トピックス

テレワーク時代のサイバーセキュリティ
―エンドポイントセキュリティの重要性―

日々巧妙化するサイバー攻撃を前に、企業はその対策に追われている。また今後、テレワークが伸展すると見られることから、社内ネットワークの外に持ち出される端末機器（エンドポイント）への対策が急がれる。本稿では、近年注目されているソリューションの紹介を通じて、エンドポイントセキュリティの重要性について解説する。

NRIセキュアテクノロジーズ サイバーセキュリティサービス事業本部
ITセキュリティアナリスト
林（はやし）　吟志（ぎんじ）
専門はサイバーセキュリティソリューションの企画・開発・運用

昨今のサイバーセキュリティ事情

独立行政法人情報処理推進機構（IPA）は2018年4月に発表した「情報セキュリティ10大脅威 2018」の中で、2017年におけるサイバーセキュリティの脅威を、個人と組織に分けてそれぞれ1位から10位まで順位付けしている。組織について見ると、1位が標的型攻撃による被害、2位がランサムウェア（身代金要求型不正プログラム）による被害となっている。

標的型攻撃は、特定の個人にメールを送り付け、マルウェアを仕込んだ添付ファイルを実行させたり、仕掛けを施したWebページへ誘導したりして、個人情報や機密情報を盗むことを目的とする。ランサムウェアもメールが主な感染源になっており、本文に記されたURLのクリックや、改ざんされたWebページの閲覧によりマルウェアに感染させるが、ランサムウェアの目的はPC内のデータを勝手に暗号化し、それを解除するための身代金を払わせることである。

これらの脅威に対抗するために、企業が主要な対策としているのがEPP（Endpoint Protection Platform）と呼ばれるソリューションの導入である。EPPの目的は、エンドポイントでのマルウェアの実行や被害を食い止めること、いわば水際のセキュリティ対策である。そのために、EPPは既知のマルウェアのパターンに基づく「シグネチャー型検知」や、正常でない動作を検出する「振る舞い解析」の機能を備えている。しかし、マルウェアの数の増加や、さまざまな亜種の出現に、「シグネチャー型検知」で追い付くことが困難になっている。さらに、近年はエンドポイントに活動の痕跡を残さないファイルレスマルウェアが登場しており、これを「振る舞い解析」で検知することは困難である。

エンドポイントの対策には、「働き方改革」の一環として今後拡大していくはずのテレワークも大きく影響する。企業のセキュリティ対策では、基本的に出口と入り口の対策に重点が置かれ、ファイアウオールやプロキシといったゲートウェイ型のセキュリティ機器によって安全な業務環境を実現するのが一般的である。ところが、テレワークではエ

レポートに掲載されているあらゆる内容の無断転載・複製を禁じます。すべての内容は日本の著作権法及び国際条約により保護されています。
Copyright © Nomura Research Institute, Ltd. All rights reserved. No reproduction or republication without written permission.

ンドポイントが社外に拡散するため、これまでの出口対策、入り口対策ではカバーできなくなることが予想される。例えば、社外で利用されるエンドポイントでセキュリティ事故が発生した場合、これまでのやり方で影響調査や対策を行うだけでは不十分のはずだ。

以上の理由から、今、エンドポイントセキュリティの再検討が求められている。

表1　EDRに求められる能力

検知能力	・従来型のマルウェアを検知できること ・機械学習技術など未知マルウェアの検知が行えること ・マルウェアが行い得る不審な挙動を検知できること
記録能力	・エンドポイント上のイベントを漏らさず、長期間取得できていること - ファイル作成・削除・読み・書きなどのディスクオペレーション - プロセスの実行、停止 - サービスの登録や実行、停止 - ネットワークアクティビティ - レジストリ操作 - ユーザーログオン・ログオフ - コマンドプロンプト、PowerShellの実行内容
調査能力	・調査方法が容易であること ・調査処理、レスポンスが高速であること ・調査対象のイベント保持期間が十分にさかのぼれること

次世代のソリューションEDR

近年、次世代のソリューションとして注目を浴びているのがEDR（Endpoint Detection and Response）である。NRIセキュアテクノロジーズ（以下、NRIセキュア）では、これまでさまざまなベンダーのEDR製品について評価・検証を行ってきた。ここではその経験から得られたノウハウを基に、EDRに求められる能力や、EDR製品が持っている能力について解説する（表1参照）。EDRの評価ポイントとしては運用の容易性なども挙げられるが、ここで挙げる項目はEDRをまさにEDRたらしめている重要なポイントである。

(1) 検知能力

前述の通り、企業ではEPPがエンドポイントにおけるセキュリティ対策の中核を担ってきた。従って、そこにEDRを導入する場合は、既存のEPPとの競合問題や、重複して発生するコストの問題を解消する必要がある。EDRがEPPと同等かそれ以上の検知能力を持っていれば、EDRをEPPの代替として導入することもできる。実際、EDR製品の中には、近年注目を浴びている機械学習エンジンを採用したりして、EPP以上の検知能力を有するものもある。なお、検知能力を比較する際は、マルウェアに対する検知率の高さに加えて、高度な手法を駆使して行われるサイバー攻撃の一連のプロセスで、その挙動をどれだけ多く確実に検知できるかという点が重要である。

(2) 記録能力

エンドポイントで日々発生するイベントを、漏らさず、長期間記録できる必要がある。エンドポイントで何が起きたかについての情報収集は従来のフォレンジック（証拠調査）ソリューションでも難しく、ベンダーが機器を回収した上で、専門家が専用ツールを用いて長時間かけて解析することでようやく可能となっていた。EDRは、この情報収集を格段に容易にする。長期間の記録が必要なのは、潜伏期間が長期に及ぶマルウェアがあるからだ。

EDRの記録能力は、ファイルレスマルウェ

レポートに掲載されているあらゆる内容の無断転載・複製を禁じます。すべての内容は日本の著作権法及び国際条約により保護されています。
Copyright © Nomura Research Institute, Ltd. All rights reserved. No reproduction or republication without written permission.

アの検知において強みを発揮する。ファイルレスマルウェアは、バイナリファイル（2進数のみで書かれたファイル）を用いず、簡易プログラミング言語によるスクリプト（機械語への変換なしにソースコードを実行できるプログラム）や、OS（基本ソフト）標準のコマンドを使用することで検知を回避する。EDRでは、スクリプトやOS標準コマンドの実行内容も詳細に記録でき、それが悪性かどうか判断することができる。ファイルレスマルウェアの迅速な検知と対処は、従来のソリューションに対するEDRの優位点である。

(3) 調査能力

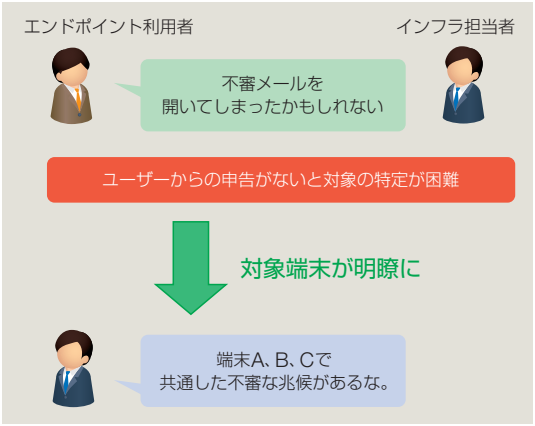
セキュリティインシデントが発生した際、エンドポイントで記録した情報を迅速に、容易に調査できることが重要である。調査には、深掘り調査、水平調査の2つの観点がある。深掘り調査では、エンドポイントで何が起きているのか、迅速な対処が必要な深刻なイベントかどうかを見極める。水平調査では、感染している危険なエンドポイントが他にもあるのかを調査する。

EDRの調査能力は、ランサムウェア対策として顕著である。ランサムウェアは、進入を許したエンドポイントを起点として他のエンドポイントに爆発的に感染が広がるという特徴がある。EDRではエンドポイントから収集した情報を保持しており、感染したエンドポイントの挙動に基づいて、被害を受けた他のエンドポイントを迅速に特定できる。

EDRの効果

上述のように、EDRを導入することによって、エンドポイントで発生したセキュリティインシデントを高レベルで検知することができ、詳細な調査や迅速な対処が可能になる。ここでは、企業内で発生し得る事例を通じて、EDRを導入して実際に何ができるようになるかを紹介する。

図1　対象エンドポイントの容易な特定



①対象エンドポイントの特定

EDRが導入されていない場合、インシデントがどのエンドポイントで発生したかを知るためには、エンドユーザーからの申告や、エンドユーザーへの確認、または周辺ネットワークのアクセスログの調査に頼らざるを得ない。これに対して、EDRではエンドポイントで発生するイベントを逐一記録・収集しており、その情報に基づいて対象のエンドポイントを特定できるため、その後の対処を円滑に行うことができる。（図1参照）

②発生事象の解明

エンドポイントでどんなインシデントが発生したのかを究明することも、EDRによって容易になる。通常、インシデントの究明は、インシデントが発生したエンドポイントを保全した上で、フォレンジックの専門家が行う必要があり、これには多くの時間と人員を

レポートに掲載されているあらゆる内容の無断転載・複製を禁じます。すべての内容は日本の著作権法及び国際条約により保護されています。
Copyright © Nomura Research Institute, Ltd. All rights reserved. No reproduction or republication without written permission.

図2　発生事象の迅速な調査

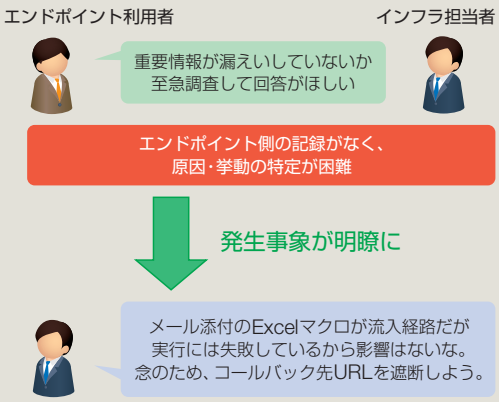
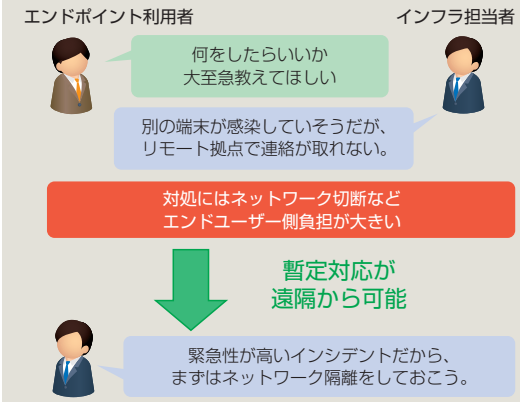


図3　遠隔操作による対処



要するのが普通であった。これに対してEDRを活用すれば、エンドポイントで記録・収集したイベントに基づいて、マルウェア実行の成否、被害レベルの特定、発生内容や感染理由の特定といった迅速な調査が可能である。（図2参照）

③遠隔操作による対処

インシデントが発生したとき、エンドユーザーの負担は非常に大きい。ネットワークケーブルを外す、端末を保全する、端末を初期化するなど、復旧に向けた一連のオペレーションを迅速に進めていく必要があるからだ。そのため、EDRには遠隔操作でネットワーク隔離などを行う機能を持つものが多い。これにより、エンドユーザーの操作を待つことなく、感染拡大を防止する処置を行うことが可能である。（図3参照）

EDRの課題と外部サービス

ここまで、EDRの優れた特性を紹介したが、EDRの効果を最大限発揮させるためには課題もある。それは、EDRを活用した調査や、調査結果に基づいた処置を行う際に、日々更新される脅威情報の把握、最新の攻撃手法に対する理解、危険な挙動と正常な挙動との違いの識別などには高度な知識が要求されることである。

しかし、セキュリティ人材の不足は日本企業にとって慢性的な課題とされてきた。NRIセキュアが2017年に実施した「企業における情報セキュリティ実態調査」では、9割に近い企業がセキュリティ人材を「不足」または「どちらかというと不足」と回答している。EDRは現在のエンドポイントにおけるサイバーセキュリティ対策として、まさに今必要なソリューションであることは間違いないが、高度な知識が必要という点は、人材不足を考えれば大きな課題といえる。この他、エンドポイントへの展開やセキュリティ運用を適切に行うことなども必要である。

これらの課題に対して、セキュリティ専門のベンダーが提供しているアウトソーシングサービスを活用することも有効である。NRIセキュアでも、運用・保守を含む「マネージドEDRサービス」を提供している。企業の“サイバーセキュリティ経営”の一助となれれば幸いである。■

レポートに掲載されているあらゆる内容の無断転載・複製を禁じます。すべての内容は日本の著作権法及び国際条約により保護されています。
Copyright © Nomura Research Institute, Ltd. All rights reserved. No reproduction or republication without written permission.