特別対談

piyokango氏 × キヤノンマーケティングジャパン
「サイバー攻撃＝ウイルス」という考えは古い?

ITセキュリティに携わる人なら、誰でも一度は閲覧したことがあるだろう「piyolog」。セキュリティ関連の出来事をまとめたサイトである。運営者のpiyokango氏は2017年、「サイバーセキュリティに関する総務大臣奨励賞」も受賞している。
今回はそのpiyokango氏と、キヤノンマーケティングジャパン株式会社でセキュリティ製品「ESETセキュリティ ソフトウェアシリーズ」に携わる西村 亮氏による対談をお届けする。両氏はこの対談の中で、今、セキュリティには何が重要で、どのような考え方が必要なのかを浮き彫りにしていく。

「piyolog」運営者 CISSP
piyokango氏

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企画本部
サイバーセキュリティ技術開発センター
サイバーセキュリティ技術検証課
西村 亮氏

最近話題のEmotetには、引き続き警戒が必要

―― 「piyolog」には次々と、サイバー犯罪やセキュリティ関連の記事がアップされていますが、最近、特にアクセス数が増えているトピックというと?

piyokango氏：Emotet※1 関連には、かなりのアクセスがあります。2019年11月末にJPCERTコーディネーションセンターが出した注意喚起を受けて、「ウチの会社は大丈夫だろうか」と調べる人が多かったんでしょう。

西村氏：Emotet自体は2014年からありますから目新しくはないですが、マスコミで報道されたことが影響して、ここまでの関心事になったんだと思います。

piyokango氏：みなさん多かれ少なかれ、身の回りに思い当たる節があったということですね。Emotetの拡散の仕組みは、数年前にあった標的型攻撃の手口をカジュアルにしたようなもので、ソーシャルエンジニアリングのテクニックが上手くハマっていますから。

西村氏：Twitterで「#Emotet」を検索すると、一般の方の投稿がずらーっと並ぶくらいの状況ですよね。

piyokango氏：「ウイルススキャンをしてみたけれど、何も引っかからなかったから大丈夫」という報告をしている企業もありますが、そういう話を聞くと不安になります。Emotetは、別のマルウェアやランサムウェアがあとから入ってきて、システムにダメージを負わせるものですから。海外では毎週、そういう被害の報告が上がっていますが、ハッカーが海外での“刈り取り”を一通り終えたら、次は……と考えると、日本でも引き続き注意していかなければなりませんね。

最近耳にしない標的型攻撃、実は被害が顕在化していないだけ?

―― キヤノンマーケティングジャパンとして、最近注意している攻撃手法はありますか?

西村氏：やはり標的型攻撃、それとゼロデイ攻撃の対策に力を入れていますね。ゼロデイ攻撃は、OSやアプリケーションの脆弱性に対する修正パッチが提供されるより前にその脆弱性を突く攻撃です。メーカーが対策用のパッチを出していない状態(あるいはパッチを当てていない状態)で攻撃されたときに、どうやって防御できるかが課題です。今は「標的型攻撃は防ぎきれるものではないので、事後対策が必要」といわれていますが、長年アンチウイルス製品を提供してきたセキュリティソリューションプロバイダーとしてはやはり「防御段階で止めたい」という思いがあります。

piyokango氏：私の主観ですが、最近一般向けの報道などで、標的型攻撃の話は聞かなくなりましたよね。では一切なくなっ

たのかというとそうではなく、実は攻撃が表面化していない、つまり被害が顕在化していないだけだろうと思っています。

西村氏：ハッカーも本当に狙いたい情報については、時間と手間をかけて攻撃を仕掛けてきますからね。

piyokango氏：ええ、だから攻撃を受けていることに気づいていない、あるいは攻撃されていることはわかっていても、それが深刻なことだと認識できていないというケースもあるでしょう。たとえばインターネット分離だとか、よく世間でいわれている対策は、数年前に標的型攻撃が話題になったときに叫ばれていたもので、それを今なお、多くの人が盲信し続けているような感じがします。 現状のトレンドとして行われている攻撃の手口を、ちゃんとふまえて対策できているのか不安です。

セキュリティ・ツールを効果的に使うには、人の知見が大切

西村氏：そういう意味では、未知の攻撃の予知や検知に役立つ“脅威インテリジェンス”の活用が重要になってきますね。ただ脅威の検知後は、封じ込めや事後対策に相応の知見が求められます。今のセキュリティ対策の現場には、そこまでできる人材は多くないように思います。

piyokango氏：ある程度までは自動化に頼るとしても、人間がそのツールの特性を理解して、自ら動くことが必要だということですね。

西村氏：はい。今は人手不足ですから自動化は不可欠ですが、すべて機械任せのままにしてしまうと、いずれ手に負えなくなってしまいます。セキュリティ担当の方にはツールの中で何が行われていて、どういう判断基準で、どういうリスクに対してアラートが出ているのかを、理解しておいていただきたいですね。本来、自動化はコストの削減や作業の効率化を目的としたものですから、全部がブラックボックス化してしまうのは、あまり望ましくありません。

piyokango氏：「ツールを入れるだけで全部やってくれるんでしょ」という人が多いと思いますが、「そうじゃないんですよ、そのツールを使って対策をしていくのは、人であり組織なんですよ」と、もっとアピールしないといけませんね。

企業のセキュリティ対策事情と、ESET製品について

―― 企業のセキュリティ対策事情について、教えてください。

西村氏：大手企業ではEDR(Endpoint Detection and Response[※2])を入れ始めていますね。ただEDRは運用が難しいので、その部分をアウトソーシングしようと考えているところも多いようです。中小企業はそういう大手の動向を窺っている……という感じでしょうか。

piyokango氏：中小企業でもEDRのマーケットが拡がっているんですね。

―― キヤノンマーケティングジャパンでもEDR製品を扱っていますよね？

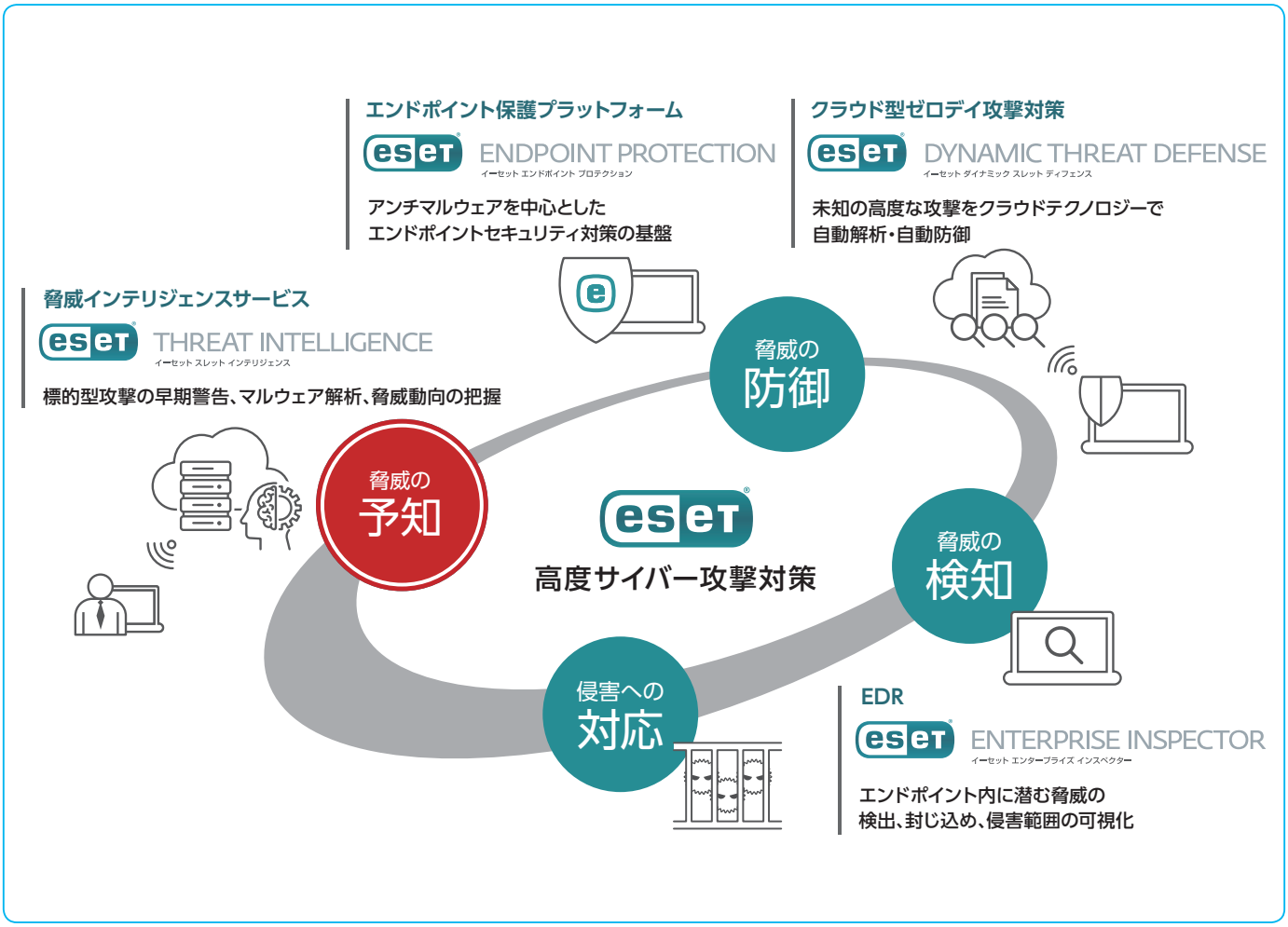
西村氏：ええ、ESET社の製品を扱っています。アンチウイルスなど防御を念頭に置いた製品としてESET Endpoint Protectionシリーズがありますが、今のサイバー攻撃にはそれだけでは対応しきれない部分があるため、ゼロデイ攻撃などの未知の高度な攻撃の対策にはESET Dynamic Threat Defense(以下、EDTD)、EDR製品としてESET Enterprise Inspector(以下、EEI)、さらに脅威インテリジェンスESET Threat Intelligence(以下、ETI)を取り揃え、攻撃の兆候把握から、事前の防御対策、侵入されたあとの検知・封じ込め対策までフォローしています。

――先ほどEDRは運用が難しいという話が出ていましたが、EEIの場合は？

西村氏：ご存じのとおり、どのEDR製品も「入れて終わり」ではなく、セキュリティ担当者の知見や、使用環境に合わせたチューニングが必要になってきます。ですからEEIを導入していただいた場合、当社の担当が1～2週間お客様のもとに出向いて、一緒にアラートの出方や動作状況を確認しながら、閾値を決めたりアラートの除外ルールをつくったり、事後対策の手法を検討したりする支援をしています。

――その他、今、名前の挙がったEDTD、ETI、それぞれの概要を簡単にご紹介ください。

西村氏：EDTDは、防御に特化したクラウドサービスです。怪しいファイルのサンプルをクラウドで受け付けて、機械学習やサンドボックスで解析し、結果を数分で返します。クラウドサービスなのでOSの枠に囚われませんし、専用のサーバーをご用意いただく必要もありません。クラウドに集まる膨大な情報を用い



包括的なセキュリティ対策が施せるESET製品群

て解析しますので、検知精度が高く、誤検知率が低いのが特長です。

脅威インテリジェンスであるETIは、SOCや研究機関で使ってもらうことを念頭に置いたものです。一般的な企業での利用はハードルが高いかもしれませんが、サイバーキルチェーンでいう「偵察」より前の段階で、攻撃の兆候をいち早く見つけることも可能です。

piyokango氏：冒頭に話に出たEmotetも、そういう兆候を的確につかめていれば「これ、うちに来るかもしれない」「来るならこうする」と事前に対策ができたと思うんですよ。

西村氏：そうですね。現在ETIは主に専門機関向けの提供ですが、インテリジェンス自体はほかのESET製品にも使われているんです。今後もETI自体はもちろん、その機能をさまざまな場面で活用することで、幅広い層に提供できるようにしていきたいと考えています。

piyokango氏：脅威インテリジェンスをバズワードとして終わらせてしまうのはもったいないので、具体的なカタチにしてもらえると、みんなが幸せで、健全な環境に近づけるんじゃないかと思います。

「サイバー攻撃＝ウイルス」だけではないことを多くの人に理解してほしい

piyokango氏：ところで今、複数の製品・サービスを紹介してもらいましたが、いろいろな製品を組み合わせると、つなぎ合わせの部分で苦労する……といったことはありませんか？

西村氏：ESETには「ESET Security Management Center」という管理プログラムがあります。ESETの製品を複数ご利用いただいていても、すべての情報が集約される仕組みになっていますから、問題ありません。

piyokango氏：なるほど、よく「いくつものセキュリティ製品やサービスが出力するログを、ほかのものと突き合わせて分析している」という話を聞くんですが、そこまで一気通貫でできるのであれば、運用コストも軽減されそうですね。

西村氏：コスト面でもそうですが「一気通貫」は、セキュリティ対策には重要な考え方です。「サイバー攻撃＝ウイルス」というのは、攻撃が「点」だったときのことで、今は「線」や「面」のように、システムやネットワーク全体を複数のセキュリティレイヤーとして捉え、多層防御の視点で対策を行うべきです。

それをもっと多くの方に理解していただきたいと思っています。

piyokango氏：「ウイルス対策ソフトが入っているのに、どうしてそれ以外のことを考えなければならないのか」という考えは根強いですね。我々、セキュリティに携わる人間がもっと声を大にして、そういう現状を変えていかなければならないと思います。

西村氏：セキュリティ担当の方々には、脅威インテリジェンスなどを通して能動的に情報収集し、その情報を経営層のようなITの専門家ではない人にもわかるように説明することが、これからますます大きな役割になっていくということを意識してもらえれば幸いです。

piyokango氏：私はセキュリティ製品の販売・開発者と対面で話すことは少ないのですが、キヤノンマーケティングジャパンさんとは課題認識についても近しいところがあるとわかりました。今後も同じ方向を向いて、頑張っていければ良いですね。

――お二方、ありがとうございました。

「いつもpiyologを拝見しています。ニュートラルな視点から、事実が簡潔に書かれているのが参考になります」という西村氏と、「面と向かってそう言われることはあまりないので、照れます」というpiyokango氏。終始、和やかな雰囲気ではあったが、次々と現れる脅威への危機感は共通しており、今後もそれぞれの方法で対抗していくことを約束して、対談は幕を閉じた。

※1 Emotet
なりすましメールに添付された文書ファイルから感染するマルウェア。メールアドレスやパスワードを窃取するほか、別のマルウェアをダウンロードさせることもある

※2 EDR(Endpoint Detection and Response)
端末上の疑わしい動きを検出・分析・調査し、組織内に潜む脅威をいち早く検知し、封じ込める機能を持つセキュリティ製品

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

●お求めは信用のある当社で

2020年3月現在

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

METI20031000MUR-642