Copyright © 2015 NTT DATA INTRAMART CORPORATION

目次

改訂情報

変更年月日	変更内容
2015-08-01	初版
2015-12-01	第2版　下記を追加／変更しました ■ 「*トラブルシューティング*」-「*「外部連携アプリケーション」画面で連携がうまくできない*」に事例を追加 ■ 「*付録*」-「*WebSphere Application Server 利用時の追加設定*」に最新の設定情報についての記述を追加 ■ 「*intra-mart Accel Platform をセットアップする*」-「*設定ファイルの編集*」に設定ファイルリファレンスへのリンクを追加
2017-08-01	第3版　下記を変更しました ■ Office 365 連携で提供している Files API の廃止に伴い、OneDrive API に変更
2018-12-01	第4版　下記を変更しました ■ 「*Microsoft 365 の準備* 」を最新の設定情報についての記述に変更 ■ 「*Microsoft Azure の準備* 」を最新の設定情報についての記述に変更 ■ 「*intra-mart Accel Platform をセットアップする* 」を最新の設定情報についての記述に変更 ■ 「*トラブルシューティング* 」を最新の設定情報についての記述に変更
2019-12-01	第5版　下記を変更しました ■ 「*HTTP通信のログ出力方法*」の im_logger_oauth_client_debug.xml について、immediateFlush タグを削除。
2020-08-01	第6版　下記を変更しました ■ 「*Microsoft Azure の準備* 」を最新の設定情報についての記述に変更
2022-06-01	第7版　下記を変更しました ■ 「*WebSphere Application Server 利用時の追加設定* 」で利用する証明書の取得先URLと適用手順を修正
2023-04-01	第8版　下記を変更しました ■ 「*Microsoft Azure の準備* 」を最新の設定情報についての記述に変更 ■ 「*Microsoft Azure の準備*」-「*アプリケーションを設定する*」にアクセス許可が必要な API を追加
2024-04-01	第9版　下記を変更しました ■ 名称変更のため、Office 365 を Microsoft 365、 Azure Active Directory（AzureAD） を Microsoft Entra ID に修正

はじめに

> **コラム**
>
> 「Azure Active Directory (AzureAD)」 の名称は 「Microsoft Entra ID」 に変更されました。
> https://learn.microsoft.com/entra/fundamentals/new-name
>
> 「Office 365」 の名称は 「Microsoft 365」 に変更されました。

本書の目的

本書では Office 365 連携 のセットアップ手順について説明します。

前提条件

以下の前提条件があります。

- リリースノートに記載されているシステム要件を満たしていること
  詳細は「 リリースノート 」-「 システム要件 」を参照してください。
- Microsoft 365 について理解していること

対象読者

以下の利用者を対象としています。

- Office 365 連携 のセットアップを行う方

注意事項

- 本書内で記載されている外部URLは、 2018年12月1日 現在のものです。
- 本書内の Microsoft 365 、 Microsoft Azure に関する説明は 2024年4月1日 現在のものです。

概要

項目

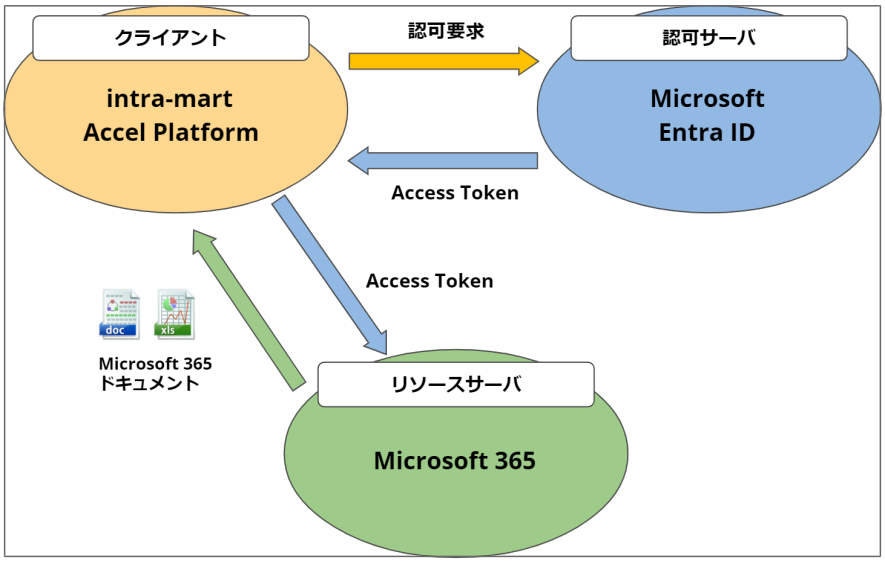
Office 365 連携 について

Office 365 連携 は OAuth2.0 を利用し、 intra-mart Accel Platform 上で Microsoft 365 のリソースの利用を可能にする機能です。

例えば、以下の様な機能が利用可能です。

- Microsoft 365 の SharePoint Online の OneDrive API を intra-mart Accel Platform 上から利用可能にする

OAuth2.0では、認可サーバ、リソースサーバ、クライアントの3つの役割が定義されています。
Office 365 連携 は例として以下のような構成で構築します。



> **コラム**
>
> OAuth 2.0 の仕様については以下を参照してください。
>
> - **The OAuth 2.0 Authorization Framework**
>   - 1.1. Roles : http://tools.ietf.org/html/rfc6749#section-1.1
>   - 1.2. Protocol Flow : http://tools.ietf.org/html/rfc6749#section-1.2

アクター

本書では以下のように定義します。

- **intra-mart Accel Platform システム管理者**
  intra-mart Accel Platform 環境の管理者
- **Microsoft Azure 管理者**
  Microsoft Azure 環境の管理者
- **Microsoft 365 管理者**
  Microsoft 365 環境の管理者

セットアップの手順について

セットアップは以下の手順で行います。

- 「*4. Microsoft 365 の準備*」
- 「*5. Microsoft Azure の準備*」
- 「*6. intra-mart Accel Platform をセットアップする*」
- 「*7. 動作確認（連携を行う）*」

Microsoft 365 の準備

Office 365 連携 に必要な関連サービスの準備を行います。
本項の内容は **Microsoft 365 管理者** 向けの作業です。
すでに構築が完了している項目は省略可能です。

項目

> **注意**
>
> Microsoft 365、Microsoft Azure についての詳細は Microsoft社 のドキュメントを参照してください。

Microsoft 365 の利用を開始する

以下のURLより、Microsoft 365 サブスクリプションアカウントを取得してください。

- https://products.office.com/ja-jp/business/office

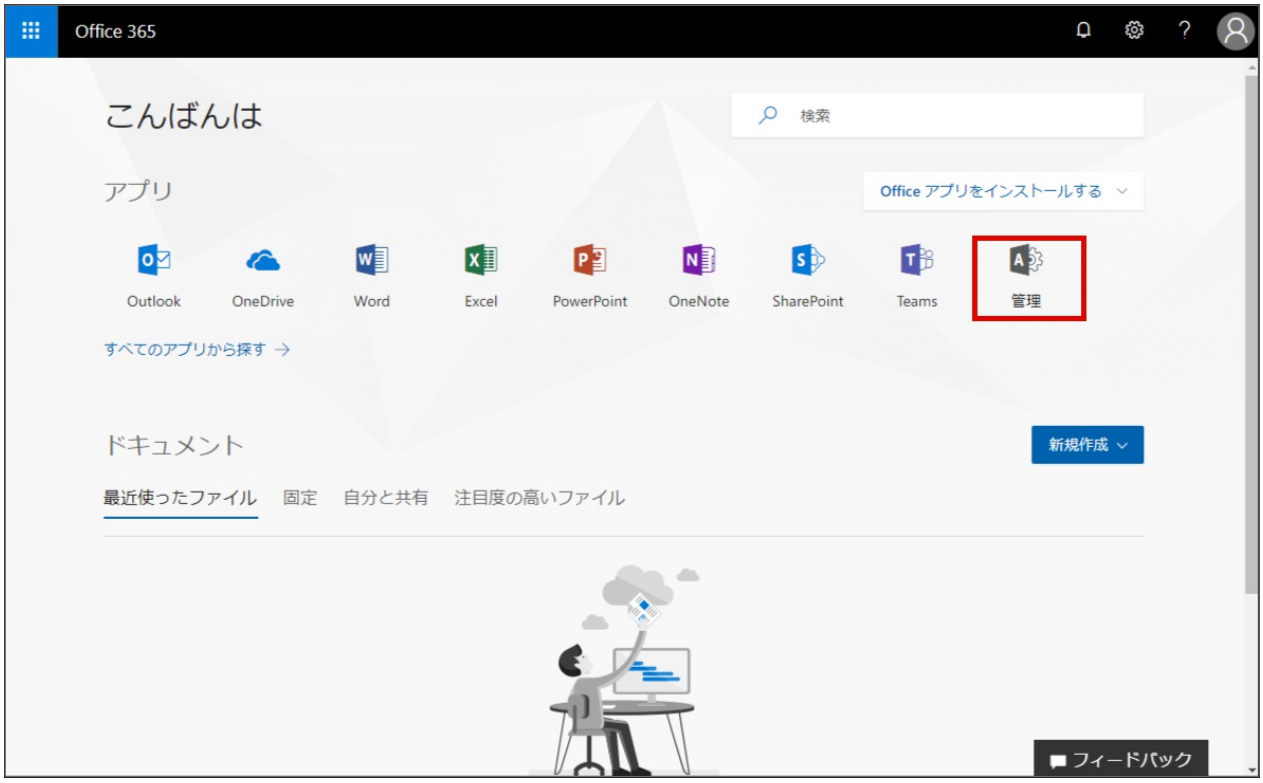
ここで取得したアカウントを **Microsoft 365 管理者ユーザ** とします。
ここで取得したMicrosoft 365のテナント名 は、 Microsoft Azure 管理者、 intra-mart Accel Platform システム管理者 が行う環境構築の際に利用します。
Microsoft 365のテナント名とは以下のように@の右側の部分を指します。

- <ユーザID>@<Microsoft 365のテナント>.onmicrosoft.com

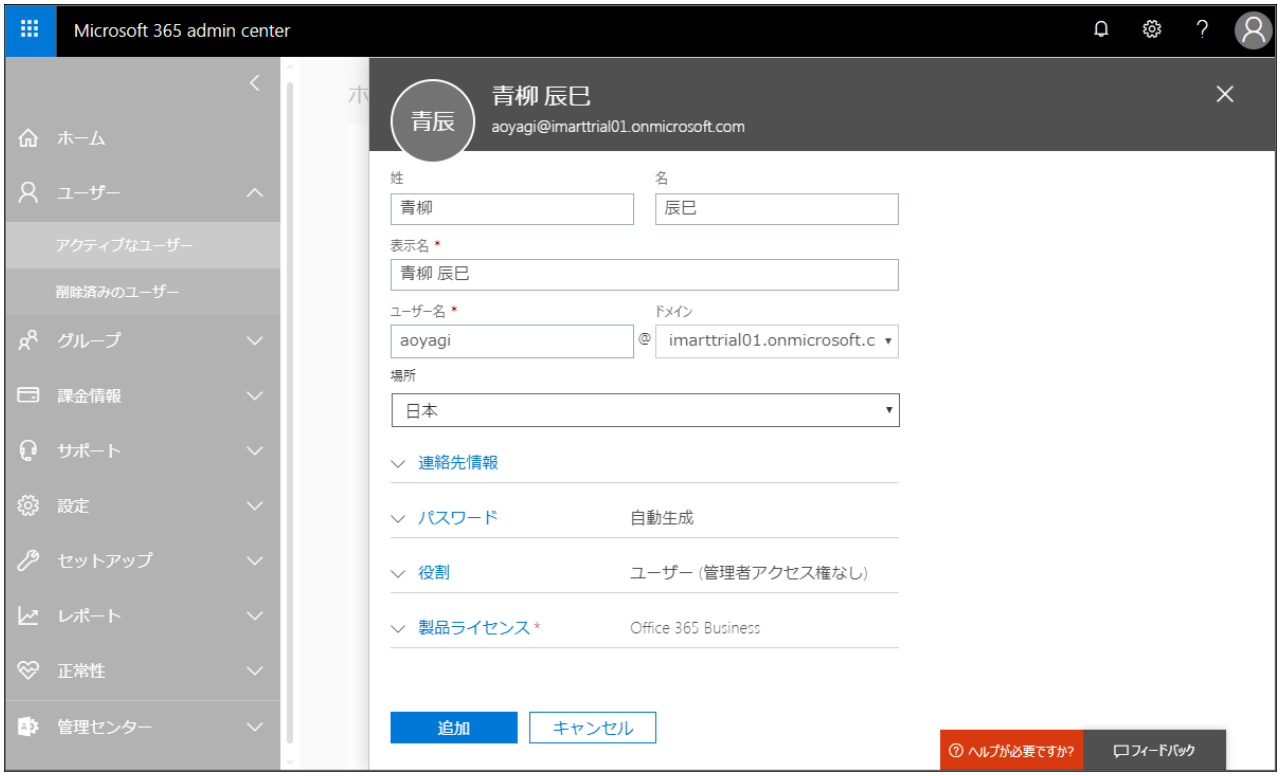
Microsoft 365 にユーザを登録する

Microsoft 365 で ユーザを作成します。
intra-mart Accel Platform 上の各ユーザに対応するユーザが必要です。
通常、intra-mart Accel Platform 上で Office 365 連携 を行うユーザごとに Microsoft 365 のユーザが必要です。

1. 以下のURLより Microsoft 365 ポータルに **Microsoft 365 管理者ユーザ** でサインインし、管理センターを表示します。
   - https://portal.office.com
2. アプリ「管理者」をクリックします。



3. サイドメニューの「ユーザ」-「アクティブなユーザ」の「ユーザの追加」より intra-mart Accel Platform との連携に利用するユーザを作成します。



Microsoft Azure の準備

Office 365 連携 に必要な関連サービスの準備を行います。
本項の内容は **Microsoft Azure 管理者** 向けの作業です。
「*Microsoft 365 の利用を開始する*」で取得した Microsoft 365 サブスクリプションアカウントを Microsoft Azure 管理者 とします。
すでに、 Microsoft Azure アカウントを保持しており、そのアカウントを Microsoft Azure 管理者 として扱う場合は、以下の「*すでに存在する Microsoft Azure 管理者ユーザから Microsoft 365 の組織のディレクトリを参照可能にする*」を行ってください。

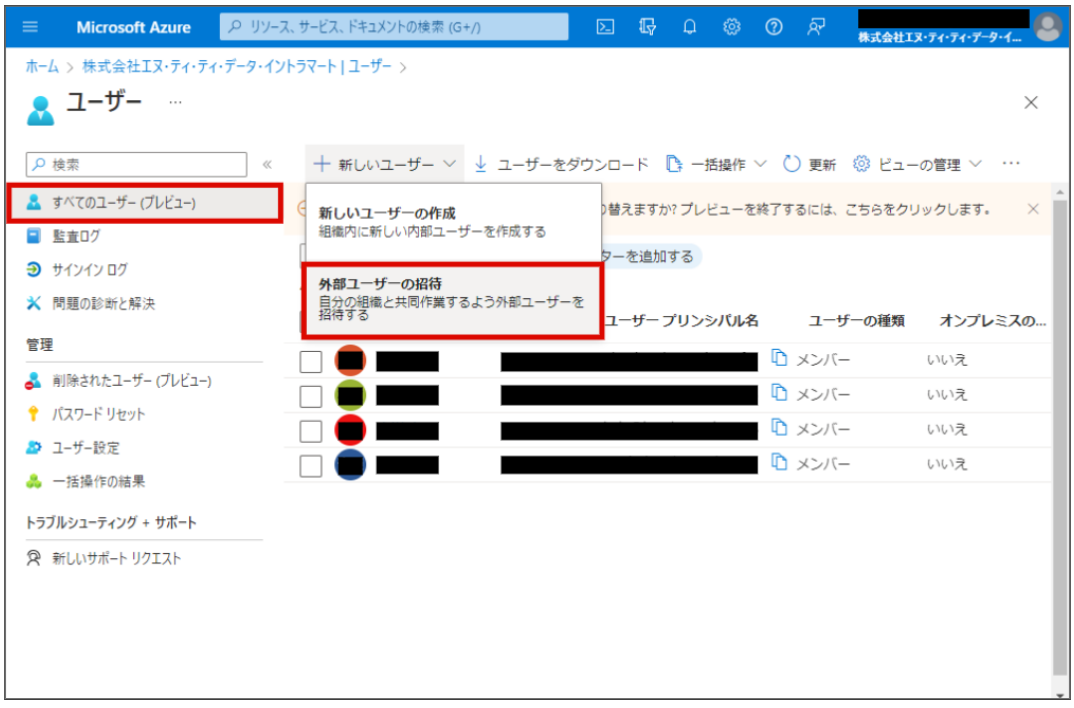
項目

注意
Microsoft 365、Microsoft Azure についての詳細は Microsoft社 のドキュメントを参照してください。

すでに存在する Microsoft Azure 管理者ユーザから Microsoft 365 の組織のディレクトリを参照可能にする

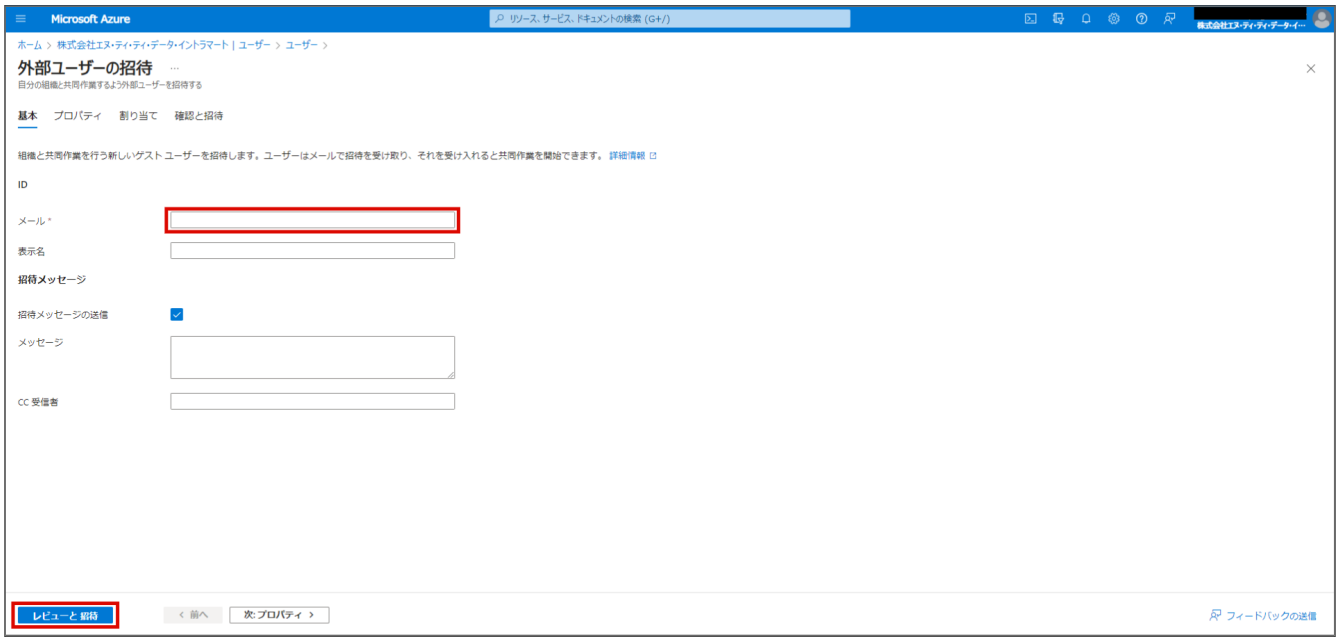
Microsoft 365 管理者ユーザ により、すでに存在する Microsoft Azure アカウントに対して Microsoft 365 の組織のディレクトリへのアクセスを行えるようにします。
以降、この Microsoft Azure アカウントを Microsoft Azure 管理者 とします。
「*Microsoft 365 の利用を開始する*」で取得した Microsoft 365 サブスクリプションアカウントを Microsoft Azure 管理者 として利用する場合、この手順は不要です。

1. 以下のURLから Microsoft Azure の管理ポータルに Microsoft 365 管理者ユーザ でサインインします。
   - https://portal.azure.com/
2. サイドメニュー「Microsoft Entra ID」をクリックします。
3. 「管理」の「ユーザー」をクリックします。
4. 「すべてのユーザー」の「新しいユーザー」をクリックして、「外部ユーザーの招待」をクリックします。



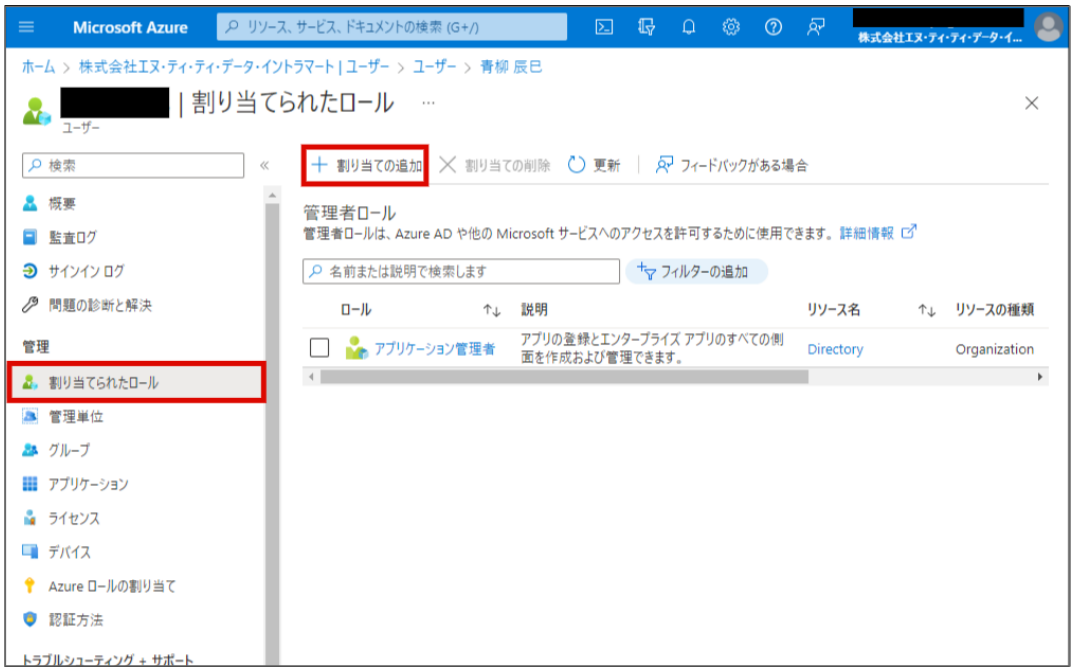
5. 「ユーザーの招待」を選択します。
6. Microsoft Azure 管理者ユーザ の情報を入力し、「レビューと招待」をクリックし、「確認と招待」タブから「招待」をクリックします。

「メール」は Microsoft Azure 管理者ユーザ のメールアドレスを入力してください。



> **コラム**
>
> プロパティタブから、ユーザ情報を設定できます。
> ロールタブから、後述するロールの割り当てを行うことができます。

7. 「すべてのユーザー」から追加されたユーザをクリックします。
8. 「管理」の「割り当てられたロール」をクリックして「割り当ての追加」をクリックし、「アプリケーション管理者」を追加します。



9. Microsoft Azure 管理者ユーザ は、招待メールを確認して Microsoft 365 の組織のディレクトリに対してのアクセス許可を承諾してください。

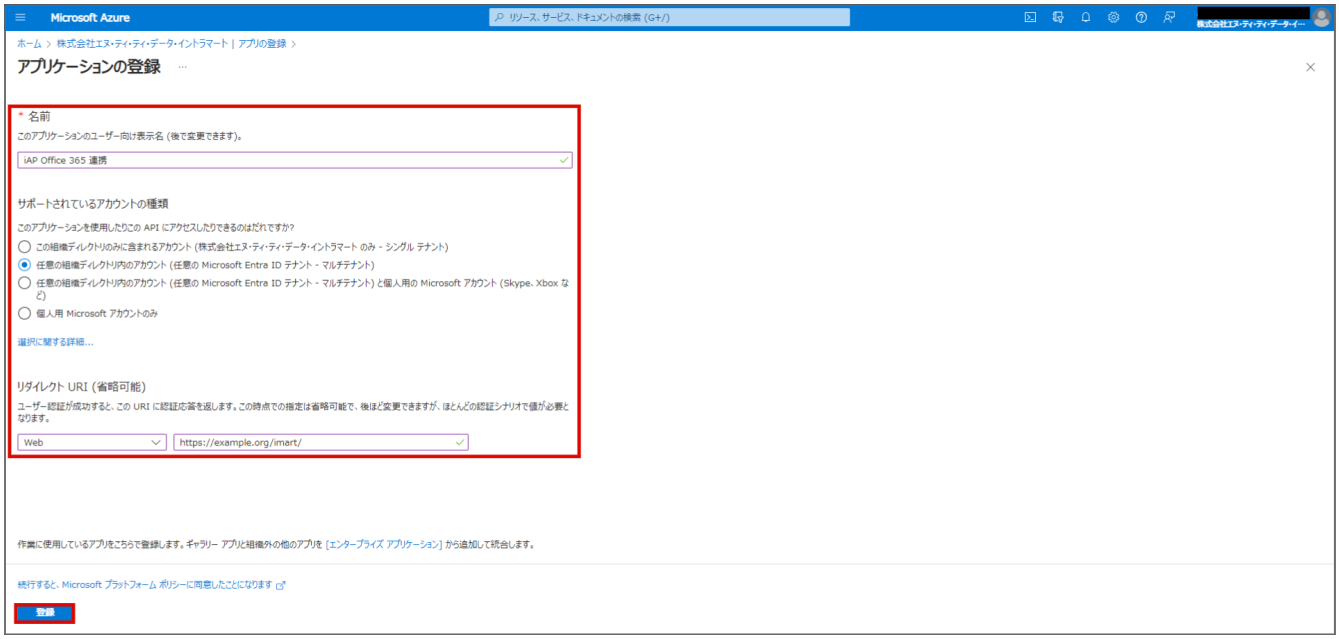
ディレクトリにアプリケーションを設定する

アプリケーションを登録する

Microsoft Azure の管理ポータルから Office 365 連携 に必要な情報をアプリケーションとして登録します。

1. 以下のURLから Microsoft Azure の管理ポータルに **Microsoft Azure 管理者ユーザ** でサインインします。
   - https://portal.azure.com/

2. サイドメニューから「Microsoft Entra ID」をクリックします。
3. 現在のディレクトリが「 Microsoft 365 の組織のディレクトリ」ではない場合は「ディレクトリの切り替え」を行います。
4. 「概要」のサイドメニュー「管理」の「アプリの登録」をクリックします。
5. 「新規登録」をクリックします。
6. 以下を入力または選択して「登録」をクリックします。
   - 名前に任意の名称を入力
   - サポートされているアカウントの種類に「任意の組織ディレクトリ内のアカウント（任意の Microsoft Entra ID テナント - マルチテナント）」を選択
   - リダイレクト URI に「Web」を選択し、 intra-mart Accel Platform のベースURL を入力



7. 以上でアプリケーションの登録は完了です。

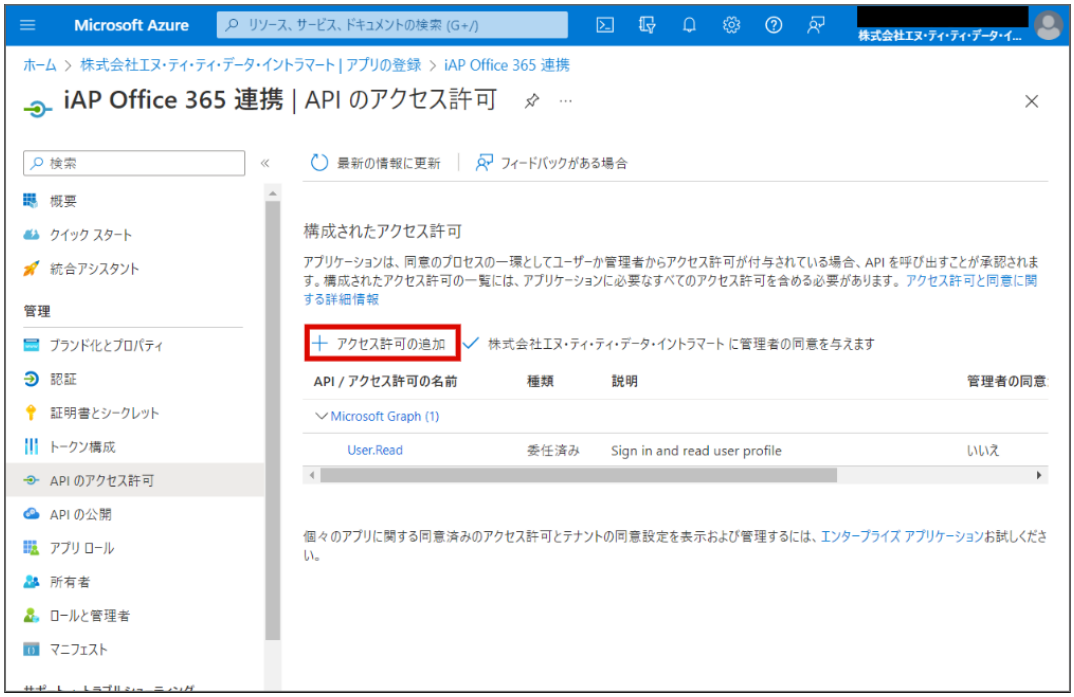
アプリケーションを設定する

Microsoft Azure の管理ポータルから登録したアプリケーションの構成を変更します。

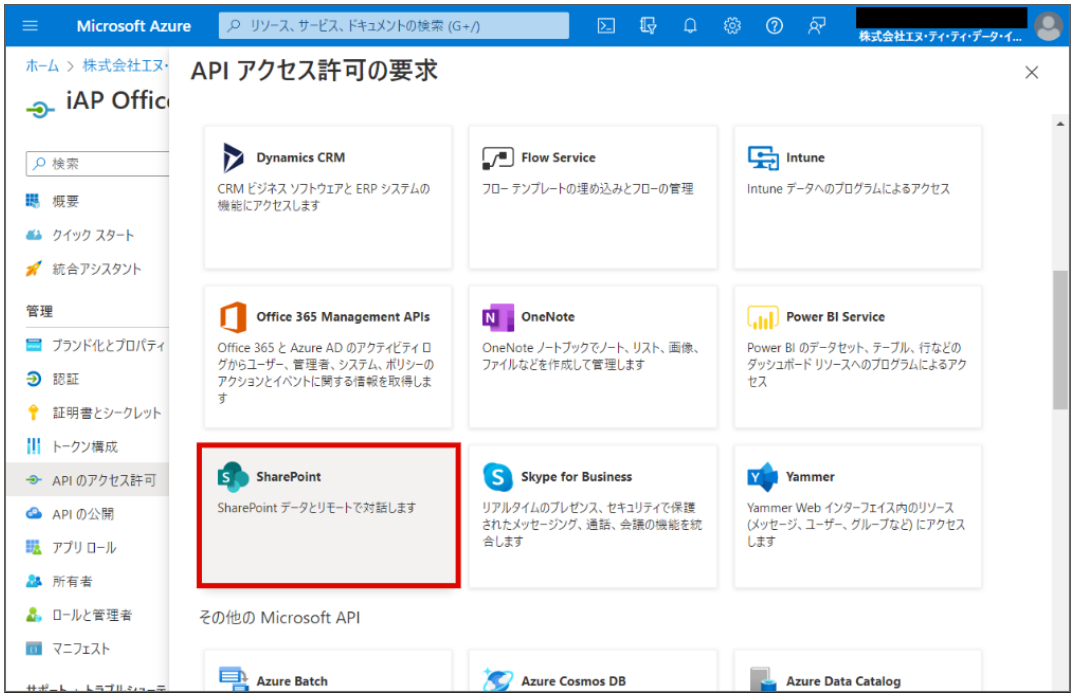
1. 先程登録したアプリの「管理」の「認証」をクリックします。
2. 「リダイレクト URL」の値を **ベースURL + /oauth/redirect** に変更して「保存」をクリックします。

3. 「管理」の「APIのアクセス許可」をクリックします。

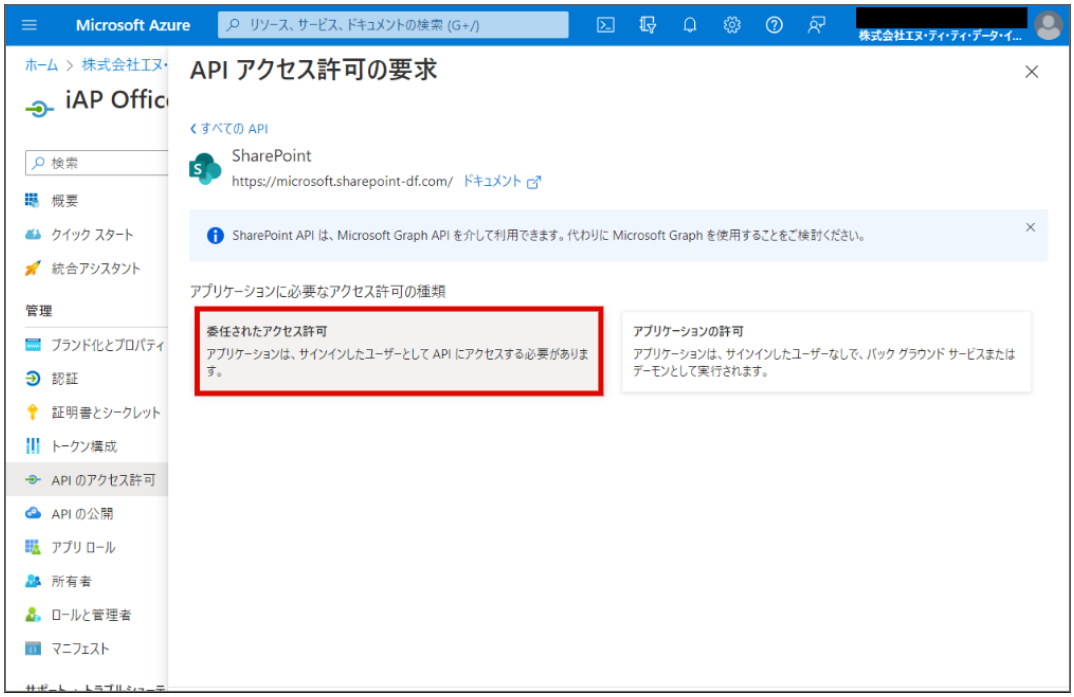
4. 「アクセス許可の追加」をクリックします。



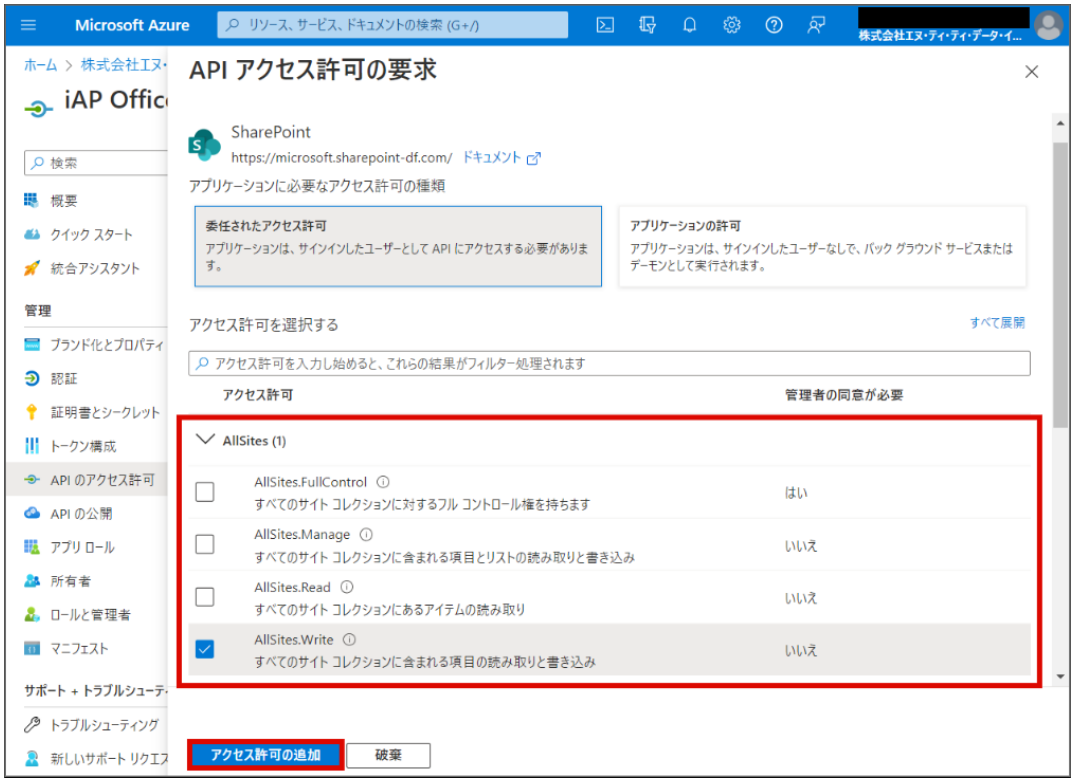
5. 「 SharePoint 」をクリックします。



6. 「アプリケーションに必要なアクセス許可の種類」の「委任されたアクセス許可」をクリックします。

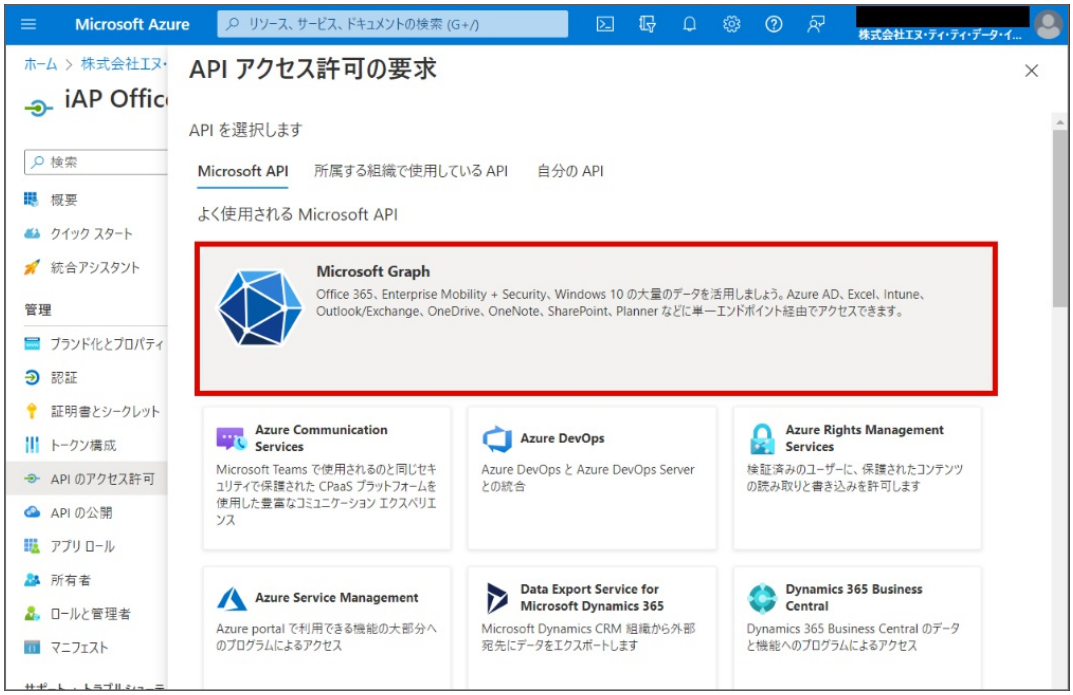


7. 「AllSites」をクリックし、「AllSites.Write」を選択し、「アクセス許可の追加」をクリックします。

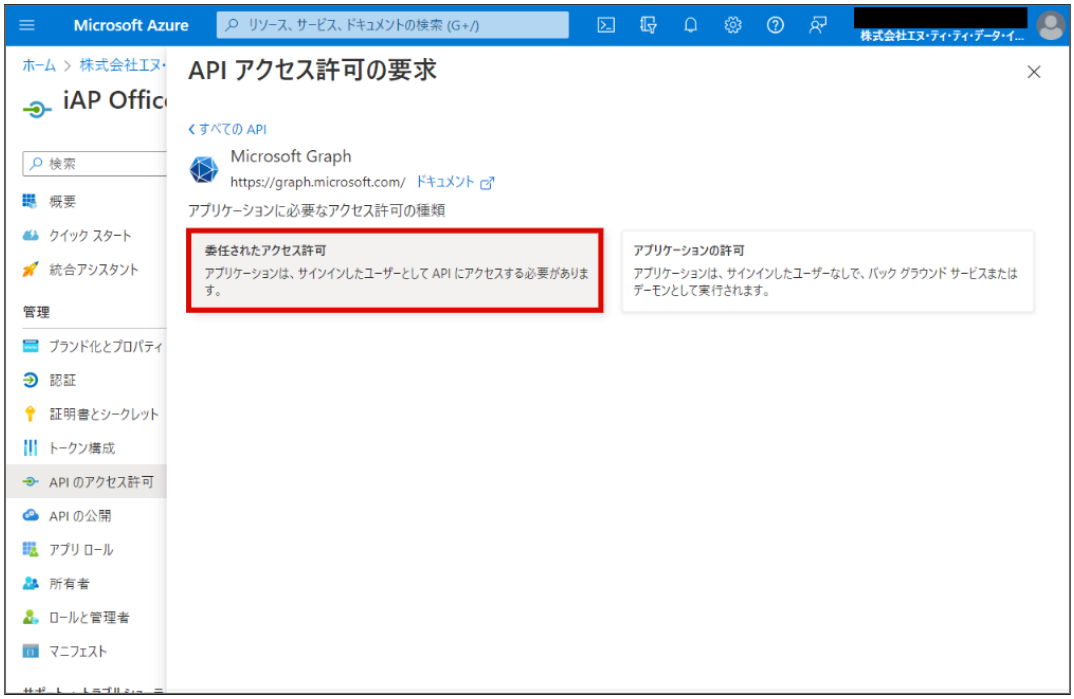


8. 「 構成されたアクセス許可 」の一覧に、「 Microsoft Graph 」に対する「User.Read」のアクセス許可がない場合は追加します。
「アクセス許可の追加」をクリックします。

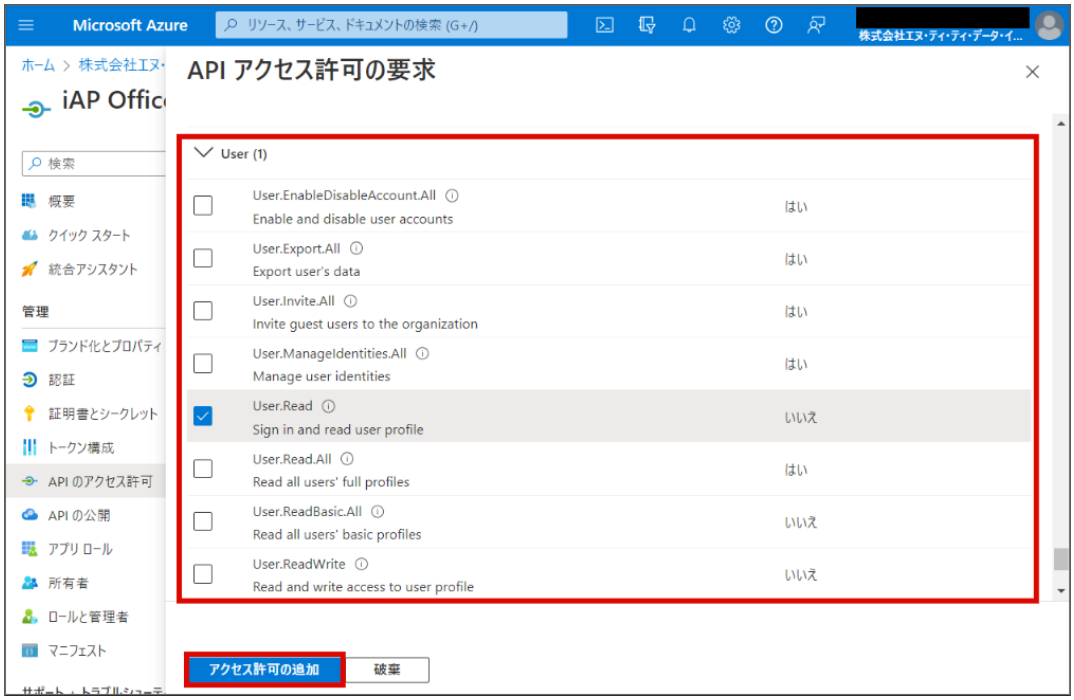
9. 「 Microsoft Graph 」をクリックします。



10. 「アプリケーションに必要なアクセス許可の種類」の「委任されたアクセス許可」をクリックします。

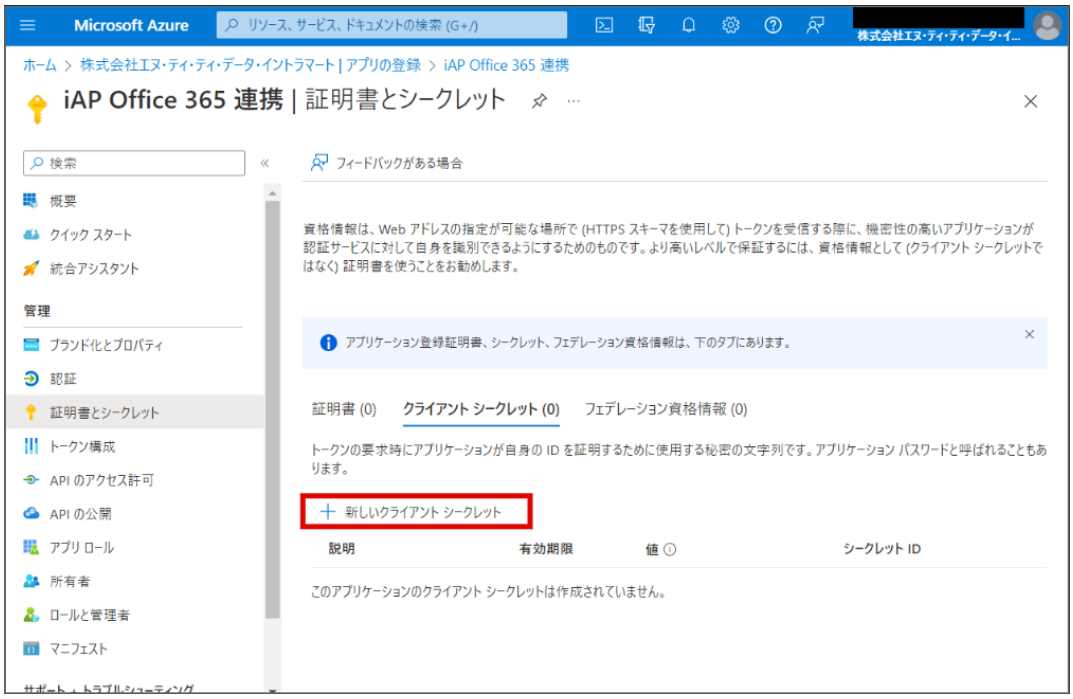


11. 「User」をクリックし、「User.Read」を選択し、「アクセス許可の追加」をクリックします。

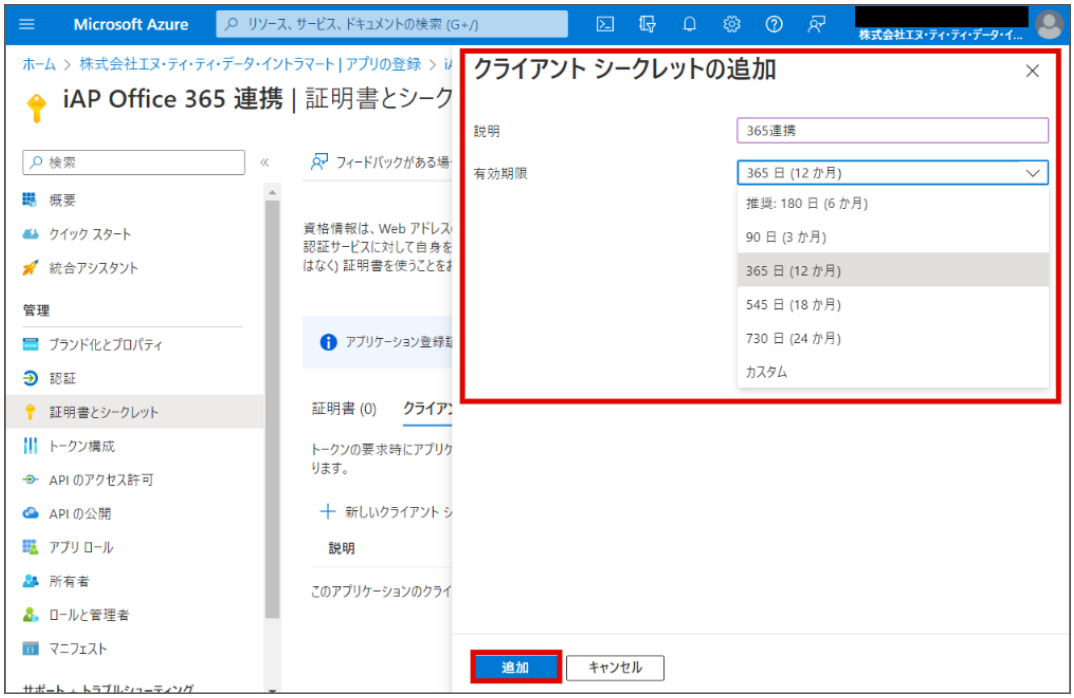


> **コラム**
>
> 「APIアクセス」の「アクセスの有効化」にて「委任されたアクセス許可」における Microsoft 365 SharePoint Online の許可設定についての詳細は Microsoft社 の以下のドキュメントを参照してください。
>
> - Microsoft Graph permissions reference :
>   - https://docs.microsoft.com/en-us/graph/permissions-reference （English）
>   - https://docs.microsoft.com/ja-jp/graph/permissions-reference （日本語）
>   - https://docs.microsoft.com/zh-cn/graph/permissions-reference （中文）

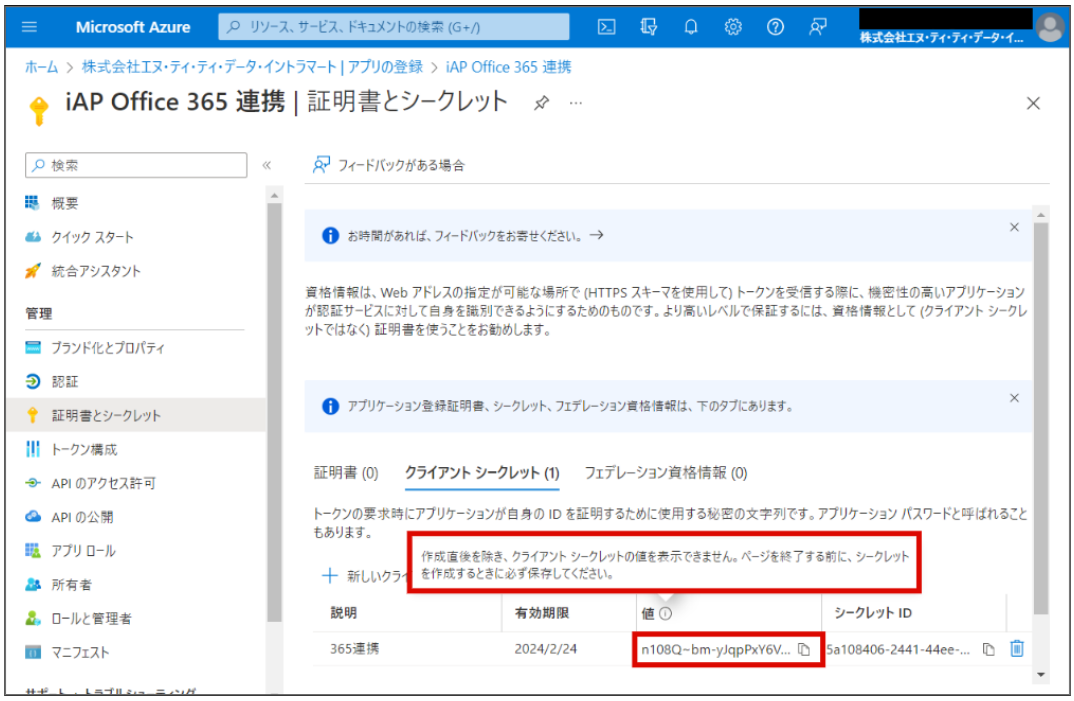
12. 「管理」の「証明書とシークレット」をクリックします。
13. 「クライアント シークレット」の「新しいクライアント シークレット」をクリックします。



14. intra-mart Accel Platform からアクセスする際に必要なキーを生成します。
    以下を入力または選択して「追加」をクリックします。
    - 説明に任意のキーの説明を入力
    - 有効期間に任意のキーの有効期限を選択



> **注意**
> キーは設定の保存後に一度のみ表示されます。移動前にキーの表示内容を退避させてください。



> **コラム**
> 有効期限が切れた場合は、上記の手順でキーを再発行する必要があります。

15. 以上でアプリケーションの設定が完了です。
    以下の内容は intra-mart Accel Platform システム管理者 が環境構築を行う際に利用します。
    - アプリケーションID （クライアントIDとして利用します）
    - キー（**設定の保存後に一度のみ表示されます**）

intra-mart Accel Platform をセットアップする

intra-mart Accel Platform システム管理者 向けの作業です。
intra-mart Accel Platform のセットアップは 「intra-mart Accel Platform セットアップガイド」 を参照してください。
ここでは追加で必要な手順を説明します。

項目

Web Application Server の設定

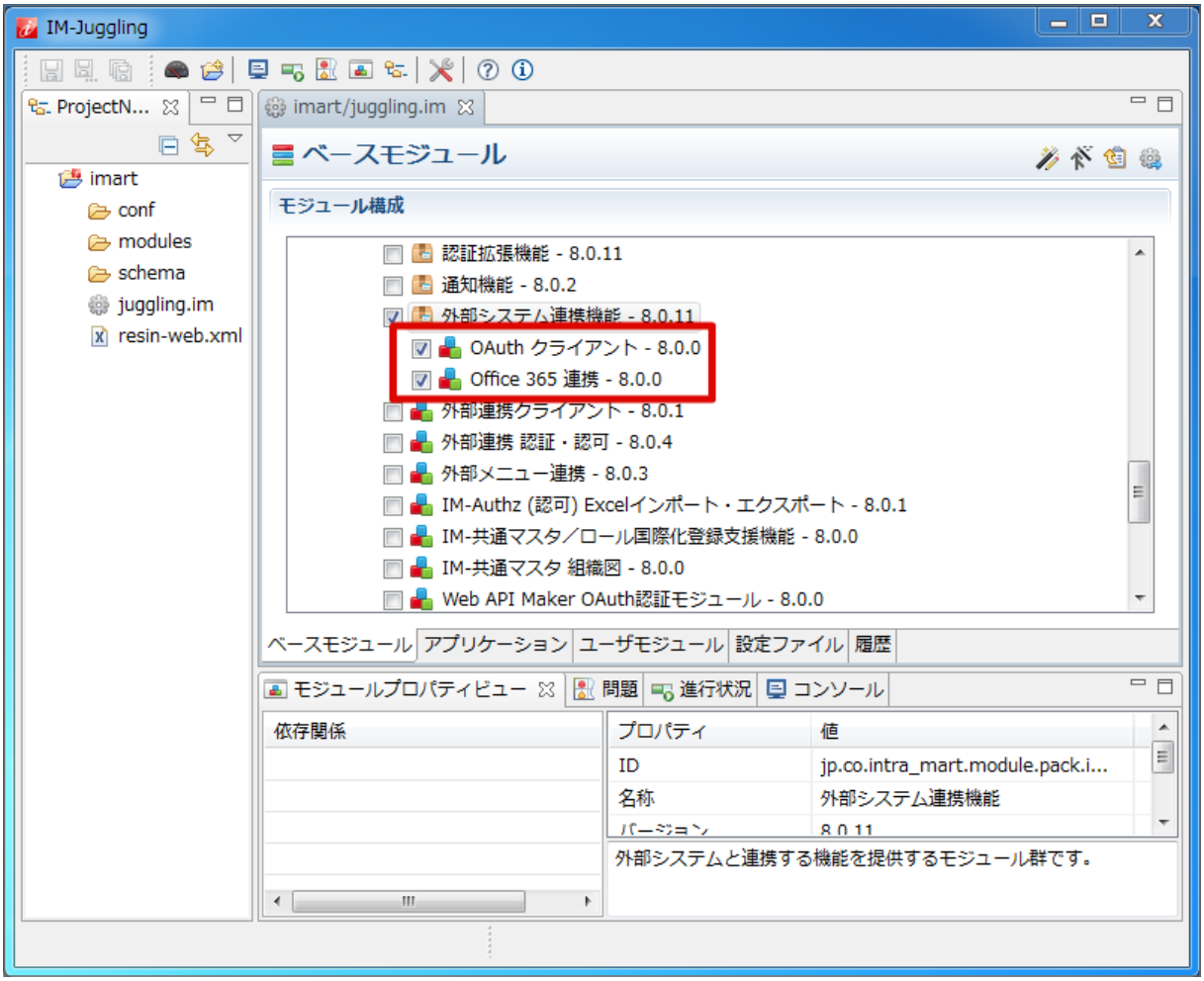
Web Application Server に WebSphere Application Server を利用する場合、 SharePoint Online を使用する際に以下のSSL証明書の認証問題が発生します。

- https://support.microsoft.com/en-us/help/2842146/you-experience-ssl-certificate-authentication-issues-when-you-use-shar （English）
- https://support.microsoft.com/ja-jp/help/2842146/you-experience-ssl-certificate-authentication-issues-when-you-use-shar （日本語）
- https://support.microsoft.com/zh-cn/help/2842146/you-experience-ssl-certificate-authentication-issues-when-you-use-shar （中文）

設定方法は「*WebSphere Application Server 利用時の追加設定*」を参照してください。

モジュールの選択

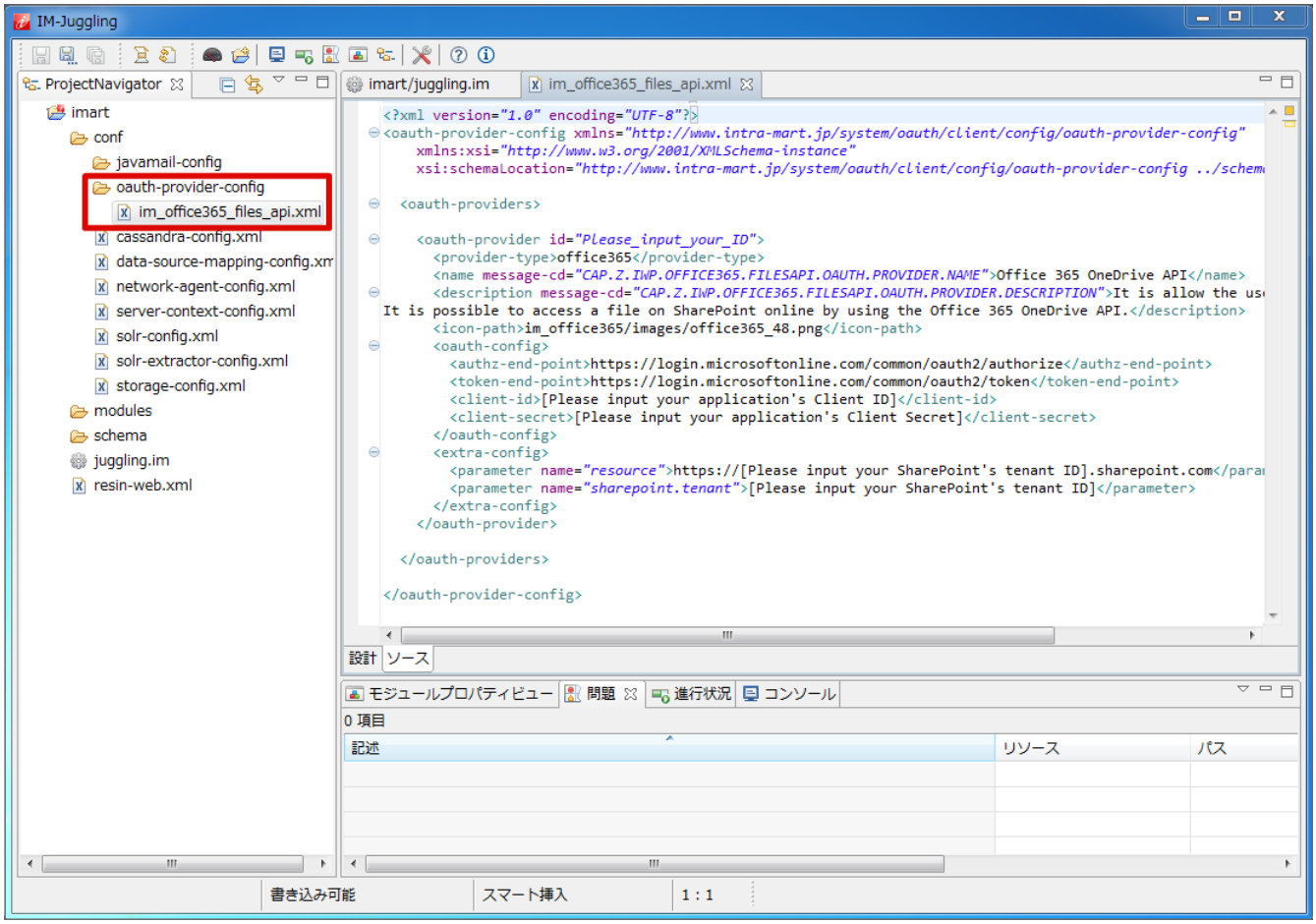
「intra-mart Accel Platform セットアップガイド」-「プロジェクトの作成とモジュールの選択」より、 Office 365 連携 , OAuth クライアント を選択します。



設定ファイルの編集

Office 365 連携 を利用するための設定ファイルを編集します。
設定ファイルの詳細については、「設定ファイルリファレンス」-「 プロバイダ設定」 を参照してください。

1. 「ProjectNavigator」内の <（プロジェクト名）/oauth-provider-config/im_office365_files_api.xml> ファイルをダブルクリックで開き、「ソース」タブを選択してください。
   利用する Microsoft 365 の環境に合わせた設定情報を記述します。




```
<?xml version="1.0" encoding="UTF-8"?>
<oauth-provider-config xmlns="http://www.intra-mart.jp/system/oauth/client/config/oauth-provider-config"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="http://www.intra-mart.jp/system/oauth/client/config/oauth-provider-config ../schema/oauth-provider-config.xsd ">

 <oauth-providers>

   <oauth-provider id="Please_input_your_ID">
    <provider-type>office365</provider-type>
    <name message-cd="CAP.Z.IWP.OFFICE365.FILESAPI.OAUTH.PROVIDER.NAME">Office 365 OneDrive API</name>
    <description message-cd="CAP.Z.IWP.OFFICE365.FILESAPI.OAUTH.PROVIDER.DESCRIPTION">It is allow the use of the Office 365 OneDrive API.
It is possible to access a file on SharePoint online by using the Office 365 OneDrive API.</description>
    <icon-path>im_office365/images/office365_48.png</icon-path>
    <oauth-config>
     <authz-end-point>https://login.microsoftonline.com/common/oauth2/authorize</authz-end-point>
     <token-end-point>https://login.microsoftonline.com/common/oauth2/token</token-end-point>
     <client-id>[Please input your application's Client ID]</client-id>
     <client-secret>[Please input your application's Client Secret]</client-secret>
    </oauth-config>
    <extra-config>
     <parameter name="resource">https://[Please input your SharePoint's tenant ID].sharepoint.com</parameter>
     <parameter name="sharepoint.tenant">[Please input your SharePoint's tenant ID]</parameter>
    </extra-config>
   </oauth-provider>

 </oauth-providers>

</oauth-provider-config>
```

プロバイダ設定

任意のプロバイダIDを指定してください。

```
<oauth-provider id="yourcompany.onmicrosoft.com">
  ・・・
</oauth-provider>
```

> **コラム**
>
> 以下のように intra-mart Accel Platform の 対象のテナントIDを指定することも可能です。
> テナントIDは半角スペースで区切って記載してください。
>
> ```
> <oauth-provider id="yourcompany.onmicrosoft.com" target-tenant="default secondary">
>   ・・・
> </oauth-provider>
> ```

OAuth設定

client-id、client-secret には Microsoft Azure 管理者 が「*アプリケーションを設定する*」で取得したクライアントID、キーをそれぞれ指定してください。

```
<oauth-provider id="yourcompany.onmicrosoft.com">
  ・・・
  <oauth-config>
    <authz-end-point>https://login.microsoftonline.com/common/oauth2/authorize</authz-end-point>
    <token-end-point>https://login.microsoftonline.com/common/oauth2/token</token-end-point>
    <client-id>623d6fb4-8761-4cff-a763-bfbbc3c780f2</client-id>
    <client-secret>rGg/kuwrGwBHx/IUyKL5izxcp9NTIMQeXMtePicJox0=</client-secret>
    <scope></scope>
  </oauth-config>
  ・・・
</oauth-provider>
```

追加設定（SharePoint）

Office 365 の OneDrive API の場合は以下のように設定します。
resource パラメータには、https://< Microsoft 365 のテナント>.sharepoint.com となるように指定します。
sharepoint.tenant パラメータに以下のように Office 365 の OneDrive API の操作対象となる Microsoft 365 のテナントを指定します。

```
<oauth-provider id="yourcompany.onmicrosoft.com">
  ・・・
  <extra-config>
    <parameter name="resource">https://yourcompany.sharepoint.com</parameter>
    <parameter name="sharepoint.tenant">yourcompany</parameter>
  </extra-config>
</oauth-provider>
```

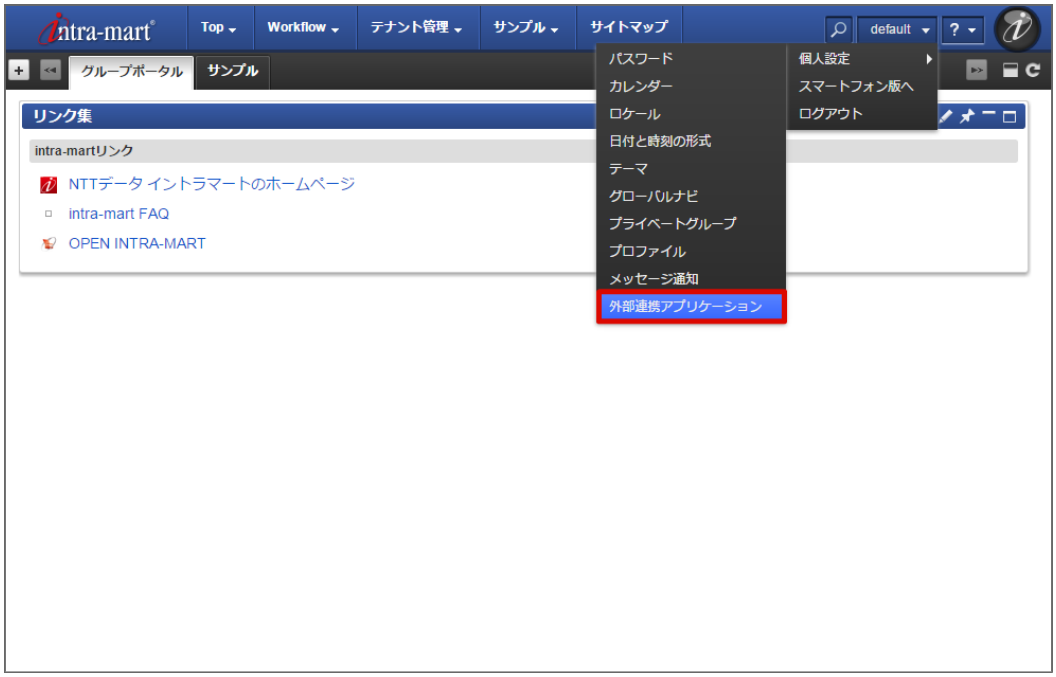
テナント環境セットアップ

- テナント環境セットアップについては、「intra-mart Accel Platform セットアップガイド」-「テナント環境セットアップ」を参照してください。

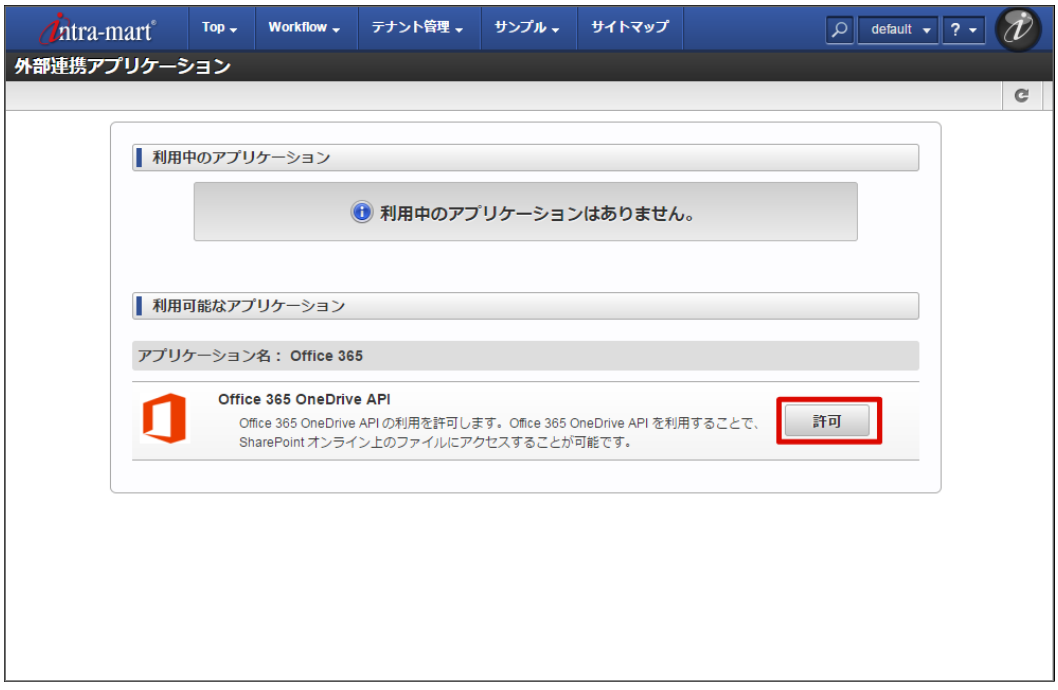
動作確認（連携を行う）

intra-mart Accel Platform システム管理者 向けの作業です。
intra-mart Accel Platform のユーザで Microsoft 365 のユーザ と連携をします。

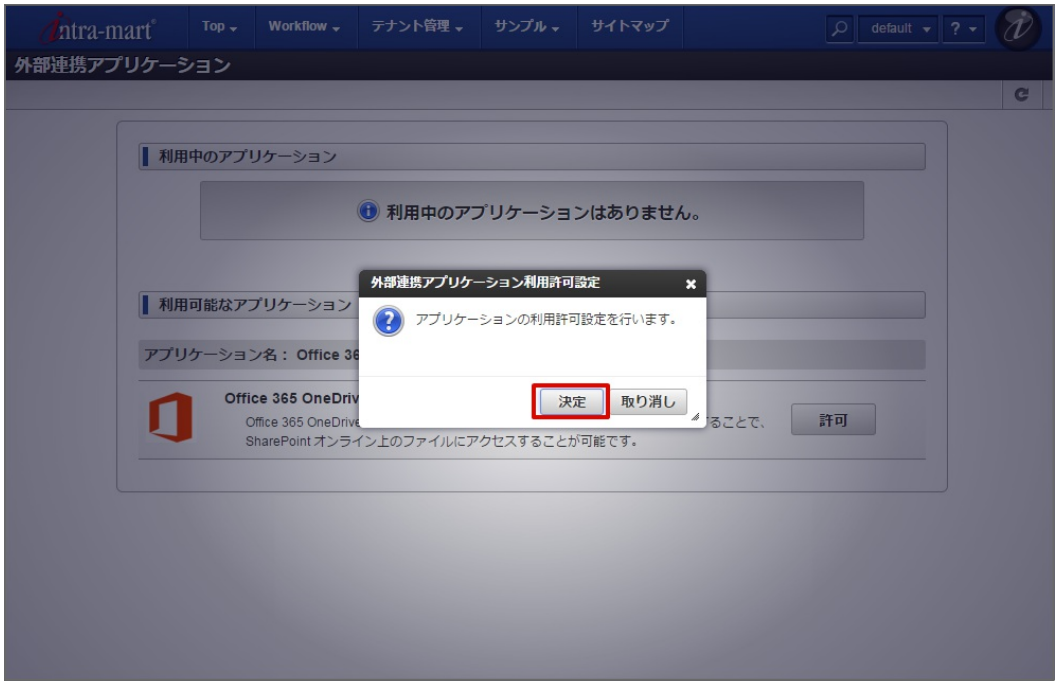
1. 任意のユーザで intra-mart Accel Platform にログインしてください。
2. ユーティリティメニューより、「個人設定」-「外部連携アプリケーション」を選択します。



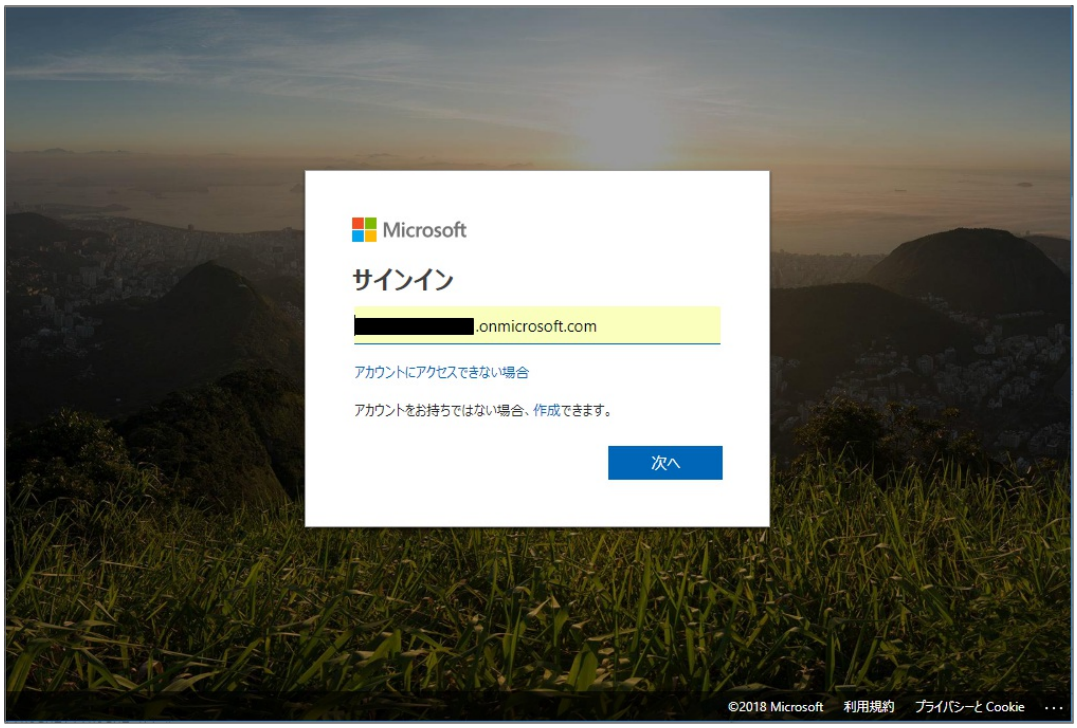
3. 「Office 365 OneDrive API」 の「許可」をクリックします。



4. 「決定」をクリックします。



5. Microsoft 365 の認証画面に遷移します。
   Microsoft 365 のユーザアカウントでサインインします。



6. サインインが完了し、以下の画面が表示されれば連携が完了します。


intra-mart
Top
Workflow
テナント管理
サンプル
サイトマップ
default
外部連携アプリケーション
「Office 365 OneDrive API」の利用を許可しました。
利用中のアプリケーション
アプリケーション名： Office 365
Office 365 OneDrive API
Office 365 OneDrive API の利用を許可します。Office 365 OneDrive API を利用することで、SharePoint オンライン上のファイルにアクセスすることが可能です。
解除
利用可能なアプリケーション
利用可能なアプリケーションはありません。

連携を解除するには

Office 365 連携 の解除は以下の手順で行います。

項目
- 設定ファイルの編集

設定ファイルの編集

intra-mart Accel Platform システム管理者 向けの作業です。

ファイル	場所
im_office365_files_api.xml	WEB-INF/conf/oauth-provider-config

```
<?xml version="1.0" encoding="UTF-8"?>
<oauth-provider-config xmlns="http://www.intra-mart.jp/system/oauth/client/config/oauth-provider-config"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xsi:schemaLocation="http://www.intra-mart.jp/system/oauth/client/config/oauth-provider-config ../schema/oauth-provider-config.xsd ">

 <oauth-providers>

   <!--
   <oauth-provider id="Please_input_your_ID">
    <provider-type>office365</provider-type>
    <name message-cd="CAP.Z.IWP.OFFICE365.FILESAPI.OAUTH.PROVIDER.NAME">Office 365 OneDrive API</name>
    <description message-cd="CAP.Z.IWP.OFFICE365.FILESAPI.OAUTH.PROVIDER.DESCRIPTION">It is allow the use of the Office 365 OneDrive API.
It is possible to access a file on SharePoint online by using the Office 365 OneDrive API.</description>
    <icon-path>im_office365/images/office365_48.png</icon-path>
    <oauth-config>
     <authz-end-point>https://login.microsoftonline.com/common/oauth2/authorize</authz-end-point>
     <token-end-point>https://login.microsoftonline.com/common/oauth2/token</token-end-point>
     <client-id>[Please input your application's Client ID]</client-id>
     <client-secret>[Please input your application's Client Secret]</client-secret>
    </oauth-config>
    <extra-config>
     <parameter name="resource">https://[Please input your SharePoint's tenant ID].sharepoint.com</parameter>
     <parameter name="sharepoint.tenant">[Please input your SharePoint's tenant ID]</parameter>
    </extra-config>
   </oauth-provider>
   -->

 </oauth-providers>

</oauth-provider-config>
```

上記のように <im_office365_files_api.xml> ファイルから、連携を解除したい Microsoft 365 の<oauth-provider>の設定を取り除いてください。
修正後 intra-mart Accel Platform を再起動してください。

トラブルシューティング

Office 365 連携 機能の利用中に発生するトラブルと対応方法を紹介します。対象の事象リンクをクリックして確認してください。

「外部連携アプリケーション」画面で連携がうまくできない

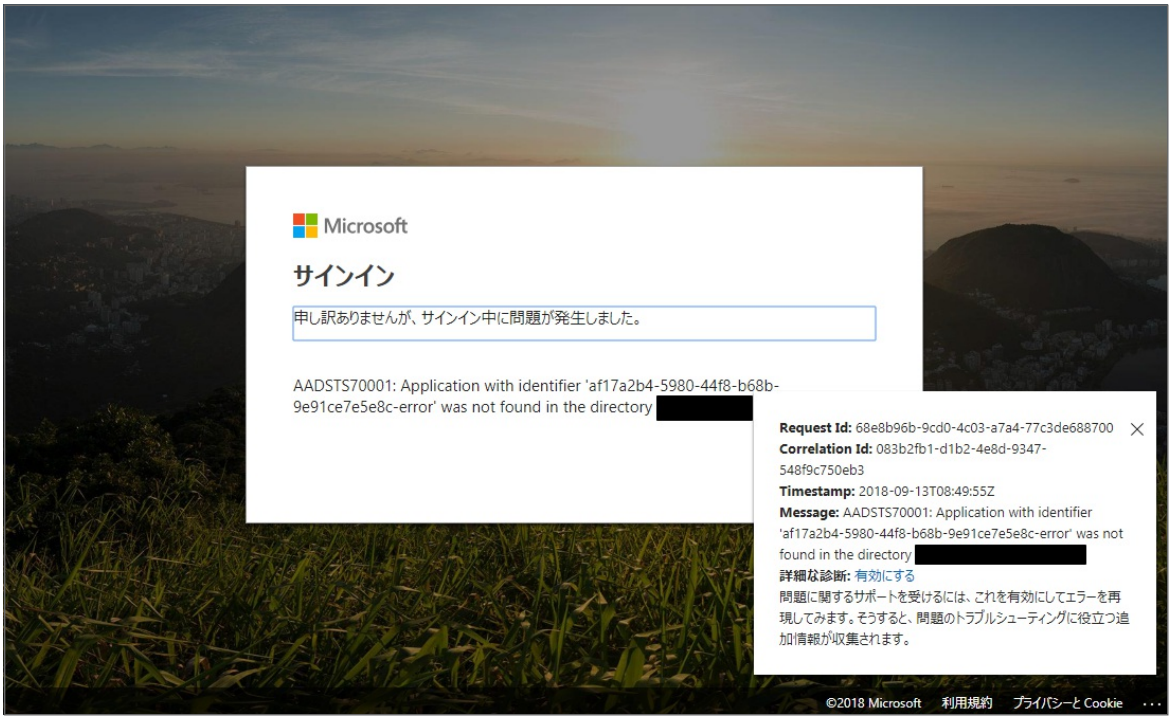
項目

「AADSTS70001: Application with identifier <クライアントID> was not found in the directory <Microsoft 365のテナントID >.onmicrosoft.com」が発生します

現象

「個人設定」-「外部連携アプリケーション」画面で「許可」ボタンクリック後、Microsoftのサインイン画面下部に以下が出力されます。

AADSTS70001: Application with identifier <クライアントID> was not found in the directory <Microsoft 365のテナントID >.onmicrosoft.com The reply url specified in the request does not match the reply urls configured for the application



原因

設定ファイルに記載したクライアントIDが間違っている可能性があります。
または Microsoft Entra ID 上に作成したアプリケーションの構成の「 マルチテナント 」が「いいえ」になっている可能性があります。

対応方法

設定ファイルに記載したクライアントIDが正しいかを確認してください。
クライアントIDの確認方法は「 *アプリケーションを設定する* 」を参照してください。設定ファイルについては「 *設定ファイルの編集* 」を参照してください。
または「マルチテナント」を「はい」に変更してください。
設定箇所については「*アプリケーションを設定する* 」を参照してください。

「不正なレスポンスを受け取りました。」が発生します

現象

「個人設定」-「外部連携アプリケーション」画面で「許可」ボタンクリック後、 intra-mart Accel Platform の画面上で「不正なレスポンスを受け取りました。」というエラーメッセージが表示されます。

原因

SecureTokenが不正である可能性があります。

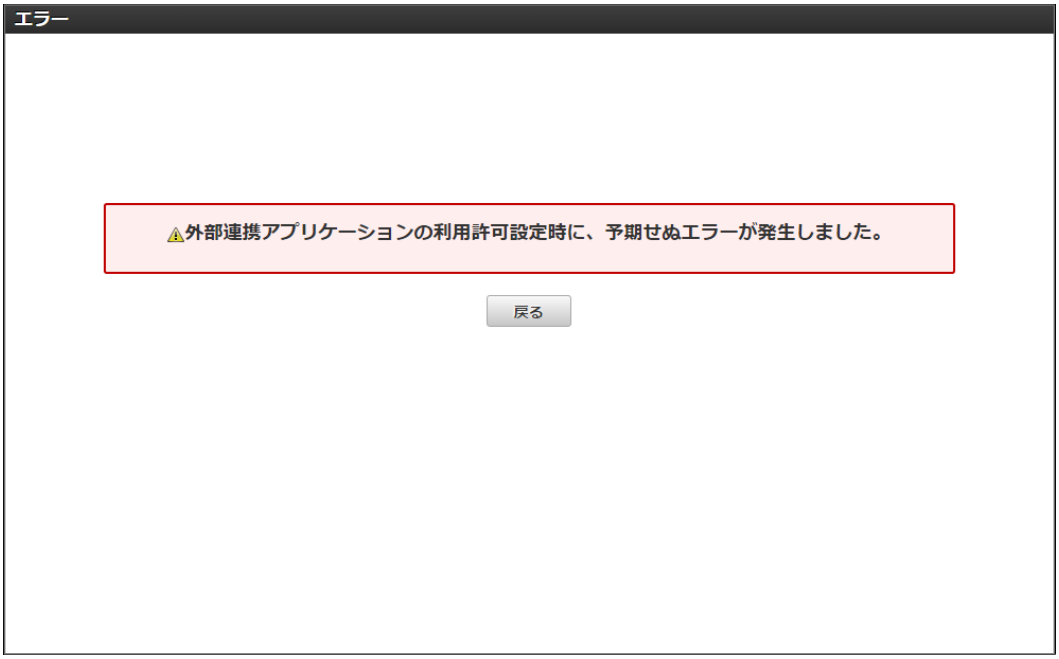
対応方法

ログアウトを実行し、再度ログイン後に実行してください。

「外部連携アプリケーションの利用許可設定時に、予期せぬエラーが発生しました。」が発生します

現象

「個人設定」-「外部連携アプリケーション」画面で「許可」ボタンクリック後、 intra-mart Accel Platform の画面上で「外部連携アプリケーションの利用許可設定時に、予期せぬエラーが発生しました。」というエラーメッセージが表示されます。



原因

外部連携アプリケーションの利用許可を行うための通信に失敗している可能性があります。

対応方法

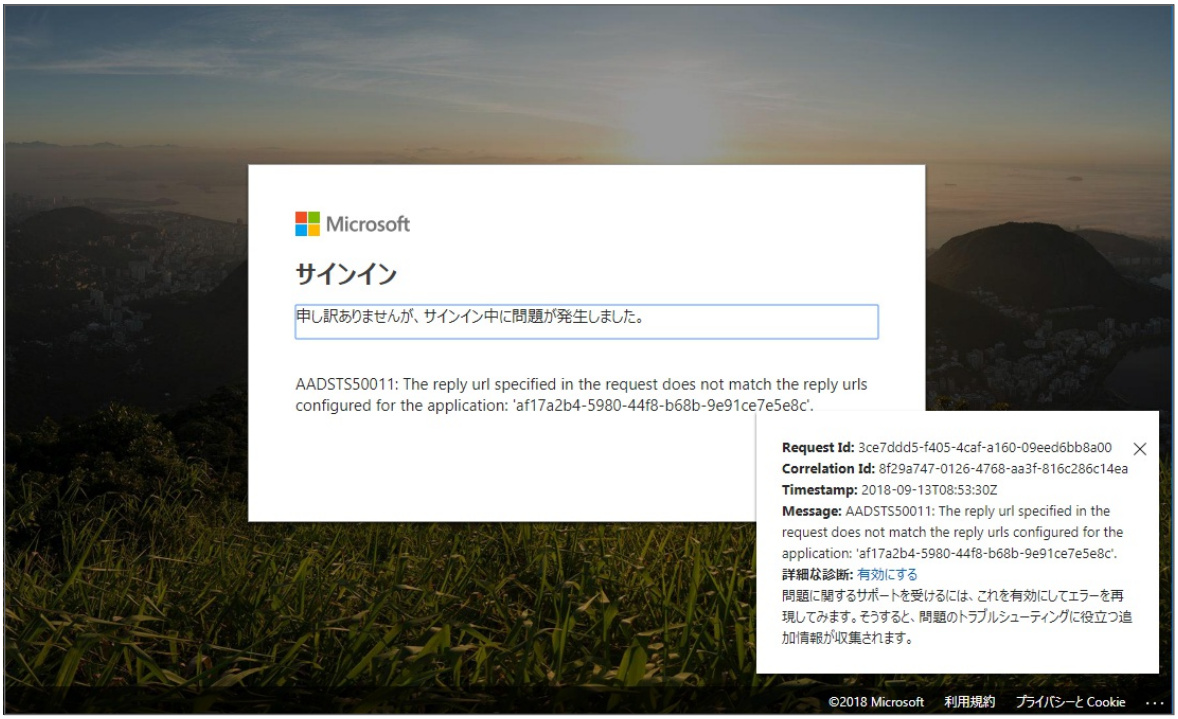
サーバに出力されているログから、エラーが発生している原因を確認してください。
Web Application Server に WebShere Application Server を利用している場合は*WebSphere Application Server 利用時の追加設定* を確認してください。

「AADSTS50011: The reply url specified in the request does not match the reply urls configured for the application: <クライアントID>」が発生します

現象

「個人設定」-「外部連携アプリケーション」画面で「許可」ボタンをクリックし、Microsoftの画面でサインインを実行後、画面下部に以下が出力されます。

AADSTS50011: The reply url specified in the request does not match the reply urls configured for the application: <クライアントID>



原因

Microsoft Entra ID 上に作成したアプリケーションの構成の「応答 URL」が不正である可能性があります。

対応方法

「応答 URL」の設定に誤りがないか確認してください。
設定箇所については「 *アプリケーションを設定する* 」を参照してください。

「AADSTS90094: <アプリケーション名> is requesting permissions, which you are not authorized to grant. Contact your administrator, who can grant permissions to this application on your behalf.」が発生します

現象

「個人設定」-「外部連携アプリケーション」画面で「許可」ボタンクリックし、Microsoftの画面でサインインを実行後、画面下部に以下が出力されます。

AADSTS90094: <アプリケーション名> is requesting permissions, which you are not authorized to grant. Contact your administrator, who can grant permissions to this application on your behalf.

原因

Microsoft Entra ID 上に作成したアプリケーションの構成の「APIアクセス」の「アクセスの有効化」にて「委任されたアクセス許可」が一般ユーザではアクセス出来ないものになっている可能性があります。

対応方法

適切なスコープを設定してください。詳細は Microsoft社 の以下のドキュメントを参照してください。
設定箇所については「 *アプリケーションを設定する* 」を参照してください。

- Office 365 application manifest and permission details : https://msdn.microsoft.com/office/office365/HowTo/application-manifest

エラーメッセージが出力される

以下のエラーメッセージが出力された場合の対処方法についての詳細は「 メッセージコードリファレンス 」を参照してください。

- [E.IWP.OAUTHCLIENT.PROCESSOR.00008] アクセストークンの発行時に、認可サーバよりエラーが返却されました。 error = unauthozed_client
- [E.IWP.OAUTHCLIENT.PROCESSOR.00008] アクセストークンの発行時に、認可サーバよりエラーが返却されました。 error = invalid_client
- [E.IWP.OAUTHCLIENT.HTTP.00003] HTTP通信の処理に失敗しました。
- [E.IWP.OAUTHCLIENT.PROCESSOR.00001] アクセストークンレスポンスの書式が不正です。
- [E.IWP.OAUTHCLIENT.PROCESSOR.00017] 指定のプロバイダ種別はサポートしていません。 providerType = NOT_office365
- [E.IWP.OFFICE365.COMMON.00005] 想定しないエラーレスポンスを受信しました。 statusCode = 401
- [E.IWP.OFFICE365.ONEDRIVESAPI.00008] HTTP通信に失敗しました。

また、Microsoft社の提供している Microsoft 365 のサインイン画面ではエラー発生時に、以下のように画面右側にエラー内容が表示されます。
表示されるエラー内容を調べることで原因と対応方法が判明する可能性があります。


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 specified in the request does not match the reply urls configured for the application: 'af17a2b4-5980-44f8-b68b-9e91ce7e5e8c'.
Request Id: 3ce7ddd5-f405-4caf-a160-09eed6bb8a00
Correlation Id: 8f29a747-0126-4768-aa3f-816c286c14ea
Timestamp: 2018-09-13T08:53:30Z
Message: AADSTS50011: The reply url specified in the request does not match the reply urls configured for the application: 'af17a2b4-5980-44f8-b68b-9e91ce7e5e8c'.
詳細な診断: 有効にする
問題に関するサポートを受けるには、これを有効にしてエラーを再現してみます。そうすると、問題のトラブルシューティングに役立つ追加情報が収集されます。
©2018 Microsoft
利用規約
プライバシーと Cookie

WebSphere Application Server 利用時の追加設定

Web Application Server に WebSphere Application Server を利用する場合、SSL 証明書の認証問題が発生します。

SharePoint Online を利用する場合の問題について

- https://support.microsoft.com/en-us/help/2842146/you-experience-ssl-certificate-authentication-issues-when-you-use-shar（English）
- https://support.microsoft.com/ja-jp/help/2842146/you-experience-ssl-certificate-authentication-issues-when-you-use-shar（日本語）
- https://support.microsoft.com/zh-cn/help/2842146/you-experience-ssl-certificate-authentication-issues-when-you-use-shar（中文）

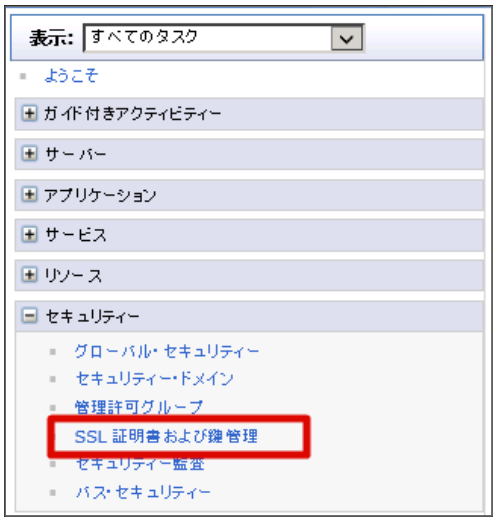
解決方法として配布されている証明書を WebSphere Application Server のトラストストアに追加する必要があります。
WebSphere Application Server 8.5.5 の場合の例を説明します。

> **注意**
>
> Office 365 連携機能は、Office 365 のサービスを利用しているため、予告無く仕様（必要な SSL 証明書）が変更される場合があります。
> 本追加設定を行っても SSL 通信のエラーが発生する場合は、エラー内容に従い、適切な SSL 証明書を追加してください。

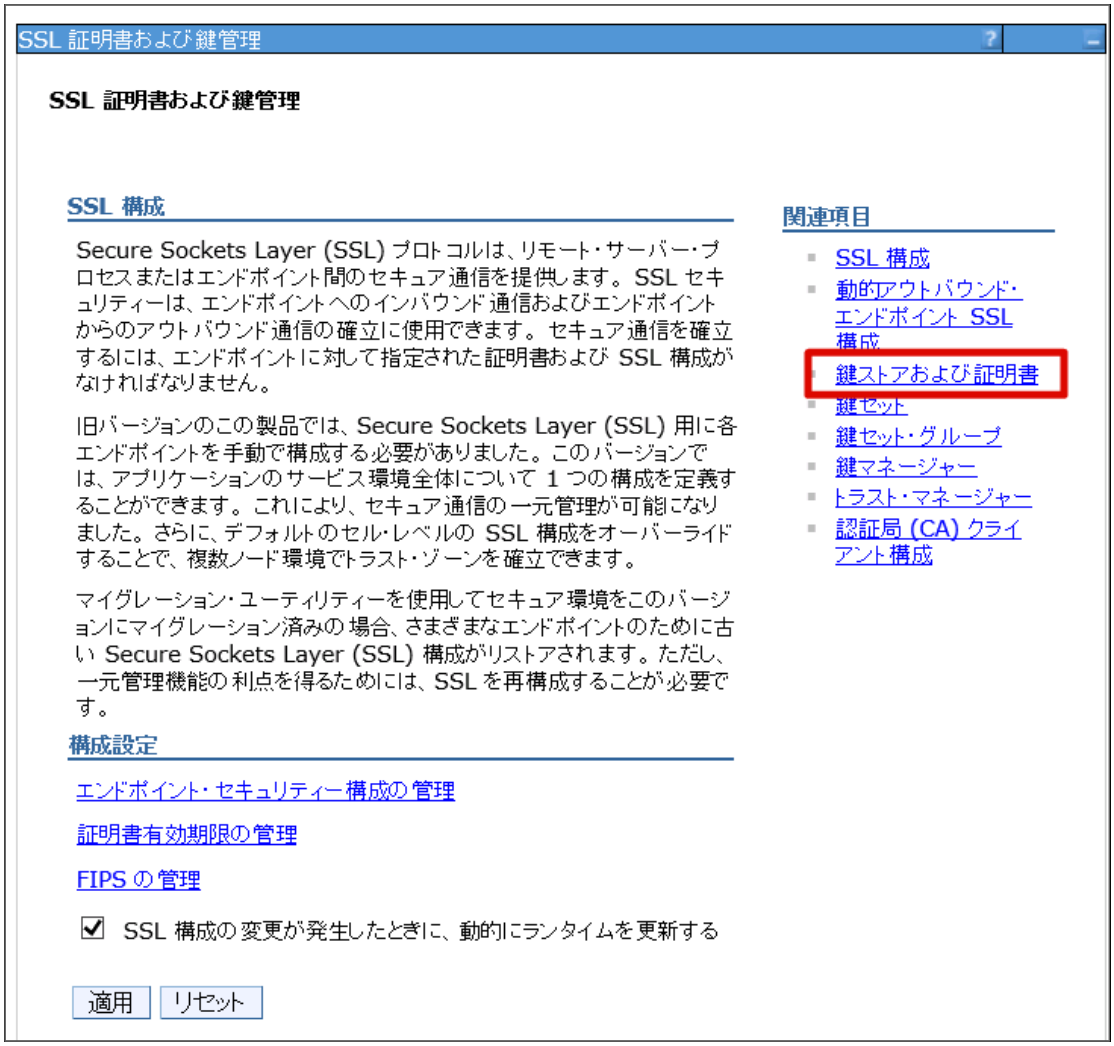
項目

Microsoft 365 ルート証明書バンドル を追加する

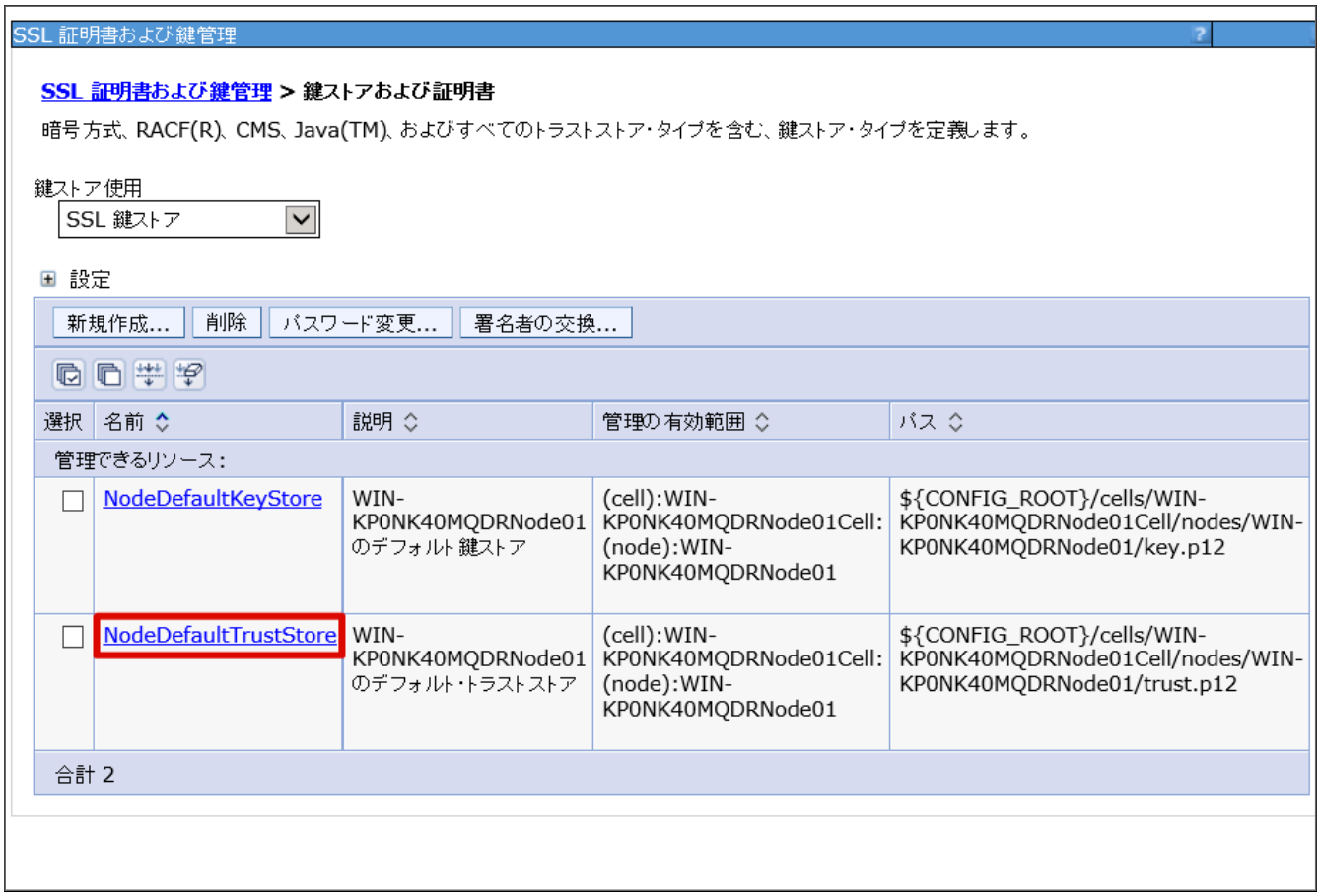
1. 以下のサイトから証明書ファイル[Microsoft 365 ルート証明書バンドル (P7B)]をダウンロードして、WebSphere Application Server 内の任意のディレクトリに配置します。
   - https://docs.microsoft.com/ja-jp/microsoft-365/compliance/encryption-office-365-certificate-chains
2. メニューから[セキュリティー]-[SSL 証明書および鍵管理]を選択します。



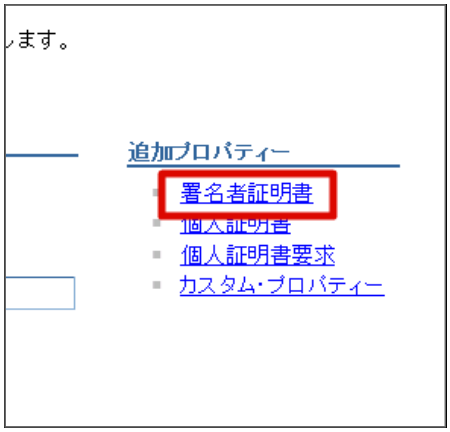
3. [鍵ストアおよび証明書]リンクをクリックします。



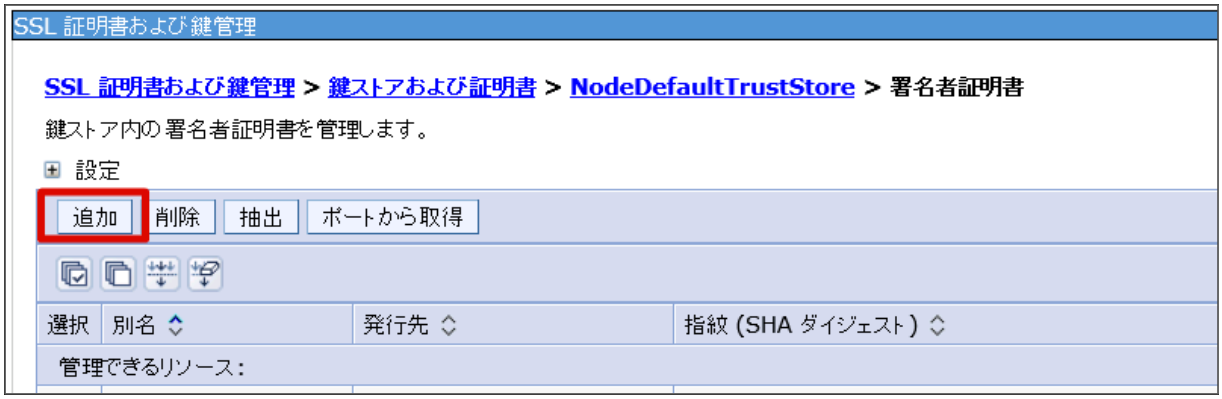
4. [NodeDefaultTrustStore]リンクをクリックします。



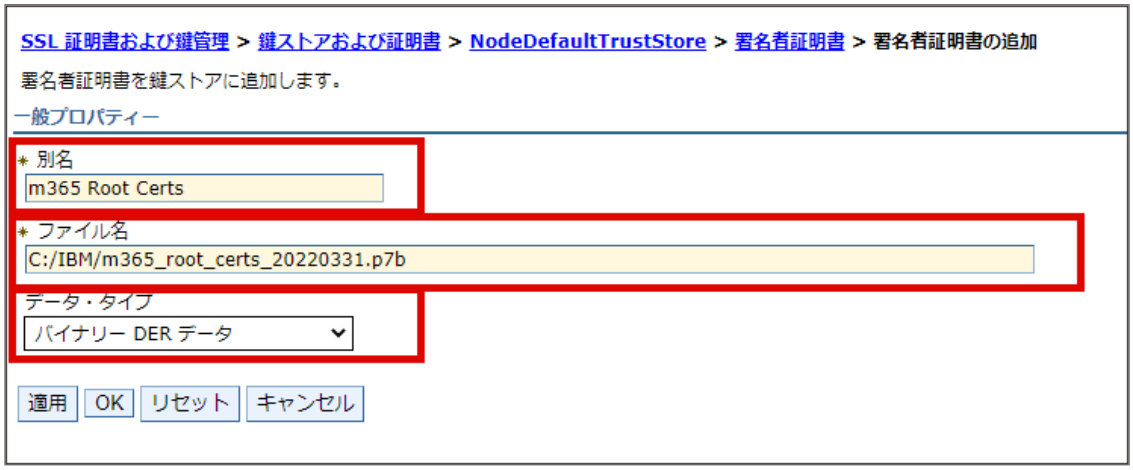
5. [署名者証明書]リンクをクリックします。



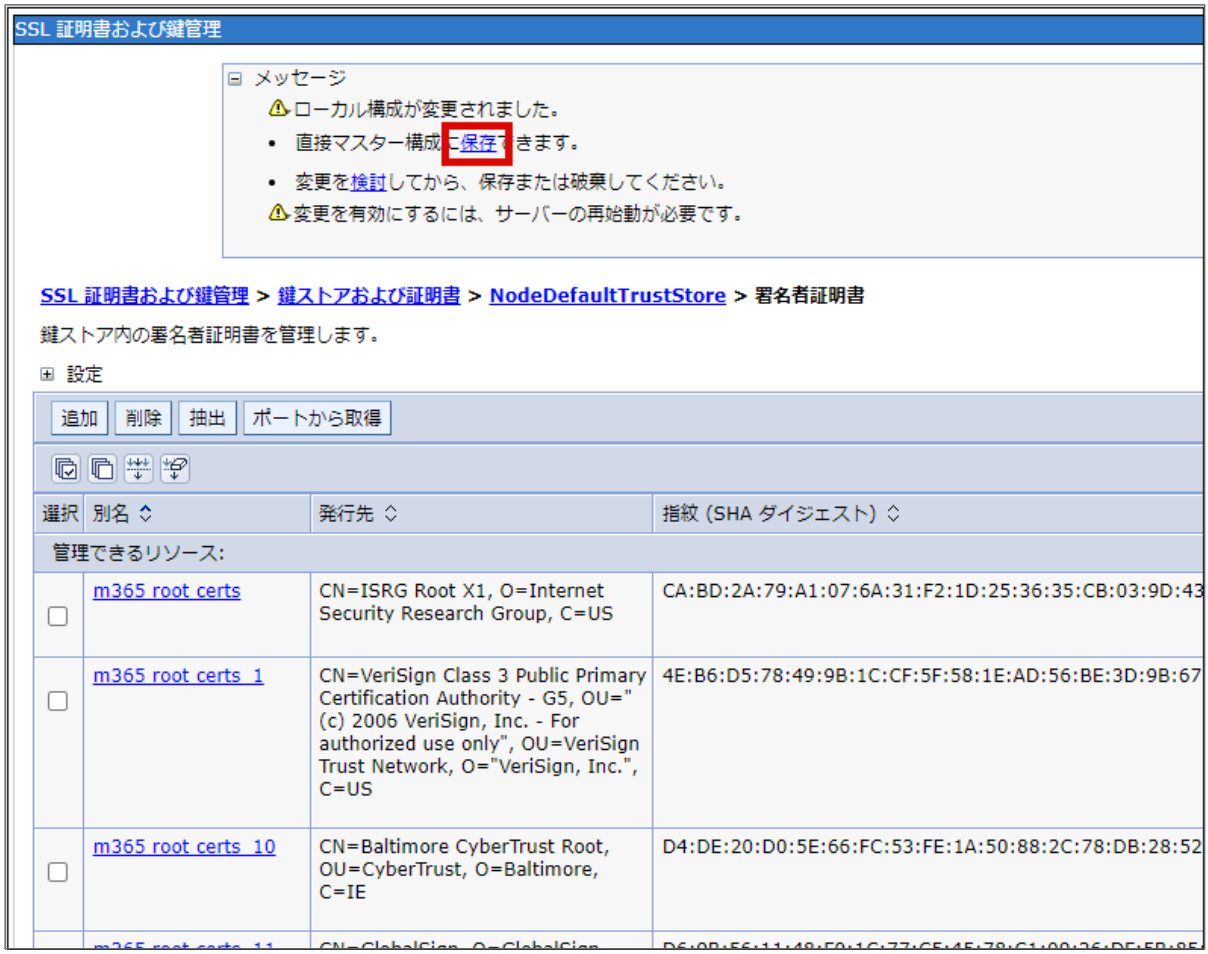
6. [追加]ボタンをクリックします。



7. 以下の項目を入力・選択し、[OK]をクリックします。
   別名に任意の文字列を入力します。例: 「m365 Root Certs」
   ファイル名に、ダウンロードした証明書ファイルへのパスを入力します。
   データ・タイプ 「バイナリー DER データ」を選択します。



8. [保存]をクリックします。



9. WebSphere Application Server を再起動することで、設定が反映されます。

HTTP通信のログ出力方法

Office 365 連携 はHTTP通信を行っています。
なにか問題が発生した際、HTTP通信の内容を解析することで、原因究明、および、解決方法の糸口に繋げることができます。

デバッグ用のログのため必要に応じて設定してください。出力頻度や量が多いため、パフォーマンスやディスク使用量に影響を与える可能性があります。
ログを出力するには、以下のファイルを指定の場所に配備し intra-mart Accel Platform を再起動してください。

ファイル	場所
im_logger_oauth_client_debug.xml	WEB-INF/conf/log

```
<included>
  <appender name="OAUTH_CLIENT_DEBUG" class="ch.qos.logback.core.rolling.RollingFileAppender">
    <file>${im.log}/platform/oauth_client/oauth_client_debug.log</file>
    <append>true</append>

    <!--
    <rollingPolicy class="ch.qos.logback.core.rolling.TimeBasedRollingPolicy">
      <fileNamePattern>
        ${im.log}/platform/oauth_client/oauth_client_debug-%d{yyyy-MM-dd}.log
      </fileNamePattern>
    </rollingPolicy>
    -->

    <rollingPolicy class="ch.qos.logback.core.rolling.FixedWindowRollingPolicy">
      <fileNamePattern>${im.log}/platform/oauth_client/oauth_client_debug%i.log</fileNamePattern>
      <minIndex>1</minIndex>
      <maxIndex>5</maxIndex>
    </rollingPolicy>

    <triggeringPolicy class="ch.qos.logback.core.rolling.SizeBasedTriggeringPolicy">
      <maxFileSize>10MB</maxFileSize>
    </triggeringPolicy>

    <encoder class="ch.qos.logback.core.encoder.LayoutWrappingEncoder">
      <layout class="jp.co.intra_mart.common.platform.log.layout.OutputStackTracePatternLayout">
        <pattern>[%d{yyyy-MM-dd HH:mm:ss.SSS}]  [%thread]  %-5level  %logger{255}  %X{tenant.id}  %X{log.id}
%X{request.id}  -  [%X{log.message.code}]  %msg%nopex%n</pattern>
        <enableOutputStackTrace>true</enableOutputStackTrace>
        <stackTraceDir>${im.log}/platform/oauth_client/exception/</stackTraceDir>
        <stackTraceFilename>'exception_'yyyy-MM-dd_HH-mm-ss'_%logId.log'</stackTraceFilename>
      </layout>
    </encoder>
  </appender>

  <logger name="jp.co.intra_mart.system.oauth.client.http" additivity="false">
    <level value="debug" />
    <appender-ref ref="OAUTH_CLIENT_DEBUG" />
  </logger>

  <!--
    <logger name="jp.co.intra_mart.system.oauth.client.service" additivity="false">
      <level value="debug" />
      <appender-ref ref="OAUTH_CLIENT_DEBUG" />
    </logger>
  -->

</included>
```

参考文献

リンク先は 2015年8月1日 時点で情報を確認しています。

OAuth 2.0

- 「The OAuth 2.0 Authorization Framework」

  https://tools.ietf.org/html/rfc6749 （English）
  http://openid-foundation-japan.github.io/rfc6749.ja.html （日本語）

Microsoft Azure

- 「Azure AD での OAuth 2.0」

  https://msdn.microsoft.com/en-US/library/azure/dn645545.aspx
- 「認証コード付与フロー」

  https://msdn.microsoft.com/en-US/library/azure/dn645542.aspx
- 「OAuth 2.0 でのエラー処理」

  https://learn.microsoft.com/en-us/previous-versions/azure/dn645540(v=azure.100)
- 「Authorization Endpoint Errors」

  https://msdn.microsoft.com/en-US/library/azure/dn645544.aspx
- 「Token Issuance Endpoint Errors」

  https://msdn.microsoft.com/en-US/library/azure/dn645548.aspx
- 「Errors from Secured Resources」

  https://msdn.microsoft.com/en-US/library/azure/dn645539.aspx

Microsoft 365

- 「Office 365 API reference」

  https://docs.microsoft.com/en-us/previous-versions/office/office-365-api/
- 「Office 365 OneDrive REST API」

  https://docs.microsoft.com/ja-jp/onedrive/developer/rest-api/
- 「Office 365 application manifest and permission details」

  https://developer.microsoft.com/en-us/graph/docs/concepts/permissions_reference
- 「Office 365 OAuth Sandbox」

  https://oauthplay.azurewebsites.net/
- 「Office 365 API 入門 - 松崎 剛 Blog」

  https://tsmatz.wordpress.com/2014/06/02/office-365-api/
- 「Azure Active Directory とは （事前準備） - 松崎 剛 Blog」

  https://tsmatz.wordpress.com/2012/09/01/azure-active-directory/
- 「Azure Active Directory の Common Consent Framework （Client 側） - 松崎 剛 Blog」

  https://tsmatz.wordpress.com/2014/04/01/azure-active-directory-common-consent-framework-client/
- 「Azure Active Directory の Common Consent Framework （Service 側） - 松崎 剛 Blog」

https://tsmatz.wordpress.com/2014/05/27/azure-active-directory-common-consent-framework-service/