多要素認証

（MFA：Multi-Factor Authentication）

2026 年 2 月版

IC-Mail を含む Microsoft365 のサービスを学外から利用する場合は、多要素認証が必須になります。

多要素認証（MFA）とは？

多要素認証（MFA）とは、ログイン時に 2 つ以上の認証要素を組み合わせて本人確認を行う仕組みです。

たとえばこんな組み合わせです：

要素の種類	例
知識情報（知っているもの）	パスワード、PIN
所持情報（持っているもの）	スマートフォン、タブレット
生体情報（本人そのもの）	指紋、顔認証

例：
「パスワード」＋「スマホに送られた認証コード」
「パスワード」＋「顔認証」

なぜ多要素認証（MFA）が必要なのか？

従来は「パスワードだけ」でログインできていましたが、次のような問題があります。
・パスワードの使い回しで漏洩しやすい
・フィッシング詐欺やウイルスで盗まれる
・知らない間に他人がログインしてしまうリスク

MFA を使うことで、仮にパスワードが漏れても、不正ログインを防止できます。
大学・企業・行政機関など、あらゆる組織が多要素認証（MFA）を標準化しています。

多要素認証（MFA）導入のメリット

・セキュリティの大幅向上
・個人情報や業務データの保護
・情報漏えい事故の抑止
・サイバー攻撃への対策

認証方法の例（本学で使用予定の方式）

以下のいずれかの方法で認証を行います：

・Microsoft Authenticator などのアプリで通知を承認 【推奨 1】

・スマートフォンに届くコードを入力（SMS） 【推奨 2】

・電話による自動音声確認 【推奨 2】

・その他（セキュリティキー等）

原則【推奨 1】・【推奨 2】どちらも登録をお願いします。

機種変更や電話番号変更した場合や、いずれかの方法に不具合が発生した場合に、認証ができなくなってしまうため、

2 つ以上の方法を登録してください。

SMS または電話のみ登録の場合は、電話番号が変更になってしまうと認証がおこなえません。

スマホアプリのみ登録の場合は、機種変更をした際に旧機種がないと機種変更後の初回認証がおこなえません。

FAQ

Q. 何度も認証するのは面倒では？

A. 学内からのアクセス（有線 LAN、無線 LAN）の場合は多要素認証が不要です。学外からのアクセスの場合は、セキュリティ向上のため多要素認証が必須となります。ご協力をお願いします。

Q. スマートフォンを持っていない場合は？

A. スマホ認証アプリ以外の代替手段（電話、SMS、PC アプリ等）を設定できます。

Q. スマートフォンの機種変更をしたらどうする？

A. P.17～20 の「多要素認証　設定の変更方法」を参考に設定を変更してください。

Q. 多要素認証を行えなくなってしまったらどうする？

A. 情報センター窓口（7 号館 4 階）に本人確認ができるもの（学生証、教職員証等）を持ってお越しください。

Q. パソコンで認証したい。

A. スマートフォンで多要素認証を設定できない方は PC アプリ、またはブラウザ拡張機能を利用することで認証が可能です。

Windows：P.21～27、macOS：P.28～33、ブラウザ拡張機能：P.34～40。

問い合わせ

多要素認証に関するお問い合わせは大学 7 号館 4 階 情報センターまでお願いします。

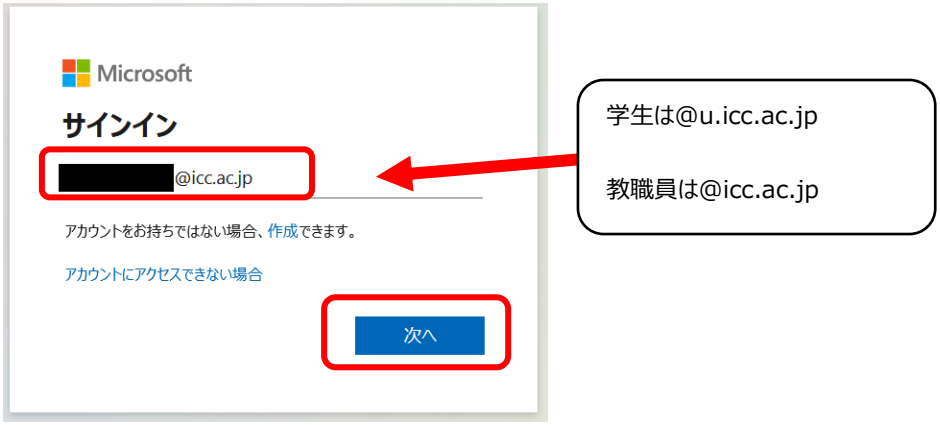
設定方法のマニュアルは次ページ以降を参照ください。

このマニュアルに掲載している画面イメージはサンプルです。実際の環境と異なる部分があります。また予告なしに変更となることがあります。

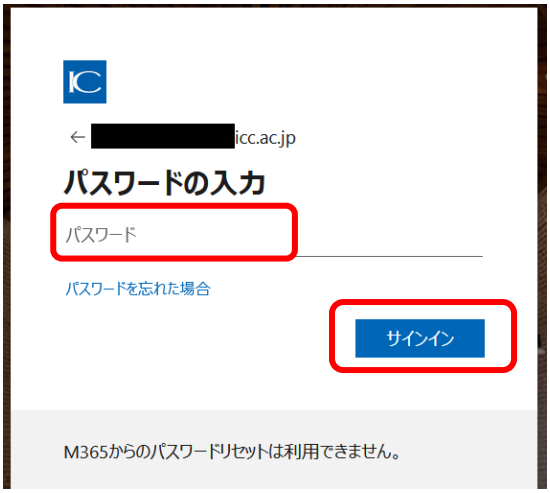
① Microsoft のアカウントページにアクセスします。

URL（https://myaccount.microsoft.com/）

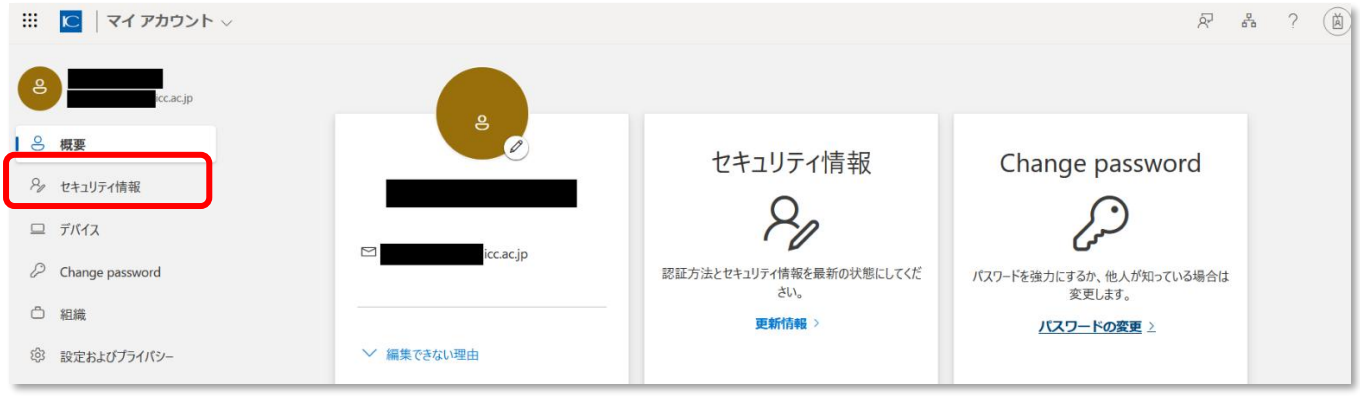
② Microsoft のログイン画面が表示されるので、「メールアドレス」を入力して次へボタンをクリックします。



③ 「パスワード」を入力してサインインボタンをクリックします。



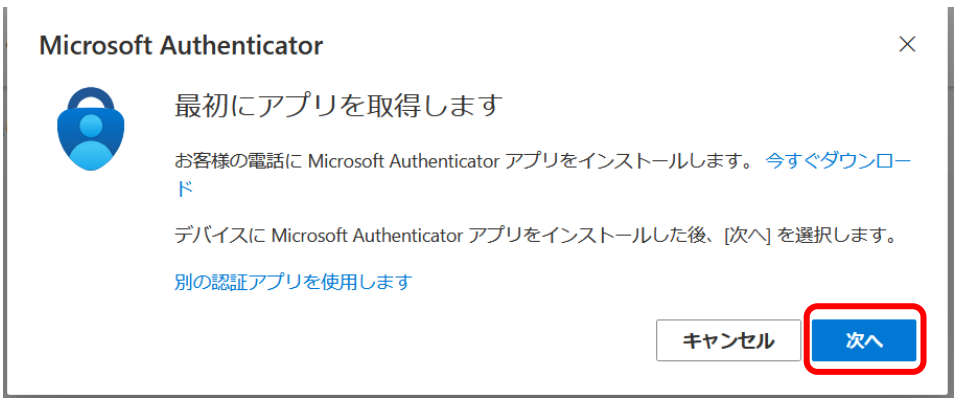
④ 「セキュリティ情報」をクリックします。



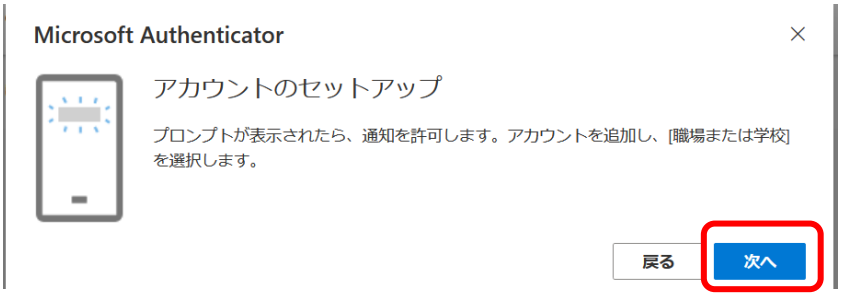
⑤ 「サインイン方法の追加」をクリックします。

⑥ ここでは「Microsoft Authenticator（モバイルアプリ）」をクリックします。電話 or SMS 認証を追加する場合は P.9 の「多要素認証事前設定　初期設定マニュアル　（SMS・電話を用いた認証）」へ。

⑦ アプリのインストールの指示が表示されます。そのまま次へボタンをクリックします。



⑧　アカウントのセットアップ指示が表示されます。そのまま次へボタンをクリックします。



⑨　QR コードが表示されます。PC にこの画面が表示されたまま、スマートフォンで次の作業を行います。

【スマートフォンでの作業】

⑩　認証を行うスマートフォンに「Microsoft Authenticator」アプリ（無料）をインストールしてください。

iPhone の場合「App ストア」、Android の場合「Google Play」の検索画面で「Microsoft Authenticator」を検索してインストールします。似たような名称のアプリがありますので間違えないように注意してください。

＜iPhone の場合＞

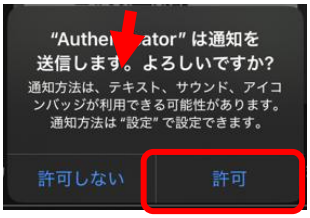
＜Android の場合＞

⑪　Microsoft　Authenticator アプリを起動。

以下、画像のようにタップを進め、「QR コードをスキャンします」をタップします。

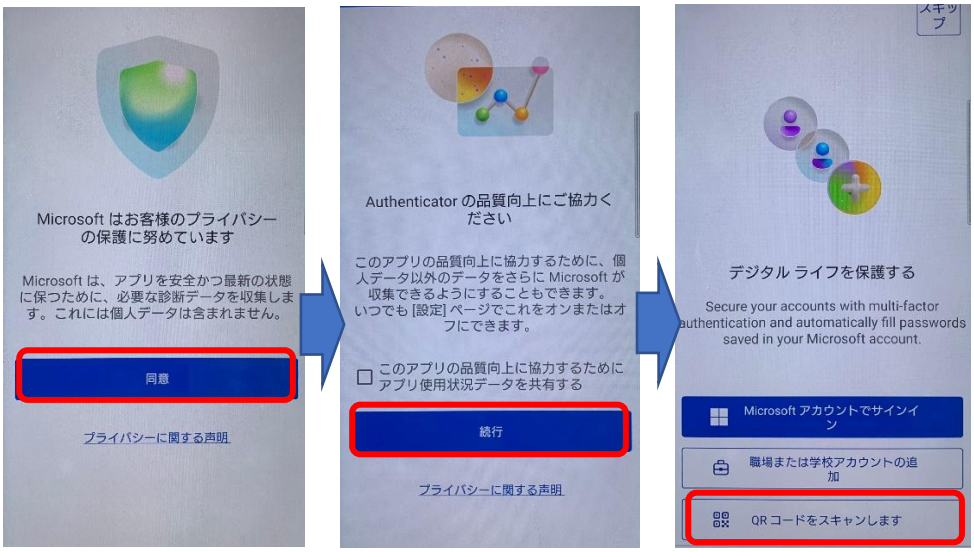
途中で以下のような通知やカメラアクセスの許可を求められたら、「許可」を選択します。

＜iPhone の場合＞

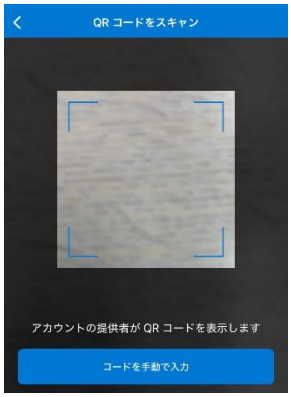


＜Android の場合＞

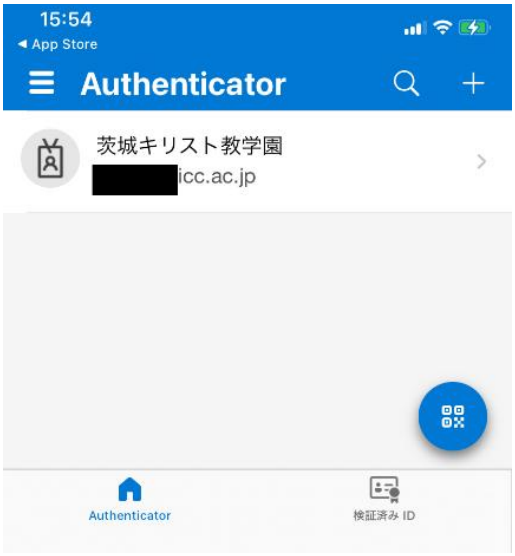
途中で以下のような通知やカメラアクセスの許可を求められたら、「許可」を選択します。



⑫　QR コードのスキャン画面で、PC 画面（P.5）に表示された QR コードをスキャンします。

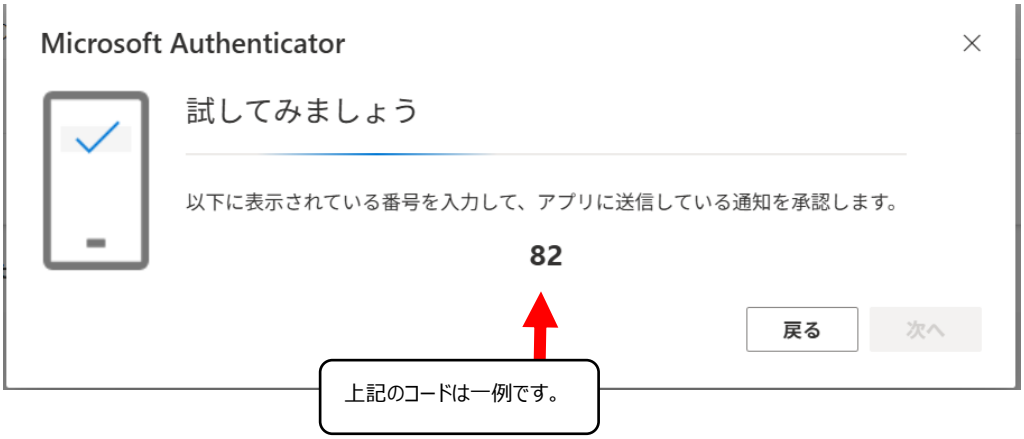


⑬　スキャンに成功するとスマホの Microsoft Authenticator アプリにアカウントが追加されていることが確認できます。



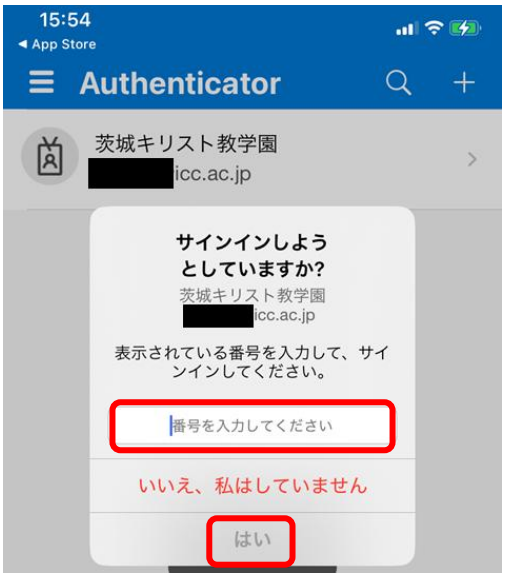
⑭　PC 画面に戻り、次へボタンをクリックします。

⑮　以下の画面を表示したまま、スマートフォンを操作します。



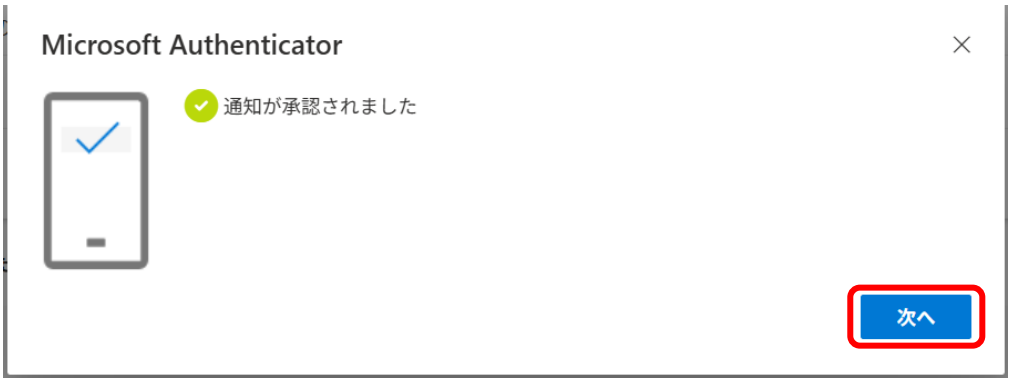
【スマートフォンでの作業】

⑯　スマートフォンの画面に「サインインしようとしていますか？」という表示がされます。
PC 画面に表示されている 2 桁の数字を入力し、「はい」をタップします。



【パソコンでの作業】

⑰　「通知が承認されました」と表示されるので、次へボタンをクリックします。



⑱　セキュリティ情報の画面に「Microsoft Authenticator」が追加されました。

以上で、Microsoft Authenticator アプリを用いた認証を設定する方法は完了です。

以降は学外ネットワークから Microsoft365 にサインインする際に、自身の設定した方法で認証を行っていただく形となります。

多要素認証　初期設定マニュアル　（SMS･電話を用いた認証）

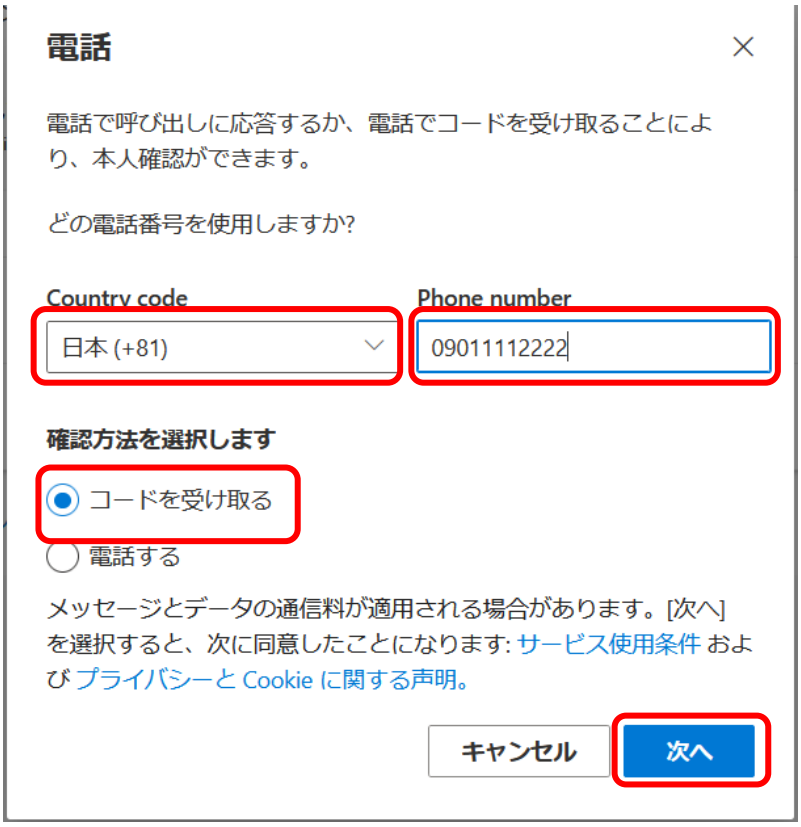
①　多要素認証事前設定　初期設定マニュアル　（モバイルアプリを用いた認証）P.3～4 の手順①～⑤までを参考に、「マイアカウント」の「セキュリティ情報」を開き、「サインイン方法の追加」をクリックします。

②　「電話」をクリックします。

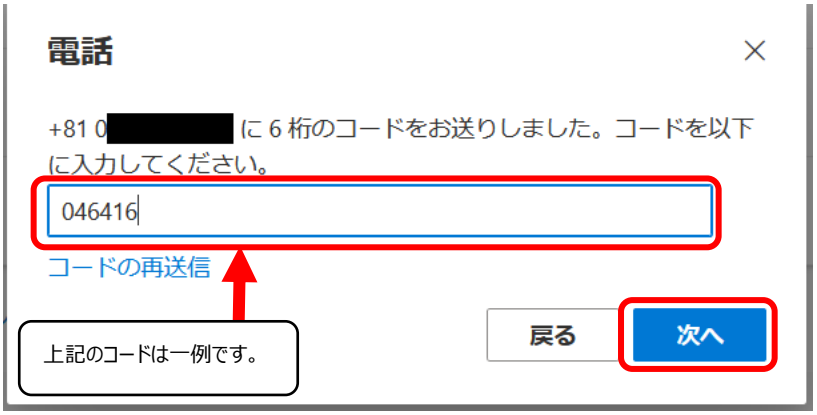
③　電話では SMS でコードを受け取る方法と、電話で着信を受け取る方法があります。

【SMS でコードを受け取る方法】

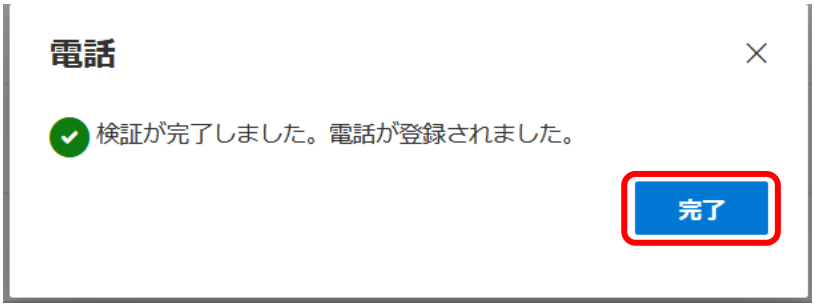
SMS-(1)　Country Code は「日本」を選択して、Phone number は電話番号をハイフンなしで入力し、確認方法は「コードを受け取る」を選択して、次へボタンをクリックします。



SMS-(2)　携帯・スマートフォンの SMS に 6 桁のコードが届くので、PC の画面に 6 桁のコードを入力し、次へボタンをクリックします。



SMS-(3)　認証に成功した画面がでるので、完了ボタンをクリックします。



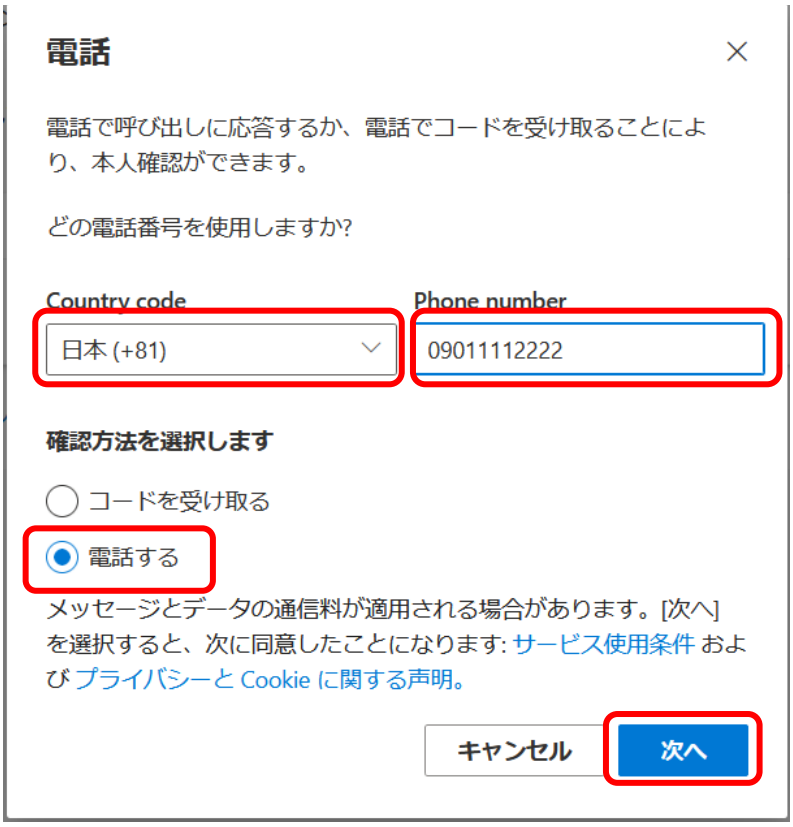
SMS-(4)　セキュリティ情報に電話が追加されました。

以上で、SMS を用いた認証を設定する方法は完了です。

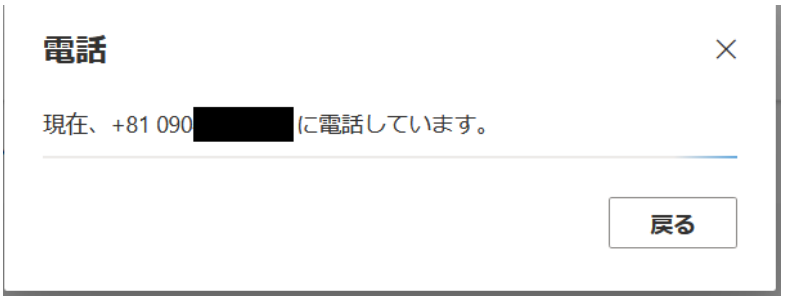
以降は学外ネットワークから Microsoft365 にサインインする際に、自身の設定した方法で認証を行っていただく形となります。

【電話で着信を受け取る方法】

電話-(1) Country Code は「日本」を選択して、Phone number は電話番号をハイフンなしで入力し、確認方法は「電話する」を選択して、次へボタンをクリックします。

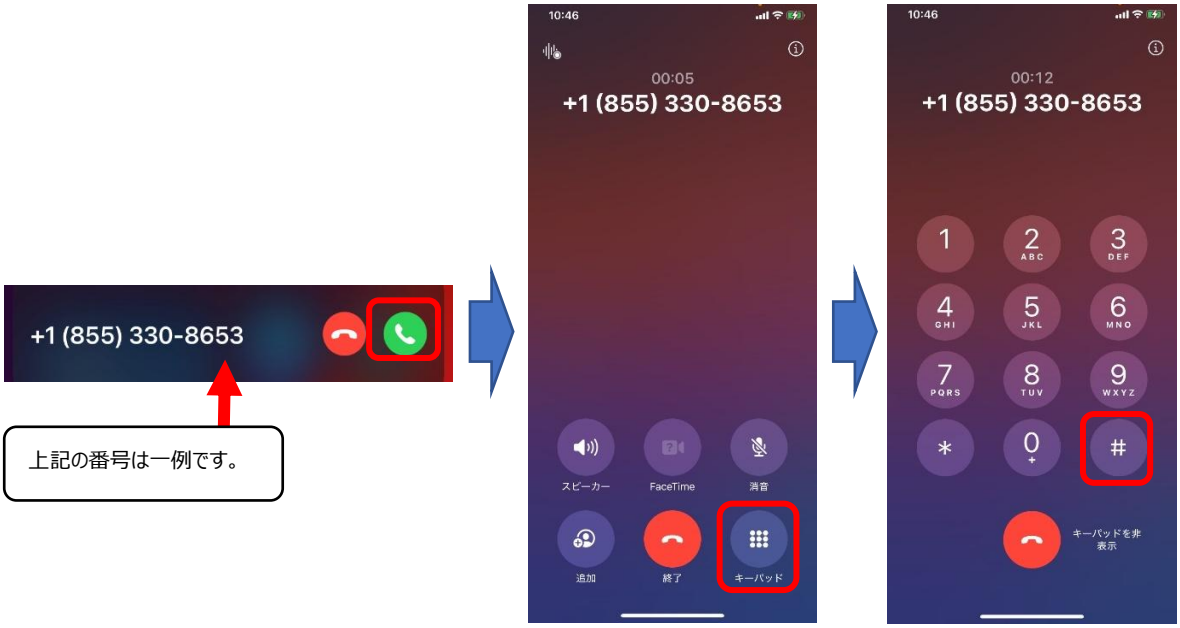


電話-(2) 先ほど指定した電話番号に Microsoft から着信があります。

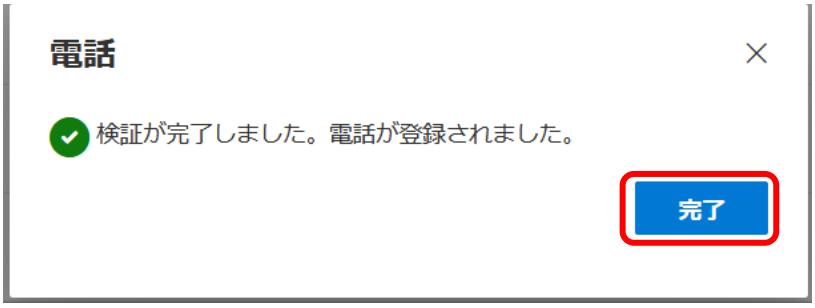


電話-(3)

電話を受けると日本語または英語で「＃」を押すように指示がありますので、キーパッドを開き「＃」をタップします。



電話-(4)　認証に成功した画面がでるので、完了ボタンをクリックします。



電話-(5)　セキュリティ情報に電話が追加されました。

以上で、電話を用いた認証を設定する方法は完了です。

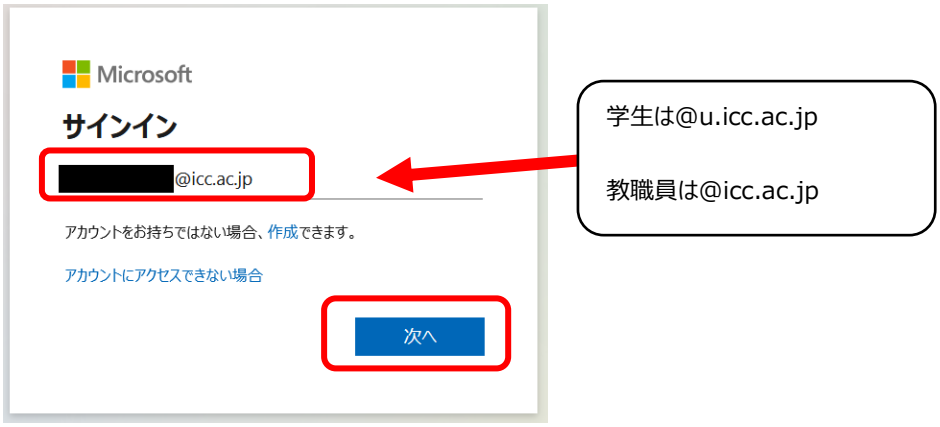
以降は学外ネットワークから Microsoft365 にサインインする際に、自身の設定した方法で認証を行っていただく形となります。

多要素認証が必須化後は、学外から Microsoft365 のサービスにサインインする途中で多要素認証の設定が求められます。

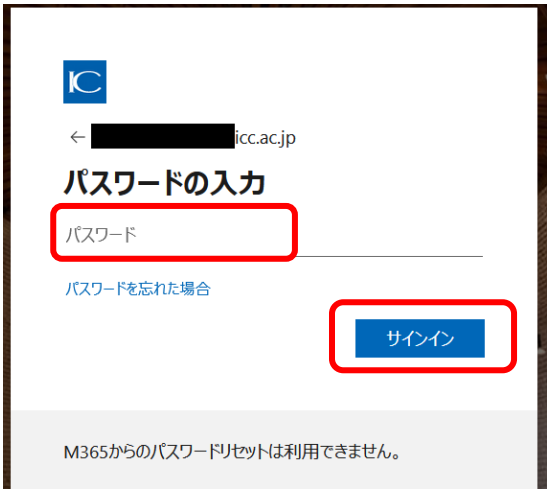
① Microsoft のアカウントページにアクセスします。

URL（https://myaccount.microsoft.com/）

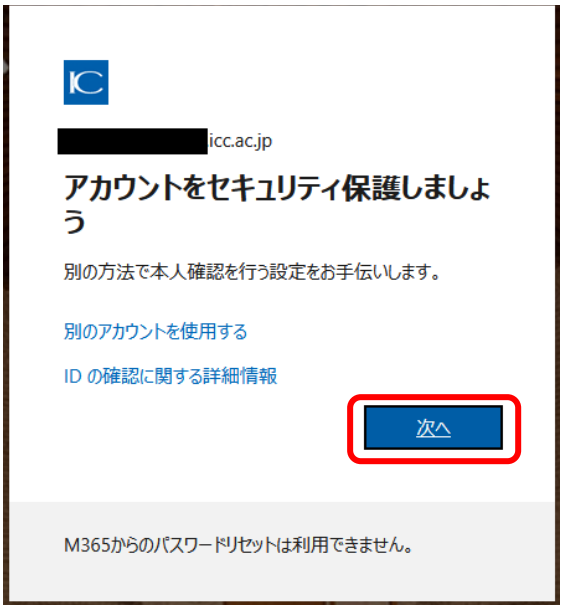
② Microsoft のログイン画面が表示されるので、「メールアドレス」を入力して次へボタンをクリックします。



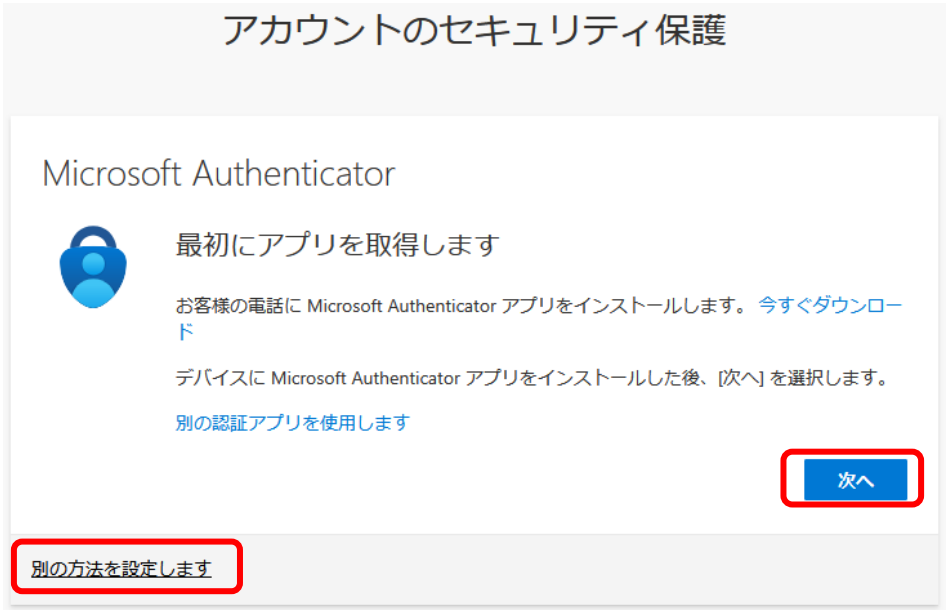
③ 「パスワード」を入力してサインインボタンをクリックします。



④ 「アカウントをセキュリティ保護しましょう」という画面が表示されます。次へボタンをクリックします。



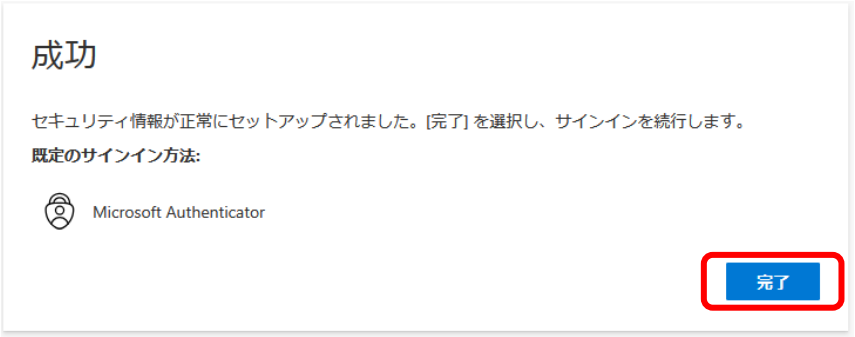
⑤ Microsoft Authenticator アプリの認証を追加する場合は、次へボタンをクリックします。
SMS・電話による認証を追加する場合は、「別の方法を設定します」をクリックします。



【Microsoft Authenticator アプリの認証方法】

P.5～9 の手順⑧～⑱を参照して、手順通り設定してください。

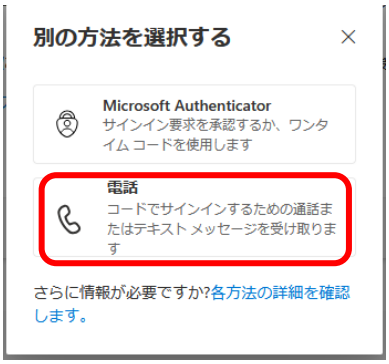
設定に成功すると以下のような成功画面が表示されますので、完了をクリックしてください。



これで Microsoft Authenticator アプリの設定は完了です。 サインイン要求の指示に従って認証してください。

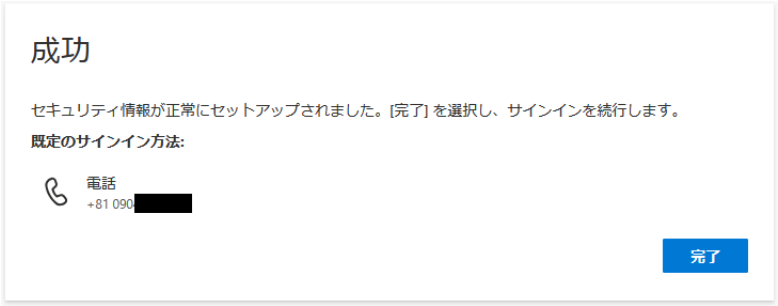
【SMS・電話の認証方法】

P.15　手順⑤の「別の方法を設定します」をクリックすると、以下の画面が表示されるので「電話」をクリックします。



P.10～13 の手順③を参照して、手順通り設定してください。

設定に成功すると以下のような成功画面が表示されますので、完了をクリックしてください。



これで SMS・電話の設定は完了です。 サインイン要求の指示に従って認証してください。

多要素認証　設定の変更方法

スマートフォンの機種変更をした場合や電話番号を変更した場合に、多要素認証の設定変更が必要になります。その際に多要素認証の設定が１つだけの場合にアクセスできなくなるため、事前に**２つ以上の多要素認証の設定**をお願いします。

多要素認証は５デバイスまで登録することができます。端末や認証方法を追加・変更・削除する場合は以下の方法を参照してください。

① Microsoft のアカウントページにアクセスします。

URL（https://myaccount.microsoft.com/）

② Microsoft のログイン画面が表示されるので、「メールアドレス」を入力して次へボタンをクリックします。

③ 「パスワード」を入力してサインインボタンをクリックします。

学外のネットワークからアクセスした場合は、多要素認証が求められます。自身が設定した方法で認証を行ってください。

【スマートフォンの機種変更をした場合】

新スマートフォンで多要素認証の設定をするまでは、旧スマートフォンの Authenticator で認証、または SMS・電話番号で認証する必要がありますのでご注意ください。

④ 「セキュリティ情報」をクリックします。

多要素認証設定後は、セキュリティ情報をクリックすると多要素認証が求められます。自身が設定した方法で認証を行ってください。

⑤ 認証方法の追加、変更、削除は以下の方法を参照してください。

【認証方法を追加する方法】

サインイン方法の追加をクリックします。

追加したい方法を選択してください。

・Microsoft Authenticator アプリの設定方法は **P.4～9 の手順⑤～⑱**を参照してください。

・SMS・電話の設定方法は **P.10～13 の手順③**を参照して、手順通り設定してください。

【電話番号を変更する方法】

「変更」をクリックします。

新しい番号を入力して設定を進めてください。

・SMS・電話の設定方法は **P.10～13 の手順③**を参照して、手順通り設定してください。

【認証方法を削除する方法】

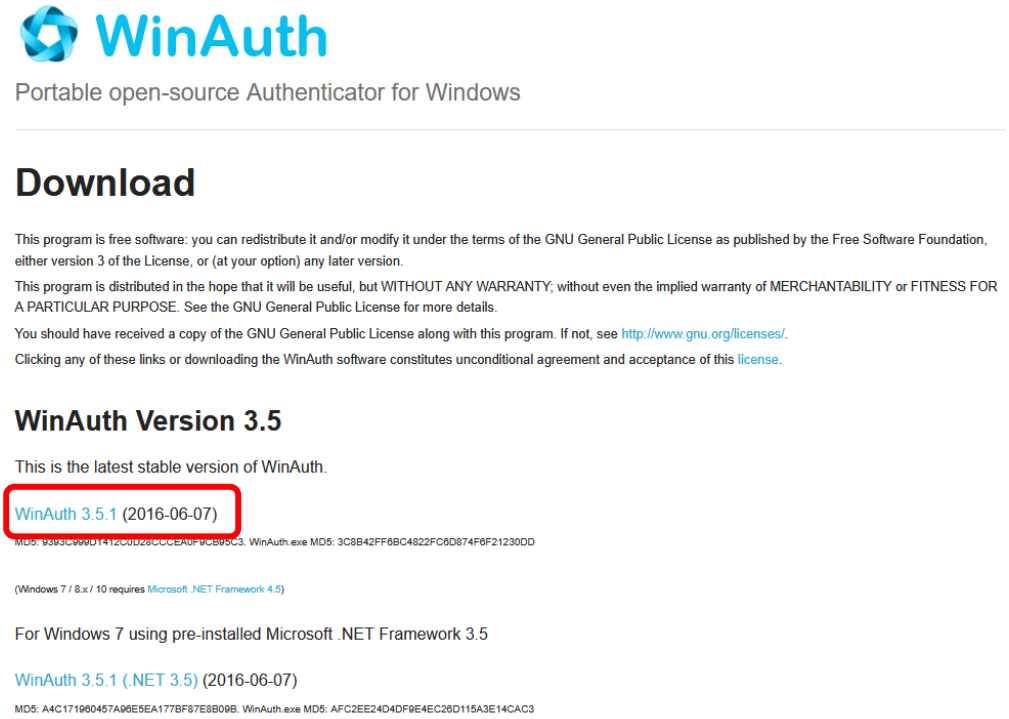
既に設定されている方法の右側の「削除」をクリックして認証方法を削除できます。

多要素認証　PC アプリ（WINAUTH）の設定の方法　（WINDOWS PC）

WinAuth というパソコン用のアプリで、多要素認証を行うことができます。（Windows OS の PC のみ）

① 以下のアドレスにアクセスし、アプリ（WinAuth）をダウンロードします。

https://winauth.github.io/winauth/download.html



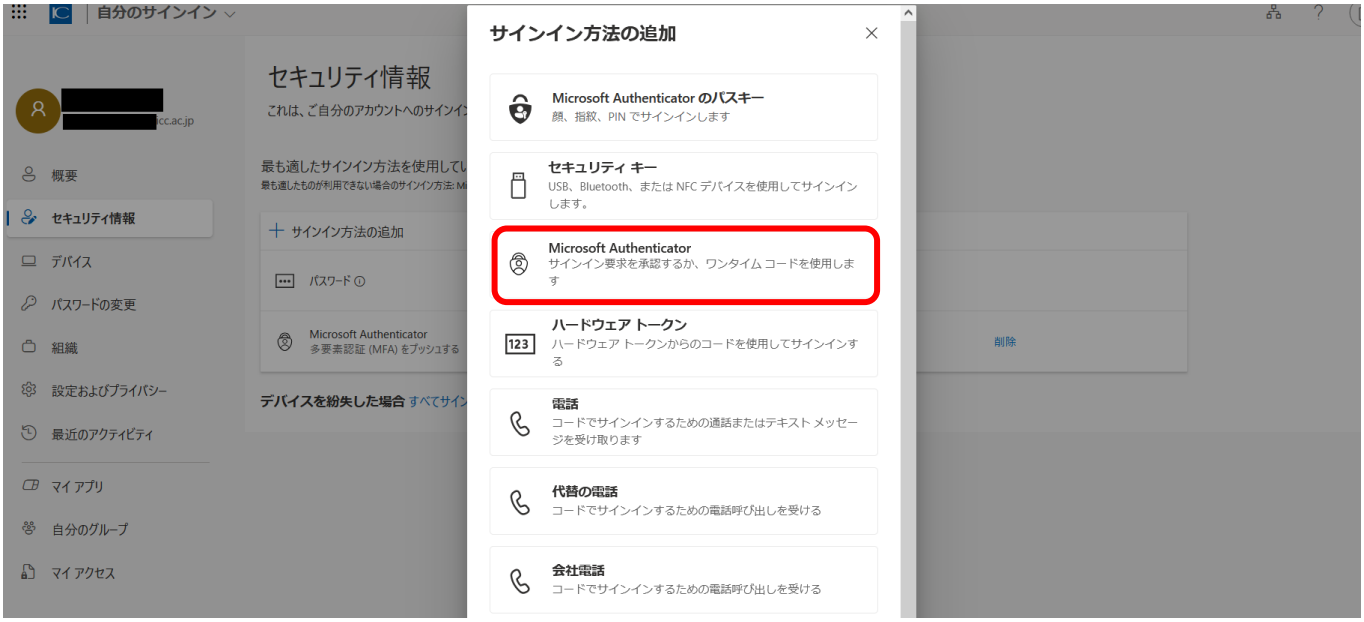
② ダウンロードした ZIP ファイルを解凍し、任意の場所に展開します。

③　アプリ（WinAuth）の展開が完了したら

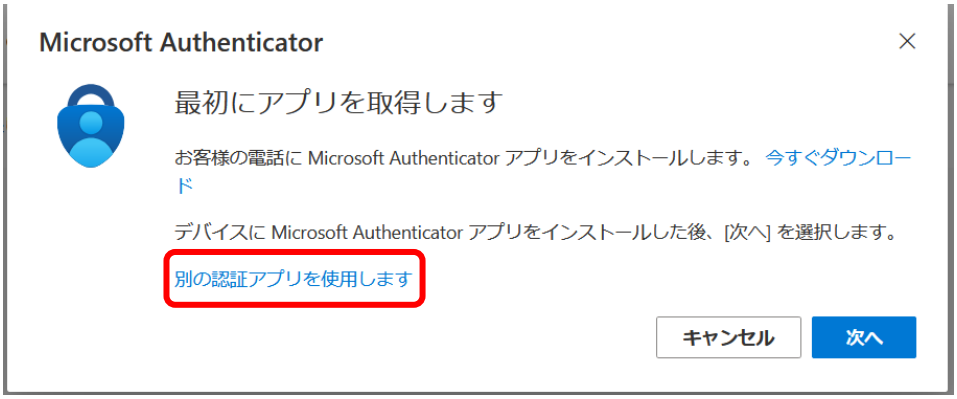
P.17～18 の手順①～④を参照して、Microsoft365 にサインイン後にセキュリティ情報まで進んでください。

④　サインイン方法の追加をクリックします。

⑤　「Microsoft Authenticator」をクリックします。

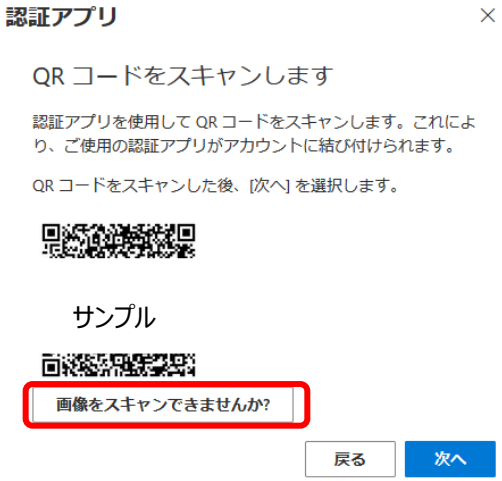


⑥　「別の認証アプリを使用します」をクリックします。

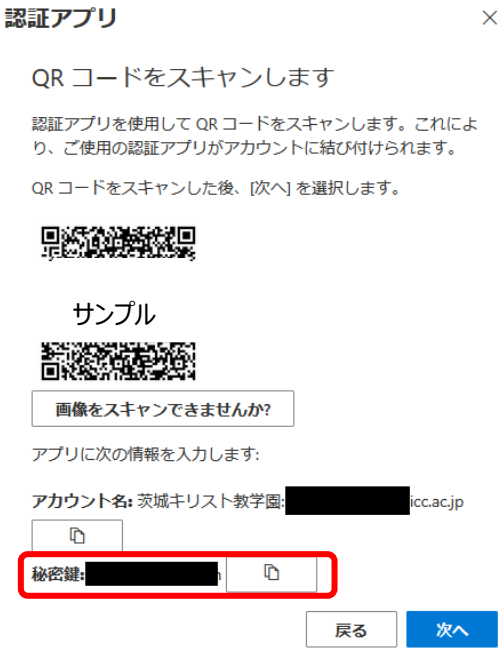


⑦ 「アカウントのセットアップ」が表示されたら、次へをクリックします。

⑧ QR コードの画面では、画像をスキャンできませんかをクリックします。

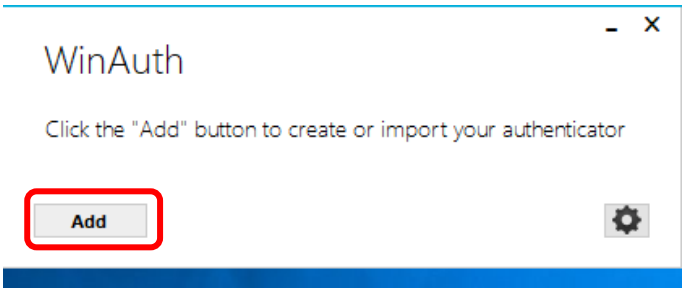


⑨ 秘密鍵が表示されます。この秘密鍵はパスワードと同様に他人に知られないようにご注意ください。

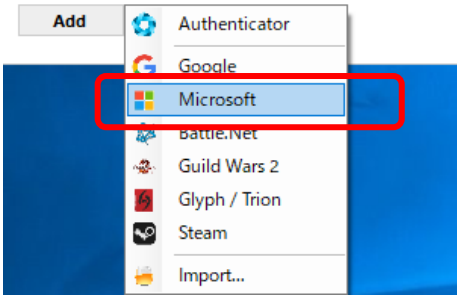


⑩　さきほどダウンロードして任意の場所に展開したアプリ（WinAuth）を起動します。

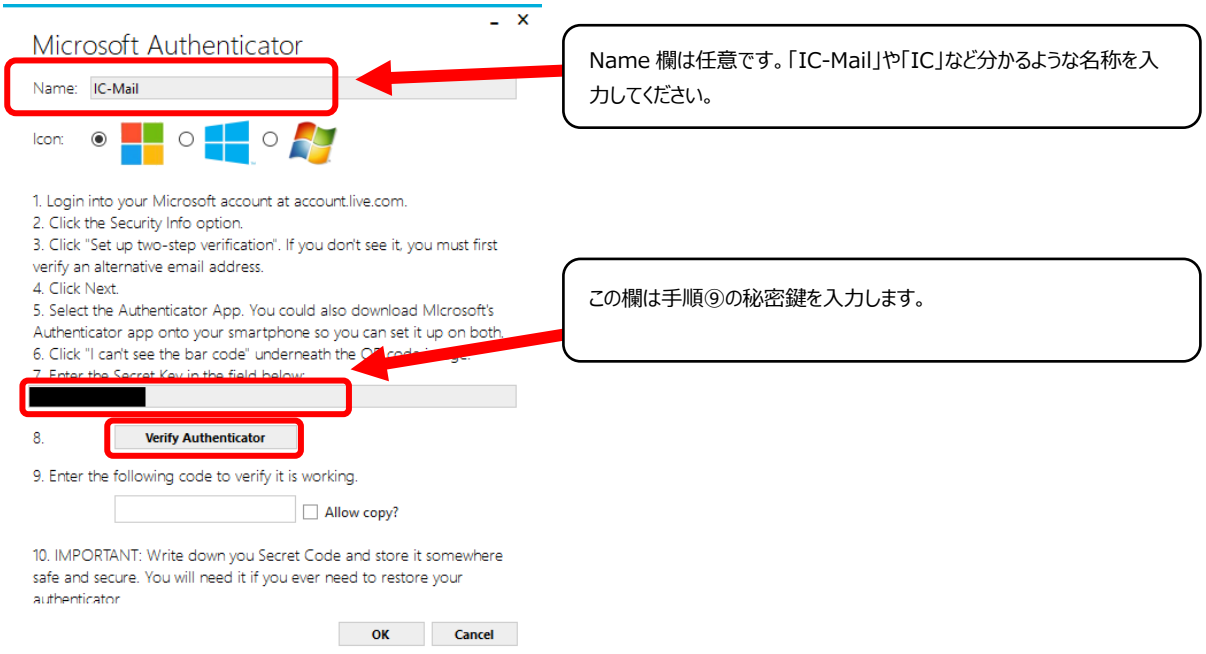
⑪　Add ボタンをクリックします。



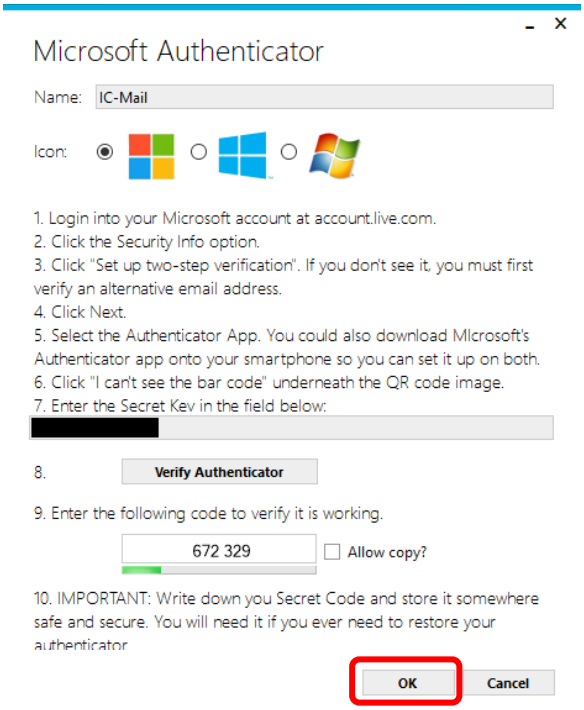
⑫　Microsoft を選択します。



⑬　設定情報を入力します。「Name」欄と「秘密鍵」欄を入力したら、Verify Authenticator をクリックします。



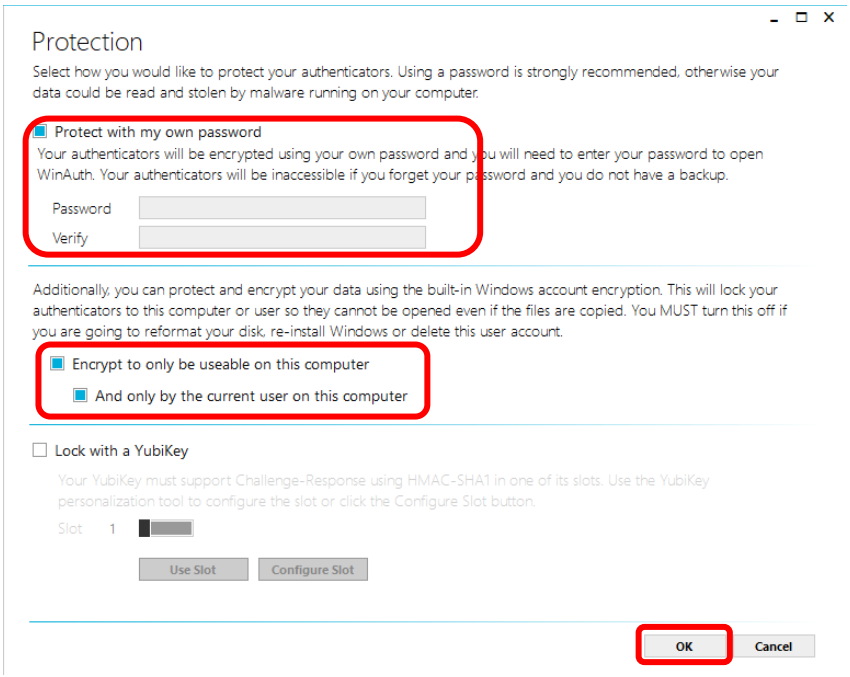
⑭ Verify Authenticator をクリックした後に、6 桁の数字が表示され、緑色のバーが右に少しずつ進みます。
緑色のバーが端に到達すると、新しい 6 桁の数字が表示されます。OK をクリックします。



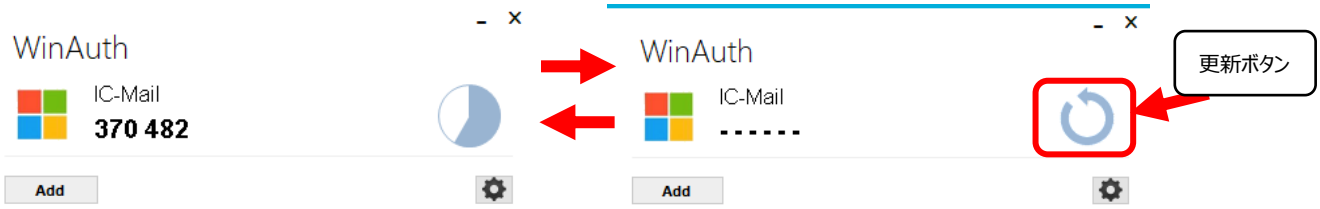
⑮ Protection 画面について、「Protect with my own password」にチェックを入れると WinAuth を起動する際にパスワードが必要になります。自分しか該当の PC を使用しない場合は、チェックは不要です。他人と共用している場合は、チェックを入れて Password 欄に任意のパスワードを設定してください。Verify 欄は Password 欄と同じものを入力してください。

「Encrypt to only be useable on this computer」と「Add only by the current user on this computer」はチェックを入れて使用してください。

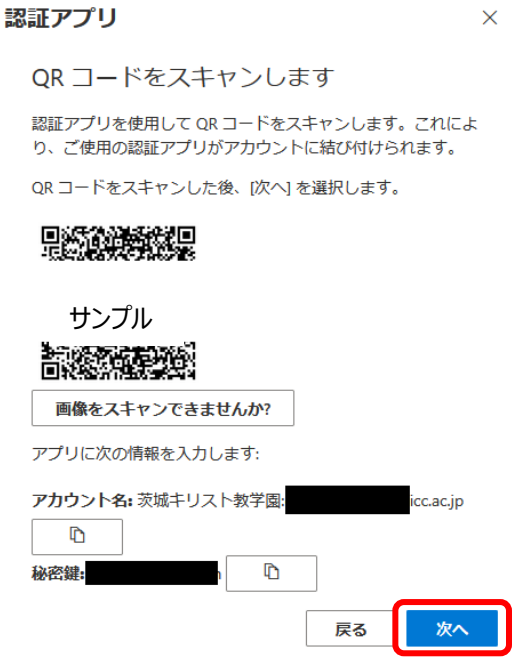
OK ボタンをクリックします。



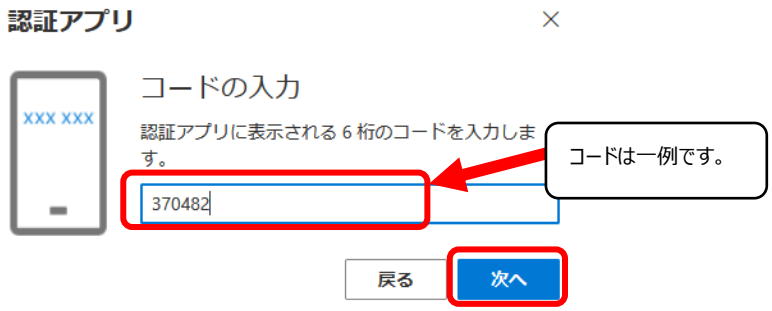
⑯ 6 桁のコードが表示される画面が表示されます。30 秒経過すると右下図のようにコードが表示されなくなります。
更新ボタンをクリックすると新しいコードが表示されます。



⑰ ブラウザに戻り、次へボタンをクリックします。



⑱ コードの入力画面になります。アプリ（WinAuth）に表示されている 6 桁のコードを入力し、次へボタンをクリックします。



⑲　セキュリティ情報に認証アプリが追加されました。

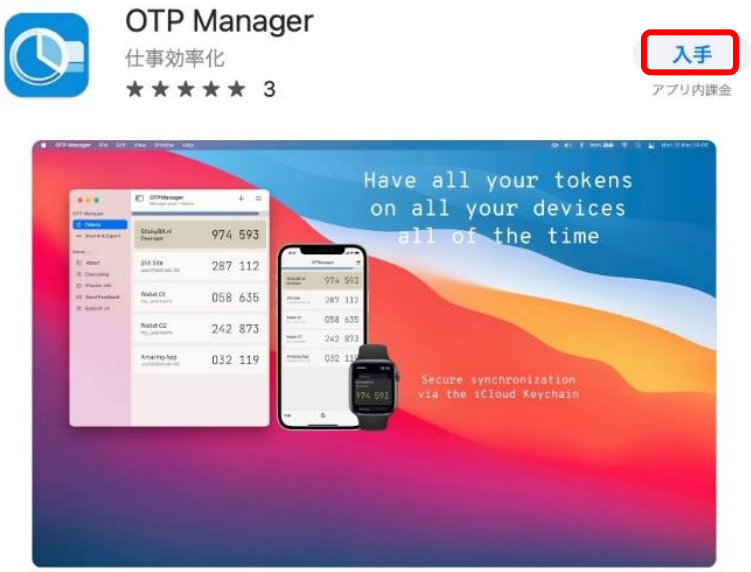
これでアプリ（WinAuth）の設定は完了です。 サインイン要求の指示に従って、WinAuth を起動しコードを入力して認証してください。

多要素認証　PC アプリ（OTP MANAGER）の設定の方法（MAC PC）

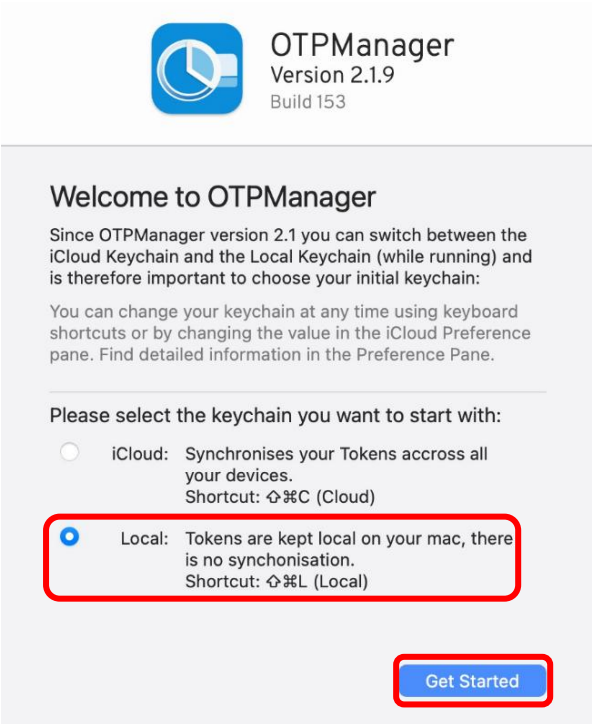
OTP Manager というパソコン用のアプリで、多要素認証を行うことができます。（macOS Big Sur(11.0)以降の PC 対応）

OTP Manager は Windows 用のアプリもありますが、ここでは Mac 用のアプリについて説明します。

① AppStore にアクセスし、アプリ（OTP Manager）をインストールします。



② OTP Manager を起動すると下図のような画面が表示されます。
Local: を選択して、Get Started ボタンをクリックしてください。

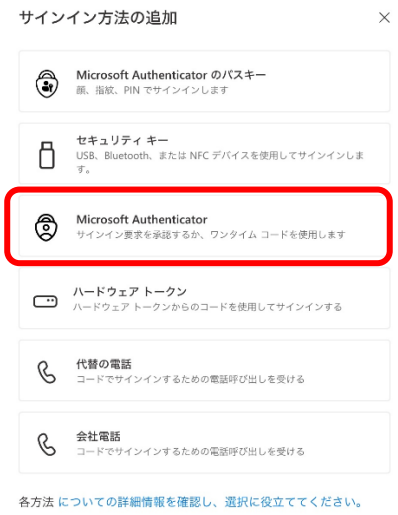


③　アプリ（OTP Manager）のインストールと起動が完了したら

P.17～18 の手順①～④を参照して、Microsoft365 にサインイン後にセキュリティ情報まで進んでください。

④　サインイン方法の追加をクリックします。

⑤　「Microsoft Authenticator」をクリックします。



⑥　「別の認証アプリを設定する」をクリックします。

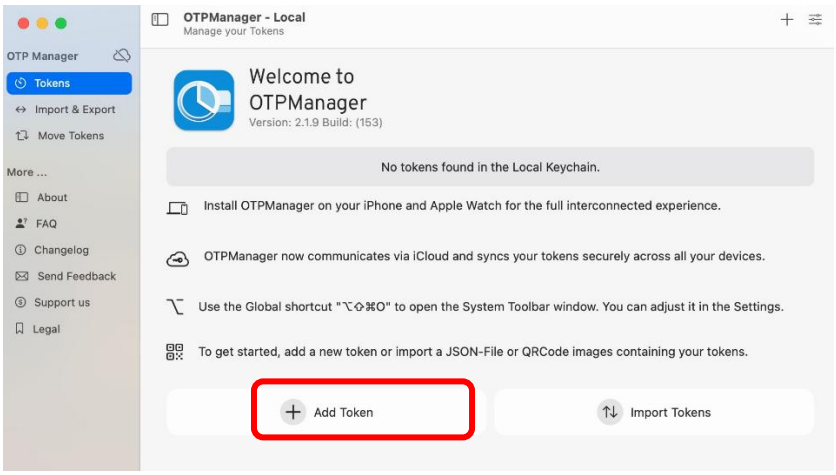
⑦ 「アプリでアカウントをセットアップする」が表示されたら、次へをクリックします。

⑧ QR コードの画面では、Can't scan the QR code?をクリックします。

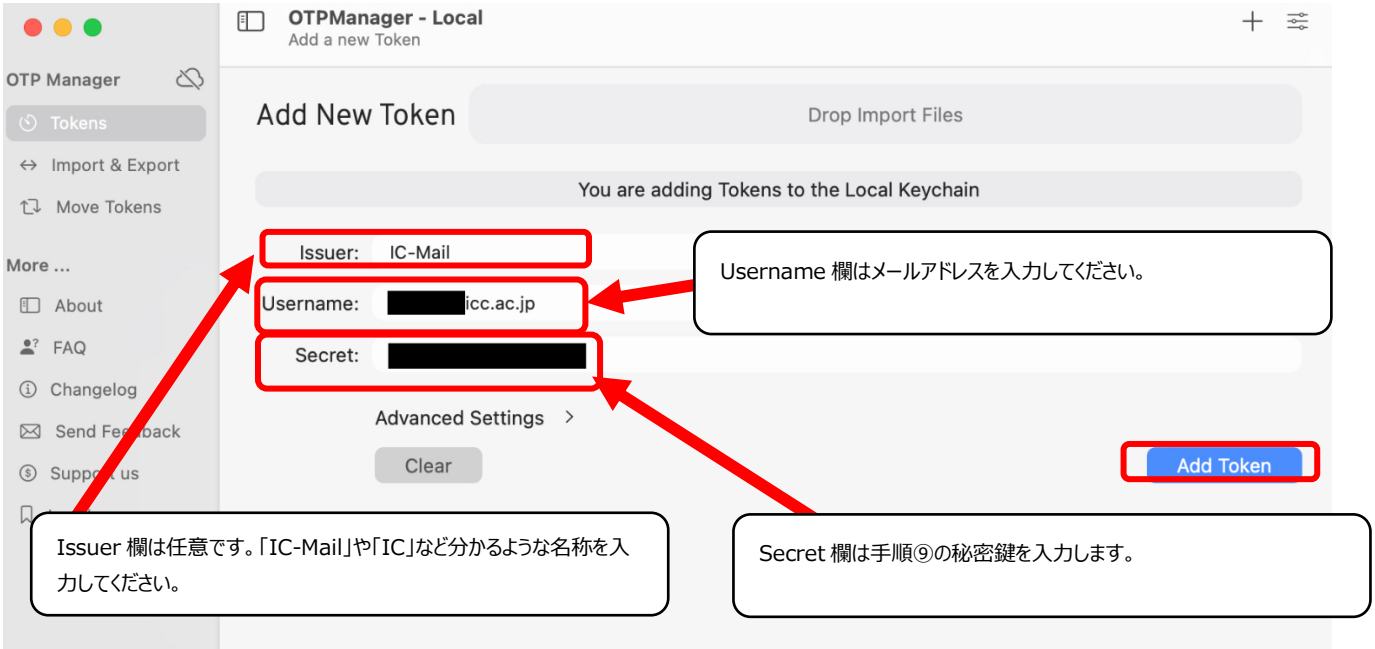
⑨ 秘密鍵が表示されます。この秘密鍵はパスワードと同様に他人に知られないようにご注意ください。

⑩　さきほどインストールしたアプリ（OTP Manager）を起動します。

⑪　Add Token ボタンをクリックします。

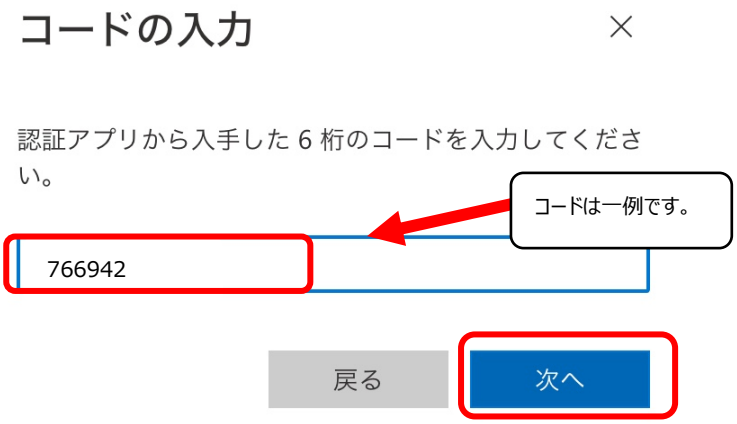


⑫　設定情報を入力します。「Issuer」欄と「Username」欄と「Secret」欄入力したら、Add Token をクリックします。

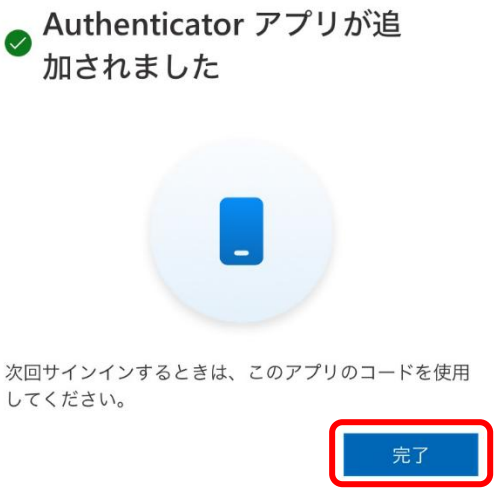


⑬ ブラウザに戻り、次へボタンをクリックします。

⑭ コードの入力画面になります。アプリ（OTP Manager）に表示されている 6 桁のコードを入力し、次へボタンをクリックします。



⑮　アプリ追加の画面が表示されたら完了ボタンをクリックします。



⑯　セキュリティ情報に認証アプリが追加されました。

これでアプリ（OTP Manager）の設定は完了です。 サインイン要求の指示に従って、OTP Manager を起動しコードを入力して認証してください。

多要素認証　ブラウザ拡張機能の設定の方法

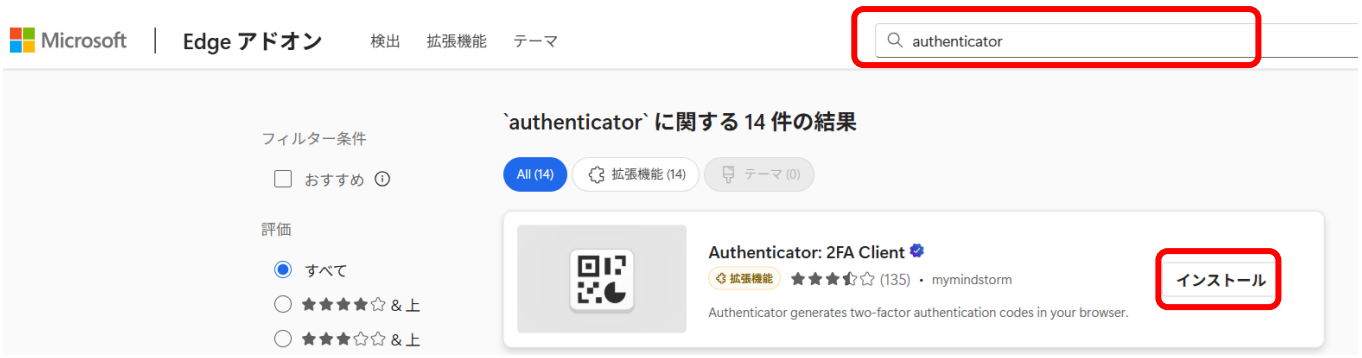
パソコンのブラウザ拡張機能で、多要素認証を行うことができます。（Windows、macOS どちらでも可能）

【Microsoft Edge】の場合

① ブラウザの Microsoft Edge を起動します。
② 右上の…ボタンをクリックして、拡張機能を選択します。

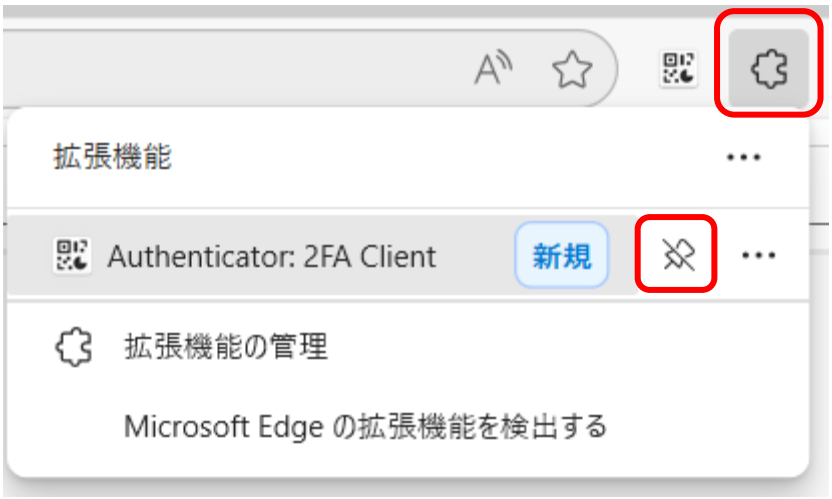
③ 「Microsoft Edge の拡張機能を検出する」をクリックします。

④　検索欄で「authenticator」と入力して検索して、「Authenticator: 2FA Client」のインストールボタンをクリックします。



⑤　「Authenticator：2FA Client」を追加しますかと表示されたら、拡張機能の追加ボタンをクリックします。

⑥　拡張機能のマークをクリックして、ツールバーに「Authenticator：2FA Client」を固定します。



⑦　これで Edge の準備は完了です。

続いて多要素認証の設定手順に進みます。「Microsoft Edge」と「Google Chrome」の手順は同様です。

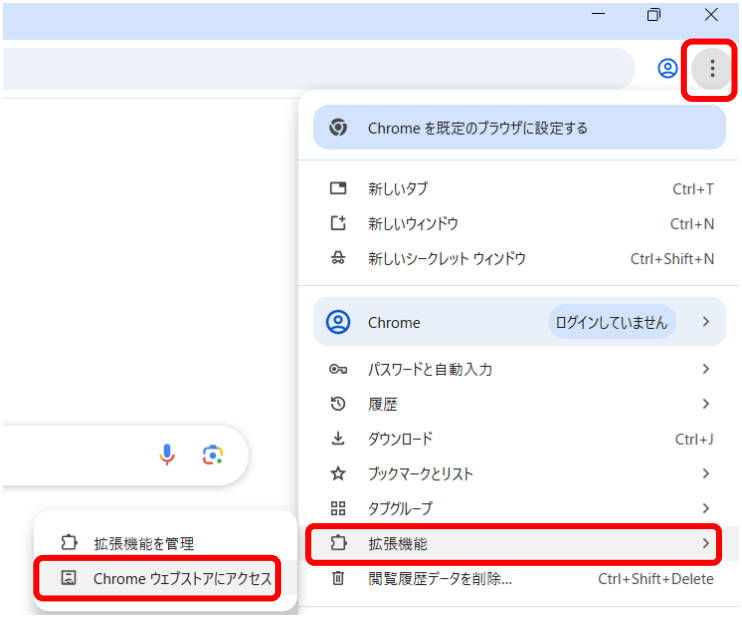
P.17～18 の手順①～④を参照して、Microsoft365 にサインイン後にセキュリティ情報まで進んでください。

セキュリティ情報まで進んだら、P.39 の手順⑧以降の作業を進めてください。

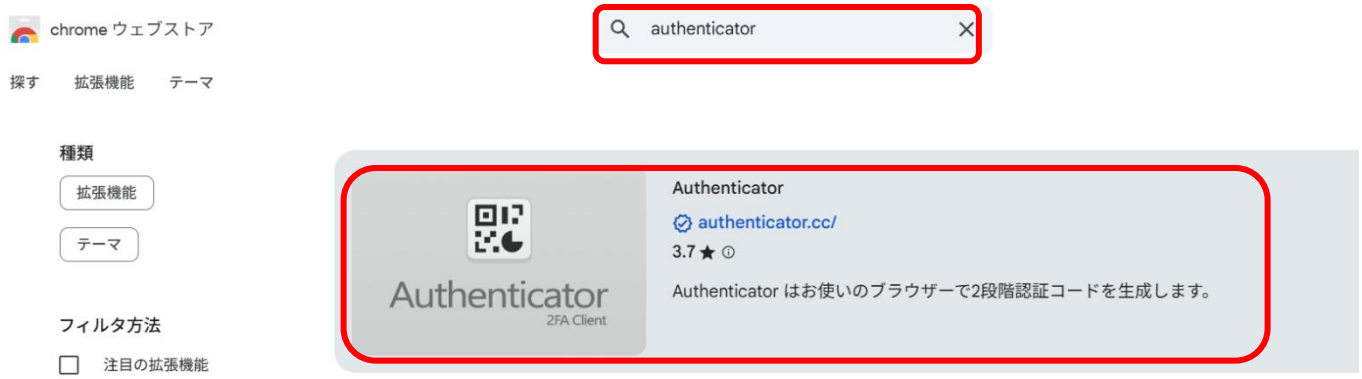
【Google Chrome】の場合

①　ブラウザの Google Chrome を起動します。

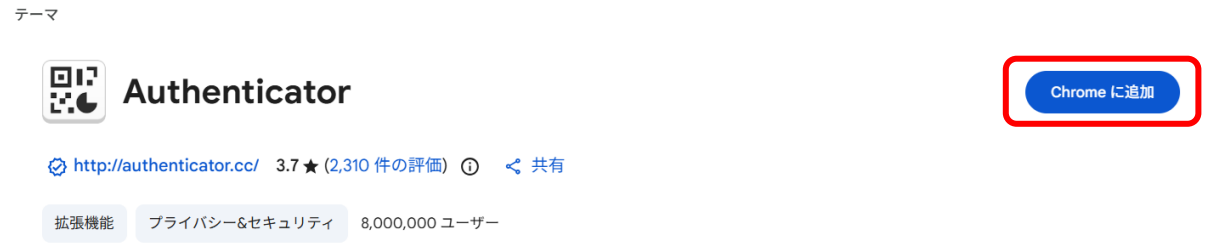
② 右上の…ボタンをクリックして、「拡張機能」－「Chrome ウェブストアにアクセス」を選択します。



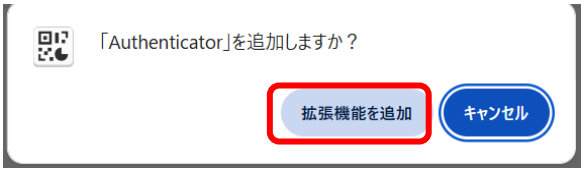
③ 検索欄で「authenticator」と入力して検索して、「Authenticator: 2FA Client」をクリックします。



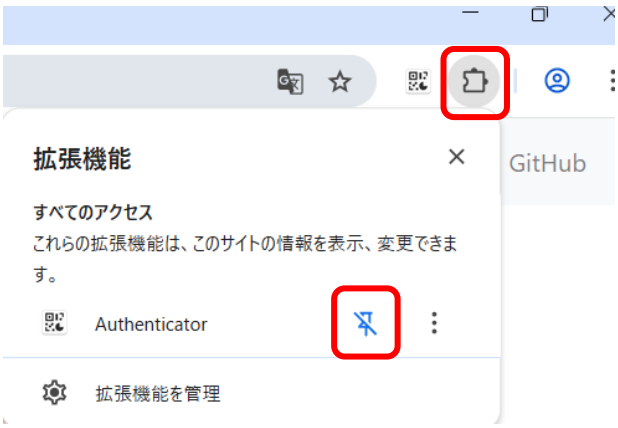
④ Chrome に追加ボタンをクリックします。



⑤ 「Authenticator」を追加しますかと表示されたら、拡張機能の追加ボタンをクリックします。



⑥　拡張機能のマークをクリックして、ツールバーに「Authenticator」を固定します。



⑦　これで Google Chrome の準備は完了です。

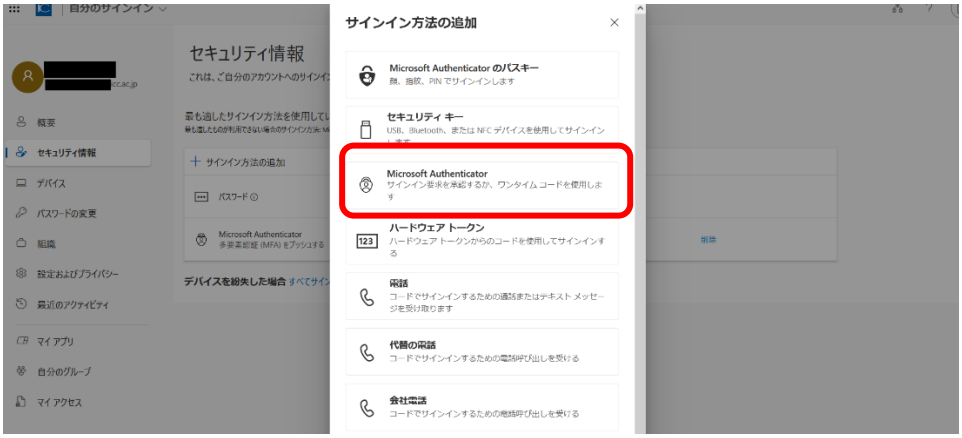
続いて多要素認証の設定手順に進みます。「Microsoft Edge」と「Google Chrome」の手順は同様です。

P.17～18 の手順①～④を参照して、Microsoft365 にサインイン後にセキュリティ情報まで進んでください。

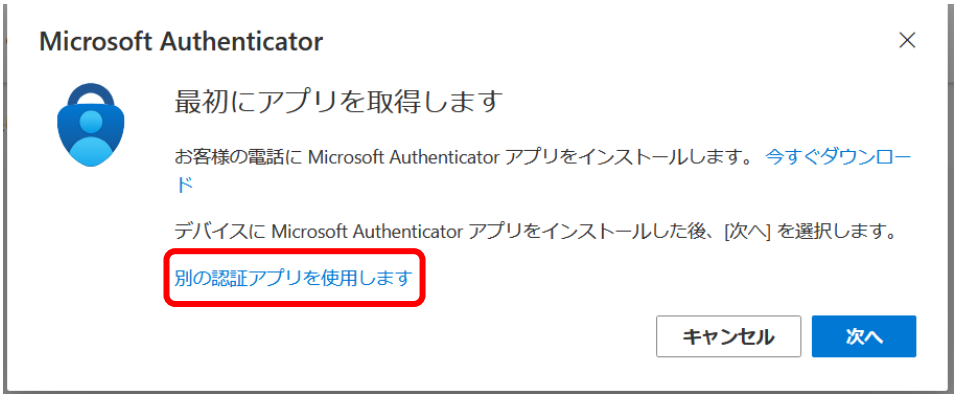
セキュリティ情報まで進んだら、以降の手順⑧に進んでください。

⑧　サインイン方法の追加をクリックします。

⑨　「Microsoft Authenticator」をクリックします。

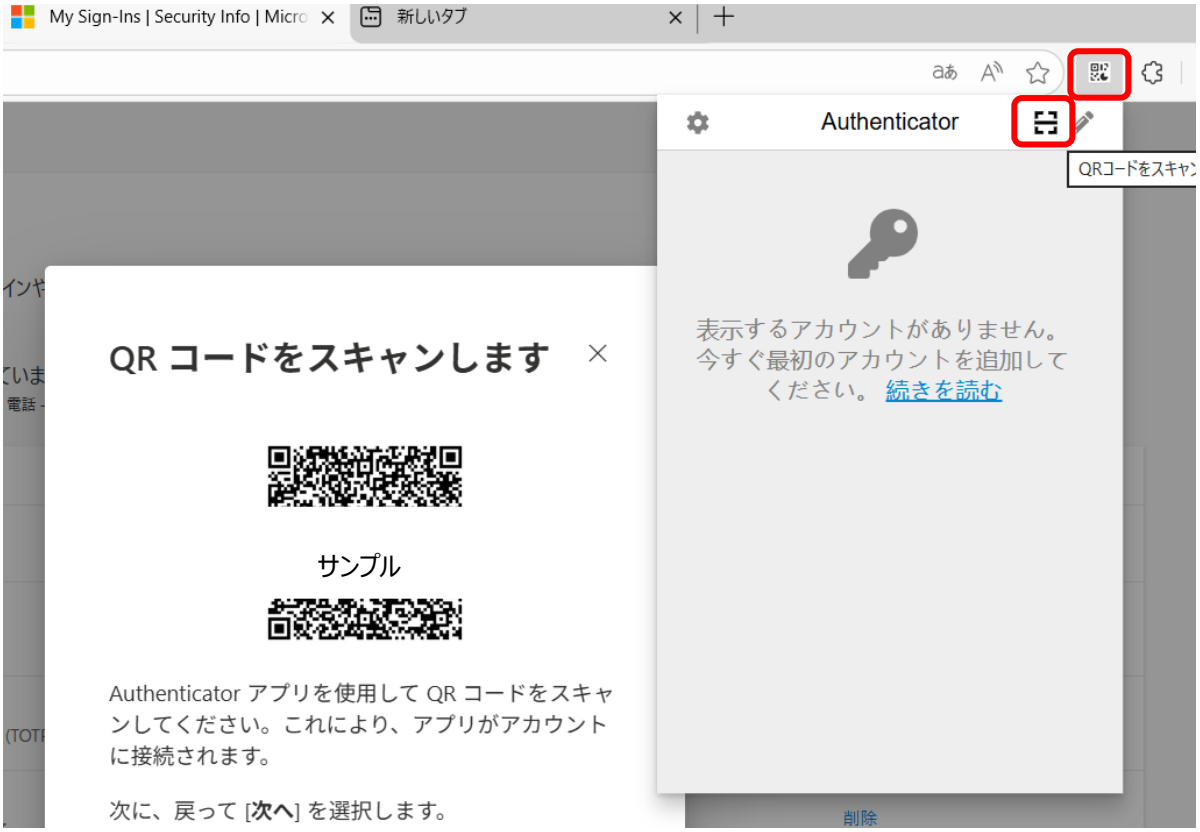


⑩ 「別の認証アプリを使用します」をクリックします。



⑪ 「アカウントのセットアップ」が表示されたら、次へをクリックします。

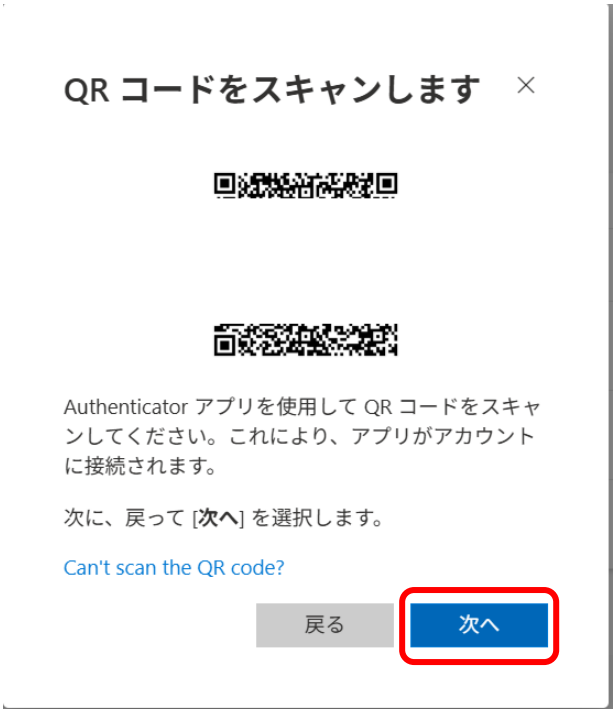
⑫ QR コードの画面が表示されたら、Authenticator のボタンをクリックして、QR コードのスキャンボタンをクリックします。



⑬ QR コードの読み取り画面になるので、QR コード部分を囲んで読み取ってください。

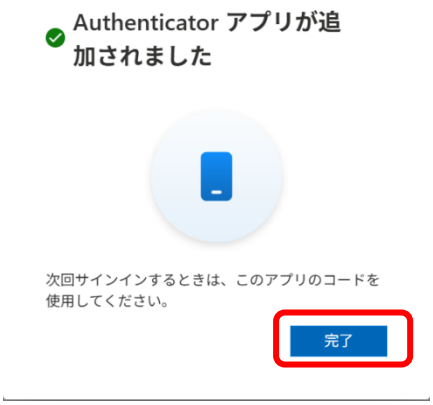
⑭ 「追加されました」と表示されたら、OK ボタンをクリックします。

⑮ 次へボタンをクリックします。



⑯　コードの入力画面になったら、Authenticator のボタンをクリックし、6 桁の認証コードを入力して次へボタンをクリックします。

⑰　追加されましたと表示されたら完了ボタンをクリックします。



⑳　セキュリティ情報に認証アプリが追加されました。

これでブラウザの拡張機能の設定は完了です。 サインイン要求の指示に従って、ブラウザ拡張機能の Authenticator を起動しコードを入力して認証してください。