

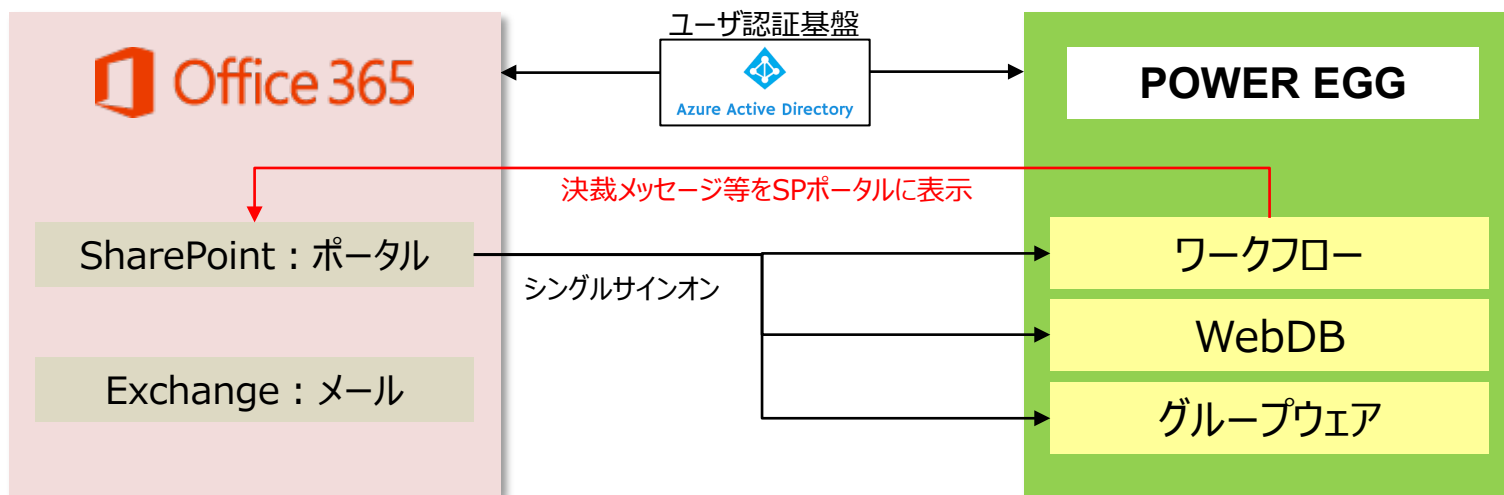
# POWER EGG 3.0 Office 365連携

2022年2月

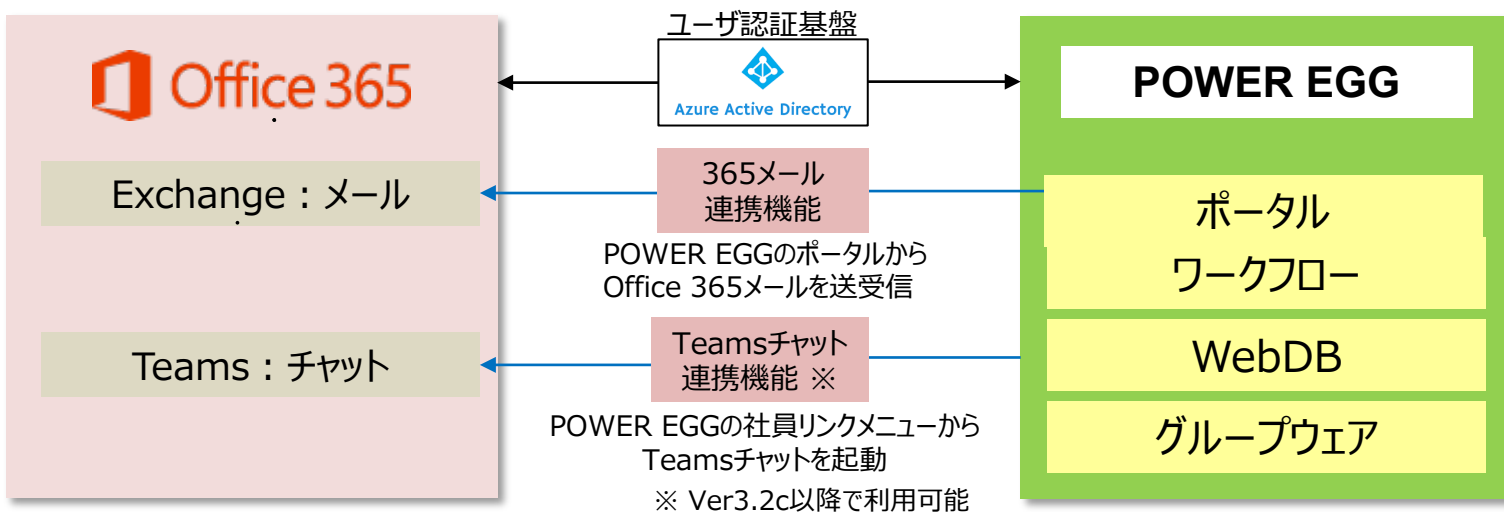
ディサークル株式会社

修正日・版	修正箇所・内容
2018/09/14 1.0版	初版 発行
2019/08/30 2.0版	Azure Active Directory管理センターのUI変更に対応
2020/06/17 3.0版	留意事項を追記
2020/11/12 4.0版	Teams連携機能に関する記述を追記、留意事項を追記
2020/11/26 5.0版	Teams連携機能はVer3.2c以降で利用できる旨を追記
2022/02/07 6.0版	Azure Active Directory管理センターのUI変更に対応 留意事項を追記

## ■ Office 365利用ユーザ向け連携モデル：パターン①



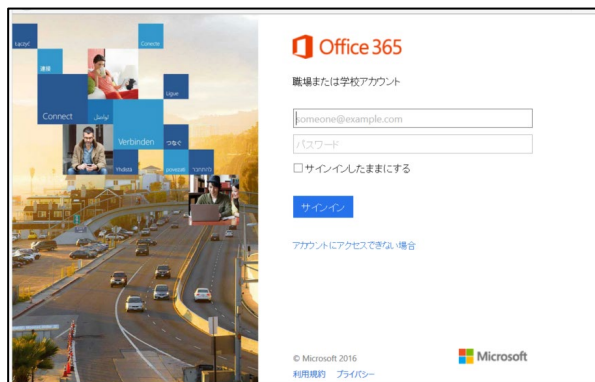
## ■ POWER EGG利用ユーザ向け連携モデル：パターン②



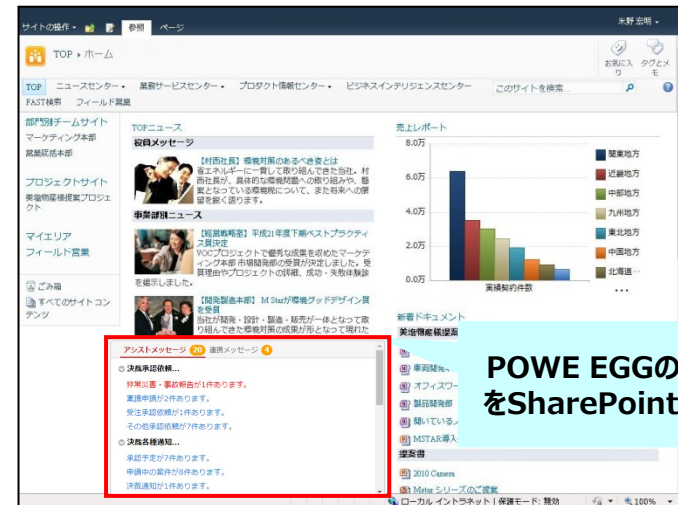
# 連携イメージ図①

## パターン1 : Office 365からPOWER EGGにシングルサインオン

### ①Office 365にログイン



### ②. SharePointにログインし、POWER EGGアシストメッセージを表示



POWER EGGの決裁メッセージをSharePointポータルに表示

### ②Office 365メニューからPOWER EGGを起動



POWER EGGを  
Office 365メニューに登録

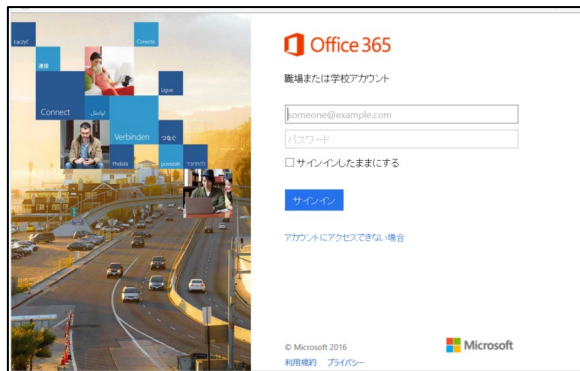
### ③POWER EGGにシングルサインオンし、ナビビューを表示



# 連携イメージ図②

## パターン2：POWER EGGからOffice 365にシングルサインオン

①POWER EGGのログイン時、Office 365(Azure AD)のログイン画面を表示



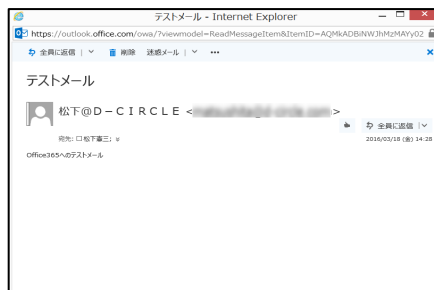
②ログイン後、ナビビューを表示



③ダイレクトボタンから  
Office 365にシングルサインオン

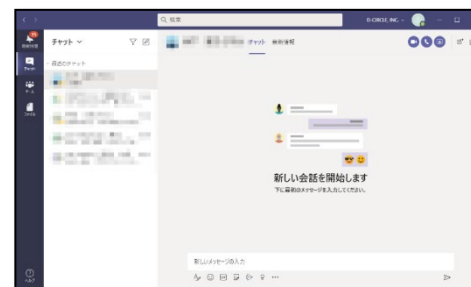


④ナビビューから  
Office 365のメールを表示



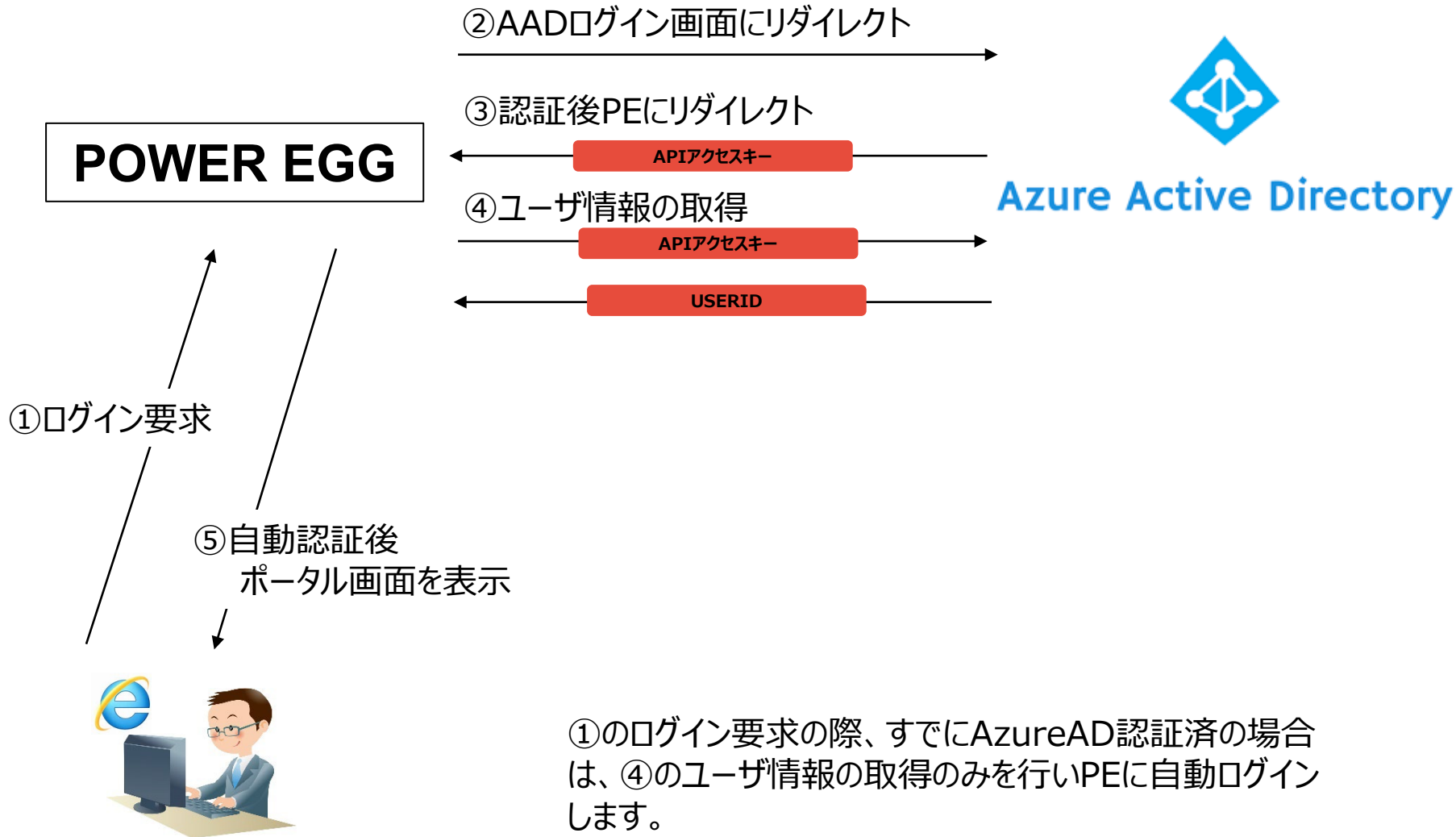
365メール  
連携機能

⑤社員リンクメニューから  
Teamsアプリを起動



Teamsチャット  
連携機能 ※

※Ver3.2c以降で  
利用可能



①のログイン要求の際、すでにAzureAD認証済の場合は、④のユーザ情報の取得のみを行いPEに自動ログインします。

認証プロトコルには、OpenIDを利用しています。

Office 365のログインIDをPOWER EGGの社員情報の「メモ 1」にセットします。

例： Office 365ログインID： imaoka@o.d-circle.com

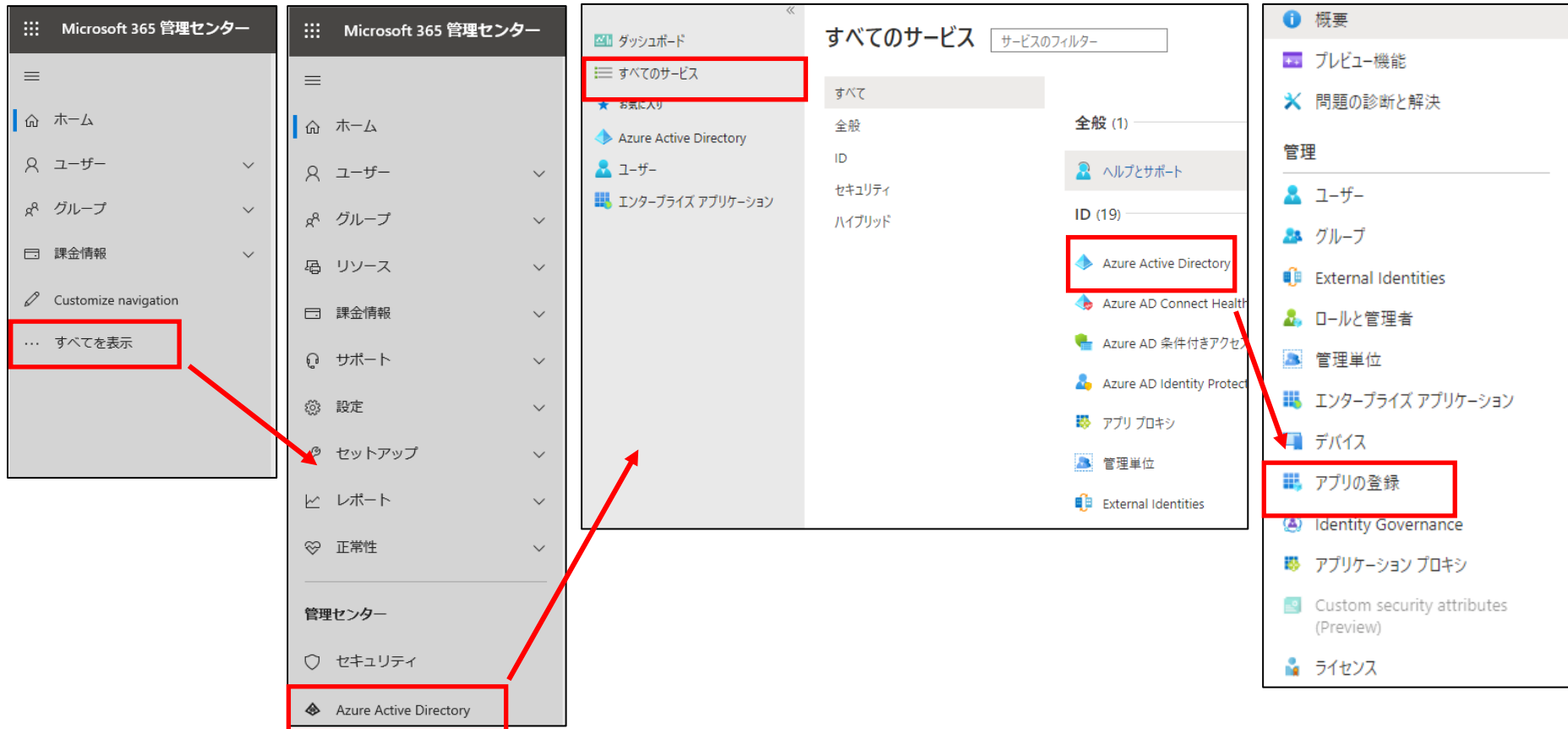


POWER EGG社員情報のメモ 1： imaoka@o.d-circle.com

ユーザー、グループ等のAzure ADとの連携機能はありませんので、POWER EGGの組織情報（社員、部門等）はPOWER EGG側にあらかじめ登録しておく必要があります。

# Azure ADへのPOWER EGGの登録

Office 365にログインし、管理画面から「Azure Active Directory 管理センター」を開き、「アプリの登録」を開きます。



The screenshot illustrates the steps to access the 'App Registrations' page in the Azure Active Directory Management Center. It is divided into three panels:

- Left Panel (Microsoft 365 管理センター):** Shows the main navigation menu. The option '... すべてを表示' (Show all) is highlighted with a red box. A red arrow points from this box to the 'Azure Active Directory' link in the bottom right corner of the panel.
- Middle Panel (ダッシュボード):** Shows the 'すべてのサービス' (All services) list. The 'すべてのサービス' link is highlighted with a red box. A red arrow points from this box to the 'Azure Active Directory' link in the right panel.
- Right Panel (Azure Active Directory 管理センター):** Shows the 'すべてのサービス' (All services) list. The 'Azure Active Directory' link is highlighted with a red box. A red arrow points from this box to the 'アプリの登録' (App Registrations) link in the rightmost panel.

The rightmost panel shows the 'Azure Active Directory 管理センター' (Azure Active Directory Management Center) navigation menu. The 'アプリの登録' (App Registrations) link is highlighted with a red box.



# Azure ADへのPOWER EGGの登録

「アプリの登録」で「新規登録」を押し、アプリケーションの登録を行います。

The screenshot shows the Azure Active Directory portal for D-CIRCLE, INC. The left sidebar contains navigation links: 概要 (Overview), プレビュー機能 (Preview features), 問題の診断と解決 (Troubleshooting), and 管理 (Management). Under Management, there are links for ユーザー (Users) and グループ (Groups). The main content area is titled 「アプリケーションの登録」 (Register an application). A red box highlights the 「+ 新規登録」 (New registration) button. A red arrow points from this button to the 「名前」 (Name) field, which contains the text 「POWEREGG」. A text box explains that the name is for identification and will appear in the Office 365 menu. Below the name field, there is a section for 「サポートされているアカウントの種類」 (Supported account types), with a radio button selected for 「この組織ディレクトリのみに含まれるアカウント (D-CIRCLE, INC. のみ - シングル テナント)」 (Accounts only in this organization's directory (D-CIRCLE, INC. only - Single tenant)). Another text box explains that the supported account type should be chosen based on the environment. Below this, the 「リダイレクト URI」 (Redirect URI) section is shown. A text box explains that the URI should be specified as follows: select 「Web」 on the left and enter 「https://[server name]/pe4j/aadlogin」 on the right. The text box also notes that the server name is the client's server name or IP address, and that the example uses o365.poweregg.net. The screenshot shows the 「Web」 option selected in a dropdown and the URI entered in the adjacent field. At the bottom, a red box highlights the 「登録」 (Register) button. A final text box instructs the user to click the register button after input.

「名前」は識別できる任意の名前（例：POWEREGG）  
※ ここで入力した名前がOffice 365のメニューに表示されます。

「サポートされているアカウントの種類」は、ご利用の環境に応じて選択してください。

「リダイレクトURI」は下記のように指定してください。

- ・左側（プラットフォームの選択）で「Web」を選択。
- ・右側（URI）で「https://[サーバ名]/pe4j/aadlogin」を入力。  
※ [サーバ名]：クライアントからアクセスするサーバ名 or IPアドレス  
本資料では例として o365.poweregg.net というサーバ名を使用します。

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

Web https://o365.poweregg.net/pe4j/aadlogin

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

入力後、登録をクリックしてください。

登録したアプリケーションの「認証」の設定を行います。



検索 (Ctrl+/) << 保存 破棄 フィードバックがある場合

プラットフォーム構成 下記項目の設定後、「保存」を押してください。

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

+ プラットフォームを追加

Web クイックスタート ドキュメント

最初に「認証」を選択してください。

「リダイレクトURI」に “https://[サーバ名]/pe4j/aadlogin4sharepoint” を追加

https://o365.poweregg.net/pe4j/aadlogin4sharepoint

URI の追加

暗黙的な許可およびハイブリッドフロー

承認エンドポイントから直接トークンを要求します。アプリケーションにシングルページアーキテクチャ (SPA) があり、承認コードフローを使用していない場合、または JavaScript で Web API を起動する場合は、アクセス トークンと ID トークンの両方を選択します。ハイブリッド認証を使用する ASP.NET Core Web アプリや他の Web アプリでは、ID トークンのみを選択します。トークンの詳細情報。

承認エンドポイントによって発行してほしいトークンを選択してください。

☐ アクセス トークン (暗黙的なフローに使用)

☒ ID トークン (暗黙的およびハイブリッドフローに使用)

サポートされているアカウントの種類

このアプリケーションを使用したりこの API にアクセスしたりできるのは

☒ この組織ディレクトリのみに含まれるアカウント (D-CIRCLE, INC. のユーザー)

☐ 任意の組織ディレクトリ内のアカウント (任意の Azure AD ディレクトリ)

https://o365.poweregg.net/pe4j/aadlogin4sharepoint

URI の追加

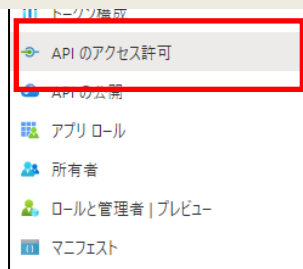
リダイレクトURIの入力欄が表示されていない場合は、「URIの追加」リンクを押してください。

「暗黙的な許可およびハイブリッドフロー」で「IDトークン」にチェックを入れてください。

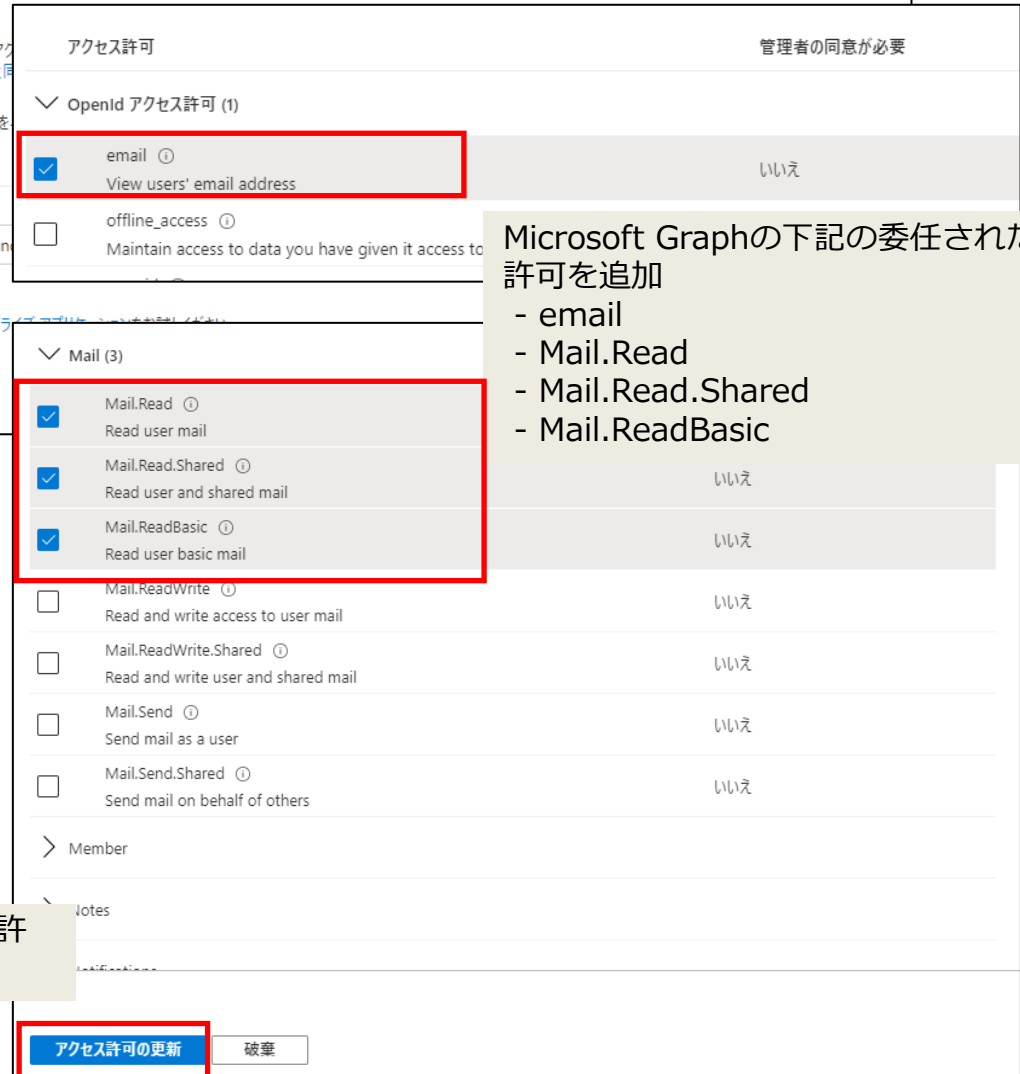
# Azure ADへのPOWER EGGの登録

アプリケーションの「APIのアクセス許可」の設定を行います。

最初に「APIのアクセス許可」を選択してください。



「Microsoft Graph」をクリック



Microsoft Graphの下記の委任されたアクセス許可を追加

- email
- Mail.Read
- Mail.Read.Shared
- Mail.ReadBasic

アクセス許可を追加後、「アクセス許可の更新」を押してください。

アプリケーションの「APIのアクセス許可」の設定を行います。

「Azure Active Directoryの名前(下記画像はD-CIRCLE, INC)に管理者の同意を与えます」をクリック



管理  
ブランド化とプロパティ  
認証  
証明書とシークレット  
トークン構成  
APIのアクセス許可  
APIの公開  
アプリロール  
所有者  
ロールと管理者  
プレビュー  
マニフェスト

構成された API / アクセス許可の名前

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 (5)

email	委任済み	View users' email address	いいえ	...
Mail.Read	委任済み	Read user mail	いいえ	...
Mail.Read.Shared	委任済み	Read user and shared mail	いいえ	...
Mail.ReadBasic	委任済み	Read user basic mail	いいえ	...

管理者の同意の確認を与えます。

D-CIRCLE, INC. のすべてのアカウントについて、要求されたアクセス許可に対する同意を付与しますか? この操作により、このアプリケーションが既に持っている既存の管理者の同意レコードが、以下の一覧の内容に一致するよう更新されます。

はい いいえ

「はい」をクリック



+ アクセス許可の追加 D-CIRCLE, INC. 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 (5)

email	委任済み	View users' email address	いいえ	...
Mail.Read	委任済み	Read user mail	いいえ	...
Mail.Read.Shared	委任済み	Read user and shared mail	いいえ	...
Mail.ReadBasic	委任済み	Read user basic mail	いいえ	...
User.Read	委任済み	Sign in and read user profile	いいえ	...

状態にチェックが付いていることを確認

同意 D-CIRCLE, INC. に付与さ... 同意 D-CIRCLE, INC. に付与さ... 同意 D-CIRCLE, INC. に付与さ... 同意 D-CIRCLE, INC. に付与さ... 同意 D-CIRCLE, INC. に付与さ...

アプリケーションの「クライアントシークレット」の設定を行います。



POWEREGG | 証明書とシークレット

検索 (Ctrl+/) < フィードバックがある場合

概要

資格情報は、Web アドレスの指定が可能な場所 (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。

最初に「証明書とシークレット」を選択してください。

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 (0) 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)

トークンの要求時にアプリケーションが自身の ID を証明するために使用する秘密の文字列です。アプリケーション パスワードと呼ばれる。

+ 新しいクライアント シークレット

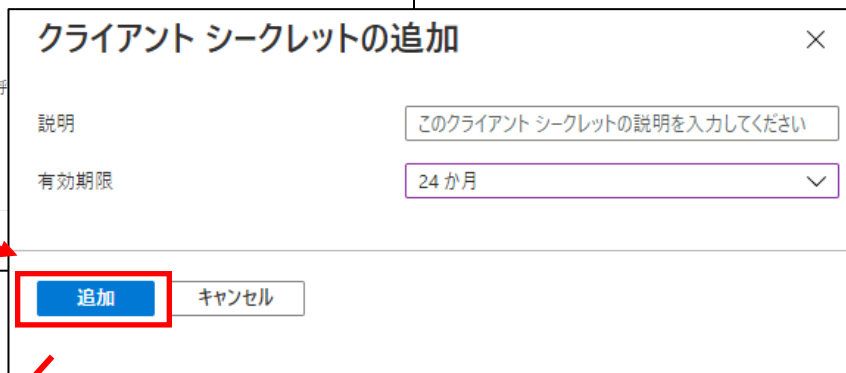
説明 有効期限 値 ①

このアプリケーションのクライアント シークレットは作成されていません。

「説明」 : 任意の説明  
「有効期限」 : 任意の有効期限

※有効期限が切れると連携できなくなるため、最長の「24 か月」を推奨します。

※有効期限が切れる前に、新しいクライアントシークレットを再作成して、POWEREGGのOffice365連携設定を更新してください。



クライアント シークレットの追加

説明 このクライアント シークレットの説明を入力してください

有効期限 24 か月

追加 キャンセル

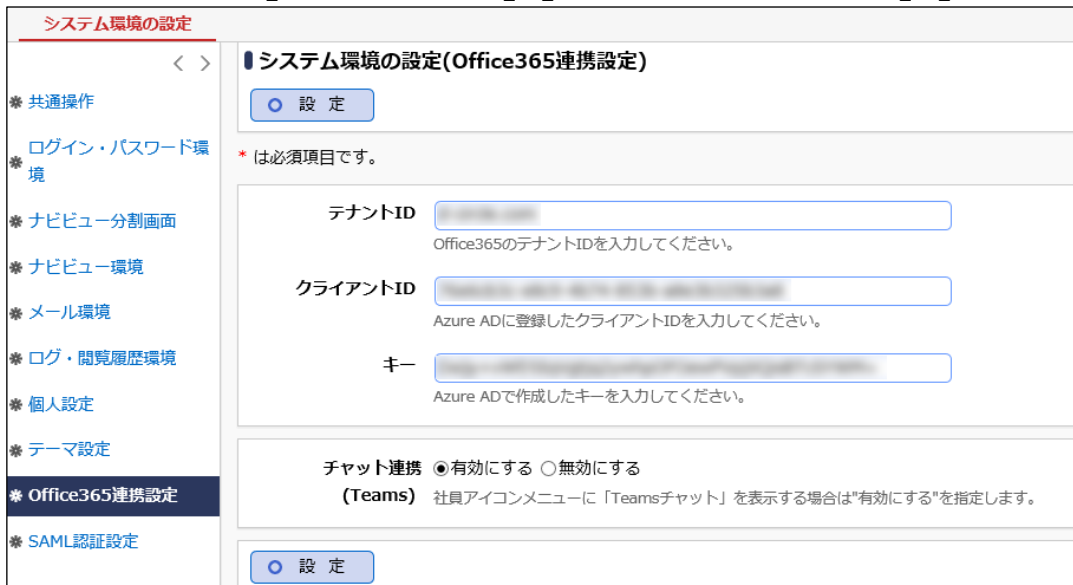
説明	有効期限	値 ①	シークレット ID
Password uploaded on Fri Feb 04 2022	2024/2/4	ukE7Q~sBPTs5muQKpB3ZG5mYil~qBHy...	8ad415d0-f643-4da4-88b5-2583f1304ae2

追加されたクライアントシークレットの「値」を、テキストファイル等に保存しておいてください。

※「値」は、後から参照できなくなります。わからなくなった場合は、クライアントシークレットを削除して再作成してください。

POWER EGG上で、Office365連携に必要な情報を設定します。

POWER EGG[システム設定]-[システム環境の設定]-[Office365連携設定]



※ チャット連携(Teams) は、Ver3.2c以降で利用可能です。

テナントID : Office365のテナントID(メールアドレスの@以降の部分、ドメイン名)  
クライアントID : アプリケーション(クライアント)ID ※ アプリケーションの「概要」で確認できます。  
キー : クライアントシークレットの「値」

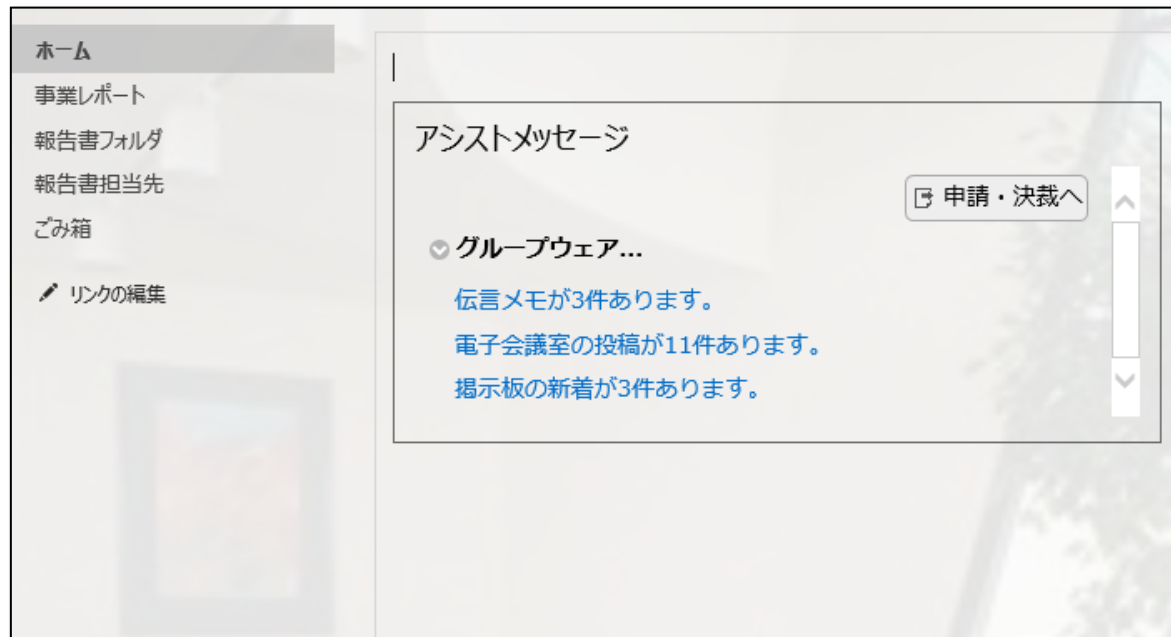


チャット連携(Teams) : 社員アイコンメニューからTeamsを起動する場合は、“有効にする”を指定

# SharePointへのアシストメッセージの表示

SharePointにWebパーツとしてPOWER EGGのURLを設定します。  
POWER EGGへのログインは、SSOで自動的行われます。

設定するURL : `https://サーバー名/pe4j/aadlogin4sharepoint`



SharePointポータルにアシストメッセージを表示する場合は、POWER EGGはhttpsプロトコルでアクセスするように設定する必要があります。  
(httpsでないと、ブラウザのセキュリティによりページが表示できません)

SharePointの設定方法の詳細は、別紙「モダンUIのポートレット登録方法」をご参照ください。

- PCリマインダー、リマインダー for iPhone、リマインダー for Androidは、Office 365のシングルサインオンには対応していません。（※POWER EGGに登録されているユーザーIDとパスワードでログインする必要があります）
- Office 365連携を行うには、POWER EGG へ HTTPS でアクセスできるよう設定する必要があります。
- Office 365連携を行うには、POWER EGG の Web サーバが以下のネットワーク要件を満たしている必要があります。
  - ・HTTPS プロトコルにてインターネットにアクセスできること
  - ・インターネット上の以下のホストの名前解決ができること  
graph.microsoft.com
- ログインしていない状態から、POWER EGGの特定のページにアクセスするときに表示される「ログイン画面」はOffice 365の認証連携に対応していません。
- POWER EGGナビビューのe-Mailタブには、Office 365の受信トレイの未読メールのみが表示されます。受信トレイ配下に作成したフォルダ内の未読メールは表示対象になりません。



- リバースプロキシや負荷分散装置を使用している場合、それらから POWER EGG サーバへの通信で、下記の HTTP リクエストヘッダが設定されるようにしてください。
  - x-forwarded-host: クライアントからアクセスするホスト名
    - ※ Apache をリバースプロキシとして使用する場合、デフォルトで設定されるため、設定不要です。
  - x-forwarded-proto: https
    - ※ POWER EGG サーバ側でも https で動作している場合は、設定不要です。
  - x-forwarded-port: クライアントからアクセスするポート番号
    - ※ 同じポート番号を使用している場合は、設定不要です。

設定例) Aapche をリバースプロキシとして使用している場合

httpd-ssl.conf の末尾の、</VirtualHost> の前に下記2行を追加し、Apache を再起動してください。

```
RequestHeader set x-forwarded-proto 'https'  
RequestHeader set x-forwarded-port '443'
```