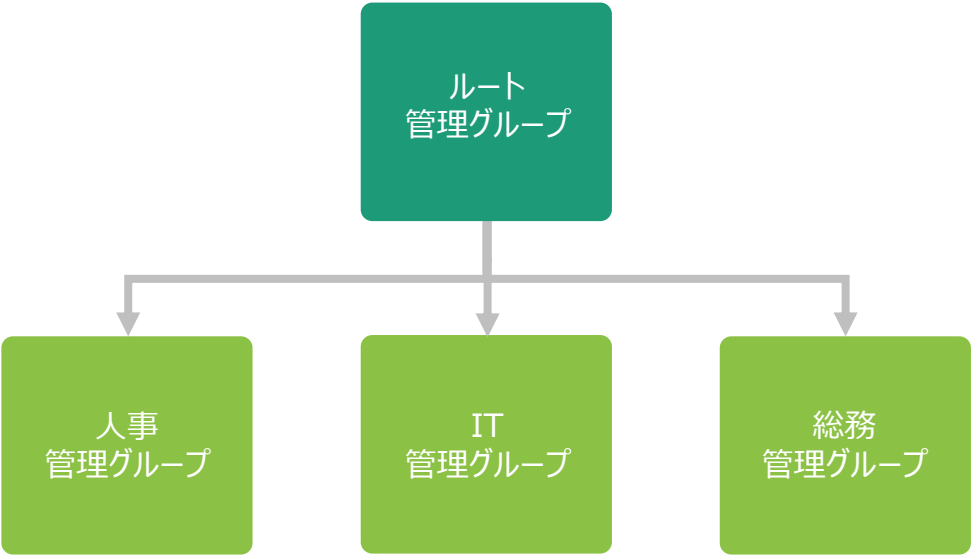


AZ-305

補足資料 Ver1.2

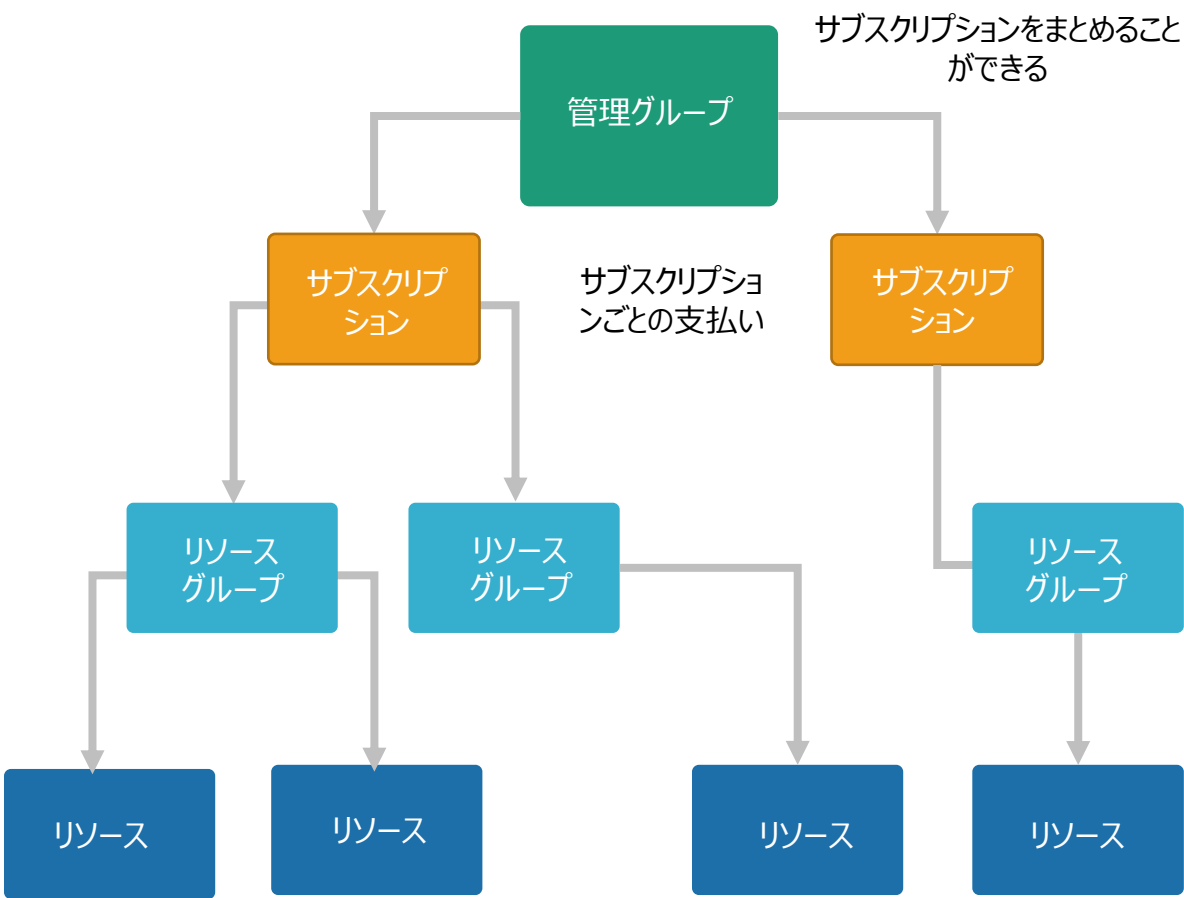
リソースグループとサブスクリプションの関係

AzureADテナント = 管理グループの階層構造

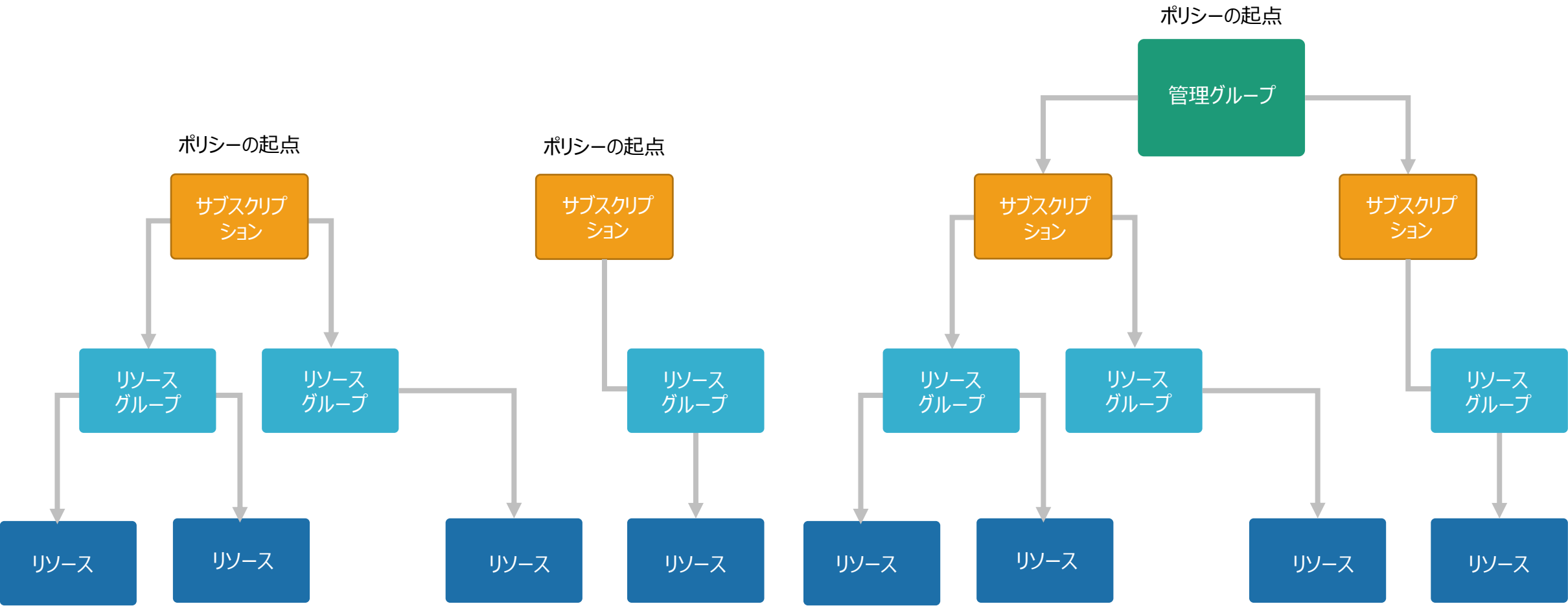


管理グループごとに請求を分けることができる

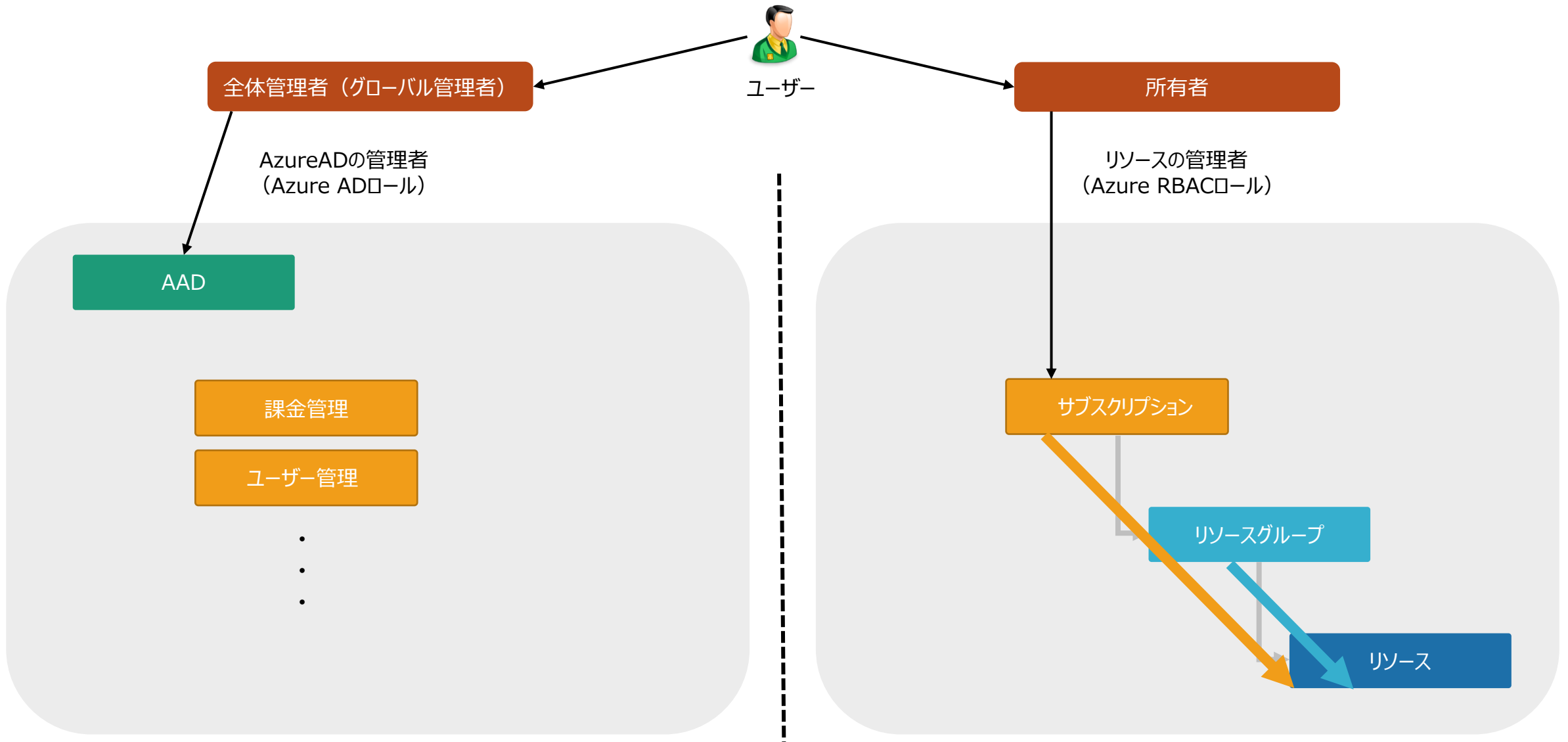
サブスクリプションの位置づけ



管理グループとポリシーの関係



ロール



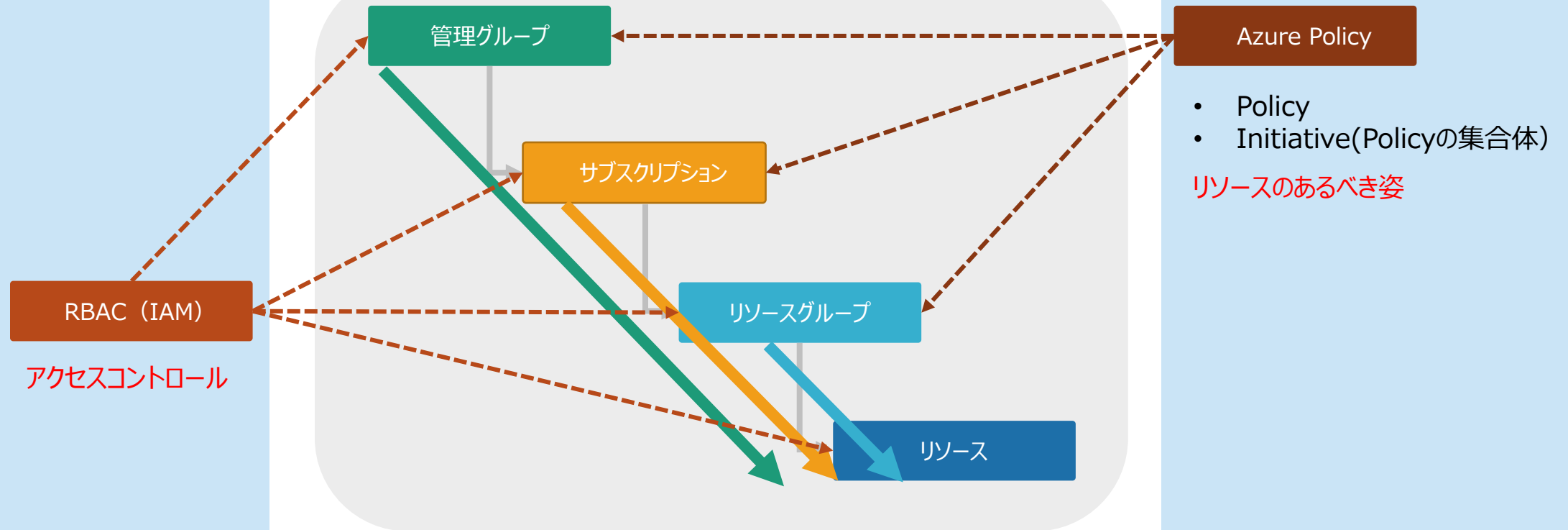
Azure階層とRBACロール

Azure Blueprints

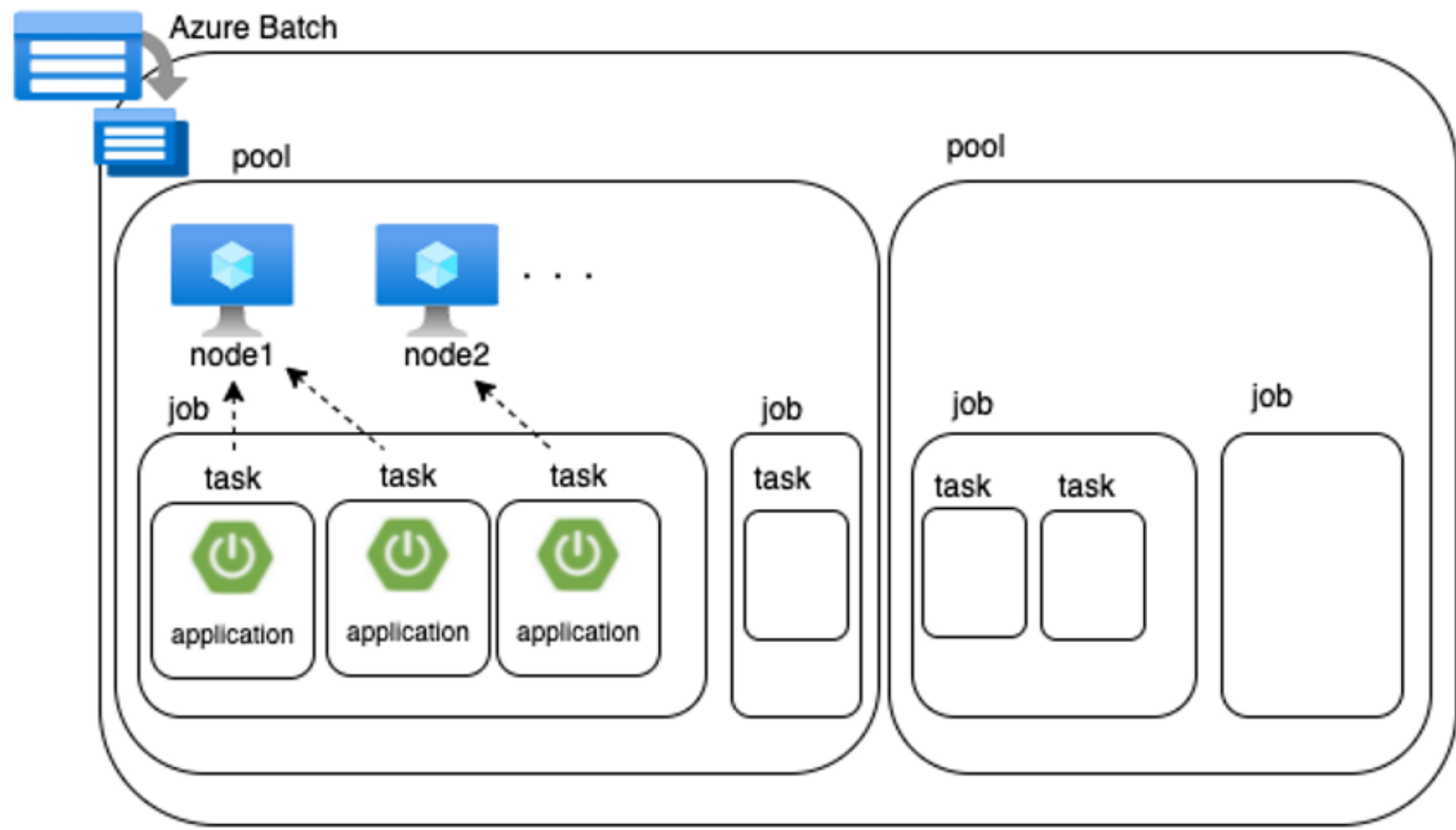
- 組織のコンプライアンス設定可能
- バージョン設定
- RBACの拒否設定

ARM Template

Azureのリソースを定義したJSONファイル



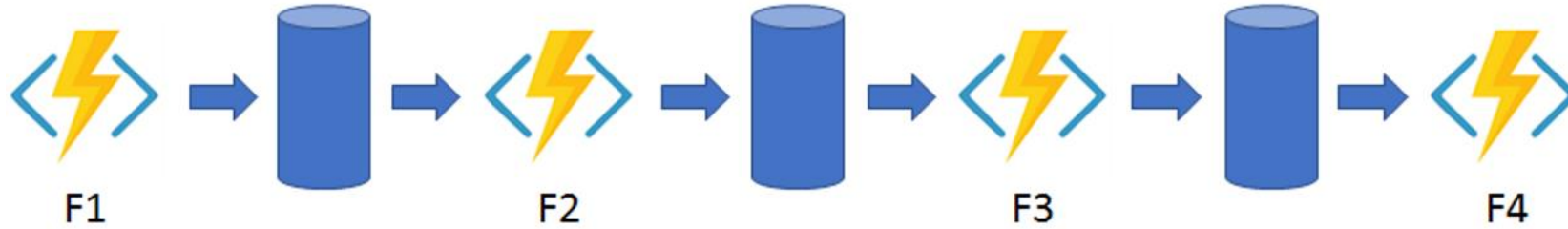
Azure Batch



Durable Functions

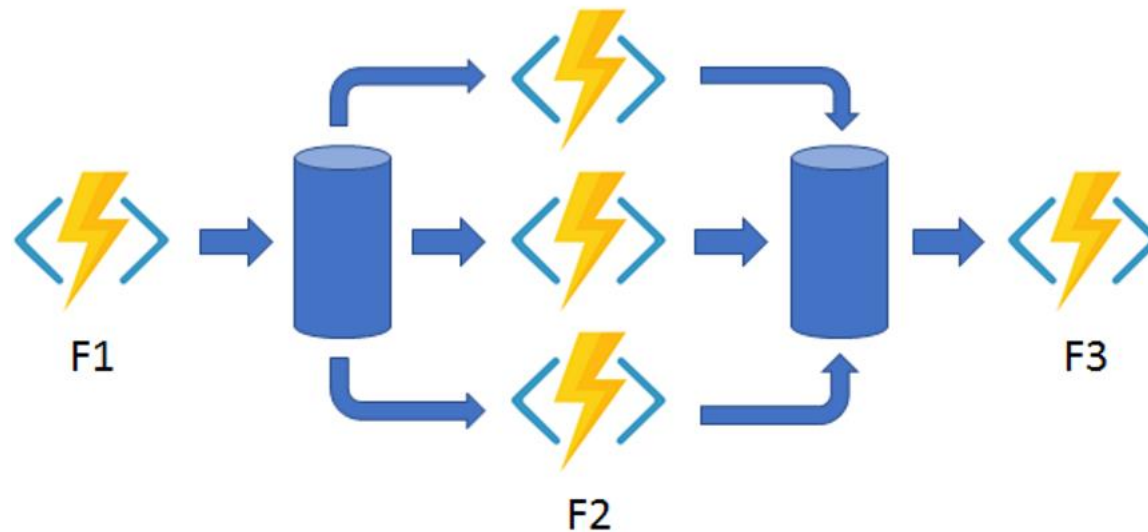
1.1. Function Chaining

Function から Function を簡単に呼べる Function Chaining パターン



1.2. Fan-out, Fan-in

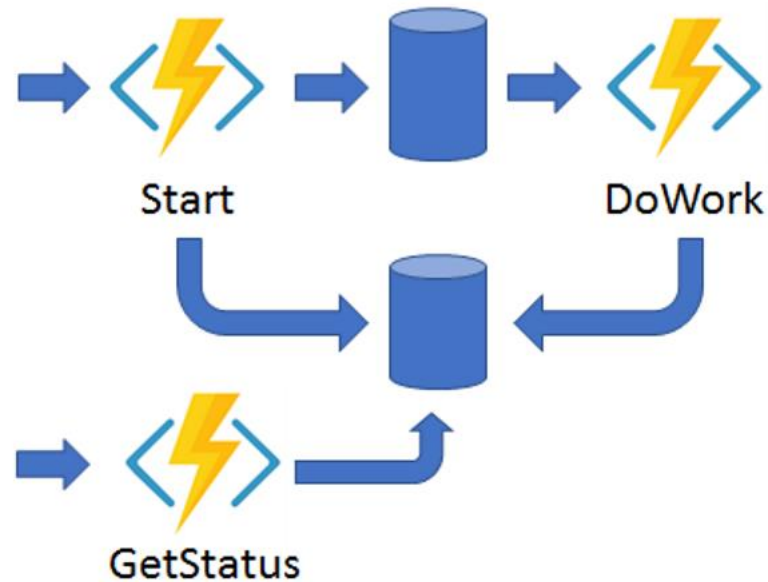
並列実行して、それが全部終わったら、次のファンクションに流す。非同期実行を、最後で待ち合わせてくれるのがみそ。



Durable Functions

1.3. Async HTTP APIs

これはロングランニングの非同期 HTTP API の実行で役に立つパターン。ロングランニングの非同期実行の function のステータスを問い合わせられるAPIが作られる。



Durable Functions

1.4. Lightweight Actors

Service Fabric でもおなじみの **Actor** を使える。つまり **Stateful** を扱えます。Service Fabric の実装とは異なってライトウェイトでシンプルな感じです。

1.5. Human interaction and timeouts

人が介入して承認とかするようなパターンです

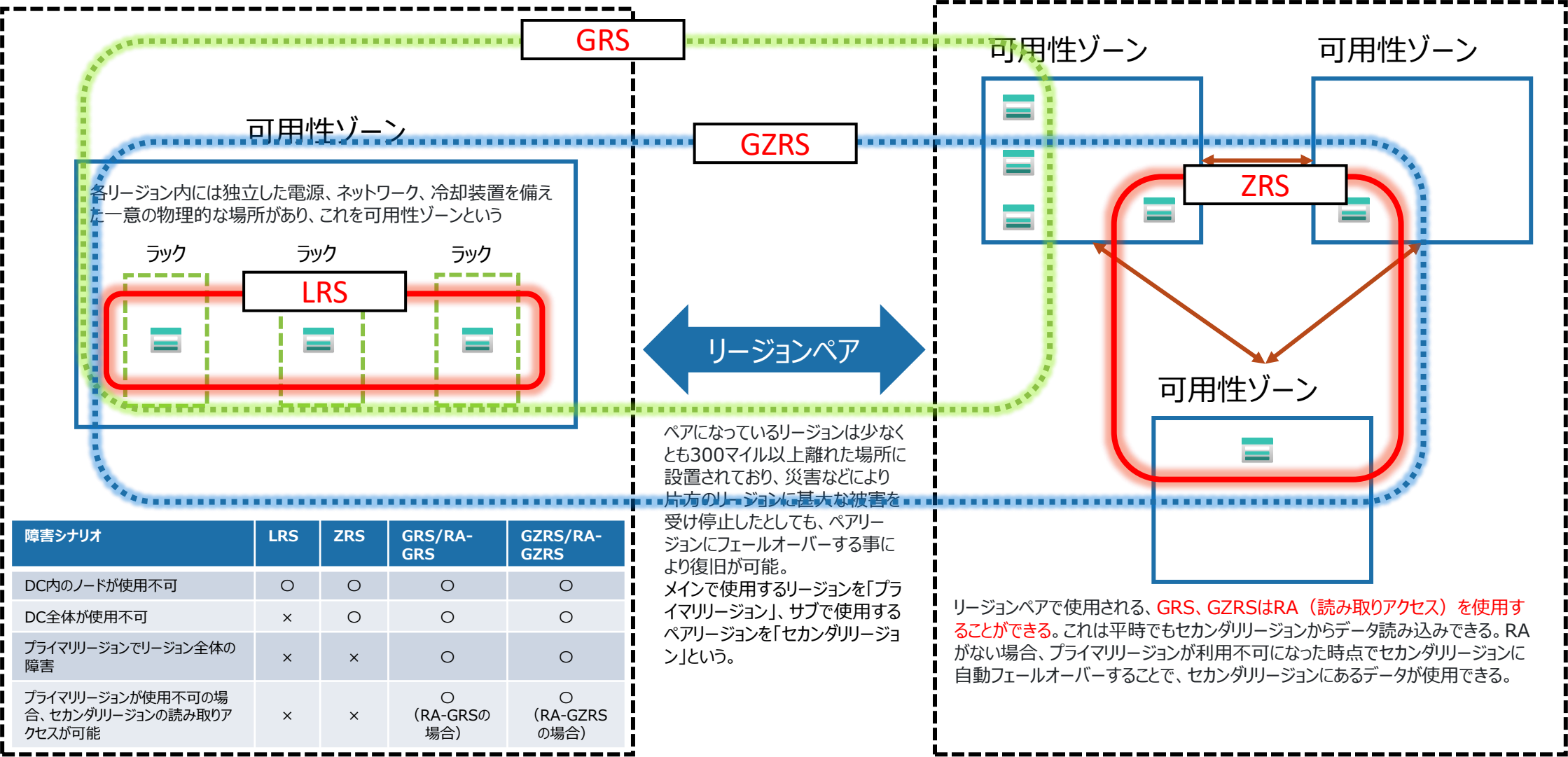


Azure Storage レプリケーション

LRS:Locally redundant storage
ZRS:zone-redundant storage
GRS:geo-redundant storage
GZRS:geo-zone-redundant storage

西日本リージョン

東日本リージョン



ストレージのアクセス層まとめ

ホット

- 他の層と比べてストレージ コストが**高め**だが、アクセス コストが**最も低**くなります。
- **頻繁にアクセス**されるデータの格納向け

クール

- ホットストレージ層に比べてストレージコストが**低**くなり、アクセスコストが**高**くなります。
- **アクセス頻度が低い**データ向け。
- 少なくとも 30 日以上保管されるデータに最適化。

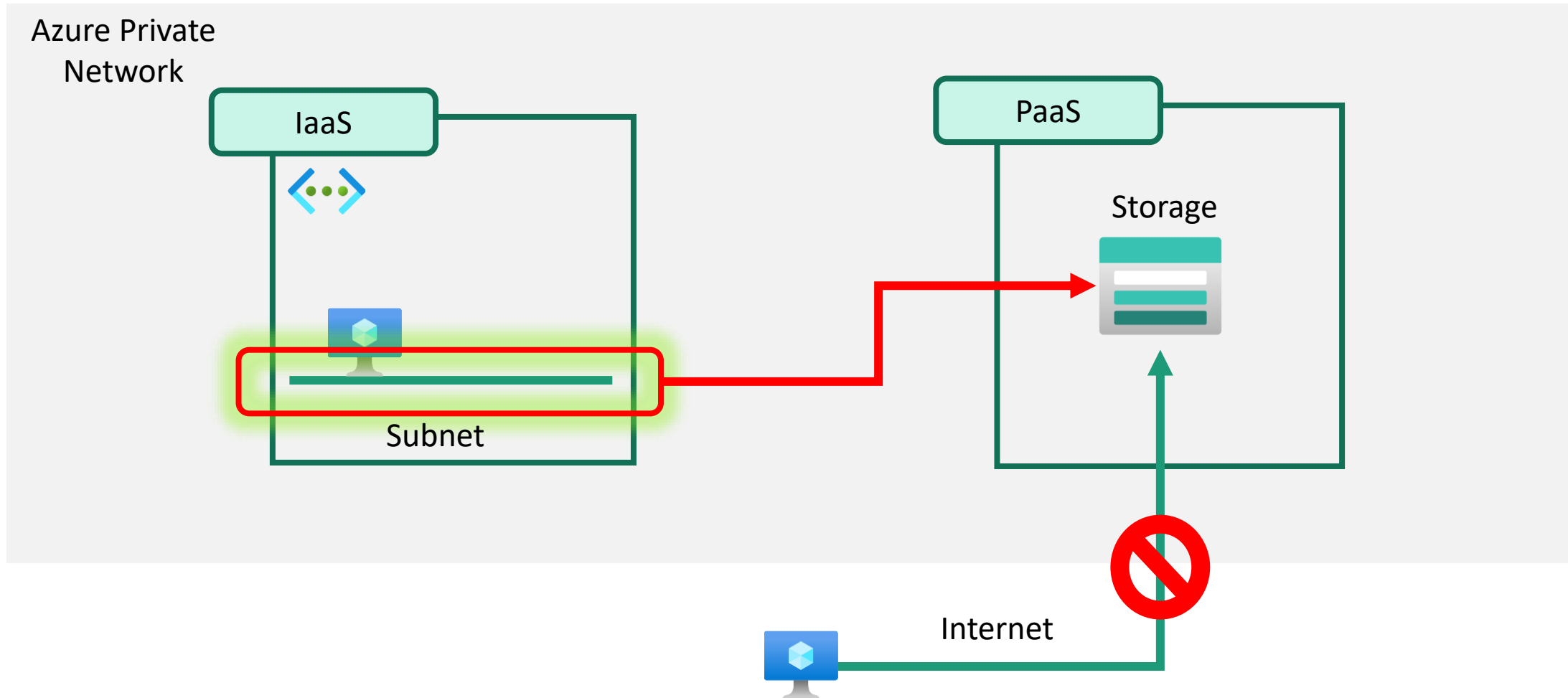
アーカイブ

- ストレージ コストが**最も低**く、他に比べてデータ取得コストが**最も高**くなります
- データの読み取り、コピー、上書き、変更を行うことはできない。
- ほとんど**アクセスされず**、少なくとも 180 日以上保管されるデータ向け。

	ホット	クール	アーカイブ
可用性	99.9%	99%	-
可用性(RA-GRS)	99.99%	99.9%	-
ストレージコスト	高い	低い	最も低い
アクセスコスト	低い	高い	最も高い
トランザクションコスト	低い	高い	最も高い
最小ストレージ存続期間	-	30日(GPv2のみ)	180日
待機時間	ミリ秒	ミリ秒	15時間未満

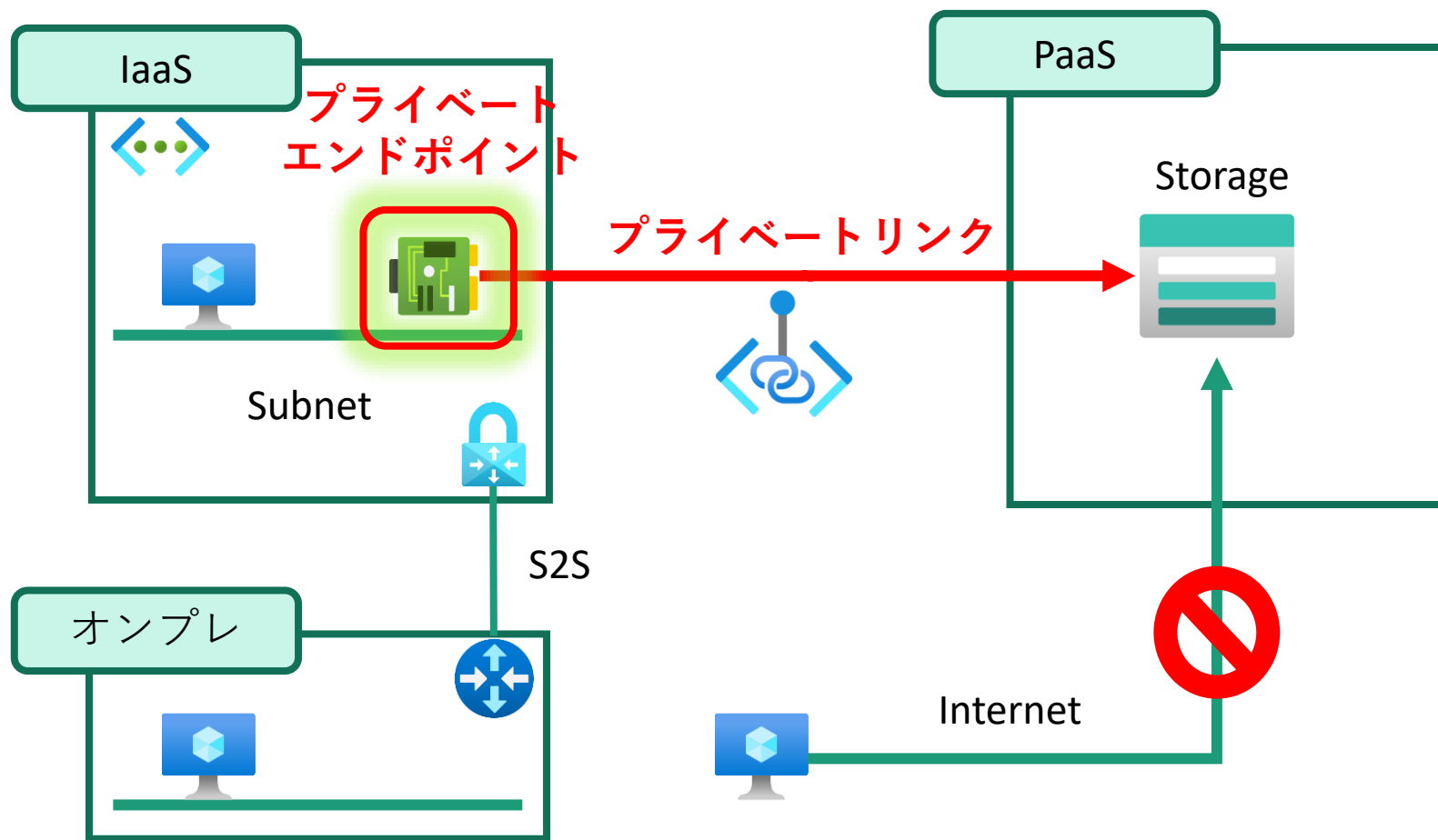
サービスエンドポイント

Azure上の各種PaaS系サービスとの接続を、**仮想ネットワーク(サブネット)からの接続に限定**してしまうセキュリティ機能



プライベートエンドポイント

- **プライベートエンドポイント**とは、プライベートリンクを実現するための仕組みの一つで、プライベートリンクサービスにプライベートで安全に接続するネットワークインターフェイスを提供する。
- プライベートリンクサービスとは**プライベートリンク**を使用するサービスのことで、 Azure Storage や Azure SQL Database などの定義済みのプライベートリンクリソースなどを指す。



SQL Database（シングルデータベース／エラスティックプール）の特徴

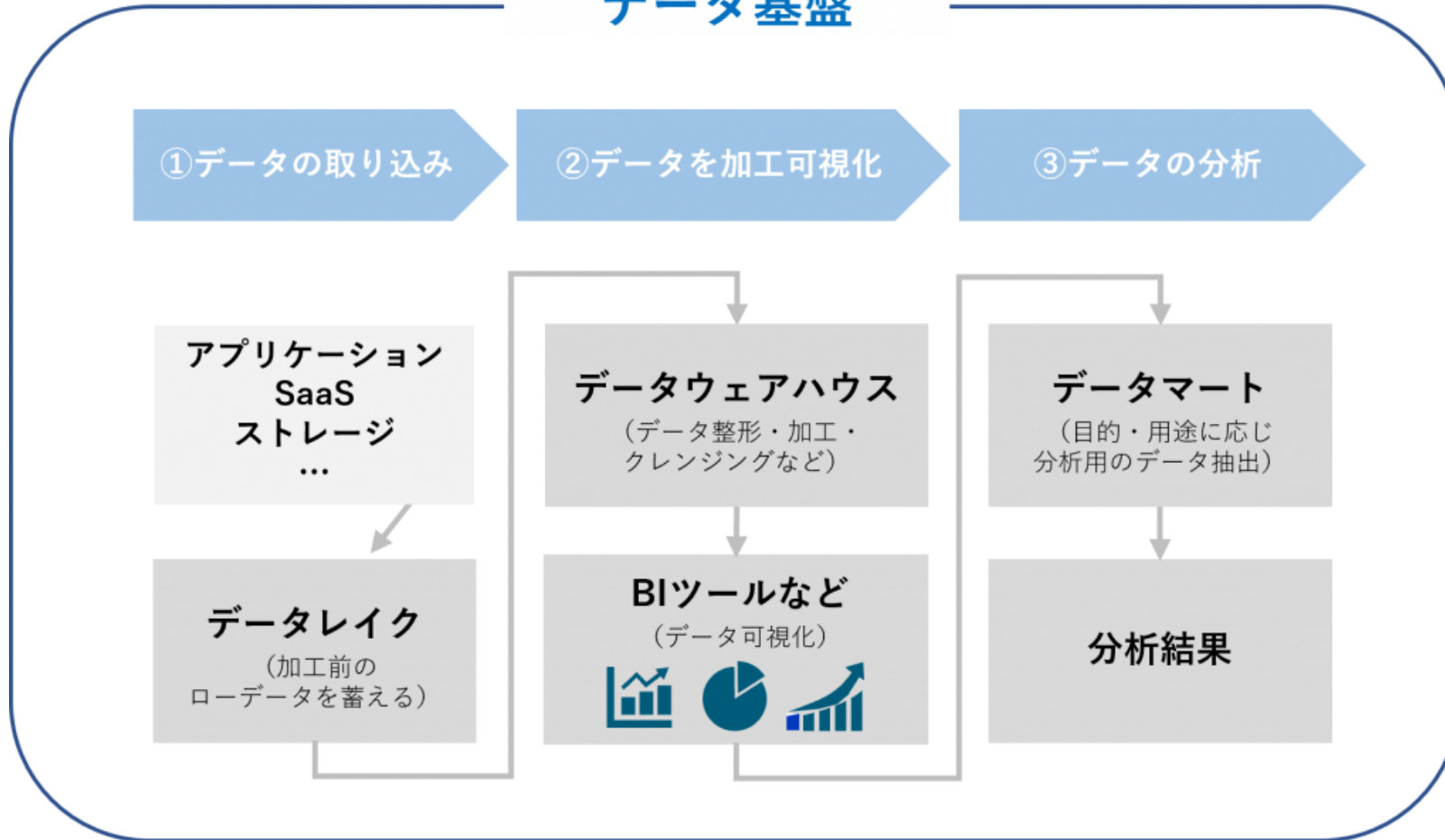
SQL Serverとの機能の違い	代替案
タイムゾーンがUTC（協定世界時）固定	日本時間を使用する必要がある場合は9時間の差を考慮するように処理を実装する
SQL Serverと同一の方法でデータベースをまたいだクエリを実行できない	エラスティッククエリやエラスティックトランザクションで代替可能かどうかを検討
リンクサーバをサポートしていない	Azure BLOBストレージを介したデータアクセス や Azure Data Factory などの機能で外部データ連携が代替可能かどうかを検討
レプリケーションはトランザクション／スナップショットのサブスクライバーのみをサポート	SQL Databaseを起点としたデータ同期が必要な場合、 Data Sync で代替可能かどうかを検討
SQL Serverのネイティブバックアップを利用できない（BACKUP／RESTOREステートメントをサポートしていない）	BACPACファイル を使用したデータベースのエクスポート／インポートで代替可能かどうかを検討
Windows認証をサポートしていない	Azure Active Directory認証 で認証管理が代替可能かどうかを検討
SQL Serverプロファイラーによるクエリ情報の取得をサポートしていない	拡張イベント で代替可能かどうかを検討
SQL Serverエージェントをサポートしていない	Azure Automation などの機能で代替可能かどうかを検討

Managed InstanceとSQL Serverの機能の違い

- ネイティブバックアップを使用して、既存SQL Serverのデータベースの移行が可能
- インスタンス内のデータベースをまたいだクエリの実行が、SQL Serverと同等の方法で可能
- SQL Serverエージェントによるジョブスケジューラーの利用が可能
- SQL Serverプロファイラーでクエリ情報の取得が可能
- レプリケーションのディストリビューター／パブリッシャーとしての利用が可能

データ基盤

データ基盤



活用するAzureサービス

- Azure DataFactory
- Azure DataLake Storage

活用するAzureサービス

- Azure Databricks
- Azure Synapse Analytics
- Azure DataLake Analytics
- Power BI

活用するAzure サービス

- Azure Machine Learning
- Azure AD
- Microsoft Sentinel

①データの取り込み

オンプレミス、クラウド上のアプリケーションやデータベース、ストレージなどに散在するデータを収集し保存します。

②データを加工可視化

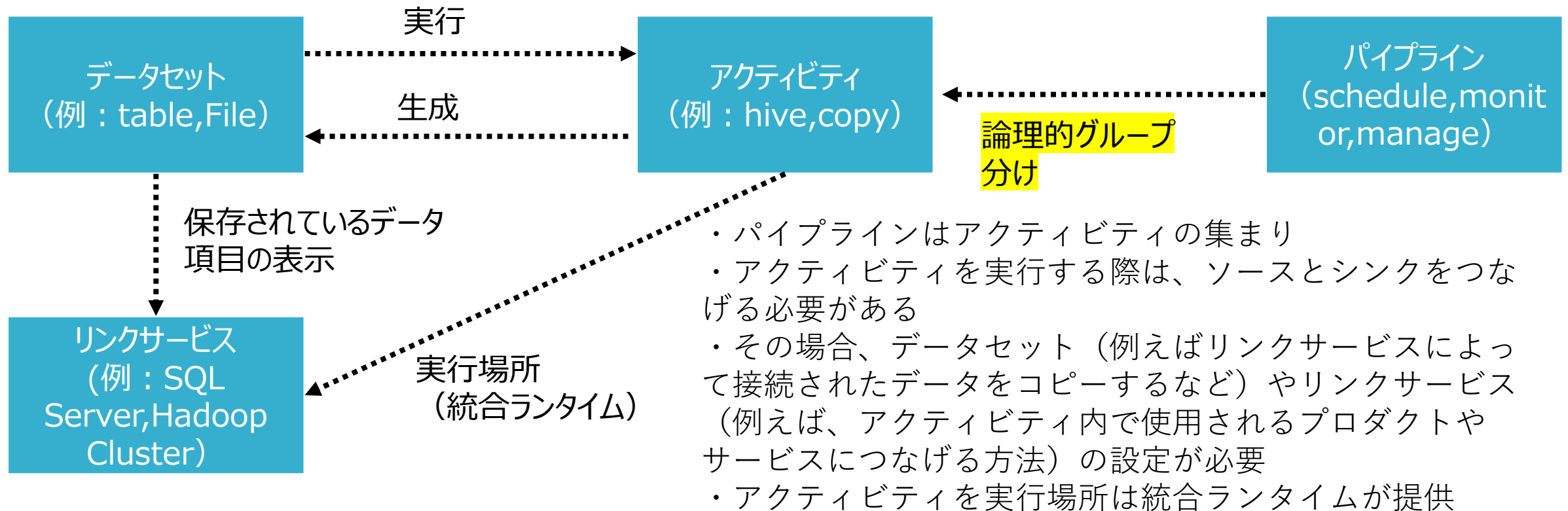
ローデータを分析しやすいように整形、加工、クレンジングします。加工したデータはグラフ化するなど可視化されます。

③ データ分析とガバナンス

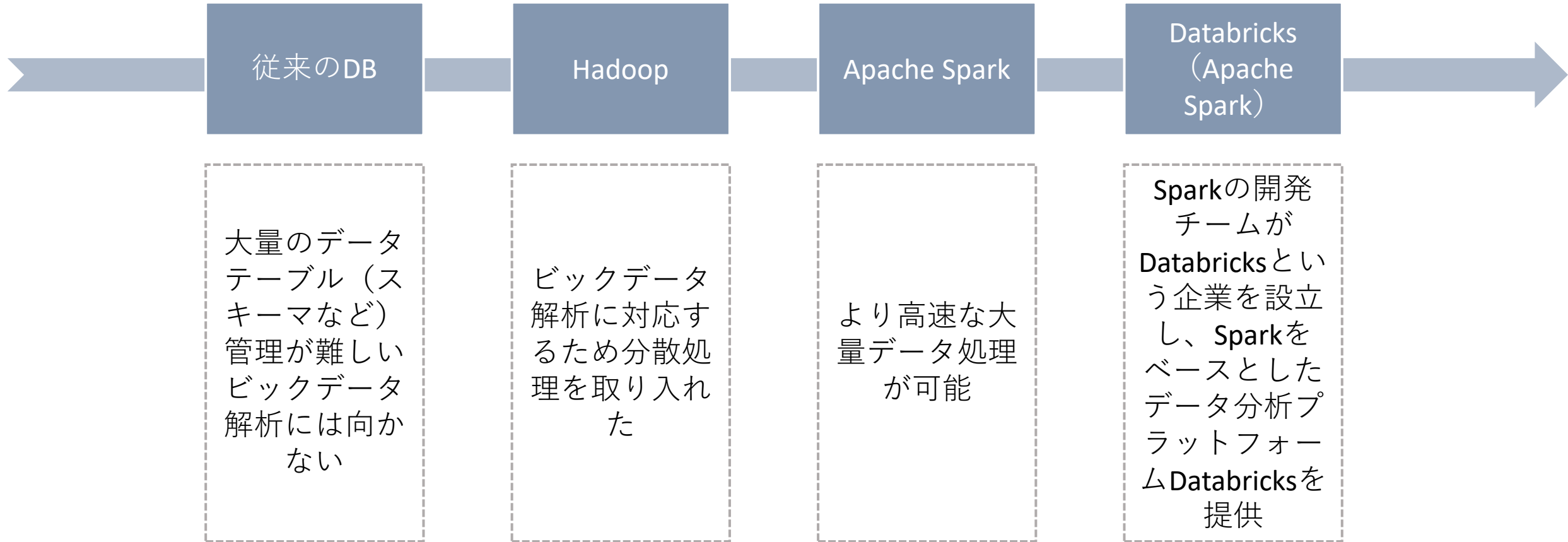
目的に合った結果が出せるよう分析手法を定めて、分析ツールを活用するなどして分析結果を導き出します。

Azure Data Factory

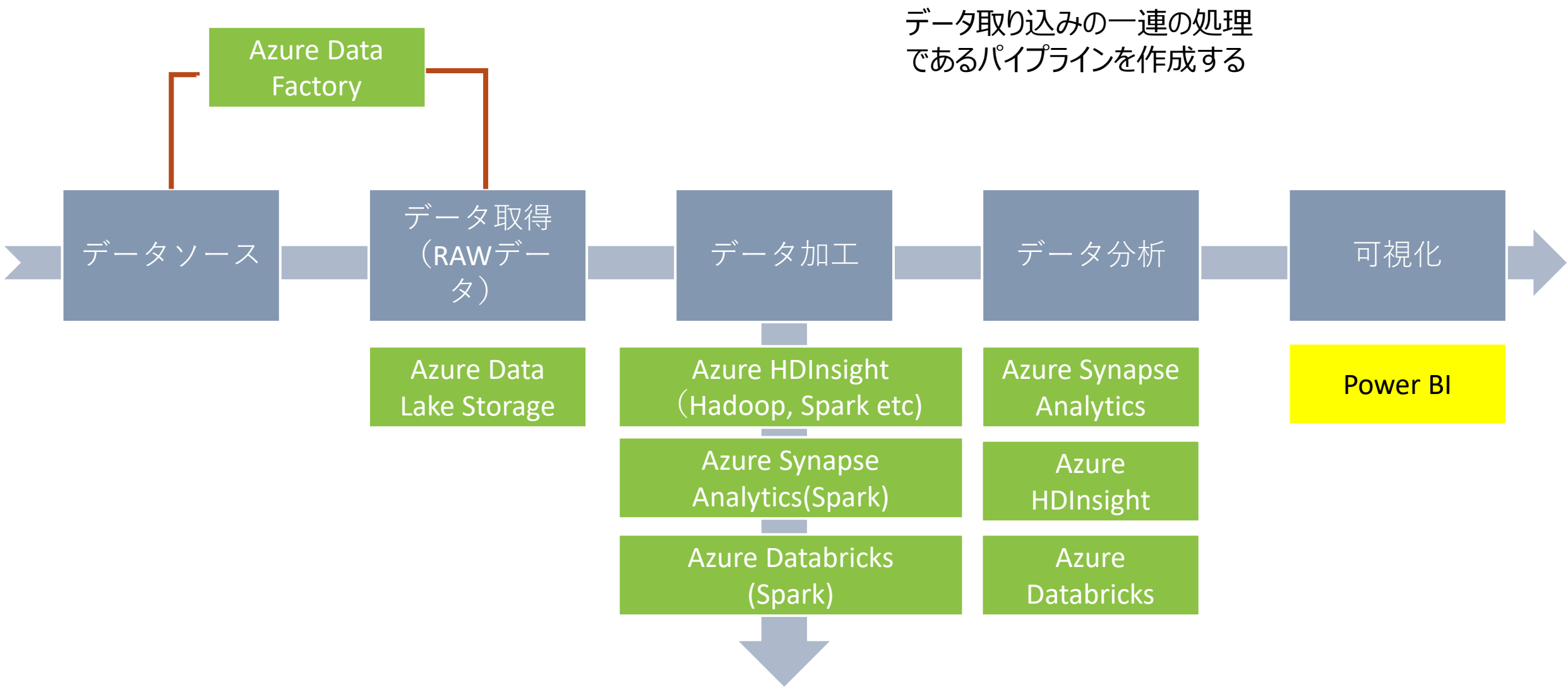
- SQLデータベースやファイルシステムなど多種多様なデータソースからデータを取得し、クレンジングしてデータストアに格納するといったデータの移動・変換を自動化するデータ統合サービスのこと
- Data Factoryには、リンクサービス、データセット、アクティビティ、パイプラインという4つの概念があります。



データ保管と処理の進化

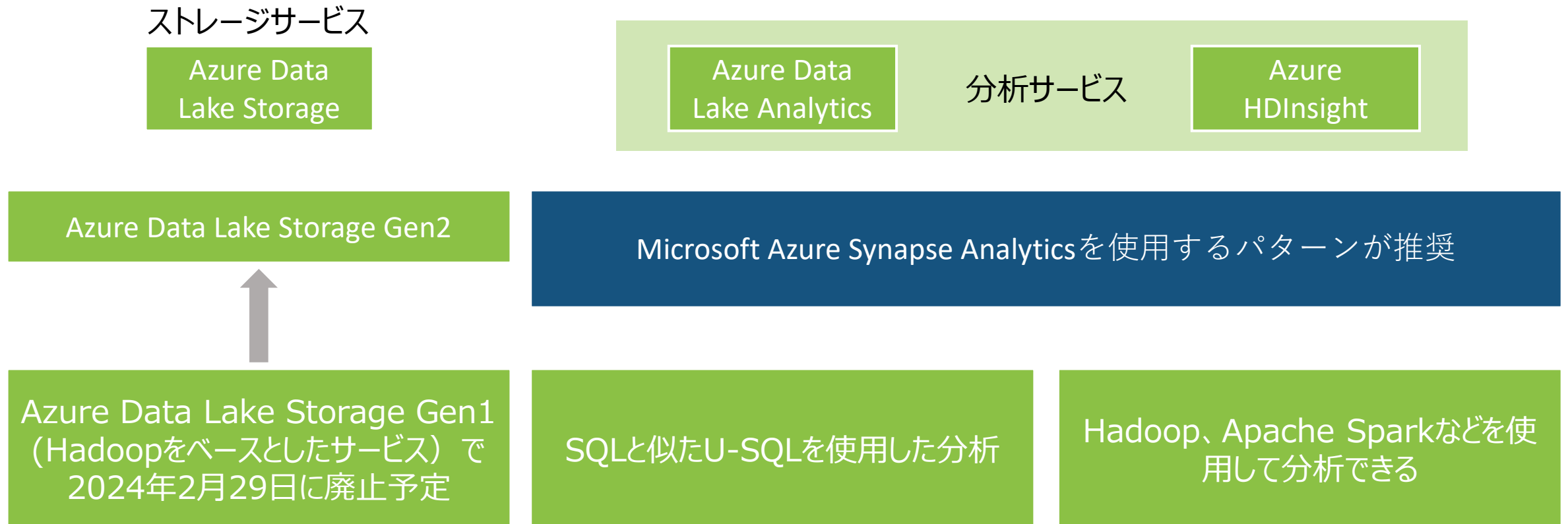


データ分析の流れを理解する



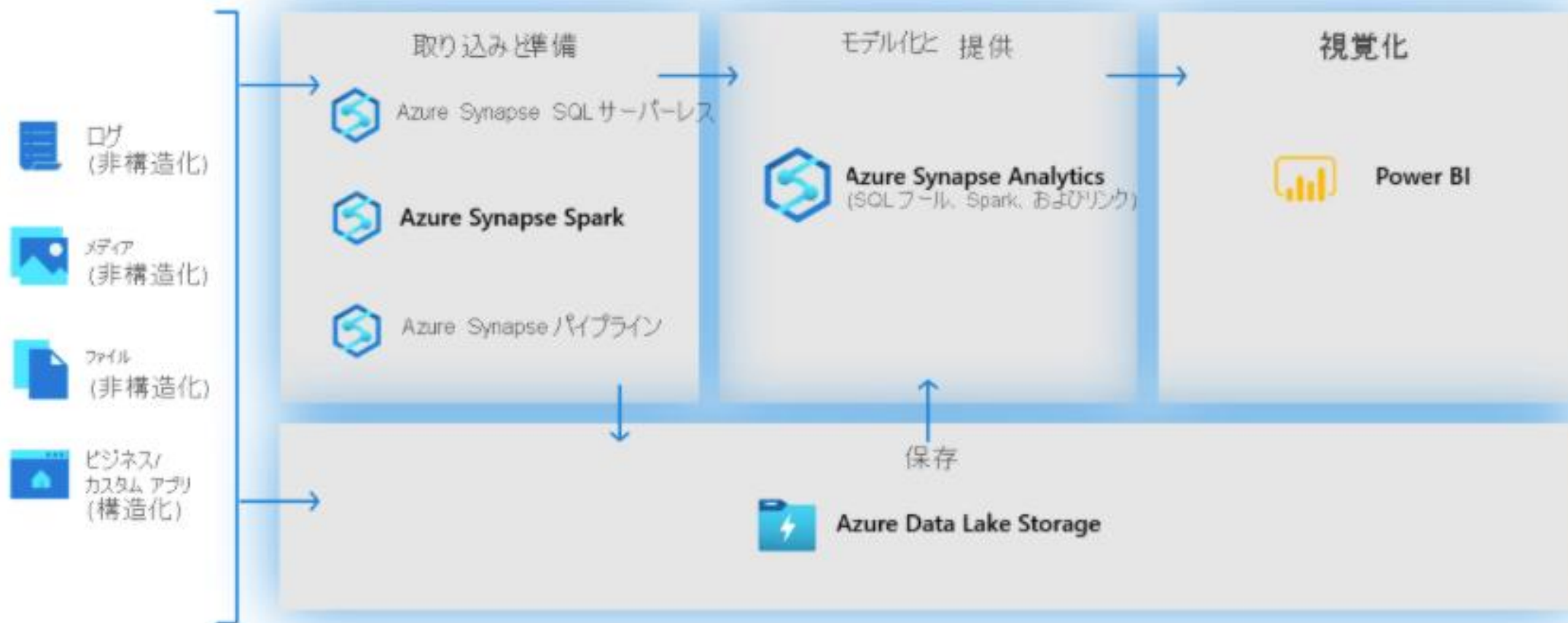
Azure Data Lake

- データレイクとは規模や形式にかかわらず全てのデータを一元的に保存できる格納庫のことです。データの形式は、RDBやCSVファイルのような規則性のある構造化データと、文書・画像・動画・音声など不規則な形式の非構造化データに大別できますが、あらゆるデータを**生データ（Raw Data）**のまま保管できることがデータレイクの最大の特徴



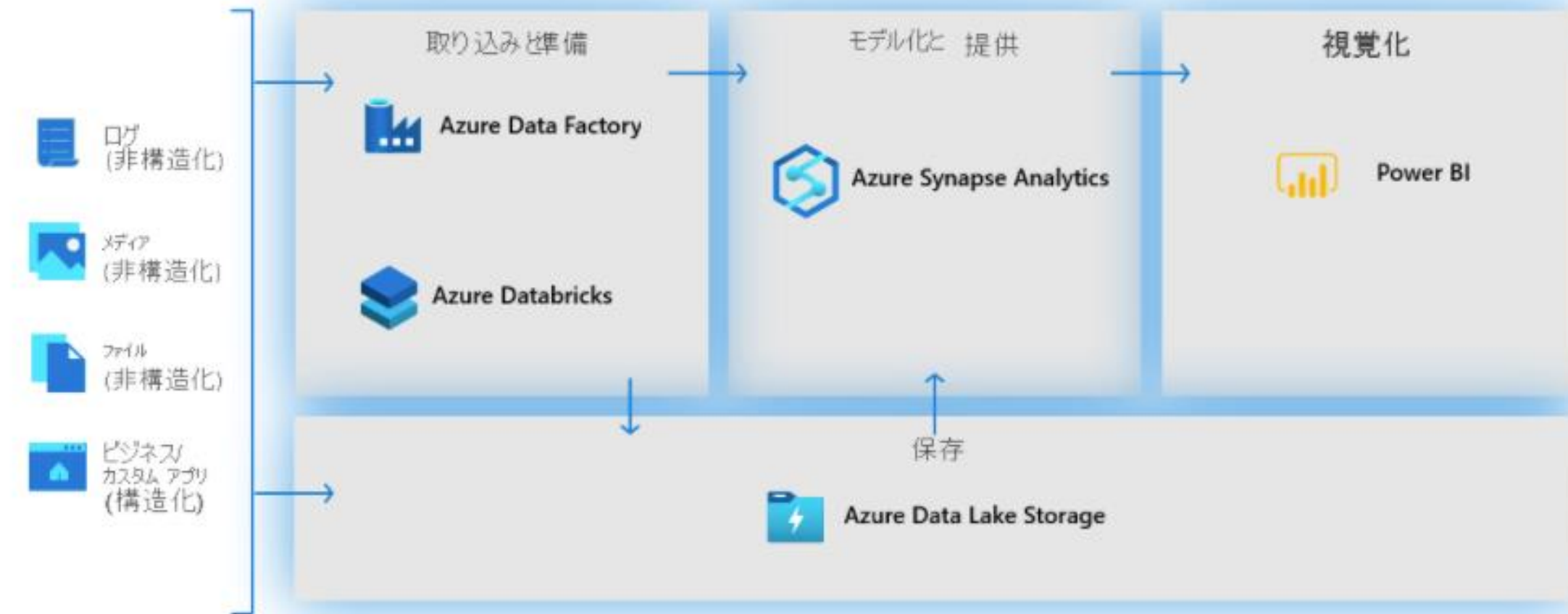
Azure Synapse Analyticsの構成

- Azure Synapse Analyticsのコンポーネントで使用できます。



Azure Synapse Analyticsの構成

- 既存サービスの一部をAzure Synapse Analyticsのコンポーネントに置き換えることも可能



メッセージとイベント

- メッセージ

- メッセージは、サービスによって生成される生データで、そのサービスではなく他の場所で使用または格納されます。メッセージにはそのメッセージを発生させるパイプラインをトリガーしたデータが含まれています。

- イベント

- イベントは、状態または状態変更の軽量の通知です。イベントの発行元は、イベントの処理方法に関して何も予測していません。通知の処理方法はイベントの処理者が決定します。

項目	メッセージ	イベント
データ	含まれる	含まれない（参照のみで軽量）
送信側が受信側を意識するか	する	しない
特徴	分散アプリで通信の処理を保証したい	ブロードキャストで利用、多くの場合一時的

Azureのメッセージングサービス

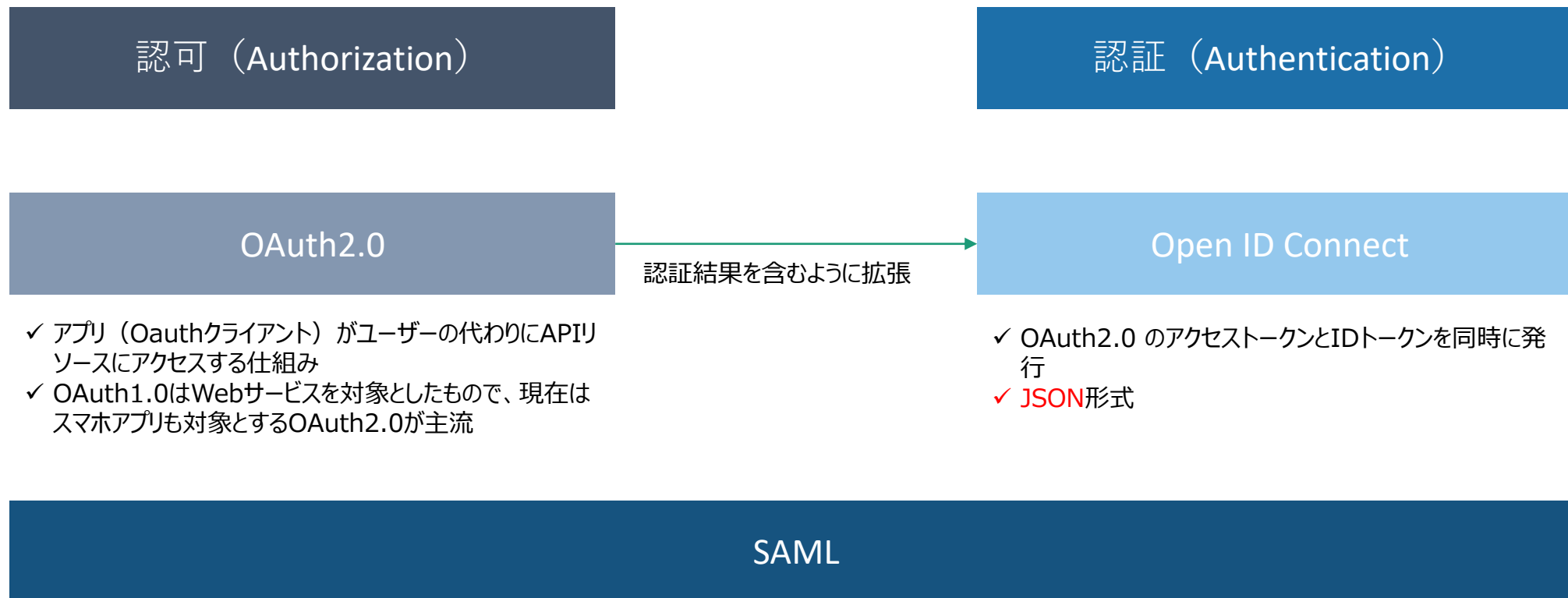
メッセージ

- **Queue Storage**
 - シンプルなメッセージキュー
 - データが多い場合
- **Service Bus**
 - キュー：単一の受信者（サブスクライバ）
 - トピック：複数の受信者（サブスクライバ）

イベント

- **Event Grid**
 - シンプルなイベント
- **Event Hubs**
 - 高スループット
 - 多数のパブリッシャー
 - セキュリティ
 - 回復性を持つイベント

SAML/Open ID Connect/OAuth 概要

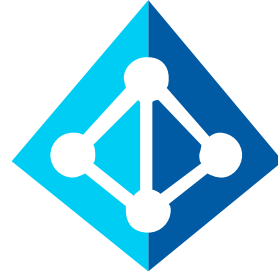


IdPにログインしてから、資格情報を再入力しなくても、SP (Salesforce、Boxなど) の多数の追加サービスにアクセスできるシングルサインオンのひとつ。SAMLは、IdPとサービスプロバイダー間で認証および承認データを交換してユーザーのIDとアクセス許可を確認し、サービスへのアクセスを許可または拒否するためのXMLベースの標準です。SAMLは古い標準なので、シングルページアプリケーション (SPA) やスマートフォンアプリケーションなどの最新のアプリケーションタイプの認証に使用するのは非常に困難です。そのために構築されていないからです。逆に、OIDCはそのようなアプリに最適です。

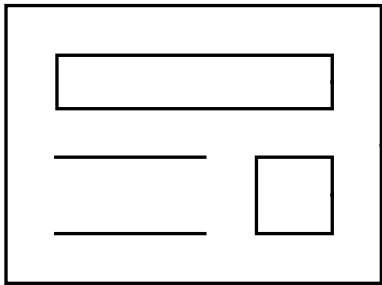
OpenID Connectは、さまざまなWebサービスなどの認証をひとつのIDでシームレスに実行する仕組みで、シングルサインオンの規格のひとつです。連携する際はユーザーに同意を求めるという動きが入る点に特徴があります。

OpenID ConnectはSAMLと似ていますが、SAMLはユーザーの同意なしで連携する・しないを判断する点が相違点です。

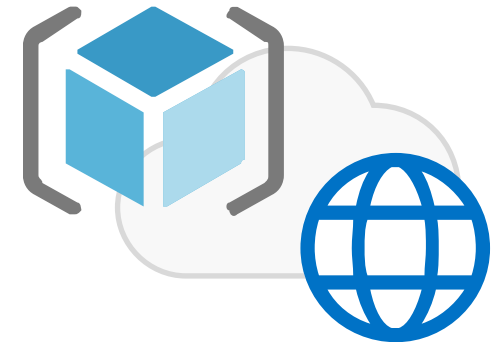
モダン認証の基本



Azure AD

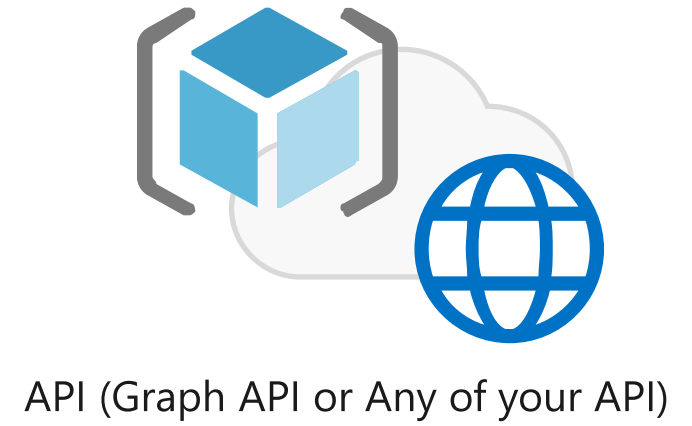
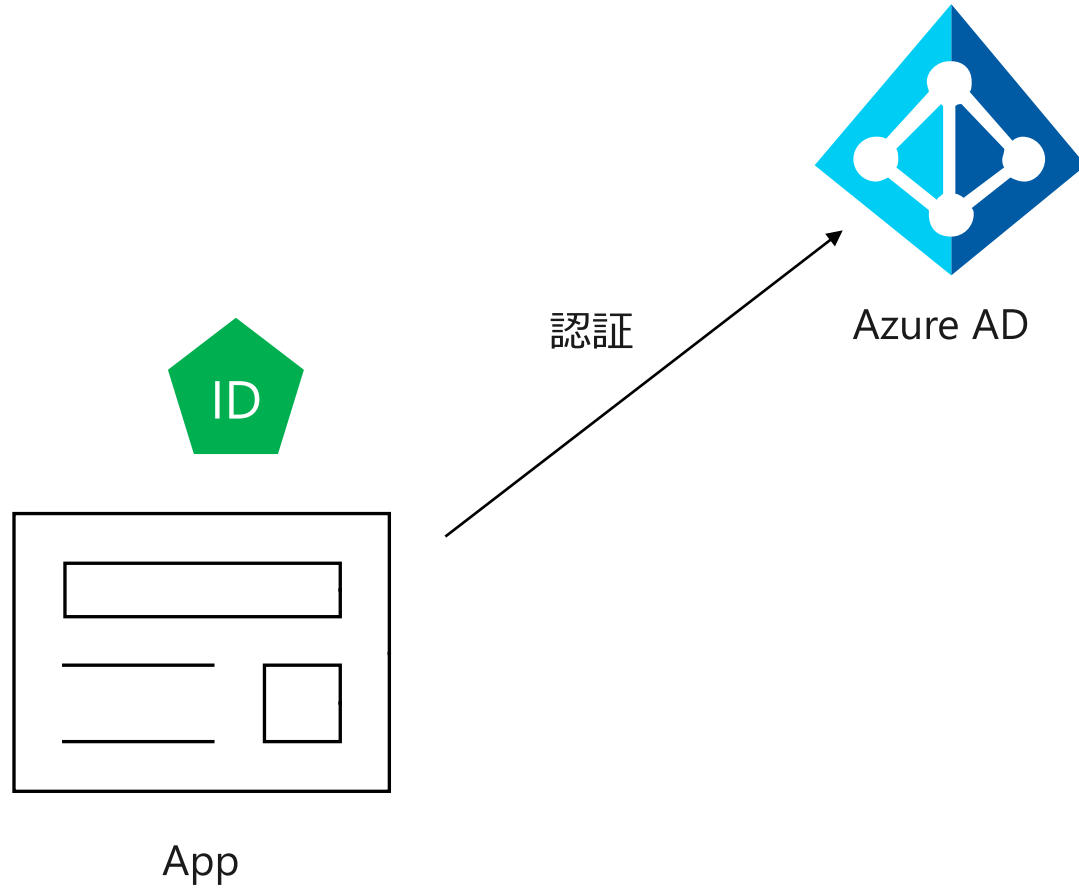


App



API (Graph API or Any of your API)

モダン認証の基本



ID token – 認証済み、ユーザー自身であることの証明

```
{ "typ": "JWT", "alg": "RS256", "kid": "1LTMzakihiRla_8z2BEJVeWMqo" }.  
{ "ver": "2.0",  
"iss": "https://login.microsoftonline.com/3338040d-6c67-4c5b-b112-36a304b66dad/v2.0",  
"aud": "6cb04018-a3f5-46a7-b995-940c78f5aef3",  
"exp": 1536361411, "iat": 1536274711, "nbf": 1536274711,  
"sub": "AAAAAAAAAAAAAAAAAAAAAAAAAAIkzqFVrSaSaFHy782bbtaQ",  
"name": "Abe Lincoln",  
"preferred_username": "AbeLi@microsoft.com",  
"oid": "00000000-0000-0000-66f3-3332eca7ea81",  
"tid": "3338040d-6c67-4c5b-b112-36a304b66dad",  
}  
.[Signature]
```

ID Token は **JWT** 形式で表現される (JWT = JSON Web Token)

ID token - 認証済み、ユーザー自身であることの証明

```
{ "typ": "JWT", "alg": "RS256", "kid": "1LTMzakihIRla_8z2BEJVXeWMqo" }.
```

```
{ "ver": "2.0",
```

Token を発行した IdP

```
"iss": "https://login.microsoftonline.com/3338040d-6c67-4c5b-b112-36a304b66dad/v2.0",
```

```
"aud": "6cb04018-a3f5-46a7-b995-940c78f5aef3",
```

Token を受け取り利用するアプリケーション

```
"exp": 1536361411, "iat": 1536274711, "nbf": 1536274711,
```

トークンの有効期間

"sub": "AAAAAAAAAAAAAAAAAAAAAAAAAAIkzqFVrSaSaFHy782bbtαα ,

```
"name": "Abe Lincoln",
```

```
"preferred_username": "AbeLi@microsoft.com",
```

ユーザーの一意識別子 (アプリ固有)

"oid": "00000000-0000-0000-66f3-3332eca7ea81",

```
"tid": "3338040d-6c67-4c5b-b112-36a304b66dad",
```

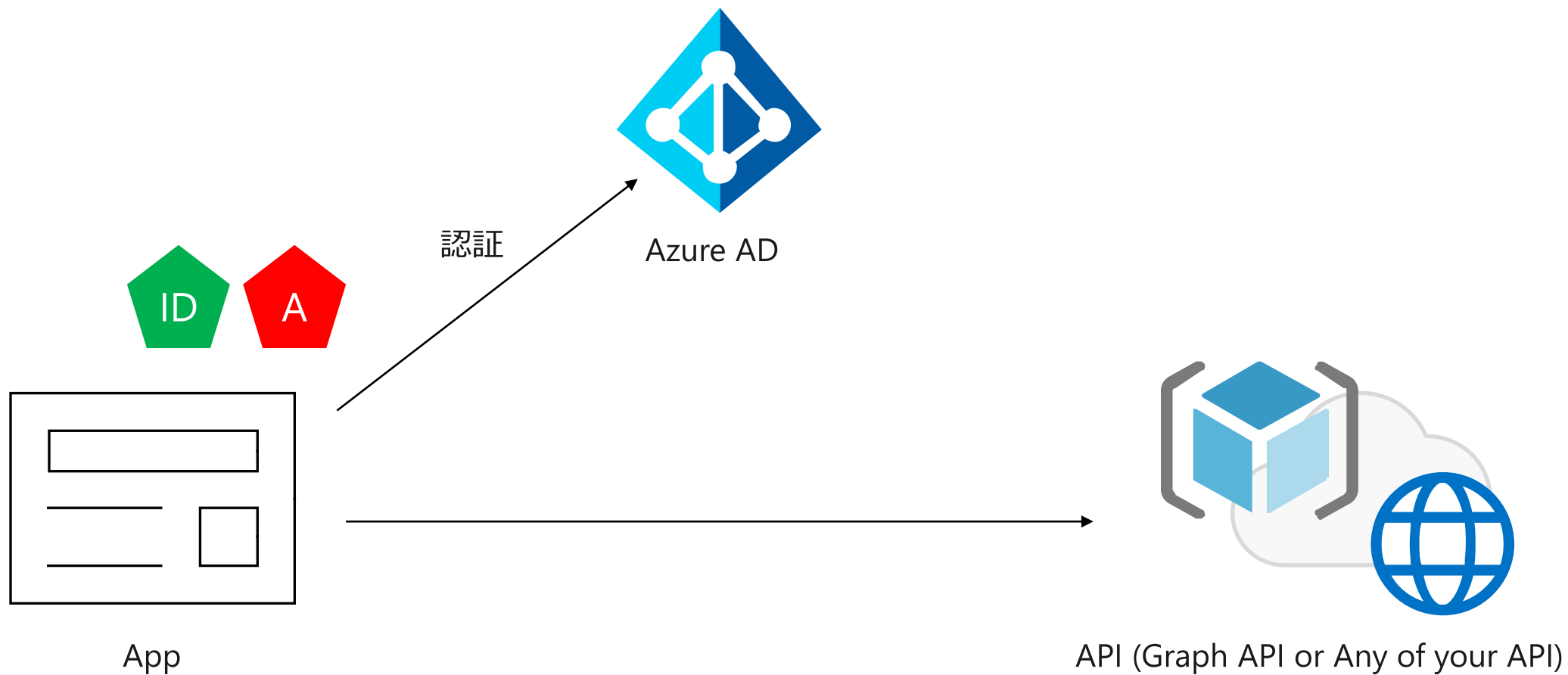
ユーザー属性値

 $\}$

[Signature]

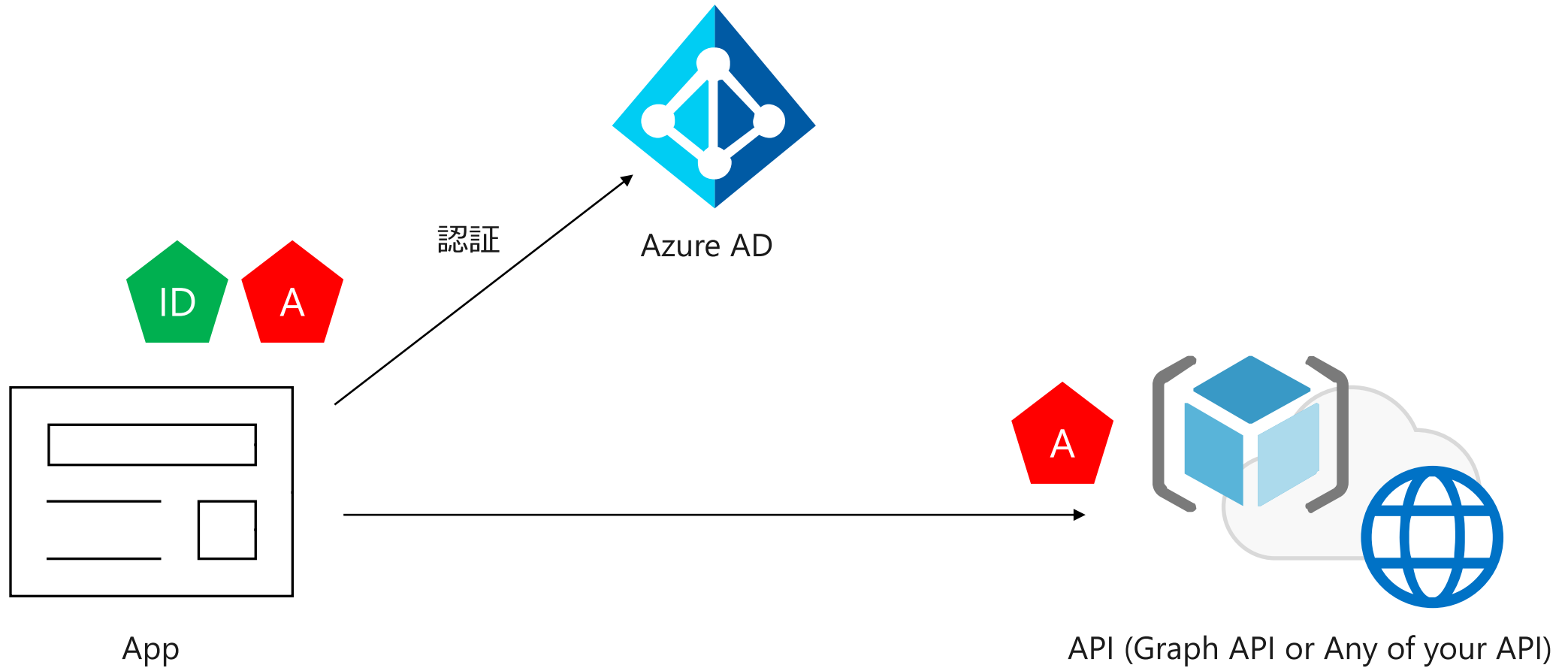
テナント固有のユーザー ID/テナント ID

モダン認証の基本

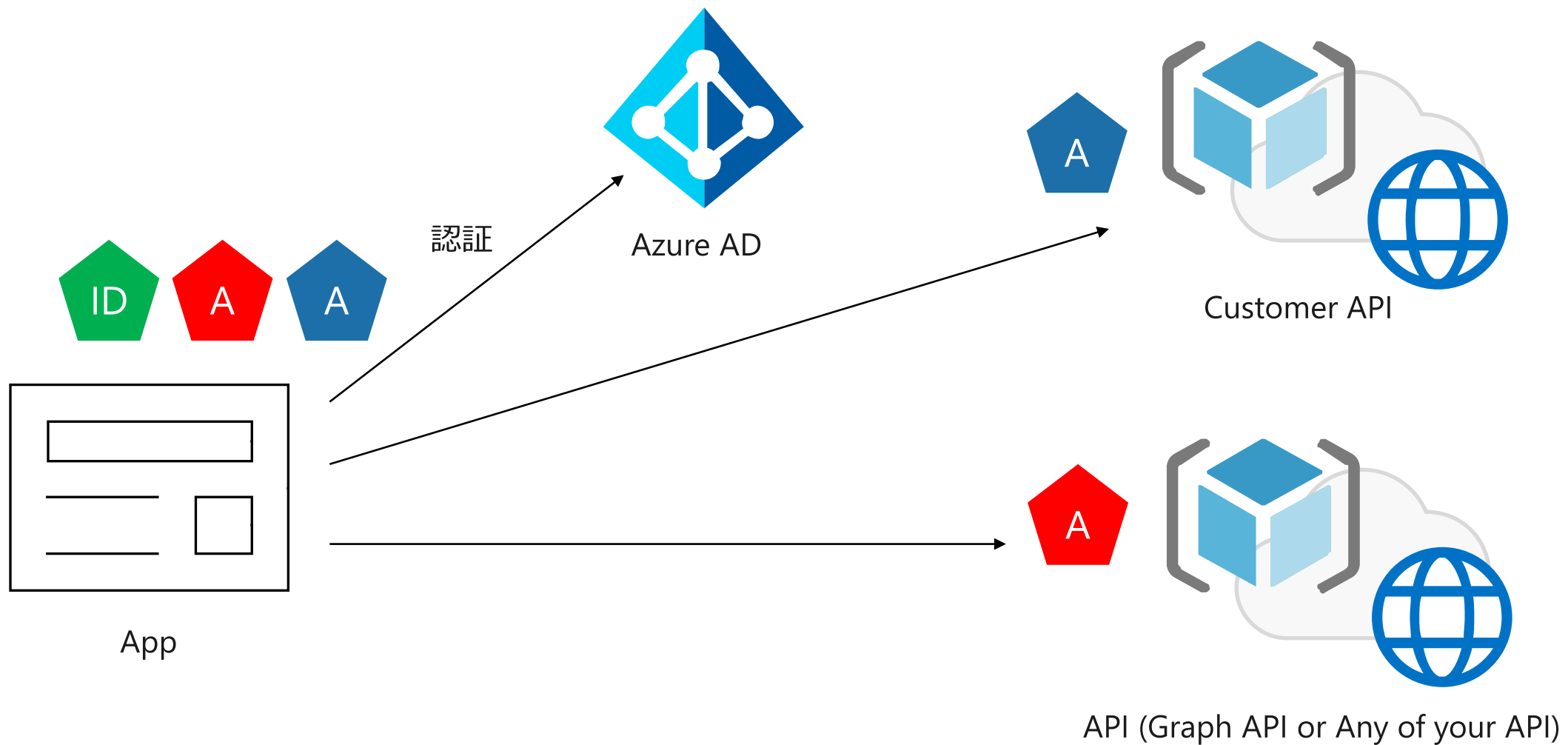


eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6Imk2bEdrM0ZaenhSY1ViMkMzbkVRN3N5SEps
WSJ9.eyJhdWQiOiI2ZTc0MTcyYi1iZTU2LTQ4NDMtOWZmNC1lNjZhMzliYjEyZTMiLCJpc3MiOiJodH
RwczoVL2xvZ2luLm1pY3Jvc29mdG9ubGluZS5jb20vNzJmOTg4YmYtODZmMS00MWFMLTkxYWlt
MmQ3Y2QwMTFkYjQ3L3YyLjAiLCJpYXQiOiE1MzcyMzEwNDgsIm5iZil6MTUzNzIzMTA0OCwiZXhw
ljoxNTM3MjM0OTQ4LCJhaW8iOiJBWFFBaS84SUFBQUF0QWFaTG8zQ2hNaWY2S09udHRSQjdIQ
nEOL0RjY1F6amNKR3hQWXkvQzNqRGFOR3hYZDZ3TkIJVKdSZ2hOUm53SjFsT2NBbk5aY2p2a295
ckZ4Q3R0djMzMTQwUmhvT0ZKNGJDQ0dWdW9DYWcxZDU9UVdlYmJlyZ0h3TFBZUS91Zjc5UVgrM
EtJaWpkcm1wNjlSY3R6bVE9PSIsImF6cCI6IjZlNzQxNzJiLWJlNTYtNDg0My05ZmY0LWU2NmEzOWJ
iMTJlMyIsImF6cGFjcil6IjAiLCJuYW1lIjoiaWJlIExpbmNvbG4iLCJvaWQiOiI2OTAyMjIzS1mZjFhLTRk
NTYtYWJkMS03ZTRmN2QzOGU0NzQiLCJwcmVmZXRjaWZWRfdXNlcmlm5hbWUiOiJhYmVsUBtaWNy
b3NvZnQuY29tliwicmgiOiJJliwic2NwIjoiaWJlIWNjZXNzX2FzX3VzZXIiLCJzdWIiOiJIS1pwZmFlVdhZGV
Pb3VZbGl0anJLUtmZIRtMjlyWDVyclYzeERxZktRliwidGlkljoiNzJmOTg4YmYtODZmMS00MWFMLT
kxYWltMmQ3Y2QwMTFkYjQ3liwidXRpljoiZnFpQnFYTFBqMGVRYTgyUy1JWUZBQSIsInZlcil6IjluM
CJ9.pj4N-w_3Us9DrBLfpCt

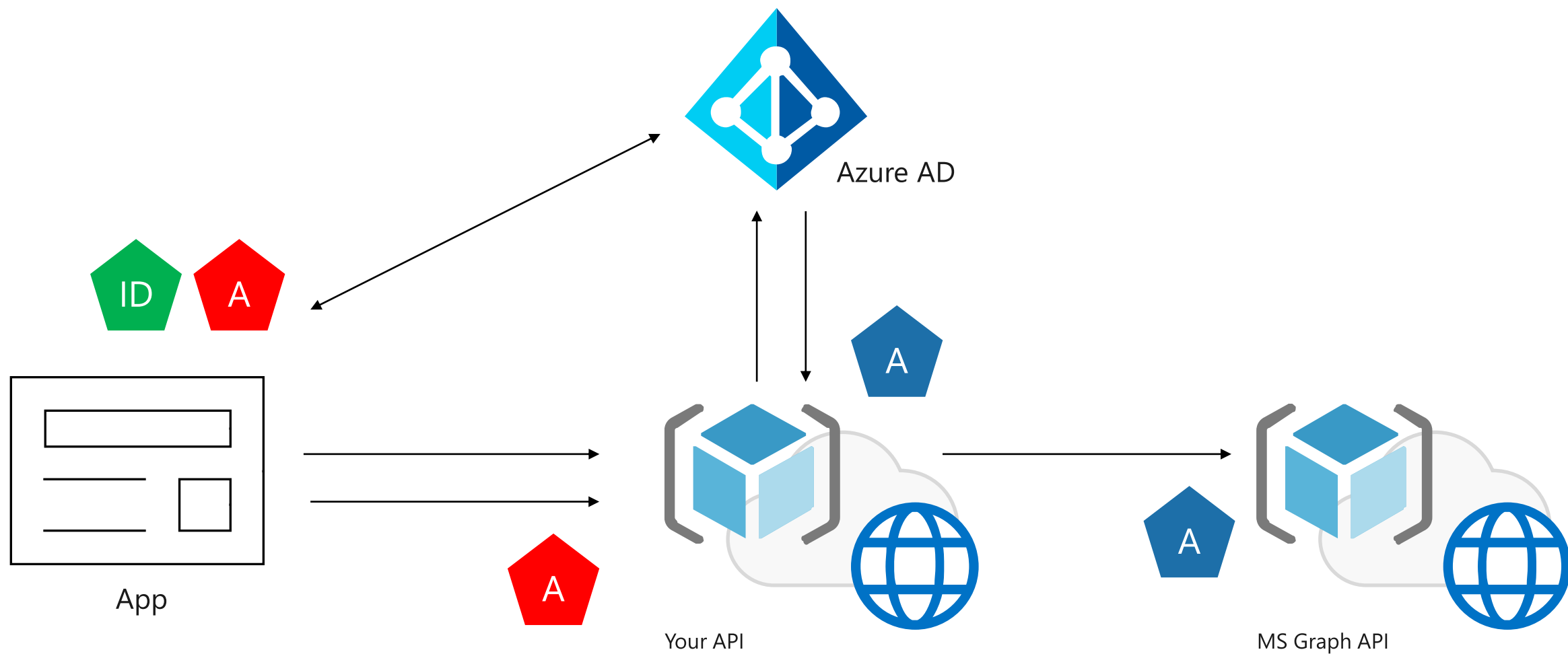
モダン認証の基本



モダン認証の基本



モダン認証の基本



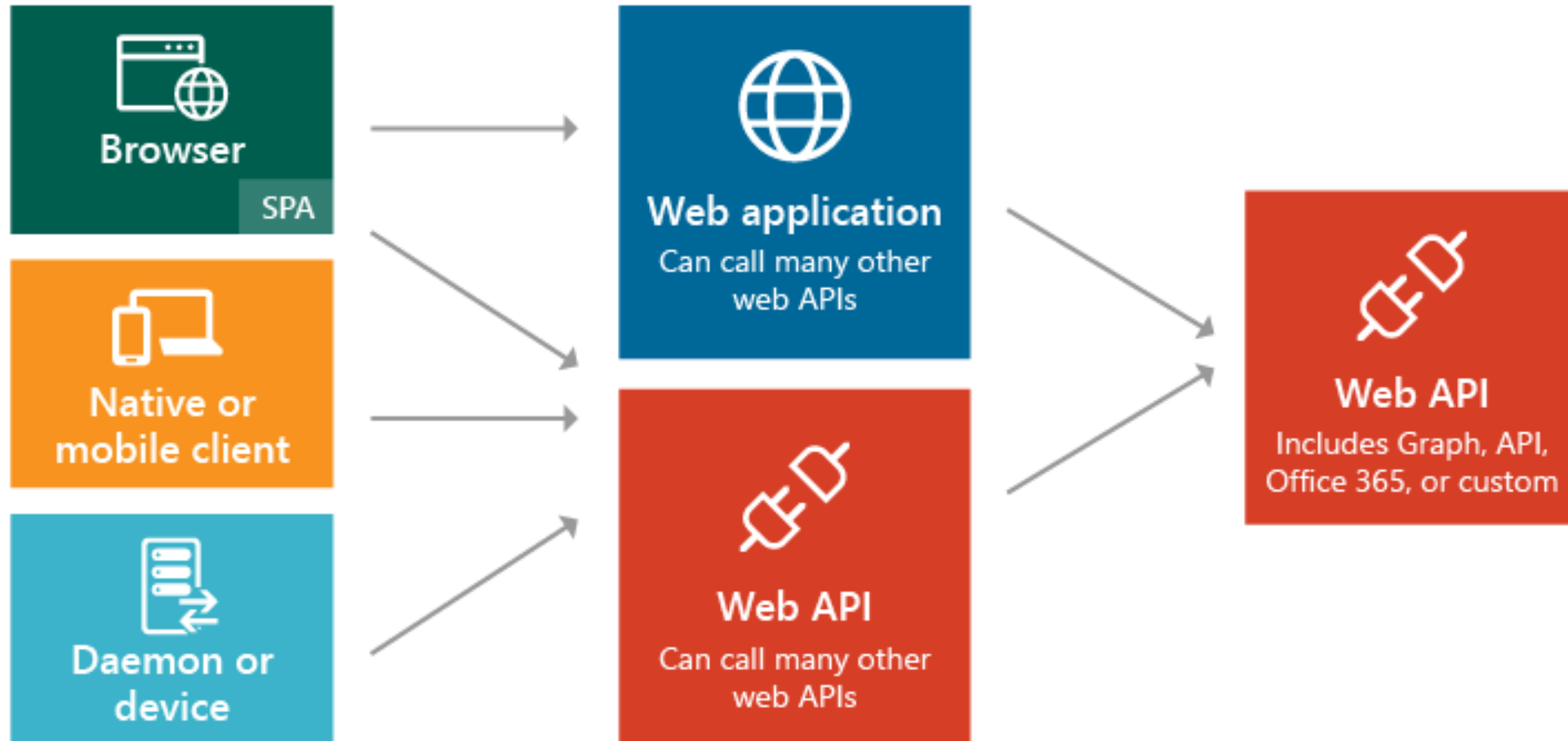
モダン認証の基本 – IT 管理者がおさえるポイント

ID Token/Access Token は Azure AD から発行される

- ID Token はアプリに本人の確認のために利用される
- Access Token は API を Call する際に利用される

Access Token は API ごとに必要となる

どんなアプリを開発するのか理解したいときの地図



どのパターンだとしても Azure AD として必要なのは “アプリケーションの登録”

アプリケーションの登録

すべてのパターンでこの作業が必要

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+/)

ホーム > YK Demo

YK Demo | アプリの登録

概要

はじめに

プレビュー機能

問題の診断と解決

管理

ユーザー

グループ

External Identities

ロールと管理者

管理単位

エンタープライズ アプリケーション

デバイス

アプリの登録

Identity Governance

アプリケーション プロキシ

ライセンス

Azure AD Connect

カスタム ドメイン名

モビリティ (MDM および MAM)

パスワード リセット

会社のブランド

ユーザー設定

プロビジョニング

新規登録

エンドポイント

トラブルシューティング

ダウンロード

新しいアプリ登録の検索のプレビューをお試しください。クリックするとプレビューが有効になります。

2020 年 6 月 30 日以降、Azure Active Directory 認証ライブラリ (ADAL) および A 供されません。アプリケーションを、Microsoft 認証ライブラリ (MSAL) および Microsoft

すべてのアプリケーション

所有しているアプリケーション

削除されたアプリ

名前またはアプリケーション ID を入力し始めると結果がフィルター処理されます

このアカウントは、

サポートされているアカウントの種類

このアプリケーションを使用したりこの API にアクセスしたりできるのはだれですか?

☒ この組織ディレクトリのみに含まれるアカウント (YK Demo のみ - シングル テナント)

☐ 任意の組織ディレクトリ内のアカウント (任意の Azure AD ディレクトリ - マルチテナント)

☐ 任意の組織ディレクトリ内のアカウント (任意の Azure AD ディレクトリ - マルチテナント) と個人の Microsoft アカウント (Skype など)

☐ 個人用 Microsoft アカウントのみ

選択に関する詳細...

リダイレクト URI (省略可能)

ユーザー認証が成功すると、この URI に認証応答を返します。この時点での指定は省略可能で、後ほど変更できますが、ほとんどのります。

Web

例: https://example.com/auth

作業に使用しているアプリをこちらで登録します。ギャラリー アプリと組織外の他のアプリを [エンタープライズ アプリケーション] から追加

続行すると、Microsoft プラットフォーム ポリシーに同意したことになります

登録

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+/)

ホーム > YK Demo

YK Demo | アプリの登録

ロールと管理者

管理単位

エンタープライズ アプリケーション

デバイス

アプリの登録

Identity Governance

アプリケーション プロキシ

ライセンス

Azure AD Connect

カスタム ドメイン名

モビリティ (MDM および MAM)

パスワード リセット

会社のブランド

ユーザー設定

プロバティ

セキュリティ

監視

サインイン

監査ログ

プロビジョニング ログ (プレビュー)

ログ

新規登録

エンドポイント

トラブルシューティング

ダウンロード

新しいアプリ登録の検索のプレビューをお試しください。クリックするとプレビューが有効になります。

2020 年 6 月 30 日以降、Azure Active Directory 認証ライブラリ (ADAL) および A 供されません。アプリケーションを、Microsoft 認証ライブラリ (MSAL) および Microsoft

すべてのアプリケーション

所有しているアプリケーション

削除されたアプリ

名前またはアプリケーション ID を入力し始めると結果がフィルター処理されます

このアカウントは、

サポートされているアカウントの種類

このアプリケーションを使用したりこの API にアクセスしたりできるのはだれですか?

☒ この組織ディレクトリのみに含まれるアカウント (YK Demo のみ - シングル テナント)

☐ 任意の組織ディレクトリ内のアカウント (任意の Azure AD ディレクトリ - マルチテナント)

☐ 任意の組織ディレクトリ内のアカウント (任意の Azure AD ディレクトリ - マルチテナント) と個人の Microsoft アカウント (Skype など)

☐ 個人用 Microsoft アカウントのみ

選択に関する詳細...

リダイレクト URI (省略可能)

ユーザー認証が成功すると、この URI に認証応答を返します。この時点での指定は省略可能で、後ほど変更できますが、ほとんどのります。

Web

例: https://example.com/auth

作業に使用しているアプリをこちらで登録します。ギャラリー アプリと組織外の他のアプリを [エンタープライズ アプリケーション] から追加

続行すると、Microsoft プラットフォーム ポリシーに同意したことになります

登録

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+/)

ホーム > YK Demo

YK Demo | アプリの登録

ロールと管理者

管理単位

エンタープライズ アプリケーション

デバイス

アプリの登録

Identity Governance

アプリケーション プロキシ

ライセンス

Azure AD Connect

カスタム ドメイン名

モビリティ (MDM および MAM)

パスワード リセット

会社のブランド

ユーザー設定

プロバティ

セキュリティ

監視

サインイン

監査ログ

プロビジョニング ログ (プレビュー)

ログ

新規登録

エンドポイント

トラブルシューティング

ダウンロード

新しいアプリ登録の検索のプレビューをお試しください。クリックするとプレビューが有効になります。

2020 年 6 月 30 日以降、Azure Active Directory 認証ライブラリ (ADAL) および A 供されません。アプリケーションを、Microsoft 認証ライブラリ (MSAL) および Microsoft

すべてのアプリケーション

所有しているアプリケーション

削除されたアプリ

名前またはアプリケーション ID を入力し始めると結果がフィルター処理されます

このアカウントは、

サポートされているアカウントの種類

このアプリケーションを使用したりこの API にアクセスしたりできるのはだれですか?

☒ この組織ディレクトリのみに含まれるアカウント (YK Demo のみ - シングル テナント)

☐ 任意の組織ディレクトリ内のアカウント (任意の Azure AD ディレクトリ - マルチテナント)

☐ 任意の組織ディレクトリ内のアカウント (任意の Azure AD ディレクトリ - マルチテナント) と個人の Microsoft アカウント (Skype など)

☐ 個人用 Microsoft アカウントのみ

選択に関する詳細...

リダイレクト URI (省略可能)

ユーザー認証が成功すると、この URI に認証応答を返します。この時点での指定は省略可能で、後ほど変更できますが、ほとんどのります。

Web

例: https://example.com/auth

作業に使用しているアプリをこちらで登録します。ギャラリー アプリと組織外の他のアプリを [エンタープライズ アプリケーション] から追加

続行すると、Microsoft プラットフォーム ポリシーに同意したことになります

登録

WD	Webinar demo app1
BO	Box
SA	Sample app data
WD	Webinar Demo2 - Daemon
NE	NetDocuments
TD	Tokens Demo React
MA	mailgate
PS	P2P Server
AW	Amazon Web Services (AWS)
MA	MailGates
BO	Box
CP	cp.com

サポートされているアカウントの種類

この組織ディレクトリのみに含まれるアカウント (シングルテナント)

通常の LOB (自社開発) アプリ開発で利用するのはこちら

任意の組織ディレクトリ内のアカウント (マルチテナント)

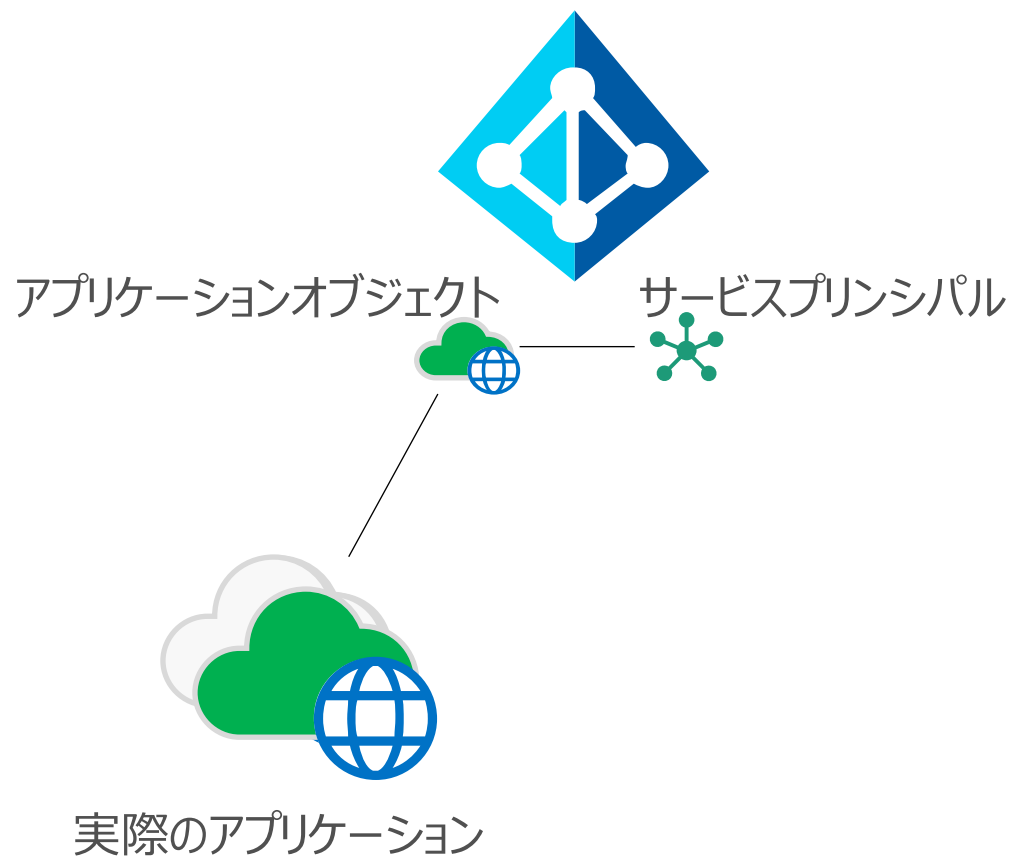
開発したアプリをグループ会社他テナントで利用などのシーン

特別な理由がない限りシングルテナント設定で作成するはずなので、テナントにマルチテナントアプリがアプリケーションとして存在していたら要チェック

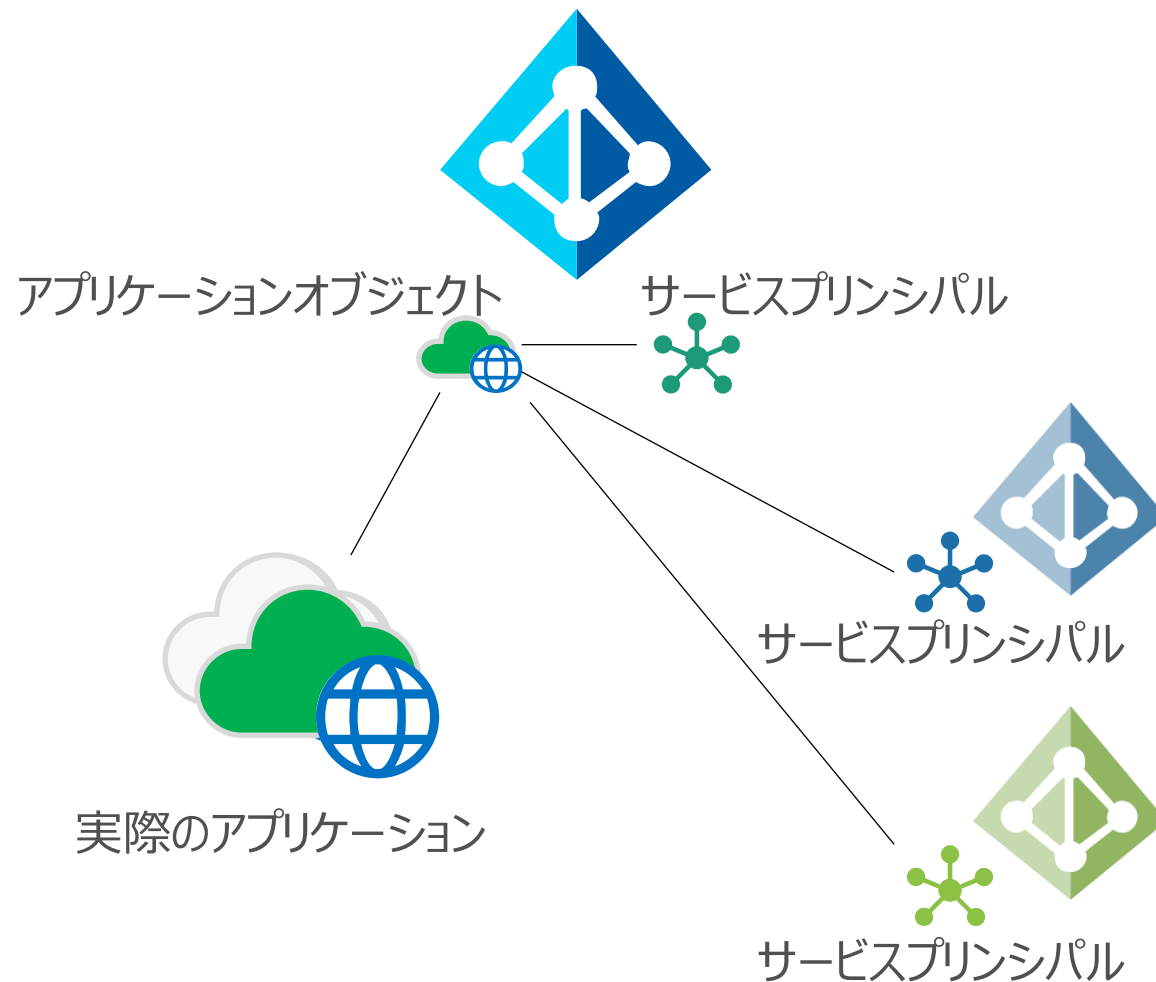
SaaS でマルチテナントアプリとして構築されているアプリは多い、なので、エンタープライズアプリとして存在するというのはよくある

テナントに作成されるオブジェクトの関係性

シングルテナントアプリ



マルチテナントアプリ



サービスプリンシパルはアプリケーションを表現する形

“エンタープライズアプリケーション” より確認できる

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+)

📧

📄

🗨️

⚙️

?

😊

webin
YK DEMO

ホーム > YK Demo > エンタープライズ アプリケーション

🏠

エンタープライズ アプリケーション | すべてのアプリケーション ...

YK Demo - Azure Active Directory

概要

📌 概要

🔧 問題の診断と解決

管理

🏠 すべてのアプリケーション

📁 アプリケーション プロキシ

⚙️ ユーザー設定

📁 コレクション

セキュリティ

🔑 条件付きアクセス

🔑 同意とアクセス許可

アクティビティ

🔄 サインイン

📊 使用状況と分析情報

📄 監査ログ

👤 プロビジョニング ログ (プレビュー)

🔑 アクセス レビュー

👤 管理者の同意要求

トラブルシューティング + サポート

←

+

新しいアプリケーション

≡

列

🖼️

プレビュー機能

💡

フィードバックがある場合

📌

新しいエンタープライズ アプリ検索のプレビューをお試しください。クリックするとプレビューが有効になります。 →

🏠	Office 365 SharePoint Online	http://office.microsoft.com/sharepoint/	ae056d9e-3dfc-4020-a77d-5b1d6fbfb881	00000003-0000-00ff
🏠	Office 365 Yammer	https://products.office.com/yammer/	eb49f537-ceb5-4276-a7c5-44b0f1406a17	00000005-0000-00ff
🏠	OneNote		79b5e030-198d-47f8-a1c8-aa5d620e04...	2d4d3d8e-2be3-4b
🏠	Outlook Groups		74251bbe-8751-4143-b187-41b7e6b35...	925eb0d0-da50-46
🏠	Power BI Service		61d8ea8e-bb12-4238-9c83-a1f1c24477...	00000009-0000-00ff
🏠	Salesforce	https://www.microsoft.com/	e85617b3-4067-47ab-a048-00150daf3dff	bcf54e42-ac4b-4b6
🏠	Skype for Business Online		f10e8aba-15c0-4b79-aeb5-842adaf538d1	00000004-0000-00ff
🏠	Token Demo Cactus API		431bc2a7-82fe-4235-985e-5d63d958dc...	deb1d876-e755-4b
🏠	Tokens Demo Herbs API		ba3b50e0-9dbf-4f47-b7b0-a3aca845e00b	5f5d6454-5cc8-444
🏠	Tokens Demo React		4255d550-cbd7-4f67-95db-4750a1ad4f...	38a71684-f89a-458
🏠	Webinar demo app1		bdeb2f1d-cfa0-4861-96b4-549489bdb0...	5588ff4b-8a50-429
🏠	Webinar Demo1		36aea5dd-419f-41e4-b3e0-791d2e704c...	99b53b26-1a2e-4b
🏠	Webinar Demo2 - Daemon		af4e7649-5ddb-4085-84d9-a39709472a...	a9c1a1fc-7269-475
🏠	Windows Virtual Desktop	https://mrs-Prod.ame.gbl/mrs-RDInfra-prod	9f925b63-3b1e-4987-8f5e-32fdac1a5c14	5a0aa725-4958-4b6
🏠	Windows Virtual Desktop Client		140444b3-ffa5-4c6a-9f7c-e4249713f6c7	fa4345a4-a730-423
🏠	Woodgrove Business Customer signin		986e566e-35c4-41df-89c0-82ddb50ec4...	b6dcc583-e7c9-4e5
🏠	試験アプリ		9172aade-81f5-4134-9068-961aa38e65...	745b5475-f545-47c

アプリケーションが二か所に出てくる謎について

アプリケーション

- アプリケーションの定義
- サービスプリンシパルを作るためのテンプレート
- トークン発行の方法、アプリからアクセスできるリソースなどの基本情報が格納されている

サービスプリンシパル

- アプリケーションのインスタンス
- 誰にトークンを発行していいのか
- 特定のプロパティがアプリケーションオブジェクトから継承される
- アプリケーションにアクセスできるユーザーや、そのアプリからアクセスできるリソースとそのユーザーの組み合わせ（アクセス許可の同意）の定義を保持している
- どういった条件でトークンを発行するのか（＝条件付きアクセスポリシー）はサービスプリンシパルを対象に設定する

運用上の各ブレードの使い分け








エンタープライズアプリケーション

- サービスプリンシパルの一覧
- SAML アプリの管理
- App Proxy アプリの管理
- パスワード SSO アプリの管理
- アプリへのアクセス許可の管理

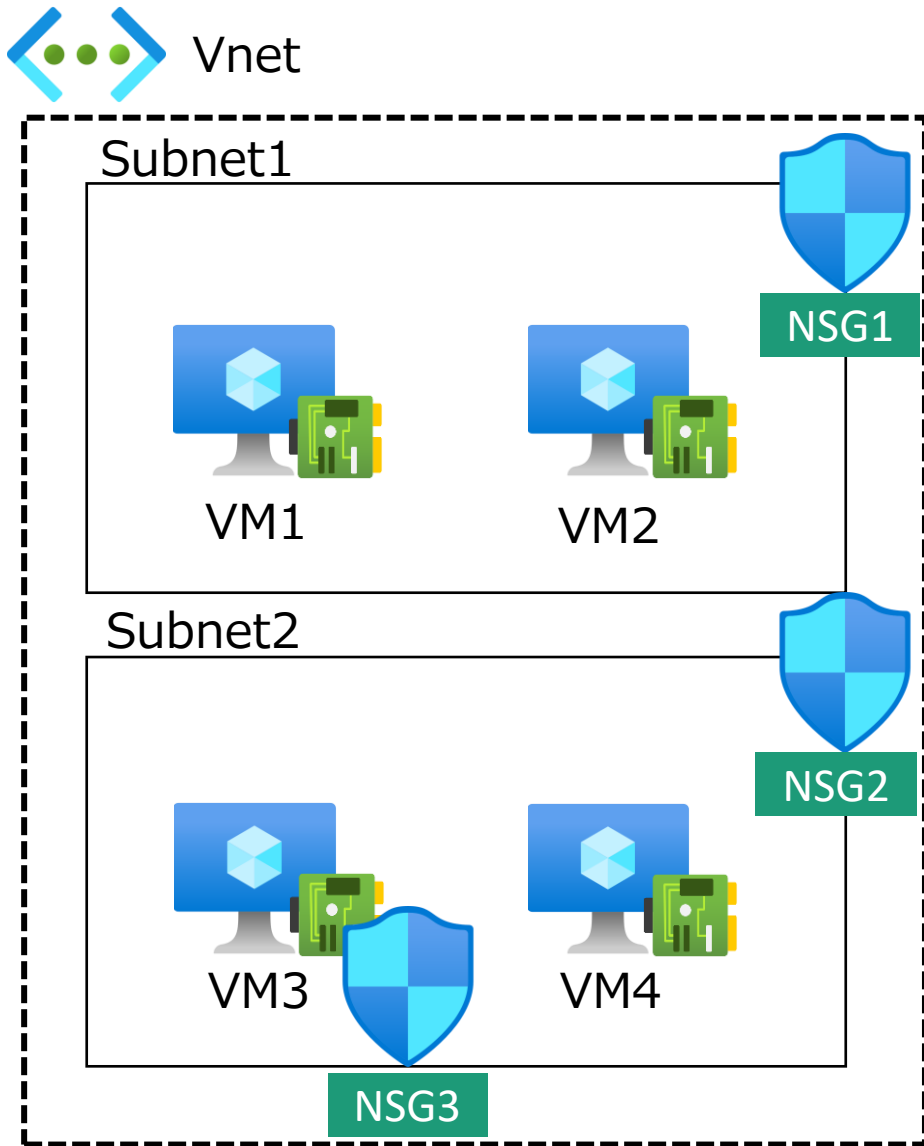
アプリの登録

- アプリケーションオブジェクトの一覧
- 自社開発 OAuth/OIDC アプリの管理
- バッチ用/Azure 管理用アプリケーションの管理

負荷分散ソリューション

Port	シングルリージョン	マルチリージョン	推奨トラフィックレイヤー
すべてのPort	<div><div>4</div><div>Load Balancer</div></div>	<div><div>7</div><div>Traffic Manager</div></div>	<div>7</div> <div>6</div> <div>5</div> <div>4</div> <div>3</div> <div>2</div> <div>1</div>
	<div><div>7</div><div>Application Gateway</div><div></div></div>	<div><div>7</div><div>Front Door</div><div></div></div>	<div>7</div> <div>6</div> <div>5</div> <div>4</div> <div>3</div> <div>2</div> <div>1</div>

NSGまとめ



NSGはSubnet、NICに対して設定できる
→Vnetではない

考え方としては、VM主体で受信時はSubnet、NICに割り当てられているNSGを適用する。送信時はNIC、Subnetに割り当てられているNSGを適用する。

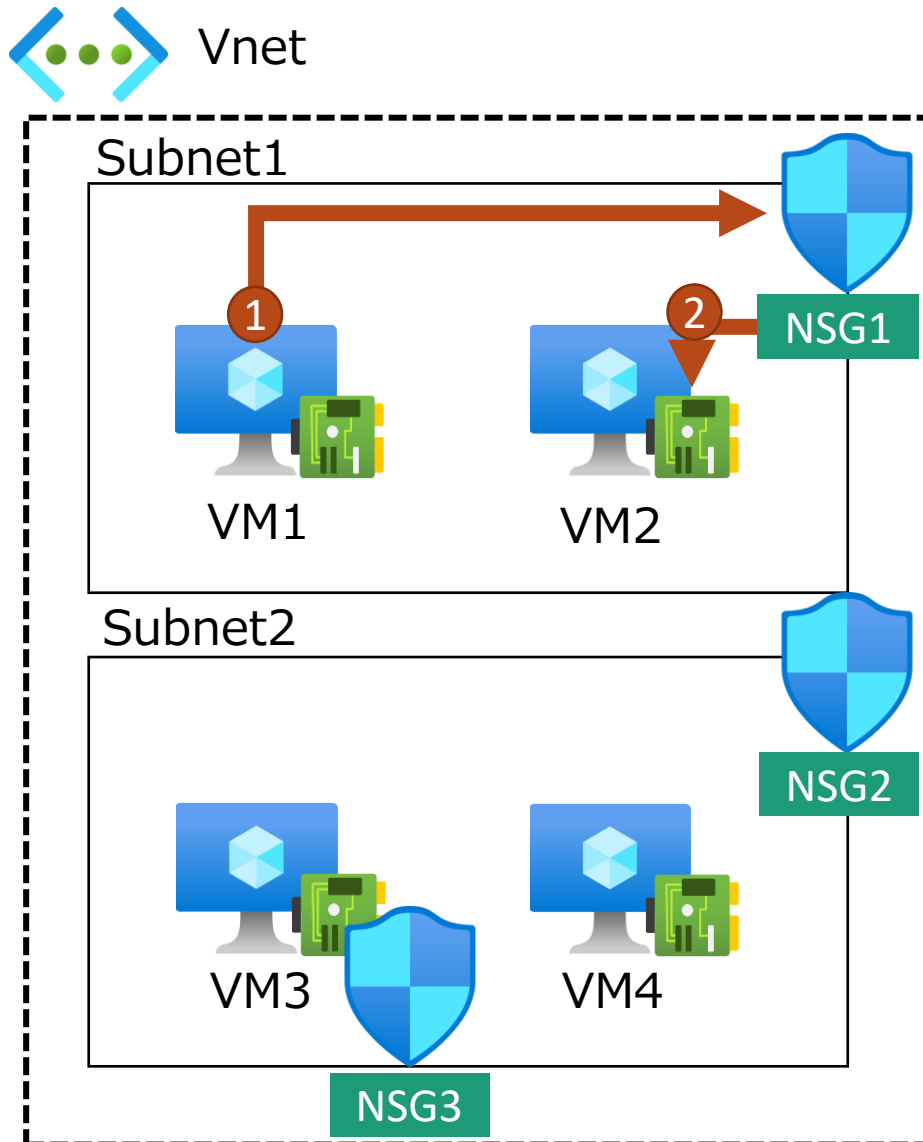
■ 受信トラフィック

受信トラフィックの場合、Azure は、サブネットに関連付けられているネットワーク セキュリティ グループがあれば、まずその規則を処理し、次にネットワーク インターフェイスに関連付けられているネットワーク セキュリティ グループがあれば、その規則を処理します。

■ 送信トラフィック

送信トラフィックの場合、Azure はネットワーク インターフェイスに関連付けられているネットワーク セキュリティ グループがあれば、まずその規則を処理し、次にサブネットに関連付けられているネットワーク セキュリティ グループがあれば、その規則を処理します。

NSGまとめ



VM1 to VM2

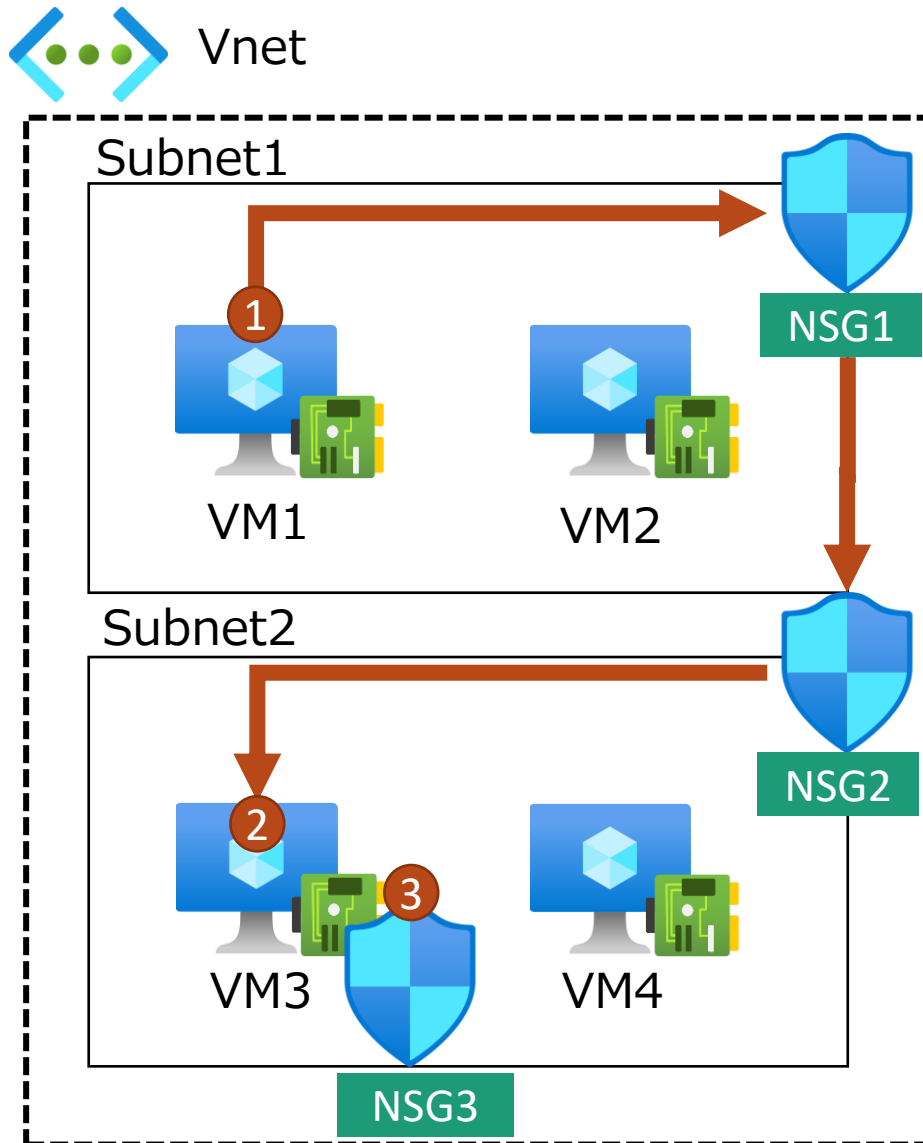
①NSG1の送信ルール（Subnet1に紐づいている）

②NSG1の受信ルール（Subnet1に紐づいている）

が評価される

→同じサブネット内であれば、隣のサーバにはフリーで繋がるわけではない。デフォルトルールで仮想ネットワーク間の通信は全ポート送受信ともに「許可」設定になっているため自在に接続ができているように見えている。

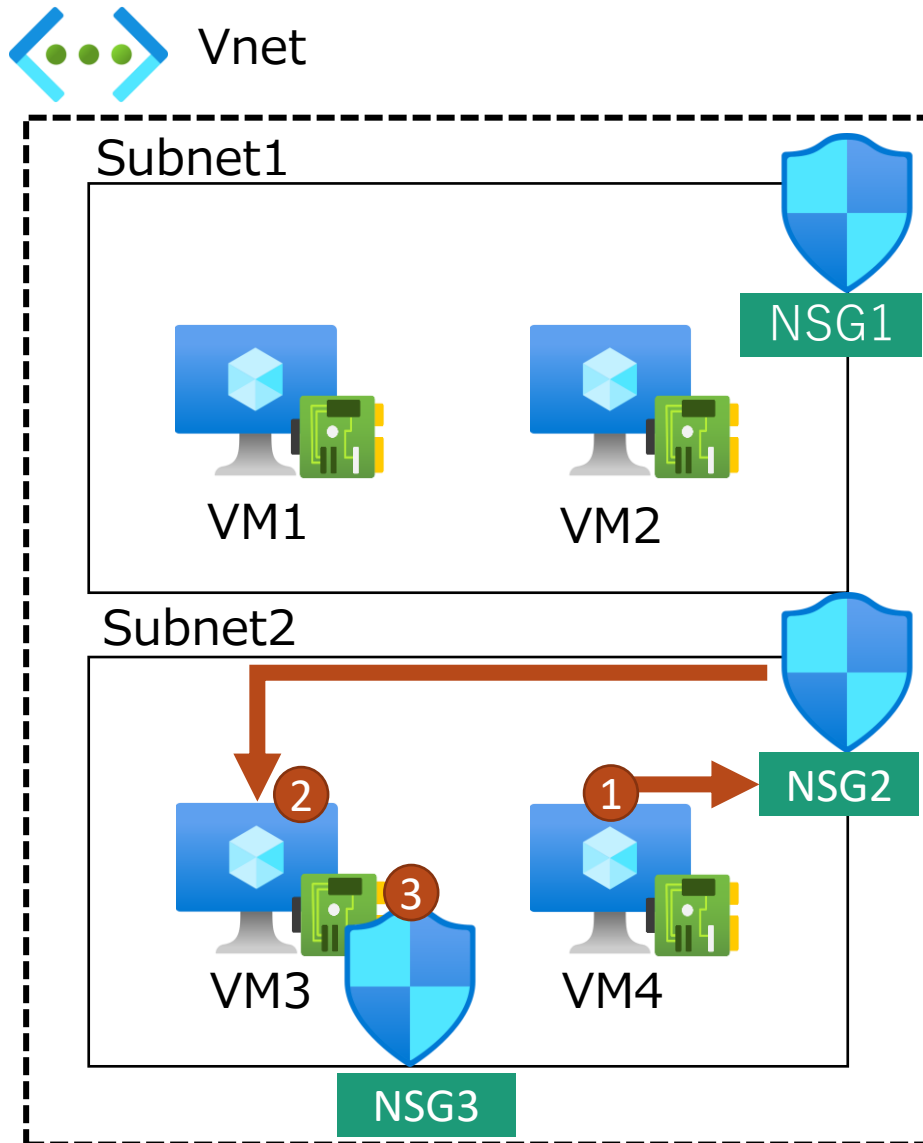
NSGまとめ



VM1 to VM3

- NSG1の送信ルール（Subnet1に紐づいている）
 - NSG2の受信ルール（Subnet2に紐づいている）
 - NSG3の受信ルール（VM3のNICに紐づいている）
- が評価される

NSGまとめ

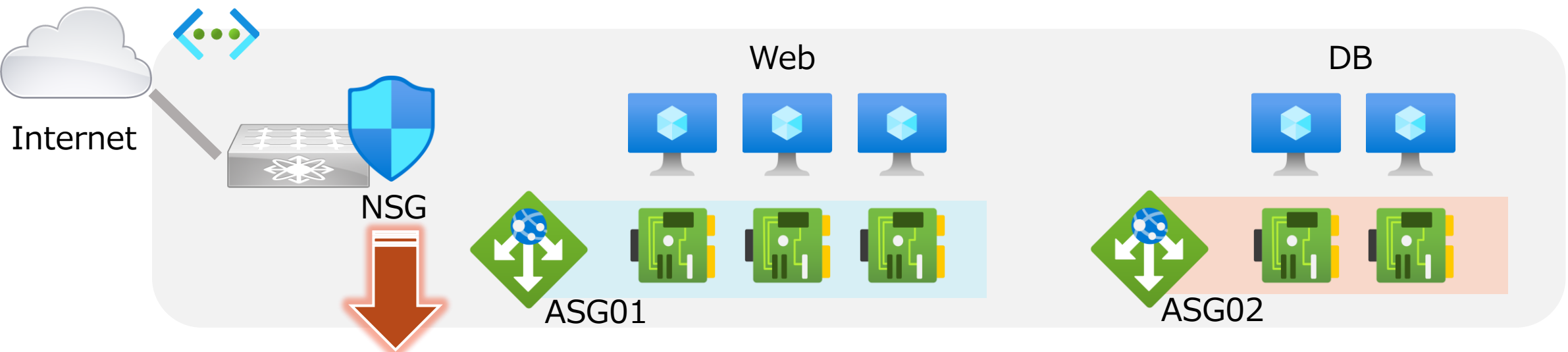


VM4 to VM3

- ①NSG2の送信ルール (Subnet2に紐づいている)
 - ②NSG2の受信ルール (Subnet2に紐づいている)
 - ②NSG3の受信ルール (VM3のNICに紐づいている)
- が評価される

ASGとは

- NSG(ネットワーク セキュリティ グループ)の拡張機能。
- 仮想マシン(NIC)をグループ化する事ができ、NSGの送信元/宛先として適用できる。同じ役割のサーバー同士をグルーピングする事で、アプリケーションの通信パターンに適応したNSG設定が容易になる。
- ※ASGは、同一リージョン内のNICを登録できます。



Source	Destination	Action
Internet	ASG01	Allow
ASG01	ASG02	Allow
Any	Any	Deny

ASGまとめ

- ASGのメリット

- NSGルールの行数を削減できる
- 保護対象サーバーが追加された際にも、NSGルールを変更する必要がない
- 保護対象サーバーのIPアドレスを意識する必要がない
- マイクロセグメンテーション

- ASGを有効にするための、3つの条件

1. 保護対象サーバーのNICにASGが適用されている事
2. 適用したASGが、NSGのルールに適用されている事
3. NSGが保護対象サーバー上のサブネットに適用されている事

※NICに対し、ASGを複数適用する事が可能

※3つの条件を全て満たした場合のみ、ASGが適用される。

NSG規定ルール

受信セキュリティ規則

優先度	名前	ソース	宛先	サービス	アクション
65000	AllowVnetInBound	VirtualNetwork	VirtualNetwork	任意/任意	Allow
65001	AllowAzureLoadBalancerInBound	AzureLoadBalancer	任意	任意/任意	Allow
65500	DenyAllInBound	任意	任意	任意/任意	Deny

送信セキュリティ規則

優先度	名前	ソース	宛先	サービス	アクション
65000	AllowVnetOutBound	VirtualNetwork	VirtualNetwork	任意/任意	Allow
65001	AllowInternetOutBound	任意	Internet	任意/任意	Allow
65500	DenyAllOutBound	任意	任意	任意/任意	Deny

サービスタグ考察

VirtualNetwork

- 仮想ネットワーク内の同一サブネット
- 仮想ネットワーク内の別サブネット
- 仮想ネットワークピアリングで接続された別仮想ネットワーク
- Site to Site接続された別の仮想ネットワーク(Azure、オンプレ)
- Point to Site接続されたクライアント側PC
- Express Routeによって接続されたオンプレ側ネットワーク
- ホストの仮想 IP アドレス、およびユーザーが定義したルートで使用するアドレス プレフィックス

よってインターネット以外すべてが該当する。安易にVirtualNetworkタグを使って受信規則をフルオープンにしてしまうと、社内の誰からも、どこからもアクセスできてしまう。

AzureLoadBalancer

Azure インフラストラクチャのロード バランサー。このタグは、Azure の正常性プローブの送信元となるホストの仮想 IP アドレス (168.63.129.16) に変換される。これにはプローブ トラフィックのみが含まれ、バックエンドリソースへの実際のトラフィックは含まれない。Azure Load Balancer を使っていない場合は、この規則をオーバーライドできます。

Internet

パブリック インターネットによってアクセスできる仮想ネットワークの外部の IP アドレス空間。このアドレス範囲には、**Azure によって所有されているパブリック IP アドレス空間が含まれている。**

送信規則でInternet向けの通信を遮断した場合、以下の事象が発生する。

- 仮想マシンに拡張機能(BGInfoなど)の追加操作をしてもデプロイが正常終了しない
- 仮想マシンの診断機能(Diagnostics)を有効にしてもストレージアカウントに結果が出力されない
- LogAnalyticsが有効なのにログが転送されてこない
- 仮想マシンのバックアップが正常に完了しない

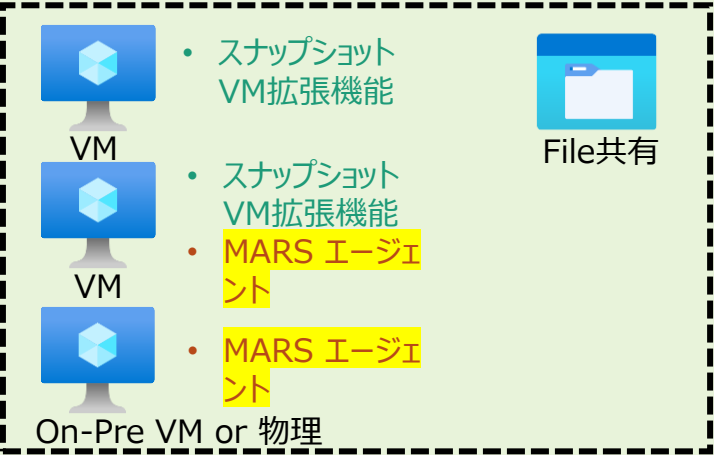
これらは全て仮想マシンのOS内からAzureのPaaSサービス(ストレージアカウント含む)への接続が行えないため発生する。

Azure Backup の整理

MARS:Microsoft Azure Recovery Services
MABS:Microsoft Azure Backup Server
DPM:System Center Data Protection Manager

A

Azure or On-pre



Azure(Recovery Services vault)



B

Azure or On-pre



Azure or On-pre

