【Microsoft Entra ID】OpenID Connectの設定手順

2025年8月27日

改定履歴

版数	発行日	改訂内容
第1版	2025年8月27日	初版発行

本資料の内容は 2025/8/27 時点のものです。製品のアップデートにより変更となる場合がございます旨でご了承ください。

Agenda

1. 前提情報
    1. 本書の目的とゴール
    2. 用語集
2. OpenID Connectの構成概要
    1. 本資料のOpenID Connectログインの構成
    2. トークンの種類と役割
    3. Microsoft Graph APIとスコープ（アクセス許可）
    4. OpenID Connect認証フローの再確認
3. OpenID Connect 設定手順
    1. 設定概要
    2. 前提条件・事前準備
    3. 手順1：Entra ID アプリのインストール
    4. 手順2：Entra ID スコープの追加設定
    5. 手順3：手順3：RP プロバイダー設定
    6. 動作確認
4. OpenID Connect認証のトラブルシューティング
    1. OpenID Connect認証のトラブルシューティング
    2. スコープ設定の確認
    3. テナント設定の確認

1. 前提情報

1.1. 本書の目的とゴール

目的

クラウドサービスとMicrosoft Entra ID間でのOpenID Connect連携を行うための実践的な設定手順を理解することを目的とします。
前回学習したOpenID Connectの概要や認証フローの知識を基に実際の設定操作を通じて、 OpenID Connect認証の構成・設定・動作確認のポイントを習得することを狙いとしています。

ゴール

本資料を学ぶことで、 OpenID Connectの設定手順を正しく理解し、設定時に発生するトラブルへの対応にも活かせる知識を身につけることを目指します。

1. **Entra IDとSaaSアプリケーションを用いたOpenID Connect構成の理解**
2. **OpenID Connect 連携に必要となるトークンやスコープ設定、Microsoft Graph API との関わりを理解**
3. **Entra IDでのアプリインストール、スコープ追加などの具体的な設定手順を習得**
4. **実際のテストユーザーを用いた動作確認手順の把握**

1.2. 用語集

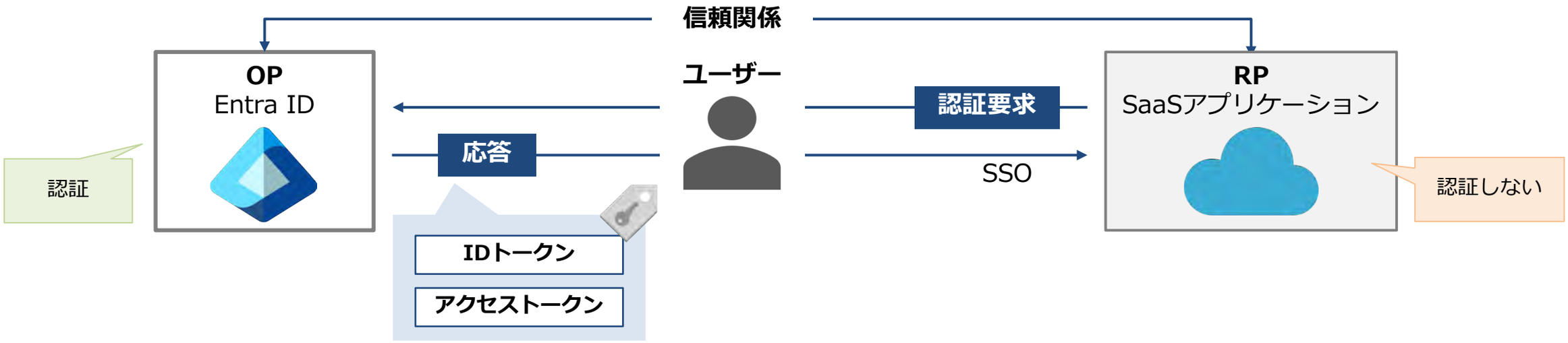
本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
1	OP（OpenID Provider）	ユーザーの認証情報や属性、権限を管理し、認証を行うシステム。ユーザーのログイン情報はOPが保持し、RPには認証結果を連携する。これにより、RPはパスワードを持たず、認証はすべてOP側で行われる。　例：Microsoft Entra ID、Google Workspace、Oktaなど。
2	RP (Relying Party)	ユーザーにサービスを提供する側のシステム（クライアントアプリケーション）。 OPで認証されたユーザー情報を受け取り、サービスを提供する。OPから受け取るIDトークンやアクセストークンを活用し、ユーザーの認証状態を確認したり、ユーザーのデータにアクセスすることが可能。 例：Webアプリケーション、モバイルアプリなど。
3	スコープ	アクセスする情報や機能の種類を指定するための項目。たとえば openid はID情報へのアクセス、email はメールアドレスの取得を意味する。認可リクエスト時に必要な権限を明示する役割を持つ。
4	リフレッシュトークン	アクセストークンの有効期限が切れた後、新しいアクセストークンを取得するために使うトークン。長期的な認証維持に利用される。
5	REST API	HTTPを使ってリソース（データ）を操作する仕組み。GET・POST・PUT・DELETEなどのメソッドで、サーバーとクライアント間の通信を行う。
6	クライアントシークレット	RP自身をOPが認証するための「秘密鍵」のようなもの。クライアントシークレットは、特にサーバーサイドで動作するアプリケーション（Confidential Client）が、OPからトークンを取得する際に、そのRPが正当なRPであることを証明するために使用される。
7	デジタル署名	電子的に文書の正当性と改ざんの有無を保証する技術。公開鍵暗号を使い、本人性と整合性を担保する。

2. OpenID Connectの構成概要

2.1. 本資料のOpenID Connectログインの構成

本資料では、**Microsoft Entra ID**（以降、Entra ID）**をOP［OpenID Provider］、対象のSaaSアプリケーションを RP[Relying Party]**とする OpenID Connect 認証構成の設定手順を説明します。
ユーザーが SaaSアプリケーション にアクセスする際、認証は Entra ID に委任され、OpenID Connectプロトコルを用いたシングルサインオン（SSO）が実現されます。
ユーザーはまず Entra ID で認証され、その結果としてIDトークンやアクセストークンなどの情報が SaaSアプリケーション（RP）に返され、セキュアなアクセスが可能になります。
RP 自体は認証を行わず、認可サーバーである Entra ID（OP）から受け取ったトークンに基づいてアクセスを許可します。



2.2. トークンの種類と役割

OpenID Connectでは、Entra ID がユーザー認証を担い、その結果を**トークン**として SaaS アプリケーションに渡します。
このトークンには「ユーザーが誰か」という情報に加え、どの情報や機能にアクセスできるかを示す**アクセス許可（スコープ）**が含まれています。

トークンとは

- ✓ OpenID Connectでは、ユーザーの認証結果を「**トークン**」というデータで アプリケーション（RP）に渡します。
- ✓ トークンは「**本人確認書類**」のようなもので、ユーザーが誰か、どの情報にアクセスできるかを示します。
- ✓ RP は**トークンを検証する**ことで、ユーザーが誰であるかを確認でき、パスワードを直接扱うことなく安全に認証を行えます。

▶ OpenID Connectで用いられるトークンの種類と役割

ログイン証明書（身分証明書） **API利用許可証（入館証＋権限情報）**

項目	IDトークン	アクセストークン
役割	ユーザーの「**認証**」を証明する（誰であるか）	ユーザーの「**認可**」を証明する（何ができるか）
含まれる情報	ユーザー情報（名前、UPN、メールなど）	許可された操作や範囲（スコープ）
主な利用者	アプリケーション（RP）	API（Microsoft Graph API など）
利用場面	ログイン時に「誰か」をアプリケーションに伝える	アプリケーションがユーザーの代わりに API を呼び出す
有効期限	短め（数分～1時間程度）	短め（数分～1時間程度）※更新はリフレッシュトークン

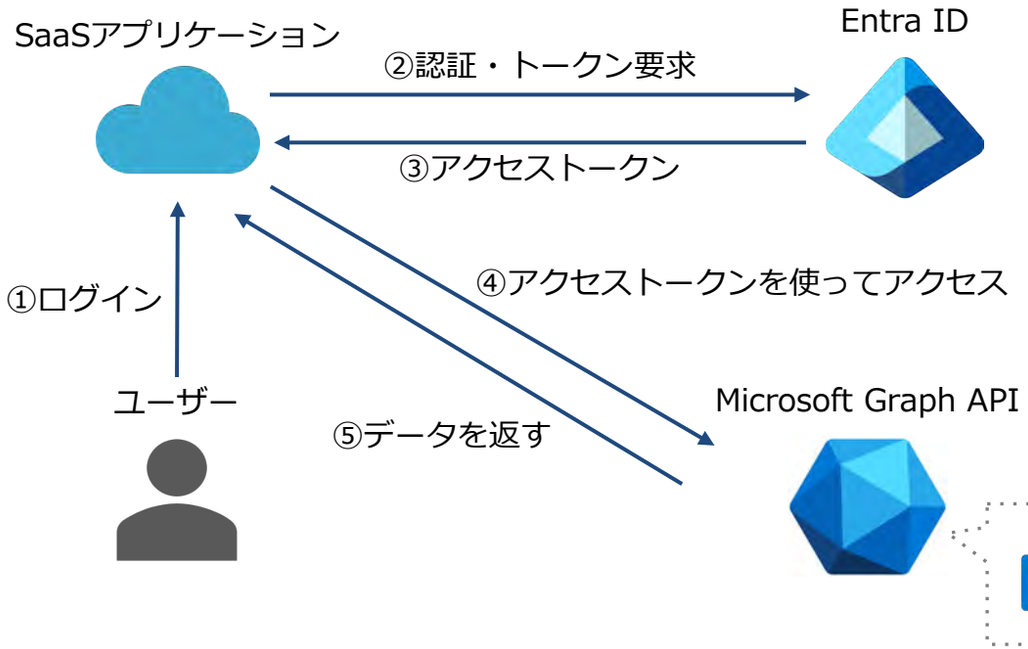
本資料ではRPが、ログイン認証にIDトークンを利用し、Microsoft Graph API呼び出し時にアクセストークンを利用します。

2.3. Microsoft Graph APIとスコープ（アクセス許可）

OpenID Connect による認証後、SaaS アプリケーションがユーザーのデータや Microsoft 365 の機能にアクセスする際には、
Microsoft Graph API を利用します。
このとき、アプリがどの情報や操作にアクセスできるかは、**アクセストークンに含まれる スコープ（アクセス許可） によって制御**されます。

Microsoft Graph APIによるデータ取得

Microsoft Graph APIは、Microsoft 365のサービス（ユーザー情報、メール、予定表、ファイルなど）に統一的にアクセスできるREST APIです。
アプリケーションはアクセストークンを使って、これらのデータを安全に取得・操作できます。



この図は、ユーザーがSaaSアプリケーションにログインして、
Microsoft Graph APIからデータを取得するまでの流れを示しています。

1. ユーザーがアプリにログイン
2. アプリがEntra IDに認証とトークンを要求
3. Entra IDがアクセストークンを発行
4. アプリがアクセストークンを使ってMicrosoft Graph APIにアクセス
5. Microsoft Graph APIが必要なデータを返す

※ OpenID Connectの詳細な認証フローは次項で説明します。

2.3. Microsoft Graph APIとスコープ（アクセス許可）

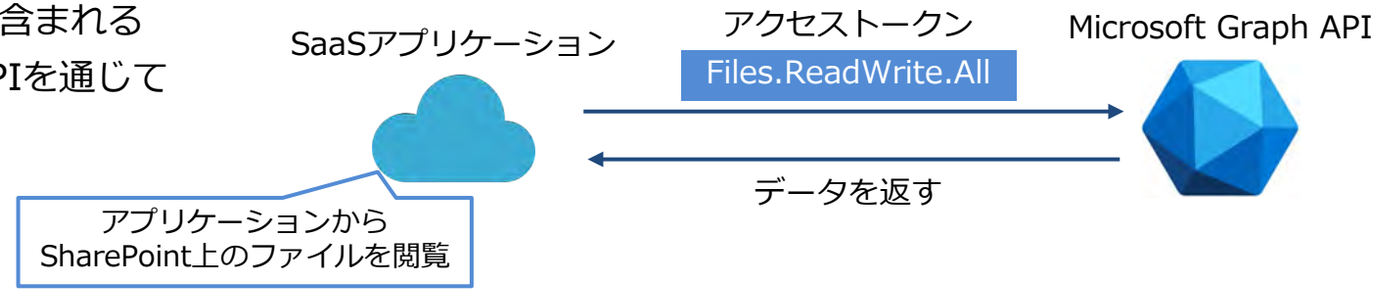
前のスライドで説明したように、アクセストークンには「どの情報にアクセスできるか」を示すスコープが含まれています。
このスライドでは、アクセストークンに含まれるアクセス権（スコープ）の構造を整理します。

アクセス許可（スコープ）と利用ケース

以下は代表的なスコープとその利用ケースです。

スコープ名	説明	アプリケーションでの利用ケース
User.Read.All	組織内のすべてのユーザー情報を読み取り	ユーザー一覧の取得、部署別表示、検索機能など
Read and write all groups	組織内のすべてのグループ情報を読み書き可能	グループの作成・更新・メンバー管理など
Sites.Read.All	SharePointサイトの情報を読み取り	サイト一覧表示、ドキュメントライブラリの参照
Files.ReadWrite.All	ユーザーのすべてのファイルを読み書き可能	OneDriveやSharePoint上のファイルの閲覧・編集・保存
Calendars.ReadWrite	ユーザーの予定表を読み書き可能	スケジュールの取得・登録・更新
Mail.Read	ユーザーのメール（受信トレイ、送信済みなど）を読み取り	アプリ内でユーザーの最新メールを一覧表示

このように、OpenID Connectによる認証とアクセストークンに含まれるスコープ設定によって、アプリケーションはMicrosoft Graph APIを通じて必要なデータを扱えるようになります。



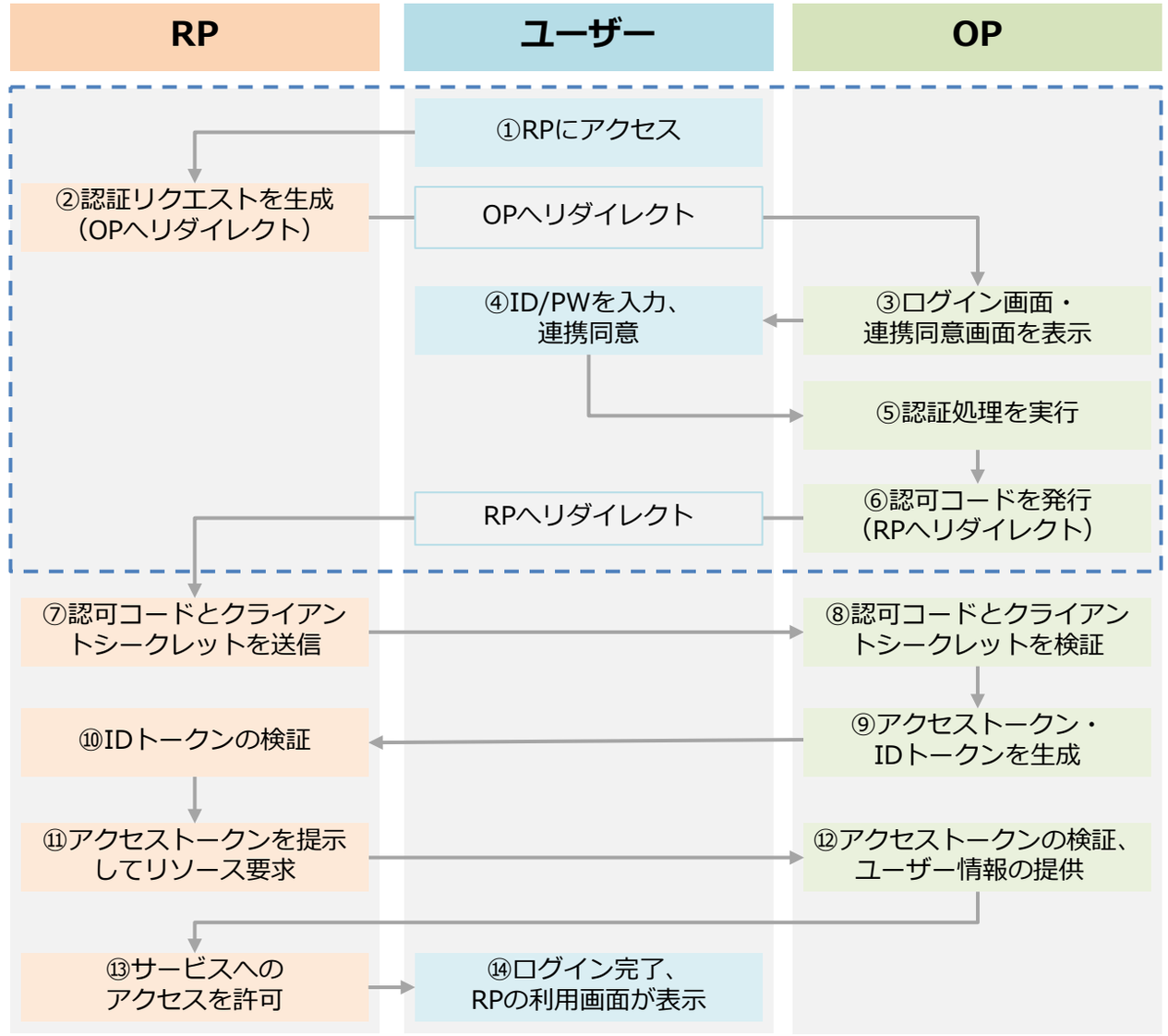
2.4. OpenID Connect認証フローの再確認

本スライドでは、別資料「認証方式とSSOの基礎知識」でご紹介したOpenID Connectの認証フローを再確認します。
後段の設定手順や動作確認とあわせて、実際の処理の流れをイメージしながらご覧ください。

最も一般的な**認可コードフロー**をベースに、OIDC認証フローについて解説します。

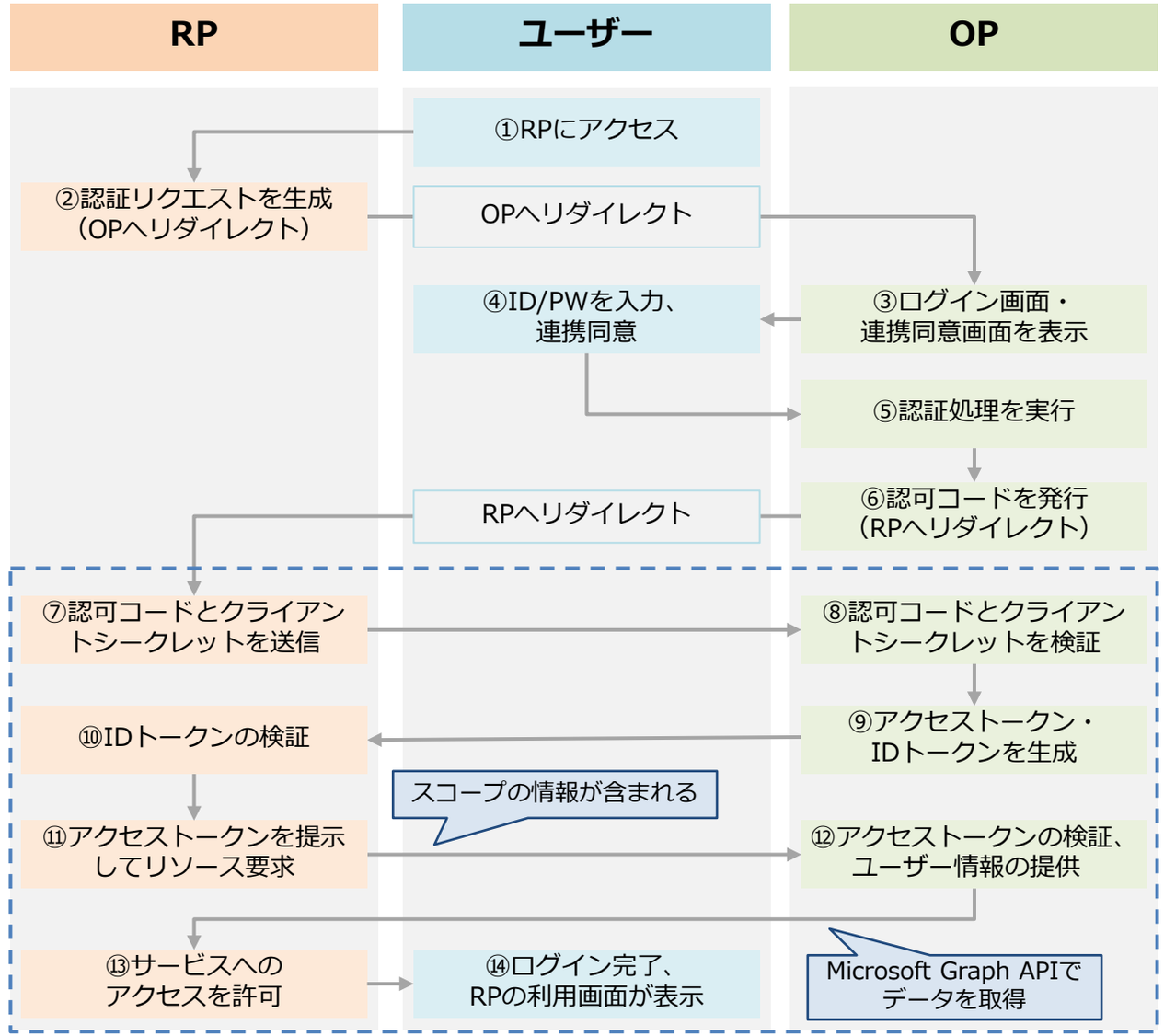
1. ユーザーが**RPのWebサイトやアプリにアクセスし、認証を開始**する。
   例）RPの画面で「Microsoftでログイン」のリンクをクリックする
2. ID連携の要求を受けたRPは、**認証リクエストを生成する。**
   ユーザーのブラウザをOPへリダイレクトさせ、認証リクエストを送信する。
3. OPはユーザーに**ログイン画面を表示**し、認証情報（IDとパスワードなど）の入力を求める。
   必要に応じて、RPがアクセスを求めているユーザー情報（例：氏名、生年月日、住所など）をユーザーに提示し、**その情報へのアクセスを許可するかどうかの同意を求める。**
4. ユーザーはログイン画面で**認証情報を入力**し、RPへの**情報連携に同意**する。
5. OPは入力された情報をもとに**ユーザーの認証を行う。**
6. 認証が成功すると、**OPはRPに「認可コード」を発行**する。
   ユーザーのブラウザをRPへリダイレクトさせ、**認可コードを送信**する。

認可コードとは、ユーザーがOPで認証されたことを一時的に示すコードで、最終的にIDトークン・アクセストークンと交換するために使われます。
トークンを安全にサーバー間通信で取得でき、漏洩リスクを防ぐことができます。



2.4. OpenID Connect認証フローの再確認

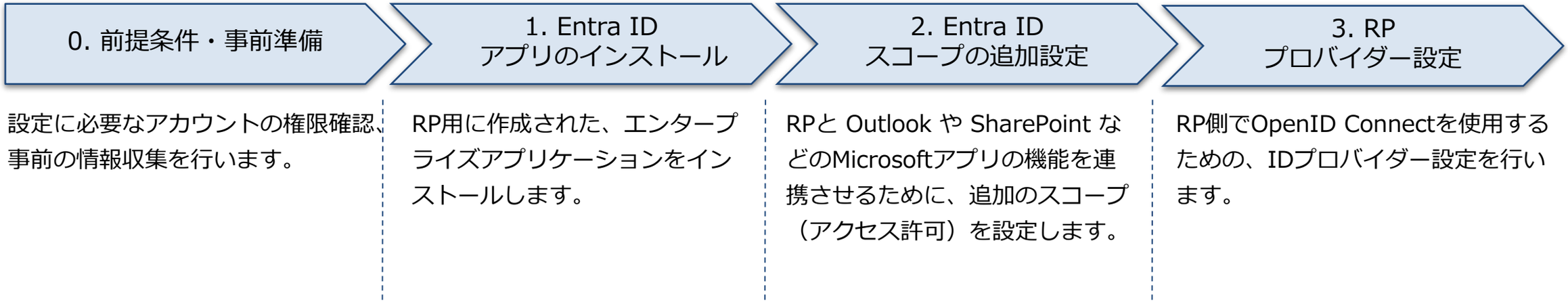
7. RPは受け取った**認可コード**と、自身の**クライアントシークレットをOPに送信**して、トークンをリクエストする。
8. OPは、受け取った**認可コードとクライアントシークレットを検証**する。
   検証では認可コードの有効性や正しいリクエストか、などを確認する。
9. OPは、検証が完了したら「**IDトークン**」と「**アクセストークン**」を生成しRPに返す。
10. RPは受け取った**IDトークンのデジタル署名を検証**し、改ざんされていないこと、有効期限内であること、正規のOPから発行されたものであることを確認する。
11. RPは、必要に応じて**アクセストークンを提示**し、**OPに対して追加のユーザー情報取得やリソースへのアクセスを要求**。（例：氏名、生年月日、住所など）
12. OPは、RPから受け取ったアクセストークンの有効性を検証し、問題なければ**アクセスが許可されているユーザー情報（属性など）をRPに提供**する。
    フローの⑦～⑪はユーザーを介さず、RPとOP間で直接行われる。
13. RPは、情報取得が完了するとユーザーを認証済みとして扱い、**サービス画面へのアクセスを許可**する。
    ユーザー情報の取得後、RPはアクセス制御をしたりプロフィールページの自動生成を行う。
14. ユーザーは**RPのサービスを利用できる**ようになる。



3. OpenID Connect 設定手順

3.1. 設定概要

本章では、Entra IDとSaaSアプリケーション間でOpenID Connectを構成するための一連の設定手順を説明します。
以下の図は、設定作業の全体の流れを示したものです。
★Entra IDのギャラリーアプリには、OpenID Connectを事前構成済みのアプリケーションが多数含まれており、
複雑な設定を必要とせず、短時間で導入ができるようになっています。



それぞれのステップで必要となる設定内容や確認ポイントについては、次のスライド以降で詳しくご案内します。

設定後は、OpenID Connectフローに基づく動作確認を行い、適切に認証が完了するかを検証します。

設定のポイント

設定作業は可能な限り**一人で実施することを推奨**します。
OPとRPで設定・検証を同時に進める場面が多いため、複数人で作業を分担すると、設定ミスや連携不備の原因となる可能性があるためです。

3.2. 前提条件・事前準備

0. 前提条件・事前準備 → 1. Entra ID アプリのインストール → 2. Entra ID スコープの追加設定 → 3. RP プロバイダー設定

本手順書の前提条件

- 本資料では、Entra ID を OP、SaaS アプリケーションを RPとした OpenID Connectの設定手順を対象としています。
  対象の SaaS アプリケーションは、社内ポータルサイトとして利用されています。
- 本手順書ではOpenID Connectの認証設定に加え、Entra ID からのユーザー・グループ同期設定も含んでおります。
- 他のOPやRP（Okta、Google Workspace、Box など）を使用する場合は、設定項目や手順が一部異なる可能性があります。
  そのため、別環境に適用される際は各サービスの公式ドキュメントをご確認の上、環境に応じて適宜読み替えてください。

事前準備

1. 管理者権限の確認

Entra IDとRPの両方で管理者権限を持つアカウントが必要です。
Entra ID：グローバル管理者の権限が必要です。
RP：グローバル管理者の権限が必要です。

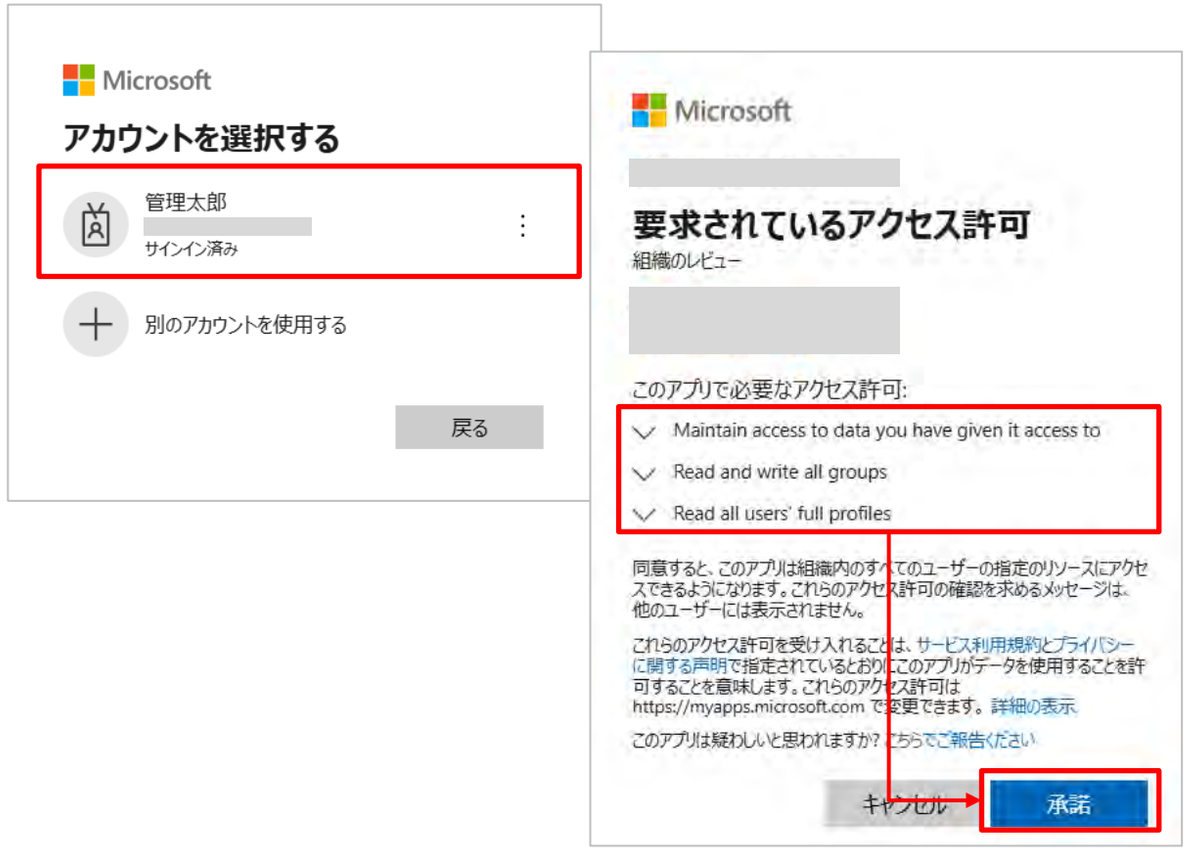
2. テストユーザーの用意

OpenID Connectの動作確認用に、テストユーザーアカウントを用意しておくと安全です。

3.3. 手順1：Entra ID アプリのインストール

0. 前提条件・事前準備 | 1. Entra ID アプリのインストール | 2. Entra ID スコープの追加設定 | 3. RP プロバイダー設定

RP 用に作成されたエンタープライズアプリケーションを Microsoft Entra ID のテナントにインストールし、RP に必要な権限を付与します。



手順

Entra IDで作業

1. RPで指定されたリンクを用いて、アプリケーションのインストール画面に遷移します。
2. Microsoft 365のグローバル管理者でログインします。
3. 必要なスコープ（アクセス許可）を確認して「承諾」をクリックします。
   承諾後、Entra IDにアプリケーションがインストールされます。

【この画面で要求されているアクセス許可】

✓ データへのアクセス権限
✓ グループの読み書き権限
✓ ユーザープロフィールの読み取り権限

SaaS アプリケーションと Entra ID を連携するために必須の権限です。

3.3. 手順1：Entra ID アプリのインストール

Entra IDで作業

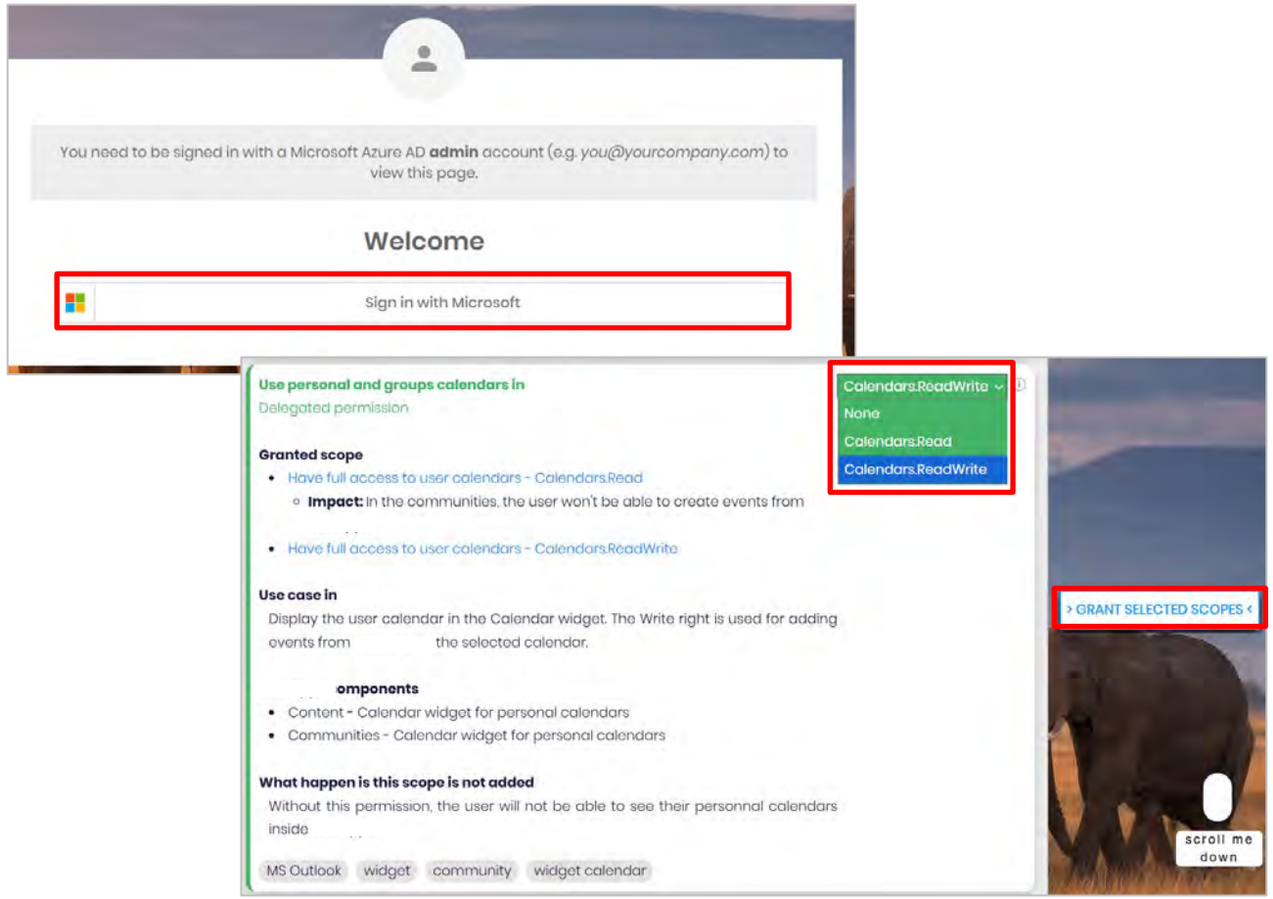
手順

4. 管理者アカウントでMicrosoft Entra 管理センターにアクセスします。
5. 左ナビゲーションの「Entra ID」＞「エンタープライズアプリ」を選択します。
6. アプリケーションの一覧からインストールしたアプリが表示されていることを確認します。

3.4. 手順2：Entra ID スコープの追加設定

0. 前提条件・事前準備 → 1. Entra ID アプリのインストール → **2. Entra ID スコープの追加設定** → 3. RP プロバイダー設定

RPと Outlook や SharePoint などのMicrosoftアプリの機能を連携させるために、追加のアクセス許可を設定します。

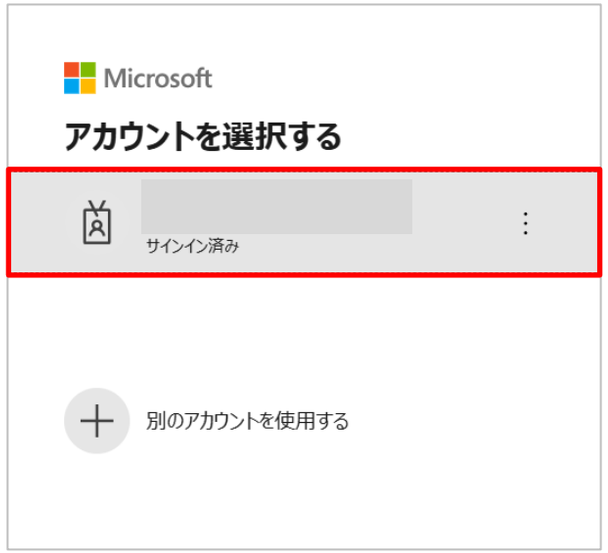


Entra IDで作業

手順

1. RPで指定されたリンクを用いて、アクセス許可の画面に遷移します。
2. Microsoft 365のグローバル管理者でログインします。
3. 必要なスコープ（アクセス許可）を付与していきます。
   例）Calendars.Read：
   ユーザーの予定表を表示するための読み取り権限
   許可がない場合、SaaSアプリケーションで予定表のデータを表示できない。
4. 付与するアクセス許可を選択したら、「GRANT SELECTED SCOPES」をクリックします。

3.4. 手順2：Entra ID スコープの追加設定

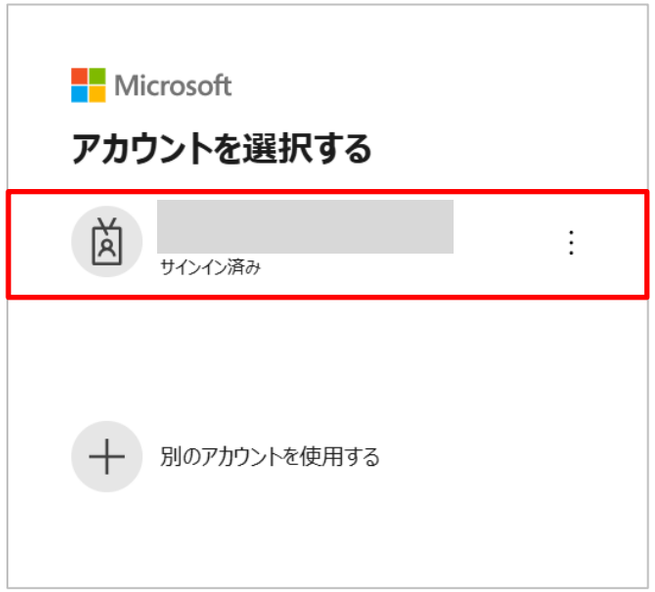


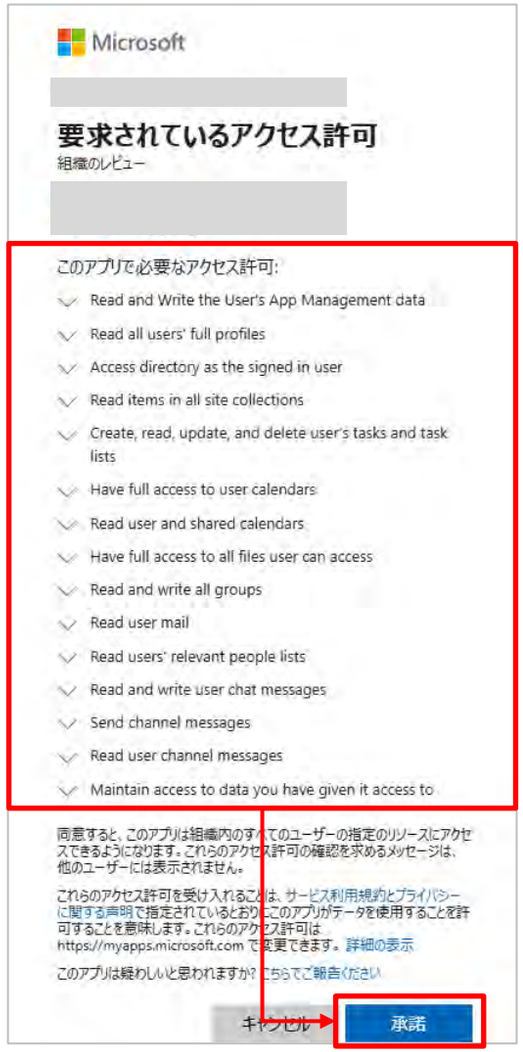
Entra IDで作業

手順

5. ログイン時と同様のアカウント（Microsoft 365のグローバル管理者）を選択して、ログインを行います。
6. アクセス許可を確認して「承諾」をクリックします。

3.4. 手順2：Entra ID スコープの追加設定

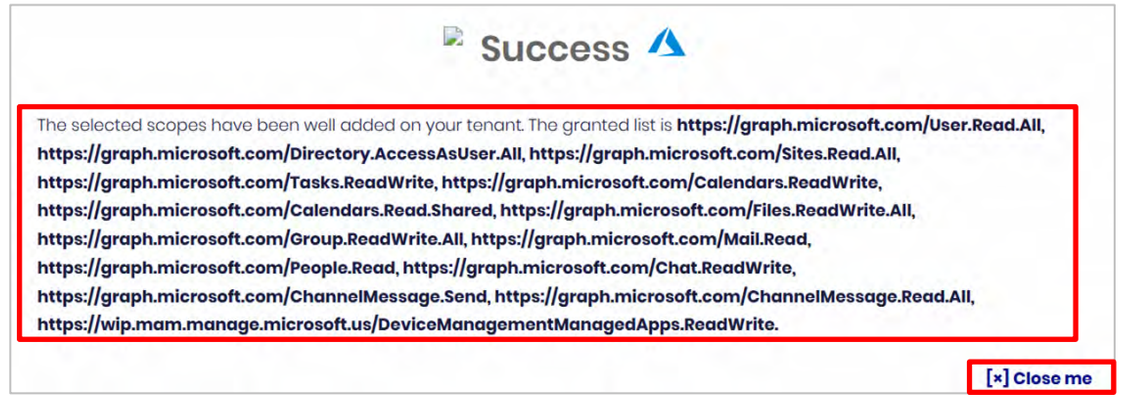




Entra IDで作業

手順

7. 同様のアカウントで、再度ログインを行います。
8. 先ほど選択したスコープ（アクセス許可）の一覧が表示されます。
   許可内容を確認して、「承諾」をクリックします。
9. 許可されたアクセス権限のリストが表示されたら、完了です。
   「Close me」をクリックして閉じます。



3.4. 手順2：Entra ID スコープの追加設定

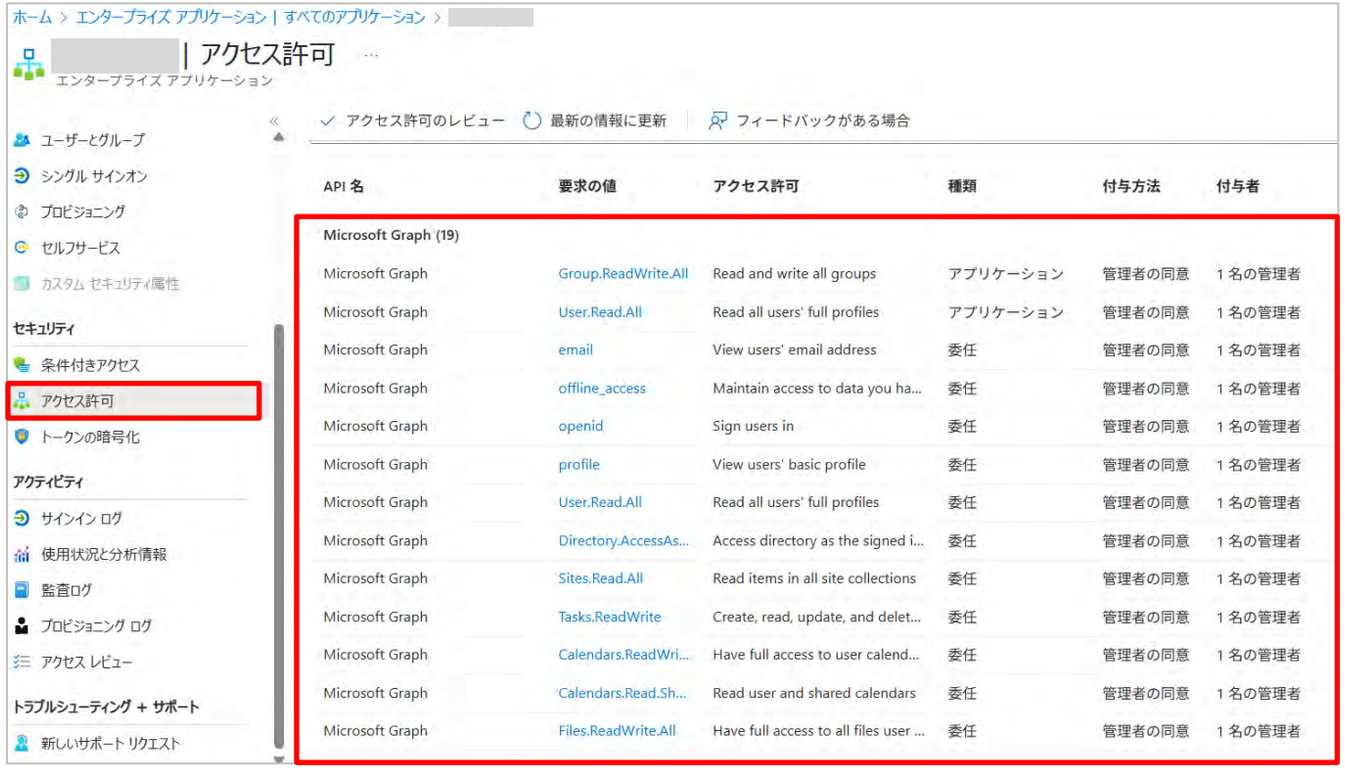
Entra IDで作業

手順

許可されたスコープはMicrosoft Entra 管理センターのエンタープライズアプリケーションから確認可能です。

10. 管理者アカウントでMicrosoft Entra 管理センターにアクセスします。
11. 左ナビゲーションの「Entra ID」＞「エンタープライズアプリ」を選択します。
12. アプリケーション一覧から、手順1でインストールしたアプリケーションをクリックします。

3.4. 手順2：Entra ID スコープの追加設定



Entra IDで作業

手順

13. 左側メニューの「アクセス許可」をクリックすると、許可した権限を確認できます。

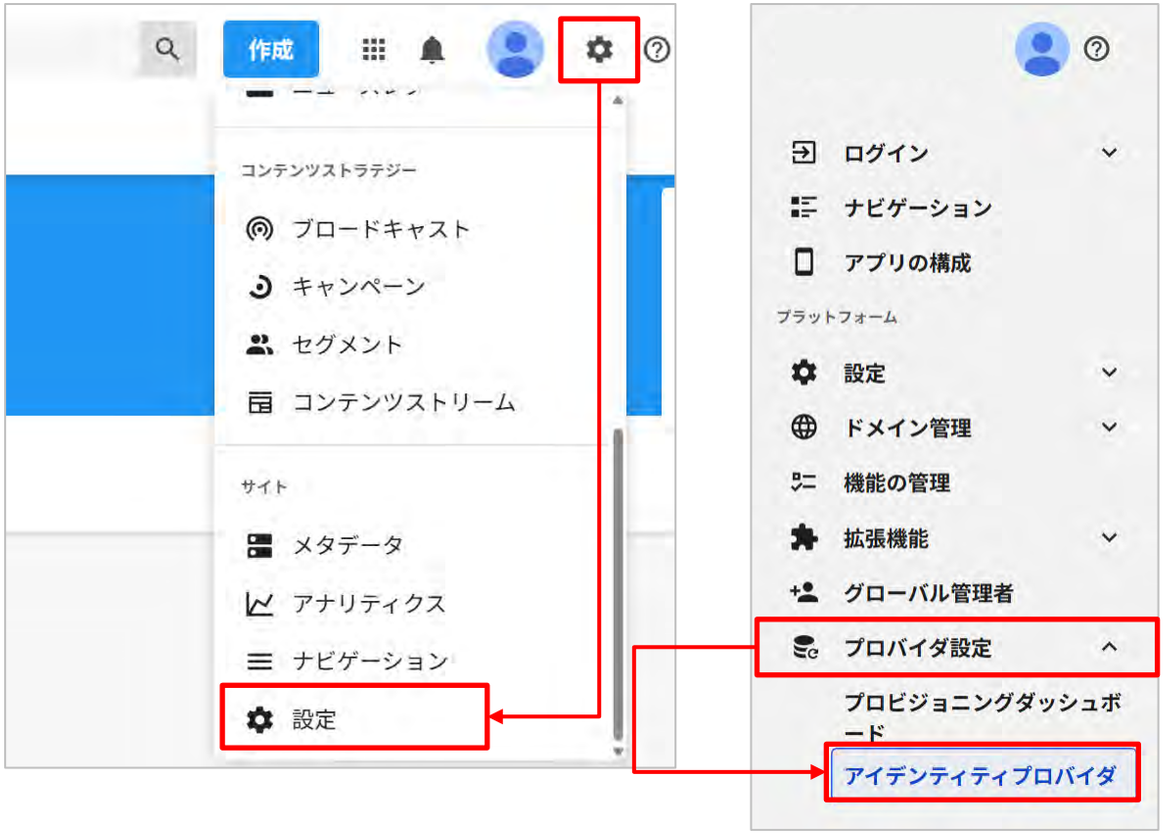
ここで追加したスコープは、ユーザーがログインする際の**アクセストークン**に含まれ、Microsoft Graph APIを通じて必要なデータの取得に使用されます。

3.5. 手順3：RP プロバイダー設定

0. 前提条件・事前準備 → 1. Entra ID アプリのインストール → 2. Entra ID スコープの追加設定 → 3. RP プロバイダー設定

RP側でOpenID Connectを使用するための、IDプロバイダー設定を行います。

SPで作業



手順

1. RPのグローバル管理者でサイトにアクセスします。
2. 右上の歯車マークをクリックし、「設定」を選択します。
3. 管理画面に遷移するため、「プロバイダ設定」＞「アイデンティティプロバイダ」を選択します。

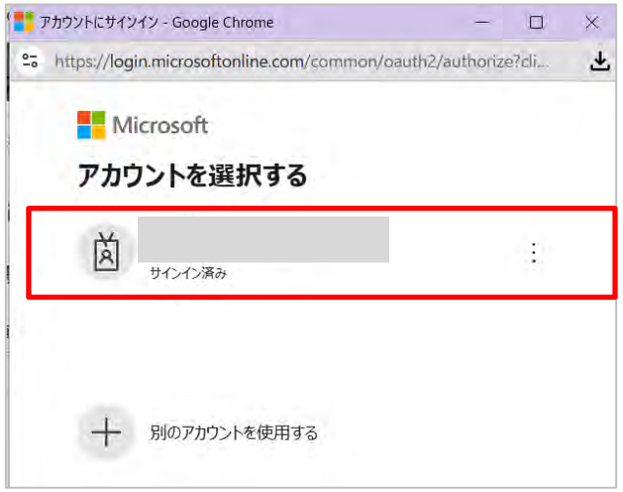
3.5. 手順3：RP プロバイダー設定

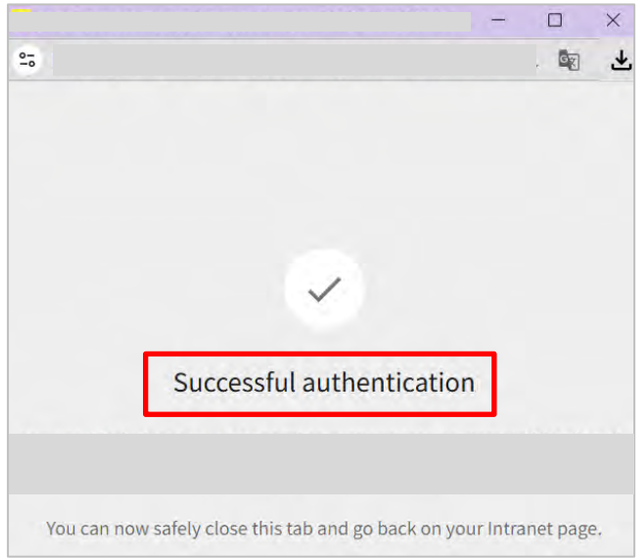
SPで作業

手順

4. 右上の「新規」＞「Microsoft」を選択します。

3.5. 手順3：RP プロバイダー設定





SPで作業

手順

5. 「名前」欄にプロバイダーの 名前 を入力します。
6. 「ソース」の「テナントID/ドメインを追加するにはご自身のアカウント情報でサインインしてください」をクリックして、対象のドメインと接続します。
7. Microsoftのグローバル管理者アカウントでサインインします。
8. 「Successful authentication」の画面が表示されたらドメインとの接続が完了です。ウィンドウを閉じます。

3.5. 手順3：RP プロバイダー設定

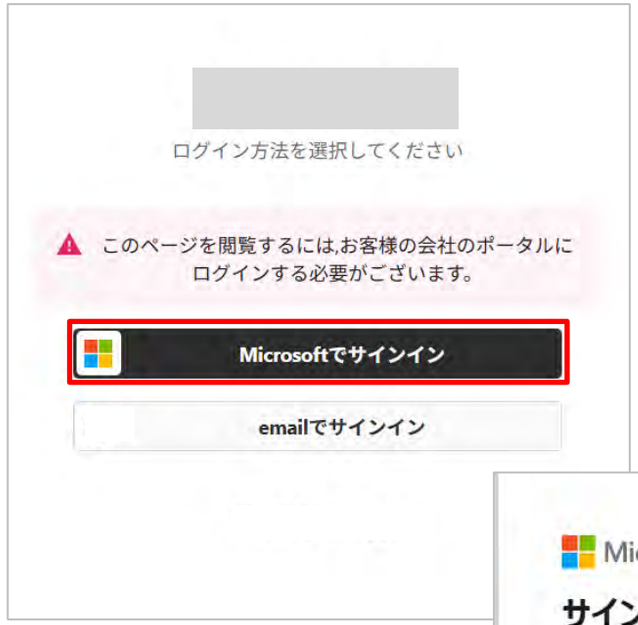
手順

SPで作業

9. オプションを設定します。
   「ログインを有効化」、「ユーザー プロビジョニングを有効化」を有効にします。
   その他のオプションも任意で有効にします。
10. 「保存」をクリックします。
11. プロバイダーの一覧に追加されたことを確認し、設定完了です。
12. ユーザー同期がかかると、RPにMicrosoft 365のユーザーが追加され、OpenID ConnectによるSaaSアプリケーションへのログインが可能になります。

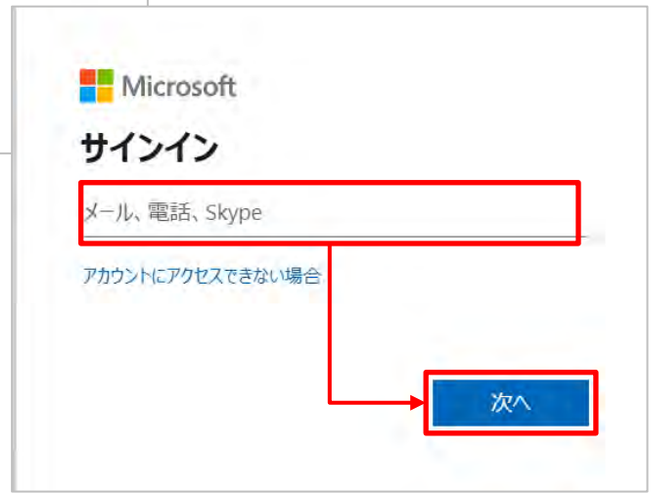
3.6. 動作確認

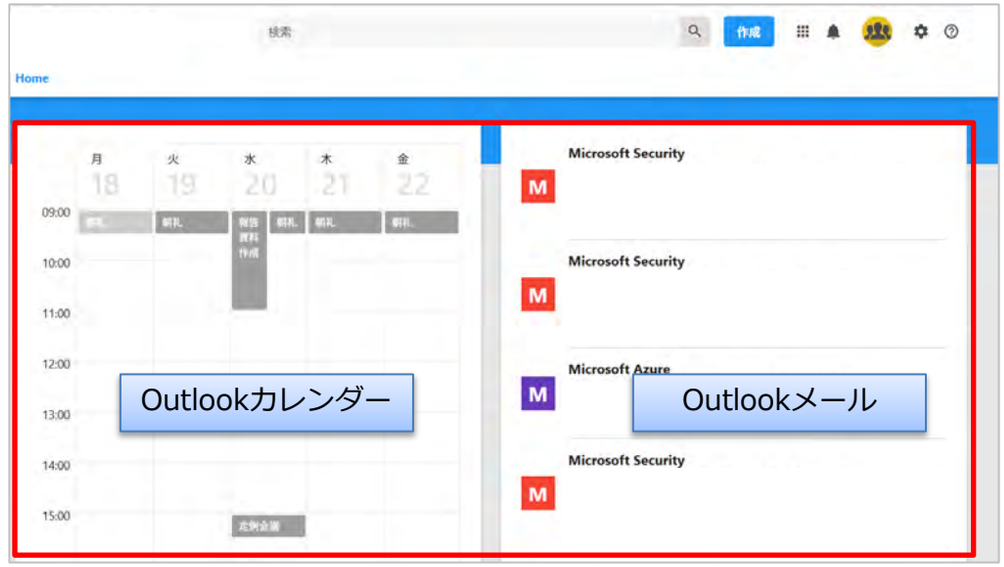
OpenID Connectの設定が完了したら、あらかじめ用意したテストアカウントを使用し、正常にログインできることを確認します。
想定通りに認証が行われるかを事前に確認することで、本番ユーザー展開時のトラブルを未然に防ぐことができます。



手順

1. シークレットモードのブラウザで、ログインを行うSaaSアプリケーションのサイトにアクセスをします。
2. 「Microsoftでサインイン」のログインボタンをクリックします。
3. 組織のMicrosoft 365アカウントでログインを実行します。
4. SaaSアプリケーションにリダイレクトするため、アクセスできることを確認して完了です。
   スコープの追加でMicrosoft 365アプリとの連携を許可している場合は、問題なくデータが表示されているかを確認します。





4. OpenID Connect認証のトラブルシューティング

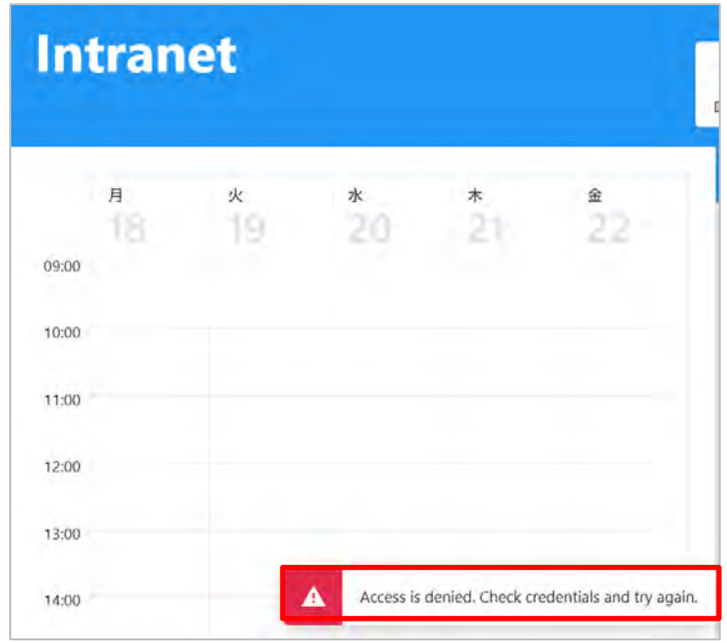
4.1. OpenID Connect認証のトラブルシューティング

OpenID Connectによるログイン失敗やエラーが発生する場合、設定ミスやスコープ不足など、さまざまな要因が考えられます。
本スライドでは、Entra IDとRP間のOpenID Connect認証における代表的なトラブルとその初期対応方法をまとめています。
問題が発生した際の確認ポイントとしてご活用ください。

確認項目	内容	補足/参考情報
1. スコープ設定の確認	認証リクエストに必要なスコープ（例：User.Read.All）が含まれているか確認	次ページにて詳しく説明します
2. テナント設定の確認	アプリがユーザーの所属するテナントに正しく登録されているか確認	次ページにて詳しく説明します
3. エラー内容の確認	表示されたエラーメッセージやエラーコードを確認	Microsoft Entra 認証と承認のエラーコード
4. ブラウザキャッシュ/SSO影響	古いセッションやキャッシュが原因である場合	シークレットモードで再試行します。
5. テストユーザーでの再現確認	特定ユーザーに依存した問題か、全体的な設定問題かを切り分ける	–

4.2. スコープ設定の確認

↓本来であればOutlookカレンダーの情報が
表示されるが、エラーが表示される。



エラー概要

アクセストークンに必要な権限（例：Site Read all, Calendars.ReadWriteなど）が含まれておらず、アプリケーションが期待通りに動作しない。

原因

・必要なスコープが追加されていない、または管理者同意が必要なスコープに対して同意が未実施（例：User.Read, email, offline_access, User.Read.All）

対処法

・［手順2：Entra ID スコープの追加設定］でのスコープの追加を再度実施する。
・Microsoft Entra 管理センターの「アクセス許可」の画面で、必要なスコープが追加されているか確認する。

補足

管理者同意が必要なスコープは、ユーザー単位では許可できないため、事前に確認しておくとトラブルを防げます。

4.3. テナント設定の確認

エラー概要

ユーザーが指定されたテナントに存在しないため、アプリケーションにアクセスできない。

原因

・RP側のプロバイダー設定で指定されたテナントIDが、アプリがインストールされている Microsoftテナントと一致していない
・対象テナントにユーザーが外部ユーザーとして招待されていない

対処法

・［手順1：Entra ID アプリのインストール］のアプリインストール先のテナントと［手順3：RP プロバイダー設定］ の手順6で接続するテナントが一致しているかを確認。
・必要に応じて、対象テナントにアプリを再インストールするか、管理者同意を取得する。