

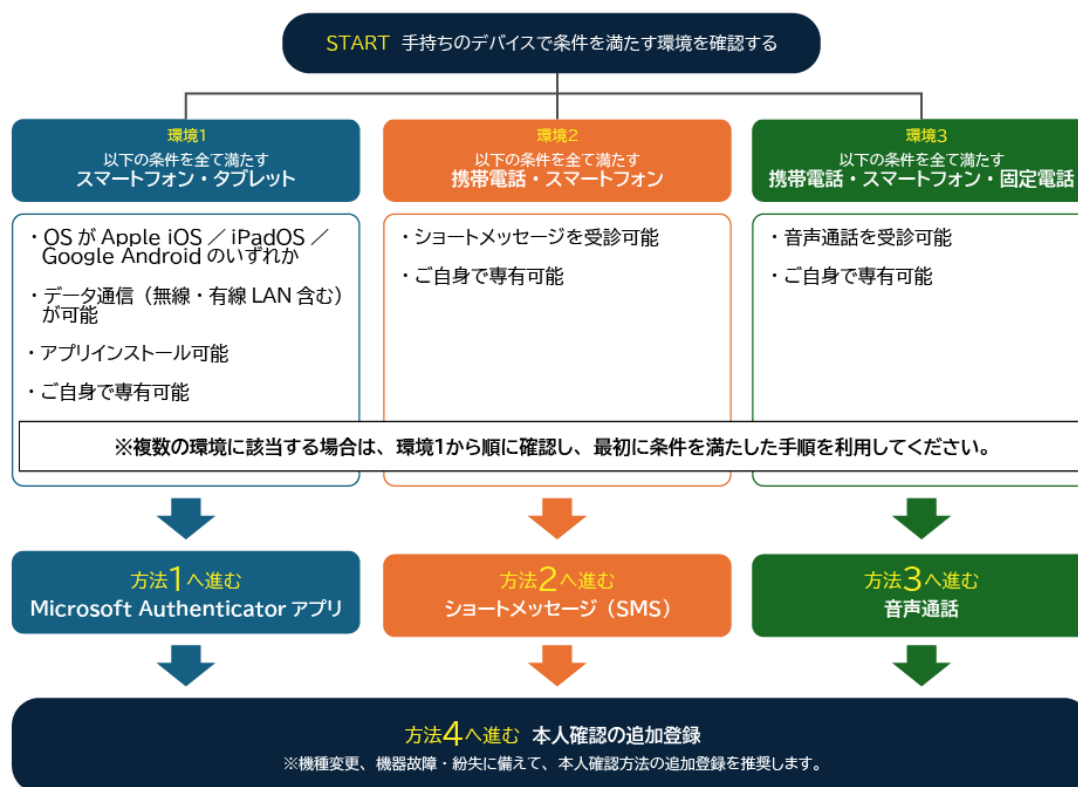
都立大教研システムにおける多要素認証(MFA)の初期設定方法

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(以下、「都立大教研システム」という。)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 3 つ示されています。ご自身の環境に応じて取りうる方法が変わるので、下図を参照の上、ご自身がどの環境に該当するかを確認して、初期設定を実施してください。複数の環境(デバイス)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を実施してください。

また、スマートフォンの機種変更に伴って、都立大教研システムのサービスが利用できなくなったというご連絡を多くいただいております。このような事態を未然に防ぐため、以下の環境1～3にて初期設定を実施した後、「4 複数の本人確認方法の追加登録」についてもご一読の上、可能な範囲で複数の本人確認方法の登録をご検討ください。

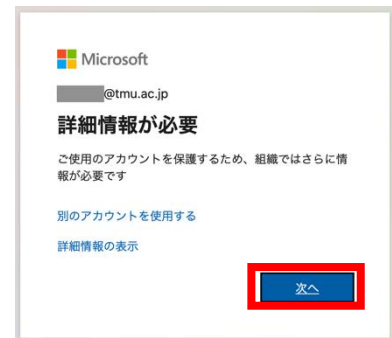
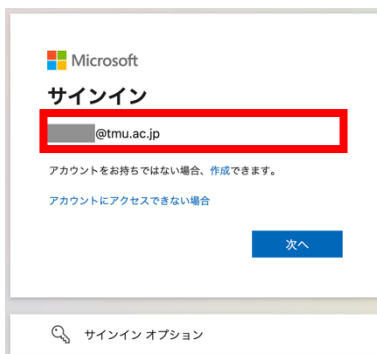
環境1	以下の4条件を全て満たすデバイス(スマートフォン、タブレット等)がある→1 へ ● OS が Apple iOS、Apple iPadOS、Google Android のいずれかで ● データ通信(無線 LAN 接続や有線 LAN 接続も含む)可能 ● アプリをインストール可能 ● ご自身で専有可能
環境2	以下の2条件を全て満たすデバイス(携帯電話やスマートフォン)がある→2 へ ● ショートメッセージを受信可能 ● ご自身で専有可能
環境3	以下の2条件を全て満たすデバイス(携帯電話、スマートフォン、固定電話)がある→4 へ ● 音声通話を受信可能 ● ご自身で専有可能



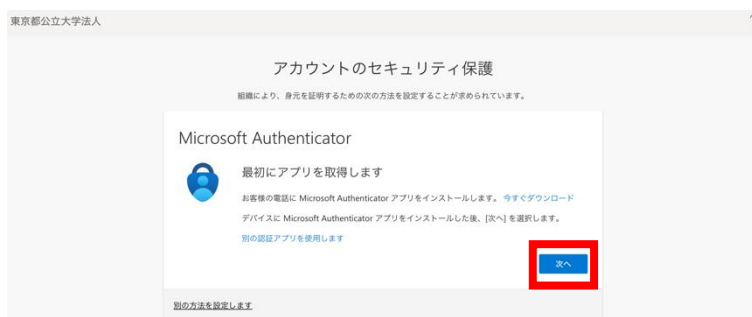
1. Microsoft Authenticator アプリを利用する

Microsoft が推奨する方法です。Microsoft Authenticator アプリをスマートフォン、タブレット等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、パソコン等の画面ができるだけ大きいデバイス)が1台必要です。

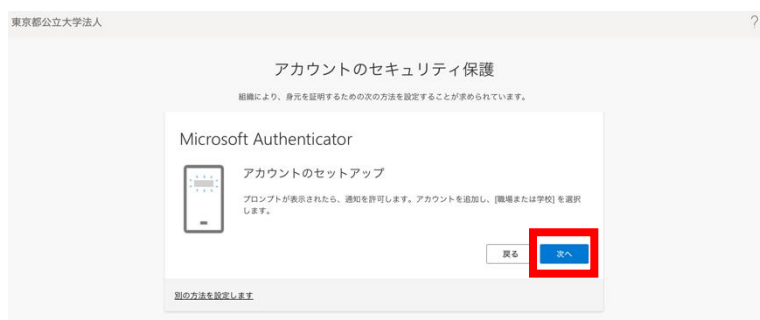
- ① 以下の4条件すべてを満たすデバイス(スマートフォンやタブレットなど)へ
<https://www.microsoft.com/ja-jp/security/mobile-authenticator-app> から Microsoft Authenticator アプリをインストールします。
 - OS が Apple iOS、Apple iPadOS、Google Android のいずれか
 - データ通信(無線 LAN 接続や有線 LAN 接続も含む)可能
 - アプリインストール可能
 - ご自身で専有可
- ② 1の①で Microsoft Authenticator アプリをインストールしたデバイス(以下、「デバイスA」という。)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、パソコン等の画面ができるだけ大きいデバイス。以下、「デバイスB」という。)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て「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。

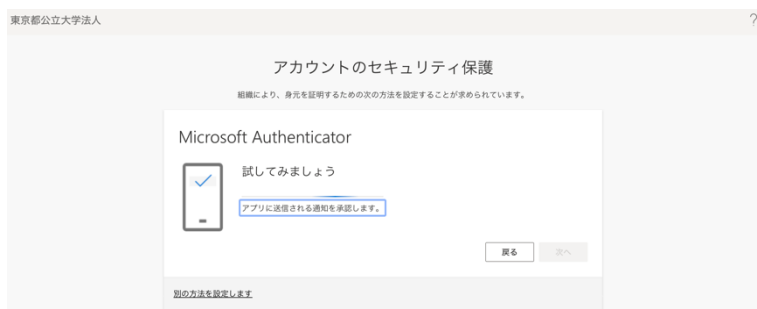


デバイスAにカメラがない、あるいは、デバイスAのカメラを利用できない場合は、デバイスBの「画像をスキャンできませんか？」ボタンをクリックし、デバイスAで「職場または学校アカウントの追加」ボタンをタップし、ポップアップ画面で「QR コードをスキャンします」をタップし、「QR コードをスキャン」画面で「またはコードを手動で入力」ボタンをタップし、デバイスBに表示された「コード」と「URL」をデバイスAの「コード」と「URL」へ入力し、デバイスBの画面の「次へ」をクリックします。

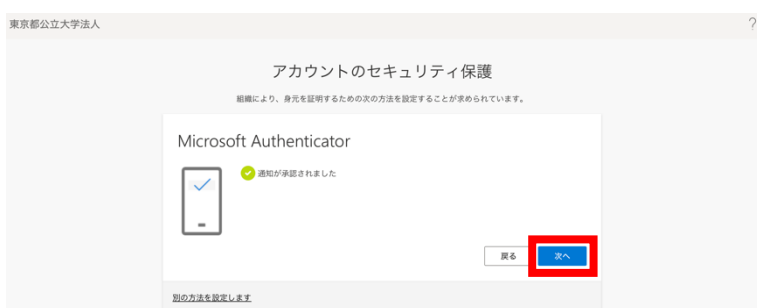


- ⑧ デバイスBに「試してみましょう」と表示されている間に、デバイスAに「サインインを承認しますか?」と表示されたら「承認」をタップします。

※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。



注意1) Microsoft Authenticator アプリには、支払に関する情報を登録する機能がありますが、支払情報等を登録せずにご利用いただけます。(クレジットカード情報の入力等は必要ありません。)

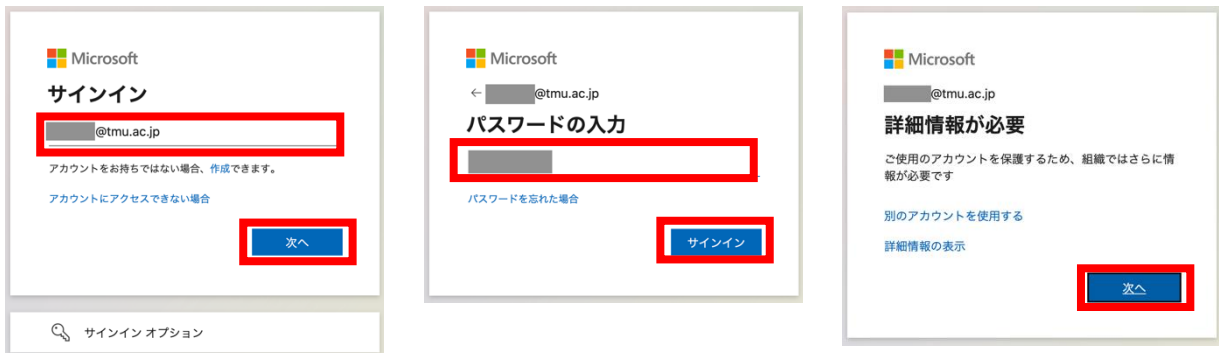
注意2) 別のデバイス(スマートフォン、タブレット端末等)へ乗り換える際には、新しいデバイスで Microsoft Authenticator アプリを設定するだけでなく、古いデバイスで Microsoft Authenticator でも移行設定が必要です。移行設定が完了するまで古いデバイスを廃止しないでください。移行方法については下記ページをご確認ください。

[Microsoft Authenticator の移行方法\(Microsoft サポートブログ\)](#)

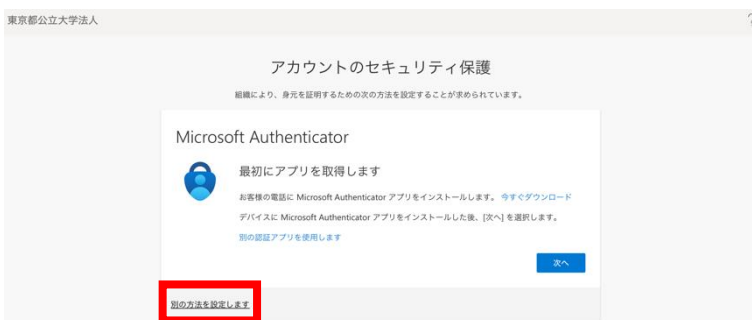
2. ショートメッセージ(short message service、SMS)を利用する

1の方法よりセキュリティが劣るとされる方法です。SMSを携帯電話、スマートフォン等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、パソコン等画面ができるだけ大きいデバイス)が1台必要です。

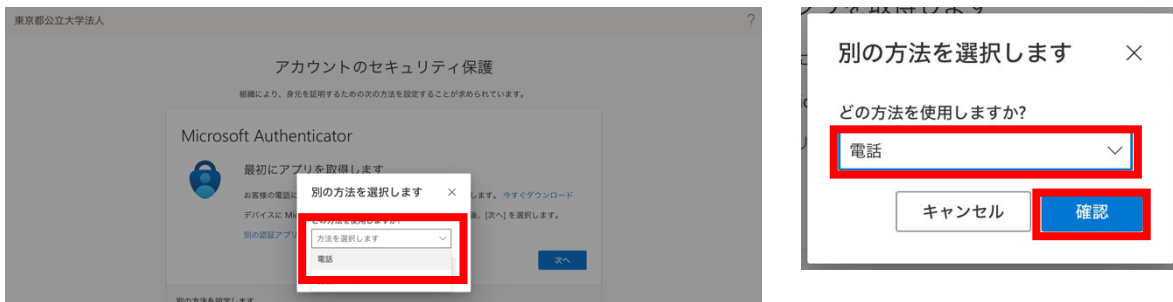
- ① 以下の2条件を満たすデバイス(携帯電話やスマートフォン)を手元に準備します。
 - SMSを受信可能
 - ご自身で専有可
- ② 2の①で準備したデバイス(以下、「デバイスC」という。)を傍に置いて、別のデバイス(タブレット、パソコン等の画面ができるだけ大きいデバイス。以下、「デバイスB」という。)で Web ブラウザを起動し、<https://aka.ms/mfasetup> へアクセスします。
- ③ デバイスBに表示される「サインイン」画面で TMU ID を入力し「次へ」ボタンをクリックし、「パスワードの入力」画面でパスワードを入力して「サインイン」ボタンをクリックし、「詳細情報が必要」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Cの電話番号を入力し、「次へ」ボタンをクリックします。

The screenshot shows the 'アカウントのセキュリティ保護' (Account Security Protection) screen. Under the '電話' (Phone) section, there is a dropdown menu for the country code, currently set to 'United States (+1)'. A red box highlights this dropdown and the '次へ' (Next) button. Below the dropdown, there is a radio button selection for 'コードをSMS送信する' (Send code via SMS) and '電話する' (Call). A text input field for the phone number is also visible, with a red box around it. The '次へ' button is at the bottom right.

- 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。

This screenshot shows the '電話' (Phone) step where a 6-digit code is entered. A red box highlights the input field for the code and the '次へ' (Next) button. The '戻る' (Back) button is also visible.

- ⑧ デバイスBの「電話」画面で「次へ」をクリックします。

This screenshot shows the '電話' (Phone) step with a confirmation message: 'SMS が検証されました。お使いの電話が正常に登録されました。' (SMS has been verified. Your phone has been successfully registered). A red box highlights the '次へ' (Next) button.

- ⑨ デバイスBの「成功」画面で「完了」をクリックします。

This screenshot shows the '成功' (Success) step with a message: 'セキュリティ情報が正常にセットアップされました。[完了] を選択し、サインインを続行します。' (Security information has been successfully set up. Select [Complete] and continue with sign-in). A red box highlights the '完了' (Complete) button.

3. 音声通話(携帯電話・スマートフォン・固定電話)を利用する

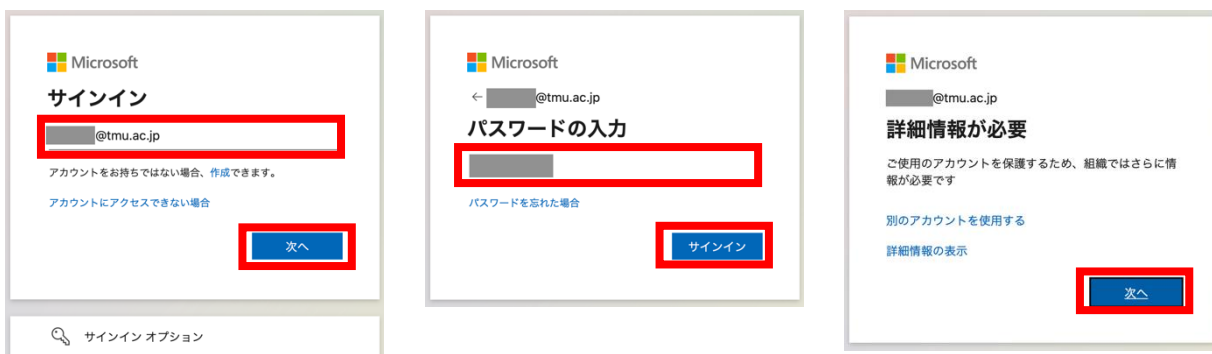
1の方法よりセキュリティと可用性が劣るとされるⁱⁱⁱ方法です。音声通話を携帯電話、スマートフォン等のデバイスで受けるよう設定します。初期設定には音声通話を受けるデバイスとは別のデバイス(タブレット、パソコン等画面ができるだけ大きいデバイス)が1台必要です。

① 以下の2条件を満たすデバイス(携帯電話、スマートフォン、固定電話)を手元に準備します。

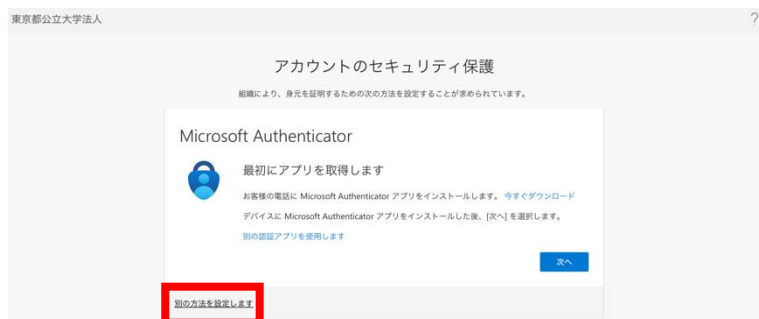
- 音声通話を受信可能
- ご自身で専有可

② 3の①で準備したデバイス(以下、「デバイスD」という。)を傍に置いて、別のデバイス(タブレット、パソコン等画面ができるだけ大きいデバイス。以下、「デバイスB」という。)で Web ブラウザを起動し、<https://aka.ms/mfasetup> へアクセスします。

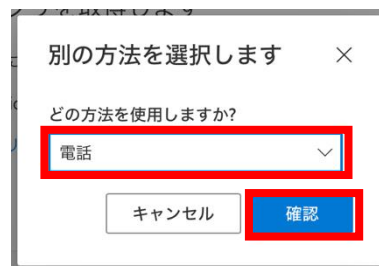
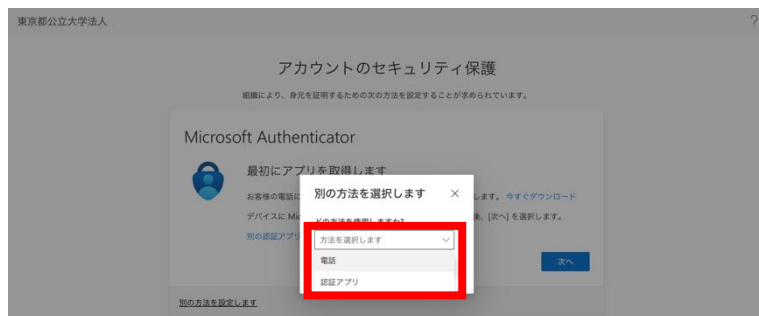
③ 「サインイン」画面で TMU ID を入力し「次へ」ボタンをクリックし、「パスワードの入力」画面でパスワードを入力し「サインイン」ボタンをクリックし、「詳細情報が必要」画面で「次へ」ボタンをクリックします。



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。

東京都市立大学法人

アカウントのセキュリティ保護

組織により、身元を証明するための次の方法を設定することが求められています。

電話

電話で呼び出しに応答するか、携帯ショートメール (SMS) によるコードの送信により、本人確認ができます。

どの電話番号を使用しますか?

United States (+1) 電話番号を入力します

☐ コードを SMS で送信する

☒ 電話する

Microsoft 365 の通信料が適用される場合があります。[次へ] を選択すると、次に開画したことになります。サービス使用条件 および プライバシーと Cookie に関する声明

次へ

別の方法を設定します

- 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。
- ※固定電話がダイヤル回線の場合は、トーンボタン(*)を押した後にシャープ(#)ボタンを押してください。

アカウントのセキュリティ保護

組織により、身元を証明するための次の方法を設定することが求められています。

電話

We're calling [redacted] now.

戻る

- ⑧ デバイスBの「電話」画面で「次へ」をクリックします。

アカウントのセキュリティ保護

組織により、身元を証明するための次の方法を設定することが求められています。

電話

✓ 通話に応答しました。お使いの電話が正常に登録されました。

次へ

- ⑨ デバイスBの「成功」画面で「完了」をクリックします。

アカウントのセキュリティ保護

組織により、身元を証明するための次の方法を設定することが求められています。

成功

セキュリティ情報が正常にセットアップされました。[完了] を選択し、サインインを続行します。

既定のサインイン方法:

電話 [redacted]

完了

4. 本人確認方法の追加登録(推奨)

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(Microsoft Authenticator アプリ等)
- 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、3 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・機種変更等で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 等の Office アプリ(サブスクリプション版)^{iv}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。

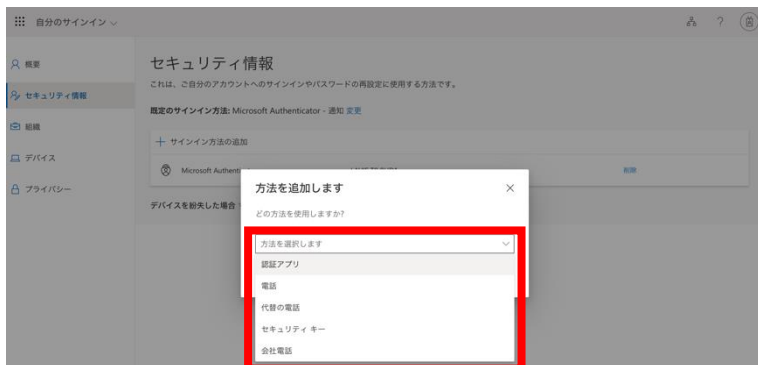
以下では、1、2、3 いずれかを実施し「セキュリティ情報」画面が表示されている、あるいは、Web ブラウザで再度 <https://aka.ms/mfasetup> へアクセスし「セキュリティ情報」画面が表示されている前提で、本人確認に用いる別の要素を追加する方法を示します。

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
- 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
- 代替の電話、会社の電話を利用する→3 の⑥へ

ⁱ 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)

ⁱⁱ <https://learn.microsoft.com/ja-jp/azure/active-directory/authentication/concept-authentication-methods#authentication-method-strength-and-security>

ⁱⁱⁱ <https://learn.microsoft.com/ja-jp/azure/active-directory/authentication/concept-authentication-methods#authentication-method-strength-and-security>

^{iv} 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。