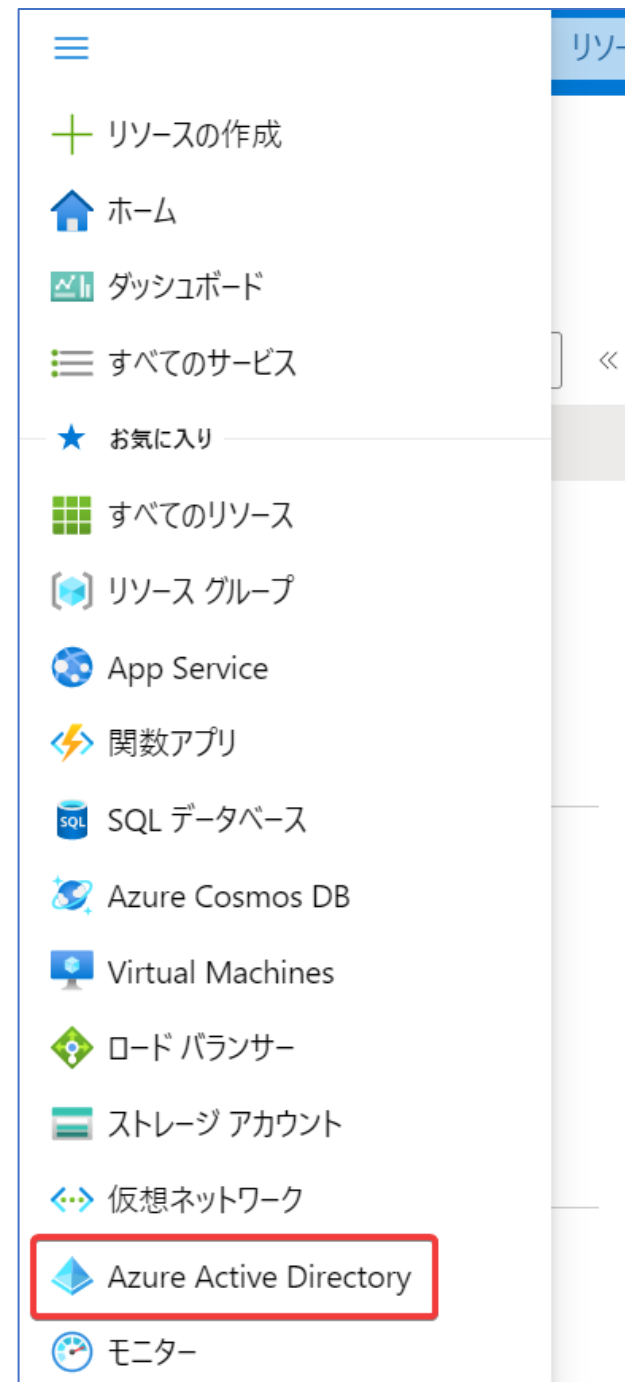




Azure Active Directory (Azure AD)

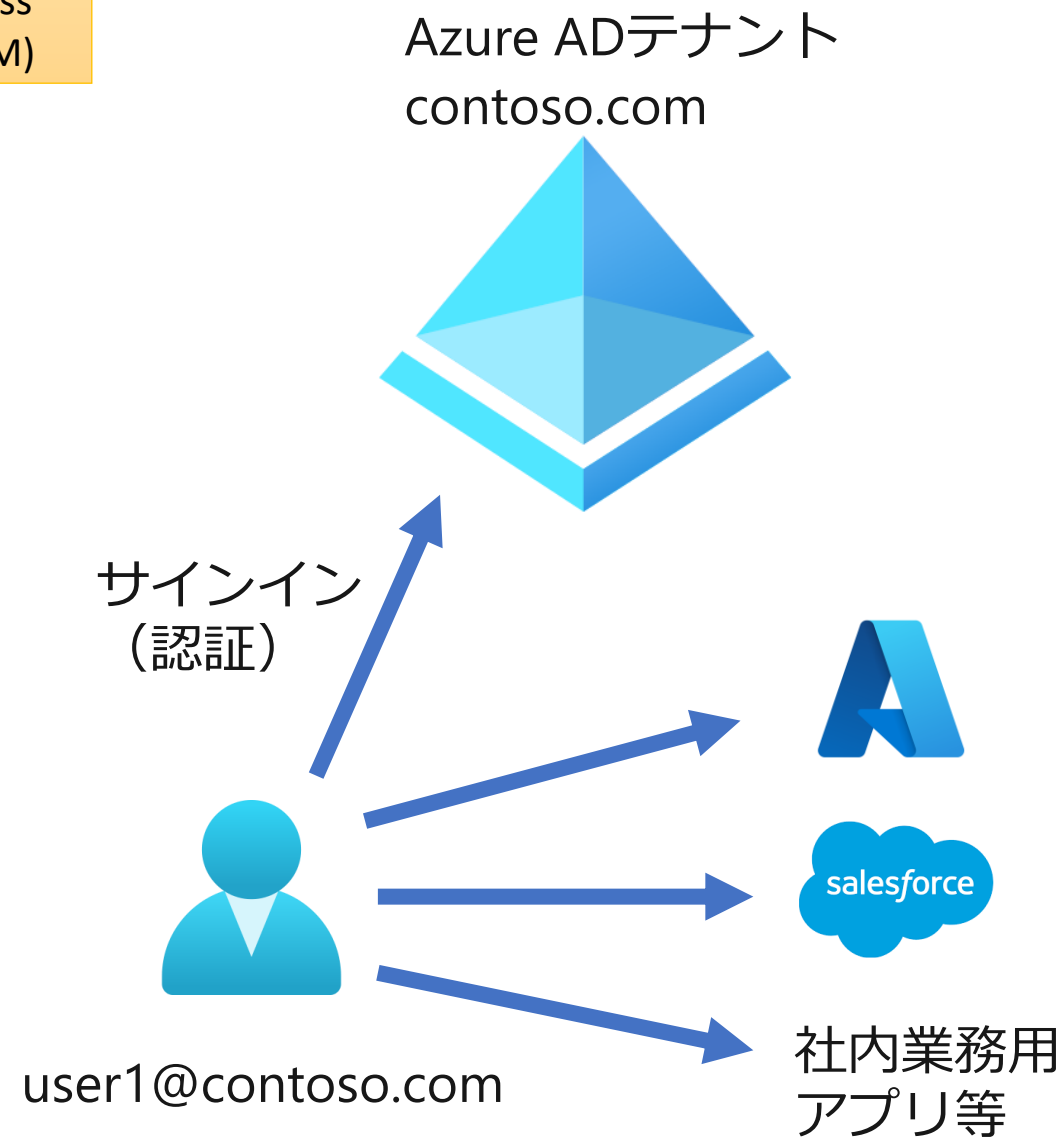
Azure ADとは？



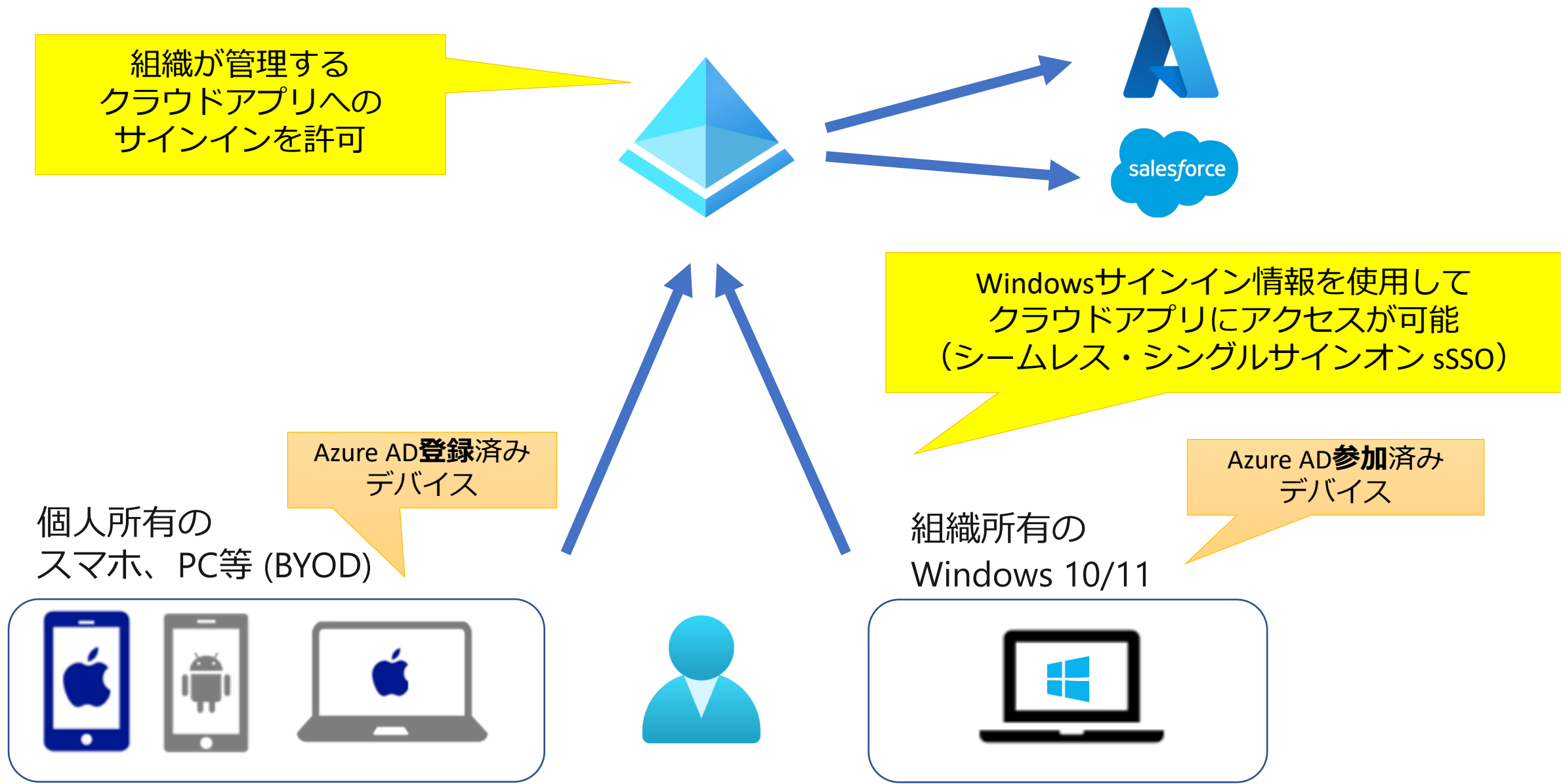
Azure AD とは

Identity and Access
Management (IAM)


- クラウドベースの「**IDおよびアクセス管理**」サービス
- ユーザーIDなどを一元管理する**認証基盤**
- Microsoft Azure、Microsoft 365などへのサインイン（**ユーザー認証**）で利用される
- クラウドアプリ（Salesforce、Dropbox、ServiceNowなど）へのサインインでも利用できる
- ユーザーが開発した独自の業務アプリなどへのサインインでも利用できる
- 一度サインインすれば、いろいろなサービスやアプリにアクセスできる（**シングルサインオン**）



Webブラウザからのサインインに加え、さまざまなデバイスからのサインインにも対応



Azure ADテナント

Azure ADで、ユーザー、グループ、アプリなどを管理する部分を「 テナント」という

Azure ADテナント
contoso.com



ユーザーID等の管理



Azure AD
ユーザー

Azure ADのテナントはそれぞれの「組織」（会社や学校など）ごとに作られる

Azure ADテナント
aaa.com



user1@aaa.com

Azure ADテナント
bbb.com



user1@bbb.com

Azure ADテナント
ccc.com



user1@ccc.com

各テナントや、そこに属するユーザーは
ドメイン名で区別される

個人ユーザーのサインアップによるAzure ADテナントとAzureサブスクリプションの作成例

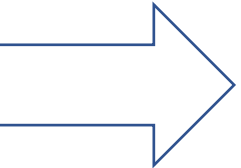
テナントとサブスクリプションが
作成される

このドメイン名はあとで変更が可能

Azure AD テナント
tarooutlook.onmicrosoft.com

Azure
サブスクリプション

Microsoftアカウントを作成
taro@outlook.jp



Azureにサインアップ

- ・ 利用規約に同意
- ・ 個人情報を登録
- ・ 支払い方法を設定



関連付け

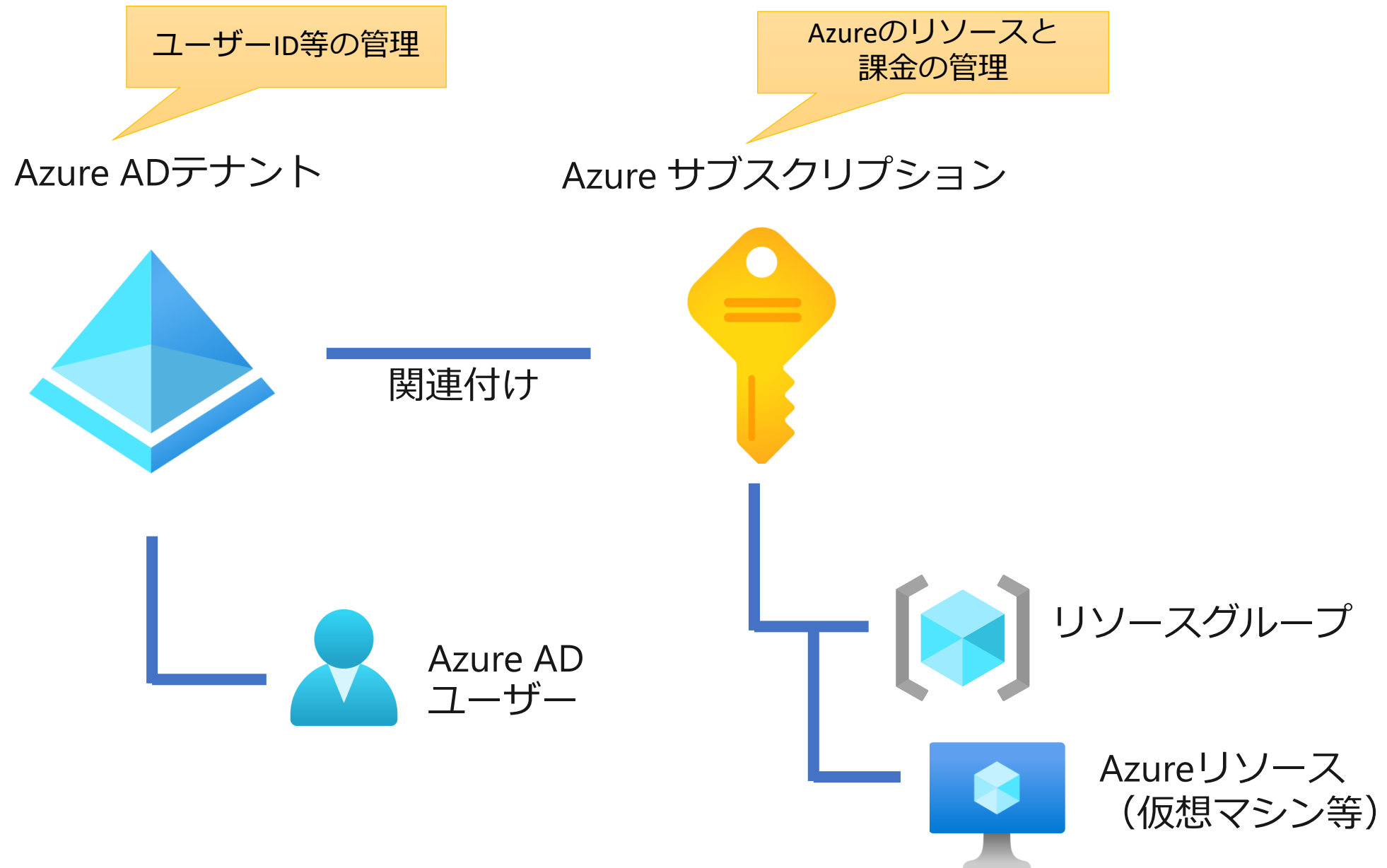


Azure AD
ユーザー

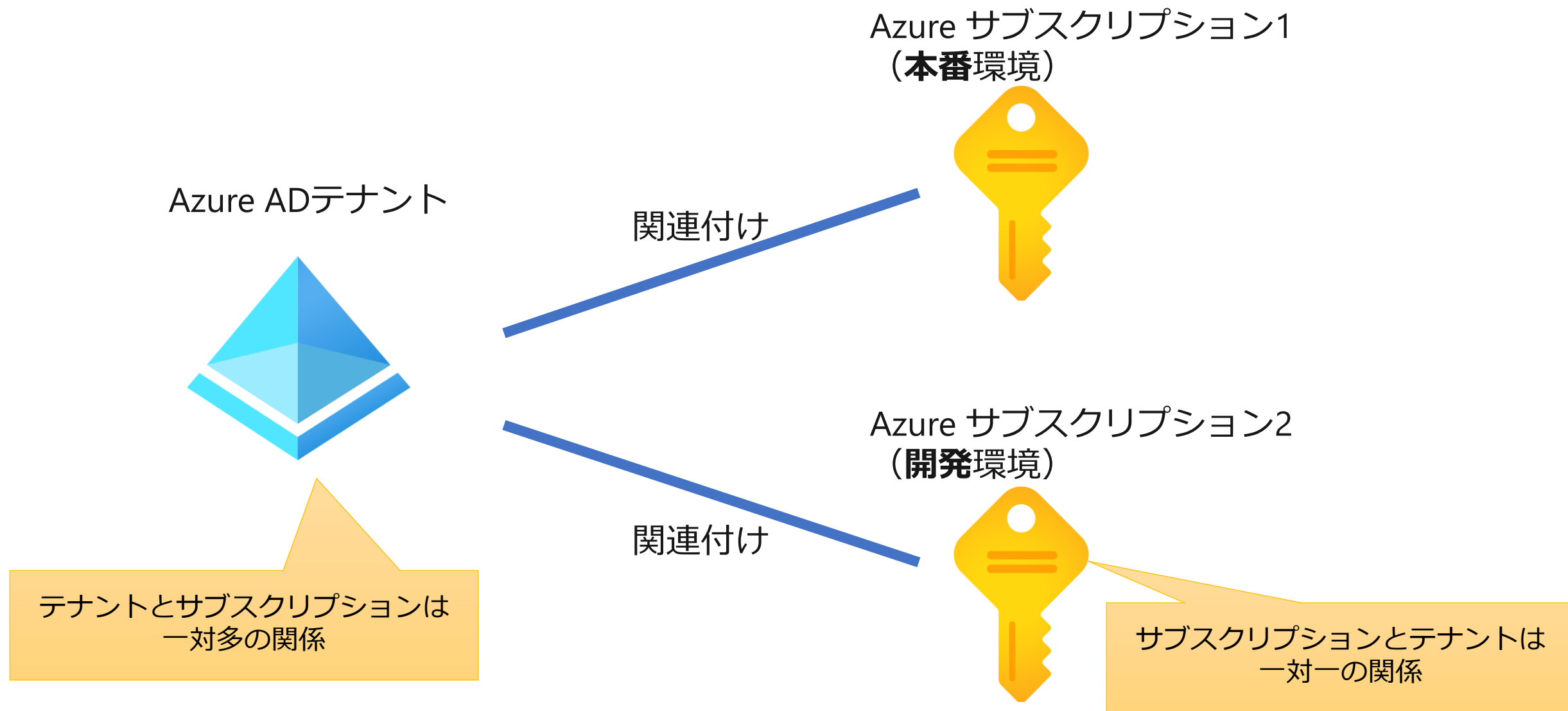
最初のAzure ADユーザーとして
テナントに登録される

Azure ADテナントと Azure サブスクリプション

「Azure ADテナント」と「Azureサブスクリプション」の違い



1つのテナントで複数のサブスクリプションを利用できる

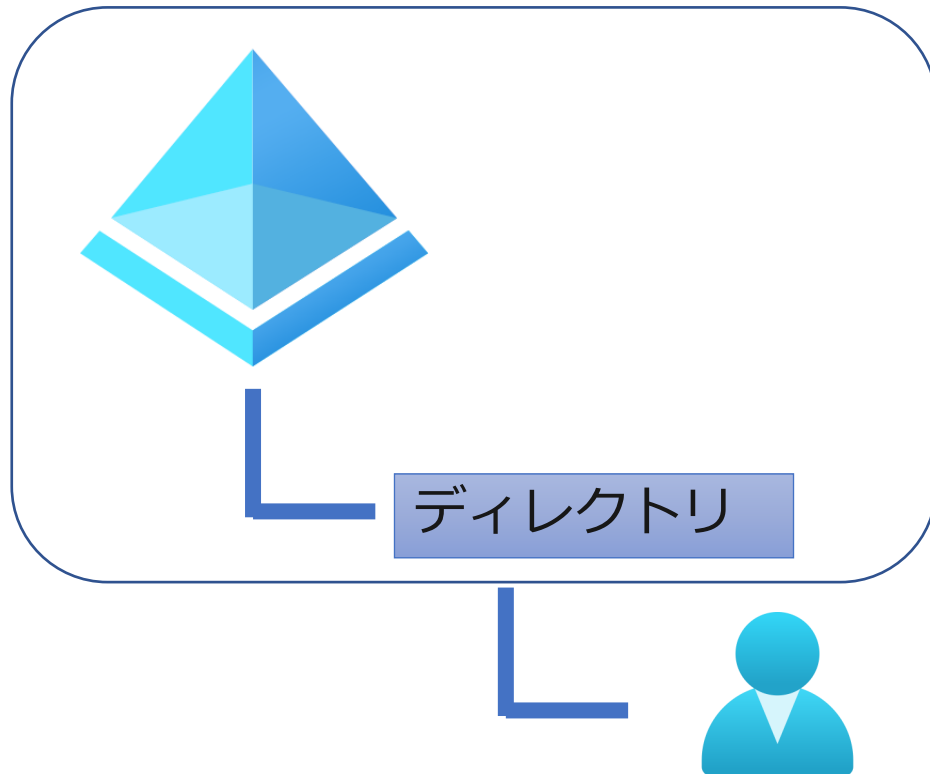


※テナントとサブスクリプションの関連付けは「信頼関係」とも呼ばれる

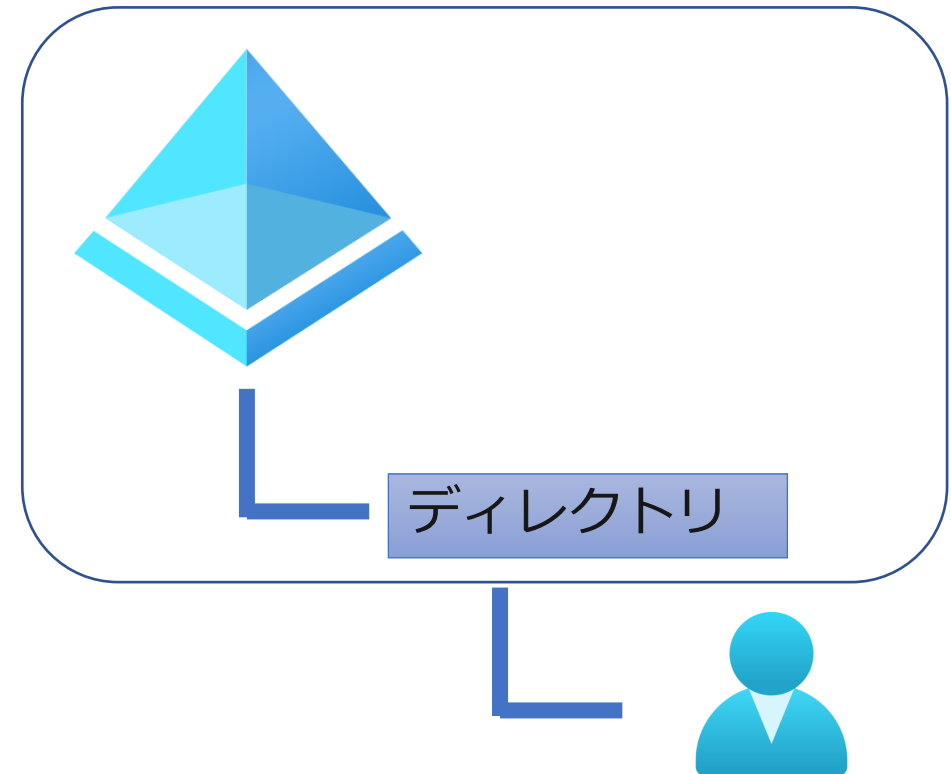
Azure ADの 「テナント」と「ディレクトリ」

各Azure ADテナントは、それぞれ、ただ1つの「ディレクトリ」を持つ

Azure ADテナント



Azure ADテナント



Azure ADのドキュメントやAzure portalなどに、たまに「ディレクトリ」という言葉が出てくるが、基本的には「テナントと同じもの」と考えてよい。
ディレクトリはテナント内部で自動的に管理されるため、特に意識する必要はない。

Active Directory Domain Service (AD DS) vs Azure AD

従来のオンプレミス環境で用いられてきた AD DS と
Azure ADの違いは？

AD DS と Azure ADの違い

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
- ユーザー、サーバー、グループなど、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
- **オンプレミスのファイアウォールの内部**で運用
- ※Active Directory = ドメインの機能を中心とする機能の集まり
- ※ドメイン = 社内のコンピューターやユーザーなどをまとめて管理する仕組み
- ※ドメインコントローラー = ドメインの機能を提供するサーバー。LDAPに基づくデータ管理、Kerberosプロトコルによる認証・承認、グループポリシーを使用した設定の一元管理を行う。

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（認証基盤）
- Microsoft Azure、Microsoft 365などのサービスへのサインインに利用される
- さまざまなクラウドアプリ（Salesforce、Dropbox、ServiceNowなど）へのサインインに利用できる
- ユーザーが開発した業務アプリなどへのサインインにも利用できる

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>

どちらも「Active Directory (AD)」という名前が付いているが・・・はっきり言って別物！

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
- 対応プロトコル: **Kerberos, NTLM, LDAP**

Azure



Azure Active Directory
(Azure AD)

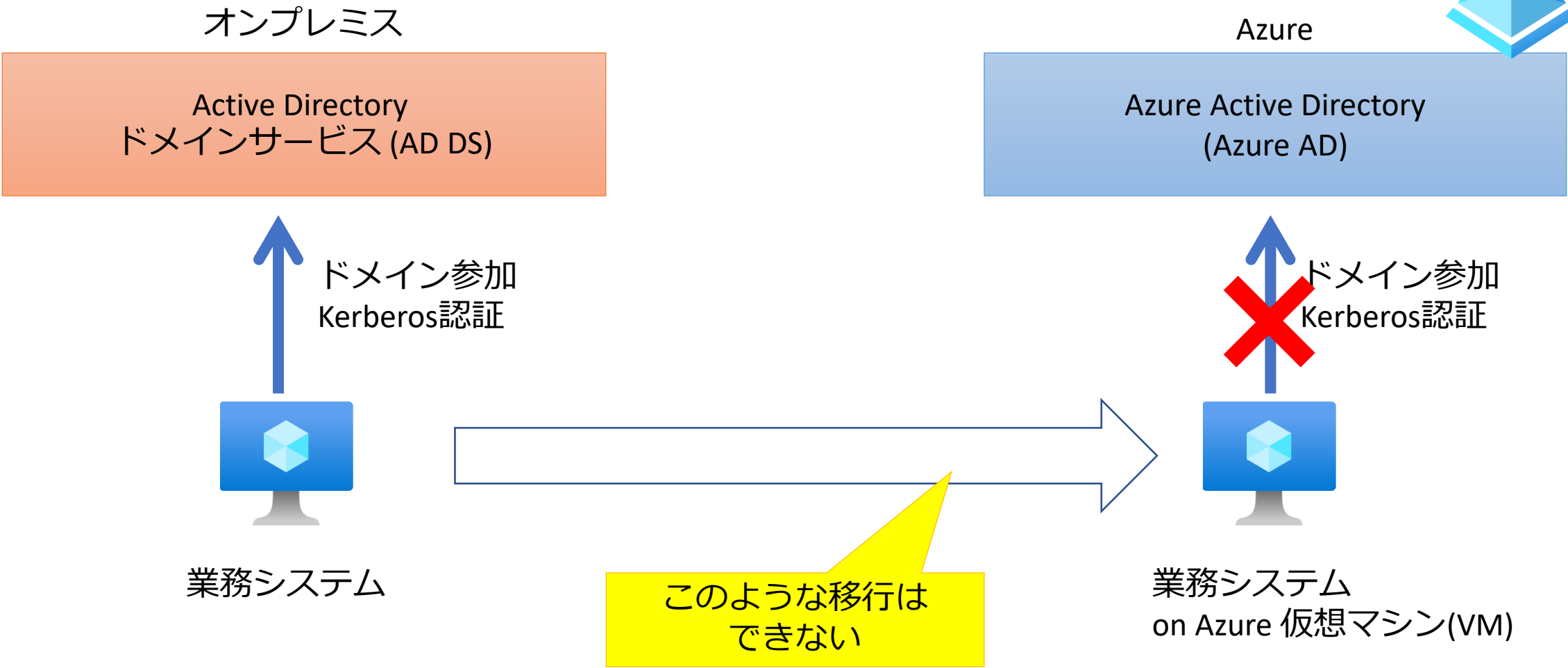
- オンプレミスのActive Directory のクラウドバージョンでは**ない**。
- オンプレミスの Active Directory を完全に置き換えることを目的としたものではない
- 対応プロトコル: **SAML, OpenID Connect, OAuth 2.0**
- **オンプレミスAD DSとの互換性はない**

https://ja.wikipedia.org/wiki/Active_Directory

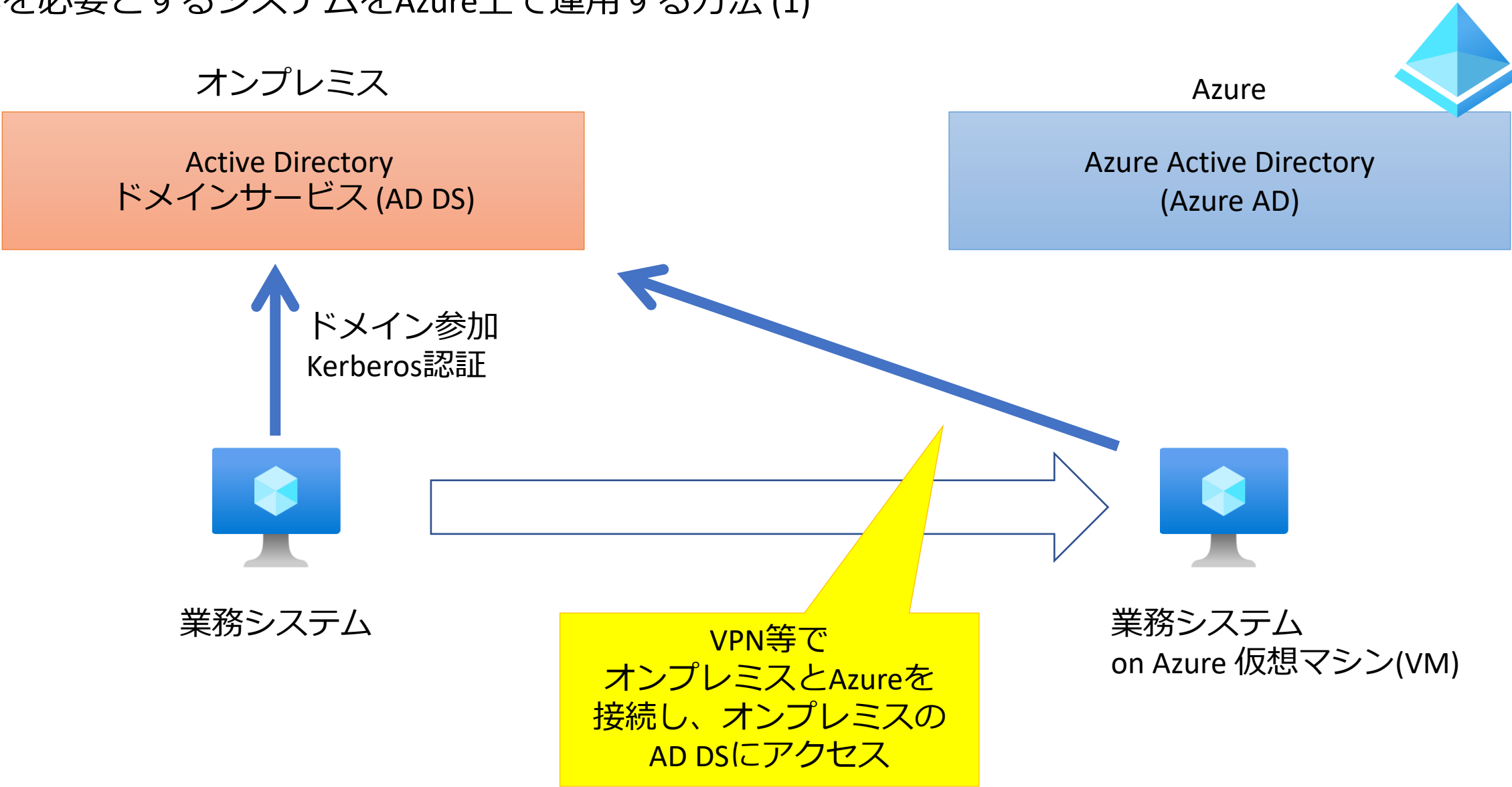
<https://docs.microsoft.com/ja-jp/windows-server/identity/ad-ds/ad-ds-getting-started>

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

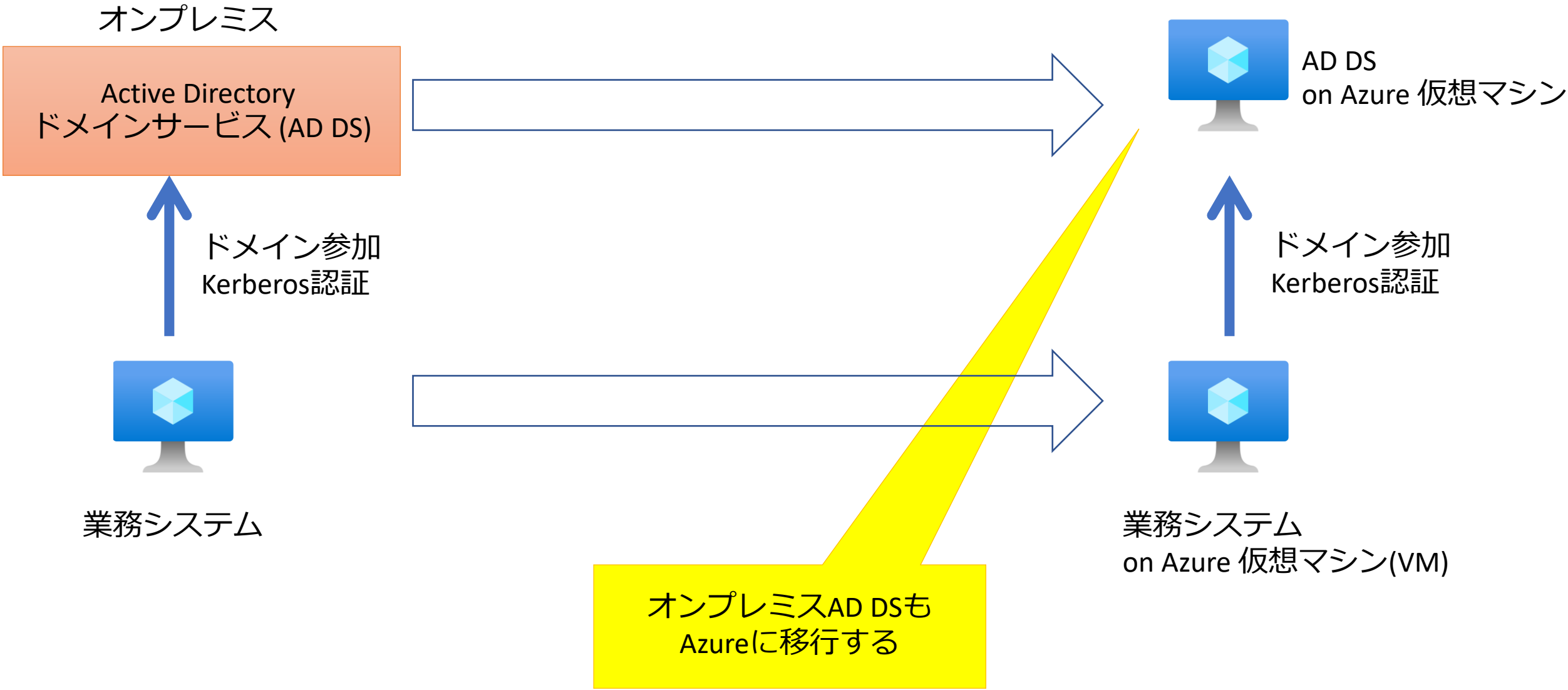
互換性がないため、AD DSの機能を必要とするシステムを Azure ADに接続することはできない



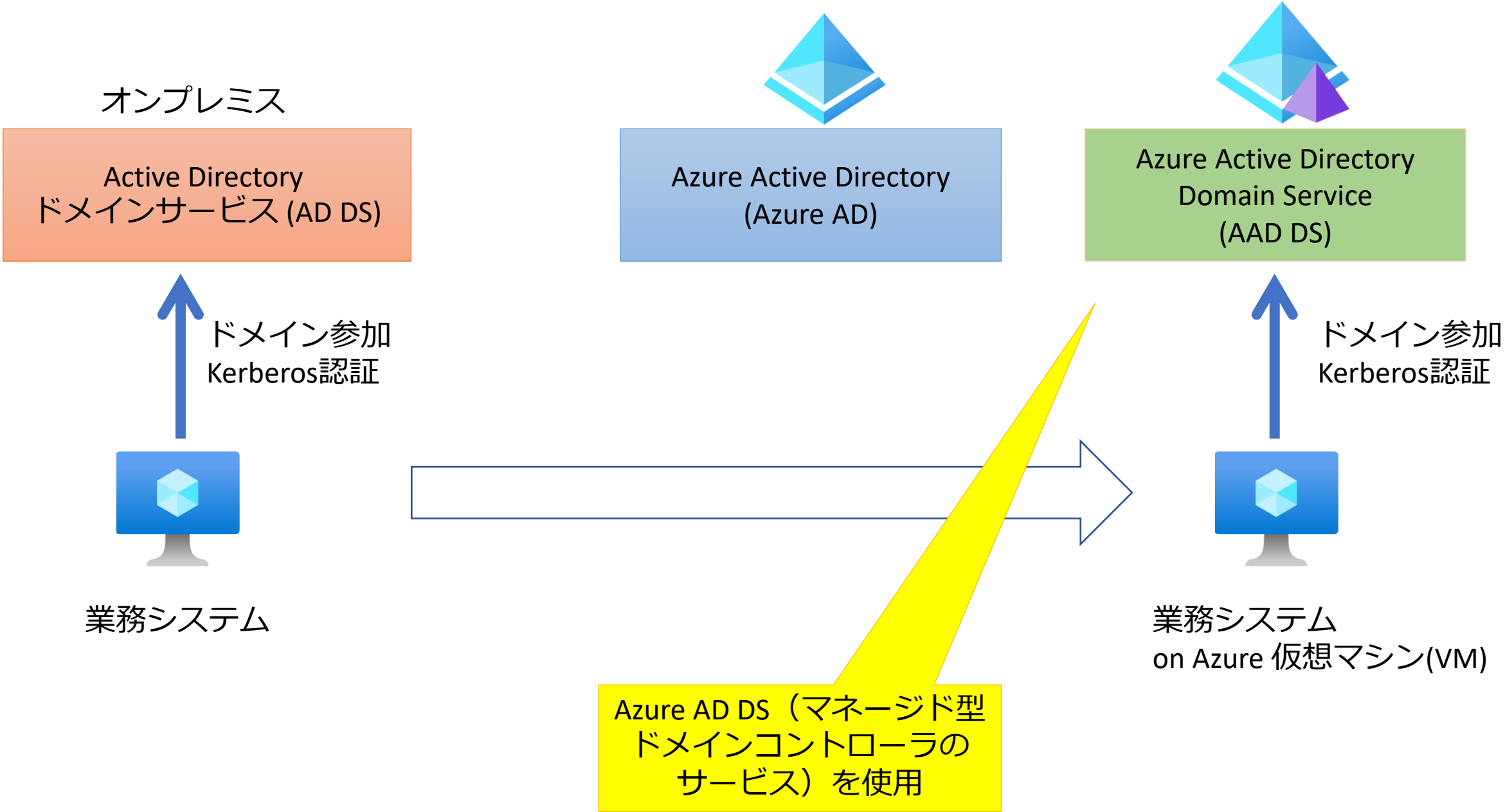
AD DSを必要とするシステムをAzure上で運用する方法 (1)



AD DSを必要とするシステムをAzure上で運用する方法 (2)



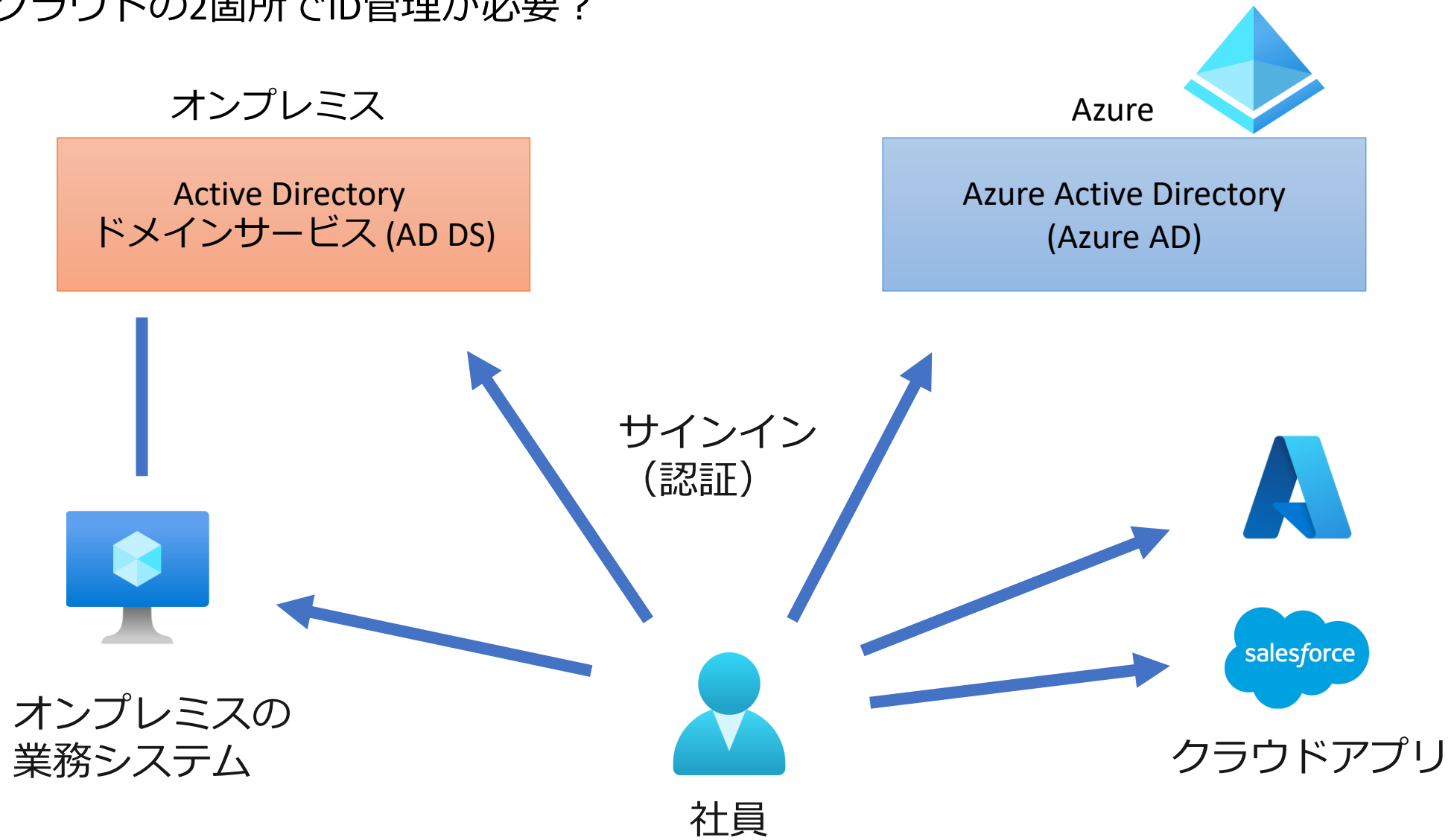
AD DSを必要とするシステムをAzure上で運用する方法 (3)



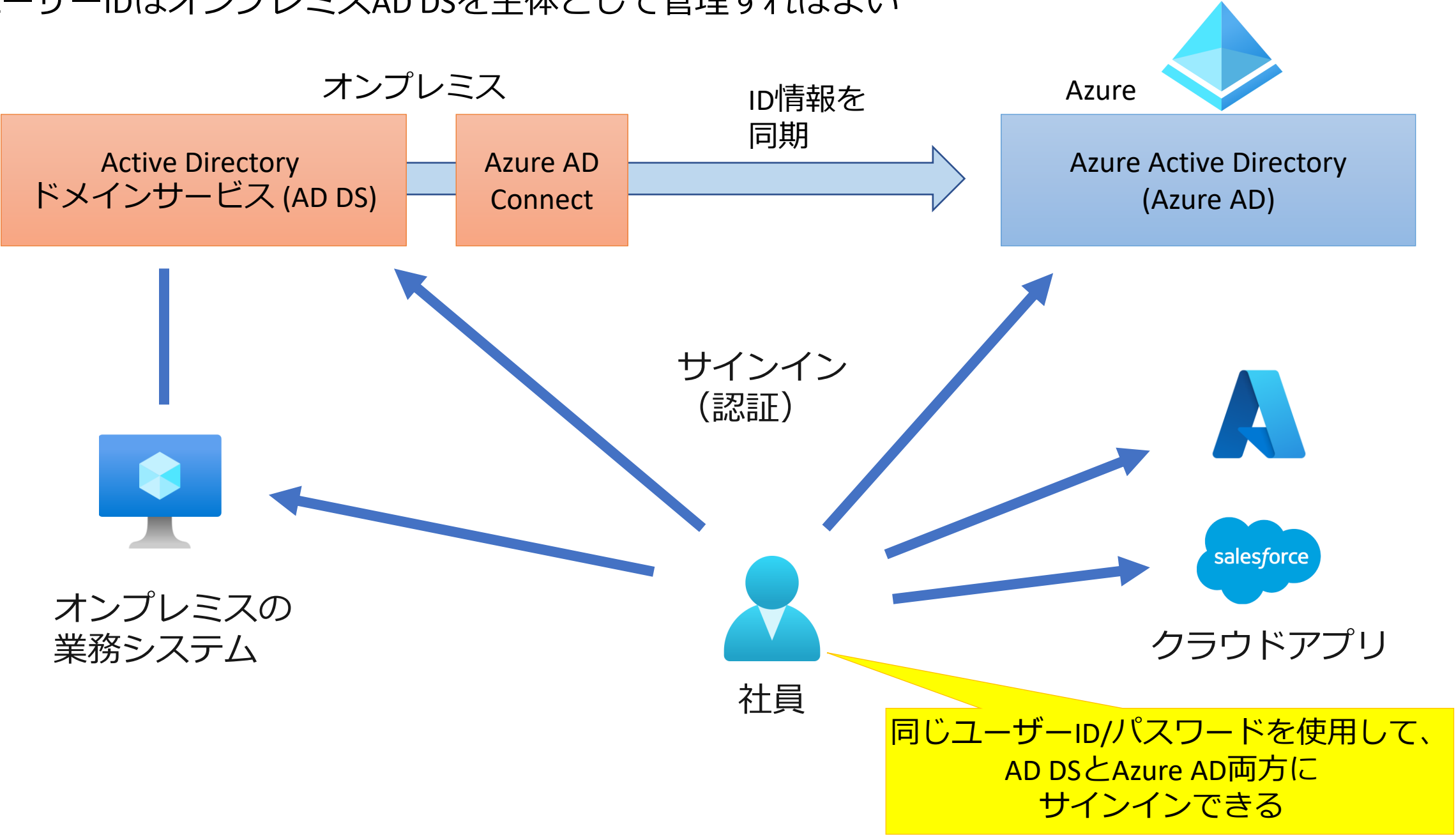
ハイブリッドID

オンプレミスAD DSとAzure ADを両方とも利用しつつ
ユーザーIDの管理を一元化

オンプレミスのAD DSを引き続き使いつつ、Azure ADも使いたい場合・・・
オンプレとクラウドの2箇所でID管理が必要？

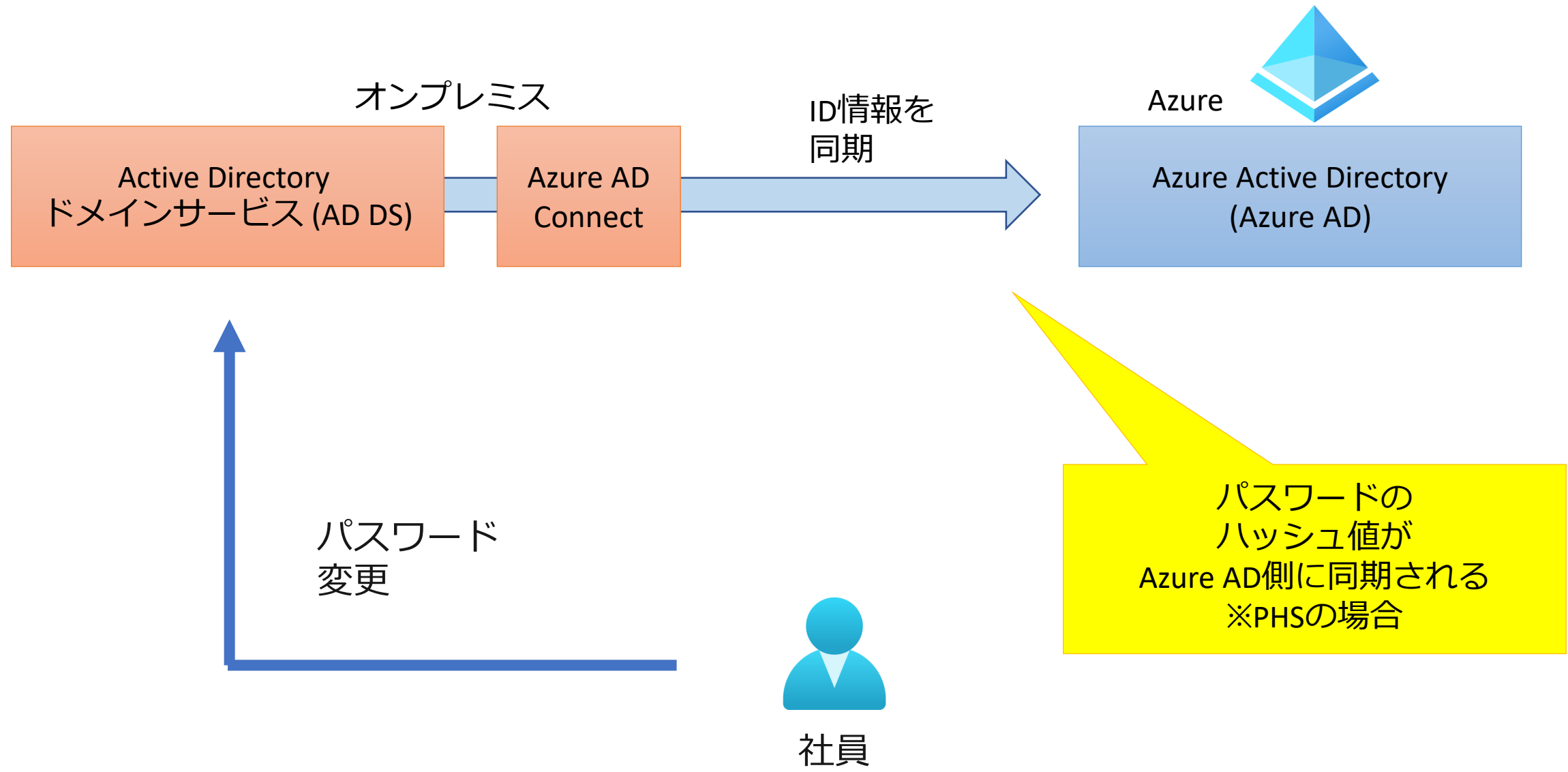


Azure AD Connect を使用して、オンプレミスのユーザーID情報をAzure ADに「同期」 (sync) できる。
ユーザーIDはオンプレミスAD DSを主体として管理すればよい

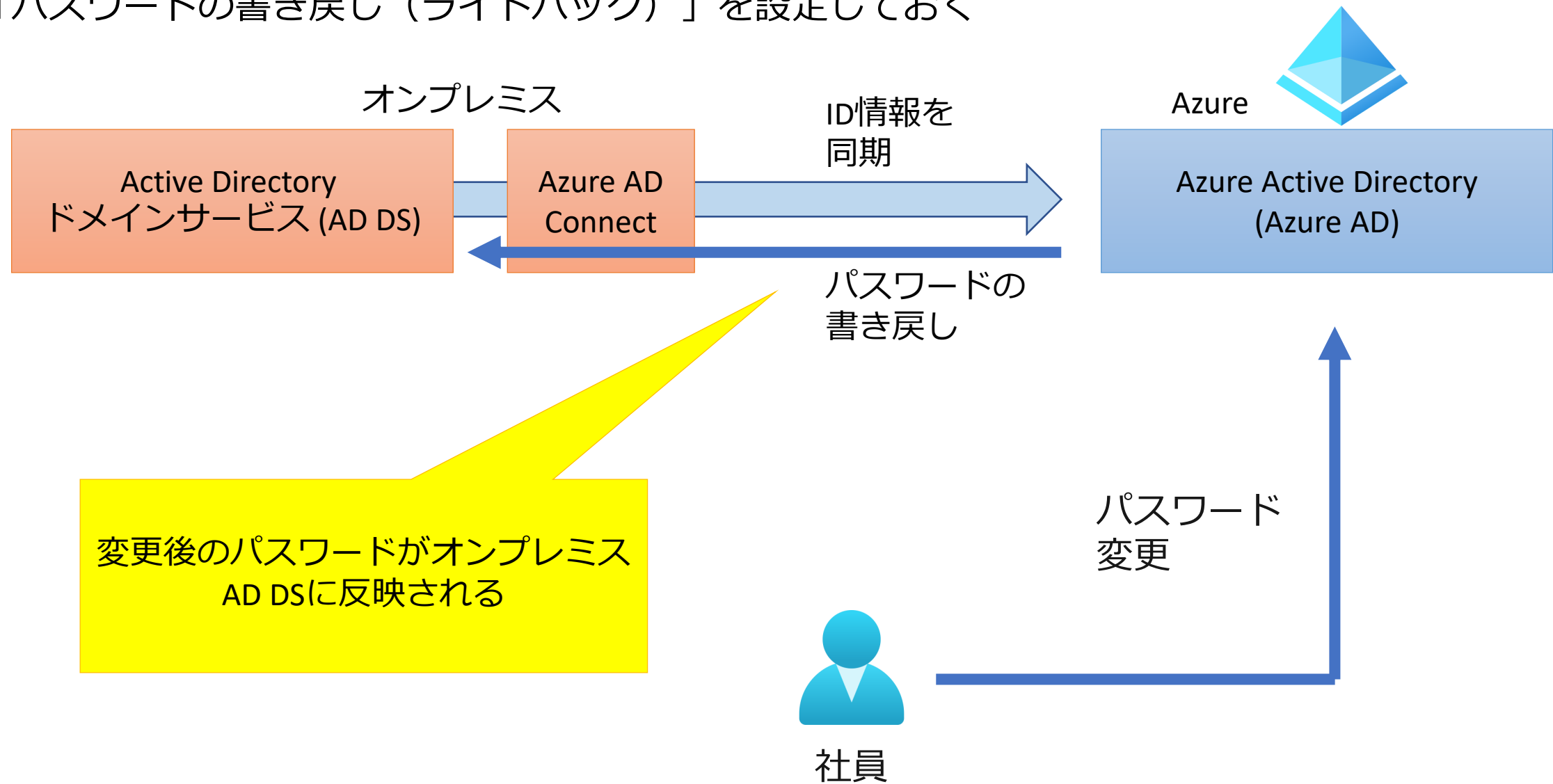


ハイブリッドIDにおける パスワード変更

オンプレ側でのパスワード変更: 特に問題なし



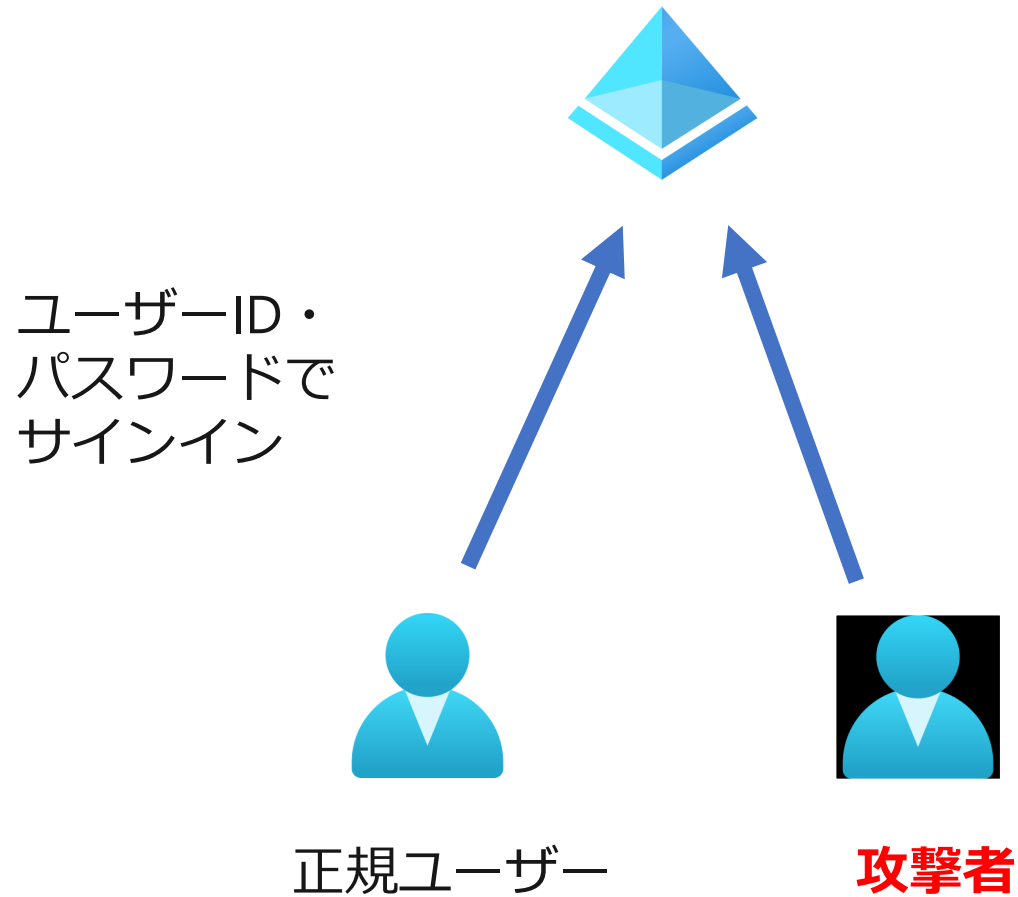
クラウド（Azure AD）側でのパスワード変更: Azure AD Connectで、「パスワードの書き戻し（ライトバック）」を設定しておく



多要素認証

(Multi-Factor Authentication, MFA)

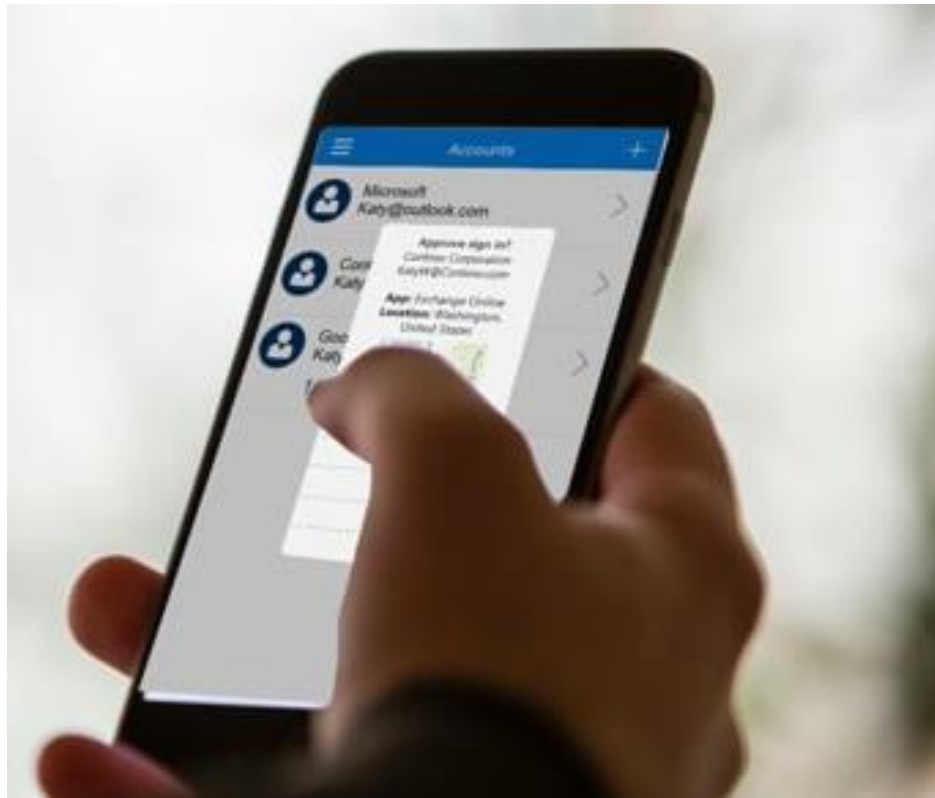
ユーザーIDとパスワードだけによる認証は、もはや危険



- 多数のユーザーIDに対しよく使われるパスワードを試行（パスワードスプレー攻撃）
- パスワードを総当りで試行（ブルートフォース攻撃）
- ユーザーを偽サイトに誘導してパスワードを盗む（フィッシング）
- キーロガーを使用してパスワードを盗む
- キー入力を肩越しに盗み見る（ショルダーハッキング）
- 管理者などになりすまし、緊急を装ってパスワードを聞き出す（ソーシャルエンジニアリング）
- ダークウェブに流出したパスワードを入手

Azure ADは**多要素認証(MFA)**に対応。モバイル向け無料アプリ「Microsoft Authenticator」も提供

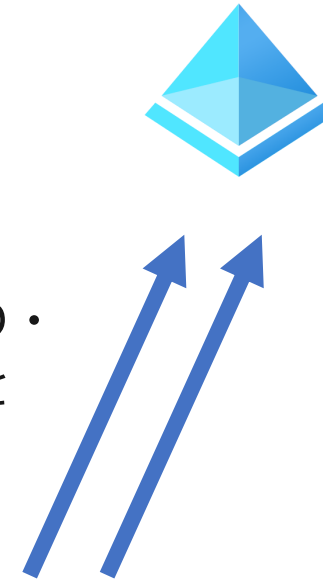
初回のみ：Azure ADへの初回サインインの際に、
所有するモバイル端末（スマホ）に「Microsoft
Authenticator」をインストールし、Azure ADと連
携させる



①ユーザーID・
パスワードを
入力



②所有するモバイ
ル端末（スマホ）
のロックを解除し、
「Microsoft
Authenticator」に
送信された通知を
タップ



もし、ユーザーがMFAを設定したデバイスを**紛失**してしまった場合は・・・

対応はマイクロソフトではなく **Azure ADテナントの管理者が行う**。

管理者は、対象ユーザーのMFA設定のリセットを実行する。

ユーザーは、新しいデバイスを使用してMFAの再設定を行う。

パスワードリセット

もし、Azure ADのユーザーがパスワードを忘れてしまった場合は・・・

対応はマイクロソフトではなく **Azure ADテナントの管理者が行う**。

Azure ADテナントの管理者は、Azure ADユーザーのパスワードを手動でリセットできる。

リセットすると仮パスワードが発行される。管理者はその仮パスワードをユーザーに伝達する。

ユーザーは、伝達された仮パスワードでサインインして、パスワードを再設定する。

ただ、この過程に **手間とコストがかかる**！

（特に、多数のユーザーが所属する組織で、手間とコストが問題となる）

Azure ADの**セルフサービスパスワードリセット（SSPR）**を有効にする。

ユーザーは必要な際に自分でパスワードのリセットを実行できる。

事前に設定されたMicrosoft Authenticatorなどを使用した本人確認の後に、新しいパスワードを設定できる。

