Panasonic

ランサムウェアに強い次世代バックアップ

Rubrik サービス紹介資料

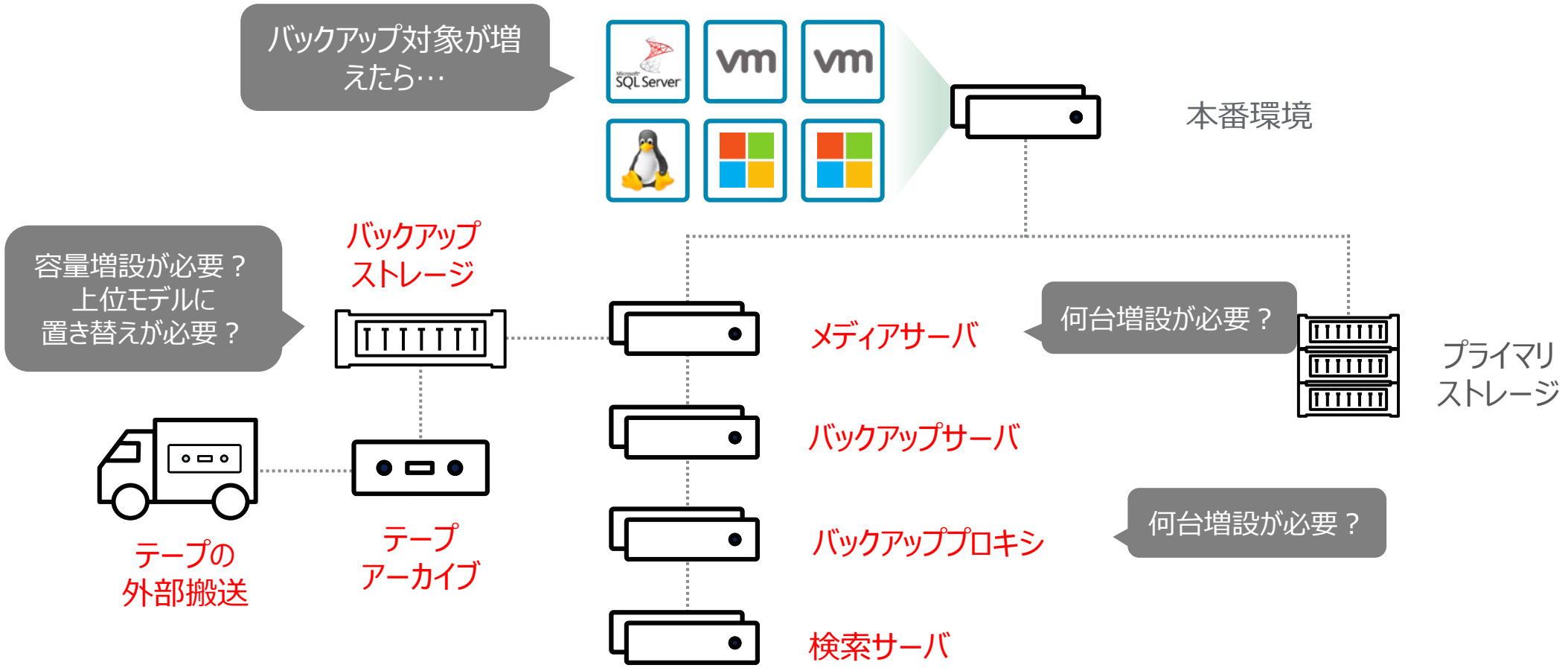
パナソニック デジタル株式会社

バックアップ環境の主な課題

#	項目	概要	想定されるリスク
1	システムの複雑化	• 従来型のバックアップでは、システムを形成するのに、必要なコンポーネントが多い • さらにバックアップ対象のシステムが拡大している中で、バックアップシステム自体が複雑に	• システムの安定稼働が維持できない • バックアップシステムの拡張が困難。継続的なデータ保護が実現できない
2	運用工数の増大/属人化	• 新しいバックアップジョブの作成や、既存ジョブのメンテナンス/調整作業で、日々の多くの工数が取られている • ジョブの作成/調整が高度で、限られた専門家しか実施できない	• 既存環境の維持に工数をとられ、新規の取り組みを加速できない（新たなデータ環境の保護に取り組めない） • 専門家の離職などにより、システムの維持を行っていくことができない
3	復旧時間の増大	• バックアップ対象のシステムが増えていたり、取得対象のデータも増大しているため、復旧に多くの時間が必要に • 別媒体や遠隔地にバックアップを保管しているため、そもそもバックアップデータを取り出すのに時間がかかる	• サービス再開までに時間を要し、ビジネスへの影響が発生する
4	不十分なセキュリティ	• サイバー攻撃による懸念が高まる中、バックアップシステム自体が、サイバー攻撃により利用できなくなる懸念 （バックアップデータの削除やバックアップシステムのダウンなどが発生）	• 復旧する手段が失われてしまう（長期のサービス停止や、データを救うための身代金の支払いなどにより大きな損失が発生）

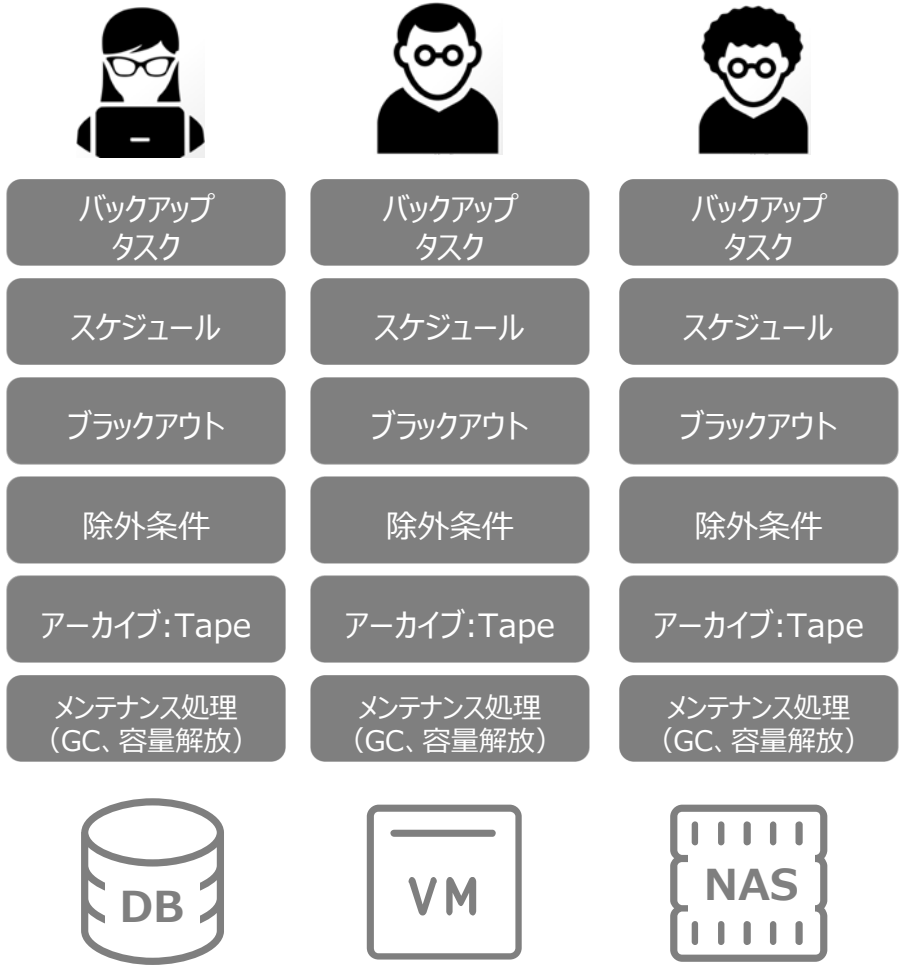
従来型バックアップシステムの課題

様々なコンポーネントで構成され、手間のかかるメンテナンスと、複雑な増設/拡張方式



従来型バックアップシステムの課題

バックアップジョブの作成、および時間内にバックアップが完了するための綿密な調整作業に多くの工数が必要



多数のシステム管理者で

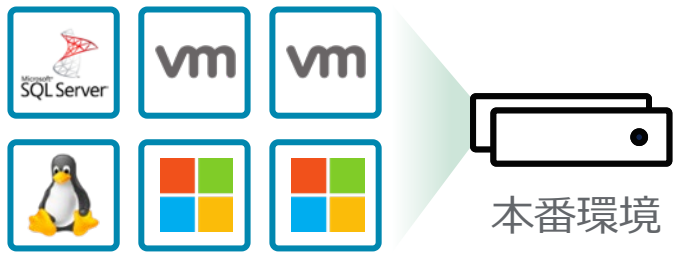
多数の事細かなバックアップジョブを

実行タイミングを考慮しながら

バックアップ対象毎に作成する必要あり

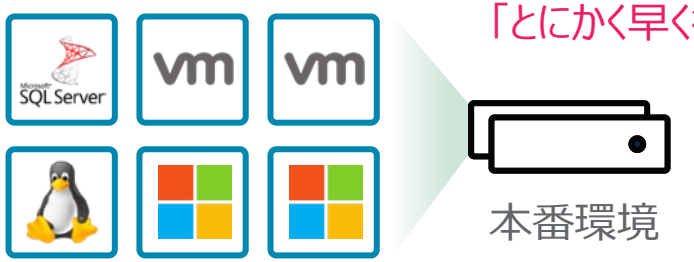
従来型バックアップシステムの課題

バックアップは取っているが、リストアにどれぐらいの時間がかかるか懸念



バックアップ取得

ユーザーからは、
「とにかく早く復旧してほしい」



リストア

当初よりもデータが大きく、
データを戻すのに想定よりも
多くの時間を要する

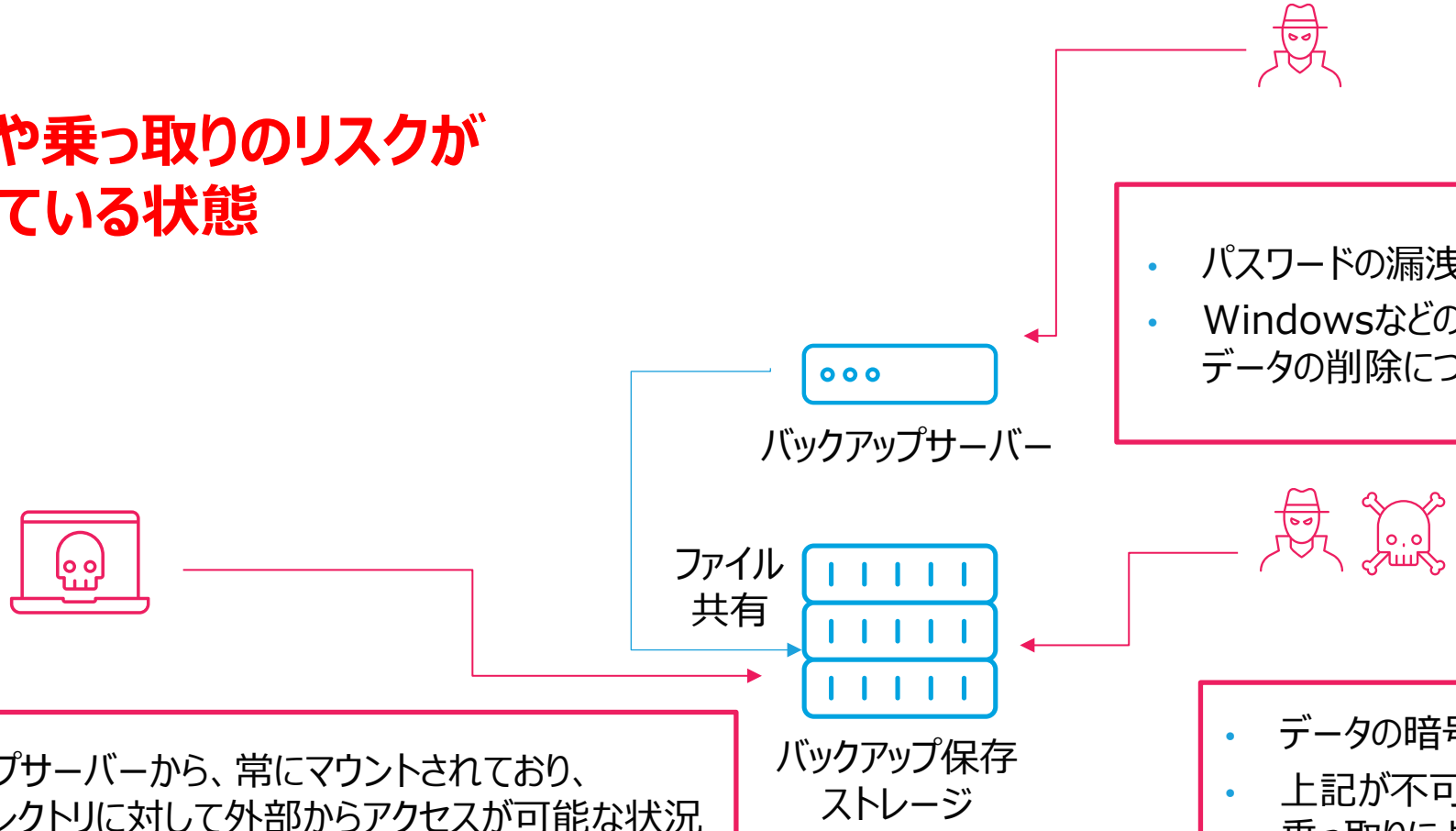
そもそもリストア作業ができる人が
限定的（属人化）

別媒体からのデータ取り出しに時間がかかる

従来型バックアップシステムの課題

サイバーアタックに対する対策が不十分。多くの脆弱性（攻撃可能なポイント）を抱えている

改ざんや乗っ取りのリスクが存在している状態



- パスワードの漏洩により容易になりすましが可能に
- Windowsなどの特権ユーザーの乗っ取りにより、データの削除につながる設定の変更が可能に

- バックアップサーバーから、常にマウントされており、共有ディレクトリに対して外部からアクセスが可能な状況

- データの暗号化や削除ができてしまう
- 上記が不可能な設定でも、権限ユーザーの乗っ取りにより解除や変更が可能に

これからのバックアップに求められる要件

セキュリティも考慮した、次世代のバックアップが必要に

ランサムウェア感染からの復旧に関わる課題

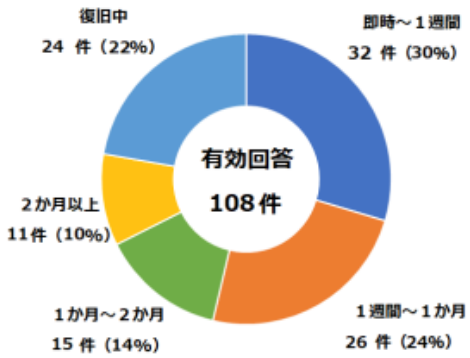
- **狙われるバックアップ**
  - 復旧の退路を断つために、ハッカーはバックアップを標的に

バックアップシステムの乗っ取り
- 管理者権限の奪取によるソフトウェア削除
- バックアップ設定の変更とデータの削除

バックアップデータの改ざん
- 外部からバックアップデータへのアクセスと削除、暗号化

- **時間がかかる復旧**
  - バックアップがあっても、安全なデータを判断して、大量のリソースに対してリストアを実施するのに非常に時間がかかる
  - 時間がかかれば損害も増大する

被害にあった企業の70%以上は、復旧に1週間以上、半分近くは1か月以上かかっている



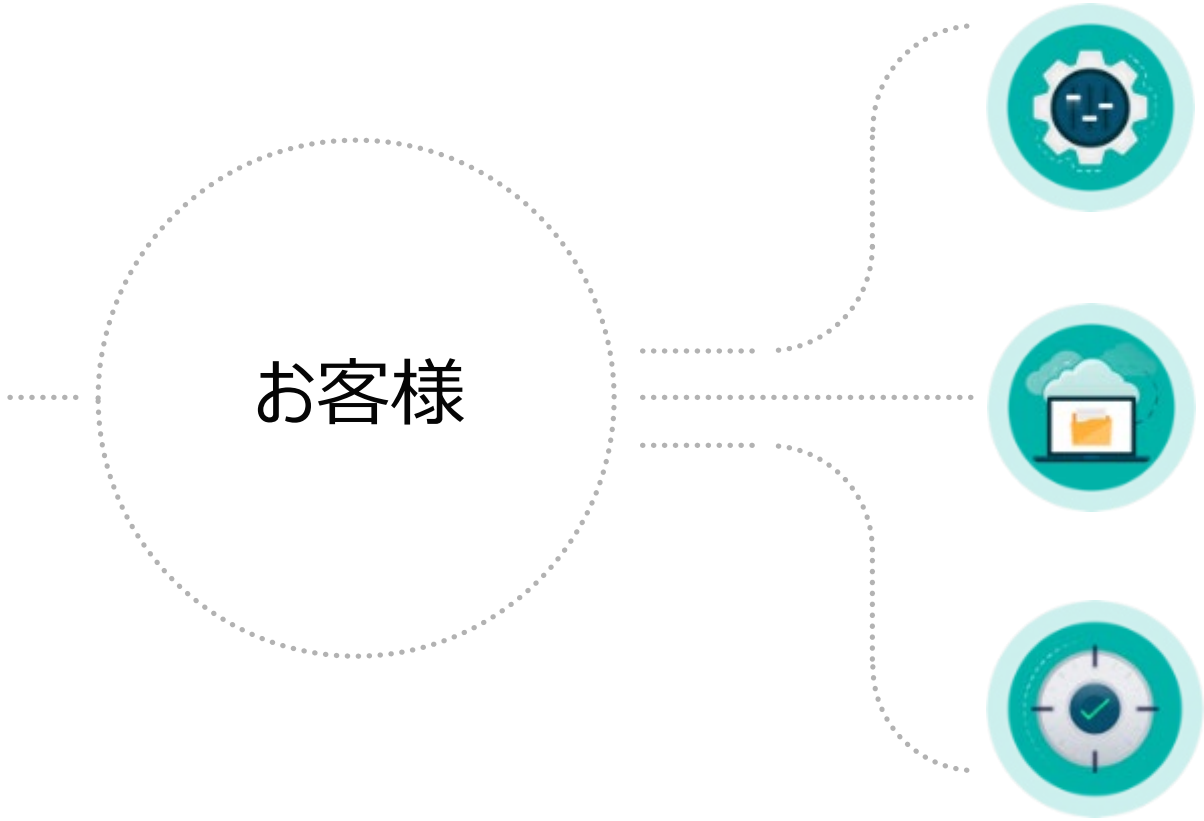
警察庁：被害からの復旧に要した期間

Gartnerが提唱する ランサムウェア対策に求められるバックアップ

Gartner：how to recover from a ransomware attack using modern backup

1. **イミュータビリティ**
   - バックアップデータの削除や改ざんを防止
2. **エアギャップ技術**
   - バックアップデータへの直接アクセスを防止
3. **インスタントリカバリ機能**
   - 高速なデータリストア技術による迅速な復旧の実現
4. **ランサムウェア検出機能**
   - バックアップデータ内のランサムウェアの検出
5. **自動的なデータリストア**
   - 一斉、かつ自動化されたデータのリストア機能

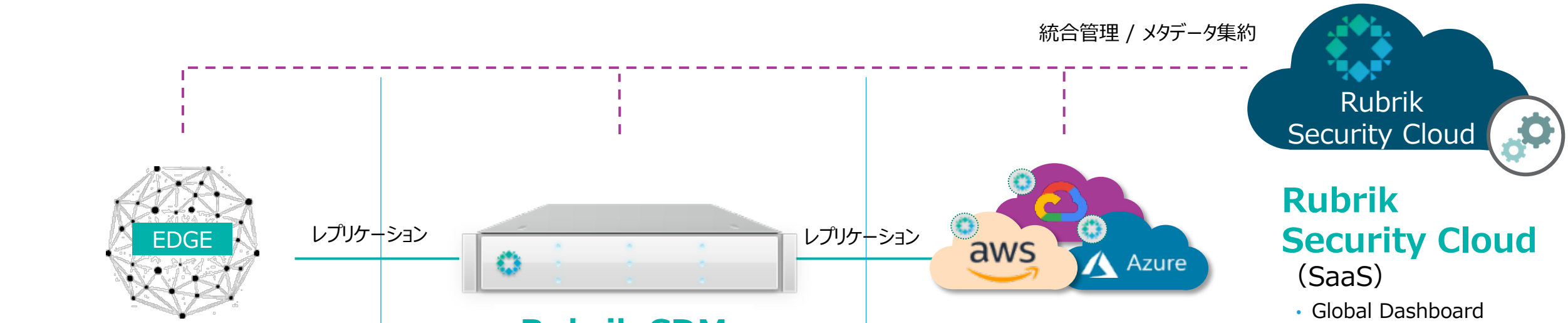
Rubrikで支援可能なこと



- 貴社基盤システムにおけるデータセキュリティの強化
  - 堅牢なデータ保護基盤の構築
  - バックアップ運用負担の低減
  - オンプレミス、クラウド、M365などにわたる、総合的なデータの保護
  - サイバーアタックに備えた、データ視点での情報の可視化・復旧手段の確保

機能概要

Rubrik 主要製品ポートフォリオ



Rubrik CDM

Edge（仮想アプライアンス）
- 店舗や工場などの拠点のデータ保護
- 仮想環境上に展開
- CDMと連携前提

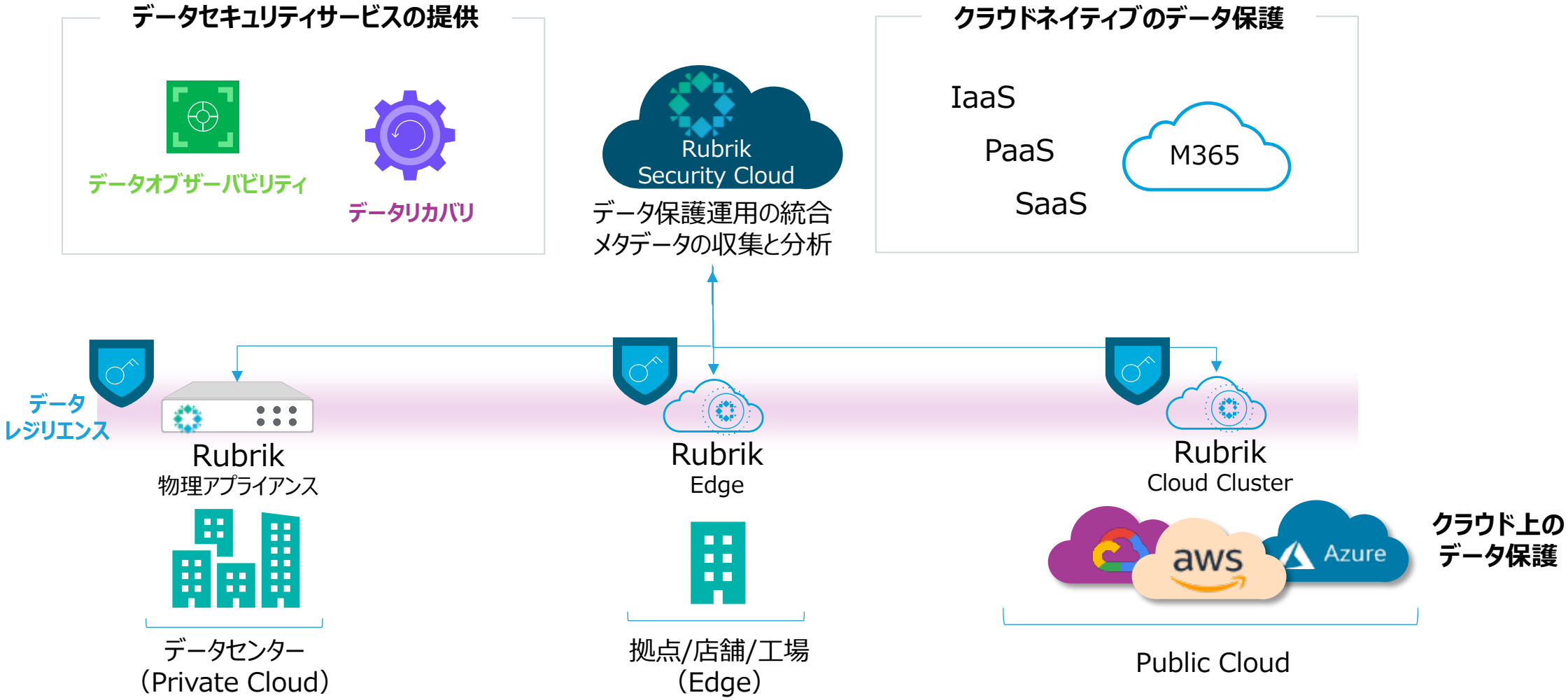
Brik（物理アプライアンス）
- VM、NAS、DB、ファイルなどの保護
- 迅速なリカバリ
- クラウドやNAS、オブジェクトへのアーカイブ
- バックアップ/アーカイブデータの活用

Cloud Cluster
- クラウド上でCDM環境を実現
- VMC on AWS や AVS、GCVE の保護

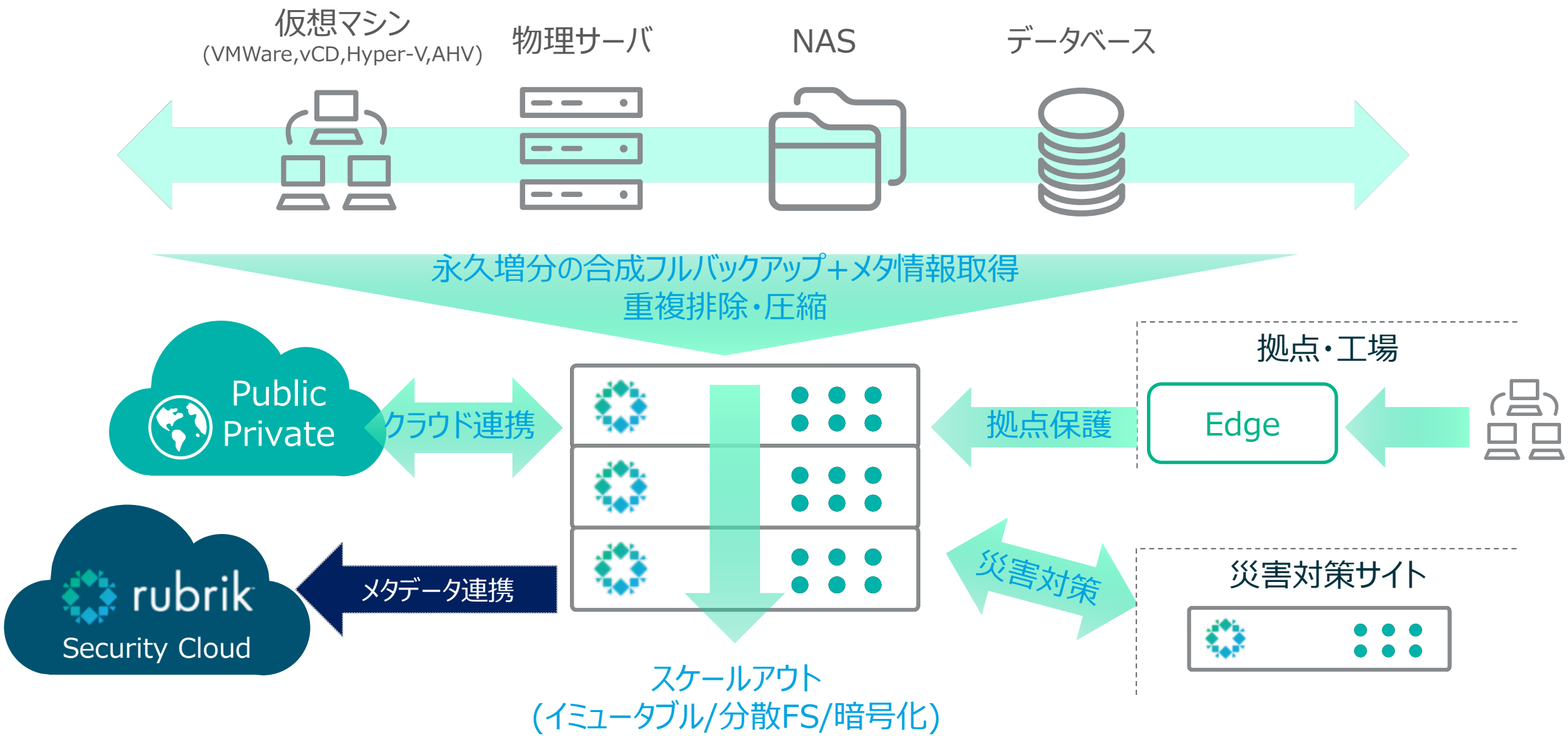
Rubrik Security Cloud（SaaS）
- Global Dashboard
- Cloud Nativeの保護
- M365の保護
- Cyber Attack の検出と復元
- 様々なSaaSサービスを提供

あらゆる場所でデータセキュリティを強化

SaaSコントロールプレーンから、バックアップを通じて企業内のデータのセキュリティを強化

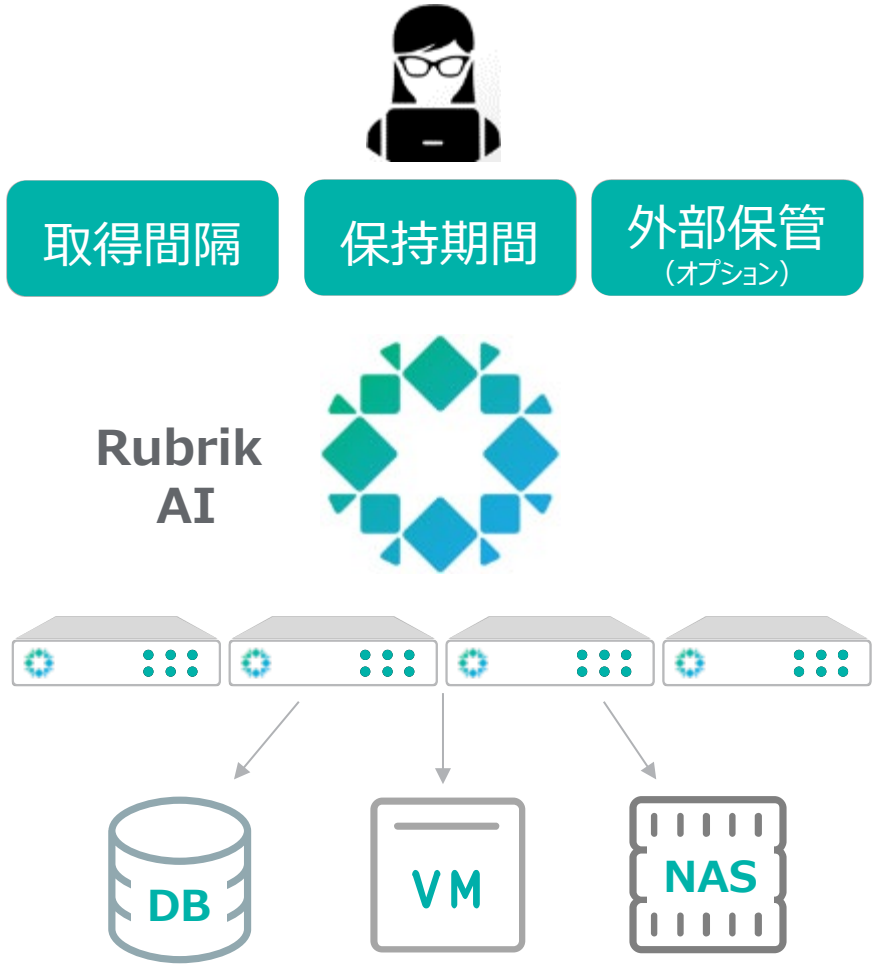


Rubrikによる統合バックアップとデータ運用



自動化とシンプル化

“ポリシー”による自動化されたバックアップ運用を実現し、複雑なバックアップジョブの作成や運用から解放



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

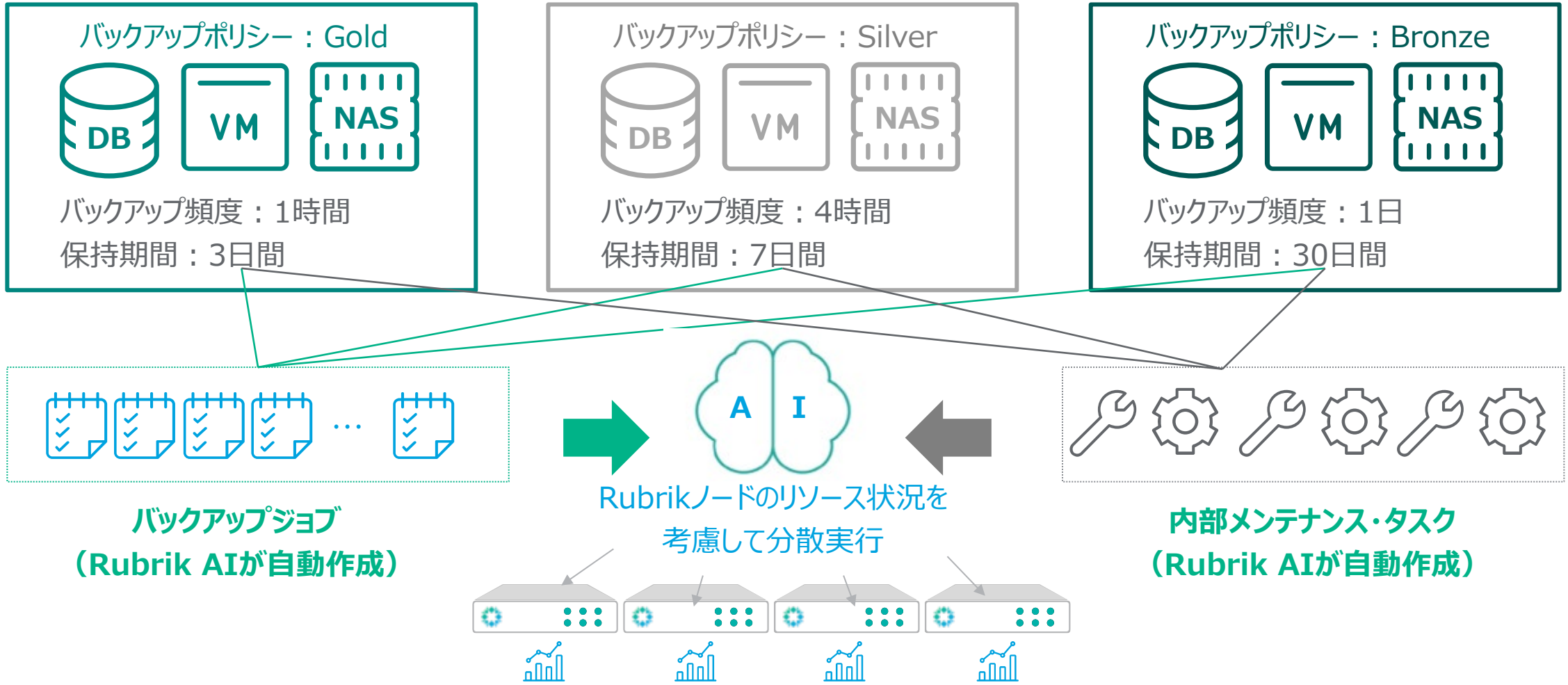
AIが最適なジョブと実行タイミングを
自動生成し

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

自動化とシンプル化

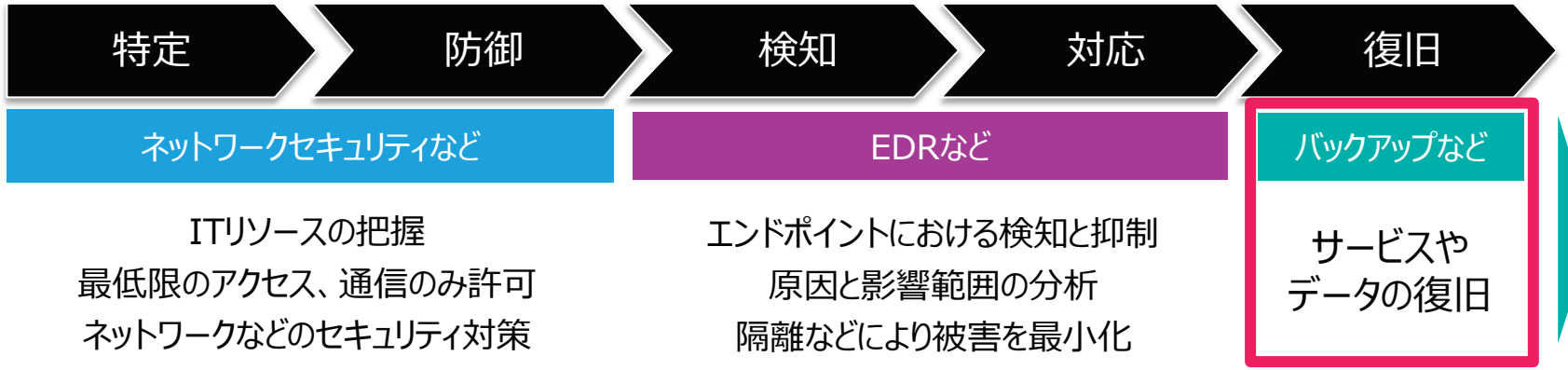
自動化エンジンが、ジョブの作成とスケジューリングを実施



これからのセキュリティ対策ではバックアップが重要に

あらゆるセキュリティ対策を実施しつつ、ランサムウェアに感染される前提での、ポストインシデント対策の強化へ

NIST：セキュリティフレームワーク



総合的なセキュリティ対策と防衛

- あらゆるリソースの把握とリスクの監視
- あらゆる境界やネットワーク、データへのセキュリティ対策の実施

最低限の権限とアクセス

- 多要素認証などID管理と認証の強化
- 最低限必要な権限やアクセスに限定

脅威の検知

- 各エンドポイントにおけるマルウェアなどの検知

インシデント対応と復旧

- 隔離による拡散の抑制
- 原因や影響範囲の分析
- データの復旧やサービスの再立ち上げ

バックアップの重要性の高まり

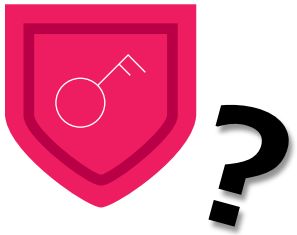
- 防御を突破され、検知を免れ、ランサムウェアに感染される前提において、早期復旧のためのバックアップは不可欠
- 各ベンダー/機関がバックアップを確実に取得することを推奨

Sophos
ランサムウェアはバックアップによって決まる。身代金を支払うのではなくバックアップからの復元により、存続可能な、管理可能な損失のみに抑制される

Fortinet
重要なシステムやデータをバックアップする。データのバックアップがビジネス要件を満たすこと、迅速に復元できるようにしておくことが重要

Gartner
すべての企業はリスク管理の一環として、ランサムウェア攻撃からの復旧策を講じるべき

感染の現場で実際に起きたこと

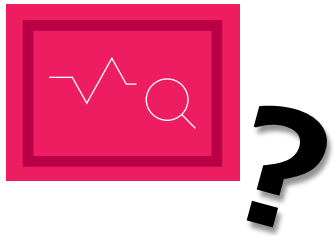


データは復旧可能か?

IT担当者

バックアップはとっていたが
バックアップデータが暗号化

OS管理者権限が奪われて
バックアップソフトが
アンインストールされてしまった

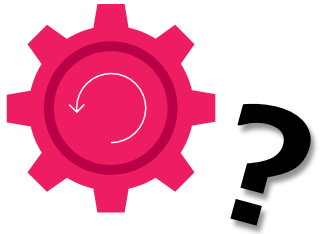


攻撃/影響の範囲は?
データの重要度は?

セキュリティ担当者

どこまで暗号化されたのか、
どこまでリストアすればいいのか

暗号化されたデータに
機密情報が入っているのか、
身代金を支払うに値するのか



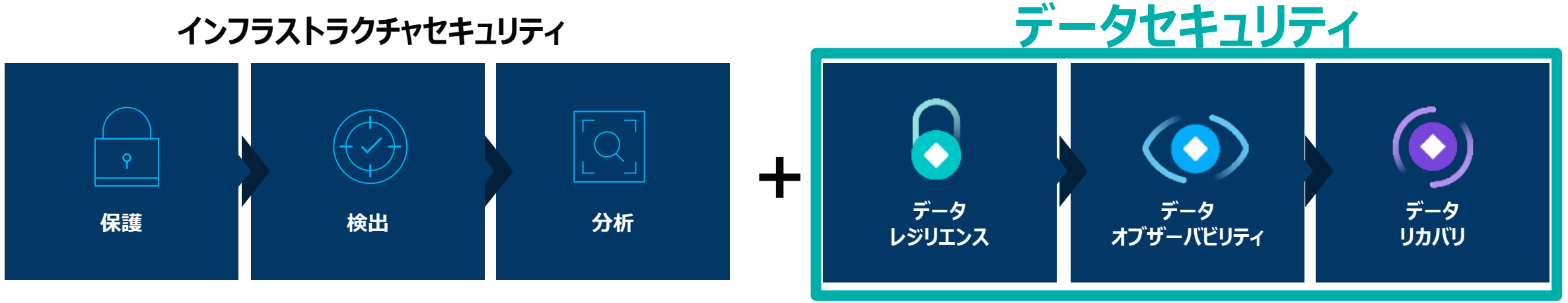
復旧により再感染しないか?
迅速に復旧できるか?

インシデント担当者

どのバックアップデータなら
安全にリストアできるのか

バックアップデータは
厳重に保管されており、
まずは取り出すことが必要

単なるバックアップではない、
確実な復旧のために、データに対する新たなアプローチが必要

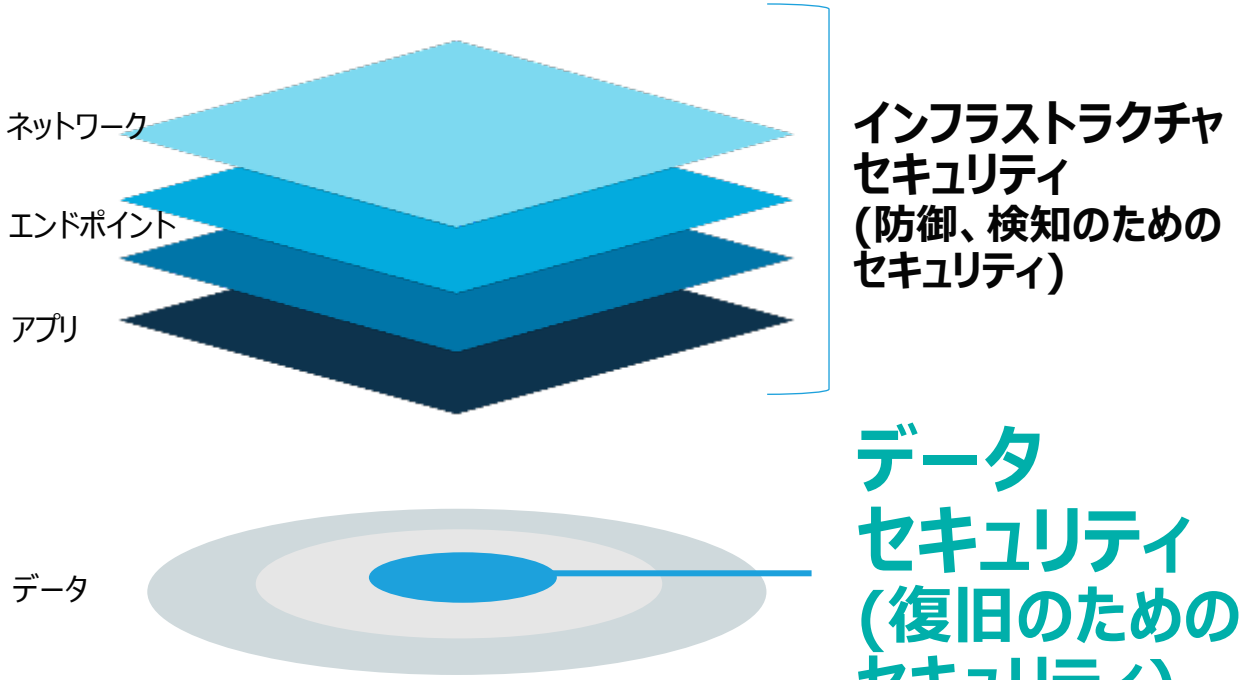


rubrik

Zero Trust
Security

データセキュリティにより、企業の”復旧力”を強化

Rubrik ゼロトラスト データセキュリティ



インフラストラクチャセキュリティ（防御、検知のためのセキュリティ）

データセキュリティ（復旧のためのセキュリティ）

Rubrikは、バックアップを通じた高度なデータセキュリティにより、サイバーアタックからの確実かつ迅速な復旧を実現

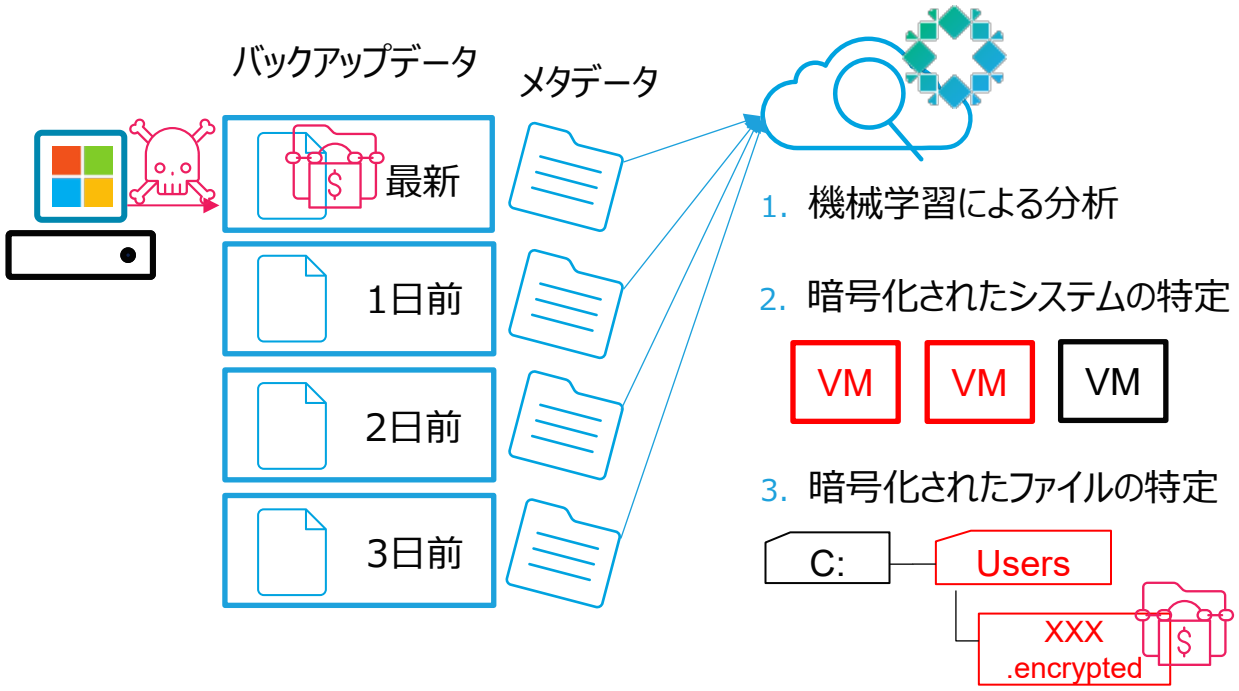
- **Data Resilience（データレジリエンス）**
  - バックアップシステムやデータを堅牢に保護し、継続的なデータ保護とデータ復旧手段を確実に確保
  - **イミュータビリティ / エアギャップ技術 など**
- **Data Observability（データ可観測性）**
  - 機械学習を活用したバックアップデータの分析を通じて、脅威の監視と検出、重要なデータに対するリスクを可視化
  - **ランサムウェア検出機能 など**
- **Data Recovery（データリカバリ）**
  - リスクあるデータを隔離し、安全に、迅速かつ自動的なデータの復旧を実現
  - **インスタントリカバリ機能 / 自動的なデータリストア など**

データオブザーバビリティ：感染したシステムの検出と影響範囲を特定

2つの方法でバックアップデータを分析し、ランサムウェア感染を検知

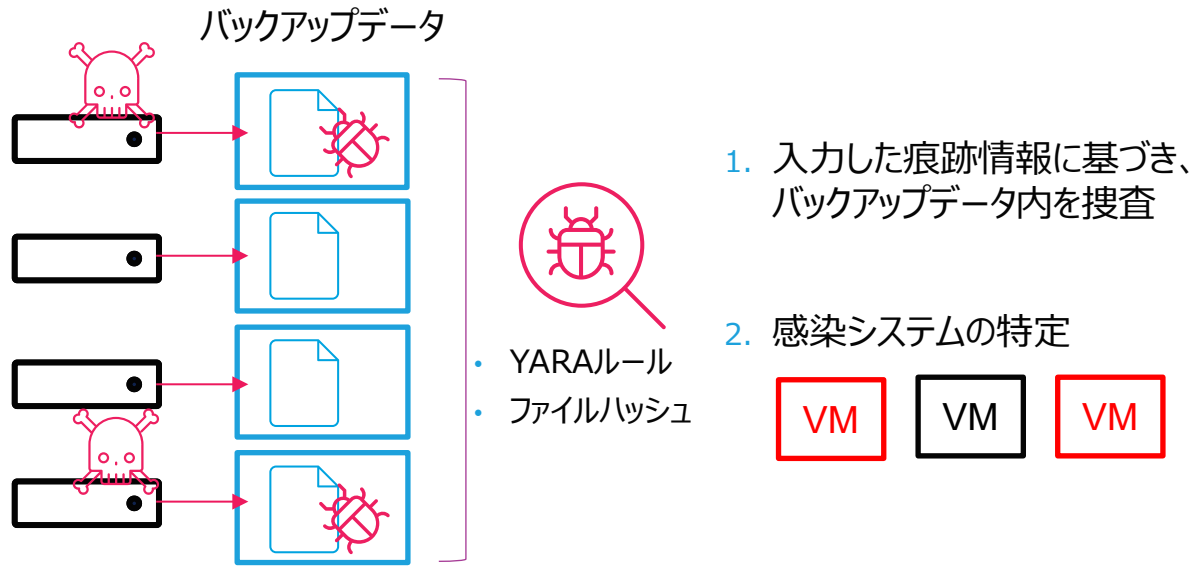
ふるまい検知 (Ransomware Investigation)

メタデータを機械学習で分析し、ランサムウェアにより
暗号化されたシステム / ファイルを検出し影響範囲を特定



脅威ハンティング（Threat Hunting）

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、いつからランサムウェアが侵入したかを検出

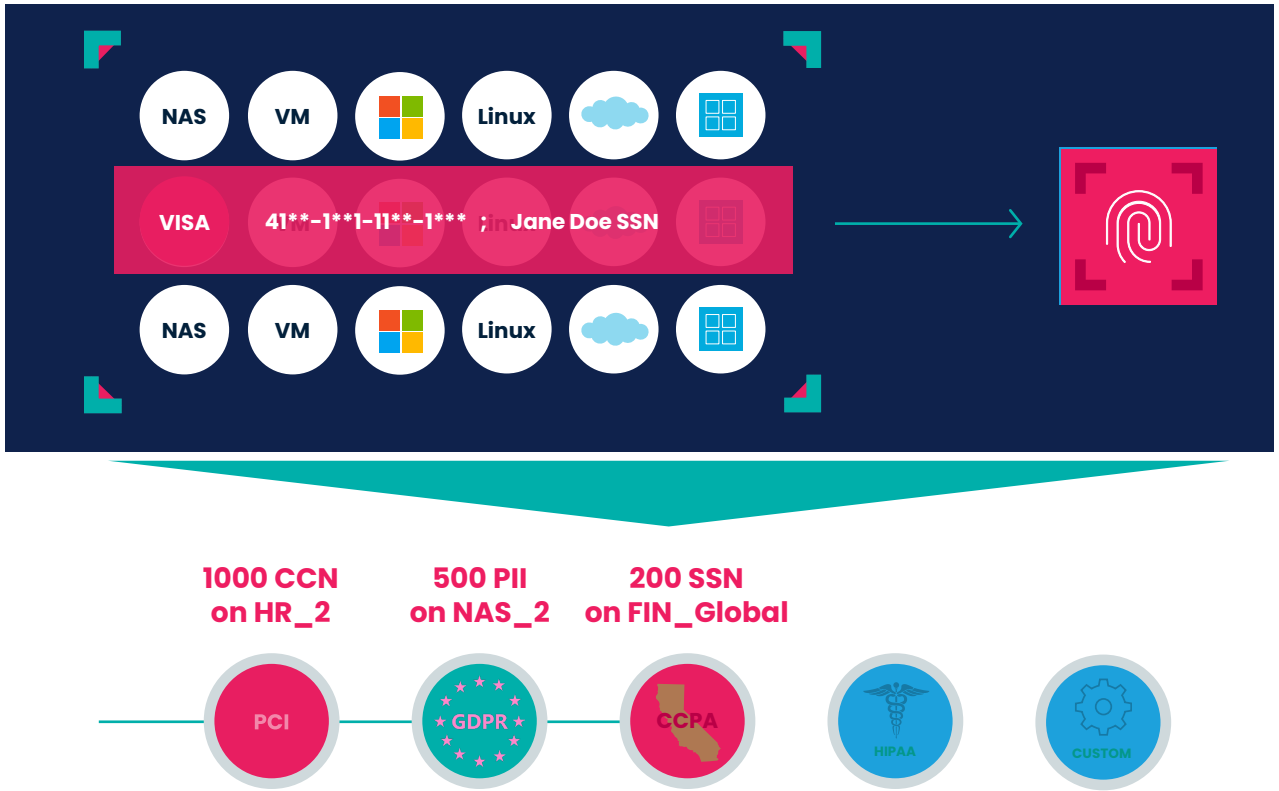


データオブザーバビリティ：機密情報を可視化し、リスクの回避と対応を迅速化

Rubrik Sensitive Data Discovery

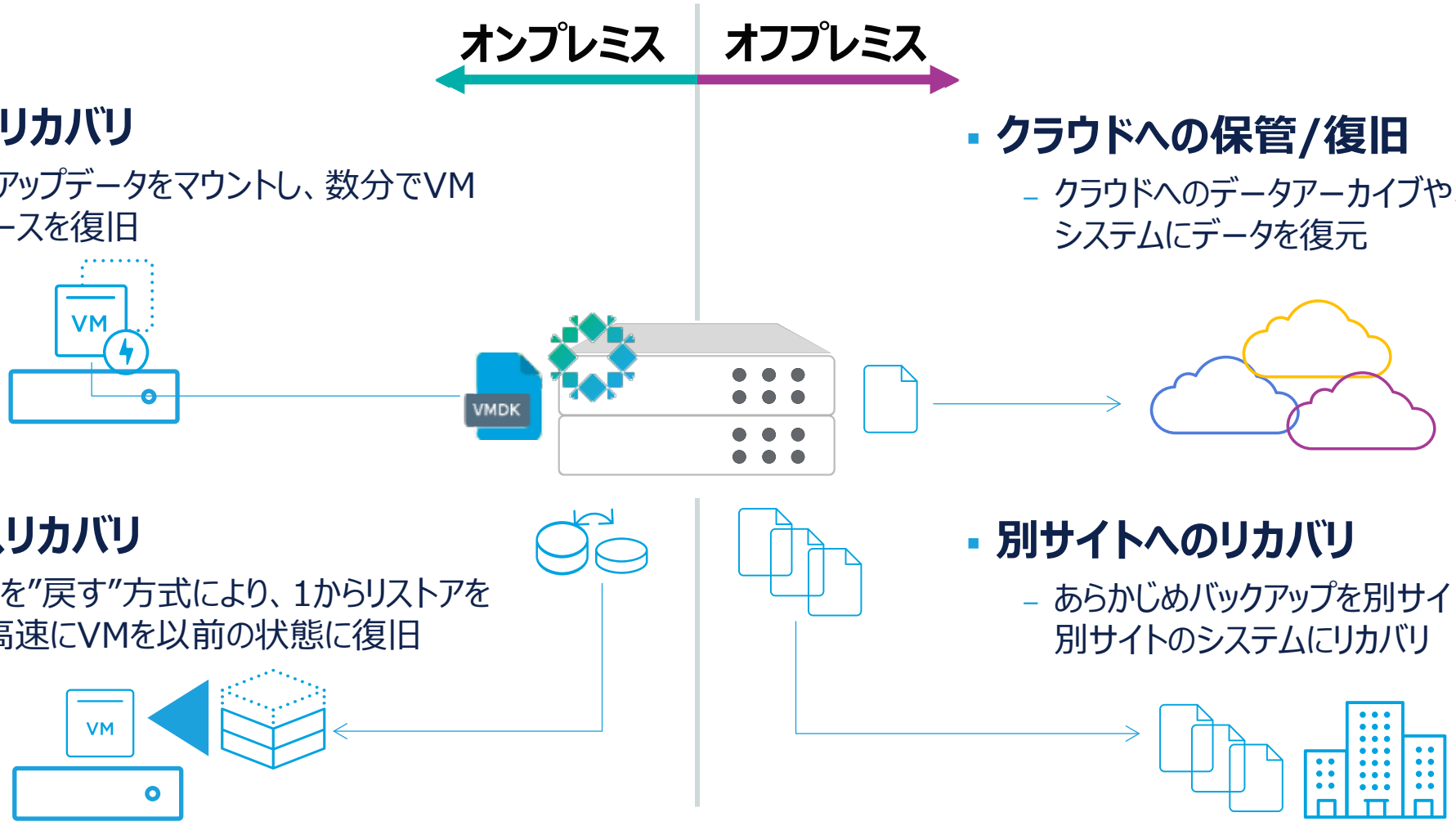
- **データのリスクアセスメントサービス**
  - バックアップデータに対して、ポリシーに基づいて自動的にキーワード検知と分類を実施
  - 機密データへのアクセス状況を可視化
  - 情報保護規制の遵守を促進

- **機密データの可視化を支援**
  - どの機密データか
  - どこに保存されているか
  - どれだけのデータが公開されているか
  - 誰がアクセスできるか



データリカバリ：迅速、かつ柔軟な復旧手段を提供

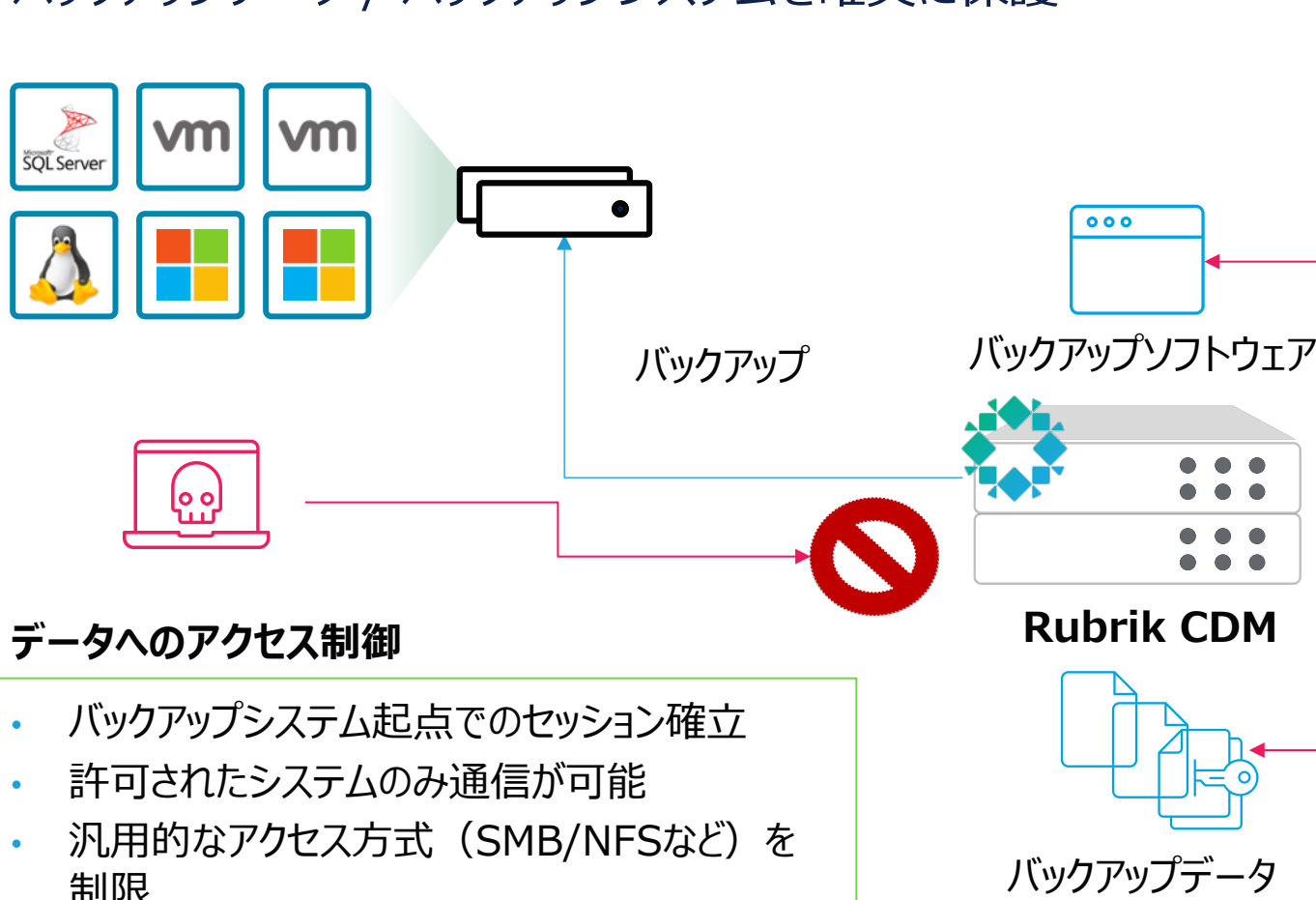
迅速な復旧手法に加えて、別サイトへのリカバリも



- **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
- **クラウドへの保管/復旧**
  - クラウドへのデータアーカイブや、クラウド側のシステムにデータを復元
- **インプレースリカバリ**
  - 差分データを”戻す”方式により、1からリストアをするよりも高速にVMを以前の状態に復旧
- **別サイトへのリカバリ**
  - あらかじめバックアップを別サイトへ複製し、別サイトのシステムにリカバリ

データレジリエンス：Rubrik CDMのデータセキュリティを実現する機能

バックアップデータ / バックアップシステムを確実に保護



なりすましの防止

- ベースOSの管理者権限は利用不可
- 多要素認証によるなりすましの防止
- ファイルの保存期間の変更を禁止

データへのアクセス制御

- バックアップシステム起点でのセッション確立
- 許可されたシステムのみ通信が可能
- 汎用的なアクセス方式（SMB/NFSなど）を制限

データの改ざん防止 / 一貫性

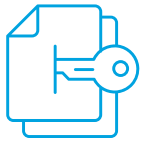
- 独自OSを採用
- Rubrikが許可したソフトウェアのみ実行許可
- データの上書きや削除が不可能なイミュータブルなファイルシステムにより暗号化を防止

データの保存形式

Patch File と Fingerprint

- データは**Patch File**に保存される
  - Rubrikファイルシステム独自の ”追記のみ可能（削除、編集不可）” な Sparse file を作成し、そこにデータを追記（Append-only File）
  - 設定などはなく、ファイルシステム上の標準の仕組みであり、ユーザー自身での属性変更などはできない
- **フィンガープリント**によるデータ一貫性の担保
  - Patch Fileを構成する論理/物理ブロックデータに対して、フィンガープリント（CRC Checksum）が作成される
  - サービスによるデータの読み込み時や、データの変換をコミットする前に、必ず比較/検証が行われる
  - 万が一不一致が検出された場合は、操作はロールバックされる

Patch File（追記のみ可 / 削除・編集不可）

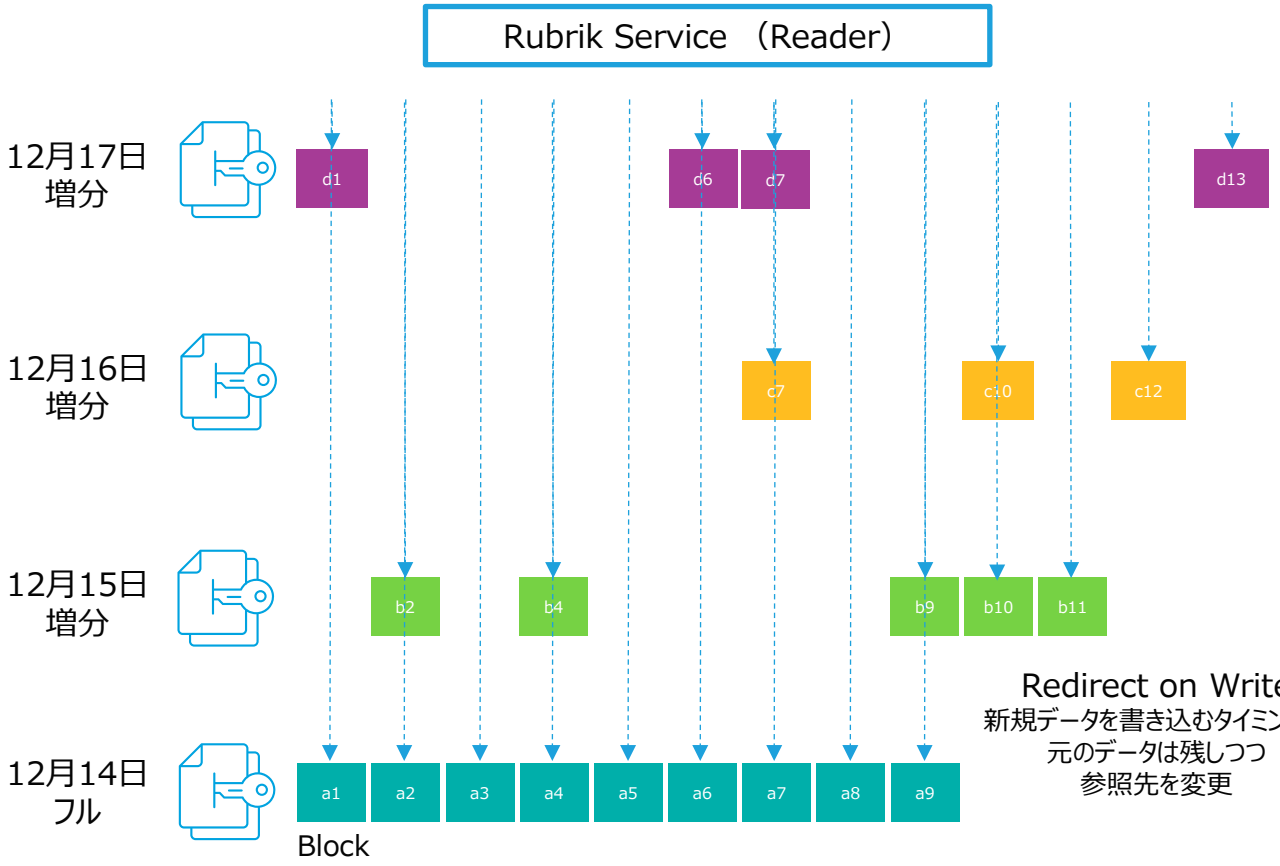


/snapshot/vm-xyz/snap0/full.patch （最初のフル）
/snapshot/vm-xyz/snap1/inc.patch （増分）
⋮

データを更新する場合でも、**全く別の場所に更新後のデータを追記**して、参照先を変更するだけ。**一度書いたデータは上書きしない。**

データ書き込みと同時に作成した**フィンガープリント情報により、書き込まれたデータが変更されたことを検知可能。**
リストアする際のデータが、バックアップ取得時と**同一データであることを担保**

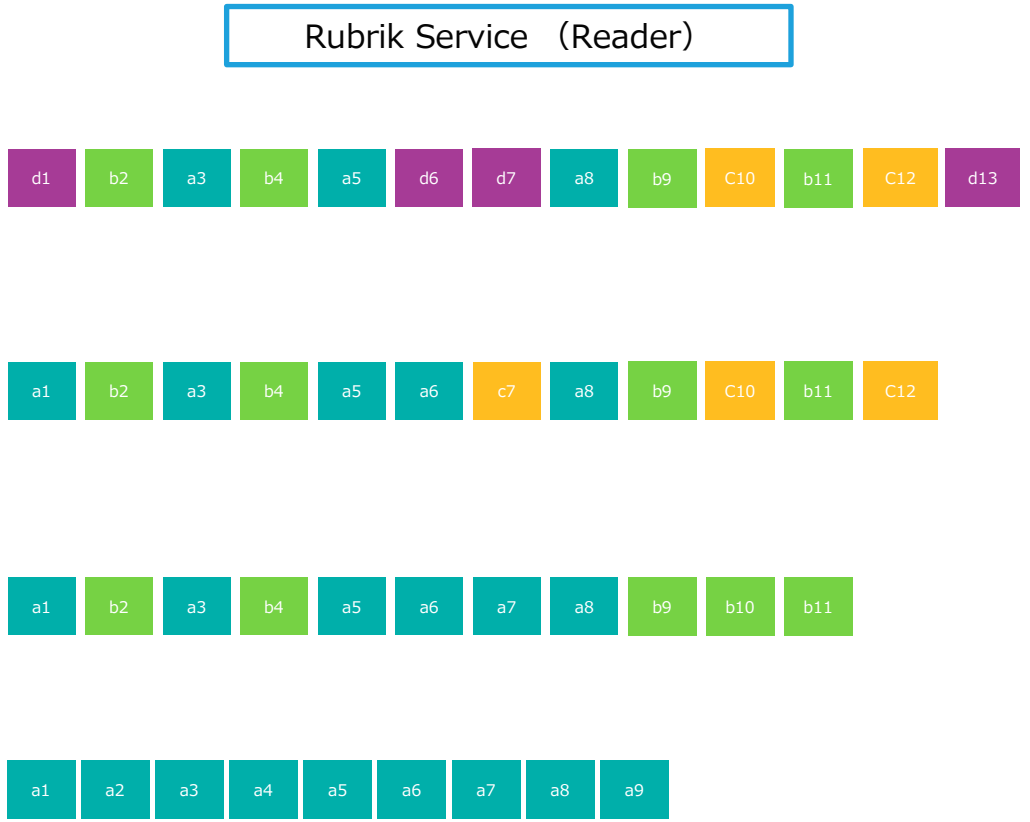
バックアップ（スナップショット）の一連の流れ



独自の”追記のみ可能”（削除、編集不可）な
Sparse file（Patch file）にデータを保存

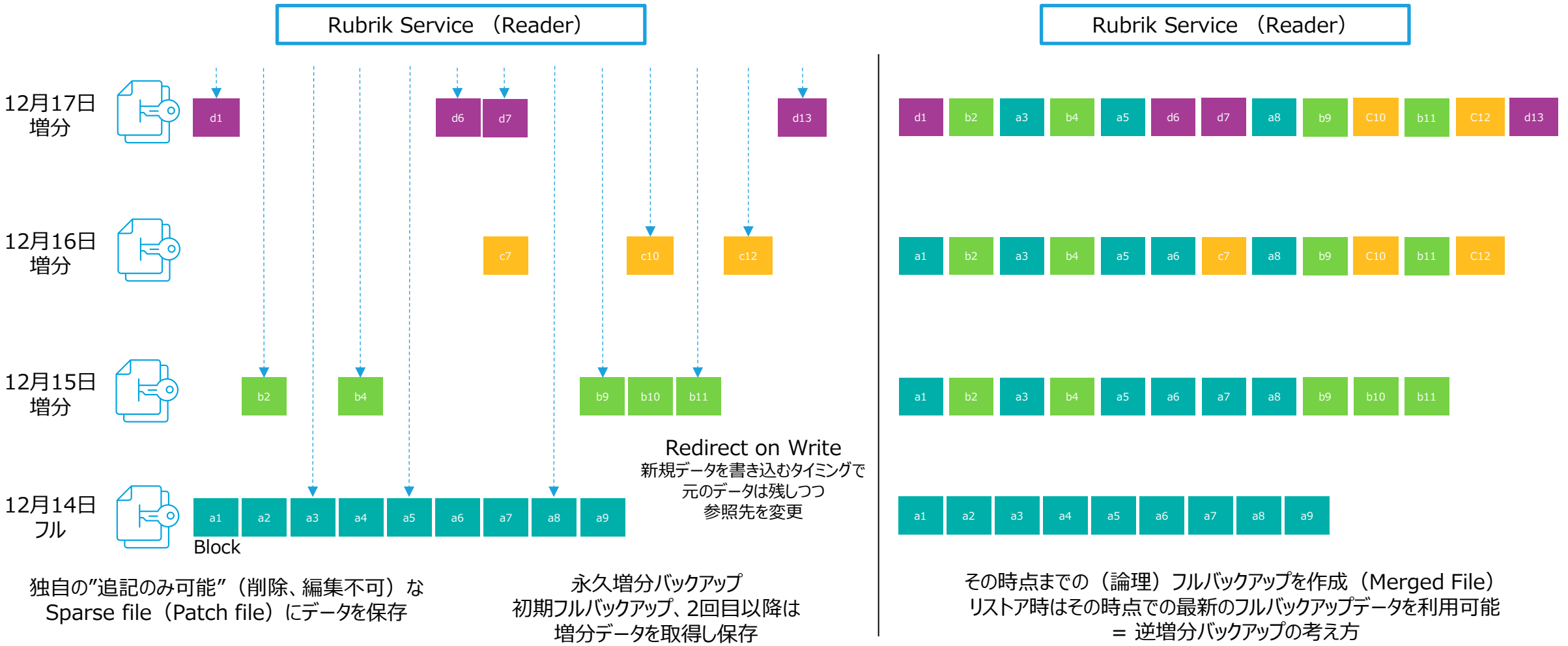
Redirect on Write
新規データを書き込むタイミングで
元のデータは残しつつ
参照先を変更

永久増分バックアップ
初期フルバックアップ、2回目以降は
増分データを取得し保存



その時点までの（論理）フルバックアップを作成（Merged File）
リストア時はその時点での最新のフルバックアップデータを利用可能
＝ 逆増分バックアップの考え方

バックアップ（スナップショット）の一連の流れ



独自の”追記のみ可能”（削除、編集不可）な
Sparse file（Patch file）にデータを保存

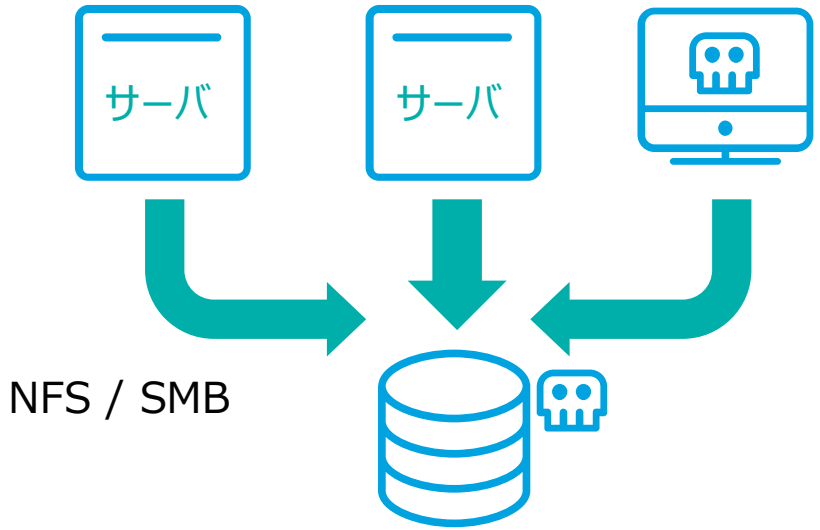
永久増分バックアップ
初期フルバックアップ、2回目以降は
増分データを取得し保存

その時点までの（論理）フルバックアップを作成（Merged File）
リストア時はその時点での最新のフルバックアップデータを利用可能
＝ 逆増分バックアップの考え方

外部からのデータへのアクセスを抑制

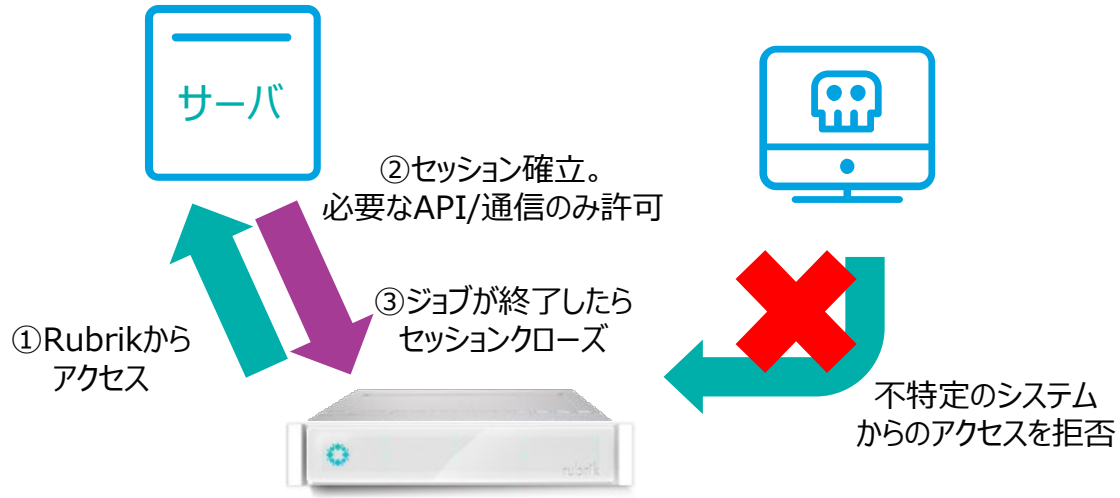
バックアップやリストア時にのみ、一時的にRubrik起点でセッションを確立

▪ 一般的なバックアップストレージ



NFS / SMBといった一般的なファイル共有プロトコルで常にマウントしている状態
外部のシステムから容易にデータにアクセスできてしまう

▪ Rubrik

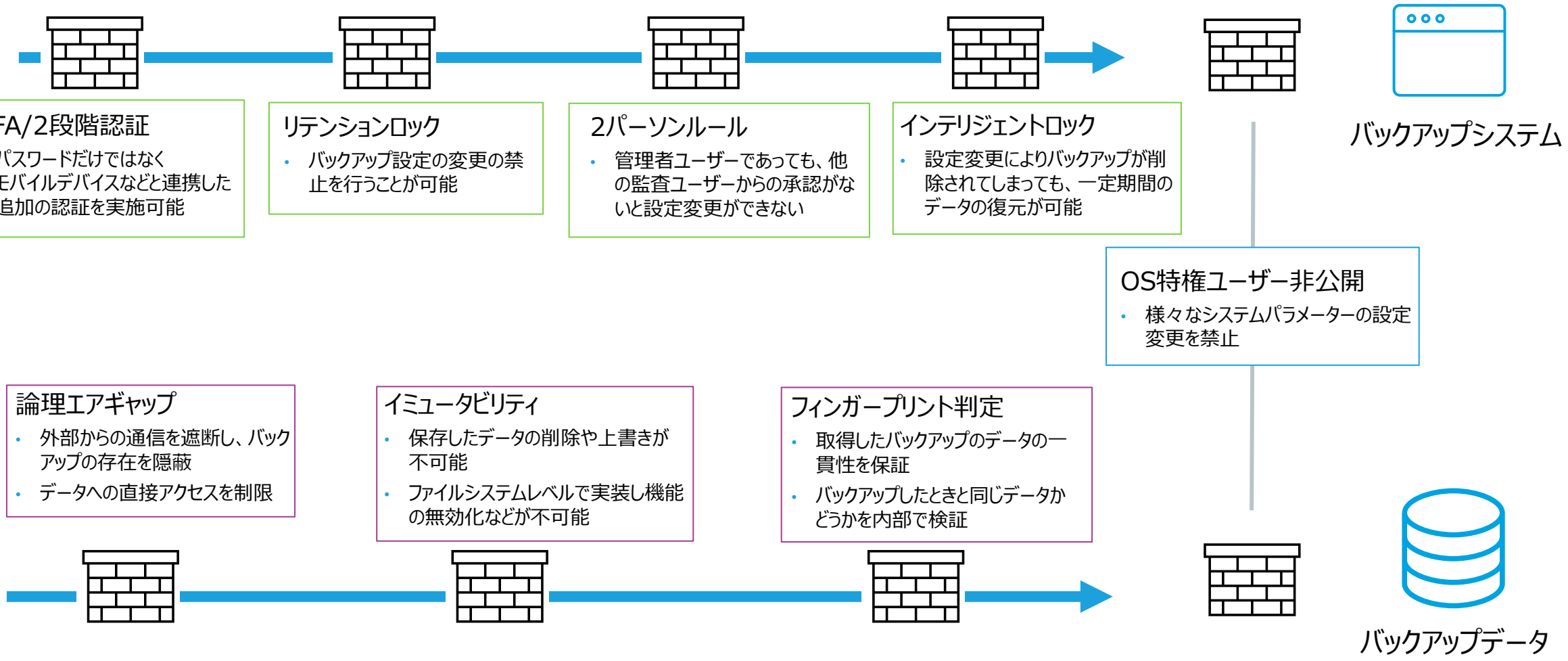


- Rubrikに登録されているシステムに対して、バックアップ取得時にRubrik起点でセッションを開設
- 上記セッション中は対象のシステムからの、認可されたAPIや通信方式でのみ、一時的な書き込みを許可
- 終了後はセッションをクローズ
- 外部のシステムからデータにアクセスできない

主なりすまし防止/設定変更防止機能

- **MFA/TOTP (Time-based one-time password)**
  - モバイルのAuthenticatorと連携し、通常のパスワード以外に、追加のワンタイムキーを入力して認証
- **SSO (Single Sign On)**
  - SAML2.0に対応したIdentity providerと連携し、シングルサインオンでのログインが可能
- **RBAC（Role-based access control）**
  - ロールを規定し、ユーザーに対するアクセス可能な情報や実施可能なタスクの制御を行うことが可能
- **2パーソンルール**
  - 管理者権限を持つアカウントが、システムやバックアップの稼働に影響ある設定を行った場合に、あらかじめ設定されたもう一人のユーザーの認可がないと実施が反映されない
  - 本機能自体の無効化においても発動される
- **リテンションロック**
  - 一度設定したバックアップの設定を、ネガティブな方向には変更できない（削除する、保存日数を少なくする、など）
  - 本機能を有効化するには、２パーソンルールを有効化することが必要
- **インテリジェントロック**
  - 設定変更などによりバックアップデータが削除されてしまった場合、一定の期間の直近のバックアップデータを復元することが可能（サポートエンジニアのみ実施可能）

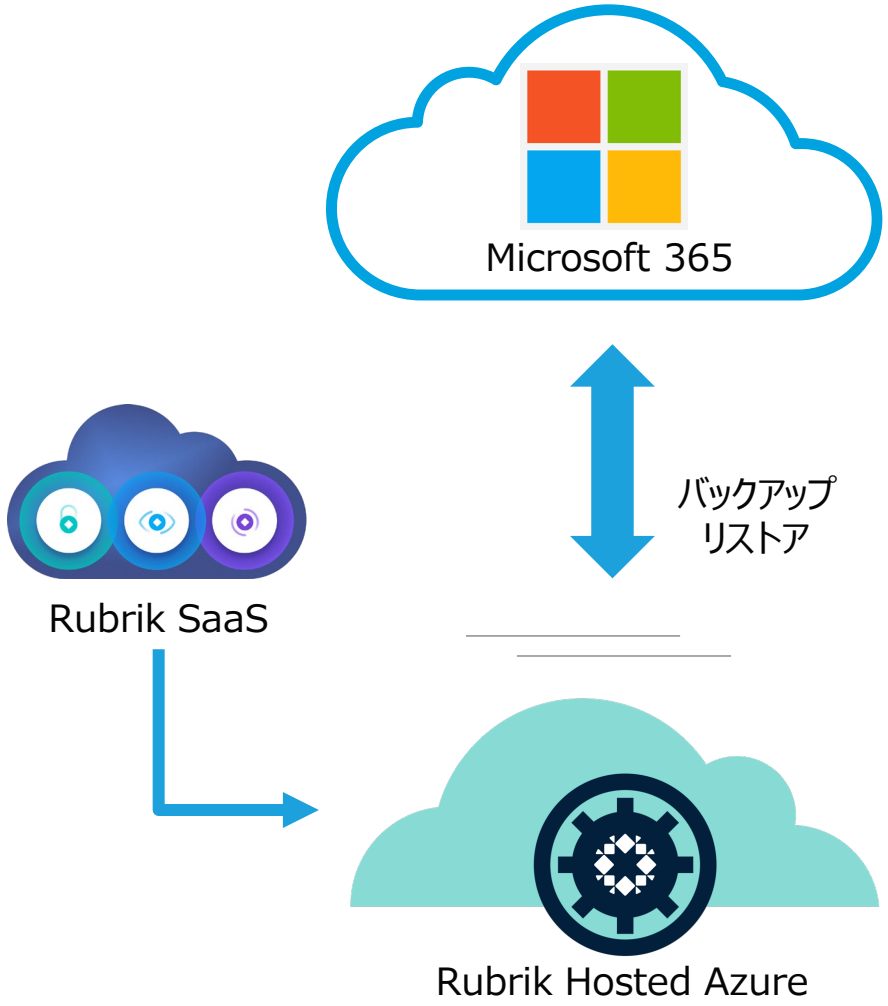
多重の（ゼロトラストな）セキュリティ対策



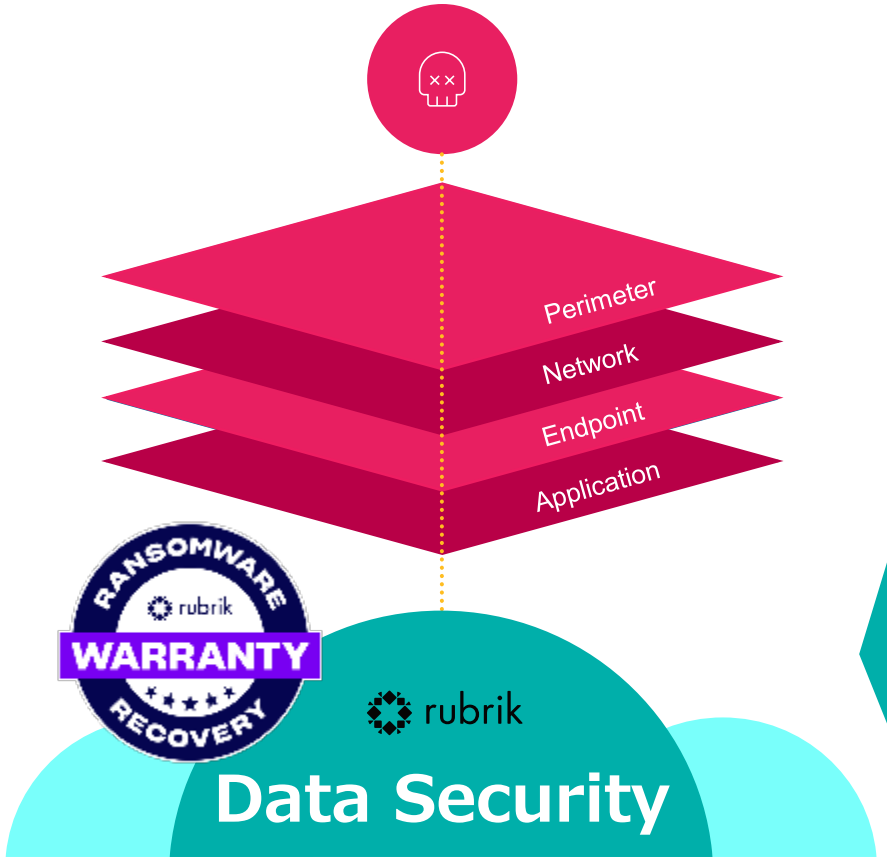
Microsoft 365 データ保護

ビジネスの基盤となるワークプレイス環境の保護と復旧を強化

- **データの長期保護や、復旧機能を提供**
  - Microsoft 365の標準機能では実現できない、コンプライアンスの強化や、迅速な復旧を実現
- **Rubrik SaaSによる設定**
  - わかりやすいインターフェースで、すぐにデータ保護を実施可能
- **Rubrikが運用するAzure環境にデータを保存**
  - お客様にてシステムを構築、運用する必要なし
  - エアギャップされたセキュアな環境でデータを保管



データセキュリティにより、企業に”復旧力”を提供



サイバーアタックから
お客様の早期のサービス/データの
確実、かつ迅速な復旧を支援

データ
レジリエンス

サイバー脅威から
データを守る

データ
オブザーバビリティ

サイバー脅威を
継続的に監視し、
迅速に分析する

データ
リカバリ

数時間以内に
業務を復旧させる

Rubrikの特徴

多様化、標的化する攻撃からバックアップシステムを確実に保護

カテゴリ	Rubrikの実装		他社実装	
イミュータビリティ	○	• ファイルシステムレベルでデータ編集/削除防止機能をあらかじめ組み込み（特許取得済み） • バックアップ設定の変更を禁止することが可能。権限あるユーザーでも本機能の設定を勝手に無効化できない • OSを直接操作可能な特権ユーザーは非公開 • システムクロック（現時刻）だけでなく、モノトニッククロック（経過時刻）を採用し、時間の改ざんからバックアップデータを保護 • 仮にバックアップデータが設定変更により削除されてしまったとしても、一定期間のデータをサルベージすることが可能	△	• イミュータビリティ機能を提供 • バックアップ設定の変更防止機能はあるが、管理者ユーザーで無効化できてしまう • 特権ユーザーが利用可能で、のっとりにより様々な設定変更ができてしまう • 時間の改ざんからの防御はできない • すべての通信が標準で暗号化されていない
エアギャップ技術	○	• 論理エアギャップ技術により、必要な時に、必要なバックアップ対象システムと、必要なプロトコルに限定されたセッションを構築し、外部からのデータアクセスを抑制	×	• NAS機能を有しており、常に外部からデータへのアクセスポイントが存在する
インスタントリカバリ	○	• バックアップデータから直接VMを起動したり、差分だけをリストアするなどの、迅速な復旧機能を提供	○	• バックアップデータから直接VMを起動する、インスタントリカバリが可能
ランサムウェア検出機能	○	• 機械学習によるふるまい検知、および痕跡情報の照合が可能で、データの暗号化前と後の両方での検知機能を提供	△	• 限定されたパラメーターからの検知で、誤検知が多い • マルウェアの検知機能においては、3rd partyのウィルス検知ツールとの連携が必要
自動的なデータリストア	○	• ランサムウェア感染時に想定される大量のリソースのリカバリのために、自動化された一斉リストアが可能	×	• DR（別サイトへ）の自動化のみ。ローカル環境の自動リストアはなし

ランサムウェアからの復旧/対策事例

復旧成功事例

ダーラム市

- 金曜日にネットワーク全体で感染
- 約80台のサーバーがランサムウェアに感染、市のサービスがダウン

- 週末に感染されていないバックアップデータからサーバーを順次リストア
- 月曜日にはサービスを開始

0% **<2日**

ラングス ビルディング サプライ

- メールを経由して感染。数十万のファイルが暗号化
- ビットコインで約15億円相当の身代金要求

- 感染されていないバックアップデータから24時間以内にすべてのサービスを再開

0%
データロス実績

<1日
復旧にかかった実際の日数

事後対策事例

国内企業（感染を契機に対策）

- 本番環境だけでなくバックアップデータも暗号化
- 約３週間業務が停止

- 早期に対策可能なシステムを導入
  - 迅速な復旧のため、誰でも復旧操作可能に
  - クラウドへのリカバリも確保

1/3
リカバリにかかる工数削減目標

<3日
復旧目標

Microsoftとのセキュリティ協業

Azure上でのデータセキュリティとビジネス継続性の実現にフォーカス

- **MicrosoftがRubrikに投資（2022年 8月）**
- **Rubrikが MISA（Microsoft Intelligent Security Association）に参画**
  - MISAは、MS社とセキュリティソフトウェアベンダーやセキュリティサービスプロバイダーとの協業エコシステム
  - 各社ソリューションにMS社のセキュリティテクノロジを活用

日本リージョン対応済み

M365データ保護 as a Service

M365 Rubrik Hosted

M365のバックアップ環境（バックアップ実行、保存）を、Rubrikからサブスクで提供

日本リージョン対応開始!!

アーカイブストレージ as a Service

Rubrik Cloud Vault

アーカイブ用のセキュアなデータ格納先ストレージサービスを、Rubrikからサブスクで提供

Rubrik運用のAzureにて提供

New!!

セキュリティイベント統合管理/分析 Azure Sentinel連携

ランサムウェア検知/分析

RSC

バックアップデータの分析結果の提供

Azure Sentinel

バックアップからの情報も含めて分析/可視化が可能に

分析結果を踏まえた

自動対応

（リストアの実施など）

ふるまい検知の仕組み

保護対象例

- Webサーバー
- DNSサーバー
- プロキシサーバー
- WSUSサーバー
- ファイルサーバ

Ransomware Investigationは2段階チェックを行うことにより、ランサムウェア感染の蓋然性を判定

第1段階チェックに該当したものは Warnings としてアラート
第2段階チェックにも該当したものは Critical としてアラート

第1段階チェック

Polaris上でメタデータを機械学習（ディープラーニング）で解析することにより、**異常な振る舞いを検知**

SaaSサービス

Rubrik Security Cloud

異常検知

第2段階チェック

Rubrikアプライアンス上でバックアップデータの中身を解析し、**暗号化（データのランダム性）の有無を判定**

③対象ファイルコンテンツの解析指示

①データバックアップ

②メタデータをアップロード

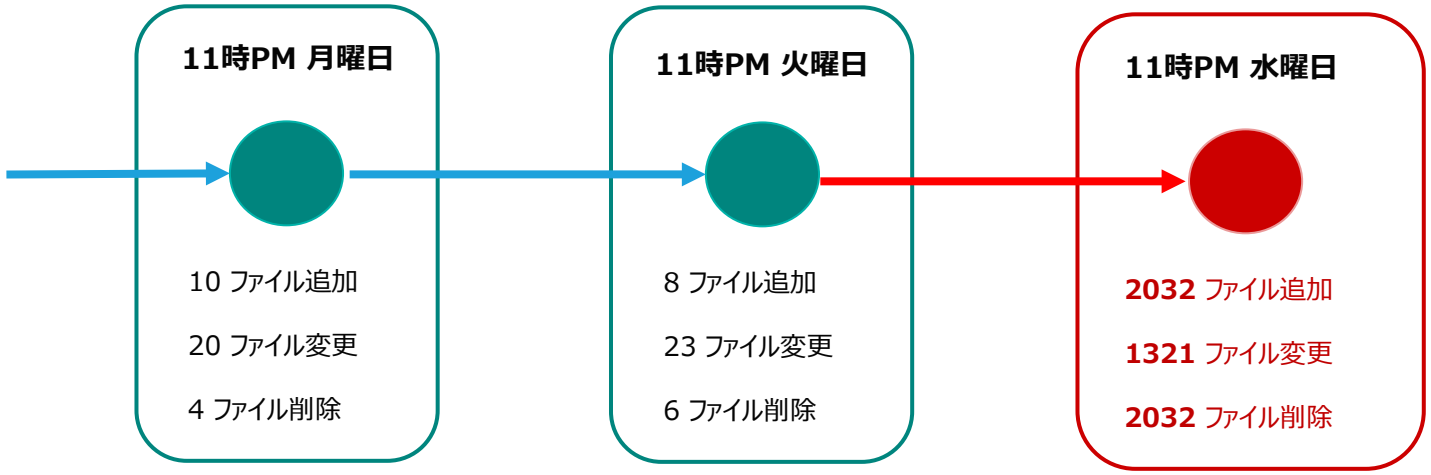
Rubrikアプライアンス

参照元：https://www.rubrik.com/blog/architecture/19/3/rubrik-radar-machine-learning-ransomware

ふるまい検知の仕組み – 第1段階

- バックアップのメタデータを活用した監視・異常検知

1. Rubrikでのバックアップ取得時にファイルシステムのメタデータファイルを習得
2. メタデータファイルをSaaS にアップロード
3. アルゴリズムによって解析
4. **異常がある場合、アラート**



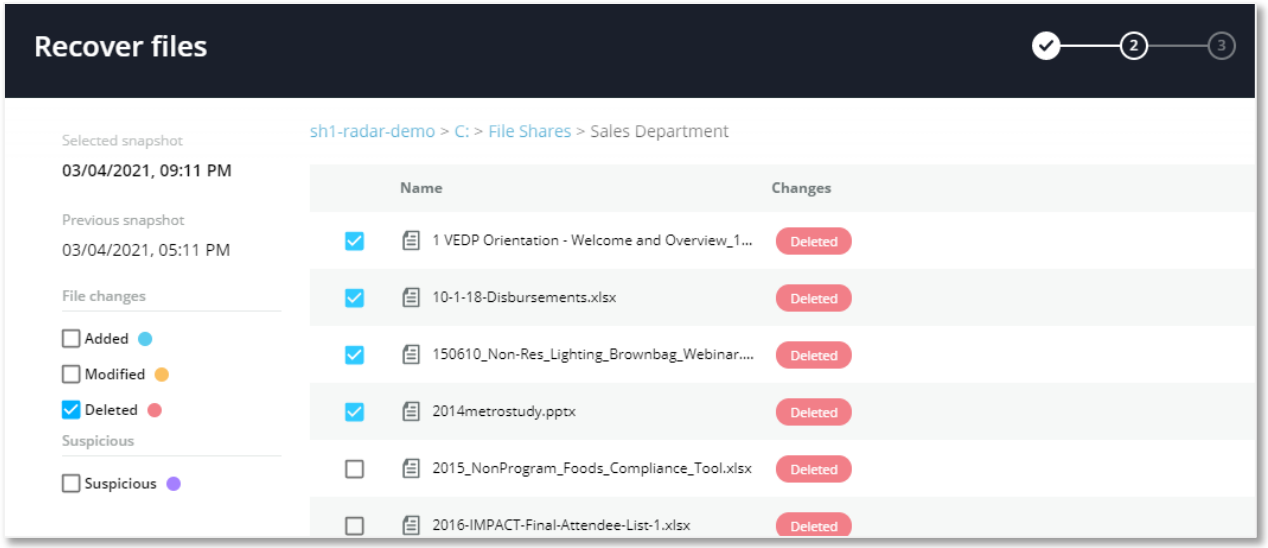
メタデータファイル
・パス
・サイズ
・ACL
・UID
・GID
・属性..etc

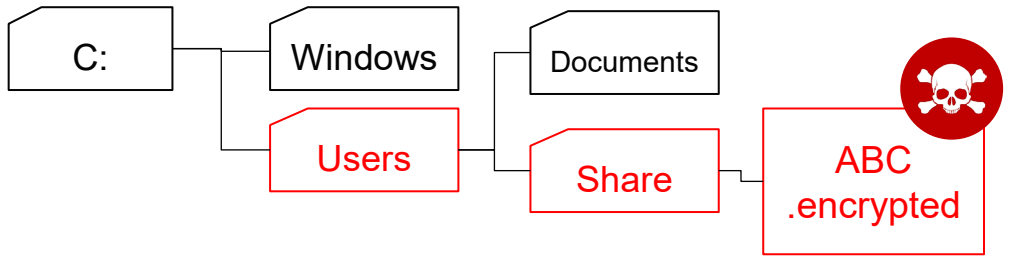
検知の制度を高めるために、
6つ以上のスナップショットがあることが推奨

本番環境に負荷を与えずに監視・検知が可能

ふるまい検知の仕組み – 第2段階

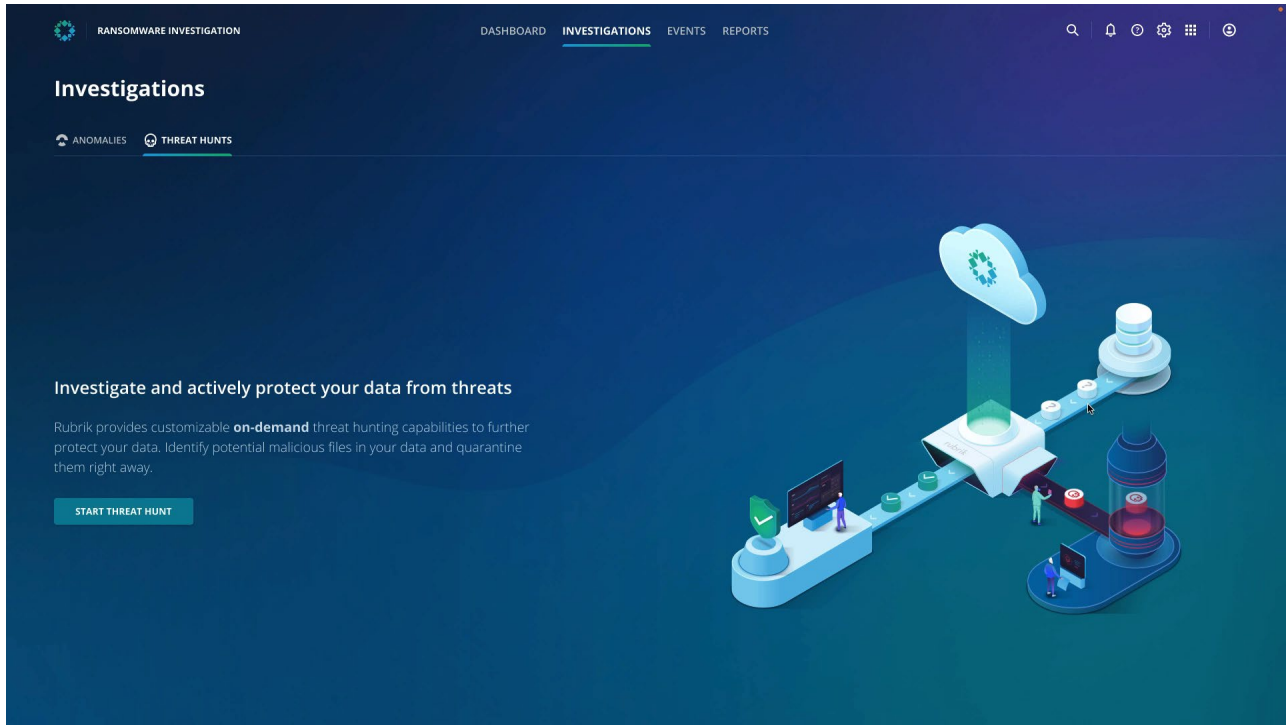
- 実際に暗号化されているファイルの有無を調査
  - SaaSから、被疑対象のバックアップを持つRubrikクラスタに対して調査を指示
  - 暗号化されているファイルを特定
- 迅速にリカバリが可能
  - 過去世代のバックアップから、暗号化前のファイルを特定
  - ファイルレベルでのリカバリを実施





脅威ハンティング：痕跡情報と照合し、ランサムウェアを検知

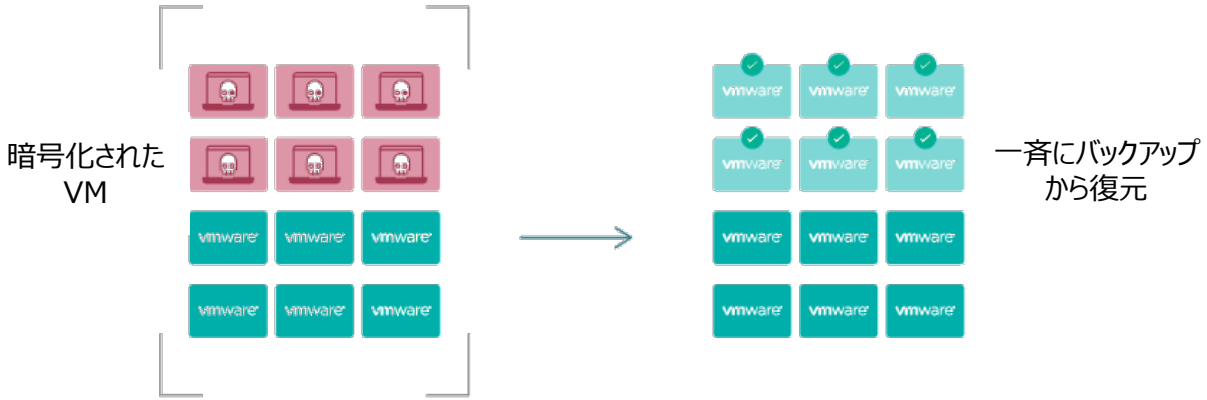
- IOC（攻撃の痕跡情報）と照合しランサムウェア検知
  - 感染開始時期を特定
  - 感染の検知パターンを強化
  - 安全なバックアップデータからのリストアを実現し、2次感染を防止
- 各種ルールを入力可能
  - YARAルール
  - ファイルハッシュ　など

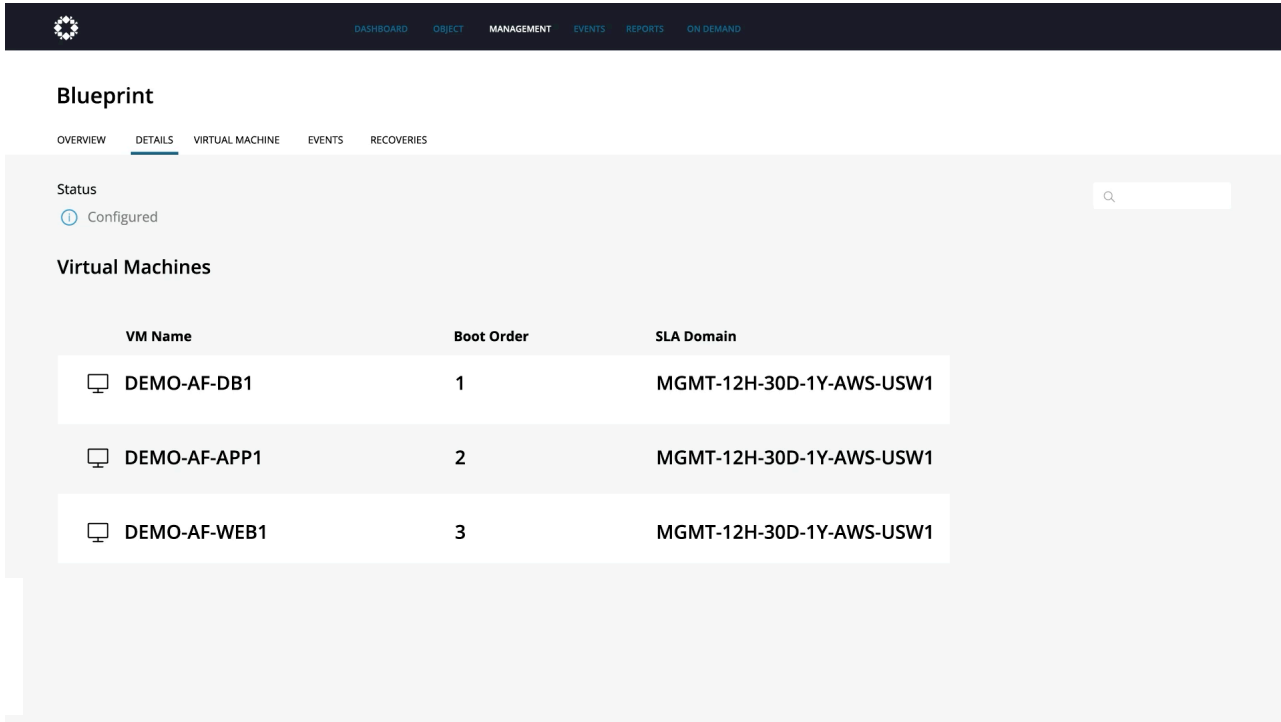


復旧プロセスを自動化し、ミスなく多くのリソースを迅速に復旧

復旧プロセスをあらかじめ定義した手順に従い自動化

- “Blueprint”に基づき、リストアの操作を自動化
- DR目的の別サイトへの復旧操作を自動化
- ローカルサイト内の同じシステムへの一斉復旧を自動化
  - VMを一斉に、ランサムウェアに感染していない時点まで、インプレースリカバリで ”巻き戻し”復旧

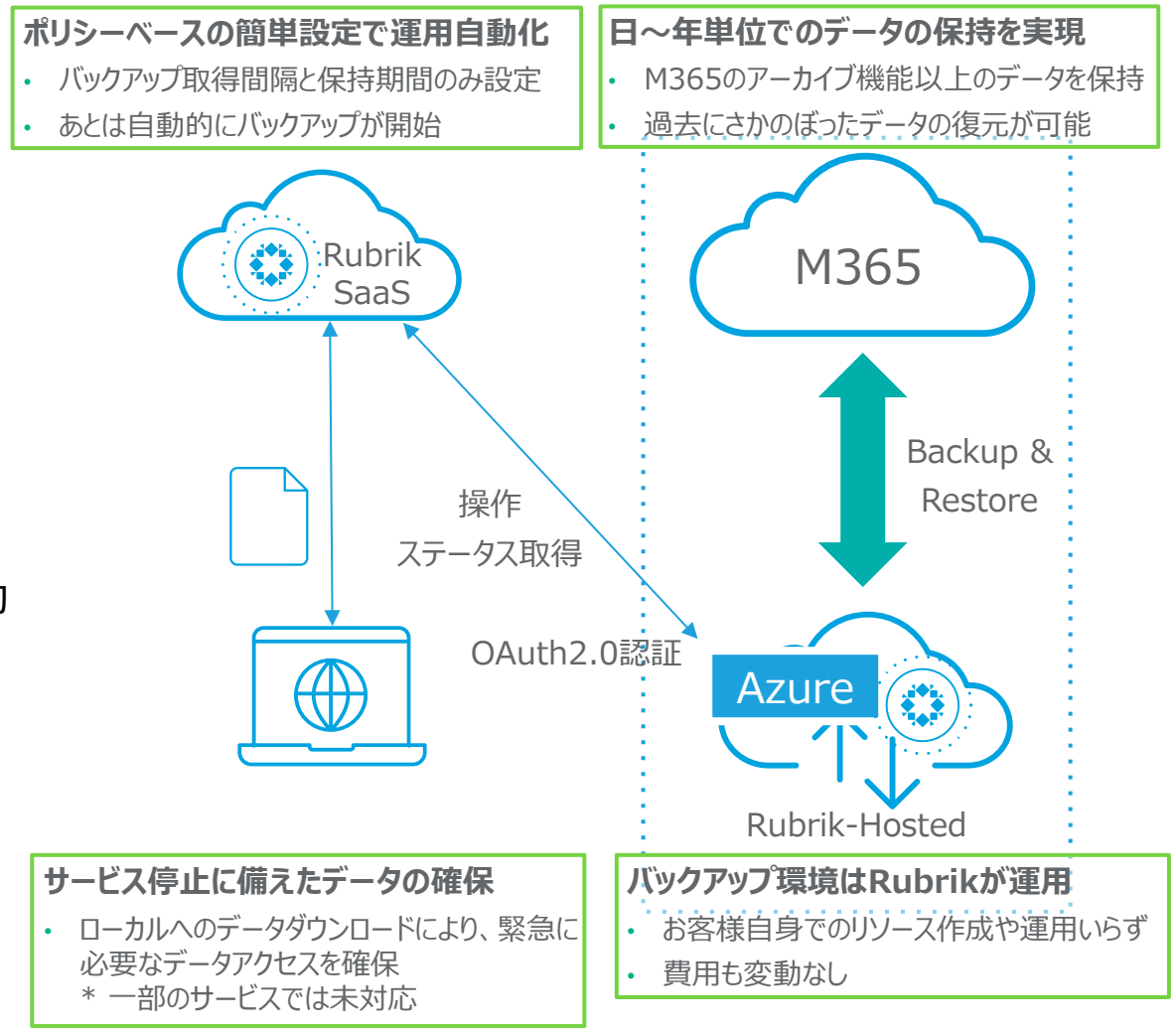




ソリューションの特徴

手離れの良いセキュアなソリューション：すぐに開始可能 ＋ ポリシーベースのバックアップ自動運用

- **ITリソースを用意することなく、すぐに開始可能**
  - 必要なのは**お客様のM365サブスクリプションのみ**
  - 以下はRubrikから提供
    - コントロールプレーン：**SaaSで提供** (Rubrik Security Cloud)
    - バックアップ処理/データストア：**Azure環境を"マネージド"で提供**
- **予測可能なコスト**
  - ユーザー数とユーザーごとに必要な容量ベースの**サブスクリプション**
  - **Azureの費用も込み**。ストレージ容量やインスタンスリソースは自動でスケール。それでも**費用の増減はなし**
- **セキュリティも考慮**
  - コントロールプレーンから直接**M365内のデータにはアクセスしない**
  - クラウド環境に閉じた処理で、**外部にデータは流さない**
  - バックアップデータは**イミュータブルな環境に保存**



これからのバックアップに求められる要件

ランサムウェアからの復旧を確実にするために

“復旧”での課題

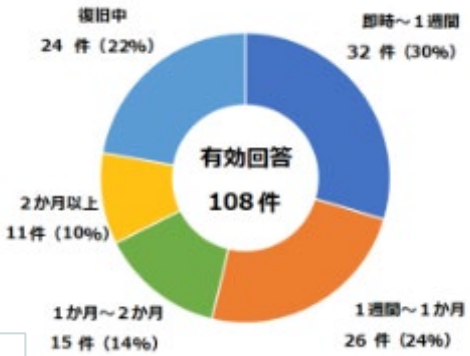
- **狙われるバックアップ**
  - 復旧の退路を断つために、ハッカーはバックアップを標的に

バックアップシステムの乗っ取り
- 管理者権限の奪取によるソフトウェア削除
- バックアップ設定の変更とデータの削除

バックアップデータの改ざん
- 外部からバックアップデータへのアクセスと削除、暗号化

- **時間がかかる復旧**
  - バックアップがあっても
    - 影響範囲を把握するのに時間がかかる
    - 安全なデータを判断するのに時間がかかる
    - 大量のリソースをリストアするのに時間がかかる
  - 時間がかかれば損害も増大する

被害にあった企業の70%以上は、復旧に1週間以上、半分近くは1か月以上かかっている



警察庁：被害からの復旧に要した期間

Gartnerが提唱する ランサムウェア対策に求められるバックアップ

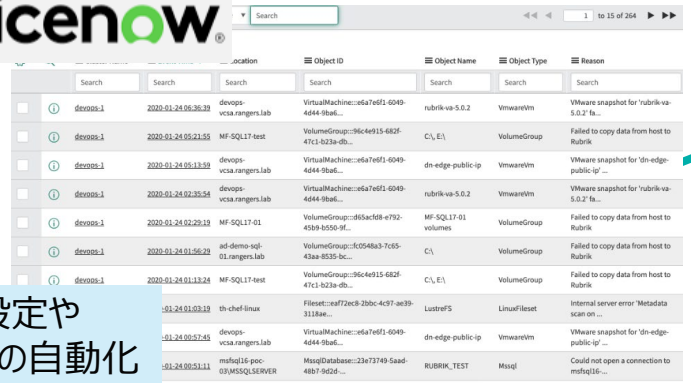
Gartner：how to recover from a ransomware attack using modern backup

1. **イミュータビリティ**
   - バックアップデータの削除や改ざんを防止
2. **エアギャップ技術**
   - バックアップデータへの直接アクセスを防止
3. **インスタントリカバリ機能**
   - 高速なデータリストア技術による迅速な復旧の実現
4. **ランサムウェア検出機能**
   - バックアップデータ内のランサムウェアの検出
5. **自動的なデータリストア**
   - 一斉、かつ自動化されたデータのリストア機能

外部連携

IT運用の自動化や、SIEM/SOARソリューションとの連携

servicenow



バックアップ設定や
リストア作業の自動化

Microsoft

Azure Sentinel

アラート/イベントの統合管理と
対応の自動化

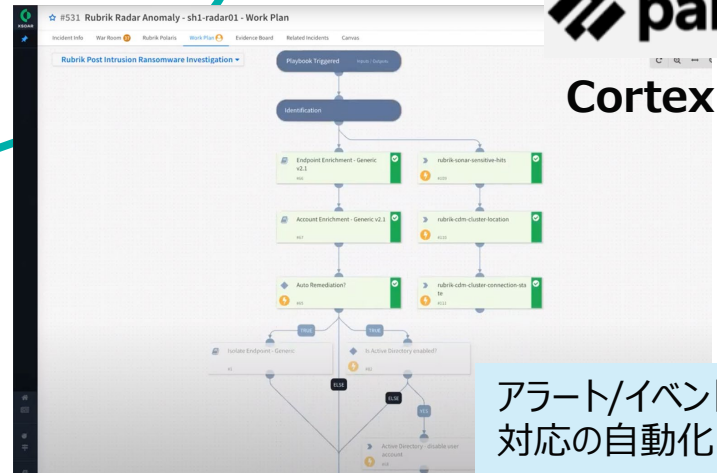
Rubrik

splunk>

アラート/イベントの統合管理

paloalto NETWORKS

Cortex XSOAR



アラート/イベントの統合管理と
対応の自動化

お問い合わせ先

パナソニック デジタル株式会社

https://service.digital.panasonic.co.jp/contact

※本資料に記載された社名および商品名などは、それぞれ各社の商標または登録商標です。