|  |
| --- |
| 第1版  2023/09/12 |

|  |
| --- |
| インストールガイドVer |
| **操作チュートリアル**  **Active Directory Federation Services連携編** |
|  |

目次

[1. 概要 1](#_Toc145349852)

[2. ADFSを使用したSAML設定手順 1](#_Toc145349853)

[2.1. Proselfでの設定 1](#_Toc145349854)

[2.1.1. このサーバー情報の設定 1](#_Toc145349855)

[2.1.2. SAML設定 3](#_Toc145349856)

[2.1.3. SP証明書設定 5](#_Toc145349857)

[2.1.4. IdP証明書自動更新設定 6](#_Toc145349858)

[2.1.5. IdP設定用データの保存 7](#_Toc145349859)

[2.1.6. LDAP連携設定 8](#_Toc145349860)

[2.2. ADFSでの設定 9](#_Toc145349861)

[2.2.1. 証明書利用者信頼の追加 9](#_Toc145349862)

[2.2.2. 要求発行ポリシーの追加 16](#_Toc145349863)

[3. シングルサインオン 23](#_Toc145349864)

[3.1. ADFSからのシングルサインオン(IdP Initiated) 23](#_Toc145349865)

[3.2. Proselfからのシングルサインオン(SP initiated) 25](#_Toc145349866)

# 概要

本チュートリアルは、Active Directory Federation Services(以下ADFSと記載)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。
* ADFSはあらかじめお客様にてご用意いただいていることを前提としております。

# ADFSを使用したSAML設定手順

ADFSを使用したSAML設定手順を記載します。

「[2.1.Proselfでの設定](#_Proselfでの設定)」、「[2.2.ADFSでの設定](#_ADFSでの設定)」の順に設定を行います。

## 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設定」の「設定」をクリックします。



**SAML認証オプション設定**

「SAMLを使用する」、「エンドポイントURL」、「IdP Initiated SSO」、「ユーザー属性 ユーザーIDのキー名」、「認証要求のNameIDポリシー」をそれぞれ設定して「設定」をクリックします。



**SAML設定**

各項目には以下のように入力します。

| 項目 | 入力内容 |
| --- | --- |
| SAMLを使用する | 「使用する」を選択します。 |
| エンドポイントURL | 「https://[サーバーアドレス]/adfs/ls」を入力します。   * [サーバーアドレス]にはADFS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。 |
| IdP Initiated SSO | IdP Initiatedを有効にする場合は「on」にします。 |
| ユーザー属性 ユーザーIDのキー名 | 「proselfid」を入力します。 |
| 認証要求のNameIDポリシー | 「urn:oasis:names:tc:SAML:2.0:nameid-format:transient」を選択します。 |

### 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)内の「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**

「IdP証明書を自動的に更新する」を「on」、「IdPメタデータ取得URL」を「https://[サーバーアドレス]/FederationMetadata/2007-06/FederationMetadata.xml」と入力して「設定」ボタンをクリックします。

* [サーバーアドレス]にはADFS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。



20

**IdP証明書自動更新設定**

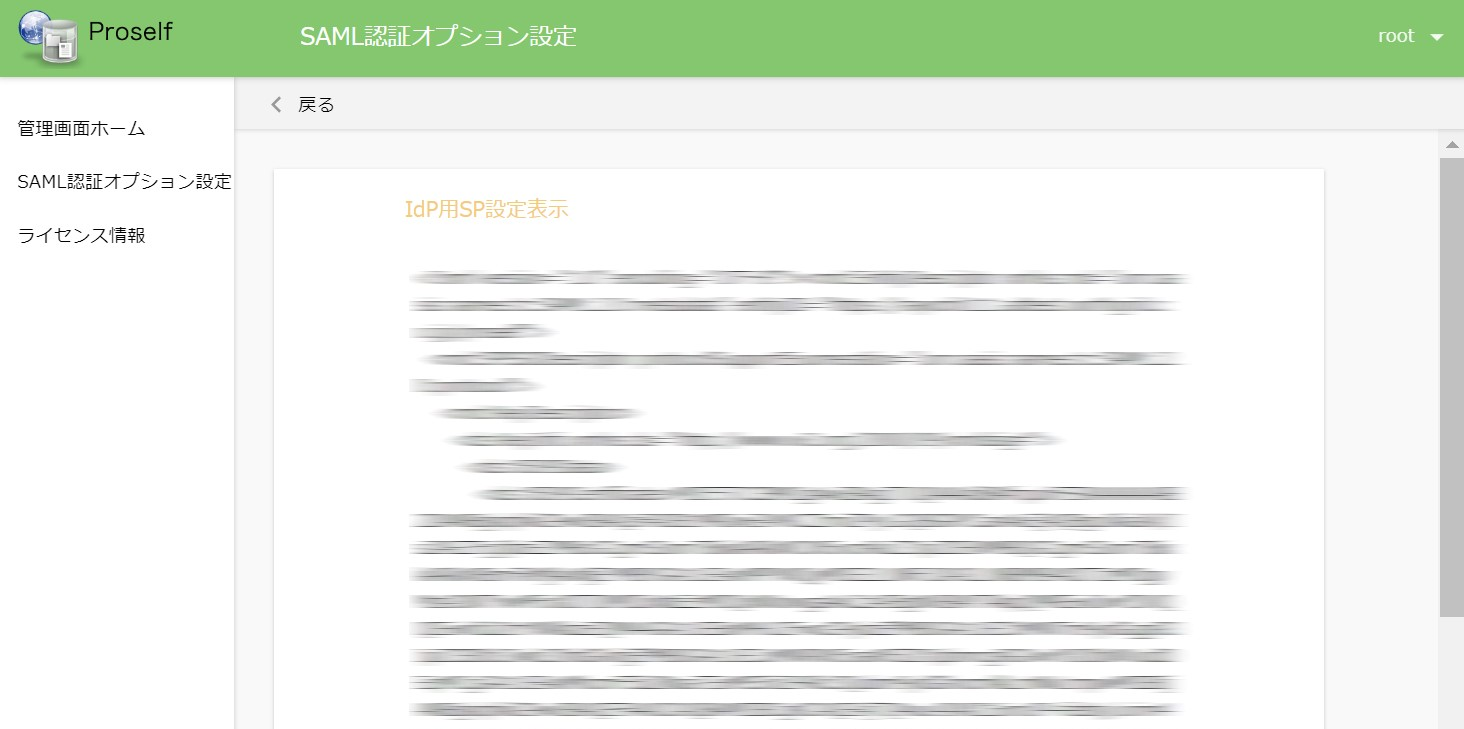
### IdP設定用データの保存

SPの設定をIdPに登録する為のxmlファイルを保存します。SAML認証オプション設定から「IdP用SP設定表示」の「設定」をクリックします。



**SAML認証オプション設定**

IdP設定用のメタデータが表示されますので、画面内のメタデータをxmlファイルとして保存し、ADFSサーバー上の任意の場所に配置します。ここでは保存したファイル名を「SP.xml」としてADFSサーバーの「C:\Temp」配下に配置します。



**IdP用SP設定表示**

### LDAP連携設定

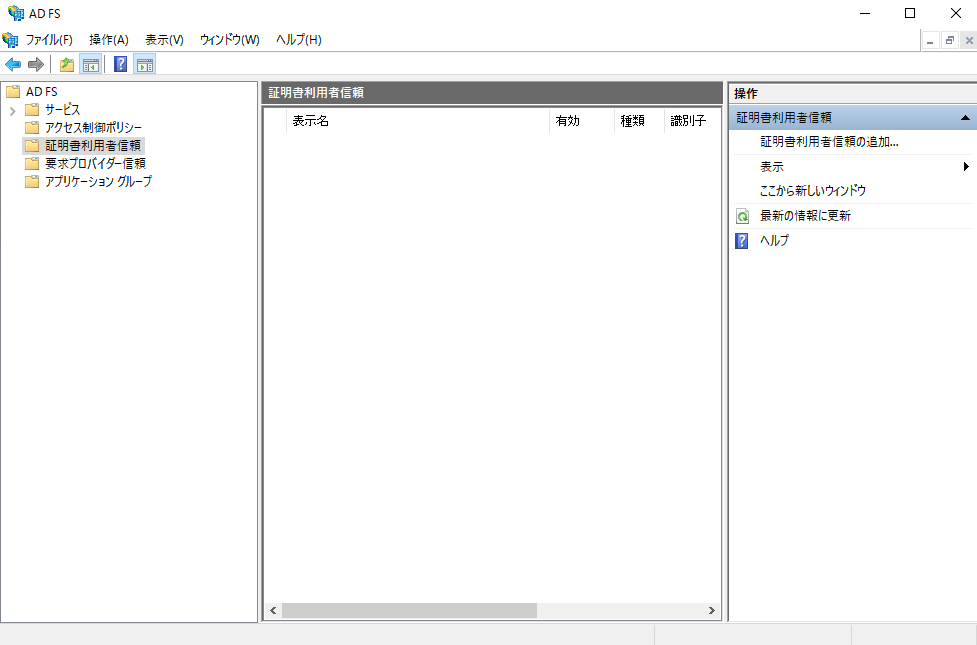
ADFSを使用してシングルサインオンを行うための準備として、Active Directoryに作成したユーザーをProselfに取り込む必要があります。

詳細につきましては、Proselfのインストールメディアに同梱している管理ガイド(AdminGuide.pdf)内の「LDAP / Active Directory 設定マニュアル」の項をご参照ください。

## ADFSでの設定

### 証明書利用者信頼の追加

「AD FSの管理」を起動して左メニューの「証明書利用者信頼」をクリックして右メニューの「証明書利用者信頼の追加」をクリックします。



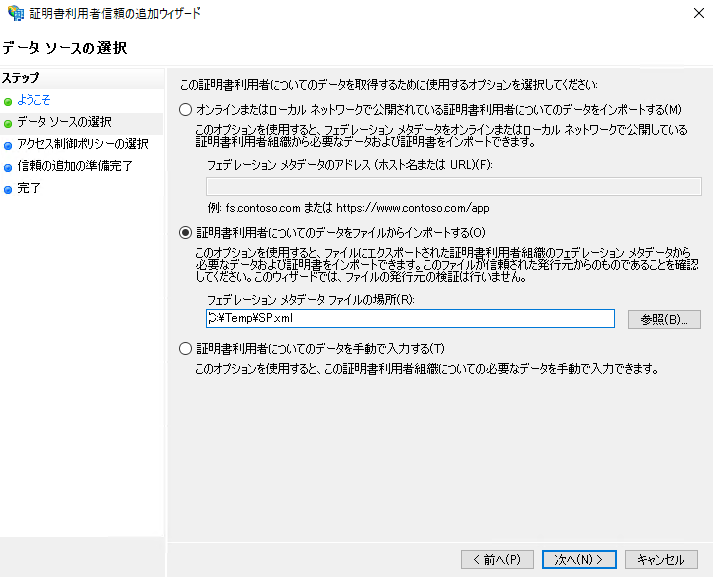
**ADFS**

「証明書利用者信頼の追加ウィザード」画面が開き、選択肢で「要求に対応する」を選択して「開始」をクリックします。



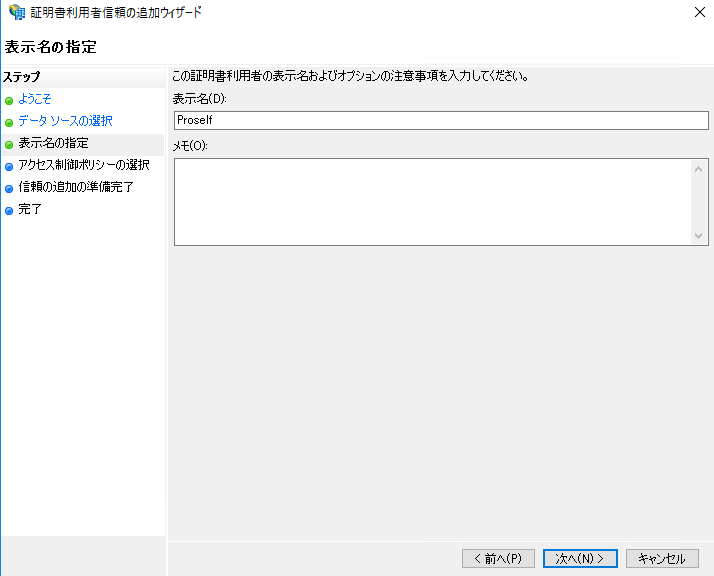
**証明書利用者信頼の追加ウィザード**

「証明書利用者についてのデータをファイルからインポートする」を選択して、「[2.1.5. IdP設定用データの保存](#_IdP設定用データの保存)」で配置したxmlファイルを指定した後、「次へ」をクリックします。



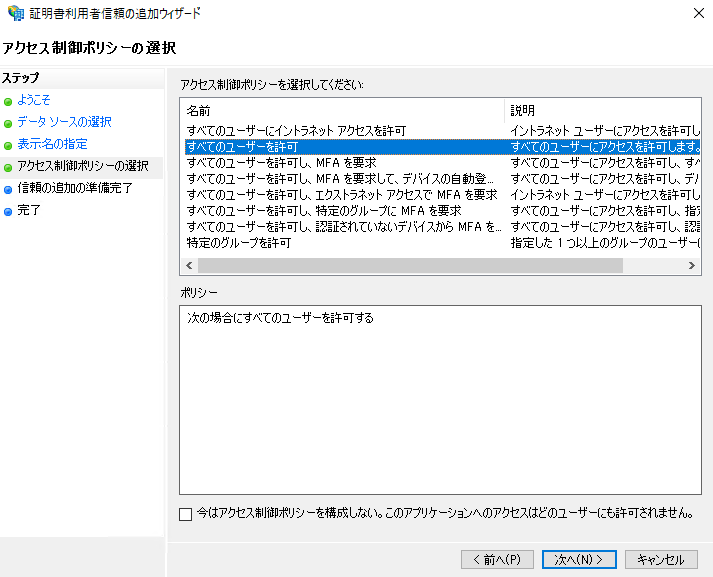
**証明書利用者信頼の追加ウィザード**

任意の表示名を入力して「次へ」をクリックします。ここでは表示名を「Proself」とします。



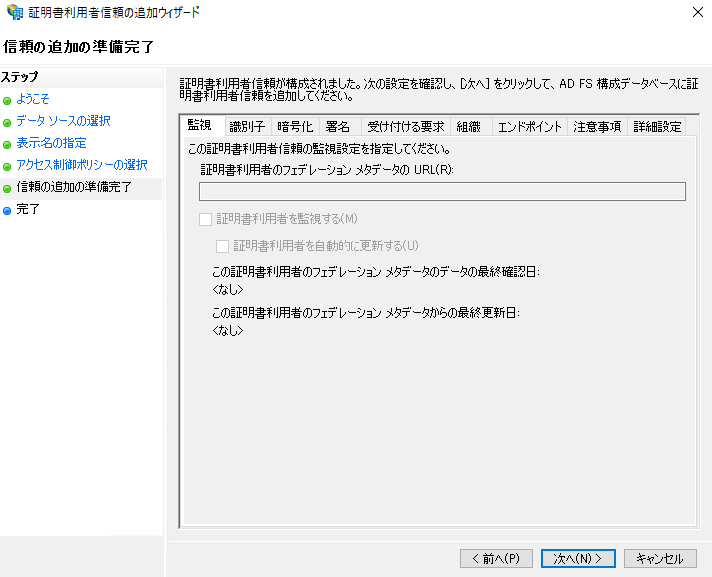
**証明書利用者信頼の追加ウィザード**

「アクセス制御ポリシーの選択」において「すべてのユーザーを許可」を選択して「次へ」をクリックします。



**証明書利用者信頼の追加ウィザード**

「信頼の追加の準備完了」が表示されるので内容を確認し問題なければ「次へ」をクリックします。



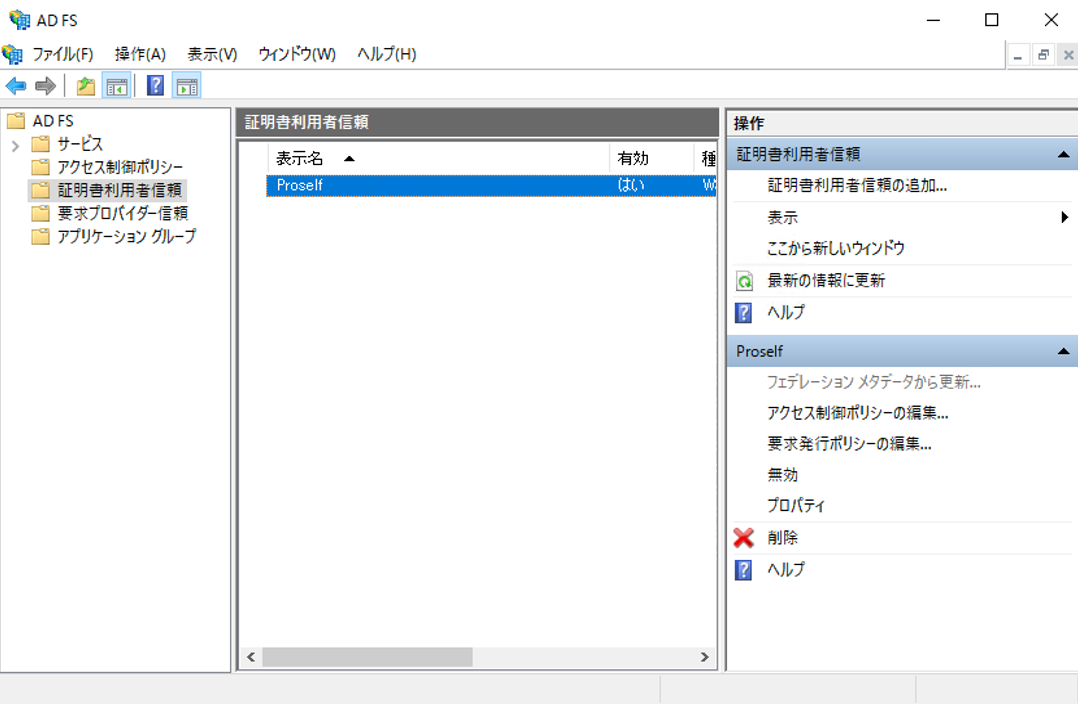
**証明書利用者信頼の追加ウィザード**

証明書利用者信頼が追加されるので「このアプリケーションの要求発行ポリシーを構成する」にチェックを入れて「閉じる」をクリックします。



**証明書利用者信頼の追加ウィザード**

「このアプリケーションの要求発行ポリシーを構成する」にチェックを入れず「閉じる」をクリックした場合は以下の通り表示名を選択後、右側の操作メニューで「要求発行ポリシーの編集」をクリックして「[2.2.2. 要求発行ポリシーの追加](#_要求発行ポリシーの追加)」に進んでください。



**ADFS**

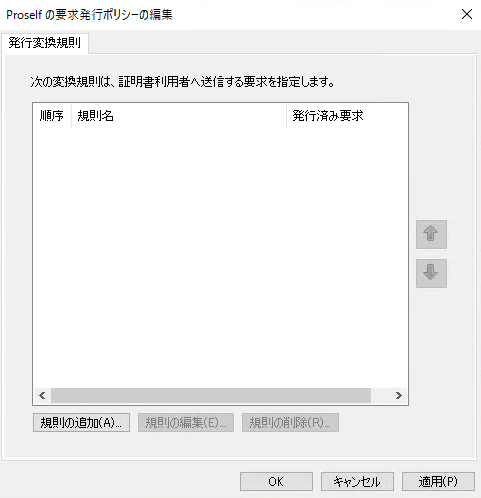
### 要求発行ポリシーの追加

以下の要求規則テンプレートを使用した規則を2つ追加します。

・入力方向の要求を変換

・LDAP属性を要求として送信

以下の「要求発行ポリシーの編集」画面で「規則の追加」をクリックします。



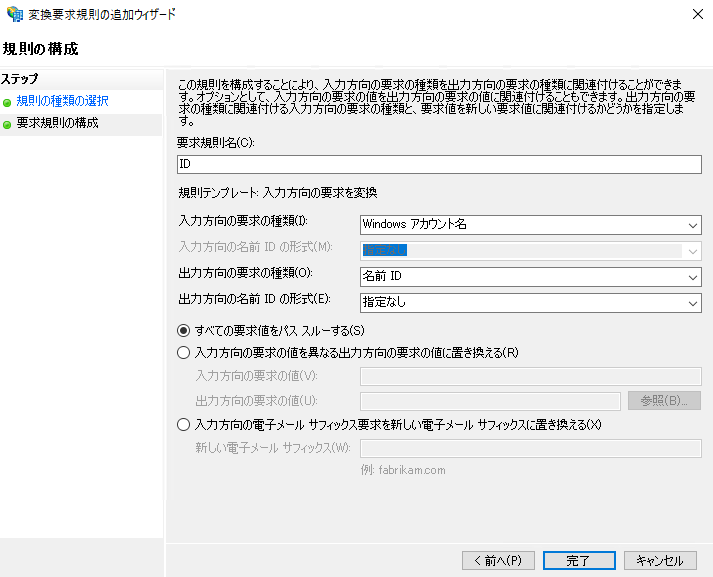
**要求発行ポリシーの編集**

「要求規則テンプレート」で「入力方向の要求を変換」を選択して「次へ」をクリックします。



**変換要求規則の追加ウィザード**

「要求規則名」、「入力方向の要求の種類」、「出力方向の要求の種類」、「出力方向の名前IDの形式」をそれぞれ設定して「完了」をクリックします。

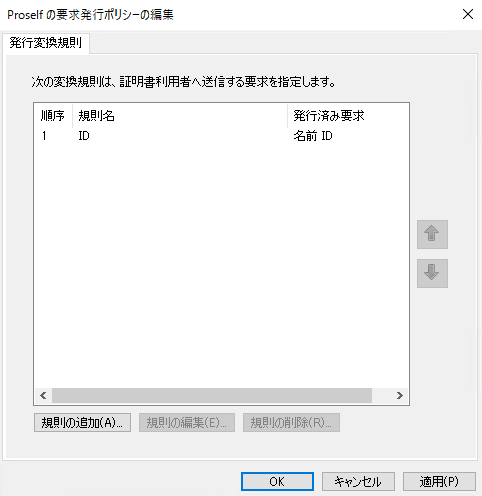


**証明書利用者信頼の追加ウィザード**

各項目には以下のように入力します。

| 項目 | 入力内容 |
| --- | --- |
| 要求規則名 | 任意の要求規則名を入力します。ここでは「ID」とします。 |
| 入力方向の要求の種類 | 「Windows アカウント名」を選択します。 |
| 出力方向の要求の種類 | 「名前 ID」を選択します。 |
| 出力方向の名前ID の形式 | 「一時 ID」を選択します。 |

規則が追加されたのを確認後、再度「規則の追加」をクリックします。



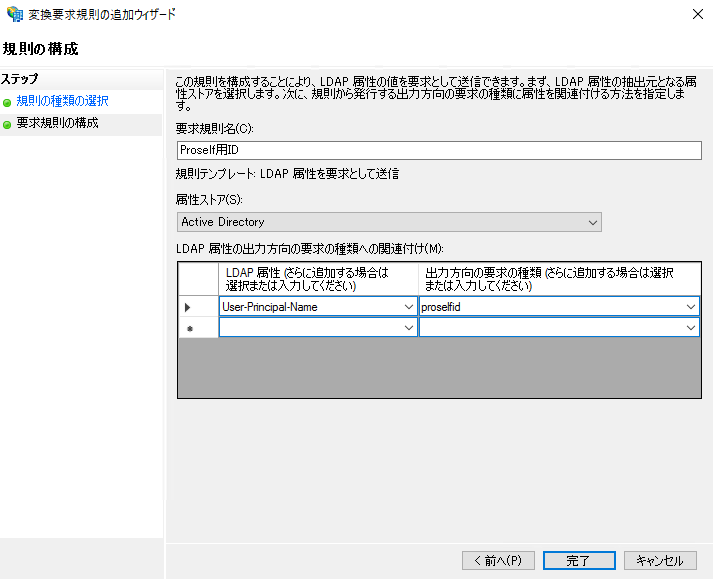
**要求発行ポリシーの編集**

「要求規則テンプレート」で「LDAP属性を要求として送信」を選択して「次へ」をクリックします。



**変換要求規則の追加ウィザード**

「要求規則名」、「属性ストア」、「LDAP属性」、「出力方向の要求の種類」をそれぞれ設定して「完了」をクリックします。



**要求発行ポリシーの編集**

各項目には以下のように入力します。

| 項目 | 入力内容 |
| --- | --- |
| 要求規則名 | 任意の要求規則名を入力します。ここでは「Proself用ID」とします。 |
| 属性ストア | 「Active Directory」を選択します。 |
| LDAP属性 | 「User-Princial-Name」を選択します。 |
| 出力方向の要求の種類 | 「[2.1.2. SAML設定](#_SAML設定)」で「ユーザー属性 ユーザーIDのキー名」に設定した「proselfid」を入力します。 |

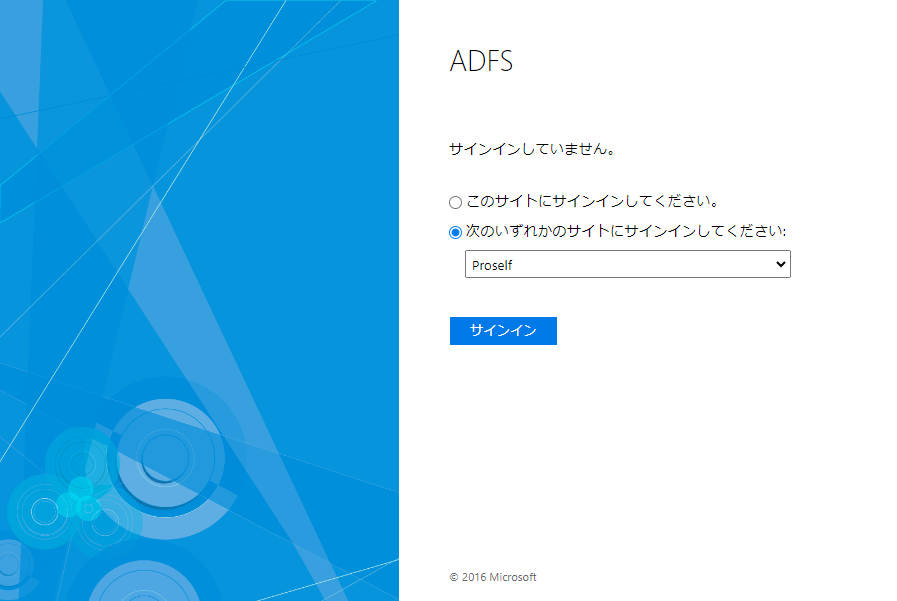
# シングルサインオン

シングルサインオンの方法としてはADFSから行う方法、Proselfから行う方法の2通りがあります。

## ADFSからのシングルサインオン(IdP Initiated)

Webブラウザで「https://[サーバーアドレス]/adfs/ls/IdpInitiatedSignOn.aspx」にアクセスし、「次のいずれかのサイトにサインインしてください」を選択して、リストから「[2.2.1. 証明書利用者信頼の追加](#_証明書利用者信頼の追加)」で指定した証明書利用者の表示名を選択して、「サインイン」をクリックします。

* [サーバーアドレス]にはADFS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。



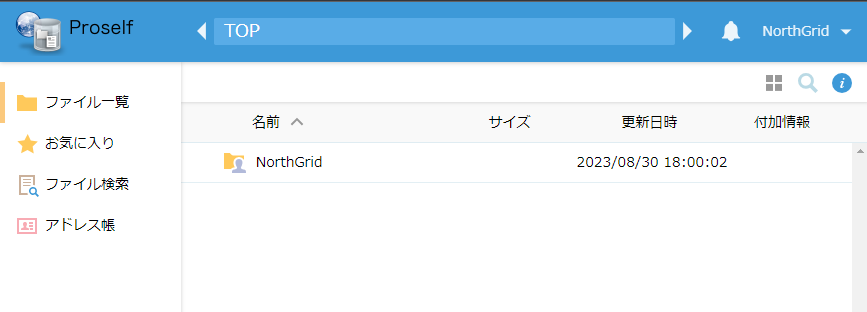
**サインイン**

LDAPサーバーに同期して作成したLDAPユーザーのユーザー ID、パスワードを入力して「サインイン」をクリックします。ユーザーIDは「ドメイン名\ユーザーID」または「ユーザーID@ドメイン名」形式で入力します。



**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**

LDAPサーバーに同期して作成したLDAPユーザーのユーザーID、パスワードを入力して「サインイン」をクリックします。ユーザーIDは「ドメイン名\ユーザーID」または「ユーザーID@ドメイン名」形式で入力します。



**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)**