3. Safe and Appropriate Use of the Information Systems

3.1. Kyoto University' s Network and Security

3.1.1. Kyoto University' s Network

Kyoto University's campus network is called KUINS (Kyoto University Integrated information Network System) and covers not only Yoshida, Uji and Katsura campuses but also more than 100 small research labs, satellite offices scattered all over Japan. KUINS is used for internal communications and access to the Internet. The internet connectivity is realized by 100Gbps lines via SINET, the academic network to serve Japanese universities and research institutions.

3.1.2. Wired LAN and Wireless LAN

Every room in all buildings within Kyoto University' s campuses is equipped with "information sockets" and connecting LAN cable to this socket is the only necessary action to use KUINS.

Also, almost all buildings are covered by wireless LAN. There are about 1,600 access points (AP) in Kyoto University. We have started three year' s expansion plan from 2014 fiscal year and we are on our way to replace old APs and to install new APs. By the end of 2016 fiscal year, all buildings will be covered by the latest 802.11ac compliant APs.

Each AP, except some minor differences, broadcasts the following SSID:

・KUINS-Air (after ECS-ID or SPS-ID authentication, connect to KUINS-III)

・Eduroam (connect to the Internet by Eduroam account given to university members)

・ISP' s WiFi services (If you have au, NTTdocomo or Softbank accounts, you can connect to Wi2_club, 0000docomo or mobilepoint2 respectively).

3.1.3. Monitoring Network Security

Kyoto University' s network KUINS has an IDS (Intrusion Detection System) and it monitors all the communication coming-in and going-out, 24 hours a day, 365 days a year. If it finds out malware related suspicious communication, we request a security confirmation to a person responsible for the targeted machine. We do these requests day by day. In 2013 fiscal year, we did 170 requests, while in 2014 fiscal year it increased to 300 because of infamous Heartbleed and Shellshock. So our security confirmation activities occur once in one or two days!

3.1.4. University-wide security depends on each person' s shoulder

IDS do not guarantee 100% security of our university network. Although the Internet is a very useful tool, if you lack necessary precautions, you may get involved in unexpected security incidents. Moreover one person' s careless mistake may cause disastrous whole university security incidents. That is typical in the Internet. Therefore, each individual' s precaution is the most important shield against attacks.

Particularly an attached file of an e-mail or a suspicious Web site is very common place where malware hides itself. So one must make one' s eyes wide open and use e-mail and Web carefully. Also updating anti-virus software, OS (operating system) and applications is a must for everyone.

3.1.5 Security Policy protects each user

Kyoto University has detailed security policies installed.

Security policies consist of three layers: "Policy" , "Standard" and "Procedure" , gradually becoming concrete. You can consult them below:

"http://www.iimc.kyoto-u.ac.jp/en/services/ismo/use/regulation.html"

People often view security policies as cumbersome and these rules restrict free actions. But it is not. If one follows these rules, one is safer and be protected from annoying security incidents. These policies include guidelines for making strong passwords, guidelines for installing wireless LAN access points, so please have a look.

If you have something to report, questions or request for consultation, please go to each faculty' s or lab' s security desk or security liaison or security contact person.

Or you can consult the Information Security Management Office of IIMC (Use a mini-guide for contact information!)

3.2. Appropriate Management of ECS-IDs and Passwords

3.2.1. Why ECS-IDs and Passwords are Necessary

The Educational Computer System must protect the rights of authorized users who use the system, and protect users' files and information. The ECS-ID and password are used to identify users. One ECS-ID corresponds to one user so that the system can recognize which user is accessing it. The password is used as information that is only known by the actual user, and it can be used for notifying the person's identity to the system.

The Educational Computer System uses the combination of an ECS-ID and its password to identify and authorize users. In other words, if the ECS-ID and password correspond, it is considered that an authorized user is accessing the system. Therefore, it is necessary to carefully manage your ECS-ID and password.

3.2.2. If Your Password Becomes Known to Others

If your password becomes known to other persons, it means they may be able to access the Educational Computer System and related services using your ECS-ID. As a result, the following problems may occur.

- Your received e-mails and your files may be viewed or be changed or deleted by others.
- You may lose your trust by sending e-mails from your account or leaving messages on message boards.
- Other disrupting actions or crimes such as cracking of computers may be perpetrated using your account.

These actions through the computer do not show the user's actual appearance, so the doer can only be known through the ECS-ID. Therefore, actions done using your ECS-ID are considered as being done by you and you will be held responsible.

3.2.3. ECS-ID and Password Management

Passwords are confidential character strings known only by the ECS-ID holder. Passwords must not become known to anyone else. Therefore, necessary caution must be used when managing your password as shown in the following points.

- Do not tell your password to anyone. Teaching Assistants (TAs) and staff members will never ask you for your password.
- Do not write your password down. Please memorize it.
- Change your password regularly. If the same password is used for a long time, the risk of it becoming known to others increases. It will also become more difficult for you to notice that your password has become known. For more details, refer to "3.3. Changing Your Password."
- The tools for guessing passwords can easily be acquired by others. By using such tools, simple passwords can easily be guessed.
- It is not permitted for others to use your ECS-ID. It is also not permitted for you to use another person's ECS-ID.
- It is very dangerous to leave a computer where you have logged on. Always lock a computer when you leave temporarily.
- If you find a computer that is left logged on by someone else, do not touch it and notify OSL TAs at the Media Center South Building.
- Do not try to use a computer that is not approved.

3.2.4. If You Think Someone Else is Using Your ECS-ID

Referring to "Appendix 3" and consult us as soon as possible.

Caution

The Educational Computer System requires that passwords be at least eight characters long.

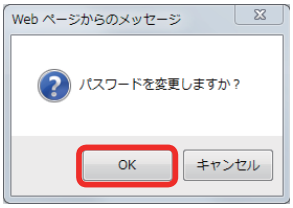
3.3. Changing Your Password

The following method can be used to change your password.

1. Access `https://ecs.iimc.kyoto-u.ac.jp/` using web browser.
2. Enter your ECS-ID and current password to login

3. Click the [パスワード変更 (Changing password)] at left.

4. Type your current password and the new password twice, and click " 実　行 ". The following window will appear, and click OK.



5. If your password is changed successfully, it says [パスワードの変更を依頼しました。(Your password has been changed.)]

3.4. Points to Keep in Mind When Using the Network

Through the Internet, computers all over the world are connected and various information services are provided. On the other hand, network usage causes various social problems. It is necessary to understand these dangers in order to use the network properly.

3.4.1. Warning about Information Security

◆ Proper Management of User IDs and Passwords

In the Educational Computer System, ECS-IDs and passwords are used to identify users and provide services such as computer terminals and e-mail. If your ECS-ID and password become known to others, problems such as those explained in “3.2.2. If Your Password Becomes Known to Others” can occur. Therefore, it is necessary to properly manage your ECS-ID and password.

◆ Warning about Computer Viruses

Computer viruses are malicious computer programs that can be received through e-mail attachments, browsing of websites, and external storage media devices such as USB Flash memory drives. Viruses then spread through networks or through external storage media such as USB Flash memory drives.

Users must keep in mind the following points.

- Do not open suspicious e-mails (attached files)
- Do not access to suspicious websites
- Do not open files from unknown sources

◆ Security Countermeasures for Your Own Computer

We request students to implement the following security countermeasures for their own computers.

- Install antivirus software and always install the latest virus definition file (pattern file).
- Always use the latest updated versions of software such as Windows OS, Microsoft Office, Adobe Reader and Flash Player.
- When connecting to a network outside of the university, make sure there is sufficient security using firewall settings.

Caution

If your computer contains a virus, it can affect many people. You may be held responsible, so it is necessary to implement sufficient security countermeasure.

3.4.2. Warning about Private Information Protection

Always use caution when handling your own or another person's private information on the network.

When inputting private information on a website, make sure that the service provider is trustworthy and that the information will be handled securely. When exchanging important information such as credit card numbers, make sure that the encrypted transmission or other safety measures by a certification body are taken to protect against impersonation.

If your e-mail address becomes known to others or if your e-mail address is made public on the Internet, a large amount of junk e-mail and virus containing e-mails may be sent to your address. Once you start receiving junk e-mail, filtering is the only countermeasure. Therefore, use caution when giving out your e-mail address.

The Educational Computer System User guidelines state that users must use their actual name, that another person's name or fictitious name must not be used and that the user must show their contact information such as their e-mail address. Therefore, it is necessary to carefully select your service provider.

3.4.3. Proper Use of Copyrighted Work

Copyrighted material such as computer software, music, videos, and publications are protected under Copyright Laws. It is necessary to understand copyrights and to use such material properly.

- When using computer software, make sure what rights the user has and then use the software within that rights.
- In order to duplicate copyrighted material outside of any exceptions in the Copyright Law, or to make access available through the network, it is necessary to acquire permission from the copyright holder.
- Quoting from another person's works in your paper without permission from the copyright holder is allowed only when specified conditions under Copyright Law are met. It is necessary to fully understand these restrictions before quoting from another's work.
- Use of photos containing other people's face is protected based on the concept of Portrait Rights. It is necessary to use caution when dealing with such rights, and it may be necessary to acquire the person's permission beforehand.

3.4.4. Crime, Disturbance, and Sexual Harassment

Recently, many crimes such as fraud and other disruptive actions have occurred through e-mail and the Internet.

- Always be aware of the risks.
- If you believe you are the victim of a crime, remain calm and handle the situation.
- If a problem occurs, do not try to resolve the problem by yourself. Receive guidance from an expert.
- If you are a victim of sexual harassment, consult the Harassment Consultation Desk of IIMC or each department.

3.4.5. Prohibited Use of P2P Type File Sharing Software

P2P type file sharing software is a kind of P2P system used to share files between connected computers. These systems become issues because they are often used to share copyrighted materials without the prior consent of the copyright holder.

It is also well known that such software is the source of information leakage due to viruses that target P2P type file sharing systems.

KUINS managing the university network requires notification when a P2P type file sharing system is used. The Educational Computer System does not make this notification and P2P type file sharing software cannot be used with the Educational Computer System.

The following programs cannot be used.

- Winny
- Share
- WinMX
- KaZaa
- eDonkey and related software (e.g. eMule)
- Gnutella and related software
  (BareShare, LimeWire, etc.)
- BitTorrent and related software
  (Including BitComet, cTorrent, Opera BitTorrent function, and Firefox AllPeers plugin)

In addition, the use of other software with functions for publishing files widely is not permitted. Most computer terminals in the Educational Computer System are restricted from having these types of software installed. However, keep in mind that there is some software that can have them installed.

3.4.6. Prohibited Use of P2P Systems Other than File Sharing

According to the KUINS usage regulations, P2P systems that are not for file sharing can be used. However, due to the design of the Educational Computer System, all communications are executed over a relay server (proxy) to the Internet. Therefore, if a P2P system is used, an overload can occur with the relay server and may cause problems for other users.

Skype and other P2P systems that are not designed as file sharing software cannot be used with the Educational Computer System.

3.5. Information Security e-Learning

All students and staff members must take the Information Security e-Leaning course. For more information about the Course, refer to the following URL.

http://www.iimc.kyoto-u.ac.jp/en/services/ismo/