ESET Cloudを紐解くとわかる、ゼロデイ対策におけるEDTDの安心感

新型コロナウイルスの感染拡大を受けゼロデイ攻撃をはじめとした未知の脅威が増大したことで、エンドポイントセキュリティも従来のアンチウイルス対策だけではなく、もう一歩ふみこんだ次世代アンチウイルス(NGAV)を導入する企業が増えている。しかしNGAVとひとくくりにしても、その特性や機能などは製品ごとにさまざまであり、選定を誤れば多くの問題を抱えることにもなりかねない。

そこで本稿では、エンジニアとしてセキュリティ製品の導入支援をしている、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市場サポート課の吉野 央樹氏と、主に製品やサービスの技術検証を行っている同社 同本部・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の西村 亮氏に、NGAVをとりまく現実と、同社のNGAVソリューションの強みについて話を聞いた。

(左)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
(右)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市場サポート課 吉野 央樹氏

未知の脅威対策ソリューションの選定で陥りがちなポイントとは

――導入支援をするなかで、未知の攻撃に対する企業側の対策の現状について、どのようにみていますか。

吉野氏：ゼロデイ攻撃をはじめとした未知の攻撃が急増したことなどを背景に、対策に動き出している企業は確実に増えています。市場にも未知の脅威に対応できることを強調したソリューションが多く提供されています。

ただ、そうした最先端ソリューションを導入している企業の担当者から話を聞くと、自社の環境をしっかりと把握していないがために、最適なソリューションがどのようなものか、いまひとつ詰められていないのではないかという懸念を感じることがあります。そのためソリューション自体はよくできていたとしても、運用やコストが重荷になったり、そもそも使いこなせなかったり、といった結果に陥ってしまうケースをよく耳にしますね。

――自社の環境に合わないソリューションを導入してしまったがために問題が生じることになる、ありがちなケースについて詳しく聞かせてください。

吉野氏：まず共通しているのが「未知の脅威が増加しているので、とにかく自社のセキュリティを強化しよう」といった漠然としたイメージだけで製品を探してしまっている点です。これは私自身への戒めとして言うのですが、セキュリティ製品を提案する側というのは、やはり自分の会社の製品を推奨するわけです。そのため、提案を受ける側はその製品が本当に自社の事情に最も適したものなのかどうか、十分に検討してから選定する必要があります。

最もよくあるのが、自社にソリューションをきちんと運用できるスキルや作業的余裕を持った人材がいないのに導入してしまうケースです。そして、そうした製品というのは得てしてコストも高いので、これでは宝の持ち腐れになってしまいます。

ほかにも、導入を進めてから製品を使うには社内のシステム構

成を変えなければいけないことが判明し、当初想定したよりもはるかに大事になってしまうこともあります。また、導入してはみたものの求めていたような機能が搭載されておらず、新たな機能を追加するたびにコストが発生しまう、といったケースもありがちですね。

――自社の環境や導入したいソリューションについて、事前に確認していたら防げたケースも多いですね。

吉野氏：あと意外と多いのが、機能を誤解しているケースです。たとえば「ふるまい検知機能」をマルウェアの「ふるまい」ではなく、人間の操作の「ふるまい」と捉えていて、ふるまい検知機能を備えたソリューションは、ユーザーがどこにアクセスしているかなどの挙動を監視してくれるものと考えていたという企業もありました。

そのため、実際に製品を導入してやっと認識に食い違いがあったことに気づくようなことにならないよう、事前に動作確認することも重要です。

いずれのケースも、大企業よりも中堅中小企業で生じている傾向が強いですね。

20年の知見が反映された「ESET Cloud」が未知の脅威を素早く解析、ブロック

――貴社が国内で提供しているクラウド型ゼロデイ攻撃対策製品「ESET Dynamic Threat Defense（EDTD）」もNGAVに近いソリューションですが、大企業はもちろん中堅中小企業の間でもかなり利用されていて、評価も高いですね。

吉野氏：ありがとうございます。EDTDは法人向けESETセキュリティ ソフトウェア シリーズの高度サイバー攻撃対策製品として2019年5月に国内リリースしましたが、すでに業種業態を問わず幅広い企業・組織に導入いただいております。

導入前は運用のしやすさやコストパフォーマンスを評価いただいて決定されるケースが多く、導入後にはそれらに加えて軽快な動作や安定性、サポートの質の高さなどを評価いただくケースが多いですね。

――他社のNGAV製品と比較したEDTDの強みはどこにあるのでしょうか。

西村氏：EDTDは、ベースとなる法人向けエンドポイントセキュリティソリューション「ESET Endpoint Protectionシリーズ（EEP）」と連携することで真価を発揮するクラウド型サンドボックスとなっています（EDTDの詳細は「担当者が語る！未知の高度なマルウェアの検知力、防御力をさらに高めるクラウドサービスとは?※」を参照）。

ESETのエンドポイントセキュリティソリューションにおいてベースとなるESET Endpoint Protectionシリーズ（EEP）

ESETセキュリティ ソフトウェアシリーズの製品であり、検知力の高さで知られているEEPとの連携自体が、EDTDの大きな特徴かつ強みであるといえるでしょう。EDTDは既存のESET製品と連携して、未知の高度なマルウェアに対する検出力・防御力をさらにもう一段高めるクラウドサービスで、そこにはエンドポイントセキュリティの世界をリードし続けているESET社の20年にわたるデータの蓄積や研究者たちの知見が反映されています。

――20年にわたるデータの蓄積や知見は、EDTDにおいてどのような点で役立っているのでしょうか。

西村氏：未知の高度な攻撃を自動解析・自動防御するEDTDの肝となる、ESET社のクラウド解析環境「ESET Cloud」がその象徴です。ESET Cloud上では、機械学習を用いたファイル解析やサンドボックスによるふるまい分析、ESETエンジンによる詳細なスキャンが行われますが、いずれの技術にも、ESET社ならではの高度な研究・技術、豊富なデータや知見が生かされています。たとえば機械学習にしても、最も大切なデータの質と量が充実しています。20年にわたり蓄積されたデータや、世界中のESETユーザー1億以上から提供されているデータを合わせて分析するわけです。

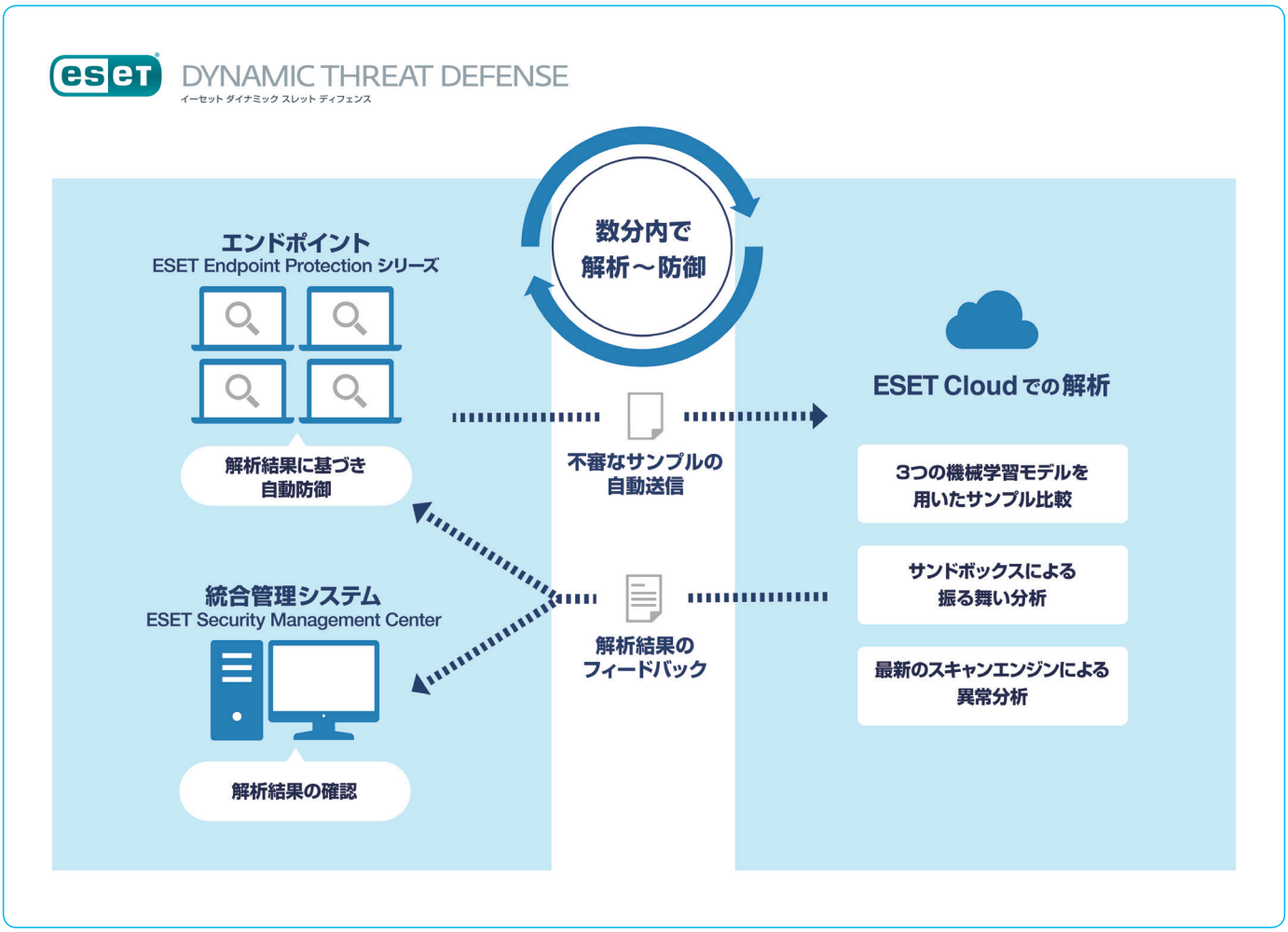
それだけではなく、研究者の分析結果も合わせて総合的な判断を行うようになっています。この研究者の知見が判断に加わるというのがポイントで、DNA分析をはじめさまざまなテクノロジーと各専門家の知見が調和した総合的な判断を、クラウドを介して行える点こそが、他社のNGAV製品にはないEDTDの強みであると自負しています。

――「ESET Cloud」があるからこそ実現するEDTDの強みには、どのようなものがありますか。

西村氏：ESET Cloudだからこそ可能な、未知の脅威を検知しブロックするまでの素早さも強みといえるでしょうね。エンドポイントで脅威を検知できなかった際にクラウドに送り判断するというソリューションはほかにも多いですが、一般的にグローバルのユーザーから寄せられた情報を順番に分析していくため、結果が反映されるまでにわずかなタイムラグが発生します。 それに対してEDTDは、いわば「ファストパス」のようなもので、非常に短時間で検体の解析を終えてエンドポイント上で未知の脅威をブロックすることができるのです。

もちろん、根幹となる検知力の高さも大きな強みです。EDTDを利用していたために未知の脅威から自社を守ることができたというケースも数多くありますし、当社内でも実績をあげています。

たとえば、2019年6月17日に新たに登録され同月に国内検出数5位になったマルウェア「DOC/Agent.DZ」を、EDTDを用いた社



20年にわたり蓄積されたESET Cloudのデータを活用するESET Dynamic Threat Defense(EDTD)

内検証の結果、サンドボックスでの挙動解析によりいち早く発見することができました。このマルウェアは日本以外ではほとんど検出が確認されておらず、99%が国内で検出されていました。これはつまり、日本を標的とした未知の脅威が増加しても、EDTDが有効であることを意味しています。

より幅広いニーズに応えていく

――EDTDの今後の展開について聞かせてください。

吉野氏：未知の脅威に対するセキュリティを強化したいという多くのお客様からのご要望に応えて、さらに提供の幅を広げていきたいですね。すでに2020年2月に、EDTDの提供範囲をこれまでの最小250ライセンスから最小100ライセンス以上へと大幅に拡大しましたが、さらに少ないライセンスでも提供できるようにしたいと考えています。そして提供の幅を広げることは、多種多様なデータがESET Cloudへと蓄積されることでもあるので、より検知力を高めることにもつながるはずです。

そして2020年8月3日にリリースしたEEPバージョン7.3では、ESET Cloudの情報をエンドポイント側でもより活用できるようになりました。最新のEEPでは、従来から行っていたエンドポイント側での機械学習の機能についても、より検知力を向上するようなアップデートが行われます。

西村氏：ESET Cloudは、市場からのフィードバックを受け、常に進化を続けています。最近では、利用者のニーズに応じて脅威に対する対応方法を選択できるようになりました。たとえば、未知の脅威らしきファイルを発見したら報告だけ行い、そのあとは様子をみることができるような仕組みや、これとは逆に、未知の脅威らしきファイルを発見した時点でそのプロセスを即時ブロックする新機能も用意しています。

このように、最新のセキュリティ動向やお客様の声を積極的に反映しながら、柔軟かつ迅速にアップデートができるのも、EDTDに限らないESETセキュリティ ソフトウェアシリーズ全般の大きな優位性ではないでしょうか。

＊＊＊

あらゆるサイバー攻撃が登場し、その攻撃も高度化していることはもちろん、新型コロナウイルスの影響により急速に変化した環境のセキュリティリスクも増大しているなか、より高度なセキュリティ対策ソリューションを導入する際は、事前に自社の環境や製品・サービスの特性を理解したうえで、選定するようにしてほしい。また、提供するベンダーがセキュリティ対策においてどのような強みや実績を有しているのかという点まで目を向けることで、失敗のない選定をすることができるはずだ。

※「https://news.mynavi.jp/kikaku/20190829-security_frontline_edtd/」