Microsoft Azure の始め方 6 回シリーズ

第5回　Azure AD テナントのIDの管理

2022年1月13日 (木) 18:00開始

担当講師

伊藤 将人（いとう まさひと）

マイクロソフト認定トレーナー【1999～】

主な担当コース

- Windows Server、Windows Client
- Exchange Server、Skype for Business Server、System Center など
- Microsoft Azure 、Microsoft 365

趣味

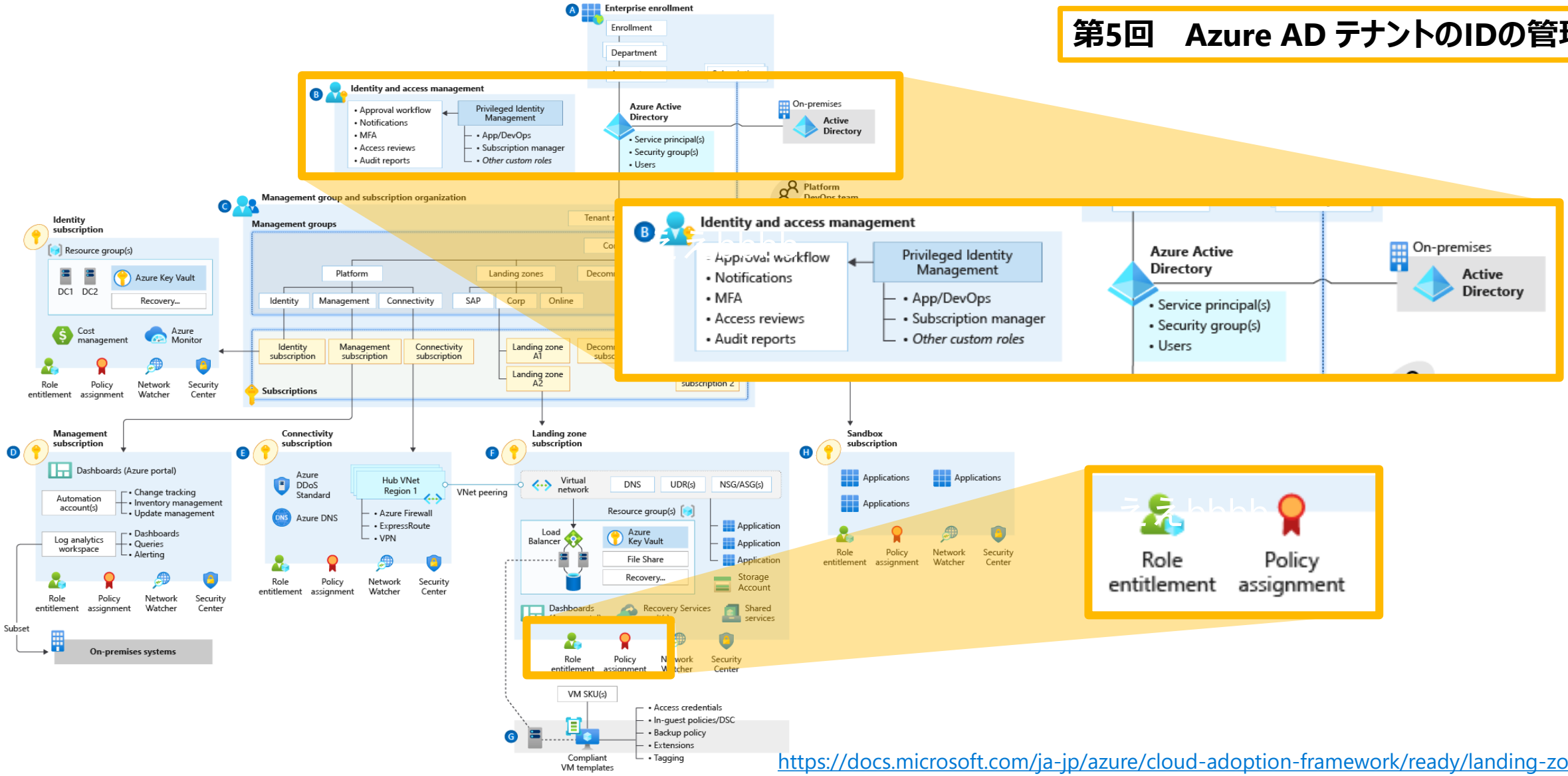
- ゴルフ

Azure 運用管理基礎

第1回　Azure の始め方	[2021/12/02]
第2回　Azure 仮想マシンの作成と管理	[2021/12/09]
第3回　Azure ネットワークとサイト接続	[2021/12/16]
第4回　Azure ストレージとデータ管理	[2021/12/23]
第5回　Azure AD テナントのIDの管理	[2022/01/13]
第6回　Azure セキュリティの管理	[2023/01/20]

Azureランディング ゾーンの概念アーキテクチャ

第5回　Azure AD テナントのIDの管理

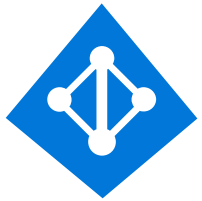


https://docs.microsoft.com/ja-jp/azure/cloud-adoption-framework/ready/landing-zone/

第5回　Azure ADテナントのIDの管理

- Azure Active Directory
- AD DS との違い
- オンプレミスとの連携
- RBACによる権限の割り当て
- Azureポリシーによるガバナンス管理
- Azure Active Directoryの価格

Azure Active Directory



■マルチテナント対応のクラウドベースの ID 管理サービス

■Webアプリケーションへの認証と承認サービスを提供

■メリットと機能

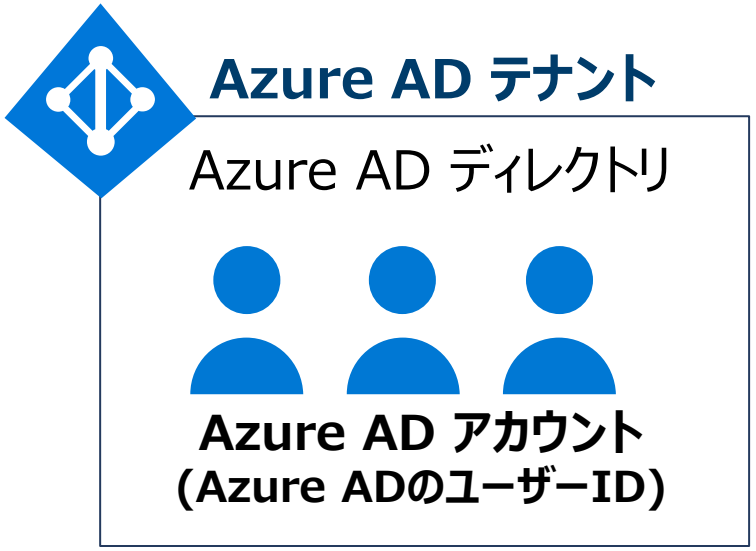
- 任意のクラウド アプリケーションやオンプレミス Web アプリケーションへのシングル サインオン
- クラウドとオンプレミス アプリケーションに安全なシングル サインオンを提供
- iOS、macOS、Android、および Windows デバイスで動作
- オンプレミスの Web アプリケーションを安全なリモート アクセスで保護
- Active Directory をクラウドへ簡単に拡張
- 機密性の高いデータとアプリケーションを保護
- セルフサービス機能でコストを削減し、セキュリティを強化

Azure AD テナント

Azure AD テナントは会社などの組織の単位です。

Azure AD テナントの登録によりAzure Active Directoryのディレクトリが作成されます。

Azure ADによりIDの管理機能とIDの認証・承認サービスが提供されます。

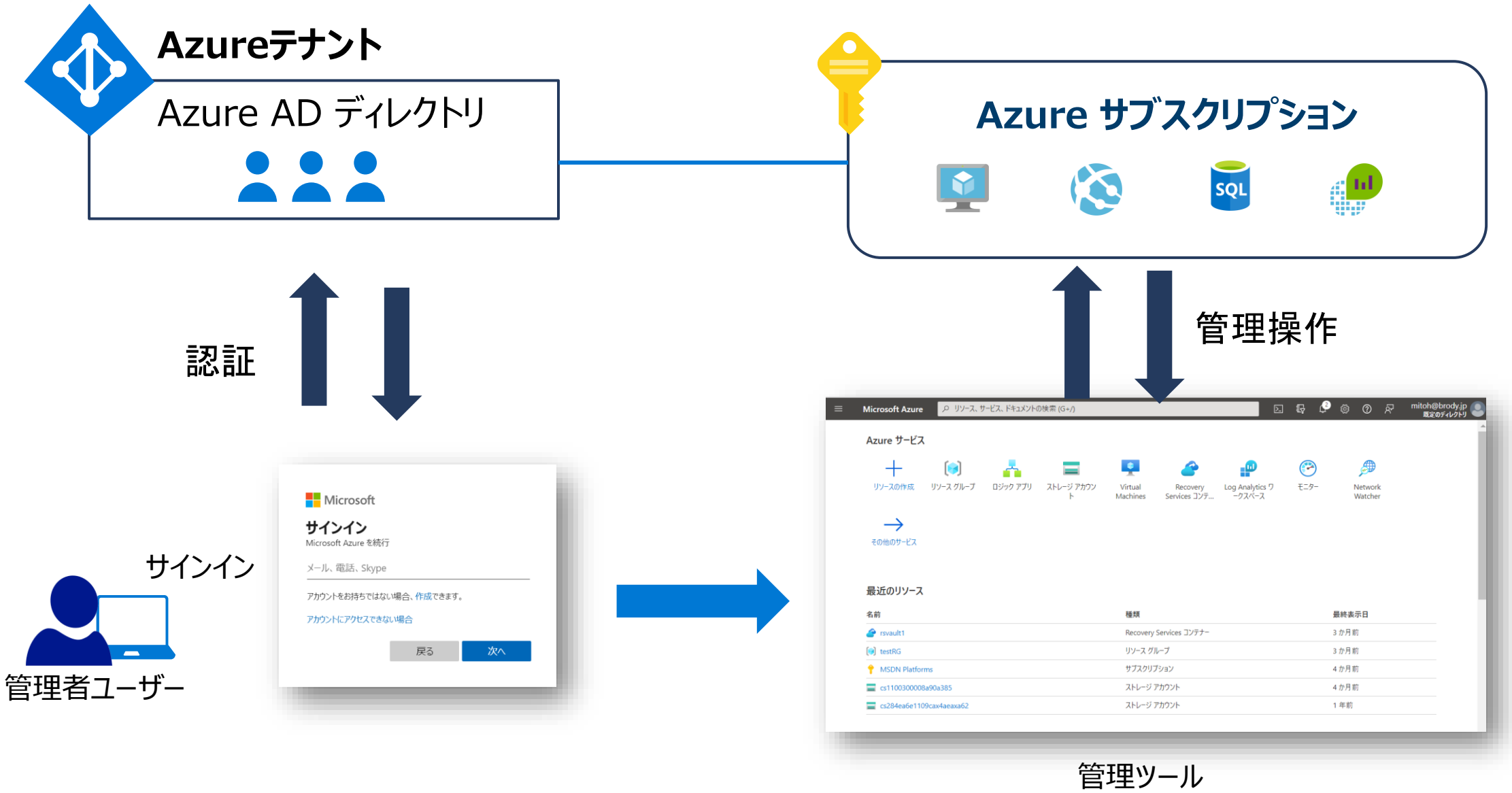


Azure ADのユーザーIDの種類

- **クラウドID**
  Azure ADディレクトリに直接登録されるID
- **ディレクトリ同期ID**
  オンプレミスとのディレクトリ同期処理により登録されるID
- **ゲストID**
  他のディレクトリによって管理され、招待により登録されるID

複数のテナントに分割したアカウント管理も可能だが、管理が複雑になるため推奨されない

Azure ADのサインイン フロー



Azure ADアカウントの作成

設定項目	説明
ユーザーの作成・ユーザーの招待	ユーザー(クラウドID)の作成かゲストIDの招待を選択します。
ユーザー名	サインイン時に使用するユーザー名(ユーザー名@ドメイン名の形式)を指定します。
名前	ユーザーの表示名を指定します。
名	名を指定します。
姓	姓を指定します。
グループ	ユーザーが所属するグループを選択します。
役割(ロール)	ユーザーが所属するロール(管理役割)を指定します。
サインインのブロック	サインインを許可するかブロックするかを指定します。
利用場所	利用する場所(国や地域)を指定します。
役職	ユーザーの役職を指定します。
部署	ユーザーの部署名を指定します。
会社名	ユーザーの会社名を指定します。
管理者	ユーザーの管理者を選択します。

Azure ADロール

Azure AD テナントの管理を行うには、管理権限が割り当てられたロールに
ユーザーIDを追加する必要があります。

ロール	説明
グローバル管理者(全体管理者)	Azure AD のすべての側面と、Azure AD の ID が使用される Microsoft サービスを管理できます。
グローバル閲覧者	グローバル管理者が読み取れるものすべての読み取りが可能ですが、更新することはできません。
ユーザー管理者	ユーザーとグループのすべての側面を、制限付きの管理者のパスワードをリセットすることも含めて、管理できます。
ヘルプデスク管理者	管理者以外のユーザーとヘルプデスク管理者のパスワードをリセットできます。

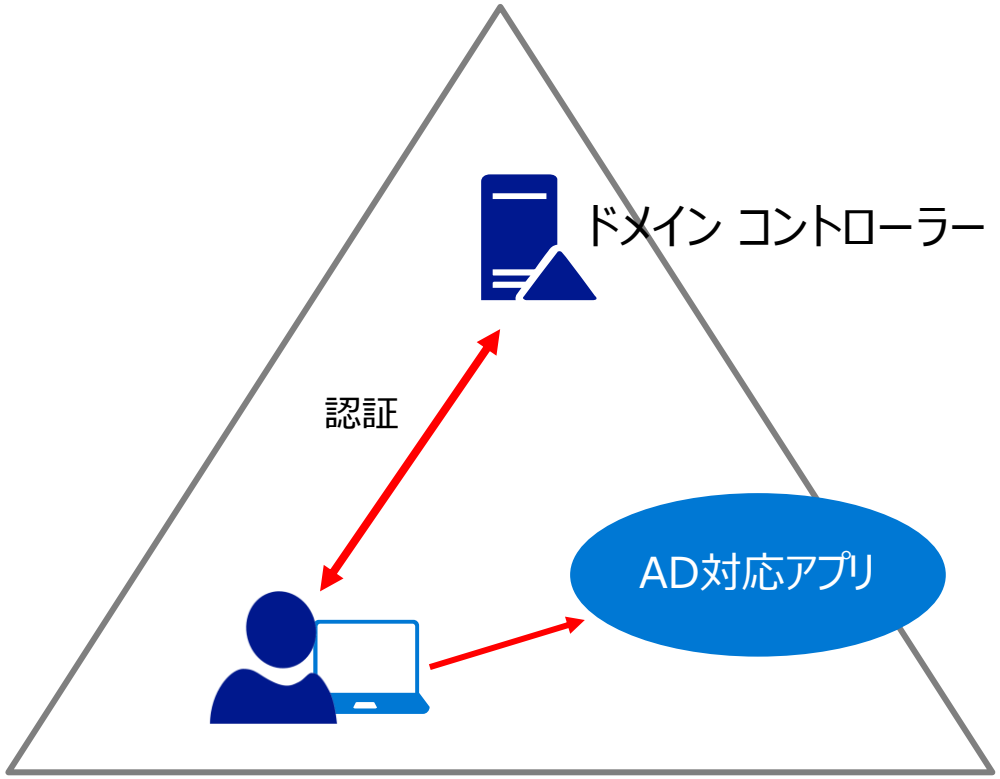
※ カスタム ロールを作成するには、Azure AD Premium P1またはP2が必要です。

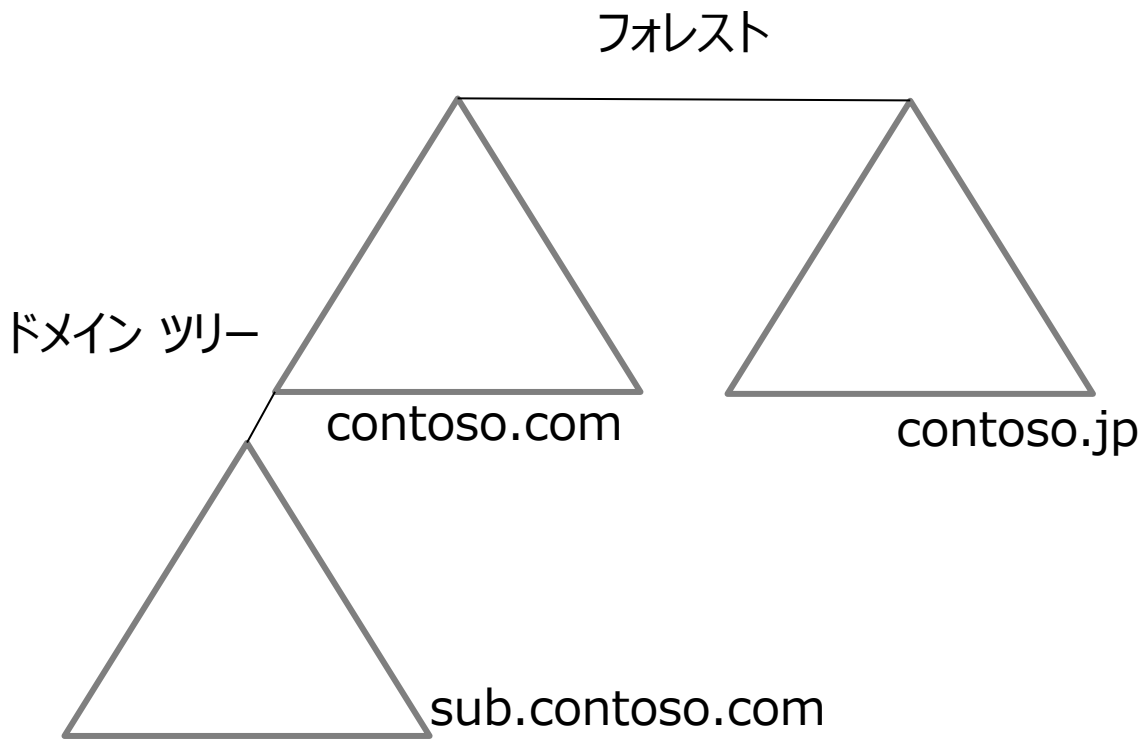
Azure ADのエディション

	Free	Microsoft 365	Premium P1	Premium P2
ディレクトリ オブジェクト	500,000	無制限	無制限	無制限
シングル サインオン	無制限	無制限	無制限	無制限
コア ID とアクセス管理	✓	✓	✓	✓
ビジネスとビジネスのコラボレーション	✓	✓	✓	✓
Microsoft 365 Apps の ID およびアクセス管理		✓	✓	✓
Premium 機能			✓	✓
詳細なグループ アクセス管理			✓	✓
条件付きアクセス			✓	✓
ID 保護				✓
ID ガバナンス				✓

Active Directory Domain Service (AD DS)

- Windows 2000以降で提供されるマイクロソフトのディレクトリサービスの名称
- 検索サービス(LDAP) ＋ 認証サービス (Kerberos V5)
- オンプレミスのID管理とAD DS対応アプリケーションへの認証と承認サービス



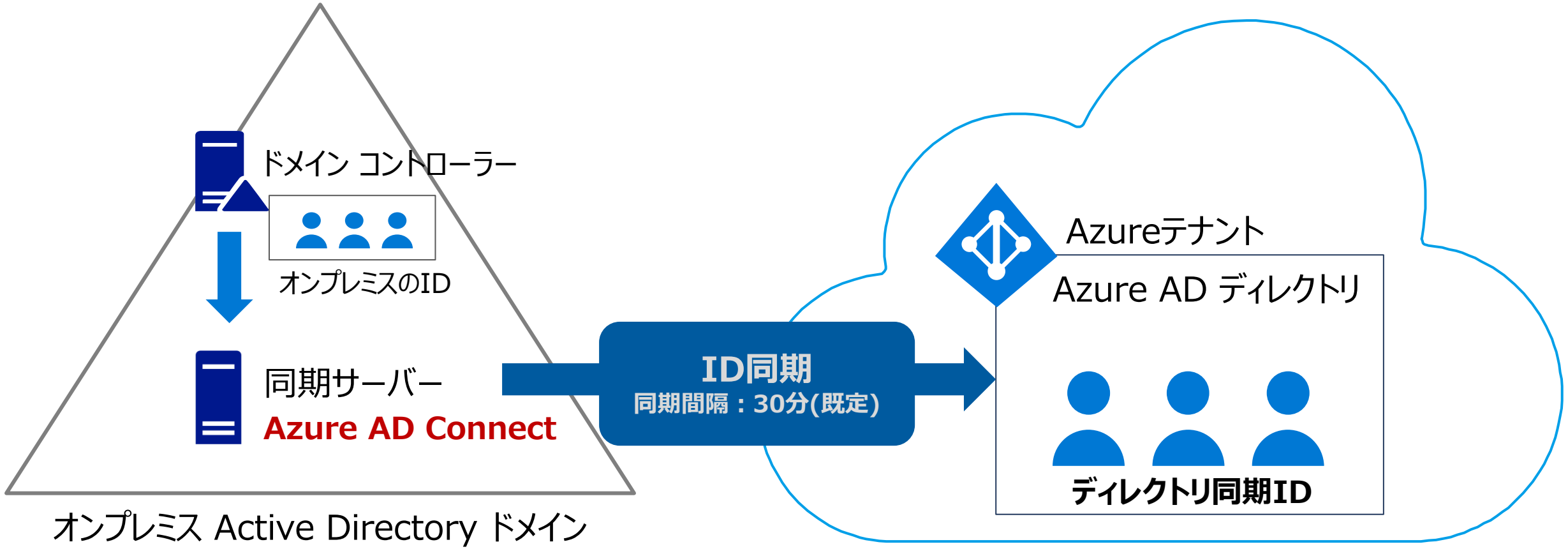


Azure AD と AD DSの違い

	Azure AD	AD DS
IDソリューション	インターネットベースのWeb アプリケーション向け	AD対応 アプリケーションや Windows ベースの機能やサービス向け
認証プロトコル	SAML、WSフェデレーション、Open ID Connect、OAuth（承認用）	Kerberos認証
クエリ	REST API クエリ	LDAP
フェデレーション サービス	Facebookなどのサードパーティ サービスとの連携が可能	AD FSを使用して構築
管理構造	フラット構造	組織単位(OU)で、オブジェクトを分散管理可能。ドメイン、ドメインツリー、フォレスト構造を使用してマルチドメインをサポート
グループ ポリシー	なし	あり

オンプレミスとの連携

オンプレミスのActive Directory のIDをAzure ADと同期することにより、オンプレミスのIDをクラウドサービスでも利用できるようになります。



ハイブリッドIDの認証オプション

■パスワード ハッシュ同期

オンプレミス AD パスワードのユーザーのハッシュを Azure AD と同期するサインイン方法

■パススルー認証

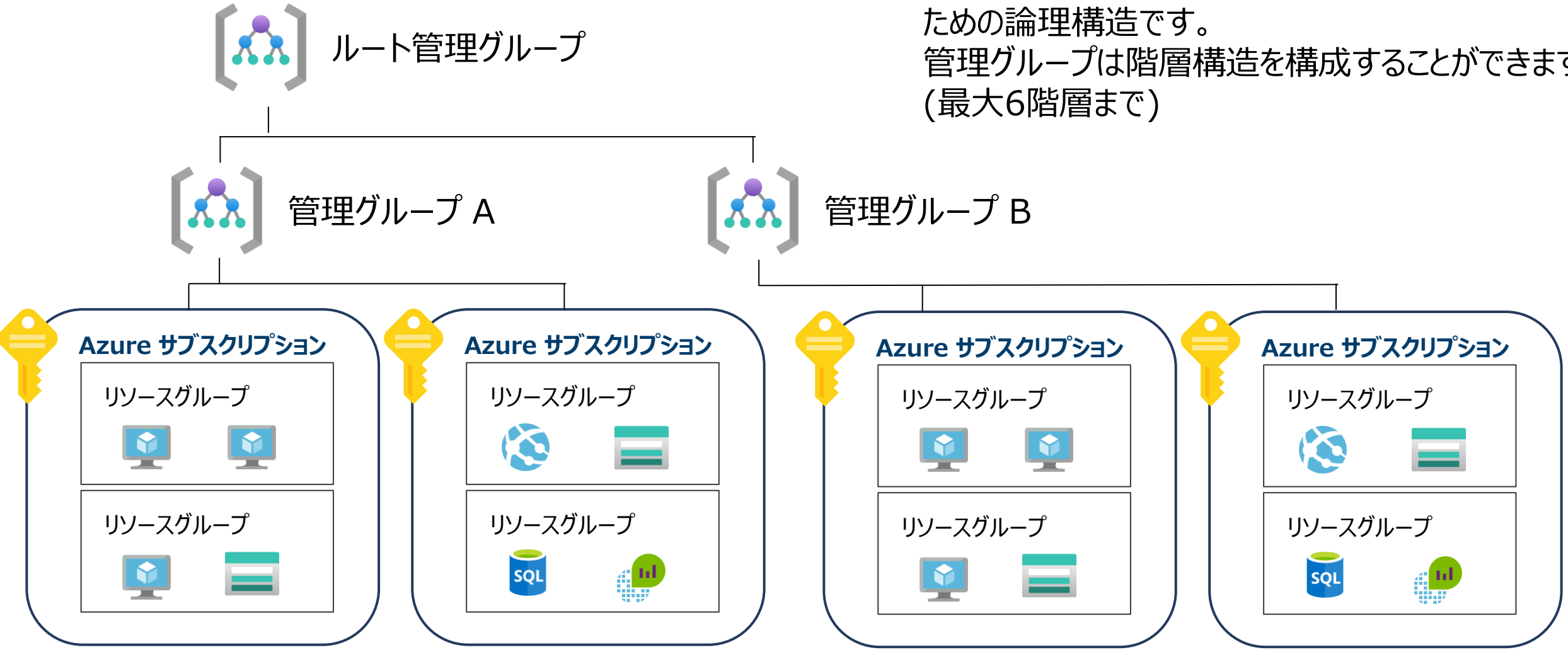
フェデレーション環境の追加インフラストラクチャを必要とせずに、ユーザーがオンプレミスとクラウドで同じパスワードを使用できるようにするサインイン方法。

■フェデレーション統合

フェデレーションは Azure AD Connect のオプション要素で、オンプレミス AD FS インフラストラクチャを使用してハイブリッド環境をセットアップするために使用できます。証明書の更新や追加の AD FS サーバー デプロイなどの AD FS 管理機能も提供されます。

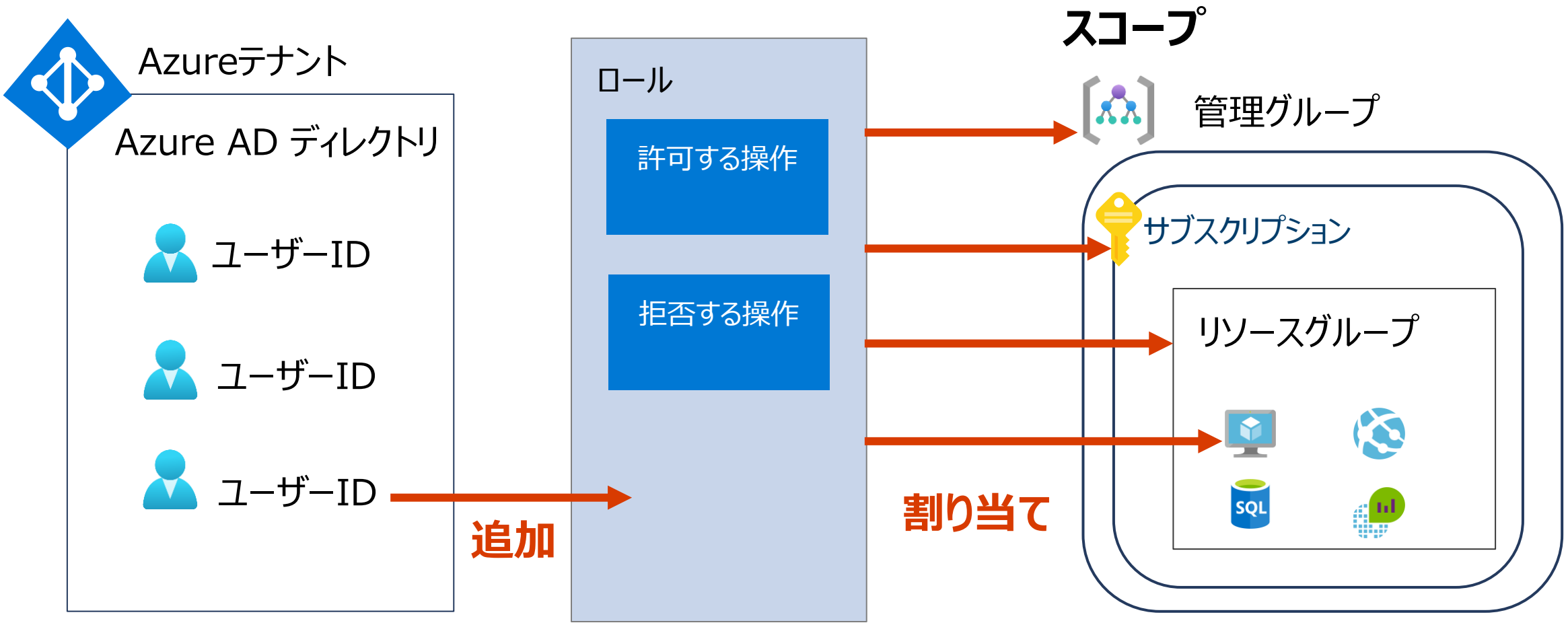
ガバナンスの適用範囲

管理グループはサブスクリプションをまとめて管理するための論理構造です。
管理グループは階層構造を構成することができます。
(最大6階層まで)



RBACによる管理権限の割り当て

■ポリシーの割り当てにより、指定したスコープに対しポリシーを適用



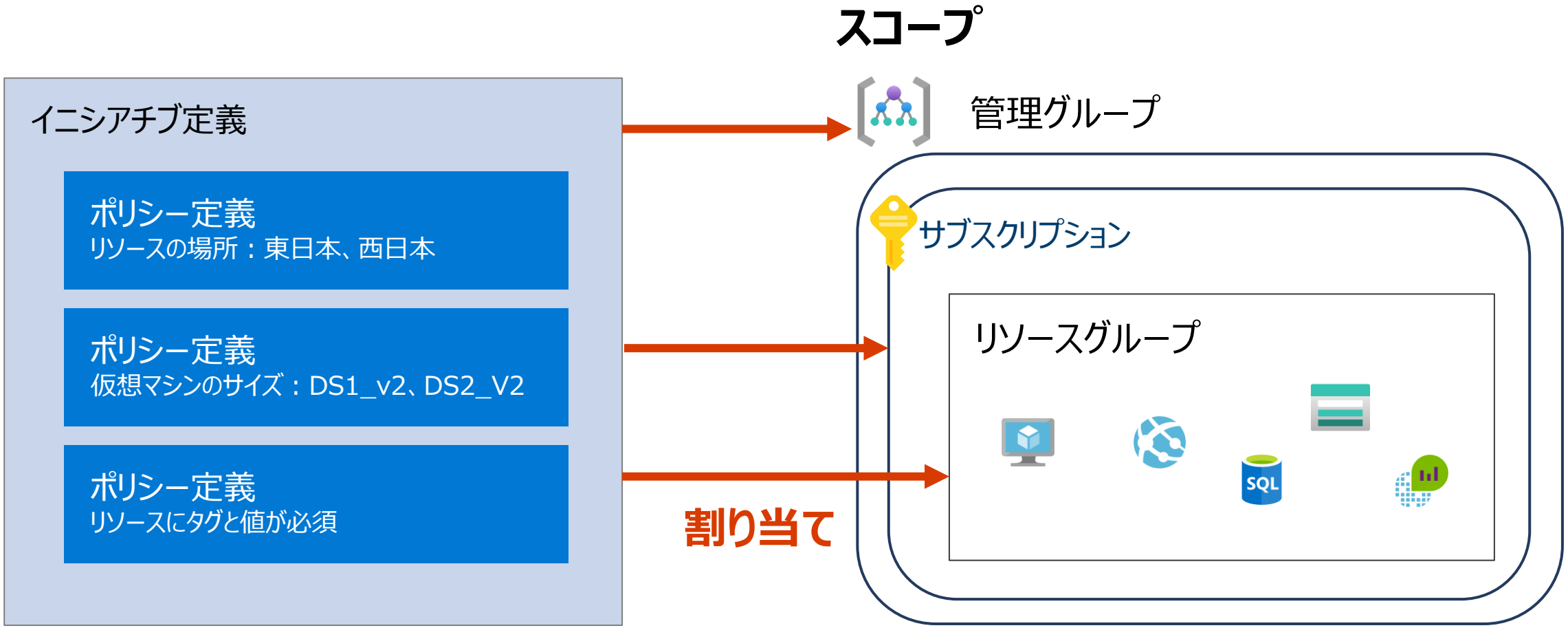
※ 上位の階層に割り当てられたロールは下位に継承されます。

ビルトイン ロール

ロール	説明
所有者	アクセス権を他のユーザーに委任する権利を含めて、スコープ内のすべてのリソースに対するフル アクセスを持ちます。
共同作成者	すべての種類の Azure リソースの作成と管理が可能ですが、アクセス権を他のユーザーに付与することはできません。
閲覧者	既存の Azure リソースを表示できます。
ユーザー アクセス管理者	Azure リソースへのユーザー アクセスを管理できます。

Azureポリシーによるガバナンス管理

■ポリシーの割り当てにより、指定したスコープに対しポリシーを適用



※ 上位の階層に割り当てられたポリシー、イニシアチブは下位に継承されます。

Azure Active Directoryの価格

- Azure AD Free
  - ✓ 無料
- Azure AD Microsoft 365
  - ✓ 無料
  - ✓ Microsoft 365 サブスクリプションが必要です。
- Azure AD Premium P1
  - ✓ ¥689.610 ユーザー/月*
- Azure AD Premium P2
  - ✓ ¥1,034.415 ユーザー/月*

* 年間契約

Microsoft

QA

Resource

- Azure 向けの Microsoft クラウド導入フレームワークのドキュメント
  https://docs.microsoft.com/ja-jp/azure/cloud-adoption-framework/overview
- Azure ランディング ゾーンとは
  https://docs.microsoft.com/ja-jp/azure/cloud-adoption-framework/ready/landing-zone/
- Azure Active Directory の価格
  https://azure.microsoft.com/ja-jp/pricing/details/active-directory/
- Azure Active Directory でのハイブリッド ID とは
  https://docs.microsoft.com/ja-jp/azure/active-directory/hybrid/whatis-hybrid-identity
- Azure Policyの概要
  https://docs.microsoft.com/ja-jp/azure/governance/policy/overview

Microsoft

Thank you