

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。

portal.azure.com/#home

Microsoft Azure

リソース、サービス、ドキュメントの検索 (G+)

Azure へようこそ!

サブスクリプションをお持ちでない場合は、次のオプションをご確認ください。



Azure の無料試用版から開始する

Azure の製品とサービスに使用できる 200 ドルの無料クレジットを取得できるだけでなく、人気の無料サービスを 12 か月間利用できます。

[開始](#) [詳細](#)



Azure Active Directory の管理

Azure Active Directory を使用して、アクセスを管理し、スマートポリシーを設定し、セキュリティを強化します。

[ビュー](#) [詳細](#)



学生特典にアクセスする

教育機関ステータスの確認後、無料のソフトウェアまたは Azure クレジットを取得するか、Azure Dev Tools for Teaching にアクセスしてください。

[エクスプローラー](#) [詳細](#)

Azure サービス

[リソースの作成](#) **Azure Active Directory** [Intune](#) [すべてのリソース](#) [Virtual Machines](#) [App Service](#) [ストレージ アカウント](#) [SQL データベース](#) [Azure Database for PostgreSQL](#) [その他のサービス](#)

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。

The screenshot shows the Azure AD portal interface for '株式会社 Phone Appli - アプリの登録'. The breadcrumb path is 'ホーム > 株式会社 Phone Appli - アプリの登録'. The main header includes the company name and 'Azure Active Directory'. A search bar is present with the placeholder text '検索 (Ctrl+/)'. A navigation menu on the left lists various management options: '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', and 'Identity Governance'. The 'アプリの登録' option is highlighted with a red dashed box. The main content area features a navigation bar with '新規登録', 'エンドポイント', and 'トラブルシューティング'. Below this is an information message about app registration enhancements and a warning about legacy app registration changes. There are two tabs: 'すべてのアプリケーション' and '所有しているアプリケーション'. A search bar for filtering apps is also visible. The table below shows a list of applications with columns for '表示名' and application details.

表示名	アプリケーション ID
RTLK	RT
RTK3	RT
torerukun-o365-apps	TO
PhoneAppli	PH
AAA	AA

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)。
torerukun-o365-apps ✓

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。
Web ▼ http://localhost ✓

[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

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+/) 削除 エンドポイント

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)

表示名 : torerukun-o365-apps

アプリケーション (クライアント) ID : 02316300... (Red dashed box)

リダイレクト URI : 1 Web, 0 パブリック クライアント

ディレクトリ (テナント) ID : 44ee95d6...

アプリケーション ID の URI : アプリケーション ID URI の追加

オブジェクト ID : 874e16d6...

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](#)

- 「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+/) 最新の情報に更新

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 (Red dashed box)

API の公開

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 を呼ぶの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) (Red dashed box)		
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

- > DeviceManagementServiceConfig
- ▼ Directory (1)
 - Directory.Read.All
Read directory data ⓘ
 - Directory.ReadWrite.All
Read and write directory data ⓘ
- > Domain
- > EduAdministration
- > EduAssignments
- > EduRoster
- > ExternalItem
- > Files
- ▼ Group (1)
 - Group.Create
Create groups ⓘ
 - Group.Read.All
Read all groups ⓘ
 - Group.ReadWrite.All
Read and write all groups ⓘ
 - Group.Selected
Access selected groups ⓘ
 - > GroupMember
 - > IdentityProvider

アクセス許可の更新 破棄

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)

- Group.Read.All
Read all groups ⓘ はい
- Directory.ReadWrite.All
Read and write directory data ⓘ はい

※ 画像は省略して表示しています。

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](#)

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。

toorerukun-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...

マニフェスト

サポート + トラブルシューテ...

新しいクライアントシークレット

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

【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。

管理 - Azure AD連携

企業情報 部署 ユーザ 共有電話帳 お知らせ ログ出力 AD連携 Sansan連携 Cisco CMX EXBeacon Azure AD連携

取得対象 紐付け設定 デフォルト値設定 処理結果

ドメイン phoneappli.net

アプリケーションID 12adf16

キー

接続テスト

メッセージ

サーバへの接続に成功しました。

閉じる

保存 手動同期

※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