サイバーセキュリティ総研

中小企業向け

# EDRの必要性

# 本パートの前提 **(基本編)**

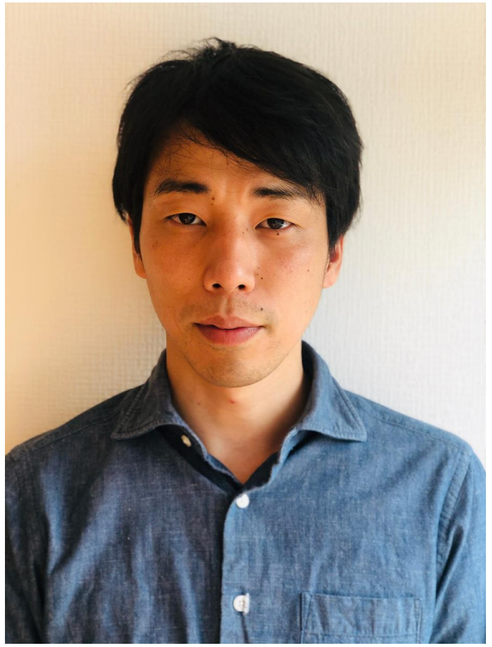
EDRについて、よく知らない、名前は知っているが詳しくは
知らないといった方向けの内容。

アンチウィルスソフト製品からEDR製品に切り替える際
セキュリティ知識のない経営者に説明しやすい内容。

# INTRODUCTION

サイバーセキュリティ総研とは、
中小企業のセキュリティ水準を高めるために情報発信を行うWEBメディア＆コミュニティです。

中立な立場で、様々なセミナーを行っています。

講師：山口智

サイバーセキュリティ総研　主任コンサルタント
主にネットワークのセキュリティエンジニアとして10年近く経験を積んだのち、EDRおよびSOCの事業に関わり、現在では200社以上のセキュリティ運用に関わっている。

# アジェンダ

中小企業向けEDRの必要性

①アンチウィルスソフトはすり抜ける

②ゼロトラスト時代のエンドポイントセキュリティ

③万が一の場合の事業停止リスクも軽減

④なぜいま中小企業にEDRがおすすめなのか？

# アンチウィルスソフトだけで感染は防げない時代

# IPA 情報セキュリティ10大脅威

◢ 情報セキュリティ10大脅威 2023

| 前年順位 | 個人 | 順位 | 組織 | 前年順位 |
|---|---|---|---|---|
| 1位 | フィッシングによる個人情報等の詐取 | 1位 | ランサムウェアによる被害 | 1位 |
| 2位 | ネット上の誹謗・中傷・デマ | 2位 | サプライチェーンの弱点を悪用した攻撃 | 3位 |
| 3位 | メールやSMS等を使った<br>脅迫・詐欺の手口による金銭要求 | 3位 | 標的型攻撃による機密情報の窃取 | 2位 |
| 4位 | クレジットカード情報の不正利用 | 4位 | 内部不正による情報漏えい | 5位 |
| 5位 | スマホ決済の不正利用 | 5位 | テレワーク等の<br>ニューノーマルな働き方を狙った攻撃 | 4位 |
| 7位 | 不正アプリによる<br>スマートフォン利用者への被害 | 6位 | 修正プログラムの公開前を狙う攻撃<br>（ゼロデイ攻撃） | 7位 |
| 6位 | 偽警告によるインターネット詐欺 | 7位 | ビジネスメール詐欺による金銭被害 | 8位 |
| 8位 | インターネット上のサービスからの<br>個人情報の窃取 | 8位 | 脆弱性対策の公開に伴う悪用増加 | 6位 |
| 10位 | インターネット上のサービスへの<br>不正ログイン | 9位 | 不注意による情報漏えい等の被害 | 10位 |
| 圏外 | ワンクリック請求等の<br>不正請求による金銭被害 | 10位 | 犯罪のビジネス化<br>（アンダーグラウンドサービス） | 圏外 |

**ランサムウェア被害がここ数年不動の1位**

出典：IPA　セキュリティ10大脅威 2023
https://www.ipa.go.jp/security/10threats/10threats2023.html

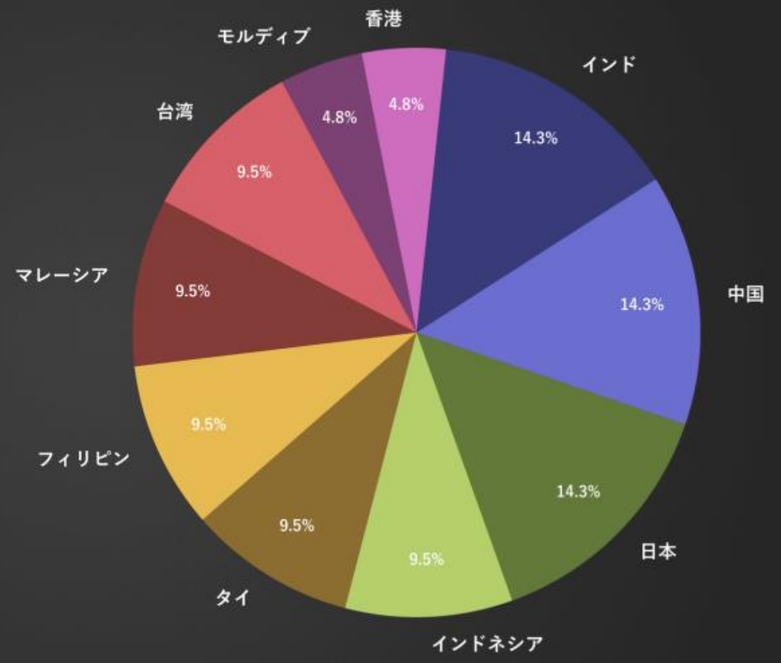
# ランサムウェア対策の強化が必要

グローバルで見ると、ランサムウェアの被害は減少傾向にあるが、**アジア地域では増加傾向**にあり、
その中で**日本はトップ**(同率)であり、対策の強化を求められている。

● 月別内訳 被害国TOP10 （2023年 1 月／アジア） (MBSD調べ)

※件数順に降順／同件数のものが含まれる場合は名前順でTOP10までを記載。

| 国名 | 件数 | 割合(%) | 前月比(件数) |
|---|---|---|---|
| インド | 3 | 14.3 | - 3 |
| 中国 | 3 | 14.3 | + 3 |
| 日本 | 3 | 14.3 | - 2 |
| インドネシア | 2 | 9.5 | + 1 |
| タイ | 2 | 9.5 | + 2 |
| フィリピン | 2 | 9.5 | + 1 |
| マレーシア | 2 | 9.5 | + 2 |
| 台湾 | 2 | 9.5 | - 2 |
| モルディブ | 1 | 4.8 | + 1 |
| 香港 | 1 | 4.8 | - 1 |




出典：MSBD マンスリーレポート
https://www.mbsd.jp/2023/cig_monthly/MBSD_Ransomware_Statistics_CIG_MonthlyReport_2023_03_JPN_Rev.1.00.pdf

本日お伝えしたい事 ( EDRの基本編)

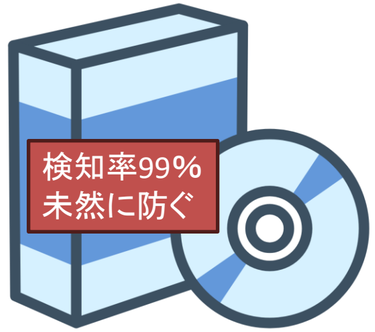
# アンチウィルスソフトはすり抜ける

# 検知率99%の幻想

アンチウィルスソフトのパッケージに記載されている検知率99%の表記。
これはあくまで理想的なラボ環境における**マーケティング用の数値**。

現代では、実際の企業で利用される環境とは大幅なギャップがある。

ニュースに取り上げられるような有名企業のランサムウェア感染は
必ず**アンチウィルスソフトをすり抜けて**発生している。



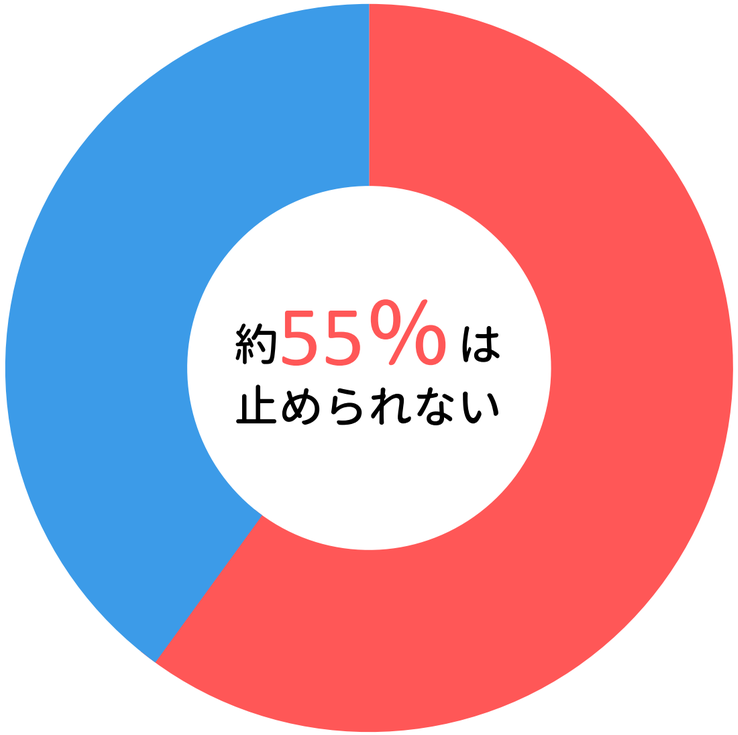
# アンチウィルスソフトは
# すり抜ける

# 実際にはアンチウィルスソフトは45%程度しか止められない

シマンテック副社長も2014年にアンチウィルスソフトは死んだと発言

特定のアンチウィルスソフトの性能が悪いなどの問題ではなく、
サイバー攻撃の高度化によって、技術的に検知出来ないマルウェアが
全体の半分以上を占めるようになった。

**セキュリティに絶対はない**




出典：ガーディアン紙
https://www.theguardian.com/technology/2014/may/06/antivirus-software-fails-catch-attacks-security-expert-symantec

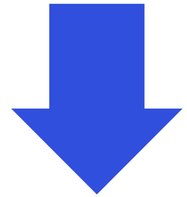
# 検知出来ない理由①
# 新種のウィルスが多い

マルウェアを作るSaaSなども登場し、
新種のマルウェアが大量生産されている状態。

2015年時点の新種マルウェアの発見数

毎日：117万種類以上

アンチウィルスソフトは簡単に言えば
マルウェアのブラックリストによるフィルタリング



ブラックリストに載っていないマルウェアは

**止められない**

# 検知出来ない理由②
# ファイルレスマルウェアも

数年前に猛威を振るったEMOTETのように、
ファイルが存在しない形式のマルウェアが増加
現在ではマルウェアの50%以上とも言われている


アンチウィルスソフトのブラックリストは
ファイルをスキャンして照合している

ファイルがない＝スキャン不可能

## 止められない


アンチウィルスソフトは
すり抜ける

# アンチウィルスソフトがすり抜ける証拠

これらの被害企業がほぼすべて、**法人向けアンチウィルスソフト**を導入している企業であるという事実。

## 暴露型ランサムウェア攻撃統計CIGマンスリーレポート － ⑰

MBSD Know your enemy. Defense leadership.

### 公となった国内被害組織概要一覧（過去1年間／2022年3月～2023年3月）(MBSD調べ)

※（Unknown）の表記は攻撃グループ名が不明または公表されていないケースを表す。
※（海外拠点）の表記は公表等により海外拠点であると判明した被害組織を表す。

| 被害月 | 攻撃グループ | 業種概要 |
|---|---|---|
| 2022/3 | (Unknown) | 検査機器メーカー |
| 2022/3 | (Unknown) | アニメ制作会社 |
| 2022/3 | (Unknown) | アクセサリーパーツ販売会社 |
| 2022/3 | (Unknown) | 大手食品メーカー |
| 2022/3 | (Unknown) | 電気機器メーカー |
| 2022/3 | (Unknown) | 電気機器販売・サービス会社 |
| 2022/3 | LockBit | タイヤメーカー(海外拠点) |
| 2022/3 | Lorenz | 大手産業機械メーカー(海外拠点) |
| 2022/3 | Conti | 自動車部品メーカー(海外拠点) |
| 2022/3 | Conti | 大手電機メーカー(海外拠点) |
| 2022/3 | Pandora | 自動車部品メーカー(海外拠点) |
| 2022/3 | Pandora | 大手出版社 |
| 2022/4 | (Unknown) | 大手酒造メーカー |
| 2022/4 | (Unknown) | 大手食品メーカー |
| 2022/4 | (Unknown) | 私立大学 |
| 2022/4 | (Unknown) | 不動産投資会社 |
| 2022/4 | (Unknown) | 食品製造機械メーカー(海外拠点) |
| 2022/4 | (Unknown) | 大手金属製品メーカー(海外拠点) |
| 2022/4 | (Unknown) | マーケティングサービス会社 |
| 2022/4 | LockBit | 精密機器メーカー |
| 2022/4 | LockBit | 建設会社 |
| 2022/4 | LockBit | プラスチック製品メーカー(海外拠点) |
| 2022/4 | LockBit | 大手建設会社 |
| 2022/4 | LockBit | 医療法人 |
| 2022/4 | Lorenz | 総合化学メーカー |
| 2022/4 | Conti | 大手電機メーカー(海外拠点) |
| 2022/4 | CryptXXX | 電子機器メーカー |
| 2022/5 | (Unknown) | 情報通信サービス会社(海外拠点) |
| 2022/5 | (Unknown) | 国内大手新聞社(海外拠点) |
| 2022/5 | (Unknown) | 医療法人社団 |
| 2022/5 | LockBit | 大手衣料品メーカー |
| 2022/5 | LockBit | 食品メーカー |
| 2022/5 | HIVE | 大手自動車部品メーカー(海外拠点) |
| 2022/6 | (Unknown) | 総合教育サービス会社 |
| 2022/6 | (Unknown) | 輸送サービス会社 |
| 2022/6 | (Unknown) | 債権回収会社 |
| 2022/6 | (Unknown) | 専門情報誌出版社 |
| 2022/6 | (Unknown) | 国立大学 |
| 2022/6 | (Unknown) | 自動車部品メーカー(海外拠点) |
| 2022/6 | (Unknown) | 福祉サービス会社 |
| 2022/6 | (Unknown) | 大手製薬会社 |
| 2022/6 | (Unknown) | WEBデザイン会社 |
| 2022/6 | LockBit | 物流サービス会社 |
| 2022/6 | LockBit | 輸送機器部品メーカー(海外拠点) |
| 2022/6 | LockBit | 医療法人 |
| 2022/6 | Snatch | デザイン会社 |
| 2022/6 | Vice Society | 自動二輪車メーカー(海外拠点) |
| 2022/7 | (Unknown) | 輸送サービス会社 |
| 2022/7 | (Unknown) | 地方商工会議所 |
| 2022/7 | (Unknown) | 投資運用会社 |
| 2022/7 | (Unknown) | インテリア製品メーカー |
| 2022/7 | (Unknown) | ホテル経営会社 |
| 2022/7 | (Unknown) | 衣料品メーカー |
| 2022/7 | (Unknown) | 医薬品販売会社 |
| 2022/7 | LockBit | 機械部品メーカー |
| 2022/7 | LockBit | 地方自治体公務ネットワーク |
| 2022/7 | ALPHV | 大手ゲームメーカー(海外拠点) |
| 2022/8 | (Unknown) | ホールディングカンパニー |
| 2022/8 | (Unknown) | 大手保険ブローカー(海外拠点) |
| 2022/8 | (Unknown) | 不動産会社 |
| 2022/8 | LockBit | 大手食品メーカー(海外拠点) |
| 2022/9 | (Unknown) | 物流機器メーカー |
| 2022/9 | (Unknown) | コンサルティング会社 |
| 2022/9 | (Unknown) | 電力会社 |
| 2022/9 | (Unknown) | イベント管理会社 |
| 2022/9 | (Unknown) | コンサルティング会社 |
| 2022/9 | LockBit | 建設会社 |
| 2022/9 | LockBit | 工業機械メーカー |
| 2022/9 | LockBit | 飼料・肥料原料販売会社 |
| 2022/9 | LockBit | 大手電機メーカー(海外拠点) |
| 2022/9 | LockBit | 酒造メーカー |
| 2022/9 | LockBit | 一級建築士事務所 |
| 2022/9 | LockBit | 自動車販売会社(海外拠点) |
| 2022/9 | LockBit | 農業協同組合 |
| 2022/9 | CHEERS | 娯楽機器メーカー |
| 2022/9 | Hive | 自動車部品メーカー(海外拠点) |
| 2022/10 | (Unknown) | 大手輸送サービス会社 |
| 2022/10 | (Unknown) | 情報通信機器メーカー |
| 2022/10 | (Unknown) | 学校法人 |

※ 特に注釈がない場合は、リークサイトに掲載された数のみに揃えた値とする。
（日本にフォーカスした一部の表／グラフのみ、公表や報道から判明した数を加味し集計）
※ 国内被害組織に関する各種データについては、海外拠点（支社／関連会社）を含む。

（※本ページの表の情報は、日本にフォーカスする関係上、リークサイトに掲載された情報に加えて国内被害組織からの公表や報道から判明した情報も含む）

アンチウィルスソフトはすり抜ける

出典：MSBD マンスリーレポート
https://www.mbsd.jp/2023/cig_monthly/MBSD_Ransomware_Statistics_CIG_MonthlyReport_2023_03_JPN_Rev.1.00.pdf

アンチウィルスソフト
はすり抜ける

じゃあどうすればいいの？

# EDRが求められる時代へ

EDR(**E**ndpoint **D**etection **R**esponse)

アンチウィルスソフトがすりぬける事を前提として

早期発見、被害を最小限にして企業にとっての致命傷を防ぐためのツール。

EDRのユースケース (被害を最小限に)

- ランサムウェアをダブルクリックしてしまったが、暗号化される前に活動を停止した
- 感染に早く気づいたため、ファイルサーバーが攻撃される前にLANを切り離して助かった
- マルウェア感染が発生したが、被害範囲の特定とシステムの復旧が短時間で終わり業務停止が1日で済んだ。

# エンドポイントセキュリティの世代の差


| | | | | | |
|---|---|---|---|---|---|
| 第1世代 | アンチウィルス | ファイル検査 | 該当機能無し | 該当機能無し | 該当機能無し |
| 第2世代 | 次世代アンチウィルス | ファイル検査 | ふるまい検知 | 該当機能無し | 該当機能無し |
| 第3世代 | EDR | ファイル検査 | ふるまい検知 | 緩和処置 | システム修復 |

# 自動車における安全対策を用いて例えるなら

事故発生
(感染)

事故後の対応

| 自動車の安全対策 | 目的 | アンチウィルスソフト | EDR |
|---|---|---|---|
| 自動ブレーキ | 未然に防ぐ | ○ | ○ |
| シートベルト | 被害を最小化 | × | ○ |
| エアバッグ | 被害を最小化 | × | ○ |
| 救急車 | 応急処置 | × | ○ |
| 病院で治療 | 回復する | × | ○ |
| ドライブレコーダー | 裁判に備える | × | ○ |

# EDRの対応（常識的な行動)

事故発生

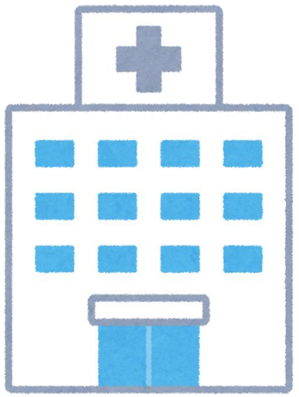
シートベルト＋
エアバッグ作動

被害を最小化

救急車

応急手当

病院で治療



入院

全治1ヶ月

# アンチウィルスソフトの対応 (異常な行動)

事故発生

シートベルト無し
エアバッグなし

救急車よばない

病院に行かない

致命傷

# ゼロトラスト時代の
# エンドポイントセキュリティ

# アンチウィルスソフトを過信(トラスト)

自動ブレーキがあるから、事故はおきないだろう

シートベルトはつけなくていいだろう
エアバッグはいらないだろう
ドライブレコーダーはいらないだろう
自動車保険に入る必要はないだろう

こういう事言ってる人がいたら
怖くないですか？

ユーザー心理

コストをかけたくない
めんどくさい
よくわからない

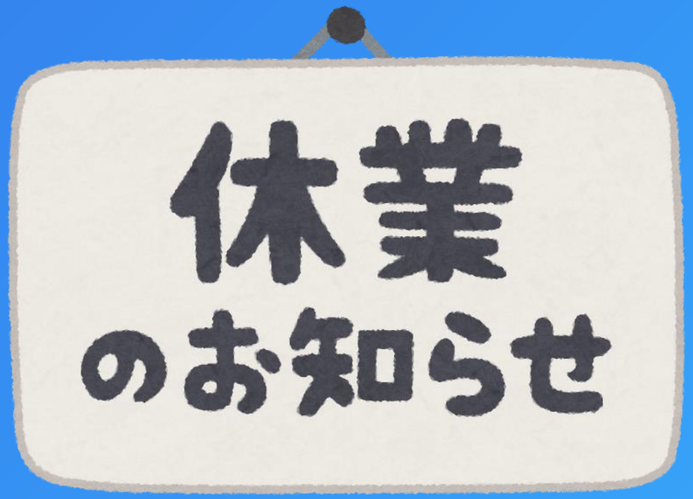
# ゼロトラストエンドポイントの考え方

## 「だろう運転」と「かもしれない運転」の違い

アンチウィルスソフトは「だろう運転」(＝**トラスト**セキュリティ)
→事故は起きない**だろう**。起きたら諦める。 (座して死を待つ)

**EDR**は「かもしれない運転」(＝**ゼロトラスト**セキュリティ)
→事故は起きる**かもしれない**。事故が起きたら最善を尽くす。

それでもまだ
アンチウィルスソフト使い続けますか？




# 事業停止リスクを下げる
# EDR

# サイバー攻撃による事業停止リスクを下げる

- トヨタ仕入れ先のランサムウェア感染による生産ラインの停止
- 名古屋港のランサムウェア感染による物流停止
- 病院のランサム被害による診療停止

など、被害が発生した場合、企業はインシデントの調査と
復旧対応に追われ、**1週間～数ヶ月、業務が停止してしまう事が多い。**

## EDRがあると

- 被害を最小限にするため、業務停止に至らないケースが多い。
- 端末のログが残っているため万が一の場合に調査が短時間で終わる。
- 修復機能によりマルウェアを除去し業務端末の復旧を短時間で完了

# 個人情報保護法への対応

改正個人情報保護法が2022年4月から施行

- 情報漏洩の可能性がある場合に、**速報・確報**を義務化
- すべての企業が対象
- 違反した場合、最大1億円の罰金と社名公開

# アンチウィルスソフトやNGAVでは情報漏洩の速報・確報に不足

個人情報保護法の定めるインシデント発生時の速報・確報において、下記のような情報が必要となるが、アンチウィルスソフトやNGAVでは、情報が不足して対応できない。

| 5W1H | 観点 | アンチウィルス | NGAV | EDR | 保護法の観点 |
|---|---|---|---|---|---|
| When いつ | タイムスタンプ | △ | ○ | ○ | 速報・確報 |
| Where どこから | 侵入経路 | × | △ | ○ | 確報 |
| Who 誰が | PC名 | ○ | ○ | ○ | 速報・確報 |
| What 何を | ウィルス名 | ○ | ○ | ○ | 速報・確報 |
| Why なぜ | 原因 | × | ○ | ○ | 確報 |
| How どのように | 二次感染の有無<br>情報搾取の挙動<br>C&C通信はあったか<br>脅威の抑制状況 | × | × | ○ | 「おそれ」の有無<br>確報 |

# 漏えい（のおそれ）の判断におけるエビデンスの重要性

■　ログの分析と「漏えい」該当性（Q&A6－1）

✓　設定ミスによる公開事例では、閲覧されていないことがアクセスログ等から確認できれば「漏えい」に該当しない

✓　一方、アクセスログが確認できない場合は漏えい（のおそれ）に該当しうる

■　マルウェア検知と漏えいのおそれ該当性（Q&A6－14）

✓　マルウェア感染のみをもって漏えいのおそれありとするのではなく、防御システムによるマルウェアの実行抑制の状況、外部通信の遮断状況等についても考慮して漏えい（のおそれ）があるかどうかを判断

✓　漏えいが疑われる状況であっても、漏えいがないことのエビデンスがあれば、漏えいなしと判断可能

✓　一方で、漏えいが疑われるが、「ログを残しておらず、今あるデータだけでは漏えいしたかどうかわからないので漏えい（のおそれ）はない」と判断することは困難ではないか

ログが取れないセキュリティ(アンチウィルス)を使っていると、
すべての検知が「漏洩のおそれ」になってしまう。

参考：森・濱田松本法律事務所 弁護士蔦大輔様 資料

# まとめ

- アンチウィルスソフトはすり抜ける
- セキュリティはゼロトラスト時代へ　(かもしれない運転へ)
- 事故がおきても諦めない体制に

# なぜ中小企業こそEDR

**EDRがあれば完璧という訳ではないが**
**中小企業にとっては現実的かつ効果的な**
**セキュリティ対策**

中小企業でも導入可能な製品が増えてきた
・少数ロットでも購入可能
・自動化されたEDR
・現実的な金額のサービス

## 理由１：アンチウィルスはすりぬける

**テレワークの拡大**や、**クラウドの利用増加**など
今までのネットワークで守れない環境も増加している。
業務端末の対策強化が一番簡単で効果的。
中小企業にとってEDRが最も現実的な対策。

## 理由２：個人情報保護法への対応

**個人情報保護法**への対応で必要なログを収集・保管するにはEDR製品を導入するのが一番効率的。
インシデント対応にかかる時間とコストを削減し、
経営リスクヘッジとしても利用できる。

## 理由３：EDRがセキュリティの中心になる

**ゼロトラストセキュリティ**が求められるなか、サイバーセキュリティの3本柱となる製品は、
**・EDR（エンドポイントの検知と対応）**
**・SASE（クラウド型ネットワークセキュリティ）**
**・認証基盤（SSO）**

ご清聴ありがとうございました。