TechTarget Japan SPECIAL

FIREEYE™

多様化するメール攻撃にどう立ち向かうべきか

最新アンケート調査に見る 今メールセキュリティに求められること

「Office 365」や「G Suite」といったクラウドサービスを利用する企業は今や多数派となりつつある（ファイア・アイ調べ）。利用の際に課題となるのは、攻撃の糸口となるメールセキュリティだ。

IT システムの在り方を見直し、クラウドへの移行を検討する企業が増えてきた。全てを移行するとまではいかなくても、「Office 365」などを採用し、これまでオンプレミスで動かしてきたアプリケーションの一部を SaaS に切り替えたり、クラウドベースのメールを利用したりするケースは珍しくなくなった。

ファイア・アイが実施した「メールセキュリティに関する意識調査 2019」(注) によると、171 人の回答者のうち 80%以上が、Office 365 などのクラウドメールサービスを利用していることが明らかになった。もはやクラウドメール利用者の方が “ マジョリティー ” という状況だ。

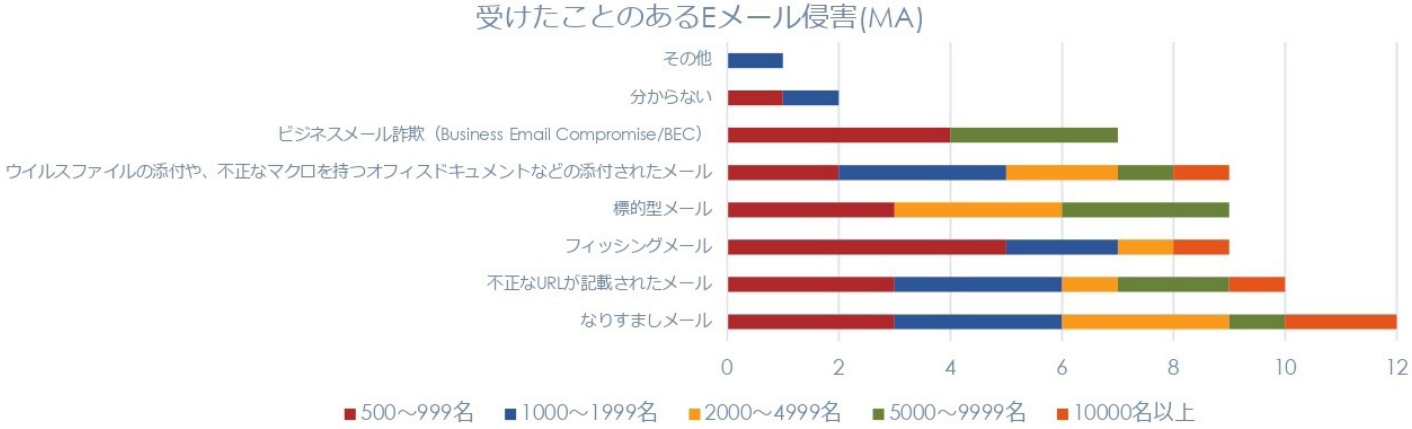
注：「メールセキュリティに関する意識調査 2019」調査概要
方法：アイティメディアが運営する複数サイトにおける Web アンケート
調査対象：従業員規模 500 人以上／年商規模 1 億円以上の企業の IT 他情シス関連部門に所属する従業員
調査期間：2019 年 1 月 22 日～ 2 月 4 日
総回答数：171 件

クラウドサービスは自社でインフラを持つ必要がないため導入の手間が少なく、運用コストも削減できるケースが少なくない。インターネットにつながる場所ならいつでもどこでも利用できることから、業務効率の向上や働き方改革への貢献も期待できる。しかし課題もある。その最たるものがセキュリティだ。

クラウドサービスを提供する事業者は、物理面、運用面でさまざまなセキュリティ対策を実施している。それは、一般的に企業が自力で実施するセキュリティ対策よりも堅牢（けんろう）なものだ。だが、クラウドで利用するアプリケーションのセキュリティは自身の責任だ。中でもメールは 9 割以上のサイバー攻撃のきっかけとなるといわれており、そのセキュリティ対策は重視しなければならないポイントだろう。調査結果を基に、現状と対策について考察する。

マルウェアもマルウェアを用いない攻撃も……メールがサイバー攻撃のきっかけになる

さまざまなサイバー攻撃が横行する現在、対策を全く講じていない企業は少数派だろう。最低限の対策としてエンドポイント PC に



※回答形式は複数回答

アンチウイルス製品を導入している企業は少なくない。

だが、前述のメールセキュリティに関する意識調査によれば、回答者の約 1 割が「なりすましメール」や「ビジネスメール詐欺（BEC）」の被害を受けたと回答している。不正な URL が記されたメールの報告も多い。このようにマルウェアを添付するのではなく、巧みな文面で受信者をだまして不正な URL に誘導したり、CEO など企業関係者を装って金銭を振り込ませたりする「マルウェアを用いないメール攻撃」に対して、アンチウイルス製品は残念ながら無力だ。

だが FireEye の「E メール脅威レポート 2018 年 1 ～ 6 月」によると、同社がブロックした攻撃の 90%がマルウェアを用いない攻撃だった。日本国内でも、Office 365 の認証情報を盗み取る目的のフィッシングメールが複数観測されている。巧みな日本語で経営者を装い国際送金を依頼する BEC の報告も複数あり、幾つかの企業で億円単位の被害が発生した事件は記憶に新しい。

とはいえ、マルウェアを用いた攻撃の脅威が消え去ったわけではない。FireEye が別途実施した調査によると、80%のマルウェアがいわば「使い捨て」であり、68%のマルウェアは特定の攻撃対象のためだけに開発されていた。こういった標的型マルウェアや未知のマルウェアに対し、シグネチャで検出するタイプのアンチウイルス製品は有効ではないのが現状だ。

クラウド型メールセキュリティに寄せられる期待と懸念

クラウド時代のセキュリティに対する課題を解決する手段として考えたいのが、クラウドベースのセキュリティ対策だ。アプリケーションやデータがクラウドにあるならば、メールセキュリティをはじめとする対策もクラウドで実施するのが自然な流れだろう。メールセキュリティに関する意識調査でも、クラウドメールサービスのオプションなど、クラウドベースのメールセキュリティ対策の採用が進む傾向が明らかになった。

一般的に、自社環境にセキュリティアプライアンスを導入すると、IT 部門は相応のリソースを用意しなければならない。電源やラックの確保、各種設定、脆弱（ぜいじゃく）性対策のために最新のパッチを常に適用し続ける、といった煩雑な運用は IT 部門にとって重い負担になる。

これに対し、クラウドベースのセキュリティは手軽に導入できることがメリットだ。導入の手間の多くはサービスベンダー側に任せられる。日々のパッチ適用や設定変更といった作業も任せられ、固定資産として所有する必要もない。これらのメリットがクラウドセキュリティサービスの採用を後押ししている。

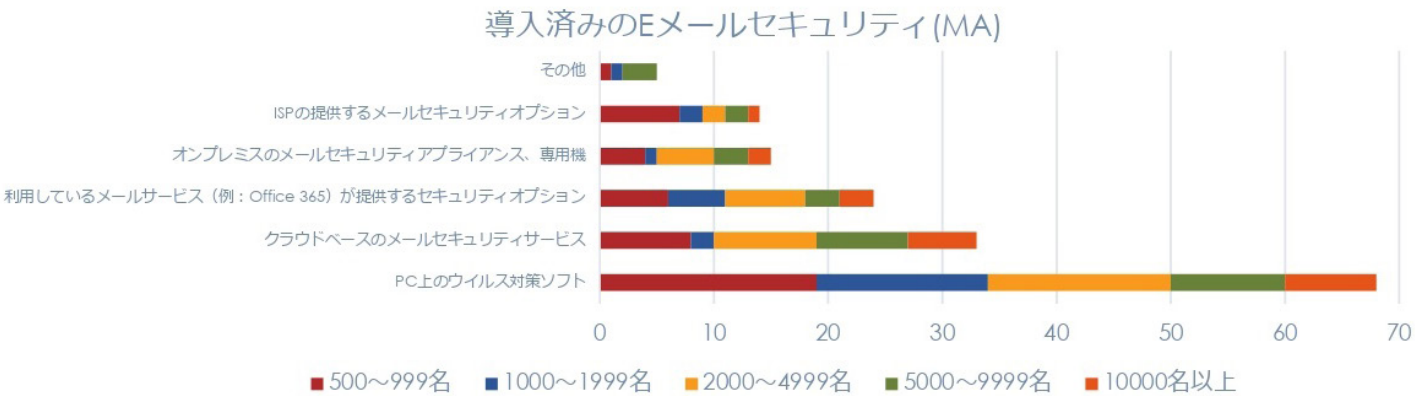
しかし、クラウドベースのセキュリティにも懸念はある。メールセキュリティに関する意識調査では、「サービス提供企業の事業継続リスク」や「取り扱いや保存方法などに起因する情報漏えいの可能性」を懸念する声が少なくなかった。「日本国外のデータセンターで処理される場合、日本国内法の適応外となる可能性があること」も懸念事項として挙がった。多くのベンダーがセキュリティサービスを提供する今、信頼できる企業を選びたいのは当然だろう。

さらに、メールセキュリティの入れ替えにおける製品選定ポイントとしては、脅威の「検知率」が最も重視されていた。「コスト（金額）」や「利便性」「移行のしやすさ」への回答を大きく上回る結果だった。

これらの結果からはクラウドならではのメリットを生かしつつ、日本国内で安定して継続的にサービスが提供されるセキュリティサービスが求められていると分かる。さらに、なりすましやフィッシングなどのマルウェアを利用しない攻撃とマルウェアを利用した攻撃の双方を、複数のテクノロジーを用いて確実に検知するサービスが求められていると考えられる。

「Secure Email Gateway」として機能するクラウドベースのメールセキュリティ

前述の E メール脅威レポート 2018 年 1 ～ 6 月によれば、サイバー攻撃の 91%はメールがきっかけとなって発生している。同社が解析したサンプルデータのうち、スパムメールでも不正なメールで



クラウドベースのメールセキュリティサービスを約 3 割の企業が利用している　※回答形式は複数回答。

もない無害なメールは32%にすぎなかった。メール経由のさまざまな脅威に対処するには、単一の方法に頼るのではなく、複数の検知手法を組み合わせる必要がある。

「FireEye E メール・セキュリティ - Cloud エディション」は、複数の手法を組み合わせ、高い検知率で不正なメールをブロックするサービスだ。特徴の一つはクラウド環境だけで利用できるメールセキュリティサービスであること。オンプレミスのメールサーバはもちろん、Office 365 や G Suite にも対応し、インラインでメール経由のサイバー攻撃を検知して対処する。同時にアウトバンドの通信も検査し、社内から危険なメールを外部に発信して「加害者になる」事態を防ぐ。

また、サンドボックス技術として長年実績のある「MVX エンジン」を活用し、添付された未知のマルウェアやメール本文に記載された不正 URL、そこからダウンロードされる未知のマルウェアなどの脅威を動的解析してブロックする。

「なりすまし」や「フィッシング攻撃」に対しては、送信者偽装対策の他、URL 分析や DNS の関係分析（「Smart DNS」）によって偽装サイトや不正サイトを検知する。あらかじめ正規の Web サイトのスクリーンショットを学習し、メールに含まれる URL が参照しているサイトのスクリーンショットと比較することで、違いがあればフィッシングとして検知するなどのユニークな対策機能も備えている。

FireEye E メール・セキュリティ - Cloud エディションは、こうしたさまざまな検知技術を組み合わせることで、正常なメールは通過させつつマルウェア攻撃とマルウェアを用いない攻撃の双方を検知、ブロックする。同社の検証結果によれば、競合サービスに比べ 40 倍の脅威を特定できる。また、URL の誤検知率は 1 週間当たり 4000 万分の 1 にとどまるという。セキュリティ分野の優れた製品やサービスを表彰する「SC Award 2019」において、FireEye E メール・セキュリティが「Trusted Award Best Email Security Solution」を受賞した事実は、その実績と実力が評価された結果といえるだろう。

日本国内データセンターでの運営

一連のセキュリティ対策の信頼性は、FireEye がこれまで蓄積してきた脅威インテリジェンスによって支えられている。世界各国で展開している FireEye 製品から得られる「マシンベースの脅威情報」に加え、グローバルな脅威動向や、インシデントレスポンスの現場から得られた情報などの「人が収集した脅威情報」を反映することで、新たな攻撃手法に対して手を打つことができる。

アンケート結果に示された通り、日本のユーザーは国内データセンターに強いニーズを持つ。海外データセンターで処理されることで、日本国内法の適応ができないといった懸念を持つためだ。これに対しファイア・アイは、日本国内にデータセンターを設置することを発表。2019 年第 2 四半期から運用を開始する。国内の異なるロケーションに 2 カ所のデータセンターを設置することで、ディザスタリカバリーにも配慮しているという。

このように、ファイア・アイは日本市場に対するサービスや設備の拡充に注力し、国内クラウドセキュリティサービスを継続する明確な意向を示している。

とはいえ、説明だけではサービスの実態を推し量るのは難しい。そこでファイア・アイは、ユーザーが懸念点として挙げた「攻撃メールの検知率」の精度を実感できる「無償 E メールセキュリティ診断サービス　for Office 365」を提供している。Office 365 のメールのうち、既に手元に受信しているメールをスキャンし直し、既存の対策で検知漏れがないかどうかを無償で確認できるサービスだ。論より証拠。不正メールの検知漏れが発生していないかどうか気になる方は、試してみてはいかがだろうか。

●関連リンク

無償 E メールセキュリティ診断サービス for Office 365

●お問い合わせ
ファイア・アイ株式会社
https://www.FireEye.jp/ | Japan@fireeye.com

東京オフィス	〒101-0054 東京都千代田区神田錦町 3-22 テラススクエア 8F	Tel. 03-4577-4401 Fax. 03-4577-4410
名古屋オフィス	〒450-0002 愛知県名古屋市中村区名駅 4-6-23 第 3 堀内ビル 9F	Tel. 052-589-7037 Fax. 052-589-7001
大阪オフィス	〒541-0041 大阪府大阪市中央区北浜 1-1-27 グランクリュ大阪北浜 301	Tel. 06-6121-3096 Fax. 06-6228-7155

※この冊子は、TechTarget ジャパン（https://techtarget.itmedia.co.jp/）とキーマンズネット（https://www.keyman.or.jp/）に 2019 年 3 月に掲載されたコンテンツを再構成したものです。
https://techtarget.itmedia.co.jp/tt/news/1903/28/news02.html