PHONE APPLI PEOPLE
MS365 SSOのための設定手順

2023年10月

PHONE APPLI

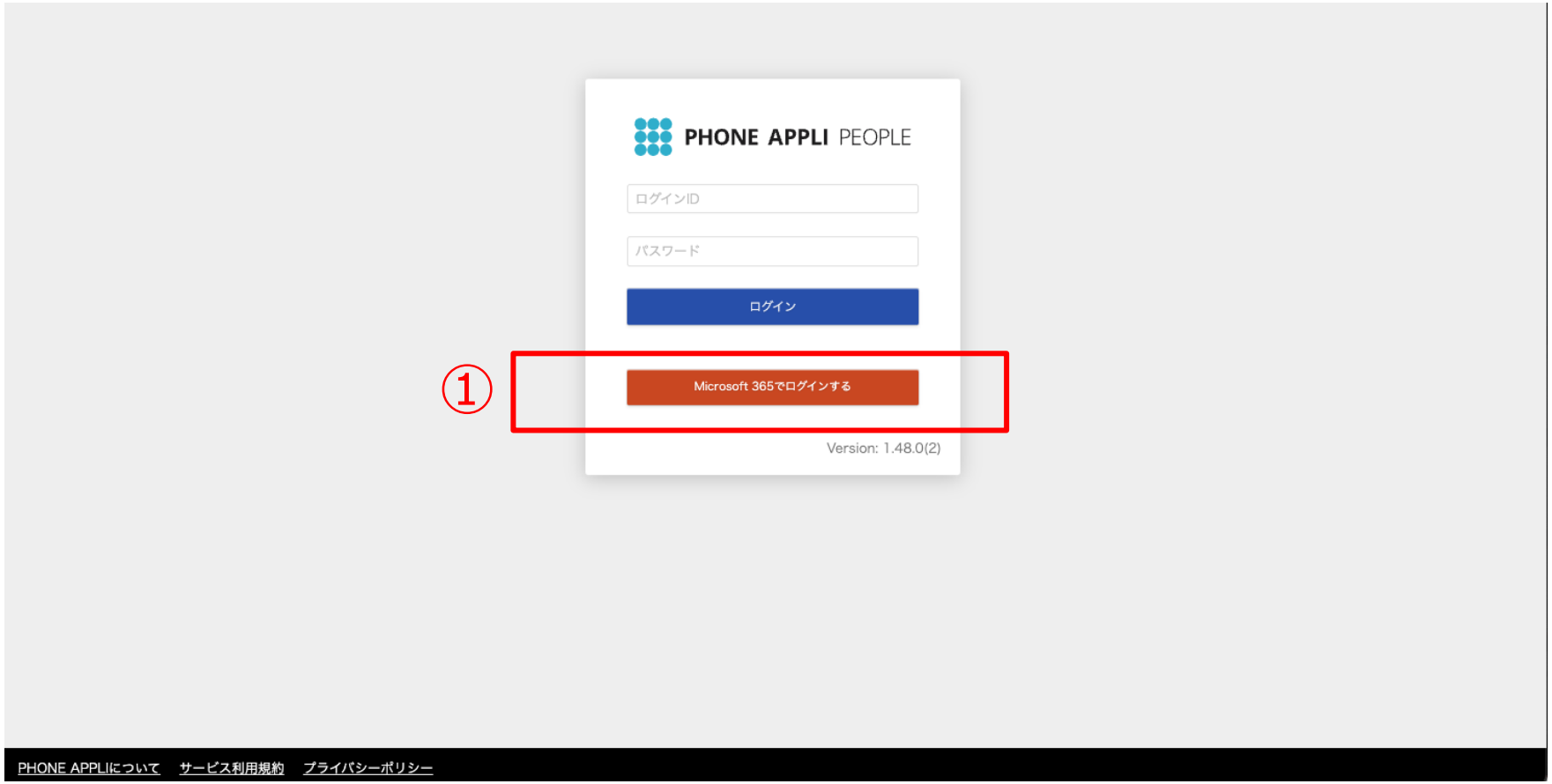
更新履歴

日付	内容
2018/04/13	初版作成
2019/01/08	追記
2019/05/15	更新
2019/06/18	更新
2020/04/18	更新
2020/04/21	更新
2020/05/28	画面の更新
2020/11/02	更新
2021/12/22	追記
2022/09/08	追記
2022/11/01	追記
2022/12/21	追記
2023/10/27	更新

目次

1. PHONE APPLI PEOPLEでSSOログインを行う（ブラウザ）

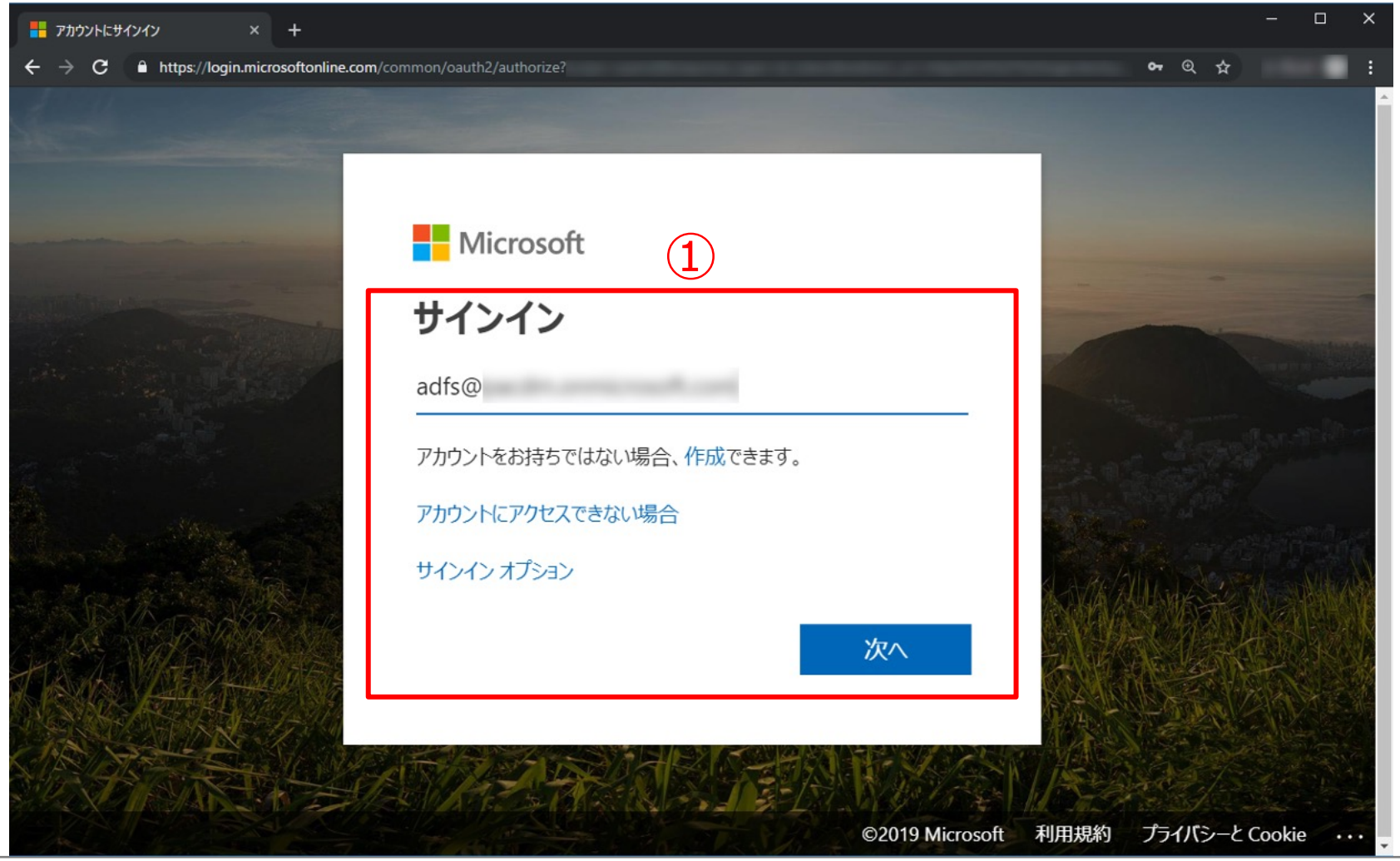
- Microsoft Entra IDの管理者アカウントにてPHONE APPLI PEOPLEのSSO認証を行います。
- 「Microsoft 365 でログインする」ボタン(下図①）をクリックします。



1. PHONE APPLI PEOPLEでSSOログインを行う（ブラウザ）

Microsoftのサインイン画面（下図①）が表示されます。

Microsoftのサインイン画面で、アカウント情報を入力してログインします。



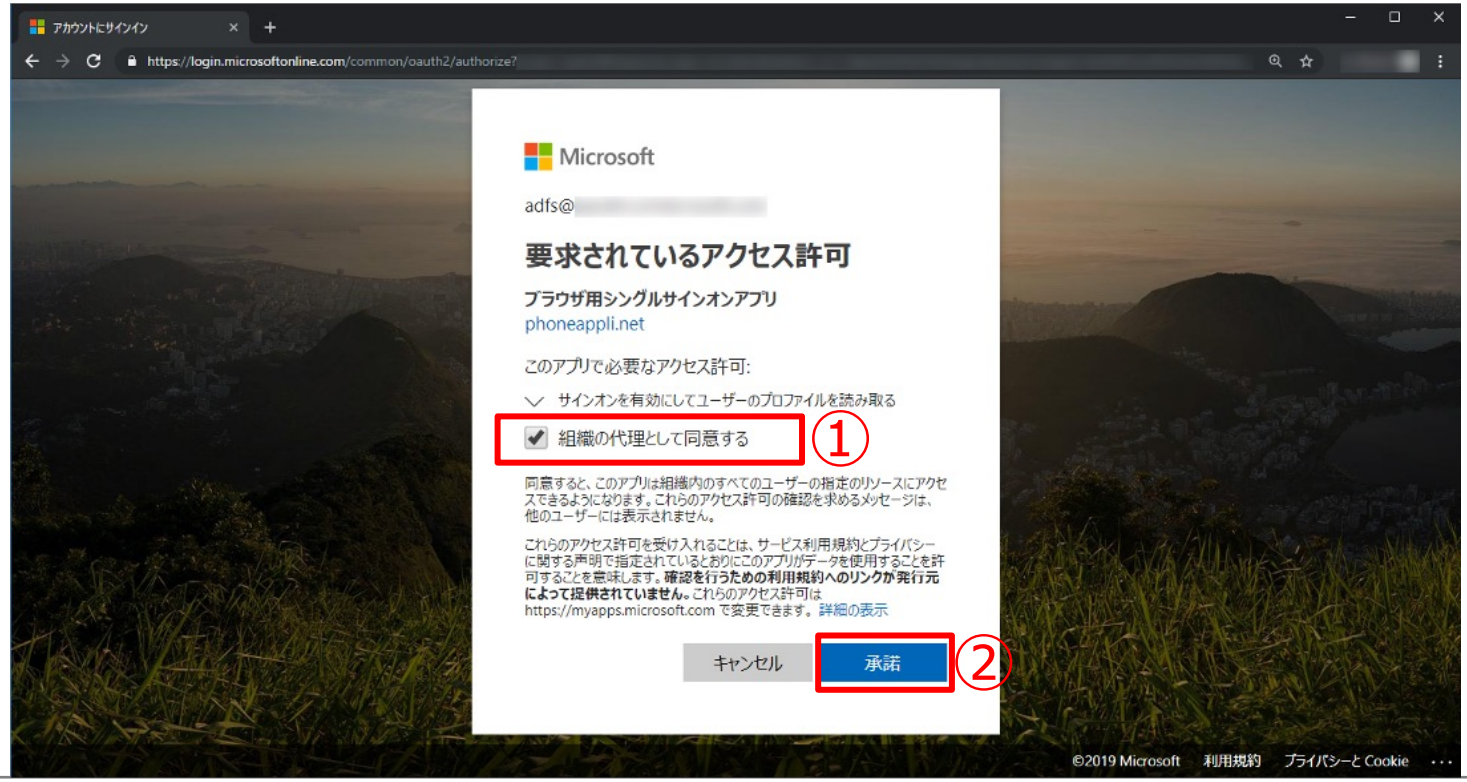
1. PHONE APPLI PEOPLEでSSOログインを行う（ブラウザ）

最初にログインする場合に限り、アプリの許可を求められるので
「組織の代理として同意する」にチェックを入れ、「承諾」をすることでWeb画面でのSSOが利用可能になります。
（下図①、②）

※事前にPHONE APPLI PEOPLEでMicrosoft Entra IDの管理者アカウントと同じユーザアカウントを作成してください。

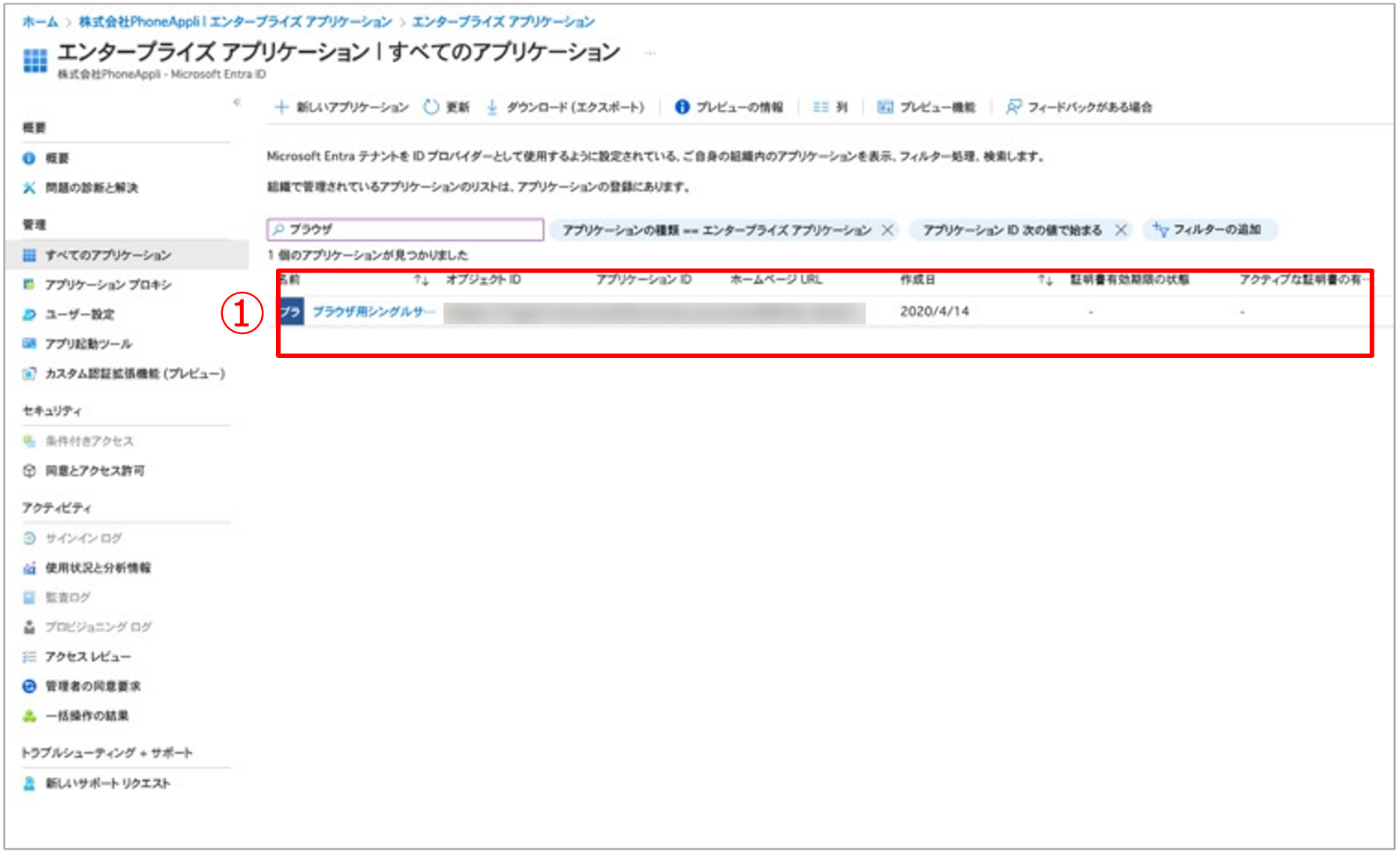
※PHONE APPLI PEOPLEのログインIDとMicrosoft Entra IDのUPNが一致しないとエラーとなります。

※2回目以降は、この画面は表示されません。



1. PHONE APPLI PEOPLEでSSOログインを行う（ブラウザ）

利用を承諾したアプリはMicrosoft Entra ID ＞エンタープライズアプリケーションに追加されます。（下図①）



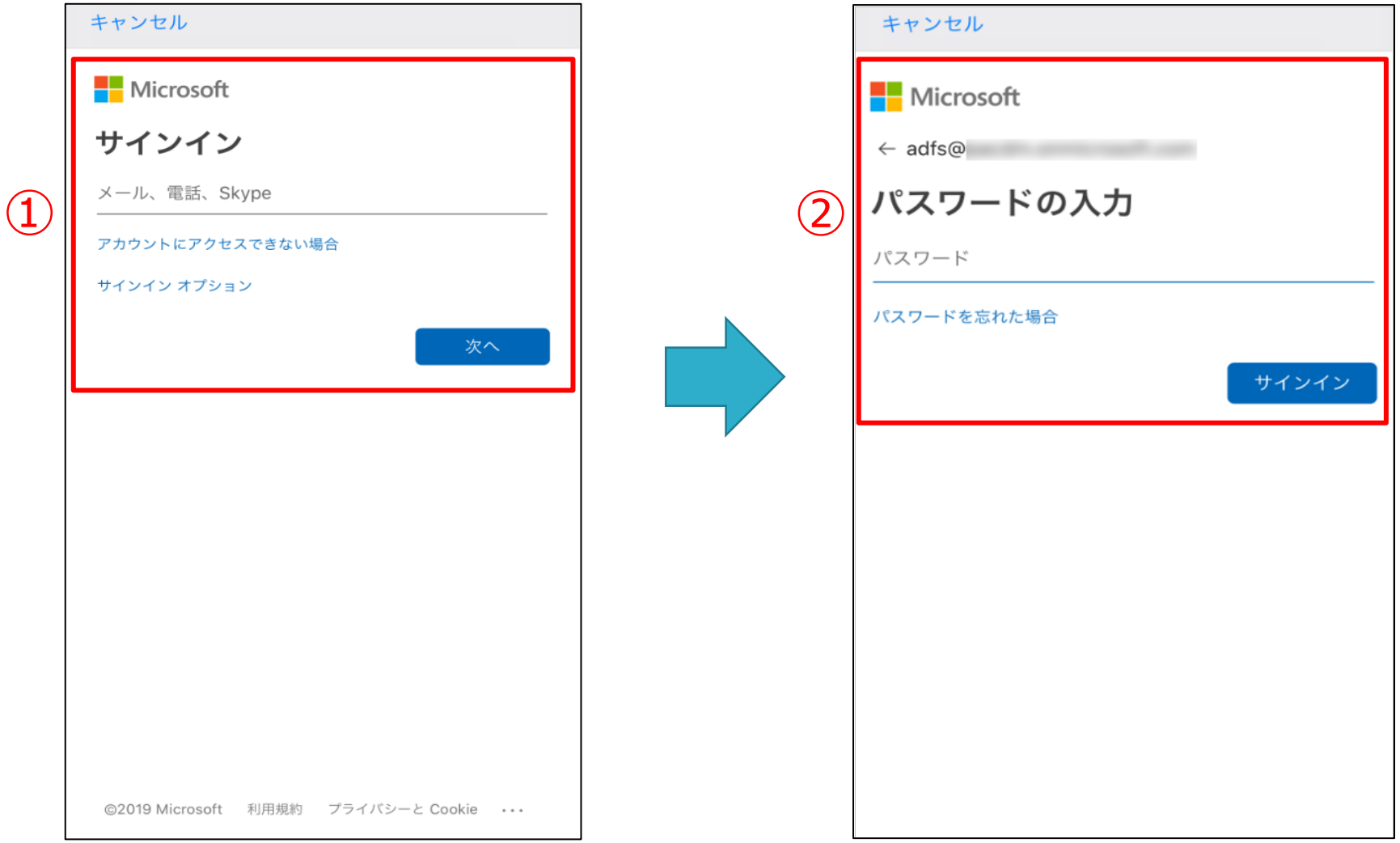
2. PHONE APPLI PEOPLEでSSOログインを行う（スマートフォン）

Microsoft Entra IDの管理者アカウントにてPHONE APPLI PEOPLEのSSO認証を行います。
「ログインID」、「サーバ」の情報を入力して「次へ」（下図①②）をタップし、
「Microsoft 365 でログインする」ボタン（下図③）をタップするとSSO用のログイン画面に遷移します。
最後に「ログイン」（下図④）ボタンをタップします。

※クライアント証明書を使用している場合は、「5.クライアント証明書を使用している場合（iPhoneのみ）」から手順を実施してください。

2. PHONE APPLI PEOPLEでSSOログインを行う（スマートフォン）

Microsoftのサインイン画面（下図①、②）が表示されるので、アカウント情報を入力してログインします。



2. PHONE APPLI PEOPLEでSSOログインを行う（スマートフォン）

最初にログインする場合に限り、アクセス許可の同意及びアプリの許可を求められるので「組織の代理として同意する」にチェックを入れ、「承諾」（下図①、②）をすることでスマートフォンでのSSOが利用可能になります。

※Web画面でのSSO利用の権限も使用するため、この時点で「ブラウザ用シングルサインオンアプリ」が同ドメインの任意のユーザによって承諾されている必要があります。

※2回目以降は、この画面は表示されません。

2. PHONE APPLI PEOPLEでSSOログインを行う（スマートフォン）

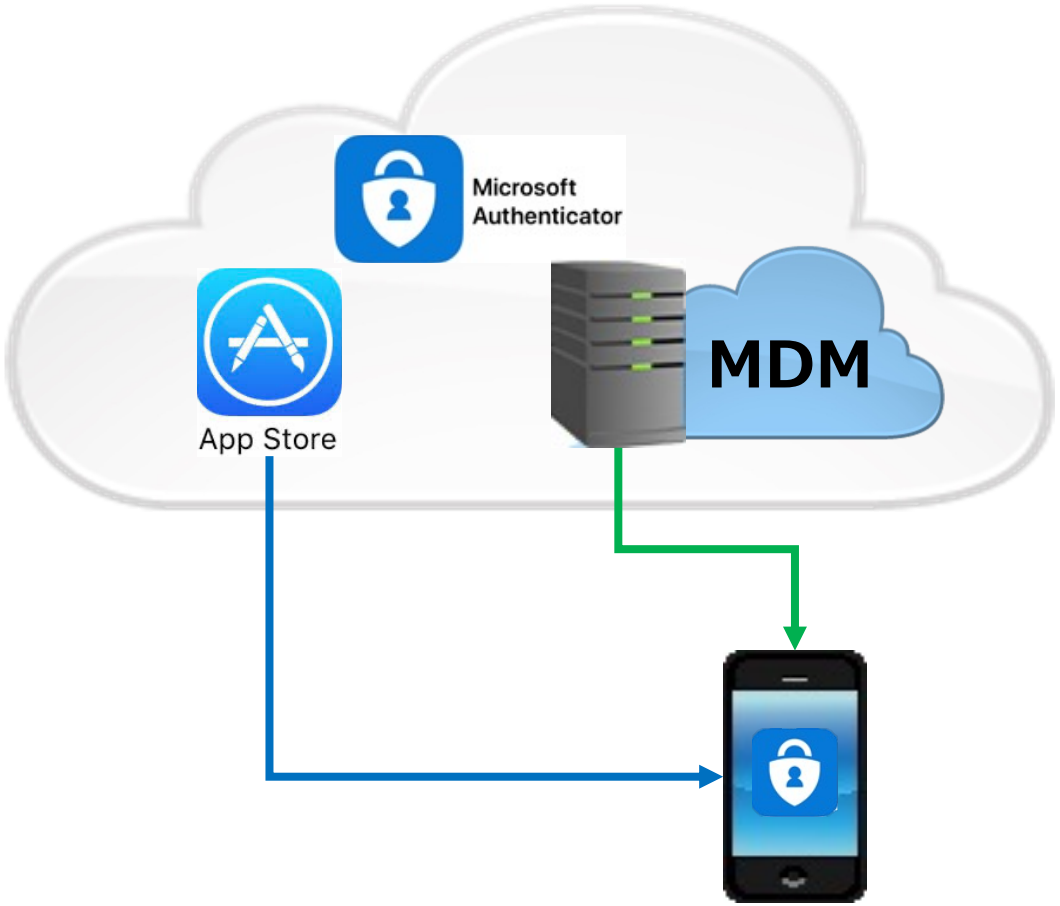
利用を承諾したアプリはMicrosoft Entra ID ＞エンタープライズアプリケーションに追加されます。（下図①）

3.　クライアント証明書をご利用されている場合（iPhoneのみ）

iPhoneに「Microsoft Authenticator」アプリをインストールします。

※本手順はクライアント証明書がインストールされている前提となります。

※本資料にはクライアント証明書をインストールする手順は含まれておりません。



※インストール後の操作は不要です。

3.　クライアント証明書をご利用されている場合（iPhoneのみ）

Microsoft Entra IDの管理者アカウントにてPHONE APPLI PEOPLEのSSO認証を行います。

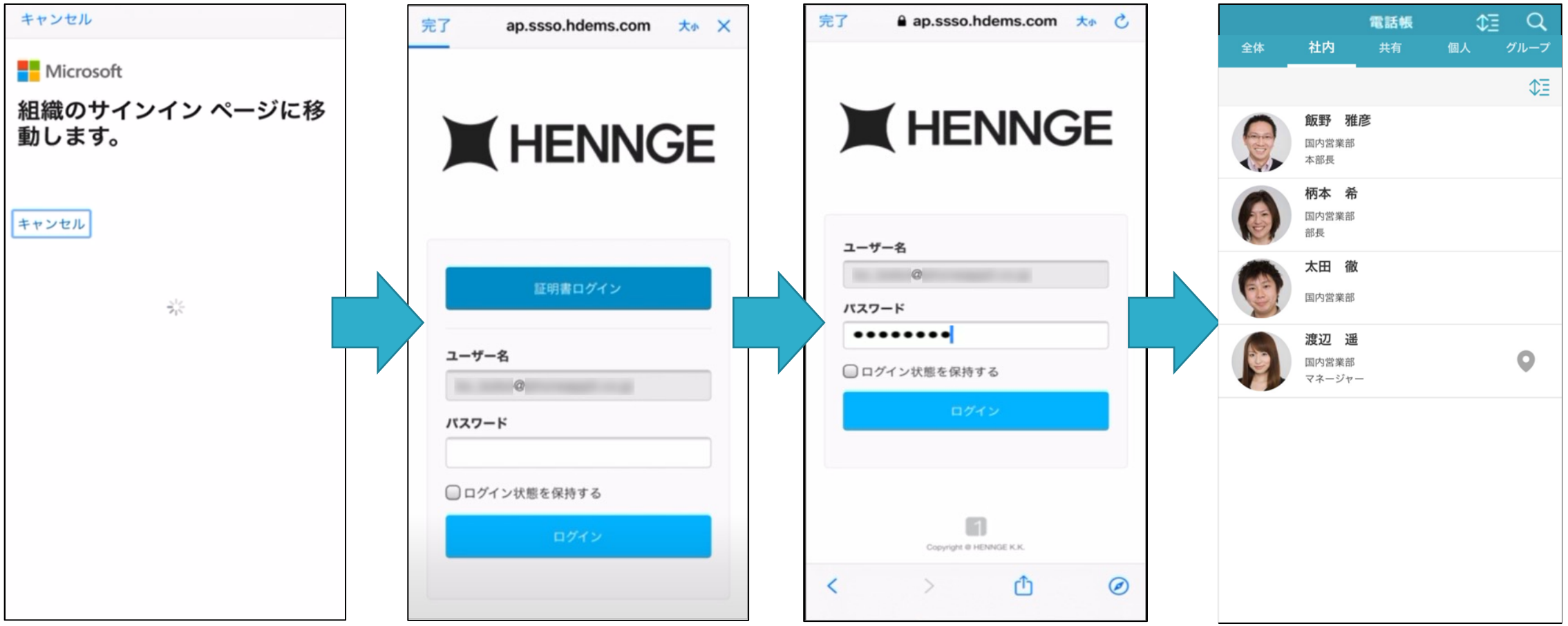
「ログインID」、「サーバ」の情報を入力して「次へ」（下図①②）をタップし、

「Microsoft 365 でログインする」ボタン（下図③）をタップするとSSO用のログイン画面に遷移します。

その後「ログイン」（下図④）ボタンをタップします。

3.　クライアント証明書をご利用されている場合（iPhoneのみ）

組織のサインイン画面に遷移し、証明書ログインからパスワードを入力することでPEOPLEにログインできます。
※以下は、HENNGE Oneの例です。



3.　クライアント証明書をご利用されている場合（iPhoneのみ）

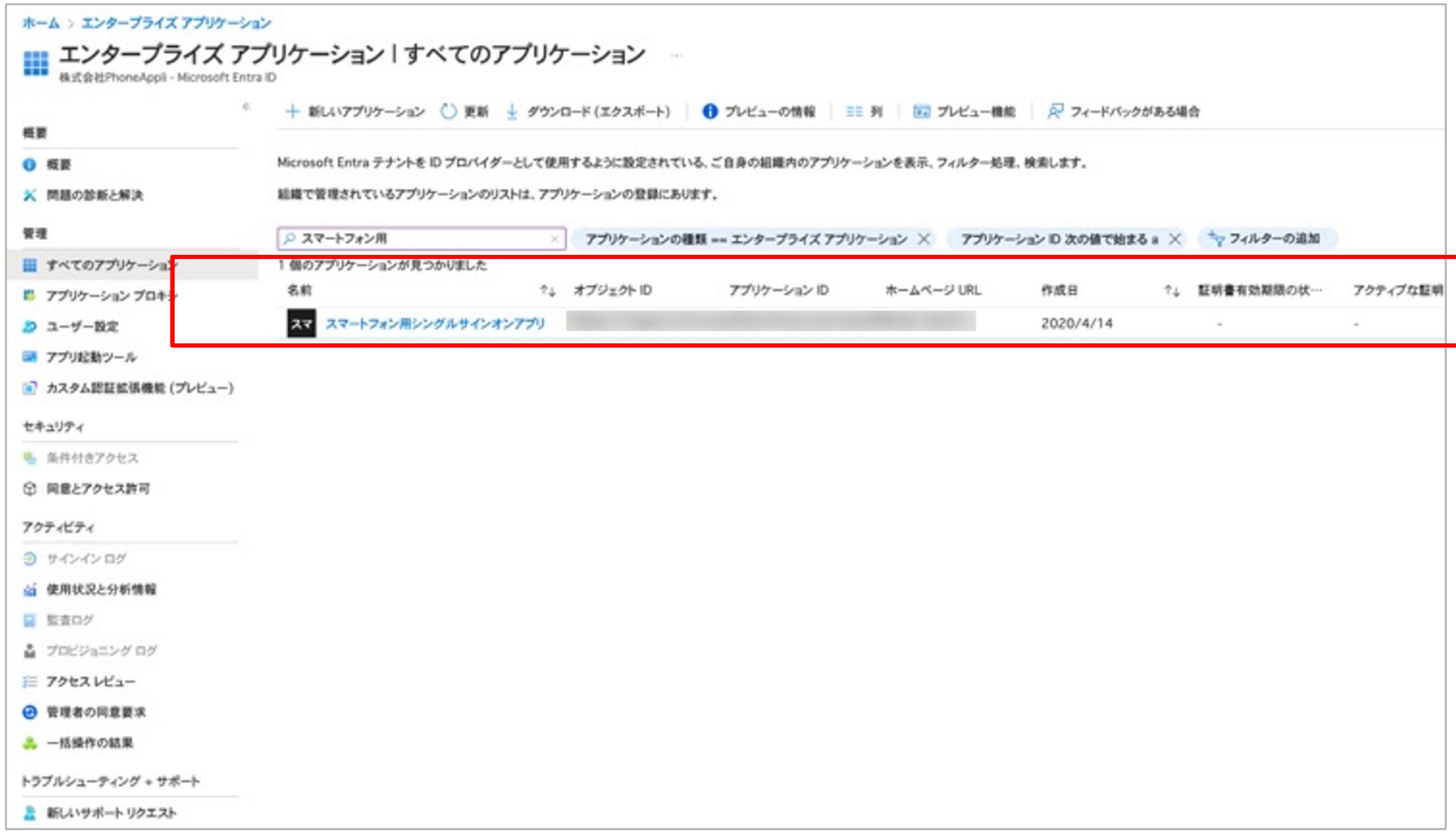
最初にログインする場合に限り、アクセス許可の同意及びアプリの許可を求められるので「組織の代理として同意する」にチェックを入れ、「承諾」（下図①、②）をすることでスマートフォンでのSSOが利用可能になります。

※Web画面でのSSO利用の権限も使用するため、この時点で「ブラウザ用シングルサインオンアプリ」が同ドメインの任意のユーザによって承諾されている必要があります。

※2回目以降は、この画面は表示されません。

3. クライアント証明書をご利用されている場合（iPhoneのみ）

利用を承諾したアプリはMicrosoft Entra ID ＞エンタープライズアプリケーションに追加されます。（下図①）



3.　クライアント証明書をご利用されている場合（iPhoneのみ）

PHONE APPLI PEOPLEへのログインが完了すると「Microsoft Authenticator」アプリに、アカウント情報等が追記されます。

4.　Azure ADで条件付きアクセスをご利用されている場合（iPhone、Android）

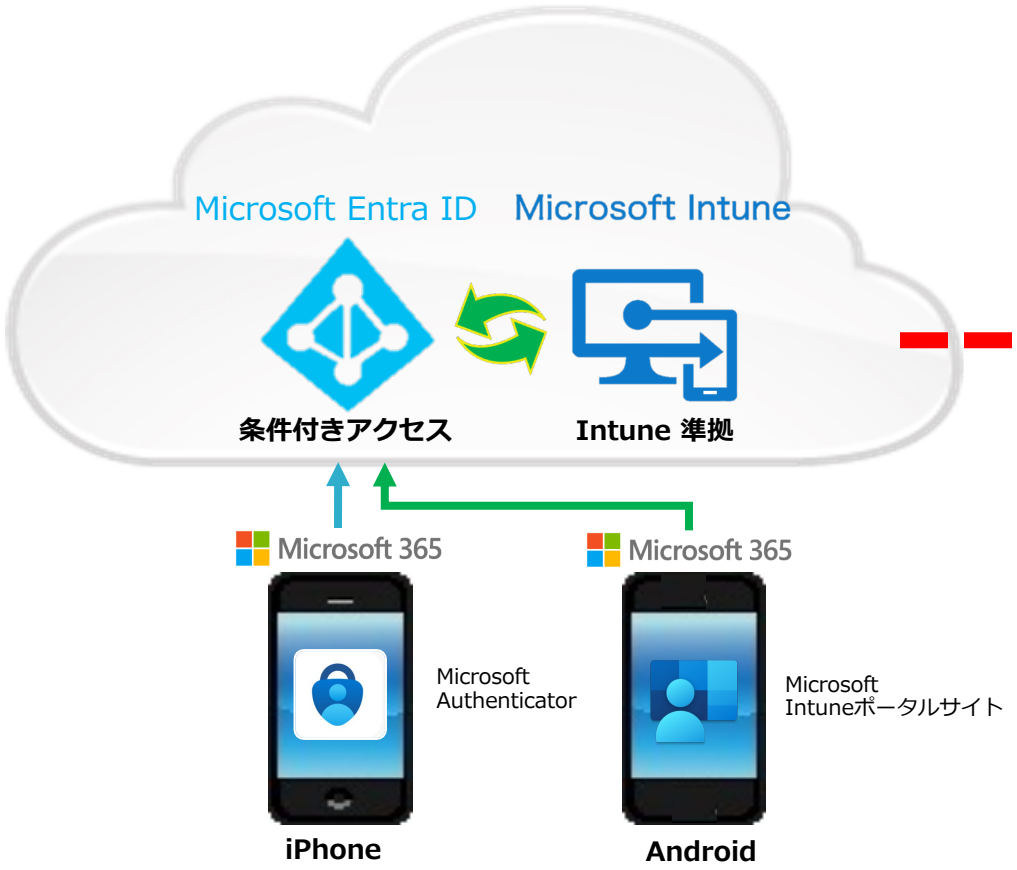
該当する下記のブローカーアプリをインストールし、「Microsoft 365 ログイン」を実施します。

・iPhoneでは「Microsoft Authenticator」アプリをインストールします。

・Androidでは「Microsoft Intune ポータル サイト」アプリをインストールします。（※Intune準拠がされている場合は手順不要）

※右下図の赤枠にある条件付きアクセスのアクセス制御（Intune準拠）をご利用される場合に上記アプリのインストールが必要となります。

※SAML認証では条件付きアクセスのアクセス制御（Intune準拠）の対応はしていないため、サポート対象外となります。



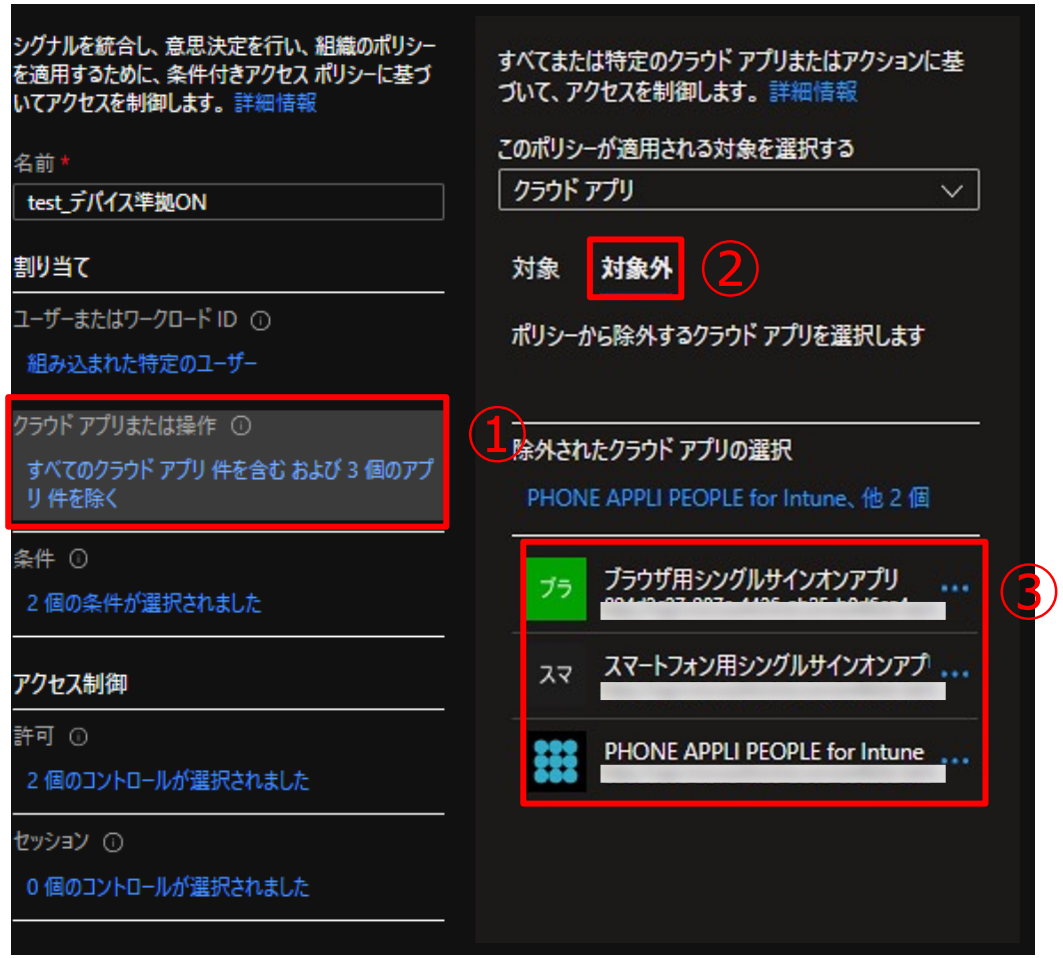
4. Microsoft Entra IDで条件付きアクセスをご利用されている場合（iPhone、Android）

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で除外設定をすることも可能です。

※ブラウザとスマートフォンで初回ログイン後、エンタープライズアプリケーション内に下記アプリを作成している必要があります。

※iPhoneとAndroidで条件付きポリシーを分けている場合は、それぞれのポリシーで除外設定を実施してください。

※iOS版アプリでv.1.38.2以降のバージョンをご利用されている場合は「PHONE APPLI PEOPLE for Intune（連絡とれるくん for Intune)」の除外設定が必要です。



・条件付きアクセスから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（左図①）をクリックします。

・対象外（左図②）をクリックします。

・下記のエンタープライズアプリケーション（左図③）を
対象外に設定して保存します。

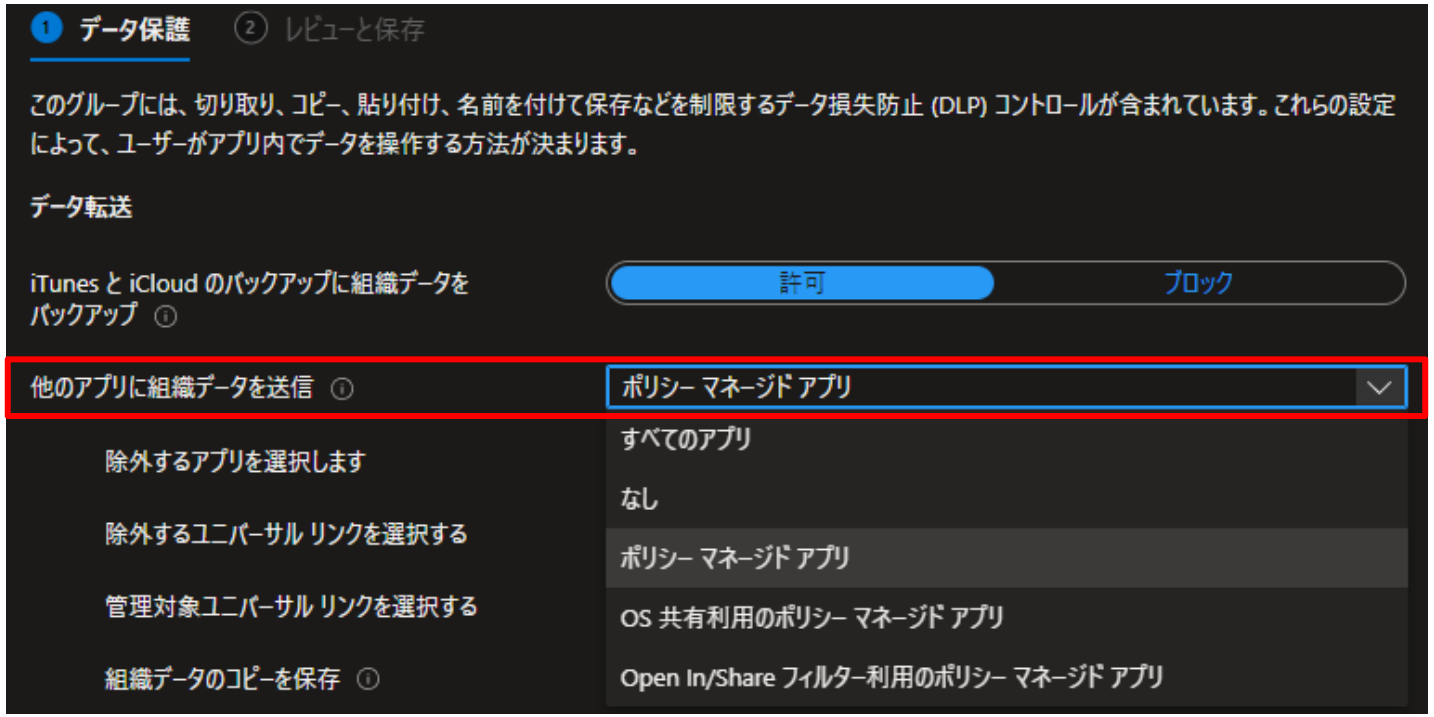
- スマートフォン用シングルサインオンアプリ
- ブラウザ用シングルサインオンアプリ
- PHONE APPLI PEOPLE for Intune（連絡とれるくん for Intune）

アプリの作成手順は「PHONE APPLI PEOPLE_MS Intune MAM設定手順.pdf」をご参照ください。

※ブローカーアプリを利用せず、Intune 保護ポリシーをアプリに割り当てる場合は
次ページの「5.Intune アプリ保護ポリシーをご利用になる場合（iPhoneのみ）」
を必ずご参照ください。

5. Intune アプリ保護ポリシーをご利用になる場合（iPhoneのみ）

PHONE APPLI PEOPLE（iOS版アプリ v.1.38.2以降）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。



「Microsoft Authenticator」アプリが必要となる場合があります

以下の保護ポリシー設定がされている場合は、
認証時に「Microsoft Authenticator」が必要となります。

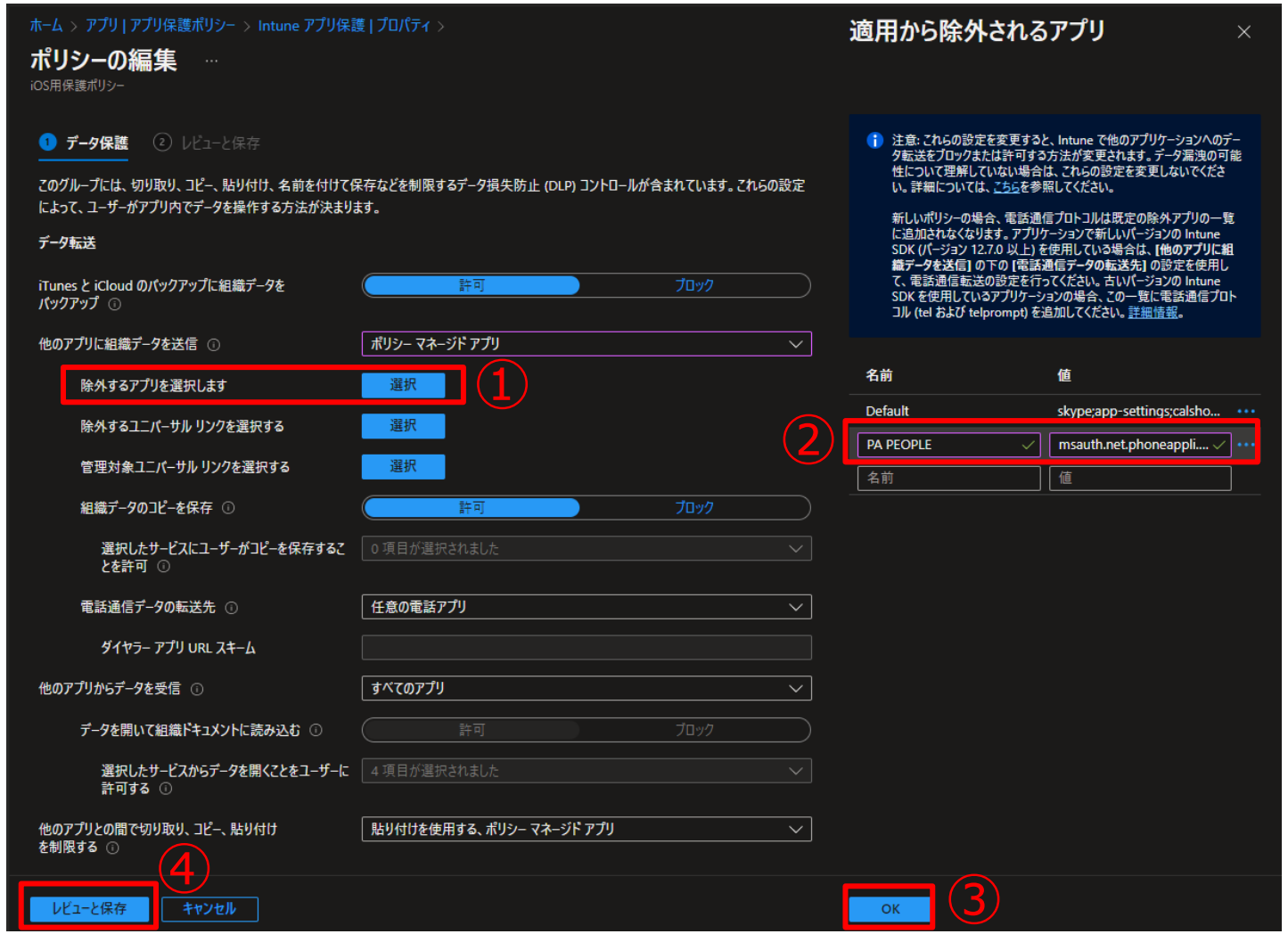
【他のアプリに組織データを送信】
・なし
・ポリシーマネージドアプリ
・OS共有利用のポリシーマネージドアプリ
・Open-In/Share フィルター利用のポリシーマネージドアプリ
※「すべてのアプリ」を選択している場合は不要です。

※Microsoft 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。

5. Intune アプリ保護ポリシーをご利用になる場合（iPhoneのみ）

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。



・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、「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」（左図①）をクリックします。

・適用から除外されるアプリより、下記設定値の名前、値（左図②）を入力し「OK」（左図③）をクリックします。

＜PHONE APPLI POPLE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

・レビューと保存（左図④）をクリックし保存します。

・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。

「働く」を変える。「生きかた」が変わる。

PHONE APPLI

info@phoneappli.net