Arcserveで行うランサムウェア対策

2022年　Arcserve Japan

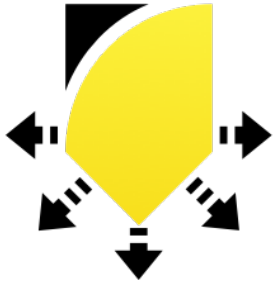
arcserve®

コンテンツ

- 1．ランサムウェアに備えたバックアップ環境構築
- 2．サイバー攻撃に先回り！Arcserve UDP のご紹介

arcserve®

1. ランサムウェアに備えたバックアップ環境構築



サイバー攻撃に先回りする対策は２つ

Ⅰ

セキュリティによる対策

＝不正な侵入やウィルス感染を防ぐための予防

Ⅱ

バックアップによる対策

＝実際のデータ破壊や改ざんに対する備え

arcserve®

I セキュリティによる対策 = 侵入させないための予防策

- ✓ 適切なファイアウォール設定による不正アクセスの遮断
- ✓ 検知率の高いセキュリティソフトを導入し、定義ファイルを常に最新の状態に保つ
- ✓ OSとソフトウェアを常に最新の状態に保つ
- ✓ メールやSNSのファイルやURLに注意（ユーザ教育）

これでも侵入や感染を 100% 防御できない

arcserve®

Ⅱ バックアップによる対策 ＝ データ破壊や改ざんに対する備え

破壊、改ざんされたファイルを

健全だった時点のバックアップから確実に復元(リストア)

できるように準備

バックアップすべき環境：

物理/仮想/クラウド、Windows/Linux、

ファイル、アプリケーション、メール などのサーバ　　クライアントＰＣ

arcserve®

攻撃に耐えるためのバックアップ体制を構築

健全な時点のバックアップデータを残すための体制が必要

複数世代を保持

バックアップデータ自体を破壊されないような体制が必要

バックアップ先は安全な場所に

オフラインで保管

arcserve®

複数世代を保持

より多くの世代のバックアップを保持することで健全なデータが残存する可能性を向上

日次で3世代を保持

3日前に感染していた場合、
全ての世代が感染

月次、週次、日次で多世代を保持

保持世代が多ければ
感染前の世代が残存する可能性 **大**

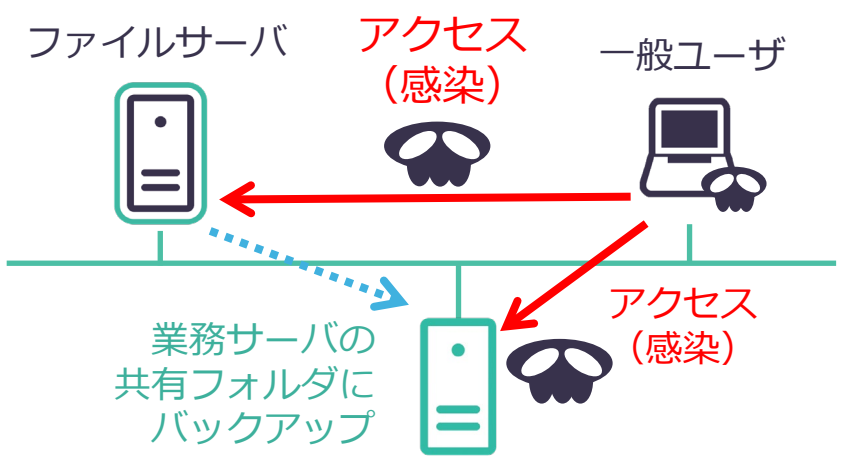
世代： バックアップ実施時点毎のバックアップ データ

arcserve®

バックアップ先は安全な場所に

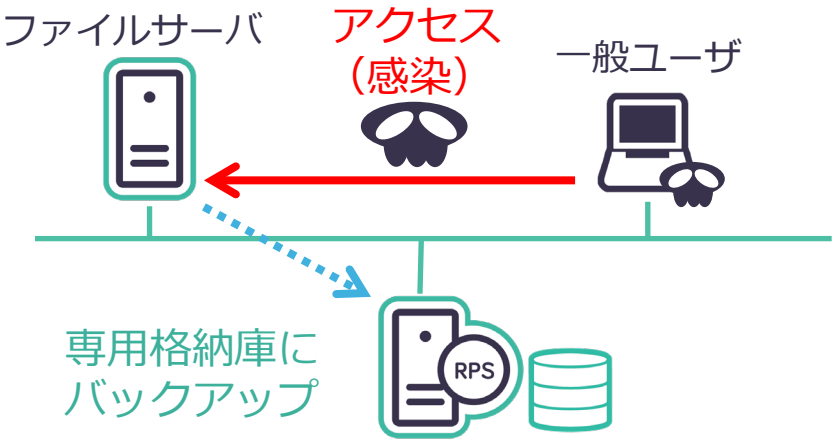
バックアップ データへのユーザ アクセスを無くし感染の確率を低減

バックアップ データを業務サーバに格納



ユーザがアクセスする場所にある
バックアップデータは感染しやすい

バックアップ データと業務データの格納場所を区分



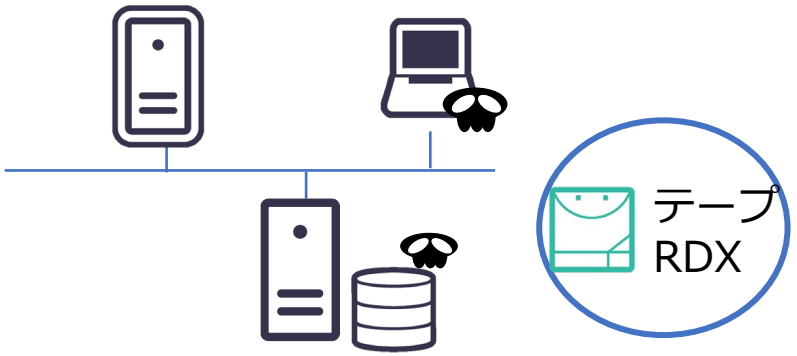
ユーザ アクセスを制限し、
バックアップデータの感染リスクを低減

arcserve®

オフラインで保管

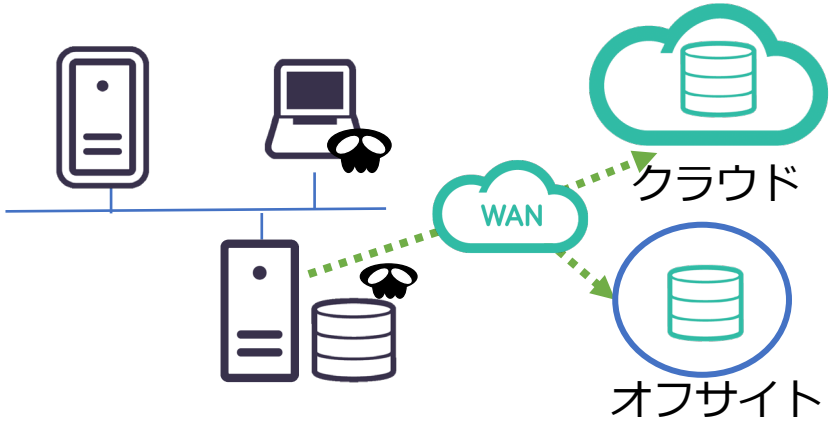
ネットワーク経由で感染するリスクを低減

取外し可能な媒体に保管



テープやRDXなどにバックアップし、
メディアを取出しオフラインで保管

オフサイト・クラウドに保管



バックアップしたデータの複製を、
遠隔地やクラウドで保管

arcserve®

復旧(業務再開)手段の決定

a. 比較的範囲の狭い被害

→ **感染したファイル/フォルダをリストア**

b. 広範囲なファイルの被害、OSやミドルウェア レベルの被害、被害範囲不明の場合

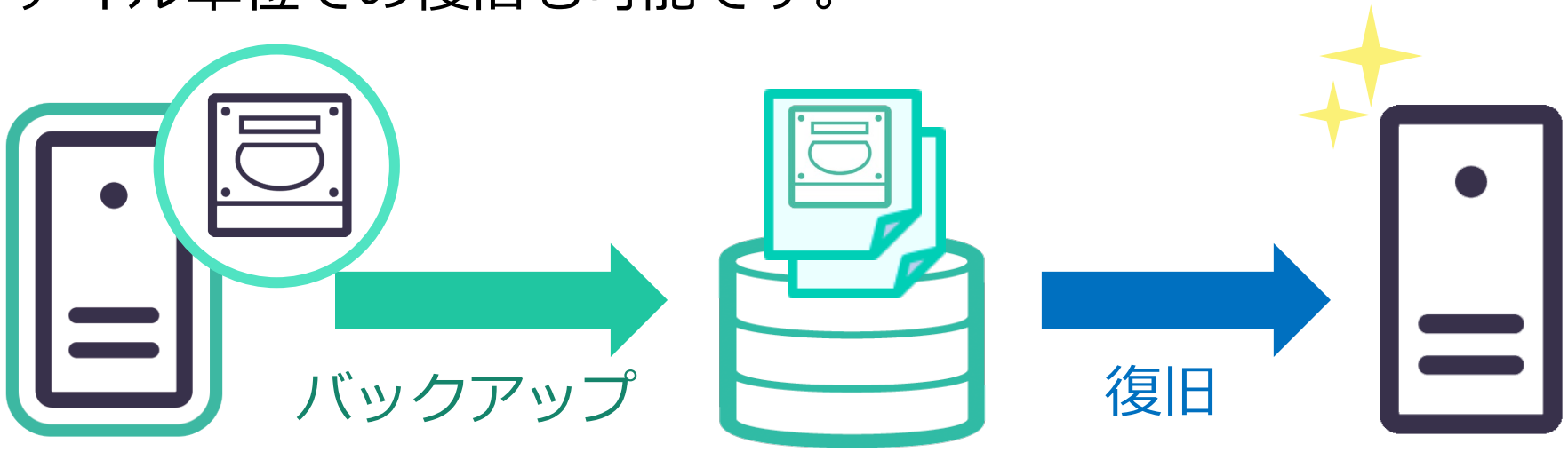
→ **サーバ、システム全体の復旧**

2. サイバー攻撃に先回り！Arcserve UDP のご紹介

簡単イメージバックアップ Arcserve UDP

イメージバックアップとは

ファイル単位ではなく、ディスク全体を丸ごと高速にバックアップします。
OSやデータを含むシステム全体をまとめて簡単に復旧できます。
個別のファイル単位での復旧も可能です。



Arcserve UDPは異なる機種への復旧やP2Vも標準サポート！

（物理から仮想への復旧）

arcserve®

初回フル以降は増分のみの運用で、らくらく世代管理

高速 バックアップ

初回のみフル バックアップ、
以降は時間の短い**永久増分**バックアップ

ディスク 使用量を削減

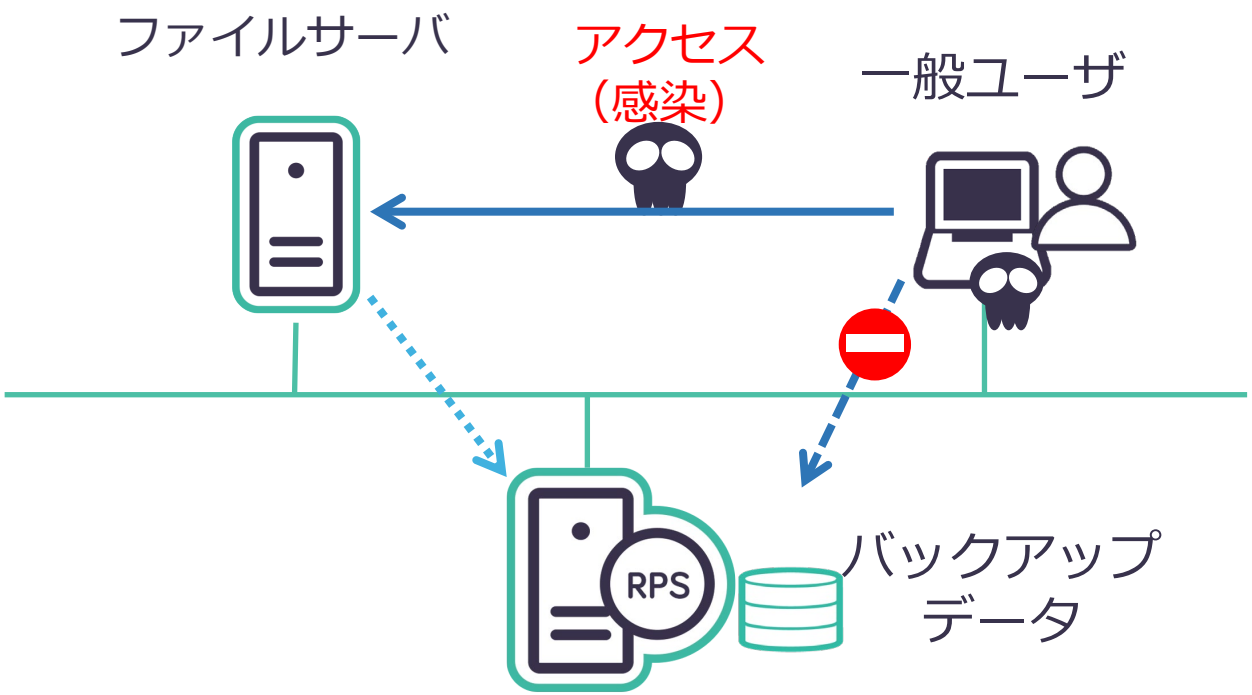
増分運用と自動的なマージ処理が
バックアップ データの**肥大化を抑制**

バックアップデータを3世代保存する場合

※初期設定では7世代を保存(最大1440世代まで設定可)

arcserve®

復旧ポイントサーバ（RPS）の導入で、
ユーザ アクセスによるバックアップ データへの感染を防止



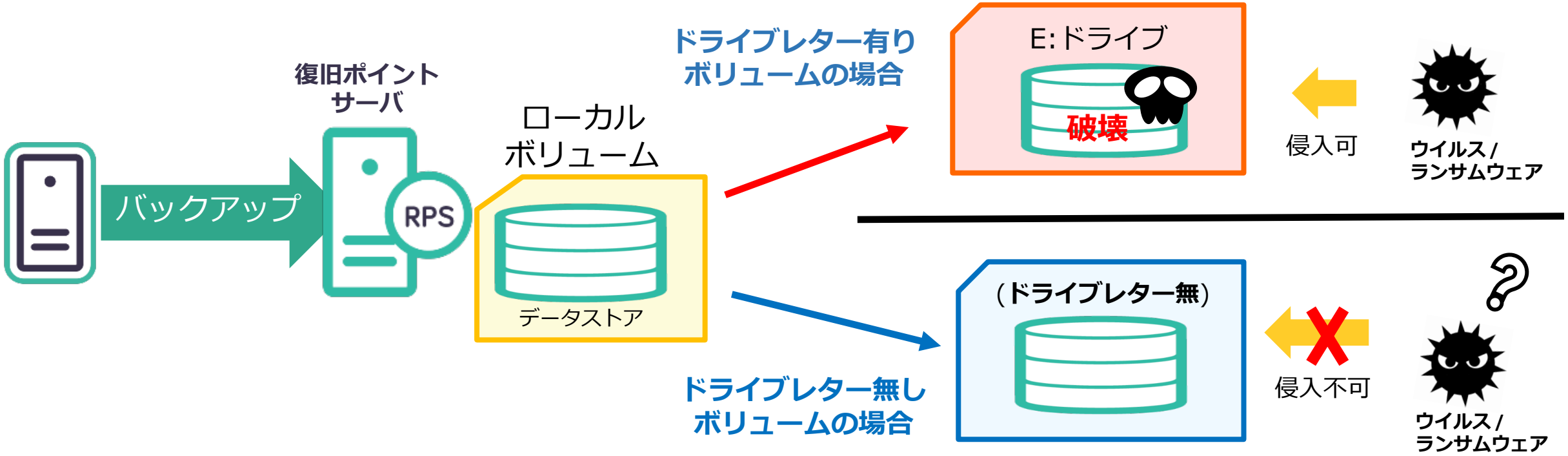
一般ユーザはアクセスできない専用の格納庫にバックアップ

arcserve®

復旧ポイントサーバのセキュリティ強化

Arcserve UDP 8.0

復旧ポイントサーバ（RPS）内の
エクスプローラーから見えない領域にバックアップデータを保管



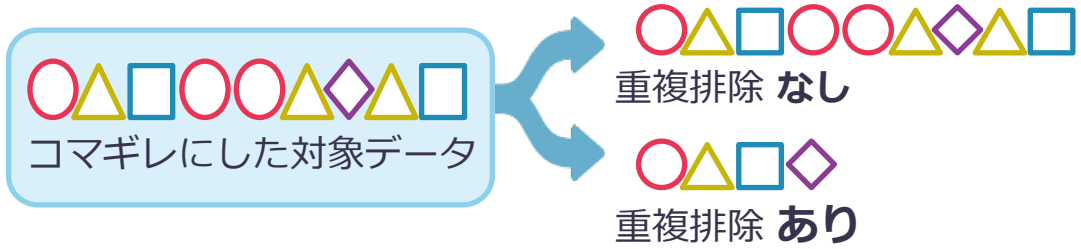
RPS 内に侵入したウイルスやランサムウェアからバックアップデータを保護

arcserve®

復旧ポイント サーバ (Recovery Point Server：RPS)

重複排除や遠隔転送を担うバックアップ データの格納庫

重複排除　データ細分化、同一ブロック排除



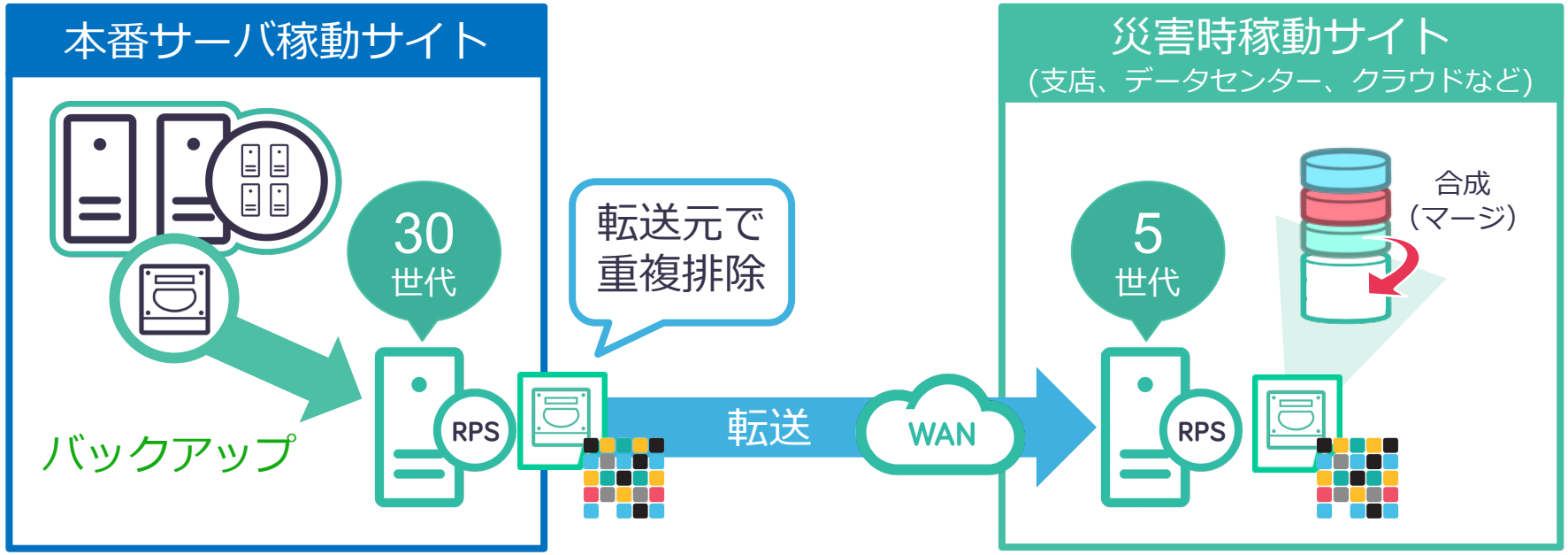
遠隔転送　RPS間でバックアップ データを転送

arcserve®

バックアップ データをオフサイト保管

◆ 災害対策として遠隔地にバックアップ データを転送

◆ クラウドや遠隔地に保管することで感染リスクを**更に低減**



重複排除で回線
使用量を更に削減

特定の曜日・時間を
指定して転送できる

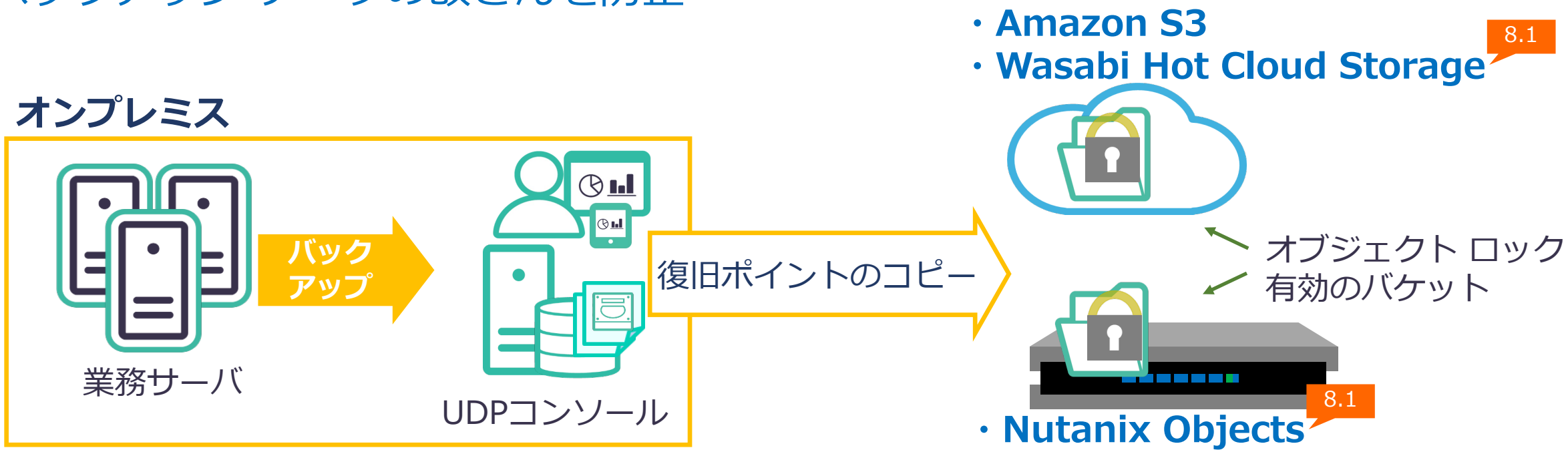
転送先での世代数を
個別に設定できる

arcserve®

オブジェクト ロック対応ストレージの利用

8.0

復旧ポイントのコピー機能が不変ストレージ（オブジェクト ロック機能）に対応
バックアップ データの改ざんを防止



法規制やコンプライアンス
などのデータ保持に利用

ストレージ側の設定で
保持期間後の削除も可能

フルイメージを戻して
システム復旧の利用が可

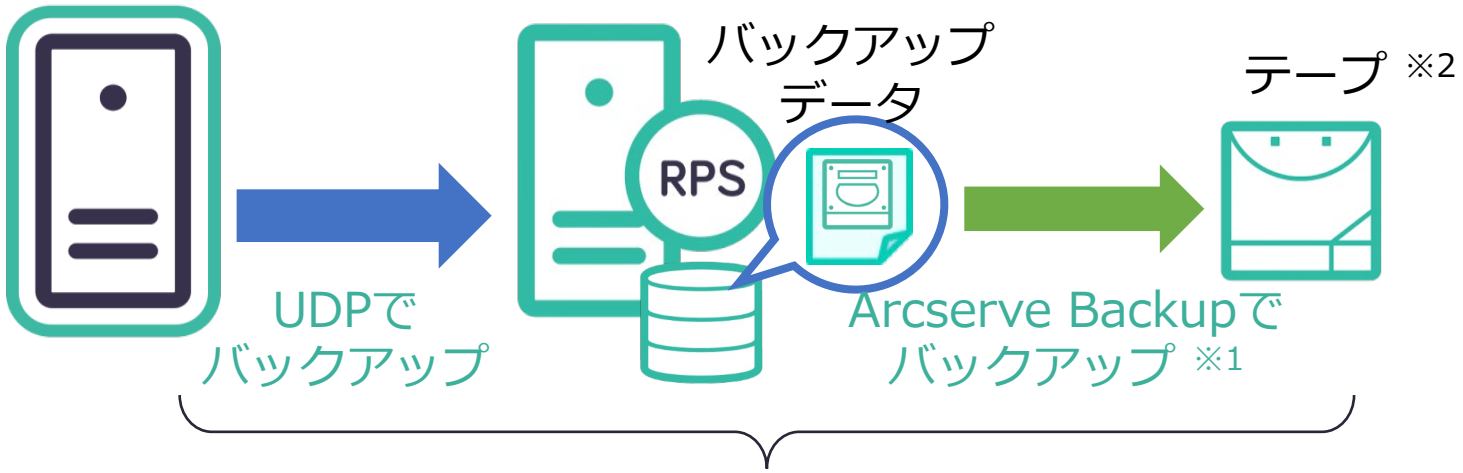
arcserve®

テープへオフライン保管

◆バックアップ データを**オフライン** & 長期保管

◆バックアップ データを、一連のバックアップ処理の中でテープにも保管

◆テープ装置/メディアの WORM (Write Once, Read Many) 機能にも対応



管理コンソールで一括設定・管理

※1 この用途でのArcserve Backup ライセンスは**無償提供**
※2 ドライブ１つのテープ装置に標準対応

arcserve®

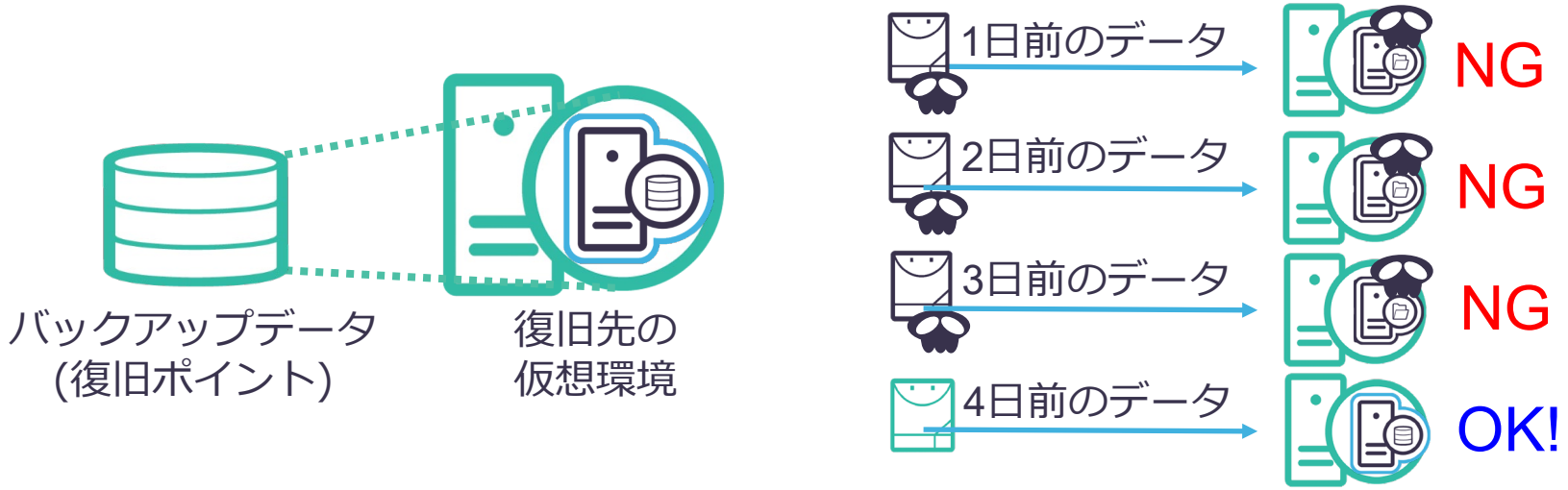
わずかな時間でサーバを起動し、感染状況を確認

- ◆ コストを抑えた早期の業務再開が可能
- ◆ どの時点までが**未感染だったかを確認する環境**を提供

インスタント VM (IVM)

簡単なウィザードの実行だけで、バックアップ データを直接参照するVMを数分で起動

仮想マシン上で感染有無を確認可能



arcserve®

Arcserve UDP 管理のセキュリティ強化 8.1

管理画面へのログオン方法として多要素認証（MFA）が利用可能に

パスワード入力に加えて、確認コードの受信/入力を必要とすることで
不正アクセス リスクを低減

arcserve

お問い合わせはこちらから

Arcserve ポータルサイト： **arcserve.com/jp**
カタログセンター （カタログ、技術資料）

https://www.arcserve.com/jp/jp-resources/catalog-center/

Arcserve カタログセンター　検索

Arcserve ジャパン ダイレクト （購入前のお問い合わせ）

例： 「この構成で必要なライセンスを教えてください」、
「Arcserve UDP はXXXに対応していますか？」、
「XXXはサポートされますか？」

フリーダイヤル： 0120-410-116
（平日 9：00～17：30　※土曜・日曜・祝日・弊社定休日を除きます）

Webフォーム：https://www.arcserve.com/jp/about/contact/call-me/

arcserve®

arcserve®