テレワーク環境で増大する脅威にもしっかり対応！
中堅・中小企業が無理なく高度なセキュリティ対策を実現できるESETのソリューションとは

新型コロナウイルスの感染予防対策としてテレワークの導入が大企業を中心に進んでいる一方で、日本企業の大部分を占める中堅・中小企業では、導入に踏み切れていないケースが多いのも現状だ。こうした背景を受けて、テレワーク導入に際しての課題とその解決となるソリューションを紹介するバーチャルフォーラム「コロナ時代を生き抜く経営 中堅・中小企業のためのテレワーク成功の秘訣」が、日本経済新聞社の主催により2021年2月9日から3月31日にかけて開催された。
同フォーラムで行われたセッションには、キヤノンマーケティングジャパン セキュリティソリューション商品企画部 課長代理の植松 智和氏が登壇。「テレワークを狙うサイバー攻撃を2分で止める方法」と題して講演を行った。本稿では、その模様をリポートする。

増大するテレワーク環境ならではの脅威

セッション冒頭で植松氏は、キヤノンマーケティングジャパン(以下、キヤノンMJ)自身におけるテレワークの実施状況について紹介した。同社では2017年からトライアルとしてテレワークを導入したが、そのきっかけとしては大きく2つの観点があったという。1つは働き方改革であり、BCPの実現のため自宅でも仕事ができるようにすること。そしてもう1つは、外勤者がどこでも仕事ができるようにするという、モバイルワークの推進である。そうしたなかで2020年、コロナ禍に見舞われたことを受けて同社ではテレワークが定常化し、その頻度も増えているという。

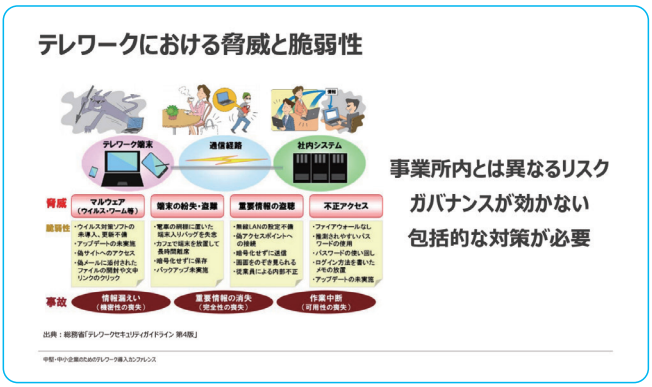
現在、キヤノンMJがテレワークの実施にあたり行っている取り組みとして、植松氏は以下の4点を挙げた。

1. モバイルPCのセキュリティ対策
2. オンラインコミュニケーションツールの活用
3. サテライトオフィスの利用
4. Microsoft 365をはじめとしたクラウド型アプリケーションの活用

こうした自社での取り組みから得られた知見も踏まえ、植松氏はテレワークにはオフィス内とは異なるどういったリスクがあるのかについて、解説した。

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

まず1つが、総務省の「テレワークセキュリティガイドライン 第4版※1」でも明記されているように、テレワークでは十分なガバナンスが効かなくなるという点だ。たとえば、ウイルス添付のメールをうっかり開いてしまったり、ウイルス対策のためのシステムやアプリケーションなどのアップデートを忘れて感染してしまったり、さらにはPCの置き忘れなどのヒューマンエラーなど、ガバナンス不足によるリスクがテレワークでは往々にして発生しがちだ。



また、ファイアウォールやUTMといったセキュリティ機器が存在しないなど、ネットワーク環境が社屋内とは大きく変わってしまうため、防御が薄くなり不正アクセスを許してしまうといったリスクもある。「オフィス内以上にさまざまなセキュリティ対策を包括的に行っていくことが、テレワークでは重要になります」と植松氏は強調した。

テレワーク環境で生じがちなセキュリティ被害とは

では、具体的にテレワーク環境において、どのようなトラブルが生じるのだろうか。まず挙げられるのが、メールやコミュニケーションツール、Webサイトの閲覧などからマルウェアに感染して業務が止まってしまうといった、インターネットの利用が増加することに起因するトラブルだ。

また、急なテレワークに対応するために、普段使っていないPCを引っ張り出してきて、OSやアプリケーションがアップデートされていないまま使用したために、脆弱性を突いたマルウェアに感染してしまうといったトラブルもある。

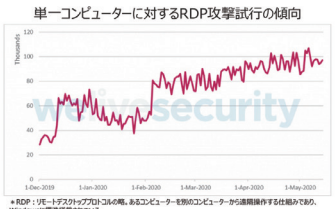
「ファイアウォールやUTMを導入されている場合も多いかと思いますが、導入時からアップデートしていないなどのケースはないでしょうか。

そうした状況を狙った攻撃も増えているため、適切なアップデートが必要です」(植松氏)

さらにPCや記憶メディアなどの持ち帰り頻度の増加から、紛失・盗難が生じて情報漏えいにつながるケースが増えている。以前から注意喚起されている事象ではあるが、依然として割合の高いインシデントのため、引き続き気をつけていく必要がある。

そして、テレワーク環境を狙った攻撃も増加しており、あるコンピュータを別のコンピュータから遠隔操作する仕組みであるRDP(リモートデスクトッププロトコル)の設定不備を狙った攻撃が、コロナ禍で急増しているという。こうした設定の不備は攻撃者も見逃さないため、特に注意が必要だ。

テレワーク環境を狙う攻撃の増加



＊RDP：リモートデスクトッププロトコルの略。あるコンピューターを別のコンピューターから遠隔操作する仕組みであり、Windowsに標準搭載されている。

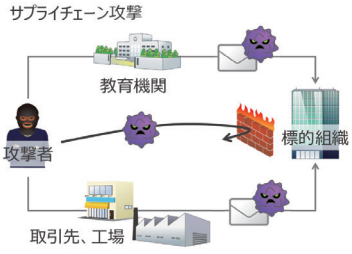
出典：ESET, spol. s r.o.
https://www.eset.com/jp/blog/welivesecurity/remote-access-risk-pandemic-cybercrooks-bruteforcing-game/

急場の環境整備
設定不備→攻撃の呼び水に

標的型ランサムウェアや暴露型ランサムウェアによる被害も増加している。これらのランサムウェアは、従来のように感染した端末内にあるファイルを暗号化して身代金を要求するに留まらず、感染端末から情報を盗み、暴露されたくなければと金銭を要求するといった二重の脅迫を行うため、被害発生時の損失も拡大してしまう。米国FBIも警告しており、今後の注意が求められる。

このように、昨今の巧妙化・悪質化した攻撃手法を如実に示すのが、サプライチェーン攻撃である。これは、セキュリティ対策の徹底した大企業ではなく、比較的に対策の弱い、その取引先や子会社などをまず狙い、そこを突破口にして最終的な標的の大企業へと侵入するという攻撃手法であり、中堅・中小企業にとっても深刻な課題となる。

巧妙化する標的型攻撃



取引先や関連会社が突破口になる恐れ

「こうした脅威の大きな変化に対して、私たちも対応していかなければなりません。働き方、働く場所の多様化が進むなか、これまでのオフィス内における境界型防御のような安全性確保は届かなります。そのため、エンドポイント単体での多重対策がより重要になります」と語った植松氏は、次世代アンチウイルスや情報漏えい防止のための暗号化、EDR(Endpoint Detection and Response)のような新しい仕組みも取り入れて、多重対策を行うことの重要性を説いた。

一般的な次世代アンチウイルスの課題とは?

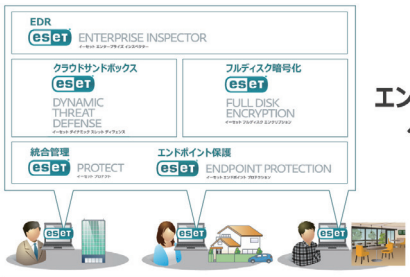
では、テレワーク環境においてますます脅威が増大するなかにあって、具体的にどのような対策が必要になるのだろうか。

ここで注目したいのが、新しいテクノロジーによるエンドポイント内での多重対策だ。AI・機械学習やビッグデータ解析といった最新のテクノロジーを採用している次世代アンチウイルス製品は、高度な分析や振る舞い検知などの仕組みを備えているので、新種の攻撃に非常に有効となる。

しかし、次世代アンチウイルスには課題もある。まず、高度な対策を端末側で行うため端末への負荷が増大してしまうことや、過剰な検出=過検知も生じがちなため、大量のアラートに悩まされるといった点が挙げられる。加えて、意外にも既知の脅威については見落としがちなため、従来製品と併用することで、両製品の相性の問題によってはフリーズが起きてしまうといったケースも多々あるのだ。

こうした課題に対してキヤノンMJでは、ESETのエンドポイントソリューションを用いた、エンドポイント単体で包括的に保護するアプローチを提唱している。具体的には、全体の統合管理、防御の基本となるエンドポイント保護のほか、EDRや次世代アンチウイルスのような新しい脅威に対応できるクラウドサンドボックス、フルディスク暗号化といった機能を持つ製品を組み合わせることにより、エンドポイント単体で包括的に保護するのである。

ESETのエンドポイントセキュリティソリューション



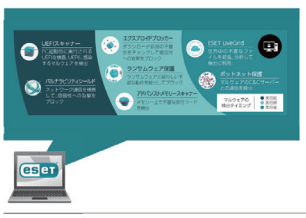
エンドポイント単体で包括的に保護

このうち基本的な防御を担うのが、エンドポイント保護プラットフォーム「ESET Endpoint Protection(EEP)」シリーズである。EEPは、アンチマルウェアを中心としたエンドポイントセキュリティ対策の基盤となるソリューションであり、軽快な動作や誤検知率の少なさなどが特徴となっている。

基本的な防御

エンドポイント保護プラットフォーム　ESET Endpoint Protection シリーズ

アンチマルウェアを中心とした、エンドポイントセキュリティ対策の基盤



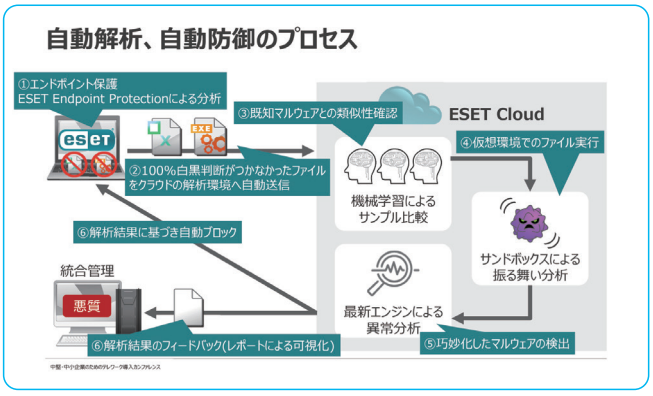
- 軽快な動作、誤検知率の低さ
- 高い検出力を支える、機械学習やヒューリスティックなどのテクノロジー
- 複数の高度なテクノロジーにより、エンドポイント単体で多層防御を実現
- 実行前・実行時・実行後の複数タイミングでもれなく検査

詳しくは>> https://eset-info.canon-its.jp/business/endpoint_protection_adv/

続いて未知の脅威からの防御を担うのが、クラウド型ゼロデイ攻撃対策製品「ESET Dynamic Threat Defense(EDTD)」だ。EDTDはほかのESET製品と連携し、ゼロデイ攻撃に用いられる未知の高度で巧妙なマルウェアに対する検出力・防御力を向上させるクラウドサービスである。

新たな脅威からの保護も2分で完了!

セッションでは、EDTDについてさらに詳しい説明をされた。ESETのエンドポイントソリューションでは、自動解析、自動防御のプロセスを実現する。まず、EEPがエンドポイント上のファイルを解析し、黒とも白とも言えない“グレー”であると判断された場合には、該当ファイルをESETのクラウド解析環境に自動送信する。クラウド上では複数の機械学習エンジンや仮想環境での振る舞い分析、そして最新エンジンを用いることで各種異常を分析。その解析結果にもとづいたフィードバックにより、巧妙化した未知のマルウェアであっても、端末でファイルが実行されるのを自動でブロックするのである。また、これと並行して解析結果はレポートにより可視化され、セキュリティ担当者の統合管理環境に送られる。



「ここまでの一連のプロセスは、おおむね2分程度で完了します。ほかにもクラウド解析のアプローチを採用した製品はありますが、このスピード感こそがESETのエンドポイントソリューションの大きな特徴となっています」と植松氏は強調した。

また、クラウドで解析している分析が完了するまではファイルを実行させない「プロアクティブ保護」の機能も備えており、さらなる安全性の向上に貢献する。さらに、ブラックボックス化がもたらす一般的なアンチウイルス製品の過検知の問題についても、EDTDであれば、まず過検知自体が生じにくいうえ、悪質と判断した理由の判断根拠が明示されたレポートを見ることで、セキュリティ担当者がしっかりと理解することができる。

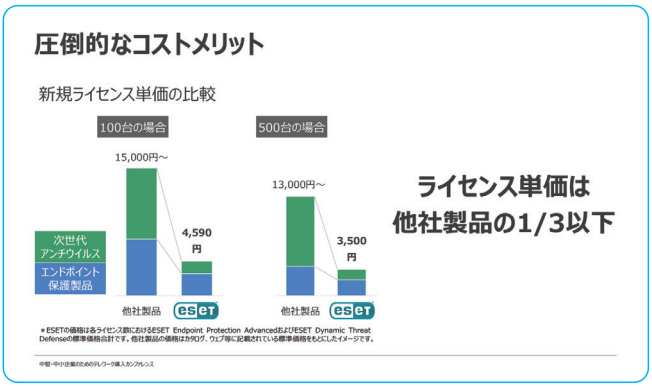
次に、ESETのエンドポイントソリューションによる未知の脅威の防御例として、植松氏は日本語環境を狙ったマルウェア「DOC/Agent.DZ」からの防御事例を挙げた。このマルウェアは、アンチウイルス製品による検知を防御・回避する高度な処理が複数存在していたが、EDTDが問題なく検知したことで、導入企業はしっかり防御することができたという。こうした日本国内を狙った攻撃であっても、EDTDはしっかりと機能することがわかる。

高度なセキュリティと圧倒的なコストメリットを両立

これまで説明したテレワーク環境における既存のセキュリティ製品の課題と、ESETのエンドポイントソリューションがそうした課題をどのように払拭できるのか、ここでおさらいしよう。

まず、端末の負荷については、高度な解析はクラウド側で実施するため端末への負荷はかからない。過剰検出・過検知も、多段階の解析と挙動レポートによる可視化で抑制する。さらに、エンドポイント保護製品(EEP)の高い検出力により防御するため、既知の脅威にも確実に対応可能だ。そして、エージェントレスであるため、端末に影響を与えず、従来製品との相性の問題も生じないのである。

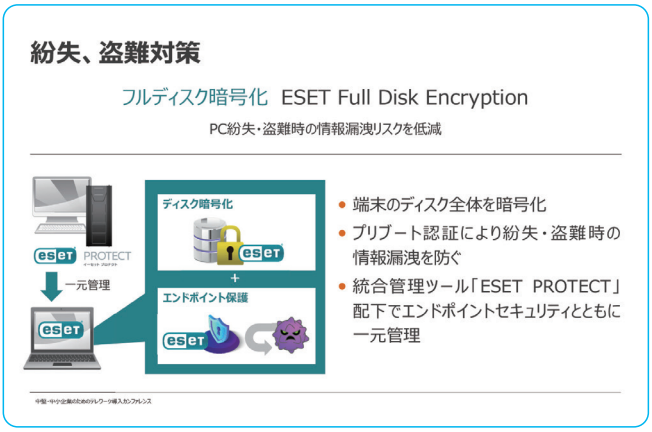
植松氏はこう語った。「さらに加えると、こうした新しいアプローチの対策方法を採用するには、コスト面も重要なファクターとなります。ESETのエンドポイントソリューションのライセンス価格は、他社製品(次世代アンチウイルスやエンドポイント保護製品)の3分の1以下と、圧倒的なコストメリットを誇っています」



では、実際にどのようなニーズがある場合に、ESETを採用すべきなのだろうか。植松氏はこれまでにESETのエンドポイントソリューションを採用するに至った具体的なニーズとして、以下の3点を挙げた。

1. 親会社からセキュリティ強化のため次世代アンチウイルスの導入を指示された
2. 現状の環境を大きく変えないで済むクラウド環境で、かつ費用も手頃にセキュリティ強化を図りたかった
3. EDRも検討したが自社の運用体制等の理由から自動防御可能なEDTDへと切り替えた

ここで植松氏は、2021年2月10日にリリースされた、フルディスク暗号化により情報漏えい対策を行う「ESET Full Disk Encryption」を紹介した。その大きな特徴は、統合管理ツール「ESET PROTECT」と連携可能な点であり、ESETのエンドポイントセキュリティとともにリスクを統合管理することで、運用負荷を軽減しながらPC紛失・盗難時の情報漏えいリスクを低減できるのだ。



最後に植松氏は、キヤノンMJが提供する高度サイバー攻撃対策に関する情報サイト※2と最新のセキュリティ情報を随時掲載している「サイバーセキュリティ情報局※3」を紹介し、情報収集の重要性を呼びかけるとともに、以下のように語り、セッションの幕を閉じた。

「働く環境としてのテレワークは実施できているものの、セキュリティ対策についてはまだまだ追いついていないといった企業・組織は多いことと思います。そうした悩みを抱えるみなさんにこそ、手軽でありながら包括的な対策が実現できるESETのソリューションをぜひ検討していただければと思います」

今後も変化していくことが予想される働き方の多様性に対して、セキュリティ対策は欠かせない要素と言える。自社に合った対策方法を知りたい方は、ぜひキヤノンMJに相談してみてはいかがだろうか。

※1 テレワークセキュリティガイドライン第4版
https://www.soumu.go.jp/main_content/000545372.pdf

※2 高度サイバー攻撃対策に関する情報サイト
https://eset-info.canon-its.jp/business/threat-solution/

※3 サイバーセキュリティ情報局
https://eset-info.canon-its.jp/malware_info/

2021年4月現在

MESET2104CMJ-PDF