

# Smart Federation管理マニュアル (外部認証連携)



2022年10月21日  
NTT BizLink株式会社

# 目次

Domain,userPoolIdの確認

外部認証連携

Azure Active Directory編

Google編

ビジネスdアカウント編

# Domain, userPoolIdの確認

Smart Federation管理メニューから各プロバイダの認証情報に必要なCognitoドメイン,ユーザープールID、およびリダイレクトURLを確認することができます。

① 管理メニューで『IDプロバイダー管理』をクリックしてください。

②-1 Microsoftの連携をする場合

『Cognitoドメイン』、『ユーザープールID』をコピーしてテキストファイルに保存してください。（後程使用します）

以降、Cognitoドメイン、ユーザープールIDを弊社から通知されたドメイン、ユーザープールIDと呼びます。

②-2 Googleの連携をする場合

『Cognitoドメイン』をコピーしてテキストファイルに保存してください。（後程使用します）

以降、Cognitoドメインを弊社から通知されたドメインと呼びます。

HOME/ IDプロバイダー管理

管理メニュー  
ユーザー管理

|             |                                     |
|-------------|-------------------------------------|
| Cognitoドメイン | smartfederation-XXXX.mc2.bizppf.net |
| ユーザープールID   | ap-northeast-1_NuXXXXXXX            |

以降、「外部認証連携 Azure Active Directory編」をご参照ください。

②-3 ビジネスdアカウントの連携をする場合

『dアカウントリダイレクトURL1』、『dアカウントリダイレクトURL2』を両方コピーしてテキストファイルに保存してください。（後程使用します）

以降、dアカウントリダイレクトURL1、2を弊社から通知されたdアカウントリダイレクトURLと呼びます。

HOME/ IDプロバイダー管理

管理メニュー  
ユーザー管理

|                  |  |
|------------------|--|
| dアカウントリダイレクトURL1 | https://XXXXXXXXX.amazoncognito.com/authorize-return       |
| dアカウントリダイレクトURL2 | https://smartfederation-XXXX.amazoncognito.com/idpresponse |

HOME/ IDプロバイダー管理

管理メニュー

|             |                                     |
|-------------|-------------------------------------|
| Cognitoドメイン | smartfederation-XXXX.mc2.bizppf.net |
|-------------|-------------------------------------|

以降、「外部認証連携 Google編」をご参照ください。

以降、「外部認証連携 ビジネスdアカウント編」をご参照ください。

# 外部認証連携 Azure Active Directory編

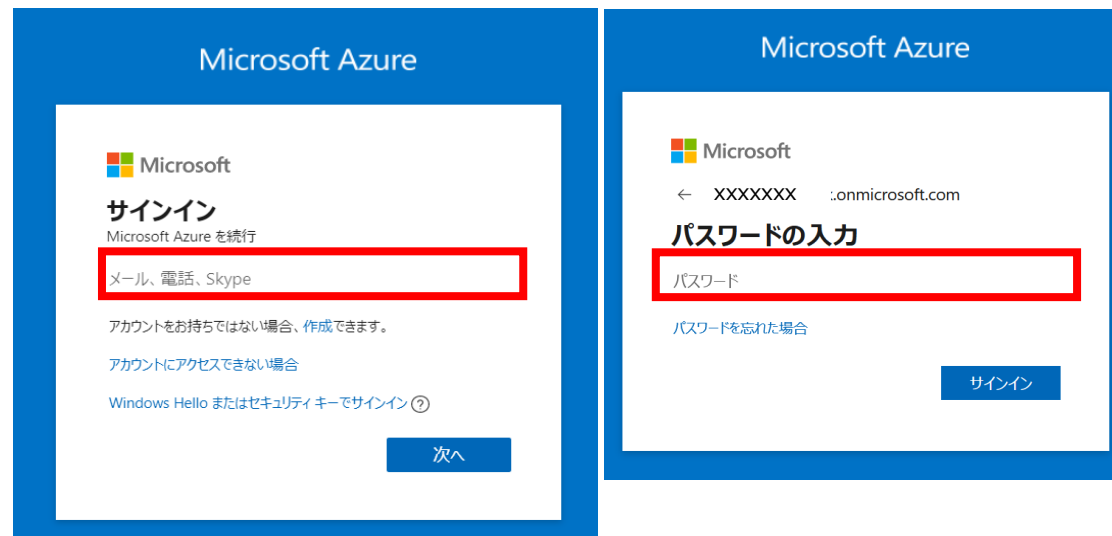
# Azure Portalのログイン

Azure Active Directoryの情報を以下の手順で確認します。

① Azure Portal (<https://portal.azure.com/>) にアクセスします。

② 連携したい Azure Active Directory を管理しているアカウントでサインインしてください。

③ サインイン後、Azureの概要画面に移動します。



# アプリの登録

① サイト上部にある検索欄で『Azure Active Directory』を検索します。

② 左の一覧にある『エンタープライズアプリケーション』を選択します。

③ アプリの登録画面に移動したら、『新しいアプリケーション』を選択します。



④独自アプリケーションの作成を押下します。

ホーム > CLテスト3ディレクトリ > エンタープライズアプリケーション >

## Azure AD ギャラリーの参照 ...

+ 独自のアプリケーションの作成 ⓘ 新しいギャラリー アプリを要求する

### 独自のアプリケーションの作成

×

フィードバックがある場合

独自のアプリケーションを開発している場合、アプリケーション プロキシを使用している場合、またはギャラリーにないアプリケーションを統合する必要がある場合は、ここで独自のアプリケーションを作成できます。

お使いのアプリの名前は何か?

TEST ✓

アプリケーションでどのような操作を行いたいですか?

オンプレミスのアプリケーションへのセキュリティで保護されたリモート アクセス用のアプリケーション プロキシを構成します

アプリケーションを登録して Azure AD と統合します (開発中のアプリ)

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)

⑤右側に「独自アプリケーションの作成」が表示されます。

⑥アプリ名を入力します。

⑦「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」を選択します。

⑧作成を押下します。

⑨シングルサインオンの設定を押下します。

ホーム > CLテスト3ディレクトリ > エンタープライズアプリケーション > Azure AD ギャラリーの参照 >

TEST | 概要 ...  
エンタープライズアプリケーション

概要

プロパティ

名前 ①

TEST

⑩SAMLを選択します。

2. シングル サインオンの設定

ユーザーが自分の Azure AD 資格情報を使用して、アプリケーションにサインインできるようにする

[作業の開始](#)

シングル サインオン方式の選択 [判断に役立つヘルプの表示](#)

無効

シングル サインオンが有効になっていません。ユーザーは、[マイ アプリ] からアプリを起動できません。

SAML

SAML (Security Assertion Markup Language) プロトコルを使用した、アプリケーションに対する多機能かつセキュリティで保護された認証。



⑪編集を押下します。

## SAML によるシングル サインオンのセットアップ

フェデレーション プロトコルに基づく SSO 実装により、セキュリティ、信頼性、エンド ユーザー エクスペリエンスが向上し、実装が容易になります。OpenID Connect または OAuth が使用されていない既存のアプリケーションの場合は、できるだけ SAML シングル サインオンを選択してください。[詳細については、こちらをご覧ください。](#)

以下をお読みください [構成ガイド](#) TEST を統合するためのヘルプ。

1

### 基本的な SAML 構成

|   |      |
|---|------|
| 識別子 (エンティティ ID)                         | 必須   |
| 応答 URL (Assertion Consumer Service URL) | 必須   |
| サインオン URL                               | 省略可能 |
| リレー状態 (省略可能)                            | 省略可能 |
| ログアウト URL (省略可能)                        | 省略可能 |

 編集

- ⑫識別子、応答URLをそれぞれ押下し、入力します。  
入力後、保存を押下します。

## 基本的な SAML 構成



フィードバックがある場合

識別子 (エンティティ ID) \* ⓘ

既定の識別子は、IDP-initiated SSO の SAML 応答の対象となります

識別子の追加

urn:amazon:cognito:sp:<弊社から通知された ユーザープールID>

urn:amazon:cognito:sp:ap-northeast-1\_NuXxxxxxxx

応答 URL (Assertion Consumer Service URL) \* ⓘ

既定の応答 URL は、IDP-initiated SSO の SAML 応答の宛先になります

応答 URL の追加

https://<弊社から通知された ドメイン > /saml2/idpresponse

https://Smart FederationXXXX.mc2.bizppf.net/saml2/idpresponse

⑬ アプリのフェデレーション メタデータURLをクリップボードにコピーしてください。

3

## SAML 署名証明書

⚠ 手順 1 で必須フィールドに入力してください

|                        |  |
|------------------------|--|
| 状態                     | アクティブ  |
| 拇印                     | 32BE7E01489B7C18A2ECD7758C179B6B16E85D6D   |
| 有効期限                   | 2026/10/25 2:45:56   |
| 通知用メール                 | cl_test3@vcbizlink.onmicrosoft.com   |
| アプリのフェデレーション メタデータ URL | <a href="https://login.microsoftonline.com/cf2bf602-a3ec-...">https://login.microsoftonline.com/cf2bf602-a3ec-...</a> <span>クリップボードにコピー</span> |
| 証明書 (Base64)           | ダウンロード   |
| 証明書 (未加工)              | ダウンロード   |
| フェデレーション メタデータ XML     | ダウンロード   |

⑭左側のメニューから「ユーザーとグループ」を押下します。



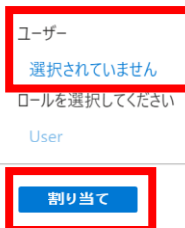
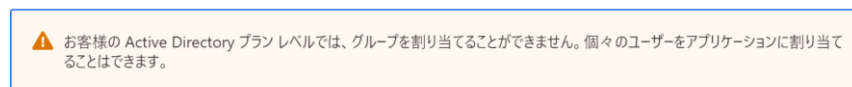
⑮「ユーザーまたはグループの追加」を押下します。



⑯ユーザーまたはグループを選択してください。



※お客さまのご契約プランによって選択できる範囲が異なります。



⑰割り当てを押下してください。

Smart Federationのテナント管理者として登録されているユーザーでログインしてください。

- ① 弊社より事前に通知されている  
ログインURL(https://)へアクセスしてください。  
ログイン画面が表示されます。

※ブックマークに登録しておくと次回以降はブックマークからアクセスできます。

- ② 管理者として登録されているユーザーIDを入力してください。
- ③ パスワードを入力してください。
- ④ 『Sign in』 ボタンを押してください。

The screenshot shows the login interface for docomo business and NTT BizLink. It features two main login paths. The first path, 'Sign in with your corporate ID', includes a button labeled 'PublicRoom'. The second path, 'Sign in with your username and password', includes input fields for 'Username' and 'Password', both of which are highlighted with red boxes. A 'Sign in' button is located at the bottom of the form. Two callout boxes provide instructions: one points to the 'Username' field with the text 'User IDを入力' and another points to the 'Password' field with the text 'パスワードを入力'.

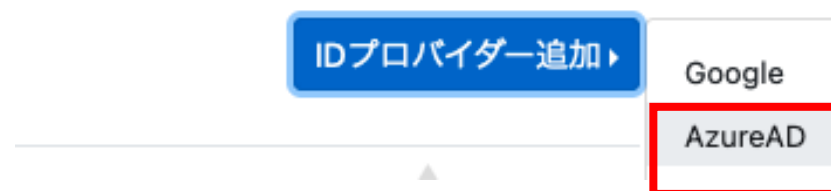
※お客さまのお申込み内容により画面が異なる場合がございます。

# Azure ADの登録

Smart Federation管理メニューのIDプロバイダー管理からAzureADを登録します。

①管理メニューで『IDプロバイダー管理』をクリックしてください。

②IDプロバイダー追加を押下し、AzureADを選択します。



③名前を入力します。  
(登録後は変更出来ません。)

④お客さま側でAzure ADに設定いただいた  
『メタデータURL』を入力します。

A screenshot of a web form titled 'IDプロバイダー追加' (Add ID Provider) with a close button (X) in the top right corner. The form has three required fields, each indicated by a yellow '必須' (Required) label:

- 'プロバイダー名' (Provider Name): A text input field containing 'AzureAD'.
- 'タイプ' (Type): A dropdown menu with 'SAML' selected.
- 'メタデータURL' (Metadata URL): A text input field containing the placeholder text 'メタデータURを入力' (Enter metadata URL).

At the bottom right of the form, there are two buttons: 'キャンセル' (Cancel) and '送信' (Send). The '送信' button is highlighted with a red rectangular border.

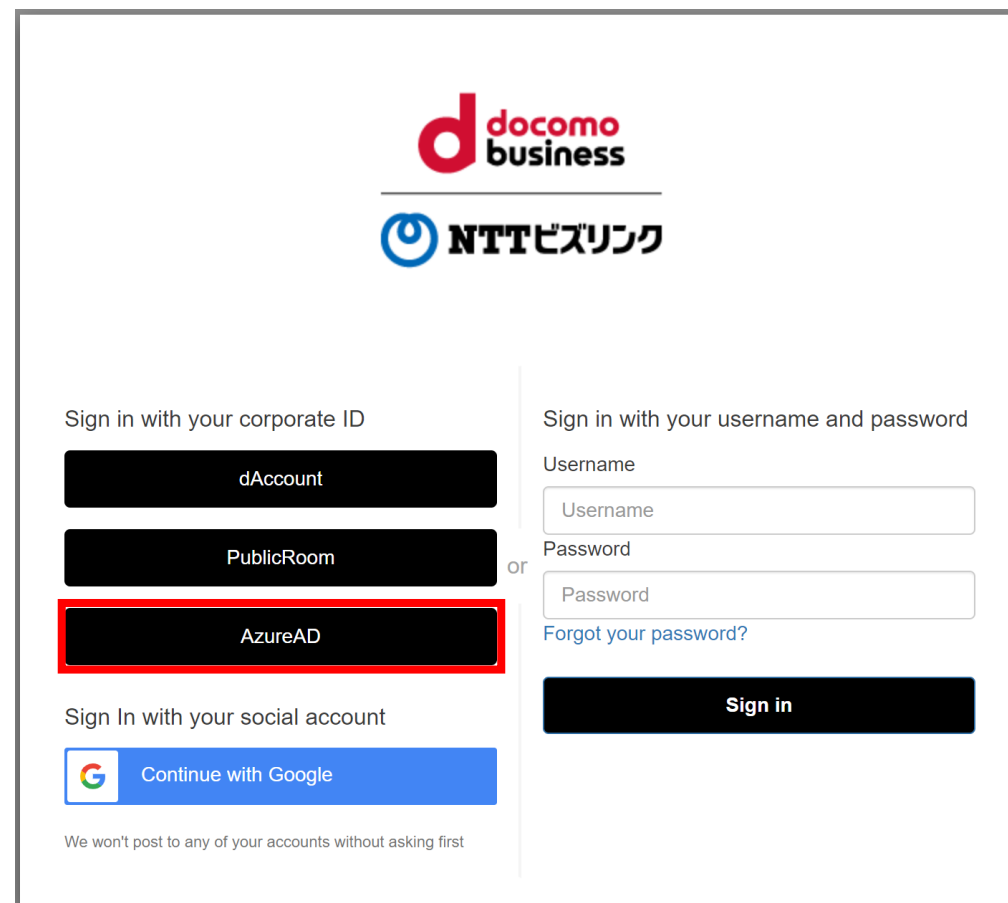
⑤『送信』をクリックします。

① Smart Federation ログインURLにアクセスしてください。

② 『Microsoftでログイン』を選択し、  
Smart Federationへ登録した  
Microsoftのアカウントで ログインしてくださ  
い。

※ Smart Federationへの登録、  
ログイン方法は以下をご参照ください。

別冊『Smart Federation管理マニュアル』  
別冊『Smart Federation利用マニュアル』



docomo business

NTT BizLink

Sign in with your corporate ID

dAccount

PublicRoom

AzureAD

Sign in with your username and password

Username

Password

Forgot your password?

Sign in

Sign In with your social account

Continue with Google

We won't post to any of your accounts without asking first

## ■ 識別子が正しく登録されていない もしくはメタデータURLが正しく登録されていない

Smart Federationのログイン画面にて「Microsoftでログイン」からSSOする際、右の画像のようなエラーが出た場合は、以下をご確認ください。

- ① Azureのアプリケーションに「識別子」の値が登録されていない、もしくは誤った値が登録されている可能性があります。正しい値が登録されているかどうかご確認ください。

※確認方法につきましては、以下を参照してください。

本マニュアル P.11

- ② Smart Federationに「メタデータURL」の値が登録されていない、もしくは誤った値が登録されている可能性があります。正しい値が登録されているかどうかご確認ください。

※確認方法につきましては、以下を参照してください。

本マニュアル P.15



### サインイン

申し訳ありませんが、サインイン中に問題が発生しました。

AADSTS700016: Application with identifier 'urn:amazon:cognito:sp:ap-northeast-1\_3axj7aXyV' was not found in the directory 'CLテスト5ディレクトリ'. This can happen if the application has not been installed by the administrator of the tenant or consented to by any user in the tenant. You may have sent your authentication request to the wrong tenant.

#### トラブルシューティングの詳細

管理者に問い合わせる場合、この情報を送信してください。

[情報をクラブボードにコピーする](#)

**Request Id:** dd32f155-0b2b-44f6-8f47-8957c05d6400

**Correlation Id:** b1ec3761-6da1-45ab-a354-aa2ee124f37d

**Timestamp:** 2022-03-24T10:13:57Z

**Message:** AADSTS700016: Application with identifier 'urn:amazon:cognito:sp:ap-northeast-1\_3axj7aXyV' was not found in the directory 'CLテスト5ディレクトリ'. This can happen if the application has not been installed by the administrator of the tenant or consented to by any user in the tenant. You may have sent your authentication request to the wrong tenant.

**サインイン エラーに確認のフラグを設定:** [フラグを有効にする](#)

この問題のサポートを受ける計画の場合は、フラグを有効にして、20分以内にエラーの再現を試みます。イベントにフラグを設定すると診断が利用できるようになり、管理者の注意が喚起されます。



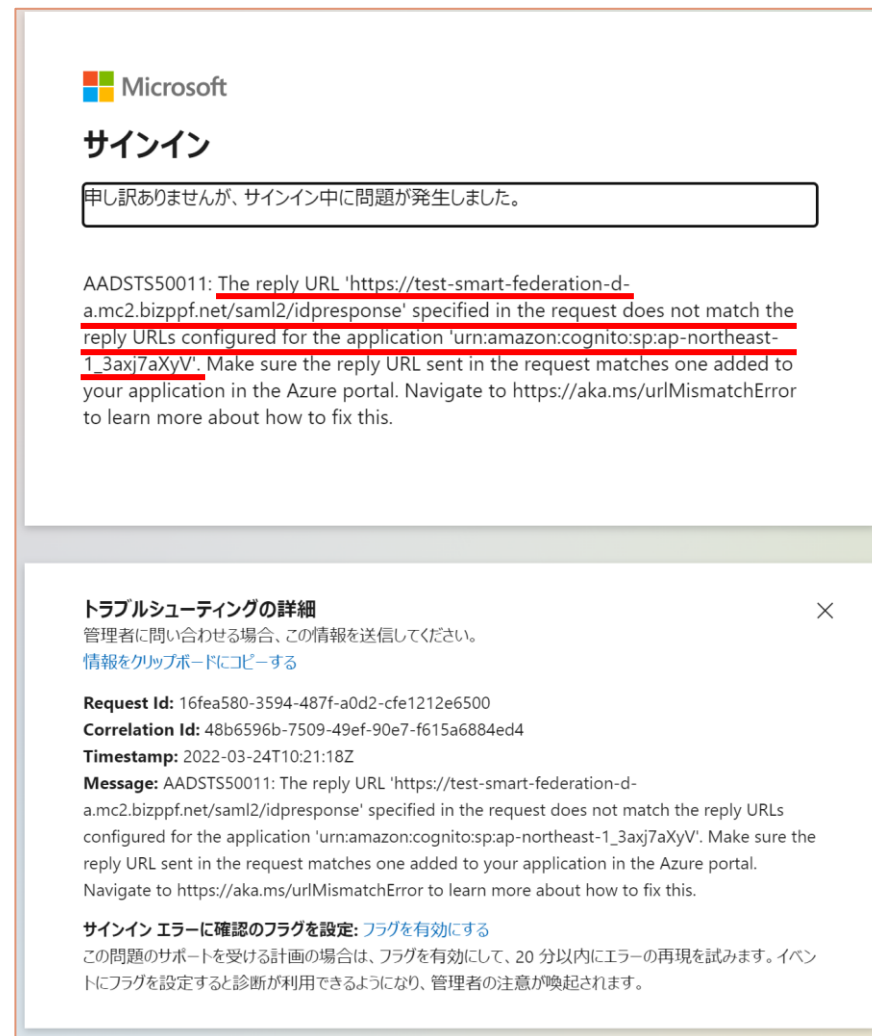
## ■ 応答URLが正しく登録されていない

Smart Federationのログイン画面にて「Microsoftでログイン」からSSOする際、右の画像のようなエラーが出た場合は、以下をご確認ください。

- ① Azureのアプリケーションに「応答URL」の値が登録されていない、もしくは誤った値が登録されている可能性があります。正しい値が登録されているかどうかご確認ください。

※確認方法につきましては、以下を参照してください。

本マニュアル P.11



Microsoft

### サインイン

申し訳ありませんが、サインイン中に問題が発生しました。

AADSTS50011: The reply URL 'https://test-smart-federation-d-a.mc2.bizppf.net/saml2/idpresponse' specified in the request does not match the reply URLs configured for the application 'urn:amazon:cognito:sp:ap-northeast-1\_3axj7aXyV'. Make sure the reply URL sent in the request matches one added to your application in the Azure portal. Navigate to <https://aka.ms/urlMismatchError> to learn more about how to fix this.

---

**トラブルシューティングの詳細** ×

管理者に問い合わせる場合、この情報を送信してください。  
[情報をクリップボードにコピーする](#)

**Request Id:** 16fea580-3594-487f-a0d2-cfe1212e6500  
**Correlation Id:** 48b6596b-7509-49ef-90e7-f615a6884ed4  
**Timestamp:** 2022-03-24T10:21:18Z  
**Message:** AADSTS50011: The reply URL 'https://test-smart-federation-d-a.mc2.bizppf.net/saml2/idpresponse' specified in the request does not match the reply URLs configured for the application 'urn:amazon:cognito:sp:ap-northeast-1\_3axj7aXyV'. Make sure the reply URL sent in the request matches one added to your application in the Azure portal. Navigate to <https://aka.ms/urlMismatchError> to learn more about how to fix this.

**サインイン エラーに確認のフラグを設定: フラグを有効にする**

この問題のサポートを受ける計画の場合は、フラグを有効にして、20 分以内にエラーの再現を試みます。イベントにフラグを設定すると診断が利用できるようになり、管理者の注意が喚起されます。

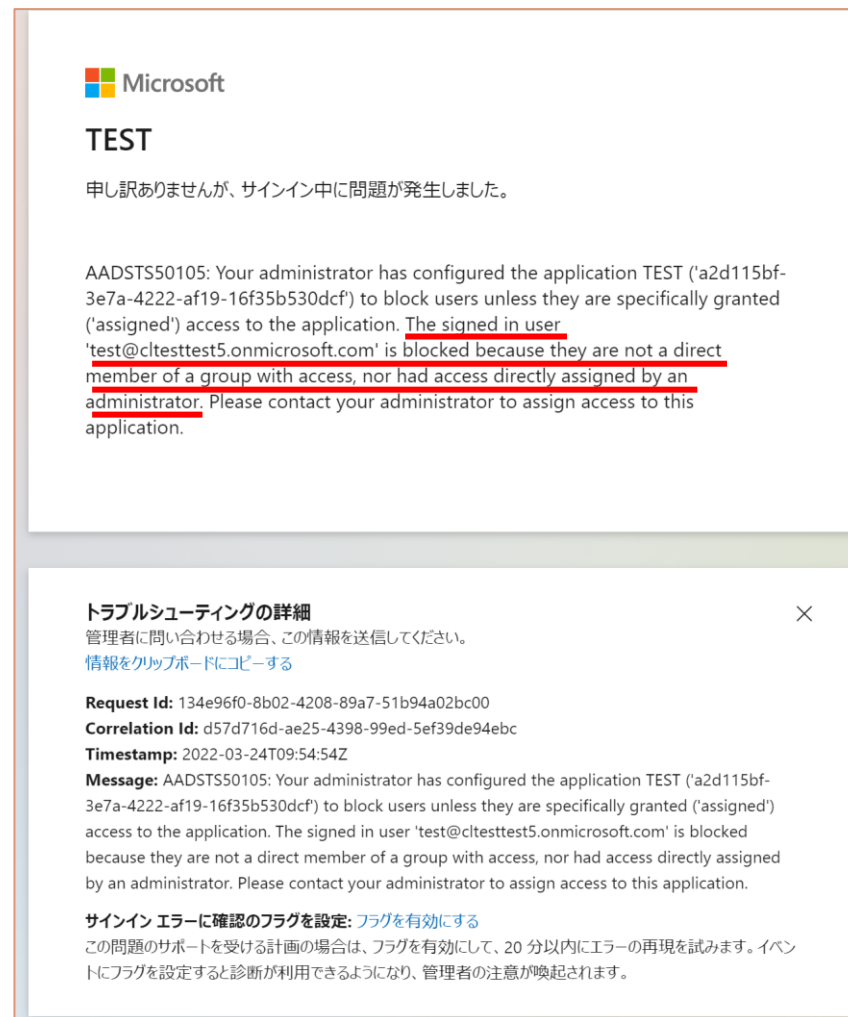
## ■ Azureのアプリケーションに ユーザーまたはグループが正しく登録されていない

Smart Federationのログイン画面にて「Microsoftでログイン」からSSOする際、右の画像のようなエラーが出た場合は、以下をご確認ください。

- ① Azureのアプリケーションにユーザーまたはグループが割り当てられていない可能性があります。  
正しいユーザーが登録されているかご確認ください。

※確認方法につきましては、以下を参照してください。

本マニュアル P.13



The screenshot shows an error message from Microsoft for an application named 'TEST'. The error message states: 'AADSTS50105: Your administrator has configured the application TEST ('a2d115bf-3e7a-4222-af19-16f35b530dcf') to block users unless they are specifically granted ('assigned') access to the application. The signed in user 'test@cltesttest5.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.'

Below the error message is a 'トラブルシューティングの詳細' (Troubleshooting details) dialog box. It contains the following information:

- Request Id:** 134e96f0-8b02-4208-89a7-51b94a02bc00
- Correlation Id:** d57d716d-ae25-4398-99ed-5ef39de94ebc
- Timestamp:** 2022-03-24T09:54:54Z
- Message:** AADSTS50105: Your administrator has configured the application TEST ('a2d115bf-3e7a-4222-af19-16f35b530dcf') to block users unless they are specifically granted ('assigned') access to the application. The signed in user 'test@cltesttest5.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.

The dialog box also includes a link to 'サインイン エラーに確認のフラグを設定: フラグを有効にする' (Set a flag for sign-in error confirmation: Enable the flag) and a note: 'この問題のサポートを受ける計画の場合は、フラグを有効にして、20 分以内にエラーの再現を試みます。イベントにフラグを設定すると診断が利用できるようになり、管理者の注意が喚起されます。' (If you plan to receive support for this issue, enable the flag and attempt to reproduce the error within 20 minutes. Setting the flag in the event allows diagnostics to be used and administrator attention is alerted.)

## ■ Smart Federationにアカウントが正しくユーザー登録されていない

Smart Federationのログイン画面にて「Microsoftでログイン」からSSOする際、右の画像のようなエラーが出た場合は、以下をご確認ください。

- ①対象のAzure ADアカウントがSmart Federationに正しくユーザー登録されていない可能性があります。Smart Federation管理者サイトにアクセスし、対象のユーザーが登録されているかどうかご確認ください。

※確認方法につきましては、以下を参照してください。

別冊『Smart Federation管理マニュアル』



## ■ お使いの端末がAzure ADのデバイス管理で許可されていない

Smart Federationのログイン画面にて「Microsoftでログイン」からSSOする際、右の画像のようなエラーが出た場合は、以下をご確認ください。

- ①お客様のAzure ADでデバイス管理設定が有効になっており、お使いの端末が許可されていない可能性があります。デバイス管理設定が有効になっている場合、許可されていない端末からはログインできません。お客様のAzure ADのデバイス管理設定で、お使いの端末が許可されているかをご確認ください。



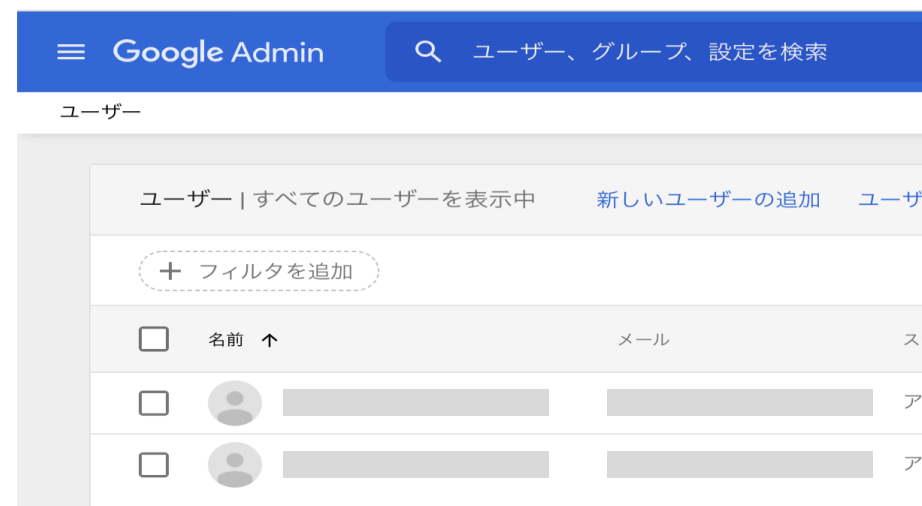
# 外部認証連携 Google編

Google Workspaceをご契約「あり」の方と「なし」の方で利用するアカウントが異なります。連携したいユーザーの種類によって設定をするアカウントを選択してください。

## ■ Google Workspaceのユーザーのみにする場合

Google Workspaceではユーザーが管理されています。

Google Workspaceに所属するユーザーのみログインを可能にする場合には、**GoogleWorkspaceのユーザーのアカウント**を利用してください。



## ■ Google Workspaceのユーザーに限定しない場合

Googleアカウントを所有するユーザーのログインを可能にする場合は、無料のGoogleアカウントでも可能です。Google Workspaceのアカウントでお作りいただいても問題ありません。

# Google Workspaceのログイン

Google Cloud Platformのプロジェクトを作成します。

①Google Cloud Platform  
(<https://console.cloud.google.com>) にアクセスします。

②Googleアカウントでログインしてください。

## ※注意

Google Workspaceのユーザーのみに制限する場合は、  
Google Workspaceのアカウントでログインしてください。

Google Workspaceのユーザーに制限しない場合は、  
任意のGoogleアカウントでログインしてください。

※お申込み時のアカウントと一致していなくても問題ありません。

③ログイン後、 Google Cloud Platformの画面に移動します。

Google  
ログイン  
Google Cloud Platform に移動する

メールアドレスまたは電話番号

メールアドレスを忘れた場合

自分のパソコンでない場合は、プライベートウィンドウを使用してログインしてください。詳細

アカウントを作成

次へ

Google  
テスト

XXXXXXXXXXXX

パスワードを入力

パスワードを表示します

パスワードをお忘れの場合

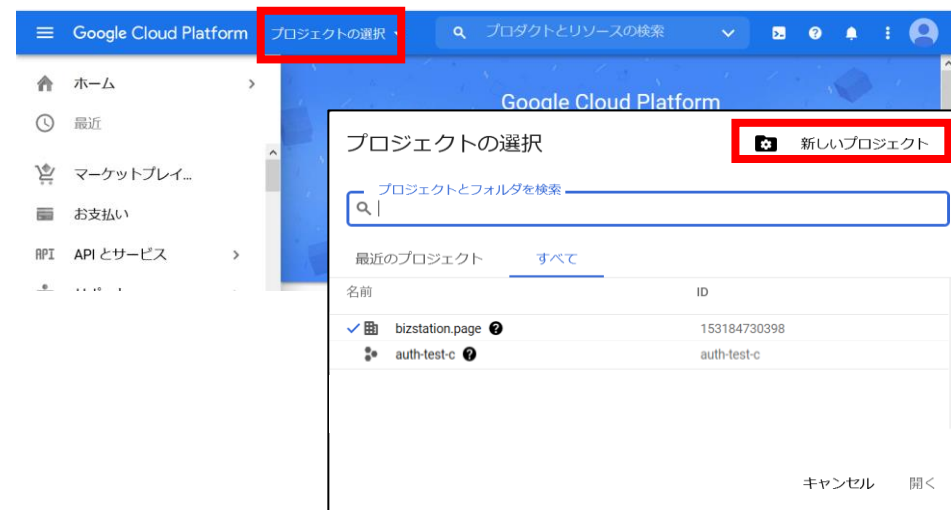
次へ



# プロジェクト作成

④ 『プロジェクト名』または『プロジェクトの選択』をクリックします。

⑤ 『新しいプロジェクト』を選択します。



⑥ 『組織』、『場所で』連携したい組織を選択します。  
※組織が作成されていない場合は組織欄が表示されません。

※注意  
Google Workspaceのユーザーのみに制限する場合は、  
Google Workspaceで所属する組織・場所を選択してください。

Google Workspaceのユーザーに制限しない場合は、  
組織・場所は任意またはなしでも問題ありません。



⑦ 『作成』をクリックします。



# Oauth 同意画面

アプリを利用できるユーザーを設定します。

- ① 先ほど作成したプロジェクトを選択します。
- ② 左の一覧にある『APIとサービス』を選択します。



- ③ 『Oauth 同意画面』をクリックしてください。

- ④ 『内部』または『外部』を選択し、作成を押してください。



- ⑤ 『Oauth 同意画面』の設定画面が表示されます。

# Oauth 同意画面

アプリを利用できるユーザーを設定します。

⑥ 『アプリ名』を入力してください。（任意文字列）

⑦ 『ユーザーサポートメール』を入力してください  
（お客さま任意メールアドレス）

⑧ 『開発者の連絡先情報』の  
『メールアドレス』を入力してください。  
（お客さま任意メールアドレス）

⑨ 『保存して次へ』をクリックしてください。

Google Cloud Platform auth-test-c

API とサービス

アプリ登録の編集

1 OAuth 同意画面 — 2 スコープ — 3 概要

アプリ情報

この情報は同意画面に表示されるため、開発者のユーザー情報と開発者への問い合わせ方法をエンドユーザーが把握できます。

アプリ名\*  
project-1016380607949  
同意を求めるアプリの名前

ユーザー サポートメール\*  
xxxxxxx@xxxx.com  
ユーザーが同意に関して問い合わせるために使用

アプリのロゴ [参照](#)

開発者の連絡先情報

メールアドレス\*  
xxxxxxx@xxxx.com  
これらのメールアドレスは、プロジェクトの変更について Google からお知らせするために使用します。

[保存して次へ](#) [キャンセル](#)

# Oauth 同意画面

⑩デフォルトの設定のまま『保存して次へ』をクリックします。

⑪Google Workspaceのユーザーに制限しない場合は、以下の画面が出てきますが、そちらも『保存して次へ』をクリックします。

Google Cloud Platform | webrc01 | プロダクトとリソースの検索

API API とサービス | アプリ登録の編集

- ダッシュボード
- ライブラリ
- 認証情報
- OAuth 同意画面**
- ドメインの確認
- ページの使用に関する契約

OAuth 同意画面 — スcope — 省略可能な情報 — 概要

アプリに関してより多くの有益な情報を Google の審査担当者に提供することによって、検証プロセスに要する期間が短縮されます。

### 省略可能な情報

過去に使用していた Google の連絡先のメールアドレスを共有する

アプリに関する最終的な詳細情報を共有してください。Google による検証に役立つ情報 (OAuth を使用するプロジェクトが他にもあればそのプロジェクト ID など) もすべて含まれます。

関連ドキュメントに追加リンクを 3 つまで指定します

**保存して次へ** キャンセル

⑫『ダッシュボードへ戻る』をクリックして終了します。

Google Cloud Platform | auth-test-c | プロダクト

API API とサービス | アプリ登録の編集

- ダッシュボード
- ライブラリ
- 認証情報
- OAuth 同意画面**
- ドメインの確認
- ページの使用に関する契約

OAuth 同意画面 — 2 スcope — 3 概要

スコープとは、アプリのユーザーに許可を求める権限を表します。スコープを定めることで、プロジェクトからユーザーの Google アカウントにある特定の種類のプライベートなユーザーデータへのアクセスが可能になります。詳細

スコープを追加または削除

### 非機密のスコープ

| API ↑       | 範囲 | ユーザー向けの説明 |
|-------------|----|-----------|
| 表示する行がありません |    |           |

### 機密性の高いスコープ

機密性の高いスコープとは、プライベート ユーザーデータへのアクセスをリクエストするスコープです。

| API ↑       | 範囲 | ユーザー向けの説明 |
|-------------|----|-----------|
| 表示する行がありません |    |           |

### 制限付きのスコープ

制限付きのスコープとは、機密性の高いユーザーデータへのアクセスをリクエストするスコープです。

| API ↑       | 範囲 | ユーザー向けの説明 |
|-------------|----|-----------|
| 表示する行がありません |    |           |

**保存して次へ** キャンセル

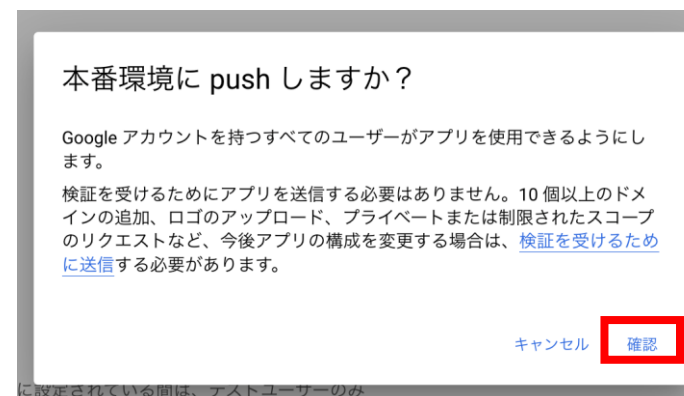
Google Workspaceのユーザーに制限しない場合のみ実施する作業です。

① 『アプリを公開』をクリックしてください。



② 『確認』をクリックしてください。

③ 『公開ステータス』が本番環境になりましたら、完成です。



# 認証情報の作成

下記の手順で認証情報の設定をしてください。

- ①左の一覧にある『APIとサービス』を選択します。
- ②『認証情報』をクリックしてください。
- ③『認証情報を作成』を選択します。
- ④『OAuth クライアント ID』を選択します。
- ⑤『アプリケーションの種類』で『ウェブアプリケーション』を選択します。



⑥名前(任意)を入力して下さい。

⑦『承認済みのリダイレクトURI』で『URIを追加』をクリックします。

⑧以下の通り入力してください

https://<弊社から通知されたドメイン>/oauth2/idpresponse

⑨『作成』をクリックしてください

## ← OAuth クライアント ID の作成

クライアント ID は、Google の OAuth サーバーで個々のアプリを識別するために使用します。アプリが複数のプラットフォームで実行される場合、それぞれに独自のクライアント ID が必要になります。詳しくは、[OAuth 2.0 の設定](#)をご覧ください。OAuth クライアントの種類の詳細

アプリケーションの種類\*  
ウェブアプリケーション

名前\*  
TEST

OAuth 2.0 クライアントの名前。この名前はコンソールでクライアントを識別するためにのみ使用され、エンドユーザーには表示されません。

❗ 下で追加する URI のドメインは、[OAuth 同意画面に承認済みドメイン](#)として自動で追加されます。

### 承認済みの JavaScript 生成元 ⓘ

ブラウザからのリクエストに使用します

+ URI を追加

### 承認済みのリダイレクト URI ⓘ

ウェブサーバーからのリクエストに使用します

+ URI を追加

Note: It may take 5 minutes to a few hours for settings to take effect

作成 キャンセル

- ⑪ 『クライアントID』と『クライアントシークレット』が表示されますのでテキストファイルに保存してください。  
(後程使用します)

## OAuth クライアントを作成しました

クライアントIDとシークレットには、常にAPIとサービスの認証情報からアクセスできます

- i** [OAuth 同意画面](#)が確認されるまで、OAuth では[プライベートデータにかかわるスコープのログイン](#)が100回までに制限されます。公開には確認プロセスが必要になる場合があり、確認プロセスには数日を要する場合があります。

クライアントID  
XXXXXXXXXXXXXXXXXXXX

クライアントシークレット  
XXXXXXXXXXXXXXXXXXXX

OK

Smart Federationの管理者として登録されているユーザーでログインしてください。

- ① 弊社より事前に通知されている  
ログインURL(https://)へアクセスしてください。  
ログイン画面が表示されます。

※ブックマークに登録しておくと次回以降はブックマークからアクセスできます。

- ② 管理者として登録されているユーザーIDを入力してください。
- ③ パスワードを入力してください。
- ④ 『Sign in』 ボタンを押してください。

The screenshot shows the login interface for docomo business and NTT BizLink. On the left, there is a 'Sign in with your corporate ID' section with a 'PublicRoom' button. On the right, there is a 'Sign in with your username and password' section. This section includes a 'Username' field (highlighted with a red box and labeled 'User IDを入力'), a 'Password' field (highlighted with a red box and labeled 'パスワードを入力'), and a 'Sign In' button. A 'Forgot your password?' link is also present. The docomo business and NTT BizLink logos are at the top.



Smart Federation管理メニューのIDプロバイダー管理からGoogleを登録します。

①管理メニューで『IDプロバイダー管理』をクリックしてください。

②IDプロバイダー追加を押下し、Googleを選択します。

IDプロバイダー追加▶

Google

AzureAD

③名前を入力します。  
(登録後は変更出来ません。)

④お客さま側でGoogleに設定いただいた『クライアントID』および『クライアントシークレット』を入力します。

⑤『送信』をクリックします。

## IDプロバイダー追加

×

必須 プロバイダー名

Google

必須 タイプ

Google

必須 クライアントID

クライアントIDを入力

必須 クライアントシークレット

クライアントシークレットを入力

キャンセル

送信

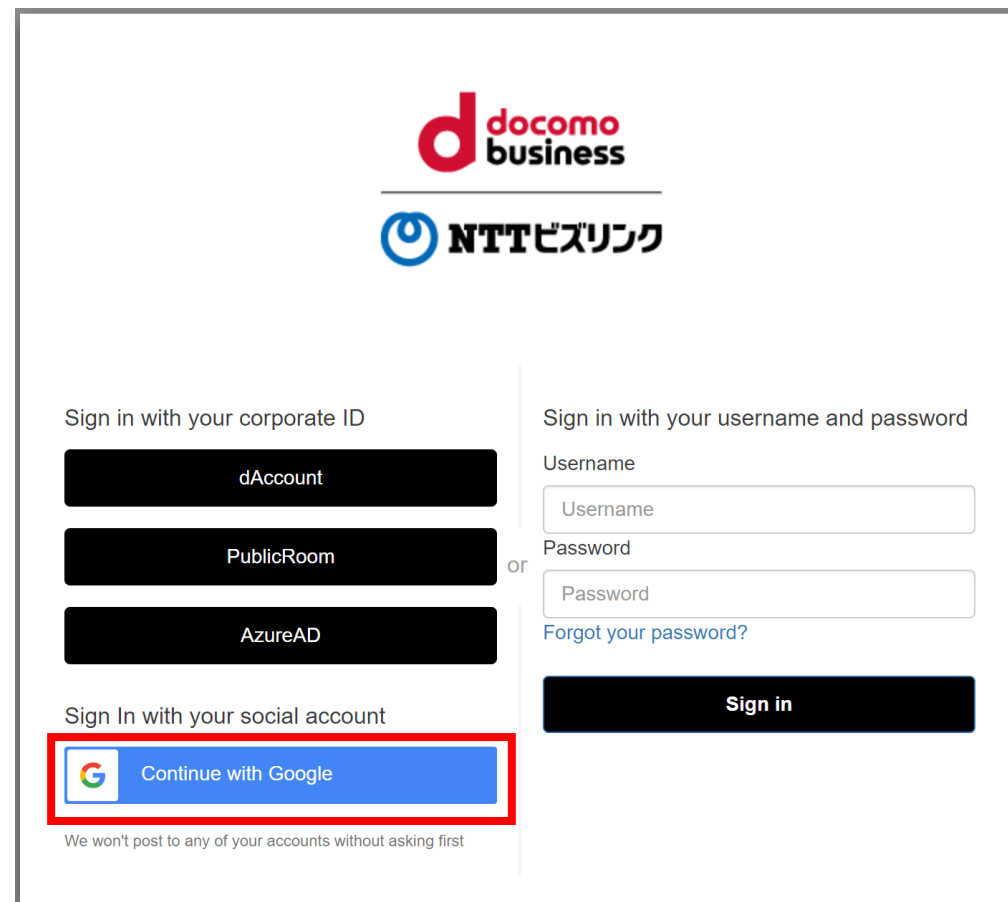
① Smart Federation ログインURLにアクセスしてください。

② 『Continue with Google』を選択し、  
Smart Federationへ登録した  
Googleのアカウントで ログインしてください。

※ Smart Federationへの登録、  
ログイン方法は以下をご参照ください。

別冊『Smart Federation管理マニュアル』

別冊『Smart Federation利用マニュアル』



docomo business

NTT BizLink

Sign in with your corporate ID

dAccount

PublicRoom

AzureAD

Sign in with your username and password

Username

Password

Forgot your password?

Sign in

Sign In with your social account

Continue with Google

We won't post to any of your accounts without asking first

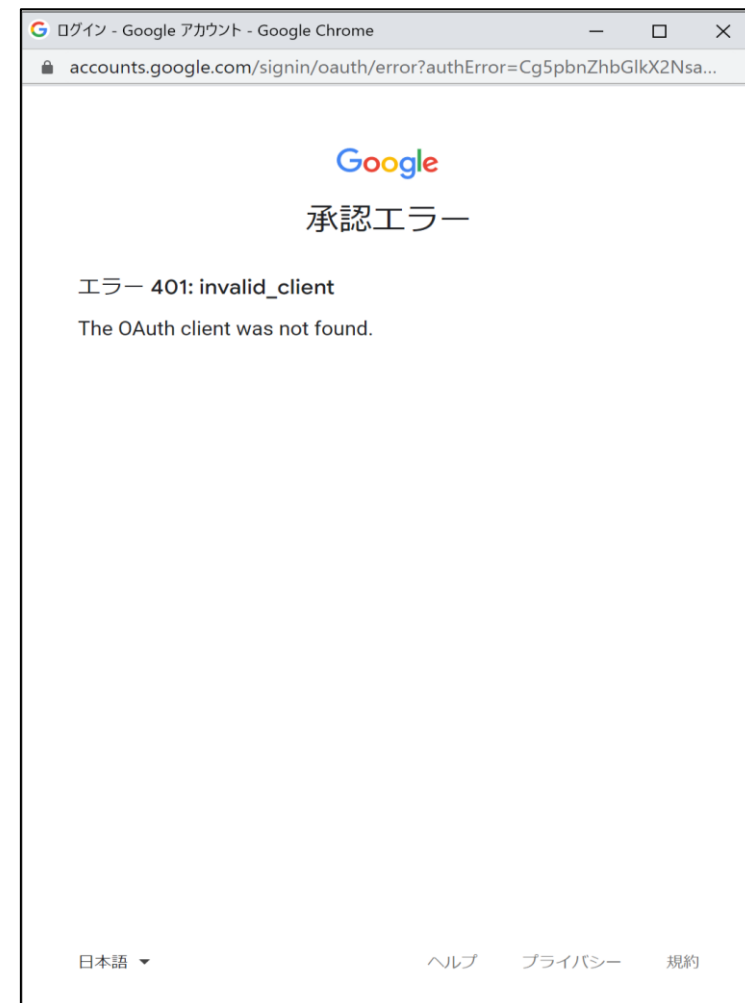
## ■クライアントIDが正しく登録されていない

Smart Federationのログイン画面にて「Googleでログイン」からSSOする際、右の画像のようなエラーが出た場合は、以下をご確認ください。

- ①Smart Federationに「クライアントID」の値が登録されていない、もしくは誤った値が登録されている可能性があります。正しい値が登録されているかどうかご確認ください。

※詳細は以下を参照してください。

本マニュアル P.34



## ■クライアントシークレットが正しく登録されていない

Smart Federationのログイン画面にて「Googleでログイン」からSSOする際、ログイン画面が再表示された場合は、以下をご確認ください。

①Smart Federationに「クライアントシークレット」の値が登録されていない、もしくは誤った値が登録されている可能性があります。正しい値が登録されているかどうかご確認ください。

※詳細は以下を参照してください。

本マニュアル P.34

The screenshot displays the login interface for docomo business and NTT BizLink. At the top, the logos for docomo business and NTTビズリンク are visible. Below the logos, there are three main sign-in sections:

- Sign in with your corporate ID:** This section contains three black buttons labeled "dAccount", "PublicRoom", and "AzureAD".
- Sign in with your social account:** This section features a blue button with the Google logo and the text "Continue with Google". Below this button, a small note reads "We won't post to any of your accounts without asking first".
- Sign in with your username and password:** This section includes a "Username" input field, a "Password" input field, a "Forgot your password?" link, and a black "Sign in" button.

The word "OR" is positioned between the corporate ID and social account sign-in sections.

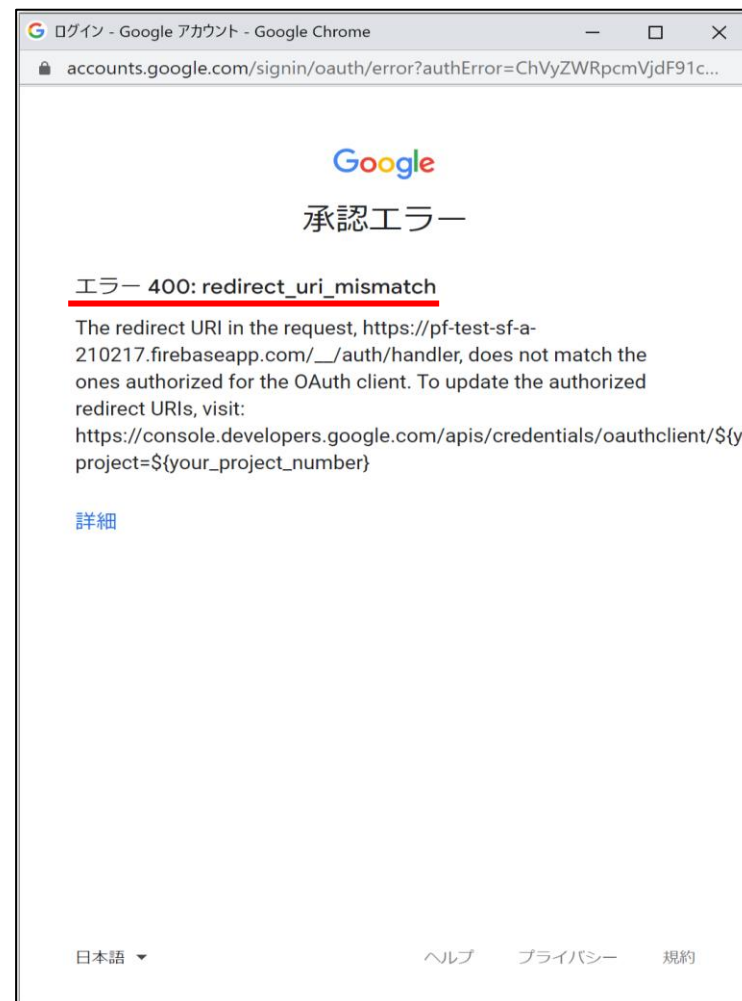
## ■ リダイレクトURIが正しく登録されていない

Smart Federationのログイン画面にて「Googleでログイン」からSSOする際、右の画像のようなエラーが出た場合は、以下をご確認ください。

- ①お客様のGoogle Cloud Platformにてご作成いただいたアプリケーションに、弊社から通知された「リダイレクトURI」の値が登録されていない、もしくは誤った値が登録されている可能性があります。正しい値が登録されているかどうかご確認ください。

※詳細は以下を参照してください。

本マニュアル P.31



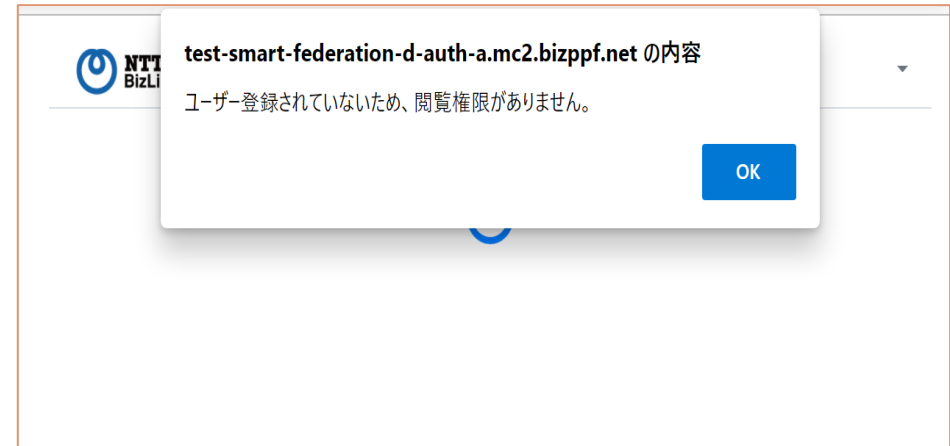
## ■ Smart Federationにアカウントが正しくユーザー登録されていない

Smart Federationのログイン画面にて「Googleでログイン」からSSOする際、右の画像のようなエラーが出た場合は、以下をご確認ください。

- ①対象のGoogleアカウントがSmart Federationに正しくユーザー登録されていない可能性があります。Smart Federation管理者サイトにアクセスし、対象のユーザーが登録されているかどうかご確認ください。

※詳細は以下を参照してください。

別冊『Smart Federation管理マニュアル』



## ■ お使いの端末がGoogle Workspaceのデバイス管理で許可されていない

お客様のGoogle Workspaceでデバイス管理設定が有効になっており、お使いの端末が許可されていない場合にもエラーが出る可能性があります。

デバイス管理設定が有効になっている場合、許可されていない端末からはログインできません。

お客様のGoogle Workspaceのデバイス管理設定でお使いの端末が許可されているかをご確認ください。

# 外部認証連携 ビジネスdアカウント編



# ドコモへのRPサイト申請

お客様がご契約中のビジネスdアカウントに、Smart Federationサイトを登録する必要があります。

弊社から通知されたdアカウントリダイレクトURLをシステム情報のリダイレクトURLの項目にご記入の上、ドコモにRPサイト申請を行ってください。

|                  |  |
|------------------|--|
| HOME/ IDプロバイダー管理 |  |
| 管理メニュー           |  |
| ユーザー管理           |  |
| dアカウントリダイレクトURL1 | https://XXXXXXXXX.amazoncognito.com/authorize-return       |
| dアカウントリダイレクトURL2 | https://smartfederation-XXXX.amazoncognito.com/idpresponse |

※dアカウントリダイレクトURLは2つ表示されますが、両方を記入の上ご申請ください

※詳しい申請方法につきましては、恐れ入りますがドコモへお問い合わせください

# ビジネスdアカウントの登録

Smart Federationの管理者として登録されているユーザーでログインしてください。

- ① 弊社より事前に通知されている  
ログインURL(https://)へアクセスしてください。  
ログイン画面が表示されます。

※ブックマークに登録しておくと次回以降はブックマークからアクセスできます。

- ② 管理者として登録されているユーザーIDを入力してください。
- ③ パスワードを入力してください。
- ④ 『Sign in』 ボタンを押してください。

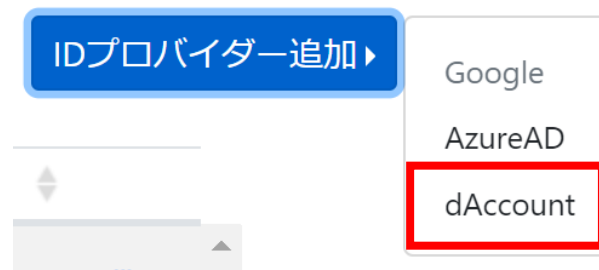
The screenshot displays the login interface for docomo business and NTT BizLink. It features two main login paths: 'Sign in with your corporate ID' (with a 'PublicRoom' button) and 'Sign in with your username and password'. The latter path includes 'Username' and 'Password' input fields, a 'Forgot your password?' link, and a 'Sign In' button. Red callout boxes highlight the 'Username' field with the instruction 'User IDを入力' and the 'Password' field with 'パスワードを入力'.

# ビジネスdアカウントの登録

Smart Federation管理メニューのIDプロバイダー管理からGoogleを登録します。

①管理メニューで『IDプロバイダー管理』をクリックしてください。

②IDプロバイダー追加を押下し、dAccountを選択します。



④ **ドコモから通知された『クライアントID』**  
および『クライアントシークレット』を入力します。

※『クライアントID』および『クライアントシークレット』  
が不明の場合は恐れ入りますがドコモにお問い合わせください

⑤『送信』をクリックします。

### IDプロバイダー追加

|    |              |                 |
|----|--------------|-----------------|
| 必須 | プロバイダー名      | dAccount        |
| 必須 | タイプ          | OIDC            |
| 必須 | クライアントID     | クライアントIDを入力     |
| 必須 | クライアントシークレット | クライアントシークレットを入力 |

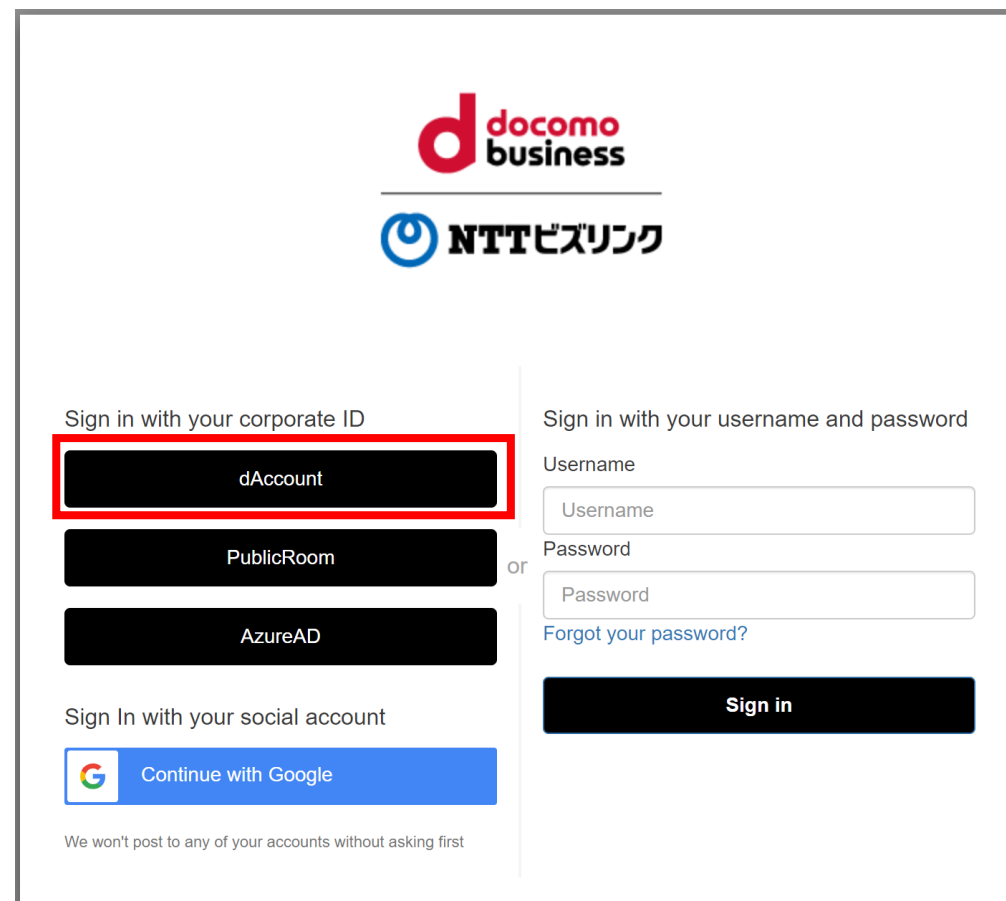
キャンセル 送信

① Smart Federation ログインURLにアクセスしてください。

② 『dAccount』を選択し、  
Smart Federationへ登録した  
dアカウントで ログインしてください。

※ Smart Federationへの登録、  
ログイン方法は以下をご参照ください。

別冊『Smart Federation管理マニュアル』  
別冊『Smart Federation利用マニュアル』



The screenshot shows the login interface for docomo business and NTT BizLink. At the top, the logos for 'docomo business' and 'NTT BizLink' are displayed. Below the logos, there are two main login sections. The left section is titled 'Sign in with your corporate ID' and contains three buttons: 'dAccount', 'PublicRoom', and 'AzureAD'. The 'dAccount' button is highlighted with a red rectangular border. The right section is titled 'Sign in with your username and password' and contains input fields for 'Username' and 'Password', a 'Forgot your password?' link, and a 'Sign in' button. At the bottom of the page, there is a section for 'Sign In with your social account' with a 'Continue with Google' button and a small disclaimer: 'We won't post to any of your accounts without asking first'.

## ■ dアカウントリダイレクトURLが正しく登録されていない

Smart Federationのログイン画面にて「dアカウントでログイン」からSSOする際、右の画像のようなエラーが出た場合は、以下をご確認ください。

- ①お客様からNTTドコモへ申請いただいたRPサイトの登録において、弊社から通知された「dアカウントリダイレクトURL1」「dアカウントリダイレクトURL2」の値が登録されていない、もしくは誤った値が登録されている可能性があります。正しい値が登録されているかどうかご確認ください。



このサイトにアクセスできません

```
https://apigateway.execute-api.ap-northeast-1.amazonaws.com/v1/oauth2/authorize?client_id=g10_0032_0001_00&redirect_uri=https%3A%2F%2Ftest-smart-federation-d-sgc1.auth.ap-northeast-1.amazonaws.com%2Foauth2%2Fidpresponse&scope=openid+accountid+email+account_info+dprofile_email+offline_access&response_type=code&state=H4slIAAAAAAAAAHVQy26DMBD8F58xsQkhWA0BzaNJo6RN26iqKmNsQAHsgBOlqfrvXXrroZfVrHZ2NDNfiKEQMY1b1ZISsN5g-nHwdvH8GswVslAG5zziXJ1bAyuHdUpO04lyRcazpiqkoswn_kk0XQOEHAilMboPRyMjQK5vWGewFLnomKlUi3PMzqbEfcGp3XDHzqqb1tJuhRlxVtcZ40e7NE0NYgLEuMoFQA lws0higAUK35DSoq1y9G6hEi5Yu5zuzsvt6rl-xfGmK2ZpZCpnHx3g4QiMu8fLy-V6LFb0EC_cdBVdEnn_nOplr2dPldrLNF0mr9vk4XNIXcPHf-5_jQ8R7L-12axhN9VyVbSVUTZXQx0NCqnnjalD_QmxkEahZHUvLNQNVRLp-owEmAgYlPlANZIHMHf8YMxzQakToO8fAYvt-qMBAAA.H4slIAAAAAAAAAAAEgAN_w6FyYOGe2htAeBiDIOox0VWktHmsvjibUerUUCmhFbG0vJe-IAAAAAA.3
```

ERR\_TUNNEL\_CONNECTION\_FAILED

## ■ クライアントIDが正しく登録されていない

Smart Federationのログイン画面にて「dアカウントでログイン」からSSOする際、右の画像のようなエラーが出た場合は、以下をご確認ください。

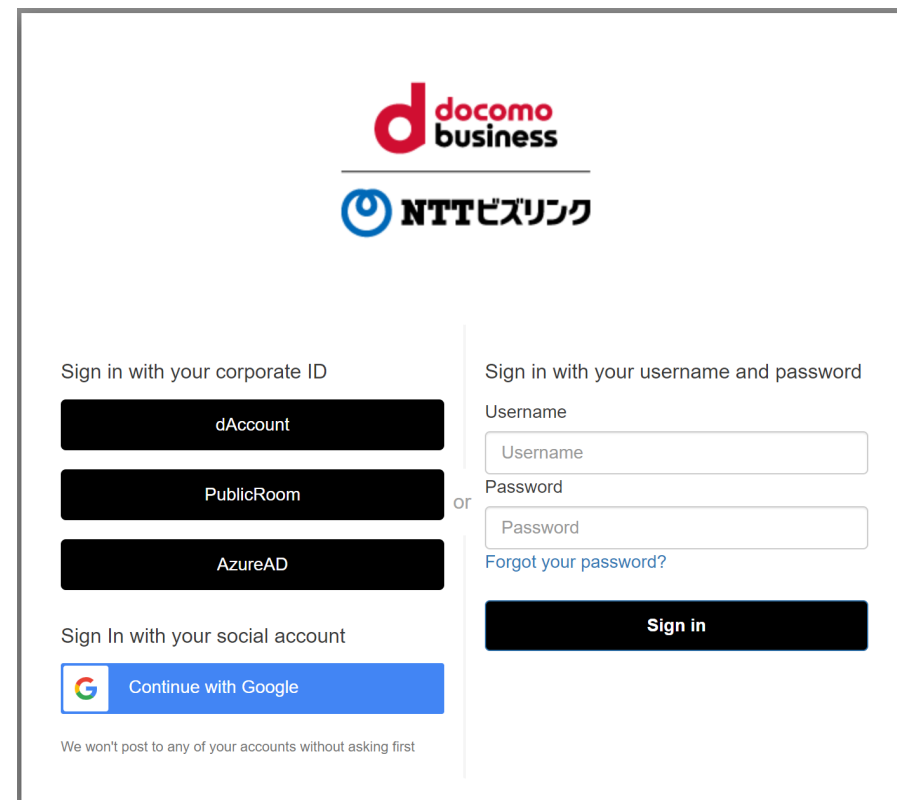
- ① Smart Federationに「クライアントID」の値が登録されていない、もしくは誤った値が登録されている可能性があります。  
正しい値が登録されているかどうかご確認ください。

正常に接続できませんでした(400)  
Invalid data.  
Connection cannot be established. (400)

## ■ クライアントシークレットが正しく登録されていない

Smart Federationのログイン画面にて「dアカウントでログイン」からSSOする際、ログイン画面が再度表示される場合は、以下をご確認ください。

- ① Smart Federationに「クライアントシークレット」の値が登録されていない、もしくは誤った値が登録されている可能性があります。  
正しい値が登録されているかどうかご確認ください。



The screenshot shows the login interface for docomo business and NTT BizLink. At the top, the logos for docomo business and NTT BizLink are displayed. Below the logos, there are two main login sections. The left section is titled "Sign in with your corporate ID" and contains three buttons: "dAccount", "PublicRoom", and "AzureAD". The right section is titled "Sign in with your username and password" and contains input fields for "Username" and "Password", a "Forgot your password?" link, and a "Sign in" button. A small "or" is placed between the two sections. At the bottom left, there is a "Sign In with your social account" section with a "Continue with Google" button. A footer note states "We won't post to any of your accounts without asking first".

## ■ Smart Federationにアカウントが正しくユーザー登録されていない

Smart Federationのログイン画面にて「dアカウントでログイン」からSSOする際、右の画像のようなエラーが出た場合は、以下をご確認ください。

- ①対象のdアカウントがSmart Federationに正しくユーザー登録されていない可能性があります。Smart Federation管理者サイトにアクセスし、対象のユーザーが登録されているかどうかご確認ください。

