がしっかりしていることも、FireEye ETPを採用する上で大きなポイントになったという。

- FireEyeをクラウドで利用できる提案（FireEye ETP）を採用
- 実際のメール受信環境で評価試験を実施、経験と知識が豊富なベンダーのサポートは不可欠

導入効果と今後の展望

実態を把握することで、今後の対策強化を目指す

短期間にセキュリティ対策の導入効果を判断するのは難しいが、現段階では、手間とコストをかけず標的型メール攻撃に対する対策を強化できたことが、大きな成果の1つだと八木氏は自信を見せる。

これまで曖昧だった実態が明確になり、監査など社内外に対して対策状況や実体を説明できるようになったと同時に、今後の対策をどう実施していくのか、その方向性を分析・判断する情報を得られるようになったことも見逃せない成果だ。

運用に関しても、通常はまったく手間がかからない。マルウェアらしきメールを受信したときにはアラートが送られて来るため、インシデントが発生する前に対応が取れるようになった、と山崎氏は評価する。

公的機関に対するハッキングや情報漏えい事件が連日報道される中、同社でも社員や経営者の意識に変化が垣間見られるという。そのよ

うな社内の雰囲気も好機と捉え、今後も情報漏えいを防ぐため、引いては社員と会社を守るため、セキュリティ対策へと積極的に取り組む姿勢を見せる両氏。ソフトバンク・テクノロジーのように特定のメーカーや製品にとらわれず、最適かつ優れたソリューションを提供してくれるベンダーの存在は貴重だと語った。



ソフトバンク・テクノロジー株式会社
中瀬 誠実（写真 右端）
笠倉 直樹（写真 右から2人目）

- 社内外に対して、対策状況や実体の説明が容易
- 運用負荷がかからず、インシデントの発生前に対応が可能
- 今後の方針や対策の判断材料として活用

お客様窓口

SBテクノロジー株式会社

〒160-0022
東京都新宿区新宿6丁目27番30号 新宿イーストサイドスクエア17階

TEL : 03-6892-3154
E-MAIL : sbt-ipsol@tech.softbank.co.jp
URL : <http://www.softbanktech.co.jp/>