|  |
| --- |
| インストールガイドVer |
| 操作チュートリアル  Google Workspace連携編 |
|  |



|  |
| --- |
| 第1版  2025/02/14 |

目次

[1. 概要 1](#_Toc190447251)

[2. Google Workspaceを使用したSAML設定手順 1](#_Toc190447252)

[2.1. Google Workspaceでの設定 1](#_Toc190447253)

[2.1.1. アプリケーションの作成 1](#_Toc190447254)

[2.1.2. ユーザーアクセスの設定 5](#_Toc190447255)

[2.2. Proselfでの設定 6](#_Toc190447256)

[2.2.1. このサーバー情報の設定 6](#_Toc190447257)

[2.2.2. SAML設定 8](#_Toc190447258)

[2.2.3. SP証明書設定 11](#_Toc190447259)

[2.2.4. ユーザー追加 11](#_Toc190447260)

[2.2.5. シングルサインオンのテスト 11](#_Toc190447261)

[2.2.6. IdP証明書の更新 12](#_Toc190447262)

[3. シングルサインオン 17](#_Toc190447263)

[3.1. Webブラウザからのシングルサインオン 17](#_Toc190447264)

[3.1.1. Google Workspaceからのシングルサインオン(IdP Initiated) 17](#_Toc190447265)

[3.1.2. Proselfからのシングルサインオン(SP initiated) 19](#_Toc190447266)

[3.2. Proself Clientからのシングルサインオン 21](#_Toc190447267)

# 概要

本チュートリアルは、Google Workspaceを使用したSAML認証を行うための設定方法について記載しております。

* 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。

# Google Workspaceを使用したSAML設定手順

Google Workspaceを使用したSAML設定手順を記載します。

なお、事前にGoogle Workspace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Google Workspaceの画面ショットは2025年1月時点のものとなっております。将来Google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。

## Google Workspaceでの設定

### アプリケーションの作成

Webブラウザで「https://admin.google.com/」にアクセスし、Google Workspaceの管理者でログインします。



**Googleログイン**

ログイン後Google管理コンソールが表示されますので、左メニューより「アプリ」>「ウェブアプリとモバイルアプリ」の順にクリックします。



**Google管理コンソール**

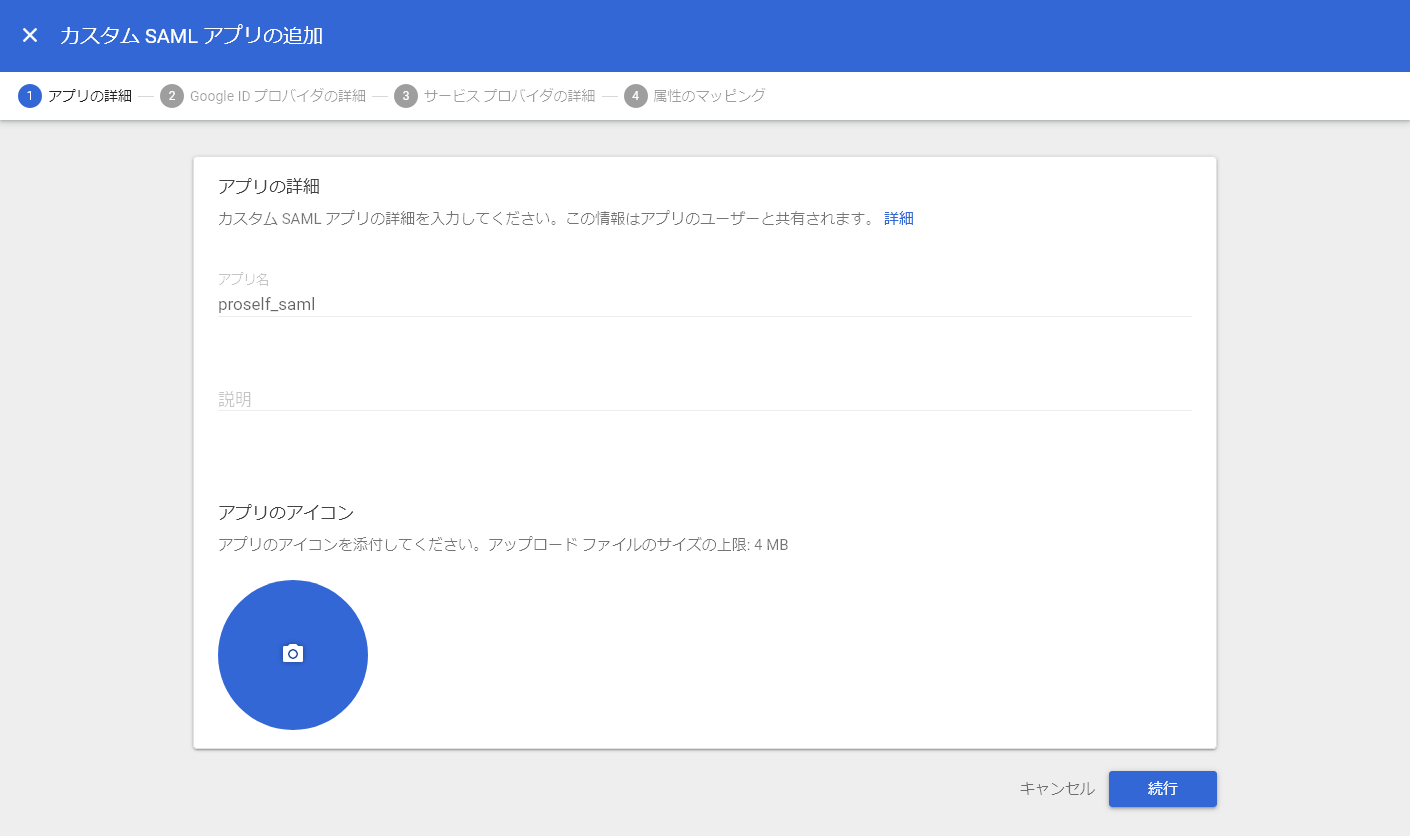
上部メニューより「アプリを追加」>「カスタムSAMLアプリの追加」の順にクリックします。



**Google管理コンソール**

カスタムSAMLアプリの追加 - アプリの詳細画面で「アプリ名」に任意の名前を入力後、「続行」をクリックします。

* 「説明」、「アプリのアイコン」の設定は任意です。



**カスタムSAMLアプリの追加 - アプリの詳細**

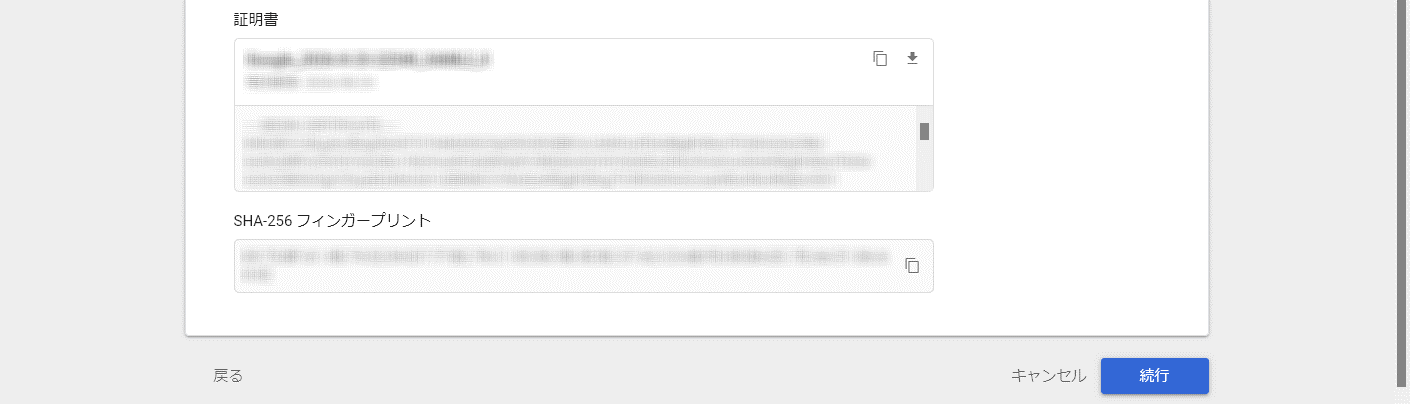
カスタムSAMLアプリの追加 - Google IDプロバイダの詳細画面で「メタデータをダウンロード」をクリックしてIdPメタデータ(XMLファイル)をダウンロードしておきます。

IdPメタデータは「[2.2.2.SAML設定](#_SAML設定)」で使用します。



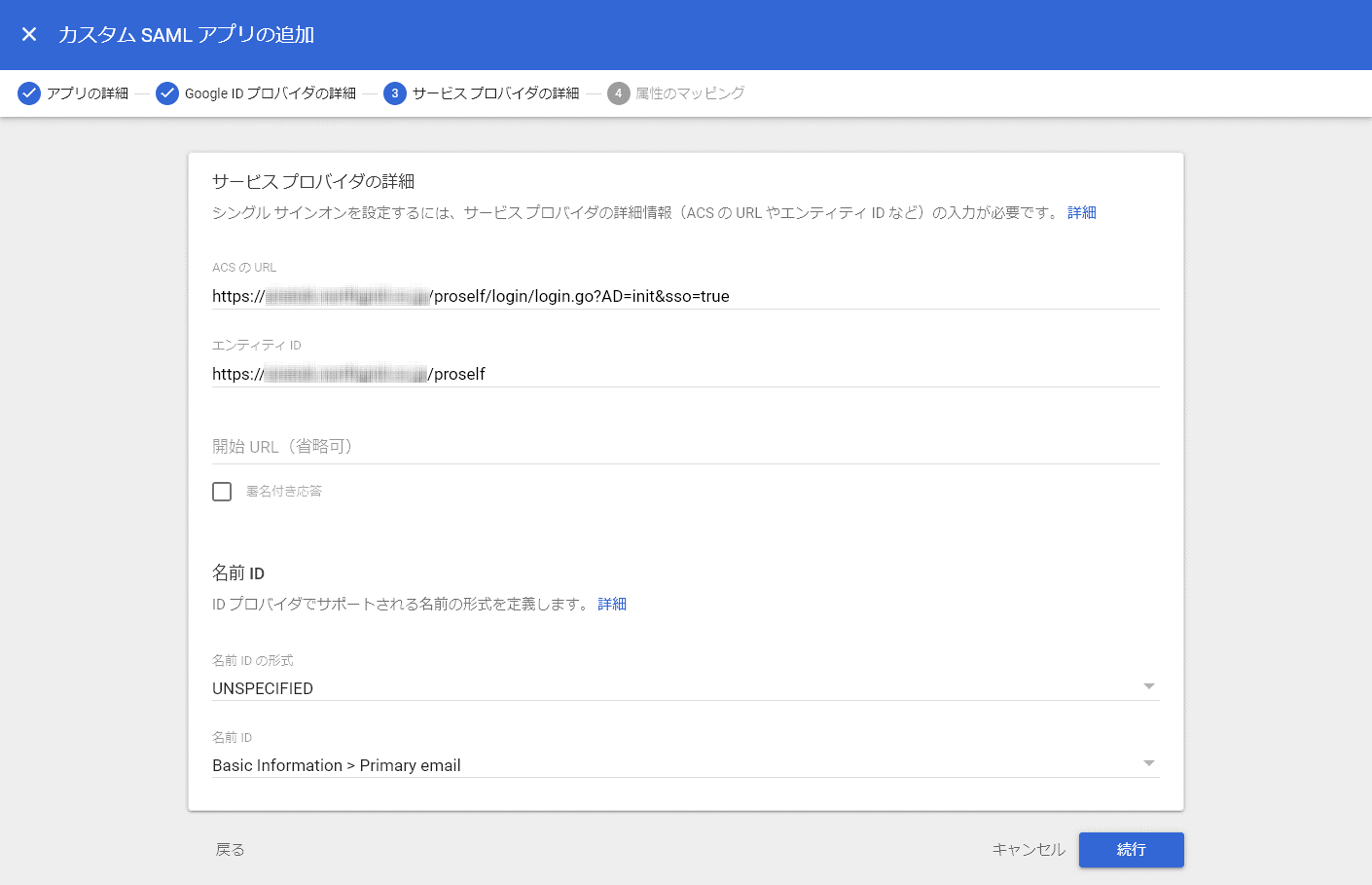
**カスタムSAMLアプリの追加 - Google IDプロバイダの詳細**

メタデータのダウンロード後、カスタムSAMLアプリの追加 - Google IDプロバイダの詳細の画面下部にある「続行」をクリックします。



**カスタムSAMLアプリの追加 - Google IDプロバイダの詳細**

カスタムSAMLアプリの追加 - サービスプロバイダの詳細画面が表示されますので、「ACSのURL」、「エンティティID」、「名前IDの形式」、「名前ID」を設定後、画面下部の「続行」をクリックします。



**カスタムSAMLアプリの追加 - サービスプロバイダの詳細**

各項目は以下のように設定します。

| 項目 | 設定内容 |
| --- | --- |
| ACSのURL(※1) | https://[サーバーアドレス]/proself/login/login.go?AD=init&sso=true |
| エンティティID(※1) | https://[サーバーアドレス]/proself |
| 名前IDの形式 | UNSPECIFIED (デフォルト) |
| 名前ID(※2) | ProselfのユーザーIDと紐づける項目を以下から選択します。  Basic Information > First Name (名)  Basic Information > Last Name (姓)  Basic Information > Primary email (メールアドレス)   * カスタム属性の設定を行うことで、上記以外の項目についてもProselfのユーザーIDと紐づけることができます。詳細につきましてはGoogle Workspace 管理者ヘルプの「ユーザー プロフィールのカスタム属性を作成する」をご参照ください。 <https://support.google.com/a/answer/6208725> |

※1　[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。

※2　設定する項目の値に「@」が含まれている場合は「@」より前をユーザーIDとして認識します。

カスタムSAMLアプリの追加 - 属性のマッピング画面では、属性内にある「マッピングを追加」をクリックして属性を設定後、画面下部の「完了」をクリックします。



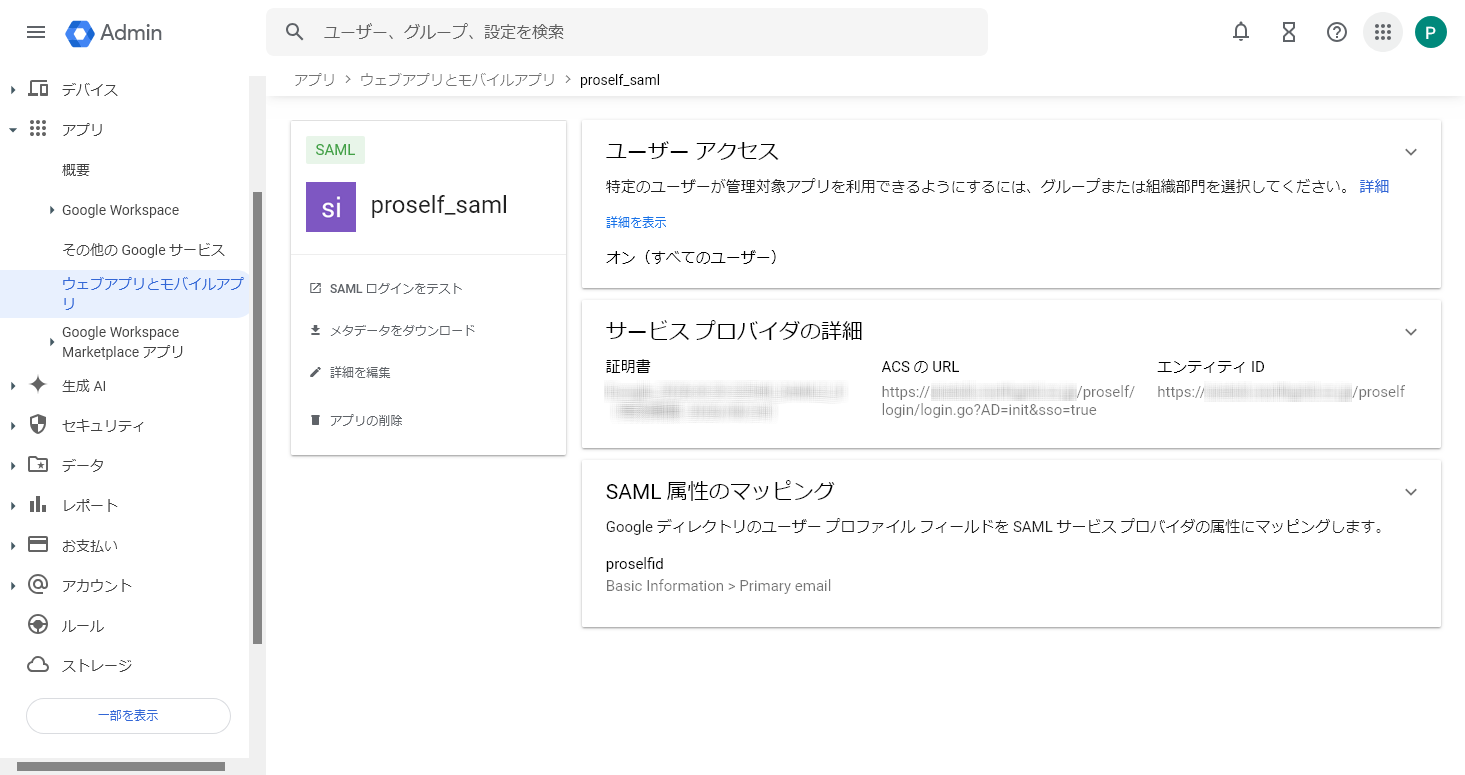
**カスタムSAMLアプリの追加 - 属性のマッピング**

各項目は以下のように設定します。

| 項目 | 設定内容 |
| --- | --- |
| Google Directoryの属性 | 上記手順で設定済みの「名前ID」を指定します。 |
| アプリの属性 | 任意の値を入力します。設定値は「[2.2.2.SAML設定](#_SAML設定)」の「ユーザー属性 ユーザーIDのキー名」で設定します。 |

### ユーザーアクセスの設定

「[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)」でアプリの追加が完了すると作成したアプリケーションの設定画面が表示されますので、ユーザーアクセスの逆三角形アイコンをクリックします。



**アプリケーションの詳細画面**

「サービスのステータス」を「オン(すべてのユーザー)」に設定し「保存」をクリックします。

* 設定が反映されるまでに時間がかかる場合があります。

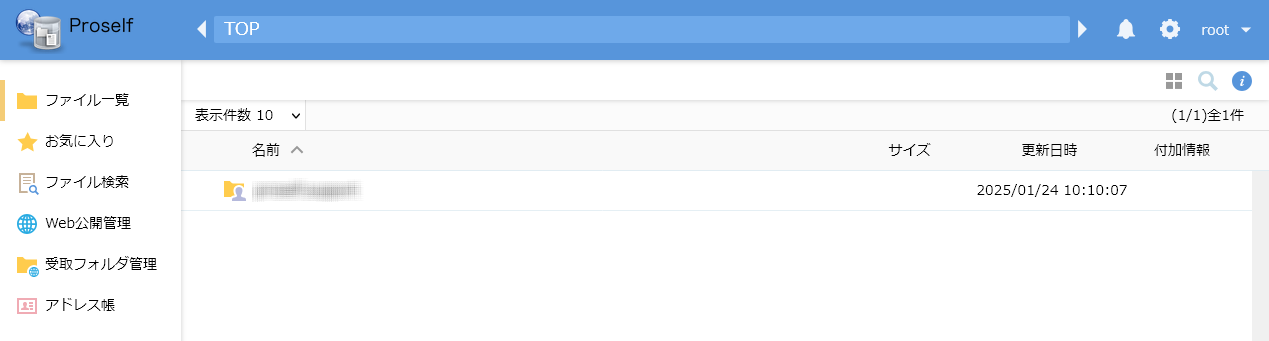


**サービスのステータス**

## 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。



**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。

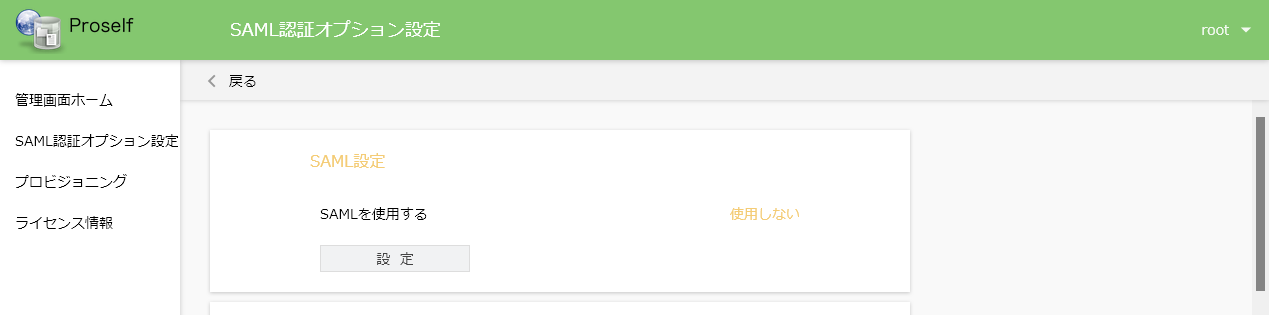


**管理画面**

SAML認証オプション設定＞SAML設定より「設定」をクリックします。



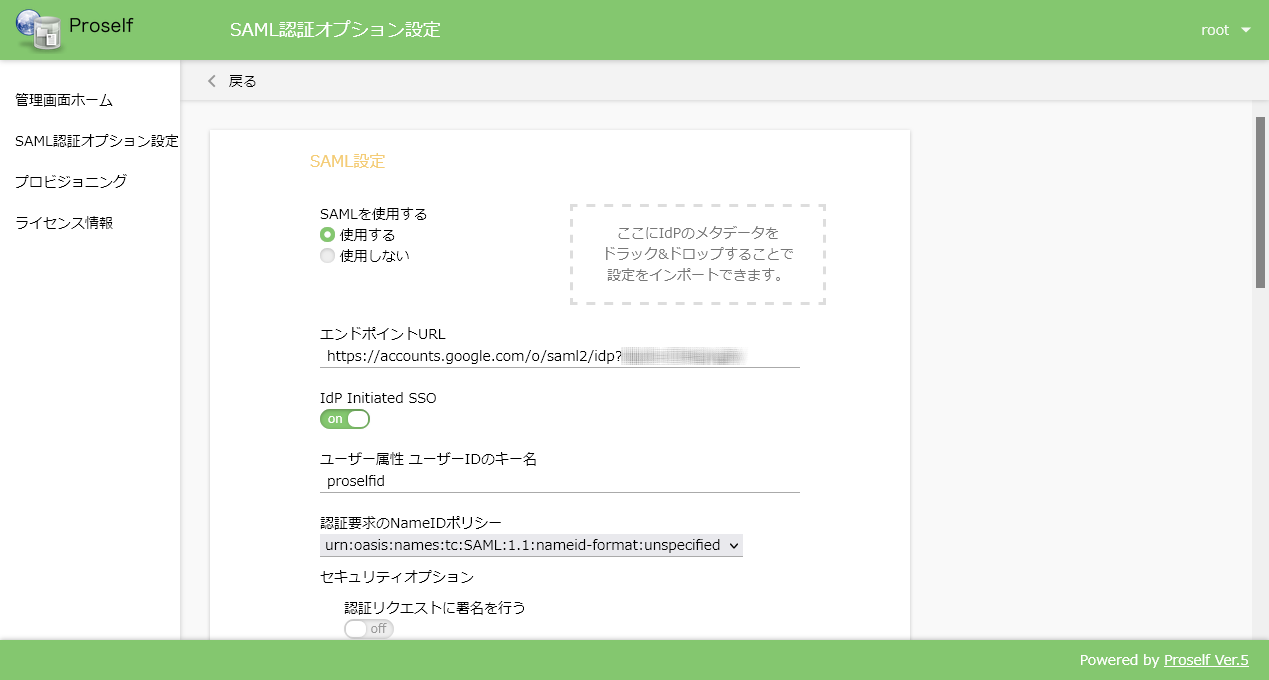
**SAML認証オプション設定**



**SAML認証オプション設定**

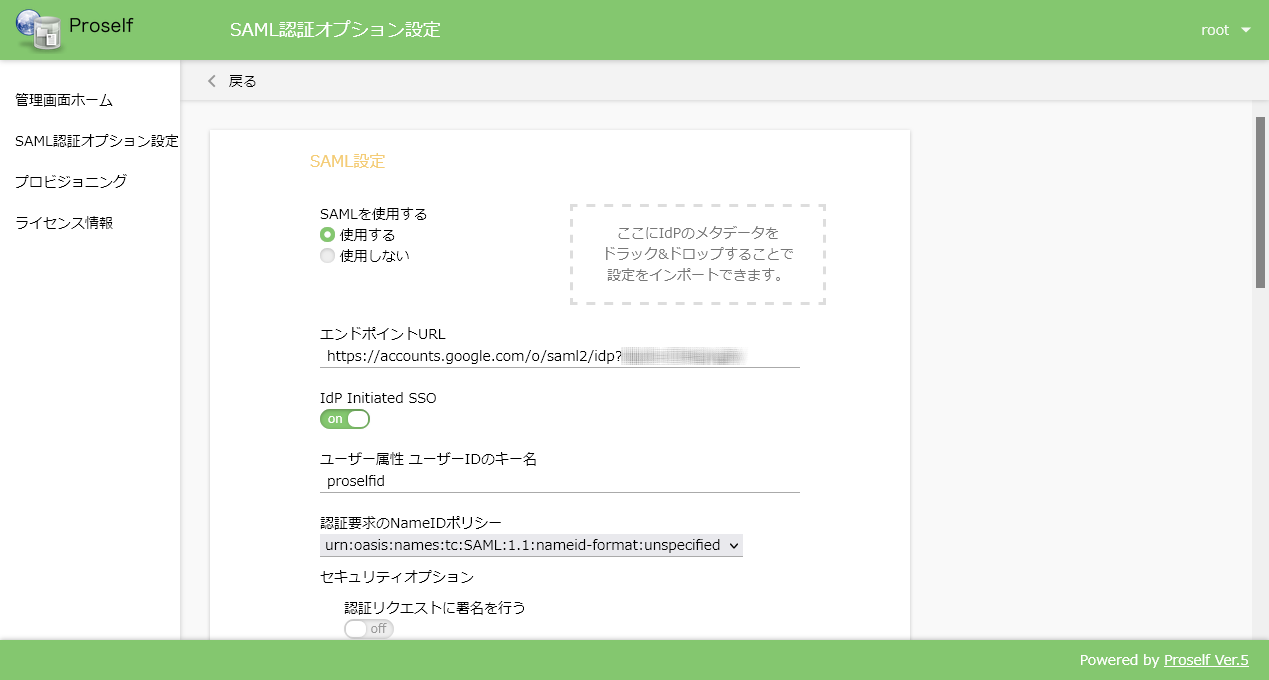
「SAMLを使用する」を「使用する」にします。

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



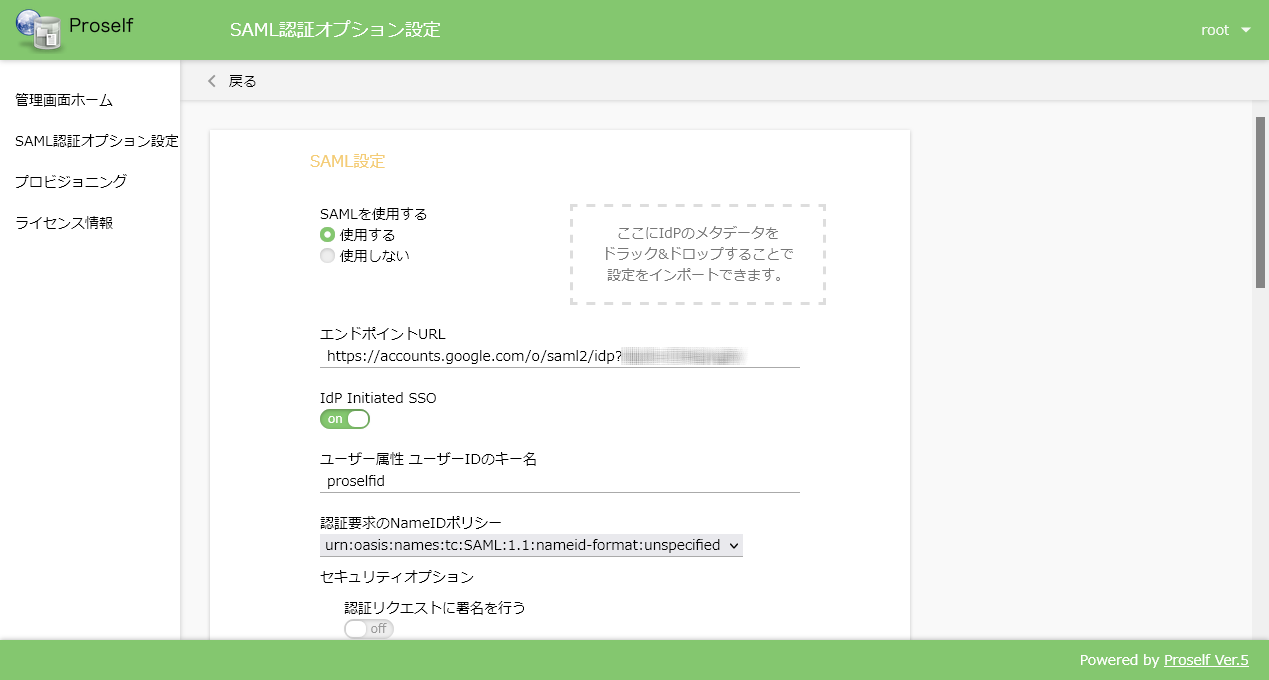
**SAML設定**

「ここにIdPメタデータを～」の枠内に「[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)」でダウンロードした「IdPメタデータ」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。

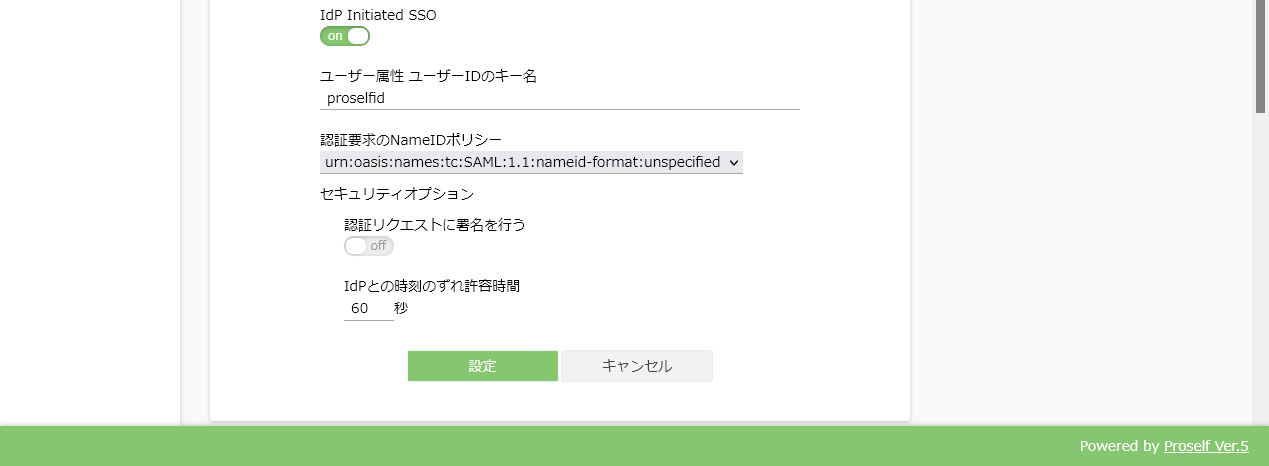


**SAML設定**

「[2.1.1.アプリケーションの作成](#_アプリケーションの作成)」で設定した「アプリの属性」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、画面上部の「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、Google Workspaceの証明書を更新した場合、更新済みのIdP証明書を手動でProselfにインポートする必要があります。詳細につきましては「[2.2.6.IdP証明書の更新](#_IdP証明書が更新された場合)」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。

### ユーザー追加

Google Workspaceで作成したユーザーをProselfに追加します。

追加するユーザーID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)」で設定した「Google Directoryの属性」に対応する属性値と一致するようにします。

| Google Workspaceの属性 | ユーザーID |
| --- | --- |
| Basic Information > First Name | Google Workspaceのユーザーの名 |
| Basic Information > Last Name | Google Workspaceのユーザーの姓 |
| Basic Information > Primary email | Google Workspaceのユーザーのメールアドレス(@より前) |

Google Workspace 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。

|  |
| --- |
| 名：north  姓：grid  メールアドレス：northgridmail@example.co.jp |

* Google Directoryの属性に「Basic Information > First Name」を指定した場合

ProselfのユーザーIDは「north」になります。

* Google Directoryの属性に「Basic Information > Last Name」を指定した場合

ProselfのユーザーIDは「grid」になります。

* Google Directoryの属性に「Basic Information > Primary email」を指定した場合

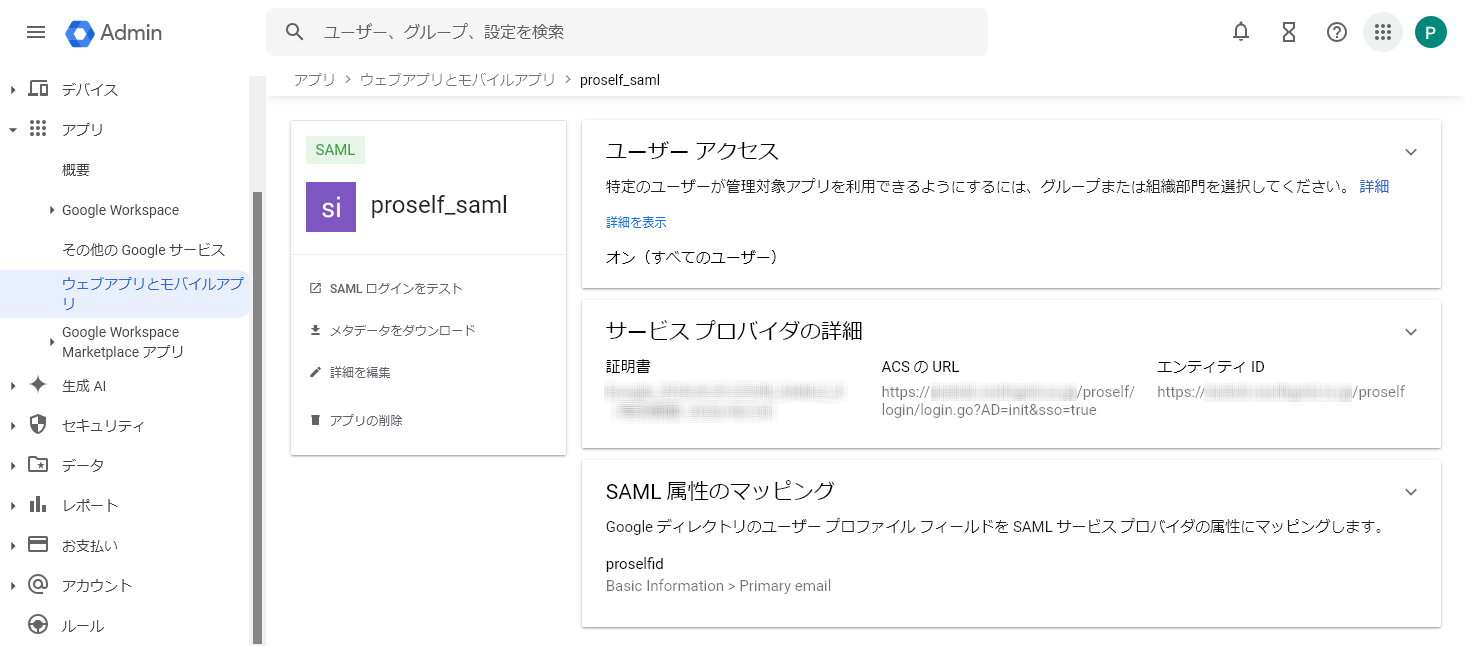
ProselfのユーザーIDは「northgridmail」になります。

### シングルサインオンのテスト

Google管理コンソールからシングルサインオンが可能かどうかのテストが可能です。

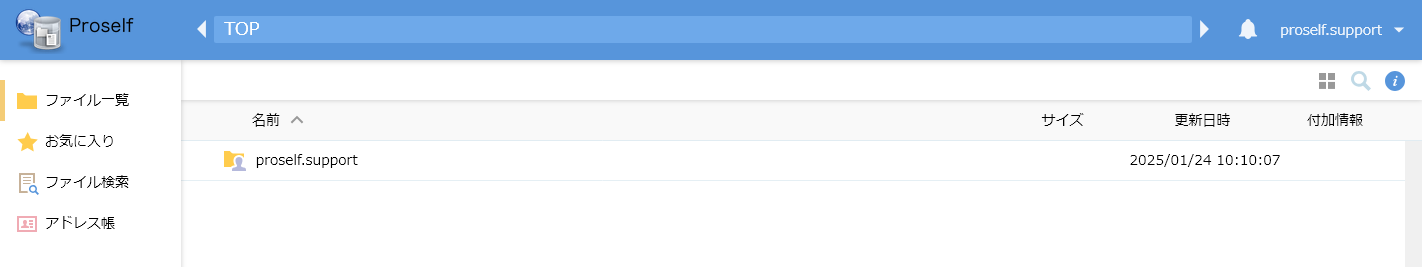
* 事前に「[2.2.2.SAML設定](#_SAML設定)」で「IdP Initiated SSO」を「on」に設定しておく必要があります。

Google管理コンソールにログイン後、アプリ詳細画面内にある「SAML ログインをテスト」をクリックします。



**SAMLログインをテスト**

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。



**Proselfログイン後の画面(ファイル一覧)**

### IdP証明書の更新

Google Workspaceの証明書を更新した場合、以下手順で更新済みのIdP証明書を手動でProselfにインポートする必要があります。

Webブラウザで「https://admin.google.com/」にアクセスし、Google Workspaceの管理者でログインします。



**Googleログイン**

ログイン後Google管理コンソールが表示されますので、左メニューより「アプリ」>「ウェブアプリとモバイルアプリ」の順にクリックします。



**Google管理コンソール**

「[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)」で作成したアプリ名の行をクリックします。



**Google管理コンソール**

アプリ詳細画面より「サービスプロバイダの詳細」をクリックします。



**Google管理コンソール**

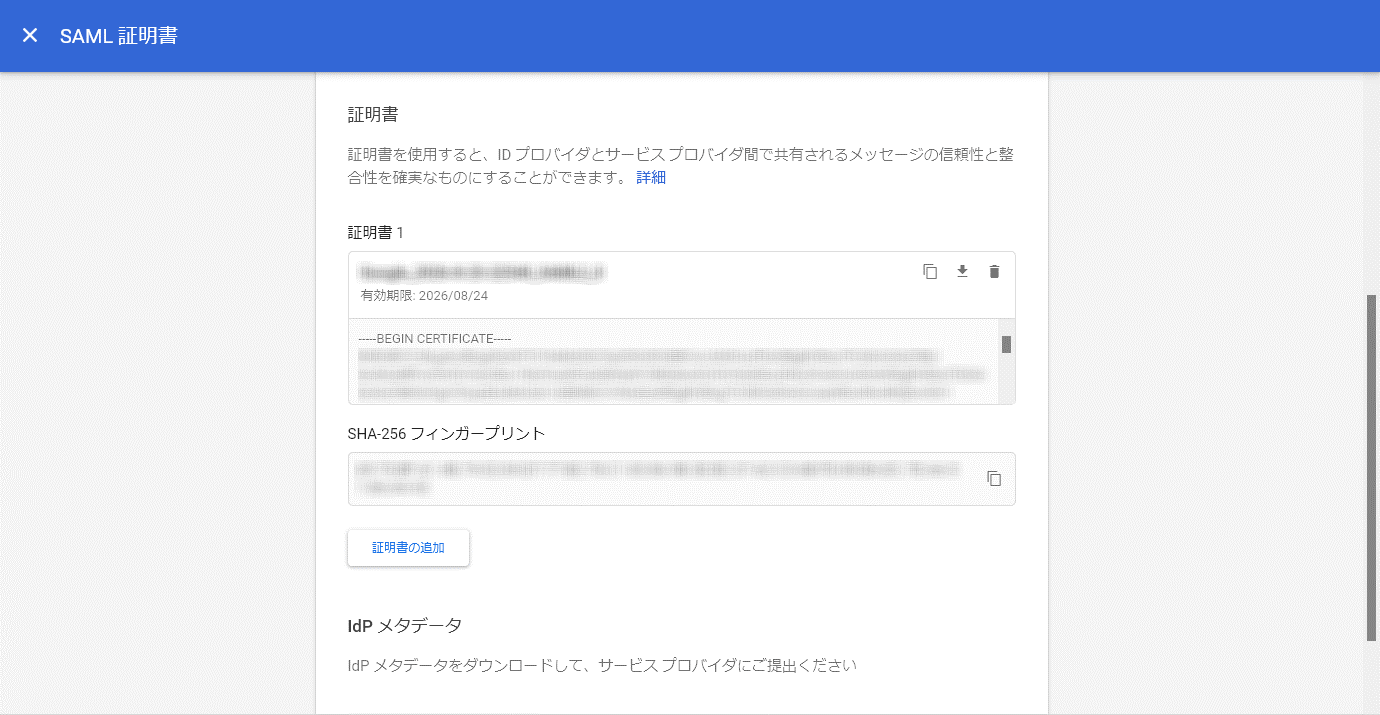
サービスプロバイダの詳細画面の「証明書」より「証明書を管理」をクリックします。



**Google管理コンソール**

SAML証明書画面に表示されている証明書よりコピーアイコンをクリックして証明書の内容をコピーします。

* ダウンロードアイコンをクリックして証明書内容をダウンロードしておくこともできます。



**SAML証明書**

Proselfの管理画面ホームより「SAML 設定」をクリックします。

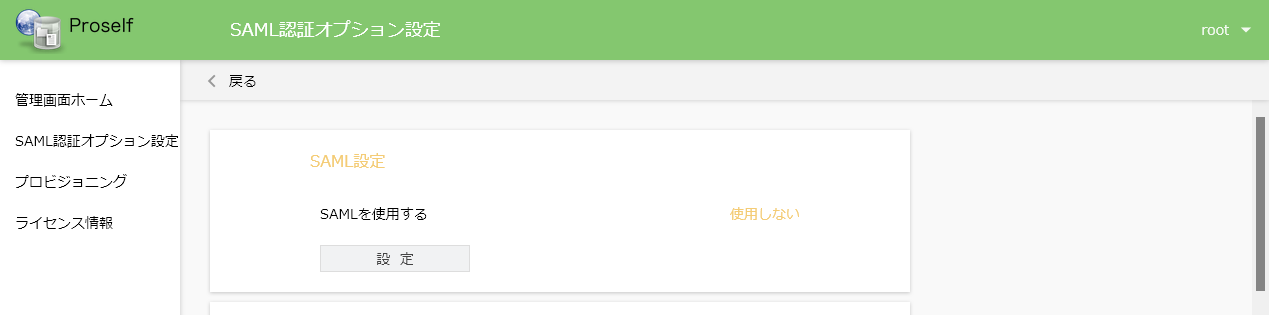


**管理画面**

SAML認証オプション設定＞SAML設定より「設定」をクリックします。



**SAML認証オプション設定**



**SAML認証オプション設定**

IdP証明書設定より「設定」をクリックします。



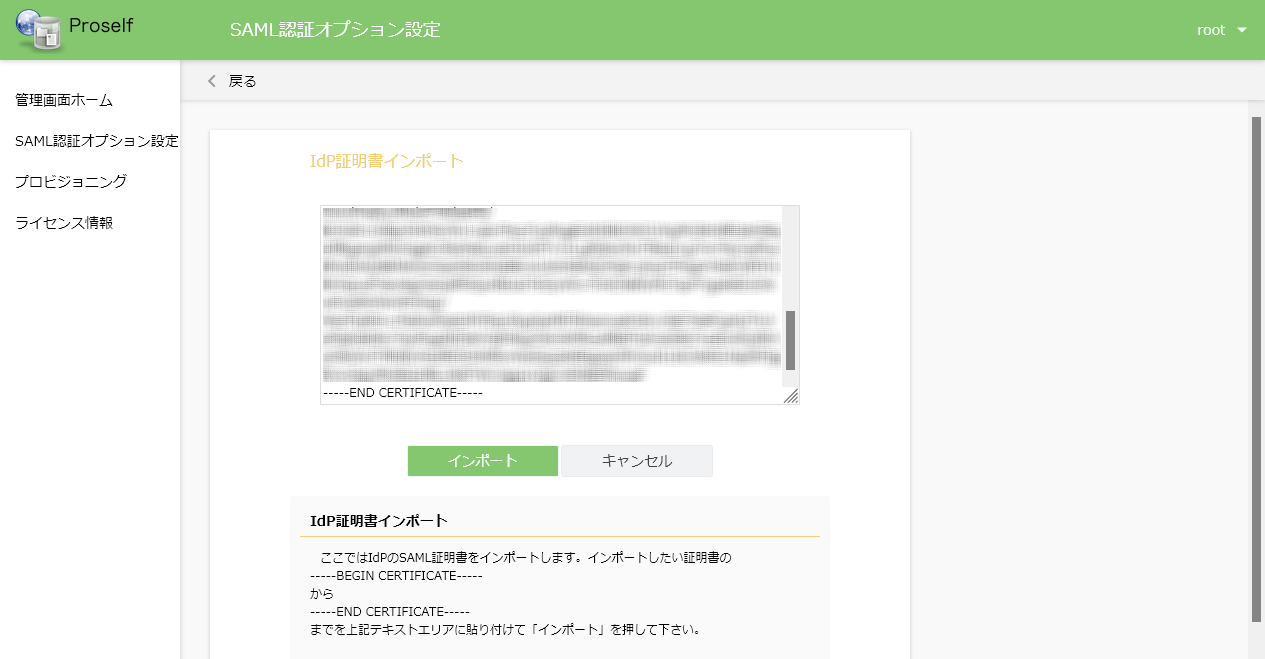
**SAML認証オプション設定**

IdP証明書インポートより「設定」をクリックします。



**IdP証明書設定**

Google Workspace上でコピーしておいた証明書の内容をテキストエリア内に貼り付け、「インポート」をクリックします。



**IdP証明書インポート**

インポートが正常に完了すると「証明書が正しくインポートされました」と表示されますので、画面上部の「戻る」をクリックします。



**IdP証明書設定**

SAML認証オプション設定のIdP証明書設定にインポートした証明書の概要が表示されます。



**SAML認証オプション設定**

# 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Google Workspaceから行う方法、Proselfから行う方法の2通りがあります。それぞれの方法については以下より記載しております。

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

* 事前に「[2.2.2.SAML設定](#_SAML設定)」で「IdP Initiated SSO」を「on」に設定しておく必要があります。

Webブラウザで「https://accounts.google.com/」にアクセスします。

Googleにサインインしていない場合はログイン画面が表示されますので、「[2.1.2.ユーザーアクセスの設定](#_ユーザーアクセスの設定)」によりアプリにアクセス可能なユーザーでログインします。



**Googleログイン**

パスワード入力後、表示されたGoogleアカウントページの右上にあるGoogleアプリ (9つの点が描かれたアイコン)をクリックします。



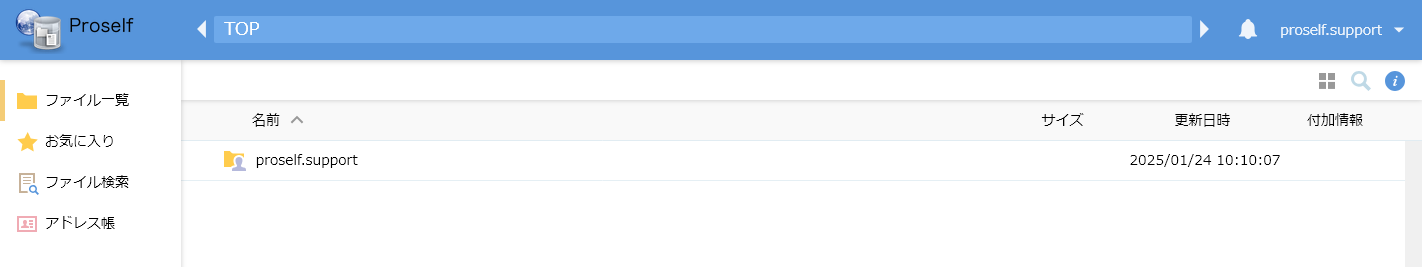
**Googleアカウントページ**

Googleアプリの一覧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)」で作成した「Proself\_saml」をクリックします。



**Googleアプリの一覧**

Proselfログイン後の画面が表示されます。



**Proself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。



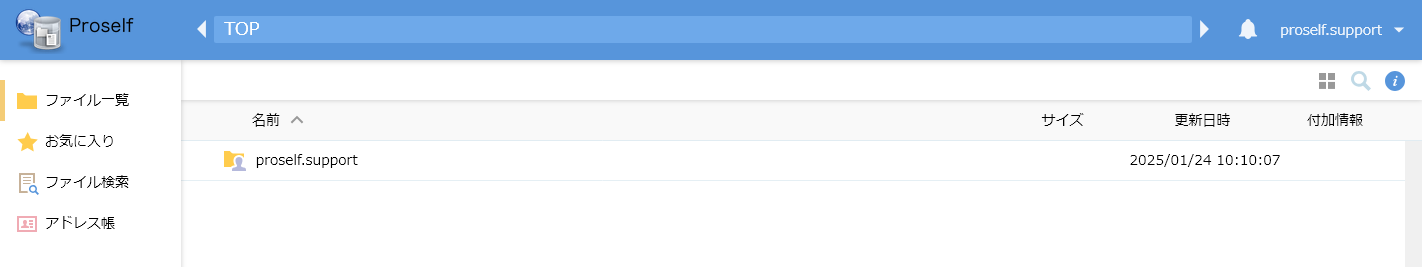
**ログイン画面**

Googleにログインしていない場合はログイン画面が表示されますので、ログインに使用するアカウントを選択します。



**Googleログイン画面**

パスワード入力後、シングルサインオンが行われProselfログイン後の画面が表示されます。



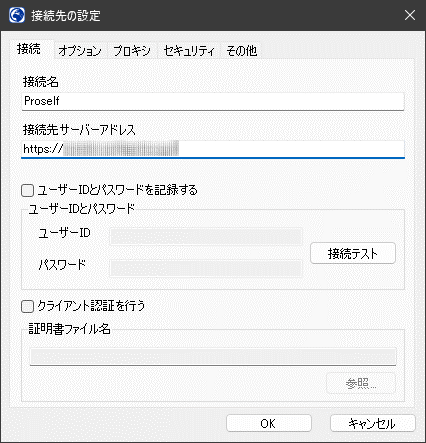
**Proselfログイン後の画面(ファイル一覧)**

## 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。

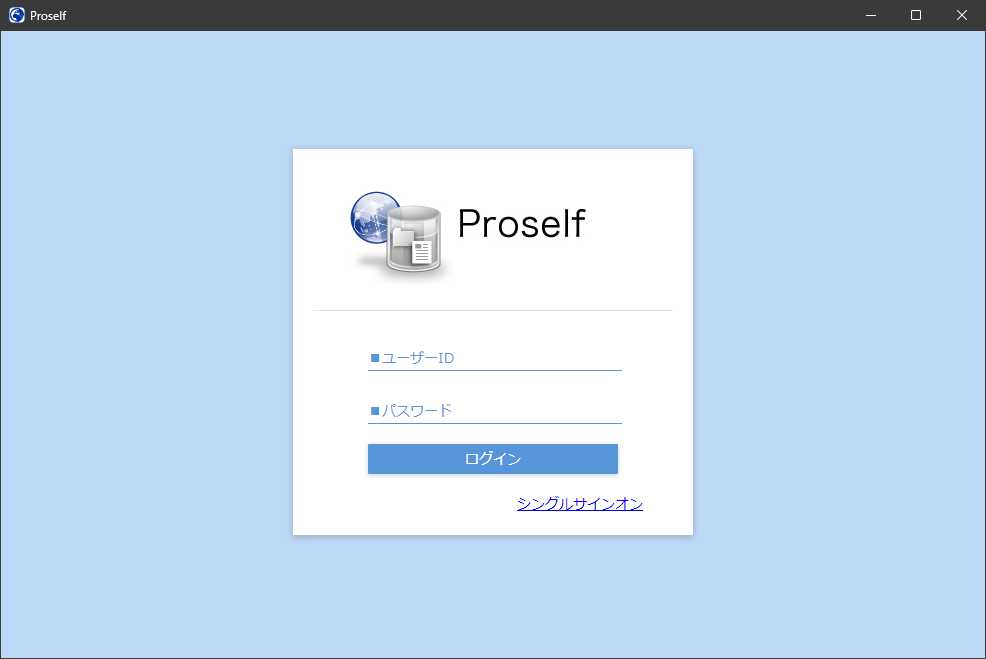
| 項目 | 入力内容 |
| --- | --- |
| 接続名 | 接続先の名前を入力します。 |
| 接続先サーバーアドレス | 以下を入力します。  https://[サーバーアドレス]/  [サーバーアドレス]には Proself をインストールしたサーバーの IP アドレスまたはFQDN(完全修飾ドメイン名)を入力します。 |
| ユーザーIDとパスワードを記録する | チェックOFFにします。 |

設定後「OK」をクリックするとWebViewでGoogleのログインページが表示されますので、「[2.1.2.ユーザーアクセスの設定](#_ユーザーアクセスの設定)」によりアプリにアクセス可能なユーザーでログインします。



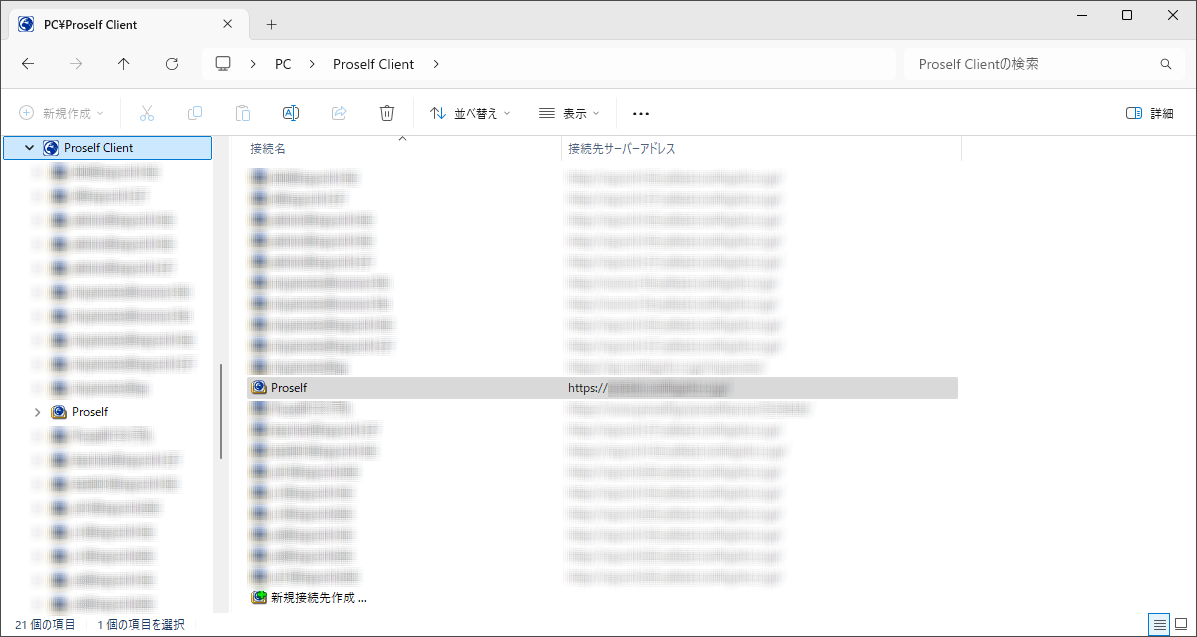
**Googleログイン画面**

* 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。



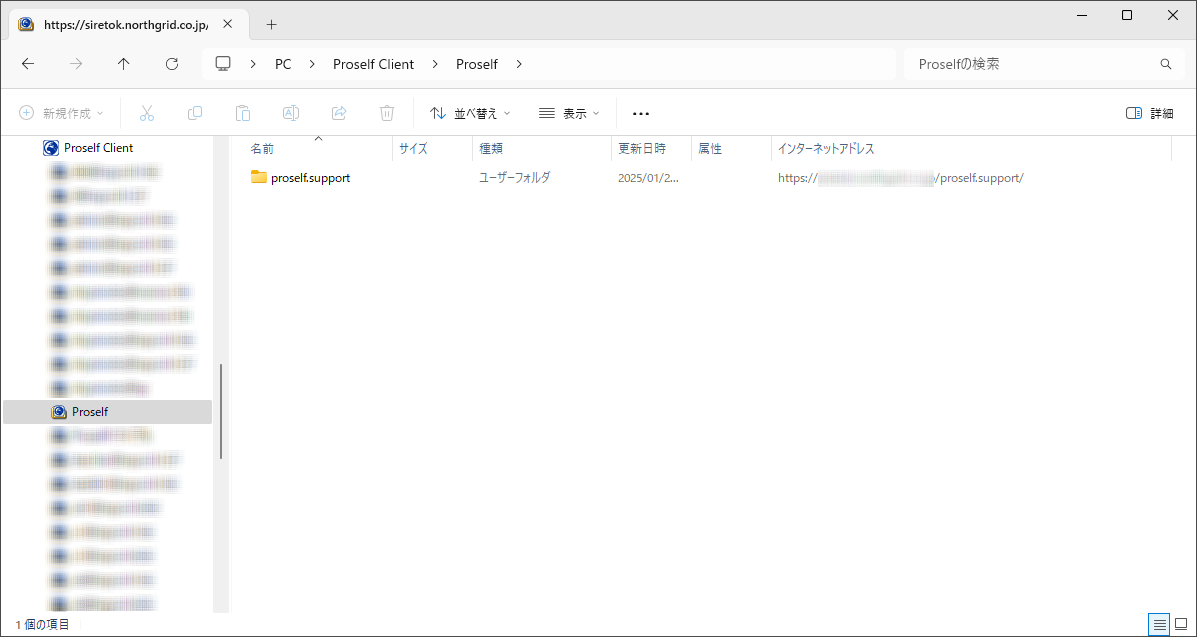
**Proselfログイン画面**

ログ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**