多要素認証-追加マニュアル（OTP Manager）

電話番号などの認証方法を設定済みで、Mac PCにOTP Managerを追加する場合のマニュアルです。

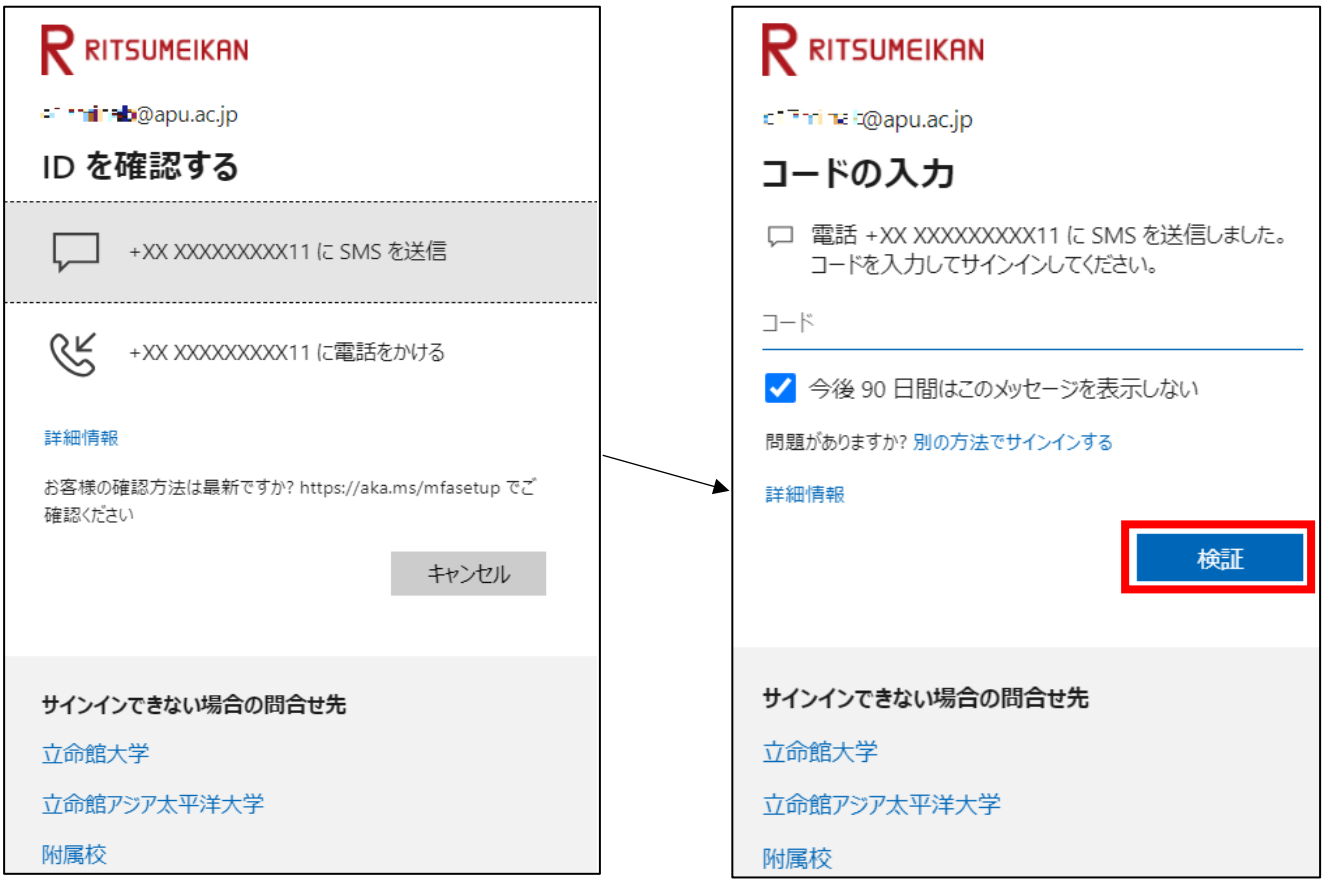
STEP.1 OTPソフトウェア［OTP Manager］をインストール する

❶AppStoreから［OTP Manager］をインストールします。

STEP.2 OTP Managerを認証方法として追加設定する

Webブラウザー

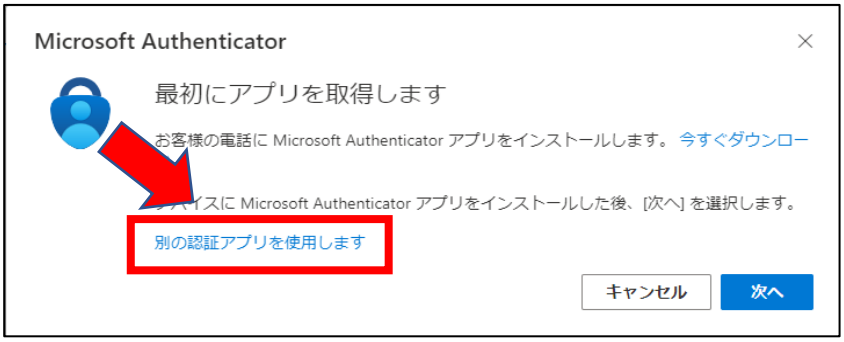
❶ Webブラウザーで [多要素認証設定ページ（https://aka.ms/mfasetup）](https://aka.ms/mfasetup) にAPUのメールアドレスとパスワードでサインインします。
すでに設定済みのデバイスなどへ認証の確認がありますので、自分の設定に基づき認証してください。
（下の画像は、電話番号をすでに設定済みの場合の例です）



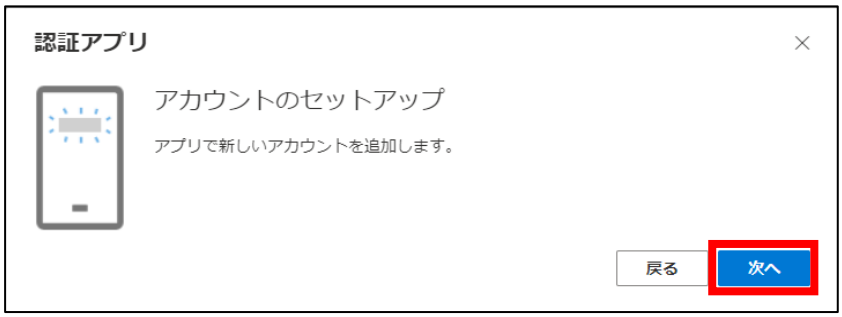
❷［セキュリティ情報］の画面が開きますので、［＋サインイン方法の追加］をクリックします。

❸［サインイン方法を追加］の画面で［Microsoft Authenticator］をクリックします。

❹［最初にアプリを取得します］画面が表示されたら、**このマニュアルではOTP Managerを使用する認証方法を追加するので、［別の認証アプリを使用します］をクリック**します。



❺［アカウントのセットアップ］画面で［次へ］をクリックします。

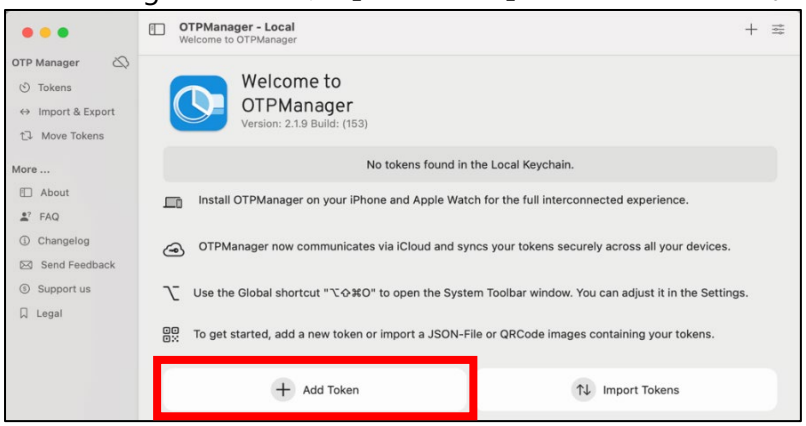


❻［QRコードをスキャンします］画面で［画像をスキャンできませんか？］をクリックします。

❼［アカウント名］と［秘密鍵］が表示されるので［秘密鍵］をコピーします。

OTP Manager

❽OTP Managerを起動し、［Add Token］をクリックします。

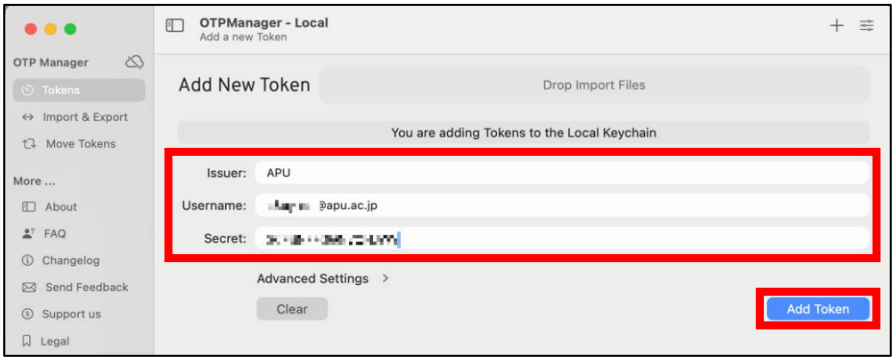


❾OTP Managerの［Add New Token］画面で以下の通り入力し、［Add Token］をクリックします。

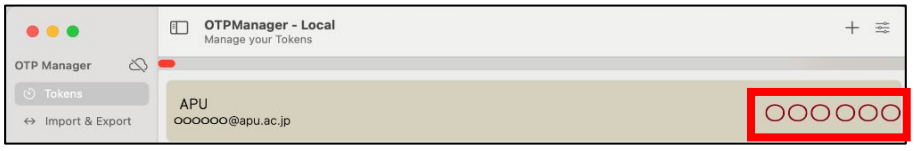
Issuer：APU

Username：APUのメールアドレス

Secret：❼の秘密鍵



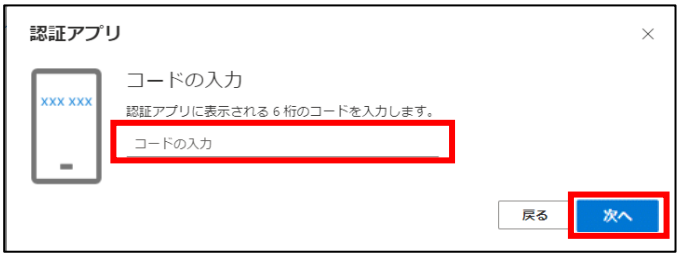
❿OTP Managerの画面に6桁の数字が表示されたことを確認します。



Webブラウザー

⓫Webブラウザーの［QRコードをスキャンします］画面で［次へ］をクリックします。

⓬［コードの入力］画面で⓾の6桁の数字を入力し、［次へ］をクリックします。



⓭［セキュリティ情報］の画面に［認証アプリ］が追加されていることが確認できたら設定完了です。
OTP ManagerとWebブラウザーを閉じてください。

❗セキュリティリスク軽減のため、認証アプリの利用が推奨されています。
既定のサインイン方法が［Authenticatorアプリまたはハードウェアトークン-コード］になっていることをご確認ください。

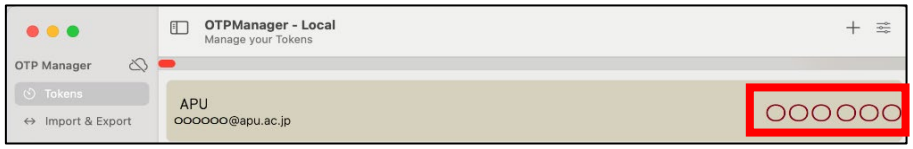
STEP.3 OTP Managerを利用してのサインイン方法

スマートフォンの機種変更などでMicrosoft Authenticatorの利用ができなくなった際や電話番号が変わり認証が受けられなくなった際はこのマニュアルで登録したOTP Managerで通知を受けることが可能です。

自宅や公共の無線LAN（Wi-Fi）や携帯電話回線など学外ネットワークからサインインする場合に多要素認証が要求されます。

OTP Manager

❶OTP Managerを起動します。

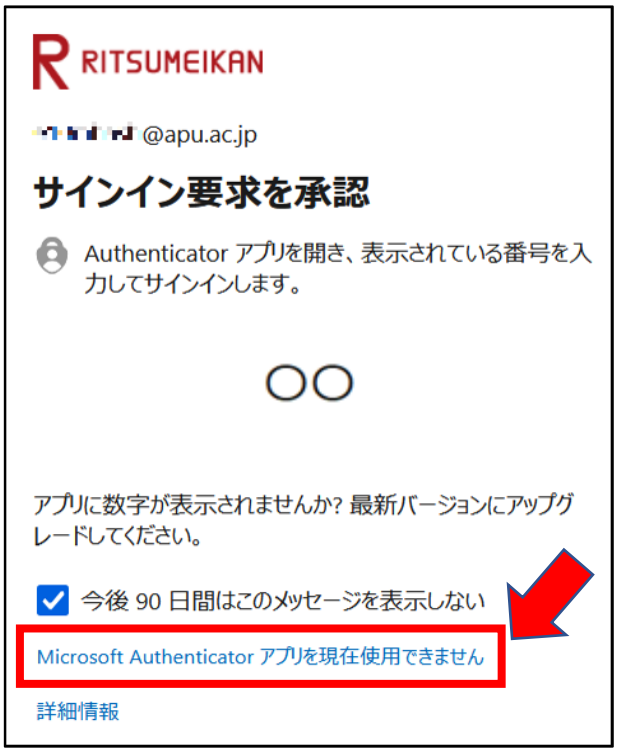


Webブラウザー

❷ APUの認証画面でメールアドレス、パスワードを入力し、［サインイン］をクリックします。

❸［サインイン要求を承認］画面の［Microsoft Authenticatorアプリを現在使用できません］をクリックします。

❗既定の認証方法が電話となっている場合は❹へ進んでください。



❹［確認コードを使用する］をクリックします。

（下の画像は、Microsoft Authenticatorをすでに設定済みの場合の例です）

❺Webブラウザーに［コードの入力］と表示されるので、OTP Managerに表示されている6桁の数字を入力し、［検証］をクリックしてください。

❗以下の通り多要素認証情報を記憶させることができます。

・Webブラウザー：サインイン時［今後90日間はこのメッセージを表示しない］にチェックすると90日間

・デスクトップアプリケーション：上記に関わらず一度の認証で長期間

（一部のデスクトップアプリケーションはWebブラウザーと同じ動作をします）