

PHONE APPLI PEOPLE Google Workspace SAML認証の設定

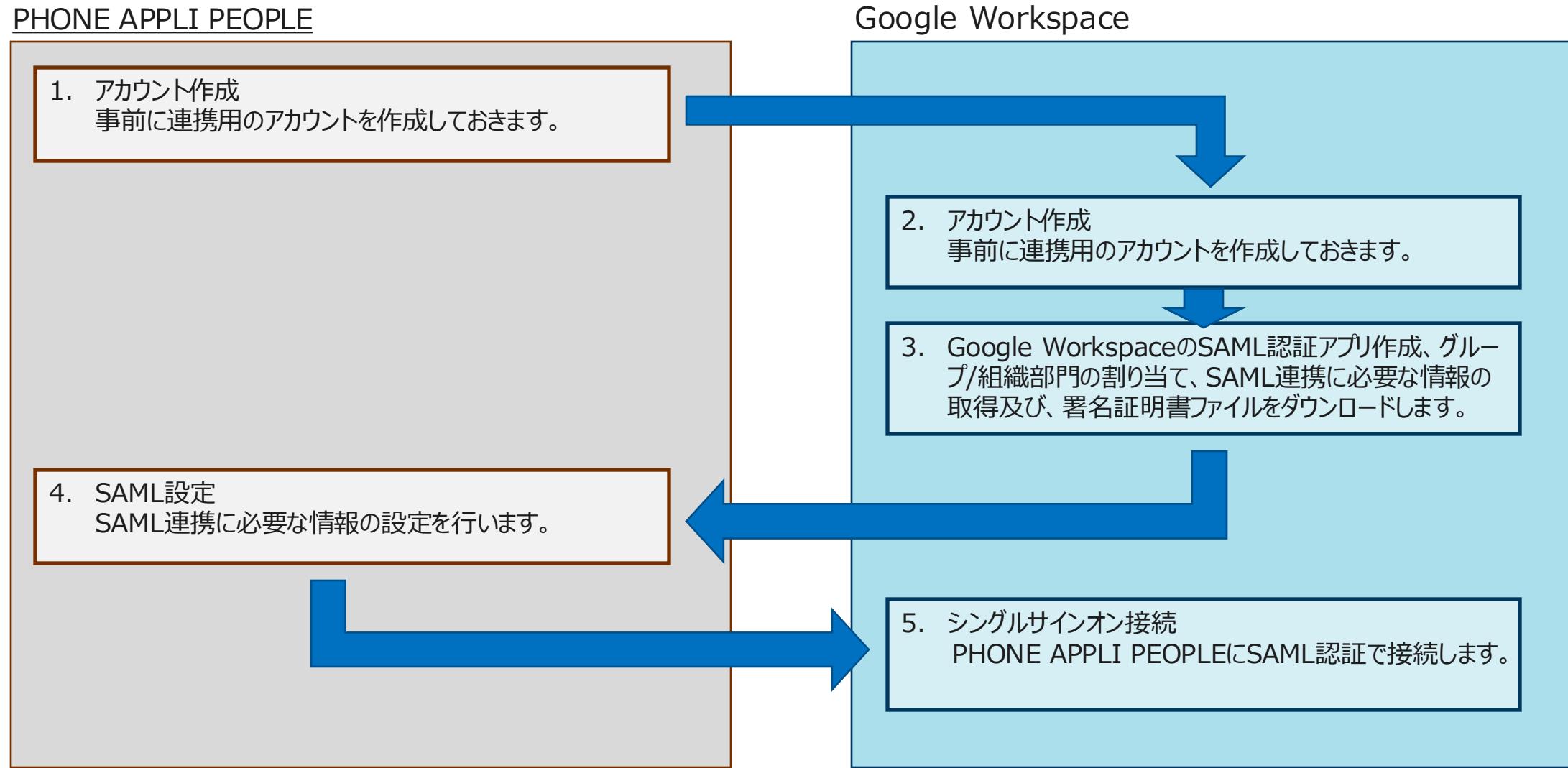
2023年 1月

目次

1. SSO設定の流れ
2. 【Google Workspace】 SAML認証アプリ作成
3. 【Google Workspace】 SAML認証アプリ グループ/組織部門の割り当て
4. 【PHONE APPLI PEOPLE】 SAML設定

1. SSO設定の流れ

Google Workspace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。



Google Workspace SAML認証アプリ作成

2. 【Google Workspace】 SAML認証アプリ作成

① 管理コンソール>アプリから「概要」をクリックします。

② 「ウェブアプリとモバイルアプリ」をクリックします。

The screenshot shows the Google Workspace Admin console interface. On the left, the navigation menu is open, showing various sections like Home, Dashboard, and Apps. The 'Apps' section is expanded, and the 'Overview' item under it is highlighted with a red box and labeled with a circled ①. In the main content area, there are four cards. The third card from the left is highlighted with a red box and labeled with a circled ②. This card is titled 'Web and mobile apps' and describes managing SAML, Android, and iOS apps. It shows 3 apps. The other three cards are: 'Google Workspace' (13 services), 'Other Google services' (64 services), and 'Google Workspace Marketplace apps' (0 apps).

2. 【Google Workspace】 SAML認証アプリ作成

- ③ 「アプリを追加」をクリックします。
- ④ プルダウンリストにある「カスタムSAMLアプリの追加」をクリックします。



The screenshot shows the Google Workspace Admin console. The left sidebar is titled 'Admin' and includes 'ホーム', 'ダッシュボード', 'ディレクトリ', 'デバイス', 'アプリ' (selected), '概要', 'Google Workspace', 'その他の Google サービス', 'ウェブアプリとモバイルアプリ' (selected), 'Google Workspace Marketplace アプリ', and 'セキュリティ'. The main content area is titled 'アプリ > ウェブアプリとモバイルアプリ'. It shows a table with three rows. The first row has a checkbox, the name 'PA', and the text '限定公開の Android アプリを追加'. The second row has a checkbox, the name 'PE', and the text '限定公開の Android ウェブアプリを追加'. The third row has a checkbox, the name 'Salesforce Sandbox', and the text 'カスタム SAML アプリの追加'. A red box highlights the 'カスタム SAML アプリの追加' option, with a red circle containing the number '4' to its right. A red box also highlights the 'アプリを追加' button in the top navigation bar, with a red circle containing the number '3' to its left.

2. 【Google Workspace】SAML認証アプリ作成

⑤ 必須項目の「アプリ名」を任意の値で入力します。 (※説明は任意)

⑥ 「続行」をクリックします。

× カスタム SAML アプリの追加

1 アプリの詳細 — 2 Google ID プロバイダの詳細 — 3 サービス プロバイダの詳細 — 4 属性のマッピング

アプリの詳細

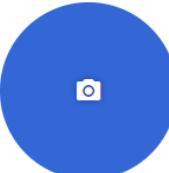
カスタム SAML アプリの詳細を入力してください。この情報はアプリのユーザーと共有されます。 [詳細](#)

⑤ アプリ名
PHONEAPPLI

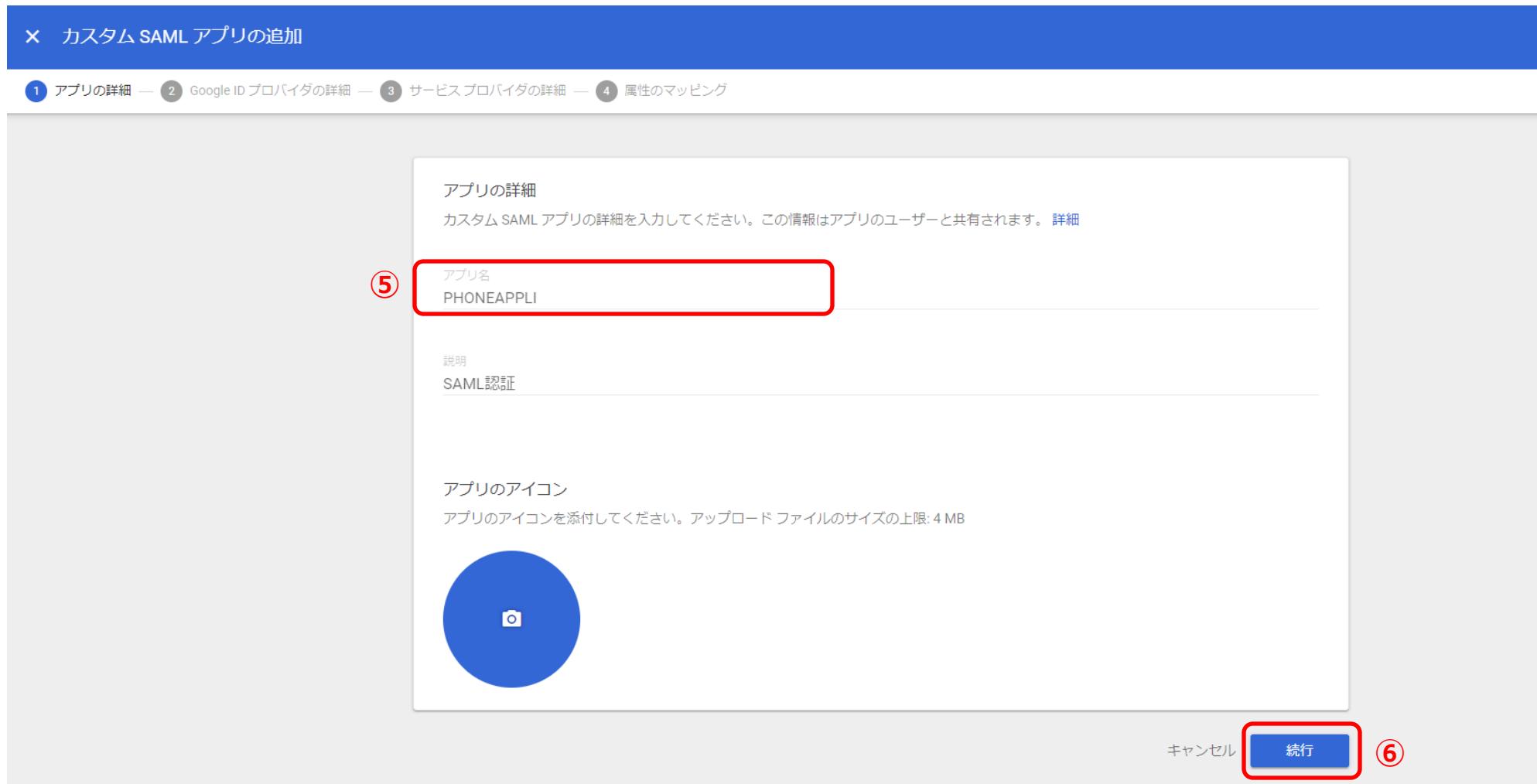
説明
SAML認証

アプリのアイコン

アプリのアイコンを添付してください。アップロード ファイルのサイズの上限: 4 MB



キャンセル 続行 ⑥



2. 【Google Workspace】 SAML認証アプリ作成

⑦ 「SSOのURL」 と⑧ 「エンティティID」 を「メモ帳」 などにコピーします。

⑨ 証明書をダウンロードし、⑩ 「続行」 をクリックします。

※PHONE APPLI PEOPLEへの設定はP15で実施します。

× カスタム SAML アプリの追加

1 アプリの詳細 — 2 Google ID プロバイダの詳細 — 3 サービスプロバイダの詳細 — 4 属性のマッピング

または

オプション 2: SSO の URL、エンティティ ID、証明書をコピーする

SSO の URL

エンティティ ID

証明書

Google_2026-2-16-184936_SAML2_0
有効期限: 2026/02/17
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----

SHA-256 フィンガープリント

⑦
⑧
⑨
⑩

戻る キャンセル 続行

アプリ > ウェブアプリとモバイルアプリ > PHONEAPPLI

SAML

PH PHONEAPPLI

SAML認証

SAML ログインをテスト

メタデータをダウンロード

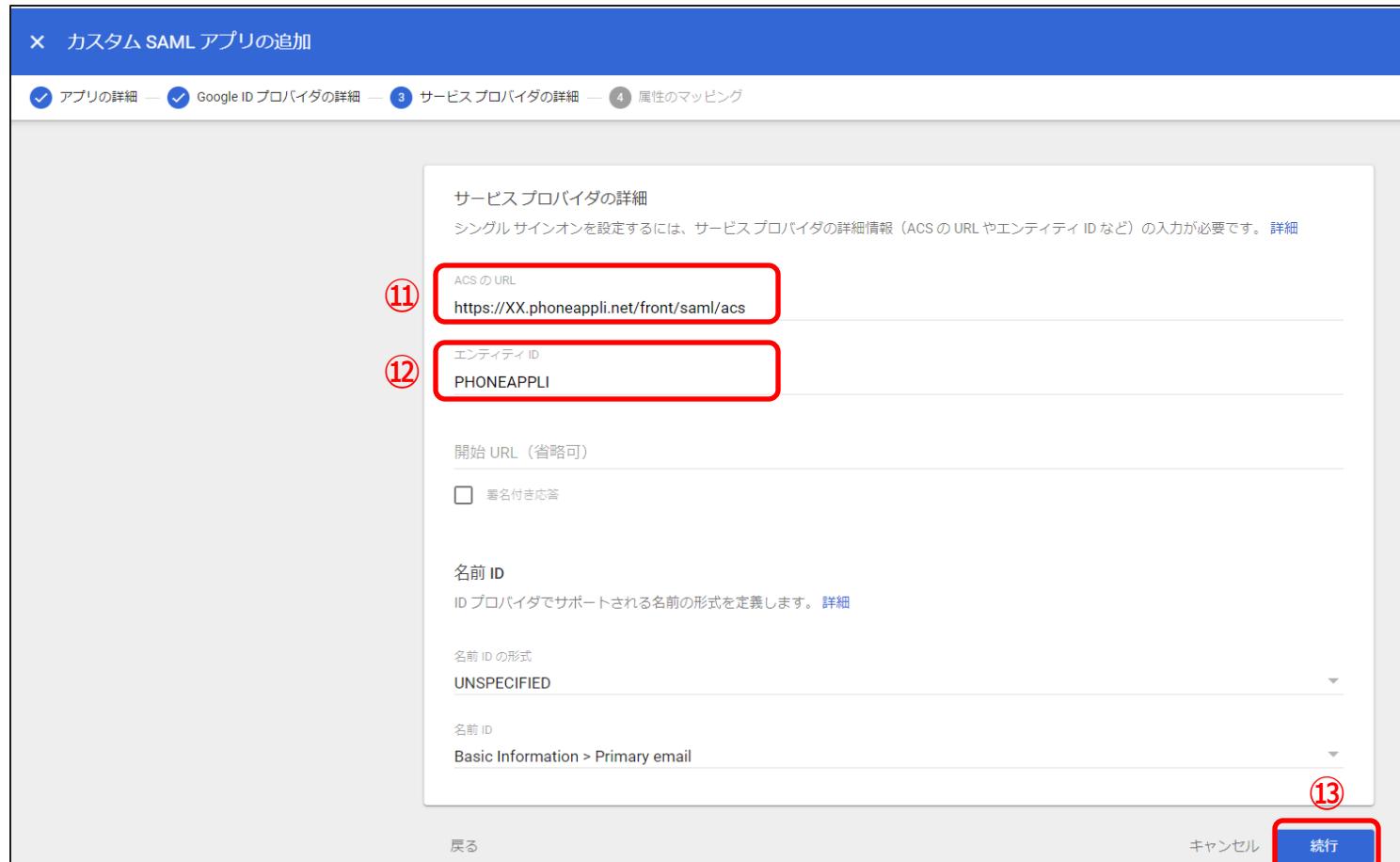
詳細を編集

アプリの削除

※アプリ作成後は、
「メタデータをダウンロード」
から同じ情報を取得できます。

2. 【Google Workspace】 SAML認証アプリ作成

- ⑪ ACSのURLにhttps://<お客様環境URL>/front/saml/acs を入力します。
- ⑫ エンティティIDとして、任意の値を入力します。
- ⑬ 「続行」をクリックし、4.属性のマッピング欄で設定が不要であれば「完了」をします。



⑪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。

<ACSのURL>

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

⑫の値（エンティティID）はGoogle Workspace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。

Google Workspace SAML認証アプリ グループ/組織部門の割り当て

3. 【Google Workspace】 SAML認証アプリ グループ/組織部門の割り当て

- ① 作成したSAML認証アプリを開き「ユーザーアクセス」をクリックします。
- ② 作成済みのグループ、または組織部門を割り当て、③サービスのステータスの「オン」にチェックを入れます。
- ④ 「保存」をクリックします。

① ユーザー アクセス

② グループ

③ オン

④ 保存

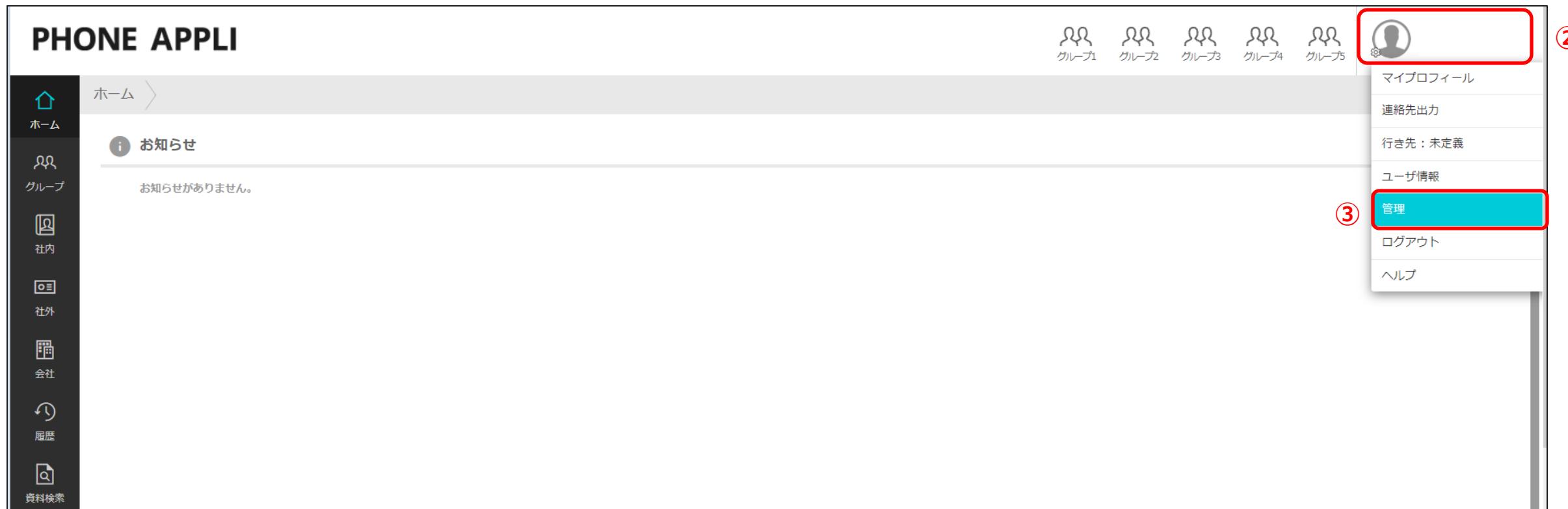
※本書ではグループの割り当て手順を記載しています。

※②のグループが表示されない場合はグループ（セキュリティ有り）を作成後に割り当てをしてください。

PHONE APPLI PEOPLE SAML設定

4. 【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。



4. 【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. The left sidebar contains icons for Home, Groups, Internal, External, Company, History, and Search. The main navigation bar includes links for Management, Enterprise Information, Groups, User, Shared Phone Book, Notifications, Sansan Integration, Log Output, and Azure AD Integration. The 'Enterprise Information' tab is selected, and the 'Logo' sub-tab is also selected, indicated by a red box and the number 4. The 'Authentication Settings' section is open, indicated by a red box and the number 5. A callout box highlights the 'Authentication Method' dropdown, which is set to 'Local Authentication & M365 SSO'. The 'SAML Authentication' option is highlighted with a red box. A red box also surrounds the 'Update' button. The bottom section shows 'Microsoft Intune' login restrictions, with a 'Login Limit' switch set to 'off'.

PHONE APPLI

管理 - 企業情報 - 社名/ロゴ

企業情報

社名/ロゴ

④

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。

⑤ 認証方式 ローカル認証 & M365 SSO

ログアウト後URL

セッションタイムアウト後URL

認証設定

認証方式

- ローカル認証 & M365 SSO
- ローカル認証 & M365 SSO
- SAML認証**
- OpenID Connect

更新

Microsoft Intuneによるログイン制限

Microsoft Intune外からインストールしたスマートフォン版アプリでのログインを制限します。

ログイン制限 off

更新

4. 【PHONE APPLI PEOPLE】 SAML設定

- ⑥ SSOエンドポイントURLを設定します。※P8の⑦で取得した値を入力します。
- ⑦ IdPエンティティIDを設定します。※P8の⑧で取得した値を入力します。
- ⑧ SPエンティティIDを設定します。※P9の⑫で登録した値を入力します。
- ⑨ IdP署名の位置を「アサーション内」に選択します。
- ⑩ 「ファイルを選択」からGoogle Workspace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	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 アサーション内
IdP公開鍵証明書	⑩ ファイルを選択 選択されていません 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 <input type="button" value="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。

「働く」を変える。「生きかた」が変わる。

PHONE APPLI