COUNTERMEASURES TO PREVENT INFORMATION INCIDENTS

Internet Service Usage Guidelines

November 2018

RITSUMEIKAN

Ritsumeikan Information Infrastructure Improvement Committee

Cloud Environment Utilization Development Subcommittee

CONTENTS

Tips, Explanations, Examples, Column

Introduction

In recent years, the internet has established itself as part of the social infrastructure,and has become ubiquitous in daily life with services for information retrieval, online shopping, making appointments and online banking.
For educational institutions, it has become indispensable for education, research and management. With the popularization of smartphones and apps, many users enjoy the convenience of using the internet without being aware of it.

On the other hand, as the number of users increases, the number of examples of misuses of information and communications technologies (ICT) including the internet, which pose a threat to economic activities and social life, also rapidly increases. Various information security related incidents (information incidents) and crimes such as information leaks, fraud, remote access and ransom demands are also growing.

In order to counter these sorts of threats, not only the information department that manages the server systems and network systems but also **the users themselves must take information security countermeasures seriously to protect their own safety. Just as with crime prevention countermeasures and traffic safety countermeasures for everyday safety, it is important to be aware of information security related risks and implement countermeasures against them.**

This manual is not written from a “what is information security” standpoint, but focuses on explaining specific countermeasures to prevent information incidents such as information leaks or destruction and fraud, and avoiding other information incidents.

You can read it from start to finish or just the parts you are interested in, but **we recommend that you first use the countermeasures checklist in Chapter 1 “Information Security-Related Threats and Countermeasures” to check how familiar you are with information security countermeasures.**

We hope this manual helps you with information security countermeasures.

Chapter1

Information Security-Related Threats and Countermeasures

Information security-related threats

As ICT services such as the internet permeate our everyday lives, cases of information incidents caused by individuals as well as cases of information incidents caused by cyberattacks have increased, and their impact is expanding. If you cause an information incident, you may be held accountable for social responsibility, such as leaking personal and privacy related information about oneself and others or even unintentionally committing a crime.

Just like how driving a car is greatly convenient but is related to traffic accidents, use of ICT including the internet is related to information incidents, so you should be aware of them.

So, how should we take countermeasures? It's the same as with crime prevention and traffic safety. **Information security countermeasures involve knowing as much as possible about information security "risks" lurking around you, i.e. events and situations that have not yet occurred but would have an impact if they arose, as well as learning the correct ways of dealing with them and putting these into practice.**

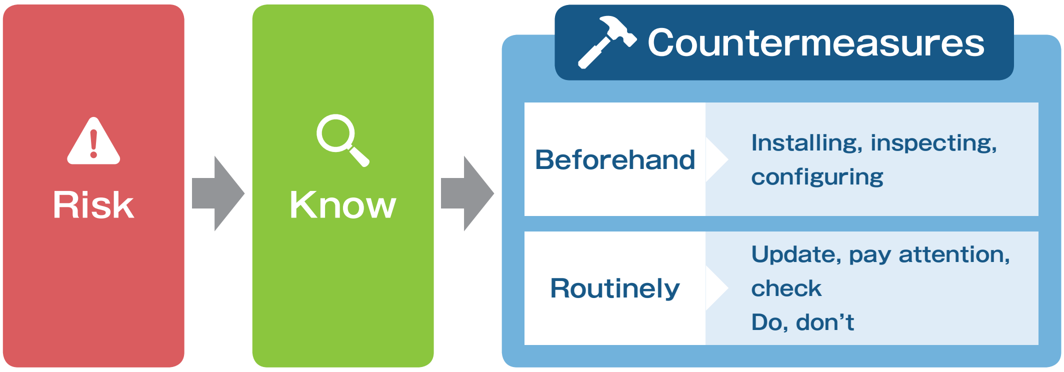

Risk
Know
Countermeasures
Beforehand
Installing, inspecting, configuring
Routinely
Update, pay attention, check
Do, don't

Figure 1 Visual example of Information security countermeasures

Information incidents arise due to various causes and have various countermeasures. The next chapter divides risk and countermeasures into 10 areas and explains each point.

The majority of information security attacks begin with a computer such as a PC or smartphone being infected with a malicious program called malware (virus) or by theft of IDs and passwords. This can lead to direct damage such as illegal use of online banking and credit cards, theft of highly confidential information, remote access and the locking of important data followed by a demand for ransom. In Countermeasures 1 and 2, “Countermeasures to prevent malware (virus) infection” and “Countermeasures to prevent ID and password theft” are explained.

The most widely used services on the internet, web and email, can infect computers with malware (viruses), which can be used to steal IDs and passwords. “Countermeasures to determine if a website or email is credible” are explained in countermeasures 3 and 4.

Due to the wide range of information devices which can be carried around besides PCs, the possibility of theft, loss, interception and configuration mistakes increases, causing information incidents to occur where personal or organization information is unintentionally leaked. In Countermeasures 5-7, “Access rights management” and “Management of mobile devices such as smartphones” are explained in order to not risk the situations described in Countermeasures 5-7, and “Encryption” is explained so that information is not leaked even when a device is stolen, lost or intercepted.

When using internet services, it’s easy to forget that you are entrusting your personal information to others. “Things to pay attention to when entrusting personal information and data to a service provider” are explained in Countermeasures 8 and 9.

Countermeasures 10 explains points other than those mentioned above.

Information security countermeasure checklist

Use the below checklist to verify your awareness of information security. If an information security countermeasure check item **is fulfilled, or if you do not use that service or device, please check the box.**

For items you did not check (including questions and words you do not understand), read and understand each of the points explained in Chapter 2, “Countermeasures to Prevent Information Incidents.”

■ Information security countermeasure checklist ■

Countermeasures 1	Malware (viruses)	
1-1	Install and utilize antivirus software on PCs and smartphones	□
1-2	Periodically update the PC and smartphone OS	□
1-3	Periodically update the firmware of devices attached to the network	□
1-4	Periodically update applications which are not part of the OS (including smartphone apps)	□
1-5	Before installing software, verify the authenticity of the manufacturer, contributors and distribution source	□

Countermeasures 2	ID and password management	
2-1	Never tell your password to anyone, even system administrators	□
2-2	Understand the importance of password strength and use strong passwords	□
2-3	Do not use (reuse) the same password across multiple services	□
2-4	Password management tools are used to manage IDs and passwords, but the password character strings themselves are not entered into the management tool	□
2-5	Proactively use multi-factor authentication, or select services with multi-factor authentication when depositing highly confidential data	□
2-6	Periodically check login history	□

Countermeasures 3 Websites

3-1	Use antivirus software that detects dangerous websites and produces warning notifications	□
3-2	Do not relax the browser's security functions more than necessary	□
3-3	Always scan files downloaded from websites for malware before using them	□
3-4	Be careful not to be led to fake websites	□
3-5	Be able to recognize scam websites and advertisements	□
3-6	If you browse to a suspicious website or get an unfamiliar warning, use antivirus software to fully scan the machine	□

Countermeasures 4 Email

4-1	Use a spam email filter and periodically check the emails sorted into the spam email folder	□
4-2	Be extremely careful when opening attached files and links in emails	□
4-3	Always suspect that unknown received emails may be fraudulent emails	□
4-3	Understand phishing emails and be able to identify them	□
4-4	Understand what targeted attack emails are and be able to identify them	□
4-5	Understand points for recognizing suspicious emails	□
4-6	Always be careful to avoid missending emails	□
4-7	Be careful not to write (or attach) highly confidential information with email	□

Countermeasures 5 Encryption

5-1	Be able to tell whether or not communications are encrypted when using a website	□
5-2	Know the likelihood of email interception	□
5-3	Understand wireless LAN (Wi-Fi) encryption methods and the risks of connecting to Wi-Fi networks outside the home and office	□
5-3	Understand the security functions of wireless routers (Wi-Fi routers) and configure them appropriately	□
5-4	Know the methods for encrypting data on devices such as PCs, smartphones, USB memory and SD cards and use these methods as necessary	□

Countermeasures 6 Access rights management

6-1	When configuring files to be shared on a PC, always give the other party the minimum permissions needed	□
6-2	When using online storage, make sure not to set confidential data as visible to the public on the internet	□
6-3	Configure the appropriate security settings for devices connected to the network	□

Countermeasures 7 Management of mobile devices such as smartphones

7-1	Configure mobile devices such as smartphones so that even if they are lost or stolen, other people cannot use them or retrieve data from them	□
7-2	Check the functions and data accessed by smartphone and tablet apps (such as the camera, location information and contact address)	□

Countermeasures 8 Personal information and the infringement of rights

8-1	Understand the collection of user information through PCs and smartphones and configure the appropriate restrictions	□
8-2	If you are using a PC that is also used by others, understand how website browsing history is recorded and how others may be able to see it	□
8-3	On social media, understand that individuals may be identified using assorted information and image location information, and pay attention to sharing settings	□
8-4	Understand the fundamentals of “Intellectual property rights,” “Personal information protection” as well as laws and regulations concerning data migration (Foreign Exchange Act, GDPR)	□

Countermeasures 9 Check the agreement with the service provider

9-1	When using a service on the internet, check whether or not the provider and service are trustworthy	□
9-2	When entering personal information into an internet website, check their personal information handling policy	□
9-3	When using services which store data such as email and online storage, check the terms and conditions to see how the service provider will use the data	□
9-4	When using services on the internet, check where the data is stored and which laws apply in the event of a dispute	□
9-5	When using services which store data such as email and online storage, prepare for data loss in events such as system malfunctions and make backups	□
9-6	When using services on the internet, be aware that the provider can change the conditions so always be prepared	□

Countermeasures 10 Other

10-1	When disposing of or transferring devices which store highly confidential information such as PCs, smartphones and network attached storage (NAS), completely erase the data or physically destroy the device	□
10-2	Understand the risks of using file-sharing software and that you are not using this kind of software	□

Chapter2

Countermeasures to Prevent Information Incidents

Countermeasures 1 Malware (viruses)

We expect that most people are familiar with the term “computer virus.” Traditionally, they were called this because they parasitize other files and programs to perform malice, similar to a biological virus. Today, there is increased malicious software that does not match the definition of previous computer viruses, such as spyware, bots and ransomware, so malicious software is now called by the abbreviation “malware.”

Because malware infection lays the foundation for any criminal act such as information theft, fraudulent online banking remittance, credit card theft, remote access and ransom demands, an attacker’s primary objective is to infect using malware. Accordingly, here we explain countermeasures to prevent malware infection.

5 key points related to malware

- 1-1 Install antivirus software
- 1-2 Update the OS
- 1-3 Update all devices connected to the network
- 1-4 Update applications
- 1-5 Only install software that can be trusted

1-1 Install antivirus software

A simple and effective malware countermeasure is to install antivirus software (also called as AV software, vaccine software, etc.) on your PCs and smartphones. Antivirus software should be configured to automatically update the definition files and detection engine. **Always use the latest version.**

However, just because antivirus software is installed does not mean you are completely safe from risk. The basic functionality of antivirus software is to protect PCs and smartphones from “well-known malware.” Malware is sold and used for cyberattacks after establishing that many types of antivirus software do not detect it. Large numbers of “unknown malware” are detected every day, so there is always a risk of infection. There is also malware which cannot be detected at the time of infection but can be detected through scheduled scans. When installing antivirus software, **configure it to scan periodically.**

In addition to the ability of recent antivirus software to detect “well-known malware,” they now have various other functions such as “detects unauthorized program actions (behavior detection, heuristic detection),” “network attack prevention (personal firewall and IPS/IDS)” and “safe area for software test executions, and detecting unauthorized program actions from its behavior (sandbox).” Each software manufacturer has a different name for it, but you should look for software that **detects unauthorized program actions (behavior detection, heuristic detection).** This increases the chance of preventing attacks from unknown malware.

Also, **since malware damage to smartphones has been widely reported, you should install antivirus software on them.**

Tips❶

Windows is usually equipped with antivirus software

Windows 8.1 and after has antivirus software installed by default with the Windows Defender feature. As a result, the “Install antivirus software” process is at least covered as a minimum. Check the current settings and do not change from the recommended settings.

Explanation 1

Is antivirus software required for macOS, Linux or iOS?

Some people believe that antivirus software is not required for operating systems such as macOS, Linux and iOS. Despite the fact these operating systems have also been reported to be affected by malware, one cause of the misunderstanding that antivirus software is unnecessary is that compared to Windows and Android, the Countermeasures 1-5 “Only install software that can be trusted” is often thoroughly enforced. The second cause is that operating systems with more users are more easily targeted for profit-oriented cyberattacks. Therefore, it cannot be said that because damages are relatively rare due to other countermeasures and market share, that antivirus software is not essential.

Also, we recommend installing antivirus software not only for detecting well-known malware, but also because it has multiple security features. (See Countermeasures 3 “Web,” Countermeasures 4 “Email,” Countermeasures 7 “Mobile devices such as smartphones”)

1-2 Update the OS

It is difficult to completely remove “functional bugs and security defects” (hereinafter, “vulnerability”) from software. Most malware exploits these vulnerabilities to infect PCs. Most computers have software called operating systems (OSs), such as Windows, macOS and Linux to run the machine, and for attackers, OSs used by many people are attractive targets for attacks. Manufacturers supply OS patches for vulnerabilities which are discovered every day, and users can reduce vulnerabilities and decrease the risk of malware by updating the OS and applying software patches. **You should check the Windows Update and Mac App Store update settings on your computer and configure security updates to be automatically applied.**

Recently, damage caused by malware targeting smartphones has also been increasing. In addition to installing suspicious apps, there have been cases reported where both Android and iOS have been infected with malware by simply opening links to websites contained in emails. Smartphones are also a type of computer, and because vulnerabilities are discovered, smartphone operating systems such as iOS and Android also need to be updated. **Even on iOS and Android, you should back up your important data before updating.**

Ref: Lookout, “モバイルセキュリティアラート：iOSを標的にした高度なモバイル攻撃が発生 (Mobile security alert: Outbreak of sophisticated mobile attacks targeting iOS)”[1]
https://blog.lookout.com/jp/2016/08/29/securityalertpegasus/

[1] This website is Japanese only.

How to check for updates on each OS

■**Windows 10**
[Settings] ❯ [Update & Security] ❯ [Windows Update]

■**macOS**
[System Preferences] ❯ [Software Update]

■**iOS**
[Settings] ❯ [General] ❯ [Software Update]

■**Android**
[Settings] ❯ [Device management] ❯ [About phone] ❯ [Software Update]

Also, **do not skip installing antivirus software or updating the OS as mentioned above.** For example, antivirus software is monitored by a security company, and OS updates (vulnerability countermeasures) are like repairing defects in a building. If there are defects in the locks or windows of a building, a security company will not be able to protect it no matter how much they monitor it.

Tips❷

OS update types and risks

There are three major types of software updates: (1) Feature addition/modification (2) System bug fixes (3) Security update. Updates are often represented in versions, and the meaning of the version numbers vary by manufacturer and software.

For example, iOS versions go from 9.3.5, 10.0, 10.0.1, 10.0.2, 10.0.3, 10.1, 10.1.1, 10.2, 10.2.1 to 10.3.

For 9.3.5

Left digit: 9
This number increases when a fundamental or drastic function addition or change is made.
An update with major function changes is called a major version upgrade.

Middle number: 3
Updates that do not change main functions, such as partial function additions or changes and vulnerability countermeasures are called minor version upgrades.

Right digit: 5
Updates that do not add or change functions, such as vulnerability countermeasures are called minor version upgrades or bug fixes.

It is important to update software as a countermeasure against malware, but on the other hand, updating can also affect user-friendliness, remove necessary programs etc. and cause new problems. Another problem could be the update itself failing. To prepare for this possibility, before performing system updates necessary for stable operation or performing OS major version upgrades that affect other software, we recommend that you backup important data and settings information plus research the safety reputation of the new version.

Explanation 2

Is it OK to use an OS that is no longer supported?

Microsoft ended support for Windows XP in 2014, which was a topic reported in the news. After support ends, software patches are not distributed even when vulnerabilities are detected. Also, no new security countermeasures will be added against cyberattacks as they become more sophisticated and ingenious. So this is like storing important information in a safe with only a lock that has widely known methods of unlocking. Even if there is still antivirus software compatible with an OS which is no longer supported, this does not mean that the state of the unsupported OS with unresolved vulnerabilities as described above is safe.

You should avoid using operating systems which are no longer supported at all costs, not only to avoid damage to yourself, but because an infected OS can become an assailant itself.

1-3 Update all devices connected to the network

PCs and smartphones are not the only devices you need to equip with vulnerability countermeasures. In recent years, network devices such as printers, multifunction machines, broadband routers (including wireless LAN access points), network attached storage (NAS) and network cameras (surveillance cameras, webcams) as well as digital consumer electronics such as TVs, HDD recorders and home video game consoles are now all connected to the internet.

Each of these devices is run by embedded software called firmware, which is equivalent to an operating system, and by connecting to the internet, there is a risk that their vulnerabilities will be targeted for attack.

When purchasing and installing equipment connected to the network, read the manual and, **if there is a firmware automatic update setting, you should set it to on. Also, if there is no automatic update option, you should periodically check the manufacturer's website for updates (vulnerability countermeasures).**

Example ❶

Damage due to network equipment misconfigurations and vulnerabilities

Starting around 2014, there have been increased incidents of exploiting vulnerabilities in surveillance cameras and network cameras (including webcams) and stealing camera images through unauthorized access. In January 2016, a website was discovered that published footage stolen from surveillance cameras from around the world, which became a big topic in newspapers and news.

Also, in May 2016, Trend Micro reported the existence of ransomware that exploited vulnerabilities in network connected TVs and disabled them.

1-4 Update applications

Software running on the OS which is used for the purpose of specific work is called application software, which includes web browsers, word processors and spreadsheets. Also, on smartphones, it has become common to abbreviate this to “app.” Malware that exploits vulnerabilities in these applications is extremely abundant, and there have been many reports of attacks on commonly used applications, especially web browsers (such as internet Explorer and Google Chrome), Adobe Flash Player, Adobe Reader, Java (Java Runtime Environment) and Microsoft Office. As will be described later in Countermeasures 3 “Web” and Countermeasures 4 “Email,” the risk of malware infections can be greatly reduced by utilizing application vulnerability countermeasures. **Applications used by many people, such as web browsers are especially prone to malware attacks, so you should try to automatically update them as much as possible.**

Regularly update apps on iOS and Android to keep them up-to-date.

1-5 Only install software that can be trusted

Refrain from carelessly installing untrustworthy software onto PCs and smartphones. You should choose software with a clearly identified manufacturer or high user ratings, and only install what you need.

Trustworthy software sources

■ **PCs**

Windows Store, Mac App Store, commercial packages at retailers, freeware such as Windows Forest and Vector

■ **Smartphones and tablets**

App Store, GooglePlay

You should only get software from reliable sources and check the manufacturer and user ratings.

Most malware targeting smartphones urges the user to install it while concealing that it is malware. There are more cases of users being seduced by advertisements such as “lengthen battery life” and “free antivirus software” than with PCs.

Also, **it is dangerous to change the initial setting that disallows app installations from unknown sources, as well as modding (so-called rooting or jailbreaking), so you should ensure to avoid doing that.**

Ref: G DATA Software AG, G DATA による2015年マルウェア動向予測(G DATA Software AG, G DATA 2015 Malware Trends Forecast)[2]
http://gshop.g-wise.co.jp/blog/presscenter/マルチターゲット型スパイウェアにより企業情報.html

Ref: How do you know if your smartphone has been compromised?
https://www.welivesecurity.com/2015/12/16/know-smartphone-compromised/

Ref: Kaspersky Rooting and Jailbreaking: What Can They Do, and How Do They Affect Security?
https://usa.kaspersky.com/blog/rooting-and-jailbreaking/1979/

[2] This website is Japanese only.

Tips 3

Understand that there is still a risk of infection

Attacks that take place during the period between when new vulnerabilities are discovered, or new methods of attack, and when manufacturers implement countermeasures are called “0 day attacks,” and these attacks are extremely difficult for end users to protect themselves against.

Information on threats due to serious vulnerabilities and emerging techniques can be obtained from sources such as news on the internet, alert emails from registered services and sites that issue security information. You should periodically review this information and respond quickly.

Ref: IPA/ISEC, IT Security Center
https://www.ipa.go.jp/security/english/index.html

Tips 4

Keyloggers

Software and hardware that records input data (logging) are known as keyloggers. Not all keyloggers are viruses; they are also used for applications like data backups, monitoring and evidence management and parental controls. However, malicious keyloggers that are designed to steal information exist on the internet. In some cases, malicious keyloggers are used to commit crimes by stealing information such as IDs, passwords and credit card numbers which are input through the keyboard of a PC with the keylogger installed. There are also keyloggers which target the clipboard as well as keyloggers which are connected in the space between the PC and the keyboard.

As a countermeasure against keyloggers, some online banking and e-commerce websites have prepared software keyboards. Make sure to use them as much as possible.

Ref: Trend Micro is702, “ネットバンクの預金残高が0に！新手のデジタル空き巣(Net Bank’s account balance is 0! New digital empty nest)”[3]
https://www.is702.jp/column/402/

[3] This website is Japanese only.

Explanation 3

Ransomware

A type of malware that demands a ransom is known as ransomware. Ransomware can lock the PC it infects and can lock files on the computer and on the network. Paying the ransom is demanded in order to open and unlock the PC and files.

Even when this demand is met, there are many cases where the data is not returned, and giving money to the criminals is linked to the birth of new forms of malware and crime, so by no means should one ever pay this ransom. **Regularly back up important data as a precaution against malware infections.**

Ref: TREND MICRO, Ransomware
https://www.trendmicro.com/vinfo/us/security/definition/RANSOMWARE

Countermeasures 2 IDs and passwords

Various services perform identity verification with a combination of ID and password. ID and password authentication operate the same way as credit card and bank account PINs, under the assumption that “only the person in question knows the password,” so if an attacker knows your ID and password, they can steal your information and money and injure a third party while impersonated as you. It’s important to properly manage your ID and password to avoid this kind of situation.

Here we will explain how IDs and passwords are leaked and countermeasures for this.

6 key points related to IDs and passwords

- 2-1 Never tell your password to anyone
- 2-2 Use strong passwords
- 2-3 Do not reuse passwords
- 2-4 Do not store unaltered passwords directly in password management tools
- 2-5 Use multi-factor authentication (MFA)
- 2-6 Check login history and change notification emails

2-1 Never tell your password to anyone

Your passwords for using online services should be known only by you. **Nobody should ever ask for your password, not even systems administrators. Be suspicious of fraud if you are asked for your password.**

Tips 5

Social Engineering

Social engineering is a criminal technique used to steal IDs and passwords, and without using ICT mechanisms. It involves skillfully taking advantage of your psychological weak spots and behavioral mistakes. Pay lots of attention towards this sort of trick.

＜Social engineering examples＞

● Asking for your password on the phone while pretending to be a systems administrator
● Watching the keys you type in (shoulder hacking)
● Rummaging through trash cans (trashing)
● Trespassing in a building

Ref: Ministry of Internal Affairs and Communications, 国民のための情報セキュリティサイト「ソーシャルエンジニアリングの対策」(“Social engineering countermeasures” information security site for citizens)[4]
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/business/staff/12.html

[4] This website is Japanese only.

2-2 Use strong passwords

Passwords can be thought of in terms of “strength.” “Strong” means “hard to guess.” For example, suppose you have a password which is a 4 digit number. Depending on the situation, in the computer world, this can be guessed in a manner of seconds.

Points when setting a password

● Easy to remember
● Do not use dictionary words or proper nouns
● Use at least 8 characters (about 12 characters is recommended)
● Combine uppercase, lowercase, number and symbol characters
● Use conversion rules and anagrams

It is very dangerous to use numbers related to you or your family’s names or personal information (such as date of birth, phone number or anniversary). You should not carelessly use personal information for passwords, especially as there have been growing numbers of cases where passwords have been guessed from the social media of an individual or persons familiar to them.

If you use words from names or dictionaries, make them hard to guess by changing parts of them to numbers or symbols. You should create strong passwords by referring to websites that have password strength checkers and tips on how to create strong passwords.

Strong password creation example

(1) Think of your favorite English phrase

Don't put all your eggs in one basket.

(2) Use a unique rule to form a string

Dpayeiob ←Formed from the first letter of each word

(3) Replace characters using a unique conversion rule

Dp@yE!06 ←Converted to symbols and numbers resembling "a," "i," "o" and "b"

We do not recommend performing only step (3) on a word from the dictionary to create a password. Character transformations such as "Password" to "P@$$w0rd" can be easily guessed by an attacker.

Ref: Trend Micro, "パスワード(Passwords)"[5]
https://www.is702.jp/column/542/

[5] This website is Japanese only.

In the past, you were encouraged to regularly change your password. But nowadays this is not necessary, and you should use a separate, strong password for each service. The reasoning behind this is that with regular password changes, remembering the password is given priority making them more likely to be predictable, simplified and reused, resulting in them being easily guessed.

Explanation 4

Brute force attacks and dictionary attacks

Weak passwords can be stolen through attacks called brute force attacks and dictionary attacks. Just as the names suggest, these attacks systematically test out combinations of words and characters, and are extremely dangerous for weak passwords.

2-3 Do not reuse passwords

Even if your password management is perfect, if a service you use has a vulnerability, your ID and password may be stolen and leaked. In this case, what if you use the same password with other services? There is a high chance that your ID and password can be used to illegally log into not just the service they were leaked from, but also into other service where you use the same ID and same password. **To avoid this kind of secondary damage, do not reuse your password.**

Explanation 5

Account list attacks

Account list attacks (also called password list attacks, list account hacking, and list attacks) are attacks where an assortment of IDs and passwords obtained through means such as hacking are tried on a variety of services. The more people reuse their passwords, the more damage is done. In 2014, an outbreak of incidents was widely reported about LINE accounts being taken over, messages sent to friends asking to "purchase a prepaid card for me," and then converting the acquired prepaid card into money. These takeovers are said to be due to an account list attack.

Also, do not set passwords by using the same password and adding the service name to the end. For example, say that a person whose Google password is "pass-google" has their password stolen by an attacker. Facebook passwords of "pass-fb" or "pass-Facebook" would be caught by account list attacks and password list attacks.

TrendMicro, アカウントリスト攻撃(Account list attacks)[6]
http://www.trendmicro.co.jp/jp/security-intelligence/threat-solution/access/index.html

[6] This website is Japanese only.

2-4 Do not store unaltered passwords directly in password management tools

The more services you use on the internet, the more accounts and passwords you need to manage. What's the best way to manage these IDs and passwords? Popular management methods are to write them in a notebook, store them in an encrypted (password protected) Word or Excel document, record them in a PC password management tool (which only uses local device storage) and record them in a smartphone application password management tool (which only uses local device storage). Nowadays, there are password management services which use cloud services and can be commonly used in all login situations.

Advantages and disadvantages of these password management methods are as follows.

Password management examples and points

Write them in a notebook

○ Not affected by internet attacks or vulnerabilities

POINT

- ●Periodically make copies in case it goes missing
- ●Do not carry it around with you because you could lose it
- ●Write them in such a way that it is difficult to see the relationship between service, ID and password
- ●Store in a locked location
- ●When reading it, make sure nobody else can see

Record in a password protected Word or Excel document

○ You only need to memorize one password

✕ Low portability compared to smartphones

POINT

- ●So that other people cannot open it, click [Protect Document]→[Encrypt with Password]
- ●To prevent peeking, change the password font color to something that is hard to understand at a glance such as grey
- ●In case of loss, make a backup in external storage which is not accessible to anyone else

Use a PC password management tool (which only uses internal device storage)

○ You only need to memorize one password

× Low portability compared to smartphones

POINT ● In case of loss, make a backup in external storage which is not accessible to anyone else

Use a smartphone app password management tool (which only uses internal device storage)

○ You only need to memorize one password

POINT ● In case of loss, make a backup in external storage which is not accessible to anyone else

Use a password management system which uses a cloud service

○ You can use it in various situations on PCs and smartphones and only need to remember one password

× It is difficult to ascertain service quality (security, continuity)

POINT ● In case of loss, make a backup in external storage which is not accessible to anyone else

Regardless of your password management method, for optimal management **do not write your password as it is.** For example, if you use a password creation method such as the one offered as an example previously in “use strong passwords,” you might want to enter “basket” into the password management tool. Because the method of converting from this to your password is stored only in your mind, there is no problem even if your password management tool’s data is leaked. To reiterate, **accounts should be managed like this with password management tools if there are too many to remember, and it is important that they are not stored in unaltered form in the password management tool.**

Tips 6

Be careful with automatic password input functions

Web browsers include password management functionality. These convenient functions store IDs and passwords when they are entered into a web site once, ask the user for confirmation, then save the credentials and automatically enter them each time the web site is accessed again in the future.

Here you should pay attention to where the saved IDs and passwords are stored and how they can be viewed. Never locally store credentials on devices such as PCs and smartphones which may be used by other people.

Up to now, there has been no problem with web browsers storing passwords on the PCs which they are running on. However, recently, web browsers such as Edge, Chrome, Safari (iCloud keychain) and Firefox sync with cloud services to share password information across multiple devices such as PCs and smartphones, which is convenient on one hand, but also makes it difficult to understand where the password information is stored and how it is managed. Do not use them without a clear understanding of where the password information is stored and how it can be used.

Tips 7

Be careful with ID collaborative trust frameworks

ID collaborative trust frameworks are efforts to link ID and personal information across different services. There are various services which link IDs in this way, and one especially well known one is social login. Social login is a service which can register accounts with and log you into a service unrelated to Google, Facebook or Yahoo! using your Google, Facebook or Yahoo! account. By linking the service with an account such as a Google account, this shares personal information associated with the user’s Google account, creates an account for the appropriate service and allows the user to login afterwords using their Google account so the user does not have to memorize a new ID and password, making this a very convenient function.

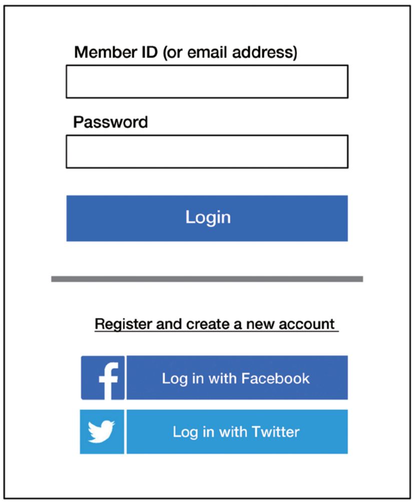

Member ID (or email address)
Password
Login
Register and create a new account
Log in with Facebook
Log in with Twitter

Figure 2 Social login example

There are also methods to fake these social logins to steal accounts. When linking your ID, verify that the service is trustworthy and stop using the service if it is poorly known.

Ref: JPCERT, alert “SNS やクラウドサービスで連携されるアカウント情報には細心の注意を(Pay close attention to account information linked to social media and cloud services)”[7]
https://www.jpcert.or.jp/pr/2015/pr150005.html

[7]This website is Japanese only.

2-5 Use multi-factor authentication (MFA)

In recent years, a technique called “multi-factor authentication” (MFA) has spread, which involves a combination of factors other than ID and password for identity verification, such as a previously distributed table of random numbers, telephone call (voice guidance), SMS, smartphone app, finger, vein matching or facial recognition. Multi-factor authentication uses two or more of the factor types, “something you know (such as a password),” “something you have (such as a smartphone, IC card or table of random numbers)” and “something you are (fingerprint, vein, iris, face),” and if one of these is disrupted, the service will be unavailable.

For example, if you are using a web service, it may request for you to enter a code sent by SMS to a cellphone or smartphone in addition to ID and password at login, and there are services such as online banking which verify identity by asking you to enter a code created by a one time code generator app on a smartphone.

This can prevent many information incidents from occurring due to password or smartphone theft. If a trustworthy service offers multi-factor authentication and asks for you to enter your phone number, you should proactively use this feature.

2-6 Check login history and change notification emails

Starting with Google, Microsoft and Yahoo!, many services now let you check your login history. Login history contains login dates and times, device information, logins and their position information. If your account is stolen and used, unusual history will be left behind, so you should periodically check the login history. Especially if you live in Japan but there is a history of logins from foreign countries, or if a login is recorded from an unfamiliar device, there may be an extremely high chance that your ID and password have been stolen. Also, there are services that automatically detect these kinds of suspicious logins and send notifications by email and SMS.

Also, when you change an account’s information or password, a change notification email is sent to the registered email address. If you are notified of a change you have no knowledge of, it is very likely that your ID and password have been stolen.

If this shows **suspicious logins or changes, immediately change your password and report this to the service provider.**

Countermeasures 3 Web

The “World Wide Web” (or “web”) and email are well-known internet services. Malware uses the “web” and “email” as routes of infection. The “web” is a structure for publishing and sharing documents (web pages) which are linked together.
A collection of web pages is called a “website” (in Japan this is also known as a home page). The web used to only include information and search engines, but before long there were many developments on the web, and now it is responsible for a wide variety of life services (web services) such as maps, reservations, shopping and banking. Because it accounts for a majority of services on the internet, some people misunderstand it as being the internet itself. Finally, the applications used for browsing the web are known as “web browsers.” Commonly used browsers include Microsoft’s Internet Explorer and Edge, Google Chrome, Apple’s Safari and Firefox, which is made by the non-profit community Mozilla.

This has caused the web to offer many services and become convenient. On the other hand, attack methods have also become sophisticated, with falsified websites (such as those with embedded mechanisms to infect with malware), websites where users can be infected with malware just by browsing them and advertisements which can infect with malware when they pop up.

Here we introduce threats surrounding the web and explain their countermeasures.

Furthermore, staff responsible for managing the web should follow “The Ritsumeikan Trust Information System Application Management Regulations[8]” and related guidelines.

[8] This English document is a translation of the original Japanese document and is for reference only.

6 key points regarding the web

- **3-1** Perform malware countermeasures
- **3-2** Do not carelessly relax the browser's security functions
- **3-3** Always scan downloaded files
- **3-4** Make sure the website is genuine
- **3-5** Be aware that many websites and advertisements are scams
- **3-6** If you are concerned about something, run a scan

3-1 Perform malware countermeasures

An attacker's primary objective is to infect a PC with malware using websites and email. **It is important to first perform malware countermeasures for safe browsing.** Please thoroughly read through Countermeasures 1 "Malware (viruses)" and perform countermeasures.

Also, the OS and antivirus software has antivirus functions specialized for websites.

For example, Windows 10 operates a function called SmartScreen by default. It has functions to prevent accessing malware-infected websites (only works on Internet Explorer and Edge) and automatically scan downloaded files (such as with Chrome), so you shouldn't disable it.

Also, commercial antivirus software contains website evaluations (web reputation), intrusion prevention systems (IPS), and behavior patterns of programs which operate through web browsers (behavior detection) to detect dangerous websites and are equipped with functions to protect the user from accessing them. You might want to use antivirus software with these features.

Explanation 6

The threat of exploit tools (kits)

Exploit tools (kits) are tools that can be planted in a website and can infect a PC with malware just by browsing the website. Exploit tools (kits) are not only installed on websites administered by the attacker, but can be arbitrarily planted in attacked websites and can be mixed in among web advertisements, displaying links that direct the user to another party's website (advertising attacks), making them very dangerous. Furthermore, this type of tool is sold over the internet, and increasingly dangerous websites are expected to increase from now on.

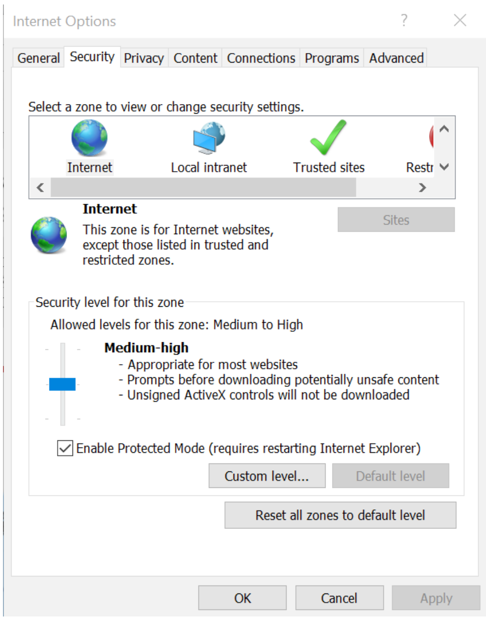
Exploit tools (kits) can infect with malware if there is even just one vulnerability in susceptible software (such as the web browser, Adobe Flash Player, Java, Adobe Reader or Microsoft Office), so thoroughly perform vulnerability countermeasures on all software you are using, starting with the OS.

Ref: Kaspersky, What are exploits and why they are so scary?
https://usa.kaspersky.com/blog/loits-problem-explanation/5719/

3-2 Do not carelessly relax the browser's security functions

Modern web browsers are equipped with website antivirus functions by default, and there are increasing cases where they have prevented access to dangerous sites and the download of dangerous files. **If the web browser produces a warning, you should look up what kind of warning it is before taking action.**

Also, because the web browser security functions are strict, some websites will not work properly. Because the web browser settings are initially set to the manufacturer's recommended settings, if a website does not work properly, **do not carelessly relax entire security functions. If absolutely necessary, you should make security setting adjustments limited only to that website.** Generally, websites that do not work properly due to web browser security measures publish the setting method in their FAQ section, so you should search there.



Select a zone to view or change security settings.

Internet
This zone is for Internet websites, except those listed in trusted and restricted zones.

Security level for this zone
Allowed levels for this zone: Medium to High

Medium-high
- Appropriate for most websites
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded

☑ Enable Protected Mode (requires restarting Internet Explorer)

Figure 3 Web browser settings (Internet Explorer 11)

3-3 Always scan downloaded files

You should suspect that files you obtain over the internet may be infected with malware. **Antivirus software should scan files that are downloaded from websites.** For applications (apps) you intend to install on your PC or smartphone in particular, you should not only scan them but also check to make sure that the distribution source and manufacturer is trustworthy.

If you have Windows 10 and the above-mentioned SmartScreen is left enabled, it will automatically scan. Also, because encrypted files such as password-protected Zip files cannot be scanned while they are encrypted, you should scan them after decryption.

3-4 Make sure the website is genuine

A common trick is to send an email impersonating a financial institution or shopping site, leading to a website where an ID, password and credit card number are entered; spoofed sites prepared by attackers are extremely elaborate and difficult to distinguish from legitimate sites. You should make sure that the URL is not different from usual, and if it is a financial institution or similar then a “green bar” should be displayed.

Explanation 7

Green bar

In some cases, you obtain a digital certificate to prove that the website is legitimate. For sites like financial institutions, the address bar displaying the URL sometimes displays a padlock icon and green, which is called a “green bar.” This involves a stricter review than for digital certificates used primarily for encryption, and is issued by the digital certificate issuing authority only after proving that the business actually exists. This guarantees that the business is credible, the URL is legitimate and there is encryption.

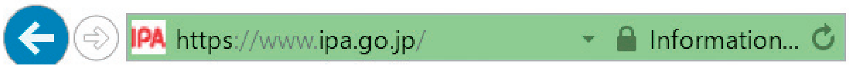


Figure 4 Green bar example (Internet Explorer 11)

3-5 Be aware that many websites and advertisements are scams

Techniques to manipulate website users, infect with malware and demand money become more sophisticated every day.

For example, some will display fraudulent advertisements disguised as system warnings, such as “malware detected,” “your PC is running slowly” and “crash imminent.” If clicked on, they will display further anxiety-inducing messages, leading the user to install or purchase antivirus, performance improvement or repair software (containing malware). Similar advertisements include “improve PC speed” and “improve smartphone battery life,” which take advantage of a sense of inconvenience that many users feel. Because this kind of software is often malware, you should thoroughly read through Countermeasures 1 “Malware (viruses)” and only use trustworthy software.

Also, if you see these types of displays when browsing any website or even when not using a web browser, you have likely been infected with a type of malware (adware).

A typical way of demanding money is one-click fraud. One-click fraud displays a message such as “Membership registration completed” when a link is merely clicked on, displays specific personal information, such as mobile phone or smartphone model or IP address, fabricates an illegal billing charge and shows threatening messages like “or we will go to your residence and office for collection” to stir up a sense of anxiety. Recently, a variant called “zero click fraud” has been discovered on adult video websites. To form a contract on the website, it is necessary to “confirm the purpose of use” after “the amount of money is displayed.” If there is no such indications, the contract is not concluded. You should ignore it or consult a consumer center (consumer hotline: no area code 188).

Ref: Tokyo, 東京くらしWEB警告表示をして、セキュリティーソフトを購入させる詐欺広告に注意(Tokyo Life WEB Beware of warning displays leading to fraudulent ads to buy security software)[9]
http://www.shouhiseikatu.metro.tokyo.jp/trouble/trouble25-sagiadvertisement-140106.html

Ref: Ministry of Internal Affairs and Communications, 国民のための情報セキュリティサイト「ワンクリック詐欺に注意」(“Beware of one-click fraud” information security website for citizens)[10]
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/security01/06.html

[9,10] This website is Japanese only.

3-6 If you are concerned about something, run a scan

As mentioned above, websites with tempting content such as adult, dating, investment and predatory business websites often include one-click fraud and exploit tools (kits).

However, even with websites that are not malicious, there are cases where attacked websites can be sources of infection, making it extremely difficult to judge whether they are safe or dangerous.（Ref: Explanation 6 “The threat of exploit tools (kits)”)

Repeating what has already been explained in Countermeasures 1 “Malware (viruses),” it is important to update the OS and applications, install antivirus software and take care to run scheduled scans and scans during downloading so that PCs and smartphones are not easily infected by malware. **If you are concerned about something, such as if you are lead to a suspicious website or see unusual displays or warnings on the screen, you should scan your entire PC or smartphone.**

Countermeasures 4 Email

Like with the 2015 Japan Pension Service information leak incident, many recently reported information leak incidents were caused by “having opened an attachment” or “having opened an included link.” These sorts of emails have become increasingly ingenious, and it has become difficult to determine if an email is malicious.

Also, there are incidents where confidential information is leaked through simple communications sent in error. Email has become established as a social telecommunications infrastructure and is used more frequently than telephone calls, but is also a communication tool where we need to be extremely careful about information incidents.

Here we introduce threats surrounding email and explain their countermeasures.

7 key points regarding email

- **4-1** Set a spam email filter for unsolicited emails
- **4-2** Be careful with attached files and links
- **4-3** Beware of scams and phishing
- **4-4** Beware of targeted cyberattacks
- **4-5** Understand points for recognizing suspicious emails
- **4-6** Beware of sending email incorrectly
- **4-7** Do not include highly confidential information

4-1 Set a spam email filter for unsolicited emails

If you use email over many years, you will inevitably receive unsolicited spam emails. Most email systems have spam email filter functions which prevent spam email from being delivered. However, these filters cannot reliably distinguish only the emails the user needs from the large numbers of email that flows through them, and there are cases where malicious email is delivered to the user’s inbox as well as cases where essential emails are delivered to the spam email folder.

To begin with, you should check if the email system you are using has a spam email detection function, and whether this toggled ON from your settings. Also, you should make a habit of periodically checking the spam email folder to make sure that necessary emails were not delivered to the spam email folder.

Ref: Spam email consolation center, “迷惑メール対策をはじめましょう(Let’s start with anti-spam measures)”[11]
http://www.dekyo.or.jp/soudan/taisaku/

[11] This website is Japanese only.

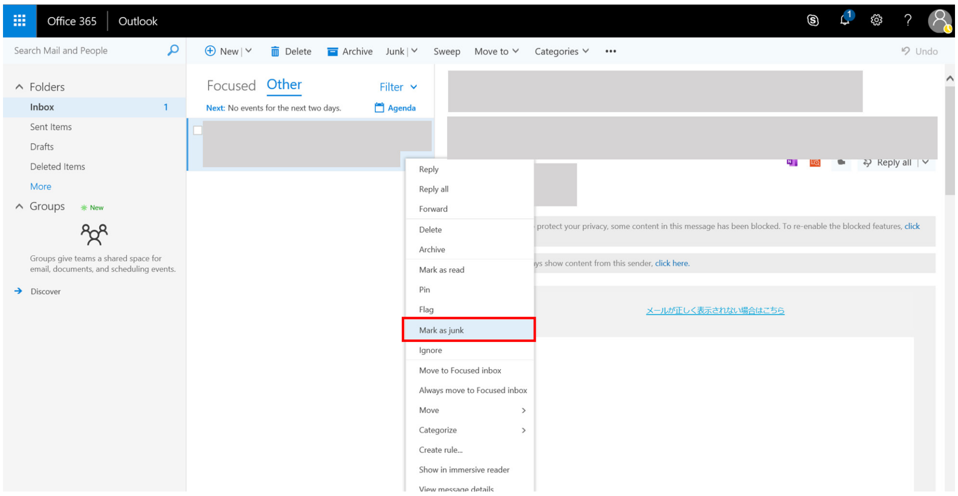
Tips 8

Spam email reporting

Modern email systems have “spam email reporting” functions. Conversely, they also have “misdetection reporting” functions. Because these reports analyze spam emails and help teach the engine how to decide, it is good to report as much as possible.

In school email environments, reporting spam email is only possible if Outlook on the web (web email) is used. Select email from the inbox to be marked as spam and perform the below operation.

Right-click→Click on [Mark as junk]



Next: No events for the next two days.

Groups give teams a shared space for email, documents, and scheduling events.

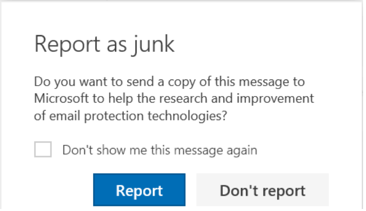
protect your privacy, some content in this message has been blocked. To re-enable the blocked features, click

ys show content from this sender, click here.

メールが正しく表示されない場合はこちら

Figure 5 Mark as junk

When a confirmation window appears, click [Report].



Report as junk

Do you want to send a copy of this message to Microsoft to help the research and improvement of email protection technologies?

□ Don't show me this message again

Figure 6 Spam email report

After reporting the spam email, move it to the spam email folder.

On the other hand, if you want to report misdetection, right-click on email caught by the spam email filter and click [Mark as not junk], or click on [It's not spam] which is displayed over the email text.

4-2 Be careful with attached files and links

Cases where malware infections come from email include cases where malware attached to the email is opened by the recipient, leading to infection, and cases where the recipient accesses a website from a URL included in the text of the email (including links in HTML emails), leading to infection. There are also cases where the recipient accesses a website that asks for their ID and password, which are then stolen.

If you do not want to open a file attached to an email but need to open it, you should save it to your computer and then scan it with antivirus software.

Nowadays there are many services which include URLs in emails, which are difficult to ascertain, so if you have doubts after looking closely at the URL and email content, you shouldn't open them. **It's important to check URLs to see if they are related to the sender.** In HTML emails, beware of link spoofing (where the link is set to direct somewhere other than the displayed URL string). If you don't know if the URL is legitimate, it is safer to follow a path for reliably accessing legitimate sites such as with bookmarks or search engines.

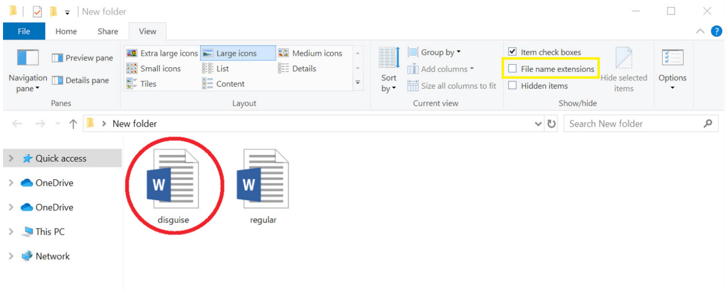
If you accidentally open an attached file or follow a link, it is still possible to avoid infection if you follow the countermeasures in Countermeasures 1 "Malware (viruses)." It is important to create an environment which cannot easily be infected by malware. Especially if using an email client such as Outlook, Thunderbird or Apple Mail, there is malware which takes advantage of mail client vulnerabilities, so you should constantly update your client.

Explanation 8

Icon Spoofing

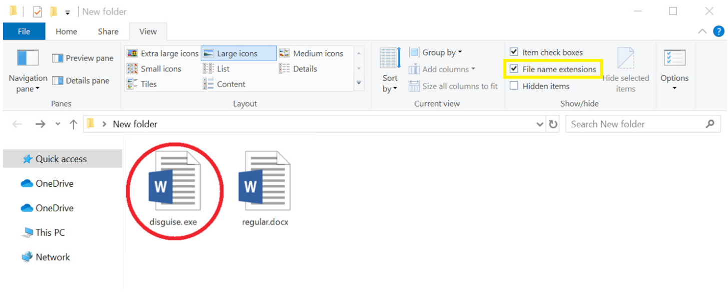
This is a technique where attached malware imitates Office document and PDF icons. Because there are many users who judge filetypes based on only the icon, this misrecognition can lead them to executing the malware.

On the other hand, because the OS uses a character string called a file extension which indicates file type (such as .docx, .pdf, .jpg or .exe appended to the end of a file) to determine what application to open the file with (or whether to execute it directly), you can check if the icon matches the file extension to know if it is spoofed (for example, a file with an image icon but an .exe extension). Because current operating systems disable the display of filename extensions by default, **you should always set filename extensions to display.**



☑ Item check boxes
☐ File name extensions
☐ Hidden items

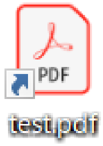
Figure 7 Spoofed icon (filename extension not displayed)



☑ Item check boxes
☑ File name extensions
☐ Hidden items

Figure 8 Spoofed icon (filename extension displayed)

There have recently been a large number of cases of malware infections reported that entail a derivation of icon spoofing. In such cases, a shortcut file (.lnk, .url) is attached which redirects the user to a malware infested website or executes an embedded program when clicked on. Shortcut files do not show file extensions when scanned or saved to the PC. To recognize them, make sure the icon does not have an “arrow” like the one shown on the right.



Ref: IPA/ISEC in JAPAN, virus and UCA incident report for October2011
https://www.ipa.go.jp/security/english/virus/press/201110/E_PR201110.html

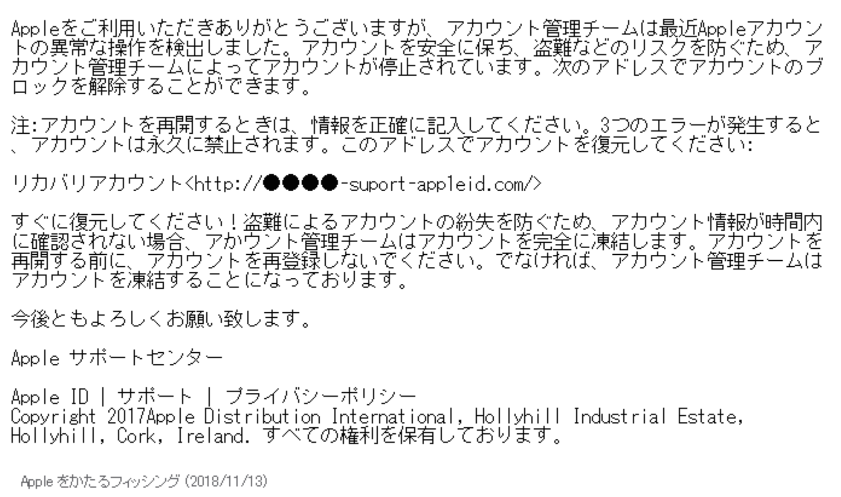
4-3 Beware of scams and phishing

Many spam emails (malicious emails) are sent to a large unspecified number of people and used to directly draw people into a scam, such as with false invoices in the text of the email, requesting a reply posing as an acquaintance or a member of the opposite sex seeking an encounter and stating that the recipient has won some sort of highly valuable prize. **It is important to first check the sender and evaluate whether or not the other party is trustworthy.** You should be very careful not to contact people you don’t recognize and to not be easily lured.

Phishing is a type of fraud where a user is guided to a fake website under the guise of a real public institution or financial institution, where the user inputs their credit card number or ID and password which is then stolen. In addition, there is an increasing number of phishing cases misrepresenting themselves as famous services such as shopping sites and online auction sites. In addition, every year it becomes more difficult to recognize suspicious emails.

Phishing email example 1 “Apple impersonation phishing”

Email content



Appleをご利用いただきありがとうございますが、アカウント管理チームは最近Appleアカウントの異常な操作を検出しました。アカウントを安全に保ち、盗難などのリスクを防ぐため、アカウント管理チームによってアカウントが停止されています。次のアドレスでアカウントのブロックを解除することができます。

注:アカウントを再開するときは、情報を正確に記入してください。3つのエラーが発生すると、アカウントは永久に禁止されます。このアドレスでアカウントを復元してください:

リカバリアカウント<http://●●●●-suport-appleid.com/>

すぐに復元してください！盗難によるアカウントの紛失を防ぐため、アカウント情報が時間内に確認されない場合、アかウント管理チームはアカウントを完全に凍結します。アカウントを再開する前に、アカウントを再登録しないでください。でなければ、アカウント管理チームはアカウントを凍結することになっております。

今後ともよろしくお願い致します。

Apple サポートセンター

Apple ID | サポート | プライバシーポリシー
Copyright 2017Apple Distribution International, Hollyhill Industrial Estate, Hollyhill, Cork, Ireland. すべての権利を保有しております。

Apple をかたるフィッシング (2018/11/13)

© Council of Anti-Phishing Japan

Reference Translation

Thank you for using Apple. Our account management team has detected recent abnormal activity with your Apple account. In order to secure your account and avoid the risk of theft, our account management team has suspended your account. You can release the block on your account at the following address.

Note: When restoring your account, please enter the correct information. If three errors occur, your account will be permanently banned. Please restore your account at this address:

Recover Account <http://●●●●-support-app1eid.com/>

Please restore immediately! To prevent account loss due to theft, our account management team will completely freeze the account if your account information is not confirmed in time. Before your account is reopened, please do not register another account. Otherwise, our account management team will freeze the account.

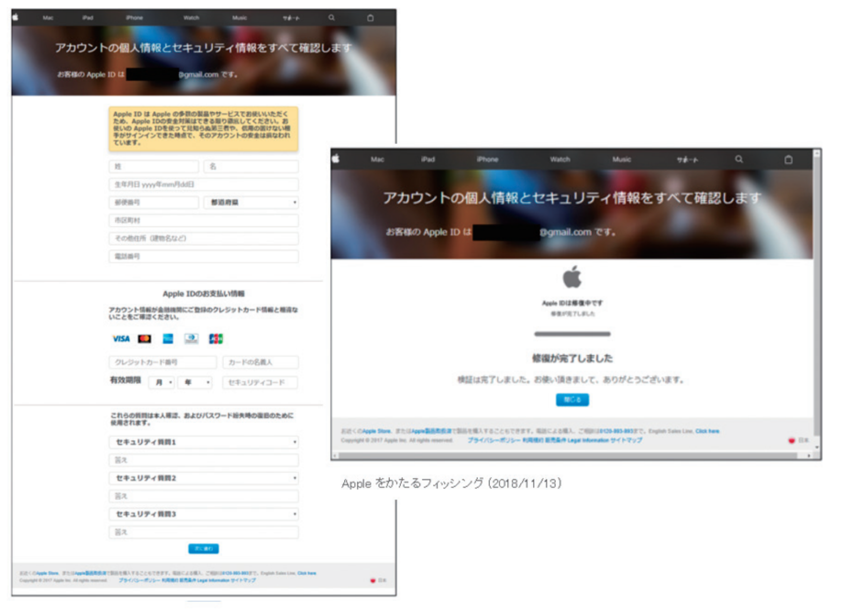
Thank you for your continued support.

Apple Support Center

Apple ID | Support | Privacy Policy
Copyright 2017 Apple Distribution International, Hollyhill Industrial Estate, Hollyhill, Cork, Ireland. All rights reserved.

Figure 9　Example 1　Email content

Linked website



アカウントの個人情報とセキュリティ情報をすべて確認します

お客様の Apple ID は [redacted]@gmail.com です。

Apple ID は Apple の多数の製品やサービスでお使いいただくため、Apple IDの安全対策はできる限り強化してください。お使いの Apple IDを使って見知らぬ第三者や、信用の置けない相手がサインインできた時点で、そのアカウントの安全は損なわれています。

姓
名
生年月日 yyyy年mm月dd日
郵便番号
都道府県
市区町村
その他住所（建物名など）
電話番号

Apple IDのお支払い情報

アカウント情報が金融機関にご登録のクレジットカード情報と相違ないことをご確認ください。

クレジットカード番号
カードの名義人
有効期限 月 年
セキュリティコード

これらの質問は本人確認、およびパスワード紛失時の復旧のために使用されます。

セキュリティ質問1
答え
セキュリティ質問2
答え
セキュリティ質問3
答え

お近くのApple Store、またはApple製品取扱店で製品を購入することもできます。電話による購入、ご相談は0120-993-993まで。English Sales Line, Click here
Copyright © 2017 Apple Inc. All rights reserved. プライバシーポリシー 利用規約 販売条件 Legal Information サイトマップ
日本

アカウントの個人情報とセキュリティ情報をすべて確認します

お客様の Apple ID は [redacted]@gmail.com です。

Apple IDは修復中です
修復が完了しました

修復が完了しました

検証は完了しました。お使い頂きまして、ありがとうございます。

閉じる

お近くのApple Store、またはApple製品取扱店で製品を購入することもできます。電話による購入、ご相談は0120-993-993まで。English Sales Line, Click here
Copyright © 2017 Apple Inc. All rights reserved. プライバシーポリシー 利用規約 販売条件 Legal Information サイトマップ
日本

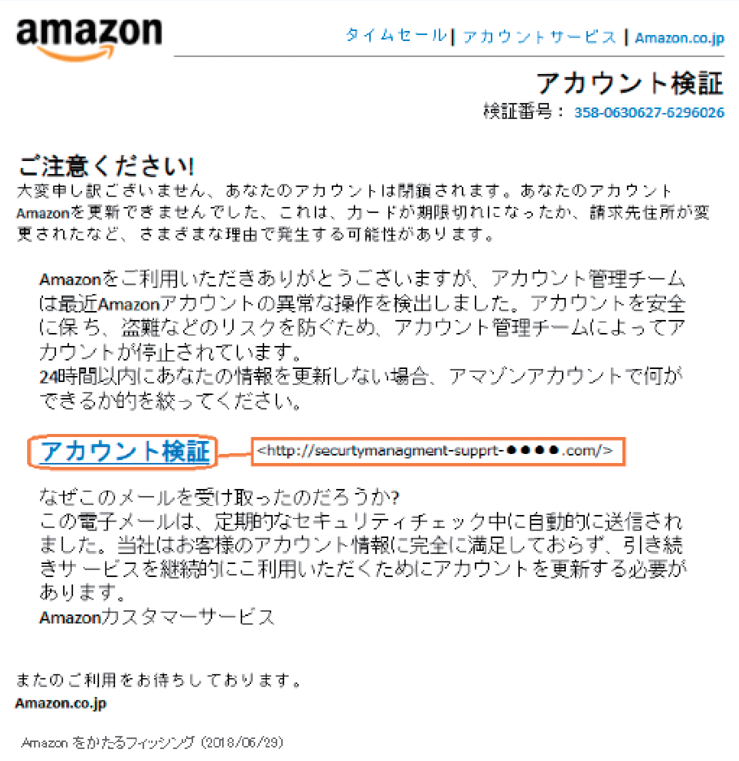
Apple をかたるフィッシング（2018/11/13）

© Council of Anti-Phishing Japan

Figure 10 Example 1 Linked website

Phishing email example 2 “Amazon impersonation phishing”

Email content



タイムセール | アカウントサービス | Amazon.co.jp

アカウント検証

検証番号： 358-0630627-6296026

ご注意ください!

大変申し訳ございません、あなたのアカウントは閉鎖されます。あなたのアカウントAmazonを更新できませんでした、これは、カードが期限切れになったか、請求先住所が変更されたなど、さまざまな理由で発生する可能性があります。

Amazonをご利用いただきありがとうございますが、アカウント管理チームは最近Amazonアカウントの異常な操作を検出しました。アカウントを安全に保ち、盗難などのリスクを防ぐため、アカウント管理チームによってアカウントが停止されています。
24時間以内にあなたの情報を更新しない場合、アマゾンアカウントで何ができるか的を絞ってください。

アカウント検証 <http://securtymanagment-supprt-●●●●.com/>

なぜこのメールを受け取ったのだろうか?
この電子メールは、定期的なセキュリティチェック中に自動的に送信されました。当社はお客様のアカウント情報に完全に満足しておらず、引き続きサービスを継続的にこ利用いただくためにアカウントを更新する必要があります。
Amazonカスタマーサービス

またのご利用をお待ちしております。
Amazon.co.jp

Amazon をかたるフィッシング (2018/06/29)

© Council of Anti-Phishing Japan

Reference Translation

Account verification
Verification number: 358-0630627-6296026

Please be careful!

We are sorry to inform you that your account has been locked. We could not update your Amazon account, which could have happened for a variety of reasons including an expired credit card or change of billing address.

Thank you for using Amazon. Our account management team has detected recent abnormal activity with your Amazon account. In order to secure your account and avoid the risk of theft, our account management team has suspended your account.

If you do not update your information within 24 hours, please focus on what you can do with your Amazon account.

Account verification
http://securtymanagment-supprt-●●●●.com/

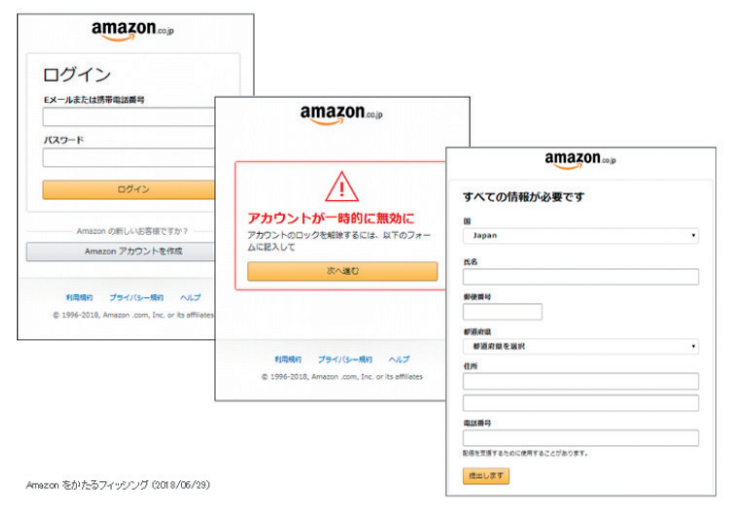
Why did I receive this email?
This email is automatically sent as part of our periodic security checks. We are not completely satisfied with your account information and need to renew your account to continue using our services.

Amazon Customer Service

We look forward to serving you again
Amazon.co.jp

Figure 11 Example 2 Email content

■ Linked website



amazon.co.jp

ログイン

Eメールまたは携帯電話番号

パスワード

ログイン

Amazon の新しいお客様ですか？

Amazon アカウントを作成

利用規約　プライバシー規約　ヘルプ

© 1996-2018, Amazon .com, Inc. or its affiliates

amazon.co.jp

アカウントが一時的に無効に

アカウントのロックを解除するには、以下のフォームに記入して

次へ進む

利用規約　プライバシー規約　ヘルプ

© 1996-2018, Amazon .com, Inc. or its affiliates

amazon.co.jp

すべての情報が必要です

国

Japan

氏名

郵便番号

都道府県

都道府県を選択

住所

電話番号

配信を支援するために使用することがあります。

提出します

Amazon をかたるフィッシング (2018/06/29)

© Council of Anti-Phishing Japan

Figure 12　Example 2　Linked website

Ref: フィッシング対策協議会(Council of Anti-Phishing Japan)[12]
https://www.antiphishing.jp/

[12] This website is Japanese only.

4-4 Beware of targeted cyberattacks

The May 2015 incident where 1.25 million pension information items were leaked from the Japan Pension Service and the June 2016 incident where 7.93 million personal information items were leaked from JTB were widely reported as targeted cyberattacks. “Targeted cyberattacks” (sometimes called simply targeted attacks), such as these two cases are rampant, where specific organizations (or individuals) are targeted to steal money or information.

“Targeted cyberattacks” involve collecting information about the targeted information through websites, social media and telephone (for individuals, information made available especially on SNS is abused. See Countermeasures 8 “personal information and rights infringement”) and emails with attached malware and/or emails with links to websites are sent under the guise of agencies and staff related to the targeted organization. When a system used by a person in the organization is infected with malware, it starts by demanding a ransom with ransomware, steals information in the PC it has a foothold in, looking for IDs and passwords while trying to hack into other PCs in the network, and finally continues attacking to obtain administrator rights on the authentication system and data stored on core systems, making it a terrible situation.

“Targeted cyber attacks” as described above often start with the attacker sending an email with cleverly designed content pretending to be an agency related to the targeted email address; this email is known as the “targeted attack email.” Targeted attack emails are characterized by their ability to target a specific person, making the content more ingenious and difficult to detect. If the target is a faculty member of the university, they could be tricked into confirming the attached file or link destination by giving them the actual department name of a government agency such as MEXT. Many incidents have been caused by such email attacks, and even faculty of this university have reported being led to a website due to a targeted attack email, entering their ID and password and having it misused.

To prevent targeted cyberattacks, it is important that all organization members understand and appropriately respond to this targeted attack email, to prevent creating a foothold for malware infection or account theft. Please be very careful, because there is a risk of endangering the entire school if even one PC is infected.

Targeted attack email example 1 Example from this university

In August 2016, a large number of faculty members received this targeted attack email with an authentication screen and website related to a well-known planned revision of the university email system. Fortunately, no specific damage has been confirmed, but a number of faculty entered their IDs and passwords into the website they were directed to.

差出人：大学のメールアカウントのアップグレード〈helpdesk@sso.ritsumei.ac.jp〉
件名：大学のサポート
文面：

注意

現在、電子メールアカウントのすべてのメンテナンス処理を行っています。
これを完了するには、スパイウェア、スパムメールに対するあなたの
アカウントを確認するために、この電子メールにすぐ返信には、次の
リンクを使用する必要があります。

更新するには、ここをクリックしてください
(実際のスパムメールにはこの部分にURLが記載されています)

このプロセスは、あなたがあなたの電子メールを失うことになる、詳細が
提供してあなたは、上記のリンクを持つアカウントを更新しないと、
私たちは、スパムからあなたの電子メールを保護するのに役立ちます

ご理解をいただき、ありがとうございます。

宜しくお願いします、
メールチーム。
管理サービスチームを占めています。

■ Reference Translation

Sender: University Email Account Upgrade <helpdesk@sso.ritsumei.ac.jp>
Subject: University Support
Content:

Attention

We are currently conducting maintenance on all email accounts. To complete this, you need to use the following link in response to this email so that we can check your account for spyware and spam email.

To update, please click here
(In the actual spam email, a URL is listed here)

In this process, your email account will be lost, but provided that you do not provide detailed information and renew your account with the link above, we will help to protect your email from spam

Thank you for your understanding.

Thank you.
Email team.
Part of the management services team.

Targeted attack email example 2 Example of MEXT impersonation targeting a university

In May 2016, university faculty received this targeted email, and MEXT issued an alert. The attached file is malware, and the sender is using the MEXT domain, but it seems that actually the email was sent through unauthorized access to another email server. The email signature is of an actual MEXT official, and it seems that an email sent by this official in the past was misused.

差出人：kenjo@mext.go.jp　〈*****-saga-saga-saga.com@saga-*****.com〉
件名：【文科省（ご連絡）】新学術領域研究の中間・事後評価について
添付ファイル：中間-事後評価に係る様式20160524.zip

平成26・27・28年度採択研究領域の領域代表者各位

お世話になっております。
○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○

本年度、中間・事後評価のスキームを見直すとともに、
評価報告書の様式の見直しを実施いたしましたので、
来年又は再来年に中間評価又は事後評価を実施することになります
先生方に、本変更点についてご報告させていただきます。
変更点につきましては、添付の事務連絡をご参照ください。

また、
実際の評価時期に作成依頼する際には変更の可能性がございますが、
本年度は使用いたしました様式をご参考までに添付いたします。
特に、今回より追加いたしました別添の"データシート"については、
来年以降は"全研究期間"について記載いただくことを予定しておりますので、
現時点よりデータ収集・整理についてご準備いただけますようお願いいたします。

なお、評価に関する例年のスケジュールは以下のとおりとなっております。
5月半ば　　　評価報告書(添付のもの)の作成を依頼(領域代表者←文科省)
6月半ば　　　評価報告書の提出(領域代表者→文科省)
9月～10月　ヒアリング
12月～1月　評価結果通知
特に、評価報告書の提出時期と、成果報告書(様式C－19及び冊子体の両方)
の提出時期が近接しておりますので、来年は例年5月半ばの作成依頼を早めに行い、
先生方の準備期間に余裕が出るように配慮する予定ではおりますので、
ご対応方よろしくお願いいたします。

今後ともどうぞよろしくお願い申し上げます。

＜本件担当＞

文部科学省研究振興局学術研究助成課
○○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○○

文面：（NHK「かぶん」ブログ http://www9.nhk.or.jp/kabun-blog/200/245719.htmlより）

■ Reference Translation

Sender: kenjo@mext.go.jp <*****-saga-saga-saga.com@saga-*****.com>
Subject: MEXT New academic research interim and post-assessment
Attached file: 中間-事後評価に係る様式20160524.zip

Research area representatives of 2014, 2015, 2016

Thank you.
○○○○○○○○○○○○○○○○○○○○○○○○○○○○○○

This year we reviewed the interim and post facto assessment scheme and revised the format of the assessment report, so next year or the following year we will conduct an interim assessment or post facto assessment.
We would like to inform the teachers about this change.
Please see the attached administrative communication for the changes.

Also, it may be possible to make changes at the actual time of evaluation when this information is requested, but this time it is attached as reference for the style used this year.
In particular, regarding the attached “data sheet” added for this time, we plan the record the “entire research period” for next year, so please be prepared for data collection and organization from now on.

The annual schedule for the evaluation is as follows.
Mid-May: Evaluation report (attached) created (area representative←MEXT)
Mid-June: Evaluation report submitted (area representative→MEXT)
Sept.-Oct.: Public hearing
Dec.-Jan.: Evaluation results posted
In particular, the evaluation report and results report submission times are close (both form C-19 and booklet), so next year we will move the creation request up to mid-May, giving greater consideration to the teachers’ planning period; thank you for your support.

Thank you.

＜Person in charge＞

Academic Research Grant Division, MEXT
○○○○○○○○○○○○○○○○○○○○
○○○○○○○○○○○○○○○○○○○○

Content: (NHK “Kabun” blog from http://www9.nhk.or.jp/kabun-blog/200/245719.html)[13]

[13] This website is currently unavailable.

4-5 Understand points for recognizing suspicious emails

Because targeted attack emails use very clever content so that the recipient does not feel suspicious, they may feel compelled to open attachments such as “Interview requests from newspapers or publishers” and “notifications and alerts from a government office.” **When checking email, if you pay attention to the sender, content and attached files, in most cases, you can prevent accidents, so please check the following points.**

〈Digital signature (proof of secure email)〉

Increasing numbers of organizations, including financial institutions are using digital signatures in emails. Digital signatures are an S/MIME mechanism that signs the email using with a certificate from a certificate authority, guaranteeing that the sender and the signer are the same, and proving that the email is not spoofed.

It is displayed differently depending on the environment in which the email is received (email client, email server), but usually one of the following icons is displayed or a message indicating safety is displayed. In addition, financial institutions etc. that send signed emails publish explanations of their signed emails on their website, so please check it.

E-signature Icon Example

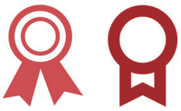


Figure 13 E-signature icon image

Also, in email environments that do not support S/MIME, it arrives as a normal email with an attachment titled “smime.p7s.”

Common characteristics of suspicious emails

〈Sender〉

- Unknown sender
- Known sender, but different from usual email address
- Lack of information on the sender (no name given, no signature)
- Sender uses a free email address (a disposable email address from Gmail or Yahoo! Mail where the organization cannot be determined from the domain name)
- The sender's email address does not match the email address in the signature

〈Letter content〉

- Camouflaged links
- URLs unrelated to the sender
- Uses unnatural expressions
- Contains spelling mistakes
- Tries to get you to do something beyond the content of the text
- Asks for your ID, password, credit card number or personal information
- Stirs up a sense of crisis
- Stresses a sense of urgency such as "Verify immediately!" or "Call right now!"
- Notification of unexpected charge, settlement or delivery
- Executable file attached (with an extension such as .exe/.scr/.cpl)
- Shortcut file attached (with a .lnk/.url extension)
- Spoofed icons
- Unnatural file extensions (such as two layers of file extensions, large numbers of space characters before the file extension)
- Has an inverted extension at the beginning of the file name, such as "fdp.file.scr"→"rcs.elif.pdf" (exploiting a function (RLO control character) for languages like Arabic which are read from right to left)

Ref: IPA, 標的型攻撃メール＜危険回避＞対策のしおり(Targeted attack emails <risk aversion> countermeasures)[14]
http://www.ipa.go.jp/security/antivirus/documents/10_apt.pdf

Ref: IPA, IPTA テクニカルウォッチ「標的型攻撃メールの例と見分け方」(IPTA technical watch "Examples of targeted attack emails and how to identify them")[15]
https://www.ipa.go.jp/security/technicalwatch/20150109.html

[14,15] This website is Japanese only.

Tips 9

Court summons due to false invoices or billing

In targeted cyberattacks, the attacker usually knows personal information such as address and full name. There are techniques where an attacker will send a false invoice through email and then use personal information to actually file a lawsuit. If the accused does not appear in court, the accuser (attacker) wins the lawsuit, thereby using the accused's countermeasure of "ignoring the false invoice" against them. Therefore, if you receive a court summons, please check with the court even if the invoice is false.

Ref: Ministry of Justice, 督促手続・少額訴訟手続を悪用した架空請求にご注意ください(Please be careful with false invoices which abuse the collection procedure and small claims lawsuit procedure)[16]
http://www.moj.go.jp/MINJI/minji68.html

[16] This website is Japanese only.

4-6 Beware of sending email incorrectly

Not all email information leak incidents are due to malicious emails sent to a user, many are due to missending emails.

There are no methods to automatically prevent missending emails, so individual caution is required. In a company, an employee's computer has a sticker that says, "before sending an email, point at the screen and check!"; missending can only be prevented with individual attention. Since it is a tool used every day, it is easy to become negligent as you get used to it, and despite increasing convenience such as smartphone usage, **be aware that slight negligence can lead to accidents. Before sending you should always check all the To, Cc and Bcc addresses to confirm you are not including any addresses you should not be sending emails to.**

Column 1

Don't forward or change senders

Because email is a communication tool that we use on a daily basis, it is natural to want to use it in ways we are used to. For example, there are many faculty members who do not use their organization (university) email and instead forward to their private emails. Since forwarding is considered to be taking out data, organizations with strict security measures prohibit or require approval for this, but this university does not impose regulations with consideration towards convenience for educational research. However, if the email system of the forwarding address has an information incident which is tied to an information leak, the individual is responsible for this.

Recently, as a countermeasure against spam email, sending domain authentication (SPF, DKIM), which checks the source server and sender, is becoming stricter. If you simply forward, important email may not reach your private inbox or may be treated as spam email which can disrupt communication.

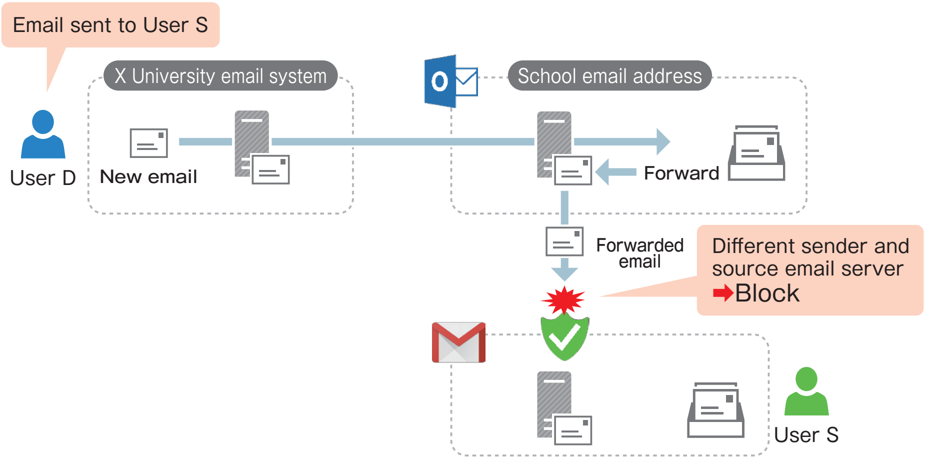


Figure 14 Example of email lost during forwarding

Also, if you want to send a new email or send a reply from the private email address you forward to, you can change the email sender to your school email address before sending. Originally, the email sender could be freely changed because a secretary might want to send it on behalf of the professor or a system uses a representative address for the sender. Using a school email address in a familiar environment (see figure 15), like with forwarding, seems to be practiced by many faculty members, but because this is identical to a malicious attacker's phishing emails and targeted attack emails where the sender is "spoofed" (spoofed email, email spoofing) (see figure 16), these are often judged as spam emails, which is a cause of lost emails.

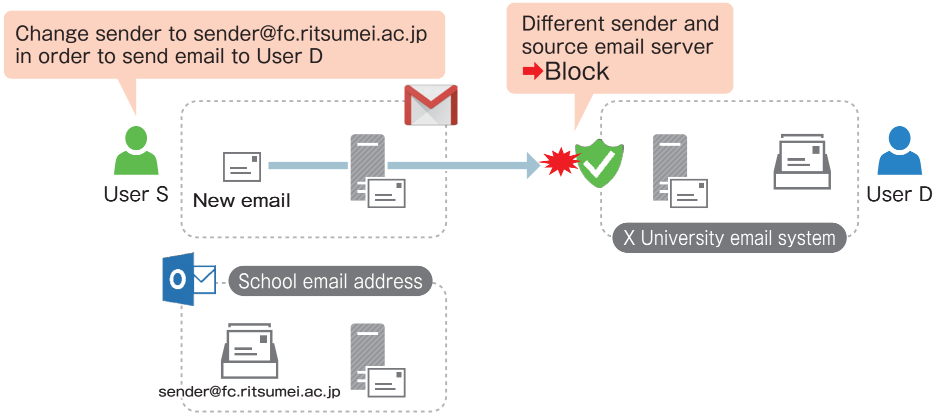

Change sender to sender@fc.ritsumei.ac.jp in order to send email to User D
Different sender and source email server
➡Block
User S
New email
User D
X University email system
School email address
sender@fc.ritsumei.ac.jp

Figure 15 Example of changing sender and losing email

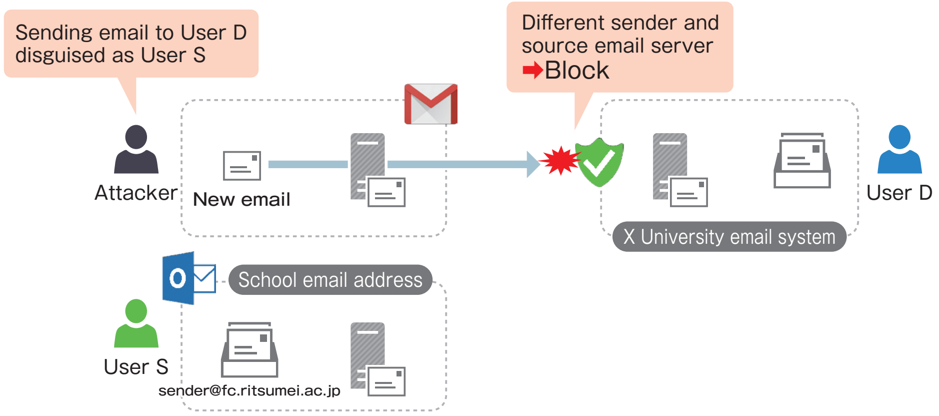

Sending email to User D disguised as User S
Different sender and source email server
➡Block
Attacker
New email
User D
X University email system
School email address
User S
sender@fc.ritsumei.ac.jp

Figure 16 Example of blocking spoofed email

In recent years, spam email prevention measures (especially outbound domain authentication) can cause forwarding and change of sender to lead to lost emails, so try to avoid this and use school email as it is to the best of your ability.

4-7 Do not include highly confidential information

Email can be compared to postcards: When you send email over the internet, you should assume that anyone could take a look at the content. (see Countermeasures 5 “Transmission and storage (encryption)”). When a postcard is mailed to a postbox, a malicious delivery worker may see it, or someone may take a look at it when the delivery worker takes their eyes off it. Because the internet is made up of networks connecting various organizations and individuals, security countermeasure standards and employee governance are not always trustworthy. As wireless communication has become more common in recent years, interception has become a much more familiar threat.

Therefore, **highly confidential information such as IDs, passwords and personal information should not be written in or attached to emails, as they could be intercepted.** During email correspondence, it is important to have the same sense that “someone might be listening (or watching)” as when conversing in a public place.

While these mechanisms are difficult and have a steep learning curve, there are ways to encrypt email such as S/MIME and PGP encryption, so it is helpful to look into these.

Also, if you need to send highly confidential information (such as files) over a network, you should encrypt them, deliver them using appropriately managed network attached storage (NAS), or by using the sharing function of online storage with authentication functions while using a file transfer service. These methods are described in detail in Countermeasures 5 “Transmission and storage (encryption)” and Countermeasures 6 “Access rights (sharing).”

Countermeasures 5

Transmission and storage (encryption)

The communication path of an information network is a system in which data is transmitted through cables, radio waves, network devices, computers, and other various devices and storage media, but the user does not know which of these routes the data is passing through. Along these different routes, there may be media that is not properly managed or administrators with malicious intentions. Therefore, when data is transmitted in a manner which can be read by anyone (called “plain text”), information may leak through interception, so please pay attention to the configuration and usage of devices that are connected to a network.

Furthermore, when a PC, storage device, USB memory, SD card, other devices or storage media are thrown away, stolen, or lost, the data on the device or storage media can be recovered if the data is saved (recorded) in plain text. Therefore, information may be leaked if a third party obtains the device or storage media.

To prevent such information leaks, encrypting plain text data along communication paths and on devices and storage media is an effective way to make the contents of the data unreadable even if a third party obtains the storage media or intercepts the communications.

This section introduces the risks of information leakage when transmitting or saving data and explains the use of encryption as a countermeasure.

4 key points related to encryption

- **5-1** Verify the encryption when using websites
- **5-2** Beware of sending emails without encryption
- **5-3** Verify the configuration when using wireless LAN (Wi-Fi)
- **5-4** Encrypt highly confidential data

5-1 Verify the encryption when using websites

There are two types of website URLs which start with either “http://” or “https://.” “http” means that plain text is used to communicate with the website (HTTP communication) while “https” means that the communication with the website (HTTPS communication) is encrypted. At one time, HTTP communication was the most common, but in recent years HTTPS communication has become mainstream. Apps for smartphones and other mobile devices now tend to require HTTPS communication.

Applications including web browsers which communicate by HTTPS first use a digital certificate issued by a certificate authority to authenticate that the website has not been spoofed (faked) before encrypting the communications. This might be somewhat difficult to understand, **but the two key points that users should be aware of are, “Is it set to HTTPS communication?” and “Can the digital certificate be trusted?”**

The first point is that you should not enter important information (ID, password, credit card number, personal information, etc.) on a website that uses HTTP communication. Be sure to check that a padlock icon (using HTTPS communication) is displayed in the address bar of the web browser.

HTTP communication

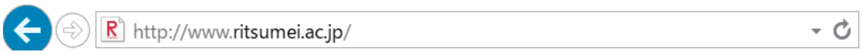

http://www.ritsumei.ac.jp/

Figure 17 HTTP communication (Internet Explorer 11)

HTTPS communication (general certificate)

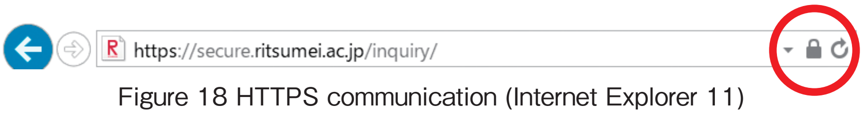
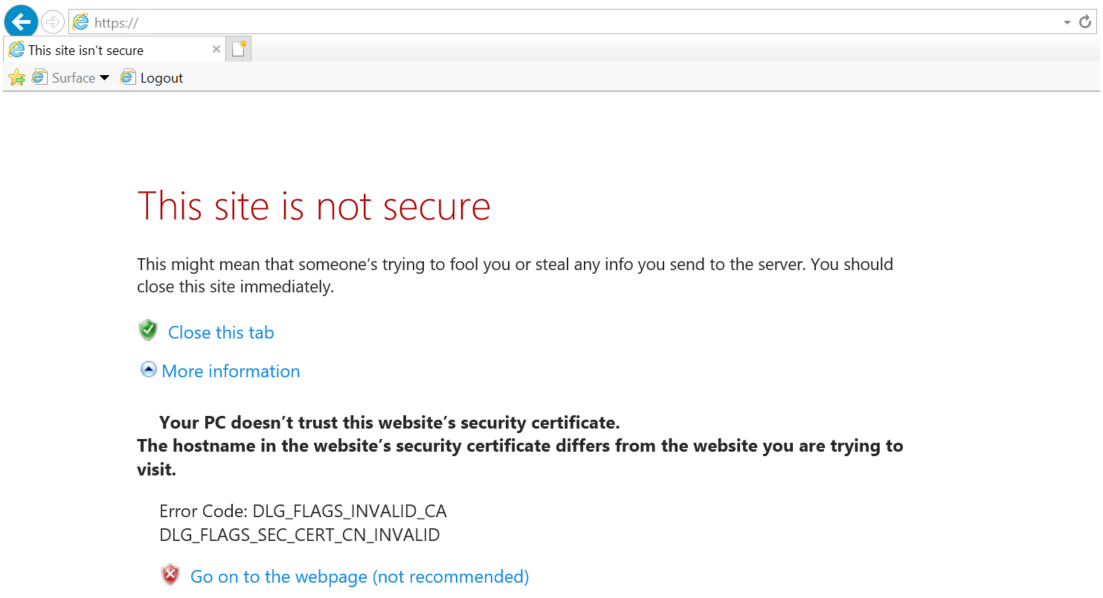

https://secure.ritsumei.ac.jp/inquiry/

Figure 18 HTTPS communication (Internet Explorer 11)

Furthermore, the web browser may display a warning screen even when the padlock is displayed if; a fake digital certificate is used, the web browser is not registered as a trusted certificate authority, the digital certificate has expired, or other irregularities are detected. When a warning appears, you may be guided to another server, made vulnerable to interception, etc. There is a possibility that the website may not be safe, so please be careful.


https://

This site isn't secure

This site is not secure

This might mean that someone's trying to fool you or steal any info you send to the server. You should close this site immediately.

Close this tab

More information

Your PC doesn't trust this website's security certificate.
The hostname in the website's security certificate differs from the website you are trying to visit.

Error Code: DLG_FLAGS_INVALID_CA
DLG_FLAGS_SEC_CERT_CN_INVALID

Go on to the webpage (not recommended)

Figure 19 Warning when there is a problem with a certificate (Internet Explorer 11)

The second point to be aware of is that a typical digital certificate guarantees that the user is definitely accessing the website represented by the URL that the user accessed. However, the digital certificate does not guarantee that the website is the site expected by the user.

A digital certificate can be obtained by a domain administrator. Therefore, a malicious attacker could obtain a misleading domain (for example, ritumei.jp) which resembles an actual organization name to operate a fake website. As a result, you must check whether the URL is a website provided by the intended organization even if you are using HTTPS communication.

Furthermore, in an increasing number of cases, financial institutions and other organizations are obtaining EV certificates, which certify the organization's actual existence through strict screening, to indicate the safety of their websites. When an EV certificate is used, the address bar turns green (green bar), and the company name appears next to the padlock icon. This allows users to more easily verify the safety of the URL.

HTTPS communication (EV certificate = Green bar)

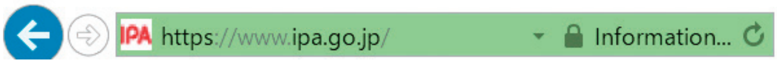


Figure 20 Green bar (Internet Explorer 11)

5-2 Beware of sending emails without encryption

Email is a service which has existed from the time when the internet was first created, there are countless email systems throughout the world, and many systems remain which do not support encryption. Email is delivered by passing through countless email systems which are unencrypted. Therefore, unencrypted sections exist along the delivery pathway at all times. As mentioned earlier, you must use the internet with the understanding that you do not know where your communications may be intercepted. (See also Countermeasures 4 “Email”)

However, there are also zones or aspects that users can encrypt on their own. These include everything from PCs, smartphones, and other devices used to browse email up to the email server which administers their own email address. This zone is where all of the data that is in your email box flows. If you are targeted by an attacker, this zone can be said to be the most dangerous. In addition, this is also the zone where there is a risk of wireless communications being intercepted, so be sure to check that wireless communications are encrypted.

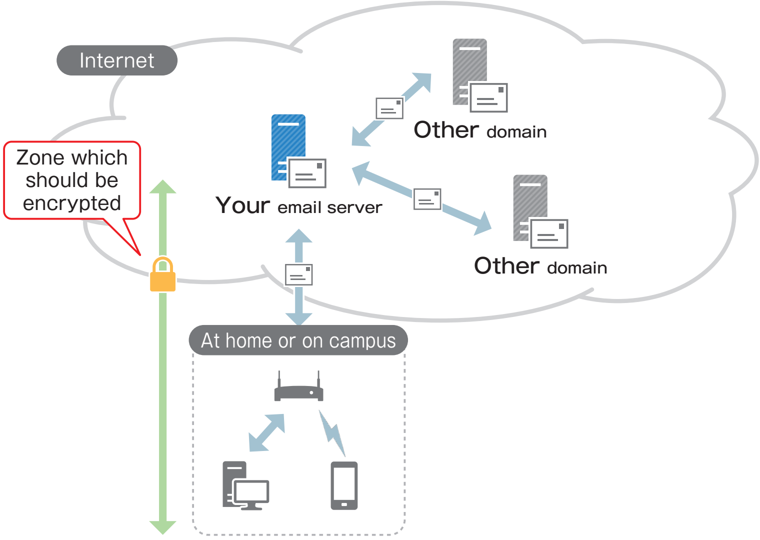


Figure 21 Email delivery route

When using web email to send and receive email with a web browser, please see “Verify the encryption when using websites” above. When using an email client to send and receive email, check the connection mode settings. If they are set to POP/IMAP/SMTP, email is sent in plain text, so be sure to change it to an encrypted connection mode setting such as POPS/IMAPS/SMTPS.

5-3 Verify the configuration when using wireless LAN (Wi-Fi)

In recent years, it has become common to connect to the internet not only on campus and at home but also at train stations, airports, hotels, cafes, Wi-Fi spots (called “public wireless LANs” and “public networks”) provided by mobile carriers, etc. In addition, an increasing number of users are setting up wireless LAN routers

(Wi-Fi routers) and wireless LAN access points (Wi-Fi access point) on their own to use a wireless LAN (Wi-Fi) at home.

The points that you should pay attention to when “configuring a connected device” are fundamentally the same as when “connecting to a network.” First, you should recognize that wireless (Wi-Fi) communications may be intercepted and decrypted depending on the communication status, and highly confidential information may fall into the hands of a malicious third party. **In particular, there is a tendency to mistakenly think that your communications are encrypted when connecting to a wireless LAN (Wi-Fi) on campus or in a public place, so please be careful.**

Table 1 Communication status and the risk of interception and decryption

Communication status	Interception and decryption
Not encrypted	Extremely dangerous
Security key (password) is public and shared	Dangerous
Using an encryption scheme with a known decryption method	Dangerous
Using an optimal encryption scheme	Safe

First, you can verify the communication status of the device being connected by checking the following items.

1. Check the wireless LAN (Wi-Fi) settings of the device being connected. If a “padlock icon” or a “security protected (= encrypted)” message is displayed, then it is encrypted.
2. The security key (password) is public and shared for networks provided in a public place including on-campus.
3. Check the encryption scheme in the detailed wireless LAN (Wi-Fi) settings of the device being connected. If the scheme is set to WPA2-PSK, then there is no problem (this will change to WPA3 in the future).

Explanation ⑨

Wireless LAN (Wi-Fi) security key

To make it easy for the reader to visualize, this security key (password), strictly speaking, does not refer to a password for deciding whether or not to use a wireless LAN (Wi-Fi). The security key is used as a key to apply the wireless LAN communication encryption. Because everyone uses the same key to transmit information, people with the same key on campus or in a public place can decrypt any intercepted communications.

In an environment such as the home where only a limited number of users know the security key (password), it is okay to use a suitable encryption scheme. However, what should you do when connecting to a network on campus or in a public place? To use the web as an example, if you are able to verify the encryption as described in Countermeasures 5-1 “Verify the encryption when using websites”, then there is no problem. The reason is that wireless LAN (Wi-Fi) encryption is an even stronger form of encryption than the HTTPS protocol used for encryption by websites. However, it is difficult to be aware of the transmissions of all devices and make sure that they are safe, so be sure to use a VPN if possible.

Explanation ⑩

What is a VPN?

A VPN (Virtual Private Network) is a system which encrypts PCs, smartphones, and other devices connecting to the internet at home or through a public wireless LAN, etc. up to the entry point of a network provided by an organization to ensure the same level of safety as when using the network from inside the organization.

A VPN allows you to encrypt all of your communications when using a free Wi-Fi spot, hotel network, or other public network that is not encrypted.

The following section explains the points that users should pay attention to when configuring a wireless LAN router (Wi-Fi router) and other devices on their own. The following steps are essentially the reverse of the process used to “connect” described above.

1. Set the security key (password).
   (It is recommended that you use a character string of 20 characters or more which is difficult to guess.)
2. Do not carelessly give out the security key (password). Run the connection set up using the device buttons.
3. Set the encryption scheme to WPA2-PSK.
4. Change the default setting for the administrator password on the device to restrict access to the control screen.

Column 2

Interference between wireless LAN (Wi-Fi) devices

While not directly related to security measures, a wireless LAN (Wi-Fi) can only be used within a predetermined and limited frequency band. In order to maintain a wireless LAN network for education research across the entire school, the network is arranged so that radio wave interference does not occur within a limited frequency band. However, when independently installed wireless LAN routers (Wi-Fi routers) and other wireless LAN (Wi-Fi) environments are present, the radio waves interfere with each other and cause problems for other faculty members and students. Therefore, please refrain from installing wireless LAN routers (Wi-Fi routers) in locations where the on-campus wireless LAN is available if at all possible.

5-4 Encrypt highly confidential data

There are various types of devices and media for storing data such as PCs, storage devices, USB memory, and SD cards. If any of these items are thrown away, stolen, or lost, there is a possibility that data may pass into the hands of third parties. If the data is encrypted, information leakage can be prevented even in such situations.

There are various methods for encrypting data. The three primary methods are “encrypting devices and folders,” “encrypting USB memory, SD cards, and other portable storage media,” and “encrypting office documents, PDFs, and compressed files (zip and other files).”

In the first method, you can encrypt the storage on a PC or smartphone using standard OS features or commercial encryption software. You can encrypt at different levels including the device (all storage), accounts, and folders. When it comes to USB connected storage, network attached storage, and other devices, there are products available with encryption features. A third party who obtains a device that was stolen, lost, or thrown away can take the device apart and directly access the internal storage (hard disk and built-in memory, etc.) to bypass the login and other OS authentication steps and steal the data. However, they cannot view the content of the data if it is encrypted. To prevent information leaks, be sure to encrypt devices which store highly confidential data.

Encryption methods for each OS

■**Windows 10**

[START] › [Input with bit] › [Manage BitLocker]
Use the BitLocker feature to encrypt the drive.

■**macOS**

[System Preferences] › [Security & Privacy] › [FileVault]
Use the FileVault feature to apply encryption at the account level.

■**iOS**

All editions of iOS are encrypted.

■**Android**

[Settings] › [Lock & Security] › [Security] › [Encryption settings] › [Encrypt phone]

However, be sure to carefully store the recovery key when using such encryption software. Without this recovery key, you may not be able to recover the OS or initialize the device.

Secondly, carrying or transferring data by portable storage media such as USB memory, SD cards, and writable CDs/DVDs may lead to information leakage incidents if they are lost, stolen, or thrown away without deleting the data. These types of portable storage media can also be encrypted using standard OS features (BitLocker and FileVault) and commercial encryption software. In addition, some types of USB memory also have encryption features. The most important thing is to properly manage portable storage media. However, be sure to apply encryption when storing highly confidential data in case something goes wrong.

Finally, you can use the features in various applications to encrypt Office documents (Word, Excel, etc.), PDF files, and data archives (ZIP, etc.) which compress multiple files. In particular, information may be leaked due to ID and password theft or incorrect shared settings when uploading (saving) data to cloud services and other online storage. To prepare for such possibilities, be sure to upload (save) an encrypted version of highly confidential data.

Countermeasures 6

Access rights (shared)

Access rights are permissions to use devices and data. As information and communications technologies become commonplace, various types of devices are connected to the internet, and different forms of information including social media, calendars, and files have become “shareable” through internet services. Configuring the scope of social media disclosure, calendar sharing, file sharing, and other settings configures the scope for sharing your information. In other words, it sets who is given access rights to your information. Furthermore, when you set up a wireless LAN (Wi-Fi) to use at home, configuring the access point determines which users and devices can access the home network, so this falls under access rights management. **Today, access rights management is a task which is not only performed by experts. Everyone who uses the internet must be aware of and take responsibility for managing access rights.** If you use the internet or devices without thinking about, “Who should access that information?” it will definitely lead to a serious information incident. In particular, information cannot be completely deleted or recovered once it has been released to the internet. You will find yourself in a situation that truly cannot be undone.

When using social media, online storage, and other services, you must be aware at all times of the extent to which different types of information are being shared and decide whether or not to grant access rights. Posting or sharing information while neglecting to check the access rights is like neglecting to perform a safety check when driving a car, which can lead to a major accident.

The following section introduces the risks when sharing data and explains the countermeasures.

3 key points regarding sharing

6-1 Be careful when sharing files on a PC

6-2 Be careful with sharing functions on cloud services

6-3 Pay attention to the settings of all devices connected to a network

Example 2

Information leak due to a default setting problem in Google Groups

In 2013, it was reported that incidents involving information leaks occurred at multiple government agencies, universities, and other institutions that were using the consumer-oriented Google Groups service for business. Because Google Groups is configured by default to allow public access, information which was restricted to authorized persons only was published to the internet. However, Google was not at fault. Generally speaking, these types of consumer-oriented services tend to publish and share information in a broad manner. The problems were caused by users who did not check the access rights, and the information was published to unintended recipients.

Do not prioritize convenience and avoid the casual use of consumer-oriented services for education, research, operation management, and other tasks without checking the access rights and other settings.

Ref: IPA, インターネットサービス利用時の情報公開範囲の設定に注意！
(Pay attention to the settings for configuring the scope of information disclosure when using internet services!)[17]
https://www.ipa.go.jp/security/txt/2013/10outline.html

[17] This website is Japanese only.

6-1 Be careful when sharing files on a PC

PCs have many different access rights settings which are extremely complex. In particular, you should pay attention to the file sharing settings. Basically, you should limit access to yourself and only allow access to specific people when necessary. Furthermore, when the group work is finished, be sure to delete the sharing settings. If you allow anyone to write to that location, it may become an entry point for a network attack or cause malware to spread, which is extremely dangerous. **When sharing files, limit who you grant access to and make it a habit to delete the settings when you have finished using the files.**

6-2 Be careful with sharing functions on cloud services

An increasing number of users are uploading (saving) their files to Dropbox, GoogleDrive, iCloud, OneDrive, Yahoo!Box, and other so-called online storage services. Locations that can connect to the internet can be accessed from anywhere. These are extremely convenient services, because they can be accessed from various devices including PCs and smartphones. Online storage is often used for transferring files, because files can be easily shared. There are two important points that you should pay attention to when using online storage.

The first point is that because most consumer-oriented online storage is set by default to share with the entire internet (see Explanation 11 “URL Publishing Features”), you must pay even more attention to the sharing features of online storage compared to file sharing on a PC. Be sure to check the restrictions applied to the person that you are sharing files with and the range of disclosure during configuration. Also make sure that you delete the files or change the sharing settings once they have been received by the other person. **Furthermore, do not share highly confidential data on services that only have features which share files with the entire Internet.** When sharing highly confidential data, choose a service which is able to restrict access to a specific individual through authentication and has robust authentication-related security features (see Countermeasures 2 “ID and password management") such as multi-factor authentication, login history, and change notification emails. Furthermore, while it may be inconvenient, it is also extremely useful to restrict the connection source network.

The second point that you should pay attention to is that you must be aware of what rights you are granting to the other person that you are sharing files with. In many cases, the rights which are granted to the other person during sharing are browse, edit, and reshare. Reshare means that you are granting the other person the right to share the file again with a third party (see Figure 22). As the saying goes, "Anyone can start a rumor, but none can stop one." The moment that you share a file with someone, it becomes difficult to prevent an information leak. However, you can avoid incorrect editing, modification, or loss by configuring the rights of the other person in an appropriate manner. **Therefore, be sure to check what operations are used and which rights are granted to the other person that you are sharing with so that only the necessary rights are given.**

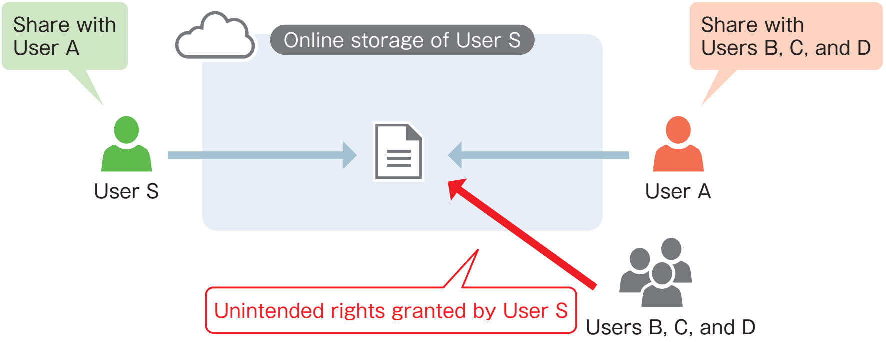


Figure 22 Resharing

Furthermore, while it can be said that entrusting your files to online storage is the riskiest, beware of all web services that you "share" and "entrust data" to including social media, calendars, as well as video and photo storage sites.

Example 3

Risks of online storage

From a security perspective, there is a significant difference between on-campus network attached storage (file servers) and off-campus online storage. That difference is the network.

The on-campus network can only be accessed by members of the campus community. However, online storage is openly available on the internet and can be accessed by attackers with malicious intent.

For example, in an information leak incident which occurred at a certain university in the fall of 2016, a phishing email (or targeted attack email) was used to steal not only the ID and password of a staffer but also the business information uploaded to an online storage service. Furthermore, the staffer's email account was used as a platform to send as many as 120,000 spam email messages.

Highly confidential information should be stored in a safe location which applies the on-campus network restrictions after setting the appropriate access rights. When using off-campus online storage for reasons of convenience, countermeasures such as restricting the connection source network are required. Alternatively, you can also use "multi-factor authentication" which was introduced in Countermeasures 2 "IDs and passwords."

Explanation 11

URL Publishing Features

Online storage, calendars (Google Calendar, etc.), video services (YouTube), and other services have a feature, which is sometimes called a "hidden URL" or "limited access URL," that publishes content only to a person who knows the URL. Those systems generate a URL which is difficult for a person or even a computer to guess that allows a user to share data only with the person who is given that URL.

At first glance, you might think that this was a safe way to share data. However, if you think about it, **this means that anyone around the world who knows the URL can access the data no matter who they are. Therefore, it cannot be said that the access rights are suitably configured.** It is similar to leaving your house key in a hard-to-find location for someone. The URL may spread if the email containing the URL is leaked, the recipient leaks the URL, or the URL is simply posted on social media. Therefore, this is not a feature which should be used for highly confidential information.

*The Google Calendar feature is called "Private URL" and can be accessed by anyone knows the URL, so caution is advised. This URL can be changed, but the public access cannot be removed. Be sure to set the access rights at the event level.

Column 3

Choosing a file transfer service

When sending and receiving large files, "file transfer services" such as Filesend, GigaFile and DataDeliver are used to handle files which contain highly confidential information. The way it works is that you upload a file to the website, and it generates a URL to share. When sending highly confidential information, there are three security aspects which you should be aware of.

First, these services are equipped with a password feature, and it is a good idea to select the password delivery method on your own instead of having it automatically sent in an email, etc. You can ensure the safety of the password by sending it through a different route than the download URL notification email such as telephone, fax, SMS, Skype, Line, and other messaging services.

Next, be sure to use a service that allows you to verify the date and time that the file was uploaded and downloaded as well as the location history. This will allow you to discover from the history if the corresponding file was accessed at an unknown time and location to identify information leaks.

Finally, the users of such services are "entrusting their data," so it is necessary to verify how the entrusted data will be handled. In addition to selecting a service provider that is clearly identified and has a strong reputation with users, be sure to check the "service agreement." See Countermeasures 9 "Check the agreement with the service provider" for the key points to check in the service agreement.

6-3 Pay attention to the settings of all devices connected to a network

As stated in Countermeasures 1-3 “Update all devices connected to the network,” you must pay attention to the settings of all devices connected to a network with a focus on access rights. Network connected devices include various devices other than PCs and smartphones such as wireless LAN routers (Wi-Fi routers), network attached storage (NAS), printers and copiers, network cameras (surveillance cameras, webcams, etc.), teleconferencing systems, large monitors, projectors, digital appliances (TVs, HDD recorders, and home video game consoles). The network settings and access rights must be appropriately configured for each device.

See Countermeasures 5-3 “Verify the configuration when using wireless LAN (Wi-Fi)” to configure a wireless LAN router (Wi-Fi router).

As stated above in Countermeasures 6-1 “Be careful when sharing files on a PC,” restrict who files are shared with and manage the IDs in an appropriate manner for network attached storage (NAS). Files must not be accessible or writable by everyone. **The internet publishing feature of a network attached storage (NAS) device must not be used to share highly confidential information.** If you absolutely must share information via the internet from the perspective of convenience, apply appropriate restrictions such as access restrictions and restrictions on the connection source network. In addition, such devices lately include various features for media sharing and internet publishing, so be sure to carefully read the manual and turn off any unnecessary features.

Example 4

Information leak incidents with network attached storage

In 2014, a faculty member at a certain university took home a network storage device which contained a list of over 30,000 student names and the grades of over 3,000 people and connected the device to a home network. The data was openly available on the Internet, because the person did not carefully check the device settings. In addition, the published data was picked up by a search engine, and the contents became searchable on the Internet.

If the person was properly aware of the importance of the information being handled, the responsibility, and need for security, they never would have taken the information off-campus in the first place.

Printers and multifunction office machines have a data storage area, so if you do not implement countermeasures for vulnerabilities and manage the access rights, the printed and scanned documents may be leaked.

Incidents have occurred where video was leaked, because countermeasures for vulnerabilities and access rights management was not implemented for webcams and security cameras.

Furthermore, various devices are now connecting to the internet. Therefore, you should apply this document to not only PCs and smartphones but also to all devices which connect to a network to check and appropriately manage the access settings (especially the access rights to the control screen) in addition to updating the firmware as discussed in Countermeasures 1-3 “Update all devices connected to the network.”

Ref: IPA, 複合機やウェブカメラ、情報家電などにも適切なアクセス制限を
(Recommendations for appropriate access restrictions for multifunction office machines, web cameras, information appliances, etc.)[18]
https://www.ipa.go.jp/security/announce/20150317-netdevice.html

[18] This website is Japanese only.

Countermeasures 7 Mobile devices such as smartphones

With the availability of lighter devices and the expansion of public wireless LAN environments, the number of opportunities to use smartphones, tablets, lightweight and compact notebook PCs, and other easily portable computers referred to as "mobile devices" on the move or away from the home and office have increased. These mobile devices are basically computers which connect to the Internet, so the same security measures as PCs are required. Therefore, you should first carry out the steps described in Countermeasures 1 "Malware (viruses)" for mobile devices as well.

The following introduces the risks concerning smartphones, tablets, lightweight and compact notebook PCs, and other mobile devices and explains the countermeasures.

2 key points concerning mobile devices

- **7-1** Take steps so that the information is not accessed if a device is stolen or lost
- **7-2** Be careful when giving access permissions, IDs and passwords to applications

7-1 Take steps so that the information is not accessed if a device is stolen or lost

There is a risk of theft or loss when carrying around a mobile device. **Of course, you should exercise caution so that your mobile device is not stolen or lost, but it is important to take steps in advance under the assumption that the device may be stolen or lost.**

First, set up a lock or user authentication on devices which access highly confidential information including email so that the devices cannot be used by other people. Furthermore, it is important that you do not use a simple pattern lock or PIN and prevent others from seeing you enter such information. Be sure to carefully wipe off the smartphone screen, because the pattern or code can become visible due to fingerprints or dirty fingers.

Next, check the OS, optional mobile carrier services, and security software for any available GPS tracking features to use in the event of theft or loss and rehearse the use of these features in advance. In addition to the tracking features, be sure to check the usage and enable the settings of emergency features which remotely lock a mobile device, change the password, stop a lost mobile device from connecting to services, and remotely erase data (remote wipe). These features can be found not only in mobile operating systems such as iOS and Android but also in Windows 10 and macOS.

On a notebook PC, be sure to enable user authentication to prevent it from being used just by booting up the computer. Furthermore, be sure to encrypt the drives on a mobile device which stores and accesses highly confidential information, because there are ways to remove a drive (hard disk, USB memory, etc.) and read the data. (See Countermeasures 5-4 “Encrypt highly confidential data”)

Additionally, be sure to limit the amount of information leaked due to theft or loss by not downloading (delete such data if you do download it) or carelessly storing and walking around with highly confidential data.

Example 5

Ratio of theft and loss in information leak incidents

According to a research report from JNSA concerning information security incidents, the ratio of incidents caused by theft and loss is as follows.

Table 2 JNSA research report on information security incidents

Survey year	Lost or forgotten	Stolen	Total
2014	12.6 %	3 %	15.6 %
2015	30.4 %	5.5 %	35.9 %
2016	13.0 %	5.3 %	18.3 %

*Includes USB memory, etc.

Educational institutions handle a lot of personal information and multiple information leak incidents have actually occurred. In 2007 and 2012, personal information was also leaked from this university due to home and vehicle burglaries.

7-2 Be careful when giving access permissions, IDs and passwords to applications

Smartphone and tablet operating systems such as iOS, Android, and Windows 10 have configuration features for managing whether or not it is okay for apps to access features and user information stored on the device. When apps are installed or launch for the first time, they check if they are permitted to access the telephone/calling features, storage, address book (contacts), accounts, other apps, location information, networks, and SMS or MMS services. Be sure to carefully check what aspects of your information are being read instead of just permitting access without closely reading these confirmation requests.

As a selling point, there are also smartphone apps that allow you to enter your ID and password for other services to provide a higher level of convenience compared to the official service. These include many apps which directly link to online banks, credit cards, digital cash, and other financial transactions. For example, there are apps which centrally manage your bank account transaction information, credit card usage information, digital cash usage information, etc. to load that information into your household account. These types of apps provide information about the bank or credit company that you use to the developers (or entrust them with the management of such information), so instead of just focusing on the convenience, carefully check that the app is officially recognized by your bank or credit card company (see Tips 7 “Be careful with ID collaborative trust frameworks”) and that the app provider is a trusted company.

Column 4

Services and apps which are not provided by the university or affiliated schools

In recent years, there have been an increasing number of cases in which student organizations, individual students, or off-campus organizations provide services and apps for students. Although there are no legal problems with such activities, these types of services and apps tend to target services provided by the university and affiliated schools that have a low level of convenience or they aggregate multiple university and affiliated school services into one. In many cases, they use a system which requires the user to login with the university ID and password and then accesses the official services through the app.

With such apps, it is not possible to check whether or not the entered ID and password or the personal information accessed with that account are being stored outside of the mobile device or whether the app is designed to allow the app providers or other third parties who are not the user to access that information.

In addition, there is a risk that the service or app provider may be responsible for the user receiving incorrect information or there may be a vulnerability in the service or app that the provider is not responsible for which leads to an information leak due to a cyber attack.

In consideration of these risks, services with issued IDs and passwords should not be used from third-party services and apps that are not authorized by the providers.

Countermeasures 8

Personal information and the infringement of rights

The phrase "big data" came into use several years ago. Simply put, big data means that it has become possible to rapidly analyze large volumes of data, so we should gather various types of data, and effectively use it in business activities. For example, the history of user behavior at an online shop is analyzed to produce ad recommendations, social media information is analyzed to display possible acquaintances, regular location information is analyzed to provide weather and traffic information for a person's place of work or home, and your location information, history of searches/entries/language changes on a website, information when an error occurred, and various other forms of information can now be collected to improve services and applications.

Furthermore, it has become possible to easily search and access information, images, music, video, and other content. In addition, content can be easily posted and shared on blogs, social media, etc.

With big data gaining momentum and content becoming easy to post and share in recent years, how should we approach the internet? This section explains what you should pay attention to in order to avoid having your personal information misused or your privacy violated and to make sure that you do not infringe another person's rights or commit an unlawful act.

4 key points regarding personal information and the infringement of rights

- **8-1** Check the information that is gathered by PCs and smartphones
- **8-2** Check the degree to which your website browsing history is shared
- **8-3** Beware of making personal information public on social media
- **8-4** Be conscious of the rights and laws concerning intellectual property and personal information, etc.

8-1 Check the information that is gathered by PCs and smartphones

The usage history and other information is actively gathered from Google accounts, Apple IDs, Microsoft accounts, and other accounts that are shared across PCs and smartphones, so there is a possibility that some information which the user may prefer not to provide is also being collected. In Android, iOS, Windows 10 and later versions, various types of information are gathered when the user selects the settings recommended by the provider as the default. Carefully check the privacy settings and restrict them to the information that you are comfortable providing.

Privacy settings in each OS

■**Windows 10**

[Settings] > [Privacy]

■**macOS**

[System Preferences] > [Security & Privacy] > [Privacy]

■**iOS**

[Settings] > [Privacy]

■**Android**

[Settings] > [Google] > [Google Account]
[Settings] > [Apps] > (Open each app) > [PERMISSIONS]

8-2 Check the degree to which your website browsing history is shared

Using a web browser to search websites, browse, and use web services integrates a lot of information concerning the user's business and privacy such as money management information, business information, individual tastes and thoughts, etc.

A PC which is shared with another user retains not only the website browsing history and other information but also the authentication information (logged-in status). **This means that not only can your history information be viewed by another**

person, but there is also a risk that the PC may log back into web services that you were using. To prevent such information from remaining on a shared PC, be sure to use the private browsing feature of the web browser when using web services. (Each of the browsers use a different name. Internet Explorer 11 and Edge have InPrivate Browsing, Chrome has Incognito mode, Firefox has Private Browsing, and Safari has Private Browsing.) After you are finished using the web services, be sure to log out and exit the web browser.

Furthermore, web browsers that link accounts with cloud services such as Edge (Microsoft accounts), Chrome (Google accounts), and Safari (Apple IDs) upload (save) the website browsing history, bookmarks, IDs, passwords, etc. to the cloud. While this feature makes such information available from any device, the browsing history, etc. is also utilized for big data in some cases. Carefully check the web browser and cloud service privacy settings and turn off any items that you do not wish to upload from your PC, smartphone, tablet, etc.

8-3 Beware of making personal information public on social media

Regarding the ethics and use of social media, please read the “Five Key Points That You Should Know When Using Social Media” (Social Media Guidelines) for students, because it is an extremely useful reference.

Caution is required when using social media not only from the perspective that your personal information may be abused, but also because of the added possibility that the private information of your friends may also be abused (through information posted by you and your social media connections). In particular, there is a possibility that an individual may be identified by combining multiple types of information such as the background which appears in an uploaded photo, etc. **Please be aware that even if an individual cannot be identified from one post, there are cases where it is possible to identify an individual through a combination of posts.**

Furthermore, personal information is being unintentionally published (mainly due to a lack of understanding of social media/service rules or technology) on social media in an increasing number of cases.

Examples of personal information being unintentionally published

- Using services without checking the scope of sharing
- Setting the scope of sharing incorrectly
- Not realizing that location information is included in photos and posts
- A friend who shared your post re-shared and published the content
- Not checking if the social media operator is collecting post content and other information and using it for unintended purposes or providing it to third parties

An increasing number of clever methods exploit such information to identify an individual and send targeted attack emails or commit fraud. **Because it is difficult to detect such elaborate methods, be sure to carefully check the social media features, scope of sharing, terms of service, and privacy policy (see Countermeasures 9-2. “Check how personal information is handled”) to avoid unintentionally publishing personal information.**

Ref: Ritsumeikan University, SNS利用にあたって知ってもらいたい5つのこと、SNSガイドライン(Five Key Points That You Should Know When Using Social Media, Social Media Guidelines)[19]
http://www.ritsumei.ac.jp/rs/sns/

Ref: Ministry of Internal Affairs and Communications, 国民のための情報セキュリティサイト「SNS利用上の注意点」(“Precautions When Using Social Media” information security site for citizens)[20]
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/security02/05.html

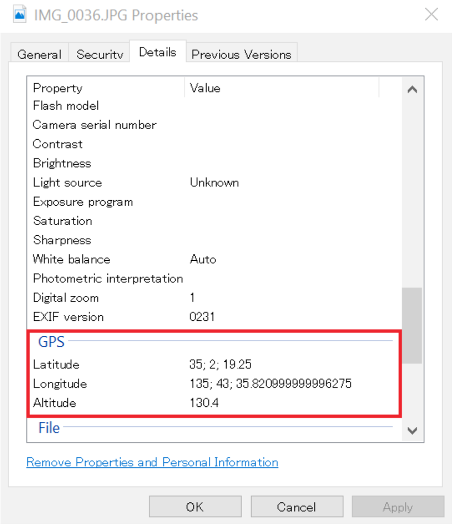
Ref: Nikkei BP, SNSの落とし穴：こんなはずじゃなかった！SNSで個人情報がダダ漏れ、取り返しのつかないことに (Social media pitfalls: This was not supposed to happen! Massive leaks of personal information on social media cannot be undone)[21]
http://www.nikkeibp.co.jp/article/matome/20131125/374827/

[19,20] This website is Japanese only.
[21] This website is currently unavailable.

Explanation ⑫

Location acquisition features and location information embedded in images

When a photo is taken on a device that can acquire the location information (mobilephones, smartphones, and some digital cameras), the information about where that photo was taken is embedded in the image (This feature is called “geotagging.” The figure below shows the information embedded by the iPhone camera when the image properties are checked on a Windows computer. The latitude and longitude information is displayed.). With the latitude and longitude information, the location can be easily determined with a map app.



IMG_0036.JPG Properties

Property	Value
Flash model	
Camera serial number	
Contrast	
Brightness	
Light source	Unknown
Exposure program	
Saturation	
Sharpness	
White balance	Auto
Photometric interpretation	
Digital zoom	1
EXIF version	0231
GPS	
Latitude	35; 2; 19.25
Longitude	135; 43; 35.820999999996275
Altitude	130.4
File	

Figure 23 Properties of a photo taken with an iPhone

There are also cases where the Twitter social media app published location information in tweets, etc. By comparing the location where a photo was taken, the location where it was posted, and the post content, it is possible to determine the type of location (home, etc.).

<Example: “Taking a photo of a cat at home and posting it”>

User A uses her real name on social media. One day, User A took a photo of her cat at home with a smartphone and published it on social media. Several days later, fake invoices, etc. started arriving at User A's home.

In addition, a person's home and place of work can be inferred through behavioral analysis. Be especially careful about location information when using social media.

Tips 10

Secret questions and social media

In Countermeasures 4 “Email,” we introduced cases where social media containing various information about a particular individual is used as preparation for targeted attack emails and fraud. Using a similar line of thinking, you should also be careful about “secret questions” and social media.

“Secret questions” are a feature for verifying the identity of a user by entering questions determined in advance during user registration, etc. that only the actual person would know, and this feature is used during procedures to reissue a password or send notifications to a user who has forgotten their password. These questions might include, “What is your mother’s maiden name?”, “What is your favorite food?”, and “What is your pet’s name?” These secret questions appear to be an effective way to confirm a person's identity, but to be honest this method is extremely dangerous. It is dangerous, because this information is known by people who are familiar to you, **it becomes easier to guess when you are making various posts on social media, and you may be unintentionally publishing the answers to the secret questions.** Due to the risk that IDs and passwords may be easily stolen in this way, there are increasing calls to discontinue the use of “secret questions” as a system of authentication.

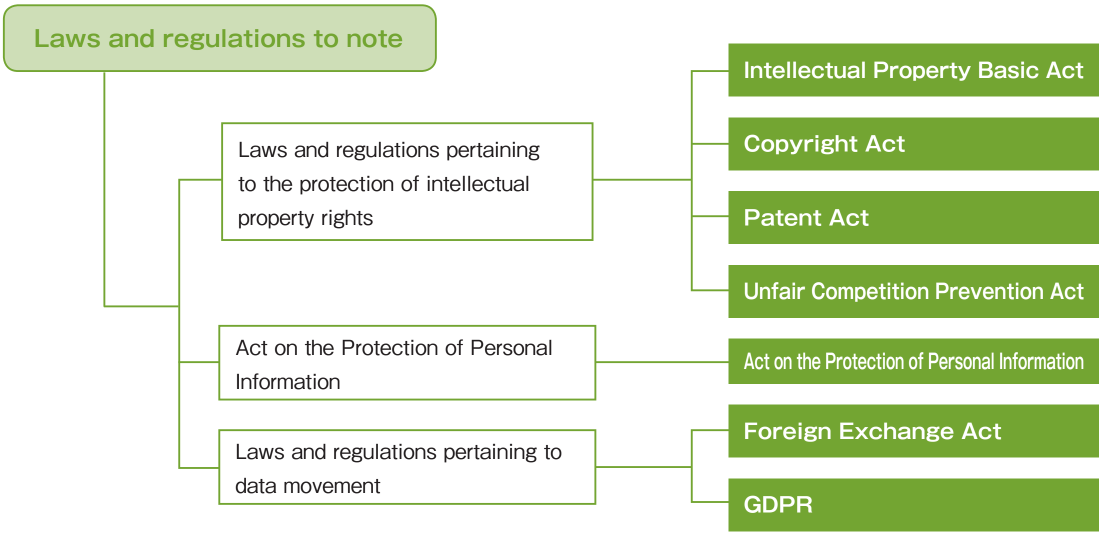
When registering the answers to “secret questions,” do not use correct answers which may be guessed.

Ref: IPA, “その秘密の質問の答えは第三者に推測されてしまうかもしれません (The Answer to That Secret Question May Be Guessed by a Third Party)”[22]
https://www.ipa.go.jp/security/txt/2015/07outline.html

[22] This website is Japanese only.

8-4 Be conscious of the rights and laws concerning intellectual property and personal information, etc.

The “Laws and regulations pertaining to the protection of intellectual property rights,” “Act on the Protection of Personal Information,” and the “Laws and regulations pertaining to data movement” are the three laws and regulations which you should be pay attention to when using the internet as shown in the figure below.


Laws and regulations to note
Laws and regulations pertaining to the protection of intellectual property rights
Intellectual Property Basic Act
Copyright Act
Patent Act
Unfair Competition Prevention Act
Act on the Protection of Personal Information
Act on the Protection of Personal Information
Laws and regulations pertaining to data movement
Foreign Exchange Act
GDPR

Citation source: 図解入門ビジネス最新ISO27001 2013の仕組みがよ～くわかる本
How - nual Business Guide Book on Understanding the Latest ISO27001 2013 System[23]

Figure 24 Laws and regulations to note

[23]This book is Japanese only.

First, we will take a look at the “Laws and regulations pertaining to the protection of intellectual property rights.” Due to the familiarity of the Internet, it has become extremely easy to obtain, duplicate, publish, and share images, music, movies, documents, and other typical content. These types of content have intellectual property rights as typified by copyright, and they are protected by laws and regulations. Under the Copyright Act, there is some tolerance regarding the use of works in classes and teaching materials “to the extent that this is found to be necessary for the purpose of school education” and “it is not-for-profit.” However, there are also cases where this is interpreted incorrectly, and the scope of usage is restricted by the usage license agreement. Consideration is needed not only for copyrights but also industrial property rights (trademark rights, patent rights, utility model rights, and design rights), trade secrets, and other general intellectual property rights. For example, if you publish a photo or video on the internet that shows the face of someone who has not provided consent, that would be an infringement of rights.

Secondly, the “Act on the Protection of Personal Information” is important to this university as an institution which handles a large amount of personal information. Under “The Ritsumeikan Trust Personal Information Protection Regulations[24]” (hereinafter, “Personal Information Protection Regulations”), faculty members are responsible for the appropriate management of personal information and shall comply with the regulations in educational research activities, operation management, and other duties based on a clear understanding of the Personal Information Protection Regulations, the Act on the Protection of Personal Information (hereinafter, “Personal Information Protection Act”), and the guidelines.

Thirdly, there is a tendency to overlook the “Laws and regulations pertaining to data movement,” so please be careful. The two important laws are the “Foreign Exchange and Foreign Trade Act” (hereinafter, “Foreign Exchange Act”) and the “General Data Protection Regulation” (EU General Data Protection Regulation, hereinafter, “GDPR”). The Foreign Exchange Act is designed from a national security export control perspective to prevent weapons and dual-use technologies from being delivered to specific regions. Information can easily cross national borders through the internet, so caution is required. The GDPR is a law for protecting personal information in the European Economic Area which is similar to the Japanese Personal Information Protection Act, but the rules are far more stringent than in Japan. In cases where personal information is acquired across borders from an individual located within the EEA area and in cases where personal information is transferred across borders from an area inside the EEA to an area outside the EEA, the GDPR standards must be satisfied, so caution is required.

[24] This English document is a translation of the original Japanese document and is for reference only.

In addition, although it is not clearly stated in the laws and regulations, the right of privacy and the right of likeness have been recognized as part of the right to the pursuit of happiness and personal rights under the concept of respect as individuals in Article 13 of the Japanese Constitution based on previous court precedents, and infringing on those rights is an unlawful act. Depending on the type of information (here we are referring to data and content), the usage may be legally regulated by a non-disclosure agreement (NDA) or product license agreement, etc.

To avoid infringing rights or committing an unlawful act, you should first **be aware that you are bound by various limits and restrictions when using data and content on the internet, so be sure to understand the restrictions regarding the extent to which you can use it, who you can show it to, etc.**

Next, **configure the appropriate access rights (see Countermeasures 6 “Access rights management”) according to the restrictions imposed on the information described above to** avoid information leaks caused by accidentally publishing or sharing **to the world of the internet where information is easily duplicated, published, and shared.**

Ref: General Incorporated Association Japan Copyright Educational Association, 著作権Q＆A (Copyright Q&A)[25]
http://jcea.info/Q&A.html

Ref: The Japan Universities Association for Computer Education, “教員のための個人情報活用ガイドライン(Guidelines for Faculty Use of Personal Information)”[26]
http://www.juce.jp/kojin_joho/
*Guidelines prior to the FY2017 amendments

Ref: Personal Information Protection Commission JAPAN
https://www.ppc.go.jp/en/index.html

[25,26] This website is Japanese only.

Explanation ⑬

Information that must not cross national borders

As mentioned in the previous section, the “Foreign Exchange Act” and the “GDPR” are representative laws which regulate the transfer of information across national borders. While it is easy to picture physical goods crossing national borders, it might be a little difficult to imagine a situation in which information “must not be removed” or “must not be transferred across national borders” in the world of the Internet.

For example, if you were to take information regulated under the “Foreign Exchange Act” and accidentally publish it on the Internet, permit someone from a specific region to access it, or share it with someone who has citizenship from a specific region, **that information would still be subject to the same regulations even if it came from a server installed on campus.** Conversely, even if a cloud service or other data storage location (data center or other location where the cloud service data is actually located) is situated in a specific region, there is no problem if access from the specific region is regulated.

Meanwhile, under the “GDPR,” the transfer of any and all information about an individual located within the EEA area to a third country outside of the EEA which does not have an “adequate level of protection (recognized by the EU as ensuring a sufficient level of data protection)” is restricted. As of 2018, Japan has not received this “adequacy decision,” which means that you must check and comply with the GDPR standards when bringing information about individuals located in the EEA area that was collected in that area to Japan (to the university or cloud services that use a Japanese data center) or when collecting information from individuals including those within the EEA area. However, it is possible to manage the information using services provided under the contractual terms from Google, Amazon, Microsoft, etc. For more details, please carefully read the FAQ for each service.

Ref: 立命館大学の安全保障輸出管理関連の資料・様式等 (Ritsumeikan University Documents and Forms Pertaining to National Security Export Controls)[27]
http://www.ritsumei.ac.jp/research/member/study_ethic/se15.html/

[27] This website is Japanese only.

Countermeasures 9

Service usage

There are various services on the internet including services for consumers and for organizations (designed for businesses and commercial use). Furthermore, there are various providers including individual operators, corporate enterprises, etc. **The users create and save data (or files) on these services. Because the users are storing data which is under their control on the service which is managed by the provider, it means that, “you are entrusting your information to the provider.”** To put it another way, using a service on the internet for business is equivalent to subcontracting business to another party. Therefore, it is important to select a trustworthy service provided by a trustworthy company when it comes to entrusting your personal information, privacy related information, and highly confidential information.

Next, you must check the terms of service and contractual terms established by the service. Once the user consents to the general conditions in the “terms of service,” “privacy policy,” etc. and begins to use the service, a legal agreement is exchanged between both parties even if the service is free. While many people probably skip over the general conditions, be sure to check them if the information being entrusted is important. The following explains which items in particular should be checked.

When entrusting information to a service, the risk of information leakage, data loss, service termination, etc. is not zero. When such an information incident or service termination risk occurs, you may be able to receive compensation as a result of a dispute, but you cannot pretend that the information security incident did not happen. It is important to prepare in advance under the presumption that a security incident could happen.

The following list introduces risks which can occur when a user entrusts their information to an internet service that they are using and explains the countermeasures.

6 key points when using a service

- **9-1** Choose a trustworthy service
- **9-2** Check how personal information is handled
- **9-3** Check how stored data is handled
- **9-4** Check where the data is stored, applicable laws and the court of jurisdiction
- **9-5** Prepare for data loss
- **9-6** Prepare for service content changes or service termination

9-1 Choose a trustworthy service

Judge whether or not an internet service can be trusted by using the certified evaluation and accreditation in addition to checking the provider's identity and user evaluations as explained in Countermeasures 1 – 5 “Only install software that can be trusted.”

As part of the provider's identity, the scale of the organization, financial situation, number of continuous years in business, and nationality are also important. To the extent possible, check the number of years since the start of service, past information security incidents and the response, etc.

With respect to user evaluations, convenience and support related evaluations are of course important, but be sure to also check in terms of the many large and famous organizations that have a certain level of market share and a track record of implementation and application in the services field.

In particular, when entrusting highly confidential information, check the service provider’s information management initiatives and the evaluations and accreditations that the organization has received. Evaluations and accreditations are the results of audits performed by the relevant institutions. Therefore, they are an objective form of evidence that the organization is implementing proper information management. A company that has received ISO/IEC27001, 27002, 27017, ISMS, CSA STAR certification, ASP and SaaS safety and reliability related information disclosure accreditation is preferable. Furthermore, if the provider is handling credit card and other payments, then the company can be evaluated if they have PCI DSS certification.

Be sure to choose a trustworthy service based not only on an evaluation of the convenience but also on these three points of view according to the confidentiality of the information being entrusted.

9-2 Check how personal information is handled

Internet-based services have a procedure through which the individual accepts the general conditions before using the service. Therefore, it is important to check the general conditions at a bare minimum. This applies not only to the Internet, but when providing personal information to receive a service, if you agree without checking the general conditions, that information may be used for purposes other than the relevant service or provided to third parties. This can result in a situation such as signing up for a credit card and seeing an increase in phone calls and emails from affiliated companies trying to sell insurance.

The active collection of personal information, usage histories, and other privacy related information is as described in Countermeasures 8 “Private information and the infringement of rights.” The general conditions always describe the purposes for which the collected information will be used and the extent to which it will be utilized. First, be sure to check the purpose of use regarding the collected information. Check if there is any mention of information usage outside of the relevant service and if so be sure to check whether the details are acceptable.

The range of use can largely be divided into “use within the relevant service,” “use including other services within the service provider,” and “provision to third parties (other services in addition to the service provider).” Check whether or not your information will be used in marketing, etc. by parties other than the service provider and if the details are acceptable.

In 2014, Culture Convenience Club (CCC), the operator of the T Point service, made headlines when they revised their privacy policy to provide the personal information received from users (T Point members) to use the T Point service to third-party T Point affiliates.

Internet-based services are inundated with the entry of personal information, **so check the scope of use and select a service after judging whether it is acceptable or not to entrust your personal and privacy related information.**

9-3 Check how stored data is handled

You must be aware that using a cloud service (email, online storage, etc.) to upload your data is different from saving data on a PC (within the device). **In particular, many apps for smartphones upload data to the internet without the user realizing it.** When it comes to data stored on the internet, that storage area is also part of the service, which means that the data is entrusted to the service provider. **In addition, you must be aware of the potential ways in which the service provider may use the entrusted data.** Many free services operate around the idea of analyzing data uploaded by users for application to service improvements and business activities.

When entrusting highly confidential information, be sure to check the relationship between the rights and the owner of that data. (See Countermeasures 8-4 “Be conscious of the rights and laws concerning intellectual property and personal information, etc.”)

First, **search the clauses in the terms of service and privacy policy, etc. for any statements regarding whether the owner of the trusted data is the “user” or “provider.”** If it is the “provider,” check whether the information is such that it is okay to transfer all of the rights. If there is no mention of the data owner, you should either contact the provider and check or decide not to use the service.

Furthermore, even if you are the owner, there will definitely be written statements concerning the processing of data to provide the service or the submission of data at the request of a legal institution, etc. In addition, there may also be some cases where the provider has some form of rights that allow the provider to use your information for purposes in addition to the provision of the relevant service (there is a very strong tendency for free, consumer-oriented services to engage in such practices).

Be sure to check “who” can view and use the information that you have entrusted and “under what conditions.”

9-4 Check where the data is stored, applicable laws and the court of jurisdiction

In the case of important information, be sure to check which country your uploaded data is being stored in. The reason is that depending on the data storage location, the information will be handled based on the laws and culture of that country. Keeping that in mind, carefully check the data storage location according to the importance of the information.

Knowing the data storage location of an internet-based service clarifies what might happen to the entrusted information and how it must be handled according to the laws and regulations relating to data movement, actions under the personal information protection act of different countries, data auditing by administrative and judicial bodies, etc.

Many incidents involving the disclosure and loss of user information or information owned by users are occurring at internet-based services. These incidents occur for various reasons including unauthorized service access, configuration or operation errors on the service side, an inside job within the provider's (or outsource) organization, malware infections within the provider's organization, and large-scale disasters.

These incidents are similar to generally provided services and business outsourcing in the sense that the incidents occur in areas outside of the user's control, so the only way to reduce the possibility of experiencing such an incident is to choose a trustworthy service as discussed above.

When an information security incident occurs on the provider side, regrettably it is not possible to retrieve the leaked information or recover the lost data. Ultimately, you will have to claim compensation for damages through a lawsuit based on the provider liabilities described in the terms of service. In such cases, the applicable laws and court of jurisdiction are important. As much as possible, select a service that clearly states it operates under Japanese law and Japanese courts to avoid being placed at a disadvantage in a dispute which falls under the applicable laws and courts of a foreign country.

9-5 Prepare for data loss

There is always a risk of data loss due to system failure, configuration and operation errors, unauthorized access, etc. Although there are differences in the rate of incidence, you must anticipate the worst case in the systems world. In 2012, Firstserver, Inc. experienced an incident in which all of the data including the backups for their rental server service was lost. The loss included the data and email for over 5,500 customer websites. Some user data has also been lost at Gmail and Dropbox in the past.

When using an internet-based service, you must endeavor to choose a service where data loss is unlikely to happen, or backup the data on your own to protect against data loss.

You can find services where data loss is unlikely to happen by verifying the backup methods (how many levels of backup exist, whether backups are stored at multiple locations). Furthermore, you should consider ways to locally export and backup important data on your own so that even if it is lost by an internet-based service, you can take steps to recover the data from a different source.

9-6 Prepare for service content changes or service termination

In 2016, Parse.com, a provider of server-side processing services for mobile apps, announced that they were shutting down, and the impact of that announcement made headlines in Japan as well. There is a risk of service termination for reasons such as provider bankruptcy, policy changes resulting from an acquisition, deteriorating conditions and declining popularity, etc. Not only is there a termination risk, but free services may start charging a fee (change in the range of paid services) or the agreement and services offered may change.

Users always bear the risks of service termination and changes in the service offerings. When conducting important business or entrusting highly confidential information to an internet-based service, you must choose a service which reduces those risks and prepare in advance in case they actually occur.

As discussed in Countermeasures 9-1 “Choose a trustworthy service,” you should check the financial status and market share of the providers and select one with a high chance of service continuity to reduce such risks.

To prepare in advance, first refer to the clauses regarding service termination in the terms of service to check how many days in advance the provider must announce the termination, where it must be announced, and the descriptions of other details. Even if it says that advance notice is provided, it is important to take a backup similar to the case of data loss. Furthermore, you should search on a regular basis for ways to migrate to similar services and means of not relying on a service as well as make efforts to not become locked into that service.

Countermeasures 10 Other

So far, we have discussed various countermeasures, but this section explains the risks and countermeasures which do not fit into the previous categories.

2 key points about other risks

- 10-1 Erase data when transferring or throwing away devices
- 10-2 Do not use file-sharing software

10-1 Erase data when transferring or throwing away devices

Caution is required when transferring or throwing away PCs, smartphones, tablets, storage devices, USB memory, SD cards, and other devices or portable storage media if you have used them to store highly confidential information even once. The reason is, **when you use OS file operations such as “Empty Recycle Bin,” “Delete,” “Format disk,” and “Restore to factory settings,” in many cases the OS only throws away the data (file) management information without deleting the data (file) itself. Therefore, there is a possibility that the data can be recovered using specialized data recovery tools.** This leads to incidents where information is leaked from used PCs.

Therefore, be sure to follow the steps below to prevent any data from being recovered when throwing away devices or portable storage media that have been used to store highly confidential information.

PCs and storage devices

PCs and storage devices are equipped with removable hard disks, SSDs, and other memory devices.

(In the case of lightweight notebook PCs and compact PCs with memory devices that cannot be removed, please see the section below regarding smartphones and tablets.)

1. Specialized data erasing tools

For PCs and storage devices that are functioning normally, it is easy to use specialized data erasing tools. Manufacturers of storage devices and USB memory sometimes distribute free tools to erase data from their own products. Various other manufacturers provide both commercial and free tools, so please look for these.
Many tools do not support SSDs, so carefully check the type of memory in the device to select a tool with the proper support.

2. Encryption

When hard disks and SSDs, etc. are encrypted (see Countermeasures 5-4 “Encrypt highly confidential data”), the data cannot be decrypted without the PC that they were removed from, so throwing them away separately is another method of disposal.
Furthermore, deleting (or initializing) the data from an encrypted hard disk or SSD, decrypting the drive, and then encrypting the drive again can prevent data recovery.

3. Physical destruction

Physical destruction is an effective method in the case of disposal or a drive that fails and does not function. Remove the hard disk or SSD from the PC or storage device and destroy it using a drill or other tool. Be careful not to injure yourself when destroying the drive.

4. Disposal, collection, and used equipment companies

Disposal, collection, and used equipment companies provide data erasing services for a fee. No effort is required, but there are costs involved. Be sure to check the vendor's reputation and hire a trustworthy company. Some vendors also issue a data erasure certificate, which can be used as a way to measure their credibility. Some vendors also indicate the steps that you should take, such as erasing data, before a device is thrown away, collected, or purchased on their website, so be sure to check in advance.

Smartphones and tablets

Embedded memory cards are used as memory devices in smartphones and tablets. These memory devices are designed so that they cannot be removed from the smartphone circuit board. If you are using a smartphone from carriers such as docomo, au, or Softbank, steps 1 through 3 below can be performed at each carrier's outlets.

If you are using the "Osaifu-Keitai" electronic money system, the data remains on the IC chip even if the device is initialized, so be sure to delete the data in advance. Generally speaking, the data will disappear if you carry out the data migration procedure for each electronic money system. If you are using a smartphone provided by a carrier, they will initialize the IC chip after the data migration.

1. Restoring the factory settings (device reset)
After encrypting a smartphone, you can prevent data from being recovered by restoring the factory settings. IOS is encrypted by default, but on Android and Windows 10, users must encrypt the device themselves. Restore the factory settings with the device in an encrypted state.

2. Physical destruction
In the case of an embedded memory card, because it fundamentally cannot be removed from the device, destroy the entire device with a drill or other tool.

3. Disposal, collection, and used equipment companies
If you ask a non-carrier shop to collect a mobile device, choose a trustworthy vendor as you would with a PC or storage device.

Portable storage media

Finally, we have USB memory, SD cards, CDs, DVDs, and other forms of portable storage media.

1. Specialized data erasing tools
As with hard disks and SSDs, the manufacturers of USB memory and SD cards often provide specialized data erasing tools, so please look for them.

2. Physical destruction
If you have access to a media shredder, check if it supports the type of media that you would like to throw away and use the shredder to physically destroy the media. SD cards, CDs, DVDs, etc. are comparatively easy to destroy using cutting nippers and other tools. Fragments may scatter, so be careful not to injure yourself when destroying the storage media.

3. Disposal and collection companies
There are also companies that provide data erasing and disposal services for USB memory and other portable storage media, so choose a trustworthy vendor as you would for PC and storage devices.

Refer to the following guidelines for users from the Japan Electronics and Information Technology Industries Association (JEITA).

- 「パソコンの廃棄・譲渡時におけるハードディスク上のデータ消去に関する留意事項」(“Points to consider regarding the erasing of data on a hard disk when disposing or transferring ownership of a PC”)[28]
- 「ストレージ上のデータ消去に関するガイドライン」(“Guidelines regarding the erasing of data on a storage device”)[29]
- 「メモリカードの廃棄・譲渡時における内部のデータ消去に関するユーザ向けガイドライン」(“Guidelines for users regarding the erasing of internal data when disposing or transferring ownership of a memory card”)[30]

[28,29,30] This document is Japanese only.

10-2 Do not use file-sharing software

Although you rarely hear about this type of software these days, back in the 2000s there were applications starting with WinMX, Winny, Share, and other P2P file sharing software (or file exchange software) that would search files on a user's PC to share (exchange) with other users.

Users relentlessly shared movies, TV shows, music, books, software, and other copyright infringing content, or what are called “pirated versions.” This behavior was viewed as a problem as it grew in popularity, and it is said that there were several hundred thousand such users just in Japan.

The first problem with P2P file-sharing software is that the purpose for many users is “to obtain copyright infringing content.” It is a crime to publish the works of another person on the internet and share them with third parties (see Countermeasures 8-4 “Be conscious of the rights and laws concerning intellectual property and personal information, etc.”).

The second problem is that there is a high risk of malware infection due to the large number of attackers who use the P2P file exchange software networks to distribute malware that is disguised as copyright infringing content.

The third problem is malware such as Antinny that misuses the features and networks of P2P filesharing software. When a system is infected with such a virus, various data files on the PC are unintentionally shared (exchanged) with the P2P network. Such viruses attracted attention around 2004 as the cause of information leaks. After information leaks caused by malware through the Winny network were reported in 2006, it became a social problem, and the Japanese government and other organizations warned users to stop using P2P filesharing software.

Because of these problems, Winny, Share, Perfect Dark, Cabos, and other file sharing software must not be used. In addition, while BitTorrent may be used to download large, multi-gigabyte files, it must not be used for illegal purposes.

Ref: NetAgent, 2015年最新P2P利用状況調査 (2015 Latest Survey of P2P Usage)[31]
http://www.netagent.co.jp/product/p2p/report/201501/01.html

[31]This website is Japanese only.

Chapter3

If an information incident occurs

The “Countermeasures to Prevent Information Incidents” section of Chapter 2 explained ways to prevent information incidents. However, as cyber attacks are becoming more advanced and elaborate every day and human errors cannot be avoided, much like traffic accidents, information incidents cannot be completely prevented from happening. Therefore, **it is important to treat information incidents as something that can happen to anyone and understand in advance what actions you should take if it does happen.**

This chapter explains the appropriate response to take when “an information incident happens” for each type of anticipated incident.

Emergency point of contact if an information incident occurs

When an information incident occurs on a network, the damage quickly spreads, so you must rapidly take the appropriate action during the “initial response” no matter what type of information incident has occurred. Furthermore, centrally managing the cause of the incident and the response and sharing information within the university helps prevent a recurrence of the incident.

If an information incident unfortunately does occur, take the appropriate response based on the “Response examples by type of information incident” described below and promptly report the incident and confer with the following “Emergency Contact Desk.”

Information Security Incident Emergency Contact Desk

http://www.ritsumei.ac.jp/rainbow/security-contact-ritsumei/

*Information incidents can happen to anyone, so you will not be held personally responsible by reporting an incident to the emergency contact desk.

Response examples by type of information incident

This section explains the appropriate response to take according to the type of information incident. Incidents which require a more rapid response are noted with the icon Initial Response . When an information incident occurs, carry out the initial response before contacting the Information Security Incident Emergency Contact Desk.

Responding to malware infections

Malware infections are a type of information incident which often go unnoticed by users and are instead discovered and pointed out by others. In some cases, such as ransomware, users directly realize the damage when a message demanding the payment of a ransom is displayed or their files become locked. The damage caused by a malware infection can rapidly spread and has a significant scope of impact, so quickly take the following actions.

Response

1 Disconnect from the network Initial Response

Remote operation, unauthorized transfers of money to online banks, external cyber attacks, proliferation to peripheral devices, and other forms of secondary damage spread through the network. Therefore, to prevent the damage from spreading, disconnect the infected device from the network by unplugging the LAN cable for a wired connection and turning off the physical switch (or turning off the OS settings if there is no switch) for the wireless LAN (Wi-Fi) for a wireless connection.

2 Backups

The information stored on an infected device may be infected by the malware, so caution is required when handling such information. If you must make a backup of the information, backup the data to external media.

3 Recovering an infected device

To use an infected device once again, perform a clean install of the OS or restore the device to the factory settings before use.

Responding to ID and password theft

Even if unauthorized access occurs as a result of ID and password theft, in many cases the users do not realize what has happened. Depending on the service, the theft may become apparent through change notification emails that they know nothing about, unauthorized login warning notifications, and by checking the login history. In some cases, a user may be contacted about a possible ID and password leak due to an information incident caused by another person.

If your ID and password are stolen, promptly take the following actions.

Response

1 Change your password Initial Response

Change your password so that the damage does not spread.

If your password has been changed and you cannot access the account, contact your system provider (Administrator) to ask for support.

2 Check the service settings

If your ID and password are stolen and an attacker fraudulently logs into your account, the service settings may be changed in a malicious way, so check the service settings.

If your university ID and password are stolen, check the email system and other service settings which use the university ID (in the case of the email system, the settings may be changed to forward messages to the attacker’s email address).

Responding to mobile devices or external media loss, information missending and unintentional information sharing

If you lose a smartphone, notebook PC, or other mobile device and it is found by a malicious person, the personal information on the mobile device may be stolen or the person may gain unauthorized access to websites using IDs and passwords saved on the device.
If USB memory, an external hard disk drive, or other storage media is lost, there is also a risk that the information stored on the lost external media may be leaked.
Sending an email in error or publishing information due to incorrectly configuring the scope of sharing in online storage, etc. may also lead to an information leak.

Take the following actions for information incidents which involve the risks of such “information leaks.”

Response

1 (For mobile devices) Delete the information or lock the device

Initial Response

If you configured the remote wipe feature as discussed in Countermeasures 7-1 “Take steps so that information is not accessed if a device is stolen or lost,” run the feature right away.

Furthermore, if you lost a smartphone or other mobile device with a service subscription, contact the mobile carrier and consult with them about taking the following actions.

- Search for the general location
- Lock the device
- Temporarily suspend the line service

2 Check the stored information

Clarify the confidentiality of the stored information as well as the scope and extent of the impact if the information were leaked.

3 Report the occurrence of an information incident

If the device contained highly confidential information such as personal information, promptly notify all parties which may be affected by that information (faculty members should contact their supervisor).

Personnel involved in the operation management of information systems (Guidelines)

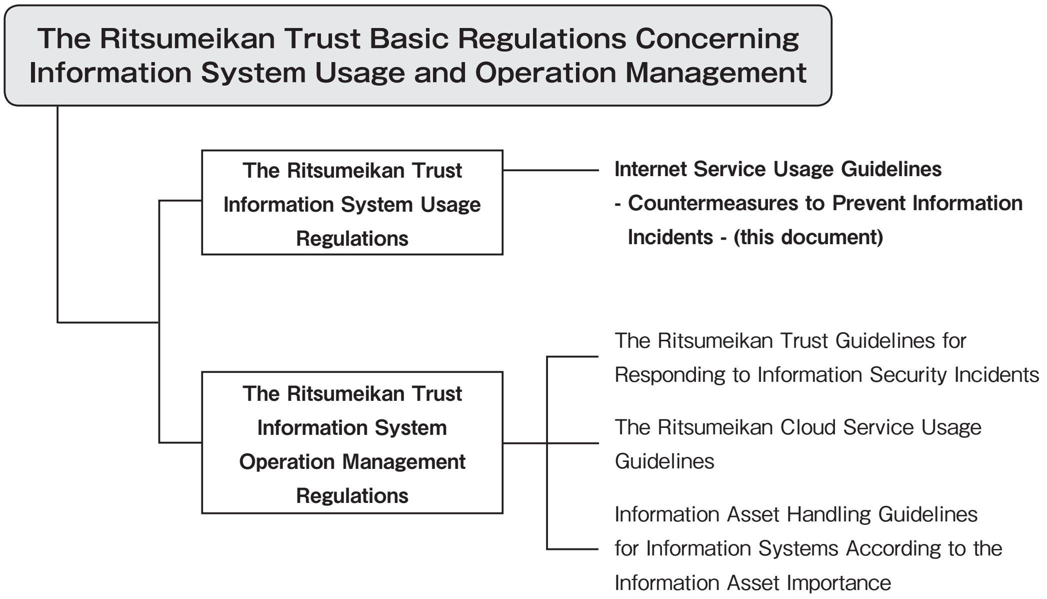
At this university, we are drawing up for operational administrators of information systems **"The Ritsumeikan Trust Guidelines for Responding to Information Security Incidents[32]"** which summarizes the precautions and specific countermeasure policies for responding to information security incidents, so personnel involved in the operation of information systems should be sure to check these guidelines.

[32] This guideline is Japanese only. A reference translation will be made in 2020.

Appendix A Related regulations

In addition to these guidelines, there are regulations and guidelines that you should pay attention to when using an information environment. **Faculty members should be sure to check the following regulations and guidelines.**

Information Security Related Regulations[33] and Guidelines[34]



The Ritsumeikan Trust Basic Regulations Concerning Information System Usage and Operation Management
The Ritsumeikan Trust Information System Usage Regulations
Internet Service Usage Guidelines - Countermeasures to Prevent Information Incidents - (this document)
The Ritsumeikan Trust Information System Operation Management Regulations
The Ritsumeikan Trust Guidelines for Responding to Information Security Incidents
The Ritsumeikan Cloud Service Usage Guidelines
Information Asset Handling Guidelines for Information Systems According to the Information Asset Importance

Fundamental points of risk management[35]

In the event that an information management or security incident occurs, report to the Risk Management Committee using the specified format.

The Ritsumeikan Trust Personal Information Protection Regulations[36]

Under Article 16, it establishes, “In regard to the handling of personal information, in the event that it is determined that the facts run counter to these regulations, such facts must be promptly investigated and reported to the school manager in charge of personal information.” Furthermore, the Secretariat (section and office) has a responsibility to contact the General Affairs Section by telephone in accordance with the situation and submit the "Personal Information Protection Case Reporting Sheet" using the specified format.

[33,36] These English Regulations are translation of the original Japanese document and is for reference only.
[34] These Guidelines are Japanese only. A reference translation will be made in 2020.
[35] This document is Japanese only.

Reference data

IPA (Information Technology Promotion Agency)

情報セキュリティ読本 (Information Security Reader (book))[37]
ISBN978-4-407-33076-2

対策のしおりシリーズ (Countermeasure Bookmark Series (Distributed PDF))[38]
http://www.ipa.go.jp/security/antivirus/shiori.html

IPA Technical Watch
標的型攻撃メールの傾向と事例分析＜2013年＞ (Trends and case study analysis of targeted attack emails <2013>)[39]
～ますます巧妙化、高度化する国内組織への標的型攻撃メールの手口～ (Techniques of targeted attack emails aimed at Japanese organizations becoming more elaborate and advanced)

IPA Technical Watch
標的型攻撃メールの例と見分け方 (Examples and ways to distinguish targeted attack emails)[40]

NISC (National Center of Incident Readiness and Strategy for Cybersecurity)

ネットワークビギナーのための情報セキュリティハンドブック（Ver.2.11） (Information Security Handbook for Network Beginners (Ver.2.11))[41]
http://www.nisc.go.jp/security-site/handbook/

Ministry of Internal Affairs and Communications

国民のための情報セキュリティサイト (Information security web site for citizens)[42]
http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/

Council of Anti-Phishing Japan

利用者向けフィッシング詐欺対策ガイドライン（2016年度版）(Phishing Fraud Countermeasure Guidelines for Users (2016 Edition))[43]
https://www.antiphishing.jp/report/guideline/

LAC (LAC Co., Ltd.)

Cyber GRID View vol.1
日本における標的型サイバー攻撃の事故実態調査レポート (Targeted Cyber Attack Incident Field Survey Report for Japan)[44]
https://www.lac.co.jp/lacwatch/report/20141216_000198.html

JNSA (NPO Japan Network Security Association)

JNSA2014年情報セキュリティインシデントに関する調査報告書 (JNSA 2014 Research Report on Information Security Incidents)[45]
JNSA2015年情報セキュリティインシデントに関する調査報告書 (JNSA 2015 Research Report on Information Security Incidents)[46]
JNSA2016年情報セキュリティインシデントに関する調査報告書 (JNSA 2016 Research Report on Information Security Incidents)[47]
http://www.jnsa.org/result/incident/

図解入門ビジネス最新ISO27001 2013の仕組みがよ～くわかる本 (How - nual Business Guide Book on Understanding the Latest ISO27001 2013 System)[48]

Written by Kazuo Uchikawa, Shuwa System Co., Ltd.
ISBN978-4-7980-3982-4

徹底攻略 情報セキュリティマネジメント教科書 平成28年度 (Complete Strategy: Information Security Management Textbook, 2016)[49]

Written by Mizuki Seto and Kenichi Saito at Wakuwaku Study World Co., Ltd.
Impress Corporation
ISBN978-4-8443-3987-8

[37,48,49] This book is Japanese only.
[38,39,40,41,42,43,44,45,46,47] This website is Japanese only.

INDEX

Internet Service Usage Guidelines

Date issued: December 1, 2019

Edited by: Ritsumeikan Information Infrastructure Improvement Committee

Issued by: The Ritsumeikan Trust
1 Nishinokyo-Suzaku-cho, Nakagyo-ku, Kyoto 604-8520

Printed and bound by: Ishida Taiseisha Inc.

RITSUMEIKAN