高度サイバー攻撃対策製品のリリースから1年を迎えた「ESET」

—— セキュリティ対策のニーズとトレンドはどう変化したのか

世界200カ国、1億ユーザーを守るESET社のセキュリティ製品。国内での提供を一手に引き受けるのが、キヤノンマーケティングジャパン(キヤノンMJ)だ。同社はゼロデイ攻撃をはじめとした未知の脅威、巧妙な攻撃の増大から日本企業を守るべく、2019年5月に「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をリリースした。それから1年が経過したいま、国内外のセキュリティ動向や日本企業のセキュリティ意識はどのように変化し、またESET製品群はどのような実績を上げ、市場でどう評価されてきたのか——キヤノンMJ セキュリティソリューション企画本部 セキュリティソリューション商品企画部 セキュリティソリューション商品企画第一課の課長代理、植松 智和氏に話を聞いた。

新しい脅威より内容や重みに変化のある従来の脅威に注意

——最近のセキュリティ動向のうち、特に気になる傾向は何でしょうか。

植松氏：2020年3月に当社が公開した2019年の国内マルウェア検出状況をまとめた「マルウェアレポート[※1]」を見ても明らかなように、2017年の日本国内における脆弱性を悪用するマルウェア検出数を100%とすると、2019年は212%という結果になっており、2年で倍以上に増加しています。背景としては、脆弱性を悪用するコードなどがディープウェブやダークウェブで売買されており、脆弱性を悪用するマルウェアの作成が容易になりつつあることなどが考えられます。

また、先日IPAが発表した「情報セキュリティ10大脅威 2020[※2]」では、組織部門での脅威の1位は5年連続で標的型攻撃が取り上げられており、引き続き最大限の警戒が必要だといえるでしょう。加えて「サプライチェーンの弱点を悪用した攻撃」も2年連続で4位となっているほか、「ランサムウェアによる被害」も5年連続で上位に位置づけられているため、これらも特に注意が必要です。このランキングを見ても、新しい脅威が台頭してきたというよりも、脅威自体は従来から発見されているものの、その中身や重みが変わってきていることが伺えます。

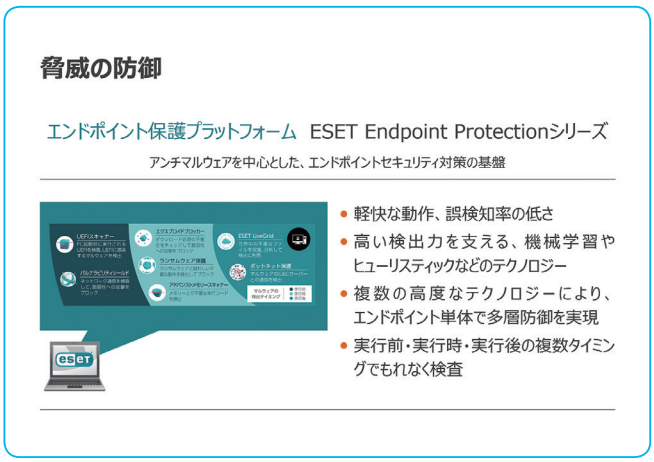
基本的なマルウェア対策にプラスαで高度サイバー攻撃対策も提供

——そもそも「高度サイバー攻撃対策製品」を2019年5月8日というタイミングで国内リリースした背景について教えてください。

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
セキュリティソリューション商品企画部
セキュリティソリューション商品企画第一課 課長代理
植松 智和氏

植松氏：以前より法人向けのエンドポイント保護製品であるESET Endpoint Protectionシリーズ(EEP)を提供しており、軽快な動作と高い検出力などによりお客様から高い評価をいただいておりました。もちろん多層防御を特長とするEEPだけでも、サイバー攻撃の脅威から十分に企業を守ることができるのは確かです。しかしながら世間では、ゼロデイ攻撃のように、侵入時に危険なものかどうか即判断ができない脅威や、標的型攻撃のような対象に合わせてカスタマイズされた攻撃、さらにはOSの機能を悪用する「ファイルレス攻撃」など、より高度かつ複雑な攻撃手法が急増していました。

このようにさまざまな脅威による被害の深刻化を受けて、従来ながらの「防御」のアプローチからもう一歩踏み込んだセキュリティ対策を実現すべく、エンドポイントセキュリティのEEPをベースとして高度サイバー攻撃対策製品を2019年5月のタイミングで市場に投入したのです。



エンドポイントセキュリティ対策の基本となるESET Endpoint Protectionシリーズ

また、ESETを導入いただくお客様も以前は従業員100未満の小規模な企業が中心でしたが、ここ数年で1,000名以上の大規模な企業、大学などの教育機関といったケースが増えてきました。そうした著名な企業・組織ほど標的型攻撃のターゲットとなる可能性が高まるうえ、より高度なセキュリティ対策のニーズも高まったことから、既存のEEPにプラスαのかたちで、より高度な対策をご提供したいという意向もありました。

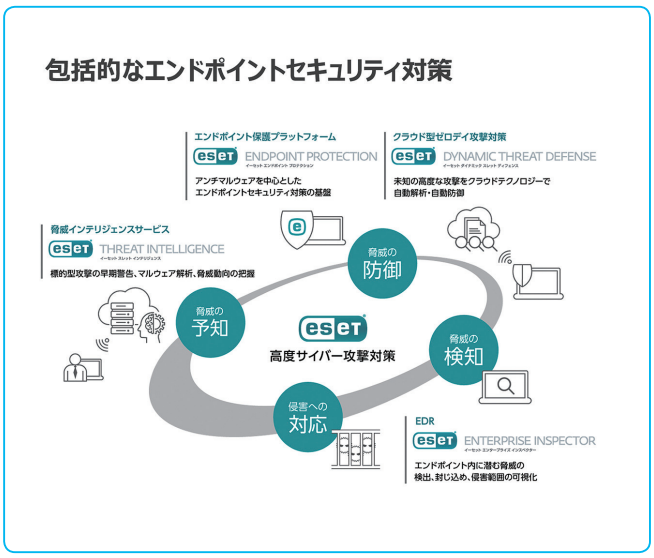
脅威の防御、検知、対応、予知までカバーする包括的なラインアップ

――これまで「ESETセキュリティ ソフトウェア シリーズ」は日本市場でどのような評価を受けてきたのでしょうか。

植松氏：ベースとなる製品であるEEPの更新率は94%と非常に高く、一度契約をいただくと長く使われるためユーザー数も右肩上がりとなっています。このように更新率が高いのも、お客様に満足いただいているからだと自負しています。一例を挙げると、日経BP社の「日経コンピュータ 顧客満足度調査」のセキュリティ対策製品部門では、当社が7年連続で1位となっています※3。内訳でも、性能・機能やサポート、コストパフォーマンス、運用性、信頼性といった、評価項目のすべてで最上位にランキングしており、それをずっと維持できている点も評価につながっているのではないでしょうか。

――高度サイバー攻撃対策製品のラインアップとそれぞれの特長を簡単に紹介してください。

植松氏：まず、ゼロデイ攻撃など未知の高度な攻撃への対策にはESET Dynamic Threat Defense(EDTD)があり、侵害に適切に対応するためのEDR製品であるESET Enterprise Inspector(EEI)、さらに脅威インテリジェンスのESET Threat Intelligence(ETI)を取りそろえています。これにより、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することができます。

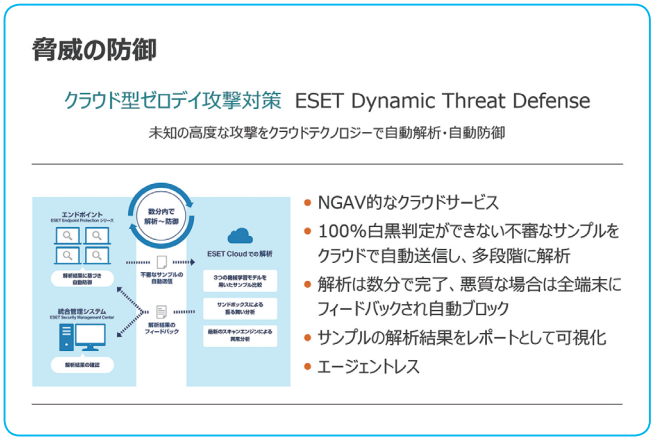


防御、検知、対応から予知までの包括的なセキュリティソリューションを展開

これらの高度サイバー攻撃対策製品のベースとなるのが、エンドポイント防御のプラットフォームとなるEEPです。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礎となるソリューションで、さまざまな機能を組み合わせた多層防御や、ファイルレス攻撃の検知機能などがひとつに集約されていて、高い検出力や軽快な動作を実現しているのが大きな特長となっています。以下、EDTD、EEI、ETIを整理してみましょう。

•ESET Dynamic Threat Defense(EDTD)

EDTDは次世代アンチウイルスソフト(NGAV)のようなクラウドサービスであり、未知の高度な攻撃をクラウドテクノロジーで自動解析・自動防御します。エンドポイント側で白黒を完全には判断できなかったファイルをクラウド側で高度かつスピーディな解析によって検知するとともに、解析結果をレポートによって可視化してくれるので、次の対策につなげることができます。



NGAVのようなクラウド型ゼロデイ攻撃対策EDTD

・ESET Enterprise Inspector（EEI）

世間でいうところのEDR製品に分類されるEEIは、エンドポイント内にひそむ脅威の検出、封じ込め、侵害範囲の可視化を行います。防ぎ切れなかった脅威を発見して、不審なファイルをブロックし、被害端末の特定と隔離を行い、悪意あるプロセスを停止する――こうした一連の対応をEEPなどと連携しつつ、ひとつのコンソールから包括的に行えるようになります。これにより、迅速かつ効率的なインシデント・レスポンスを支援します。

ESETシリーズにおけるEDR製品EEI

・ESET Threat Intelligence（ETI）

ベースとなるEEPとEDTD、EEIまでの組み合わせについては、昨今の脅威動向をふまえると、どの企業にも対応してほしいと思います。そしてさらに進んだセキュリティ対策を実現するのが、脅威インテリジェンスサービスのETIです。これは、世界中で1億台以上にもおよぶESET製品のセンサーから収集した脅威情報を提供するサービスで、標的型攻撃の早期警告やマルウェア解析、脅威動向の把握に役立つものとなっています。顧客や自社を狙う潜在的な攻撃予兆や、悪質な疑いがあるファイル、URLなどの情報を提供するため、今はまだ見えない攻撃や将来発生しうる攻撃予兆を把握して、攻撃者に対して先回りした対応を可能にします。

「今は見えていない攻撃」や「将来発生しうる攻撃」の予兆を把握できるETI

今後の展開のキーワードは「クラウド」と「サービス」

――今後リリースを予定している新製品／サービスはありますか。

植松氏：2020年5月8日よりEEIの運用監視サービスを提供開始いたしました。EEIのようなEDR製品というのは、エンドポイント側で見逃される不審な脅威をあぶり出す有益なツールではあります。しかしながら、これまでの多くのセキュリティ製品のように「入れてしまえばあとはシステム側が自動的に対処してくれる」といった性質のものではありません。最終的には人による判断が求められるため、すべての企業がEDRを使いこなせるわけではないというのが現状です。

そこで、EEIの運用監視までを当社が引き受けてしまおうというのが運用監視サービスです。このサービスでは、不審な脅威をあぶり出すのに加えて、24時間365日の監視も提供いたします。

――最後に、日本市場における今後の抱負についてお聞かせください。

植松氏：これはESET製品に限らず当社のセキュリティ事業全般にいえることですが、今後は「クラウド」と「サービス」にさらに重きを置いて展開します。EDTDやETIはクラウドで提供されていますが、クラウドのリソースを活かすことで高度な解析をいち早く行うことができるほか、ESET社が有する最新の脅威情報と連携しやすくなるため、ESET製品においてもクラウドの活用は欠かせません。そうしたなか、ESET製品の新たなクラウドサービスも2020年から2021年にかけてリリースを予定しています。

サービスについても、従来のツールとサポートの提供に加えて、内容を強化していきます。社内の体制強化はもちろん、今後は他のセキュリティベンダーとの協業も視野に入れていきたいと考えています。また、以前よりESETセキュリティ パートナー プログラム（ESPP）というESETのパートナー間での協業を促進するプログラムによって全国網でのお付き合いがありますので、そうしたパートナーとの取り組みも強化していきたいですね。

――ESETを中心とした輪が広がりそうですね。ありがとうございました。

※1 キヤノンMJが運営する「サイバーセキュリティラボ」が発表した「2019年年間マルウェアレポート」より
※2 2020年1月にIPAより公開された「情報セキュリティ10大脅威 2020」より
※3 株式会社日経BPが毎年発表している「顧客満足度調査」より

エンドポイント保護プラットホーム

ENDPOINT PROTECTION
イーセット エンドポイント プロテクション

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

DYNAMIC THREAT DEFENSE
イーセット ダイナミック スレット ディフェンス

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。

EDR (Endpoint Detection and Response)

ENTERPRISE INSPECTOR
イーセット エンタープライズ インスペクター

ESET Enterprise Inspectorは、エンドポイントレベルでのマルウェア対策を30年にわたり手がけてきたESET社の経験を基に開発されたEDR製品です。組織内の端末から収集したさまざまなアクティビティをもとに、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割り出し、封じ込めることができます。

脅威インテリジェンスサービス

THREAT INTELLIGENCE
イーセット スレット インテリジェンス

ESET Threat Intelligenceは、マネージドセキュリティサービス事業者やSOCサービス事業者などのセキュリティサービスプロバイダー、およびCSIRTやSOCなどのセキュリティ対策部門を有する企業・組織向けの脅威インテリジェンスサービスです。お客さまは本サービスによりサイバー攻撃の予兆や攻撃手法の解析、世界で使われている攻撃ツールの検出状況などを把握し、「今は見えていない攻撃」や「将来発生しうる攻撃」を予測できるため事前にサイバーセキュリティ対策を講じ被害を最小限に抑えることが可能です。

● 製品の詳細情報はこちら >> https://eset-info.canon-its.jp/business/

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

開発元：ESET, spol. s r.o.
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

2020年5月現在
MESET20051000MUR-646