

# IBLook サービス フェデレーション設定ガイド

第六版 2024 年 4 月 17 日

株式会社 ビービーシステム

*Copyright (c) 2018-2024, Big Bang System Corporation. All rights reserved.*

本書に記載された事項で発生したいかなる事態もその責務を負いません。また、本書は作成日時点での情報をもとに記述しています。(株)ビービーシステムは予告なく本書の内容を変更する事があります。

その他、本書に記載されているサービス名、製品名または会社名は、各社の商標または登録商標です。本書では TM マーク、R マークは明記していません。

## 目次

はじめに.....	1
1. ADFS サーバーでの設定手順.....	2
【ご注意】 .....	12
2. Microsoft Azure ポータルでの設定手順.....	13
2.1 アプリの新規作成 .....	13
2.2 API のアクセス許可 設定.....	16
3. HENNGE One での設定手順 .....	18
4. リダイレクト URL の設定変更手順 .....	23
4.1 ADFS サーバーでの設定変更手順 .....	23
4.2 Microsoft Azure ポータルでの設定手順 .....	26
4.3 HENNGE One での設定手順.....	28
4.4 製品管理サイトの設定変更手順.....	30

## はじめに

本ガイドでは、フェデレーション認証を利用する際の、ADFS サーバー、Microsoft Azure ポータルまたは HENNGE One での設定手順について説明します。

※本ガイド中の画面は作成時点のものです。

## 1. ADFS サーバーでの設定手順

本章では、ADFS サーバーでの設定手順を説明します。

ADFS サーバーでの設定後、弊社サーバー側の設定が必要となりますので、インターネットからアクセス可能な ADFS サーバー名を Online サービス事務局<online-info@bbsystem.co.jp>までご提供ください。

※ADFS サーバーにインターネットからアクセスできない環境の場合は、フェデレーションメタデータ「FederationMetadata.xml」をファイルに保存してご提供ください。ただしファイルを使用して設定する場合、ADFS サーバーのトークン署名証明書更新時についても、弊社サーバー側の設定が必要となります。証明書の更新に併せて弊社サーバー側の設定をしないと ADFS 認証を利用できなくなりますので、証明書を更新前にご連絡ください。

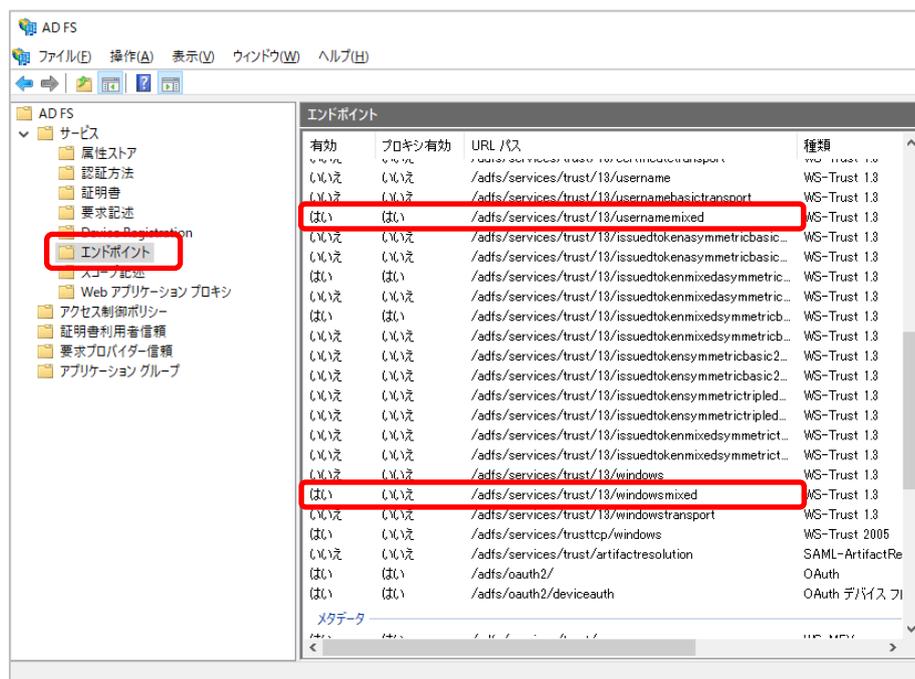
※「FederationMetadata.xml」の URL は次の通りです。

<https://<AD FS サーバー名>/FederationMetadata/2007-06/FederationMetadata.xml>

【例】

<https://adfs.example.com/FederationMetadata/2007-06/FederationMetadata.xml>

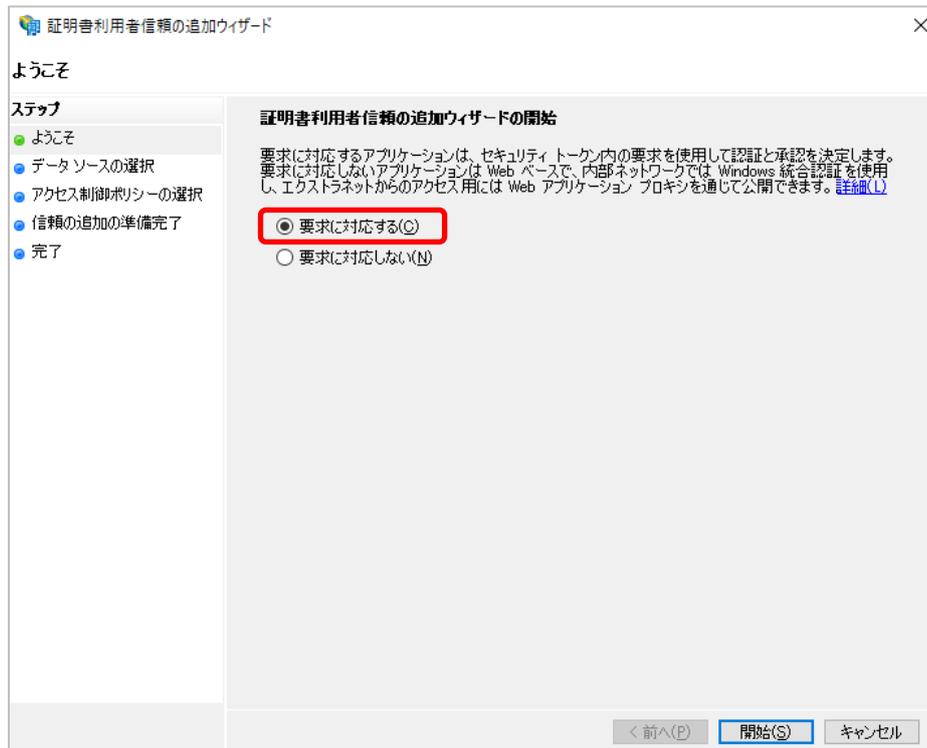
- 1) ADFS サーバー上の「ADFS の管理」ツールを起動し、[サービス] - [エンドポイント]を開きます。
- 2) 一覧から種類が“WS-Trust 1.3”、URL パスが “/adfs/services/trust/13/usernamemixed” および “/adfs/services/trust/13/windowsmixed” の行を選択し、有効にします。



- 3) ADFS 2.0 のサービスを再起動します。
- 4) 同様に[証明書利用者信頼]を選択し、「証明書利用者信頼の追加」を選択します。



- 5) ウィザードを開始します。
- 6) 「ようこそ」画面で「要求に対応する」を選択し、「開始」ボタンをクリックします。



- 7) 「データソースの選択」画面で「証明書利用者についてのデータを手動で入力する」を選択し、「次へ」ボタンをクリックします。

The screenshot shows the 'Certificate User Information Addition Wizard' dialog box, specifically the 'Data Source Selection' step. The left sidebar lists the steps: ようこそ, データソースの選択 (highlighted), 表示名の指定, 証明書の構成, URLの構成, 識別子の構成, アクセス制御ポリシーの選択, 信頼の追加の準備完了, and 完了. The main area contains instructions and three radio button options. The third option, '証明書利用者についてのデータを手動で入力する(D)', is selected and highlighted with a red box. Below it, a note states: '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。' At the bottom, there are buttons for '< 前へ(P)', '次へ(N) >' (highlighted), and 'キャンセル'.

- 8) 「表示名の指定」画面で任意の表示名を入力し、「次へ」ボタンをクリックします。

The screenshot shows the 'Certificate User Information Addition Wizard' dialog box, specifically the 'Display Name Specification' step. The left sidebar lists the steps: ようこそ, データソースの選択, 表示名の指定 (highlighted), 証明書の構成, URLの構成, 識別子の構成, アクセス制御ポリシーの選択, 信頼の追加の準備完了, and 完了. The main area contains instructions and two input fields. The '表示名(D):' field is highlighted with a red box and contains the text 'IBLook B2C'. Below it is a 'メモ(O):' text area. At the bottom, there are buttons for '< 前へ(P)', '次へ(N) >' (highlighted), and 'キャンセル'.

- 9) 「証明書の構成」画面で、証明書の指定は行わずに「次へ」ボタンをクリックします。

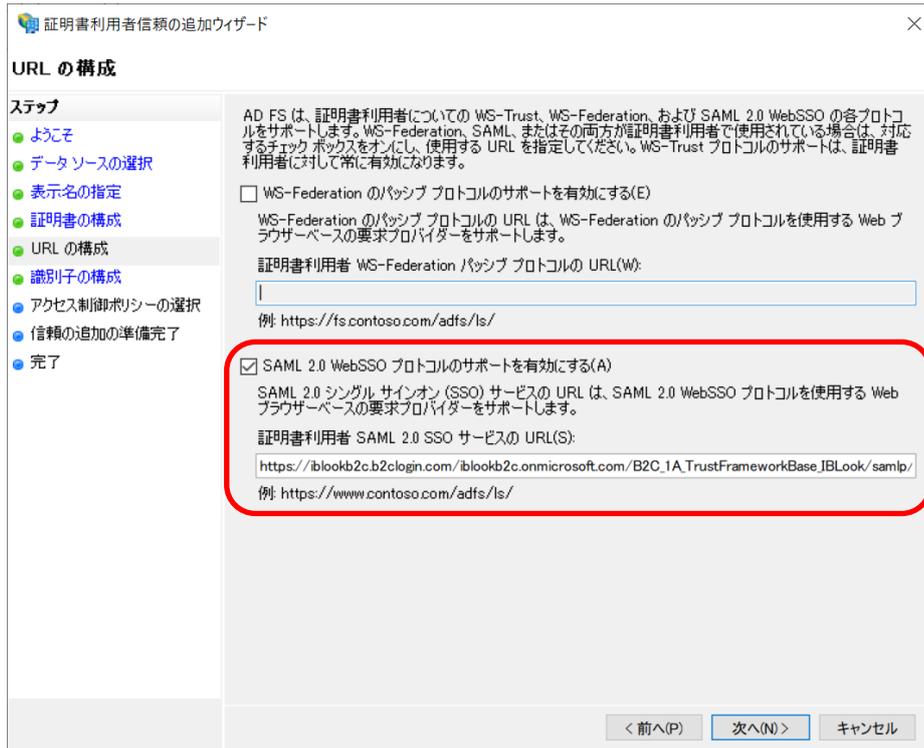


- 10) 「URL の構成」画面で、「SAML 2.0 WebSSO プロトコルのサポートを有効にする」チェックボックスをオンにし、「証明書利用者 SAML 2.0 SSO サービスの URL」欄に下記の値を入力して、「次へ」ボタンをクリックします。

※大文字小文字も正しく入力してください。

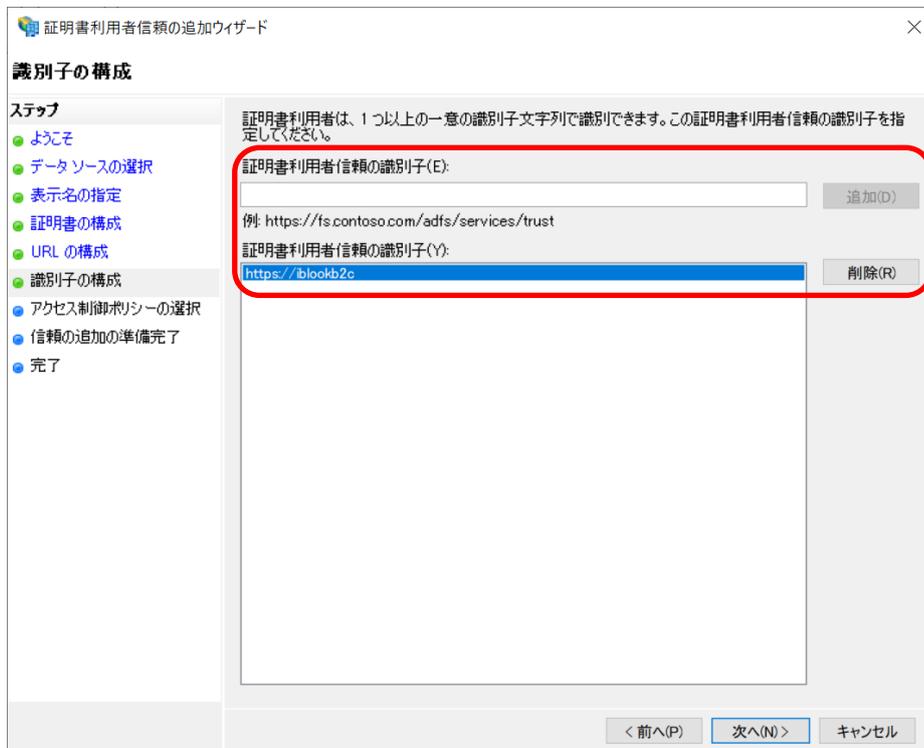
※一行で入力してください。

項目名	設定値
証明書利用者 SAML 2.0 SSO サービスの URL	https://iblookb2c.b2clogin.com/iblookb2c.onmicrosoft.com/B2C_1A_TrustFrameworkBase_IBLook/samlp/so/assertionconsumer

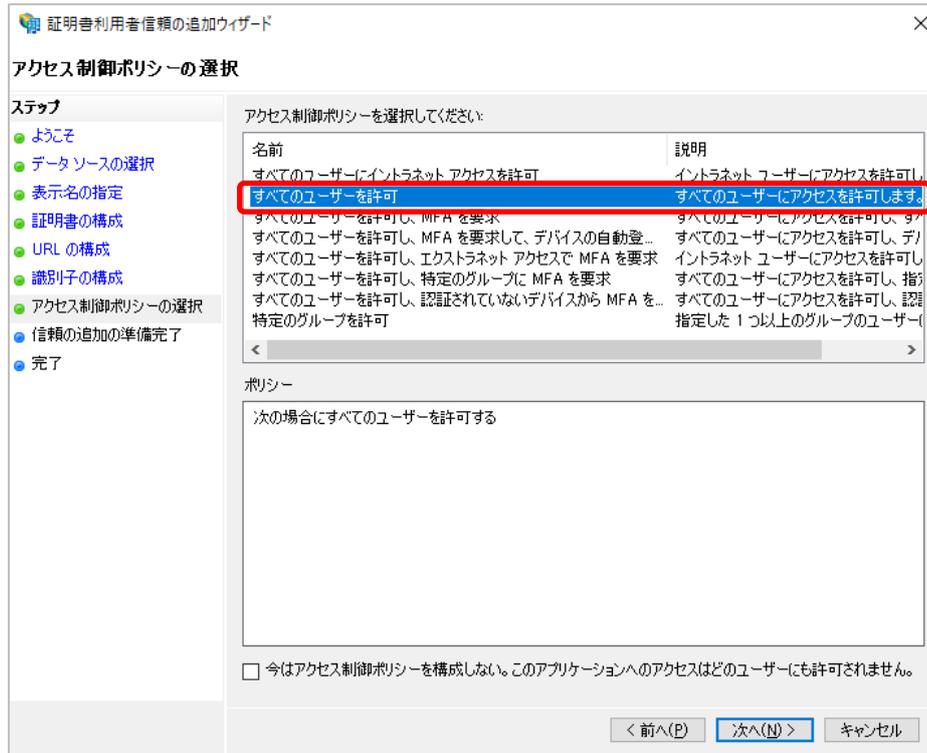


- 11) 「識別子の構成」画面で、「証明書利用者信頼の識別子」欄に「https://iblookb2c」を入力し、「追加」ボタンをクリックします。入力した内容が一覧に追加されたら、「次へ」ボタンをクリックします。

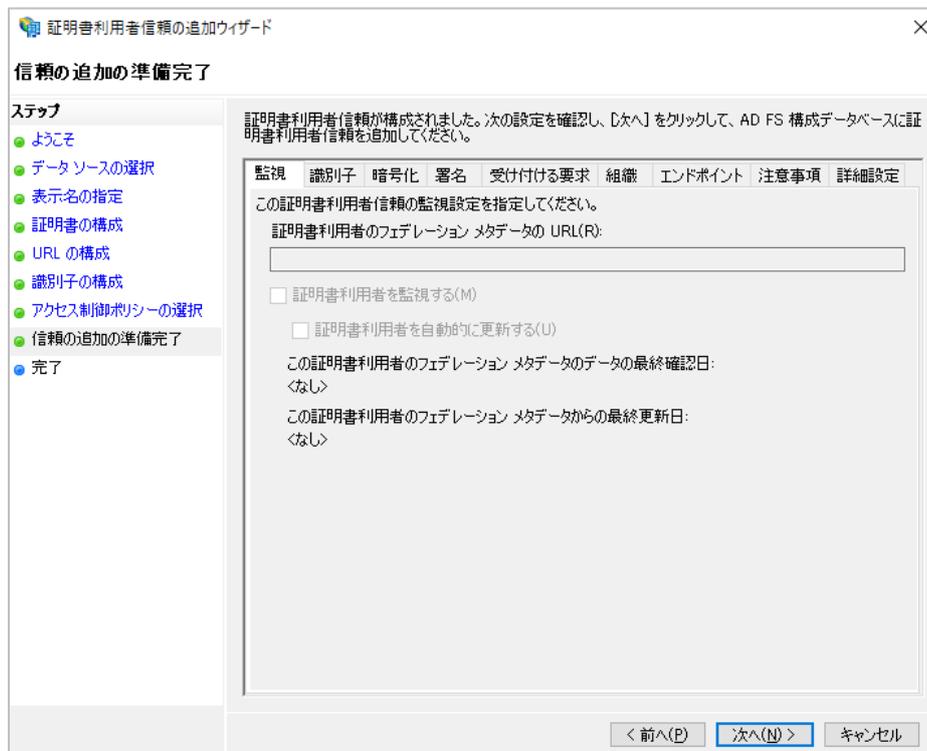
※大文字小文字も正しく入力してください。



- 12) 「アクセス制御ポリシーの選択」画面で、「すべてのユーザーを許可」を選択して、「次へ」ボタンをクリックします。



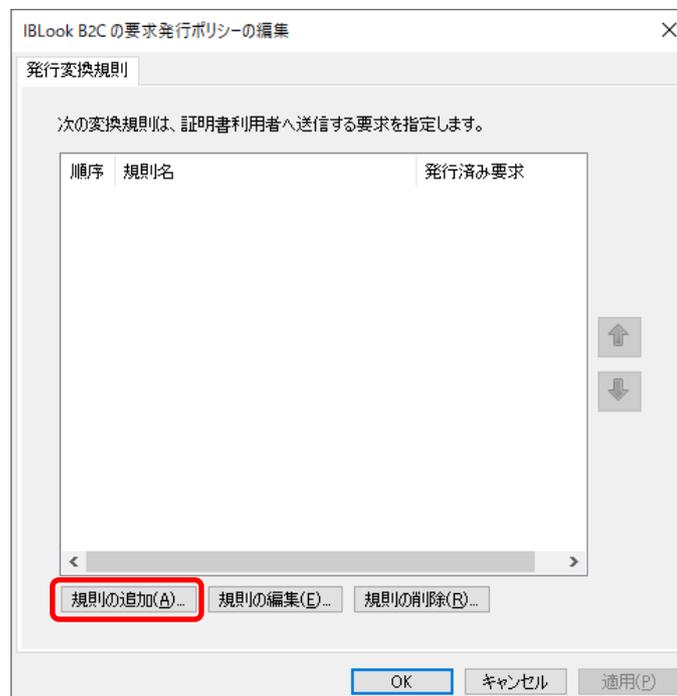
- 13) 「信頼の追加の準備完了」画面で、設定を確認し、「次へ」ボタンをクリックします。



- 14) 「完了」画面で、「閉じる」ボタンをクリックします。



- 15) 「要求発行ポリシーの編集」ダイアログボックスが自動的に表示されるので、「規則の追加」ボタンをクリックします。



- 16) 「規則テンプレートの選択」画面で、「要求規則テンプレート」欄から「LDAP 属性を要求として送信」を選択し、「次へ」ボタンをクリックします。

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(Q):

LDAP 属性を要求として送信

要求規則テンプレートの説明

[LDAP 属性を要求として送信] 規則テンプレートを使用すると、Active Directory などの LDAP 属性ストアから属性を選択して、証明書利用者に要求として送信できます。この規則の種類では、1 つの規則から複数の属性を複数の要求として送信できます。たとえば、この規則テンプレートを使用して、displayName および telephoneNumber の各 Active Directory 属性から認証済みユーザーの属性値を抽出して、これらの値を 2 つの異なる出力方向の要求として送信する規則を作成できます。この規則を使用して、ユーザーのすべてのグループメンバーシップを送信することもできます。グループメンバーシップを個別に送信する場合は、[グループメンバーシップを要求として送信] 規則テンプレートを使用します。

< 前へ(P)   次へ(N) >   キャンセル

17) 「要求規則の構成」画面で、以下の項目を設定し、「完了」ボタンをクリックします。

項目名	設定値
要求規則名	AD
属性ストア	Active Directory
LDAP 属性の出力方法の要求への関連付け	
項目名	設定値
LDAP 属性 (1 行目)	User-Principal-Name
出力方向の要求の種類 (1 行目)	UPN
LDAP 属性 (2 行目)	Employee-ID
出力方向の要求の種類 (2 行目)	名前 ID

変換要求規則の追加ウィザード

**規則の構成**

ステップ

- 規則の種類を選択
- 要求規則の構成

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

要求規則名(C):  
AD

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)
	User-Principal-Name	UPN
	Employee-ID	名前 ID
▶▶		

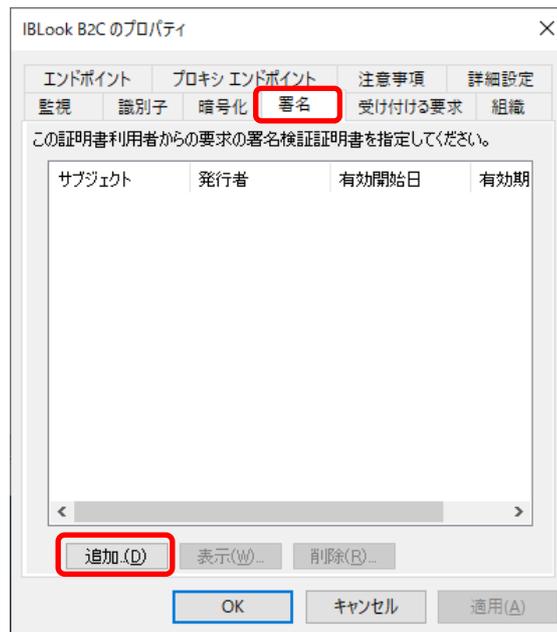
< 前へ(P)   **完了**   キャンセル

18) 「要求発行ポリシーの編集」ダイアログ ボックスに戻り、「OK」ボタンをクリックします。

19) 「ADFS の管理」ツールに戻り、「証明書利用者信頼」を選択します。

20) 作成した証明書利用者信頼を選択し、「プロパティ」をクリックします。

21) プロパティ画面で、「署名」タブをクリックして、「追加」ボタンをクリックします。

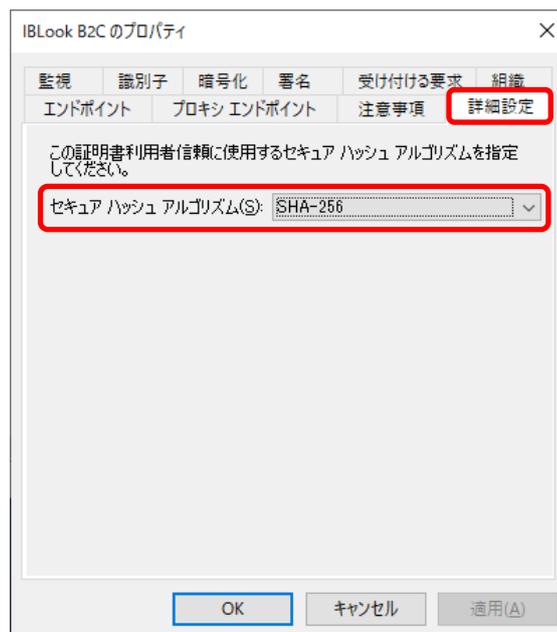


22) 署名証明書を下記の URL からダウンロードして展開し、「追加」ボタンをクリックして追加します。

※証明書の期限が切れる前に、証明書を更新する必要があります。

- [https://bbscdn.blob.core.windows.net/download/IBLook\\_cer.zip](https://bbscdn.blob.core.windows.net/download/IBLook_cer.zip)

23) プロパティ画面で、「詳細」タブをクリックし、「セキュア ハッシュ アルゴリズム」欄から「SHA-256」を選択して、「OK」ボタンをクリックします。



## 【ご注意】

お客様の ADFS サーバーと弊社サービスとで継続してフェデレーション認証を実施するためには、以下の証明書の期限が過ぎる前に、証明書を更新する必要があります。

- お客様側の証明書

ファイル「FederationMetadata.xml」を使用したフェデレーション認証を設定している場合、お客様が ADFS サーバーのトークン署名証明書を更新する度に、弊社サーバー側に新しい証明書を追加する必要があります。

証明書を更新後、プライマリ化する前に、「FederationMetadata.xml」をファイルに保存して弊社までご提供ください。

※ 「FederationMetadata.xml」は次の URL から参照可能です。

<https://<AD FS サーバー>/FederationMetadata/2007-06/FederationMetadata.xml>

【例】

<https://adfs.example.com/FederationMetadata/2007-06/FederationMetadata.xml>

- 弊社側の証明書

手順 21 で追加した署名検証証明書の更新時期に、新しい証明書をご提供します。

証明書の期限が過ぎる前に、新しい証明書を手順 21 に沿って追加してください。

## 2. Microsoft Azure ポータルでの設定手順

本章では、Microsoft Azure ポータルでの設定手順を説明します。

Microsoft Azure ポータルでの設定後、弊社サーバー側の設定が必要となりますので、フェデレーション メタデータ「FederationMetadata.xml」にアクセス可能な URL を Online サービス事務局<online-info@bbsystem.co.jp>までご提供ください。

※「FederationMetadata.xml」の URL は次の通りです。

`https://login.microsoftonline.com/<ドメイン名>/FederationMetadata/2007-06/FederationMetadata.xml`

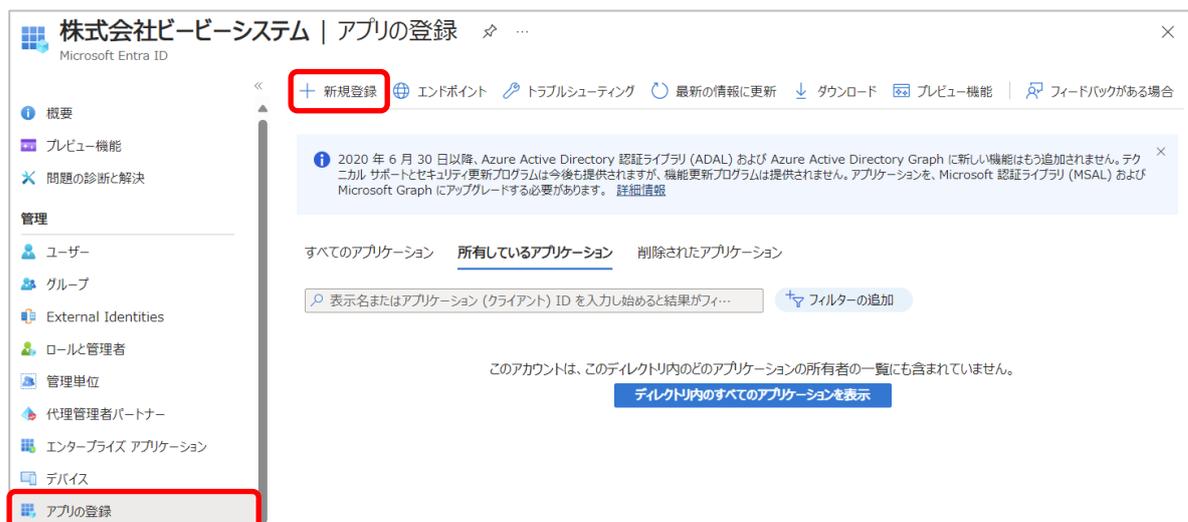
【例】

`https://login.microsoftonline.com/example.onmicrosoft.com/FederationMetadata/2007-06/FederationMetadata.xml`

### 2.1 アプリの新規作成

本節では、Microsoft Entra ID(旧：Azure Active Directory)内でのアプリの新規作成の手順を説明します。

- 1) Microsoft Azure ポータルにサインインします。
  - `https://portal.azure.com/`
- 2) 「Azure サービス」から「Microsoft Entra ID」を選択します。
- 3) 「アプリの登録」を開き、「新規作成」をクリックします。



- 4) 「アプリケーションの登録」画面で以下の項目を設定し、「登録」ボタンをクリックします。

項目名	設定値
名前	IBLook B2C
サポートされているアカウントの種類	この組織ディレクトリのみに含まれるアカウント
リダイレクト URI	https://www.iblook.net

### アプリケーションの登録

\* 名前  
このアプリケーションのユーザー向け表示名 (後で変更できます)。  
IBLook B2C

サポートされているアカウントの種類  
このアプリケーションを使用したりこの API にアクセスしたりできるのはだれですか?  
 この組織ディレクトリのみに含まれるアカウント (株式会社 ビービーシステム のみ・シングルテナント)  
 任意の組織ディレクトリ内のアカウント (任意の Azure AD ディレクトリ・マルチテナント)  
 任意の組織ディレクトリ内のアカウント (任意の Azure AD ディレクトリ・マルチテナント) と個人の Microsoft アカウント (Skype、Xbox など)  
 個人用 Microsoft アカウントのみ

選択に関する詳細..

リダイレクト URI (省略可能)  
ユーザー認証が成功すると、この URI に認証応答を返します。この時点での指定は省略可能で、後ほど変更できますが、ほとんどの認証シナリオで値が必要となります。  
Web https://www.iblook.net

続行すると、Microsoft プラットフォーム ポリシーに同意したことになります。

登録

- 5) アプリケーションの登録完了後、「API の公開」を開き、「追加」リンクをクリックします。



- 6) 「アプリ ID の URI の設定」画面で「アプリケーション ID の URI」の値を「api://iblookb2c」に変更後、「保存」ボタンをクリックします。  
※大文字小文字も正しく入力してください。

×

**アプリケーション ID URI の編集**

この Web API を識別するために使用するグローバルに一意の URI。スコープのプレフィックスであり、アクセス トークンでは audience クレームの値でもあります。また、識別子 URI と呼ばれます。

アプリケーション ID の URI

- (ア) 「認証」を開き、「URI の追加」リンクをクリックし、以下の URL を追加後、「保存」ボタンをクリックします。

※大文字小文字も正しく入力してください。

※一行で入力してください。

<b>リダイレクト URI</b>
https://iblookb2c.b2clogin.com/iblookb2c.onmicrosoft.com/B2C_1A_TrustFrameworkBase_IBLook/samlp/sso/assertionconsumer



## 2.2 API のアクセス許可 設定

本節では、「2.1 アプリの新規作成」に続き、作成したアプリに対して API のアクセス許可を設定する手順を説明します。

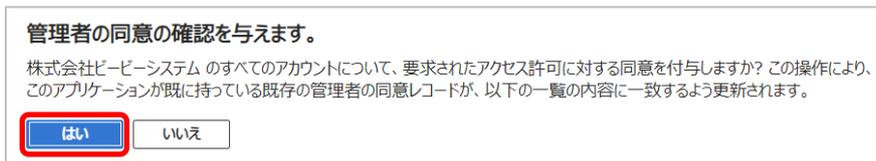
- 1) [API のアクセス許可]をクリックします。



- 2) [構成されたアクセス許可] - [<管理者アカウント名>に管理者の同意を与えます]をクリックします。



3) 表示されるメッセージを確認して[はい]をクリックします。



4) 「同意の付与に成功しました」と表示されることを確認します。



### 3. HENNGE One での設定手順

本章では、HENNGE One での設定手順を説明します。

HENNGE One での設定後、弊社サーバー側の設定が必要となりますので、フェデレーション メタデータ「FederationMetadata.xml」にアクセス可能な URL を Online サービス事務局<online-info@bbsystem.co.jp>までご提供ください。

- 1) HENNGE One 管理者サイトにサインインします。
  - <https://ap.sso.hdems.com/admin/〇〇〇>(利用ドメイン名)
- 2) サイドメニューから[システム]-[サービスプロバイダー設定]を選択し、「サービスプロバイダーの追加」をクリックします。



- 3) 「サービスプロバイダーの追加」画面で「カスタム」ボタンをクリックします。



4) 画面内で以下の項目を設定し、「次へ」ボタンをクリックします。

※大文字小文字も正しく入力してください。

※それぞれ一行で入力してください。

項目名	設定値
名前	IBLook B2C
ACS URL	https://iblookb2c.b2clogin.com/iblookb2c.onmicrosoft.com/B2C_1A_TrustFrameworkBase_IBLook/samlp/so/assertionconsumer
Entity ID	https://iblookb2c
Name ID	{user.upn}
ログイン URL	https://www.iblook.net
固有番号	任意の数字
セッション有効時間(時間)	任意の数字

サービスプロバイダーの追加

名前 ? IBLook B2C

ACS URL ? https://iblookb2c.b2clogin.com/iblookb2c.onmicroso

Entity ID ? https://iblookb2c

署名鍵 ? 2048-bits (推奨) ▼

Name ID ? {user.upn}

ログインURL ? https://www.iblook.net

固有番号 ? 1

セッション有効時間 (時間) ? 8

+ 次へ

- 5) 登録完了メッセージが表示されます。



- 6) 「サービスプロバイダー設定」画面で「署名方式」の値を「アサーション」に変更します。

The screenshot shows the "サービスプロバイダー設定" (Service Provider Settings) form. The "基本設定" (Basic Settings) section includes the following fields:

- 名前 (Name): IBLook B2C
- ダイレクトログインURL (Direct Login URL): https://ap.sso.hdems.com/portal1/bbsonline.net/
- ACS URL: https://iblookb2c.b2clogin.com/iblookb2c.onmicros
- Entity ID: https://iblookb2c
- ログインURL (Login URL): https://www.iblook.net
- 署名方式 (Signature Method): アサーション (Assertion) - This field is highlighted with a red box.
- 署名鍵 (Signature Key): 2048-bits (推奨) (2048-bits (Recommended))

A "送信" (Send) button is located at the bottom of the form.

- 7) 「サービスプロバイダー設定」画面最下の「属性の設定」から、「属性の追加」ボタンをクリックします。

The screenshot shows the "属性の設定" (Attribute Settings) section. It features a table with columns for "属性" (Attribute) and "値" (Value). A red box highlights the "+ 属性の追加" (Add Attribute) button. A "送信" (Send) button is located at the bottom of the section.

- 8) 「属性の設定」に以下の値を設定し、「送信」ボタンをクリックします。

※大文字小文字も正しく入力してください。

項目名	設定値
属性	o365upn
値	{user.upn}

サービスプロバイダー設定

固有番号 ? 1

セッション有効時間 (時間) ? 8

非表示 ?

ロゴ画像 ?  ファイルが選択されていません  
 ロゴを削除

現在のロゴ: ロゴが選択されていません

属性の設定

属性	値
o365upn	{user.upn}

- 9) 変更完了メッセージが表示されます。

サービスプロバイダー設定

成功: サービスプロバイダーが変更されました

- 10) サイドメニューから[ユーザー]-[アクセスポリシーグループ]を開き、利用ユーザーを含むポリシー設定の「編集」を開きます。
- 11) 「アクセスポリシーグループの編集」画面で「許可するサービスプロバイダー」から「IBLook B2C」のチェックをオンにし、「送信」ボタンをクリックします。

- 12) 変更完了メッセージが表示されます。

## 4. リダイレクト URL の設定変更手順

本章では、フェデレーション認証をご利用のお客様が新しいリダイレクト URL に切り替えるための、設定変更手順について説明します。

- ※ 現行のリダイレクト URL (<https://login.microsoftonline.com/...>) は、2020 年 12 月 4 日に廃止される事が Microsoft 社から公開されています。  
当日までには切り替えを実施頂きますようお願い致します。

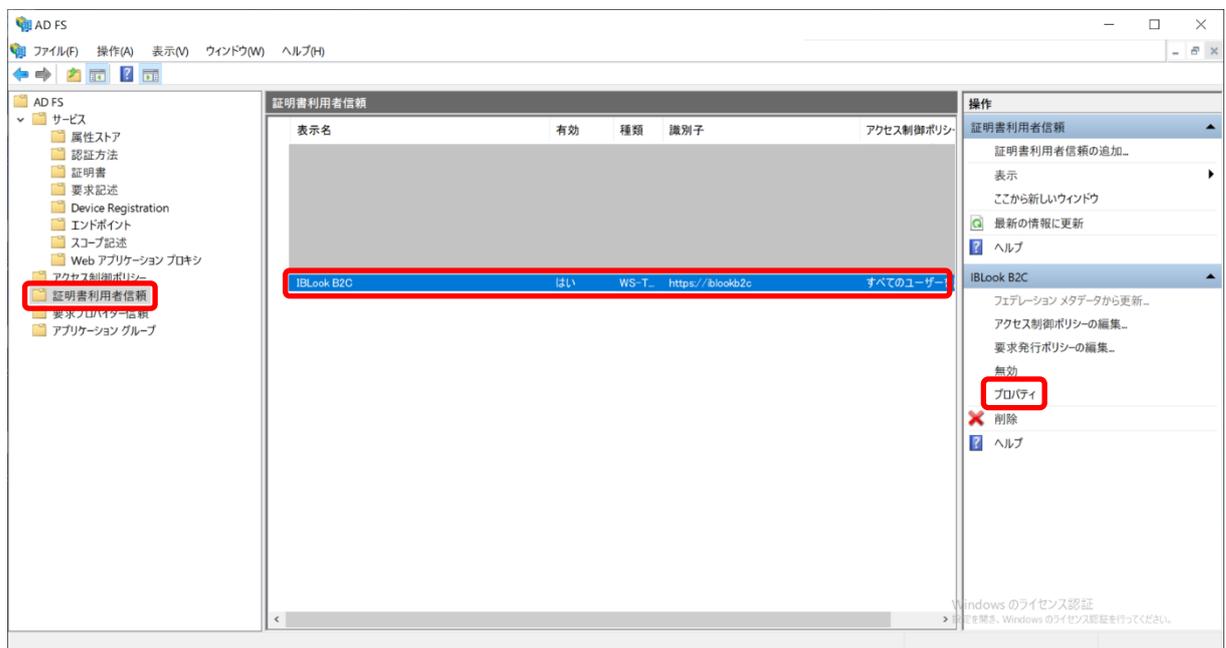
### 4.1 ADFS サーバーでの設定変更手順

ADFS サーバーでリダイレクト URL を切り替えるための、設定変更手順を説明します。

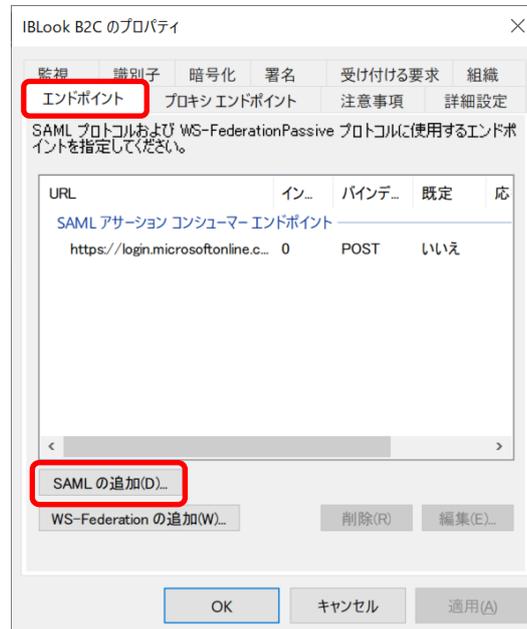
設定後、製品管理サイトで設定変更が必要となります。

詳細については、「4.4 製品管理サイトの設定変更手順」をご参照ください。

- 1) ADFS サーバー上の「ADFS の管理」ツールを起動し、[証明書利用者信頼]を開きます。
- 2) 一覧から「IBLook B2C」の行を選択し、「プロパティ」をクリックします。



- 3) プロパティ画面で、「エンドポイント」タブをクリックし、「SAML の追加」ボタンをクリックします。



- 4) 「エンドポイントの追加」画面で以下の項目を設定し、「OK」ボタンをクリックします。

※大文字小文字も正しく入力してください。

※それぞれ一行で入力してください。

項目名	設定値
エンドポイントの種類	SAML アサーション コンシューマー
バインディング	POST
インデックス	1 ※他のエンドポイントと重複しない数値
信頼された URL	https://iblookb2c.b2clogin.com/iblookb2c.onmicrosoft.com/B2C_1A_TrustFrameworkBase_IBLook/samlp/sso/assertion consumer

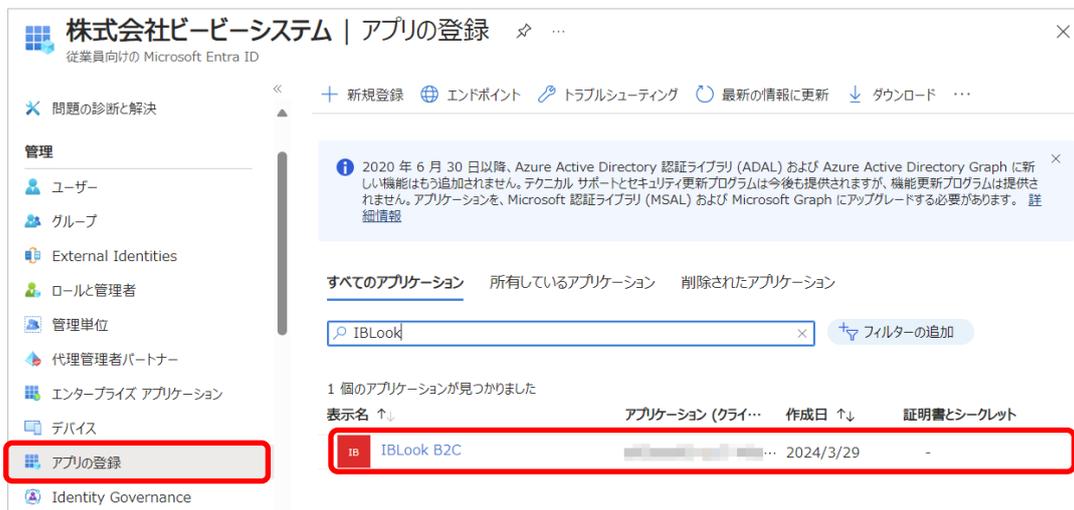
- 5) プロパティ画面で、「詳細」タブをクリックし、「セキュア ハッシュ アルゴリズム」欄から「SHA-256」を選択して、「OK」ボタンをクリックします。

## 4.2 Microsoft Azure ポータルでの設定手順

Microsoft Azure ポータルでリダイレクト URL を切り替えるための、設定変更手順を説明します。  
設定後、製品管理サイトで設定変更が必要となります。

詳細については、「4.4 製品管理サイトの設定変更手順」をご参照ください。

- 1) Microsoft Azure ポータルにサインインします。
  - <https://portal.azure.com/>
- 2) 「Azure サービス」から「Microsoft Entra ID」を選択します。
- 3) 「アプリの登録」を開き、「すべてのアプリケーション」から「IBLook B2C」をクリックします。



- 4) 「認証」を開き、「リダイレクト URI」欄に以下の URL を追加します。  
※大文字小文字も正しく入力してください。  
※それぞれ一行で入力してください。

リダイレクト URI

```
https://iblookb2c.b2clogin.com/iblookb2c.onmicrosoft.com/B2C_1A_TrustFrame  
workBase_IBLook/samlp/sso/assertionconsumer
```

5) 「保存」 ボタンをクリックします。

IBLook B2C | 認証

検索

フィードバックがある場合

概要

クイック スタート

統合アシスタント

管理

ブランド化とプロパティ

**認証**

証明書とシークレット

トークン構成

API のアクセス許可

API の公開

アプリ ロール

所有者

ロールと管理者

マニフェスト

プラットフォーム構成

このアプリケーションが対象としているプラットフォームまたはデバイスによっては、リダイレクト URI、特定の認証設定、プラットフォームに特有のフィールドなど追加構成が必要となる場合があります。

+ プラットフォームを追加

Web

リダイレクト URI

ユーザーが正常に認証またはサインアウトされた後に認証応答 (トークン) を返すときに宛先として受け入れられる URI。要求に入れてログイン サーバーに送信するリダイレクト URI は、ここに一覧表示されているものと一致する必要があります。これは応答 URL とも呼ばれます。リダイレクト URI と制限の詳細情報

https://www.iblook.net

https://iblookb2c.b2clogin.com/iblookb2c.onmicrosoft.com/B2C\_1A\_TrustFrameworkBase\_IBLook/samlp/ss...

URI の追加

保存 破棄

### 4.3 HENNGE One での設定手順

HENNGE One でリダイレクト URL を切り替えるための、設定変更手順を説明します。

設定後、製品管理サイトで設定変更が必要となります。

詳細については、「4.4 製品管理サイトの設定変更手順」をご参照ください。

- 1) HENNGE One 管理者サイトにサインインします。
  - <https://ap.sso.hdems.com/admin/〇〇〇>(利用ドメイン名)
- 2) サイドメニューから[システム]-[サービスプロバイダー設定]を選択し、「IBLook B2C」の編集アイコンをクリックします。



- 3) 「サービスプロバイダー設定」画面で「ACS URL」欄に以下の URL を設定します。  
※大文字小文字も正しく入力してください。  
※それぞれ一行で入力してください。

ACS URL
<a href="https://iblookb2c.b2clogin.com/iblookb2c.onmicrosoft.com/B2C_1A_TrustFrameworkBase_IBLook/samlp/sso/assertionconsumer">https://iblookb2c.b2clogin.com/iblookb2c.onmicrosoft.com/B2C_1A_TrustFrameworkBase_IBLook/samlp/sso/assertionconsumer</a>

- 4) 「送信」 ボタンをクリックします。

サービスプロバイダー設定

基本設定

名前 ? IBLook B2C

ダイレクトログインURL ? https://ap.sso.hdems.com/portal1/bbsonline.net/

ACS URL ? https://iblookb2c.b2clogin.com/iblookb2c.onmicroso

Entity ID ? https://iblookb2c

ログインURL ? https://www.iblook.net

署名方式 ? アサーション

署名鍵 ? 2048-bits (推奨)

送信

- 5) 変更完了メッセージが表示されます。

サービスプロバイダー設定

成功: サービスプロバイダーが変更されました

## 4.4 製品管理サイトの設定変更手順

本章では、製品管理サイトでの設定変更手順を説明します。

- 1) 製品管理サイトを開き、管理者アカウントでサインインします。
  - <https://portal.bbsonlineservices.net/>

- 2) 「管理」サイトを開き、「IBLook」を選択します。

---

ご契約済みのサービスのみメニューに表示されます。

---

- 3) IBLook 設定画面が開くので、「フェデレーション リダイレクト先」項目を「1:b2clogin」に変更します。



- 4) 「保存」を選択します。

以上