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?

ゼロデイ攻撃に代表される未知の脅威が猛威を振るう昨今では、残念ながら従来のマルウェア対策だけでは十分な対策とはいえなくなっている。こうした背景を受けてキヤノンマーケティングジャパン(キヤノンMJ)では2019年5月、法人向けESETセキュリティ ソフトウェア シリーズの新製品となる「ESET Dynamic Threat Defense(EDTD)」の提供を開始した。

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・防御力をさらに高めるクラウドサービスだ。本稿では、ESETシリーズ独自の機能やメリットを持つEDTDの製品発売までの経緯から今後の展望などについて、EDTDを発売するにあたり、マーケティングを担当している植松 智和氏と、EDTDの技術検証を担当している中村 菜摘氏にインタビューした話をお届けする。

左:キヤノンマーケティングジャパン株式会社
エンドポイントセキュリティ企画本部 エンドポイントセキュリティ企画部
エンドポイントセキュリティ企画第一課 チーフ
植松 智和氏

右:キヤノンマーケティングジャパン株式会社
エンドポイントセキュリティ企画本部 エンドポイントセキュリティ技術開発部
エンドポイントセキュリティ技術検証課
中村 菜摘氏

ユーザーは導入の手間いらず 導入後もクラウドで高度な解析を“自動”で実施

――まずはESET Dynamic Threat Defense(以下、EDTD)を提供することとなった背景を簡単に教えていただけますか。

植松氏:昨今増加する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による被害が多発しています。また、エンドポイントを狙う標的型サイバー攻撃も、対象に合わせて「カスタマイズ」されることで検知が難しくなっていたり、OSの機能を悪用する「ファイルレス攻撃」が多発していたり、さまざまな脅威による被害の深刻化を受け、2019年5月より当社が提供したのがEDTDです。

――脅威による攻撃への対策として提供されたEDTDとは、どのような製品なのでしょうか。

植松氏:EDTDは、これらの未知の高度な脅威に速やかに対処できる機能を持ちつつ、サンドボックスの機能や機械学習(AI)の技術を取り入れたクラウドセキュリティソリューションとなっています。世間でいうところの「次世代エンドポイントセキュリティ製品」に近い製品だといえるでしょうね。

――クラウドセキュリティソリューションとのことですが、導入形態はどのようなかたちになるのですか。

中村氏:EDTDは単独の製品ではありますが、ESETのエンドポイントセキュリティ製品と連携することで真価を発揮するオプション的なサービスとなっています。法人向けESET Endpoint Protectionシリーズ(以下、EEP)のバージョン7以降と、管理サーバー「ESET Security Management Center」を導入している環境であれば、EEPの設定画面からEDTDを有効にするだけで、後は自動的に連携して処理が実行されるようになります。エンドポイント側には、アプリやエージェントなどの追加インストールは必要ありません。

判断が難しい“グレー”もしっかり分析、誤検知も少ないEDTDのさまざまな特長

―― EDTDの一番の特長を教えてください。

植松氏：エンドポイントにインストールされているEEPと連携して動作すること自体がほかにはない優れた特長といえるでしょう。エンドポイントにメールやWebからファイルがダウンロードされると、最初にEEPが自動的に多角的な解析を実行してマルウェアかどうかを判断します。このときに「マルウェアと断定はできないが、不審なファイル」という“グレー”な判断結果だった場合には、自動的にEDTDのクラウドに転送して、クラウド上で詳細な解析を実行します。解析はおおむね2、3分程度で完了し、もし悪質なファイルだった場合には自動で防御を行います。

―― EDTDはクラウド上で動作をするというのも特長かと思いますが、それに関してはいかがでしょうか。

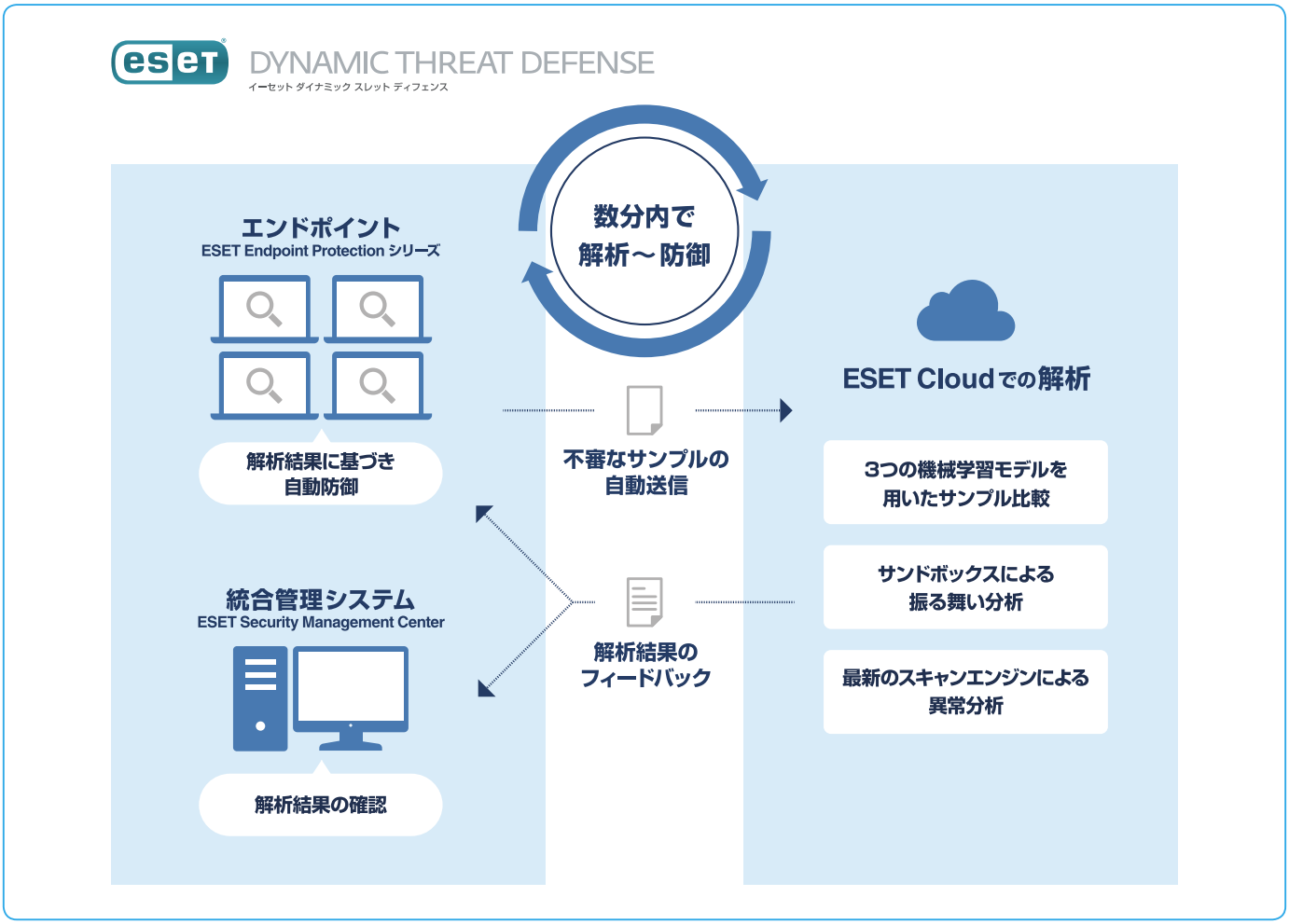
中村氏：もちろんESET社のクラウド解析環境はEDTDの大きな特長となっています。クラウド上では、機械学習を用いたファイル分析やサンドボックスによる振る舞い分析、ESETエンジンによる詳細なスキャンが行われます。いずれの技術にも、エンドポイントセキュリティの世界をリードし続けているESET社の高度な知見が反映されています。

キヤノンマーケティングジャパン株式会社
エンドポイントセキュリティ企画本部
エンドポイントセキュリティ企画部
エンドポイントセキュリティ企画第一課 チーフ
植松 智和氏

キヤノンマーケティングジャパン株式会社
エンドポイントセキュリティ企画本部
エンドポイントセキュリティ技術開発部
エンドポイントセキュリティ技術検証課
中村 菜摘氏

―― サンドボックスに関しては、安価にその環境を持てるのもメリットでしょうか。

中村氏：サンドボックスはOSや言語など多種多様な環境が用意されていて、実際にファイルを実行することで、どこに危険性があるかを可視化してレポートしてくれます。利用する側からす



端末で見つけた不審なサンプルを送ることができるクラウドベースの解析環境「ESET Cloud」を利用したESET Dynamic Threat Defense

れば手軽に導入・運用が可能でありながら、実はその裏では高度な処理が行われているというわけですね。そしてこれらの特長を有するEDTDであれば、未知の脅威に対する防御の即時性を高めるのと同時に、自社を取り巻く脅威の可視化ができることも特長となっています。

―― そのほか、性能面での特長があれば教えてください。

中村氏：当社がEDTDを提供するなかで技術検証を行っている立場としては、誤検知の少なさ、つまり信頼性の高さと、動作の軽快さも特長としてあげたいですね。

ESET社では従来から一貫して「誤検知ゼロ」を目標に掲げていて、第三者テスト機関であるAV-Comparativesからも「最も誤検知率が低いベンダー[※1]」と評価されています。EDTDにもそれが反映されており、積極的にファイルをクラウドに送りながら、しっかりと多角的な解析を行うために、誤検知や過検知の件数は少ないと感じています。

さらに動作の軽快さについても、ESET製品自体がAV-Comparativesで「最もシステムへの影響が小さい製品[※2]」として以前より評価されている性能をそのまま受け継いでおり、EEPにEDTDの機能を有効にしても気づかないほど軽快です。

クライアントより送信されたファイルの一覧および分析情報(一部抜粋)を確認することができる

すでに日本国内のみを狙った最新のマルウェアを検知した実績も!

―― 国内での提供開始以来、具体的な成果があれば教えてください。

植松氏：当社ではESET製品が国内で検出したマルウェアに関するさまざまなデータを分析した「マルウェアレポート」を毎月発表しているのですが、 その最新版(2019年7月時点) で、「DOC/Agent.DZ」というマルウェアが、2019年6月17日に登録された新しいマルウェアでありながら6月全体の国内検出数の5位になったと報告しています。このマルウェアは、日本語環境を狙ったダウンローダーが仕込まれたExcelファイルを添付したばらまき型メールで拡散されており、実に99%が国内で検出され、日本以外ではほとんど検出が確認されていません。

DOC/Agent.DZは、画像ファイルにデータを隠蔽する「ステガノグラフィー」という手法を備えており、難読化を多重にも施すといった巧妙な手口を持っています。しかし、EDTDを導入済みの当社環境において、その存在をいち早く発見することができたのです。この事実は、EDTDであれば、日本語環境に特化した未知の脅威であっても検知して防御が可能であることを意味しています。

アイコン	ステータス	説明
	不明	ファイルは分析されませんでした。
	未感染	検出エンジンはサンプルを悪意があるものとして特定していません。
	不審 非常に不審	検出エンジンは不審であるとファイル動作を評価しましたが、明確に悪意があるわけではありません。
	悪意	ファイル動作は悪意があるとみなされます。

状態	説明
Dynamic Threat Defenseに送信	ファイルは分析のためESET Cloudに送信されました。
分析中	分析を実行中です。
完了	ファイルが正常に分析されました。
再分析中	以前の結果がありますが、ファイルは再分析されています。

日本語環境にも対応しており、社内検証では実際のマルウェア検出にも成功している

大企業からスタートアップまで大きな反響が

――まだ国内リリースから日が浅いですが、反響はいかがでしょうか。

植松氏：ありがたいことに、様々な企業・組織からEDTDに関する問い合わせをいただいています。そうしたなかには、他社の次世代エンドポイントセキュリティ製品を導入したものの、誤検知の多さや運用の手間が課題となっており、それを解消したいというケースも多いですね。

――他社製品を導入した企業からみても、EDTDの運用の手軽さは魅力ということですね。

植松氏：あと少し意外だったのが、比較的規模の小さな企業からの問い合わせも多いことです。EDTDのように高度な脅威から防御するセキュリティ製品というのは、セキュリティ意識の高い大企業のニーズが中心になると当初予想していたのですが、実際には中小規模の企業からのニーズも大きかったわけです。標的型攻撃のターゲットが、比較的対策の進んだ大企業よりも、その取引先である中堅・中小企業へと移りつつあったり、東京2020オリンピック・パラリンピックをはじめとした大規模なイベントが今後続くなかで、日本の企業・団体を狙ったサイバー攻撃が増加することが予想されていたりなど、高度なセキュリティ対策の必要性が、必ずしも企業の規模や業種を問わなくなっていることが背景としてあげられるでしょうね。

EDTDは導入コストも安く、専任のIT管理者やセキュリティ管理者がいない規模のお客様でも導入しやすいので、当社としてもそうしたニーズに応えていきたいと考えています。

――ESETそしてEDTDの提供に関する今後の抱負についてお聞かせください。

中村氏：従来のESET製品にEDTDを加えることで、より高いレベルの安全・安心が得られるのだということを、少しでも多くの方々に知っていただけるよう努めていきたいですね。

植松氏：現在は最小250ライセンスからの販売となっていますが、先ほどお話ししたようにより小規模な企業からの引き合いも多いので、まずはそれ以下のライセンスでも提供できるようESET社と検討しているところです。そして、EDTDを含めたESET製品トータルの力で、日本中のお客様のエンドポイントをしっかりと守り続けていきます。

――力強い言葉、ありがとうございました。

※1　2019年3月「サイバーセキュリティアワードAV-Comparatives」より

※2　2019年4月「AV-ComparativesおよびVirus Bulletin」より

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

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

2019年9月現在

MEDT1909CMJ-PDF