

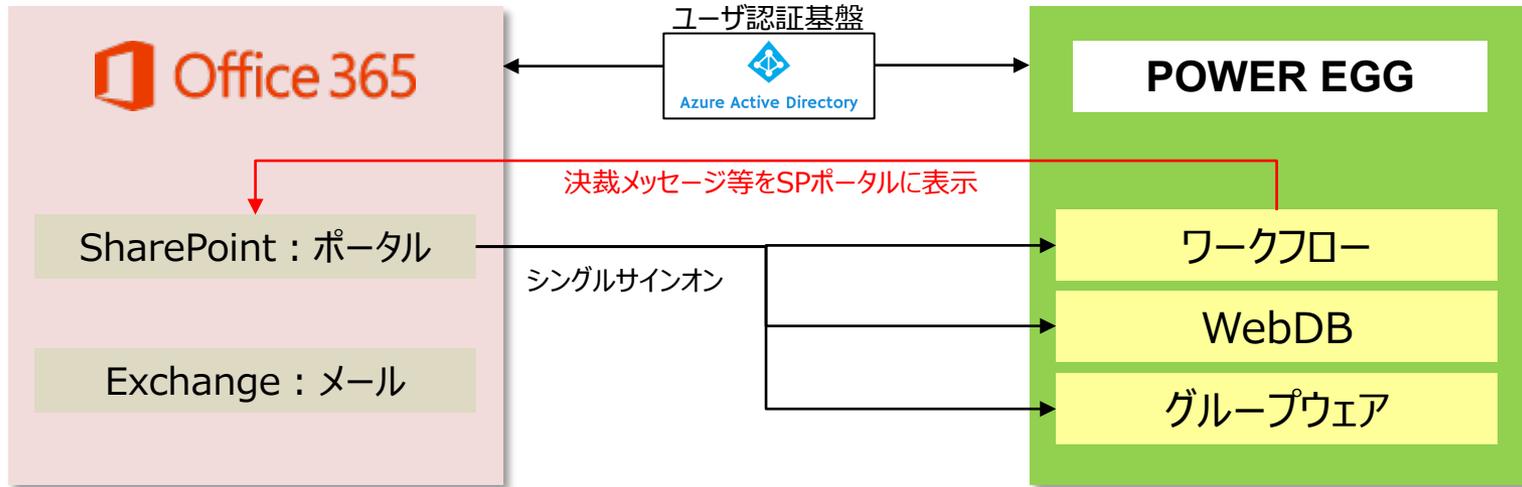
# POWER EGG 3.0 Office 365連携

2023年11月

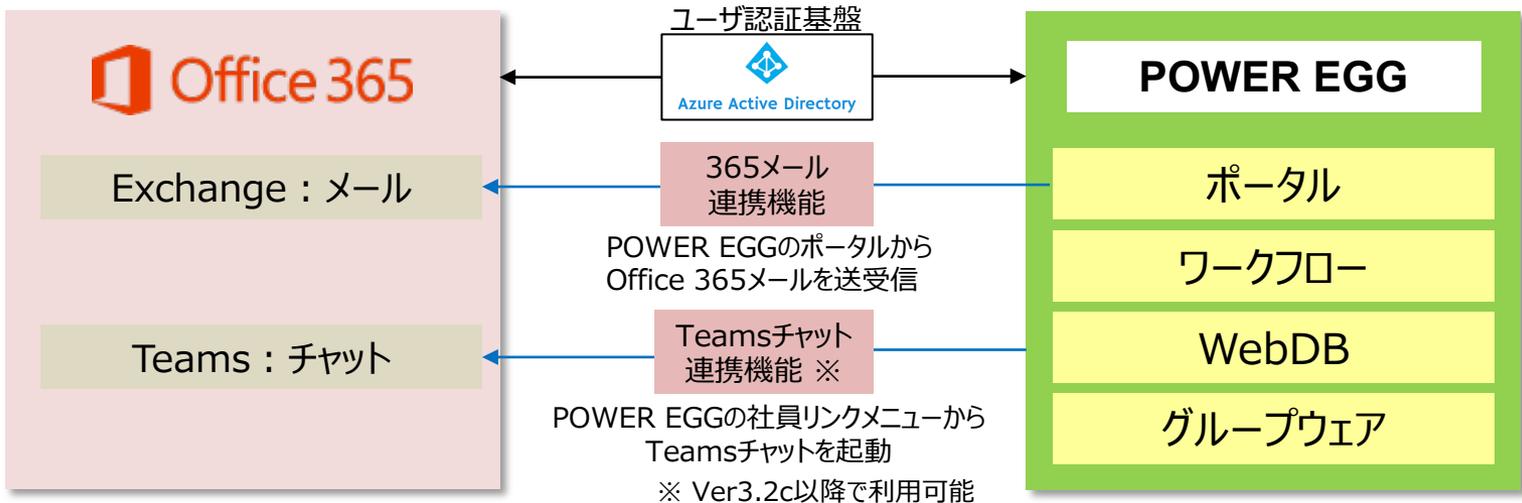
ディサークル株式会社

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
2023/01/12 7.0版	Azure Active Directory管理センターのUI変更に対応 シングルサインオンを行うURLに関するページを追加 留意事項を追記
2023/11/08 8.0版	Azure Active Directoryから Microsoft Entra IDへの名称変更、および管理センターのUI変更に対応 SharePoint 連携を使用する場合の設定について追記

## 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



②Office 365メニューからPOWER EGGを起動



③POWER EGGにシングルサインオンし、ナビビューを表示



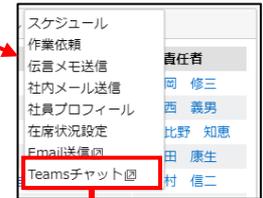
# 連携イメージ図②

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

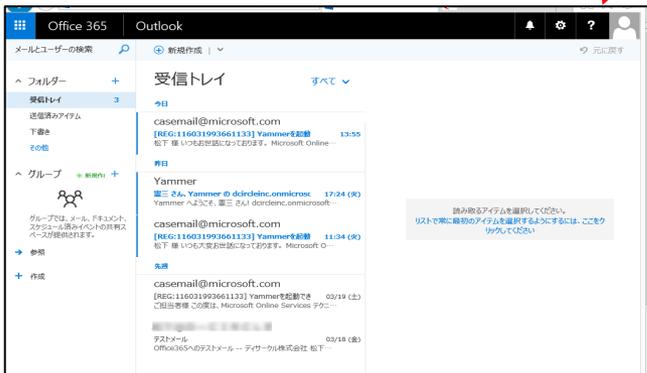
①POWER EGGのログイン時、Office 365(Azure AD)のログイン画面を表示



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



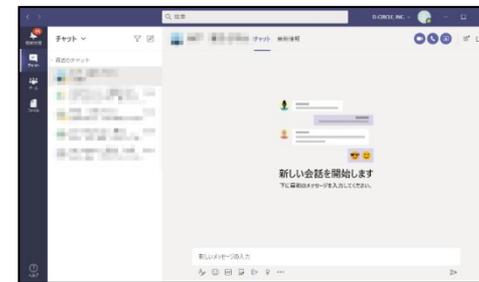
④ナビビューからOffice 365のメールを表示



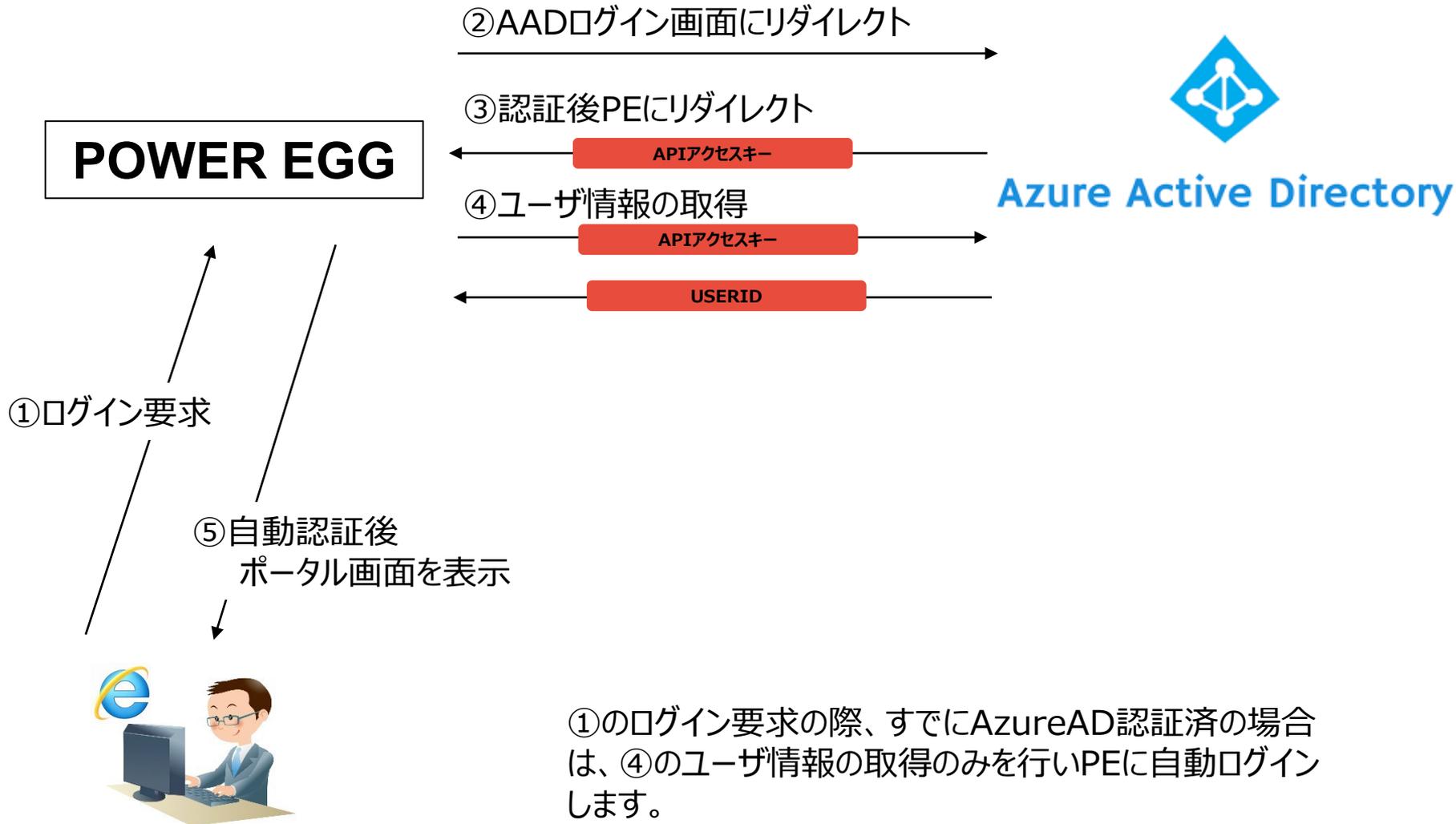
365メール連携機能

Teamsチャット連携機能 ※

⑤社員リンクメニューからTeamsアプリを起動



※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

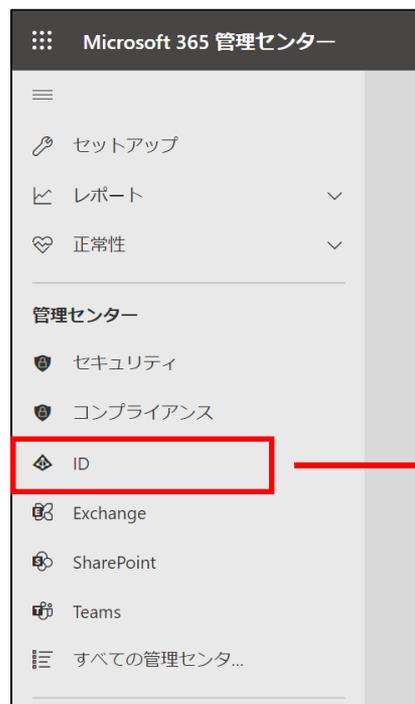
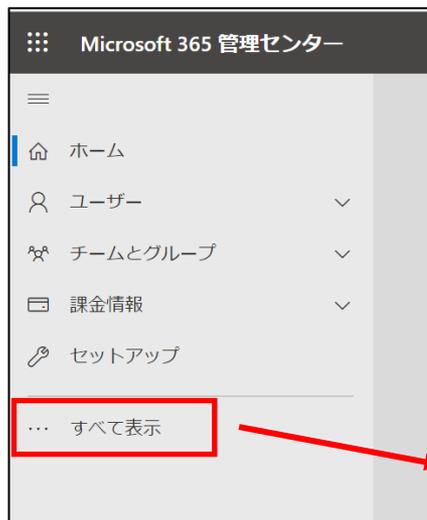


POWER EGG社員情報のメモ1： imaoka@o.d-circle.com

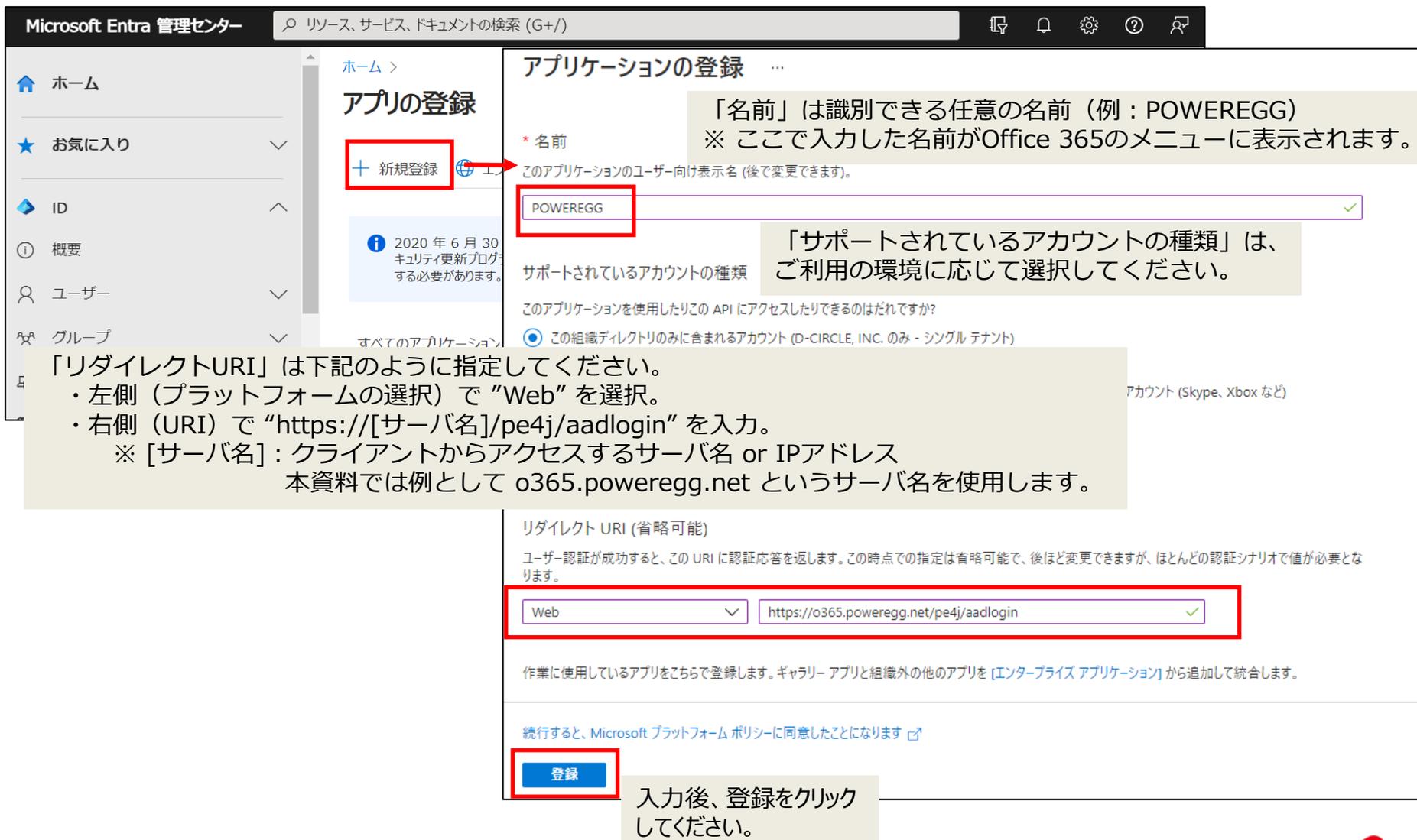
ユーザー、グループ等のAzure ADとの連携機能はありませんので、POWER EGGの組織情報（社員、部門等）はPOWER EGG側にあらかじめ登録しておく必要があります。

# Azure ADへのPOWER EGGの登録

Office 365にログインし、管理画面から「Microsoft Entra 管理センター」を開き、「アプリケーション」の中の「アプリの登録」を開きます。



「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。



Microsoft Entra 管理センター

ホーム > アプリの登録

+ 新規登録

「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。

\* 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)。  
POWEREGG

「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。

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だれですか?  
 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)  
 組織ディレクトリと他のディレクトリにまたがるアカウント (Skype, Xbox など)

「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

フィードバックがある場合

プラットフォームを追加

Web

リダイレクト URI

ユーザーが正常に認証またはサインアウトされた後に認証応答表示されているものと一致する必要があります。これは応答 URI

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

https://o3665.poweregg.net/pe4j/aadlogin

https://o3665.poweregg.net/pe4j/aadlogin4sharepoint

URI の追加

フロントチャネルのログアウト URL

ここでは、アプリケーションがユーザーのセッション データをクリアするように要求を送信します。これは、シングル サインアウトが正常に動作するために必要です。

例: https://example.com/logout

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。アプリケーションは、単独の承認コードフロー、または承認コードフローを使用していない場合、または JavaScript で Web 承認コードフローを使用している場合、または ASP.NET Core Web アプリケーションが承認コードフローを使用している場合、承認コードフローを使用します。

「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。

承認エンドポイントによって発行して使用する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

上記項目の設定後、「保存」を押してください。

保存 破棄

最初に「認証」を選択してください。

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

URI の追加

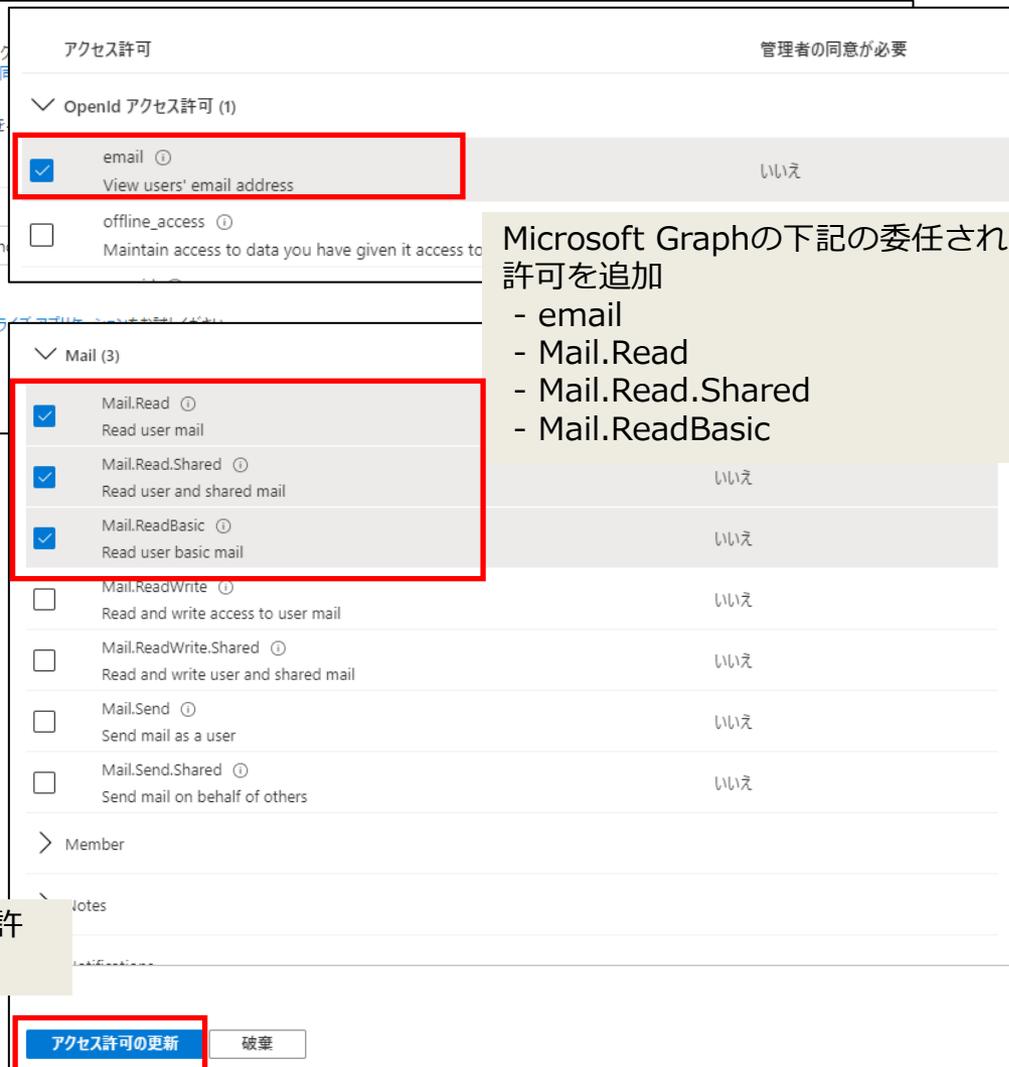
リダイレクトURIの入力欄が表示されていない場合は、「URIの追加」リンクを押してください。

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  
マニフェスト

構成されたアプリケーションは、同意のプロセスを完了してユーザーが管理コンソールにアクセスできるようにする必要があります。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  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	...

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」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	<input checked="" type="checkbox"/> D-CIRCLE, INC. に付与さ...
Mail.Read	委任済み	Read user mail	いいえ	<input checked="" type="checkbox"/> D-CIRCLE, INC. に付与さ...
Mail.Read.Shared	委任済み	Read user and shared mail	いいえ	<input checked="" type="checkbox"/> D-CIRCLE, INC. に付与さ...
Mail.ReadBasic	委任済み	Read user basic mail	いいえ	<input checked="" type="checkbox"/> D-CIRCLE, INC. に付与さ...
User.Read	委任済み	Sign in and read user profile	いいえ	<input checked="" type="checkbox"/> D-CIRCLE, INC. に付与さ...

状態にチェックが付いていることを確認

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  
クイックスタート  
統一  
管理  
プロパティ

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...

+ 新しいクライアントシークレット

説明 有効期限 値

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「730日（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

有効期限

追加 キャンセル

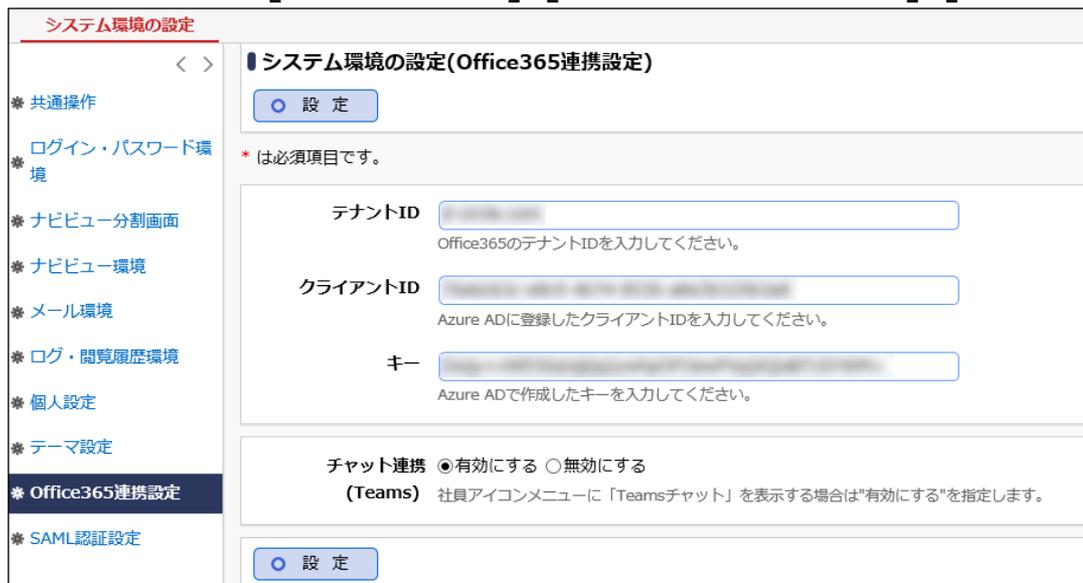
説明	有効期限	値	シークレット ID
Password uploaded on Fri Feb 04 2022	2024/2/4	ukE7Q~sBPTs5muQKpB3ZG5mYil~qBHy...	8ad415d0-f643-4da4-88b5-2583f1304ae2

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、Ver.3.2c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

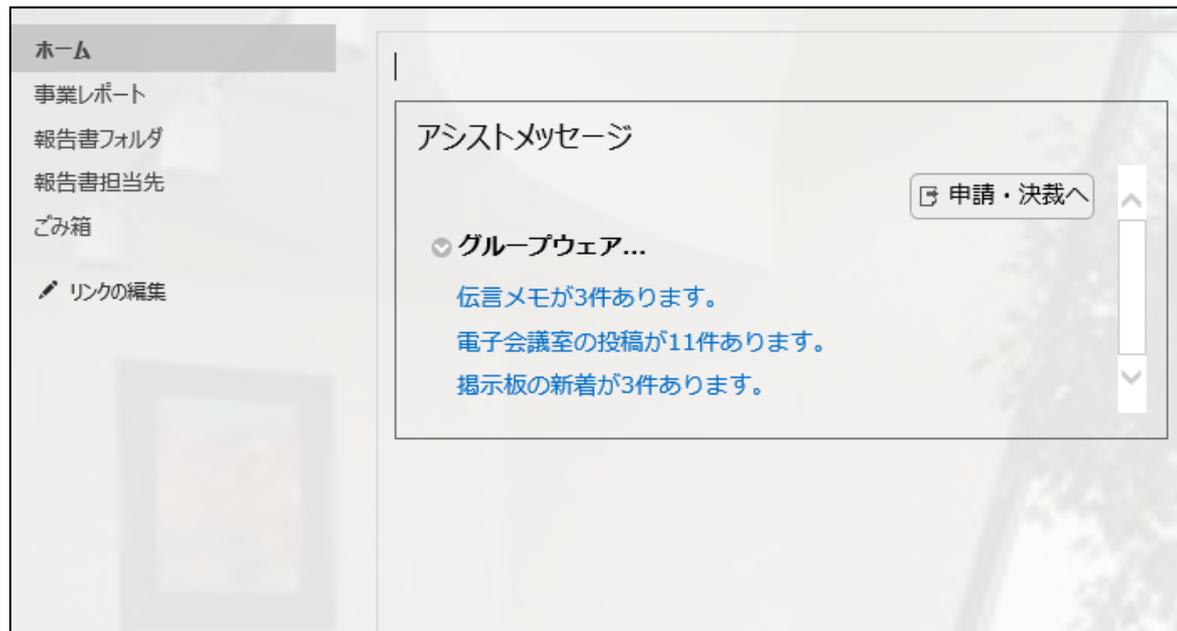
POWER EGGへOffice 365のアカウントでシングルサインオンする場合、下記のURLにアクセスします。

URL : <https://サーバー名/pe4j/aadlogin>

- ※ POWER EGGへアクセスするブラウザで事前にOffice 365へサインインしていない場合、Office 365のサインイン画面へ移動されます。  
Office 365へサインインすると、POWER EGGにシングルサインオンされます。

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で自動的に行われます。

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。

SharePointポータルにアシストメッセージを表示する際、ブラウザの制限により、POWER EGG サイトへの Cookie 情報の送信が正しく行われず、正常に表示されない場合があります。この問題を回避するため、下記の通り、POWER EGG のアプリケーションサーバで Cookie に「SameSite=None」属性を追加する設定を行ってください。

なお、POWER EGG オープンクラウド（POC）のお客様につきましては、弊社にてこの設定を行うため、SharePoint 連携を使用される場合はサポートまでご連絡ください。

## ・ Glassfish 版の場合

### 1. 下記ファイルをエディタで開く

C:¥PE4J¥Apache24¥conf¥extra¥httpd-ssl.conf

※C:¥PE4Jの部分は、POWEREGGのインストール先に応じて読み替えて下さい。

### 2. </VirtualHost>の前に下記の1行を追加

Header edit Set-Cookie ^(.\*)\$ \$1;SameSite=None

(設定例)

変更前 : </VirtualHost>

変更後 : Header edit Set-Cookie ^(.\*)\$ \$1;SameSite=None  
</VirtualHost>

### 3. 「POWEREGG HTTP Server」サービスを再起動

- Interstage 版の場合

1. 下記ファイルをエディタで開く

C:¥Interstage¥F3FMahs¥conf¥httpd.conf

※C:¥Interstageの部分は、Interstageのインストール先に応じて読み替えて下さい。

2. <VirtualHost \*:443>セクションの </VirtualHost>の前に下記の1行を追加

Header edit Set-Cookie ^(.\*)\$ \$1;SameSite=None

(設定例)

変更前 : </VirtualHost>

変更後 : Header edit Set-Cookie ^(.\*)\$ \$1;SameSite=None  
</VirtualHost>

3. 「Interstage HTTP Server 2.4」サービスを再起動

- 下記機能は、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）
  - PCリマインダー
  - リマインダー for iPhone
  - リマインダー for Android
  - スマートフォン版
  - 組織図エディタ
- 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。
- SAML認証連携との併用はできません。

- 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) Apache 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'
```