Fiscal year **2024**

NAGOYA UNIVERSITY INFORMATION SECURITY

If you've experienced an information security incident, contact us

052-789-4393 (Ext. 4393)
security@icts.nagoya-u.ac.jp

Carefully Read the Information Security Guidelines

The university has established the Information Security Guidelines based on the Information Security Policy. When using an information device connected to the Nagoya University Integrated Communication Environment (NICE), the campus-wide network, conduct usage after first thoroughly familiarizing yourself with the security policy and guidelines.

Management of Authentication Data (User Names and Passwords)

If you disclose your password to another person, that person will be able to impersonate you. If the person commits a cybercrime, then you may be held responsible. Never disclose your password to anyone. If you write down the password on a piece of paper, please keep it locked away or otherwise strictly within your control. Also, make sure to use a different password for each service you use.
Tools for cracking passwords also exist in the world. Passwords composed of a word or a combination of words found in dictionaries, or only a few characters are easily cracked. Please use passwords that are composed of 10 or more characters and contain 4 types of characters — upper and lowercase letters, numbers and symbols.

Applying Security Patches

When a potential security issue related to system software or application programs on IT equipment in use is discovered, a program fix (security patch) is made available by the software developer. Users should periodically check for warnings and update notifications on developer web sites, and take necessary steps to maintain security.
In case of some old softwares, the support may have expired and no fixes are distributed. Please do not use such software, please upgrade to the latest one.
On the website of the Information and Communications, vulnerability information of the OS and application software is posted, so please refer to it as appropriate.
Try to turn on features that automatically install security patches, such as Windows Update and Microsoft Update.

Computer Viruses

Computer viruses are spread mainly via e-mail. The methods used to spread them constantly become more sophisticated. For example, a large number of e-mails that disguises credit card company have been observed. If you access the link described in such e-mails, the virus will be downloaded to your computer. In many cases, the name of the sender is forged, so be careful by not opening suspicious file attachments even when the e-mail appears to be from someone you know. Depending on the infecting virus, many computers connected to the network may be attacked automatically. Also, the infecting virus may create a "back door" breach for unauthorized access, which can be used to make your computer attack others without your knowledge.
If you think you are infected with a virus, disconnect the device from the network (by unplugging the LAN cable or turning off Wi-Fi) and contact the person in charge at the time of the information security incident.

Fishing and Smishing

Phishing scams are spreading, in which people are led to sites that steal credit card numbers, PIN number, passwords, etc. by pretending to be e-mails from financial institutions or smartphone manufacturers. Suspicious e-mails do not open. You need to be careful not to access suspicious Web pages or download applications or programs from suspicious sites. There has also been an increase in the number of cases of smishing, in which authentication information and PIN numbers are stolen using SMS (Short Message Service) on smartphones.
In the unlikely event that you access a suspicious Web page, disconnect the device from the network (unplug the LAN cable, turn off Wi-Fi, etc.) and contact the person in charge of the information security incident.

Fake Warning Tech Support Scams

Scams are spreading in which fake warning screens about computer viruses or system corruption are displayed while browsing the internet, and demands for money for the installation of unnecessary software or tech support contracts are made. Cleverly crafted fake screens using the logos of actual companies are displayed and alarm sounds and audio warnings are played to frighten users into contacting the scammers through the contact details on the screen.
Don't thoughtlessly follow the instructions in a warning, close out your browser and run a scan using anti-virus software. If the fake warning doesn't go away even after restarting your browser, or if a virus is detected, contact us using the contact details for information security incidents.

Copyrights and Intellectual Property Rights

Copying or distributing music CDs or software without the permission of the copyright-holder is a violation of copyright law. Using peer-to-peer (P2P) file-sharing programs for such purposes is not allowed. Using illustrations, photographs, logos, or other materials created by another person for your own web page, or distributing or exchanging said materials through a network or other means without the permission of the copyright-holder is not allowed. Illicit acquisition of software (purchase of a pirated copy or acquisition through Winny or the like) and use of such software is not allowed. To prevent illicit use, Nagoya University and other organizations monitor the use of Winny and other P2P file-sharing programs for copyright violations. As a rule, the use of the file-sharing programs Winny, WinMX, Share, Gnutella, Xunlei and BitTorrent is prohibited in Nagoya University. Knowingly downloading illegally distributed music or video is a criminal offense.

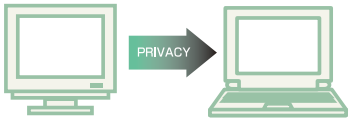
Information Leakage

Examination questions and academic records must not be saved on a computer hard disk without protection because of the possibility of leakage of important information. Take precautions such as encryption through implementation of devices (such as hardware keys) for ensuring data security and preventing data leaks. When carrying personal information off-site, follow Tokai National Higher Education and Research System Rules on the Protection of Personal Information. When transporting a notebook computer that contains important information, exercising heightened caution is necessary in order to prevent leakage of information through loss or misplacement of the computer. When operating a computer in a setting such as a commuter train, the information may be visible to persons in adjacent seats, which, depending on the type of information displayed, may be a problem.

Unauthorized Access

The Act on the Prohibition of Unauthorized Computer Access prohibits persons who have not been assigned authentication data — i.e. unauthorized users — from attempting to use computers which require authentication data. Violations may be subject to criminal penalties (up to 3 years imprisonment or a fine of up to 1 million yen).
Using another person's authentication information or helping someone else to do so is a violation of the Act on the Prohibition of Unauthorized Computer Access. Tampering with or destroying information that is not authorized to be rewritten is also a violation of the Act on the Prohibition of Unauthorized Computer Access.

Privacy



E-mail messages, forum posts, and the like that contain information relating to the privacy of another person should not be sent or posted without that person's consent.
Also, you should avoid posting it on SNS.
Even if the inquiry is from someone close to you, you should avoid providing other people's e-mail addresses or any other information related to your privacy. You should take appropriate measures, such as obtaining the consent of the person before responding.

Information Security Training for New Students

Awareness and acquiring knowledge of information security by each individual user are important in maintaining an appropriate level of information security. The Information & Communications conducts Information Security Training for New Students. Please be sure to attend the sessions. When you pass on Information Security Training for New Students, campus information services become available.

►https://icts.nagoya-u.ac.jp/en/security/training.html

Yearly Information Security Check

We carry out Yearly Information Security Check every school year in order to confirm the security level of Nagoya University is kept by the appropriate standard, by complying the information security guideline for all people belonging to Nagoya University, and to confirm it whether information security measures are proper or not. Please carry it out by all means. If you do not take Yearly Information Security Check, you will be penalized with an account lock and will not be able to use any campus information services.

►https://icts.nagoya-u.ac.jp/ja/security/annual-check.html

All new students need to carry out both Information Security Training for New Students and Yearly Information Security Check.

Links

Nagoya University Information & Communications
https://www.icts.nagoya-u.ac.jp/en/

JPCERT Coordination Center
https://www.jpcert.or.jp/english/

IPA: IT Security
https://www.ipa.go.jp/security/english/index.html

Metropolitan Police Department Information Security Forum(in Japanese)
https://www.keishicho.metro.tokyo.lg.jp/kurashi/cyber/

National center of Incident readiness and Strategy for Cybersecurity
https://www.nisc.go.jp/eng/

Aichi Prefectural Police Cybercrime Countermeasures
https://www.pref.aichi.jp/police/anzen/cyber/

Nagoya University Information

Information & Communications

Nagoya University Information & Communications

The Information & Communications(I&C) was established on April 1, 2006, with the aim of providing overall coordination among departments and other areas, and promoting comprehensive information services with respect to all information-related aspects of Nagoya University.

Collection and Provision of Security Information

Information technology is advancing with each passing day, and unforeseeable new problems may sometimes occur. I&C collects new technical information relating to security, and works to keep the level of information security at the university up to date. I&C makes information on new computer viruses, security holes, and the like available to everyone via such means as e-mail and the web. You can use the Information Security Office to report information.

▶Information Security Office
Phone:052-789-4393 (Ext. 4393)
E-Mail:security@icts.nagoya-u.ac.jp

Security Incident Response

In the event of various kinds of security incidents, including cyberterrorism and network crime, I&C works in liaison with managers and staff to investigate the incident. In the case of a serious incident, I&C interrupts or shuts down networks and systems, identifies the causes, and provides support for restoring service. Following this, I&C then investigates measures to prevent recurrence.

Security Awareness Activities

Aiming to cultivate awareness of information security on the part of students, faculty, and staff at Nagoya University and maintain high levels of security, I&C plans and conducts activities that include security training for new students and security technology workshops for system administrators.