How to setting TOTP(One-time password) (From off-campus・Google Authenticator)

TUT Information media center

Our university has introduced two-factor authentication (TOTP authentication) using one-time passwords which based on time to ensure identity and prevent unauthorized using of important systems. This authentication requires one-time passwords in addition to the username and password which user remembered to achieve strong authentication. A one-time password can be generated only on the smartphone which user owns.

Therefore, it is necessary to install an application for using TOTP authentication on your smartphone in advance and register it with University's user authentication system. This section describes the procedure for registering the one-time password application 'Google Authenticator' in the authentication infrastructure system.

This document describes the procedure for setting from off-campus network. Please see https://imc.tut.ac.jp/totp for the procedure of setting from on-campus network.

The authentication method is switched depending on the type of access source network (on-campus or off-campus). For example, on-campus networks can be authenticated only with a username and password, but off-campus networks require TOTP authentication in addition to that. In this classification, the following networks are classified as "off-campus".

- Connection from off-campus by VPN
- Wired guest network (Village Tenpaku etc.)
- Wireless network SSID: eduroam
- Wireless network SSID: tutguest

What to prepare

- Account Information Notification (This procedure requires your own username and password)
- Matrix code (From the document "Notification of Your Matrix Code")
- Environment which you can receive the password recovery email address

Please refer to https://imc.tut.ac.jp/passwordreset if you have not acquired the authentication matrix code or have not registered the password recovery email address.
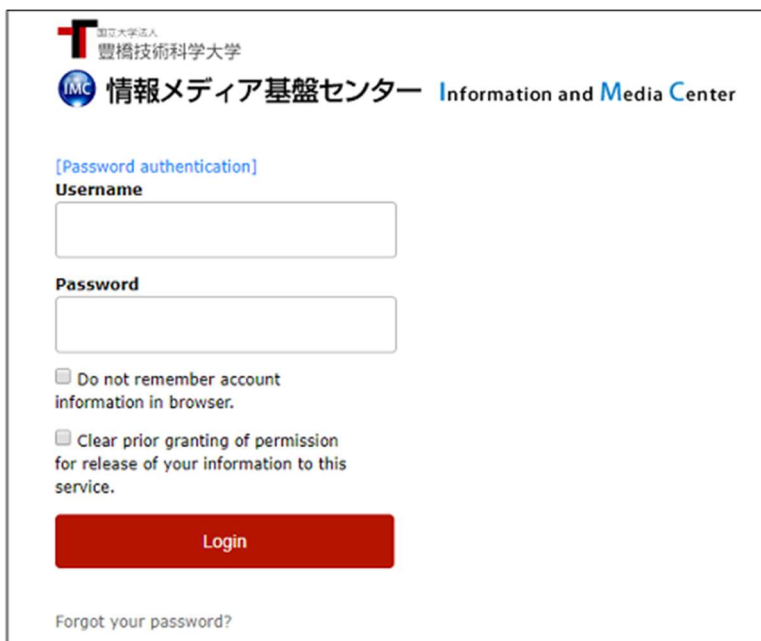
Procedure of registering the one-time password App

1. Connect your PC and smartphone for the setting to the network.

2. Check the date and time on your PC and smartphone are correct.

3. Install Google Authenticator on your smartphone.

   Google Authenticator
   iOS: https://apps.apple.com/jp/app/google-authenticator/id388497605
   Android: https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2

4. Display "User Profile Maintenance" page in the PC browser.
   To display the "User Profile Maintenance" page, click "Change password" in quick menu on
   the home page of the Information Media Center (https://imc.tut.ac.jp/).

5. On the "Password Authentication" screen, entry username and password listed on "Account
   Information Notification".

6. Click "Register the one-time password generator" on the User Profile Maintenance page.

7. "Matrix authentication" screen will be displayed. Entry the value which corresponding to the coordinates on PC browser by referring to the authentication matrix code.

For example, if the value in row F and column 5 of "Notification of Your Matrix Code" is "12" and the value in row F and column 3 is 55, enter 1255··· and so on. Repeat this for the number of coordinates shown.

8. Select 「Agree」

9. The QR code will be displayed on PC browser. Start Google Authenticator on the smartphone and scan the QR code.

To register your one-time password (OTP) generator to the university authentication system, follow the steps below.

1. Install a OTP generator such as Google Authenticator or Microsoft Authenticator to your smartphone.

iPhone/iPad   Android

Google Authenticator   Google Authenticator
Microsoft Authenticator Microsoft Authenticator

2. Scan the QR code below with your OTP generator. If your OTP generator does not read the QR code correctly, manually enter the registration key KAKVDZBBJWZT6GPL into your OTP generator.

キー：

3. Enter the 6-digit one-time password generated by your OTP generator and press the "Register" button.

[ ] [Register]

※There is some possibility of being displayed "Registered" sign, even if you have not registered the one-time password application. In that case, click the "Reissue" button.

Your one-time password (OTP) generator has already been registered to the university authentication system.
Do you need to overwrite its registration?
If you need to overwrite its registration, click the "Re-register" button.
If you do not need to do so, click the "Logout" button.
[Re-register] [Logout]

Follow the steps below on the Google Authenticator app.

①Tap 「設定を開始」（start setting）
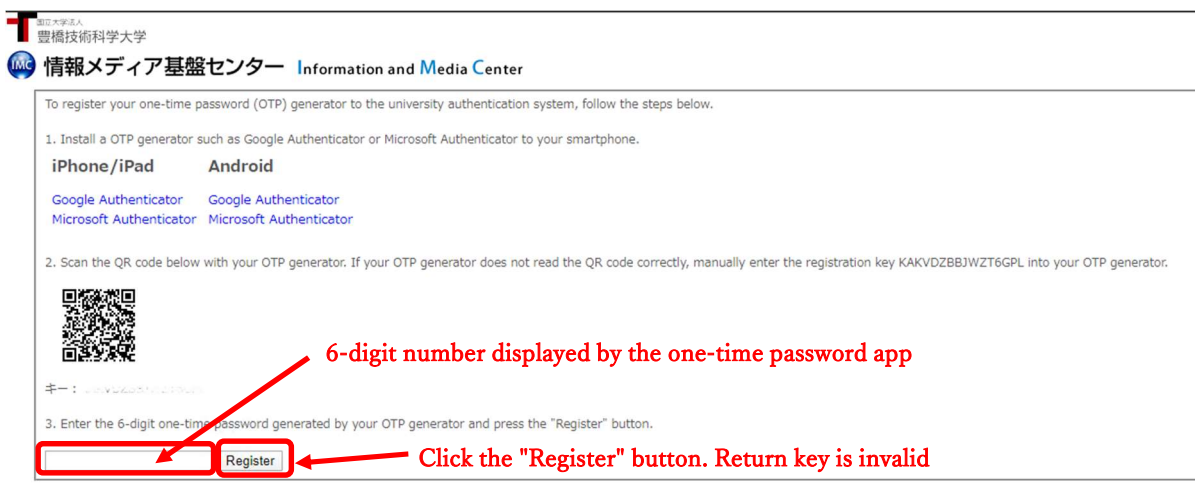

②Tap「バーコードをスキャン」（Scan the barcode）

③The「バーコードをスキャン」(Scan the bar code) screen will appear. Scan the QR code displayed on the browser.

When the QR code is displayed in green frame, it will be scanned automatically and a 6-digit number will be displayed as shown below.

認証システム

tutimc

096 990

10. If you're successful with the scan, a 6-digit number will be displayed. Enter the number in the entry field of the PC browser and click the "Register" button.

豊橋技術科学大学
情報メディア基盤センター Information and Media Center

To register your one-time password (OTP) generator to the university authentication system, follow the steps below.

1. Install a OTP generator such as Google Authenticator or Microsoft Authenticator to your smartphone.

iPhone/iPad   **Android**

Google Authenticator   Google Authenticator
Microsoft Authenticator Microsoft Authenticator

2. Scan the QR code below with your OTP generator. If your OTP generator does not read the QR code correctly, manually enter the registration key KAKVDZBBJWZT6GPL into your OTP generator.

キー：

6-digit number displayed by the one-time password app

3. Enter the 6-digit one-time password generated by your OTP generator and press the "Register" button.

Register

Click the "Register" button. Return key is invalid

11. Registration is completed when the PC browser displays "Processing completed successfully". Click the "OK" button.

12. After the registration, access the multi-factor authentication test page
(https://example.imc.tut.ac.jp/mfa-test/) with PC browser and check the registered one-
time password application works properly. If authentication is successful, the screen shown
on the right is displayed.