

# PHONE APPLI PEOPLE

## Microsoft Intune モバイル アプリケーション管理 設定手順

2022/12/01

株式会社PHONE APPLI

# 更新履歴

| 更新日        | 頁  | 更新内容   |
|------------|----|--|
| 2021/03/12 | 全体 | 新規作成   |
| 2022/06/17 | 9  | 「できません。アプリの保護ポリシー適用のみ対応しています。」から「できます。アプリの構成ポリシーを利用することで対応しています。」へ修正                                   |
| 2022/06/17 | 6  | ラッピングIntune対応したPA PEOPLE というのは、2022/06/17現在では存在しないため、前提条件を削除。PA PEOPLE(RTK)の(RTK)を削除。RTK を 連絡とれるくんに変更。 |
| 2022/06/17 | 7  | ラッピングIntune対応したPA PEOPLE というのは、2022/06/17現在では存在しないため、前提条件を削除。PA PEOPLE(RTK)の(RTK)を削除。RTK を 連絡とれるくんに変更。 |
| 2022/06/17 | 3  | 現在のページに沿って目次を修正  |
| 2022/06/17 | 4  | 注意事項に、「「PHONE APPLI PEOPLE」または「PA PEOPLE」と表記されている部分は、お客様状況により、適宜「連絡とれるくん」と読み替えてください。」を追記               |
| 2022/06/21 | 7  | ※Androidでは、アプリ構成ポリシーの「IntuneMAMUPN」の設定は不要です。<br>の注意文言を追加。  |
| 2022/12/01 | 全体 | iPhone版アプリのADAL→MSALへのライブラリ変更対応により、必要な設定を追記。   |

# 目次

1. はじめに
  - 1.1 はじめに
  - 1.2 PA PEOPLEのMS Intune MAM対応とは？
2. iPhoneでのアプリ保護ポリシーの設定の流れ
  - 2.1 アプリ保護ポリシーの適用にあたって必要な作業
  - 2.2 エンタープライズアプリケーションの作成とアクセス許可
  - 2.3 設定後の確認
  - 2.4 注意事項
  - 2.5 アプリ保護ポリシー適用の流れ (iPhone)
3. iPhoneにて特定のアプリ保護ポリシーをご利用の場合の設定作業
  - 3.1 特定のアプリ保護ポリシーを利用されている場合
4. iPhoneにて条件付きアクセスをご利用の場合の設定作業
  - 4.1 Azure ADで条件付きアクセスを利用されている場合
  - 4.2 ブローカーアプリをインストールできない場合
5. Androidでのアプリ保護ポリシーの設定の流れ
  - 5.1 アプリ保護ポリシー適用の流れ (Android)
6. PA PEOPLEへのログイン制限について (iPhone、Android共通)
  - 6.1 PA PEOPLEへのログイン制限
7. よくある質問
  - 7.1 よくある質問

# 1. はじめに



# 1.1 はじめに

## ■ 概要

本資料はMicrosoft Intune モバイルアプリケーション管理にて「PHONE APPLI PEOPLE」を利用するためのMicrosoft 365の設定手順となります。

## ■ 注意事項

- ・ 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。
- ・ 「PHONE APPLI PEOPLE」または「PA PEOPLE」と表記されている部分は、お客様状況により、適宜「連絡とれるくん」と読み替えてください。

## ■ 保護ポリシーについて

MS Intune MAMでは「アプリ保護ポリシー」というプロファイルを作成し、アプリケーションに適用することで、アプリケーションの動作を制御します。

PA PEOPLEスマートフォン版アプリの機能を利用できる保護ポリシーについては、「PHONE APPLI PEOPLE\_MS Intune MAM保護ポリシーについて.xlsx」を参照してください。

なお、PHONE APPLIで確認している設定と差異がある場合は、トライアルなどでご確認ください。  
基本的にお客様の保護ポリシーを適用したPA PEOPLEにて、ご利用いただきたい機能が動作する場合はご利用いただいて問題ありません。  
ただし「MS Intune MAM」の制御によって、一部機能が動作しないことが判明した場合、MS Intune MAM利用における制限事項となります。  
それは、「MS Intune MAM」の制御によってPA PEOPLEの機能が制限されているため、PA PEOPLE側での対応はできないためです。

## 1.2 PA PEOPLEのMS Intune MAM対応とは？

**Microsoft Intune** ×  **PHONE APPLI PEOPLE**

「PHONE APPLIE PEOPLE」スマートフォン版アプリは、Microsoft Intuneの「Microsoft Intune モバイル アプリケーション管理」(MS Intune MAM)に対応し、MS Intune上で「アプリ保護ポリシー」の適用が可能となります。

お客様独自のアプリ保護ポリシーで「PHONE APPLI PEOPLE」を運用できます。

※本対応はスマートフォン版アプリの対応となります。

※ご利用には、Intune ポータルサイトのサインインアカウントとPA PEOPLEログインアカウントが同一である必要があります。

※お客様独自のアプリ保護ポリシーの設定をされている場合、一部追加設定が必要になる場合がございます。

## 2. iPhoneでのアプリ保護ポリシーの設定の流れ

## 2.1 アプリ保護ポリシーの適用にあたって必要な作業

「PA PEOPLE(連絡とれるくん) iPhone版アプリ v.1.38.2」以降をご利用になる場合は、アプリをダウンロードする前に、管理者様によるアプリ利用設定の作業が必要です。

(Android版アプリの場合は、本設定は必要ありません。)

本章ではiPhone版アプリ利用設定の作業が必要となる環境・条件の説明と、作業手順について説明していますので、内容をご確認の上、作業の実施をお願いいたします。



## 2.2 エンタープライズアプリケーションの作成とアクセス許可 1/2

① 利用しているアプリケーション名を確認し、ブラウザから以下のURLへのアクセスをお願いします。

※以下URLをコピーし、メモ帳に貼り付け、

**{tenant-id}**を、AzureのテナントIDに書き換えてブラウザでアクセスしてください。

なお、AzureのテナントIDは「Azure Active Directory > 概要」画面でテナントIDを確認できます。

A) PHONE APPLI PEOPLEをご利用の場合

エンタープライズアプリケーションの名称は「PHONE APPLI PEOPLE for Intune」となります。

[https://login.microsoftonline.com/{tenant-id}/adminconsent?client\\_id=8b8dde6e-b378-4f50-bb65-8982ed1f8e29](https://login.microsoftonline.com/{tenant-id}/adminconsent?client_id=8b8dde6e-b378-4f50-bb65-8982ed1f8e29)

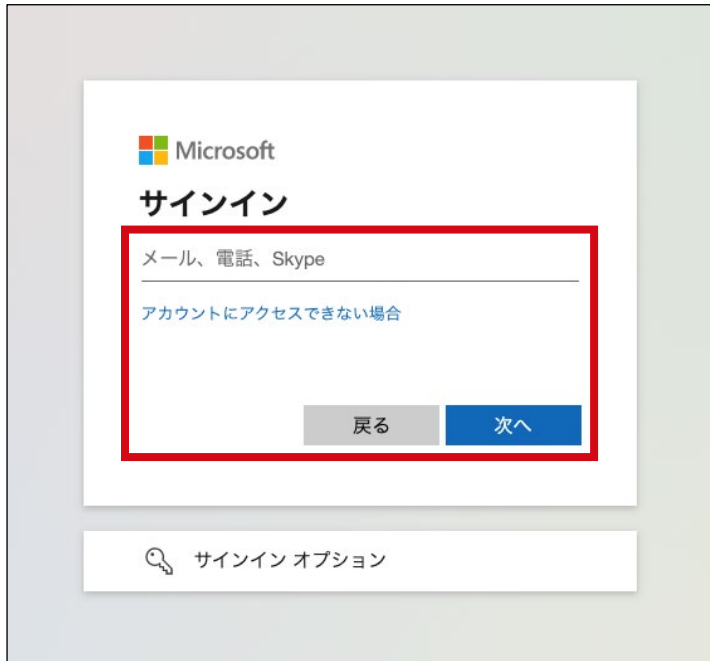
B) 連絡とれるくんをご利用の場合

エンタープライズアプリケーションの名称は「連絡とれるくん for Intune」となります。

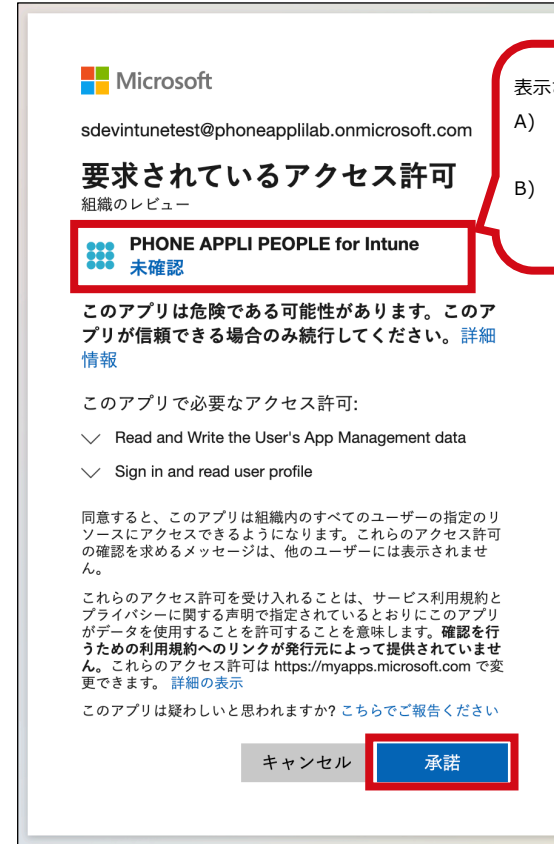
[https://login.microsoftonline.com/{tenant-id}/adminconsent?client\\_id=03b83714-979c-4b8d-99ff-540bbfe1e08f](https://login.microsoftonline.com/{tenant-id}/adminconsent?client_id=03b83714-979c-4b8d-99ff-540bbfe1e08f)

## 2.2 エンタープライズアプリケーションの作成とアクセス許可 2/2

② ブラウザ上で以下の操作をしてください。



URLへアクセスすると、サインインを求められるため、Azureのグローバル管理者でサインインを行う。



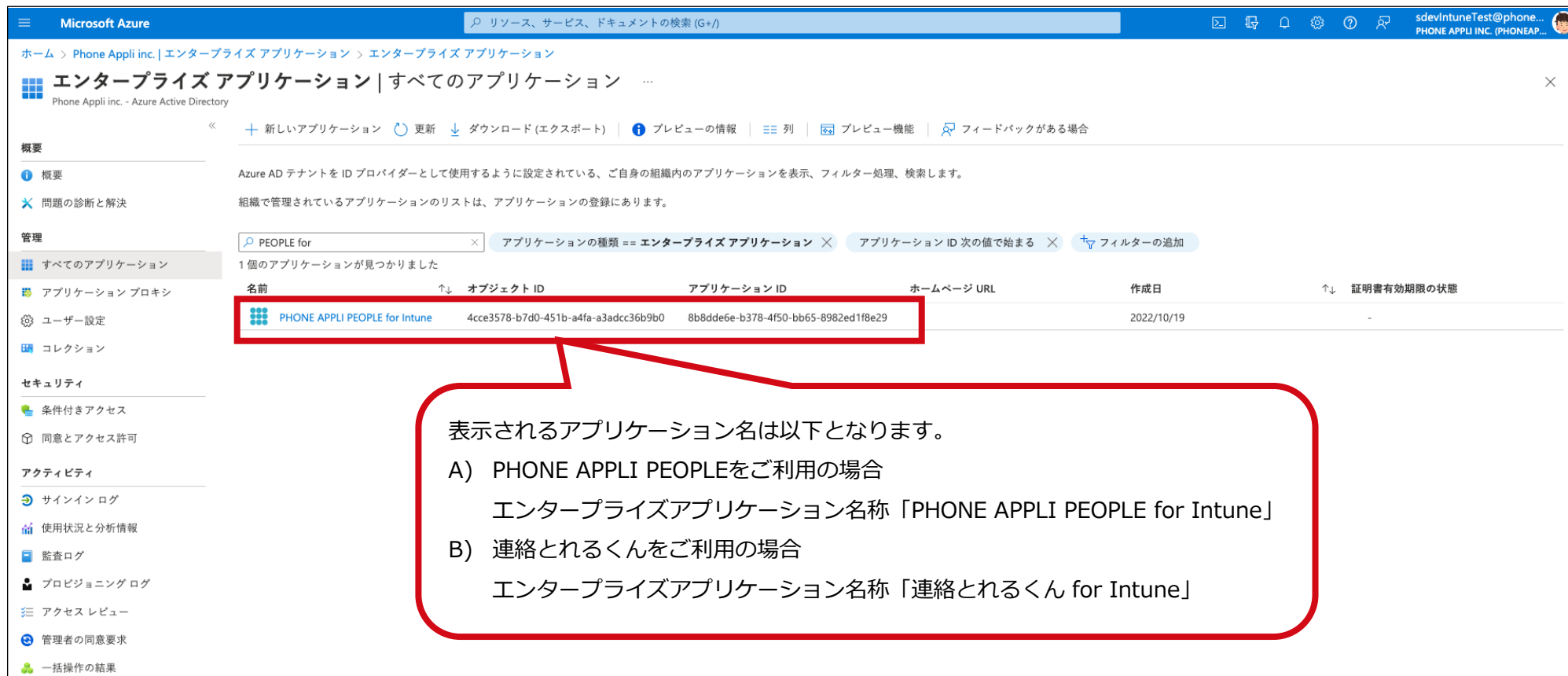
表示されるアプリケーション名は以下となります。

- A) PHONE APPLI PEOPLEをご利用の場合  
エンタープライズアプリケーション名称「PHONE APPLI PEOPLE for Intune」
- B) 連絡とれるくんをご利用の場合  
エンタープライズアプリケーション名称「連絡とれるくん for Intune」

表示されているエンタープライズアプリケーション名に間違いがないことを確認し、「承諾」をクリックする。

## 2.3 設定後の確認

作業後、エンタープライズアプリケーションが新規で作成されるため、Azure AD上にも表示されているかを確認してください。表示されていれば、作業は完了です。



The screenshot shows the Microsoft Azure portal interface. The main content area displays the 'Enterprise Applications' page for 'Phone Appli inc. - Azure Active Directory'. A search filter 'PEOPLE for' is applied, resulting in one application being listed: 'PHONE APPLI PEOPLE for Intune'. The application details shown are:

| 名前                            | オブジェクト ID                            | アプリケーション ID                          | ホームページ URL | 作成日        | 証明書有効期限の状態 |
|-------------------------------|--------------------------------------|--------------------------------------|------------|------------|------------|
| PHONE APPLI PEOPLE for Intune | 4cce3578-b7d0-451b-a4fa-a3adcc36b9b0 | 8b8dde6e-b378-4f50-bb65-8982ed1f8e29 |            | 2022/10/19 | -          |

A red callout box contains the following text:

表示されるアプリケーション名は以下となります。

- A) PHONE APPLI PEOPLEをご利用の場合  
エンタープライズアプリケーション名称「PHONE APPLI PEOPLE for Intune」
- B) 連絡とれるくんをご利用の場合  
エンタープライズアプリケーション名称「連絡とれるくん for Intune」

## 2.4 注意事項

- 既にご利用中のお客様環境では、設定作業が完了する前に「PA PEOPLE(連絡とれるくん) iPhone版アプリ v.1.38.2(または当該バージョン以降のアプリ)」にアップデートしご利用いただく場合、**セッションが切れる**と、「管理者の承諾を要求する」画面がiPhone版アプリ上に表示されます。

当該画面は、エンドユーザ操作時にも表示されるため、エンドユーザ様は事実上、「PA PEOPLE(連絡とれるくん) iPhone版アプリ」にログインできなくなります。

そのため、「PA PEOPLE(連絡とれるくん) iPhone版アプリ v.1.38.2」がリリースされる前に、必ず本書の設定作業を完了させてください。

### セッションが切れる主な要因

- ✓ 新規インストール（現行のiPhone版アプリを削除し、最新のiPhone版アプリをインストール）
- ✓ Azureの管理者による明示的なセッション削除
- ✓ Azureにおけるアカウントのパスワード変更

※これらはPHONE APPLI社で確認ができた、セッションが切れるタイミングです。

その他にもセッションが切れる要因はあると想定されますが、

Azureの機能や仕様に依存するため、PHONE APPLI社で全ての要因を把握し、ご案内することはできません。

- iPhone版の「PHONE APPLI PEOPLE」と「連絡とれるくん」の両方をご利用いただく環境では、「2.1 エンタープライズアプリケーションの作成とアクセス許可」と「2.2 設定後の確認」をそれぞれのアプリケーション名で実施してください。（同じ作業をアプリケーション名を変えて2回作業する）
- PA PEOPLE（連絡とれるくん） v.1.38.2以降 を使用してアプリ保護ポリシーを取得する場合は、Microsoft Authenticator の使用が必須となります。



## 2.5 アプリ保護ポリシー適用の流れ (iPhone) 1/2

### ■ 管理者によるMS Intune管理画面の作業

- ① PA PEOPLEを「アプリ」に追加します。
  - アプリ名「PHONE APPLI PEOPLE」で検索し、登録します。
  - 「ポータル サイトでおすすぬめアプリとして表示する」は「はい」を選択します。
  
- ② アプリ保護ポリシーでPA PEOPLEをカスタムアプリとして登録し、ポリシーを設定します。
  - リストにアプリが表示されなければ、パッケージ名に以下のバンドルIDを指定して追加します。  
PA PEOPLE : net.phoneappli.people  
連絡とれるくん : net.phoneappli.renraku
  
- ③ アプリ構成ポリシーを作成し、PA PEOPLEに適用します。
  - ※以下が手順の詳細です。
  - こちらを設定しないとアプリ保護ポリシーが適用されません。
    1. 「アプリ」 - 「アプリ構成ポリシー」 - 「+追加」をクリックします。
    2. 表示されたメニューから「マネージド デバイス」を選択します。
    3. ポリシーに名前を付けて、以下のように設定します。
      - プラットフォーム : 「iOS/iPadOS」
      - 対象アプリ : PA PEOPLE
    4. 右図の構成ポリシー設定を入力します。
  
- ④ 設定した情報をユーザに割り当てます

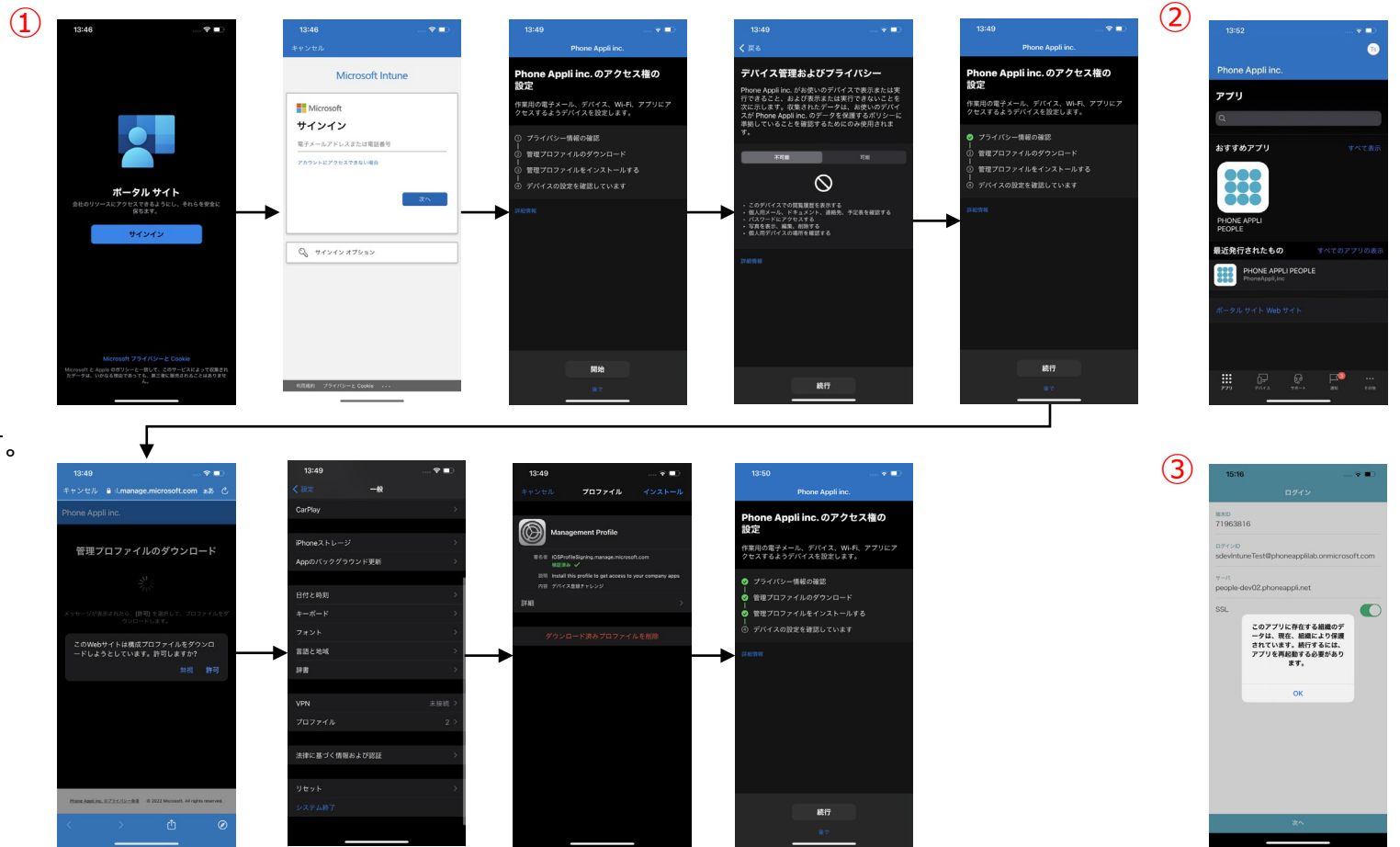
#### 構成ポリシー 設定

```
<dict>  
<key>IntuneMAMUPN</key>  
<string>{{userprincipalname}}</string>  
</dict>
```

# 2.5 アプリ保護ポリシー適用の流れ (iPhone) 2/2

## ■エンドユーザーによる端末側の初期設定

- ① 「Intune ポータル サイト」アプリをダウンロードし、有効なMSアカウントでログインし、画面の案内通りに進みます。
- ② 配信されているPA PEOPLEをインストールします。
- ③ 「OK」をタップします。  
※強制終了しない場合にはアプリ保護ポリシーの取得に失敗しているため、設定の見直しが必要です。



- ④ 再度、PA PEOPLEを起動しログインします。

※ 「Intune ポータル サイト」 にサインインするアカウントとPA PEOPLEログインアカウントが同一である必要があります。

### 3. iPhoneにて特定のアプリ保護ポリシーを ご利用の場合の設定作業



# 3.1 特定のアプリ保護ポリシーを利用されている場合 1/2

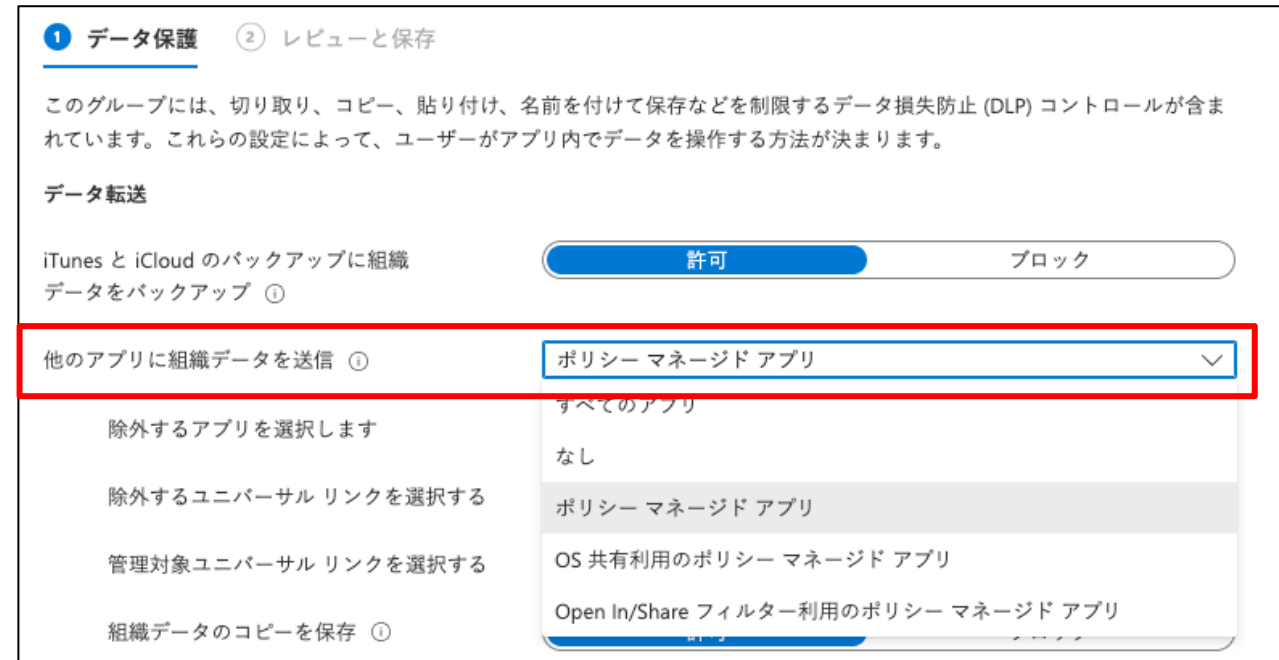
iPhone版 v.1.38.2以降のPA PEOPLE（連絡とれるくん）をIntune アプリ保護ポリシーで割り当て、且つ、下記のアプリ保護ポリシーを適用してご利用される場合は、認証時にブローカーアプリとなる「Microsoft Authenticator」のインストールが必要です。

認証時に「Microsoft Authenticator」が必要となるアプリ保護ポリシーは以下の通りです。

### 【他のアプリに組織データを送信】

- なし
- ポリシーマネージドアプリ
- OS共有利用のポリシーマネージドアプリ
- Open-In/Share フィルター利用のポリシーマネージドアプリ

※「すべてのアプリ」を選択している場合は不要です。



※Microsoft社の仕様変更により、現在該当していない設定値においても「Microsoft Authenticator」アプリが必要となる場合があります

※Microsoft Authenticatorをインストールできない場合は、次ページに記載されている除外設定をご参照ください。



# 3.1 特定のアプリ保護ポリシーを利用されている場合 2/2

ブローカーアプリ（Microsoft Authenticator）をインストールできない場合はアプリ保護ポリシーの除外設定をして利用することも可能ですが、今後Microsoft社の仕様変更により、「Microsoft Authenticator」アプリが必須となる場合があります。

※除外設定ができない場合、認証方式をMicrosoft 365 SSOからローカル認証またはSAML認証に変更してご利用いただくことも可能です。

アプリ保護ポリシーの除外設定する方法は以下の通りです。

1. Intuneのアプリ保護ポリシーから該当するポリシーを選択します。
2. 「他のアプリに組織データを送信」配下の「除外するアプリを選択します」より「選択」（右図①）をクリックします。
3. 「適用から除外されるアプリ」に、下記設定値の名前、値（右図②）を入力し「OK」（右図③）をクリックします。

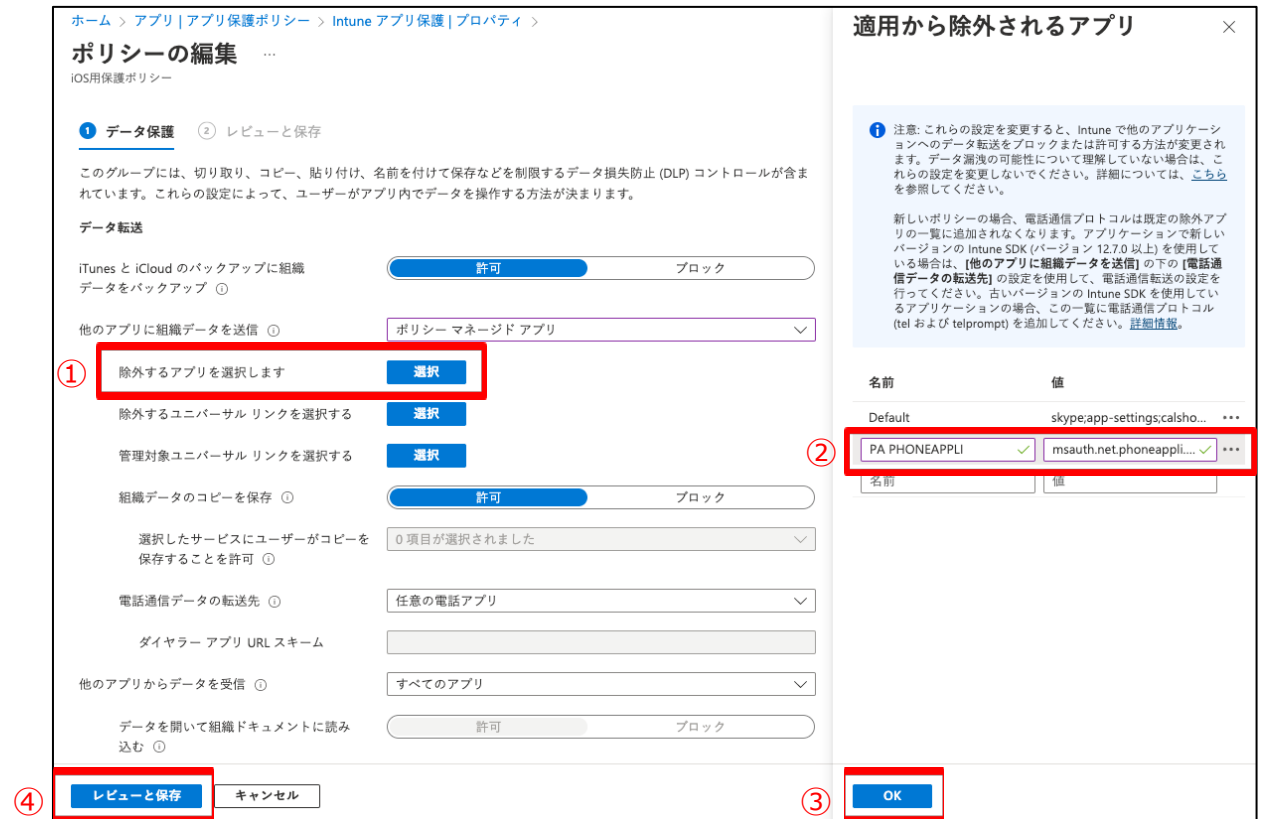
<PHONE APPLI POPLIをご利用の場合>

名前： PA PEOPLE（※任意）  
値： `msauth.net.phoneappli.people`

<連絡とれるくんをご利用の場合>

名前： RENRAKU（※任意）  
値： `msauth.net.phoneappli.renraku`

4. 「レビューと保存」（右図④）をクリックし保存します。
5. 端末の同期を行い、最新のアプリ保護ポリシーを取得します。



## 4. iPhoneにて条件付きアクセスをご利用の場合の設定作業

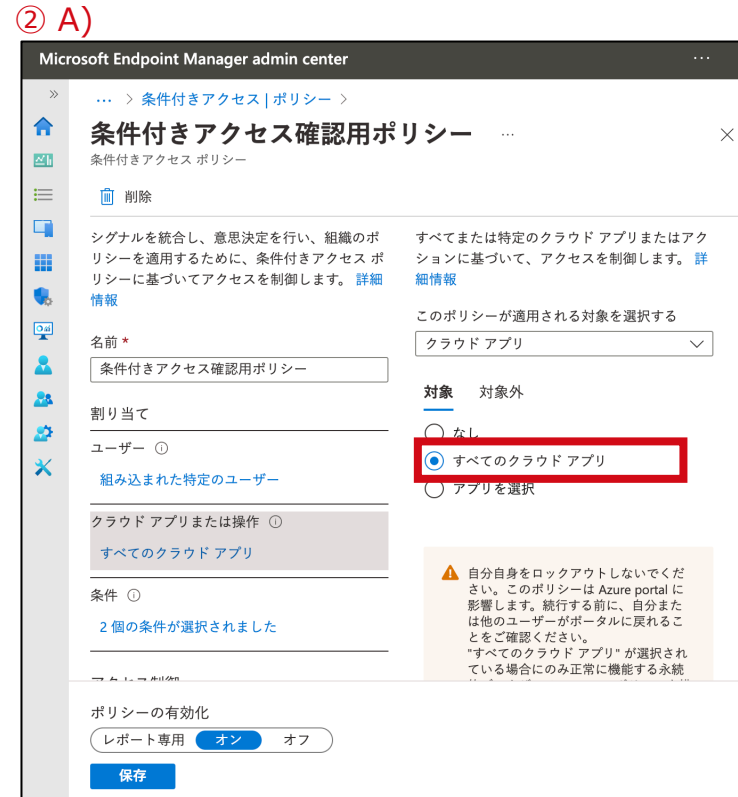
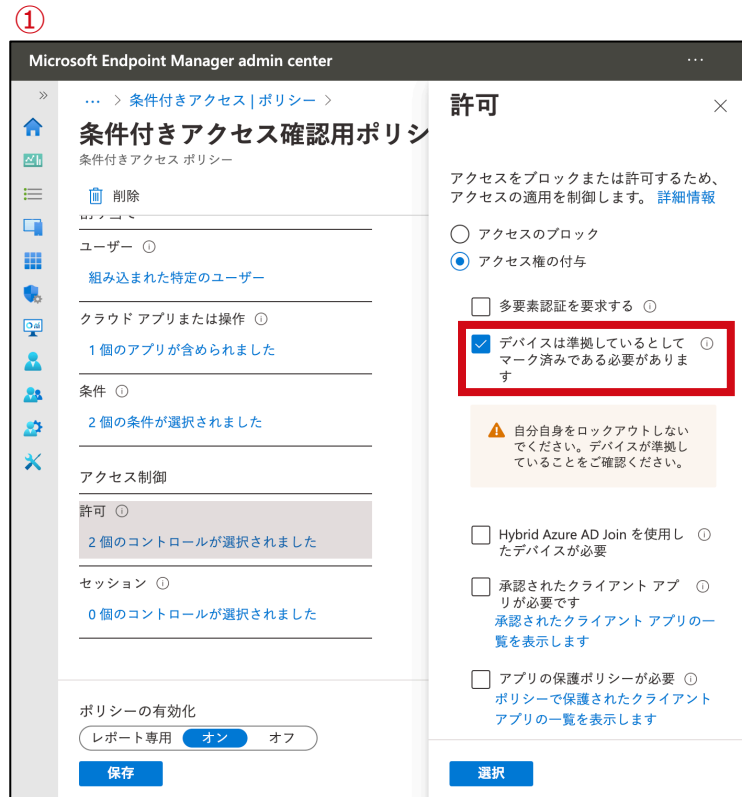


# 4.1 Azure ADで条件付きアクセスを利用されている場合

Azure ADにて条件付きアクセスを利用していて、且つ、Microsoft Intune環境下におけるiPhone版PA PEOPLE(連絡とれるくん)アプリに条件付きアクセスを適用する場合は、ブローカーアプリ「Microsoft Authenticator」アプリをインストールし、「Microsoft 365 サインイン」を実施します。

以下はIntune準拠の条件付きアクセスを利用する場合の設定例です。

- ① Azure Portal 上の条件付きアクセス設定画面にて、「デバイスは準拠しているとしてマーク済みである必要があります。」にチェックが入っていることを確認します。
- ② 以下から、条件に合わせて、手順を選択してください。
  - A. 全てのクラウドアプリに条件付きアクセスを適用する場合 → 「すべてのクラウドアプリ」を選択します。
  - B. 条件付きアクセスポリシーをPA PEOPLE(連絡とれるくん)のみに適用する場合 → 対象アプリとして「PHONE APPLI PEOPLE for Intune (連絡とれるくん for Intune)」を選択します。
- ③ 「ポリシーの有効化」が“オン”となっていることを確認し、「保存」をクリックします。



## 4.2 ブローカーアプリをインストールできない場合

企業ポリシーなど何らかの理由によりブローカーアプリをインストールできない場合は、条件付きアクセスをPA PEOPLE(連絡とれるくん)に適用できません。

ただし、条件付きアクセスの対象外として、ご利用いただくことも可能です。条件付きアクセスの対象外とする手順について説明します。

- ① 該当する条件付きポリシーを選択し、「クラウドアプリまたは操作」をクリックします。
- ② 「対象外」をクリックします。
- ③ 下記アプリを「対象外」に設定し、「ポリシーの有効化」が“オン”となっていることを確認し、「保存」をクリックします。

A) PA PEOPLE(連絡とれるくん)のMicrosoft 365シングルサインオンを利用している場合

- スマートフォン用シングルサインオンアプリ
- ブラウザ用シングルサインオンアプリ
- PHONE APPLI PEOPLE for Intune (連絡とれるくん for Intune)

B) PA PEOPLE(連絡とれるくん)のMicrosoft 365シングルサインオンを利用していない場合

- PHONE APPLI PEOPLE for Intune (連絡とれるくん for Intune)

シグナルを統合し、意思決定を行い、組織のポリシーを適用するために、条件付きアクセスポリシーに基づいてアクセスを制御します。 [詳細情報](#)

すべてまたは特定のクラウド アプリまたはアクションに基づいて、アクセスを制御します。 [詳細情報](#)

このポリシーが適用される対象を選択する

名前 \*  
条件付きアクセス確認用ポリシー

割り当て

ユーザー ①  
組み込まれた特定のユーザー ①

クラウド アプリまたは操作 ①  
すべてのクラウド アプリ 件を含む および 3 個のアプリが除外されました

条件 ①  
2 個の条件が選択されました

アクセス制御

許可 ①

このポリシーが適用される対象を選択する

クラウド アプリ

② 対象 対象外

ポリシーから除外するクラウド アプリを選択します

除外されたクラウド アプリの選択

③ ブラウザ用シングルサインオンアプリ、他 2 個

PHONE APPLI PEOPLE for Intune ...  
8b8dde6e-b378-4f50-bb65-8982ed1f...

スマ スマートフォン用シングルサイン ...  
a3186af7-6849-4aed-8b8b-2b2c10f0...

ブラ ブラウザ用シングルサインオンア ...  
894d2c27-987c-4426-ab25-b0d6ea4...



## 5. Androidでのアプリ保護ポリシーの設定の流れ

# 5.1 アプリ保護ポリシー適用の流れ（Android） 1/3

## ■ 管理者によるMS Intune管理画面の作業

- ① PA PEOPLEを「アプリ」に追加します。
  - GooglePlay上のアプリURLを登録します。
    - PA PEOPLE : <https://play.google.com/store/apps/details?id=net.phoneappli.people&hl=ja&gl=US>
    - 連絡とれるくん : <https://play.google.com/store/apps/details?id=net.phoneappli.renraku&hl=ja&gl=US>
  - 「ポータル サイトでおすすめアプリとして表示する」は「はい」を選択します。
  
- ② アプリ保護ポリシーでPA PEOPLEをカスタムアプリとして登録し、ポリシーを設定します。
  - リストにアプリが表示されなければ、パッケージ名には以下のパッケージIDを指定して追加します。
    - PA PEOPLE : net.phoneappli.people
    - 連絡とれるくん : net.phoneappli.renraku
  - ※Androidでは、アプリ構成ポリシーの「IntuneMAMUPN」の設定は不要です。
  
- ③ 設定した情報をユーザに割り当てます。

# 5.1 アプリ保護ポリシー適用の流れ (Android) 2/3

## ■エンドユーザによる端末側の初期設定

① 「Intune ポータル サイト」アプリをダウンロードし、有効なMSアカウントでログインし、画面の案内通りに進みます。



② 「機器管理アプリを有効にしますか?」の画面が表示されたら、「この機器管理アプリを有効にする」をタップし、「完了」をタップします。



※ 「Intune ポータル サイト」にサインインするアカウントとPA PEOPLEログインアカウントが同一である必要があります。

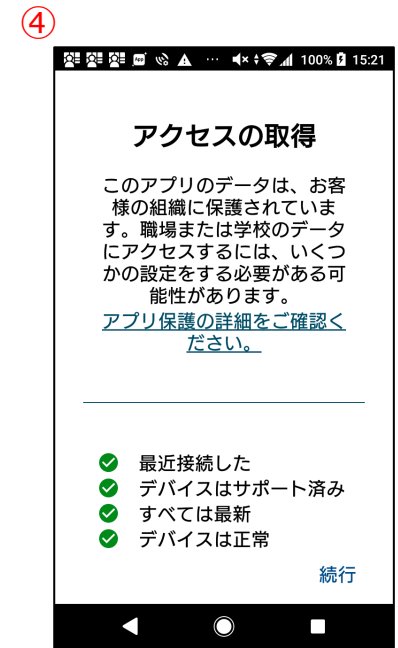
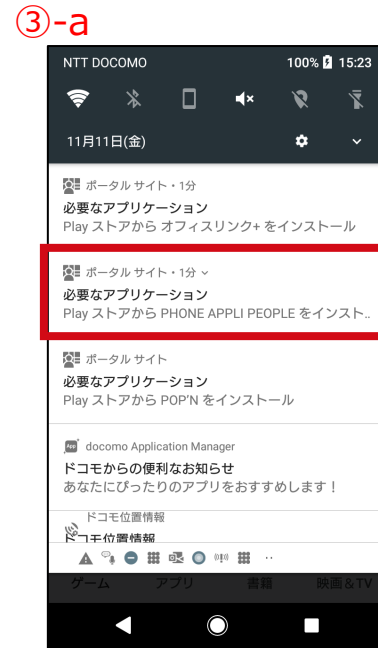


# 5.1 アプリ保護ポリシー適用の流れ (Android) 3/3

- ③ インストールを促す通知をタップして、Google PlayからPA PEOPLEをインストールします。  
(右の画面③-a、③-b)

もしくは、Google Playから直接PA PEOPLEをインストールします。  
(右の画面③-b)

※上記、どちらの方法を選択した場合でも、手順①②で行われたIntuneポータルサイトアプリの設定が終わり、PA PEOPLEのインストールが完了した時点で、PA PEOPLEにアプリ保護ポリシーが適用されます。



- ④ PA PEOPLEを起動します。  
(初回起動時に「アクセスの取得」画面が表示されるので、「続行」をタップします。)



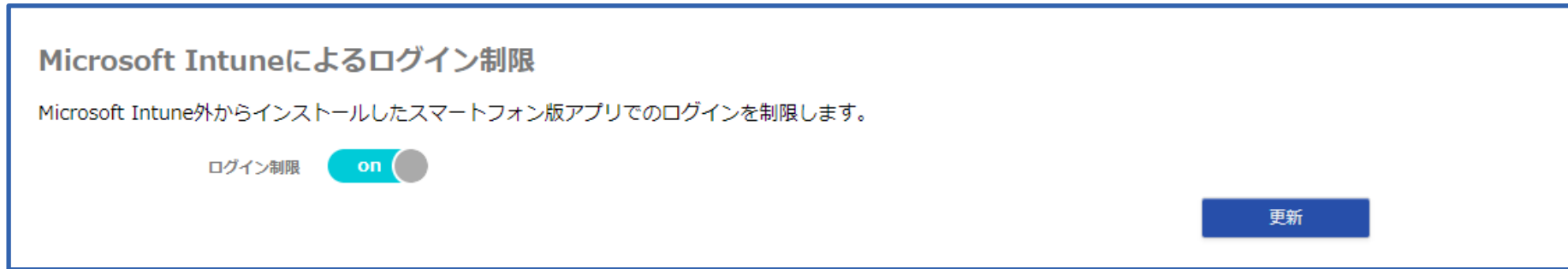


## 6. PA PEOPLEへのログイン制限について (iPhone、Android共通)

# 6.1 PA PEOPLEへのログイン制限

PA PEOPLEの管理者機能では、「MS Intune MAM」によって制御されているスマートフォン版アプリによるログインのみを許可することができます。

「ログインユーザ顔アイコン > 管理 > 企業情報 > 社名/ロゴ」画面  
「Microsoft Intuneによるログイン制限」



「MS Intune MAM」による制御有無と当該管理機能によるON/OFFの組み合わせによるログイン可否は以下の通りです。

| MS Intune MAM<br>による制御 | ログイン制御 |       | 備考 |
|------------------------|--------|-------|----|
|                        | ON     | OFF   |    |
| 有                      | ログイン可  | ログイン可 |    |
| 無                      | ログイン不可 | ログイン可 |    |

※ PCブラウザ版PA PEOPLEはこの機能の影響を受けず、常にログイン可能です。



## 7. よくある質問

# 7.1 よくある質問

Q : MS Intune対応によって、アプリの設定値を自動入力することができますか？

A : できます。アプリの構成ポリシーを利用することで対応しています。

Q : アプリ保護ポリシー適用によって〇〇〇〇の機能が使えなくなりました。使えるようにできますか？

A : MS Intune MAMの機能によって制限されているため、PA PEOPLE側では対応できません。  
アプリ保護ポリシーの関連する設定箇所を変更し、動作することをご確認ください。

Q : Intune ポータルサイトからダウンロードしたPA PEOPLEでログインしようとする時、「Intune ポータル サイトのアカウントと一致していません。ログインIDを正しく入力してください。」と表示され、ログインできません。これはどのような状態で、どうすればログインできますか？

A : PA PEOPLEでは第三者による、アプリからの不正アクセスを制限するため、MS Intuneで制御されたIntune ポータルサイトにサインインしたアカウントとの整合性をチェックしています。  
Intune ポータルサイトのサインインアカウントとPEOPLEのログインIDが一致するようにユーザを作成してください。

Q : 以前あるユーザが利用していたiPhone端末を別ユーザで使おうとしたところ、PA PEOPLEにログインできませんでした。これはどのような状態で、どうすればログインできますか？

A : M365の認証情報が端末に残っているため発生している可能性があります。以下の手順を実施し、解消しないかお試しください。

## パターン1

1. Intune ポータルサイトに別のユーザとしてサインインする
2. アプリ起動時に複数のM365アカウントを検知した際に表示される画面で実際に使用するアカウントを選択する
3. 上記1でIntune ポータルサイトにサインインしたアカウントで、PA PEOPLEにログイン

## パターン2(パターン1で解消されない場合)

1. (Intune ポータルサイトにサインインしている情報が残っている場合は)Intune ポータルサイトからサインアウトする
2. 「一般 > 設定 > プロファイルとデバイス管理」からIntune ポータルサイトのプロファイルを削除する
3. (上記2で解決しない場合)、「設定 > 一般 > リセット > 全てのコンテンツと設定を消去」を選択する
4. その後、Intune ポータルサイトにサインインしなおし、そのアカウントで、PA PEOPLEにログイン



「働く」を変える。「生きかた」が変わる。

# PHONE APPLI

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