At the Institute of Information Management and Communication, we are preparing for the introduction of a multi-factor authentication so that faculty, staff, etc. of Kyoto University can use the internal information services more securely. The plan is to start the trial of multi-factor authentication from summer 2020 and have all faculty and staff employ the said authentication method by 2021 when using the faculty & staff groupware and the university email system KUMail.

In this section, we will explain what multi-factor authentication is and why we need it, and then we will talk about Kyoto University's plan to implement it.

What is multi-factor authentication?

The authentication method which uses an ID and password to verify a user's identity when logging in to an information-related service has been used widely a long time. However, if users rely only on passwords to verify their identity, the use of additional methods to verify identity in addition to passwords has been rapidly spreading in recent years, with others easily impersonating them and logging into the service unlawfully when their password leaks.

Online banks are using dedicated devices and social network services are using smartphone apps and text messages (SMS) to strengthen the identity verification system.

In summary, the system of verifying identity through multiple factors, not just a password, is called multi-factor authentication. Beside the password-based authentication, various other methods can be used, such as a one-time password (password that is valid for only one login session), fingerprint or face authentication, and a method that uses a small USB device.

Need for multi-factor authentication

Multi-factor authentication has been introduced into various services in recent years. Kyoto University is preparing to install these systems, because more and more services can be used with just one user ID and because the methods of illegally obtaining user IDs and passwords have become more advanced and elaborate.

For example, although in recent years, phishing emails have become difficult to identify even if you read it carefully as scammers use tactics such as disguising the email as a reply to emails you have sent, a few years ago, most phishing emails were easily recognizable by their obviously suspicious content. Phishing websites have been designed to look exactly like the real websites. They are now difficult to distinguish, and there is a higher risk of entering ID and password.

With there being many versions of malware that are not detectable by antivirus software, ways of infecting computers with viruses have become elaborate.

Mass leaks of IDs and passwords have continually occurred across various services worldwide. The risk of unauthorized logins will be extremely high if a user continues to use other services with the same combination of user ID or email address and password as what leaked.

As such, the risk of user IDs and passwords leaking is growing.

Shifting the focus to our internal IT services, with the IT services accumulating important information more and more, an integrated authentication infrastructure was built in 2006, and by 2020, the infrastructure was linked to over 150 internal systems. The faculty and staff can now use a combination of ID and password for various services to access important information, but the consequences we will face when the IDs and passwords leak have become much more damaging.

Therefore, because the risk of password leaks is higher and damages from unauthorized logins are greater, there is a need to conduct more reliable identity verification with multi-factor authentication.

Multi-factor authentication which will be introduced at Kyoto University

Kyoto University is preparing to have a Time-based One-time Password available for use. From here on, it will be referred to as TOTP. The TOTP used in this university is a 6-digit number that differs for each user, updated every 30 seconds. This will be available for use by installing a Smartphone app or a plugin on the browsers that you usually use such as Chrome and Firefox.

Figure 1: Example of TOTP display app on smartphone

Figure 2: Example of TOTP display with browser's plugin

When asked to enter the TOTP for authentication, check the password as shown in the figures and enter the TOTP displayed that moment. Ideally, once you authenticate with TOTP, you will not be required to enter TOTP for a few days.

Implementation schedule

The multi-factor authentication trial is scheduled to start from the summer of 2020 in the faculty & staff groupware and KUMail, the university email system for faculty and staff. We will introduce the multi-factor authentication with password and TOTP during the trial only for those who request it. We will plan modifications if necessary after receiving feedback from users during the trial.

From 2021, we plan to require all users to go through multi-factor authentication when using faculty & staff groupware and the university email system KUMail.

After that, we intend to implement multi-factor authentication for other services including those used by students. Services that handle important information will be prioritized. Furthermore, a trial of FIDO (Fast lDentity Online), which is even safer than TOTP and expected to become widespread in the future, is planned as well.

(Takaaki Komura, System Design Division, IIMC)

Schedule with ease!

How are you scheduled for events such as meetings during your daily work? Coordinating schedules by emails and phone calls requires confirming with participants and is time-consuming and inefficient. Let us introduce several ways to schedule events efficiently using the new faculty & staff groupware.

Method 1.Garoon Scheduler

In Garoon's Scheduler, you can easily share suggested dates for an event to the participating group members using the function "Arrange Appointments." Additionally, you can have other users write their convenient date and time in the comment section of the tentative schedule that is shared. This allows you to check the availability of all members at once.

Please refer to the faculty & staff groupware manual "06_Schedule" for specific instructions for the "Arrange Appointments" function. [For the exact location of the manual, refer to 4. Manuals and FAQs]

Method 2.Google Forms

If you want to keep your schedule private from others, we recommend using Google Forms. By using Google Forms, you can check the availability of the participating members in a survey format. It has templates such as "Find a Time," so you can easily create a form. Google will automatically calculate the survey results for you, making it easy to decide a date.

Google Forms has various other templates besides scheduling, so please use it according to your needs.

Refer to the following on how to coordinate dates using Google Forms.

1. Access Google Forms (https://docs.google.com/forms/).
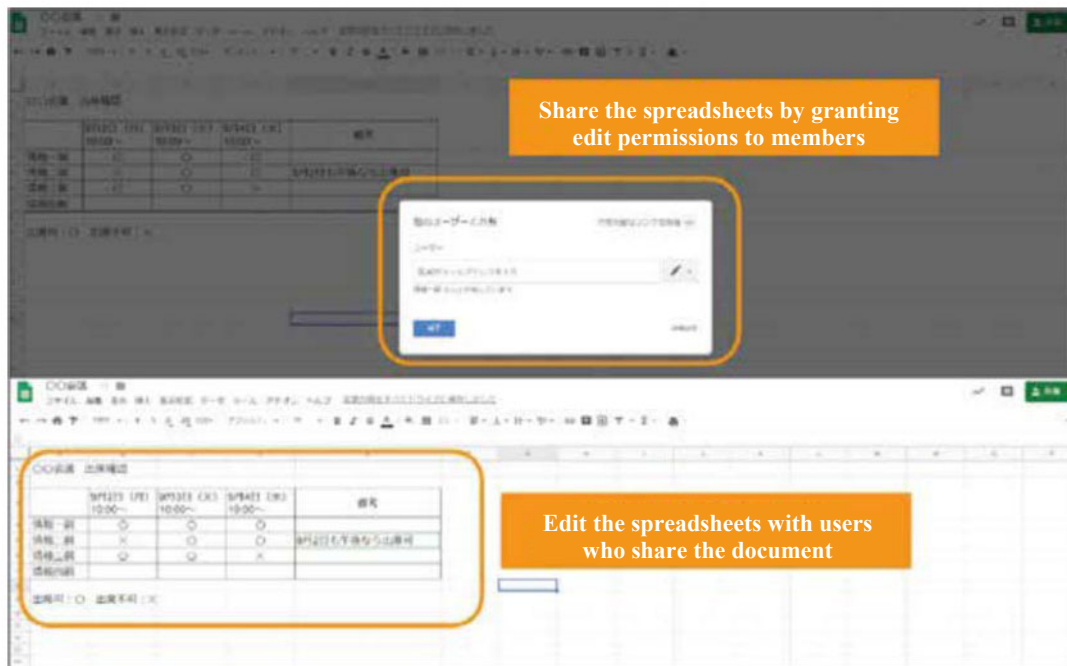2. Click "Template gallery."
3. Choose an appropriate template such as "Find a Time."
4. After editing the form, email it to the members of your group by clicking "send" or share the URL.

    Reference: Google Help—How to Use Google Forms

    http://support.google.com/docs/answer/6281888?h1=ja&ref_topic=6063584

Method 3.Google Sheets

Google Sheets is convenient if you don't mind sharing your schedule with others. Google Sheets allows you to share a spreadsheet created for coordinating dates with other members. Members who you share it with can edit the spreadsheet at any time, so you can easily work out a schedule by having them enter their availability directly into the file.

Refer to the following on how to coordinate dates using Google Sheets.

1. Access Google Sheets (https://docs.google.com/spreadsheets/).

2. Create a new spreadsheet by clicking "Blank" or click "Template gallery" and choose a suitable template.

3. After editing the spreadsheet, click "Share" and email it to the members of your group or share the URL.

    Reference: Google Help—How to Use Google Sheets

    https://support.google.com/docs/answer/6000292?h1=ja&ref_topic=9055343

Method 4.Shibosuke

Although if you are coordinating dates for an event that includes students, please use Shibosuke adapted to Shibboleth authentication of our internal SPS-ID/ECS-ID, only faculty and staff can use services in methods 1–3 mentioned above. In Shibosuke, you can create an event, enter date suggestions, and share it with other members of your group by sending an email or through the URL. The group members who you shared it with can then register their schedule on the event page or check other group members' answers at once.

Refer to the following on how to coordinate dates using Shibosuke.

   - How to use Shibosuke

      Reference:https://shibosuke.net/wiki/pages/viewpage.action?pageId ニ 1114390

(Yuki Narita, Business System Management Team, Information Infrastructure Division, IT Planning Office/Planning and Information Management Department, IIMC)

Let's Try! Information Security Ratings

My name is Toda. I was transferred to the Information Security Management Office in April 2019. Usually, there tends to be a trade-off between security and convenience, but I hope to make safety and convenience compatible.

As when we do not know which information to protect, we cannot plan our countermeasures, the most important security challenge for Kyoto University is that we are not very accustomed to determining information security levels. Therefore, so that everyone can start determining information security levels, we created the "Starting Guide for Information Security Ratings" that focuses on data confidentiality, which is the foundation of security, and published it in December 2019 on the Institute of Information Management and Communication's website.

This editorial will briefly introduce the procedures of the rating information security level. In this example, we are creating a list that summarizes a student number, name, and evaluation points of exams and reports to grade our students.

Step 1. Determining the information security level (What is its level of confidentiality?)

In the criteria of determining the information security level at Kyoto University in Appendix 5 to 12, they show standard examples. The criteria of determining information security level for student information are in Appendix 5, so check the section on scoring table (red frame) based on the contents of materials you want to create. Since the section regarding confidentiality has a "2," we will rate it "Confidential Information Level 2."

Step 2. Determining the restrictions (Who are the readers?)

The restrictions shown in the section of the scoring table (red frame) says "Limited to those related to distributors and authorities," so access will be limited to them. (*Haifu* had typographical error so we will revise it.)

Step 3. Clarifying security level and handling restrictions

Indicate the information security level as [Information with Confidentiality Level 2: Limited to those related to distributors and authorities] on the top right of the document and in the file name.

Classification	Name of information (name of file, etc.)	Overview of information	Rating Confidentiality Integrity Availability	Quantity limit	Type of device for storage	Note
Grade						
	Assessment on graduation	Student number, name, acquired credits, material on grades for determining graduation, university's academy examination report, report of investigators, etc.	2	Limited to those related to distributors and authorities, no transmission allowed		
			2			
			2			
	List of grades and number of credits earned	Student number, name, grade, number of credits earned	2	Limited to those related to distributors and authorities		Only if there are items related to the individual such as student number, name, etc. Includes data belonging to faculties.
			2			
			2			
	Scoring table	Student number, name, unadjusted score, grades	2	Limited to those related to distributors and authorities		Only if there are items related to the individual such as student number, name, etc. Includes data belonging to faculties.
			2			
			2			

Excerpted from Appendix 5

While you cannot go forward unless you take the first step, at first you might make mistakes, feel confused, or find it troublesome. It is important that each and every one of you determines and clarifies the information security level and handles the information according to the level displayed.

(Yosuke Toda, Head of Information Security Management Office, Information Infrastructure Division, IT Planning Office/Planning and Information Management Department, IIMC)

IIMC, Kyoto University
Institute for Information Management and Communication, Kyoto University