

# PHONE APPLI PEOPLE

## Azure AD連携のためのMS365設定手順

2022年12月

# PHONE APPLI

# 更新履歴

更新日	頁	更新内容
2018/11/23	全体	新規作成
2018/12/28	全体	補足情報を追加
2019/7/24	全体	設定手順内容の更新
2019/10/24	一部	設定手順内容の更新
2019/11/6	一部	設定手順内容の更新
2020/2/14	全体	設定手順内容の画面更新
2020/4/21	一部	名称の更新
2020/11/2	全体	名称の更新
2021/11/1	一部	必要となるアクセス許可を更新
2022/12/23	一部	設定手順内容の更新

# 目次

## ■ 目次

1. はじめに
2. Azure ADにアプリを追加する
3. APIのアクセス許可の設定
4. クライアントシークレットを発行する
5. PHONE APPLI PEOPLEに登録する

# 1. はじめに

## ■概要

本資料は「PHONE APPLI PEOPLE」のオプション機能である「Azure AD連携」機能を利用するためのMicrosoft 365の設定手順となります。

## ■注意事項（2019/5/10時点）

- ・ Microsoft 365はクラウドサービスであるため、実際の画面UIや設定手順とは差異がある可能性があります。
- ・ Microsoft 365のUI変更やAPIの変更に伴って、本設定手順も変更される可能性があります。
- ・ 本手順にて取得する「クライアントシークレット」には有効期限があり、失効すると、「PHONE APPLI PEOPLE」の「Azure AD連携」機能が利用できなくなります。  
失効前に「クライアントシークレット」を再発行し、「PHONE APPLI PEOPLE」管理画面より再登録してください。

## ■設定作業のための条件

- ・ Microsoft 365アカウント（管理者権限有り）  
Microsoft 365を操作するアカウントに必要なディレクトリロールは特にありません。
- ・ 設定箇所  
本手順はARM上（<https://portal.azure.com/>）での設定方法となります。  
クラシックポータル上（<https://manage.windowsazure.com/>）で設定をする場合は、Azureサブスクリプションを割り当てる必要があります。  
※割り当てるサブスクリプションは、テナント内のものであれば問題ありません。

## 2. Azure ADにアプリを追加する 1/3

- ARM (<https://portal.azure.com/>) にMicrosoft 365の管理者アカウントでログインし、Azure サービス内の「Azure Active Directory」を選択します。



## 2. Azure ADにアプリを追加する 2/3

- ・「アプリの登録」>「新規登録」を選択します。



ホーム > 株式会社 Phone Appli - アプリの登録

株式会社 Phone Appli - アプリの登録  
Azure Active Directory

検索 (Ctrl+/)

概要  
はじめに  
管理  
ユーザー  
グループ  
組織の関係  
ロールと管理者  
エンタープライズ アプリケーション  
デバイス  
アプリの登録  
Identity Governance

新規登録 エンドポイント トラブルシューティング

新しく強化されたアプリの登録へようこそ (一般提供になりました)。新機能

アプリの登録 (レガシ) からの変更点を確認する場合 [詳細情報](#)  
アプリの登録 (レガシ) の使用を続けますか? [前に戻って理由をお聞か](#)

すべてのアプリケーション 所有しているアプリケーション

名前またはアプリケーション ID を入力し始めると結果がフィルター処理

表示名	
RT	RTLK
RT	RTK3
TO	torerukun-o365-apps
PH	PhoneAppli
AA	AAA

## 2. Azure ADにアプリを追加する 3/3

- ・以下のように設定し、「登録」をクリックします。

名前

→任意のアプリケーション名を入力します。

サポートされているアカウントの種類

→「この種類のディレクトリ内のアカウントのみ」を選択します

アプリケーションの種類

→「Web」を選択します。

リダイレクトURL

→任意の値を入力します。

※当該値は利用しませんが、必須項目のため入力します。

### 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 (後ほど変更できます)。

**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?

☒ この組織のディレクトリ内のアカウントのみ (株式会社 P h o n e A p p l i )

☐ 任意の組織のディレクトリ内のアカウント

☐ 任意の組織のディレクトリ内のアカウントと、個人用の Microsoft アカウント (Skype、Xbox、Outlook.com など)

[選択に関する詳細...](#)

**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。

[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](#)

### 3. APIのアクセス許可の設定 1/4

- 「作成したアプリ」が開くのでアプリケーション（クライアント）IDをコピーします。

ホーム > 株式会社 P h o n e A p p l i - アプリの登録 > torerukun-o365-apps

torerukun-o365-apps

検索 (Ctrl+/)

概要

クイックスタート

管理

ブランド

認証

証明書とシークレット

トークン構成 (プレビュー)

削除 エンドポイント

少しお時間があれば、Microsoft ID プラットフォーム (以前)

表示名 : torerukun-o365-apps

アプリケーション (クライアント) ID : 02316300-1624-4684-8000-000000000000

ディレクトリ (テナント) ID : 44ee95d6-4b86-4280-a359-1c94aa15e151

オブジェクト ID : 874e16d6-4b86-4280-a359-1c94aa15e151

リダイレクト URI : 1 Web, 0 パブリック クライアント

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... : torerukun-o365-apps

新しく強化されたアプリの登録へようこそ。アプリの登録 (レガシ) からの変更点を確認することをご希望ですか? [詳細情報](#)

**【ポイント】**  
以下のアプリケーション（クライアント）IDが、PHONE APPLI PEOPLE「Azure AD連携」画面の「アプリケーションID」に入力する値となります。  
※右側をクリックするとコピーできます。

- 「APIのアクセス許可」を選択し、「Microsoft Graph(1)」をクリックします。

torerukun-o365-apps - API のアクセス許可

検索 (Ctrl+/)

概要

クイックスタート

管理

ブランド

認証

証明書とシークレット

トークン構成 (プレビュー)

API のアクセス許可

API の公開

最新の情報に更新

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 P h o n e A p p l i 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
Microsoft Graph (1)		
User.Read	委任済み	Sign in and read user profile



### 3. APIのアクセス許可の設定 2/4

- ・以下のように選択し、「API アクセスの追加」欄の「完了」をクリックします。

アプリケーションに必要なアクセス許可の種類  
→「アプリケーションの許可」を選択します。

アクセス許可を選択する  
→「アクセス許可」配下にある以下を選択します。

- ・ Group → Group.Read.All (Read all groups)
- ・ User → User.Read.All (Read all users' full profiles)

#### API アクセス許可の要求

Microsoft Graph  
<https://graph.microsoft.com/> [ドキュメント](#)

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ーモンとして実行されます。

#### API アクセス許可の要求

##### ▼ Directory (1)

- |   |    |
|---|----|
| <input checked="" type="checkbox"/> Group.Read.All<br>Read all groups ⓘ             | はい |
| <input type="checkbox"/> Directory.ReadWrite.All<br>Read and write directory data ⓘ | はい |

※ 画像は省略して表示しています。

#### API アクセス許可の要求

> DeviceManagementServiceConfig

##### ▼ Directory (1)

- |   |  |
|---|--|
| <input checked="" type="checkbox"/> Directory.Read.All<br>Read directory data ⓘ     |  |
| <input type="checkbox"/> Directory.ReadWrite.All<br>Read and write directory data ⓘ |  |

> Domain

> EduAdministration

> EduAssignments

> EduRoster

> ExternalItem

> Files

##### ▼ Group (1)

- |   |  |
|---|--|
| <input type="checkbox"/> Group.Create<br>Create groups ⓘ                    |  |
| <input checked="" type="checkbox"/> Group.Read.All<br>Read all groups ⓘ     |  |
| <input type="checkbox"/> Group.ReadWrite.All<br>Read and write all groups ⓘ |  |
| <input type="checkbox"/> Group.Selected<br>Access selected groups ⓘ         |  |

> GroupMember


> IdentityProvider


アクセス許可の更新

破棄

### 3. APIのアクセス許可の設定 3/4

- ・設定した項目を確認します。  
「委任されたアクセス許可」配下の、「User.Read (Sign in and read user profile)」も含まれていることを確認してください。

 最新の情報に更新




 アプリケーションに対するアクセス許可を追加しています。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。

#### 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 P h o n e A p p l i 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 (4)				...
Directory.Read.All	アプリケーシ...	Read directory data	はい	 株式会社 P h o n e A ... ...
Group.Read.All	アプリケーシ...	Read all groups	はい	 株式会社 P h o n e A ... ...
User.Read	委任済み	Sign in and read user profile	-	...
User.Read.All	アプリケーシ...	Read all users' full profiles	はい	 株式会社 P h o n e A ... ...

### 3. APIのアクセス許可の設定 4/4

- 以下の手順を実行します。

「～～に管理者の同意を与えます」をクリックし、「はい」を実施後、状態がになることを確認してください。

※Azure AD連携のためのアプリに対しての「アクセス許可に対する同意の付与」は、ディレクトリロールが「全体管理者」ではないユーザで実施しようとするとエラーになります。

 最新の情報に更新

株式会社 P h o n e A p p l i 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

はい

いいえ

必要なすべてのアクセス許可を含める必要があります。[アクセス許可の同意に関する詳細情報](#)

+ アクセス許可の追加

株式会社 P h o n e A p p l i 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 (4)				...
Directory.Read.All	アプリケーシ...	Read directory data	はい	 株式会社 P h o n e A ...
Group.Read.All	アプリケーシ...	Read all groups	はい	 株式会社 P h o n e A ...
User.Read	委任済み	Sign in and read user profile	-	...
User.Read.All	アプリケーシ...	Read all users' full profiles	はい	 株式会社 P h o n e A ...

## 4.クライアントシークレットを発行する

- ・「証明書とシークレット」を選択し、「新しいクライアントシークレット」を選択します。  
「クライアントシークレットの追加」で「説明」を入力し、「有効期間」から期間を選択します。  
※期間は任意で選択してください。
- ・「追加」をクリックすることで、クライアントシークレットが発行されるため取得してください。  
※このページを離れると取得不可となります。

torerukun-o365-apps - 証明書とシークレット

検索 (Ctrl+/)

概要

クイックスタート

管理

ブランド

認証

**証明書とシークレット**

トークン構成(プレビュー)

API のアクセス許可

API の公開

所有者

ロールと管理者(プレビュー)

マニフェスト

サポート + トラブルシューティング

トラブルシューティング

新しいサポートリクエスト

クライアント シークレットの追加

説明

有効期限

☐ 1 年

☐ 2 年

☒ なし

追加 キャンセル

クライアント シークレット

トークンの要求時にアプリケーションが自身の ID を証明することもあります。

**+ 新しいクライアント シークレット**

説明

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

【ポイント】  
このクライアントシークレットの値が、  
PHONE APPLI PEOPLEの「Azure AD連携」管理画面の、  
「キー」に入力する値となります。

クライアント シークレット		
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。アプリケーションが呼びばれることもあります。		
+ 新しいクライアント シークレット		
説明	有効期限	値
key	2299/12/31	qO...

## 5. PHONE APPLI PEOPLEへ登録する

- 以下の手順を実行します。

「管理」→「Azure AD連携」をクリックしてください。

「取得対象」にて以下を登録し、接続テストをクリックし、「サーバへの接続に成功」した後に「保存」してください。

→ドメイン (Microsoft365のドメインを入力)

アプリケーションID (Azure ADで取得したアプリケーション (クライアント) IDを入力してください。)

キー (Azure ADで取得したクライアントシークレットの値を入力してください。)

※「アプリケーションID」と「キー」は読み替えて登録してください。

The screenshot shows the '管理 - Azure AD連携' (Management - Azure AD Connection) page. The '取得対象' (Target for acquisition) tab is selected. The 'Azure AD連携' (Azure AD Connection) menu item is highlighted. The form contains the following fields and buttons:

- 取得対象** (Target for acquisition):
  - ドメイン (Domain): phoneappli.net
  - アプリケーションID (Application ID): 12adf16
  - キー (Key): [Redacted]
- 接続テスト** (Connection Test) button
- メッセージ** (Message) box:
  - サーバへの接続に成功しました。 (Connection to the server was successful.)
  - 閉じる** (Close) button
- 保存** (Save) and **手動同期** (Manual Sync) buttons

Red dashed boxes and arrows indicate the sequence: 1. Click 'Azure AD連携'. 2. Enter domain, application ID, and key. 3. Click '接続テスト'. 4. Click '保存'.

※画像は省略して表示しています。

「働く」を変える。「生きかた」が変わる。

# PHONE APPLI

[info@phoneappli.net](mailto:info@phoneappli.net)