

【Office 365 二要素認証の利用手順書】

Microsoft Office 365 の二要素認証においては、以下の4つの認証方法を選択することができます。

通常は1のSMSによるコード受信を選択することをおすすめします。

※2の場合、音声着信が必要となるためシーンによっては使いづらい場合があります。

※3・4のモバイルアプリは常駐アプリとなり、スマートフォン等のバッテリー消費につながります。

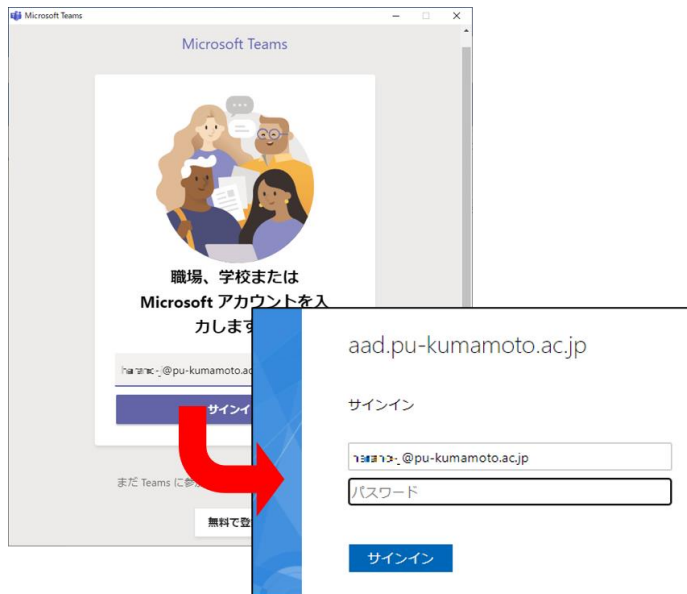
※海外での携帯電話ローミング中はSMS・音声着信に着信料が発生するため、3・4の方法を活用してください。

1. 携帯電話でSMS（無料）を受信し、記載されたコードを入力
→ [二要素認証案内サイト](#)をご参照ください。
→本書では2～3の利用手順を案内します。
2. 携帯／固定電話で着信（無料）し確認処理を行う
[P.2 ～ P.5](#)
3. モバイルアプリ「Microsoft Authenticator」から承認処理を行う
[P.6 ～ P.13](#)
4. モバイルアプリ「Microsoft Authenticator」に表示されたコードを入力
[P.14 ～ P.20](#)

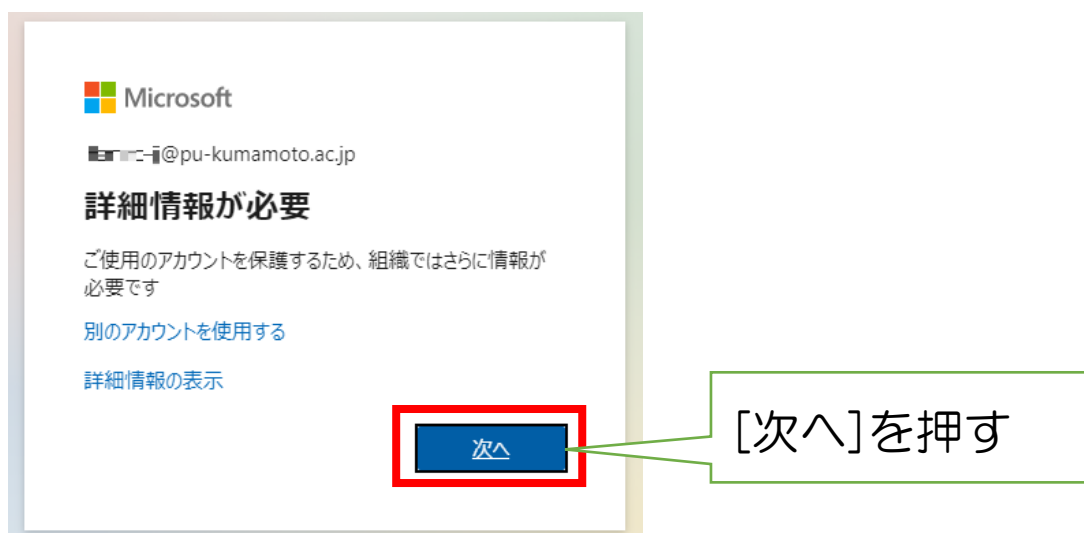
2. 携帯／固定電話で着信（無料）し確認処理を行う

A. 初回登録手順

①Office 365 サービスに学内アカウント・パスワードでログインする（以下は Teams の例）。



②「詳細情報が必要」との表示が出るため、「次へ」を押す。



③「追加のセキュリティ確認」画面が表示される。下図を参考に、着信用の番号を登録し、「次へ」を押す。

④指定した電話番号にマイクロソフトから自動音声による着信があるので、音声の指示し従い電話機の操作を行う。

※2020年12月現在、**#キー**を押して確認を完了させる流れとなる。

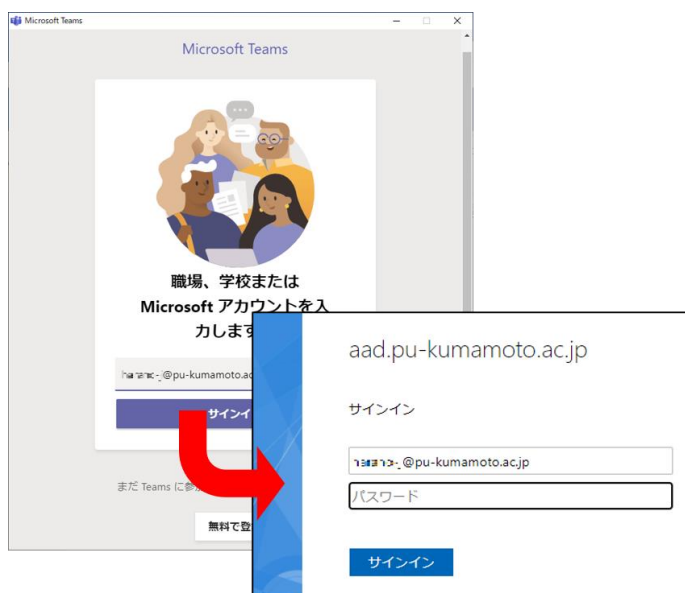
操作を行うと、以下のようにメッセージが変化する。

⑤処理が完了すると、「確認に成功しました。」と表示されるため、「完了」ボタンを押して終了する。

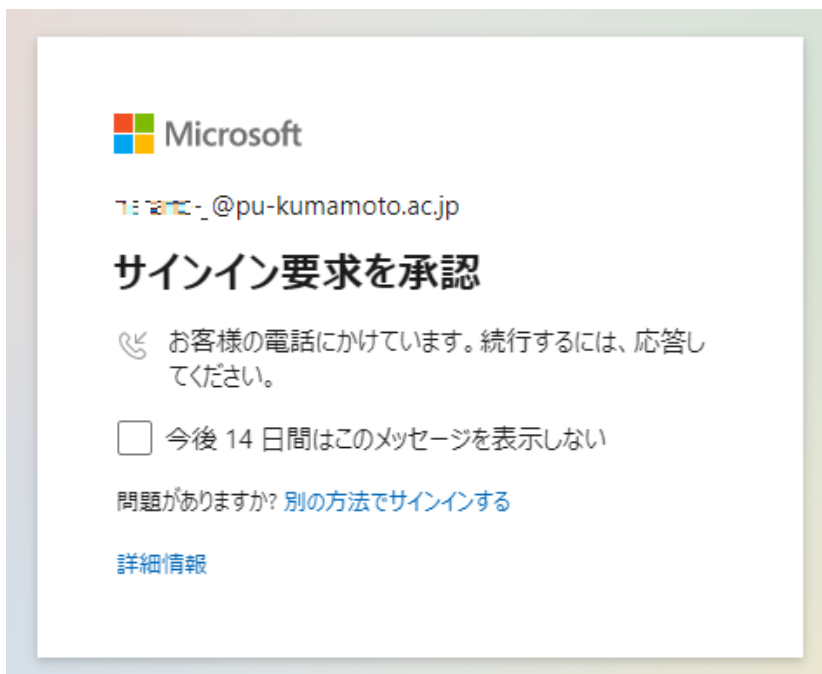


B. 次回以降の認証手順

①Office 365 サービスに学内アカウント・パスワードでログインする（以下は Teams の例）。



②以下の画面に遷移すると同時に、初回登録時に指定した電話番号あてにマイクロソフトより着信がある。



音声の指示に従い電話機の操作を行う。

※2020年12月現在、**#キー**を押して認証を完了させる流れとなる。

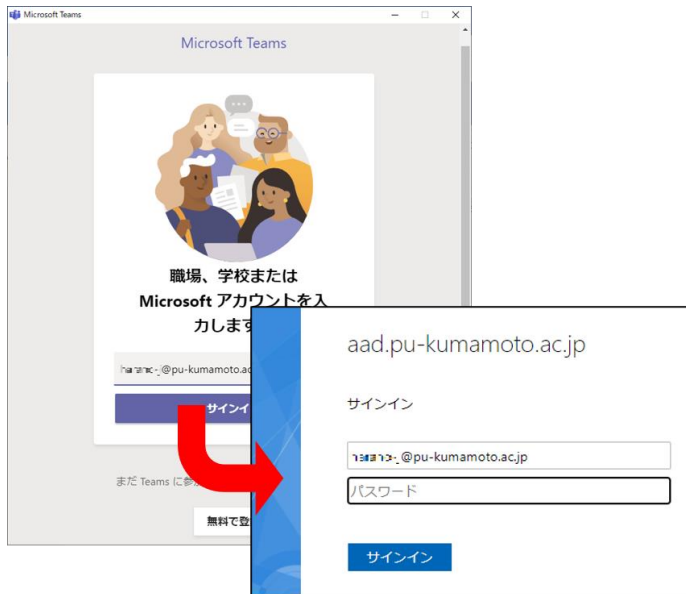
※「今後14日間はこのメッセージを表示しない」にチェックすると、ログインする端末を信頼し、二要素認証が14日間行われないため便利。

③認証が完了すると、自動的にログイン対象のサービス画面に遷移する。

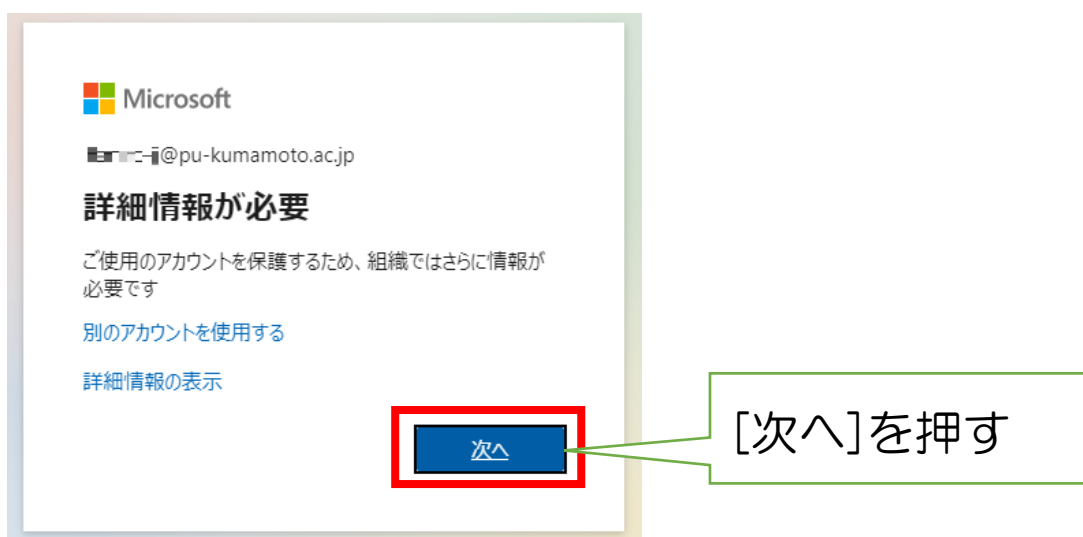
3. モバイルアプリ「Microsoft Authenticator」から承認作業を行う

A. 初回登録手順

①Office 365 サービスに学内アカウント・パスワードでログインする（以下は Teams の例）。



②「詳細情報が必要」との表示が出るため、「次へ」を押す。



③「追加のセキュリティ確認」画面が表示される。手順1のプルダウンから「モバイルアプリ」を選択する。最初に「セットアップ」を押し、Microsoft Authenticator アプリのセットアップを行う。

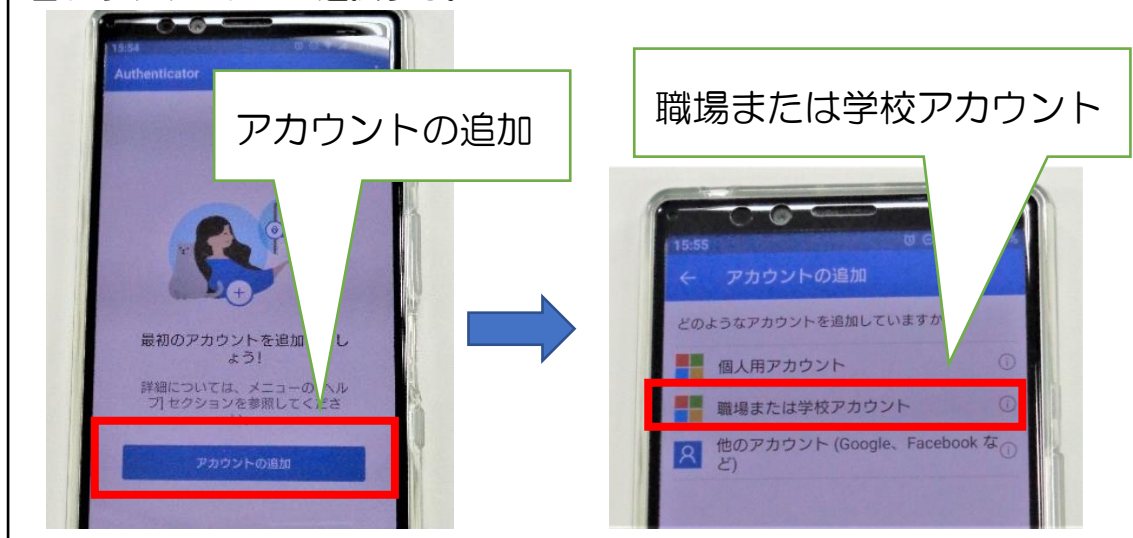
④「モバイルアプリケーションの構成」画面が表示される。まず、AppStore や Google Play Store からアプリケーションのダウンロードを行う。「Microsoft Authenticator」でストア内検索をするとよい。

⑤アプリインストール後、初期画面が表示される。プライバシーポリシーへ「同意します」を選択する（左画面）。その後、右画面に遷移するため、「QRコードをスキャンします」を選択する。



※本画面は初回起動時のみ表示される。

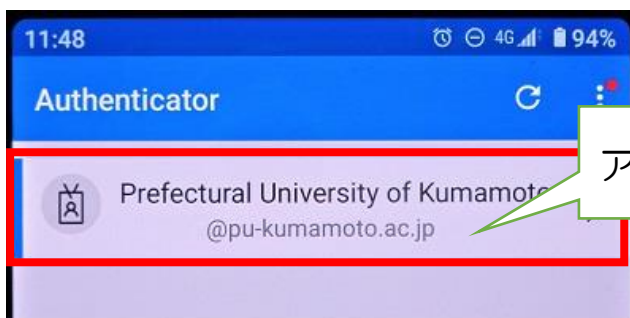
アプリを立ち上げなおしたり、アカウントの再連携を行う場合は、ホーム画面より以下のように選択する。



⑥「モバイルアプリケーションの構成」画面の QR コードをスキャンする。



⑦アカウントの追加が完了し、アプリのホーム画面に自分のアカウントが表示された状態となる。



⑧アカウントを選択すると、以下の画面のようにコードが表示される。この表示により正しくアプリと Office 365 アカウントが連携できていることが確認できる。



⑩ 「モバイルアプリケーションの構成」画面の「次へ」を押す。

モバイル アプリケーションの構成

次の手順でモバイル アプリケーションを構成してください。

1. Windows Phone、Android、または iOS の Microsoft Authenticator アプリをインストールします。
2. アプリでアカウントを追加し、「職場または学校アカウント」を選択します。
3. 下の画像をスキャンしてください。



画像をスキャンできない場合は、アプリケーションに次の情報を入力してください。
コード: 398 581 303
URL: <https://mobileappcommunicator.auth.microsoft.com/mac/MobileAppCommunicator.svc/184188947>

アプリケーションに 6 桁のコードが表示されている場合、[次へ] を選択します。

次へ キャンセル

⑪ 「追加のセキュリティ確認」画面に戻る。「モバイルアプリケーションが構成されました」とメッセージが出ていることを確認する。

「モバイルアプリをどのような用途で使用されますか？」の「**確認のための通知を受け取る**」にチェックし、「次へ」を押す。

Microsoft

追加のセキュリティ確認

パスワードに電話の確認を追加することにより、アカウントを保護します。アカウントをセキュリティで保護する方法についてビデオを見る

手順 1: ご希望のご連絡方法をお知らせください。

モバイル アプリ

モバイル アプリをどのような用途で使用されますか?

確認のため通知を受け取る

確認コードを使用する

これらの確認方法を使用するには、Microsoft Authenticator アプリをセットアップする必要があります。

セットアップ **通知と確認コード用にモバイル アプリが構成されました**

次へ

⑫モバイルアプリに届いた通知を開くと、自動的にモバイルアプリが起動し承認を要求されるため、「承認」を押す。

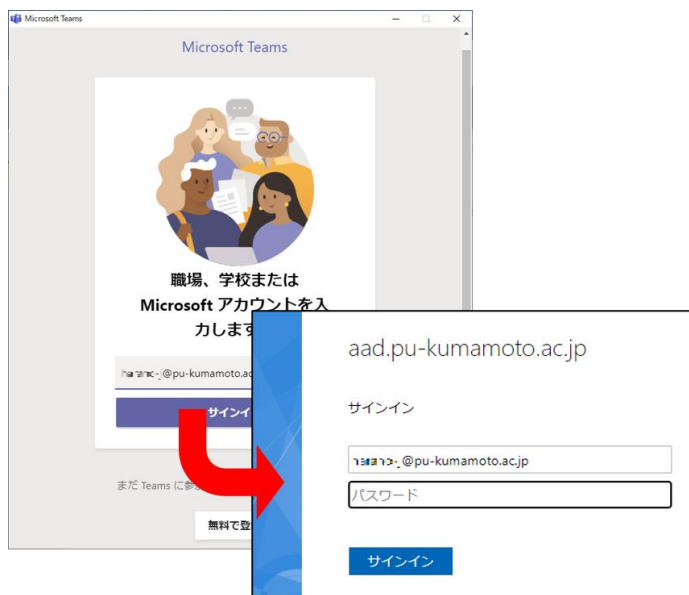


⑬「確認に成功しました」と表示されたあと、自動的に「手順3：モバイルアプリにアクセスできなくなった場合」に進む。
必要に応じて電話番号を登録し、「完了」を押して終了する。



B. 次回以降の認証手順

①Office 365 サービスに学内アカウント・パスワードでログインする（以下は Teams の例）。

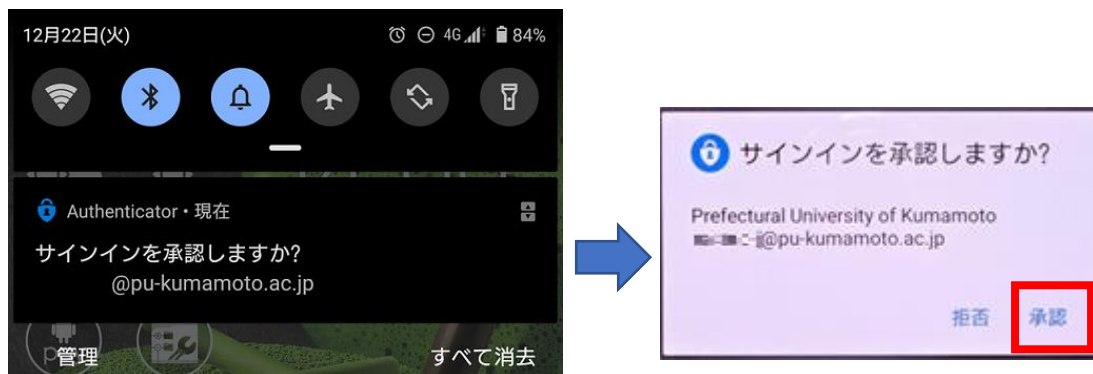


②以下の画面に遷移すると同時に、モバイルアプリに承認要求の通知が送信される。



※「今後 14 日間はこのメッセージを表示しない」にチェックすると、ログインする端末を信頼し、二要素認証が 14 日間行われないため便利。

③モバイルアプリに届いた通知を開くと、自動的にモバイルアプリが起動し承認を要求されるため、「承認」を押す。

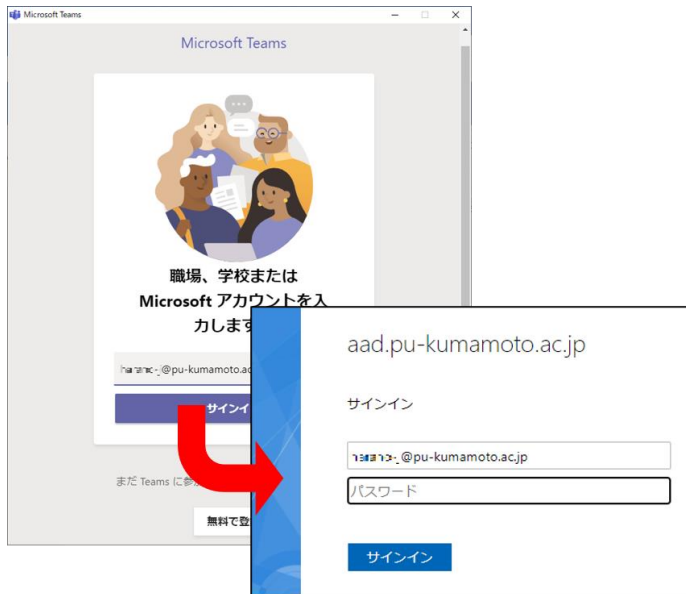


④認証が完了すると、自動的にログイン対象のサービス画面に遷移する。

4. モバイルアプリ「Microsoft Authenticator」に表示されたコードを入力

A. 初回登録手順

- ①Office 365 サービスに学内アカウント・パスワードでログインする（以下は Teams の例）。



- ②「詳細情報が必要」との表示が出るため、「次へ」を押す。



③「追加のセキュリティ確認」画面が表示される。手順1のプルダウンから「モバイルアプリ」を選択する。最初に「セットアップ」を押し、Microsoft Authenticator アプリのセットアップを行う。

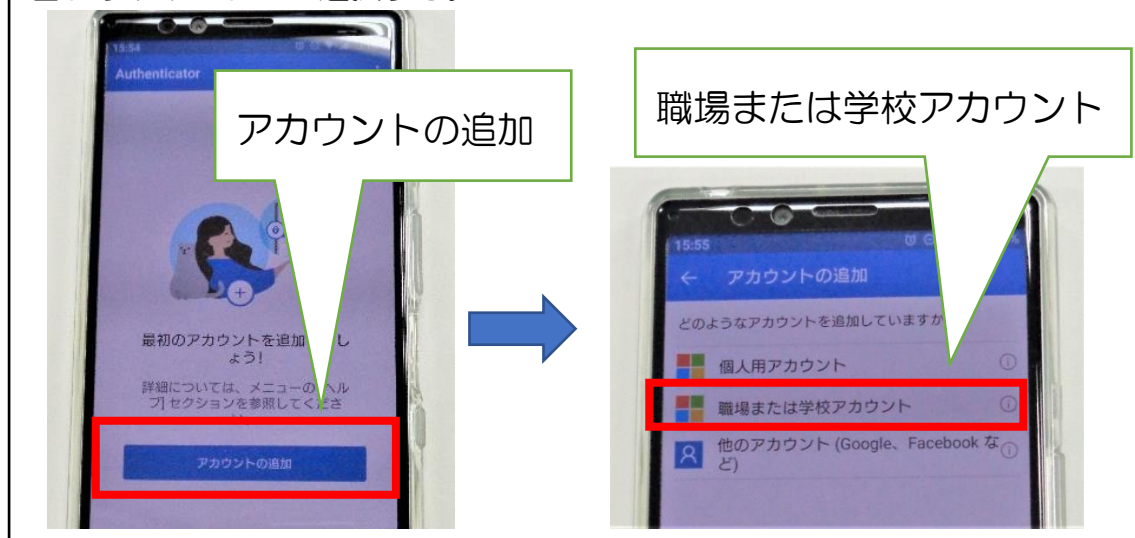
④「モバイルアプリケーションの構成」画面が表示される。まず、AppStore や Google Play Store からアプリケーションのダウンロードを行う。「Microsoft Authenticator」でストア内検索をするとよい。

⑤アプリインストール後、初期画面が表示される。プライバシーポリシーへ「同意します」を選択する（左画面）。その後、右画面に遷移するため、「QRコードをスキャンします」を選択する。



※本画面は初回起動時のみ表示される。

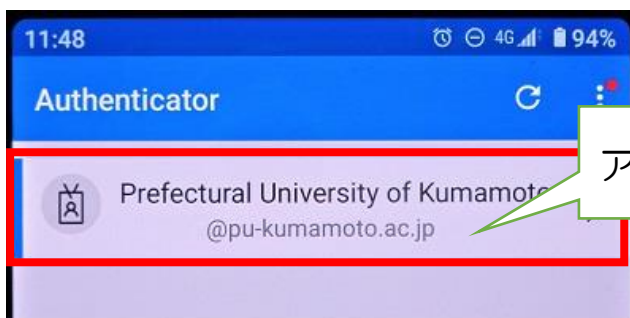
アプリを立ち上げなおしたり、アカウントの再連携を行う場合は、ホーム画面より以下のように選択する。



⑥「モバイルアプリケーションの構成」画面の QR コードをスキャンする。



⑦アカウントの追加が完了し、アプリのホーム画面に自分のアカウントが表示された状態となる。



⑧アカウントを選択すると、以下の画面のようにコードが表示される。この表示により正しくアプリと Office 365 アカウントが連携できていることが確認できる。



⑩ 「モバイルアプリケーションの構成」画面の「次へ」を押す。

モバイル アプリケーションの構成

次の手順でモバイル アプリケーションを構成してください。

1. Windows Phone、Android、または iOS の Microsoft Authenticator アプリをインストールします。
2. アプリでアカウントを追加し、「職場または学校アカウント」を選択します。
3. 下の画像をスキャンしてください。



画像をスキャンできない場合は、アプリケーションに次の情報を入力してください。
コード: 398 581 303
URL: <https://mobileappcommunicator.auth.microsoft.com/mac/MobileAppCommunicator.svc/184188947>

アプリケーションに 6 桁のコードが表示されている場合、[次へ] を選択します。

次へ キャンセル

⑪ 「追加のセキュリティ確認」画面に戻る。「モバイルアプリケーションが構成されました」とメッセージが出ていることを確認する。

「モバイルアプリをどのような用途で使用されますか？」の「**確認コードを使用する**」にチェックし、「次へ」を押す。

Microsoft

追加のセキュリティ確認

パスワードに電話の確認を追加することにより、アカウントを保護します。アカウントをセキュリティで保護する方法についてビデオを見る

手順 1: ご希望のご連絡方法をお知らせください。

モバイル アプリ

モバイル アプリをどのような用途で使用されますか?

確認のため通知を受け取る

確認コードを使用する

これらの確認方法を使用するには、Microsoft Authenticator アプリをセットアップする必要があります。

セットアップ **通知と確認コード用にモバイル アプリが構成されました。**

次へ

⑫モバイルアプリを起動後、自身のアカウント内に表示された6桁のコードを入力し、「確認」を押す。

Microsoft

追加のセキュリティ確認

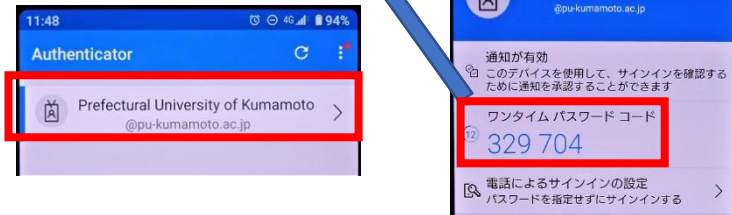
パスワードに電話の確認を追加することにより、アカウントを保護します。 [アカウントをセキュリティで保護する方法についてビデオを見る](#)

手順 2: モバイル アプリから確認パスワードを入力してください

アプリケーションに表示されている確認コードを入力してください。

キャンセル 確認

(モバイルアプリホーム画面)



⑬自動的に「手順 3：モバイルアプリにアクセスできなくなった場合」に進む。必要に応じて電話番号を登録し、「完了」を押して終了する。

Microsoft

追加のセキュリティ確認

パスワードに電話の確認を追加することにより、アカウントを保護します。 [アカウントをセキュリティで保護する方法についてビデオを見る](#)

手順 3: モバイル アプリにアクセスできなくなった場合

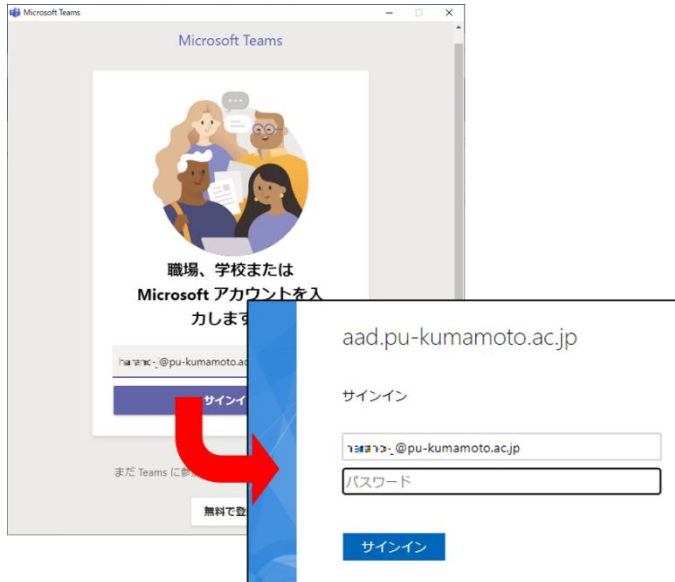
国/地域を選択してください

完了

電話番号はアカウントのセキュリティのためにのみ使用されます。標準の電話料金と SMS 料金が適用されます。

B. 次回以降の認証手順

①Office 365 サービスに学内アカウント・パスワードでログインする（以下は Teams の例）。



②以下の画面に遷移する。モバイルアプリを起動後、自身のアカウント内に表示された6桁のコードを入力する。



※「今後 14 日間はこのメッセージを表示しない」にチェックすると、ログインする端末を信頼し、二要素認証が 14 日間行われなため便利。

③認証が完了すると、自動的にログイン対象のサービス画面に遷移する。