ランサムウェアに備える
バックアップ運用例とベストプラクティス

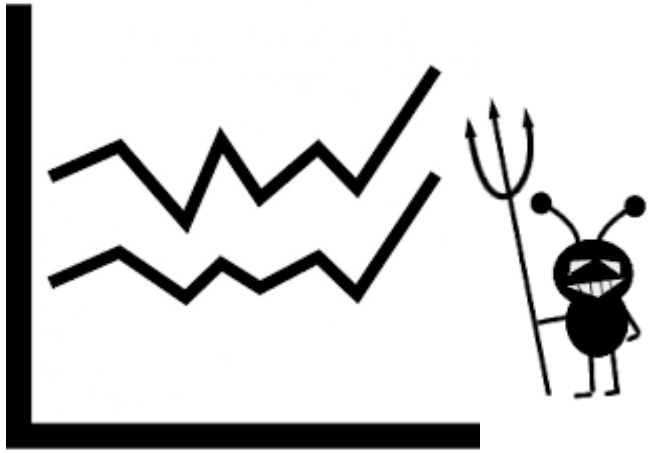
2022年 Arcserve Japan

arcserve®

Rev 1.1

※本資料はランサムウェアによる被害リスクを低減する資料であり、感染被害を完全に防ぐことをお約束するものではありません。

ランサムウェアにご注意を！！



WARNING

身代金要求型不正プログラム

『ランサムウェア』

感染報告が急増中です！！

ランサムウェアの危険性・・・

・データを暗号化して身代金を要求される

・**顧客情報などの機密を流出**させると脅迫される（二重の脅迫）

・基幹システムのデータが失われ、**長期間の事業停止**に追い込まれるケースも

本資料の構成

1. ランサムウェアに備えるバックアップ運用例とベスト プラクティス

ランサムウェア攻撃に対しては「セキュリティによる対策」と「バックアップによる対策」の両輪をバランスよく行う必要があります。この章では特に「バックアップによる対策」に焦点を当て、ランサムウェアからデータを守るための運用のベスト プラクティスを紹介します。Arcserve 製品の設定例も紹介していますが、それ以外のバックアップ製品を使用している方にも役に立つ内容です。

2. サーバのデータ保護 ～ ランサムウェア対策に最適！！Arcserve UDP のご紹介

この章ではバックアップによるランサムウェア対策の3つのポイントを実現するのに最適な、イメージ バックアップ ソフトウェア Arcserve UDP を紹介します。

3. クライアント PC のデータ保護 ～ Arcserve UDP で実現する効率的なバックアップ環境

ランサムウェアの感染源にもなりうるクライアント PC のバックアップも重要です。この章では Windows PC のバックアップを行う上で便利な Arcserve UDP の機能をご紹介します。

4. バックアップ アプライアンス ～ Arcserve UDP 9000 シリーズのご紹介

Arcserve UDP はソフトウェア ライセンスとは別に、アプライアンス形態での購入も可能です。導入が簡単な Arcserve UDP Appliance の概要を紹介します。

5. イミュータブル（不変）ストレージ ～ Arcserve OneXafe 4500 シリーズのご紹介

Arcserve UDP はソフトウェア ライセンスとは別に、アプライアンス形態での購入も可能です。導入が簡単な Arcserve UDP Appliance の概要を紹介します。

1. ランサムウェアに備える
バックアップ運用例とベスト プラクティス

ランサムウェアを使った攻撃に先回りする対策は２つ

ランサムウェア対策には「感染しないための対策（感染予防）」と、
万が一「感染してしまった場合のデータ復旧対策」の両方が必要です。

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

セキュリティによる対策（ランサムウェアに感染/システムに侵入されないために）

ソフトウェアやネットワーク機器を最新の状態に保つ

OS やハイパーバイザー、ネットワーク機器などのインフラ基盤を最新の状態に保ち、脆弱性を解消することで感染リスクを低減します。2020年以降は **VPN の脆弱性**からネットワークに侵入し、ランサムウェアを展開するケースも増えており、特に点検が必要です。

セキュリティソフトウェアを導入し定義ファイルを最新の状態に保つ

アンチウイルス ソフトウエアなどセキュリティ ソフトを導入し、最新ウイルスに対応した定義ファイルを常に最新の状態に保つことで、ランサムウェアを含むマルウェアへの感染リスクを低減します。

メールや SNS の添付ファイルや URL に注意し、従業員教育を行う

メールや SNS の添付ファイルを開くことや、メール文中の URL をクリックすることでランサム ウェアやトロイの木馬に感染する可能性があります。特に、2022年現在大流行している Emotet などのマルウェアは、感染端末のメール ボックスを利用して高度に送信者に成り済ましており、**初見ではマルウェアとの判断が難しい**場合があります。改めての従業員教育が必要です。

arcserve®

バックアップによる対策（改ざん/暗号化されたデータを復旧するために）

万が一の感染に備えて復旧の対策を持つことは急務です！
バックアップデータからのリストアが有効です。

バックアップはいざというときの保険ではなく、確実に簡単にデータの復旧が出来る事が重要です。
業務の重要性からバックアップ対象に優先度をつけ、確実にバックアップを取得、定期的に復旧が可能なことを確認してください。

●確実にバックアップをとっておくべき環境

業務サーバ、仮想基盤、ファイル サーバ、アプリケーション サーバ、メールサーバ、業務用端末（CAD）など

●出来ればバックアップをとっておきたい環境（※）

クライアント PC 環境など

（※）クライアントPC内の重要データはサーバへ格納し、そのサーバをバックアップする運用を先ずは徹底します。

arcserve®

攻撃に耐えるためのバックアップ – 3つのポイント

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

POINT 1 バックアップを複数世代保持

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

POINT 2 バックアップ環境の保全

POINT 3 データのオフライン保管/二重化

POINT 1

バックアップを複数世代保持

ランサムウェアに感染したデータのバックアップではシステムの復旧はできません。より**多くの世代**、より**長期間**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が向上します。

日次で3世代を保持

3日前に感染していた場合、
感染前の状態には復旧できない

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**

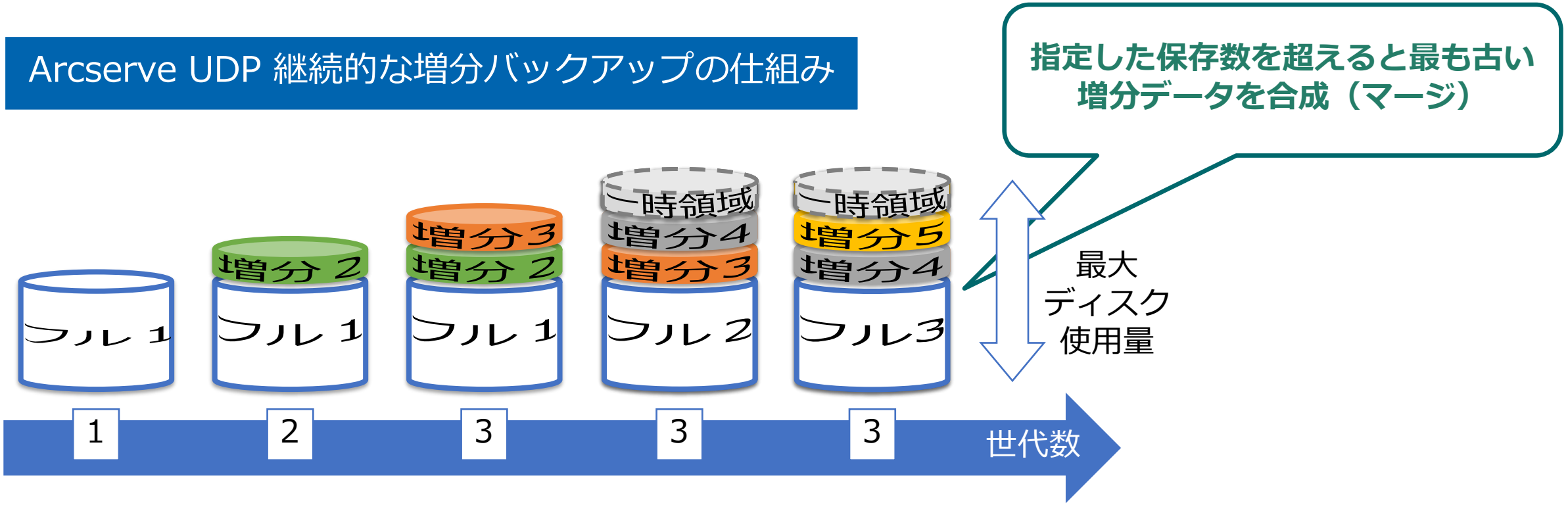
arcserve®

POINT 1

バックアップを複数世代保持 ～ 増分バックアップによるディスクの効率化

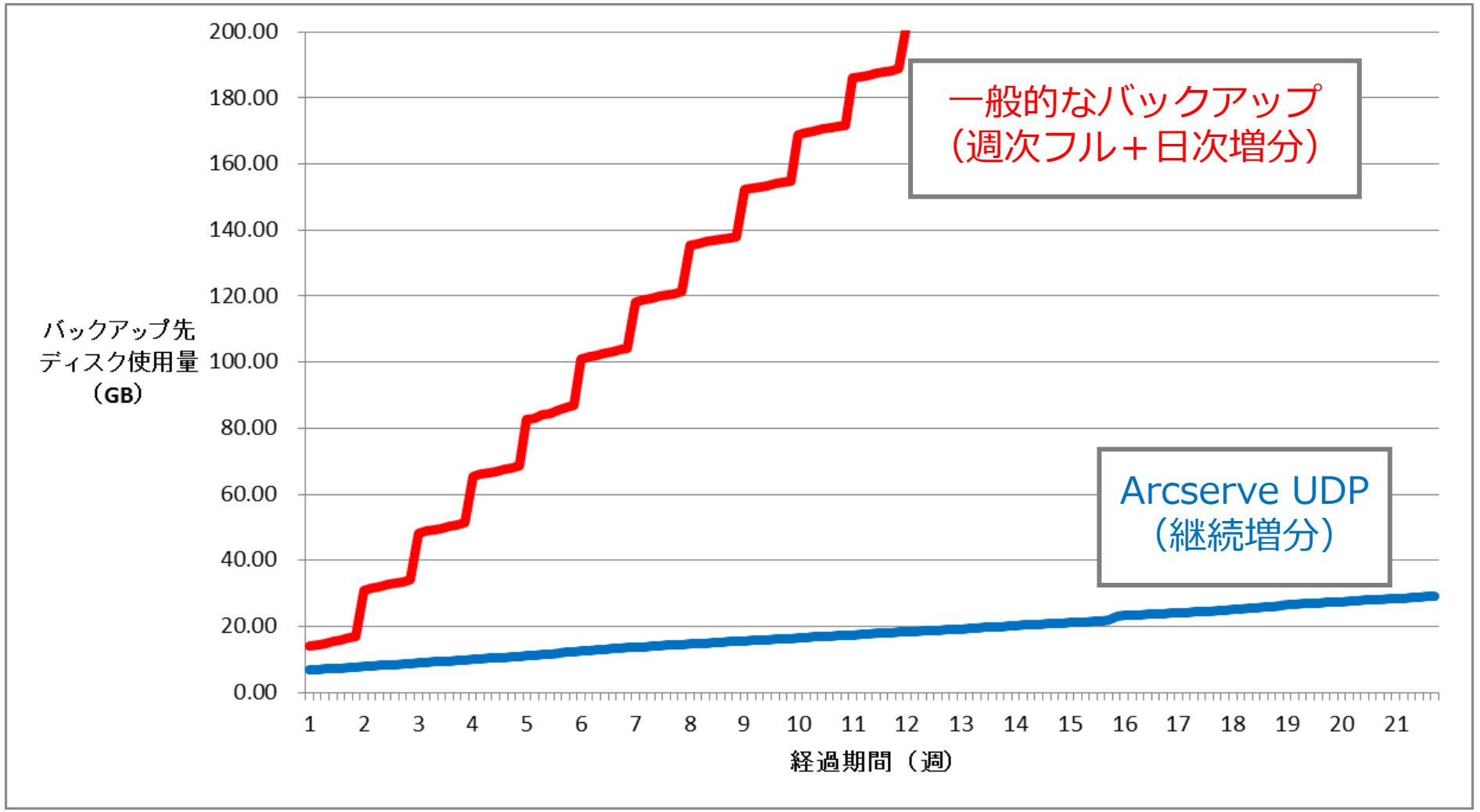
複数世代のバックアップではバックアップ先ストレージの容量確保が課題……。
Arcserve UDP では増分バックアップを継続的に行い、**フル バックアップの取り直しが原則不要**なため、
少ないディスク使用量で多くの世代を保持できます。

Arcserve UDP 継続的な増分バックアップの仕組み



※3世代保持の例。初期設定では7世代を保持し、最大1440世代まで設定可。

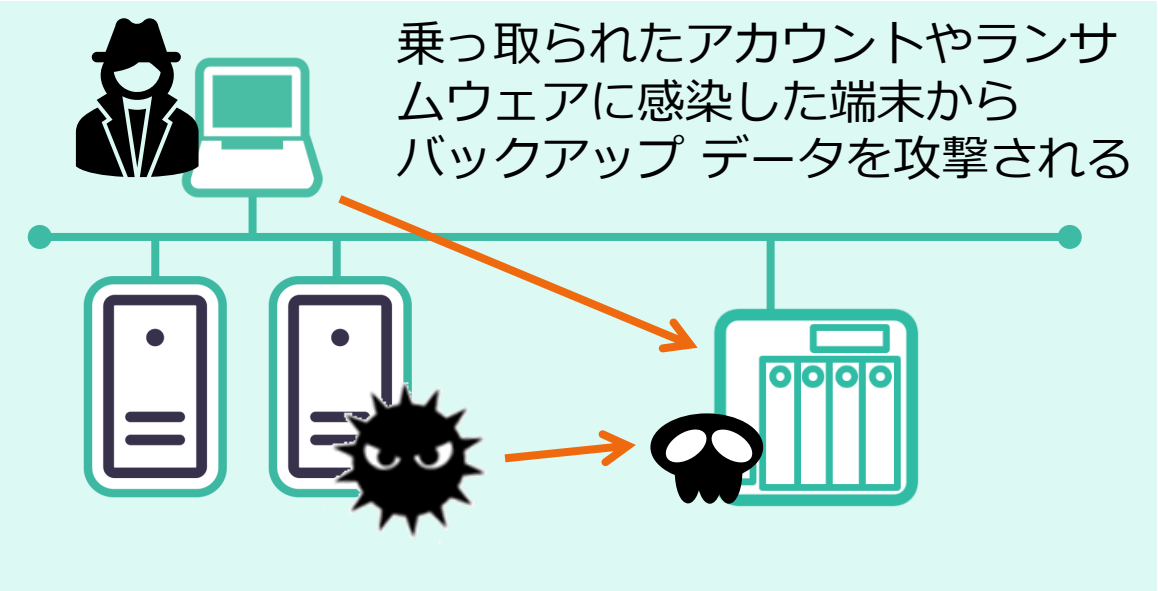
（参考）Arcserve UDP：継続的な増分バックアップの効果



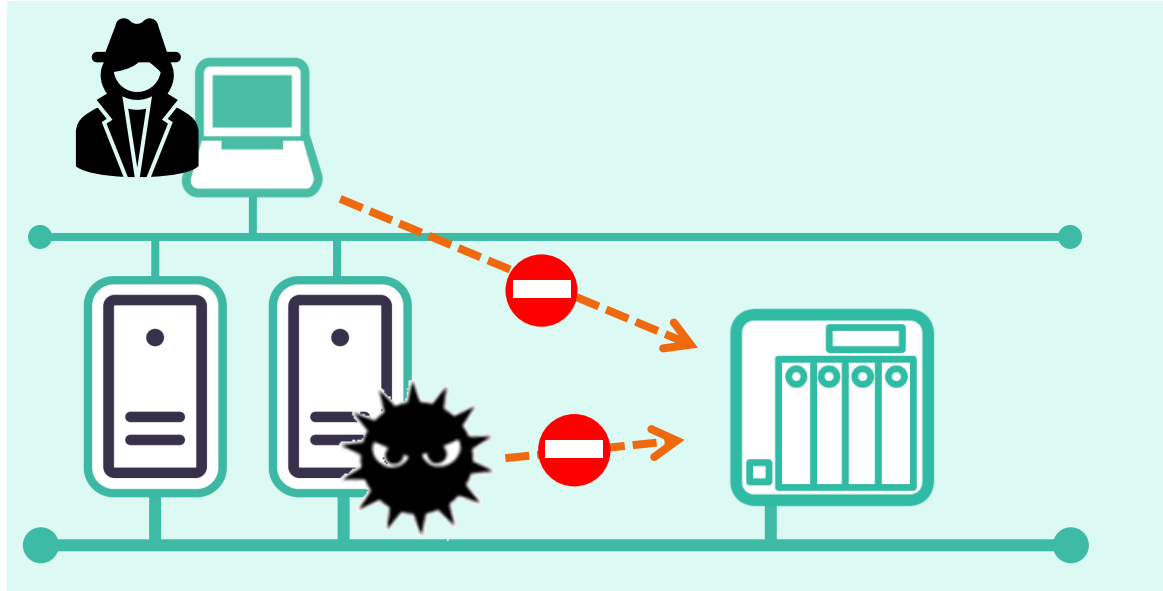
POINT 2 バックアップ環境の保全 ～ NAS にバックアップしている場合

バックアップ環境もネットワークに接続されている限り、ランサムウェアによって暗号化されたり、侵入型攻撃によって破壊されたりするリスクが存在します。バックアップ環境への**無用なアクセスを抑制**し、**データを破壊されるリスクを低減**する必要があります。

【対策前】
初期設定のままの NAS をバックアップ先として使用



【対策後】
NAS のセキュリティ設定を見直すとともに、バックアップ専用 LAN を利用



Point　NAS メーカーの Web サイトで「アクセス管理機能」や「総当たり攻撃対応機能」、「脆弱性対応パッチ」などの情報を確認！！

POINT 2

バックアップ環境の保全 ～ バックアップ サーバの不正ログイン防止

Arcserve UDP では統合管理コンソールのログインに**二要素認証**を有効化できます。不正なログインによりバックアップ データを破壊されるリスクを低減できます。

Arcserve UDP 8.1

確認コードは電子メールやモバイル認証アプリで受信

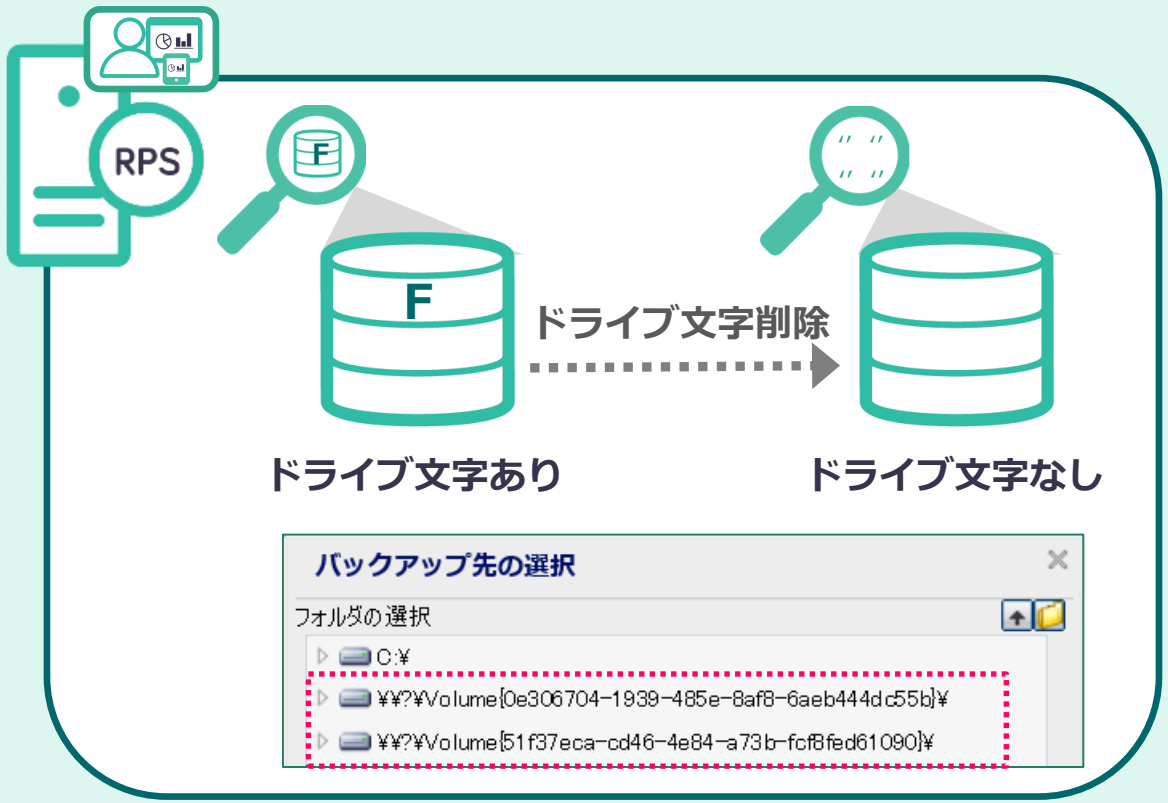
TOTP（Time based One Time Password）

MOTP（Mail based One Time Password）

POINT 2 バックアップ環境の保全 ～ バックアップ データの隠匿

Arcserve UDP の復旧ポイントサーバ（RPS）では、ドライブ文字がないドライブをバックアップ先に指定できます。RPS に侵入されても、データを発見/破壊されるまでの**時間を稼ぎます**。

Arcserve UDP 8.0



レジストリを設定してバックアップ先に選択

エクスプローラから見えない領域にバックアップ データを保存

攻撃者がデータを破壊するまでの時間を稼ぐ

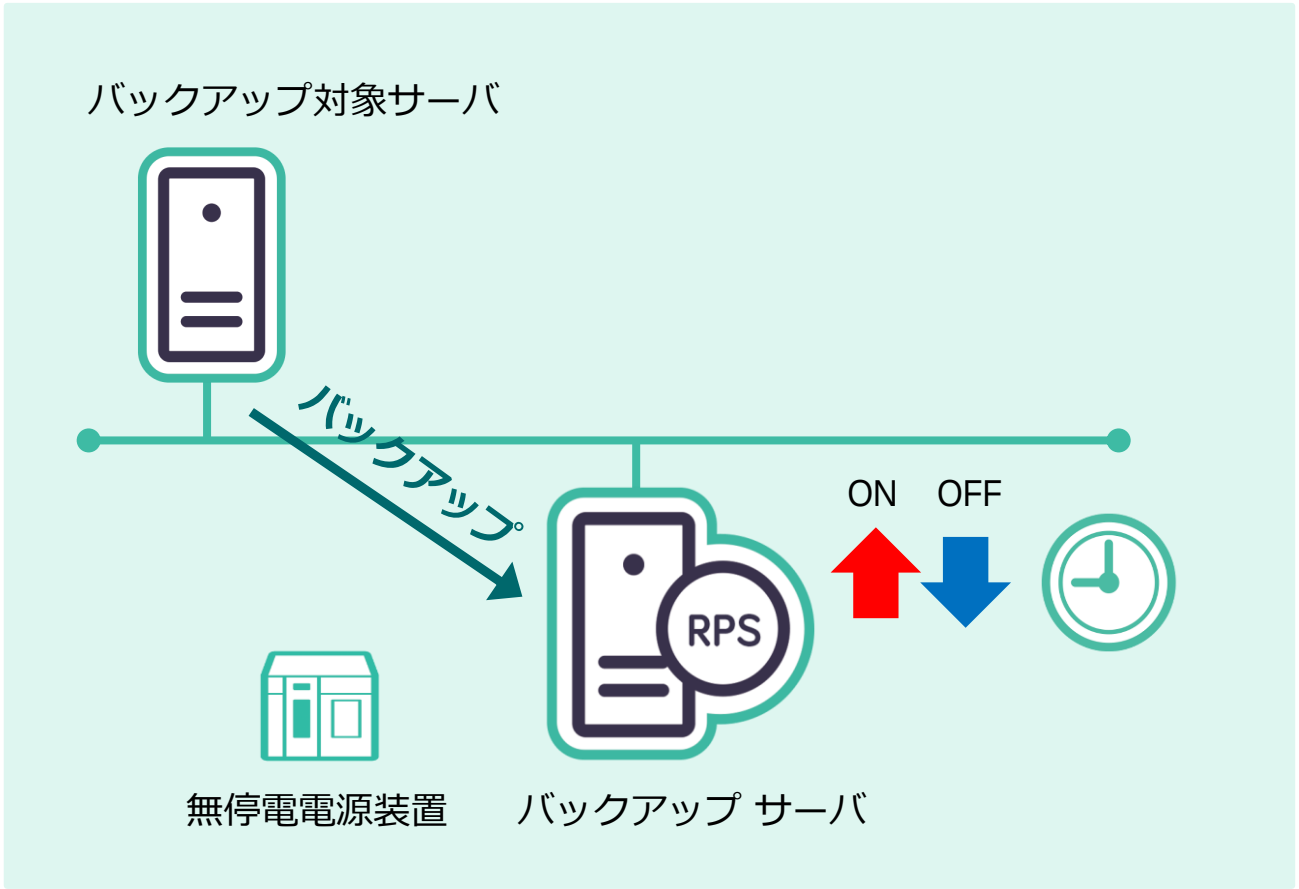
継続増分や重複排除にも対応

arcserve®

POINT 2

バックアップ環境の保全 ～ バックアップ サーバの一時的なオフライン化

バックアップ サーバはバックアップしている間だけ電源をオン。バックアップ終了後はシャットダウンする事で、不正アクセスやデータ暗号化のリスクを低減します。



電源ONは、OSや無停電電源装置（UPS）の制御ソフトウェア、または運用管理ソフトウェアなどを活用。バックアップの時間にバックアップ サーバの自動で電源を入れます。

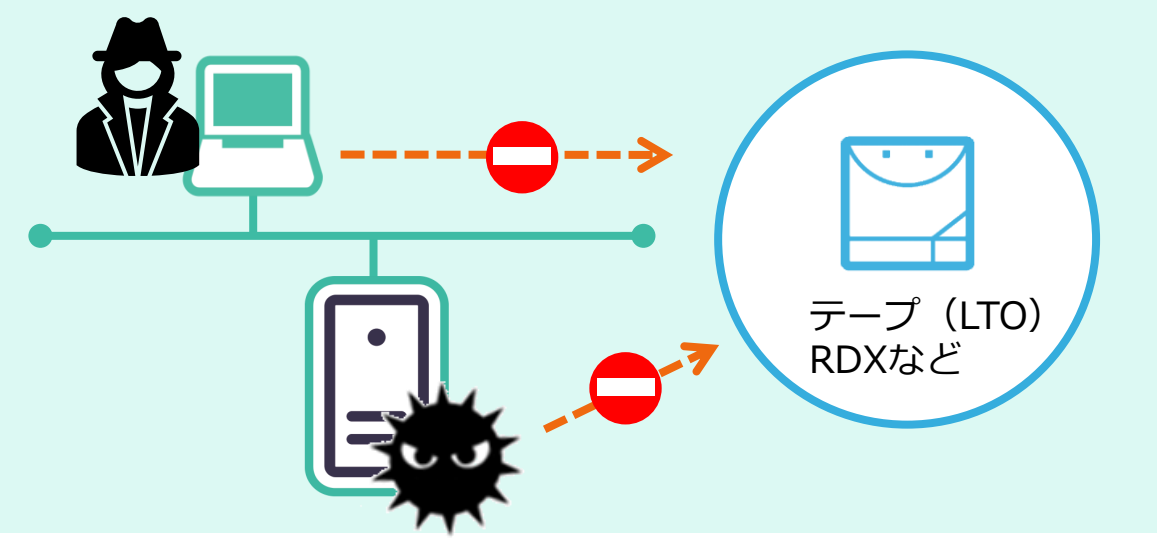
電源OFFはバックアップソフトの実行後スクリプト機能を活用。バックアップが終了後に、バックアップ サーバでシャットダウンスクリプトを実行し、自動でシャットダウンします。

arcserve®

POINT 3 データのオフライン保管/二重化

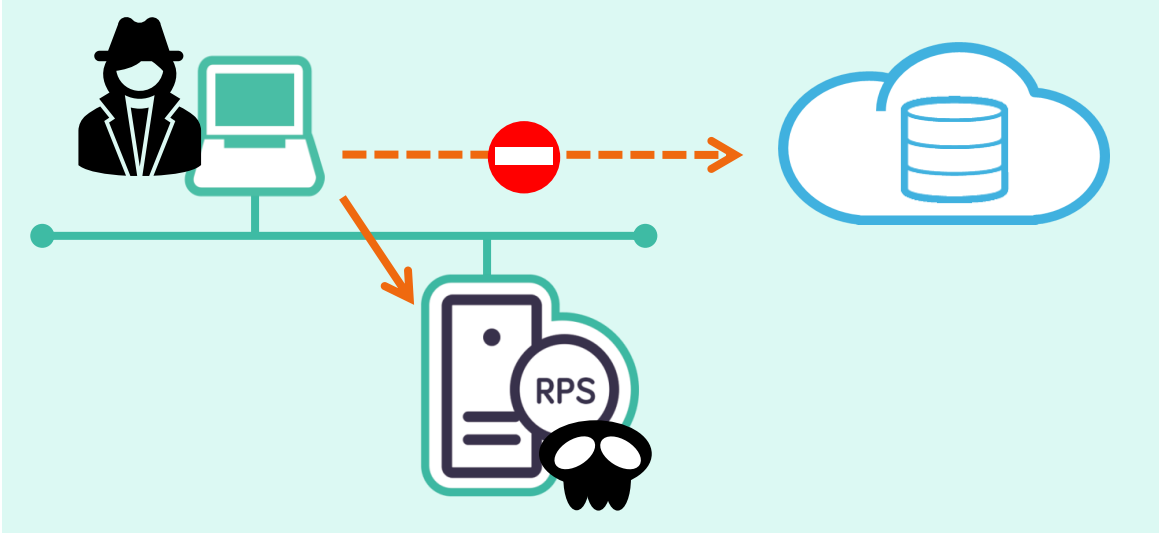
テープなどへのオフライン保管

バックアップ データがネットワークに接続されている限り、ランサムウェアによって暗号化されたり、侵入型攻撃によって破壊されたりするリスクは払拭できません。そこで、**物理的にアクセスできない場所（オフライン）**にバックアップ データを保管し、データの破壊を防止します。



クラウドへのデータ退避（二重化）

バックアップ データをクラウドにコピーしておくことも有効です。クラウドのデータを操作できる専用の**アカウントを分けておく**ことで、万一オンプレミスの管理者アカウントが乗っ取られてもデータを守れます。

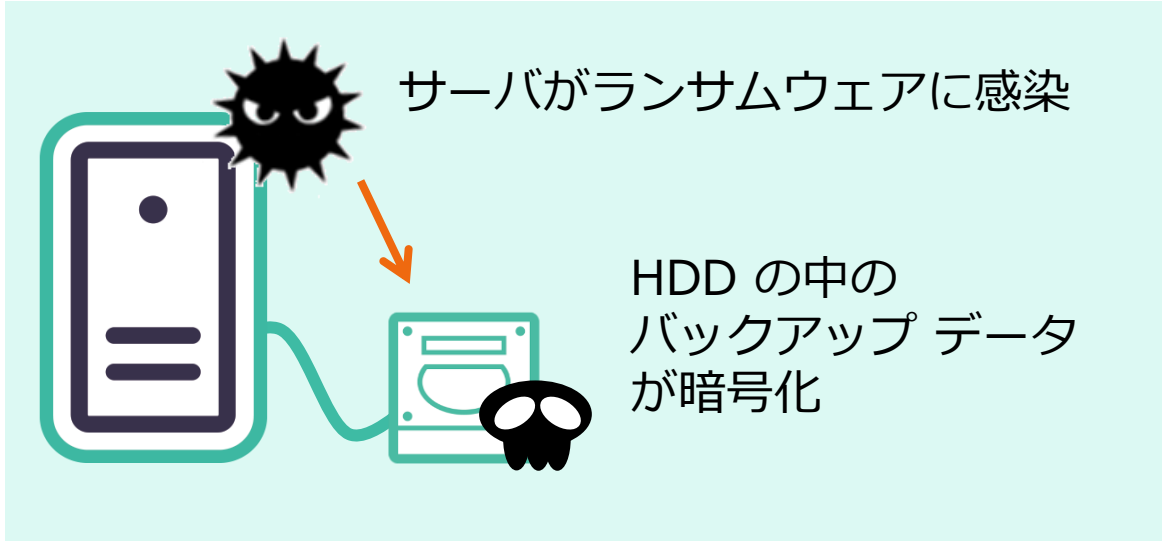


arcserve®

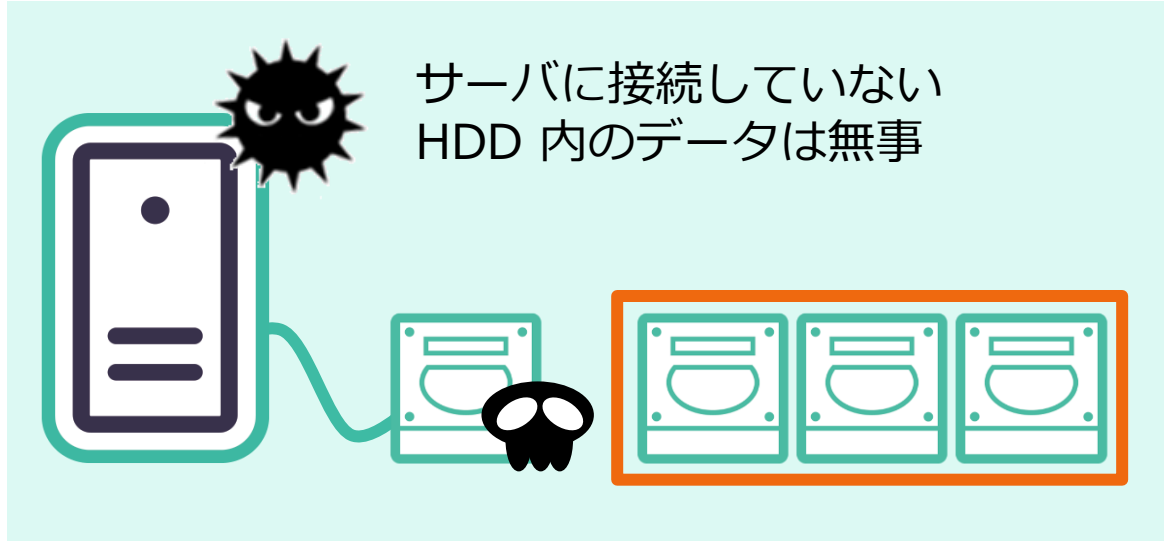
POINT 3 データのオフライン保管/二重化 ～ バックアップ用 HDD のローテーション

バックアップ データの保存に外付け HDD を使用している場合は、**HDD を増設してオフライン保管を実現**します。週に1回等の頻度で HDD を付け替える事で、過去のバックアップを攻撃から守ります。

【対策前】
バックアップ用 HDD を繋ぎっぱなし



【対策後】
HDD 4台でローテーションしてバックアップ



Point 複数のHDD を使ってバックアップの保存世代数を増やすことで、潜伏期間が長いランサムウェアにもある程度耐えられる！！

POINT 3 データのオフライン保管/二重化 ～ クラウドへのデータ退避

Arcserve UDP の RPS に保管されたバックアップ データは Arcserve UDP Cloud Hybrid に複製（レプリケート）できます。Arcserve UDP Cloud Hybrid にアクセスするための**アカウントはオンプレミスとは分離**されており、侵入型攻撃によるアカウント剽窃のリスクを分散できます。

お客様オフィス、データセンターなど

バックアップ

RPS

データの複製

Arcserve UDP Cloud Hybrid

日常的なデータ破損やシステム障害には、手元のバックアップから**迅速に復旧！**

災害やランサムウェアによるサイト障害時には、**クラウド**にあるバックアップから復旧！

arcserve®

POINT 3 データのオフライン保管/二重化 ～ オブジェクト ロック ストレージへのコピー

Arcserve UDP では、オブジェクト ロックが可能なストレージにバックアップ データをコピーできます。オブジェクト ロックは**一定期間書き換え不能**で、データの安全性を高めます。

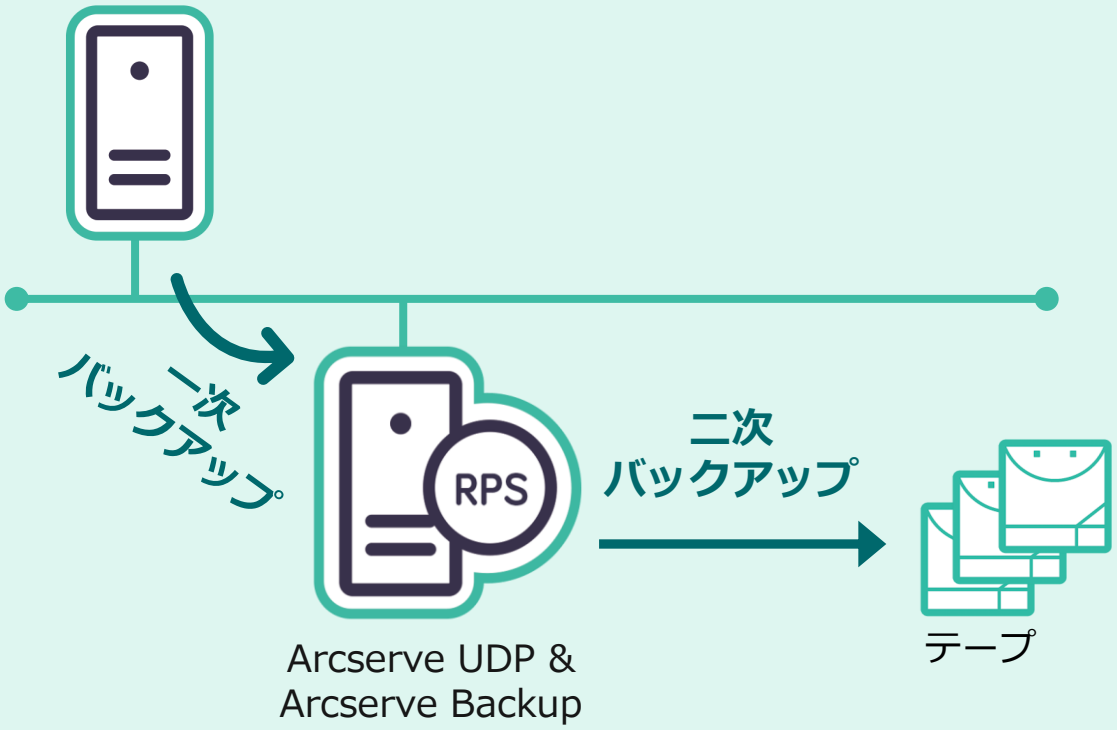
Arcserve UDP 8.0

- 書き換え不可の２次保管先に バックアップ データの安全保管
- データの長期保管 (保管期間は S3 バケット側で設定)
- オブジェクト ロックの ガバナンスとコンプライアンスの ２つのモードに対応

POINT 3

データのオフライン保管/二重化 ～ テープへの二次バックアップ

Arcserve UDP ではディスクに保存したイメージ バックアップ データをさらにテープに二次バックアップできます。**オフライン保管とバックアップ データの二重化を両立**し、データの安全性をさらに高めます。



**Arcserve UDP を購入すると
テープ連携用の Arcserve Backup が
基本無料でついてくる！**

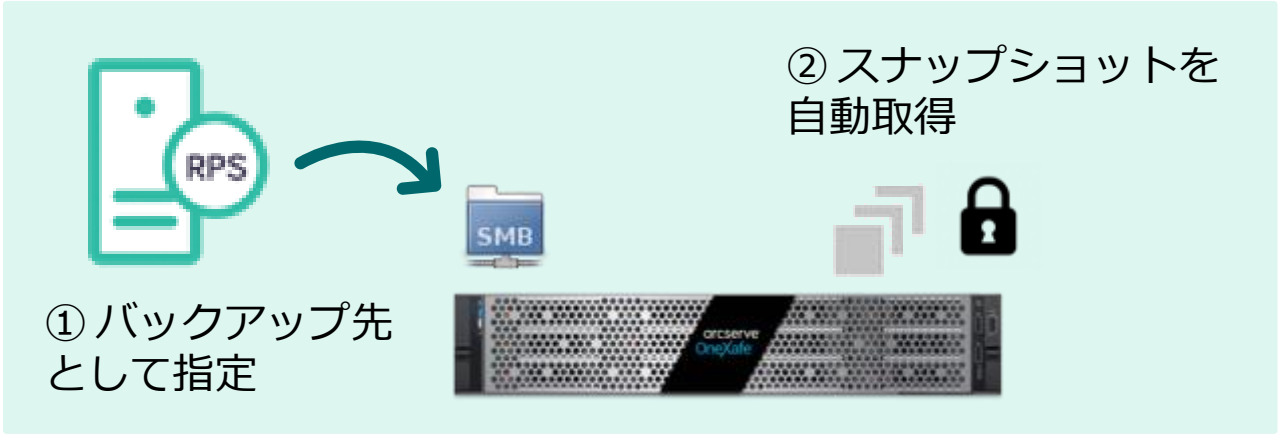
テープのオフライン保管でランサムウェアや侵入型攻撃からデータを守る。

重複排除データストアをそのままテープにバックアップできる。

arcserve®

POINT 3 データのオフライン保管/二重化 ～ イミュータブル（不変）ストレージへのバックアップ

Arcserve OneXafe はバック グラウンドで定期的に”不変な”スナップショットを取得するバックアップ専用 NAS です。データが改ざん/削除されも、スナップショットを使って正常時の状態に復旧できます。



Arcserve UDP や Arcserve Backup の設定/運用をそのまま活かせる！

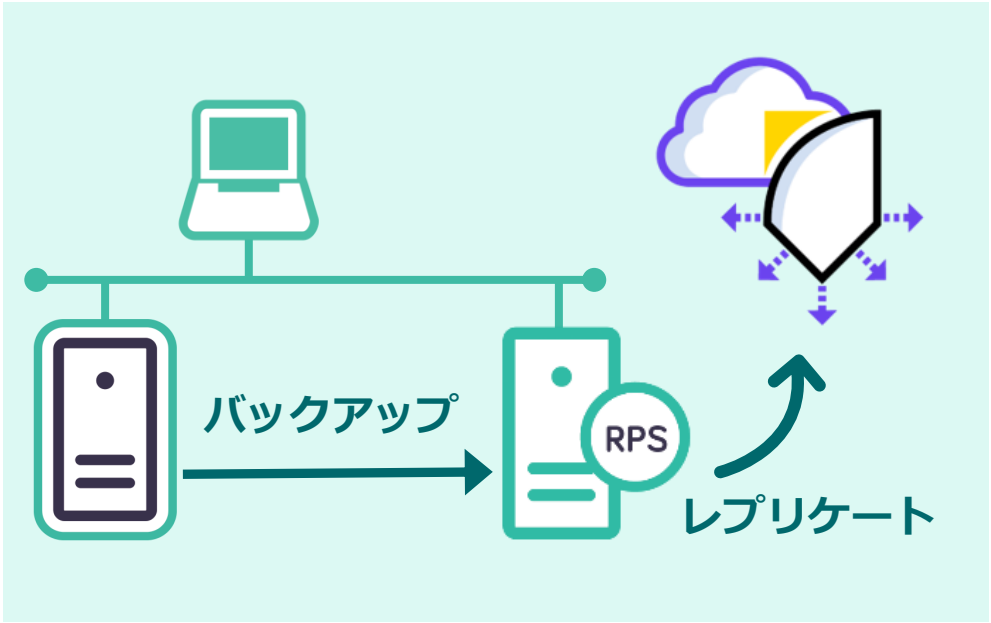
大容量のバックアップ データを オンプレミスに保管できる。

テープ交換のような 定期的な作業は不要！

まとめ：安全なバックアップ環境

ランサムウェア被害にあっても比較的短期間に業務を再開できている企業/組織は多く、そのポイントは**やはり適切なバックアップ**です。一方で、バックアップ データを狙う攻撃も多発しており、**バックアップ データ自体の保護**を意識した運用が必要です。

複数のランサムウェア対策を組み合わせたバックアップ運用例



- □ Arcserve UDP 復旧ポイント サーバ（RPS）にバックアップ。
- □ 継続的な増分バックアップと重複排除を有効にし、30 日分のバックアップを保存。
- □ Arcserve UDP コンソールのログインには二要素認証を利用。
- □ バックアップ データを Arcserve UDP Cloud Hybrid にレプリケート

※ 本運用案はランサムウェアによる被害リスクを低減する例であり、被害を完全に防ぐことをお約束するものではありません。

更に・・・ビジネス継続の対策（感染した後の対応処理）

バックアップ運用の保全性を確保できたら、次のステップとして、ランサムウェアなどに
感染してしまった場合を想定した、業務再開までの対応処理を計画しておく事が有効です。
以下の運用が重要となります。

POINT 1 **感染事故の影響調査**

POINT 2 **システム復旧手段の確保**

POINT 3 **業務再開手段の選択**

POINT 1

感染事故の影響調査

感染した事が判明した場合、**直ちにその影響範囲を確認**する必要があります。

・ランサムウェアの種別は何か？
・どこから感染したのか？
・どこまで感染しているか？
・いつから感染していたか？
・社外に感染させていないか？

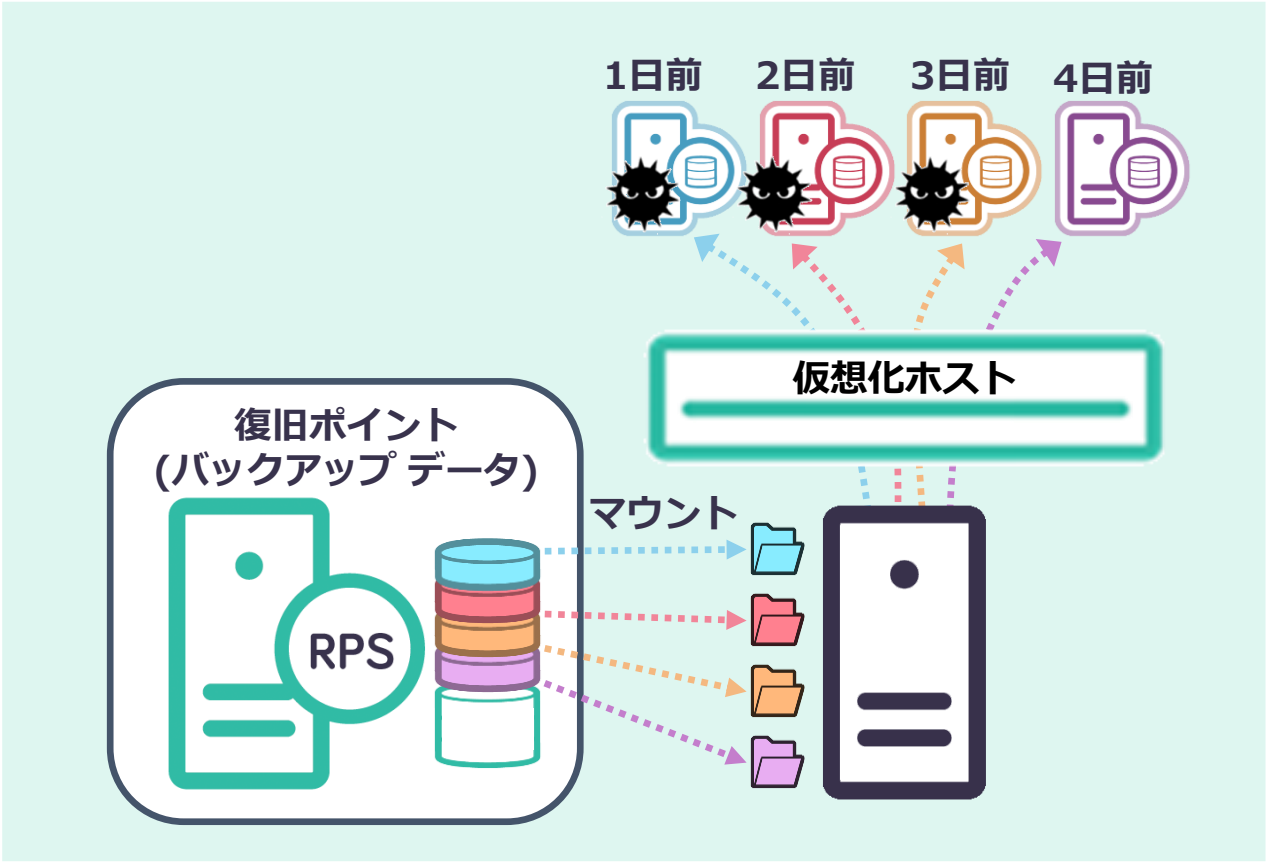
ランサムウェアの種別を特定する事で、感染経路や影響範囲が推定できます。
感染源が確認できたら感染源を速やかにネットワークから隔離し、感染の再拡大を防ぎます。
社外に影響を与えた可能性がある場合は、相手先へも速やかに連絡を取ります。
また、被害の内容によっては警察や関係当局へ被害相談する事も検討します。

バックアップ運用としては、**『いつから感染していたか』『どこまで感染しているか』**を見極める事で、
健全なバックアップデータの特定ができます。
健全なバックアップデータが特定できれば、業務の手戻り範囲と業務再開の目処を付けることができます。

POINT 1

感染事故の影響調査 ～ 安全なバックアップ世代を確認

Arcserve UDP のインスタント VM 機能では、復旧ポイント参照して仮想マシンを作成します。リストア処理が不要で短時間（インスタント）に起動できるのが特徴です。
インスタント VM を起動し動作確認を行えば**正常な状態のバックアップ データを短時間で特定**できます。



感染ノードの世代データで同時起動

最小のディスク容量でVM起動
(バックアップ データからマウント)

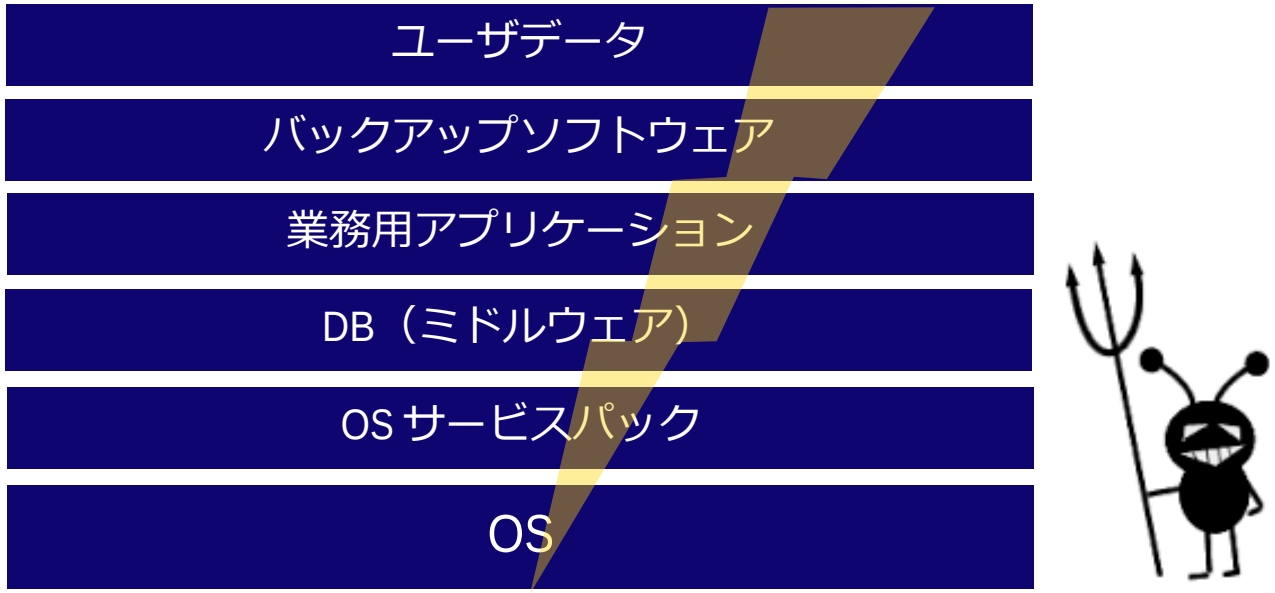
バックアップ データへの
書き込みなし

POINT 2

システム復旧手段の確保

ランサムウェアなどのウイルス感染で、最悪の場合はシステム全体の復旧を行わなければなりません。OS、ミドルウエア、アプリケーションなどシステムの構成要素を全てリカバリする必要があり、データだけのバックアップでは不十分です。

そこでシステム全体をリカバリする事を前提としたバックアップ方法を準備します。



POINT 2

システム復旧手段の確保 ～ Arcserve のシステム復旧（業務再開）手段

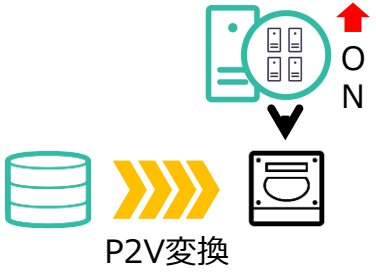
Arcserve Backup Disaster Recovery Option（DRO）

ウィザードに従って手順を進めることで簡単・確実にシステムを復旧できます。**テープからの直接リストア**も可能です。

Arcserve UDP ベアメタル復旧

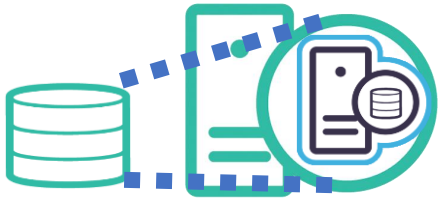
簡単な操作手順でサーバ丸ごとリストアします。バックアップしたサーバとは**別筐体のサーバへのリストアも可能**です。オプション不要で、標準機能として利用できます。

Arcserve UDP 仮想スタンバイ



バックアップしたサーバ イメージをあらかじめ P2V して仮想マシンのスタンバイを作成します。本番サーバの障害が発生した際は、スタンバイの仮想マシンを立上げて**迅速に業務再開**します。

Arcserve UDP インスタントVM



バックアップ データを直接参照し、仮想マシンとして起動します。仮想スタンバイと異なり、**あらかじめ P2V しておく必要がありません**が、本番運用するには別途リストア作業が必要です。

Arcserve Replication / High Availability（Arcserve RHA） フルシステム シナリオ

サーバのシステム全体をリアルタイムに複製します。本番サーバに障害が発生した際は、複製されたシステムを仮想マシンとして起動し、業務を再開します。HAであれば切替を自動で行えます。ただし、複数世代のデータ保持はできないため、ランサムウェア対策には向いていません。物理障害や災害時の業務継続目的にご利用いただく事が多い製品/機能です。

POINT 3

業務再開手段の選択

システム復旧（業務再開）手段は幾つか方法がありますが、
ポイントとなるのは、以下の２つの要素を計画に入れることです。

『RPO：目標復旧ポイント（いつの時点に戻れればよいか）』
『RTO：目標復旧時間（いつまでに復旧出来ればよいか』

RPO は世代管理の基本的な指標ともなります。リスクを考慮しつつ無理のない運用計画を立てます。
RTO は業務再開までの時間設定です。ビジネス インパクトを考慮しシステム毎に優先順位をつけた運用計画を立てます。

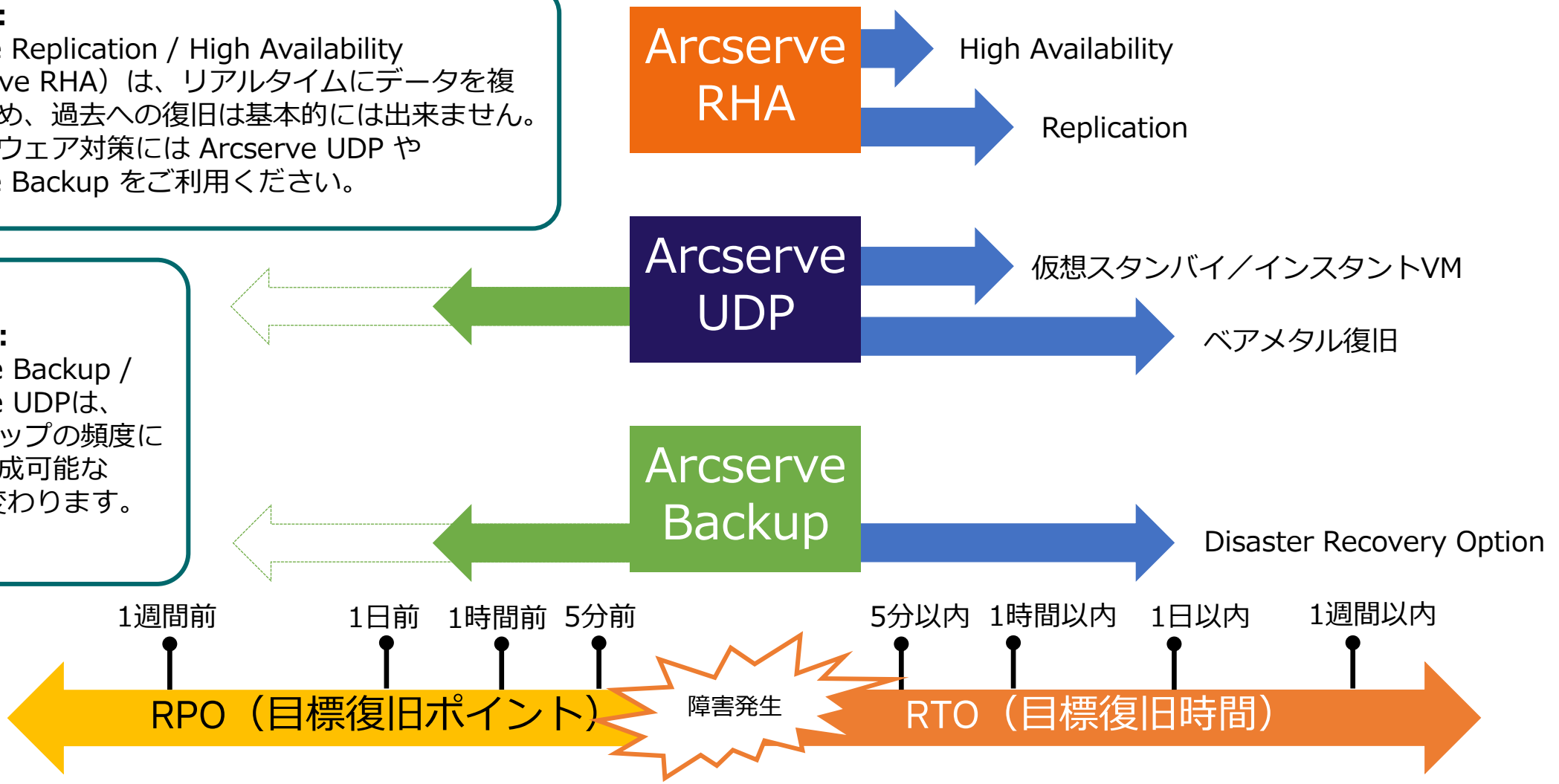
arcserve®

POINT 3

業務再開手段の選択 ～ 目標復旧ポイントと目標復旧時間の設定

Point 1 :
Arcserve Replication / High Availability（Arcserve RHA）は、リアルタイムにデータを複製するため、過去への復旧は基本的には出来ません。ランサムウェア対策には Arcserve UDP や Arcserve Backup をご利用ください。

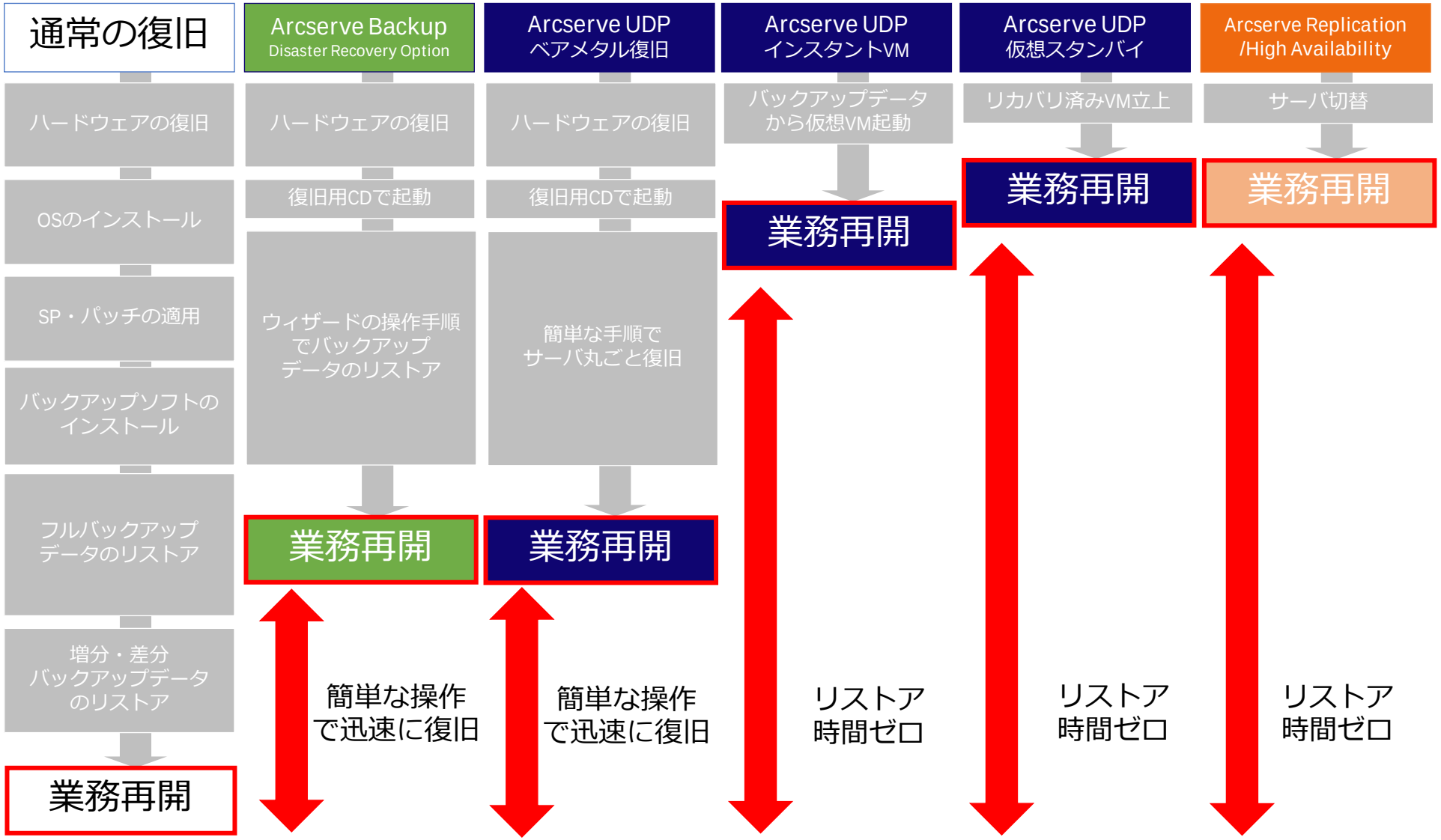
Point 2 :
Arcserve Backup / Arcserve UDPは、バックアップの頻度によって達成可能な RPO が変わります。



arcserve®

POINT 3

業務再開手段の選択 ～ 業務再開までの時間比較



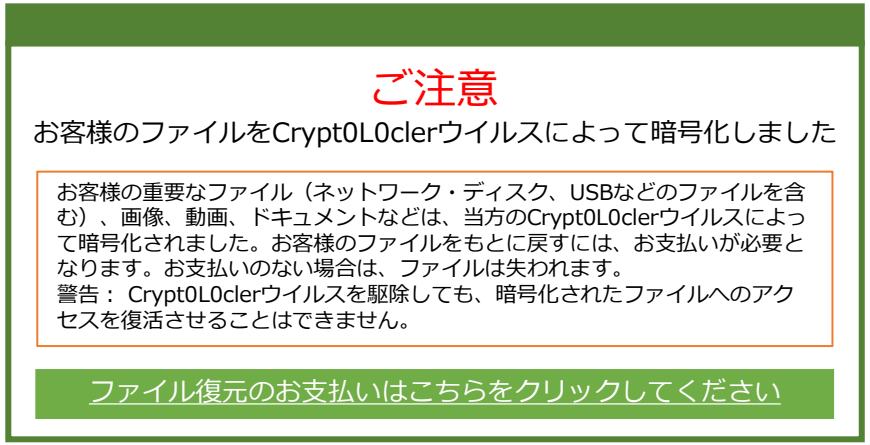
（参考）ランサムウェアとは（1/2）

ランサムウェアとは

ランサムウェアとはデータを暗号化するコンピュータ ウイルスの一種です。暗号化されたデータを元に戻すことと引き換えに身代金（Ransome）を要求する事からこう呼ばれます。

個人の PC だけではなく、企業の基幹システムや病院の電子カルテなど重要なシステムが停止に追い込まれる事例が頻出しており、大きな社会問題になっています。

身代金を支払ってもほとんどの場合、暗号化の解除やシステムの復旧はされず問題は解決しません。企業・組織自身でデータを守る方法が求められています。



※ランサムウェア感染イメージ

ランサムウェアの種類と特徴

ランサムウェアには幾つもの種類があり、犯罪組織が日々新しい攻撃手法を開発しています。脆弱性に対するセキュリティ対策が確立される前に拡散してしまう「ゼロディ・アタック」も報告されており、常に十分な警戒が必要です。

CryptoLocker	2013年暗号化ランサムウェアとして出現。ビットコインを使って支払いを要求。
Locky	2015年末に出現、ばらまき型メールによる感染で流行。感染端末だけではなくネットワーク上のファイルも暗号化。
WannaCry	2017年に出現し大流行。ネットワークを介して感染拡大する特徴をもつ。
Maze	2019年に出現。機密情報を窃取した上で公開すると脅迫する暴露型ランサムウェアとして流行。

（参考）ランサムウェアとは（2/2）

ランサムウェアの感染経路

従来型のランサムウェアでは、主に**メールの添付ファイル**と **Web サイト**からの感染が報告されていました。

しかし、2017年以降流行した WannaCry や Petya のように、ネットワークの脆弱性を突いて感染を拡大するものがあります。

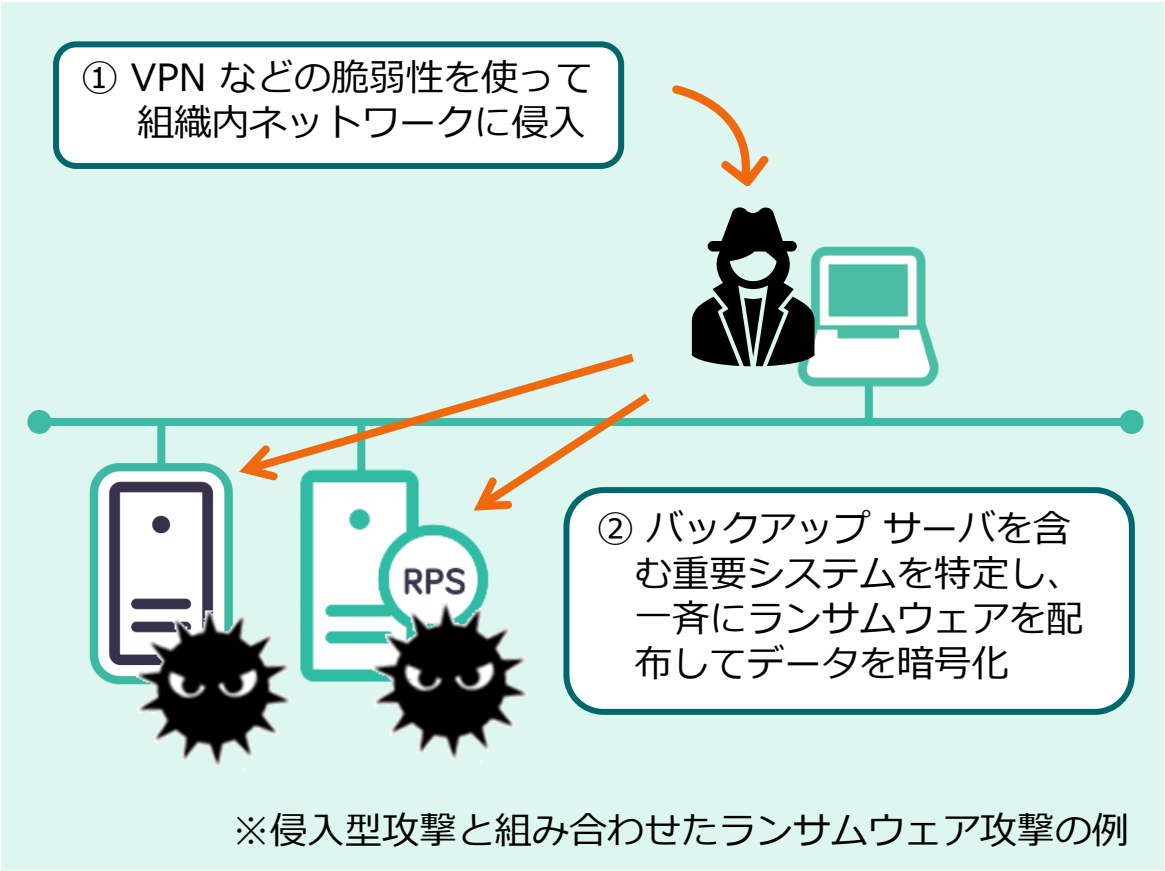
加えて、日本国内では2020年頃より侵入型攻撃（標的型攻撃）と組み合わせ、組織内の重要システムを特定した上で一気にランサムウェアを配布・データを暗号化する手口が広がっています。

ファイア ウォールや VPN機器、ハイパーバイザー、OS など IT インフラ全体の**脆弱性対策**がこれまで以上に重要になっています。

ランサムウェアの拡散

ランサムウェアには自己増殖機能があるものもあり、社内のネットワークを経由し他のコンピュータにも感染を拡大します。

さらに、ランサムウェアには潜伏期間があるものがあり、気づかないうちに社内に蔓延してしまい被害規模が大きくなる危険があります。



※侵入型攻撃と組み合わせたランサムウェア攻撃の例

arcserve®

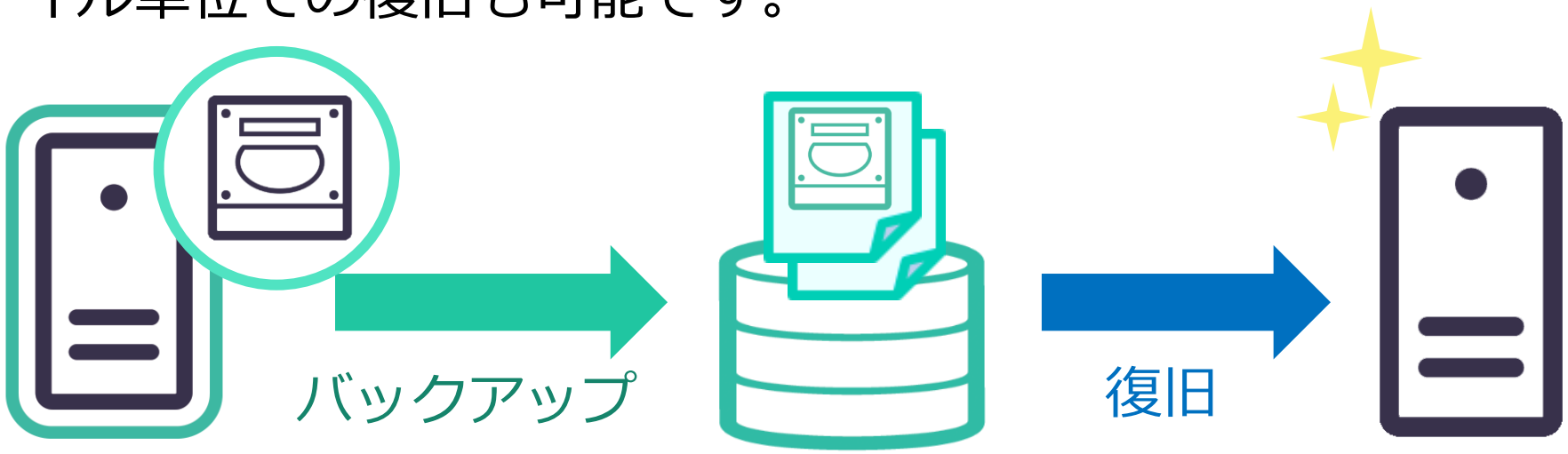
2. サーバのデータ保護

～ ランサムウェア対策に最適！！
Arcserve UDP のご紹介

超簡単イメージバックアップ
Arcserve Unified Data Protection（UDP）

イメージバックアップとは

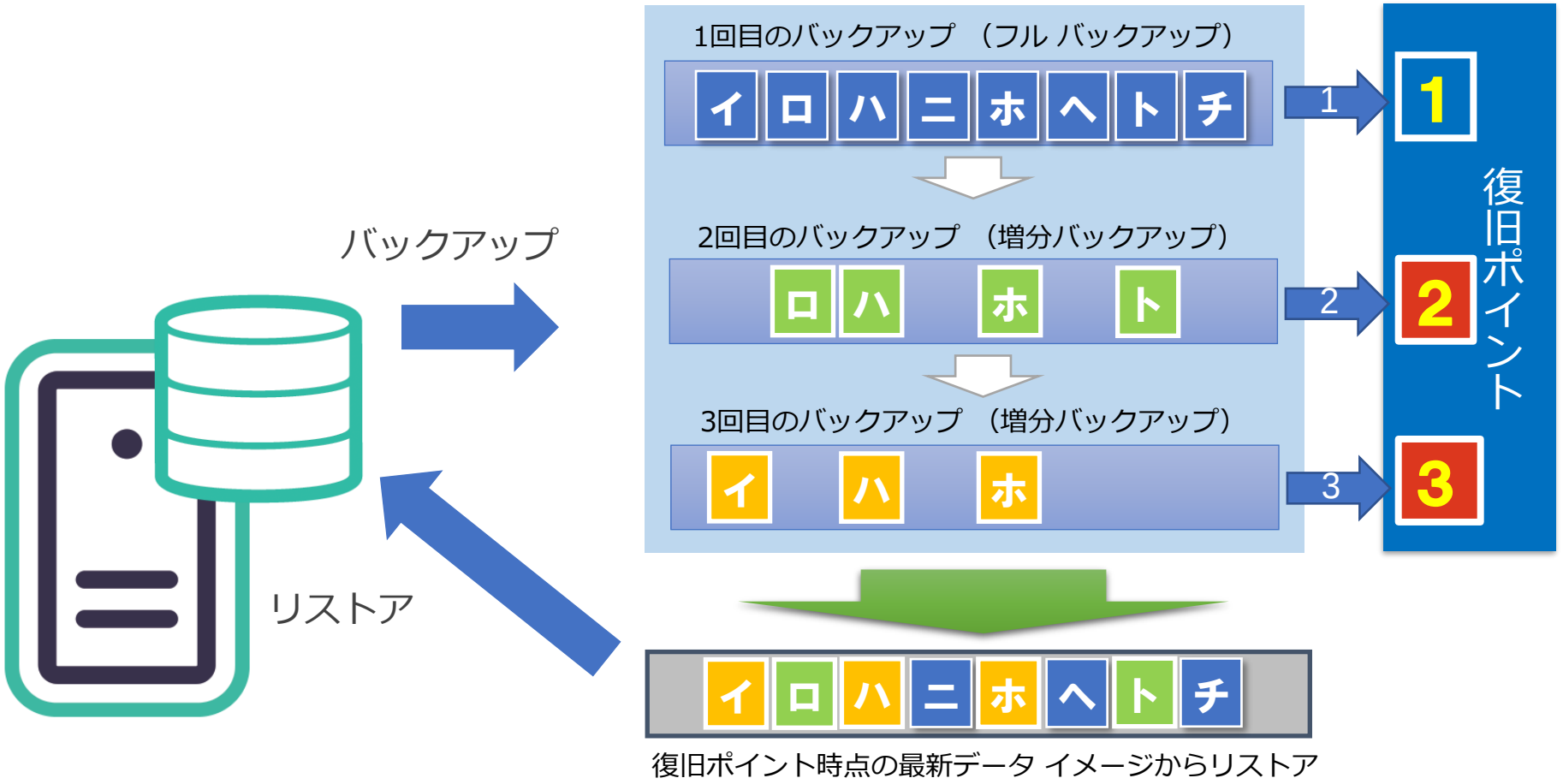
ファイル単位ではなく、ディスク全体を丸ごと高速にバックアップします。
OSやデータを含むシステム全体をまとめて簡単に復旧できます。
個別のファイル単位での復旧も可能です。



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 UDP の継続的な増分バックアップはリストアも簡単！

ブロックレベルの増分運用で**データ量を最適化**
増分運用なのに**リストアは１回**で復旧可能！



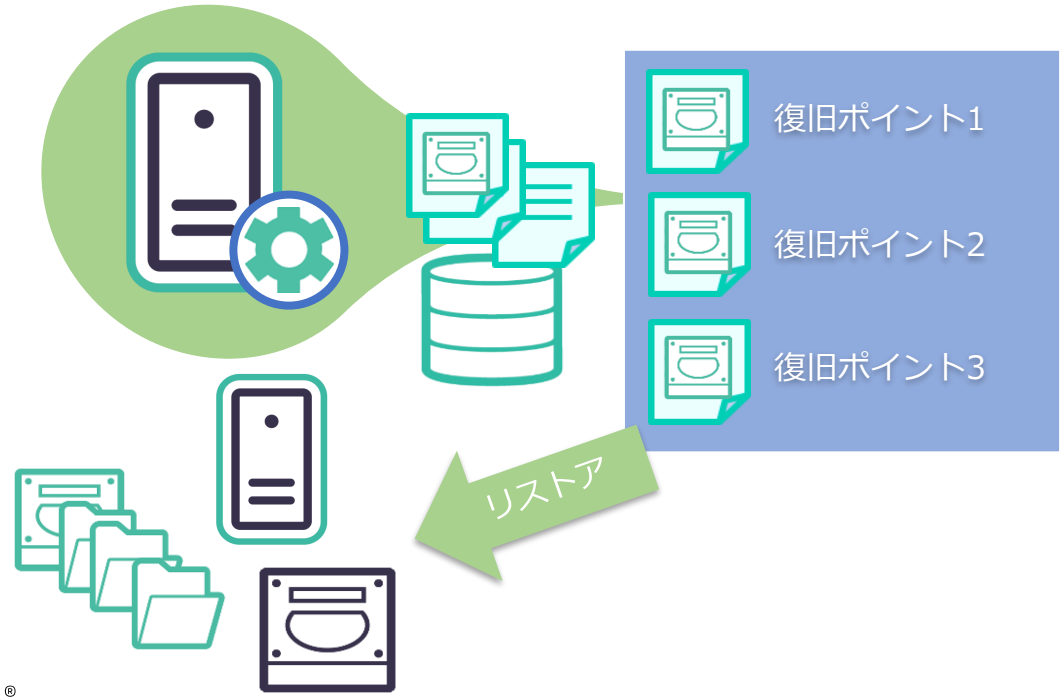
Arcserve UDP は簡単操作でファイル単位のリストア”も”可能

システム全体もファイル個別にもリストア可能。
使い慣れたエクスプローラからドラッグアンドドロップで
ファイルを簡単にリストアすることもできます。

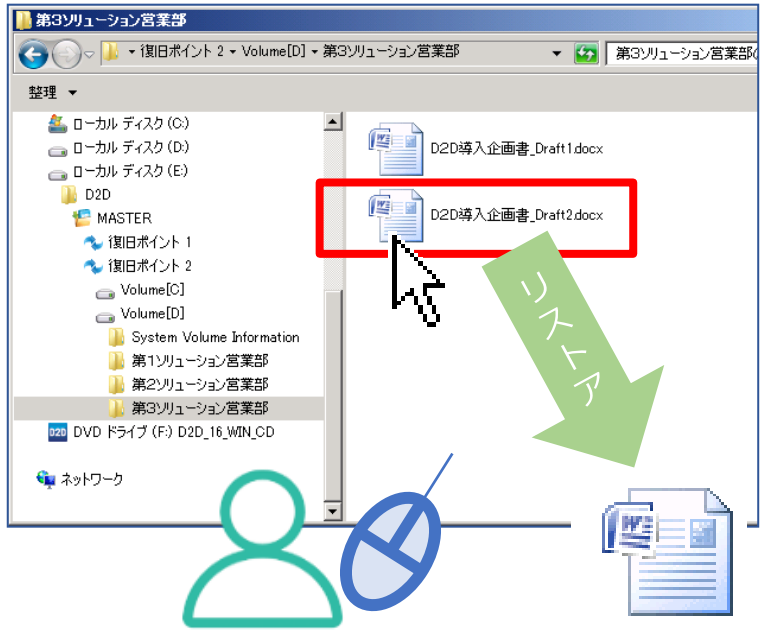
こんな所が便利！

➔ 利用者自身で以前バックアップしたファイルを取り出せる

➔ 管理者工数が削減される



ドラッグ＆ドロップでファイル単位のリストア

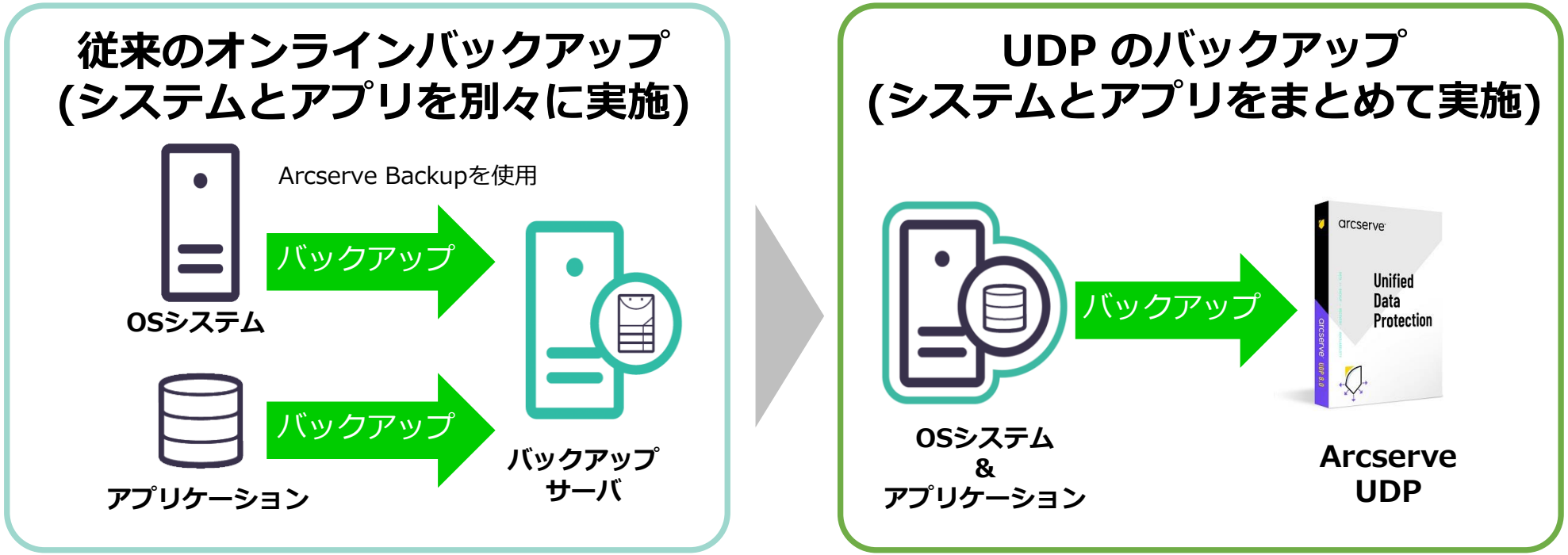


※エクスプローラからのリストアには管理者権限が必要です

Arcserve UDP：システムとアプリケーションのオンライン バックアップ

こんな時に便利！

- Oracle Database、SQL Server、Exchange Server、SharePoint Server、Active Directory 等を止めずにバックアップしたい
- アプリケーションの復旧を簡単にしたい



システム バックアップとデータ バックアップの統合で運用がシンプルに！

arcserve®

Arcserve UDP：柔軟なバックアップスケジュール (設定例)

- 曜日を指定したバックアップスケジュール例

追加 削除

	タイプ	説明	日	月	火	水	木	金	土	時刻
		増分 バックアップの開始: 10:00 午後		✔	✔	✔	✔	✔		10:00 午後

- 日次・週次・月次のバックアップスケジュール例

追加 削除

	タイプ	説明	日	月	火	水	木	金	土	時刻
		1 日 1 回の 増分 バックアップ	✔	✔	✔	✔	✔	✔	✔	10:00 午後
		週 1 回の 増分 バックアップ						✔		10:00 午後
		月 1 回の 増分 バックアップ						5/30		10:00 午後

- 曜日指定した日次・週次・月次のバックアップスケジュール例

追加 削除

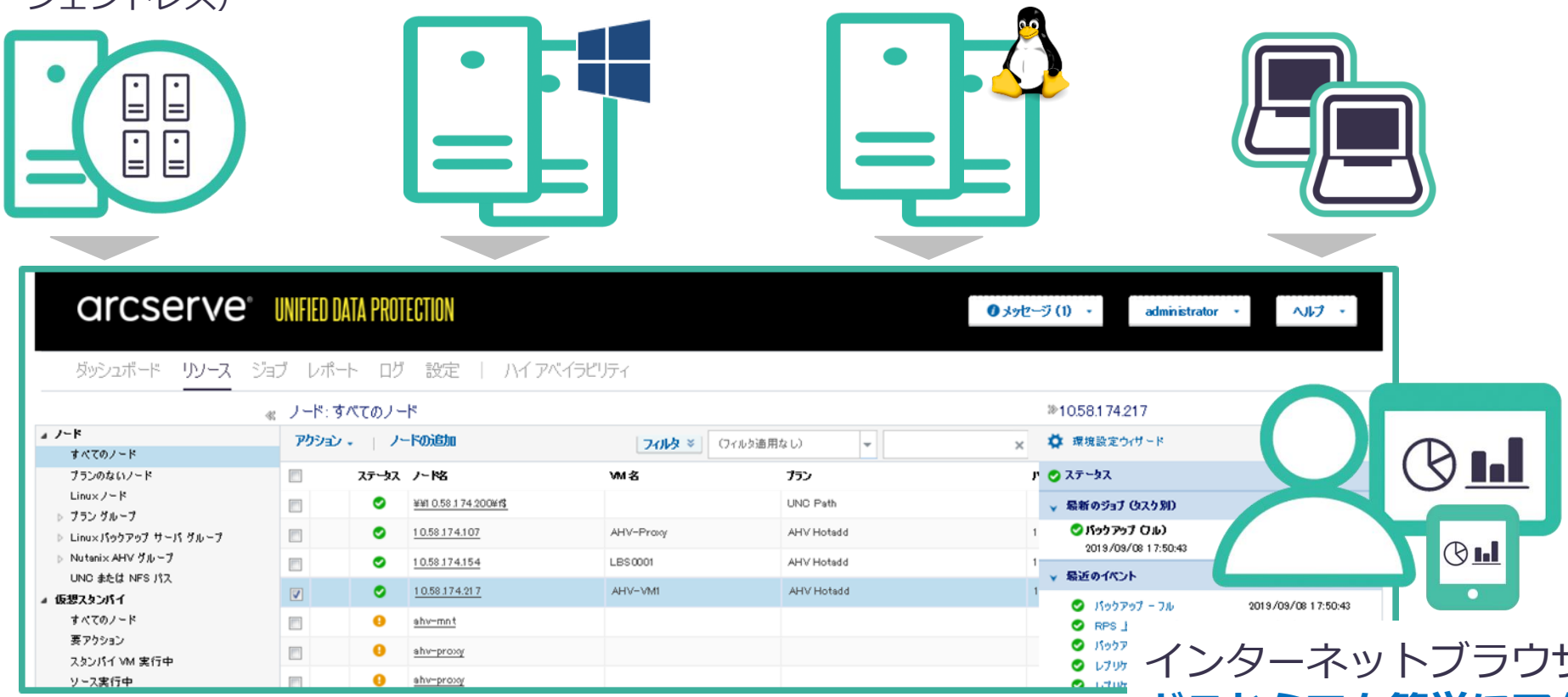
	タイプ	説明	日	月	火	水	木	金	土	時刻
		増分 バックアップの開始: 10:00 午後		✔	✔	✔	✔			10:00 午後
		週 1 回の 増分 バックアップ						✔		10:00 午後
		月 1 回の 増分 バックアップ						5/30		10:00 午後

Arcserve UDP なら１つのコンソールですべてを管理できる

こんな時に便利！

- Windows / Linuxをまとめてバックアップしたい
- 物理や仮想環境、クラウドのバックアップをまとめて管理したい

仮想マシン（エージェントレス）　物理サーバ（Windows）　物理サーバ（Linux）　クライアントPC



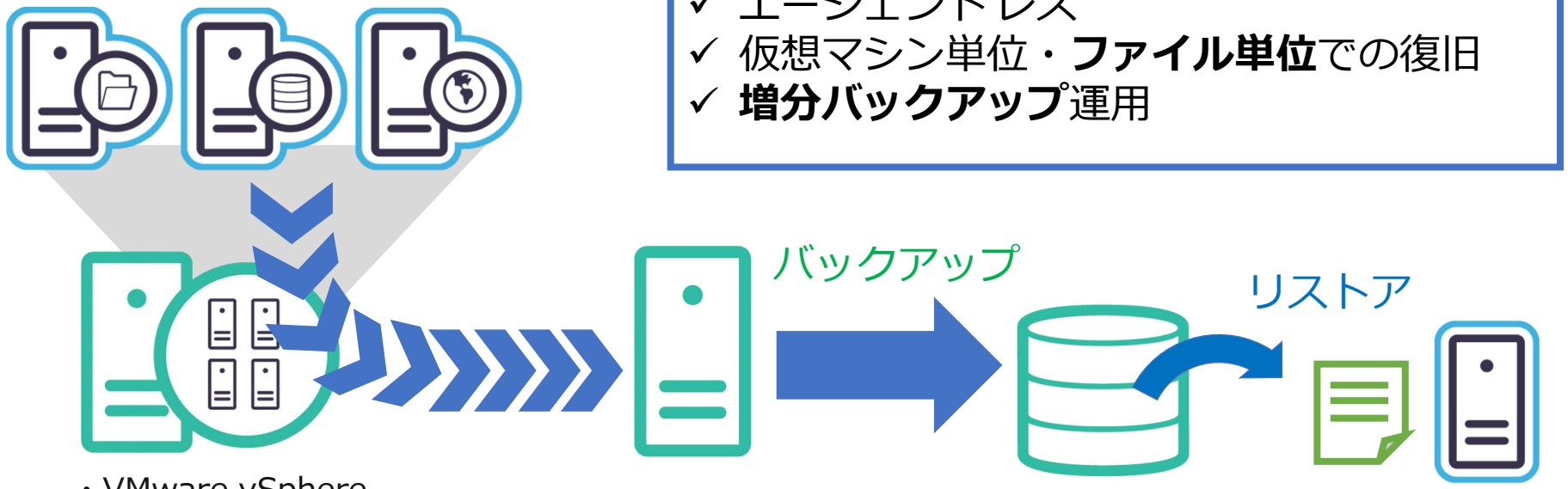
インターネットブラウザを使って
どこからでも簡単にアクセス可能

Arcserve UDP：仮想環境のエージェントレス バックアップ

VMware vSphere、Microsoft Hyper-V、Nutanix AHV の仮想マシンを **エージェント レス** でバックアップ

仮想保護の3大要件を同時に実現

- ✓ エージェントレス
- ✓ 仮想マシン単位・**ファイル単位**での復旧
- ✓ **増分バックアップ**運用



・VMware vSphere
・Microsoft Hyper-V
・Nutanix AHV

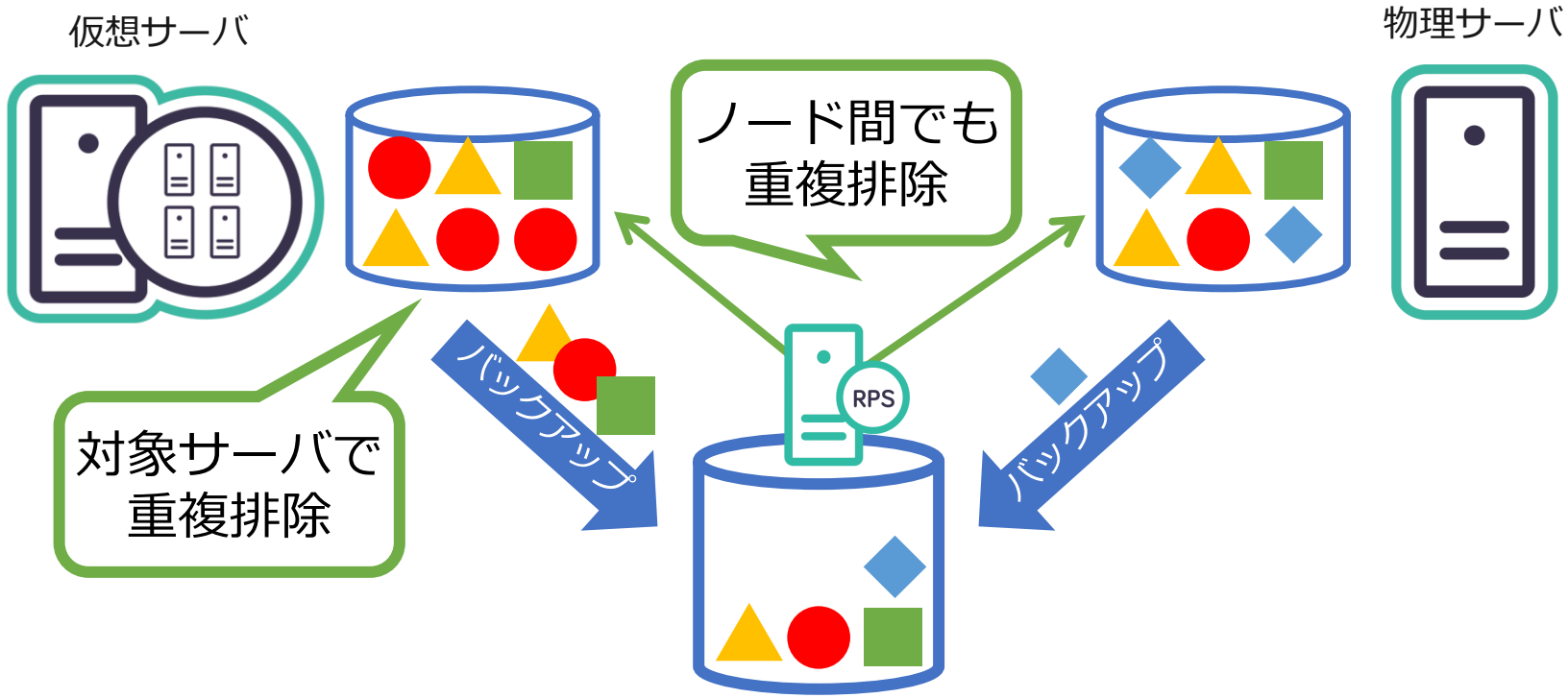
arcserve®

Arcseve UDP：RPS 利用でバックアップ データの重複排除が可能

こんな時に便利！

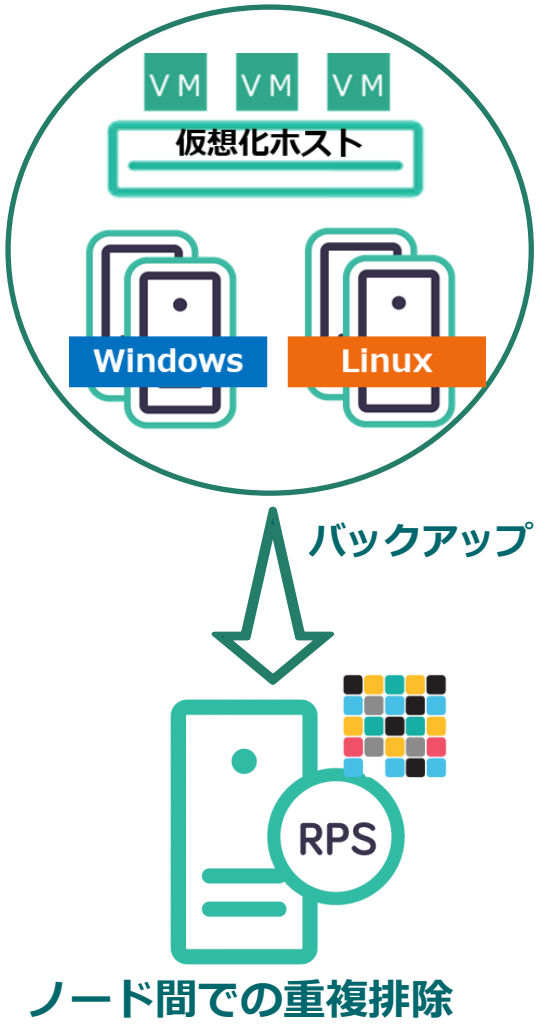
➔ バックアップデータ容量を少なく保存したい

➔ ネットワークに流れるデータ量を少なくしたい



ブロック増分バックアップ＋重複排除を利用して
更に少ない容量で多くの世代を保管できる

Arcserve UDP 重複排除事例



霧島ホールディングス株式会社 様

削減効果 **84.4 %**

270 GB
↓
42 GB

株式会社ドン・キホーテ 様

削減効果 **71.4 %**

7 TB
↓
2 TB

サンマテオ クレジット ユニオン 様

削減効果 **82 %**

25 TB
↓
4.5 TB

株式会社クレオ 様
(ご契約120社分の取得結果)

削減効果 **60 %**

18.3 TB
↓
7.3 TB
(削減効果から算出)

arcserve®

Arcserve UDP：バックアップデータの転送（レプリケート）

こんな時に便利！

➔ バックアップ データを**遠隔地に保管**しておきたい

➔ WANに流れるデータは**更に**少なくしたい

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

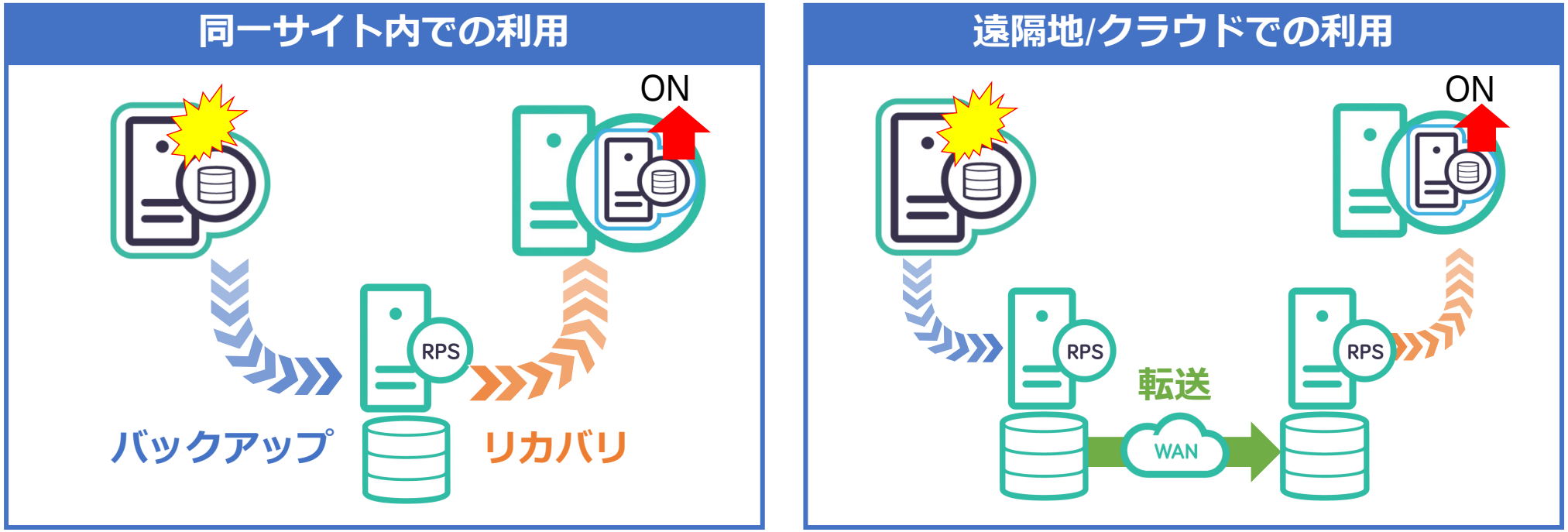
※ レプリケート先には復旧ポイントサーバ（RPS）が必要です。Arcserve UDP Cloud Hybrid には RPS がインストールされており、レプリケート先として利用することが出来ます。

Arcserve UDP：仮想スタンバイ サーバの自動作成

こんな時に便利！

➔ 障害時に**リカバリするよりも早く**環境を利用したい

➔ 災害時には遠隔地でサーバを**即時利用**したい



復旧済みの仮想マシンで素早く業務を再開

ローカル / 遠隔地でも構成できる

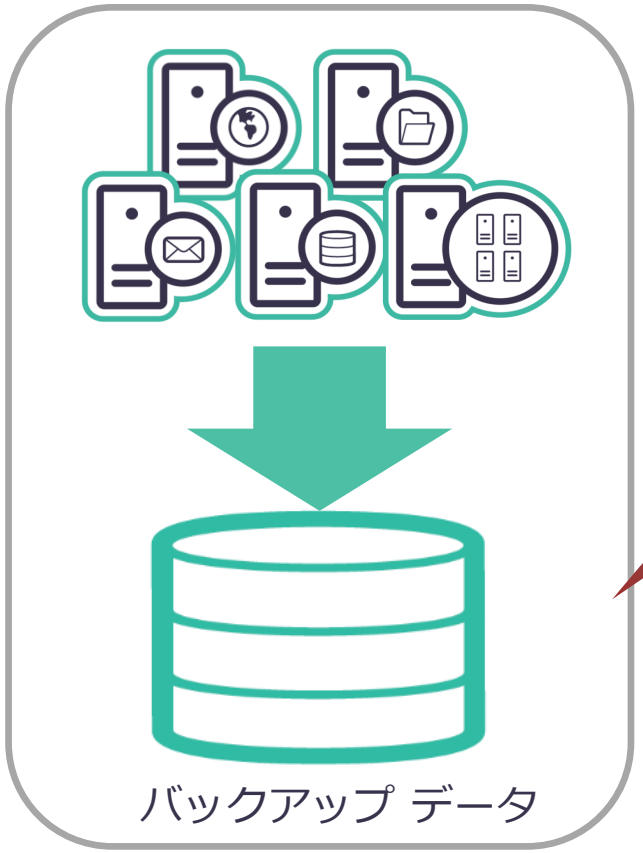
複数のスナップショットから適切な時点に戻せる

※ クラウド環境としてArcserve UDP Cloud Hybrid、AWS EC2、MS Azureをサポート

Arcserve UDP：インスタント VM

こんな時に便利！

➔ **代替環境をあらかじめ用意していない**場合でも直ぐに業務を再開したい
➔ ウイルスなどの被害時に**本番サーバの替わり**を用意したい



数ステップの
簡単なウィザードで
僅か10分ほどで起動

インスタントVM

復旧先の仮想環境
（vSphere / Hyper-V / AHV / AWS EC2 / MS Azure）※

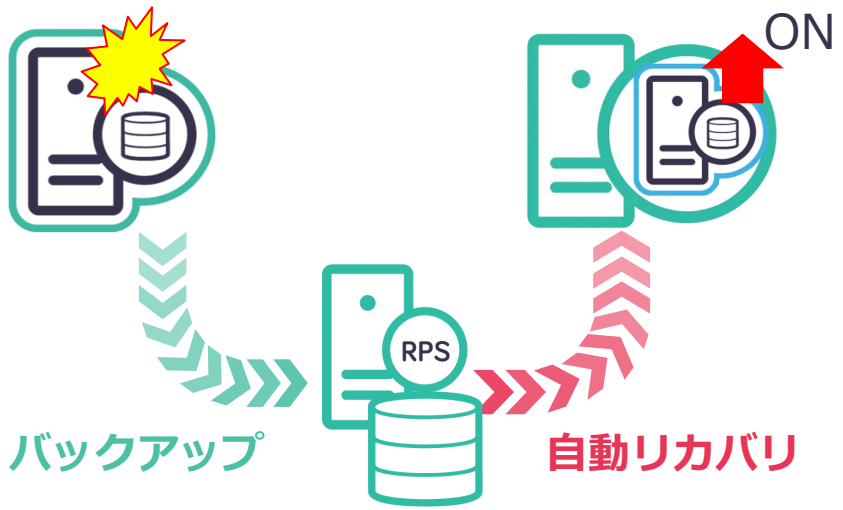
バックアップデータから直接サーバ起動

※Windows は vSphere, Hyper-V, Arcserve UDP Cloud Hybrid 環境のみ

Arcserve UDP：仮想スタンバイとインスタント VMとの違い

仮想スタンバイ

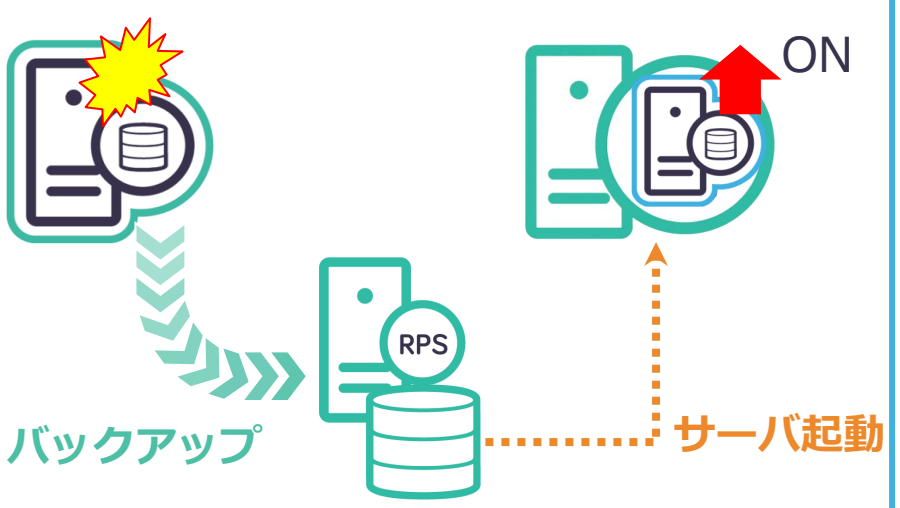
低遅延



- バックアップ時にリカバリまで実行済
- バックアップ データを参照しないVMを起動するので、遅延が少ない
- スタンバイVM分のディスクが必要
- Windows をサポート

インスタント VM

低コスト



- 事前準備が不要
- バックアップデータを参照するVMを起動
- VM 格納用のディスク領域は不要
- Windows & Linux をサポート
- バックアップ データの健全性確認に利用できるので、ランサムウェア対策にもお勧め

3. クライアント PC のデータ保護

～ Arcserve UDP Workstation Edition で実現する効率的なバックアップ環境

企業のクライアントバックアップに求められる要件

企業のクライアントＰＣバックアップのシステムでは、**運用台数が多い**事と**組織的取組**としてバックアップ環境の構築をする必要がある事から、**パソコン単体用のバックアップツールとは異なる機能要件**が求められます。

運用負荷が少ない	クライアントＰＣは台数が多いため、運用負荷が少なくて済むバックアップ環境が必要
一元管理が可能	クライアントＰＣは台数が多いため、一元的に効率よく管理が出来るバックアップ環境が必要
バックアップポリシーに基づいた運用が可能	企業として求められるバックアップポリシーに基づくバックアップ運用が実現可能な環境が必要
バックアップが効率的	クライアントＰＣの業務生産性を損なわず、また、バックアップ先のディスク容量を効率的に利用できるなどの環境が必要

企業のクライアントバックアップに求められる要件

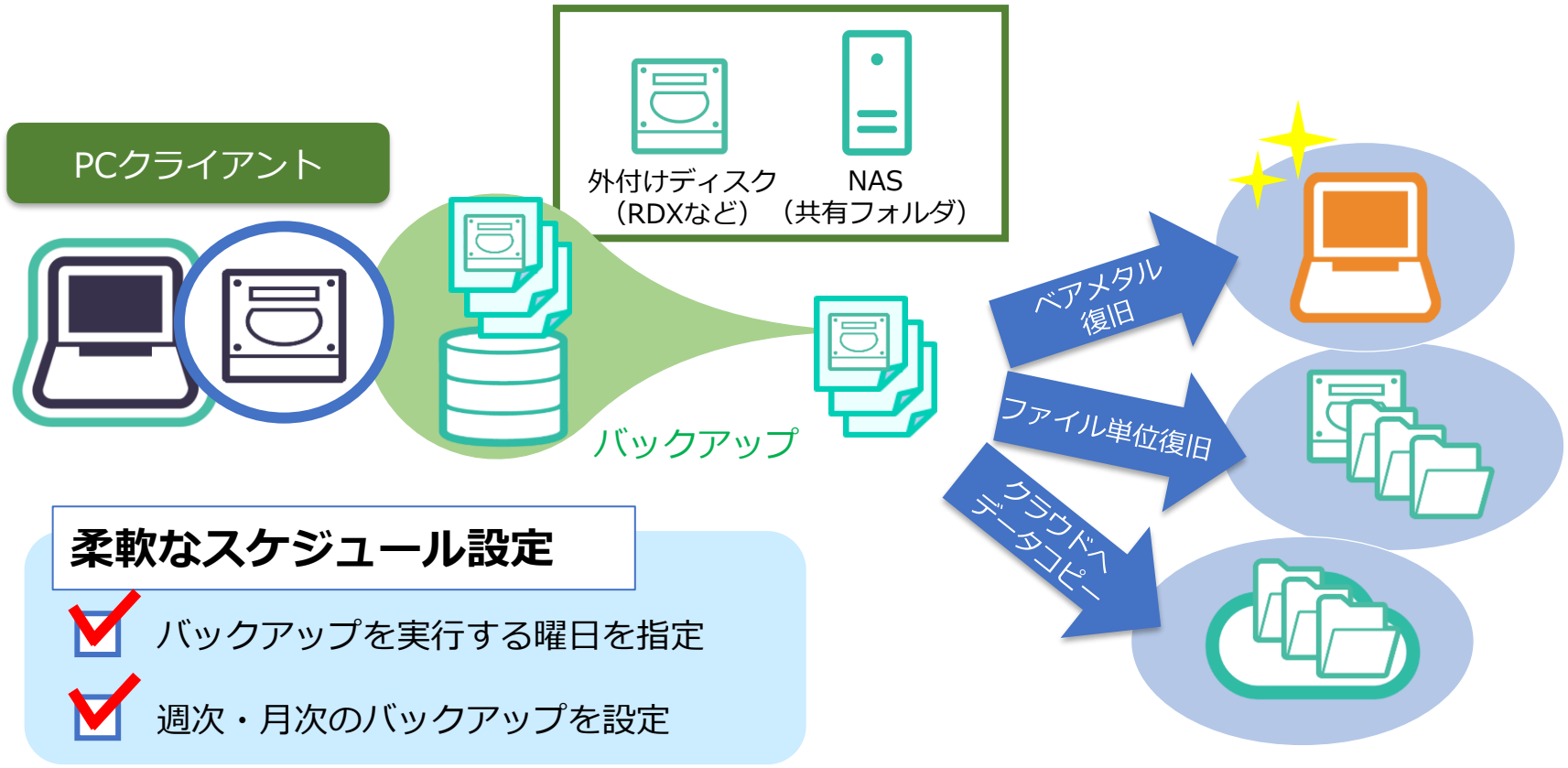
企業のクライアントＰＣバックアップのシステムでは、**運用台数が多い**事と**組織的取組**としてバックアップ環境の構築をする必要がある事から、**パソコン単体用のバックアップツールとは異なる機能要件**が求められます。

- **運用負荷が少ない**
- **一元管理が可能**
- **バックアップポリシーに基づいた運用が可能**
- **バックアップが効率的**

Arcserve UDP Workstation Edition

Arcserve UDP の自立型エージェント

Arcserve UDP のエージェントはバックアップ サーバが無くてもエージェント単体でバックアップ／リストアが実施できる「**自立型エージェント**」。
PCクライアントを手間なく簡単にバックアップ・リカバリ運用したいというニーズに応えます。

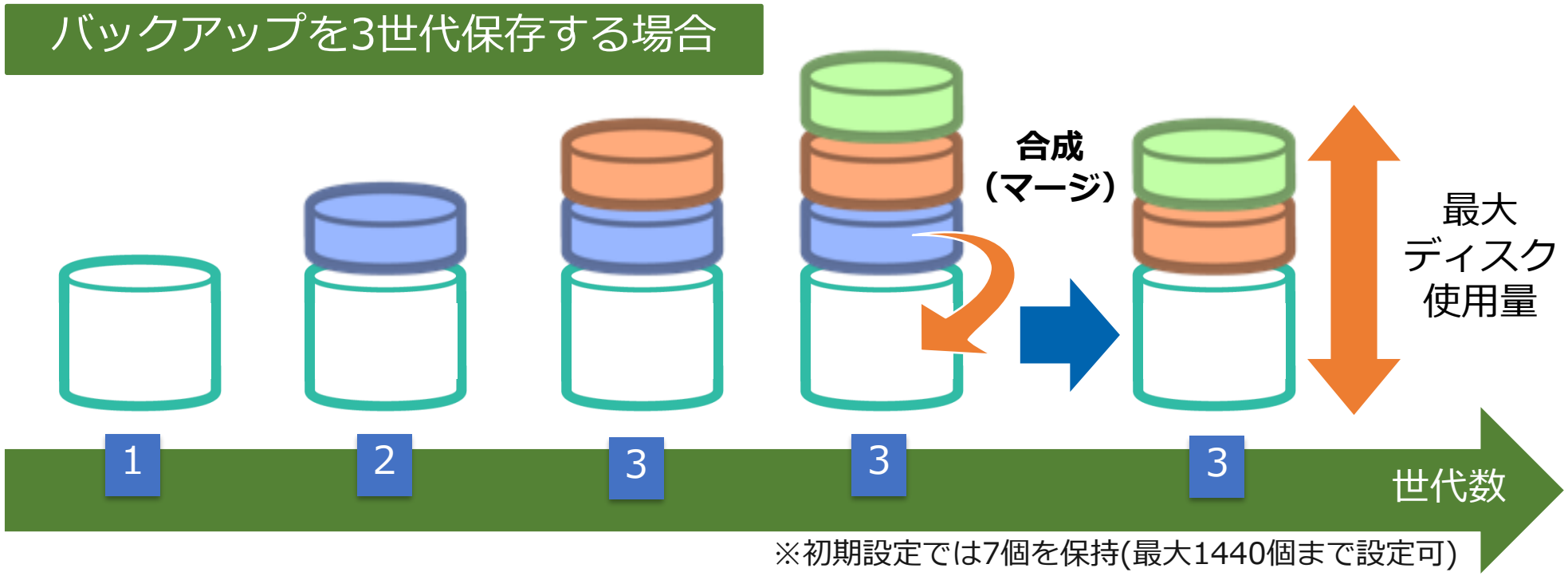


Arcserve UDP：継続的な増分バックアップで利用者の負担を軽減

バックアップ データの自動メンテナンス機能

フル バックアップは初回のみでOK！

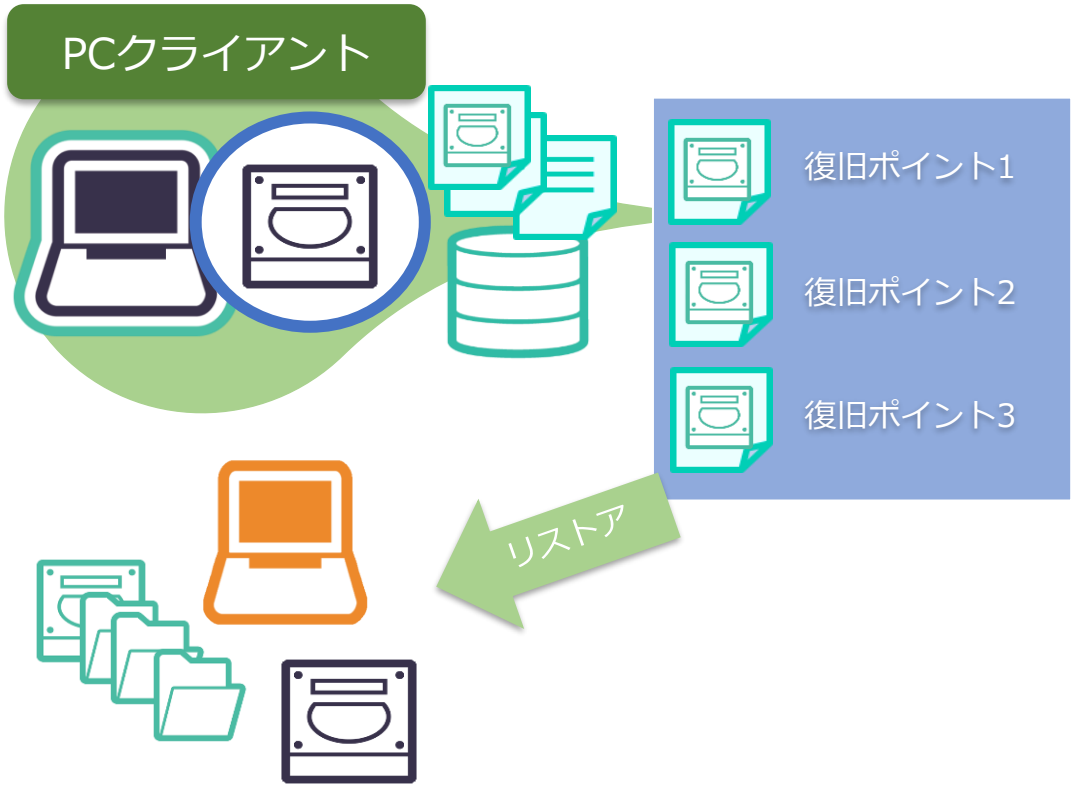
バックアップの世代数が設定された数(※)を超えた場合、最も古い増分データとフル バックアップを合成（マージ）させ、フル バックアップの世代を更新。毎回増分バックアップなので**バックアップの処理時間が短く、PC利用者の業務に大きな負担をかけません。**



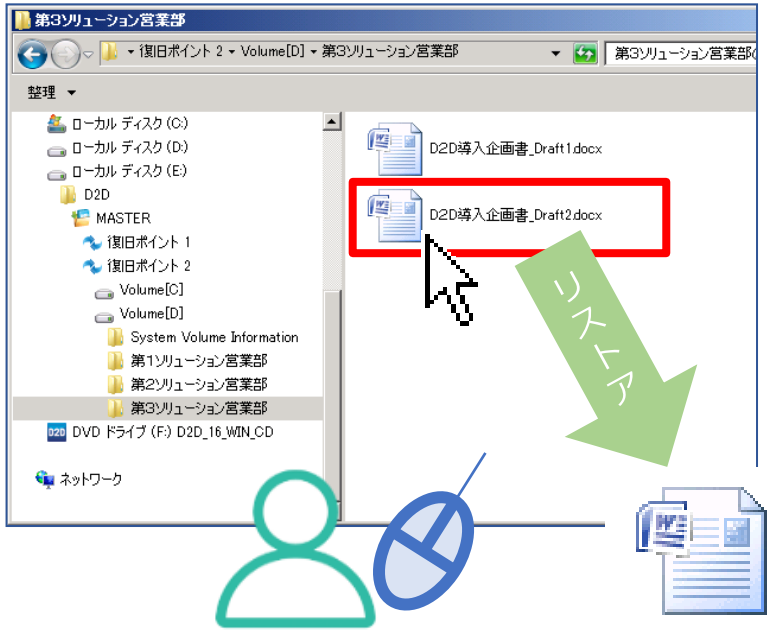
Arcserve UDP なら簡単操作でファイル単位のリストア”も”可能

Q: イメージバックアップだとシステム全体しか戻せないの？

A: Arcserve UDP ではシステム全体もファイル個別にもリストアが可能です。
使い慣れたエクスプローラからドラッグ＆ドロップで簡単にリストアすることもできます。



ドラッグ＆ドロップでファイル単位のリストア

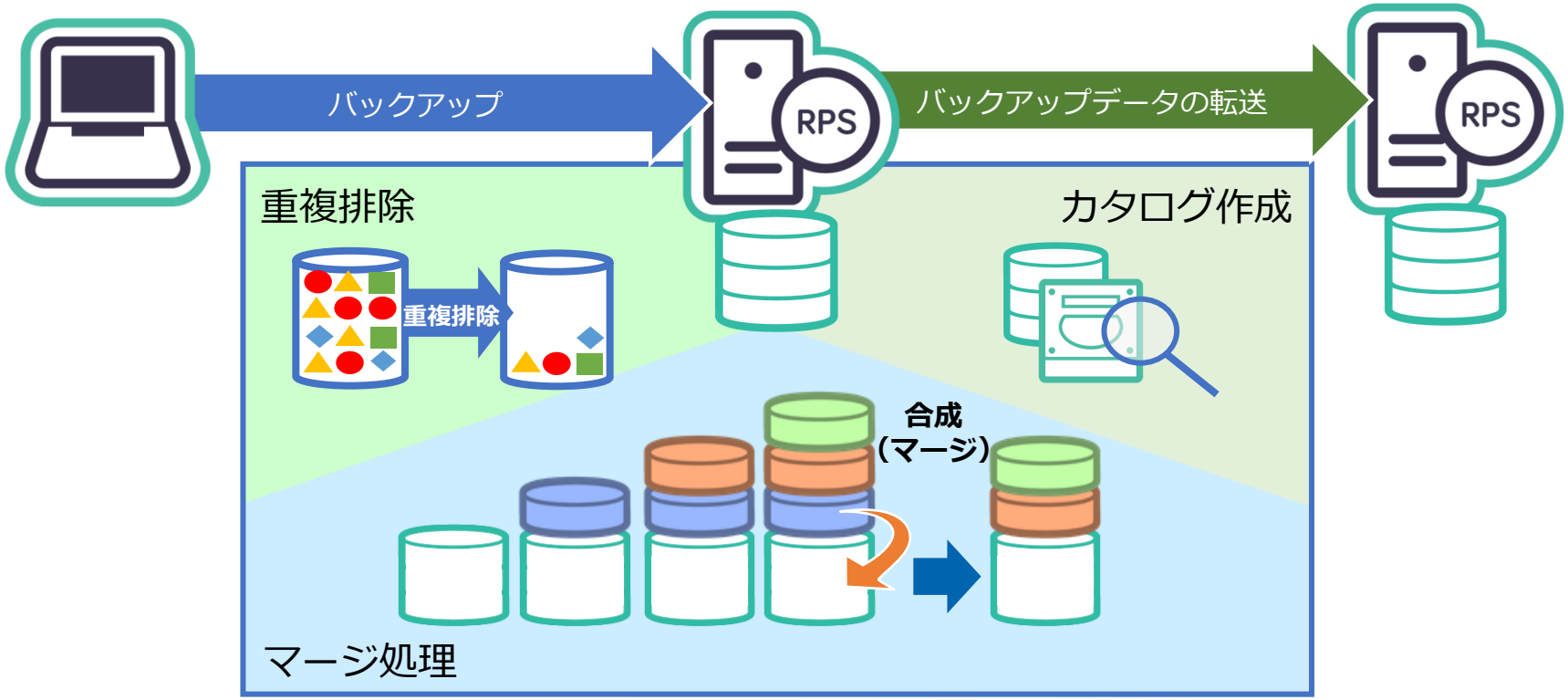


※エクスプローラからのリストアには管理者権限が必要です

Arcserve UDP 復旧ポイントサーバ（RPS）

復旧ポイントサーバ　Recovery Point Server (RPS)

Arcserve UDP エージェントから送られてくるバックアップデータの保管および管理サーバ。
重複排除、マージ・カタログ作成の代行、復旧ポイントの複製を行う際に利用できます。更にRPS間でバックアップデータの転送が可能、災害対策にも有効です。



Arcserve UDP 統合管理 コンソール

Arcserve UDP コンソール

効果

一元管理で、バックアップ環境を見える化
リモートインストールで、導入作業の負担を軽減

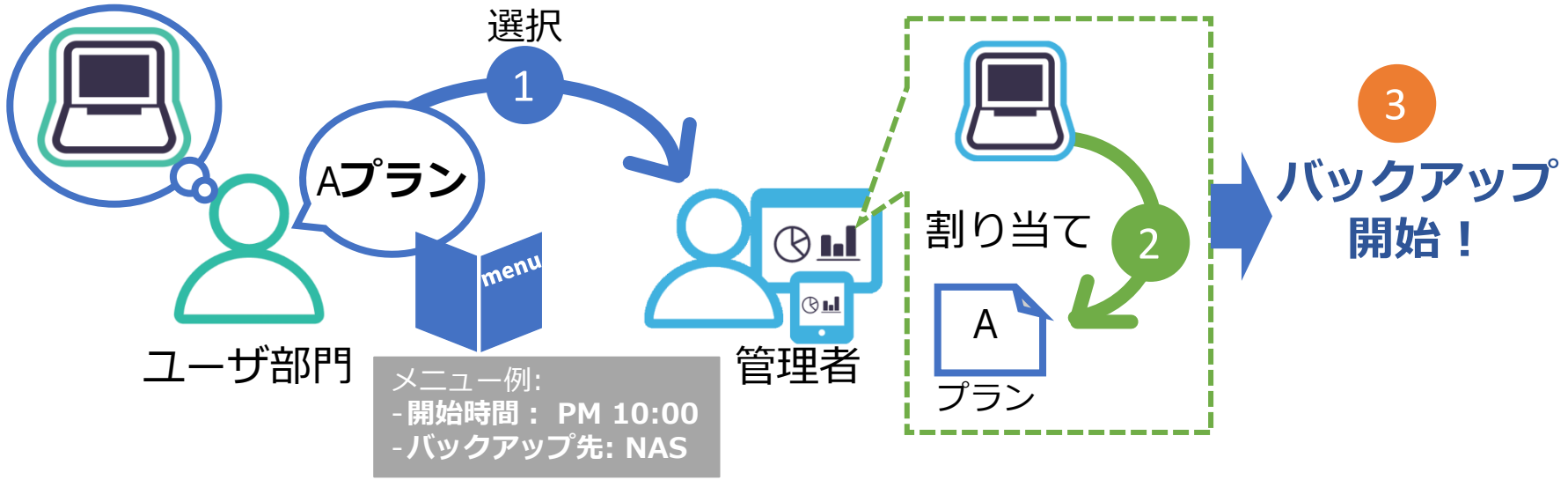
台数の多いクライアントPCのバックアップ状況を統合管理サーバで**一元的に管理**できます。
また、新しく接続されたPCはリモートインストールで現地へ行かずに設定作業が可能で
導入作業の負担が軽減されます。

Arcserve UDP 統合管理 コンソール

ブラウザ画面から**バックアップの状況確認、バックアッププランの追加・配布、レポートの確認**
などの操作を行うことができます。
台数の多いクライアントPCも統合管理画面で**一元的に管理**が可能です。

Arcserve UDPでできる、プランを使ったメニュー化のメリット

あらかじめバックアップの**「プラン」**を設定し、対象クライアントに割り当てる設定方法。バックアップの**メニュー化**と**設定の簡略化**が出来ます。



ユーザ部門：
重要度、業務運用などに合わせプランを**選択**

統合基盤管理者：
対象クライアントをプランに**割り当てる**だけでバックアップが開始

複数のPCクライアントをまとめて簡単に設定可能!!

4. バックアップ アプライアンス

～ Arcserve UDP の簡単導入
Arcserve UDP 9000 シリーズのご紹介

Arcserve UDP Appliance 9000 シリーズとは？

Arcserve UDP をプリインストールしたバックアップ専用アプライアンス。
中規模環境のバックアップをより**簡単**に、**シンプル**にします。

従来モデルの 8000 シリーズから CPU、メモリ、SSD を新世代のものに更新するとともに、
オンボードのネットワークを 10GBase-T ×2ポートに強化しています。

Arcserve UDP Appliance 9000 シリーズ ここがすごい！

1、インストール不要の簡単セットアップ

バックアップ/リカバリに必要な管理コンポーネントはすべてインストール済。ウィザードに従い基本的な設定をするだけで**すぐに使えます**。

2、バックアップ用に最適化されたハードウェア

重複排除機能用のSSDを標準搭載。**メモリ/SSDのサイジングが必要ありません**。
バックアップ先の容量を 4TB ～ 80TB の間で選ぶだけ！

3、Arcserve UDP のライセンスを使い放題

バックアップ対象の数や容量に関わらず、Arcserve UDP Advanced Edition のライセンスが使い放題。後から**サーバ台数が増えても安心**です。

arcserve®

Arcserve UDP 9000 シリーズのメンテナンス内容と価格例

サポート窓口

Arcserveテクニカルサポート
（ソフトウェア版と同じ窓口）

メンテナンス期間

納品から**5年間**の
メンテナンスが標準セット

サポート対応

・Arcserveテクニカルサポートにて窓口対応。
・ハードウェア故障は**オンサイト**（現地訪問）対応が可能
（部品交換が必要な場合、現地訪問は問題特定から4時間駆けつけ目標（※））
・Arcserve UDPの**無償アップグレード**が可能
（アップグレード作業はお客様にて実施いただきます）

※　サービス拠点(札幌、仙台、東京、名古屋、大阪、広島、福岡)より30km圏内での目標となります。

Arcserve UDP 9200（12TB）

合計：3,800,000円 (税抜)

Arcserve UDP 9000 シリーズの拡張性：ストレージ/テープへの接続

イーサネット、SAS、FC などのカードを増設できます。

ランサムウェア対策としてオフライン保管が可能な**テープ デバイス**への二次バックアップが可能になります。

[Arcserve UDP 9000 シリーズ背面パネル]

※　増設カードはオプションとして購入する必要があります。

※　1Uモデルは最大2つ、2Uモデルは最大6つ増設できます。

Arcserve UDP 9000 シリーズの拡張性：ソフトウェア アップグレード

Arcserve UDP 9000 シリーズの標準機能（Advanced Edition）を強化し、
Premium / Premium Plus Edition の機能が使用できるようになるオプションもあります。

Edition 別機能一覧	Advanced / Advanced(AHV)	Premium	Premium Plus	利用できる製品
イメージ バックアップ / 共有フォルダ (CIFS/NFS ※1) のバックアップ	●	●	●	Arcserve UDP
バックアップ データの重複排除や転送（レプリケート）	●	●	●	
統合管理	●	●	●	
仮想マシンのエージェントレス バックアップ（vSphere/Hyper-V/AHV ※1）	●	●	●	
仮想スタンバイ/インスタントVM	●	●	●	
バックアップ データのテープ保管（D2D2T）	●	●	●	
VSS ライタを利用したアプリケーションのオンライン バックアップ	●	●	●	
アシュアードリカバリとSLAレポート		●	●	
役割ベースの管理		●	●	
ハードウェアスナップショット対応（NetApp/Nimble/3PAR/DellEMC Unity）		●	●	
Arcserve Backup すべての機能/全エージェント/全オプションの利用 ※2		●	●	Arcserve Backup
Arcserve Replication ファイル サーバのデータ複製		●	●	Arcserve Replication/HA
Arcserve Replication アプリケーション サーバのデータ複製			●	
Arcserve High Availability ファイル / アプリケーション サーバの自動切替			●	

※1：購入時に申請いただく事で、AHV 上の仮想マシンまたは Nutanix Files のバックアップを行うための Advanced Edition for Nutanix ライセンスを提供いたします。
※2：「すべての機能/全エージェント/全オプション」とは、日本語の動作要件に記載されている製品（機能）が対象です。

arcserve®

5. イミュータブル（不変）ストレージ

～ Arcserve OneXafe 4500 シリーズのご紹介

イミュータブル（不変）ストレージ Arcserve OneXafe とは？

Immutable：不変の、変わらない

Arcserve OneXafe は SMB/NFS 共有を提供するバックアップ専用 NAS（※）です。バック グラウンドで定期的に”不変な”スナップショットを取得します。

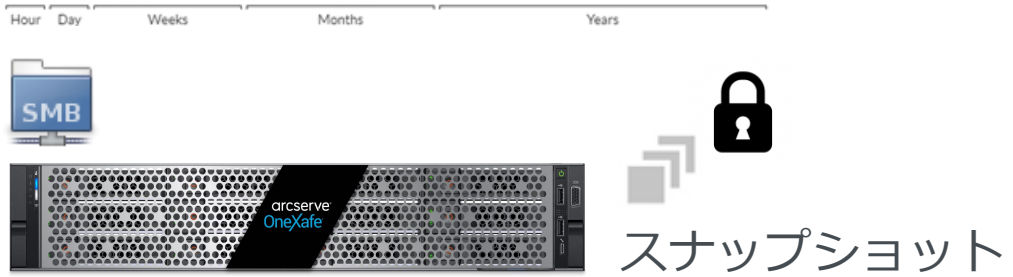
ランサムウェアや不正アクセスによりデータに改ざんや削除があっても、
スナップショットを使って正常時の状態に復旧できます。

※ Arcserve UDP または Arcserve Backup のバックアップデータの保存先として利用する事をサポートします。

バックアップ データが破壊される前の状態に簡単に復旧

1 バックアップ データが共有領域に書き込まれます。

2 OneXafeは90秒おきにスナップショットを取得します。



3 ランサムウェアや攻撃者は、”不変な”スナップショットを変更することはできません。

4 スナップショットにより、バックアップデータが破壊される前の状態に復旧できます。

Arcserve OneXafe の特長

・**堅牢性の確保**
- 自動的に変更不可のスナップショットを取得
  ※直近の1時間については90秒ごと、それより古いデータは1時間ごと、1日ごと、1週間ごとに
  スナップショットを保持。
- 3つのディスクへ自動的にデータ ブロック冗長化し、ディスク障害に対応

・**ストレージの効率利用**
- 重複排除、圧縮

・**容易な管理**
- クラウド ベースでどこからでも管理

加えて・・
・**定評ある Arcserve サポートが利用可能に**
・**使いやすい日本語の技術資料を提供予定**

arcserve®

利用ケース

ランサムウェア対策のため二次バックアップ先を複数案検討した結果、Arcserve OneXafe が採用されました。

不採用

案1：クラウド
ストレージにコピー

✕ インターネット回線に対してバックアップデータが大きく、既定の時間でコピーが終わらない。

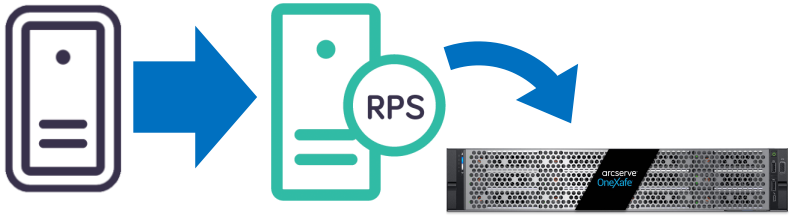
不採用

案2：テープに
二次バックアップ

✕ テープを定期的にトラブルなく交換できる人材がいない。

採用！

案3：OneXafe に
二次バックアップ



○ OneXafe なら LAN 内に設置できるので、大容量もOK！

○ OneXafe ならテープ交換のような定期的な作業は不要！

arcserve®

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. Arcserve may make improvements in or changes to the content described in this document at any time.