# システム設定マニュアル
# 製品共通
# SAML認証マニュアル

# 目次

はじめに
セットアップ手順（IdP:AD FSの場合）
セットアップ手順（IdP: Microsoft Entra IDの場合）
トラブルシューティング
制限事項

# はじめに

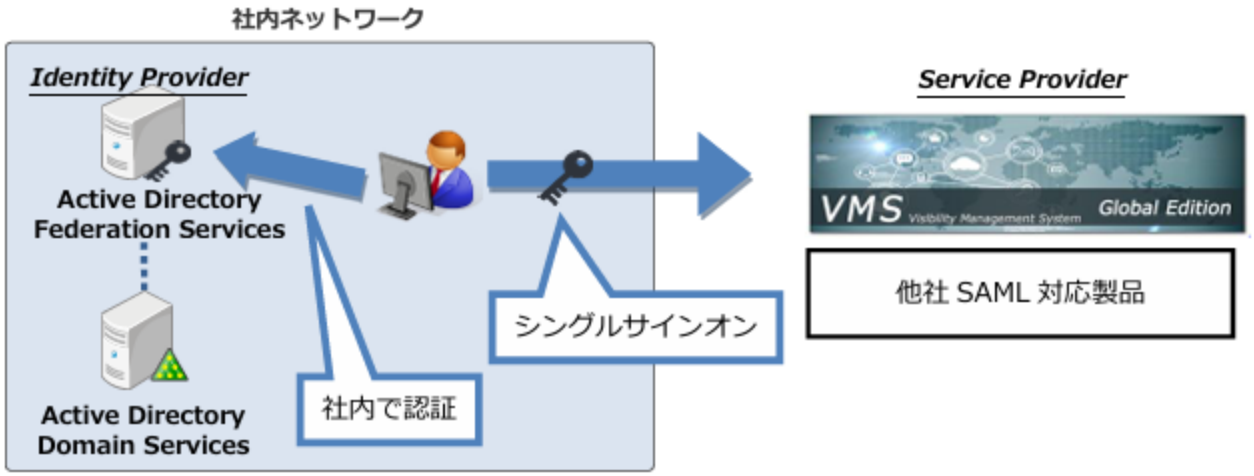
SAML認証とは、NI製品へのログインの際、SAMLのプロトコルを利用し、シングルサインオン（自動ログイン）を可能とするオプション製品です。

> ⚠ 注意
>
> - ご利用いただくにあたり、制限事項があります。「制限事項」を参照してください。

## SAML認証の概要

### SAMLとは

SAMLとは、認証、認可、ユーザ属性情報などをXMLで送受信するための仕様です。
SAML認証では、SAML2.0の仕様に基づいたシングルサインオン処理を行います。




具体的には、SAML認証の導入により以下のようなことが可能となります。

- 社内のActive Directoryドメインに参加しているPCから、NI製品へのシングルサインオン
  （※IdPにAD FSを利用し、認証方法に「Windows認証」を利用している場合）
- 他社SAML対応製品（Google Apps、Microsoft 365等）に同様の方法でシングルサインオン

⚠ 注意

- SAML認証はActive DirectoryとNI製品のユーザー/グループマスターを連携させるものではありません。
- モバイル端末を利用する場合、AD FSプロキシサーバー等を利用し、IdPが外部からアクセス可能である必要があります。

### SAMLの用語解説

SAML認証で用いられる特有の用語について、解説します。

| 用語 | 詳細 |
| --- | --- |
| Identity Provider<br>（以下、IdP） | 認証・認可の情報を提供する役割を担います。<br>IdPで認証されたユーザーはSPのサービスにアクセス可能となります。<br>例：AD FS、Microsoft Entra ID |
| Service Provider<br>（以下、SP） | シングルサインオン対象のWebアプリケーションを指します。<br>IdPが発行した認証・認可の情報に応じてユーザーにサービスを提供します。<br>例：NI製品、Google Apps、Microsoft 365 |
| バインディング<br>（Binding） | SAMLメッセージの送信方法を規定したもの。<br>例：HTTP Redirect Binding、HTTP POST Binding |
| Active Directoryドメインサービス（以下、AD） | Microsoft社によって開発されたディレクトリ・サービス・システム。<br>ユーザーとコンピュータリソースを管理するコンポーネント群の総称です。 |
| Active Directoryフェデレーションサービス<br>（以下、AD FS） | Windows Serverの機能です。<br>ADのユーザー情報を使用した認証が可能です。<br>SAML認証ではIdPに相当します。 |
| Microsoft Entra ID | Microsoft社が提供するクラウドベースのIDおよびアクセス管理サービスです。<br>フェデレーションサーバーの機能も有します。<br>SAML認証ではIdPに相当します。 |

## 認証方法について

以下2通りの認証方法が利用可能です。

> Hint
>
> - 認証方法は設定画面で切り替え可能です。

### ■パスワード認証

IdPのログイン画面にて、ID/パスワードを入力することで認証されます。

**■Windows認証**

ドメインにログイン済みのWindows PCにて、Microsoft Edge、またはGoogle Chromeを使用している場合、自動で認証されます。
それ以外の場合、認証ダイアログが表示され、ID/パスワードを入力することで認証されます。

⚠ 注意

- Windows認証を利用する場合、コントロールパネルから下記の設定を行う必要があります。
  1. インターネット オプション> セキュリティに移動します。
  2. 「ローカルイントラネット」が選択された状態で、「レベルのカスタマイズ」ボタンをクリック します。
  3. ユーザー認証> ログオンで「イントラネットゾーンでのみ自動的にログオンする」を選択し、「OK」ボタンをクリックします。
  4. 「ローカルイントラネット」が選択された状態で、「サイト」ボタンをクリックします。
  5. 「詳細設定」ボタンをクリックします。
  6. 「このWebサイトをゾーンに追加する」部分に「https://」を 入力し、「追加」ボタンをクリックします。
     ※<IdPサーバーのアドレス>は、システム管理者にお問い合わせください。
  7. ご使用のブラウザを再起動します。
     「ローカルイントラネット」ではなく「インターネット」、または「信頼済みサイト」として設定される場合は、上記の「3」で「現在のユーザー名とパスワードで自動的にログオンする」を選択してください。

## ユーザーアカウント連携方法について

SAML認証では、IdPとNI製品間でユーザーアカウントの紐付けが必要です。ユーザーアカウントの紐付けには、以下の2通りの方法が利用可能です。

Hint

- ユーザーアカウント連携方法は、設定画面の「仮名」の項目で切り替え可能です。

**■仮名を利用する方法**

IdPが発行するランダム文字列（仮名ID）を用いて認証を行います。

- 各ユーザーは初回ログイン時に、仮名取得の作業を行う必要があります。仮名取得後、次回のログイン時からシングルサインオンが可能となります。
- NI製品の社員ログインIDと、IdPのユーザーIDを一致させておく必要はありません。

**■社員ログインIDを利用する方法（仮名を利用しない方法）**

NI製品の社員ログインIDとIdPのユーザーIDをシステムが自動で紐付け認証を行います。

- 各ユーザーは初回ログイン時からシングルサインオンが可能となります。
- NI製品の社員ログインIDと、IdPのユーザーIDを一致させておく必要があります。

## IdPによる動作の違い

基本的にはSAML2.0に対応したIdP製品であれば認証可能ですが、IdP製品により一部機能が制限される場合があります。

【IdPのシングルサインオン機能対応表】

| 機能名 | AD FS | Microsoft Entra ID |
|---|---|---|
| 認証方法：パスワード認証 | ○ | ○ |
| 認証方法：Windows認証 | ○ | × |
| 仮名 | ○ | ○ |

補足

- IdPの動作確認はAD FS、Microsoft Entra IDでのみ行っております。
  動作確認済みシステム構成は、「セットアップ手順（IdP:AD FSの場合）」「セットアップ手順（IdP:Microsoft Entra IDの場合）」をご確認ください。

# 設定の流れ

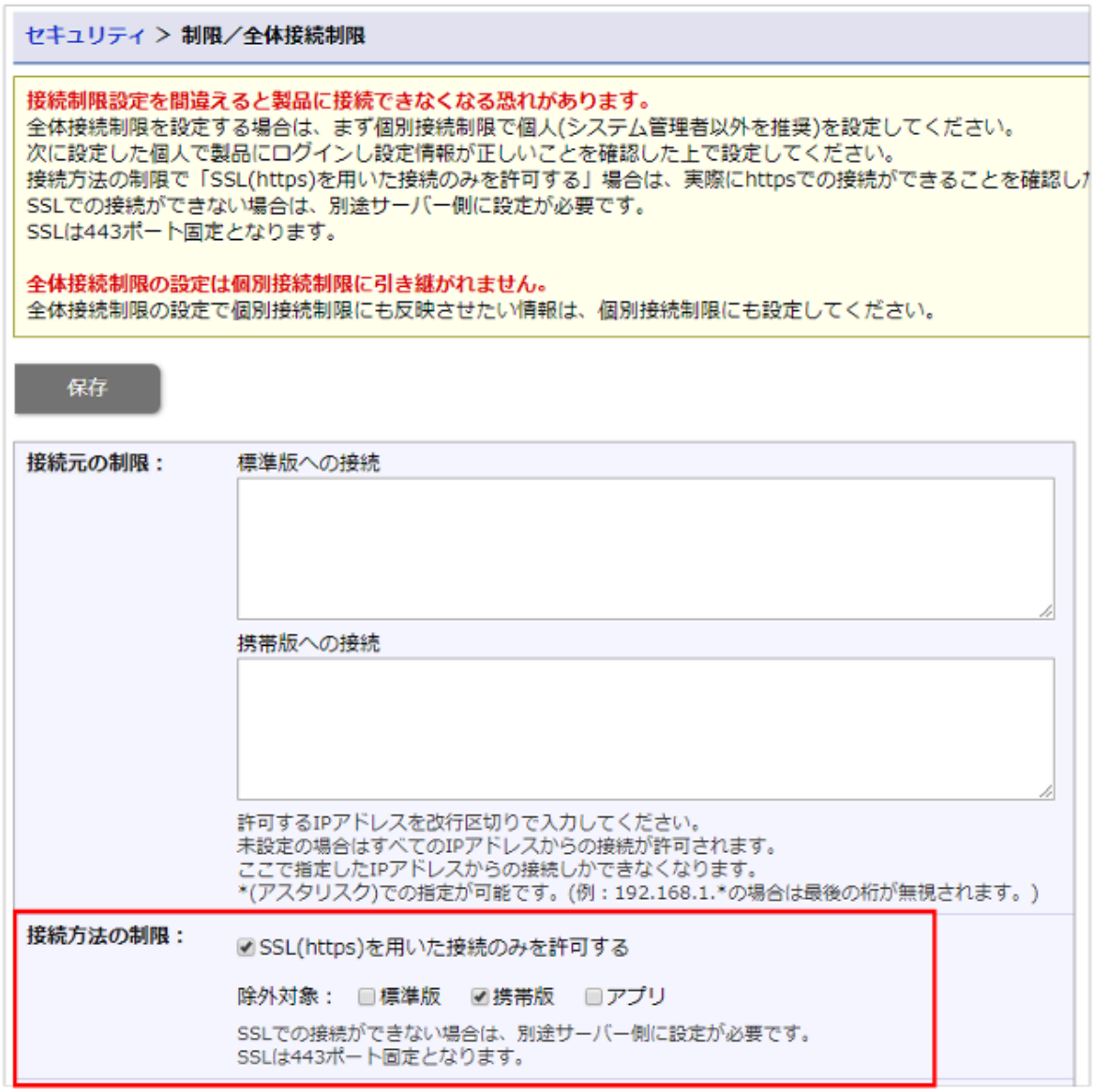
### 事前準備

設定を行う前に以下の作業が必要です。

- NI製品へ社員情報の登録
- ディレクトリサービス（Active Directory、Microsoft Entra ID）動作環境の構築
- ディレクトリサービス（Active Directory、Microsoft Entra ID）へユーザーアカウントの登録

### SSL(https)での接続設定を行う

SAML認証を利用する場合、SSL(https)での接続が必須となります。
システム設定画面のセキュリティ＞全体接続制限より、「SSL(https) での接続のみ許可する」にチェックして、「保存する」をクリックします。※携帯版はSAML認証に非対応のため、http接続も可能です。



**設定ステップ**

SAML認証によるシングルサインオンを利用するには、以下の設定ステップを実施します。

Hint

- IdPとSP間でメタデータを交換し、信頼関係を構築する必要があります。

### Step1.NI製品の設定

NI製品のシステム設定を行い、SPメタデータをダウンロードします。 IdPのメタデータをNI製品にアップロードします。

### Step2.IdPの設定

SPメタデータをアップロードし、IdPの設定を行います。

### Step3.仮名ID取得（※仮名を利用する場合のみ）

各ユーザーが初回ログイン後に、オプション設定画面より、仮名IDを取得します。

### Step4.動作確認

シングルサインオンが可能であることを確認します。

# セットアップ手順（IdP:AD FSの場合）

## システム構成

以下の構成でセットアップを行います。

**認証サーバー**

| | |
|---|---|
| ディレクトリサービス | AD |
| IdP | AD FS |
| OS | Windows Server 2016 Standard<br>Windows Server 2019 Standard<br>Windows Server 2022 Standard |
| IdPサーバーのアドレス | adfs.ni-saml.com<br>（※設定手順内のIdPサーバーのアドレスは、実際に使用するものに置き換えてください。） |

※ADとAD FSは、同一のサーバー上で稼働するものとします。
※AD、AD FSのインストール手順の詳細は、Microsoft社の情報をご確認ください。

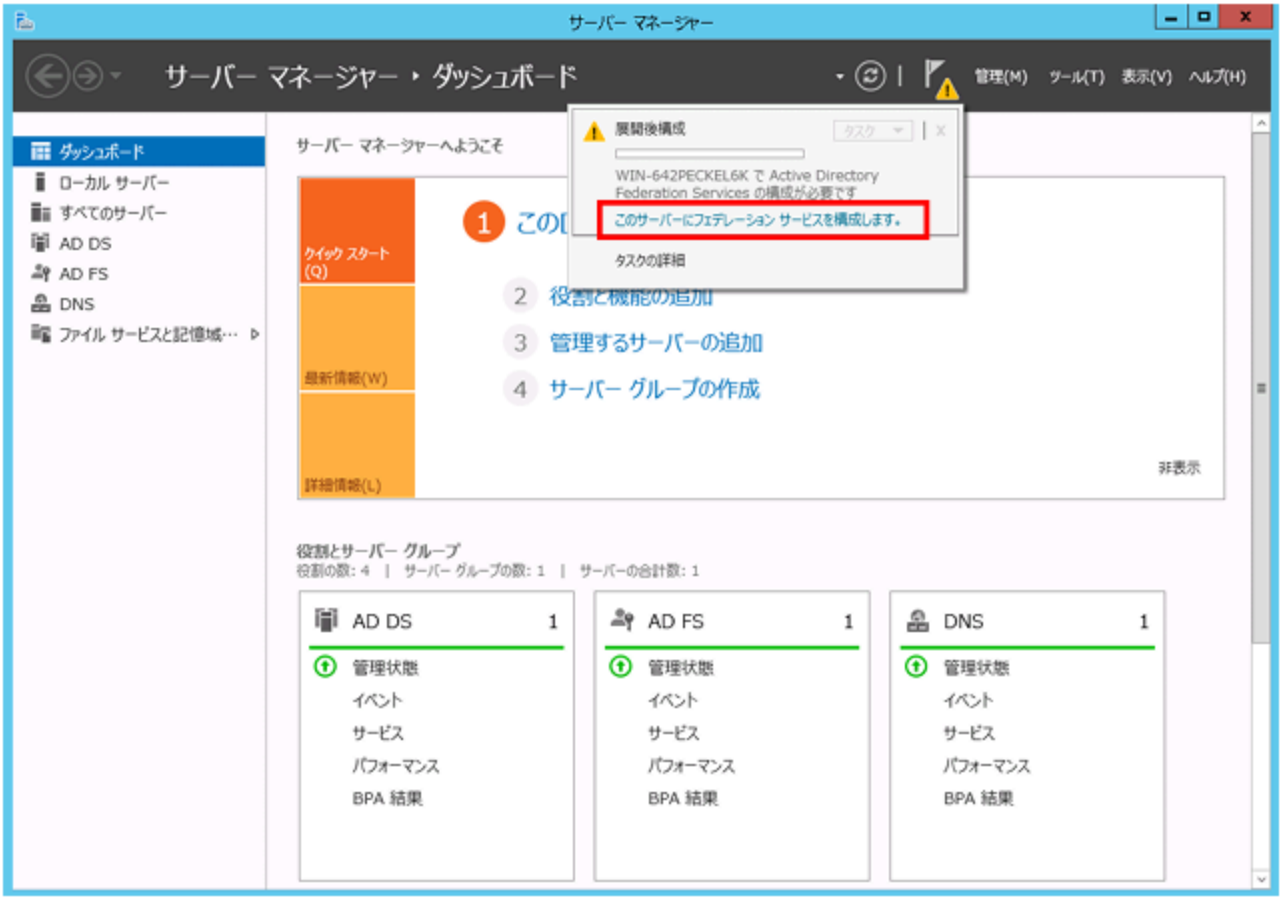
# 事前準備

## 事前準備：証明書の準備

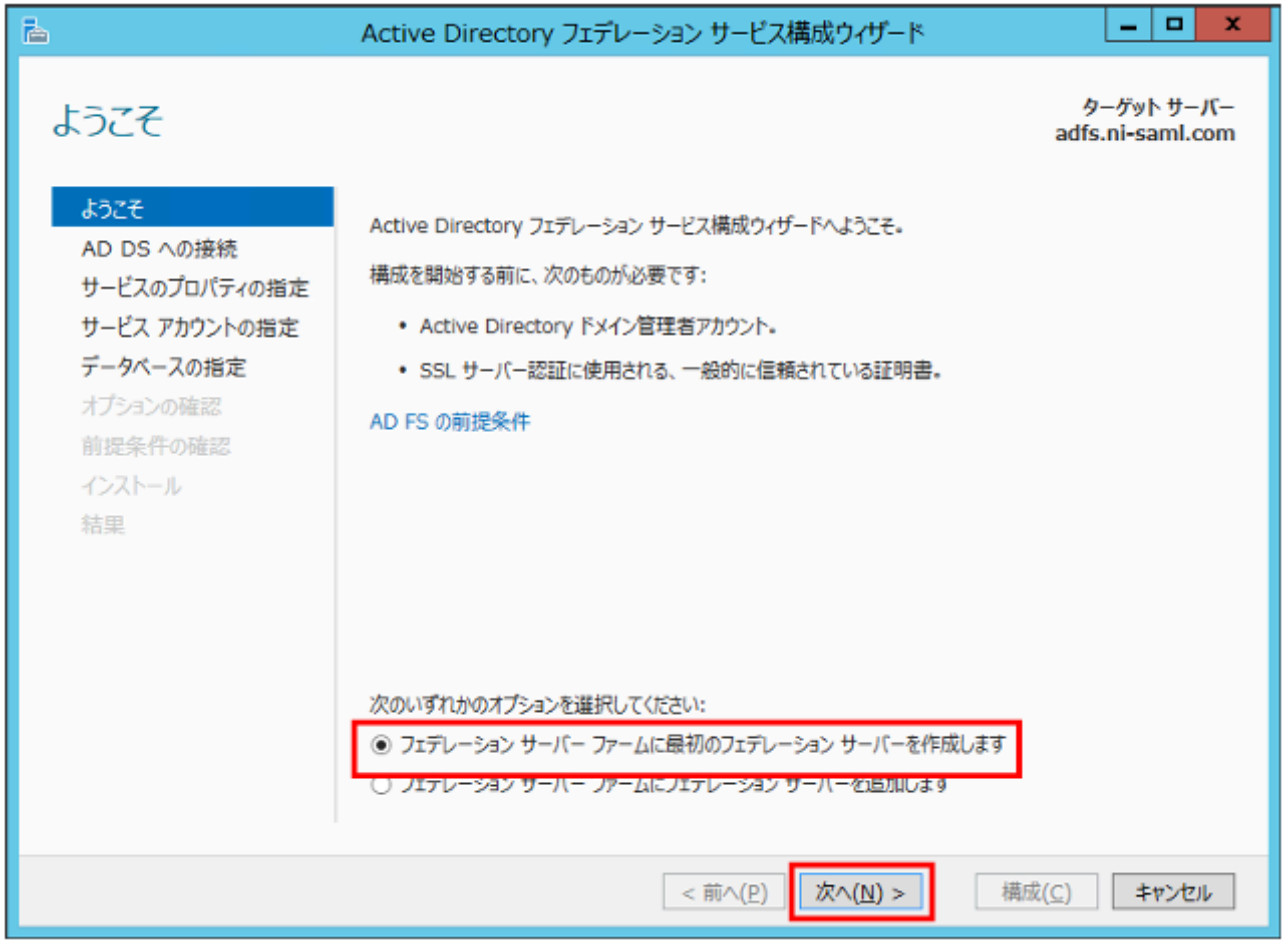
第三者認証機関が承認した、認証に使用するAD FSのサーバー証明書を.pfx形式でエクスポートします。
証明書を取得する一般的な方法には、OpenSSLを使用する方法、Certreq.exeを使用する方法、IISを使用する方法の3種類があります。（※詳細は認証局の設定手順にしたがってください。）
OpenSSLを使用する方法は、以下Microsoft社の情報もご確認ください。
https://docs.microsoft.com/ja-jp/azure/app-service/configure-ssl-certificate#export-certificate-to-pfx

## 事前準備：AD FSの構成

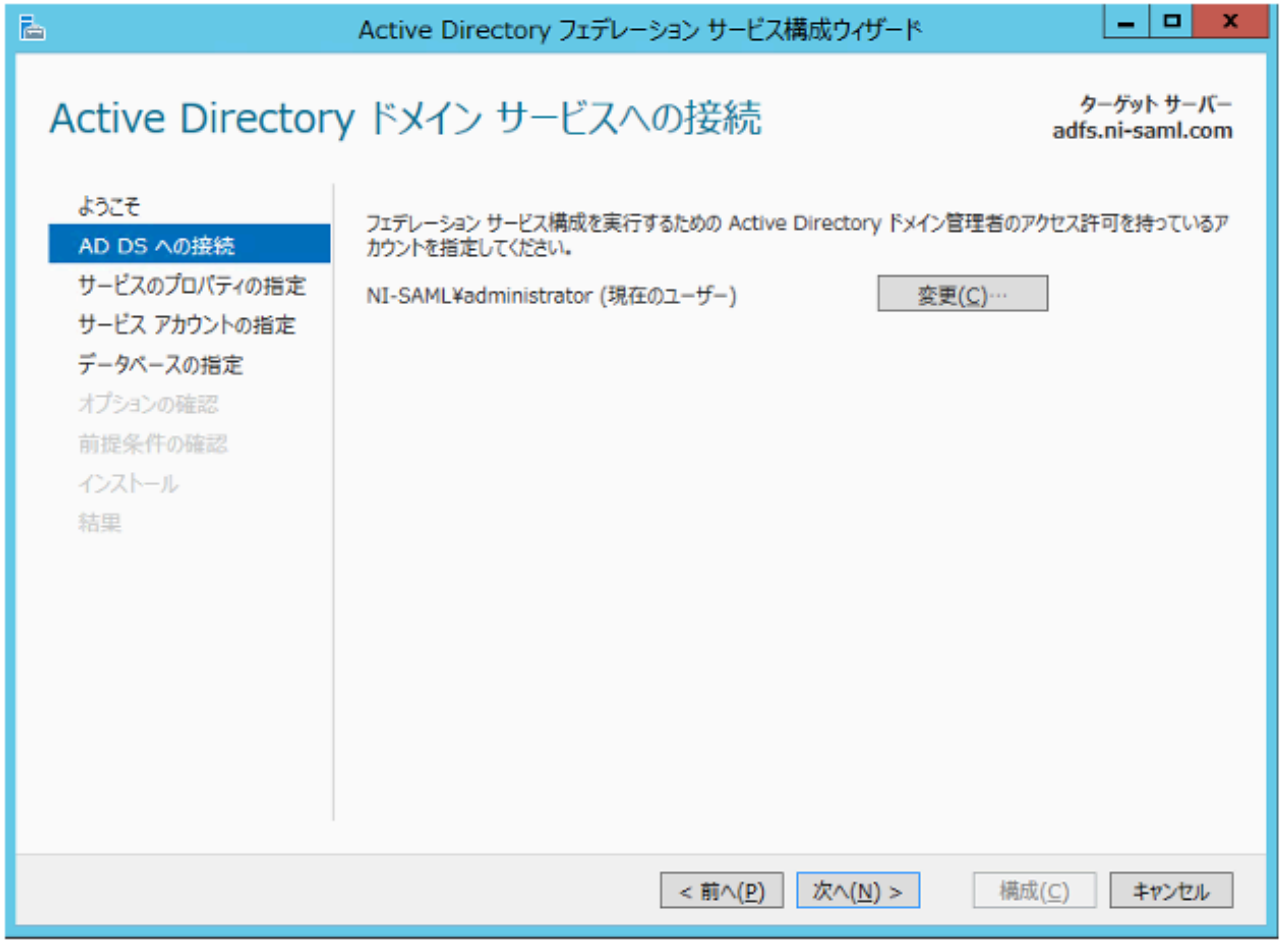
1. サーバーマネージャーより「このサーバーにフェデレーションサービスを構成します。」をクリックします。



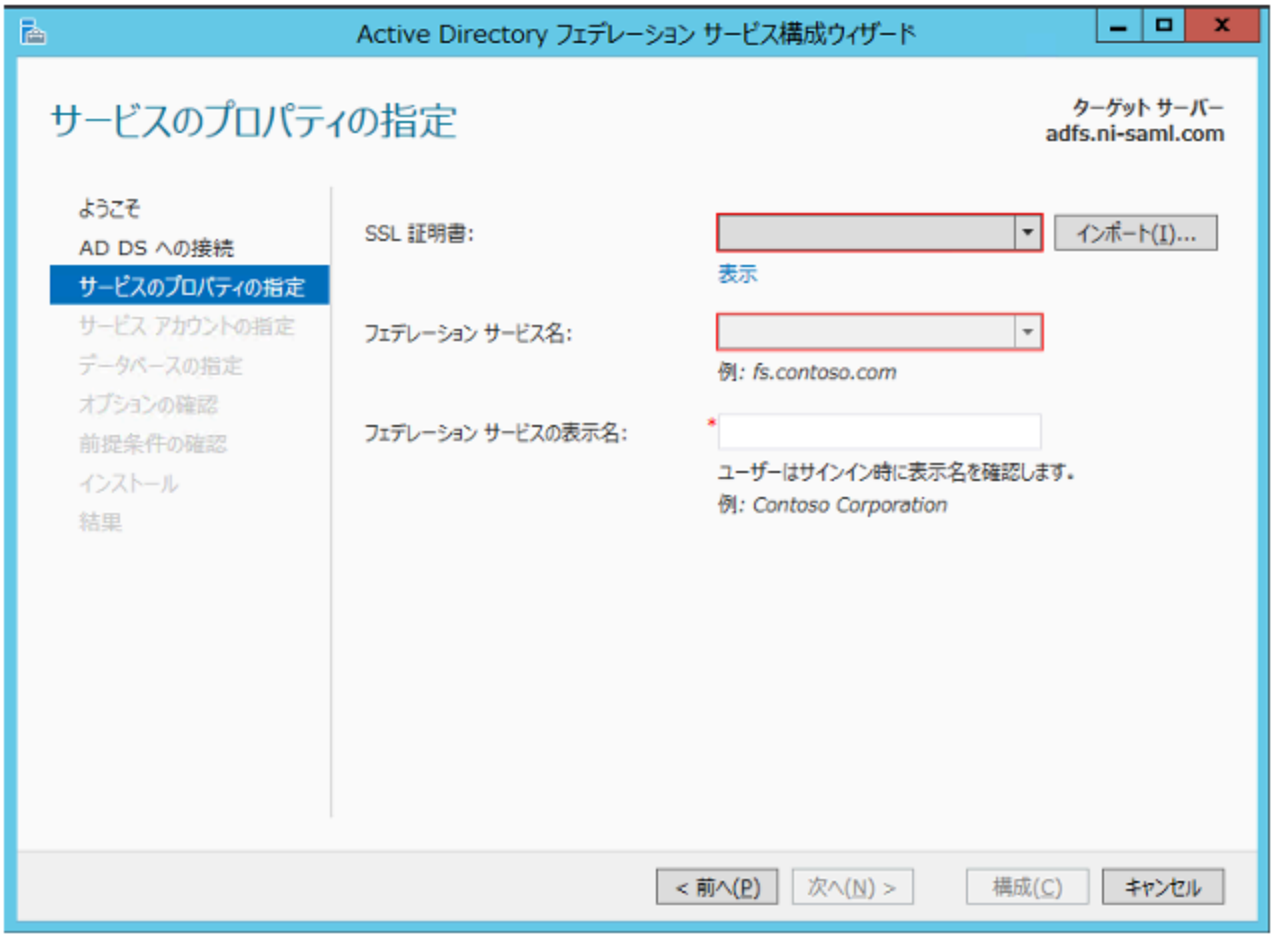
2. 「フェデレーションサーバーファームに最初のフェデレーションサーバーを作成します」を選択し、「次へ」をクリックします。

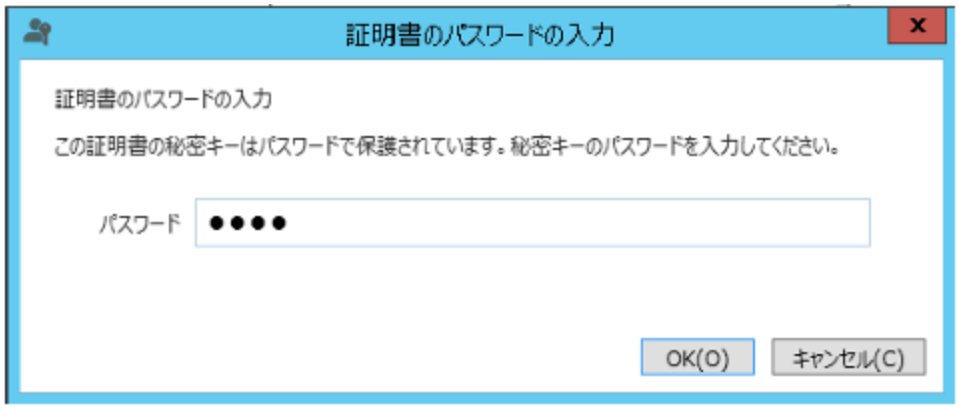


3. 「次へ」をクリックします。

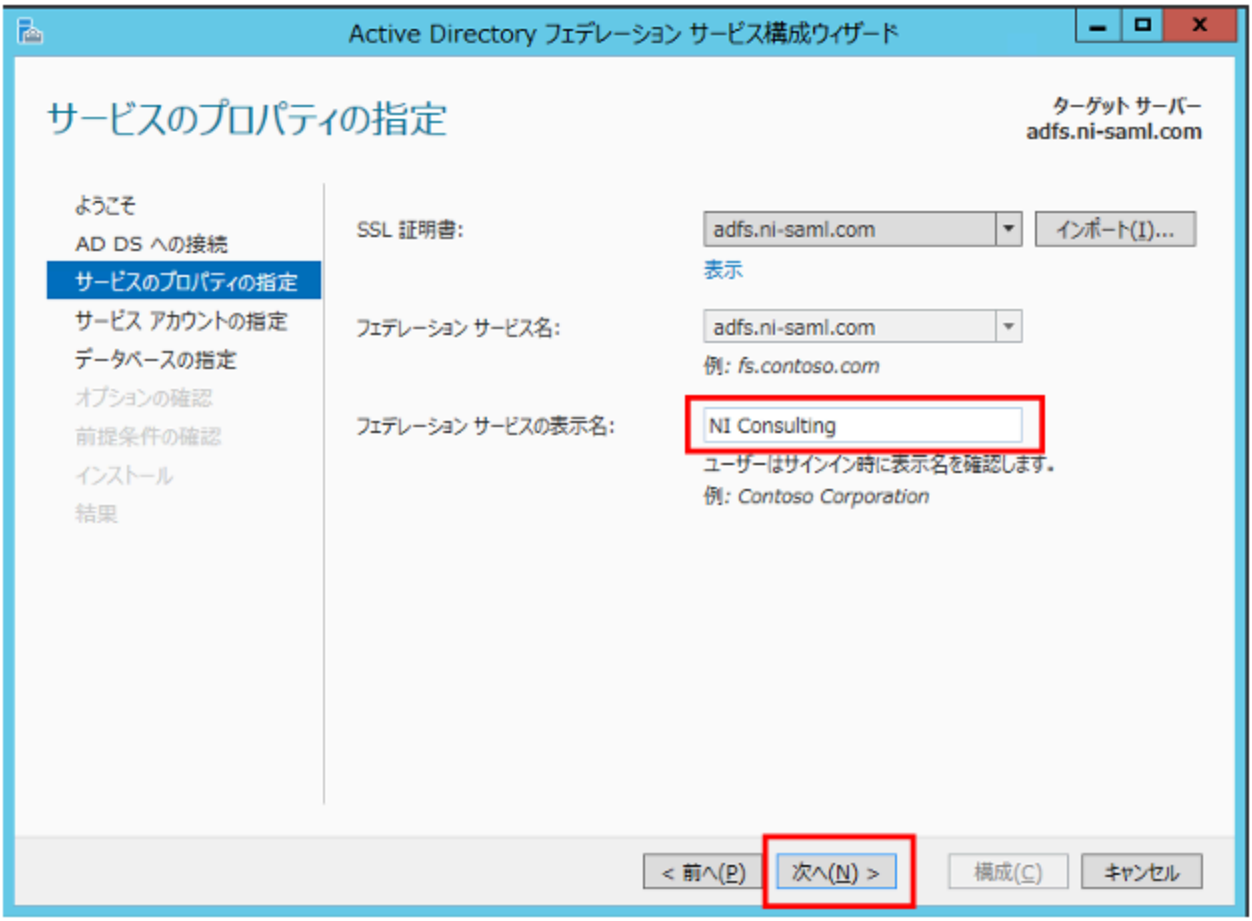


4. 「インポート」をクリックし、.pfx形式の証明書ファイルを選択します。
   証明書にパスワードが設定されている場合は入力して「OK」をクリックします。

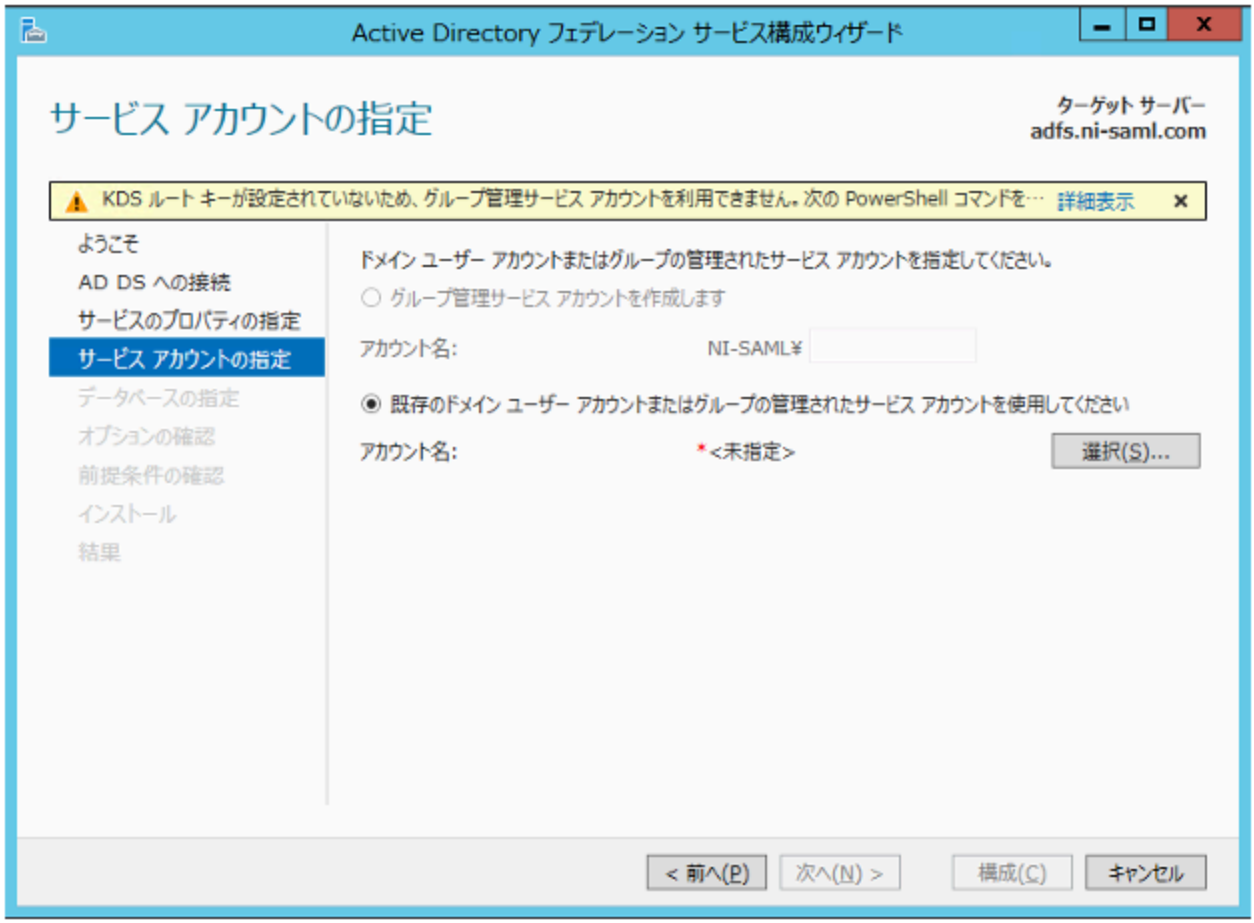


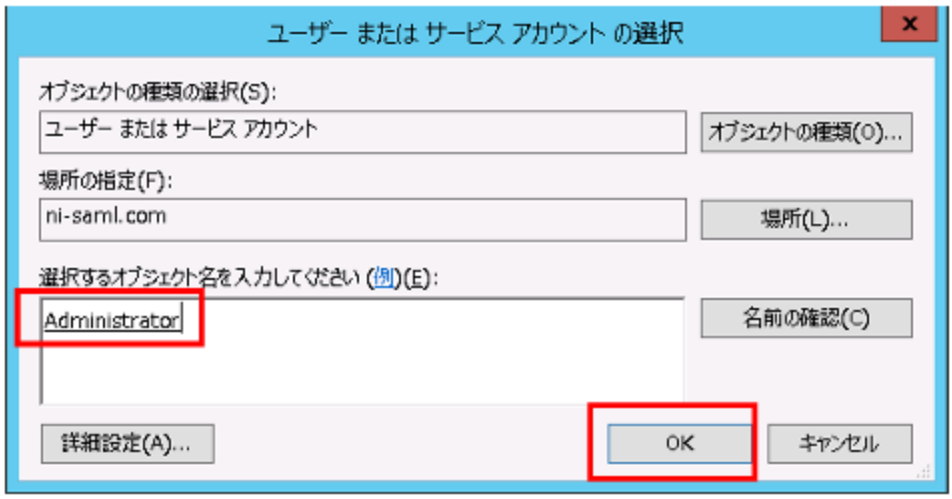



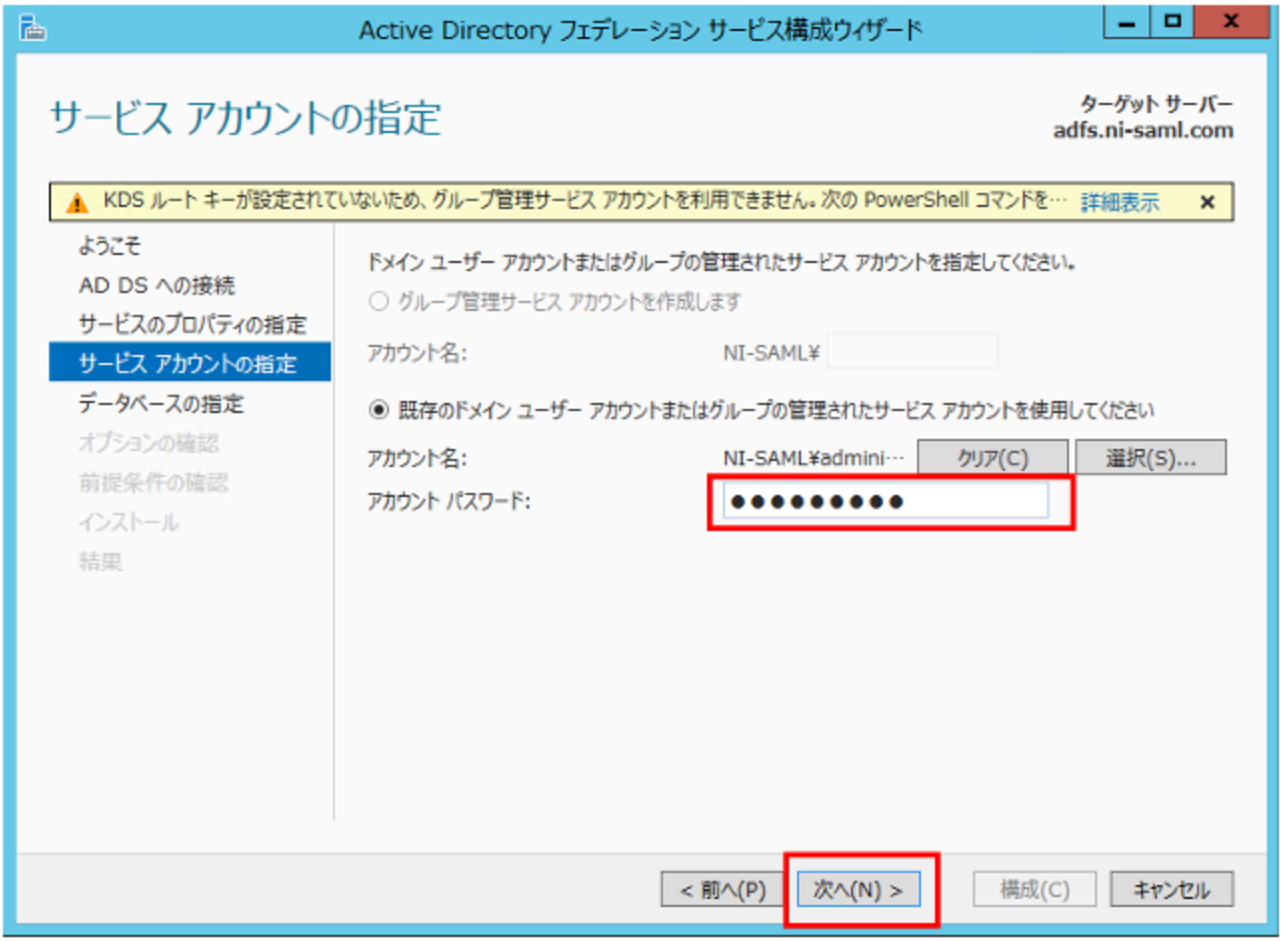
5. フェデレーションサービスの表示名を入力し、「次へ」をクリックします。
※表示名は、パスワード認証使用時に、IdPのログイン画面に表示される名称です。



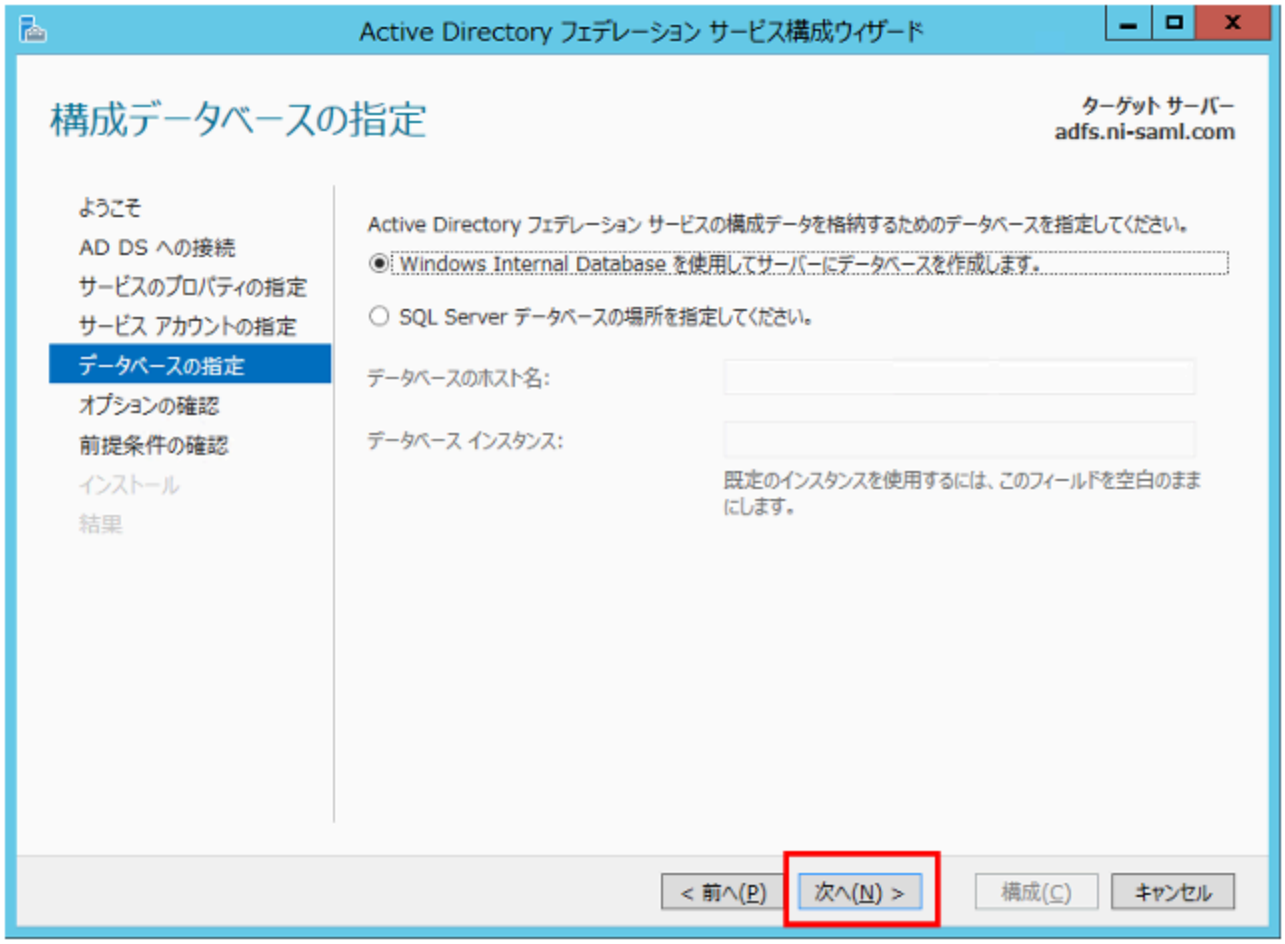
6. サービスアカウントに「Administrator」を選択し、パスワードを入力し、「次へ」をクリックします。



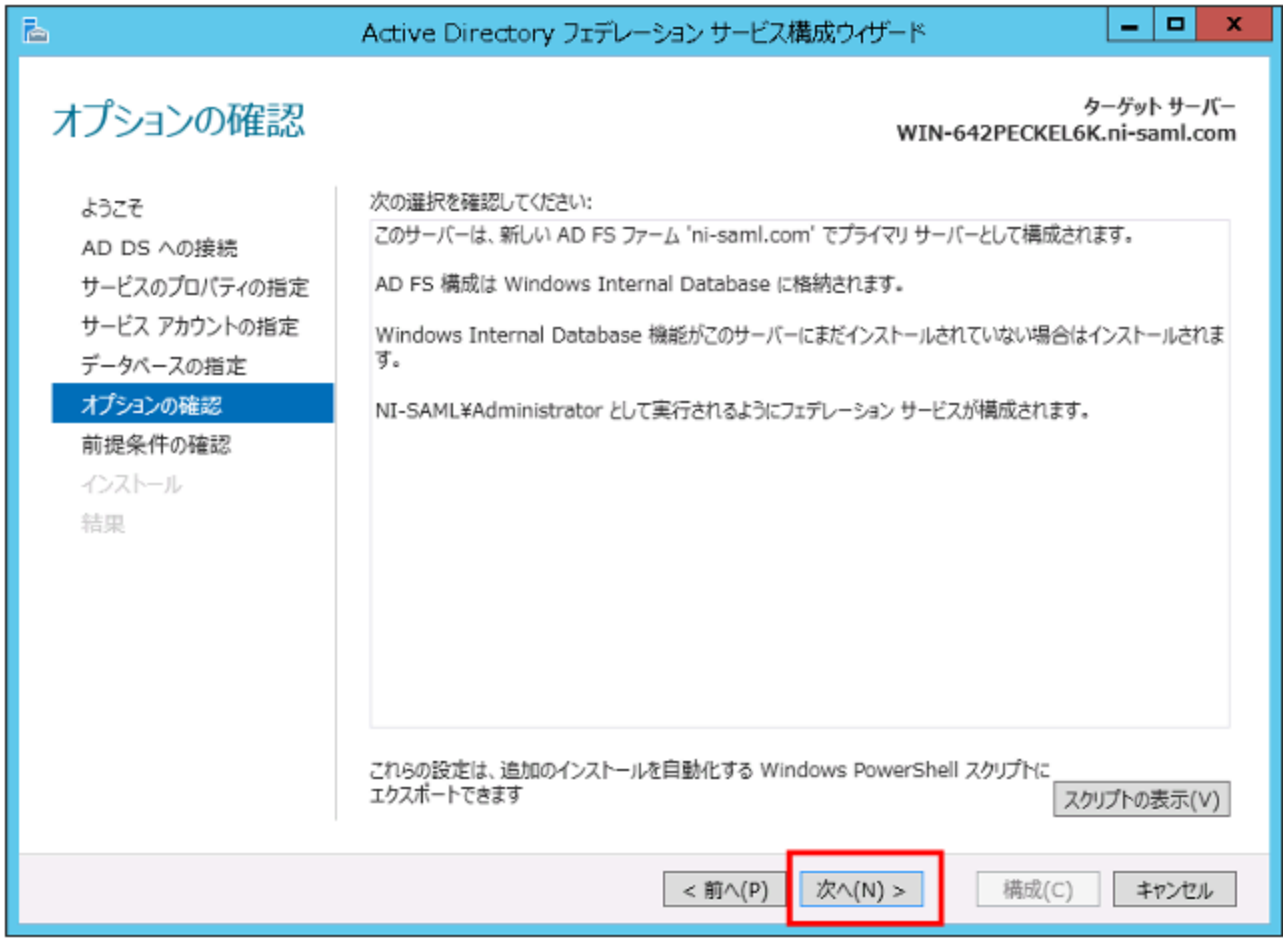




Active Directory フェデレーション サービス構成ウィザード
サービス アカウントの指定
ターゲット サーバー
adfs.ni-saml.com
KDS ルート キーが設定されていないため、グループ管理サービス アカウントを利用できません。次の PowerShell コマンドを… 詳細表示
ようこそ
AD DS への接続
サービスのプロパティの指定
サービス アカウントの指定
データベースの指定
オプションの確認
前提条件の確認
インストール
結果
ドメイン ユーザー アカウントまたはグループの管理されたサービス アカウントを指定してください。
グループ管理サービス アカウントを作成します
アカウント名:
NI-SAML¥
既存のドメイン ユーザー アカウントまたはグループの管理されたサービス アカウントを使用してください
アカウント名:
NI-SAML¥admini…
クリア(C)
選択(S)...
アカウント パスワード:
●●●●●●●●●
< 前へ(P)
次へ(N) >
構成(C)
キャンセル

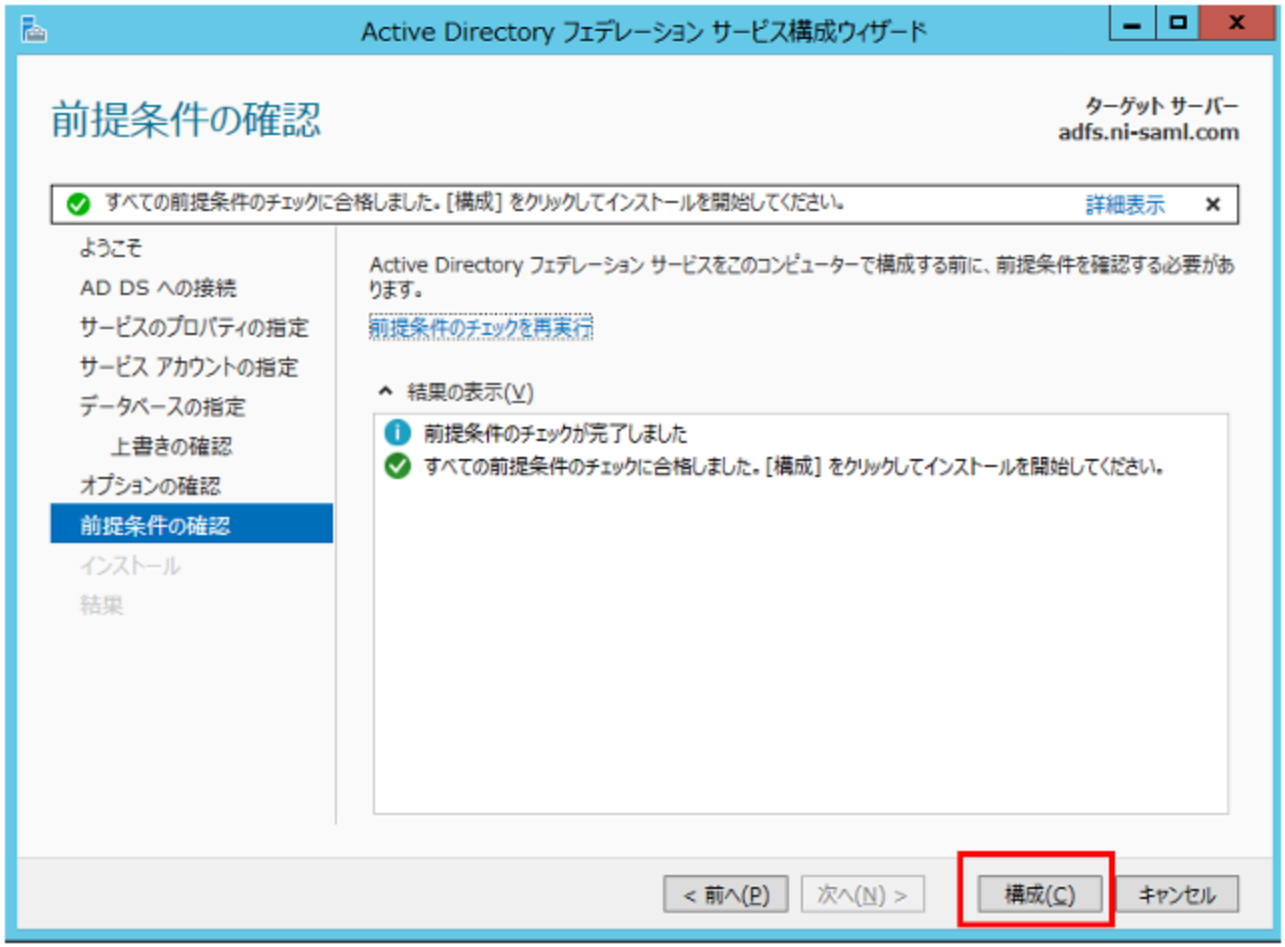
7. 「Windows Internal Databaseを使用してサーバーにデータベースを作成します。」を選択して、「次へ」をクリックします。

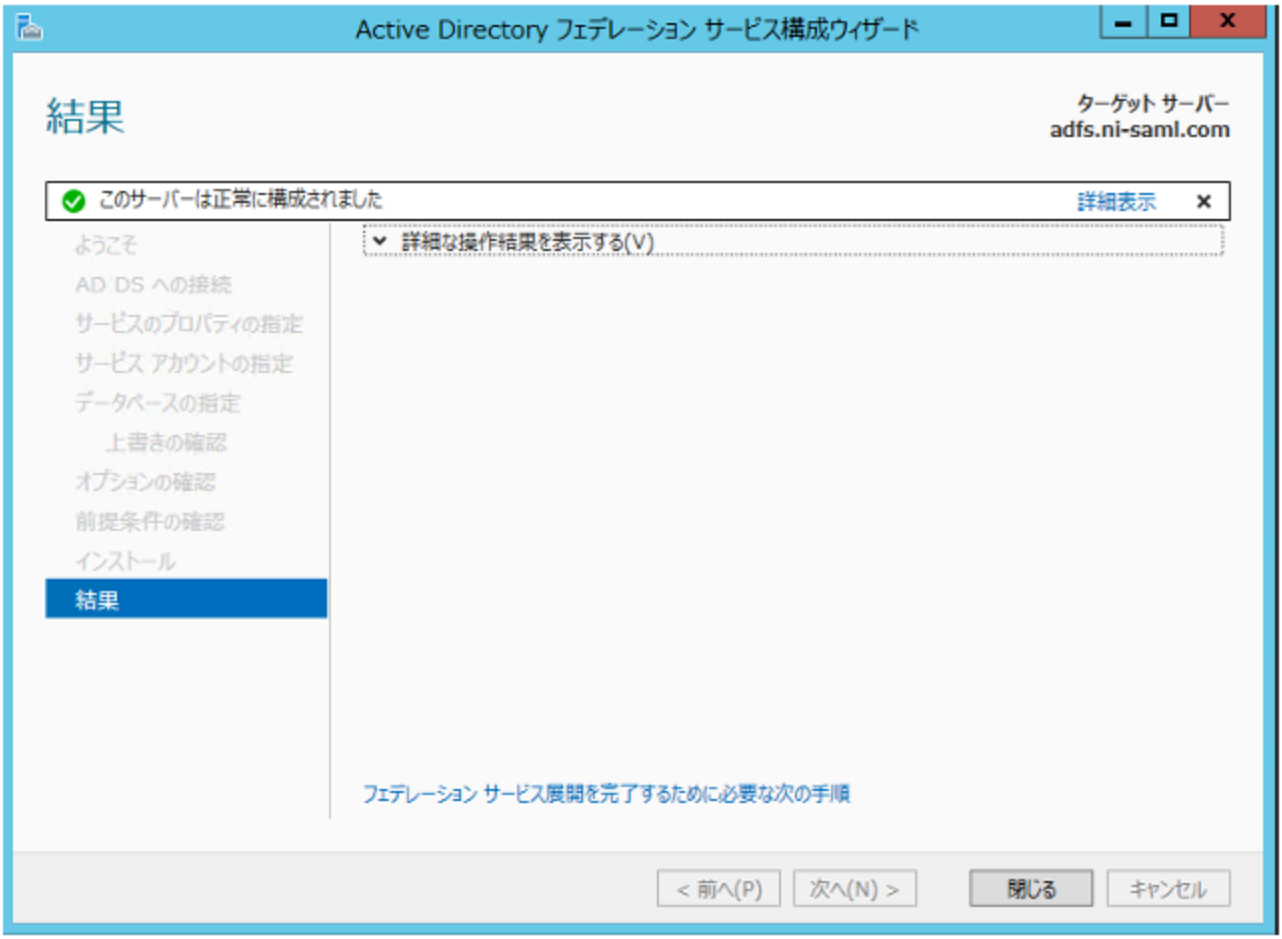


8. 「次へ」をクリックします。



9. 「構成」をクリックします。
画面に「このサーバーは正常に構成されました」と表示されることを確認します。




Active Directory フェデレーション サービス構成ウィザード
結果
ターゲット サーバー
adfs.ni-saml.com
このサーバーは正常に構成されました
詳細表示
ようこそ
AD DS への接続
サービスのプロパティの指定
サービス アカウントの指定
データベースの指定
上書きの確認
オプションの確認
前提条件の確認
インストール
結果
詳細な操作結果を表示する(V)
フェデレーション サービス展開を完了するために必要な次の手順
< 前へ(P)
次へ(N) >
閉じる
キャンセル

## NI製品の設定

### システム設定

1. システム設定の「セキュリティ」タブより「SAML認証」を選択します。
   ⇒「認証／SAML認証」画面が表示されます。

2. 以下の項目を入力し、「保存」ボタンをクリックします。

| 項目名称 | 説明 | 設定値 |
|---|---|---|
| シングルサインオン設定 | | |
| シングルサインオン | シングルサインオンを利用するかしないかを設定します。 | 利用する |
| 有効範囲 | SAML認証を許可する接続元IPアドレスを改行区切りで指定します。空白の場合は、すべての接続でSAML認証を行います。 | ※補足を参照 |
| Service Provider(NI製品)設定 | | |
| エンティティID | Service Providerの識別子。任意の文字列を設定します。<br>※初期値のURLから変更する必要はありません。 | https://xxx.xxx.xxx.xxx/ni/ |
| エンドポイントURL | SAMLレスポンスを受信するURLです。<br>※Identity Providerのセットアップに使用する固定値です。 | － |
| 仮名 | 仮名IDを用いた認証を利用するかしないかを設定します。 | 利用する/利用しない |
| 認証方法 | 認証にパスワード認証を用いるか、Windows認証を用いるかを設定します。 | Windows認証/パスワード認証 |
| ログアウトURL | NI製品からログアウト後に遷移するURLを設定します。 | https://<IdPサーバーのアドレス>/adfs/ls/?wa=wsignout1.0<br>（※IdPのログアウト画面） |

補足

- NI製品からログアウトする際に、IdPからもログアウトする必要がない場合は、ログアウトURLに下記URLを設定することで、通常のNI製品ログイン画面に遷移します。

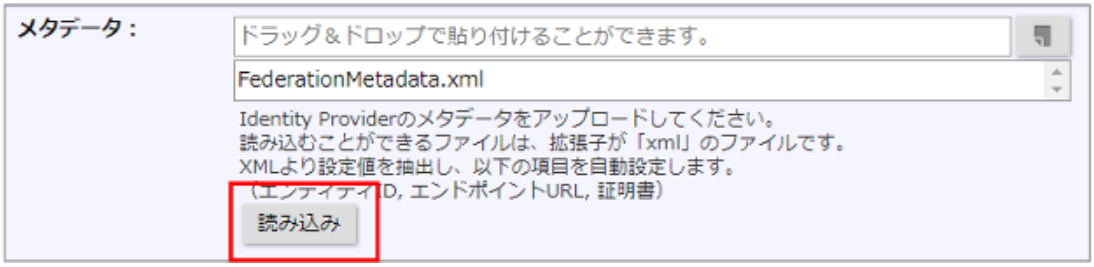
  **https://<任意のNI製品URL>?saml=no**

- 社内端末のIPアドレスを「有効範囲」に指定することで、モバイル端末など社外からの接続によりIdPに接続不可の場合は、「有効範囲」外となるため、SAML認証が適用されず、通常のログイン画面が表示されます。

注意

- エンティティID、仮名を変更した場合、IdPの再設定が必要になります。
- 仮名を利用するかしないかで、IdPの設定手順が異なります。

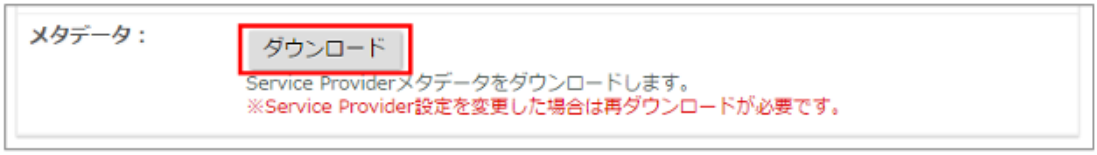
3. IdPメタデータをアップロードします。
   下記URLにブラウザでアクセスし、IdPメタデータXMLファイルをPCに保存します。
   **https://<IdPサーバーのアドレス>/FederationMetadata/2007-06/FederationMetadata.xml**
   NI製品システム設定「認証／SAML認証」画面の、Identity Provider設定の「メタデータ」に 上記で保存したIdPメタデータXMLファイルを添付します。
   「読み込み」ボタンをクリックします。




   以下の設定項目が自動で入力されます。

| 項目名称 | 説明 | 設定サンプル値 |
|---|---|---|
| Identity Provider設定 | | |
| エンティティID | Identity Providerの識別子を設定します。 | http://<IdPサーバーのアドレス>/adfs/services/trust |
| エンドポイントURL | SAMLリクエストを送信するURLを設定します。 | https://<IdPサーバーのアドレス>/adfs/ls/ |
| 証明書 | Identity Providerが署名に使用する公開鍵を設定します。<br>カンマ区切りで複数証明書を指定できます。 | Base64エンコードされた文字列 |

4. SPメタデータをダウンロードします。
   Service Provider(NI製品)設定の「メタデータ」の「ダウンロード」ボタンをクリックします。




   ⇒SPメタデータXMLファイルがダウンロードされます。「IdPの設定(Windows Server 2016－ADFS)」にて使用します。

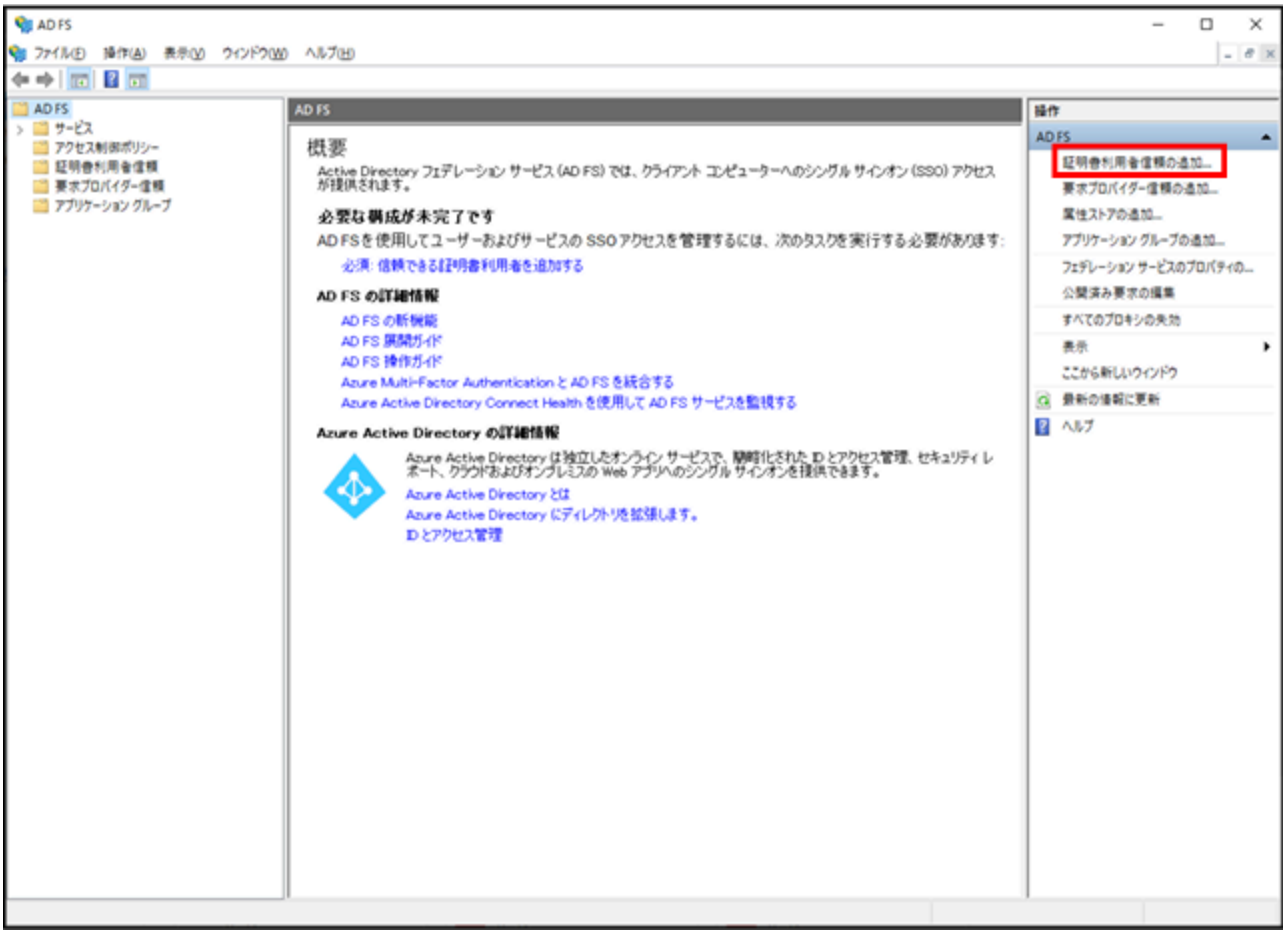
5. 「保存」ボタンをクリックします。

# IdPの設定(Windows Server 2016－ADFS)

IdPサーバーで下記の設定を行います。

### 証明書利用者信頼（SP）の追加

1. AD FSの管理ツールを表示し、「証明書利用者信頼の追加」をクリックします。

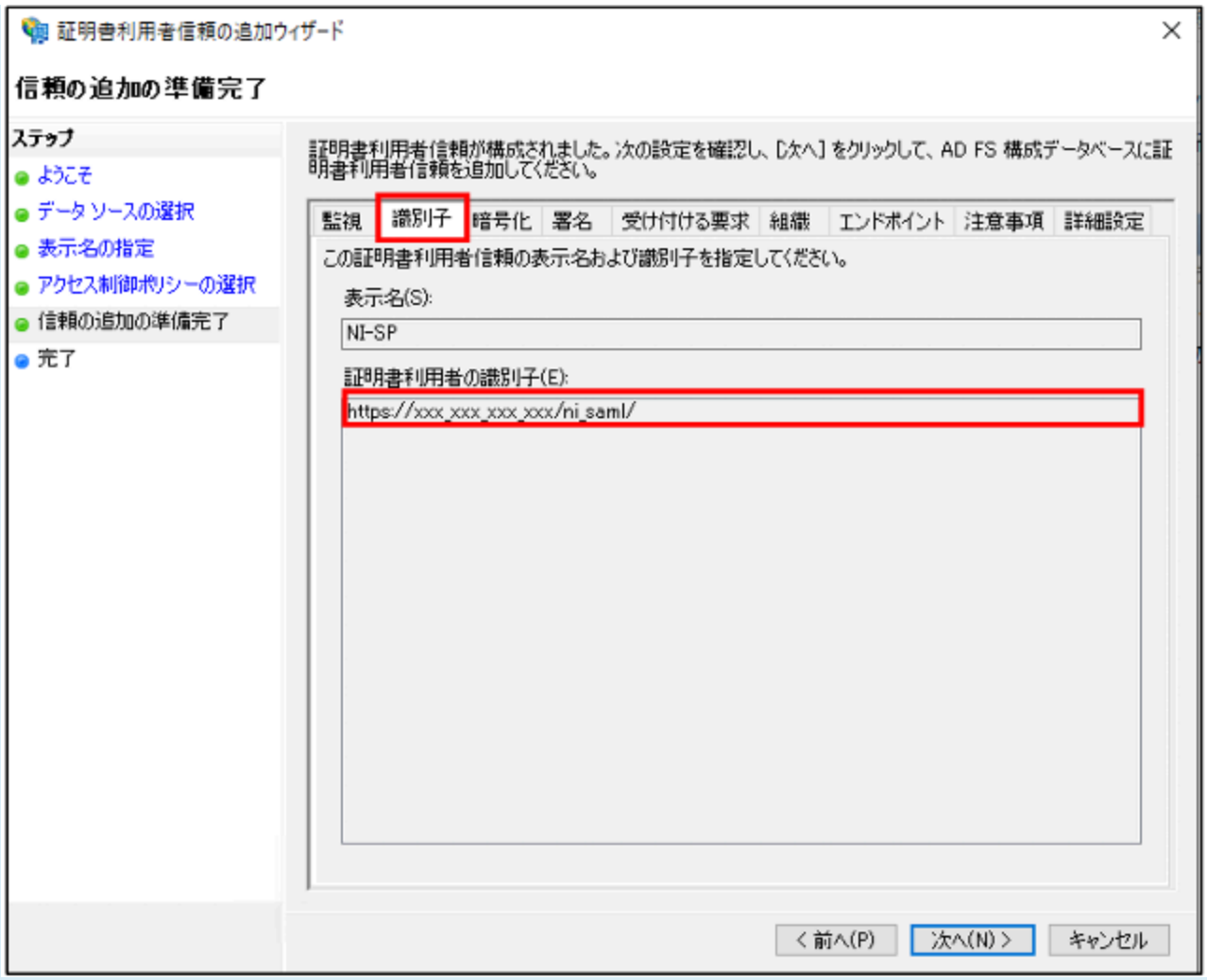


2. 証明書利用者信頼の追加ウィザードが表示されたら、「要求に対応する」を選択し、「開始」をクリックします。

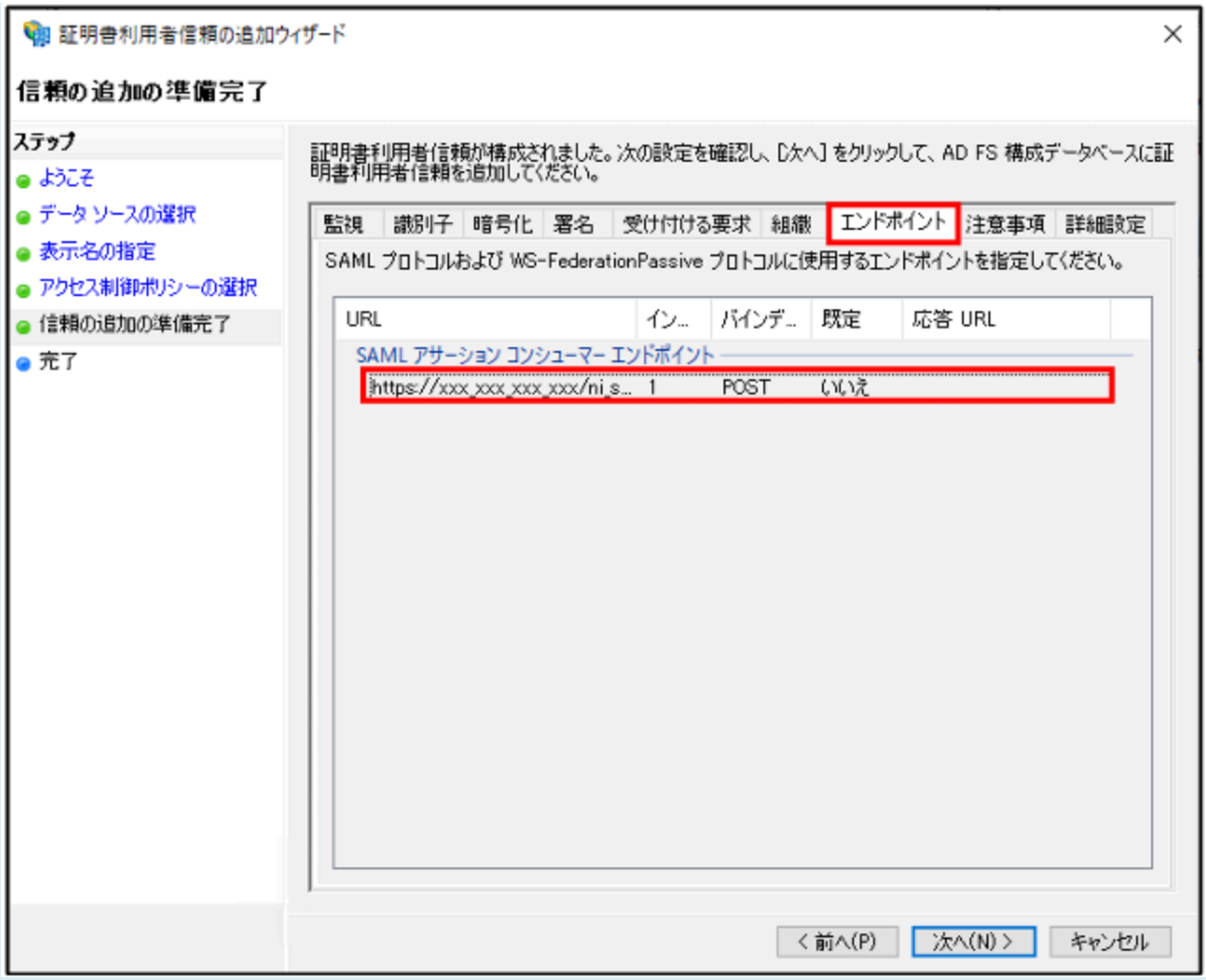
3. 「証明書利用者についてのデータをファイルからインポートする」を選択し、「参照」ボタンをクリックします。
「システム設定」でダウンロードしたSPメタデータを選択します。


## 補足

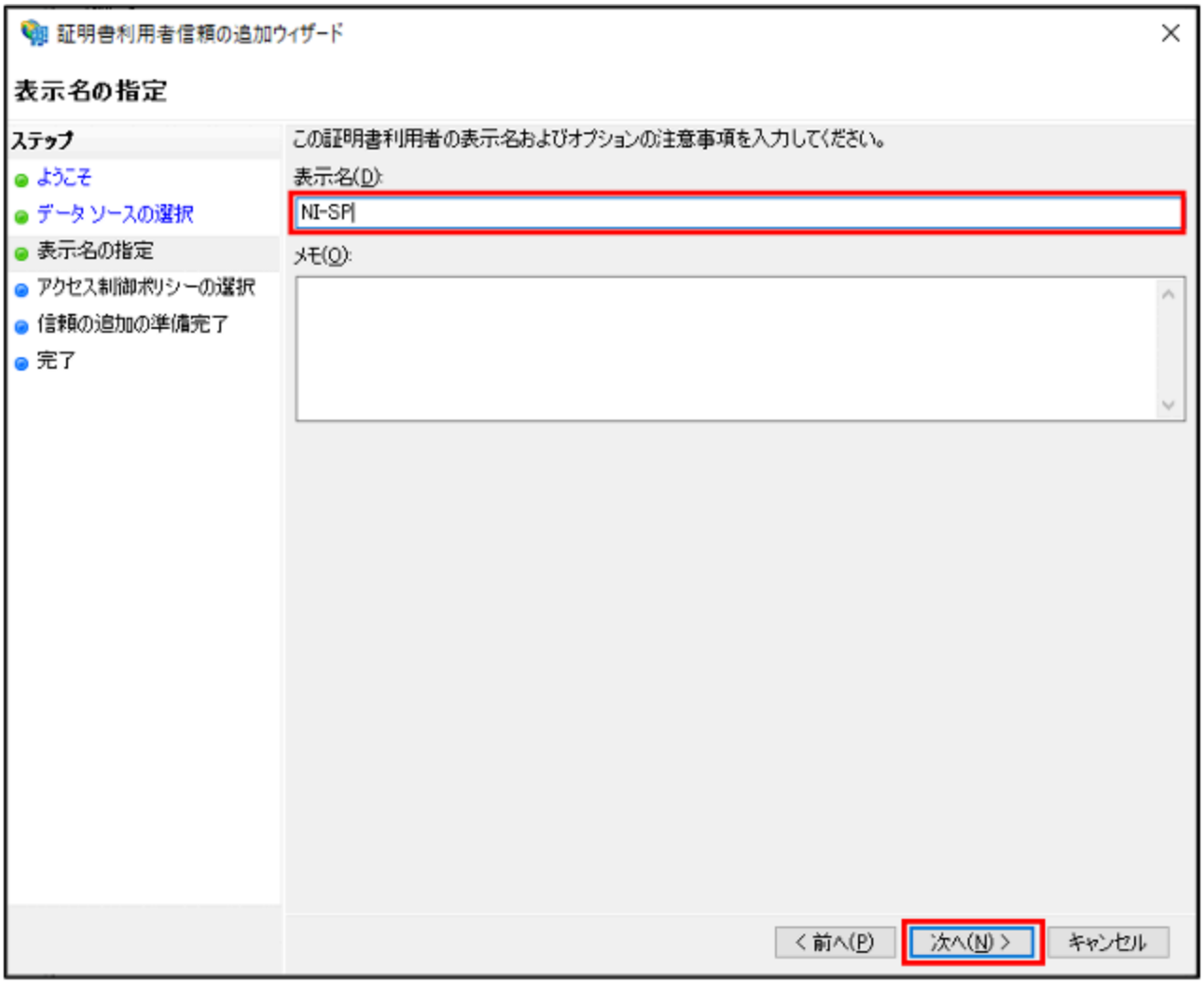
- SPメタデータをインポートすることで、以下の値が自動でセットされます。
セットされた値は、「信頼の追加の準備完了」の項で確認することができます。
「証明書利用者の識別子」：NI製品システム設定画面の「エンティティID」の値がセットされます。



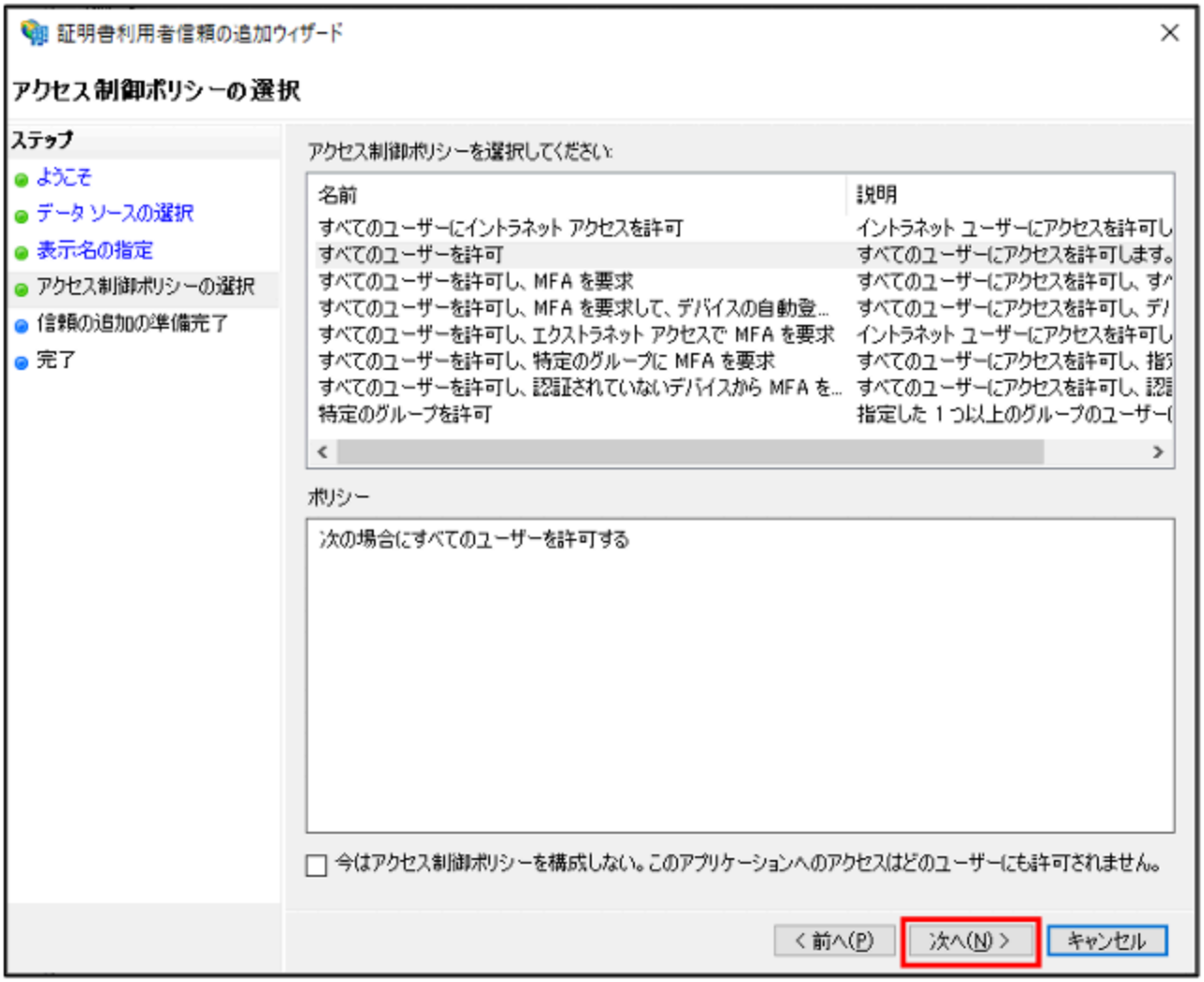

「SAML アサーション コンシューマー エンドポイント」：NI製品システム設定画面の「エンドポイントURL」の値がセットされます。


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
SAML プロトコルおよび WS-FederationPassive プロトコルに使用するエンドポイントを指定してください。
URL
イン...
バインデ...
既定
応答 URL
SAML アサーション コンシューマー エンドポイント
https://xxx.xxx.xxx.xxx/ni_s... 1 POST いいえ
< 前へ(P)
次へ(N) >
キャンセル

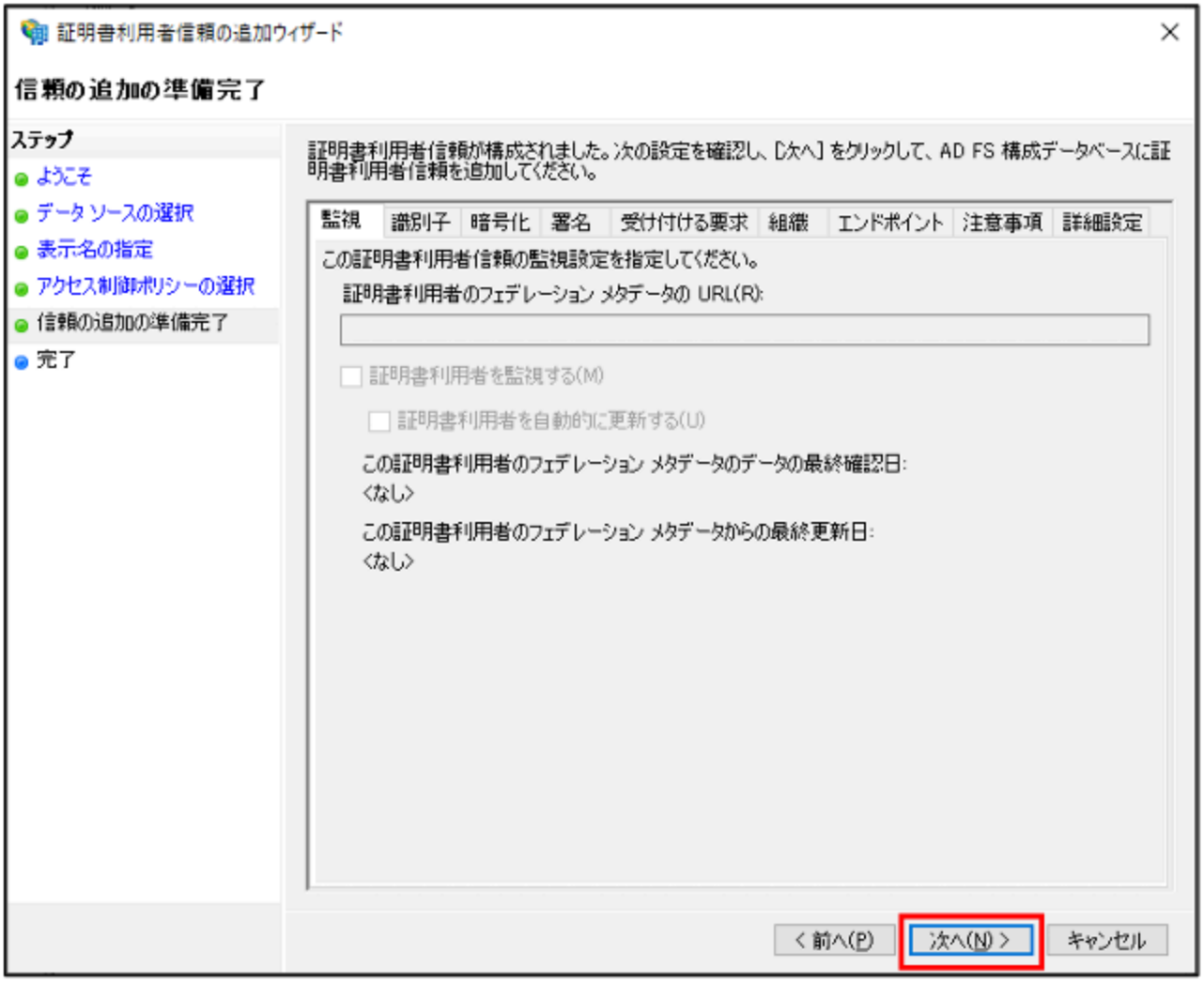
4. 表示名を入力し、「次へ」をクリックします。
※表示名はAD FSの管理ツール上で表示される名称です。



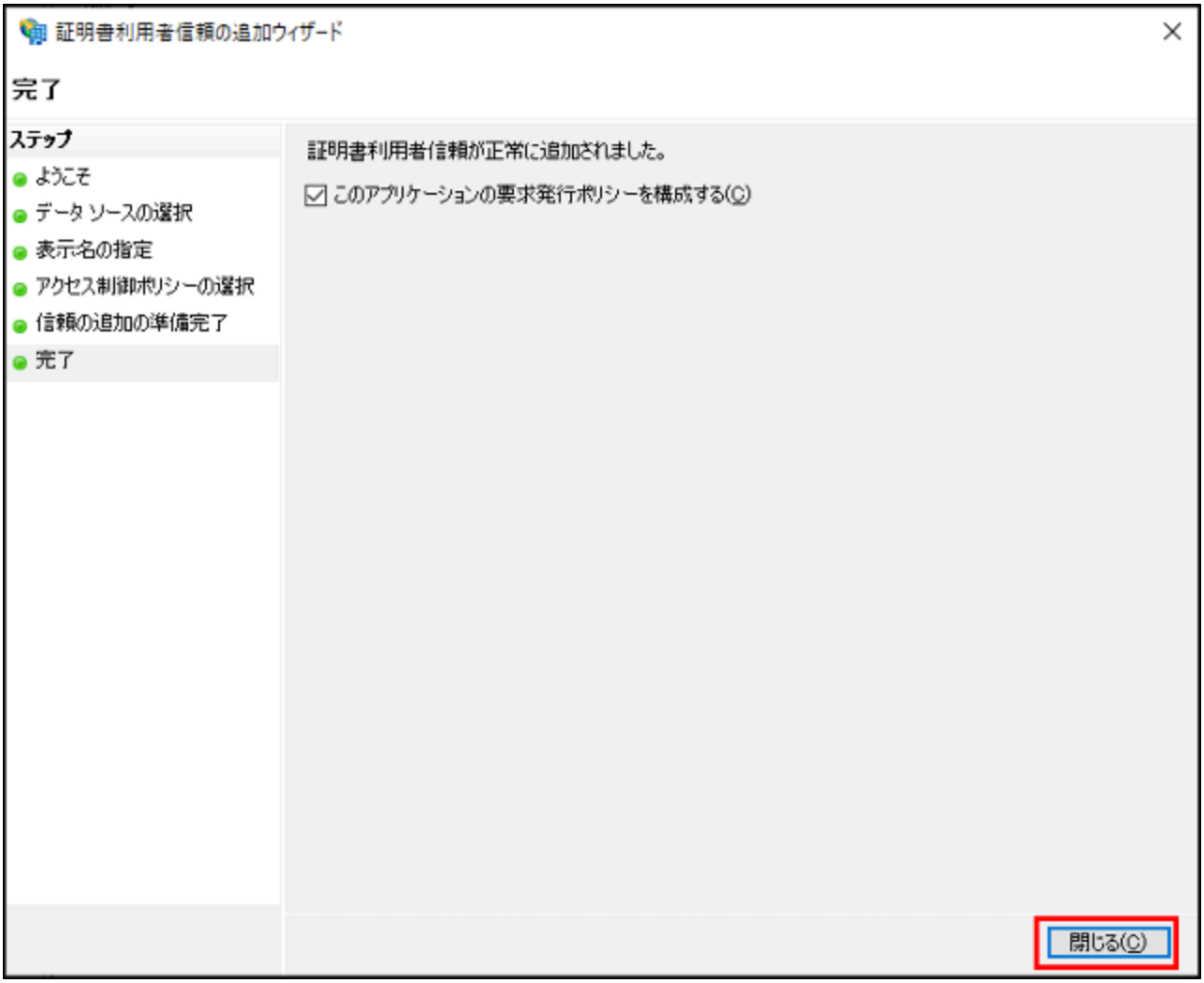
5. 表示された画面のまま、「次へ」をクリックします。



6. 「次へ」をクリックします。

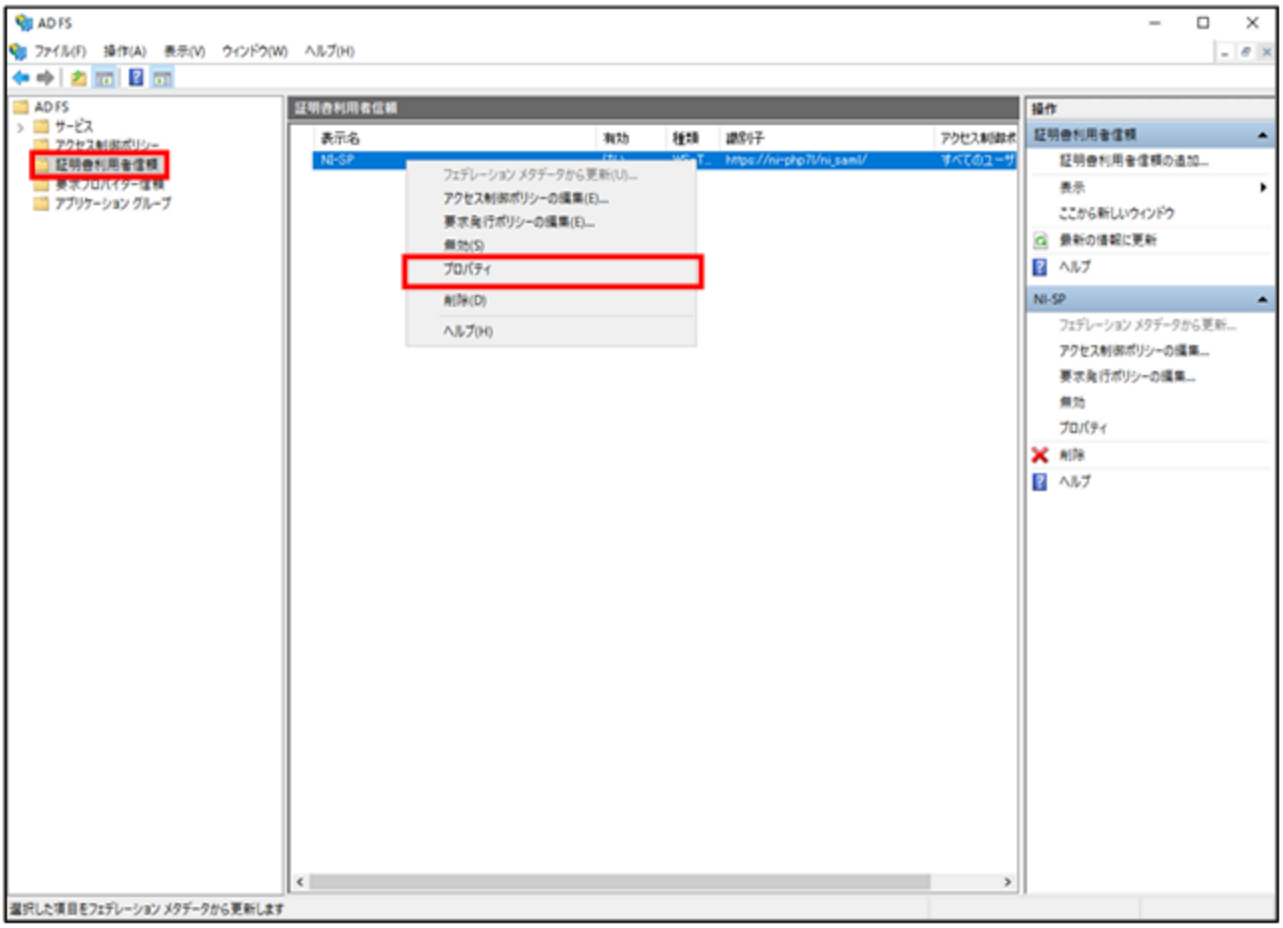


7. 証明書利用者信頼の追加が完了したので、「このアプリケーションの要求発行ポリシーを構成する」にチェックを付けたまま、「閉じる」ボタンをクリックします。



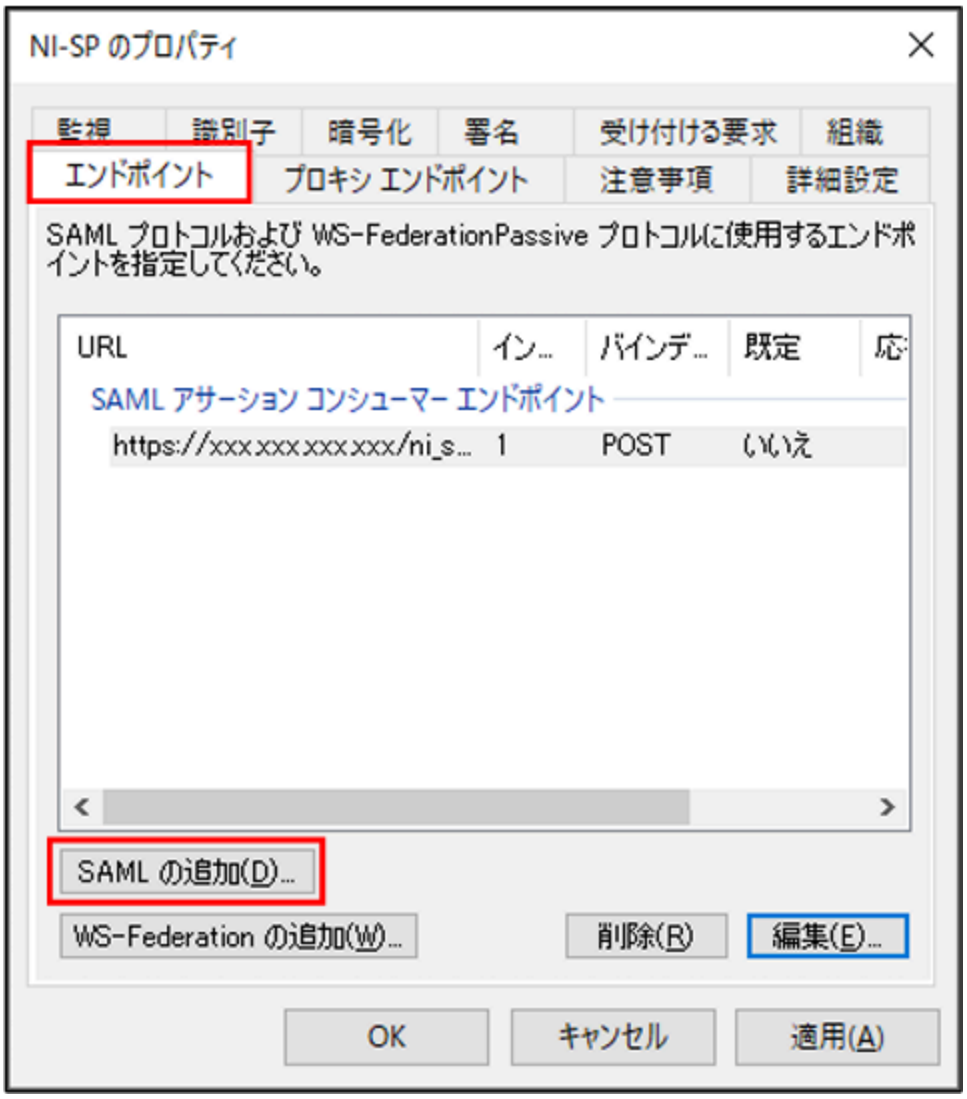
## エンドポイントURLの追加

1. AD FSの管理ツールを表示し、「証明書利用者信頼」メニューを選択します。
   追加した証明書利用者信頼を右クリックし、「プロパティ」を選択します。



2. SAMLリクエスト用エンドポイントの追加

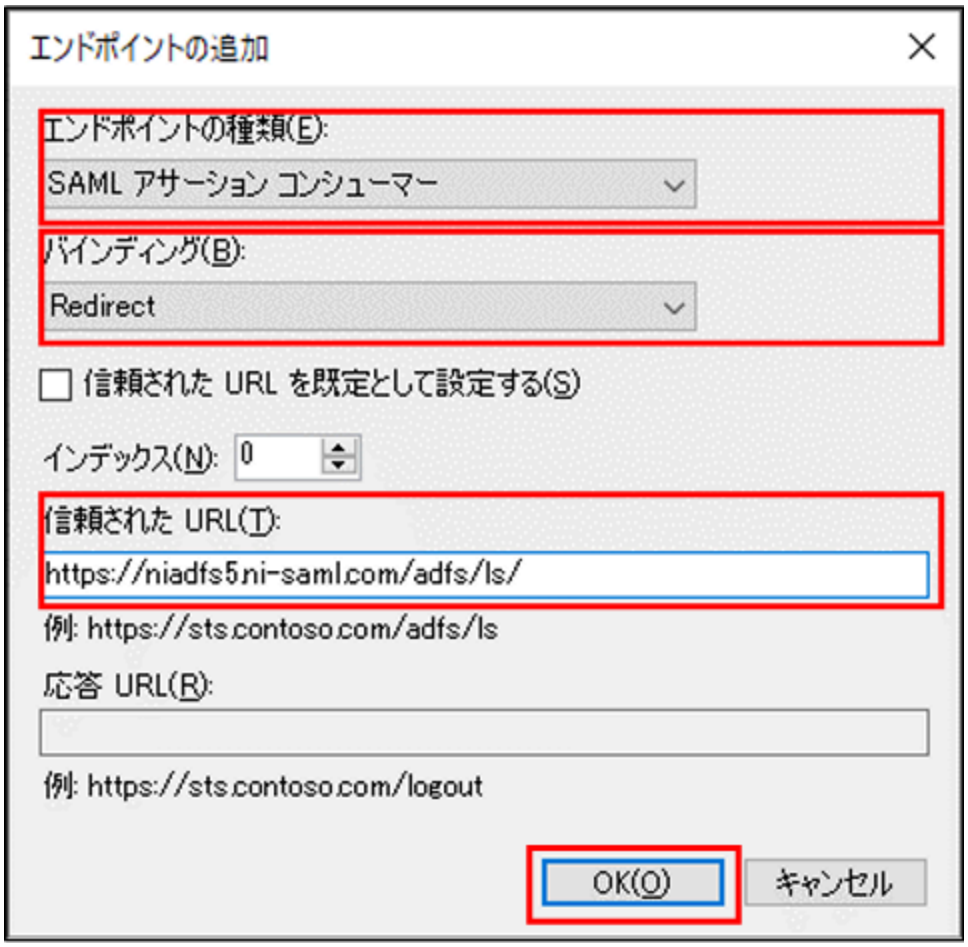
「エンドポイント」タブを選択し、「SAMLの追加」をクリックします。




下記の値を設定し、「OK」をクリックします。

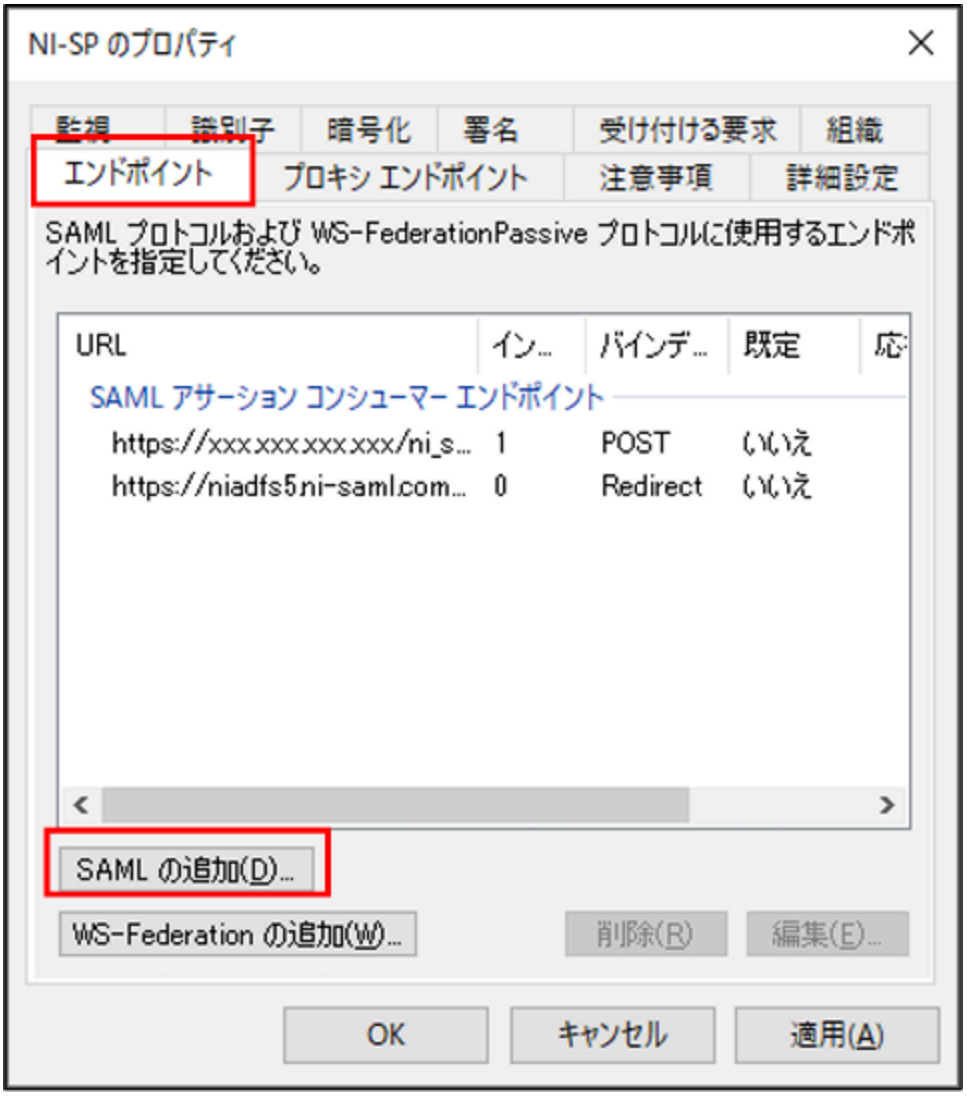
- エンドポイントの種類：「SAMLアサーションコンシューマー」を選択します。
- バインディング：「Redirect」を選択します。
- 「信頼されたURL」：次のURLを入力します。

  **https://<IdPサーバーのアドレス>/adfs/ls/**


エンドポイントの追加
エンドポイントの種類(E):
SAML アサーション コンシューマー
バインディング(B):
Redirect
信頼された URL を既定として設定する(S)
インデックス(N):
0
信頼された URL(T):
https://niadfs5.ni-saml.com/adfs/ls/
例: https://sts.contoso.com/adfs/ls
応答 URL(R):
例: https://sts.contoso.com/logout
OK(O)
キャンセル

3. ログアウト用エンドポイントの追加

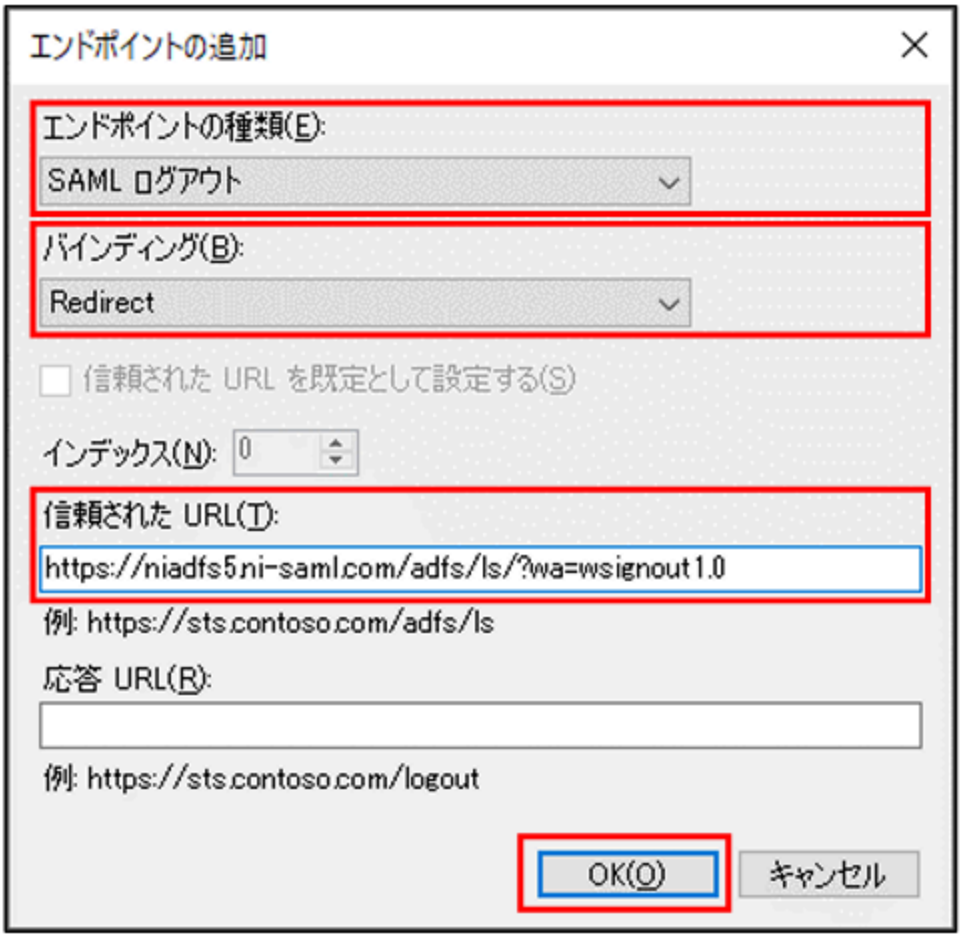
「エンドポイント」タブを選択し、「SAMLの追加」をクリックします。



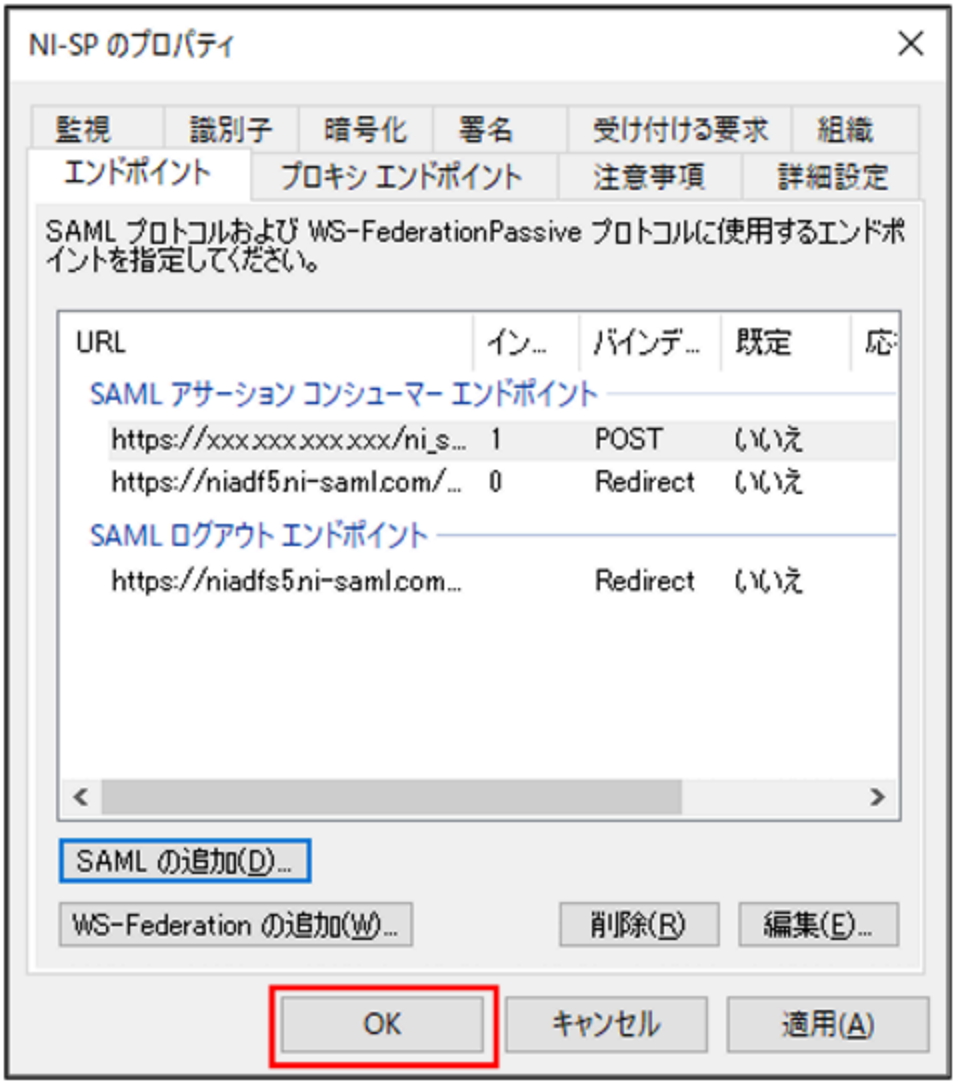

下記の値を設定し、「OK」をクリックします。

- エンドポイントの種類：「SAMLログアウト」を選択します。
- バインディング：「Redirect」を選択します。
- 「信頼されたURL」：次のURLを入力します。

  **https://<IdPサーバーのアドレス>/adfs/ls/?wa=wsignout1.0**


エンドポイントの追加
エンドポイントの種類(E):
SAML ログアウト
バインディング(B):
Redirect
信頼された URL を既定として設定する(S)
インデックス(N):
0
信頼された URL(T):
https://niadfs5.ni-saml.com/adfs/ls/?wa=wsignout1.0
例: https://sts.contoso.com/adfs/ls
応答 URL(R):
例: https://sts.contoso.com/logout
OK(O)
キャンセル

4. 「OK」をクリックします。



## 変換要求規則の追加

### ■仮名を利用する場合

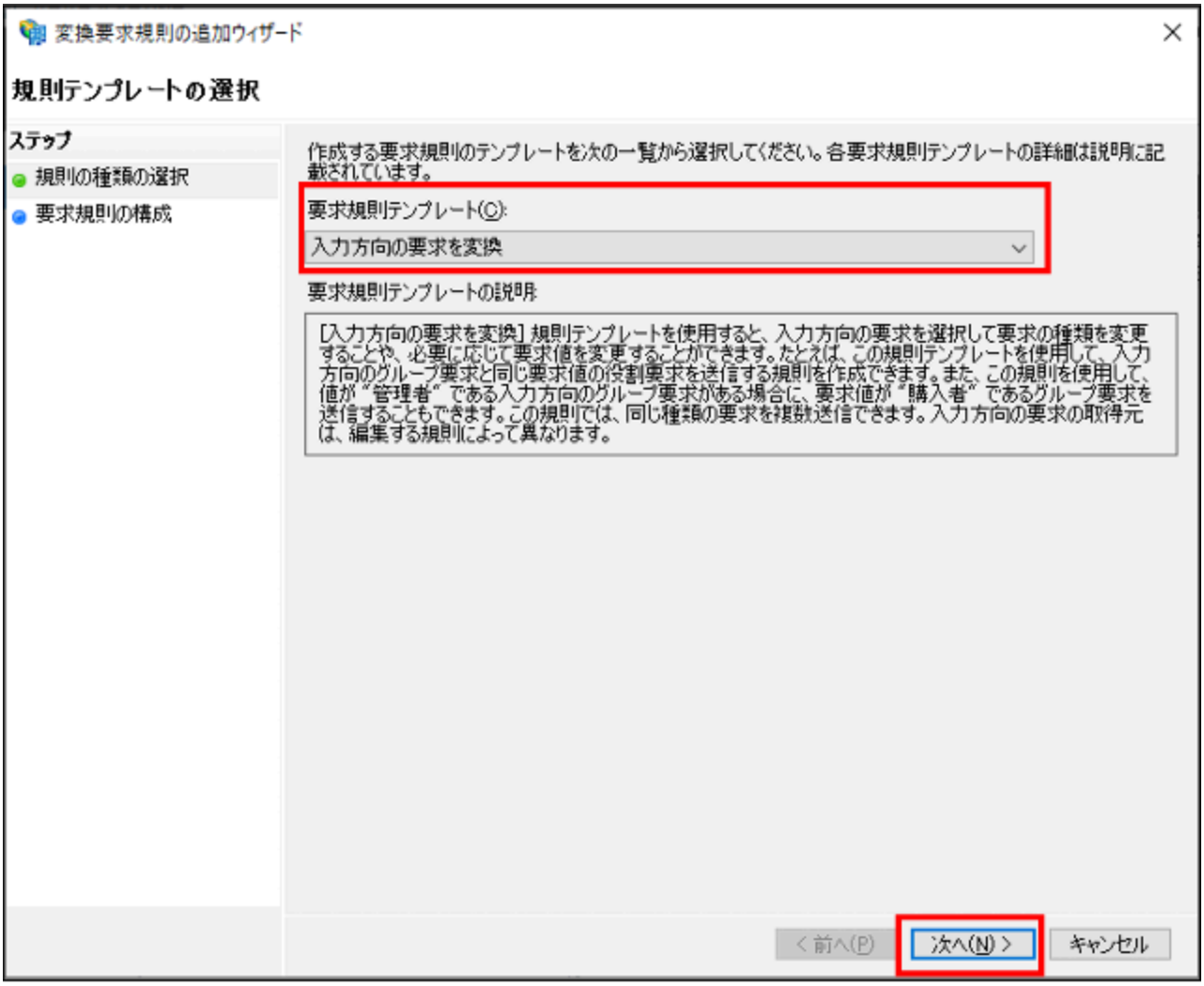
> 補足
>
> - NameIDとして、ランダムな識別子（仮名）を返すように設定を行います。

1. 以下の2つの変換要求規則を追加します。
   要求規則テンプレートに「カスタム規則を使用して要求を送信」を選択して、「次へ」をクリックします。

2. 以下のカスタムルールをコピー&ペーストし、完了をクリックします。

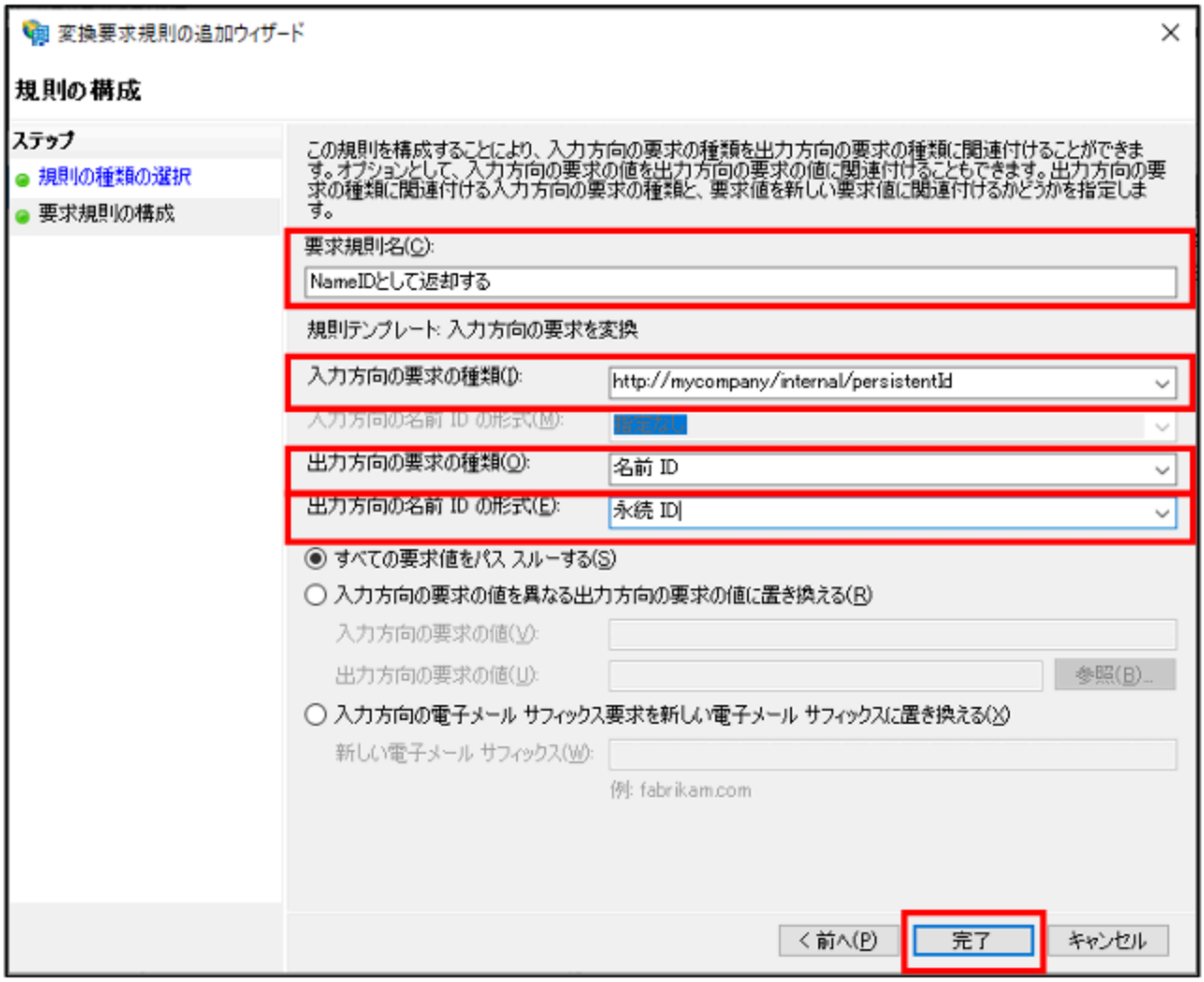
**c:[type ==**
**“http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname” ]=> add(**
**store = “_OpaqueIdStore”,**
**types = (“http://mycompany/internal/persistentId”),**
**query = “{0};{1};{2}”,**
**param = “ppid”,**
**param = c.Value,**
**param = c.OriginalIssuer);**

3. 「入力方向の要求を変換」を選択し、「次へ」をクリックします。

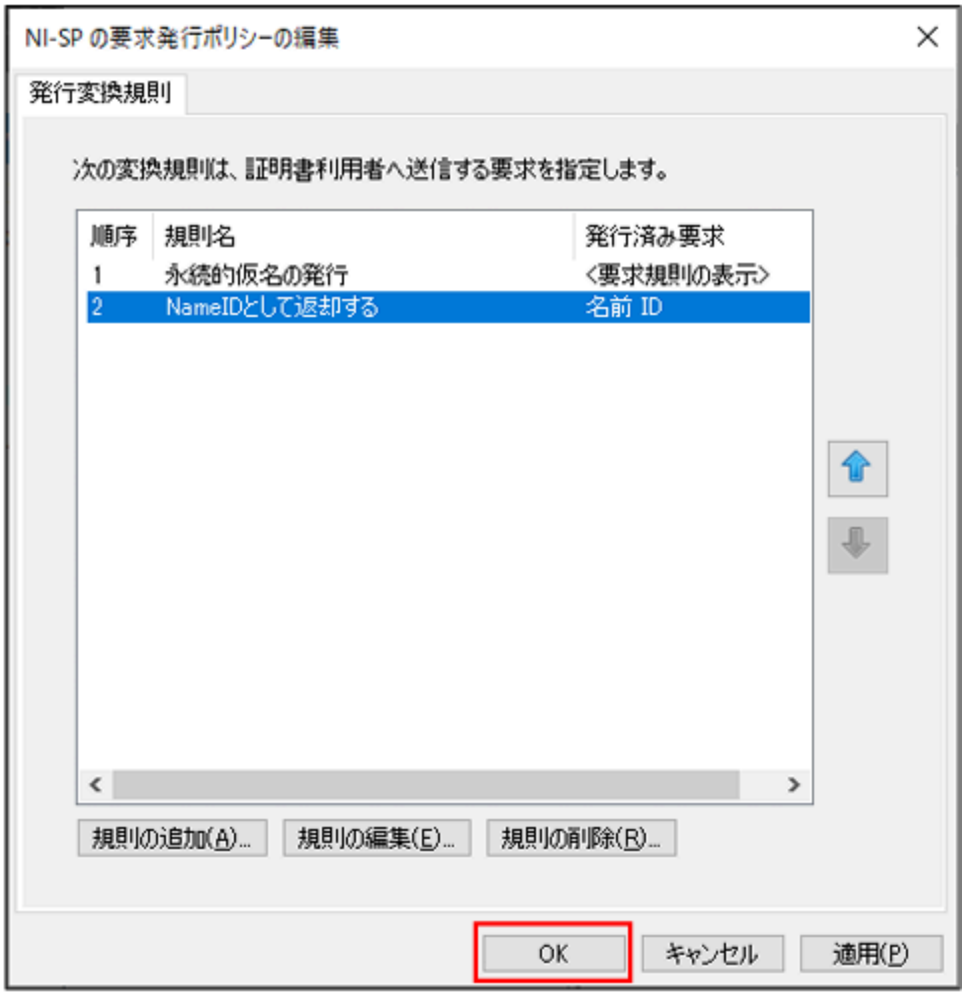



以下の値を選択し、「完了」をクリックします。

- 要求規則名：任意の名称を入力します。
- 入力方向の要求の種類：「http://mycompany/internal/persistentId」をコピー&ペーストで入力します。
- 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：「永続ID」を選択します。


変換要求規則の追加ウィザード
規則の構成
ステップ
規則の種類の選択
要求規則の構成
この規則を構成することにより、入力方向の要求の種類を出力方向の要求の種類に関連付けることができます。オプションとして、入力方向の要求の値を出力方向の要求の値に関連付けることもできます。出力方向の要求の種類に関連付ける入力方向の要求の種類と、要求値を新しい要求値に関連付けるかどうかを指定します。
要求規則名(C):
NameIDとして返却する
規則テンプレート: 入力方向の要求を変換
入力方向の要求の種類(I):
http://mycompany/internal/persistentId
入力方向の名前 ID の形式(M):
出力方向の要求の種類(O):
名前 ID
出力方向の名前 ID の形式(E):
永続 ID
すべての要求値をパス スルーする(S)
入力方向の要求の値を異なる出力方向の要求の値に置き換える(R)
入力方向の要求の値(V):
出力方向の要求の値(U):
参照(B)...
入力方向の電子メール サフィックス要求を新しい電子メール サフィックスに置き換える(X)
新しい電子メール サフィックス(W):
例: fabrikam.com
< 前へ(P)
完了
キャンセル

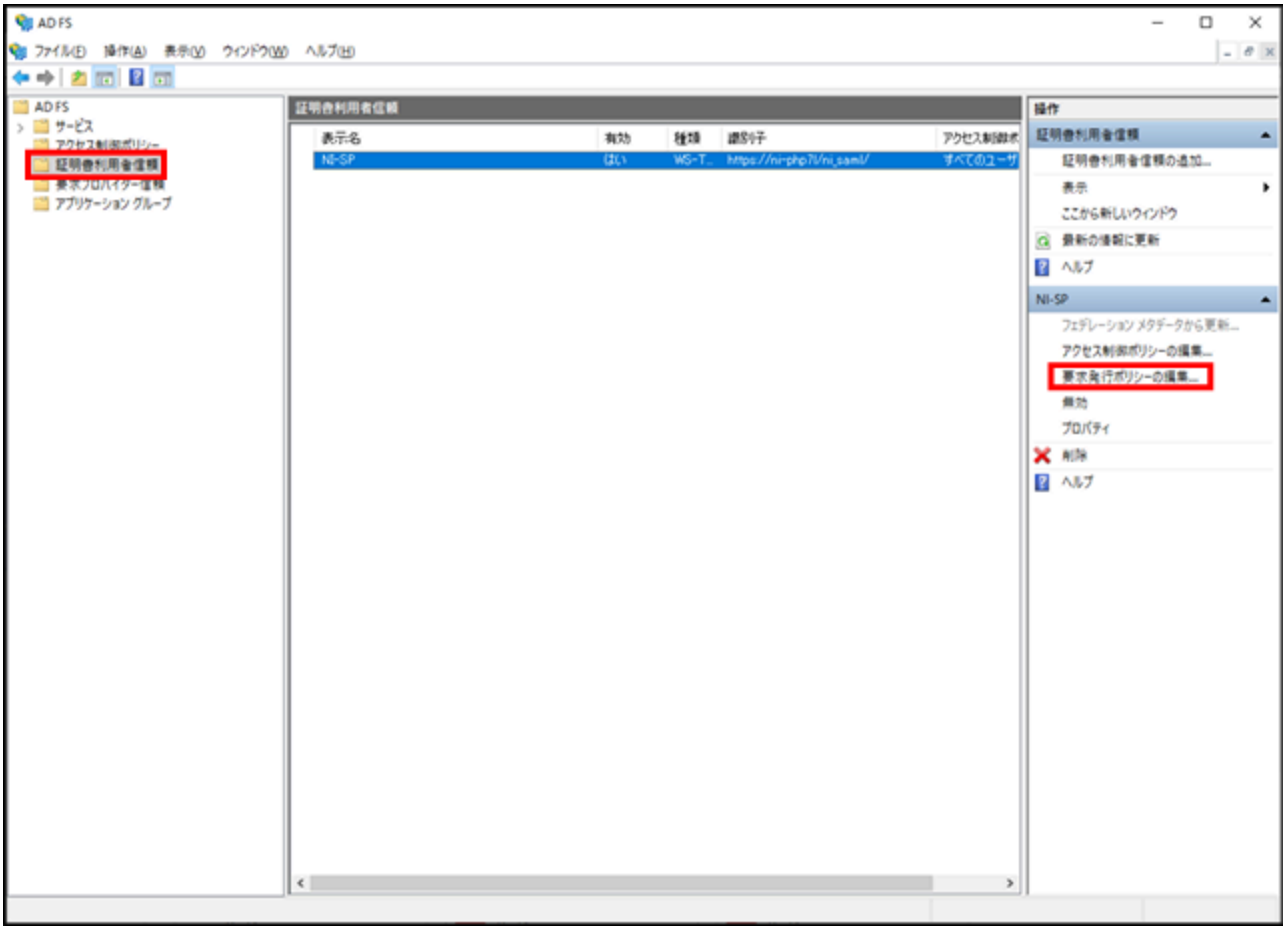
4. 「OK」をクリックします。



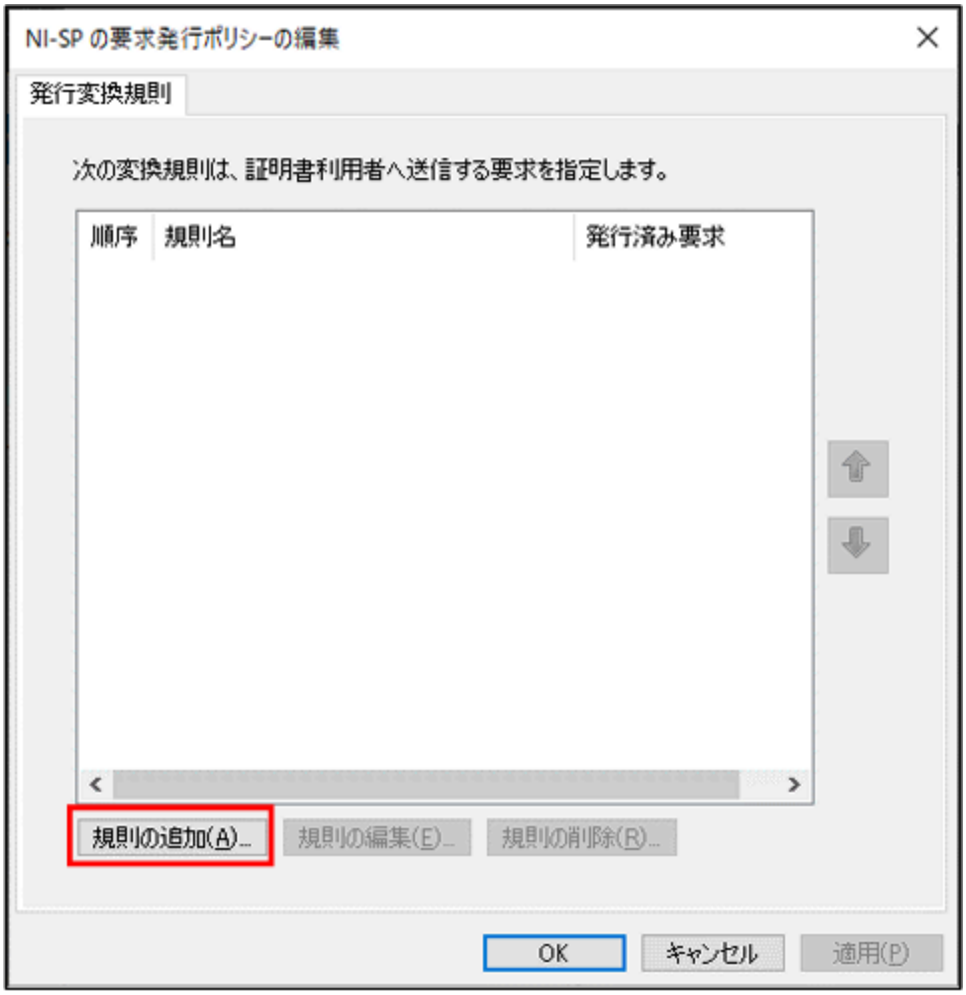
**■仮名を利用しない場合**

> **補足**
>
> - NameIDとして、ADのユーザー情報を返すように設定を行います。

1. AD FSの管理ツールを表示し、「証明書利用者信頼」メニューを選択します。
   追加した証明書利用者信頼をクリックし、画面右側の「要求発行ポリシーの編集」を選択します。

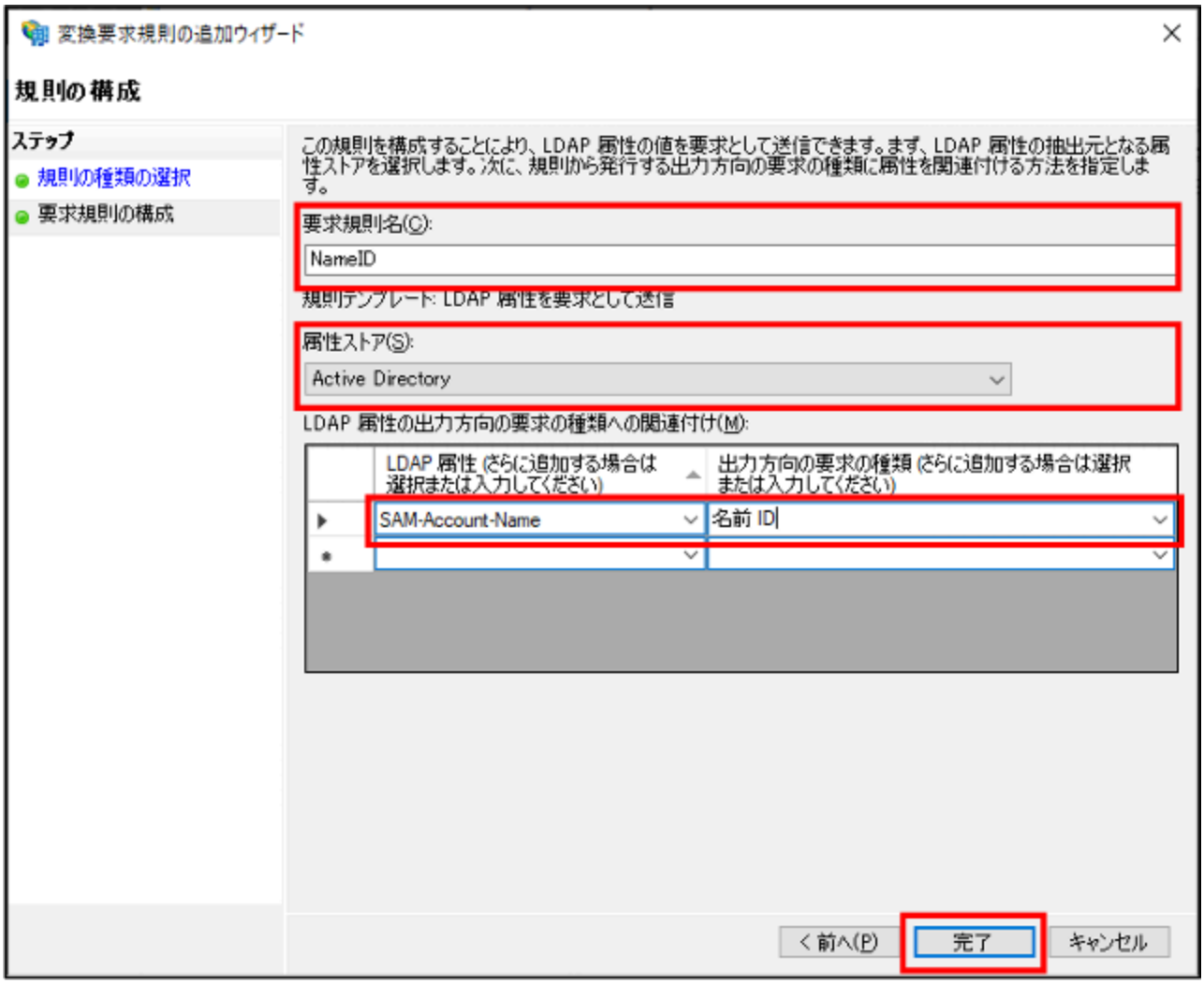


2. 「規則の追加」ボタンをクリックします。



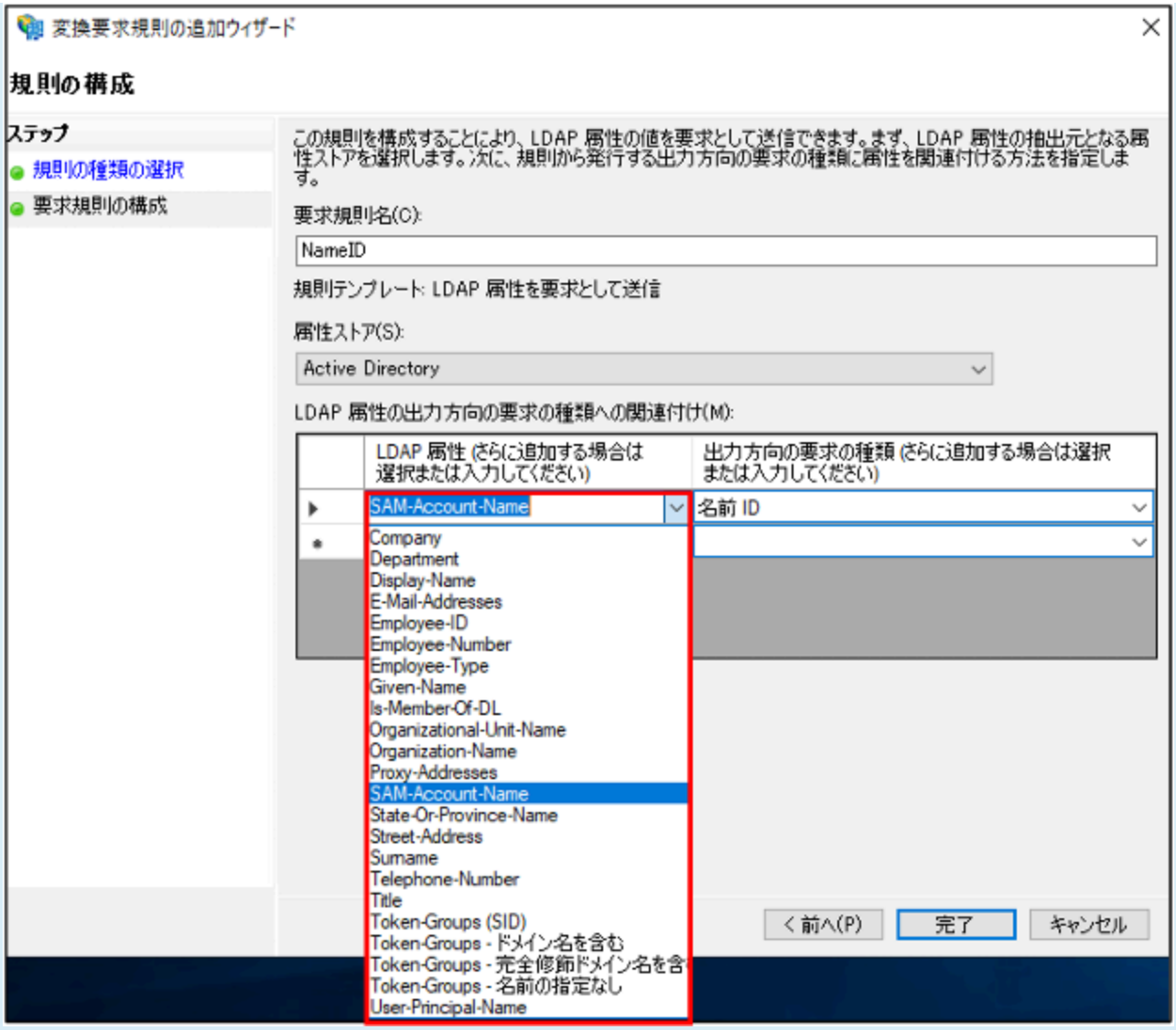
3. 以下の要求規則を追加します。
   要求規則テンプレートに「LDAP属性を要求して送信」を選択し、「次へ」をクリックします。


   以下の値を選択し、「完了」をクリックします。
   - 要求規則名：任意の名称を入力します。
   - 属性ストア：「Active Directory」を選択します。
   - LDAP属性：「SAM-Account-Name」
     ※ここでは検証のため、ADの「ユーザーログオン名(Windows 2000より前)」に紐づく「SAM-Account-Name」を選択しています。
     LDAP属性については、補足を参照してください。
   - 出力方向の要求の種類：「名前ID」を選択します。



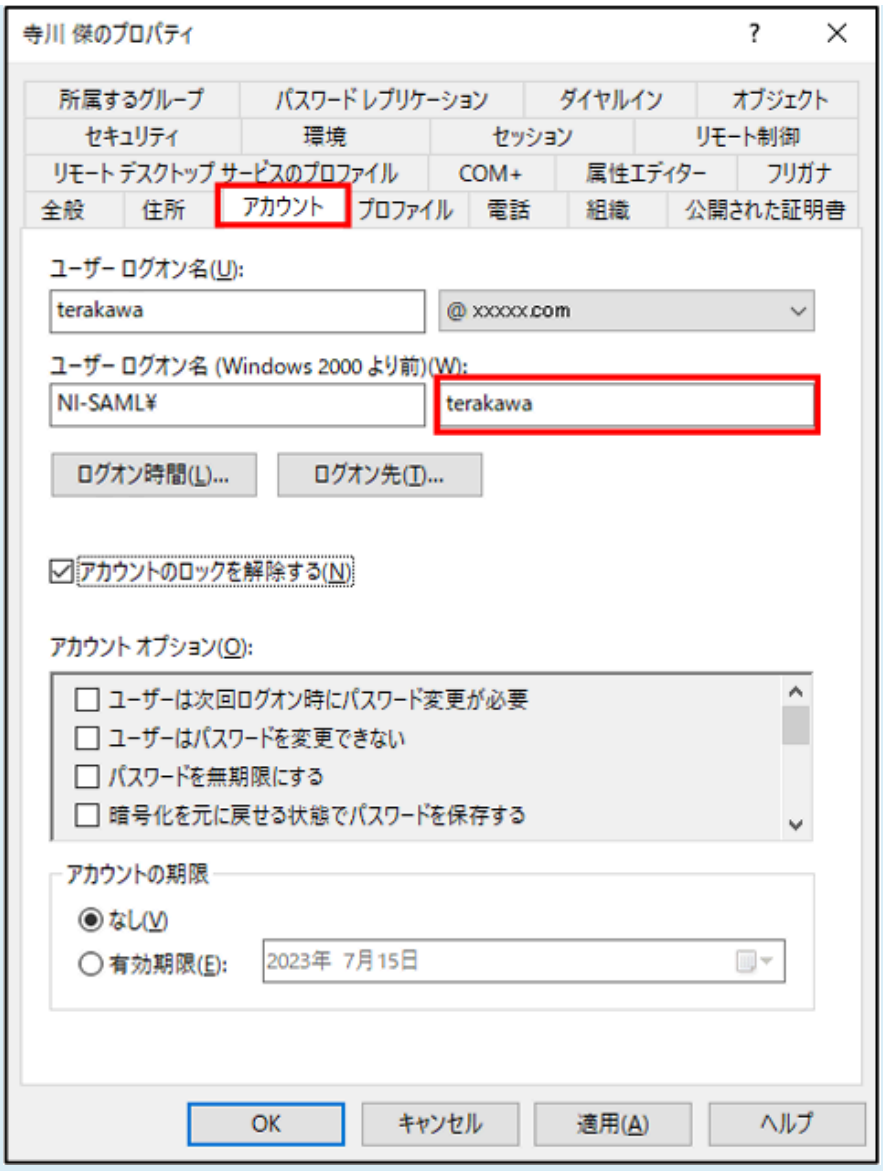

## 補足

- LDAP属性には、「SAM-Account-Name」以外の項目も選択できます。
  ユーザー情報が一意に識別できる項目を選択してください。

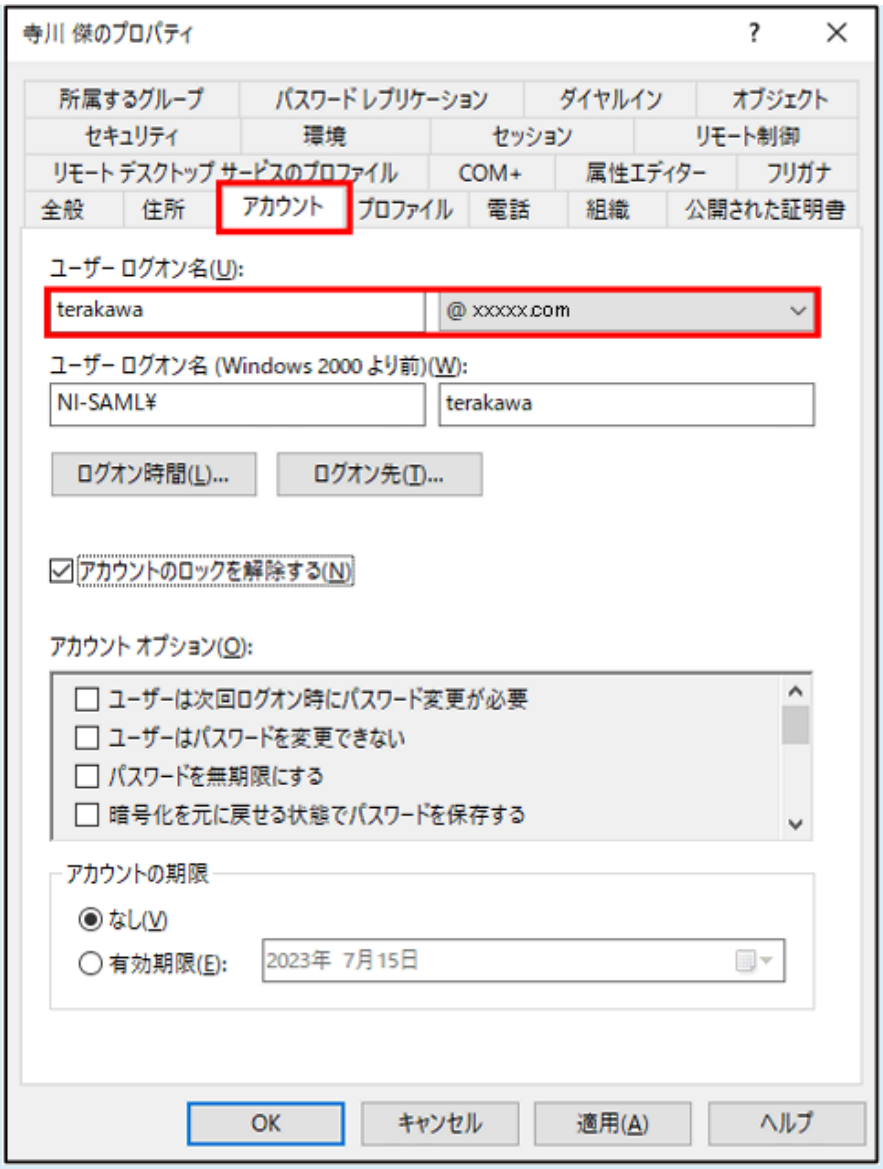



一般的に使用される「LDAP属性」の選択肢とADの情報との紐づけは以下のようになります。

- LDAP属性「SAM-Account-Name」
  ADの「ユーザーログオン名(Windows 2000より前)」を使用します。




- LDAP属性「User-Principal-Name」
  ADの「ユーザーログオン名」を使用します (@以降含む)。

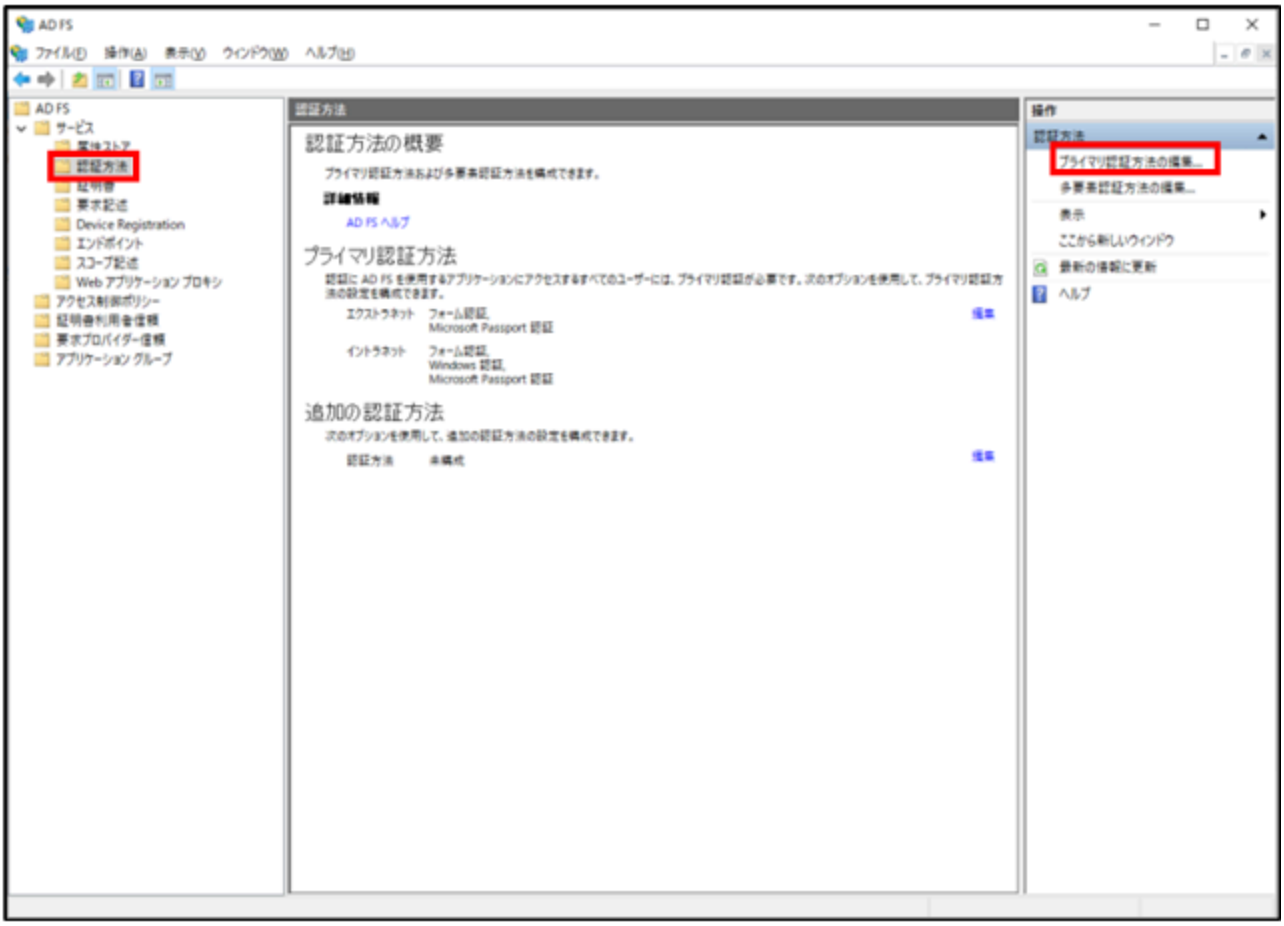



- LDAP属性「E-Mail-Addresses」
  ADの「電子メール」を使用します。


寺川 傑のプロパティ
所属するグループ
パスワード レプリケーション
ダイヤルイン
オブジェクト
セキュリティ
環境
セッション
リモート制御
リモート デスクトップ サービスのプロファイル
COM+
属性エディター
フリガナ
全般
住所
アカウント
プロファイル
電話
組織
公開された証明書
寺川 傑
姓(L):
寺川
名(F):
傑
イニシャル(I):
表示名(S):
寺川 傑
説明(D):
事業所(C):
電話番号(T):
その他(O)...
電子メール(M):
terakawa@xxxxx.com
Web ページ(W):
その他(R)...
OK
キャンセル
適用(A)
ヘルプ

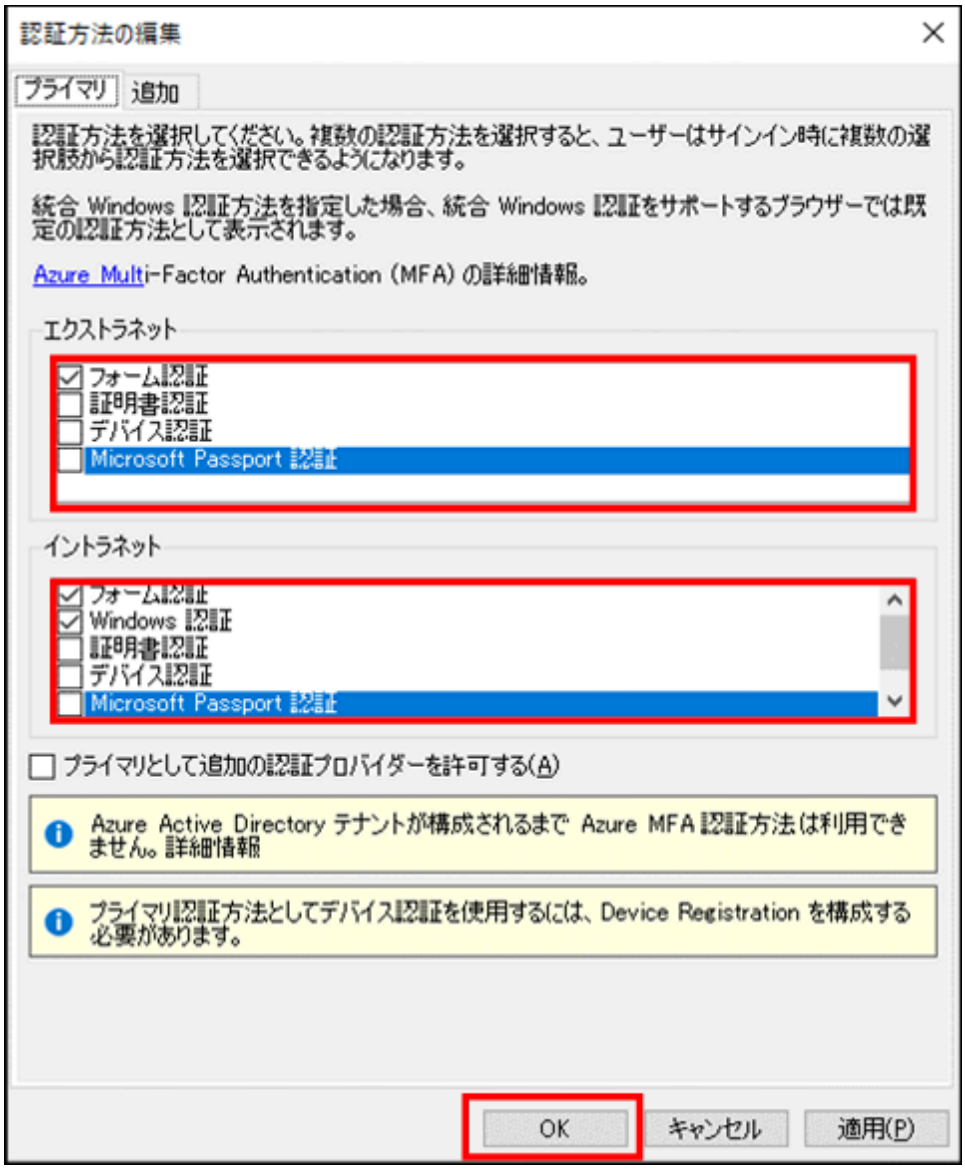
## 認証ポリシーの設定

1. AD FSの管理ツールを表示し、「認証方法」メニューを選択します。
   プライマリ認証方法の編集をクリックします。



2. 利用する認証方法を有効にし、「OK」をクリックします。
   - **パスワード認証の場合**
     エクストラネット：「フォーム認証」にチェックします。
     イントラネット：「フォーム認証」にチェックします。

   - **Windows認証の場合**
     エクストラネット：「フォーム認証」にチェックします。
     イントラネット：「フォーム認証」と「Windows認証」にチェックします。



## IdPの設定(Windows Server 2019)

Windows Server 2016 同様の手順となります。
「IdPの設定(Windows Server 2016－ADFS)」を参照してください。

## IdPの設定(Windows Server 2022)

Windows Server 2016 同様の手順となります。
「IdPの設定(Windows Server 2016－ADFS)」を参照してください。

## ▶ 仮名ID取得

> ⚠ 注意
>
> - 仮名を利用する場合のみ、各ユーザーが下記の作業を行う必要があります。

### オプション設定

1. 仮名を利用する場合、初回ログイン時はシングルサインオンに失敗するため、通常のNI製品ログイン画面より、ID/パスワードを入力し、ログインしてください。

2. NI製品の「オプション設定」画面を表示し、「SAML認証」を選択します。
   ⇒「SAML認証」画面が表示されます。

3. 「取得する」ボタンをクリックして、Identity Providerから仮名IDを取得します。
   ※新規ウィンドウが開き、Identity Providerへ接続します。仮名ID取得後にWindowは自動的に閉じられます。

4. 最後に「保存」ボタンを押します。

## 動作確認

1. NI製品の任意のURLにブラウザでアクセスします。

2. IdPにログインします。
   パスワード認証の場合、AD FSのログイン画面にて、ID/パスワードを入力することで認証されます。


3. Windows認証の場合、ドメインにログイン済みのWindows PCにて、Microsoft Edge、またはGoogle Chromeを使用しているときは、自動で認証されます。
   それ以外の場合、認証ダイアログが表示され、ID/パスワードを入力することで認証されます。

4. NI製品の目的のURLが表示されます。

### 補足

- Windows Helloなど多要素認証によるログインの場合も同様の動作となります。

# トラブルシューティング

補足

- AD FSで発生するエラーについて記載します。
- NI製品のアクセスログに出力されているエラーログへの対処については、「トラブルシューティング」を参照してください。

## AD FSのエラーについて

### ■AD FSのエラー画面

以下のような画面が表示された場合、AD FS側でエラーが発生しています。

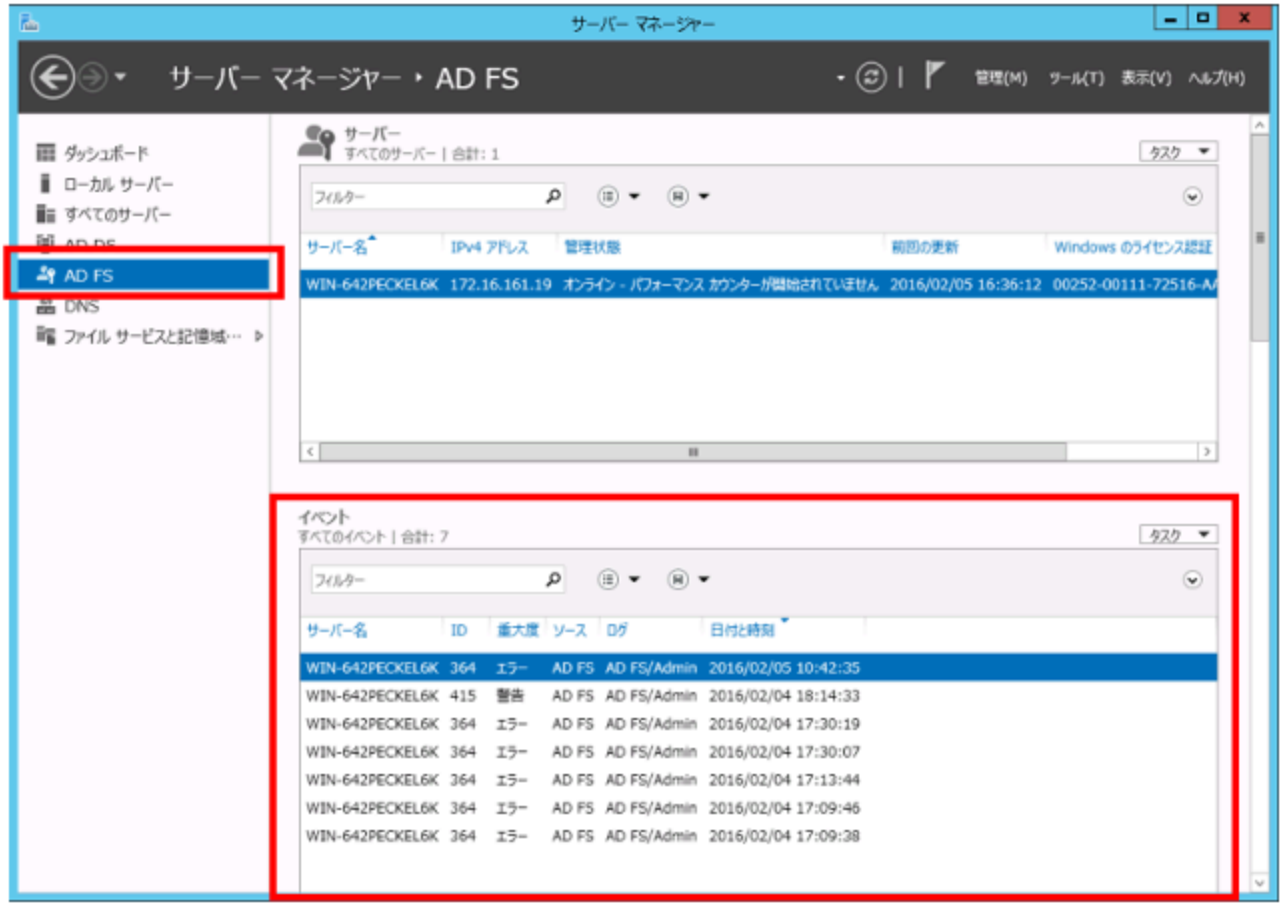
通常のログイン画面のURLに「?saml=no」を追加し、NI製品へログインしてください。

**例）NI Collabo 360**
**https://xxx.xxx.xxx.xxx/ni/niware/portal/index.php?saml=no**

**例）Sales Force Assistantシリーズ**
**https://xxx.xxx.xxx.xxx/ni/<各製品>/main/index.php?saml=no**

**■AD FSのエラー詳細確認**

エラーの内容を確認するには、IdPのサーバーマネージャーのメニューより「AD FS」を選択し、「イベント」項目をチェックします。



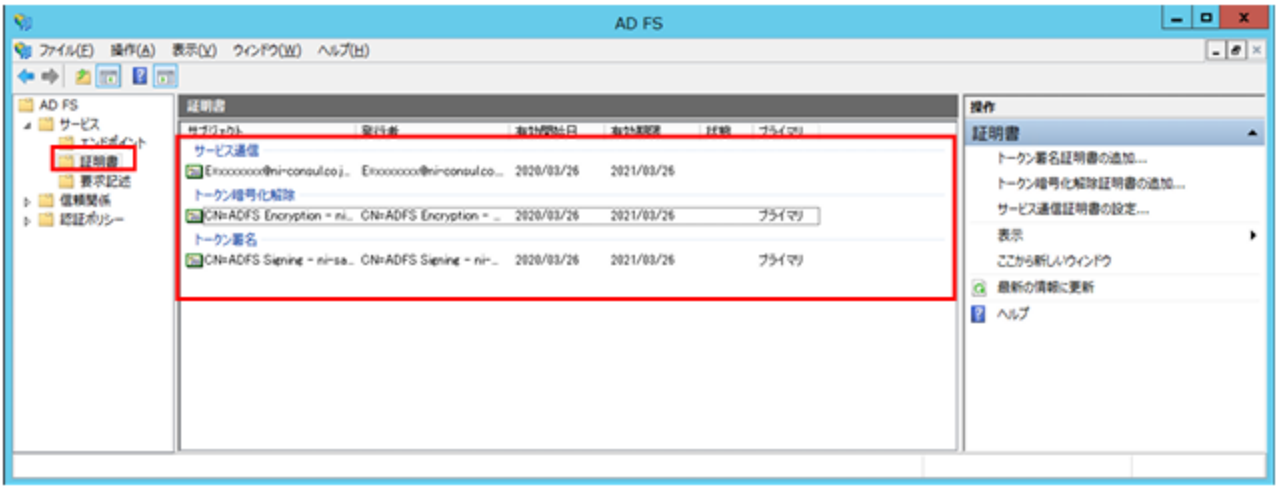

AD FSの設定不備が原因で発生する主要なエラーを以下に記載します。

| エラーID | エラーメッセージ | 対応方法 |
| --- | --- | --- |
| 364 | パッシブな要求のフェデレーション中にエラーが発生しました。<br><br>追加データ<br>… | 認証中にエラーが発生すると、必ずログに出力されるメッセージです。<br>※パッシブな要求＝Webブラウザからの要求 |
| 364 | パッシブな要求のフェデレーション中にエラーが発生しました。<br>追加データ<br>プロトコル名:<br>Saml<br>証明書利用者:<br>https://xxx.xxx.xxx.xxx/ni/<br>例外情報:<br>Microsoft.IdentityServer.Web.InvalidScopeException:<br>MSIS7007: 要求された証明書利用者信頼<br>'https://xxx.xxx.xxx.xxx/ni/'は指定されていないか、またはサポートされていません。証明書利用者信頼が指定されていた場合は、証明書利用者信頼にアクセスするための許可がない可能性があります。詳細については、管理者に問い合わせてください。<br>場所<br>Microsoft.IdentityServer.Web.Protocols.Saml.SamlSignInContext.Validate()<br>場所 Microsoft.IdentityServer.Web.Protocols… | SPのエンティティIDが誤っています。<br>（※上記原因の場合、エラーID：364以外のエラーメッセージは出力されません。）<br>証明書利用者信頼のプロパティの[識別子」タブから証明書利用者の識別子が正しいことを確認してください。 |
| 261 | 要求で、証明書利用者'https://xxx.xxx.xxx.xxx/ni/'に構成されていないアサーション コンシューマー サービスのURL'https://xxx.xxx.xxx.xxx/ni/zcom/service/index.php?p=saml'が指定されました。<br>アサーション コンシューマー サービスのURL:<br>https://xxx.xxx.xxx.xxx/ni/zcom/service/index.php?p=saml<br>証明書利用者: https://xxx.xxx.xxx.xxx/ni/<br>この要求は失敗しました。<br>ユーザー操作<br>AD FSの管理スナップインを使用して、この証明書利用者用に指定されたURLを持つアサーション コンシューマー サービスを構成してください。 | SPのエンドポイントURLが誤っています。<br>証明書利用者信頼のプロパティの「エンドポイント」タブから「SAMLアサーション コンシューマ<br>ーエンドポイント」のURLが正しいことを確認してください。 |
| 321 | SAML認証要求に、満たすことができないNameIDのポリシーがありました。<br>要求元: https://xxx.xxx.xxx.xxx/ni/<br>名前識別子の形式:<br>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent<br>SPNameQualifier: | 仮名IDの利用有無に対し、IdP側の設定が正しく実施できていません。<br>「変換要求規則の追加」項の手順が正しく実行できているか、確認してください。 |

| エラーID | エラーメッセージ | 対応方法 |
| --- | --- | --- |
| | 例外の詳細:<br>MSIS7070: SAML要求に、発行されたトークンでは要件が満たされないNameIDPolicyが含まれていました。要求されたNameIDPolicy: AllowCreate: True Format: urn:oasis:names:tc:SAML:2.0:nameid-format:persistentSPNameQualifier: 。実際の NameID プロパティ: Format: ,NameQualifier: SPNameQualifier: , SPProvidedId: 。<br>この要求は失敗しました。<br>ユーザー操作<br>AD FSの管理スナップインを使用して、 必要な名前識別子を発行する構成を設定してください。 | |
| 273 | 要求で、証明書利用者'https://xxx.xxx.xxx.xxx/ni/'に対して構成またはサポートされていないアサーション コンシューマー サービスが指定されました。<br>要求パラメーター: ''、'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST'、'https://xxx.xxx.xxx.xxx/ni/zcom/service/index.php?p=saml'<br>証明書利用者: https://xxx.xxx.xxx.xxx/ni/<br>この要求は失敗しました。<br>ユーザー操作<br>AD FSの管理スナップインを使用して、この証明書利用者用に指定されたパラメーターを持つアサーション コンシューマー サービスを構成してください。SAMLアーティファクトが要求された場合は、アーティファクト解決サービスが有効になっているかどうかも確認してください。 | IdPのエンドポイントURL設定に、誤ったバインディングが指定されています。<br>「エンドポイントURLの追加」項の手順が正しく実行できているか、確認してください。 |

# 運用時の注意

## 証明書の更新について




AD FSは、以下の3種類の証明書を利用して動作しています。

1. サービス通信証明書
   「AD FSの構成」にて適用した、SSL(https)通信のための証明書です。
   適用した証明書の期限に応じて、手動で更新を行ってください。

2. トークン暗号化解除証明書
   利用していません。

3. トークン署名証明書
   AD FSのセットアップ時に自動で作成される自己署名証明書です。
   有効期限は既定では1年となっており、自動で更新されます。
   また、AD FSでは、自動証明書ロールオーバー機能(トークン署名証明書の自動更新)があり、既定ではこの機能が有効となっています。自動証明書ロールオーバーが発生した場合、証明書の有効期限5日前にNI製品へのシングルサインオンでエラーが発生します。
   対策として、AD FSの自動証明書ロールオーバー機能を無効にする、証明書の有効期限延長があります。
   詳細は、Microsoft社の情報をご確認ください。

   有効期限切れ、有効期限延長により証明書が更新されると、「システム設定」の「3.IdPメタデータをアップロードします。」を再実行する必要があります。

# セットアップ手順（IdP: Microsoft Entra IDの場合）

## ▶ システム構成

以下の構成でセットアップを行います。

**認証サーバー**

| | |
|---|---|
| IdP | Microsoft Entra ID |

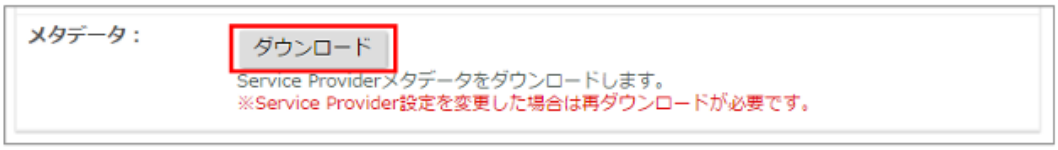
※Microsoft Entra IDの全てのエディションにてSAML認証機能が利用可能です。
ただし、Microsoft社がエディション毎の提供機能範囲を変更する可能性があります。
詳細はMicrosoft社の情報をご確認ください。
https://learn.microsoft.com/ja-jp/entra/fundamentals/whatis

# IdPの設定

## SPメタデータの準備

1. NI製品システム設定の「セキュリティ」タブより「SAML認証」を選択します。
   ⇒「認証／SAML認証」画面が表示されます。

2. SPメタデータをダウンロードします。
   Service Provider(NI製品)設定の「メタデータ」の「ダウンロード」ボタンをクリックします。




   ⇒SPメタデータXMLファイルがダウンロードされます。「Microsoft Entraアプリケーションの作成・設定」にて使用します。

## Microsoft Entraアプリケーションの作成・設定

1. ブラウザにて下記URLにアクセスし、Microsoft Entra管理センターの画面を表示します。
   https://entra.microsoft.com

2. メニュー「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」を表示し、「新しいアプリケーション」をクリックします。


3. 「独自のアプリケーションの作成」をクリックします。


4. 任意のアプリ名を入力します。

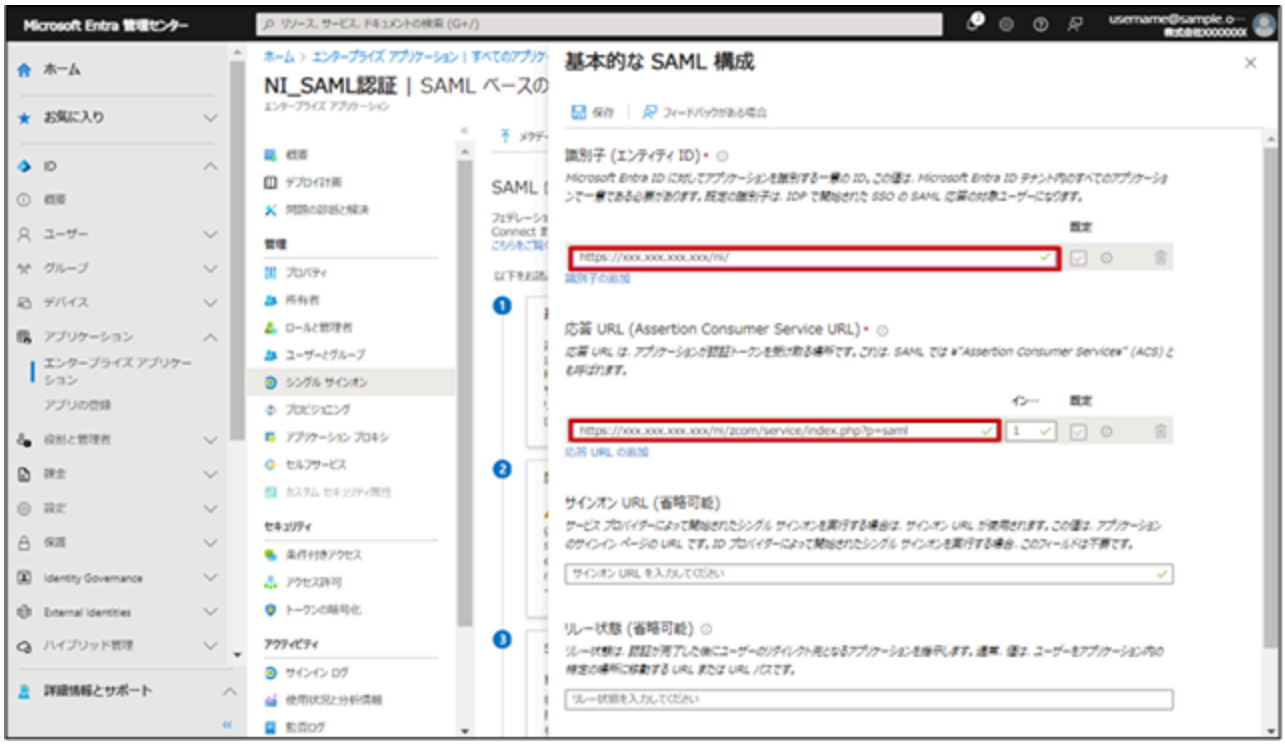
5. 「ギャラリーに見つからないその他のアプリケーションを統合します（ギャラリー以外）」を選択し、「作成」をクリックします。
   ⇒任意のアプリ名でアプリケーションが作成され、概要ページが表示されます。

6. 「シングルサインオン」を選択します。


7. 「SAML」を選択します。

8. 「メタデータ ファイルをアップロードする」をクリックします。

9. 「SPメタデータの準備」でダウンロードしたSPメタデータを選択し、追加ボタンをクリックします。
⇒値がセットされます。


## 補足

- SPメタデータをアップロードすることで、以下の値が自動でセットされます。
「識別子(エンティティID)」：NI製品システム設定画面の「エンティティID」の値がセットされます。
「応答URL」：NI製品システム設定画面の「エンドポイントURL」の値がセットされます。

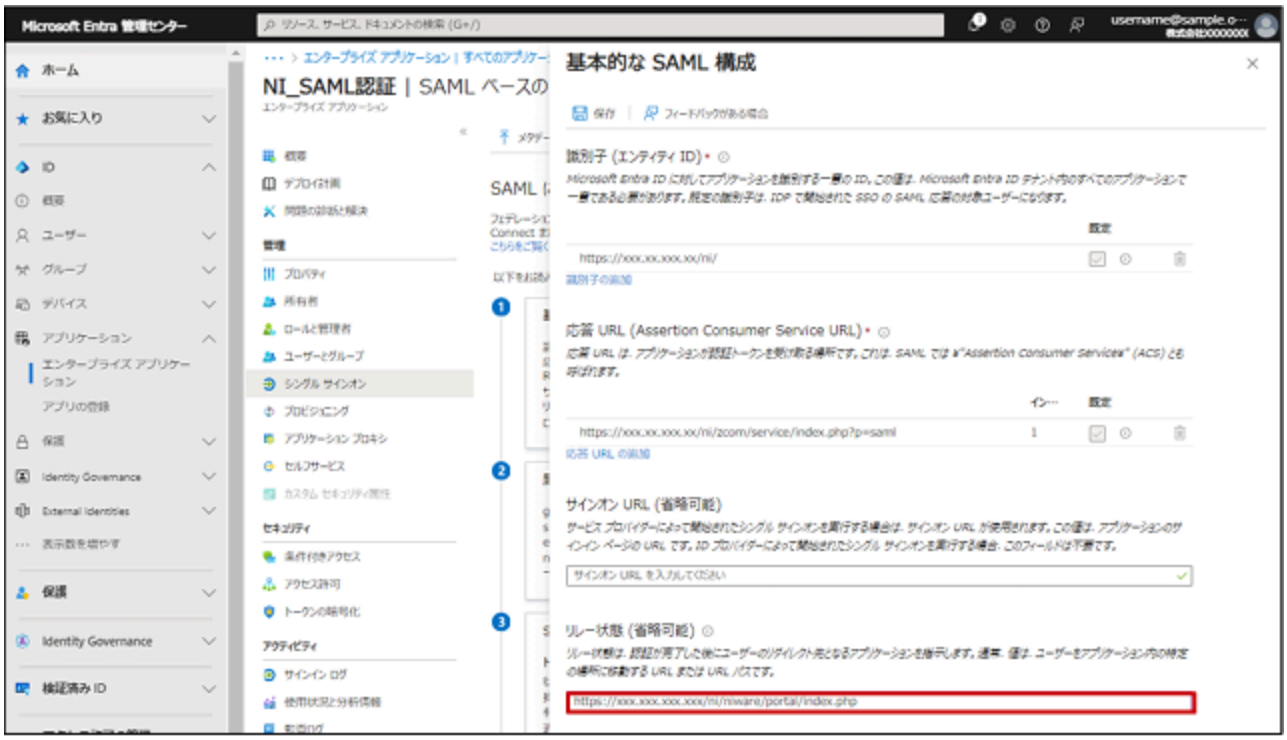
10. 必要な値をセットします。

> ⚠ 注意
>
> - 「IdPを起点としたシングルサインオン（IdP Initiated SSO）」を利用する場合、下記の値をセットする必要があります。
>  「NI製品を起点としたシングルサインオン」のみを利用する場合は、不要です。

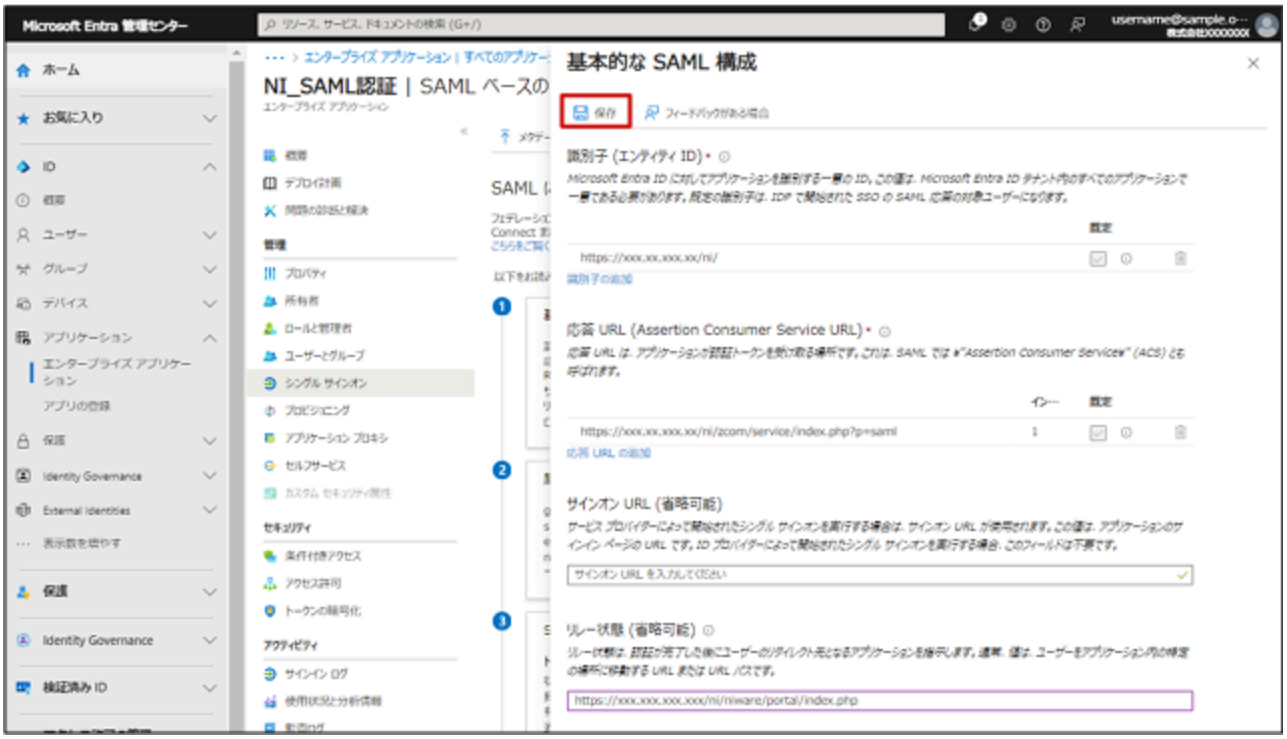
自動セットされた値に加え、ログイン後に表示したい製品のログイン画面のURLを「リレー状態」へセットしてください。

【例】
NI Collabo 360を表示する場合：
https://xxx.xxx.xxx.xxx/ni/niware/portal/index.php

Sales Force Assistantシリーズを表示する場合：
https://xxx.xxx.xxx.xxx/ni/<各製品>/main/index.php

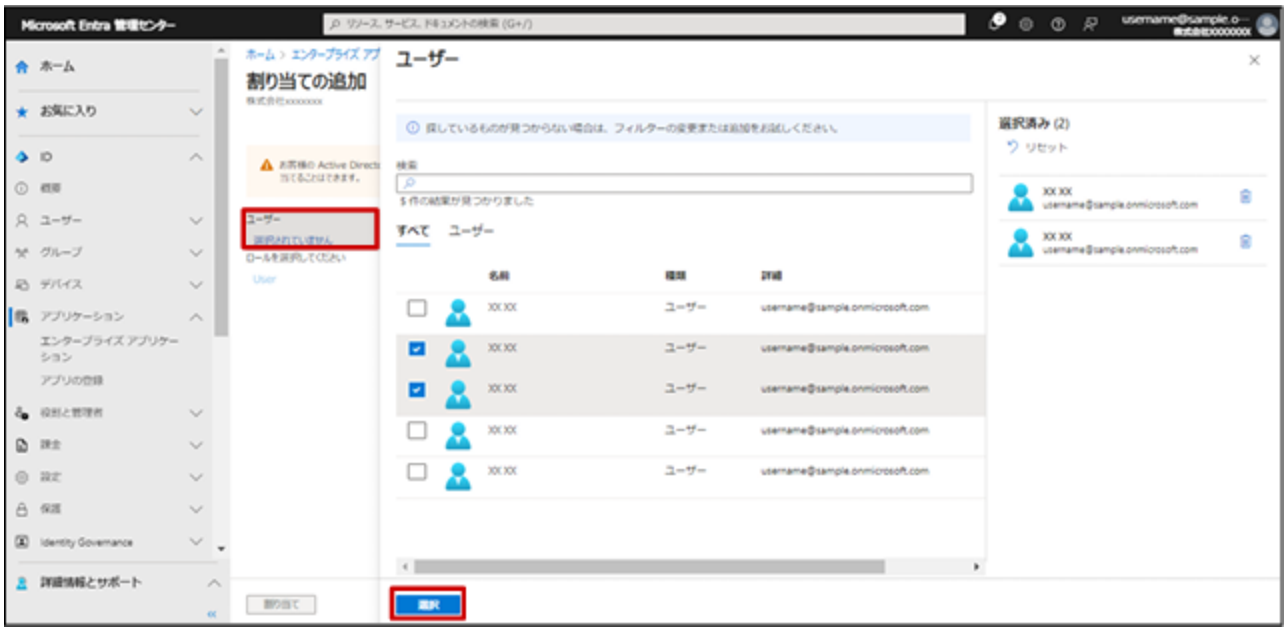


11. 「保存」ボタンをクリックします。
⇒アプリケーションのSAML設定が変更されます。




12. 「ユーザーとグループ」を選択し、「ユーザーまたはグループの追加」をクリックします。

13. アプリケーションを使用するユーザーを選択し、「割り当て」をクリックします。
⇒アプリケーションのアクセス設定が変更されます。

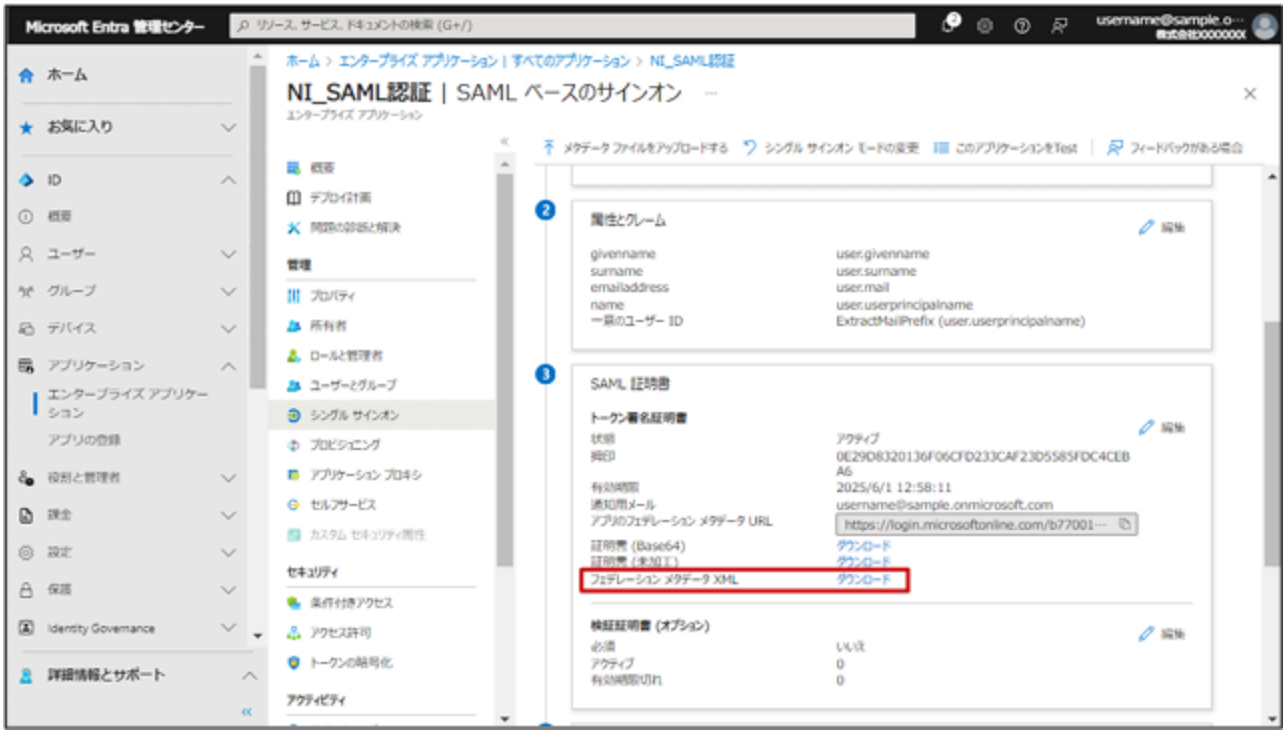



# NI製品の設定

## Microsoft Entra IDの設定値を確認する

1. 追加したMicrosoft Entraアプリケーションの画面を表示し、「シングルサインオン」をクリックします。

2. 画面より、Microsoft Entra IDの設定に必要となる「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、XMLファイルを保存します。




## システム設定

1. システム設定の 「セキュリティ」タブ より「SAML認証」を選択します。
   ⇒「認証／SAML認証」画面が表示されます。

2. 以下の項目を入力し、「保存」ボタンをクリックします。

| 項目名称 | 説明 | 設定値 |
| --- | --- | --- |
| シングルサインオン設定 | | |
| シングルサインオン | シングルサインオンを利用するかしないかを設定します。 | 利用する |
| 有効範囲 | SAML認証を許可する接続元IPアドレスを改行区切りで指定します。空白の場合は、すべての接続でSAML認証を行います。 | ※補足を参照 |
| Service Provider(NI製品)設定 | | |
| エンティティID | Service Providerの識別子。任意の文字列を設定します。<br>※初期値のURLから変更する必要はありません。 | https://xxx.xxx.xxx.xxx/ni/ |
| エンドポイントURL | SAMLレスポンスを受信するURLです。<br>※Identity Providerのセットアップに使用する固定値です。 | – |
| 仮名 | 仮名IDを用いた認証を利用するかしないかを設定します。 | 利用する/利用しない |
| 認証方法 | 認証にパスワード認証を用いるか、Windows認証を用いるかを設定します。 | パスワード認証 |
| ログアウトURL | NI製品からログアウト後に遷移するURLを設定します。 | https://login.microsoftonline.com/common/wsfederation?wa=wsignout1.0 |

### 補足

- NI製品からログアウトする際に、IdPからもログアウトする必要がない場合は、
  ログアウトURLに下記URLを設定することで、通常のNI製品ログイン画面に遷移します。

  **https://<任意のNI製品URL>?saml=no**
- 社内端末のIPアドレスを「有効範囲」に指定することで、モバイル端末など社外からの接続によりIdPに接続不可の場合は、「有効範囲」外となるため、SAML認証が適用されず、通常のログイン画面が表示されます。

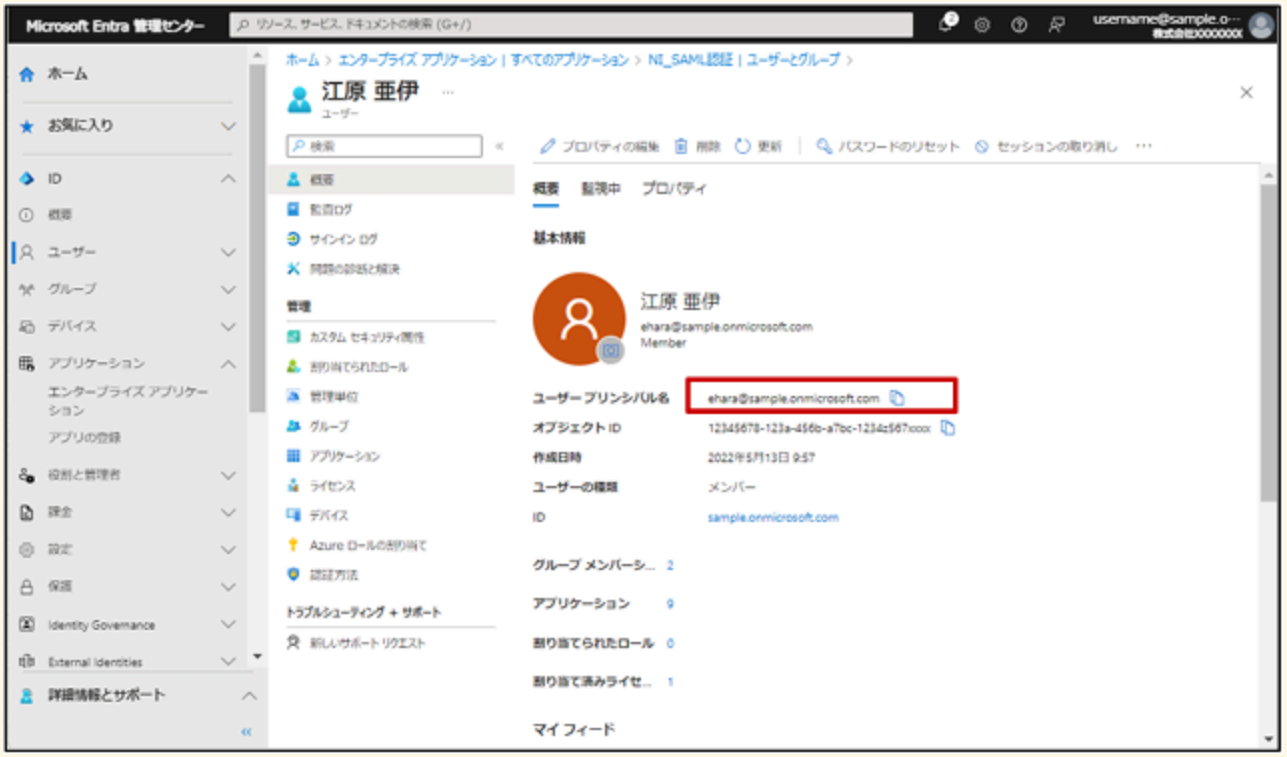
### 注意

- Microsoft Entra IDは、認証方法「Windows認証」に対応していません。
- エンティティIDを変更した場合、IdPの再設定が必要になります。

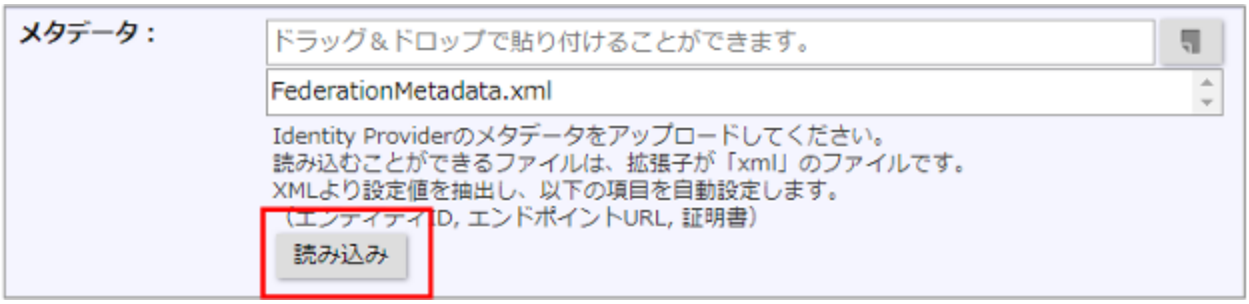
- NI製品の社員ログインIDと、
  Microsoft Entra IDのユーザーIDを一致させておく必要があります。
  Microsoft Entra IDのユーザーIDは、以下の画面から確認できます。
  1. Microsoft Entraアプリケーションの画面から、「ユーザーとグループ」をクリックします。

  2. 対象のユーザーをクリックします。


3. Microsoft Entra IDのユーザーIDが「ユーザープリンシパル名」として表示されます。



3. IdPメタデータをアップロードします。
   NI製品システム設定「認証／SAML認証」画面の、Identity Provider設定の「メタデータ」にMicrosoft Entraアプリケーションからダウンロードした「フェデレーションメタデータXML」を添付します。
   「読み込み」ボタンをクリックします。




   以下の設定項目が自動で入力されます。

| 項目名称 | 説明 | 設定サンプル値 |
|---|---|---|
| Identity Provider 設定 | | |
| エンティティID | Identity Providerの識別子を設定します。 | https://sts.windows.net/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx/ |
| エンドポイントURL | SAMLリクエストを送信するURLを設定します。 | https://login.microsoftonline.com/xxxxxxxx-xxxx-xxxx-xxxxxxxxxxxxxxxx/saml2 |
| 証明書 | Identity Providerが署名に使用する公開鍵を設定します。<br>カンマ区切りで複数証明書を指定できます。 | Base64エンコードされた文字列 |

4. 「保存」ボタンをクリックします。

# ▶ 仮名ID取得

> ⚠ 注意
>
> - 仮名を利用する場合のみ、各ユーザーが下記の作業を行う必要があります。

### オプション設定

1. .仮名を利用する場合、初回ログイン時はシングルサインオンに失敗するため、通常のNI製品ログイン画面より、ID/パスワードを入力し、ログインしてください。

2. NI製品の「オプション設定」画面を表示し、「SAML認証」を選択します。
   ⇒「SAML認証」画面が表示されます。

3. 「取得する」ボタンをクリックして、Identity Providerから仮名IDを取得します。
   ※新規ウィンドウが開き、Identity Providerへ接続します。仮名ID取得後にWindowは自動的に閉じられます。

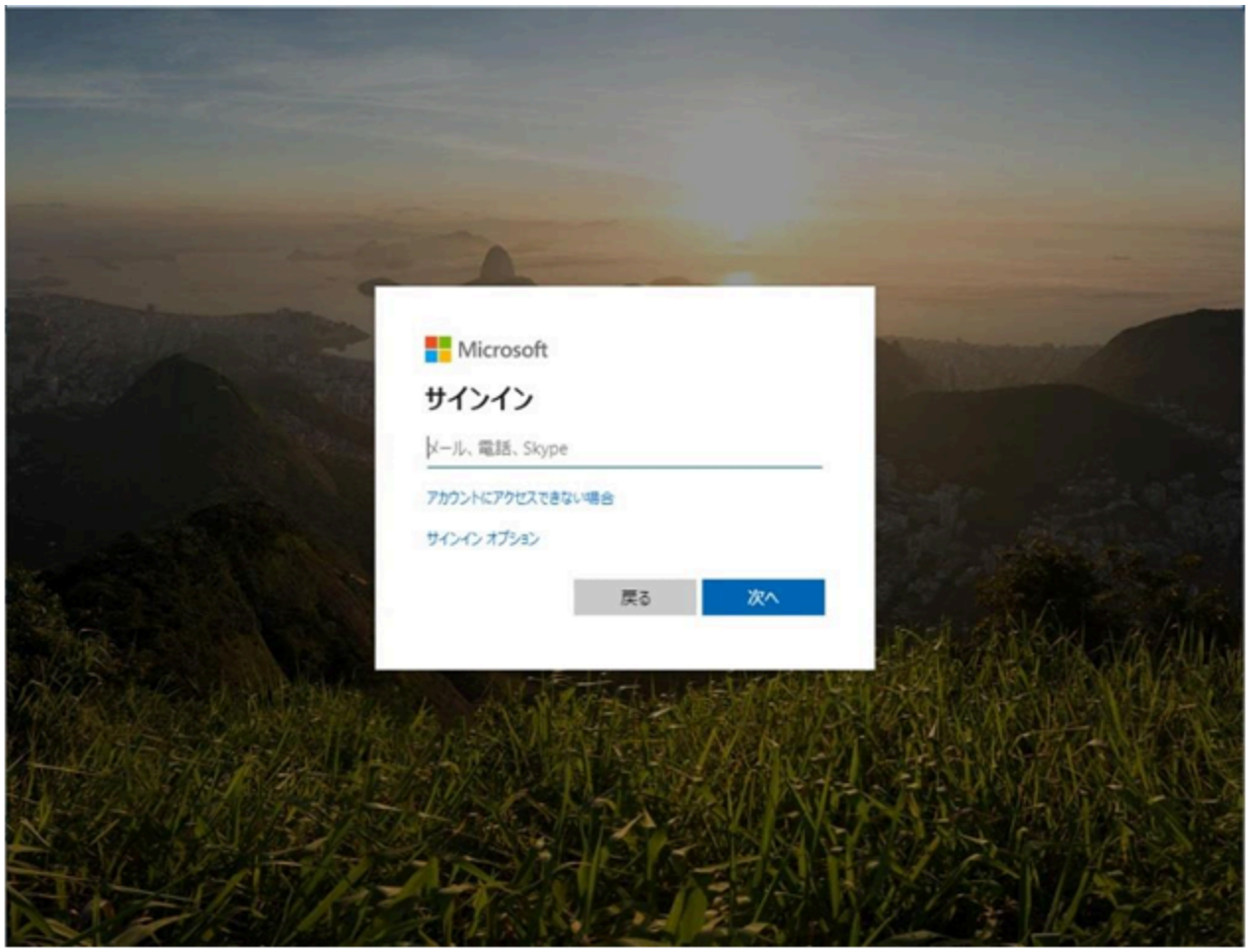
4. 最後に「保存」ボタンを押します。

## 動作確認

### NI製品を起点としたシングルサインオン

1. NI製品の任意のURLにブラウザでアクセスします。

2. IdPにログインします。
   Microsoft Entra IDのログイン画面にて、ID/パスワードを入力することで認証されます。




3. NI製品の目的のURLが表示されます。

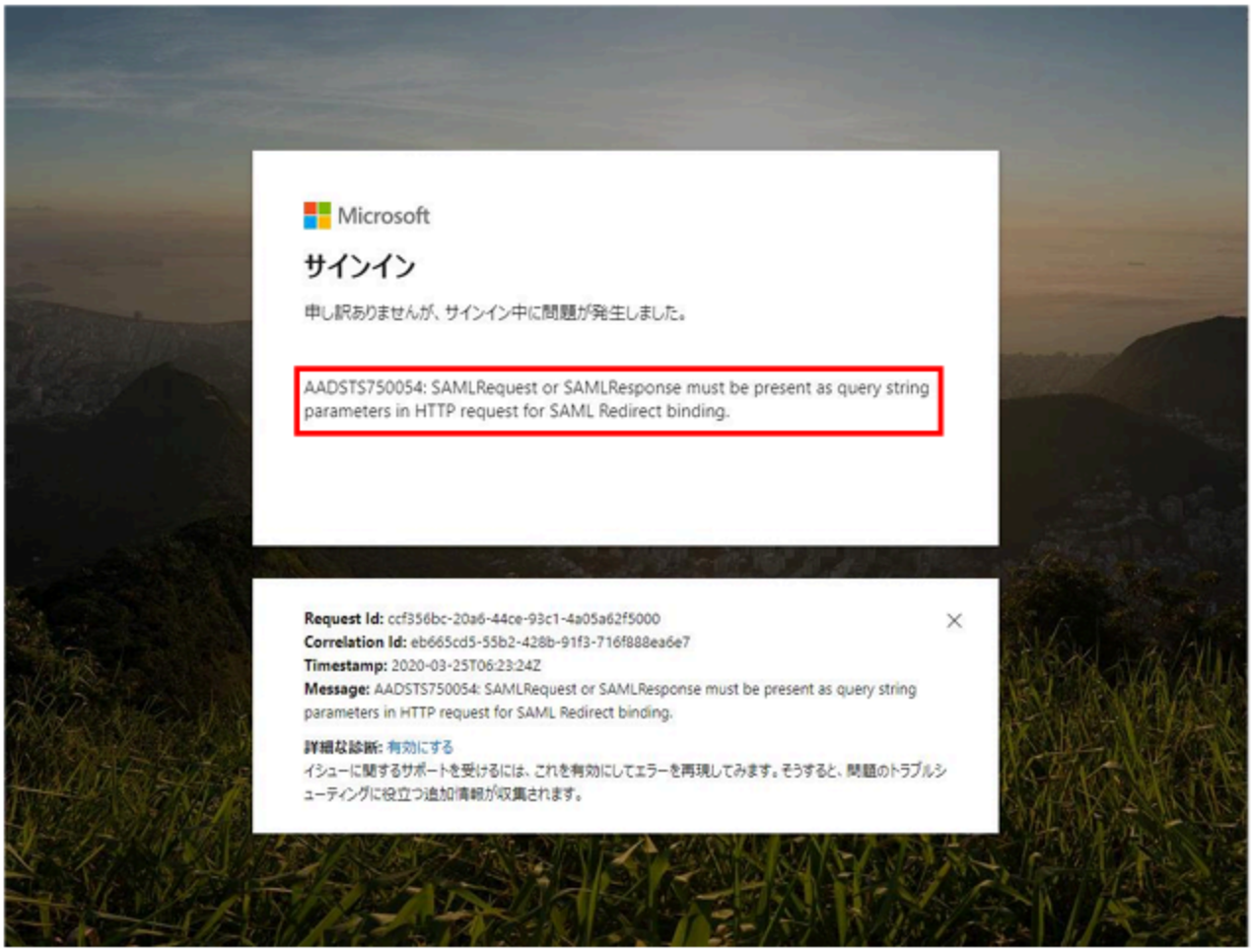
> **補足**
>
> - Microsoft Entra IDのユーザー情報でログイン済みのWindows PCにて、Microsoft Edgeを使用しているときは、自動で認証されます。
> - Windows Hello for Businessなど多要素認証によるログインの場合も同様の動作となります。

## トラブルシューティング

> **補足**
>
> - Microsoft Entra IDで発生するエラーについて記載します。
> - NI製品のアクセスログに出力されているエラーログへの対処については、「トラブルシューティング」を参照してください。

### Microsoft Entra IDのエラー画面

以下のような画面が表示された場合、Microsoft Entra ID側でエラーが発生しています。



通常のログイン画面のURLに「?saml=no」を追加し、NI製品へログインしてください。

例）NI Collabo 360
https://xxx.xxx.xxx.xxx/ni/niware/portal/index.php?saml=no

例）Sales Force Assistantシリーズ
https://xxx.xxx.xxx.xxx/ni/<各製品>/main/index.php?saml=no

## Microsoft Entra IDのエラー詳細確認

Microsoft Entra IDのエラー画面にて、赤枠内のメッセージを参照します。

| エラーID | エラーメッセージ | 対応方法 |
|---|---|---|
| AADSTS70001 | Application with identifier ‘https://xxx.xxx.xxx.xxx/ni/’was not found in the directory xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx | SPのエンティティIDが誤っています。<br>NI製品システム設定>ServiceProvider(NI製品)設定>「エンティティID」と、Microsoft Entraアプリケーション設定の「アプリケーションID/URI」に同じ値を設定してください。 |
| AADSTS75011 | Authentication method ‘Password’ by which the user authenticated with the service doesn’t match requested authentication method ‘WindowsIntegrated’ | 認証方法に「Windows認証」を指定した場合に表示されます。<br>「パスワード認証」に変更してください。 |
| AADSTS50105 | Your administrator has configured the application xxxxx(‘xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx ‘) to block users unless they are specifically granted (‘assigned’) access to the application. The signed in user ‘ xxxxxxxx @ xxxxxx.onmicrosoft.com’ is blocked because they are not a direct member of a group with access, nor had access directly assigned by an administrator. Please contact your administrator to assign access to this application. | 作成したMicrosoft Entraアプリケーションを使用する権限がないユーザーでサインインした場合に表示されます。Microsoft Entraアプリケーションのアクセス設定を変更してください。 |

## 運用時の注意

### 証明書の更新について

Microsoft Entra IDは、以下の証明書を利用して動作しています。
トークン署名証明書
Microsoft Entra IDでは、定期的にロールオーバー(トークン署名証明書の更新)が発生します。
ロールオーバーされた場合、「システム設定」の「3. IdPメタデータをアップロードします。」を再実行する必要があります。

詳細は、Microsoft社の情報をご確認ください。
https://learn.microsoft.com/ja-jp/entra/identity-platform/signing-key-rollover

# トラブルシューティング

## シングルサインオンができない場合の対応方法

以下の手順で対応を行ってください。

1. IdPのエラー画面が表示されている場合
   各IdPのトラブルシューティングを参照してください。
   → AD FSのトラブルシューティング
   → Microsoft Entra IDのトラブルシューティング

2. 通常のログイン画面が表示される場合
   ID/パスワードを入力して NI製品にログインし、システム設定画面の「運用管理> アクセス／アクセスログ」に、エラーメッセージが出力されていないかを確認してください。
   →SAML認証のログを確認する
   →SAML認証エラーの原因を調べる

3. IdPにアクセスできない場合
   ブラウザに「このウェブページにアクセスできません」、「このページは表示できません」などのメッセージが表示される場合、端末からIdPに接続できていません。
   次の項を参照してください。
   →IdPに接続不可の端末からNI製品にアクセスする

4. エラーメッセージが出力されていない場合
   システム設定画面の「セキュリティ＞ 認証／SAML認証」から、以下の設定が正しいことを確認します。
   →シングルサインオンを「利用する」設定になっているかどうか
   →有効範囲が正しく設定されているかどうか

## SAML認証のログを確認する

システム設定画面の「運用管理> アクセスログ」より、SAML認証についてのログを確認できます。
ログは区分「ログイン画面の接続監視」で出力されます。

| メッセージ | 説明 |
| --- | --- |
| SAML認証によるシングルサインオンに成功しました。[XXX] | 正常にシングルサインオンした際に表示されます。（※XXX:ログインしたユーザー名） |
| SAML認証によるシングルサインオンに失敗しました。(XXX) | シングルサインオン処理に問題があった場合に表示されます。<br>「SAML認証エラーの原因を調べる」項を参照して、設定値を見直してください。（※XXX:エラーの詳細メッセージ） |
| NameIDに該当するユーザーが見つかりませんでした。(XXX) | 仮名を利用する際に、仮名IDの設定を行っていない状態で、シングルサインオンを実行した際に表示されます。<br>オプション設定画面より、仮名ID取得を行ってください。（※XXX:仮名ID） |
| NameIDに該当するユーザーが複数見つかりました。 | 複数のNI製品ユーザーが、同じIdPのアカウントと紐付いた状態でシングルサインオンを実行した際に表示されます。<br>再度オプション設定画面より、仮名ID取得を行い、正しいアカウントにてログインしてください。 |
| SAML認証対応製品ではありません。 | SAML認証に対応していない製品から、シングルサインオン処理が行われた際に表示されます。 |
| 使用停止中です。[XXX] | 使用停止中のユーザーに対して、シングルサインオンした際に表示されます。 |
| ロックアウト中です。[XXX] | パスワードを連続で間違えたことによりロックアウト状態のユーザーに対して、シングルサインオンした際に表示されます。 |

## SAML認証エラーの原因を調べる

SAML認証によるシングルサインオン処理に問題があった場合に出力されるメッセージと、対応方法の一覧です。
以下の形式でアクセスログが出力されます。
SAML認証によるシングルサインオンに失敗しました。(**<エラーカテゴリ>：<エラーメッセージ詳細>**)

| エラーカテゴリ | エラーメッセージ詳細 | 対応方法 |
|---|---|---|
| Invalid array settings | sp_entityId_not_found | SPのエンティティIDが設定されていません。正しい値を設定してください。 |
| | idp_entityId_not_found | IdPのエンティティIDが設定されていません。正しい値を設定してください。 |
| | idp_sso_not_found | IdPのエンドポイントURLが設定されていません。正しい値を設定してください。 |
| | idp_sso_url_invalid | IdPのエンドポイントURLがURLの書式になっていません。正しい値を設定してください。 |
| | idp_cert_or_fingerprint_not_found_and_required | IdPの証明書が設定されていません。正しい値を設定してください。 |
| invalid_response | The status code of the Response was not Success, was Requester -> urn:oasis:names:tc:SAML:2.0:status:InvalidNameIDPolicy | システム設定画面「セキュリティ＞認証／SAML認証」のService Provider(NI製品)設定＞「仮名」の値がセットアップ時から変更されています。<br>値を修正するか、再度IdPの設定を行ってください。 |
| | invalid_response: The status code of the Response was not Success, was Responder -> urn:oasis:names:tc:SAML:2.0:status:NoAuthnContext | AD FSの認証ポリシーの設定で、認証方法が無効となっています。<br>「認証ポリシーの設定」の手順が正しく実行できていることを確認してください。 |
| | Signature validation failed. SAML Response rejected | システム設定画面「セキュリティ＞認証／SAML認証」のIdentity Provider(NI製品)設定＞「証明書」の値が正しくありません。<br>再度Identity Providerのメタデータを取得し、アップロードしてください。<br><br>※IdP側で署名鍵が更新された場合、このエラーが表示されます。 |

## IdPに接続不可の端末からNI製品にアクセスする

ブラウザに「このウェブページにアクセスできません」、「このページは表示できません」などのメッセージが表示される場合、以下の原因が考えられます。

1. IdPのアドレスの名前解決に失敗している。
   端末のDNSサーバーの設定を確認してください。

2. IdPが社内ネットワークにある場合に、モバイル端末など、社外ネットワークからNI製品にアクセスしている。
   システム設定画面「セキュリティ＞認証／SAML認証」の「有効範囲」の設定により、接続元IPアドレスに応じて、SAML認証を行うか、通常のログイン画面を表示するかを自動で切り替えられます。
   社内接続でのみSAML認証を行いたい場合、有効範囲に社内端末のIPアドレスを指定してください。
   指定されたIPアドレス以外からアクセスした場合は、通常のログイン画面が表示されます。


   または、ログイン画面のURLに「?saml=no」を追加してNI製品にアクセスすることで、どの端末でも通常のログイン画面を表示できます。

   例）NI Collabo 360
   https://xxx.xxx.xxx.xxx/ni/niware/portal/index.php?saml=no

   例）Sales Force Assistantシリーズ
   https://xxx.xxx.xxx.xxx/ni/<各製品>/main/index.php?saml=no

   ただし、有効範囲を設定せず、上記URLでアクセスした場合は、ログアウト時に「このウェブページにアクセスできません」、「このページは表示できません」などのメッセージがブラウザに表示されますが、正常な動作となります。

# 制限事項

## 技術的・運用的制限

- SSL(https)接続の利用が必須となります。
  「SSL(https)での接続設定を行う」を参照してください。
- Windows認証を使用する場合、コントロールパネルでの設定が必要です。
  「Windows認証」を参照してください。
- 以下の場合はSAML認証は行わず、通常のログイン画面が表示されます。
  携帯版サイトにアクセスしている。
  スマホ向けアプリでNI製品にアクセスしている。
- SAMLの仕様では、IdPが社内ネットワーク内であっても、シングルサインオン可能ですが、NI製品に社外からアクセスを行ったり、モバイル端末からアクセスする場合には、IdPを外部から参照可能なサーバー構成にする、もしくはプロキシサーバーを構築する必要があります。
- SAML認証メッセージの暗号化には対応していません。

## 対応製品

SAML認証は、以下の製品に対応しています。

- Sales Force Assistant シリーズ
  Sales Force Assistant 顧客創造
  Sales Force Assistant 顧客創造R
  Sales Force Assistant 顧客深耕
  Sales Force Assistant 深耕創造
  Sales Force Assistant 顧客深耕R
  Sales Force Assistant 顧客深耕AO
  Sales Force Assistant ABM
  ※顧客の声オプション含む
- NI Collabo 360
- MapScorer
- nyoibox
- Approach DAM
- Sales Quote Assistant
- Sales Billing Assistant