2024 年 4 月 23 日
教育研究支援課
情報システム

2 要素認証の事前設定について

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。

・大学側で 2 要素認証を有効化する前に 2 要素認証の初期設定を事前に行う場合

・大学が有効化を行った後に、学内 LAN に接続して初期設定を行う場合

アプリと電話の登録方法となります。手段が 1 つだけの場合、障害が発生した際、アクセス不可となってしまいますので、アプリと電話の両方を設定することを推奨しています。

1. まずは PC での操作となります。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 （※URL 注意 ×https:）

   学外ネットワークの場合、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 アカウントのユーザ名

   パスワード：ounet アカウントのパスワード

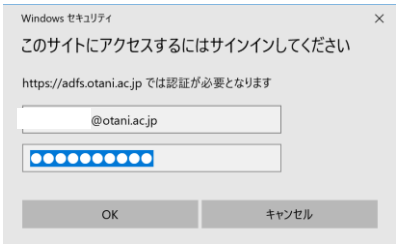
   （ounet アカウントのユーザ名、パスワードは OTANI UNIPA と同じ）

   学内 LAN に接続している場合は、以下の情報を入力してください。

   ユーザ名： ounet アカウントのユーザ名@otani.ac.jp

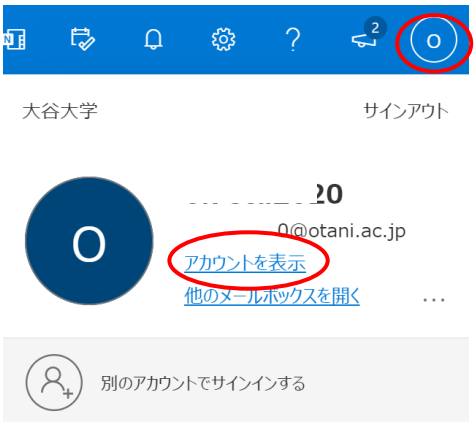
   パスワード：ounet アカウントのパスワード

   (ユーザー名の後に@otani.ac.jp が必要となります)

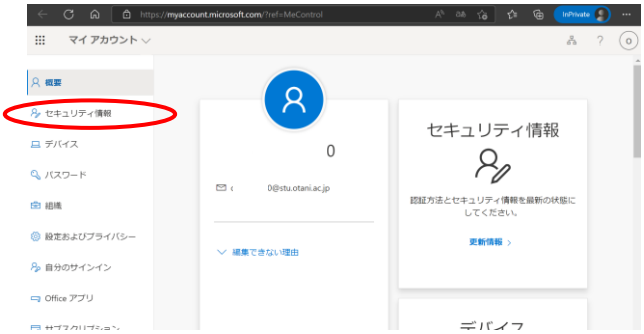


2024 年 4 月 23 日
教育研究支援課
情報システム

2. Web メールが開きますので、右上のアイコンをクリックし、「アカウントを表示」をクリックします。



3. マイアカウントのメニューページに遷移しますので、「セキュリティ情報」をクリックします。

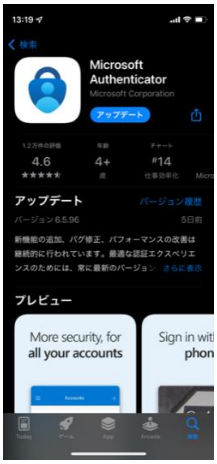


4. 以下の画面が表示されますので、サインイン方法の追加をクリックします。

5. サインイン方法の追加の画面が出ますので、追加したい認証方法を選択します。

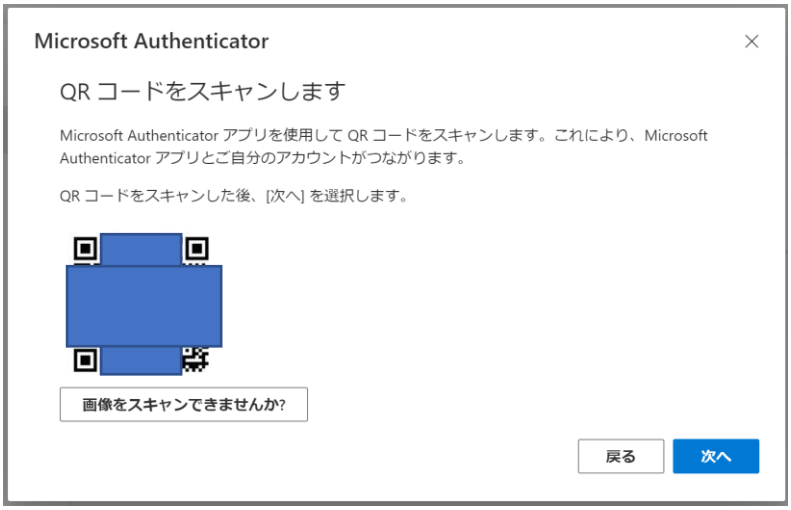
6. このマニュアルでは大学推奨の「認証アプリ」を選択します。「追加」をクリックします。(電話の登録は p7 の手順 13 からを参照)

7. アプリのインストールの指示が表示されますので、認証を行うスマートフォンに Microsoft Authenticator のアプリをインストールしてください。



8. スマートフォン上で通知を求められたら許可を行います。アカウントを追加し、[職場または学校]とありますが、いったんそのまま「次へ」をクリックします。

9. 自身の PC のブラウザ上にその時生成された自分専用の QR コードが表示されますので、スマートフォンの Microsoft Authenticator アプリで読み取ります



Microsoft Authenticator アプリを起動します。「同意する」をタップします。

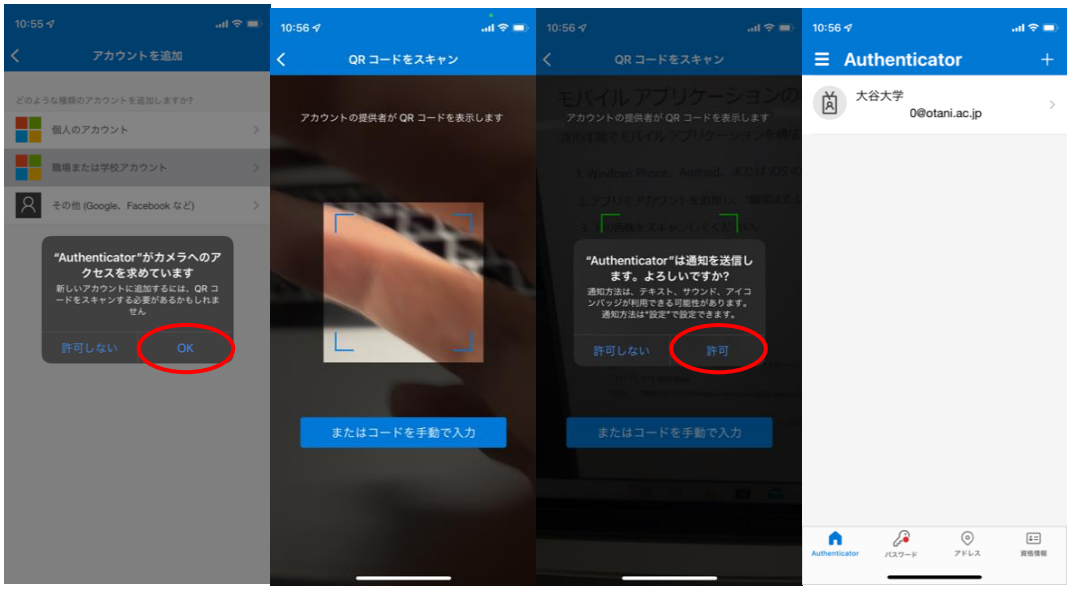
10-1. 先ほどの８の画面では「職場または学校のアカウント」からアカウントの追加を行うよう促されていますが、「QR コードをスキャンします」をタップし、９の画面の QR コードをスキャンしてください。アプリにアカウントが追加され、アプリ側の設定は完了となります。

2024 年 4 月 23 日
教育研究支援課
情報システム

10-2. なお、10-1 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ることとなります。選択も一部異なりますので注意してください。

「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。

カメラのアクセス許可を聞かれますので、許可します。カメラが動き、QR コードのスキャンを行います。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。(**登録はまだ終わっていませんので注意してください**)



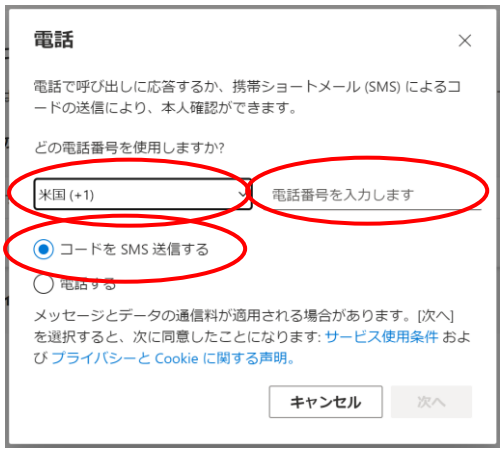
11. PC で「次へ」をクリックすると、PC に 2 桁の数字が表示されます。スマートフォンの Microsoft Authenticator アプリにて 2 桁の数字の入力を求められますので、入力します。入力を行うまで、PC 上では以下の画面が表示されます。

12. スマートフォンアプリで数字 2 桁入力すると、PC の画面で以下の画面が表示されます。

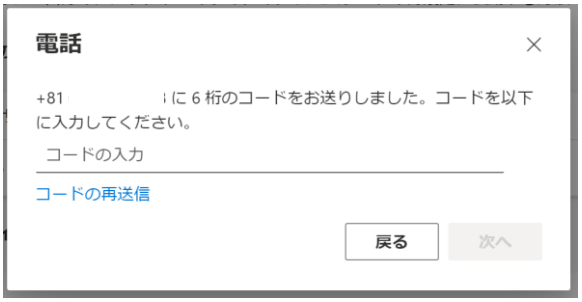
13. 設定が完了し、以下のように設定が表示されます。これで 2 要素認証のアプリの設定は完了です。ただし、アプリでの障害発生時にアクセスできなくなるリスクを回避するため、アプリに加えて、電話番号も登録を推奨します。

14. 同じように「電話」を追加します。手順 4 および 5 を行い、電話を選択し、「追加」をクリックします。

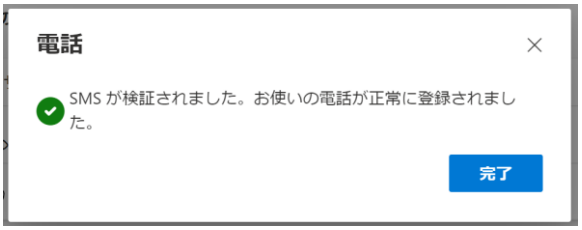
15. 電話番号を入力し、SMS でコードを受けるか、電話の着信でコードを聞くか選択します。電話番号については、左は国コードで「日本(+081)」を選択してください。
右側の「電話番号を入力します」の部分に、電話番号を入力してください。
例えば、携帯電話なら 090 など省略なしに入れてもらえば問題ありません。
コードの取得は SMS を推奨しています。入力後、「次へ」をクリックします。



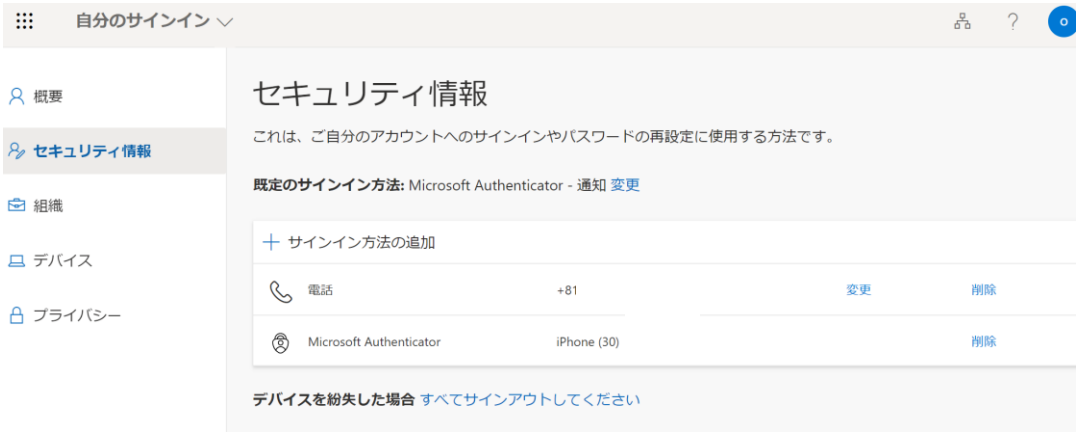
16. コードが送られてきますので、入力して「次へ」をタップします。



17. 登録が完了しましたので、「完了」をクリックします。



18. 電話も追加されていることを確認して、設定完了となります。



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認証での許可を行うか、SMS で届いたコードを入力するかしていただく形となります。

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