|  |
| --- |
| 第4版  2024/04/18 |

|  |
| --- |
| インストールガイドVer |
| **操作チュートリアル**  **Microsoft Entra ID**  **(旧Azure Active Directory)**  **連携編** |
|  |

目次

[1. 概要 1](#_Toc164341310)

[2. Entra IDを使用したSAML設定手順 1](#_Toc164341311)

[2.1. Entra IDでの設定 2](#_Toc164341312)

[2.1.1. アプリケーションの作成 2](#_Toc164341313)

[2.1.2. ユーザー、グループの割り当て 4](#_Toc164341314)

[2.1.3. Entra IDの設定・情報取得 7](#_Toc164341315)

[2.2. Proselfでの設定 13](#_Toc164341316)

[2.2.1. このサーバー情報の設定 13](#_Toc164341317)

[2.2.2. SAML設定 15](#_Toc164341318)

[2.2.3. SP証明書設定 19](#_Toc164341319)

[2.2.4. IdP証明書自動更新設定 20](#_Toc164341320)

[2.2.5. ユーザー追加 21](#_Toc164341321)

[2.2.6. シングルサインオンのテスト 23](#_Toc164341322)

[3. Entra IDを使用したSAML設定手順(プロビジョニング) 25](#_Toc164341323)

[3.1. Proselfでの設定 25](#_Toc164341324)

[3.1.1. 新規ユーザー登録デフォルト設定 25](#_Toc164341325)

[3.1.2. SCIM連携設定 27](#_Toc164341326)

[3.1.3. 認証トークン発行 30](#_Toc164341327)

[3.2. Entra IDでの設定 33](#_Toc164341328)

[3.2.1. プロビジョニングの開始 39](#_Toc164341329)

[3.2.2. プロビジョニングの即時実行 44](#_Toc164341330)

[3.3. ユーザーの属性連携設定 49](#_Toc164341331)

[4. シングルサインオン 52](#_Toc164341332)

[4.1. Webブラウザからのシングルサインオン 52](#_Toc164341333)

[4.1.1. Entra IDからのシングルサインオン(IdP Initiated) 52](#_Toc164341334)

[4.1.2. Proselfからのシングルサインオン(SP initiated) 53](#_Toc164341335)

[4.2. Proself Clientからのシングルサインオン 55](#_Toc164341336)

# 概要

本チュートリアルは、Microsoft Entra ID(旧Azure Active Directory)を使用したSAML認証を行うための設定方法について説明しています。

* SAML認証を行うにはSAML認証オプションをインストールしている必要があります。
* SAML認証オプションはEnterprise Editionのみ利用可能です。
* 便宜上、以降ではMicrosoft Entra ID をEntra IDと記載しております。

# Entra IDを使用したSAML設定手順

Entra IDを使用したSAML設定手順を記載します。

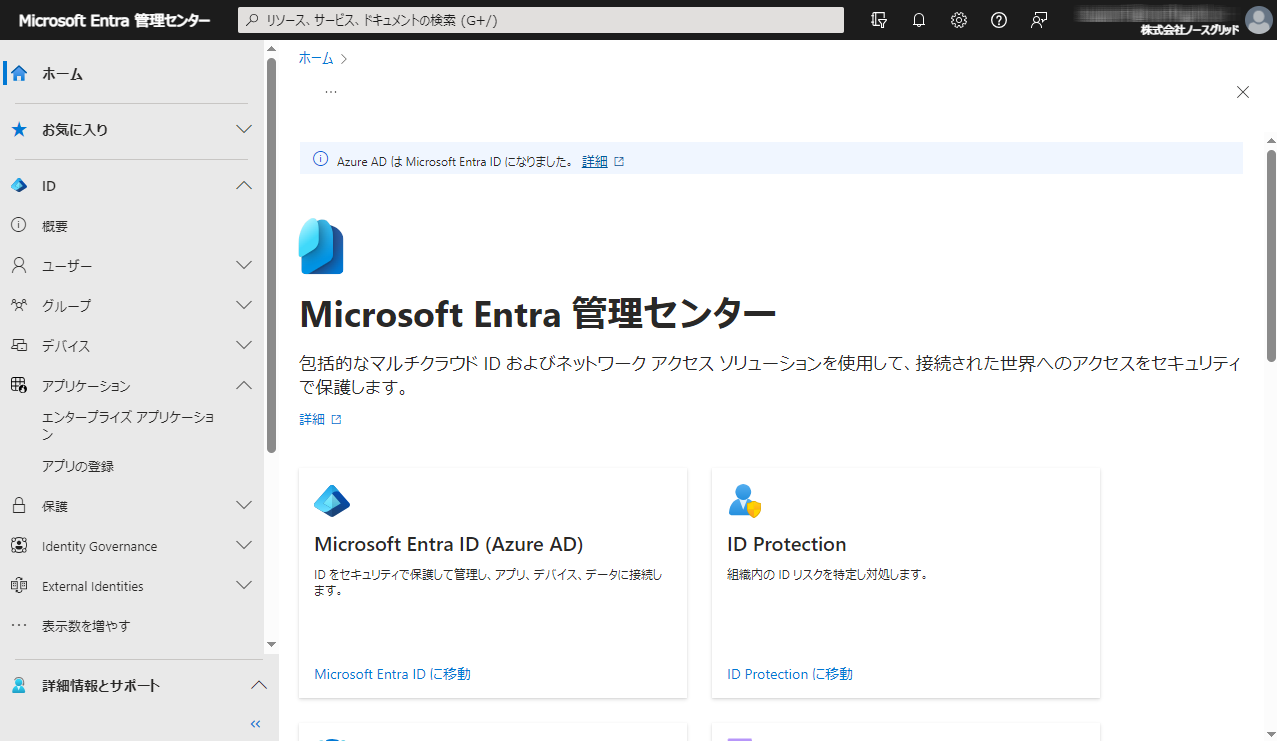
なお、事前にEntra IDにユーザーを登録しておく必要があります。

* 本チュートリアルで使用しているEntra IDの画面ショットは2024年4月時点のものとなっております。将来Entra ID側のインターフェースが変更される等で異なってくる場合がありますため、あらかじめお含みおきください。

## Entra IDでの設定

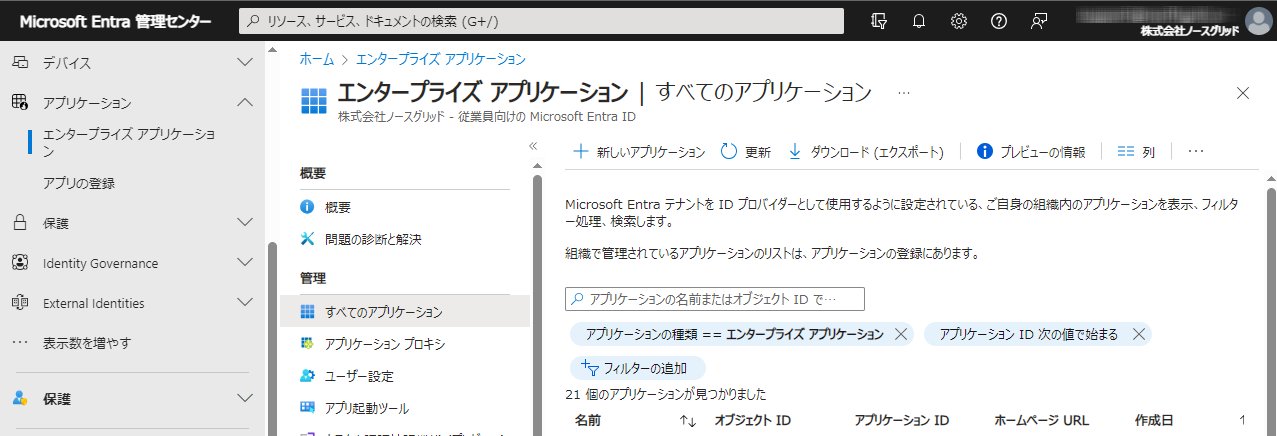
### アプリケーションの作成

Webブラウザで「https://entra.microsoft.com/」にアクセスし、Microsoft Entra IDにログインするとMicrosoft Entra管理センターのホーム画面が表示されますので、左メニューより「ID」>「アプリケーション」>「エンタープライズ アプリケーション」の順でクリックします。



**Microsoft Entra管理センター**

上部メニューより「新しいアプリケーション」をクリックします。



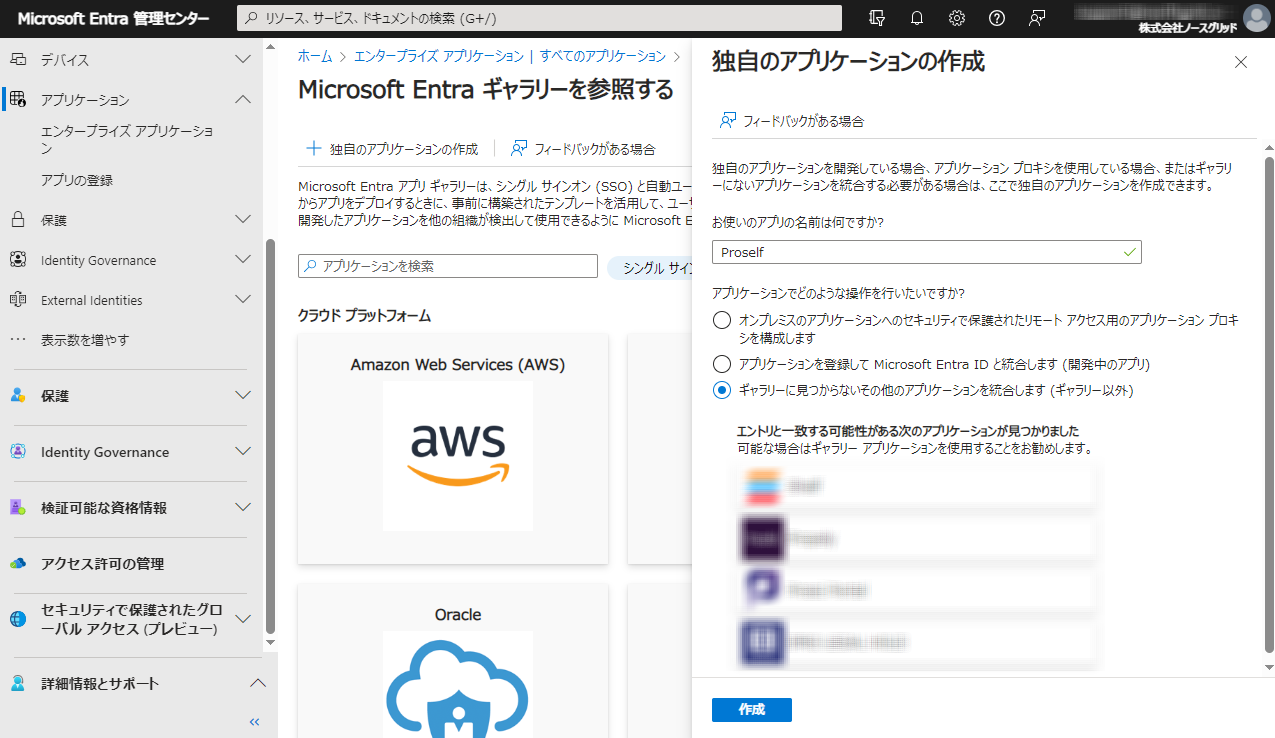
**すべてのアプリケーション**

上部メニューより「独自のアプリケーションの作成」をクリックします。



**Microsoft Entra ギャラリーを参照する**

表示される画面上で任意のアプリケーション名を入力し「作成」をクリックします。本手順では「Proself」という名前で作成します。



**独自のアプリケーションの作成**

### ユーザー、グループの割り当て

「[2.1.1.アプリケーションの作成](#_アプリケーションの作成)」で作成したアプリケーションに対し、ユーザー、グループを割り当てます。

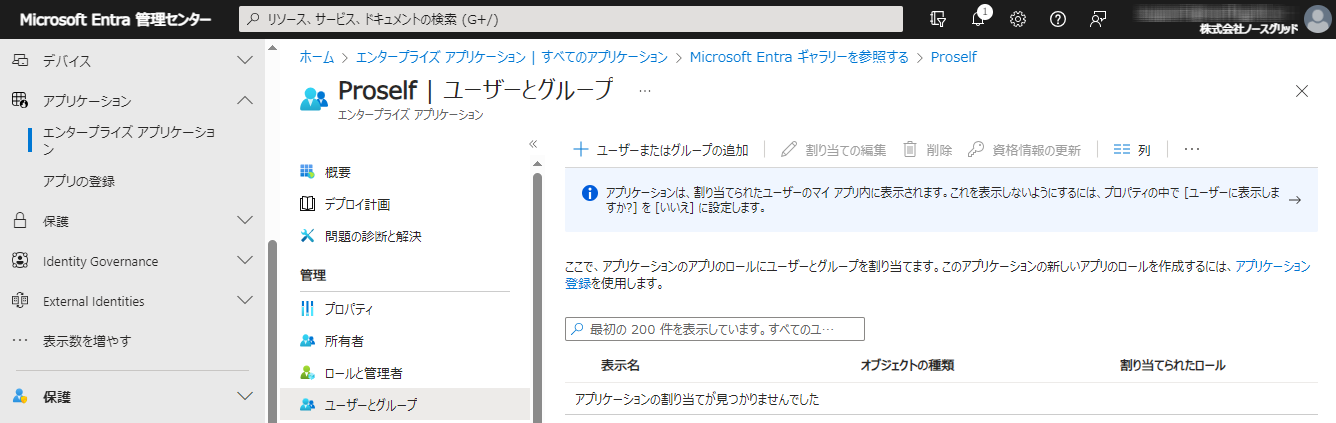
概要画面の「1。ユーザーとグループの割り当て」より「ユーザーとグループの割り当て」をクリックします。



20

**概要-プロパティ**

上部メニューより「ユーザーまたはグループの追加」をクリックします。



20

**ユーザーとグループ**

割り当ての追加画面の「ユーザー」より「選択されていません」をクリックします。



20

**割り当ての追加**

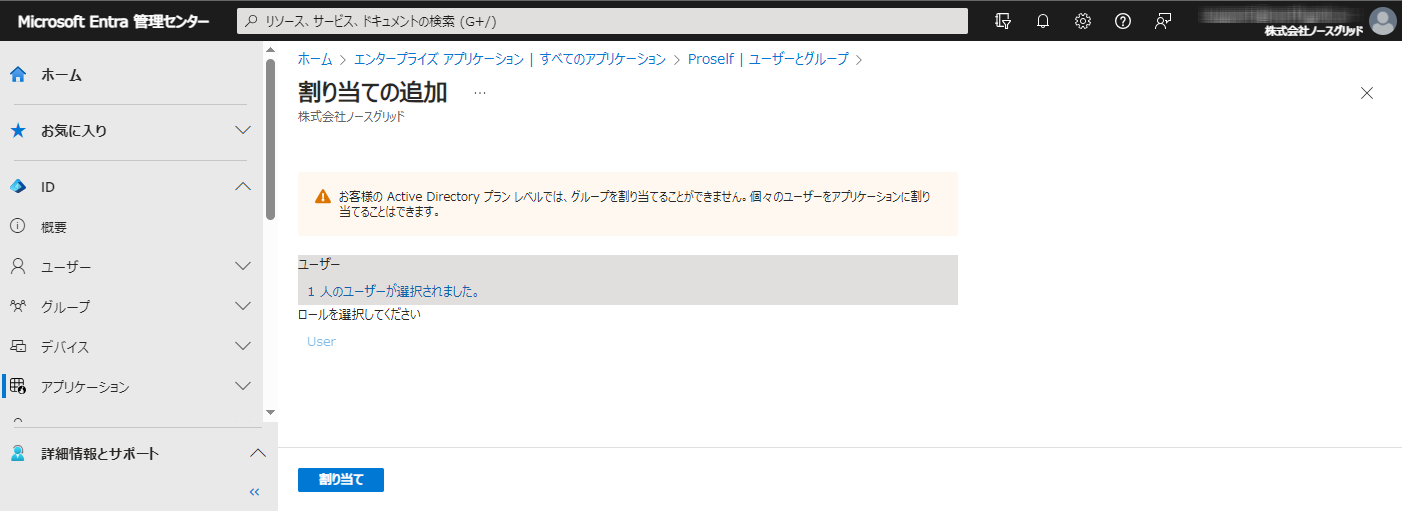
ユーザー、グループのチェックをONにして「選択」をクリックします。



20

**ユーザー**

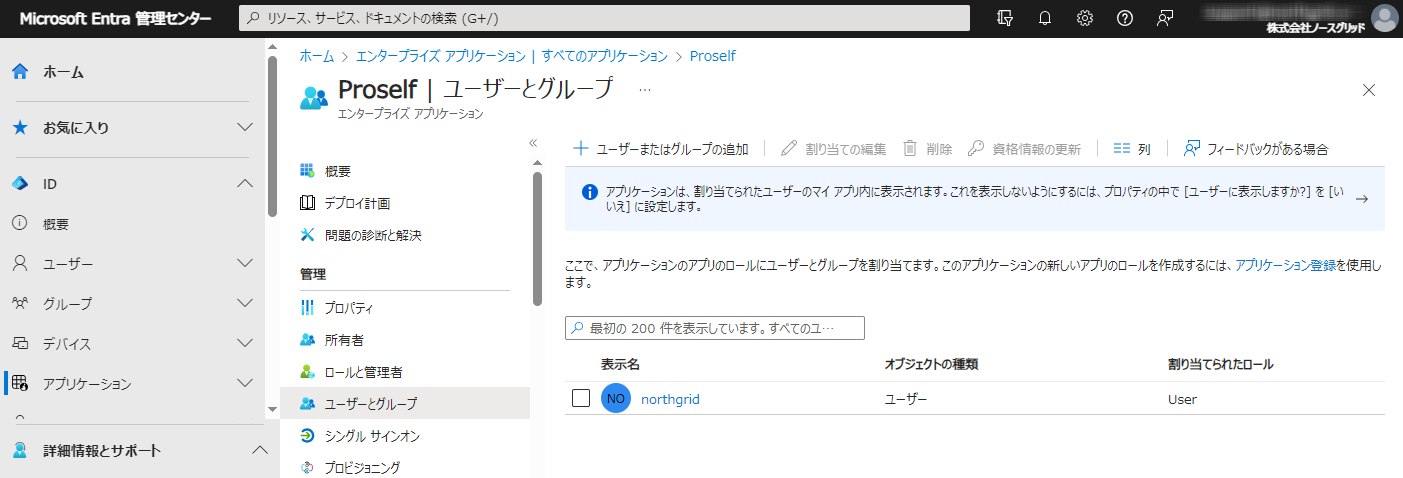
割り当ての追加画面の「ユーザー」に選択されている旨のメッセージが表示されていることを確認し、「割り当て」をクリックします。



20

**割り当ての追加**

作成したアプリケーションにユーザー、グループが割り当てられていることを確認します。



20

**ユーザーとグループ**

### Entra IDの設定・情報取得

概要画面の「2。シングル サインオンの設定」より「作業の開始」をクリックします。



20

**概要-プロパティ**

シングル サインオン方式の選択より「SAML」をクリックします。



**シングル サインオン方式の選択**

「基本的な SAML 構成」より「編集」をクリックします。



20

**SAML によるシングル サインオンのセットアップ**

必須項目である「識別子」、「応答URL」を追加するため、「識別子を追加」、「応答URLの追加」をクリックします。



20

20

**基本的な SAML 構成**

「識別子」、「応答 URL」をそれぞれ設定し「保存」をクリックします。

****

20

20

20

**基本的な SAML 構成**

各項目には以下のように入力します。

| 項目 | 入力内容 |
| --- | --- |
| 識別子 | https://[サーバーアドレス]/proself |
| 応答 URL | https://[サーバーアドレス]/proself/login/login.go?AD=init&sso=true |

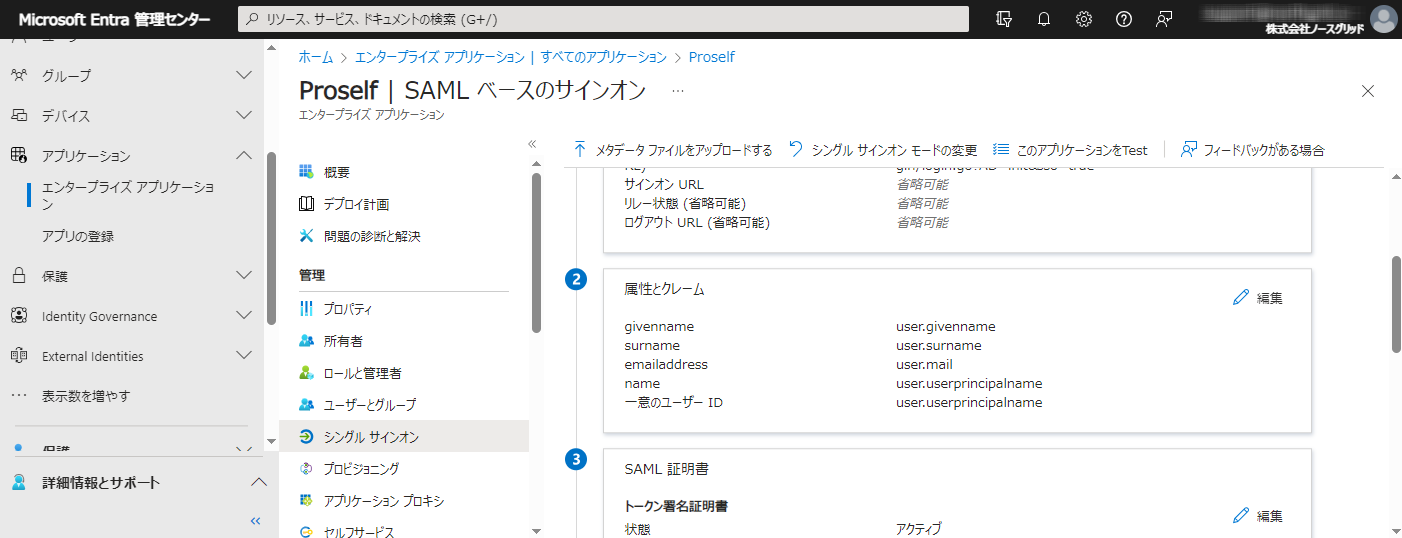
* [サーバーアドレス]には Proself をインストールしたサーバーの IP アドレスまたはFQDN(完全修飾ドメイン名)を入力します。

正常に登録が完了すると「基本的な SAML 構成」に登録した識別子と応答URLが表示されることを確認できます。



**SAML によるシングル サインオンのセットアップ**

次に、「属性とクレーム」より「編集」をクリックします。



20

**SAML によるシングル サインオンのセットアップ**

「属性とクレーム」画面に表示されるクレーム名を控えておきます。控え終わったら画面右上の×をクリックして前の画面に戻ります。

* 控えたクレーム名は「[2.2.2.SAML設定](#_SAML設定)」で使用します。



**属性とクレーム**

なお、デフォルトで表示されているユーザーの属性値と表示名の対応は以下の通りです。

| 属性値 | 表示名 |
| --- | --- |
| user.mail | 電子メール |
| user.givenname | 名 |
| user.userprincipalname | ユーザープリンシパル名 |
| user.surname | 姓 |

* 標準出荷状態では属性値に「@」が含まれていた場合、「@」より前の部分を属性値として認識します。(電子メール、ユーザー名等)

「SAML 証明書」より「フェデレーション メタデータ XML」の「ダウンロード」をクリックしてXMLファイルをダウンロードします。ダウンロードしたXMLファイルは「[2.2.2.SAML設定](#_SAML設定)」で使用します。

また、「[2.2.4.IdP証明書自動更新設定](#_IdP証明書自動更新設定)」で使用するため、「アプリのフェデレーション メタデータ URL」の右側に表示されるURLを控えておきます。

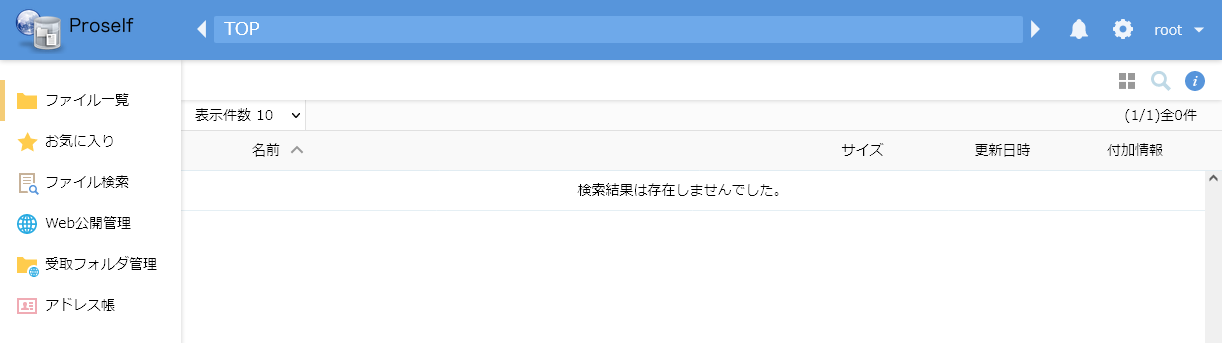


**SAML によるシングル サインオンのセットアップ**

## Proselfでの設定

### このサーバー情報の設定

管理者ユーザーでProselfにログイン後、上部メニューの歯車アイコンをクリックします。



20

**ユーザー画面**

管理画面ホームより「システム設定」をクリックします。



**管理画面**

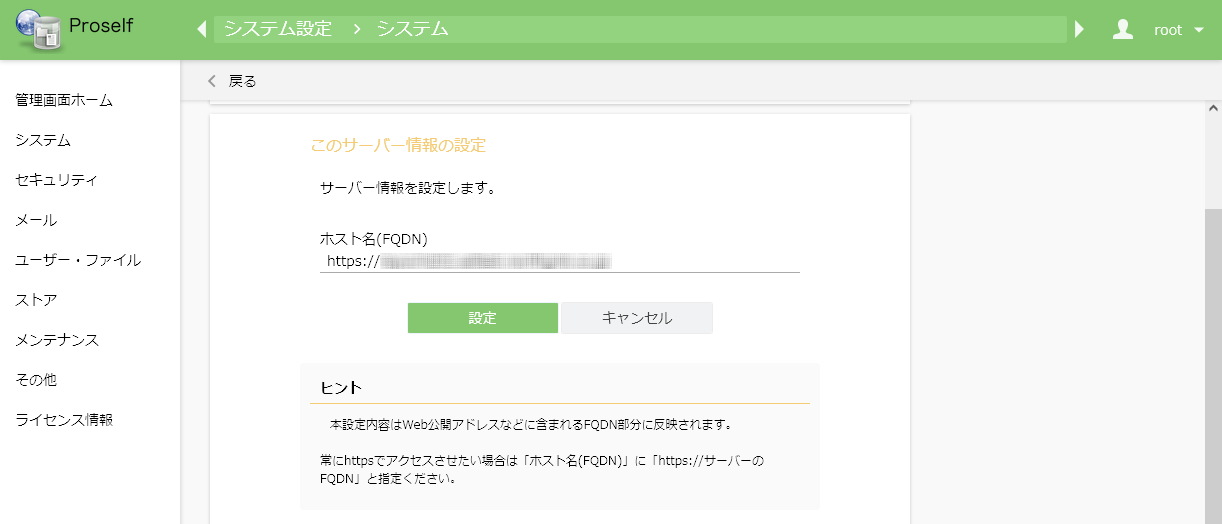
「システム」より「このサーバー情報の設定」をクリックします。



**システム**

「このサーバー情報の設定」の「ホスト名(FQDN)」に「https://[サーバーアドレス]」を入力して「設定」をクリックします。

* [サーバーアドレス]には Proself をインストールしたサーバーの IP アドレスまたはFQDN(完全修飾ドメイン名)を入力します。



**このサーバー情報の設定**

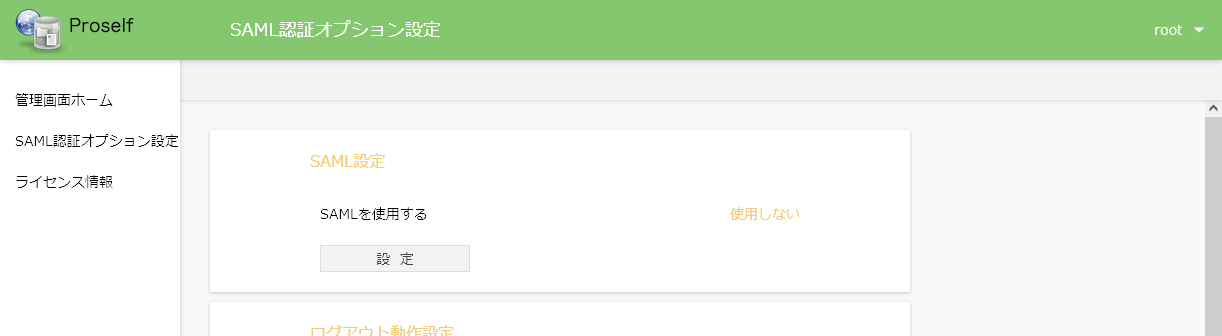
### SAML設定

管理画面ホームより「SAML 設定」をクリックします。



**管理画面**

「SAML設定」の「設定」をクリックします。



20

**SAML認証オプション設定**

「SAMLを使用する」を「使用する」にします。

IdP Initiatedを有効にする場合は「IdP Initiated SSO」を「on」にします。



20

20

**SAML設定**

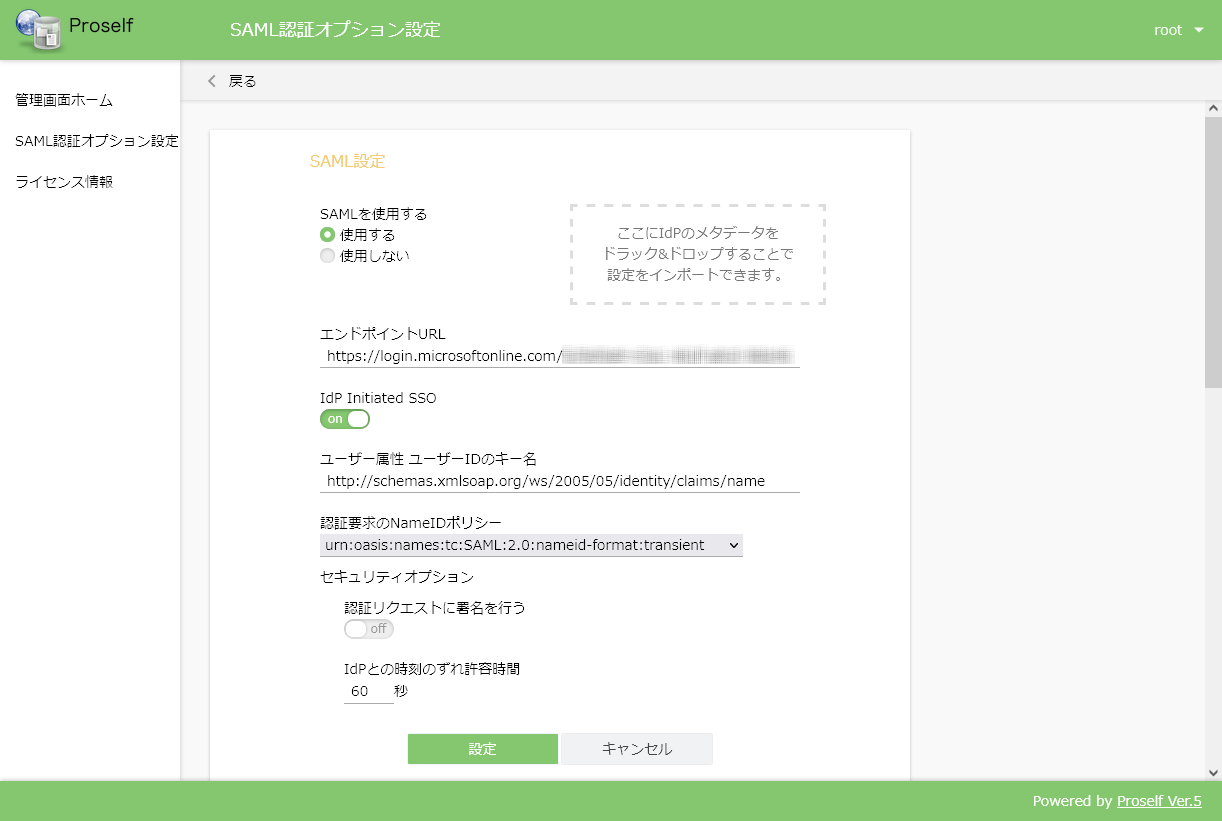
「ここにIdPメタデータを～」の枠内に「[2.1.3. Entra IDの設定・情報取得](#_Azure_ADの設定・情報取得)」でダウンロードした「フェデレーション メタデータ XML」をドラッグ&ドロップします。「エンドポイントURL」やIdP証明書が自動的にインポートされます。



**SAML設定**

「[2.1.3. Entra IDの設定・情報取得](#_Azure_ADの設定・情報取得)」で控えておいたクレーム名を「ユーザー属性 ユーザーIDのキー名」に入力し「設定」ボタンをクリックします。

その後、「戻る」ボタンをクリックして前の画面に戻ります。



**SAML設定**

SAML認証オプション設定画面の「IdP証明書設定」でIdP証明書が自動でインポートされていることを確認します。



**SAML認証オプション設定**

なお、IdP証明書の情報が更新された際に、Proselfが自動的にIdPのメタデータを取得し情報を更新するよう設定することができます。詳細につきましては「[2.2.4.IdP証明書自動更新設定](#_IdP証明書自動更新設定)」をご参照ください。

### SP証明書設定

SP証明書の設定を行います。

詳細につきましては、SAML認証オプションのインストールメディアに同梱しているインストールガイド(InstallGuide.pdf)内「SP証明書設定」の項をご参照ください。

### IdP証明書自動更新設定

IdP証明書の自動更新設定を行います。

SAML認証オプション設定から「IdP証明書設定」の「設定」をクリックします。



**SAML認証オプション設定**

次に「IdP証明書自動更新設定」の「設定」をクリックします。



**SAML認証オプション設定 - IdP証明書設定**

「IdP証明書を自動的に更新する」を「on」、「IdPメタデータ取得URL」に「[2.1.3.Entra IDの設定・情報取得](#_Entra_IDの設定・情報取得)」で控えておいた「アプリのフェデレーション メタデータ URL」を入力して「設定」ボタンをクリックします。



**IdP証明書自動更新設定**

### ユーザー追加

Entra IDで割り当てたユーザーをProselfに追加します。

追加するユーザーIDは「[2.2.2. SAML設定](#_SAML設定)」で指定したクレーム名に対応する属性値と一致するようにします。



**ユーザー一覧**

以下に指定したクレーム名に対応するユーザーIDの設定例を記載します。

| ユーザー属性 ユーザーIDのキー名 | ユーザーID |
| --- | --- |
| user.mailのクレーム名 | Entra IDのユーザーの電子メール(@より前) |
| user.givennameのクレーム名 | Entra IDのユーザーの名 |
| user.userprincipalnameのクレーム名 | Entra IDのユーザーのユーザープリンシパル名(@より前) |
| user.surnameのクレーム名 | Entra IDのユーザーの性 |

Entra IDに登録している以下ユーザーをProselfに追加する場合の例を記載します。

|  |
| --- |
| 電子メール：northgridmail@example.co.jp  名：north  ユーザープリンシパル名：northgrid@example.com  姓：grid |

* **「ユーザー属性 ユーザーIDのキー名」に「user.mail(電子メール)」のクレーム名を指定した場合**ProselfのユーザーIDは「northgridmail」になります。
* **「ユーザー属性 ユーザーIDのキー名」に「user.givenname(名)」のクレーム名を指定した場合**ProselfのユーザーIDは「north」になります。
* **「ユーザー属性 ユーザーIDのキー名」に「user.userprincipalname(ユーザープリンシパル名)」のクレーム名を指定した場合**ProselfのユーザーIDは「northgrid」になります。
* **「ユーザー属性 ユーザーIDのキー名」に「user.surname(姓)」のクレーム名を指定した場合**ProselfのユーザーIDは「grid」になります。

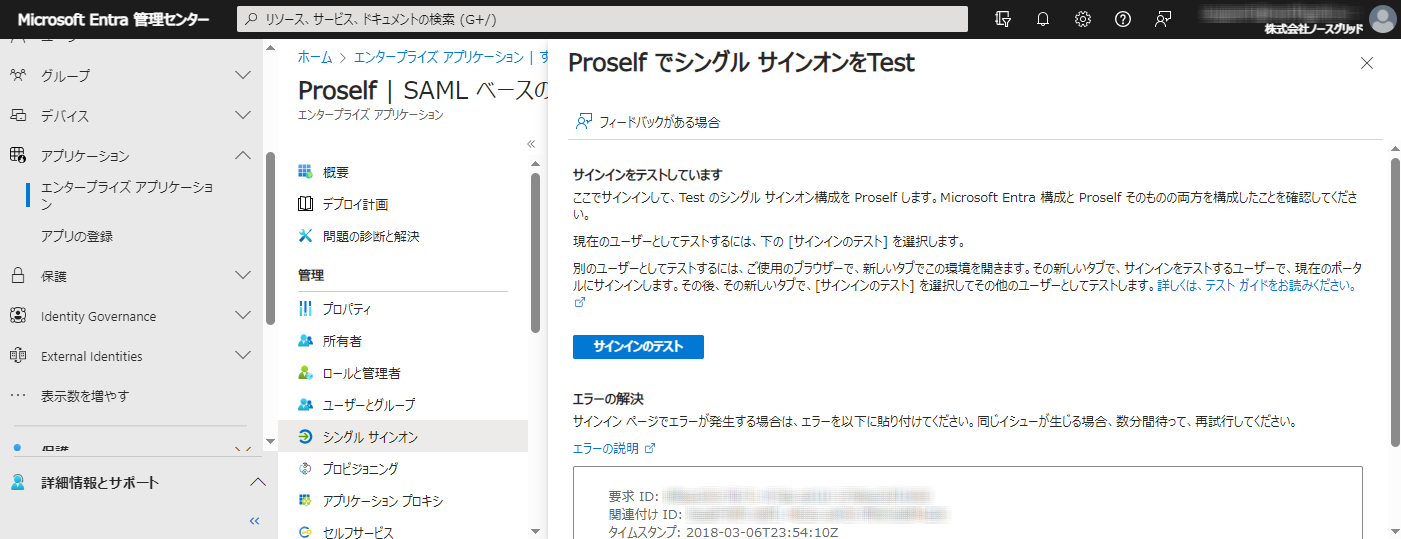
### シングルサインオンのテスト

Entra IDのSAML ベースのサインオン「Proself でシングル サインオンをTest」より「Test」をクリックします。



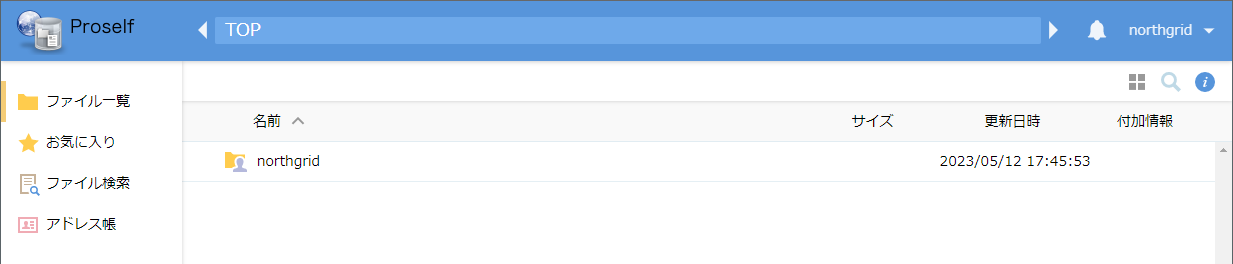
**SAML ベースのサインオン**

「サインインのテスト」をクリックします。



**シングル サインオンをTest**

シングルサインオンに成功してProselfログイン後の画面が表示されることを確認します。

****

**ログイン後の画面(ファイル一覧)**

# Entra IDを使用したSAML設定手順(プロビジョニング)

Proself Ver5.70、SAML認証オプションVer5.70より、Entra IDのプロビジョニング機能を用いてProselfにユーザー、グループ情報の同期が可能となりました。

以下ではその手順を記載しております。

なお、本手順を実施する前に「[2. Entra IDを使用したSAML設定手順](#_Entra_IDを使用したSAML設定手順)」(※)の実施が必要です。

* 「[2.2.5. ユーザー追加](#_ユーザー追加)」、「[2.2.6. シングルサインオンのテスト](#_シングルサインオンのテスト)」を除きます。

## Proselfでの設定

### 新規ユーザー登録デフォルト設定

Entra IDのプロビジョニング機能により作成されるユーザーに対するデフォルト設定を行います。

デフォルト設定は事前に作成した専用の管理者ユーザーで行うことをおすすめいたします。

専用の管理者ユーザーにてProselfにログイン後、管理画面ホームより「ユーザー管理」をクリックします。



**管理画面**

新規ユーザー登録デフォルト設定画面で各項目の設定を行った上で画面上部の「設定」をクリックします。

* 標準出荷状態ではデフォルト設定情報が登録されていないため、何も設定しない場合でも必ず「設定」をクリックしてください。



**新規ユーザー登録デフォルト設定**

### SCIM連携設定

SCIM連携設定を行います。

管理画面ホームより「SAML 設定」をクリックします。



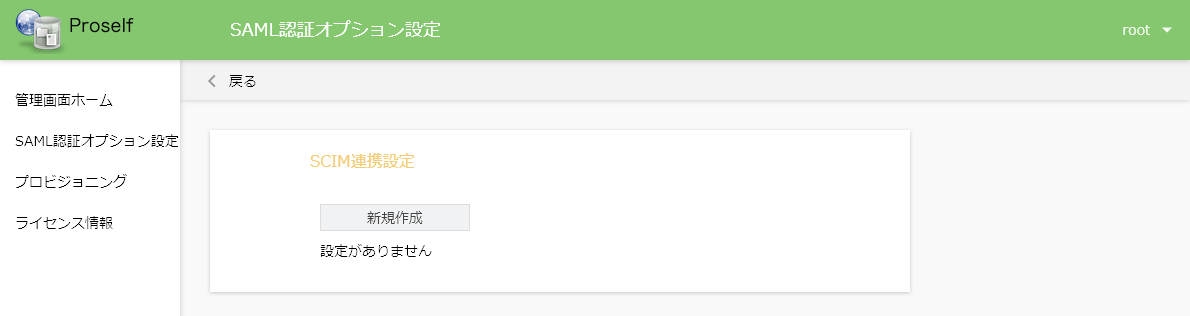
**管理画面**

プロビジョニングをクリックします。



**SAML認証オプション設定**

SCIM連携設定より「新規作成」をクリックします。



**SAML認証オプション設定**

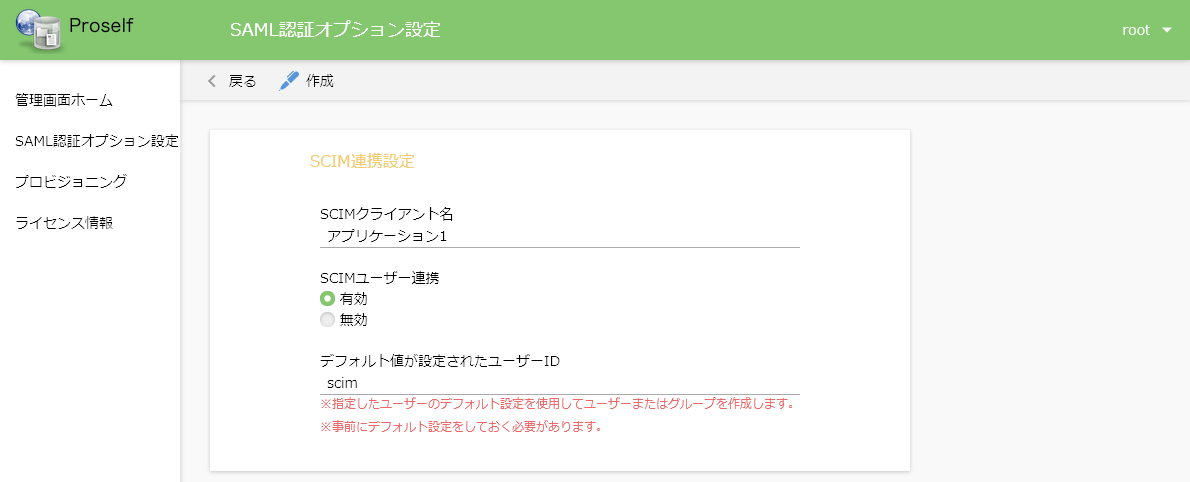
さらに、SCIM連携設定より「設定」をクリックします。



**SAML認証オプション設定**

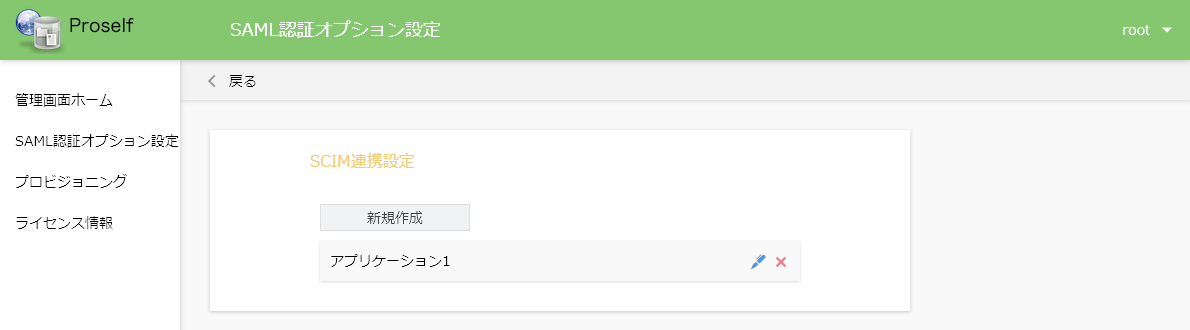
SCIM連携設定画面で各項目を設定します。

SCIMクライアント名、SCMIユーザー連携「有効」、デフォルト値が設定されたユーザーIDには「[3.1.1.新規ユーザー登録デフォルト設定](#_新規ユーザー登録デフォルト設定)」で使用した専用の管理者ユーザーのユーザーIDを設定の上、画面上部の「作成」をクリックします。



**SCIM連携設定**

作成したSCIMクライアント名がリストに表示されます。



**SCIM連携設定**

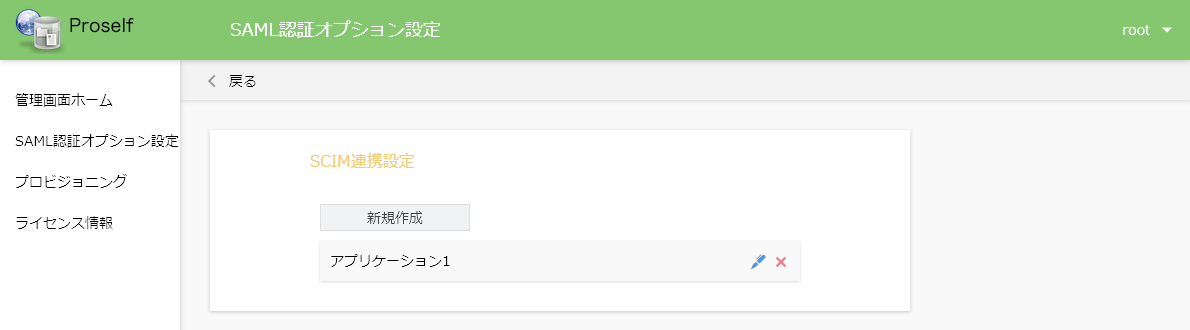
* 設定完了後はユーザー一覧画面に「連携」列が追加されます。



**ユーザー一覧**

### 認証トークン発行

「[3.1.2.SCIM連携設定](#_SCIM連携設定)」で作成済みのSCIMクライアント名か、その右側にあるペン型のアイコンをクリックします。



**SCIM連携設定**

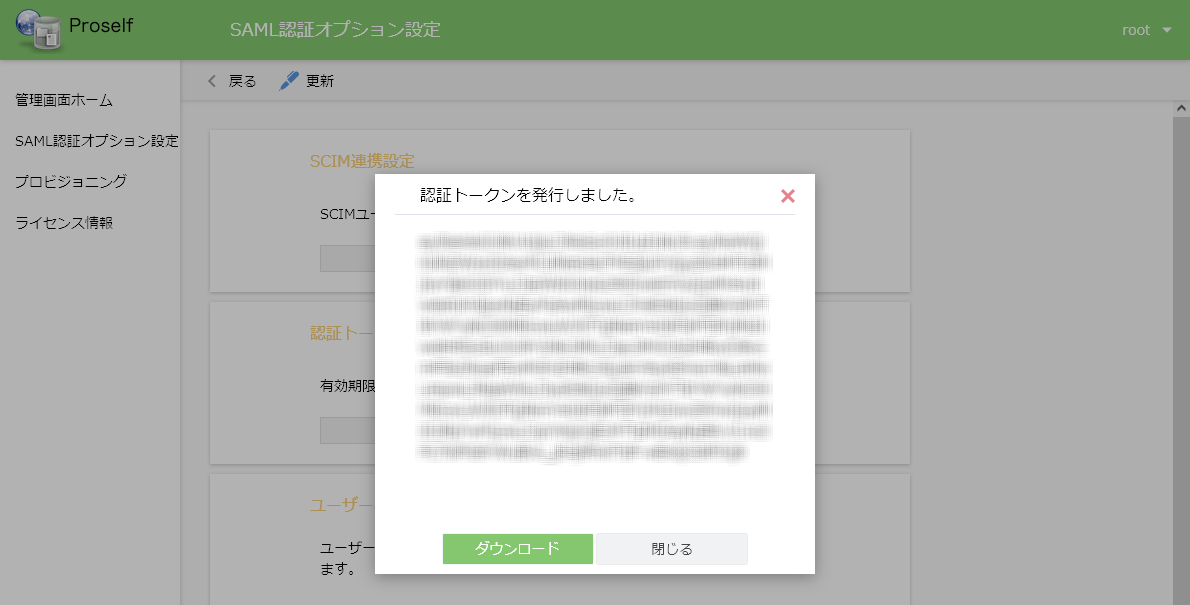
認証トークンより「トークン発行」をクリックします。



**SCIM連携設定**

認証トークンが発行されますので、「ダウンロード」をクリックして保存します。

保存したファイルには画面上に表示された認証トークンが記載されており、この内容を「[3.2.1.プロビジョニングの開始](#_プロビジョニングの開始)」使用します。



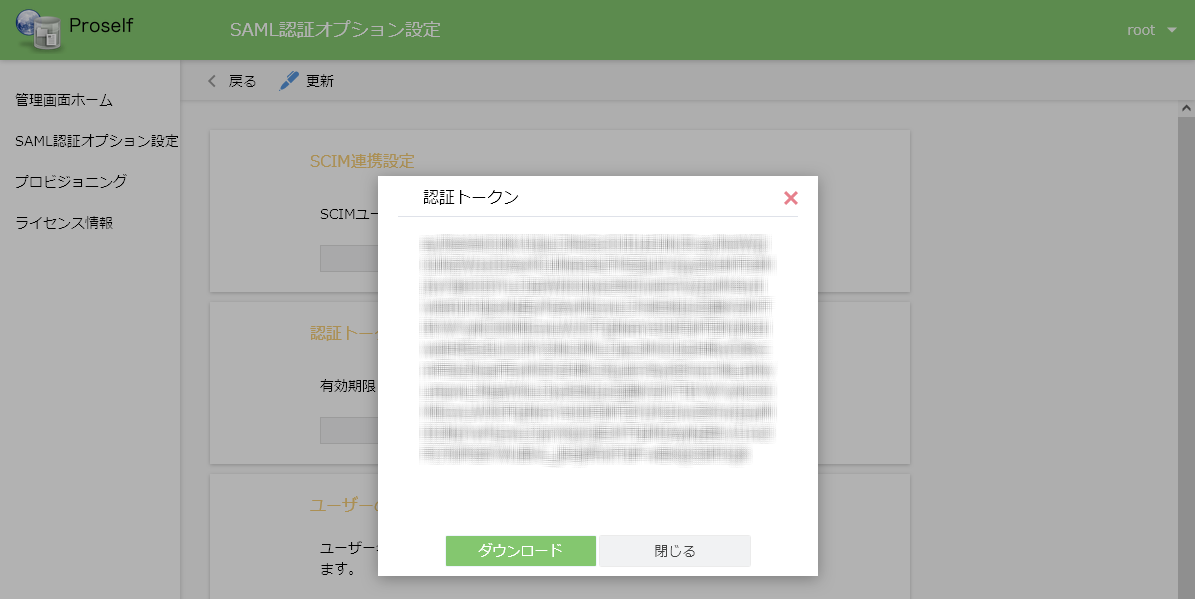
**認証トークン発行完了画面**

トークン発行後、SCIM連携設定画面の「認証トークン」が以下のような情報が表示されます。



**SCIM連携設定**

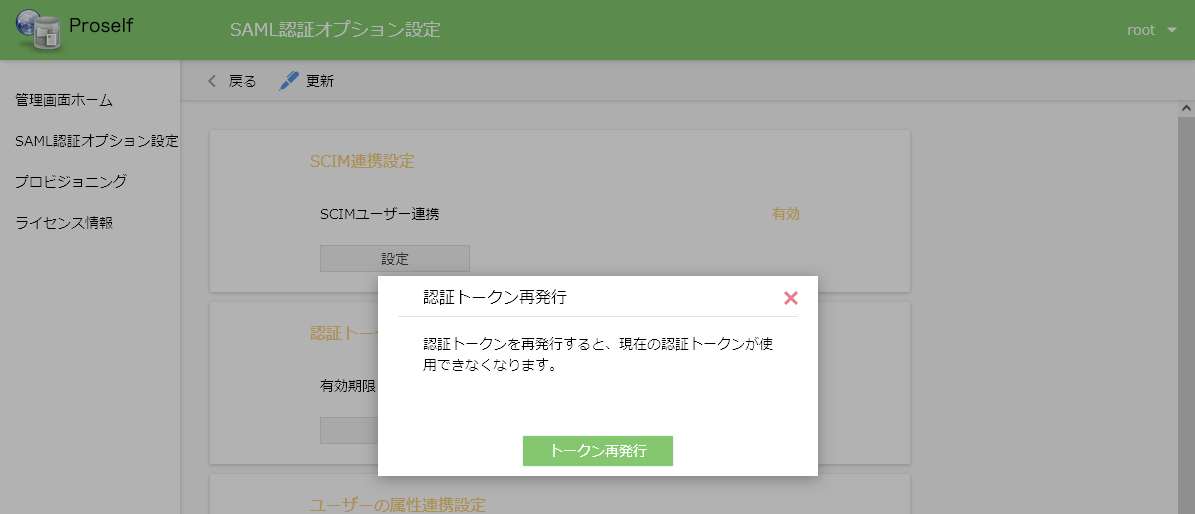
「表示」をクリックすると発行済みのトークンが表示され、ダウンロードを行うことができます。



**認証トークン**

トークンを再発行したい場合は「トークン発行」をクリックします。

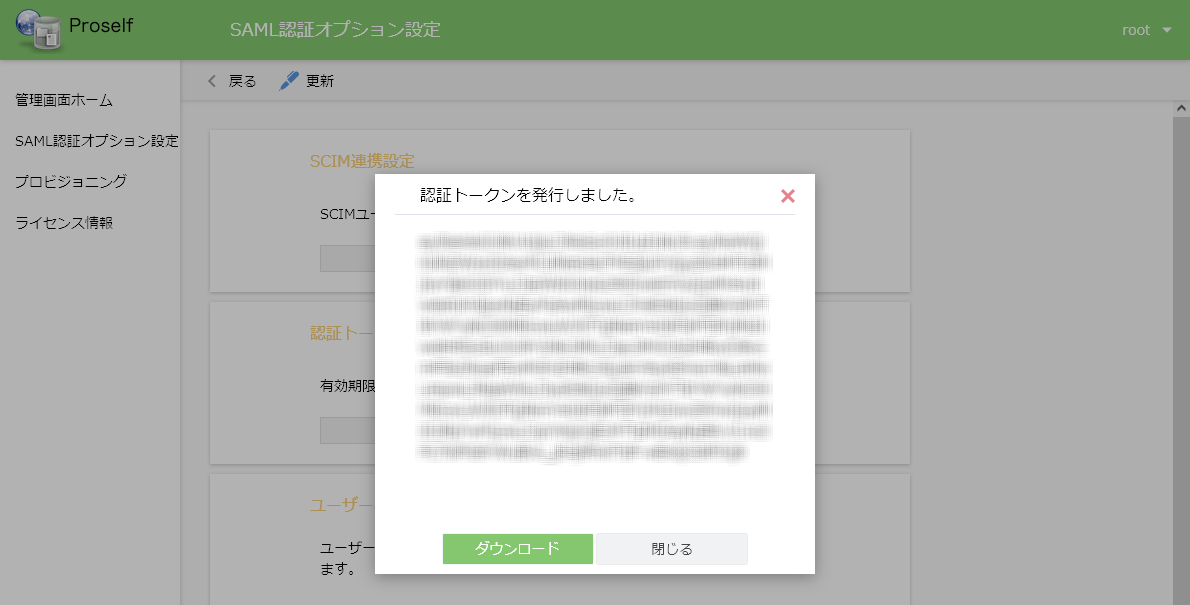
以下のような確認画面が表示されますので、「トークン再発行」をクリックします。



**認証トークン再発行**

認証トークンが再発行されます。

再発行後のトークンは再度Entra IDに設定する必要がありますため、画面内の「ダウンロード」をクリックして保存後、「3[.2.1.プロビジョニングの開始](#_プロビジョニングの開始)」を行います。



**認証トークン発行完了画面**

## Entra IDでの設定

「[2.1.1.アプリケーションの作成](#_アプリケーションの作成)」で作成したアプリケーションに対し、プロビジョニングの設定を行います。

概要画面の「3。ユーザー アカウントのプロビジョニング」より「作業の開始」をクリックします。



20

**概要-プロパティ**

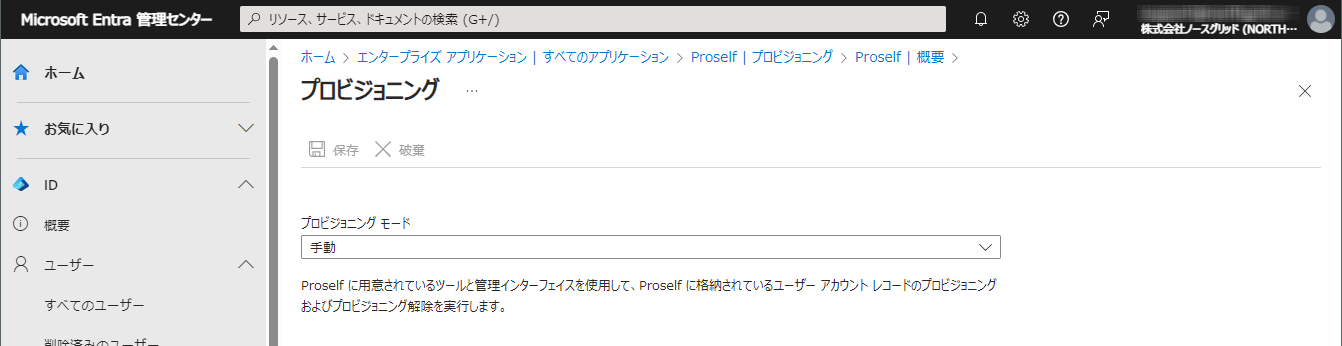
「作業の開始」をクリックします。



20

**プロビジョニング**

プロビジョニングモードを「手動」から「自動」に切り替えます。



**プロビジョニング**

管理者資格情報等の項目が表示されますので各項目に入力します。



**プロビジョニング**

各項目には以下のように入力します。

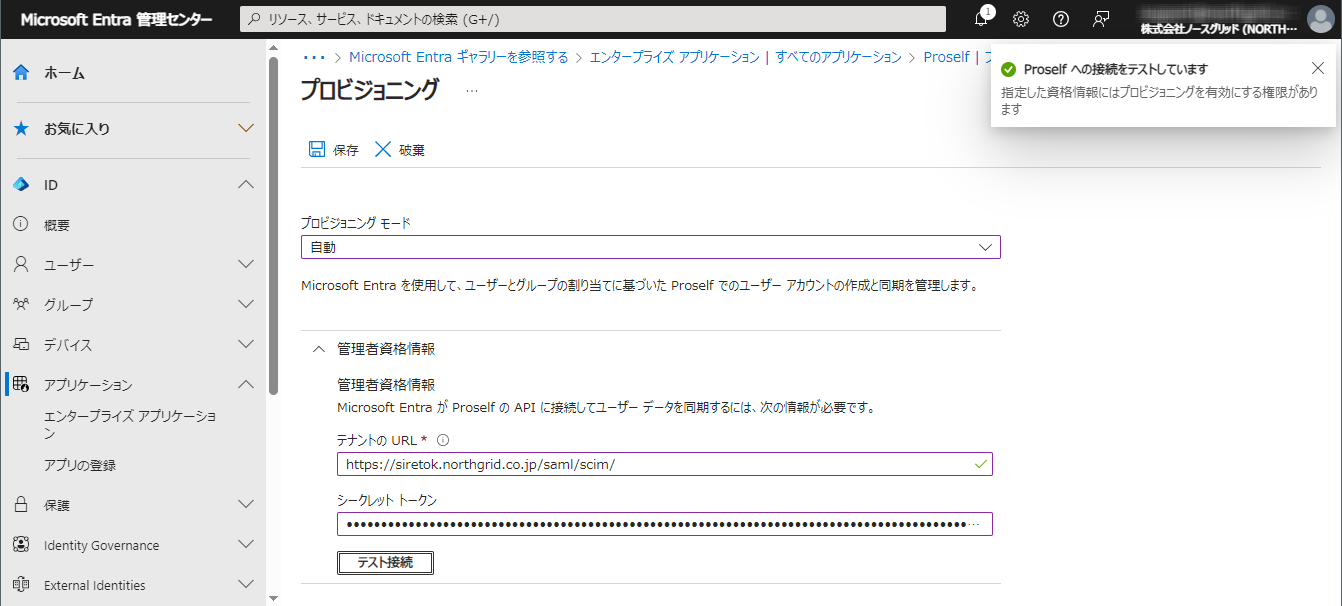
| 項目 | 入力内容 |
| --- | --- |
| テナントのURL | https://[サーバーアドレス]/saml/scim/ |
| シークレットトークン | 「[3.1.3.認証トークン発行](#_認証トークン発行)」で発行した認証トークンを入力します。 |

* [サーバーアドレス]には Proself をインストールしたサーバーの IP アドレスまたはFQDN(完全修飾ドメイン名)を入力します。

各情報を入力後に「テスト接続」をクリックします。

テスト接続の結果に問題がないことを確認後、画面上部の「保存」をクリックし設定を保存します。

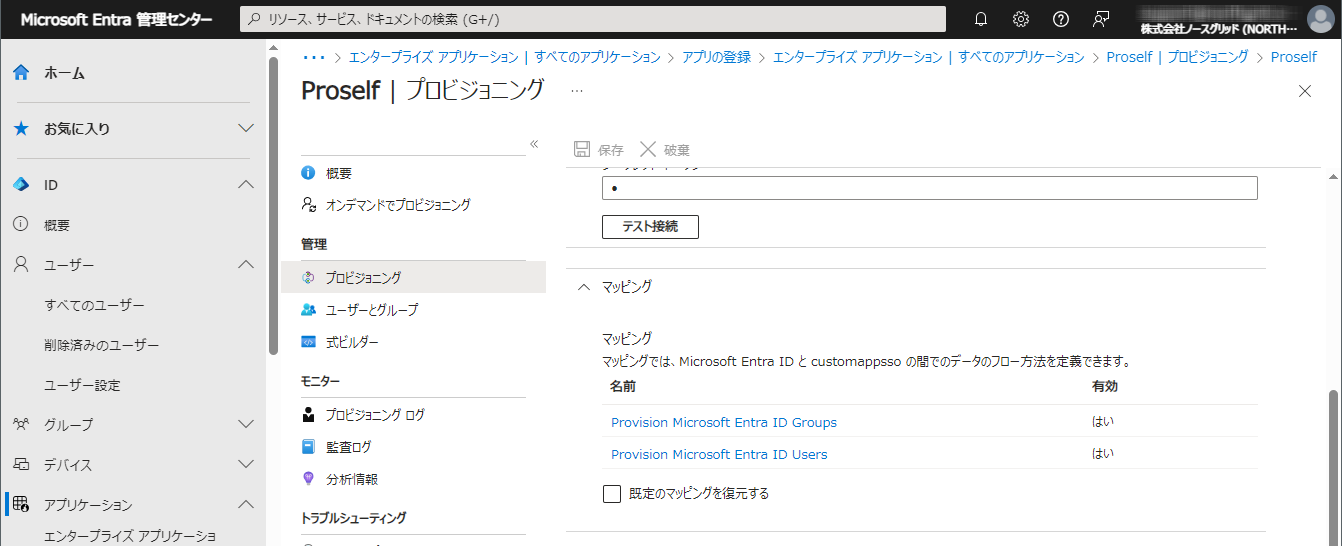
* テスト接続の結果に問題がある場合は「保存」をクリックしてもエラーメッセージが表示され、設定を保存することはできません。



20

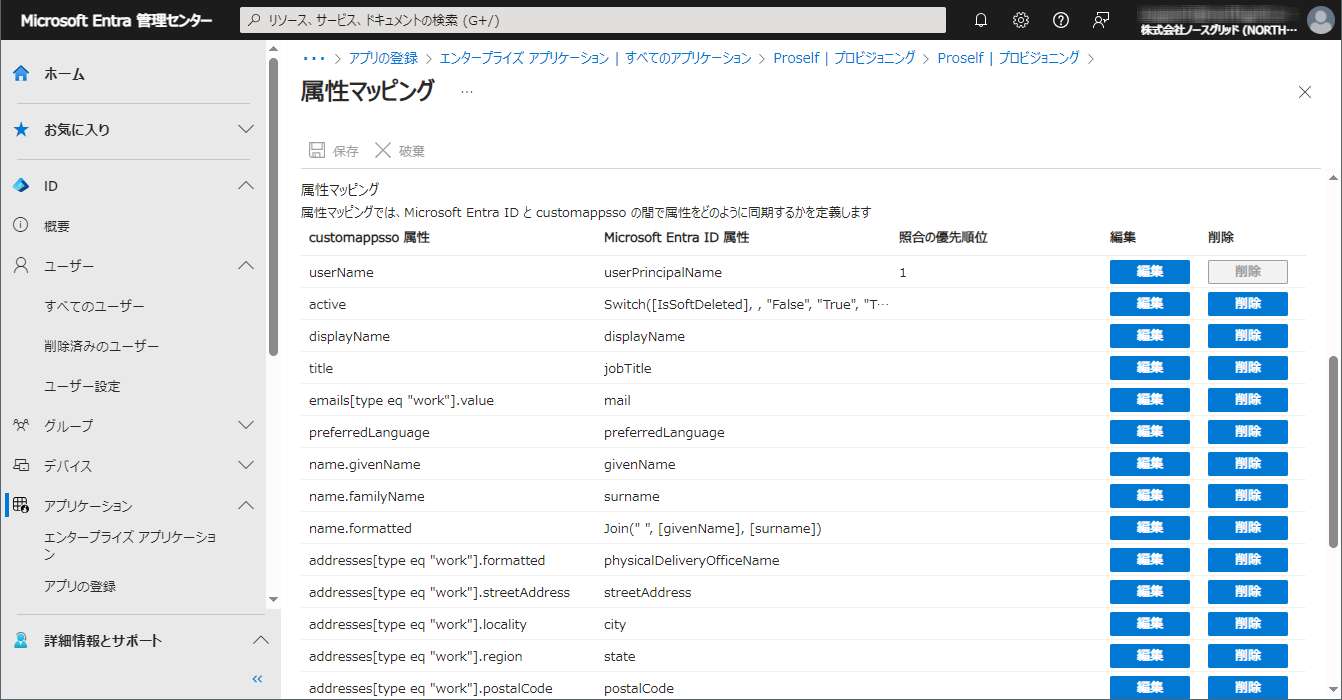
**プロビジョニング**

保存後、マッピングの項目が追加されますので、「Provision Microsoft Entra ID Users」をクリックします。



**プロビジョニング**

属性マッピング画面で「customappsso属性」の列が「active」となっている行の「編集」をクリックします。



**属性マッピング**

マッピングの種類を「式」から「直接」に変更します。



**属性の編集**

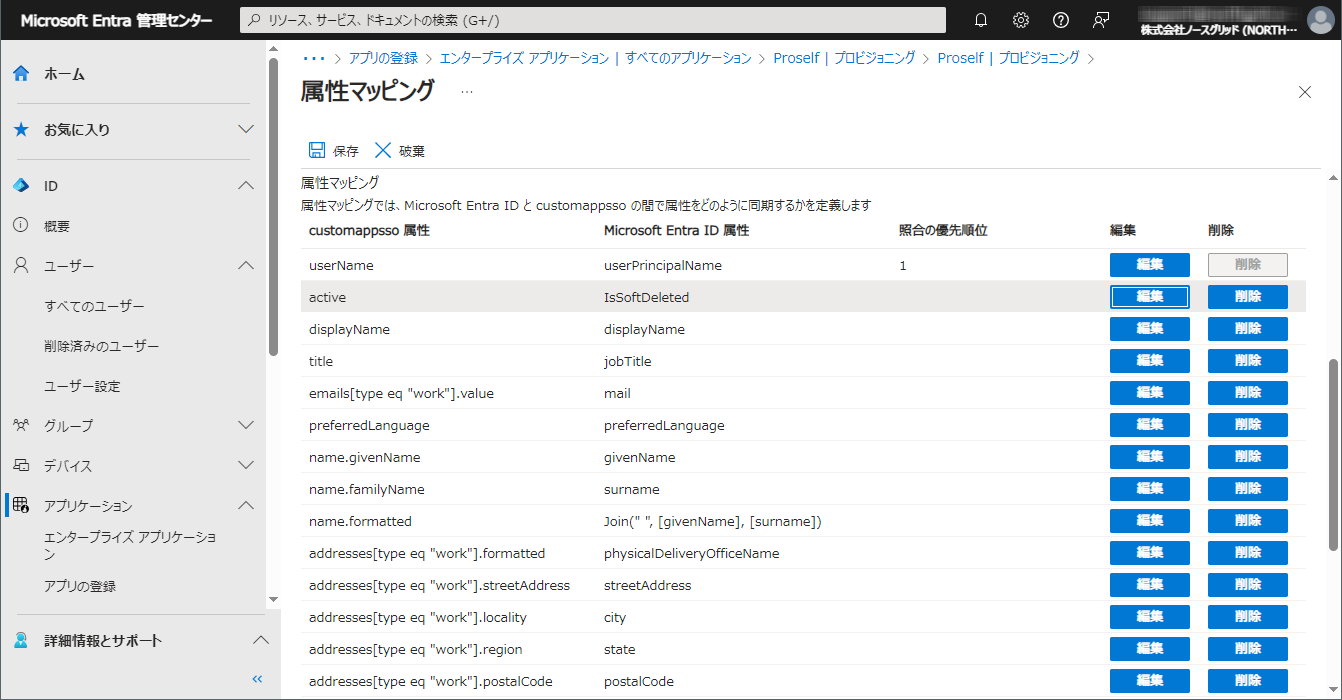
ソース属性より「IsSoftDeleted」を選択後、画面下部の「OK」をクリックします。

* 他の設定については変更の必要はございません。



**属性の編集**

属性マッピングの画面に戻りますので、画面上部の「保存」をクリックして設定を保存します。



**属性マッピング**

設定としては以上で完了です。

設定後は次項の「[3.2.1プロビジョニングの開始](#_プロビジョニングの開始)」を実施し、Proself上にSCIM連携ユーザーを作成します。

### プロビジョニングの開始

プロビジョニング概要画面の上部メニューより「プロビジョニングの開始」をクリックします。



**プロビジョニング - 概要**

開始されると以下のように「プロビジョニングの開始」がグレーアウトされます。



**プロビジョニング - 概要**

Entra IDがProselfに対して通信を行い、SCIM連携ユーザーがProselfに作成されます。

* 作成されたユーザーの「連携」列にチェックが入ります。



**ユーザー一覧(プロビジョニング開始前)**



**ユーザー一覧(プロビジョニング開始後)**

|  |
| --- |
| **注意点：**  デフォルトではユーザープリンシパル名(@より前)がProselfに作成されるユーザーのIDとして使用されます。  そのため、「[2.2.2.SAML設定](#_SAML設定)」で指定する「ユーザー属性 ユーザーIDのキー名」に「user.userprincipalname」のクレーム名以外を指定している場合は設定変更が必要です。   * 設定変更を行わない場合、「[4.シングルサインオン](#_シングルサインオン)」で記載している手順でシングルサインオンを行うことができません。   例として、「ユーザー属性 ユーザーIDのキー名」に「user.mail」のクレーム名を指定している場合の設定変更手順を以下に記載します。   1. プロビジョニングのマッピングより「Provision Microsoft Entra ID Users」をクリックします。   **プロビジョニング**   1. 属性マッピング画面で「customappsso属性」列が「userName」となっている行の「編集」をクリックします。   **属性マッピング**   1. 属性の編集画面のソース属性を「userPrincipalName」から「mail」に変更して画面下部の「OK」をクリックします。   **属性の編集**  **属性の編集**   1. 属性マッピング画面で「customappsso属性」列の「userName」に対応する「Microsoft Entra ID属性」列が「mail」となっていることを確認し、画面上部の「保存」をクリックします。   **属性マッピング** |

なお、Entra IDのプロビジョニングによるユーザー同期は40分間隔で行われるため、プロビジョニング開始後に「[2.1.2.ユーザー、グループの割り当て](#_ユーザー、グループの割り当て)」を実行してもProself側に即時反映はされません。

即時反映をさせたい場合は「[3.2.2.プロビジョニングの即時実行](#_プロビジョニングの即時実行)」をご参照ください。

### プロビジョニングの即時実行

プロビジョニングの即時実行の方法として以下があります。

* プロビジョニング概要画面のメニューより「要求時にプロビジョニングする」を実施する
* プロビジョニング停止後、プロビジョニング開始を実施する。

以下よりそれぞれの手順について記載しております。

**要求時にプロビジョニングする場合**

プロビジョニング概要画面のメニューより「要求時にプロビジョニングする」をクリックします。



**プロビジョニング - 概要**

「要求時にプロビジョニング」画面でユーザー選択を行い、画面下部にある「プロビジョニング」をクリックします。

* 本機能によって1度に連携できるユーザーは1名のみという制約があります。



**要求時にプロビジョニング**

プロビジョニングが完了すると、「アクションの実行」画面が表示されます。



**アクションの実行**

以下は、アプリケーションにユーザー1名を追加で割り当てた後に上記を実施した場合における、ユーザー一覧の例となります。



**ユーザー一覧(プロビジョニング実施前)**



**ユーザー一覧(プロビジョニング実施後)**

**プロビジョニング停止後、プロビジョニング開始を実施する場合**

プロビジョニング概要画面のメニューより「プロビジョニングの停止」をクリックします。



**プロビジョニング - 概要**

プロビジョニングの停止確認画面で「OK」をクリックします。



**プロビジョニングの停止**

停止を確認後、再度「プロビジョニングの開始」をクリックします。



**プロビジョニング**

以下はアプリケーションにユーザー2名を追加で割り当てた場合における、ユーザー一覧の例です。



**ユーザー一覧(プロビジョニング開始前)**



**ユーザー一覧(プロビジョニング開始後)**

## ユーザーの属性連携設定

「[3.2.Entra IDでの設定](#_Entra_IDでの設定)」で設定する属性マッピング画面における「customappsso属性」をProselfに設定すると、SCIM連携時にProselfに作成されるユーザーのメールアドレス、名前等の情報を設定することができます。



**プロビジョニングの属性マッピング**

SCIM連携設定のユーザーの属性連携設定より「設定」をクリックします。



**SCIM連携設定**

連携する属性画面で、SCIM連携ユーザーの属性を設定し、画面上部の「更新」をクリックします。以下例では「名前」にcustomappsso属性の「name.formatted」を指定しております。



**SCIM連携設定 - 連携する属性**

上記設定後は「[3.2.1.プロビジョニングの開始](#_プロビジョニングの開始)」または「[3.2.2.プロビジョニングの即時実行](#_プロビジョニングの即時実行)」を実施します。

以下例では、Proselfに作成されるユーザーに名前が設定されております。



**ユーザー一覧(プロビジョニング開始前)**



**ユーザー一覧(プロビジョニング開始後)**

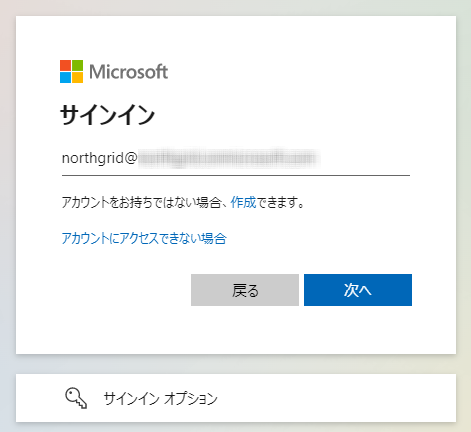
# シングルサインオン

## Webブラウザからのシングルサインオン

Webブラウザからシングルサインオンを行う場合はEntra ID から行う方法、Proselfから行う方法の2通りがあります。

### Entra IDからのシングルサインオン(IdP Initiated)

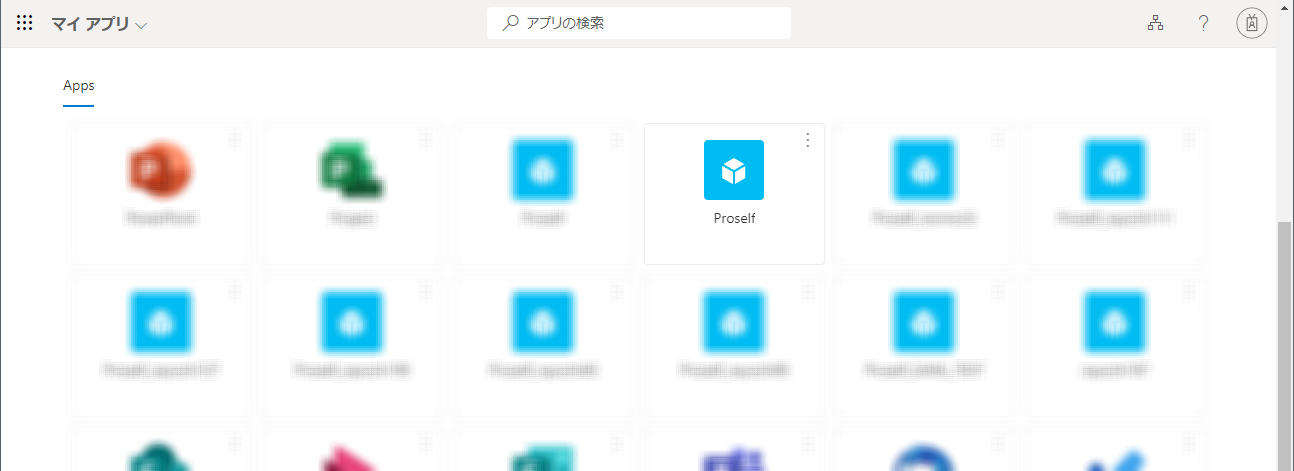
Webブラウザで「https://myapplications.microsoft.com/」にアクセスし、「[2.1.2. ユーザー、グループの割り当て](#_ユーザー、グループの割り当て)」で割り当てたユーザーでEntra IDにサインインします。



**サインイン**

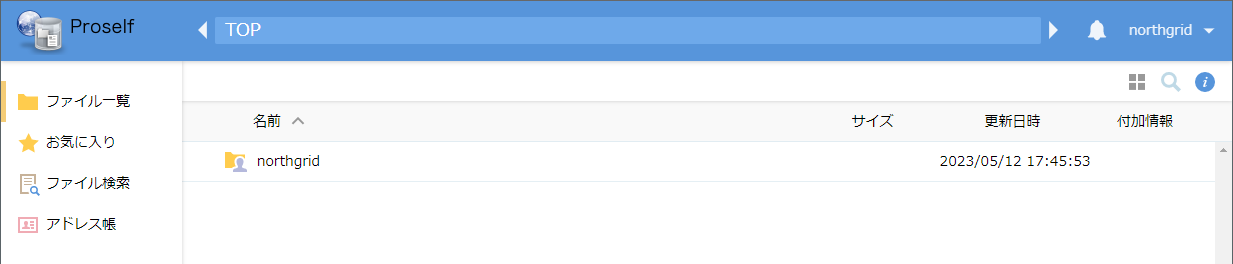
アプリ ダッシュボードよりアプリケーションをクリックします。

ここでは「[2.1.1.アプリケーションの作成](#_アプリケーションの作成)」にて作成した「Proself」をクリックします。



**アプリ ダッシュボード**

Proselfログイン後の画面が表示されます。

****

**ログイン後の画面(ファイル一覧)**

### Proselfからのシングルサインオン(SP initiated)

「https://[サーバーアドレス]/」にアクセスします。

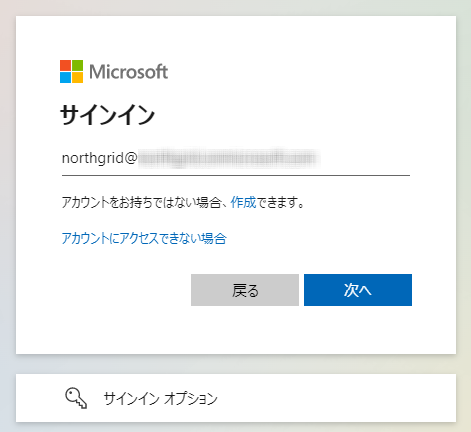
* [サーバーアドレス]には Proself をインストールしたサーバーの IP アドレスまたはFQDN(完全修飾ドメイン名)を入力します。

SAML認証オプション設定において「認証サーバーへの自動リダイレクト設定」を有効としていない場合は以下のようにProselfのログイン画面が表示されますので、シングルサインオンをクリックします。



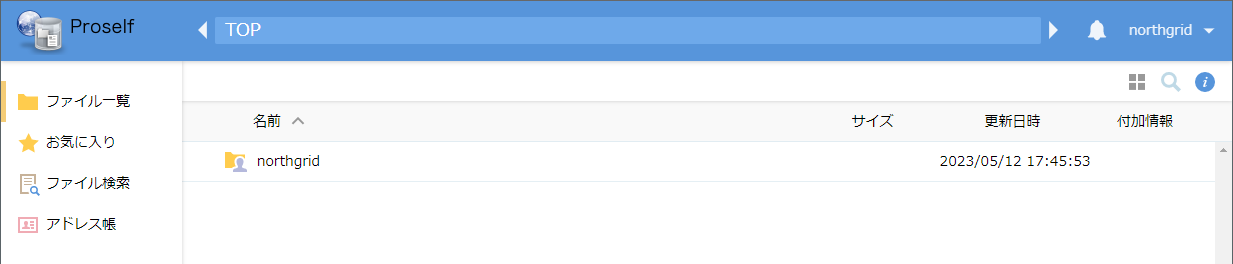
**ログイン画面**

Entra IDにサインインしていない場合はサインインページが表示されますので、「[2.1.2. ユーザー、グループの割り当て](#_ユーザー、グループの割り当て)」で割り当てたユーザーでEntra IDにサインインします。



**サインイン**

Proselfログイン後の画面が表示されます。

****

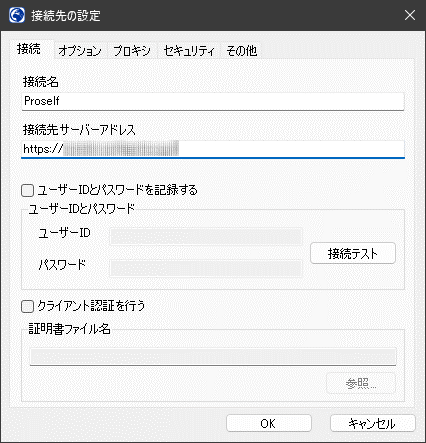
**ログイン後の画面(ファイル一覧)**

## Proself Clientからのシングルサインオン

Proself Ver5.70、SAML認証オプションVer5.70、Proself Client Ver2.50よりProself Clientからのシングルサインオンが可能です。

* Webブラウザと異なり、Proselfからのシングルサインオン(SP initiated)のみ可能です。

Proself Clientの接続先を作成または編集します。

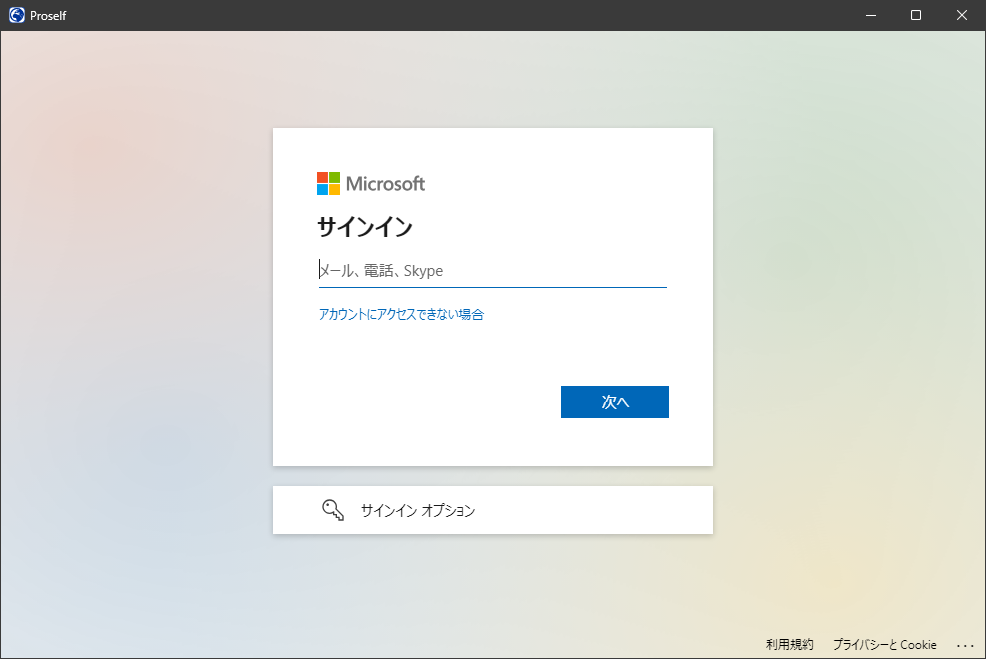


**接続先の設定**

Proself Clientの接続先の設定においては以下を設定します。

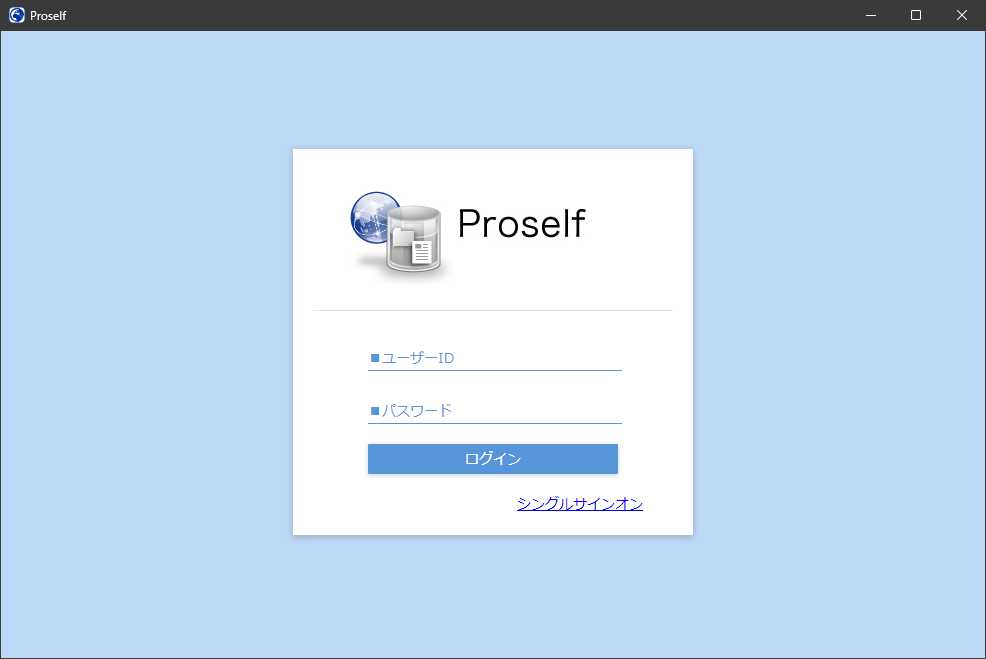
| 項目 | 入力内容 |
| --- | --- |
| 接続名 | 接続先の名前を入力します。 |
| 接続先サーバーアドレス | 以下を入力します。  https://[サーバーアドレス]/  [サーバーアドレス]には Proself をインストールしたサーバーの IP アドレスまたはFQDN(完全修飾ドメイン名)を入力します。 |
| ユーザーIDとパスワードを記録する | チェックOFFにします。 |

設定後「OK」をクリックするとWebViewでEntra IDのサインインページが表示されますので、「[2.1.2. ユーザー、グループの割り当て](#_ユーザー、グループの割り当て)」で割り当てたユーザーでEntra IDにサインインします。



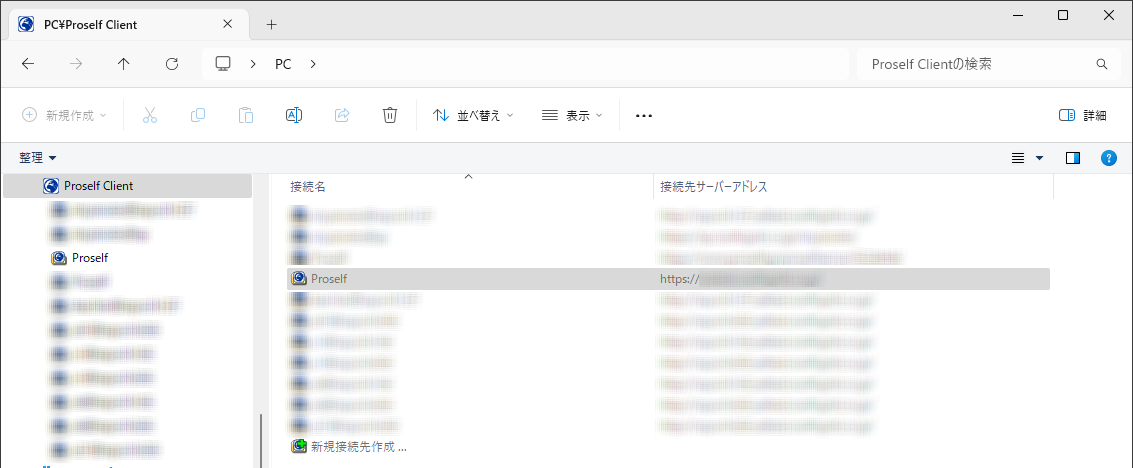
**Entra IDサインイン画面**

* 以下のようにProselfのログイン画面が表示された場合は「シングルサインオン」をクリックします。



**Proselfログイン画面**

サインインに成功した場合は接続先が保存されますので、保存した接続名をクリックしサーバーに接続にします。



**接続名一覧**

サーバーに接続するとユーザーフォルダ/グループフォルダの一覧が表示されます。



**ユーザーフォルダ/グループフォルダ一覧**