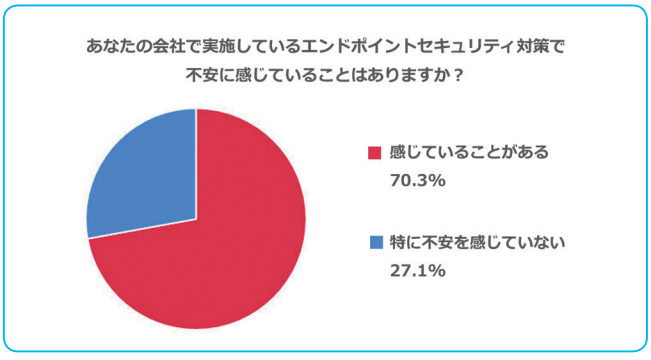
エンドポイントセキュリティ対策に関する最新調査からみえた、次世代アンチウイルスの課題

近年のエンドポイントセキュリティ対策において、従来のアンチウイルスだけではなく、もう一歩ふみこんだ対策として次世代アンチウイルス(NGAV)を導入している企業が増えている。とはいえ、ひと口にエンドポイントセキュリティといっても対策の範囲は企業によってさまざまで、その認識も異なるのが現実だ。そこで今回、IT関連の業務に携わる方々を対象に、エンドポイントセキュリティに関するアンケートを実施した。本稿では、その結果を紐解きながら、企業のエンドポイントセキュリティの現状と担当者の意識について浮き彫りにしていきたい。

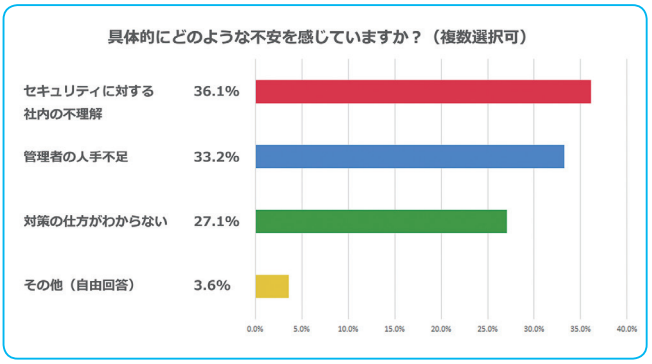
7割のIT担当者がエンドポイントセキュリティに「不安」

まず「あなたの会社で実施しているエンドポイントセキュリティ対策で不安に感じていることはありますか？」という質問については、約7割ものIT担当者が何らかの不安を感じていると回答している。その背景として、エンドポイントは端末の台数が多いことが挙げられるだろう。かつてセキュリティ対策の中心であったファイアウォールやルーターなどのネットワーク間をつなぐ機器は、あくまで“点”であるため設置する数も少なくて済んだ。対して現在のセキュリティ対策で最重要となるエンドポイント端末は、当然ながらその数が非常に多い。そのためIT担当者にしてみれば、エンドポイント端末のセキュリティ確保に対して、より強い不安を感じるのは無理もない。

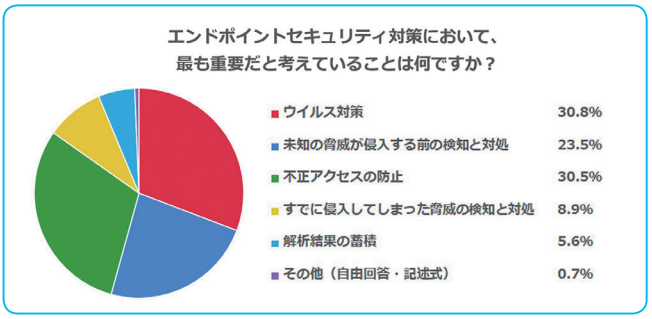


もうひとつ、昨今のクラウドシフトへの進展もエンドポイントセキュリティの重要性を高めている。各種業務アプリがクラウドで提供されているなかで、さまざまな機密情報の保管場所も社内のファイルサーバーからクラウドへとシフトしている。すると守るべきポイントも、作業を行うエンドポイント端末と、アプリやデータが存在するクラウドという両端へと集中してきているのである。とりわけ、ここに来てテレワークやモバイルワークの需要が急拡大していることも、クラウドサービスを利用する圧倒的多数のエンドポイント端末について、セキュリティの確保が強く問われる理由といえるだろう。

具体的にどのような不安を感じているのかについては、セキュリティ対策に対する社内の理解が得られないことや、管理するIT担当者の人材不足に続き、対策の仕方がわからないという不安も3割弱を占めていた。攻撃手法が日々変化するなか、新しい高度な攻撃に対応するためのスキル不足や人員不足を感じているIT担当者が多いものと推測される。また利用するツールについても、以前のようにアンチウイルス製品を用いて定義ファイルを常に最新のものに更新していれば、最低条件を満たせた状況とは大きく変わってきている点も見逃せない。

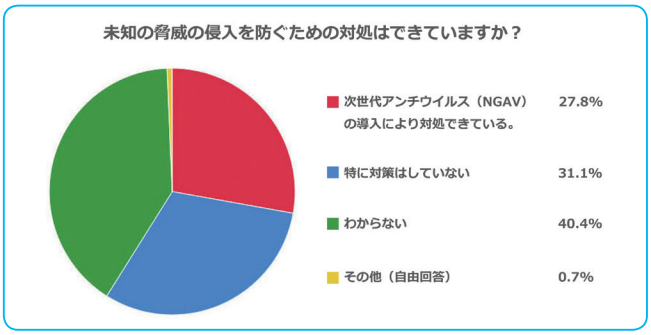


また、エンドポイントセキュリティ対策において特に「ウイルス対策」「未知の脅威が侵入する前の検知と対処」を重要視するという回答で半数以上を占めているところをみると、やはり「未知の脅威」に関して関心が高いことがうかがえる。



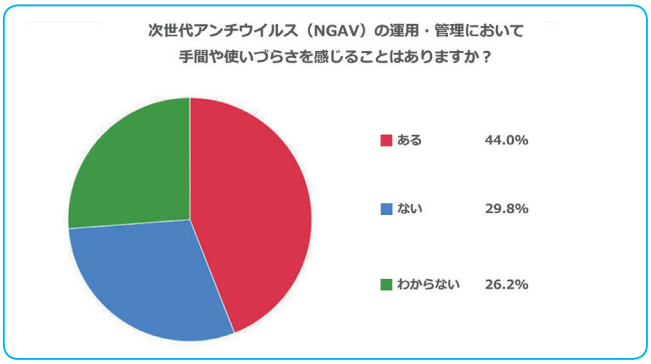
未知の脅威への対策が意外と進んでいない理由とは

では、実際に企業は未知の脅威に対してどのような対策を取っているのだろうか？ アンケート結果では、未知の脅威に有効とされるNGAVを導入している企業は3割弱しかいなかった。一方で未知の脅威に対する対策を特にしていないとした企業は3割を超えている。その理由としては、まず中堅中小企業を中心に対策コストが確保できないこと、次に従来ながらのベーシックなウイルス対策だけで手一杯で、未知の脅威への対策があと回しになりがちなこと、そして数年前にNGAVが騒がれたものの導入してみると決して万能ではないという評価が広まったことなどが挙げられるだろう。



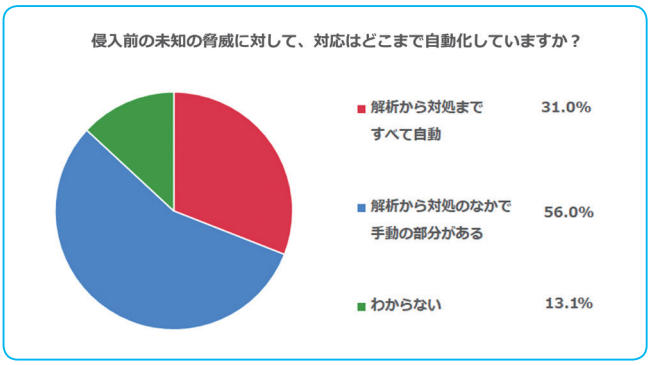
とはいえ最新の攻撃手法では、ターゲットとなる企業がどのような対策を行っているかしっかり調査したうえで、対象に合わせた攻撃を行うなど、攻撃ツールをカスタマイズする傾向が強まっている。そのため、アンチウイルス製品だけではエンドポイントの安全は確保できないのが現実だ。

もはや必須といえるNGAVであるが、その運用・管理の際に手間や使いづらさを感じているIT担当者が約4割強もいた理由のひとつとして、一般的にNGAVというのはアグレッシブに攻撃の兆候をみつけてくるため、どうしても誤検知や過検知が増える傾向にある点が挙げられるだろう。担当者はいちいち本当に攻撃であるかどうか確認しなければならず、手間が増えてしまうのである。

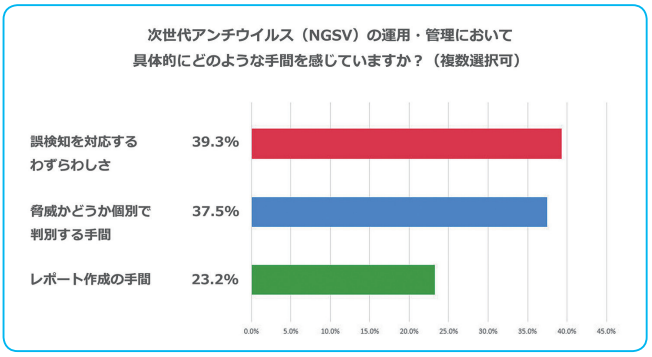


もうひとつ、多くの場合、既存のアンチウイルス製品を補完するかたちで個別にNGAVを導入しているケースが多いことも理由としてあるだろう。二種類の製品をそれぞれ管理することになるため、特にベンダーが異なる場合は教育だけでもコストや手間が余計にかかってしまうのだ。

そこで、侵入前の未知の脅威への対応をどこまで自動化できているか聞いてみたところ、半数以上が解析または対処の場面で手動による対応を行っていることがわかった。セキュリティ担当者の人材不足が叫ばれているにもかかわらず、手動の対応が多ければ担当者にはさらなる負担がかかってしまうことになる。



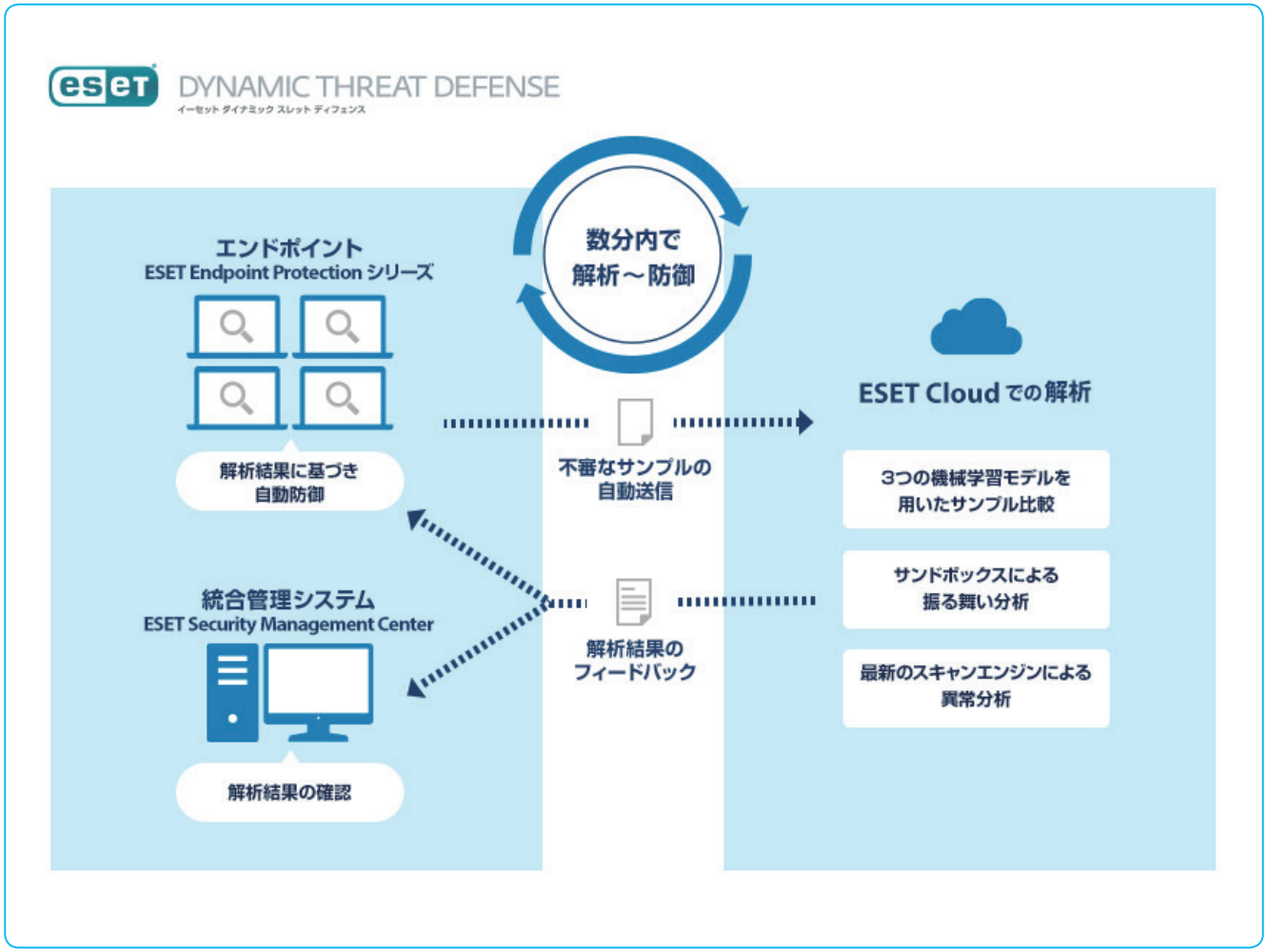
では、具体的にどのような手間を感じているのだろうか。やはりこの質問の回答から浮き彫りになったのが、誤検知に対応するわずらわしさや、脅威かどうか個別で判別する手間といった、多くのNGAVに共通する課題であった。



クラウドテクノロジーの活用で未知の脅威対策の自動化と可視化を実現するクラウド型ゼロデイ攻撃対策製品EDTD

調査結果からは、エンドポイントセキュリティ対策に不安を抱きながらも、既存のNGAVの管理画面や、コスト面での課題に頭を悩ませている企業が多いことが明らかになった。そこで紹介したいのが、キヤノンマーケティングジャパンが提供する「ESET Dynamic Threat Defense(EDTD)」である。ひと言で説明すると、EDTDは前述したような課題を解決できるNGAVである。EDTDは「法人向けESETセキュリティ ソフトウェア シリーズ」の一製品という位置づけであり、既存のESET製品とクラウドテクノロジーを連携することで、ゼロデイ攻撃に用いられる高度な未知の脅威に対する検出力や防御力をさらに高めてくれる。

このベースとなるESETのアンチウイルス「ESET Endpoint



未知の脅威を自動解析、自動防御

Protectionシリーズ(以下、EEP)」は、単体でも検知力の高さで知られているが、そこでグレーと判断したファイルを、機械学習やサンドボックスといった最新のテクノロジーを駆使したEDTDのクラウド解析環境でしっかりと判断するようになっている。このように、検知のプロセスが何段階にもシームレスにつながることで、誤検知を大幅に抑えることに成功しているのだ。

つまりEDTDは単独の製品ではあるものの、EEP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いえる。このため、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、自動的に連携される。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の必要はない。こうしたアンチウイルスとの一体化により、運用管理もひとつのソリューションとして集約できるうえ、社内への教育も統一することが可能となるのだ。

また、EDTDが解析に要する時間はクラウド上でおおむね5分以内。仮に不正なファイルを見つけたとしても自動的に即時ブロックするなど、迅速に対応することで被害を最小限に抑えてくれる。解析結果を確認して手動で対処をする手間がないため、ゼロデイ攻撃に用いられるような未知の脅威に対する管理と運用の自動化も格段に進むだろう。

さらにEDTDは、未知の脅威への対応までを自動化するだけでなく、クラウドで解析したファイルの判定結果をわかりやすいレポート形式で報告してくれる。たとえば「不正な通信をしようとしていた」「正常なアプリの動作とは異なる」など、具体的かつ丁寧に説明してくれるため、高度な専門知識がなくても自社のセキュリティの状況をしっかりと可視化して把握できるのだ。不審なファイルの形式、ファイル送信の多い部門など、自社の傾向をより理解して対策が進めやすくなり、担当者の経験値向上やスキルアップにもつなげられる。

大企業から中小企業まで導入しやすく サプライチェーン攻撃にも有効

このようにNGAVとして数々のメリットを有するEDTDだが、EEPのオプションとして提供されるためわずか千円ほどの追加費用で導入が可能だ。そのEEPも4～5千円程度ときわめてリーズナブルとなっている。一般的なNGAVの価格が安くても1万円以上することを思えば、導入のハードルはきわめて低いといえるだろう。このような価格で提供可能なのも、ひとつはクラウ

ドテクノロジーであることが大きい。

数々の特徴を有するEDTDは、大企業はもちろんのこと、中堅中小企業からのニーズも高い。そうした動向を受け、これまで最小250ライセンス以上からの提供としていたが、2020年2月より最小100ライセンス以上からの提供へと、大幅に提供範囲を拡大している。これにより、サプライチェーン攻撃をはじめとした脅威のターゲットとなる大企業はもちろん、その関連会社や子会社における未知の脅威への対策も進むはずだ。

今回の調査によって明らかになった、日本企業の間に広がるエンドポイントセキュリティに対する不安感も、EDTDによって劇的に解消されることが期待できるといえるだろう。未知の脅威への対処はもちろん、管理・運用の自動化による担当者の負担軽減も実現することができるEDTDを、ぜひ検討してみてはいかがだろうか。

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

2020年4月現在

MEDTD20041000MUR-644