

2 要素認証の有効化後の学外ネットワークからの初期設定方法

(PC およびスマートフォンでの設定)

本学では、2022 年後期途中より 2 要素認証を運用しています。概要やマニュアルなど詳細については、以下のサイトを確認してください。

<https://web.otani.ac.jp/mfa>

2 要素認証を利用するにあたり、必ず個人で初期設定を行う必要があります。このマニュアルは、以下の場合の設定の際に利用してください。

・大学が有効化を行った後に、自宅など学外のネットワークで初期設定を行う場合

1. 学内 LAN 以外の回線(自宅など)に接続し、自身の所持している PC など（スマホのみで設定する場合は別マニュアルを参照）で、大学 HP(<https://www.otani.ac.jp>)の下部、「在学生・留学生の方」のリンク内「大谷大学 Web mail」からもしくは、次の URL から Web メールにアクセスする

<http://webmail.otani.ac.jp>

大学の認証ページが表示されるので、以下の情報を入力する

ユーザ名： ounet アカountのユーザ名

パスワード：ounet アカountのパスワード

ounet アカountのユーザ名、パスワードは OTANI UNIPA と同じ



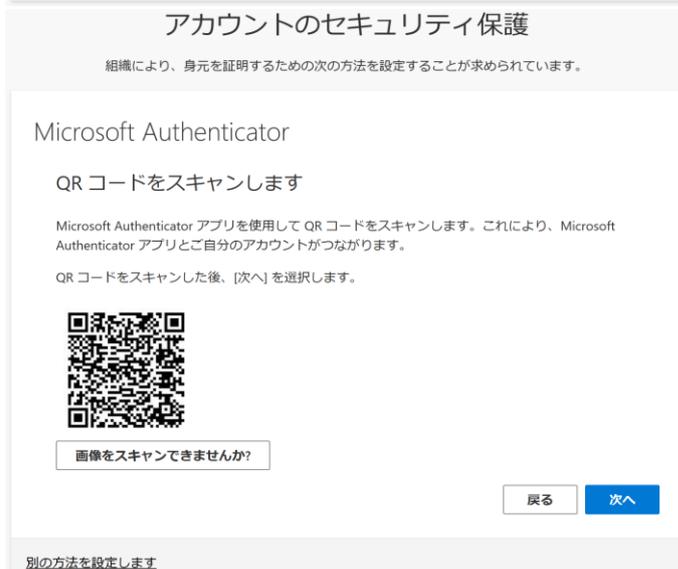
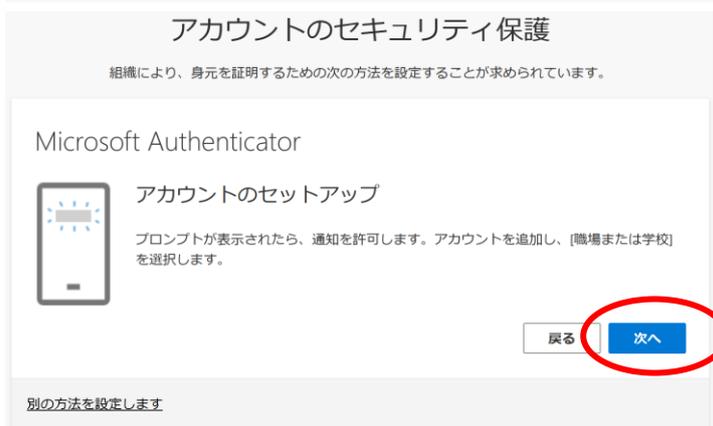
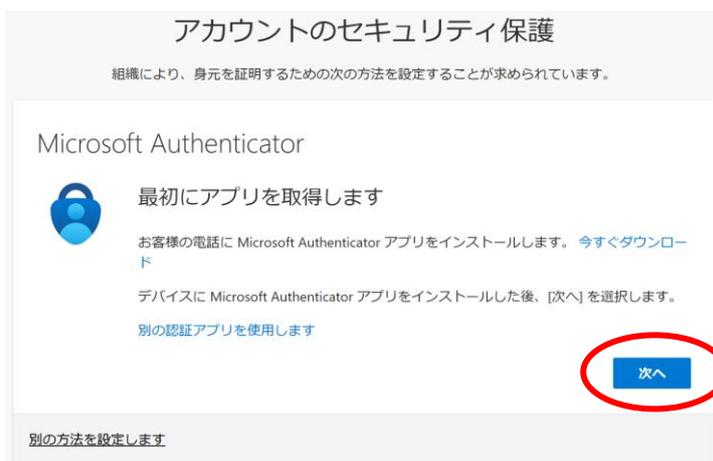
ユーザー名とパスワードを入力してください。

サインイン

2. 以下のようなウィンドウが表示され追加の情報を求められるので「次へ」をクリック



3. パスワード以外に2要素目の認証を行うため、表示される画面に従って設定を行います。画面の表示に従い、スマートフォンにMicrosoft Authenticator アプリをインストールしますが、いったん「次へ」を2回クリックし、QRコードが表示される画面まで進めてください。QRコードが表示されたら次はスマートフォンを操作しますので、画面はそのままにしておいてください。



この画面で手順4へ

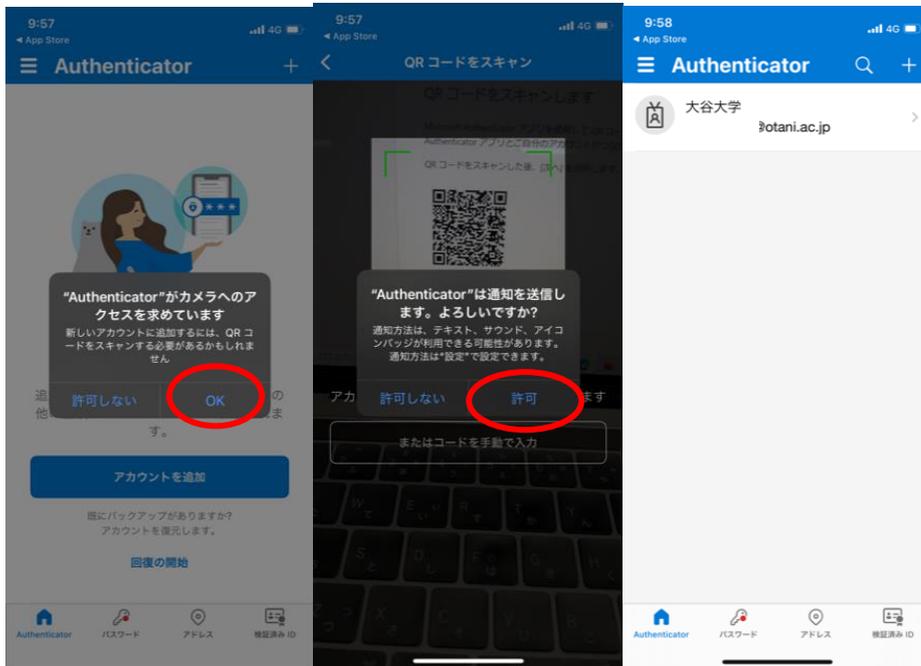
4. 次にスマートフォンの方で操作を行います。スマートフォンで、認証用アプリである「Microsoft Authenticator」を検索し、インストールします。似たようなアプリもありますので、間違えてインストールしないようご注意ください。



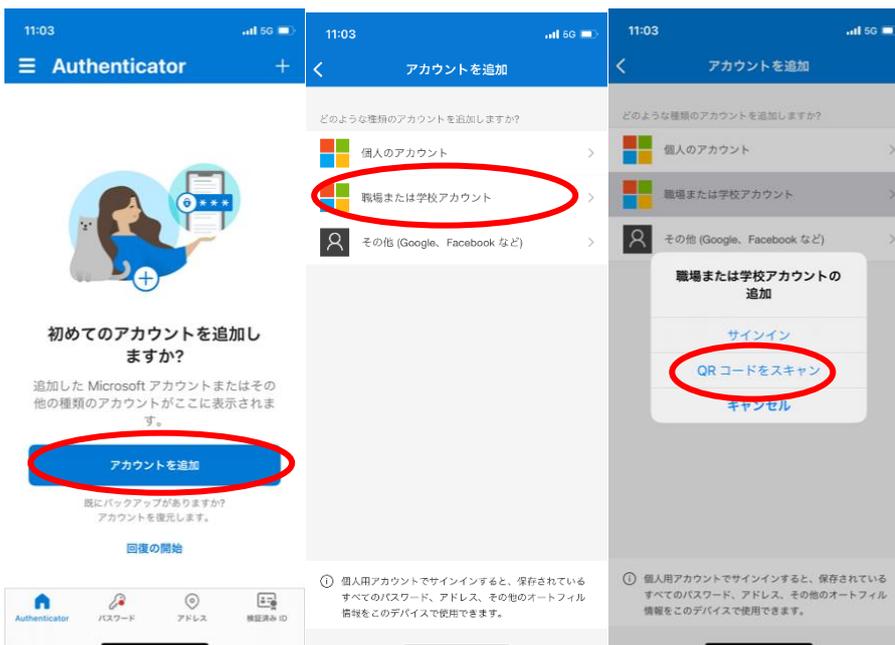
5. Microsoft Authenticator アプリを起動します。「承諾する」をタップします。次の画面に遷移しますので、「続行」をタップします。先ほどの手順3の画面では「職場または学校のアカウント」からアカウントの追加を行うよう促されていますが、「QRコードをスキャンします」をタップします。



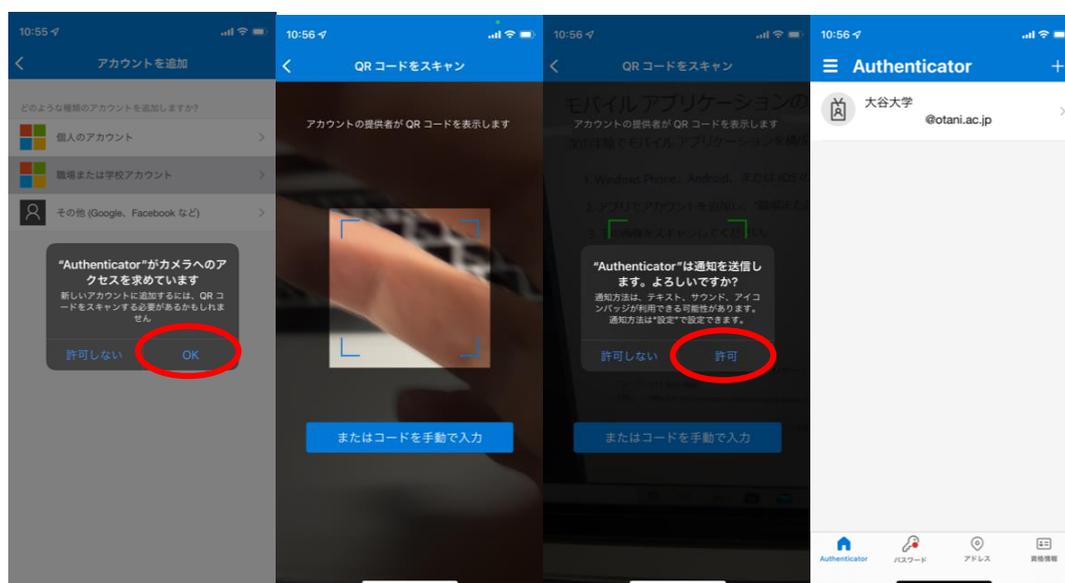
6-1. 手順3でPC側に表示した画面のQRコードをスキャンします。なお、QRコードをスキャンするために、カメラのアクセスは許可とし、通知についてもアプリの動作に必要で、必ず「許可」をタップしてください。アカウント名が表示され、アプリ側の設定は完了ですが、次にPC側の操作が必要となり、手順7に進んでください。



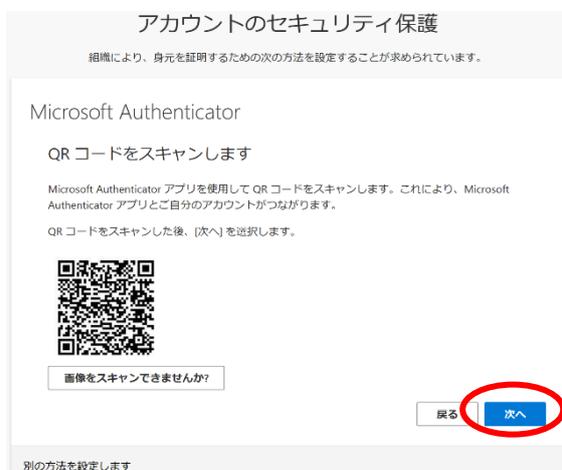
6-2. なお、6-1はアプリのインストール後すぐの画面から進める方法ですが、一度アプリを閉じた後の追加など、初期の設定時以外は次のような画面で進めます。「アカウントを追加」をタップし、「職場または学校アカウント」をタップし表示される「QRコードをスキャン」を選択する。



カメラの許可を聞かれますので、許可します。カメラが動き、QRコードのスクリーンを行います。通知の許可を聞かれますので「許可」してください。設定が登録されます。



7. 次に、引き続き PC 端末側の設定となります。QRコードの画面が表示されている状態ですので、「次へ」をクリックします。



8. 試してみましようという画面が表示され、2桁の数字が表示されます。



9. 次にスマートフォン側で、Microsoft Authenticator のアプリの通知が届きますので、8の手順で表示された2桁の数字を入力して「はい」をタップします。「はい」の位置は毎回変わりますので、間違えないように注意してください。また、自身がメールや Teams などにアクセスしようとしていない状況であれば、「いいえ、私はしていません」を選択してください。



10. 再度 PC 側の画面を確認すると、スマートフォンで認証を行ったため、「通知が承認されました。」という表示が出ますので、「次へ」をタップします。



11. 以上で2要素認証のアプリの設定は完了となります。「完了」をクリックします。



本設定はクラウドに保存されているため、端末やアプリごとに初期設定をおこなう必要はありません。この初期設定さえ行えば、必要な場面で2要素認証を求められるため、求められた場合に認証アプリで許可を行う形となります。

2要素認証における設定の変更や更新、削除などについては、別のマニュアルを準備していますので、以下より参照してください。

<https://web.otani.ac.jp/mfa>

また、2要素認証について問題がある場合は、総合研究室、情報サポート室の情報教育アシスタントまたは、響流館 1F 情報処理準備室(教育研究支援課事務室)までお問い合わせください。

ounet@sec.otani.ac.jp