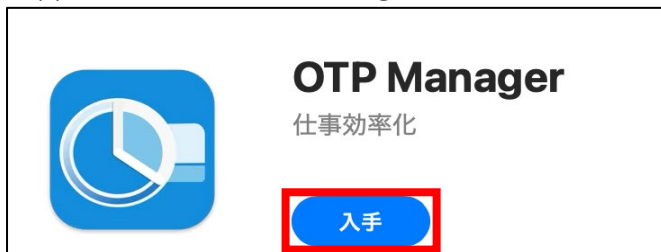


## 多要素認証-追加マニュアル (OTP Manager)

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

① AppStore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

① Webブラウザで [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)



② [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。



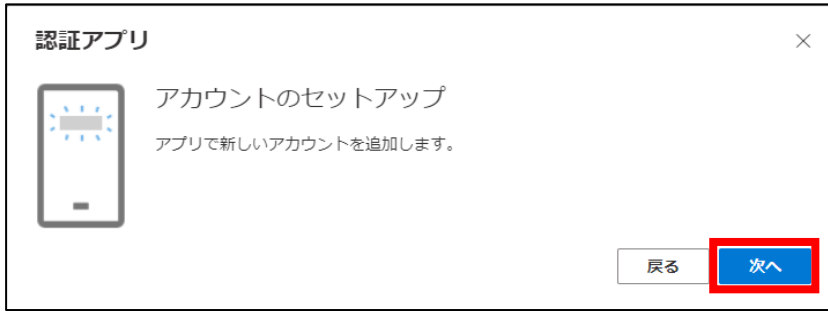
③ [サインイン方法を追加] の画面で [Microsoft Authenticator] をクリックします。



④ [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。



- ⑤ [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。



- ⑥ [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。

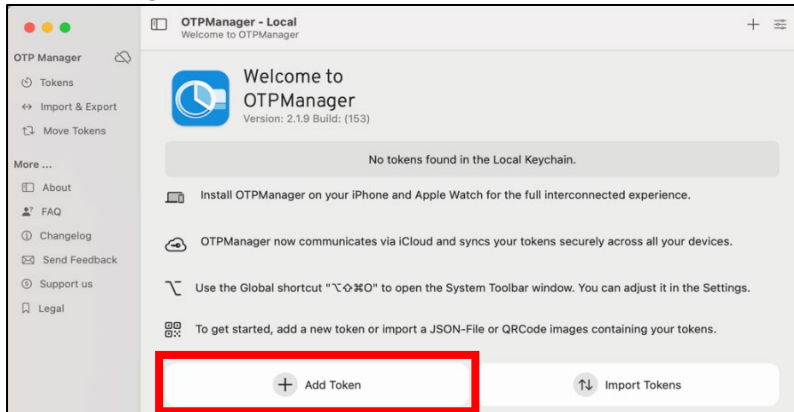


- ⑦ [アカウント名] と [秘密鍵] が表示されるので [秘密鍵] をコピーします。



## OTP Manager

⑧ OTP Managerを起動し、 [Add Token] をクリックします。

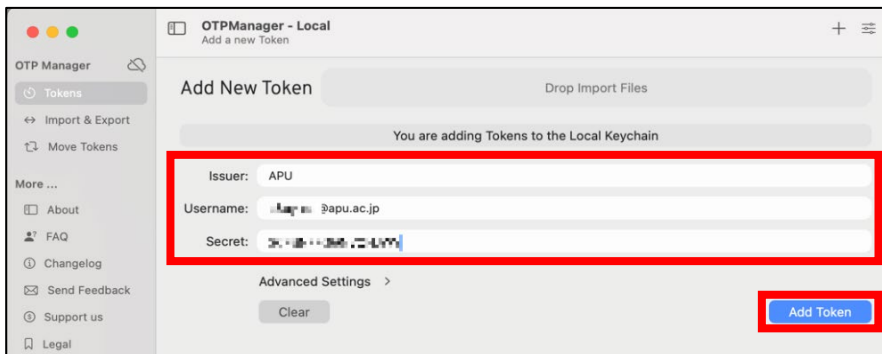


⑨ OTP Managerの [Add New Token] 画面で以下の通り入力し、 [Add Token] をクリックします。

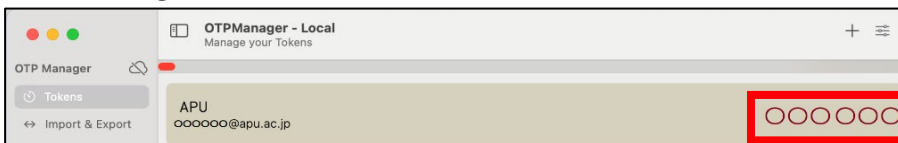
Issuer : APU

Username : APUのメールアドレス

Secret : ⑦の秘密鍵



⑩ OTP Managerの画面に6桁の数字が表示されたことを確認します。

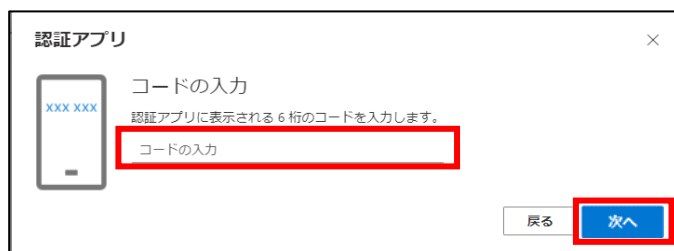


## Webブラウザ

- ⑪ Webブラウザの [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。



- ⑫ [コードの入力] 画面で⑩の6桁の数字を入力し、[次へ] をクリックします。



- ⑬ [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

① OTP Managerを起動します。



### Webブラウザ

② 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。

③ [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④へ進んでください。



④ [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)

The screenshot shows the RITSUMEIKAN login interface. At the top, the logo and email address '@apu.ac.jp' are visible. Below this, the heading 'IDを確認する' is present. A section for Microsoft Authenticator is shown with the text 'Microsoft Authenticator アプリで要求を承認する'. A red box highlights the option '123 確認コードを使用する', with a red arrow pointing to it. Below this, there is a '詳細情報' section with a link to 'https://aka.ms/mfasetup' and a 'キャンセル' button. At the bottom, there is a 'サインインできない場合の問合せ先' section with links for '立命館大学', '立命館アジア太平洋大学', and '附属校'.

⑤ Webブラウザに [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。

The screenshot shows the RITSUMEIKAN login interface for code entry. The heading is 'コードの入力'. Below it, there is a message: 'モバイル デバイスの認証アプリに表示されているコードを入力してください'. A red box highlights the 'コード' input field. Below the input field, there is a checkbox labeled '今後 90 日間はこのメッセージを表示しない' which is checked. A '詳細情報' link is visible below the checkbox. A blue '検証' button is located at the bottom right of the form area. At the bottom, there is a 'サインインできない場合の問合せ先' section with links for '立命館大学', '立命館アジア太平洋大学', and '附属校'.

📌 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：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ブラウザと同じ動作をします)