最新の統計や金融庁の報告から考える！
今求められるランサムウェア対策とは

東京エレクトロン デバイス株式会社

CN BU CN営業本部
アカウント第二営業部
寺田涼太

目次

- ランサムウェアの現状
- 金融業界におけるランサムウェア対策
- 東京エレクトロンデバイスが提案するランサムウェア対策ソリューション

ランサムウェアの現状

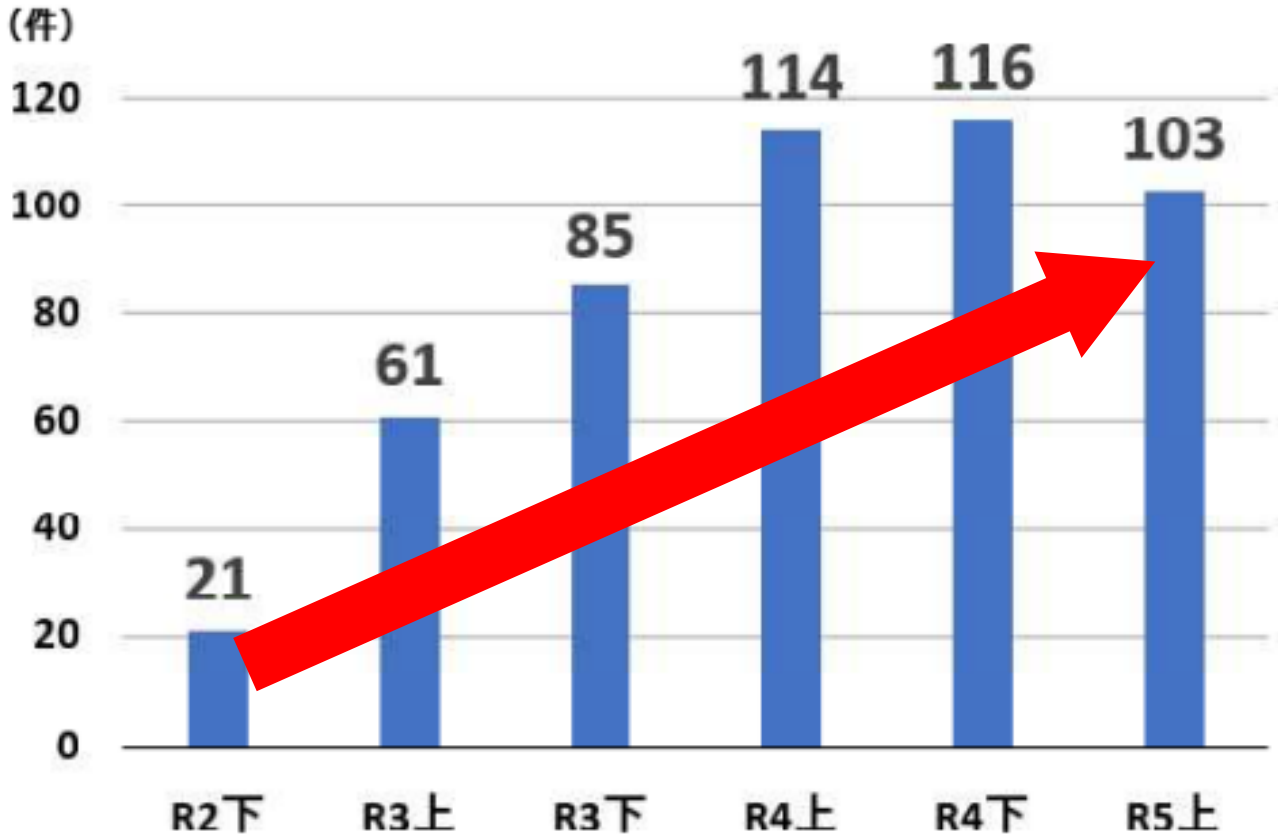
IPA「情報セキュリティ10大脅威」

ランサムウェアによる被害は4年連続で1位の脅威

順位	組織	2023年	2022年	2021年
1位	**ランサムウェアによる被害**	**1位**	**1位**	**1位**
2位	サプライチェーンの弱点を悪用した攻撃	2位	3位	4位
3位	内部不正による情報漏洩	4位	5位	6位
4位	標的型攻撃による機密情報の窃取	3位	2位	2位
5位	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	6位	7位	5位

出典：IPA情報セキュリティ10大脅威 2024

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



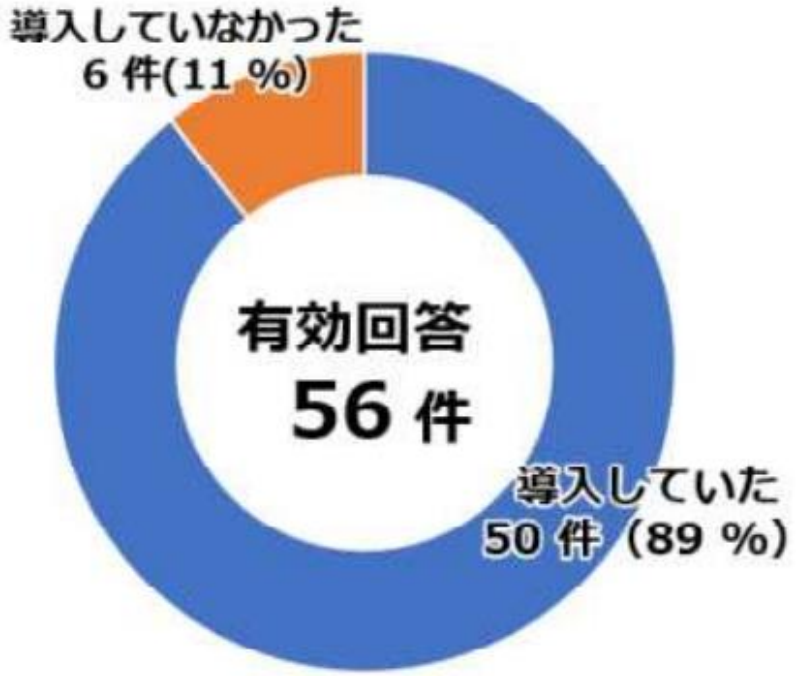
2020年下期から
被害件数が5倍増

出典：令和5年上半期におけるサイバー空間をめぐる脅威の情勢等について（警察庁）

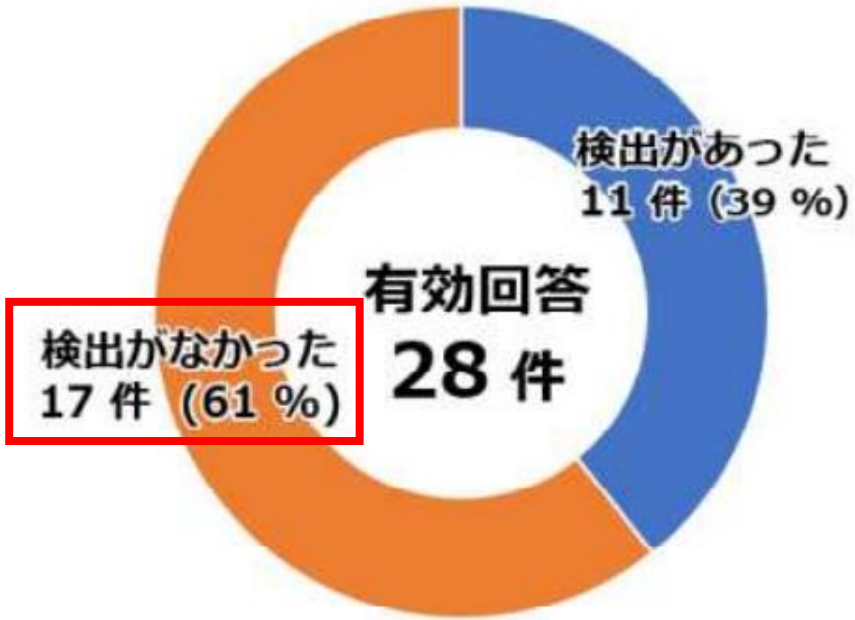
ウイルス対策ソフト等の導入・活用状況

対策ソフトを導入していながら60%は検出できず

導入状況



検知の有無



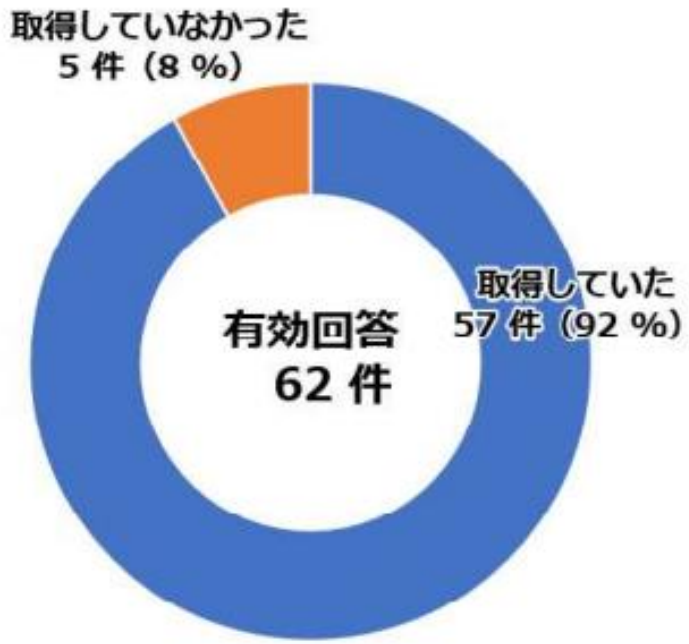
侵入を前提としてランサムウェア攻撃の振る舞いを検出できる仕組みが必要

出典：令和5年上半期におけるサイバー空間をめぐる脅威の情勢等について（警察庁）

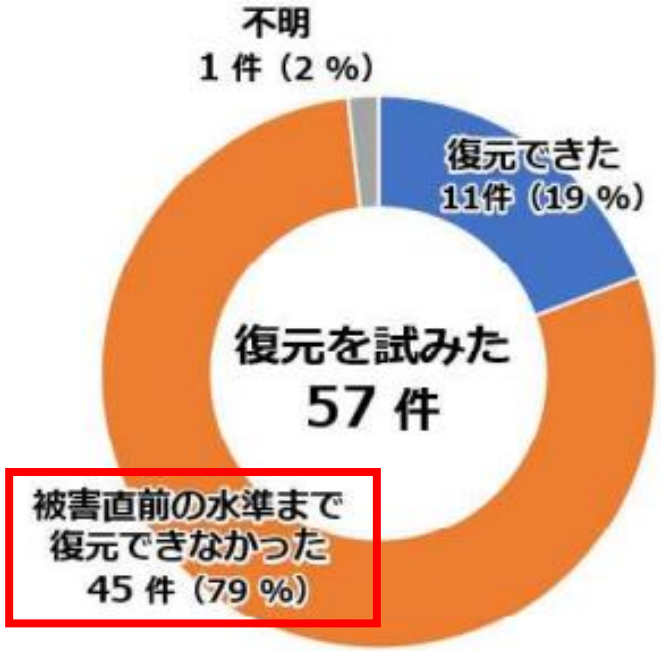
バックアップの取得・活用状況

バックアップを取得していても80%は復元できなかった

取得有無



復元結果



復元できなかった理由

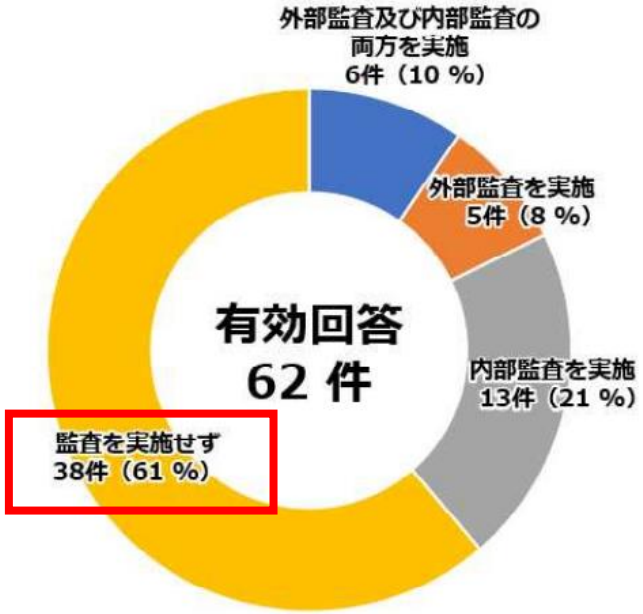
バックアップも攻撃対象であるという前提で確実にデータを保護・復旧できる仕組みが必要

出典：令和5年上半期におけるサイバー空間をめぐる脅威の情勢等について（警察庁）

セキュリティ監査・診断の有無

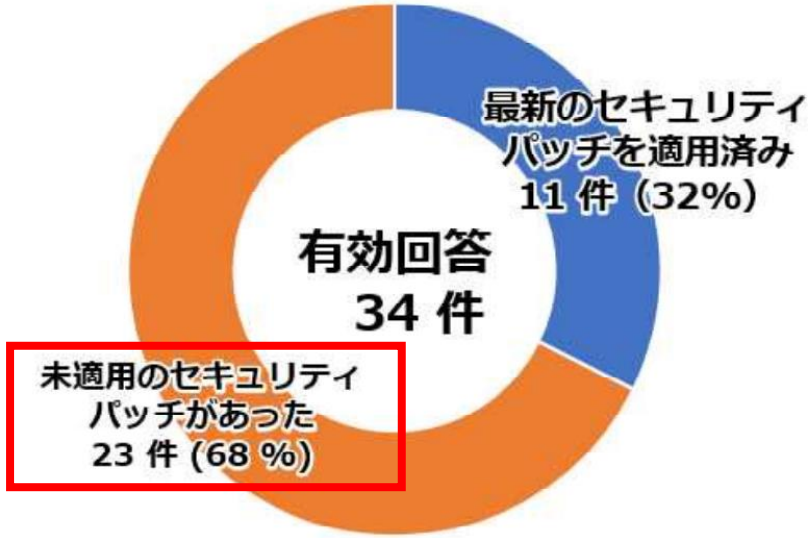
60%は監査を実施せず

セキュリティ監査実施状況



68%は未適用の
セキュリティパッチがあった

侵入経路とされる機器の
セキュリティパッチの適用状況



自社のセキュリティ状況を定期的に可視化・改善する仕組みが必要

出典：令和5年上半期におけるサイバー空間をめぐる脅威の情勢等について（警察庁）

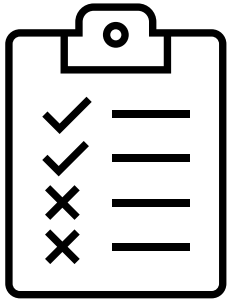
今求められる対策とは？

エンドポイントを守る

“侵入前に全てを防ぐのは不可能”
を前提とした高度な振る舞い検知

データを守る

“バックアップも攻撃対象である“
ことを前提とした確実なデータ保護
と復旧



セキュリティを評価する

継続的な評価を行うことで
自社のセキュリティ状況を定期
的に可視化・改善

ランサムウェアに対する
セキュリティの有効性確認

金融業界において求められる
ランサムウェア対策

金融分野におけるサイバーセキュリティ強化に向けた取組方針(Ver.3.0)

（1）モニタリング・演習の高度化

（a）大手行等
海外大手金融機関における先進事例を参考にしたサイバーセキュリティの高度化に着目しつつ、
通年検査においてサイバーセキュリティ管理態勢を検証する。

（b）地域金融機関
金融機関がリスク管理を高度化すべき範囲が拡大している中で、**サイバーセキュリティに関する基礎的な管理態勢の実効性を向上させるために、継続的な取組みが必要である。**

（c）その他業態
証券会社や外国為替証拠金取引業者、保険会社等については、サイバーセキュリティに関する基礎的な取組みにおいて進捗が認められる一方、インシデントも複数発生していることを踏まえ、**引き続き、検査・モニタリングを通じて、サイバーセキュリティ管理態勢を検証する。**

金融機関はそれぞれの規模・特性に応じ、サイバーセキュリティ管理態勢を整備し、実効性を確保する必要があるが、
これまで、**他の金融機関対比での自組織の位置付けや改善すべき領域を特定するツールが必ずしも広く用いられてこなかった。**

➢ 業種、規模問わず、サイバーセキュリティ管理態勢の検証が求められている

出典：金融分野におけるサイバーセキュリティ強化に向けた取組方針（Ver. 3.0）

金融分野におけるサイバーセキュリティ強化に向けた取組方針(Ver.3.0)

（2）新たなリスクへの備え - ③サイバーハイジーンの徹底

高度化するサイバー攻撃に対する防御として、高機能なセキュリティ製品を導入するなど技術的施策が有効だが、インシデントの原因には、
ソフトウェアの脆弱性へのセキュリティパッチの適用漏れなど、基本的な行動が徹底されていない事例も見られる。

特定のセキュリティ製品だけに依存することなく、IT 資産の適切な管理、速やかなセキュリティパッチ適用などの
基本的な行動を組織全体に浸透させる取組み（いわゆるサイバーハイジーン）が重要。

- **高機能なセキュリティ製品の導入だけでなく、脆弱性対応やセキュリティパッチ適用、IT資産の管理等の基本的な行動が重要**

出典：金融分野におけるサイバーセキュリティ強化に向けた取組方針（Ver. 3.0）

金融セクターのランサムウェアに対するレジリエンスに関するG7の基礎的要素

要素6：インシデントからの復旧

サイバーセキュリティ管理の範囲は、インシデントの未然防止から、インシデント発生時の検知、特定、対応、業務の早期復旧や顧客影響の軽減といった**レジリエンス（いわゆる復元力）の強化**へと拡がっている。

金融機関においては、未然防止の施策に加え、インシデントによって業務が中断した場合も、業務や顧客への影響を許容水準内に収めるよう、訓練・テスト等を通じて、**業務やサービスの強靭性や冗長性を高めることが一層求められている。**

金融機関は、**ランサムウェアへのレジリエンスをもたらす特徴を備えたバックアップ戦略を検討すべき**である。
これらのソリューションには、**保存されたデータの改変、削除、又は暗号化*を防止するシステムが含まれ得る。**

金融機関は、**ランサムウェアがバックアップデータの感染を試みようとしている**かもしれず、かつ、
ランサムウェア攻撃自体が明らかになるよりも**かなり前から感染を開始しているかもしれないことを考慮すべき**である。

*これらの品質の一部又は全部を備えたバックアップ技術は**「イミュータブル」**と呼ばれることがある。

- **インシデント発生時の検知、特定、対応、復旧といったレジリエンス強化が重要**
- **データの改変、削除、暗号化を防止できるイミュータブルなバックアップが必要**

出典：金融セクターのランサムウェアに対するレジリエンスに関するG7の基礎的要素（仮訳）

東京エレクトロンデバイスが提案する
ランサムウェア対策ソリューション

東京エレクトロンデバイスが提案するランサムウェア対策ソリューション

エンドポイントを守る

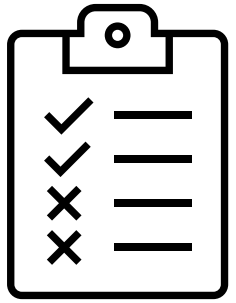
SentinelOne

自律型EDR

データを守る

rubrik

高度なデータ保護機能を持つバックアップ



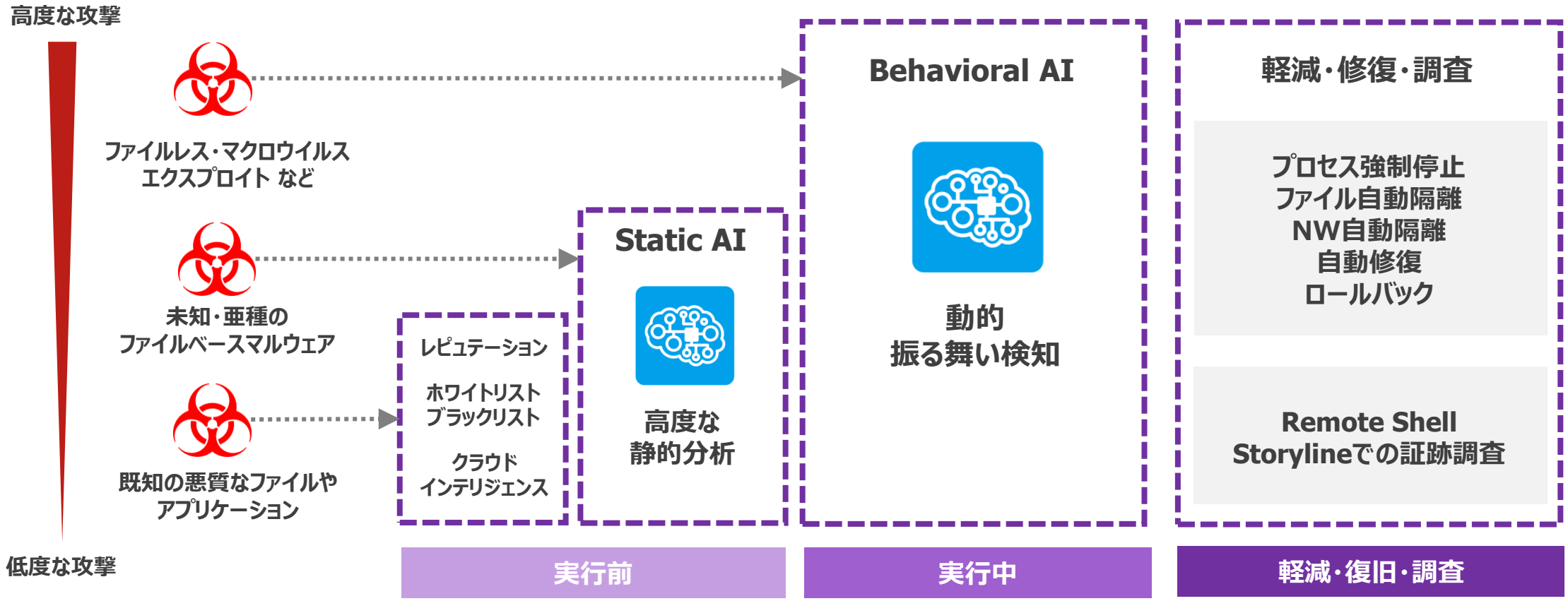
セキュリティを評価する

PENTERA

自動セキュリティ診断プラットフォーム

SentinelOne：自律型EDR

- AIを搭載した自律型EDR・サイバーセキュリティプラットフォーム



SentinelOneの特徴

高い検知力

- 2種類のAIエンジンによる多段検知
- MITREの評価結果に裏付けられた検知力

人手に頼らない インシデント対応

- 端末内の挙動分析を自動化
- 検知・防御・軽減・修復を自動実行

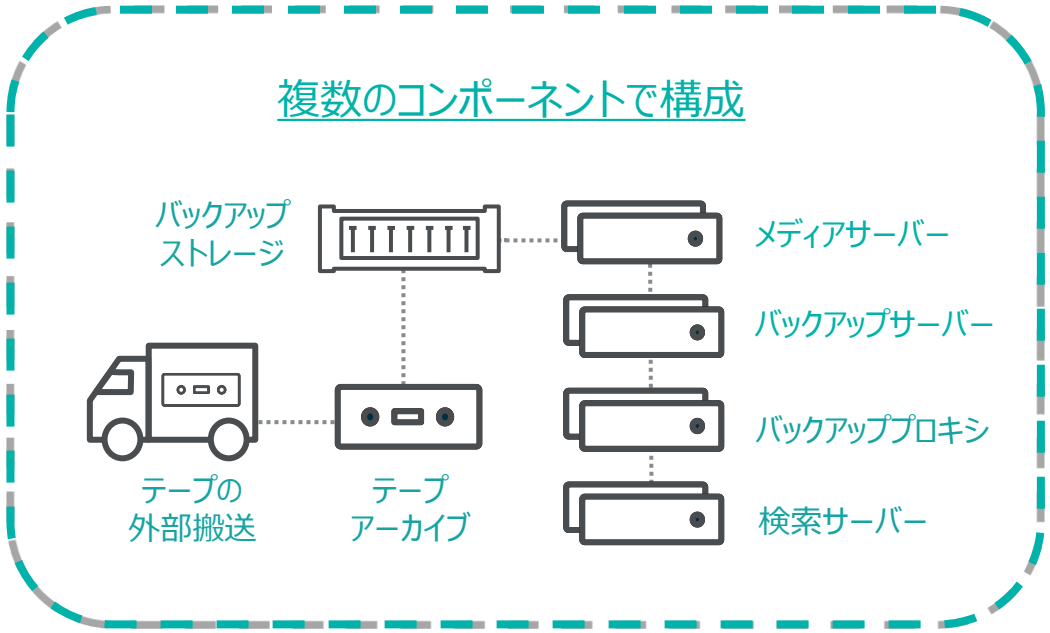
マルウェア感染からの 修復力

- マルウェアによる汚染箇所を完全修復
- ランサムウェアに暗号化されたファイルもロールバック

Rubrik：高度なデータ保護機能を持つバックアップ

はじめに、Rubrikとは？

従来のバックアップ環境



Rubrikが実現するバックアップ環境

1台でバックアップ環境を実現

Rubrikが提供する高度なデータ保護機能

データレジリエンス

- イミュータブル（変更不可）システムによる暗号化防止
- エアギャップ技術による不正アクセスの防止

データオブザーバビリティ

- 過去のバックアップデータとの差異を機械学習により分析
- ランサムウェアを検知し、安全なデータからの復旧を支援

データリカバリ

- インスタントリカバリ機能などの多彩なリストア方式
- 暗号化されたファイルをピンポイントで特定し迅速に復旧

Pentera：自動セキュリティ診断プラットフォーム

PENTERA

onnect Beyond

- **攻撃者視点での診断を自動化し、継続的な診断によりセキュリティ耐性を把握する**

ペネトレーションテストを自動化

対象のIPアドレスレンジのスキャンからテスト実施、
その後のレポート発行までを自動化

攻撃の可視化と優先修復

攻撃の全てのステップを提示
脅威に直面する可能性が高い順に修復手順を提示

エージェントレススキャン

稼働しているシステムへの変更は不要

ASMとBAS

ASM
（Attack Surface Management）

組織の外部（インターネット）からアクセス可能な
IT資産を発見し、それらに存在する脆弱性などの
リスクを継続的に検出・評価する一連のプロセス

Pentera Surface

**IT資産の発見、脆弱性の把握だけでなく
疑似攻撃による本当のリスクを可視化**

BAS
（Breach and Attack Simulation）

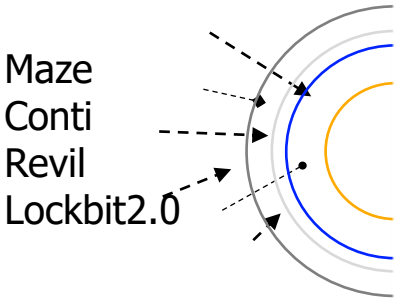
組織内に存在するセキュリティインフラに対して
攻撃者が実際に使用するテクニックを用いた
攻撃をシミュレーションするツール

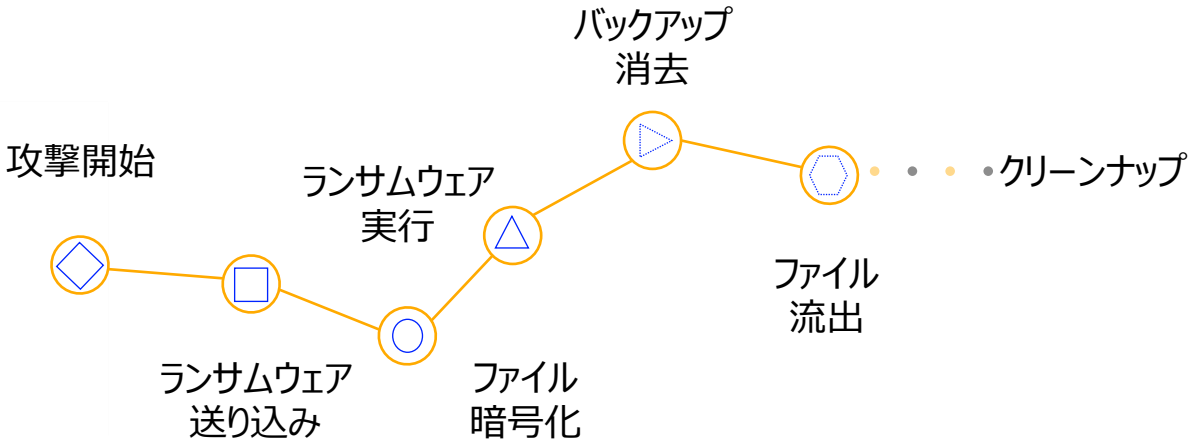
Pentera Core

**シミュレーションではない疑似攻撃によって
本当に対策が必要な箇所を把握**

ランサムウェア診断機能

実在する攻撃者グループをシミュレート

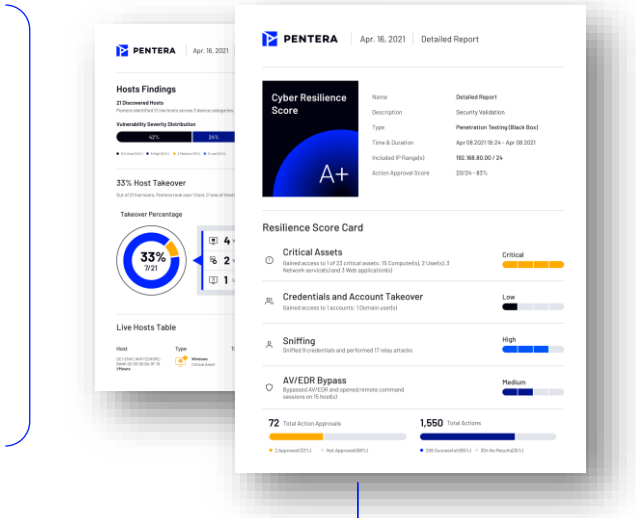




マルウェアの送り込みから情報流出までのフローを再現

MITRE ATT&CK フレームワークへのマッピング

ランサムウェアに特化したレポート



セキュリティ製品有効性

脆弱性 & 攻撃結果

対処方法

ランサムウェアグループによる攻撃フロー全てを忠実に再現
想定被害範囲やセキュリティの有効性、利用された脆弱性や対処方法等を提示

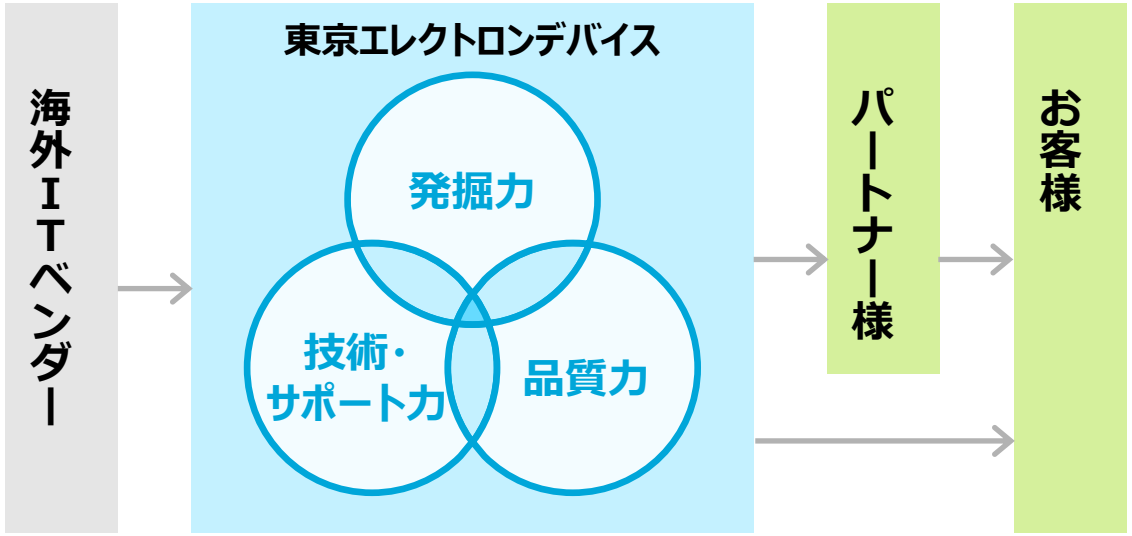
東京エレクトロン デバイス

東京エレクトロンデバイス 会社紹介

会社概要

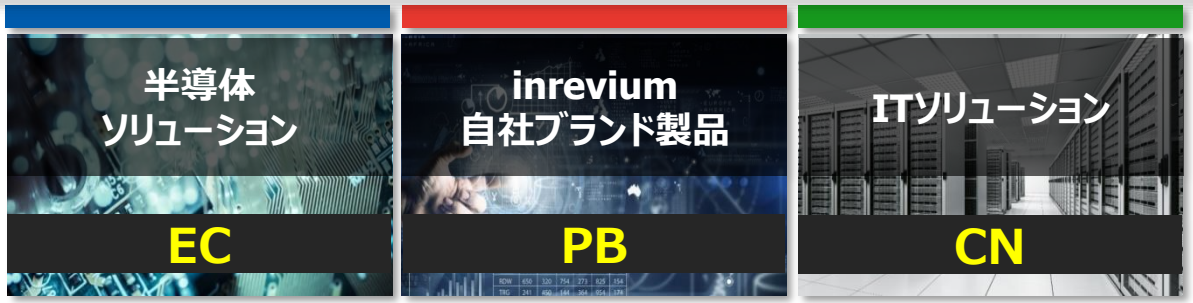
会社名	： 東京エレクトロン デバイス株式会社（TED）
設立	： 1986年3月3日
代表	： 代表取締役社長　徳重　敦之
株式	： 東京証券取引所 プライム市場（証券コード：2760）
資本金	： 24億9千5百万円
売上高	： 2,403億50百万円（2023年3月期）
従業員	： 連結: 1,318名（2023年3月31日現在）

CN BU



「**発掘力**」「**技術・サポート力**」「**品質力**」を活かし
お客様が求める最先端技術を「**高品質**」で提供

事業内容



CNフォーカスエリア

取り扱いソリューション

Connect Beyond

Security

テレワーク/クラウドアクセス関連ソリューション

ZTNA	SWG	CASB	IDaas
SSE/SASE netskope			SSO/多要素認証 okta

エンドポイント	HSM	シークレット管理
Active EDR/XDR SentinelOne	ENTRUST THALES	Hashicorp HashiCorp Vault

社内/トラストネットワーク関連ソリューション

Firewall	VPN	WAF
paloalto NETWORKS FORTINET	f5	f5 Distributed Cloud Services

Wi-Fi	DNS/DHCP	NDR
Cognitive Wi-Fi ARISTA Extreme networks	infoblox.	ARISTA

脆弱性対策

ASV
AI PenTest、ASM PENTERA

その他取扱い製品

その他の取り扱い製品については
以下のWebよりご覧ください。

https://cn.teldevice.co.jp/

Infrastructure

クラウド管理

CSPM/SSPM	IaC	CNAPP
netskope	Hashicorp HashiCorp Terraform	WIZ

クラウド

パブリッククラウド	
aws	Azure

AI/DLソリューション

GPU	Accelerator
NVIDIA	cerebras

仮想化基盤ソリューション

HCI	3Tier
NUTANIX	PURESTORAGE

ファイルストレージソリューション

Scale Out		Scale Up
Power Scale DELL Technologies	PURESTORAGE	Unity XT DELL Technologies

ネットワークソリューション

IP Clos	L2/L3スイッチ		ADC
JUNIPER NETWORKS	DCNW ARISTA NVIDIA	キャンパス Extreme networks	f5

バックアップソリューション

クラウドバックアップ対応	
rubrik	VEEAM

東京エレクトロン デバイス

本日のまとめ

エンドポイントを守る

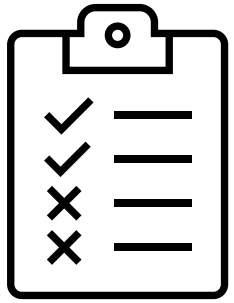
SentinelOne

自律型EDRで
即時検知、即時対処

データを守る

rubrik

ランサムウェア対策の最後の砦として
高度なデータ保護を実現



セキュリティを評価する

PENTERA

継続的な診断による
ランサムウェアへの耐性評価、改善

各製品の詳細を知りたい方はアンケートに製品名をご記入ください

onnect Beyond

共に創る　新たな価値を

東京エレクトロン デバイス