都立大教研システムにおける MFA の初期設定方法

なりすましやID乗っ取りによる情報セキュリティ障害を防止するため、東京都立大学の教育研究用情報システム(以降、都立大教研システム)には多要素認証(multi-factor authentication、MFA)が導入されています。MFAの導入により、都立大教研システムのサービスを利用する際、IDとパスワードによる従来の本人確認に加えて、別の要素による本人確認が実施されます。

以下では、都立大教研システムのMFA[1]において本人確認に用いる別の要素を初期設定する方法が4つ示されています。ご自身の状況に応じて取りうる方法が変わるので、ご自身がどの状況に該当するかを確認の上、初期設定してください。複数の状況に該当する場合は、もっとも小さい数字に対応する方法で初期設定した上で、6 をご覧ください。

状況1 以下の4条件すべてを満たすデバイス(スマートフォンやタブレットなど)がある→1 へ
- OS が Apple iOS、Apple iPadOS、Google Android のいずれかである
- データ通信(無線 LAN 接続や有線 LAN 接続も含む)可能である
- アプリをインストール可能である
- 自分が専有可能である

状況2 以下の2条件すべてを満たすデバイス(携帯電話やスマートフォン)がある→2 へ
- ショートメッセージを受信可能である
- 自分が専有可能である

状況3 以下の3条件すべてを満たすデバイス(ノートPC[2])がある→3 へ
- データ通信(無線 LAN 接続や有線 LAN 接続も含む)可能である
- Web ブラウザ(Google Chrome、Microsoft Edge、Mozilla Firefox)へ機能拡張を追加可能である
- 自分が専有可能である、あるいは、PC上のIDを共有していない

状況4 以下の2条件すべてを満たすデバイス(携帯電話やスマートフォン)がある→4 へ
- 音声通話を受信可能である
- 自分が専有可能である

状況5 以下の条件を満たすデバイス(固定電話)がある→5 へ
- 音声通話を受信可能である
- プッシュ音を送出可能である

[1] 東京都立大学を設置運営する東京都公立大学法人が契約する Microsoft 365 で提供される Azure Active Directory MFA(Azure AD MFA)

[2] デスクトップPCの場合は別紙「PCを用いるMFAのための設定手順」を参照してください

1. Microsoft Authenticator アプリを利用する

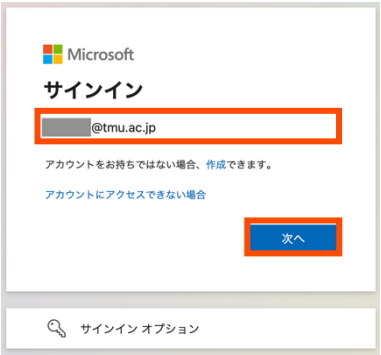
Microsoft が推奨する方法です。Microsoft Authenticator アプリをスマートフォンやタブレットなどのデバイスへインストールして設定します。初期設定には Microsoft Authenticator アプリをインストールするデバイスとは別のデバイス(タブレットやパソコンなど画面ができるだけ大きいデバイス)が1台必要です。

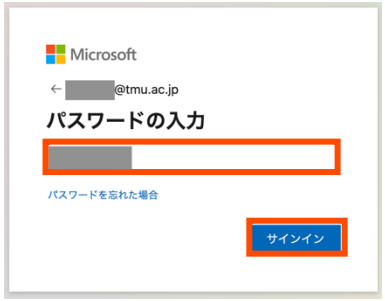
① 以下の4条件すべてを満たすデバイス(スマートフォンやタブレットなど)へ https://www.microsoft.com/ja-jp/security/mobile-authenticator-app から Microsoft Authenticator アプリをインストールします
- OS が Apple iOS、Apple iPadOS、Google Android のいずれかである
- データ通信(無線 LAN 接続や有線 LAN 接続も含む)可能である
- アプリをインストール可能である
- 自分が専有可能である

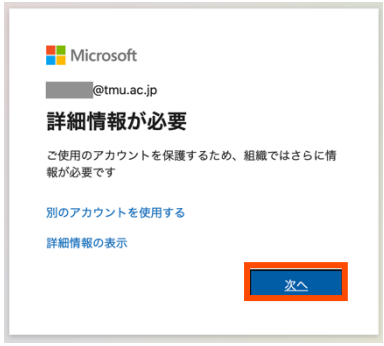
② 1 の①で Microsoft Authenticator アプリをインストールしたデバイス(以降、デバイスA)で、同アプリを起動し「同意」ボタンをタップし「続行」ボタンをタップします
※「このアプリの品質向上に協力するためにアプリ使用状況データを共有する」チェックボタンはチェックしてもしなくても大丈夫です

③ デバイスAを傍に置いて、別のデバイス(タブレットやパソコンなど画面ができるだけ大きいデバイス、以降デバイスB)で Web ブラウザを起動し https://aka.ms/mfasetup へアクセスします

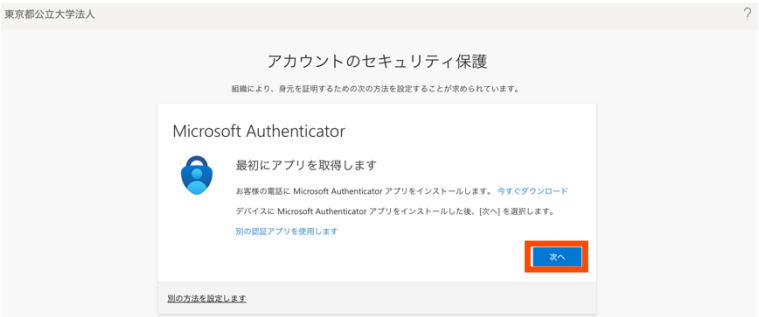
④ デバイスBに表示される「サインイン」画面で TMU ID を入力し「次へ」ボタンをクリックし、「パスワードの入力」画面でパスワードを入力し「サインイン」ボタンをクリックし、「詳細情報が必要」画面で「次へ」ボタンをクリックします



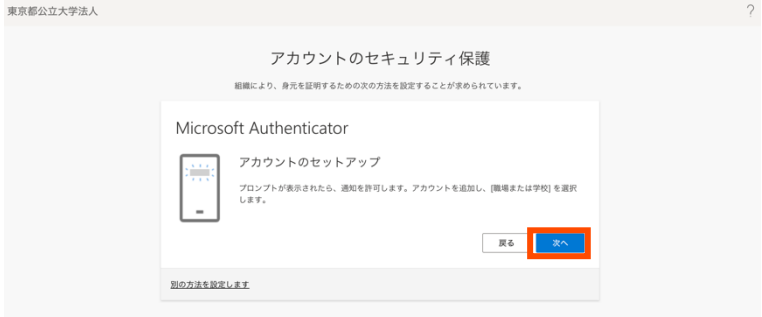




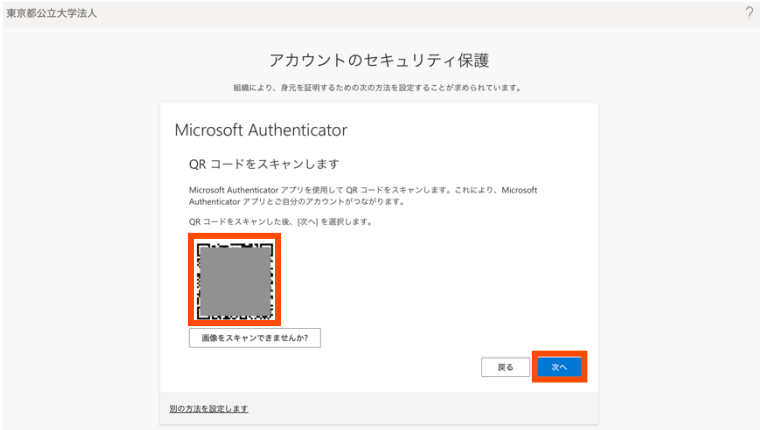
⑤ 「最初にアプリを取得します」画面で「次へ」ボタンをクリックします



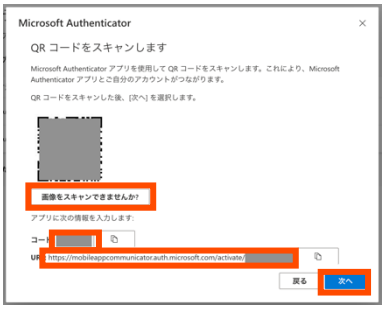
⑥ 「アカウントのセットアップ」画面で「次へ」ボタンをクリックします



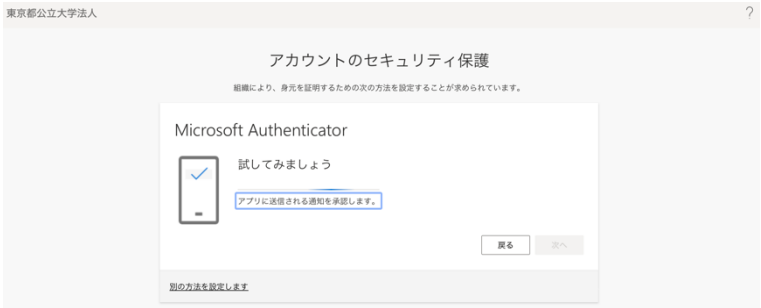
⑦ 「QR コードをスキャンします」画面が表示されたら、デバイスAで「職場または学校アカウントの追加」ボタンをタップし、ポップアップ画面で「QR コードをスキャンします」をタップし、デバイスBに表示されたQR コードをスキャンし、デバイスBの画面の「次へ」をクリックします
※Microsoft Authenticator アプリについてカメラあるいは写真撮影に関する許可を求められたら「アプリの使用時のみ」あるいは「許可」をタップします



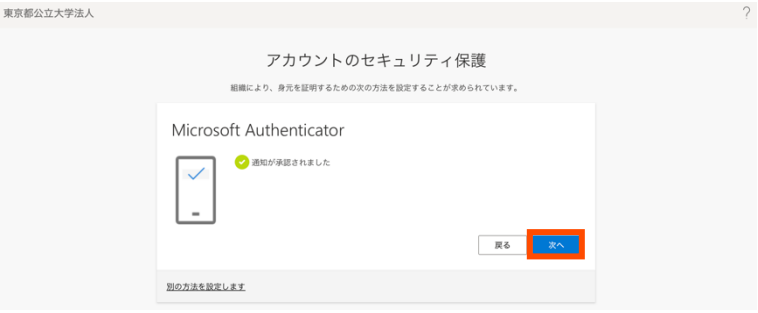
デバイスAにカメラがない、あるいは、デバイスAのカメラを利用できない場合は、デバイスBの「画像をスキャンできませんか？」ボタンをクリックし、デバイスAで「職場または学校アカウントの追加」ボタンをタップし、ポップアップ画面で「QR コードをスキャンします」をタップし、「QR コードをスキャン」画面で「またはコードを手動で入力」ボタンをタップし、デバイスBに表示された「コード」と「URL」をデバイスAの「コード」と「URL」へ入力し、デバイスBの画面の「次へ」をクリックします



⑧ デバイスBに「試してみましょう」と表示されている間に、デバイスAに「サインインを承認しますか？」と表示されたら「承認」をタップします
※デバイスAで「サインインを承認しますか？」とさらに表示され、パスコードの入力や生体認証を求められる場合があります



⑨　デバイスBの「通知が承認されました」画面で「次へ」ボタンをクリックします



⑩　デバイスBの「成功」画面で「完了」ボタンをクリックします

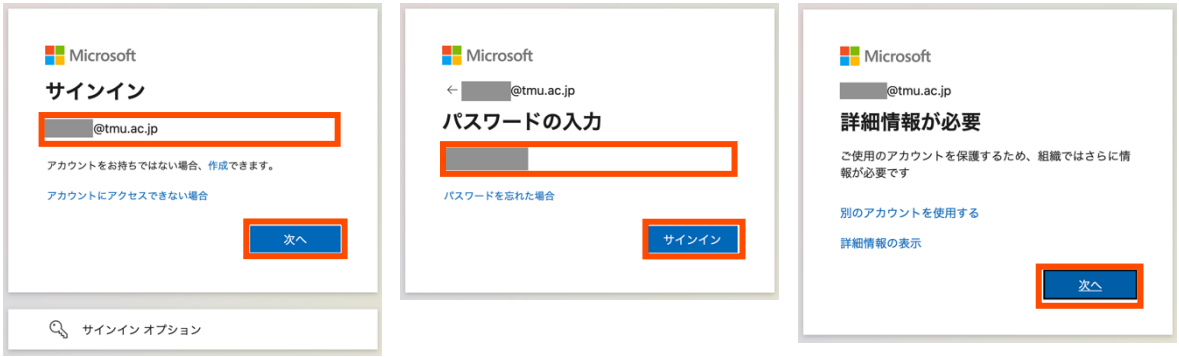
2. ショートメッセージ(short message service、SMS)を利用する

1 の方法よりセキュリティが劣るとされる[3]方法です。SMSを携帯電話やスマートフォンなどのデバイスで受信するよう設定します。初期設定にはSMSを受信するデバイスとは別のデバイス(タブレットやパソコンなど画面ができるだけ大きいデバイス)が1台必要です。

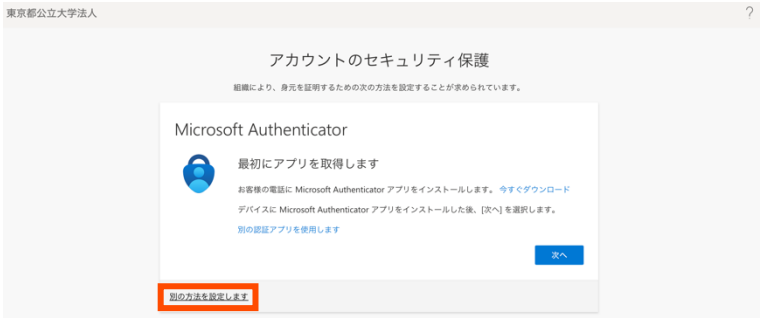
① 以下の2条件を満たすデバイス(携帯電話やスマートフォン)を手元に準備します
- SMSを受信可能である
- 自分が専有可能である

② 2 の①で準備したデバイス(以降、デバイスC)を傍に置いて、別のデバイス(タブレットやパソコンなど画面ができるだけ大きいデバイス、以降デバイスB)で Web ブラウザを起動し https://aka.ms/mfasetup へアクセスします

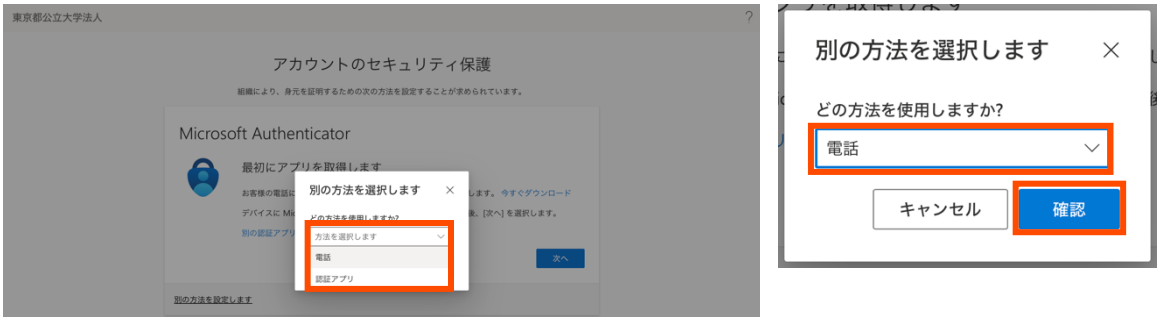
③ デバイスBに表示される「サインイン」画面で TMU ID を入力し「次へ」ボタンをクリックし、「パスワードの入力」画面でパスワードを入力し「サインイン」ボタンをクリックし、「詳細情報が必要」画面で「次へ」ボタンをクリックします



④ 「最初にアプリを取得します」画面で「別の方法を設定します」をクリックします



⑤ 「別の方法を選択します」画面で「方法を選択します」から「電話」を選択し、「確認」ボタンをクリックします



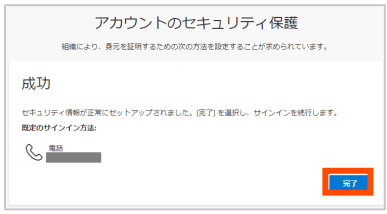
[3] https://learn.microsoft.com/ja-jp/azure/active-directory/authentication/concept-authentication-methods#authentication-method-strength-and-security

⑥ 「電話」画面で「米国（+1）」を「日本（+81）」へ変更し、デバイスCの電話番号を入力し、「次へ」ボタンをクリックします

⑦ デバイスCで受信したSMSに書かれている6桁のコードを、デバイスBの「電話」画面へ入力し、「次へ」ボタンをクリックします

⑧ デバイスBの「電話」画面で「次へ」をクリックします

⑨ デバイスBの「成功」画面で「完了」をクリックします



3. ノートPCの認証アプリを利用

1 の方法より可用性が劣るとされる方法です。Authenticator 機能拡張をノートPC[4]などのデバイスの Web ブラウザへ追加して設定します。初期設定にはノートPCなどのデバイスが1台必要です。

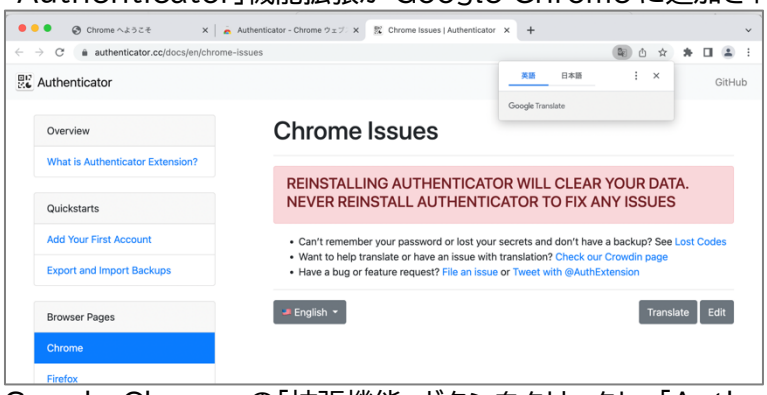
① 以下の3条件を満たすデバイス(ノートPC)を手元に準備します
- データ通信(無線 LAN 接続や有線 LAN 接続も含む)可能である
- Web ブラウザ(Google Chrome、Microsoft Edge、Mozilla Firefox)へ機能拡張を追加可能である
- 自分が専有可能である、あるいは、PC上のIDを共有していない

② 3 の①で準備したデバイスで Google Chrome を起動し、以下の URL(Chrome ウェブストア内の「Authenticator」のページ)にアクセスします
https://chrome.google.com/webstore/detail/authenticator/bhghoamapcdpbohphigoooaddinpkbai?hl=ja
※ここでは Google Chrome を用いていますが、この機能拡張は Microsoft Edge や Mozilla Firefox でも利用することができますので、適宜読み替えてください

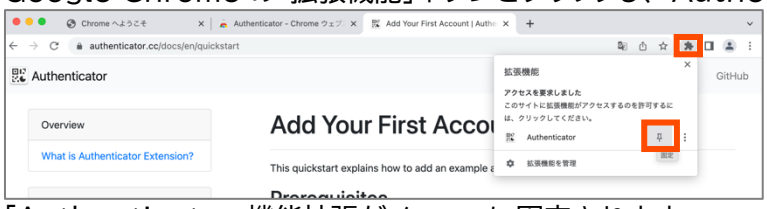
③ 「Authenticator」画面で「Chrome に追加」ボタンをクリックします

④ 「「Authenticator」を追加しますか？」画面で「拡張機能を追加」ボタンをクリックします

⑤ 「Authenticator」機能拡張が Google Chrome に追加されます



⑥ Google Chrome の「拡張機能」ボタンをクリックし、「Authenticator」の「固定」をクリックします

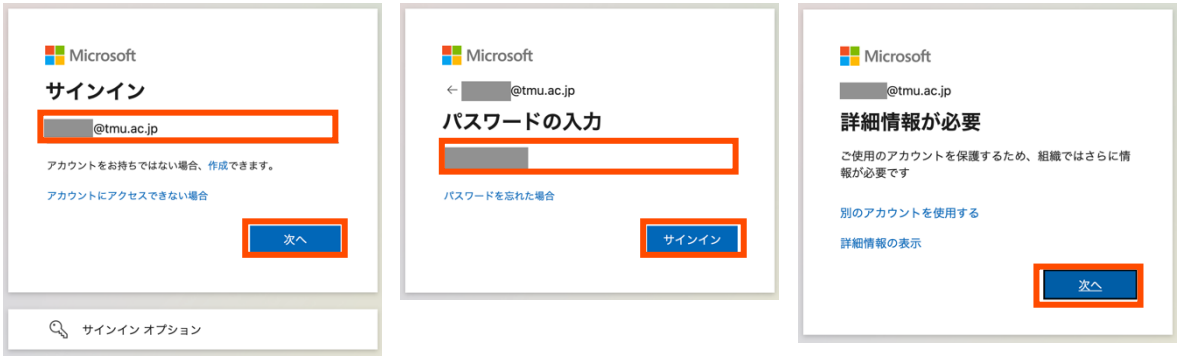


⑦ 「Authenticator」機能拡張がメニューに固定されます

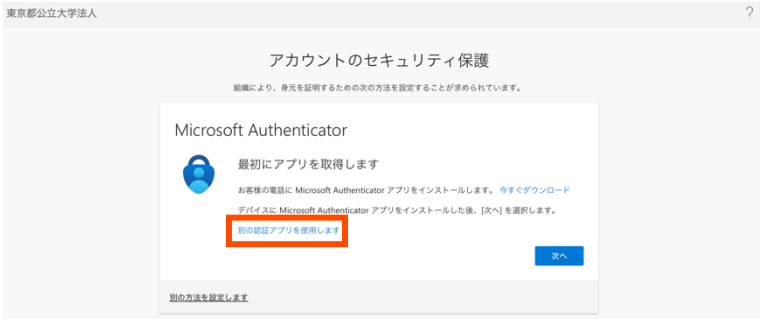
[4] デスクトップPCの場合は別紙「PCを用いるMFAのための設定手順」を参照してください

⑧ Google Chrome で https://aka.ms/mfasetup へアクセスします

⑨ 「サインイン」画面で TMU ID を入力し「次へ」ボタンをクリックし、「パスワードの入力」画面でパスワードを入力し「サインイン」ボタンをクリックし、「詳細情報が必要」画面で「次へ」ボタンをクリックします

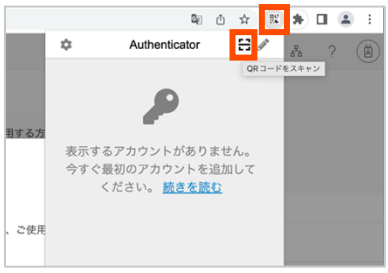


⑩ 「最初にアプリを取得します」画面で「別の認証アプリを使用します」をクリックします

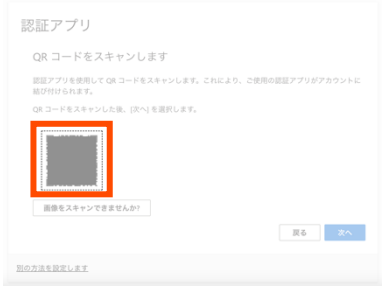


⑪ 「アカウントのセットアップ」画面で「次へ」ボタンをクリックします

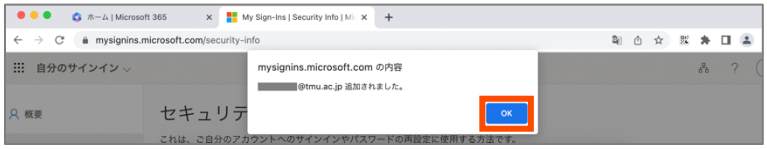
⑫ 「QR コードをスキャンします」画面が表示されたら、Google Chrome のメニューから「Authenticator」をクリックし、「QR コードをスキャン」をクリックします



⑬　QR コードの周りをドラッグして枠で囲います



⑭　画面上部に「<TMU ID>が追加されました。」と表示されたら「OK」をクリックします



⑮　「次へ」をクリックします

⑯　「コードの入力」と表示されたら、メニューから「Authenticator」をクリックします

⑰ 「Authenticator」アプリに表示されているコードをクリックすると、初回は「「Authenticator」が追加の許可をリクエストしています」と表示されるので、「許可する」をクリックします。

⑱ アクセス要求許可後に「Authenticator」アプリに表示されているコードを再度クリックすると、「コピーしました。」と表示されます

⑲ コピーしたコードを入力し、「次へ」をクリックします

⑳ 「成功」画面で「完了」をクリックします

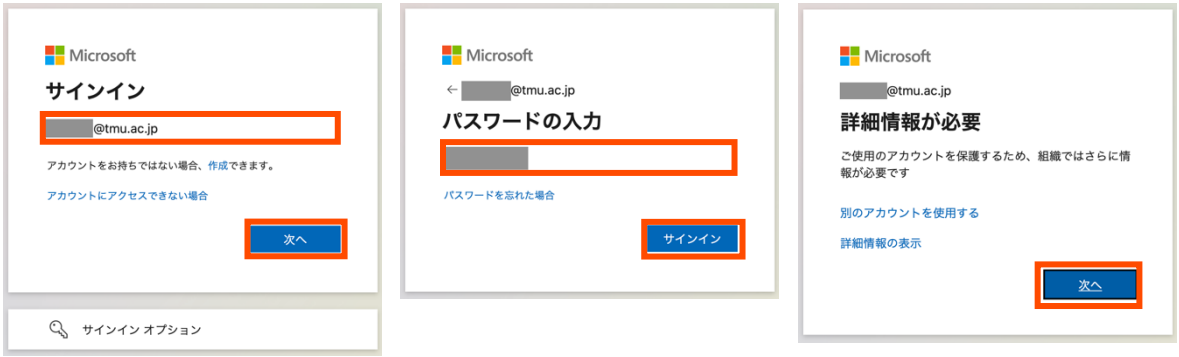
4. 音声通話(携帯電話・スマートフォン)を利用する

1 の方法よりセキュリティと可用性が劣るとされる[5]方法です。音声通話を携帯電話やスマートフォンなどのデバイスで受けるよう設定します。初期設定には音声通話を受けるデバイスとは別のデバイス(タブレットやパソコンなど画面ができるだけ大きいデバイス)が1台必要です。

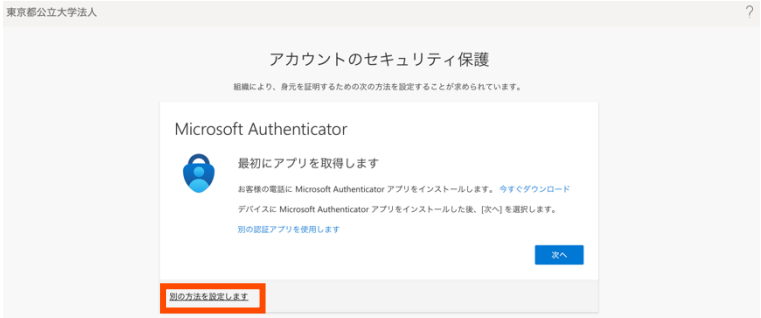
① 以下の2条件を満たすデバイス(携帯電話やスマートフォン)を手元に準備します
- 音声通話を受信可能である
- 自分が専有可能である

② 4 の①で準備したデバイス(以降、デバイスD)を傍に置いて、別のデバイス(タブレットやパソコンなど画面ができるだけ大きいデバイス、以降デバイスB)で Web ブラウザを起動し https://aka.ms/mfasetup へアクセスします

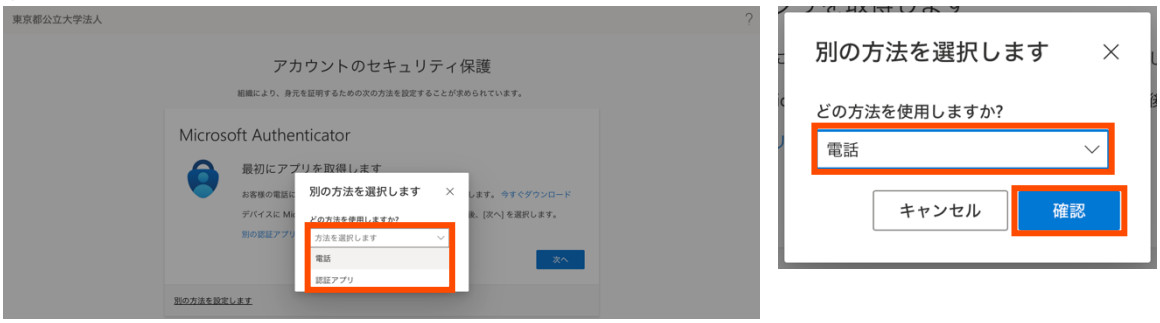
③ 「サインイン」画面で TMU ID を入力し「次へ」ボタンをクリックし、「パスワードの入力」画面でパスワードを入力し「サインイン」ボタンをクリックし、「詳細情報が必要」画面で「次へ」ボタンをクリックします



④ 「最初にアプリを取得します」画面で「別の方法を設定します」をクリックします



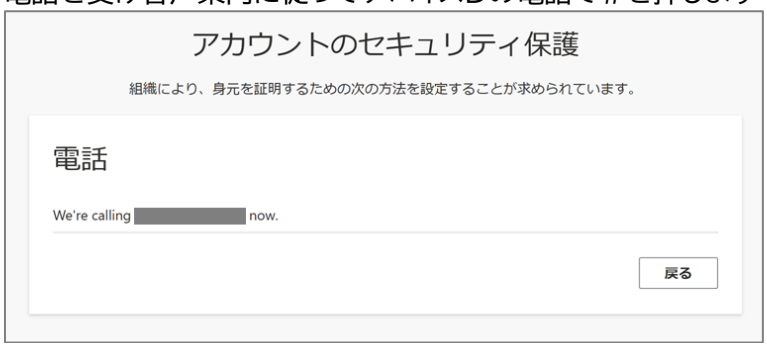
⑤ 「別の方法を選択します」画面で「方法を選択します」から「電話」を選択し、「確認」ボタンをクリックします



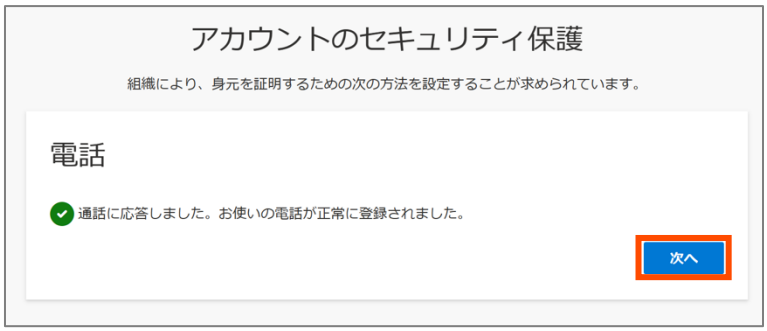
[5] https://learn.microsoft.com/ja-jp/azure/active-directory/authentication/concept-authentication-methods#authentication-method-strength-and-security

⑥　「電話」画面で「米国（+1）」を「日本（+81）」へ変更し、デバイスDの電話番号を入力し、「電話する」を選択し、「次へ」ボタンをクリックします

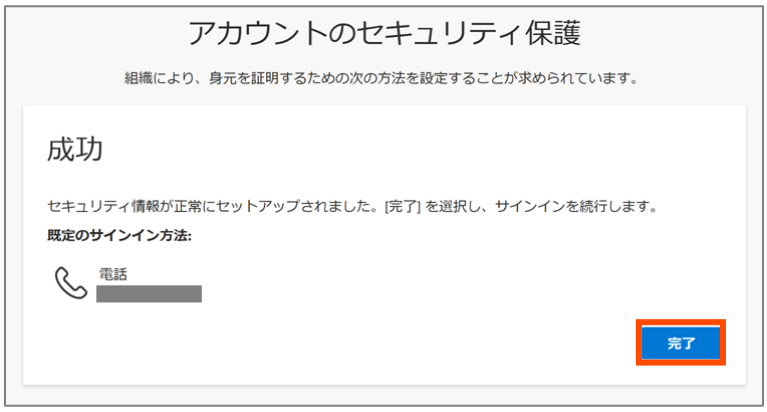
⑦　デバイスBの「電話」画面が表示されている間に Microsoft からデバイスDへ電話がかかってくるので、電話を受け音声案内に従ってデバイスDの電話で＃を押します



⑧　デバイスBの「電話」画面で「次へ」をクリックします



⑨　デバイスBの「成功」画面で「完了」をクリックします



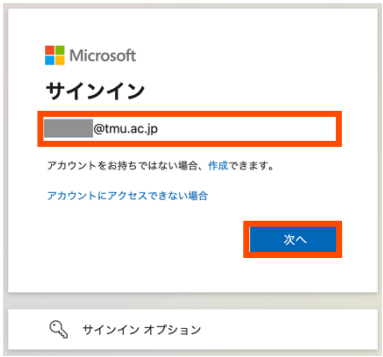
5. 音声通話(固定電話)を利用する

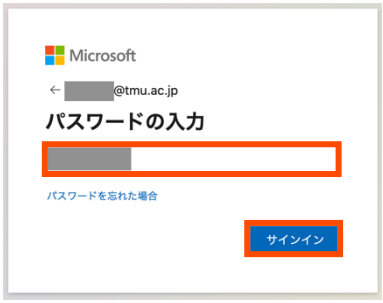
1 の方法よりセキュリティが劣り、本人確認が生じるたびにその固定電話で対応しなければならないため可用性が著しく劣るとされる方法です。音声通話を固定電話などのデバイスで受けるよう設定します。初期設定には音声通話を受けるデバイスとは別のデバイス(タブレットやパソコンなど画面ができるだけ大きいデバイス)が1台必要です。

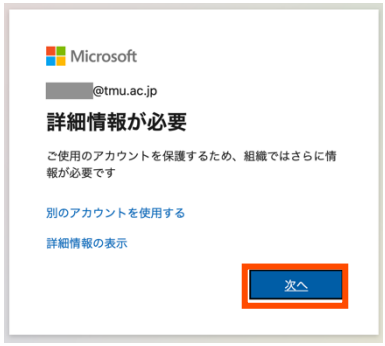
① 以下の2条件を満たすデバイス(固定電話)を手元に準備します
- 音声通話を受信可能である
- プッシュ音を送出可能である

② 5 の①で準備したデバイス(以降、デバイスE)を傍に置いて、別のデバイス(タブレットやパソコンなど画面ができるだけ大きいデバイス、以降デバイスB)で Web ブラウザを起動し https://aka.ms/mfasetup へアクセスします

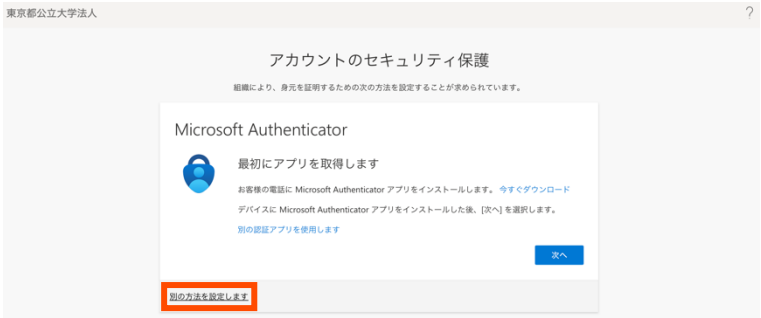
③ 「サインイン」画面で TMU ID を入力し「次へ」ボタンをクリックし、「パスワードの入力」画面でパスワードを入力し「サインイン」ボタンをクリックし、「詳細情報が必要」画面で「次へ」ボタンをクリックします



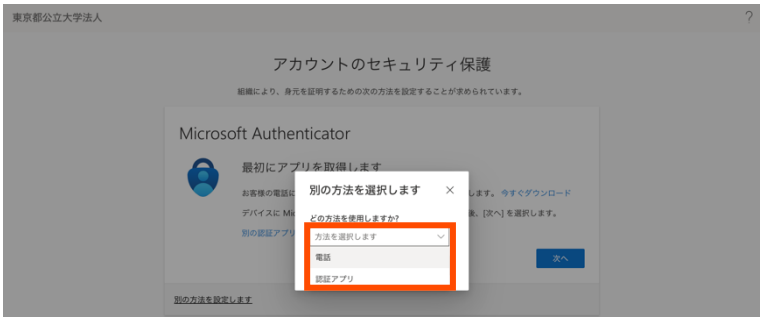


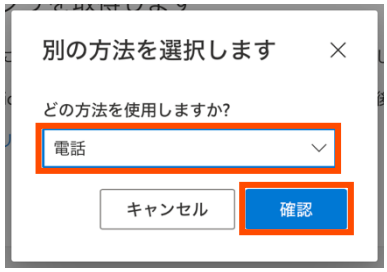


④ 「最初にアプリを取得します」画面で「別の方法を設定します」をクリックします



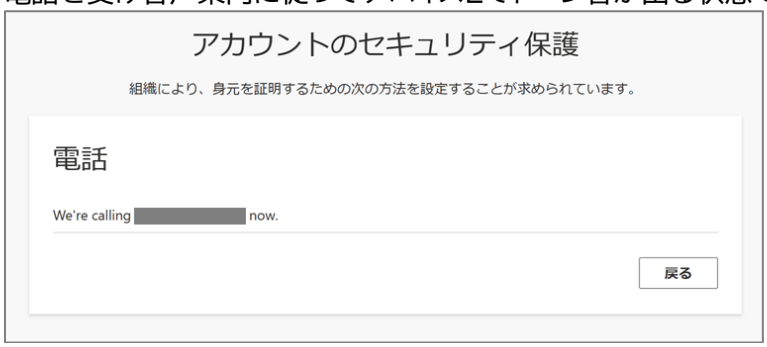
⑤ 「別の方法を選択します」画面で「方法を選択します」から「電話」を選択し、「確認」ボタンをクリックします



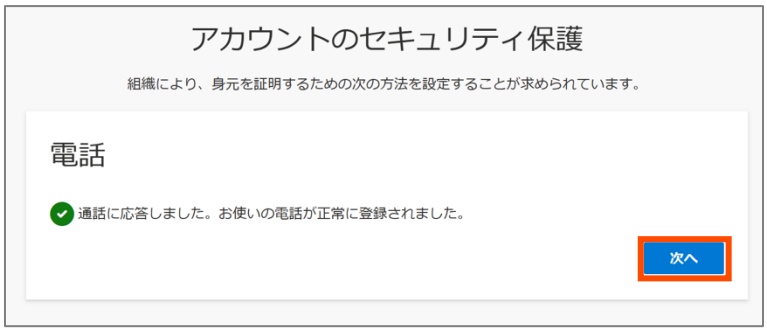


⑥　「電話」画面で「米国（+1）」を「日本（+81）」へ変更し、デバイスDの電話番号を入力し、「電話する」を選択し、「次へ」ボタンをクリックします

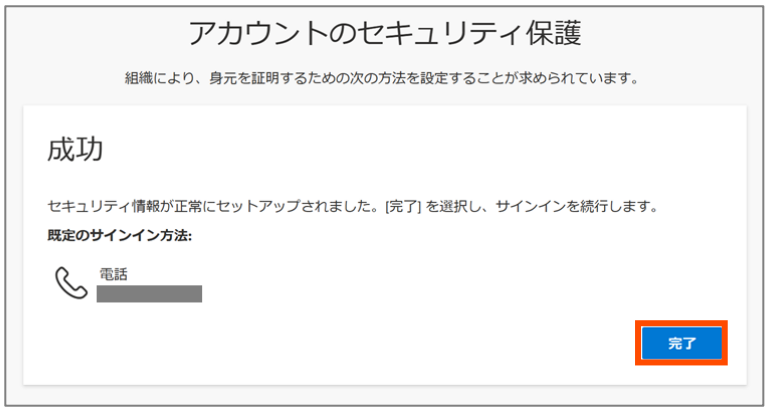
⑦　デバイスBの「電話」画面が表示されている間に Microsoft からデバイスEへ電話がかかってくるので、電話を受け音声案内に従ってデバイスEでトーン音が出る状態で＃を押します



⑧　デバイスBの「電話」画面で「次へ」をクリックします



⑨　デバイスBの「成功」画面で「完了」をクリックします



6. 複数の状況に該当する場合

本人確認に用いる別の要素は1つに限定されず、複数の要素を追加することが可能です。追加できる別の要素は、初期設定で登録できる

- 認証アプリ
- 電話

に加えて

- 代替の電話
- セキュリティ キー
- 会社の電話

があります。複数の登録がある場合、本人確認時にどの別の要素を利用するか選択できます。

また、1 のアプリ、2 のSMS、4 の音声通話を同一のスマートフォンに対して設定した場合、そのスマートフォンが故障・紛失・盗難など利用できない状況になると、サービスを利用できないだけでなく Word・Excel・PowerPoint などの Office 系アプリ(サブスクリプション版)[6]を利用できなくなる可能性もあります。携帯できるデバイスが複数ある場合は、複数のデバイスを登録することを推奨します。同時に、紛失・盗難には十分注意してください。

以下では、1～5 のいずれかを実施し「セキュリティ情報」画面が表示されている、あるいは、Web ブラウザで再度 https://aka.ms/mfasetup へアクセスし「セキュリティ情報」画面が表示されている前提で、本人確認に用いる別の要素を追加する方法を示します。なお、Authenticator 機能拡張を同じデバイスの別のブラウザに追加して利用する場合は、別のブラウザから https://aka.ms/mfasetup へアクセスしてください。

① 「サインイン方法の追加」をクリックします

② 「方法を追加します」画面で「方法を選択します」から追加したい別の要素を選択し、「追加」ボタンをクリックします

- Microsoft Authenticator アプリを別のデバイスへインストールして利用する→認証アプリ
- Authenticator 機能拡張を別のデバイスの Web ブラウザに追加して利用する→認証アプリ
- 大学の居室の電話への音声通話を利用する→会社の電話
- その他の電話への音声通話を利用する→代替の電話

③ 追加する別の要素に応じて対応する方法を参照し実施してください

- Microsoft Authenticator アプリを別のデバイスへインストールして利用する→1 の⑤へ
- Authenticator 機能拡張を別のデバイスの Web ブラウザに追加して利用する→3 の⑩へ
- 代替の電話、会社の電話を利用する→5 の⑥へ

---

[6] 東京都立大学を設置運営する東京都公立大学法人が契約する Microsoft 365 で提供されるオンライン版およびインストール版アプリ