cybozu.com

Active Directory フェデレーションサービスとの認証連携

サイボウズ株式会社

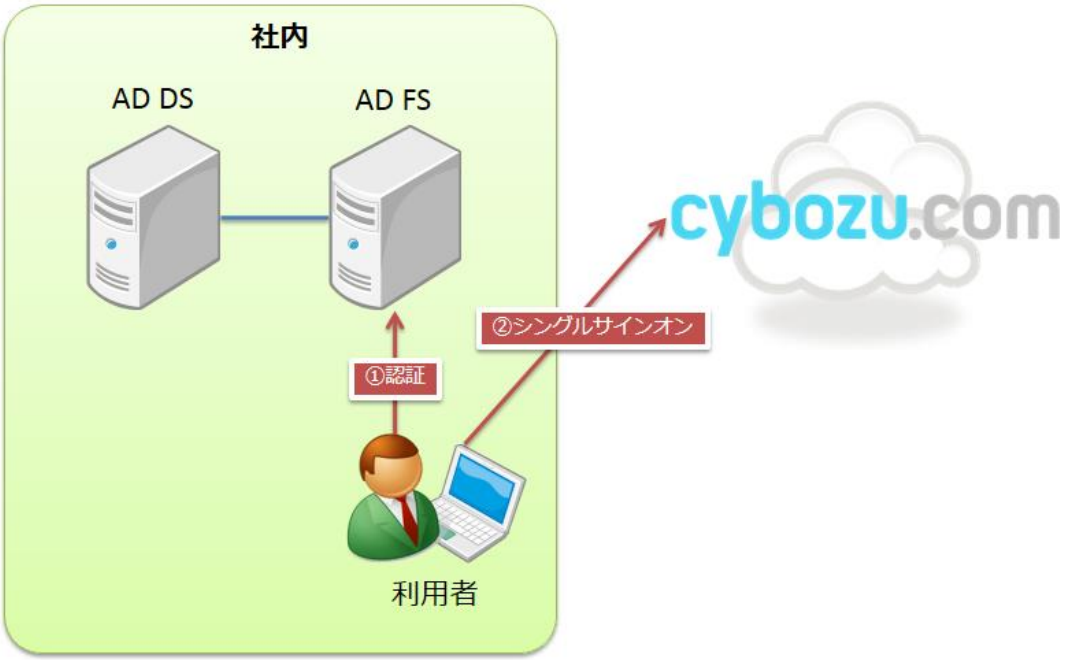
第 1 版

Cybozu

目次

1 はじめに

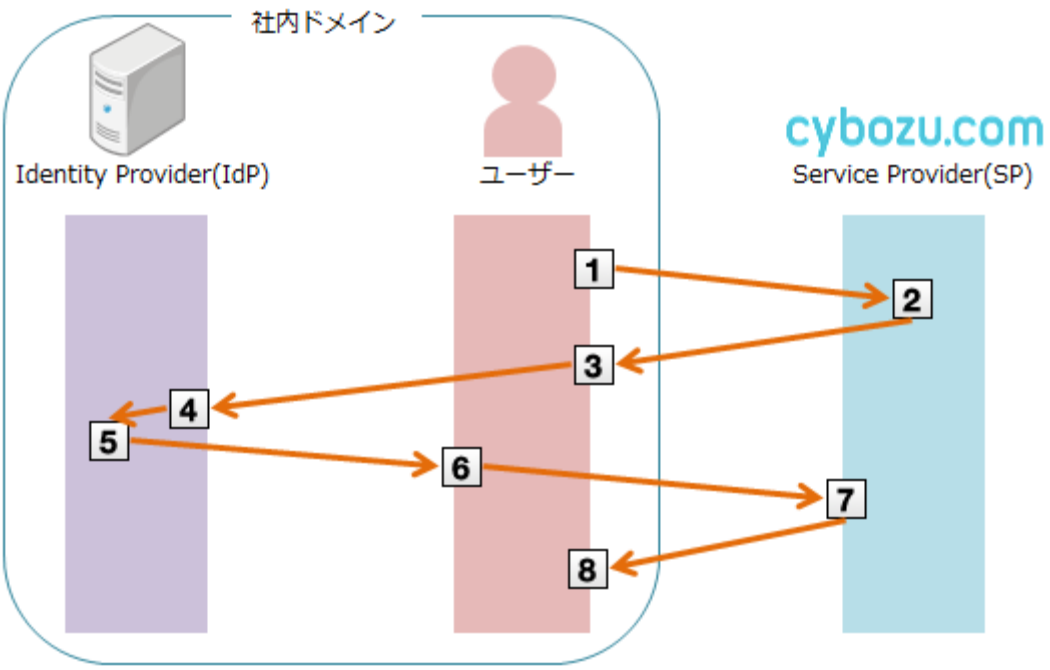
本書では Active Directory フェデレーション サービス 2.0 (以下、AD FS)を使って cybozu.com へシングルサインオンを行う手順を説明します。
AD FS との認証連携には SAML を利用します。



2 システム構成

- Active Directory Domain Services(以下、AD)と AD FS は、同一のサーバー上で稼働するものとします。

  ※ 検証のため同一サーバー構成としています。実際の運用における構成はマイクロソフト社の情報をご確認下さい。
- AD サーバーの OS は、Windows Server 2008 R2 Standard(SP1)とします。
- クライアント PC の OS は、Windows 7 Professional(SP1)、ブラウザは Internet Explorer 10 とします
- サーバー、クライアント PC の Windows ファイアウォールは無効化しています。
- SAML を使った連携の流れは以下の通りです。(AD FS が IdP に該当します)



1. ユーザーが cybozu.com にアクセスします。
2. cybozu.com が SAML リクエストを生成します。
3. ユーザーが、SP から SAML リクエストを受け取ります。
4. IdP がユーザーを認証します。
5. IdP が SAML レスポンスを生成します。
6. ユーザーが、IdP から SAML レスポンスを受け取ります。
7. cybozu.com が SAML レスポンスを受け取り、検証します。
8. SAML レスポンスの内容に問題がない場合は、ユーザーが cybozu.com にログインした状態になります。

3 事前準備

cybozu.com に環境が必要となります。
環境が無い場合は、「サイボウズドットコム ストア」から試用環境を申し込んで下さい。

サイボウズドットコム ストア
https://www.cybozu.com/jp/service/com/trial/
※「お試しになるサービス」は任意のサービスを選択して下さい

4 AD のセットアップ

手順は割愛します。マイクロソフト社の情報をご確認下さい。
本環境では、コンピュータ名を "adfs" と設定したサーバーに AD をインストールし、ドメイン名を example.local と設定しました。

5 AD FS のセットアップ

5.1 AD FS のインストール

cybozu.com との設定を行う前に、アイデンティティ・プロバイダ(IdP)となる AD FS 2.0 のインストールを行います。

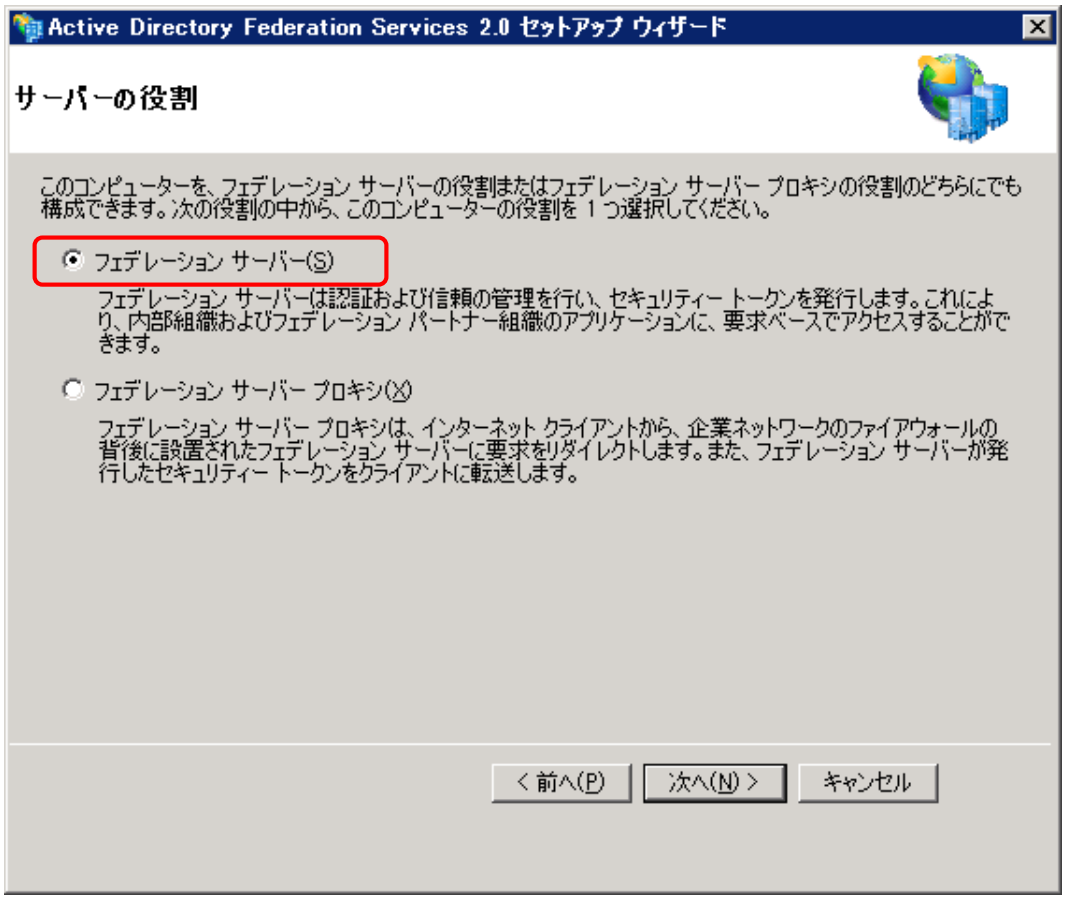
1. AD FS のインストールモジュールを以下のサイトよりダウンロードします。

   Active Directory Federation Services 2.0 RTW
   http://www.microsoft.com/ja-jp/download/details.aspx?id=10909

   ※ インストール先の OS ごとにアーカイブが分かれています。
   Windows Server 2008 R2 環境にインストールする場合は、
   「RTW¥W2K8R2¥amd64¥AdfsSetup.exe」をダウンロードします。

2. ダウンロードしたファイル(adfssetup.exe)を実行すると、「Active Directory Federation Services 2.0 セットアップ ウィザード」が開始されます。

3. ウィザードを進め、「サーバーの役割」で「フェデレーション サーバー」を選択します。そのままウィザードを進めればインストールが完了します。

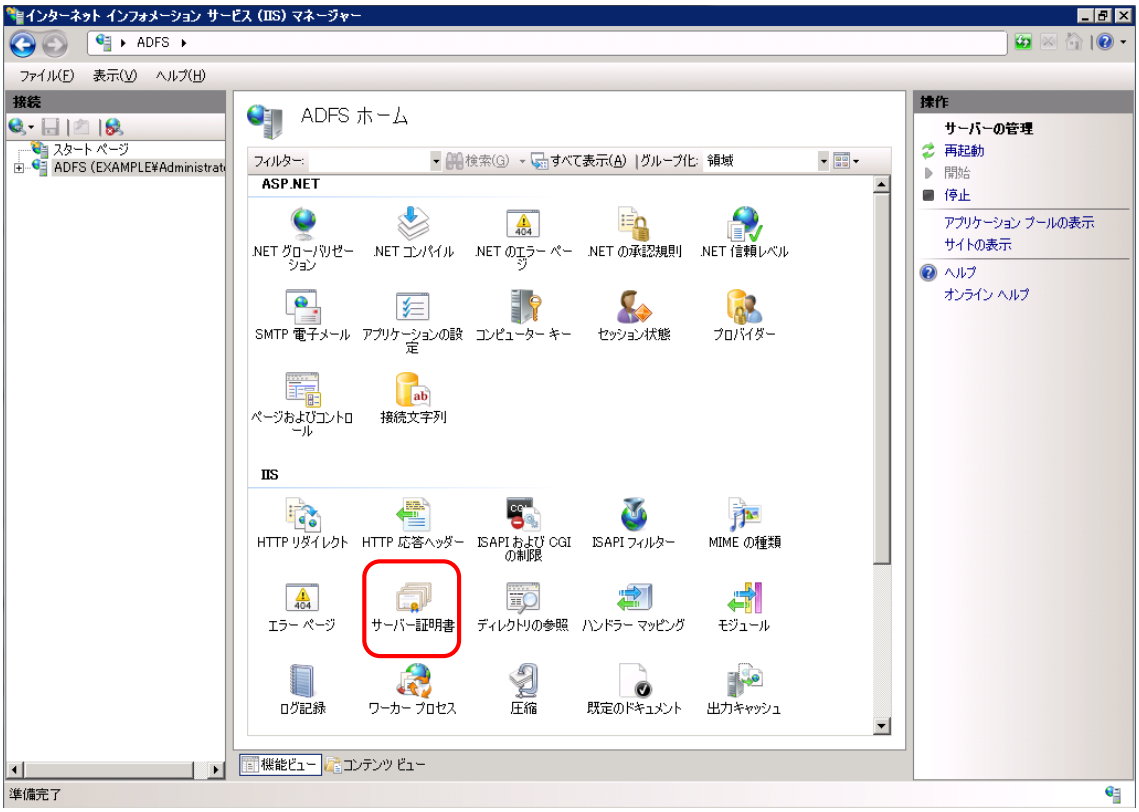


5.2 AD FS で必要となる証明書の作成

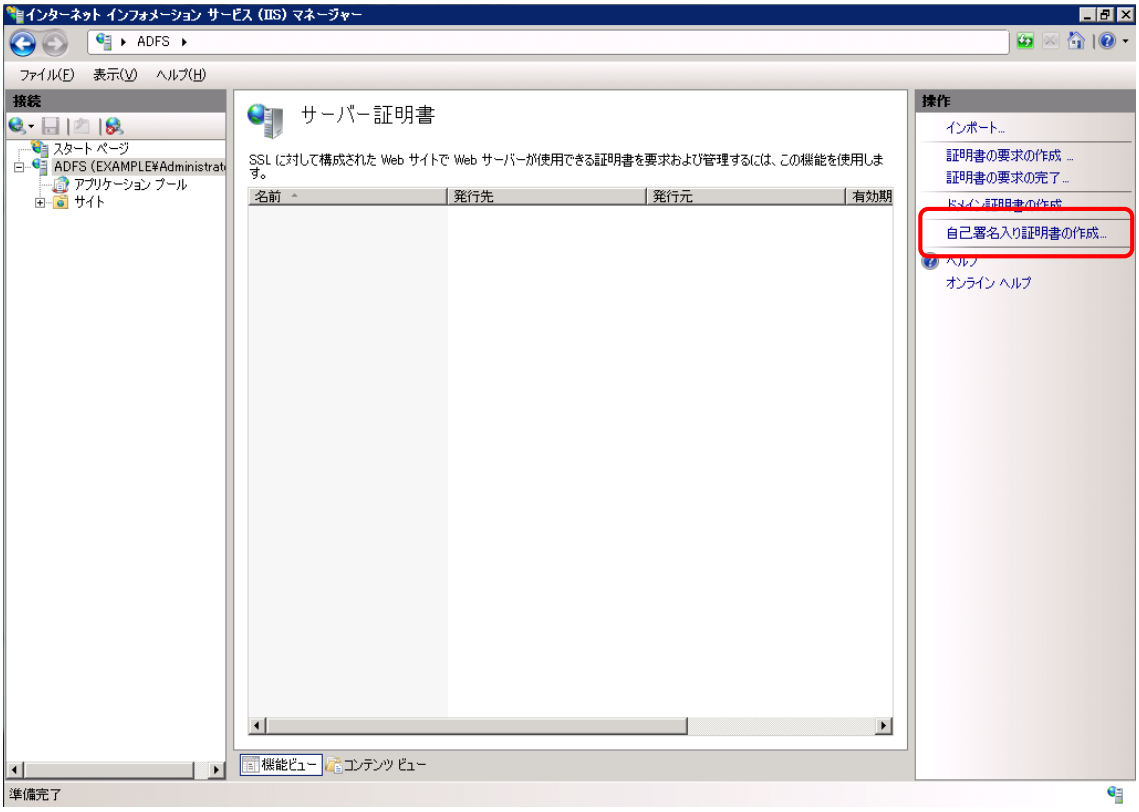
※ 本環境では IIS を使って自己署名証明書を作成します

1. 管理ツールから「インターネットインフォメーションサービス(IIS)マネージャー」を起動します。

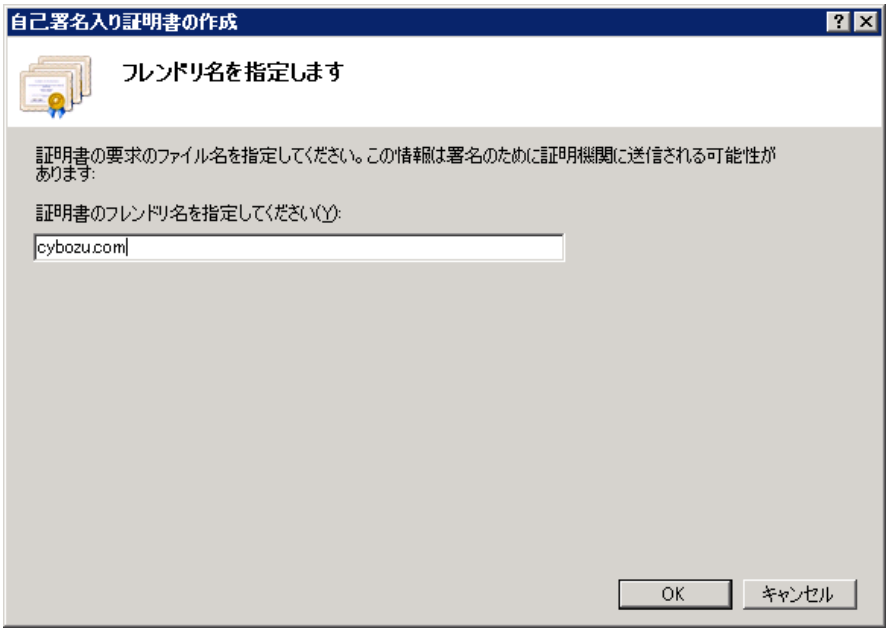
2. ホスト名を選択し、「サーバー証明書」をダブルクリックします。



3. 中央のペインに「サーバー証明書」が表示されたら、右ペインの操作ウィンドウから「自己署名入り証明書の作成」をクリックします。

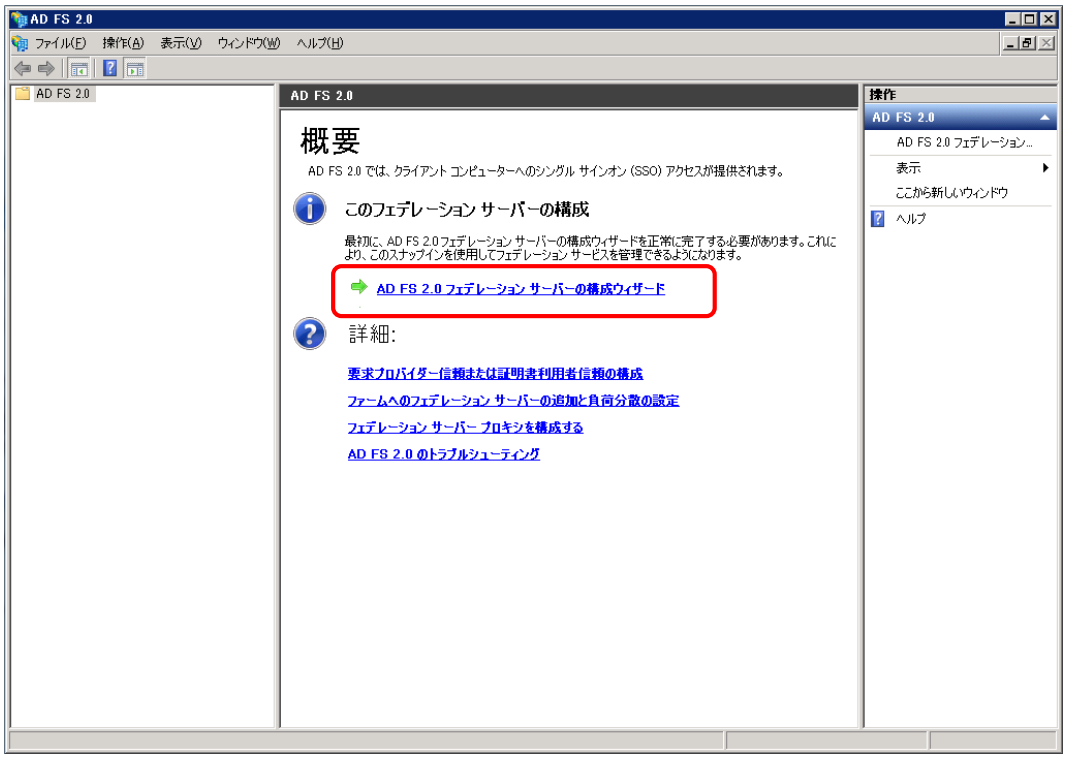


4. 「自己署名入り証明書の作成」ダイアログが表示されますので、証明書のフレンドリ名を入力します。フレンドリ名は証明書を識別するために使うため、任意の情報で構いません。

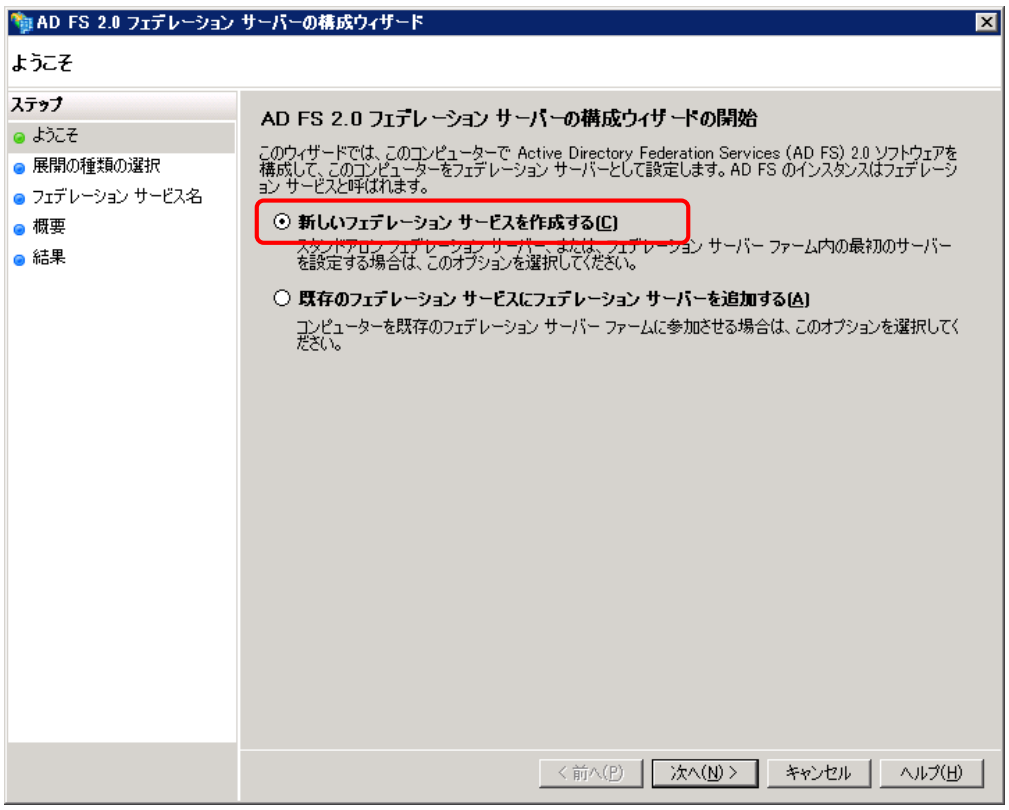


5.3 フェデレーションサーバーの構成

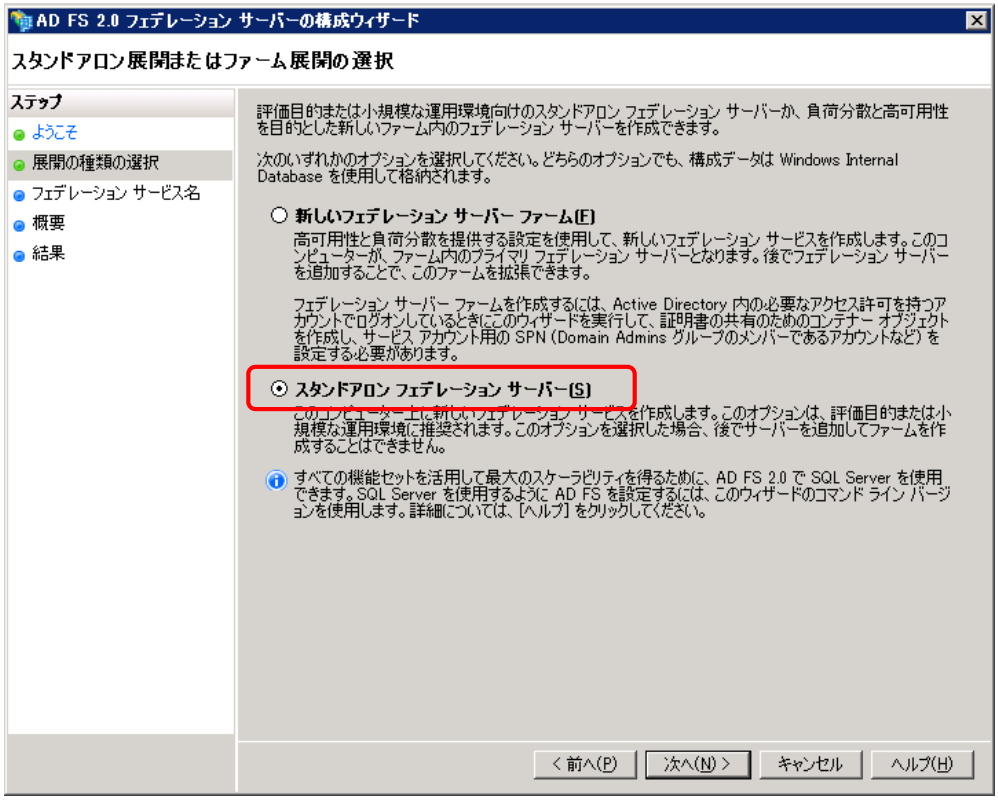
1. 管理ツールから「AD FS 2.0 の管理」を起動します。
中央のペインの「AD FS 2.0 フェデレーション サーバーの構成ウィザード」をクリックすると、「AD FS 2.0 フェデレーション サーバーの構成ウィザード」が開始されます。



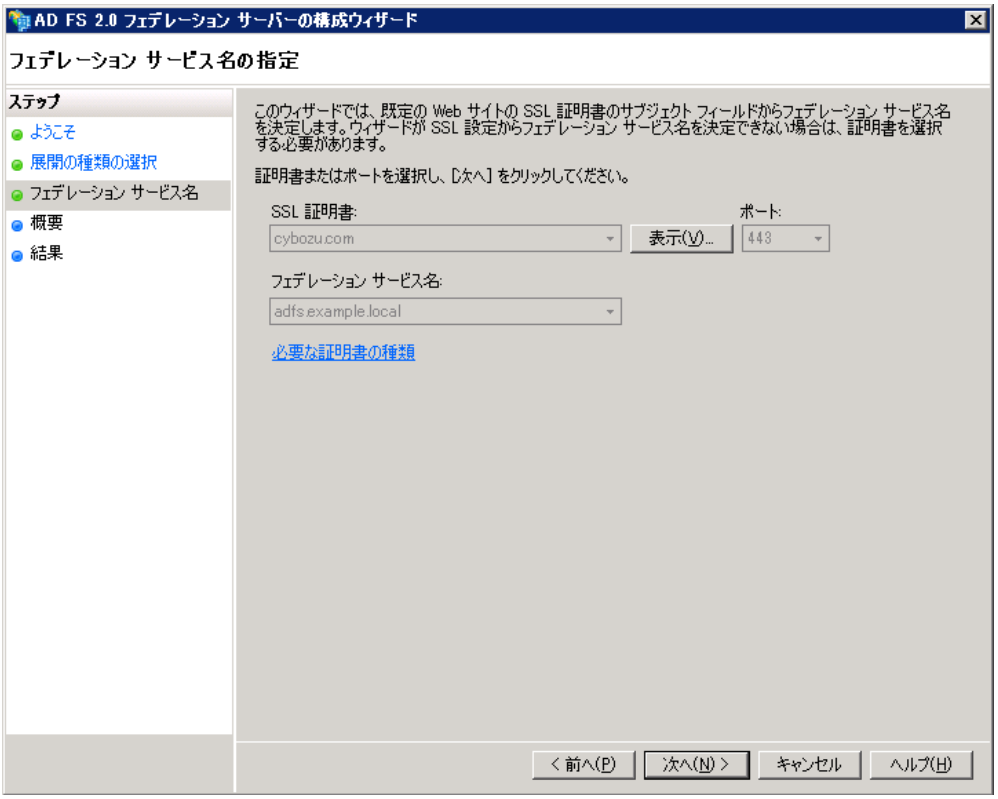
2. 最初にフェデレーション サービスの構成を選択します。「新しいフェデレーション サービスを作成する」を選択し、「次へ」をクリックします。



3. 「スタンドアロン フェデレーションサーバー」を選択し、「次へ」をクリックします。



4. 事前の手順で作成した SSL 証明書が選択されている事を確認し、「次へ」をクリックします。そのままウィザードを進めればインストールが完了します。



5.4 cybozu.com と AD FS 2.0 の認証連携の設定

Service Provider メタデータのダウンロード

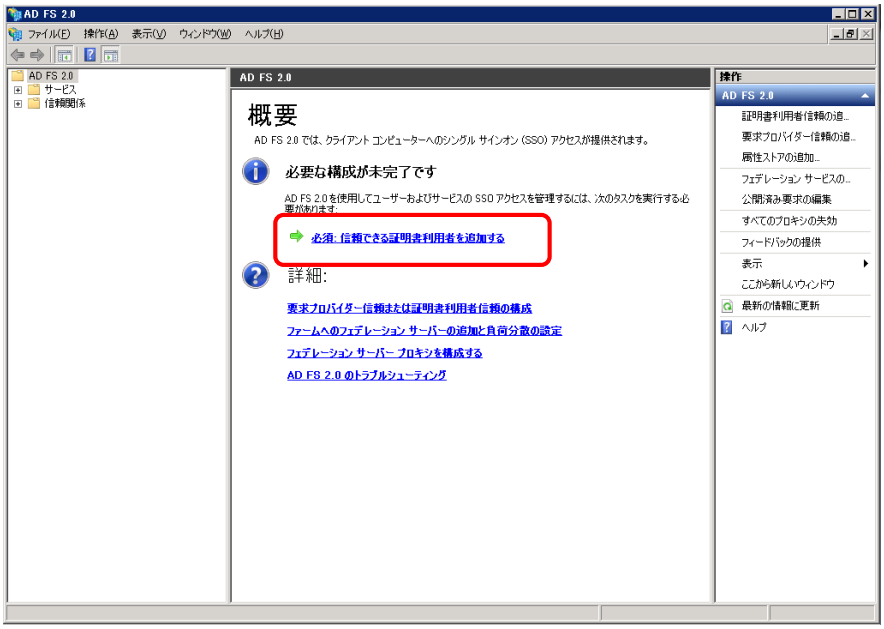
1. cybozu.com 共通管理に cybozu.com 共通管理者でログインします。
2. 「システム管理 > セキュリティ > ログイン」画面に移動し、「SAML 認証を有効にする」にチェックを入れます。

3. 「Service Provider メタデータのダウンロード」をクリックし、spmetadata.xml を保存します。

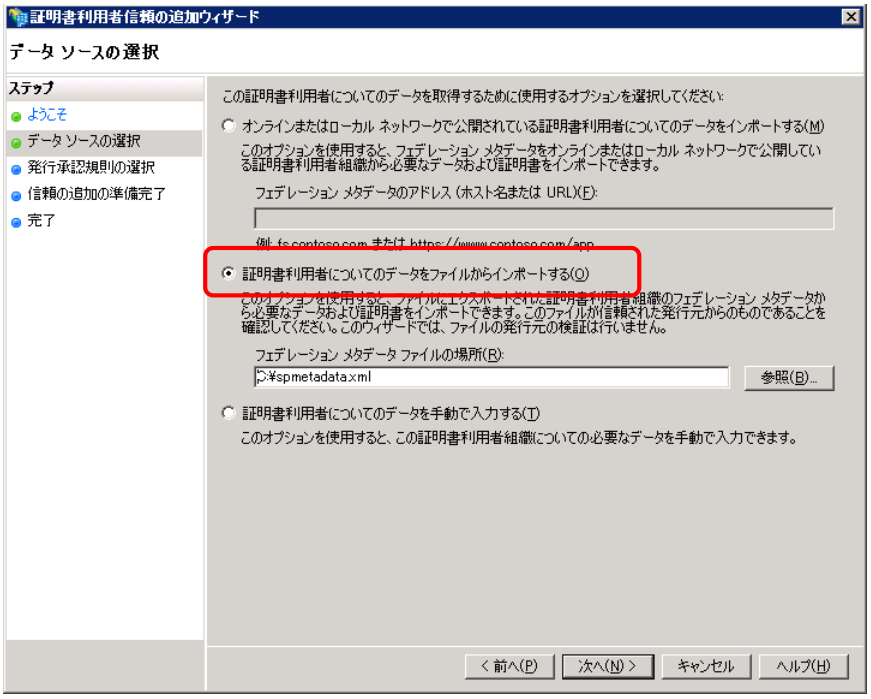
AD FS の設定

※　認証要求元として cybozu.com を信頼する設定を行います

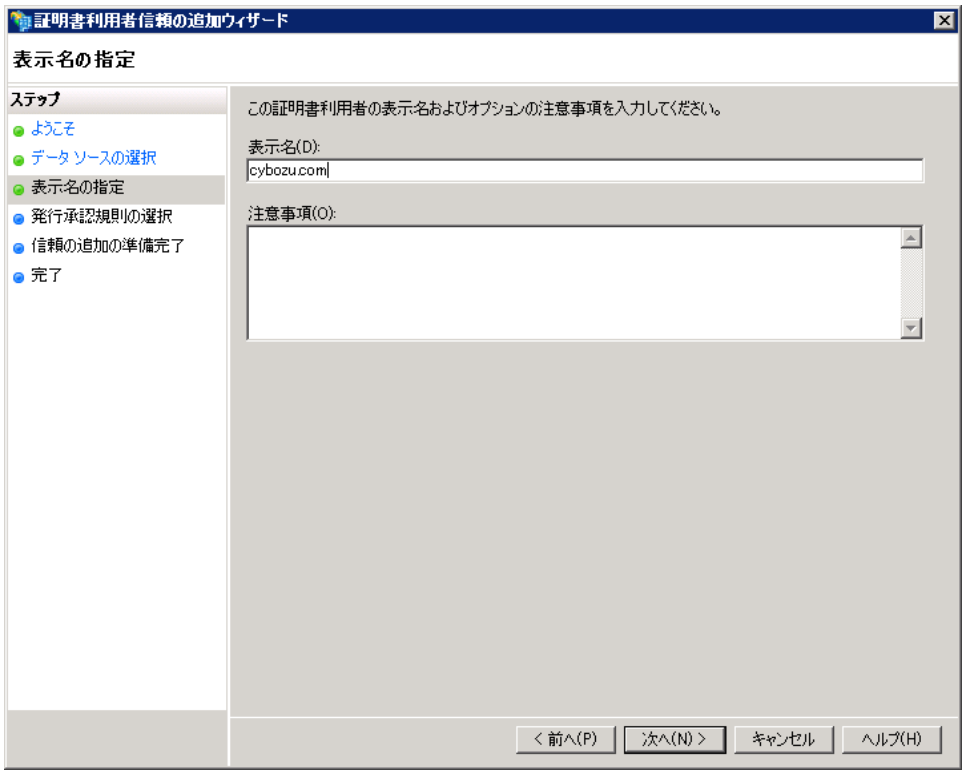
1. 管理ツールから「AD FS 2.0の管理」を起動します。
   中央のペインの「必須：信頼出来る証明書利用者を追加する」をクリックすると、「証明書利用者信頼の追加ウィザード」が開始されます。



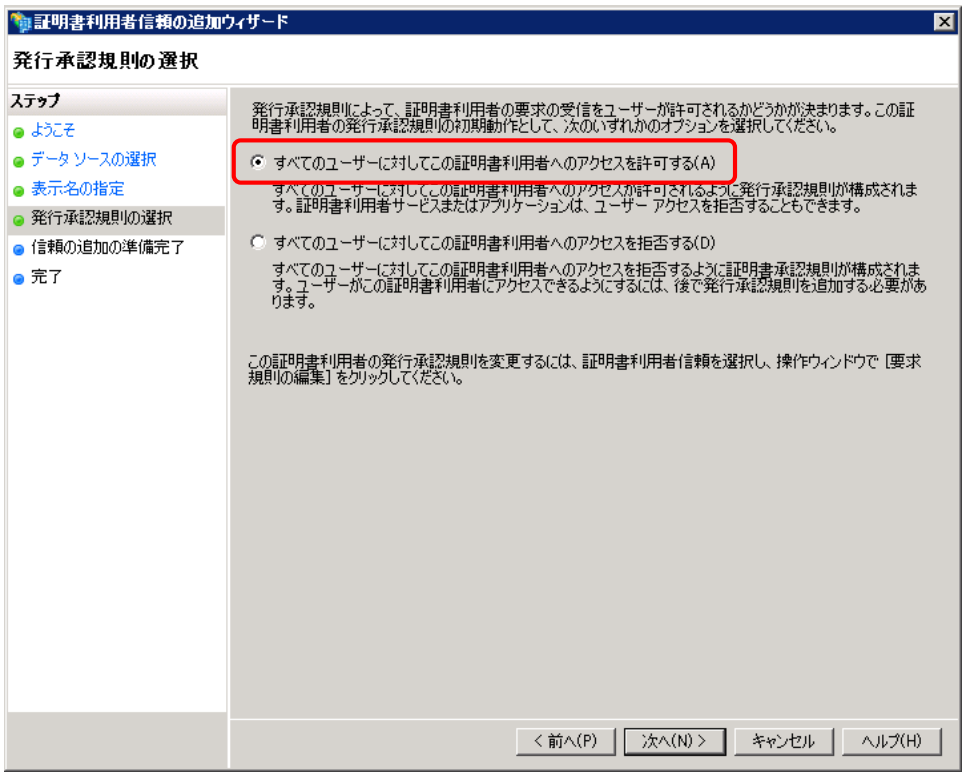
2. 「データソースの選択」で「証明書利用者についてのデータをファイルからインポートする」を選択し、前の手順でダウンロードした spmetadata.xml を指定し、「次へ」をクリックます。



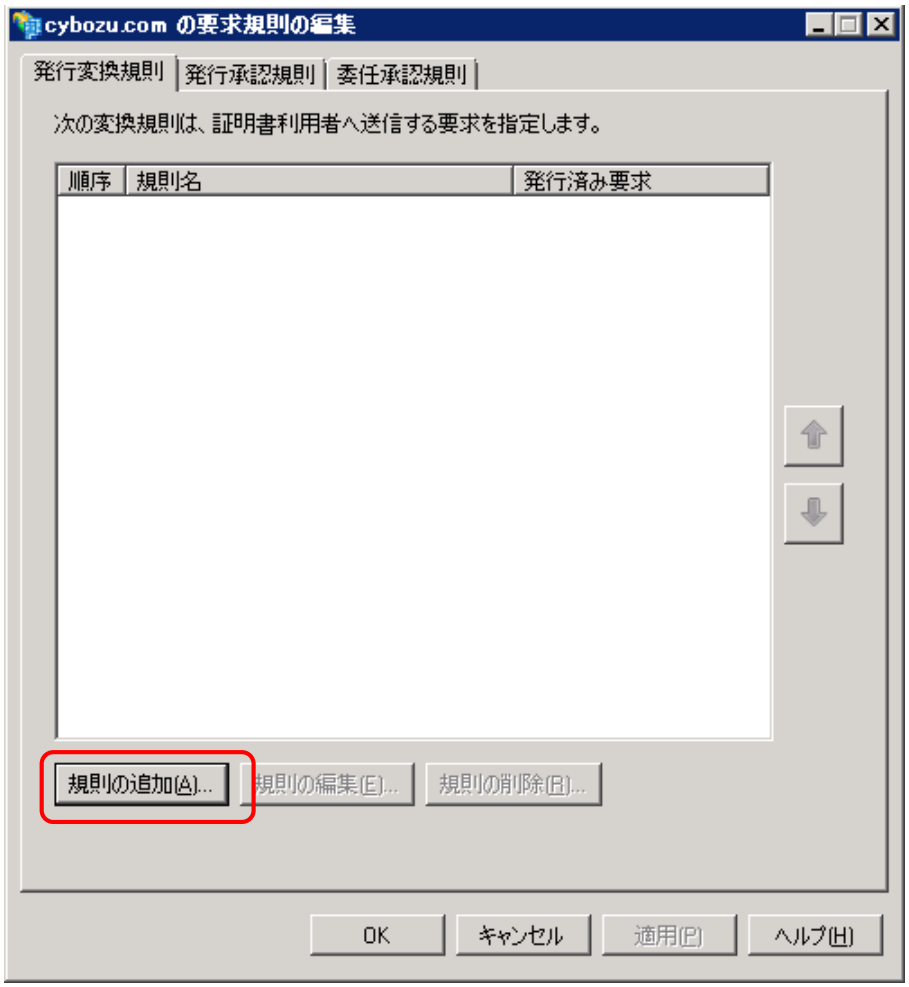
3. 「表示名の指定」で「表示名」を入力し、「次へ」をクリックします。
表示名は設定を識別するために使うため、任意の情報で構いません。



4. 「発行承認規則の選択」で「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。
そのままウィザードを進めれば設定が完了します。

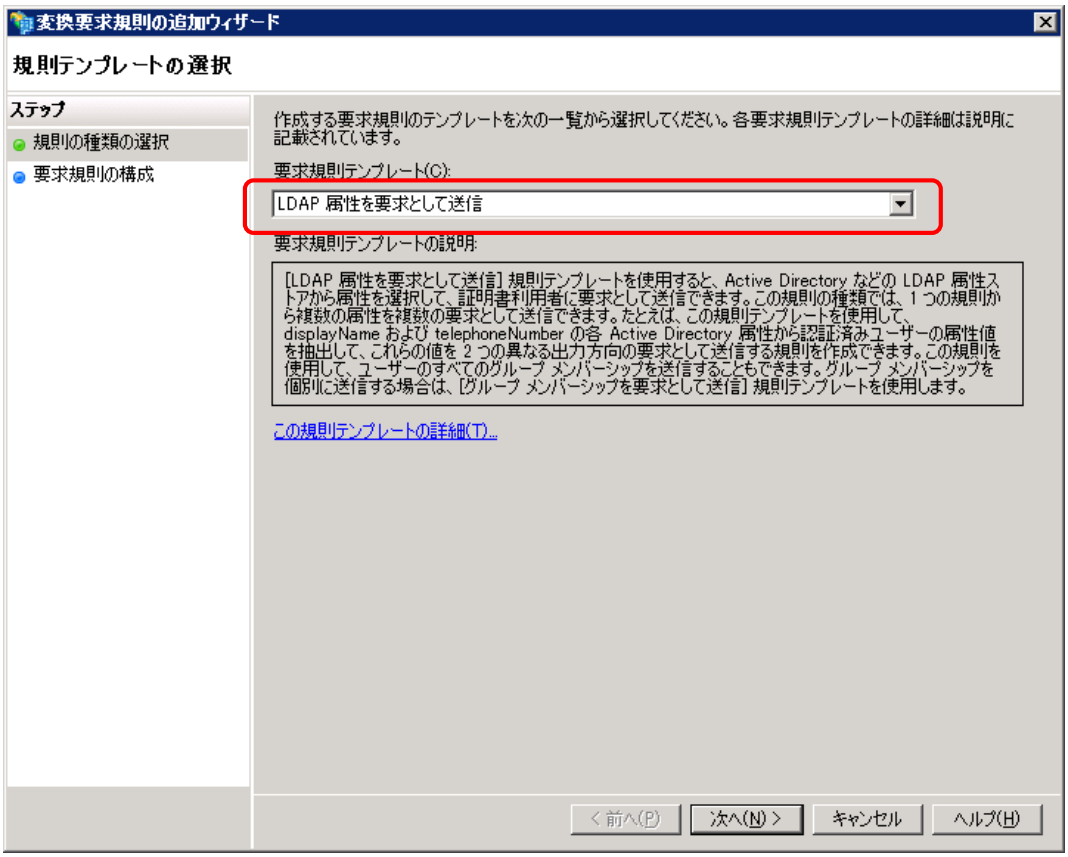


5. 「<表示名>の要求規則の編集」ダイアログが起動したら、「発行変換規則」タブを選択し、「規則の追加」をクリックします。



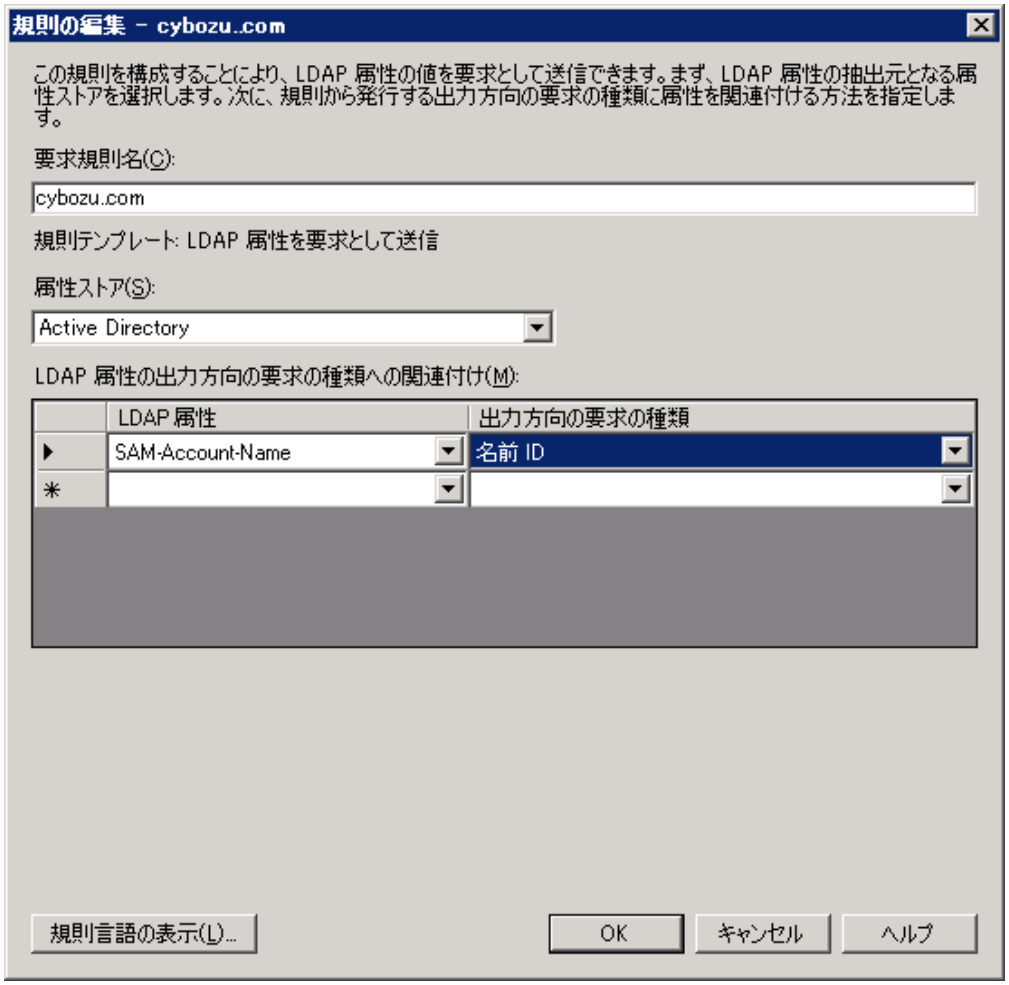
※ ダイアログが起動しなかった場合は、「AD FS 2.0の管理」の左ペインから「信頼関係 > 証明書利用者信頼」を選択し、右ペインから「証明書利用者信頼の追加」を選択します。

6. 「規則の種類の選択」で「要求規則テンプレート」が「LDAP属性を要求として送信」を選択し、「次へ」をクリックします。

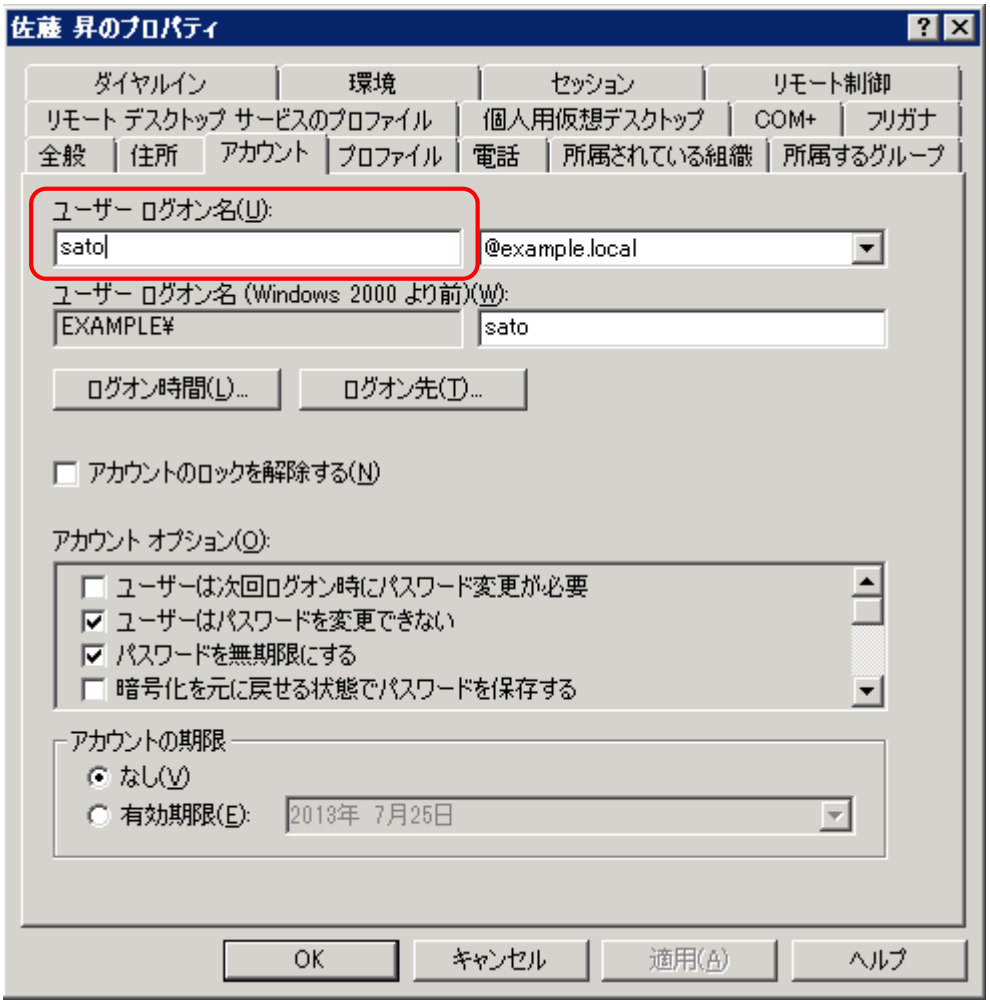


7. 「要求規則の構成」で以下のように設定し、「完了」をクリックします。

設定項目	設定内容
要求規則名	任意の文字列を入力
属性ストア	Active Directory
LDAP属性	SAM-Account-Name
出力方向の要求の種類	名前 ID



※　上記の設定の場合、Active Directory に作成されたユーザーの「ユーザー ログオン名」が cybozu.com に作成されたユーザーの「ログイン名」と一致する事で認証の連携が行われます。

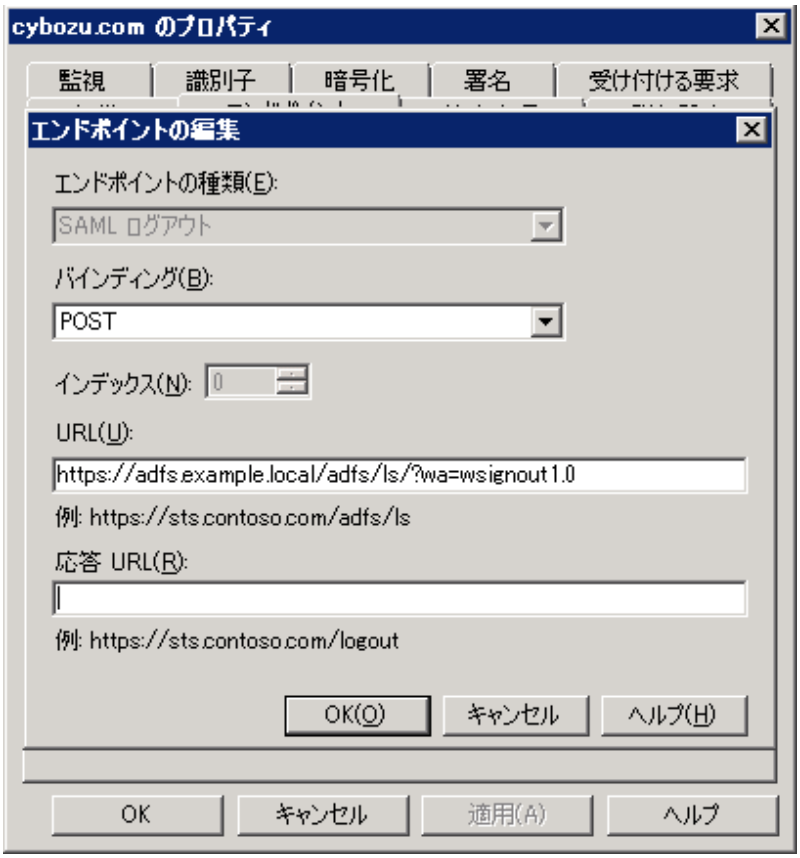


8. ログアウト用のエンドポイントを作成するため、「AD FS 2.0の管理」の左ペインから「信頼関係 > 証明書利用者信頼」を選択し、作成した証明書利用者信頼の設定をダブルクリックします。

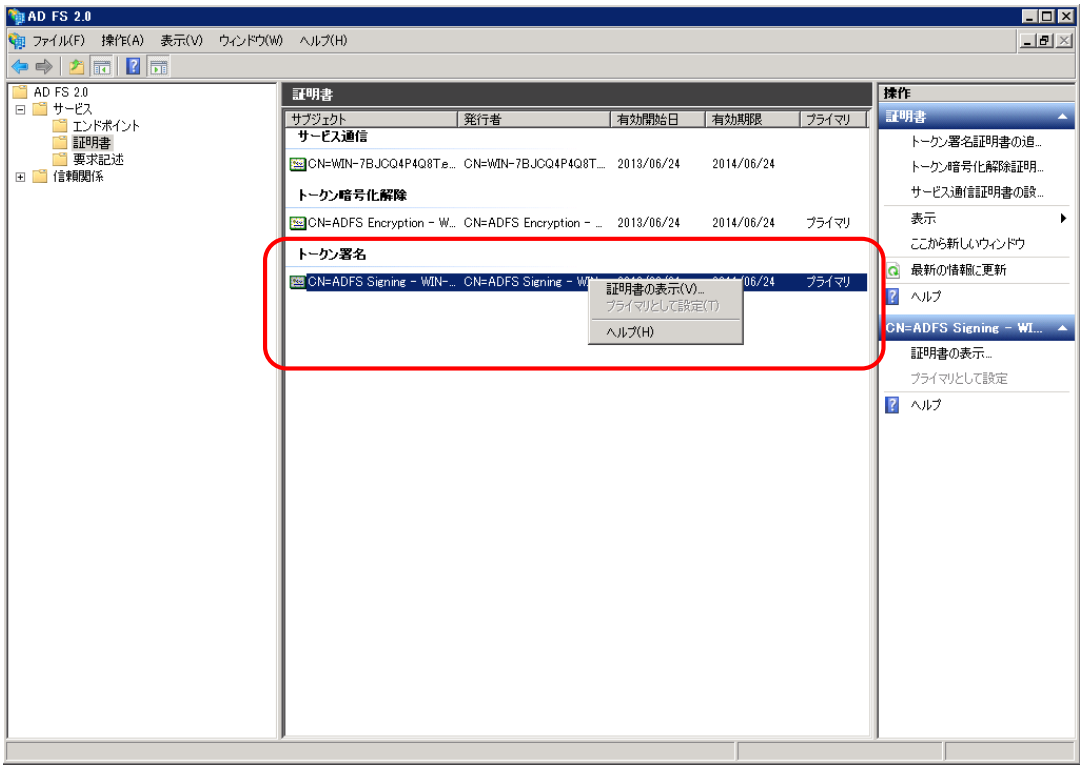
9. 「エンドポイント」タブをクリックし、「追加」をクリックします。

10. 「エンドポイントの追加」で以下のように設定し、「完了」をクリックします。

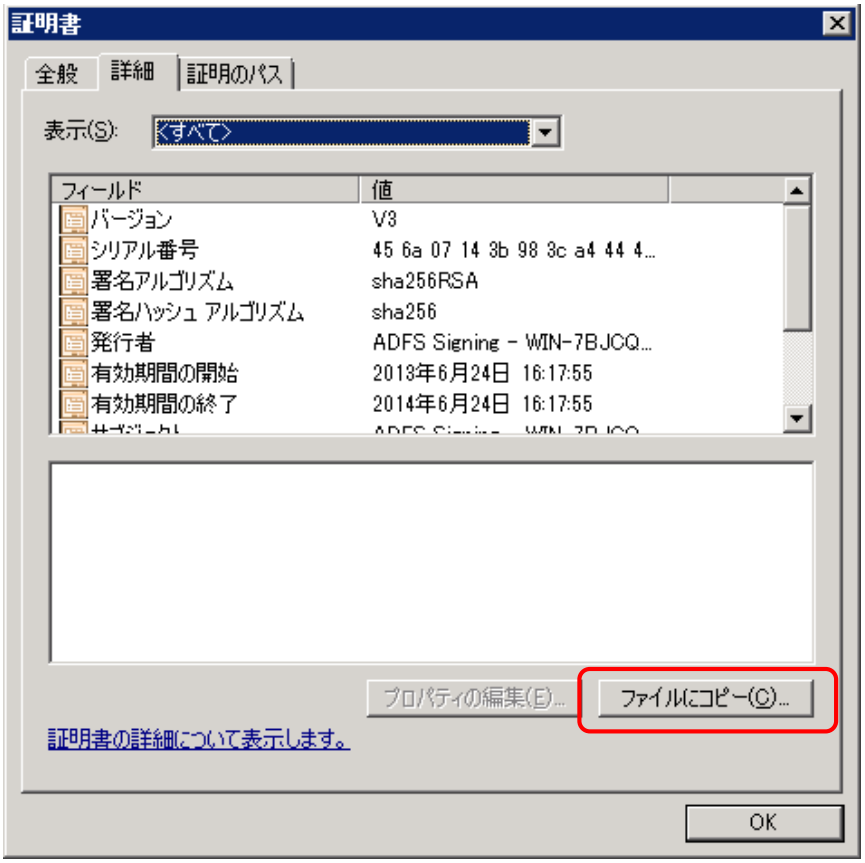
設定項目	設定内容
エンドポイントの種類	SAML ログアウト
バインディング	POST
URL	https://AD FSサーバーのアドレス /adfs/ls/?wa=wsignout1.0
応答 URL	空白



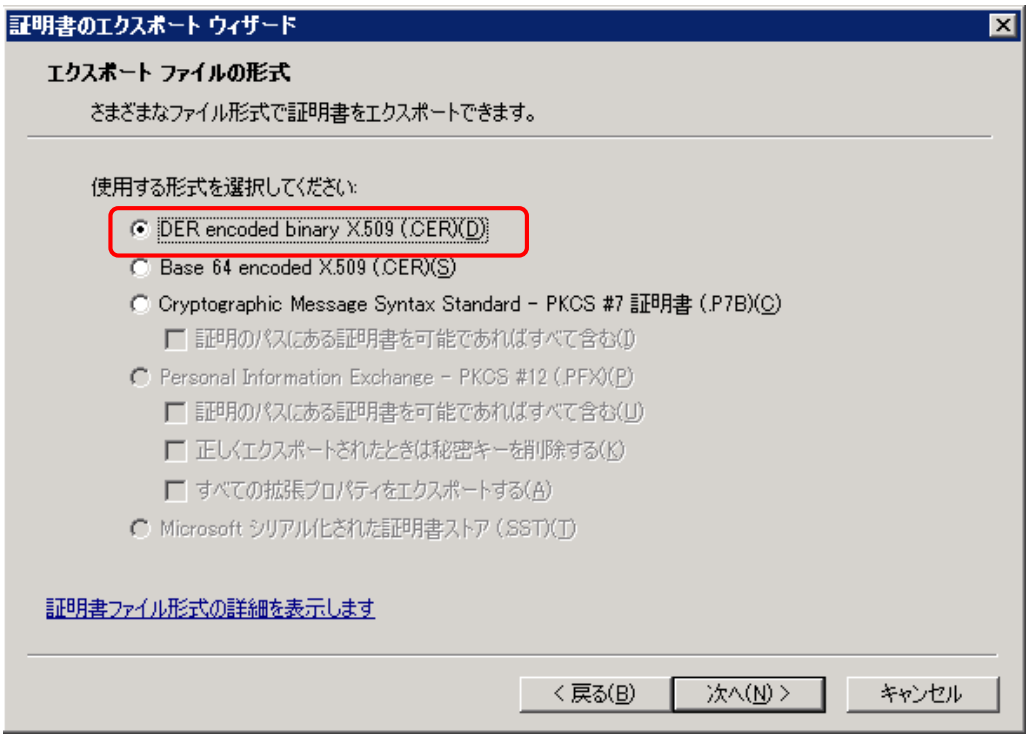
11. 「AD FS 2.0の管理」の左ペインから「サービス > 証明書」を選択し、中央ペインからトークン署名の証明書を右クリックし「証明書の表示」を選択します。



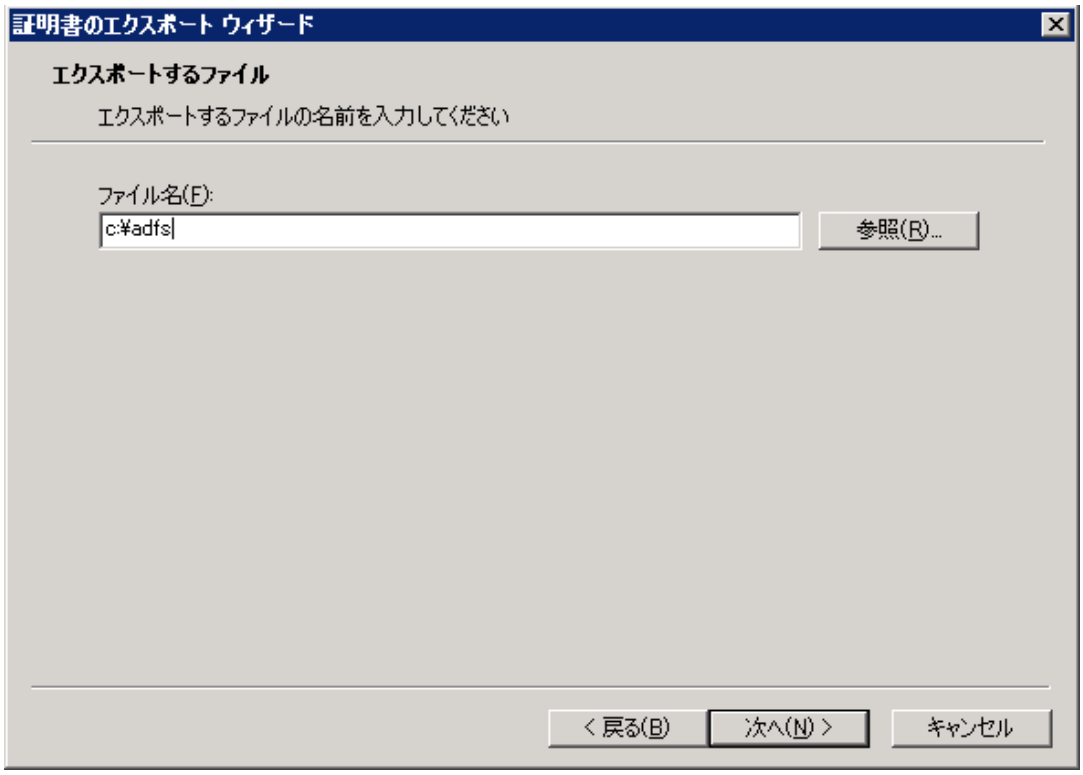
12. 「証明書」ダイアログで「詳細」タブを開き、「ファイルにコピー」をクリックすると、「証明書のエクスポートウィザード」ダイアログが起動します。



13. 「エクスポート ファイルの形式」で「DER encoded binary X.509 (.CER)」を選択し、「次へ」をクリックします。



14. 「エクスポートするファイル」に任意のファイルパスを入力し、「次へ」をクリックします。(拡張子は自動で付与されます)



15. 「証明書のエクスポートウィザードの完了」で「完了」をクリックすると、指定したフォルダに証明書が保存されます。

cybozu.com の設定

1. cybozu.com 共通管理に cybozu.com共通管理者でログインします。
2. 「システム管理 > セキュリティ > ログイン」画面に移動し、「SAML認証を有効にする」にチェックを入れます。
3. 以下のように設定し、「保存」をクリックします。

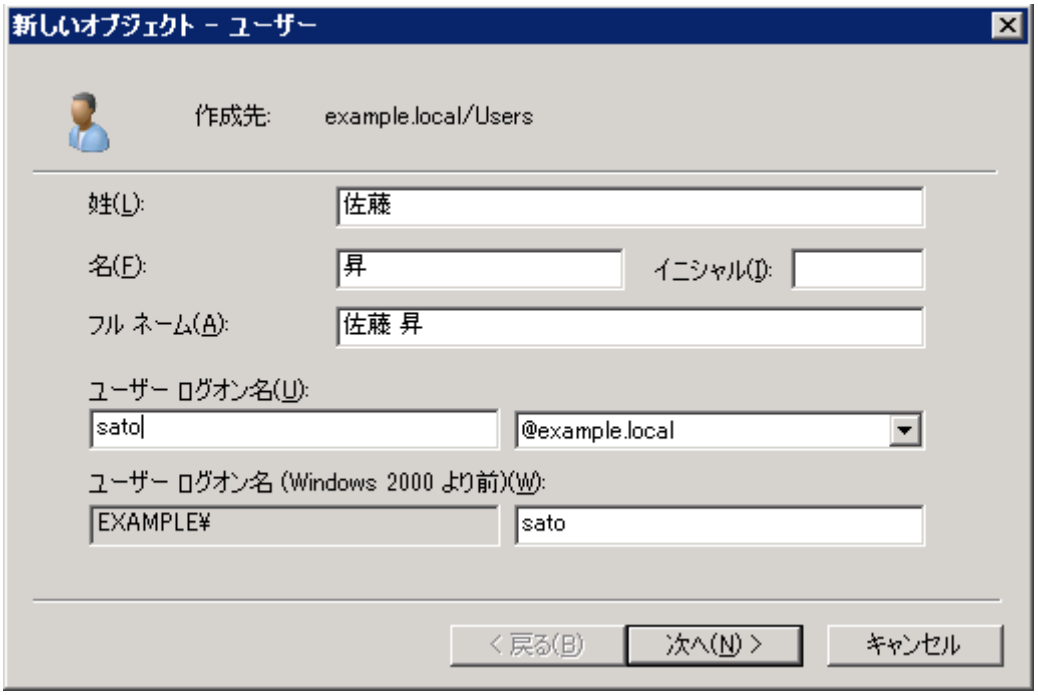
設定項目	設定内容
エンドポイントの種類	SAML ログアウト
Identity ProviderのSSOエンドポイントURL（HTTP-Redirect）	https://AD FSサーバーのFQDN/adfs/ls
cybozu.com からのログアウト後に遷移する URL	https://AD FSサーバーのアドレス/adfs/ls/?wa=wsignout1.0
Identity Providerが署名に使用する公開鍵の証明書	前の手順でエクスポートした証明書

5.5 ユーザーアカウントの作成

※ Active Directory と cybozu.com にユーザーアカウントを作成します。

Active Directory にユーザーを作成する

1. 管理ツールから「Active Directory」を起動します。
2. 任意のグループや OU を右クリックし、新規作成 > ユーザー をクリックします。
3. 必要な情報を入力します。ユーザーログオン名には cybozu.com で登録予定のログイン名と同じ情報を入力します。



cybozu.com にユーザーを作成する

1. 以下の手順に従い、ユーザーを追加します。

   ユーザーを追加する / cybozu.com ヘルプ
   https://help.cybozu.com/ja/general/admin/add_user.html
   ※ ログイン名は Active Directory に追加したユーザーのログオン名と一致させます

6. クライアント PC の設定

1. Internet Explorer を起動します。
2. [ツール] > [インターネット オプション] > [セキュリティ]に移動します。
3. 「インターネット」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。
4. 「ユーザー認証」 > 「ログオン」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、「OK」ボタンをクリックします。
5. Internet Explorer を終了します。

7. cybozu.com へのアクセス

1. クライアント PC で Active Directory にログインします。
2. Internet Explorer を起動し、cybozu.com にアクセスします。

3. シングルサインオンが行われ、cybozu.com へログインされます。

※ cybozu.com からログアウトした時は以下の画面が表示されます。

※ cybozu.com にアクセスした際、以下のエラーメッセージが表示される場合があります。
自己署名の証明書を利用している事が原因で、「このサイトの閲覧を続行する（推奨されません)。」をクリックする事でシングルサインオンが可能です。
エラーを表示させないようにしたい場合は、クライアント PC に証明書をインストールして下さい。