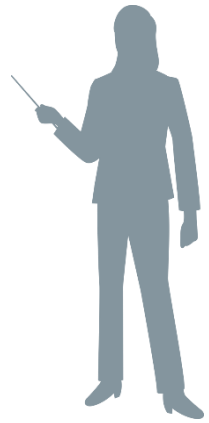
Information Security Training

FY 2018

Table of Contents



1. Introduction

In terms of information security, the world around KEK has changed drastically with the emergence of new types of threats, including targeted email attacks. However, the importance of implementing basic information security measures will not diminish even when the surrounding environment is changing.

To raise the overall level of information security within KEK, you are asked this fiscal year to relearn the “Measures to Prevent Damages Caused by Computer Viruses” and “Measures to Prevent Unauthorized Logins,” both of which are part of the basic information security measures.

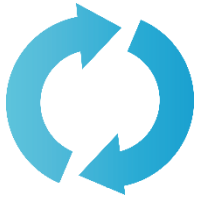
2. Measures to Prevent Damages Caused by Computer Viruses

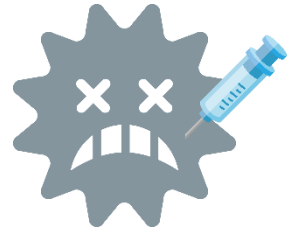
Purposes of these measures

When computers are infected with computer viruses, unintended operation may be executed*1, and it may have a big impact on you and KEK's business operation, not just directly but also indirectly*2.

Basic measures to be taken

- As long as no any specific problems occur, update your OS and software with the latest versions.
- Install antivirus software.





*1 Leakage of ID, password, and other information, damage, and attacks on others.

*2 For example, the time required to conduct an investigation and examine ways of preventing recurrence.

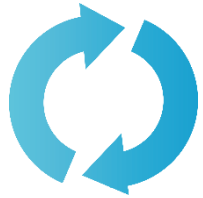
2-1. [Basic Measure] Updating OS and Software with the Latest Version as Long as No Any Specific Problems Occur

Specific action : Apply security patches on operating systems and software.
Check the manufacturers' websites for procedures of applying security patches.

Expected result : Resolution of security issues related to OS and software and mitigation of risks of computer virus infection that exploits these issues.

Note : Connecting PCs with old operating systems that are no longer supported to the network is dangerous. Particularly with Windows OS, you are not allowed to connect PCs with Windows XP, Vista, 8 (except 8.1), Windows Server 2003 R2, and older Windows operating systems to the KEK LAN.

Note : Pay particular attention to Web browsers (e.g., Internet Explorer), PDF viewers (e.g., Acrobat), JAVA, Flash, and Microsoft Office.

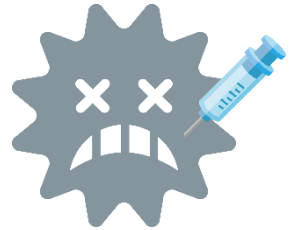


2-2. [Basic Measure] Installing Antivirus Software (1)

Specific action : Make sure antivirus software is always running to detect, quarantine, and remove computer viruses.

Expected result : Mitigation of risks of computer virus infection.

Note : Be sure to install antivirus software for Windows and Mac OS (including macOS).

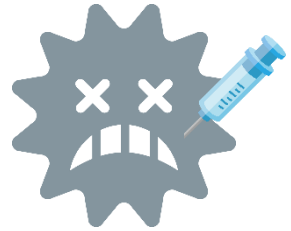


2-2. [Basic Measure] Installing Antivirus Software (2)

Specific action : Set your antivirus software to update its definition file automatically.

Expected result : Enhanced capability to detect new types of computer viruses that are created daily.

Note : Make sure the license for your antivirus software has not expired.
If it is expired, antivirus software's definition files will not be updated.



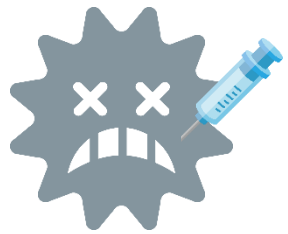
2-2. [Basic Measure] Installing Antivirus Software (3)

Specific action : As long as no any specific problems occur, run a full scan. For example, set your antivirus software to run a full scan periodically (at least once a week).

Expected result : You may be able to identify and remove undetected computer viruses that you let in to your PC unintentionally from an email or website.

Request : Run a full scan regularly whenever possible, even if it slightly interferes with your work.

Note : Antivirus software is usually not set to run full scans on a regular basis. Be sure to check the settings.



3. Measures to Prevent Unauthorized Logins

Purposes of these measures

- Simple passwords are easy to guess (crack), and
  the use of simple passwords leads to a higher risk of unauthorized logins.
- There are risks in using the same password for different systems. If your password is compromised in one of the systems, it could be used for unauthorized login in other systems.

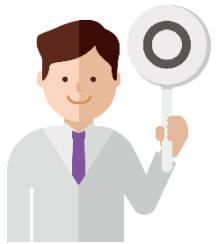
Basic measures to be taken

- **Use secure passwords.**
- **As long as no any specific problems occur, do not use the same password for multiple systems.**

3-1. [Basic Measure] Using Secure Passwords

Specific action : Use long and complex passwords.

Expected result : Mitigation of risks of third party guessing or cracking your passwords successfully.



Examples of secure passwords: Passwords that satisfy all conditions below.
- Longer password length*1
- Contains numbers and symbols (E.g., @, %, and $)
- Contains both uppercase and lowercase letters

Examples of insecure passwords: Passwords that satisfy one of the conditions below.
- Set of keys on the keyboard (E.g., qwertyui and zxcvbnm)
- Same character string as the user ID
- Same as the user's name, phone number, or birthday
- Simple character string (E.g., 123456 or abcd)
- Words in the dictionary

*1: Reference: https://en.wikipedia.org/wiki/Password_strength

3-2. [Basic Measure] Not Using the Same Password for Multiple Systems (1)

Specific action : Use different passwords for different systems.
Do not use the same password.

Expected result : Mitigation of risks of your password being used for unauthorized access to multiple systems when your password is compromised in one of the systems.

3-2. [Basic Measure] Not Using the Same Password for Multiple Systems (2)

Request : Do not use the same password for the systems inside and outside KEK.
Pay particular attention to passwords used for KEK's services that also can be accessed from the Internet.
(E.g., Webmail (post/mail.kek.jp) and VPN service)

Request : **If you can browse the past login information, look at the sources of login attempts and see if any are suspicious.**
For Webmails (post/mail.kek.jp), you can check the source IP address, date, and time for each login attempt on the "Mail Home" page.

4. Network Monitoring

- KEK uses security monitoring services provided by third parties*1 to look for suspicious activities in the communication*2 between the KEK LAN and the Internet.

- There is an increasing trend in catching data transmissions sent/received by applications considered as suspicious communication unrelated to our business and having to request the administrator to conduct investigations. Remember this fact when connecting your smartphone*3 to the KEK LAN.

*1 Private security businesses and National Institute of Informatics
*2 Communication with certain characteristics, such as the use of IP addresses or hostnames suspected as being involved in unauthorized accesses in the past.
*3 Many apps installed on smartphones are not related to our business.

5. What to Do When Something is Not Right

Emergency response contact regarding information security:

KEK CSIRT
029-879-6285
csirt@kek.jp

As long as no any specific problems occur, disconnect the “abnormal” device/equipment from the network and promptly contact the KEK CSIRT.

Examples of abnormality

- A login event that you do not recognize.
- Opening a file attached to a suspicious email.
- Hearing a clicking sound from the PC when you have not clicked any button/key.
- Discovering a Web page that has been tampered with.