

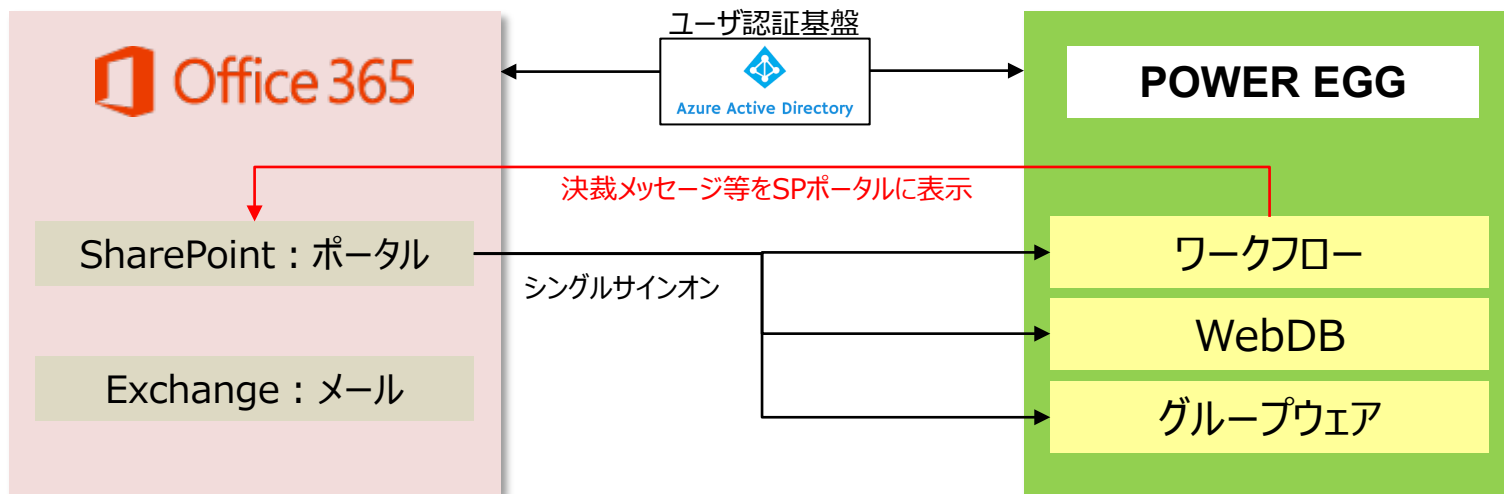
POWER EGG 3.0 Office 365連携

2023年1月

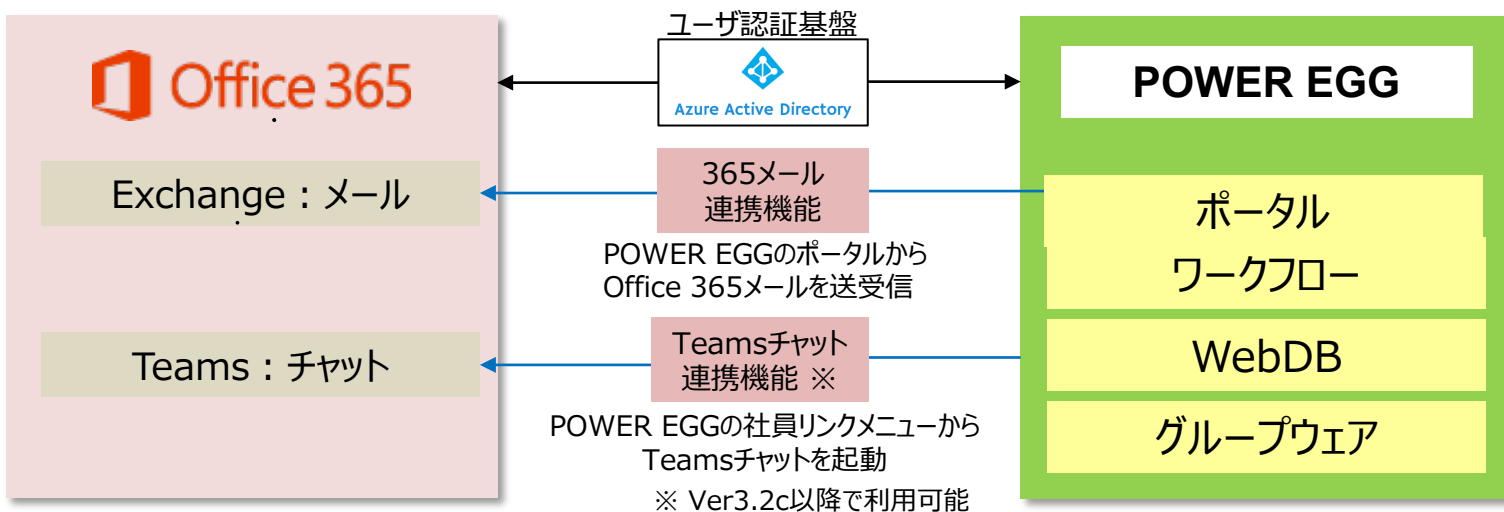
ディサークル株式会社

| 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 |

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



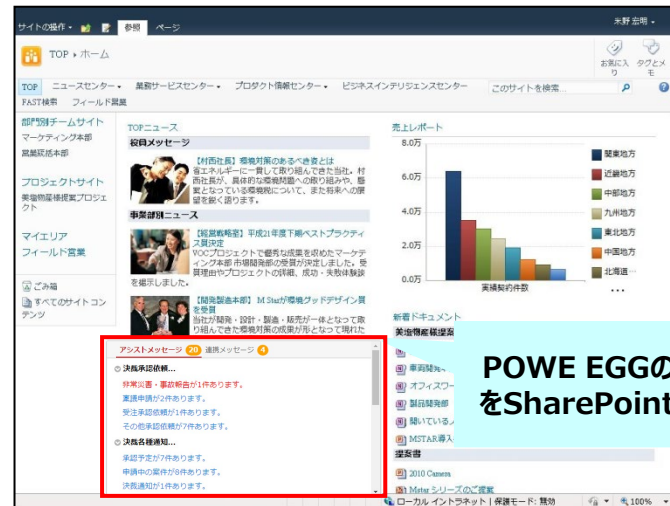
連携イメージ図①

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



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



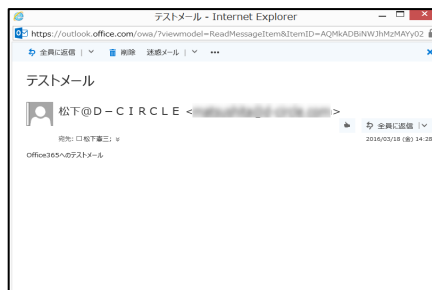
②ログイン後、ナビビューを表示



③ダイレクトボタンからOffice 365にシングルサインオン

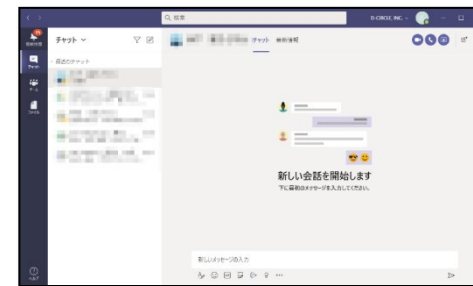


④ナビビューからOffice 365のメールを表示



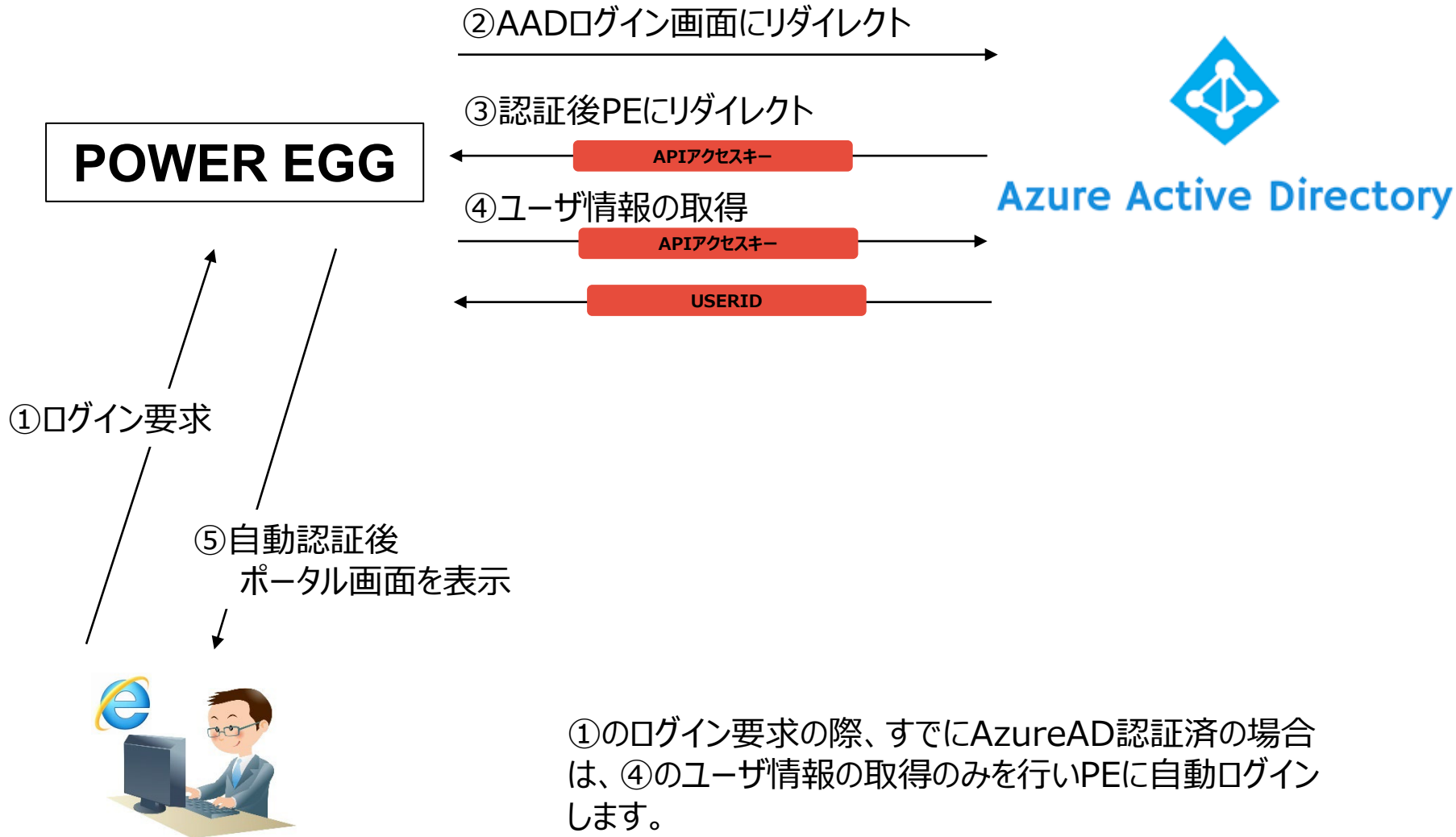
365メール連携機能

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



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。

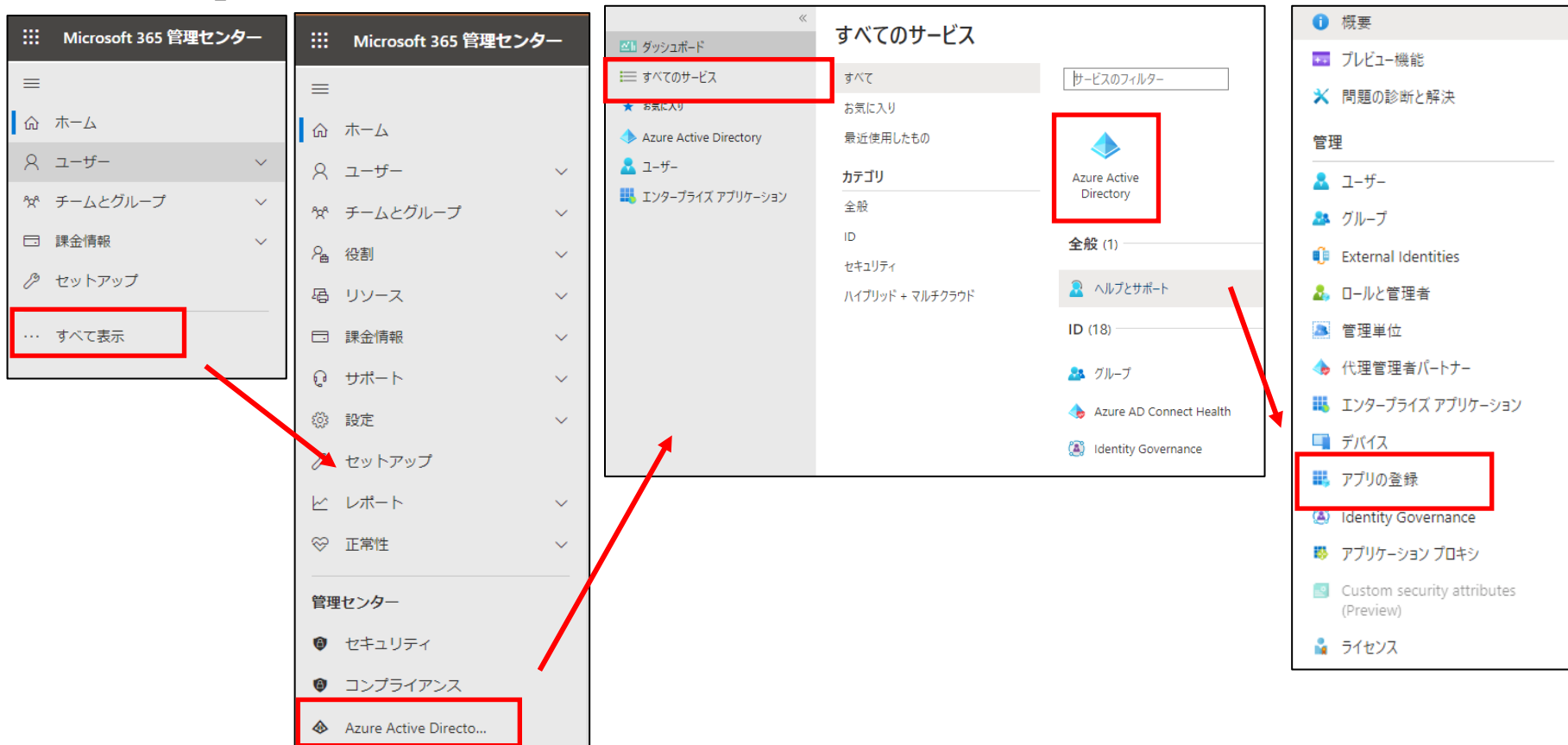
例： Office 365ログインID： imaoka@o.d-circle.com



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。

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 image shows a sequence of three screenshots from the Microsoft 365 Admin Center, illustrating the steps to reach the 'App Registrations' page:

- Left Screenshot:** The 'Microsoft 365 管理センター' (Microsoft 365 Admin Center) navigation menu. The 'すべて表示' (Show all) option at the bottom is highlighted with a red box. A red arrow points from this box to the 'Azure Active Directory' link in the '管理センター' (Admin Center) section at the bottom.
- Middle Screenshot:** The 'すべてのサービス' (All services) page. The 'すべてのサービス' (All services) link in the left sidebar is highlighted with a red box. A red arrow points from this box to the 'Azure Active Directory' service icon in the main content area.
- Right Screenshot:** The 'Azure Active Directory' management page. The 'アプリの登録' (App Registrations) link in the left sidebar is highlighted with a red box. A red arrow points from this box to the 'ヘルプとサポート' (Help and support) link in the main content area.

「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。

「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。

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)
 その他のディレクトリに接続されたアカウント (Skype, Xbox など)

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

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

「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。

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。

The screenshot shows the 'Authentication' settings for an application in Azure AD. The left sidebar has '認証' (Authentication) highlighted. The main content area is titled 'Web' and includes the following sections:

- リダイレクト URI**: A list of URIs. A text box highlights the instruction: 「リダイレクトURI」に “https://[サーバ名]/pe4j/aadlogin4sharepoint” を追加. A new URI, https://o3665.poweregg.net/pe4j/aadlogin4sharepoint, is being added to the list. A callout box points to the 'URIの追加' (Add URI) button.
- フロントチャネルのログアウト URL**: A text input field with the example https://example.com/logout.
- 暗黙的な許可およびハイブリッドフロー**: A section with a text box stating: 「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. The 'IDトークン (暗黙的およびハイブリッドフローに使用)' checkbox is checked and highlighted with a red box.

At the bottom, a text box says: 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. The '保存' (Save) button is highlighted with a red box.

Additional callouts include: 「最初に「認証」を選択してください。」 (Select 'Authentication' first.) and 「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。」 (If the redirect URI input field is not displayed, click the 'Add URI' link.)

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。



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承認する必要があります。アクセス許可と同意

アクセス許可の追加 ✓ D-CIRCLE, INC. 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 an |

「Microsoft Graph」をクリック

アクセス許可 管理者の同意が必要

OpenId アクセス許可 (1)

| | |
|--|-----|
| <input checked="" type="checkbox"/> email (1) View users' email address | いいえ |
| <input type="checkbox"/> offline_access (1) Maintain access to data you have given it access to | |

Mail (3)

| | |
|---|-----|
| <input checked="" type="checkbox"/> Mail.Read (1) Read user mail | |
| <input checked="" type="checkbox"/> Mail.Read.Shared (1) Read user and shared mail | いいえ |
| <input checked="" type="checkbox"/> Mail.ReadBasic (1) Read user basic mail | いいえ |
| <input type="checkbox"/> Mail.ReadWrite (1) Read and write access to user mail | いいえ |
| <input type="checkbox"/> Mail.ReadWrite.Shared (1) Read and write user and shared mail | いいえ |
| <input type="checkbox"/> Mail.Send (1) Send mail as a user | いいえ |
| <input type="checkbox"/> Mail.Send.Shared (1) Send mail on behalf of others | いいえ |

Member

Notes

アクセス許可の更新 破棄

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

構成されたアクセス許可

アプリケーションは、同意の付与を必要とするアクセス許可を要求する場合があります。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。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

最初に「証明書とシークレット」を選択してください。

証明書とシークレット

新しいクライアントシークレット

追加

「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

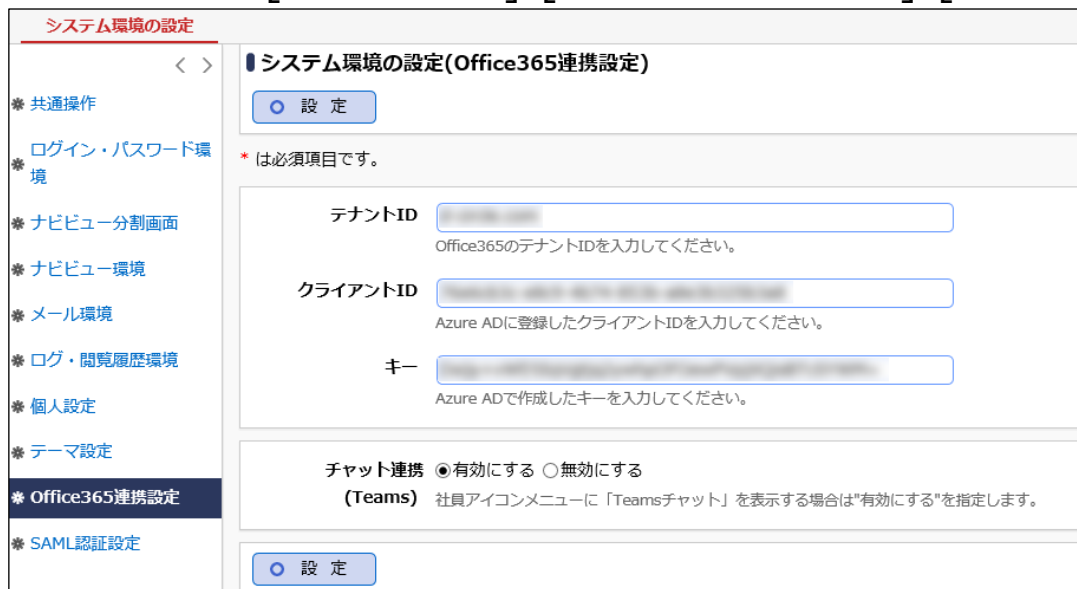
| 説明 | 有効期限 | 値 | シークレット ID |
|--------------------------------------|----------|------------------------------------|--------------------------------------|
| Password uploaded on Fri Feb 04 2022 | 2024/2/4 | ukE7Q~sBPTs5muQKpB3ZG5mYil~qBHy... | 8ad415d0-f643-4da4-88b5-2583f1304ae2 |

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

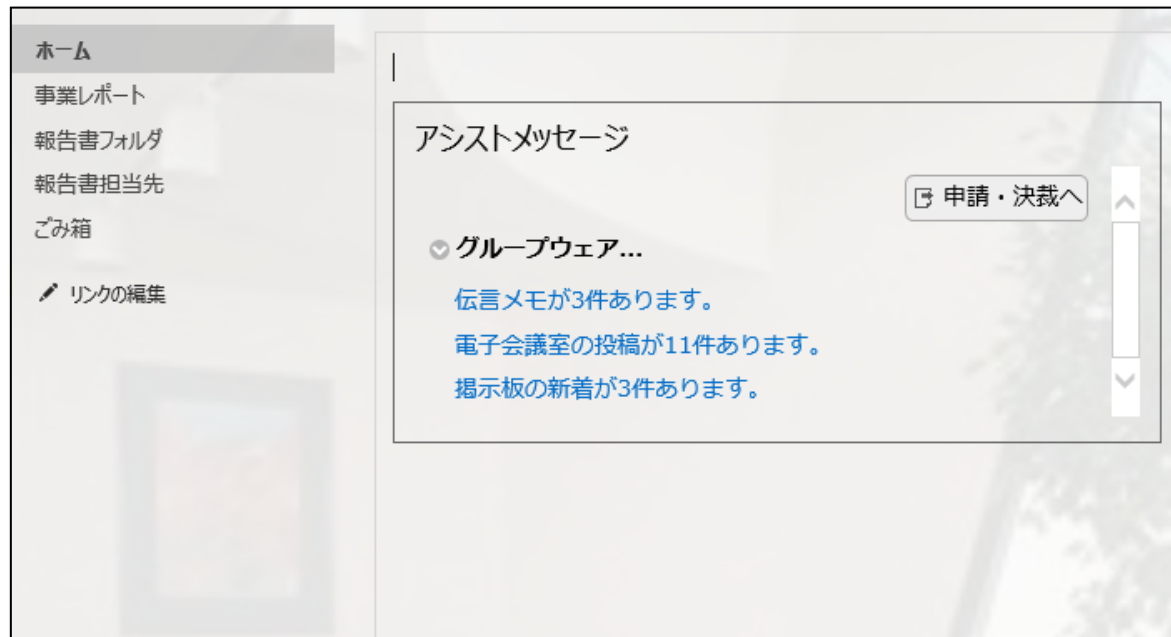
POWER EGGへOffice 365のアカウントでシングルサインオンする場合、下記のURLにアクセスします。

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。

- 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'
```