Panasonic

復旧失敗率74%の現実から学ぶ 最新バックアップ戦略 ～従来型では防げないランサム対策を解説～

【講演者】
パナソニック インフォメーションシステムズ株式会社　　花村康充

花村　康充

Hanamura Yasumitsu

パナソニック インフォメーションシステムズ
プラットフォームサービス事業部

アジェンダ

復旧失敗の実態と原因分析

従来型バックアップの限界と“サイバーRTO”の考え方

実践的なバックアップ戦略の設計ポイント

導入事例

実際に導入して分かったメリット/デメリット

まとめ

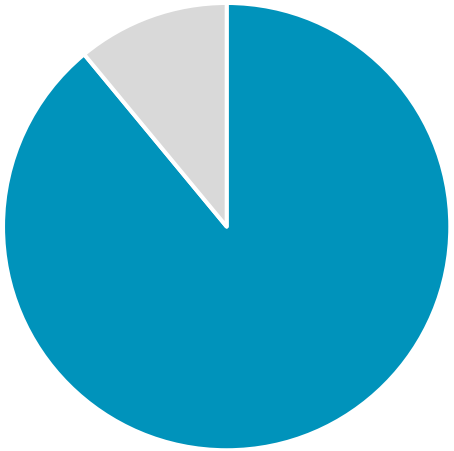
復旧失敗の実態と原因分析

復旧失敗の実態と原因

バックアップ実施率

89%

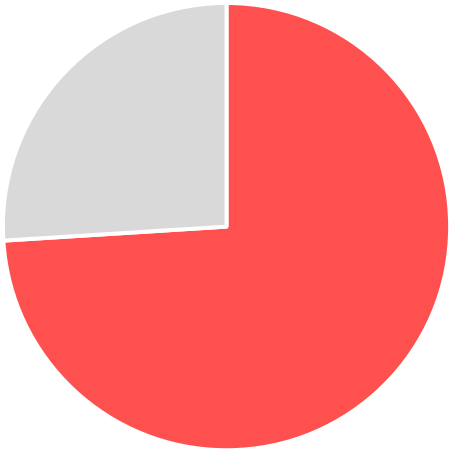
攻撃を受けた企業の89%がバックアップを取得していました。



復旧失敗率

74%

バックアップから復旧できた企業はわずか26%でした。



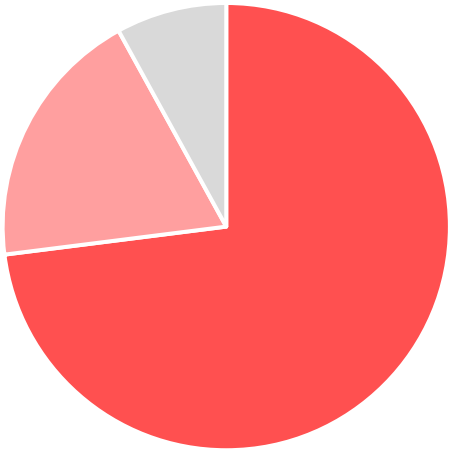
復旧失敗の主な理由

バックアップも暗号化

73%

運用不備

19%



東海大学の事例

2025年4月にインシデント発生、7月に最終調査報告。学生・教職員のユーザーID 4万3千件が暗号化されました。
アプリケーションのハブとしての役割を果たす認証基盤部分が攻撃されてしまった事例です。

東海大学 在学生・保護者向けポータル（TIPS） | 本学教職員向け情報 | JP / EN / 中文 Google 提供

1.経緯

＜原因＞

学外の情報セキュリティ専門機関の調査によると、現時点ではその経路および方法は解明されていないものの、フィッシングなど何らかの手段で学園関係者のアカウント情報が窃取されたことが根本的な原因であり、攻撃者は窃取したアカウント情報を使って学園ネットワークへ不正に侵入し、ランサムウェアを実行した可能性が高いと推測しています。

＜暗号化された情報＞

（1）学園関係者の認証情報

学生・教職員 ／ユーザーID 43,451件、ハッシュ化されたパスワード、大学が発行した各学生・教職員等のメールアドレス 43,451 件※2

※2）暗号化された情報の総数は、一部ログの喪失等があって特定できないため、現時点で判明している最大数として記載しております。

（2）WEBサーバのコンテンツ（個人情報は含まれておりません）

JAXAの事例

2023年6月から2024年にかけて複数回のサイバー攻撃を受けました。Microsoft 365に不正アクセスされ、1万以上の文書ファイルが不正閲覧・持ち出しされた可能性があります。
それだけでなく、同時にActive Directoryも同時に攻撃されていました。

JAXA 組織情報 事業内容 Fan!Fun!JAXA! JAXA Channel お問い合わせ English

プレスリリース・記者会見等

TOP > プレスリリース・記者会見等 > JAXAにおいて発生した不正アクセスによる情報漏洩について

ポスト いいね！334 B! 30

JAXAにおいて発生した不正アクセスによる情報漏洩について

2024年（令和6年）7月5日

国立研究開発法人宇宙航空研究開発機構

宇宙航空研究開発機構（JAXA）において昨年発生した不正アクセスによる情報漏洩への対応状況について、以下のとおりお知らせいたします。

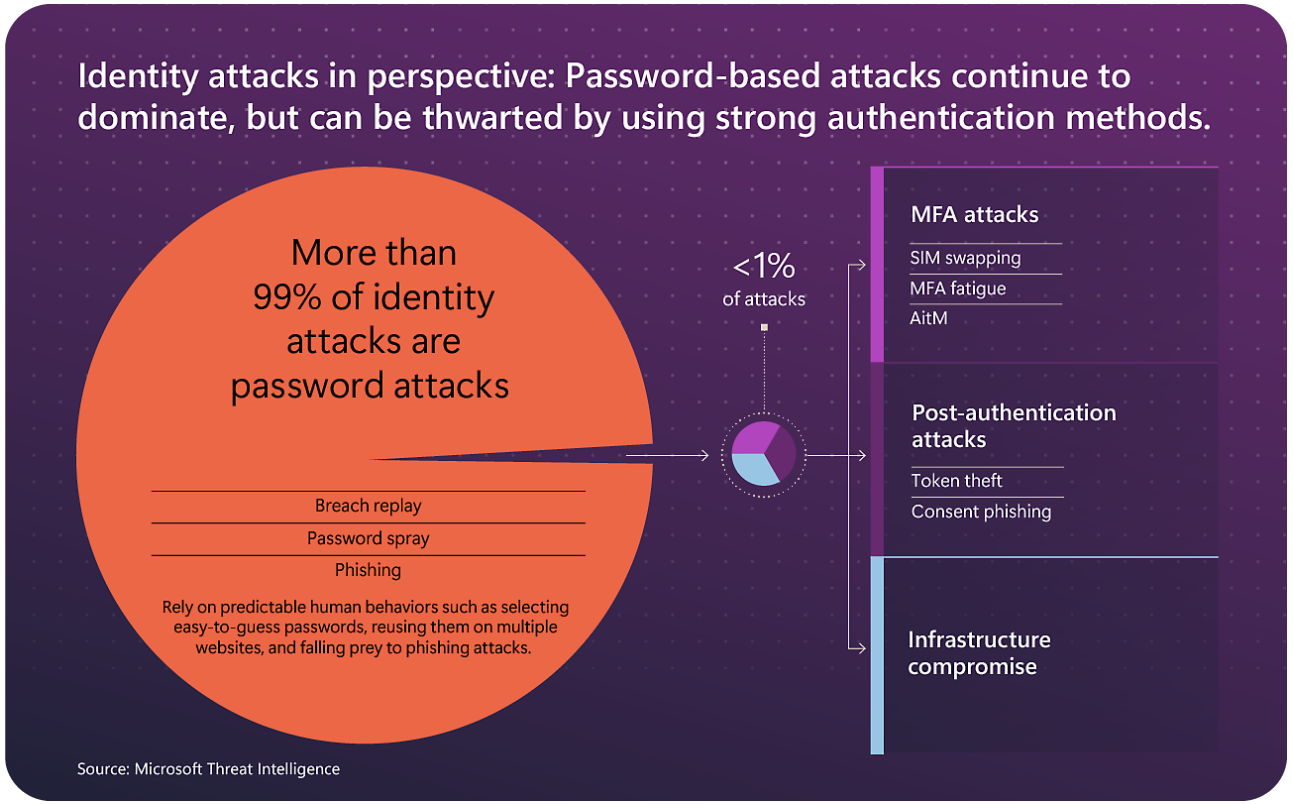
昨年10月、外部機関からの通報に基づき、JAXAの業務用イントラネットの一部のサーバに対する不正アクセス（以下、「本インシデント」といいます）を認知しました。その後速やかに不正通信先との通信遮断等の初期対応を実施しつつ、専門機関及びセキュリティベンダー等とも連携して調査を行い、事案の解明、対策の策定及び実施に取り組んできました。本インシデントの概要は別紙のとおりですが、その中で、JAXAが管理していた情報の一部（外部機関と業務を共同で実施するにあたっての情報及び個人情報）が漏洩していたことを確認いたしました。

本インシデントについて、関係する皆様には多大なるご迷惑をお掛けしましたこと、深くお詫び申し上げます。

Panasonic

IDに関連する攻撃の脅威

“Microsoft Entra のデータによると、**ID 攻撃は 1 日あたり 6 億件発生**していますが、そのうち **99% 以上はパスワードベースの攻撃**です。Microsoft では、ここ 1 年間に**毎秒 7,000 件のパスワード攻撃**をブロックしています。この種の脅威がきわめて幅広く執拗に行われていることがわかります。”

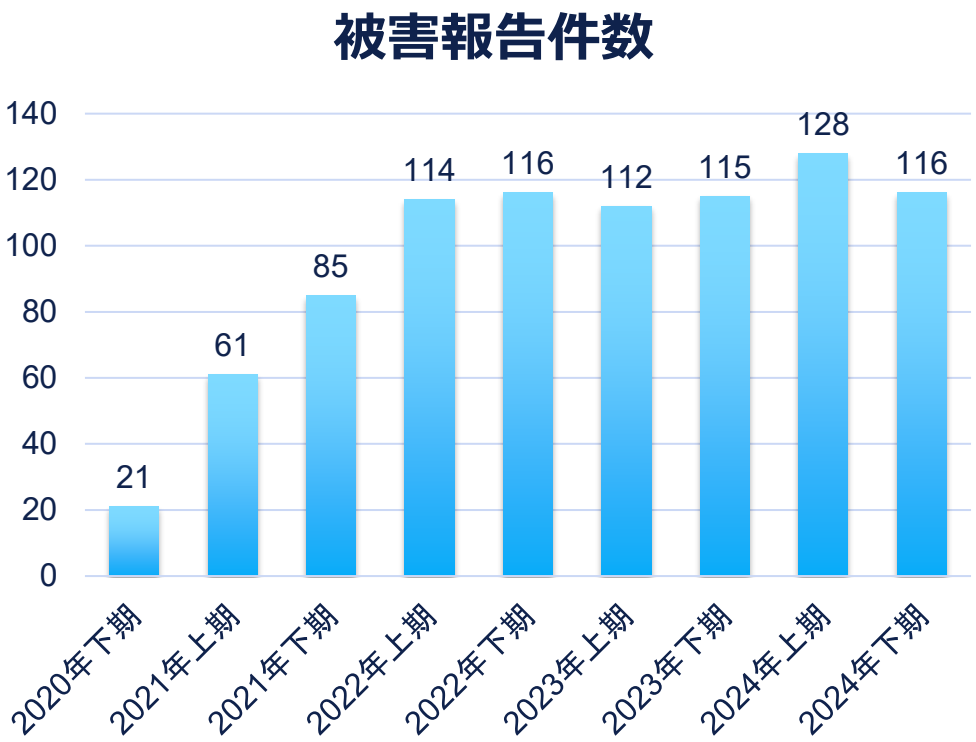


Microsoft社「Microsoft デジタル防衛レポート 2024」より

Panasonic

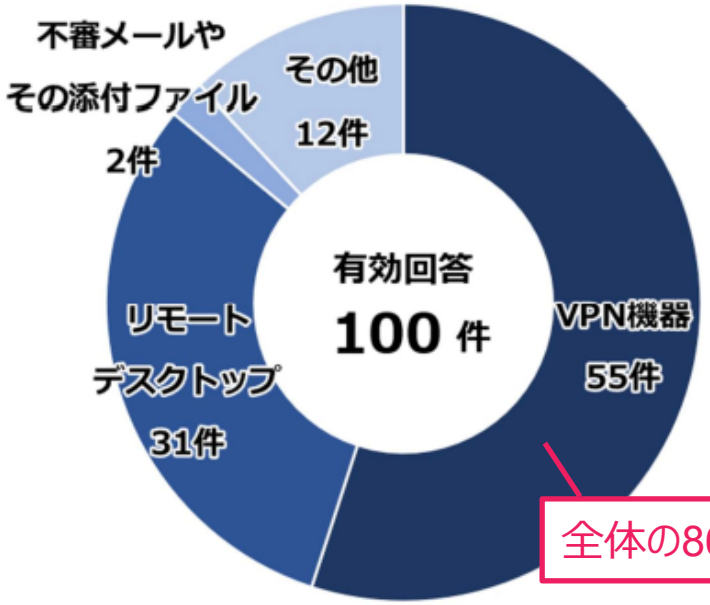
日本国内でも猛威を奮うランサムウェアの脅威

日本国内におけるランサムウェア被害報告件数の推移



出典：警察庁「令和6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」

ランサムウェアの感染経路



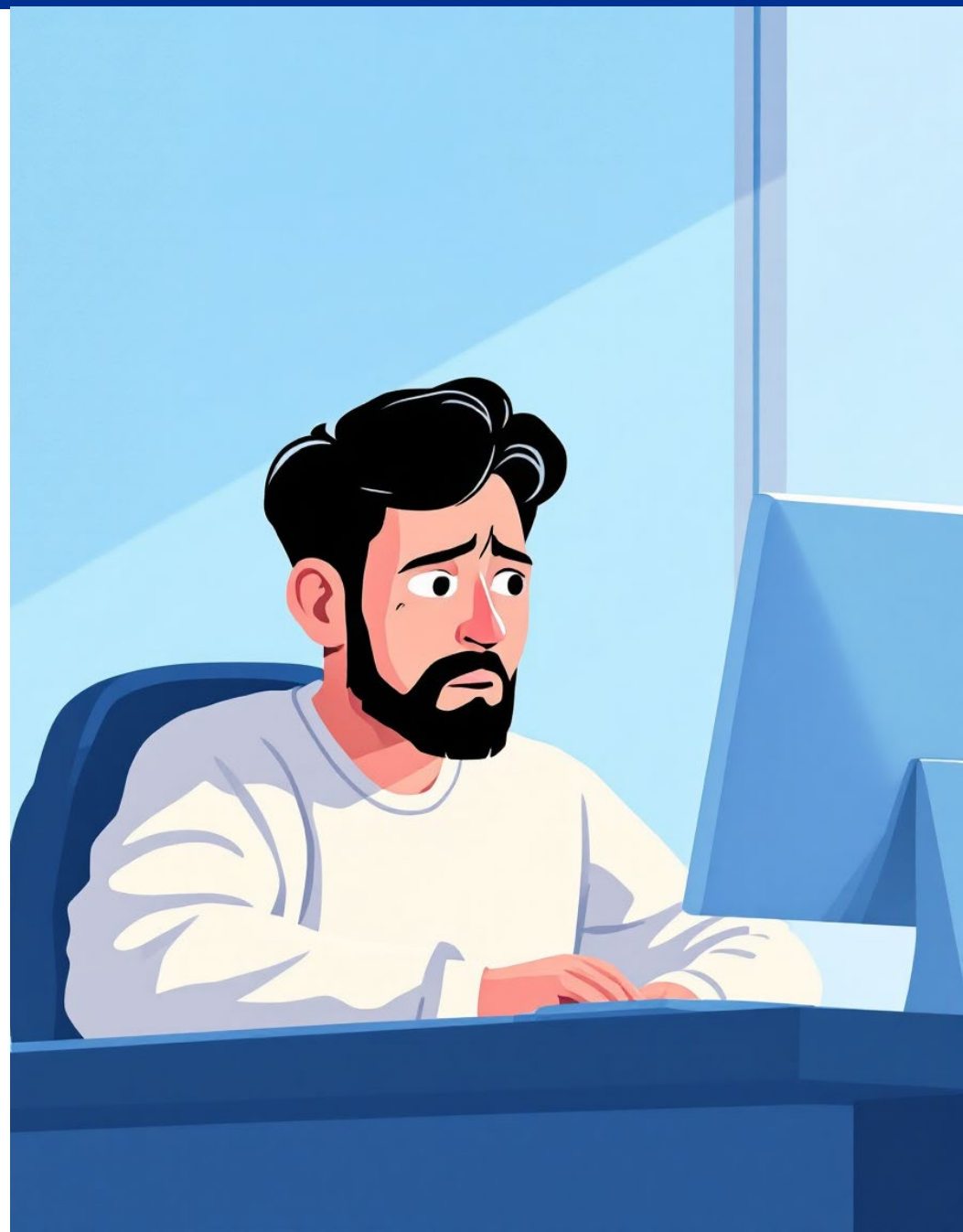
全体の86%が外部からの侵入

脆弱性情報とパッチが公開されてから適用するまでの間に攻撃される「**ゼロデイ攻撃**」の可能性が高い

Panasonic

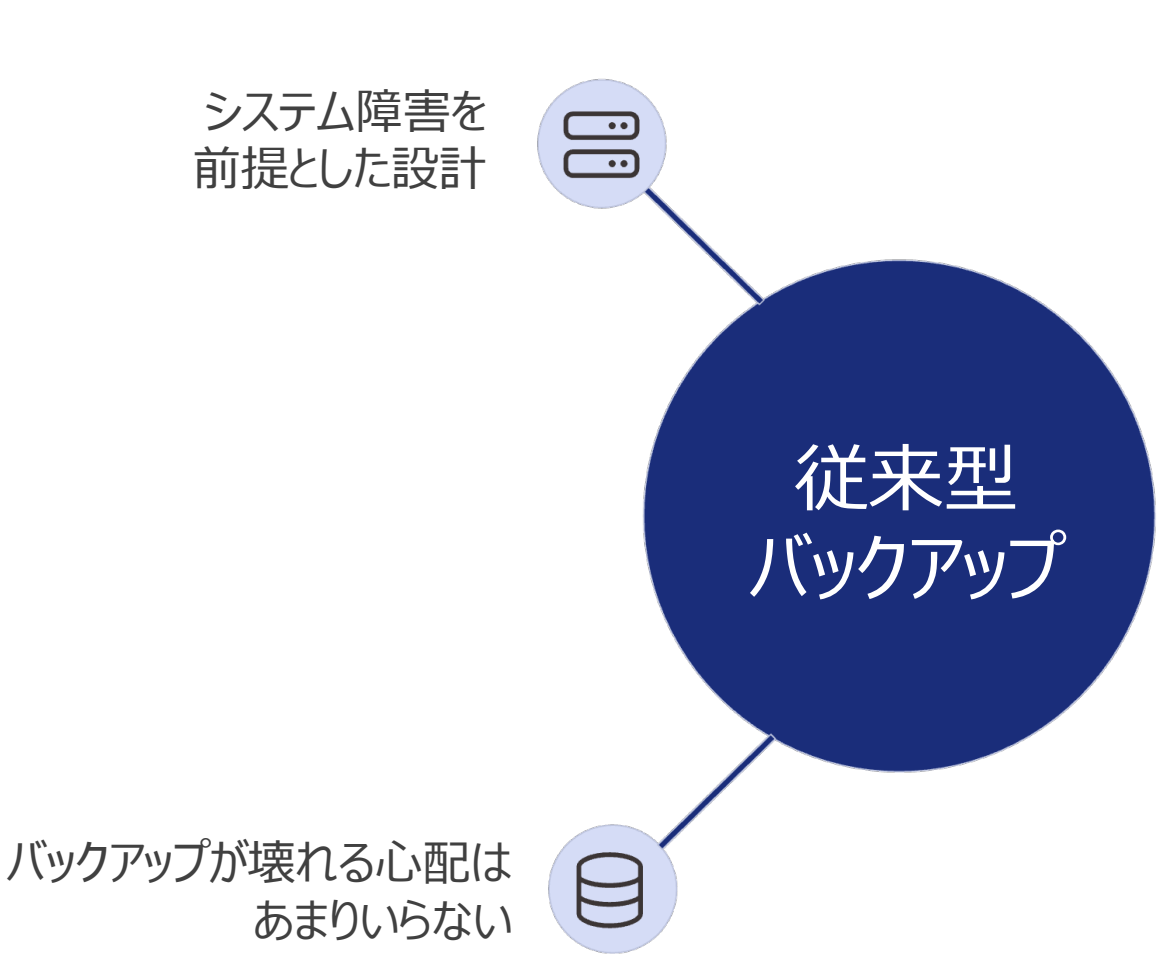
防御だけでは不十分

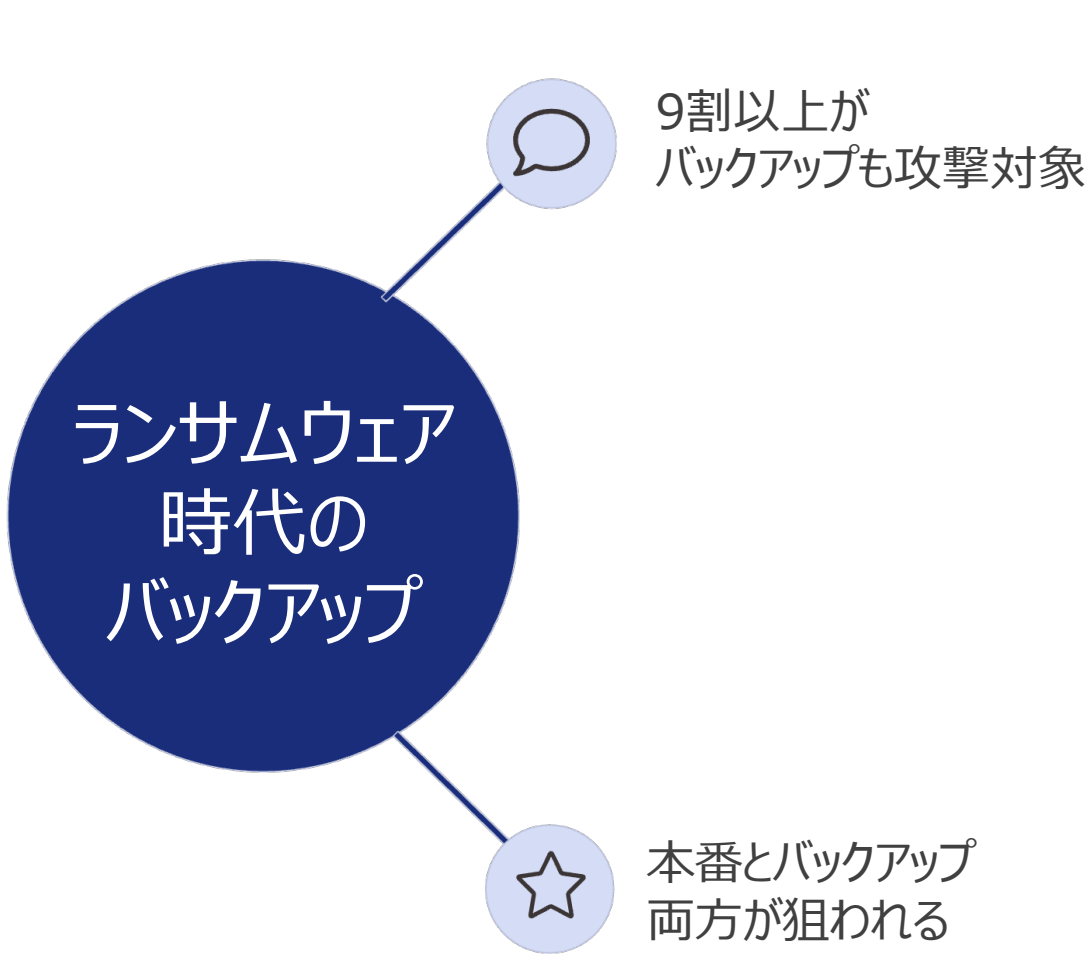
どれだけ保護しても中に入られてしまう隙があるのであれば、**戻せる設計**を組み込む必要があります。



従来型バックアップの限界と“サイバーRTO”の考え方

従来型バックアップの限界





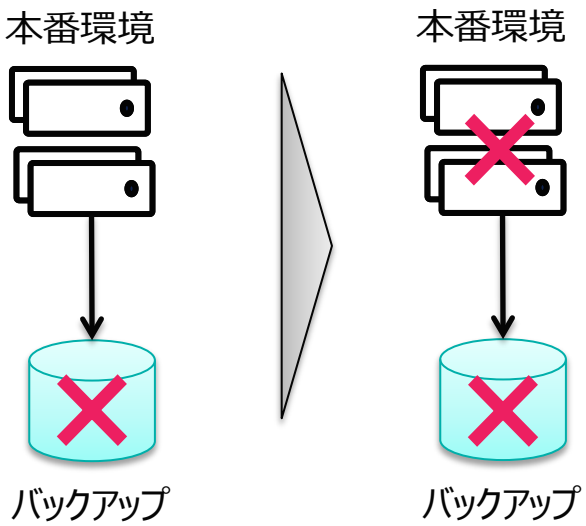
攻撃者の気持ち

身代金を得るために、1日でも長く復旧を遅らせたい

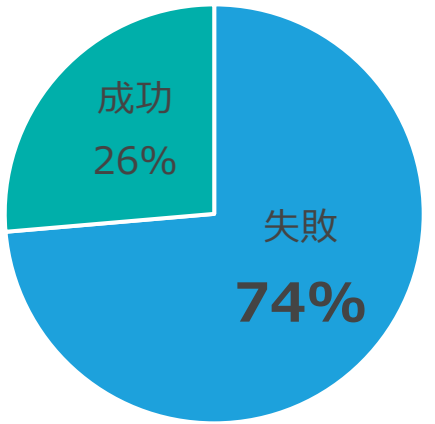
⇒復旧を遅らせようと、さまざまな悪意ある手段が取られる

バックアップデータの暗号化

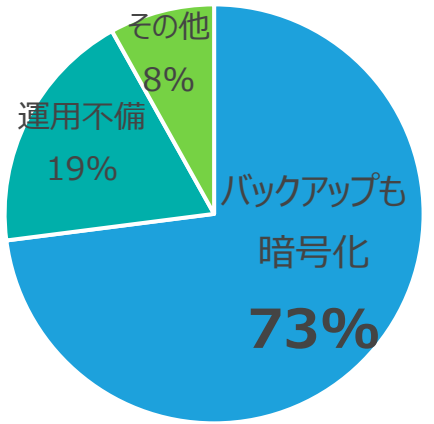
復旧手段を破壊するために、**バックアップデータを先に暗号化**し、その後に本番環境を暗号化する



ランサムウェア被害時にバックアップから復元できたか？



復元結果できなかった理由



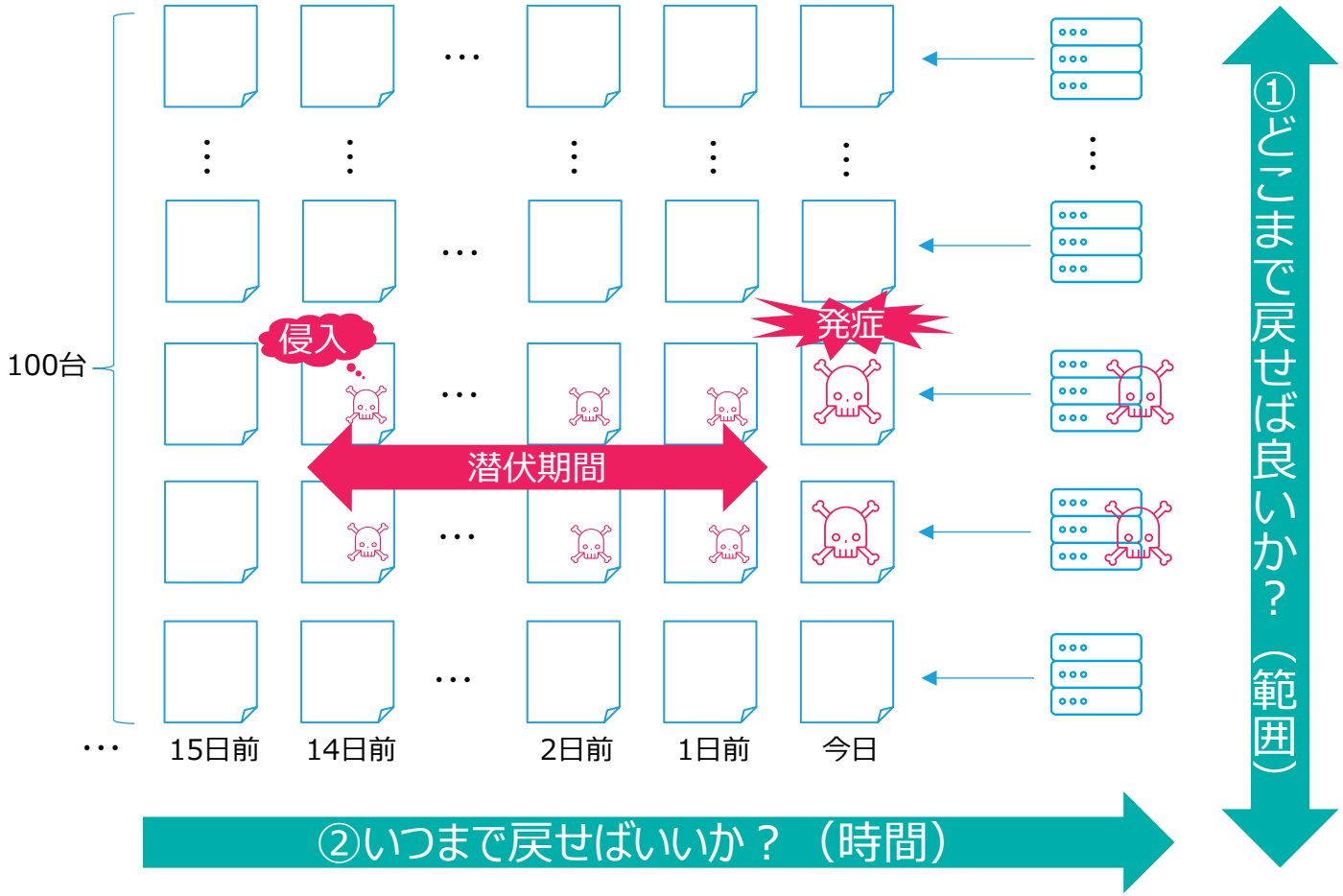
バックアップが被害を受けると、復旧コストは**8倍**に！

出典：警察庁 令和6年におけるサイバー空間をめぐる脅威の情勢について

復旧の複雑さ

ランサムウェア被害を受けた場合は、必ずしも直近に戻せば良いというわけではない

⇒被害範囲、クリーンポイントの把握に時間がかかる



1 **影響範囲調査**

サーバ100台のうち2台が発症した場合、
残り98台は無事か？
⇒1ヶ月

2 **クリーンポイント特定**

どれくらいの期間、潜伏していたか？
何日前のバックアップならクリーンか？
⇒1ヶ月

3 **合計**

1ヶ月＋1ヶ月＝2ヶ月

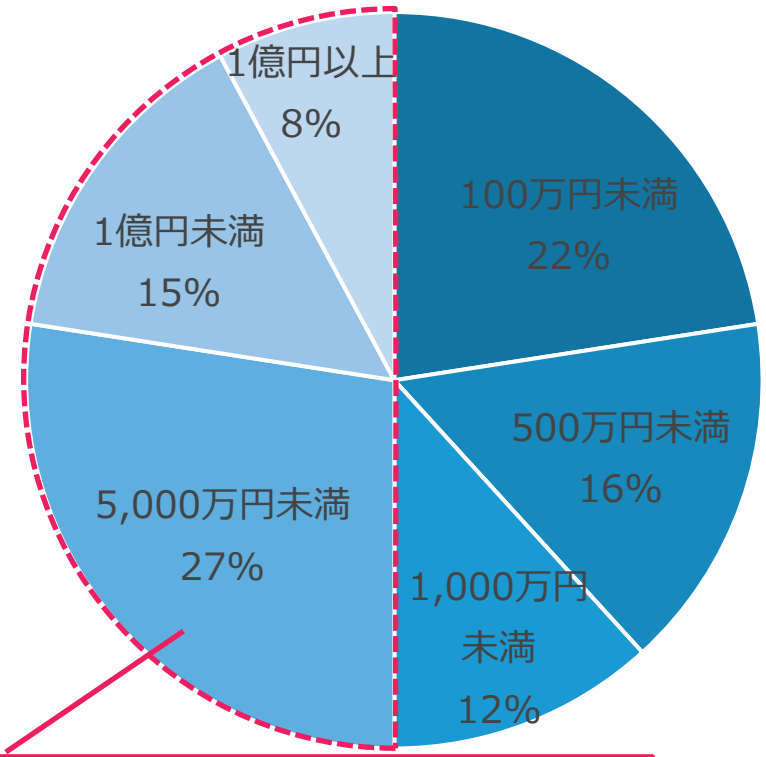
Panasonic

復旧時の運用において重要な4軸

1 被害範囲の把握	2 クリーンポイントの把握	3 機密データへの影響把握	4 マルウェア検出と隔離
Where ?	When ?	Which ? / How much ?	What to do ?
どこが被害を受けた？ （リストアすべき範囲）	いつのデータに戻せば良い？ （クリーンなバックアップデータ）	影響は甚大？ （機密情報の安否）	マルウェアにどう対応すべき？ （どのマルウェアが侵入したか）

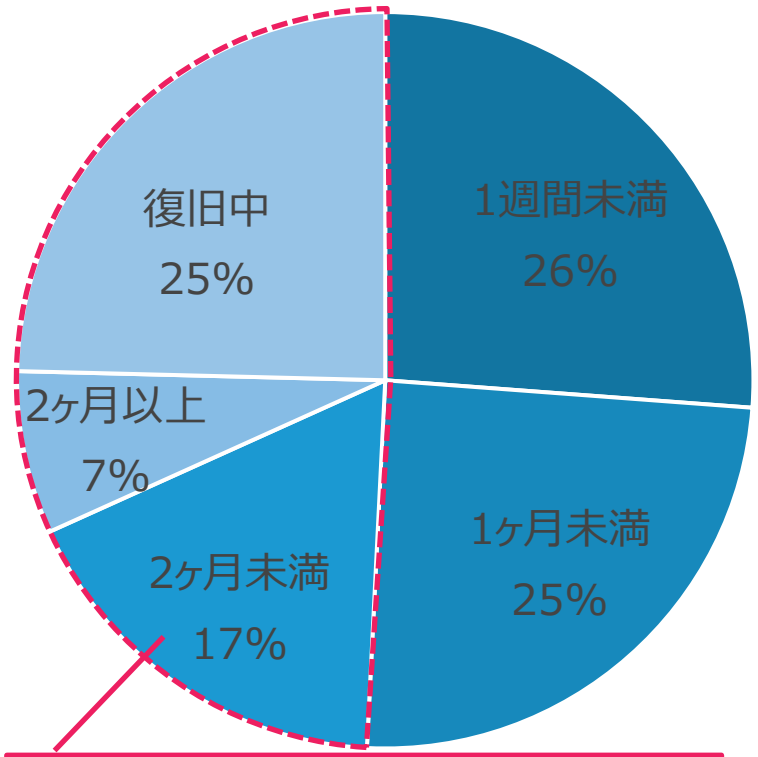
（補足）ランサムウェア被害からの復旧にかかる時間と費用

復旧に要した調査費用の総額



1000万円以上の費用を要したものが
全体の50%

復旧に要した期間



１ヶ月以上かかっても復旧できていない
ケースが全体の49%

出典：警察庁 令和6年におけるサイバー空間をめぐる脅威の情勢について

Panasonic

バックアップも標的に

常に**「バックアップも狙われている」**という前提で対策を講じる必要があります。

復旧判断の4軸

迅速な復旧のためには、
Where/When/Which/What to do
の4軸で判断基準を設計することが不可欠です。

実践的なバックアップ戦略の設計ポイント

サイバーRTOを短縮するための3つの視点

- 技術
- 運用
- 体制

① バックアップ設計（技術面）

重要なポイント

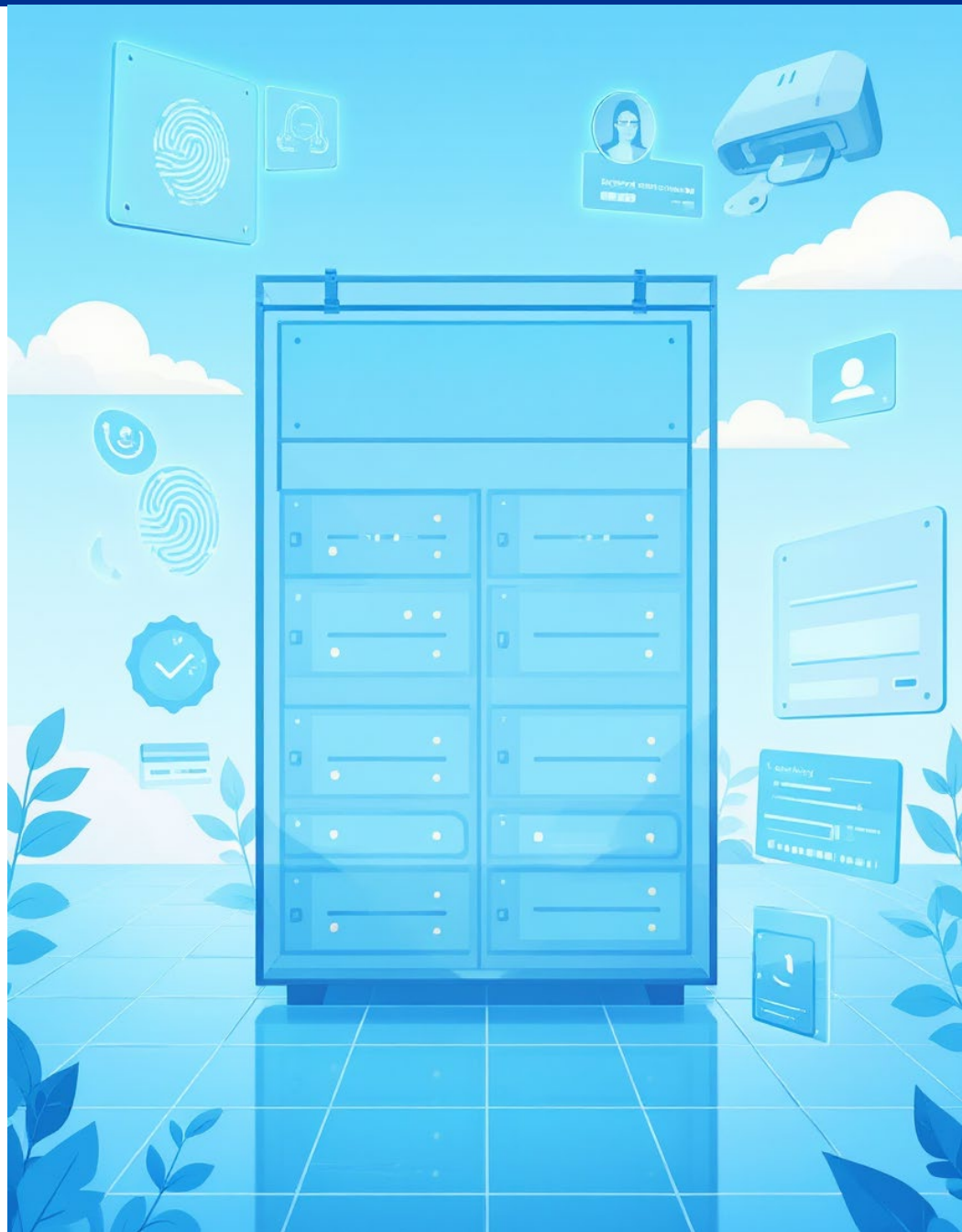
⚠ 攻撃者はまずAD/EntraIDなどの認証基盤を狙う

⚠ これが破壊されると、すべてのサービスが使用不可になると同義

⚠ ファイルやVMだけでなく、ID情報をバックアップ対象に含め、バックアップデータを攻撃者に破壊されないようにする

実施すべきアクション

- AD/EntraIDのバックアップ可否を確認
- 復旧手順に「認証基盤の再構築」を含める
- バックアップデータは改ざんできないイミュータビリティ機能を持ったストレージに保存する



② バックアップの可観測性（オブザーバビリティ）を高める（技術＋運用）

重要なポイント

⚠ 復旧対象の特定には「どこが被害を受けたか」「いつまで戻せばいいか」の判断が必要

⚠ そのためには、バックアップの状態・履歴・異常検知などを見える化する必要がある

実施すべきアクション

- バックアップごとのメタデータ（ファイル数、変更履歴、暗号化兆候など）を記録・分析
- ランサムウェアの痕跡を検知できる仕組み（振る舞い検知／脅威モニタリング）
- クリーンな復旧ポイントを自動で特定できる機能の導入

③ 復旧体制の事前構築（体制面）

サイバー攻撃時は「誰が」「何を」「どの順番で」復旧するかを即座に判断する必要がある

実施すべきアクション

役割分担の明確化

復旧責任者・実行者・承認者の役割を事前に定義し、混乱を防ぐ

復旧優先順位の定義

業務影響度に基づいた復旧対象の優先順位を事前に設定する

手順書整備・定期演習

復旧手順書を整備し、机上訓練でも良いので定期的な演習を実施する

弊社がおすすめするバックアップソリューション

復旧時の運用において重要な4軸

1 被害範囲の把握	2 クリーンポイントの把握	3 機密データへの影響把握	4 マルウェア検出と隔離
Where ?	When ?	Which ? / How much ?	What to do ?
どこが被害を受けた？ （リストアすべき範囲）	いつのデータに戻せば良い？ （クリーンなバックアップデータ）	影響は甚大？ （機密情報の安否）	マルウェアにどう対応すべき？ （どのマルウェアが侵入したか）

rubrik

データオブザーバビリティ

どこが被害を受けたのか、いつまで戻せばいいのかを特定

Panasonic

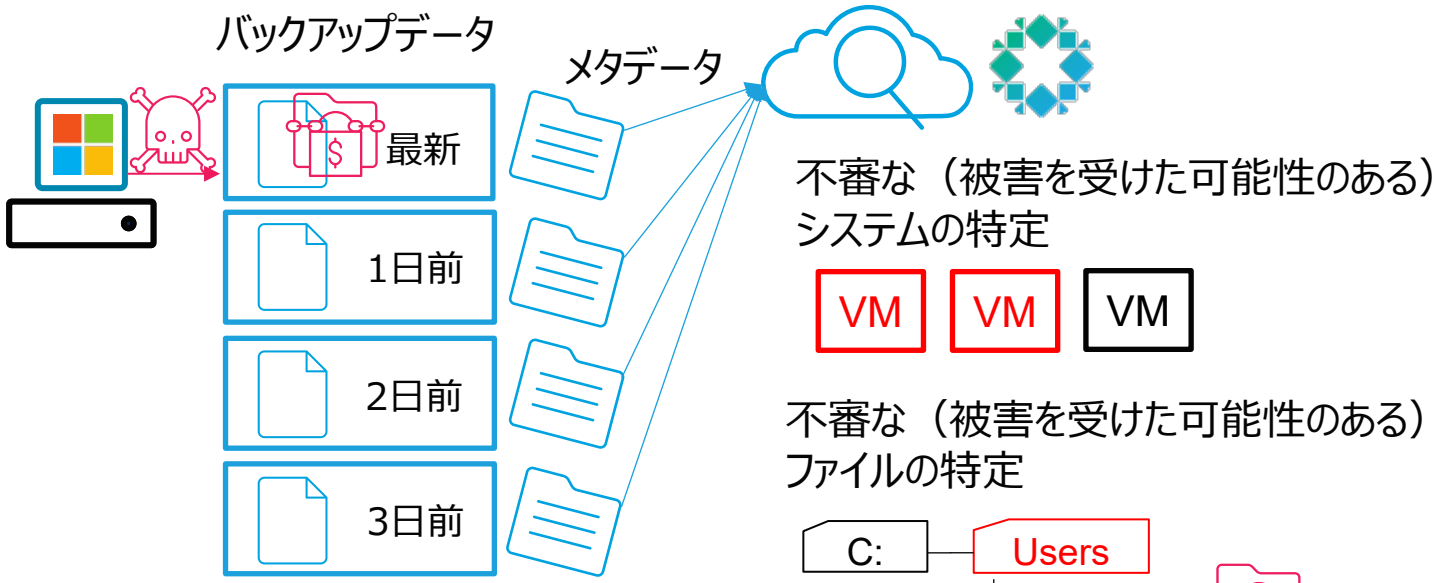
データオブザーバビリティ：

振る舞い検知（Anomaly Detection）によって どのファイル/システムが被害を受けたのか判断可能

①どこまで戻せば良いか？（範囲）

ファイルが暗号化された？
大量にファイルが削除された？

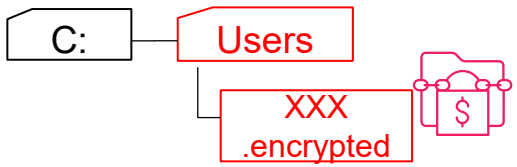
バックアップファイルのメタデータを機械学習で分析し、
いつもと違う振る舞いを検出



不審な（被害を受けた可能性のある）
システムの特定

VM VM VM

不審な（被害を受けた可能性のある）
ファイルの特定



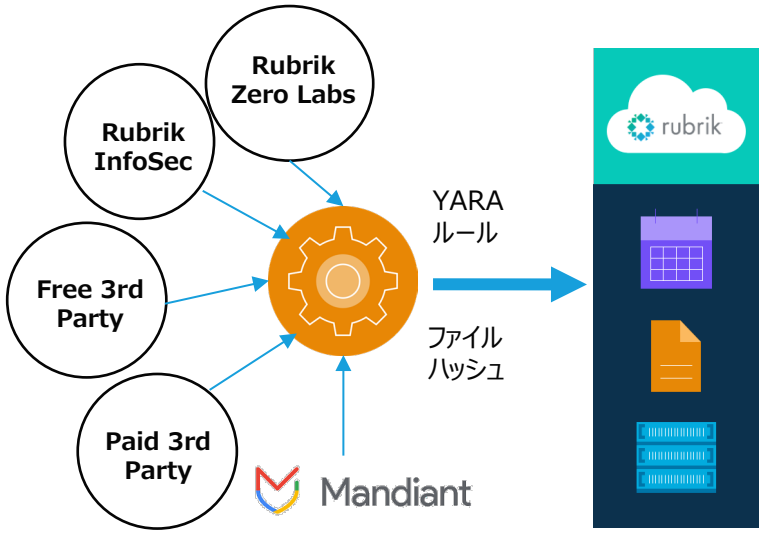
バックアップを取得するたびに
分析処理を行うため、
被害の早期検知が可能！

rubrik

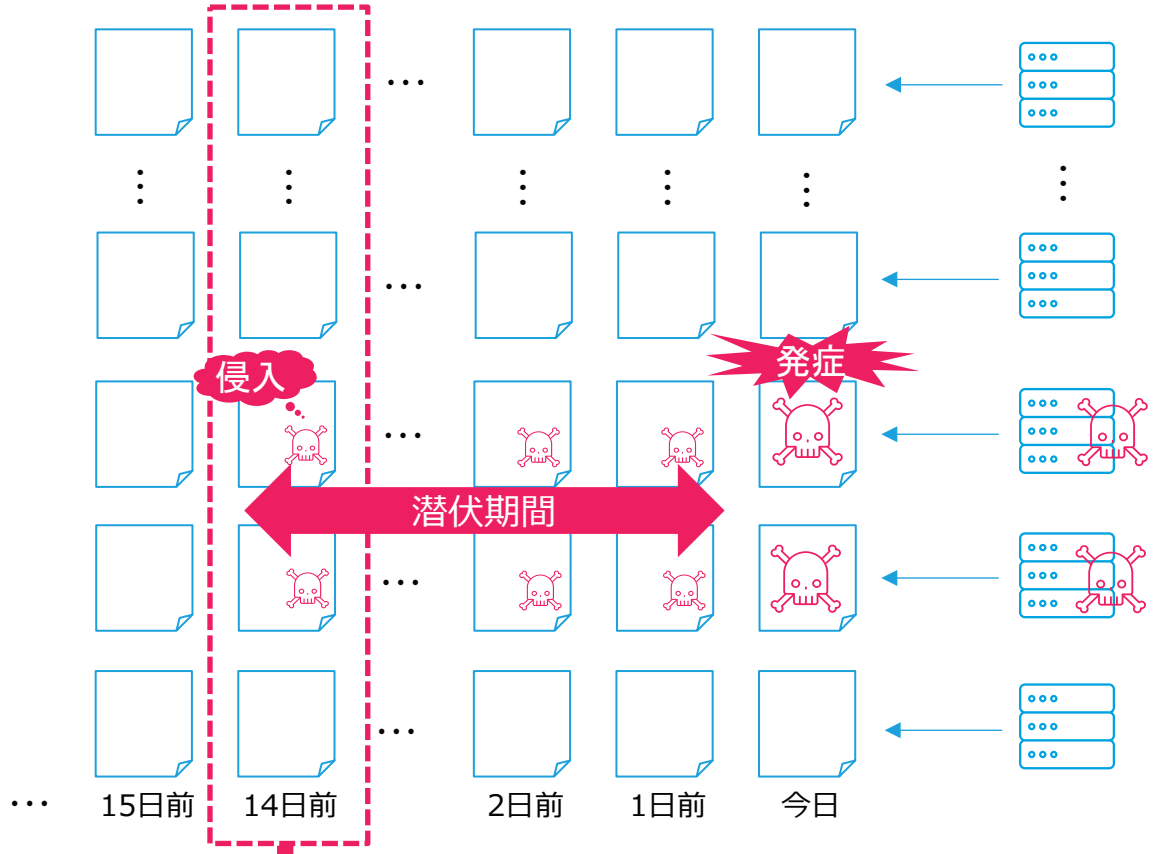
データオブザーバビリティ：

脅威モニタリング（Threat Monitoring）によって どのバックアップデータをいつまで戻すべきか判断可能

バックアップを取得するたびに、バックアップデータ内の
ランサムウェア痕跡情報をスキャンし、感染有無を検知



※痕跡情報はRubrikから自動的に最新のものをアップロード



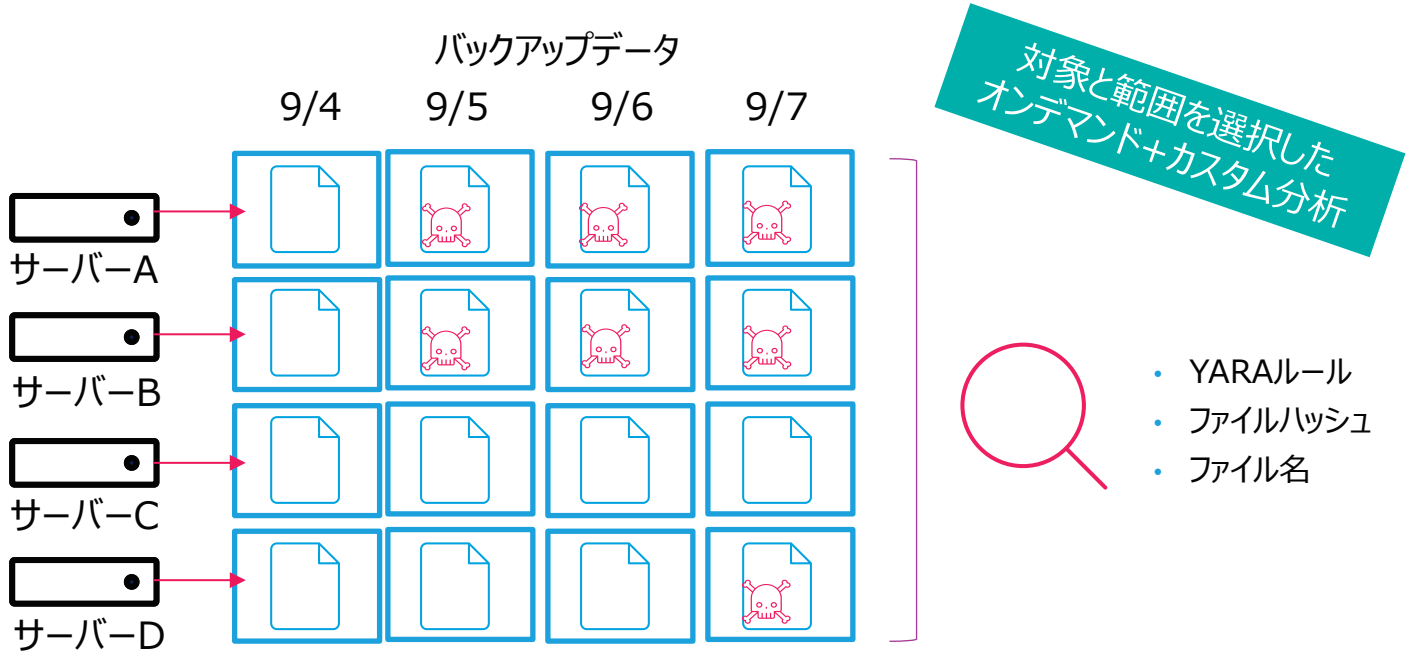
侵入したタイミングで検知できるため、
発症前に対処可能なケースもあり

②いつまで戻せばいいか？（時間）

データオブザーバビリティ：

脅威ハンティング（Threat Hunting）で特定のランサムウェアがいつから侵入したのか検知可能

入力されたYARAルールなどの痕跡情報とバックアップデータを
照合し、どのバックアップデータなら侵入していないかを調査
(ランサムウェアの痕跡情報を入力してオンデマンド分析)



ランサムウェア被害から復旧までにかかる時間の内訳

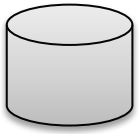
バックアップが暗号化
された場合

ゼロからのシステム再構築作業…

3ヶ月＋

3ヶ月＋

バックアップが暗号化
されない場合
（＋①データ回復力）



影響範囲（リストア対象）の調査

どのシステムの、どのデータを戻すべき?

1ヶ月

マニュアルで、各サーバーやVM 1台ずつログイン
データをチェックし、どの範囲が被害をうけているか確認

いつの時点まで戻すべきかの調査

感染前のバックアップはいつか？

1ヶ月

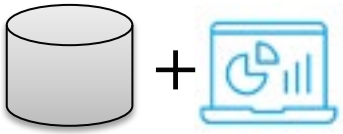
バックアップのリストア＆ランサム有無の確認作業を
クリーンなバックアップが見つかるまで延々と繰り返す

バックアップデータの
リストア

1～3日

2ヶ月＋

バックアップデータの分析
機能もある場合
（＋②データ可観測性）



1日

1日

1～3日

3～5日

rubrik

Rubrik導入事例

Panasonic

事例背景と要求事項

背景

お客様は金融機関様

ランサムウェア感染を見据えたシステム構成が必要

HCI基盤更改に合わせてバックアップシステムも更改

より安価な遠隔地バックアップ

要求事項　データの堅牢性を高めるバックアップシステムへの刷新

①ランサムウェアに耐えうるバックアップシステム

②安価なストレージへの遠隔地バックアップ

③HCI基盤拡張に追従するバックアップシステム

要求事項へのRubrik適合度

①ランサムウェアへの対応

- ✓ 特許取得済みの改ざん防止機能
- ✓ 暗号化検知

②安価な遠隔地バックアップ

- ✓ NFSストレージへの遠隔地バックアップ

③HCI基盤拡張への追従

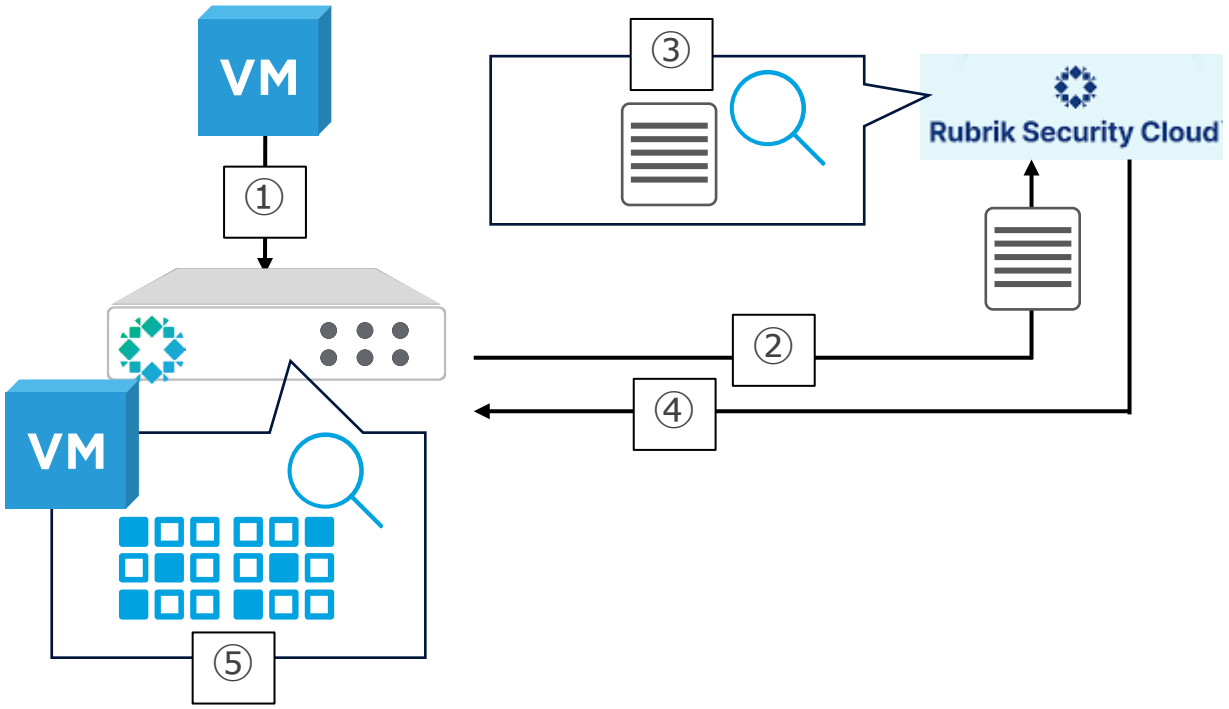
- ✓ HCIライクなスケールアウトアーキテクチャ

改ざん防止（イミュータブル）機能も製品ごとに実装方式が異なる

カテゴリ	Rubrik		製品A（既存製品）		製品B		製品C	
方式	○	**独自ファイルシステム**で実現	△	イミュータブル ストレージと連携で実現	△	Linux改ざん防止機能 (強化リポジトリ) と連携で実現	○	独自ファイルシステムで実現
特権ユーザ	○	OSを直接操作可能な **特権ユーザーは非公開**	×	特権ユーザーは利用可能 なため、のっとりにより 設定変更ができてしまう	×	特権ユーザーは利用可能 なため、のっとりにより 設定変更ができてしまう	○	OSを直接操作可能な **特権ユーザーは非公開**
時間改ざん	○	**時間の改ざんに対応**	×	非対応	×	非対応	×	非対応

Rubrikが最もイミュータビリティ性が高いと判断し、Rubrikを提案

独自の高速かつ高精度な暗号化検知機能



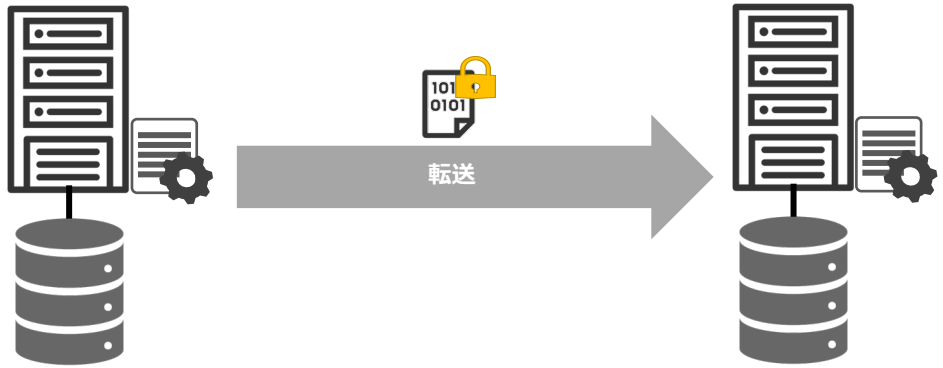
① 仮想マシンバックアップ
② バックアップデータのメタデータをアップロード
③ メタデータを解析（第1段階）
→異常がなければここで終了
④ 実際のバックアップデータの調査を依頼
⑤ バックアップデータのランダム性をチェック（第2段階）
→異常があればアラート発報

2段階チェックにより速度と正確性が両立され、**検知精度99.8%**
サービスインから1年半経過したが、**一度も誤検知なし**

Panasonic

②安価な遠隔地バックアップ

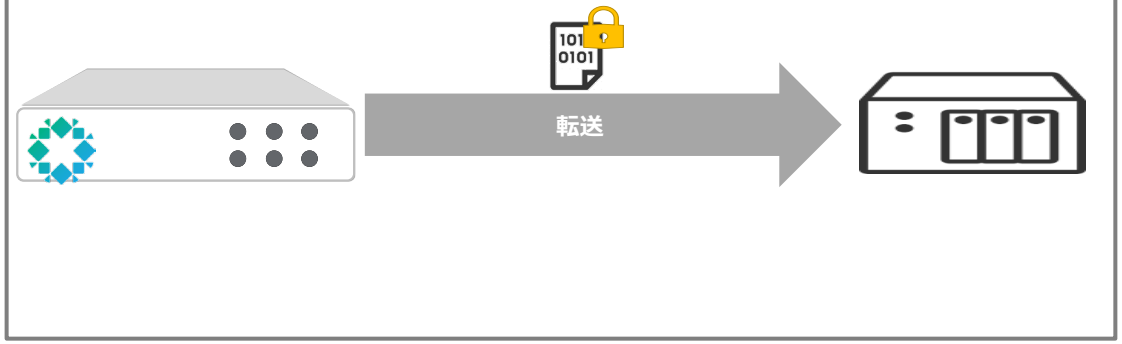
既存環境



☒ 遠隔地バックアップのために同一構成を準備

- バックアップデータ転送にリモートサイトにもプライマリサイトと**同様の構成が必要**
- ハードウェア＋Windowsライセンス＋バックアップソフトライセンスにより**高額**

新環境



☑ 機能を犠牲にしない安価な遠隔地バックアップ

- **NFS v3対応**であればバックアップデータ転送可能
- 汎用NAS採用により**大幅なコストダウン**
- 以下機能も使用可能
  - **転送データ暗号化**
  - **圧縮/増分転送**

Panasonic

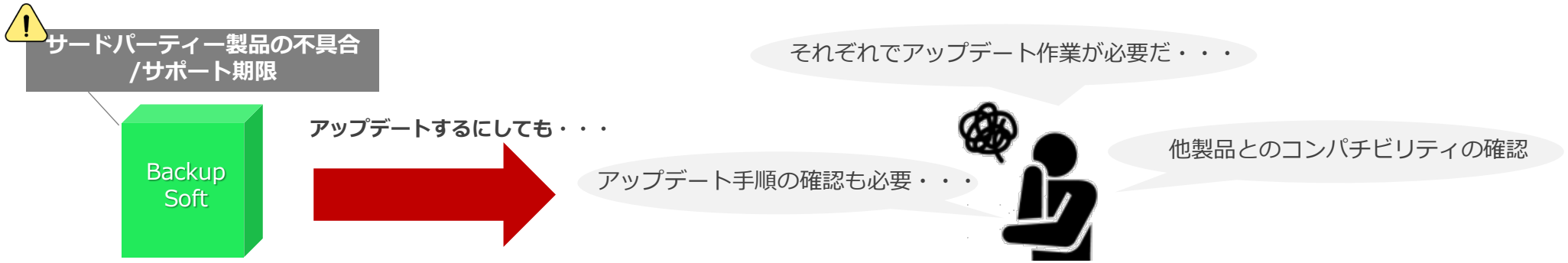
実際に導入して分かったRubrikのメリット/デメリット

メリット 01

オールインワンパッケージ構成による簡単なアップデート

従来

・従来のバックアップソフトは、OS/DBはサードパーティー製品を採用しており、
サードパーティー製品起因（脆弱性やサポート期限等）のアップデートが必要になることがある



実際、直近1年でもIPA（独立行政法人情報処理推進機構）は、毎月Windows Updateの早急な実施を推奨しており、内9回は実際に脆弱性を悪用した攻撃が確認されている

Rubirk

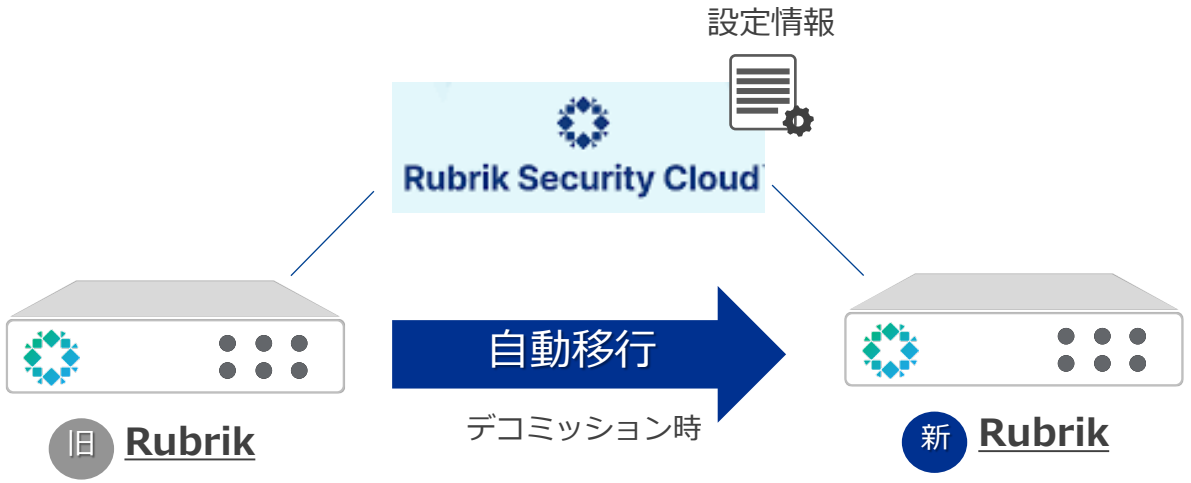
・Rubrikは、オールインワンパッケージ構成のため
上記を意識せず、数回のクリックでのアップデートが可能

・ローリングアップデートによる無停止アップデートも可能

メリット 02

リプレイス時の作業負荷を大幅に軽減

・設定はRubrikが提供するSaaS形式の管理コンソールで保持され、リプレイス時の設定移行作業が不要
→ バックアップデータもデコミッション（ノード切り離し）時に自動移行
→ 初回フルバックアップ取り直しに伴うヘビーな移行設計が不要



メリット 03

サポートトンネル/サポートアクセスによるトラブル負荷軽減

・Rubrikのサポートエンジニアが直接環境アクセスを行うためログ収集や設定連携が基本的に不要
・オールインワンのためベンダー間で、たらい回しも発生しない

デメリット 01

バックアップ定義の割り当ては1つ

・**バックアップ対象に対し、特定曜日だけバックアップ時刻変更することが標準設定では不可**
※ただし、スクリプトによるオンデマンドバックアップ処理にて実現は可能

日 Sun	月 Mon	火 Tue	水 Wed	木 Thu	金 Fri	土 Sat
23:00	23:00	23:00	22:00	23:00	23:00	23:00

デメリット 02

シャーシ単位でのスケールアウトが必要

・**ノード単位での追加が不可**
・**シャーシ（4ノード）単位での追加が必要**

デメリット 03

ベアメタルリストアが複雑

・**リカバリーメディア作成機能がなく、WindowsADKを使用したブートメディアの作成が必要**
※ただし、ブートメディアを作成するスクリプトはRubrik社から提供有
・**ベアメタルリストアはコマンド作業が必要**

まとめ

Panasonic

まとめ

- 守るだけでなく、「戻せる」バックアップを構築すること
- 「どこが被害を受けたのか（Where）」「いつまで戻せばいいのか（When）」「影響はどの程度か（Which/How much）」「マルウェアにどう対応すべきか（What to do）」の4軸を明確化すること
- ID情報をバックアップ対象に含め、攻撃者に破壊されないようにすること
- バックアップのオブザーバビリティ（可観測性）を高めること
- 事前に復旧フローを定義し、関係者間で共有しておくこと

Panasonic