

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

目次

| | | |
|------|---|----|
| 1. | はじめに..... | 1 |
| 1.1. | 本ガイドについて..... | 1 |
| 1.2. | 環境情報..... | 2 |
| 2. | ArcGIS Online / ArcGIS Enterprise と ADFS の連携設定..... | 4 |
| 2.1. | ArcGIS Online / ArcGIS Enterprise に ADFS を Idp として登録..... | 4 |
| 2.2. | ADFS に ArcGIS Online / ArcGIS Enterprise を SP として登録..... | 9 |
| 2.3. | 動作確認..... | 18 |
| 3. | 参考情報..... | 21 |
| 3.1. | ユーザー名の命名規則の設定方法..... | 21 |

1. はじめに

1.1. 本ガイドについて

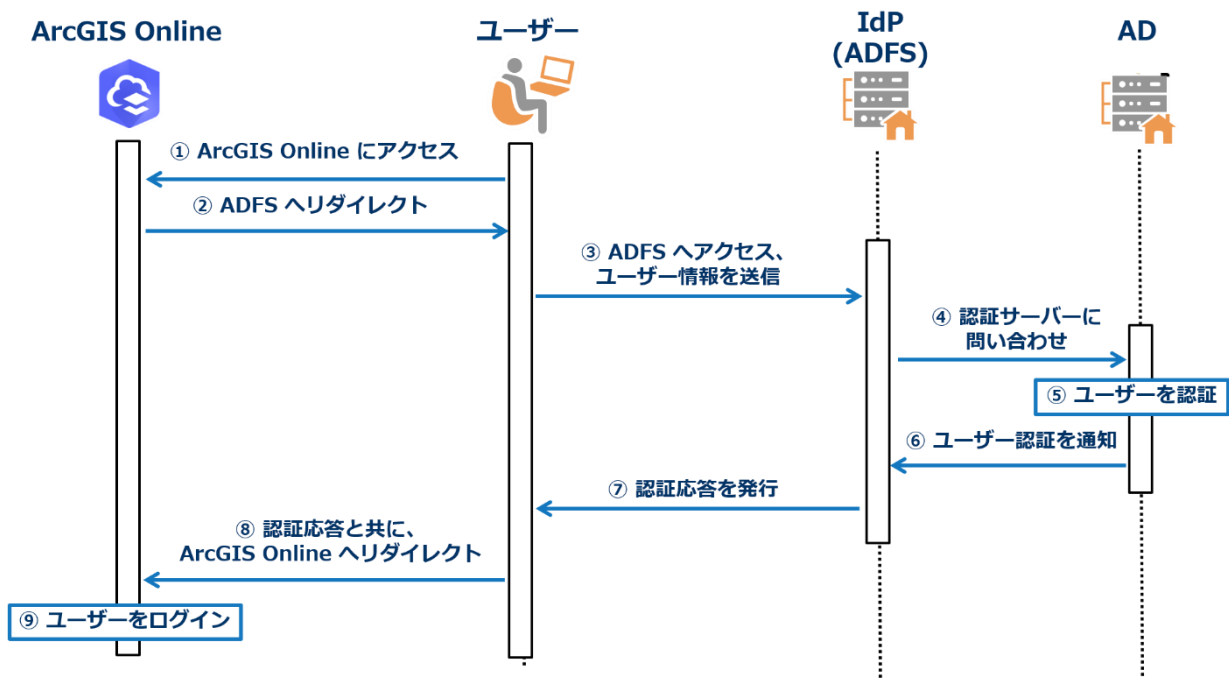
Active Directory Federation Service（以下、ADFS）は、組織内で使用している Active Directory（以下、AD）の ID を使用して、アプリケーションやクラウド サービスへのシングル サインオン（以下、SSO）を実現する Microsoft のソリューションです。ArcGIS Online / ArcGIS Enterprise では、ADFS と連携することで、組織内の AD で使用している ID による SSO を行うことができます。本ガイドでは、ADFS を用いた ArcGIS Online / ArcGIS Enterprise への SSO 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 に準拠しているため、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があります。

- ・ [2.1. ArcGIS Online に ADFS を Idp として登録](#)
- ・ [2.2. ADFS に ArcGIS Online を SP として登録](#)

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。

ログイン

メンバーが以下の方法のいずれかを使用してサインインできるように、組織のサインインページをカスタマイズします。ここに表示される順序によって、サインインページに表示される順序が決まります。

ArcGIS ログイン

ユーザーは、ArcGIS ログインでサインインできます。

SAML ログイン

ユーザーが組織の既存の SAML ID プロバイダーを使用して、ArcGIS にサインインできるよう組織を設定できます。

SAML ログインの設定 [↓ サービスプロバイダーのメタデータのダウンロード](#)

4. [1つの ID プロバイダー] を選択します。

SAML ログインの設定 ×

構成の選択 プロパティの指定

1つの ID プロバイダー

ユーザーが、組織によって管理された既存のエンタープライズ認証情報を使用してサインインできるようにします。これは、最も一般的な構成です。

ID プロバイダーのフェデレーション

既存の組織間のフェデレーション (SWITCHaai フェデレーションなど) に属しているユーザーが、そのフェデレーションによってサポートされている認証情報を使用してサインインできるようにします。

次へ
キャンセル

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 ID プロバイダーの設定をクリックして設定を反映します。

SAML ログインの設定 ✕

構成の選択
プロパティの指定

名前:

ユーザーは次の条件で加入できます:

自動
 管理者から招待されたとき

エンタープライズ ID プロバイダーのメタデータソース

URL
 ファイル
 設定パラメーター

ファイルを選択

> 高度な設定を表示

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。

ログイン

メンバーが以下の方法のいずれかを使用してサインインできるように、組織のサインインページをカスタマイズします。ここに表示される順序によって、サインインページに表示される順序が決まります。

ArcGIS ログイン

ユーザーは、ArcGIS ログインでサインインできます。

SAML ログイン

ユーザーが組織の既存の SAML ID プロバイダーを使用して、ArcGIS にサインインできるよう組織を設定できます。

✓ ADFS
✎

↓ サービス プロバイダーのメタデータのダウンロード

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

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）。

SAML ログインの編集 ✕

名前:

ユーザーは次の条件で加入できます:

自動 管理者から招待されたとき

エンタープライズ ID プロバイダーのメタデータソース

URL ファイル 設定パラメーター

ログイン URL (リダイレクト):

ログイン URL (POST):

証明書:

▲ ▼

[> 高度な設定を表示](#)

・ ArcGIS Enterprise に ADFS を Idp として登録

- 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>
- 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。
- [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。

SAMLを使用したエンタープライズログイン



ユーザーが既存のオンプレミスのシステムと同じユーザー名とパスワードを使用して Portal for ArcGIS にサインインできるように、組織サイトを設定できます。

これには、ID フェデレーションというテクノロジーを活用します。このセクションでは、2つの操作を設定できません。

エンタープライズログインでは、次の2つの構成がサポートされています。

1つのIDプロバイダー

ユーザーが、組織によって管理された既存のエンタープライズ認証情報を使用してサインインできるようにします。これは、最も一般的な構成です。

IDプロバイダーのフェデレーション

既存の組織間のフェデレーション (SWITCHaai フェデレーションなど) に属しているユーザーが、そのフェデレーションによってサポートされている認証情報を使用してサインインできるようにします。

エンタープライズログインの設定

サービスプロバイダーの取得

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。

IDプロバイダーの設定



ポータルエンタープライズIDプロバイダーを設定するプロパティを指定します。

名前:

ADFS

ユーザーは次の条件で加入できます:

自動 アカウントをポータルに追加した後

エンタープライズIDプロバイダーのメタデータは以下から提供されます:

URL ファイル 設定パラメーター

ファイル:

ファイルを選択

FederationMetadata.xml

高度な設定を表示

IDプロバイダーの設定

キャンセル

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。

SAMLを使用したエンタープライズ ログイン



ユーザーが既存のオンプレミスのシステムと同じユーザー名とパスワードを使用して Portal for ArcGIS にサインインできるように、組織サイトを設定できます。

これには、ID フェデレーションというテクノロジーを活用します。このセクションでは、2つの操作を設定できます。

エンタープライズログインでは、次の2つの構成がサポートされています。

- 1つのIDプロバイダー

ユーザーが、組織によって管理された既存のエンタープライズ認証情報を使用してサインインできるようにします。これは、最も一般的な構成です。

- IDプロバイダーのフェデレーション

既存の組織間のフェデレーション (SWITCHaai フェデレーションなど) に属しているユーザーが、そのフェデレーションによってサポートされている認証情報を使用してサインインできるようにします。

[エンタープライズログインの編集](#)
[エンタープライズログインの削除](#)
[サービスプロバイダーの取得](#)

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。



- 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。

証明書利用者信頼の追加ウィザード

データ ソースの選択

ステップ

- ようこそ
- データソースの選択
- 表示名の指定
- アクセス制御ポリシーの選択
- 信頼の追加の準備完了
- 完了

この証明書利用者についてのデータを取得するために使用するオプションを選択してください:

オンラインまたはローカル ネットワークで公開されている証明書利用者についてのデータをインポートする(M)
このオプションを使用すると、フェデレーション メタデータをオンラインまたはローカル ネットワークで公開している証明書利用者組織から必要なデータおよび証明書をインポートできます。

フェデレーション メタデータのアドレス (ホスト名または URL)(F):

 例: fs.contoso.com または https://www.contoso.com/app

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(O)
このオプションを使用すると、ファイルにエクスポートされた証明書利用者組織のフェデレーション メタデータから必要なデータおよび証明書をインポートできます。このファイルが信頼された発行元からのものであることを確認してください。このウィザードでは、ファイルの発行元の検証は行いません。

フェデレーション メタデータ ファイルの場所(R):

証明書利用者についてのデータを手動で入力する(T)
このオプションを使用すると、この証明書利用者組織についての必要なデータを手動で入力できます。

< 前へ(P)

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。

The screenshot shows a wizard window titled "証明書利用者信頼の追加ウィザード" (Certificate User Trust Addition Wizard). The current step is "表示名の指定" (Specify Display Name). The left sidebar lists the steps: ようこそ (Welcome), データソースの選択 (Select Data Source), 表示名の指定 (Specify Display Name), アクセス制御ポリシーの選択 (Select Access Control Policy), 信頼の追加の準備完了 (Trust Addition Preparation Complete), and 完了 (Complete). The main area contains the instruction "この証明書利用者の表示名およびオプションの注意事項を入力してください。" (Please enter the display name and optional notes for this certificate user.) Below this, there is a text box for "表示名(D):" (Display Name) containing "nk226 ArcGIS Online" and a larger text area for "メモ(O):" (Memo). At the bottom right, there are three buttons: "< 前へ(P)" (Previous), "次へ(N) >" (Next), and "キャンセル" (Cancel).

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。

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

ステップ

- ようこそ
- データソースの選択
- 表示名の指定
- アクセス制御ポリシーの選択
- 信頼の追加の準備完了
- 完了

証明書利用者信頼が構成されました。次の設定を確認し、[次へ] をクリックして、AD FS 構成データベースに証明書利用者信頼を追加してください。

監視 識別子 暗号化 署名 受け付ける要求 組織 エンドポイント 注意事項 詳細設定

この証明書利用者信頼の監視設定を指定してください。

証明書利用者のフェデレーション メタデータの URL(R):

証明書利用者を監視する(M)

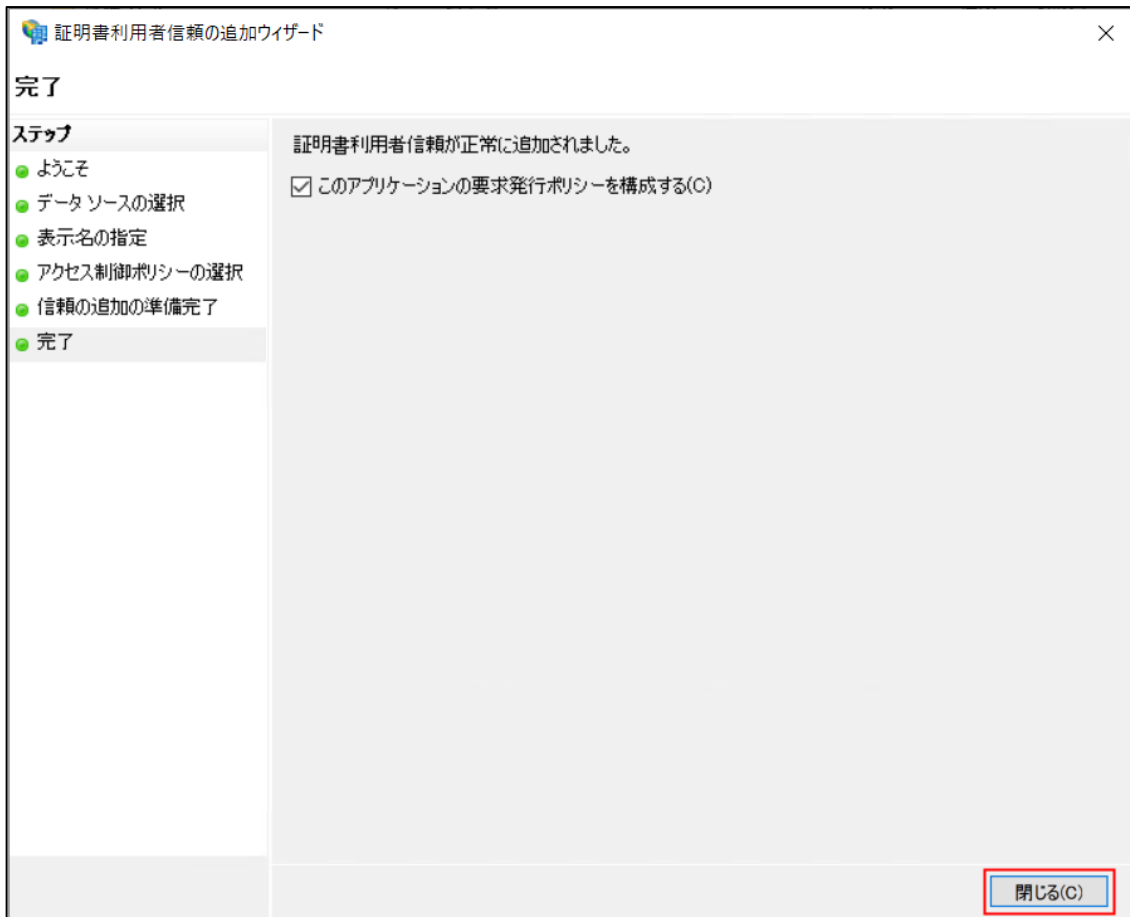
証明書利用者を自動的に更新する(U)

この証明書利用者のフェデレーション メタデータのデータの最終確認日:
<なし>

この証明書利用者のフェデレーション メタデータからの最終更新日:
<なし>

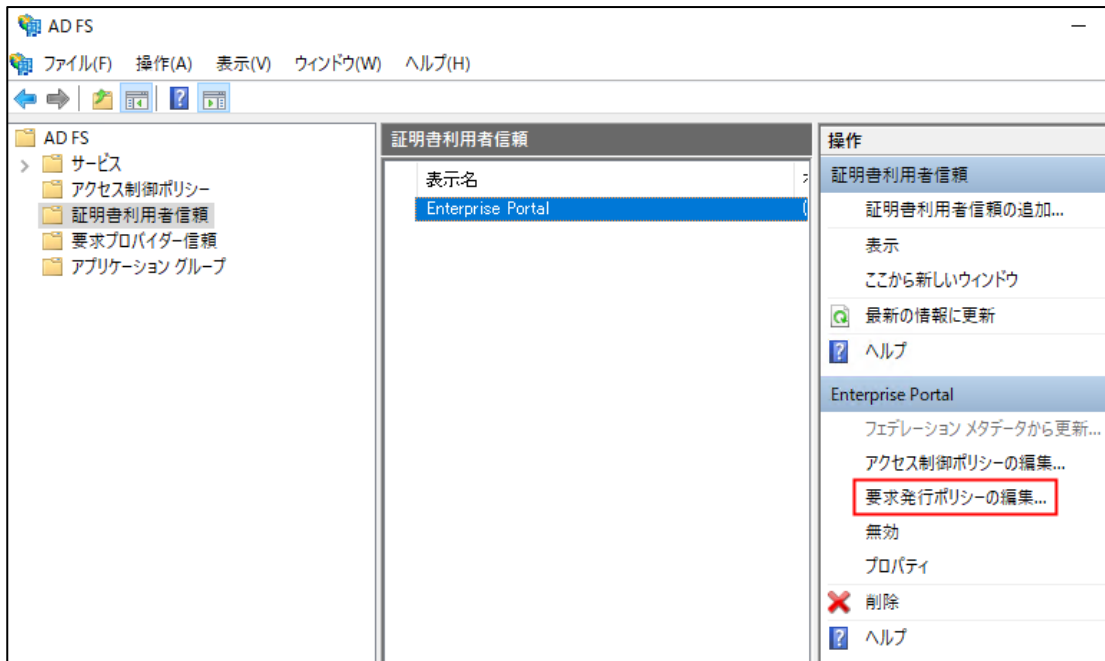
< 前へ(P) 次へ(N) > キャンセル

12. [閉じる] をクリックします。

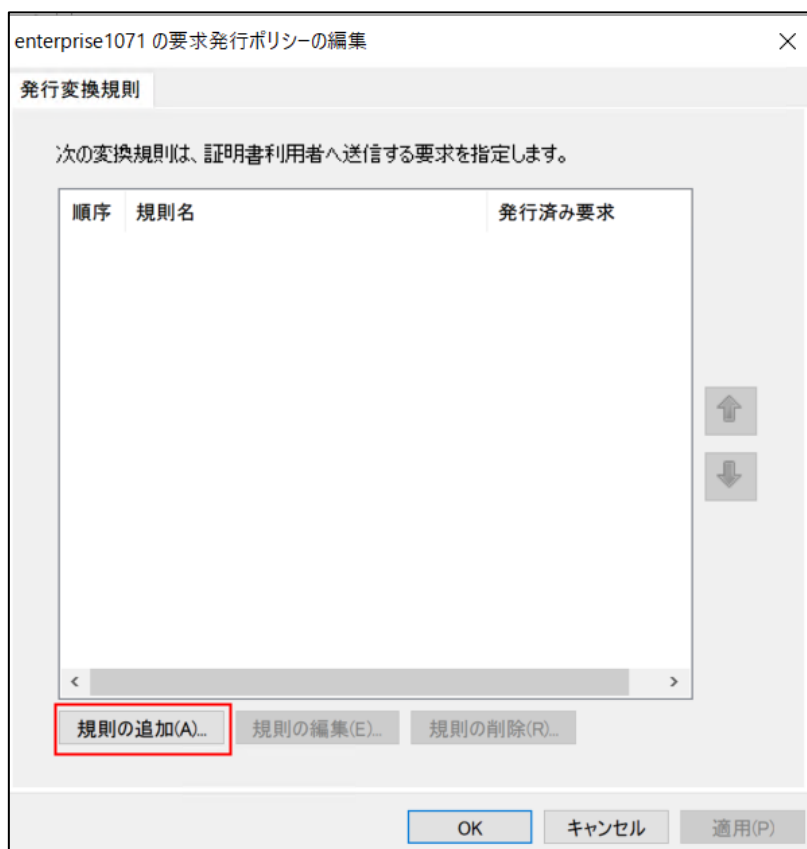


13. 要求発行ポリシーを設定します。[要求発行ポリシーの編集] をクリックし、要求発行ポリシーの編集画面を開きます。

(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 |

変換要求規則の追加ウィザード

規則の構成

ステップ

- 規則の種類を選択
- 要求規則の構成

この規則を構成することにより、LDAP 属性の値を要求として送信できます。まず、LDAP 属性の抽出元となる属性ストアを選択します。次に、規則から発行する出力方向の要求の種類に属性を関連付ける方法を指定します。

要求規則名(C):
DefaultClaims

規則テンプレート: LDAP 属性を要求として送信

属性ストア(S):
Active Directory

LDAP 属性の出力方向の要求の種類への関連付け(M):

| | LDAP 属性 (さらに追加する場合は選択または入力してください) | 出力方向の要求の種類 (さらに追加する場合は選択または入力してください) |
|---|-----------------------------------|--------------------------------------|
| | SAM-Account-Name | 名前 ID |
| | Display-Name | 名前 |
| ▶ | E-Mail-Addresses | 電子メール アドレス |
| * | | |

< 前へ(P) 完了 キャンセル

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"
```

```
{  
  "disableServicesDirectory":false,"defaultIDPUsernameSuffix":"agent108final","enableAutomaticAccountCreation":false,"webgisServerTrustKey":"EW9q11oRZst6pas8u/413r5J0yDzn4xgw1sPGs1zIYg=  
  ,allowedProxyHosts":"agent108final.esri.com"}]
```

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/>

Copyright(C) Esri Japan. 無断転載を禁ず

本書に記載されている社名、商品名は、各社の商標および登録商標です。

本書に記載されている内容は改良のため、予告なく変更される場合があります。

本書の内容は参考情報の提供を目的としており、本書に含まれる情報はその使用先の自己の責任において利用して頂く
必要があります。

