

多要素認証の設定

【パソコンを用いた設定方法】

多要素認証の設定手順について記載しています。



改版 2026.07.17

CONTENTS

多要素認証とは、パスワード入力に加えて、本人しかできない追加の認証を設定することで、本人以外のなりすましを防止する方法です。アカウントが盗み取られると、本学サービスに外部侵入を許し、学内外に重大な損害を及ぼします。このような危険を未然に防ぐ方法として、多要素認証を導入します。

設定は、①QRコード ②SMSの2通りありますが、必ず**どちらも**設定してください。

👉 片方の手段が使えない場合に代替手段としてもう一方の手段を使用するためです。

● 設定方法

① Authenticator の設定	P. 2
② SMS の設定	P. 6
③ 利用（多要素認証によるサインイン方法）	P. 8

● Q&A

2 台目のスマートフォンにも Microsoft Authenticator を登録できますか？	P. 9
スマートフォンを機種変更するときの設定を知りたいです。 ※ 下記に注意してください。	P. 9
電話番号が変更になりました。何か設定は必要ですか？	P. 9-10

⚠ 機種変更する際の注意

必ず**機種変更前のスマートフォンが手元にある状態**で、新しいスマートフォンを認証設定してください。

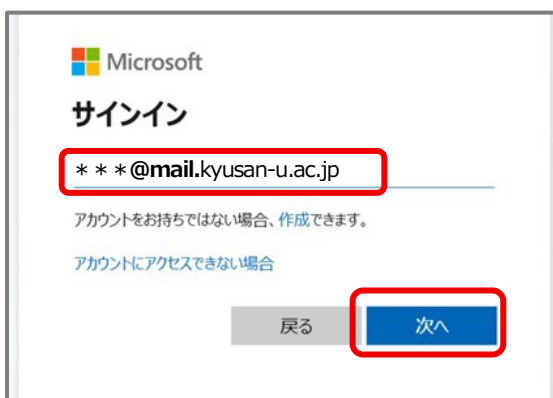
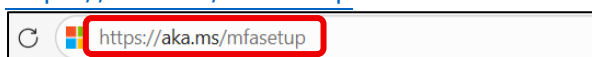


① Authenticator の設定

👉 設定に入る前に**使用中のパソコン、スマートフォンの Microsoft365 アプリ (OneDrive、Teams、Outlook、Word、Excel 等)** は必ず**全て閉じてください**。

パソコンで以下のサイトへアクセスします。

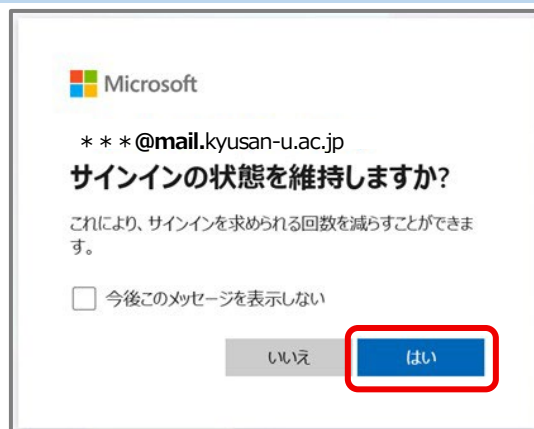
<https://aka.ms/mfasetup>



サインイン画面が表示されますので、
教職員：「ユーザ ID@mail.kyusan-u.ac.jp」
を入力し、「次へ」をクリックします。



パスワード欄へ「Microsoft365 パスワード」
(K'sLife 等を利用する時のパスワードと同じ)
を入力し、「サインイン」をクリックします。



「はい」をクリックします。



セキュリティ情報のページが表示されます。
「サインイン方法の追加」をクリックします。



「サインイン方法の追加」の項目から
「Microsoft Authenticator」をクリックします。

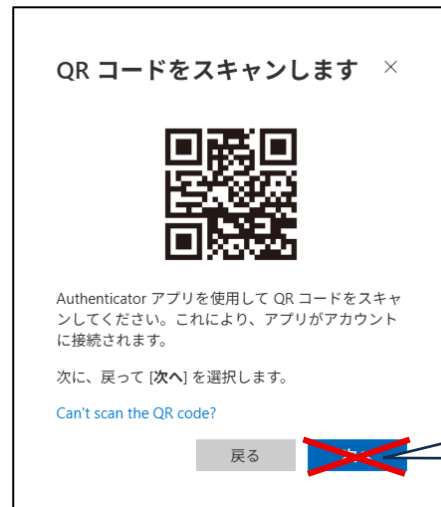
👉 **指定の認証方式以外は選択しないでください！**



「Microsoft Authenticator」のインストール画面が表示されますので、「次へ」をクリックします。



「次へ」をクリックします。



この画面を表示したままにして、パソコンでの操作を止めてください。
まだ何もクリックしないでください。



以降、スマートフォンでの操作になります。
次ページへ進んでください。

ここからスマートフォンでの操作です。(青色ページ)

アンドロイド



iphone



スマートフォンで上記 QR コードを読み込み、「Microsoft Authenticator」をインストールします。
 インストール済みの方は次へ進んでください。

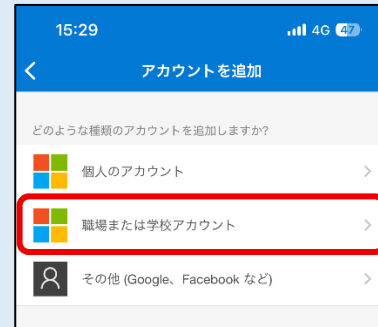


Microsoft Authenticator アプリを起動します。

初めてアプリを起動する方は、上記の画面が表示される場合があります。
 右上の「スキップ」⇒「続行」まで進めてからアプリを閉じてください。



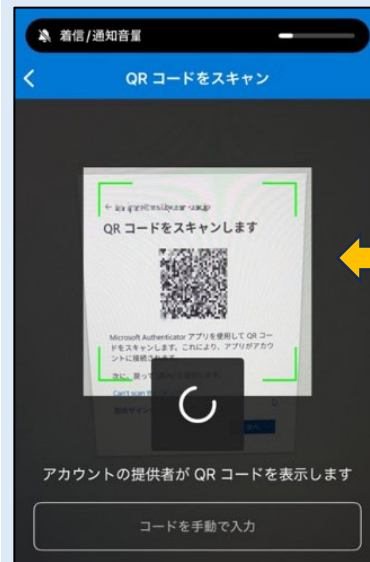
Microsoft Authenticator アプリ画面右上の「+」をタップします。



「職場または学校アカウント」をタップします。



「QR コードをスキャン」をタップします



パソコン画面の QR コード



カメラが起動したら、先ほどパソコンに表示されていた QR コードを読み取ります。



アカウントが追加されます。

ここからは、パソコンでの操作になります。

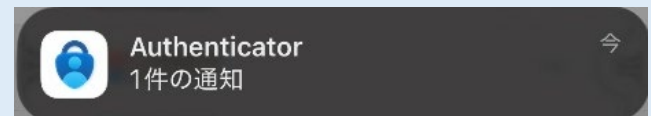


上記パソコン画面の「次へ」をクリックします。
(読取後、自動的に下記の画面に変わる場合あり)



パソコンの画面に認証コード(2桁数字)が表示され、同時にスマートフォンへ通知が届きます。

ここからスマートフォンでの操作です。(青色ページ)



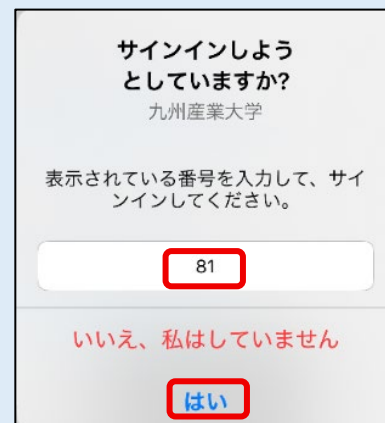
スマートフォンに届いた通知を開きます。

👉 通知が届かない場合は、スマートフォンの設定で

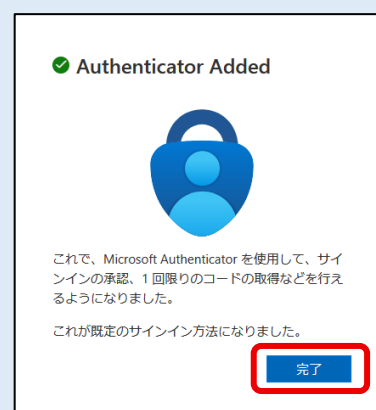
Microsoft Authenticator アプリの通知が「ON」

になっているかご確認ください。

👉 スマートフォンに**パスワード**や**生体認証**を設定している場合は、途中でロック解除を求められます。
その場合はロックを解除して次へ進んでください。



パソコン画面に表示された認証コード(2桁数字)をスマートフォンに入力し、「はい」をタップします。



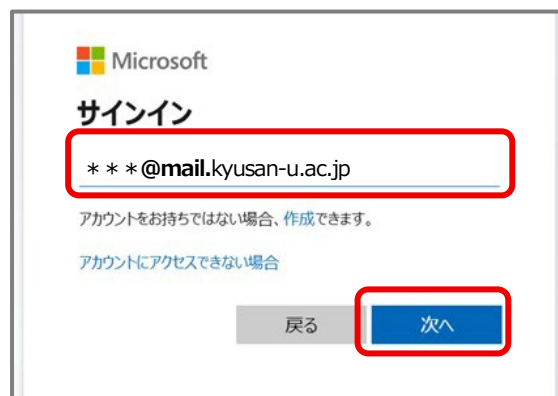
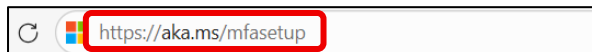
上記の登録完了画面が表示されますので、「完了」をタップして設定は完了です。

以上で① Authenticator の設定は完了です。
次ページ「②SMS の設定」へ進んでください。

② SMS の設定

パソコンで以下のサイトへアクセスします。

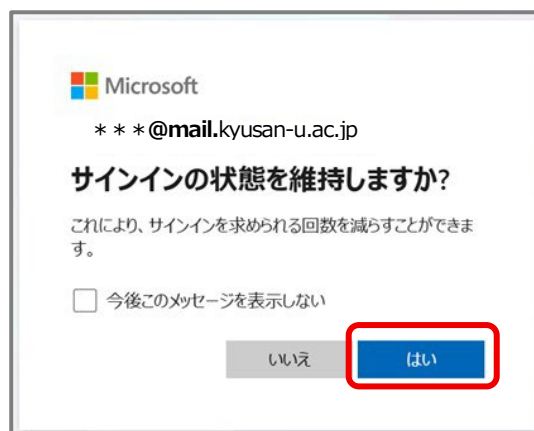
https://aka.ms/mfasetup



サインイン画面が表示されますので、
教職員：「ユーザ ID@mail.kyusan-u.ac.jp」
を入力し、「次へ」をクリックします。



パスワード欄へ「Microsoft365 パスワード」
(K'sLife 等を利用する時のパスワードと同じ)
を入力し、「サインイン」をクリックします。



「はい」をクリックします。



セキュリティ情報のページが表示されます。
「サインイン方法の追加」をクリックします。



「サインイン方法の追加」の項目から
「電話」をクリックします。

👉 指定の認証方式以外は選択しないでください！

電話番号の追加

電話にテキスト コードを送信して本人確認を行います。

国番号
日本 (+81)

プルダウンメニューで
日本 (+81) を選択

Phone number
090 * * * * *

0 ゼロから入力

確認方法を選択します
☒ コードの SMS 送信

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]を押すと、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。

戻る 次へ

以下の通り、選択及び入力を行います。

- ・国番号：プルダウンメニューで**日本 (+81)**を選択
- ・Phone number：**スマートフォンの電話番号**
- ・確認方法：**コードのSMS送信**

☞ 誤って日本 (+81) 以外の選択をした場合、通知先への通信費を請求される場合があります。

「次へ」をクリックします。



入力した電話番号のスマートフォンにポップ通知が表示されますのでタップします。

☞ 機種により画面や表示方法が異なる場合があります。

Microsoft 認証に確認コード ***** を使用します。

届いたメッセージに **6桁の番号**が確認できます。
この番号を下記の「電話番号の確認」へ入力します。

電話番号の確認

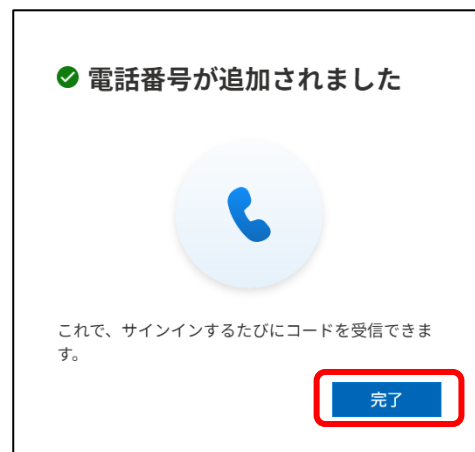
+81090 * * * にお送りしたコードを入力してください。

6桁の番号を入力

コードが届きませんか?

次へ

「次へ」をクリックします。



「完了」をクリックします。

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: Microsoft Authenticator - 通知 変更

+ サインイン方法の追加

電話 +81090 * * *

電話 入ってる

パスワード 最終更新日時: 1年前

Microsoft Authenticator 多要素認証 (MFA) をプッシュする iPhone

Microsoft Authenticator 入ってる

「セキュリティ情報」の画面で

- ・電話
- ・Microsoft Authenticator

の登録が確認できれば、全ての設定は完了です。
お疲れさまでした。

③ 利用（多要素認証によるサインイン方法）

自宅や公共の無線 LAN（Wi-Fi）や携帯電話回線など学外ネットワークから、多要素認証が必要なサービスにアクセスすると、ID・パスワードを入力した後に、多要素認証を要求されます。

Microsoft Authenticator による認証

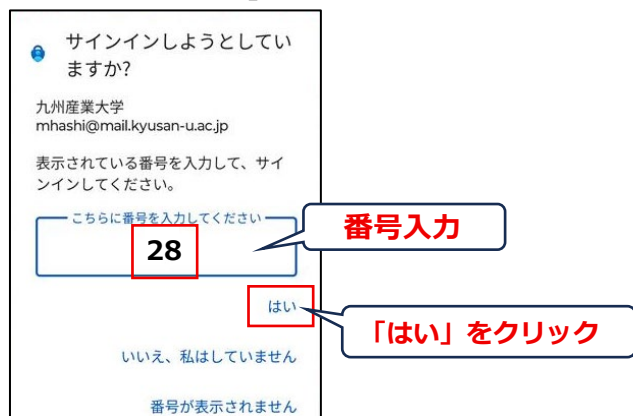
① 認証画面でメールアドレスとパスワード入力後、多要素認証を求められます。

<パソコンの画面>



<スマートフォンの画面>

② 多要素認証の設定で利用したスマートフォンに通知が来るので、①で表示される数字（例は 28）を入力して「はい」をタップします。



◆正しい番号が入力されると認証完了

SMS による認証

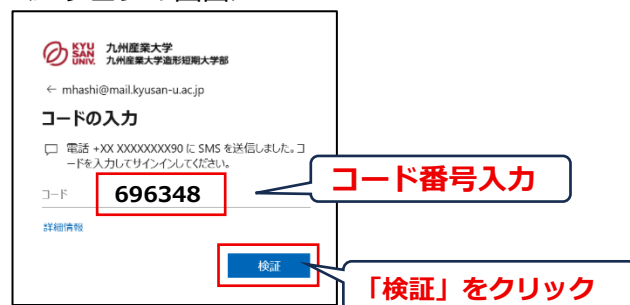
① 認証画面でメールアドレスとパスワード入力後、「サインイン要求を承認」画面が表示されたら、「アプリを使用できません」をクリック。

<パソコンの画面>



② スマートフォン（携帯電話）に送信された 6 桁のコード番号を入力し、検証をクリック。

<パソコンの画面>



◆正しい番号が入力されると認証完了

Q1：2 台目のスマートフォンにも Microsoft Authenticator を登録できますか。

A：はい、登録できます。

次の順序で設定してください。

1. 1 台目のスマートフォン（認証登録済み）を用意します。
以下、設定中に認証を求められた場合は、このスマートフォンで認証してください。



2. 2 台目のスマートフォンにて、P.2～P.5 を参考に、Microsoft Authenticator のインストール及び認証設定をしてください。
※P.6『②SMS の設定』は不要です。



👉 複数のスマートフォンに認証設定しておくことで機種不具合等による接続トラブルを未然に防げます。

Q2：スマートフォンを機種変更するときの設定を教えてください。

A：次の順序で設定してください。

👉 認証手段として **機種変更前のスマートフォンが必要**です。手段を失うと、復旧に管理者による対応が必要となります。【休業中は対応致しかねます】

1. 機種変更前のスマートフォンを用意し、WiFi でインターネットに接続しておきます。
以下、設定中に認証を求められた場合は、このスマートフォンで認証してください。



2. 新しいスマートフォンを用意し、通話及びインターネットに接続できる状態にします。



3. 新しいスマートフォンにて、P.2～P.5 を参考に、Microsoft Authenticator のインストール及び認証設定をしてください。
※P.6『②SMS の設定』は不要です。

👉 電話番号に変更がある場合は、一旦すべてのアプリを閉じて、引き続き **Q3** の操作を行ってください。

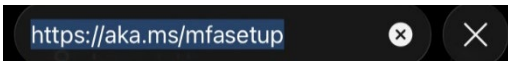
Q3：電話番号を変更しました。設定は必要ですか？

A：SMS 認証で登録した電話番号を変更する

必要があります。次の順序で設定してください。

1. スマートフォンから以下へアクセスし「セキュリティ情報」へのサインインを進めます。

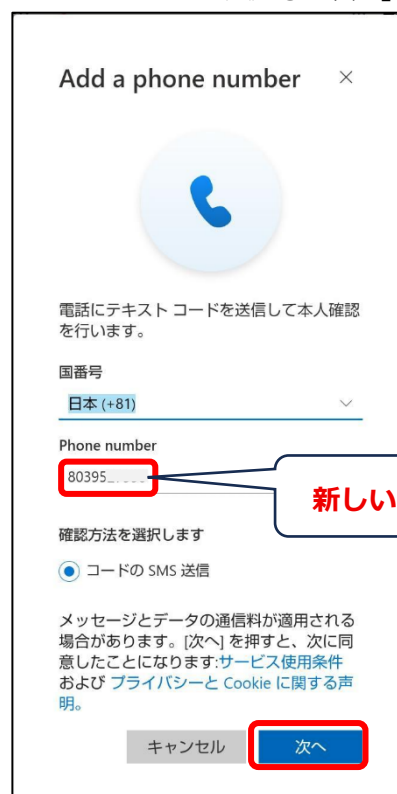
<https://aka.ms/mfasetup>



2. 下記の「セキュリティ情報」が表示された後、現在の電話番号の下「変更」をタップします。

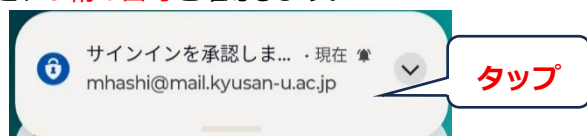


3. 下記の画面に変わったら、新しい電話番号を Phone number へ入力し「次へ」をタップします。



新しい電話番号を入力

- 4.ポップ通知が表示されますのでタップしてメッセージを開き、**6桁の番号**を確認します。



Microsoft 認証に確認コード **0330429** を使用します。

- この番号を下記の「電話番号の確認」へ入力し「次へ」をタップします。

電話番号の確認

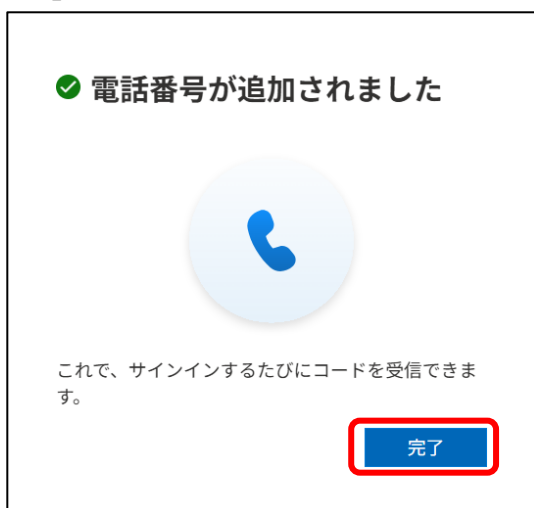
+81090*** にお送りしたコードを入力してください。

6桁の番号を入力

コードが届きませんか?

次へ

5. 「完了」をタップします。



以上で新しい電話番号の登録は完了です。