@IT Special

FIREEYE™

“アラート疲れ”に悩むEDRの運用現場から

エンドポイント対策製品の選び方―― “脅威インテリジェンス”がカギとなる

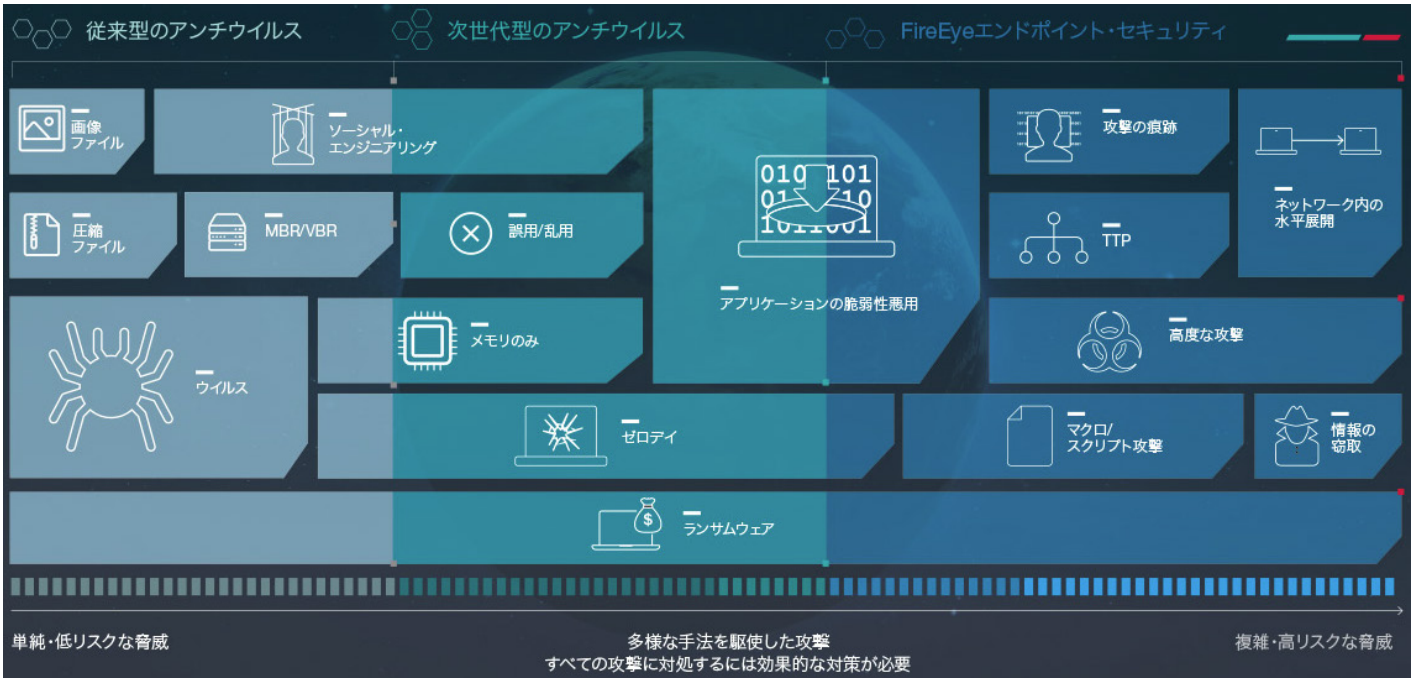
重要性が増すエンドポイントのセキュリティ対策。だが、多過ぎるアラートに疲れていないだろうか？　本稿ではエンドポイント・セキュリティ対策の選び方を解説。ベンダー選びで注意をしたい 3 つのポイントを紹介しよう。

ビジネスにおいて IT の価値が高くなるにつれて、サイバー犯罪者にとっても IT システムやデータを攻撃する動機が強くなっている。デジタルトランスフォーメーションや働き方改革などの取り組みが進み、IoT（モノのインターネット）や AI（人工知能）など IT の活用シーンが増えるほどに、サイバー攻撃を受ける恐れも増すということだ。いっそうのセキュリティ対策強化が求められる。

エンドポイント（端末）は、ユーザー自身が実務をこなし、貴重なデータにアクセスする場所であることから、特に狙われやすい。

こうした状況では、旧来の “ 社内でがっちり守られたネットワーク向けのセキュリティ対策 ” では、IT 資産を十分に保護できないことは明らかである。また、ターゲットに最適化された標的型攻撃が主流となった現在では、パターンファイルをベースとした汎用（はんよう）的な保護も力不足だ。さらに侵害が発生した場合に「正しく復旧する」ことも難しい。そこで復旧に役立つ新しい対策手法として「EDR（エンドポイント ディテクション&レスポンス）」の導入が進んでいる。

ただし、EDR も他の多様なセキュリティ対策と同様に、導入後の運用が非常に重要だ。人材不足の課題に悩まされている中で、適切な運用を行うためにはどうすればよいのだろうか。どのような技術やソリューションが必要なのだろうか。



従来型アンチウイルス（左）が単純かつ低リスクな不正ファイルの検知にフォーカスしているのに対し、EDR（右）は侵入後の水平展開や痕跡調査など、より高度な攻撃への対応にフォーカスしている

“アラート疲れ”に悩むEDRの運用現場

貴重な情報やデータにアクセスするエンドポイントは、サイバー犯罪者にとって金鉱脈のようなものである。最近では、しっかりと固められた境界の外部で端末を利用することも多い。逆に境界内部であれば安全だろうと過信して個々のセキュリティ対策がおろそかになっている場合も少なくない。さらに、ユーザーのリテラシーが向上せず、ヒトが脆弱（ぜいじゃく）性となっている可能性も高い。サイバー犯罪者にとって、エンドポイントとはちょっと“掘る”だけで金を得られる、費用対効果の高い領域と捉えられているのだ。

エンドポイントを保護する施策として、長くアンチウイルスツールが活用されてきた。これらのツールでは、ウイルスが持つ特徴をパターン化して、マッチしたものを排除するという手法が採られてきた。だが、すでに最新のサイバー攻撃に対して十分に保護できないことが知られている。

そこで注目されているのが、EDR である。ソフトウェアの“不審な挙動”の検出と調査に焦点を当てた技術だ。ありていに言えば、怪しい動きをするものを全て危険な可能性があると見なし、脅威の取りこぼしをなくしているのだ。

しかし、その結果、EDR が出力するアラートがどうしても増えてしまう。アラートが上がれば精査しなければならないため、管理者に高い負荷がかかっているのが現状だ。運用で疲弊してしまった結果、アラートを無視したり、設定を変えてアラートが出ないようにしてしまったりするケースも少なくない。これでは本末転倒である。

では、EDR のアラートをどのように生かすべきなのか。どのような運用をすべきなのか。この課題に対する答えはこうだ。「脅威インテリジェンスが重要な鍵を握る」。

EDRを生かすのは脅威インテリジェンス

EDR では侵害の影響範囲を調べ、どの程度に深刻なのかを把握して、効率よく対処することが必要である。つまり、検知した脅威について、どれほど深い関連情報を把握できるかという点が非常に重要な要素となる。この“情報の深さ”を担うのが、脅威インテリジェンスだ。

セキュリティ市場では、IP アドレスやドメインなどのレピュテーション（信頼性情報）やパブリックドメインのものなど、さまざまな脅威インテリジェンスが流通している。EDR ソリューションを選定する際には、そのソリューションがどのような脅威インテリジェンスと、どのように連携しているのかがポイントとなる。

具体的には、

1. どのようなセキュリティ対策情報がまとめられているのか
2. どのような情報を収集しているのか
3. どのような情報収集、分析、活用のプロセスを採用しているのかという点に注目したい。

各社が提供している脅威インテリジェンスの中には、情報が浅かったり、他社から購入したりしているものもある。一方、あるベンダーは、被害者の情報と攻撃者の情報、デバイスから収集された情報を総合的に組み合わせたものを“脅威インテリジェンス”と呼んでいる。

一般にインテリジェンスは 2 種類に区分される。公開情報の“オシント”と人間同士の接触から得られる“ヒューミント”だ。先ほどのベンダーはヒューミントを得意としているといえるだろう。

エンドポイント対策における脅威インテリジェンスでは、機器が取得する「IoC（Indicators of Compromise）」――すなわちセキュリティ侵害の痕跡や証拠の中に、管理者にとって有益で正しい情報がどれほど含まれているのかが重要である。

EDR ソリューションの導入で確認すべき 3 つのポイント

1. **脅威の判定**にはどのような情報を使っているのか
2. 脅威インテリジェンスを**どのように入手**しているのか
3. EDR の導入で、**セキュリティ運用がどのように変わるのか、効率化**されるのか

一般的な EDR ソリューションの中には、AI やパターンマッチングで攻撃の痕跡を分析して、アラートを上げるものもある。この手法では脅威に関するデータベースが少ないときに類推による情報が含まれてしまい、結果として必要以上のアラートを出力してしまう。言ってみれば、「怪しい動きをする人物は全て万引き犯かもしれない」と捕まえてしまうようなものである。この場合、誤認逮捕を防ぐため、一度声を掛けた「不審者」に対して全て取り調べを行い、本当の犯人かどうかを識別する作業が必要となる。

先進的なベンダーの脅威インテリジェンスでは、非常に多くのデータを取得しており、脅威の振る舞いに関するあらゆる情報を保持している。つまり、先の例えで言えば万引き犯（犯罪グループ）の行動に関する膨大な情報を保有し、そのデータから、確実に問題のある人物だけをピックアップすることが可能になるのだ。

エンドポイントに話を戻せば、その結果、脅威として断定するための詳細な条件を情報として持つことになり、本当に重要な脅威のみを検出でき、適切なアラートだけを出力できる。これが運用管理負荷の軽減につながる。

「かもしれない」検出を可能な限り排除し、本当に危険な脅威のみをしっかり見分ける、いわば「誤認逮捕を生まないシステム」といえるだろう。

ヒトも機械も最大限に活用する、EDR と EPP の両方を包含したファイア・アイのエンドポイント対策

ファイア・アイの提供するエンドポイント・セキュリティは、EDR と EPP（Endpoint Protection Platform）の両方の機能を包含する包括的エンドポイント対策だ。既知の脅威に効果的な“パターンマッチング”、エクスプロイトの挙動を発見する“振る舞い検知”、そして専門家（Mandiant チーム）による優れた“脅威インテリジェンス”をベースとする侵害インジケーターなど、複数レベルの対策を組み合わせている。また最新技術として、ファイア・アイの専門知識に基づく機械学習をベースとした保護エンジン「MalwareGuard」を搭載、パターンマッチングだけでは検出できない未知脅威の検出にも対応している。

ファイア・アイの Mandiant チームは、企業のインシデントレスポンスの現場から得られた攻撃者に関する情報を脅威インテリジェンスとして蓄積。さらに攻撃者のコミュニティーからの情報も得ているという。加えて言語学者などの、一見するとセキュリティとは無関係な専門家も加わっているところがユニークで、広範囲な情報ソースを基に脅威インテリジェンスを作り上げていることが分かる。

「Mandiant をはじめとするヒトの要素を重視しているのが、ファイア・アイの特色です。他のセキュリティベンダーやセキュリティソリューションと比べて、はるかに多くの脅威情報を保有しているのです。当社の EDR は、この優れた脅威インテリジェンスが源となって、エンドポイントを的確かつ効率よく保護できます」（ファイア・アイの技術本部 シニア グローバル ソリューション アーキテクトの中川和芳氏）

ファイア・アイの脅威インテリジェンス

●お問い合わせ
ファイア・アイ株式会社
https://www.FireEye.jp/ | Japan@fireeye.com

東京オフィス	〒101-0054 東京都千代田区神田錦町 3-22 テラススクエア 8F	Tel. 03-4577-4401 Fax. 03-4577-4410
名古屋オフィス	〒450-0002 愛知県名古屋市中村区名駅 4-6-23 第 3 堀内ビル 9F	Tel. 052-589-7037 Fax. 052-589-7001
大阪オフィス	〒541-0041 大阪府大阪市中央区北浜 1-1-27 グランクリュ大阪北浜 301	Tel. 06-6121-3096 Fax. 06-6228-7155

※この冊子は、@IT（https://www.atmarkit.co.jp/）に 2019 年 6 月に掲載されたコンテンツを再構成したものです。
https://www.atmarkit.co.jp/ait/articles/1906/27/news006.html