Panasonic

ランサムウェア被害を未然に防ぐ

次世代セキュリティ対策のポイント紹介セミナー

主催：パナソニック インフォメーションシステムズ

まつお　　かずよし

松尾 和世司

パナソニック インフォメーションシステムズ株式会社
営業統括部　セールスイノベーション部　マーケティングチーム

製造業における生産管理システムの構築、インフラ運用、
データセンターセキュリティ担当などを経て現職。

マーケティング施策の立案と実行および、
お客様にITのトレンドや最新技術情報をお届けする
エヴァンジェリストとして活動。

資格
経済産業省認定 情報処理安全確保支援士
（登録番号：007992）

CONTENTS

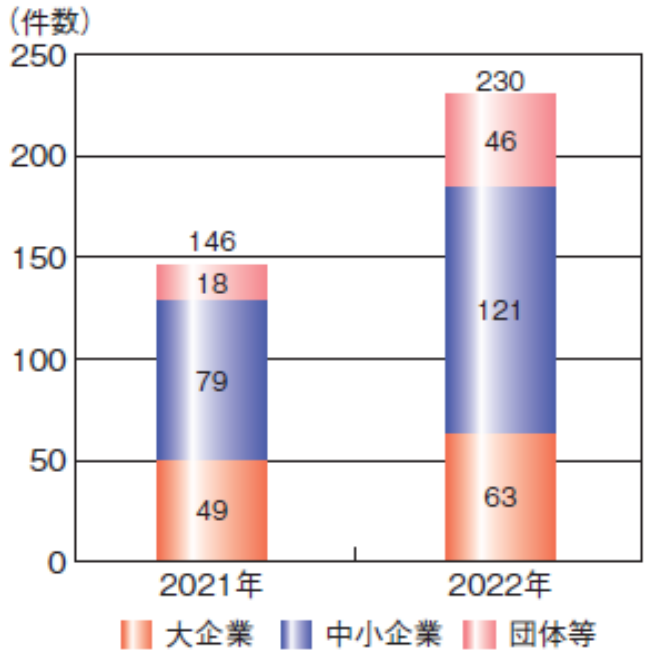
パナソニック インフォメーションシステムズ Panasonic

パナソニック インフォメーションシステムズ Panasonic

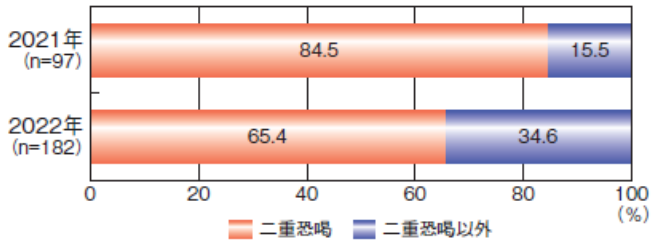
Chapter - 1

サイバー攻撃のトレンド

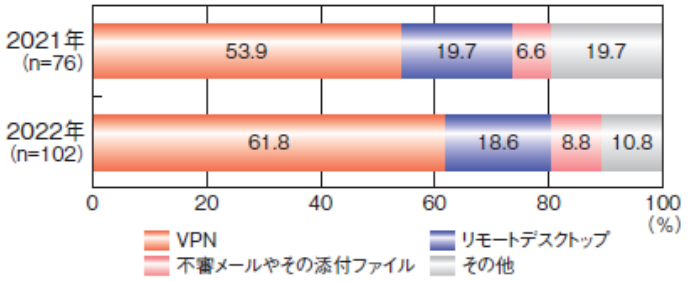
国内でランサムウェア被害が増加



■図 1-1-12　国内のランサムウェアによる被害件数(2021 ～ 2022 年)
(出典)警察庁「令和 3 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」「令和 4 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」を基に IPA が作成



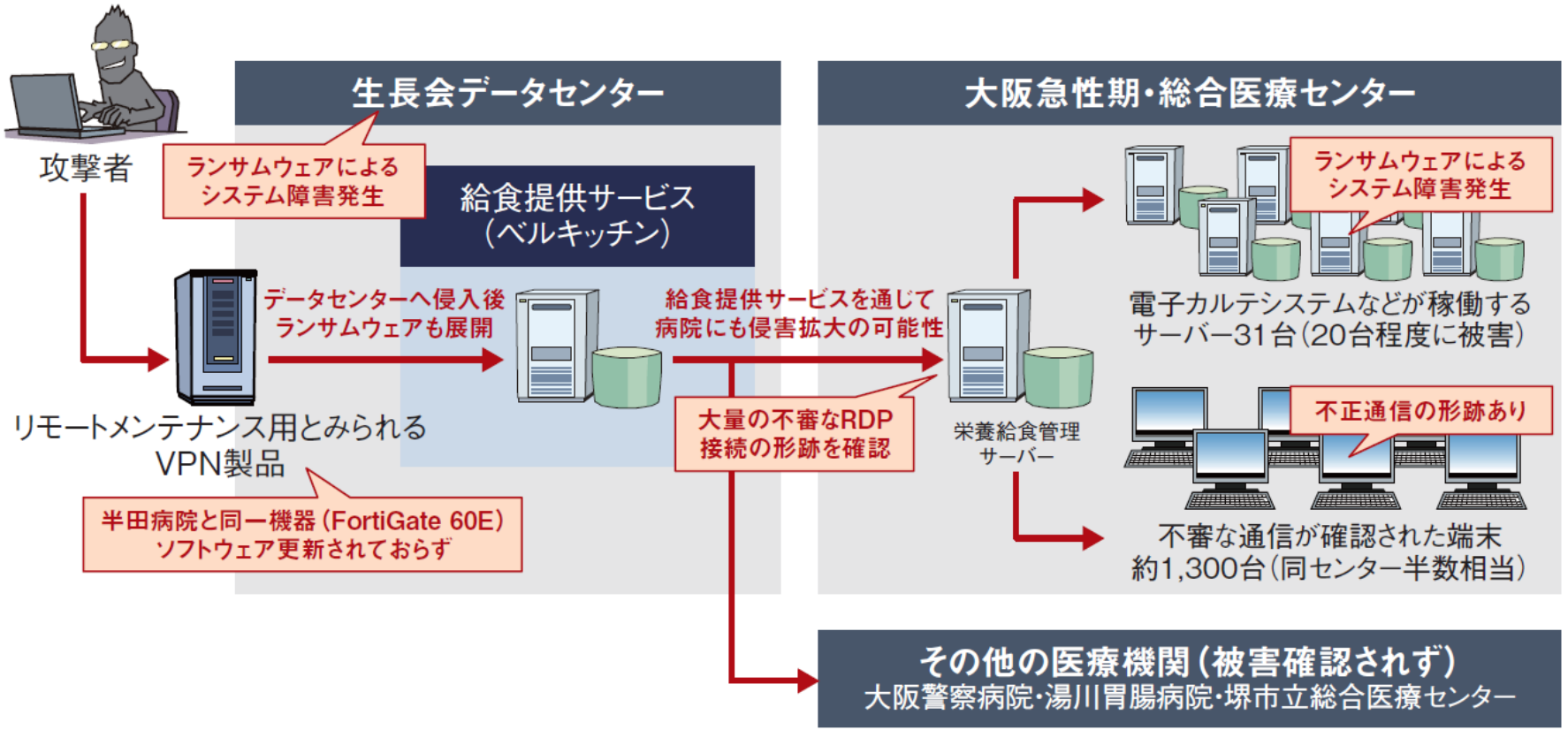
■図 1-1-13　手口別の報告件数割合(2021 ～ 2022 年)
(出典)警察庁「令和 3 年におけるサイバー空間をめぐる脅威の情勢等について」「令和 4 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が作成



■図 1-1-14　ランサムウェアの感染経路(2021 ～ 2022 年)
(出典)警察庁「令和 3 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」「令和 4 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」を基に IPA が作成

【引用元】情報セキュリティ白書2023: https://www.ipa.go.jp/publish/wp-security/2023.html

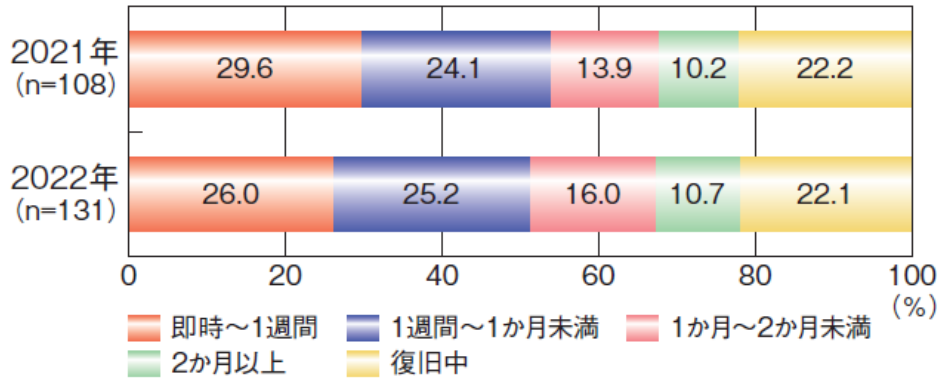
サプライチェーンを狙った攻撃が活発



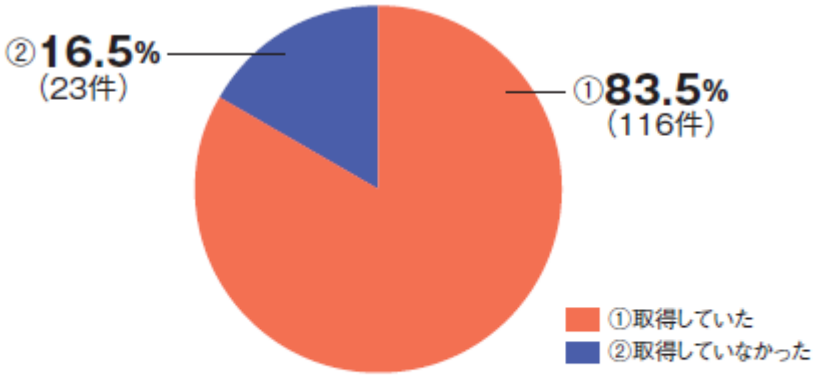
■図 1-2-2　大阪急性期・総合医療センターが受けたと見られる攻撃の流れ
（出典）piyolog「ランサムウエア起因による大阪急性期・総合医療センターのシステム障害についてまとめてみた※30」を基に IPA が編集

【引用元】情報セキュリティ白書2023: https://www.ipa.go.jp/publish/wp-security/2023.html

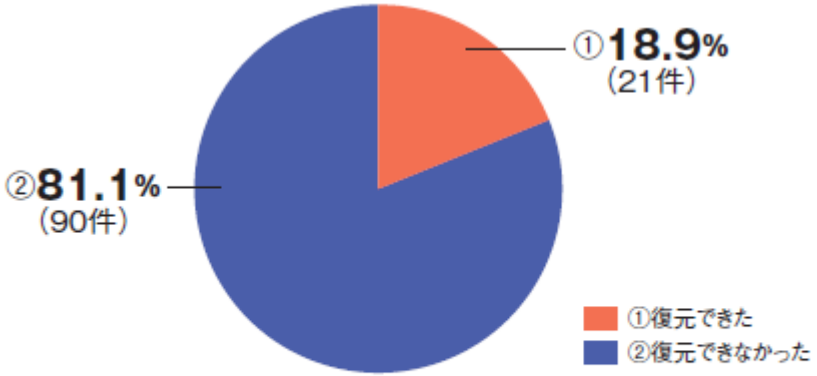
バックアップからの復旧時間も長期化
データ復元できないケースも多い



■図 1-1-15　復旧に要した期間（2021 ～ 2022 年）
（出典）警察庁「令和 3 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」「令和 4 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」を基に IPA が作成



■図 1-1-17　バックアップ取得の有無（2022 年、n=139）
（出典）警察庁「令和 4 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」を基に IPA が編集

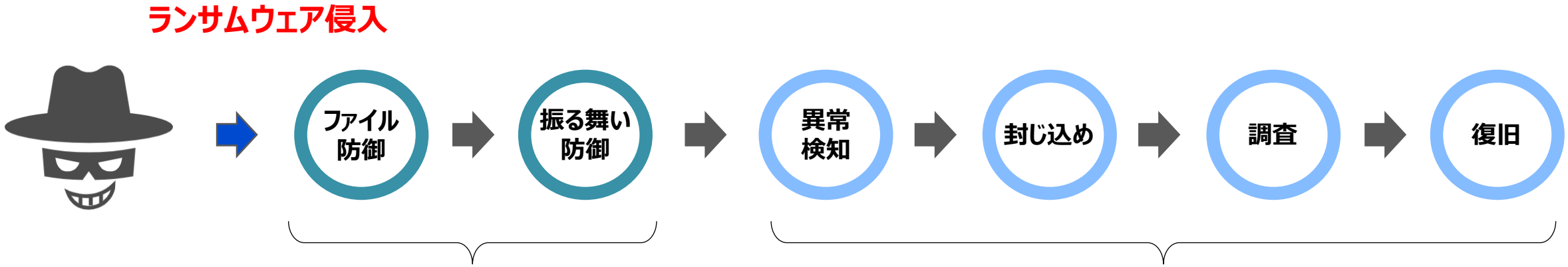


■図 1-1-18　バックアップからの復元結果（2022 年、n=111）
（出典）警察庁「令和 4 年におけるサイバー空間をめぐる脅威の情勢等について」を基に IPA が編集

【引用元】情報セキュリティ白書2023: https://www.ipa.go.jp/publish/wp-security/2023.html

なぜランサムウェア被害が防げないのか？

攻撃が巧妙化し、封じ込めを行う前に感染を広げてしまう



ランサムウェアが活動する前に攻撃を防ぐことが重要

EPP（Endpoint Protection Platform）：エンドポイント保護プラットフォーム
EDR（Endpoint Detection and Response）：エンドポイントでの検出と対応

Panasonic

予防ファーストアプローチ

2022年10月

大阪急性期医療センター

種類: Phobos

被害: システム障害による業務停止

経路: 給食委託事業者のVPN

2023年6月

名古屋港運協会

種類: LockBit

被害:ターミナルシステムに障害が発生

社会インフラ、企業の信頼を脅かす

サイバー攻撃

予防

サイバー攻撃を防御する

被害や感染を限りなく少なくする

事後対処

サイバー攻撃は防御できない

早期発見を行い、調査、対処をする

Panasonic

Chapter - 2

攻撃を未然に防ぐポイント

セキュリティ製品の変遷

アンチウイルス等

EDR等

自律型セキュリティ

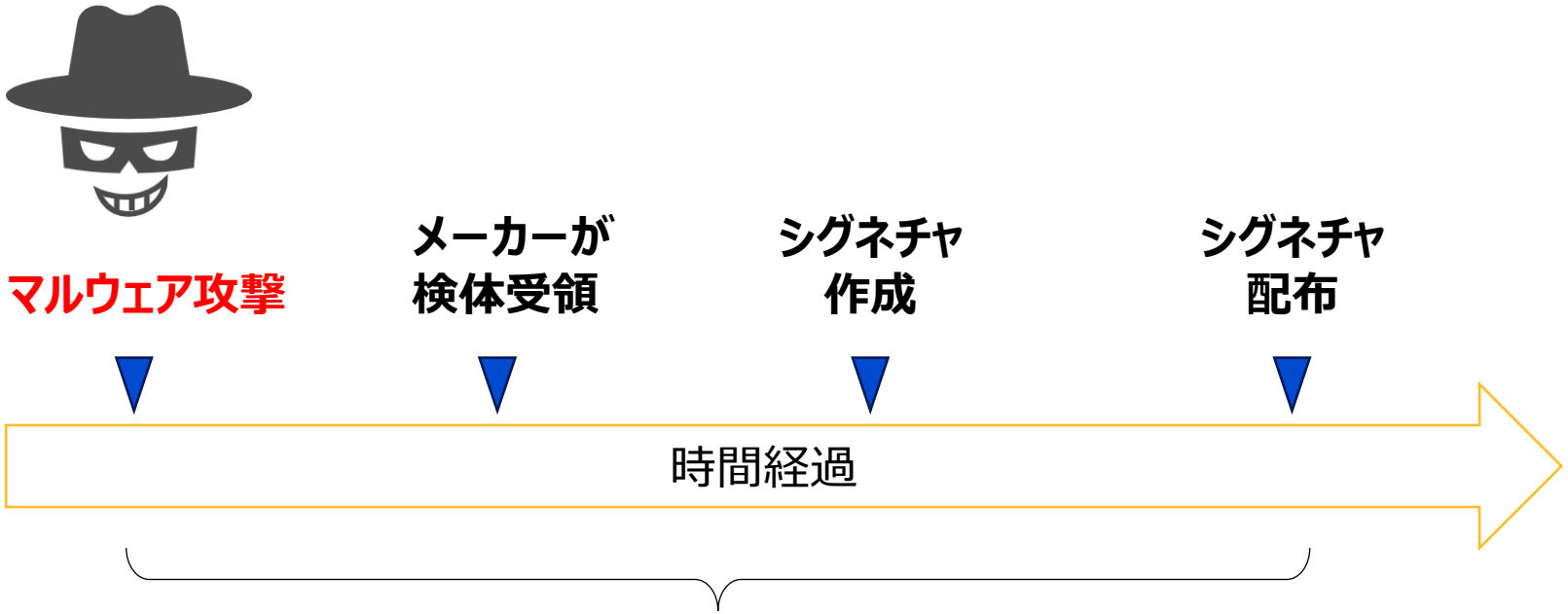
特徴

誰かが攻撃を受けることで初めてシグネチャが作成される

Panasonic

シグネチャ型の限界

誰かが攻撃を受けシグネチャが作成されるまでは無防備



この間が無防備になる
未知のマルウェアには対応不可

Panasonic

セキュリティ製品の変遷

第1世代
シグネチャ
(前科者リスト活用型)

アンチウイルス等

第2世代
機械学習
検知＆対処

EDR等

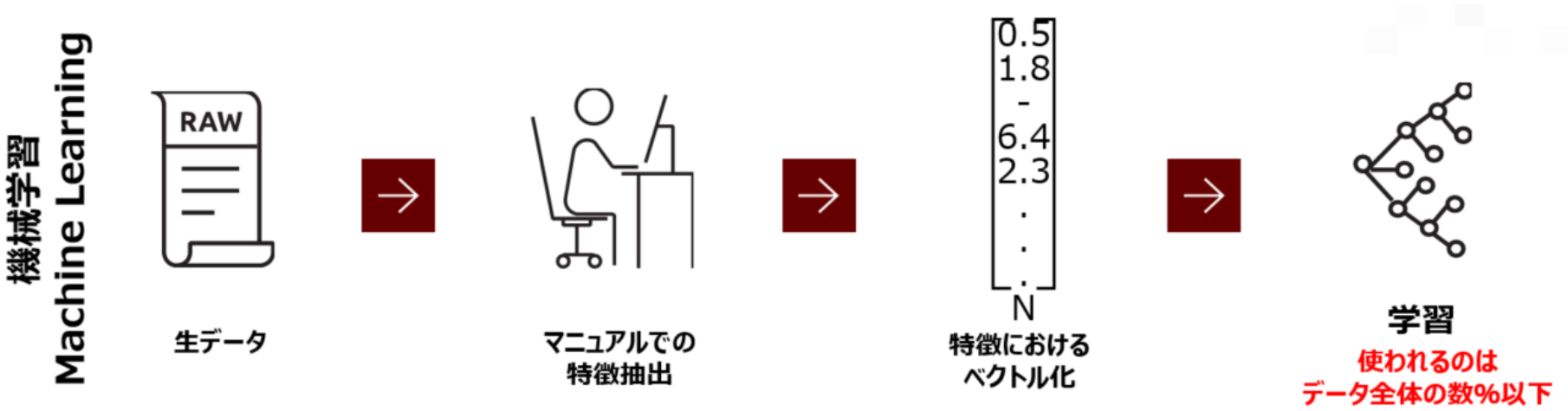
特徴

未知のマルウェアに対応するため、感染後の「ふるまい」を検知

第3世代
ディープラーニング
レジリエントな
セキュリティ

自律型セキュリティ

機械学習の限界と課題



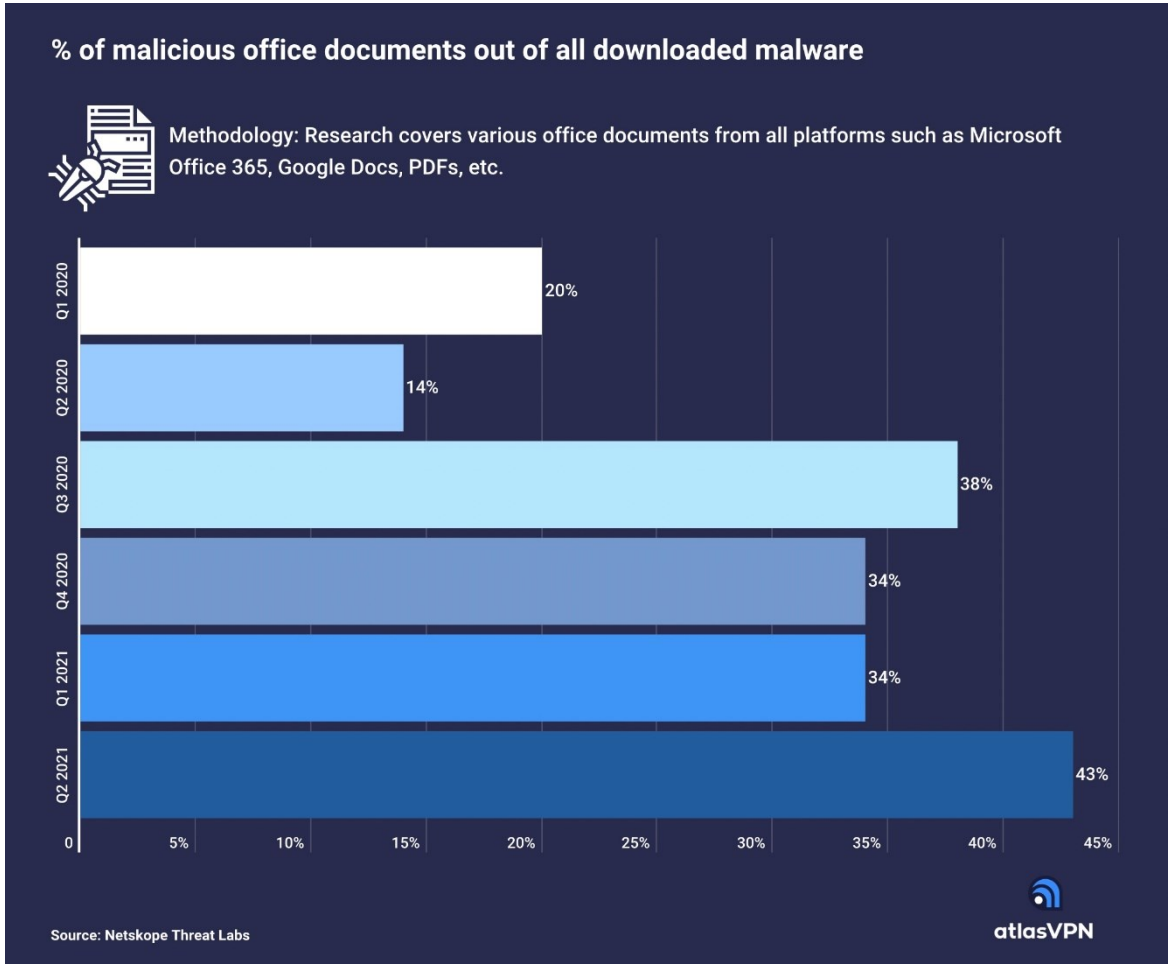
【課題】
- モデル生成に時間とコストが必要
- 教師データは人依存となり誤検知や過検知が不可避
- 攻撃が巧妙化し検知できないケースが増加

参照：NVIDIA「人工知能、機械学習、ディープラーニングの違いとは」

Panasonic

脅威ドキュメントファイルを防ぐ難しさ

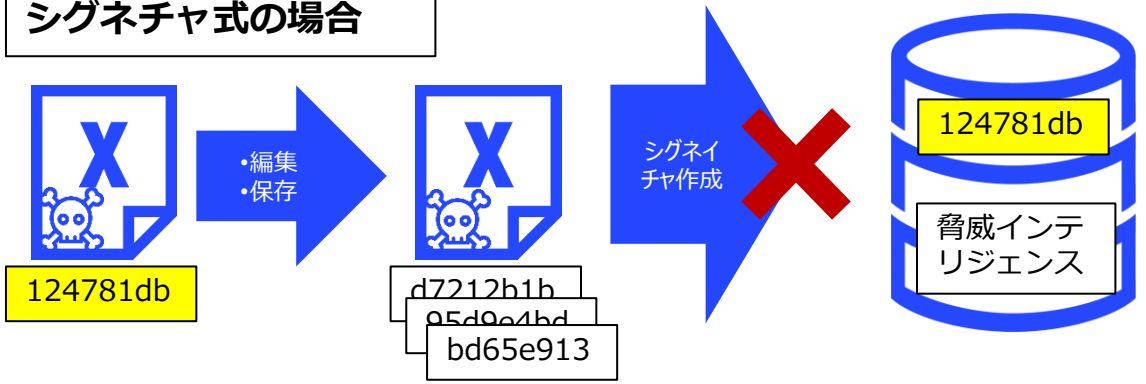
マルウェアの43%は悪意のあるOffice文書から感染



出典: Atlas VPN based on Netskope Threat Lab Cloud and Threat Report: July 2021 Edition

ほぼ全てのセキュリティ製品は、未知の脅威ドキュメントを防御できない

シグネチャ式の場合



編集・保存するだけで異なったファイルになる為、
膨大なファイル数のシグネチャを作成する事はできない

機械学習型AI（振る舞い検知）の場合

機械学習AIはそもそもドキュメントファイルをスキャンできない

Panasonic

セキュリティ製品の変遷

第1世代
シグネチャ
(前科者リスト活用型)

アンチウイルス等

第2世代
機械学習
検知＆対処

EDR等

第3世代
ディープラーニング
レジリエントな
セキュリティ

自律型セキュリティ

特徴

未知の脅威に対する高い防御力を有し、マルウェアを実行前に検知

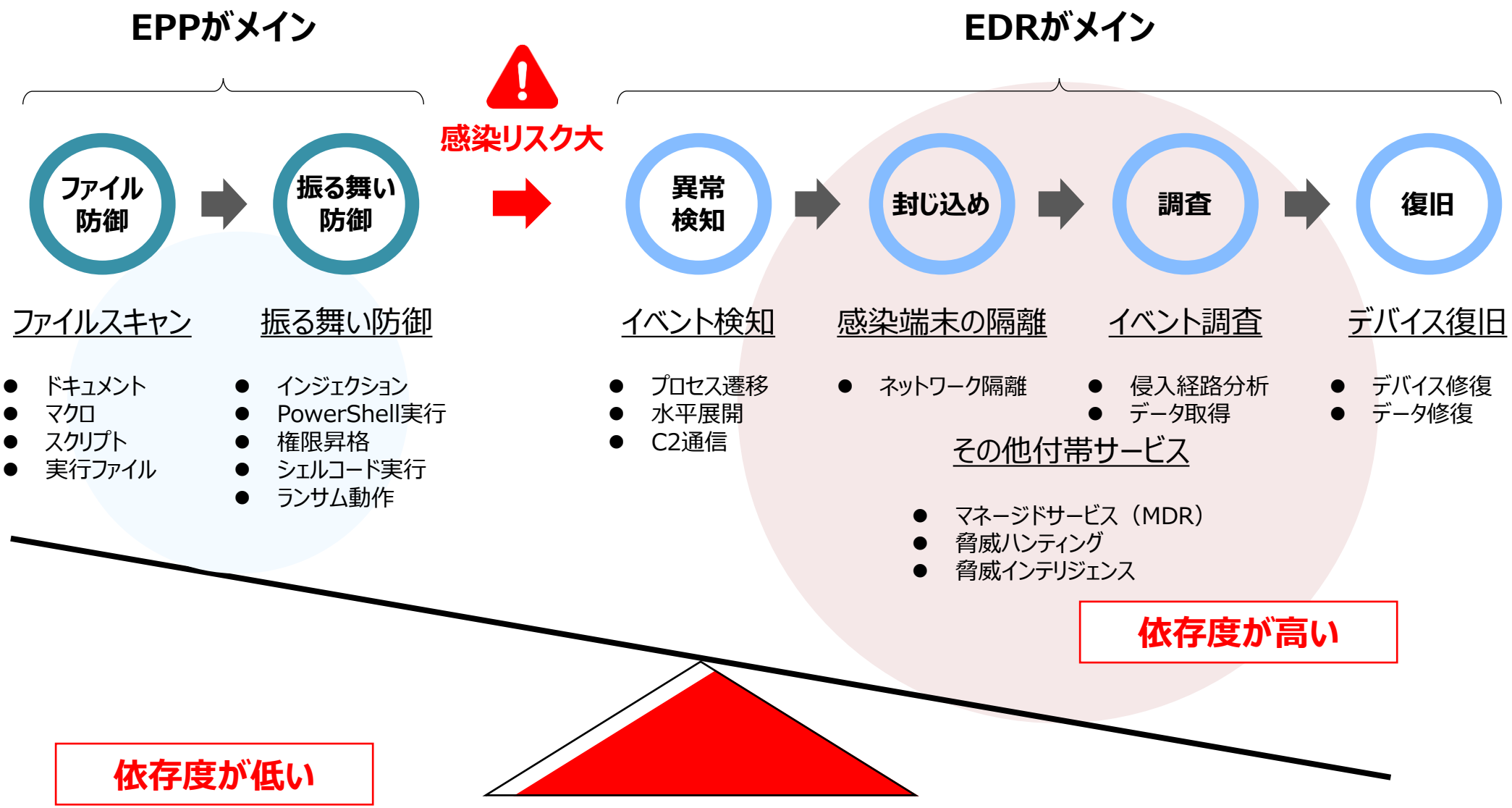
Panasonic

パナソニック インフォメーションシステムズ Panasonic

Chapter - 3

ディープラーニングを活用した新世代エンドポイントセキュリティ

EDRへの依存度を下げることが重要



EPP（Endpoint Protection Platform）：エンドポイント保護プラットフォーム
EDR（Endpoint Detection and Response）：エンドポイントでの検出と対応

Panasonic

Deep Instinct

ディープラーニングを活用した次世代エンドポイントセキュリティ

ディープインスティンクト

最先端のAI技術(深層学習)

予防ファースト

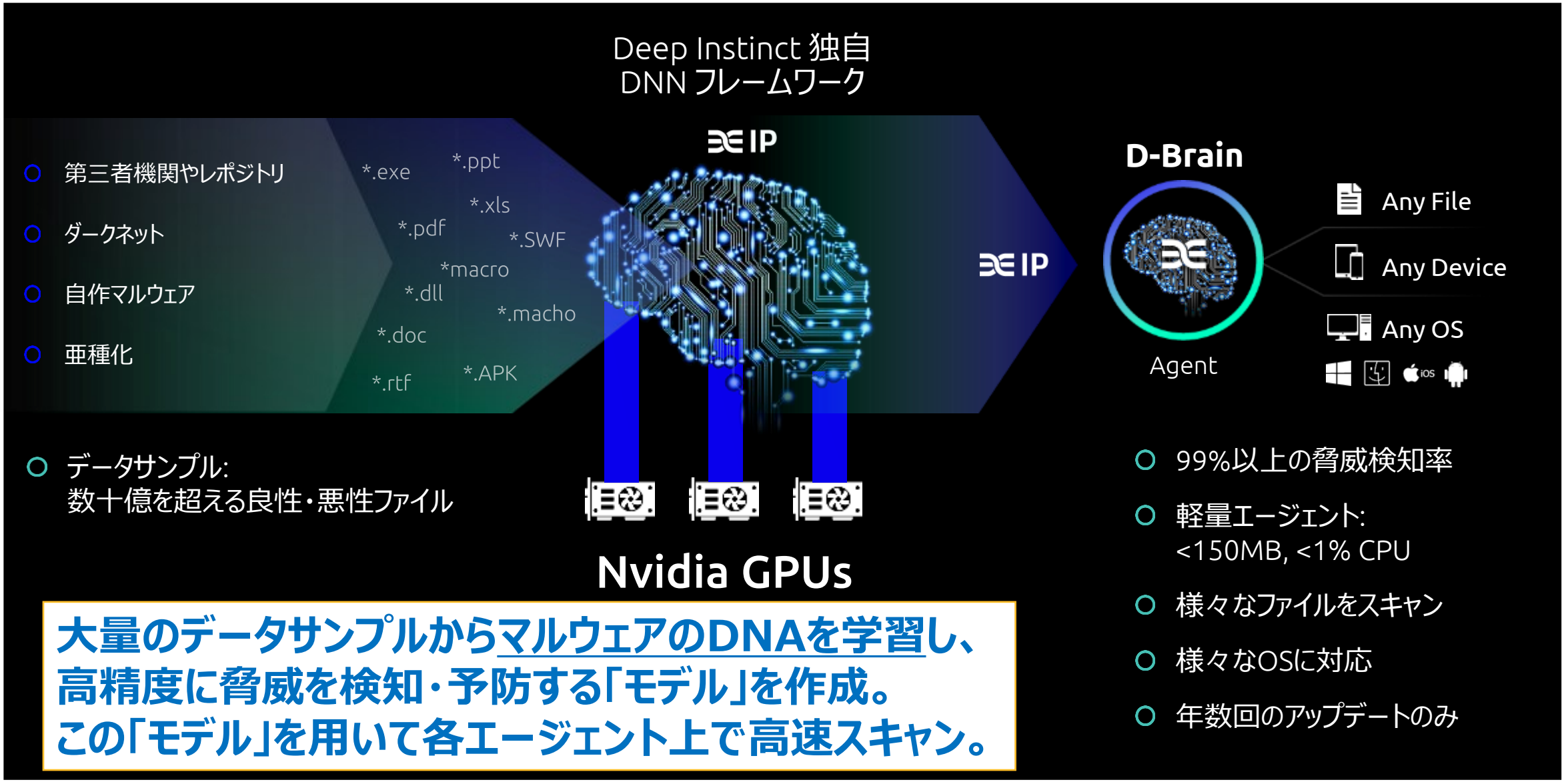
自律型セキュリティ

特徴

- 未知の脅威に対する**圧倒的な防御力**
- 機械学習と比較して**少ない過検知/誤検知**
- 高速なファイルスキャンで**PCへの負担小**
- 静的解析でマルウェアを**”実行前”に検知**
- ひとつのモジュールで実現する**多層防御**
- EDR+SOCより**安価にセキュリティを強化**

Panasonic

ディープラーニングを活用した学習と予測



- データサンプル:
  数十億を超える良性・悪性ファイル

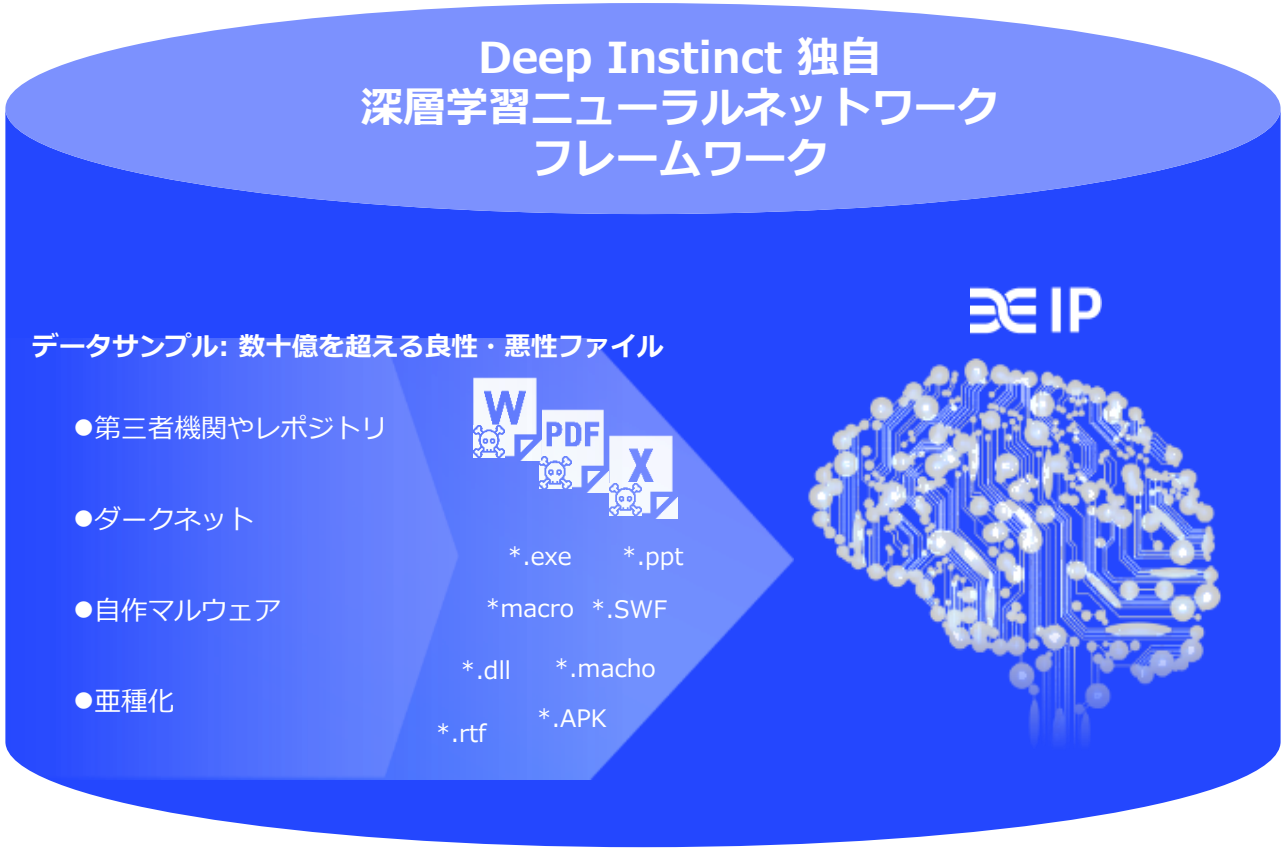
- 99%以上の脅威検知率
- 軽量エージェント:
  <150MB, <1% CPU
- 様々なファイルをスキャン
- 様々なOSに対応
- 年数回のアップデートのみ

**大量のデータサンプルからマルウェアのDNAを学習し、
高精度に脅威を検知・予防する「モデル」を作成。
この「モデル」を用いて各エージェント上で高速スキャン。**

Panasonic

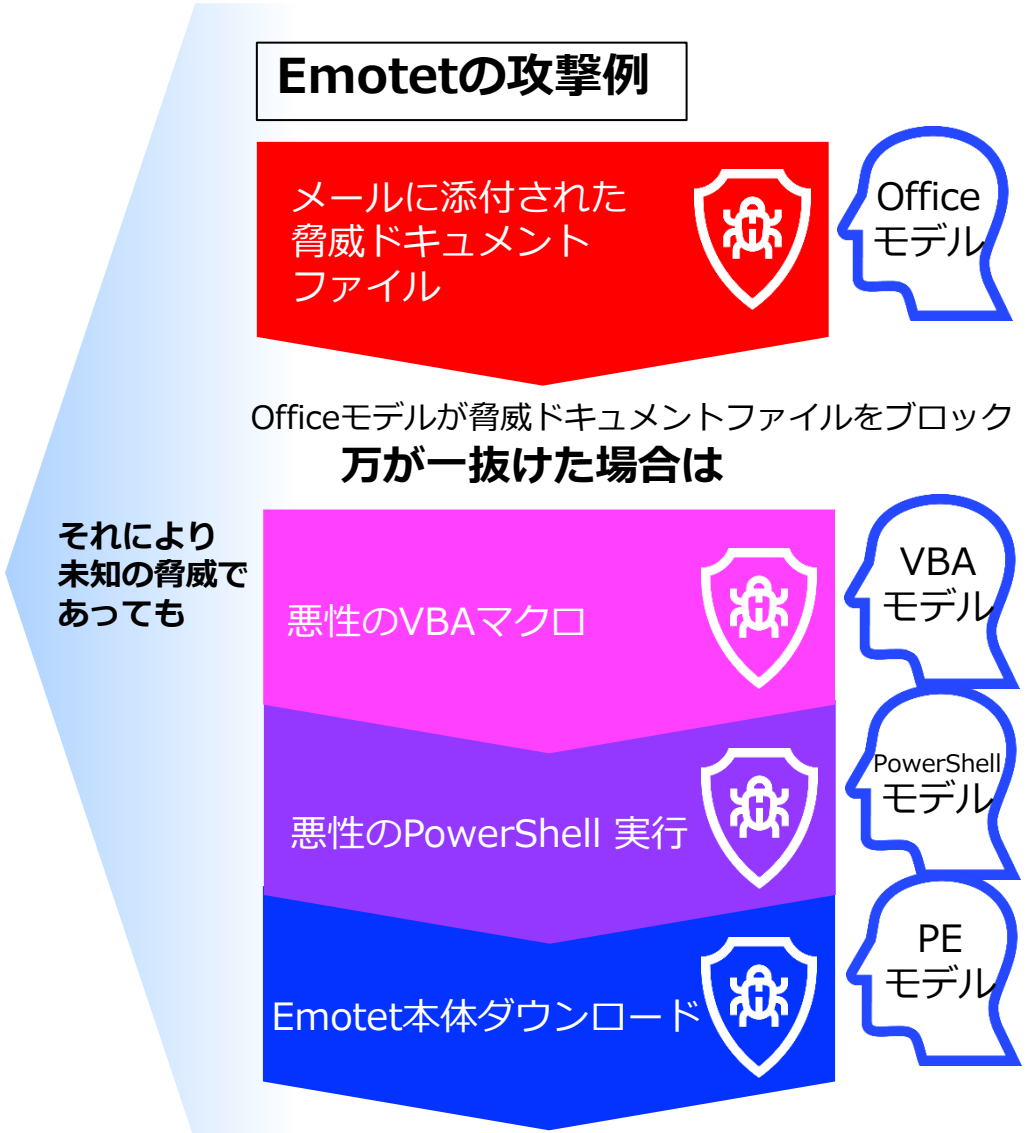
未知の脅威ドキュメントを実行前に防御

未知の脅威ドキュメントによる攻撃も99%以上防御が可能



深層学習により、ドキュメントファイルもAIが学習
それ以外にも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
実行ファイル以外のファイルが学習出来るのは**世界で唯一**

Emotetの攻撃例



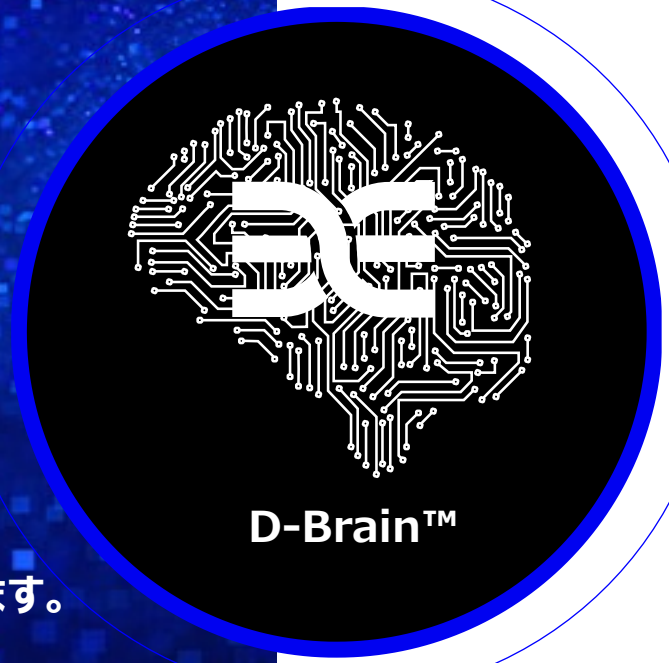
Panasonic

未知のマルウェアを予防可能

予測による予防の実績

Deep Instinct のモデル　D-Brain は、
日々登場するマルウェアを登場のはるか前に
予測しており初見でブロックして感染を予防しています。

これがレジリエントな予防であり
第3世代 DeepGen セキュリティであり
Deep Instinct です。



EMOTET 新種
20ヶ月以上前 のモデルで検知

SNAKE/EKANS
18ヶ月以上前 のモデルで検知

MAZE
20ヶ月以上前 のモデルで検知

Sodin
17ヶ月以上前 のモデルで検知

RagnaLocker
18ヶ月以上前 のモデルで検知

Taidoor RAT
21ヶ月以上前 のモデルで検知

NetWalker
22ヶ月以上前 のモデルで検知

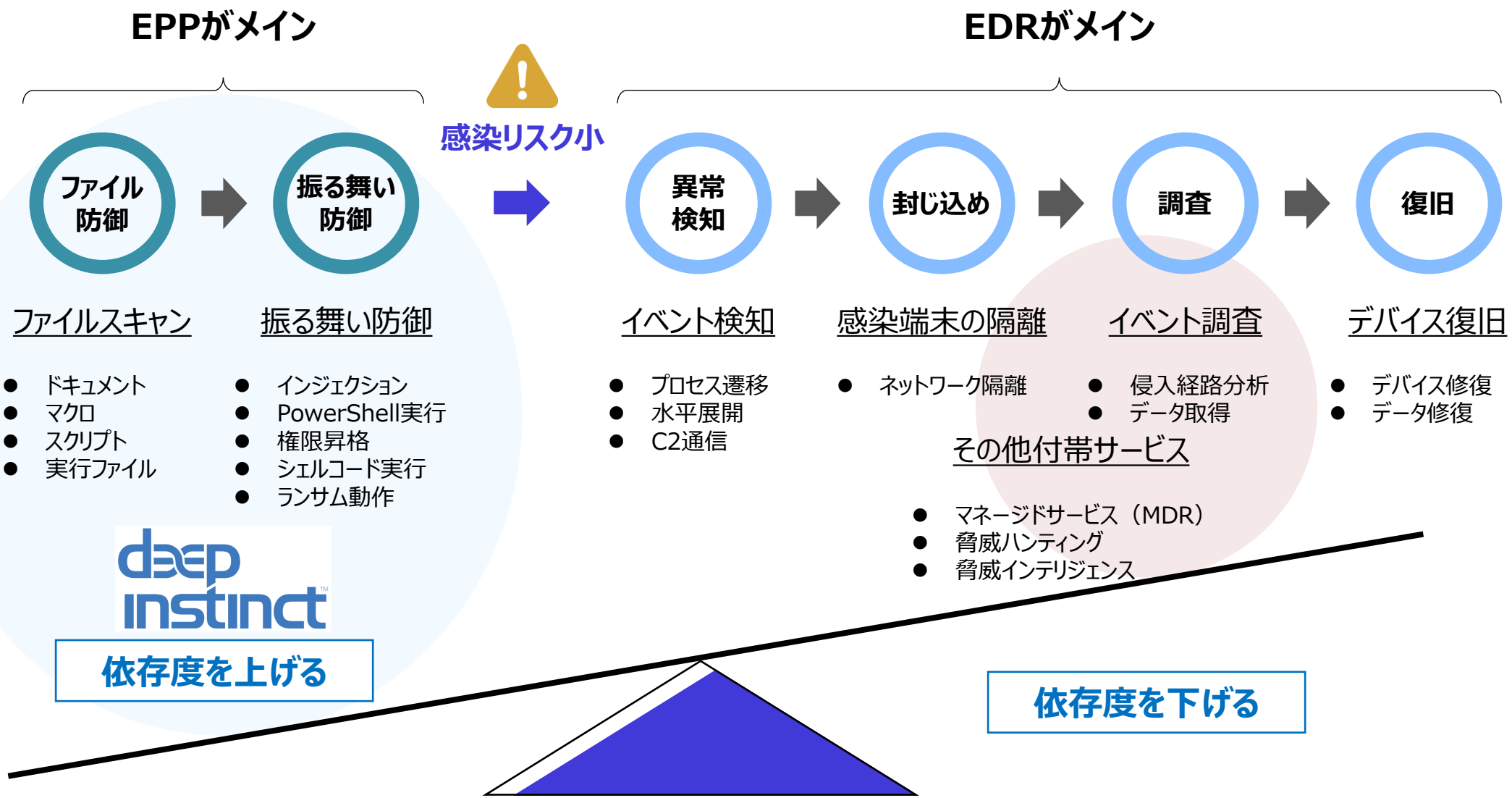
RansomEXX
22ヶ月以上前 のモデルで検知

DarkSide Ransomeware
18ヶ月以上前 のモデルで検知

Pandra
26ヶ月以上前 のモデルで検知

Panasonic

EPPとEDRの守備範囲：本来あるべき姿



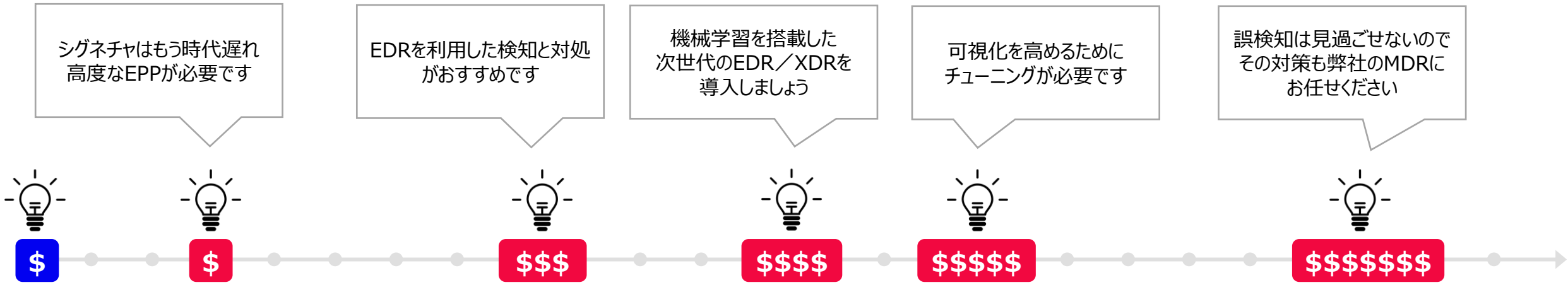
EPP（Endpoint Protection Platform）：エンドポイント保護プラットフォーム
EDR（Endpoint Detection and Response）：エンドポイントでの検出と対応

Panasonic

エンドポイントにおける 総保有コスト(TCO)

事後対処が増加すると結果的に**外部サービス**への**依存度も高まる**

シフトライトによるコスト増大



シフトレフトによるコスト削減

セキュリティ運用において**外部サービス**への極度な**依存を減らす**

Panasonic

Deep Instinct の 特徴まとめ

◆ 未知の脅威が予防できる

- 既知や未知問わず幅広い脅威へ対応
  (PE、PDF、Office、PowerShell、Image、Macro、Script等)
- 脅威が実行される前に予防が可能

◆ 幅広いOSサポート

- Windows、macOS、Android、ChromeOS、Linux、iOS
  ※iOSでは静的解析/動的解析の機能は実装されておりません。

◆ 動作が軽い

- 従来のAV製品に比べてリソース消費が少なく、動作が軽い
- 毎日のアップデートやフルスキャンが必要ない

◆ オフラインでも動作

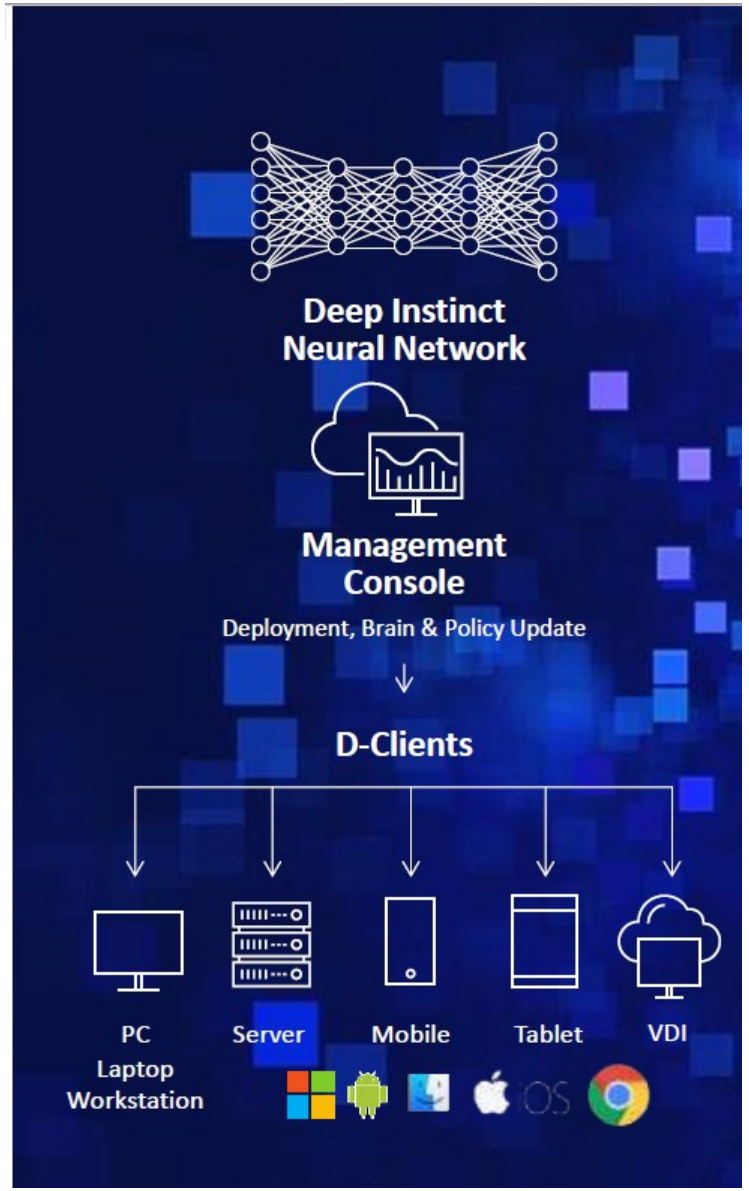
- 検知能力はインターネット接続有無に依存せず

◆ 運用の簡易性

- シグネチャ更新やフルスキャンの定常運用が必要ない
- 新しいマルウェアに対応するための緊急アップデートも不要
- 振る舞い検知と比べてアラートが少なく運用負荷が低い

◆ 総保有コスト（TCO）の削減

- 予防効果により事後対策に係るコストを大幅に削減



Panasonic

まとめ

- ✓ 既知だけではなく未知のマルウェアも**実行前に防御**
- ✓ 精度の高いモデルによる**99%以上**の検知率
- ✓ 従来製品の運用に比べ、管理負荷を**大幅削減**

deep instinct™

未知のマルウェア対策は Deep Instinct にお任せください！

パナソニックISは情報技術開発株式会社様と連携し、セキュリティソリューションを提供いたします。

Panasonic

Chapter - 4

パナソニック インフォメーションシステムズについて

ONE Panasonic IT

私たちの使命

デジタルと人の力で
「くらし」と「しごと」を幸せにする。

PX Panasonic Transformation

MISSION

お客さま、お取引先さま、従業員に、
ITによる本質的な価値を提供、経営に直接貢献。

ITを創る喜びを

- お客さまの → 便利と嬉しいへ
- お取引先さまとの → シナジーへ
- 従業員の → キャリア形成と成長へ

VISION

私たちはビジネスに寄り添う、Co-Creatorです。
お客さまの「くらし」と「しごと」を共に考え、共に創ります。

私たちはInnovatorです。
新しい技術、働き方で、スピーディに、想像の先を実現します。

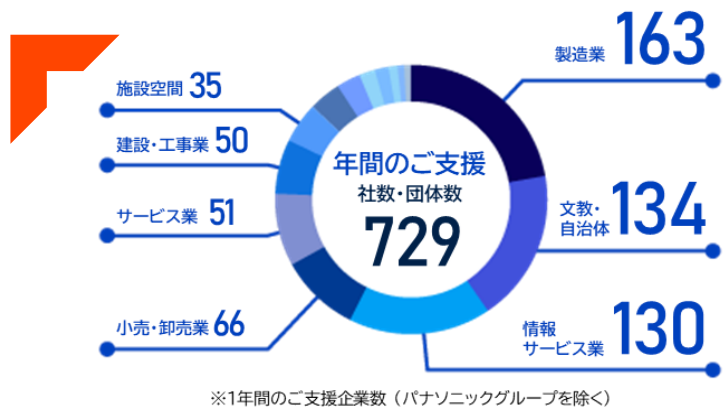
私たちはOne Panasonic ITです。
認め合い、学び合い、高め合って、皆で成長し続けます。

VALUE

- **想像、その先を創造**
  お客さまの夢をかなえるために ITの匠集団として、想像の先を創造する
- **多様性、信頼、成長**
  多様性を認め合い、時にぶつかり、高め合う
- **速く、広く、深く、つなぐ**
  つなぐ価値を最大化 ビジネスとIT、人や組織、人のこころをつなぐ
- **データが語る、語らせる**
  答えのヒントはデータにある。データに語らせる
- **衆知・自律化集団**
  全員参加で衆知を集め、変革を常態化
- **主役は、「わたし」**
  変革の主役は「わたし」

一般市場向けビジネス

パナソニックグループでの挑戦を通じ、B2B市場へ価値を提供



※1年間のご支援企業数（パナソニックグループを除く）

データ統合・活用
クラウド連携
システム統合
企業間取引
データ戦略

働き方改革
テレワーク
RPA
勤務管理
クラウドストレージ

施設空間
チケッティング
POS
会員管理
データ分析

基幹業務
製造業務
販売業務
CRM
文書管理

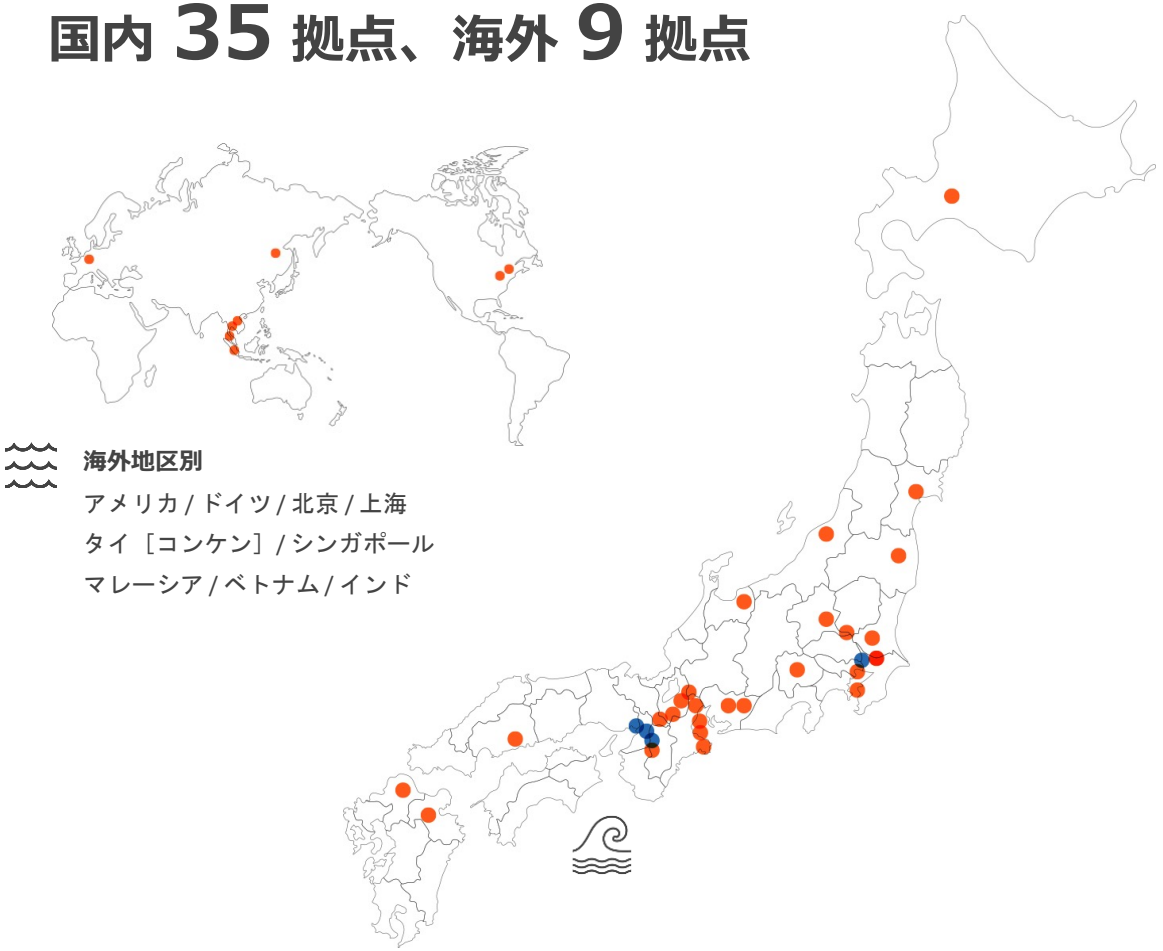
製造現場支援
製造IoT
映像監視
フィールド業務支援
業務モバイルアプリ

文教・自治体
PC教室管理
BYOD
教員用端末
教務支援

会社概要

会社名	パナソニックインフォメーションシステムズ株式会社
本社所在地	大阪　〒530-0013 大阪府大阪市北区茶屋町19番19号 TEL：06-6906-2801（代表） 東京　〒104-0061 東京都中央区銀座8丁目21番1号 TEL：03-5148-5634（代表）
設立年月日	1999年2月22日
事業内容	情報サービス
資本金	1,040百万円
主要取引銀行	三井住友銀行 大阪本店営業部 三井住友信託銀行 大阪本店営業部
許認可など	特定建設業 電気通信工事業　（特-3）第157588号 一般建設業電気工事業　（般-3）第157588号 届出電気通信業者　E-63-00084
関係会社	親会社　パナソニックホールディングス株式会社 連結子会社　パナソニック ネットソリューションズ株式会社 松下信息系統（上海）有限公司

国内 35 拠点、海外 9 拠点



海外地区別
アメリカ / ドイツ / 北京 / 上海
タイ［コンケン］/ シンガポール
マレーシア / ベトナム / インド

Deep Instinctについてもっと詳しく知りたい方へ

お問い合わせや無料相談をご利用ください

お問い合わせ