



金融業界に欠かせないデータ保護！ ランサムウェア対策を強化する バックアップのポイント

東京エレクトロン デバイス株式会社

CN営業本部 アカウント第二営業部

寺田 涼太・久山慶

※本資料に掲載されている会社名・製品・サービス名・ロゴは各社の商標または登録商標です。
また、写真・ロゴマーク・その他の著作物に関する著作権はそれぞれの権利を有する各社に帰属します。

- 01** **金融業界で求められるバックアップ.....P.5**
- 02** **東京エレクトロンデバイスが提案するバックアップソリューション.....P.15**
- 03** **東京エレクトロンデバイスの紹介とまとめ.....P.27**



- 東京エレクトロン デバイス株式会社（TED）
- CN BU アカウント第二営業部
- 寺田 涼太（てらだ りょうた）
- 経歴
 - ✓ 2021年4月：入社（アカウント第二営業部 第一グループ）
 - ✓ 2023年4月：アカウント第二営業部 インサイドセールスグループ
 - ・ 新規顧客開拓をミッションとした営業活動
 - ・ 金融業界向けの営業活動（業界分析やソリューション提案、セミナー開催）
 - ・ 自動ペネトレーションテストツール「Pentera」のプロダクト担当
 - ・ セキュリティソリューション拡販のプロジェクトメンバー
- 趣味
 - サウナ
 - 美味しいものを作ること、食べること、飲むこと

- **知識：金融業界におけるバックアップ戦略のポイントを理解する**
- **解決策：ランサムウェア対策に有効なバックアップソリューションを知る**
- **次の一歩：バックアップ体制強化に向けた計画のための材料を手に入れる**

01

金融業界で求められるバックアップ.....P.5

02

東京エレクトロンデバイスが提案するバックアップソリューション.....P.15

03

東京エレクトロンデバイスの紹介とまとめ.....P.27

金融業界では・・・

1. 「ランサムウェア対策」を意識したバックアップが重要

2. 意識すべき重要な要素は「イミュータブル」

※データの改変、削除、暗号化を防止できる機能を持つバックアップ



金融庁のガイドライン等について

2.3.3 データ保護 【基本的な対応事項】

- **ランサムウェア攻撃のリスクを考慮して**、バックアップ期間や頻度を検討すること。
また、同一ネットワーク内のバックアップファイルを探索して削除するランサムウェアのタイプがあることを踏まえて、
改ざん耐性バックアップシステムの利用、組織内ネットワークから切り離れた複数環境での保管や媒体等へのバックアップ

2.5.2.6 復旧 【基本的な対応事項】

- バックアップからの復旧の際には、攻撃の手法に応じて、**既にバックアップデータ等が改ざんされている可能性や、マルウェア等に感染している可能性に留意**すること。

**ランサムウェア攻撃のリスクを考慮したバックアップシステムの利用
復旧の際にはすでにバックアップデータが改ざんされている可能性などに留意する**

【問28】 重要なシステムにおけるランサムウェア感染等によるデータの破壊を想定したバックアップ対策として、あてはまるものを選択してください。

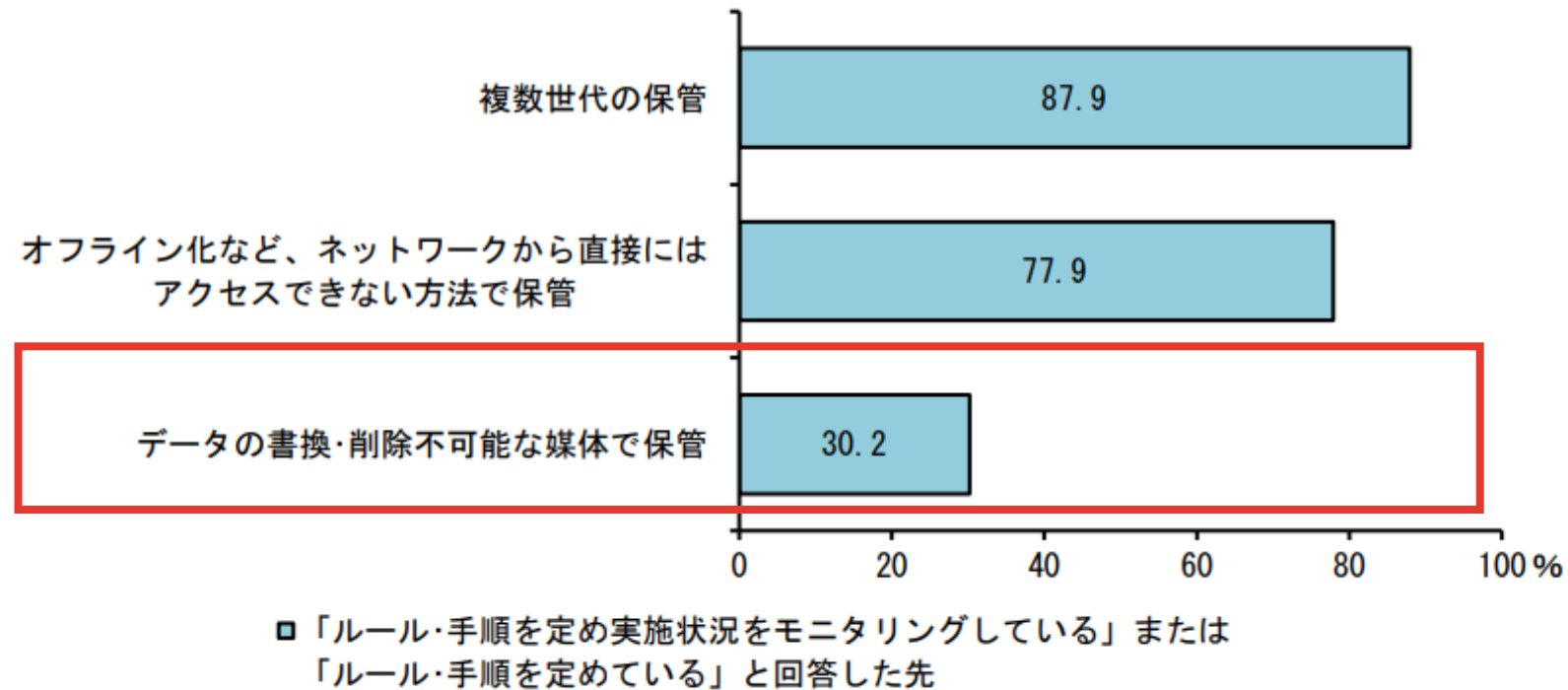
※重要なシステムとは、自組織として業務運営上特に重要と認識しているシステム（例：勘定系、顧客情報を扱うシステムなど）

1. ルール・手順を定めており、対策の実施状況をモニタリングしている
2. ルール・手順を定めている
3. ルール・手順を定めていない

対策	回答欄 (上記1～3から選択)
1. 複数世代の保管	
2. オフライン化など、ネットワークから直接にはアクセスできない方法で保管	
3. データの書換・削除不可能な媒体で保管	
4. バックアップからの復旧テストの定期的な実施	

ランサムウェア感染によるデータの破壊を想定したバックアップが求められている

図表 22 重要なシステムにおけるバックアップデータの破壊・改ざんを想定した対策



早期復旧のためにデータの書換・削除不可な媒体による破壊・改ざん対策が必要

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**へと広がっている。

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**かもしれない、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。

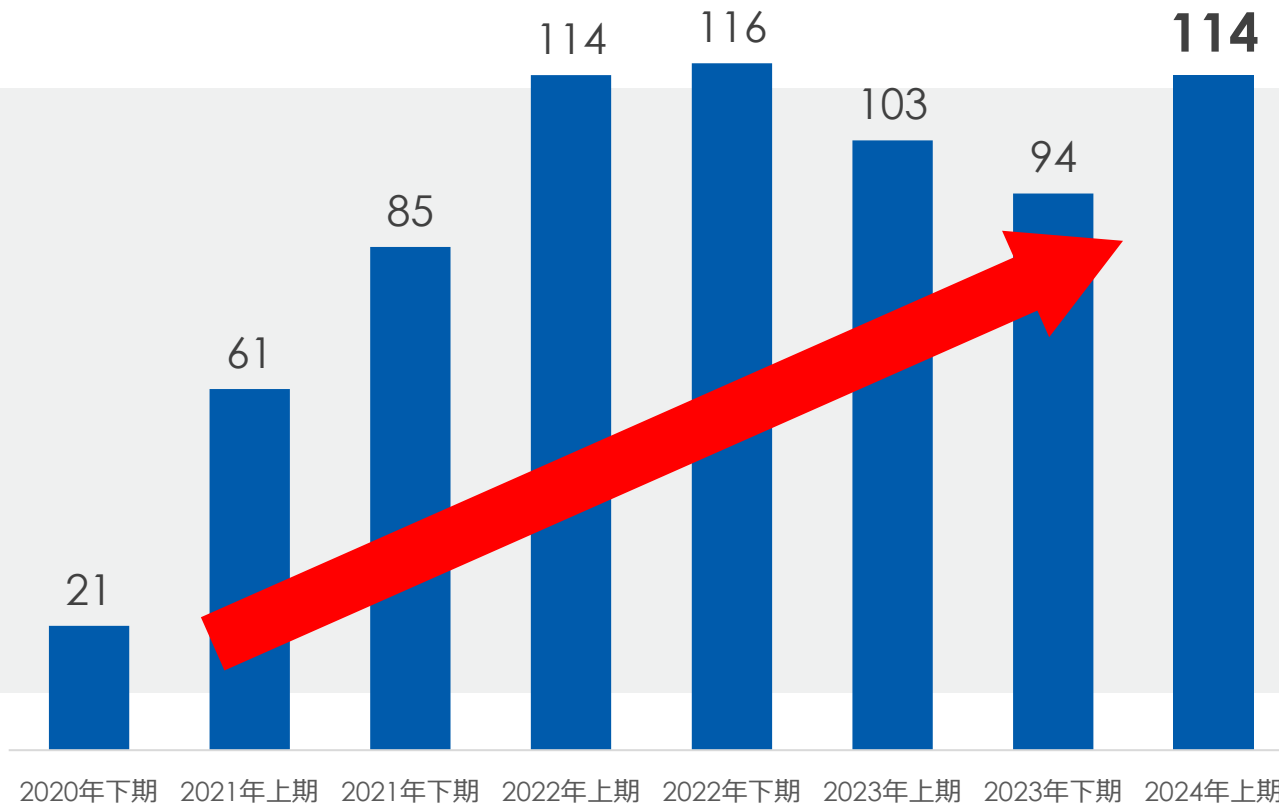
*これらの品質の一部又は全部を備えたバックアップ技術は「**イミュータブル**」と呼ばれることがある。

**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を検討すべき
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**



なぜランサムウェア対策を意識した バックアップが必要なのか？

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年下半期から
被害件数が **5倍** となり

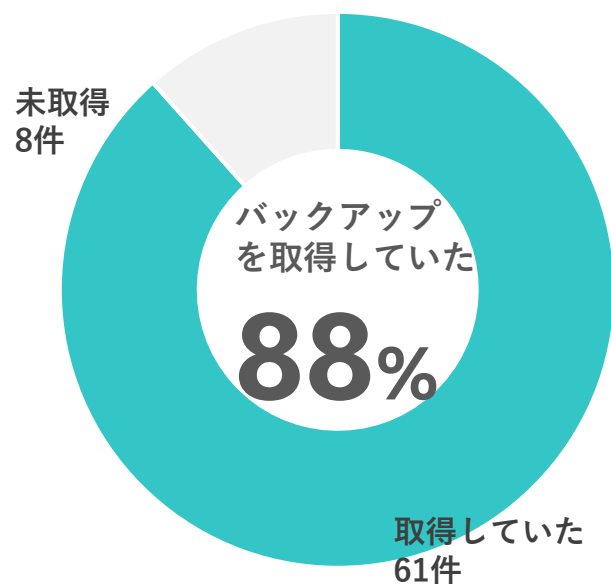
2022年上半期以降

高い水準で推移

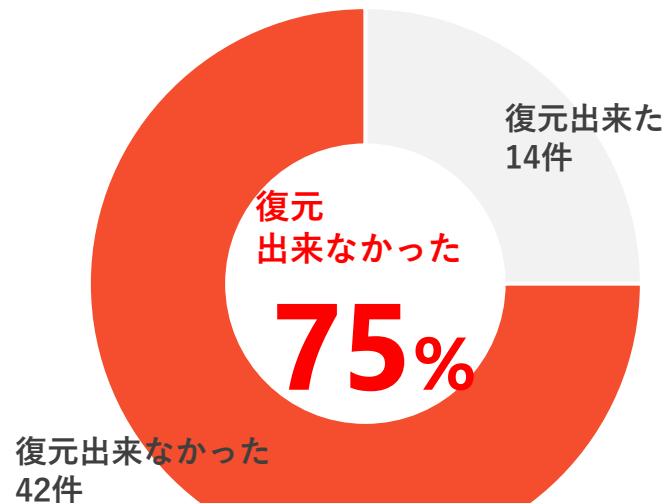
バックアップを取得していても**75%**は復元できなかった

復元できなかった理由の**67%**は暗号化されていた

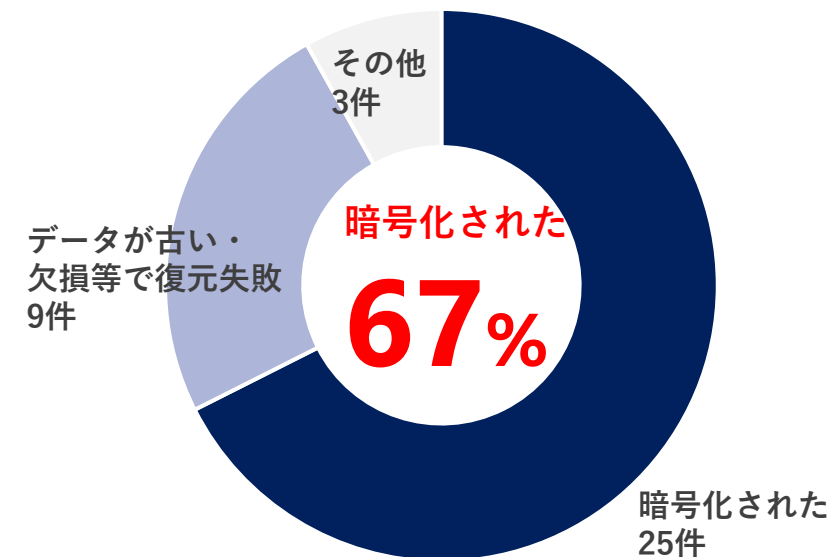
バックアップ取得の有無



復元結果



バックアップを利用して
復元できなかった理由



01 金融業界で求められるバックアップ..... P.5

02 東京エレクトロンデバイスが提案するバックアップソリューション..... **P.15**

03 東京エレクトロンデバイスの紹介とまとめ..... P.27



東京エレクトロン デバイス株式会社（TED）

CN BU アカUNT第二営業部

久山 慶（クヤマ ケイ）

- 担当業務

- ✓ 新規顧客開拓をミッションとした営業活動
- ✓ 金融業界向けの営業活動
（業界分析やソリューション提案、セミナー開催）
- ✓ セキュリティ、AI、Cloudソリューション拡販のプロジェクトメンバー

- 趣味

- ✓ 筋トレ
- ✓ 登山



東京エレクトロンデバイスが提案する バックアップソリューション



- ✓ 多段階のイミュータブル
- ✓ 高度な脅威スキャン
- ✓ 煩雑なジョブ管理を自動化

**セキュリティ要件が重要な
中規模-大規模バックアップ環境におすすめ**



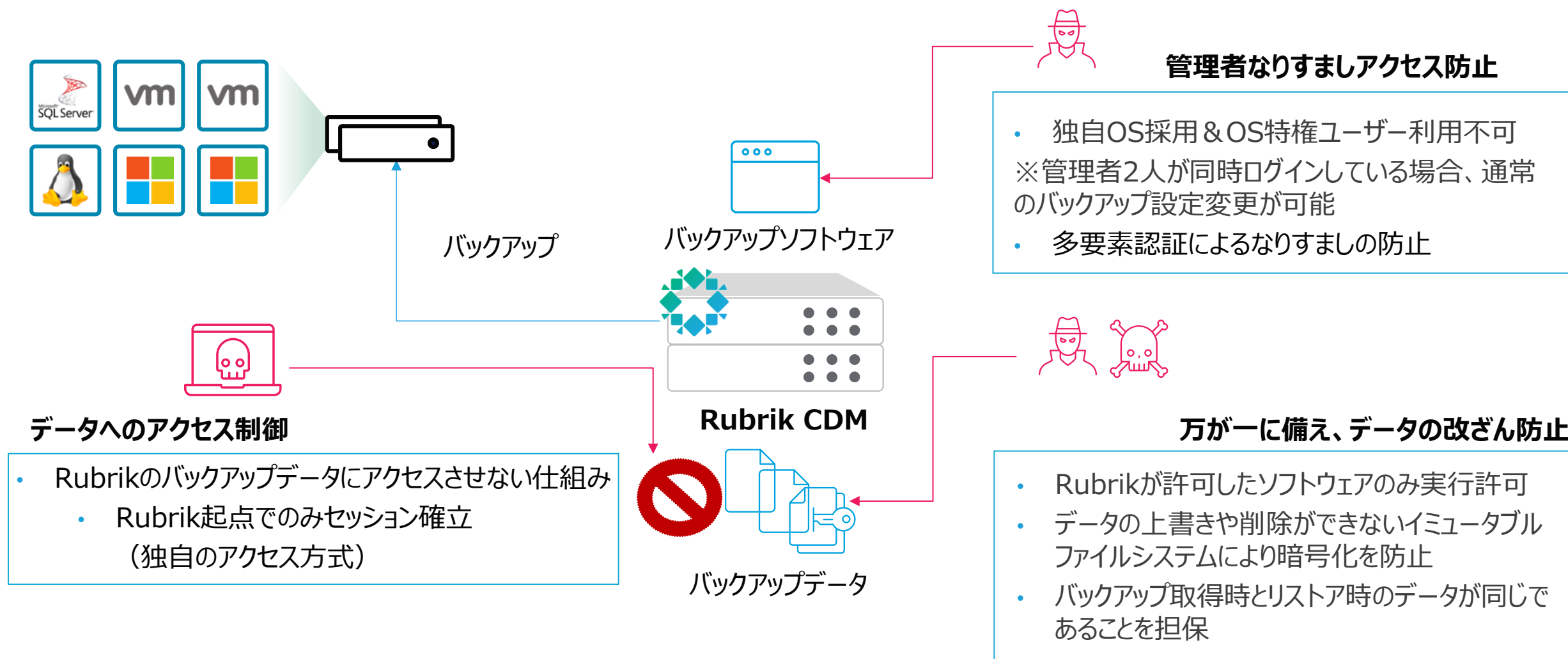
- ✓ 柔軟な構成で実現するイミュータブル&DR
- ✓ 廉価にマルウェアの活動を監視・検出
- ✓ 幅広いバックアップ対象を素早くリカバリ

**コストを抑えつつランサムウェア対策がしたい
小規模-中規模バックアップ環境におすすめ**



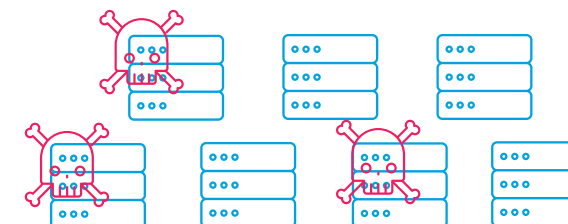
バックアップソリューション Rubrik

Rubrikは多段階にイミュータブルの仕組みを搭載



侵害されたデータをバックアップしてしまった場合、
迅速に下記を判断する必要がある

- ✓ 被害を受けている範囲は？
- ✓ いつから被害を受けているのか？



侵入監視

Threat Monitoring

- バックアップ取得後に自動的にマルウェアの痕跡情報をスキャン
- マルウェアが環境内に存在しているかどうかを監視

マルウェア混入の早期把握

被害検出

Anomaly Detection

- 一連のバックアップデータの変更度合を学習し、データの更新量や、ファイルの追加/削除の量から不審なバックアップデータを特定
- ファイルレベルで、暗号化の有無を分析により検出
- 明確にランサムウェアによるものとわかる場合は、その特定されたランサムウェアの種類を表示

サーバー調査時間短縮：数週間 → 数日

調査

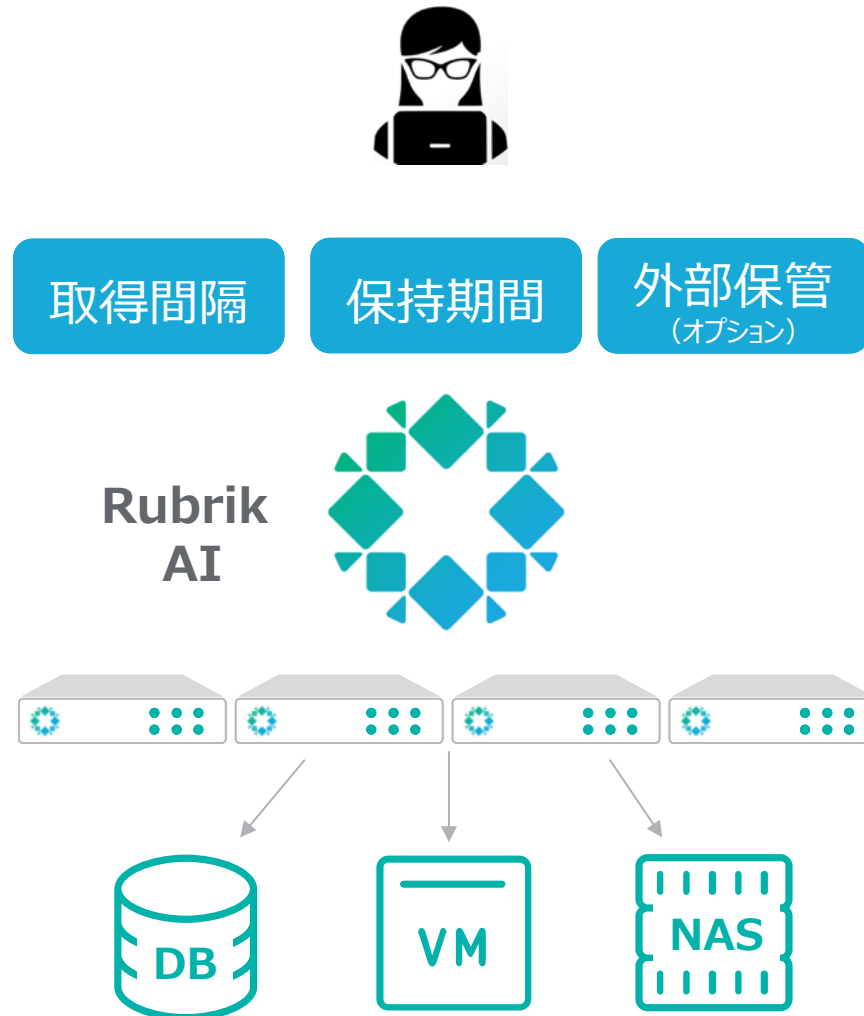
Threat Hunting

- これまで取得してきたバックアップデータ内に、ランサムウェアが存在しているか（痕跡情報のスキャン）を、オンデマンドで一括して分析を実施
- クリーンなバックアップデータ（世代）の特定を支援

リストア調査時間短縮：数週間 → 数日

煩雑なジョブ管理を自動化

Rubrikのポリシーベース・バックアップ



一人のシステム管理者でも

単純なポリシーを設定するだけで

AIが最適なジョブと実行タイミングを
自動生成し

リソース状況を考慮しながら
各ノードにジョブを自動分散

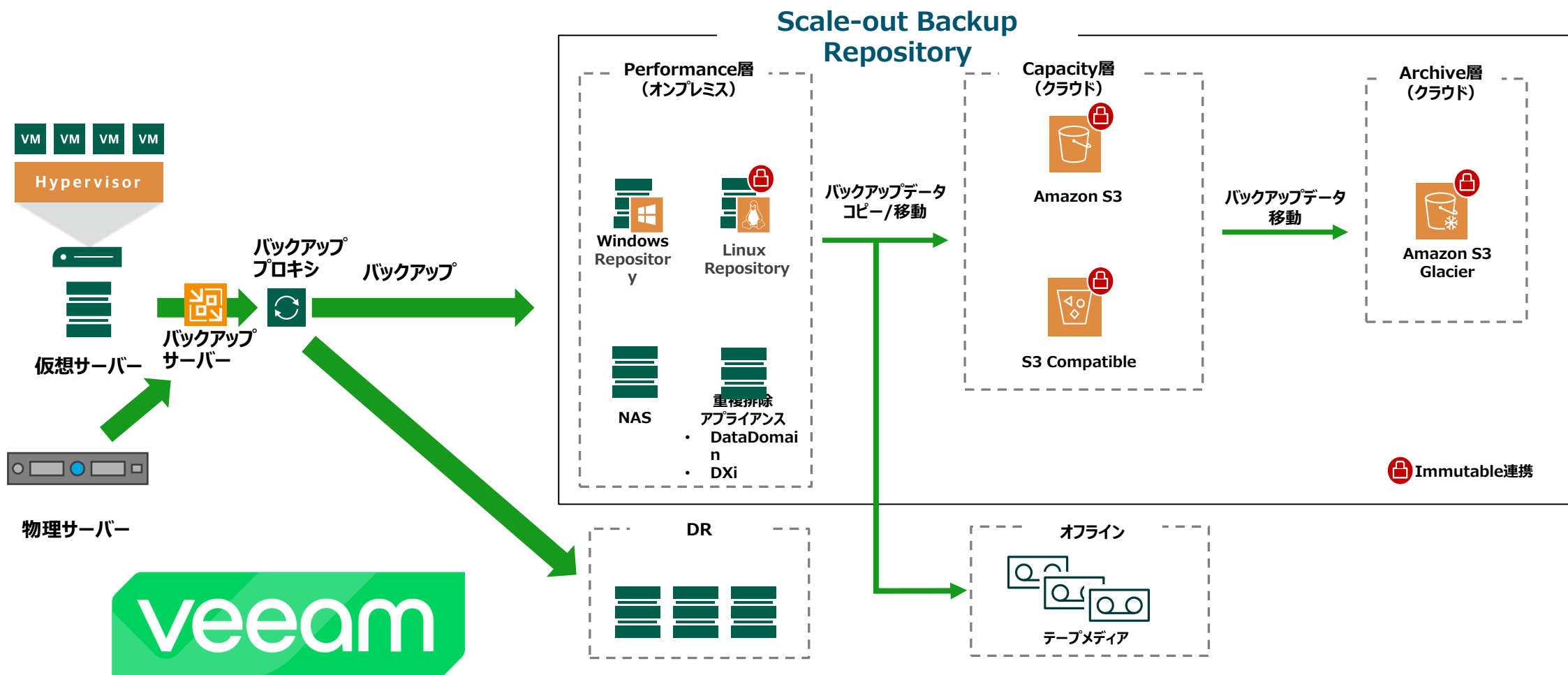
1つのポリシーで
様々なバックアップ対象を保護可能！



バックアップソリューション Veeam

柔軟な構成で実現するイミュータブル&DR

- ✓ Linux Repository もしくはオブジェクトストレージに格納したバックアップデータの改変を防止
- ✓ 物理メディアによる外部保管



※バックアップデータからマルウェアを検出し、疑わしいステータス表示が出た場合、バックアップデータの確認を行う機能でございます

	マルウェア検出方法	スキャンするオブジェクト	対象	ステータス表示
静的検知	シグネチャベースの検出	ゲストインデックスデータ	✓ マルウェアのシグネチャ ✓ 名前変更されたファイル ✓ 削除されたファイル	Suspicious
	ファイルエントロピー分析	データストリーム内のブロックデータ	✓ 暗号化されたファイル ✓ Onion Links ✓ 身代金メモ	Suspicious
	ルールベースの検出（YARA）	復元ポイント	最後のクリーンな復元ポイントを検索	Infected
動的検知	ウイルス対策スキャン	復元ポイント	ウイルス対策対応ソフト（※1）で確認	Infected

※1Veeamと連携が可能なウイルス対策対応ソフト一覧（例）は下記の通りです。



- Symantec Protection Engine
- ESET
- Windows Defender
- Kaspersky Security 10 and 11
- Bitdefender Endpoint Security Tools
- SentinelOne
- Trellix、など

幅広いバックアップ対象を素早くリカバリ



NAS
(Windows, Linux, SMB, NFS)



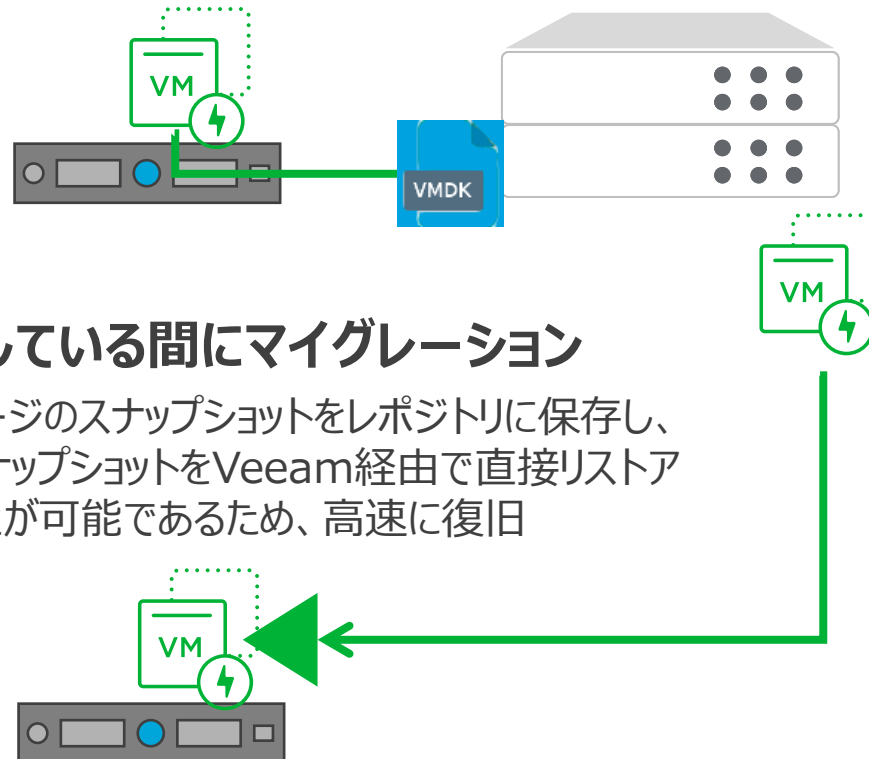
VM
(ESXi, Hyper-v, AHV)



DB
(Oracle, SQL, など)

■ インスタントリカバリ

- 直接バックアップデータをマウントし、数分でVMやデータベースを復旧



■ マウントしている間にマイグレーション

- ストレージのスナップショットをレポジトリに保存し、そのスナップショットをVeeam経由で直接リストアすることが可能であるため、高速に復旧



- 01 金融業界で求められるバックアップ..... P.5
- 02 東京エレクトロンデバイスが提案するバックアップソリューション..... P.15
- 03 東京エレクトロンデバイスの紹介とまとめ..... P.27**



東京エレクトロンデバイスについて

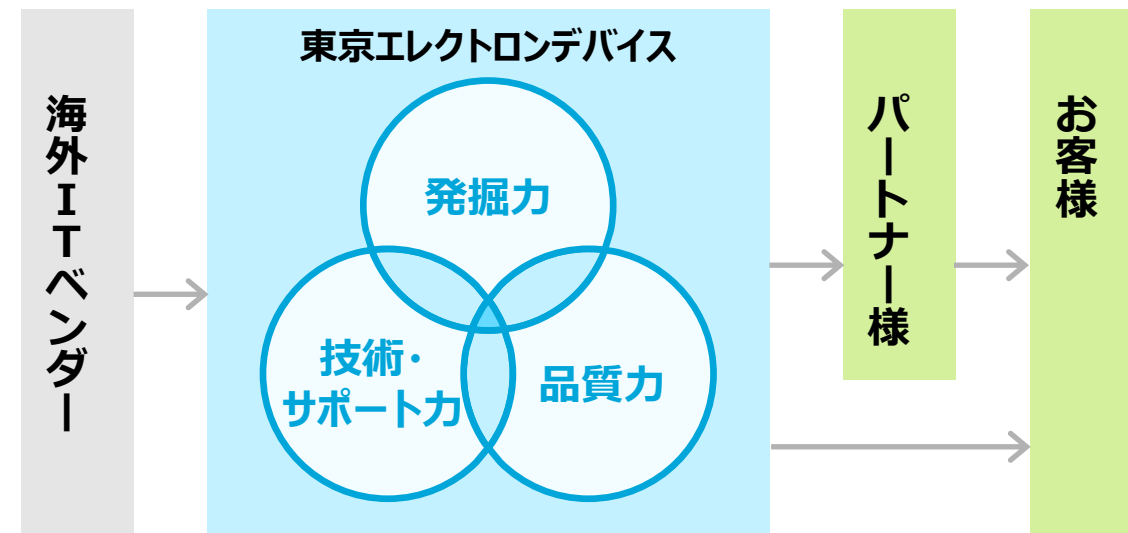
会社概要

会社名	: 東京エレクトロ 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	: 2,428億88百万円 (2024年3月期)
従業員	: 連結: 1,357名 (2024年3月31日)

事業内容



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

CNフォーカスエリア



CN BU ITソリューション一覧

Security

テレワーク/クラウドアクセス関連ソリューション

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



エンドポイント HSM シークレット管理
Active EDR/XDR Hashicorp



社内/トラストネットワーク関連ソリューション

Firewall VPN WAF



Wi-Fi DNS/DHCP NDR
Cognitive Wi-Fi DNSセキュリティ
ARISTA infoblox ARISTA
Extreme networks

セキュリティ診断

ASV

PenTest, ASM



データ分析

SIEM/SOAR/UEBA



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/CNAPP SSPM IaC



クラウド

パブリッククラウド



AI/DLソリューション

GPU Accelerator



仮想化基盤ソリューション

HCI 3Tier



ファイルストレージソリューション

Scale Out Scale Up

Power Scale



Unity XT



ネットワークソリューション

IP Clos L2/L3スイッチ ADC



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の魅力まとめ



- ✓ 多段階のイミュータブル
- ✓ 高度な脅威スキャン
- ✓ 煩雑なジョブ管理を自動化

**セキュリティ要件が重要な
中規模-大規模バックアップ環境におすすめ**



- ✓ 柔軟な構成で実現するイミュータブル&DR
- ✓ 廉価にマルウェアの活動を監視・検出
- ✓ 幅広いバックアップ対象を素早くリカバリ

**コストを抑えつつランサムウェア対策がしたい
小規模-中規模バックアップ環境におすすめ**



共に創る 新たな価値を



東京エレクトロン デバイス