アンチウイルスは時代遅れ!?

EDRの機能とその効果

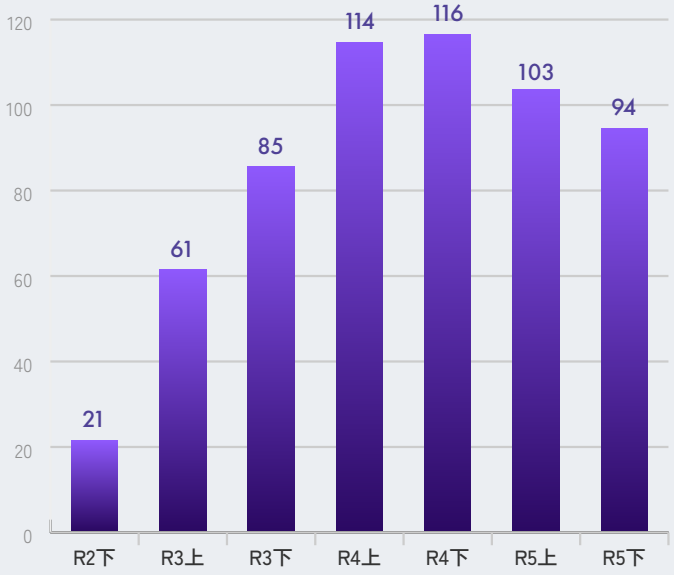
AMIYA

目次

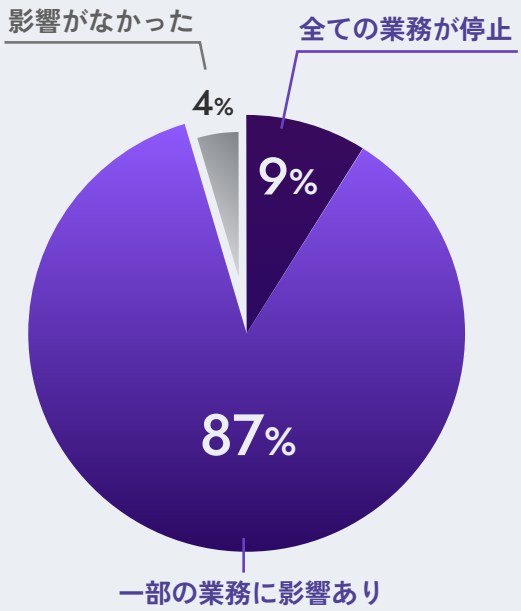
従来型セキュリティ対策の限界

日本企業は今、かつてないサイバー攻撃の脅威にさらされています。令和5年には197件のランサムウェア被害が警察庁に報告されており※1、被害件数は近年高い水準で推移しています。
ランサムウェア被害は、業務に大きな影響を及ぼします。かつてのサイバー攻撃は、個人を狙ったメール送付により端末をロックするなど、局所的な被害にとどまることが多いものでした。しかし近年のランサムウェアは、企業ネットワークへの侵入後、全システムを侵害して重要データを暗号化し、全ネットワークを停止させて身代金を要求します。警視庁の調査でも、ランサムウェア被害に遭った企業の実に96%が、ランサムウェア被害が業務に影響を及ぼしたと回答しています。サイバー攻撃はもはや、企業の事業継続を揺るがす大きな脅威なのです。

企業・団体等における ランサムウェア被害の報告件数の推移



ランサムウェア被害が業務に与えた影響



※1出典：警察庁「令和5年におけるサイバー空間をめぐる脅威の情勢等について」 https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf

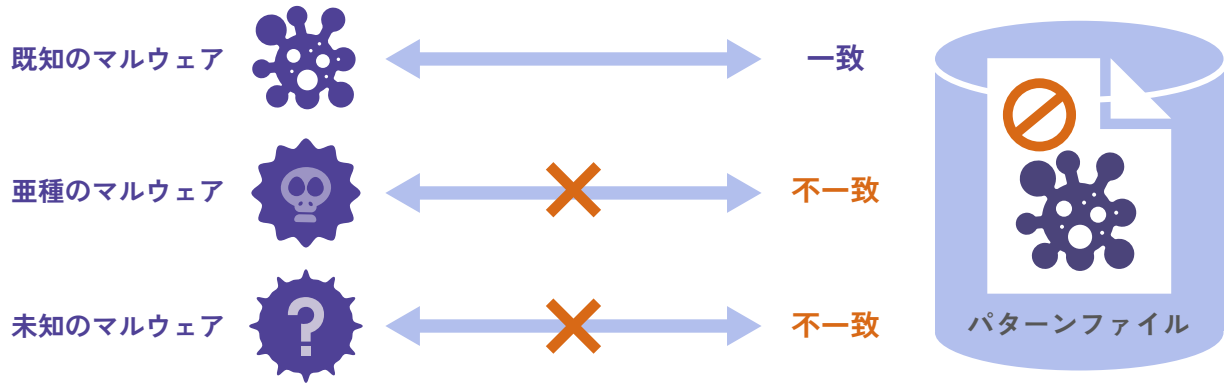
さらに、サイバー攻撃の手口はますます多様化・巧妙化しており、脅威の侵入を防ぐことを目的とする「事前対策」のアプローチに基づく従来のサイバー攻撃対策では、侵入を防ぎきることができなくなっています。
そこで現在重要視されているのが、「事後対策」です。事後対策では、異常や不審な挙動が発生した場合に即座に検知・復旧させ、被害を最小限に留めることを目的とします。
このような経緯で誕生したのが、「EDR」です。EDRは、攻撃の侵入を即時検知し、被害の拡大を防ぐ事後対策を目的としており、現在急速に普及している注目のソリューションです。
本書では、EDR誕生の背景や、機能、導入の効果など、EDRについて詳しく紹介していきます。

02

アンチウイルスでは検知できない攻撃が増加

1980年代以降、コンピュータウイルスの登場とともに、生まれたアンチウイルス製品。長年、マルウェアのネットワーク侵入を防ぐ「事前対策」として、企業を脅威から守ってきました。
アンチウイルス 製品において要となっているのが、「パターンマッチング方式」と呼ばれる技術です。パターンマッチング方式とは、マルウェアや感染ファイルに見られるデータのパターンをデータベース化し、コンピュータ上に同様のパターンとマッチするファイルがないか、コンピュータをスキャンして調べる方法です。不正ファイルと同じパターンを持つファイルがあれば、アンチウイルス製品が不正なファイルとして検出します。
しかし近年、マルウェアはその改良型である亜種を含めると、1日に100万個から200万個も新種が発見されています。そのため、パターンマッチング方式では、新種のマルウェアの解析や登録が追い付かず、亜種のマルウェアや未知のマルウェアは検出することができません。

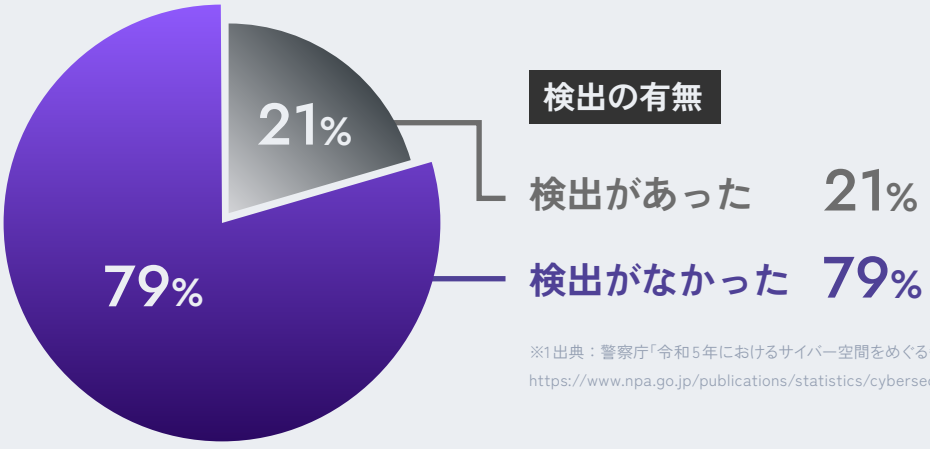
アンチウイルス　侵入時に、実行ファイルにてパターンマッチングを行い検知



マルウェア（新種・亜種）は1日に100万個、ランサムウェア（亜種）は、半年で1万個作成される

▶▶▶ **パターンマッチングの仕組みでは追従できない**

警視庁の調査においても、79%の企業がウイルス対策ソフトではランサムウェアを検出できなかったことが明らかになっています。
アンチウイルスではもはや、近年のサイバー攻撃の侵入を防ぐことができないのです。このような背景から、事前対策のアプローチとパターンマッチング方式による脅威の検出には限界があるという認識が広がりました。
そこで誕生したのが「EDR」です。

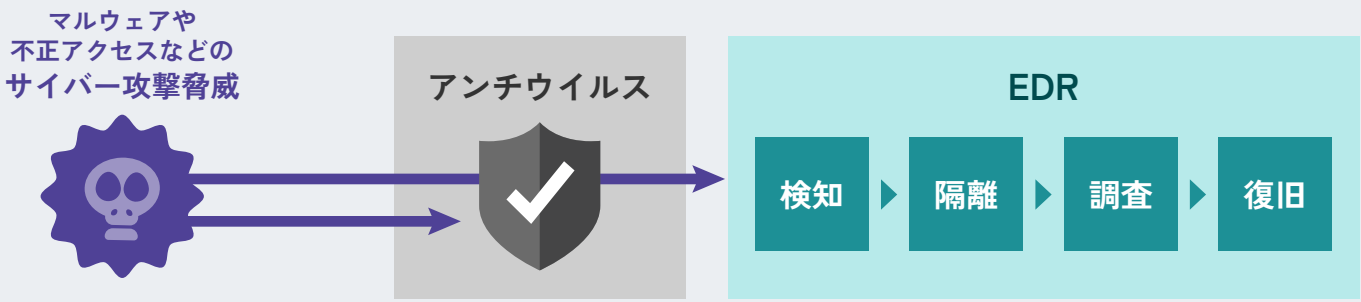


※1出典：警察庁「令和5年におけるサイバー空間をめぐる脅威の情勢等について」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R5/R05_cyber_jousei.pdf

03

侵入後の被害拡大を防ぐ「EDR」

EDR（Endpoint Detection and Resonse）とは、エンドポイント（ネットワークの末端に接続された端末やコンピュータなど）を監視し、不審なふるまいを検知して早期復旧するためのソリューションです。



EDRの基本機能

1 検知

侵入したマルウェアや不正アクセスを検知します。エンドポイントのログを収集・解析し、マルウェアや不正アクセスなど、サイバー攻撃の不審な挙動を検知します。検知した不審な挙動はレポートやアラートとして即座にセキュリティ管理者に通知します。

2 隔離

不審な挙動を検知すると、該当するエンドポイントで実行中のプログラムを自動で停止します。侵入を受けた端末に脅威を隔離し、被害拡大を防止します。通知を受けたセキュリティ管理者がリモートで作業を行い、脅威が侵入した端末をネットワークから遮断するといった対応をすることも可能です。

3 調査

EDRが収集したログ情報を基に、侵入したマルウェアの種類や脅威の侵入経路を調査できます。EDRで検索をかけ、被害端末を特定し、影響範囲を割り出すこともできます。管理者がリモートで調査することも可能です。

4 復旧

隔離したエンドポイントのマルウェアの駆除やデータの復旧を行います。マルウェアの駆除やデータの復旧が完了すれば、端末の初期化等の作業をすることなくエンドポイントを再稼働させることができます。

EDR導入の効果

EDRを導入すると、主に次の二つの大きな効果を得ることができます。

1 サイバー攻撃の被害拡大を防止

パターンマッチングで検出されない未知のマルウェアの侵入や不正アクセスを受けた場合、侵入された事実に気が付かないうちに被害が拡大してしまいます。またアンチウイルスソフトでは、マルウェアの隔離は行いますが、その後の被害端末のネットワーク遮断などには対応していません。
一方EDRはエンドポイントを監視し、ふるまいの異常を検知するため、パターンマッチングで検出できない未知のマルウェアや、不正アクセスなどのサイバー攻撃の脅威を早期に検知することができます。また、被害拡大を抑えるためのネットワーク分離などの対応もリモートから対応できるため、即時の対応で被害の拡大を防止することができます。

2 インシデント対応を効率化

インシデント対応のための原因や影響範囲の特定、復旧作業が長引いてしまうと、顧客への影響も大きく企業の社会的信頼の失墜に繋がりかねません。
EDRは端末横断的な調査が得意であるため、脅威検知後の原因・影響範囲の特定がスムーズです。また、データの復旧までを自動で行うEDRもあり、復旧を迅速に行うことができます。そのため、インシデント発生後の対応を効率化し、調査や復旧にかかる時間を短縮することができます。

05

EDRの課題

このような大きなメリットがあるEDRですが、実は大きな課題があります。
それは、運用が難しい、ということです。
EDRは侵入した脅威の検知と事後対応を目的としたソリューションであるため、EDRが検知したイベントとログの情報をもとに、セキュリティ管理者が調査・対応を行う必要があります。さらには、不審な挙動を検知するとアラートで管理者に知らせてくれますが、その検知は実際にサイバー攻撃である場合もあれば、通常の挙動を誤検知している場合もあります。
これらのインシデント調査・対応や誤検知かどうかの判断には専門知識や高度な技術力が必要になります。これらの知見がなく、調査や判断に時間がかかってしまうと、運用負荷が膨大となってしまいます。しかし、セキュリティ人材不足が叫ばれる今日、高度な知識をもったセキュリティ管理者の確保は至難の業です。

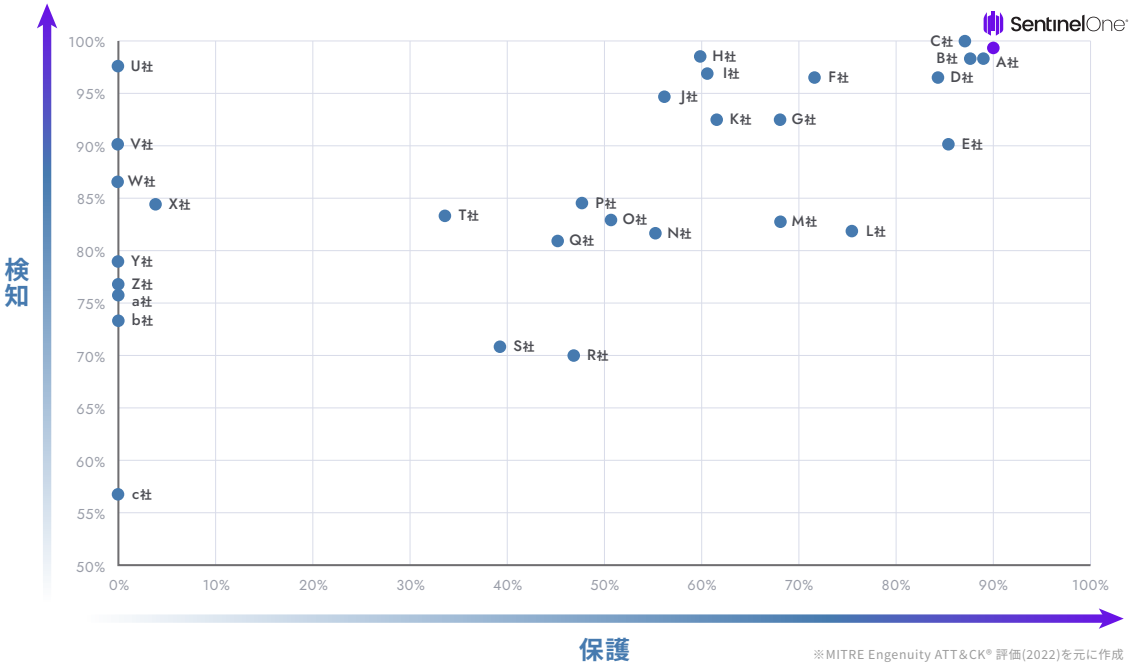
自律型EDR SentinelOne®

06

そこでご紹介するのが、自律型EDR SentinelOneです。SentinelOneは、インシデントの検出から隔離・修復まで、AIがすべて自動対応する、AI自律型の次世代EDR。人的対応を削減し、専門知識や高度な技術がなくても負荷なくEDRを運用できます。さらに、脅威の検知・無効化から修復まで即時完了するため、インシデント対応にタイムラグが生じず、セキュリティリスクも大幅に低減します。

さらに！ 世界最高峰の保護・検知能力

MITRE Engenuity ATT & CK® 評価により証明された世界最高峰の保護・検知能力。
高度化したサイバー攻撃の脅威から徹底防御します。



※MITRE Engenuity ATT&CK® 評価(2022)を元に作成

07

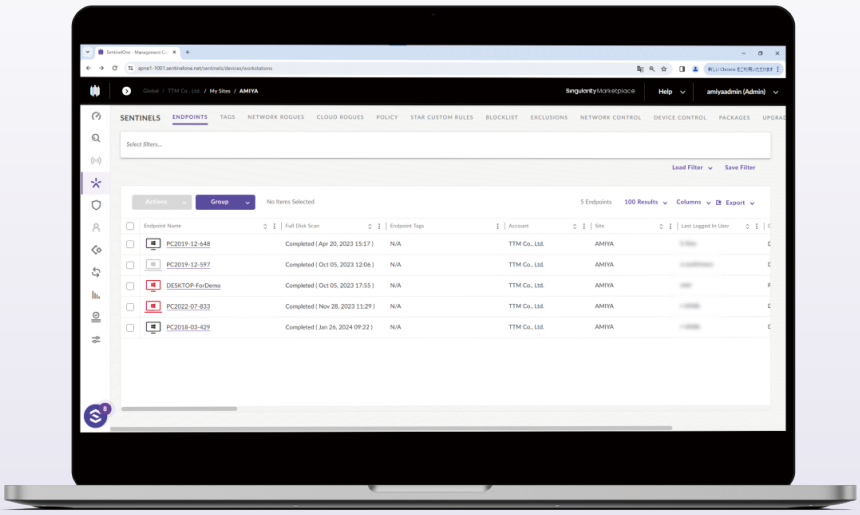
おわりに

EDRで次世代セキュリティを

本書では、注目のソリューションEDRについて、EDR誕生の背景や、機能、導入の効果など、EDRについて詳しく紹介してきました。EDRは、従来の事前防御のみでは侵入を防ぎきれなくなったサイバー攻撃の脅威を最小化する事後対策を目的として、エンドポイント（ネットワークの末端に接続された端末やコンピュータなど）を監視し、不審なふるまいを検知して早期復旧するためのソリューションです。
激化するサイバー攻撃。事前対策のセキュリティのみでは、セキュリティの大きなリスクが潜んでいることになります。まだ大丈夫、と思っているうちに被害が起きてしまっては取り返しがつきません。早めにEDRを導入することで、信頼性と企業価値向上に繋がります。
AMIYAは、長年お客様のセキュリティ課題をコンサルティング・解決してきたノウハウを生かし、「今抱えているセキュリティ課題を相談したい」「自社に必要なセキュリティ対策がわからない」といった、お悩み相談を無料で受け付けております。EDR導入についての課題など、セキュリティの課題についてお気軽にお問い合わせください。

自律型EDR

SentinelOne®



詳しい製品概要資料をご覧になりたい方はこちら

製品概要資料ダウンロード（無料）

お申し込みや詳しい製品のご紹介をご希望の方は以下にお問い合わせください

電話でのお問い合わせ
03-6822-9996

メールでのお問い合わせ
bv-sales@amiya.co.jp

株式会社網屋 データセキュリティ事業部

Secure the Success.

網屋の事業は、セキュリティ。

セキュリティ製品やサービスを自ら開発・製造・販売する、セキュリティの総合プロバイダです。

サイバー攻撃は、経済的余裕度に関係なく、全ての事業法人がターゲットになります。

サイバー攻撃の脅威を「セキュリティの自動化」で解決し、

高水準のセキュリティを誰でも享受できる社会を創りたい。

それが私たちのアイデンティティです。

AMIYA

株式会社 網屋

https://www.amiya.co.jp/

〒103-0007
東京都中央区日本橋浜町3-3-2
トルナーレ日本橋浜町 11F
TEL: 03-6822-9999
FAX: 03-6822-9998