キヤノンマーケティングジャパン株式会社

ソリューション理解から製品比較のポイントまで

―― EDRまるわかりガイド

INDEX

企画・制作 マイナビニュース

サイバー攻撃の手口が巧妙化している昨今、脅威の侵入すべてを防ぐことは難しいのが現状だ。そこでいま、侵入後の対策を主機能とするセキュリティ製品として注目を集めているのが“EDR(Endpoint Detection and Response)”というソリューションである。本連載では、標的型攻撃に代表される高度なサイバー攻撃への対策に有用とされるEDRの解説と、導入検討に役立つ製品の比較ポイントの紹介を中心に、エンドポイントセキュリティの新定番たるEDRを徹底解剖したい。

第1回 次世代エンドポイントセキュリティ「EDR」とは

○ 事前対策に加えて事後対策の必要性が叫ばれている理由とは

標的型攻撃やランサムウェアをはじめとして、サイバー攻撃はますます高度化・巧妙化しており、いまや企業経営の屋台骨まで脅かしかねない最重要リスクの1つとなっている。このサイバー攻撃のターゲットとなるのが、企業が保持するさまざまな「情報」である。

それは、決算などに関わる情報、新技術や新製品に関する情報、そして顧客や取引先、従業員の個人情報など、あらゆる機密情報におよぶことになる。もしも、こうした情報がサイバー攻撃によってひとたび流出してしまえば、企業が被る損害は計り知れないものとなり得ることは、実際の情報漏えい事件からもおわかりいただけるのではなかろうか。

このような動向を受けて、国も企業に対し情報セキュリティ対策の徹底を促しているが、なかでも着目すべきなのが、経済産業省が独立行政法人情報処理推進機構(IPA)とともに策定した「サイバーセキュリティ経営ガイドライン」だろう。

経営者がサイバー攻撃から企業を守るための理念や行動を記したこのガイドラインは、2017年11月に改訂され「V2.0」となったが、V1.0から重要な変更がいくつかあった。そのなかでも最大の変更点といえるのが、「攻撃の検知」に関する、「サイバーセキュリティリスクに対応するための仕組みの構築」など事後対策の重要性と必要性についての記述が大幅に追加されたことである。経済産業省では改訂の理由について、昨今のサイバー攻撃の巧妙化により事前対策だけでは対処が困難となっていることを強調しているのだ。

従来の情報セキュリティ対策では、サイバー攻撃による自社への侵入を防ぐための事前対策を重点的に行っていた。しかし前述のようなサイバー攻撃の巧妙化により100%侵入を阻止することは難しくなってきている。そこで、サイバー攻撃により侵入されてしまう可能性があることを前提とし、もし侵入されてしまったとしても、侵入をいち早く検知して状況を把握し、迅速かつ適切な対応をとることで被害を最小限に抑えるという事後対策もまた、事前対策と同様にいまの企業には強く求められているというわけだ。

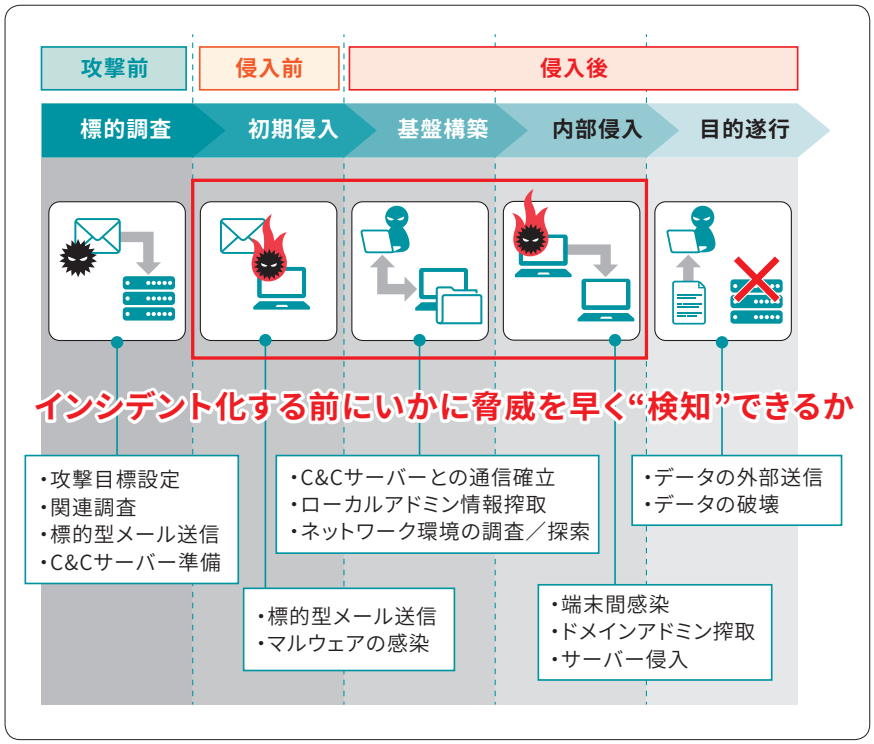
○ 一大ブームを巻き起こしている「EDR」

この事後対策を効果的に実施するには、それを実現するソリューションの活用や日頃からの体制の整備と運用が必要となってくる。なかでも必須となるソリューションとして多くの企業が導入を進めているのが「EDR(Endpoint Detection and Response=エンドポイントでの検知と対応)」だ。

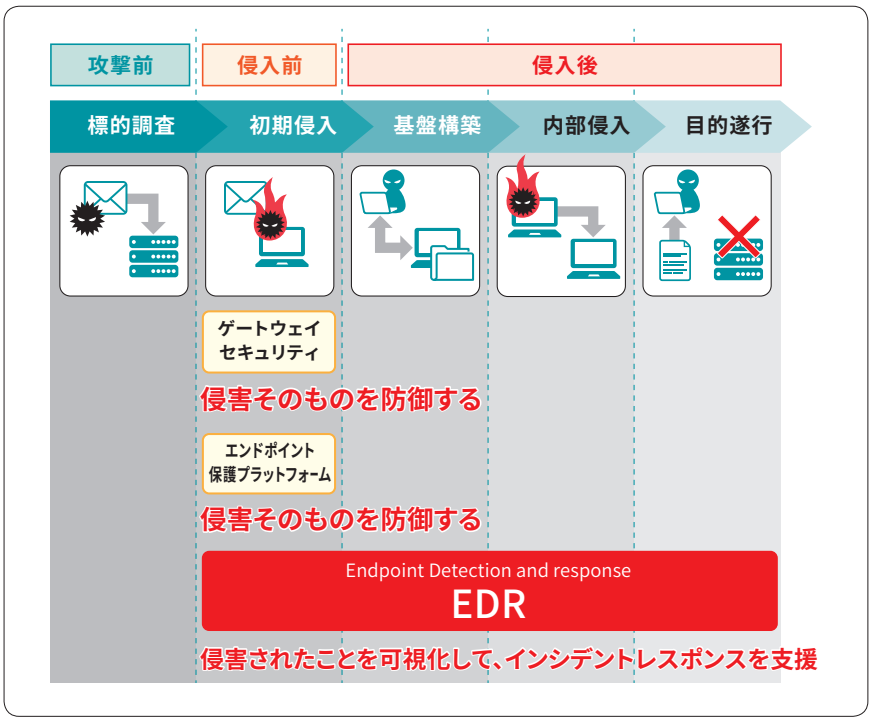
EDRは、PCやサーバーなどのエンドポイントにおける脅威を検知し、インシデントレスポンスを支援するセキュリティソリューションである。エンドポイントの挙動(ログ)の詳細な調査により、既に侵入し潜伏している攻撃者(脅威)の「検知」や、インシデント発覚後の被害実態調査や原因究明といった「対応」を行うことを可能にする。

しかし注意すべきは、EDRというのはアンチウイルスやファイアウォールのように、導入するだけで自動的にサイバー攻撃から守ってくれるようなタイプのソリューションとは一線を画するという点だ。あくまで情報システム担当者やセキュリティ担当者が、インシデントの初動対応や調査のためのツールとして能動的に使いこなすことが前提となっているのがEDRなのである。この点をしっかり理解していなかったため、PoC(実証試験)を実施したものの導入を見送ったり、導入したもののうまく使いこなせなかったりというケースも多いという。

そして近年では“EDRブーム”の様相も呈していることから、各セキュリティベンダーがこぞってEDR製品をリリースしてお



標的型攻撃をモデルにしたサイバー攻撃対策の勘所



サイバー攻撃対策におけるEDRの立ち位置

り、玉石混交状態にある。しかし、前述のようにEDRというのは利用者側がどう使いこなすかが鍵を握るため、製品選びにはほかのセキュリティ製品以上に慎重になる必要があり、検討すべき項目は、EDRを導入する目的や、自社の運用体制、製品の誤検知率、カスタマイズ性など多岐にわたってくる。

本連載では、EDR製品を選ぶにあたり抑えておくべきポイントや、それらのポイントを満たすEDRソリューションにはどのようなものがあるのかなどについて解説していきたい。

第2回 EDRを選ぶとき、絶対に抑えるべきポイント

まずは目的の明確化を

EDRというのはアンチウイルスやファイアウォールのように、導入するだけで自動的にサイバー攻撃から対象を守ってくれるソリューションとは異なり、情報システム担当者やセキュリティ担当者が調査ツールとして能動的に使いこなすことが前提となっている。そのため、社内でEDRをどう使おうとしているのか、最初に目的を明確にしておかないと、“PoC(実証試験)をやってお

しまい”という結果になりかねない。

この目的は企業によってまちまちだが、たとえばCSIRTを設置している企業であれば、設置していない企業以上にインシデントレスポンスを支援するツールとしてEDRの実力が発揮できるだろう。また、フォレンジックや内部監査といったコンプライアンスの遵守、不正防止といった用途にも有効だ。いずれにせよ、どのEDR製品を導入するかの議論以前に、まずは自社のインシデントレスポンスの体制や手順が整っているのかを確認するようにしたい。

どれだけ検知できるか

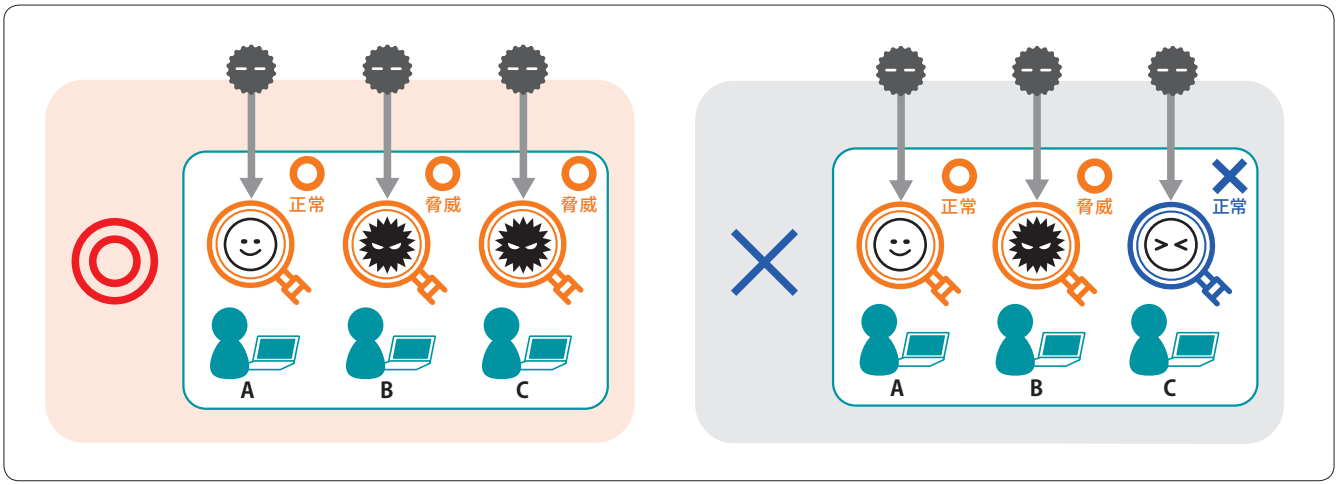
それでは、 いよいよここからが本題。EDR製品を選定する際に必ず抑えておきたい比較ポイントについて解説していこう。

POINT❶ >> 検知力

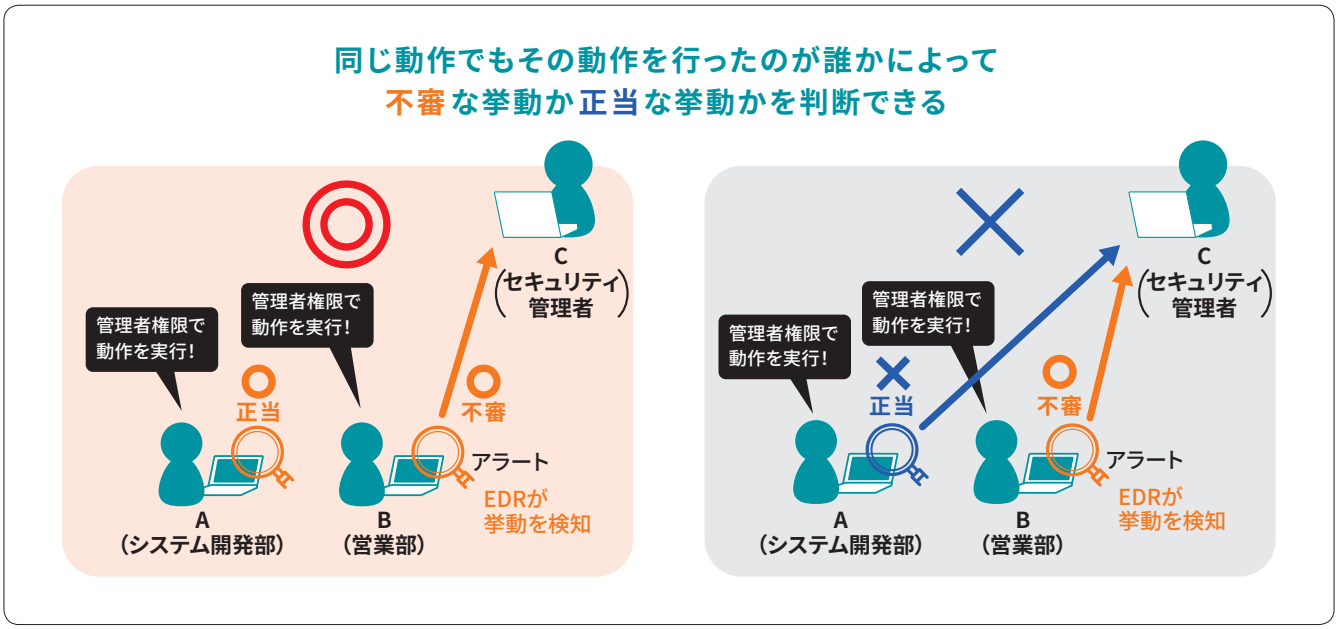
EDRを導入した企業が実際に運用を行うなかでまず直面する課題が「誤検知」だ。

エンドポイントにおける「本当は脅威ではない挙動」までEDRが脅威とみなしてしまい、アラートが頻発してしまうといったケースがその最たる例である。こうなると担当者は調査に追われてしまい、しかも調査してみると脅威ではなかったというケースばかりとなるため、本物の脅威を検知したアラートに対しても「またか」と軽んじて見逃してしまう事態に陥りかねない。EDRが“オオカミ少年”となってしまうのは笑えない話だが、こうしたケースは実際にみられている。

EDRはエンドポイントの挙動を継続的に監視して、そこから一定のルールに沿って「不審な挙動(=脅威の可能性)」を検出する。しかし、 不審な挙動をEDRが検出できな



POINT❶ 通常の挙動を脅威と誤検知することなく、本物の脅威だけを正しく検知する正確性が重要



POINT❷ 動作を行ったのがシステム開発に携わる部門の社員か一般社員かによって、その挙動の正当性を判断できるカスタマイズのしやすさもポイント

かったり、もしくは通常の挙動も含めて何でもかんでも不審な挙動と判断してアラートを出し続けたりしたのでは、そもそもの前提が崩れてしまう。安全な挙動も脅威とみなすタイプの誤検知についてはルール設定との兼ね合いもあるので、その点については後述することとする。

なので、ここではまずEDRがアンチウイルスやファイアウォールといった既存のセキュリティ製品とは異なり、見過ごしてしまった脅威に速やかに対処するためのものであること。それゆえに脅威となりうるあらゆる挙動を検出できる高度な検出エンジンを備え、高い検知力を持つ製品を選ぶということをポイントとしてあげたい。

そして、できればエンジンも1つではなく、複数のものを組み合わせていたほうが、それだけ多角的な解析が行えるため検知率が高まるだろう。さらに、昨今ではAIや機械学習などを用いた検出エンジンも登場してきており、そうした最新のテクノロジーとの組み合わせも重要なポイントとなるだろう。

また、EDRは自社に潜む脅威を可視化して対策を行うためのものであるため、単に検知できるというだけでは十分ではない。なぜ脅威であると判断したのか、その判断理由まで示せることが必要となってくる。

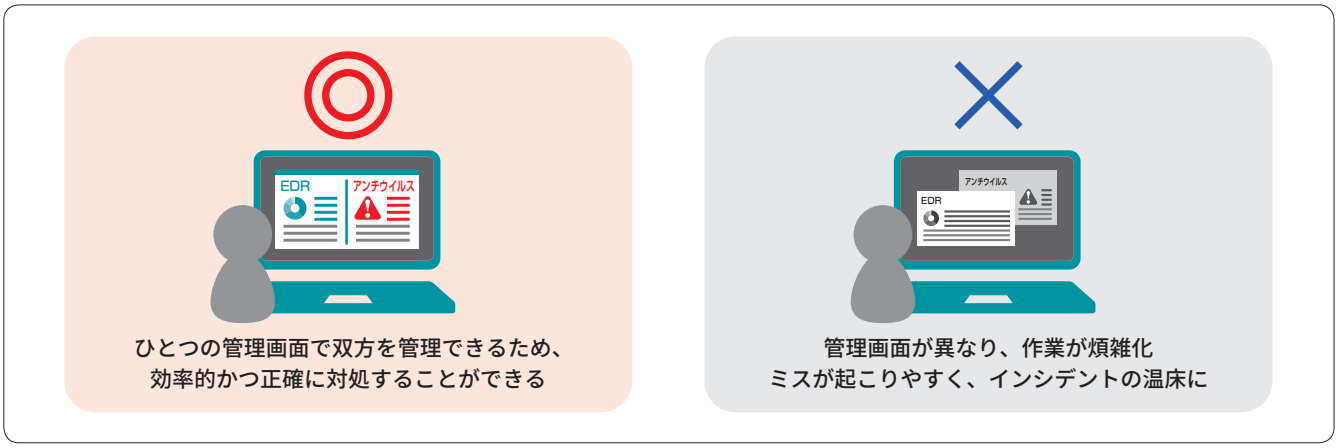
実際の運用を想定して

POINT❷ >>運用性/カスタマイズ性

前述のとおり、EDRはエンドポイントの挙動を継続的に監視して、そこから一定のルールに則り「不審な挙動(=脅威の可能性)」を検出するものだが、検出した挙動を脅威と判定する基準は企業ごとにかなり異なってくる。仮に、【管理者権限で実行ファイルを開く】という挙動があったとして、それはユーザーの意図した「正当な挙動」かもしれないし、もしくはマルウェアなどが引き起こした「不正な挙動」かもしれない。

このように【エンドポイントにおいて管理者権限で実行ファイルを開く】という挙動が検出された際、EDRにはどちらに判断してほしいのかという基準は、企業ごとにまちまちであるはずだ。さらに、営業や企画などの部門では基準のハードルを比較的低く、逆に総務・人事や研究開発などの多くの機密情報を扱う部門ではハードルを高めにといったように、同じ企業であってもルールが異なってくることも多い。

そのため、EDRの導入後には、検知ルールを自社環境に合わせて最適化する作業が必須となるし、運用開始後もそれを継続的にチューニングしていかなければならない。このチューニングやカスタマイズのし



POINT❸ EDRとアンチウイルスを同じブランドの製品で運用することで、効率的かつより高いセキュリティを実現

やすさもEDR製品選びのポイントといえるだろう。

○ 既存製品との共存を考える

POINT❸ ≫ アンチウイルス、アンチマルウェア製品との相性

意外と見落としがちで導入後に問題が生じやすいのがこのポイントだ。いまやほとんどの企業がアンチウイルス製品を導入しているはずだが、こうした製品もEDRと同じくエンドポイントを守るセキュリティ製品であるため、バラバラの製品を導入してしまうと大局的な目的は同じであるのに管理は別々……、という非効率な運用を求められることとなる。

また両者の競合の問題にも配慮する必要がある。アンチウイルスもEDRも多くがシステムの最深部の情報まで取得できるカーネルモードで稼働するため、エンドポイント上で共存した際の影響をしっかり見極めねばならない。 場合によってはシステム自体が強制的にシャットダウンしてしまうといったリスクも想定される。利便性とセキュリティとはトレードオフの関係とよくいわれるが、アンチウイルスとEDRの競合の影響でエンドポイントのパフォーマンスが下がってしまったのでは、エンドユーザーのストレスが高まり、ひいては企業全体の生産性低下をも招きかねない。

こうした共存に関わる問題を避けるには、アンチウイルス製品と同じブランドのEDR製品を選ぶのが得策だ。特にアンチウイルスと連携して動作するようなEDRであれば、問題を避けるばかりか、より高いセキュリティの実現にも寄与することだろう。

このほかにも、コストやベンダーの実績、サポート体制、果てはクラウドかオンプレミスか、など、製品を選ぶうえで抑えておきたいポイントはあるものの、ここでは最も重要かつ見落としがちなもの、そしてEDRだからこそそのポイントにフォーカスさせていただいた。 本連載の最終回となる第3回は、本稿で取り上げた抑えるべきポイントを網羅した「 理想的なEDR製品」たる『ESET Enterprise Inspector』をベンダー担当者の声とともに紹介する。

キヤノンマーケティングジャパン
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
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
西村 亮氏

第３回 数多あるEDR製品の最適解「ESET Enterprise Inspector」

○すべての選定ポイントを満たすEDR製品

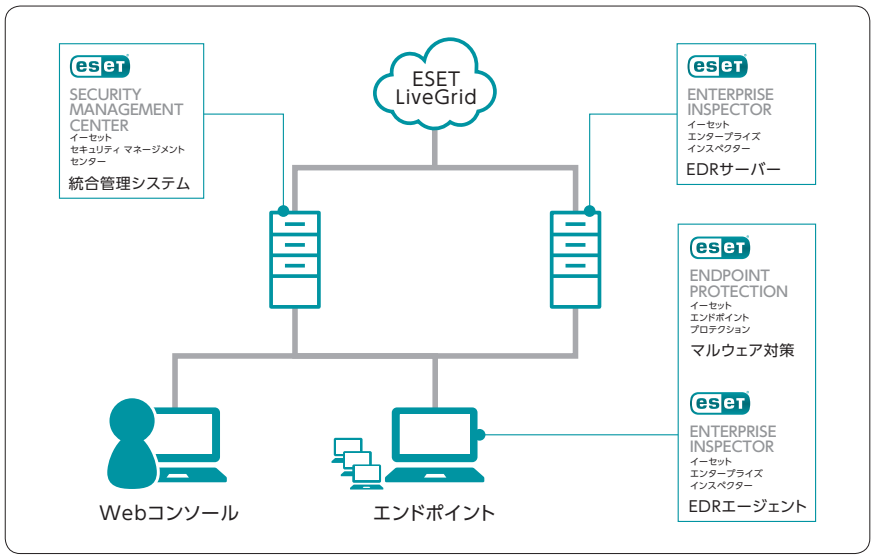
目下さまざまなベンダーからEDR製品がリリースされているが、選定する際には検知力や運用性/カスタマイズ性、既存のアンチウイルス製品との共存性など、抑えるべきポイントがいくつもある(本連載第2回参照)。

そして、抑えたいポイントのすべてを満たすEDR製品が、キヤノンマーケティングジャパン(キヤノンMJ) が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して国内リリースした「ESET Enterprise Inspector (以下EEI)」である。

○ ESETだから誇れる高い検知力

EEIは、ESETのエンドポイントセキュリティ製品と連携して動作するEDR製品となっている。EEIを含めESETブランドの製品には、30年にもおよぶエンドポイントセキュリティの研究によるノウハウが反映されており、世界中の企業、そして第三者機関からも高い評価を受けている。

キヤノンMJ 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 チーフの植松 智和氏はこう話す。「ESETの多層型エンドポイント保護プラットフォームを活かすことができるEEIは、すべてのエンドポイントから大量の関連データを収集しリアルタイムに分析することで、エンドポイントにおけるあらゆる脅威に対する、迅速かつ総合的な防御、検知、対応を支援します」



EEIはローカルのルールだけでなく、LiveGridの評価を組み合わせて脅威を判断するため、常に最新情報での検知を可能とする

EEIは、法人向けESET Endpoint Protectionシリーズ(以下EEP)のバージョン7以降と、統合管理システム「ESET Security Management Center(以下ESMC)」を導入している環境で利用することができる。監視対象とするエンドポイント(PCやサーバー)ごとにライセンスが付与され250ライセンスから提供される。

EEIの特徴のなかで、まず着目したいのは高い検知力だ。EEIは、ESETの多層防御のアプローチにより、サイバーキルチェーンのあらゆる段階の脅威を迅速に検知することができる。その多層防御を構成する要素の1つ「ESET LiveGrid(以下LiveGrid)」では最新の機械学習テクノロジーが活用されている。

LiveGridは、世界中の1.1億台にもおよぶESETユーザーからマルウェアやマルウェアと疑われるファイルを収集するクラウド型システムだ。収集した情報は、20年以上の実績を持つESETの機械学習機能を用いて解析され、正当なアプリケーションかマルウェアかを自動判定する。そこで新たな脅威と認められた場合には、検出エンジンやソフトウェアの安全性評価の結果にその情報が即座に反映される仕組みとなっている。

キヤノンMJ 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の西村 亮氏は「エンドポイント単体で脅威をみるのではなく、そこでも判断しきれなかった疑わしいファイルはLiveGridのクラウド側で解析し判断するという多層構造となっています。脅威かどうかを判断する根拠となる情報の母数が非常に多いため、より正確な判断を行うことができるというのは、EEIをはじめESETブランドの製品全体の強みであると自負しています」とESETだからできる構造的な強みを語る。

さらに植松氏はこう続ける。「当社でEEIを提供するにあたっての技術検証を行っていますが、EDR製品としてのEEIの検知力の高さや誤検知の少なさは特筆に値するといっていいでしょう。ESET社では従来から一貫して『誤検知ゼロ』を目標に掲げており、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※』と評価されています。EEIにも誤検知の少なさが反映されており、それは信頼性の高さにもつながっているのです」

※サイバーセキュリティアワードAV-Comparatives「サマリーレポート2018」より

●シンプルに、やりたいことを実現する運用性

運用性とカスタマイズ性においてもEEIは優れた性能を持つ。EDRはエンドポイントの挙動を継続的に監視して、そこから一定のルールに則って「不審な挙動(=脅威の可能性)」を検出する仕組みを持つが、この脅威と判定する判断基準は企業や部門ごとにまちまちである。

そのためEDRの導入後には、判定ルールを自社環境にあわせて最適化するとともに、その後も継続的にチューニングしていく必要がある。EEIには、このチューニングやカスタマイズが効率的に行えるようさまざまな機能が備わっている。

チューニングの過程について植松氏は次のように説明する。「EEIを導入したばかりの頃は数多くのアラートが生じることでしょう。そこで個々のアラートの内容をみていくと、ちゃんと脅威として検知した理由が詳しく記述されているので、セキュリティ担当者はそれをみながらこれは正常な動作だからアラートは必要ないなどとワンクリックで設定していけるようになっています」

たとえばリモートワークを推奨している部門やチームであれば、【リモートワークで使用している端末による外部からの接続に対しては、特定のアラートを上げないように調整する】といった具合である。こうして企業ごと、部門ごと、さらにはチームごとなど、それぞれの特性に応じたチューニングが、EEIであれば容易に行えるのである。

「当社では、お客さまの事情にあわせたEEIの最適化から実運用が軌道に乗るまでの支援も行っています。最終的にはお客さま自身がルールを設定していけるまで、しっかりとサポートします」(植松氏)

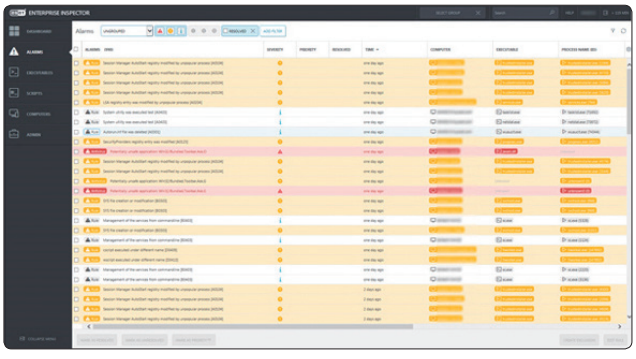
「セキュリティ運用の自動化という機運も一部ではありますが、完全に機械任せにしてしまうと、それがブラックボックス化してしまい、何が行われているかわかりません。EEIであれば脅威ではなく正常な可能性までもその根拠として示してくれるので、より適切な判断が行えるようになります」(西村氏)

さらに、EEIには多角的な切り口でダッシュボードが用意されているなど、セキュリティ担当者が求める結果を追いやすいよう直感的なUI設計がなされている。

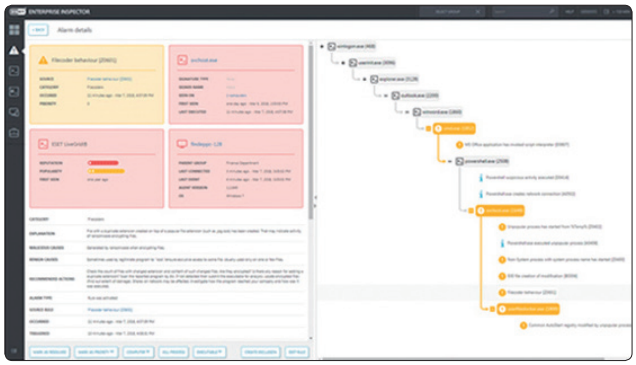
これに関し植松氏は「EEIのダッシュボードでは、アラート単位や実行ファイル単位、コンピュータ単位など、さまざまな視点から解析を行うことができます。『管理者がやりたいことをシンプルに実現できる』ようにデザインされたEDRがEEIなのです」と力説する。

●アンチウイルスとの連携でより高度なセキュリティを実現

EEIはアンチウイルス機能を持つEEPシリーズと連携して稼働するよう設計されているため、脅威を包括的に防御し可視化することができる。EEIでは、監視対象のエンドポイントに、ESMCを使った一括配布などによりエージェントをインストールする。このEEIエージェントはEEPと連携動作し、カーネルモードで動作するEEP(センサー)が収集したプロセス情報などをサーバーに転送する仕組みとなっている。EEIエージェ



ワンクリックで設定可能なアラートの一覧画面



各アラートの詳細を示すProcess Tree

どによりエージェントをインストールする。このEEIエージェントはEEPと連携動作し、カーネルモードで動作するEEP（センサー）が収集したプロセス情報などをサーバーに転送する仕組みとなっている。EEIエージェントは主に転送処理を担うため軽量で、さらにユーザーモードで動作するので、エンドポイントのシステムに影響を与えるリスクも低い。

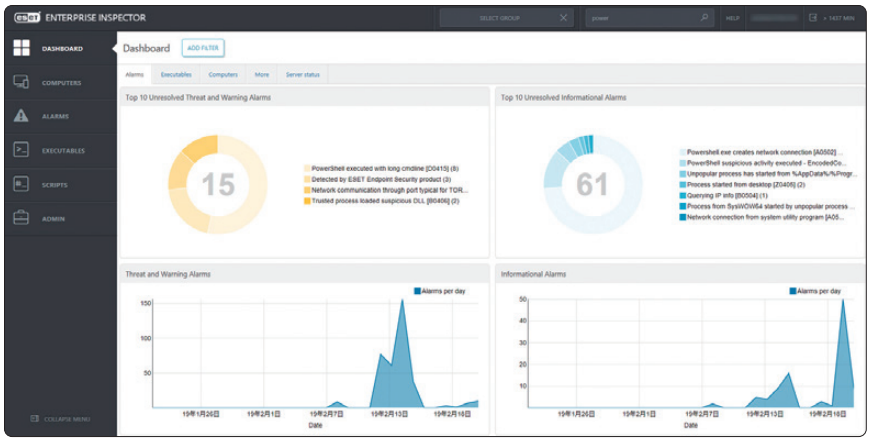
「EEPでマルウェアを検知した際には、その情報はEEIにも伝えられるため、検知後の被害調査なども迅速に行えます。またESMCから統合管理できるため、EEIの導入によって管理ツールが増える心配も不要です。そしてEEIの管理コンソールは、すでにEEPに触れているセキュリティ担当者であれば直感的に使えるデザインとなっています」（西村氏）

ESETシリーズにおけるEEIの役割と今後の展望

キヤノンMJとしては、EEIを軸にESETブランドのさらなる展開を図っていく構えだ。

「自社だけでは運用が難しいというお客さまには、マネージドサービスとしてのEEIの提供も検討しているところです。包括的なエンドポイントのセキュリティについては、ぜひ当社にお声がけいただければ、きっと期待に応えてみせます」――植松氏は力を込めて宣言した。

さて、「EDRまるわかりガイド」と題し、3回にわたる連載形式でEDRについて必要な情報を紹介してきたが、いかがだっただろうか。情報セキュリティ対策はもはや次のステージへと進んでおり、そこではEDRのようなツールの活用が欠かせないことがおわかりいただけたのではないか。何から手をつければいいのかわからない、そんな場合であっても決して躊躇する必要はない。まずはキヤノンMJに相談してみていただきたい。



ESETユーザーであれば“お馴染み”のWebコンソール

第4回 アップデートでさらなる機能強化を果たした「ESET Enterprise Inspector」

事前対策と事後対策を統合したセキュリティ対策をデザイン

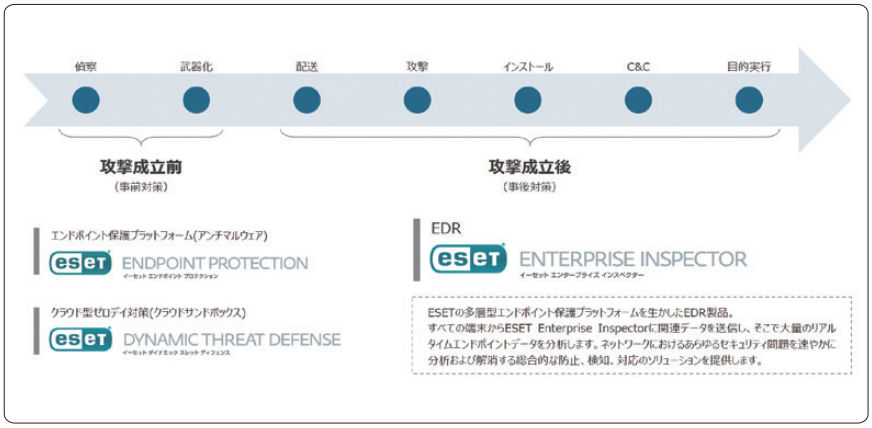
幅広いエンドポイントセキュリティ製品をラインアップしているESETシリーズは、30年にもおよぶ歴史のなかでさまざまな研究を積み重ねており、その成果がEEIにも反映されている。だからこそ、世界中の企業や第三者機関から高い評価を受けているのだろう。では、新型コロナウイルスの感染拡大による社会の変化には、どのように対応しているのだろうか。

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商品企画部 課長代理の植松 智和氏はこう話す。「コロナ禍を受け、多くの企業では在宅ワークをはじめとしたテレワークを導入するなど、1年ほどの間に大きな変化が起きています。このため以前であれば自社ネットワークの外側から内部へと向けた攻撃を重点的に防御すればよかったのですが、いまや保護すべき対象は自社の境界内部に留まらず、社外にも守るべき資産が存在しています」

ESET製品では、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盤として「ESET Endpoint Protection シリーズ（以下EEP）」という製品があり、攻撃を成立させないことをコンセプトとした防御を行う（事前対策）。一方、EEIでは、エンドポイントのあらゆるイベントを集約・分析することで、EEPだけでは発見しづらい脅威の検知や封じ込めなど、攻撃成立後の対処をコンセプトとしている（事後対策）。つまり、両製品を組み合わせることで、事前・事後どちらの対策もより強固なものとなるのだ。

コロナ禍でテレワークが定着しつつあるなか、従来の「境界防御」では防ぎきれない攻撃が浮き彫りになっている。そのような現状において、エンドポイントを守るためのセキュリティ強化として、両製品の活用はとても有効と言えるだろう。

植松氏も「EEPとEEIを組み合わせることで、幅広い領域を防御可能とする、事前対策と事後対策を統合したセキュリティ対策をデザインできることは、ESET製品の強みだと自負しています」と語る。



運用性とカスタマイズ性の高さもEEIの魅力

EEIがほかのEDR製品と比べて優れている点は多々あるが、高いレベルの運用性と柔軟かつ容易なカスタマイズ性はその代表的なものと言える。エンドポイントの挙動を継続的に監視して、そこから一定のルールに則って「不審な挙動(＝脅威の可能性)」を検出するのがEDRだが、ある挙動を脅威と判定するか否かの判断基準というのは、企業ごと、さらには部門ごとに異なってくる。そのためEDRの運用にあたっては、脅威を判定するルールを自社環境に最適化したうえで、そのあとも継続的にチューニングしていく必要があるのだ。

このチューニングやカスタマイズを効率的に行えるよう、さまざまな機能を有しているのがEEIである。たとえばEEIからあがってくる個々のアラートの内容をみていくと、なぜ脅威として検知したのか、その理由が詳しく記述されている。この情報をもとに、セキュリティ担当者は個々のアラートについて、きっかけとなった動作に応じた挙動をワンクリックで設定していくことができる。加えてEEIは、企業ごと、部門ごと、さらにはチームごとなど、それぞれの事情に応じたチューニングも容易に行える。キヤノンMJでは、こうした導入先の事情に合わせたEEIの最適化をはじめ、実運用が軌道に乗るまでの支援も行っており、最終的には自社だけでルールを設定していけるよう手厚いサポートを提供している。

新バージョンで加わる数々の新機能

2021年2月26日より提供を開始したEEI V1.5ではさまざまな新機能が加わっているが、そのひとつとなるのが「ターミナル(Remote PowerShell)機能」の実装である。これにより、Webコンソールから端末に対してRemote PowerShell経由でアクセスし、PowerShellコマンドを実行することが可能となった。侵害端末の調査や修復、重要情報の保全などが、担当者が利用現場に直接出向くことなく、さらにはユーザーの業務利用を止めることなく、リモートで実施できるようになったのである。キヤノンITソリューションズで技術検証にあたる西村亮氏は「EDRとしての機能に加え、Windowsの強力なPowerShellを用いることにより、よりきめ細やかに対応できるようになりました。これにより、侵害などが発生した場合の速やかな対処や、さまざまな調査がEEIの管理コンソール上だけで実現できるようになっています」と語る。

もうひとつの大きな機能追加はMITRE社が開発しているセキュリティに関するナレッジベース「MITRE ATT&CK Framework」のリファレンスを、コンソール上に表示される検出アラートのリンクからワンクリックで参照可能となったことだ。リファレンスは攻撃に使われたテクニックの詳細について解説されているため、状況の把握とそのあとの対応について、迅速かつ的確な判断を促せるようになる。

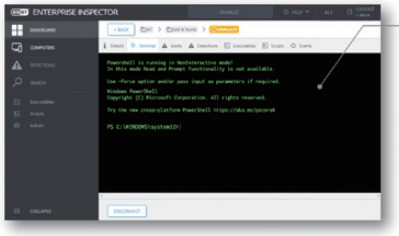
そして最後に紹介するのが、Googleが運営するウイルス判定サイト「VirusTotal」もしくはサードパーティーのソースに対し、ハッシュ値を用いたカスタムリンクを設定可能となったことだ。「EEIでももちろん、ハッシュ値によるブロックや、プロセスの強制停止をワンクリックで実施可能です。サードパーティーのソースを利用することで、ファイルをブロックする根拠をより明確にすることができます」と西村氏は語り、外部ナレッジの活用に期待を込めた。

ほかにも新バージョンでは外部連携も強化されており、REST APIによる外部連携によってアクションの自動化が可能となるとともに、RSET APIを介してEEIそのものの運用自動化もサポートする。「こうしてルールベースで自動化することによって、貴重な人間による手間をおさえつつ、速やかな対処が可能になっています」と西村氏は語る。

デモ画面にみる、正規ツールであってもグレーな挙動に警告

ここでEEIのコンソール上にアラートが表示された際の対処法を知るべく、実際の画面をみてみよう。

西村氏はEEI V1.5のデモ画面を操作しながら「EEIのコンソールが、直感的なUIとなっているため、ある程度のセキュ



リモートからのライブレスポンスをサポート

- 詳細調査のための情報取得
- システムのイベントログ取得
- 重要ファイルのバックアップ
- 攻撃者が生成したファイル等の削除
- 攻撃者が変更したレジストリキーの復旧　など

ライブレスポンスとは？

- コンソールへ直接接続してコマンドやツールを実行し、システムを稼働させたまま情報収集を行う手法
- 主にメモリ上に展開されているプロセス、ファイル、レジストリ、ネットワークなどの揮発性の情報取得に使用する

- リモートからエンドポイントへ直接接続してインシデントレスポンスが可能
- ユーザーのワークフローを止めることなく、侵害端末へのきめ細かな対応が可能
- 同一の管理コンソールからリアルタイムで調査・対応・修復を実施できる

EEIの検出アラートから、攻撃に使用されたテクニックの詳細を参照可能

ESET ENTERPRISE INSPECTOR　MITRE ATT&CK

VirusTotalにハッシュ値を用いたカスタムリンクを設定可能

ESET ENTERPRISE INSPECTOR　VirusTotal

リティ知識があれば、アラートに対する的確な操作が容易にできます。V1.4を利用しているユーザーがこの画面を一見すると、ユーザーからみたときの画面上にそれほどの変化はないかもしれませんが、その内部で取れるイベントが増えていて、検知性能の向上につながっています」と説明した。

次に、Officeアプリからスクリプトインタープリターが呼ばれたことを検出した際のアラート画面をみていく。まずは情報確認のためプロセスツリーをみてみると、エクスプローラーからWordを実行し、コマンドプロンプトからPowerShellを実行している。次にPowerShellでは2つのアラートが上がっているので内容を確認すると、実行ファイルが2つあって、最終的にスケジューラーのタスクが実行されていることがわかる。

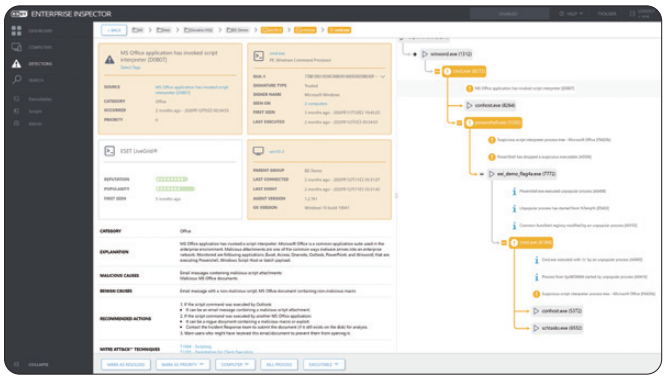
「EEIでは、アラートの危険度によって表示するときの色をわけており、悪質で危険な挙動の場合は赤色のアラートで表示されます。しかし、このデモ画面ではいずれも赤色ではなく黄色のアラートとなっているのがおわかりいただけるかと思います。黄色は完全に危険というわけではないグレーな領域を指しており、Officeアプリのような正規のツールであっても、グレーな挙動を検出できるのがEDR製品の強みと言えます。特に最近のサイバー攻撃では、正規ツールを使うことでマルウェア検知を逃れるという手法が増えていますので、非常に有効と言えるでしょう」と西村氏は語る。

このように、EEIの管理画面ではわかりやすい操作性はもちろん、脅威に関する情報について、一貫して同じ画面で確認することができる。さらに、同じくESET製品であるEEPとも連携しているので、EEPで検出したマルウェアなどの情報も確認することができ、ここでも管理者の手間を省くことができるようになっている。

ここまでコロナ禍における事前・事後対策の重要性と、その対策において効果を発揮するEEIについて、運用性やカスタマイズ性、そしてまもなく提供開始される新バージョンの機能追加について紹介してきた。

植松氏は最後に「バージョンナンバーでは一般的に言うところのマイナーバージョンアップかもしれませんが、最新版ではメジャーバージョンアップと言っていいほどのかなりの機能強化を行っています。EDRという製品自体が比較的新しく、脅威も日々更新されていますので、不審な挙動に対する検出機構などもそうした変化に対応してアップデートすることが欠かせないからです。今後もバージョンアップの際には、最新のセキュリティトレンドに対応した数多くの新機能が搭載されていくことでしょう」と今後も変化する状況に対応していく姿勢を語ってくれた。

新たな生活様式へと変化するなかで、さまざまな脅威が新たな手法で攻撃を続けている。これからもEEIはそうした攻撃に対応し、さらなるバージョンアップをしていくことだろう。コロナ禍においてセキュリティ強化を図ろうと検討している方は、ぜひキヤノンMJに相談してみてはいかがだろうか。



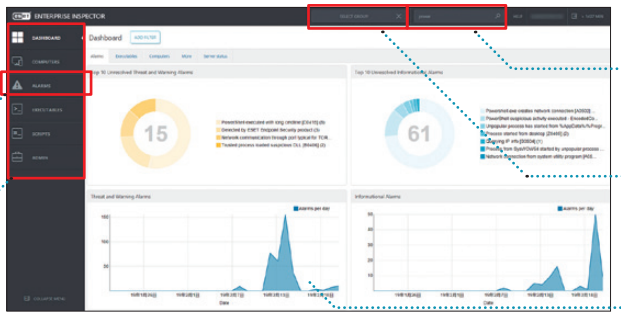
※第1〜4回の記事はマイナビニュースに連載した記事を再編集したものです

潜む脅威を速やかに発見し対処する

組織内の端末から収集したさまざまなログ情報をもとに、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る EDR 製品です。

- 疑わしいファイルや悪意ある挙動を可視化
- 迅速なインシデントレスポンスを支援
- 柔軟なルール・フィルタ設定による誤検知抑制

ESET Enterprise Inspector
画面イメージ



【ALARMS】
クライアントで検出されたアラームが表示されます。

【メインセクション】
操作可能な各種メニューが表示されます。

【簡易検索ツール】
コンピューター名、実行ファイル名、スクリプトなどをキーに検索することができます。

【SELECT GROUP】
グループやコンピューターを選ぶことで集計対象、範囲を絞り込むことができます。

メインセクションやタブで選択したものに応じて、メイン画面が切り替わります。アラーム情報など、各種情報が表示されます

■ 価格表

ESET Enterprise Inspector

ライセンス数	企業向け		教育機関向け		官公庁向け	
	新規・追加	更新	新規・追加	更新	新規・追加	更新
250 - 499	¥2,840	¥1,990	¥1,420	¥995	¥2,130	¥1,493
500 - 999	¥2,610	¥1,830	¥1,305	¥915	¥1,958	¥1,373
1,000 - 1,999	¥2,370	¥1,660	¥1,185	¥830	¥1,778	¥1,245
2,000 - 4,999	¥2,130	¥1,490	¥1,065	¥745	¥1,598	¥1,118
5,000 - 9,999	¥1,900	¥1,330	¥950	¥665	¥1,425	¥998
10,000以上	応相談					

- ライセンス数は、インストールするクライアントおよびサーバーの台数でカウントします
- 新規購入は250ライセンスから、追加購入は1ライセンスからお求めいただけます
- 追加ライセンスの価格は、すでに導入しているライセンス数に追加ライセンス数を加えた合計ライセンス数の価格ゾーンが適用されます

■ ESET Enterprise Inspectorの利用には、下記いずれかのエンドポイント保護プログラムの導入およびESET Security Management Centerによる管理が必要です。
・ESET Endpoint Security(V7)　・ESET Endpoint アンチウイルス(V7)　・ESET File Security for Microsoft Windows Server(V7)

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

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

●お求めは信用のある当社で

2021年4月現在

MEEI2104CMJ-PDF