目次

- 1. 改訂情報
- 2. はじめに
  - 2.1. 本書の目的
  - 2.2. 前提条件
  - 2.3. 対象読者
  - 2.4. 注意事項
- 3. 概要
  - 3.1. Office 365 連携 について
  - 3.2. アクター
  - 3.3. セットアップの手順について
- 4. Office 365 の準備
  - 4.1. Office 365 の利用を開始する
  - 4.2. Office 365 にユーザを登録する
- 5. Microsoft Azure の準備
  - 5.1. Microsoft Azure サブスクリプションを取得する
  - 5.2. Microsoft Azure AD ディレクトリを作成する
  - 5.3. アプリケーションを登録する
  - 5.4. アプリケーションの構成を変更する
- 6. intra-mart Accel Platform をセットアップする
  - 6.1. Web Application Server の設定
  - 6.2. モジュールの選択
  - 6.3. 設定ファイルの編集
  - 6.4. テナント環境セットアップ
- 7. 動作確認（連携を行う）
- 8. 連携を解除するには
  - 8.1. 設定ファイルの編集
- 9. トラブルシューティング
  - 9.1. 「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
  - 9.2. エラーメッセージが出力される
- 10. 付録
  - 10.1. WebSphere Application Server利用時の追加設定
  - 10.2. HTTP通信のログ出力方法
- 11. 参考文献
  - 11.1. OAuth 2.0
  - 11.2. Microsoft Azure
  - 11.3. Office 365

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

はじめに

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。
- Office 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、 2015年8月1日 現在のものです。
- 本書内の Office 365 、 Microsoft Azure に関する説明は 2015年8月1日 現在のものです。

概要

項目
- Office 365 連携 について
- アクター
- セットアップの手順について

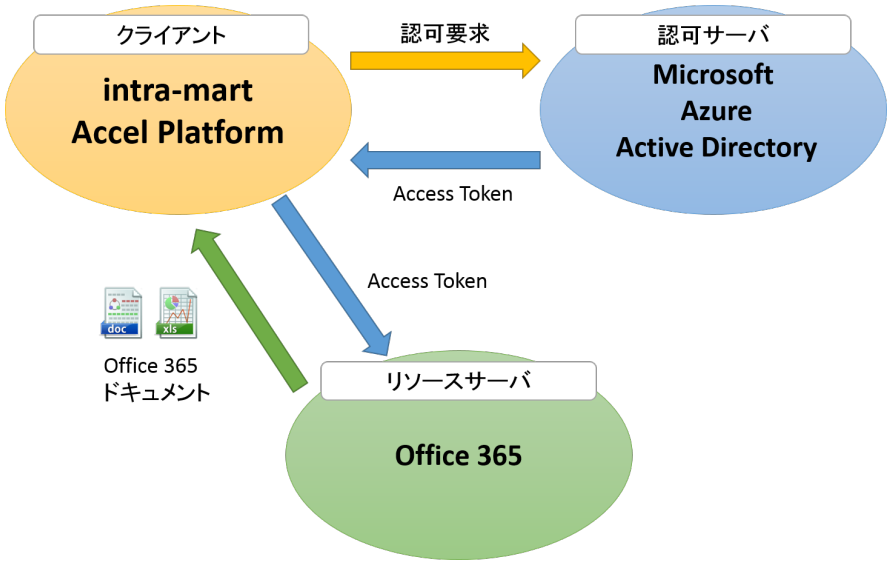
Office 365 連携 について

Office 365 連携 は OAuth2.0 を利用し、 intra-mart Accel Platform 上で Office 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。

- Office 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
- **Office365 管理者**
  Office 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. Office 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）*」

Office 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 **Office 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することが可能です。

項目

- Office 365 の利用を開始する
- Office 365 にユーザを登録する

> **注意**
>
> Office 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。

Office 365 の利用を開始する

以下のURLより、Office 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://www.microsoft.com/ja-jp/office/365/

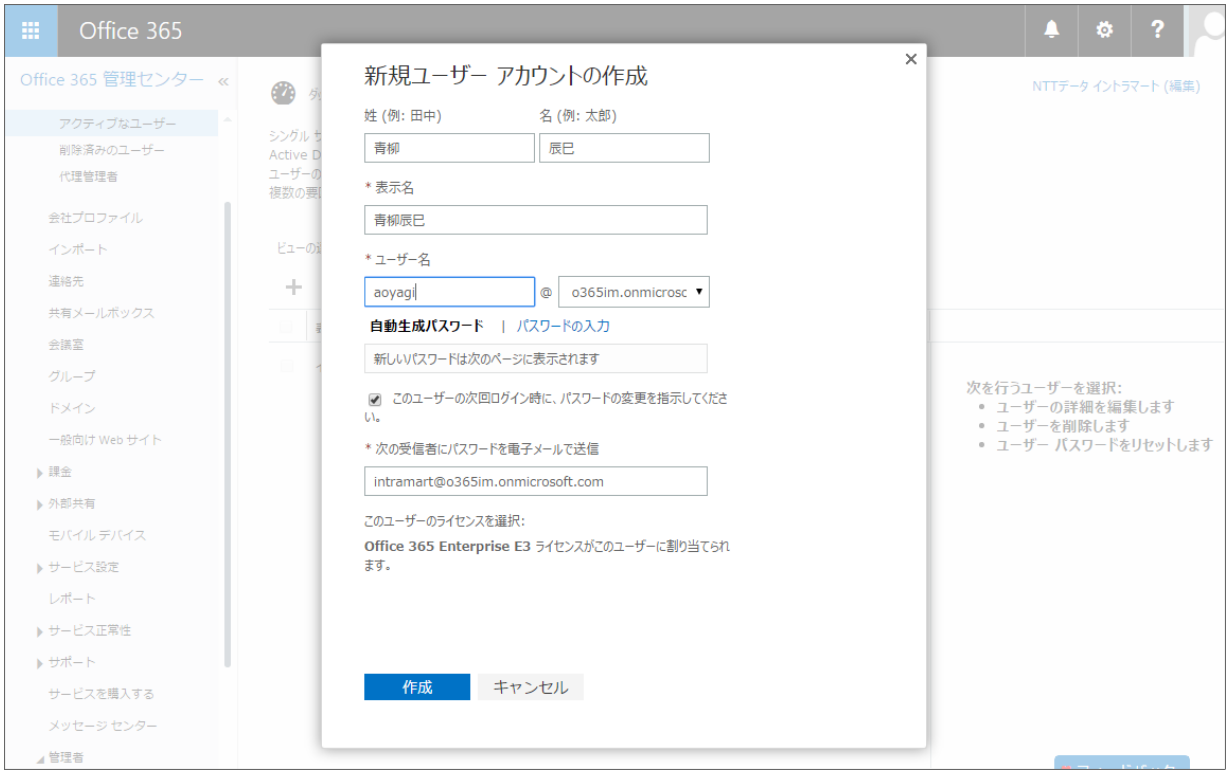
ここで取得したアカウントを **Office 365 管理者ユーザ** とします。
ここで取得したOffice 365のテナント名 は、 Microsoft Azure 管理者、 intra-mart Accel Platform システム管理者 が行う環境構築の際に利用します。
Office 365のテナント名とは以下のように@の右側の部分を指します。

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

Office 365 にユーザを登録する

Office 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 Office 365 のユーザが必要です。

1. 以下のURLより Office 365 ポータルに **Office 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. サイドメニューの「ユーザー」-「アクティブなユーザー」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。
すでに構築が完了している項目は省略することが可能です。

項目

- Microsoft Azure サブスクリプションを取得する
- Microsoft Azure AD ディレクトリを作成する
- アプリケーションを登録する
- アプリケーションの構成を変更する

注意
Office 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 Azure サブスクリプションを取得する

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

- http://azure.microsoft.com/

ここで取得したアカウントを **Microsoft Azure 管理者ユーザ** とします。

コラム
Office 365 管理者ユーザ のアカウントで Microsoft Azure Active Directory (以降、 Microsoft Azure ADとする）を作成することも可能です。
以下の手順で行います。

1. Office 365 ポータルに **Office 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。
2. サイドメニューの「管理者」-「Azure AD」から Microsoft Azure サブスクリプションを取得します。

この方法で Microsoft Azure サブスクリプションを取得した場合、 Office 365 の組織と Microsoft Azure ADが紐付けられるため、後述の「*Microsoft Azure AD ディレクトリを作成する*」という作業は不要です。

コラム
Office 365 管理者 と **Microsoft Azure 管理者** の役割を明確に区別したい場合は以下の方法が可能です。
Office 365 管理者ユーザ のアカウントとは別に Office 365 のサブスクリプションのアカウントを再度取得し、 Microsoft Azure ADを作成します。
以下の手順で行います。

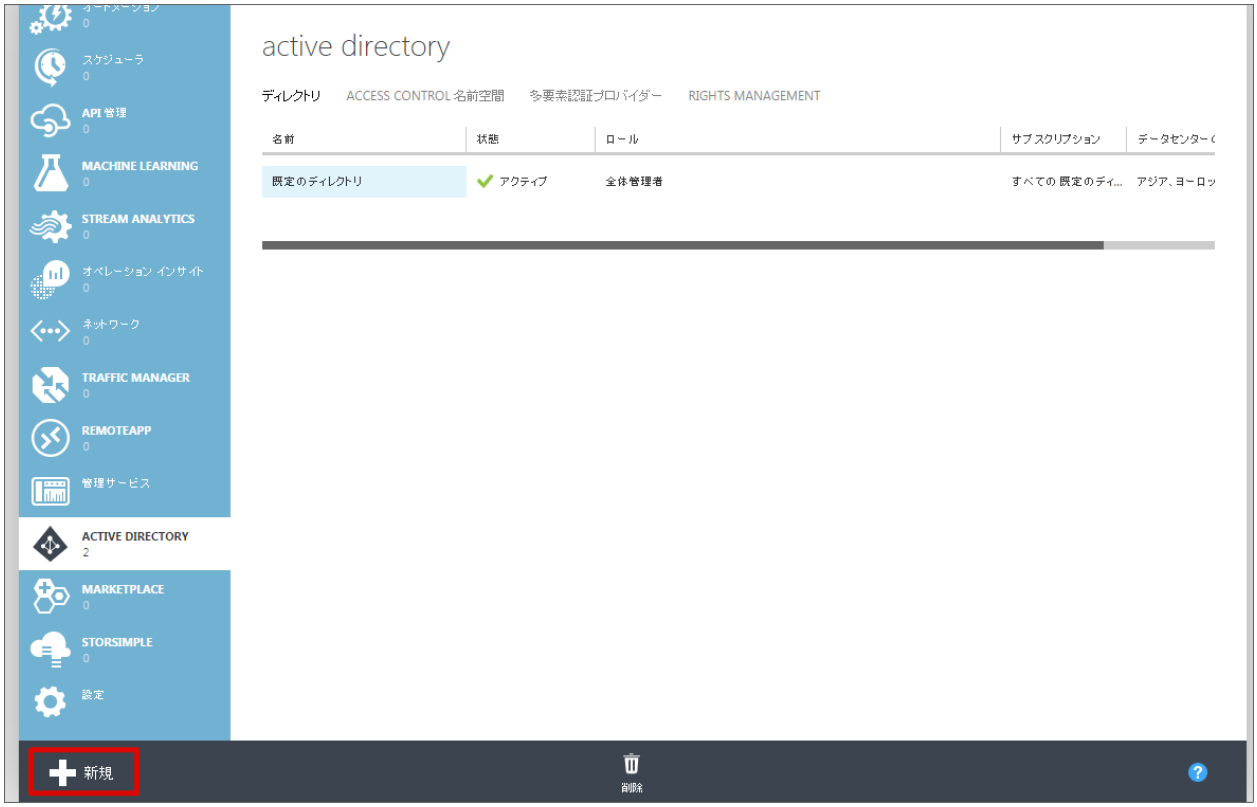
1. Office 365 サブスクリプションを取得します。ここで取得したアカウントを **Microsoft Azure 管理者ユーザ** とします。
2. Office 365 ポータルに **Microsoft Azure 管理者ユーザ** でサインインし、管理センターを表示します。
3. サイドメニューの「管理者」-「Azure AD」から Microsoft Azure サブスクリプションを取得します。

この方法で Microsoft Azure サブスクリプションを取得した場合、 後述の「*Microsoft Azure AD ディレクトリを作成する*」という作業は不要です。

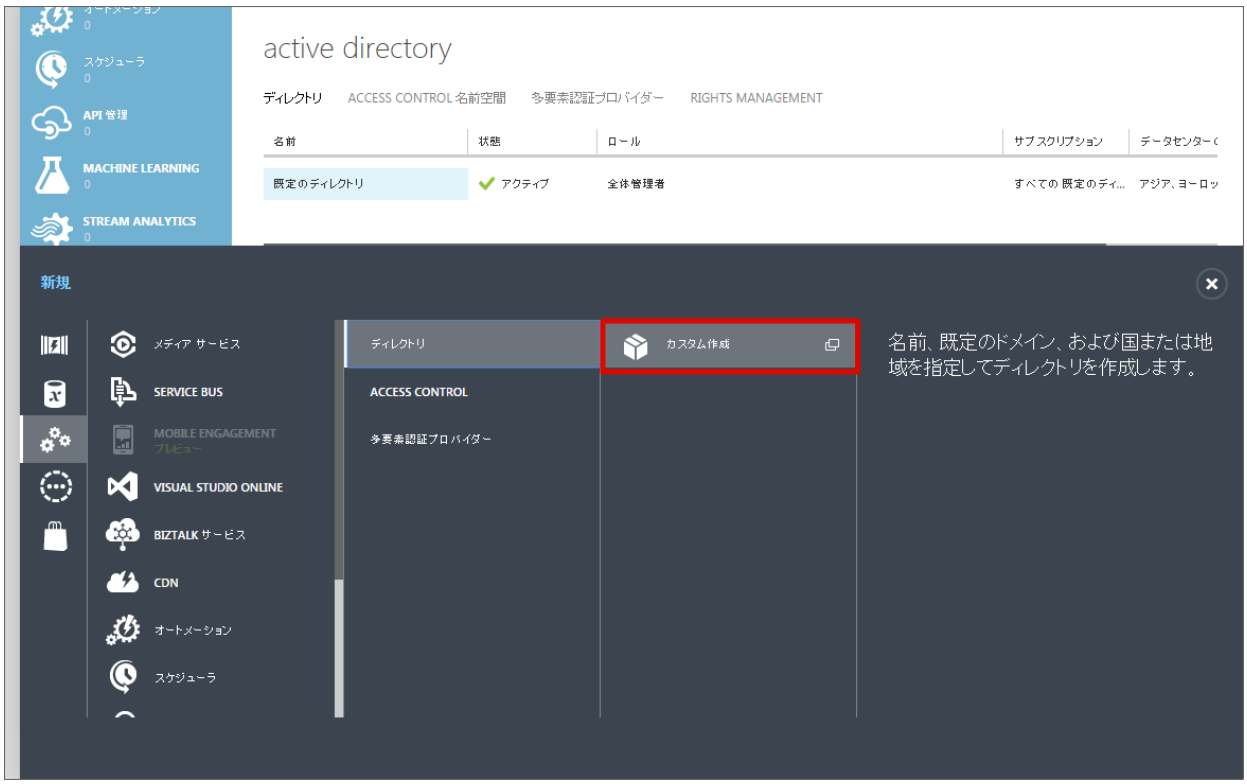
Microsoft Azure AD ディレクトリを作成する

Microsoft Azure 管理ポータルから Microsoft Azure AD ディレクトリを作成します。

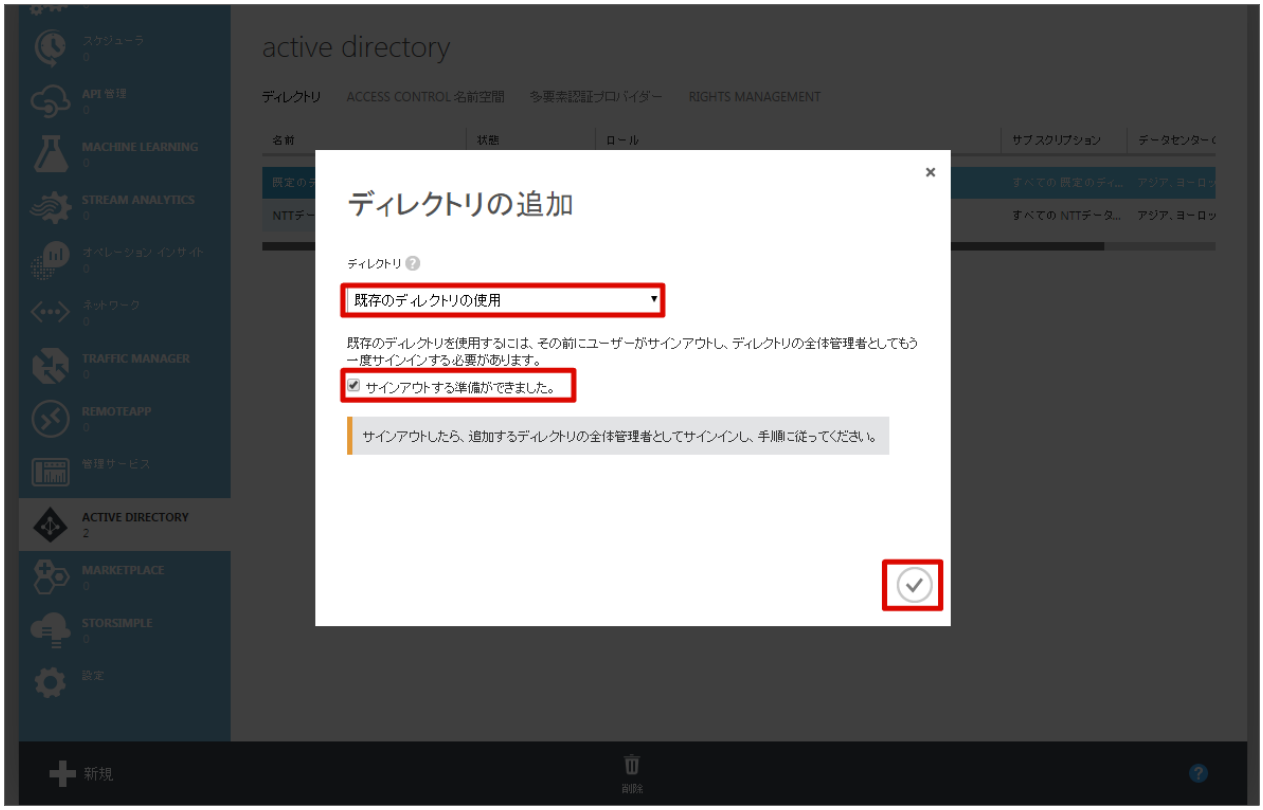
1. 以下のURLから Microsoft Azure の管理ポータルに **Microsoft Azure 管理者ユーザ** でサインインします。
   - http://manage.windowsazure.com/
2. 画面左下の「新規」を選択します。



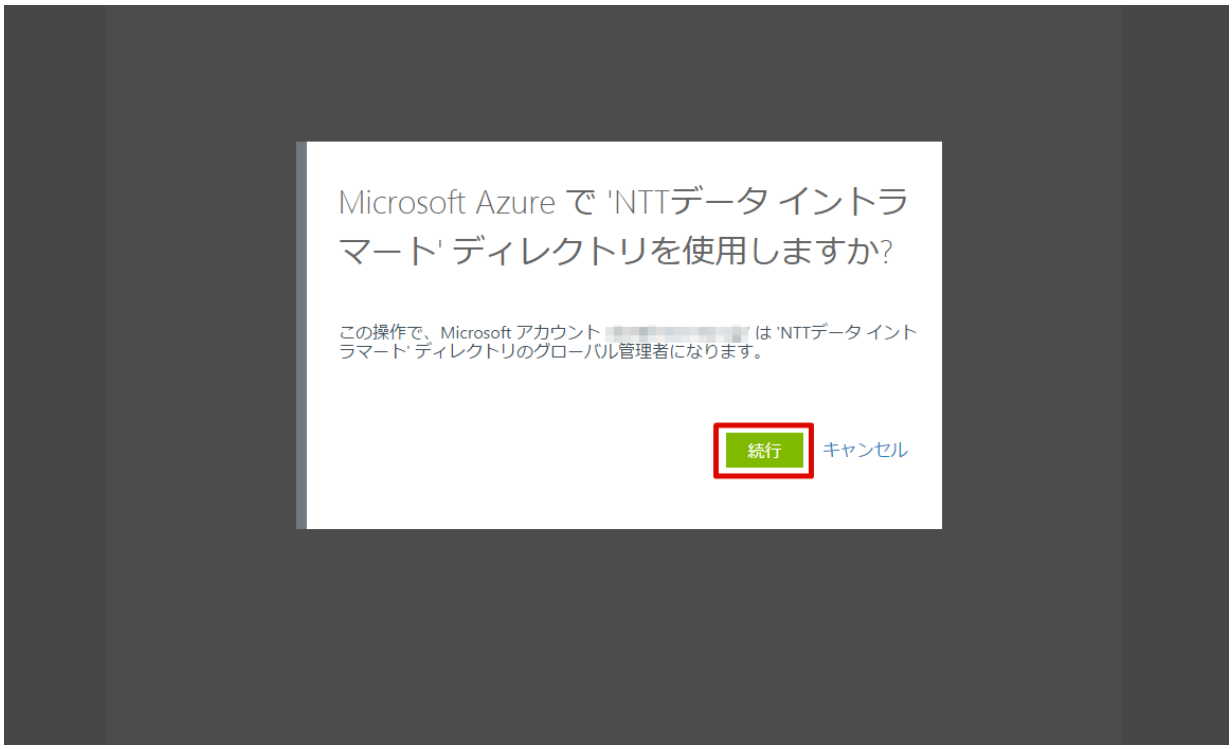
3. [APP SERVICES] -> [ACTIVE DIRECTORY] -> [ディレクトリ] -> [カスタム作成] を選択。



4. 「既存のディレクトリの使用」を選択し、「サインアウトする準備ができました」にチェックを入れ、チェックボタンをクリックします。



5. Microsoft Azure のサインイン画面が表示されたら、**Office 365 管理者ユーザ** のアカウントでサインインしてください。
6. サインイン後、以下の画面に遷移するので「続行」をクリックします。

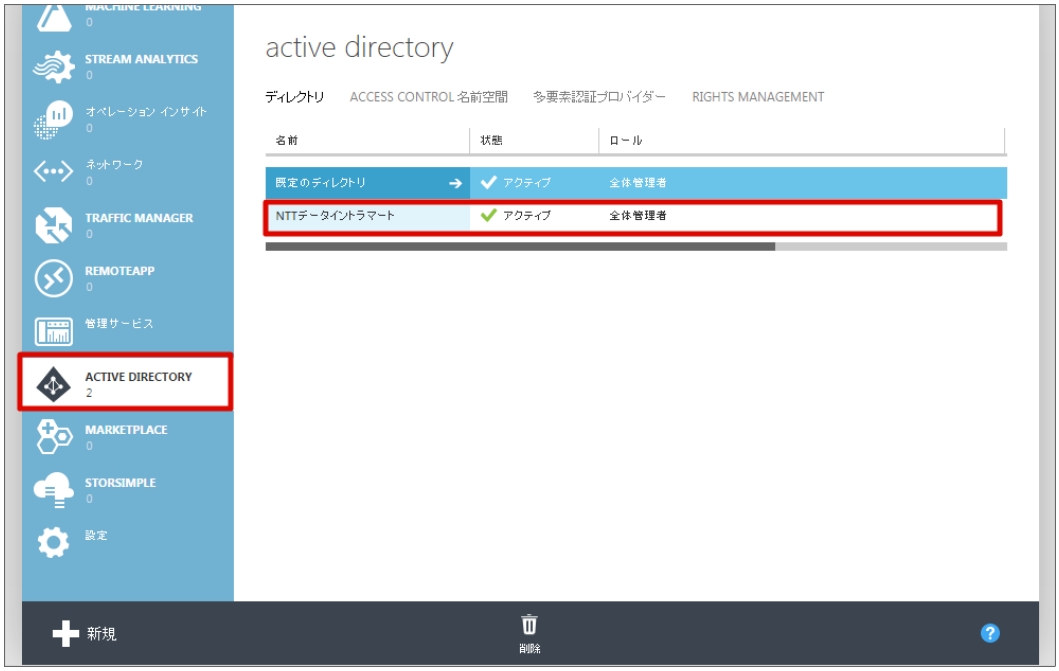


7. 以上で Office 365 の組織と Microsoft Azure AD の連携が完了します。

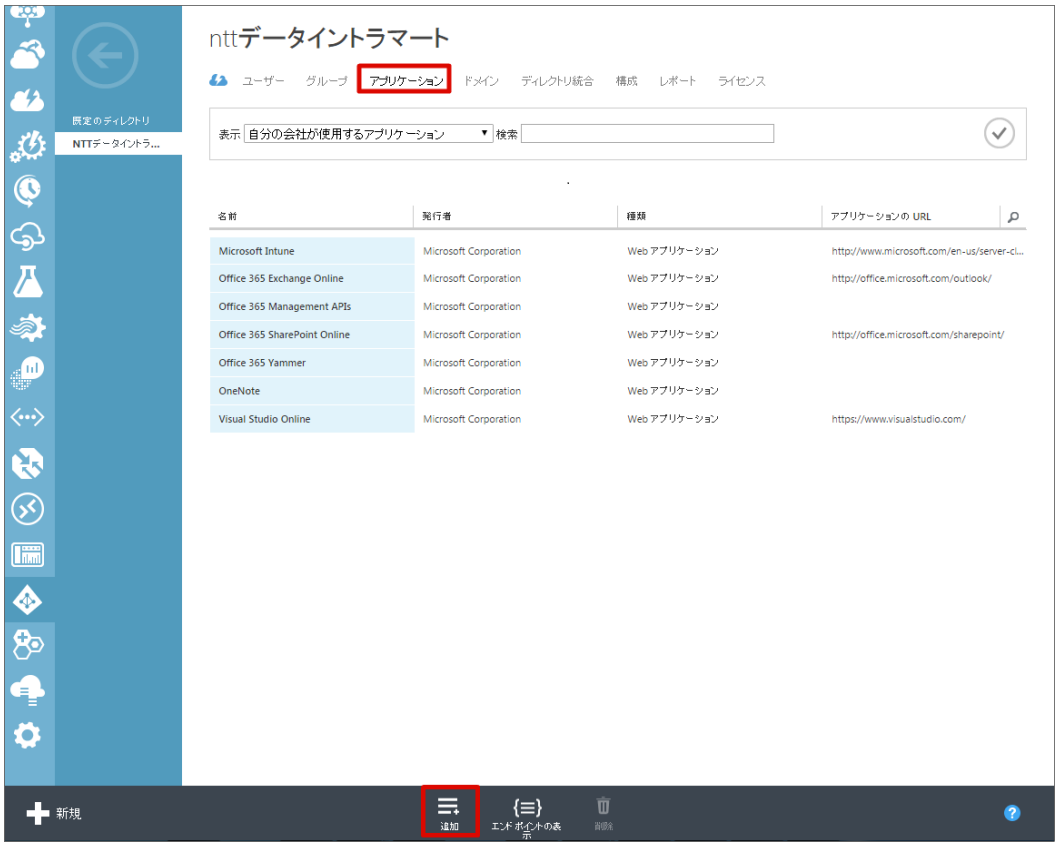
アプリケーションを登録する

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。

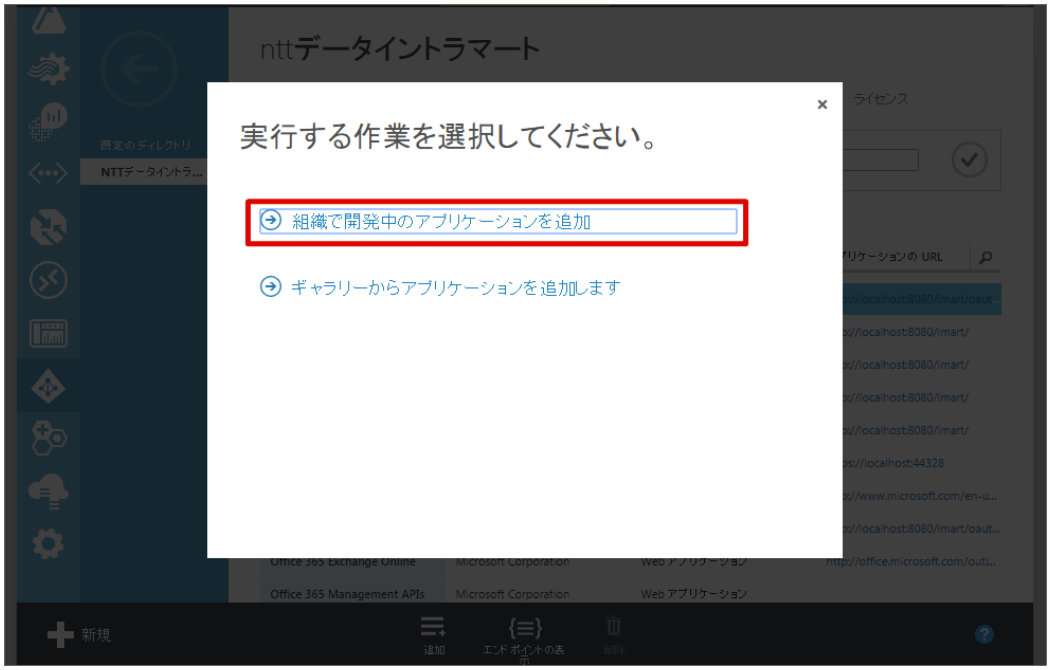
1. 以下のURLから Microsoft Azure の管理ポータルに **Microsoft Azure 管理者ユーザ** でサインインします。
   - http://manage.windowsazure.com/
2. サイドメニューから「ACTIVE DIRECTORY」を選択後、Office 365 の組織のディレクトリを選択します。



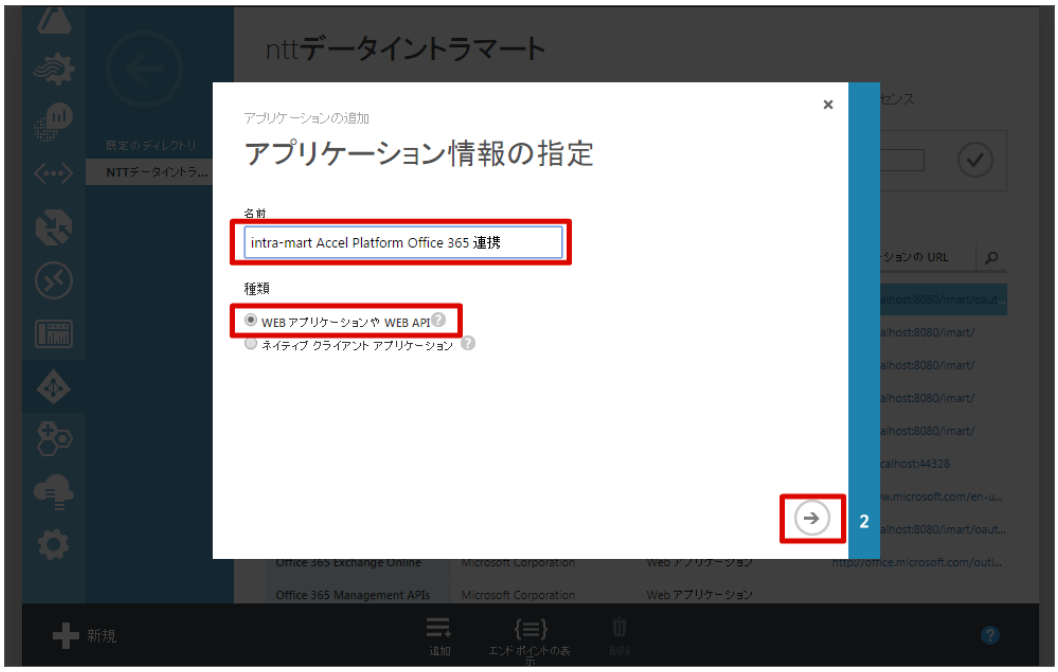
3. 「アプリケーション」を選択し、「追加」を選択します。



4. 「組織で開発中のアプリケーションを追加」を選択します。



5. 「名前」に任意の名称を入力、「種類」に 「WEBアプリケーションやWEB API」 を選択し、矢印をクリックします。



6. 「サインオンURL」 は intra-mart Accel Platform の ベースURL を入力します。

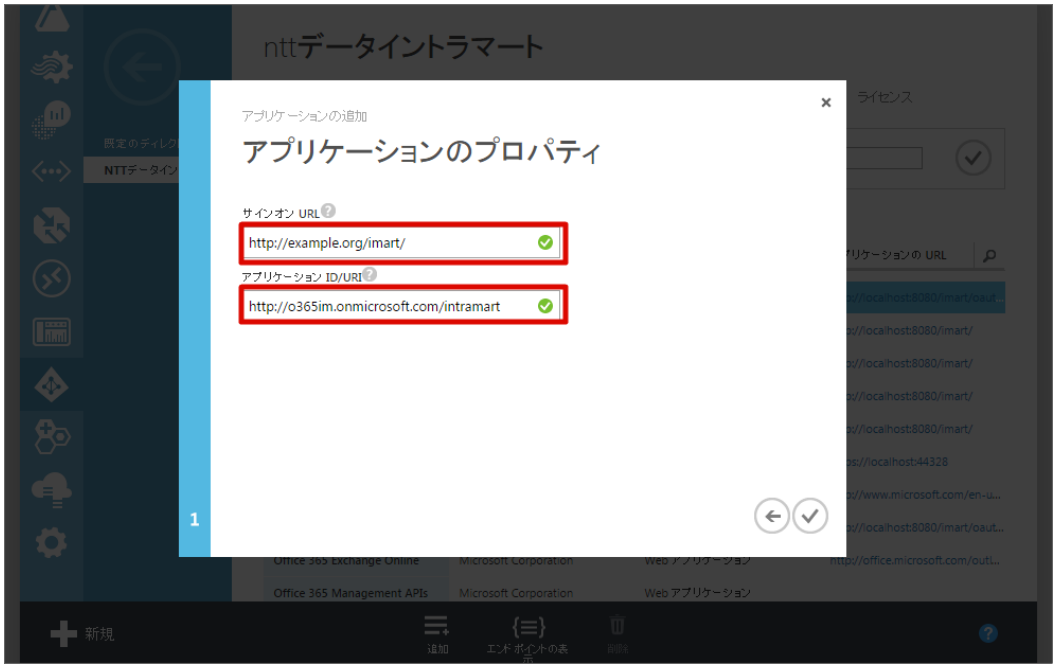
   例：http://example.org/imart/

   「アプリケーション ID/URI」 は以下のように入力します。

   - http://<Office 365のテナント>.onmicrosoft.com/<ディレクトリ内で一意の値>

   <Office 365 のテナント> は *Office 365 の利用を開始する* で Office 365 管理者 が取得した Office 365 サブスクリプションアカウントの@の右側の部分を指します。

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



7. 右下のチェックをクリックし作成を実行します。

8. 以上でアプリケーションの登録は完了です。

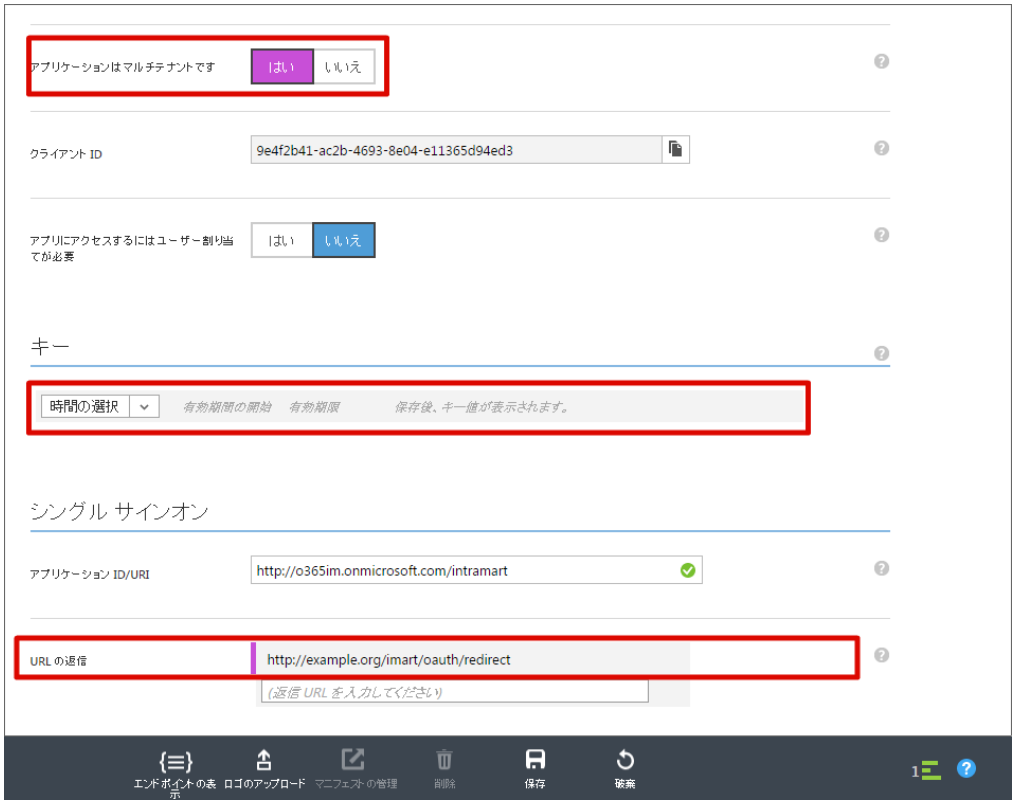
アプリケーションの構成を変更する

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。

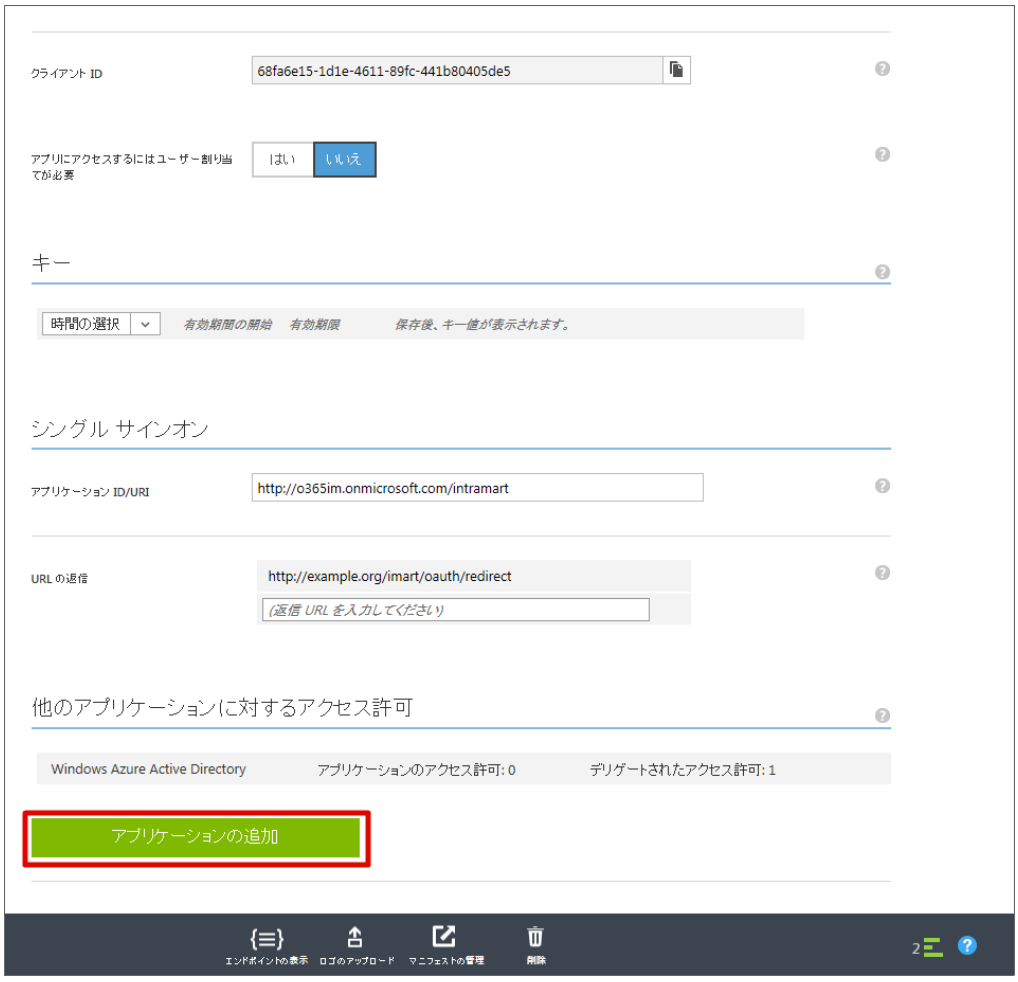
1. 構成を選択します。

2. 「アプリケーションはマルチテナントです」を「はい」に変更します。
「キー」を追加します。キーは設定の保存後に一度のみ表示されます。
「URLの返信」は以下のように入力します。
   - < intra-mart Accel Platform >/oauth/redirect

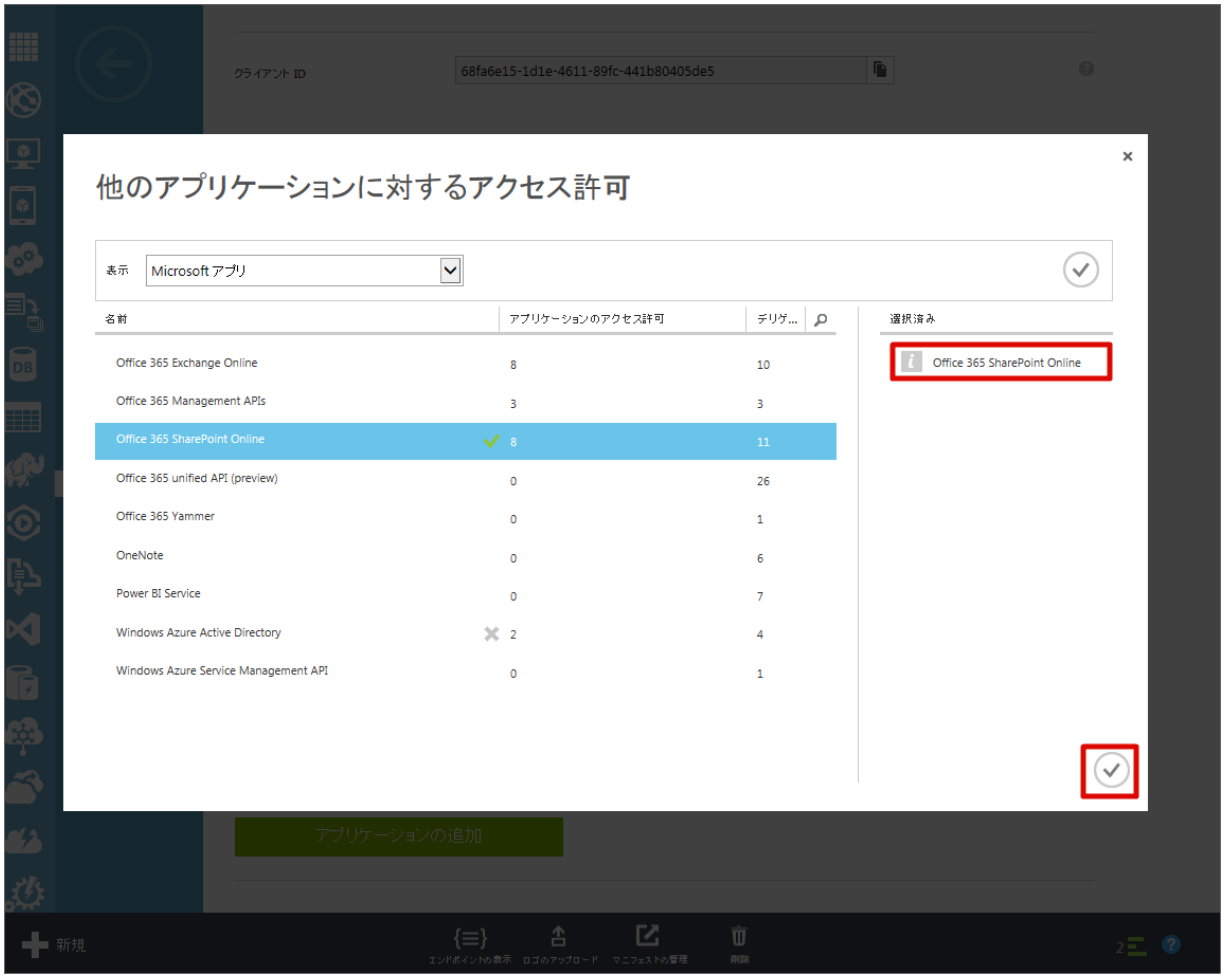
     例：http://example.org/imart/oauth/redirect



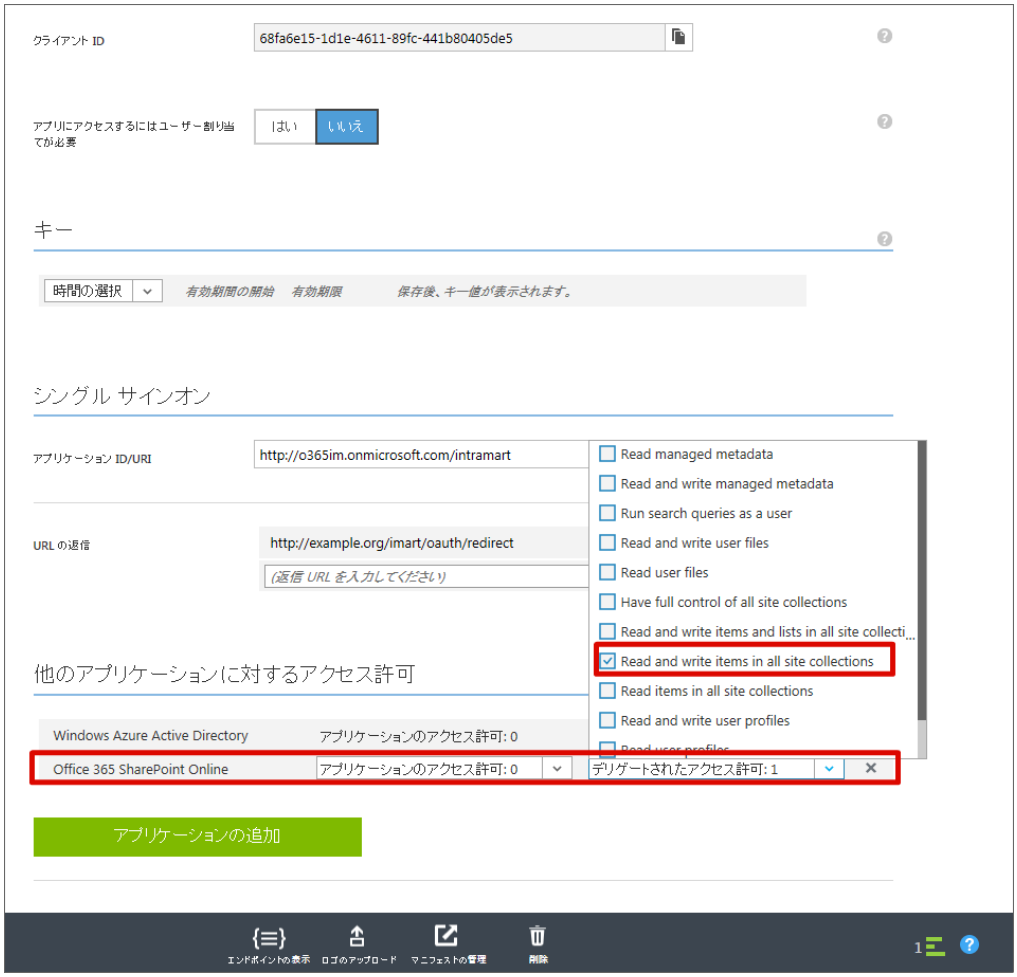
3. 「アプリケーションの追加」をクリックします。



4. アプリケーションを新たに追加し、「チェック」ボタンをクリックします。 ここでは、例として 「Office 365 SharePoint Online」を追加しています。

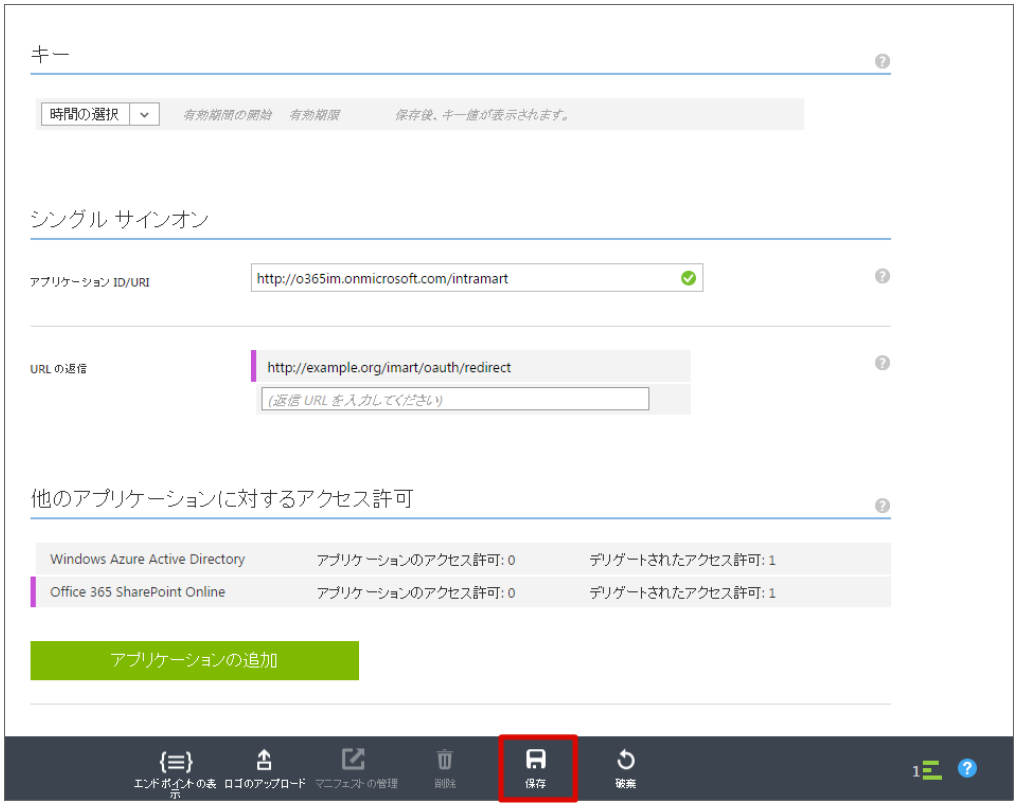


5. 「他のアプリケーションに対するアクセス許可」を適切に設定します。
   例として Office 365 連携 の提供している Office 365 の OneDrive API を 利用可能にするには、「Office 365 SharePoint Online」の「デリゲートされたアクセス許可」に「Read and write items in all site collections」を設定してください。



> **コラム**
>
> 「他のアプリケーションに対するアクセス許可」における Office 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。
>
> - Office 365 application manifest and permission details :
>   https://msdn.microsoft.com/office/office365/HowTo/application-manifest

6. 「保存」を実行します。



7. 以上でアプリケーションの構成変更が完了します。
   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。
   - クライアントID
   - 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
- モジュールの選択
- 設定ファイルの編集
  - プロバイダ設定
  - OAuth設定
  - 追加設定（SharePoint）
- テナント環境セットアップ

Web Application Server の設定

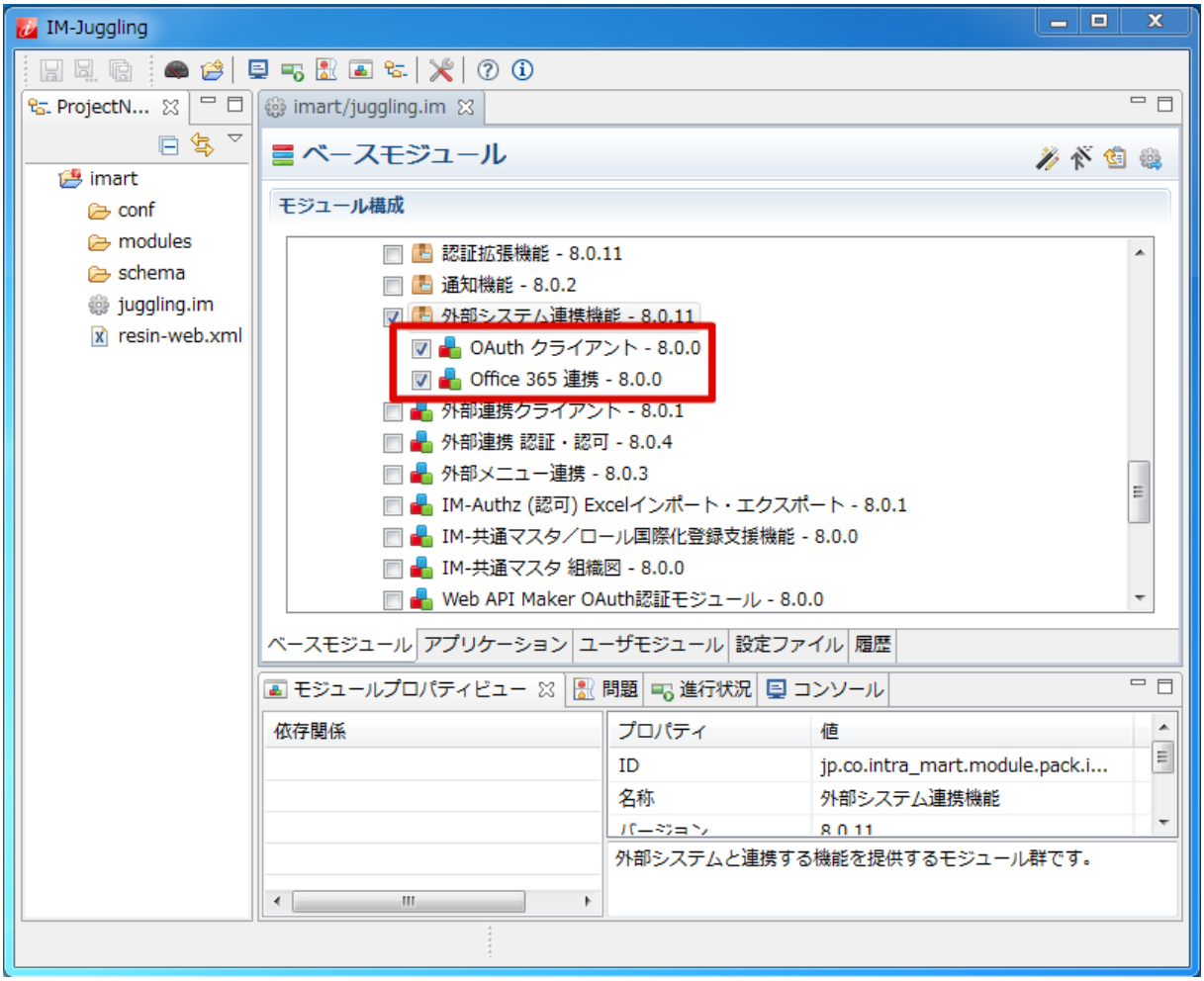
Web Application Server に WebSphere Application Server を利用する場合、 SharePoint Online を使用する際に以下のSSL証明書の認証問題が発生します。

- https://support.microsoft.com/en-us/kb/2842146 （English）
- https://support.microsoft.com/ja-jp/kb/2842146 （日本語）
- https://support.microsoft.com/zh-cn/kb/2842146 （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

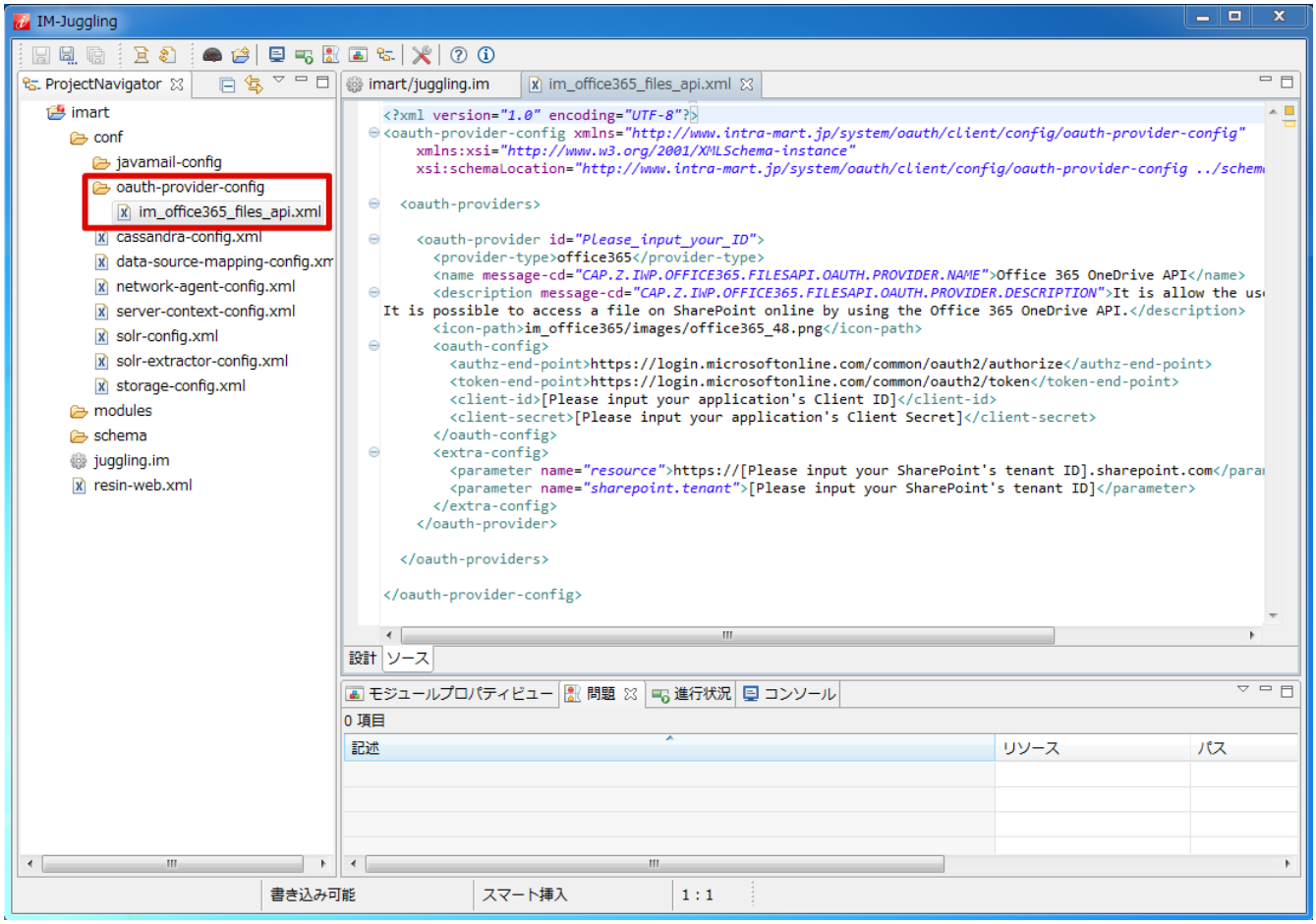
「 intra-mart Accel Platform セットアップガイド 」-「 プロジェクトの作成とモジュールの選択 」より、 Office 365 連携 , OAuth クライアント を選択します。



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 Office 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「*アプリケーションの構成を変更する*」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://< Office 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 Office 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>
```

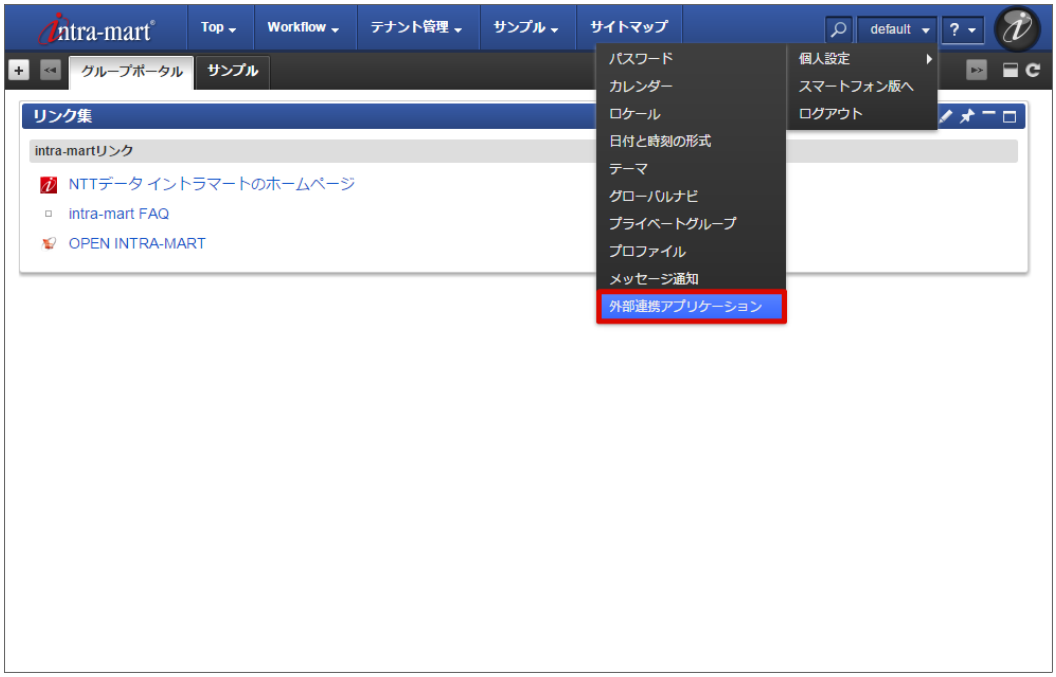
テナント環境セットアップ

- 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。

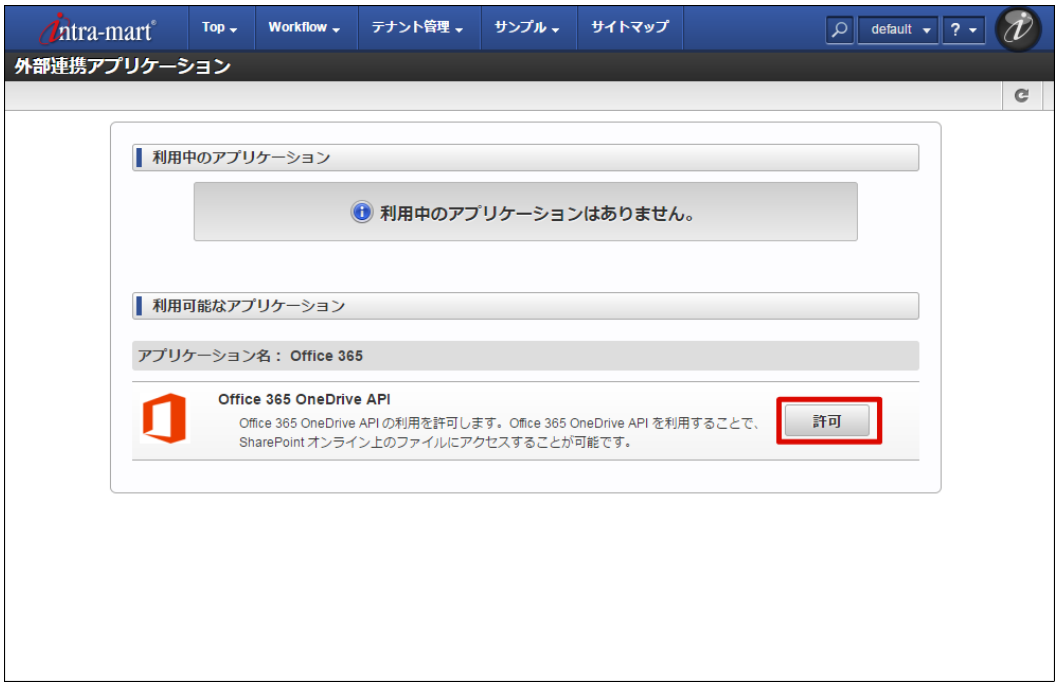
動作確認（連携を行う）

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 Office 365 のユーザ と連携をします。

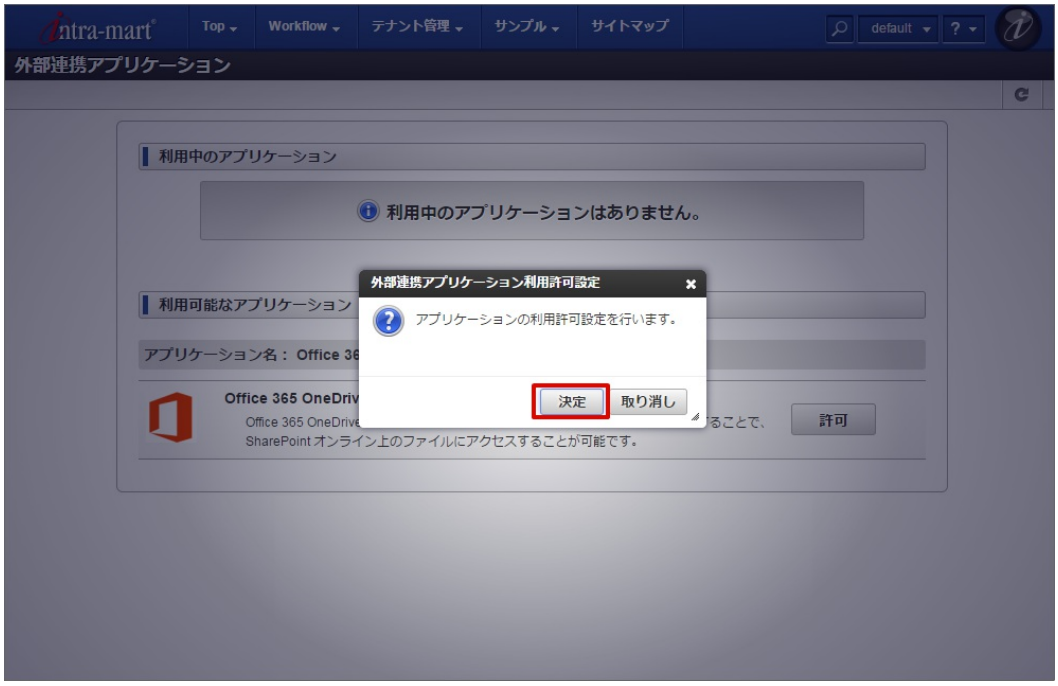
1. 任意のユーザで intra-mart Accel Platform にログインしてください。
2. ユーティリティメニューより、「個人設定」-「外部連携アプリケーション」を選択します。



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

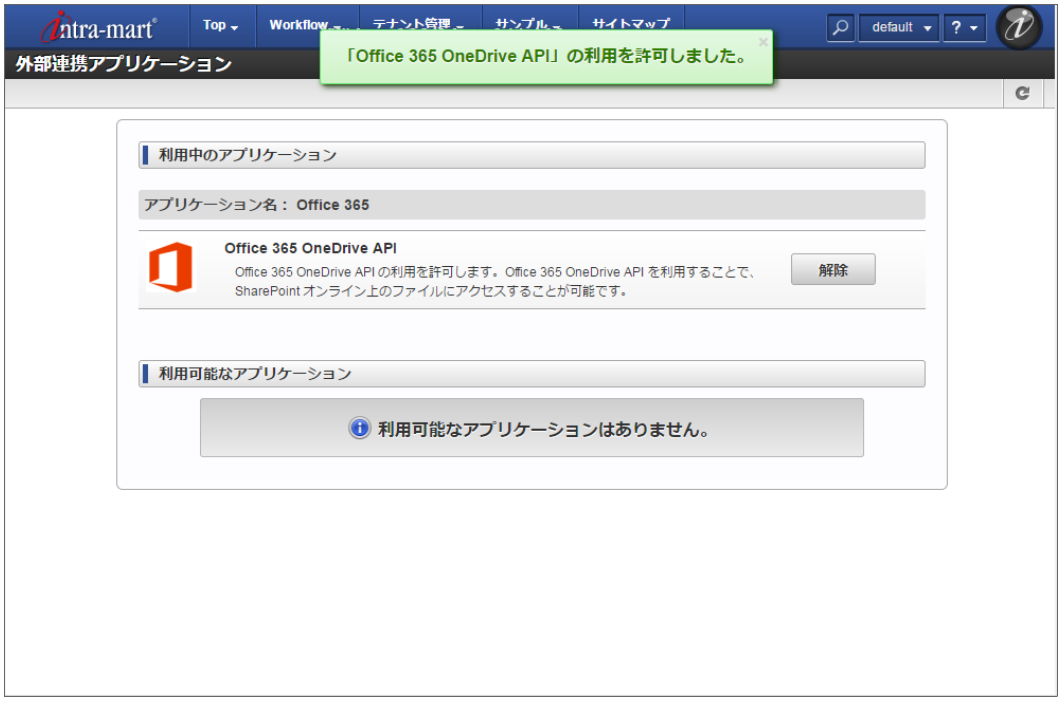


4. 「決定」をクリックします。



5. Office 365 の認証画面に遷移します。
   Office 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 Office 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 <Office 365のテナントID >.onmicrosoft.com」が発生します
  - 現象
  - 原因
  - 対応方法
- 「不正なレスポンスを受け取りました。」が発生します
  - 現象
  - 原因
  - 対応方法
- 「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
  - 原因
  - 対応方法
- 「AADSTS50011: The reply address 'http://example.org/imart/oauth/redirect' does not match the reply addresses configured for the application: <クライアントID>」が発生します
  - 現象
  - 原因
  - 対応方法
- 「AADSTS90093: This operation can only be performed by an administrator. Sign out and sign in as an administrator or contact one of your organization's administrators.」が発生します
  - 現象
  - 原因
  - 対応方法
- 「AADSTS90093: Calling principal cannot consent due to lack of permissions.」が発生します
  - 現象
  - 原因
  - 対応方法

「AADSTS70001: Application with identifier <クライアントID> was not found in the directory <Office 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の「その他の技術情報:」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 <Office 365のテナントID >.onmicrosoft.com

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 Azure AD 上に作成したアプリケーションの構成の「アプリケーションはマルチテナントです」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「 *アプリケーションの構成を変更する* 」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「アプリケーションはマルチテナントです」が「はい」に変更してください。
設定箇所については「*アプリケーションの構成を変更する* 」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。

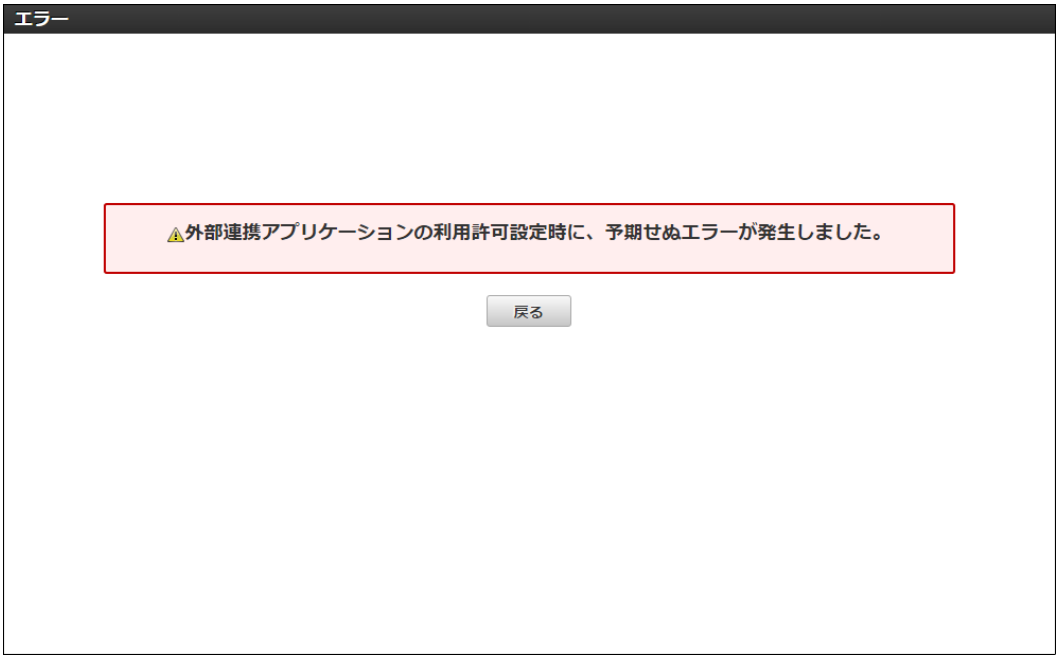
対応方法

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 address 'http://example.org/imart/oauth/redirect' does not match the reply addresses 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、画面下部の「その他の技術情報:」に以下が出力されます。

AADSTS50011: The reply address 'http://example.org/imart/oauth/redirect' does not match the reply addresses configured for the application: <クライアントID>

原因

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

対応方法

「URLの返信」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「 *アプリケーションの構成を変更する* 」を参照してください。

「AADSTS90093: This operation can only be performed by an administrator. Sign out and sign in as an administrator or contact one of your organization's administrators.」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、画面下部の「その他の技術情報:」に以下が出力されます。

AADSTS90093: This operation can only be performed by an administrator. Sign out and sign in as an administrator or contact one of your organization's administrators.

原因

Microsoft Azure AD 上に作成したアプリケーションの構成の「他のアプリケーションに対するアクセス許可」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「 *アプリケーションの構成を変更する* 」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

「AADSTS90093: Calling principal cannot consent due to lack of permissions.」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、画面下部の「その他の技術情報:」に以下が出力されます。

AADSTS90093: This operation can only be performed by an administrator. Sign out and sign in as an administrator or contact one of your organization’s administrators.

原因

Microsoft Azure AD 上に作成したアプリケーションの構成の「他のアプリケーションに対するアクセス許可」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「 *アプリケーションの構成を変更する* 」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 Office 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。


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。
正しくない要求を受信しました。
その他の技術情報:
Correlation ID: a69a6fb4-56eb-4ecc-aa08-8154892e5407
Timestamp: 2015-07-29 04:06:54Z
AADSTS90093: Calling principal cannot consent due to lack of permissions.

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/kb/2842146 （English）
- https://support.microsoft.com/ja-jp/kb/2842146 （日本語）
- https://support.microsoft.com/zh-cn/kb/2842146 （中文）

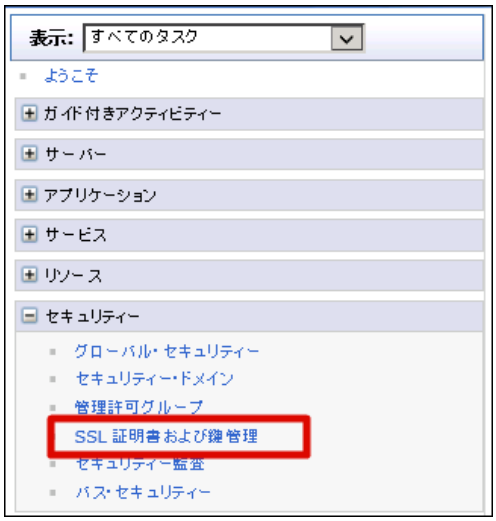
解決方法として配布されている証明書を WebSphere Application Server のトラストストアに追加する必要があります。
WebSphere Application Server 8.5.5 の場合の例を説明します。

> **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。

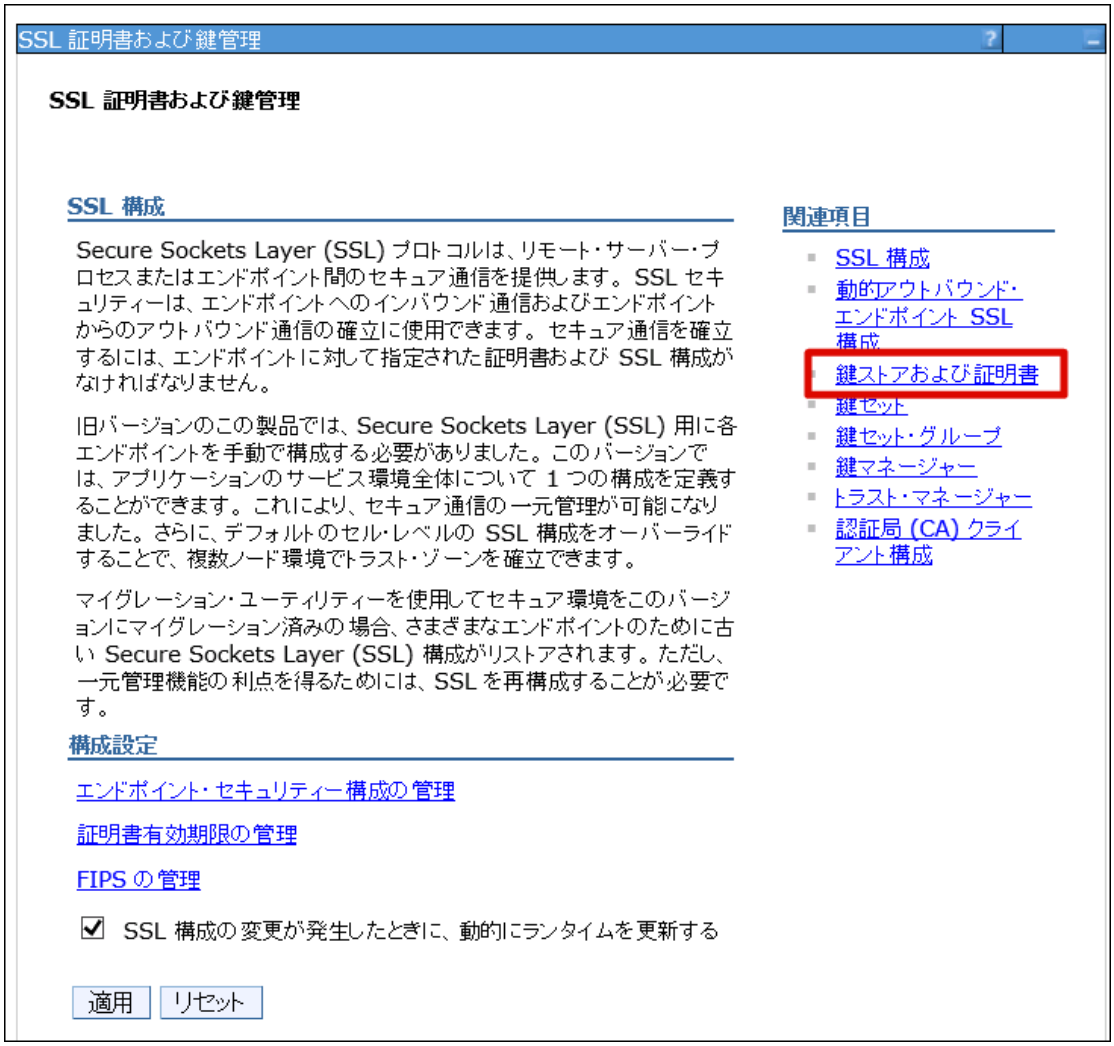
項目
- Baltimore CyberTrust Rootを追加する
- VeriSign Class 3 Primary CA - G5を追加する

Baltimore CyberTrust Rootを追加する

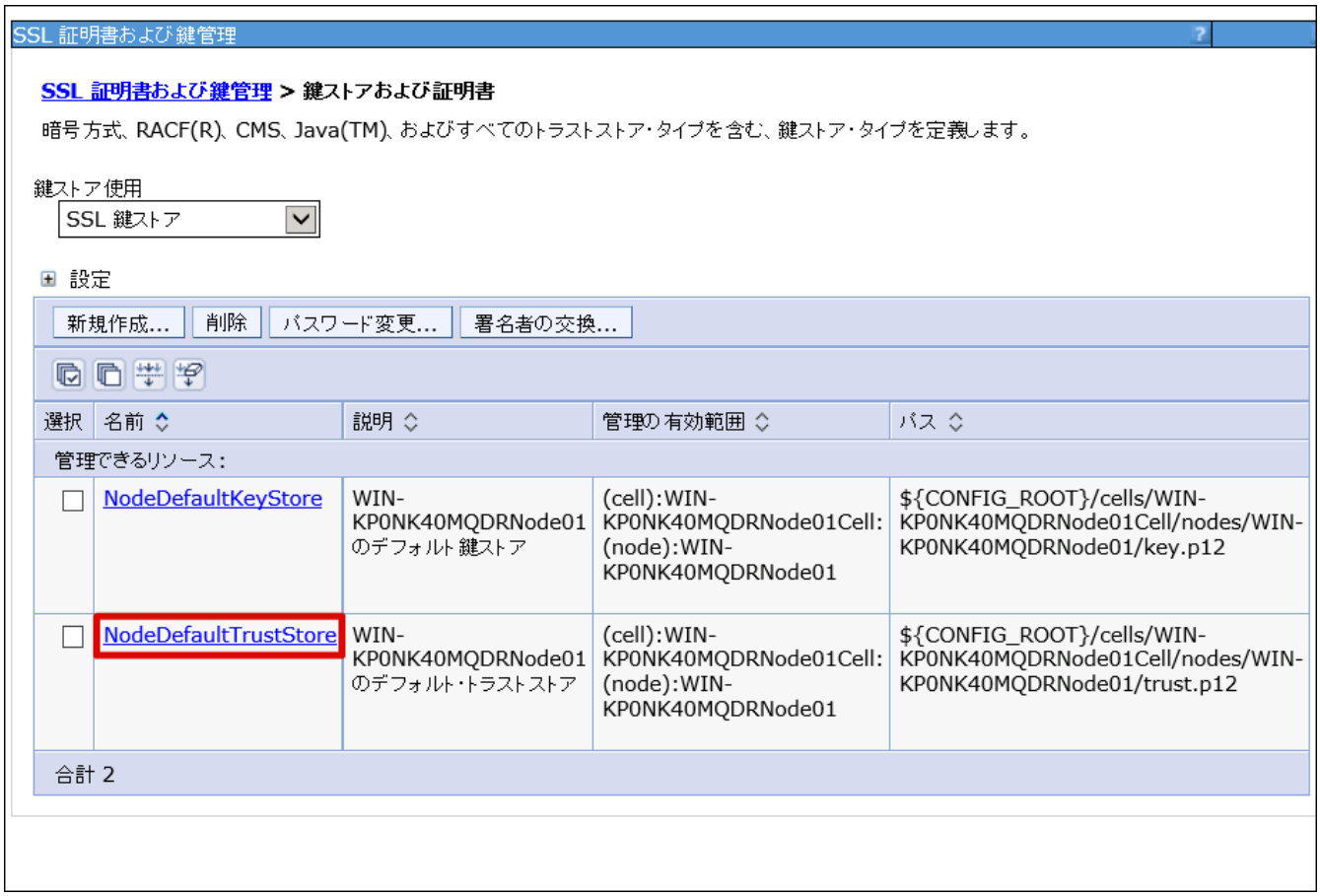
1. 以下のURLから証明書ファイルをダウンロードして、WebSphereサーバ内の任意のディレクトリに配置します。
   - https://cacert.omniroot.com/bc2025.crt
2. メニューから[セキュリティー]-[SSL 証明書および鍵管理]を選択します。



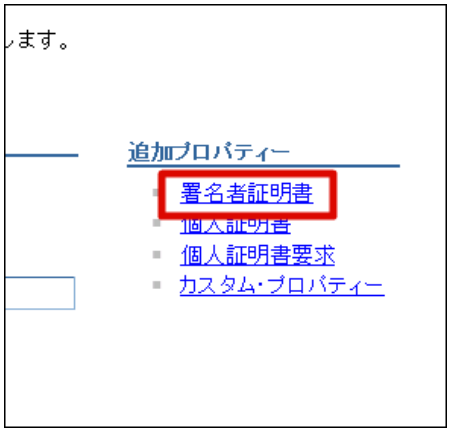
3. [鍵ストアおよび証明書]リンクをクリックします。



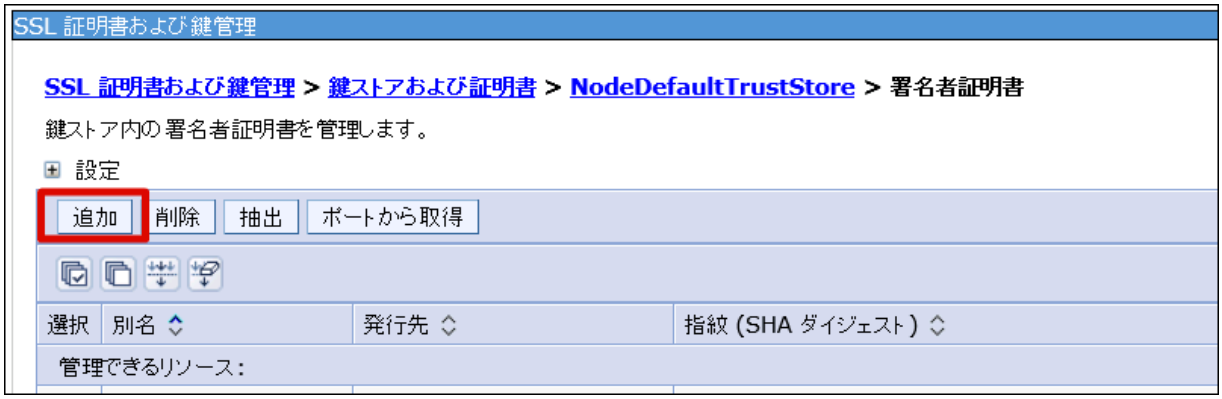
4. [NodeDefaultTrustStore]リンクをクリックします。



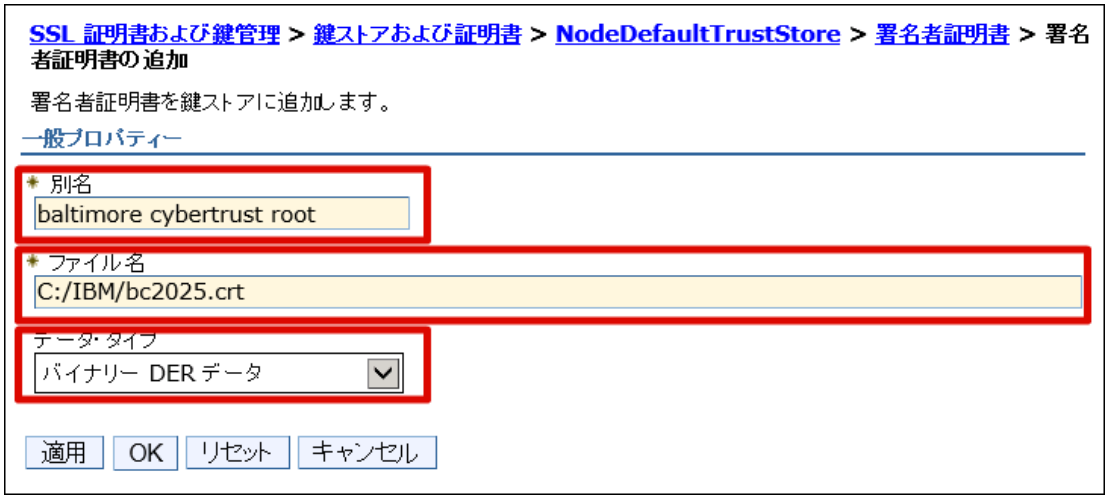
5. [署名者証明書]リンクをクリックします。



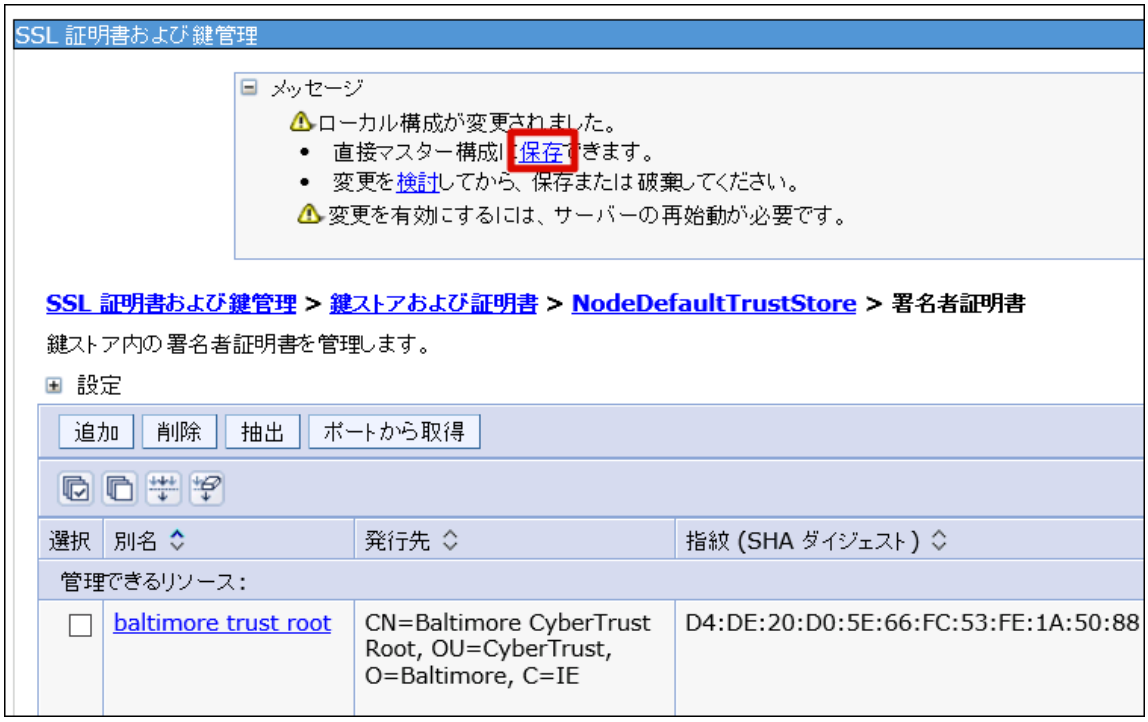
6. [追加]ボタンをクリックします。



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: 「baltimore cybertrust root」
   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。



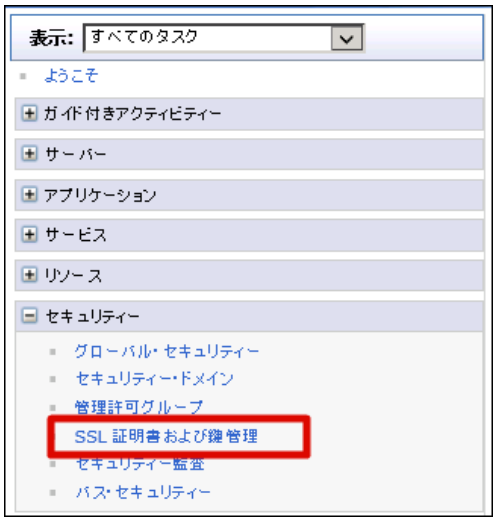
8. [保存]をクリックします。



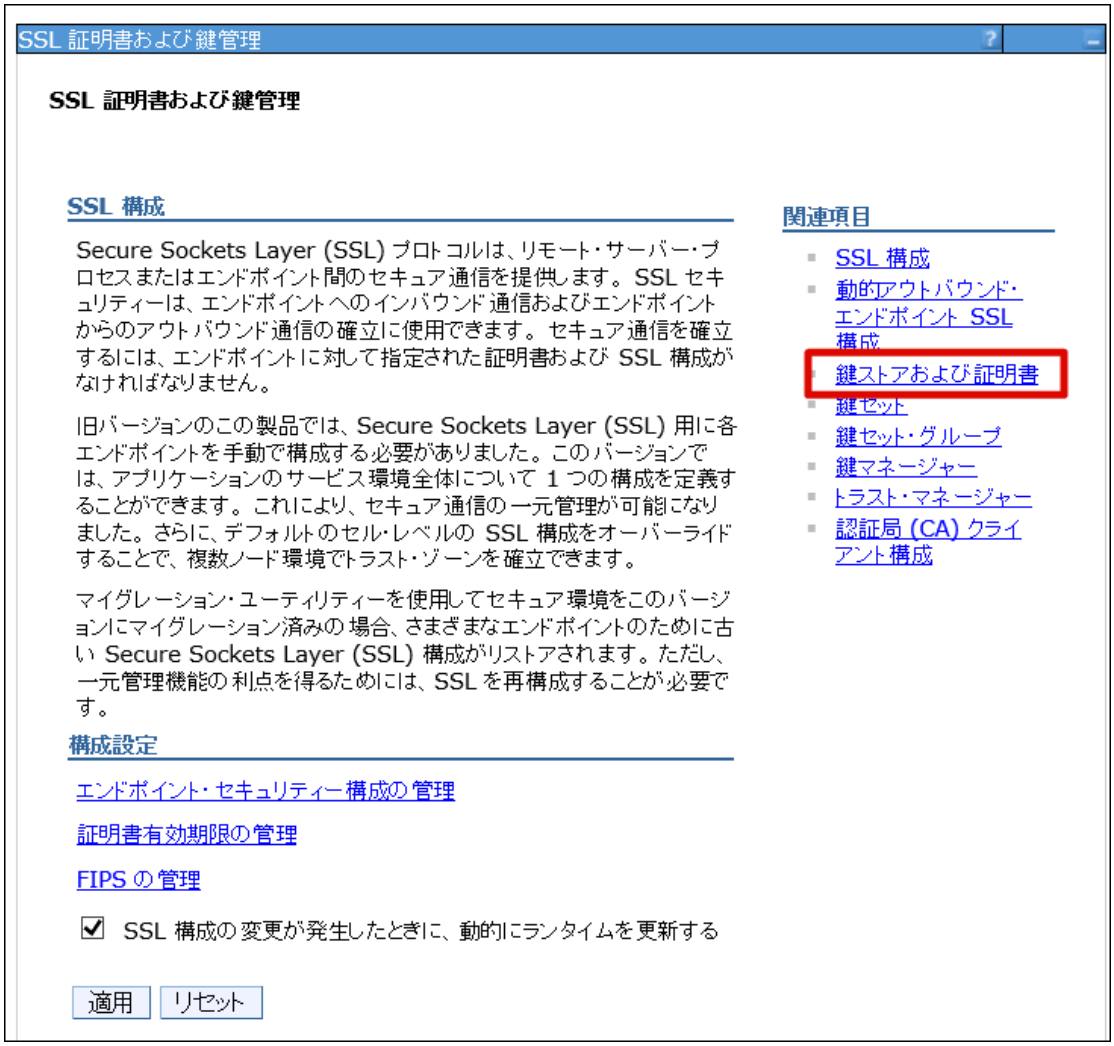
9. WebSphereサーバを再起動することで、設定が反映されます。

VeriSign Class 3 Primary CA - G5を追加する

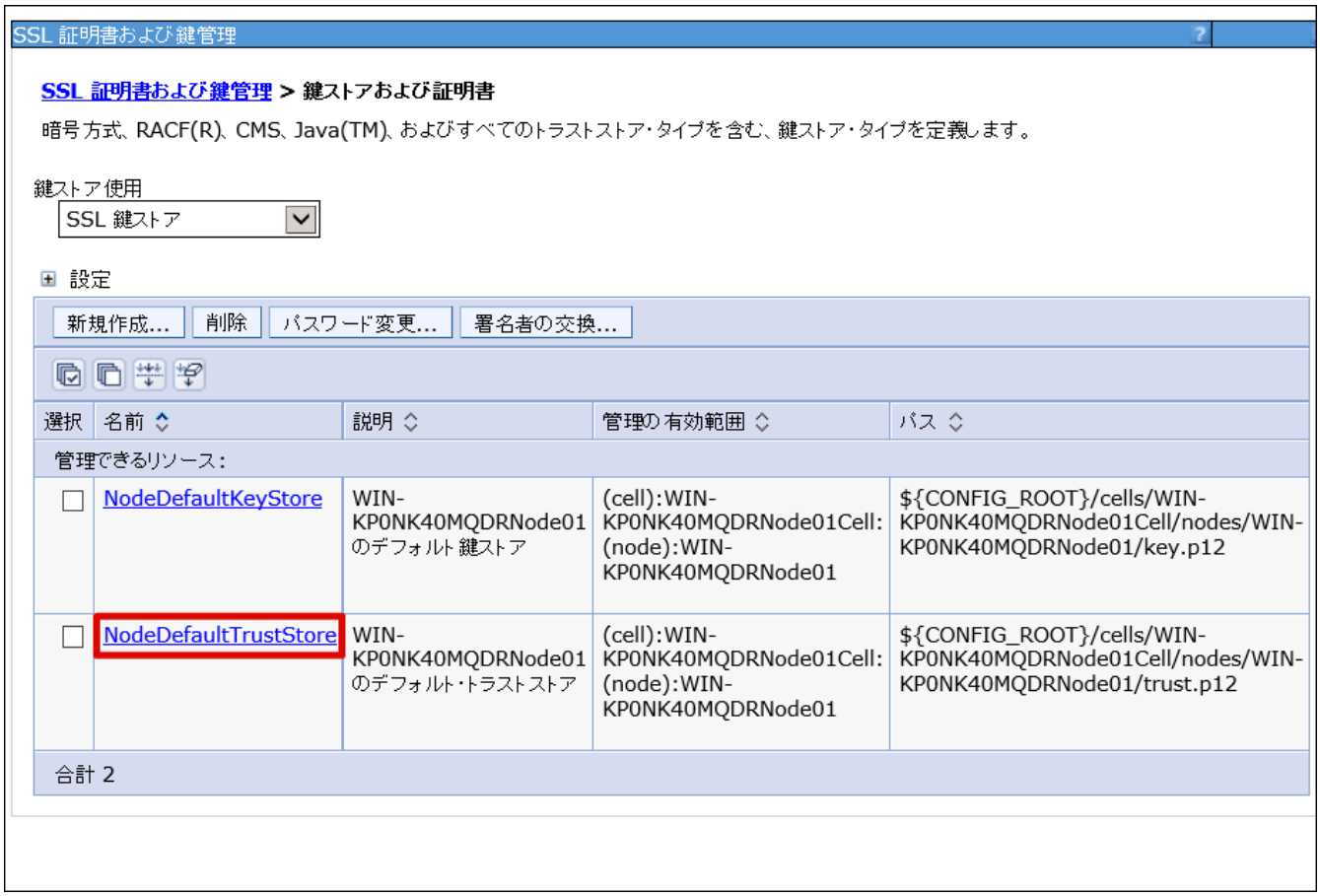
1. 以下のURLから「VeriSign Class 3 Primary CA - G5」証明書ファイルをダウンロードして、WebSphereサーバ内の任意のディレクトリに配置します。
   - https://www.symantec.com/page.jsp?id=roots
2. メニューから[セキュリティー]-[SSL 証明書および鍵管理]を選択します。



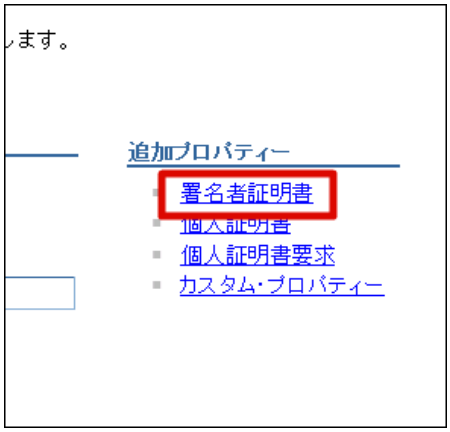
3. [鍵ストアおよび証明書]リンクをクリックします。



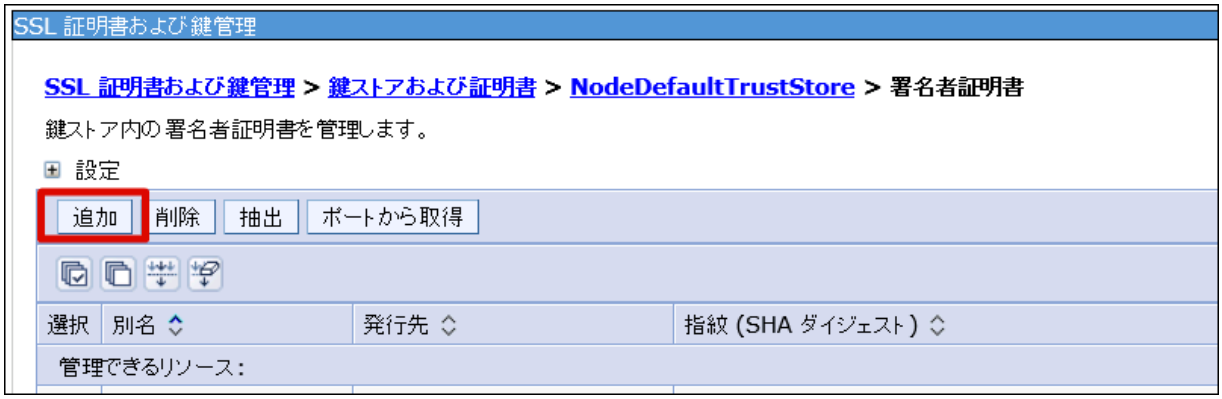
4. [NodeDefaultTrustStore]リンクをクリックします。



5. [署名者証明書]リンクをクリックします。

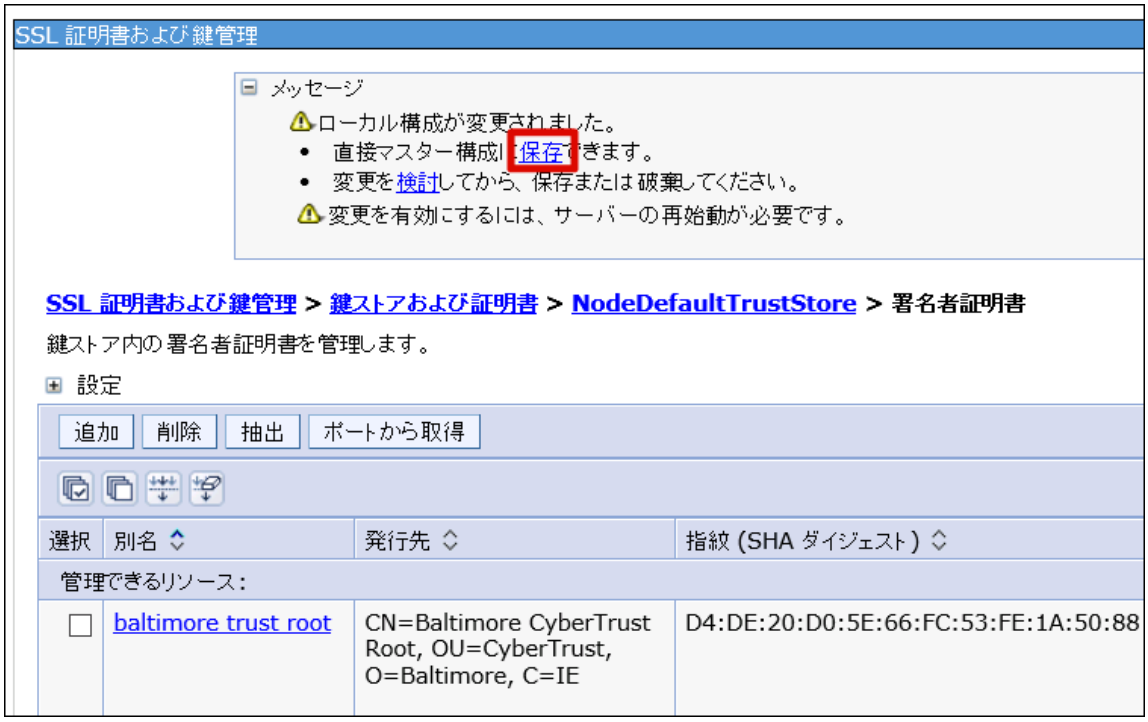


6. [追加]ボタンをクリックします。



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: 「VeriSign Class 3 Primary CA」
   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 「Base64 エンコード ASCII データ」を選択します。

8. [保存]をクリックします。



9. WebSphereサーバ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>
      <immediateFlush>true</immediateFlush>
    </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 （English）
  https://msdn.microsoft.com/ja-jp/library/azure/dn645545.aspx （日本語）
  https://msdn.microsoft.com/zh-CN/library/azure/dn645545.aspx （中文）

- 「認証コード付与フロー」

  https://msdn.microsoft.com/en-US/library/azure/dn645542.aspx （English）
  https://msdn.microsoft.com/ja-jp/library/azure/dn645542.aspx （日本語）
  https://msdn.microsoft.com/zh-CN/library/azure/dn645542.aspx （中文）

- 「OAuth 2.0 でのエラー処理」

  https://msdn.microsoft.com/en-US/library/azure/dn645540.aspx （English）
  https://msdn.microsoft.com/ja-jp/library/azure/dn645540.aspx （日本語）
  https://msdn.microsoft.com/zh-CN/library/azure/dn645540.aspx （中文）

- 「Authorization Endpoint Errors」

  https://msdn.microsoft.com/en-US/library/azure/dn645544.aspx （English）
  https://msdn.microsoft.com/ja-jp/library/azure/dn645544.aspx （日本語）
  https://msdn.microsoft.com/zh-CN/library/azure/dn645544.aspx （中文）

- 「Token Issuance Endpoint Errors」

  https://msdn.microsoft.com/en-US/library/azure/dn645548.aspx （English）
  https://msdn.microsoft.com/ja-jp/library/azure/dn645548.aspx （日本語）
  https://msdn.microsoft.com/zh-CN/library/azure/dn645548.aspx （中文）

- 「Errors from Secured Resources」

  https://msdn.microsoft.com/en-US/library/azure/dn645539.aspx （English）
  https://msdn.microsoft.com/ja-jp/library/azure/dn645539.aspx （日本語）
  https://msdn.microsoft.com/zh-CN/library/azure/dn645539.aspx （中文）

Office 365

- 「Office 365 API reference」

  https://msdn.microsoft.com/en-us/office/office365/api/api-catalog

- 「Office 365 OneDrive REST API」

  https://dev.onedrive.com/README.htm

- 「Office 365 application manifest and permission details」

  https://msdn.microsoft.com/office/office365/HowTo/application-manifest

- 「Office 365 OAuth Sandbox」

  https://oauthplay.azurewebsites.net/

- 「Office 365 API 入門 - 松崎 剛 Blog」

  http://blogs.msdn.com/b/tsmatsuz/archive/2014/06/02/office-365-api-programming.aspx

- 「Azure Active Directory とは (事前準備) - 松崎 剛 Blog」

  http://blogs.msdn.com/b/tsmatsuz/archive/2012/09/01/windows-azure-active-directory-aad-basics.aspx

- 「Azure Active Directory の Common Consent Framework (Client 側) - 松崎 剛 Blog」

  http://blogs.msdn.com/b/tsmatsuz/archive/2014/04/02/microsoft-azure-active-directory-user-consent-administrator-consent-for-multi-tenant-application.aspx

- 「Azure Active Directory の Common Consent Framework (Service 側) - 松崎 剛 Blog」

  http://blogs.msdn.com/b/tsmatsuz/archive/2014/05/27/microsoft-azure-active-directory-consent-ui-permissions-asp-net-web-api-programming-and-impersonation.aspx