ArcGIS Online / ArcGIS Enterprise - Active Directory Federation Service 連携ガイド

esri ジャパン

目次

1. はじめに

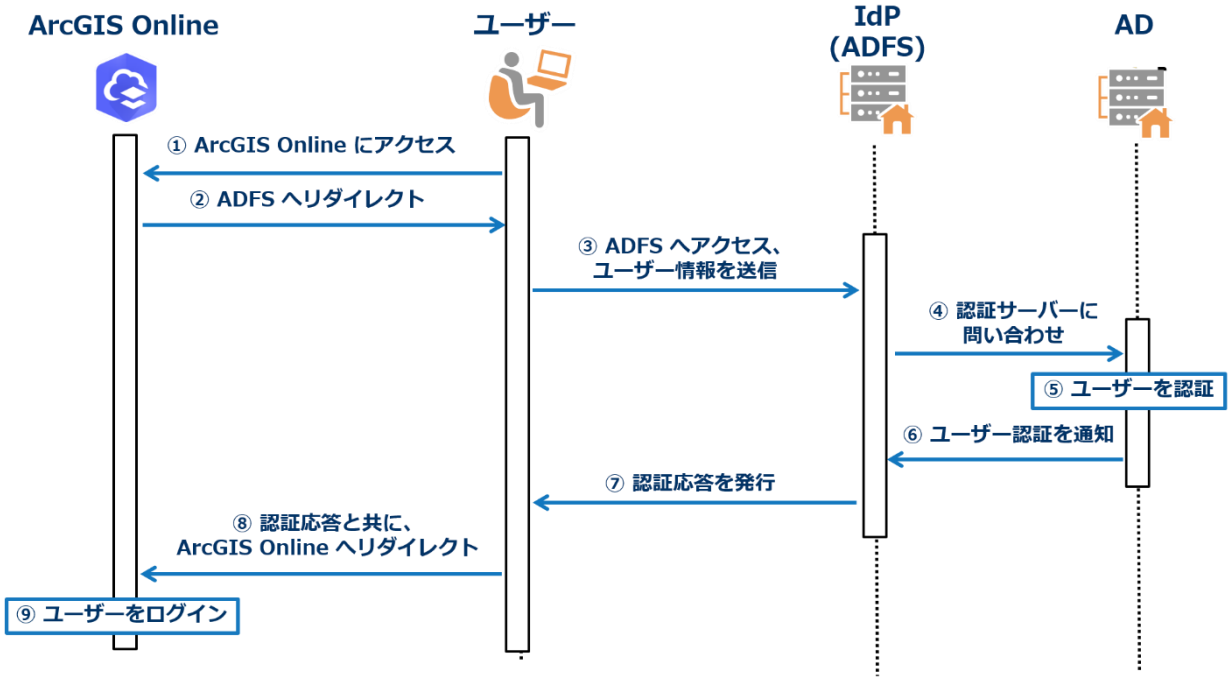
1.1. 本ガイドについて

Active Directory Federation Service（以下、ADFS） は、組織内で使用している Active Directory（以下、AD）の ID を使用して、アプリケーションやクラウド サービスへのシングル サインオン（以下、SSO）を実現する Microsoft のソリューションです。ArcGIS Online / ArcGIS Enterprise では、ADFS と連携することで、組織内の AD で使用している ID による SSO を行うことが出来ます。本ガイドでは、ADFS を用いた ArcGIS Online / ArcGIS Enterprise への SSO が可能になるまでの手順について紹介します。

※ ADFS 以外を使用した ID プロバイダー（Idp）については、ArcGIS Online 公式ガイドの SAML IDP を参照してください。

ArcGIS Online / ArcGIS Enterprise は、エンタープライズ ログインのアカウント構成に SAML (Security Assertion Markup Language) 2.0 をサポートしています。SAML は、認証サーバーである ID プロバイダー（Idp：本ガイドでは ADFS が該当）とサービスを提供するアプリケーションであるサービス プロバイダー（SP：本ガイドでは ArcGIS Online / ArcGIS Enterprise が該当）との間で認証/認可データを安全に交換するためのオープン規格です。ArcGIS Online / ArcGIS Enterprise は SAML 2.0 に準拠しており、この規格に準拠する Idp と統合することができます。本ガイドで紹介する ADFS は SAML 2.0 に準拠しているので、Idp として ArcGIS Online / ArcGIS Enterprise で使用することができます。
エンタープライズ ログインを構成することで、組織サイトのメンバーは、エンタープライズ システムにアクセスするときと同一のログイン情報（1 つの ID・パスワード）を使用して ArcGIS Online / ArcGIS Enterprise に SSO でログインすることが可能となります。また、ID・パスワードの再入力を行わずに利用できる環境を実現することができます。

ユーザーが ArcGIS Online にアクセスして SSO するまでの流れを下記に示します（ArcGIS Enterprise の場合も同様です）。



① ユーザーが ArcGIS Online にアクセスします。
② ArcGIS Online は認証要求と共にリクエストを ADFS へリダイレクトします。
③ ユーザーは ADFS へアクセスし、ユーザー情報を ADFS に送信します。
④ ADFS は認証要求を受けると、ユーザーやコンピューターの情報を集中管理する Windows Active Directory（以下、AD）へユーザー情報を送信します。
⑤ AD はユーザーを認証します。
⑥ ユーザー認証を ADFS へ通知します。
⑦ ユーザーが認証されたことを ADFS が確認した後、ADFS はアサーション（認証応答）を発行し、ユーザーに送信します。
⑧ ユーザーは ADFS から送られたアサーションとともに、ArcGIS Online へリダイレクトします。
⑨ ArcGIS Online はアサーションを確認した後、ユーザーをログインさせます。

1.2. 環境情報

本ガイドで使用する ADFS および AD の環境情報を以下に記載します。なお、連携の手順では、ArcGIS

Online / ArcGIS Enterprise 上での設定に加えて、ADFS への設定も行いますが、本ガイドではこれらの設定は ADFS をインストールしている端末（Windows Server 2019）で行います。

環境情報	内容	備考
ADFS をインストールしているマシンの OS	Windows Server 2019	
ADFS マシン名	adfsserver.ppsej.co.jp	
AD をインストールしているマシンの OS	Windows Server 2019	

2. ArcGIS Online / ArcGIS Enterprise と ADFS の連携設定

本章では、ArcGIS Online / ArcGIS Enterprise と ADFS を連携させるための設定の手順について説明します。本ガイドで記載している手順は、ADFS をインストールした端末上で行います。連携までの手順は以下になります。なお、以下に記載している設定画面は、 ArcGIS Online は 2020 年 7 月時点での画面、ArcGIS Enterprise はバージョン 10.8 時点での画面であり、今後のアップデートで変更される場合もあります。

2.1. ArcGIS Online / ArcGIS Enterprise に ADFS を Idp として登録

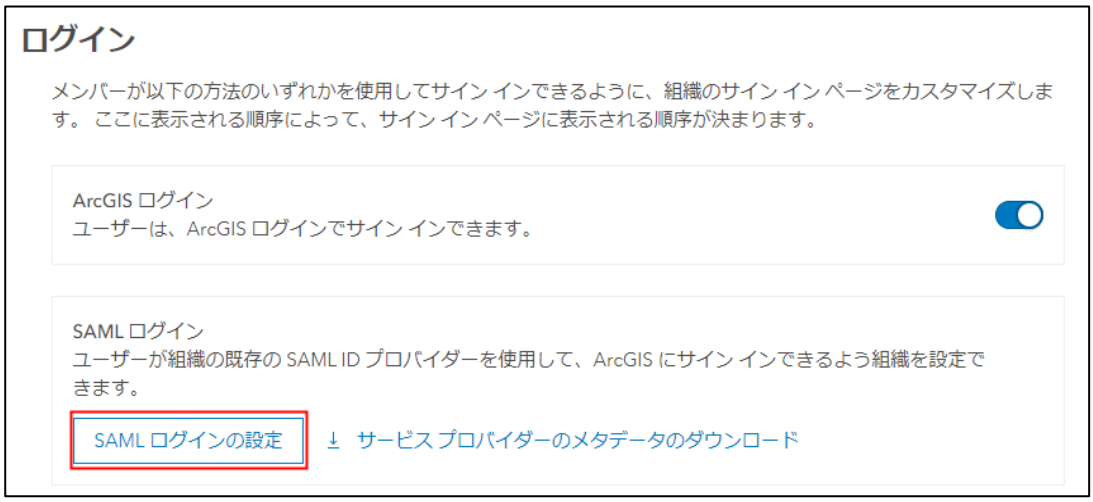
ADFS をエンタープライズ Idp として ArcGIS Online / ArcGIS Enterprise に登録します。以下では、ArcGIS Online と ArcGIS Enterprise の場合に分けて、手順を記載します。

・ArcGIS Online に ADFS を Idp として登録

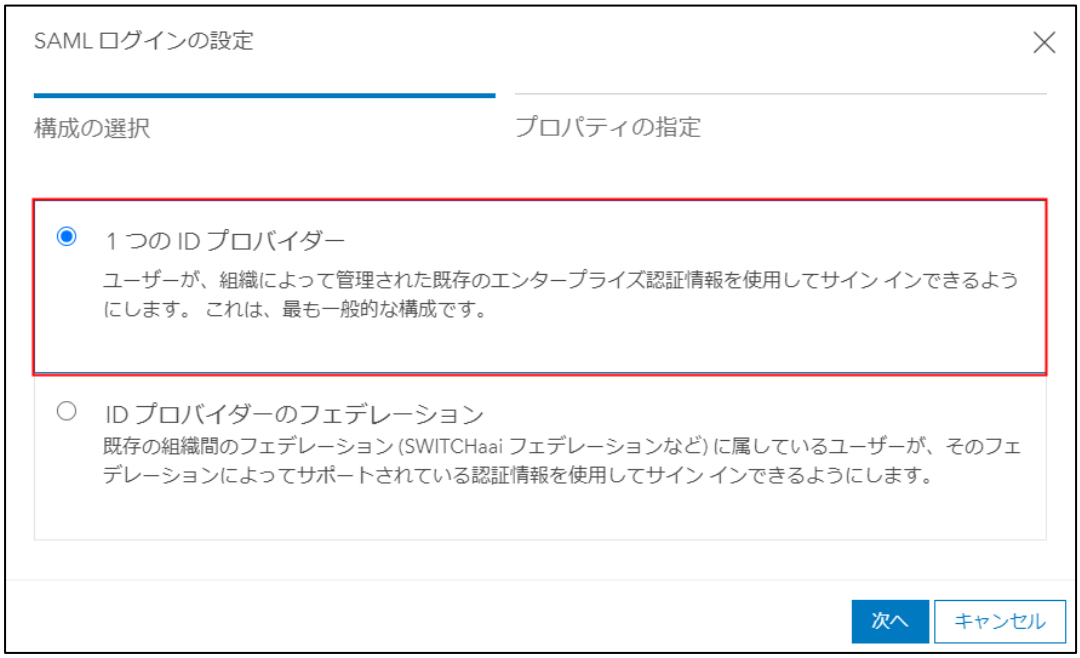
1. 以下の URL にアクセスし、ADFS のメタデータを取得します。
   https://<ADFS マシン名>/ FederationMetadata/2007-06/FederationMetadata.xml
   例：https://adfsserver.ppsej.co.jp/FederationMetadata/2007-06/FederationMetadata.xml

2. ArcGIS Online で管理者権限のあるユーザーでログイン後、[組織] → [設定] → [セキュリティ] を選択します。

3. [ログイン] セクションで、[SAML ログインの設定] オプションを選択します。



4. [1 つの ID プロバイダー] を選択します。



5. [ID プロバイダーの設定] ウィンドウが表示されます。このウィンドウでは、任意の名前を入力し、ユーザーが [自動] または [管理者から招待されたとき] のどちらで組織に加入できるかを選択します（入力した名前は、SAML ログイン ボタンに表示されます)。メタデータソースに [ファイル] を選択し、手順 1 で取得した ADFS のメタデータ ファイルを選択します。[高度な設定を表示] についてはデフォルト設定です。こちらの ID プロバイダーの設定は、あとで編集も可能です。内容に問題がなければ IP プロバイダーの設定をクリックして設定を反映します。

6. 設定反映後は以下のような画面になります。設定を変更する場合は、編集ボタン（下図赤枠の鉛筆ボタン）をクリックします。

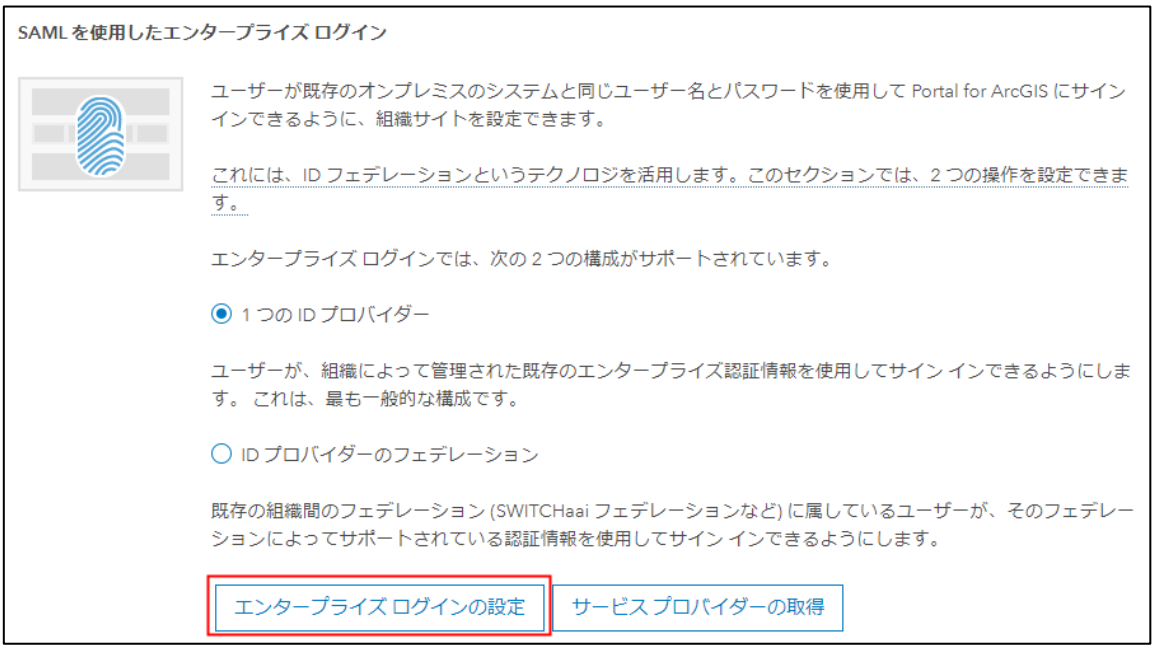
7. 編集ボタンをクリックすると次のような ID プロバイダーの編集画面が表示されますので、必要に応じて設定を行ってください。ログインと同時にユーザーを ArcGIS Online の組織サイト

に加入させる場合は、[ユーザーは次の条件で加入できます] 下の [自動] を選択します（本ガイドでは [自動] と設定しました）。

・ArcGIS Enterprise に ADFS を Idp として登録

1. 以下の URL にアクセスし、ADFS のメタデータを取得します。
   https://<ADFS マシン名>/FederationMetadata/2007-06/FederationMetadata.xml
   例：https://adfsserver.ppsej.co.jp/FederationMetadata/2007-06/FederationMetadata.xml

2. ArcGIS Enterprise で管理者権限のあるユーザーでログイン後、[組織] → [設定] → [セキュリティ] を選択します。
3. [SAML を使用したエンタープライズ ログイン] セクションで、[エンタープライズ ログインの設定] をクリックします。



4. [ID プロバイダーの設定] ウィンドウが表示されます。ArcGIS Online での手順と同様、任意の名前を入力し、ユーザーが [自動] または [管理者から招待されたとき] のどちらで組織に加入できるかを選択します。メタデータソースに [ファイル] を選択し、手順 1 で取得した ADFS のメタデータ ファイルを選択します。

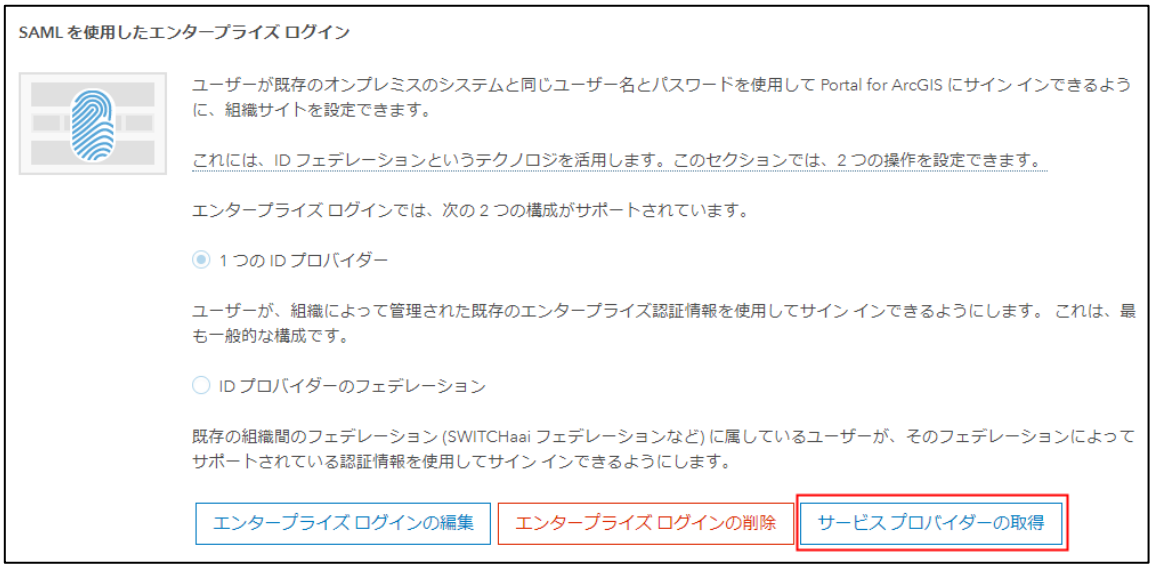
2.2. ADFS に ArcGIS Online / ArcGIS Enterprise を SP として登録

ArcGIS Online / ArcGIS Enterprise を信頼できるサービス プロバイダー（SP）として ADFS に登録します。以下に、ADFS に ArcGIS Online / ArcGIS Enterprise を SP として登録する手順を記載します。

5. ArcGIS Online / ArcGIS Enterprise のメタデータをダウンロードします。

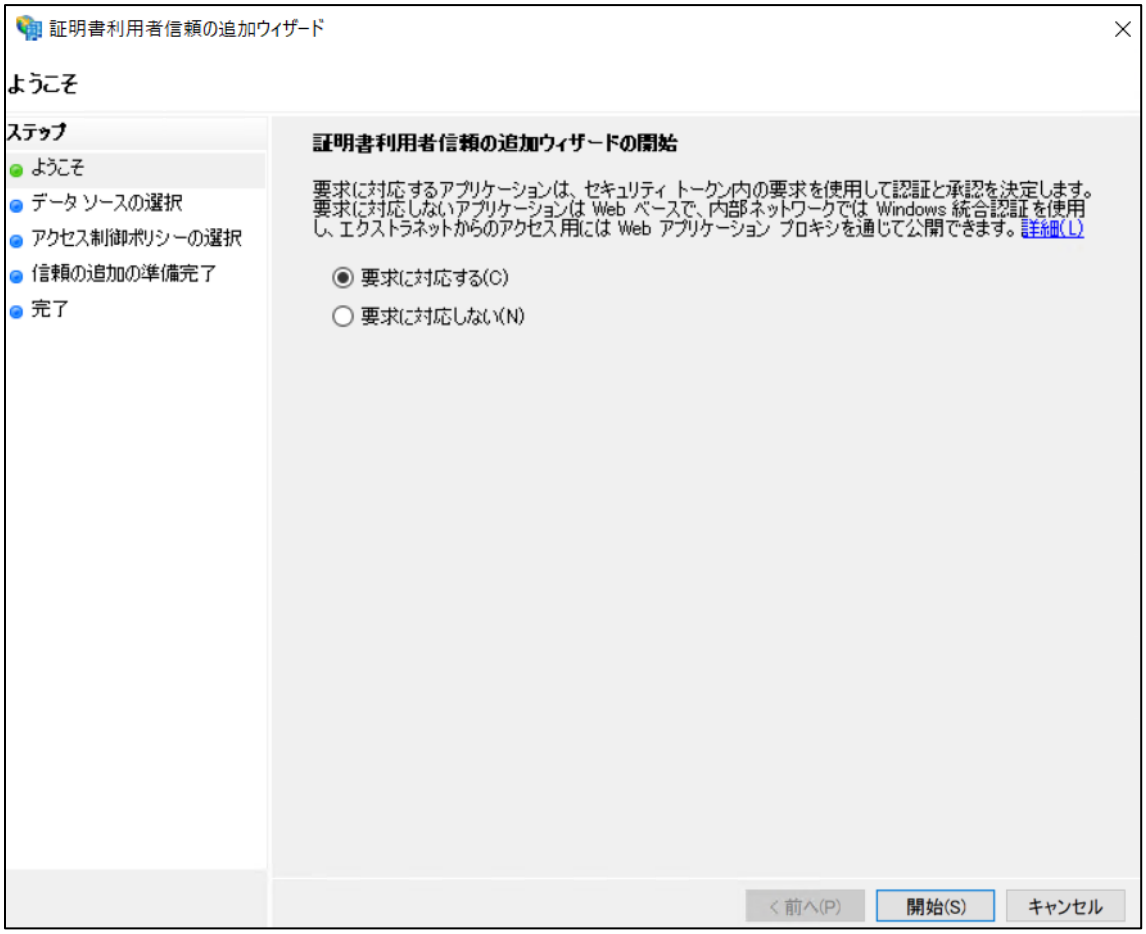
   a. ArcGIS Online / ArcGIS Enterprise で管理者権限のあるユーザーでログイン後、[組織] → [設定] → [セキュリティ] をクリックします。
   b. ArcGIS Online の場合： [ログイン] → [SAML ログイン] の [サービス プロバイダーのメタデータのダウンロード] をクリックし、 ArcGIS Online のメタデータを ADFS マシン上に保存します。

ArcGIS Enterprise の場合：[SAML を使用したエンタープライズ ログイン] セクションで、[サービスプロバイダーの取得] をクリックし、ArcGIS Enterprise のメタデータを ADFS マシン上に保存します。

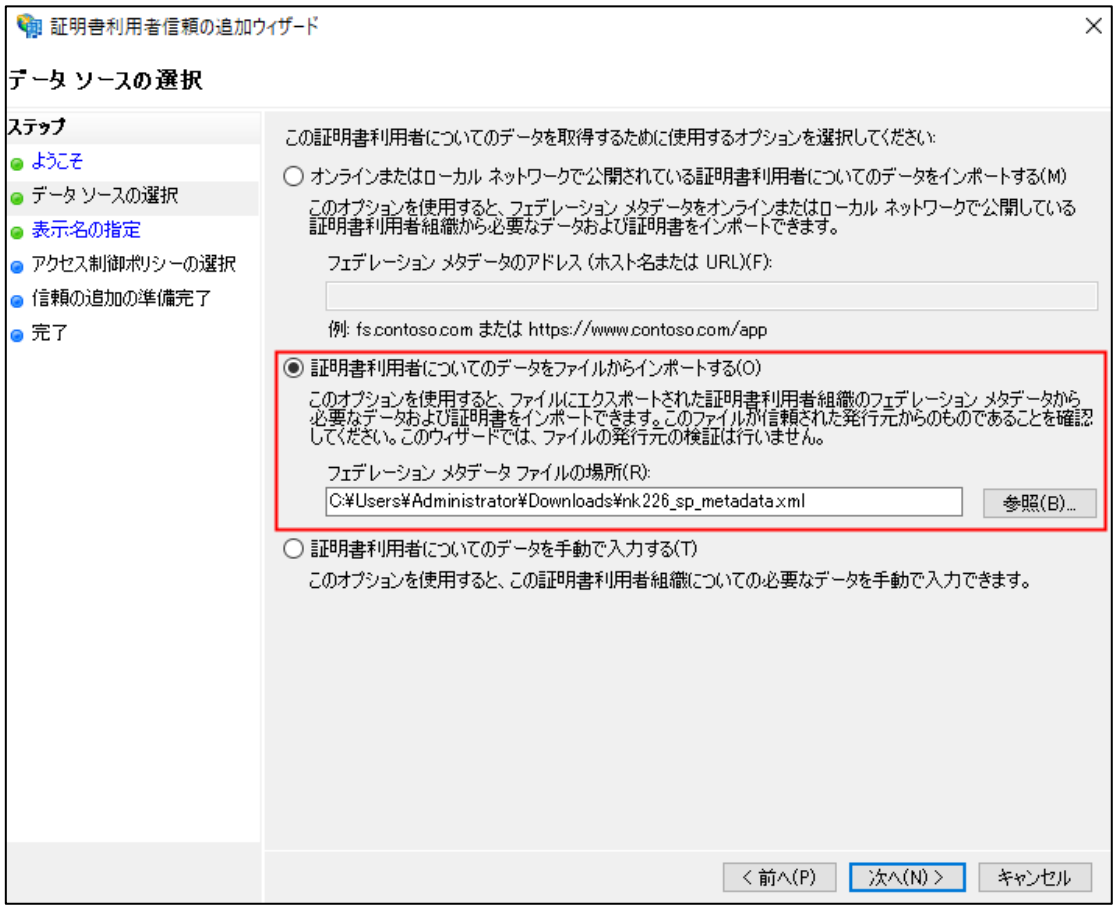


6. ADFS マシン上で、[スタート] → [Windows 管理ツール] → [ADFS の管理] を開きます。
7. [証明書利用者信頼] → [証明書利用者信頼の追加] をクリックします。

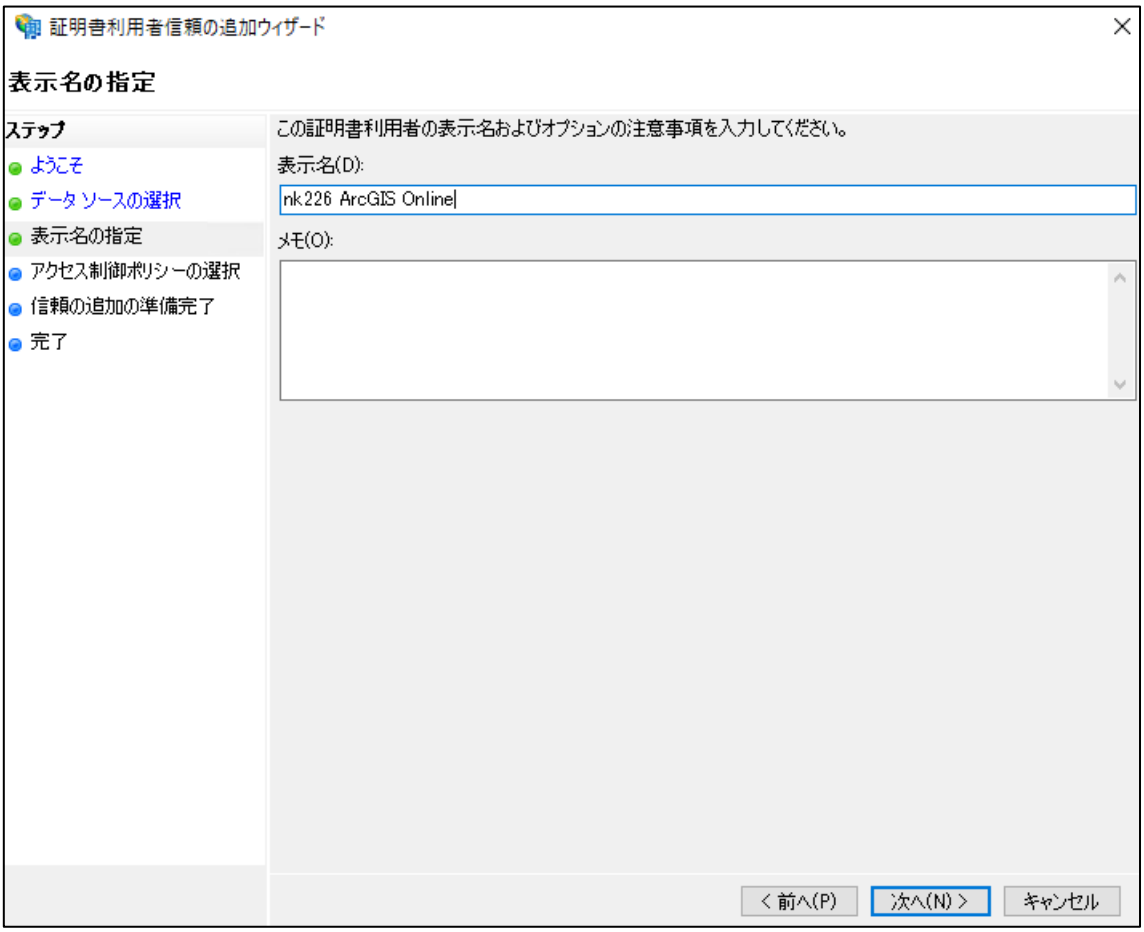
8. 証明書利用者信頼の追加画面が表示されます。[要求に対応する] を選択した状態で、[開始] をクリックします。



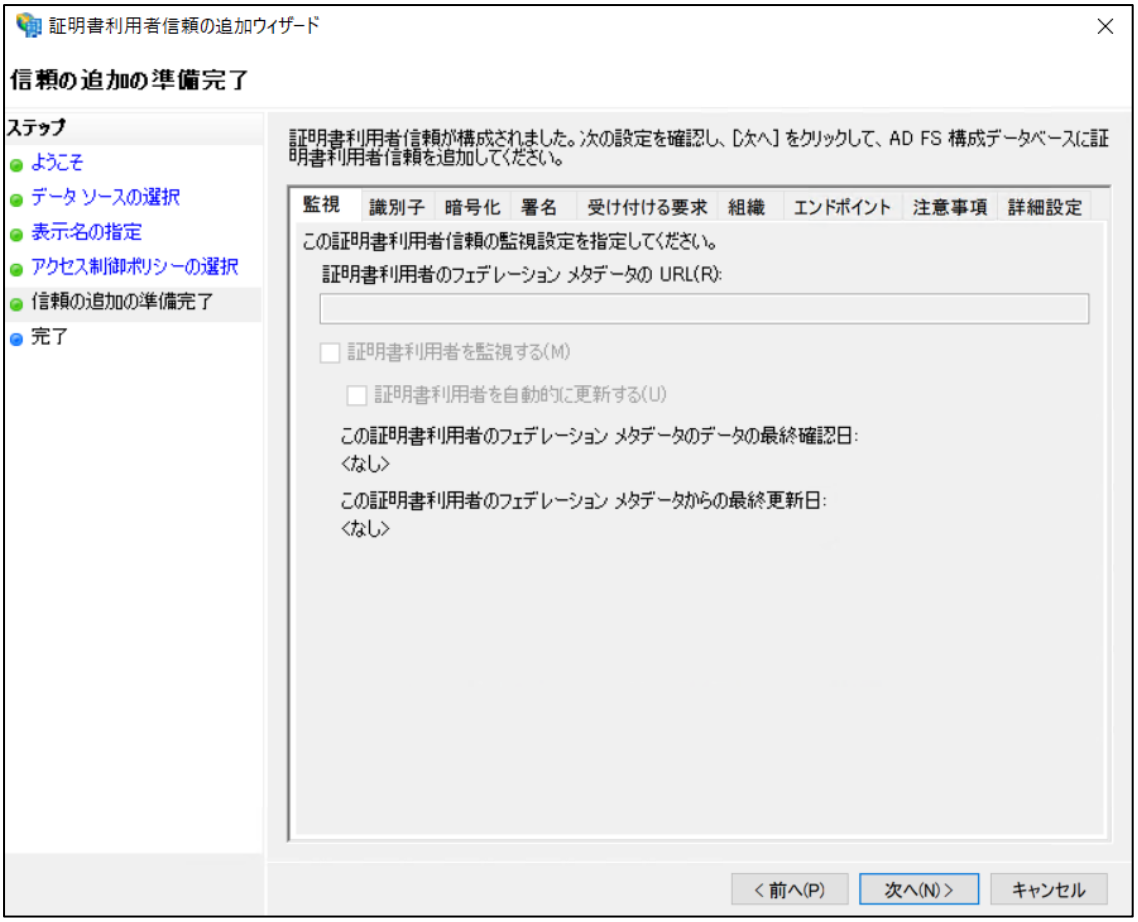
9. 手順 1 でダウンロードした ArcGIS Online / ArcGIS Enterprise のメタデータを ADFS にインポートします。 [証明書利用者についてのデータをファイルからインポートする] を選択し、ダウンロードした ArcGIS Online / ArcGIS Enterprise のメタデータを選択します。[次へ] をクリックします。



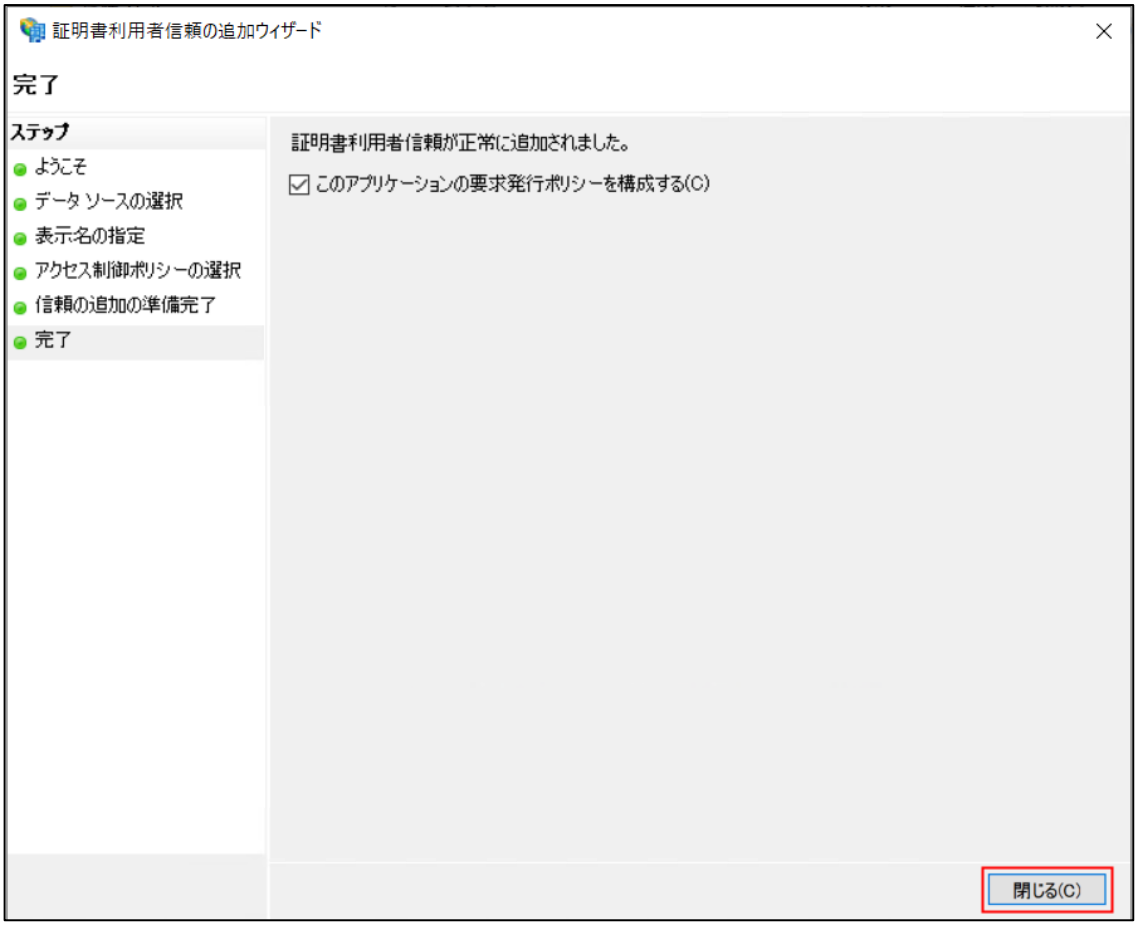
10. 証明書利用者の表示名を入力します。任意の文字を入力し、[次へ] をクリックします。



11. 設定内容の確認画面が表示されます。設定内容に問題がなければ、[次へ] をクリックします。

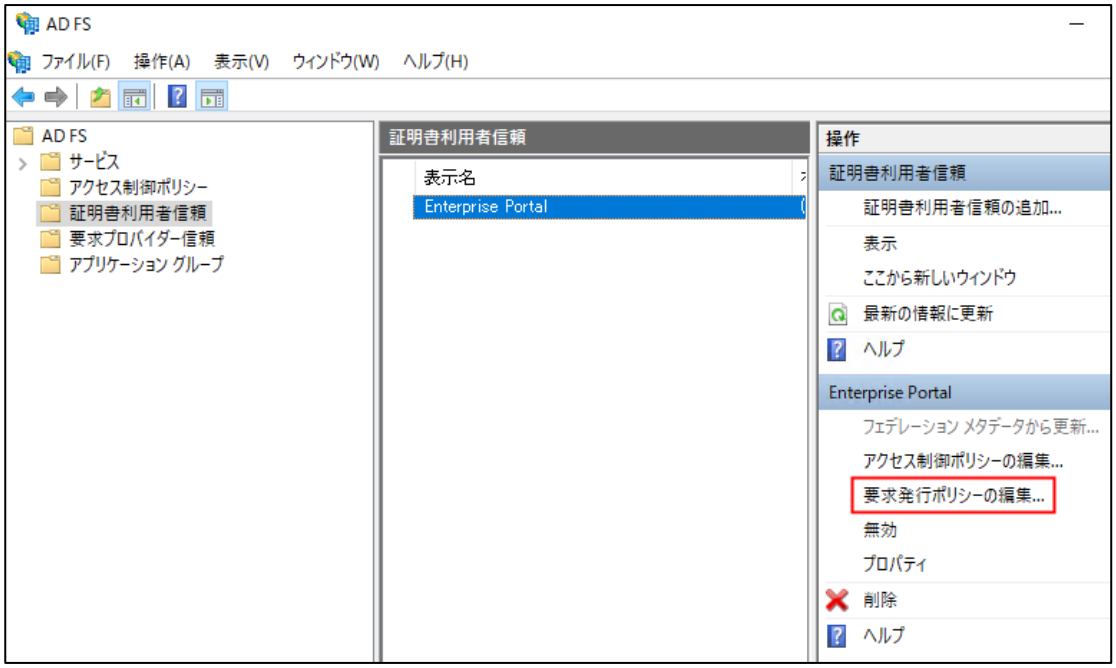


12. [閉じる] をクリックします。

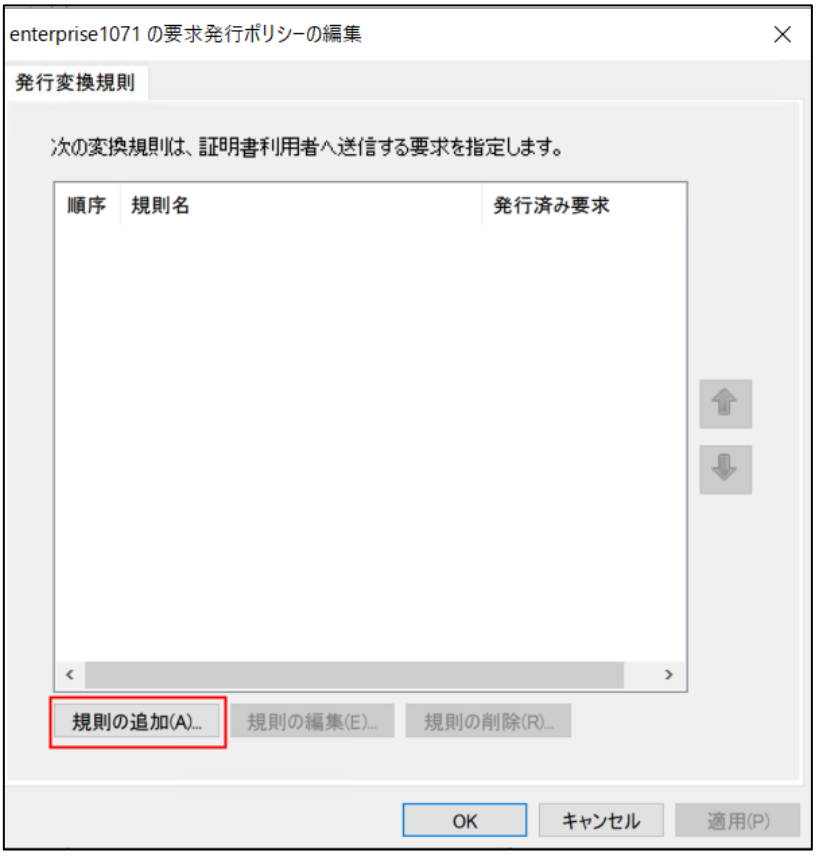


13. 要求発行ポリシーを設定します。[要求発行ポリシーの編集] をクリックし、要求発行ポリシーの編集画面を開きます。

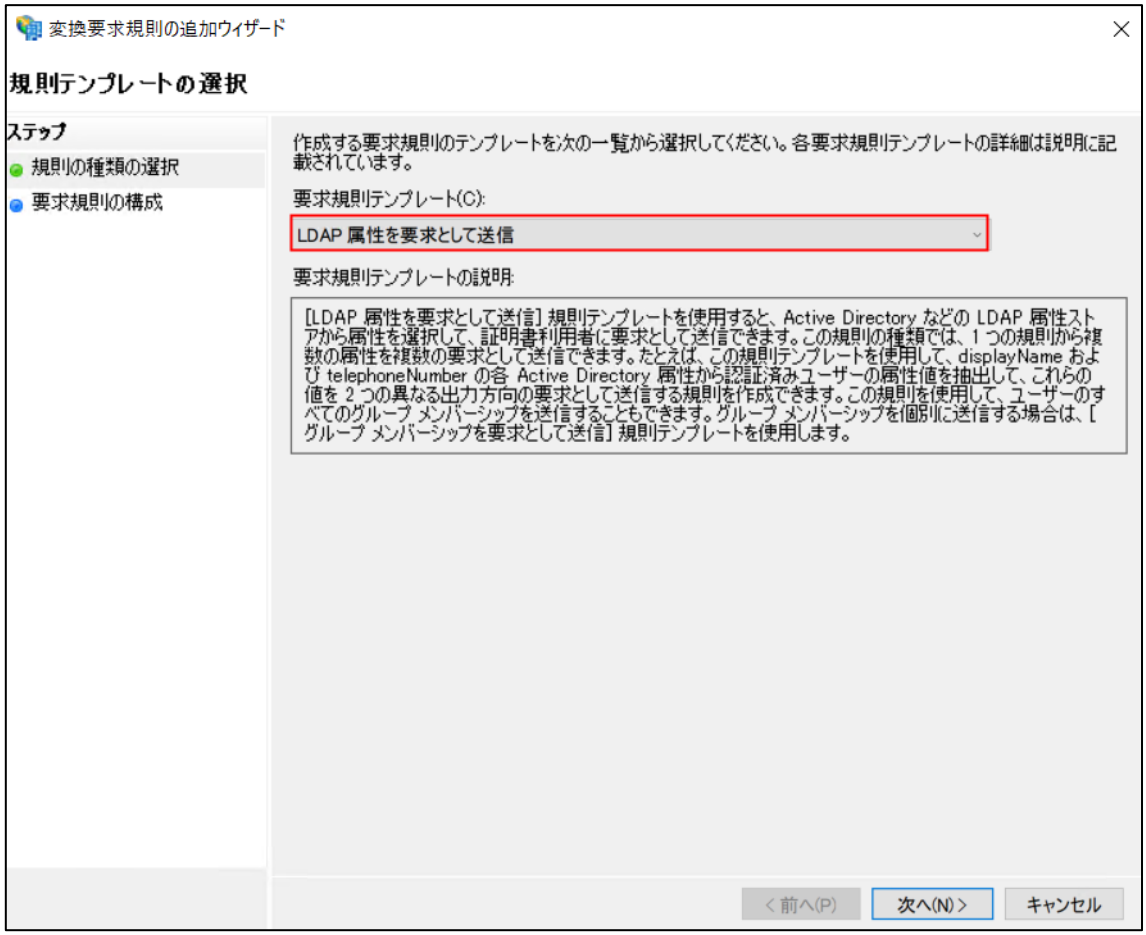
（前の手順で [このアプリケーションの要求発行ポリシーを構成する] にチェックを入れている場合、編集画面が自動的に開きます。）



14. 要求発行ポリシーの編集画面が表示されます。[規則の追加] をクリックします。

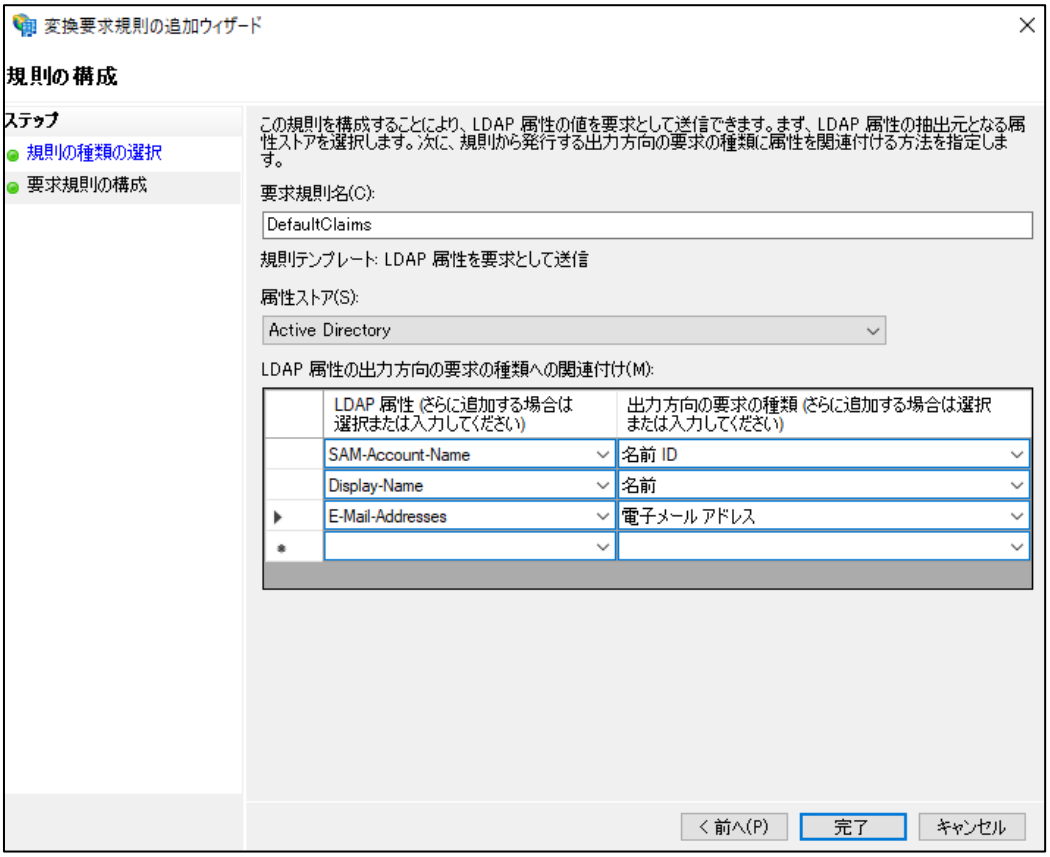


15. 規則テンプレートの選択画面が表示されます。[LDAP 属性を要求として送信] テンプレートを選択し、[次へ] をクリックします。



16. ArcGIS Online / ArcGIS Enterprise に送信するユーザー属性の設定を行います。要求規則名に任意の名前を入力し、属性ストアに [Active Directory] を選択します。
LDAP 属性の出力方向の要求の種類への関連付けの設定では、ArcGIS Online / ArcGIS Enterprise へ送信する LDAP 属性を設定します。[出力方向の要求の種類] の [名前 ID] はログイン時に使用するユーザー名になるので、ユーザーを一意に識別する LDAP 属性（SAM-Account-Name もしくは User-Principal-Name）を指定します（本ガイドでは SAM-Account-Name を指定）。また、[名前 ID] 以外の AD ユーザー属性を ArcGIS Online / ArcGIS Enterprise のユーザー属性に適用することができます。一例として、AD ユーザーの [名前] および [電子メール アドレス] 属性の、ArcGIS ユーザー属性への適用先を下表に示します。設定が終わったら、[完了] をクリックします。ADFS の設定は以上で完了です。

LDAP 属性	出力方向の要求の種類	ArcGIS でのユーザー属性の適用先
SAM-Account-Name	名前 ID	ユーザー名
Display-Name	名前	名前（名）
E-mail-Addresses	電子メール アドレス	電子メール



2.3. 動作確認

ADFS による SAML ログインを使用して ArcGIS Online / ArcGIS Enterprise にアクセスできるか確認します。

1. ArcGIS Online / ArcGIS Enterprise 組織サイトにアクセスし、ログイン ボタン（「2. ArcGIS Online と ADFS の連携設定」 の手順 5 で入力した名前が表示されています）を選択します。

2. ADFS のログイン画面が表示されます。ユーザー名（「2.2 ADFS に ArcGIS Online / ArcGIS Enterprise」の手順 12 で指定した SAM-Account-Name 属性)、パスワードを入力し、[サインイン] をクリックします。

ArcGIS Online / ArcGIS Enterprise の組織サイトにログインされます。

ArcGIS Online の場合、ユーザー名の命名規則は 「ユーザー名_<サブドメイン>」 となります（下図の赤枠部分）。

ArcGIS Enterprise の場合、ユーザー名の命名規則は「ユーザー名」となります。

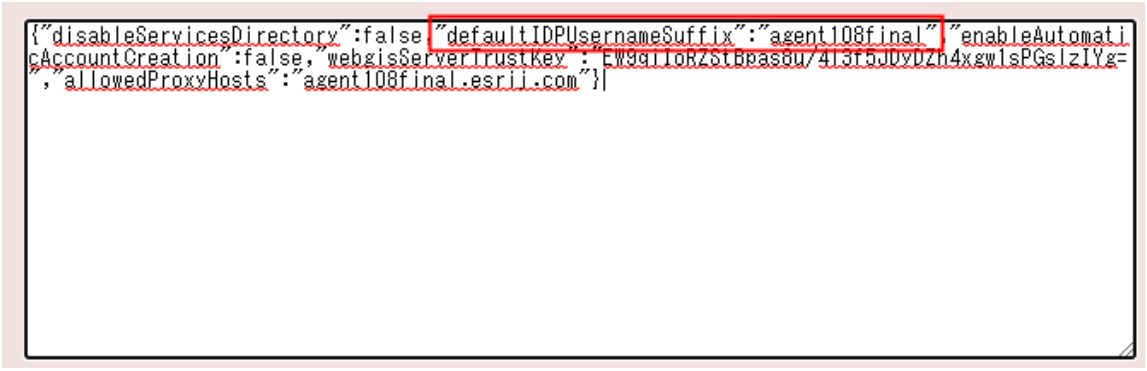
（ArcGIS Enterprise では、ユーザー名の命名規則を別途設定することで、AGOL と同様にユーザー名を「ユーザー名_<設定値>」とすることが可能です。設定方法は「3.1. ユーザー名の命名規則の設定方法」をご参照ください。）

以上で動作確認は終了です。

3. 参考情報

3.1. ユーザー名の命名規則の設定方法

1. Portal for ArcGIS の管理用アプリケーションである Portal Administrator Directory にアクセスします。
   URL：https://FQDN:7443/arcgis/portaladmin
2. [Security] → [Config] をクリックします。
3. [Update Security Configuration] をクリックします。
4. JSON オブジェクト内に以下の内容を追記します。
   "defaultIDPUsernameSuffix":"agent108final"



5. [Update Configuration] をクリックします。

ArcGIS Online / ArcGIS Enterprise -Active Directory Federation Service 連携ガイド

2020 年 4 月 7 日　初版

ESRI ジャパン株式会社

https://www.esrij.com/