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(スマホのみでの設定方法)

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

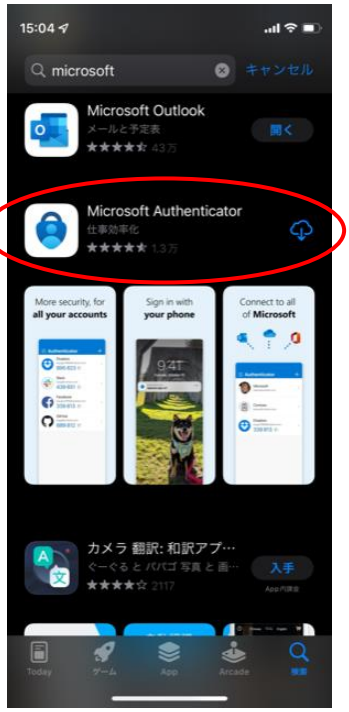
2 要素認証を利用するにあたり、必ず個人で初期設定を行う必要があります。このマニュアルは、以下の場合の設定の際に利用してください。

・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

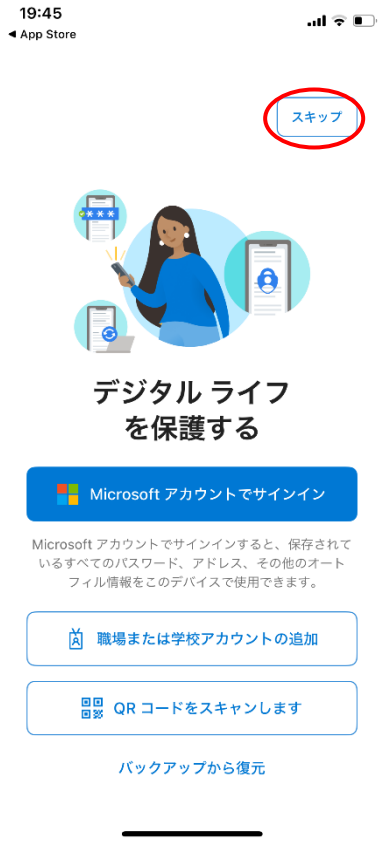
アプリと電話の登録方法となります。手段が 1 つだけの場合、障害が発生した際、アクセス不可となってしまいますので、アプリと電話の両方を設定することを推奨しています。特に電話を登録しておくと、電話番号を変えずに機種変更するならば、新しい機種でもそのままショートメッセージで認証することは可能です。

1. はじめにスマートフォンの認証アプリでの設定方法を案内します。まずは、認証のためのアプリとして、「Microsoft Authenticator」をスマートフォンにインストールしてください。(よく似たアプリがありますので、間違えないよう注意してください。)
   (アプリが利用できずに電話での登録のみを希望の場合は、手順５から始めてください。)



2. インストールが完了したら、アプリを起動します。「承諾する」をタップし、次の画面で「続行」をタップします。

3. 次の設定画面に遷移しますが、右上の「スキップ」をタップします。



4. 以下の画面まで進んだら、いったんアプリでの操作は完了です。

5. 次にブラウザでインターネット接続を行います。スマートフォンのブラウザで office.com にアクセスします。

   https://www.office.com

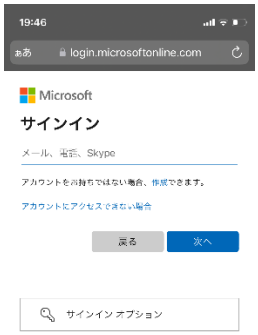
   google 検索などから、office.com を検索していただいてもアクセスできます。
   右上の人のアイコンをタップします。

2024 年 4 月 23 日
教育研究支援課
情報システム

6. サインインの画面に移行しますので、以下の情報を入力してください。

ounet アカウントのユーザー名@otani.ac.jp

ounet アカウントのユーザー名は、OTANI UNIPA のユーザー名と同じです。
入力後、「次へ」をタップします。



7. 次に、大学の認証ページが表示されますので、以下の情報を入力してください。

ユーザー名：ounet アカウントのユーザー名@otani.ac.jp

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ー名およびパスワードは、OTANI UNIPA と同じです。
「サインイン」をタップします。

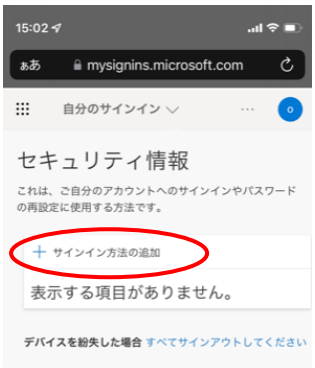
8. サインインを維持するか確認の画面が表示されますので、現在サインした大学のアカウントしか利用しないということであれば、「はい」をタップすると、その後必要になる認証の回数が減ります。（いいえ、はい、どちらを選択しても構いません。）

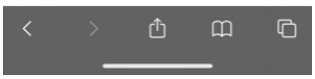
9. サインインが完了すると、以下のようなページに移行します。
右上のアイコンをタップします。

10.以下のようなメニューが右上部に表示されますので、「アカウントを表示」をタップします。

11.以下のようなメニュー画面が表示されますので、セキュリティ情報の部分の、「更新情報」のリンクをタップします。

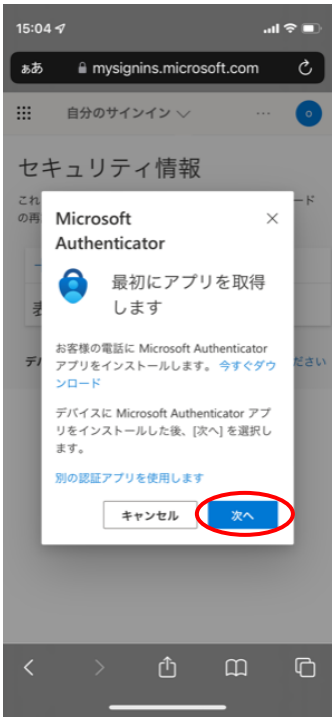
12.次に、セキュリティ情報のページが表示されますので、「サインイン方法の追加」をタップします。



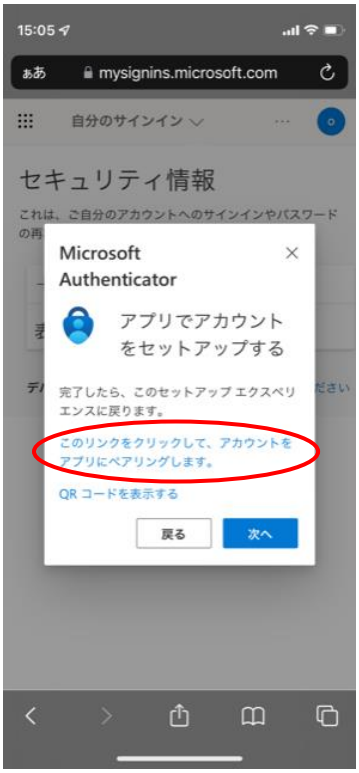


13.まずは、アプリでの認証方法の追加方法を示します。「認証アプリ」を選択して、「追加」をタップします。（アプリが利用できない電話番号の登録のみの方は、手順 23 へお進みください。）

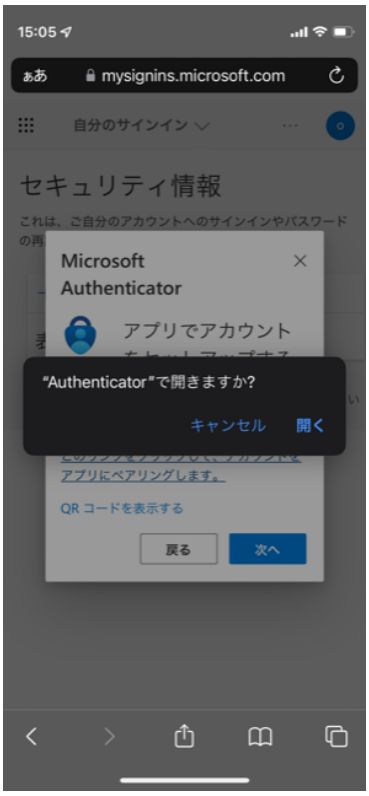
14. アプリのインストールを促す画面が表示されます。「Microsoft Authenticator」アプリを、インストール済みですので、「次へ」をタップします。



15. 次に、以下の画面が表示されます。、「このリンクをクリックして、アカウントをアプリにペアリングします。」をタップします。



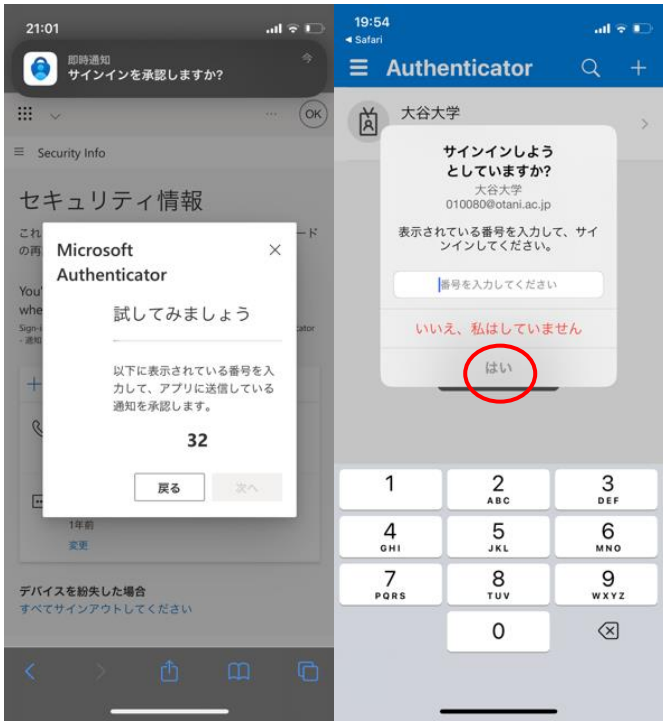
16. Authenticator で開きますか？と表示されますので「開く」をタップします。



17. アプリ側で通知の許可など表示されますので、「許可」をタップします。

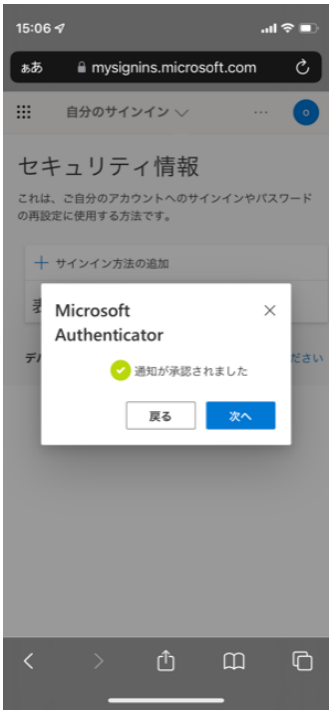
18. 次にアプリのロックが有効になります。「OK」をタップします。

19. ブラウザ側に戻ると、「試してみましょう」の画面が表示され 2 桁の数字が表示されます。アプリから、サインインの承認の通知が届きますので、2 桁の数字を入力して「はい」をタップします。

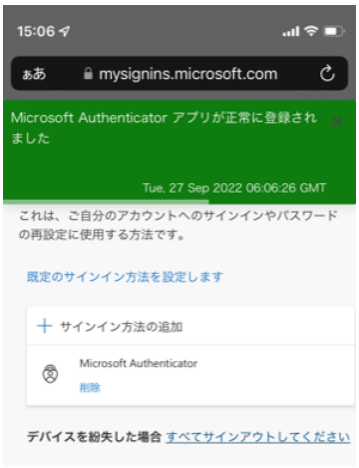


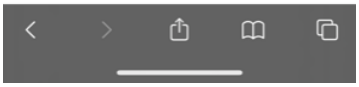
20. アプリ側で、機種によって Face ID の使用許可が問われます。パスコード以外に Face ID も許可する場合は、「OK」をタップしてください。

21. 通知から許可を行うと、通知が承認されましたと表示されますので、「次へ」をタップします。

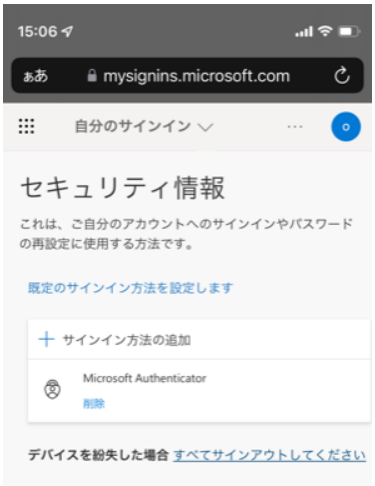


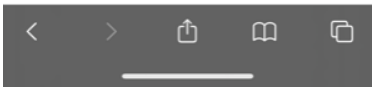
22. 以上で設定が完了し、アプリケーションでの認証設定が登録完了となります。





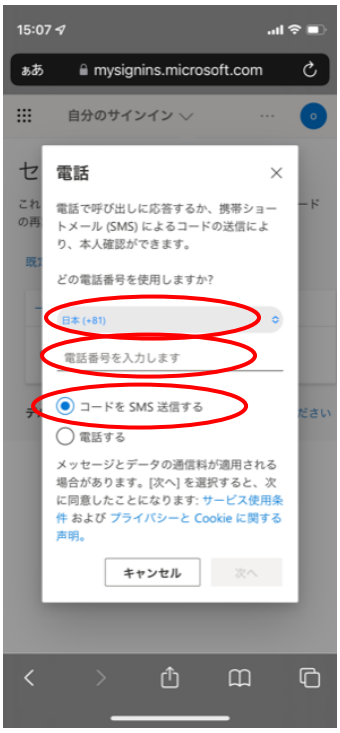
23. 引き続き、電話の登録方法を示します。「サインイン方法の追加」をタップします。



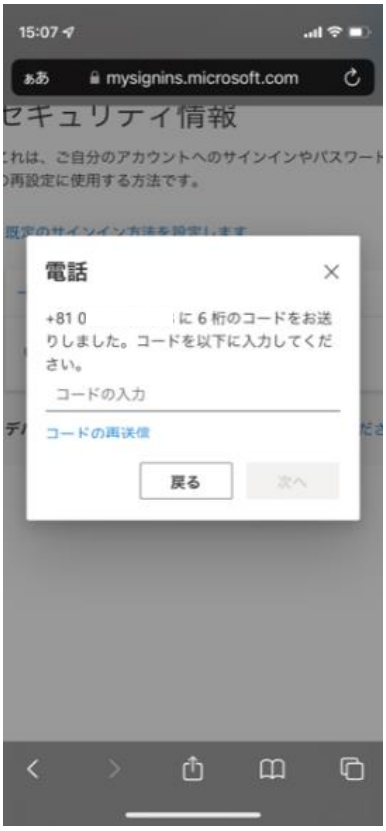


24. 電話を選択し、「追加」をタップします。

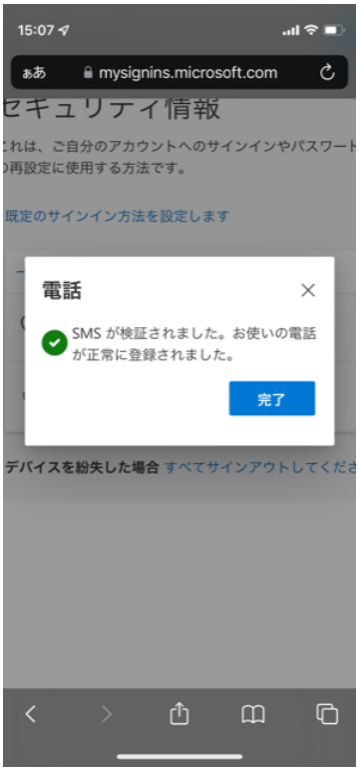
25. 以下の画面が表示されますので、どの電話番号を使用しますか?の下部について、**日本(+081)**を選択します。また、その下の段に電話番号を入力してください。国コードを先ほど選択しましたが、ここの入力については、特に省略などは不要で、通常の携帯電話の電話番号(090-など)を入力してください。SMS(ショートメッセージ)でコードが届く設定を行う場合は、「コードを SMS に送信する」(推奨)を選択してください。コードが電話音声で届く設定を行う場合は、「電話する」を選択します。
「次へ」をタップします。



26. コードが SMS で届きますので、そちらのコードを入力して、「次へ」をタップします。

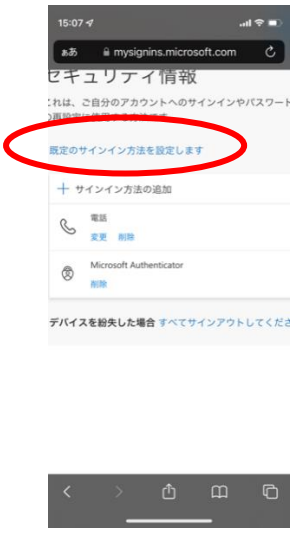


27. 以上で電話番号の登録は完了です。「完了」をタップします。



28. 以上で、アプリ及び電話番号の初期設定は完了となります。電話と Microsoft Authenticator が登録されているのが確認できます。

29. 最後に、既定のサインイン方法を設定します。2 つ以上の認証方法を登録した場合、どの方法を優先して認証を行うか設定することが可能です。「既定のサインイン方法を設定します」をタップします。



30. 認証アプリと電話(SMS)の登録を行った場合、サインインの方法として、以下の中から選択が可能です。自身が設定した認証方法の選択肢が上がってこない場合は、その設定を誤っています。別の認証方法を少なくとも 1 つ追加し、該当の表示されない認証方法を削除して再設定してください。なお、1 種類の登録しかない状態で、それを削除すると次からサインインできなくなる可能性がありますので注意してください。

・電話 – 通話

実際に電話がかかってきて音声でコードを聞き取ります。

・電話 – テキスト

ショートメッセージ(SMS)でコードが送られてくるのでそれで認証します。

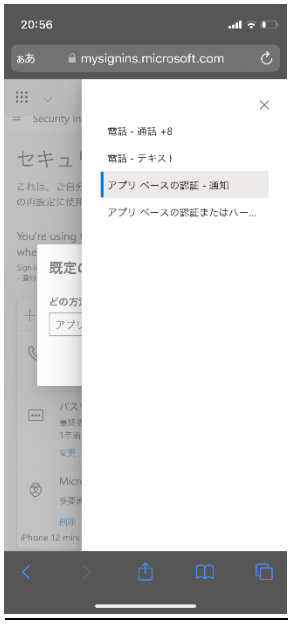
・アプリベースの認証 – 通知

(推奨)スマートフォンの通知で認証が求められます。手軽に利用可能です。

・アプリベースの認証またはハードウェアトークン・コード

Microsoft Authenticator アプリの設定したアカウントに表示されるコードを入力する方法です。ネットワークがつながっていなくても利用できます。ただし、30 秒ごとにコードが変わりますので、利用は少し手間がかかります。

上記から優先される認証を選択してください。アプリベースの認証 –通知もしくは、電話 – テキストの設定が利用しやすいかと思います。既定の方法が設定出来たら 2 要素認証の設定は完了です。



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