
明治学院大学 Microsoft 365

多要素認証 設定マニュアル

Multi-Factor Authentication : MFA

明治学院大学 情報センター

2023年9月27日



目次

1 はじめに.....	3
1-1 多要素認証の必要性.....	3
1-2 多要素認証(MFA)とは.....	3
1-3 多要素認証を要求されるログイン.....	3
1-4 多要素認証の対象者.....	3
2 設定作業の流れ.....	4
3 準備.....	5
3-1 認証のタイプを決める.....	5
(1) 電話認証.....	5
(2) SMS 認証.....	5
(3) アプリ認証.....	5
3-2 設定作業の事前準備.....	6
(1) 電話認証の事前準備.....	6
(2) SMS 認証の事前準備.....	6
(3) アプリ認証の事前準備.....	6
4 設定の手順.....	7
4-1 MGメールにサインイン.....	7
4-2 設定の開始.....	7
(A) 「詳細情報が必要」メッセージからの開始.....	7
(B) 「Outlook」からの開始.....	8
4-3 タイプ別の設定手順.....	8
(1) 電話認証.....	9
(2) SMS 認証.....	10
(3) アプリ認証.....	11
5 設定の確認 / 追加 / 変更 / 削除.....	14
5-1 「サインイン方法」を追加したいとき.....	14
5-2 「規定のサインイン方法」を別の方法に変更したいとき.....	14
5-3 不要なサインイン方法を削除したいとき.....	14
5-4 電話番号の認証タイプを変更したいとき.....	14
6 認証.....	15
6-1 認証を要求される場面.....	15
6-2 認証の手順.....	15
(1) 電話認証.....	15
(2) SMS 認証.....	15
(3) アプリ認証.....	15
6-3 認証を試行して動作を確認する方法.....	16
6-4 認証における注意点.....	16
7 その他.....	17
7-1 登録 / 登録解除.....	17
7-2 よくある質問.....	17
7-3 問い合わせ先.....	17

1 はじめに

1-1 多要素認証の必要性

本学では、学生・教職員に対して、大学としてのアカウント「MAINアカウント」を配布しています。

MAINアカウントは「ID」と「パスワード」で構成され、統合認証システムにより、Microsoft 365やmanabaなど様々な学内サービスに対して、個々のサインインを省略し効率よく利用できます。

その反面、単純なパスワードを推測されたり、解析プログラムによる方法で取得されたり、何らかの方法でパスワードが盗まれ、「なりすまし」による学内システムへ不正にアクセスされると、学内外に重大な損害を及ぼす恐れがあります。そのため、近年、多くの大学がMicrosoft365のセキュリティ強化を目的とした「多要素認証」を導入しています。

1-2 多要素認証(MFA)とは

- 認証方法の3要素とは、
 - ① 知識情報 : 自分が知っている、ID、パスワードや秘密の質問など
 - ② 所持情報 : 自分が所持している、スマホや携帯電話など
 - ③ 生体情報 : 自分の身体の、指紋、顔、虹彩など
- 多要素認証とは、
 - 上記の2つ以上の要素を組み合わせることで認証する方法です。
 - 本人以外からの不正アクセスを防止する効果があります。
- Microsoft365 では、現在の「知識情報」の認証に、「所持情報」による認証を追加します。
 - ① 知識情報 : MAINメインアカウント (IDとパスワード) ←現状
 - ② 所持情報 : スマートフォンや携帯電話、固定電話等の認証 ←これを追加します

1-3 多要素認証を要求されるログイン

- 学外ネットワーク（自宅や外部の無線LAN（Wi-Fi）、携帯電話回線など）から、MAINアカウントでサインインする際に、多要素認証を要求されます。
- 認証情報は、ブラウザや端末に一定期間記憶されている場合があります。

1-4 多要素認証の対象者

- 教員、学生、卒業生、職員に対して、必須と申請制に分かれます。
- 対象者、スケジュール等の詳細は、メールにて通知します。

3 準備

3-1 認証のタイプを決める

- 認証の種類は、下記の3タイプです。各自で所持している端末の種類により、タイプを選択してください。
- 認証方法の詳細は、「6.認証」(P.15)を参照

	認証方法	スマホ	携帯電話	固定電話
1	電話認証 (音声)	○	○	○
2	SMS認証 (ショートメッセージ)	○	○	×
3	アプリ認証 (Microsoft Authenticator)	○	×	×

(1) 電話認証



- 対象端末：スマホ / 携帯 / 固定電話
- 認証方法：自動音声の電話がかかります。その指示に従い操作します。
- 通信方法：電話 (音声送信)

(2) SMS 認証



- 対象端末：スマホ / 携帯
- 認証方法：SMSに確認コードが届きます。そのコードを認証画面に入力します。
- 通信方法：電話 (テキスト送信)

(3) アプリ認証



- 対象端末：スマホ
- 認証方法：認証画面に表示された番号を、スマホのアプリに入力します。
- 通信方法：インターネット

■ 注意点

- 機種変更や電話番号の変更に備えて、2つ以上の方法を登録してください。
- 別の端末で、同じタイプの方法を選択することも可能です。
- 携帯電話番号を登録した場合、電話認証とSMS認証の両方が選択できます。
- 設定した認証方法の変更は、いつでも可能です。
- タブレットやトークン等の機器は、対応していない場合があります。自己責任で利用してください。

■ 登録例 (参考) ※ひとつ目の認証は、電話認証を推奨します。



	スマホユーザー	携帯ユーザー
ひとつ目の認証	スマホ : 電話認証	携帯 : 電話認証
ふたつ目の認証	スマホ : アプリ認証	自宅電話 : 電話認証
予備	固定電話 : 電話認証	タブレット : アプリ認証

3-2 設定作業の事前準備

- 設定作業は、途中でネットワークが途切れないよう、良好な通信環境で行ってください。
- 設定作業が長時間になると、「タイムアウト」になります。また、設定を複数回繰り返すと、「アカウントにロック」がかかる場合もありますので、作業がスムーズに行えるよう準備を整えてから開始してください。

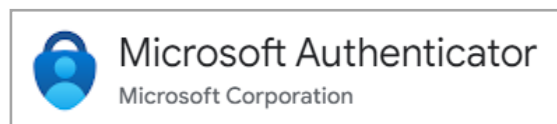
(1) 電話認証の事前準備

- 対象となる電話をすぐにとれる環境下で行ってください。

(2) SMS 認証の事前準備

- SMSを受信できるスマホ・携帯電話を準備してください。

(3) アプリ認証の事前準備



- 公式アプリサイト（App Store / Google Play）から「**Microsoft Authenticator**」をダウンロードして、インストールしてください。
※検索では、他社の認証アプリも表示されますので、注意して選択してください。
- 詳細は、下記の「Microsoft公式サイト」を参照してください。
[Microsoft のスマートフォン認証アプリ | Microsoft Security](#)
- 下記のQRコードからもアクセスできます。



Google Play



App Store

4 設定の手順

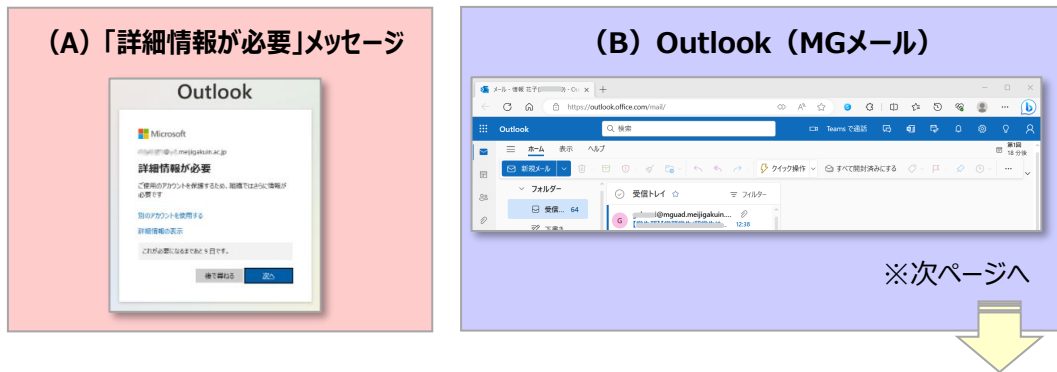
4-1 MGメールにサインイン

- パソコンで[Microsoft 365 \(MGメール\) にサインイン](#)します。



4-2 設定の開始

- 接続しているネットワークの違い（学内/学外）や、対象アカウントの多要素認証の設定期間開始前/後などの条件により、2種類の表示があります。表示されたパターンの手順を参照してください。



(A) 「詳細情報が必要」メッセージからの開始

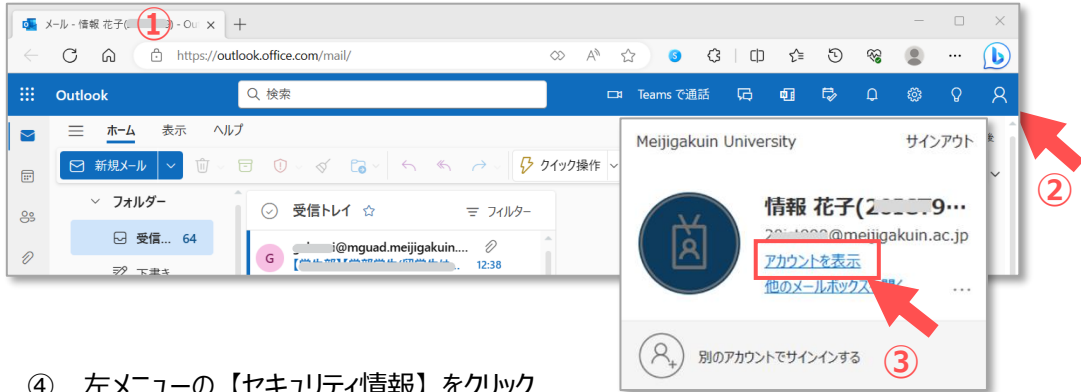
- ① 「詳細情報が必要」のメッセージに【次へ】をクリック
- ② 「アカウントのセキュリティ保護」のメッセージは、認証タイプにより、クリック位置が異なります。
 - a) 電話 / SMS → 【別の方法を設定します】をクリック
 - b) アプリ → 【次へ】をクリック



- ③ 4-3 「タイプ別の設定手順」に進みます。

(B) 「Outlook」からの開始

- ① Outlook (MGメール) が開きます。
- ② Outlookの【ユーザーアイコン】(アカウントマネージャー) をクリック
- ③ 【アカウントを表示】をクリック



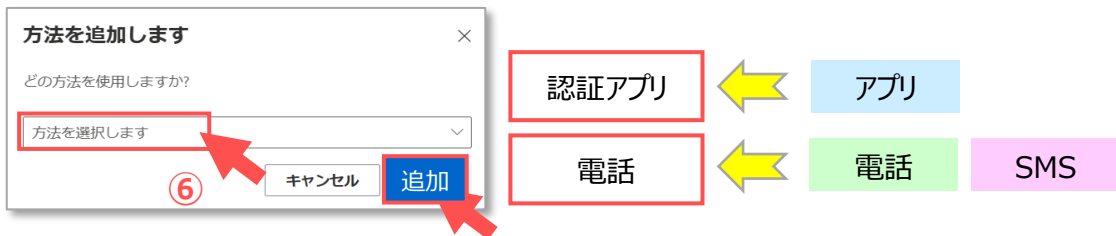
- ④ 左メニューの【セキュリティ情報】をクリック



- ⑤ 【+ サインイン方法の追加】をクリック



- ⑥ 【方法を選択します】の選択肢から、「方法」を選択し、【追加】をクリック
 - a) アプリを使用する → 【認証アプリ】を選択
 - b) アプリを使用しない → 【電話】を選択



4-3 タイプ別の設定手順

- タイプ別の設定手順のページを参照してください。
 - (1) 電話認証 ※P.9 参照
 - (2) SMS認証 ※P.10 参照
 - (3) アプリ認証 ※P.11~13 参照

(1) 電話認証

- ① 【電話】を選択して、【追加】をクリック。

方法を追加します

どの方法を使用しますか?

電話

キャンセル 追加



- ② 「電話」のメッセージが表示されます。

電話

電話で呼び出しに응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?

日本 (+81) 07011111111

コードを SMS 送信する

電話する

メッセージとデータ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、次に同意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。

キャンセル 次へ

- a) 「日本」を選択
b) 電話番号 (ハイフンなし) を入力
c) 「電話する」をチェック

上記をセットして、【次へ】をクリック

電話

We're calling +81 07011111111 now.

戻る

- ③ 指定した電話番号の端末にMicrosoftから、電話 (自動音声) がかかってきます。

例) 「こちらはMicrosoftです。サインインしようとしたか?
サインインする場合は、「#」キーを押してください。」
⇒音声で指示された電話機のボタンを押します。



- ④ 確認メッセージに【完了】をクリック。

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。

完了

- ⑤ セキュリティ情報に電話認証が追加されます。

セキュリティ情報

これは、ご自分のアカウントへのサインインやパスワードの再設定に使用する方法です。

既定のサインイン方法: 電話 - テキスト +81 05...1 変更

+ サインイン方法の追加

電話 +81 05...1 変更 削除

(2) SMS 認証

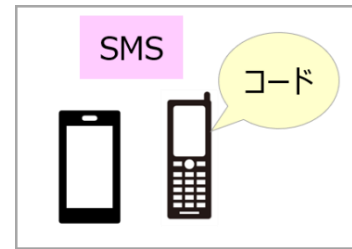
- ① 【電話】を選択して、【追加】をクリック。

方法を追加します

どの方法を使用しますか?

電話

キャンセル 追加



- ② 「電話」のメッセージが表示されます。

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?

米国 (+1)

電話番号を入力します

コードをSMS送信する

電話する

メッセージとデータ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、次に同意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。

キャンセル 次へ

- a) 「日本」を選択
b) 電話番号 (ハイフンなし) を入力
c) 「コードをSMS送信する」をチェック

上記をセットして、【次へ】をクリック

- ③ 指定した電話番号の端末にMicrosoftから、SMS (ショートメッセージ) で確認コード (6桁の数字) が届きます。
- ④ コードを入力して、【次へ】をクリック。

確認コード

SMS

電話

+81 09C-411 に6桁のコードをお送りしました。コードを以下に入力してください。

コードの入力 **コードを入力**

コードの再送信

戻る 次へ

- ⑤ 【完了】をクリック。

電話

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。

完了

- ⑥ セキュリティ情報にSMS認証が追加されます。

セキュリティ情報

これは、ご自分のアカウントへのサインインやパスワードの再設定に使用する方法です。

既定のサインイン方法: 電話 - テキスト +81 09-411-1111 変更

+ サインイン方法の追加

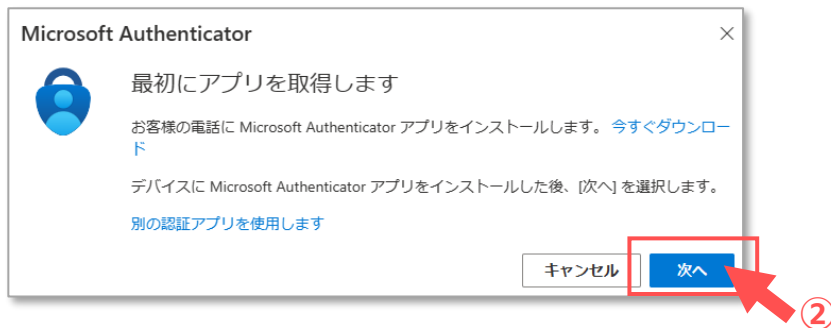
電話 +81 09-411-1111 変更 削除

(3) アプリ認証

- ① 【認証アプリ】を選択して、【追加】をクリックします。



- ② 「最初にアプリを取得します」のメッセージに【次へ】をクリック。
※認証アプリは、事前にインストールしておいてください。 2-4ページ参照



- ③ 「アカウントのセットアップ」のメッセージに【次へ】をクリックします。



- ④ 「QRコードをスキャンします」のメッセージが表示されます。



- ⑤ スマホで、「Microsoft Authenticator」を起動します。
- ⑥ 右上の【スキップ】をタップ
- ⑦ 右上の【+】または、【アカウントを追加】をタップ
- ⑧ 【職場または学校アカウント】をタップ

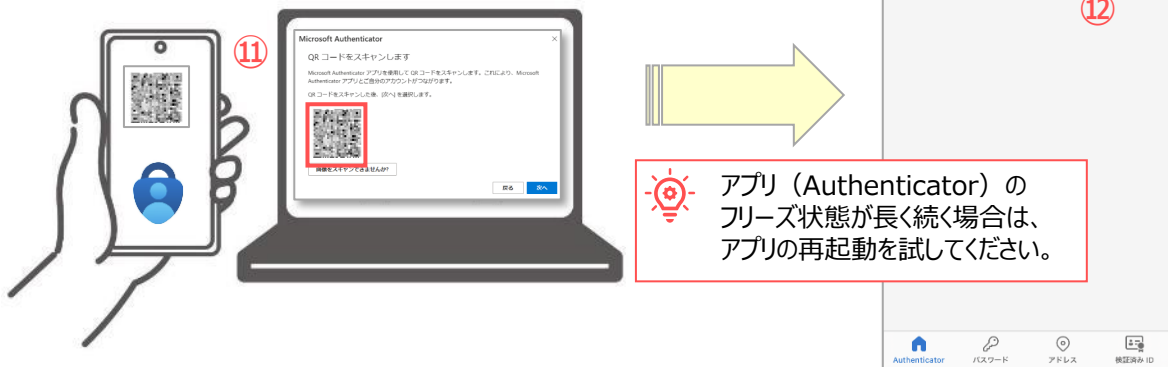
! 各種の条件により、画面や手順が若干異なります。



- ⑨ 【QRコードをスキャン】をタップ
- ⑩ 「カメラのアクセス許可」 → 【OK】をタップすると、カメラが起動します。



- ⑪ PCに表示されている【QRコード】をスマホのカメラで読み取ります。 ※④参照
※「通知の送信」を要求された際は、【許可】をクリック
- ⑫ 「Microsoft Authenticator」にMAINアカウントが追加されます。

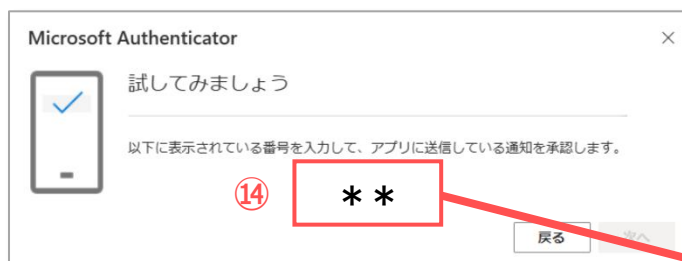


! アプリ (Authenticator) のフリーズ状態が長く続く場合は、アプリの再起動を試してください。

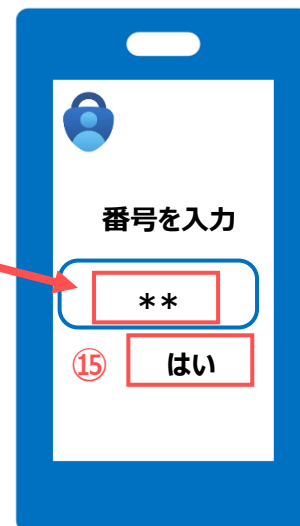
- ⑬ パソコン画面に戻り、④「QRコードをスキャンします」のメッセージに、【次へ】をクリック。



- ⑭ 画面に「試してみましょう」のメッセージが表示されます。



- ⑮ スマホに、認証画面が表示されます。
- ・ パソコンに表示された【番号】を入力
 - ・ 【はい】をタップ



- ⑯ 「通知が承認されました」のメッセージに【次へ】をクリック。



- ⑰ セキュリティ情報にアプリ認証が追加されます。



5 設定の確認 / 追加 / 変更 / 削除

- Microsoft 365の「セキュリティ情報」を確認します。

「セキュリティ情報」の開き方は、【4-2. (B) 「Outlook」からの開始】を参照
または、[セキュリティサイト](https://mysignins.microsoft.com/security-info) (<https://mysignins.microsoft.com/security-info>) にアクセスします

- 追加/変更/削除が必要なときは、下記の方法で行います。



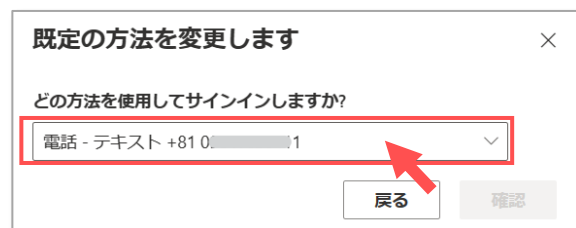
5-1 「サインイン方法」を追加したいとき

- 【+ サインイン方法の追加】をクリック ※4-2 (B) 参照

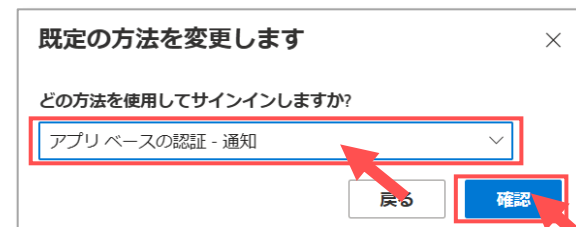
5-2 「規定のサインイン方法」を別の方法に変更したいとき

- 既定のサインイン方法の【変更】をクリック

- ① 【変更】をクリック
- ② 選択枠をクリック
設定されている方法が表示されます。



- ③ 既定 (デフォルト) にしたい方法を選択
- ④ 【確認】をクリック



5-3 不要なサインイン方法を削除したいとき

- 該当する端末の右側の【削除】をクリック

5-4 電話番号の認証タイプを変更したいとき

- 該当する電話の右側の【変更】をクリック

※「電話」は、SMS認証 (テキスト) と電話認証 (音声) との入替えができます。

6 認証

6-1 認証を要求される場面

- 学外ネットワーク（自宅や外部の無線LAN、携帯電話回線など）から、Microsoft 365にサインインするとき。
- Microsoft 365「マイアカウント」内の「セキュリティ情報」にアクセスするとき。



6-2 認証の手順

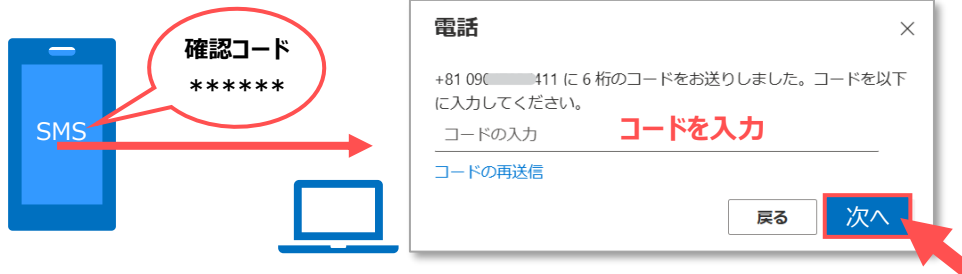
(1) 電話認証

- ① 指定した電話番号の端末にMicrosoftから、電話（自動音声）がかかります。
- ② 「こちらはMicrosoftです。サインインしようとしたらか？ サインインする場合は、「#」キーを押してください。」
- ③ 音声で指示された「ボタン」を押します。



(2) SMS 認証

- ① 登録した電話番号のSMS（ショートメッセージ）に【コード】が送信されます。
- ② PC画面に表示されたメッセージに【コード】を入力して、【次へ】をクリックします。



(3) アプリ認証

- ① PC画面に「サインイン要求を承認」のメッセージが表示されます。
- ② スマホアプリ「Microsoft Authenticator」にメッセージが届きます。
- ③ PC画面に表示された【番号】をスマホアプリに入力し、【はい】をタップします。



6-3 認証を試行して動作を確認する方法

- ① パソコンのWebブラウザで、プライベート（シークレット） ウィンドウを起動
- ② Microsoftのセキュリティサイトにアクセス
(<https://mysignins.microsoft.com/security-info>)
- ③ MAINアカウントでサインイン ※省略あり
- ④ 「規定のサインイン方法」で認証要求が送信されます。
- ⑤ 端末を使用して認証します。



6-4 認証における注意点



● 不審な認証の要求には「承認」しないでください。

- 自分がサインインを試みていないのに認証を要求された場合は、悪意のある攻撃者がサインインを試みている可能性もあります。必ず「拒否」をしてください。
- 電話の場合は、すぐに電話を切ってください。
- 普段その電話を利用する方にも、不用意に承認しないよう伝えておいてください。
- パスワードを窃取されている可能性が高いため、速やかにパスワードを変更してください。

● 登録したスマホや携帯電話を紛失したときは、

- 学内ネットワークに接続するなど、ログインできるパソコンがある場合は、速やかに紛失した端末の登録を削除してから、Microsoft 365のパスワードを変更し、サインアウトしてください。
- 紛失した端末の認証登録を削除できない場合は、情報センターにご連絡ください。

● 電話番号やスマートフォンを変更する時は、

- 対象となる電話番号やスマートフォンが使用できるうちに、パソコンで対象の番号や端末の登録を削除しておいてください。

※予め削除せずに以下のようなパターンで進めてしまった場合、何もできなくなってしまう。

- 携帯番号しか登録していないのに、携帯番号を変更してしまう。
- スマホアプリしか登録していないのに、スマホを機種変更してしまう。
- 携帯番号とスマホアプリを登録したが、携帯番号とスマホを同時に変更してしまう。

※このような状況になってしまった場合は、情報センターにご連絡ください。

● キャリア回線が圏外の場所や、日本国外で使用するときは、

- SMSや電話認証は、圏外、日本国外では受信できない場合があります。
- Wi-Fi接続が可能な場合は、アプリ（Microsoft Authenticator）を使用してください。
- 予め、アプリを登録しておくことをおすすめします。

7 その他

7-1 登録 / 登録解除

- 情報センター オンラインガイドを参照してください。
[Meiji Gakuin University \(mguolg.info\)](https://mguolg.info) セキュリティ情報 > 多要素認証

7-2 よくある質問

● Microsoft公式サイト

[職場または学校アカウントの2段階認証に関する一般的な問題 - Microsoft サポート](#)
[Microsoft Authenticator アプリの使い方 - Microsoft サポート](#)
[Microsoft 認証アプリをダウンロードしてインストールする - Microsoft サポート](#)

● スマホから、セキュリティサイトにアクセスする方法は？

右のQRコードのサイトから、アクセスしてください。
(<https://mysignins.microsoft.com/security-info>)



● その他

- 情報センター オンラインガイドを参照してください。
[Meiji Gakuin University \(mguolg.info\)](https://mguolg.info) セキュリティ情報 > 多要素認証 > FAQ

7-3 問い合わせ

- ご不明な点は、情報センター（白金）までお問合せ下さい。