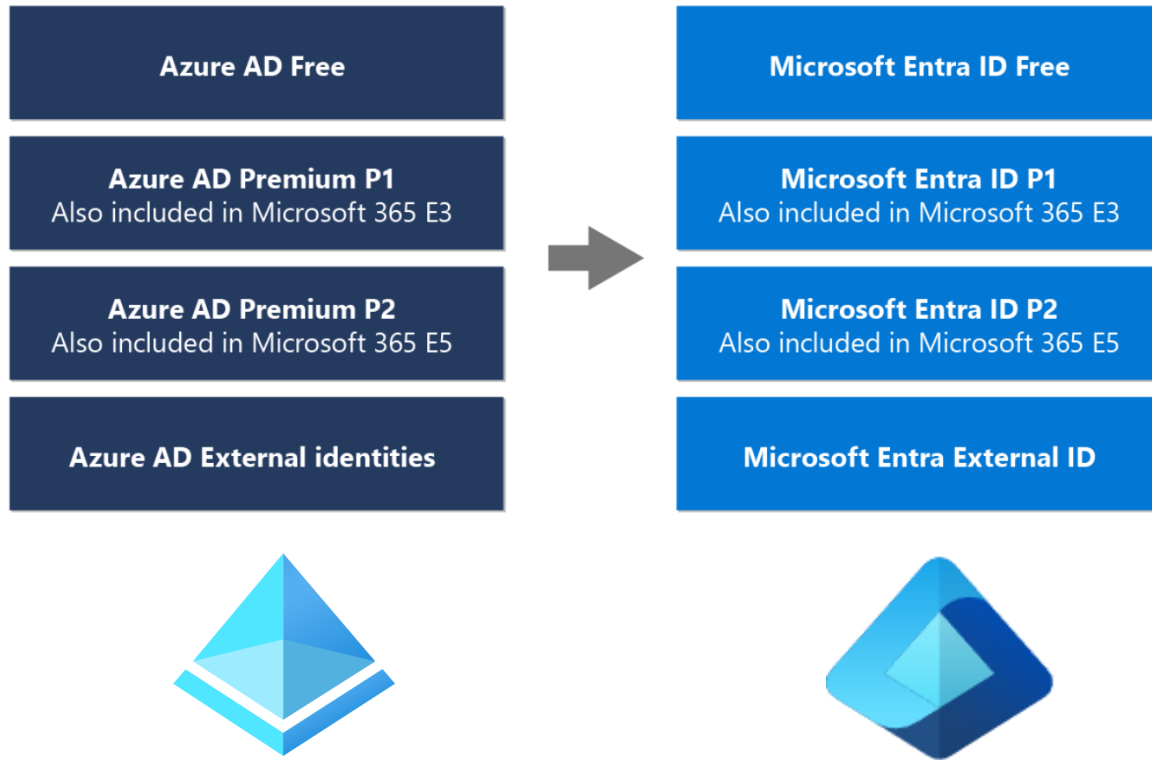




Azure Active Directory
(Azure AD)
→ Entra ID



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。



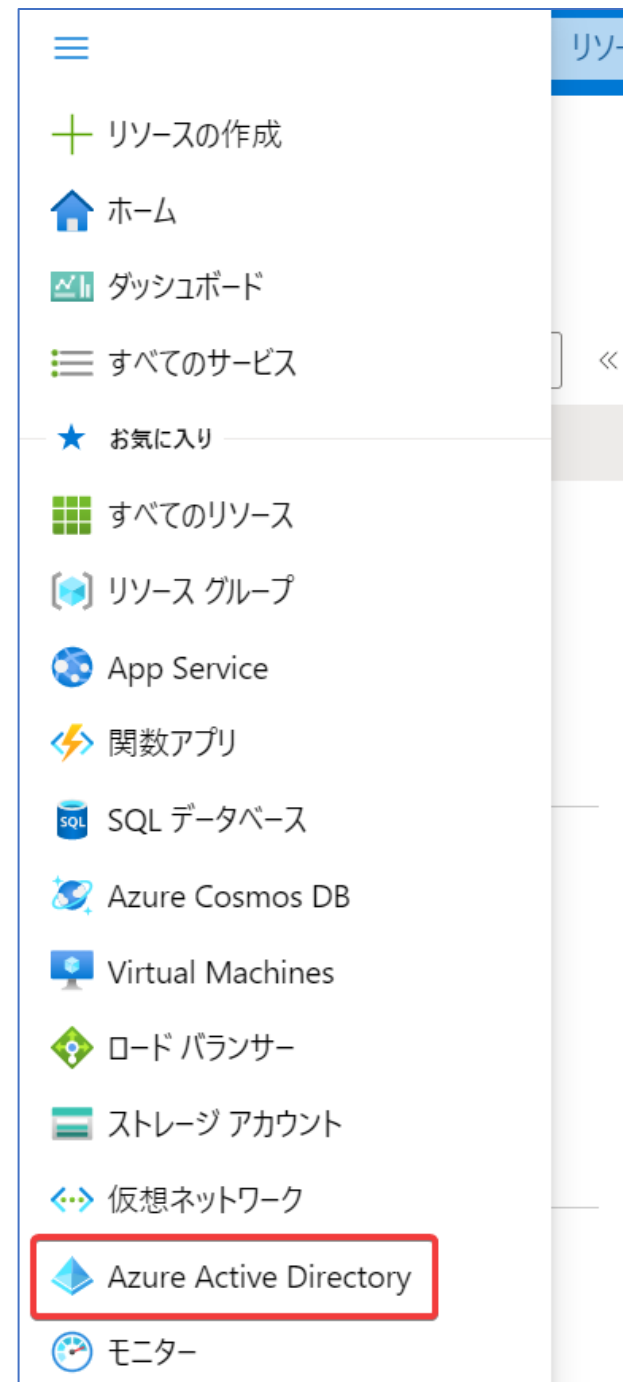
ドキュメント、Azure portal（管理画面）などの対応は現在進行中。
旧名称の「Azure AD」として表示されている部分もまだたくさんある。
→本資料では旧名称「Azure AD」で解説

<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/>

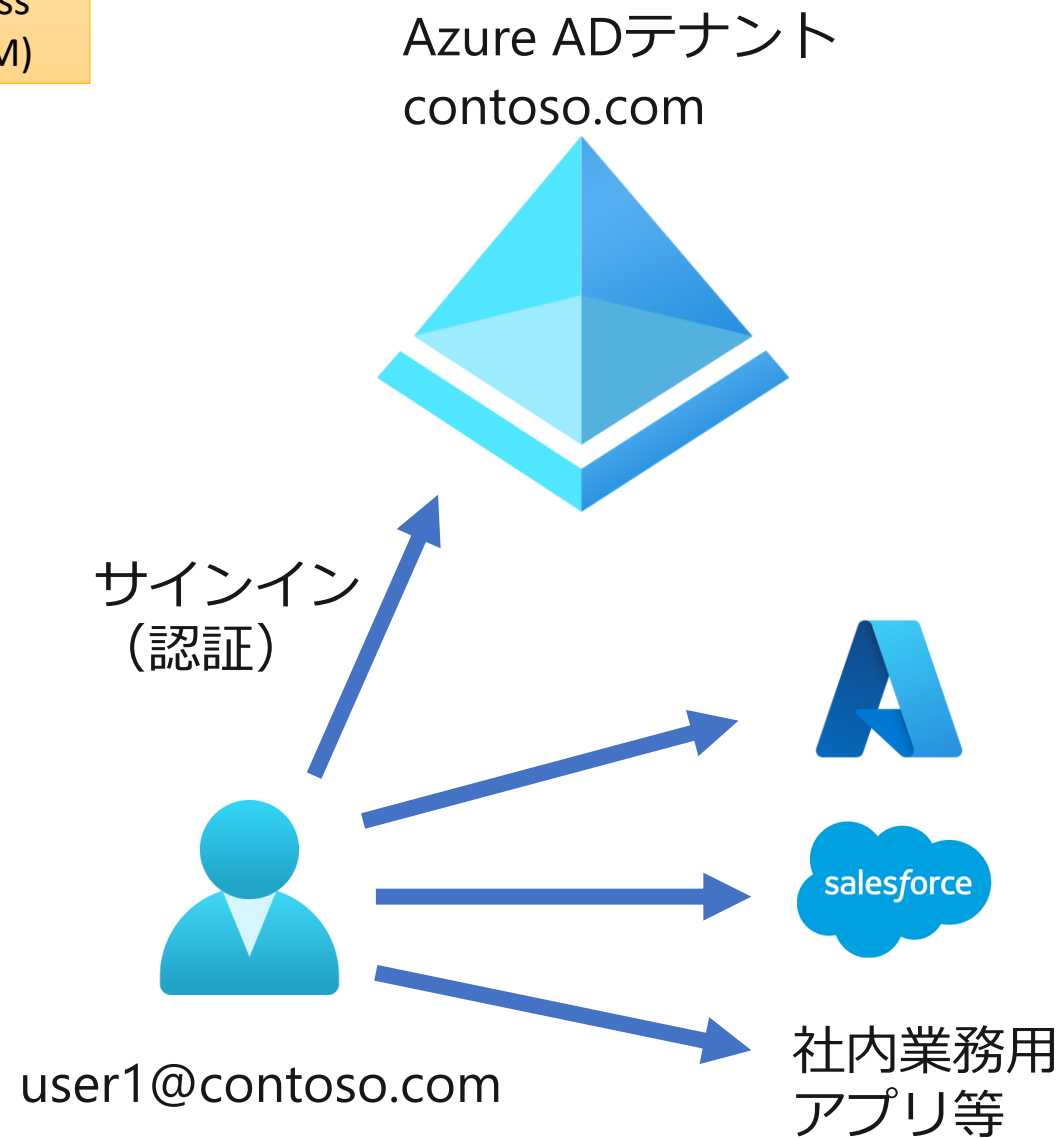
Azure ADとは？



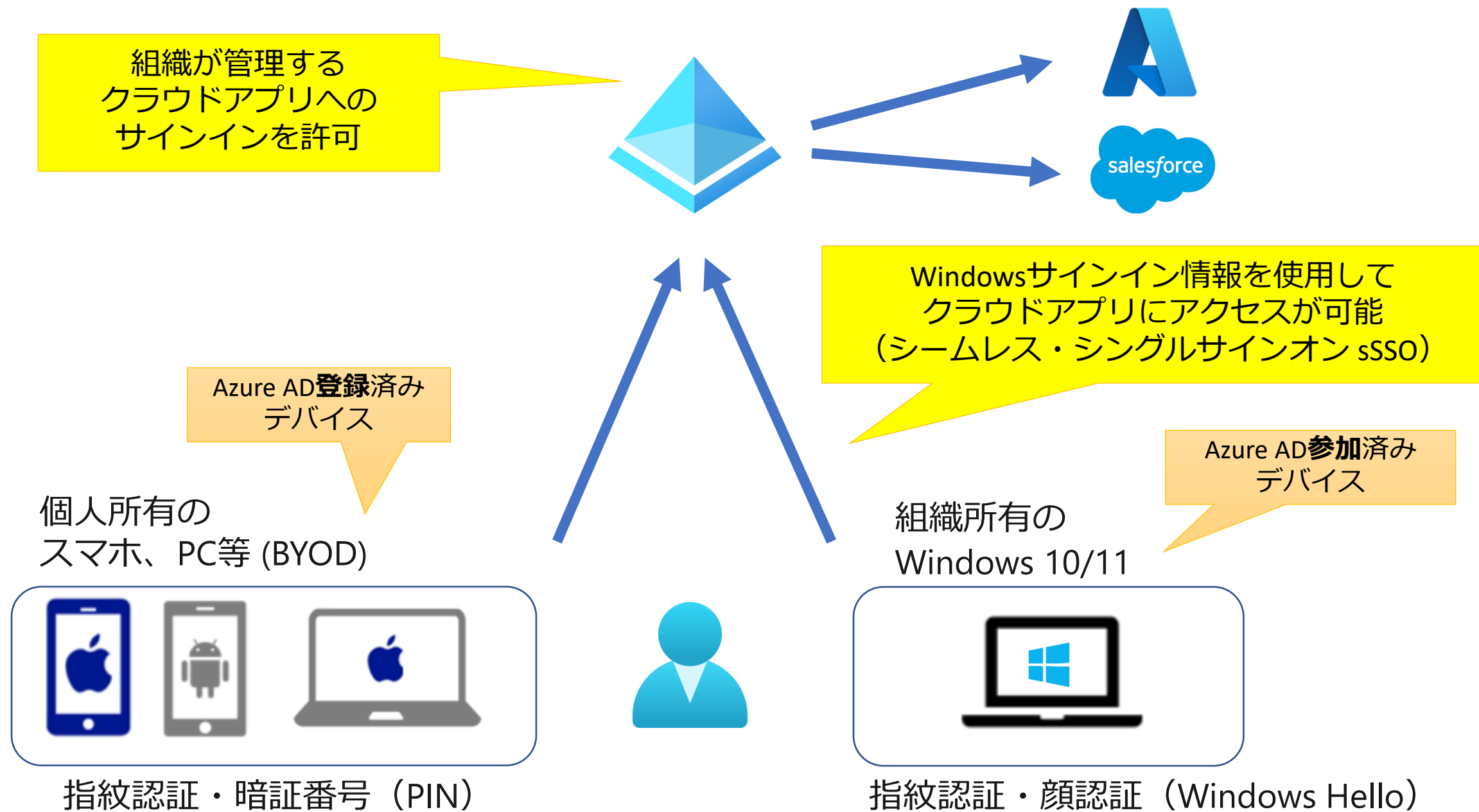
Azure AD とは

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





Active Directory Domain Service (AD DS) vs Azure AD

オンプレミス環境で用いられている 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、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

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、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

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>

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

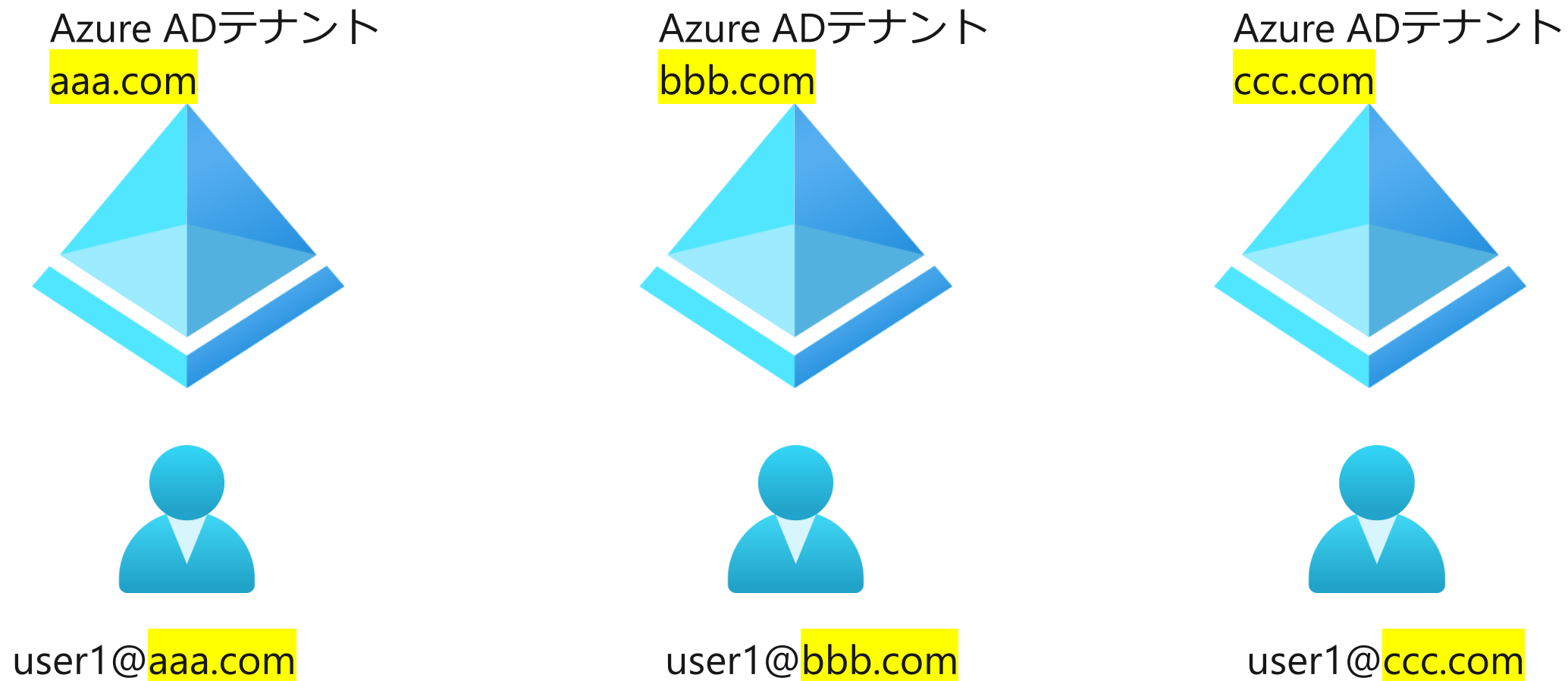


ユーザーID等の管理



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



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」で運用するが、
検証用などのテナントを追加することも簡単にできる

Azureへ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

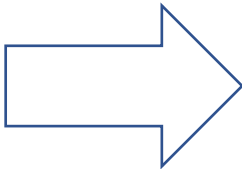
テナントとサブスクリプションが
作成される

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



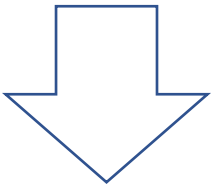
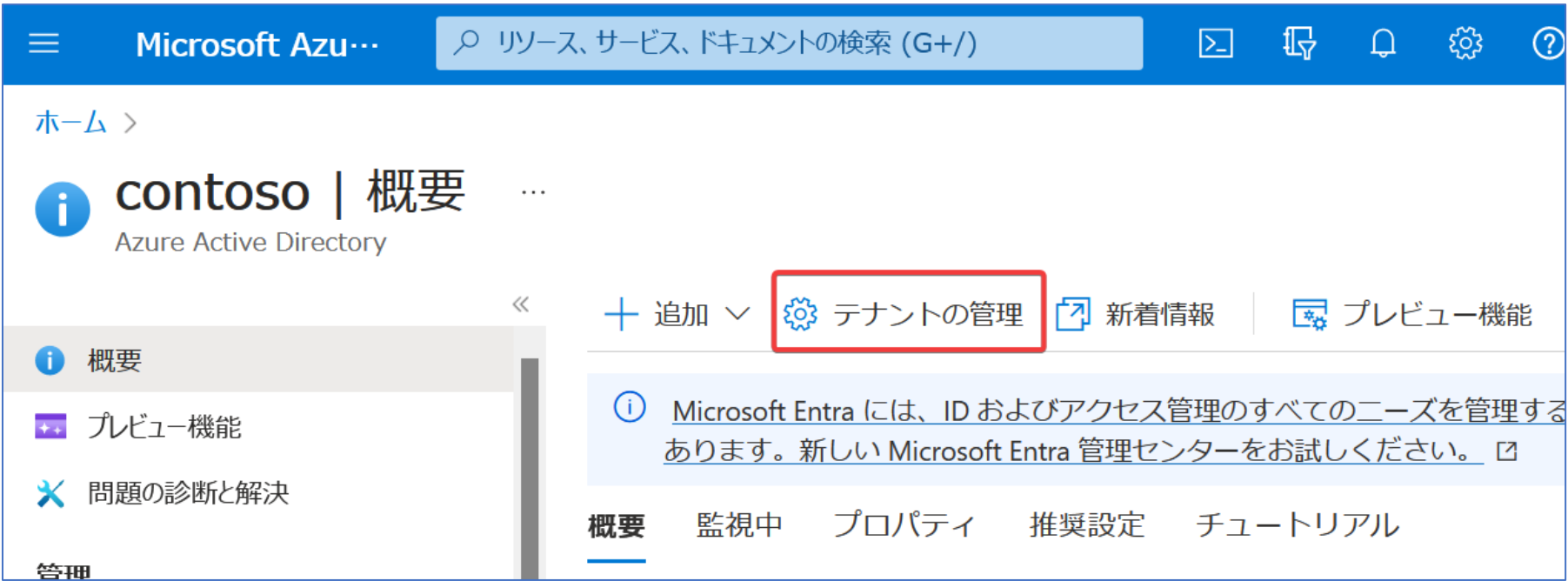
関連付け



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 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

リソース、サービス、ドキュメントの検索 (G+)

切り替え

お気に入り すべてのディレクトリ

検索

ディレクトリ名 ↑↓

★ aaa.com	(現在のテナント)	✓ 現在
★ bbb.com	(新しいテナント)	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

Azure AD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。

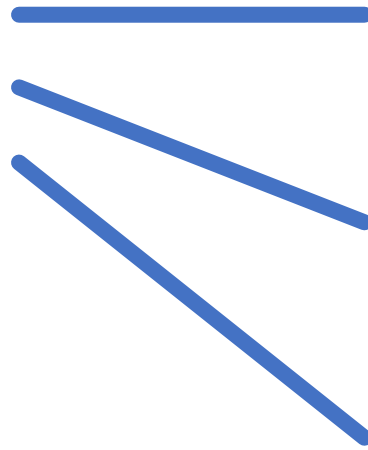
Azure ADテナント



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

Azure AD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

Azure ADテナント



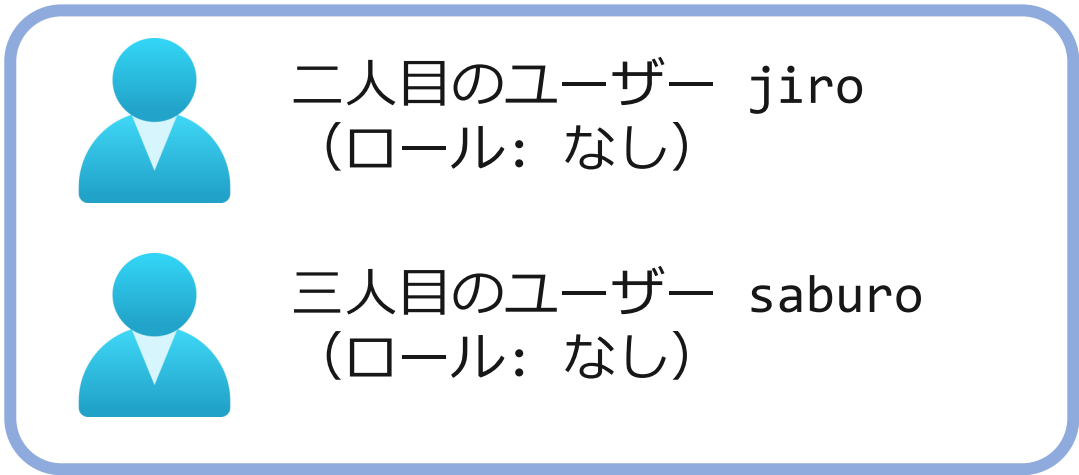
最初のユーザー taro
(ロール: グローバル管理者)



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。

Azure AD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)

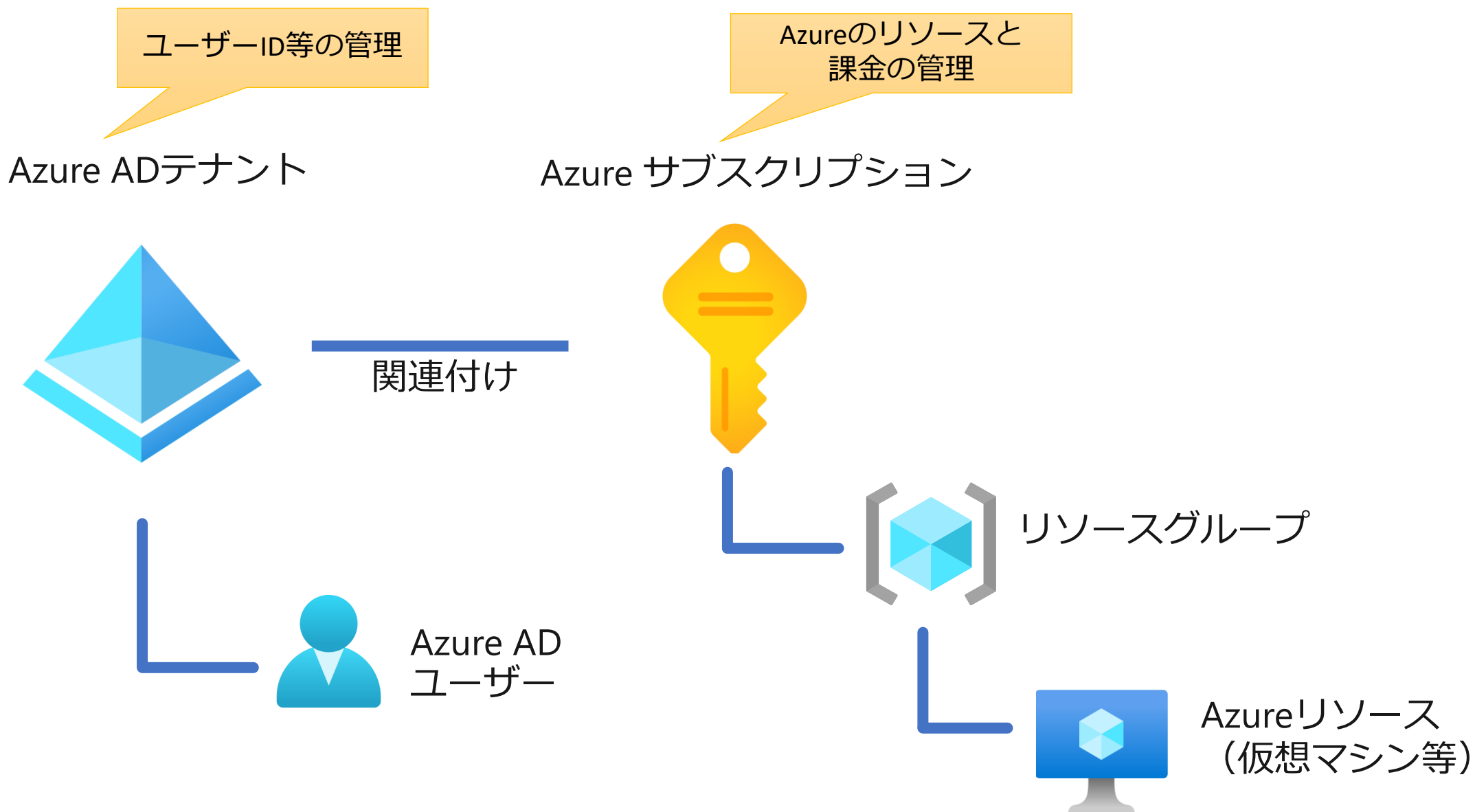
ルール ビルダーまたはルール構文テキスト ボックスを使用して、動的メンバーシップの規則を作成または編集できます。 [詳細情報](#)

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

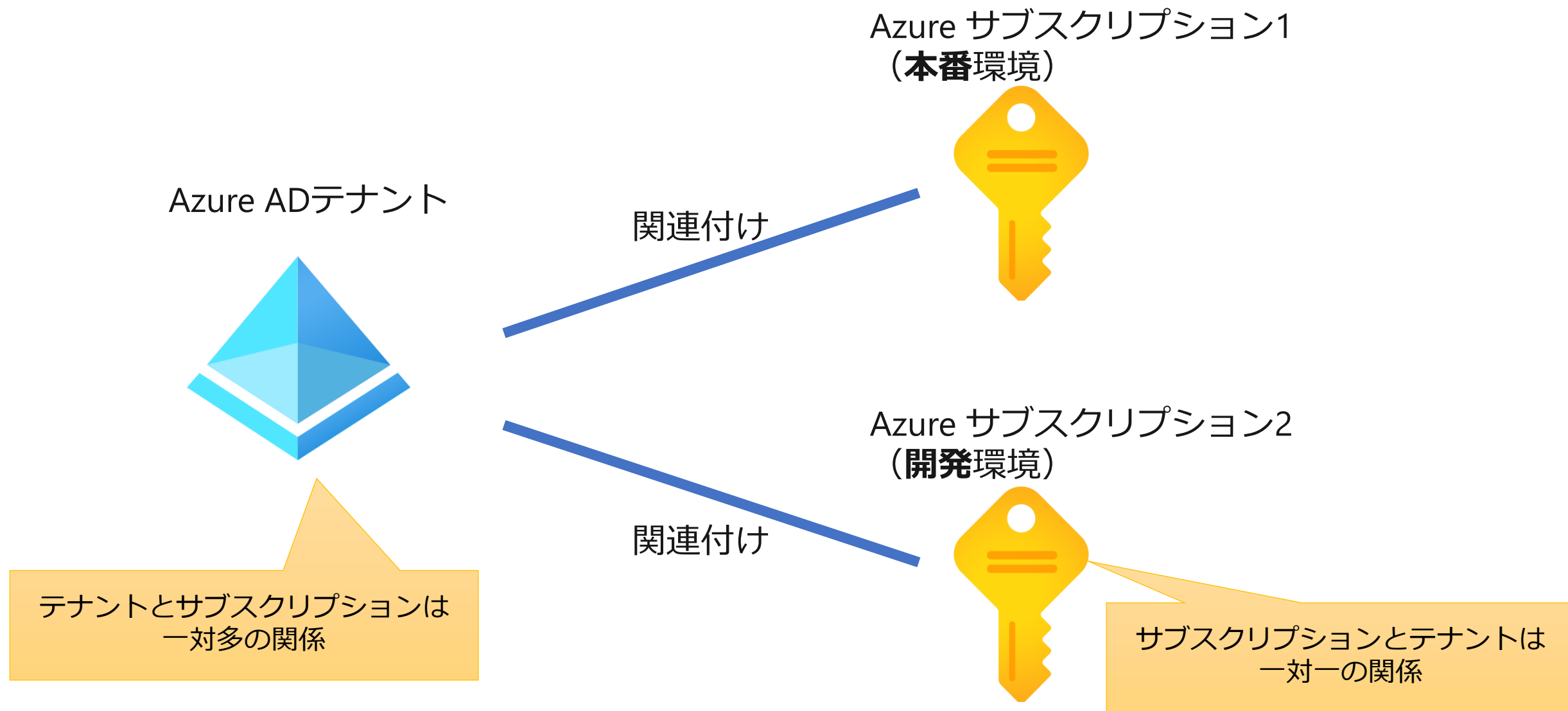


Azure ADテナントと Azure サブスクリプション

「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

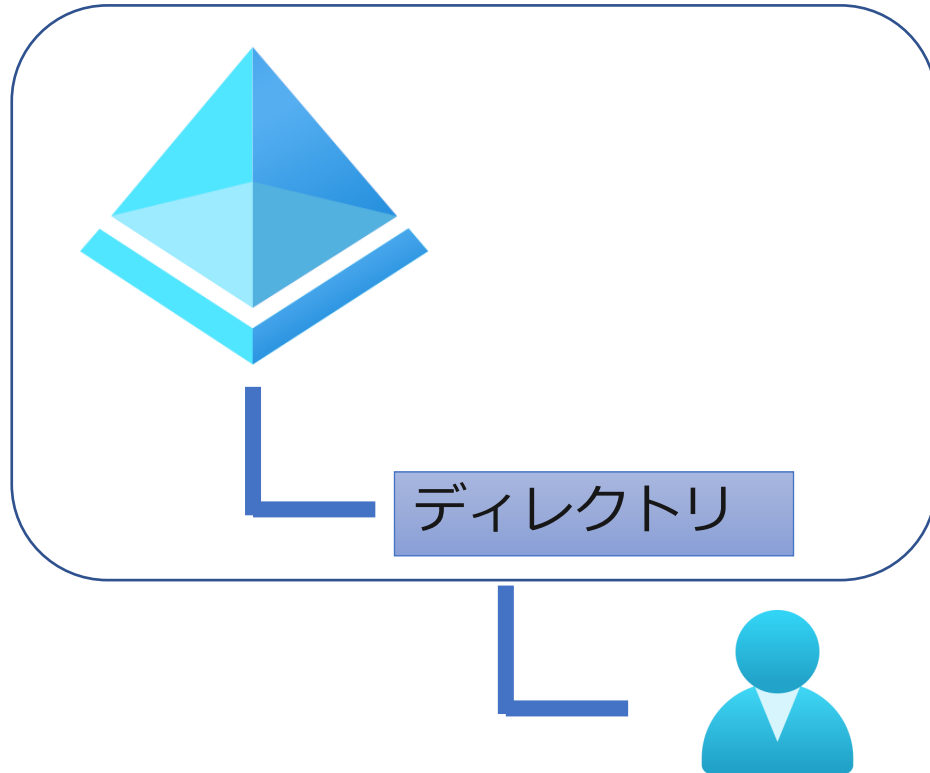


Azure ADの 「テナント」と「ディレクトリ」

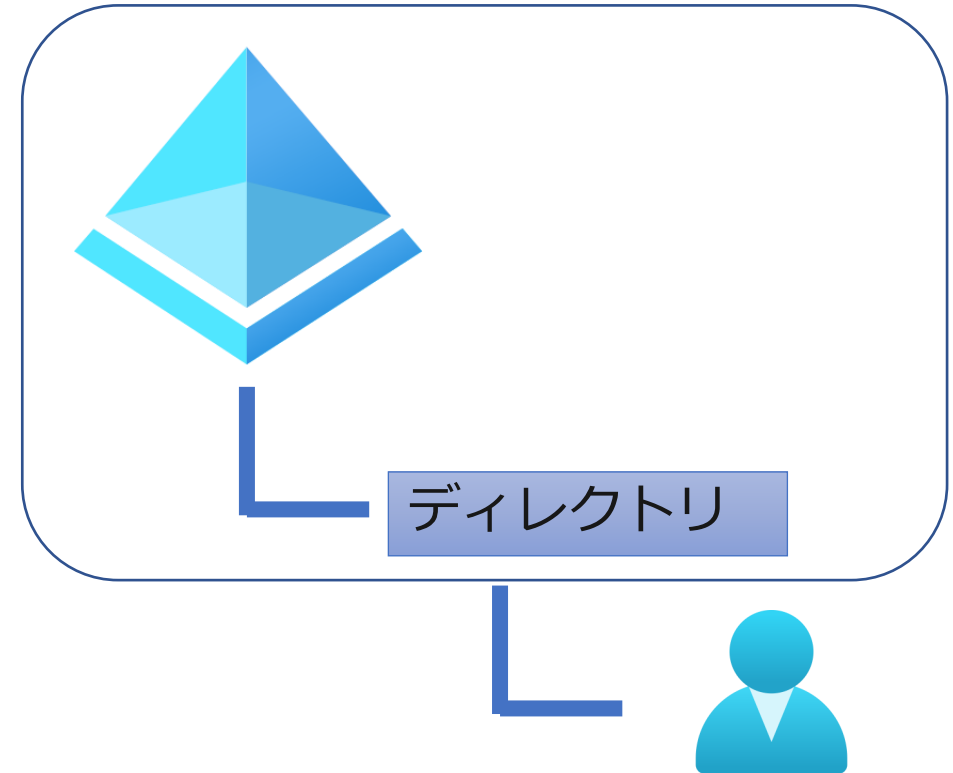
テナント ≡ ディレクトリ

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



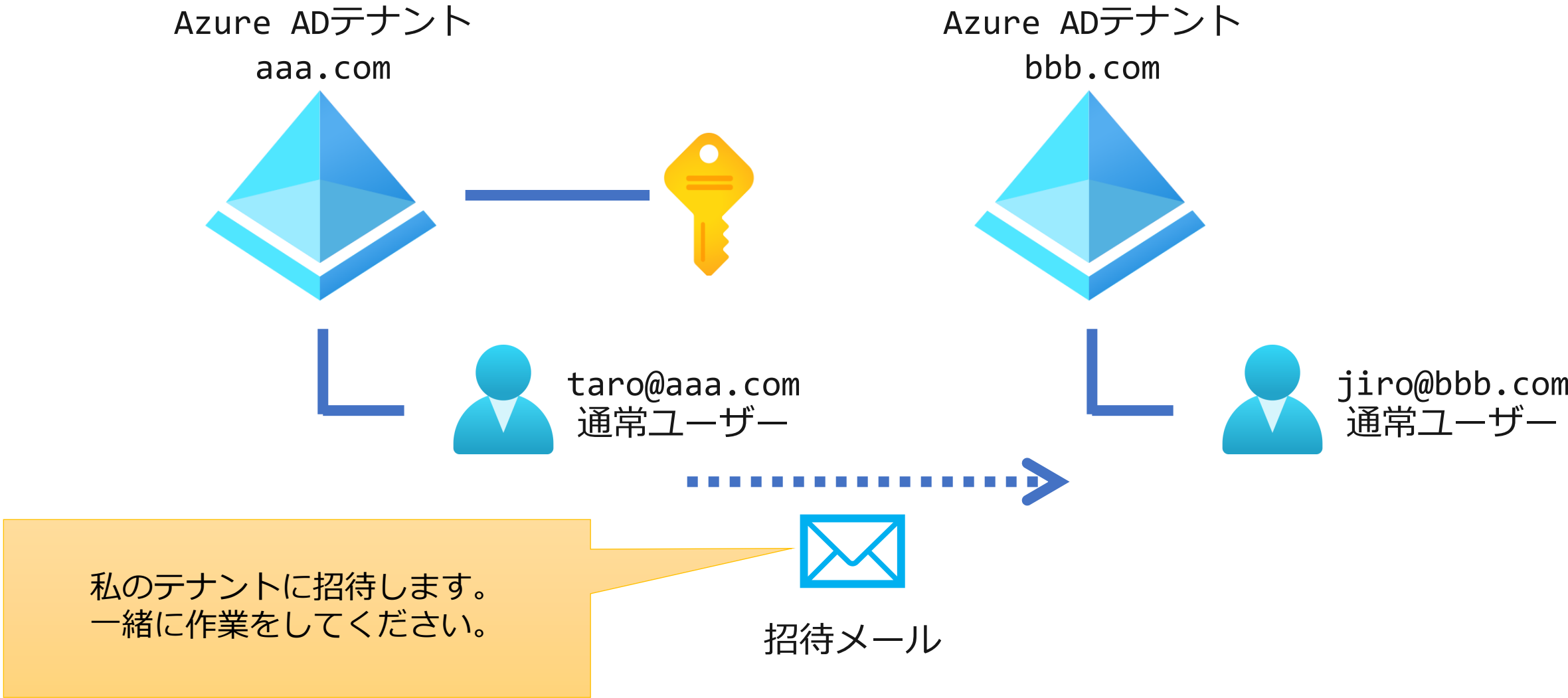
Azure ADテナント



「ディレクトリ」は「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。

Azure ADテナント
aaa.com



Azure ADテナント
bbb.com



taro@aaa.com
通常ユーザー



jiro@bbb.com
ゲストユーザー



jiro@bbb.com
通常ユーザー



招待メール



受理

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

Azure ADのエディション

4種類のエディション

Azure ADには、4種類の**エディション**がある。無料で使用することもできるが、**Azure ADの高度な機能**を使用するには、有料の Azure AD Premium P1 / Premium P2 が必要となる。

<div><div>Azure Active Directory Free</div><div>無料</div><div>無料エディションの Azure AD は商用オンライン サービス (Azure、Dynamics 365、Intune、Power Platform など) のサブスクリプションに含まれています。¹</div></div>	<div><div>Office 365</div><div>無料</div><div>Azure AD の追加機能が Office 365 E1、E3、E5、F1、F3 のサブスクリプションに含まれています。²</div></div>	<div><div>Azure Active Directory Premium P1</div><div>¥750 ユーザー/月</div><div>Azure AD Premium P1 (Microsoft 365 E3 に含まれています) は 30 日間無料試用が可能です。Azure と Office 365 のサブスクリプションのお客様は Azure AD Premium P1 をオンラインで購入できます。</div></div>	<div><div>Azure Active Directory Premium P2</div><div>¥1,130 ユーザー/月</div><div>Azure AD Premium P2 (Microsoft 365 E5 に含まれています) は 30 日間無料試用が可能です。Azure と Office 365 のサブスクリプションのお客様は Azure Active Directory Premium P2 をオンラインで購入できます。</div></div>
---	---	--	--

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)
アクセスレビュー (P2)
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 Azu...

リソース、サービス、ドキュメントの検索 (G+/)

dev18@contoso1800...
CONTOSO (CONTOSO180...

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 - Azure Active Directory

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

フィードバックがある場合

名前	合計	割り当て済み	使用可能
Azure Active Directory Premium P2	100	0	100

Microsoft Azu...

リソース、サービス、ドキュメントの検索 (G+/)

dev18@contoso18...
CONTOSO (CONTOSO...

ホーム > contoso | ユーザー > ユーザー > yamada

yamada | ライセンス

ユーザー

検索

ビュー)

割り当てられたロール

管理単位

グループ

アプリケーション

ライセンス

デバイス

割り当て

再処理

更新

列

フィードバックがある場合

製品	状態	有効なサービス	割り当てパス
Azure Active Directory Premium P2	アクティブ	4/4	直接

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 >

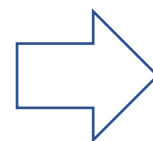
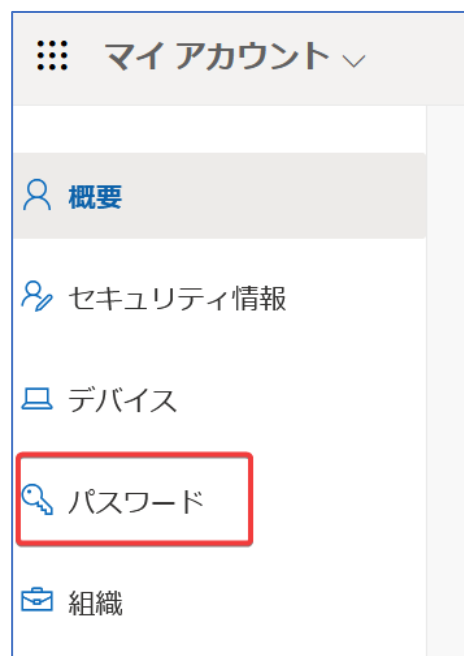
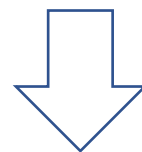
Q. ライセンスの利用場所とはなんですか？

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。**

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、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**Azure ADテナントの管理者が行う**。

Azure AD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、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、**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

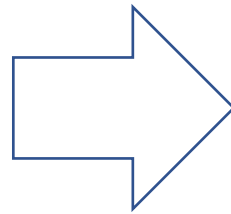
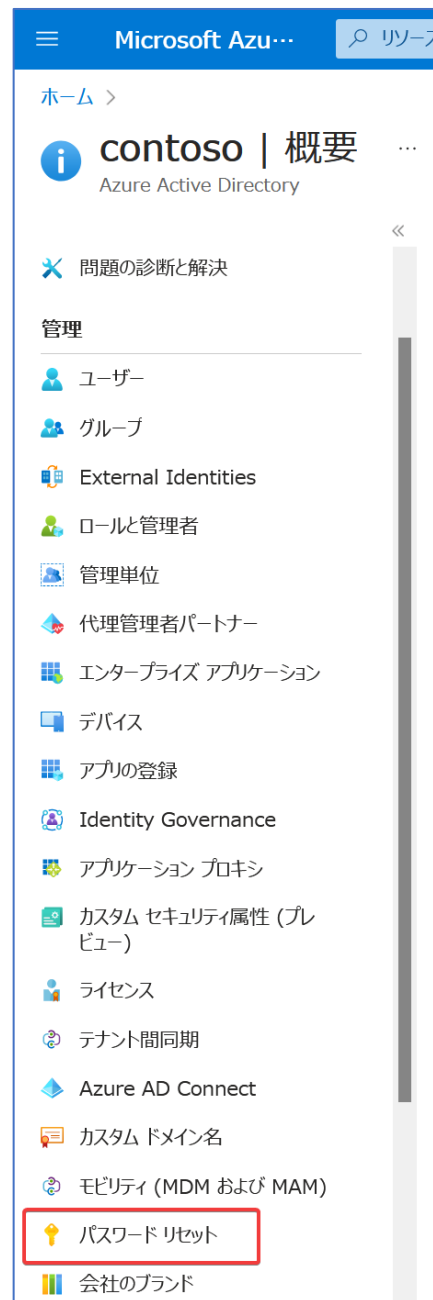
セルフサービスパスワードリセットの必要性

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Azure ADの**セルフサービスパスワードリセット (SSPR)** を設定できる。
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