CUSTOMER STORY

FireEye

増え続ける標的型メールの脅威をシャットアウト
高い検知力で不審メールを効率的に検知・隔離し、運用負荷も軽減

～ Office 365のメールセキュリティを大幅強化 ～

SoftBank Technology

ソフトバンク・テクノロジー株式会社

概要

業界

ICTサービス事業

ソリューション

FireEye Email Threat Prevention

利点

不審なメールを高精度に検知・隔離し、高い防御力を発揮

誤検知・過検知の抑制により無駄な運用コストを削減

アラート通知メールの日本語化による使い勝手の向上

会社概要

「クラウド」「セキュリティ」「ビッグデータ」関連のソリューションを得意とし、国内エンタープライズ企業向けにビジネスを展開する。クラウドビジネスでは、Microsoft Office 365の導入や自社サービスの提供など、800社、150万ユーザーを超える国内最大級の導入実績を持つ。セキュリティビジネスでは、サイバー攻撃対策ソリューションの他、自社が保有する24時間365日稼働のセキュリティ運用監視センターで、クラウドに集積されるセキュリティ製品のログを、AIを活用し分析を行うなど、素早く精度の高い運用・監視サービスを提供している。

多種多様なセキュリティソリューションを手掛けるソフトバンク・テクノロジーでは、顧客に販売している標的型メール対策ソリューション「FireEye ETP」を自社内においても全面導入。極めて費用対効果の高い標的型メール対策を実現するとともに、FireEye ETPの機能を国内ユーザー向けに補完する独自製品の開発・提供で、自社ソリューションの価値を高めることにも成功した。

顧客に提供する「FireEye Email Threat Prevention」を自社内でも試験的に導入・運用

ソフトバンクグループはもちろんのこと、グループ外の大手企業や官公庁のクライアントに対しても幅広くICTサービスを提供しているソフトバンク・テクノロジー株式会社（以下、SBT）はさまざまなクラウドサービスの導入・運用サービスを手掛ける国内屈指のクラウドインテグレータとして知られているが、セキュリティ事業にも注力している。従来のサイバー攻撃に対するセキュリティ製品の導入支援に加え、侵入されることを前提とした、セキュリティ運用・監視サービスや被害を受けた場合の各種原因調査・復旧対応支援サービスの提供など、顧客ビジネスの安全を日々守っている。

同社では顧客に製品を提供するに当たり、まずは自社内で製品を導入・運用し、その有効性を必ず確認するというポリシーを貫いている。そのため、同社が手掛ける多様なセキュリティ製品群は基本的に自社内で導入しており、それらを組み合わせた強固な多層防御の仕組みを構築してきた。

業務推進本部長 CIO 橘勝也氏によれば、ファイア・アイ株式会社（以下、ファイア・アイ）が提供するクラウド型の標的型メール攻撃対策製品「FireEye Email Threat Prevention（以下、ETP）」も、そうした製品の1つだったという。

「製品の有効性を確かめるために、また自社内に構築・運用ノウハウを溜めるためにも、実際にETPを自社導入することにしました。まずは、標的型メール攻撃にさらされる危険性が高いと思われる外部公開アドレス約40個を対象に、ETPを導入しました」

こうしてしばらく、絞り込んだ数のメールアドレスを対象にETPの運用を続けてきたが、やがて「全社のメールアドレスにも適用したい」との機運が高まってきた。業務推進本部情報システム部長 千家敬比古氏によれば、その背景には近年高まり続ける標的型メール攻撃の脅威があったという。

「当時から弊社ではかなり強固な多層防御の体制を築いていましたが、実在の会社を名乗った巧妙なフィッシングメールや標的型メールが増加傾向にありました。このままでは、具体的な被害に発展する恐れや、不審メールの確認など、それ

「機能面では蓄積された脅威情報をベースとした検知力の高さ、運用面では精度の高いアラートが評価ポイント。SBT独自のアラート通知メールの日本語化も提供開始し、お客様から好評価を頂いています」

を防止するための対応工数が膨れ上がることが想定されたことから、公開アドレスのみならず、標的型メールの検知や隔離について全社で対策を行う決断をしました」

メールセキュリティ強化のためにETPを全社導入

全社に標的型メール対策を導入するに当たり、真っ先に候補に挙がったのが、既に社内で成果を上げていたETPだった。他のメールセキュリティ製品との比較検討も行った結果、実績面に加え、機能や費用対効果の面でも「ETPが最も適している」との評価があらためて得られたという。

「機能面での評価ポイントは、蓄積された脅威情報をベースとした『検知力の高さ』でした。さらに、運用面での評価ポイントは、精度の高いアラートでした。情報システム部門としては、セキュリティ対策後の運用負荷も重要な選定基準です。アラートの数が多すぎる、あるいは精度が悪く大量の誤検知や過検知があった場合、危険と判断されるアラートが埋もれないように多くの工数を使って確認せざるを得ない状況になります。ETPの精度の高いアラートが、こういった運用面の不要な負担を削減し、効果的な対応を実現できると考えました。」（橘氏）

またETPに関しては、既に社内で運用ノウハウも溜まっていたため、なおさら運用に掛かる手間を抑えられると判断した。こうして同社は2017年11月、ETPの全社導入を正式決定。まずは、情報システム部門とセキュリティ担当部門に対して先行導入し、2018年2月、残りのメールアドレス千数百個に対して、一気にETPを適用した。

ETPの全社展開後、想定以上に多くのメールが検知されたという。業務推進本部 情報システム部 室井佳浩氏は、全社展開後の状況について次のように述べる。

「全社展開してからわずか3カ月強の間で、約660件のアラートがETPから上がってきました。これだけの数の潜在的なリスクが可視化・除去できたと考えると、非常に大きな成果が上がっていると評価しています。また、ETPが不審なメールを自動的に隔離し、隔離したことをユーザーにメールで通知するため、ユーザーから不審なメールの問い合わせを受けてヘルプデスクが一つひとつ確認し、判断して隔離対応していた導入前の状況からは、運用面の負荷もかなり軽減することができました。」

アラート通知メールを日本語化する仕組みを独自提供

SBTのメール環境は、Microsoft Office 365のクラウドメールに統一されており、従業員個人のメールボックスにメールが配送される手前でETPによる検閲を行い、不審なメールを検知した際の隔離と、宛先ユーザーに対する隔離通知メールの送信までを自動で行っている。

隔離通知メールを受け取った従業員から「隔離されたメールの内容を確認したい」との要望が出た場合は、SBTセキュリティ監視・運用チームの専門家による慎重な精査の上、安全であると判断された場合のみ参照を許可している。ただし現時点ではそのような要望はほとんど上がっておらず、ETPの誤検知・過検知の少なさを実感できているという。

さらに同社のパートナーでもあるSBTでは、高い技術力を活かして、デフォルト状態では英語で記述される通知メールを日本語化する仕組みを開発した。

「英語のアラートでは、ユーザーが正しく理解できない、あるいは読み飛ばしてしまう可能性が高まります。そこでメールを日本語化する仕組みを開発しました。この機能は2018年5月から弊社がETPを導入したお客様向けにも提供を開始しており、お客様からも好評価を頂いています。」（千家氏）

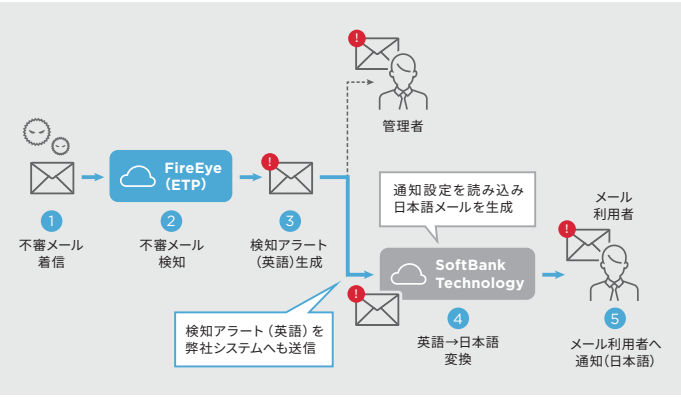
同社では今後、グループ会社に対してもETPを展開していくことや、ETPとログ分析プラットフォームを連携し、より高度なセキュリティ対策と効果的な運用を実現していくとしている。

「サイバー攻撃は高度化しており、各セキュリティ製品のアラートやログを個別に見るだけでは本当の脅威に気付けなくなってきています。それぞれのアラートを互いに突き合わせた相関分析を行うことで、防御だけでなく侵入に備えた、高度なセキュリティ対策を実現してきたいと考えています。ETPとその他のセキュリティ製品の連携も順次拡大して、より強固なセキュリティ対策を実現していきたいですね。そして、これらの対応で得られたノウハウは、弊社のお客様にも還元し、ファイア・アイと一緒に、安全な社会に貢献していきたいです。」（橘氏）

業務推進本部
本部長
CIO
橘勝也 氏

業務推進本部
情報システム部
部長
千家敬比古 氏

業務推進本部
情報システム部
室井佳浩 氏



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
TEL: 03-4577-4401 | Japan@FireEye.com
www.FireEye.jp

FireEye