Panasonic

「EDRで十分と思っていませんか？」

THE SECURITY MEASURES ARE SUFFICIENT WITH EDR?

未知のランサムウェア被害を未然に防ぐ方法とは

はじめに

サイバー攻撃による被害は依然として増え続けており、中でもランサムウェア攻撃が企業に与える被害は甚大なものです。サイバー攻撃への本質的な対策はそもそもマルウェアを侵入させないこと。

しかし

ほとんどの企業が導入しているEDR製品は、
マルウェアが侵入してから対策を行うため
被害を食い止めることができません。

そこで今注目されているのが、

未知のマルウェアを99%以上の高い検知率で予防できる「Deep Instinct」です。

当資料では

実は知られていないサイバー攻撃対策における問題点やその解決方法

を解説していきます。

目次

サイバー攻撃は日々進化し続けている

多くの企業が多層でのセキュリティ対策を講じている中、なぜサイバー攻撃の脅威は日々増しているのでしょうか。企業のセキュリティ対策を強化するには、まずその要因を知ることが重要です。

サイバー攻撃の脅威が日々増している要因

サイバー攻撃テクノロジーの発達

近年、新種や亜種などの未知のマルウェアが急増しており、既存のツールでは対策しきれない。

社内研修/周知による対策の限界

メールを用いたサイバー攻撃が90%を占めており、人の手による対策では不十分。

ネットワークセキュリティの限界

近年では暗号化トラフィックが急増中。また、パスワード付zipファイルはネットワーク上で中身を確認できず、マルウェアの侵入を許してしまう。

POINT > これまで通りのセキュリティ対策では、**サイバー攻撃による被害を食い止められない**

企業存続を揺るがしかねないランサムウェアによる被害

IPAが発表した「情報セキュリティ10大脅威2023」によると、企業におけるランサムウェアの脅威度は3年連続で1位という結果が出ています。また、近年サプライチェーン攻撃による取引先を狙ったランサムウェアが増えていることから「自社のランサムウェア対策は万全だろうか」と疑念を抱いている方も多いはずです。ランサムウェアは、以下のような多大な被害を企業に与えます。

ランサムウェアによって企業が受ける被害

データを暗号化される

感染した端末やネットワーク上のデータにアクセスができなくなる。機密情報をインターネット上に公開される恐れがある

身代金を要求される

データの暗号化解除・データの消去・流出阻止のために身代金を要求される。支払ったとしても暗号化解除・データ消去・流出防止が約束されているわけではない

通常業務の稼働停止

ランサムウェアによるシステム障害が発生した場合は、企業の通常業務が停止する

企業のブランド信用低下

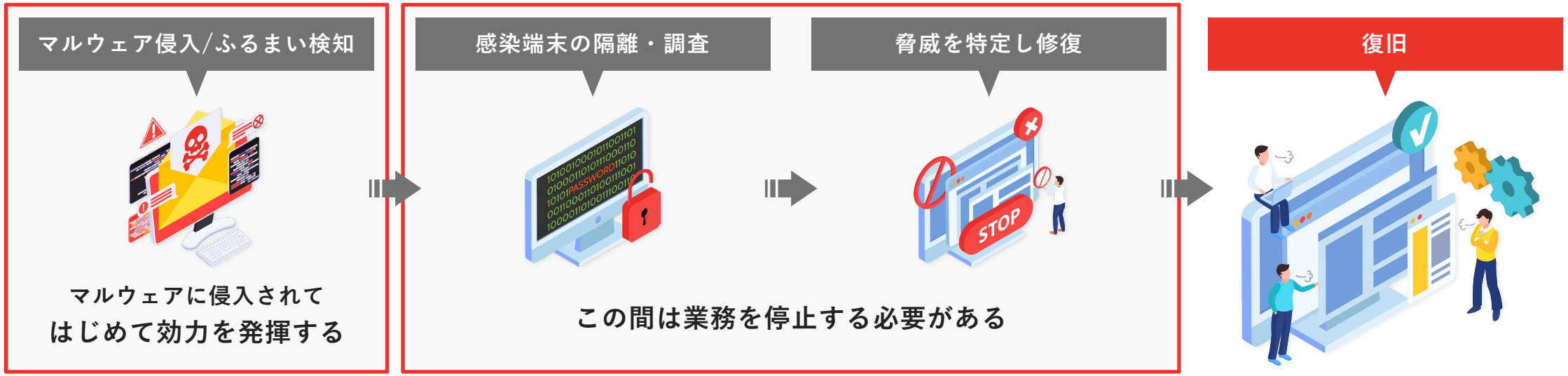
ランサムウェアに感染したという事実は、企業のブランドイメージを著しく低下させる

POINT > ランサムウェアは身代金を要求されるだけでなく企業価値も低下させるため、徹底的な対策が必要

EDRはマルウェアの侵入ありきで効果を発揮する

ランサムウェア被害はわずかな攻撃でも致命的なダメージとなりかねません。そこで、ランサムウェアをはじめとしたセキュリティ対策として、多くの企業に導入されているのがEDR（Endpoint Detection and Response）です。しかし、EDRは振る舞い検知により事後的にマルウェアの動作をブロックするため、ある程度の攻撃を許してしまいます。また、マルウェアが侵入してから復旧するまでに、業務を停止せざるを得ないのも難点でしょう。

EDRの仕組み



POINT > 企業をランサムウェアの被害から守るには、**EDRだけでは不十分**

本質的なセキュリティ対策はそもそもマルウェアを動作させないこと

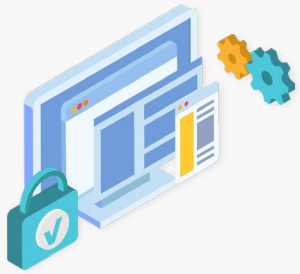
サイバー攻撃の脅威が増していくなか、これから必要となるランサムウェア対策は「そもそもマルウェアを動作させない」ことです。マルウェアが動作しなければ、ランサムウェアによる被害を受けずに済みます。そのためにはEPP（Endpoint Protection Platform）製品の導入が必要です。

EPPの仕組み

マルウェアを侵入前に検知

マルウェアの動作を防ぐ

対象のファイルを隔離/対処プロセスを停止



業務を停止する必要がない

脅威の特定

POINT ＞ マルウェアを動作させない本質的なセキュリティ対策のためには、**EPP製品の活用が不可欠**

Deep Instinctは既知・未知のマルウェアを99%検知する

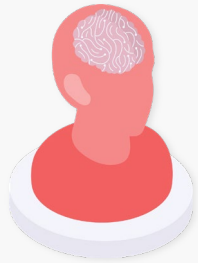
EPP製品の中でも、既知だけではなく新種や亜種など未知のマルウェアを99%実行前に防御するのが「Deep Instinct」です。大量のデータサンプルからマルウェアのDNAを学習し、脅威を検知・予防する「モデル」を生成。深層学習により、ドキュメントファイルもAIが学習します。さらに、攻撃プロセスに使われる他のファイルやスクリプトも学習可能です。

Deep Instinctの仕組み

数十億を超えるデータサンプル

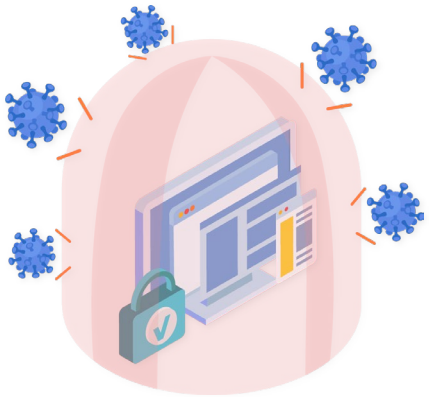
- 第三者機関やレポジトリ
- 自作マルウェア
- ダークネット
- 亜種化

Deep Instinct 独自のDNN※フレームワーク



データサンプルからマルウェアのDNAを学習。高精度に脅威を検知・予防する「モデル」を生成する

※DNN … Deep Neural Network



未知のマルウェアによる攻撃も
99%以上防御できる

POINT > Deep Instinctなら、未知のランサムウェアが動作する前に検知し予防策を取れる

Deep Instinctはセキュリティコストも削減する

Deep Instinctはディープラーニング（AI）を活用したEPP製品であり、以下のような特徴があります。EDR製品の場合は、マルウェアが侵入した後の対応に多大なコストがかかりますが、Deep Instinctの場合はセキュリティコストを最小限に抑えることが可能です。

Deep Instinctの付加価値

動作が軽い

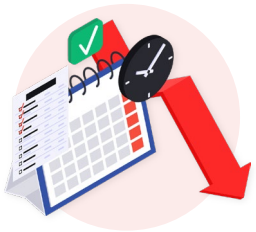
リソース消費が少なく、毎日のアップデートやフルスキャンをする必要がない

運用コストを削減できる

ふるまい検知と比べてアラートが少なく、運用負荷を軽減できる

オフラインでも動作する

検知能力はインターネット接続有無に依存しない



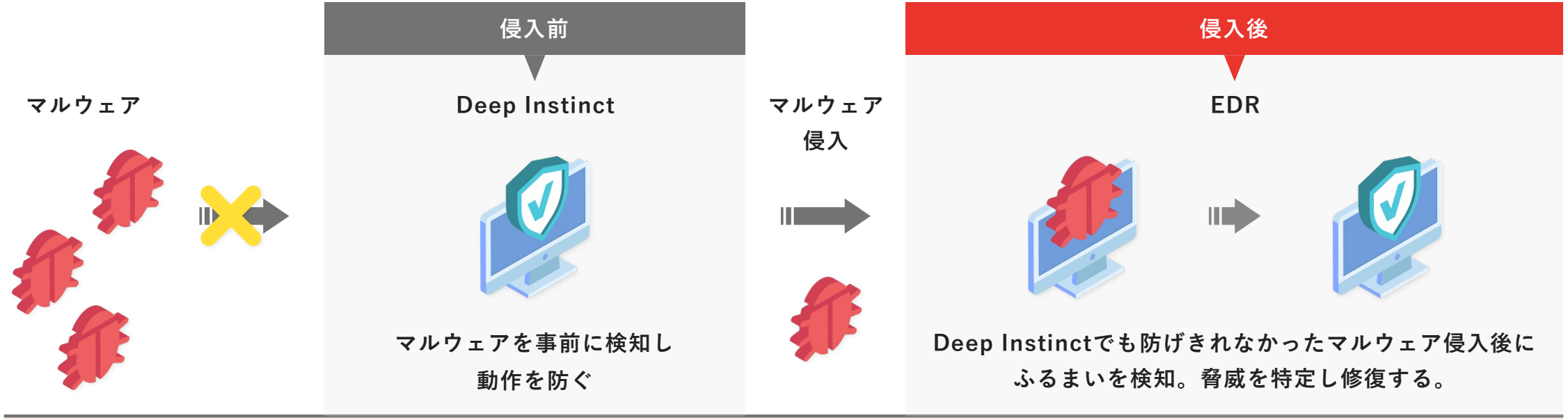
TCOを削減できる

マルウェアを動作させないため、事後対策に係るコストを大幅に削減できる

POINT > Deep Instinctはセキュリティコストを減らしつつ、マルウェアを動作させない優れた製品

ランサムウェア被害を限りなく100%阻止する方法とは？

冒頭でもお伝えした通り、セキュリティ対策を万全にするにはマルウェアを動作させないことが肝心です。そのためにDeep Instinctは効力を発揮します。しかし、Deep Instinctでもマルウェアの動作を100%防げるわけではありません。そこで鍵となるのが、EDR製品との併用です。Deep Instinctで、マルウェアの動作を防御しつつ、もしもの時にはEDRでも対処ができるという盤石の体制を整えることこそ、正しいランサムウェア対策と言えるでしょう。



POINT > EPPとEDRを併用することで、企業をランサムウェア被害から守る

ランサムウェア対策には「Deep Instinct」が欠かせない時代へ

サイバー攻撃が進化し続けている中、そもそもマルウェアの動作を防ぐという本質的な価値を提供するのがDeep Instinctです。
既知のマルウェアはもちろん、未知のマルウェアの動作も防げることから、企業に甚大な被害を与えるランサムウェア対策を徹底したい企業には必須のツールと言えるでしょう。また、セキュリティにかかるコストも大幅に削減できるため、「設備投資、維持管理にかかる総費用を削減しつつより確実なセキュリティ対策を実施したい」という場合にも、ぜひ導入を検討してみてください。

Deep Instinctのご導入をお考えの方は、
パナソニック デジタル株式会社にお問合せください

お問い合わせはこちら

ご連絡先

パナソニック デジタル株式会社

大阪本社 TEL／06-6906-2801 住所／〒530-0053 大阪市北区末広町2番40号

東京本社 TEL／03-5148-5634 住所／〒104-0061 東京都中央区銀座8丁目21番1号

Panasonic