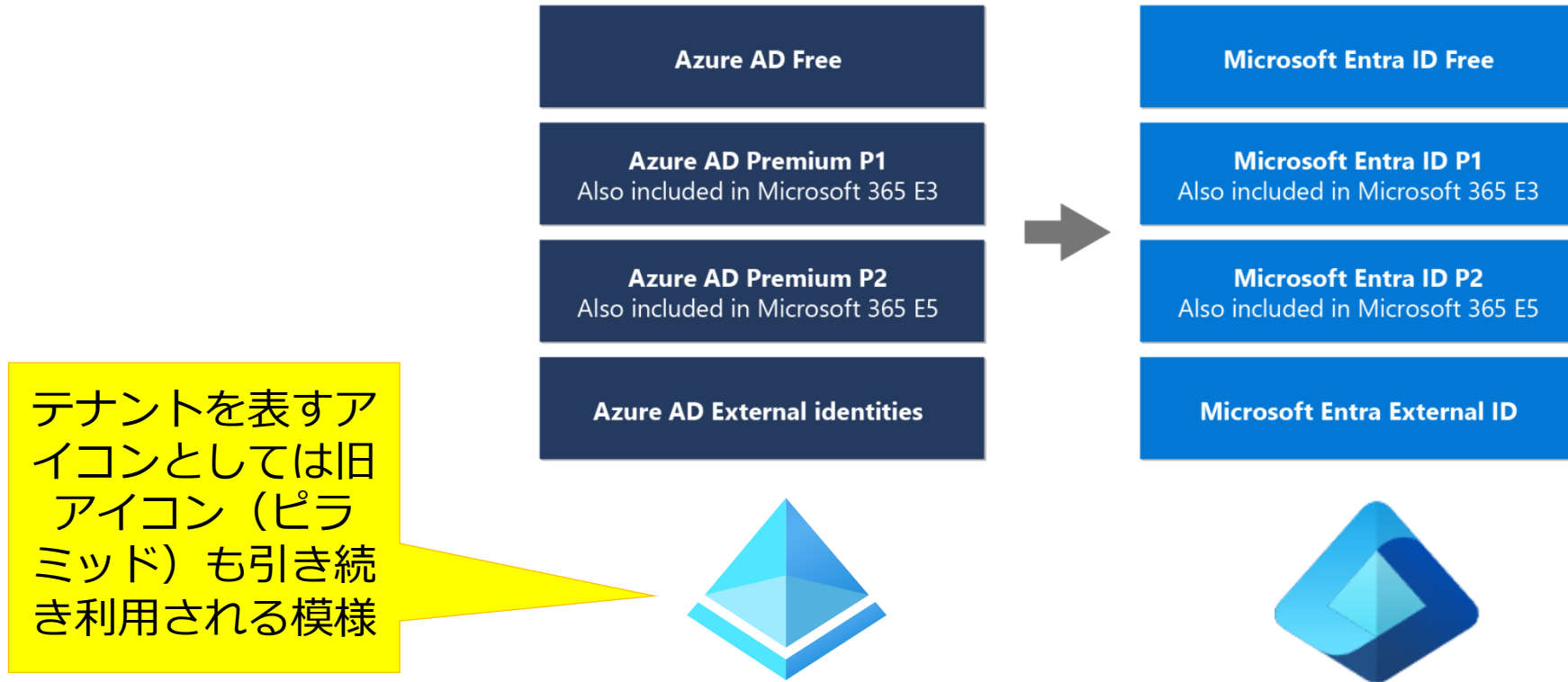




Microsoft Entra ID
(旧 Azure AD)



2023/7/11～、Azure ADは「Entra ID」に名称変更（リブランディング）。ただし、機能・料金には変更はない。



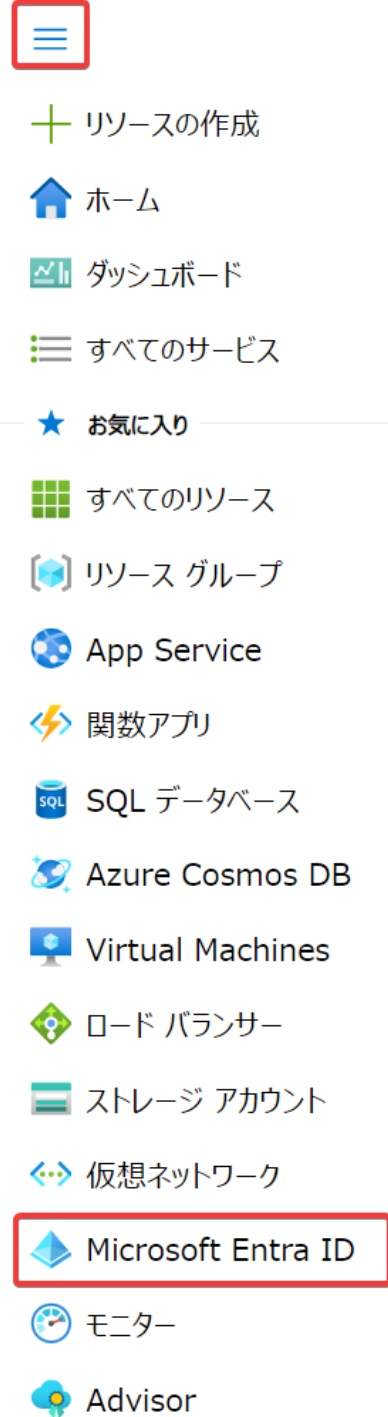
ドキュメント、Azure portal（管理画面）などの対応は現在進行中。
旧名称の「Azure AD」として表示されている部分もまだたくさんある。
→本資料では新名称「Entra ID」で解説

<https://mitomoha.hatenablog.com/entry/2023/08/05/024849>

<https://learn.microsoft.com/ja-jp/azure/active-directory/fundamentals/new-name>

<https://news.microsoft.com/ja-jp/2023/07/12/230712-azure-ad-is-becoming-microsoft-entra-id/>

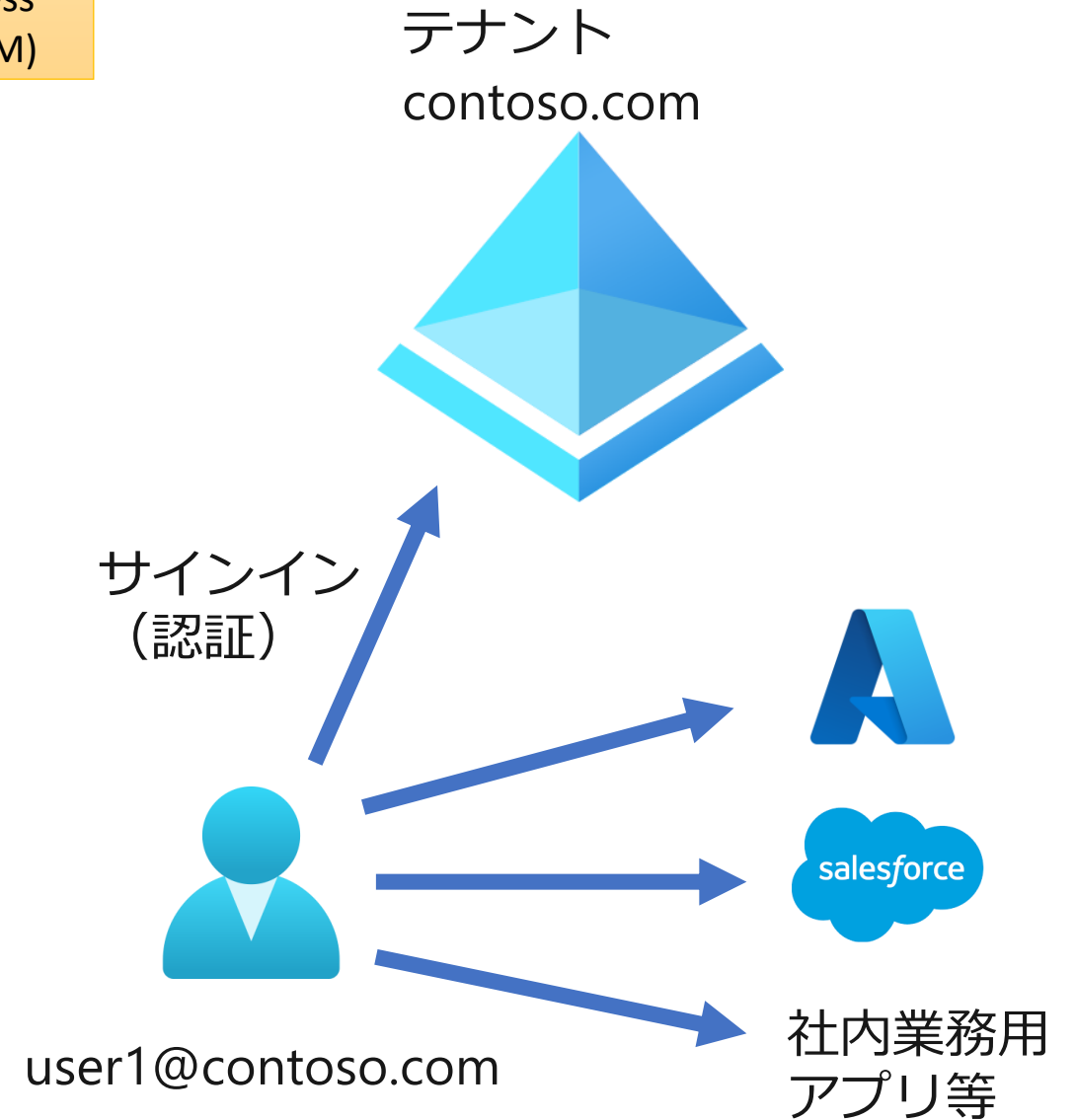
Entra IDとは？



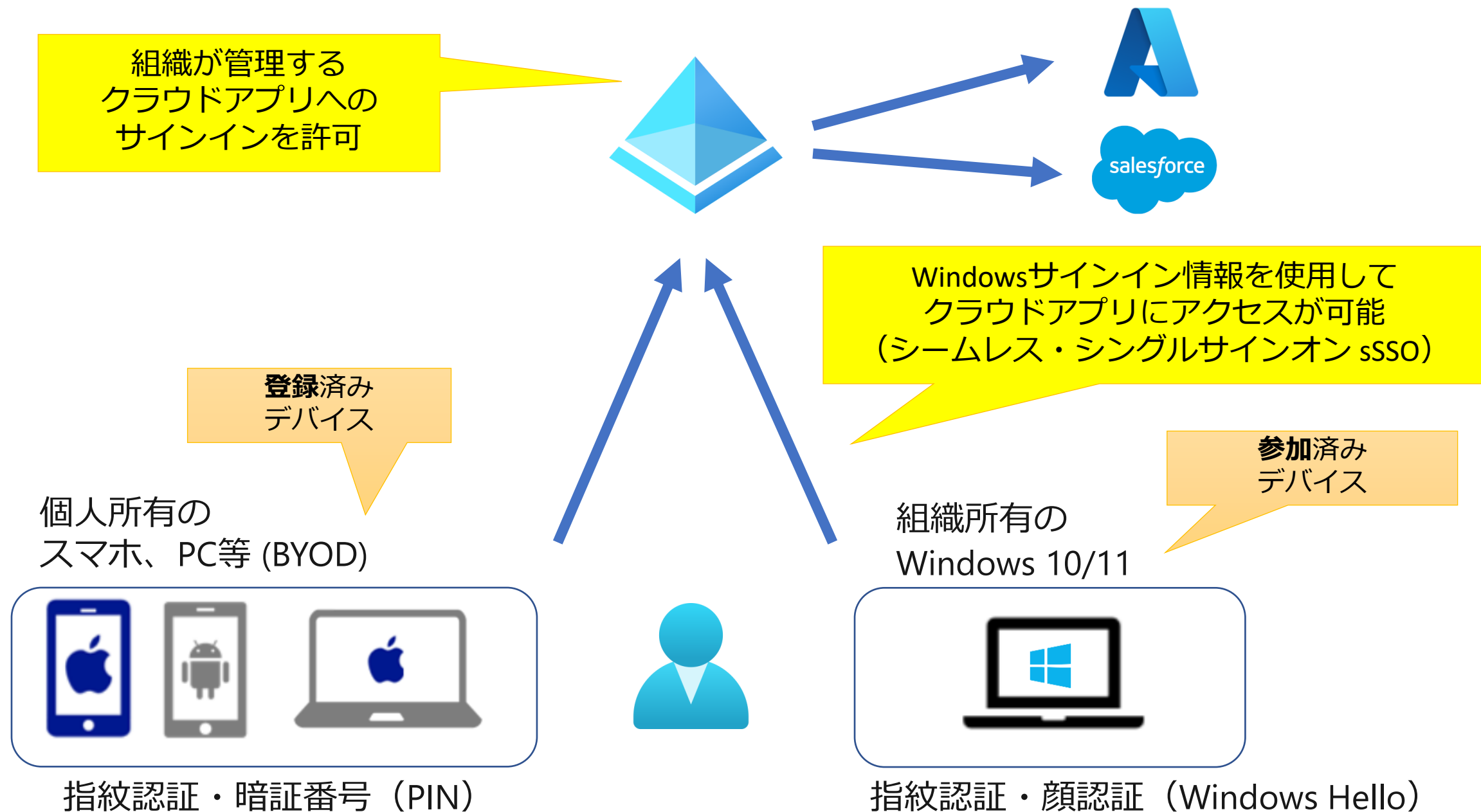
Entra ID とは

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
- サードパーティ製のクラウドアプリ（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





Active Directory Domain Service (AD DS) vs Entra ID

オンプレミス環境で用いられている AD DS と
Entra IDの違いは？

AD DS と Entra ID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、ボリューム、プリンターなどのネットワーク上の**オブジェクト**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。

クラウド

Microsoft Entra ID
(旧 Azure Active Directory)



- **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
- 2023/7 Azure Active Directoryが「Microsoft Entra ID」に名称変更。

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>

この2つは別のもの。互換性はない。

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**

クラウド

Microsoft Entra ID
(旧 Azure Active Directory)





- 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, WS Federation**
- **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>

テナント



 Microsoft Azure  リソース、サービス、ドキュメント

ホーム > Contoso | 概要 >


テナントの管理 ...


 作成  更新  列 |  スイッチ  削除

現在のテナント: Contoso

 テナントの検索  フィルターの追加

1 件の結果の 1 を表示しています

<input type="checkbox"/>	組織名	↑↓
<input type="checkbox"/>	 Contoso (既定)	

Entra ID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

Entra IDテナント
contoso.com



ユーザーID等の管理



Azure AD
ユーザー

Entra ID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



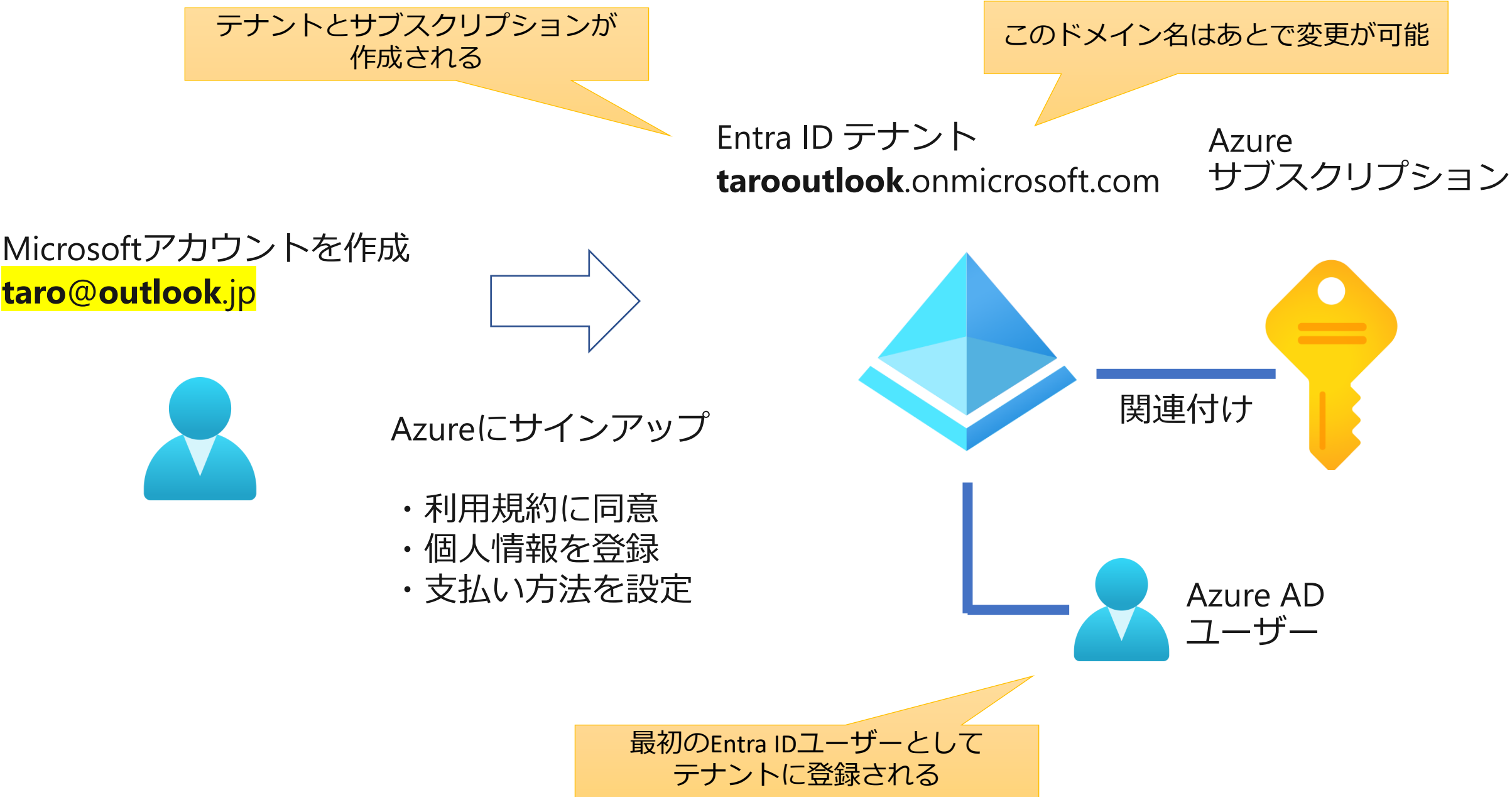
各テナントや、そこに属するユーザーは
ドメイン名で区別される

新しいテナントの作成

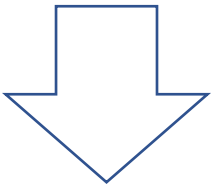
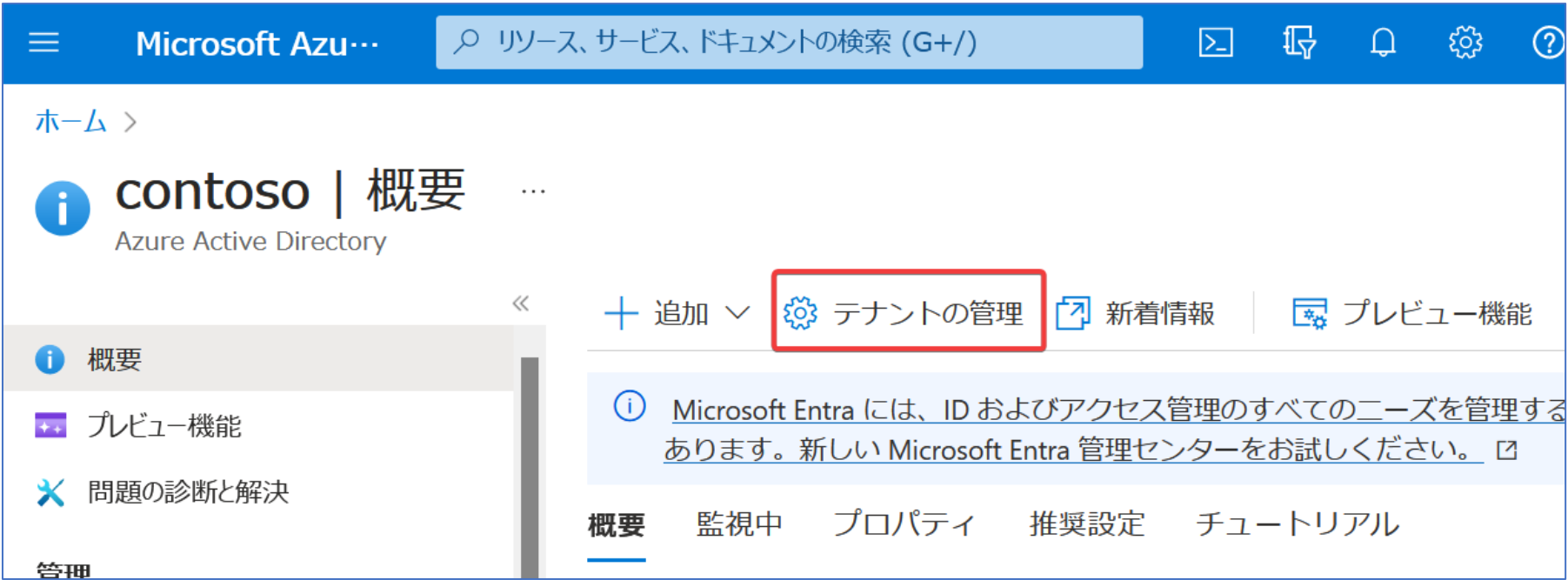
基本的には「1組織1テナント」で運用する。

検証用などのテナントを追加することもできる

AzureへのサインアップによるEntra IDテナントとAzureサブスクリプションの作成例



Azure portalからは、検証などに使用するための別テナントを簡単に作成することもできる



追加のテナントを作成した場合、「ディレクトリとサブスクリプション」ボタンで切り替えができる

 Microsoft Azure

お気に入り

すべてのディレクトリ

ディレクトリ名 ↑↓

☆ aaa.com (現在のテナント)

☆ bbb.com (新しいテナント)

✓ 現在

切り替え

「ディレクトリ」は
「テナント」と
同じ意味

ユーザーとグループ

テナントを作成した際、最初のユーザーには、**グローバル管理者**ロールが割り当てられる。
テナントの**グローバル管理者**は、**そのテナントのすべての操作**が可能。

テナント



最初のユーザー taro
(ロール: **グローバル管理者**)

テナントに、別のユーザーを作成する例

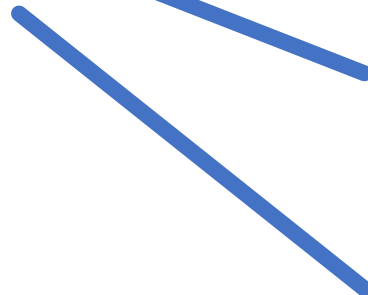
テナント



最初のユーザー taro
(ロール: グローバル管理者)



二人目のユーザー jiro
(ロール: なし)



三人目のユーザー saburo
(ロール: なし)

テナントにグループを作り、ユーザーをグループに入れる例

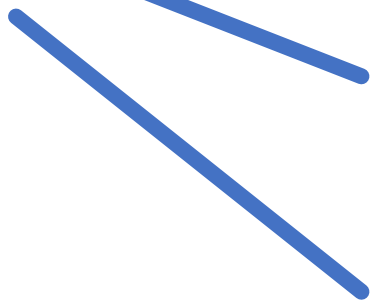
テナント



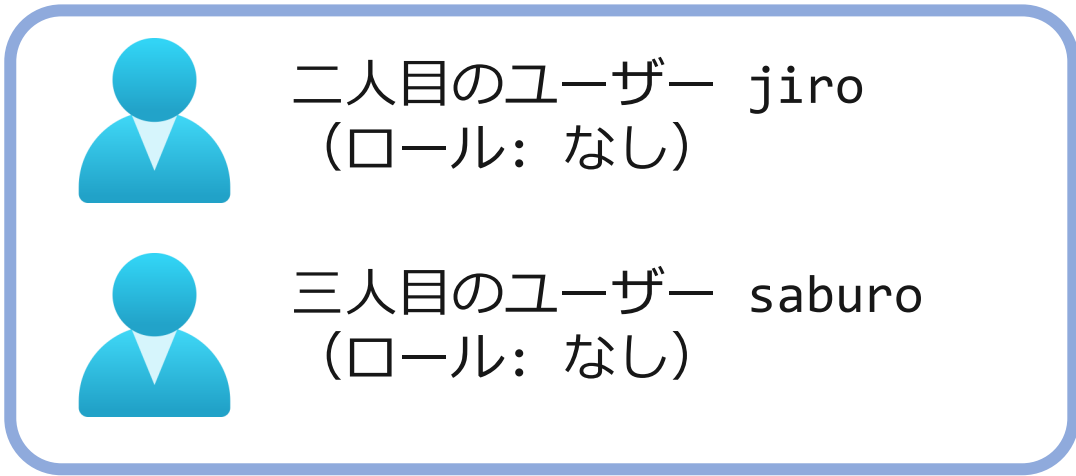
最初のユーザー taro
(ロール: グローバル管理者)



二人目のユーザー jiro
(ロール: なし)



三人目のユーザー saburo
(ロール: なし)



Managers グループ
(ロール: なし)

グループにも、ロールを割り当てできる。
グループに割り当てたロールは、グループ内のすべてのユーザーに反映される。

テナント



最初のユーザー taro
(ロール: グローバル管理者)



二人目のユーザー jiro
(ロール: なし)



三人目のユーザー saburo
(ロール: なし)

jiroとsaburoは、ユーザー管理者として、他のユーザーの管理（追加など）を実行できる。

Managers グループ
(ロール: **ユーザー管理者**)

ユーザーには、さまざまな「プロパティ」を設定できる。

Microsoft Azu...

リソース、サービス、ドキュメントの検索 (G+/)

4

ホーム > contoso | ユーザー > ユーザー >

新しいユーザーの作成 ...

組織内に新しい内部ユーザーを作成する

基本 ●

プロパティ

割り当て

確認と作成

ID

名

姓

ユーザーの種類

メンバー

ジョブ情報

役職

マネージャー

会社名

部署

人事部

従業員 ID

従業員の種類

従業員入社日

レビューと 作成

< 前へ

次: 割り当て >

jobTitle

department

動的グループ（メンバーシップの種類: 動的ユーザー）を使用すると、ルールを指定して、条件を満たすユーザーを自動的にグループに所属させることができる。

動的メンバーシップ ルール

保存

破棄

フィードバックがある場合

ルールの構成

ルールの検証 (プレビュー)

ルールビルダーまたはルール構文テキストボックスを使用して、動的メンバーシップの規則を作成または編集できます。

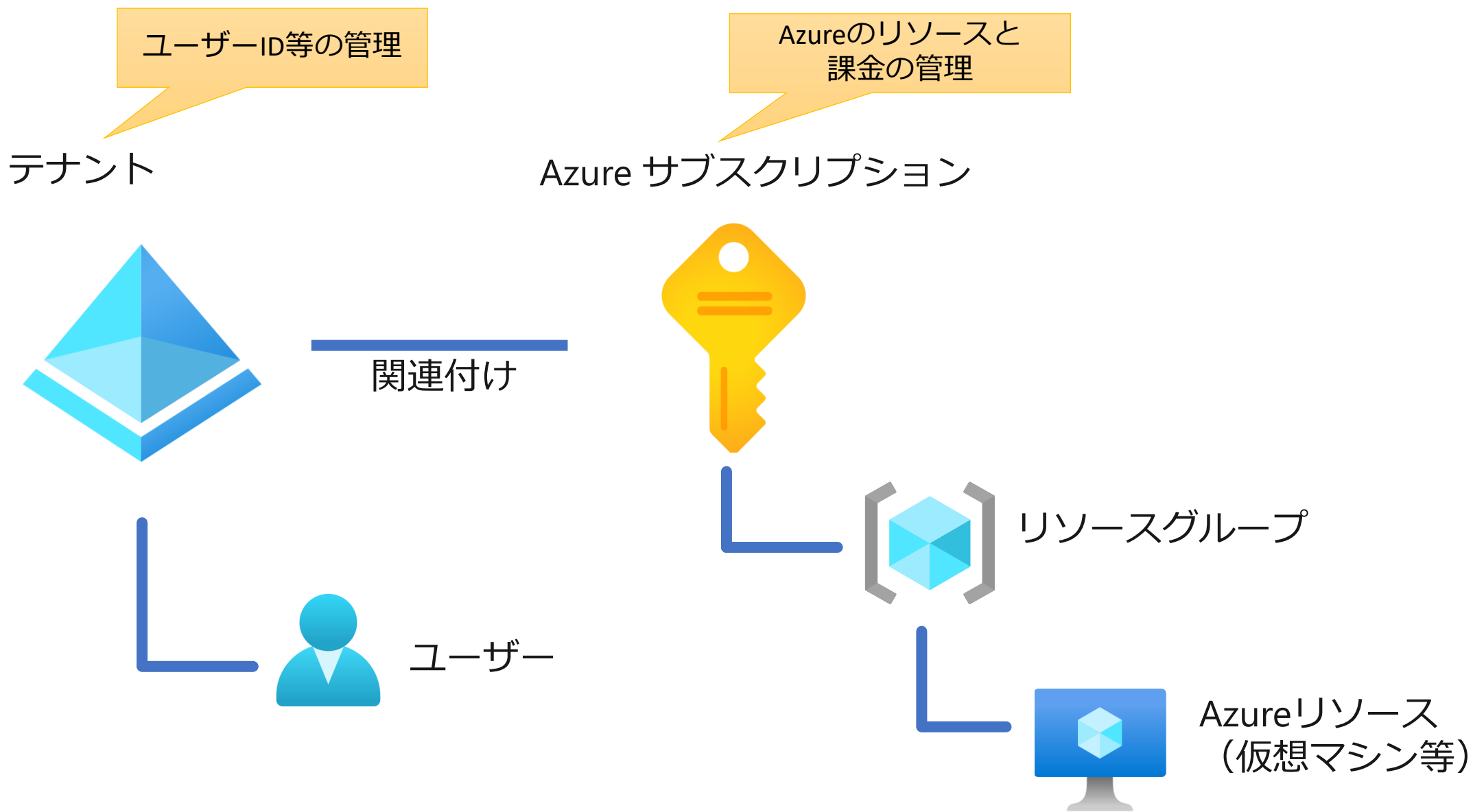
詳細情報

および/または	プロパティ	演算子	値
	jobTitle	Equals	マネージャー

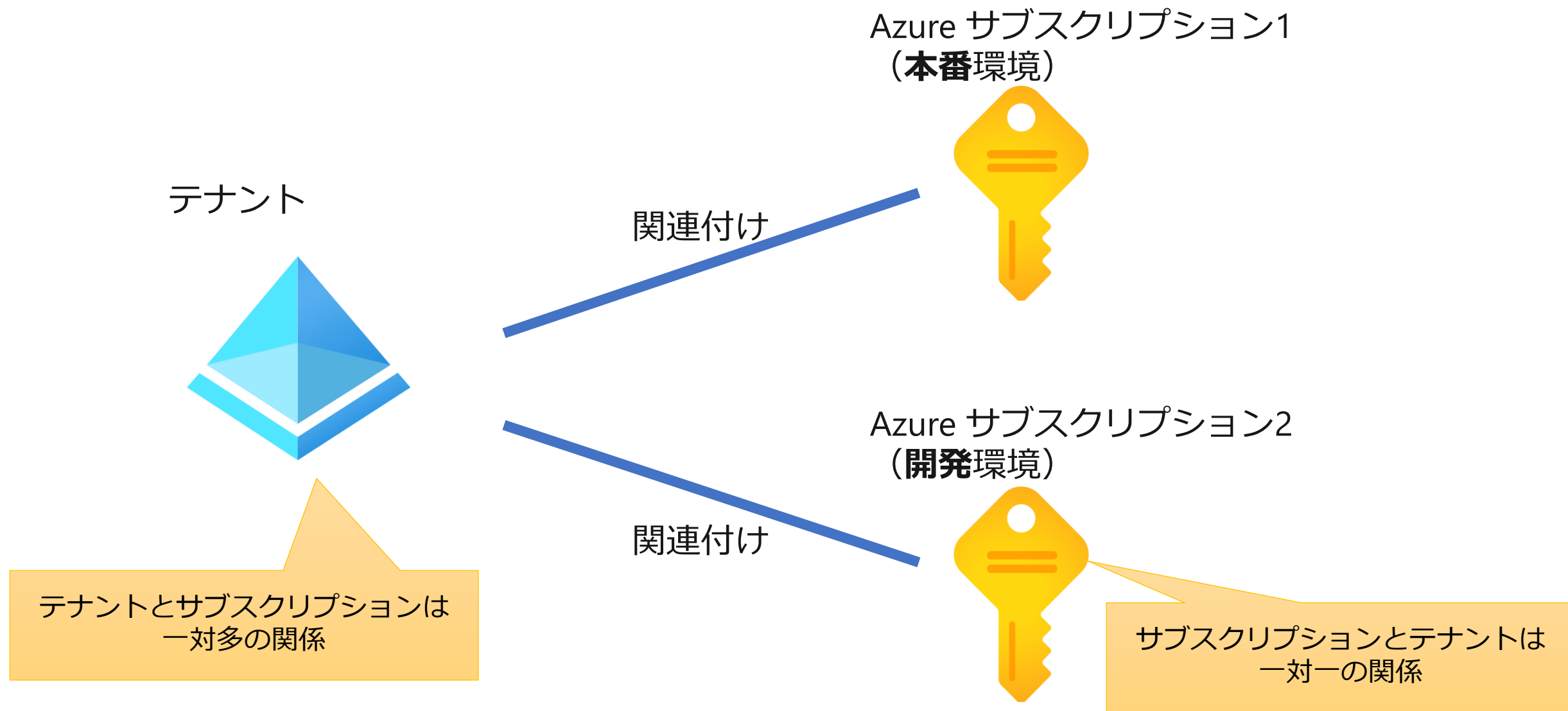


テナントと Azure サブスクリプション

「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

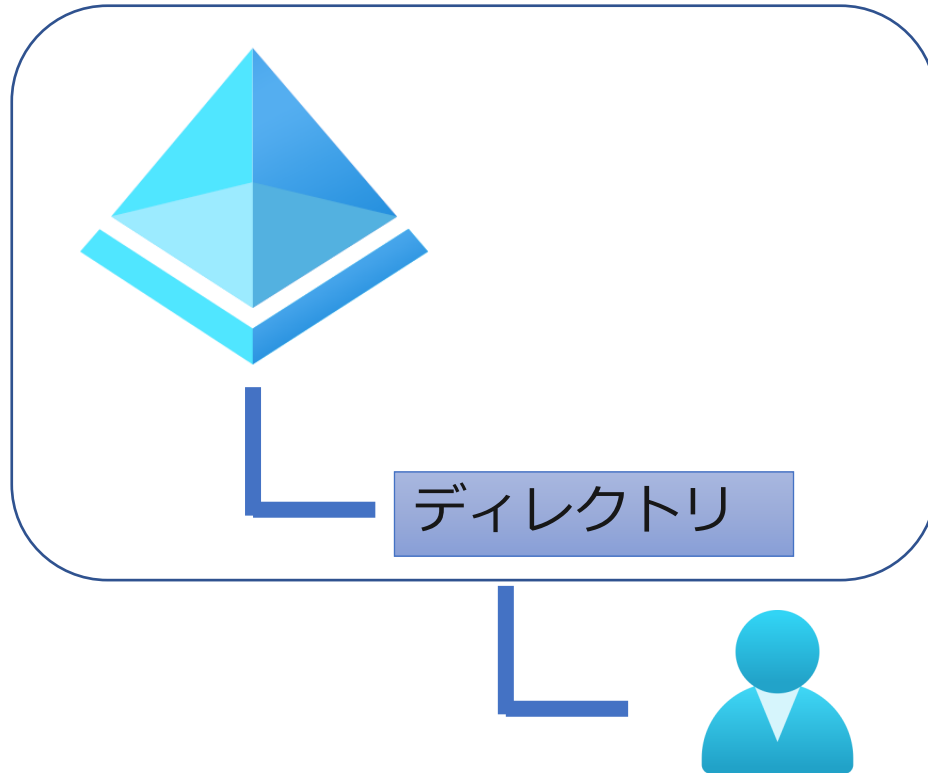


「テナント」と「ディレクトリ」

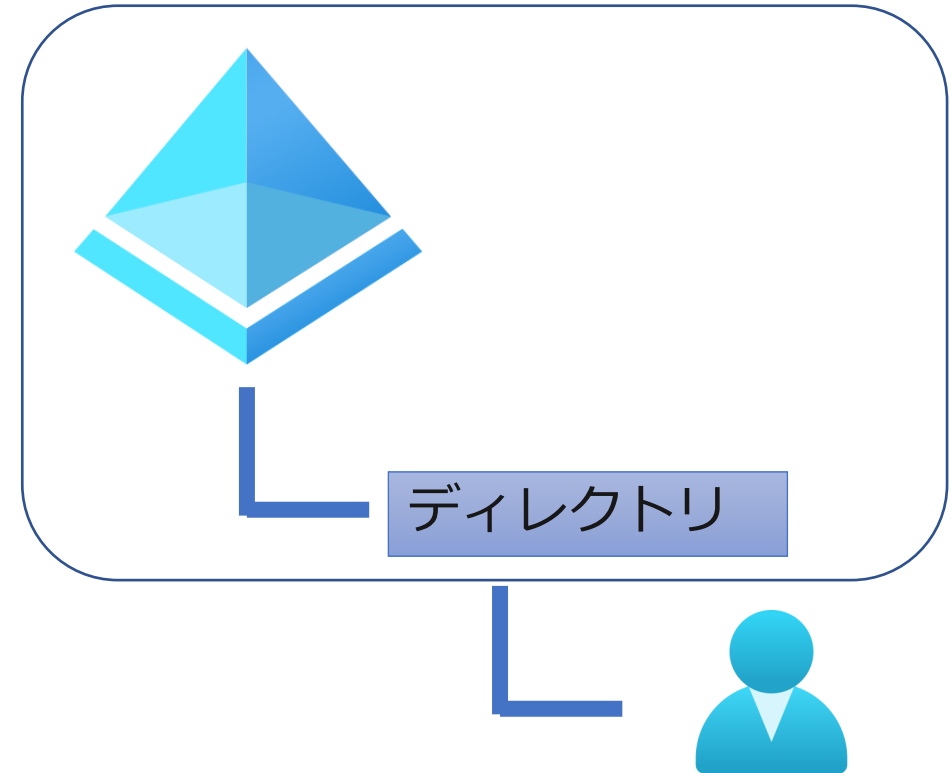
テナント ≡ ディレクトリ

各Entra IDテナントは、それぞれ、**ただ1つ**の「ディレクトリ」を持つ。
ディレクトリはテナントの中のしくみであり、**ユーザーによるディレクトリの管理は不要**。

Azure ADテナント



Azure ADテナント



Azure portalやAzureのドキュメントで、テナントのことを「ディレクトリ」と呼ぶ場合がある。

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+)

ポータル

ディレクトリとサブスクリプション

ディレクトリとサブスクリプション

検索メニュー

ディレクトリとサブスクリプション

外観とスタートアップ ビュー

言語と地域

本人情報

サインアウトと通知

Azure portal 全体のすべてのサービスとリソースは、基本的なフィルター処理から選択内容を継承します。また、選択内容は保存され、次回に Azure portal にサインインするか Azure portal を再度読み込んだときに、再度読み込まれます。

既定のサブスクリプション フィルター ⓘ

高度なフィルター ⓘ

サブスクリプションが表示されない場合、別のディレクトリに切り替えます。

ディレクトリ ⓘ

ディレクトリを切り替えると、ポータルが再度読み込まれます。選択したディレクトリは、ポータルで使用可能なサブスクリプション、リソース グループ、リージョンのフィルターに影響を与えます。ディレクトリの詳細情報。↗

現在のディレクトリ ⓘ : Contoso () .onmi... スタートアップディレクトリ ⓘ : 最終アクセス日時

お気に入り すべてのディレクトリ

検索

ディレクトリ名 ↑↓ ドメイン ↑↓ ディレクトリ ID ↑↓

★ Contoso

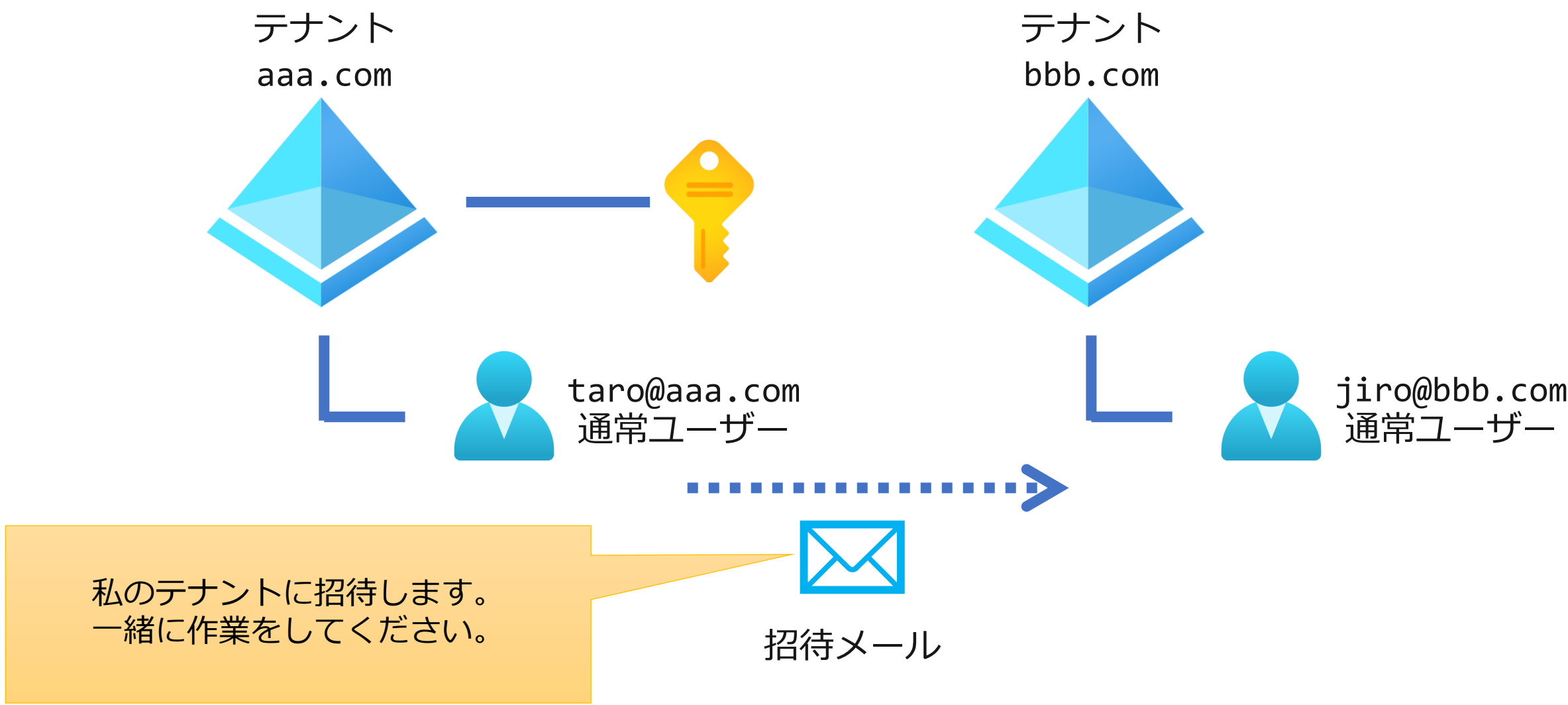
✔ 現在

) .onmicrosoft...

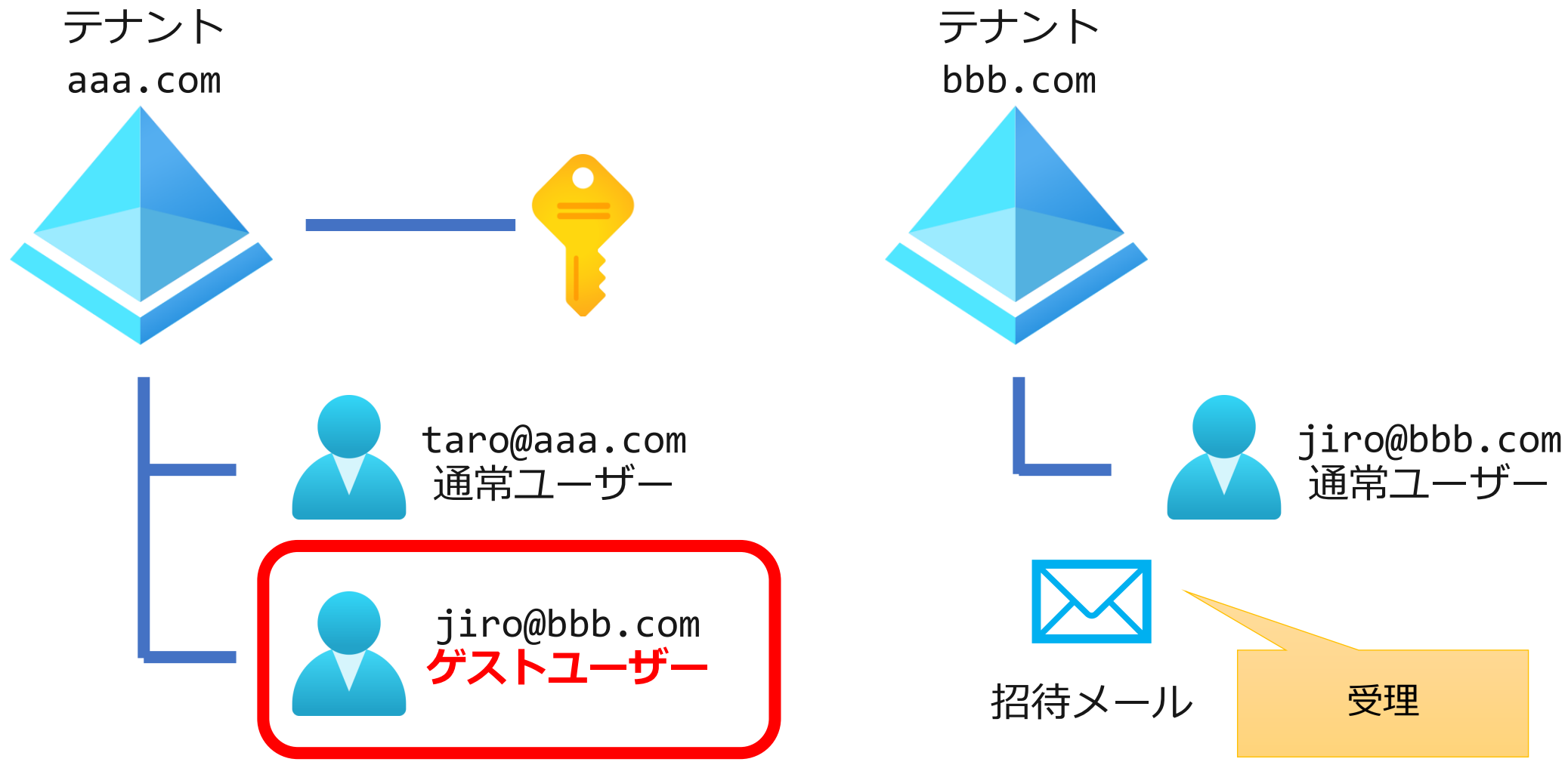
「ディレクトリ」 → 「テナント」と読み替えてよい

ゲストユーザーの招待

別のテナントのユーザーを、自分のテナントに招待することができる。



招待を受けると、招待されたテナントの**ゲストユーザー**となる。



ユーザーは、招待されたテナントに切り替えて、ゲストユーザーとして作業を行うことができる



お気に入り すべてのディレクトリ

検索

ディレクトリ名 ↑↓

★ bbb.com (自分のテナント)

✓ 現在

★ aaa.com (招待されたテナント)

切り替え

「ディレクトリ」は
「テナント」と
同じ意味

Entra IDの価格

Entra IDは、無料で使用することもできるが、**高度な機能**を使用するには、有料の Entra ID P1（旧 Azure Active Directory Premium P1） / Entra ID P2（旧 Azure Active Directory Premium P2）が必要となる。
さらに高度なIDガバナンス機能を利用するためには、P1 / P2 に加え、Entra ID Governance を購入する。

		最も包括的	お客様オファーをご利用いただけます ²
Microsoft Entra ID Free 無料	Microsoft Entra ID Premium P1 ¥750 ユーザー/月	Microsoft Entra ID Premium P2 ¥1,130 ユーザー/月	Microsoft Entra ID Governance ¥880 ユーザー/月
Microsoft のクラウド サブスクリプション (Microsoft Azure、Microsoft 365 など) に含まれています。 ¹	Azure Active Directory P1 (Microsoft Entra ID P1 になります) は単体製品として購入できますが、大企業向けの Microsoft 365 E3 と中小規模企業向けの Microsoft 365 Business Premium にも含まれています。 価格には消費税は含まれていません。	Azure Active Directory P2 (Microsoft Entra ID P2 になります) は単体製品として購入できますが、大企業向けの Microsoft 365 E5 にも含まれています。 価格には消費税は含まれていません。	Entra ID ガバナンスは ID ガバナンスの高度な機能を集めたセットであり、Microsoft Entra ID P1 と P2 のお客様が購入できます。 価格には消費税は含まれていません。

パスワードライトバック (P1)

アプリケーションプロキシ (P1 or P2)

管理単位 (P1)

会社のブランドの構成 (P1)

セルフサービスパスワードリセット (P1)

動的グループ (P1)

条件付きアクセス (P1)

Identity Protection (P2)

Privileged Identity Management (P2)

(基本的な) アクセスレビュー (P2)

(基本的な) エンタイトルメント管理 (P2)

テナントで Premium P1 や Premium P2 のライセンスを購入し、ユーザーに割り当てる

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+)

ホーム > Contoso | ライセンス > ライセンス

ライセンス | すべての製品

Contoso - Microsoft Entra ID

概要

問題の診断と解決

管理

ライセンスされた機能

すべての製品

セルフサービス サインアップ製品

試用/購入

割り当て

請求書

列

フィード

名前

MICROSOFT ENTRA ID P2

Microsoft Entra ID P2 を使用すると、高度なセキュリティ機能、機能豊富なレポート、アプリケーションに対するルール ベースの割り当てにアクセスできます。エンド ユーザーは、セルフサービス機能とカスタマイズされたブランドを利用できるようになります。

詳細情報

無料試用版

Microsoft Entra ID P2 は、多要素認証、ポリシーに基づく管理、エンドユーザーのセルフサービスなど、追加の機能によってディレクトリを強化します。[機能の詳細情報](#)

試用版には 100 個のライセンスが含まれており、有効期限はライセンスを認証した日から 30 日間です。有料版へのアップグレードを希望される場合は、Microsoft Entra ID P2 をご購入いただく必要があります。[価格の詳細情報](#)

Microsoft Entra ID P2 は、Azure サービスとは別にライセンスが付与されます。このライセンス認証を確認すると、[マイクロソフト オンライン サブスクリプション契約](#) と [プライバシーに関する声明](#) に同意したことになります。

アクティブ化

ライセンスを割り当てるユーザーには、事前に「**利用場所**」プロパティを設定しておく必要がある

Microsoft Azu...

リソース、サービス、ドキュメントの検索 (G+/)

ホーム > contoso | ユーザー > ユーザー >

新しいユーザーの作成 ...

組織内に新しい内部ユーザーを作成する

その他のメール

+ メールの追加

FAX 番号

保護者による制限

年齢グループ

未成年に対する同意

設定

利用場所

日本

レビューと作成

< 前へ

次: 割り当て >

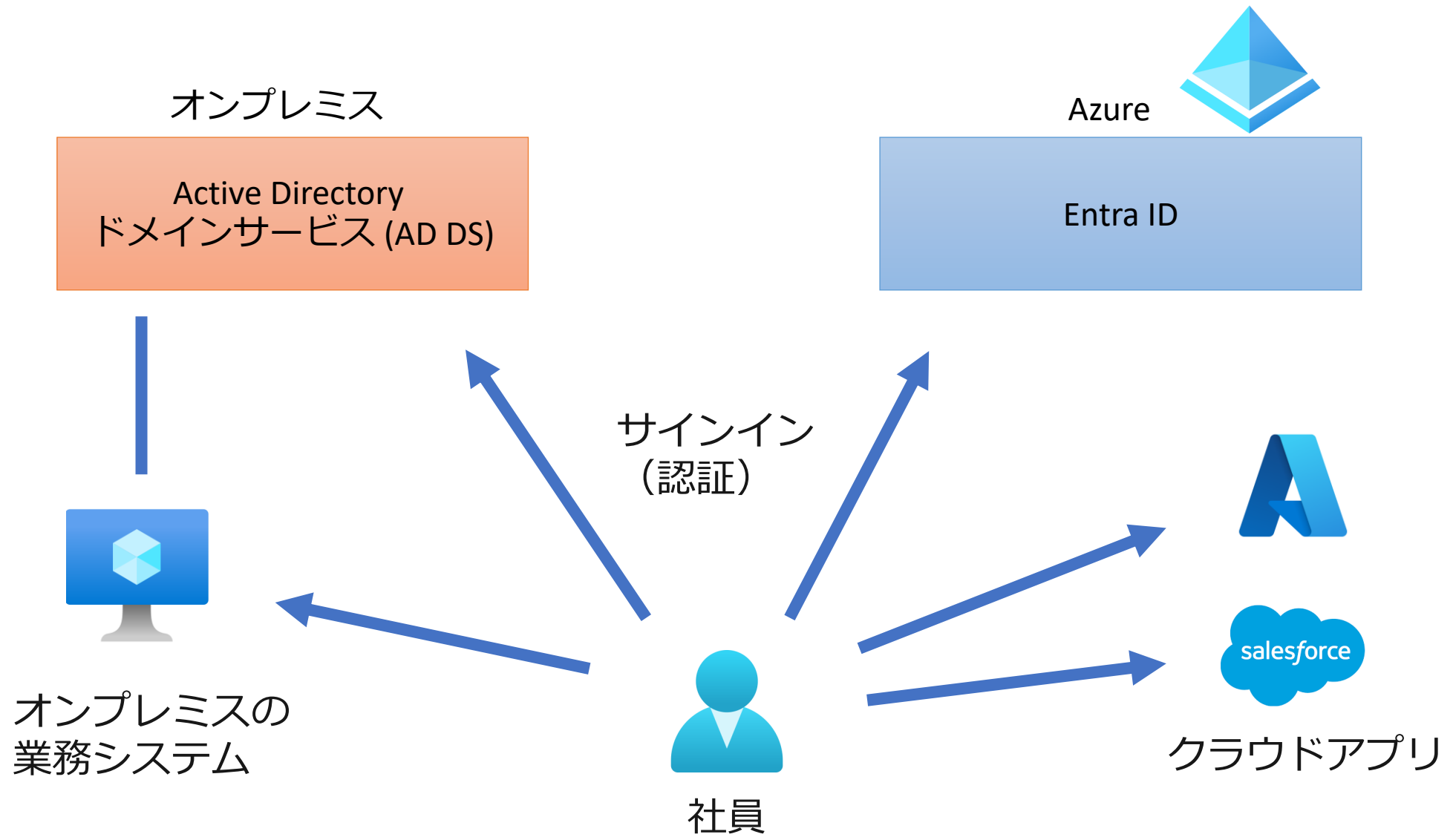
Q. ライセンスの利用場所とはなんですか？

A. そのユーザーがライセンスを使用する地域を設定します。**サービスと機能を使用できるかどうかは、国または地域によって異なるため利用場所の選択が必要です。**

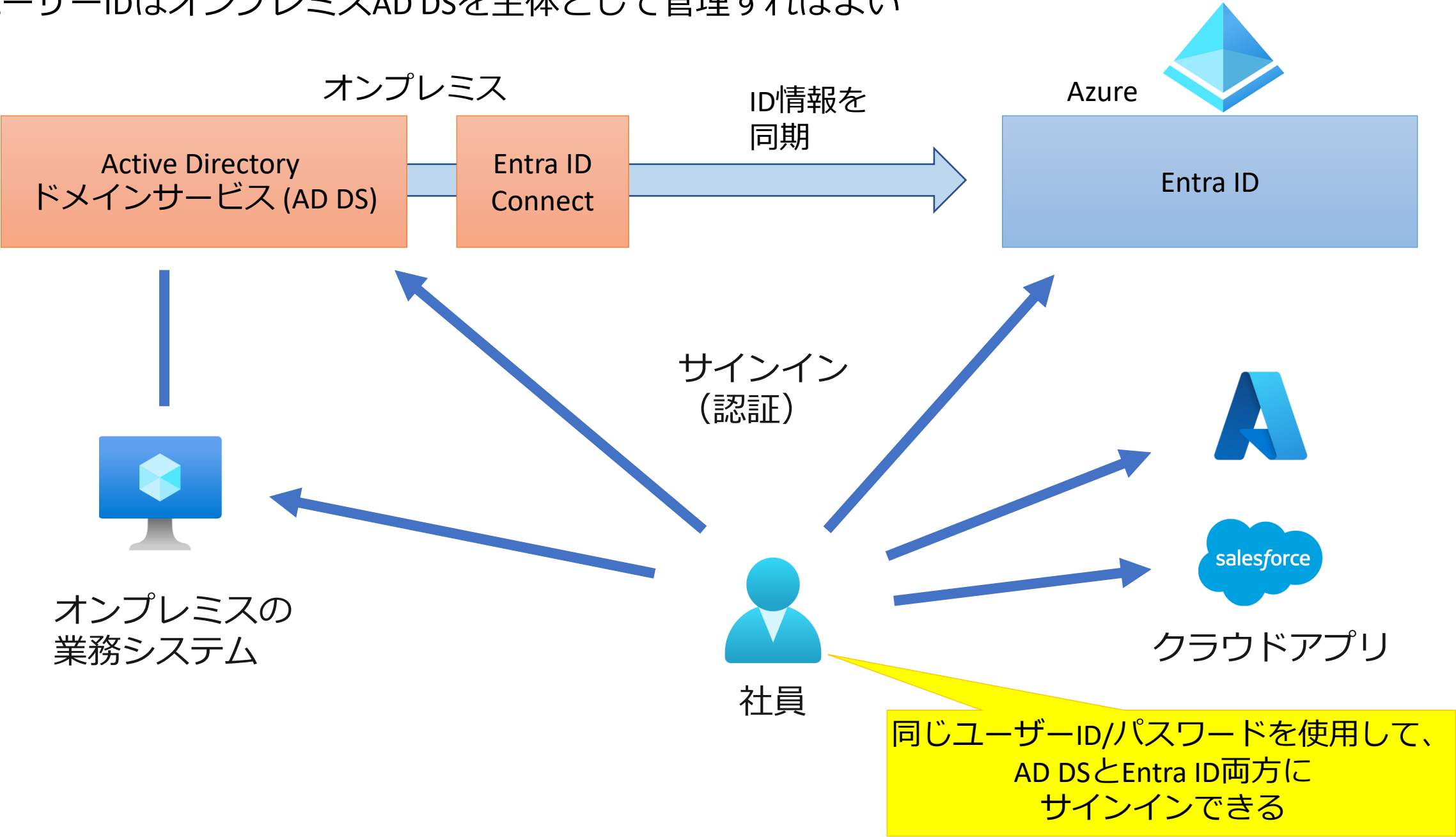
ハイブリッドID

オンプレミスAD DSとEntra ID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、Entra IDも使いたい場合・・・

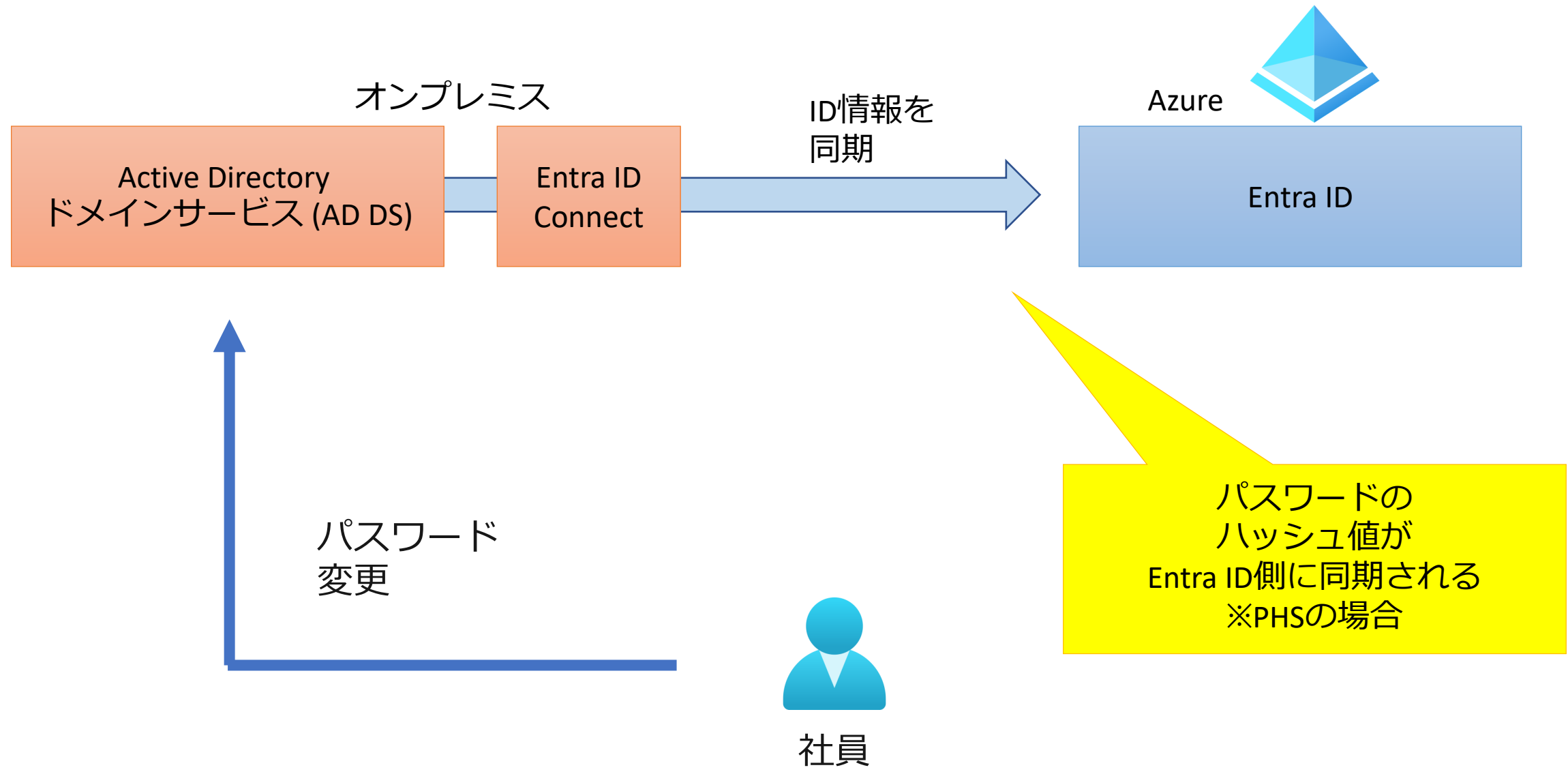


Entra ID Connect を使用して、オンプレミスのユーザーID情報をEntra IDに「同期」 (sync) できる。
ユーザーIDはオンプレミスAD DSを主体として管理すればよい

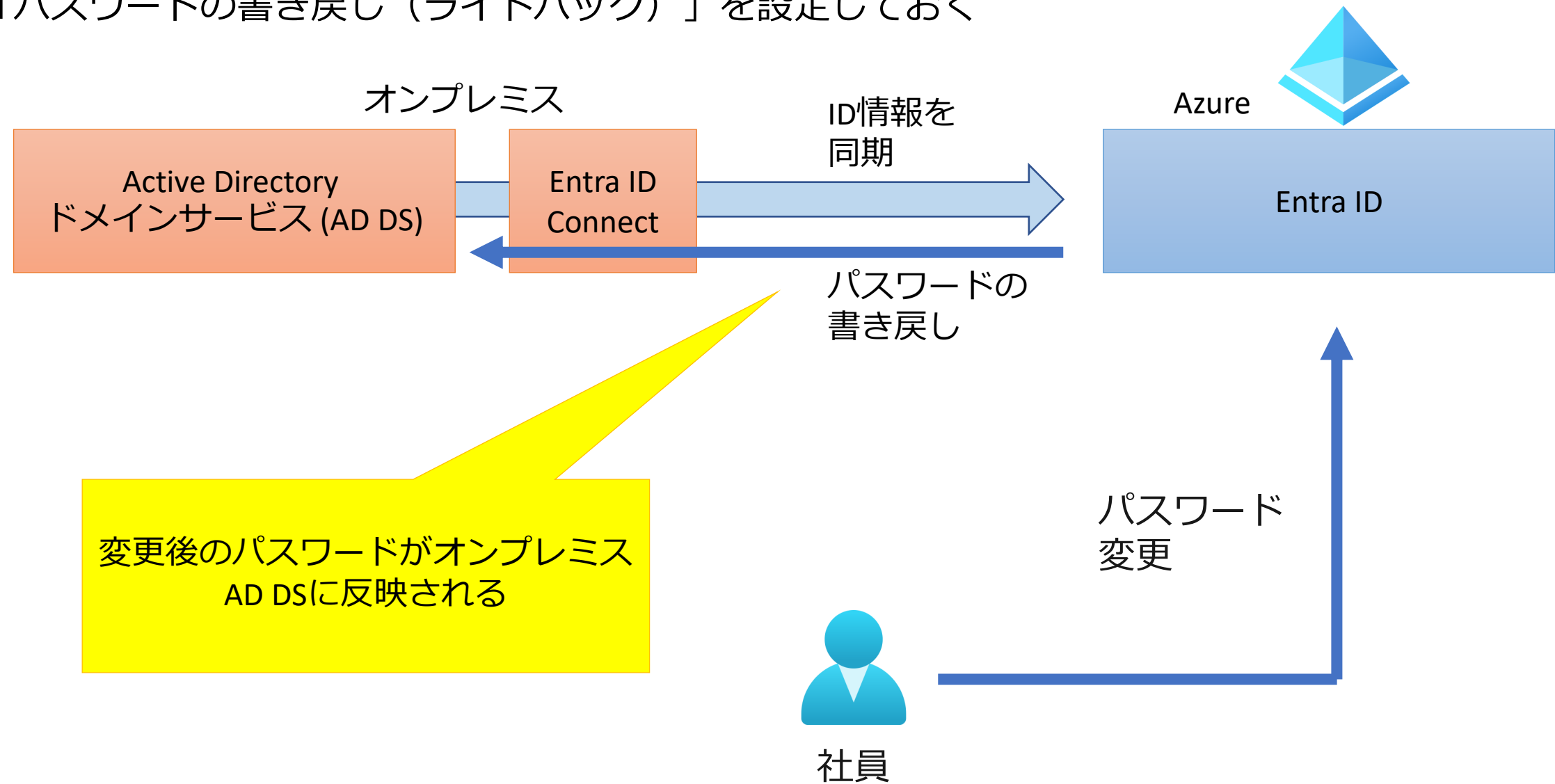


ハイブリッドIDにおける パスワード変更

オンプレ側でのパスワード変更: 特に問題なし



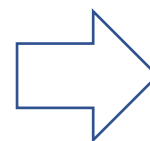
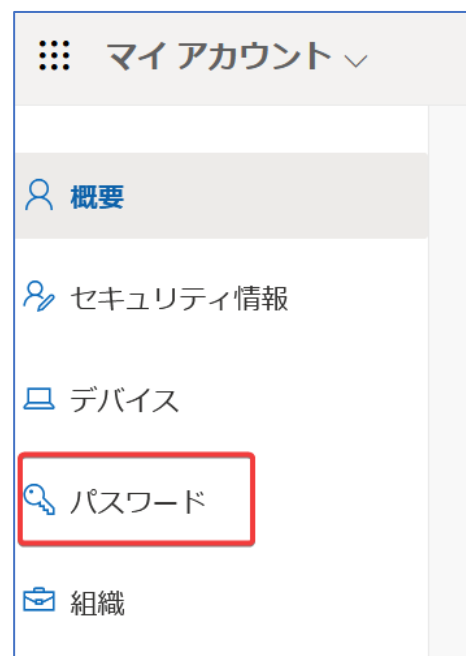
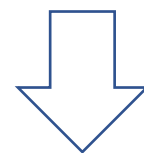
クラウド（Entra ID）側でのパスワード変更: Entra ID Connectで、「パスワードの書き戻し（ライトバック）」を設定しておく



パスワードの変更

ユーザーが自分のパスワードを別のものに変更するには？

ユーザーは、**現在の自分のパスワードを知っている**、自分のパスワードを別のものに変更できる。



Microsoft

パスワードの変更

強力なパスワードが必要です。8 から 256 文字のパスワードを入力してください。一般的な単語や名前は含めないでください。また、大文字、小文字、数字、および記号を組み合わせたパスワードにしてください。

ユーザー ID
dev18@contoso1800.onmicrosoft.com

古いパスワード
.....

新しいパスワードの作成
パスワードの安全性

新しいパスワードの確認入力

送信 キャンセル

パスワードリセット

ユーザーが自分のパスワードを忘れてしまい、新しいパスワードを再設定したい場合は？

もし、Entra ID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**テナントの管理者が行う**。

テナントの管理者（グローバル管理者、ユーザー管理者などのロールを持つユーザー）は、テナントの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、**一時パスワード**が発行される。管理者はその**一時パスワード**をユーザーに伝達する。

ユーザーが、管理者から伝達された**一時パスワード**でサインインすると、直後に、自分のパスワードの再設定を求められる。

管理者によるユーザーのパスワードのリセット

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+/)

ホーム > contoso | ユーザー > ユーザー >

test1

ユーザー

検索

プロパティの編集

削除

更新

パスワードのリセット

...

概要

監査ログ

サインイン ログ

問題の診断と解決

概要

監視中

プロパティ

基本情報

パスワードのリセット

test1

ユーザー

'test1@contoso017org.onmicrosoft.com' には、次回サインイン時に変更する必要がある一時的なパスワードが割り当てられます。一時的なパスワードを表示するには、[パスワードのリセット] をクリックしてください。

パスワードのリセット

パスワードのリセット

test1

✓

パスワードがリセットされました

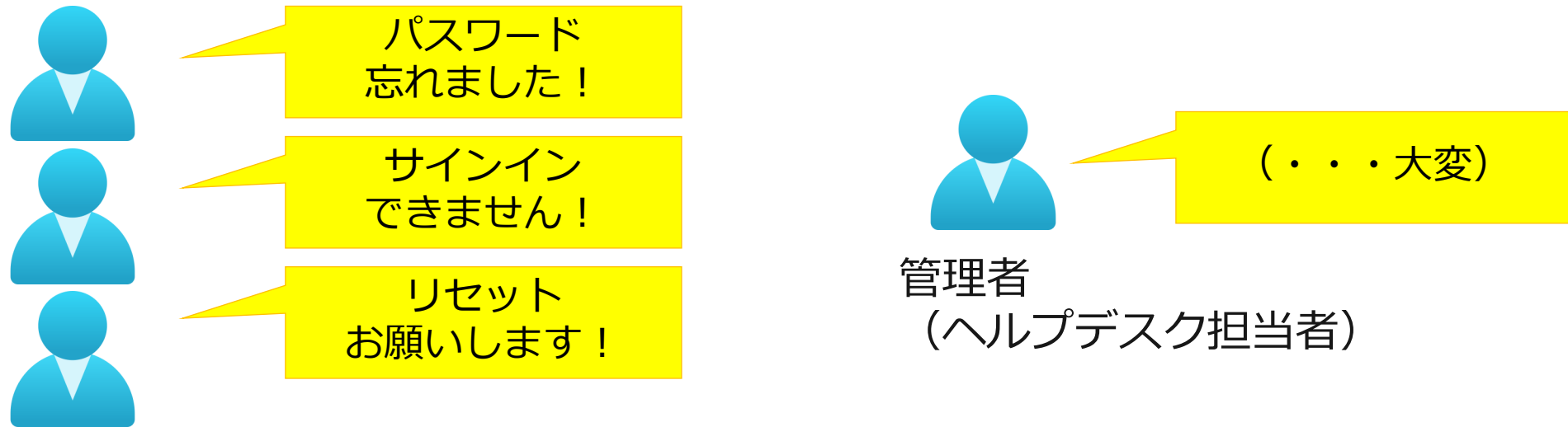
サインインできるようにユーザーにこの一時パスワードを提供します。

一時パスワード ⓘ

Daba8545

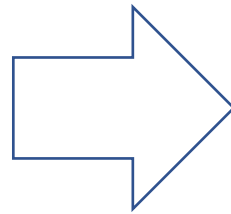
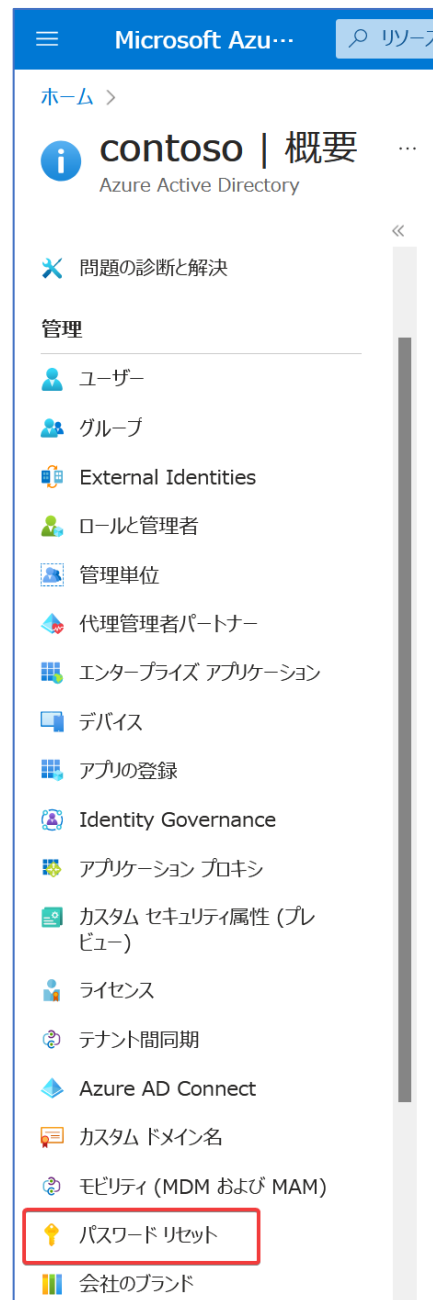
セルフサービスパスワードリセットの必要性

組織にユーザー数が多いと、パスワードのリセット対応件数も増加し、**ヘルプデスク担当者の手間とコストが増加する。**



管理者はテナントで**セルフサービスパスワードリセット (SSPR)**を有効化できる。すると、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**できるようになり、ヘルプデスク担当者が個別に対応する必要がなくなる。リセットの際は、メールや電話などを使用した本人確認が求められる。本人確認に必要な情報（メールアドレスや電話番号など）は事前に設定しておく。


セルフサービスパスワードリセット (SSPR) の有効化



※「選択済み」で、グループを選択すると、そのグループのユーザーのみ、SSPRを有効にできる。

セルフサービスパスワードリセット (SSPR) によるパスワードのリセット

Microsoft Azure

 Microsoft

← dev17@contoso017org.onmicrosoft.com

パスワードの入力

.....

[パスワードを忘れた場合](#)

サインイン

Microsoft

アカウントを回復する

確認ステップ 1 > 新しいパスワードの選択

確認に使用する連絡方法を選択してください

☒ 携帯電話に SMS 送信

お客様の電話に確認コードを含むテキストメッセージを送信しました。

☐ 携帯電話に発信

次へ

キャンセル

Microsoft

アカウントを回復する

確認ステップ 1 ✓ > 新しいパスワードの選択

* 新しいパスワードの入力:

パスワードの安全性

* 新しいパスワードの確認入力:

完了

キャンセル