D- 10

2025年9月5日(金) 11:40-12:20

Panasonic

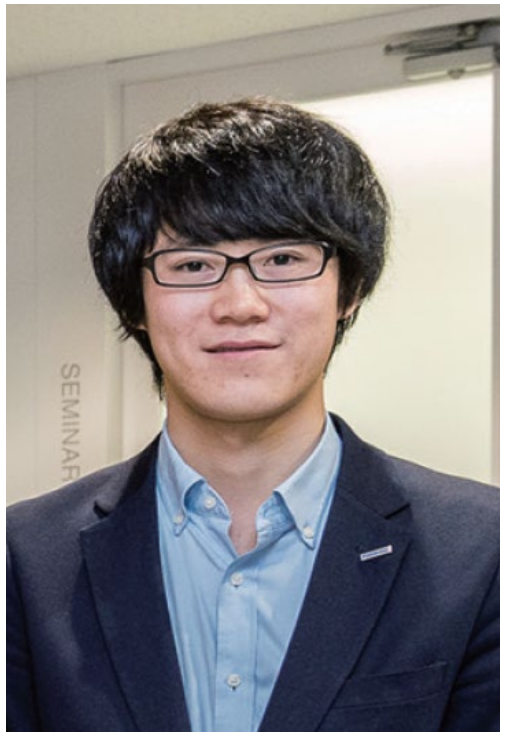
金融機関の現場から見るランサム対策
Rubrik導入の実例とSIerの本音レビュー

【講演者】

Rubrik Japan株式会社　三浦 かなこ

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

講演者の紹介



Panasonic
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

パナソニック インフォメーションシステムズ株式会社
プラットフォームサービス事業部
エンタープライズインフラソリューション部
第２デジタルワークスペースチーム

rubrik

三浦 かなこ　氏

Rubrik Japan株式会社
Senior Account Executive

アジェンダ

パナソニック インフォメーションシステムズ 会社紹介

はじめに

ランサムウェア被害から迅速に復旧するための”サイバーリカバリ”とは？

Rubrik導入事例

実際に導入して分かったRubrikのメリット/デメリット

まとめ

会社紹介

Panasonic

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 〒530-0053　大阪府大阪市北区末広町2番40号　Panasonic XC　OSAKA 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)
代表取締役　社長執行役員	阿部　裕
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

パナソニック インフォメーションシステムズ 2つの事業

パナソニック グループ向け

パナソニックグループのIT中核企業として
ITでグループの事業を支援

B2B市場 向け

お客様のDX実現のため
優れたITサービスでビジネス変革を支援

ITのプロ集団として
パナソニックグループでの挑戦を通じ
お客様へ価値を提供します

Panasonic

はじめに

Panasonic

要求事項の変化

従来	現在
● 高速なバックアップ ● 遠隔地への二次バックアップ ● オンプレミス環境保護	● ランサムウェア対策 ● 迅速な復旧 ● クラウドを含むハイブリッド保護

バックアップシステムへの要求事項は変化してきており、各社が対応を進めている

一方で、

実装方式や機能の完成度は製品ごとに大きく異なる

真に要求事項に対応した製品を選定することが重要

ランサムウェア被害から迅速に復旧するための”サイバーリカバリ”とは？

Rubrik Japan株式会社
Senior Account Executive
三浦 かなこ

rubrik

最近トレンドになっている”サイバーリカバリ”という用語をご存知でしょうか？

rubrik

多様化していくバックアップの目的：
従来型バックアップと“サイバーリカバリ”の目的の違い

従来型バックアップの目的

システム障害からの復旧

サイバーリカバリの目的

システム障害からの復旧

＋

ランサムウェア被害に遭った
場合の復旧

金融業界で”サイバーリカバリ”の需要が高まっている理由①

2024年10月4日の金融庁の金融機関向けの監督指針改定内容：

金融庁サイバーセキュリティガイドライン：サイバーセキュリティ管理態勢

「2.サイバーセキュリティ管理態勢」は、本ガイドラインのメインパートにあたる部分です。以下の6項目について、大きく「**基本的な対応事項（125項目）**」、「**対応が望ましい事項（50項目）**」に分けて推奨事項の記載があります。このうち「基本的な対応事項」については、本ガイドラインでは「いわゆる**サイバーハイジーン**と呼ばれる事項」との記載があります。サイバーハイジーンについては下記の記事でも解説していますので、ご確認ください。

① サイバーセキュリティ管理態勢構築

基本方針・規定の策定、業務プロセス整備、資源確保・人材育成、リスク管理部門による態勢監視、内部監査

② サイバーセキュリティリスクの特定

情報資産管理、リスク管理プロセス（脅威・脆弱性情報の収集・分析、リスク評価等）、脆弱性管理・診断、演習・訓練

③ サイバー攻撃の防御

多層防御、認証・アクセス管理、教育・研修、データ保護、システムセキュリティ対策（ハードウェア・ソフトウェア管理、ログ管理、セキュリティ・バイ・デザイン、ネットワーク防御、クラウドサービス利用時の対策）

👉 **④ サイバー攻撃の検知**

監視（未承認デバイス・ソフトウェアやネットワーク監視、アクセスの監視、データセンターなどへの入出管理など）

👉 **⑤ サイバーインシデント対応および復旧**

インシデント対応計画およびコンティンジェンシープラン※の策定（初動対応・分析・封じ込め・根絶・復旧、顧客対応・組織内外との連携、広報）

※災害や事故など想定外の事態が起きた際に行う、あらかじめ決められた対応策や手順のこと。

⑥ サードパーティーリスク管理

サプライチェーンリスク管理（外部委託先やサードパーティーシステムのリスク管理・監視、サードパーティとの役割分担・責任分界点の明確化など）

出典：2024年10月18日付
https://www.trendmicro.com/ja_jp/jp-security/24/j/securitytrend-20241008-02.html

rubrik

金融業界で”サイバーリカバリ”の需要が高まっている理由②

高まる “オペレーショナル・レジリエンス” の確保に向けた動き

「オペレジ（業務の強靭性・復旧力）とは、サイバー攻撃などが発生しても、重要な業務を最低限維持すべき水準において提供し続ける能力をいう。 想定外の事象が生じた場合に、金融システムの重要な業務を提供できなくなるおそれがあり、**未然防止策を尽くしてもなお、業務中断が生じることを前提に、 早期復旧・影響範囲の軽減を確保する枠組み**」

DORA

（**D**igital **O**perational **R**eadiness **A**ssessment）

- 金融企業に対する、新たなオペレジの規制
- 2025年初頭までに準拠が必要で、**違反が発見されると罰則がある**

FFIEC

（**F**ederal **F**inancial **I**nstitutions **E**xamination **C**ouncil）

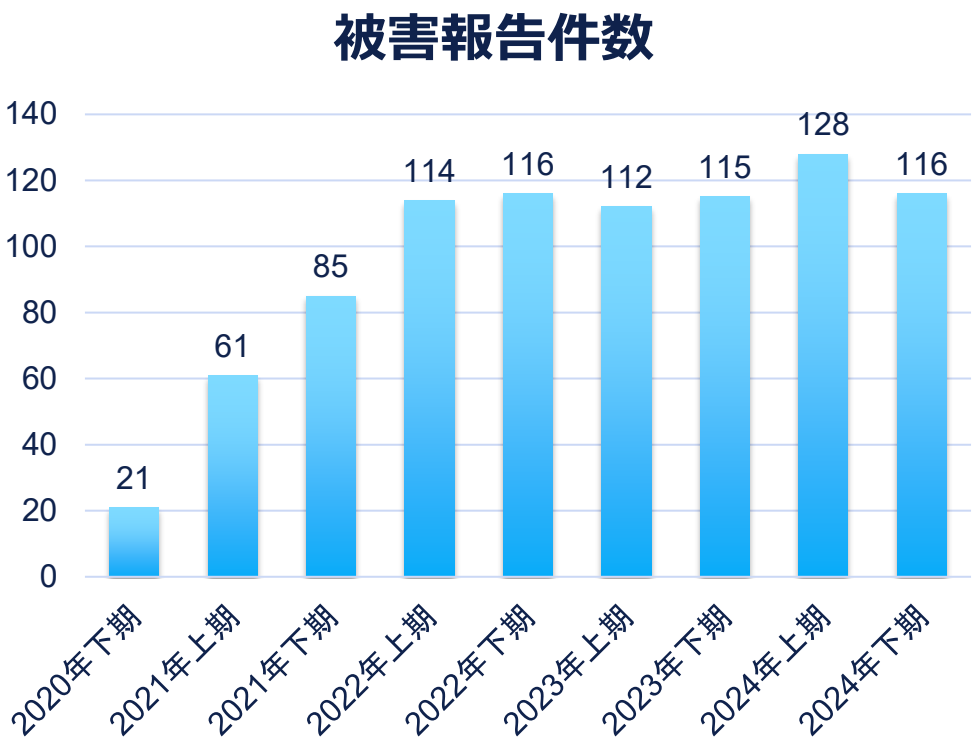
- 2023年、従来から発行しているハンドブックにレジリエンスの観点を含めたサードパーティのリスク管理に関するガイドラインを追加
- ガイドラインは助言的だが、**違反が発見された場合は規制当局（FDICなど）が制裁措置を行う**

金融庁

- 2022年、オペレーショナル・レジリエンスに関する基本的な考え方を提示
- 日本ではまだ義務化されておらず、原則ベースのガイドラインに近い
- ただし、重要性は増しており、**将来的に監督指針に格上げされる可能性があると言われている**

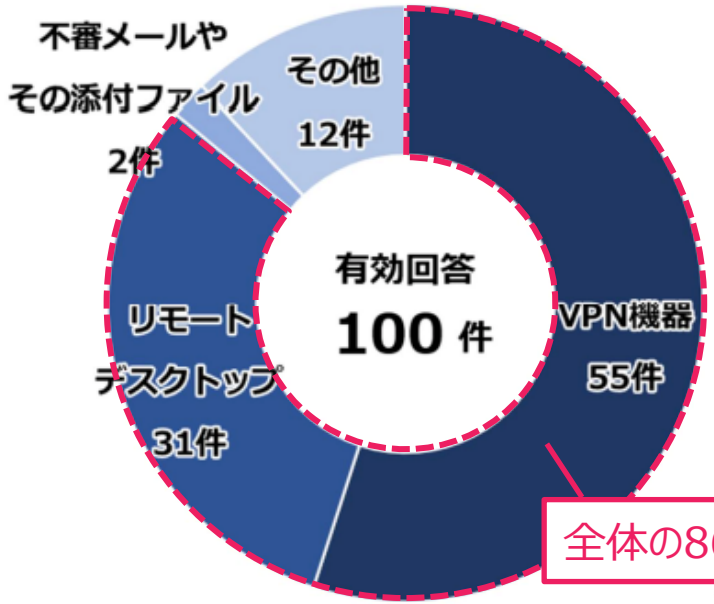
日本国内でも猛威を奮うランサムウェアの脅威

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



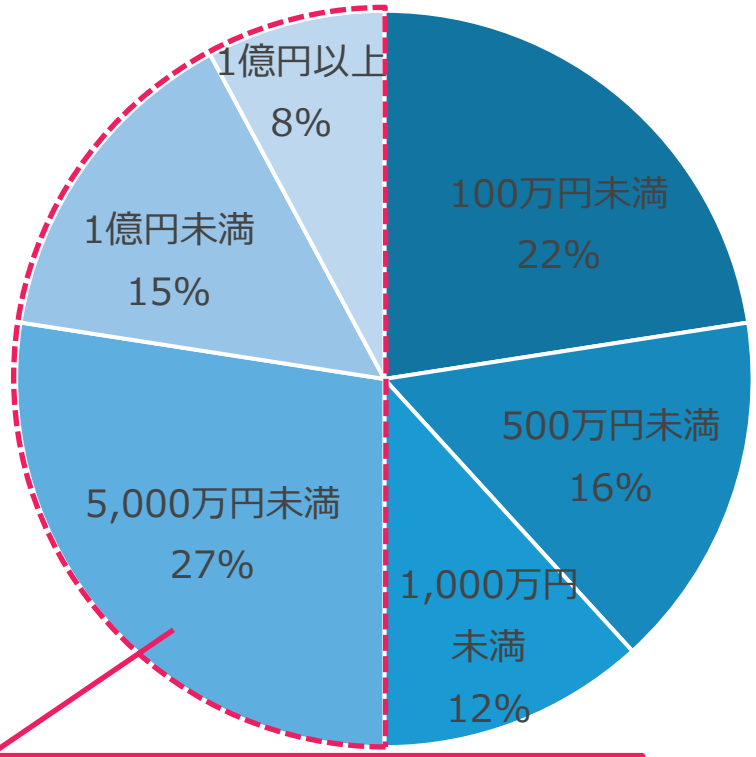
全体の86%が外部からの侵入

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

rubrik

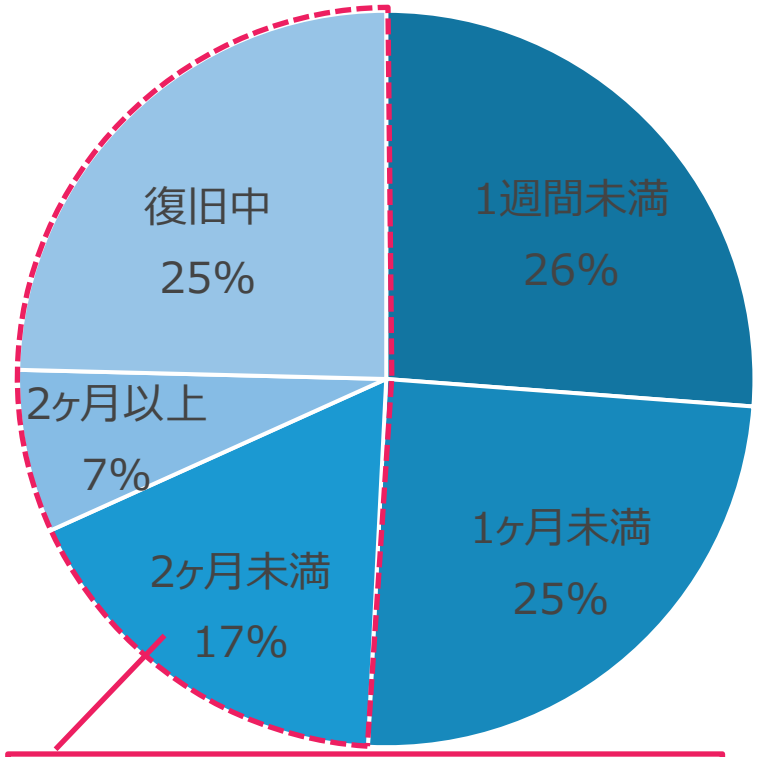
ランサムウェア被害からの復旧にかかる時間と費用

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



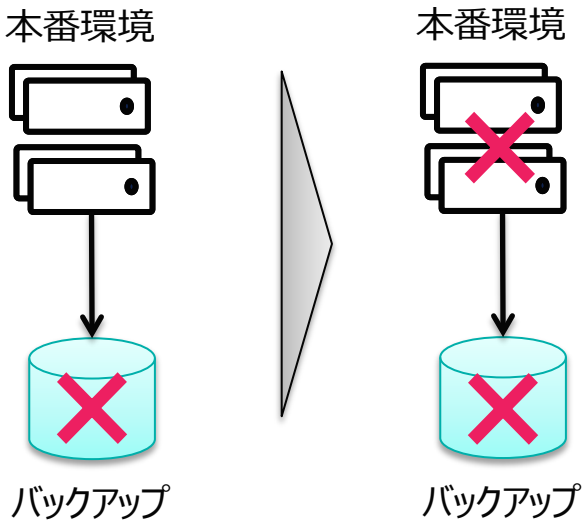
１ヶ月以上かかっても復旧できていない
ケースが全体の49%

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

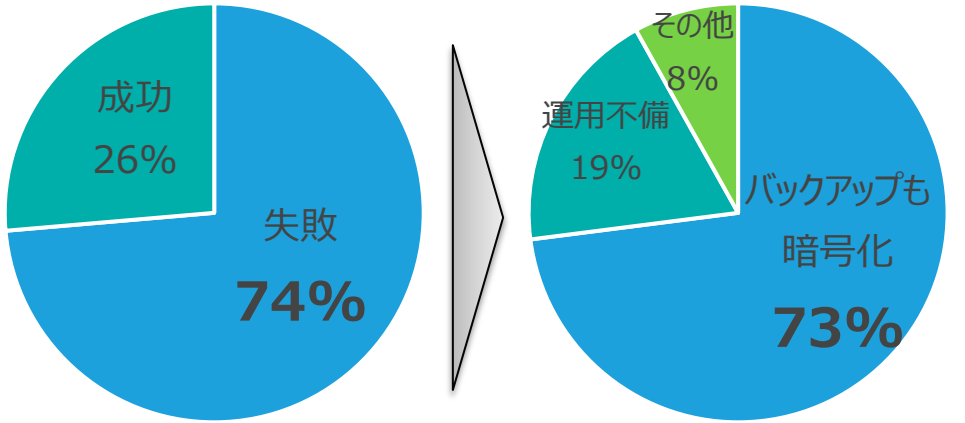
ランサムウェア被害に遭った場合、“従来型のバックアップ”では迅速な復旧が難しい理由①
復旧を遅らせるために、様々な悪意ある手段が取られる

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？

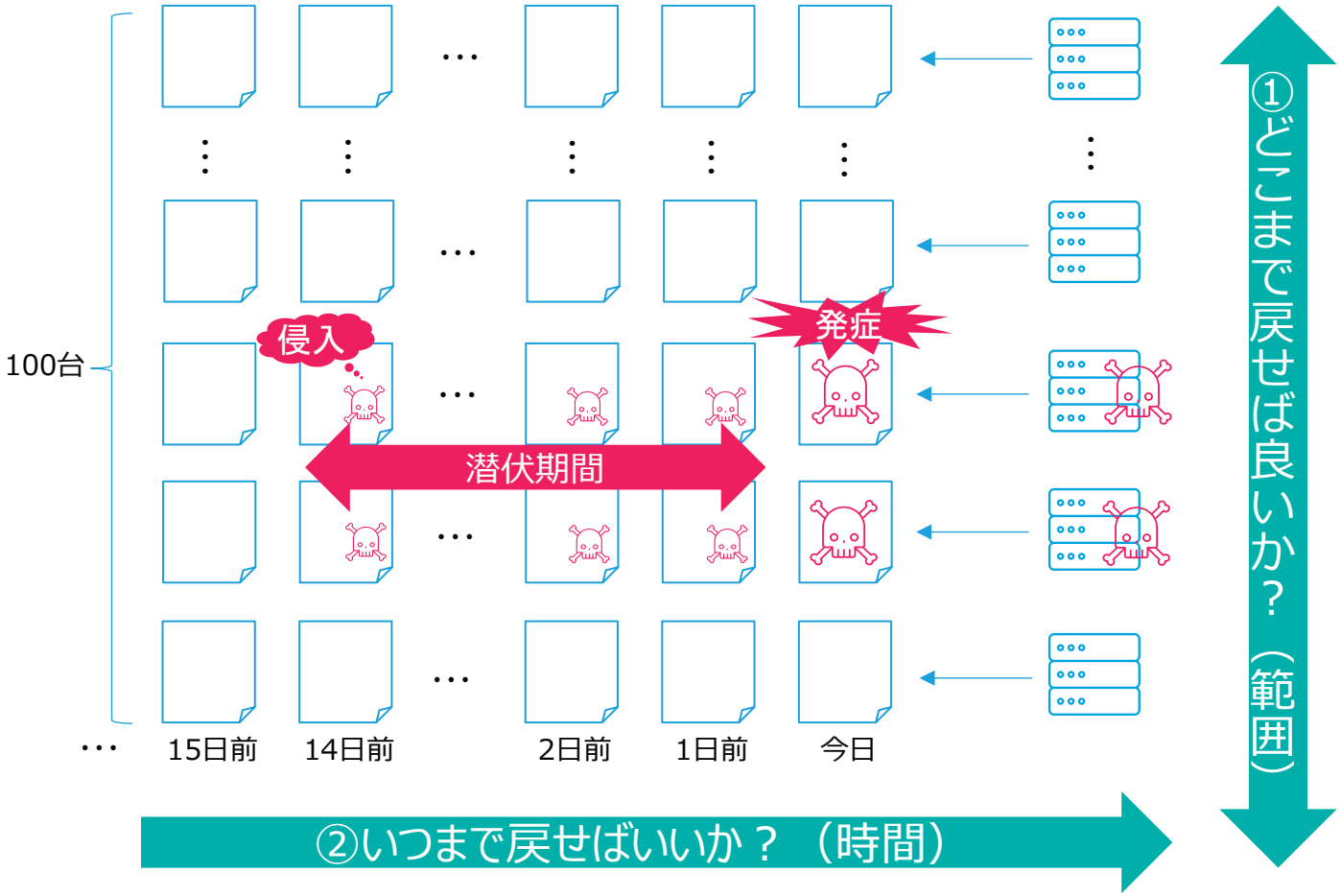


復元結果できなかった理由

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

ランサムウェア被害に遭った場合、“従来型のバックアップ”では迅速な復旧が難しい理由②
被害範囲（＝復旧対象）の把握に時間がかかる



システム障害との違い

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訳ではない**。
影響範囲、感染タイミングを調査しないと、どこまで戻すべきかの判断がつかない。

ランサムウェア被害から安全かつ迅速に復旧するためには？

絶対的な データ回復力	正確な データ可観測性	最適な データ復旧
絶対に**改竄、乗っ取りができないバックアップ**を構築すべし	被害範囲を正確に特定するために、**バックアップデータを分析**すべし	復旧プロセスを確立し、**誰でも復旧可能な仕組み**を作るべし

Rubrikの機能に置き換えると・・・

①データレジリエンス

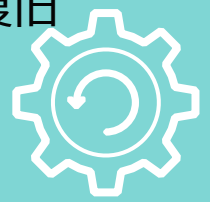
バックアップデータをあらゆる攻撃から
とにかく確実に守る

②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

③データリカバリ

誰でも簡単、かつ迅速に、
安全なデータを復旧

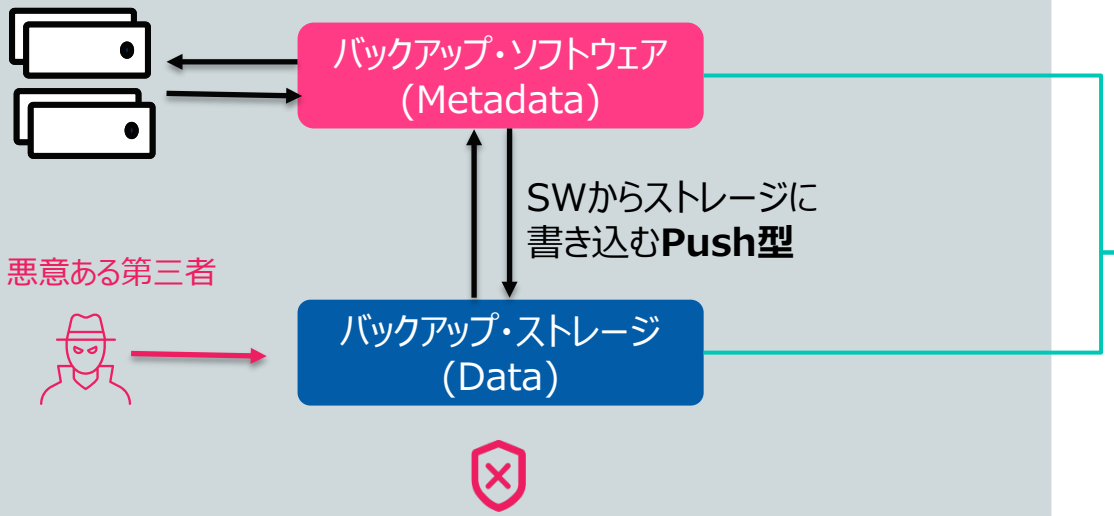


rubrik

①データレジリエンス：

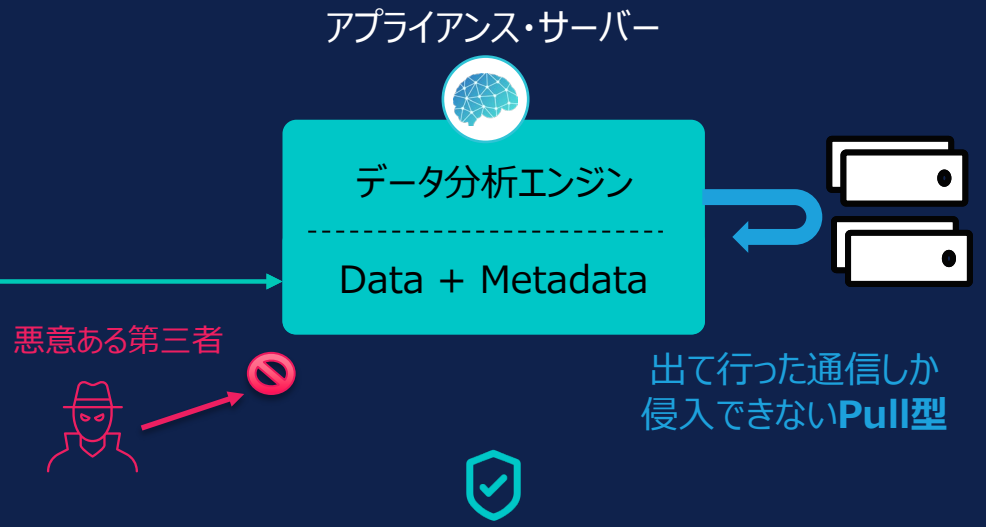
Rubrikが”ハードウェア＋ソフトウェア一体型”にこだわる理由

従来型のバックアップ＆リカバリ



「FireWallで守られた社内ネットワークの中に侵入されることは無い」という前提で作られたシステム構成
（フル・トラスト・アーキテクチャ）

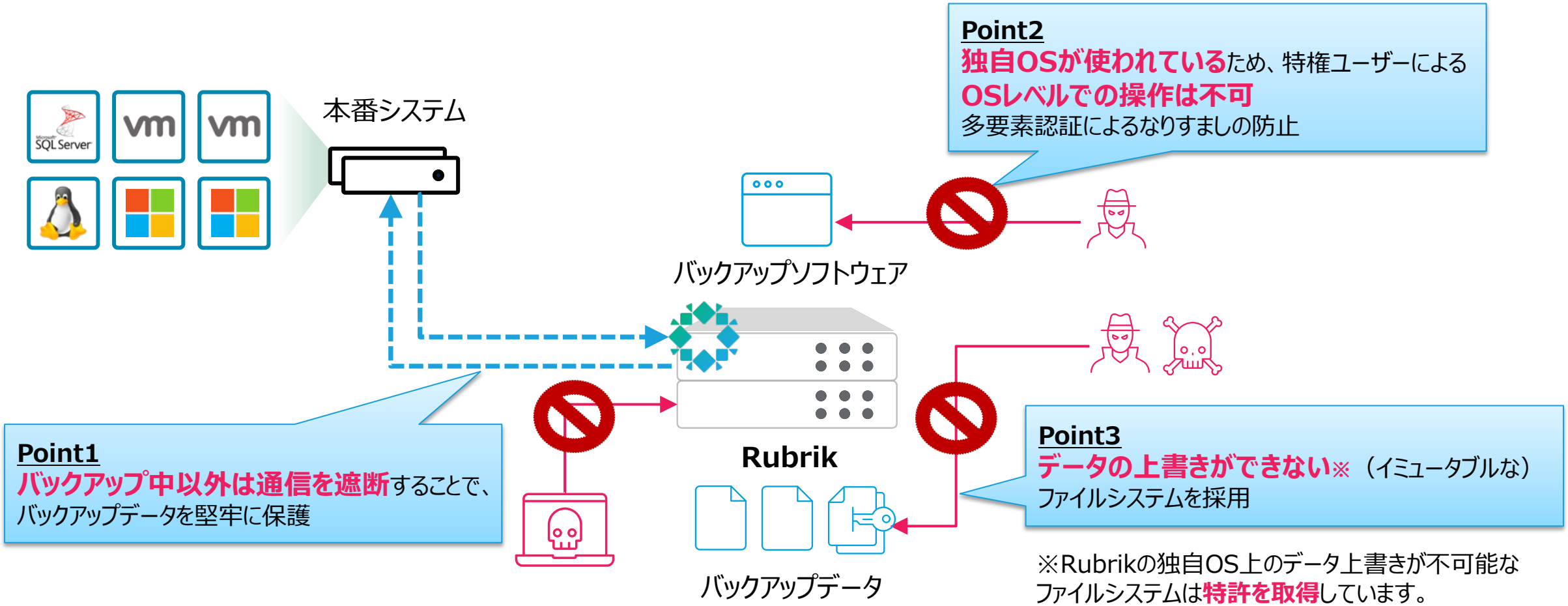
Rubrik のHW＋SW一体型



「どれだけしっかり防御しても、社内ネットワークの中に侵入される可能性はある」という前提で作られたシステム構成
（ゼロ・トラスト・アーキテクチャ）

①データレジリエンス：

「侵入」されてもデータを「破壊」させないRubrikの仕組み



Point1
バックアップ中以外は通信を遮断することで、
バックアップデータを堅牢に保護

Point2
独自OSが使われているため、特権ユーザーによる
OSレベルでの操作は不可
多要素認証によるなりすましの防止

Point3
データの上書きができない※（イミュータブルな）
ファイルシステムを採用

※Rubrikの独自OS上のデータ上書きが不可能な
ファイルシステムは**特許を取得**しています。

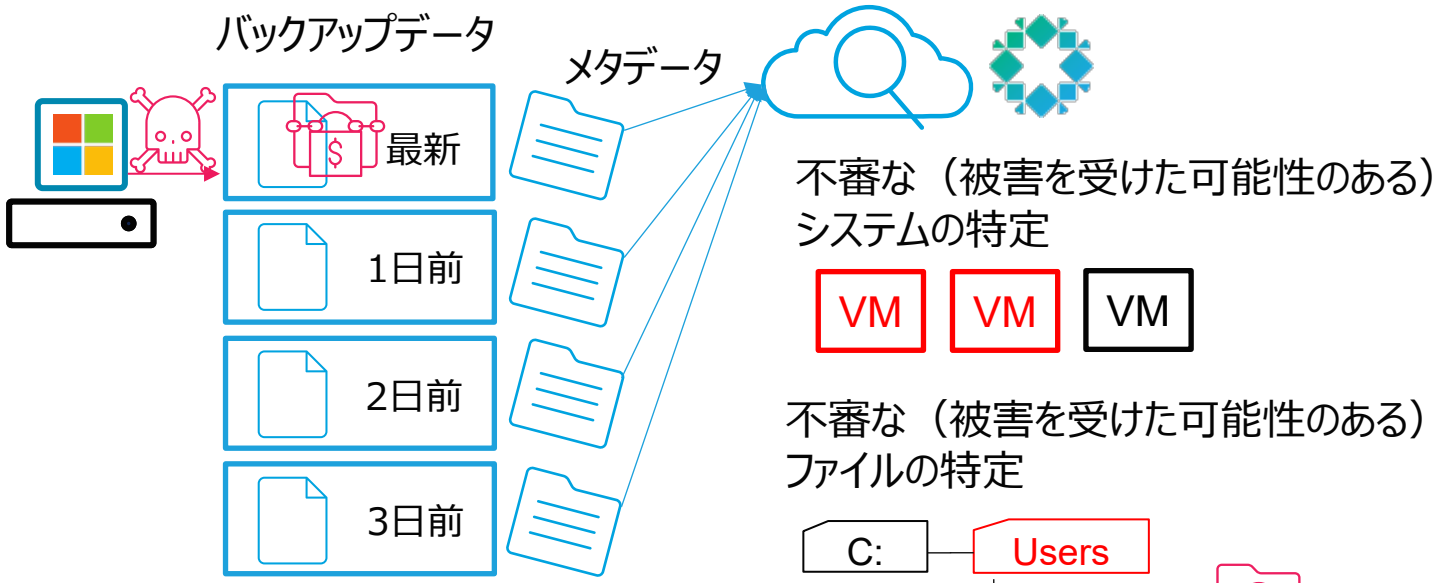
②データオブザーバビリティ：

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？

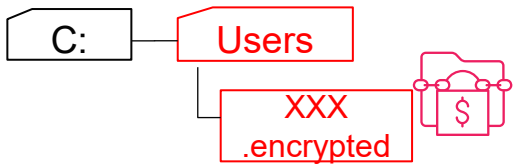
バックアップファイルのメタデータを機械学習で分析し、
いつもと違う振る舞いを検出



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



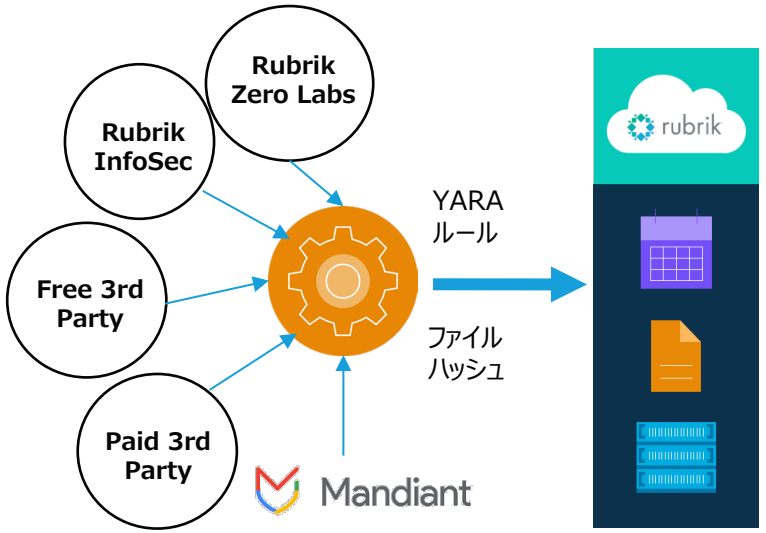
バックアップを取得するたびに
分析処理を行うため、
被害の早期検知が可能！

rubrik

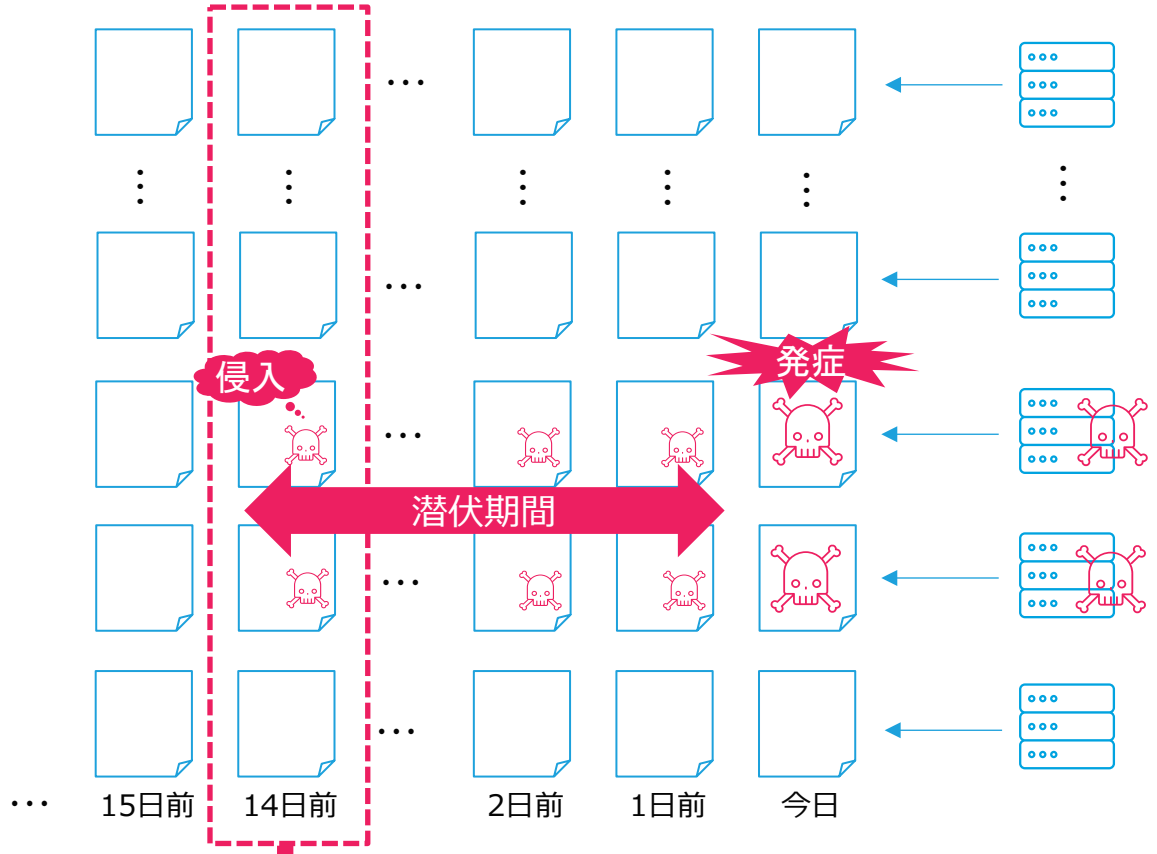
②データオブザーバビリティ：

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



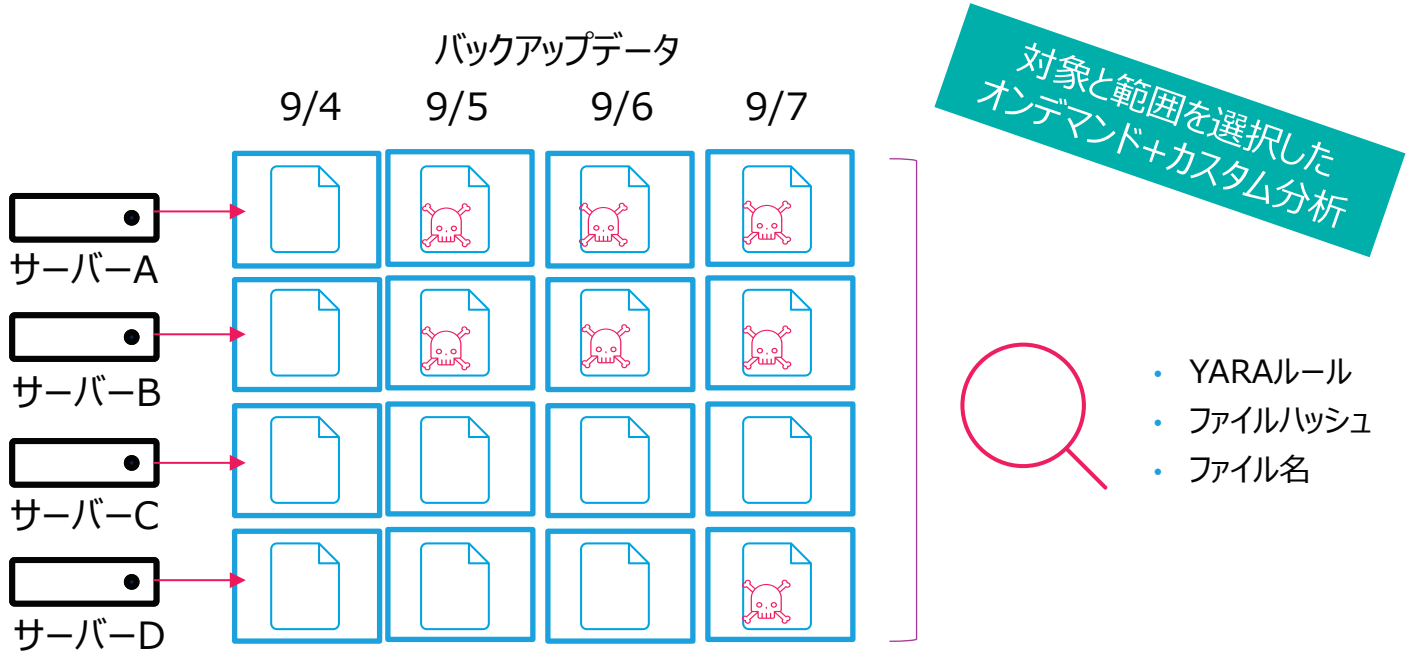
侵入したタイミングで検知できるため、
発症前に対処可能なケースもあり

②いつまで戻せばいいか？（時間）

②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

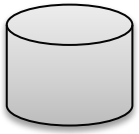
バックアップが暗号化
された場合

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

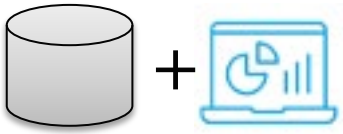
バックアップのリストア＆ランサム有無の確認作業を
クリーンなバックアップが見つかるまで延々と繰り返す

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

バックアップ&リカバリ ソフトウェア市場

Gartner

(2025年)

Figure 1: Magic Quadrant for Backup and Data Protection Platforms

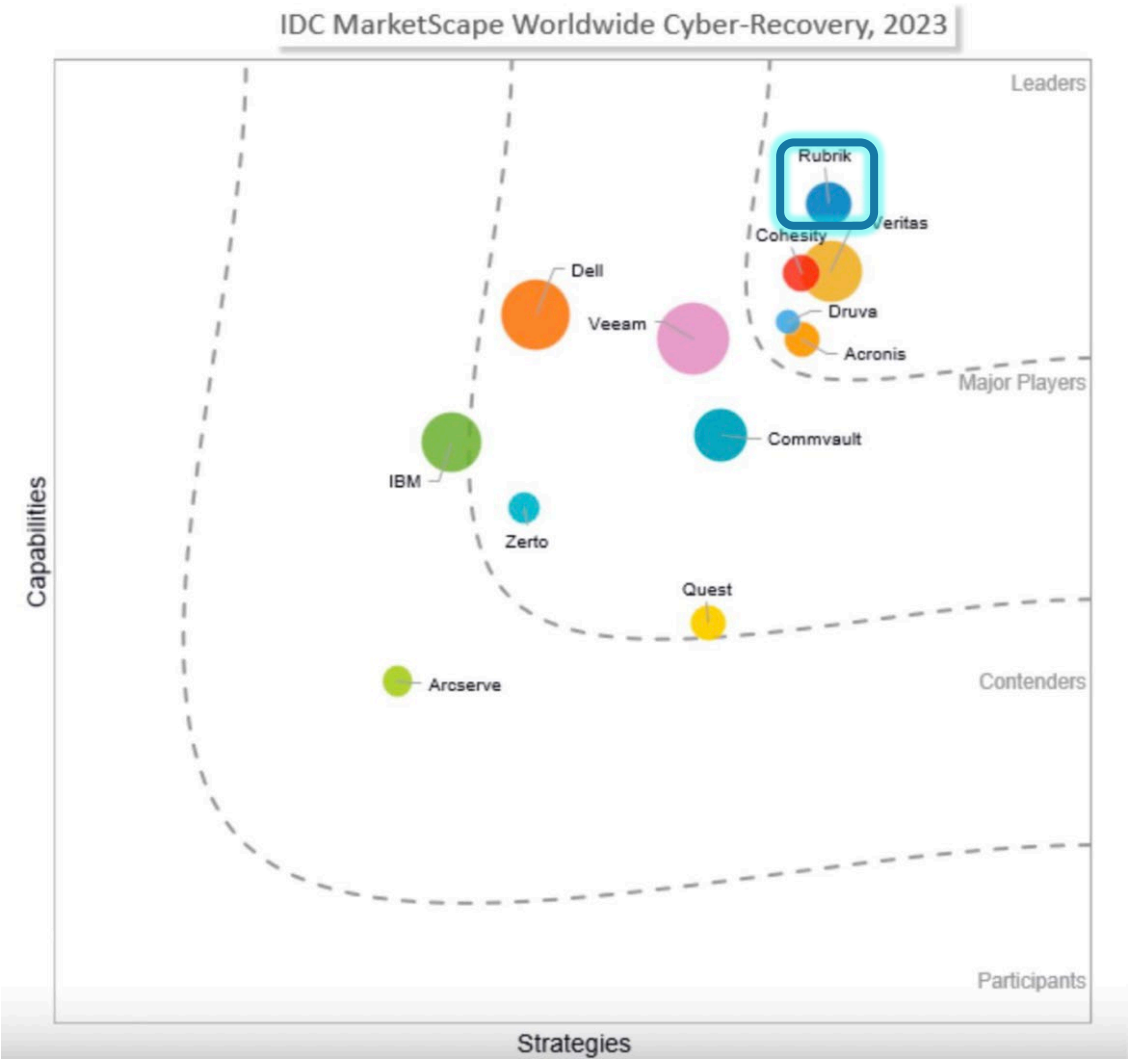
Gartner

グローバルサイバーリカバリ ベンダー評価

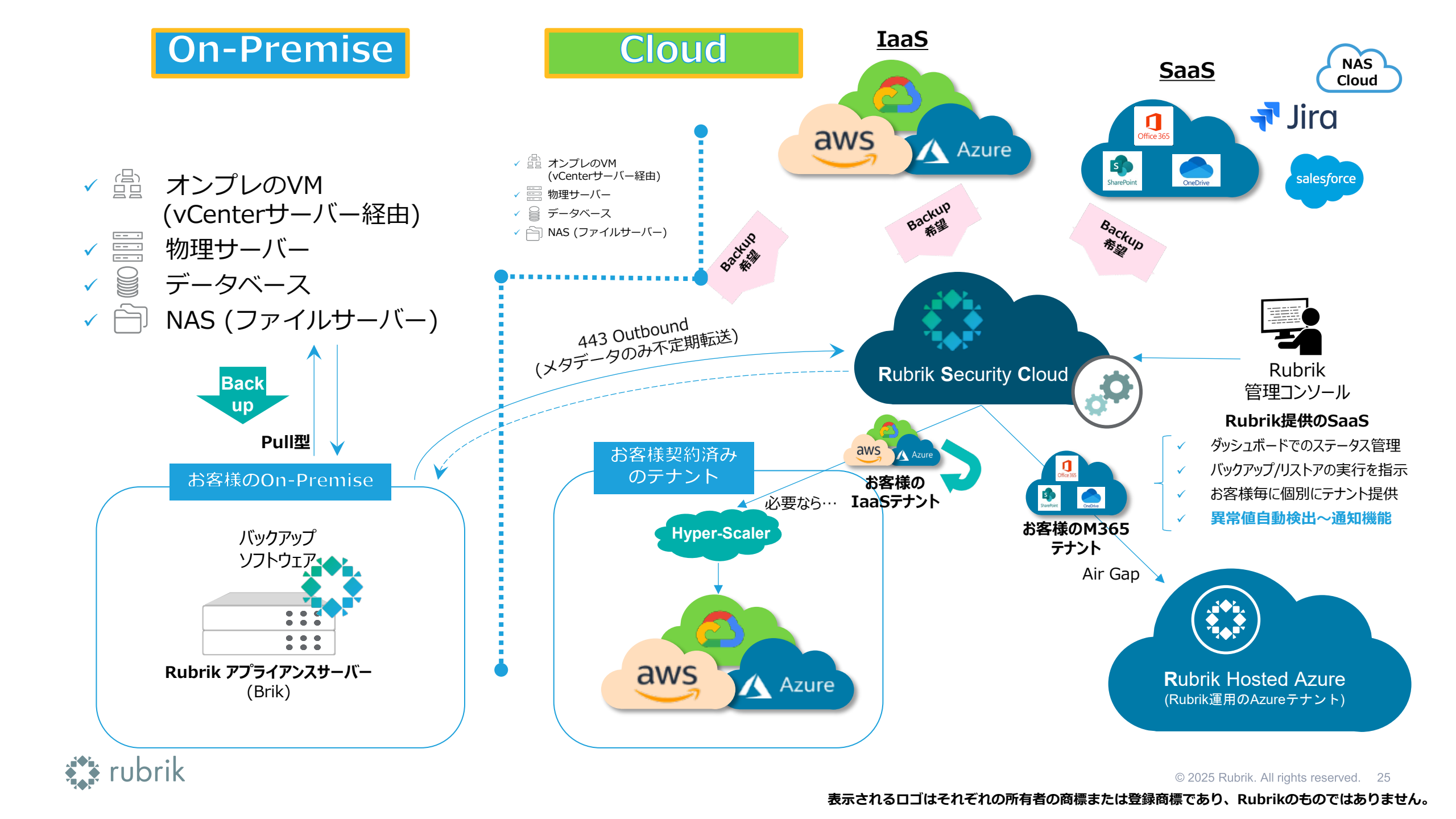
IDC

(2023年)

IDC MarketScape Worldwide Cyber-Recovery Vendor Assessment



rubrik



Don’t Backup.

Go Forward.

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

②HCI基盤拡張に追従するバックアップシステム

③安価なストレージへの遠隔地バックアップ

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
- ✓ 多重なセキュリティ

②HCI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

③安価な遠隔地バックアップ

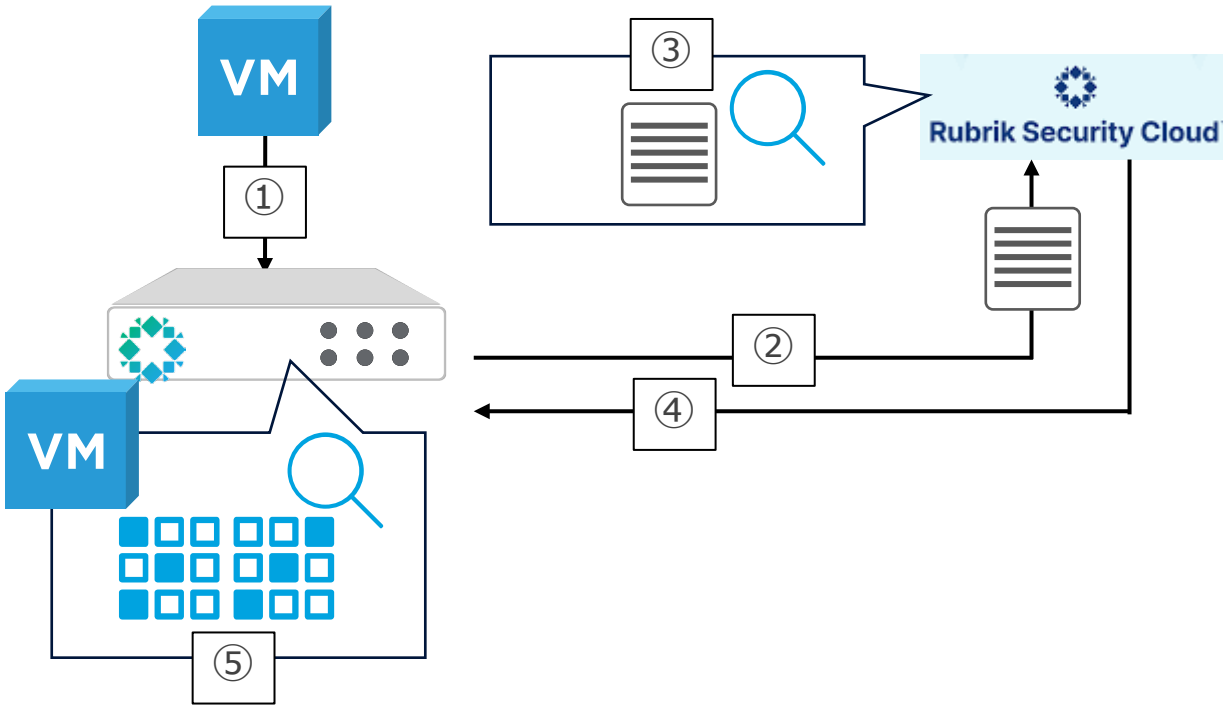
- ✓ NFSストレージへの遠隔地バックアップ

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

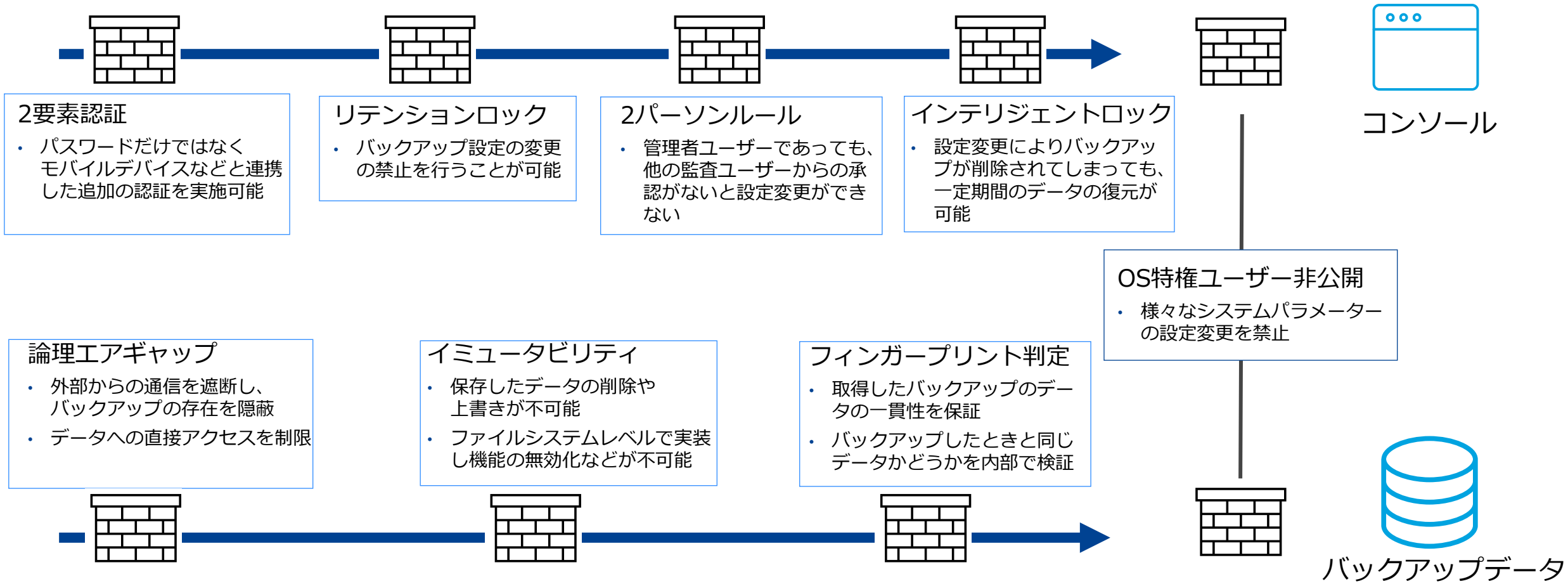


① 仮想マシンバックアップ
② バックアップデータのメタデータをアップロード
③ メタデータを解析（第1段階）
→異常がなければここで終了
④ 実際のバックアップデータの調査を依頼
⑤ バックアップデータのランダム性をチェック（第2段階）
→異常があればアラート発報

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**

①ランサムウェアへの対応

内部犯や誤削除にも対応可能な多重のセキュリティ



2パーソンルール、インテリジェントロックなど<u>コンソールに対するセキュリティ機能</u>も豊富

Panasonic

実績と第三者評価による裏付け

1. **100% のバックアップシステム保護実績**
   特許取得の強固なセキュリティ機能により、
   ランサムウェア被害が発生した150社で100%の復旧実績

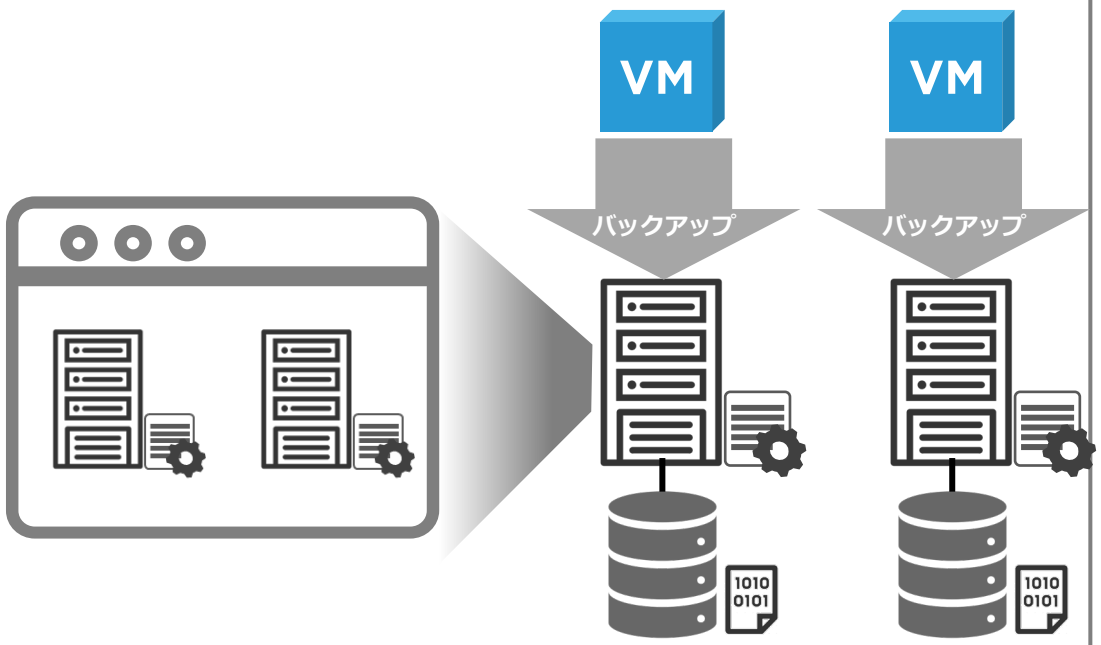
2. **第三者評価機関最高評価**
   当時、第三者評価機関においてセキュリティおよび
   ランサムウェア防御分野で唯一の最高評価

3. **6,000社超の導入実績**
   グローバルで6,000社以上の導入実績があり、
   前年比49%の売上成長率を記録
   国内金融機関にも数多く導入

②HCI基盤スケールアウトへの追従

既存環境

✓ スケールアウト可能



☒ 複雑かつ非効率なスケールアウト

【アーキテクチャ】

- スケールアウト可能 = **単一コンソールでの統合管理**
- 論理的には**区別**される

【スケールアウト作業】

- 設定が**個別管理**であるため、ゼロから設定が必要

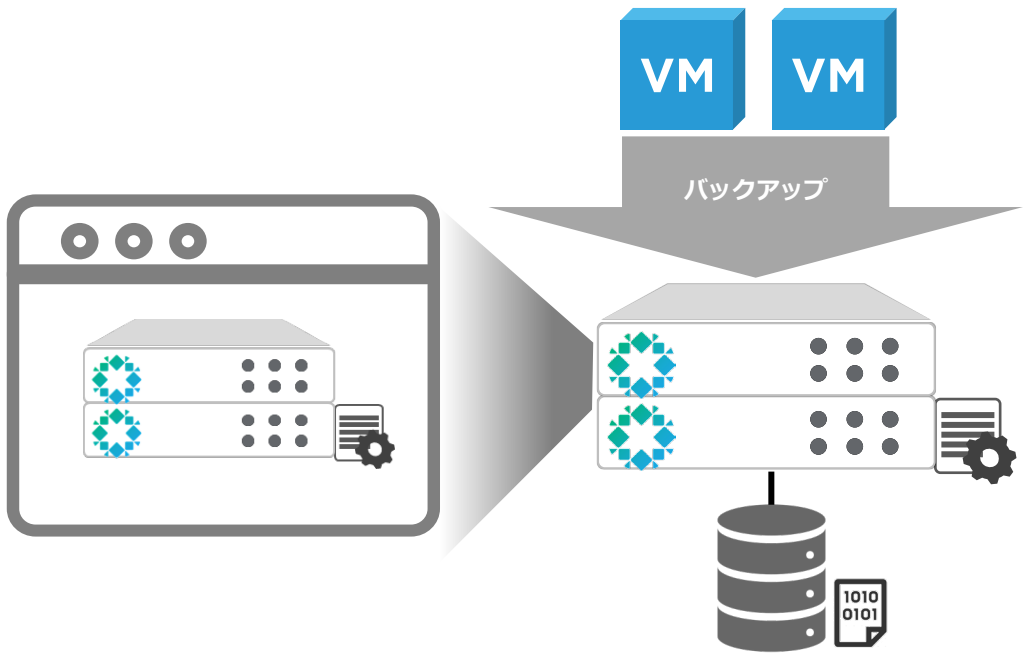
【リソース管理】

- 運用によりノード間でリソース使用状況に偏りが出た場合、バックアップ対象の分散を**管理者が実施**
- バックアップデータもそれぞれで保持され、**重複排除がグローバルに動作しない**

②HCI基盤スケールアウトへの追従

新環境

✓ スケールアウト可能



☑ シンプルかつ効率的なスケールアウト

【アーキテクチャ】

- スケールアウト可能 = HCIライクなスケールアウト
- 論理的には単一

【スケールアウト作業】

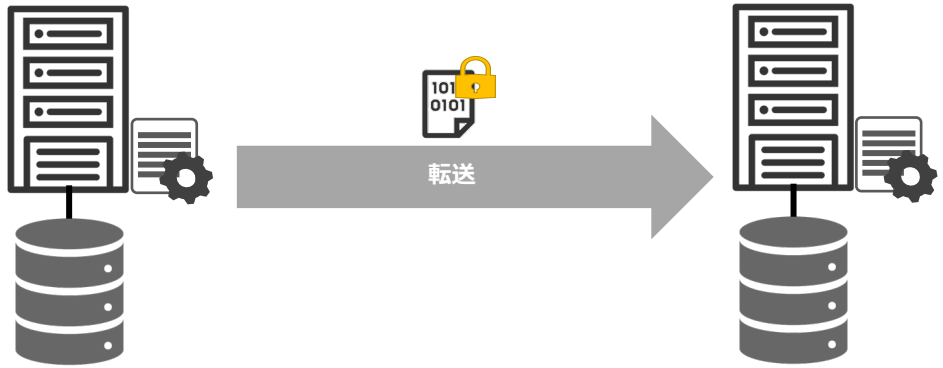
- クラスタで設定を共有しており、追加ノードはIP等の基本設定のみでOK

【リソース管理】

- クラスター単位で各ノードのリソースを共有するため、ノード間での残リソースの偏りが発生しない
- クラスタとしてバックアップデータを保持し、重複排除がグローバルで動作する

③安価な遠隔地バックアップ

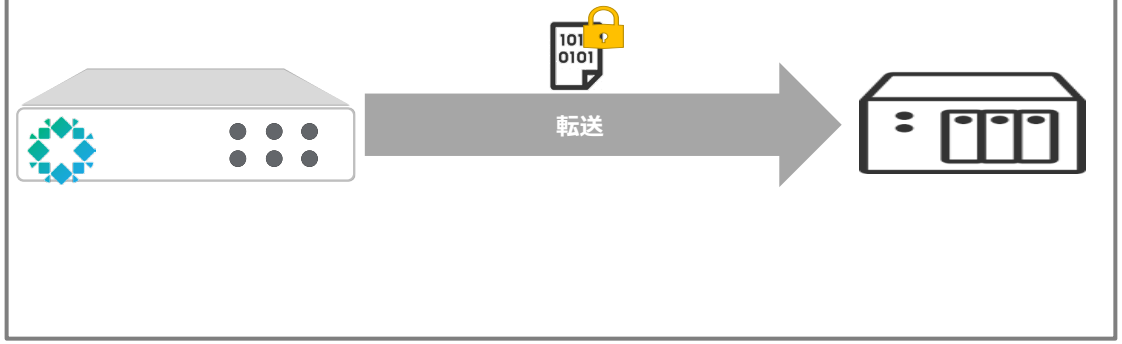
既存環境



☒ 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

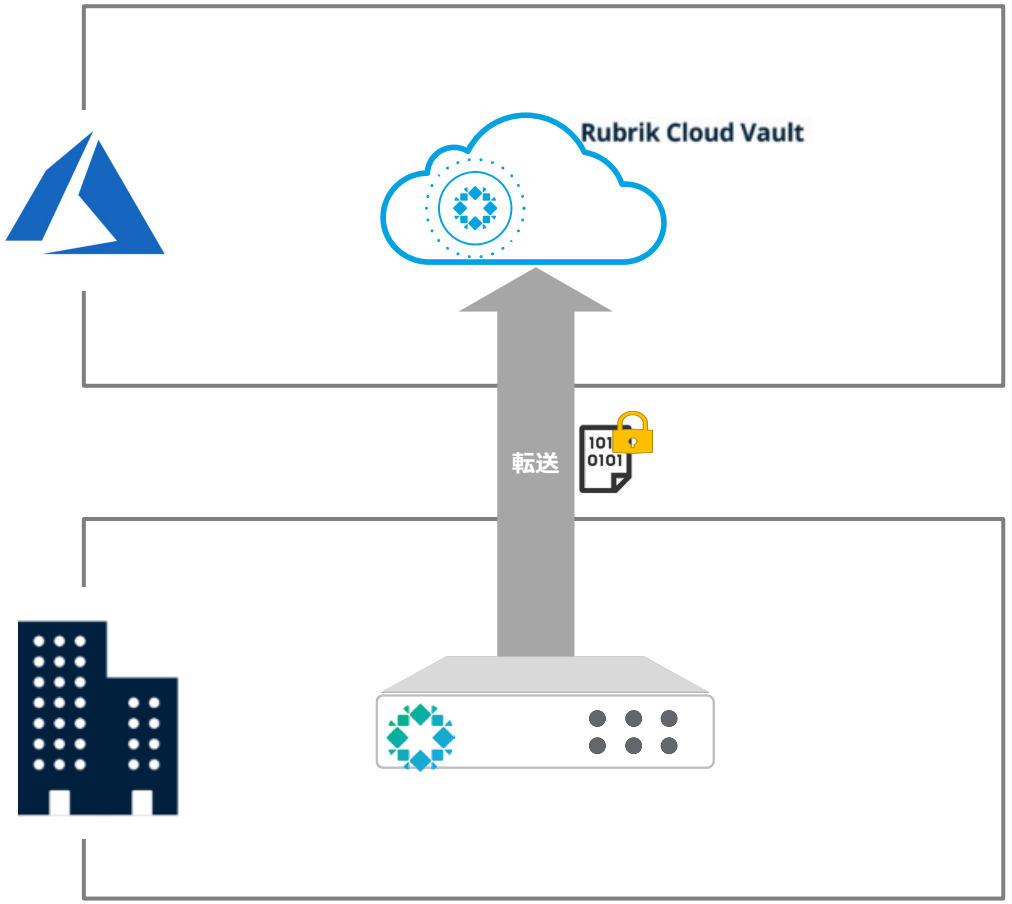
- **NFS v3対応**であればバックアップデータ転送可能
- 汎用NAS採用により**大幅なコストダウン**
- 以下機能も使用可能
  - **転送データ暗号化**
  - **圧縮/増分転送**

Panasonic

“遠隔地バックアップはクラウドにしたい”というケースにも対応可能

Rubrik Cloud Vault (RCV)

- **Rubrik提供のストレージサービス**
  - マイクロソフト社と緊密に連携し、Rubrikが運用するAzure基盤上にて提供される、ストレージサービス
  - Rubrikバックアップアプライアンスで取得したデータをセキュアなクラウド環境上に保管することが可能
- **セキュアなデザイン**
  - 論理的にエアギャップされたストレージ環境をAzure上に構築
  - Rubrikが提供するバックアップサービスのみからのアクセスを許可
  - ストレージ内のデータは、データの削除や改ざんが不可能な、イミュータビリティを構成
  - ストレージ内のデータは、暗号化により保護
- **運用レス/予測可能なコスト**
  - Azure契約/構築作業不要
  - RubrikのSaaSコンソール（Rubrik Security Cloud）から、対象のアプライアンスに追加を実施
  - 費用については固定（変動なし）、かつストレージへのアクセスや、ネットワークダウンロードの課金もすべて込み



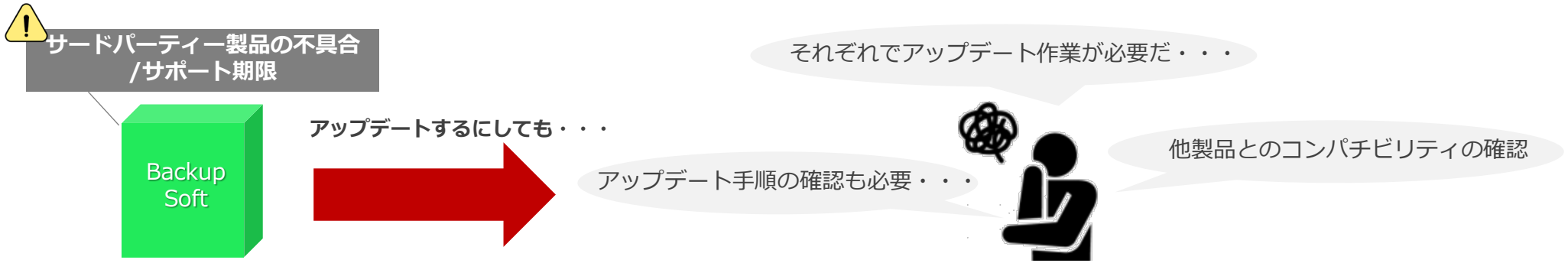
実際に導入して分かったRubrikのメリット/デメリット

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

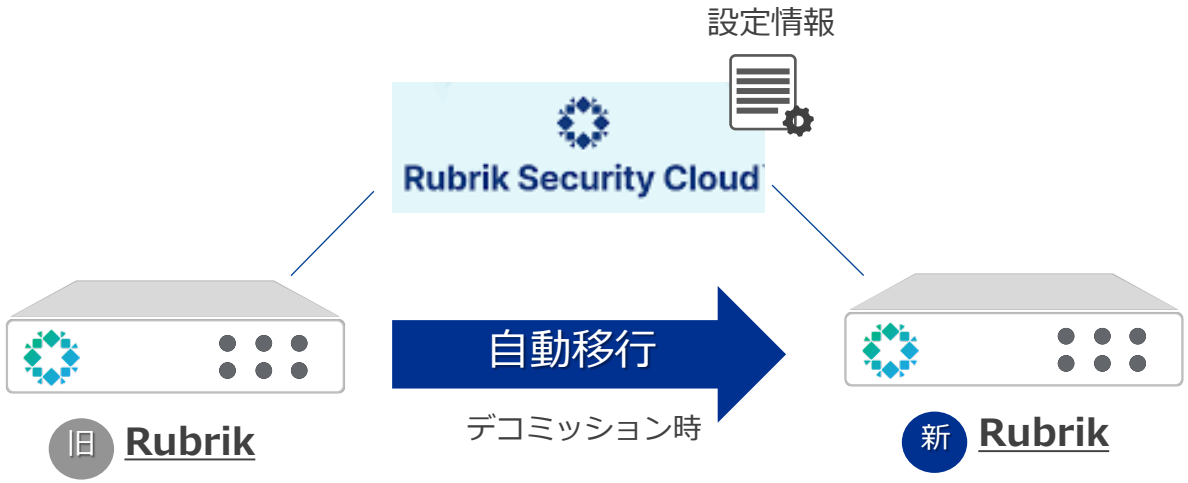
・Rubrikは、オールインワンパッケージ構成のため
上記を意識せず、数回のクリックでのアップデートが可能

・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

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

・**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

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

- 変化する要求事項に“真に対応した機能”であるか比較して見定める必要があります。

- アップデートや障害対応といった導入前には見落としがちな“運用コスト”も踏まえた製品選定を行うことが重要です。

Rubrikでは、第三者評価機関と実績が示す
“最高レベルのランサムウェア対策”だけでなく、
オールインワンによる“運用コストの低減”が実現できます。

Panasonic