PHONE APPLI PEOPLE MS365 SSOのための設定手順

2024年7月

PHONE APPLI



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
2024/07/05	更新



- 1. PHONE APPLI PEOPLEでSSOログインを行う(ブラウザ)
- 2. PHONE APPLI PEOPLEでSSOログインを行う(スマートフォン)
- 3. クライアント証明書をご利用されている場合(iOSのみ)
- 4. Microsoft Entra IDで条件付きアクセスをご利用されている場合(iOS、 Android)
- 5. Intune アプリ保護ポリシーをご利用になる場合(iOSのみ)

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

		PHONE APPLI PEOPLE	
		ログインD	
		ログイン	
	1	Microsoft 365でログインする	
		Version: 1.48.0(2)	
E APPLIについて サービス利用規約 プライバシーポリシー	_		

PHO

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。



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] (下図1)にチェックを入れ、 [承諾] (下図2)をすることでWeb画面でのSSOが利用可能になります。

※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。



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)。

*	+ いいアプリケーら	ペン じ 更新 🛓 ダウン	ロード (エクスポート) 🛛 🧿 フ	レビューの情報 🛛 🧾 利	12 プレビュー機能 /	🖗 フィードバックがある場合	
0 板景	Microsoft Entra テナン	小を旧プロバイダーとして使り	用するように設定されている、ご自	身の組織内のアプリケーション	を表示、フィルター処理、検索	L#f.	
× 問題の診断と解決	絵織で管理されている7	プリケーションのリストは、アプ	リケーションの登録にあります。				
9 1	P 7554		アプリケーションの種類 == :	エンタープライズ アプリケーショ	ン X 779ケーション	D 次の値で始まる × ちってィル・	ターの追加
オペモのアプリケーション	1 毎のアプリケーションが	が見つかりました					
B アプリケーション プロキシ	品約	↑↓ オブジェクト ID	アプリケーション Ю	ホームページ URL	作成日	↑↓ 証明書有効期間の状態	アクティブな証明書の有・
◎ ユーザー設定	ブラ ブラウザ用シン	JA9-			2020/4/14	8	82
アプリ起動ツール							
☆ カスタム認証拡張機能(プレビュー)							
セキュリティ							
条件付きアクセス							
③ 同意とアクセス許可							
アクティビティ							
9 #4>4>DØ							
道 使用状況と分析情報							
※表ログ							
プロビジョニング ログ							
≡ 7クセスレビュー							
管理者の同意要求							
👃 一括操作の結果							
・ラブルシューティング = サポート							
BC 1444-1 10721							

Microsoft Entra IDの管理者アカウントでPHONE APPLI PEOPLEのSSO認証を行います。 「ログインID」「サーバ」(下図1)の情報を入力して[次へ](下図2)をタップし、 [Microsoft 365 でログインする] (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)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、「3.クライアント証明書を使用している場合(iOSのみ)」から手順を実施してください。

	ログイン		\leftarrow	ログイン		\leftarrow	ログイン
	端末D 16072526		端末ID 16072526			端末ID 16072526	
	ログインID LoginID		ログインID adfs@			サーバ	
(I)	ש–ו ג www.∉ample.com		パ <mark>スワード</mark> Password			SSL	ON
	SSL		サーバ				
	サーバ は弊社から提供されている URLをご入力ください。 例: reprakul torerukun com		SSL	ON			
	*https://は不要です。						
		3	Micro	soft 365 でログインする		通常	アカウントでログインする
\bigcirc)					
	次へ			ログイン	(4)		ログイン

PHONE APPLI 「働く」を変える。「生きかた」が変わる。

Microsoftのサインイン画面(下図12)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。

	キャンセル		キャンセル
	Microsoft		Microsoft
	サインイン		← adfs@
(1)	メール、電話、Skype 	(2)	パスワードの入力
	アカウントにアクセスできない場合		パスワード
	サインイン オプション		パスワードを忘れた場合
	次へ		サインイン
	©2019 Microsoft 利用規約 プライバシーと Cookie ・・・		

最初にログインする場合に限り、アクセス許可の同意およ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] (下図1)にチェックを入れ、 [承諾] (下図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。

	キャンセル]
	Microsoft	
	adfs@	
	要求されているアクセス許可	
	スマートフォン用シングルサインオンアプリ アプリ情報	
	このアプリで必要なアクセス許可:	
	◇ Access SSO_Server (ブラウザ用シングルサインオンアプリ)	
_	◇ サインオンを有効にしてユーザーのプロファイルを読み取る	
(1)	🛃 組織の代理として同意する	
\smile	同意すると、このアプリは組織内のすべてのユーザーの指定のリソース にアクセスできるようになります。これらのアクセス許可の確認を求め るメッセージは、他のユーザーには表示されません。	
	同意すると、ブラウザ用シングルサインオンアプリ でもお客様のユーザ ー プロファイル情報にアクセスできるようになります。	
	これらのアクセス許可を受け入れることは、サービス利用規約とプライ パシーに関する声明で指定されているとおりにこのアプリがデータを使 用することを許可することを意味します。確認を行うための利用規約へ のリンクが発行元によって提供されていません。これらのアクセス許可 は https://myapps.microsoft.com で変更できます。 詳細の表示	
	キャンセル 承諾	2
		J

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)。

	* + 新しいアプリケーション 🕚 更新 🛓 タ	グウンロード (エクスボート)	● プレビューの情報 🔡	= 列 🛛 🔛 プレビュー機能	1 R 74-Friy95	ある場合		
0 板菱	Microsoft Entra テナントを ID プロバイダーとし	て使用するように設定されてい	いる、ご自身の組織内のアプリケー	ーションを表示、フィルター処理	1. 検索します。			
★ 問題の診断と解決	結構で管理されているアプリケーションのリストは、	アプリケーションの登録にあ	リます。					
ह त्व	● スマートフォン用	× アプリケーションの	権賢 == エンタープライズ アプリ	ケーション × アプリケー	ション 印 次の値で始まる	a × 🦙 フィルターの追加		
オペてのアプリケーション	1個のアプリケーションが見つかいました						-	_
D アプリケーション プロキシ	名約	↑↓ 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	↑↓ 証明書有効期間の状…	アクティブな証明	6
9 ユーザー設定	スマ スマートフォン用シングルサインオンアプ	N			2020/4/14	32	12	(
アプリ記動ツール								
↑ カスタム認証証価機能(プレビュー)								
キュリティ								
業件付きアクセス								
○ 同意とアクセス許可								
アクティビティ								
9 サインインログ								
a 使用状況と分析情報								
 使用状況と分析情報 監査ログ 								
 ・ ・ ・								
 使用状況と分析情報 数型ログ プロビジョニングログ ブクセスレビュー 								
 ● 使用状況と分析情報 ● 転車ログ ● プロビジョニング ログ ■ アクセス レビュー ● 管理者の同意要求 								

iOS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。



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

「ログインID」「サーバ」(下図1)の情報を入力して[次へ](下図2)をタップし、 [Microsoft 365 でログインする] (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)をタップします。



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。



最初にログインする場合に限り、アクセス許可の同意およ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] (下図1)にチェックを入れ、 [承諾] (下図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。

	キャンセル	
	 Microsoft adfs@ 要求されているアクセス許可 スマートフォン用シングルサインオンアプリ アプリ情報 このアプリで必要なアクセス許可: 	
	✓ Access SSO_Server (ブラウザ用シングルサインオンアプリ)	
	サインオンを有効にしてユーザーのプロファイルを読み取る 和細の代理として同意する	
U		
	同意すると、このアプリは組織内のすべてのユーザーの指定のリソース にアクセスできるようになります。これらのアクセス許可の確認を求め るメッセージは、他のユーザーには表示されません。	
	同意すると、ブラウザ用シングルサインオンアブリ でもお客様のユーザ ー プロファイル情報にアクセスできるようになります。	
	これらのアクセス許可を受け入れることは、サービス利用規約とプライ パシーに関する声明で指定されているとおりにこのアプリがデータを使 用することを許可することを意味します。確認を行うための利用規約へ のリンクが発行元によって提供されていません。これらのアクセス許可 は https://myapps.microsoft.com で変更できます。 詳細の表示	
	キャンセル 承諾	2

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)。

	* + 新しいアプリケーション 🖒 更新 🛓 3	ダウンロー	ド(エクスポート)	● プレビューの情報 🔡	列 12 プレビュー機	E 🛛 74-Friss	がある場合	
	Microsoft Entra テナントを ID プロバイダーとし	て使用す	るように設定されてい	、ご自身の組織内のアプリケー ます。	ーションを表示。フィルター処日	夏、検索します。		
RE	■■ CTECK(10) / // ->=>>>/////		アプリケーションの細	×1. 15 エンタープライズ アプリ	ケーション × アプリケー	ーション 印 次の値で始ま	る a × 👘 フィルターの追加	
オペモのアプリケーショ	1 個のアプリケーションが見つかりました	N			- F.M. (1) - F.F.			
7プリケーション プロキャ	88	ং, র	プジェクト ID	アプリケーション ID	ホームページ URL	作成日	↑↓ 証明書有効期間の状…	アクティブな巨明
ユーザー設定	スマ スマートフォン用シングルサインオンアフ	70				2020/4/14	82	12
アプリ転動ツール								
カスタム認証証価機能 (プレビュー)								
コリティ								
ショリティ 毎年付きアクセス								
コリティ 単作付きアクセス 同意とアクセス許可								
キュリティ 単作付きアクセス 同島とアクセス許可 フティビティ								
キュリティ ・ 単件付きアクセス ・ 同意とアクセス許可 ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・ ・								
キュリティ 単作付きアクセス) 同意とアクセス許可 クティビティ) サインイン ログ) 使用状況と分析情報								
キュリティ 単作付きアクセス 回意とアクセス許可 クティビティ サインイン ログ 使用状況と分析情報 販売ログ								
 キュリティ 単件付きアクセス 同意とアクセス許可 ウティビティ サインイン ログ 使用状況と分析情報 転車ログ プロビジュニング ログ 								
キュリティ 単作付きアクセス 同意とアクセス許可 ティビティ サインイン ログ 使用状況と分析情報 転去ログ プロビジョニング ログ アクセス レビュー								
キュリティ 単件付きアクセス 同意とアクセス許可 クティビティ サインイン ログ 使用状況と分析情報 転妻ログ プロビジュニング ログ アクセス レビュー 管理者の同意要求								

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加されます。



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

・iOS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。



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

※ iOS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
 - <u>PHONE APPLI PEOPLE for Intune</u>(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(iOS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(iOS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、なおかつ、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。

 データ保護 レビューと保存 このグループには、切り取り、コピー、貼り付け、名前を付けて保 によって、ユーザーがアプリ内でデータを操作する方法が決まりま データ転送 	そ存などを制限するデータ損失防止 (DLP) コントロールが含まれています。これらの設定 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
iTunes と iCloud のバックアップに組織データを バックアップ ①	許可 ブロック	• 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
他のアプリに組織データを送信 ①	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
除外するアプリを選択します	すべてのアプリ	※「9へ(のアノリ」を選択している場合は个安で9。
応ん ナフコール サル リンクチョウナフ	なし	
际介9るユニハーリル リノンを进行9る	ポリシー マネージド アプリ	
管理対象ユニバーサルリンクを選択する	OS 共有利用のポリシー マネージド アプリ	
組織データのコピーを保存 ①	Open In/Share フィルター利用のポリシー マネージド アプリ	※ 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。

※ 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。

5. Intune アプリ保護ポリシーをご利用になる場合(iOS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。

ホーム > アプリ アプリ保護ポリシー > Intune アプリ保護 ポリシーの編集 … iOS用保護ポリシー	度 プロパティ >	適用から除外されるアプリ ×	• 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」配下にある「除外するアプリを選択しま
 データ保護 レビューと保存 このグループには、切り取り、コピー、貼り付け、名前を付けてき によって、ユーザーがアプリ内でデータを操作する方法が決まりま データ転送 iTunes と iCloud のバックアップに組織データを 	R存などを制限するデータ損失防止 (DLP) コントロールが含まれています。これらの設定 ます。 許可 フロック	注意:これらの設定を変更すると、Intuneで他のアプリケーションへのデータ転送をブロックまたは許可する方法が変更されます。データ漏洩の可能性について理解していない場合は、これらの設定を変更しないでください。詳細については、ごららを参照してください。 新しいポリシーの場合、電話通信プロトコルは既定の除外アプリの一覧に追加されなくなります。アプリケーションで新しいパージョンの Intune SDK (パージョン 12.7.0 以上)を使用している場合は、[他のアプリに組織データを送信]の下の[電話通信影子への転送え方]の設定を使用して、電話通信電送の設定を行ってください、古いパージョンの Intune CDV たた明12/13-27 (パーションの時後、マー、野に声を読得してした。)	す」の[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」で下記設定値の名前、値(左図2)を 入力し[OK] (左図3)をクリックします。
パックアップ ○ 他のアプリに組織データを送信 ○ 除外するアプリを選択します	ボリシーマネージドアプリ 選択 3842	30k を使用しているアンサンションの場合、この一見に電話通信プロドコル (tel および telprompt) を追加してください。詳細情報。 名前 値 Default skype;app-settings;calsho ・・・	<phone appli="" popleをご利用の場合=""> 名前: PA PEOPLE(任意) 値 : msauth.net.phoneappli.people</phone>
除か9 るエーハーリル リンクを選択する 管理対象ユニパーサル リンクを選択する 組織データのコピーを保存 ① 選択したサービスにユーザーがコピーを保存するこ	選択 2 選択 10ック 0項目が選択されました >	PA PEOPLE msauth.net.phoneappli 名前 值	<連絡とれるくんをご利用の場合> 名前: RENRAKU(任意) 値 : msauth.net.phoneappli.renraku
とを許可 ① 電話通信データの転送先 ① ダイヤラー アプリ URL スキーム	任意の電話アプリ ✓		 ・ [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。
100アノリからアークを受信 ① データを開いて組織ドキュメントに読み込む ① 選択したサービスからデータを開くことをユーザーに 許可する ①	すへ(の)・ノリ 許可 ブロック 4項目が選択されました		
他のアプリとの間で切り取り、コピー、貼り付け を制限する ① レビューと保存 キャンセル		ок	

「働く」を変える。「生きかた」が変わる。

PHONE APPLI

info@phoneappli.net