

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。

PHONE APPLI PEOPLE

1. アカウント作成
事前に連携用のアカウントを作成しておきます。

4. SAML設定
SAML連携に必要な情報の設定を行います。

Workspace ONE Access

2. アカウント作成
事前に連携用のアカウントを作成しておきます。

3. Workspace ONE AccessのSAML認証アプリ作成、
ユーザ/ポリシーの割り当て、SAML連携に必要な情報の
取得及び、署名証明書ファイルをダウンロードします。

5. シングルサインオン接続
PHONE APPLI PEOPLEにSAML認証で接続します。



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 *⑤
SAML 2.0

構成 *⑤
 URL/XML 手動

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

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

アプリケーション ID *⑧
PhoneAppli

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。

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
PhoneAppli

説明
-

アイコン

カテゴリ
-

構成

認証タイプ
SAML 2.0

構成
手動

キャンセル 戻る 保存して割り当て 保存

※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。



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。

割り当て

☑ アプリケーション: 「PhoneAppli」 は正常に更新されました。

選択されたアプリ: PhoneAppli

① ユーザー/ユーザー グループ

Q ユーザーまたはグループを検索

選択されたユーザー/ユーザー グループ	展開の種類	資格タイプ
割り当てが見つかりません。		

キャンセル ② 保存



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。

Workspace ONE™ Access

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** ロール

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** Magic Link

ポリシーを追加 編集 削除 デフォルト ポリシーの編集 ネットワーク範囲

ポリシー名	適用先
<input type="radio"/> default_access_policy_set	0 アプリケーション
<input checked="" type="radio"/> PhoneAppliPolicy	1 アプリケーション

※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。

ポリシーの編集

1 定義
2 構成
3 サマリ

定義

説明①

適用先①
Q カタログからアプリケーション

	名前	↑	タイプ	UUID
⑤	<input checked="" type="checkbox"/> PhoneAppli		SAML 2.0	

⑥

キャンセル 次へ

※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。
- ⑤ Workspace 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。



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。

The screenshot displays the PHONE APPLI application interface. At the top left, the title 'PHONE APPLI' is visible. The top right corner features a navigation bar with five group icons labeled 'グループ1' through 'グループ5', and a user profile icon circled in red with a circled '2' next to it. Below the navigation bar, a sidebar on the left contains icons for 'ホーム', 'グループ', '社内', '社外', '会社', '履歴', and '資料検索'. The main content area shows a 'ホーム' header and an 'お知らせ' (Notice) section with the message 'お知らせがありません。' (No notices). On the right side, a dropdown menu is open, listing options: 'マイプロフィール', '連絡先出力', '行き先：未定義', 'ユーザ情報', '管理' (highlighted in blue and circled in red with a circled '3' next to it), 'ログアウト', and 'ヘルプ'.

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 displays the 'PHONE APPLI' management interface. The top navigation bar includes '管理 - 企業情報 - 社名/ロゴ' and various settings tabs. The '企業情報' tab is active, and the '社名/ロゴ' sub-tab is selected. The main content area is titled '認証設定' (Authentication Settings). A red box highlights the '認証方式' (Authentication Method) dropdown menu, which is currently set to 'ローカル認証 & M365 SSO'. A red circle with the number '5' is placed next to this dropdown. A red arrow points from this dropdown to a larger, magnified view of the dropdown menu on the right. In this magnified view, the 'SAML認証' option is highlighted with a red box. Below the dropdown menu is a blue '更新' (Update) button, also highlighted with a red box. The interface also shows a 'Microsoft Intuneによるログイン制限' (Login Restriction by Microsoft Intune) section with a toggle switch set to 'off' and another '更新' (Update) button at the bottom.

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。

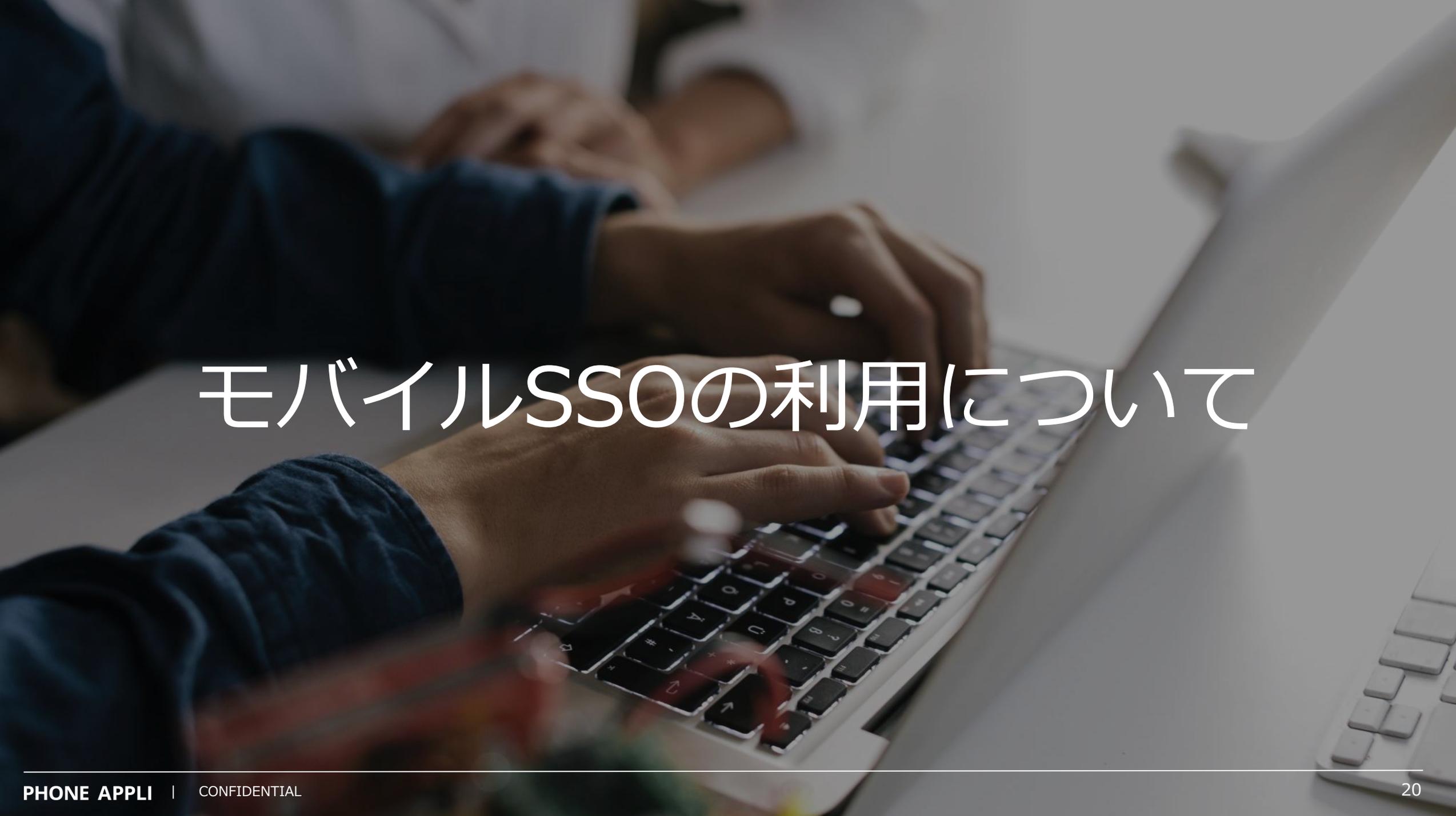
認証設定

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 <input type="text"/> 必須入力項目です。
IdP URL	IdPエンティティID ⑦ <input type="text"/> 必須入力項目です。
	SPエンティティID ⑧ <input type="text"/> 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 <input type="button" value="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

※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。



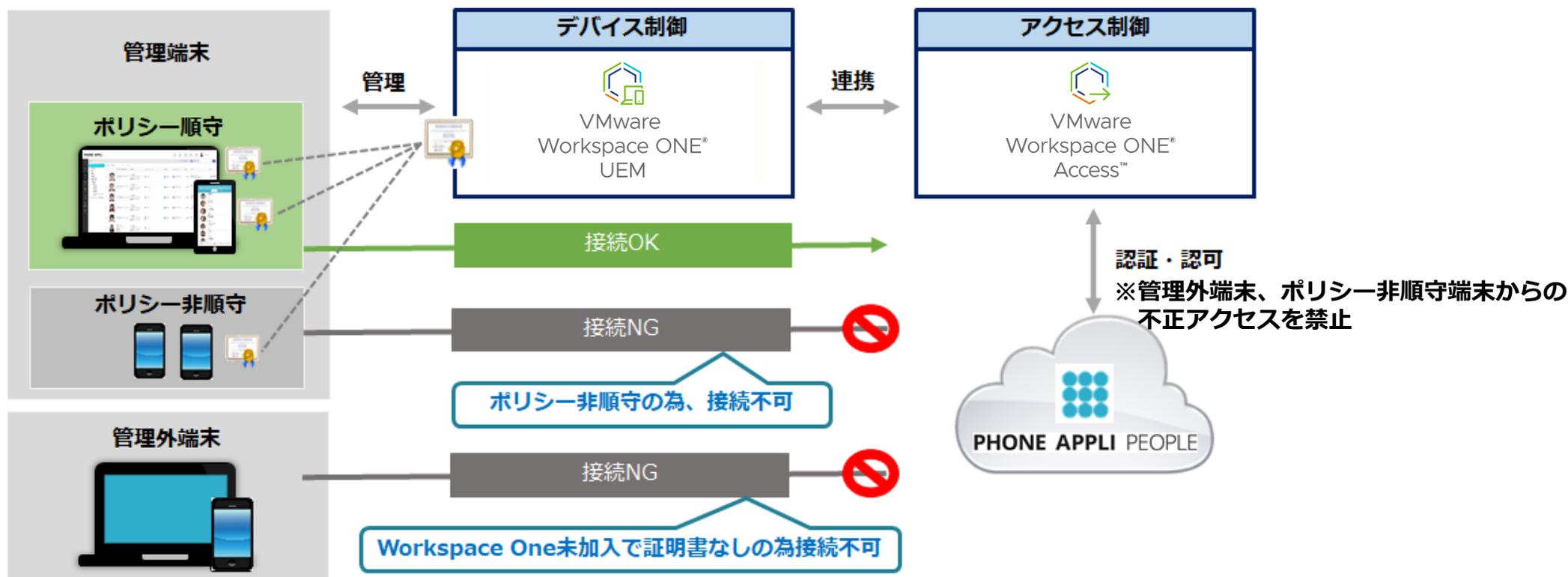
モバイルSSOの利用について

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のため、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、VMware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