EDR (Endpoint Detection and Responce)

豊島 隆司
Takashi TOYOSHIMA

1　はじめに

近年，ネットワークに接続できる端末が急速に普及し，ディジタルデータとして重要なデータや個人情報がより多く扱われるようになった．多くの分野においてデータや手続きのディジタル化が行われる中で，個人や企業が保有する価値のある情報を不正に入手するために，数多くのサイバー攻撃が実行されている．

サイバー攻撃から情報および機器を守る手段は，ファイアウォールや侵入検知および侵入防止システムの設置，アンチウイルスソフトウェアの導入など，数多く存在する．しかし，サイバー攻撃に対する対策を行った状態であっても攻撃を完全に防御できる訳ではなく，防衛手段をすり抜ける攻撃が存在する．この侵入を阻止できない攻撃に対して，侵入後の挙動を監視して対処を行い攻撃を防ぐという手法が生み出された．

2　EDR

2.1　概要

EDR (Endpoint Detection and Response) とはサイバー攻撃対策の手法の一種であり，PC 等の端末上で，攻撃の検知および攻撃に対しての対応を行い，端末とデータを保護する．攻撃の検知は実行中のプログラムやデータの操作の挙動を監視することにより実現され，攻撃を受けている最中または攻撃後に検知される．攻撃に対しての対応はデータを守ることを目的に実行され，攻撃の被害拡大の阻止，再発の防止，攻撃前の状態への復帰が行われる．

この手法が提唱された要因として，従来の対策では対処できない標的型攻撃の増加という問題が挙げられる．

2.2　標的型攻撃

標的型攻撃は特定の組織に狙いを定めて実行されるサイバー攻撃の一種である．標的型攻撃の概要図を Fig. 1 に示す．

標的型攻撃は従来の主なサイバー攻撃である無差別型攻撃とは異なり，攻撃対象となる組織のセキュリティについて情報を得た上で実行される．

攻撃者は攻撃の初めに，事前に収集した情報を基にソーシャルエンジニアリングや端末上のソフトウェアの脆弱性を利用して端末に侵入する．侵入の方法の一つとして，入手した標的のメールアドレスに対して関係者を装いメールを送信し，メールに添付された不正なファイルを端末の利用者に実行させる方法が挙げられる．

標的の端末への侵入後は実行された不正なプログラムを用いて，データの不正な送受信を行うための通信路であるバックドアを端末に作成する．バックドアの作成後，バックドアを通して端末の遠隔操作を行い，目的の情報の収集や破壊を実行する．

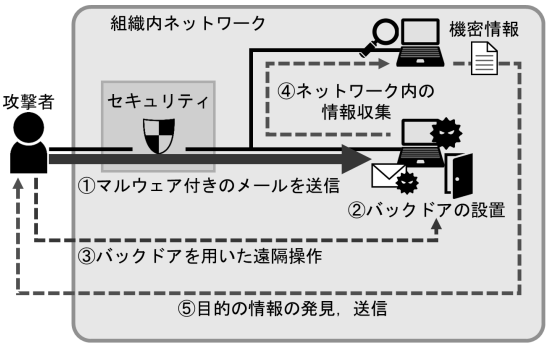

Fig.1　標的型攻撃の概要

バックドアを通して行われる通信はセキュリティシステムを迂回する．そのため，ファイアウォールや侵入検知などのネットワーク上のセキュリティでは攻撃の検知が不可能である．また，標的型攻撃を受けた際にはウイルス等のマルウェアを検知できない場合が多いため，マルウェアの検出により端末を防衛するアンチウイルスでは対処を行うことができない．標的型攻撃はネットワーク上のセキュリティやアンチウイルス等の，攻撃を未然に防ぐ従来の手法では防ぐことができない脅威である．

2.3　EDR と従来のエンドポイントセキュリティ

EDR は保護対象の端末上で実行されるエンドポイントセキュリティの一種であり，従来のエンドポイントセキュリティである EPP (Endpoint Protection Platform) と組み合わせて使用される．EDR のみのセキュリティでは全ての攻撃に対応することは不可能であるため，攻撃による被害を抑制するためには既存の手法との連携が重要である．

EPP はマルウェアによる攻撃を未然に防ぐ手法であり，アンチウイルスが EPP の一種に該当する．アンチウイルスではマルウェアの特徴を示した定義ファイルと端末内のファイルのパターンマッチングを行い，マルウェアが動作を実行する前に検出して対応を行う．しかし，定義ファイルに記載されていないマルウェアの検出は不可能なため，未知のマルウェアや，マルウェアを使用しない攻撃を防ぐことができない．そのため，アンチウイルスでは標的型攻撃を受けた際，侵入を検知できなかった場合に，侵入後も攻撃を検知できずに継続して攻撃を受ける危険性がある．標的型攻撃に対しては，EDR を併用することにより，侵入を防ぐことができなかった場合でも攻撃を検知し，被害を抑止することが可能である．

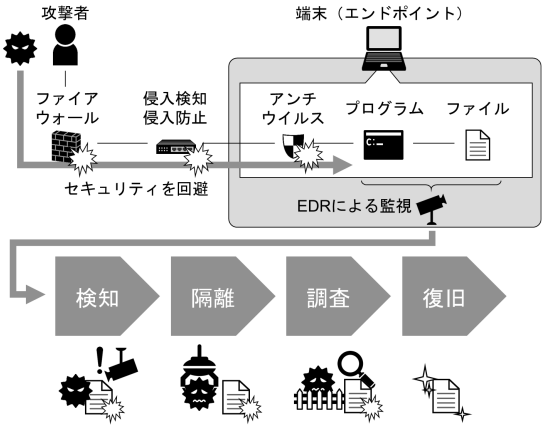

Fig.2　EDR を用いたセキュリティの概要

2.4　EDR のシステム概要

EDR を用いたセキュリティシステムの概要図を Fig. 2 に示す．EDR が機能するのは攻撃が端末に達した場合のみであり，到達以前にファイアウォール等のネットワーク上のセキュリティやアンチウィルスソフトウェアなどの端末上のセキュリティによって対応された場合には EDR は機能しない．EDR の機能は攻撃の検知と攻撃および発生した事態への対応の 2 つの要素により構成される．

攻撃の検知においてはプログラムの挙動，データの操作を監視し，異常な動作を行ったプログラムを特定する．攻撃が検知された場合には，攻撃に関係したプログラムやファイルについて，対応が行われる．

攻撃に対しての対応は，隔離と調査，復旧の 3 つの工程に分かれる．3 つの工程により被害の発生と拡大を阻止し，攻撃による影響を防ぐ．攻撃が検知された際に最初に実行されるのは脅威の隔離であり，プログラムの動作の停止や，データの流出を防ぐために端末をネットワークから切り離す動作を行う．隔離の次に行う調査では，攻撃の情報を集めることで，侵入ルートや被害の影響範囲を確認し，挙動を記憶することで同様の攻撃に対する耐性を高めることができる．調査の後の復旧では攻撃によって操作されたデータを元に戻す動作を行う．

3　EDR の導入事例

3.1　日本マクドナルド株式会社

日本マクドナルド株式会社は 2018 年にセキュリティ対策として EDR 製品の Cybereason EDR を社内の 6000 台の PC に導入した [3]．EDR の導入以前に，既にファイアウォールや侵入検知，侵入防止のネットワークセキュリティおよびアンチウイルスを導入済みであった．しかし，既に侵入済みの脅威の検知が困難であったため，企業内部の端末の状態の可視化およびセキュリティの強化のために EDR を導入した．実際に，メールに添付された Excel ファイルを介して Windows の PowerShell を悪用する攻撃を検知し，攻撃による被害が出る前に脅威の除去に成功した事例が報告されている．

3.2　株式会社資生堂

株式会社資生堂では 2017 年に，セキュリティ対策として EDR 製品である Windows Defender ATP を社内の PC に導入した [4]．Windows Defender は Windows 10 に標準で搭載されたセキュリティ対策ソフトウェアであり，Windows Defender ATP はライセンスの購入により Windows Defender に追加される EDR 機能である．既存のセキュリティ製品では脅威が侵入した場合の対応をユーザー自身で行う必要があり，難度が高く，また，原因究明のためのログデータを損失するリスクがあった．Windows Defender ATP では，ネットワーク管理者が遠隔操作により脅威への対応を行うことが可能であり，脅威の対応におけるリスクを減らすことができる．また，脅威への対応を他社製のソフトウェアを用いずに実現することにより，セキュリティの脆弱性を減らせることが強みである．

4　EDR の現状と今後の展望

近年では，標的型攻撃の被害の他にも，ランサムウェアによる被害や，許可なく暗号通貨の採掘を行い計算能力を奪うマルウェアの登場など，サイバー攻撃の種類および被害は多岐に渡る．多くの個人情報を扱っている企業が被害を受けた際には，企業の信頼に影響が及び，存続に響く自体にまで発展しかねない．情報の価値が高まる中，今後の展望として，企業において EDR 製品の採用が増加していくものと思われる．

EDR の現状として，サイバー攻撃の被害に対する復旧を手動で行う場合が多いという問題が存在する．EDR の機能の発展として，これからは脅威の検出能力の強化や対応の自動化が進むと考えられる．また，現在流通している EDR を搭載したセキュリティソフトウェアは企業向けの製品が主であり，個人向けにはほとんど流通していない．個人においてもサイバー攻撃の脅威は無視できるものではなく，将来的には個人向けの EDR 製品も出現すると考えられる．

参考文献

1) EDR とは何か？～EDR の基礎知識―Cybereason, https://www.cybereason.co.jp/blog/edr/2224/, 参照　Apr.23, 2018
2) EPP+EDR : エンドポイントサイバーセキュリティの未来―KASPERSKY, https://blog.kaspersky.co.jp/epp-edr-importance/20412/, 参照　Apr.23, 2018
3) 導入事例 : 日本マクドナルド株式会社―Cybereason, https://www.cybereason.co.jp/products/case-studies/mcdonalds/, 参照　May.8, 2018
4) お客様事例　株式会社資生堂―日本マイクロソフト, https://customers.microsoft.com/ja-JP/story/shiseido, 参照　Apr.29, 2018