👆 What is multi-factor authentication for **IMC accounts**?
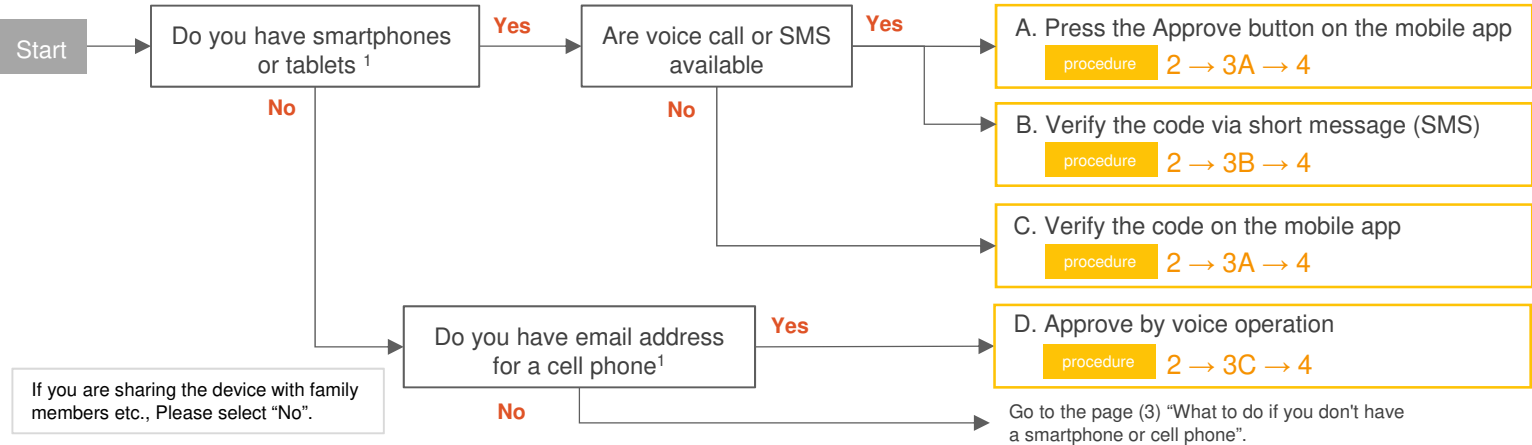
- ✓ **An IMC account** is a number, which is a **string of 3 to 8 alphanumeric characters** (for staff) , **lowercasing the first letter of your student number** (for student).
- ✓ An IMC account is used for **Hirodai mail, VPN access and** login for **Microsoft365, Teams**, etc.
- ✓ When accessing from off-campus, authentication by a second factor (a device different from the computer) is required.

Setup instructions page
(IMC account)

The setting depends on the device used as the second factor. Please prepare your smartphone, cell phone, or other second devices.

1 Decide the second factor you use

Start → Do you have smartphones or tablets [1] → **Yes** → Are voice call or SMS available → **Yes** →

A. Press the Approve button on the mobile app
procedure 2 → 3A → 4

B. Verify the code via short message (SMS)
procedure 2 → 3B → 4

(Are voice call or SMS available) **No** →
C. Verify the code on the mobile app
procedure 2 → 3A → 4

(Do you have smartphones or tablets) **No** → Do you have email address for a cell phone[1] → **Yes** →
D. Approve by voice operation
procedure 2 → 3C → 4

If you are sharing the device with family members etc., Please select "No".

(Do you have email address for a cell phone) **No** →
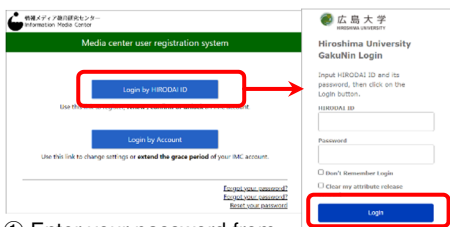Go to the page (3) "What to do if you don't have a smartphone or cell phone".

2 Apply Multi-Factor Authentication using your personal computer

Access the **IMC Registration System** with your computer browser and apply to [login by HIRODAI ID].
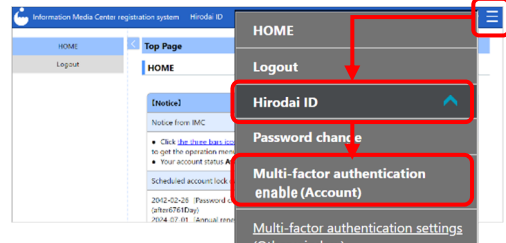
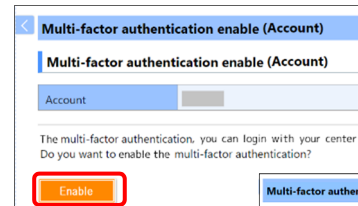https://reg.huc.hiroshima-u.ac.jp   Access the URL

① Enter your password from [Login by HIRODAI ID]
IF you log in from an off-campus network and the message " MFA has not been setup yet." is displayed, please configure MFA for your HIRODAI ID first.

② Click [広大ID] in menu ≡
→ Multi-factor authentication enable(Account)
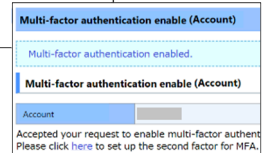(or Multi-factor authentication Initialize（Account))

③ Click [Enable]
(or [Initialize])
※ It takes up to 30 minutes for the [Enable] to be reflected in the system.
※ After 30 days of account registration, the button will change to [Initialize] .

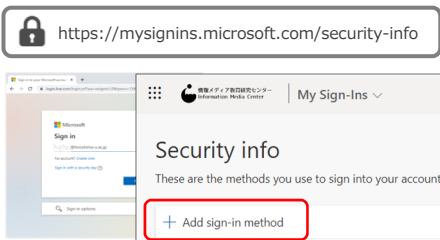④ Click [**here**] to go to STEP 3.

3A Setup with mobile app

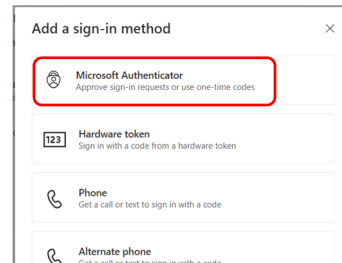Download the app and read the QR code.

Google Play で手に入れよう   App Store からダウンロード

Download

Microsoft Authenticator

① Install [Microsoft Authenticator].
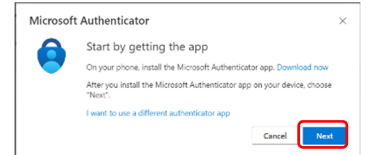
https://mysignins.microsoft.com/security-info

② Sign in Microsoft365 [Security info] on your computer. → [Add sign-in method]
※ If the [More information required] screen is displayed, click [Next] and go to ④
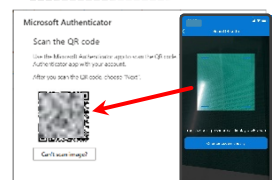
③ Click [Microsoft Authenticator] app

※ If you selected "C. Confirm the code with the mobile app and ente it" in step 1, select "I want to use a different authenticator app".
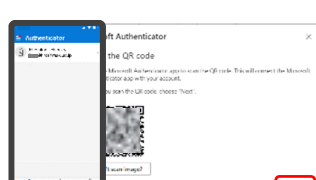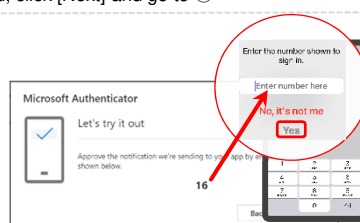
④ Click [Next]

⑤ Click [Next]

⑥ Launch the application
→ [Add]
→ [Work or school account]
→ [Scan the QR code]

⑦ " Hiroshima University IMC account@hiroshima-u.ac.jp" appears on your phone, click [Next].

⑧ Enter the notified number into the smartphone app, Tap [Yes].

⑨ Click [Next].   Go to 3B or 4

Please enter your phone number in case you need it.

3B Set up with short massage (SMS)

Specify and confirm the phone number to receive the code via SMS.
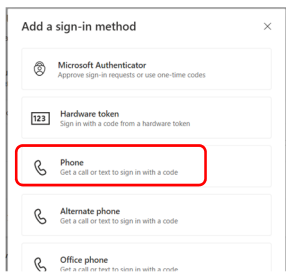
🔒 https://mysignins.microsoft.com/security-info

① Sign in Microsoft365
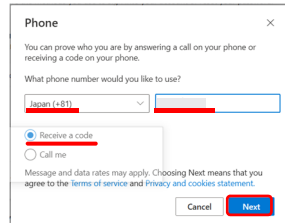[Security info] on your computer.
→ [Add sign-in method]

※ If the [More information required] screen
is displayed, click [Next] and go to ④

② Click [Phone]

③ [Country/Region]
[Enter your phone number]
→ [Receive a code] → [Next]

④ A confirmation code (short message)
will be sent to your registered
phone number.
→ Input number and [Next].

⑤ "Verification complete. ……."
is displayed, Click [Done]

3C Set up with voice call

Specify and confirm the phone number to receive voice call.

🔒 https://mysignins.microsoft.com/security-info

① Sign in Microsoft365
[Security info] on your computer.
→ [Add sign-in method]

※ If the [More information required] screen
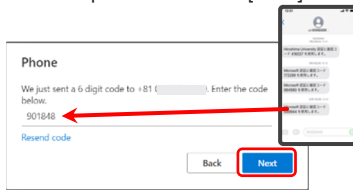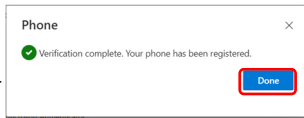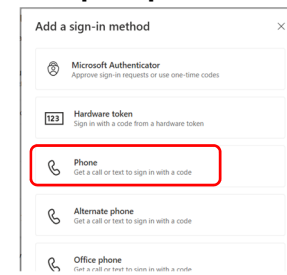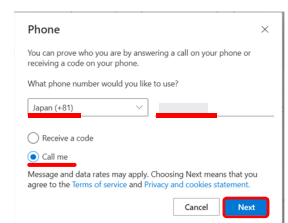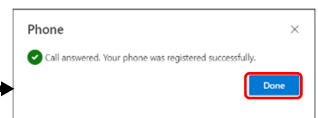is displayed, click [Next] and go to ④

② Click [Phone]

③ [Country/Region]
[Enter your phone number]
→ [Call me] → [Next]

④ Receive voice call and follow
the guidance to operate the phone.

⑤ "Call answered. …successfully"
is displayed, Click [Done]

Go to 4

4 Confirm the MFA configuration after set up

Finally, **sign out once, close your web browser** and then let's confirm whether multi-factor authentication actually works.
Multi-factor authentication will be skipped when you access from the campus network, check the operation from the off-campus network. However, you can check the operation by accessing "Security Information" even from the campus network.

When the security
information is displayed,
the setting is complete .
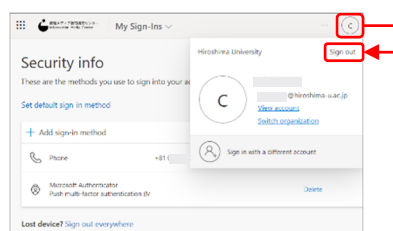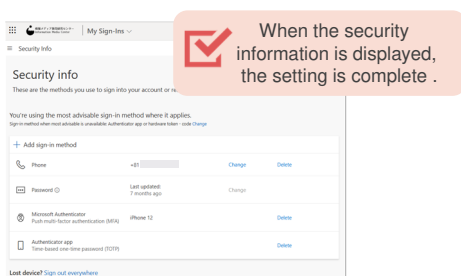
① [Security Information] page will appear,
click [Sign out] from the profile icon ,
and then web browser will also be closed.

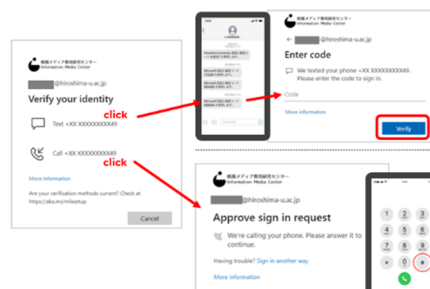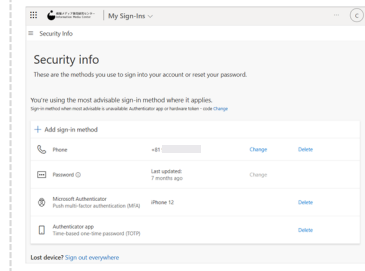🔒 https://mysignins.microsoft.com/security-info

② Access Office365 [Security Information]
on your computer
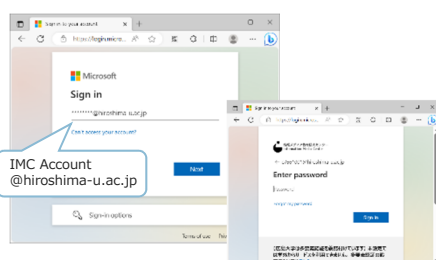
[Approve on the mobile app]

[Verify the code by SMS]

[Approve by voice operation]

④ Authenticate with the second factor

⑤ Login completed

## 🔍 How to add or change the second factor after setting multi-factor authentication

If you want to change the settings after setting up MFA,
you can do this from the Microsoft365 portal [Security Information] .

① Sign-in to Microsoft365
    Click on the profile icon in the upper right corner.
        → View account
            → Security Information > [UPDATE INFO].

When you access [Security Information] from the campus network,
you will be asked for multi-factor authentication. Please authenticate
before accessing the site.

②   ・In the case of adding a second factor.
            [Click the "Add sign-in method"]
    ・In the case of changing the phone number.
            [Click the "Change"]

①

②
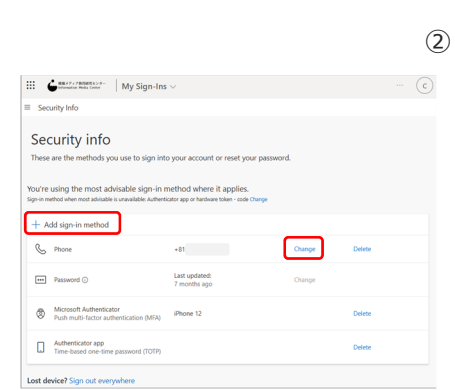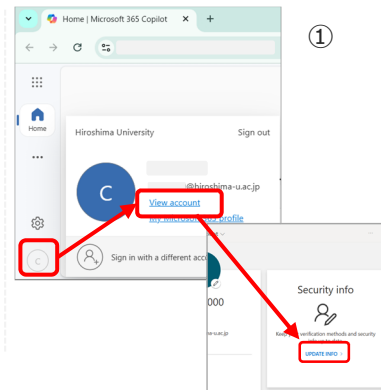
◆   If the second factor authentication is not available, please refer to "How to reconfigure the application (multi-factor authentication for IMC accounts)".
(https://www.media.hiroshima-u.ac.jp/services/mfa/mfa4imcaccount/mfa-imc-app-resetting/)
Click to access the page

Please be sure if you use an email client

Hirodai Mail (Microsoft365 Exchange Online) supports advanced/modern authentication (OAuth2.0).

If you want to use your email client after setting up MFA, you will need to set the advanced/modern authentication. You cannot send or receive e-mails without changing the settings.

Advanced/modern authentication is an authentication method that uses a mechanism called an access token to ensure higher security in order to solve the security problems of conventional authentication using IDs and passwords (basic authentication).It is possible to access email service with multi-factor authentication by using mail client that supports advanced/modern authentication.

Thank you for your understanding and to use an email client that supports advanced authentication or the latest Microsoft or Apple email client.

> **Email clients that support advanced authentication (as of October 2021)**
>   Outlook app for iOS/Android, macOS/iOS standard email client,
>   Thunderbird (78.3.1 or later), Becky! Internet Mail (v2.75.02 or later), etc.

How to configure Thunderbird for Oauth2.0 is introduced on the IMC website.

IMC Webpage
 → All Services
 → Hirodai Mail
 →mail software
    → Example configuration for Thunderbird

https://bit.ly/2XFSL8h

❓ When in trouble

● Is there any way to check the current configuration status?
    ✓   When sign in an Office365 from an off-campus network (home, smartphone tethering, eduroam, etc.),
        if you are asked for the second factor, multi-factor authentication is enabled.
● After setting up MFA, I can no longer send or receive Hirodai email. What should I do?
    ✓   If you are using e-mail software that does not support multi-factor authentication, you will need to set an
        app password. Please check "Additional security settings (application password)" on the previous page.
● What should I do if I have changed my phone or a deleted the authentication application?
    ✓   You need to reconfigure. Please follow the instructions of "How to add or change the second factor after
        setting multi-factor authentication" or "How to reconfigure the application(multi-factor authentication for
        IMC accounts" to reconfigure second factor.
● What should I do if I want to disable multifactor authentication due to trouble?
    ✓   You cannot disable, but you can initialize. In setting according to Step 2, select "Multi-factor
        authentication initialize (Account)" and reconfigure.

IMC FAQ Site

⚠ What to do if you don't have a smartphone or a cell phone

Multi-factor authentication can be performed using an extension of the web browser of the computer being used.
Please use this service only if you set a login password on your computer and manage it well so that it cannot be used by others.

FAQ page
https://help.media.hiroshima-u.ac.jp/index.php?solution_id=1170