

# PHONE APPLI PEOPLE Workspace ONE SAML認証の設定

2022年 8月

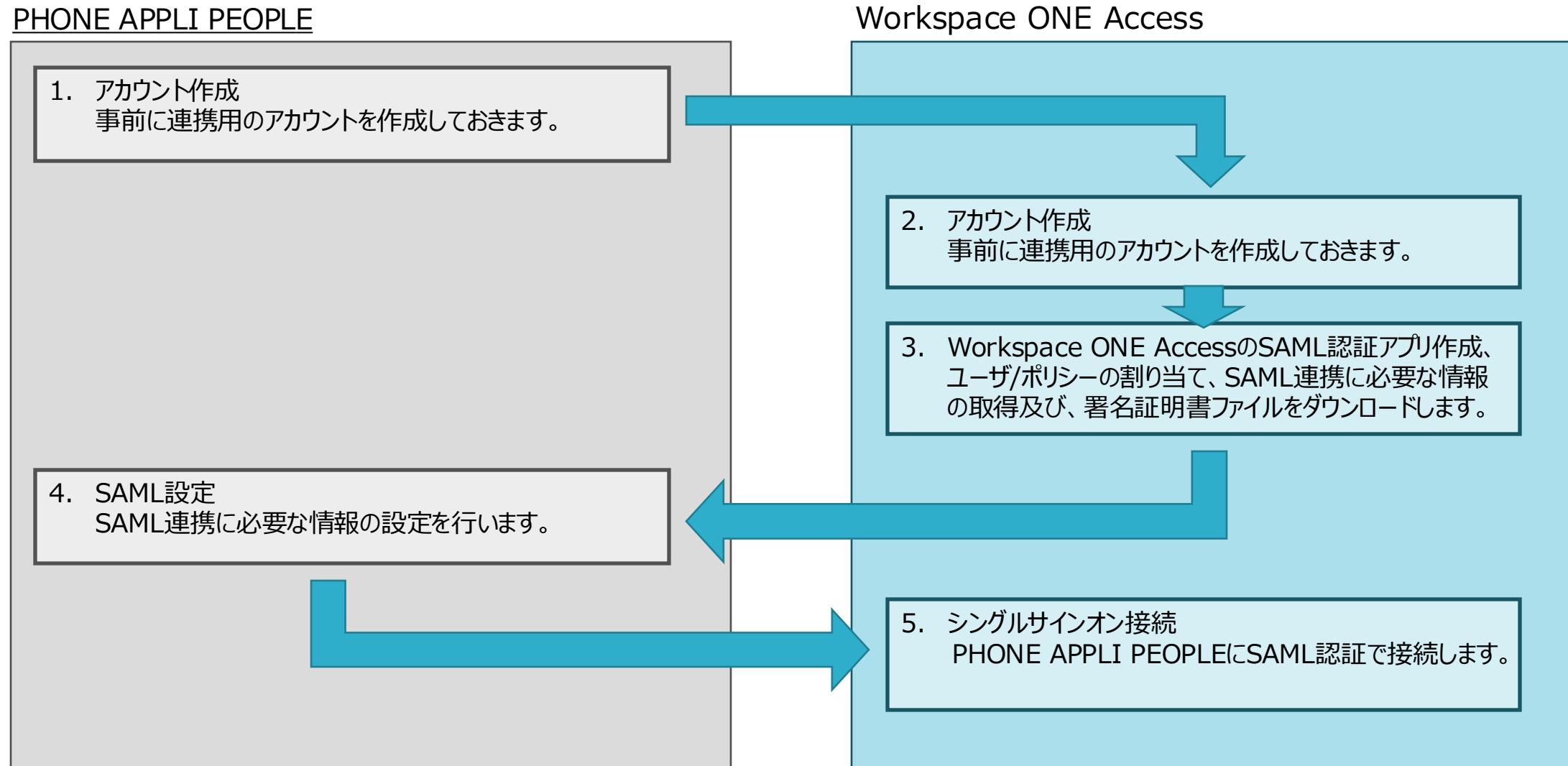
PHONE APPLI

# 目次

1. SSO設定の流れ
2. 【Workspace ONE Access】 SAML認証アプリ作成
3. 【Workspace ONE Access】 SAML認証アプリ ユーザ割り当て
4. 【Workspace ONE Access】 SAML認証アプリ ポリシー割り当て
5. 【Workspace ONE Access】 SAML設定値確認、署名証明書のダウンロード
6. 【PHONE APPLI PEOPLE】 SAML設定
7. 【Workspace ONE】 モバイルSSOの利用について

# 1. SSO設定の流れ

Workspace ONE AccessとのSSOに必要な流れは以下の通りとなります。本書では3. 4. の手順を記載しています。



# Workspace ONE Access SAML認証アプリ作成

## 2. 【Workspace ONE Access】SAML認証アプリ作成

- ① 管理画面の「カタログ」をクリックします。
- ② 「新規」をクリックします。



## 2. 【Workspace ONE Access】 SAML認証アプリ作成

③ 定義の「名前」にアプリ名を入力します。

④ 「次へ」をクリックします。

新規 SaaS アプリケーション

×

1 定義

2 構成

3 アクセス ポリシー

4 サマリ

定義

名前 \* ①

PhoneAppli

説明 ①

アイコン ①

ファイルを選択...

キャンセル

次へ ④

## 2. 【Workspace ONE Access】 SAML認証アプリ作成

- ⑤ 2構成の「認証タイプ」でSAML 2.0を選択し、「構成」で手動にチェックを入れます。
- ⑥、⑦に同じURLとして、<https://<お客様環境URL>/front/saml/acs>を入力します。
- ⑧アプリケーションIDとして、任意の値を入力します。⑨「次へ」をクリックします。

新規 SaaS アプリケーション

1 定義  
2 構成  
3 アクセス ポリシー  
4 サマリ

シングル サインオン

認証タイプ \*①  
SAML 2.0  
構成 \*①  
 URL/XML  手動  
⑤

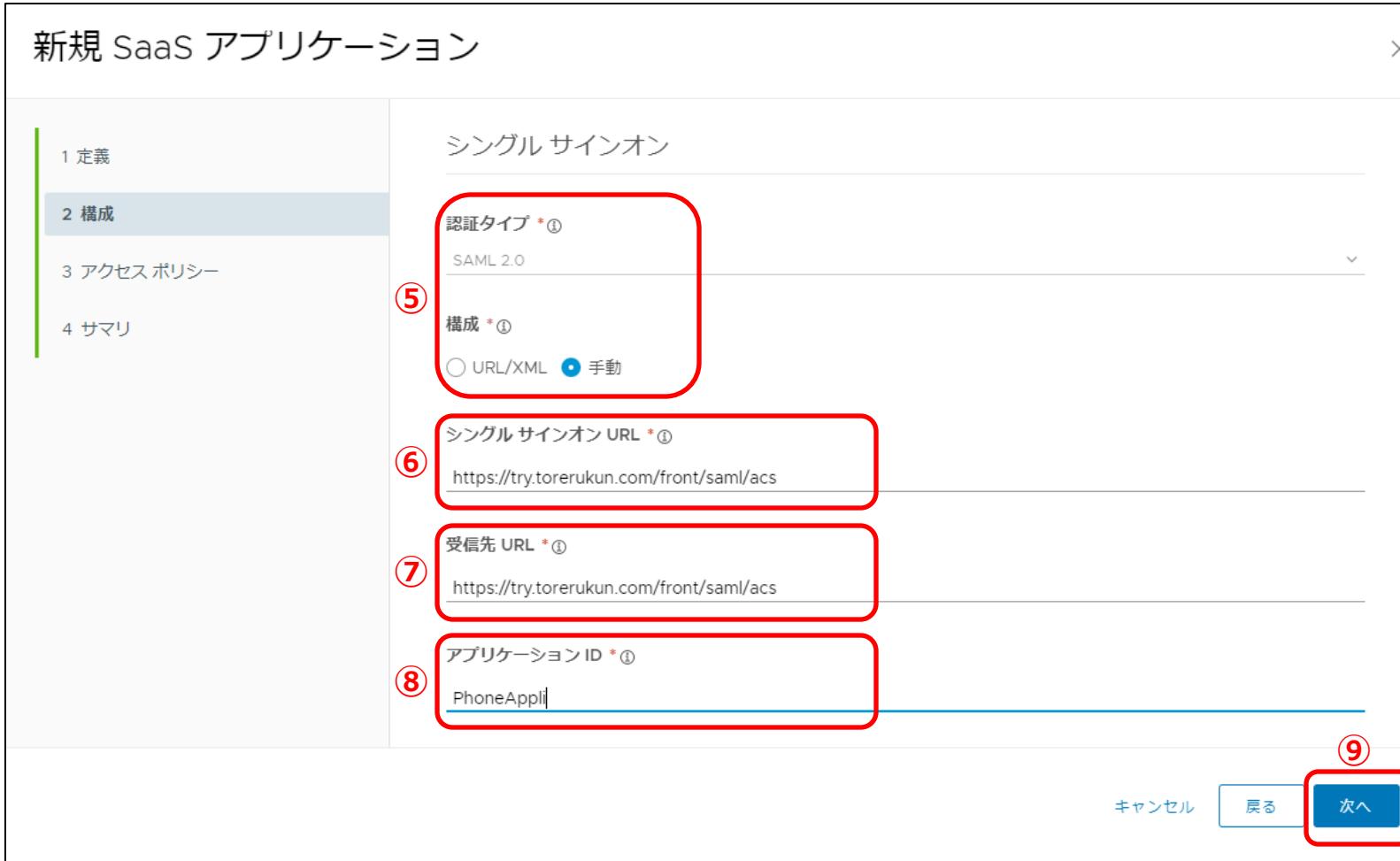
シングル サインオン URL \*①  
https://try.torerukun.com/front/saml/acs  
⑥

受信先 URL \*①  
https://try.torerukun.com/front/saml/acs  
⑦

アプリケーション ID \*①  
PhoneAppli  
⑧

⑨

キャンセル 戻る 次へ



⑥⑦のお客様環境URLはPHONE APPLI PEOPLEのテナントURLになります。

URLが<https://XX.phoneappli.net>の場合、設定値として以下を登録します。

＜シングルサインオン URL＞

<https://XX.phoneappli.net>/front/saml/acs

＜受信先 URL＞

<https://XX.phoneappli.net>/front/saml/acs

⑧の値（アプリケーションID）はWorkspace ONEとPHONE APPLI PEOPLEで同じ値を設定する必要があります。

※PHONE APPLI PEOPLEでは、「SPエンティティID」に同じ値を登録します。

## 2. 【Workspace ONE Access】 SAML認証アプリ作成

- ⑩ 3 アクセスポリシーで既存のポリシーを選択し、4 サマリで入力値に問題が無いことを確認します。
- ⑪ 「保存して割り当て」をクリックします。※次項目の「3. 【Workspace ONE】 SAML認証アプリ ユーザ割り当て」へ続きます。



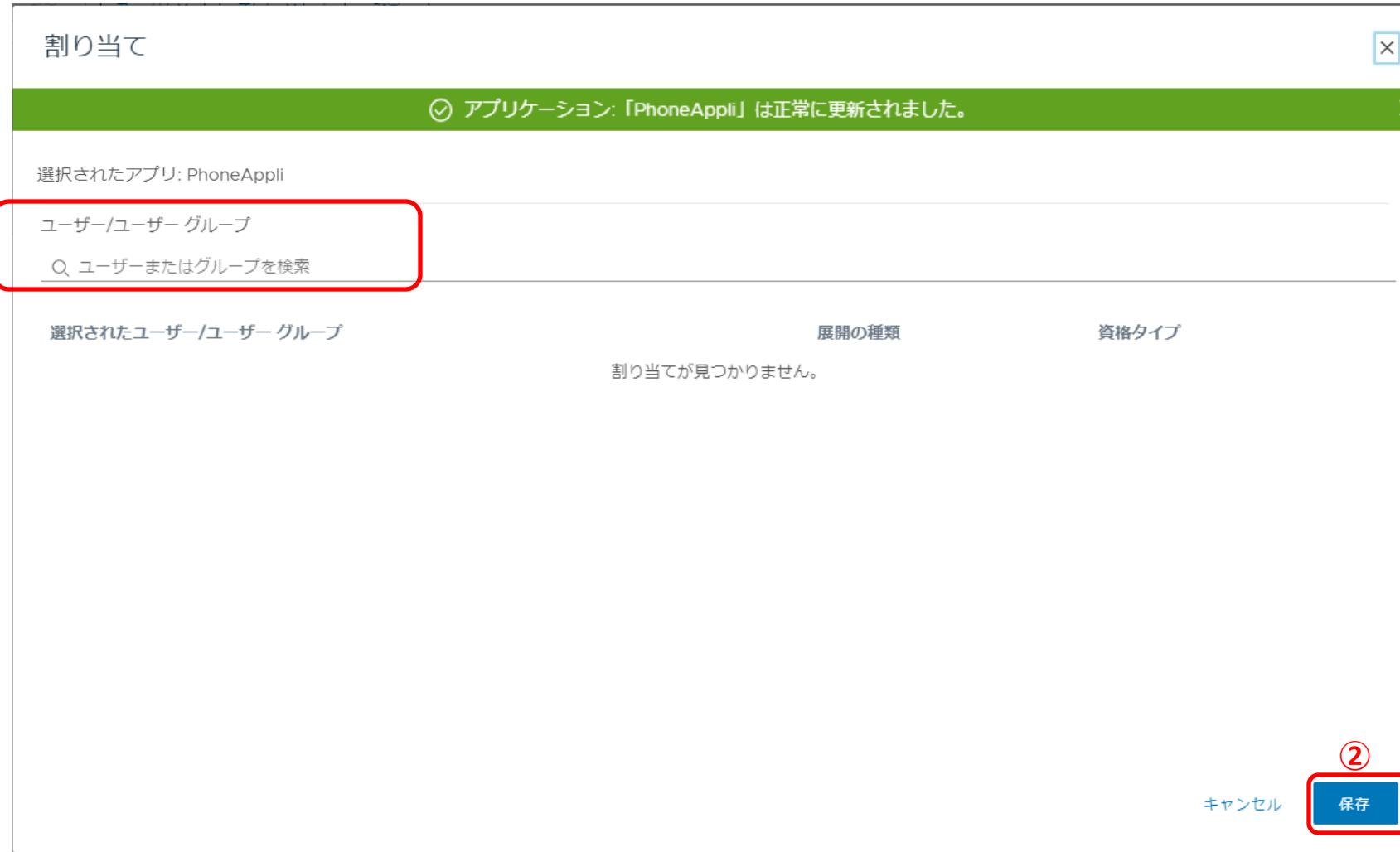
※⑩の既存ポリシーがない場合はデフォルトのポリシーを選択し、新規でポリシー作成後にポリシーの割り当てを変更してください。

A photograph of a campfire with bright orange and yellow flames. In the background, a large, dark silhouette of a mountain range is visible against a sky filled with warm, orange and yellow hues of a setting sun.

# Workspace ONE Access SAML認証アプリユーザ割り当て

### 3. 【 Workspace ONE Access 】 SAML認証アプリ ユーザ割り当て

- ① 「ユーザ/ユーザグループ」、「展開の種類」、「資格タイプ」を選択します。
- ② 「保存」をクリックします。





# Workspace ONE Access SAML認証アプリ ポリシー割り当て

## 4. 【 Workspace ONE Access 】 SAML認証アプリ ポリシー割り当て

- ① 「IDとアクセス管理」タブをクリックします。
- ② 「ポリシー」をクリックし、③対象となるポリシーを選択、または「ポリシーを追加」で新規ポリシーを作成します。  
※本書では事前に作成していた対象となるポリシーを選択しています。

The screenshot shows the 'Workspace ONE™ Access' interface. The top navigation bar has tabs: ダッシュボード, ユーザーとグループ, カタログ, **IDとアクセス管理** (which is highlighted with a red box and labeled ①), ロール. Below the navigation is a sub-navigation bar with tabs: ディレクトリ, ID プロバイダ, パスワード回復アシスタント, 認証方法, **ポリシー** (which is highlighted with a red box and labeled ②). The main content area shows a table for policy assignment. The table has columns: ポリシー名 (Policy Name) and 適用先 (Scope). There are two rows:

- Row 1:  [default\\_access\\_policy\\_set](#) 0 アプリケーション (0 Applications)
- Row 2: **③  [PhoneAppliPolicy](#)** 1 アプリケーション (1 Application)

The row for 'PhoneAppliPolicy' is highlighted with a red box and labeled ③.

※ポリシーを新規作成した場合、前項で作成したSAML認証用アプリのアクセスポリシーにてポリシーの割り当てを変更する必要があります。

## 4. 【 Workspace ONE Access 】 SAML認証アプリ ポリシー割り当て

- ④ 「ポリシーの編集」より、1 定義の「適用先」カタログからアプリケーションをクリックします。
- ⑤ SAML認証用に作成したアプリにチェックを入れます。
- ⑥ 「次へ」を3 サマリまでクリックし、保存します。



※本書では設定していませんが、新規ポリシーの場合は「2 構成」でポリシールールの設定が必要です。



# Workspace ONE Access

## SAML設定確認、 署名証明書のダウンロード

## 4. 【Workspace ONE Access】 SAML設定確認、署名証明書のダウンロード

- ①「カタログ」タブをクリックし、②「設定」をクリックします。
- ③「設定」画面のSaaSアプリより「SAMLメタデータ」をクリックします。
- ④【署名証明書】の「ダウンロード」をクリックし、署名証明書をダウンロードします。
- ⑤Workspace ONE AccessのテナントURLをコピーし、SSOエンドポイントURLとIDPエンティティIDの設定値を作成します。



The image shows the Workspace ONE Access interface. On the left, the 'Catalog' tab is selected (marked with a red box and number 1), and the 'Settings' button is highlighted (marked with a red box and number 2). A large red arrow points from this screen to the right. On the right, the 'Settings' screen is displayed, showing the 'SAML メタデータ' (SAML Metadata) section (marked with a red box and number 3). Below it is a large text area containing a certificate (marked with a red box and number 4). At the bottom of this area are three buttons: 'Copy', 'Download' (which is highlighted with a red box and number 4), and 'Regenerate'.

⑤お客様環境URL（Workspace ONE AccessのテナントURL）が  
<https://XXX-XXX.vmwareidentity.asia> の場合、以下設定値を作成します。

<SSO エンドポイントURL> ※次項でPA PEOPLEに登録する設定値です。  
<https://XXX-XXX.vmwareidentity.asia/SAAS/auth/federation/sso>

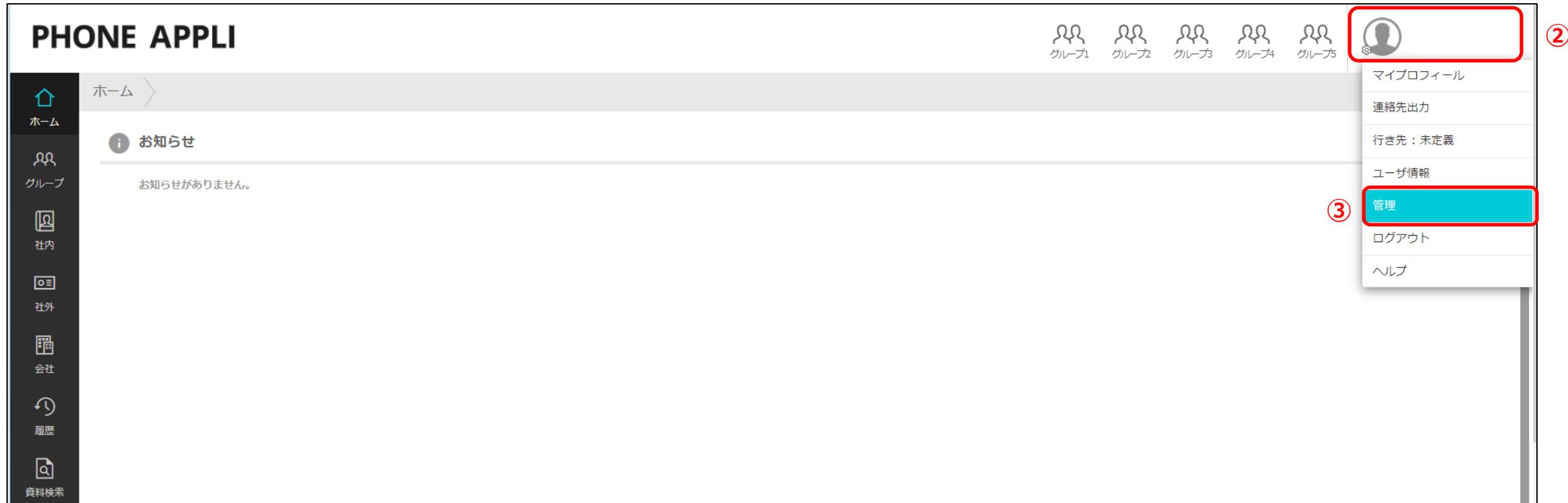
<IDPエンティティID> ※次項でPA PEOPLEに登録する設定値です。  
<https://XXX-XXX.vmwareidentity.asia/SAAS/API/1.0/GET/metadata/idp.xml>



# PHONE APPLI PEOPLE SAML設定

## 5. 【PHONE APPLI PEOPLE】 SAML設定

- ① PHONE APPLI PEOPLEに管理者アカウントでログインします。
- ② 右上の【設定】をクリックします。
- ③ 【管理】をクリックします。



## 5. 【PHONE APPLI PEOPLE】 SAML設定

④【企業情報】タブの【社名/ロゴ】をクリックします。

⑤認証方式を【SAML認証】に設定し、更新します。



The screenshot shows the PHONE APPLI PEOPLE application interface. On the left is a vertical sidebar with icons for Home, Groups, Internal, External, and History. The main navigation bar includes links for Home, Groups, Internal, External, and History. The top right features icons for five groups and a user profile. The main content area has a breadcrumb path: 管理 - 企業情報 - 社名/ロゴ. The '企業情報' tab is selected (highlighted with a red box and step 4). Below it, the '認証設定' tab is selected (highlighted with a red box and step 5). A callout arrow points from the '認証方式' dropdown on the main page to the 'SAML認証' option in the expanded dropdown on the right. The 'SAML認証' option is highlighted with a red box. A large red box also highlights the '更新' (Update) button. The expanded '認証設定' dialog box shows the '認証方式' dropdown with the following options: ローカル認証 & M365 SSO, ローカル認証 & o365 SSO, SAML認証 (highlighted with a red box), and OpenID Connect.

## 5. 【PHONE APPLI PEOPLE】 SAML設定

- ⑥ SSOエンドポイントURLを設定します。※P15の⑤で作成した値を入力します。
- ⑦ IdPエンティティIDを設定します。※P15の⑤で作成した値を入力します。
- ⑧ SPエンティティIDを設定します。※P7の⑧に登録したアプリケーションIDの値を入力します。
- ⑨ IdP署名の位置を「レスポンス内」に選択します。
- ⑩ 「ファイルを選択」からWorkspace ONE Accessでダウンロードした署名証明書をアップロードし、⑪更新をクリックします。

**認証設定**

ログイン時の認証方法とログアウト・セッションタイムアウト後の遷移先を設定できます。

認証方式 SAML認証

ログアウト後URL

セッションタイムアウト後URL

SSOエンドポイントURL ⑥ 必須入力項目です。

IdP URL

IdPエンティティID ⑦ 必須入力項目です。

SPエンティティID ⑧ 必須入力項目です。

IdPの署名の位置 ⑨ レスポンス内

IdP公開鍵証明書 ⑩ ファイルを選択 指定されていません  
RSAかDSAのアルゴリズムで生成された、公開鍵の証明書ファイルを添付します。  
X.509形式の証明書のみ利用できます。

⑪ 更新

※本書では設定していませんが、「ログアウト後URL」、「セッションタイムアウト後URL」は任意の値を設定することが可能です。

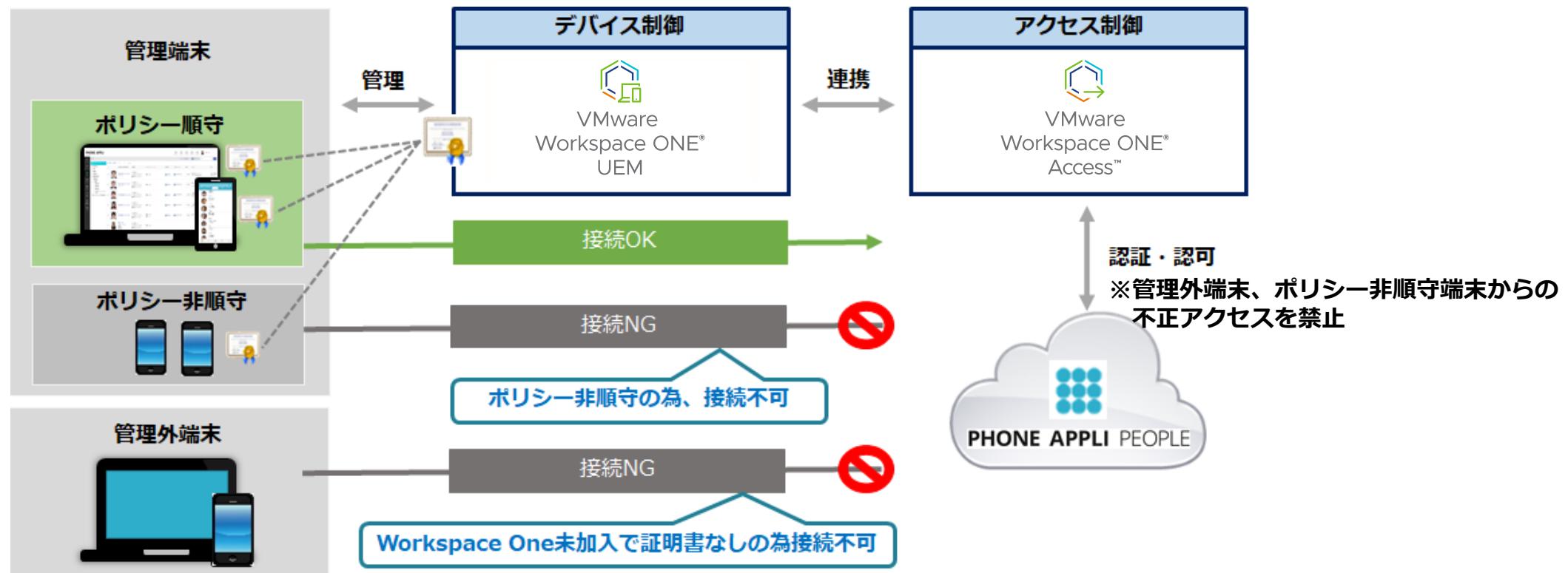
# モバイルSSOの利用について

## 6. 【Workspace ONE】モバイルSSOの利用について

Workspace ONE UEMとWorkspace ONE Accessを連携して「モバイルSSO」を利用する場合は、MDM機能でのアプリ配布、初期設定値（サーバーURLやログインIDなど）の自動入力に加えて、KDC証明書（Kerberos認証用）とデバイス証明書（SCEP）を端末のプロファイルに配布が可能なため、管理外端末からの不正アクセス防止やSAML認証のログイン操作を簡易にすることができます。

※モバイルSSOの設定方法については、WMware社もしくはWorkspace ONEの取り扱いベンダー様にお問い合わせください。

### ゼロトラストのコンポーネントとしてWorkspace ONEを活用



※PHONE APPLI では、Workspace ONE UEMとモバイルSSOに関してのお問い合わせやサポート対応は受け付けておりません。

「働く」を変える。「生きかた」が変わる。

**PHONE APPLI**

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