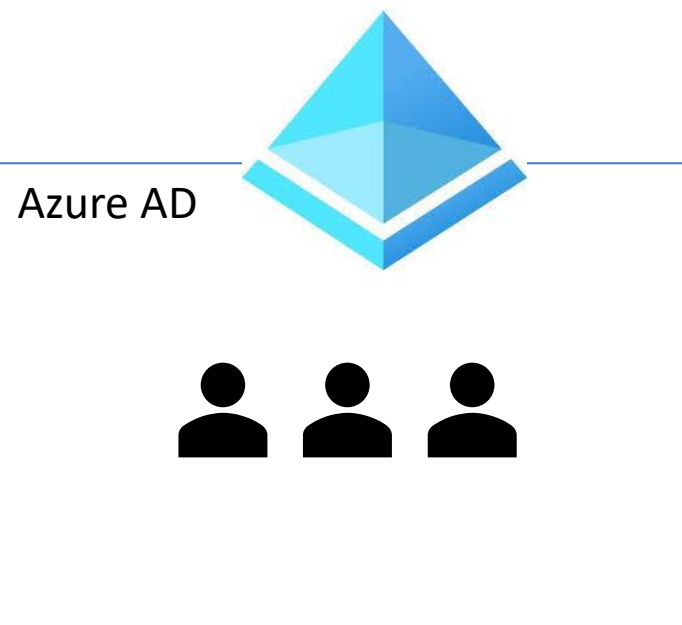


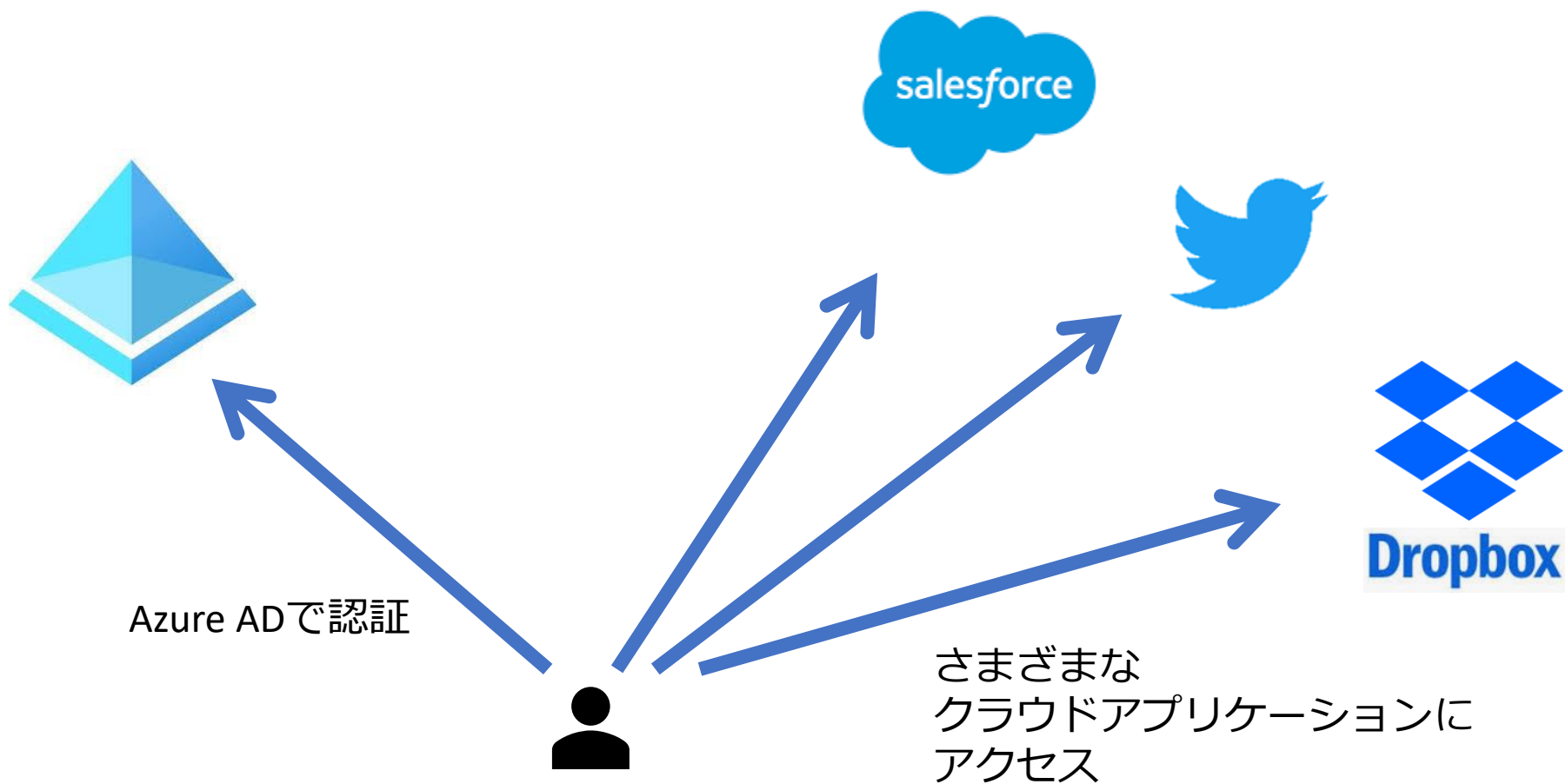
- Module 1 ID
  - Azure Active Directory (Azure AD)
    - Azure AD : Azure ADで実現できること
    - Azure AD の概念 : テナントなどの用語
    - AD DS と Azure AD : オンプレミスのAD DSとの違い
    - Azure AD エディション : 4種類のエディションとライセンス
    - Azure AD 参加 / 登録 : デバイスからのAzure ADアクセス
    - セルフサービス パスワード リセット(SSPR) : パスワードリセット
  - ユーザーとグループ
    - ユーザー アカウント : ユーザーの種類は3つ
    - ユーザー アカウントの管理 : ユーザー管理の知識
    - 一括ユーザー アカウント : 大量のユーザーをCSVで一括登録
    - グループ アカウント : グループ管理の知識
    - 複数のディレクトリの管理 : ディレクトリの独立性
    - デモンストレーション - ユーザーとグループ
  - ラボ1

- Module 1 ID
  - Azure Active Directory (Azure AD)
    - Azure AD : Azure ADで実現できること
    - Azure AD の概念 : テナントなどの用語
    - AD DS と Azure AD : オンプレミスのAD DSとの違い
    - Azure AD エディション : 4種類のエディションとライセンス
    - Azure AD 参加 / 登録 : デバイスからのAzure ADアクセス
    - セルフサービス パスワード リセット(SSPR) : パスワードリセット
  - ユーザーとグループ
    - ユーザー アカウント : ユーザーの種類は3つ
    - ユーザー アカウントの管理 : ユーザー管理の知識
    - 一括ユーザー アカウント : 大量のユーザーをCSVで一括登録
    - グループ アカウント : グループ管理の知識
    - 複数のディレクトリの管理 : ディレクトリの独立性
    - デモンストレーション - ユーザーとグループ
  - ラボ1

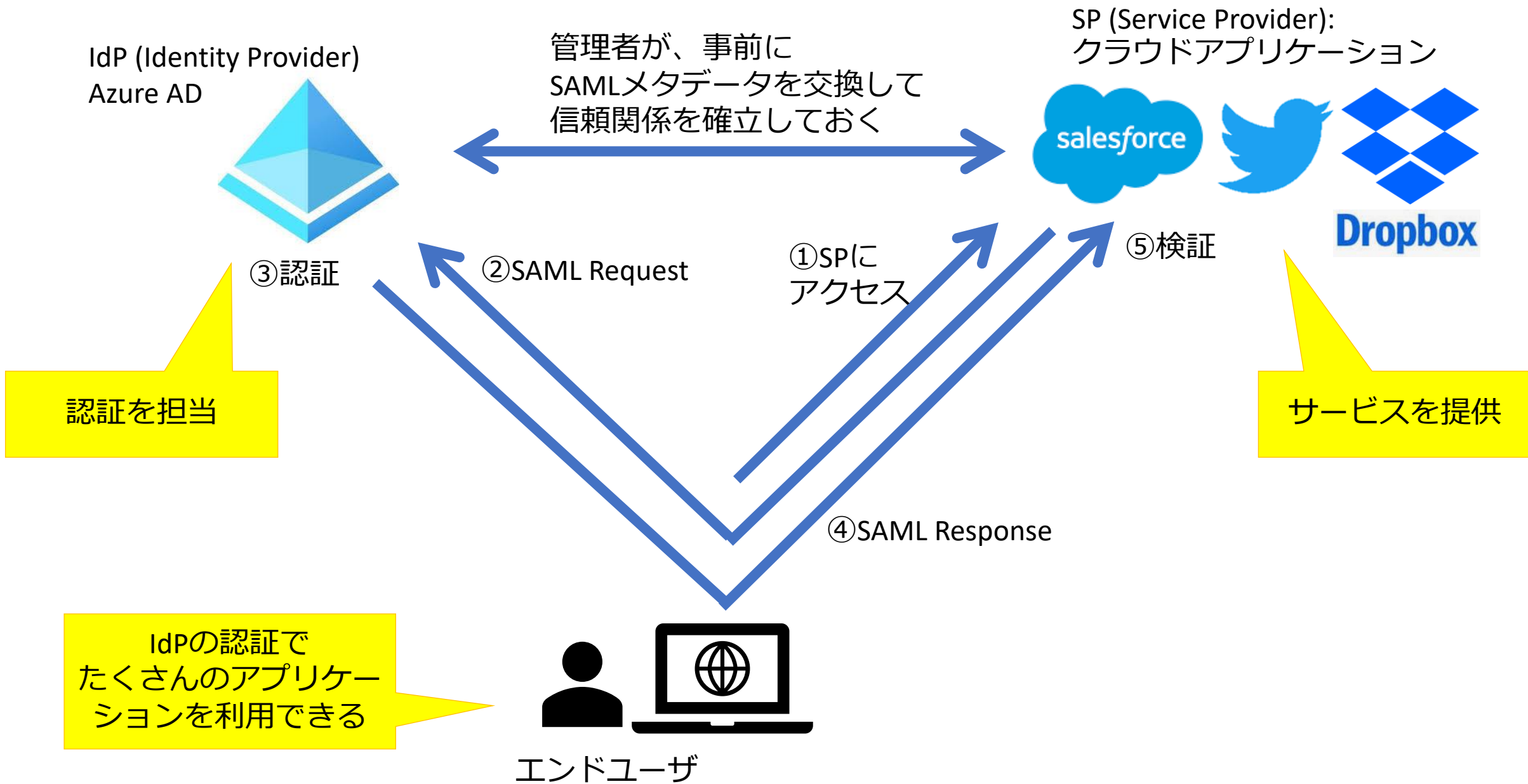
- Module 1 ID
  - Azure Active Directory (Azure AD)
    - Azure AD : Azure ADで実現できること
    - Azure AD の概念 : テナントなどの用語
    - AD DS と Azure AD : オンプレミスのAD DSとの違い
    - Azure AD エディション : 4種類のエディションとライセンス
    - Azure AD 参加 / 登録 : デバイスからのAzure ADアクセス
    - セルフサービス パスワード リセット(SSPR) : パスワードリセット
  - ユーザーとグループ
    - ユーザー アカウント : ユーザーの種類は3つ
    - ユーザー アカウントの管理 : ユーザー管理の知識
    - 一括ユーザー アカウント : 大量のユーザーをCSVで一括登録
    - グループ アカウント : グループ管理の知識
    - 複数のディレクトリの管理 : ディレクトリの独立性
    - デモンストレーション - ユーザーとグループ
  - ラボ1



クラウドベースの  
ID管理

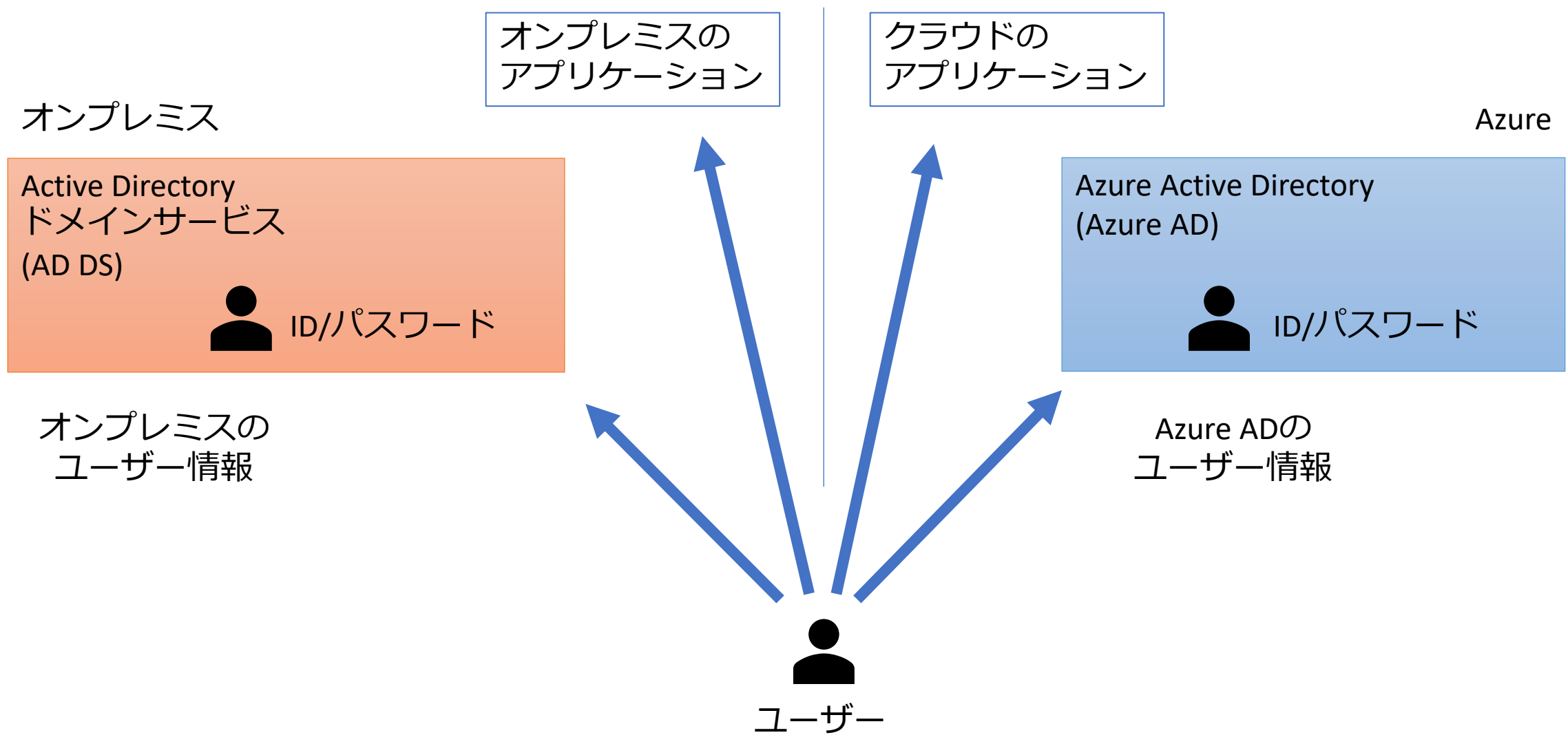


# SAML(Security Assertion Markup Language) によるSSO(Single Sign On)



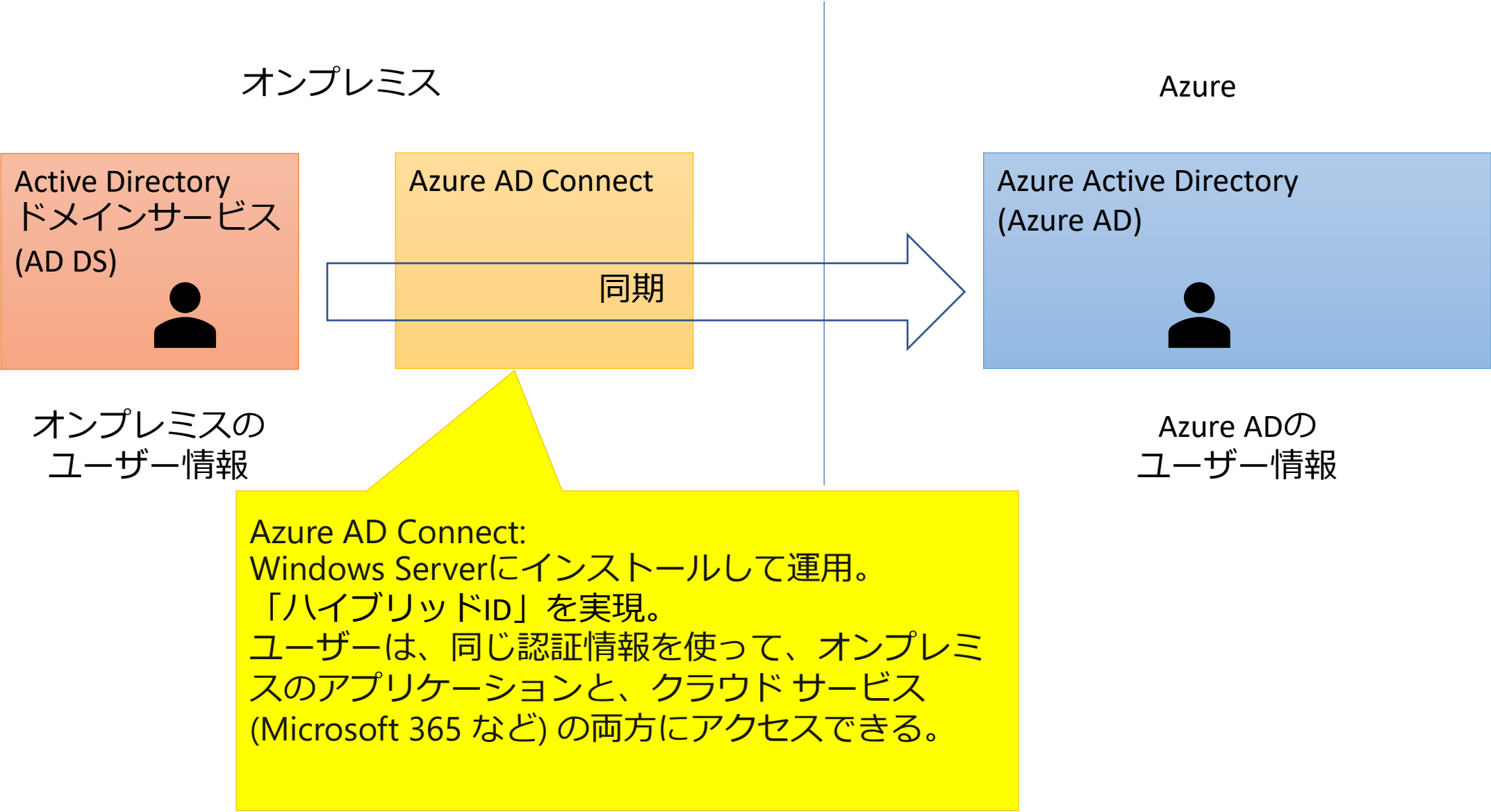
- **アプリケーション プロキシ**とは、ユーザーがリモート クライアントからオンプレミス Web アプリケーションにアクセスできるようにする Azure AD の機能です。
- アプリケーション プロキシには、クラウドで実行されるアプリケーション プロキシ サービスと、オンプレミス サーバーで実行されるアプリケーション プロキシ コネクタの両方が含まれています。
- Azure AD、アプリケーション プロキシ サービス、およびアプリケーション プロキシ コネクタは連携して、Azure AD から Web アプリケーションにユーザーのシングル サイン オン トークンを安全に渡します。

ユーザーが、両方の環境へログインする必要がある場合

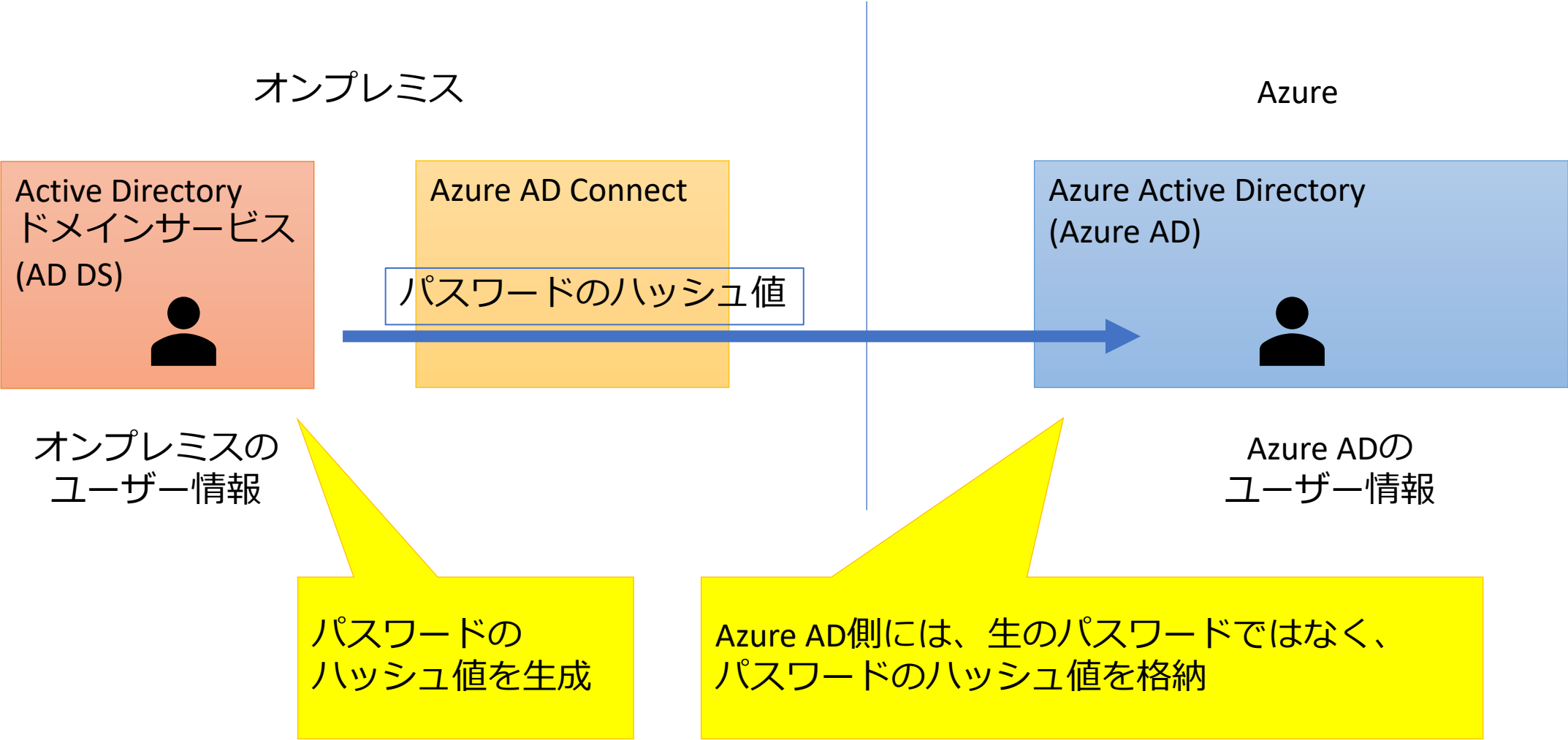




Azure AD Connect を利用して、オンプレミスのIDをAzure ADへと同期させる



Azure AD Connect の同期方法の例 > パスワード ハッシュ 同期



<https://docs.microsoft.com/ja-jp/learn/modules/manage-users-and-groups-in-aad/6-azure-ad-connect>

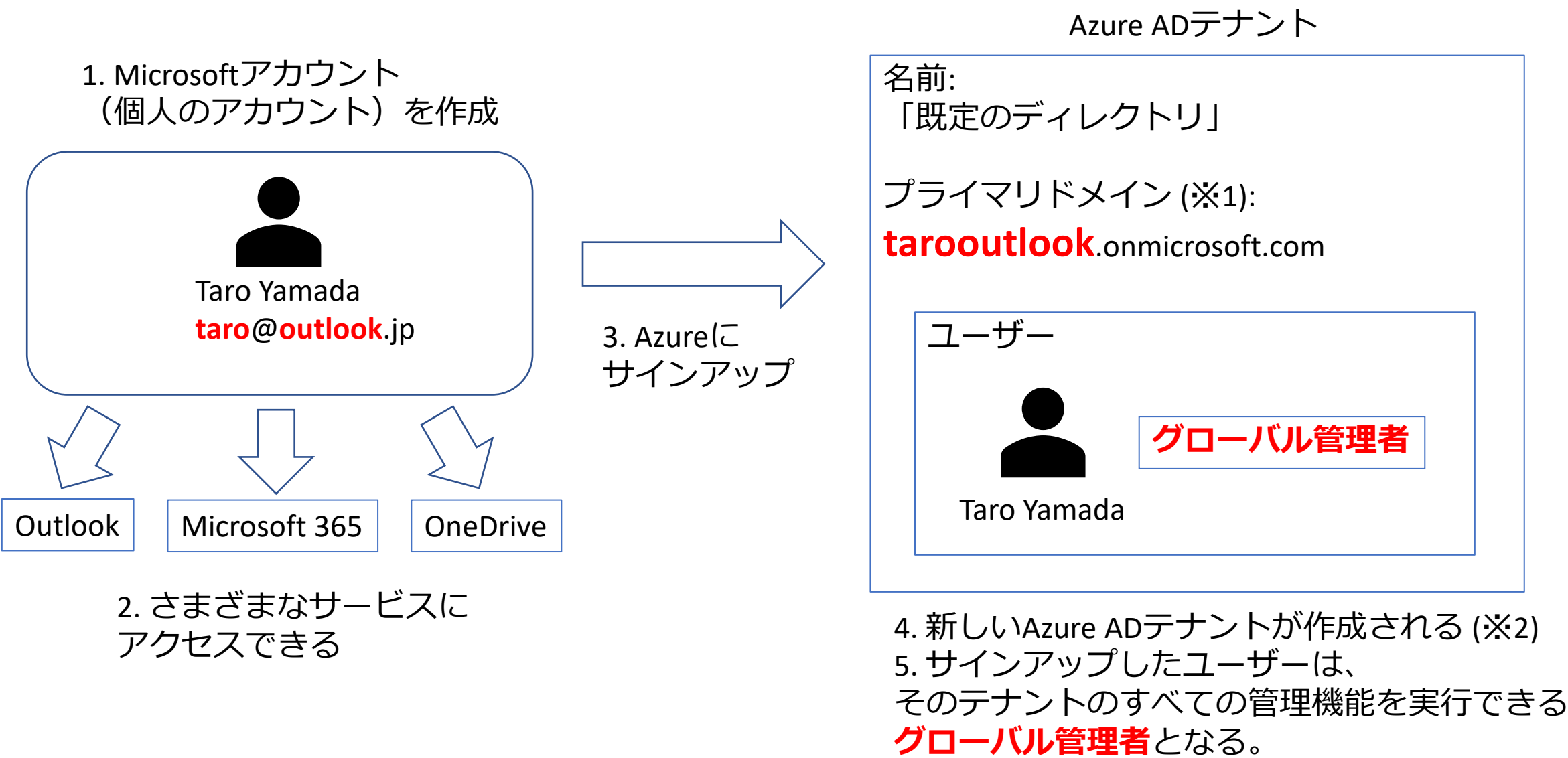
<https://docs.microsoft.com/ja-jp/azure/active-directory/hybrid/whatis-phs>

# まとめ：Azure ADでできること

- ユーザーのIDを管理
- アプリケーションへのシングルサインオンを提供
  - クラウドアプリケーション
  - オンプレミスアプリケーション
- さまざまなデバイスに対応
  - iOS/macOS/Android/Windows
- オンプレミスのIDをAzure ADへと同期
  - オンプレミスと同じIDでAzure ADにサインイン

- Module 1 ID
  - Azure Active Directory (Azure AD)
    - Azure AD : Azure ADで実現できること
    - Azure AD の概念 : テナントなどの用語
    - AD DS と Azure AD : オンプレミスのAD DSとの違い
    - Azure AD エディション : 4種類のエディションとライセンス
    - Azure AD 参加 / 登録 : デバイスからのAzure ADアクセス
    - セルフサービス パスワード リセット(SSPR) : パスワードリセット
  - ユーザーとグループ
    - ユーザー アカウント : ユーザーの種類は3つ
    - ユーザー アカウントの管理 : ユーザー管理の知識
    - 一括ユーザー アカウント : 大量のユーザーをCSVで一括登録
    - グループ アカウント : グループ管理の知識
    - 複数のディレクトリの管理 : ディレクトリの独立性
    - デモンストレーション - ユーザーとグループ
  - ラボ1

# Azure のサインアップ



※1：初期ドメイン、規定のドメインとも。変更不可、削除不可。

※2：テナントは、Microsoft Azure, Microsoft Intune, Microsoft 365などにサインアップすると、自動的に作成される。

Azure ADのテナント：各テナントは「組織」を表す

Azure テナント

(会社A)

Azure テナント

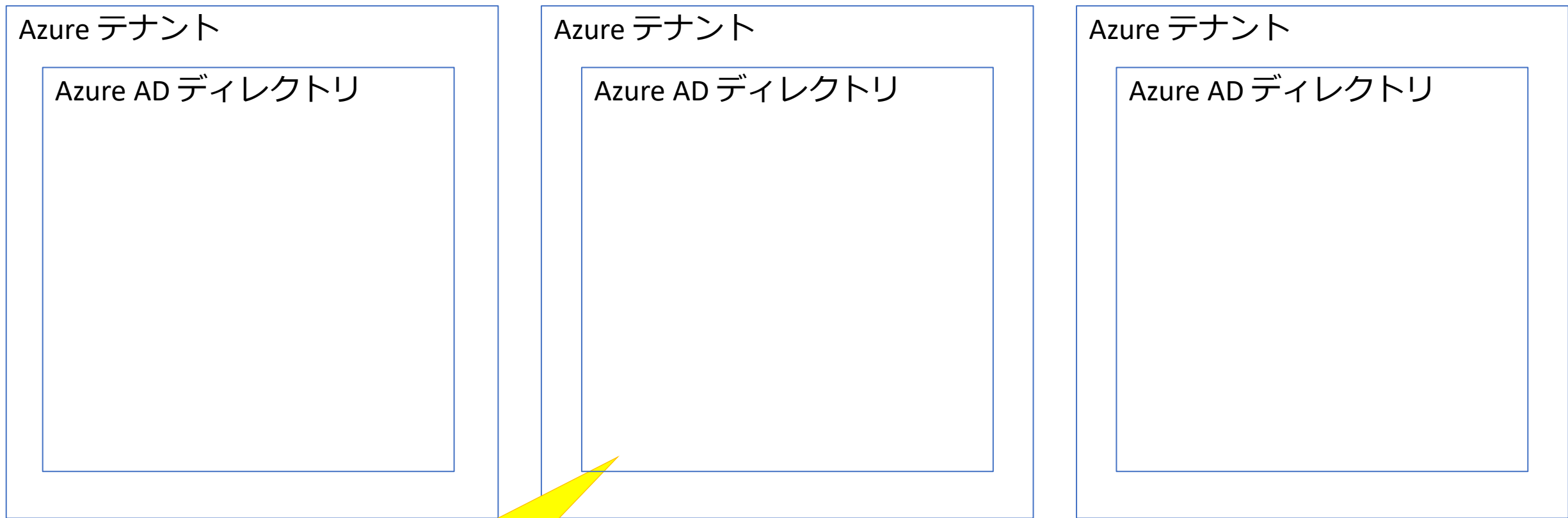
(会社B)

Azure テナント

(会社C)

Azure ADの世界に  
たくさんのテナントが  
存在する

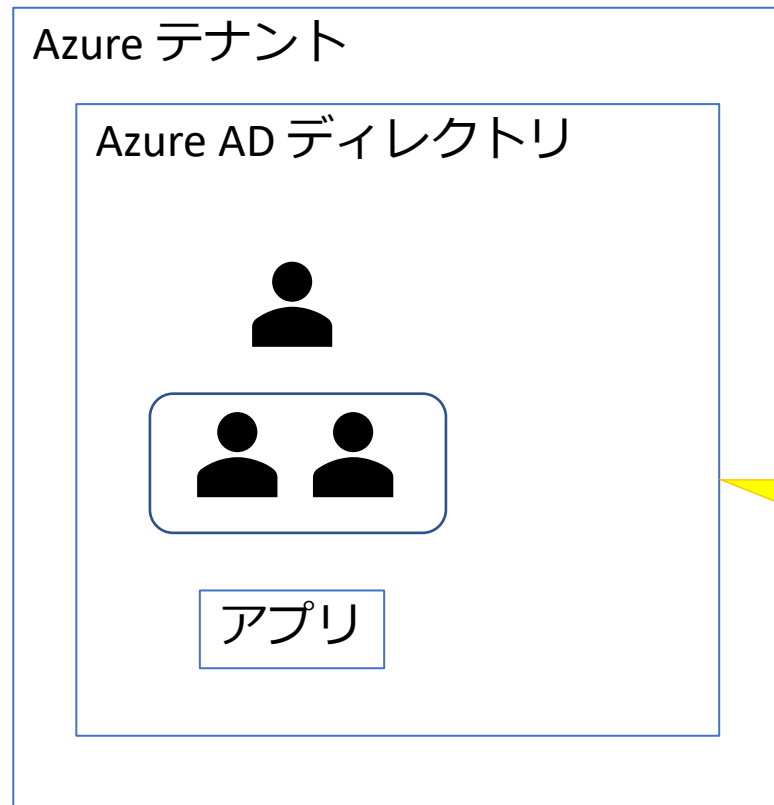
# テナントとディレクトリ



各テナントには  
専用の「Azure ADディレクトリ」  
が用意される

1つのテナントに  
1つのディレクトリがあるので  
テナント≒ディレクトリと  
考えてよい

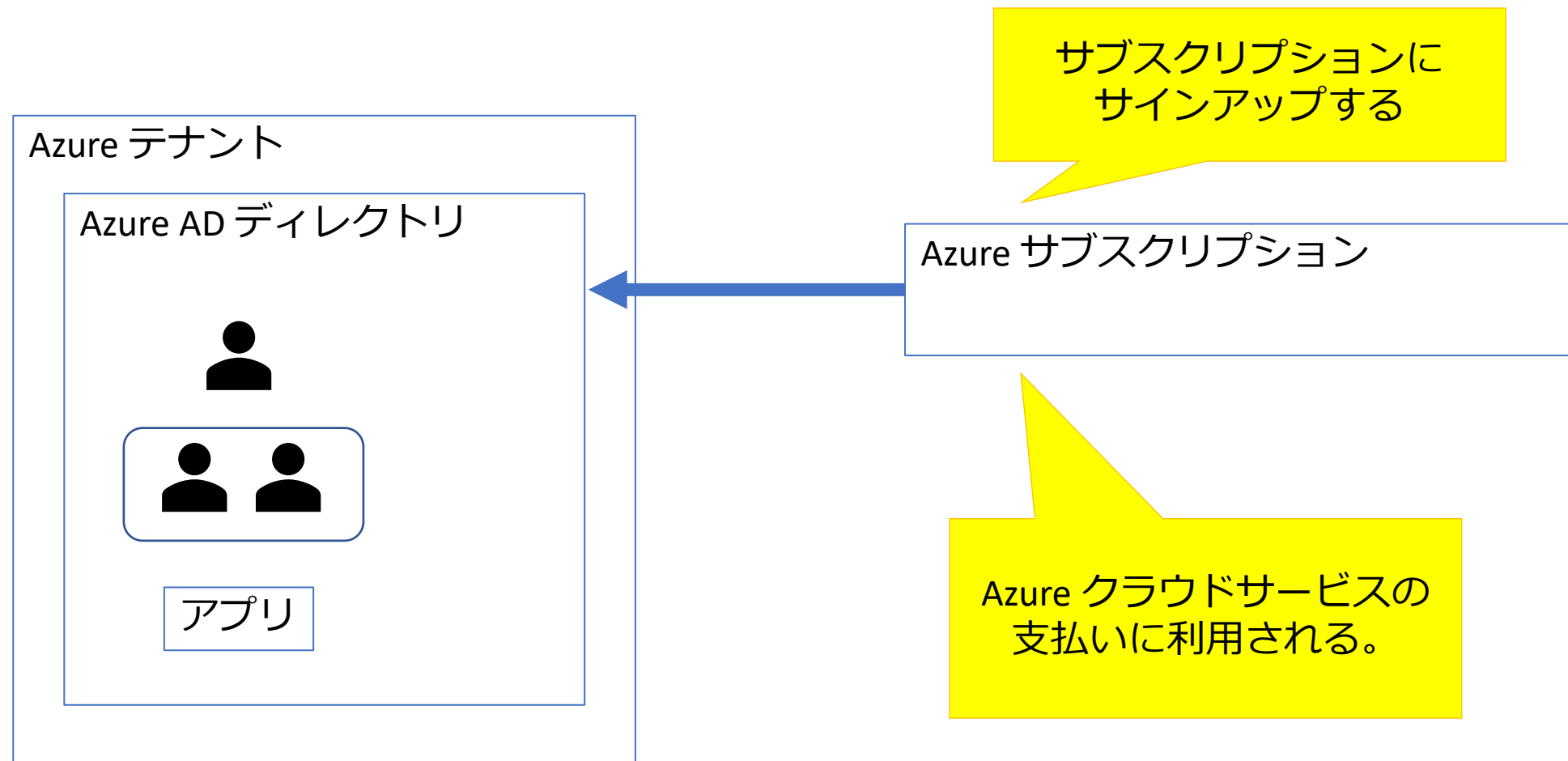
# ディレクトリ



ディレクトリの中には、  
ユーザー、グループ、  
アプリなどが所属する

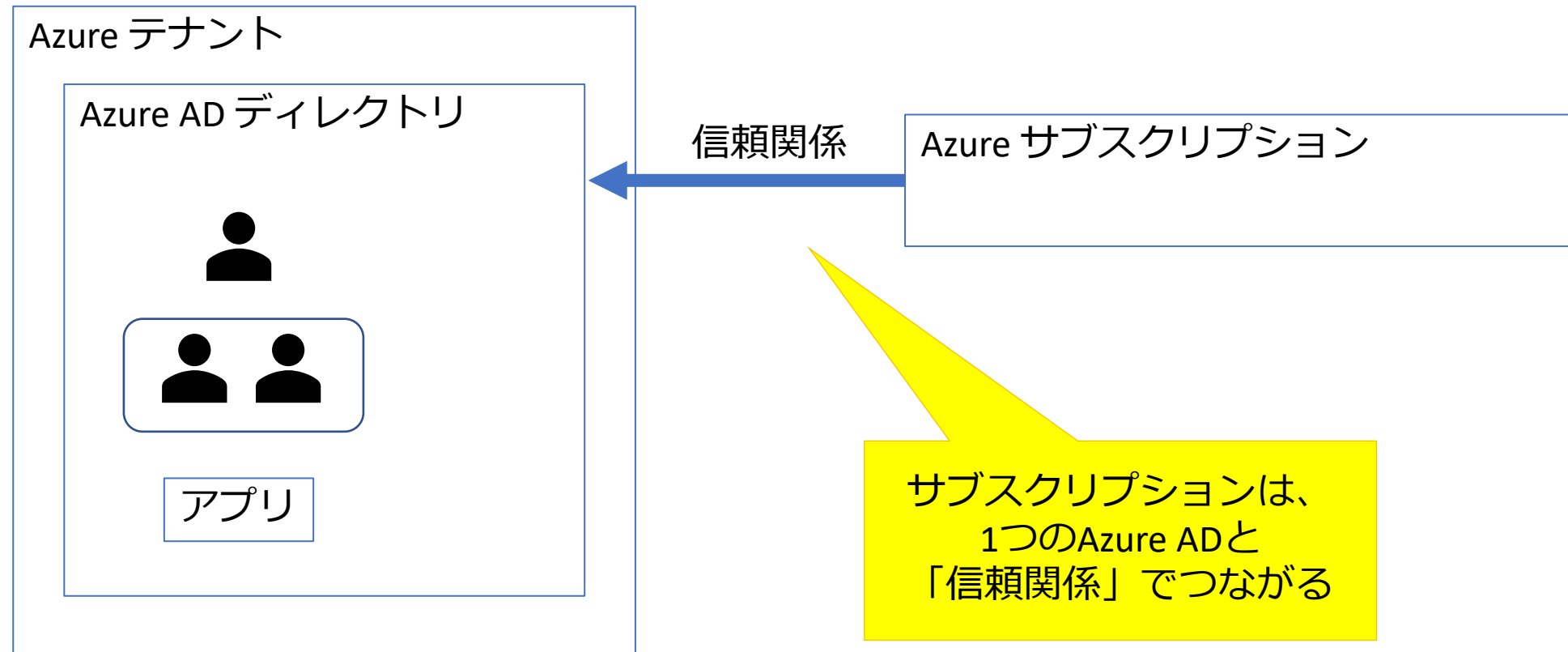


# サブスクリプション

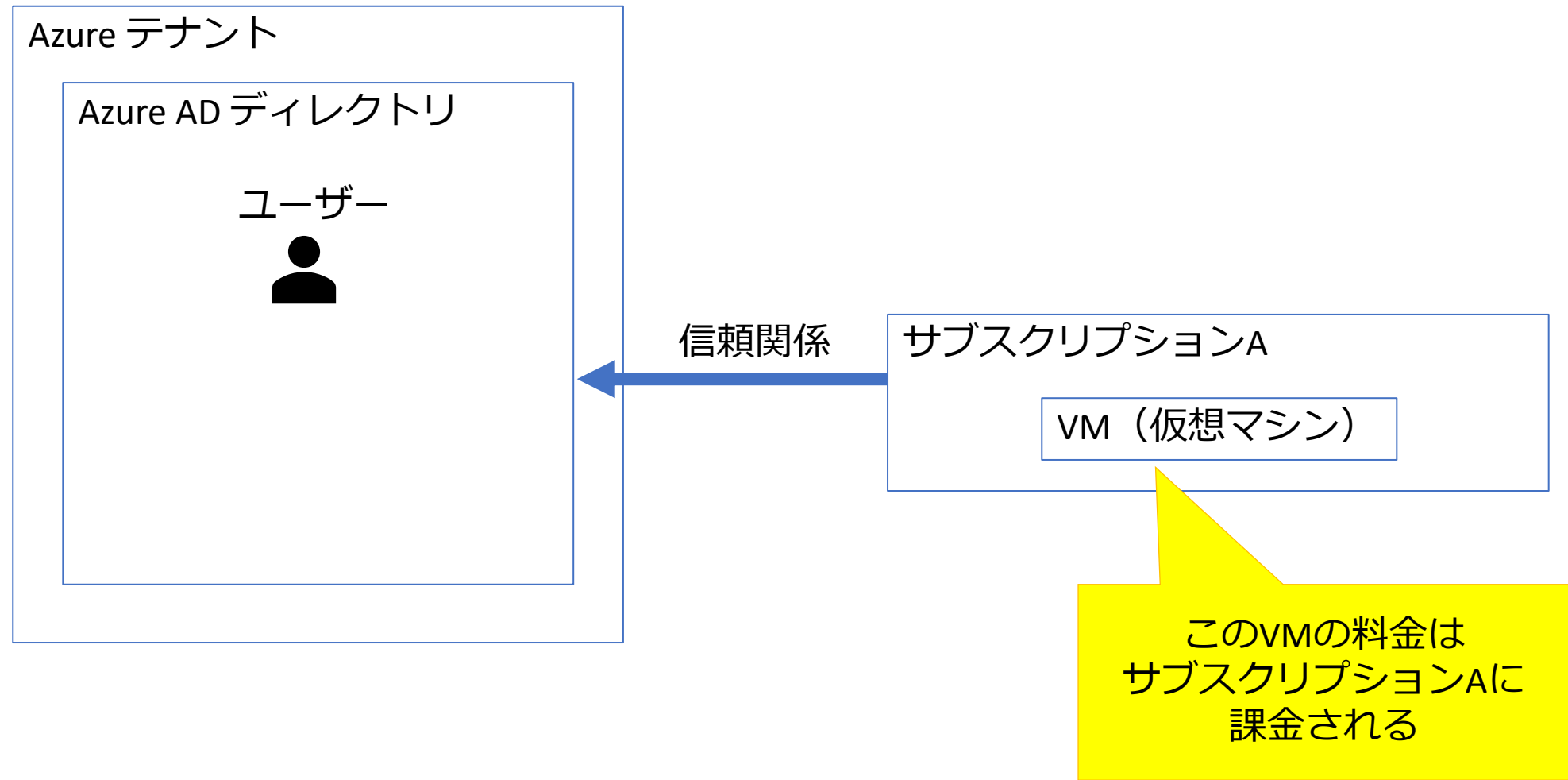


※サブスクリプションは、支払いのほかに、リソースの管理などの役割も持ちます。

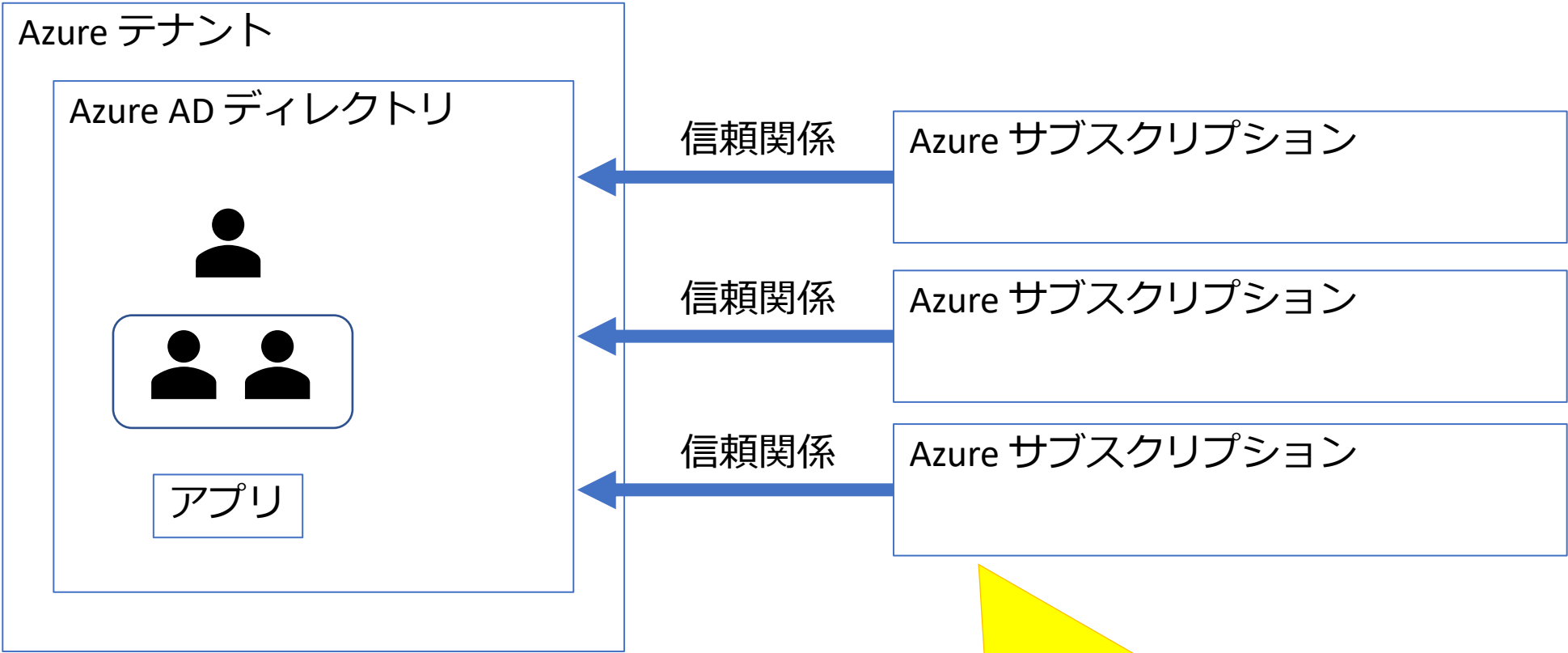
# サブスクリプション



# サブスクリプションの役割：支払い（※）



# Azure ADのテナント



複数のサブスクリプションが、  
1つのAzure ADディレクトリと  
信頼関係を持つことができる

- Module 1 ID
  - Azure Active Directory (Azure AD)
    - Azure AD : Azure ADで実現できること
    - Azure AD の概念 : テナントなどの用語
    - AD DS と Azure AD : オンプレミスのAD DSとの違い
    - Azure AD エディション : 4種類のエディションとライセンス
    - Azure AD 参加 / 登録 : デバイスからのAzure ADアクセス
    - セルフサービス パスワード リセット(SSPR) : パスワードリセット
  - ユーザーとグループ
    - ユーザー アカウント : ユーザーの種類は3つ
    - ユーザー アカウントの管理 : ユーザー管理の知識
    - 一括ユーザー アカウント : 大量のユーザーをCSVで一括登録
    - グループ アカウント : グループ管理の知識
    - 複数のディレクトリの管理 : ディレクトリの独立性
    - デモンストレーション - ユーザーとグループ
  - ラボ1

# Azure AD と AD DS の位置づけ

## オンプレミス

Active Directory  
ドメインサービス (AD DS)

- **1999/12** Windows 2000 Serverで導入
- **オンプレミスのファイアウォールの内部**で運用
- ネットワーク上の**オブジェクト**（サーバー、ボリューム、プリンター、ユーザー、グループ）の情報を集中管理

## Azure

Azure Active Directory  
(Azure AD)

- **2013/4** Windows Azure Active Directory GA
- **クラウドベース**のIDおよびアクセス管理サービス
- Microsoft Azure、Microsoft 365、Microsoft Intune、Microsoft Dynamics 365などのクラウドベースのサービスの認証基盤

[https://ja.wikipedia.org/wiki/Active\\_Directory](https://ja.wikipedia.org/wiki/Active_Directory)

<https://docs.microsoft.com/ja-jp/windows-server/identity/ad-ds/ad-ds-getting-started>

<https://docs.microsoft.com/ja-jp/learn/modules/manage-users-and-groups-in-aad/2-create-aad>

# Azure AD と AD DS は別のも

## オンプレミス

Active Directory  
ドメインサービス (AD DS)

- **グループ ポリシー**や**組織単位 (OU)** を使用して、オンプレミスのコンピュータやユーザーを管理

## Azure

Azure Active Directory  
(Azure AD)

- オンプレミスのActive Directory のクラウドバージョンでは**ない**。オンプレミスの Active Directory を完全に置き換えることを目的としたものでも**ない**

Azure AD Connectを  
使った同期が可能

[https://ja.wikipedia.org/wiki/Active\\_Directory](https://ja.wikipedia.org/wiki/Active_Directory)

<https://docs.microsoft.com/ja-jp/windows-server/identity/ad-ds/ad-ds-getting-started>

<https://docs.microsoft.com/ja-jp/learn/modules/manage-users-and-groups-in-aad/2-create-aad>

- Module 1 ID
  - Azure Active Directory (Azure AD)
    - Azure AD : Azure ADで実現できること
    - Azure AD の概念 : テナントなどの用語
    - AD DS と Azure AD : オンプレミスのAD DSとの違い
    - Azure AD エディション : 4種類のエディションとライセンス
    - Azure AD 参加 / 登録 : デバイスからのAzure ADアクセス
    - セルフサービス パスワード リセット(SSPR) : パスワードリセット
  - ユーザーとグループ
    - ユーザー アカウント : ユーザーの種類は3つ
    - ユーザー アカウントの管理 : ユーザー管理の知識
    - 一括ユーザー アカウント : 大量のユーザーをCSVで一括登録
    - グループ アカウント : グループ管理の知識
    - 複数のディレクトリの管理 : ディレクトリの独立性
    - デモンストレーション - ユーザーとグループ
  - ラボ1



- Module 1 ID
  - Azure Active Directory (Azure AD)
    - Azure AD : Azure ADで実現できること
    - Azure AD の概念 : テナントなどの用語
    - AD DS と Azure AD : オンプレミスのAD DSとの違い
    - Azure AD エディション : 4種類のエディションとライセンス
    - Azure AD 参加 / 登録 : デバイスからのAzure ADアクセス
    - セルフサービスパスワードリセット(SSPR) : パスワードリセット
  - ユーザーとグループ
    - ユーザー アカウント : ユーザーの種類は3つ
    - ユーザー アカウントの管理 : ユーザー管理の知識
    - 一括ユーザー アカウント : 大量のユーザーをCSVで一括登録
    - グループ アカウント : グループ管理の知識
    - 複数のディレクトリの管理 : ディレクトリの独立性
    - デモンストレーション - ユーザーとグループ
  - ラボ1

- Module 1 ID
  - Azure Active Directory (Azure AD)
    - Azure AD : Azure ADで実現できること
    - Azure AD の概念 : テナントなどの用語
    - AD DS と Azure AD : オンプレミスのAD DSとの違い
    - Azure AD エディション : 4種類のエディションとライセンス
    - Azure AD 参加 / 登録 : デバイスからのAzure ADアクセス
    - セルフサービス パスワード リセット(SSPR) : パスワードリセット
  - ユーザーとグループ
    - ユーザー アカウント : ユーザーの種類は3つ
    - ユーザー アカウントの管理 : ユーザー管理の知識
    - 一括ユーザー アカウント : 大量のユーザーをCSVで一括登録
    - グループ アカウント : グループ管理の知識
    - 複数のディレクトリの管理 : ディレクトリの独立性
    - デモンストレーション - ユーザーとグループ
  - ラボ1

- Module 1 ID
  - Azure Active Directory (Azure AD)
    - Azure AD : Azure ADで実現できること
    - Azure AD の概念 : テナントなどの用語
    - AD DS と Azure AD : オンプレミスのAD DSとの違い
    - Azure AD エディション : 4種類のエディションとライセンス
    - Azure AD 参加 / 登録 : デバイスからのAzure ADアクセス
    - セルフサービス パスワード リセット(SSPR) : パスワードリセット
  - ユーザーとグループ
    - ユーザー アカウント : ユーザーの種類は3つ
    - ユーザー アカウントの管理 : ユーザー管理の知識
    - 一括ユーザー アカウント : 大量のユーザーをCSVで一括登録
    - グループ アカウント : グループ管理の知識
    - 複数のディレクトリの管理 : ディレクトリの独立性
    - デモンストレーション - ユーザーとグループ
  - ラボ1

- Module 1 ID
  - Azure Active Directory (Azure AD)
    - Azure AD : Azure ADで実現できること
    - Azure AD の概念 : テナントなどの用語
    - AD DS と Azure AD : オンプレミスのAD DSとの違い
    - Azure AD エディション : 4種類のエディションとライセンス
    - Azure AD 参加 / 登録 : デバイスからのAzure ADアクセス
    - セルフサービス パスワード リセット(SSPR) : パスワードリセット
  - ユーザーとグループ
    - ユーザー アカウント : ユーザーの種類は3つ
    - ユーザー アカウントの管理 : ユーザー管理の知識
    - 一括ユーザー アカウント : 大量のユーザーをCSVで一括登録
    - グループ アカウント : グループ管理の知識
    - 複数のディレクトリの管理 : ディレクトリの独立性
    - デモンストレーション - ユーザーとグループ
  - ラボ1

- Module 1 ID
  - Azure Active Directory (Azure AD)
    - Azure AD : Azure ADで実現できること
    - Azure AD の概念 : テナントなどの用語
    - AD DS と Azure AD : オンプレミスのAD DSとの違い
    - Azure AD エディション : 4種類のエディションとライセンス
    - Azure AD 参加 / 登録 : デバイスからのAzure ADアクセス
    - セルフサービス パスワード リセット(SSPR) : パスワードリセット
  - ユーザーとグループ
    - ユーザー アカウント : ユーザーの種類は3つ
    - ユーザー アカウントの管理 : ユーザー管理の知識
    - 一括ユーザー アカウント : 大量のユーザーをCSVで一括登録
    - グループ アカウント : グループ管理の知識
    - 複数のディレクトリの管理 : ディレクトリの独立性
    - デモンストレーション - ユーザーとグループ
  - ラボ1

- Module 1 ID
  - Azure Active Directory (Azure AD)
    - Azure AD : Azure ADで実現できること
    - Azure AD の概念 : テナントなどの用語
    - AD DS と Azure AD : オンプレミスのAD DSとの違い
    - Azure AD エディション : 4種類のエディションとライセンス
    - Azure AD 参加 / 登録 : デバイスからのAzure ADアクセス
    - セルフサービス パスワード リセット(SSPR) : パスワードリセット
  - ユーザーとグループ
    - ユーザー アカウント : ユーザーの種類は3つ
    - ユーザー アカウントの管理 : ユーザー管理の知識
    - 一括ユーザー アカウント : 大量のユーザーをCSVで一括登録
    - グループ アカウント : グループ管理の知識
    - 複数のディレクトリの管理 : ディレクトリの独立性
    - デモンストレーション - ユーザーとグループ
  - ラボ1

- Module 1 ID
  - Azure Active Directory (Azure AD)
    - Azure AD : Azure ADで実現できること
    - Azure AD の概念 : テナントなどの用語
    - AD DS と Azure AD : オンプレミスのAD DSとの違い
    - Azure AD エディション : 4種類のエディションとライセンス
    - Azure AD 参加 / 登録 : デバイスからのAzure ADアクセス
    - セルフサービス パスワード リセット(SSPR) : パスワードリセット
  - ユーザーとグループ
    - ユーザー アカウント : ユーザーの種類は3つ
    - ユーザー アカウントの管理 : ユーザー管理の知識
    - 一括ユーザー アカウント : 大量のユーザーをCSVで一括登録
    - グループ アカウント : グループ管理の知識
    - 複数のディレクトリの管理 : ディレクトリの独立性
    - デモンストレーション - ユーザーとグループ
  - ラボ1

- Module 1 ID
  - Azure Active Directory (Azure AD)
    - Azure AD : Azure ADで実現できること
    - Azure AD の概念 : テナントなどの用語
    - AD DS と Azure AD : オンプレミスのAD DSとの違い
    - Azure AD エディション : 4種類のエディションとライセンス
    - Azure AD 参加 / 登録 : デバイスからのAzure ADアクセス
    - セルフサービス パスワード リセット(SSPR) : パスワードリセット
  - ユーザーとグループ
    - ユーザー アカウント : ユーザーの種類は3つ
    - ユーザー アカウントの管理 : ユーザー管理の知識
    - 一括ユーザー アカウント : 大量のユーザーをCSVで一括登録
    - グループ アカウント : グループ管理の知識
    - 複数のディレクトリの管理 : ディレクトリの独立性
    - デモンストレーション - ユーザーとグループ
  - ラボ1



- Module 1 ID
  - Azure Active Directory (Azure AD)
    - Azure AD : Azure ADで実現できること
    - Azure AD の概念 : テナントなどの用語
    - AD DS と Azure AD : オンプレミスのAD DSとの違い
    - Azure AD エディション : 4種類のエディションとライセンス
    - Azure AD 参加 / 登録 : デバイスからのAzure ADアクセス
    - セルフサービス パスワード リセット(SSPR) : パスワードリセット
  - ユーザーとグループ
    - ユーザー アカウント : ユーザーの種類は3つ
    - ユーザー アカウントの管理 : ユーザー管理の知識
    - 一括ユーザー アカウント : 大量のユーザーをCSVで一括登録
    - グループ アカウント : グループ管理の知識
    - 複数のディレクトリの管理 : ディレクトリの独立性
    - デモンストレーション - ユーザーとグループ
  - ラボ1