proofpoint.

メールセキュリティ対策の強化に取り組む燦ホールディングス スパムメールと標的型攻撃対策強化を目指して、PROOFPOINT EMAIL PROTECTIONと PROOFPOINT TARGETED ATTACK PROTECTIONを導入

燦ホールディングス株式会社
SAN HOLDINGS

専門葬儀社グループとして国内最大手の燦ホールディングスでは、中期経営計画で「リスクマネジメントの強化」を掲げ、その一環として情報セキュリティ対策の抜本的な見直しを進めている。課題の一つだったスパムメール対策を強化するために、同社はメールセキュリティ製品を一新。問題のあるメールを高精度に発見・除去する「Proofpoint Email Protection」を、さらに標的型攻撃にも対応するため、SaaS型のサンドボックス「Proofpoint Targeted Attack Protection」を導入した。

企業情報

燦ホールディングス株式会社
https://www.san-hd.co.jp/

葬祭事業、ライフエンディングサポート事業を展開する企業グループの持株会社。葬祭事業がビジネスとして確立していなかった1932年に創業し、80年以上にわたってホスピタリティサービスを提供する。首都圏、近畿圏で葬祭事業を展開する公益社をはじめ、複数の葬祭会社を傘下に持つ。事業規模は専門葬儀社最大手、1994年には業界初の株式上場。2001年9月に東京証券取引所市場第一部に上場。

課題

従来のメールセキュリティ製品はスパムメールのすり抜けが多く、それを対策するために情報システム部門が手作業で対応していた

ソリューション

問題のあるメールを検出・除去する「Proofpoint Email Protection」、および未知の脅威を検知するサンドボックス「Proofpoint Targeted Attack Protection（TAP）」を導入

効果

問題のあるメールの検出精度が高く、情報システム部門の業務負荷が軽減したプルーフポイントのTAPとパロアルトネットワークスのクラウドベースの脅威分析サービスWildFireとの連携により、未知のゼロデイ攻撃を対策できたという安心感が得られる

燦ホールディングスは、葬祭サービスを提供する公益社、葬仙、タルイの3社と、葬祭サービスに必要な機能を提供する葬儀関連会社のエクセル・サポート・サービスを傘下に持つ持株会社。1932年に大阪市で創業して以来、80年以上にわたり葬祭ビジネスの先駆け的存在として業界をリードしてきた。1994年には業界で初めて株式を上場し、2001年には業界初となる東京証券取引所市場第一部への上場を果たしている。現在は人口が集中する首都圏、近畿圏を中心にグループ全体で64会館を運営。年間1万件以上に及ぶ葬儀の施行実績を持つなど、その事業規模は国内屈指だ。

同社では、2016～2018年度の3カ年にわたる「グループ中期経営計画」を策定した。中期経営計画には「サービス品質向上への体制強化と仕組みの構築」をはじめとする6つの重点課題が掲げられているが、その一つに「リスクマネジメントの強化」という課題が挙がっている。グループの持続的な成長と中長期的な企業価値の向上を図るには、リスクマネジメントをさらに強化する必要があるという同社の考え方を強く反映させた内容だ。

そんなリスクマネジメントの強化策として、中期経営計画が策定される前から着手していたのが、情報セキュリティ対策の抜本的な見直しだ。情報セキュリティ対策強化に取り組む理由について、燦ホールディングス 情報システム部長の清水 一宏氏は次のように説明する。

「当社グループは、専門葬儀社としては最大手、東証一部上場企業として万全な情報セキュリティ対策を講じることが社会的責務だと考えています。しかしながら、従来のセキュリティ対策は決して十分とは言えず、実際にメールによる標的型攻撃やランサムウェアの被害に遭うというインシデントも発生していました。そこでメールセキュリティに関する模擬訓練を実施して調査したところ、メールを扱う社員の一定数が本文内の不正なURLをクリックしてしまうという実態が明らかになりました」（清水氏）

防ぎきれないスパムメールが課題に

セキュリティ対策を強化するために、燦ホールディングスが最初に着手したのは、内部ネットワークとインターネットの境界に設置したファイアウォールのリプレースだった。実はこれが、のちに「Proofpoint Email Protection」の導入につながることになる。グループ全社のシステムインフラを統括する立場にある情報システム部 システム課長の二神 正裕氏は、こう語る。

「当時運用していたファイアウォールでは、高トラフィック時にダウンしてネットワーク全体が不通になるといった問題が発生することもありました。障害の原因を突き止めたくても詳細な通信内容を把握できず、その運用は情報システム部門の業務負荷を高める一因になっていました。当社は事業の特性上、土日祝日も含めて24時間365日、ネットワークを安定運用する必要があります。どんなに高トラフィックでも、決して落ちることのない新たなゲートウェイに入れ替えることが急務でした」（二神氏）

比較検討の結果、同社が採用したのは、パロアルトネットワークスの次世代ファイアウォールだった。また同時に、情報システム部門にとって大きな課題だった運用負荷を軽減するために、セキュリティ運用監視サービスの導入も決めた。2015年3月のことだ。

新しいファイアウォールの運用開始後は、ネットワークにトラブルが発生することもなく、安定稼働が続いている。しかしその一方で、ファイアウォールだけでは解決が難しい新たな課題も浮き彫りになってきた。情報システム部 システム課の米良 幸司氏は、最も利用されるメールセキュリティの脆弱性が目立つようになったと話す。

「当社ではファイアウォールとは別にメールセキュリティアプライアンスを導入して対策を講じていましたが、既存製品はスパムメールのすり抜けが多く、それを対策するために私たちが手作業で対応していました」（米良氏）

燦ホールディングス株式会社
情報システム部長
清水 一宏 氏

燦ホールディングス株式会社
情報システム部 システム課長
二神 正裕 氏

燦ホールディングス株式会社
情報システム部 システム課
米良 幸司 氏

SaaS型のサービス形態が導入の決め手

燦ホールディングスではこれまで、メールセキュリティアプライアンスとエンドポイントのウイルス対策ソフトウェアを併用し、メール経由で侵入してくるマルウェアや大量のスパムメールを防いでいた。しかしスパムメールは一向に減らず、設定の強度を高めると顧客とのメールのやりとりに支障を来すという課題もあった。

こうしたメールセキュリティの課題を解決するために、同社はセキュリティ運用監視サービスを提供するシステム・インテグレーションベンダーに相談したという。

「いくら対策してもすり抜けてくるスパムメールを何とかしたい、とベンダー様に相談しました。そのときに紹介されたのが『Proofpoint Email Protection』でした」（二神氏）

Proofpoint Email Protection は、外部から内部へのメール通信を制御する「インバウンドセキュリティ」と内部から外部のメールを制御する「アウトバウンドセキュリティ」の両方に対応するメールセキュリティソリューションだ。オンプレミス環境に設置するハードウェアアプライアンスのほかに、サーバー仮想化環境で利用できる仮想アプライアンス、プルーフポイントがクラウドサービスとして提供するSaaSという3つの形態が用意されており、ビジネスシーンに合わせて導入できる。

二神氏は、2016年5月にはプルーフポイント社製品を紹介するセミナーに参加。このセミナーで問題のあるメールを検出・除去するProofpoint Email Protectionの機能を確認したという。12月には、部長の清水氏もセミナーに参加した。

2017年になってからProofpoint Email Protectionのトライアルを実施。実際に導入してテストと検証を繰り返し、最終的に正式導入することを決定した。

二神氏によると、Proofpoint Email Protectionの採用を決めた理由はいくつかあるという。その一つは、機器を導入することなくSaaS型のクラウドサービスでメールセキュリティを実現できることだ。

また、先に導入していたパロアルトネットワークスが提供するクラウドベースの脅威分析サービス「WildFire」と連携可能なサンドボックス「Proofpoint Targeted Attack Protection（TAP）」もSaaSで用意されており、添付ファイルだけでなくURLリンクも含めた標的型攻撃を対策できることも導入理由に挙げている。

「プルーフポイントがこの分野において世界的なリーダーのポジションにあること、セキュリティ運用監視サービスを提供するシステムインテグレーターが取り扱っていることも評価しました」（二神氏）

問題のあるメールを高精度に検出・除去

Proofpoint Email Protectionの本番運用を開始したのは、2017年8月のことだった。導入効果はすぐに表れたという。

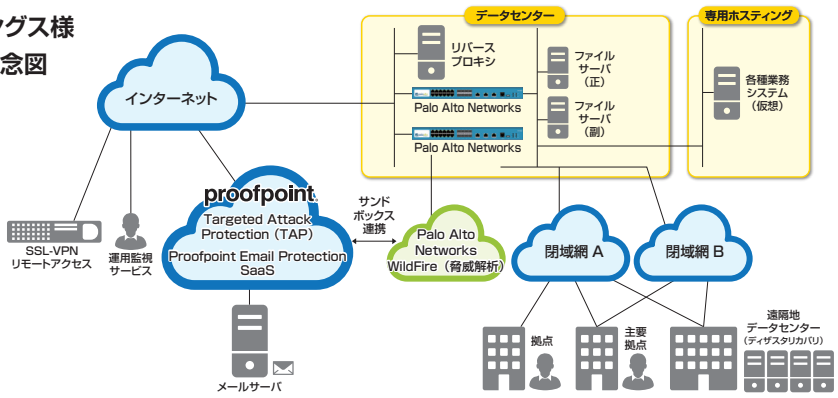
「Proofpoint Email Protectionは、以前に利用していたメールセキュリティアプライアンスと比較して、問題のあるメールの検出精度がはるかに高いと実感しています。これにより、従来は情報システム部で行っていたチューニング作業の業務負荷が激減するという効果がもたらされました。休日夜間対応は皆無になり、私の体調もよくなりました。」（米良氏）

また、プルーフポイントのTAPとパロアルトネットワークスのWildFireとの連携により、未知のゼロデイ攻撃にも対策できたという安心感が得られたことも、大きな導入効果だという。

Proofpoint Email Protectionの導入により、スパムメールをはじめとするメールセキュリティの課題を解決できた燦ホールディングスだが、今後もセキュリティ対策の強化・改善に継続的に臨んでいく構えだ。

「今後も製品開発ベンダーのプルーフポイント様、当社のセキュリティ運用監視を担当するシステムインテグレーター様と協力しながら、さらなるセキュリティ強化に取り組んでいきたいと考えています」（二神氏）

燦ホールディングス様
ネットワーク概念図



PROOFPOINTについて
Proofpoint Inc. (NASDAQ:PFPT) は、先進的脅威およびコンプライアンス上のリスクから人の働き方と組織を守る、次世代のサイバーセキュリティ企業です。Proofpoint はメール、モバイルアプリ、ソーシャルメディアなどを使った先進的攻撃からユーザーを守るサイバーセキュリティの専門家を助け、重要な情報を保護し、何か起こった際には迅速に対応できるように、チームに正しいインテリジェンスを提供します。Proofpoint のソリューションは現代のモバイルおよびソーシャル化されたIT 環境に対応し、クラウドとビッグデータベースの解析プラットフォームを活用して最新の先進的脅威に対抗します。フォーチュン100 企業のうち50 社を含むあらゆるサイズの組織が、Proofpoint のソリューションを利用しています。

©Proofpoint, Inc. Proofpoint は、米国およびその他の国々における Proofpoint, Inc. の商標です。本書に記載されたその他すべての商標は、それぞれの所有者に帰属します。