Using Gifu University Microsoft 365 outside the University:

Multi-factor Authentication User's Manual

Released August 2020

Created by Information & Communications

Table of Contents

1. Overview of Multi-factor Authentication for Using Gifu University Microsoft 365 Outside the University

Gifu University allows for various apps to be accessed using a single user ID and password, using a service called Microsoft 365 (formerly Office 365) to which the University subscribes. Each app provided by the service can be accessed simply by entering a user ID and password (signing in) once.

Although this is convenient for users, if a user's user ID and password ("account" hereafter) are stolen, it can provide an attacker with external access to Gifu University services and could result in serious damage both inside and outside the university. In recent years, an increasing number of organizations are implementing multi-factor authentication to prevent this from occurring.

Compared with conventional authentication where a user merely enters a user ID and password, multi-factor authentication is a scheme that more strongly ensures the authenticity of connections or operations made by the user or registered device that is attempting to authenticate (i.e., logging into a system or confirming some operation), by making use of a one-time password (*1), biometric authentication (*2), or a dedicated authentication device (*3).

This manual describes what needs to be done to use multi-factor authentication when accessing Gifu University Microsoft 365 apps from outside the University, as well as how to use this form of authentication.

* Multi-factor authentication is not required when using Microsoft 365 while connected to the internal university network.

*1 One-time password: A password that is valid only for a certain period of time, or for a certain number of logins

*2 Biometric authentication: A method of authentication that uses information from the body, such as the user's fingerprint or face

*3 Dedicated authentication device: Some examples include inserting a USB dongle into a PC or other system, or scanning an authentication card with a card reader

◆ Who this applies to:

Those who have been issued an individual account from Gifu University and who use Microsoft 365

◆ Devices that can be registered for use (one device and one phone number):

Smartphones, etc. purchased using public or personal funds

* Devices should always be carried with the user when on a business trip or other excursion.

* Explanations in this manual mainly assume the use of a smartphone

◆ Contact information:

Information Management Core 1F

Email: imc-help@gifu-u.ac.jp

Tel: +81-58-293-2041 (Extension 2041)

Flowchart: Multi-factor Authentication for Microsoft 365 (University Edition)

*** Use of Non-University Edition of Microsoft 365 should be handled on your own.**

If you have an older style mobile phone, you do not need to download the app

Download the authentication app to the authentication device (your smartphone)

iPhone app　　Android app

* It is recommended to install the app in case the device is lost, etc.

Register and configure the authentication device
(After applying the system, first sign in with an off-campus connection)

Access Microsoft 365 (formerly Office 365) while connected from outside the University, specify the authentication method, configure information, and then make sure to confirm operation
Select one of the following four methods (① and ② are recommended for older style mobile phones, while ③ and ④ are recommended for smartphones)

① Authentication using mobile phone (voice)	② Authentication using mobile phone (text message)	③ Authentication using authentication app (approval notification)	④ Authentication using authentication app (confirmation code)

Use multi-factor authentication when signing in to use Microsoft 365 while connected from outside the University (not required for use when connected on university grounds)

① Authentication using mobile phone (voice)	② Authentication using mobile phone (text message)	③ Authentication using authentication app (approval notification)	④ Authentication using authentication app (confirmation code)

* The authentication method can be changed if required

Begin using Microsoft 365 apps

2. PREPARING FOR USE (INSTALLING THE APP ONTO THE AUTHENTICATION DEVICE)

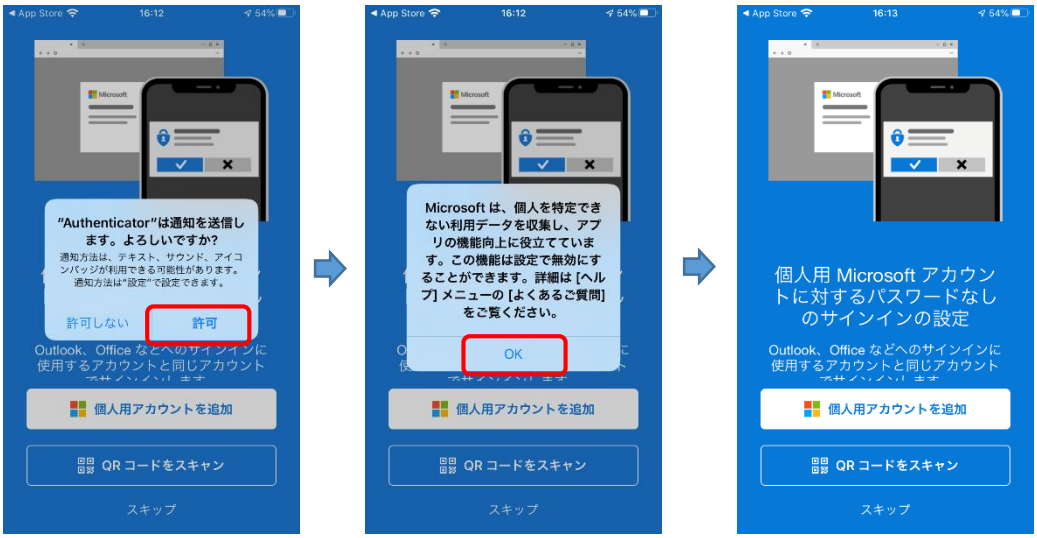
(1) iOS DEVICES (EXPLAINED HERE USING AN iPhone)

① Search for the following app in the App Store and then install it.

"Microsoft Authenticator" (a free app provided by Microsoft)

② After install the app, you have to confirm the following the first time you launched it.

Tap "Allow" for "Send notifications (display notifications on smartphone)" and then tap "OK" for "Privacy (gathering information that cannot be used to identify an individual)."



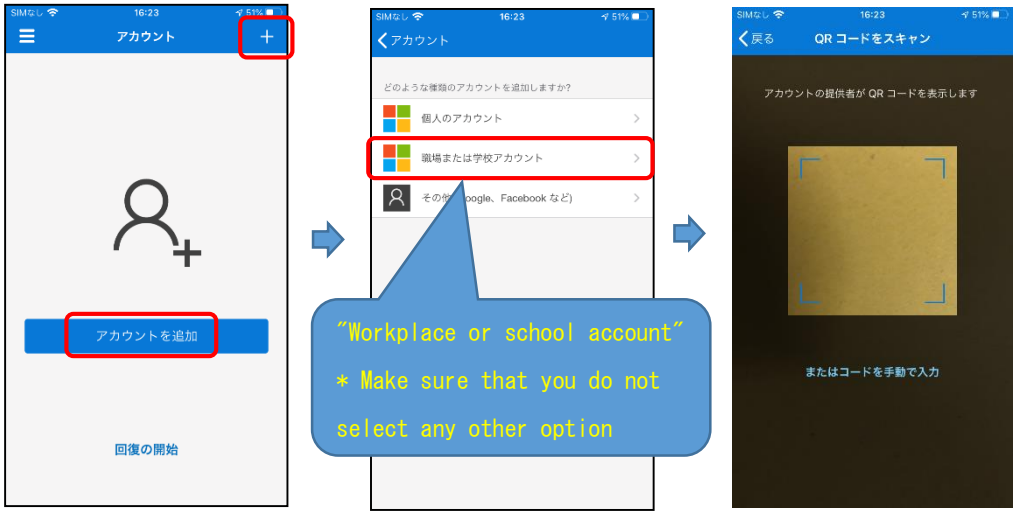
③ Tap "Scan QR code" to start the QR code camera. If the QR code scanning camera screen appears, proceed to **3. Register and Configure the Authentication Device (First Time Only)**.

* If you are asked to provide "access to the camera" during the initial scan, select "OK" and proceed to ④. You may close the app if required.


App Store
16:13
54%
アカウント
"Authenticator"がカメラへのアクセスを求めています
新しいアカウントに追加するには、QR コードをスキャンする必要があるかもしれません
許可しない
OK
アカウントを追加
回復の開始
App Store
16:13
53%
戻る
QR コードをスキャン
アカウントの提供者が QR コードを表示します
または手動でサインイン

④ If you close and relaunch the app, the order in which the screens are displayed may differ from when the account was configured. Select the screens in the following order to display the QR code camera screen.

＊ "Add account" (tap "+" on the upper right to add if already configured) → "Workplace or school account" → Camera screen

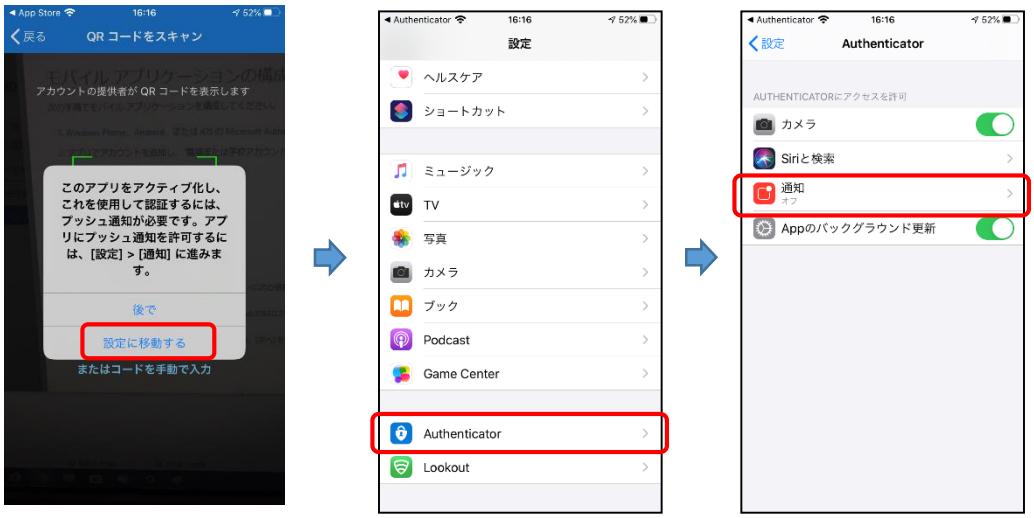


Based on iOS settings, a function called "App lock" may be enabled when launching the app. This applies even stricter restrictions on app usage, by requiring the user to authenticate using a fingerprint or facial authentication, or by entering a passcode.

Note that app lock settings, turned OFF in the app settings. However, it is not recommended.

⑤ If a message regarding "Activating this app..." appears, follow the procedure below.

1) Go to Settings → Authenticator → Notifications



2) Change "Allow notifications" from OFF (gray) to → ON (green)

* Although several items will be displayed, there is no need to change them.

(2) FOR Android DEVICES (DESCRIBED HERE USING A SMARTPHONE)

① Search for the following app in the Google Play Store and then install it.

"Microsoft Authenticator" (a free app provided by Microsoft)

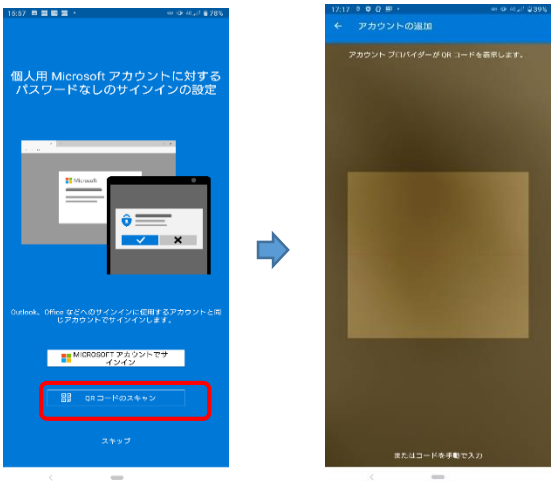
② After installing the app, you have to confirm the following the first time, you launched it.

Tap "Allow" for "Send notifications (display notifications on smartphone)" and then tap "OK" for "Privacy (gathering information that cannot be used to identify an individual)."

③ Tap "Scan QR code" to start the QR code camera. If the QR code scanning camera screen appears, proceed to **3. Register and Configure the Authentication Device (First Time Only)**.

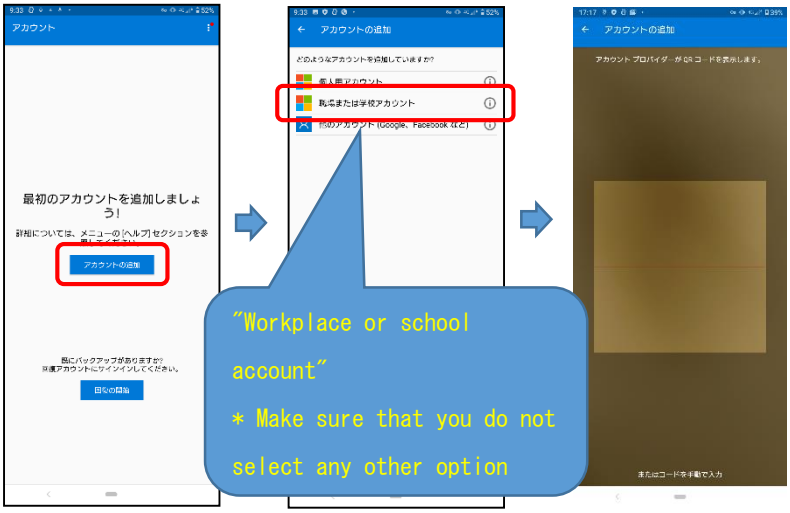
* If you are asked to provide "Permission to take photos and videos (access to camera)" during the initial scan, select "OK."

* You may close the app if required. However, you will need to follow the procedure described in ④ ("Add account" → Workplace or school account" → Camera screen).



④ If you close and relaunch the app, the order in which the screens are displayed may differ from when the account was configured. Select the screens in the following order to display the QR code camera screen.

＊ "Add account" → "Workplace or school account" → Camera screen

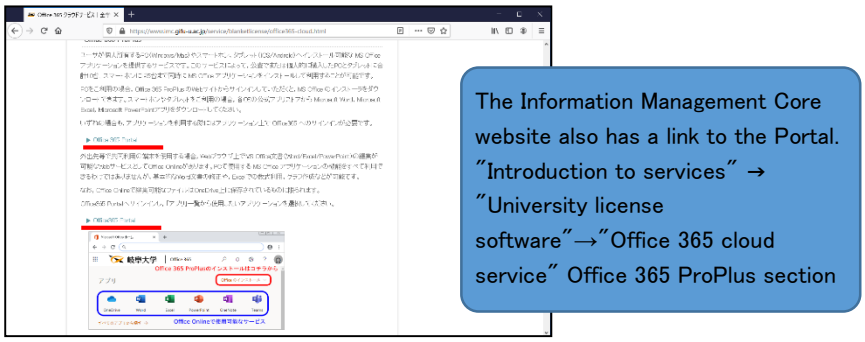


3. REGISTER AND CONFIGURE THE AUTHENTICATION DEVICE (FIRST TIME ONLY)

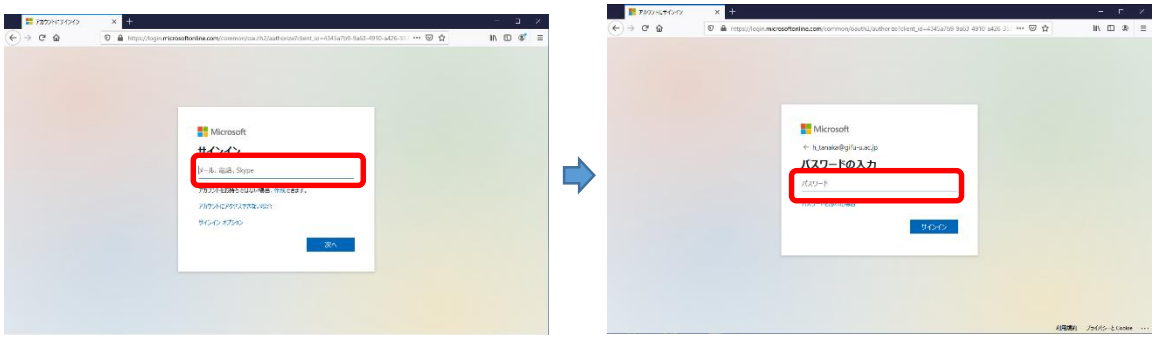
(1) FOR ALL DEVICES

① Connect to the Microsoft 365 Portal (https://portal.office.com) while connected from outside the University. The procedure may not be as described here if connected to the internal Gifu University network.

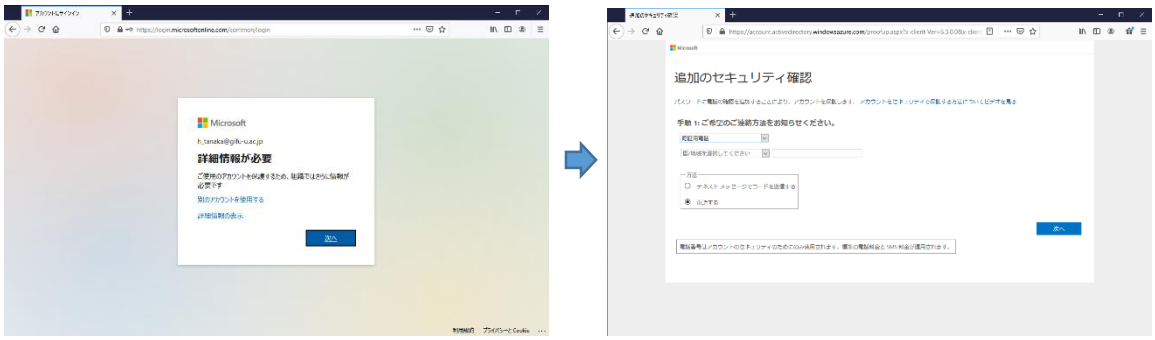
＊ Registering an authentication device is extremely important, so please make sure to do this from a trusted PC.



② Your sign-in information will be confirmed. Enter your personal email address and password.



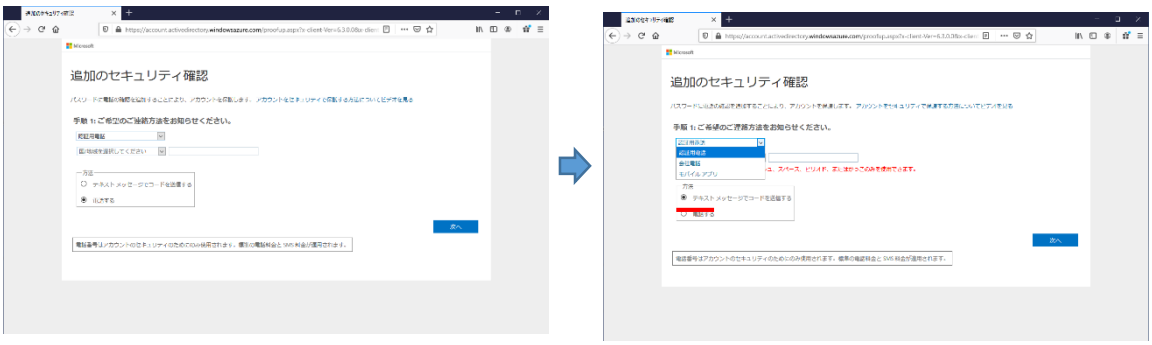
③ You will be asked to configure your detailed information. Click "Next" to proceed to the "Confirm additional security information" screen.

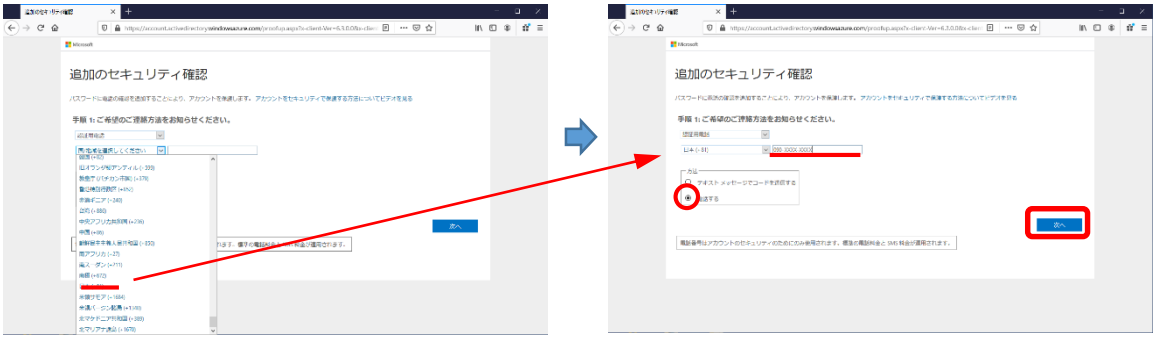


Four methods will be explained here. If you are using a smartphone, it is recommended to use one of the app methods ((4) or (5)). If you are using an older style mobile phone, it is recommended to use one of the phone methods ((2) or (3)). After you finish configuring the settings, please be sure to confirm the operation.

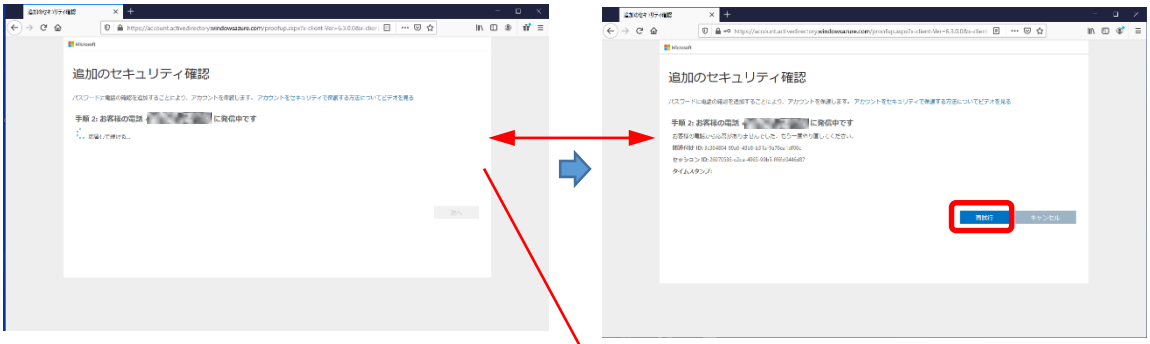
(2) ADDITIONAL SECURITY SETTINGS (AUTHENTICATION USING PHONE [VOICE])

Select "Authentication phone" as the authentication device. Do not select "Company phone" (doing so is prohibited).





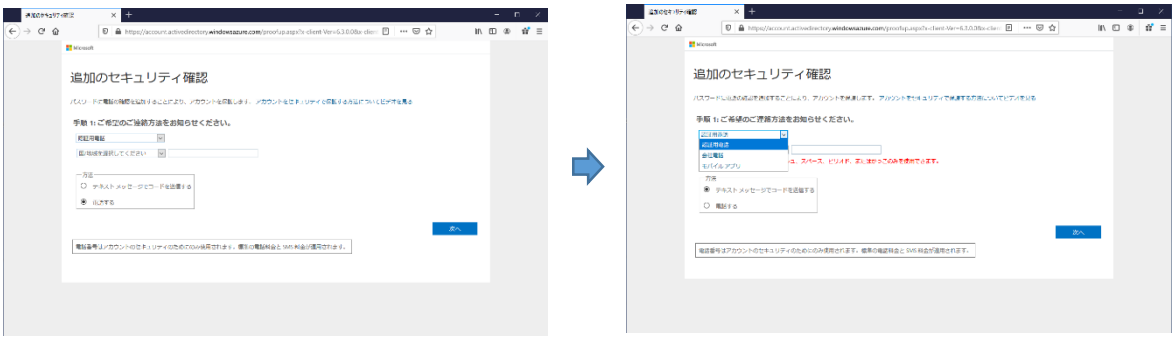
Here, you have to enter "Country/region" and the authentication mobile phone number and "Call" for "Method". Then, click "Next."



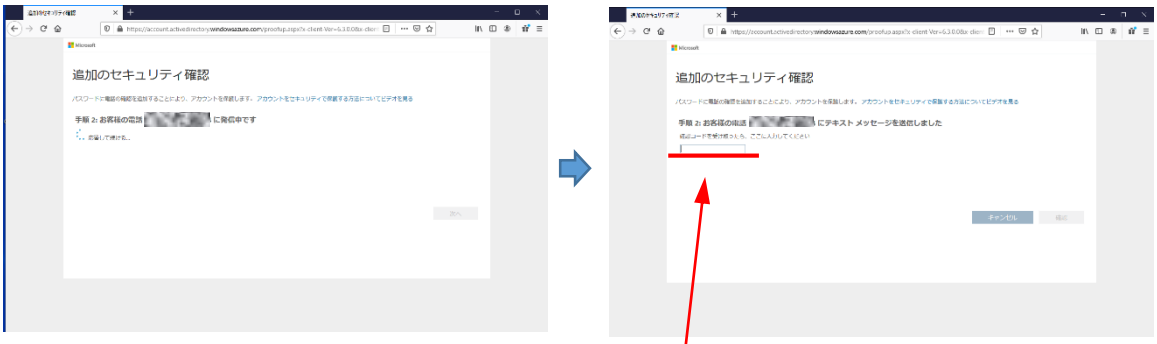
1. Click "Next" to receive a call.
2. When you answer the call, a voice will ask you to "press # to confirm." Press # on your phone.
3. If you could not respond or press # within the allotted time, a message asking you to "please try again" will be displayed on the PC screen. Click "Retry" to try again.
4. If successful, a message stating "confirmed successfully" will be displayed on the PC screen. Click "Finish" to complete the process.

(3) ADDITIONAL SECURITY SETTINGS (AUTHENTICATION USING PHONE [TEXT MESSAGE])

Select "Authentication phone" as the authentication device.



Here, you have to enter "Country/region" and the authentication mobile phone number and "Send code by text message" for "Method". Then, click "Next."

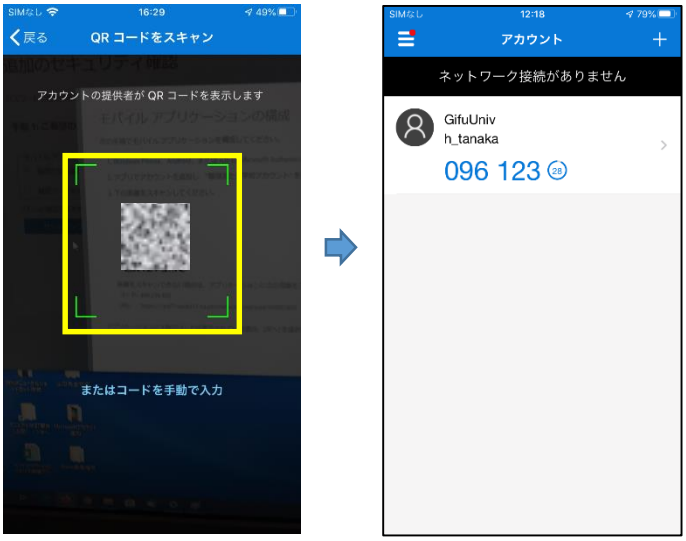


1. Click "Next" to receive an SMS message on your phone.
2. The PC screen will display a message asking you to "enter the confirmation code you received." Enter the code included in the SMS message and then click "Confirm."
3. If you do not enter the code within the allotted time, a message asking you to "please try again" will be displayed on the PC screen. Click "Retry" to try again.
4. If successful, a message stating "confirmed successfully" will be displayed on the PC screen. Click "Finish" to complete the process.

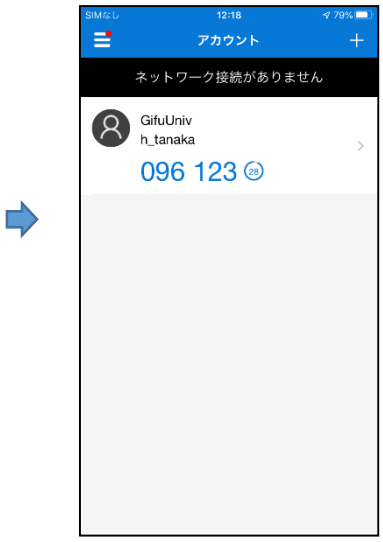
(4) ADDITIONAL SECURITY SETTINGS (AUTHENTICATION USING MOBILE APP [RECEIVE NOTIFICATION])

① Select "Mobile app" for the authentication device and "Receive notification for confirmation" for the mobile app usage method. Click "Setup" to display a QR code.

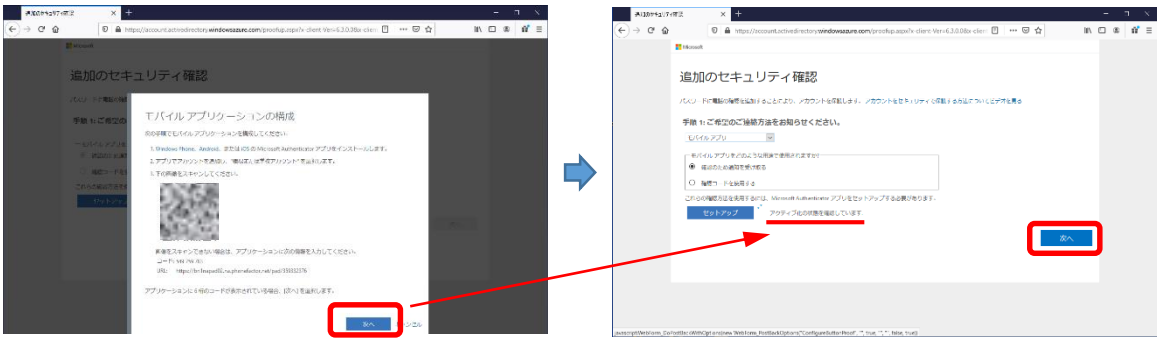
② Scan the QR code using the device on which you installed the app.
(This procedure is the same for both iOS and Android.)



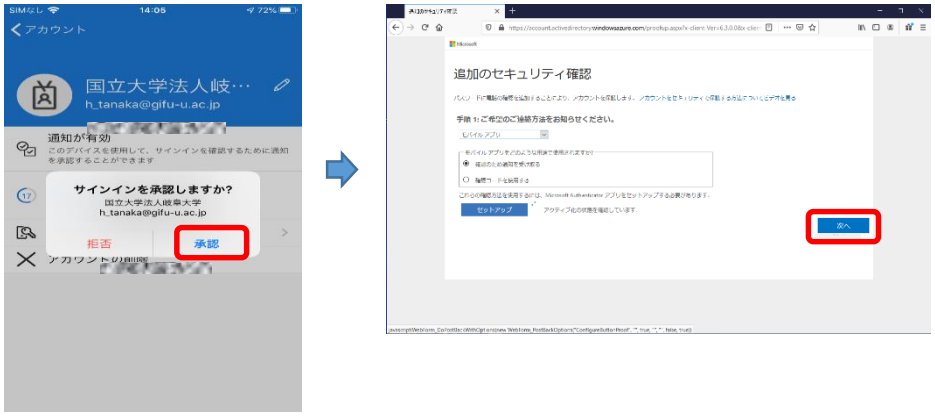
③ If the scanning fails, tap "Or manually enter a code" and enter the code and URL shown on the PC screen.



④ When the one-time password is displayed on the registered device, click "Next" on the PC. Although it may take several minutes, the following messages will be displayed in order on the screen: "Confirming activation status" → "Mobile app configured for notifications and confirmation codes." Click "Next."



⑤ Once a message stating "now contacting your mobile application device" appears on the PC, a message asking "approve sign-in?" will be displayed on the device. Tap "Approve." Once a message stating "confirmation successful" is displayed on the PC, registration has been successfully completed. Click "Next" to continue.

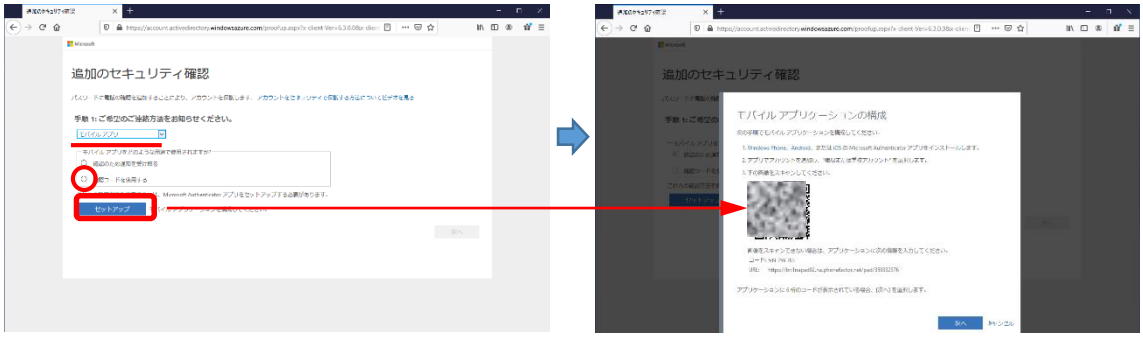


⑥ The "What to do if the mobile app could not be accessed" screen is displayed on the PC. Set the "Country/region" and the authentication mobile phone number and then click "Next." If the "Continue to use existing application" screen appears, click "Finish" to stop configuring the settings. You may be taken to the Microsoft 365 sign-in page after this.

＊ Although the app may be registered with multiple devices, only a single authentication method may be used.

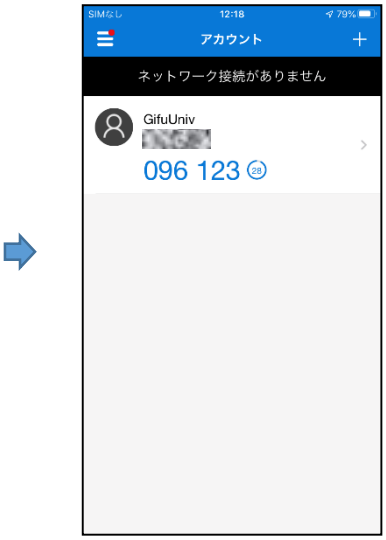
(5) ADDITIONAL SECURITY SETTINGS (AUTHENTICATION USING MOBILE APP [USE CONFIRMATION CODE])

① Select "Mobile app" for the authentication device and "Use a confirmation code" for the mobile app usage method. Click "Setup" to display a QR code.

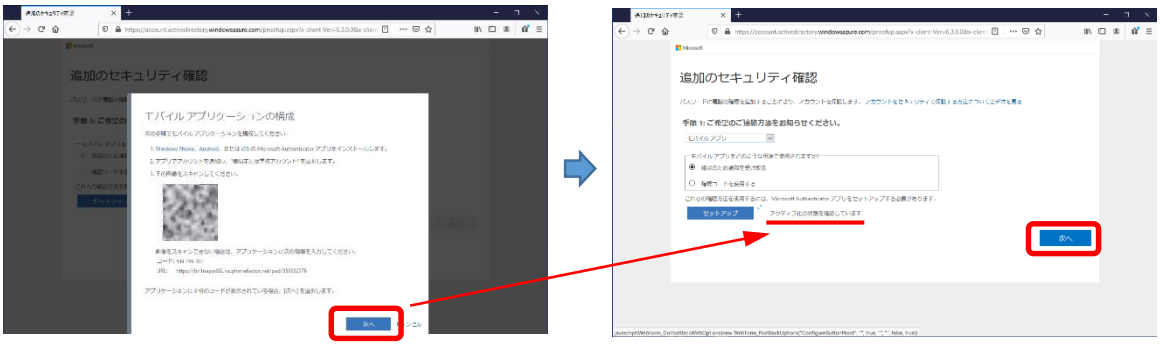


② Scan the QR code using the device on which you installed the app.
(The procedure is the same for both iOS and Android.)

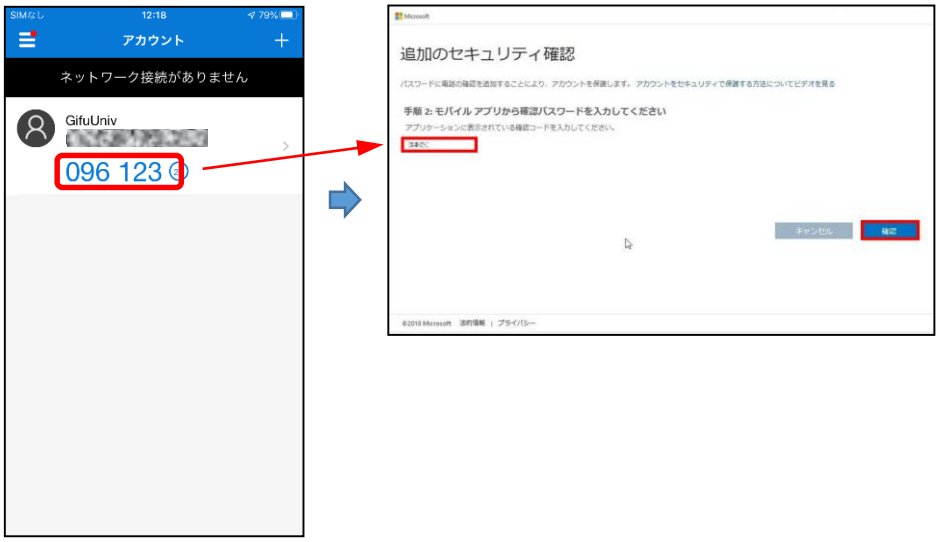
③ If scanning fails and you are unable to scan the code, tap "Or manually enter a code" and enter the code and URL shown on the PC screen.



④ When the one-time password is displayed on the registered device, click "Next" on the PC. Although it will take several minutes, the following messages will be displayed in order on the screen: "Confirming activation status" → "Mobile app configured for notifications and confirmation codes." Click "Next."



⑤ On the "Enter the confirmation password from the mobile app" screen on the PC, enter the code (six digits) displayed on the device, and then click "Confirm." Once a message stating "confirmation successful" is displayed on the PC, registration has been successfully completed. Click "Next" to continue.



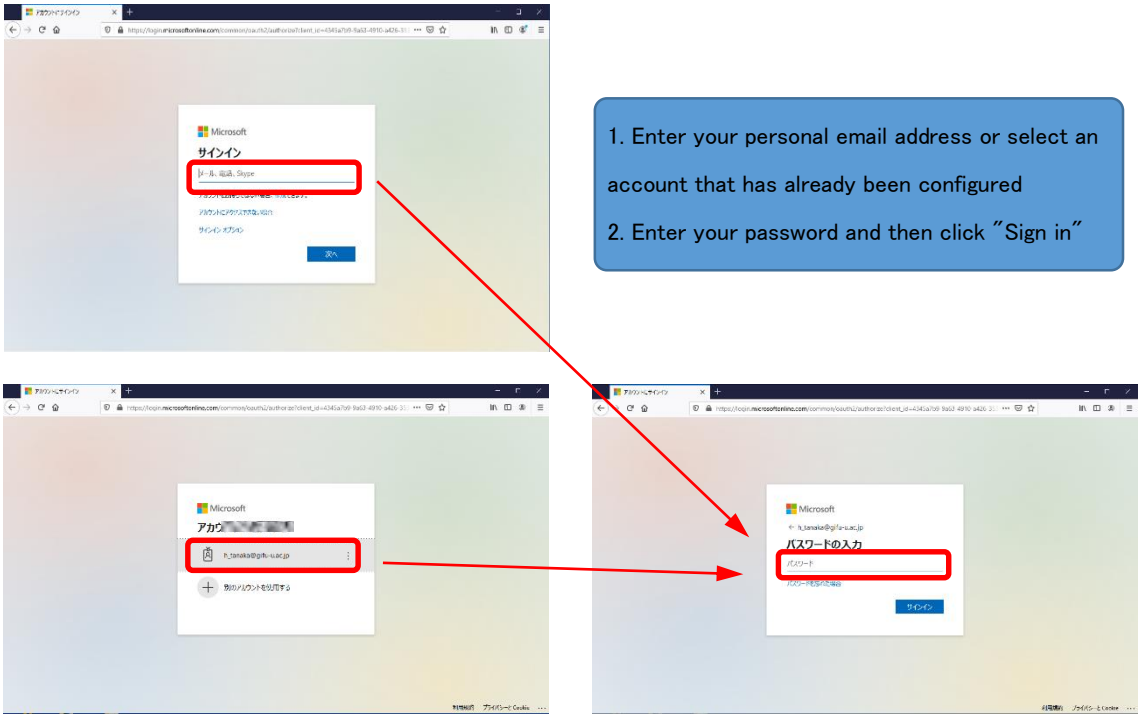
⑥ The "What to do if the mobile app could not be accessed" screen is displayed on the PC. Set the "Country/region" and the authentication mobile phone number and then click "Next." If the "Continue to use existing application" screen appears, click "Finish" to stop configuring the settings. You may be taken to the Microsoft 365 sign-in page after this.

* Although the app may be registered with multiple devices, only a single authentication method may be used.

4. SIGNING-ON AFTER INITIAL SIGN-ON (ACCESSING FROM OUTSIDE THE UNIVERSITY ONLY)

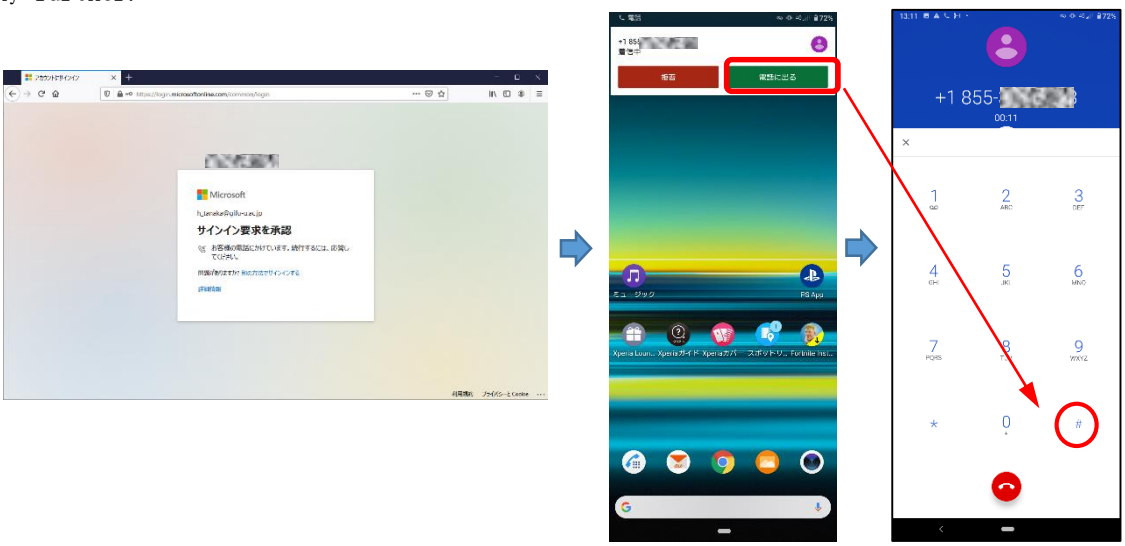
(1) IF AUTHENTICATION USING PHONE (VOICE) WAS CONFIGURED

① When you attempt to access Microsoft 365 you will be asked to sign in.



② A call will be made to the registered phone number. Answer the phone call and then press "#" when prompted to do so. If you cannot authenticate within the allotted time, another phone call will be made to the phone, or you will need to "Retry" on the PC.

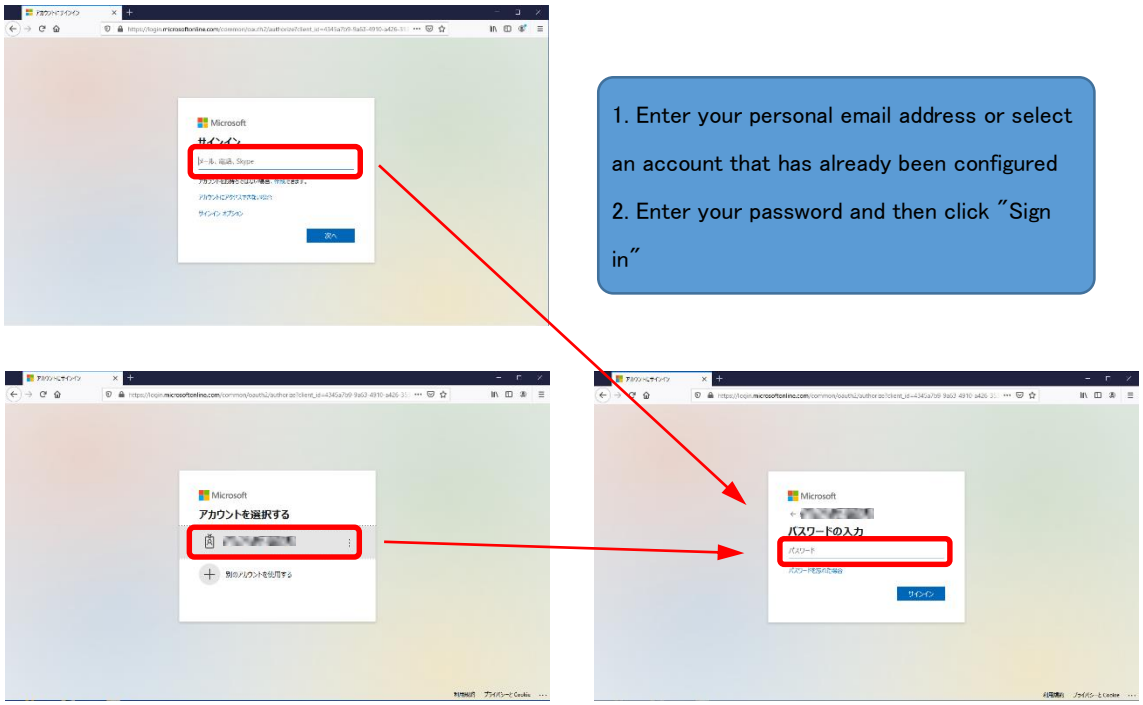
＊ If authentication succeeds, you will not need to operate the registered device any further.



③ After signing in successfully, you may be asked to confirm whether to stay signed in. Select to do so (if required) to proceed to the Microsoft 365 screen.

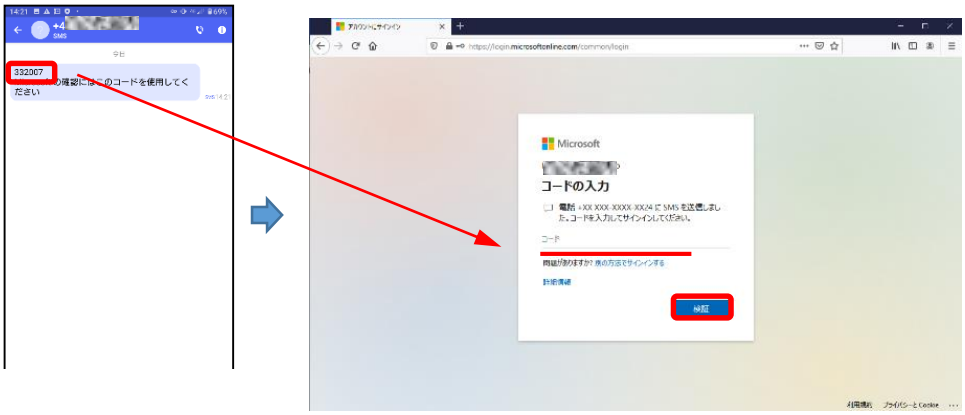
(2) IF AUTHENTICATION USING PHONE (TEXT MESSAGE) WAS CONFIGURED

① When you attempt to access Microsoft 365 you will be asked to sign in.



② A message (SMS) will be sent to the registered phone number. On the PC, enter the code included in the message and then click "Verify." If you cannot authenticate within the allotted time, you will need to click "Retry" on the PC.

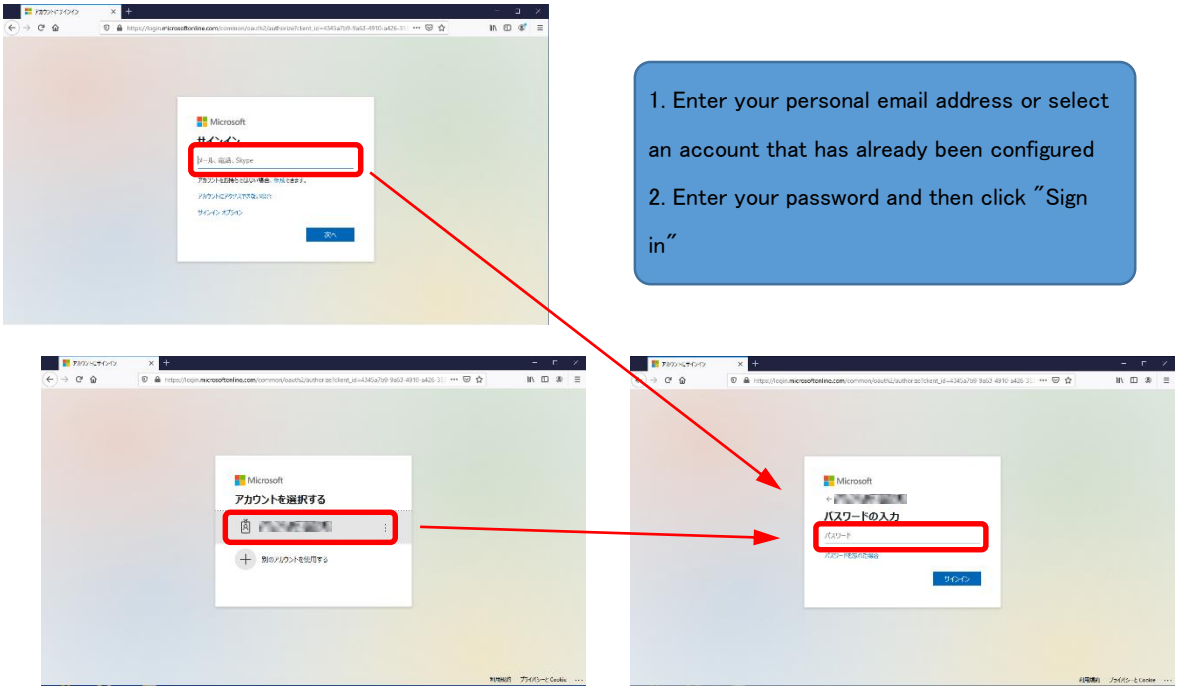
＊ If authentication succeeds, you will not need to operate the registered device any further.



③ After signing in successfully, you may be asked to confirm whether to stay signed in. Select to do so (if required) to proceed to the Microsoft 365 screen.

(3) IF AUTHENTICATION USING MOBILE APP (RECEIVE NOTIFICATION) WAS CONFIGURED

① When you attempt to access Microsoft 365 you will be asked to sign in.



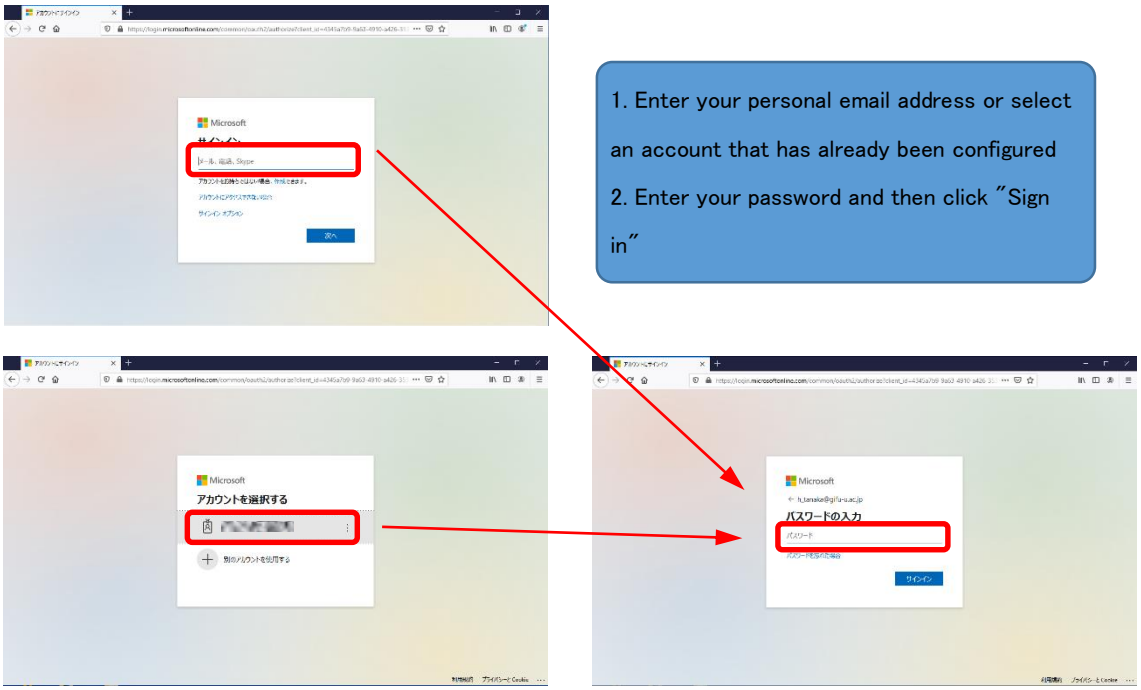
② A message asking you to "approve the sign-in request" will appear on the PC, and a sign-in approval notification will be received by the Microsoft Authenticator app on the registered device. Open the app and tap "Approve." If you cannot authenticate within the allotted time, you will need to click "Retry" on the PC.

* If authentication succeeds, you will not need to operate the registered device any further.

③ After signing in successfully, you may be asked to confirm whether to stay signed in. Select to do so (if required) to proceed to the Microsoft 365 screen.

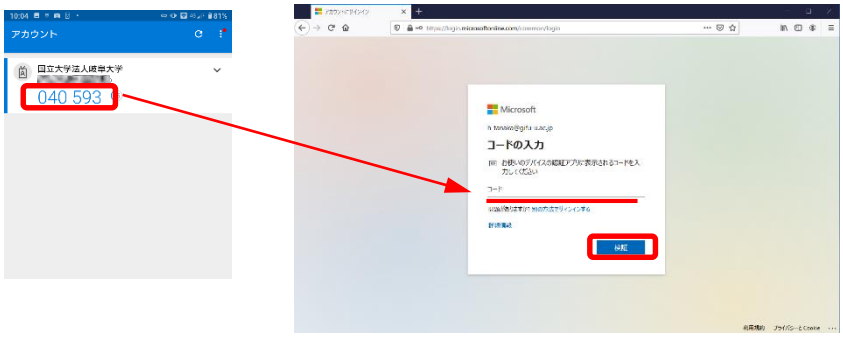
(4) IF AUTHENTICATION USING MOBILE APP (USE CONFIRMATION CODE) WAS CONFIGURED

① When you attempt to access Microsoft 365 you will be asked to sign in.



② A message asking you to "enter code" will be displayed on the PC. Verify the code shown in the Microsoft Authenticator app on the registered device, enter the code on the PC, and then click "Verify." If you cannot authenticate within the allotted time, you will need to click "Retry" on the PC.

* If authentication succeeds, you will not need to operate the registered device any further.

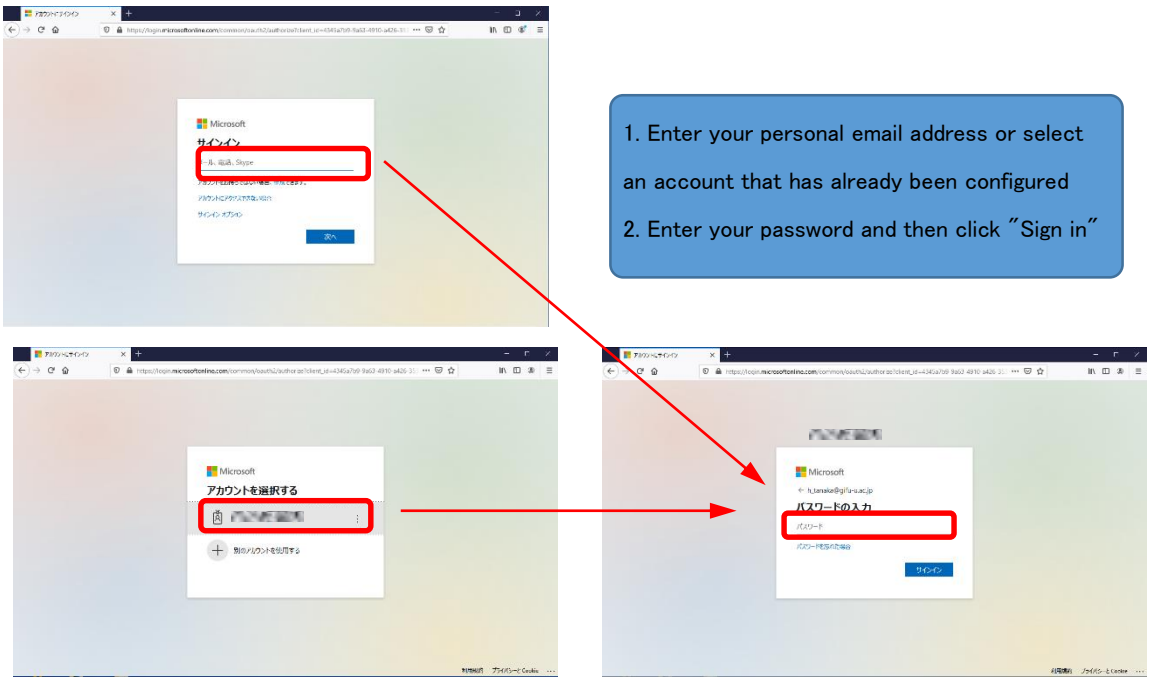


③ After signing in successfully, you may be asked to confirm whether to stay signed in. Select to do so (if required) to proceed to the Microsoft 365 screen.

5. CHANGING THE AUTHENTICATION METHOD

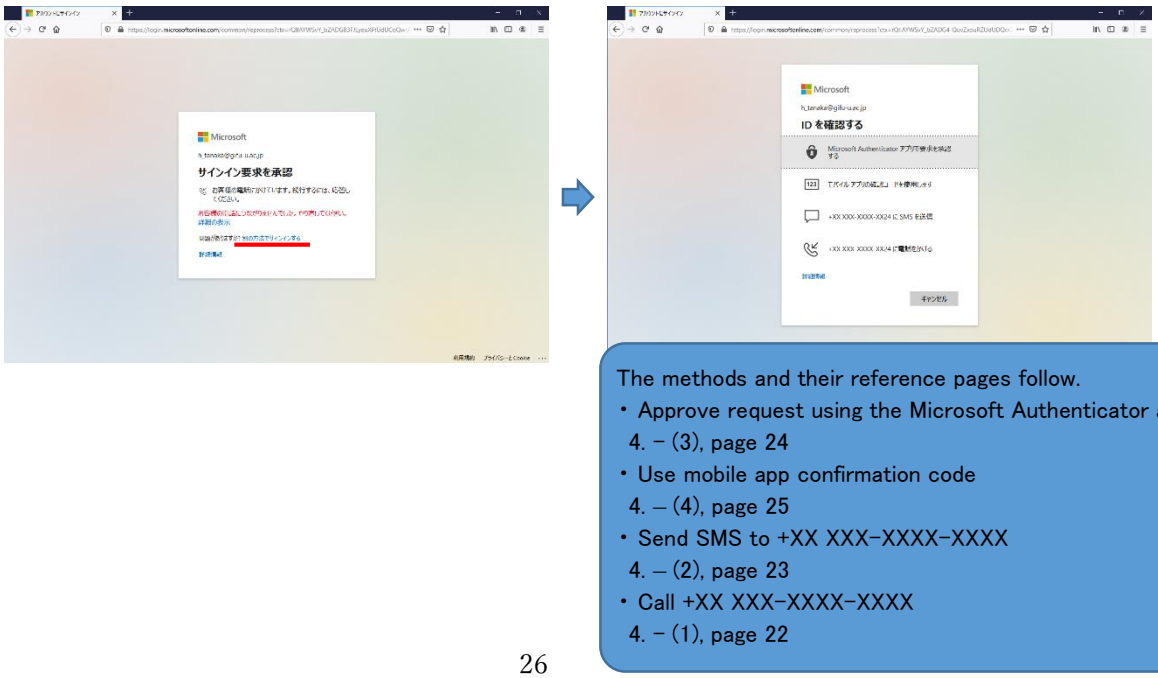
(1) CHANGING THE METHOD WITHOUT SIGNING IN USING THE CONFIGURED METHOD

① Enter your information up to the password for signing into Microsoft 365, but instead of signing in wait a short while.



② An error will be displayed. Click "Sign in using another method" to display methods you have configured. Select the method to use.

* If the checkbox next to a method is not checked on the following additional security screen, the method may not appear as an option.



(2) CHANGING TO A METHOD THAT HAS NOT BEEN CONFIGURED (SAME PROCEDURE FOR ALL DEVICES)

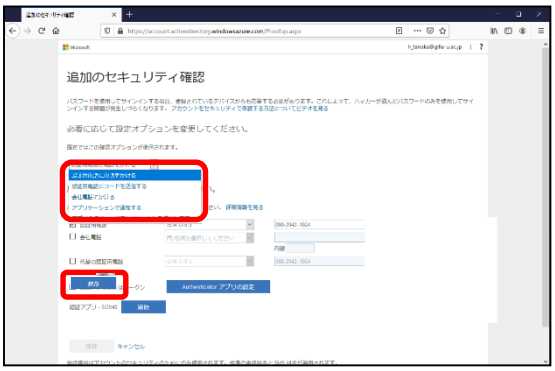
① Normally, this is done by reconfiguring the initial settings as described in sections 2 and 3.

The procedure to follow if this method does not work is described here.

② After signing into Microsoft 365, use the following URL to access the "Additional security confirmation" page.

https://account.activedirectory.windowsazure.com/Proofup.aspx

* This URL is subject to change without notice due to Microsoft specifications.



The settings are as follows.

・Default option: The currently configured method is displayed
Select the method to change
・Call authentication phone: Voice
・Send code to authentication phone: SMS
・Call work phone: Use prohibited
Notify with application: Approval request
・App confirmation code: Confirmation code in app

・Method to use for response (check only required items)
・Authentication phone: Select this for a phone (voice)
・Alternate authentication phone: Alternate authentication phone if primary authentication phone or app cannot be used
・Authentication app or token: Smartphone app

・Authentication app: Device name displayed if it has been registered
If you switch to a different device, "Delete" both the PC and previous device, and then re-register them in "Authenticator app settings"

(3) CHANGE METHOD TO CALLING THE AUTHENTICATION PHONE

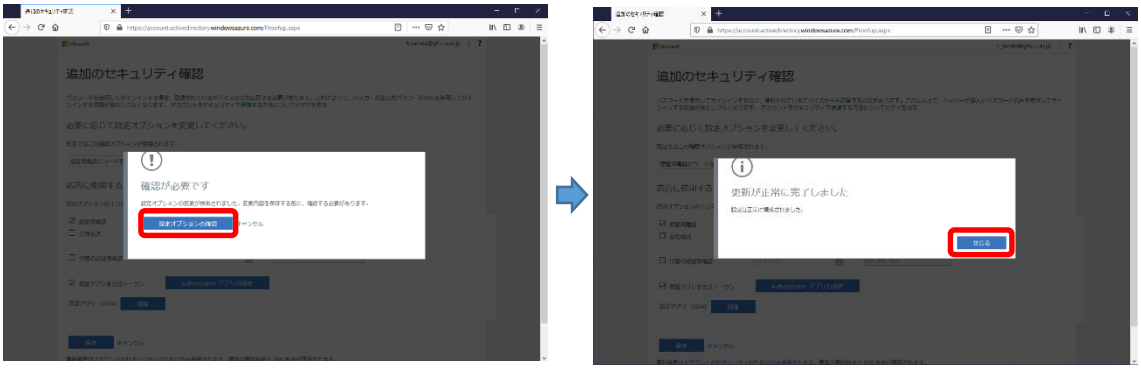
① On the "Additional security confirmation" screen, configure the following.

Default option: Call authentication phone

Method used for response: Check the "Authentication phone" checkbox, and then set "Country/region" and the authentication mobile phone number

② Clicking "Save" will display the "Confirmation required" screen. Click "Confirm configuration options" to receive a call on the registered number. Press "#."
If successful, a message stating "successfully updated" will be displayed on the PC screen. Click "Close" to complete the configuration. The "Profile" screen may then be displayed on the PC.

* On the profile screen, make sure to never select "Disable device" for the device you are currently using. Doing so will require the device to be re-enabled by an Information Management Core administrator.



(4) CHANGE METHOD TO SENDING A CODE TO THE AUTHENTICATION PHONE

① On the "Additional security confirmation" screen, configure the following.
Default option: Send code to authentication phone
Method used for response: Check the "Authentication phone" checkbox, and then set "Country/region" and the authentication mobile phone number

② Clicking "Save" will display the "Confirming phone" screen. Check the code in the message received on the phone, and then enter it on the PC.
If successful, a message stating "successfully updated" will be displayed on the PC screen. Click "Close" to complete the configuration. The "Profile" screen may then be displayed on the PC.

* On the profile screen, make sure to never select "Disable device" for the device you are currently using. Doing so will require the device to be re-enabled by an Information Management Core administrator.

(5) CHANGE METHOD TO APP NOTIFICATION

① If you have not yet installed the app, refer to **2. Preparing for Use** and install the app on the authentication device.

② On the "Additional security confirmation" screen, configure the following.

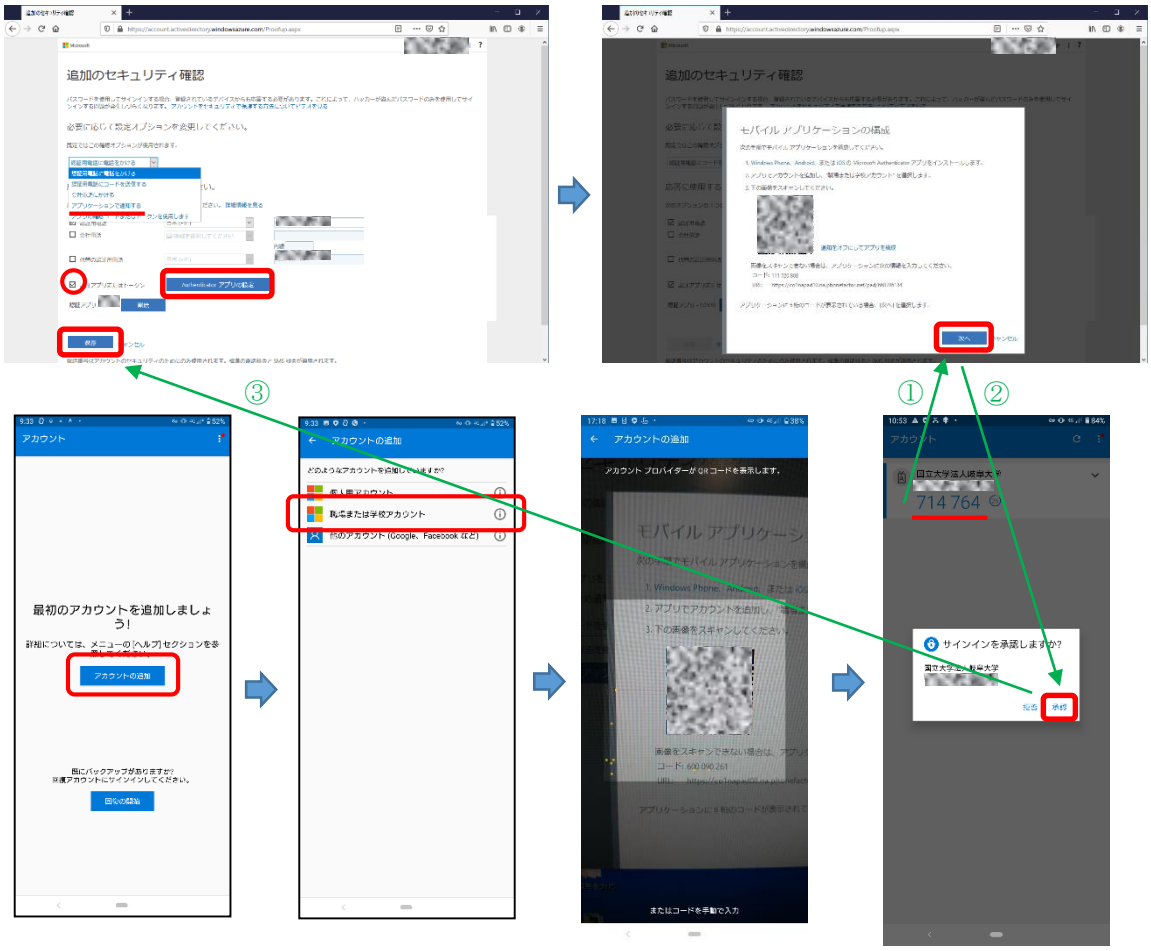
Default option: Notify with application

Method used for response: Check the "Authentication app or token" checkbox

Authentication app: If any devices are displayed, "Delete" them

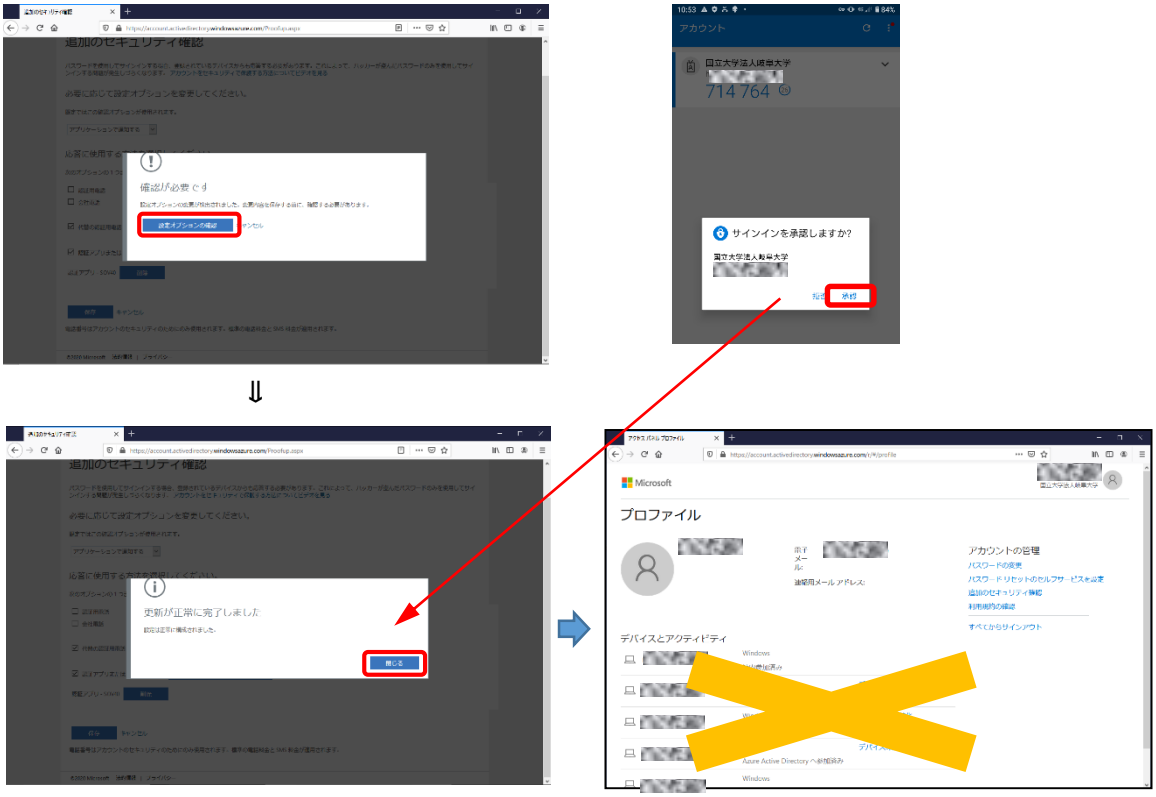
* If an alternate authentication phone is required, set "Country/region" and the authentication mobile phone number.

③ Click "Authenticator app settings" to display the QR code. Scan this code using the camera app. Once configuration on the app is successfully completed and the code is displayed, click "Next" on the PC. You will be asked for your approval on the app. Tap "Approve." The device will be displayed for the authentication app on the original screen. Confirm that "Default option" is set to "Notify with application" and then click "Save" (in order of ①②③ (green) in the figures below).



④ On the "Confirmation required" screen on the PC, click "Confirm configuration options." A sign-in approval notification will be received by the Microsoft Authenticator app on the registered device. Open the app and tap "Approve." When the PC screen switches to a message stating "successfully updated," click "Close." Configuration is complete when the PC switches to the profile screen.

* On the profile screen, make sure to never select "Disable device" for the device you are currently using. Doing so will require the device to be re-enabled by an Information Management Core administrator.



(6) CHANGE METHOD TO USING CONFIRMATION CODE FROM MOBILE APP

① If you have not yet installed the app, refer to **2. Preparing for Use** and install the app on the authentication device.

② On the "Additional security confirmation" screen, configure the following.

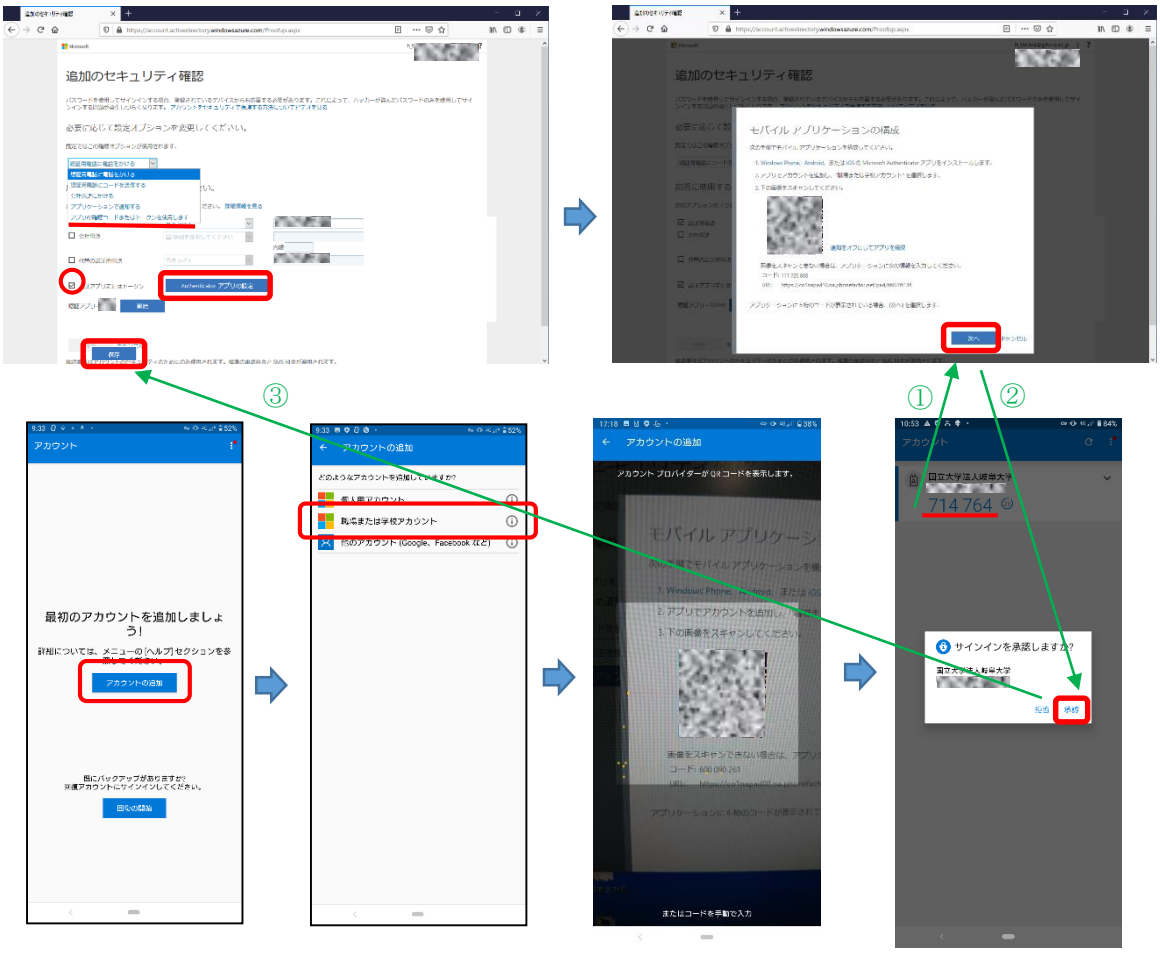
Default option: Use app confirmation code or token

Method used for response: Check the "Use authentication app or token" checkbox

Authentication app: If any devices are displayed, "Delete" them

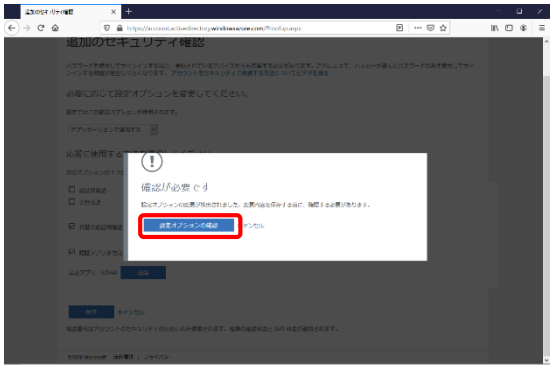
* If an alternate authentication phone is required, set "Country/region" and the authentication mobile phone number.

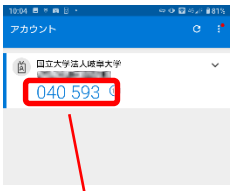
③ Click "Authenticator app settings" to display the QR code. Scan this code using the app camera. Once configuration on the app is successfully completed and the code is displayed, click "Next" on the PC. You will be asked for your approval on the app. Tap "Approve." The device will be displayed for the authentication app on the original screen. Confirm that "Default option" is set to "Use app confirmation code or token" and then click "Save" (in order of ①②③ (green) in the figures below).



④ On the "Confirmation required" screen on the PC, click "Confirm configuration options." On the "Confirming app or token" screen, you will be asked to "enter the confirmation code or token displayed in the app." Enter the confirmation code from Microsoft Authenticator on the registered device. When the screen switches to a message stating "successfully updated," click "Close." Configuration is complete when the PC switches to the profile screen.

* On the profile screen, make sure to never select "Disable device" for the device you are currently using. Doing so will require the device to be re-enabled by an Information Management Core administrator.




アカウント
国立大学法人岐阜大学
040 593


追加のセキュリティ確認
アプリまたはトークンの確認中

⇒


Microsoft
プロファイル
アカウントの管理
デバイスとアクティビティ

6. Important Notes

① Devices registered according to the procedures in this manual must be strictly managed in accordance with Gifu University Password Guidelines 3.4 and 3.5. Ensure that these resources are managed and used appropriately.
Actions such as leaving the app screen open on a registered device or failing to delete a message after use may unnecessarily allow users other than the intended user to access Gifu University systems. Please make sure to handle information appropriately after use.

② It is recommended to confirm an operation assuming use outside the university after registration for devices registered according to the procedures in this manual. When phone numbers and other information are registered according to the procedures in this manual, only the most recently registered information will be valid. Multiple app devices may be registered.

③ If you begin using a different device, please make sure to delete any relevant messages, apps, and information from the previous device. You will then need to register the new device.

④ If you must use Gifu University Microsoft 365 from outside the university but cannot register, please contact Information Management Core through your department.
* No links will be provided in an email on how to prepare for use or begin using this service. Please access this information from the Information Management Core website, or add the link as a favorite.

⑤ If you lose a registered device, please either initialize the registered device as soon as possible or refer to "5. Changing the Authentication Method" in this manual to delete the registration for the lost device, change your registration to another device, or change the authentication method. If doing so will be difficult, please contact Information Management Core.
(Email: imc-help@gifu-u.ac.jp extension 2041)
* It is recommended to enable remote initialization for your device in case it is lost.

⑥ If you have any other questions or concerns about use, please contact Information Management Core (Email: imc-help@gifu-u.ac.jp extension 2041).