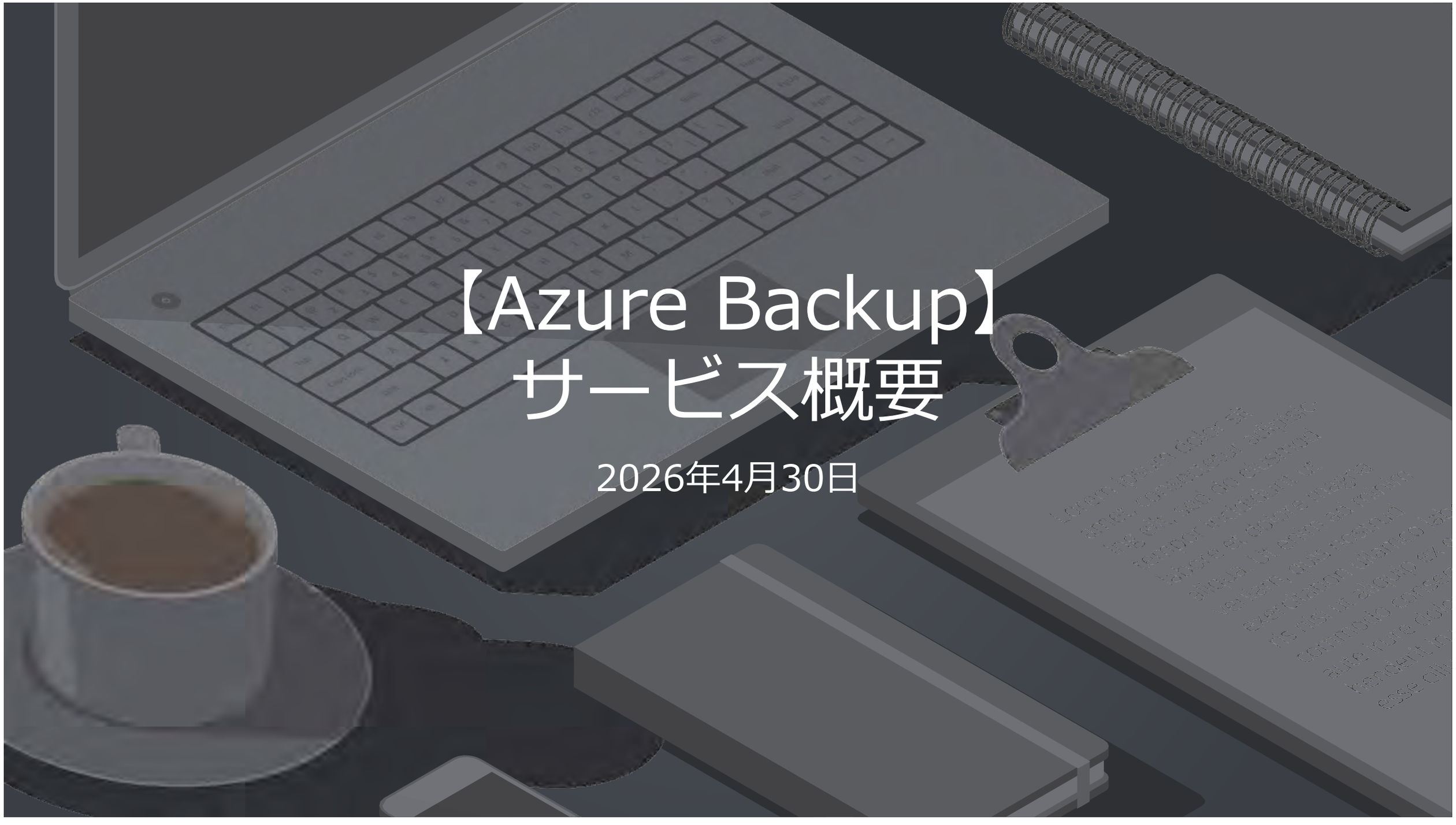


【Azure Backup】サービス概要

2026年4月30日

改訂履歴

版数	発行日	改訂内容
第1版	2026年4月30日	初版発行

本資料の内容は 2026/4/30 時点のものです。製品のアップデートにより変更となる場合がございます旨ご了承ください。

Agenda

1. 前提情報
    1. 用語集
2. バックアップ取得の背景
    1. バックアップの重要性
3. Azure Backup とは
    1. Azure Backup の概要
    2. 対象ワークロード
    3. Azure Backup 利用の流れ
4. Azure Backup の仕組み
    1. バックアップ方式
    2. 実装方式
    3. 整合性モデル
    4. 復元の考え方
5. 利用メリットと注意点
    1. 利用メリットと注意点
6. 活用シナリオ
    1. シナリオ①：Azure IaaS を中心とした標準バックアップ
    2. シナリオ②：セキュリティ対策を意識したバックアップ
    3. シナリオ③：ハイブリッド環境でのバックアップ
7. Azure Backup の料金
    1. 課金形態

1. 前提情報

1.1. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
1	Azure	Microsoft が提供するクラウドプラットフォーム。仮想マシン、ストレージ、ネットワーク、データベースなどの各種クラウドサービスを提供する。
2	Microsoft Entra ID	Microsoft が提供するクラウドベースの ID・認証管理サービス。ユーザー認証、アクセス制御、MFA などを提供する。
3	Azure Backup	Microsoft が提供する、Azure の標準バックアップサービス。Azure VM や Azure Files、オンプレミス環境の一部ワークロードに対して、バックアップと復元を提供する。
4	Recovery Services コンテナー	Azure Backup における管理単位。バックアップ対象、バックアップポリシー、復旧ポイントを論理的に管理するための専用リソース。
5	バックアップポリシー	バックアップの取得頻度や実行時刻、保持期間などの運用ルールを定義する設定。Recovery Services コンテナー単位で管理される。
6	Azure VM	Azure 上で提供される仮想マシン（IaaS）。Azure Backup の主要なバックアップ対象の一つ。
7	Azure ポータル	Azure サービスの管理を行うための Web ベースの管理画面。 リソースの作成・設定・監視・課金確認などを一元的に操作できる。
8	Azure Files	Azure 上で提供されるファイル共有サービス。Azure Backup ではサービス直接連携によりバックアップされる。
9	RBAC（Role Based Access Control）	役割（ロール）に基づいてアクセス権限を制御する仕組み。 Azure では、ユーザーやサービスに対して操作可能な範囲を細かく制御できる。
10	VM 拡張機能	Azure VM に追加される機能コンポーネント。Azure Backup では、VM のバックアップ実行時に拡張機能を通じてデータ取得が行われる。

1.1. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
11	MARS（Azure Backup エージェント）	オンプレミスサーバーに直接インストールして使用する Azure Backup のエージェント。主にファイル／フォルダー単位のバックアップに利用される。
12	MABS（Azure Backup Server）	オンプレミス環境に構築するバックアップ専用サーバー。複数サーバーやワークロードを集中的にバックアップできる。
13	BCP（Business Continuity Plan）	災害や障害が発生した際にも、事業を継続または早期復旧するための計画。
14	DR（Disaster Recovery）	災害や大規模障害発生時に、システムやサービスを復旧・継続させるための対策や仕組み。
15	ポイントインタイムリストア	データベースなどのサービスにおいて、特定の過去時点を指定してその時点のデータ状態に復元する機能。 Azure SQL Database などの PaaS サービスでは、このポイントインタイムリストア機能がサービスに標準で組み込まれている。
16	Azure Site Recovery	Azure 上で提供される DR サービス。システムの継続稼働や迅速な切り替えが必要な場合に利用される。
17	本番環境 / 検証環境	業務システムが実際に利用されている環境を本番環境、検証やテスト目的で使用される環境を検証環境と呼ぶ。
18	ランサムウェア	データを暗号化・破壊し、復旧と引き換えに金銭を要求するマルウェアの一種。
19	SQL Server	Microsoft が提供するリレーショナルデータベース製品。オンプレミスや Azure VM 上で利用される。
20	MFA（多要素認証）	ID とパスワードに加え、追加の認証要素を要求する認証方式。管理者アカウントの保護に使用される。
21	クラウドネイティブ	クラウド環境での利用を前提に設計・提供されるサービスやアーキテクチャの考え方。 インフラの構築や保守をユーザーが行う必要がなく、スケーラビリティ、自動化、可用性、セキュリティといったクラウドの特性を活かして利用できる点が特徴。

1.1. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
22	SAP HANA	SAP（ドイツのソフトウェア企業）が提供するインメモリ型データベース。大規模業務システムや基幹システムで利用されることが多く、高速なデータ処理やリアルタイム分析に強みを持つ。
23	Azure SQL Database	Microsoft Azure が提供する PaaS 型のリレーショナルデータベースサービス。Azure Backup の直接的なバックアップ対象ではない。
24	Exchange Online / OneDrive / SharePoint Online	Microsoft 365 で提供される SaaS 型サービス。メール、ファイル保存、チーム共有などを提供する。Azure Backup の対象外。
25	保持ポリシー（Microsoft 365）	Microsoft 365 上のデータを削除・変更させない、または一定期間後に削除するためのデータ保持ルール。 コンプライアンスや情報統制を目的とした機能であり、バックアップとは仕組みや目的が異なる。
26	NAS（Network Attached Storage）	ネットワーク経由で利用される専用ストレージ装置。通常、Azure Backup の直接対象外。
27	ストレージアプライアンス	専用用途向けに提供されるストレージ機器。OS やエージェントを導入できないものは Azure Backup の対象外となる。
28	VMware / Hyper-V	オンプレミス環境で利用される仮想化基盤ソフトウェア。Azure Backup は仮想基盤そのものを直接バックアップする機能は持たない。
29	リージョン	クラウドサービスが提供される地理的な拠点。Azure Backup の Recovery Services コンテナーは特定リージョンに紐づいて作成される。
30	RPO（Recovery Point Objective）	許容されるデータ損失の最大時間。どの時点までデータを戻せる必要があるかを示す指標。
31	ハイブリッド環境	オンプレミス環境とクラウド環境（Azure など）が併存して利用されている構成。

1.1. 用語集

本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
32	Azure Storage	Azure が提供するクラウドストレージサービスの総称。Blob、File、Queue などのサービスを含む。
33	Azure Storage Account	ユーザーが作成・管理する Azure Storage の論理単位。Azure Backup のバックアップデータ保存先とは異なる。
34	ネットワーク帯域	ネットワークで単位時間あたりに転送可能なデータ量。バックアップや復元の実行時間に影響する。
35	記憶領域	データを保存するための容量。バックアップデータ量は保持期間や変更量に応じて増減する。
36	Azure 管理プレーン	Azure リソースの作成・設定・管理といった制御を行う管理基盤。バックアップの設定や制御は管理プレーン経由で行われる。
37	スナップショット	ある時点のデータ状態を別で保持する仕組み。Azure Files のバックアップなどで利用される。
38	ワークロード	業務システムやアプリケーション、データベースなど、クラウドやサーバー上で処理される単位。
39	フォールバック	本来想定していた処理や状態が取得できなかった場合に、代替手段に切り替えること。Azure Backup では整合性モデルで用いられる。
40	コンテナーロック	Azure のリソースロック機能。Recovery Services コンテナーに設定することで、削除や変更を防止できる。
41	Soft Delete	バックアップデータが削除された場合でも、一定期間は完全に消去せず、復元できる状態で保持する仕組み。Azure Backup では、誤操作や不正操作によるバックアップデータの即時削除を防ぐために利用される。

1.1. 用語集

本書で使用する用語及び略称を以下の通り定義します。

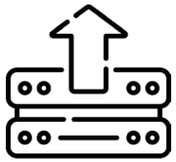
No.	用語	説明
42	IaaS PaaS SaaS	IaaS（Infrastructure as a Service）： 仮想マシンやネットワークなどのインフラをクラウド上で提供するサービス形態。 OS やミドルウェア、アプリケーション、バックアップの設計・運用はユーザー側で行う。 PaaS（Platform as a Service）： OS やミドルウェアをクラウド側で管理し、アプリケーションの開発・実行に集中できるサービス形態。 バックアップや復元などの運用機能は、サービス側に標準で組み込まれている場合がある。 SaaS（Software as a Service）： アプリケーションをクラウドサービスとして提供する形態。 インフラや OS、ミドルウェア、アプリケーション、データ管理までをサービス提供側が担い、ユーザーは機能を利用することに専念できる。

2. バックアップ取得の背景

2.1. バックアップの重要性

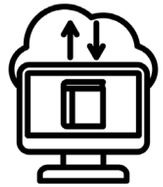
企業システムでは、障害や災害、人的ミスなど、予期せぬ事象によるデータ消失リスクが常に存在します。このようなリスクに備える手段として、過去の状態にデータを復旧できるバックアップは従来から不可欠な基本対策として位置づけられてきました。
近年はシステムのクラウド化が進む中で、クラウド環境の特性を踏まえたバックアップ手段の選択が重要なポイントとなっています。

クラウドを活用したバックアップ設計が求められる背景



オンプレミス環境における
バックアップ運用の限界

従来のオンプレミス環境では、バックアップ用のサーバーやストレージを自社で用意・運用するケースが一般的でした。
そのため、**初期コストや保守・運用負荷が高く、データ量の増加に対する柔軟な拡張が難しい**という課題があります。
また、災害や障害が発生した場合に**本番環境と同一拠点に配置されたバックアップデータ自体が失われるリスク**も考慮する必要があります。



BCP / DR 観点での備えの強化

事業継続計画（BCP）や災害復旧（DR）の観点からは、障害発生時でも業務を継続、または速やかに復旧できる体制が求められます。
そのためには、**データを本番環境とは物理的に離れた場所で安全に管理することが重要**です。
オンプレミス環境でこれを実現しようとすると、遠隔地拠点の構築や運用に大きなコストと手間がかかります。このような背景から、**クラウドを活用したバックアップ手段が現実的な選択肢**として検討されるようになっています。

ランサムウェア被害の増加

近年、企業システムを標的としたランサムウェア被害が増加しており、データの暗号化や削除によって業務停止に至る事例も発生しています。
こうしたサイバー攻撃は、本番データだけでなく、**同一環境や同一権限配下にあるバックアップデータにも影響を及ぼす可能性**があります。
そのため、**バックアップを取っているだけでは不十分**であり、**攻撃対象から切り離された形でバックアップを確保すること**が、重要な対策の一つとなっています。

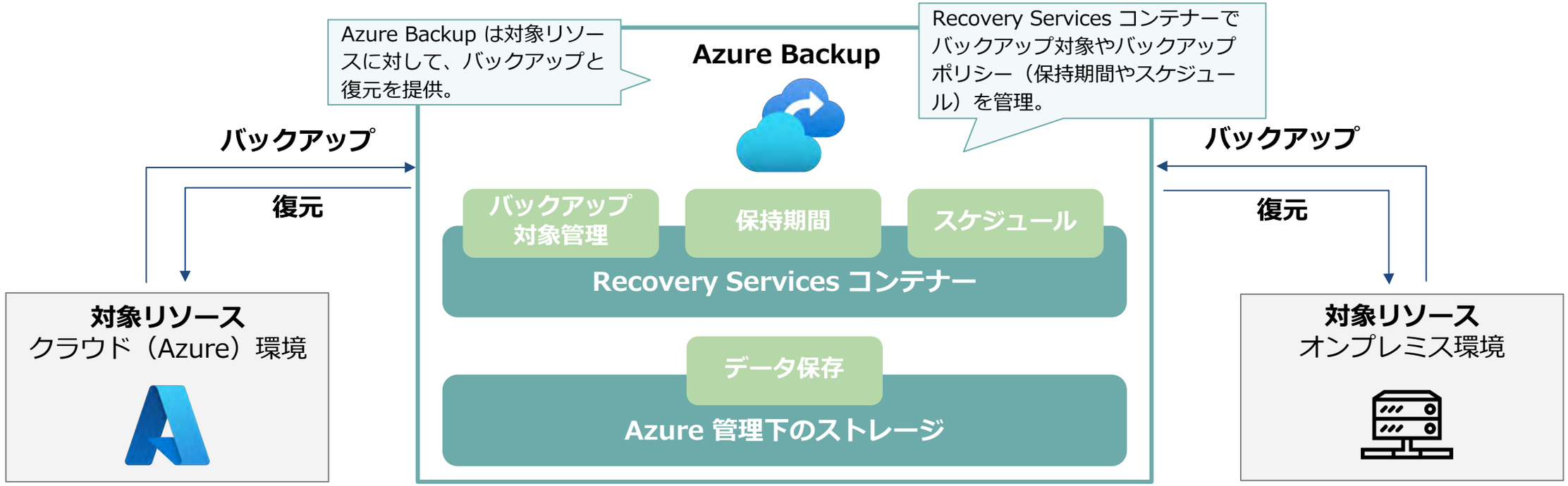
3. Azure Backup とは

3.1. Azure Backup の概要

Azure Backup は、Microsoft が提供するクラウドネイティブなバックアップサービスです。
Azure 上で稼働する仮想マシン（VM）やファイルサービス、さらにオンプレミス環境の一部ワークロードを対象に、Azure が管理するバックアップ基盤上でバックアップと復元を提供します。

Azure Backup の概要

Azure Backup では、Recovery Services コンテナーと呼ばれる専用リソースを中心にバックアップを構成します。
Recovery Services コンテナーを管理単位としてバックアップを管理し、実際のバックアップデータは Microsoft によって管理される Azure 管理下のストレージに保存されるため、本番環境から直接アクセスされにくく誤操作や攻撃の影響を受けにくい構成となっています。



3.2. 対象ワークロード

Azure Backup は、Azure 環境における主に IaaS ワークロード（Azure VM、Azure VM 上で稼働するアプリケーション、Azure Files） 、およびオンプレミス環境の一部ワークロードを対象にバックアップを提供します。
Azure 上のすべてのサービスがバックアップ対象となるわけではないため、対象外のサービスについては各サービスに適したバックアップ手段を別途検討する必要があります。

バックアップ可能な主なワークロード

■ Azure VM

Azure Backup は、**Azure 上で稼働する仮想マシン（Azure VM）をバックアップ対象としています。**
OS ディスクやデータディスクを含めた仮想マシン全体を保護でき、障害内容に応じてファイル単位での復元も可能です。
Azure 環境における基本的なバックアップ手段として、最も利用されるワークロードの一つです。

■ Azure VM 上で稼働するアプリケーション

Azure VM 上で稼働するアプリケーション（SQL Server や SAP HANA など）については、**仮想マシンのバックアップを通じて保護されます。**
アプリケーションの種類や構成に応じてアプリケーション整合性を考慮したバックアップが可能であり、業務アプリケーションを仮想マシン上で運用している場合でも Azure Backup を利用したデータ保護が可能です。

■ Azure Files

Azure Files 上のファイル共有をバックアップすることができます。**ファイル共有単位でのバックアップおよび復元が可能**で、誤って削除されたファイルの復旧や、特定時点の状態への復元に利用できます。

■ オンプレミス環境（MARS / MABS）

Azure Backup エージェント（MARS）や Azure Backup Server（MABS）を利用することで、**オンプレミス環境の一部ワークロード（サーバー上のファイルやアプリケーションデータ）を Azure にバックアップすることが可能です。**

3.2. 対象ワークロード

対象外となる主なワークロード

■ **PaaS サービス**

Azure SQL Database などの PaaS サービスは、Azure Backup を利用して直接バックアップを取得することはできません。
これらのサービスでは、可用性や復旧を含めた設計があらかじめ組み込まれており、自動バックアップやポイントインタイムリストアなどの機能がサービス標準として提供されています。
そのため、**PaaS サービスでは Azure Backup ではなく、各サービスが提供するバックアップ・復元機能を前提にデータ保護を検討する必要があります。**

■ **SaaS サービス**

Microsoft 365 などの SaaS サービスは、Azure Backup を利用して直接バックアップを取得することはできません。
代表的な Exchange Online、OneDrive、SharePoint Online などのデータも同様に、Azure Backup の対象外です。
Microsoft 365 では、ゴミ箱や保持ポリシーといったデータ保護機能がサービス標準として提供されていますが、これらはバックアップとは異なる仕組みです。
そのため、Microsoft 365 などの **SaaS サービスでは Azure Backup ではなく、専用のバックアップ手段を別途検討する必要があります。**

■ **オンプレミス環境における対象外の例**

オンプレミス環境において、以下のようなワークロードは Azure Backup で直接バックアップできません。
そのため、各ワークロードに適したバックアップ手段を別途検討する必要があります。

- NAS やストレージアプライアンス
- 仮想化基盤（VMware / Hyper-V の管理基盤そのもの）
- OS を持たない専用機器やサービス
- エージェントやバックアップサーバーを導入できないシステム

※オンプレミス環境における Azure Backup は、Azure Backup エージェント（MARS）や Azure Backup Server（MABS）を導入できるサーバーや仮想マシンなどを対象としています。

3.3. Azure Backup 利用の流れ

Azure Backup では、Recovery Services コンテナーを管理単位として、「バックアップ対象の登録 → バックアップポリシーの定義 → 自動バックアップの実行 → 復旧ポイントの管理」という一連の流れでバックアップを構成・運用します。
以下では、この流れを順に追いながら各ステップの内容や設計上のポイントを説明します。

① バックアップ対象の登録

Azure Backup では、まずバックアップ対象となるリソースを Recovery Services コンテナーに登録します。
登録されたリソースのみが Azure Backup の管理対象となり、以降はバックアップポリシーの割り当て、バックアップの実行、復元操作の対象として扱われます。

登録する内容例

- **管理単位の切り分け**
  本番環境・検証環境、システムごとなど、バックアップをどの単位で管理するかを設計します。運用や障害時の影響範囲を考慮し、適切な管理単位でバックアップ管理を行うことが重要です。
  Recovery Services コンテナーは、これらの管理単位をふまえて作成・設計されることが一般的です。
- **Recovery Services コンテナーの選定**
  バックアップ対象を、どの Recovery Services コンテナーで管理するかを決定します。
  既存のコンテナーを利用するか、新たにコンテナーを作成するかを含め、バックアップ構成上の管理をどのコンテナーに配置するかを検討します。
- **バックアップ対象の種類**
  Azure VM、Azure Files、オンプレミスサーバーなど、対象とするワークロードを登録します。
  -Azure VM や Azure Files は Azure ポータルから既存リソースを選択して登録
  -オンプレミスサーバーは Azure Backup エージェント（MARS）や Azure Backup Server（MABS）をインストール・構築して登録

3.3. Azure Backup 利用の流れ

バックアップ対象の登録 → バックアップポリシーの定義 → 自動バックアップの実行 → 復旧ポイントの管理

設計上のポイント

✓ **コンテナーは後から変更・統合できない**

Recovery Services コンテナーは、作成後に他のコンテナーへ移動したり、複数のコンテナーを統合したりすることができません。
一度どのコンテナーでバックアップを管理するかを決定すると、その構成を前提とした運用が継続されるため、初期のコンテナー設計と選定が重要です。

✓ **コンテナー作成前にリージョンや管理範囲を確定する**

Recovery Services コンテナーは特定のリージョンにひも付いて作成されます。
Azure 上のデータソースをバックアップする場合、コンテナーはデータソースと同じリージョンに配置する必要があります。
そのため、どのリージョンでバックアップを管理するか、また本番・検証などをどの管理単位で分けるかといった設計を、事前に検討しておく必要があります。
なお、リージョンや管理単位は後から変更できず、設計を変更したい場合は新たにコンテナーを作成しバックアップ構成を作り直す必要があるため、コンテナー作成前に設計を固めておくことが重要です。

✓ **バックアップ対象の選定**

バックアップ対象として登録されたリソースに対してコストが発生するため、すべてのリソースを一律にバックアップ対象とするのではなく、要件に応じて対象を選定する必要があります。重要なデータを扱う業務サーバーを優先的にバックアップ対象とするなどの設計が重要です。

3.3. Azure Backup 利用の流れ

バックアップ対象の登録 → **バックアップポリシーの定義** → 自動バックアップの実行 → 復旧ポイントの管理

② バックアップポリシーの定義

次に、バックアップポリシーの定義と割り当てを行います。
バックアップポリシーは Azure Backup における運用ルールであり、「いつバックアップを取得するか」「どれくらいの期間データを保持するか」といった設定を定義します。
バックアップポリシーは Recovery Services コンテナー単位で管理されます。同じコンテナー内の各バックアップ対象に適用するポリシーを個別に選択できるほか、複数のバックアップ対象に対して同一のポリシーを割り当てることも可能です。

項目	内容	設計時の考慮点
取得頻度	バックアップを取得する間隔（例：日次、週次など）を定義	業務データの更新頻度や、どの程度のデータ損失を許容できるか（RPO）を考慮
実行時刻	バックアップを実行する時刻を定義	業務時間帯を避けるなど、本番システムへの影響を最小限にする
保持期間（短期）	日次バックアップなど、直近の復旧ポイントを保持する期間を定義	日常的な誤操作や障害から迅速に復旧できる期間の確保が必要
保持期間（長期）	月次・年次など、長期間保持するバックアップを定義	監査要件や法令対応、長期的なデータ保管要件を考慮

3.3. Azure Backup 利用の流れ

バックアップ対象の登録 → **バックアップポリシーの定義** → 自動バックアップの実行 → 復旧ポイントの管理

設計上のポイント

✓ **取得頻度 × 保持期間 = コストと復元範囲に直結**
バックアップを高頻度で取得し長期間保持するほど、復元できる範囲は広がりますが、その分バックアップストレージの使用量が増え、コストも増加します。（※ Azure Backup の課金要素については本資料の7章をご確認ください。）
業務要件（RPO）とコストのバランスを考慮したバックアップポリシーの設計が重要です。

✓ **ポリシー定義により、環境全体で一貫したバックアップ運用が可能**
バックアップポリシーをあらかじめ定義しておくことで、Recovery Services コンテナー単位で環境全体に、統一されたルールに基づくバックアップ運用が可能になります。
新しいリソースを追加する場合も、既存のポリシーを割り当てるだけで同じルールを適用できます。

3.3. Azure Backup 利用の流れ

バックアップ対象の登録 → バックアップポリシーの定義 → **自動バックアップの実行** → 復旧ポイントの管理

③ 自動バックアップの実行

バックアップ対象とバックアップポリシーが設定されると、
以降のバックアップはバックアップポリシーに基づき、Azure Backup によって自動的に実行されます。

バックアップ処理の流れ（※詳細な仕組みは4章にて説明。）

1．バックアップポリシーで定義されたスケジュールに基づき、Azure Backup がバックアップ処理を開始。
2．対象ワークロードに応じて、VM 拡張機能や Azure Backup エージェントを通じて整合性モデルを考慮したバックアップが実行される。
3．取得されたバックアップデータは、Recovery Services コンテナーの管理下で Azure 管理下のストレージに保存される。
4．バックアップ完了後、取得時点の状態が復旧ポイントとして管理される。

ポイント

✓ **バックアップは Azure Backup により自動で実行**
割り当てられたバックアップポリシーのスケジュールに従い、バックアップは自動的に実行されます。

✓ **バックアップの成功 / 失敗は Azure ポータルで確認可能**
各バックアップ処理はジョブとして記録され、Azure ポータルから成功・失敗の状態や実行結果を確認できます。
失敗時の原因確認や、運用監視につなげることが可能です。

✓ **本番システムを稼働させたままバックアップを取得**
バックアップは、本番システムの利用を継続したまま実行されるため、業務への影響を最小限に抑えた運用が可能です。

3.3. Azure Backup 利用の流れ

バックアップ対象の登録 → バックアップポリシーの定義 → **自動バックアップの実行** → 復旧ポイントの管理

補足：バックアップデータの保存先

Azure Backup によって取得されたバックアップデータは、Microsoft によって管理される Azure 管理下の専用ストレージに保存されます。
このストレージは基盤技術として Azure Storage を利用していますが、ユーザーが作成・管理する Azure Storage Account そのものではありません。
Azure Backup では、ユーザーが作成・管理する Azure Storage Account ではなく、Azure 管理下のストレージにバックアップデータを保存することで、安全性と運用性を両立しています。

Azure 管理下のストレージと Azure Storage Account の違い

観点	Azure 管理下のストレージ	Azure Storage Account（ユーザー管理）
利用用途	Azure Backup によるバックアップデータの保存専用	アプリケーション・業務データなど汎用的なデータ保存
管理者	Microsoft（Azure Backup サービス）	ユーザー
作成・削除	ユーザー操作不可	ユーザーが作成・削除
直接アクセス・設定変更	不可 （ユーザーによる直接アクセスは不可） （復元操作は Azure Backup を通じて実施）	可能 （冗長性・ネットワークなどをユーザーが設定）

3.3. Azure Backup 利用の流れ

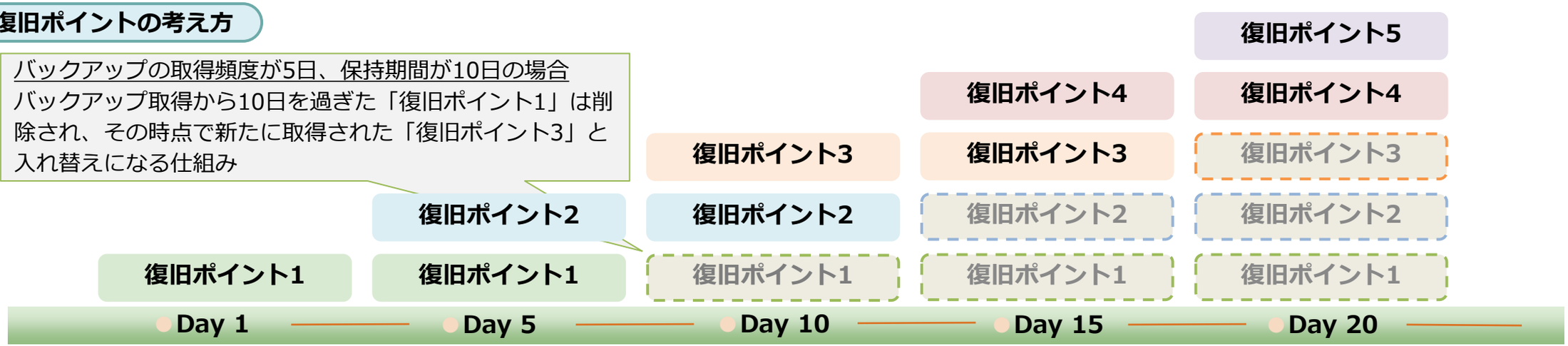
バックアップ対象の登録 → バックアップポリシーの定義 → 自動バックアップの実行 → **復旧ポイントの管理**

④ 復旧ポイントの管理

取得されたバックアップデータは、それぞれ復旧ポイント（バックアップ取得時点のデータ状態）として管理されます。
復旧ポイントはバックアップポリシーで定義された保持期間に従って管理され、保持期間を超えた復旧ポイントは自動的に削除されます。
複数の復旧ポイントが時系列で保持・入れ替えされ、復元時は保持される復旧ポイントの中から必要な時点に復元することが可能です。

復旧ポイントの考え方

<u>バックアップの取得頻度が5日、保持期間が10日の場合</u>
バックアップ取得から10日を過ぎた「復旧ポイント1」は削除され、その時点で新たに取得された「復旧ポイント3」と入れ替えになる仕組み



設計上の注意点

✓ **復旧ポイントの削除**
保持期間を超えた復旧ポイントは自動的に完全削除され、削除後にその時点の状態へ復元することはできません。

✓ **保持期間の定義**
保持期間はバックアップポリシーに基づいて管理されるため、復旧ポイントごとに保持期間を個別に変更・カスタマイズすることはできません。

3.3. Azure Backup 利用の流れ

バックアップ対象の登録 → バックアップポリシーの定義 → 自動バックアップの実行 → **復旧ポイントの管理**

補足：復旧ポイント管理の内部処理（データの再配置）について

各復旧ポイントはすべてのデータを復旧ポイントごとに独立して保持しているわけではなく、ストレージ効率化のため複数の復旧ポイント間でデータを共有しています。

保持期間を超えた復旧ポイントで起きること

保持期間を超えて「復旧ポイント1」が期限切れとなった場合、「復旧ポイント1」 は削除されます。
その際、「復旧ポイント1」が参照していたデータのうち、

- 後続の復旧ポイント（復旧ポイント2 以降）の**復元に必要なデータ：後続の復旧ポイントの構造に再配置**されます。
- 後続の復旧ポイントでは**使用されていないデータ：ストレージから解放（完全削除）**されます。

→「復旧ポイント1 のデータが丸ごと引き継がれる」のではなく、後続の復旧ポイントを復元するために必要なデータのみが残される仕組みです。

※ 復旧ポイント1 に含まれていたデータの一部が残ることになりますが、これはストレージ効率化のための内部処理です。復旧ポイント1 という「特定の時点に復旧できる状態」は完全に削除され、保持期間を超えた復旧ポイントの時点に復元することはできません。

4. Azure Backup の仕組み

4.1. バックアップ方式

一般的なバックアップの方法には完全バックアップ、差分バックアップ、増分バックアップの3種類があります。このうち、Azure Backupでは**初回バックアップは完全バックアップ**、**それ以降は増分バックアップ**を採用しています。それぞれの特徴は以下の通りです。

バックアップ方式

■ 完全バックアップ

バックアップ対象全体を完全にコピーする方法です。バックアップのたびにすべてのデータをコピー・保管するため、大量のネットワーク帯域と記憶領域が必要です。

- └ 最後のバックアップデータのみあれば復元が可能
- └ **Azure Backupでは初回バックアップ時のみに使用される**

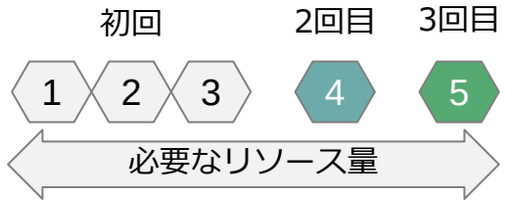
■ 差分バックアップ

初回は完全バックアップを行い、それ以降は初回バックアップデータと比較して変更された箇所をコピーする方法です。完全バックアップよりもコピーする箇所が少ないため、実行時間や使用するネットワーク帯域・記憶領域を減らせます。

- └ 復元には初回バックアップデータと最後の差分バックアップデータが必要

※差分バックアップは一般的なバックアップ方式の一つですが、Azure Backup では採用されていません。

■ 増分バックアップ



初回は完全バックアップを行い、それ以降は前回のバックアップデータと比較して変更された箇所をコピーする方法です。前回との比較になるため、初回と比較する差分バックアップよりもさらに実行時間・ネットワーク帯域・記憶領域の効率が良くなります。

- └ 復元には、初回バックアップデータとすべての増分バックアップデータが必要
- └ **Azure Backupでは、初回バックアップ以降は増分バックアップが採用される**

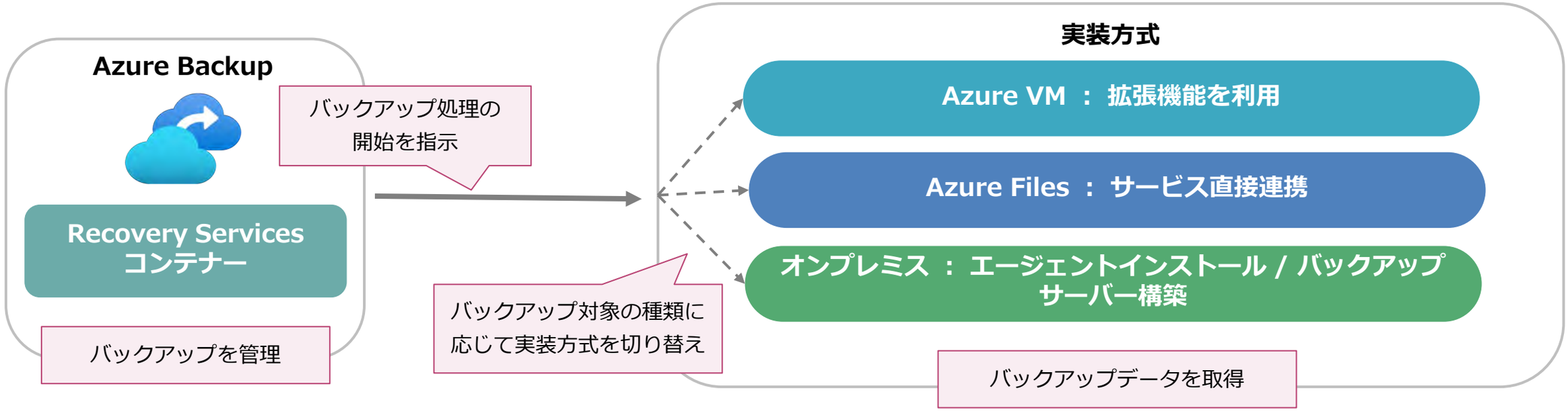
4.2. 実装方式

Azure Backup は、バックアップ対象の種類に応じて実装方式（バックアップ処理を実行する仕組み）を切り替えています。
本項では、実装方式の概要を整理したうえで、Azure VM・Azure Files・オンプレミス環境それぞれについてどのようにバックアップ処理を実行しているかを整理します。

実装方式の概要

Azure Backup におけるバックアップ処理は、以下役割で成り立っています。

- ■Azure Backup サービス ： バックアップのスケジュール管理、処理の開始指示を行う
- ■Recovery Services コンテナー ： バックアップ対象・バックアップポリシー・復旧ポイントを管理する制御点
- ■実装方式（拡張機能 / サービス連携 / エージェント） ： 実際にデータ取得（バックアップ処理）を実行する



4.2. 実装方式

バックアップ対象の種類（Azure VM・Azure Files・オンプレミス環境）に応じた実装方式について、以下に整理します。

Azure VM：拡張機能を利用

Azure VM のバックアップでは、**Azure VM 拡張機能が利用されます。**
拡張機能はバックアップ有効化時に Azure Backup が自動的に導入し、設定されたバックアップポリシーに基づいてバックアップ実行時のみ動作します。

■機能概要

1. Azure Backup サービスがバックアップを開始
2. Azure 管理プレーン経由で VM 拡張機能に実行指示
3. 拡張機能が OS・ファイルシステム・アプリケーションと連携してバックアップデータを取得
4. バックアップポリシーに基づき、Azure Backup サービスが復旧ポイント管理を実施

Azure Files：サービス直接連携

Azure Files のバックアップでは、拡張機能やエージェントは使用されません。
Azure Files サービスと Azure Backup が直接連携し、設定されたバックアップポリシーに基づいてバックアップが実行されます。

■機能概要

1. Azure Backup サービスがバックアップを開始
2. Azure Files サービス側でファイル共有のスナップショットを取得
3. Azure Backup がそのスナップショットを管理対象として認識
4. バックアップポリシーに基づき、 Azure Backup サービスが復旧ポイント管理を実施

オンプレミス：エージェントインストール / バックアップサーバー構築

オンプレミスのバックアップでは、**エージェントインストールもしくはバックアップ専用サーバーを構築することでバックアップを実行します。**

■MARS（Azure Backup エージェント）
・オンプレミスサーバーに直接インストール
・ファイル / フォルダー単位のバックアップが中心
・軽量でシンプルな構成

■MABS（Azure Backup Server）
・専用のバックアップサーバーを構築
・複数サーバー・ワークロードを集中管理
・より高度なバックアップ要件に対応

4.3. 整合性モデル

Azure Backup では、バックアップ対象や構成に応じて整合性モデルが適用されます。
バックアップ自体は成功しても、バックアップデータ取得時の整合性レベルによって復元後の挙動が異なるため、整合性モデルへの理解が必要です。
整合性モデルは、ユーザーがバックアップ設定時に選択・指定するものではありません。バックアップ対象やその時点の状態に応じて、取得可能な整合性を Azure Backup が自動的に判断し、可能な範囲で整合性を確保するという考え方が採用されています。

整合性モデルとは

整合性モデルとは、バックアップ取得時にデータをどのレベルまで整合性の取れた状態として保存するかを示す考え方です。
整合性のレベルによって、復元後の挙動が異なります。
Azure Backup における整合性モデルとして、基本となるのは主に「アプリケーション整合性」と「ファイルシステム整合性」の2つです。

バックアップ対象ごとの整合性モデル対応

- **アプリケーション整合性**
  バックアップ取得時にアプリケーションの状態を考慮し、復元後すぐに利用可能な状態を目指す整合性モデル。
- **ファイルシステム整合性**
  ディスクやファイル構造として破損しない状態でバックアップを取得する整合性モデル。
  データは壊れていないが、アプリケーションによっては起動時に回復処理（ログリプレイ等）が必要な場合がある。

○：条件が満たされれば取得可能　△：ワークロードや構成に依存　×：取得不可

バックアップ対象	アプリケーション整合性	ファイルシステム整合性
Azure VM	○	○
Azure VM 上のアプリケーション	○	○
Azure Files	×	○
オンプレミス	△	○

▶ すべてのバックアップ対象で「アプリケーション整合性が取れる」わけではありません。

4.3. 整合性モデル

Azure Backup は、バックアップ対象の種類、OS やアプリケーションの状態、実装方式などの情報を基に、バックアップ実行時に整合性の取得可否を判断します。

整合性取得の基本的な流れ

Azure Backup は、バックアップ実行時に次のような順序で処理を行います。

1. **まずはアプリケーション整合性が取得できるかを試みる**
2. アプリケーション整合性が**取得できない場合は、ファイルシステム整合性でバックアップを取得**
3. 実行時の状態によっては、アプリケーション整合性が取得できず、想定した整合性レベルに達しない結果となる場合もある

★バックアップ成功＝常にアプリケーション整合性が保証されるわけではありません。

整合性の結果はバックアップ対象・構成・実行時の状態に依存し、その時点で取得可能な最良の整合性を確保したバックアップが作成されます。

ポイント

✓ **整合性の結果は Azure ポータルで確認可能**

整合性の結果は、バックアップジョブの詳細として確認できます。バックアップの成功 / 失敗、アプリケーション整合性を取得できたか、取得できなかった場合はファイルシステム整合性にフォールバックしたか、などの情報を確認可能です。

✓ **ユーザーは整合性が取得されやすい状態を作ることが重要**

整合性モデルはユーザーが直接指定することはできませんが、OS やアプリケーションの状態、実装方式に適した構成、バックアップ実行タイミングの調整などにより、より高い整合性が取得されやすい状態を整えることが重要です。

4.4. 復元の考え方

バックアップ取得の最終的な目的は、障害や誤操作が発生した際にバックアップ取得時点の状態（復旧ポイント）へデータを復元できることです。
本項では、Azure Backup における復元の考え方としてどのような復元が可能かと復元手順の概要を整理します。

復元の種類

同一リソースへの復元

- 元のリソースに復元する方法
- 現在のデータを上書きするため、障害発生時の原状回復に利用される

別リソース・別環境への復元

- 別のリソースや環境として復元する方法
- 検証環境への復元や切り戻し確認、影響調査用途に有効

ファイル単位での復元

- バックアップ全体ではなく、必要なファイルのみを復元する方法
- 誤操作による削除や上書き対応に有効

※復元結果は、バックアップ取得時に確保された整合性モデルに依存します。
アプリケーション整合性が取得できている場合は、復元後アプリケーションをそのまま利用できる可能性が高いですが、ファイルシステム整合性の場合は、**データは破損しないがアプリケーション側で回復処理や再起動が必要な場合がある**ことを認識しておく必要があります。

ポイント

✓ **上書き・影響範囲を考慮する**
同一リソースへの復元は、現在のデータを上書きする可能性があります。ネットワーク設定や依存関係への影響も考慮が必要です。

✓ **整合性結果を前提に復元後の対応を考える**
アプリケーション整合性が取れていない場合は、起動確認やデータチェックを前提とし、復元＝即業務再開ではないケースも想定したうえで復元作業を実施する必要があります。

4.4. 復元の考え方

復元時の基本的な流れ

Azure Backup による復元は、Azure ポータルを起点として以下の手順で行います。

STEP 01

復旧ポイントを選択

- Azure ポータルから、Recovery Services コンテナーに登録されているバックアップ対象を選択。
- 保持期間内の復旧ポイントの中から、復元したい時点を選択。

※ 復元結果は、選択した復旧ポイント取得時の整合性に依存する。

STEP 02

復元方法を選択

- バックアップ対象に応じて、利用可能な復元方法を選択。
  - ○ 同一リソースへの復元
  - ○ 別リソース・別環境への復元
  - ○ ファイル単位での復元（対応ワークロードのみ）

STEP 03

Azure Backupによる復元が開始

- 復元方法を選択すると、Azure Backup が復元処理を制御し、対象に応じた仕組み（拡張機能・サービス連携・エージェント等）を通じて復元を実行。
- 復元処理の進捗や結果は Azure ポータルで確認可能。

STEP 04

復元後の確認・対応

- 復元完了後、復元された状態を確認。
  - ○ データが想定どおり戻っているか
  - ○ アプリケーションが正常に動作するか
- 整合性モデルに応じて、再起動や回復処理が必要な場合は対応を実施。

5. 利用メリットと注意点

5.1. 利用メリットと注意点

これまで説明した Azure Backup の仕組みや特徴をふまえて、主なメリットと注意点を整理します。

メリット

- **Azure 標準のマネージドバックアップサービス**
  Microsoft が Azure 上であらかじめ提供しているバックアップサービスのため、バックアップ専用サーバやストレージを個別に構築・保守する必要がない。バックアップの設定や状態確認は Azure ポータルから一元管理が可能。
- **コンテナー中心設計によるデータ管理**
  Recovery Services コンテナーを管理の中心として、バックアップ対象やバックアップポリシーをまとめて管理。
  バックアップ対象となる環境全体のバックアップ状況を把握しやすい設計。
- **ポリシーベースによる自動バックアップ運用**
  バックアップの取得頻度や保持期間をバックアップポリシーとして定義することで、バックアップは自動的に実行される。
  日常的な運用作業を最小限に抑えた安定運用が可能。
- **幅広いワークロードと柔軟な復元に対応**
  Azure VM や Azure Files に加え、オンプレミス環境（MARS / MABS）にも対応。バックアップ全体復元やファイル単位復元など、障害内容に応じた復元方法を選択できる。

注意点

- **すべての Azure / Microsoft サービスが対象ではない**
  Azure Backup は Azure VM や Azure Files を中心としたワークロード向けのサービスであり、PaaS サービスや Microsoft 365 データなどはバックアップ対象外。事前に保護対象と対象外を明確に整理する必要がある。
- **DR（災害対策）用途を単独で担うサービスではない**
  Azure Backup はデータを過去の状態に戻すことを目的としたバックアップサービスであり、システムの継続稼働を目的とした DR サービスではない。
  災害対策としての迅速な切り替えが必要な場合は、Azure Site Recovery など他サービスとの併用を前提に設計する必要がある。
- **Recovery Services コンテナーの設計変更が容易ではない**
  Recovery Services コンテナーは、作成後にリージョン変更や他コンテナーへの移動・統合ができない。管理単位やリージョンは後から変更できないため、設計段階で慎重に検討する必要がある。
- **コストは保護対象数と保持期間に応じて発生**
  Azure Backup の料金は、保護されるインスタンス数とバックアップデータの保持量に基づいて課金される。バックアップを取得していなくても保持している限りコストが発生するため、取得頻度や保持期間は業務要件に基づき適切に設計する必要がある。

6. 活用シナリオ

6.1. シナリオ①：Azure IaaS を中心とした標準バックアップ

本章では、Azure Backup を活用するシナリオを3つ紹介します。

背景・課題

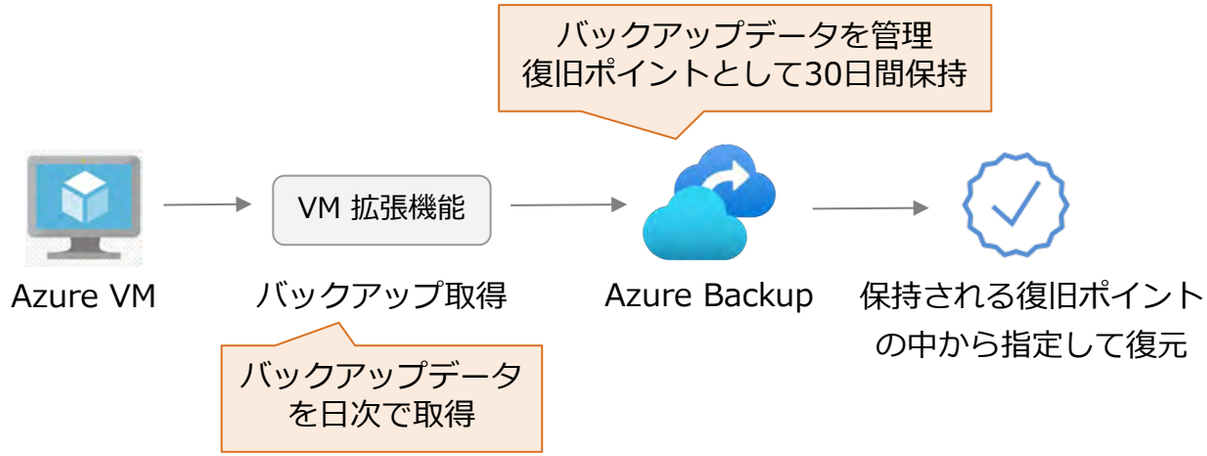
- Azure VM 上で業務システムを運用している
- 障害 / 誤操作 / 更新失敗などに備え、サーバー単位でのバックアップが必要
- 手動バックアップや個別運用では運用負荷・設定漏れ・属人化のリスクが高いため、**復元できる仕組みが欲しい**

運用イメージ・効果

- ✓ バックアップは**バックアップポリシーに基づき自動実行**
- ✓ 運用担当者が個別に操作する必要がない
- ✓ バックアップ対象となるサーバー追加時は、**既存バックアップポリシーを適用可能**
- ✓ 基本的なデータ保護を実現し、復旧ポイントを指定して必要な時点に戻せる

Azure Backup の設計

- 対象ワークロード：Azure VM
- 実装方式：VM 拡張機能を利用したバックアップ
- 管理単位：
  - ・本番環境単位で Recovery Services コンテナーを作成
  - ・Recovery Services コンテナー内の同一要件の VM には、同じバックアップポリシーを適用
- バックアップポリシー例：
  - ・取得頻度：日次1回
  - ・保持期間：短期保持（例：30日）
  - ・整合性：可能な場合はアプリケーション整合性
    取得できない場合はファイルシステム整合性



6.2. シナリオ②：セキュリティ対策を意識したバックアップ

背景・課題

- ランサムウェアや内部不正により、**本番データだけでなくバックアップデータも破壊されるリスクが高まっている**
- 管理者権限を奪取された場合、バックアップの削除・無効化が被害拡大につながる
- バックアップを取っているだけでは、十分な対策とは言えない

運用イメージ・効果

- ✓ バックアップは Azure 管理下のストレージに保存され、**直接操作不可**
- ✓ Soft Delete により、**削除操作が行われても一定期間は復旧可能**
- ✓ 権限分離・MFA により、**管理者権限を奪取された場合の被害を抑制**

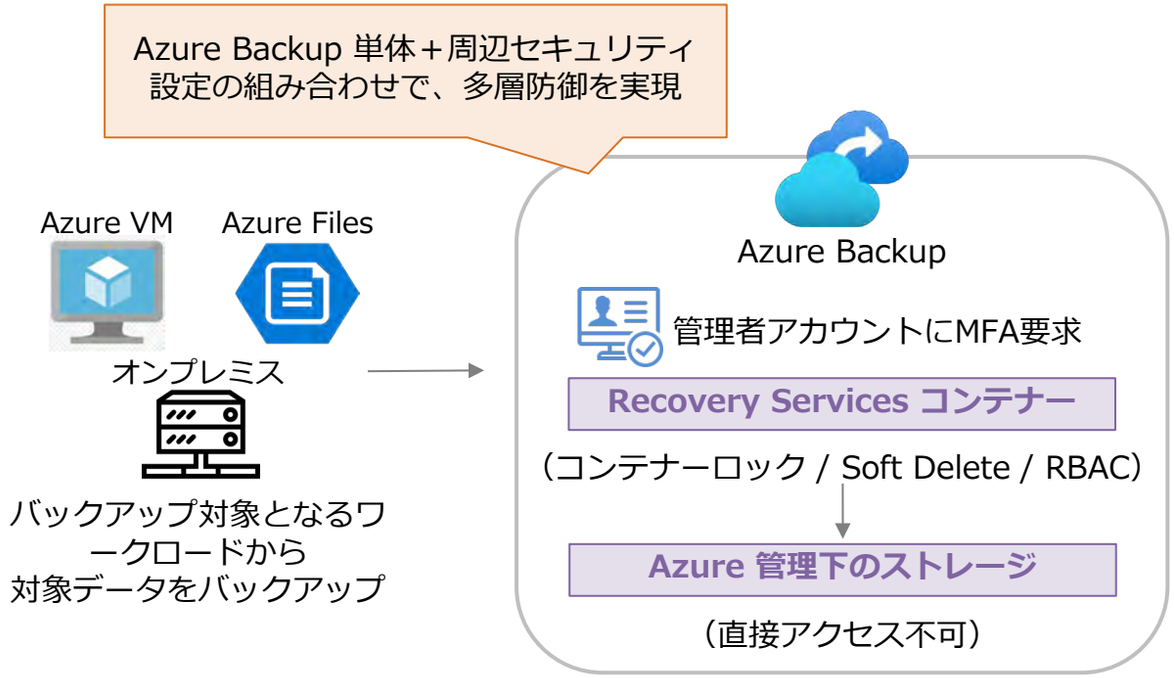
Azure Backup の設計

対象ワークロード

- 重要データを扱う業務サーバー（Azure環境 / オンプレミス環境）

セキュリティを意識した設計

- **コンテナーロックによる変更防止**：
  Recovery Services コンテナーに対してリソースロックを設定し、意図しない削除や変更を防止
- **削除・改ざんを防ぐ仕組みの活用**：
  Azure Backup の機能である Soft Delete により、誤操作や不正操作によるバックアップデータの即時削除を防止
  ※ Soft Delete は、削除操作に対する保護機能であり、バックアップポリシーで定義された保持期間を超えた復旧ポイントの削除を防ぐものではありません。
- **権限の分離（RBAC）**：本番環境の管理者とバックアップ管理者の権限を分離し、最小権限で運用
- **管理操作の保護（MFA など）**：バックアップ管理者アカウントに対して、MFA を含む認証強化を実施



※ コンテナーロック、RBAC、MFA 等は、Azure Backup 標準の機能ではなく、Azure / Microsoft Entra ID 側で別途設計・設定が必要なセキュリティ機能です。

6.3. シナリオ③：ハイブリッド環境でのバックアップ

背景・課題

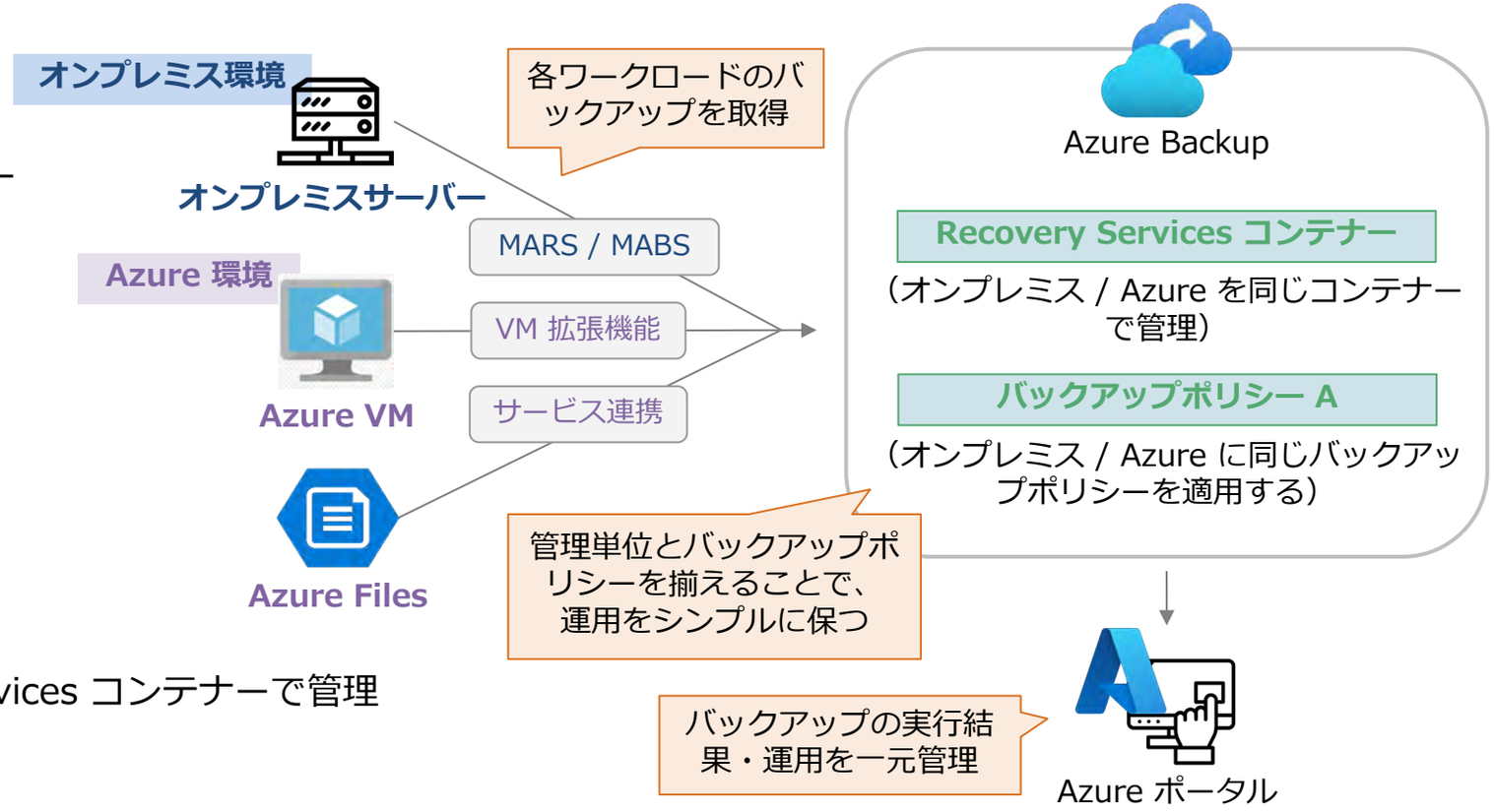
- システム移行においてすべてを一度にクラウド移行できず、**オンプレミス環境と Azure 環境が併存して運用している**
- オンプレミス環境と Azure 環境では管理手法が異なるため、バックアップ運用も分断されやすい

運用イメージ・効果

✓ ハイブリッド環境でも、Azure Backup により**バックアップ運用を統一**
✓ Azure 移行後も**バックアップ設計を大きく変更せずに運用継続可能**なため、将来的なオンプレミス廃止・Azure 完全移行に対応しやすい

Azure Backup の設計

- 対象ワークロード：重要データを扱う業務サーバー（Azure環境 / オンプレミス環境）
- 実装方式：
  オンプレミス環境
  ・Azure Backup エージェント（MARS）
  ・Azure Backup Server（MABS）
  Azure 環境
  ・Azure VM：VM 拡張機能
  ・Azure Files：直接サービス連携
- 設計ポイント
  ・オンプレミスと Azure を同一の Recovery Services コンテナーで管理
  ・バックアップポリシーは可能な範囲で共通化



7. Azure Backup の料金

7.1. 課金形態

Azure Backup の利用に専用のライセンス等を購入する必要はありません。Azure Backup は、Azure の標準サービスとして利用した分だけ課金される従量課金制で提供されます。

Azure Backup の課金要素

Azure Backup の料金は、主に次の 2つの要素で構成されます。

- **保護されたインスタンス課金**

  バックアップ対象として登録されたリソース（Azure VM / Azure Files / オンプレミスなど）に対して発生

  → バックアップを有効化した時点で、対象リソースは「保護されたインスタンス」として扱われます。
  保護されたインスタンスへの課金は、バックアップ対象の種類ごとに定義された区分に基づいて発生します。

  → バックアップを取得していない日があっても、保護状態である限り課金対象となります。

- **バックアップストレージ課金**

  Azure 管理下のストレージに保存されているバックアップデータ量に対して発生

  → バックアップデータは保持期間に応じてストレージ上に保持されるため、保持期間の設計がストレージに対するコストに直結します。

※ Azure Backup の課金形態について詳しくは Microsoft 公式サイトをご確認ください。

コストに影響する設計ポイント

- **バックアップ対象の選定**：すべてのリソースを一律にバックアップするのではなく、重要なデータを扱う業務サーバーを優先してバックアップ対象とします。
- **業務要件に応じて 取得頻度 × 保持期間 を設計**：取得頻度を高くすると復旧ポイントが増え、その保持期間を長くすると長期間遡った復元が可能になりますが、その分ストレージコストも増加します。
  業務要件に対してどこまで復元できれば十分かを明確にした上での設計が重要です。