標的型サイバー攻撃対策の次の一手、EDR* とは

» 感染防止を目的としたエンドポイント対策は実施していても、未知の脅威をすべて防ぐことは不可能。今は侵入を前提とした対応策が求められている。その役割を担うのが、エンドポイントにおける活動の記録と、従来型のエンドポイント対策では検知できない不審な挙動の検知を行う EDR* 製品である。

* EDR : Endpoint Detection and Response

目次

内容

セキュリティ インシデント発生、終息宣言までのプロセスは？

実社会におけるインシデント対応の例

何者かにオフィスに侵入され、会社の情報資産が盗まれていた――。このようなインシデントに気づいたとき、会社はまず何を知ろうとするでしょうか？

それは、「誰が、どういった経路でオフィスに侵入し、どのようにして情報資産を盗んだか？ 他に被害はないか？」であるはずです。犯人やその手口・侵入経路や影響範囲、そして侵入を許した原因が特定できなければ、次の犯行を阻止する有効な手だては講じられません。その結果、同一の攻撃者による被害に再度見舞われたり、同様の攻撃によってさらなるダメージを受けたりする可能性が高くなります。

また、盗まれた会社の情報資産が、顧客情報や機密情報など、ビジネスに大きなインパクトを与えるものであった場合、顧客や株主などのステークホルダーに対し、盗難の原因と再発防止の施策を明確に示す必要に迫られるはずです。そうした説明責任をしっかりと果たす上でも、セキュリティ侵害の原因調査・原因究明が必要とされるのです。

実社会において、侵入経路や侵入後の活動を把握するために使われるのが、監視カメラです。監視カメラは、その撮影範囲における人間の行動（アクティビティ）を記録し続けます。何も事件や事故が起きなければ、一定期間後にその記録（ログ）は削除されるでしょう。しかし、何らかの事件が発生した場合、その記録は調査のために使われます。実際に、監視カメラに写っていた記録が事件解決に役立っていることは、よく報道されている通りです。近年、自動車への取付が普及しているドライブレコーダーも同様の役割を果たしています。

図 1 監視カメラ（左）とドライブレコーダー（右）

サイバー攻撃に対するインシデント対応

上記は実社会におけるインシデント対応の例ですが、インシデント発生時に求められる調査は、標的型攻撃などのサイバー攻撃によるセキュリティ インシデントにおいても同様に必要です。

例えば、標的型サイバー攻撃による不正プログラムの侵入を検知し、それに感染した端末が特定できたとしましょう。その際、感染端末をネットワークから隔離するといった初動をすばやく取ることは重要ですが（その後の調査を可能とするため、ソフトウェアの機能を使って隔離することが望ましい）、それだけでは事態の終息には至りません。事態を収拾させるには、セキュリティ侵害の**原因を特定**し、二次的な被害の発生や被害の拡大をすみやかに防ぐことが不可欠です。そのためにも、どのような経路をたどって脅威が侵入したのか（**侵入経路**）、他の端末に不正プログラムが潜んでいないか（**感染範囲**）をスピーディに調べたうえで、被害拡大／二次被害の回避、再発防止の施策をしっかりと講じていくことが必要とされるのです。

EDR とは

標的型サイバー攻撃によるインシデント発生時の対応の迅速化に向けて、近年、必要性が認識され、注目を集めているのが「エンドポイント（端末）の解析」であり、それを実現する **EDR（Endpoint Detection and Response）**製品の活用です。

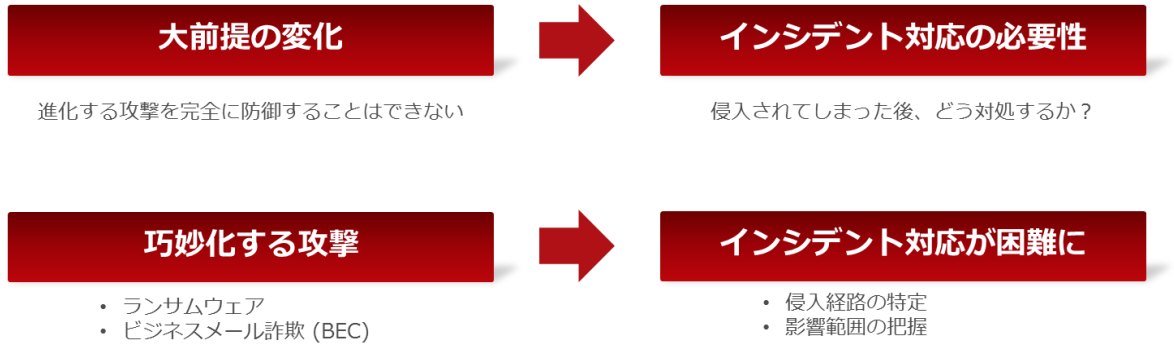
EDR は、エンドポイントを監視し、インシデントの検知・封じ込め・調査・エンドポイント復旧などを実現する技術（製品）です。今日の EDR 製品には、このうち**インシデント調査**の機能が多く実装されています。

EDR 製品は、実社会における監視カメラが人の動きを記録するのと同じように、端末の挙動（システムのアクティビティ）を記録し、その調査・解析によって脅威侵入の原因や経路、影響範囲を迅速に割り出す機能を備えています。インシデント対応においては、システムの動作記録や状態から、過去に起きたことを可視化することが求められますが、EDR 製品はまさにそれを効率化する仕組みです。

EDR が求められる背景

ではなぜ、これまでの対策にプラスして、EDR 製品の活用が必要とされ、また、注目を集めているのでしょうか。理由の一つは、標的型サイバー攻撃の高度化によって、従来の「対策していれば、脅威の侵入は原則として防げる」という大前提が変化しているからです。現在は「進化する攻撃を完全に防御することはできない」という前提に基づき、「脅威の侵入を前提とした対策」の強化が求められているのです。

図 2　EDR が求められる背景



今日の標的型サイバー攻撃は、標的組織用に個別化された攻撃を仕掛けることが多く、その攻撃によって端末に「未知の脅威」が侵入するリスクが常にあります。仮に、そうした脅威によって何らかのインシデントが引き起こされたとき、他の潜在脅威や侵入原因などを調査する能力が低ければ、被害拡大のおそれが高まります。その事態を危惧するユーザが増えてきたことが、EDR 製品に対する注目度の高まりにつながっています。

例えば、一般的な従来型のアンチウイルスソフトは、脅威情報（パターンファイル）とのマッチングによって端末に潜入した不正プログラムを検出・駆除します。これは「**既知の脅威**」を端末から排除するうえで有効なソリューションで、導入することで端末の感染リスクを引き下げることができます。また、サンドボックスやネットワークセンサー（ネットワークを監視し、脅威をセンシングするツール）によって通信・ファイルの解析を行えば、「未知の脅威[1]」の検知力を高め、「怪しげな動きを示す端末」を特定することが可能になります。さらに、ネットワークセンサーやサンドボックスで解析した脅威情報を IDS/IPS（不正侵入検知・侵入防御システム）やゲートウェイ製品、あるいはアンチウイルス ソフトと連携させれば、検知した新たな脅威の侵入や外部との不正通信を即座にブロックしたり、端末上での脅威の動きにすばやくストップをかけたりすることが可能になります。

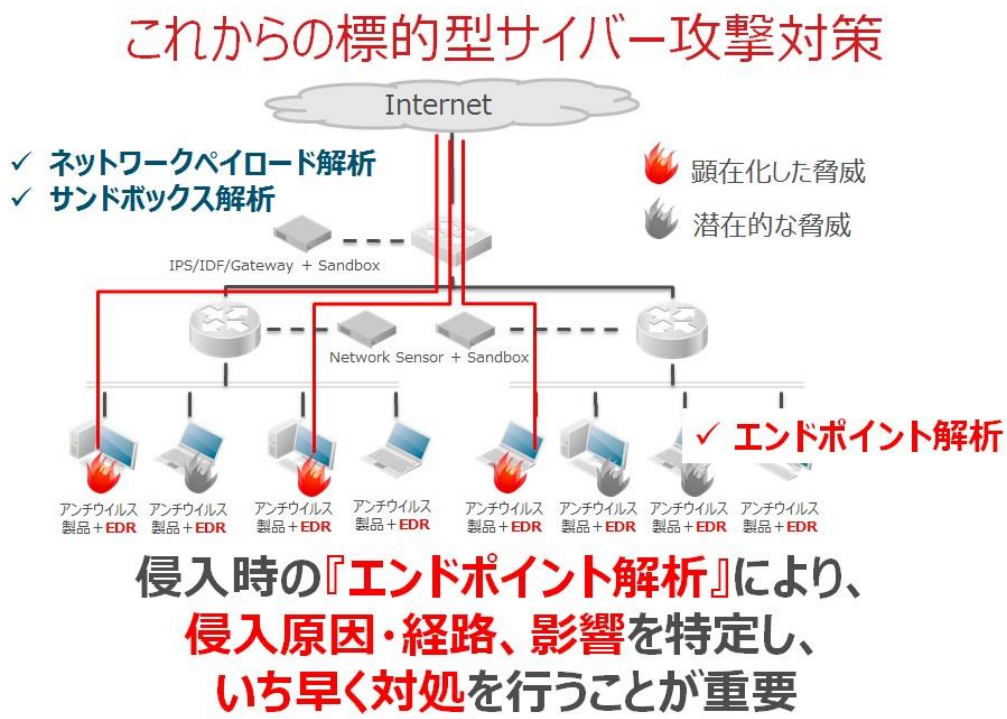
とはいえ、これらの対処は、あくまでも「解析によって顕在化した脅威」に対するもので、「**端末に潜在する脅威**」に対するものではありません。また、IDS/IPS／ゲートウェイ、あるいはネットワークセンサー、サンドボックスなどで防御を固めても、あらゆる標的型サイバー攻撃が完璧に検知・ブロックできる保証はなく、さらに、解析によって不審な端末が特

[1] すべての未知の脅威に対応できるわけではありません。

定できたとしても、どのような経路をたどってその端末に脅威が侵入したのか、あるいは、攻撃がどの範囲に及んでいるかを迅速に把握することも難しいのです。

EDR 製品による端末の（システムアクティビティの）調査・解析は、そうした対策上の隙間を埋め、インシデント対応の遅れによって被害が拡大するリスクを抑える有効なソリューションと言えます。

図 3　これからの標的型サイバー攻撃対策



トレンドマイクロの EDR：

Trend Micro Endpoint Sensor™

トレンドマイクロは、EDR 機能を備えた「Trend Micro Endpoint Sensor」（以下、Endpoint Sensor と記載）を提供しています。

この Endpoint Sensor では、記録したシステム アクティビティに対する調査――具体的にはファイル名や IP アドレス等のキーワード、Open IOC [2]、YARA ルール[3]による調査――を行い、侵入原因や経路、影響範囲のすみやかな可視化をサポートします。

また、トレンドマイクロが提供する振る舞い検知ルール「Attack Discovery Rule」による脅威の検知に加えて、エンドユーザ様が定義した IOC による検知も可能。さらに、検知した脅威を「Deep Discovery Analyzer」（トレンドマイクロのサンドボックス製品）と連携して詳細な解析を行い、リスクを判定することもできます。

EDR 製品として、顕在化した脅威のみならず、潜在的な脅威の特定や攻撃の発見もスピードアップします。

また、すでに「ウイルスバスター コーポレートエディション」をご利用いただいている場合、コーポレートエディションのプラグイン経由で Endpoint Sensor のモジュールを各端末に配信できるため、導入時の負荷を軽減することが可能です。

以下では、EDR 製品の 2 つの主要機能、Detection（検知機能）と Response（調査機能）について、より具体的な機能と活用方法を見ていきましょう。

EDR = Endpoint Detection and Response

Detection：検知

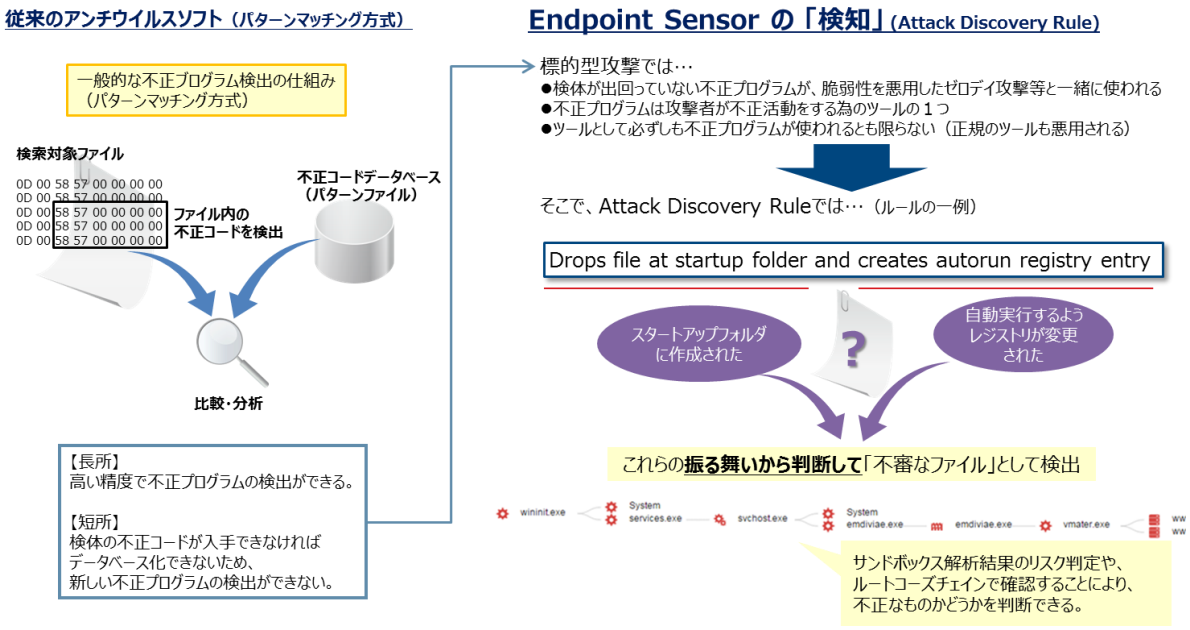
Endpoint Sensor の主要機能の一つは、Detection（検知）です。まず、トレンドマイクロでは Endpoint Sensor に対してデフォルトで、標的型サイバー攻撃の振る舞いを検知するルール「Attack Discovery Rule」を提供しており、このルールに合致する脅威を検知します。また、これに加えて、エンドユーザ様自らが定義した IOC による検知も可能です。

[2] Open IOC：脅威侵入の痕跡（IOC：Indicators of Compromise）を定義するためのオープンなデータ規格

[3] YARA ルール：不正プログラムの特定・分類に用いられるオープンソースのツール（YARA）で用いられるルール

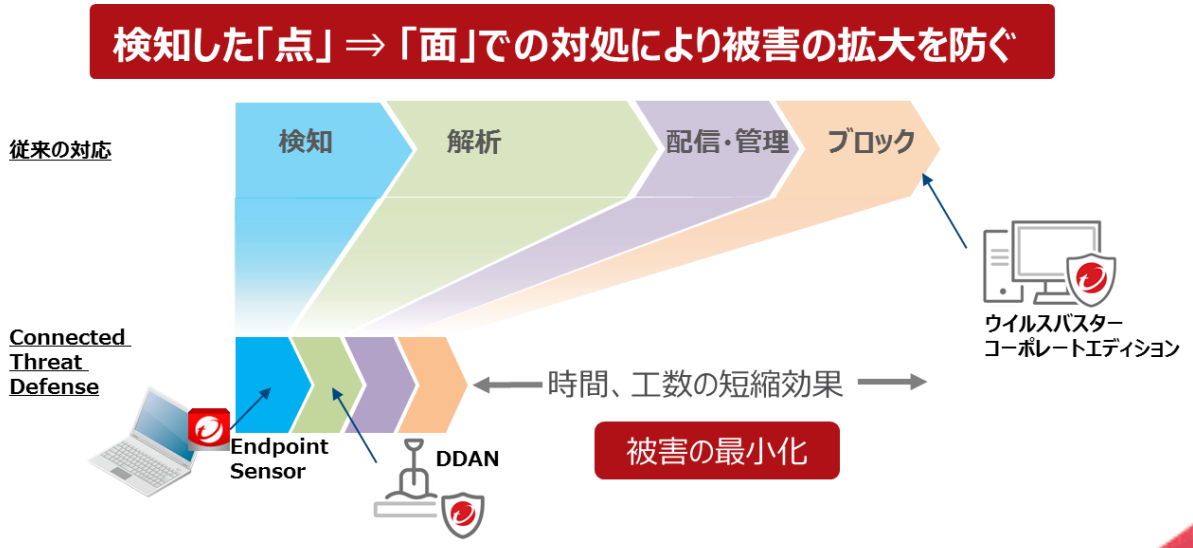
このような検知ルールで検知した脅威は「**Deep Discovery Analyzer**」（DDAN：トレンドマイクロのサンドボックス製品）と連携して詳細な解析を行い、そのリスクを判定することもできます。

図 4 従来のアンチウイルス製品による検知と、振る舞い検知の違い



さらに、DDAN で「リスク高」と判定された不審なファイルや URL は、トレンドマイクロの製品間連携による自動防御（**Connected Threat Defense：CTD**）の機能を用いて、ウイルスバスター コーポレートエディションが導入されている端末等に共有し、その後の活動をブロック可能。これにより、Endpoint Sensor **の検知から防御の自動化**を実現することもできます

図 5 Endpoint Sensor で検知して DDAN に送信～製品間連携による自動防御（CTD）

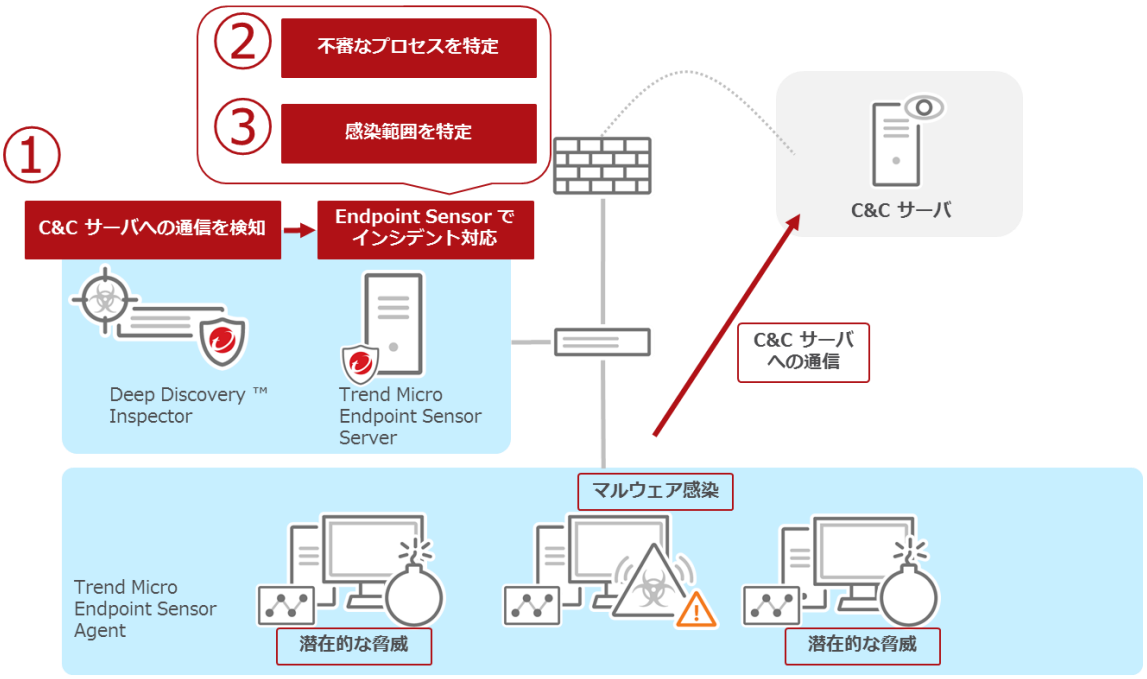


Response： 調査機能

Endpoint Sensor の主要機能の二つ目は、Response（調査）です。ここでは、インシデント発生時の**影響範囲の調査**を例にあげましょう。

Endpoint Sensor を使えば、ネットワークセンサー機器等で検知した不審な通信先の情報から、その通信を行っている端末とプロセスを特定できます（下図の①）。さらに、その不正通信を行っているプロセスを起動した親ファイルを、過去にさかのぼって特定できます（下図の②）。最後に、顕在化した脅威から、潜在化している脅威――感染は完了しているが、まだ不正な通信を行っていない端末――を見つけて対処することで、自社環境内に同じマルウェアに感染した端末がないことを明確にでき、これによって**インシデントの終息宣言が行えます**。

図 6 Endpoint Sensor を使った影響範囲の調査



まとめ

今日、ほぼすべての企業が不審者の侵入や資産の盗難を防ぐためにオフィス・店舗・倉庫などの出入口のセキュリティに万全を期しているはずです。それでも、犯罪者の侵入を100%阻止できる保証はなく、内部犯行のリスクもゼロとは言えません。そうした万が一の事態に備え、出入口や重要資産の在り処に監視カメラを設置し、その撮像記録をのちの調査・捜査に生かせるようにしておくことが当たり前のように行われています。

現在、標的型サイバー攻撃の高度化により、組織の中にいつ脅威が侵入しても不思議ではない状況が到来しています。そう考えれば、実社会と同様の「万が一の事態への備え」をサイバーの世界でも固めるべき時がきているのではないでしょうか。

これまでトレンドマイクロでは「標的型サイバー攻撃には、侵入を前提とした対策が必要である」と注意喚起を行ってきました。標的型サイバー攻撃による被害が経営を揺るがしかねない問題となり、多くの被害が顕在化している今、「うちの組織は大丈夫だろうか？」といった懸念や、インシデントが発生した場合の「原因は？ 被害の範囲は？」といった根本的な問題が解決されるまで、事態が終息したとは言えません。こうした課題の解決に向けて、鍵を握るソリューションが EDR なのです。

TREND MICRO

トレンドマイクロ株式会社

www.trendmicro.co.jp

東京本社
〒151-0053 東京都渋谷区代々木2-1-1
新宿マインズタワー
TEL.03-5334-3601（法人お問い合わせ窓口）
FAX.03-5334-3639

大阪営業所
〒532-0003 大阪府大阪市淀川区宮原3-4-30
ニッセイ新大阪ビル13F
TEL.06-6350-0330　FAX.06-6350-0591

名古屋営業所
〒460-0002 愛知県名古屋市中区丸の内3-22-24
名古屋桜通ビル7F
TEL.052-955-1221　FAX.052-963-6332

福岡営業所
〒812-0011 福岡県福岡市博多区博多駅前2-3-7
シティ21ビル7F
TEL.092-471-0562　FAX.092-471-0563