【Microsoft Entra ID】SAMLの設定手順

2025年7月30日

改定履歴

版数	発行日	改訂内容
第1版	2025年7月30日	初版発行

本資料の内容は 2025/7/30 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. SAML構成の概要
    1. 本資料のSAML構成
    2. SAML設定に必要な情報
    3. SAML認証フローの再確認
3. SAML認証 設定手順
    1. 設定概要
    2. 前提条件・事前準備
    3. 手順1：SP プロバイダー設定
    4. 手順2：Entra ID アプリの作成
    5. 手順3：Entra ID SAML SSOを設定
    6. 手順4：Entra ID マッピング属性
    7. 手順5：Entra ID メタデータをダウンロード
    8. 手順6：SP メタデータをインポート
    9. 手順7：Entra ID ユーザーのSAMLを有効にする
    10. 動作確認
4. SAMLログイン失敗時のトラブルシューティング

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SAML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SAML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、SAML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、SAML認証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SAML構成の理解**
2. **SAML連携に必要な設定情報の把握と構成要素の関連付け**
3. **Entra IDでのSAMLアプリ設定、属性マッピング、証明書連携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	IdP[Identity 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IdPが保持し、サービス提供者（SP）には認証結果を連携する。これにより、SPはパスワードを持たず、認証はすべてIdP側で行われる。 例：Microsoft Entra ID、Okta、Google Workspaceなど。
2	SP[Service Provider]	ユーザーにサービスを提供する側のシステム。IdP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。 IdPから受け取る認可情報を活用し、管理者機能の許可や特定ユーザーへの機能制限も行うことが可能。 例：Salesforce、Slack、Boxなど。
3	SAMLアサーション（Assertion）	IdPが発行するXML形式の認証情報。ユーザーの認証状態や属性情報（名前、メールアドレスなど）、認可情報（アクセス権限）、デジタル署名などの情報を持つ。
4	SaaS (サース、サーズ)	インターネット経由でソフトウェアをクラウドサービスとして利用できる仕組み。 正式には「Software as a Service」の略称で、従来のインストール型ソフトウェアとは異なり、サービス提供事業者のサーバー上で動作する。
5	エンティティ（Entity）ID	SAMLプロトコルにおいてSPやIdPを一意に識別するための文字列
6	エンタープライズアプリケーション	Entra IDのエンタープライズ アプリケーションとは、外部や社内のアプリをEntra IDと連携させ、シングルサインオン（SSO）やアクセス制御を行うための管理対象。ユーザーやグループの割り当て、認証ポリシーの設定などが可能。

1.2. 用語集

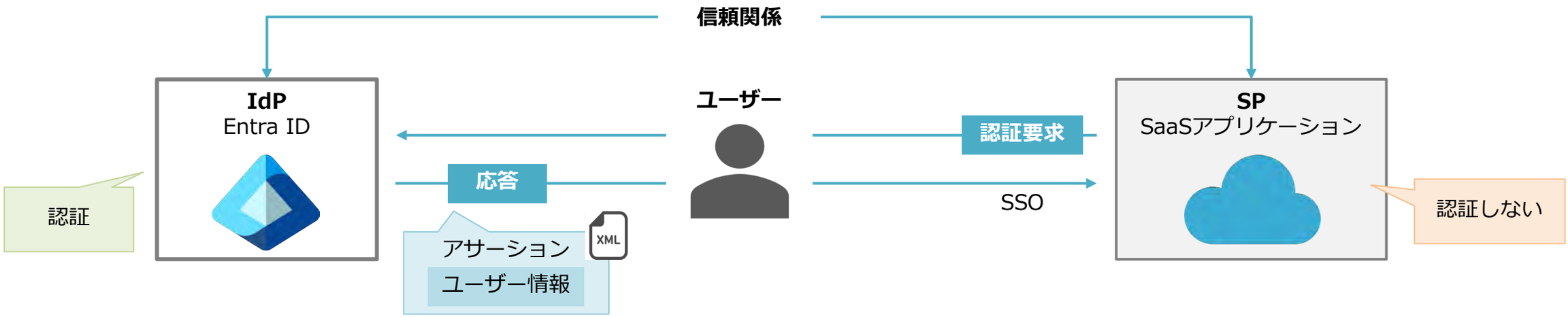
本書で使用する用語及び略称を以下の通り定義します。

No.	用語	説明
7	UPN	UPN（User Principal Name）とは、Microsoft Entra IDなどの認証システムでユーザーを一意に識別するためのID形式で、通常は「ユーザー名@ドメイン名」の形をしている。 例）taro@example.com UPNはサインイン時のユーザー識別やSAMLなどの認証プロトコルでも使用される。
8	SAML JIT	SAML JIT（Just-In-Time）プロビジョニングとは、SAML認証を使ってユーザーが初めてアプリケーションにサインインしたタイミングで、そのユーザー情報を自動的に作成・登録する仕組み。 IdPから送られてくるSAMLアサーションに含まれる属性情報（氏名、メールアドレス、所属など）をもとに、SP側でユーザーアカウントを即時に生成する。
9	Entra ID グローバル管理者	Entra IDにおける最上位の管理ロールで、すべての機能や設定にアクセス可能。 ユーザー管理、アプリ登録、セキュリティポリシー設定、ライセンス割り当てなど、全体の管理を担うため、原則として最小限のユーザーのみに割り当てることが推奨される。
10	Entra ID クラウド アプリケーション管理者	Entra ID 上のエンタープライズ アプリケーション（SaaSアプリ等）の登録・設定を管理できるロール。 アプリの追加、構成、シングルサインオン（SSO）の設定などを行えるが、ユーザーの管理権限は持たない。グローバル管理者の権限を細分化したロールの一つ。

2. SAML構成の概要

2.1. 本資料のSAML構成

本資料では、**Microsoft Entra ID**（以降、Entra ID）**をIdP[Identity Provider]、対象のSaaSアプリケーションを SP[Service Provider]**とする SAML 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、**SAML 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、その結果として認証状態や属性情報を含むアサーションが SP に渡され、セキュアなアクセスが可能になります。**SP 自体は認証を行わず、IdP（Entra ID）からの情報に基づいてアクセスを許可**します。



2.2. SAML設定に必要な情報

設定手順に入る前に、SAML 連携に必要となる各種情報や設定項目について、あらかじめ整理して説明します。
これにより、後続の手順をスムーズに進められるようにします。

▶ SP側で必要となる情報（Entra IDから取得）

設定項目	説明
フェデレーション メタデータ XML	SAML連携において、**IdPとSP間の信頼関係を確立するための構成情報をXML形式で記述したファイル**。このファイルを使用することで、手動で各設定値（URLや証明書など）を入力せずに、SAML連携に必要な情報を自動的に取得・設定できる仕組みを提供する。 主に、IdPのエンティティ ID（識別子）、署名用証明書、SSOエンドポイント、NameIDFormat（ユーザー識別形式）、属性情報の定義などが含まれている。
IdPのエンティティ ID（識別子）	メタデータに含まれる。SAML連携で**認証する側（IdP）を一意に識別するためのID**であり、通常URL形式の文字列で表される。SP側で信頼できるIdPとして登録するために使用される。
署名用証明書	SAMLメタデータに含まれる**公開鍵証明書**で、IdPが発行する**SAMLアサーションの正当性をSPが検証するために使用**される。有効期限も設定される。
SSOエンドポイント	メタデータに含まれる。SPがユーザーの認証を依頼する際に、**SAML認証要求を送信するIdP側のURL**。
NameIDFormat（ユーザー識別形式）	メタデータに含まれる。SAML認証において**ユーザーを識別するために使用される「識別子の形式」を定義**するもの。（例：email、UPNなど）
属性情報の定義	認証時に**SAMLアサーションに含めるユーザー属性の種類を定義**する。 実際の値は含まれず、どの属性を渡すかの設計情報が含まれる。

2.3. SAML設定に必要な情報

▶ IdP（Entra ID）側で必要となる情報（SPから取得）

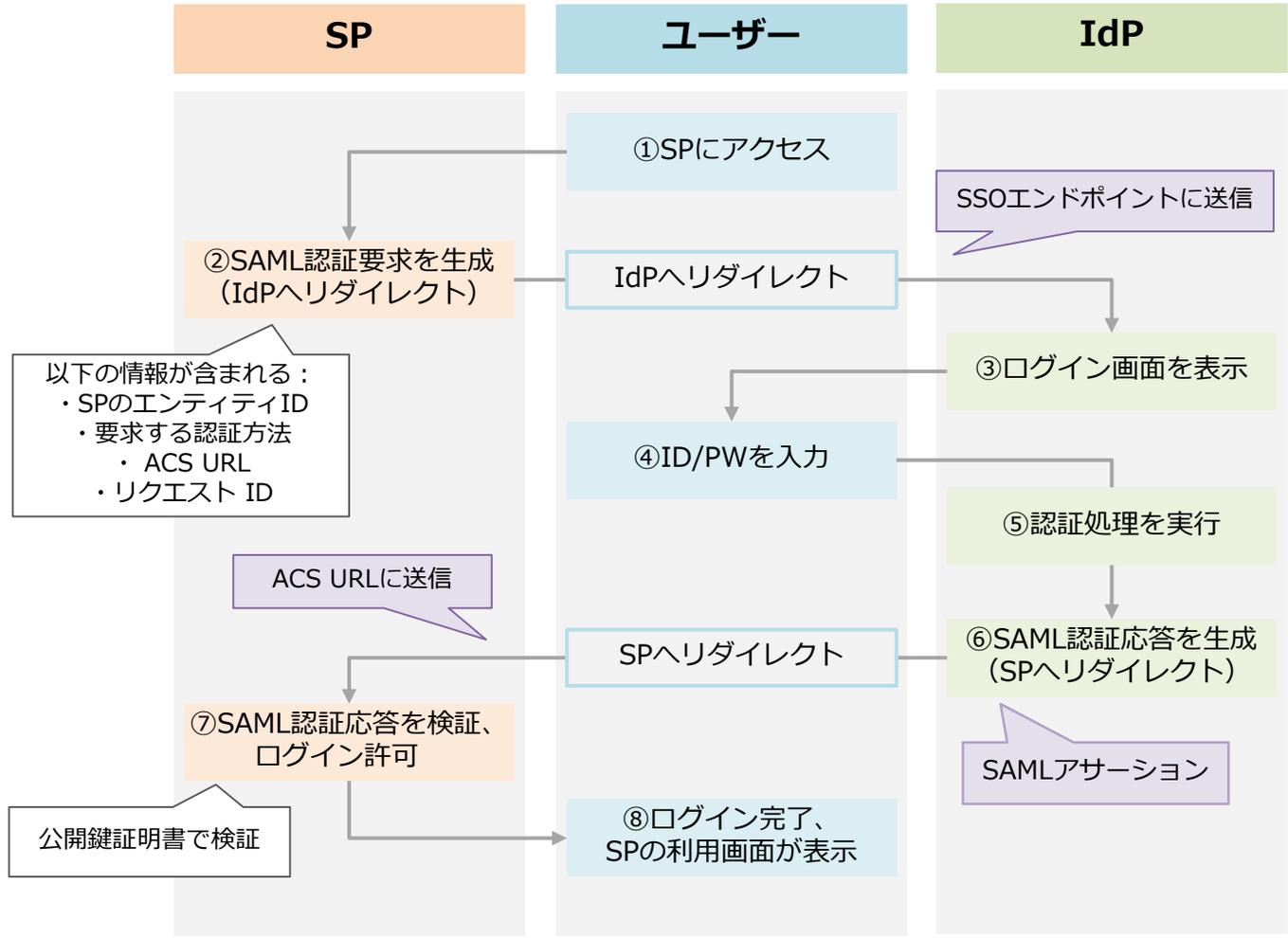
設定項目	説明
SPのエンティティ ID（識別子）	SAML連携で**サービス提供側（SP）を一意に識別するためのID**。通常はSPが提供するURL形式の文字列を指定する。
応答URL (Assertion Consumer Service [ACS] URL)	**SAML認証応答を受け取るSP側のエンドポイント**のこと。IdPは、認証が成功した後にSAMLアサーションを含む、SAML認証応答を URL 宛に送信する。
リレー状態（任意）	**IdP 開始のログインフロー**を使用する場合、**認証後のリダイレクト先を指定**し、ユーザーをSPの特定のページへ誘導する。

次のスライドでは、別資料「認証方式とSSOの基礎知識」でご紹介したSAMLの認証フローを再確認します。
認証フローには、IdPスタートとSPスタートの2種類があり、それぞれの流れの中で、本章で整理した各種情報がどの場面で利用されるかを併せて記載しています。
後段のSAML認証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。

2.3. SAML認証フローの再確認

SP起点

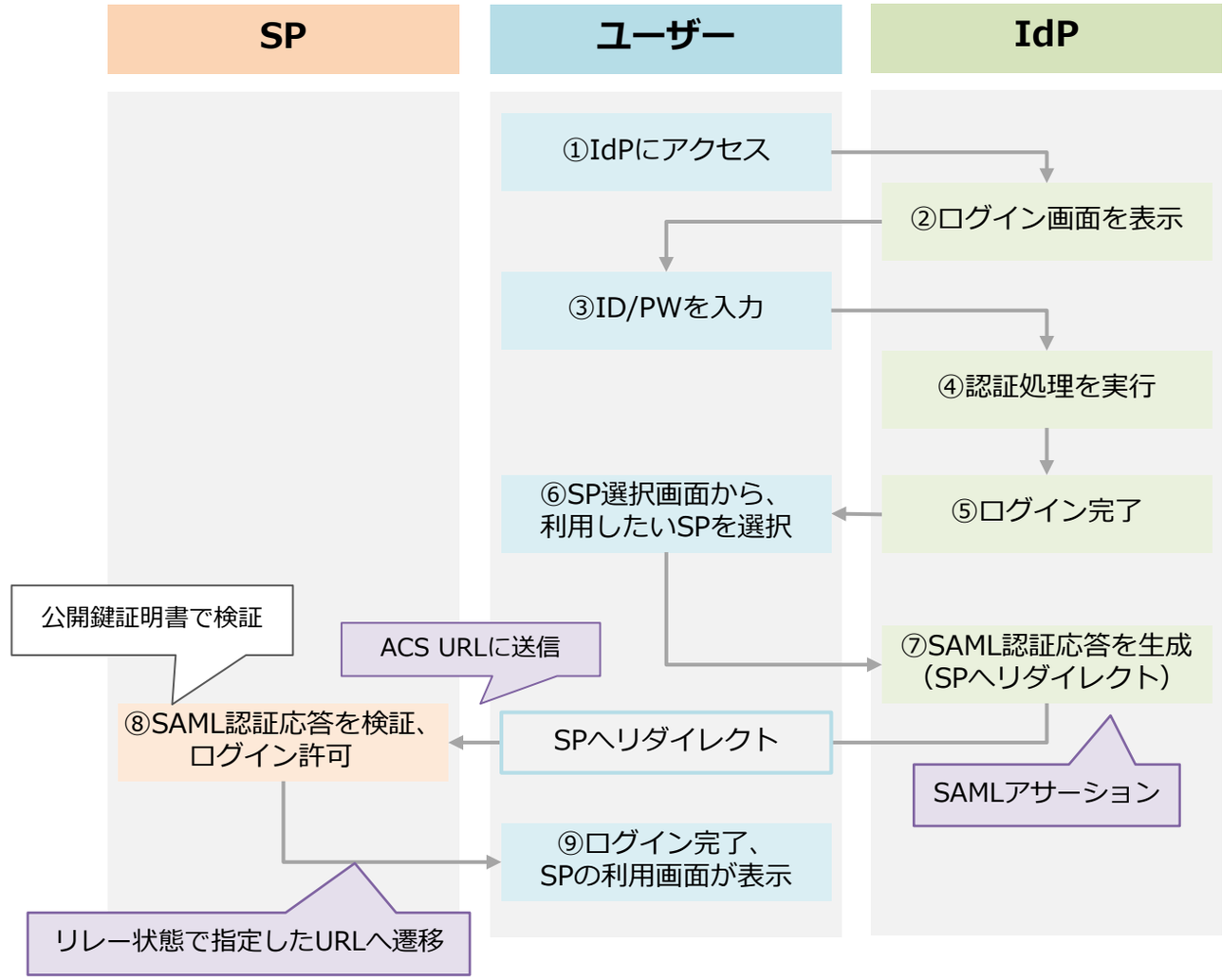
1. ユーザーがWebブラウザから、**SPのサイトにアクセス**する。
2. **SPはSAML認証要求を生成**する。
   ユーザーのブラウザを**IdPへリダイレクト**させ、SAML認証要求をIdPに送信する。
3. IdPはユーザーに**ログイン画面を表示**し、認証情報（IDとパスワードなど）の入力を求める。
4. ユーザーはIdPのログイン画面で**認証情報を入力**する。
5. IdPは入力された情報をもとに**ユーザーの認証を行う**。
6. 認証が成功したら、IdPはSAMLアサーションを含む、**SAML認証応答を生成**する。アサーションにはユーザーの属性情報や認証状態、認可情報、デジタル署名などが含まれる。
   IdPはSAML認証応答を、**ユーザーのブラウザ経由でSPにリダイレクトして送信**する。
7. SPは受け取った**SAML認証応答を検証**し、発行元（IdP）が信頼できるか、有効期限が切れていないか、ユーザー属性が正しいかなどを確認する。
   検証により、アサーションの改ざんを防止し、SAML認証の信頼性を担保している。
8. すべての検証が完了すると、SPはユーザーを認証済みとして扱い、**ユーザーはSPのサービス画面にアクセス**できるようになる。



2.3. SAML認証フローの再確認

IdP起点

1. ユーザーがWebブラウザから**IdPのポータルサイトにアクセス**する。
2. IdP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。
3. ユーザーはIdPのログイン画面で**認証情報を入力**する。
4. IdPは入力された情報をもとに**ユーザーの認証を行う**。
5. 認証に成功すると、**IdPへのログインが完了**する。
6. ユーザーはIdPのポータル上で利用可能なSPの一覧から、**アクセスしたいSPを選択**する。
7. IdPはSAMLアサーションを含む**SAML認証応答を生成**する。
   アサーションには、ユーザーの属性情報、認証状態、認可情報、デジタル署名などが含まれる。
   IdPはSAML認証応答を、**ユーザーのブラウザ経由でSPにリダイレクトして送信**する。
8. SPは受け取った**SAML認証応答を検証**し、発行元（IdP）が信頼できるか、有効期限が切れていないか、ユーザー属性が正しいかなどを確認する。
   検証により、アサーションの改ざんを防止し、SAML認証の信頼性を担保している。
9. すべての検証が完了すると、SPはユーザーを認証済みとして扱い、**ユーザーはSPのサービス画面にアクセス**できるようになる。



3. SAML認証 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SAML認証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。
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、SAML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。

0. 前提条件・事前準備	1. SP プロバイダー設定	2. Entra ID アプリの作成	3. Entra ID SAML SSOを設定	4. Entra ID マッピング属性	5. Entra ID メタデータをダウンロード	6. SP メタデータをインポート	7. Entra ID ユーザーのSAMLを有効にする
設定に必要なアカウントの権限確認、事前の情報収集を行います。	SP側でSAML認証を使用するための、IDプロバイダー設定を行います。	Entra IDでSP用のエンタープライズアプリケーションを作成します。	作成したアプリに対して、SAMLベースのSSOを設定します。	SAML認証時にSPへ正しいユーザー情報（emailやUPNなど）を渡すために、必要に応じて属性のマッピングを編集します。	Entra ID側で生成されたSAMLメタデータ（XML形式）をダウンロードします。	ダウンロードしたEntra IDのメタデータをSPにインポートし、SAML連携を確立します。	対象ユーザーに対してSAML認証を有効化し、実際にSSOが機能するようにします。

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。
IdPとSP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. SP プロバイダー設定 → 2. Entra ID アプリの作成 → 3. Entra ID SAML SSOを設定 → 4. Entra ID マッピング属性 → 5. Entra ID メタデータをダウンロード → 6. SP メタデータをインポート → 7. Entra ID ユーザーのSAMLを有効にする

本手順書の前提条件

- 本資料では、Entra ID を IdP、SaaS アプリケーションを SPとした SAML 連携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。
- ユーザーのプロビジョニング設定（例：SCIM等）は含んでいません。認証（SAML SSO）に関する設定のみにフォーカスしています。
- 他のIdPやSP（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SPの両方で管理者権限を持つアカウントが必要です。
Entra ID：グローバル管理者や、クラウド アプリケーション管理者の権限が必要です。
SP：グローバル管理者の権限が必要です。

2. ユーザー属性の確認

Entra IDのユーザーに対して、[email]や[userPrincipalName（UPN）]などの属性が正しく設定されていることを確認します。
特に、SPが期待する属性（例：email）がEntra IDに存在するかを確認します。

3.2. 前提条件・事前準備

事前準備

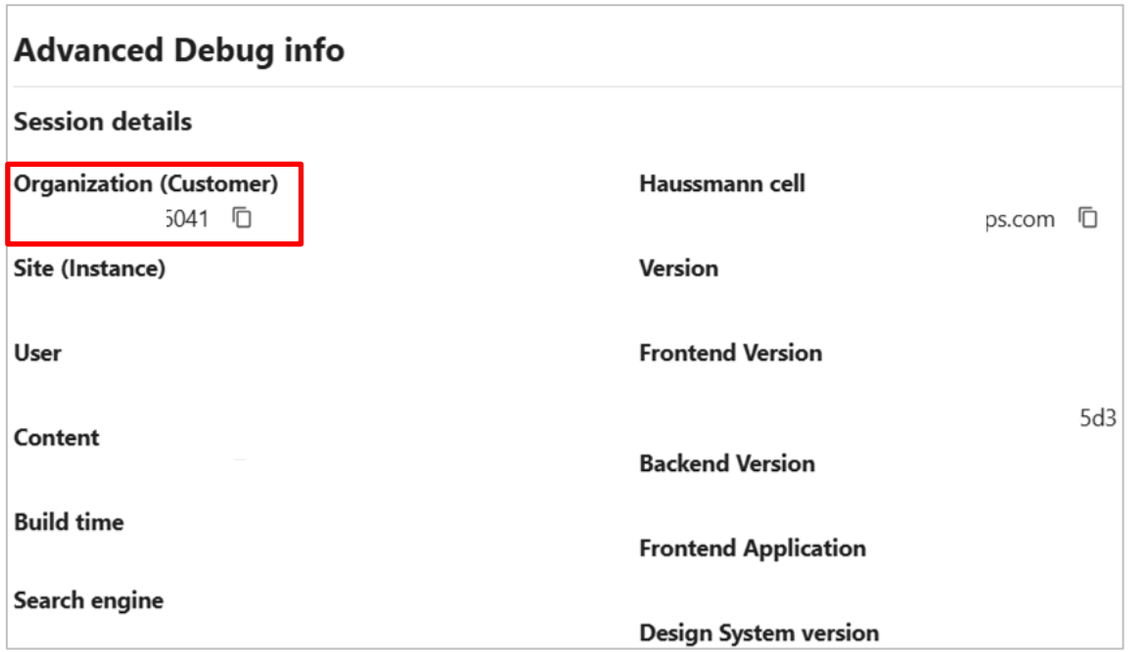
3. テストユーザーの用意

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

4. Customer IDの取得

［3.5. Entra ID SAML SSOを設定］手順4で利用するCustomer IDは、SPの「Advanced Debug info」から取得することが可能です。

※Advanced Debug info：現在使用されているSPのプラットフォームやサイトに関する技術情報が含まれています。



SPで作業

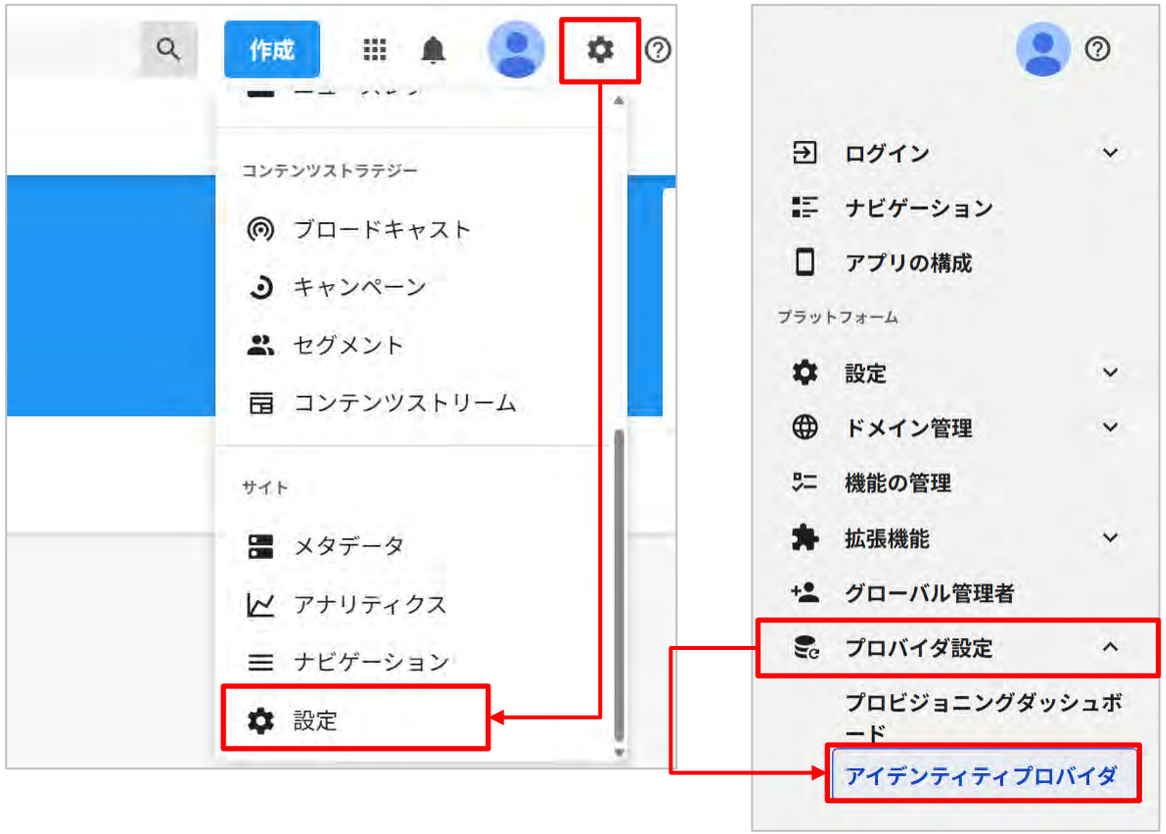
手順

1. SPのグローバル管理者でサイトにアクセスします。
2. キーボードの ［CTRL + SHIFT + ?］を押して、 Advanced Debug info を開きます。
3. ［Organization (Customer)］の値をコピーします。

3.3. 手順1：SP プロバイダー設定

0. 前提条件・事前準備 → 1. SP プロバイダー設定 → 2. Entra ID アプリの作成 → 3. Entra ID SAML SSOを設定 → 4. Entra ID マッピング属性 → 5. Entra ID メタデータをダウンロード → 6. SP メタデータをインポート → 7. Entra ID ユーザーのSAMLを有効にする

SP側でSAML認証を使用するための、IDプロバイダー設定を行います。



手順

SPで作業

1. SP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、「プロバイダー設定」＞「アイデンティティプロバイダ」を選択します。

3.3. 手順1：SP プロバイダー設定

SPで作業

手順

4. 右上の「新規」＞「SAML V2」を選択します。

3.3. 手順1：SP 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。
   これはSPログイン画面のSAMLボタンに表示される名称です。
6. 「ログインを有効化」のオプションを有効にします。
7. 以下設定はオプション設定のため、必要に応じて有効にします。

- 自動ログイン：既にSAMLアカウントにログインしているSPユーザーを自動的に認証する場合に使用します。
  全ユーザーが、設定したプロバイダを使用して強制的にログインが行われます。
- オンザフライのユーザー作成を許可：SAML JIT が有効となり、初めてログインしたときに SAML の情報を使用してアカウントを作成できます。

3.3. 手順1：SP プロバイダー設定

SPで作業

手順

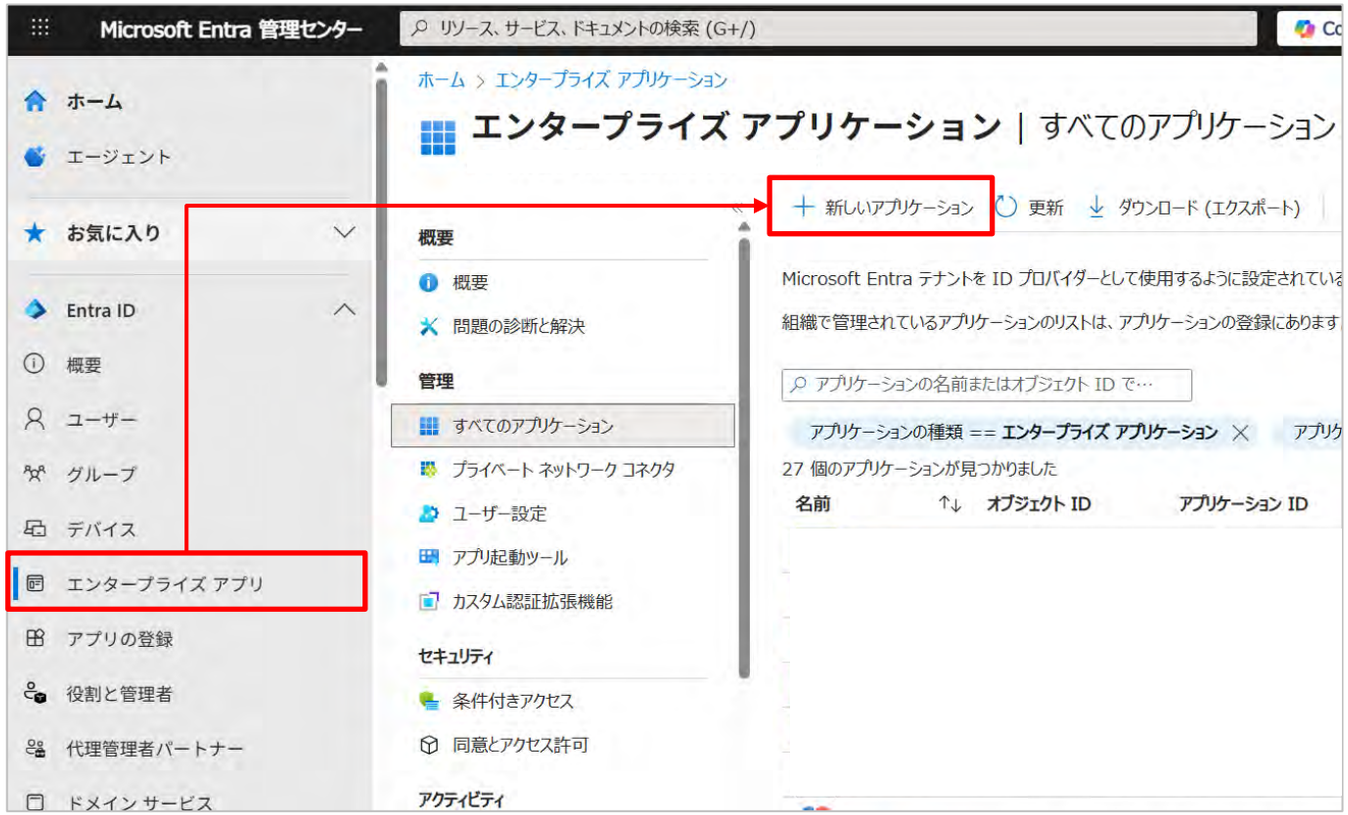
8. 「ログインボタンの可視性」でSAMLのログインボタンを表示する場所を選択します。
   ウェブのみ、モバイルアプリ、ウェブとモバイルアプリの3つの選択肢があります。
9. ログインボタンをカスタマイズします。
10. 「**プロバイダーリファレンス**」をコピーしてメモしておきます。
    この値は、Entra IDの設定時に必要となります。

メタデータのインポートは後続手順「3.8. SP メタデータをインポート」で実施するため、この画面では保存を行わず、そのままの状態で次の手順に進んでください。
※メタデータをインポートせずに画面を保存しても、プロバイダーは作成されません。

3.4. 手順2：Entra ID アプリの作成

0. 前提条件・事前準備 → 1. SP プロバイダー設定 → **2. Entra ID アプリの作成** → 3. Entra ID SAML SSOを設定 → 4. Entra ID マッピング属性 → 5. Entra ID メタデータをダウンロード → 6. SP メタデータをインポート → 7. Entra ID ユーザーのSAMLを有効にする

Entra IDでSP用のエンタープライズアプリケーションを作成します。

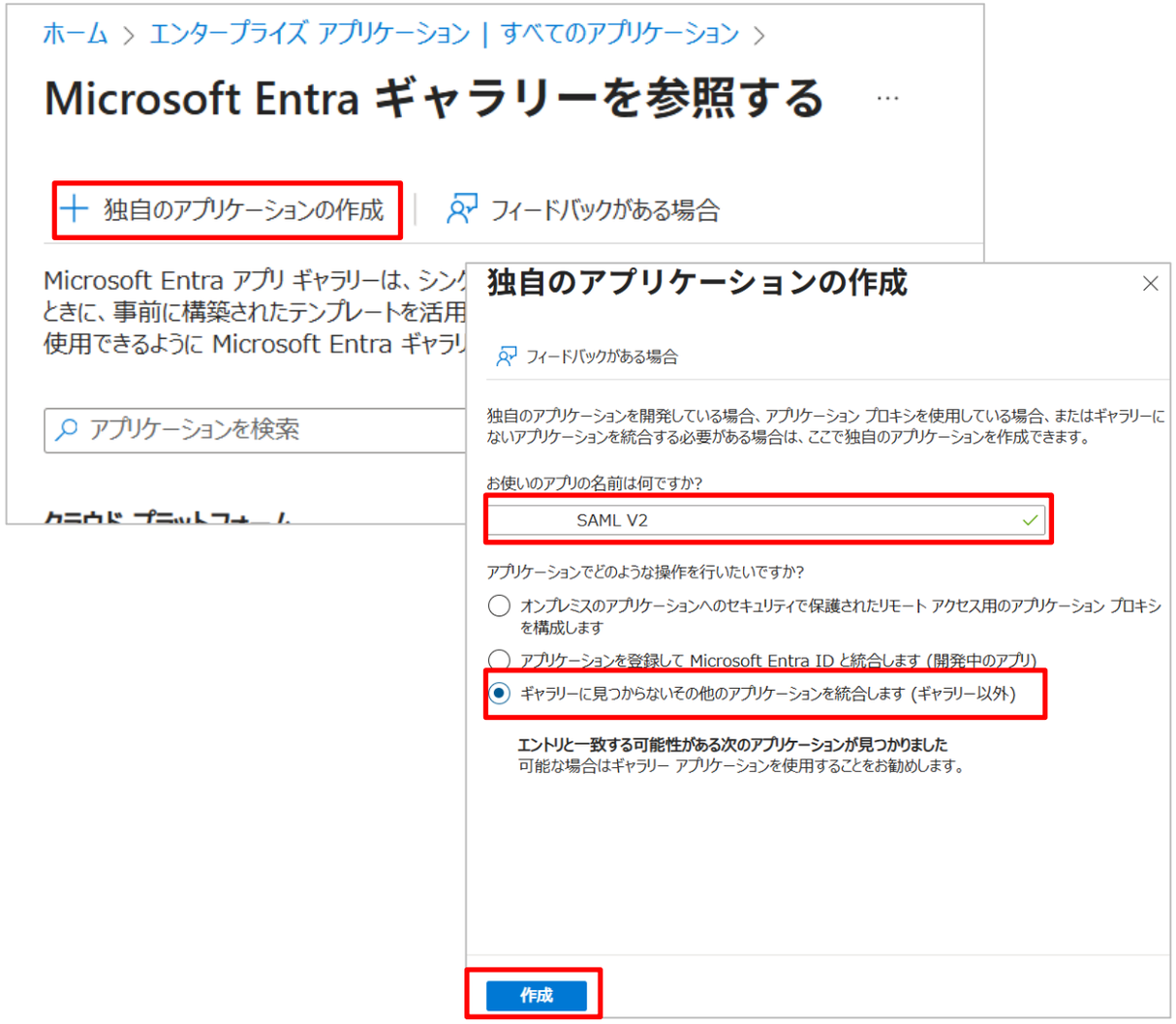


手順

Entra IDで作業

1. Microsoftの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。
2. 左ナビゲーションの「エンタープライズアプリ」を選択します。
3. 「＋新しいアプリケーション」をクリックします。

3.4. 手順2：Entra ID アプリの作成



Entra IDで作業

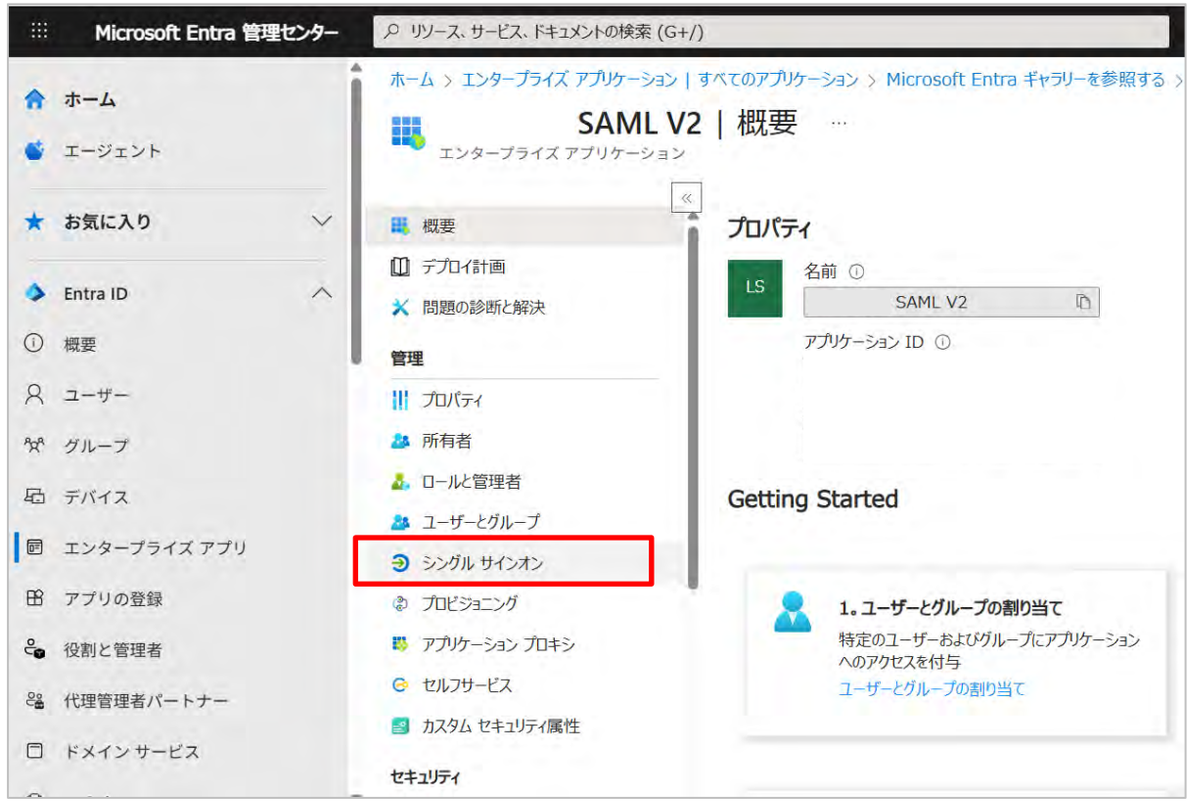
手順

4. 「＋独自のアプリケーションの作成」をクリックします。
5. アプリ名を入力します。これはユーザーがアクセス可能なMicrosoft 365のアプリランチャー名として表示されます。
6. 「ギャラリーに見つからないその他のアプリケーションを統合します（ギャラリー以外）」を選択します。
7. 「作成」をクリックして完了です。

3.5. 手順3：Entra ID SAML SSOを設定

作成したアプリに対して、SAMLベースのSSOを設定します。

Entra IDで作業



手順

1. 前工程で作成したアプリの概要画面を開き、左ナビゲーションから「シングル サインオン」をクリックします。
2. シングル サインオン方式から「SAML」を選択します。

3.5. 手順3：Entra ID SAML SSOを設定

Entra IDで作業

手順

3. 「基本的なSAML構成」の「編集」をクリックします。

3.5. 手順3：Entra ID SAML SSOを設定

Entra IDで作業

手順

4. 「識別子の追加」をクリックし、SPのエンティティIDを追加します。
5. SPから指定された、下記URLを入力します。
   {organization-id}：事前準備で取得したSPのCustomer ID
   {saml-provider-reference}：［SP プロバイダー設定］の手順10で取得したプロバイダーリファレンスの値

```
https://login.[SPサービス名].com/v1/saml2/sp/{organization-id}/{saml-provider-reference}
```

3.5. 手順3：Entra ID SAML SSOを設定

Entra IDで作業

手順

6. 「応答 URLの追加」をクリックし、SAML認証応答を送信するACSURLを追加します。
7. SPから指定された、下記URLを入力します。

```
https://login.[SPサービス名].com/v1/saml2callback
```

3.5. 手順3：Entra ID SAML SSOを設定

Entra IDで作業

手順

8. オプションですが、IdP開始のログインフローの場合「リレー状態」にSPのバニティURL（カスタムドメインが設定されたURL）または、プラットフォームURLを入力します。
9. 「保存」をクリックして完了です。

3.6. 手順4：Entra ID マッピング属性

SAML認証時にSPへ正しいユーザー情報（emailやUPNなど）を渡すために、必要に応じて属性のマッピングを編集します。
多くの場合、Entra ID アプリの SAML 設定では、「属性とクレーム」セクションのデフォルト設定をそのまま使用できます。
ただし、ユーザーの UPNとメールアドレスが異なる場合は、ログインやSAML JITによるユーザー作成が失敗する可能性があるため、
追加の設定が必要です。

手順

Entra IDで作業

1. 前工程で作成したアプリの概要画面を開き、左ナビゲーションから「シングル サインオン」をクリックします。
2. 「属性とクレーム」の「編集」をクリックします。
3. 「一意のユーザー識別子（名前ID）」を選択します。

留意事項

SPとIdP（Entra ID）で参照される属性名やキーとなる識別子は、利用する製品によって異なります。
そのため、SP側でどの属性をキーとして扱っているか（例：NameIDにemailを要求する、またはUPNを期待する など）を確認のうえ、適切にマッピングを調整する必要があります。

3.6. 手順4：Entra ID マッピング属性

Entra IDで作業

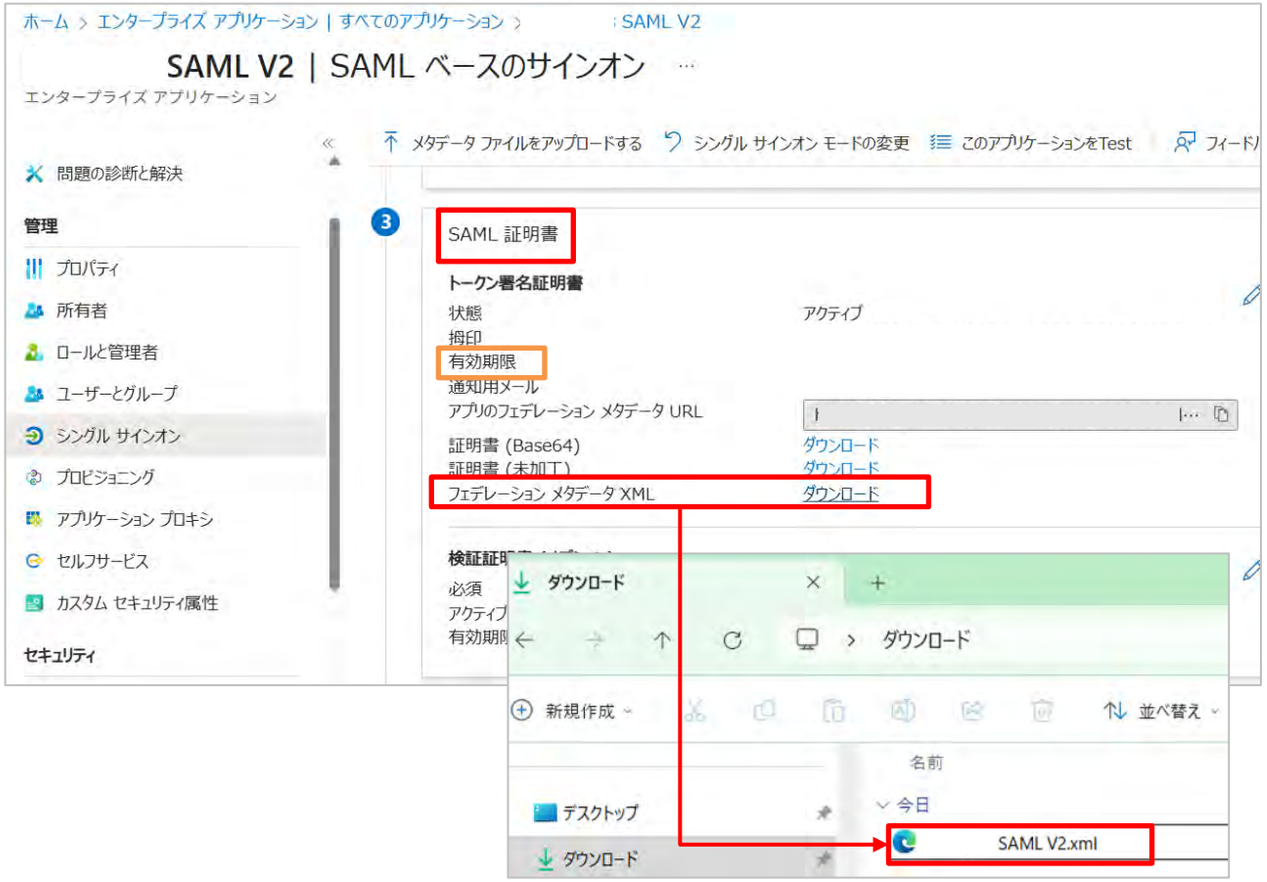
手順

4. 「ソース属性」を［user.mail］に変更します。
5. 「保存」をクリックして完了です。

3.7. 手順5：Entra ID メタデータをダウンロード

Entra ID側で生成されたSAMLメタデータ（XML形式）をダウンロードします。

Entra IDで作業



手順

1. 前工程で作成したアプリの概要画面を開き、左ナビゲーションから「シングル サインオン」をクリックします。
2. 「SAML証明書」の「フェデレーション メタデータ XML」にある「ダウンロード」をクリックします。
3. XMLファイルがPCにダウンロードされたことを確認して完了です。

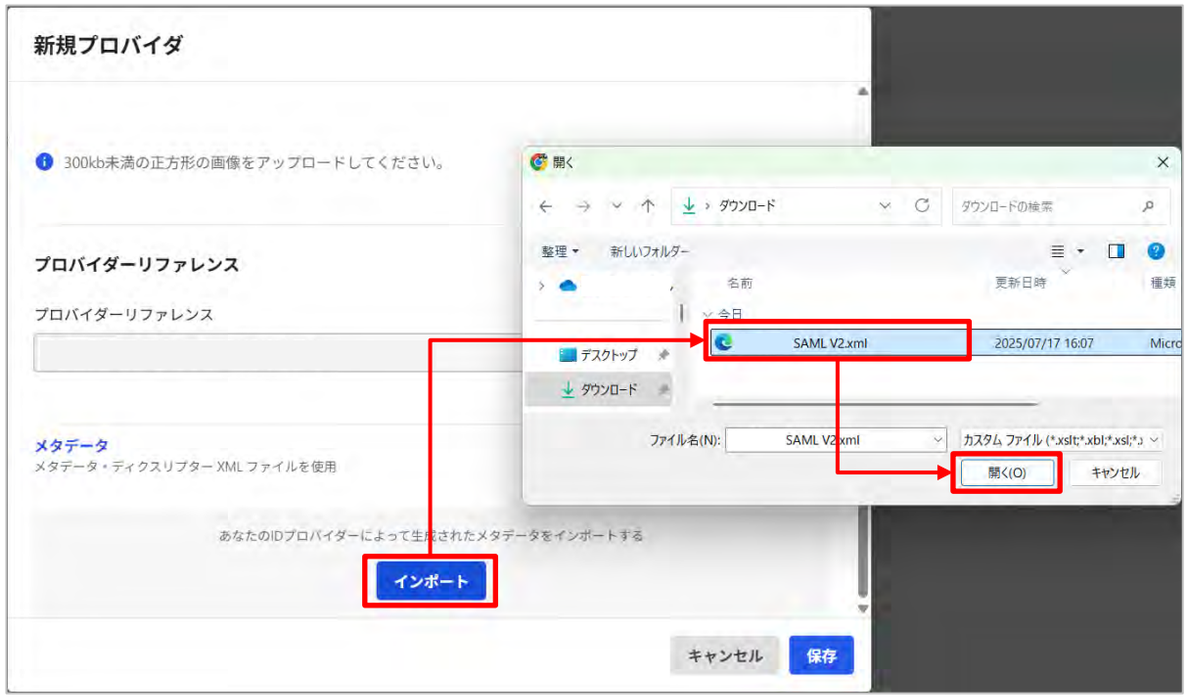
証明書の有効期限

Entra ID のメタデータには証明書が含まれており、デフォルトで有効期限が3年間です。構成時に自動生成され、有効期限の変更はできません。
有効期限が近づくと、60日・30日・7日前に通知メールが送信されます。
SPによってはメタデータを手動でアップロードするため、有効期限前にEntra ID から再取得し、手動で更新する必要があります。

3.8. 手順6：SP メタデータをインポート

ダウンロードしたEntra IDのメタデータをSPにインポートし、SAML連携を確立します。

SPで作業



手順

1. ［3.3. SP プロバイダー設定］のプロバイダ設定画面で、「インポート」から前の手順で取得したメタデータをインポートします。
2. 「保存」をクリックして完了です。

3.9. 手順7：Entra ID ユーザーのSAMLを有効にする

0. 前提条件・事前準備 → 1. SP プロバイダー設定 → 2. Entra ID アプリの作成 → 3. Entra ID SAML SSOを設定 → 4. Entra ID マッピング属性 → 5. Entra ID メタデータをダウンロード → 6. SP メタデータをインポート → **7. Entra ID ユーザーのSAMLを有効にする**

対象ユーザーに対してSAML認証を有効化し、実際にSSOが機能するようにします。

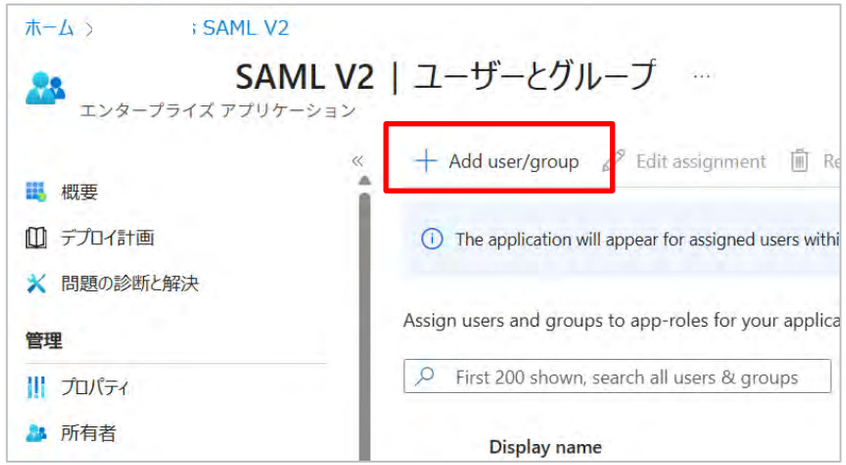
Entra IDで作業

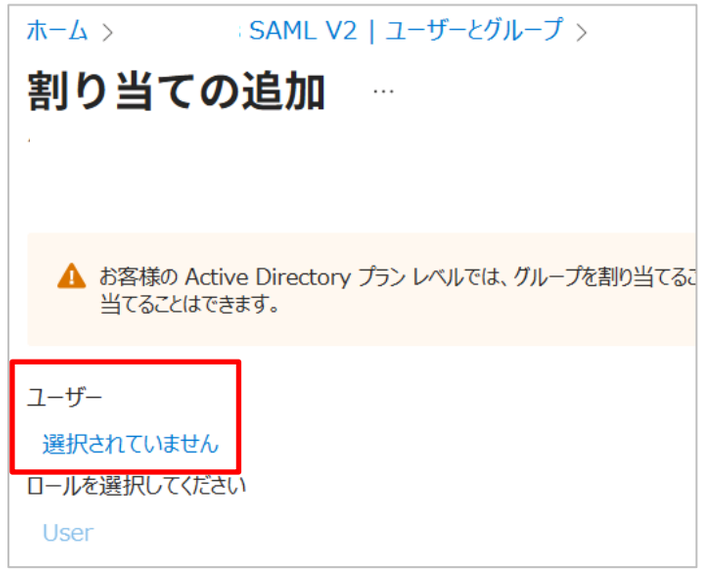
手順

1. 前工程で作成したアプリの概要画面を開き、
   「ユーザーとグループの割り当て」をクリックします。

3.9. 手順7：Entra ID ユーザーのSAMLを有効にする

Entra IDで作業



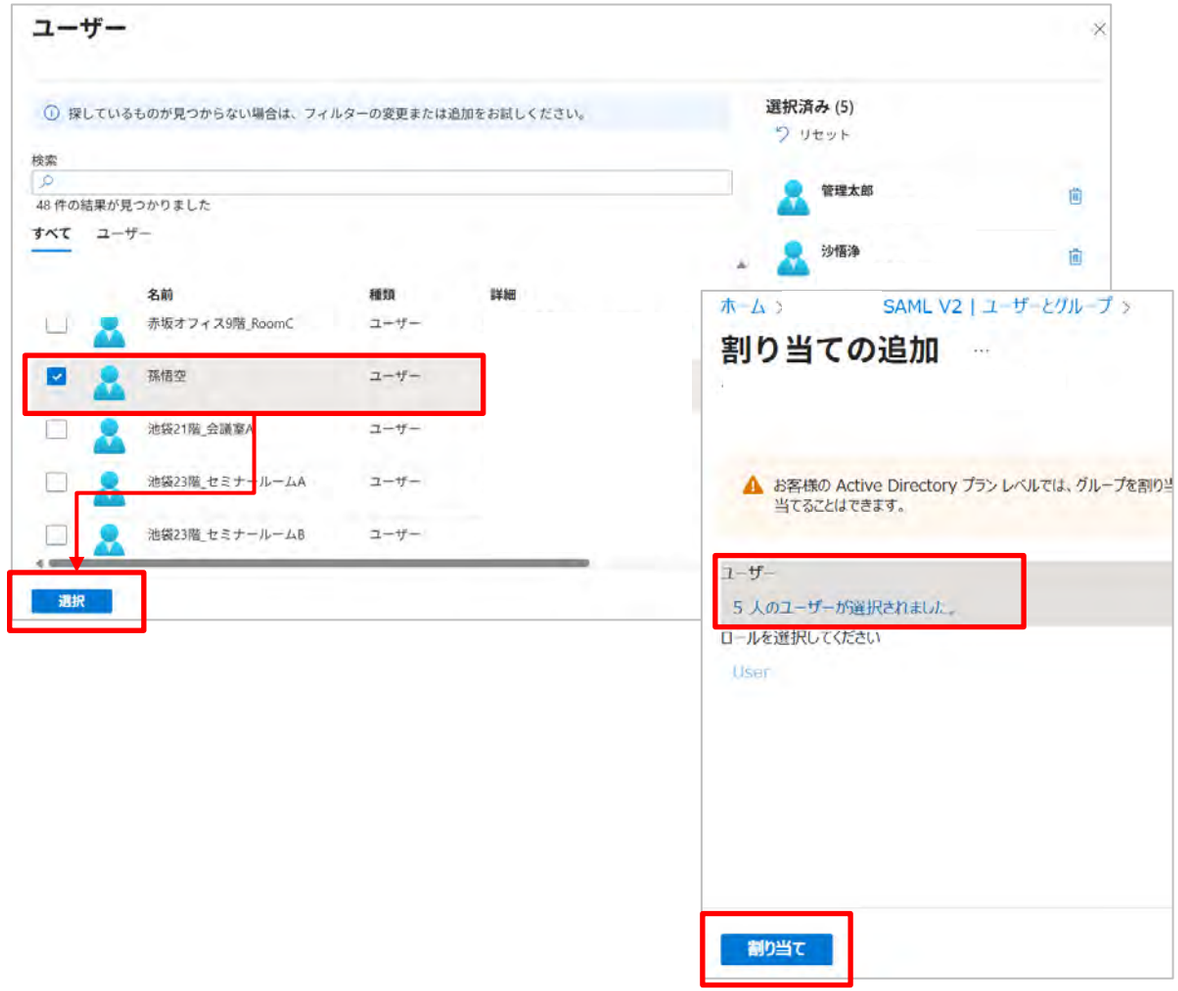


手順

2. 「＋Add user/group」クリックします。
3. ユーザー＞「選択されていません」をクリックします。
   ※Microsoft Entra ID P1/P2ライセンスの場合は、グループ単位の割り当ても可能です。

3.9. 手順7：Entra ID ユーザーのSAMLを有効にする

Entra IDで作業



手順

4. 追加するユーザーまたはグループにチェックを付けて、「選択」をクリックします。
5. ユーザーまたはグループが選択されたら、「割り当て」をクリックして完了です。

これでSAML認証の設定はすべて完了です。

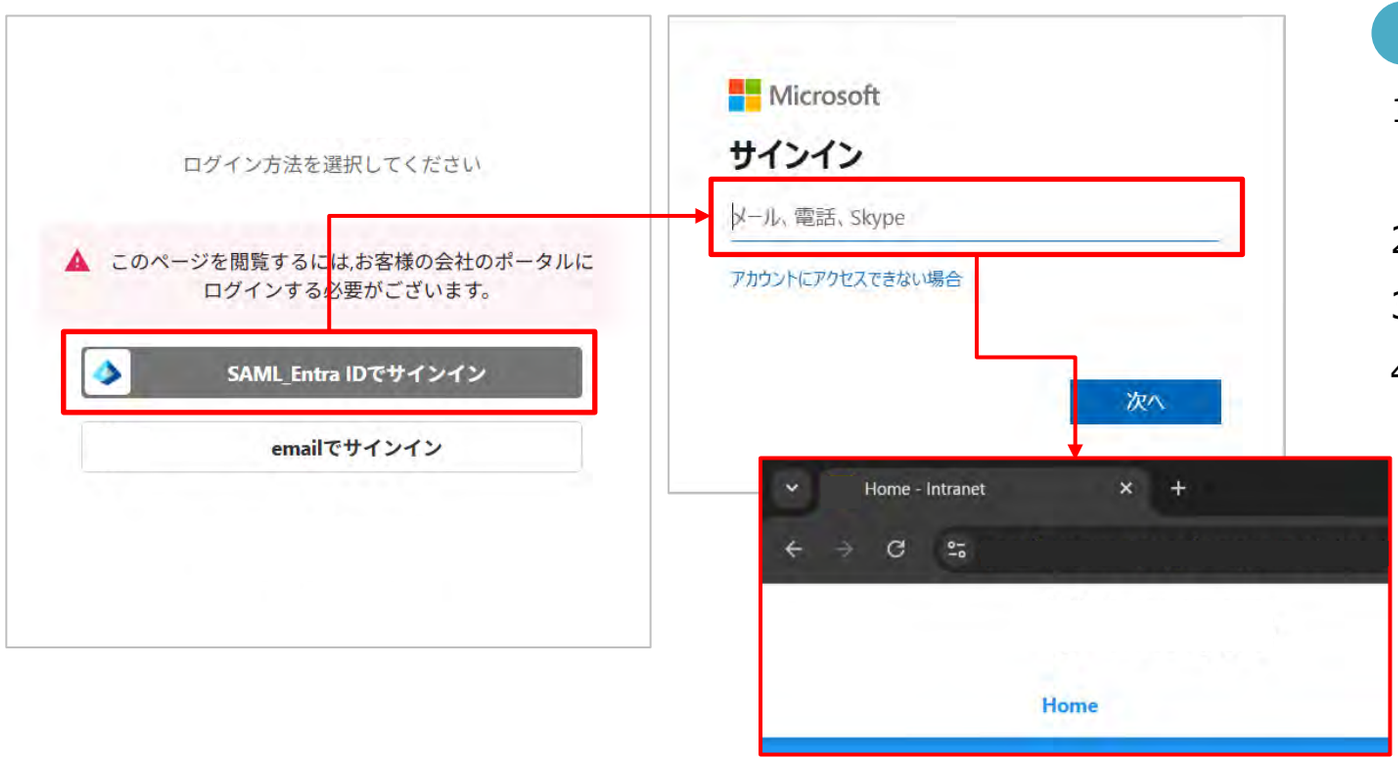
最後にログインの動作確認を行います。

3.10. 動作確認

SAML連携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、IdP起点・SP起点の両パターンで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。

SP起点

このスライドでは、SP起点（SPログインスタート）での、SAML認証によるSPへのログイン動作を確認する手順を説明します。



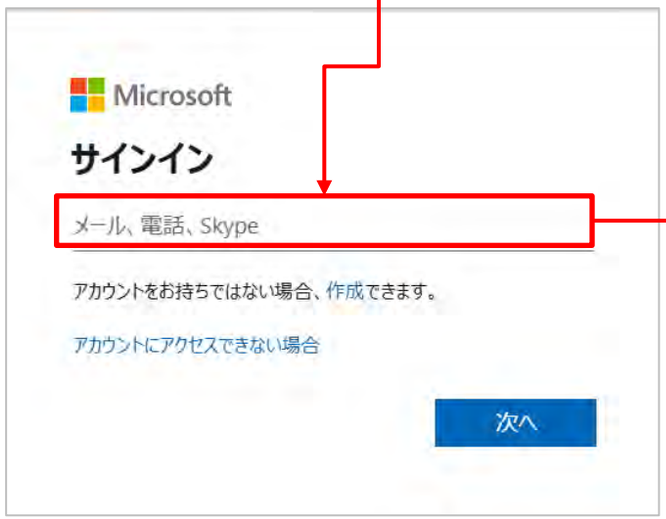
手順

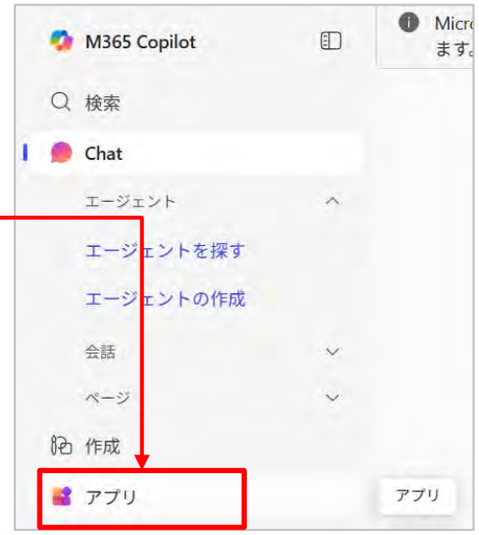
1. シークレットモードのブラウザで、ログインを行うSPのサイトにアクセスをします。
2. SAMLのログインボタンをクリックします。
3. 組織のMicrosoft 365アカウントでログインを実行します。
4. SPにリダイレクトするため、アクセスできることを確認して完了です。

3.10. 動作確認

IdP起点

このスライドでは、IdP起点（Microsoftログインスタート）での、SAML認証によるSPへのログイン動作を確認する手順を説明します。



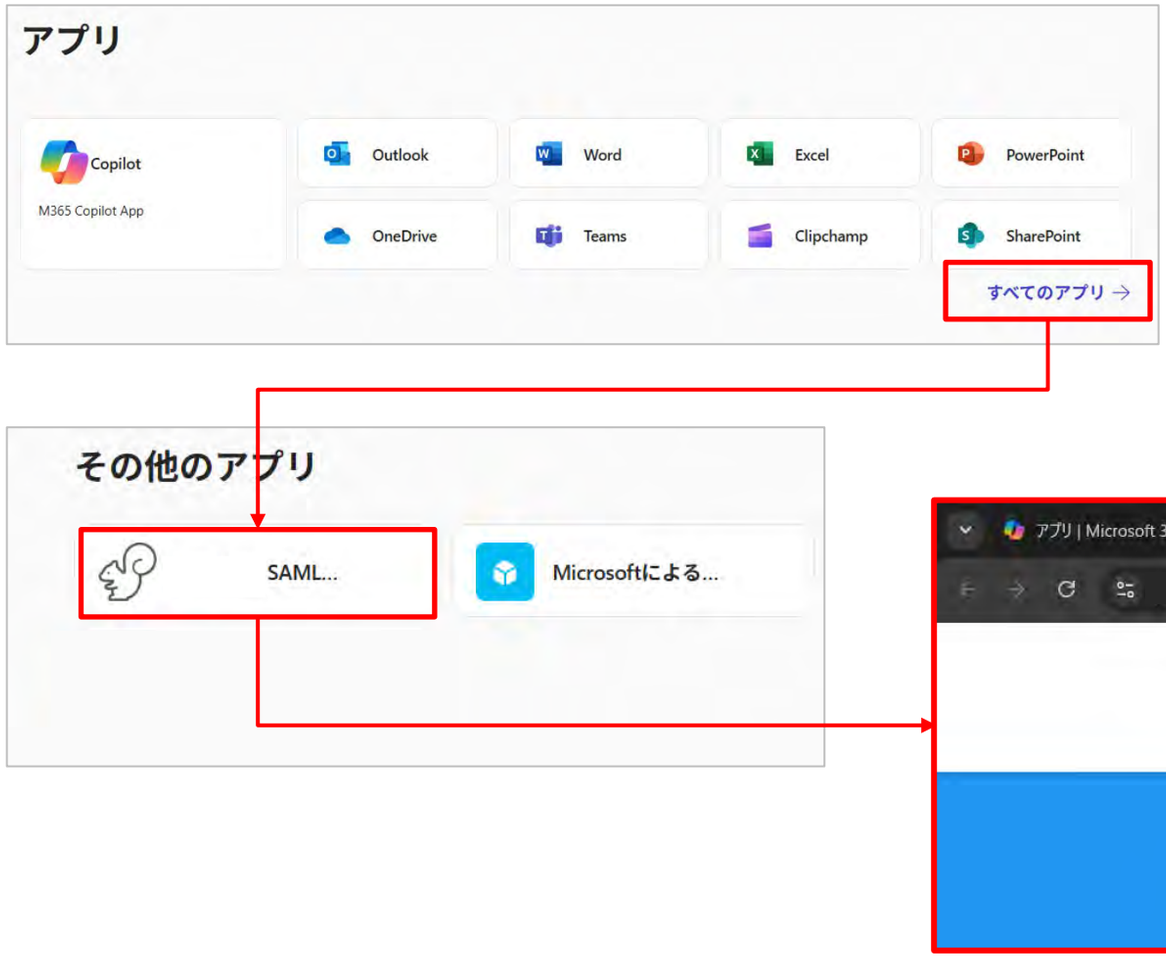


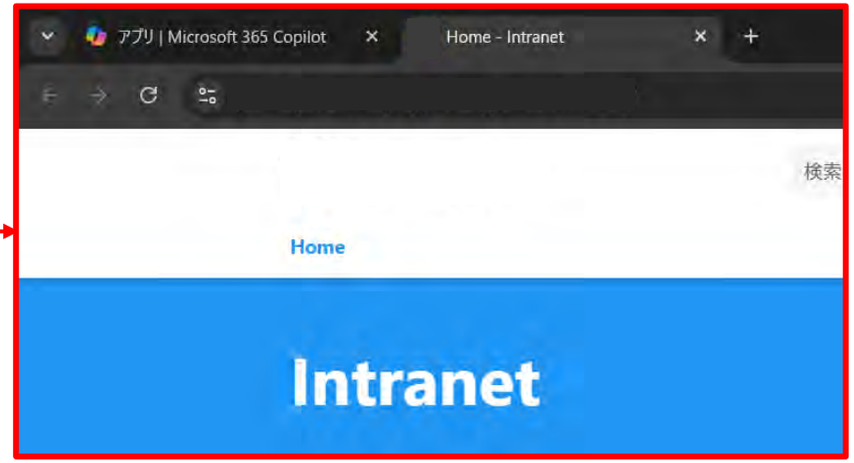
手順

1. シークレットモードのブラウザで［https://www.office.com/］に移動し、「サインイン」を選択します。
2. 組織のMicrosoft 365アカウントでサインインを行います。
3. ログインが完了したら、左ナビゲーションの「アプリ」を選択します。

3.10. 動作確認

IdP起点





手順

4. 「すべてのアプリ」をクリックします。
5. Entra IDで作成したアプリをクリックします。
6. SP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。

4. SAMLログイン失敗時のトラブルシューティング

4.1. SAMLログイン失敗時のトラブルシューティング

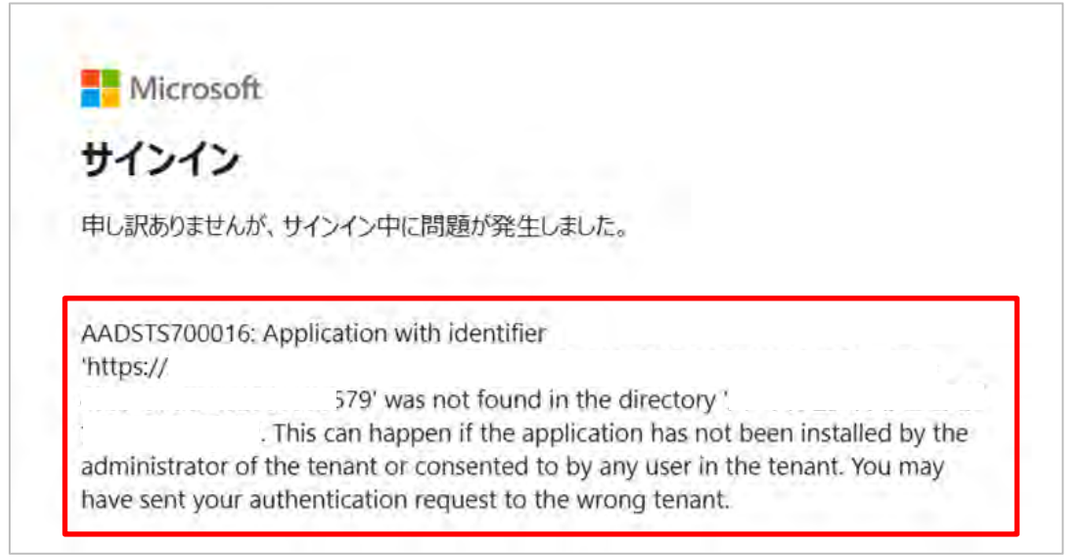
SAML連携によるログインに失敗する場合、設定ミスや属性の不一致など、さまざまな要因が考えられます。
本スライドでは、Entra IDとSP間のSAML認証でログインできない場合に確認すべき主なポイントを整理しています。
トラブル発生時の初動対応としてご活用ください。

確認項目	内容	補足/参考情報
1. 設定内容の再確認	Entra IDの設定値（ACS URL, エンティティ ID など）が正しいか確認	次ページにて詳しく説明します
2. ユーザー・グループの割り当て	Entra IDのエンタープライズアプリに対して、対象のユーザーまたはグループが割り当てられているかを確認	次ページにて詳しく説明します
3. ユーザー属性の確認	SAMLで渡すユーザー情報（UPNやemail）が、Entra IDとSP双方で一致しているかを確認	［3.6. 手順4：Entra ID マッピング属性］を確認します。
4. 証明書の有効期限	有効期限切れ、もしくは不一致がないか	［3.7. 手順5：Entra ID メタデータをダウンロード］で証明書の有効期限を確認します。
5. 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
6. 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。
7. 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	–

4.1.1. 設定内容の再確認

SAML認証でログインに失敗した場合、以下のようなエラーメッセージが表示されることがあります。

それぞれのエラーに対して、確認すべきポイントは以下の通りです。



エラー概要

エラーコード：AADSTS700016

エラーメッセージ概要：指定されたアプリケーション識別子（Identifier）が、
Entra IDのテナントに存在しないため、認証リクエストを処理できません。

原因

・Entra IDに登録されたSPの識別子（エンティティID）が間違っている

・アプリケーションがEntra IDのテナントに登録されていない

対処法

・SP側で指定されたエンティティIDを再確認し、Entra ID で設定した値と一致しているかチェック
（［3.5. 手順3：Entra ID SAML SSOを設定］の手順4を再確認）

・Entra ID 管理画面 ＞「エンタープライズアプリケーション」からアプリが存在するか確認

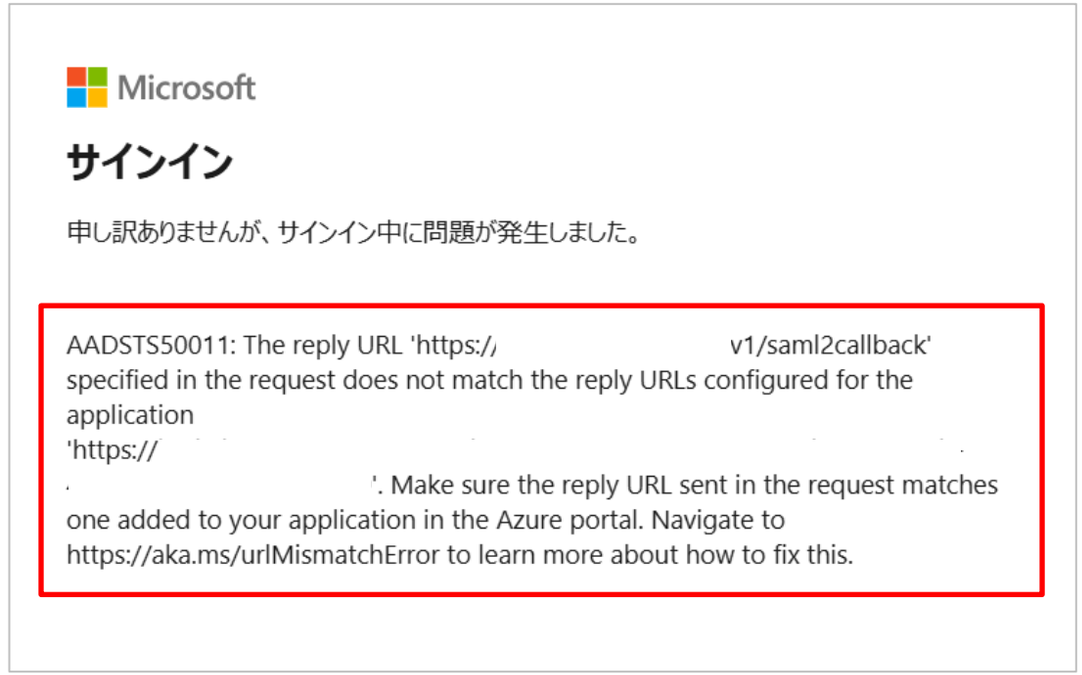
補足

エンティティ ID は、SAML 認証においてEntra IDが認証リクエストの送信元（SP）を識別するための一意の ID です。
Entra ID側の「識別子（Identifier）」として登録されており、SP 側の設定とEntra ID側の設定が完全一致している必要があります。
一致していない場合、Entra IDはそのリクエストを信頼できないものと判断し、認証を拒否します。

4.1.1. 設定内容の再確認

エラー概要

エラーコード：AADSTS50011
エラーメッセージ概要：リクエストに指定された 応答URLが、Entra ID に登録されたアプリケーションの 応答URLと一致しません。



原因

・Entra IDに登録されたアプリケーションの応答URLと、SAML認証要求で、SPから送信されたURLが一致していないため
・末尾のスラッシュ有無 (.../saml2callback vs .../saml2callback/) や、URLのタイプミス

対処法

・SP側で指定された応答URLを再確認し、Entra ID 側の設定と一致しているかチェック
（［3.5. 手順3：Entra ID SAML SSOを設定］の手順6を再確認）

補足

応答URL は、SAML 認証後にEntra IDがレスポンスを返す先のURLです。
SPから送信されるSAML認証要求に含まれる応答URLと、Entra ID 側の設定が完全一致している必要があります。

4.1.1. 設定内容の再確認

エラー概要

SAML認証後に遷移する画面（＝Entra IDのリレー状態に設定されたURL）が、対象の組織と一致していないため、SP側で拒否されています。

原因

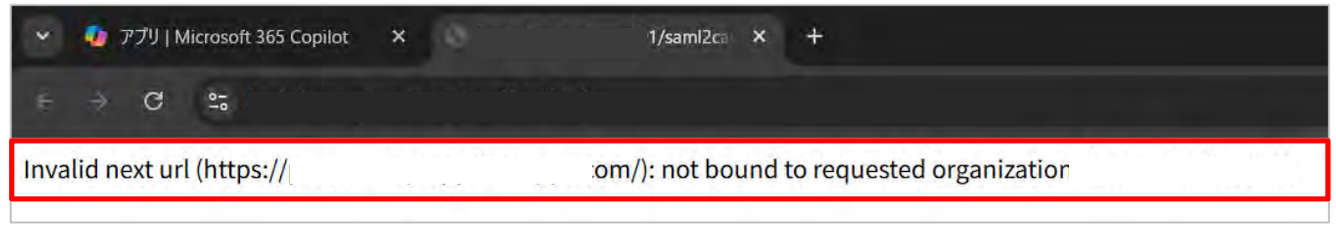
・Entra ID側のSAML構成で、「リレー状態」に誤ったURLを設定していた
・SP（SP）では、組織ごとに許可されたURLが制限されており、他の組織向けのURLが指定されているとエラーになる

対処法

・Entra ID 側で設定した「リレー状態」のURLが正しいかをチェック、SPの組織IDに対応したURLを使用する必要がある
（［3.5. 手順3：Entra ID SAML SSOを設定］の手順8を再確認）

補足

リレー状態は、IdP起点のログインの場合に、SAML 認証後にユーザーを遷移させる URL を指定する仕組みです。
この URL は、認証対象のSP組織に紐づいている必要があり、他の組織の URL を指定するとエラーになります。



4.1.2. ユーザー・グループの割り当て

SAML認証においては、対象ユーザーやグループがEntra ID のアプリケーションに正しく割り当てられていることが必須です。
割り当てがない場合、ユーザーはアプリへのアクセスが拒否され、ログインができません。

エラー概要

エラーコード：AADSTS50105
エラーメッセージ概要：Entra IDのアプリはユーザーへの割り当てが必要と構成されていますが、ユーザーにはアクセス権限が割り当てられていません。

原因

Entra ID管理者が、SP アプリに対して「割り当てられたユーザーのみアクセス可能」という設定をしているため、ユーザーがそのアプリに割り当てられていないことでアクセスが拒否されています。

対処法

・Entra ID管理者がユーザーにアプリのアクセス権を割り当てる　（「3.9. 手順7：Entra ID ユーザーのSAMLを有効にする」の手順を再確認）
・グループ経由で割り当てる場合は、ユーザーがそのグループに所属しているか確認

補足

Entra IDでは、アプリケーションに対して「すべてのユーザーがアクセス可能」または「割り当てられたユーザーのみアクセス可能」の設定ができます。
「割り当てられたユーザーのみ」はセキュリティ強化のための設定ですが、利用者が多い場合はグループ単位での割り当てが推奨されます。