



- 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. 連携方式について
 - 3.3. アクター
 - 3.4. セットアップの手順について
- 4. Microsoft 365 の準備
 - 4.1. Microsoft 365 の利用を開始する
 - 4.2. Microsoft 365 にユーザを登録する
- 5. Microsoft Azure の準備
 - 5.1. 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
 - 5.2. ユーザ単位で連携する方式（認可コードフロー）のアプリケーションを設定する
 - 5.3. システム間で連携する方式（クライアントクレデンシャルフロー）のアプリケーションを設定する
- 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. OAuthプロバイダを設定する（システム間連携）
 - 7.1. プロバイダを登録する
- 8. 動作確認（連携を行う）
- 9. 連携を解除するには
 - 9.1. ユーザ単位で連携する方式の場合
 - 9.2. システム間で連携する方式の場合
- 10. トラブルシューティング
 - 10.1. 「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
 - 10.2. エラーメッセージが出力される
- 11. 付録
 - 11.1. WebSphere Application Server 利用時の追加設定
 - 11.2. HTTP通信のログ出力方法
- 12. 参考文献
 - 12.1. OAuth 2.0
 - 12.2. Microsoft Azure
 - 12.3. Microsoft 365

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
2026-10-01	第10版 下記を追加／変更しました 「連携方式について」を追加し、システム間で連携する方式（クライアントクレデンシャルフロー）の説明を追加 「Microsoft Azure の準備」 - 「システム間で連携する方式（クライアントクレデンシャルフロー）のアプリケーションを設定する」を追加 「OAuth プロバイダを設定する（システム間連携）」を追加 「intra-mart Accel Platform をセットアップする」、「動作確認（連携を行う）」、「連携を解除するには」にシステム間で連携する方式についての記述を追加 「Microsoft Azure の準備」の既存の手順を最新の Microsoft Entra ID の管理ポータルに合わせて変更 「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」を最新の Microsoft Entra ID の管理ポータルに合わせた記述に変更

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。

項目

- Office 365 連携 について
- 連携方式について
- アクター
- セットアップの手順について
 - ユーザ単位で連携する方式（認可コードフロー）
 - システム間で連携する方式（クライアントクレデンシャルフロー）

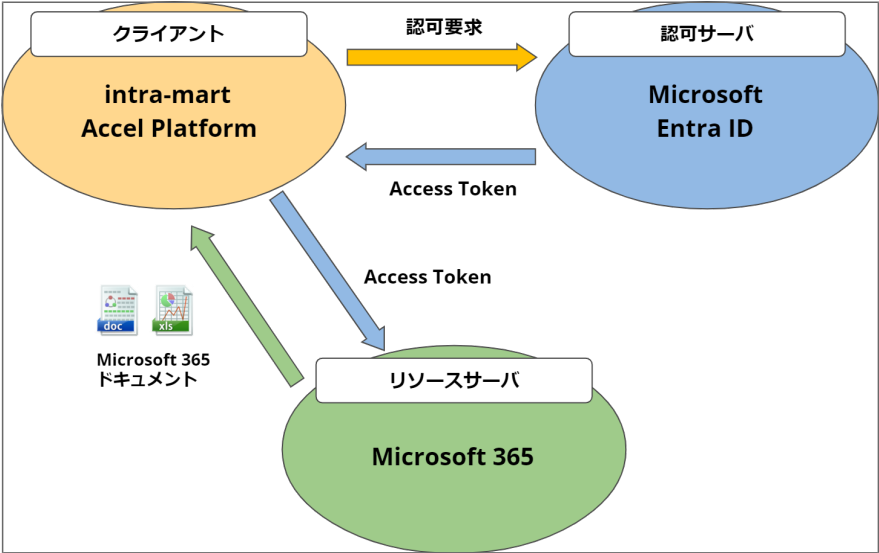
Office 365 連携 について

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>

連携方式について

Office 365 連携 では、以下の2つの連携方式を利用できます。
利用する方式に合わせて、各章の手順を行ってください。

項目	ユーザ単位で連携する方式	システム間で連携する方式
OAuth 2.0 のフロー	認可コードフロー	クライアントクレデンシャルフロー
Microsoft 365 へアクセスする主体	intra-mart Accel Platform にログインしているユーザ	intra-mart Accel Platform （アプリケーション）
利用者による許可の操作	必要（各ユーザが「外部連携アプリケーション」で許可します）	不要

項目	ユーザ単位で連携する方式	システム間で連携する方式
Microsoft Entra ID での認証情報	クライアントシークレット	証明書
Microsoft Entra ID での API のアクセス許可	委任されたアクセス許可	アプリケーションの許可（管理者の同意が必要）
本書で説明する設定方法	設定ファイル（oauth-provider-config）をシステム管理者 が編集します	「OAuthプロバイダ設定」画面から テナント管理者 が登録します

- **ユーザ単位で連携する方式**
ユーザごとに Microsoft 365 のアカウントと連携し、そのユーザの権限で Microsoft 365 のリソースにアクセスします。
- **システム間で連携する方式**
ユーザの操作を介さず、intra-mart Accel Platform がアプリケーションとして Microsoft 365 のリソースにアクセスします。バッチ処理など、ユーザに依存しない連携を行う場合に利用します。

本書では、ユーザ単位で連携する方式は設定ファイルで設定する手順、システム間で連携する方式は「OAuthプロバイダ設定」画面で設定する手順を説明します。

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
- **intra-mart Accel Platform テナント管理者**
intra-mart Accel Platform のテナントの管理者

セットアップの手順について

セットアップは連携方式ごとに以下の手順で行います。

ユーザ単位で連携する方式（認可コードフロー）

- 「[Microsoft 365 の準備](#)」
- 「[Microsoft Azure の準備](#)」 - 「[ユーザ単位で連携する方式（認可コードフロー）のアプリケーションを設定する](#)」
- 「[intra-mart Accel Platform をセットアップする](#)」
- 「[動作確認（連携を行う）](#)」

システム間で連携する方式（クライアントクレデンシャルフロー）

- 「[Microsoft 365 の準備](#)」
- 「[Microsoft Azure の準備](#)」 - 「[システム間で連携する方式（クライアントクレデンシャルフロー）のアプリケーションを設定する](#)」
- 「[intra-mart Accel Platform をセットアップする](#)」
- 「[OAuthプロバイダを設定する（システム間連携）](#)」

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

- [Microsoft 365 の利用を開始する](#)
- [Microsoft 365 にユーザを登録する](#)



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。

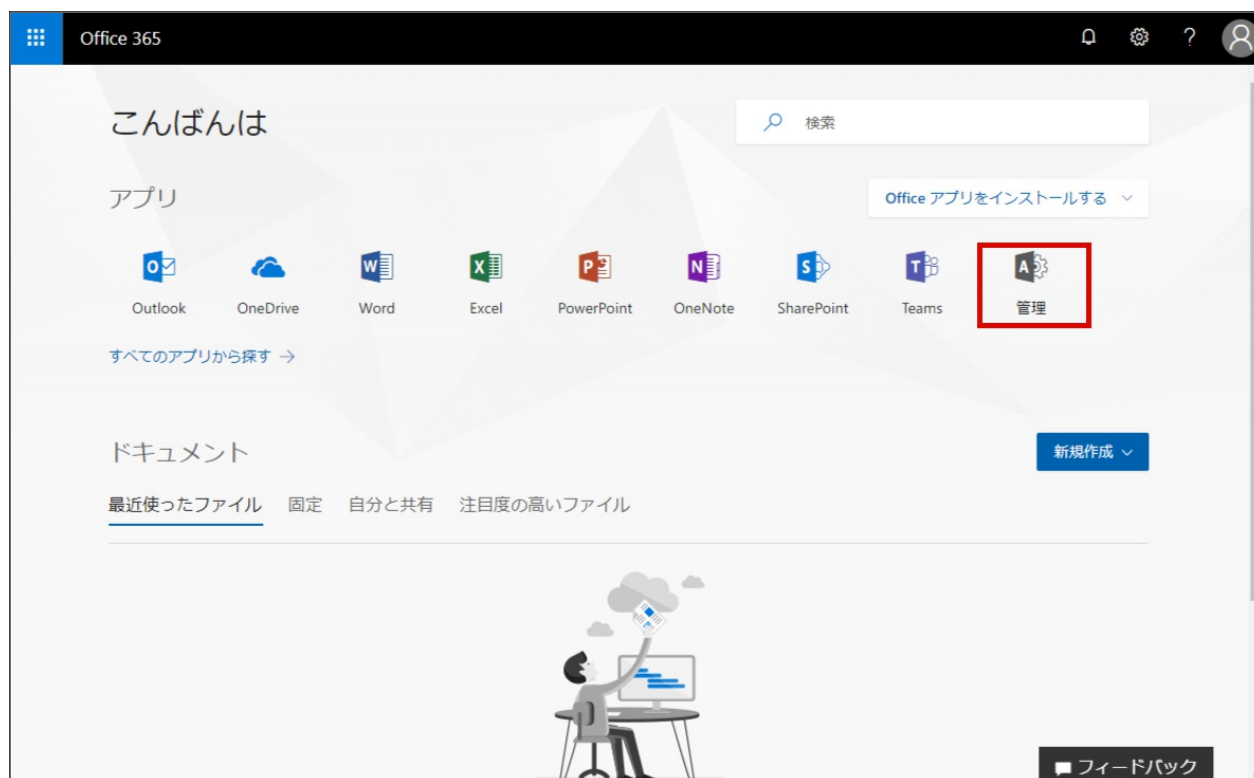
intra-mart Accel Platform 上の各ユーザに対応するユーザが必要です。

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 365 admin center

ホーム ユーザー アクティブなユーザー 削除済みのユーザー グループ 課金情報 サポート 設定 セットアップ レポート 正常性 管理センター

青柳 辰巳
aoyagi@imarttrial01.onmicrosoft.com

姓 名
青柳 辰巳

表示名 *
青柳 辰巳

ユーザー名 * ドメイン
aoyagi @ imarttrial01.onmicrosoft.c

場所
日本

連絡先情報

パスワード 自動生成

役割 ユーザー (管理者アクセス権なし)

製品ライセンス * Office 365 Business

追加 キャンセル

ヘルプが必要ですか? フィードバック

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。
アプリケーションの設定は、連携方式によって手順が異なります。連携方式については「[連携方式について](#)」を参照してください。

- ユーザ単位で連携する方式の場合は、「[ユーザ単位で連携する方式（認可コードフロー）のアプリケーションを設定する](#)」を行ってください。
- システム間で連携する方式の場合は、「[システム間で連携する方式（クライアントクレデンシャルフロー）のアプリケーションを設定する](#)」を行ってください。

項目

- [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](#)
- [ユーザ単位で連携する方式（認可コードフロー）の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](#)
 - [アプリケーションを設定する](#)
- [システム間で連携する方式（クライアントクレデンシャルフロー）の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](#)
 - [証明書をアップロードする](#)
 - [APIのアクセス許可を設定する](#)
 - [管理者の同意を与える](#)



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。

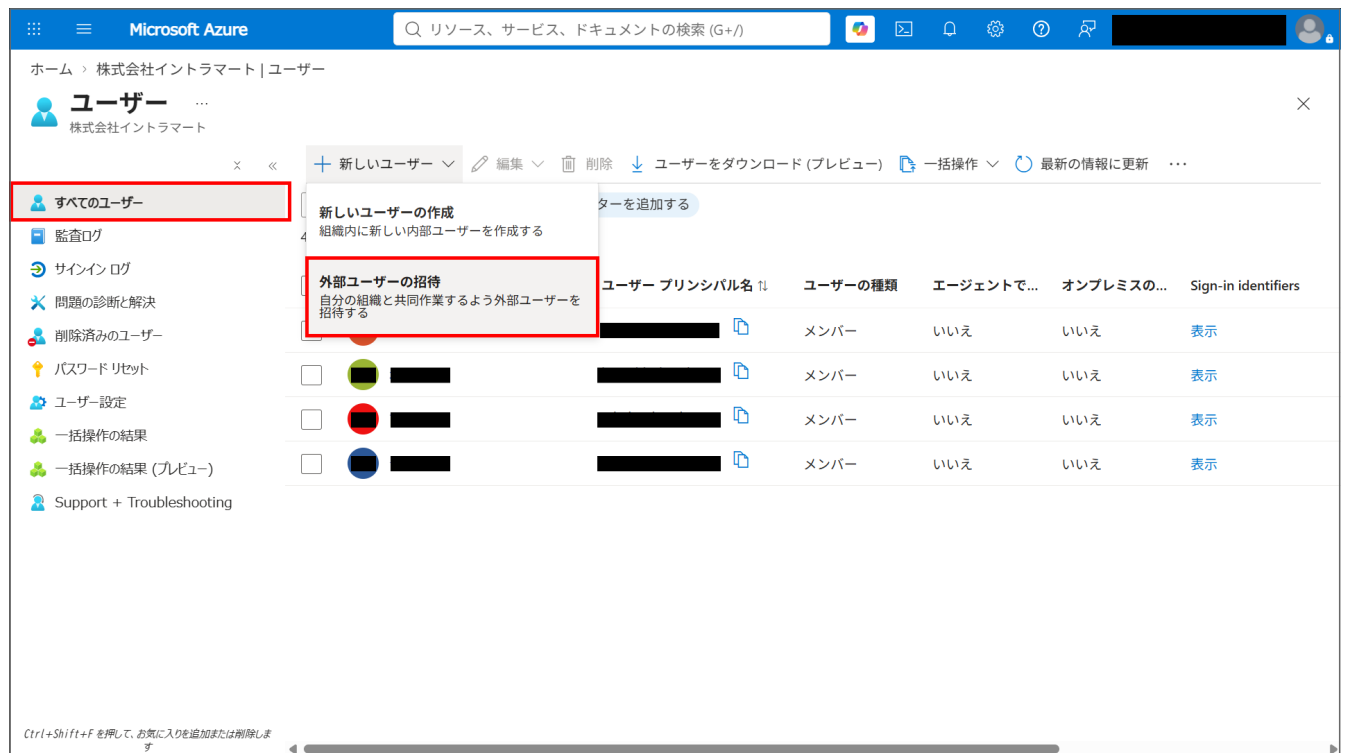
すでに存在する Microsoft Azure 管理者ユーザから Microsoft 365 の組織のディレクトリを参照可能にする

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. 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 アドレス」には 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。

Microsoft Azure

ホーム > 株式会社イントラマート | ユーザー > ユーザー

外部ユーザーの招待 ...

自分の組織と共同作業するよう外部ユーザーを招待する

基本 プロパティ 割り当て 確認と招待

Starting December 2025, B2B invitation emails will be sent from your organization's primary domain (e.g., contoso.onmicrosoft.com) instead of Microsoft.com. [Learn More](#)

組織と共同作業を行う新しいゲスト ユーザーを招待します。ユーザーはメールで招待を受け取り、それを受け入れると共同作業を開始できます。 [詳細情報](#)

ID

メール アドレス ① *

表示名

招待メッセージ

招待メッセージの送信 ☒

メッセージ

CC 受信者

レビューと 招待

次へ: プロパティ

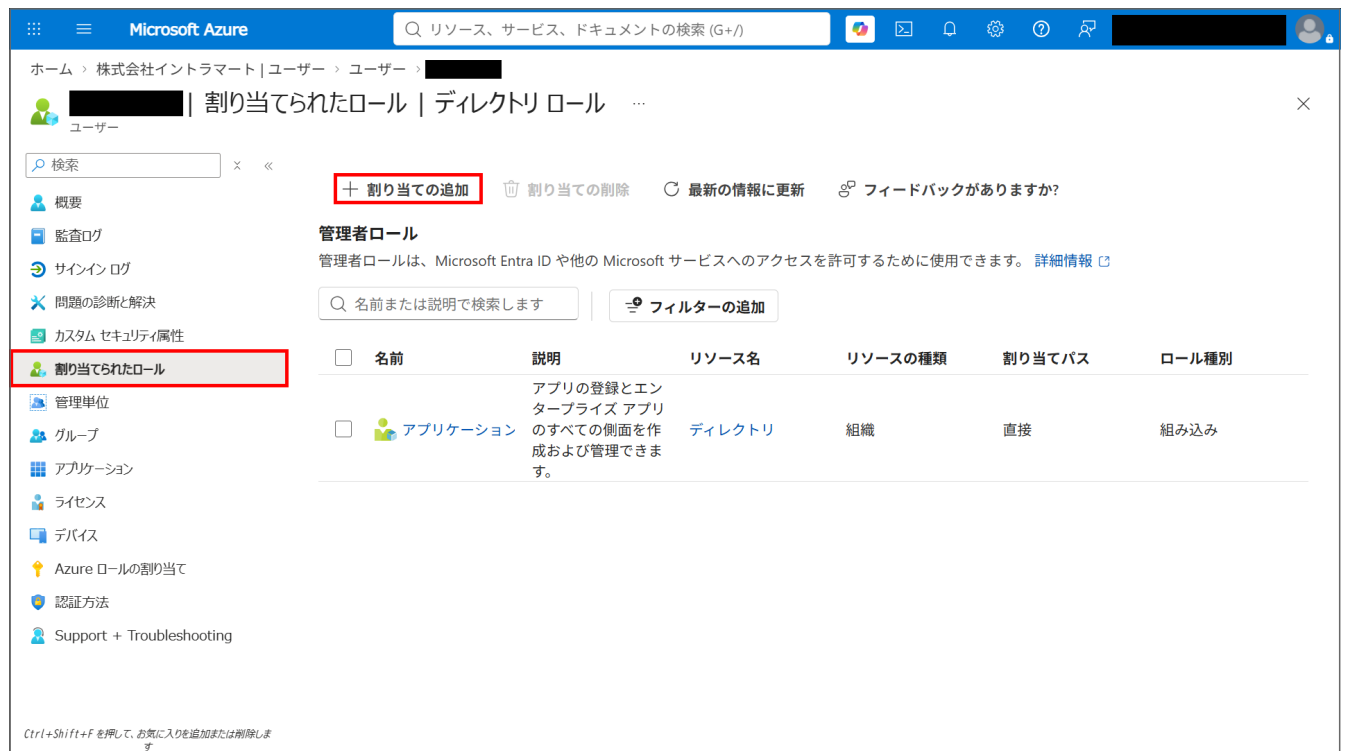
フィードバックの送信



コラム

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

6. 「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。
7. 「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。



8. 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。

ユーザ単位で連携する方式（認可コードフロー）の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。

- 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/>
- サイドメニューから「Microsoft Entra ID」をクリックします。
- 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。
- 「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。
- 「新規登録」をクリックします。
- 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「複数の Entra ID テナント」を選択し、「すべてのテナントを許可する」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



コラム

「複数の Entra ID テナント」を選択すると、「すべてのテナントを許可する」「特定のテナントのみを許可する（プレビュー）」を選択できます。

本書では「すべてのテナントを許可する」を選択した場合の手順を説明します。

「特定のテナントのみを許可する（プレビュー）」はプレビュー機能です。利用する場合は Microsoft 社のドキュメントを参照してください。

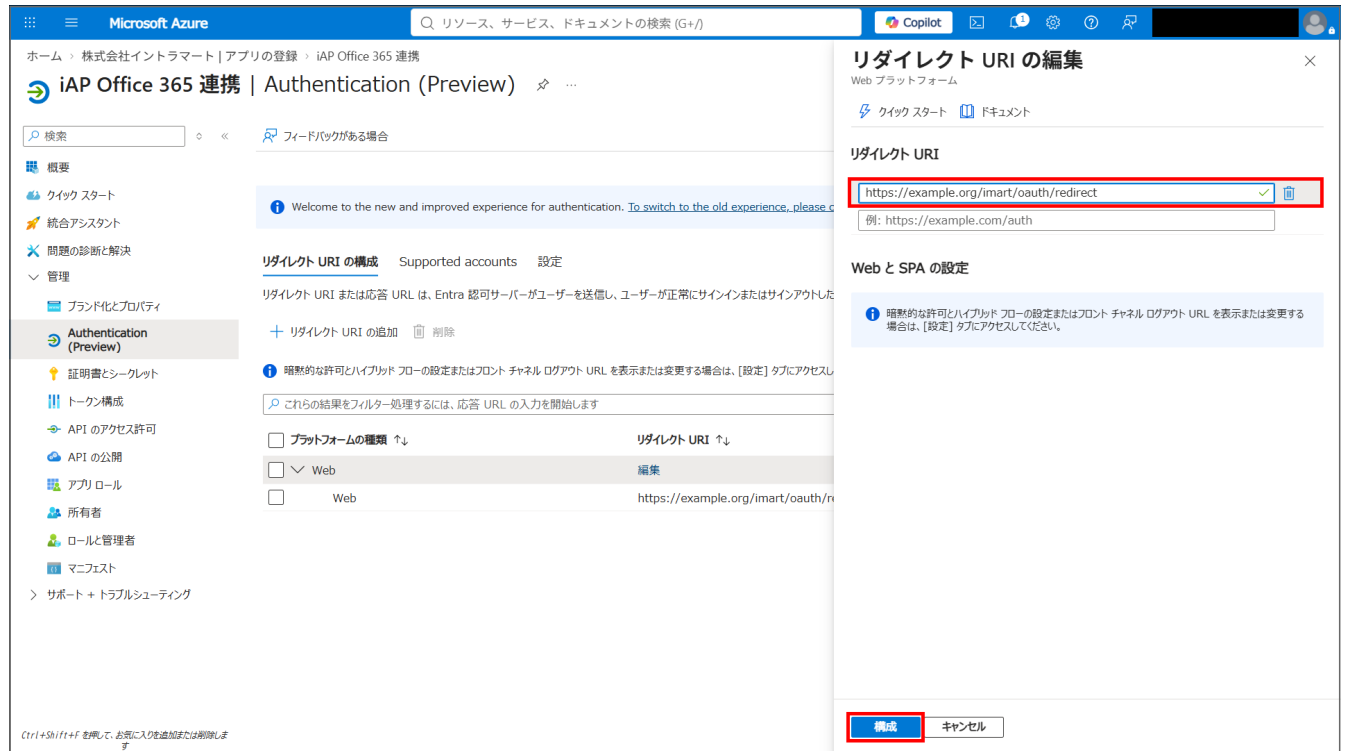
7. 以上でアプリケーションの登録は完了です。

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。

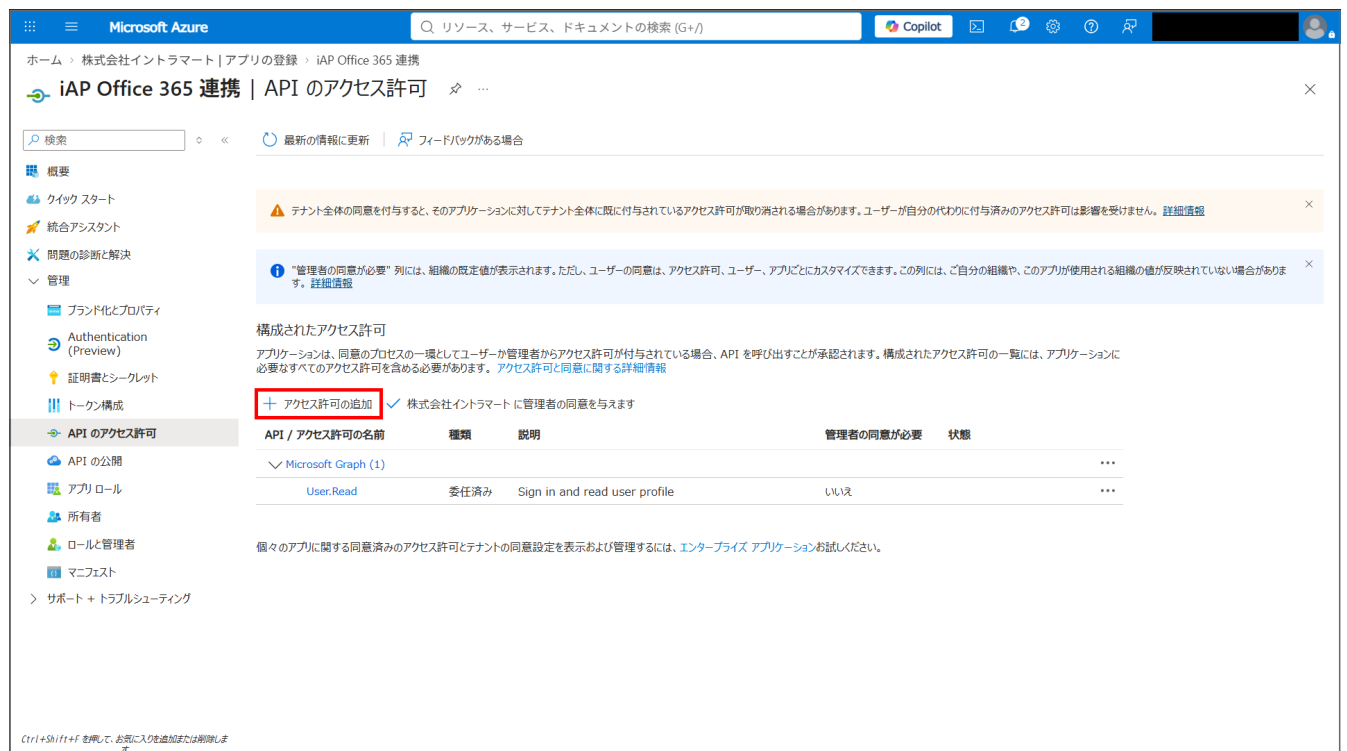
1. 先程登録したアプリの「管理」の「Authentication (Preview)」をクリックします。

- 「リダイレクト URI の構成」タブで、プラットフォームの種類「Web」の「編集」をクリックします。
- 「リダイレクト URI」の値を **ベースURL + /oauth/redirect** に変更して「構成」をクリックします。



The screenshot shows the Microsoft Azure portal interface. The main content area is titled 'iAP Office 365 連携 | Authentication (Preview)'. On the right, a sidebar titled 'リダイレクト URI の編集' (Edit Redirect URI) is open. It shows a list of redirect URIs for the 'Web' platform. The first entry is 'https://example.org/imart/oauth/redirect', which is highlighted with a red box. Below it, there is a '構成' (Configure) button, also highlighted with a red box. The left sidebar shows the 'API のアクセス許可' (API Permissions) section selected.

- 「管理」の「APIのアクセス許可」をクリックします。
- 「アクセス許可の追加」をクリックします。



The screenshot shows the Microsoft Azure portal interface. The main content area is titled 'iAP Office 365 連携 | API のアクセス許可'. It displays a table of permissions for the 'Microsoft Graph' API. The 'アクセス許可の追加' (Add Permission) button is highlighted with a red box. The table below shows the permissions for the 'Microsoft Graph' API.

API / アクセス許可の名前	種類	説明	管理者の同意が必要	状態
Microsoft Graph (1)				
User.Read	委任済み	Sign in and read user profile	いいえ	...

- 「SharePoint」をクリックします。

Microsoft Azure

ホーム > 株式会社イントラマート | アプリの登録 > iAP Office 365 連携

iAP Office 365 連携 | API のアクセス許可

検索

概要

クイック スタート

統合アシスタント

問題の診断と解決

管理

ブランド化とプロパティ

Authentication (Preview)

証明書とシークレット

トークン構成

API のアクセス許可

API の公開

アプリ ロール

所有者

ロールと管理者

マニフェスト

サポート + トラブルシューティング

API アクセス許可の要求

Dynamics CRM

CRM ビジネス ソフトウェアと ERP システムの機能にアクセスします

Intune

Intune データへのプログラムによるアクセス

Office 365 Management APIs

Office 365 と Microsoft Entra ID のアクティビティ ログからユーザー、管理者、システム、ポリシーのアクションとイベントに関する情報を取得します

OneNote

OneNote ノートブック、ノート、リスト、画像、ファイルなどを作成して管理します

Power Automate

フロー テンプレートの埋め込みとフローの管理

Power BI Service

Power BI のデータセット、テーブル、行などのダッシュボード リソースへのプログラムによるアクセス

SharePoint

SharePoint データとリモートで対話します

Skype for Business

リアルタイムのプレゼンス、セキュリティで保護されたメッセージング、通話、会議の機能を統合します

Yammer

Yammer Web インターフェイス内のリソース (メッセージ、ユーザー、グループなど) にアクセスします

その他の Microsoft API

Azure Batch

クラウドにおける大規模な並列アプリケーションと HPC アプリケーションをスケジューリングします

Azure Cosmos DB

あらゆる規模に対応する、オープン API を備えた高速 NoSQL データベース

Azure Data Explorer

ほぼリアルタイムの複雑な分析ソリューションを構築するため、TB 単位のデータに対してアドホック クエリを実行する

Azure Data Explorer (with Multifactor Authentication)

ほぼリアルタイムの複雑な分析ソリューションを構築するため、TB 単位のデータに対してアドホック クエリを実行する

Azure Data Lake

ビッグ データ分析シナリオのストレージとコンピューティングへのアクセス

Azure Data Manager for Energy

Azure Data Manager for Energy サービス API へのプログラムによるアクセス

構成されたアクセス許可

アプリケーションは、同意のプロセスの一環としてユーザーが管理者からアクセス許可を必要とするすべてのアクセス許可を含める必要があります。アクセス許可と同意に同意します。

アクセス許可の追加

株式会社イントラマートに管理者の同意を

API / アクセス許可の名前

種類

説明

Microsoft Graph (1)

User.Read

委任済み

Sign in and read user profile

個々のアプリに関する同意済みのアクセス許可とテナントの同意設定を表示お

Ctrl+Shift+F を押して、お気に入りのリンクを追加または削除します

7. 「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。

Microsoft Azure

ホーム > 株式会社イントラマート | アプリの登録 > iAP Office 365 連携

iAP Office 365 連携 | API のアクセス許可

検索

概要

クイック スタート

統合アシスタント

問題の診断と解決

管理

ブランド化とプロパティ

Authentication (Preview)

証明書とシークレット

トークン構成

API のアクセス許可

API の公開

アプリ ロール

所有者

ロールと管理者

マニフェスト

サポート + トラブルシューティング

API アクセス許可の要求

すべての API

SharePoint

https://microsoft.sharepoint.com

ドキュメント

SharePoint API は、Microsoft Graph API を介して利用できます。代わりに Microsoft Graph を使用することも検討ください。

アプリケーションに必要なアクセス許可の種類

委任されたアクセス許可

アプリケーションは、サインインしたユーザーとして API にアクセスする必要があります。

アプリケーションの許可

アプリケーションは、サインインしたユーザーなしで、バックグラウンド サービスまたはデモンとして実行されます。

アクセス許可の追加

破棄

Ctrl+Shift+F を押して、お気に入りのリンクを追加または削除します

8. 「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。

Microsoft Azure

ホーム > 株式会社イントラマート | アプリの登録 > iAP Office 365 連携

iAP Office 365 連携 | API のアクセス許可

検索

概要

クイック スタート

統合アシスタント

問題の診断と解決

管理

ブランド化とプロパティ

Authentication (Preview)

証明書とシークレット

トークン構成

API のアクセス許可

API の公開

アプリ ロール

所有者

ロールと管理者

マニフェスト

サポート + トラブルシューティング

API アクセス許可の要求

アクセス許可を選択する

アクセス許可を入力し始めると、これらの結果がフィルター処理されます

“管理者の同意が必要” 列には、組織の既定値が表示されます。ただし、ユーザーの同意は、アクセス許可、ユーザー、アプリごとにカスタマイズできます。この列には、ご自分の組織や、このアプリが使用される組織の値が反映されていない場合があります。詳細情報

アクセス許可

管理者の同意が必要

AllSites (1)

アクセス許可	管理者の同意が必要
☐ AllSites.FullControl ① すべてのサイト コレクションに対するフル コントロール権を持ちます	はい
☐ AllSites.Manage ① すべてのサイト コレクションに含まれる項目とリストの読み取りと書き込み	いいえ
☐ AllSites.Read ① すべてのサイト コレクションにあるアイテムの読み取り	いいえ
☒ AllSites.Write ① すべてのサイト コレクションに含まれる項目の読み取りと書き込み	いいえ

EnterpriseResource

Migration

MyFiles

Project

アクセス許可の追加

破棄

9. 「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。

Microsoft Azure

ホーム > 株式会社イントラマート | アプリの登録 > iAP Office 365 連携

iAP Office 365 連携 | API のアクセス許可

検索

概要

クイック スタート

統合アシスタント

問題の診断と解決

管理

ブランド化とプロパティ

Authentication (Preview)

証明書とシークレット

トークン構成

API のアクセス許可

API の公開

アプリ ロール

所有者

ロールと管理者

マニフェスト

サポート + トラブルシューティング

API アクセス許可の要求

アクセス許可を選択する

アクセス許可を入力し始めると、これらの結果がフィルター処理されます

“管理者の同意が必要” 列には、組織の既定値が表示されます。ただし、ユーザーの同意は、アクセス許可、ユーザー、アプリごとにカスタマイズできます。この列には、ご自分の組織や、このアプリが使用される組織の値が反映されていない場合があります。詳細情報

アクセス許可

管理者の同意が必要

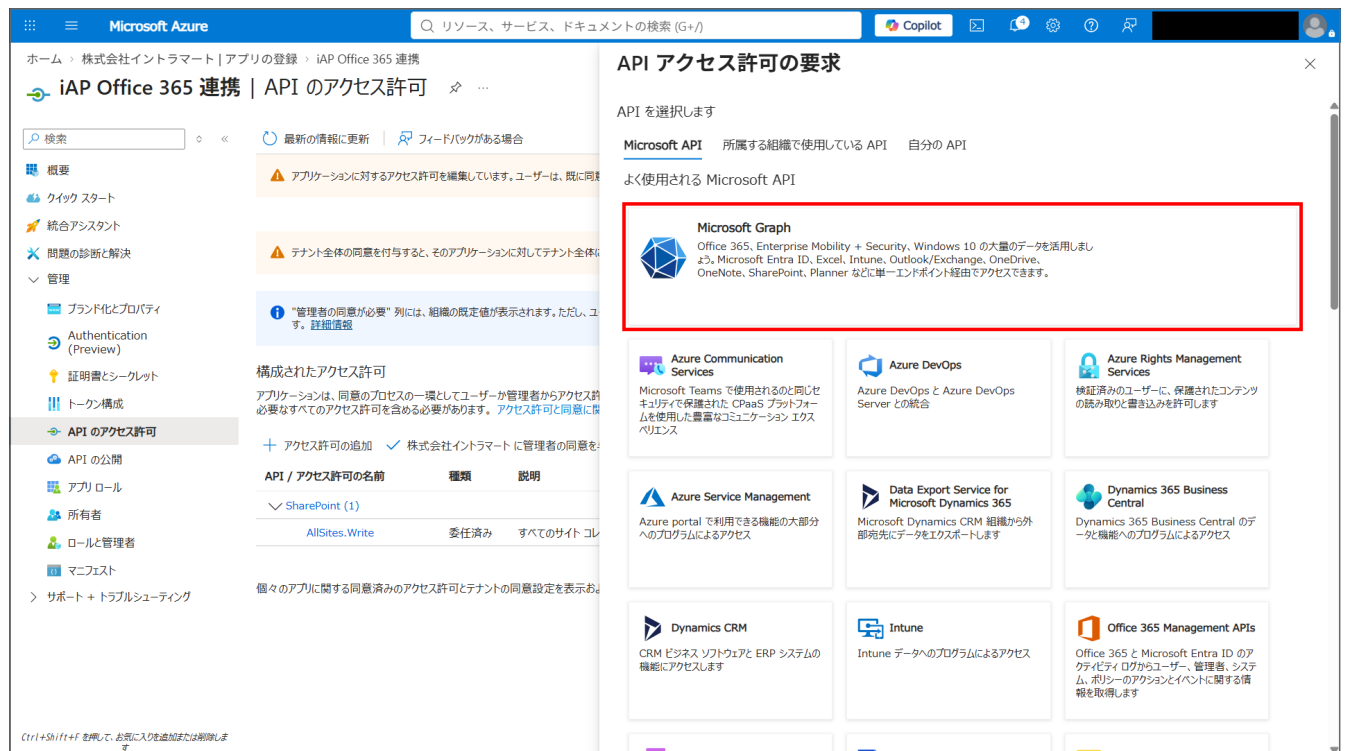
状態

SharePoint (1)

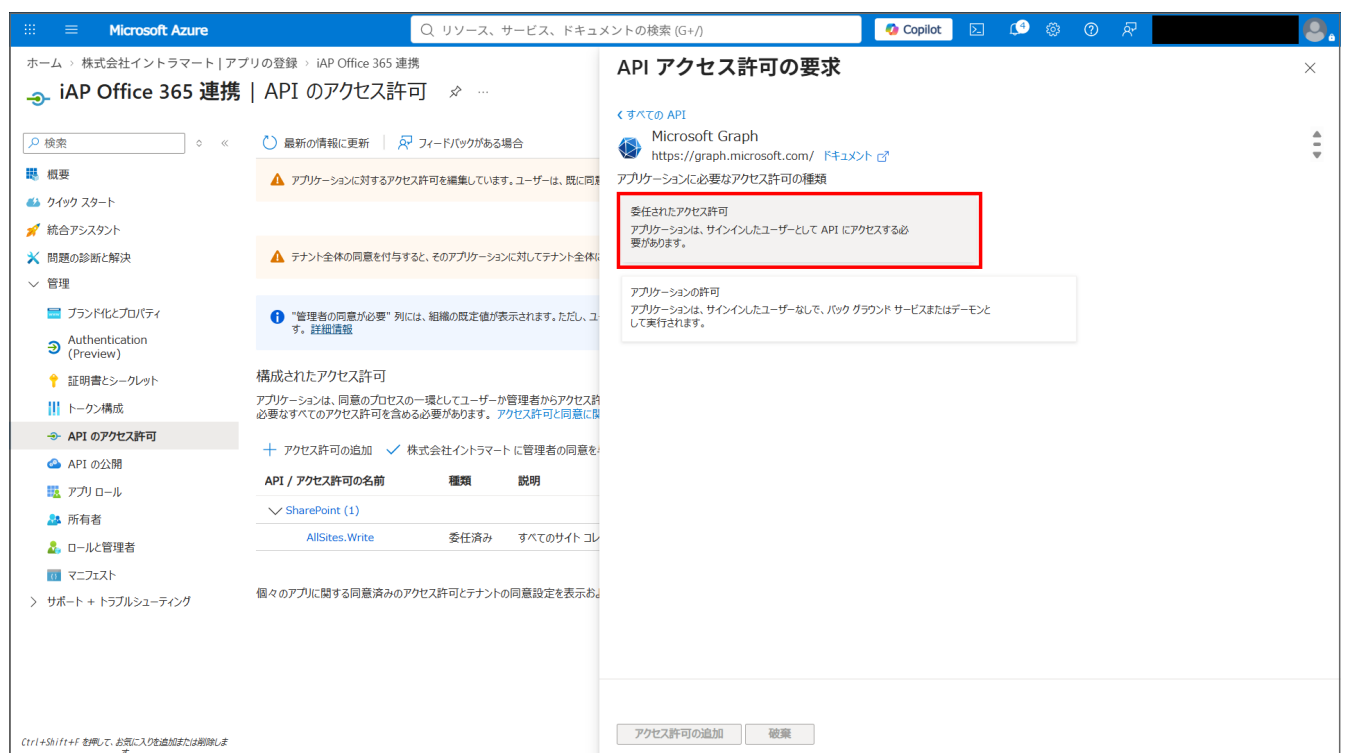
アクセス許可	管理者の同意が必要	状態
☒ AllSites.Write ① すべてのサイト コレクションに含まれる項目の読み取りと書き込み	いいえ	...

個々のアプリに関する同意済みのアクセス許可とテナントの同意設定を表示および管理するには、[エンタープライズ アプリケーション](#)を試してください。

10. 「Microsoft Graph」をクリックします。



11. 「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。



12. 「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のアクセス許可」で設定する「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://learn.microsoft.com/en-us/graph/permissions-reference> (English)
 - <https://learn.microsoft.com/ja-jp/graph/permissions-reference> (日本語)
 - <https://learn.microsoft.com/zh-cn/graph/permissions-reference> (中文)

- 「管理」の「証明書とシークレット」をクリックします。
- 「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。



- 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。

16. 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（クライアント）ID（クライアントIDとして利用します）

- キー（クライアント シークレットの「値」。設定の保存後に一度のみ表示されます）

システム間で連携する方式（クライアントクレデンシャルフロー）のアプリケーションを設定する

システム間で連携する方式で利用するアプリケーションを登録します。

ユーザ単位で連携する方式で登録したアプリケーションとは別に、新しくアプリケーションを登録してください。

i コラム

この方式では、クライアントシークレットではなく証明書を利用して認証します。
事前に、証明書（公開鍵）と、その証明書に対応する秘密鍵を用意してください。

- 証明書（公開鍵）は、以下の「[証明書をアップロードする](#)」で Microsoft Azure にアップロードします。ファイル形式は .cer、.pem、.crt のいずれかです。
- 秘密鍵は、intra-mart Accel Platform 側の設定（「[OAuth プロバイダを設定する（システム間連携）](#)」）で利用します。ファイル形式は PEM 形式 または PKCS#12 形式 です。
- RSA 鍵を利用する場合、鍵長は 2048 ビット以上としてください。

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「シングル テナントのみ - <組織名>」を選択
 - リダイレクト URI は入力不要

Microsoft Azure

ホーム > 株式会社イントラマート | アプリの登録

アプリケーションの登録

* 名前
このアプリケーションのユーザー向け表示名 (後で変更できます)。
IAP Office365 連携 ✓

サポートされているアカウントの種類
このアプリケーションを使用したり、この API にアクセスしたりできるアカウントの種類を選択します
シングル テナントのみ - 株式会社イントラマート 選択に関するヘルプ

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

作業に使用しているアプリをこちらで登録します。ギャラリー アプリと組織外の他のアプリを [\[エンタープライズ アプリケーション\]](#) から追加して統合します。

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

登録

i コラム

この方式では、アクセストークンの取得時に Microsoft 365 の組織のディレクトリ（テナント）ID を指定します。そのため、サポートされているアカウントの種類に「複数の Entra ID テナント」を選択しても動作は変わりません。ただし、ほかの組織のディレクトリから利用されないよう、「シングル テナント」を選択することを推奨します。

7. 以上でアプリケーションの登録は完了です。

「概要」に表示される以下の値を控えておきます。

- アプリケーション（クライアント）ID
- ディレクトリ（テナント）ID

The screenshot shows the Microsoft Azure portal interface for the 'IAP Office365 連携' application. The left sidebar contains navigation options like 'クイック スタート', '統合アシスタント', '問題の診断と解決', '管理', 'ブランド化とプロパティ', 'Authentication (Preview)', '証明書とシークレット', 'トークン構成', 'API のアクセス許可', 'API の公開', 'アプリ ロール', '所有者', 'ロールと管理者', and 'マニフェスト'. The main content area is titled 'IAP Office365 連携' and includes a search bar, action buttons (非アクティブ化, 削除, エンドポイント), and a '概要' (Overview) tab. The '概要' tab shows the following details:

- 表示名: IAP Office365 連携
- クライアントの資格情報: 証明書またはシークレットの追加
- リダイレクト URI: リダイレクト URI を追加する
- アプリケーション ID の URI: アプリケーション ID URI の追加
- ローカル ディレクトリでのマネ...: IAP Office365 連携
- 状態: アクティブ化済み

Below the details, there are two informational messages: one about providing feedback for the Microsoft ID platform and another about the deprecation of ADAL and Azure AD Graph. At the bottom, there is a section titled 'Microsoft ID プラットフォームを使用してアプリケーションを作成する' with a brief description and a '詳細情報' link.

証明書をアップロードする

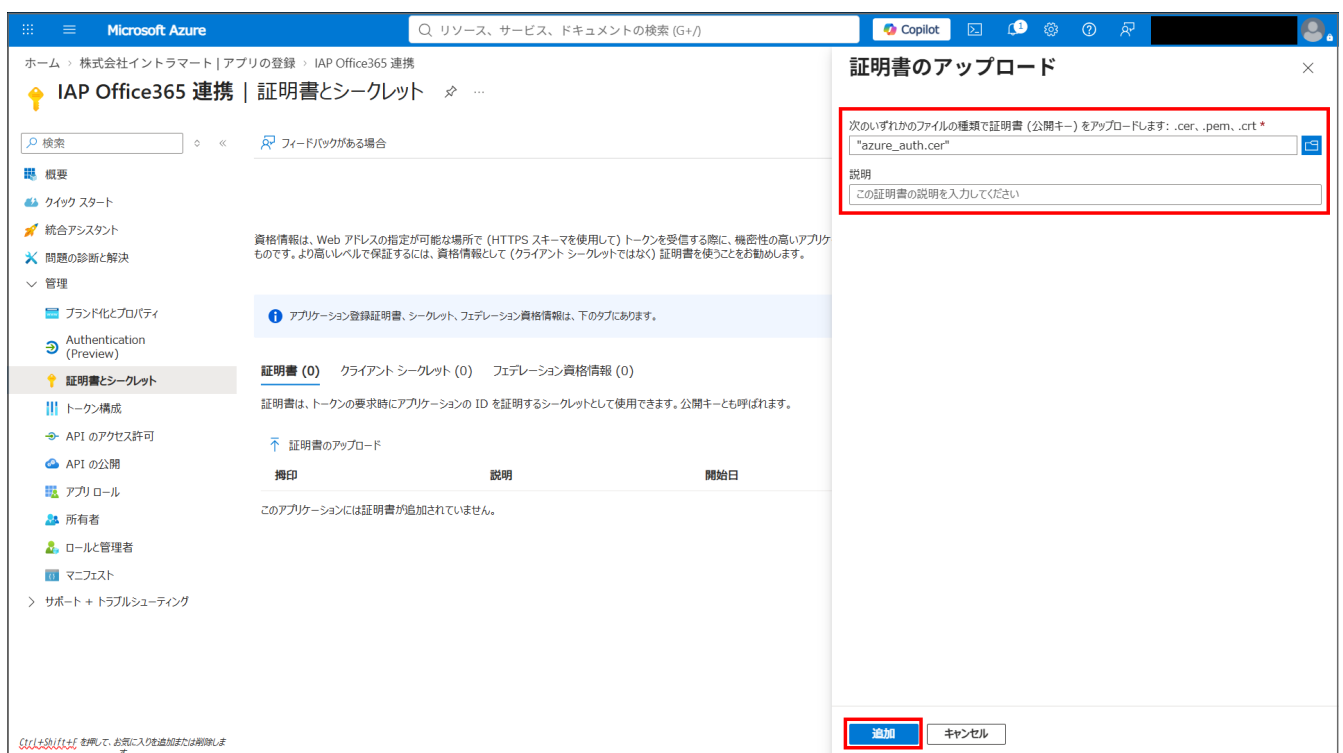
登録したアプリケーションに、認証に利用する証明書（公開鍵）をアップロードします。

1. 先程登録したアプリの「管理」の「証明書とシークレット」をクリックします。
2. 「証明書」タブをクリックし、「証明書のアップロード」をクリックします。

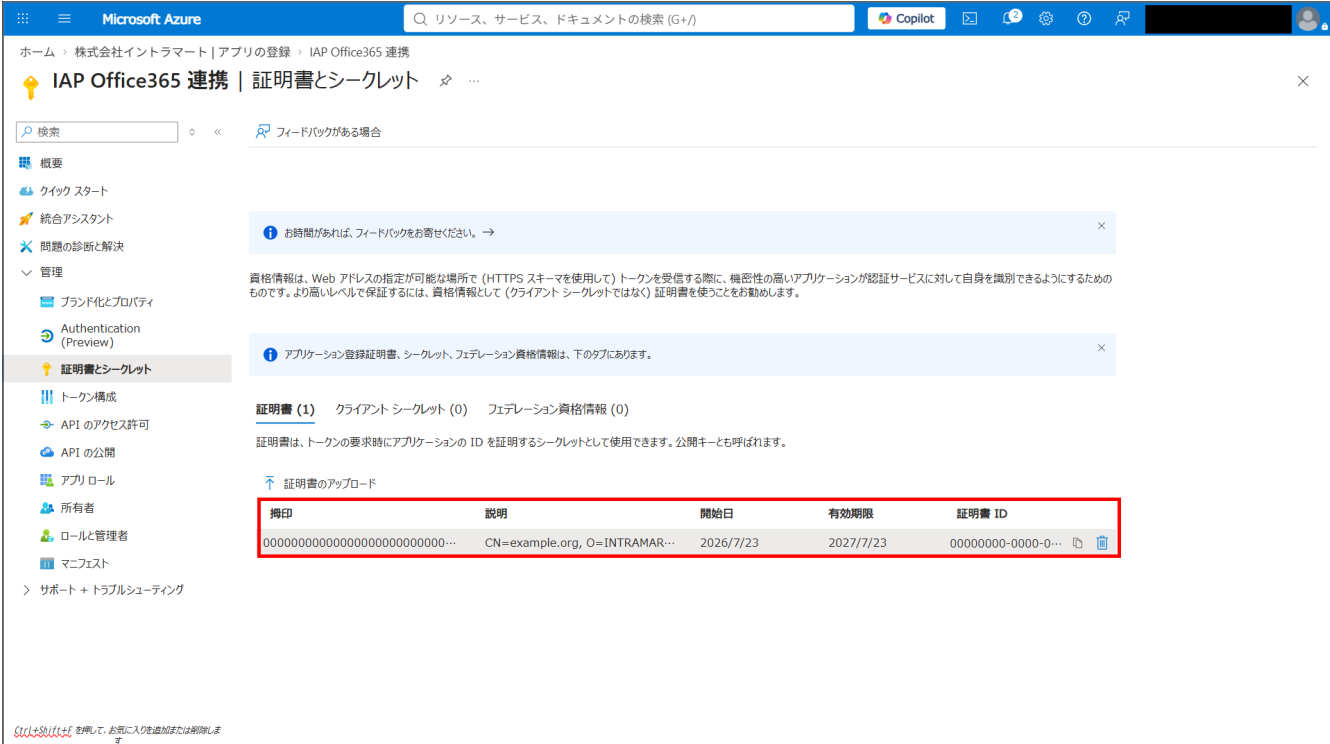


3. 以下を入力または選択して「追加」をクリックします。

- アップロードする証明書（公開鍵）ファイルを選択
- 説明に任意の説明を入力



4. 「証明書」の一覧に、アップロードした証明書が表示されます。
表示された「拇印」の値を控えておきます。



Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+/J)

Copilot

ホーム > 株式会社イントラマート | アプリの登録 > IAP Office365 連携

IAP Office365 連携 | 証明書とシークレット

検索 フィードバックがある場合

概要

クイックスタート

統合アシスタント

問題の診断と解決

管理

ブランド化とプロパティ

Authentication (Preview)

証明書とシークレット

トークン構成

API のアクセス許可

API の公開

アプリ ロール

所有者

ロールと管理者

マニフェスト

サポート + トラブルシューティング

お時間があれば、フィードバックをお寄せください。 →

資格情報は、Web アドレスの指定が可能な場所で (HTTPS スキーマを使用して) トークンを受信する際に、機密性の高いアプリケーションが認証サービスに対して自身を識別できるようにするためのものです。より高いレベルで保証するには、資格情報として (クライアント シークレットではなく) 証明書を使うことをお勧めします。

アプリケーション登録証明書、シークレット、フェデレーション資格情報は、下のタブにあります。

証明書 (1) クライアント シークレット (0) フェデレーション資格情報 (0)

証明書は、トークンの要求時にアプリケーションの ID を証明するシークレットとして使用できます。公開キーとも呼ばれます。

証明書のアップロード

拇印	説明	開始日	有効期限	証明書 ID
00000000000000000000000000000000...	CN=example.org, O=INTRAMAR...	2026/7/23	2027/7/23	00000000-0000-0...

Ctrl+Shift+F を押して、お票に入力を追加または削除します

コラム

「拇印」は intra-mart Accel Platform 側の設定で、追加設定の「x5t」として設定します。
画面に表示されている値（16進数）をそのまま設定してください。

コラム

証明書の有効期限が切れた場合は、新しい証明書をアップロードし、intra-mart Accel Platform 側の秘密鍵と「x5t」の値を更新する必要があります。

APIのアクセス許可を設定する

intra-mart Accel Platform がアプリケーションとして SharePoint Online にアクセスするための権限を設定します。

1. 「管理」の「APIのアクセス許可」をクリックします。
2. 「アクセス許可の追加」をクリックします。
3. 「SharePoint」をクリックします。
4. 「アプリケーションに必要なアクセス許可の種類」の「アプリケーションの許可」をクリックします。

Microsoft Azure

ホーム > 株式会社イントラマート | アプリの登録 > IAP Office365 連携

IAP Office365 連携 | API のアクセス許可

検索

概要

クイック スタート

統合アシスタント

問題の診断と解決

管理

ブランド化とプロパティ

Authentication (Preview)

証明書とシークレット

トークン構成

API のアクセス許可

API の公開

アプリ ロール

所有者

ロールと管理者

マニフェスト

サポート + トラブルシューティング

構成されたアクセス許可

アプリケーションは、同意のプロセスの一環としてユーザーが管理者からアクセス許可を必要とするすべてのアクセス許可を含める必要があります。アクセス許可と同意に詳細情報

アクセス許可の追加

株式会社イントラマートに管理者の同意を

API / アクセス許可の名前

種類

説明

Microsoft Graph (1)

User.Read

委任済み

Sign in and read

個々のアプリに関する同意済みのアクセス許可とテナントの同意設定を表示お

API アクセス許可の要求

すべての API

SharePoint

https://microsoft.sharepoint.com ドキュメント

SharePoint API は、Microsoft Graph API を介して利用できます。代わりに Microsoft Graph を使用することをご検討ください。

アプリケーションに必要なアクセス許可の種類

委任されたアクセス許可

アプリケーションは、サインインしたユーザーとして API にアクセスする必要があります。

アプリケーションの許可

アプリケーションは、サインインしたユーザーとして、バックグラウンド サービスまたはデモンストラとして実行されます。

アクセス許可の追加

破棄

5. 「Sites」をクリックし、「Sites.ReadWrite.All」を選択し、「アクセス許可の追加」をクリックします。

Microsoft Azure

ホーム > 株式会社イントラマート | アプリの登録 > IAP Office365 連携

IAP Office365 連携 | API のアクセス許可

検索

概要

クイック スタート

統合アシスタント

問題の診断と解決

管理

ブランド化とプロパティ

Authentication (Preview)

証明書とシークレット

トークン構成

API のアクセス許可

API の公開

アプリ ロール

所有者

ロールと管理者

マニフェスト

サポート + トラブルシューティング

構成されたアクセス許可

アプリケーションは、同意のプロセスの一環としてユーザーが管理者からアクセス許可を必要とするすべてのアクセス許可を含める必要があります。アクセス許可と同意に詳細情報

アクセス許可の追加

株式会社イントラマートに管理者の同意を

API / アクセス許可の名前

種類

説明

Microsoft Graph (1)

User.Read

委任済み

Sign in and read

個々のアプリに関する同意済みのアクセス許可とテナントの同意設定を表示お

API アクセス許可の要求

OneDrive

SharePointCrossTenantMigration

SharePointTenantSettings

SitesMetadataAdmin

Sites (1)

Sites.FullControl.All

Have full control of all site collections

はい

Sites.Manage.All

Read and write items and lists in all site collections

はい

Sites.Read.All

Read items in all site collections

はい

Sites.ReadWrite.All

Read and write items in all site collections

はい

Sites.Selected

Access selected site collections

はい

TenantReports

TermStore

User

アクセス許可の追加

破棄

コラム

「Sites.ReadWrite.All」を付与すると、組織のすべてのサイトコレクションにアクセスできます。アクセスするサイトを限定したい場合は、「Sites.ReadWrite.All」の代わりに「Sites.Selected」を選択してください。「Sites.Selected」を選択した場合は、アクセスを許可するサイトごとに、このアプリケーションへの権限を別途付与する必要があります。詳細は Microsoft 社の以下のドキュメントを参照してください。

- Overview of Selected permissions in OneDrive and SharePoint :
 - <https://learn.microsoft.com/en-us/graph/permissions-selected-overview> (English)
 - <https://learn.microsoft.com/ja-jp/graph/permissions-selected-overview> (日本語)
 - <https://learn.microsoft.com/zh-cn/graph/permissions-selected-overview> (中文)

アプリケーションの許可は、管理者の同意を与えるまで利用できません。

1. 「APIのアクセス許可」の「<組織名> に管理者の同意を与えます」をクリックします。

Microsoft Azure

ホーム > 株式会社イントラマート | アプリの登録 > IAP Office365 連携

IAP Office365 連携 | API のアクセス許可

検索

最新の情報に更新 | フィードバックがある場合

概要

アプリケーションに対するアクセス許可を編集しています。ユーザーは、既に同意したことがある場合でも同意が必要になります。

テナント全体の同意を付与すると、そのアプリケーションに対してテナント全体に付与されているアクセス許可が取り消される場合があります。ユーザーが自分の代わりに付与済みのアクセス許可は影響を受けません。 [詳細情報](#)

“管理者の同意が必要” 列には、組織の既定値が表示されます。ただし、ユーザーの同意は、アクセス許可、ユーザー、アプリにカスタマイズできます。この列には、ご自分の組織や、このアプリが使用される組織の値が反映されていない場合があります。 [詳細情報](#)

構成されたアクセス許可

アプリケーションは、同意のプロセスの一環としてユーザーが管理者からアクセス許可が付与されている場合、API を呼び出すことが承認されます。構成されたアクセス許可の一覧には、アプリケーションに必要なすべてのアクセス許可を含める必要があります。 [アクセス許可と同意に関する詳細情報](#)

+ アクセス許可の追加 ☒ 株式会社イントラマート に管理者の同意を与えます

API / アクセス許可の名前	種類	説明	管理者の同意が必要	状態
Microsoft Graph (1)				
User.Read	委任済み	Sign in and read user profile	いいえ	...
SharePoint (1)				
Sites.ReadWrite.All	アプリケーション...	Read and write items in all site collections	はい	株式会社イントラマートに... ...

個々のアプリに関する同意済みのアクセス許可とテナントの同意設定を表示および管理するには、[エンタープライズ アプリケーション](#)をお試しください。

2. 確認のメッセージが表示されますので、「はい」をクリックします。
3. 「構成されたアクセス許可」の一覧で、追加したアクセス許可の状態が「<組織名> に付与されました」となっていることを確認します。

Microsoft Azure

ホーム > 株式会社イントラマート | アプリの登録 > IAP Office365 連携

IAP Office365 連携 | API のアクセス許可

検索

最新の情報に更新 | フィードバックがある場合

概要

要求されたアクセス許可の管理者の同意が正常に付与されました。

テナント全体の同意を付与すると、そのアプリケーションに対してテナント全体に付与されているアクセス許可が取り消される場合があります。ユーザーが自分の代わりに付与済みのアクセス許可は影響を受けません。 [詳細情報](#)

“管理者の同意が必要” 列には、組織の既定値が表示されます。ただし、ユーザーの同意は、アクセス許可、ユーザー、アプリにカスタマイズできます。この列には、ご自分の組織や、このアプリが使用される組織の値が反映されていない場合があります。 [詳細情報](#)

構成されたアクセス許可

アプリケーションは、同意のプロセスの一環としてユーザーが管理者からアクセス許可が付与されている場合、API を呼び出すことが承認されます。構成されたアクセス許可の一覧には、アプリケーションに必要なすべてのアクセス許可を含める必要があります。 [アクセス許可と同意に関する詳細情報](#)

+ アクセス許可の追加 ☒ 株式会社イントラマート に管理者の同意を与えます

API / アクセス許可の名前	種類	説明	管理者の同意が必要	状態
Microsoft Graph (1)				
User.Read	委任済み	Sign in and read user profile	いいえ	株式会社イントラマートに... ...
SharePoint (1)				
Sites.ReadWrite.All	アプリケーション...	Read and write items in all site collections	はい	株式会社イントラマートに... ...

個々のアプリに関する同意済みのアクセス許可とテナントの同意設定を表示および管理するには、[エンタープライズ アプリケーション](#)をお試しください。



コラム

管理者の同意を与えるには、アプリケーション管理者、クラウド アプリケーション管理者 または 特権ロール管理者 のいずれかのロールが必要です。

「[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](#)」で「アプリケーション管理者」を割り当てた Microsoft Azure 管理者 は、この操作を行えます。

詳細は Microsoft 社の以下のドキュメントを参照してください。

- アプリケーションに対してテナント全体の管理者の同意を付与する：
 - <https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/grant-admin-consent> (English)
 - <https://learn.microsoft.com/ja-jp/entra/identity/enterprise-apps/grant-admin-consent> (日本語)
 - <https://learn.microsoft.com/zh-cn/entra/identity/enterprise-apps/grant-admin-consent> (中文)

4. 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 の テナント管理者 が「[OAuth プロバイダを設定する \(システム間連携\)](#)」を行う際に利用します。

- アプリケーション (クライアント) ID
- ディレクトリ (テナント) ID
- 証明書の拇印
- 証明書に対応する秘密鍵

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。

ここでは追加が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/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)

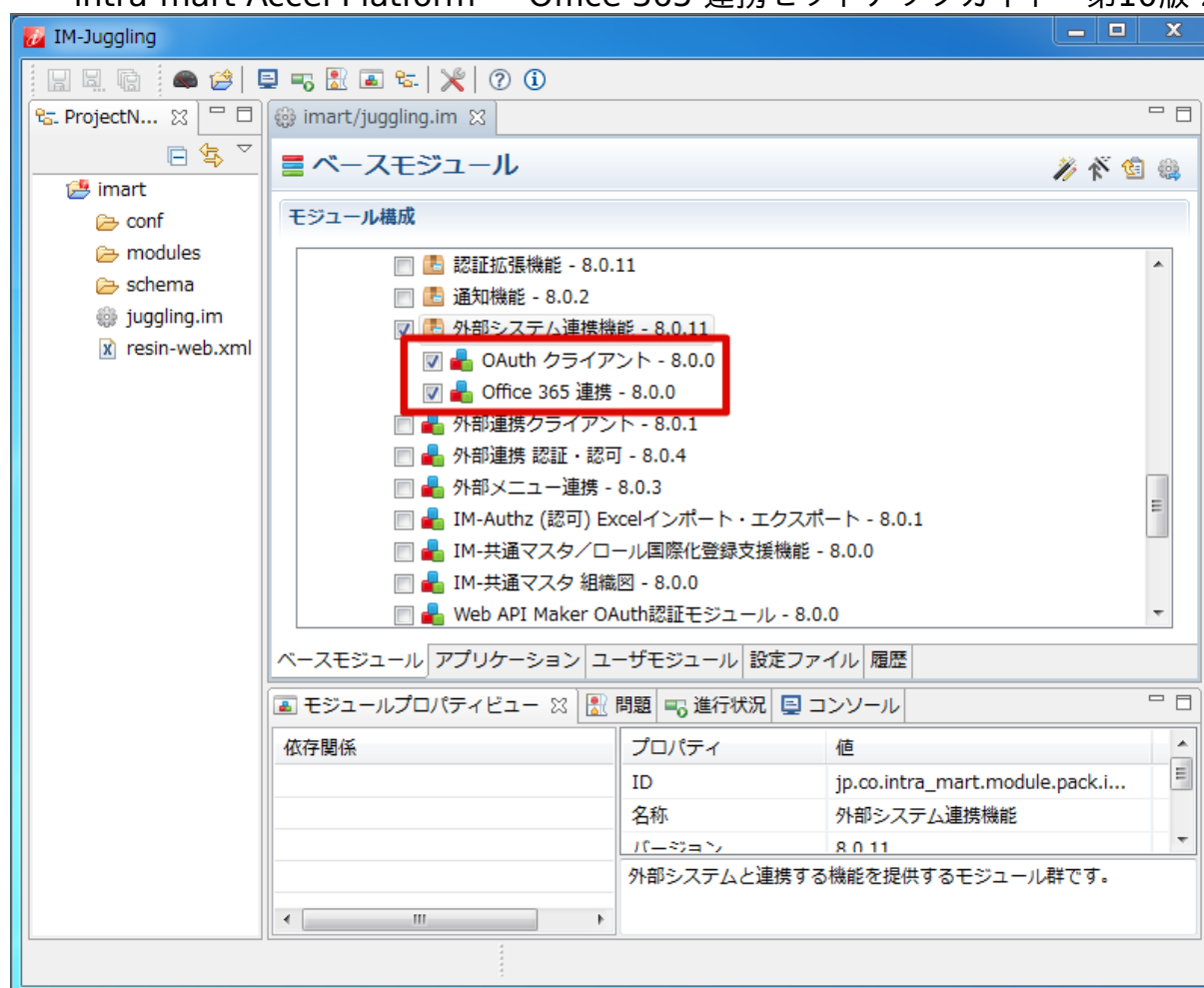
設定方法は「[WebSphere Application Server 利用時の追加設定](#)」を参照してください。

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。

システム間で連携する方式を利用する場合も、Office 365 連携 の選択が必要です。

Office 365 連携 を選択すると、「OAuthプロバイダ設定」画面でプロバイダ種別「office365」を選択できます。



設定ファイルの編集

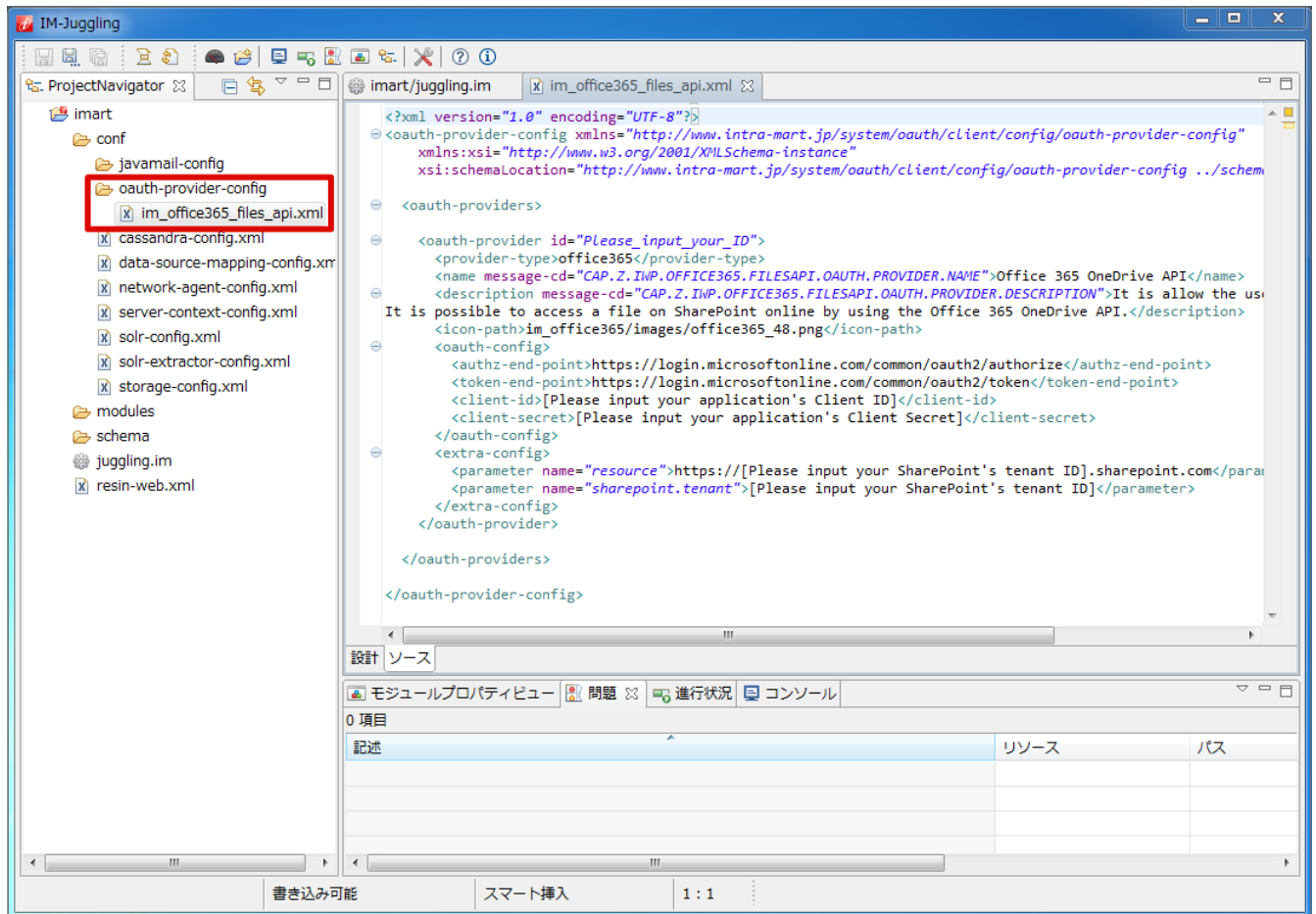
Office 365 連携 を利用するための設定ファイルを編集します。
この手順は、ユーザ単位で連携する方式の場合に行います。

コラム

システム間で連携する方式の場合、設定ファイルの編集は不要です。
セットアップの完了後に、テナント管理者が「[OAuth プロバイダを設定する（システム間連携）](#)」を行ってください。

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.DESRIPTION">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>00000000-0000-0000-0000-000000000000</client-id>
```

```
<client-secret>0000000~00000000000000000000000000000000</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。

intra-mart Accel Platform テナント管理者 向けの作業です。

システム間で連携する方式（クライアントクレデンシャルフロー）を利用する場合に、「OAuthプロバイダ設定」画面から Microsoft 365 と連携するためのプロバイダを登録します。

ユーザ単位で連携する方式の場合、この手順は不要です。

項目

- [プロバイダを登録する](#)



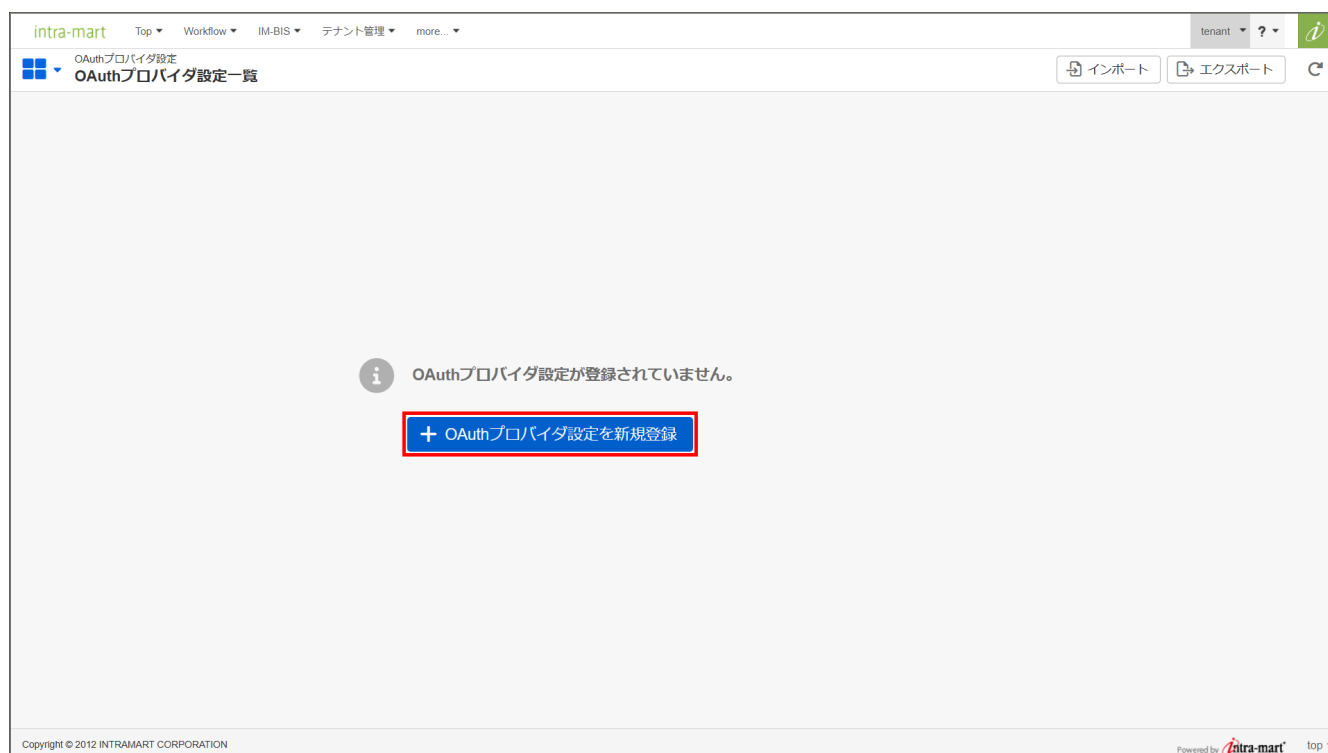
コラム

この作業は、「[intra-mart Accel Platform をセットアップする](#)」でテナント環境セットアップが完了した後に行います。事前に Microsoft Azure 管理者 から、「[システム間で連携する方式（クライアントクレデンシャルフロー）のアプリケーションを設定する](#)」で控えた以下の情報を受け取ってください。

- アプリケーション（クライアント）ID
- ディレクトリ（テナント）ID
- 証明書の拇印
- 証明書に対応する秘密鍵

プロバイダを登録する

1. テナント管理者 で intra-mart Accel Platform にログインします。
2. 「サイトマップ」→「OAuthクライアント」→「OAuthプロバイダ設定」→「OAuthプロバイダー一覧」をクリックします。
3. 「新規登録」をクリックします。



コラム

OAuthプロバイダ設定が1件も登録されていない場合は、「OAuthプロバイダ設定を新規登録」をクリックします。

4. 「プロバイダ設定」に以下を入力します。
 - プロバイダIDに任意のIDを入力
 - 名前に任意の名称を入力

- 説明、アイコンは必要に応じて設定

intra-mart Top Workflow IM-BIS テナント管理 more...

tenant ? i

← OAuthプロバイダ設定 OAuthプロバイダ - 新規登録

プロバイダ設定

このプロバイダを識別する情報を設定します。

プロバイダID* office365-provider
プロバイダIDは登録後に変更できません。

名前* Office365連携プロバイダ

説明

アイコン  ファイルを選択 クリア

接続先の設定

接続する認可サーバと、そこで認証されるための情報を設定します。認証方式によって入力する項目が変わります。

接続方式

認証方式*

☐ 認可コード
ユーザの認可を得てアクセストークンを取得します。

☒ クライアントクレデンシャル
JWTアサーション (RFC 7523) でアクセストークンを取得します。ユーザ操作は不要です。

 認証方式を選択すると、必要な設定項目が表示されます。

登録

Copyright © 2012 INTRAMART CORPORATION

Powered by intra-mart top ↑

5. 「接続先の設定」の「接続方式」で以下を選択します。

- 認証方式に「クライアントクレデンシャル」を選択
- プロバイダ種別に「office365」を選択

intra-mart Top Workflow IM-BIS テナント管理 more...

tenant ? i

← OAuthプロバイダ設定 OAuthプロバイダ - 新規登録

接続先の設定

接続する認可サーバと、そこで認証されるための情報を設定します。認証方式によって入力する項目が変わります。

接続方式

認証方式*

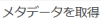
☐ 認可コード
ユーザの認可を得てアクセストークンを取得します。

☒ クライアントクレデンシャル
JWTアサーション (RFC 7523) でアクセストークンを取得します。ユーザ操作は不要です。

プロバイダ種別* office365

認可サーバの情報

認可サーバURL

認可サーバのURL (発行者識別子 / issuer) またはメタデータURL (i.e. well-known/...) を入力してください。入力値は保存されません。 

発行者識別子 (issuer)

トークンエンドポイント*

クライアント情報

クライアントID*

鍵形式*

登録

Copyright © 2012 INTRAMART CORPORATION

Powered by intra-mart top ↑



コラム

プロバイダ種別「office365」は、「intra-mart Accel Platform をセットアップする」のモジュールの選択で Office 365 連携を選択している場合に選択できます。

6. 「接続先の設定」の「認可サーバの情報」に以下を入力します。

- トークンエンドポイントに「https://login.microsoftonline.com/<ディレクトリ (テナント) ID>/oauth2/v2.0/token」を入力

intra-mart Top Workflow IM-BIS テナント管理 more...

tenant ?

OAuthプロバイダ設定
OAuthプロバイダ - 新規登録

接続先の設定

接続する認可サーバと、そこで認証されるための情報を設定します。認証方式によって入力する項目が変わります。

接続方式

認証方式 *

☐ 認可コード
ユーザの認可を得てアクセストークンを取得します。

☒ クライアントクレデンシャル
JWTアサーション (RFC 7523) でアクセストークンを取得します。ユーザ操作は不要です。

プロバイダ種別 *

office365

認可サーバの情報

認可サーバURL

メタデータを取得

認可サーバのURL (発行者識別子 / issuer) またはメタデータURL (/ well-known/...) を入力してください。入力値は保存されません。

先行者識別子 (issuer)

認可サーバが自身を識別するURLです。認可サーバURLから自動取得できます。

トークンエンドポイント *

https://login.microsoftonline.com/00000000-0000-0000-000000000000/oauth2/v2.0/token

認可サーバURLから自動取得できます。

クライアント情報

クライアントID *

鍵形式 *

登録

Copyright © 2012 INTRAMART CORPORATION

Powered by intra-mart top

7. 「接続先の設定」の「クライアント情報」に以下を入力または選択します。

- クライアントIDにアプリケーション (クライアント) ID を入力
- 鍵形式に秘密鍵の形式 (「PEM」または「PKCS12」) を選択
- 秘密鍵に証明書に対応する秘密鍵を設定 (ファイルから読み込む、または テキストを貼り付ける)
- キーストアパスワード、秘密鍵パスワード、鍵エイリアスは、秘密鍵に合わせて必要に応じて入力
- 署名アルゴリズムを選択 (例: RS256)

intra-mart Top Workflow IM-BIS テナント管理 more...

tenant ?

OAuthプロバイダ設定
OAuthプロバイダ - 新規登録

トークンエンドポイント *

https://login.microsoftonline.com/00000000-0000-0000-000000000000/oauth2/v2.0/token

認可サーバURLから自動取得できます。

クライアント情報

クライアントID *

00000000-0000-0000-000000000000

鍵形式 *

PEM

秘密鍵 *

☒ ファイルから読み込む ☐ テキストを貼り付ける

ここにファイルをドラッグ&ドロップ または [ファイルを選択](#)

private.key 2026/07/23 18:18:11 1.7 KB

秘密鍵パスワード

署名アルゴリズム *

RS256

その他の設定

認可サーバに要求する権限と、認可リクエストに付与する内容を設定します。

アクセス範囲

アクセス範囲 (スコープ)

登録

Copyright © 2012 INTRAMART CORPORATION

Powered by intra-mart top



コラム

秘密鍵は、「[証明書をアップロードする](#)」でアップロードした証明書と対になるものを設定してください。
RSA 鍵の場合、鍵長が 2048 ビット未満のものは設定できません。

8. 「その他の設定」に以下を入力します。

- アクセス範囲 (スコープ) に「https://< Microsoft 365 のテナント>.sharepoint.com/default」を入力

 コラム

 コラム

 コラム

33

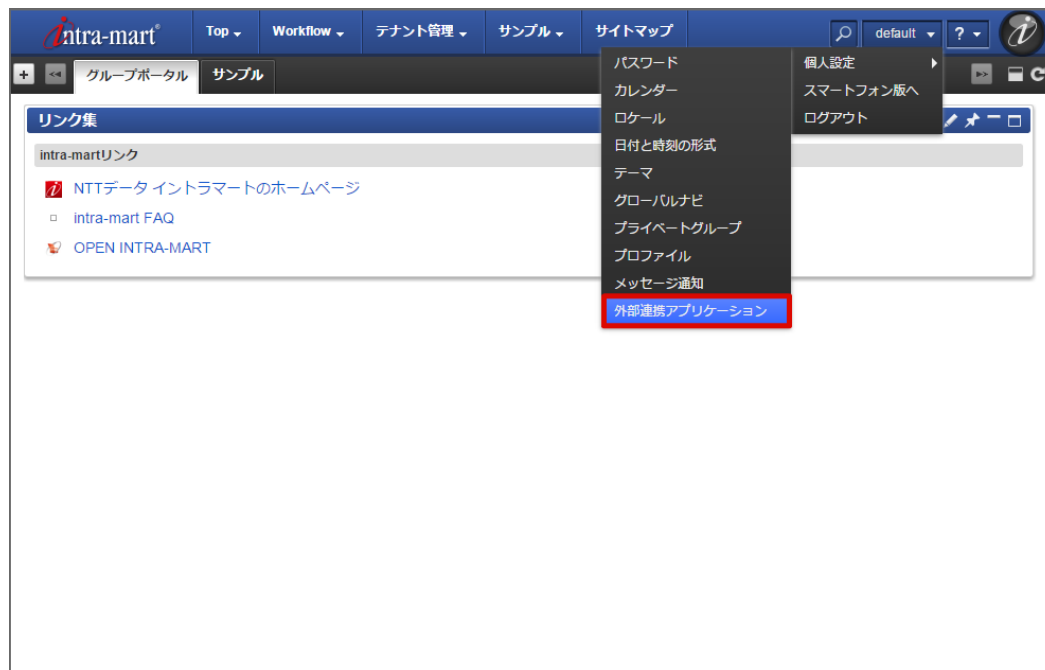
intra-mart Accel Platform システム管理者 向けの作業です。

intra-mart Accel Platform のユーザで Microsoft 365 のユーザ と連携をします。

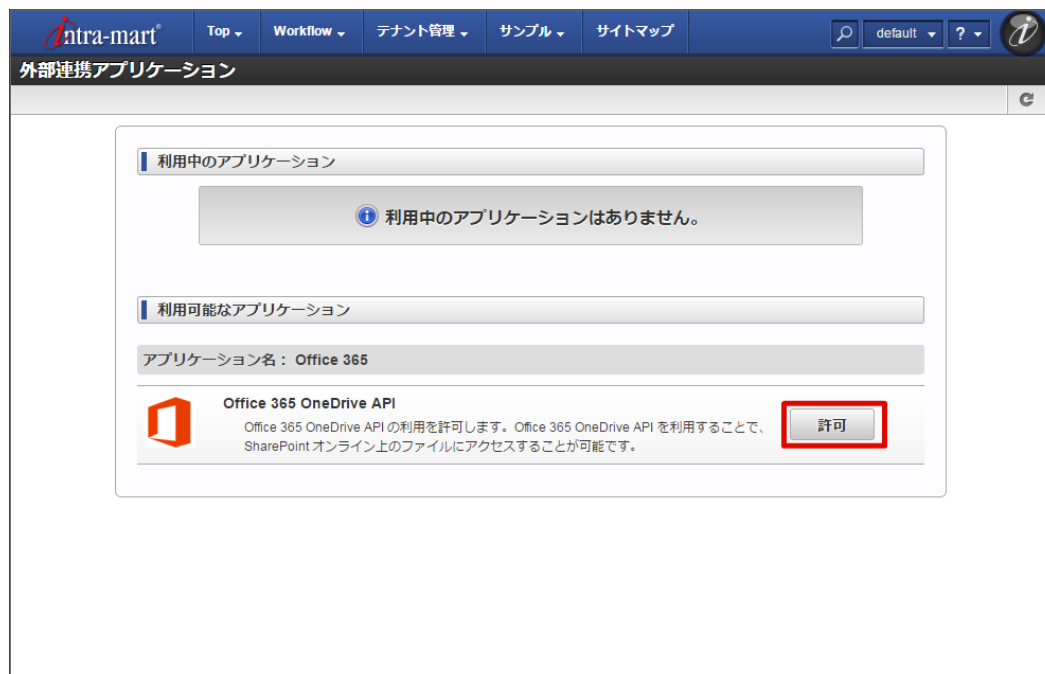
この手順は、ユーザ単位で連携する方式の場合に行います。

システム間で連携する方式の場合、ユーザによる連携の操作は不要です。

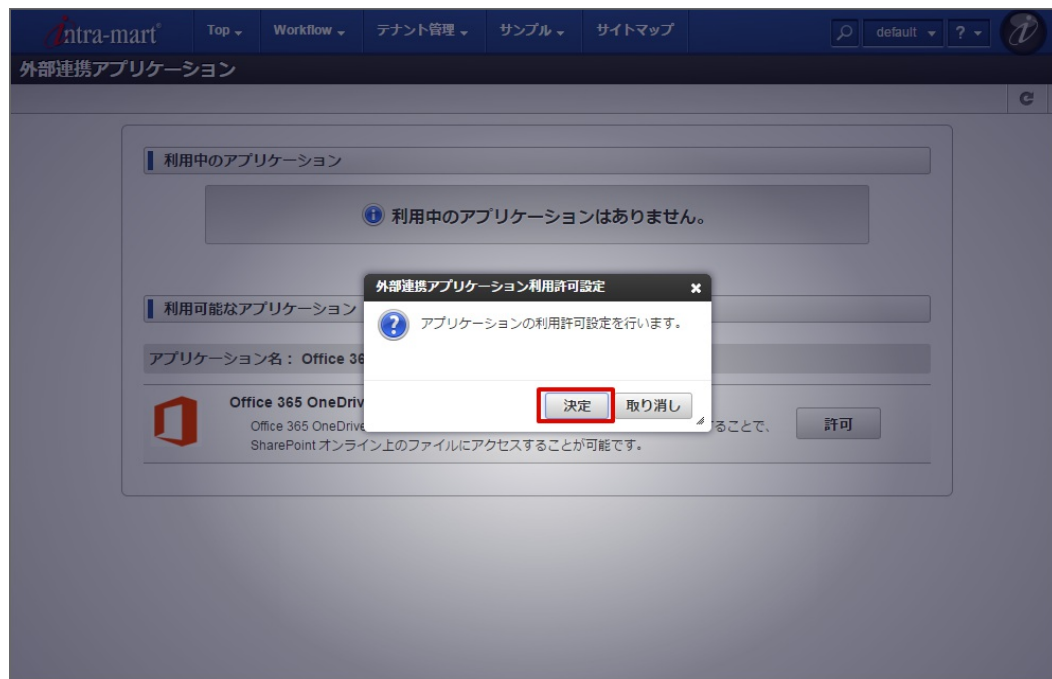
1. 任意のユーザで intra-mart Accel Platform にログインしてください。
2. ユーティリティメニューより、「個人設定」-「外部連携アプリケーション」を選択します。



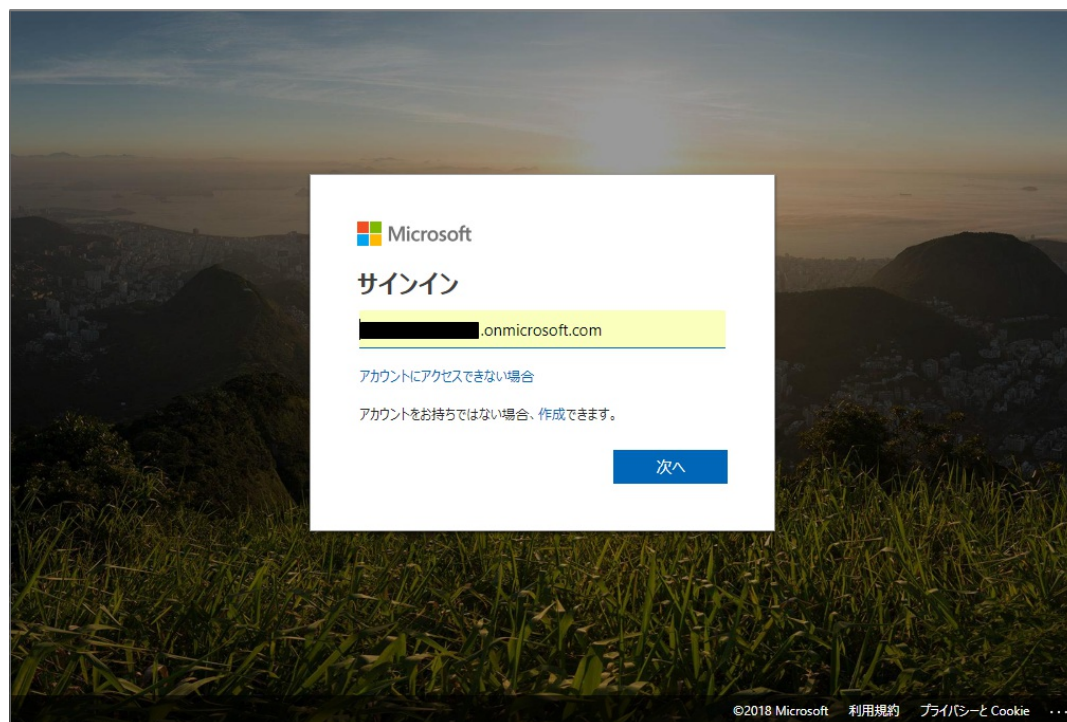
3. 「Office 365 OneDrive API」 の「許可」をクリックします。



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。



Office 365 連携 の解除は以下の手順で行います。

項目

- ユーザ単位で連携する方式の場合
- システム間で連携する方式の場合

ユーザ単位で連携する方式の場合

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

設定ファイルを編集します。

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.DESCRPTION">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。

システム間で連携する方式の場合

intra-mart Accel Platform テナント管理者 向けの作業です。

「OAuthプロバイダ設定」画面から、登録したプロバイダを削除します。

1. テナント管理者 で intra-mart Accel Platform にログインします。
2. 「サイトマップ」→「OAuthクライアント」→「OAuthプロバイダ設定」→「OAuthプロバイダー一覧」をクリックします。
3. 連携を解除したいプロバイダをクリックします。

4. 「削除」をクリックします。



コラム

Microsoft Azure の管理ポータルで、「[システム間で連携する方式（クライアントクレデンシャルフロー）のアプリケーションを設定する](#)」で登録したアプリケーションも不要な場合は削除してください。

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

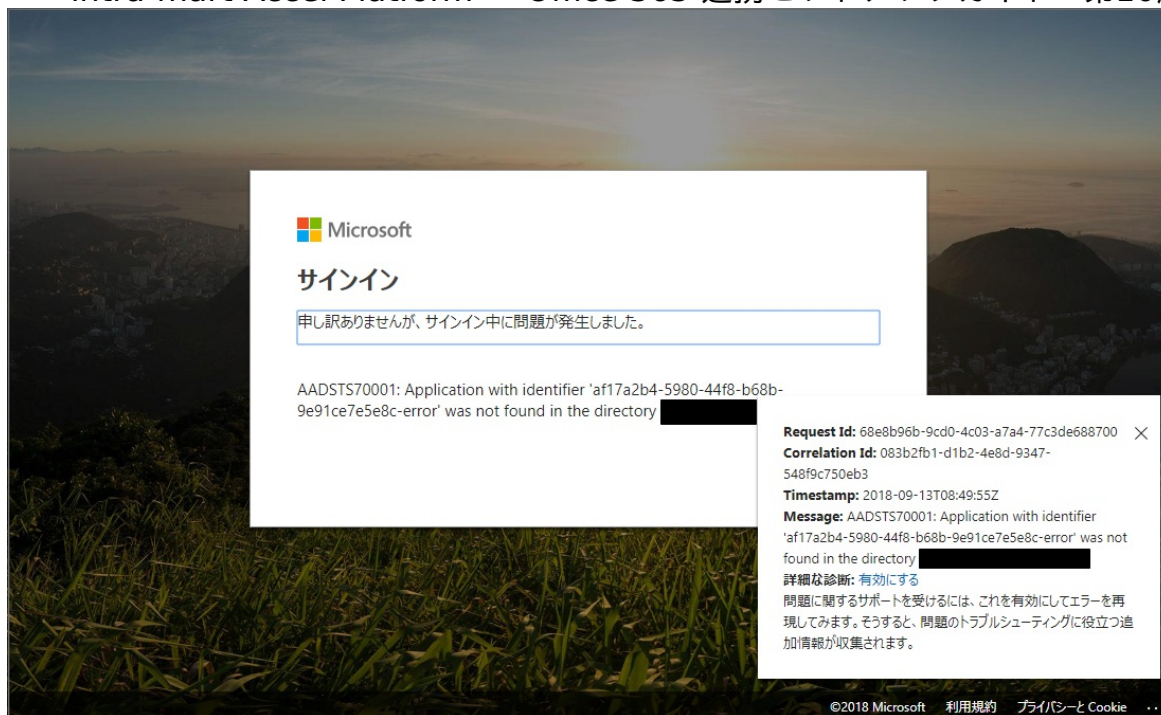
- 「AADSTS70001: Application with identifier <クライアントID> was not found in the directory <Microsoft 365のテナントID >.onmicrosoft.com」が発生します
 - 現象
 - 原因
 - 対応方法
- 「不正なレスポンスを受け取りました。」が発生します
 - 現象
 - 原因
 - 対応方法
- 「外部連携アプリケーションの利用許可設定時に、予期せぬエラーが発生しました。」が発生します
 - 現象
 - 原因
 - 対応方法
- 「AADSTS50011: The reply url specified 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
 - 原因
 - 対応方法
- 「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
 - 原因
 - 対応方法

「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「サポートされているアカウントの種類」に「複数の Entra ID テナント」以外が選択され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。

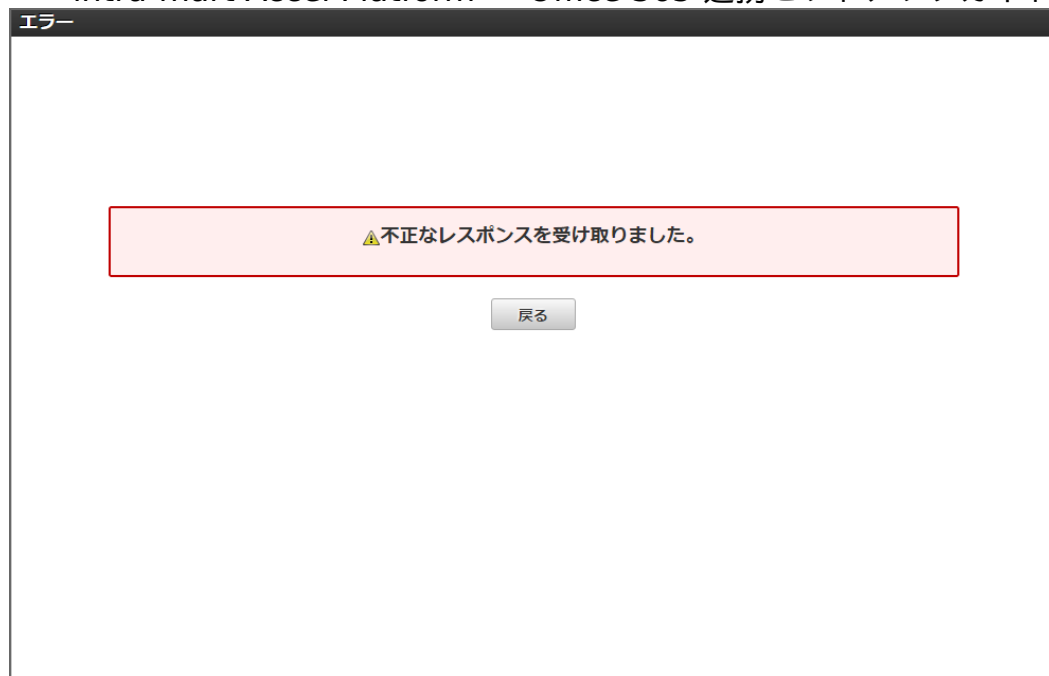
または「サポートされているアカウントの種類」を「複数の Entra ID テナント」（「すべてのテナントを許可する」）に変更してください。変更は、アプリケーションの「管理」の「Authentication (Preview)」の「Supported accounts」タブから行います。

設定値については「[アプリケーションを登録する](#)」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。

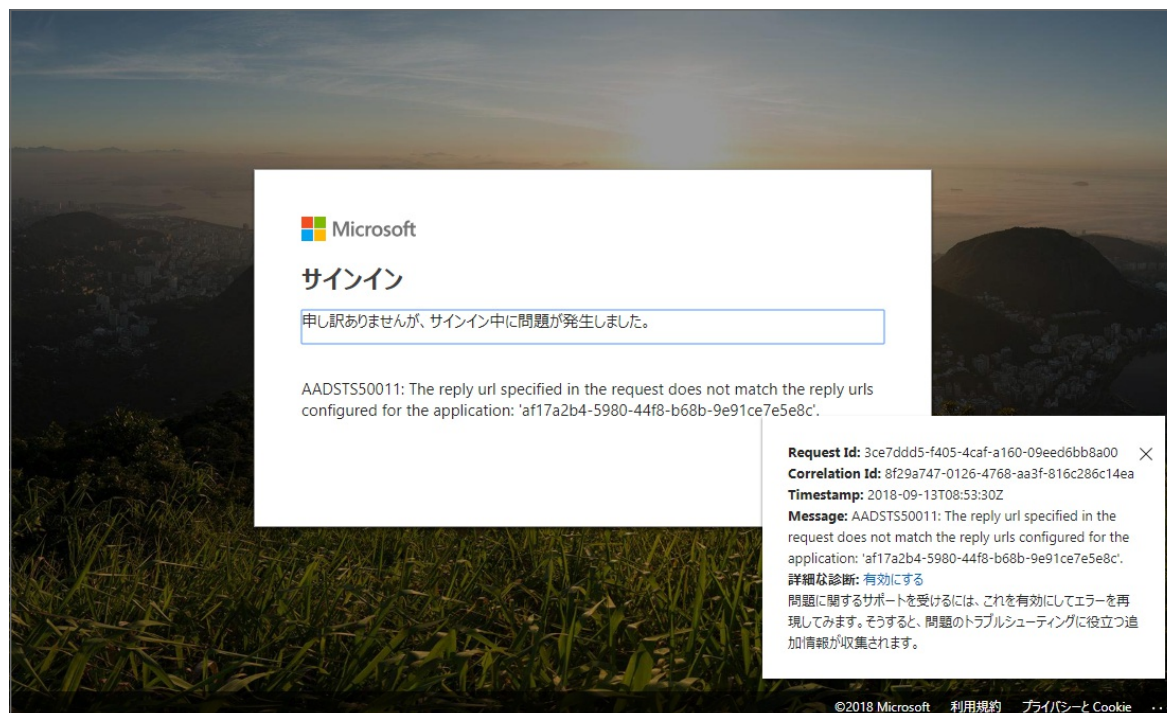
Web Application Server に WebSphere Application Server を利用している場合は[WebSphere Application Server 利用時の追加設定](#)を確認してください。

「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「リダイレクト URI」が不正である可能性があります。

対応方法

「リダイレクト URI」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。

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「APIのアクセス許可」で設定した「委任されたアクセス許可」に、一般ユーザでは同意できないアクセス許可が含まれ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。

- Microsoft Graph permissions reference :
 - <https://learn.microsoft.com/en-us/graph/permissions-reference> (English)
 - <https://learn.microsoft.com/ja-jp/graph/permissions-reference> (日本語)
 - <https://learn.microsoft.com/zh-cn/graph/permissions-reference> (中文)

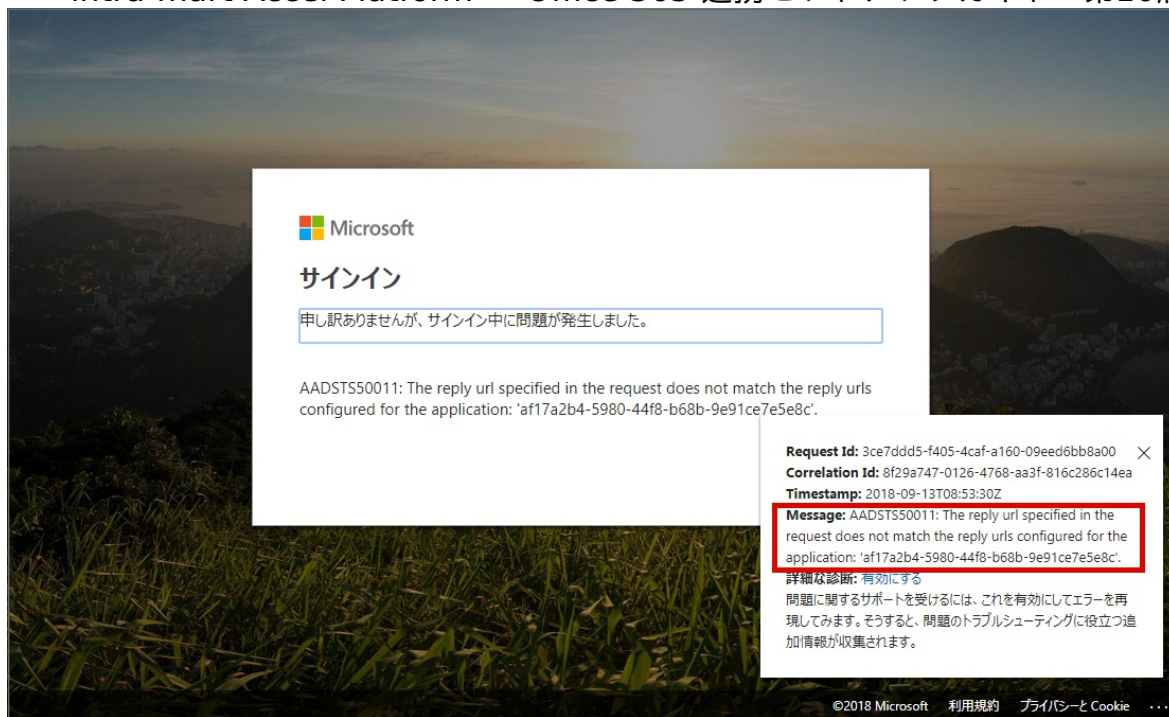
エラーメッセージが出力される

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。



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。

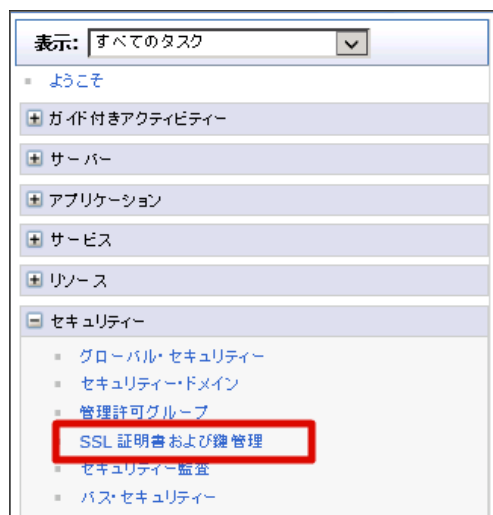
本追加設定を行っても SSL 通信のエラーが発生する場合は、エラー内容に従い、適切な SSL 証明書を追加してください。

項目

- [Microsoft 365 ルート証明書バンドル を追加する](#)

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]-[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。

SSL 証明書および鍵管理

SSL 証明書および鍵管理

SSL 構成

Secure Sockets Layer (SSL) プロトコルは、リモート・サーバー・プロセスまたはエンドポイント間のセキュア通信を提供します。SSL セキュリティーは、エンドポイントへのインバウンド通信およびエンドポイントからのアウトバウンド通信の確立に使用できます。セキュア通信を確立するには、エンドポイントに対して指定された証明書および SSL 構成がなければなりません。

旧バージョンのこの製品では、Secure Sockets Layer (SSL) 用に各エンドポイントを手動で構成する必要がありました。このバージョンでは、アプリケーションのサービス環境全体について 1 つの構成を定義することができます。これにより、セキュア通信の一元管理が可能になりました。さらに、デフォルトのセルレベルの SSL 構成をオーバーライドすることで、複数ノード環境でトラスト・ゾーンを確立できます。

マイグレーション・ユーティリティを使用してセキュア環境をこのバージョンにマイグレーション済みの場合、さまざまなエンドポイントのために古い Secure Sockets Layer (SSL) 構成がリストアされます。ただし、一元管理機能の利点を得るためには、SSL を再構成することが必要です。

構成設定

[エンドポイント・セキュリティ構成の管理](#)
[証明書有効期限の管理](#)
[FIPS の管理](#)

☒ SSL 構成の変更が発生したときに、動的にランタイムを更新する

適用

リセット

関連項目

- SSL 構成
- 動的アウトバウンド・エンドポイント SSL 構成
- 鍵ストアおよび証明書**
- 鍵セット
- 鍵セット・グループ
- 鍵マネージャー
- トラスト・マネージャー
- 認証局 (CA) クライアント構成

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

SSL 証明書および鍵管理

SSL 証明書および鍵管理 > 鍵ストアおよび証明書

暗号方式、RACF(R)、CMS、Java(TM)、およびすべてのトラストストア・タイプを含む、鍵ストア・タイプを定義します。

鍵ストア使用

SSL 鍵ストア

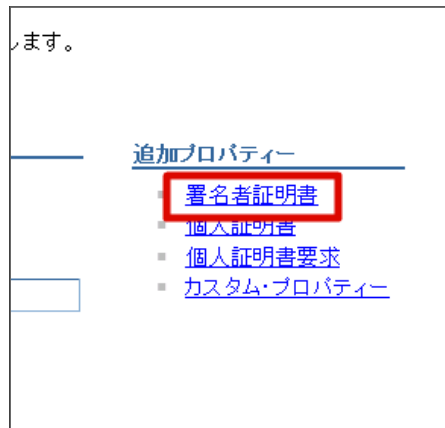
設定

新規作成... 削除 パスワード変更... 署名者の交換...

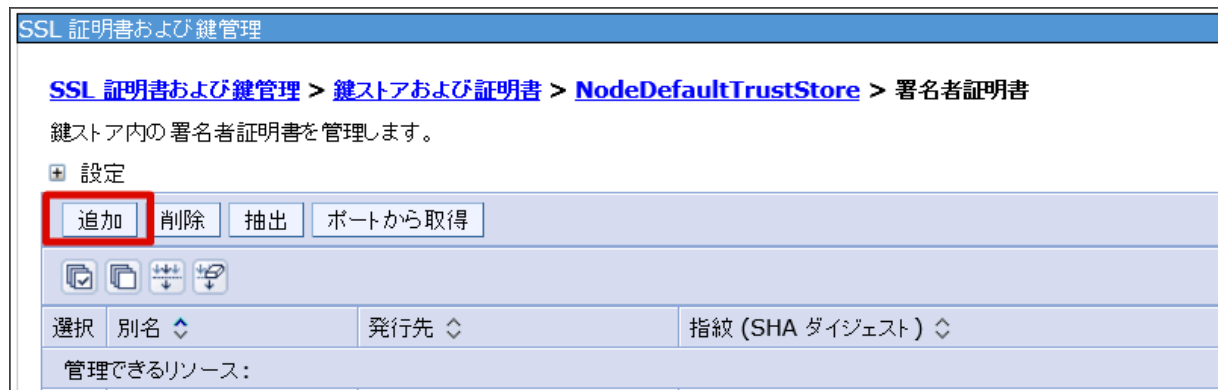
選択	名前	説明	管理の有効範囲	パス
☐	NodeDefaultKeyStore	WIN-KP0NK40MQDRNode01 のデフォルト 鍵ストア	(cell):WIN-KP0NK40MQDRNode01Cell:(node):WIN-KP0NK40MQDRNode01	\${CONFIG_ROOT}/cells/WIN-KP0NK40MQDRNode01Cell/nodes/WIN-KP0NK40MQDRNode01/key.p12
☐	NodeDefaultTrustStore	WIN-KP0NK40MQDRNode01 のデフォルト・トラストストア	(cell):WIN-KP0NK40MQDRNode01Cell:(node):WIN-KP0NK40MQDRNode01	\${CONFIG_ROOT}/cells/WIN-KP0NK40MQDRNode01Cell/nodes/WIN-KP0NK40MQDRNode01/trust.p12

合計 2

5. [署名者証明書]リンクをクリックします。



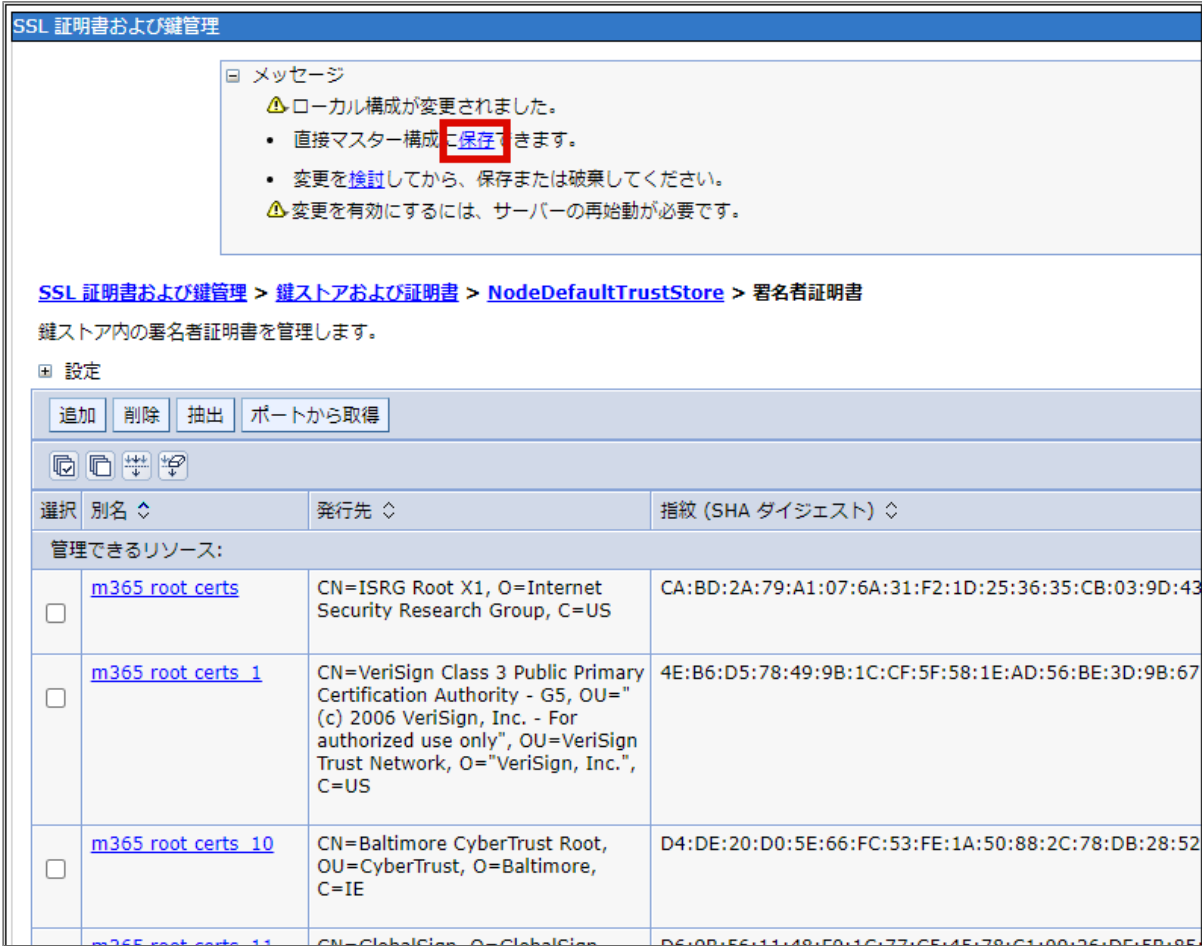
6. [追加]ボタンをクリックします。



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>

```

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\(v=azure.100\)](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」

