キヤノンMJ・ESETのセキュリティイベントが開催！
ニューノーマル時代のビジネスを考える

各日テーマに合わせたセミナーやディスカッションを専門家が展開

新型コロナウイルス感染症拡大の影響により社会情勢が大きく変化し、多くの企業でテレワークの実施やクラウドの利用が急速に拡大した一方、企業の変化に乗じたサイバー攻撃も急増している。“ニューノーマル時代”と呼ばれるこれからの世界で進むビジネス変革を、セキュリティでどのように支えていけばいいのだろうか――。こうした課題解決を目指したオンラインイベント「Canon Security Days / ESET Security Days 2020 VIRTUAL（以下CSD/ESD）」が、キヤノンマーケティングジャパンとイーセットジャパンの共催により開催された。2020年11月10日（火）～13日（金）の4日間にわたるイベントでは、有識者・研究者・技術者・ベンダーなど専門家が登壇し、最新の市場動向や次世代に求められる対策／セキュリティソリューションについて解説がなされた。

イベント初日の基調講演には、内閣官房内閣サイバーセキュリティセンター 内閣参事官の上田 光幸氏が登壇。「サイバーセキュリティ2020と最近の動向」というテーマのもと、Society 5.0に向けたDXの推進に対して、現在政府が推進しているサイバーセキュリティ関連政策について、今後の方向性とともに解説された。

また2日目の基調講演には「次の20年を戦い抜くための情報セキュリティ」と題して株式会社アクティブディフェンス研究所 代表取締役 忠鉢 洋輔氏による講演がなされた。経営者、管理職向けにサイバー攻撃に対する予算組みについて事例とともに紹介し、中小企業のクラウド化の重要性など技術面での解説のほか、情報セキュリティに関する法律やガイドラインについても紹介された。

本稿では、コロナ禍によって高まったセキュリティリスクに対し、具体的に対策を検討をする際にぜひ参考にしていただきたいセッションとして、「ESETトラック」で講演されたキヤノンマーケティングジャパンの植松 智和氏、峯森 惇平氏のセッションを、以下で詳しく紹介する。

変化は攻撃者にもチャンス ―セキュリティも“クラウド”がカギに

初日のESETトラックでは、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 課長代理の植松 智和氏が「チャンスとリスクは表裏一体。DXを支えるサイバーセキュリティ」と題してセッションを行った。

現在、コロナ禍における感染拡大防止策として、あらゆる領域で「非接触」が求められたことで、ビジネスはもちろん生活のなかでもオンラインの促進が加速している。しかし、そのような変化に対して植松氏は「新型コロナウイルスの影響で私たちの身のまわりで起きた変化に対して、攻撃者はこの変化を狙う攻撃を増加させています」と、注意を促した。

その代表的なものとして、植松氏はRDP（リモート デスクトップ プロトコル）を狙う攻撃の増加を紹介した。コロナ禍を受けて急きょ導入したリモートワーク環境では、準備不足による設定不備が多くみられ、攻撃の呼び水になっているという。


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

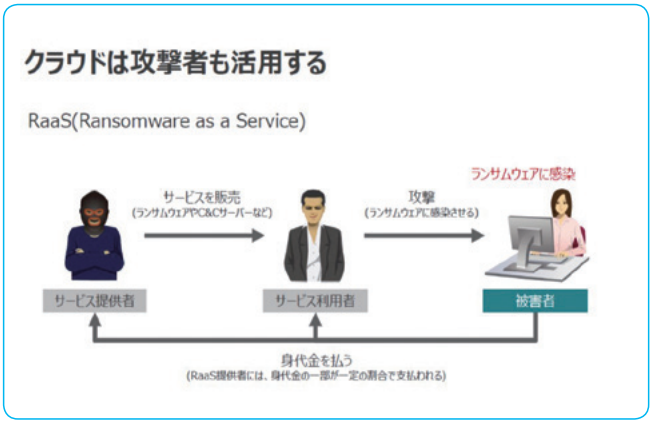
また、非接触を実現するはずのオンラインコミュニケーショ

ンツールでも、脆弱性についてさまざまな問題が指摘されている。さらに、新型コロナウイルスに関するカナダ政府の公式追跡アプリを装ったランサムウェアも発見されている。

「攻撃者は変化に対して我々以上に俊敏に対応します。つまり、変化を突くような脅威は常についてまわるのだということを理解していなければなりません」と植松氏は強調した。

そしてこれからの社会は、いまよりもさらに変化していくと予想される。「クラウドファースト」「デジタルファースト」が叫ばれるなか、今後はデジタルを前提にした考え方やそれにもとづいた取り組みが一層進むだろう。重要な機能・情報はクラウドに存在することで、クラウドを積極的に利活用する、ユーザーシップへの転換が求められてくる。

ユーザーシップへの転換は攻撃者もまた同様であり、RaaS(Ransomware as a Service)といった、SaaSのように利用料金だけで攻撃環境が手に入りやすいサービスも登場している。猛威を振るう標的型ランサムウェアや暴露型ランサムウェアに共通しているのが、暗号化と同時に情報搾取を行い、盗むだけでなく金銭が支払われないと情報を流出させると脅す「ドキシング＝晒し」による二重の脅迫が行われ、損害が拡大する点だ。



「こうした最新の標的型サイバー攻撃などを完全に防ぐのは難しいため、侵害を前提とした対応することが重要になります」とした植松氏は、キヤノンマーケティングジャパンが提唱する2021年を見据えたセキュリティ対策の考え方として「クラウドを守る対策」と「クラウドで守る対策」の2つを紹介した。

このうちクラウドを守るのが、2021年提供予定のMicrosoft 365向けセキュリティ「ESET Cloud Office Security」であり、メール(Exchange Online)やストレージ(OneDrive)のセキュリティ対策を可能とする。ここではESETの優れたテクノロジーにより、マルウェアやスパムメール、フィッシングに対抗する。SharePoint、TeamsはもちろんMicrosoft以外のクラウドサービスにも対応予定だ。

続いて「クラウドで守る対策」は、一連のESET高度サイバー攻撃対策製品群である。

「今後はさらにクラウドを生かして守っていく姿勢がカギとなります。脅威インテリジェンスとクラウドサンドボックスの2つはすでにクラウドサービスとして提供していますが、2021年よりEDRやエンドポイント保護でもクラウド版を提供予定です」とした植松氏は、各製品について詳しく解説を行った。

まとめとして植松氏は「2021年には今年以上の変化が起きることでしょう。その変化をうまく活用してビジネスチャンスとするのはもちろんですが、それは攻撃者にとってもビジネスチャンスであることを忘れてはなりません」と強調し、その対策方法として「クラウドを使って守ること、クラウドそのもので守ることや、侵害を前提とする対策が重要になってきます」とクラウド活用の重要性について協調した。

そしてセッションの最後に「チャンスとリスクは表裏一体であり、DX推進のためにはそれに応じた適切なセキュリティ対策が必要となります。私たちは『デジタルセキュリティでお客さまのビジネス変革を支える』という姿勢を貫いていきますので、ぜひ我々のソリューションでお手伝いができれば幸いです」と締めくくった。

テレワークで増大するサイバーリスクと有効な解決策を問う

2日目のESETトラックでは「ひとり情シスのお悩み解消！安心安全なテレワーク環境構築術」というタイトルのもと、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事業企画部　情報処理安全確保支援士の峯森　惇平氏がセッションを行った。


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事業企画部
情報処理安全確保支援士
峯森 惇平氏

コロナ禍によりテレワークが浸透しDXが進んだ一方、セキュリティについてはさまざま

な課題が生じている。なかでもWeb会議やテレワークが普及したことで増加したBYODは、個人所有の端末にガバナンスが効かないという点で課題とされている。

「働く環境が違っても、扱う情報は同じである点に注意が必要です。しかし、ひとり情シスはとにかく忙しいので、新しい環境の整備にリソースを費やせないのが現実といえるでしょう」と峯森氏は訴えた。

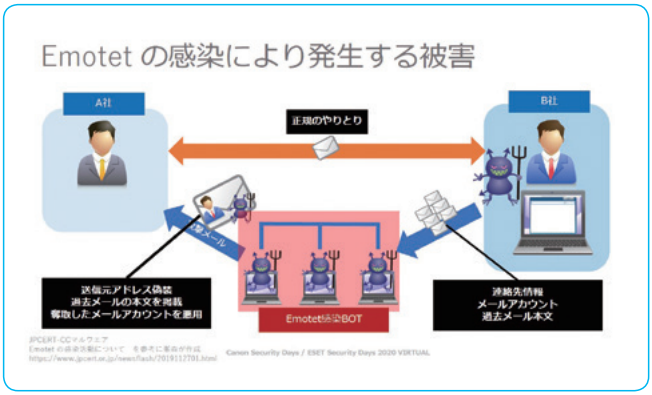
実際、セッションで紹介されたある調査によると「サイバーセキュリティ対策は最優先課題だけど課題解決の最善策がよくわからない」とした情シス担当者の割合は79%にも上っているという。峯森氏も「テレワークで推進されている環境のリスクに対して、ルール・リテラシーは追いついているでしょうか」と問いかけた。

次に峯森氏はセキュリティインシデントについて「サイバー攻撃の高度化は、コロナ禍であろうとテレワーク時代であろうと関係なく進み、必ずやってきます」と強調した。

「攻撃者は、対策の甘いところを狙います。サプライチェーン攻撃では取引先や関係会社などにおけるセキュリティ対策の弱いところを狙うため、ひとり情シスの会社であっても、こうした攻撃への対策をしなければなりません」(峯森氏)

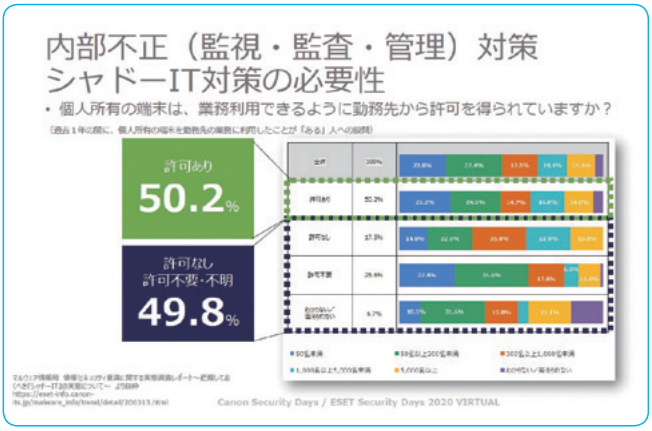
ここで峯森氏は、最近、特に流行しているマルウェアとして「Emotet」を紹介した。このマルウェアは、第一波、第二波、第三波と感染のキャンペーンを張る傾向がみられ、機能拡張がされた結果、いまや非常に高度なマルウェアになっており、さらにEmotet亜種の感染も拡大しているという。

「これまでのマルウェアは主にメールの添付で送り込まれるため、 受信者側もなかなか開かなくなっていますが、Emotetは返信型メールという手法で、やり取りしている正規メールを模してきます。しかも拡張モジュールによってランサムウェアを実行するなど機能アップもされており、感染すると金銭の要求をされるといった被害に陥ってしまうのです」(峯森氏)



また、フィッシングサイトにも注意が必要だ。フィッシングサイトとメール・被害報告は急増しており、URL件数は231%に増加、報告件数も252%に増加している。

さらに内部不正(監視・監査・管理)対策、シャドーIT対策も必要だ。キヤノンマーケティングジャパンが行った調査では、過去1年の間に、個人所有の端末を勤務先の業務に利用したことが「ある」人の半分近くが「許可なし」で利用していたことがわかった。また、企業の管理が及ばないデバイスやクラウドサービスを利用するシャドーITの利用についても、ガバナンスを効かせる必要がある。



「テレワークにおけるセキュリティリスクを考える際には、従来の境界型防御だけでなく、5GやIoTが普及し働き方改革が進められていくにあたって、各ネットワーク、端末などが今後どうなっていくかまで考えなければなりません。セキュリティインシデントはたった一度の事故で事業存続の危機につながるほど、経営に与えるインパクトが重大です。いまやセキュリティ対策は業務課題というよりも、事業継続のための経営課題であると断言できます。ひとり情シスの皆様からは経営層へはビジネスインパクトという言葉を用いた提言が必要といえます」(峯森氏)

経営者が考えるべきセキュリティ対策としては、以下の6つが挙げられる。

1. 私有端末活用対策(BYOD)
2. セキュリティレベルが低い無線LAN対策
3. 社有端末の持ち帰り対策
4. 高度サイバー攻撃への備え
5. マルウェア・フィッシングサイト対策
6. 情報漏洩事故対策

具体的に注力していくべき対策としては、まず在宅勤務中は社員間の相互監視が効かないため、メール添付のマルウェア開封やフィッシングサイトへの誤接続などのリスクが増大する。そこで解決策となるのが高性能なアンチウイルスソフトであり、ESETシリーズの「ESET Endpoint Protection Advanced」が有効だ。

また、高度サイバー攻撃については、いままでとは異なる攻撃手法であるため従来ながらの対策では対応できず、事業継続への重大な侵害リスクとなる。ここで必要となるのが早期検出であり、サンドボックス環境の導入によるゼロデイ攻撃対策を実現する「ESET Dynamic Threat Defense」が効果を発揮する。

さらに自宅と会社との間のクライアント端末移動が急増することから、紛失・盗難・置き忘れなどの端末ロスト可能性が増加する。つまり、端末に格納されている重要情報の流出リスクが急増するのだ。この課題の解決策となるのがHDDフルディスク暗号化とPCの集中管理であり、リリース予定の新製品である「ESET Full Disk Encryption」が有効となる。

「万が一紛失しても社有端末のHDD内の情報は暗号化され大切な情報は守ることができます」とした峯森氏は「テレワークの6つのリスクに対策できるESETシリーズの3つの製品を紹介しました。少しでも関心があればぜひご相談ください」と語りかけてセッションを締めくくった。

4日間にわたって開催されたCanon Security Days / ESET Security Days 。ニューノーマル時代のビジネスを考えていくうえで、新しい環境に合ったセキュリティ対策の必要性について考えることができたイベントであった。テレワークやWeb会議など、新しいビジネス環境に合わせたセキュリティ対策について詳しく知りたい方は、ぜひキヤノンマーケティングジャパンに相談してみてはいかがだろうか。

エンドポイント保護プラットホーム

eset ENDPOINT PROTECTION

イーセット エンドポイント プロテクション

製品の詳細情報はこちら

▶https://eset-info.canon-its.jp/business/endpoint_protection/

新種・亜種のマルウェアを検出する「ヒューリスティック技術」をコアに、高度化・巧妙化する脅威に対してさまざまなアプローチによる「多重防御機能」で、脆弱性をついた攻撃や有害サイトへのアクセスによるマルウェア感染など、さまざまな脅威からエンドポイント端末を守ります。

クラウド型ゼロデイ攻撃対策製品

eset DYNAMIC THREAT DEFENSE

イーセット ダイナミック スレット ディフェンス

製品の詳細情報はこちら

▶https://eset-info.canon-its.jp/business/edtd/

ESET Endpoint Protectionシリーズの検出力・防御力をさらに高めるクラウドサービスです。ゼロデイ攻撃に用いられるような未知の高度なマルウェアに対する検出・防御の即時性を高め、ESET Endpoint Protectionシリーズのユーザーは、端末への新規プログラムインストールをする必要がなく、手軽に多層防御機能を強化することができます。

製品に関する情報はこちらでご確認いただけます。

Home Page セキュリティソリューション ホームページ

canon.jp/it-sec

●お求めは信用のある当社で

2020年12月現在

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

MESET2012CMJ-PDF