Information Security Training

“Information Security Measures” for Protecting Information Assets

Information assets handled by educational and research organizations that must be protected:

- Student information
- Operational information
- Research information
- Alumni information
- Client information, etc.

Information Security

Maintaining the **confidentiality, integrity, and availability** of information assets

In this training, “Information security” covers **digital data** among various information assets.

Confidentiality	Only allowing authorized persons to access information	**Information leaks** **Unauthorized access**
Integrity	Maintaining the information one possesses in an accurate and complete state	**Data falsification** **Data loss**
Availability	Allowing authorized persons to access information whenever they need it	**Service discontinuation** **Operations discontinuation**

Information Security Measures

Human, physical, and technical measures for protecting information assets from **information security threats,** causing information security incidents.

Information security incidents:
Events that (may) lead to loss of information security

Human Security	Preventing the occurrence of “human” negligence	• Establishing regulations and guidelines • Conducting teaching, training, etc.
Physical Security	Measures for “items” you can touch	• Fixing your PC with an antitheft wire • Controlling access to areas where PCs are installed, etc.
Technical Security	Measures for “data” you cannot touch	• Installing security software • Setting passwords, etc.

Information Security Threats

Threats Covered in this Training

- Cases of incidents within Ritsumeikan
- Items needed special attention in educational or research institutions

Cyber attacks — ★ Malware ★ Phishing ★ Tech support scams ★ Targeted attacks

Human error — ★ Careless information leaks

Internal irregularities

Information-technology Promotion Agency (IPA), Japan "10 Major Security Threats"

The IPA selects threats after receiving reports of information incidents and disseminates information (alerts, vulnerabilities, specific countermeasures, etc.).

The selection committee includes security experts and corporate executives, **and they rank the threats in each year by individual and organization.**

Last year's order	Individual	order	Organization	Last year's order
1st	Fraudulent use of individual information through phishing ★	**1st**	Damage from ransomware ★★	1st
2nd	Libel, slander, and spreading false information online	**2nd**	Malicious attacks on vulnerabilities in supply chain	3rd
3rd	Financial demands through threats and fraudulent tactics using email, SMS, etc.	**3rd**	Theft of confidential information using targeted attacks ★★★	2nd
4th	Fraudulent use of credit card information	**4th**	Information leaks due to internal irregularities	5th
5th	Fraudulent use of smartphone settlement	**5th**	Attacks targeting the "new normal" working style, including telework, etc.	4th
7th	Damage to smartphone users by illegal apps	**6th**	Attacks targeting the period before a modified program is released (zero-day attack)	7th
6th	Internet fraud involving tech support scams ★	**7th**	Financial damage caused by business email compromise (BEC) ★★	8th
8th	Theft of personal information from internet services	**8th**	Increase in malicious attacks following release of vulnerability measure information	6th
10th	Illegal login to internet services ★	**9th**	Damage from careless information leaks ★	10th
Out-of-range	Financial damage because of inappropriate billing, such as one-click billing, etc.	**10th**	Commercialization of crime (underground services)	Out of range

10 Major Security Threats 2023: Information-technology Promotion Agency (IPA), Japan https://www.ipa.go.jp/security/10threats/10threats2023.html

Information System Regulations and Guidelines (System Diagram)

Basic Regulations	Regulations	Guidelines
The Ritsumeikan Trust Basic Regulations Concerning Information System Usage and Operation Management	The Ritsumeikan Trust Information System Usage Regulations	**Internet Service Usage Guidelines**
	The Ritsumeikan Trust Information System Operation Management Regulations	Information Asset Handling Guidelines for Information Systems According to the Information Asset Importance
		The Ritsumeikan Trust Information System Operation Management Guidelines
		The Ritsumeikan Trust Cloud Service Usage Guidelines
		The Ritsumeikan Trust Domain and Server Certificate Usage Guidelines
	The Ritsumeikan Trust CSIRT Operation Regulations	**The Ritsumeikan Trust Guidelines for Responding to Information Security Incidents**

This training
is intended as an introduction to guidelines
for system users.

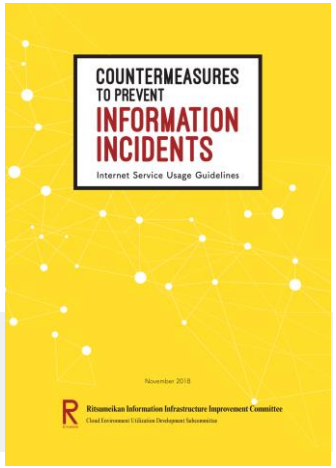
RITSUMEIKAN IT SUPPORT

Regulations and Guidelines

Guidelines for Information System Users

Internet Service Usage Guidelines

We shall explain some specific information security measures that should be adopted to prevent information security incidents in advance while discussing some cases as examples.



Use the **checklist**
to check your own level of understanding!

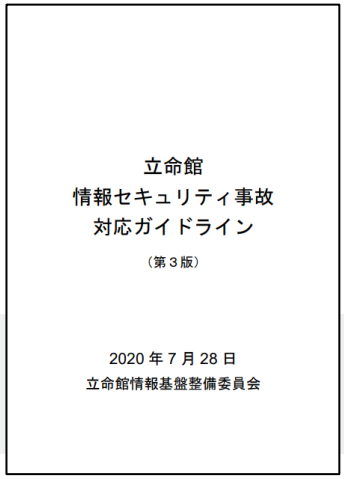
Measure 1 ★	Malware (viruses)	Measure 6 ★	Access rights (sharing)
Measure 2 ★	IDs and Passwords	Measure 7	Mobile devices, such as smartphones
Measure 3 ★	Web	Measure 8	Personal information and the infringement of rights
Measure 4 ★	Email	Measure 9	Service usage
Measure 5	Transmission and storage (encryption)	Measure 10	Others

RITSUMEIKAN IT SUPPORT

Internet Service Usage Guidelines

The Ritsumeikan Trust Guidelines for Responding to Information Security Incidents

Guidelines for information system users and information system operation administrators on the necessary response flow and response details in the event of an information security incident.


立命館
情報セキュリティ事故
対応ガイドライン
（第３版）
2020 年 7 月 28 日
立命館情報基盤整備委員会

For **rapid response when incidents occur**,
it is necessary to confirm what to do in advance!

Chapter2	Preparation in anticipation of information security incidents 1. Ascertaining the response system when an information security incident occurs 2. Ascertaining the contact flow when an information security incident occurs
Chapter 3 ★	Responding rapidly and appropriately when an information security incident occurs 1. For information system users: Flow and content of response (2. For information system managers: Flow and content of response)
Chapter 4	Reviewing and sharing of information after information security incidents

RITSUMEIKAN IT SUPPORT

The Ritsumeikan Trust Guidelines for Responding to Information Security Incidents

Content Covered in the Training

[A] Information Security Threats and Incident Cases

[A-1] "Malware" Cyber Attack
- Damage and outbreak factors
- Case (Emotet)

[A-2] "Phishing" Cyber Attack
- Damage and outbreak factors
- Case

[A-3] "Tech Support Scams" Cyber Attack
- Damage and outbreak factors
- Case

[A-4] "Targeted Attacks" Cyber Attack
- Damage and outbreak factors
- Case (phishing + ransomware)

[A-5] Human Error

[B] Information Security Measures

[B-1] Important Considerations While Using Email/Web
- Always be cautious of fraud and phishing
- Do not relax security settings
- Use the "latest" setup for the user environment

[B-2] Appropriate Account Management
- Appropriate password setting management
- Multifactor authentication settings
- Check sign-in history

[B-3] Precautions to Take While Sharing Files
- Beware of human errors
- Selection of appropriate file sharing methods
- Setting of appropriate access rights

[C] Response When an Incident Occurs

Information Security Threats and Incident Cases

Malware Damage and Outbreak Factors

[A-1]

Malware General name for malicious software.

Damage — Infected with malware

- Data corruptions
- Illegal communications (remote operations) to steal information

Connected to the network while infected with malware

Possibility of spreading malware to other devices, systems, and services through the network

Risk of large-scale information leaks and operational shutdowns

Factors — Malware infection routes

Downloading and installing **files** or software **with malware**

Email attachments
Download from the **website**

Malware infection because of neglecting of **vulnerability countermeasures**

- Usage of an old OS, application or web browser, etc.
- Relaxation of the security functionality settings on PC or web browser
- Failure to deploy security software

Common Types of Malware

	Virus	Modifies part of the program and self-propagates
Bot	**Worm**	Exists individually but self-propagates
	Trojan horse	Infiltrates by disguising itself as a useful program, etc.
Key logger	**Spyware**	Conceals itself inside the PC and steals information
	Backdoor	Your PC can be operated from an external point
Tech support scams	**Adware**	Displaying unauthorized advertising, etc. without permission
Emotet	**Botnet**	Automatically executes processes Bot set group
	Ransomware	Encrypts files and demands money in exchange for unlocking them

✓ **Emotet**
Spreads globally since 2019.
Information leak incidents have occurred at many educational institutions within Japan.

Case

✓ **Ransomware**
Targeted attacks are conducted and led to large-scale business shutdown.

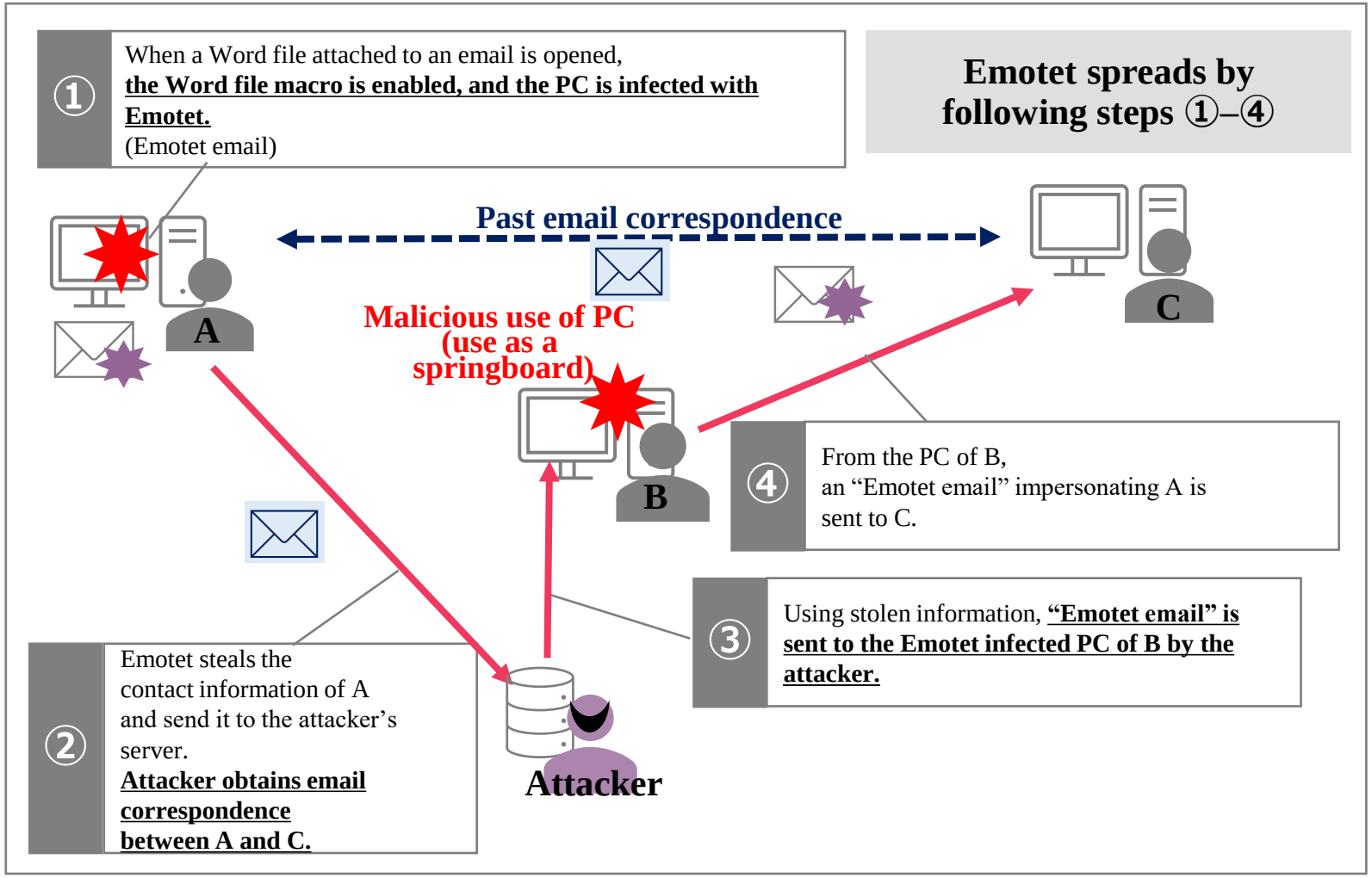
Case

Point

- Every day, new types of malware are created, and these cannot all be detected by security software.
- From “individual damage” to “large-scale attacks targeting organizations.”
- Most incidents are caused by **individual email and web use**.

Case Malware “Emotet”

[A-1]



- When a file in a malicious Word format is attached and the Word macro is enabled and it provides a way for the attacker to infiltrate, thereby infecting the PC with Emotet.
- When it is infected with Emotet, **ID/password information and personal information are stolen, email accounts are used as a springboard**, and “Emotet” emails are dispersed maliciously both internally and externally to A’s organization.
- As Emotet emails **steal emails used for correspondence in the past and are sent as replies to those past emails,** the recipient does not notice that they are Emotet emails.

Countermeasure

Do not casually open attachments when **receiving emails.**

Necessary steps for safely using email:

- **Always keep OS/software updated**
- **Implement security software**

Phishing Damage and Outbreak Factors

[A-2]

Phishing

Fraudulent acts in which information is stolen by luring users to a fake website impersonating a real organization and forcing them to enter personal information.

Damage

Stolen information and malicious use of information

Information entered in phishing site
ex) Name, address, email address,
credit card information, ID/password

Status of stolen information

May be sold on the black market
and **maliciously used for various attacks**

Consequence of stolen ID/passwords

May be used to get **illegal access to systems and services**

Reusing Ritsumeikan ID/passwords is prohibited

Factors

Common patterns in phishing

Fake authentication screens **may be displayed for the purpose of stealing IDs/passwords**

- Receiving **emails/SMS impersonating actual organizations**
  ex) Financial organizations, electronic commerce (EC) site, post office, home delivery company, administrative institutions
  One's own organization's system department/system administrator
  System notifications from email and storage services, etc.
- **Content that provokes a sense of crisis**, suggesting that damage will occur unless you do something.
- A fake site is displayed when accessing the URL in the main body of the email.

The actual email address and URL are impersonated;
the email body is not unnatural and resembles with the real one;
and all of these become more and more sophisticated and difficult to detect with time.

Point

- Beware of email/SMS with content that provokes a sense of crisis.
- Stolen information may be maliciously used by attackers in a variety of ways.

Case Phishing

[A-2]

NG The displayed sender name is “MS-Enterprise”, but the email address domain differs from the official Microsoft one.

⚠ There also have been **cases where the malicious party pretended to be a Ritsumeikan system administrator.**

Phishing email

Keep or Change for XXXXXX

Ms Enterprise
宛先 XXXXXX@st.ritsumei.ac.jp

Ms Enterprise

Contact

Official domain microsoft.com

no-reply@tipply.pl

Display details

Microsoft

XXXXXX@st.ritsumei.ac.jp password is set to expire today dd/mm/yyyy...

Keep Password

You can keep or change your password so you do not get locked out of your account...
Regards

The information contained in this message and any attachments is intended only for the use of the individual or entity to which it is addressed and may contain Information that is privileged confidential and exempt from disclosure under applicable law if you have received this message in error you are prohibited from copying
Distributing or using the information please contact the sender immediately by return email and delete the original message...

Access the link given in the main body of the email

Official domain https://login.microsoftonline.com/common/oauth...

NG The URL domain is different from the **official Microsoft domain.**

Phishing site

Sign in
https://youpleaesseto.info/

As the attacker already has your email address,
when you enter the password, both your email address and password will be stolen.

Microsoft

Enter password

Password

Keep me signed in

Forgot my password

Use the Microsoft Authenticator app instead

Sign in

Countermeasure

- As the displayed sender’s name and link can be falsified, **check the domain in the email address and in the URL link.**
- If you do not recognize an email, you should **directly contact the official contact point for the sender’s organization.**

Official Domain	School	Domain
	Ritsumeikan University/affiliated schools	ritsumei . ac . jp
	Ritsumeikan Asia Pacific University	apu . ac . jp
	The Ritsumeikan Trust	ritsumeikan-trust . jp

Domain

This is a name or address that is registered on the internet and employed to differentiate between computers and networks in the internet.

Examples of highly trusted domains		
	ac.jp	Institutions of higher education or educational corporations
	ed.jp	Primary or secondary educational institutions and educational institutions for children under the age of 18
	go.jp	Japanese government agencies, research institutions under the jurisdiction of ministries and agencies, special corporations, and independent administrative corporations
	lg.jp	Local government organizations and administrative services provided by such organizations

Point

Check delimiters, such as dots (.) and slashes (/):

[URL] up to first slash (/) after "https://"

[Email address] after the @ mark

OK

PDF page published on the RITSUMEIKAN IT support site under the title "Internet service usage guidelines":

https://**it.support.ritsumei.ac.jp**/hc/article_attachments/4410975757593/guideline-internetservice.pdf

Domain | Location of the displayed file | Name of the displayed file

NG

Hyphens are used in the domain section to make it resemble the official domain

https://**it.support.ritsumei-ac-jp.com**/~~~

Domain

The section other than the domain uses the same characters as the public domain

https://**it.support.com**/ritsumei/ac/jp/~~~

Domain

Domain is not ac.jp

https://**it.support.ritsumei.xyz**/~~~

Domain

There are some services that do not use the official domain even when provided by Ritsumeikan; therefore, please inquire the contact point for the relevant service if you cannot verify if it is a genuine service or not.

Damage Caused by Tech Support Scams and Outbreak Factors

[A-3]

Tech support scams

Method of attack where false warning messages are displayed while viewing websites to cause anxiety.

Damage

If you follow warning messages

If you click the warning message

You will access a website for malware distribution and be **infected by the malware.**

If you make an inquiry to a fake support site

When one follows the instructions, illegal software has been installed, which steals **one's remote operation privileges.** **Thus, malware is installed and information is stolen.** **Financial demands are then made as a support fee**.

Factors

Reasons why people are tricked by tech support scams

Why a false warning message is displayed?

- **Web browser notification settings** may be added and changed while you are browsing the web unintentionally.
- You are infected with adware (malware) displaying false warning messages.

Why are people tricked by tech support scams?

As the **content and method of the notification trigger anxiety,** the user is placed in a situation where he/she cannot think clearly and make rational decisions.

Characteristics of tech support scams that trigger anxiety

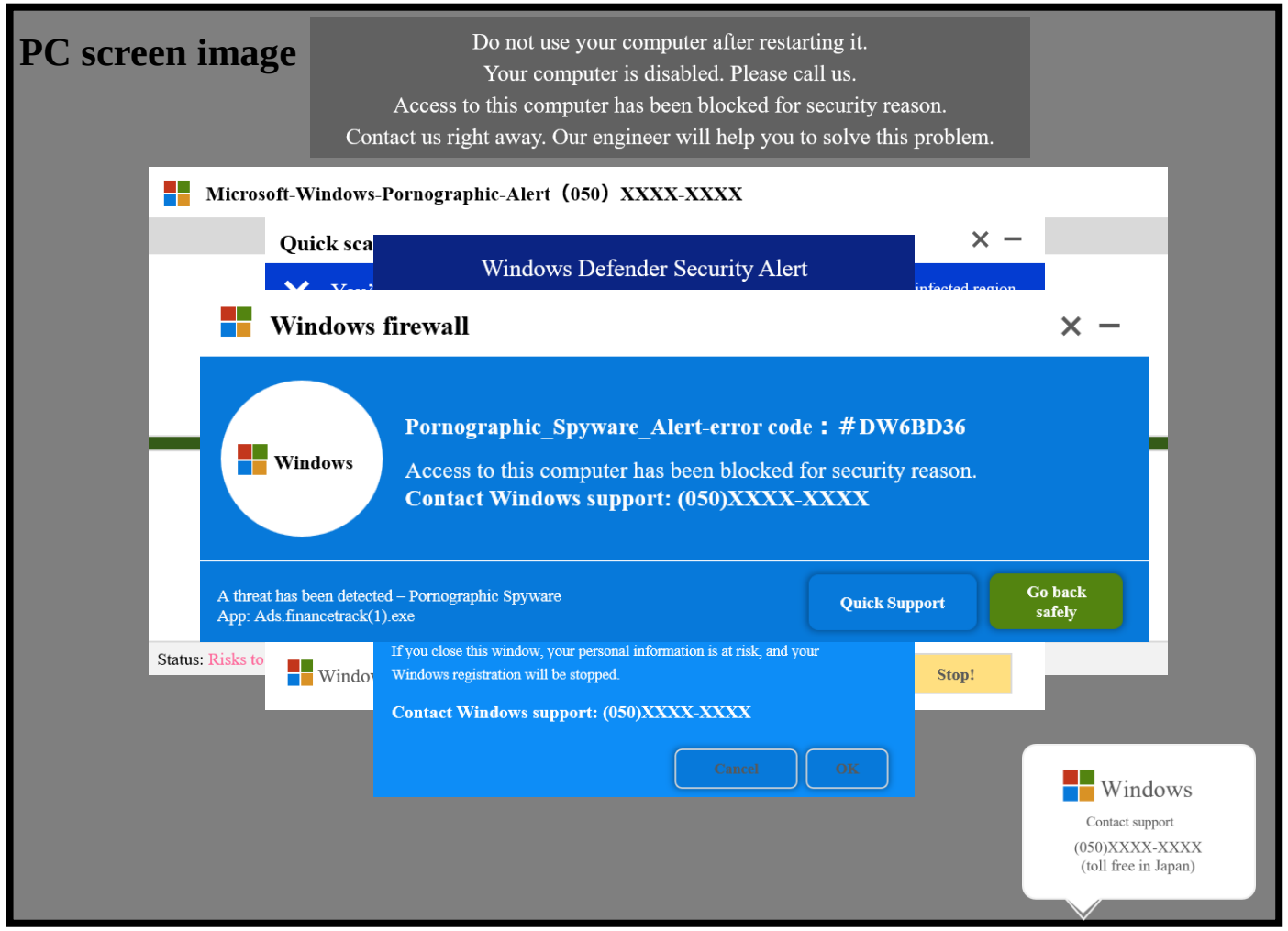
- Notifications open with a series of warnings and they are fixed in a full-screen display. As the "Close" button is hidden, it is not possible to close the screen.
- Loud warning sounds and warning announcements play relentlessly.
- These warnings use the logos of actual companies and services and often use those of PC security functions and antivirus software specifically.

Point

Do not get tricked when the content and method of notification trigger anxiety, and understand the case so that you can make rational judgments.

Case Tech Support Scams

[A-3]



Security warning notifications are displayed one after the other, and loud warning sounds and announcements are played.

If you contact the telephone number displayed, you will be connected to an operator who speaks in imperfect Japanese.

They instruct you to install software and remotely control the system while falsely claiming that an error has occurred.

They will recommend you to select a fee-based support agreement and make you enter personal information on a fake site.

Countermeasure

- Do not allow web browser's notifications easily.
- Do not easily click warning notifications.
  (risk of malware infection)
- Do not call the telephone number displayed in the warning notification.
  (a telephone number is not normally included in a genuine warning screen)

In the case of a remote operation:

- As it is difficult to identify the type of attack, **it is recommended that you reformat your PC**.

Targeted Attacks

[A-4]

Targeted Attacks

Cyber attacks with the purpose of **stealing confidential information or obstructing the operations of specific organizations** use more sophisticated attacks to infiltrate organizations.

Large-scale Damage

Ransomware

Phishing

- As advanced attacks are launched against **specific organizations, such attacks are difficult to notice.**
- **Educational and academic institutions** with student information **and research information are targeted by attackers.**

Targets the "**individual**" in an organization and uses malware infection and account theft as an entry point for large-scale attacks

Cyber attacks targeting academic-related/think tank researchers, etc. (reminder)

National center of Incident Readiness and Strategy for Cybersecurity (NISC)/The Cyber Affairs Bureau of the National Police Agency November 30, 2022

Characteristics

- **Emails** are sent from people pretending to be employees or members of real organizations, **requesting lecturers for events, lectures, interviews, or introducing materials or manuscripts**.
- **URL links are included in the body of email** correspondence regarding the coordination of schedules and content, or **files will be attached with names, such as materials, manuscripts, etc**. If you click the said URL or open the attachment, you will be infected with malware.

ex) Sending email addresses

- Display name (name of person being spoofed) <a suspicious email address that you do not recognize>.
- <name of person being spoofed>@<symbol of organization being spoofed>.com
- <name of person being spoofed>@<symbol of organization being spoofed>.org
- <name of person being spoofed>@<well-known free email※ domain>

※ yahoo.co.jp, gmail.com, outlook.com, etc.

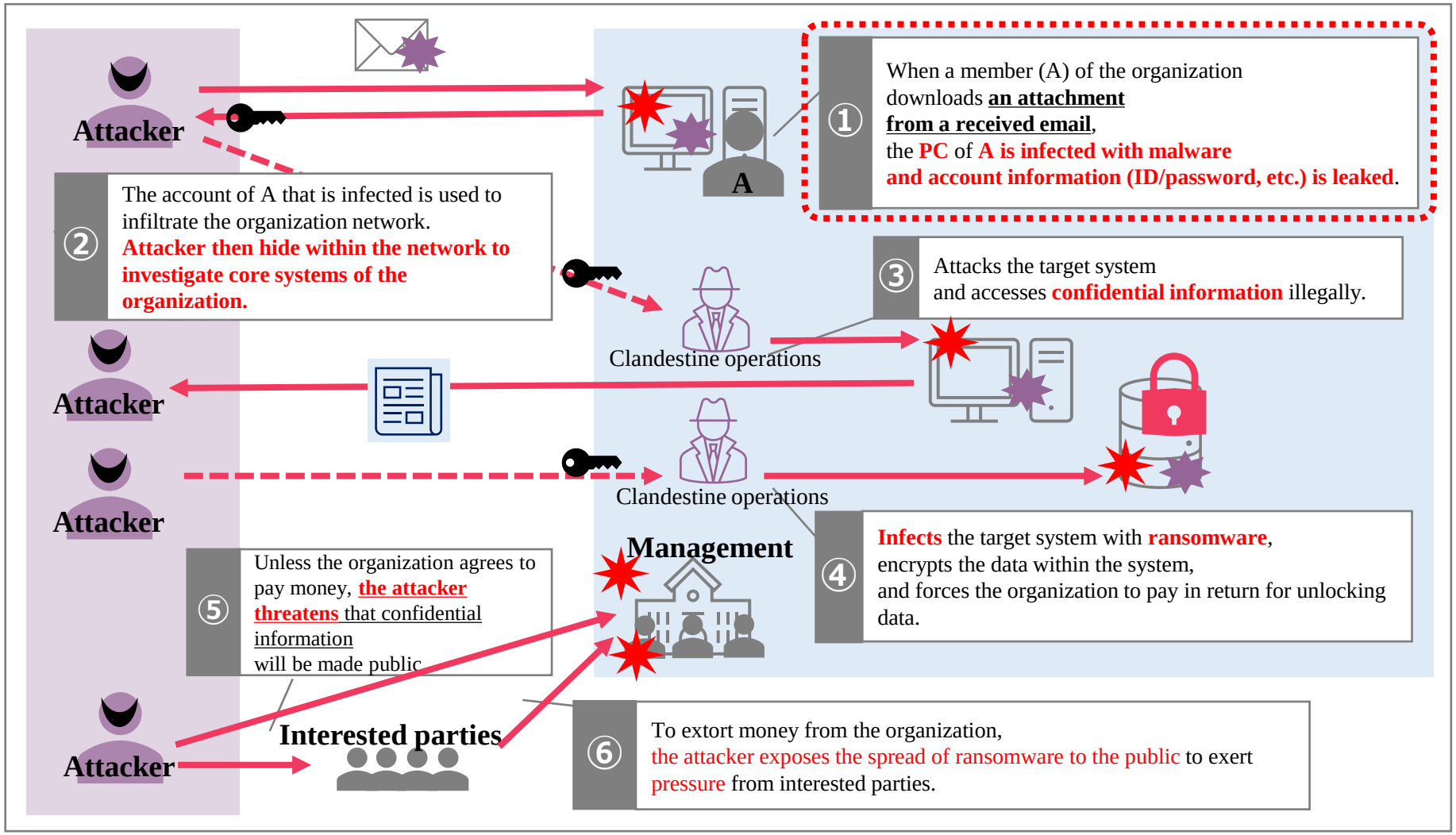
ex) Email subject

- [Request] Please allow us to interview you
- Request to participate as guest at research meeting [●●●●●●※]
- [Attendance request] ●●●●●● *Study meeting

※● contains the name of a real organization, etc.

Case Targeted Attacks

[A-4]



Example of an email targeting A — Targeted Email

- Spoofed email that impersonates members of an actual organization from whom A receives e-mails.
- A separate stolen email account is used to send a related email based on the contents of past correspondences.

Purpose of targeted attacks

Against individuals
- Research information of academic-related personnel

Against organizations
- Stealing students' personal information
- Stealing confidential information, such as operational information.
- Demands for money
- Obstruction of business activities

Ransomware

Countermeasure

Malware and phishing measures to prevent account theft

Case Human Error

[A-5]

Case①

When sending a blanket email,
one should put all recipients in BCC but
mistakenly put them in CC.
The contact email addresses could be seen by
all email recipients.

Only if you have a habit of checking the recipient before sending email

Case ②

The **students share PC with another** user while
still signed into private email and OneDrive,
and thus, others could view the contents of
the email and OneDrive.

Only if you follow clearly set rules when using shared PCs

Case③

A **USB memory** device with
files, including information assets have been **lost.**

A password is set for the file; however, it was
a **simple password** that is easy to guess.

Only if you set a strong password

Case④

Files containing information assets
are stored in online storage (of an organization service),
and a **link is shared by email**.

Access rights are not
set for the online storage, and hence,
any recipient of the email
could access it.

Only if you were using online storage that have access rights

Case⑤

Files containing information assets are sent as attachments, but
it is sent to a gmail email address
mistakenly typed as "**～@gmai.com.**"

Doppelganger domain problem

The mail with the attachment and **the email with the password are sent to the same wrong email address.**

PPAP problem

Page. 23

Point

It is essential to not only prevent human error "from occurring" but
also take necessary **measures to keep information leaks to a minimum**!

Information Security Measures

Important Considerations While Using Email/Web

[B-1]

Always be cautious of fraud and phishing

- ✓ **Before opening emails**
- ✓ **Before downloading attachments**
- ✓ **Before accessing links within the body of the email**

Recognize **"suspicious" points** and do not easily allow access/downloading.

- ☐ **Confirm that the domain is correct** for email addresses and URLs.
- ☐ When confirming account information and billing information, do not access them through a link provided in an email body but confirm by **directly accessing from the official website.**

Do not relax security settings

Ritsumeikan's email uses the Microsoft security functionality, and thus, email suspected of malware or phishing is isolated before reaching the inbox (email quarantine function). **Check the quarantine notification email, and do not remove any emails other than those that are clearly detected as threat.**

RITSUMEIKAN IT SUPPORT What is Email quarantine

Use the "latest" setup for the user environment

- ✓ **Software (OS/application)**
- ✓ **Web browser**
- ✓ **Network equipment (routers, etc.)**

To eliminate vulnerabilities that serve as entry points for cyber attacks, use the latest version **(automated updates recommend).**

Be sure to check the **alert information sent out by the Ritsumeikan CSIRT** regarding the cyber attack cases reported by Ritsumeikan and **security-related information provided by government agencies, etc.**

RITSUMEIKAN IT SUPPORT RITSUMEIKAN IT Support Site **Notification**

Authentication

Check the identity of the user.

Method of authentication				
	①	Knowledge information	Information known only to the person concerned	Password, PIN number, Secret questions, etc.
	②	Possession information	Items owned only by the person concerned	Smartphone Hardware token , Employee ID, IC card, etc.
	③	Biometric information	Physical characteristics of the person concerned	Fingerprints, Face, Iris, Retina, Veins, etc.

Ritsumeikan ID uses ① and ② for Multifactor authentication

Multifactor authentication

To increase security strength, an authentication method is used that combines multiple authentication methods from ① to ③.

- To prevent unauthorized access, it is necessary for each authentication method to be highly protected.
- There is a high risk of knowledge information being stolen by cyber attacks:
  - Phishing
  - Malware infection
  - Account list attack
  - Brute-force attack (round-robin attacks)

To prevent illegal access in advance

- **Manage appropriate password setting**
- **Set up multifactor authentication**
- **Check access history**

Authorization

Enable only permitted users to access.

When file sharing

- **Select appropriate file sharing methods**
- **Set appropriate access rights**

Appropriate Account Management

[B-2]

Appropriate Password Setting Management

- ☐ Set **strong passwords** that are hard to guess.
- ☐ **Never reuse passwords** from other services.
- ☐ **Never share passwords with other people.**

Points to note when setting passwords:
- Do not use dictionary words or proper nouns.
- Use 8 or more characters (at least 12 characters are recommended).
- Use a combination of uppercase, lowercase, numbers, and symbols.
- Use conversion rules and anagrams that are easy to remember.

If you reuse passwords, passwords used in other services could be leaked, and risk of cyber attack increases.

Reference) **Have I Been Pwned** https://haveibeenpwned.com/
Website from which you can check your account information (combination of email address/password) regarding previous personal information leak incidents.

Multifactor Authentication Settings

For Ritsumeikan accounts, multifactor authentication is mandatory.
When using other services, set available multifactor authentication.

If you receive an unexpected request for multifactor authentication,
do not approve the request and check your sign-in history.
If there are any sign-ins that you are unaware of,
please **change the password immediately.**

Check Sign-in History

Microsoft365
My sign-ins (Preview)
https://mysignins.microsoft.com/

Ascertain what type of sign-in history is logged from everyday use in advance, and regularly check for suspicious history.

If a suspicious sign-in is detected in your Ritsumeikan account, you will be sent a notification email.
Once you receive the email, promptly implement security measures.
If there are any sign-ins that you are unaware of, report this to the RAINBOW service desk.

Precautions to Take While Sharing Files

[B-3]

Beware of Human Errors

Ensure that information leaks due to email mistaken transmissions caused by email address mistakes or wrong selection of CC or BCC do not occur.

When sharing files using attachments, human error can easily occur and as "transmission errors" corresponds to "information leaks." Therefore, **measures to keep information leaks to a minimum** are essential!

Selection of Appropriate File Sharing Methods

Select an appropriate method of sharing files according to rules for handling information assets in Ritsumeikan (and other similar regulations).

Low

Confidentiality

High

- **Email Attachments**
  Considering the nature of email (possibility of communication route sniffing),
  avoid handling sensitive information.
- **Online Storage**
  As this is stored on an external network,
  keep the storage time to a minimum.
  Manage account properly.
  Set appropriate access rights.
- **Office File Server** (only for office staffs)
  As these are saved on the campus network,
  set appropriate access rights.

The customary method of sending confidential files by email, **in which "a Zip file with a password is attached to an email"** is **not recommended from a security perspective**, so use file sharing based on online storage (see the following slide for details).

Method of using external services

RITSUMEIKAN IT SUPPORT

Utilize OneDrive

Setting of Appropriate Access Rights

Be mindful of who should have access to the information and set appropriate access rights (Authorization).

PPAP

Method of **sending a Zip encrypted file with a password** as an attachment and **sending the password by email.**

PPAP is not effective against recent security threats.
As it is a method with a high security risk for both sender and recipient, avoid using this method.

P : Send a **P**assword-attached Zip encrypted file
P : Send the **P**assword
A : Encryption = **A**ngoka(暗号化) in Japanese
P : **P**rotocol

Reason it is not recommended

If the file is encrypted,
the email system's malware detection function and security software will not function efficiently.

It is customary to send the password-attached Zip file and password using the same method (email); however, this is not an effective countermeasure in terms of transmission errors and account theft.

- If you send the email to a wrong address, the password will also be sent to the same address and the person receiving it can open the file.
- If an information security incident occurs for either the sender or recipient, the email account may be stolen or configured to automatically forward the email to the attacker.

Point

When sending files (sharing), do not use "PPAP", which has a high security risk. Instead, utilize **online storage in which access rights are appropriately set (e.g., OneDrive, etc.).**
After sharing files, delete them rather than leaving them on the online storage.

Response When an Incident Occurs

Response When an Incident Occurs

[C]

By taking a prompt initial response when you think an incident may have occurred, you can limit damages to a minimum!

Account Theft

Initial response

Malware Infection

① **Unplugging (disconnecting) from network**
② **Changing password**
③ **Malware scan (removal)**
④ **Check access history**
⑤ **Checking account settings**

Make sure to **record content of response** so that your report is organized over a timeline!

RITSUMEIKAN IT SUPPORT

Change your password and check email system settings

Report to Ritsumeikan CSIRT

- **Circumstances in which incident occurred**
  Why do you think an incident has occurred?
  What were you doing when it occurred?
- **Content of initial response**
  What did you do before making the report?
- **Damage status**
  What kind of usage environment was it?
  Network to which you were connected when the incident occurred
  Devices used
  What information assets were potentially affected?

RITSUMEIKAN IT SUPPORT

【For those on campus】Ritsumeikan CSIRT Information Security Incident Emergency Point of Contact (PoC)

Secondary measures

Instructions from Ritsumeikan CSIRT

※ Possible **leak of personal information**
→ **Need to report** to the **Office of General Affairs**