Microsoft 365に“+α”のセキュリティを!
テレワークによる利用増に応える「ESET Cloud Office Security」

テレワークが急速に普及したことで、ビジネスにおけるコミュニケーションも従来からある電話、メールを用いたものだけでなく、ITを活用したチャットやビデオ会議を含むコラボレーションと表されるものへと変化を遂げている。なかでも、Word、Excel、PowerPointといったお馴染みの業務ツールに加え、メール(Exchange Onlineなど)や、ビデオ会議・チャット・通話(Teams)、クラウドストレージ(OneDrive)、ファイル共有(SharePoint)機能を提供する「Microsoft 365」は、コロナ禍におけるビジネスの変化で最も利用増加が顕著になったコラボレーションツールといっても過言ではない。

しかし、こうした利用拡大の背景には、社内外を問わず頻度が増えるコミュニケーション・コラボレーションを狙う新たなセキュリティ上の脅威も生じており、対策の強化が叫ばれていることも事実である。これを受け、キヤノンマーケティングジャパン(以下、キヤノンMJ)は、2021年7月1日、包括的なエンドポイントのセキュリティ対策を実現する「ESET PROTECTソリューション(以下、EPソリューション)」とともに、Microsoft 365向けのクラウドセキュリティサービスである「ESET Cloud Office Security(以下、ECOS)」の提供を開始した。ここでは、ECOSにより、Microsoft 365のセキュリティ対策がどのように強化されるのかなど、同製品の詳細を、プロダクトマーケティングを担当する植松 智和氏にうかがった話を紹介したい。

利用拡大にともなう新たな脅威に備えて

――EPソリューションと同時に提供が開始されたECOSとは、どのようなサービスであり、どういった背景から生まれた製品なのでしょうか?

植松氏:ひと言で言えば、Microsoft 365のセキュリティを強化するクラウドサービスがECOSです。ECOSは、オンラインコラボレーションツールであるMicrosoft 365を利用して共有するファイルや送受信するメールのマルウェア対策、スパムメール対策、フィッシング対策を強化します。

ご存じのとおり、コロナ禍によるテレワークの急速な普及をはじめ、ワークスタイルの変革が進むなか、クラウドメールのみならず、ビデオ会議やチャット、クラウドストレージなどコラボレーションツールの利用が急拡大しています。なかでも利用増が著しいのが、多くの企業で使われているOfficeやグループウェアをクラウド化したサービスであるMicrosoft 365です。

一方、コラボレーションツールの利用拡大、これによる働く環境の変化にともない、脅威も増大しています。その代表的なものが、実在するアンチウイルスベンダーを装って安心感を与えてマルウェアが仕込まれた添付ファイルを開かせようとする心理的特性を悪用したスパムメールや、組織侵入のためのログイン情報を盗み出す目的などさまざまなサイバー攻撃のきっかけとしても使用されるフィッシングメール、マルウェア感染したファイルのアップロードによる、コミュニケーションツールやクラウドストレージを介したマルウェア感染です。

とくに心理面から生じるリスクというのは、意外と見落とされがちですが、実はかなり大きなファクターなのです。オフィス内であれば、正当なメールなのか判断がつきかねない場合でも、オフィス内の同僚に相談したり、社内のヘルプデスクに相談したりといったことが気軽に行えますが、テレワークの場合には油断して“つい”そのメールの添付ファイルを開いてしまい、それをきっかけにマルウェアに感染して情報漏えいの被害を引き起こしてしまうことになります。

キヤノンマーケティングジャパン株式会社
セキュリティソリューション商品企画部 課長代理
植松 智和 氏

実際、ESET社とイギリスのある調査会社が実施したコロナ禍におけるテレワークに関する調査でも、働く環境の変化により多くの人がストレスを抱え、普段オフィスでは決して行わなかったような、リスクに対しての“大胆な”行動を取りがちに……、という結果が発表されているほどです。

そして、こうした脅威はコラボレーションツールの代表格であるMicrosoft 365においても例外ではありません。Exchange OnlineやTeamsの利用はもちろんのこと、社内ではSharePointで資料を共有したり、社外の取引先とはOneDriveでファイルをやり取りしたりといったケースも増えているはずです。このため、Microsoft 365を足がかりとした攻撃が増えることが十分に予想されますので、先手を打って十分なセキュリティ対策が施せるよう、ESETならではの知見や技術を活かしてECOSを開発したのです。

なぜ標準のセキュリティ機能だけでは万全ではないのか?

――Microsoft 365にもセキュリティ機能が標準搭載されていますが、ECOSはこれを補完するものなのでしょうか?

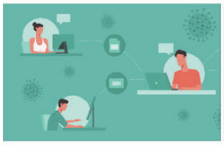
環境変化に伴う新たな脅威

心理的特性を悪用するマルスパム(マルウェア付きメール)

- 実在するアンチウイルスベンダーを装い、安心感を与えて添付ファイルを開かせようとするメール
- パスワード付きZIPとその展開パスワードを添えて、警戒心を与えずにファイルを展開させようとするメール
- 標的型攻撃など様々なサイバー攻撃のきっかけに使用されるフィッシングメール

さまざまなサイバー攻撃のきっかけとしても使用されるフィッシングメール

- 組織侵入のためのログイン情報を盗み出す目的のフィッシング
- 特定の組織や個人を狙う、巧みな標的型スピアフィッシング攻撃
- ビジネスメール詐欺による金銭被害



コミュニケーションツールやクラウドストレージを介したマルウェア感染

- マルウェア感染したファイルのアップロード
- 共有による感染ファイルの内部・外部ユーザーへの送信
- 複数デバイスをまたがる感染ファイルの拡散

コラボレーションツールに対するセキュリティ対策強化の必要性

植松氏：確かに標準でもセキュリティ機能が搭載されていますが、Windows端末のセキュリティ対策を考えてみるとわかりやすいでしょう。多くの企業では、Windows端末のセキュリティ対策として、Microsoft Defenderではなく、当社のESETをはじめとしたセキュリティ専業ベンダーのエンドポイントセキュリティ製品を導入しているのではないでしょうか？

Microsoft 365にしても同様で、ESETにはセキュリティベンダーとしての長年のノウハウや知見があるからこそ、標準機能だけでは補えない領域までもシステムやデータを保護することが可能なのです。いわば、標準に“プラスα”のセキュリティを実現するのがECOSだと考えていただければわかりやすいでしょう。また、優れたコストパフォーマンスもECOSの特長です。より高度な脅威に対応しようとした際、Microsoft 365単体では上位プランの契約を必要としますが、ECOSの導入であれば、高いセキュリティレベルを上位プランの契約よりも安い価格で実現します。

Microsoft 365のセキュリティ対策を強化するさまざまな機能

――ECOSの具体的な仕組みや特徴について教えてください。

植松氏：これまでお話した通り、ECOSはMicrosoft 365のセキュリティ対策を強化するクラウドサービスであり、Exchange OnlineやTeams、OneDrive、SharePointといったコラボレーションツールで授受

特徴

高度な脅威からMicrosoft 365を保護

- Microsoft 365の標準セキュリティ機能をすり抜ける脅威をESETの多層テクノロジーで防御
- 高度な機械学習を中心としたESETのテクノロジーがマルウェアやランサムウェアの感染・拡散を防ぐ
- 高度なフィッシングやビジネスメール詐欺(BEC)も検知

簡単でスピーディーに導入

- API連携だけでMicrosoft 365のセキュリティ対策を簡単に実現
- クラウドサービスのためサーバー構築が不要ですぐに利用可能
- メール配送経路の変更など、複雑な導入作業は不要

管理・運用が容易

- Microsoft 365からユーザー・グループ情報を自動取得するため、ECOSで追加作業が不要
- 保護対象ユーザーを指定できるため、スモールスタートとスケールアップが可能
- 常に最新の状態にバージョンアップされ、新たな脅威もしっかりと防御

するファイルとメールの脅威からユーザーを保護します。

また、クラウドサービスであることから、ネットワーク経路を変更することなく、API連携により速やかに導入できるのも強みとしています。

マルウェア対策については、ESETの検出エンジンが誇る検出力の高さや誤検知の少なさがそのまま生かされていますので、SharePointやOneDriveでのファイルのやり取りの際にマルウェアなどが含まれた場合にも、事前に防御することが可能です。ESETならではのエンドポイント保護で培われたレピュテーション、サンドボックス、DNA検出、ランサムウェア保護、アドバンストメモリースキャナー、スクリプトスキャナーなどの多層防御により、脅威を精度高く検出し排除できるのです。

また、スパムメール対策やフィッシングメール対策のいずれにも、マルウェア対策と同様に、ESETの30年以上にわたる知見とノウハウが反映された高度なテクノロジーが活かされています。メール本文と件名をチェックし、フィッシングサイトへのリンクを特定することも可能です。そして、これもクラウドサービスの特性として、常に最新の脅威データベースと連動しているため、新たな脅威からもしっかりと防御することができるのです。

さらに管理・運用面についても、Microsoft 365からユーザー・グループ情報を自動取得するため、ECOS側での追加作業は生じません。加

主な機能

マルウェア対策

- 送受信メールや添付ファイル(Exchange Online)、クラウドストレージ上のファイル(OneDrive、Microsoft Teams、SharePoint Online)をマルウェアから保護
- エンドポイント保護で培われたレピュテーション、サンドボックス、DNA検出、ランサムウェア保護、アドバンストメモリースキャナー、スクリプトスキャナーなどの多層防御が脅威を精度高く検出し排除

スパムメール対策

- 各種の第三者機関から高い評価を得ている最先端のスパムメール対策エンジンが、高い検出力で迷惑メールや不要なメールを除外
- 常にアップデートされるクラウド上のスパムメールデータベースが、新たに発生するスパムメールも迅速に検出

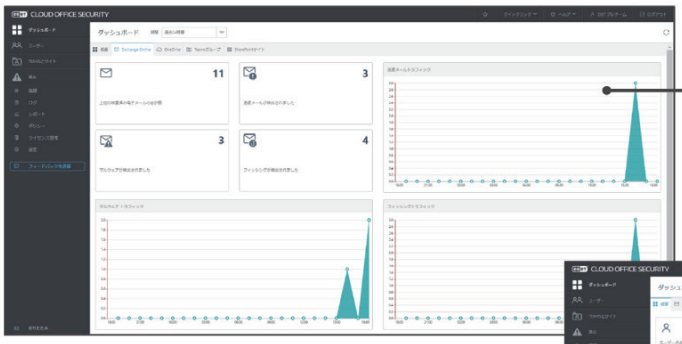
フィッシング対策

- メール本文と件名をチェックし、フィッシングサイトへのリンクを特定
- 絶えず更新される最新のフィッシングデータベースと連携し、ユーザーが不正なメールからフィッシングサイトへアクセスするのを防ぐ

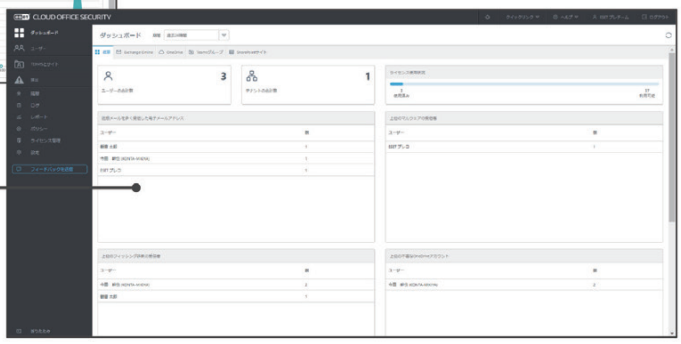
管理機能

- Webコンソールからユーザー管理や検出状況・隔離状況の確認、ポリシーの適用などを実施
- 機械学習による検出レベル、レポートレベルを細かくチューニング
- マルスパムやフィッシングメールの受信が多いユーザーや、不審なOneDriveアカウントなどの統計情報をダッシュボード表示
- Exchange Online、OneDriveの検出統計データはメールで管理者に送付することも可能

管理画面イメージ(ダッシュボード)



検出されたマルウェア付きメールやフィッシングメールの数、OneDrive、Microsoft Teams、SharePoint Onlineで検出したマルウェアの数、時間ごとの検出数などを表示



迷惑メールやフィッシングメールを多く受けたユーザーや、マルウェア受信の多いユーザーなどの検出統計が表示され、攻撃対象となっているユーザーの傾向を把握可能

えて、保護対象となるユーザーを指定できますので、機密情報を取り扱う部門からまずは導入し、その後に全社へと拡大していくなど、スモールスタートとスケールアップが可能となっています。

管理機能については、Webコンソールからユーザー管理や検出状況・隔離状況の確認が行えるようになっており、ポリシーの適用なども実施できます。迷惑メールやフィッシングメールを多く受信しているユーザーや、不審なOneDriveアカウントなどの統計情報をダッシュボード上に表示することで、攻撃対象となっているユーザーの傾向を把握することも可能です。こうした情報をもとに、攻撃の対象となっている可能性のあるユーザーに対して注意喚起を行うことで、セキュリティレベルの向上につなげることができます。

――ECOSを導入することによって、エンドユーザーにはどのようなメリットがもたらされるのでしょうか。

植松氏：ECOSはMicrosoft 365を使用する際に“裏側”で稼働して常に安全を見守るソリューションですので、エンドユーザー側はその存在を意識することはまずないでしょう。仮にマルウェアが添付されたメールが送られた場合には、そのメールをブロックしたという報告はありますが、「何かを設定する」といったことをエンドユーザーが行うことはありません。基本的には、エンドユーザーは何も気にすることなく、安心してMicrosoft 365を使ってもらえる――それこそがECOSの最大のメリットだと自負しています。

――ECOSはEPソリューションの最上位ラインナップである「ESET PROTECT Complete クラウド」にも実装されていますが、対策の精度や顧客担当者の負荷といった観点から、ECOS単体での導入と、ESET PROTECT Complete クラウドでの導入、どちらをおすすめしますか？

植松氏：お客さまの環境やニーズに応じてどちらも考えられるでしょう。

エンドポイントに関しては他社製の製品を導入済みで、Microsoft 365の保護に特化するのであれば、ECOS単体での導入も“あり”だと思います。ECOSはマルチベンダー型のセキュリティ対策を実現したい場合にも適したクラウドサービスとなっていますから。

ただし、総合的なセキュリティ対策を実現したいのであれば、やはりESET PROTECT Complete クラウドでの導入をおすすめします。同ソリューションは、Microsoft 365の保護はもちろんのこと、エンドポイント保護、クラウドサンドボックス、フルディスク暗号化、クラウド型セキュリティ管理ツールをオールインワンで統合しているので、導入すると同時に包括的なエンドポイントセキュリティ対策を実現できるからです。

――最後に、テレワーク下のリスクについて対策を考えているセキュリティ担当者に向けたメッセージをお願いします。

植松氏：そもそもコラボレーションツールが爆発的に普及したのがコロナ禍以降ですので、比較的新しいインフラであるといえます。そのため、コラボレーションツール自体がリスクになるという認識が、まだ十分に浸透していないのではないかと危惧しています。

これだけテレワークが浸透して、コラボレーションツールが活発に使われるようになったいま、そこのリスクは増えることはあっても減ることはないでしょう。ですので、今後もより重要性を増していくことが確実なコラボレーションツールについて、現時点からしっかりとしたセキュリティ対策を行っておくことは、近い将来のセキュリティレベルを左右する重要なファクターであると考えられます。

製品に関する情報はこちらでご確認いただけます。

セキュリティソリューション ホームページ
canon.jp/it-sec

開発元：ESET, spol. s r.o.

Canon キヤノンマーケティングジャパン株式会社

〒108-8011 東京都港区港南2-16-6 CANON S TOWER

●お求めは信用のある当社で

2021年9月現在

MECOS2109CMJ-PDF