

# SAML 認証マニュアル



Copyright ( C ) NI Consulting Co., Ltd. All rights reserved.

1.はじめに	2
1-1.SAML 認証の概要	2
1-2.設定の流れ	7
2.セットアップ手順 (IdP:AD FS の場合)	9
2-1.システム構成	9
2-2.事前準備	9
2-3.NI 製品の設定	16
2-4.IdP の設定(Windows Server 2012 R2)	18
2-5.IdP の設定(Windows Server 2016 – ADFS)	32
2-6.IdP の設定(Windows Server 2019)	48
2-7.仮名 ID 取得	49
2-8.動作確認	50
2-9.トラブルシューティング	51
2-10.運用時の注意	55
3.セットアップ手順 (IdP: Microsoft Entra ID の場合)	56
3-1.システム構成	56
3-2.IdP の設定	56
3-3.NI 製品の設定	63
3-4.仮名 ID 取得	67
3-5.動作確認	68
3-6.トラブルシューティング	69
3-7.運用時の注意	70
4.トラブルシューティング	71
4-1.シングルサインオンができない場合の対応方法	71
4-2.SAML 認証のログを確認する	72
4-3.SAML 認証エラーの原因を調べる	73
4-4.IdP に接続不可の端末から NI 製品にアクセスする	74
5.制限事項	75
5-1.技術的・運用的制限	75
5-2.対応製品	75

# 1.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。



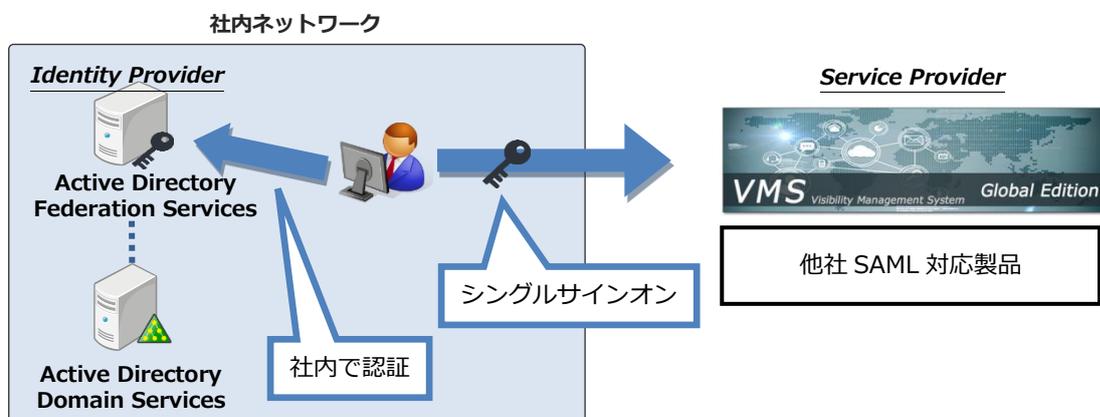
・ご利用いただくにあたり、制限事項があります。「[5.制限事項](#)」を参照してください。

## 1-1.SAML 認証の概要

### 1-1-1.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



- ・ 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。

## 1-1-2.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 (以下、IdP)	認証・認可の情報を提供する役割を担います。 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。 例：AD FS、Microsoft Entra ID
Service Provider (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。 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。 例：NI 製品、Google Apps、Microsoft 365
バインディング (Binding)	SAML メッセージの送信方法を規定したもの。 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。 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 (以下、AD FS)	Windows Server の機能です。 AD のユーザー情報を使用した認証が可能です。 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。 フェデレーションサーバーの機能も有します。 SAML 認証では IdP に相当します。

### 1-1-3. 認証方法について

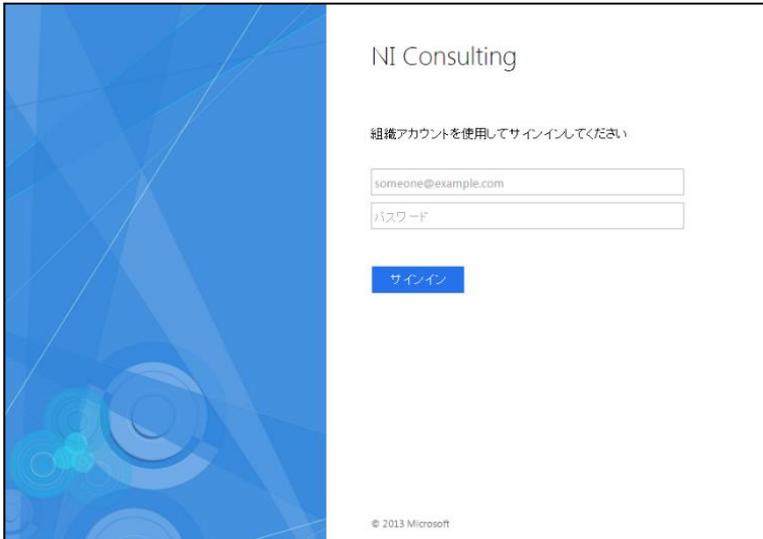
以下 2 通りの認証方法が利用可能です。



・ 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。



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://<IdP サーバーのアドレス>」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。

#### 1-1-4.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。



- ・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。

#### 1-1-5.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	○	○



- ・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、下記 2.~4.のセットアップ手順をご確認ください。

## 1-2.設定の流れ

### 1-2-1.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) ユーザーアカウントの登録

### 1-2-2.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。

セキュリティ > 制限/全体接続制限

**接続制限設定を間違えると製品に接続できなくなる恐れがあります。**  
全体接続制限を設定する場合は、まず個別接続制限で個人(システム管理者以外を推奨)を設定してください。  
次に設定した個人で製品にログインし設定情報が正しいことを確認した上で設定してください。  
接続方法の制限で「SSL(https)を用いた接続のみを許可する」場合は、実際にhttpsでの接続ができることを確認し、  
SSLでの接続ができない場合は、別途サーバー側に設定が必要です。  
SSLは443ポート固定となります。

**全体接続制限の設定は個別接続制限に引き継がれません。**  
全体接続制限の設定で個別接続制限にも反映させたい情報は、個別接続制限にも設定してください。

保存

接続元の制限:

標準版への接続

携帯版への接続

許可するIPアドレスを改行区切りで入力してください。  
未設定の場合はすべてのIPアドレスからの接続が許可されます。  
ここで指定したIPアドレスからの接続しかできなくなります。  
\*(アスタリスク)での指定が可能です。(例: 192.168.1.\*の場合は最後の桁が無視されます。)

接続方法の制限:

SSL(https)を用いた接続のみを許可する

除外対象:  標準版  携帯版  アプリ

SSLでの接続ができない場合は、別途サーバー側に設定が必要です。  
SSLは443ポート固定となります。

## 1-2-3.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。



### Point

・ 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。

### Step 1

#### 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。



### Step 2

#### 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。

## 2. セットアップ手順 (IdP:AD FS の場合)

### 2-1. 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 2012 R2 Standard Windows Server 2016 Standard Windows Server 2019 Standard  (※基本的に上記すべての OS で設定方法は同様であるが「IdP の設定」のみ、OS の種類によって画面が異なるため、2-4～2-6 と分けて記載します。)
IdP サーバーのアドレス	adfs.ni-saml.com  (※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。

### 2-2. 事前準備

#### 2-2-1. 証明書の準備

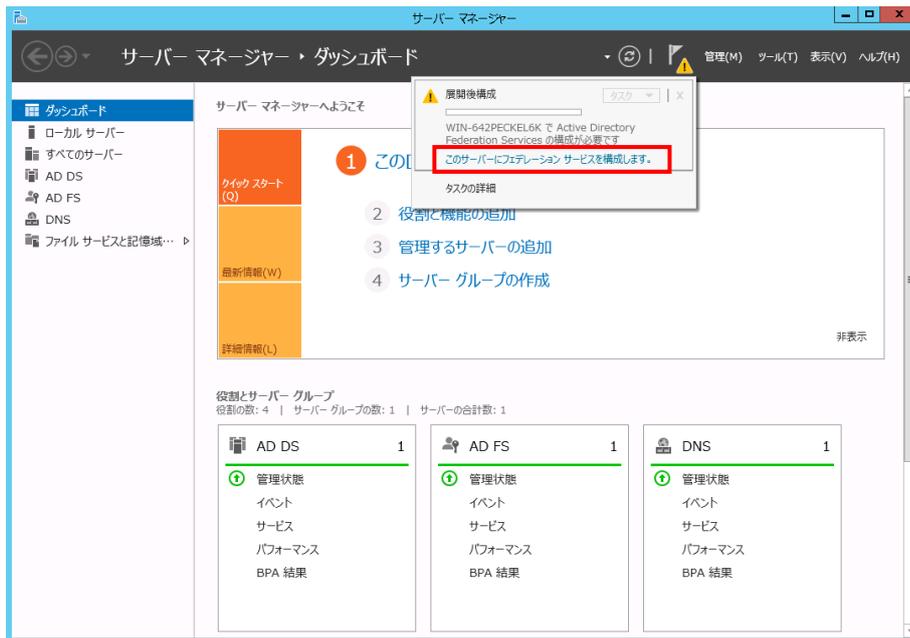
第三者認証機関が承認した、認証に使用する AD FS のサーバー証明書を.pfx 形式でエクスポートします。証明書を取得する一般的な方法には、OpenSSL を使用する方法、Certreq.exe を使用する方法、IIS を使用する方法の 3 種類があります。(※詳細は認証局の設定手順にしたがってください。)

OpenSSL を使用する方法は、以下 Microsoft 社の情報もご確認ください。

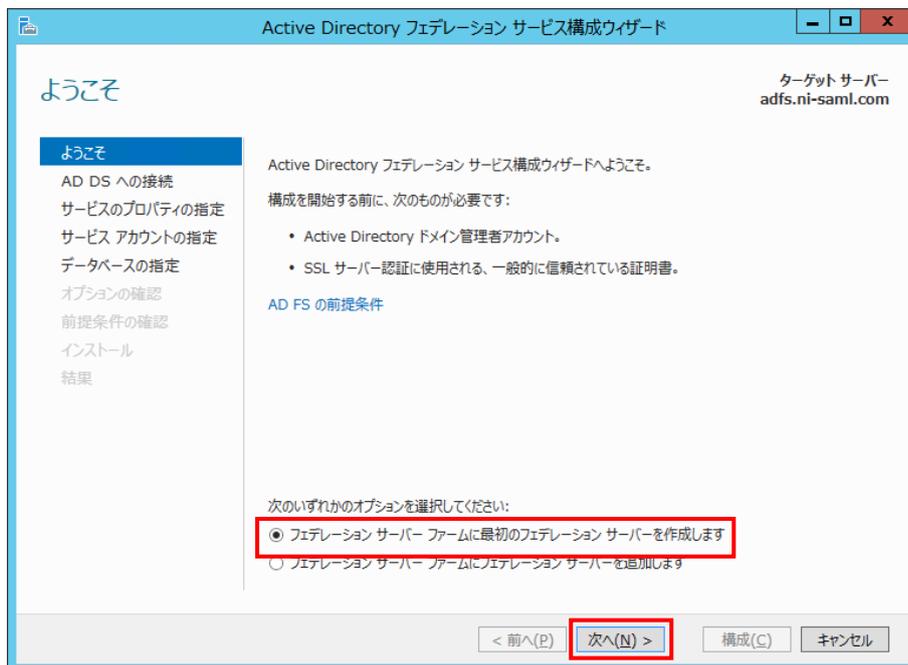
<https://docs.microsoft.com/ja-jp/azure/app-service/configure-ssl-certificate#export-certificate-to-pfx>

## 2-2-2.AD FS の構成

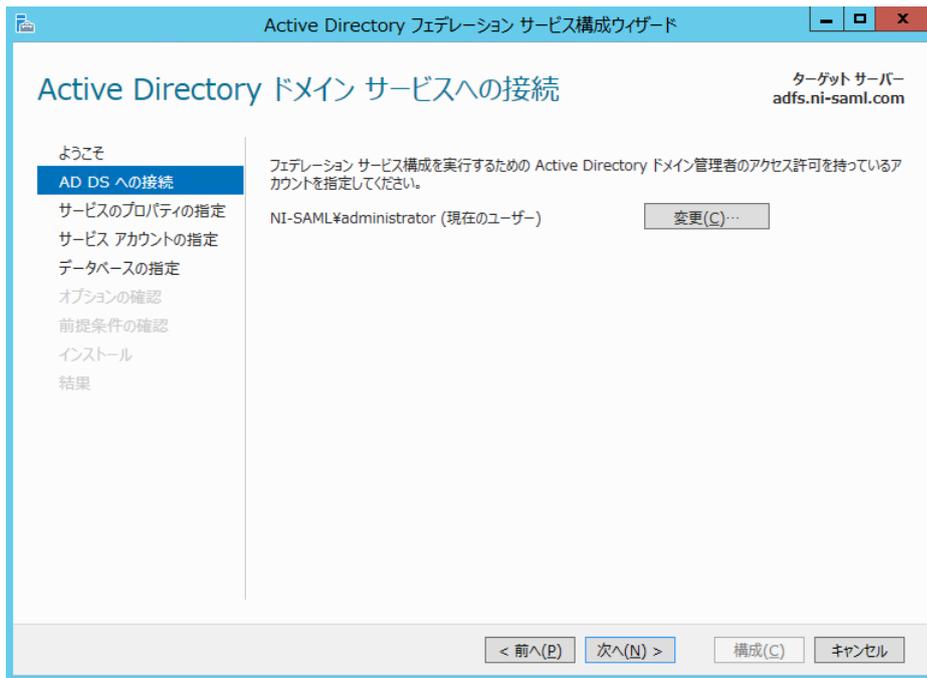
1. サーバーマネージャーより「このサーバーにフェデレーションサービスを構成します。」をクリックします。



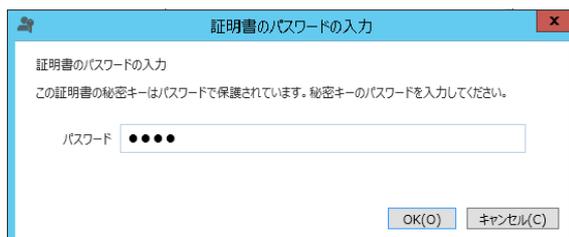
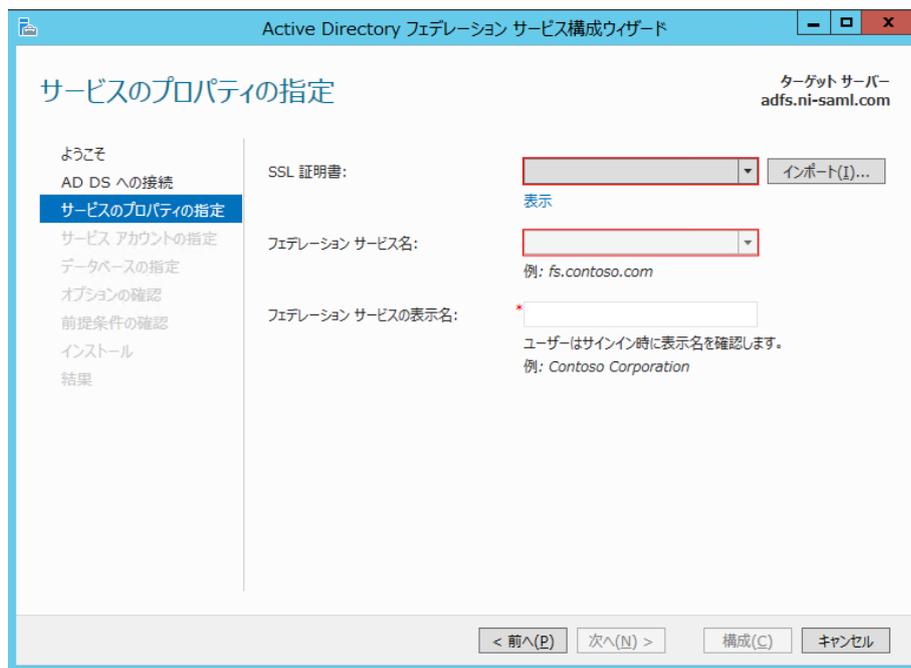
2. 「フェデレーションサーバーファームに最初のフェデレーションサーバーを作成します」を選択し、「次へ」をクリックします。



3. 「次へ」 をクリックします。

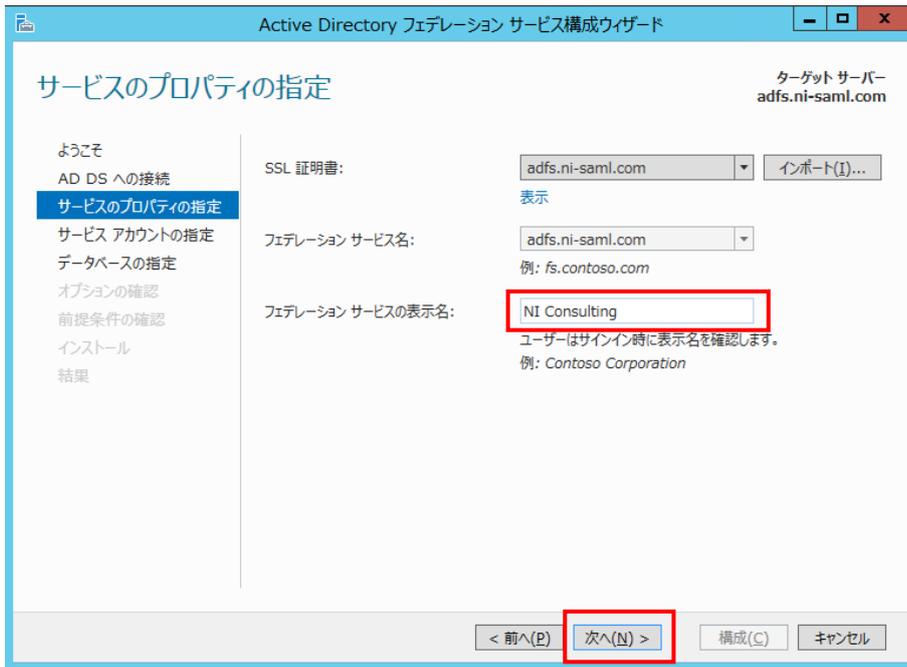


4. 「インポート」 をクリックし、.pfx 形式の証明書ファイルを選択します。  
証明書にパスワードが設定されている場合は入力して「OK」 をクリックします。

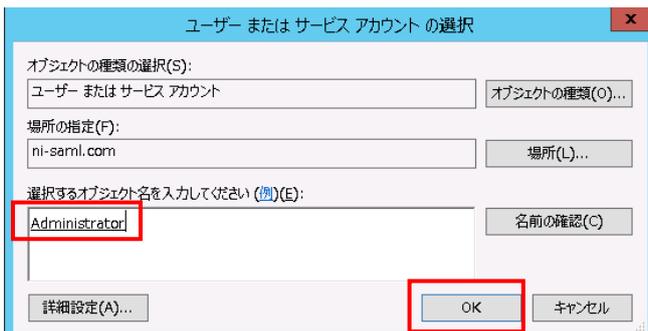
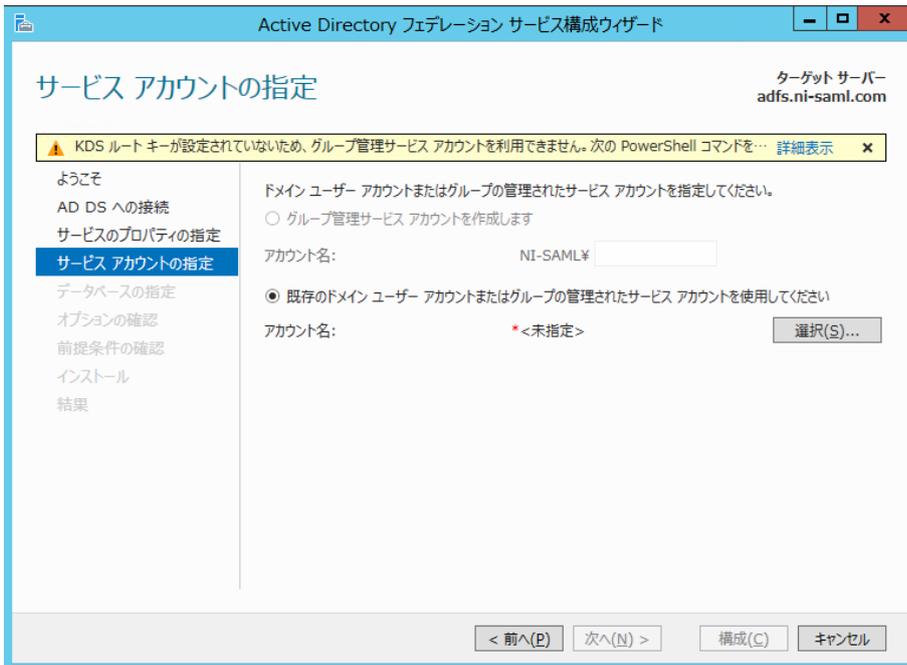


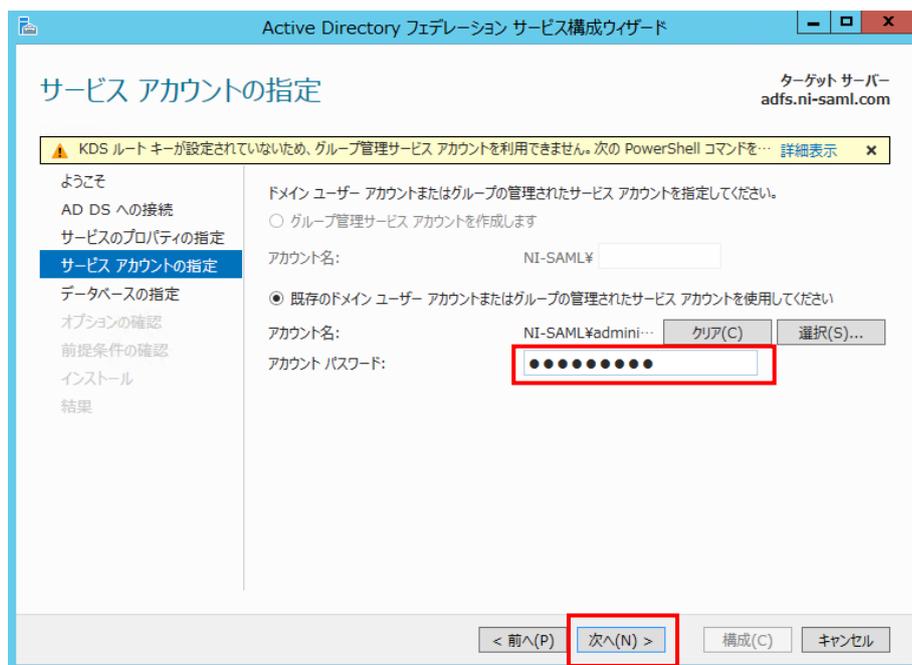
5. フェデレーションサービスの表示名を入力し、「次へ」をクリックします。

※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。

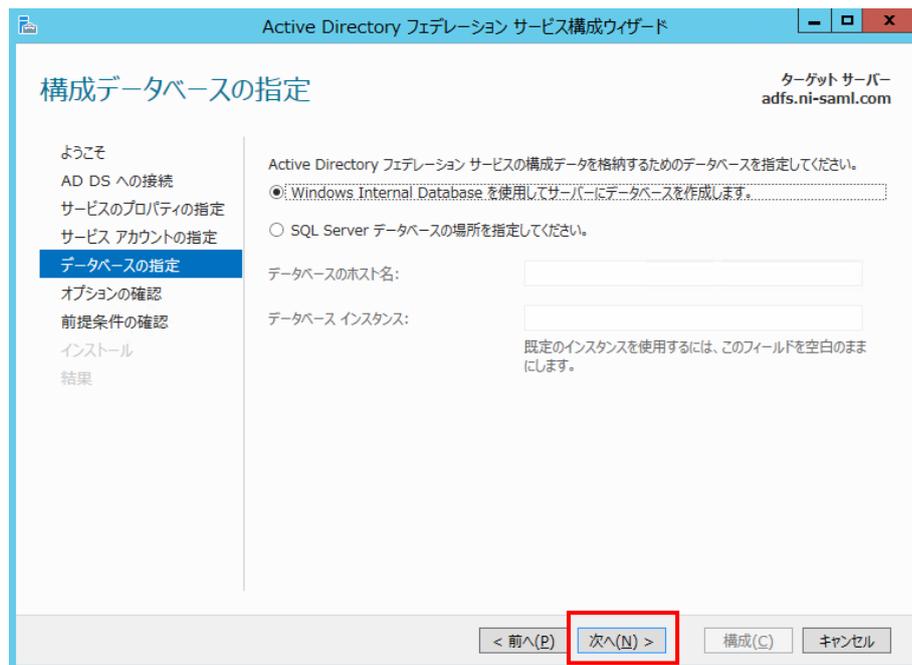


6. サービスアカウントに「Administrator」を選択し、パスワードを入力し、「次へ」をクリックします。

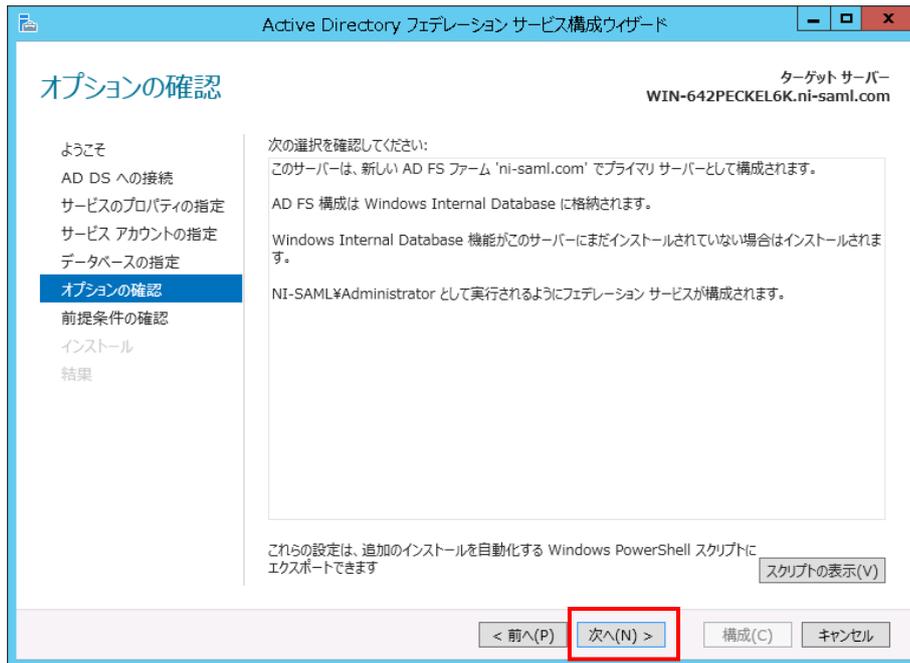




7. 「Windows Internal Database を使用してサーバーにデータベースを作成します。」を選択して、「次へ」をクリックします。

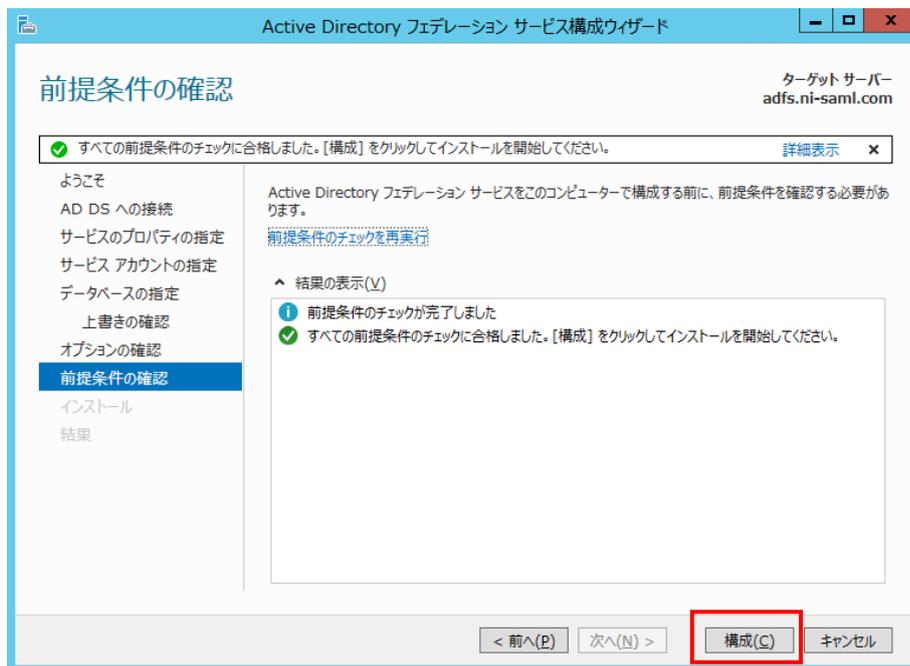


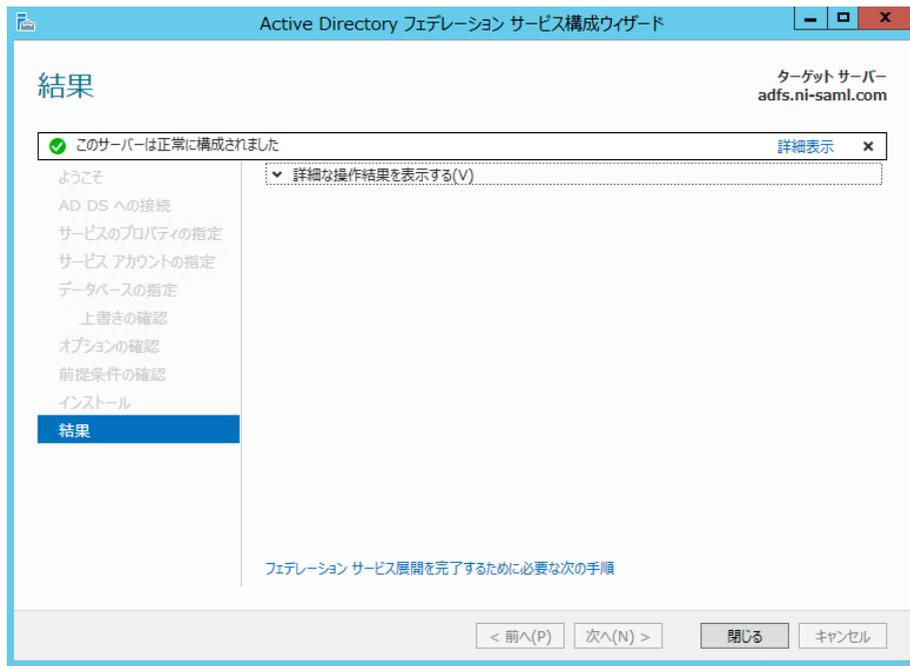
8. 「次へ」 をクリックします。



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。





## 2-3.NI 製品の設定

### 2-3-1.システム設定

1.システム設定の セキュリティ 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、  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。 ※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。 ※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 (※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。

メタデータ: ドラッグ&ドロップで貼り付けることができます。  
FederationMetadata.xml  
Identity Providerのメタデータをアップロードしてください。  
読み込むことができるファイルは、拡張子が「xml」のファイルです。  
XMLより設定値を抽出し、以下の項目を自動設定します。  
(エンティティID, エンドポイントURL, 証明書)  
**読み込み**

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。 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。

メタデータ: **ダウンロード**  
Service Providerメタデータをダウンロードします。  
※Service Provider設定を変更した場合は再ダウンロードが必要です。

⇒SP メタデータ XML ファイルがダウンロードされます。次項「[2-4.IdP の設定 \(Windows Server 2012 R2\)](#)」または「[2-5.IdP の設定\(Windows Server 2016 – ADFS\)](#)」にて使用します。

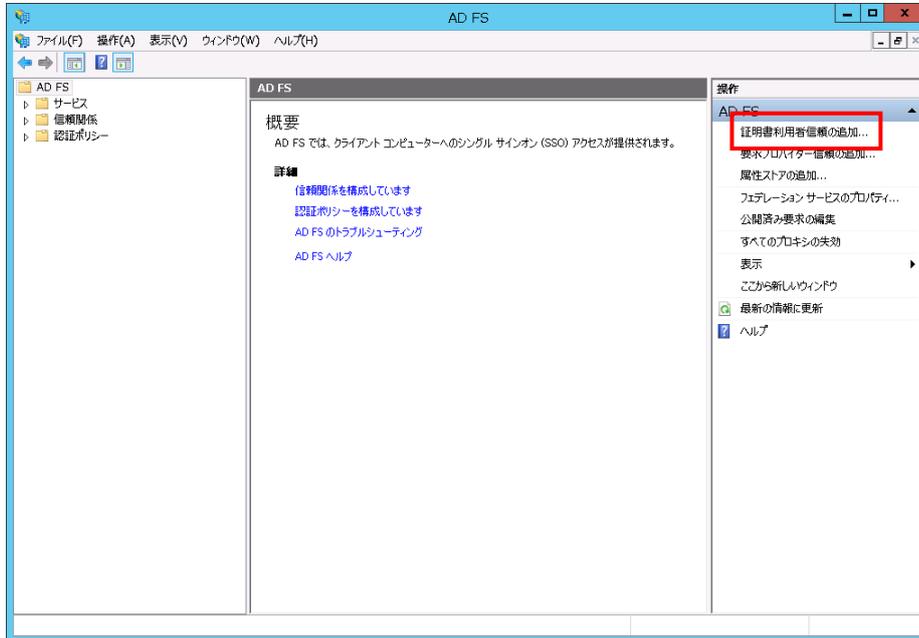
5. **保存** ボタンをクリックします。

## 2-4.IdP の設定(Windows Server 2012 R2)

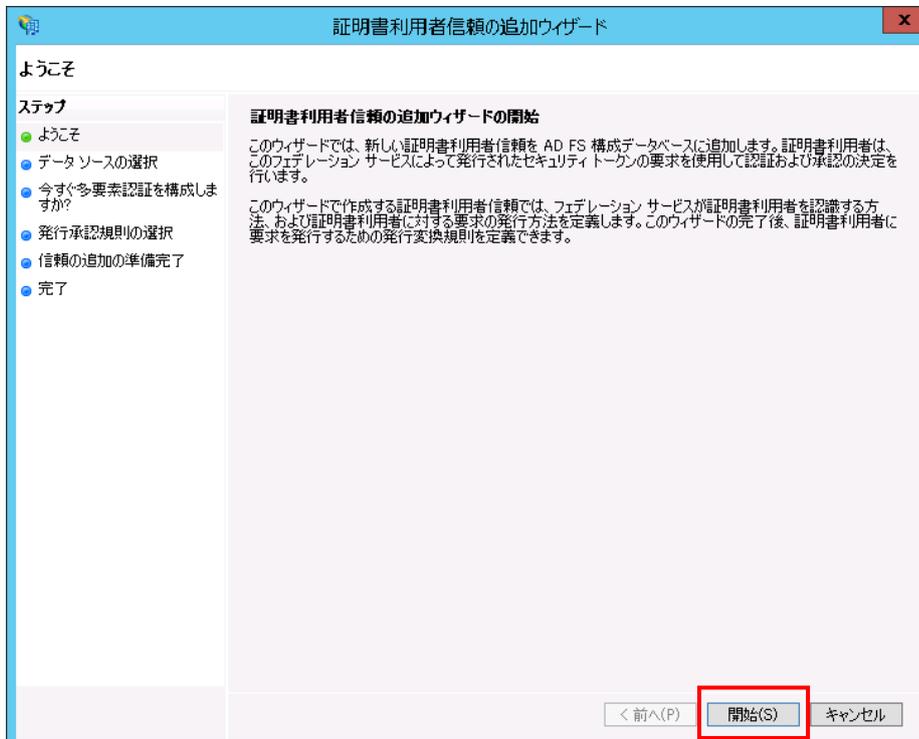
IdP サーバーで下記の設定を行います。

### 2-4-1.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、「開始」をクリックします。



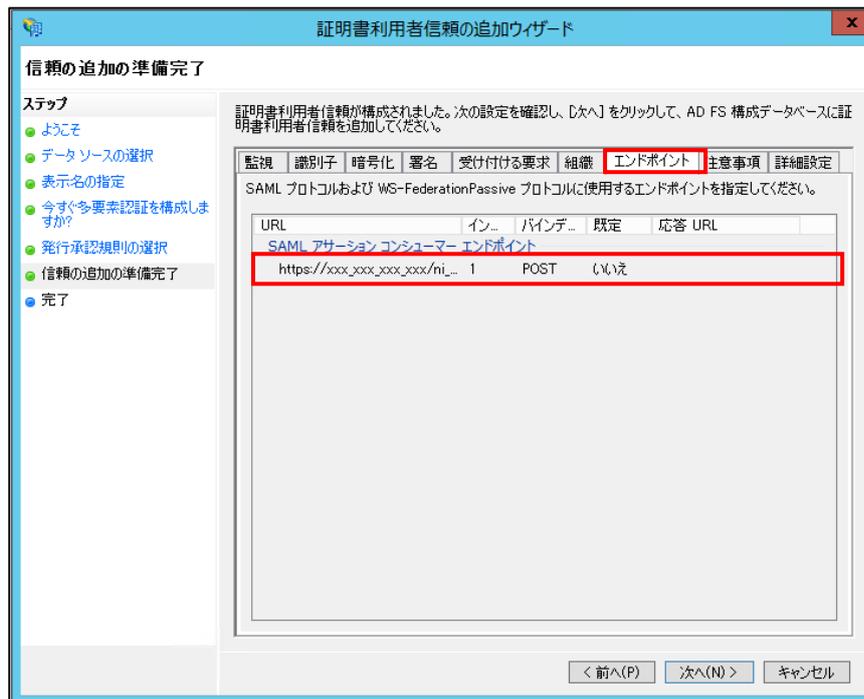
3. 「証明書利用者についてのデータをファイルからインポートする」を選択し、「参照」ボタンをクリックします。

「[2-3-1.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。

- ・ 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。

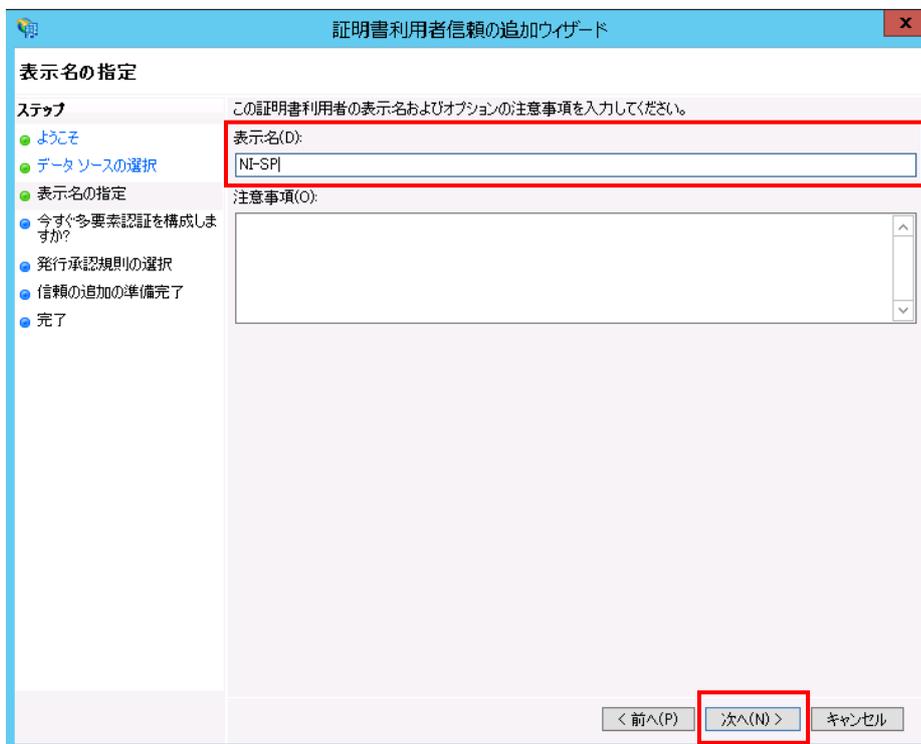


「SAML アサーション コンシューマー エンドポイント」: NI 製品システム設定画面の「エンドポイント URL」の値がセットされます。

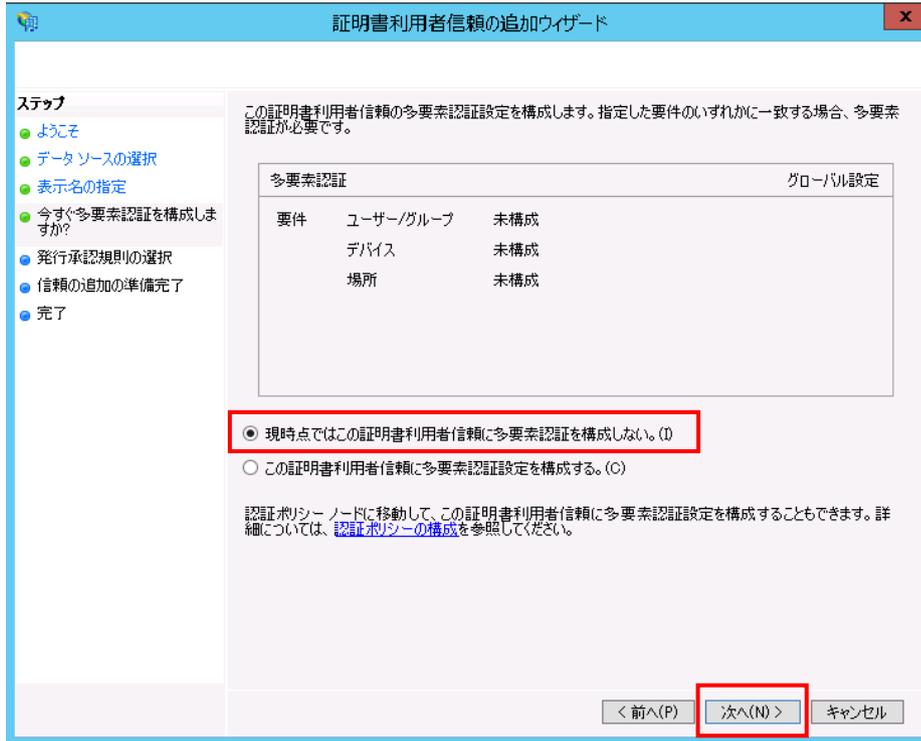


4. 表示名を入力し、「次へ」をクリックします。

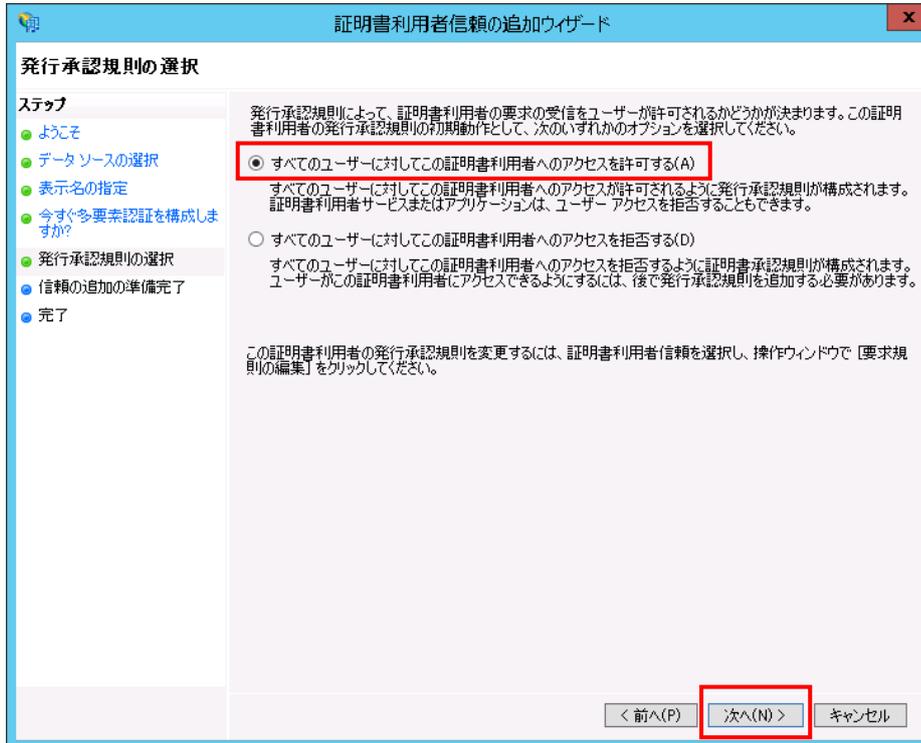
※表示名は AD FS の管理ツール上で表示される名称です。



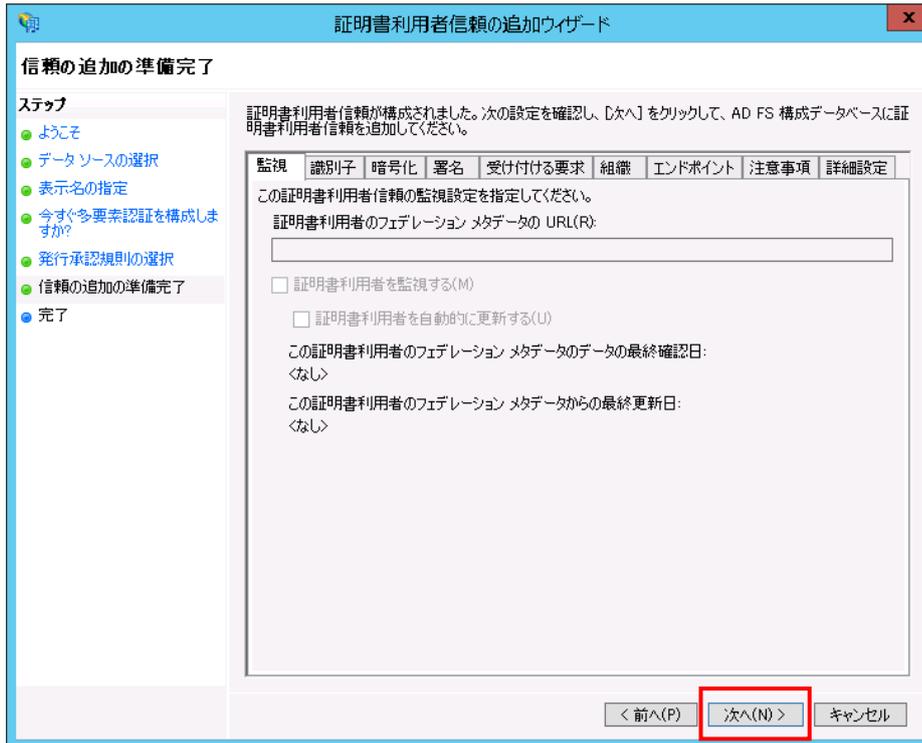
5. 「現時点ではこの証明書利用者信頼に他要素認証を構成しない」を選択し、「次へ」をクリックします。



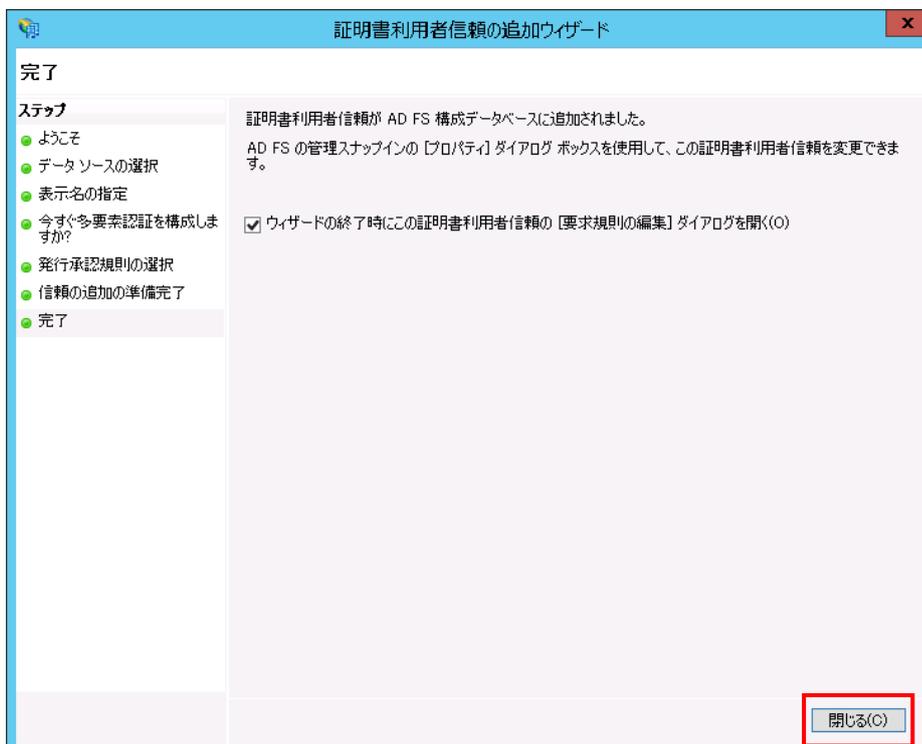
6. 「すべてのユーザーに対してこの証明書利用者へのアクセスを許可する」を選択し、「次へ」をクリックします。



7. 「次へ」 をクリックします。

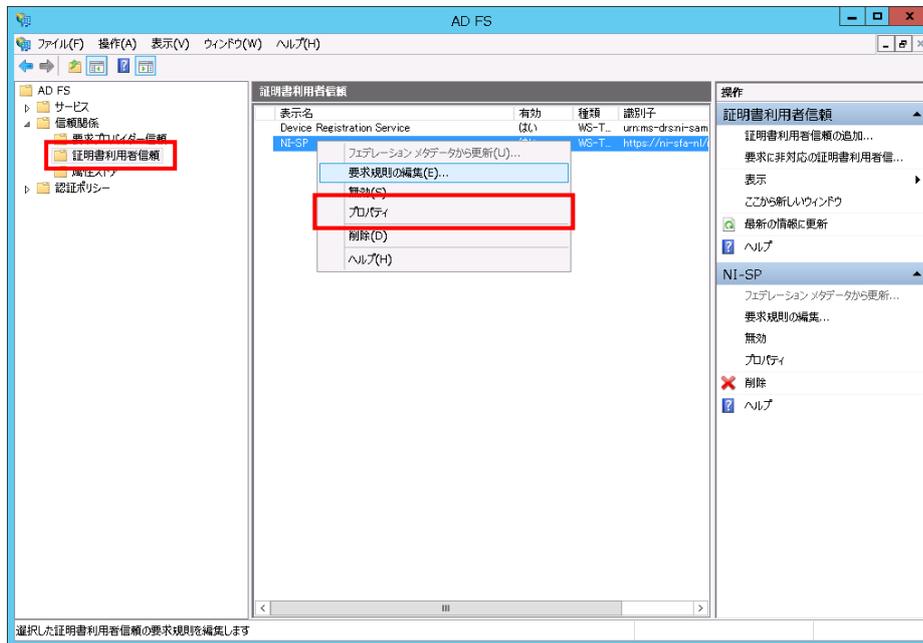


8. 証明書利用者信頼の追加が完了したので、「閉じる」 ボタンをクリックします。



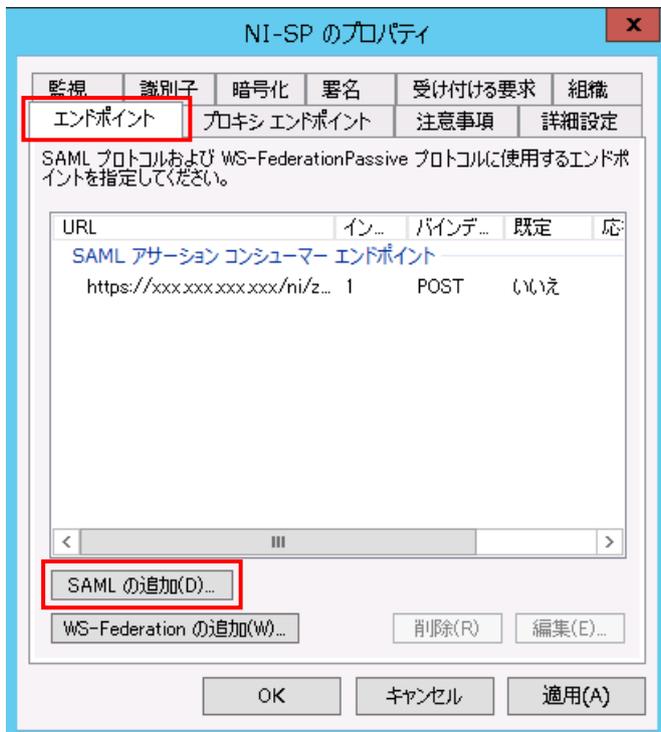
## 2-4-2.エンドポイント URL の追加

- 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://adfsni-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。

NI-SP のプロパティ

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 プロキシエンドポイント 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
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/z...	1	POST	(い)え	
https://adfsni-saml.com/ad...	0	Redirect	(い)え	

SAML の追加(D)...

WS-Federation の追加(W)... 削除(R) 編集(E)...

OK キャンセル 適用(A)

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(I): https://adfs.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。

NI-SP のプロパティ

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	プロキシ 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
<b>SAML アサーション コンシューマー エンドポイント</b>				
https://xxx.xxx.xxx.xxx/ni/z...	1	POST	(Y)え	
https://adfs.ni-saml.com/ad...	0	Redirect	(Y)え	
<b>SAML ログアウト エンドポイント</b>				
https://adfs.ni-saml.com/ad...		Redirect	(Y)え	

SAML の追加(D)...

WS-Federation の追加(W)... 削除(R) 編集(E)...

OK キャンセル 適用(A)

## 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。

変換要求規則の追加ウィザード

規則テンプレートの選択

ステップ

- 規則の種類を選択
- 要求規則の構成

作成する要求規則のテンプレートを次の一覧から選択してください。各要求規則テンプレートの詳細は説明に記載されています。

要求規則テンプレート(0):

要求規則テンプレートの説明

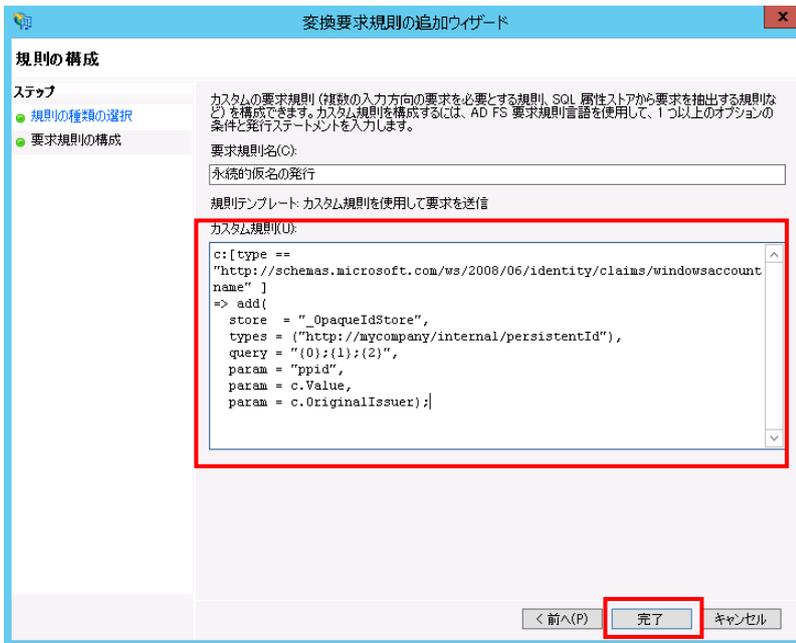
カスタム規則を使用すると、規則テンプレートでは作成できない規則を作成できます。カスタム規則は、AD FS 要求規則言語で記述します。次の機能を使用する場合は、カスタム規則を作成する必要があります。

- ・ SQL 属性ストアから要求を送信する
- ・ カスタムの LDAP フィルターを使用して LDAP 属性ストアから要求を送信する
- ・ カスタム属性ストアから要求を送信する
- ・ 複数の入力方向の要求がある場合にのみ要求を送信する
- ・ 入力方向の要求の値が複雑なパターンと一致する場合にのみ要求を送信する
- ・ 入力方向の要求の値に複雑な変更を加えて要求を送信する
- ・ 以降の規則で使用するだけの目的で要求を作成する

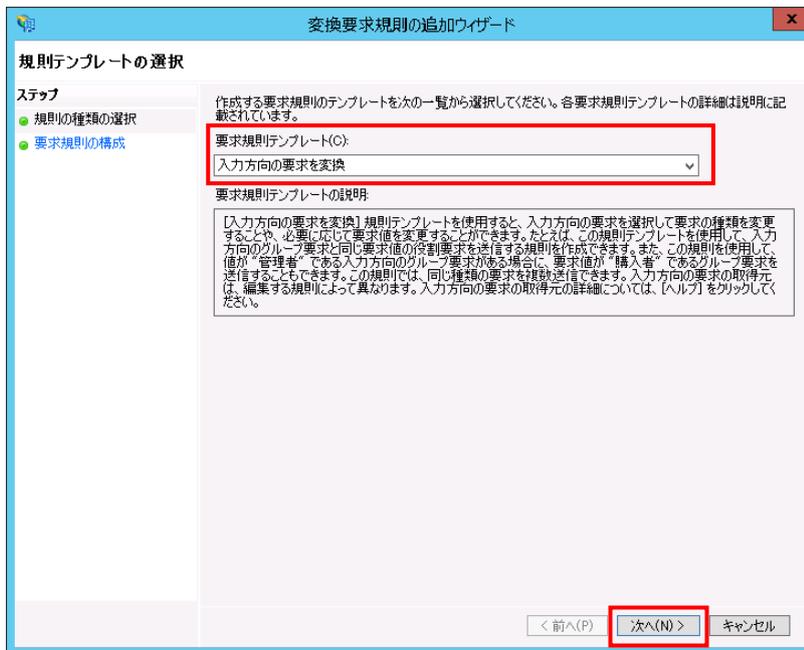
< 前へ(P)   **次へ(N) >**   キャンセル

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);
```



「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

- 規則の種類を選択
- 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

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: 指定なし

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

すべての要求値をバースルーする(S)  
 入力方向の要求の値を具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

2. 「OK」をクリックします。

NI-SP の要求規則の編集

発行変換規則 | 発行承認規則 | 委任承認規則

次の変換規則は、証明書利用者へ送信する要求を指定します。

順序	規則名	発行済み要求
1	永続的仮名の発行	<要求規則の表示>
2	NameIDとして返却	名前 ID

規則の追加(A)... 規則の編集(E)... 規則の削除(R)...

OK キャンセル 適用(P)

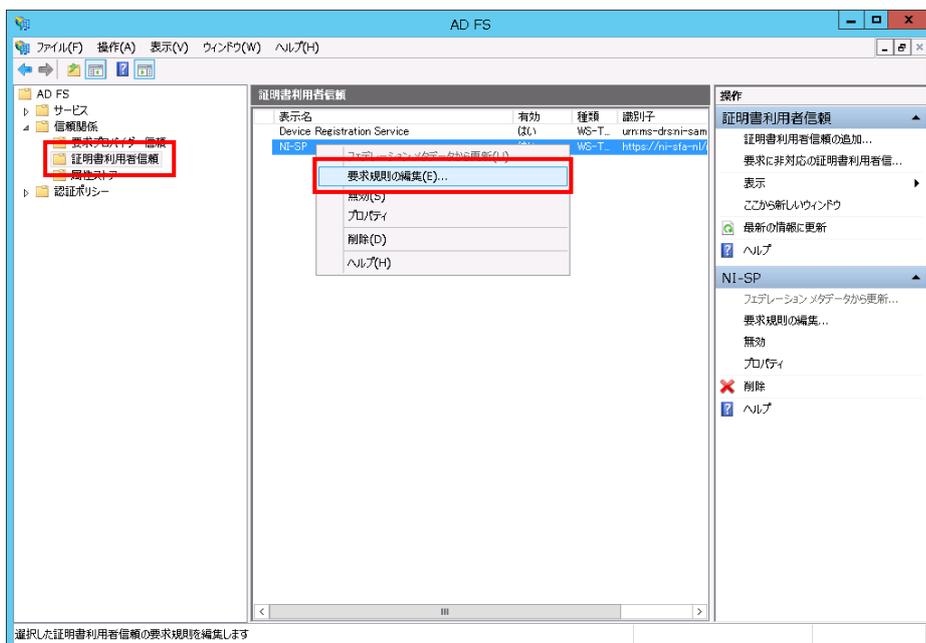
## 仮名を利用しない場合

  
**補足**

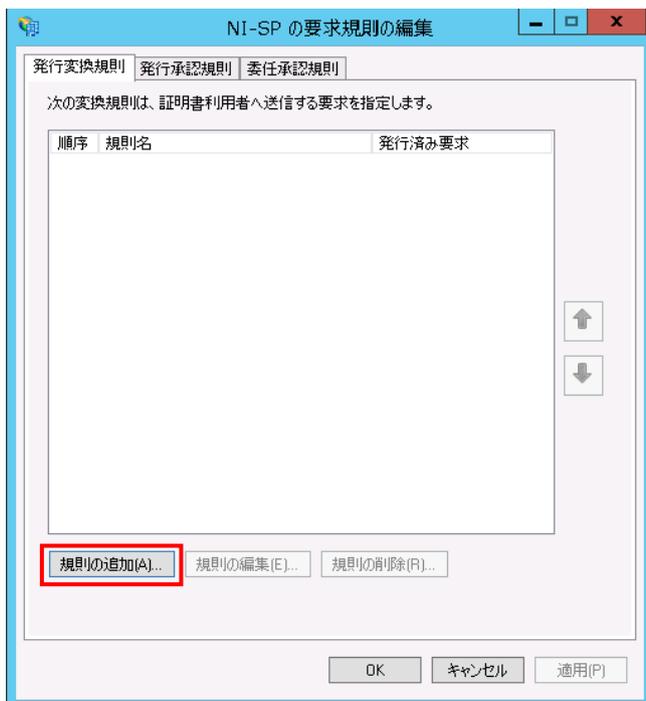
- ・ NameID として、AD のユーザー情報を返すように設定を行います。

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右クリックし、「要求規則の編集」を選択します。

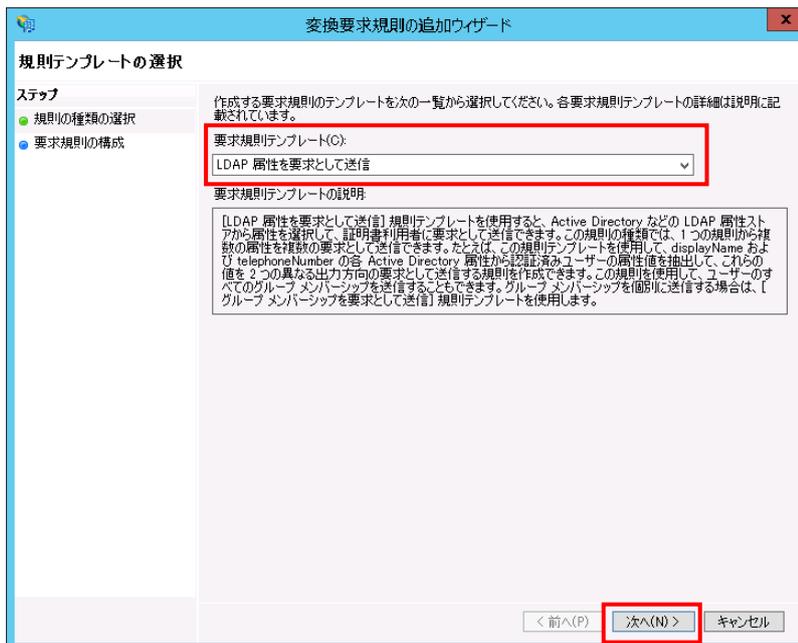


2. 「規則の追加」ボタンをクリックします。



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。



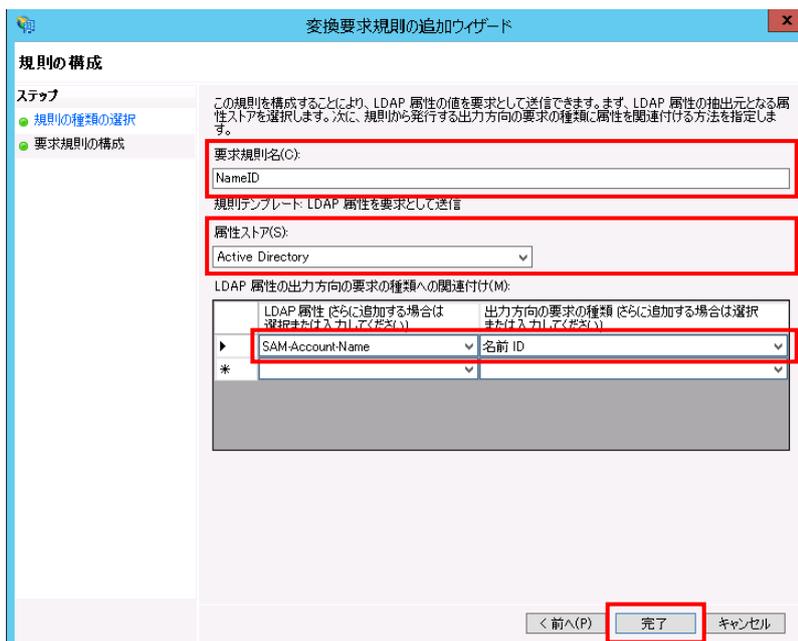
以下の値を選択し、「完了」をクリックします。

- ・ 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、「[2-5-3.変換要求規則の追加](#)」の「[仮名を利用しない場合](#)」を参照してください。

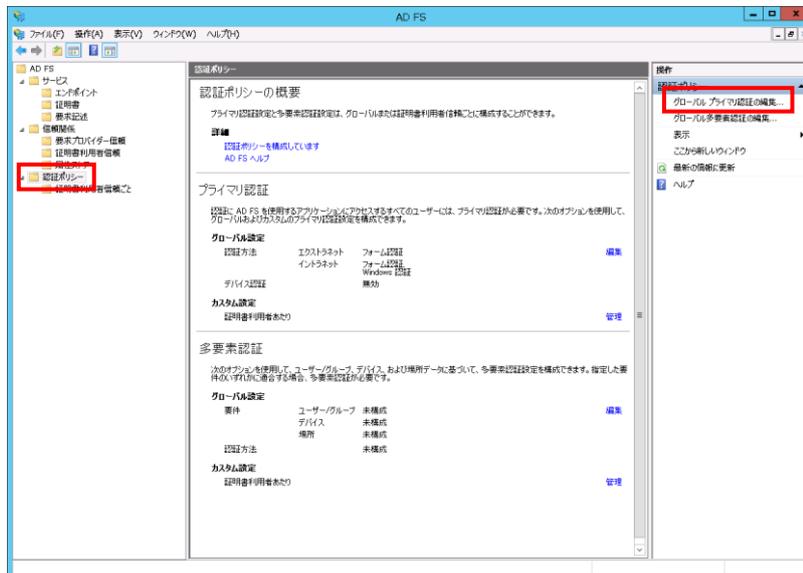
- ・ 出力方向の要求の種類：「名前 ID」を選択します。



## 2-4-4. 認証ポリシーの設定

1. AD FS の管理ツールを表示し、「認証ポリシー」メニューを選択します。

グローバルプライマリ認証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

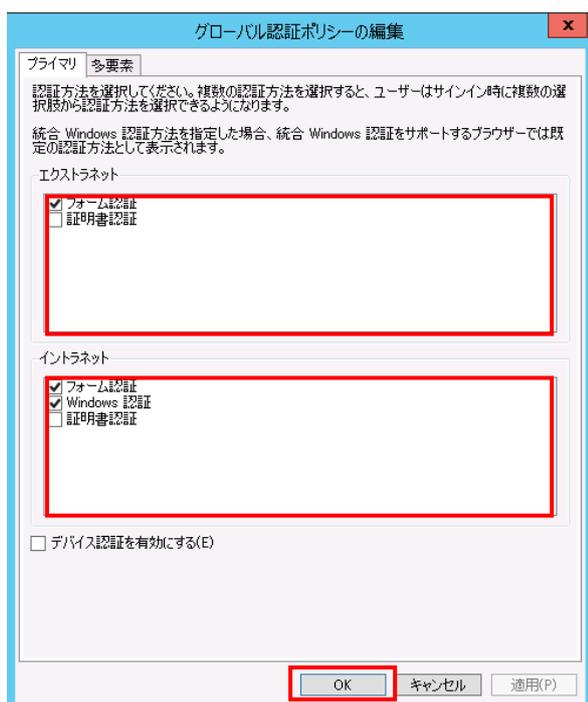
エクストラネット：「フォーム認証」にチェックします。

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。

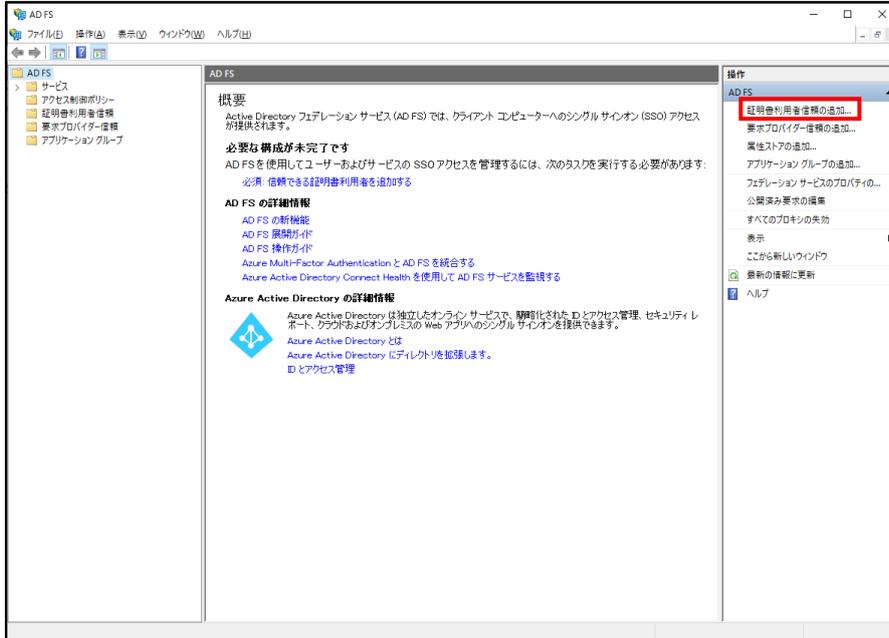


## 2-5.IdP の設定(Windows Server 2016 – ADFS)

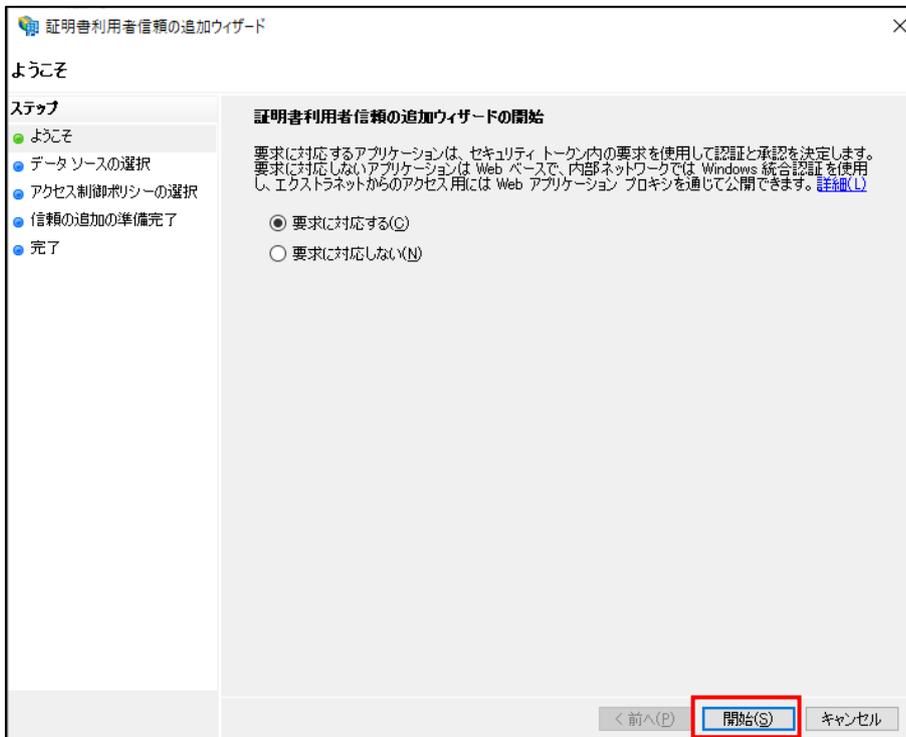
IdP サーバーで下記の設定を行います。

### 2-5-1.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。
- 「[2-3-1.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。

証明書利用者情報の追加ウィザード

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
- アクセス制御ポリシーの選択
- 情報の追加の準備完了
- 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)(E):

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(B):

C:\Users\Administrator\Desktop\sp\_metadata.xml

証明書利用者についてのデータを手動で入力する(I)  
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(B)   次へ(N) >   キャンセル

- ・ 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、「情報の追加の準備完了」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。



証明書利用者情報の追加ウィザード

情報の追加の準備完了

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
- 情報の追加の準備完了
- 完了

証明書利用者情報が構成されました。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情報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

この証明書利用者情報の表示名および識別子を指定してください。

表示名(S):

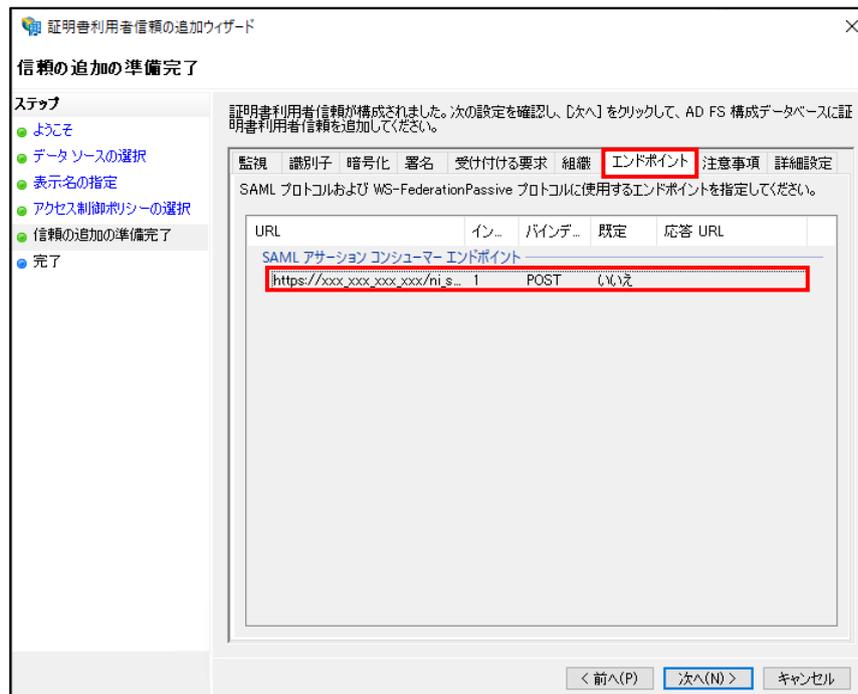
NI-SP

証明書利用者の識別子(E):

https://xxx.xxx.xxx.xxx/ni\_saml/

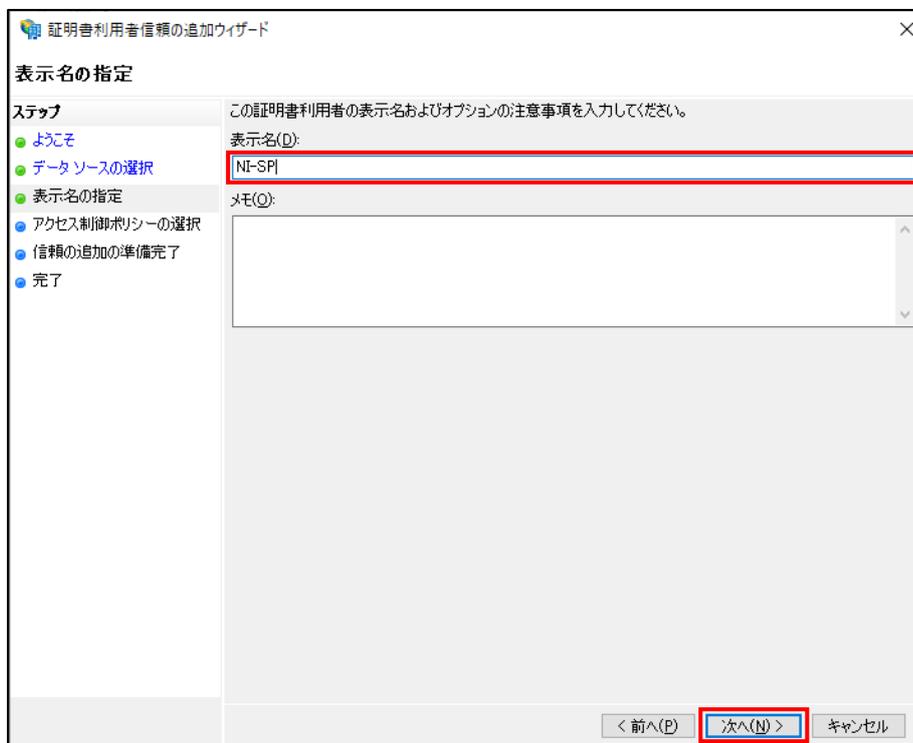
< 前へ(B)   次へ(N) >   キャンセル

「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。

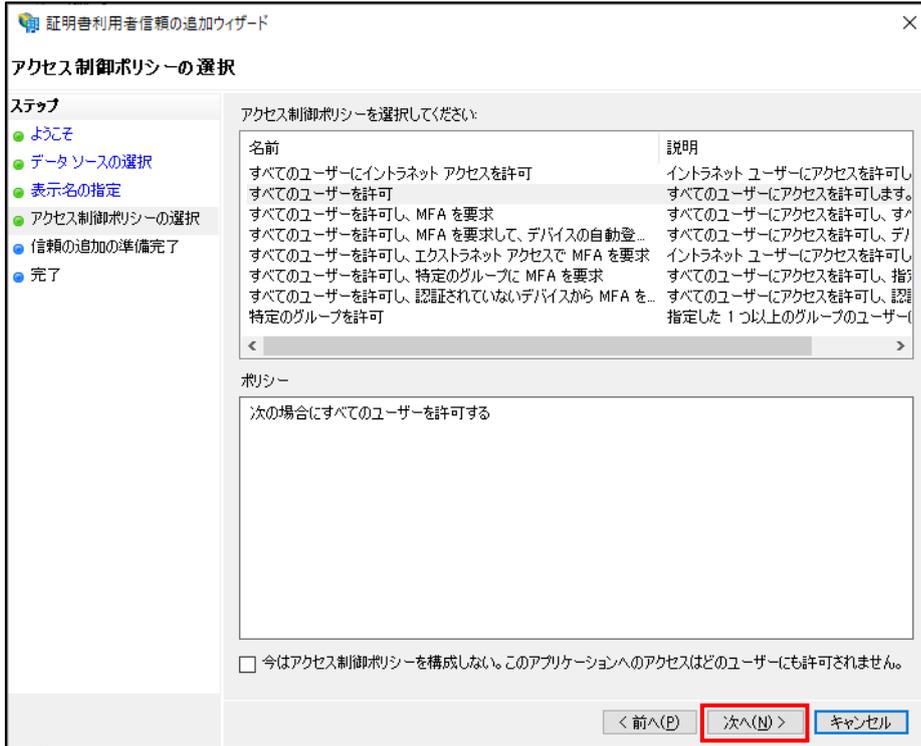


4. 表示名を入力し、「次へ」をクリックします。

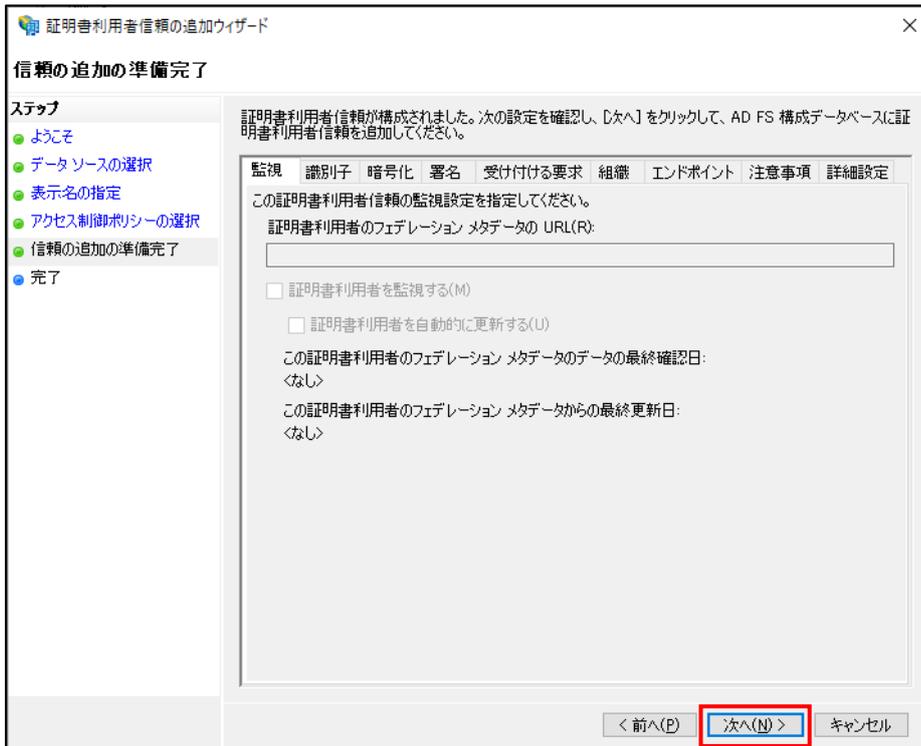
※表示名は AD FS の管理ツール上で表示される名称です。



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。

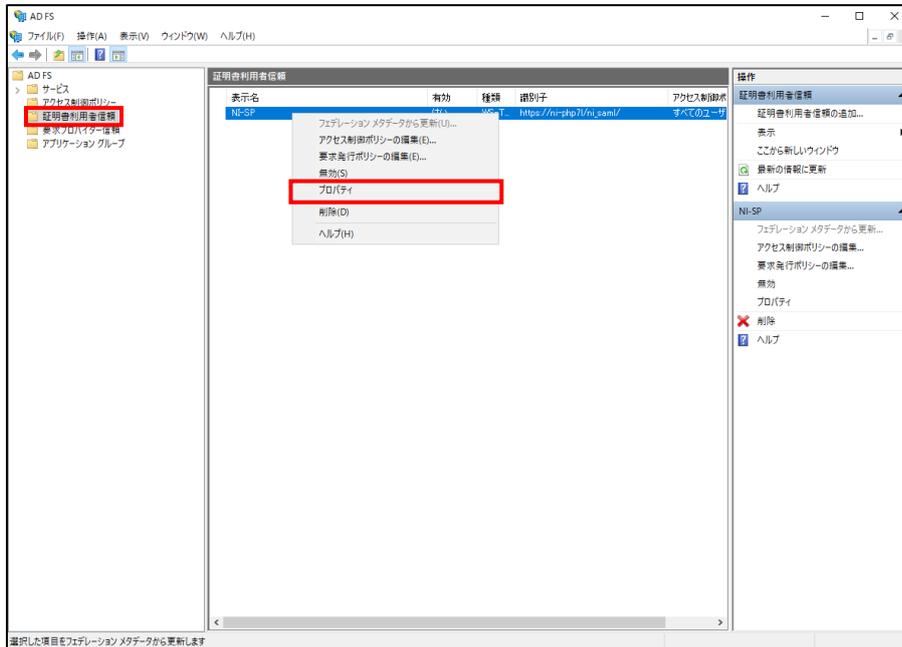


7. 証明書利用者信頼の追加が完了したので、「このアプリケーションの要求発行ポリシーを構成する」にチェックを付けたまま、「閉じる」ボタンをクリックします。



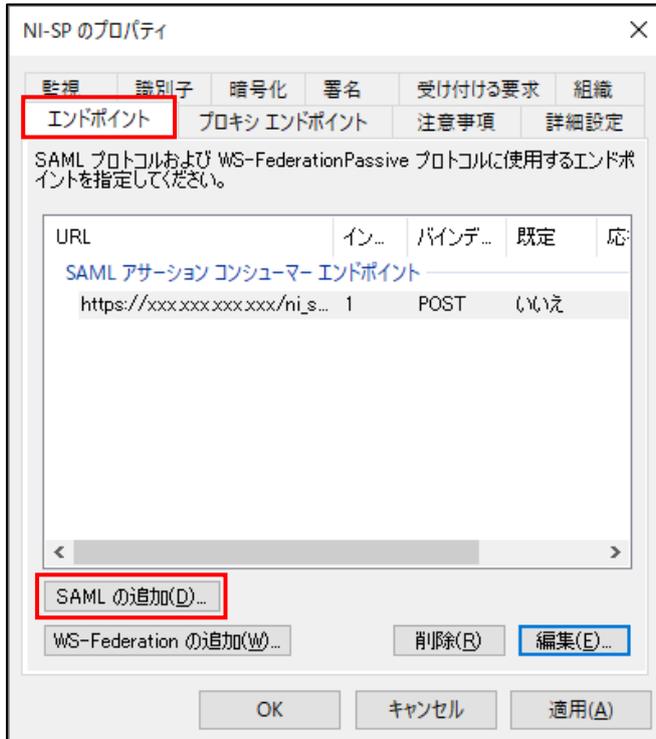
## 2-5-2.エンドポイント URL の追加

- 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。

NI-SP のプロパティ

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 プロキシエンドポイント 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...
<b>SAML アサーションコンシューマー エンドポイント</b>				
https://xxxx.xxxxxxxx.ni_s...	1	POST	(いいえ)	
https://niadfs5.ni-saml.com...	0	Redirect	(いいえ)	

SAML の追加(D)...

WS-Federation の追加(W)... 削除(R) 編集(E)...

OK キャンセル 適用(A)

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://niadfs5ni-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。

NI-SP のプロパティ

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 プロキシエンドポイント 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
<b>SAML アサーション コンシューマー エンドポイント</b>				
https://xxx.xxx.xxx.xxx/ni_s...	1	POST	(Y)え	
https://niadf5ni-saml.com/...	0	Redirect	(Y)え	
<b>SAML ログアウト エンドポイント</b>				
https://niadfs5ni-saml.com...		Redirect	(Y)え	

SAML の追加(D)...

WS-Federation の追加(W)...

削除(R) 編集(E)...

OK キャンセル 適用(A)

## 2-5-3.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。

変換要求規則の追加ウィザード

規則テンプレートの選択

ステップ

- 規則の種類を選択
- 要求規則の構成

作成する要求規則のテンプレートを次の一覧から選択してください。各要求規則テンプレートの詳細は説明に記載されています。

要求規則テンプレート(C):  
カスタム規則を使用して要求を送信

要求規則テンプレートの説明

カスタム規則を使用すると、規則テンプレートでは作成できない規則を作成できます。カスタム規則は、AD FS 要求規則言語で記述します。次の機能を使用する場合は、カスタム規則を作成する必要があります。

- ・ SQL 属性ストアから要求を送信する
- ・ カスタムの LDAP フィルターを使用して LDAP 属性ストアから要求を送信する
- ・ カスタム属性ストアから要求を送信する
- ・ 複数の入力方向の要求がある場合にもみ要求を送信する
- ・ 入力方向の要求の値が複雑なパターンと一致する場合にもみ要求を送信する
- ・ 入力方向の要求の値に複雑な変更を加えて要求を送信する
- ・ 以降の規則で使用するための目的で要求を作成する

< 前へ(B)   次へ(N) >   キャンセル

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);
```



「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。

交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、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(N):  
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(O):

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

すべての要求値をバースルーする(S)  
 入力方向の要求の値を具なる出力方向の要求の値に置き換える(B)  
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(O)  
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

2. 「OK」をクリックします。

NI-SP の要求発行ポリシーの編集

発行変換規則

次の変換規則は、証明書利用者へ送信する要求を指定します。

順序	規則名	発行済み要求
1	永続的仮名の発行	<要求規則の表示>
2	NameIDとして返却する	名前 ID

規則の追加(A)... 規則の編集(E)... 規則の削除(R)...

OK キャンセル 適用(P)

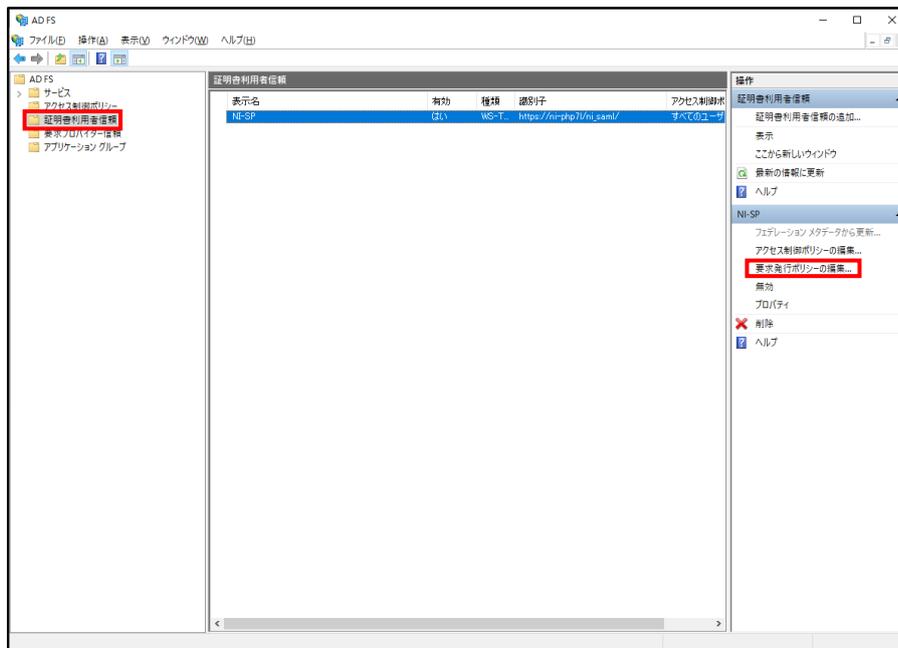
## 仮名を利用しない場合

  
**補足**

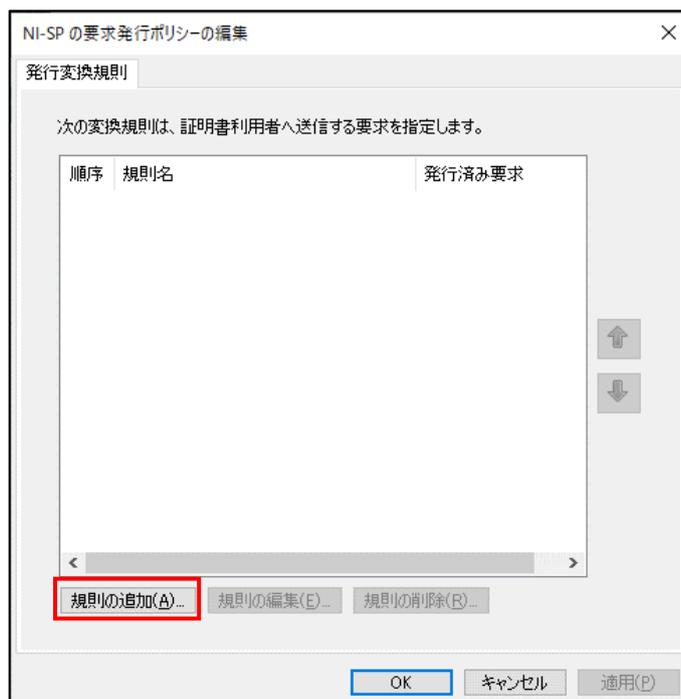
- ・ NameID として、AD のユーザー情報を返すように設定を行います。

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。



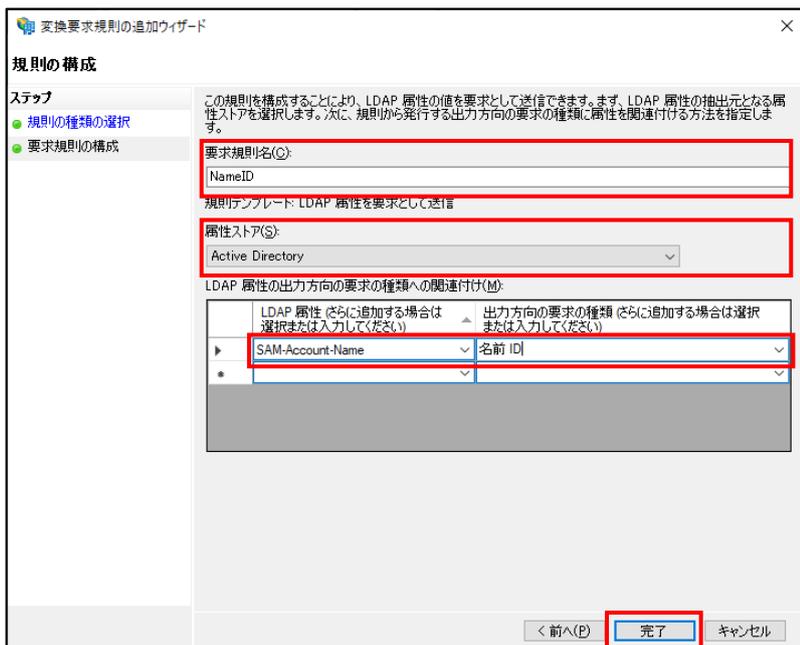
以下の値を選択し、「完了」をクリックします。

- ・ 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。



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。

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、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に関連付ける方法を指定します。

要求規則名(C):  
NameID

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
Company	
Department	
Display-Name	
E-Mail-Addresses	
Employee-ID	
Employee-Number	
Employee-Type	
Given-Name	
Is-Member-Of-DL	
Organizational-Unit-Name	
Organization-Name	
Proxy-Addresses	
SAM-Account-Name	
State-Or-Province-Name	
Street-Address	
Surname	
Telephone-Number	
Title	
Token-Groups (SID)	
Token-Groups - ドメイン名を含む	
Token-Groups - 完全修飾ドメイン名を含む	
Token-Groups - 名前指定なし	
User-Principal-Name	

< 前へ(P) 完了 キャンセル



補足

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。

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	プロフィール
		電話	組織
			公開された証明書

ユーザー ログオン名(U):  
terakawa @xxxxx.com

ユーザー ログオン名 (Windows 2000 より前)(W):  
NI-SAML¥ terakawa

ログオン時間(L)... ログオン先(O)...

アカウントのロックを解除する(N)

アカウント オプション(O):

- ユーザーは次回ログオン時にパスワード変更が必要
- ユーザーはパスワードを変更できない
- パスワードを無期限にする
- 暗号化を元に戻せる状態でパスワードを保存する

アカウントの期限

なし(N)

有効期限(E): 2023年 7月 15日

OK キャンセル 適用(A) ヘルプ

• 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)。

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	プロフィール	電話	組織	公開された証明書

ユーザー ログオン名(U):  
terakawa @xxxxx.com

ユーザー ログオン名 (Windows 2000 より前)(W):  
NI-SAML¥ terakawa

ログオン時間(L)... ログオン先(O)...

アカウントのロックを解除する(N)

アカウント オプション(O):

- ユーザーは次回ログオン時にパスワード変更が必要
- ユーザーはパスワードを変更できない
- パスワードを無期限にする
- 暗号化を元に戻せる状態でパスワードを保存する

アカウントの期限

なし(W)

有効期限(E): 2023年 7月 15日

OK キャンセル 適用(A) ヘルプ



• 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	プロフィール	電話	組織	公開された証明書

寺川 傑

姓(L): 寺川

名(E): 傑 イニシャル(I):

表示名(S): 寺川 傑

説明(O):

事業所(O):

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

## 2-5-4. 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

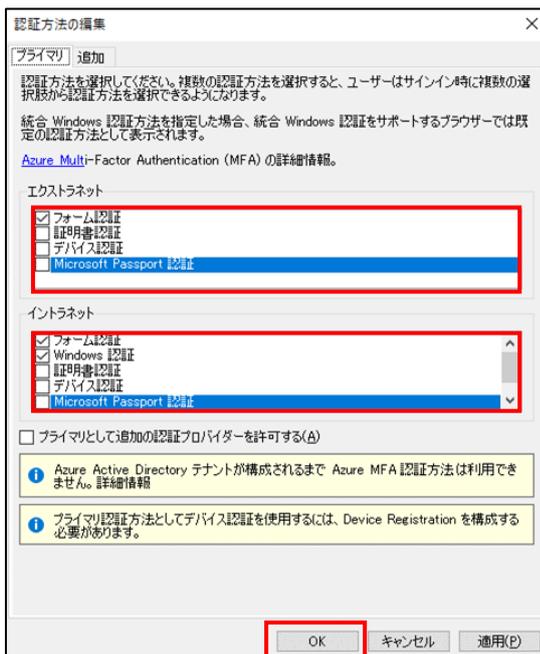
エクストラネット : 「フォーム認証」にチェックします。

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。



## 2-6.IdPの設定(Windows Server 2019)

Windows Server 2016 同様の手順となります。

「[2-5.IdPの設定\(Windows Server 2016-ADFS\)](#)」を参照してください。

## 2-7.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。

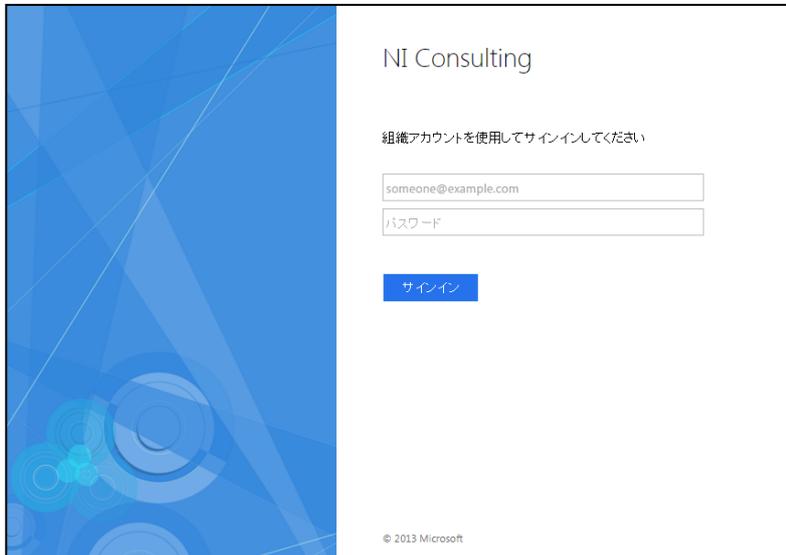
### 2-7-1.オプション設定

- 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.  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  ボタンを押します。

## 2-8.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。



- ・ 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。

## 2-9.トラブルシューティング

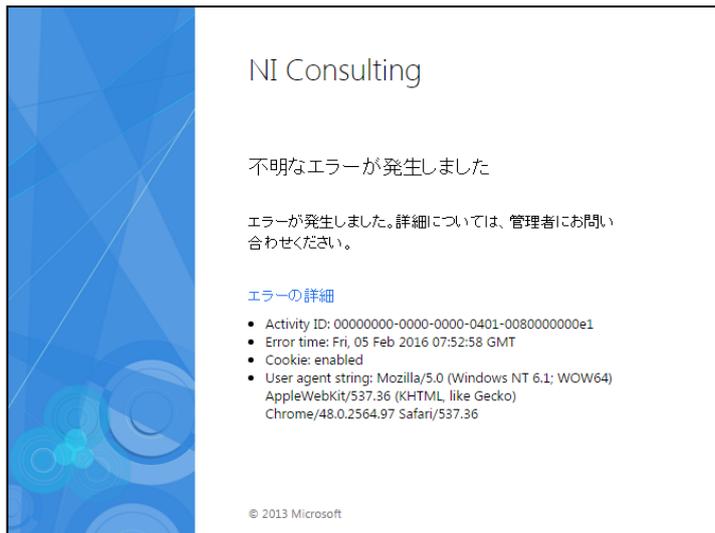


補足

- ・ 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、「[4.トラブルシューティング](#)」を参照してください。

### 2-9-1.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

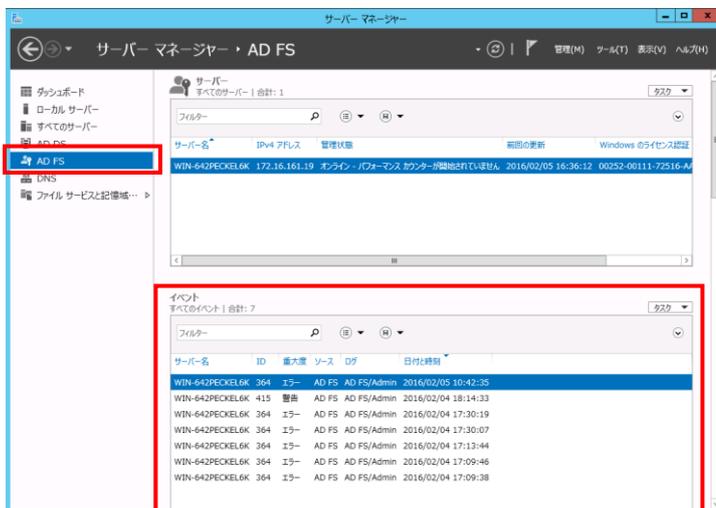
<https://xxx.xxx.xxx.xxx/ni/niware/portal/index.php?saml=no>

例) Sales Force Assistant シリーズ

<https://xxx.xxx.xxx.xxx/ni/<各製品>/main/index.php?saml=no>

## 2-9-2.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。



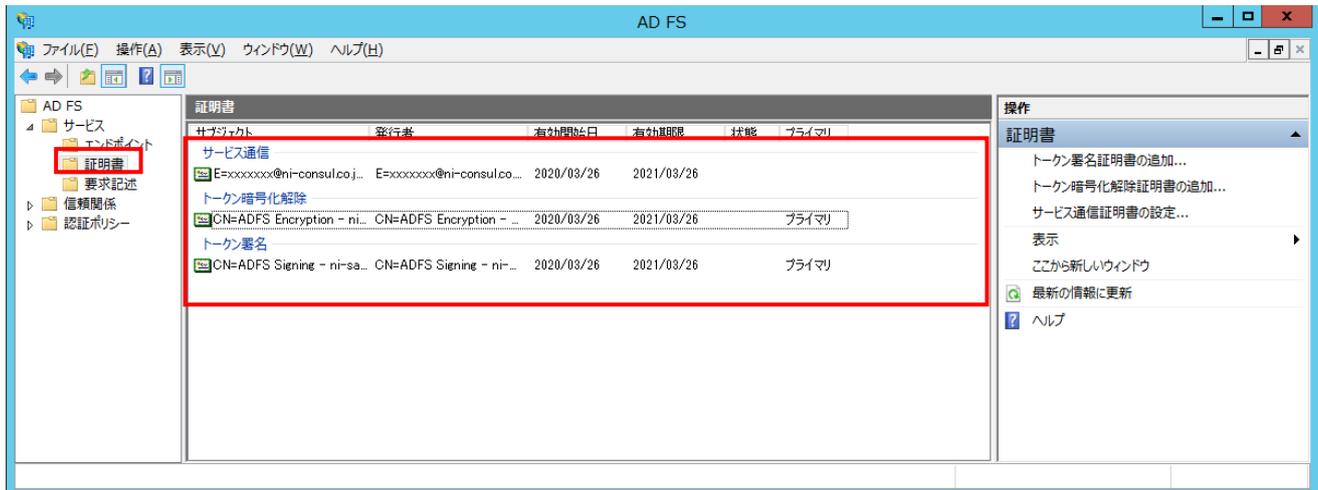
AD FS の設定不備が原因で発生する主要なエラーを以下に記載します。

エラーID	エラーメッセージ	対応方法
364	<p>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。</p> <p>追加データ ...</p>	<p>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。</p> <p>※パッシブな要求 = Web ブラウザからの要求</p>
364	<p>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。</p> <p>追加データ</p> <p>プロトコル名: Saml</p> <p>証明書利用者: https://xxx.xxx.xxx.xxx/ni/</p> <p>例外情報: Microsoft.IdentityServer.Web.InvalidScopeException: MSIS7007: 要求された証明書利用者信頼 '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、管理者にお問い合わせください。</p> <p>場所 Microsoft.IdentityServer.Web.Protocols.Saml.SamlSignInContext.Validate() 場所 Microsoft.IdentityServer.Web.Protocols...</p>	<p>SP のエンティティ ID が誤っています。</p> <p>(※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。)</p> <p>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。</p>
261	<p>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。</p> <p>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</p> <p>証明書利用者: https://xxx.xxx.xxx.xxx/ni/</p> <p>この要求は失敗しました。</p> <p>ユーザー操作</p> <p>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。</p>	<p>SP のエンドポイント URL が誤っています。</p> <p>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。</p>

エラーID	エラーメッセージ	対応方法
321	<p>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。</p> <p>要求元: https://xxx.xxx.xxx.xxx/ni/</p> <p>名前識別子の形式: urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</p> <p>SPNameQualifier:</p> <p>例外の詳細:</p> <p>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:persistent SPNameQualifier: 。実際の NameID プロパティ: Format: , NameQualifier: SPNameQualifier: , SPProvidedId: 。</p> <p>この要求は失敗しました。</p> <p>ユーザー操作</p> <p>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。</p>	<p>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。</p> <p><a href="#">「2-4-3 変換要求規則の追加」</a> 項の手順が正しく実行できているか、確認してください。</p>
273	<p>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。</p> <p>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'</p> <p>証明書利用者: https://xxx.xxx.xxx.xxx/ni/</p> <p>この要求は失敗しました。</p> <p>ユーザー操作</p> <p>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。</p>	<p>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。</p> <p><a href="#">「2-4-2 エンドポイント URL の追加」</a> 項の手順が正しく実行できているか、確認してください。</p>

## 2-10.運用時の注意

### 2-10-1.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

「[2-2-2 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。

[https://docs.microsoft.com/ja-jp/archive/blogs/jpntsblog/ad-fs-%E3%81%AE%E8%87%AA%E5%8B%95%E8%A8%BC%E6%98%8E%E6%9B%B8%E3%83%AD%E3%83%BC%E3%83%AB%E3%82%AA%E3%83%BC%E3%83%90%E3%83%BC%E6%A9%9F%E8%83%BD%E3%81%AB%E3%81%A4%E3%81%84%E3%81%A6](https://docs.microsoft.com/ja-jp/archive/blogs/jpntsblog/ad-fs-%E3%81%AE%E8%87%AA%E5%8B%95%E8%A8%BC%E6%98%8E%E6%9B%B8%E3%83%A D%E3%83%BC%E3%83%AB%E3%82%AA%E3%83%BC%E3%83%90%E3%83%BC%E6%A9%9 F%E8%83%BD%E3%81%AB%E3%81%A4%E3%81%84%E3%81%A6)

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、「[2-3-1 システム設定](#)」項の「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。

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

### 3-1. 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>

### 3-2. IdP の設定

#### 3-2-1. 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 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。次項「[3-2-2. Microsoft Entra アプリケーションの作成・設定](#)」にて使用します。

## 3-2-2. Microsoft Entra アプリケーションの作成・設定

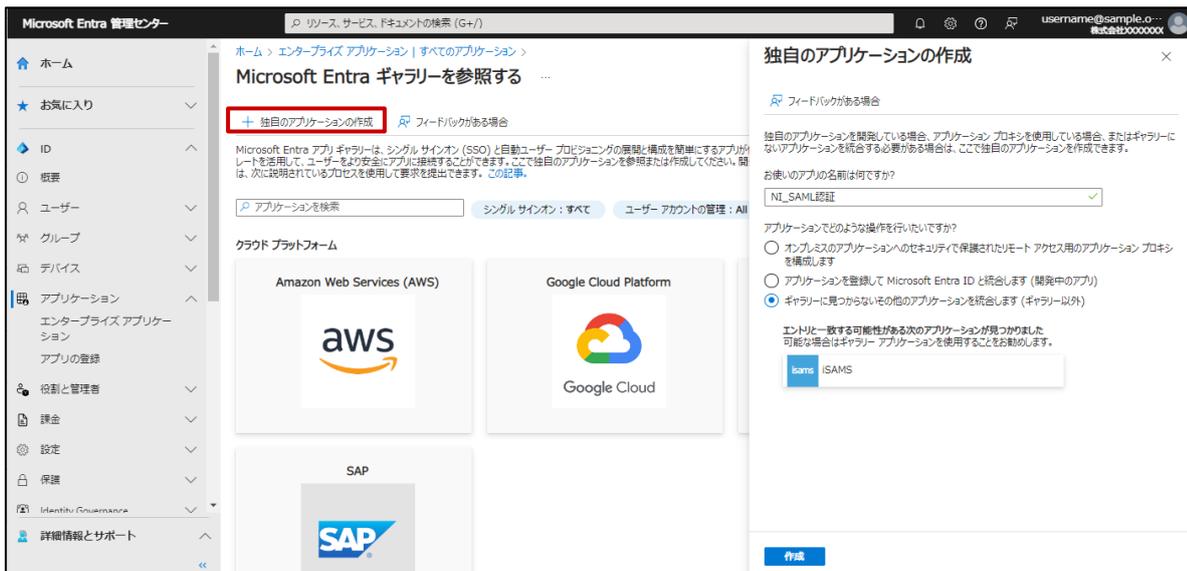
1. ブラウザにて下記 URL にアクセスし、Microsoft Entra 管理センターの画面を表示します。

<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. 「3-2-1. 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。

「[3-5-1. 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`

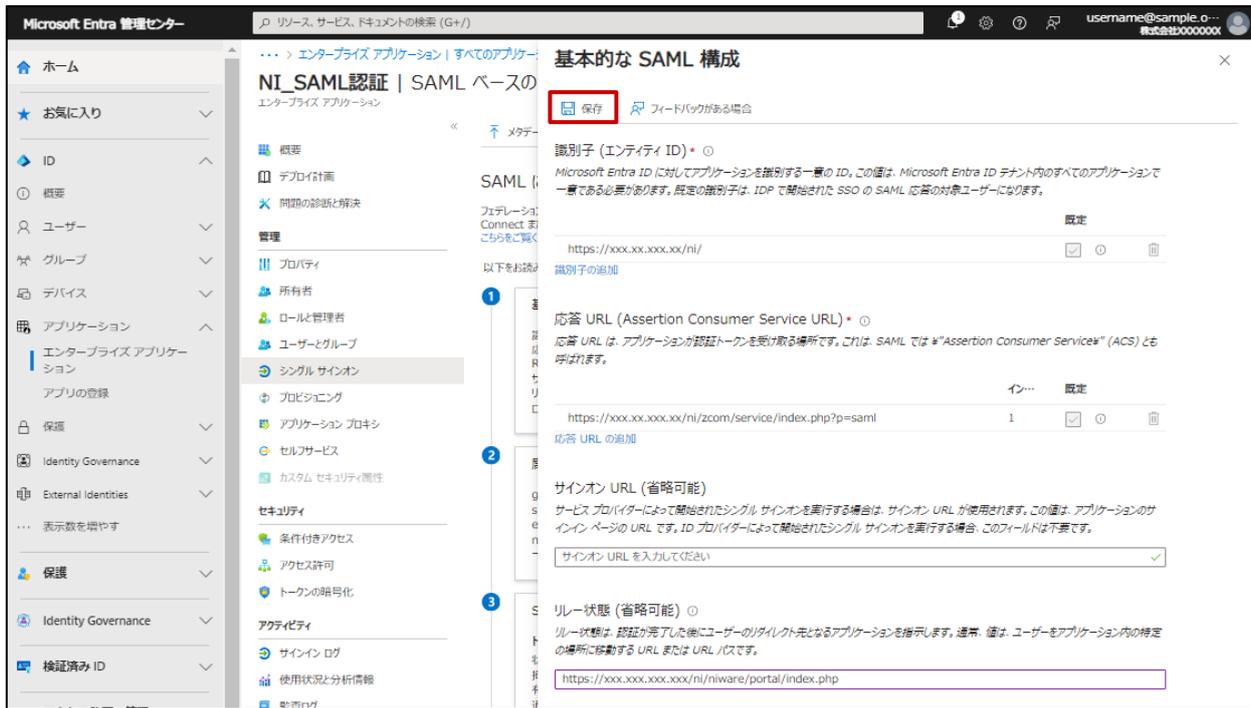
Sales Force Assistant シリーズを表示する場合 :

`https://xxx.xxx.xxx.xxx/ni/<各製品>/main/index.php`

The screenshot shows the Microsoft Entra Management Center interface. The left sidebar contains navigation options like 'ホーム', 'お気に入り', 'ID', '概要', 'ユーザー', 'グループ', 'デバイス', 'アプリケーション', '保護', 'Identity Governance', 'External Identities', '表示数を増やす', '保護', 'Identity Governance', and '検証済み ID'. The main content area is titled '基本的な SAML 構成' (Basic SAML Configuration) for 'NI\_SAML認証 | SAML ベースのエンタープライズ アプリケーション'. It includes a '識別子 (エンティティ ID)' field with the value 'https://xxx.xxx.xxx.xxx/ni/'. Below it is the '応答 URL (Assertion Consumer Service URL)' field with the value 'https://xxx.xxx.xxx.xxx/ni/zcom/service/index.php?p=saml'. The 'サインオン URL (省略可能)' field is set to 'サインオン URL を入力してください'. The 'リレー状態 (省略可能)' field is highlighted with a red box and contains the URL 'https://xxx.xxx.xxx.xxx/ni/niware/portal/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。

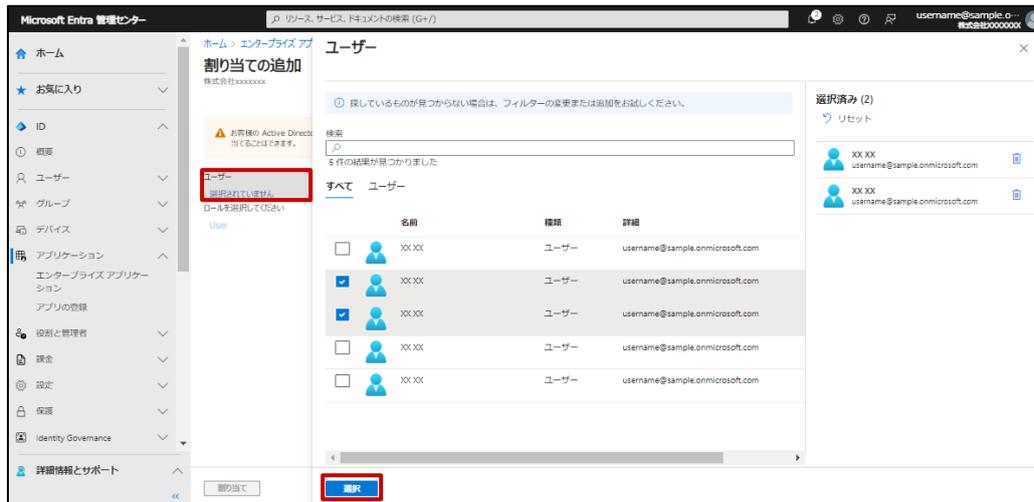


12. 「ユーザーとグループ」 を選択し、「ユーザーまたはグループの追加」 をクリックします。



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。

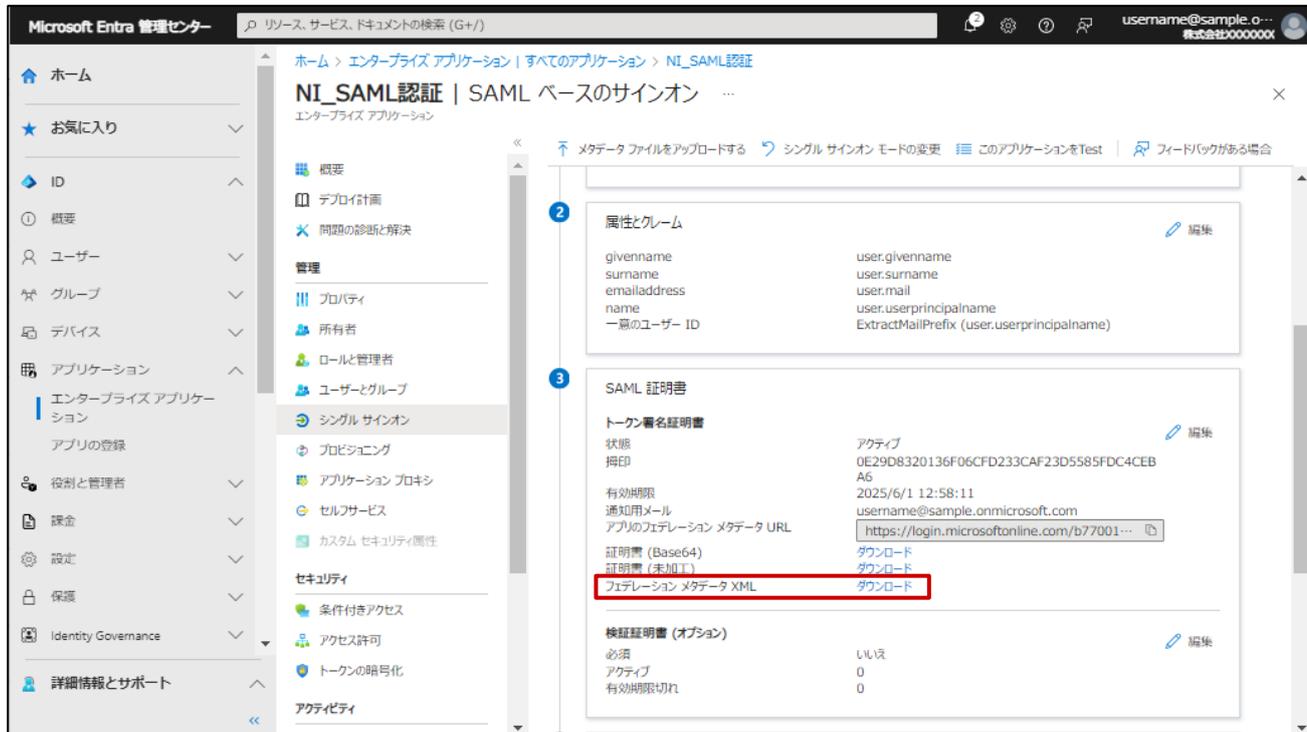
⇒アプリケーションのアクセス設定が変更されます。



## 3-3.NI 製品の設定

### 3-3-1. 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 の設定に必要な「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。



### 3-3-2.システム設定

1.システム設定の セキュリティ 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。 ※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。 ※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

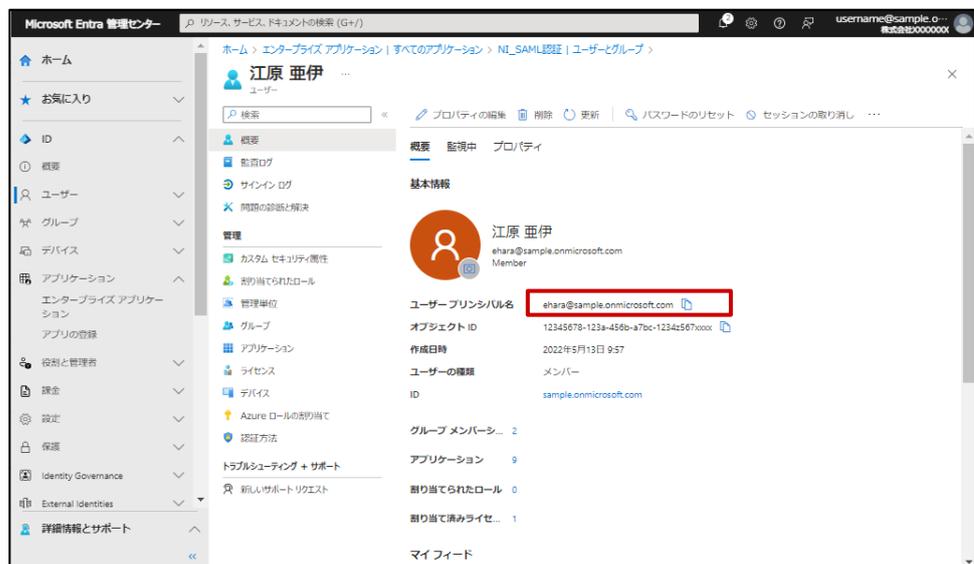
- ・ 社内端末の IP アドレスを「有効範囲」に指定することで、モバイル端末など社外からの接続により IdP に接続不可の場合は、「有効範囲」外となるため、SAML 認証が適用されず、通常のログイン画面が表示されます。

- 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。

メタデータ： ドラッグ&ドロップで貼り付けることができます。

FederationMetadata.xml

Identity Providerのメタデータをアップロードしてください。  
読み込むことができるファイルは、拡張子が「xml」のファイルです。  
XMLより設定値を抽出し、以下の項目を自動設定します。  
(エンティティID, エンドポイントURL, 証明書)

**読み込み**

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/xxxxx-xxx-xxxx-xxxx-xxxxxxxxxxx/
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-xxxx-xxxxxxxxxxx/saml2
証明書	Identity Provider が署名に使用する公開鍵を設定します。 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。

## 3-4. 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。

### 3-4-1. オプション設定

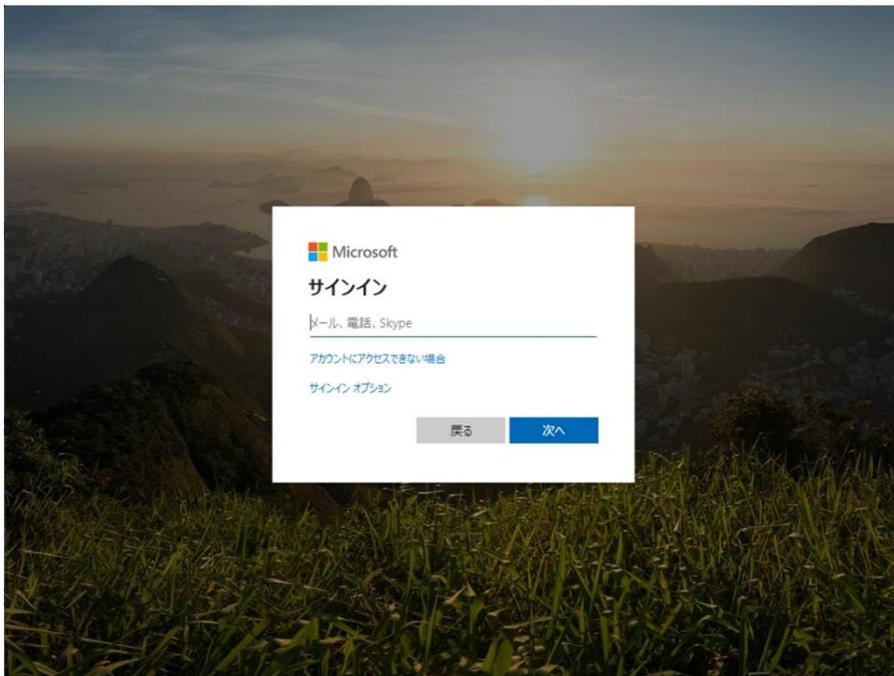
1. 仮名を利用する場合、初回ログイン時はシングルサインオンに失敗するため、通常の NI 製品ログイン画面より、ID/パスワードを入力し、ログインしてください。
2. NI 製品の「オプション設定」画面を表示し、「SAML 認証」を選択します。  
⇒ 「SAML 認証」画面が表示されます。
3.  ボタンをクリックして、Identity Provider から仮名 ID を取得します。  
※新規ウィンドウが開き、Identity Provider へ接続します。仮名 ID 取得後に Window は自動的に閉じられます。
4. 最後に  ボタンを押します。

## 3-5.動作確認

### 3-5-1.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。

## 3-6.トラブルシューティング

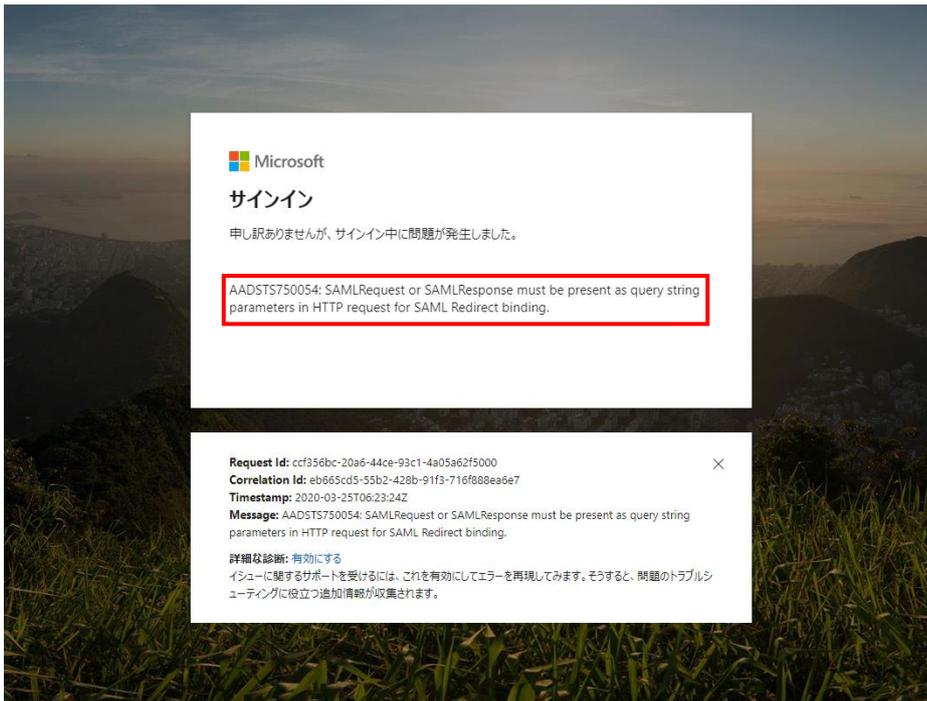


補足

- ・ 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、「[4.トラブルシューティング](#)」を参照してください。

### 3-6-1. 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>

### 3-6-2. 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。 NI 製品システム設定 > Service Provider(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」を指定した場合には表示されます。 「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は表示されます。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。

## 3-7.運用時の注意

### 3-7-1.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、「[3-3-2 システム設定](#)」項の「4. 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>

## 4.トラブルシューティング

### 4-1.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。

→[4-2.SAML 認証のログを確認する](#)

→[4-3.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。

→[4-4.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

## 4-2.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。 <a href="#">「4-3.SAML 認証エラーの原因を調べる」</a> 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。 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。 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。

### 4-3.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。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。 「 <a href="#">2-4-4.認証ポリシーの設定</a> 」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。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。 ※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。

## 4-4.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、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。

## 5.制限事項

### 5-1.技術的・運用的制限

- ・SSL(https)接続の利用が必須となります。  
「[1-2-2.SSL\(https\)での接続設定を行う](#)」項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](#)」項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。

### 5-2.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

○ 商標

本説明書に登場する会社名、製品名は各社の登録商標、商標です。

○ 免責

本説明書に掲載されている手順による操作の結果、ハード機器に万一障害などが発生しても、弊社では一切の責任を負いませんのであらかじめご了解ください。

○ 発行

2024年4月16日 第14版

株式会社 **NI**コンサルティング

サポートデスク

E-mail : [support@ni-consul.co.jp](mailto:support@ni-consul.co.jp) Fax : 082-511-2226

営業時間 : 月曜日～金曜日 9:00～12:00、13:00～17:00 (当社休業日、土・日・祝日を除く)