10 Major Security Threats 2022

～People believe someone must have taken countermeasures.
There shouldn't be such a sweet deal!～

[For Organizations]

IT Security Center (ISEC)
Information-Technology Promotion Agency (IPA), Japan
July 2022

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

What is “10 Major Security Threats”？

- Report issued by IPA every year since 2006
- IPA determines candidate threats based on security incidents and attack cases/trends in the previous year
- “10 Major Security Threats Committee” which consists of system operators in organizations and security professionals etc. votes for candidate threats
- IPA explains the outline, damage cases, and measures, etc. of “10 Major Security threats” selected from the vote

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

Characteristics of “10 Major Security Threats”

Threats to various entities and people

Threats to watch out are different depending on the entity or people

- People who use computers or smartphones at home, etc.

“Individuals”

- Organizations such as companies or government agencies
- System administrators, employees, and staff of the organization

“Organizations”

IPA explains threats from two perspectives: “Individuals” and “Organizations”

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

10 Major Security Threats
- Threat Ranking

Threats for Individuals	Rank	Threats for Organizations
Phishing Fraud for Personal Information	1	Ransomware Attacks
Cyberbullying and Fake News	2	Confidential Information Theft by APT
Extortion of Money by Blackmail or Fraudulent Methods with Email, SNS, etc.	3	Attacks Exploiting Supply Chain Weaknesses
Fraudulent Use of Leaked Credit Card Information	4	Attacks on New Normal Work Styles such as Teleworking
Fraudulent Use of Smartphone Payment	5	Information Leakage by Internal Fraudulent Acts
Internet Fraud by Fake Warnings	6	Increase in Exploitations following the Release of Vulnerability Countermeasure Information
Malicious Smartphone Applications	7	Attacks Targeting before the Release of Security Patches (Zero-day Attacks)
Personal Information Theft from Services on the Internet	8	Financial Loss by Business Email Compromise
Unauthorized Use of Internet Banking Credentials	9	Suspension of Business due to Unexpected IT Infrastructure Failure
Unauthorized Login to Services on the Internet	10	Unintentional/Accidental Information Leakage

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

Basic Security Measures

- Various threats, but “Attack Vectors” can be categorized to some major attack vectors
- Importance of basic security measures has not changed for many years
- Always keep the below ”Basic Security Measures” in mind

Attack Vectors	Basic Security Measures	Purpose
Software Vulnerability	Keep software up to date	Eliminate vulnerabilities and reduce risk from attacks
Virus Infection	Use antivirus software	Block attacks
Password Theft	Use strong password and authentication	Reduce risk from password theft
Improper Configuration	Review configurations	Prevent attacks targeting improper configuration
Social Engineering	Know about threats and attack methods	Understand measures which should be focused on

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

”Additional” Basic Security Measures

- Use of cloud services is becoming more common these days
- Need to prepare "additional" basic security measures assuming the use of cloud services

Target of Preparation	Additional Basic Security Measures	Purpose
All incidents	Clarify (understand) the scope of responsibility	Clarify (understand) who (which organization) is responsible for responding to incidents
Cloud Service Outage	Prepare alternative plans	Prepare alternative plans to ensure that business operations do not stop
Cloud Service Specification Change	Review settings	Correct settings that were unintentionally changed due to specification changes (prevent information leakage or exploitation to attacks due to inadequate settings)

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

10 Major Security Threats 2022 For Organizations

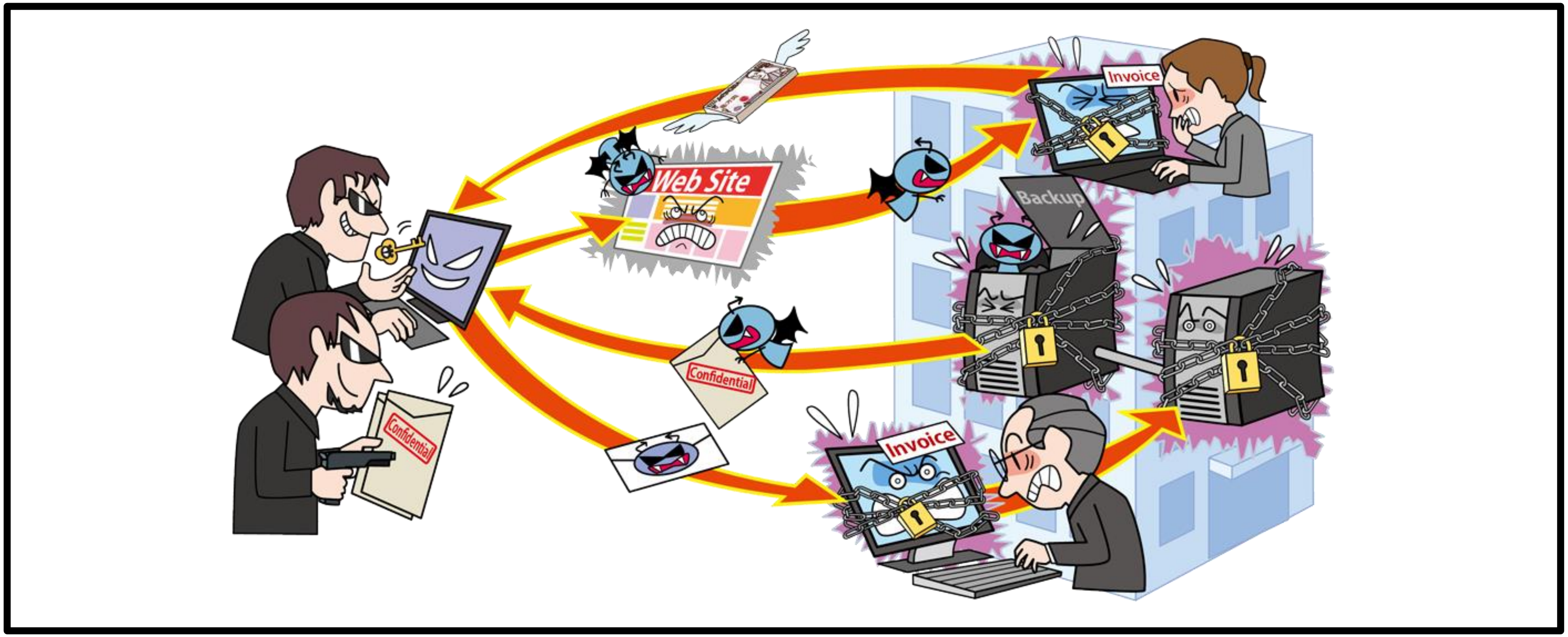
Explanation of Each Threat

※”Basic Security Measures” described in the previous section is assumed to be implemented and is not included in the following description.

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【1】Ransomware Attacks

～Social infrastructures can be severely impacted～



- Encrypt files stored on computers, etc. with ransomware and make them unavailable
- Extort money in exchange for restoration of encrypted files
- In some cases, threaten to make the stolen information public unless a ransom is paid

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【1】Ransomware Attacks

〜Social infrastructures can be severely impacted〜

● Attack Methods

- Infect computers with virus (ransomware) and extort money

■ Emails

- Trick a target user into opening an attachment
- Forcing users to click on links in emails

■ Drive-by downloads from compromised websites

- Tamper with websites to trick a target user into downloading ransomware
- Trick a target user into browsing the tampered websites using email, etc.

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【1】Ransomware Attacks

〜Social infrastructures can be severely impacted〜

● Attack Methods

- Infect computers with virus (ransomware) and extort money

Exploiting Vulnerabilities

- Exploit software vulnerabilities to execute (infect) virus
- Infect computers one after another over the network using exploit kits, etc.

Unauthorized Access

- Gain unauthorized access to target's servers via remote desktop used for the purpose of management, etc.
- Execute (infect) virus on accessed servers

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【1】Ransomware Attacks

〜Social infrastructures can be severely impacted〜

● Cases and Trends in 2021(1)

Ransomware attack on a hospital in Tokushima

- In October 2021, the system of a hospital in Tokushima Prefecture was infected with ransomware, and electronic medical records and accounting system became inaccessible.
- Although ransom was demanded for decryption, the hospital refused.
- The hospital stopped accepting new patients until the system was restored.
- In January 2022, regular medical care was resumed.

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【1】Ransomware Attacks

～Social infrastructures can be severely impacted～

● Cases and Trends in 2021(2)

Prolonged damage due to backup encryption

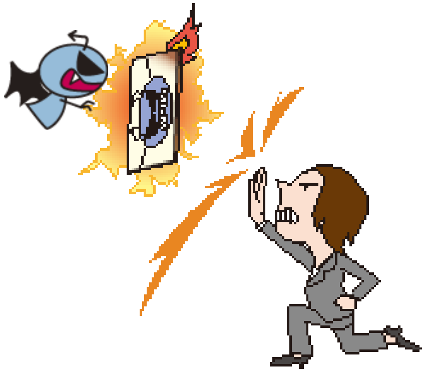
- Flour mill company was cyber attacked and infected with ransomware.
- Server that managed the online backup of the system was also encrypted.
- Early recovery was unable and filing the company's quarterly financial reports was delayed.

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【1】Ransomware Attacks

〜Social infrastructures can be severely impacted〜

- Countermeasures
  - Senior Management
    - Establishment of organizational framework
      - Secure budget for countermeasures and perform countermeasures continuously
      - Assign a CIO or other responsible person with expertise



Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【1】Ransomware Attacks

～Social infrastructures can be severely impacted～

Countermeasures

System Administrators, Employees

- Preventions
  - Establish CSIRT that can respond promptly and continuously
  - Enable multi-factor authentication settings
  - Don't easily click on attachments and URLs
  - Don't run software of unknown origin
  - Expedite equipment vulnerability countermeasures
    - Apply patches promptly
    - Stop using OS that are no longer supported
  - Use security tools and review settings
    - Restrict application execution and enable email and web filtering
    - Review policy settings and enable blocking settings as much as possible

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【1】Ransomware Attacks

～Social infrastructures can be severely impacted～

● Countermeasures

System Administrators, Employees

- Preventions
  - - Segregate networks
  - - Minimize access privileges of shared servers and strengthen administration
  - - Take countermeasures to prevent unauthorized access to public servers
  - - Perform backups

    ※Consider backups with reference to "3-2-1 Backup Rules"

    ※Regularly check that you can recover from the backups

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【1】Ransomware Attacks

〜Social infrastructures can be severely impacted〜

● Countermeasures

System Administrators, Employees

- Actions after attack detected

  - Report to and consult with predefined contacts in accordance with the organization's policy
    ※Supervisors, CSIRT, related organizations, public agencies, etc.
  - Recover from backups
  - Use decryption tools
  - Investigate impact and detect causes, strengthen countermeasures
  - Execute quarantine quickly to prevent expanding the damage to related organizations and business partners

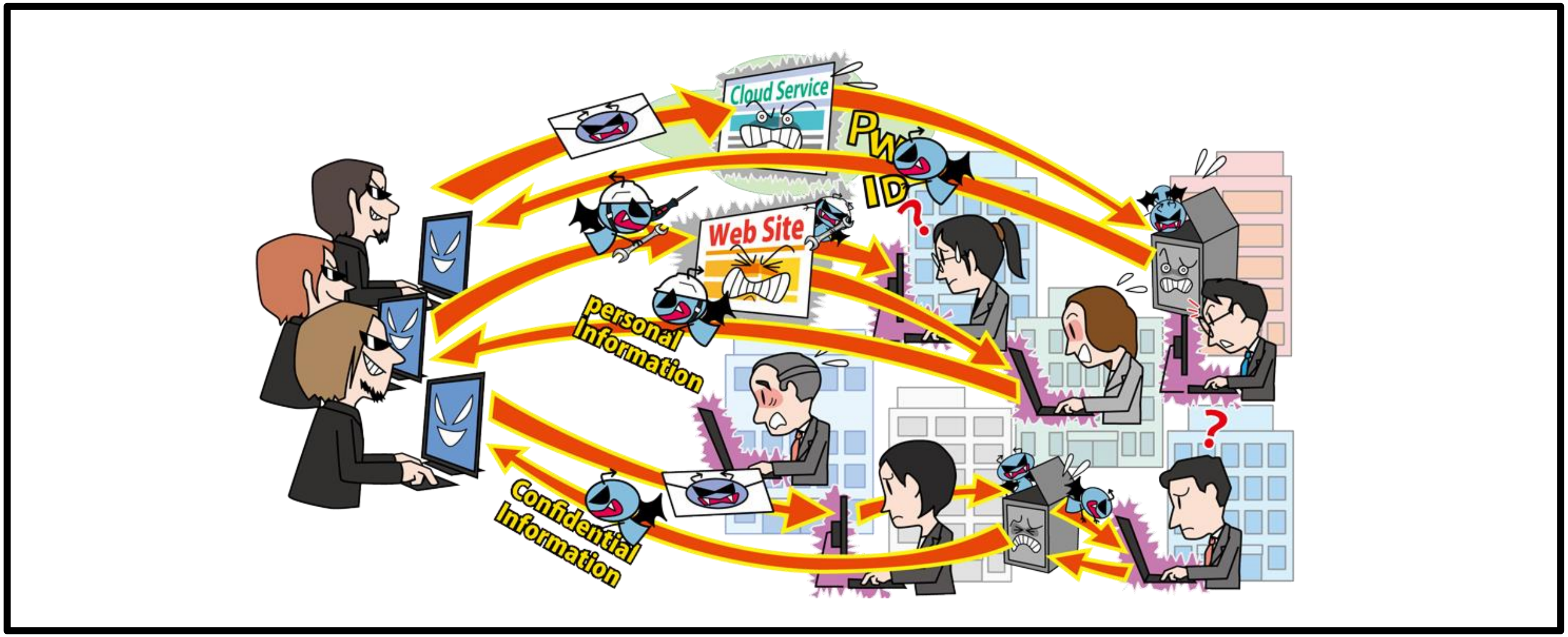
<Exceptional measure>

Although not recommended, there have been cases in the past where the company paid ransom due to the organization's circumstances (e.g., when encrypted files are life-threatening).

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【2】Confidential Information Theft by APT (Advanced Persistent Threat)

〜Cyber attacks are becoming more organized〜



- Infect computers of a specific organization with virus by email, etc.
- Infiltrate the organization's network and gradually increase the impact range of attacks for long periods
- Steal the organization's confidential information or disrupt systems of the organization

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【2】Confidential Information Theft by APT (Advanced Persistent Threat)

〜Cyber attacks are becoming more organized〜

Attack Methods

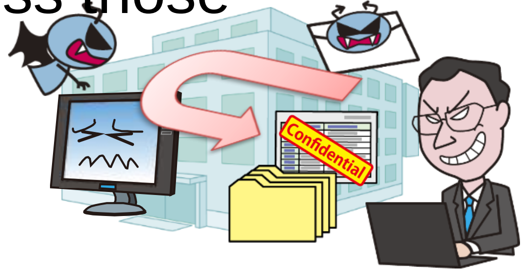
- Infect the target of attack with virus by email, website, etc.

Targeted Email Attacks

- Trick the target to open malicious attached files
- Trick the target to click on links to falsified websites

Watering Hole Attack

- Observe websites which the target organization often use
- Tamper with those websites to download viruses
- Employees of the target organization access those websites and get infected with viruses



Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【2】Confidential Information Theft by APT (Advanced Persistent Threat)

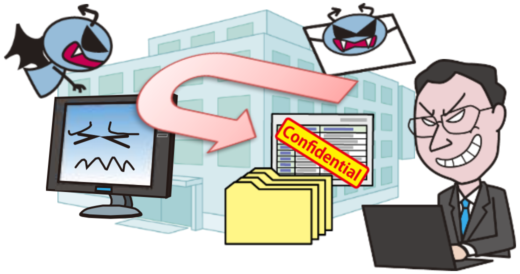
～Cyber attacks are becoming more organized～

Attack Methods

- Gain unauthorized access and steal credentials
- Infiltrate the in-house system and infect it with virus

Unauthorized Access

- Gain unauthorized access to cloud services, web servers, or VPN used by the target organization and steal credentials, etc.
- Infiltrate the in-house system via legitimate routes by exploiting the stolen credentials, and infect computers or servers with virus



Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【2】Confidential Information Theft by APT (Advanced Persistent Threat)

～Cyber attacks are becoming more organized～

● Cases and Trends in 2021(1)

Information leakage from information sharing tool

- In May 2021, a major system integrator announced that a project information sharing tool provided by the company had been illegally accessed.
- Some of the information entrusted by customers was leaked.
- The tool was used for project management (development process, source, task management, etc.) for such as system development among the company, group companies, external partners, and customers.

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【2】Confidential Information Theft by APT (Advanced Persistent Threat)

～Cyber attacks are becoming more organized～

● Cases and Trends in 2021(2)

Information sharing on cyber attacks

- Reports from the Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP)
- Reports of information on cyber attacks to IPA from J-CSIP participating organizations
- Information considered to be APT attack email in 2021: 36 cases
- [Reports from July to September 2021] Although it is unclear whether this was targeted attack, URL link information was embedded in an image file downloaded from free illustration material site which the rapporteur frequently used. Security software detected it as an invalid file.

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【2】Confidential Information Theft by APT (Advanced Persistent Threat)

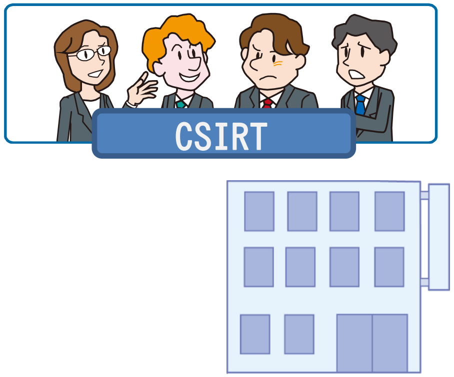
〜Cyber attacks are becoming more organized〜

- Countermeasures
  - Senior Management
    - Establishment of organizational framework

      - Establish CSIRT that can respond promptly and continuously

      - Secure budget for countermeasures and perform countermeasures continuously

      - Develop a security policy



Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

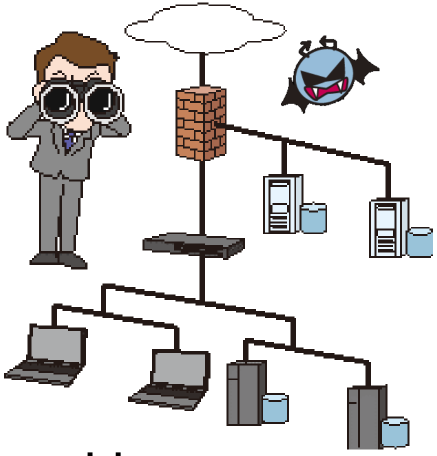
【2】Confidential Information Theft by APT (Advanced Persistent Threat)

～Cyber attacks are becoming more organized～

- Countermeasures

Information Security Officers, System Administrators

- Preventions / Improvement of response ability



- Manage information and develop rules
- Collect information on cyber attacks continuously
- Implement cybersecurity trainings for employees
- Implement incident response drills regularly

  ※Establish response and communication methods with relevant personnel, security vendors, and specialists
- Apply security patches to management terminals continuously
- Understand the status of security measures using integrated operation management tools, etc.

  ※Visualize risks by managing the software update status of PCs used by employees and staff

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

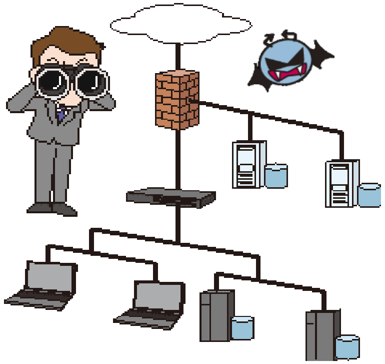
【2】Confidential Information Theft by APT (Advanced Persistent Threat)

～Cyber attacks are becoming more organized～

● Countermeasures

Information Security Officers, System Administrators

- Preventions / Improvement of response ability
  - Create and maintain an application permission list
  - Minimize access privileges and strengthen administration
  - Segregate networks
  - Fortify critical servers (access control, encryption, etc.)
  - Understand the implementation status of security measures of business partners
  - Improve security measures including overseas offices, etc.



Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【2】Confidential Information Theft by APT (Advanced Persistent Threat)

～Cyber attacks are becoming more organized～

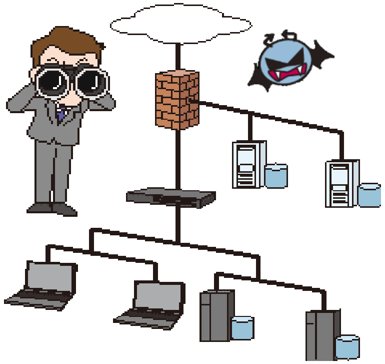
- Countermeasures
  - Information Security Officers, System Administrators
    - Early detection

      - Implement UTM, IDS / IPS, WAF, Virtual patching, etc.

      - Monitor and defend endpoints using EDR, etc.
    - Actions after attack detected

      - Respond to the incident with CSIRT operation

      - Investigate impact and detect causes, strengthen countermeasures



Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【2】Confidential Information Theft by APT (Advanced Persistent Threat)

～Cyber attacks are becoming more organized～

- Countermeasures
  - Employees, Staff
    - Preventions (usually organization-wide)

      - Do not easily click on attachments or links
    - Actions after attack detected

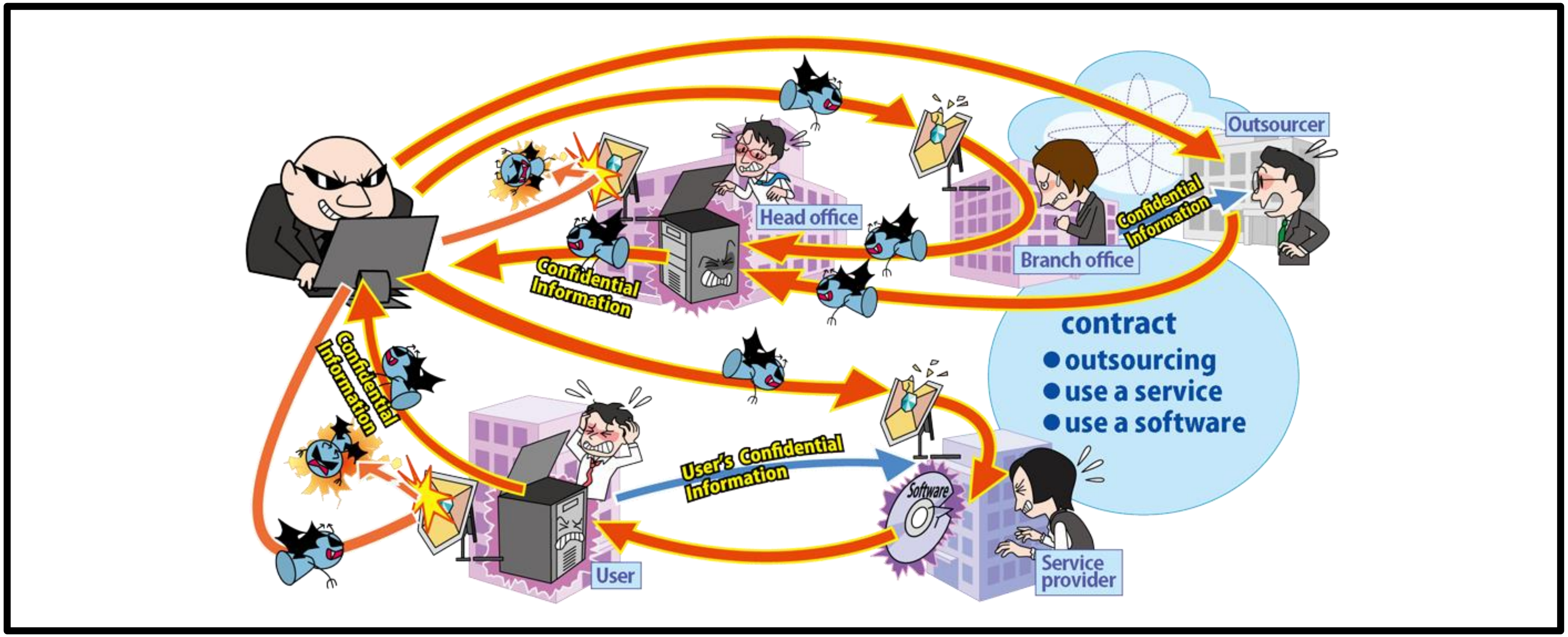
      - Report to and consult with predefined contacts in accordance with the organization's policy

      ※Supervisors, CSIRT, related organizations, public agencies, etc.

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【3】Attacks Exploiting Supply Chain Weaknesses

〜As supply chain attacks are on the rise globally, review the risks once again〜



- In a series of supply chains such as procurement of raw materials and parts, manufacturing, inventory control, logistics, sales, outsourcing, etc., organizations with weak cybersecurity measures are targeted as a foothold of attacks
- Information leaks from business partners, or outsourcing partners which are delegated partial work

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【3】Attacks Exploiting Supply Chain Weaknesses

～As supply chain attacks are on the rise globally, review the risks once again～

Attack Methods

- Target organizations with weak security measures

  - Attack business partners/outsourcing partners/ contractors of the target organization and steal their confidential information regarding the target organization
  - Attack software developers, MSP (Managed Service Providers; third-party company that manages a customer's corporate network, etc.), etc. as a foothold to attack the target
    - Embed virus in a software update to infect users who apply the update, etc.

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【3】Attacks Exploiting Supply Chain Weaknesses

〜As supply chain attacks are on the rise globally, review the risks once again〜

- Cases and Trends in 2021(1)
  - Global increase in supply chain attacks
    - Number of supply chain attacks targeting open-source software (OSS) exceeded 12,000 in 2021, approximately 650% increased from 2020.
    - Among engineers who operate cloud services, etc., 36% have experienced incidents such as information leakage, and 83% are concerned that companies are vulnerable to information leakage caused by misconfiguration of cloud services.

【3】Attacks Exploiting Supply Chain Weaknesses

〜As supply chain attacks are on the rise globally, review the risks once again〜

- Cases and Trends in 2021(2)
  - Ransomware attacks on subsidiaries and overseas offices
    - In April 2021, a U.S. subsidiary of a Japanese optical equipment manufacturer suffered a ransomware attack.
    - Approximately 300 GB of data which contains financial and customer information, etc. was stolen and published on the dark web.
    - Cybercrime group issued a criminal statement.

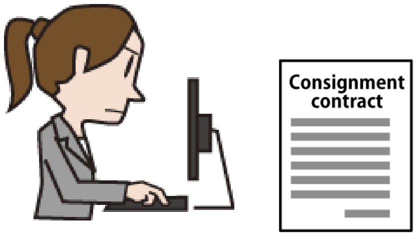
Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【3】Attacks Exploiting Supply Chain Weaknesses

〜As supply chain attacks are on the rise globally, review the risks once again〜

Countermeasures

Organizations



- Preventions
  - Enforce rules for outsourcing and information management
  - Implement operational rules of incident response including a reporting structure
  - Select trustworthy business partners or outsourcing partners
  - Consider multiple potential business partners
  - Verify deliverables
  - Confirm the coverage of the contract
  - Manage outsourcing partners
- Actions after attack detected
  - Investigate impact and detect causes, strengthen countermeasures
  - Compensation to damage or impact of the attack

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【3】Attacks Exploiting Supply Chain Weaknesses

〜As supply chain attacks are on the rise globally, review the risks once again〜

● Countermeasures

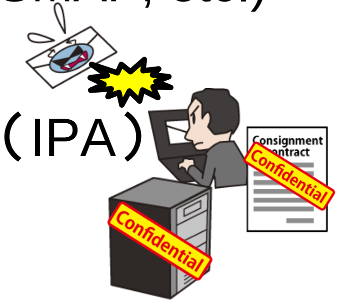
Organizations (Organizations involved in supply chains)

- Preventions

  - Confirm and audit information security measures of business partners and contractors
  - Obtain security certifications (ISMS, Privacy mark, SOC2, ISMAP, etc.)
  - Utilize documents published by public authorities

    「Preparation for security threats against supply chains」（IPA）

    「Cybersecurity Management Guidelines」(METI/IPA)



- Actions after attack detected

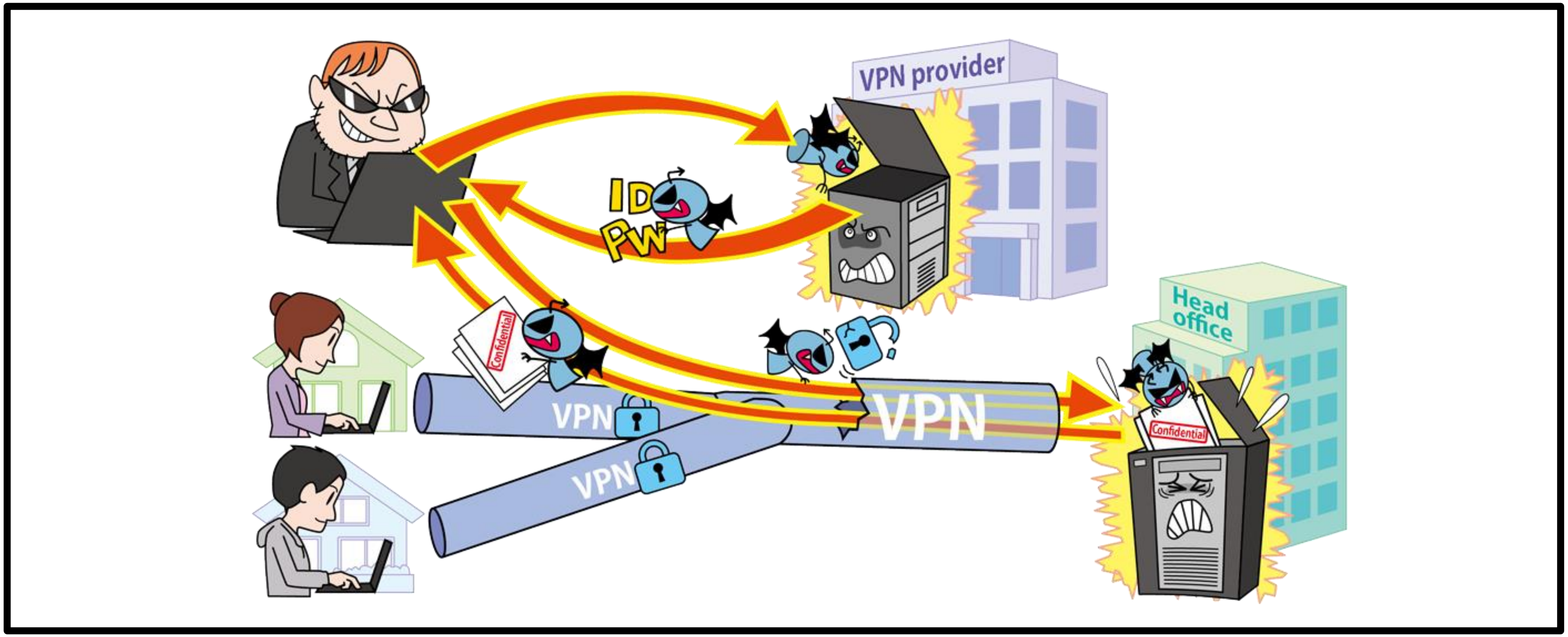
  - Report to and consult with predefined contacts in accordance with the organization's policy

    ※Supervisors, CSIRT, related organizations, public agencies, etc.

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【4】Attacks on New Normal Work Styles such as Teleworking

～ Security for teleworking requires cohesion between the company and its employees ～



- Teleworking became widespread due to COVID-19 pandemic began in 2020
- As utilization of web conferencing services and VPN began in earnest, attacks targeting them occurred
- Risks of prying eyes at web conferences and virus infection of computers for teleworking

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【4】Attacks on New Normal Work Styles such as Teleworking

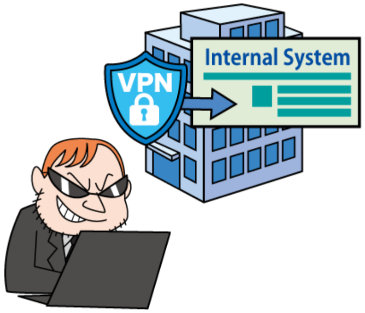
～ Security for teleworking requires cohesion between the company and its employees ～

● Attack Methods / Occurrence Factors

- Inadequate teleworking environment and administration system

- Unauthorized access by exploiting vulnerabilities in teleworking software
- Inadequate administration system due to sudden shift to teleworking
- Use of private computers and home networks

※Risks of information leakage from places where the organization's security measures are not applied



Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【4】Attacks on New Normal Work Styles such as Teleworking

～ Security for teleworking requires cohesion between the company and its employees ～

● Cases and Trends in 2021(1)

■ VPN credentials leakage due to exploitation of a vulnerability

- In September 2021, a vulnerability in VPN products was exploited and credentials were stolen.
- Credentials for tens of thousands of companies were disclosed on the Internet.
- Approximately 1,000 Japanese companies, mainly small and medium-sized enterprises, were affected.
- Information about the exploited vulnerabilities and countermeasures was already released in 2019.
- VPN products that have not been applied update program may be targeted.

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【4】Attacks on New Normal Work Styles such as Teleworking

～ Security for teleworking requires cohesion between the company and its employees ～

Cases and Trends in 2021(2)

Surge of brute force attacks on remote desktops

- After WHO (World Health Organization) declared COVID-19 a pandemic, the number of brute force attacks attempting unauthorized logins to RDP increased.
- Number of attacks increased about three times, from 93.1 million before the declaration (February 2020) to 277.4 million after the declaration (March 2020).
- As of April 2021, the monthly number of attacks remains over 300 million.

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【4】Attacks on New Normal Work Styles such as Teleworking

～ Security for teleworking requires cohesion between the company and its employees ～

● Countermeasures

Organizations (Teleworkers)

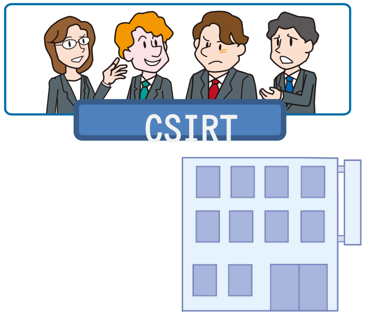
- Preventions

  - Comply with the organization's teleworking rules (Devices to be used, network environment, work locations, etc.)

- Actions after attack detected

  - Report to and consult with predefined contacts in accordance with the organization's policy

    ※Supervisors, CSIRT, related organizations, public agencies, etc.



Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

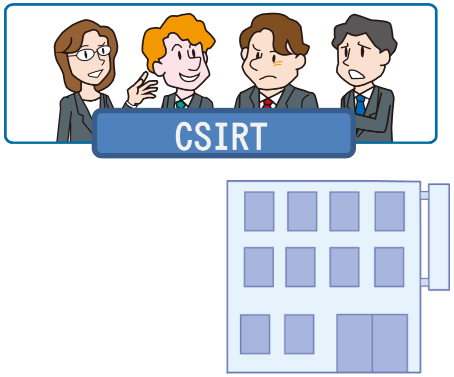
【4】Attacks on New Normal Work Styles such as Teleworking

～ Security for teleworking requires cohesion between the company and its employees ～

● Countermeasures

Organizations (Senior Management)

- Establishment of organizational framework
  - Establish CSIRT
  - Secure budget for countermeasures and perform countermeasures continuously
  - Develop a security policy of teleworking
  - Establish workflows and internal reporting system when problems occur



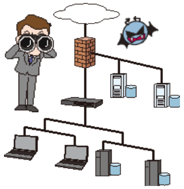
Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【4】Attacks on New Normal Work Styles such as Teleworking

～ Security for teleworking requires cohesion between the company and its employees ～

● Countermeasures

Organizations (Information Security Officers, System Administrators)



- Preventions (including preparations)

  - Adopt teleworking environments with strong security features such as thin client, VDI, and ZTNA/SDP, etc.
  - Establish teleworking regulations and operation rules

    ※Consider the difference between company-owned computers and private computers
  - Implement cybersecurity trainings for employees
  - Collect and disseminate information on vulnerabilities of software used and manage the status of countermeasures
  - Apply security patches (VPN devices, network equipment, computers)
  - Enforce network level authentication (NLA)
  - Enable multi-factor authentication settings

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【4】Attacks on New Normal Work Styles such as Teleworking

～ Security for teleworking requires cohesion between the company and its employees ～

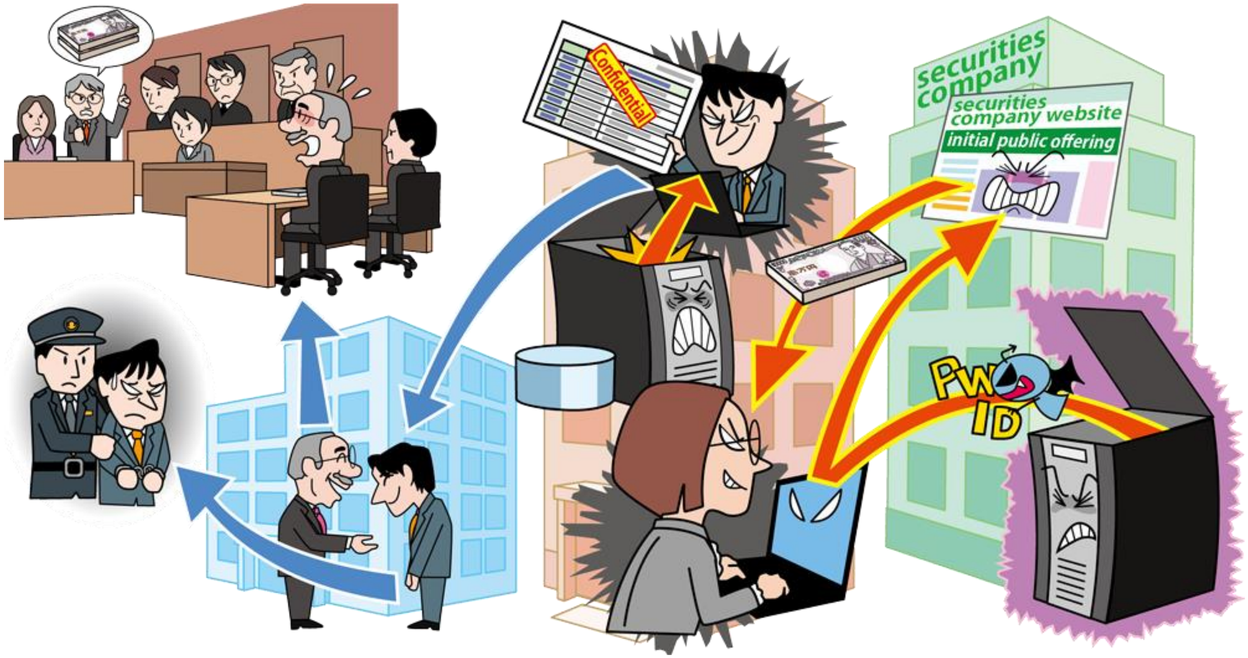
● Countermeasures

- Organizations (Information Security Officers, System Administrators)
  - Early detection
    - Perform appropriate logging and monitor continuously
    - Monitor and protect networks
    - Implement UTM, IDS / IPS, WAF, Virtual patching, etc.
  - Actions after attack detected
    - Respond to the incident with CSIRT operation
      ※Investigate teleworking environments remotely
    - Investigate impact and detect causes, strengthen countermeasures

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【5】Information Leakage by Internal Fraudulent Acts

～ Don't let internal fraudulent acts. Don't use information obtained by fraudulent acts.～



- Leakage of confidential information by employees or former employees of the organization
- Loss of social credibility of the organization due to fraudulent act of concerned personnel and financial loss due to compensation for damage

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【5】Information Leakage by Internal Fraudulent Acts

～ Don't let internal fraudulent acts. Don't use information obtained by fraudulent acts.～

● Attack Methods

- Internal employees can access easily to important information
- Provide information to the outside with malicious intent

Exploitation of access authority

- Obtain important information of the organization by exploiting the granted password
- Damage becomes greater if users are granted more than necessary access authority

Exploitation of former employee's account

- Obtain information using the account used before leaving the job

Unauthorized bringing out of internal information

- Bring out internal information fraudulently using USB flash drive, HDD, email, cloud storage, smartphone camera, paper media, etc.

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【5】Information Leakage by Internal Fraudulent Acts

～ Don't let internal fraudulent acts. Don't use information obtained by fraudulent acts.～

● Cases and Trends in 2021(1)

Major telecommunications carrier filed a claim for damages against former employee's new employer

- In January 2021, a former employee of a major telecommunications carrier was arrested for illegally taking network technology information with him when he changed jobs to another company in the same industry.
- The former employee disclosed the confidential information to his new employer.
- The company that suffered from the information leakage filed a civil lawsuit against the former employee's new employer, demanding that the former employee stop using the information, destroy it, and pay 1 billion yen in damages.

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【5】Information Leakage by Internal Fraudulent Acts

～ Don't let internal fraudulent acts. Don't use information obtained by fraudulent acts.～

Cases and Trends in 2021(2)

Unauthorized use of customer information of business partners

- In March 2021, a former employee of a company that was entrusted with the maintenance and operation of a securities company's system was arrested for illegally obtaining and using the company's customer information while on duty.
- The former employee used the IDs, passwords, PINs, etc. of 15 customers to spoof the customers, sell securities, and make unauthorized withdrawals of cash.
- The total amount of damage was approximately 200 million yen.

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

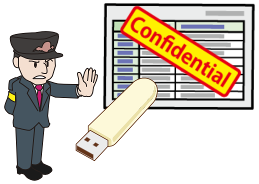
【5】Information Leakage by Internal Fraudulent Acts

〜 Don't let internal fraudulent acts. Don't use information obtained by fraudulent acts.〜

● Countermeasures

Senior Management, Administrators

- Preventions



- Develop basic policy for fraudulent act measures
- Identify information assets and lay out a response framework

  ※Identify critical assets and rank their importance, and then assign an administrator of critical information
- Manage and protect critical/sensitive information
  - Establish and operate procedures for registration, modification, and deletion of user IDs and access rights for important information
  - Immediately delete user IDs, etc. that are no longer needed as a result of employee transfer or leaving from the company
  - Conduct appropriate management and periodic audits of these IDs
  - Consider measures such as prohibiting the sharing of user IDs, and introducing tools such as DLP
- Implement physical controls

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【5】Information Leakage by Internal Fraudulent Acts

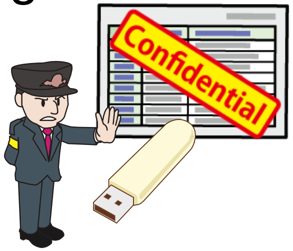
～ Don't let internal fraudulent acts. Don't use information obtained by fraudulent acts.～

● Countermeasures

Senior Management, Administrators

- Improvement of information literacy/ethics

  - Enforce workforce management and compliance trainings



- Early detection

  - Monitor system operation logs

- Actions after attack detected

  - Report to and consult with predefined contacts in accordance with the organization's policy

  ※Supervisors, CSIRT, related organizations, public agencies, etc.

  - Investigate impact and detect causes, strengthen countermeasures

  - Punish internal fraudulent actors appropriately

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【6】Increase in Exploitations following the Release of Vulnerability Countermeasure Information

～ Could that vulnerability affect your organization? Collect information and take appropriate action!～

Vulnerability X patch to fix
Protect everyone!

- Attackers exploit vulnerability information released for vulnerability countermeasures
- In recent years, the time between the release of vulnerability information and the distribution of exploit code and full-scale attacks has become shorter
- Vulnerabilities in widely-used products cause a large-scale damage

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【6】Increase in Exploitations following the Release of Vulnerability Countermeasure Information

～ Could that vulnerability affect your organization? Collect information and take appropriate action!～

● Attack Methods

- Attack with exploitation of published vulnerability information
- Target those who have not yet taken countermeasures or are taking time to take countermeasures

- Exploitation of vulnerabilities which have not yet taken countermeasures
  - Exploit vulnerabilities (N-day vulnerabilities) that exist between the time the countermeasure information is released and the time the user completes the countermeasure
- Use of publicly available attack tools
  - Exploitation tools that exploit released vulnerabilities are created in a short period of time and become available and being distributed on the Internet (dark web, etc.)
  - Vulnerability exploitation features may be implemented in open-source tools, and these can be exploited by attackers

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【6】Increase in Exploitations following the Release of Vulnerability Countermeasure Information

～ Could that vulnerability affect your organization? Collect information and take appropriate action!～

● Cases and Trends in 2021(1)

Vulnerability in "Apache Log4j", a Java log output library

- On December 9, 2021, a vulnerability in Apache Log4j was disclosed, which allows remote execution of arbitrary code (CVE-2021-44228) .
- The following day, a proof-of-concept code (POC) was released, and many exploitations were observed.

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【6】Increase in Exploitations following the Release of Vulnerability Countermeasure Information

～ Could that vulnerability affect your organization? Collect information and take appropriate action!～

Cases and Trends in 2021(2)

Attacks targeting Movable Type vulnerability

- On October 20, 2021, a vulnerability (CVE-2021-20837) in Movable Type was disclosed.
- On October 26, a POC was released.
- On October 27, communications attempting to probe the vulnerability were observed.
- On November 1 and after, attacks that exploited the vulnerability were observed.
- On November 7, a website was tampered.

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【6】Increase in Exploitations following the Release of Vulnerability Countermeasure Information

〜 Could that vulnerability affect your organization? Collect information and take appropriate action!〜

● Countermeasures

Individuals/Organizations (System Administrators/Software users)

- Preventions

  - Identify assets and lay out a response framework
  - Collect vulnerability countermeasure information and take prompt actions based on the information
  - Monitor networks and block attack communications
  - Use software and versions that are provided excellent security support
  - Shut down servers temporarily, etc.

- Early detection

  - Implement UTM•IDS / IPS • WAF, etc.

- Actions after attack detected

  - Report to and consult with predefined contacts in accordance with the organization's policy

    ※Supervisors, CSIRT, related organizations, public agencies, etc.

  - Investigate impact and detect causes, strengthen countermeasures

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【6】Increase in Exploitations following the Release of Vulnerability Countermeasure Information

～ Could that vulnerability affect your organization? Collect information and take appropriate action!～

● Countermeasures

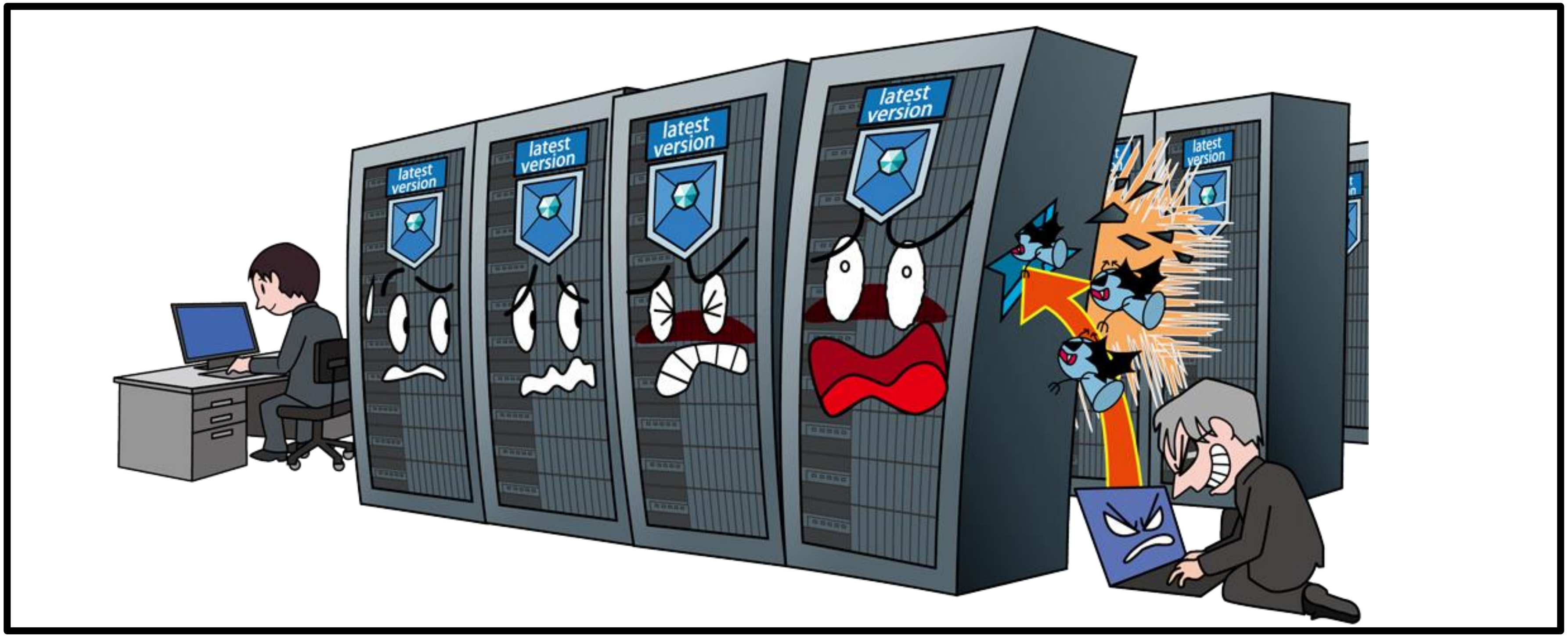
Organization (Development vendors)

- Management of product security, laying out a response framework
  - Grasp embedded software in products and ensure its management (Utilize the SBOM)
  - Collect vulnerability-related information
  - Create a response procedure when vulnerabilities are discovered
  - Establish a system to promptly disseminate information

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【7】Attacks Targeting before the Release of Security Patches (Zero-day Attacks)

～ Zero-day vulnerabilities are nuisance to security personnel ～



- Attacks exploiting vulnerabilities are executed before the release of vulnerability fixes (patches) and workarounds
- Difficult to take precautionary measures for attack prevention, and there is a risk of becoming a victim before you aware of it

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【7】Attacks Targeting before the Release of Security Patches (Zero-day Attacks)

～ Zero-day vulnerabilities are nuisance to security personnel ～

● Attack Methods

- If the vulnerability is not recognized by the development vendor, etc., a fix (patch) will not be created for it
- The vulnerability is exploited before the fix is released

- Vulnerabilities discovered before the release of a fix (patch) are exploited
  - Difficult to take precautionary measures for attack prevention, and organizations in an unprotected state are targeted

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【7】Attacks Targeting before the Release of Security Patches (Zero-day Attacks)

～ Zero-day vulnerabilities are nuisance to security personnel ～

Cases and Trends in 2021(1)

Zero-Day Attacks on VPN Products

- On April 20, 2021 (U.S. time), Pulse Secure disclosed a vulnerability in its VPN product “Pulse Connect Secure”.
- Remote third parties could bypass authentication and execute arbitrary code exploiting the vulnerability.
- In the United States, attacks exploiting the vulnerability had already been observed at the time of the disclosure.
- Until a fix was released on May 6, users of the product had to take temporary workarounds or temporarily stop using the product.

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【7】Attacks Targeting before the Release of Security Patches (Zero-day Attacks)

～ Zero-day vulnerabilities are nuisance to security personnel ～

Cases and Trends in 2021(2)

Zero-Day Attacks on Windows Print Spooler

- On July 1, 2021, Microsoft released information regarding a vulnerability in the Windows Print Spooler.
- The vulnerability, called "PrintNightmare," could allow attackers to execute arbitrary code, etc.
- No fixes were available at the time of disclosure.
- Users had to apply workarounds and mitigations from July 7 until the phased release of fixes.

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【7】Attacks Targeting before the Release of Security Patches (Zero-day Attacks)

〜 Zero-day vulnerabilities are nuisance to security personnel 〜

- Countermeasures
  - Organizations (System Administrators)
    - Preventions
      - Identify information assets and lay out a response framework
      - Monitor networks and block attack communications
      - Monitor and defend endpoints using EDR, etc.
      - Use software and versions that are provided excellent security support
      - Collect and disseminate information on vulnerabilities of software used and manage the status of countermeasures
    - Early detection
      - Implement UTM, IDS / IPS, WAF, Virtual patching, etc.

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【7】Attacks Targeting before the Release of Security Patches (Zero-day Attacks)

～ Zero-day vulnerabilities are nuisance to security personnel ～

● Countermeasures

■ Organizations (System Administrators)

- Actions before the release of a fix
  - Apply workarounds or mitigations
  - Stop using the software temporarily
- Actions after the release of a fix
  - Apply the fix

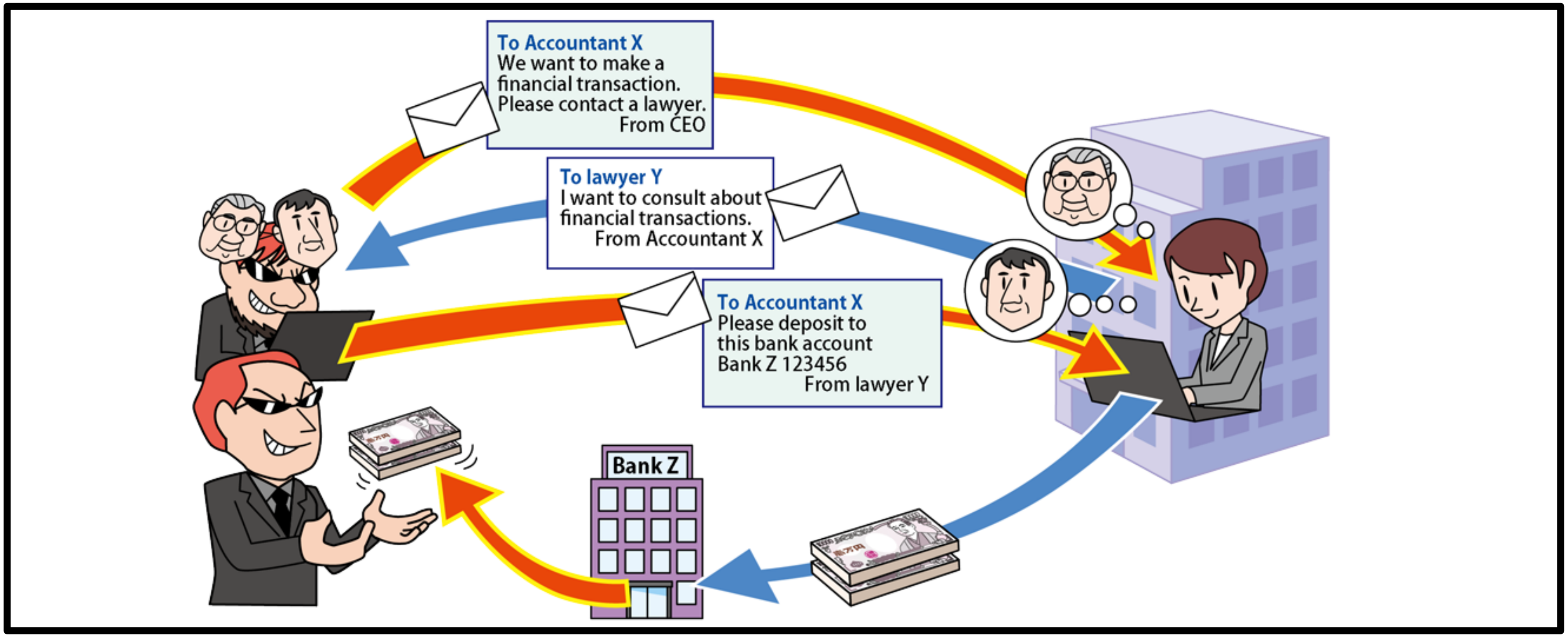
    Disable workarounds or mitigations as necessary
- Actions after attack detected
  - Report to and consult with predefined contacts in accordance with the organization's policy

    ※Supervisors, CSIRT, related organizations, public agencies, etc.
  - Investigate impact and detect causes, strengthen countermeasures

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【8】Financial Loss by Business Email Compromise (BEC)

～ Confidential requests from senior management and account change requests from clients should be confirmed by phone ～



To Accountant X
We want to make a financial transaction.
Please contact a lawyer.
From CEO

To lawyer Y
I want to consult about financial transactions.
From Accountant X

To Accountant X
Please deposit to this bank account
Bank Z 123456
From lawyer Y

- Spoof a CEO/senior management or business partners email account
- Fake emails and trick organization's accountant or financial officer
- Request the accountant or financial officer to transfer money to the attacker's bank account

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【8】Financial Loss by Business Email Compromise (BEC)

〜 Confidential requests from senior management and account change requests from clients should be confirmed by phone 〜

● Attack Methods

- Steal business information etc. of target organization using some means
- Send remittance request email using stolen information

- Disguise invoice as the one with business partners
- Spoof a CEO or senior management account
- Abuse stolen email accounts of target organization
- Spoof an authoritative third-party account
- Steal information as an act of fraud preparation

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【8】Financial Loss by Business Email Compromise (BEC)

～ Confidential requests from senior management and account change requests from clients should be confirmed by phone ～

● Cases and Trends in 2021(1)

Attack targeting an overseas affiliate by spoofing a company executive

- In August 2021, a person in charge of an overseas affiliate of a company participating in the Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP) received a business scam email that spoofed the company's executive.
- The email asked the receiver to contact a lawyer at an actual law firm, saying "I want to make a personal request for a highly confidential financial transaction".
- The sender's (From) display name was set to the company executive's name and email address, but the email was sent from a free email address.
- An email address was set up in the CC, which is a fake -mail address of a lawyer.

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【8】Financial Loss by Business Email Compromise (BEC)

～ Confidential requests from senior management and account change requests from clients should be confirmed by phone ～

● Cases and Trends in 2021(2)

Observed scam emails spoofing regular employees

- According to Trend Micro's threat trend monitoring of Business Email Compromise (BEC), the number of detections of BEC increased from January to September 2021.
- Especially, the number of detections rose sharply in August.
- Trend Micro observed that the attackers were not only spoofing senior executives, etc., but also spoofing regular employees.

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【8】Financial Loss by Business Email Compromise (BEC)

～ Confidential requests from senior management and account change requests from clients should be confirmed by phone ～

- Countermeasures
  - Organizations
    - Preventions

- Establish business workflows which make corporate governance works

  Establish rules and systems that prevent deals at the discretion of individuals or by order of individuals

- Establish business workflows that does not rely on email
- Grant electronic signature (S/MIME, PGP) to emails ※Prevent spoofing

<Verification of the email authenticity>

- Confirm authenticity by multiple means other than email
- Pay attention to unusual emails
- Pay attention to the sender's mail domain
- Pay attention to emails that rush you to judgment

<Proper management of email accounts>

- Manage passwords properly and utilize login notification function, multi-factor authentication, etc.

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【8】Financial Loss by Business Email Compromise (BEC)

～ Confidential requests from senior management and account change requests from clients should be confirmed by phone ～

- Countermeasures
  - Organizations
    - Actions after BEC recognition

      - Report to and consult with predefined contacts in accordance with the organization's policy

        ※Supervisors, CSIRT, related organizations, public agencies, etc.

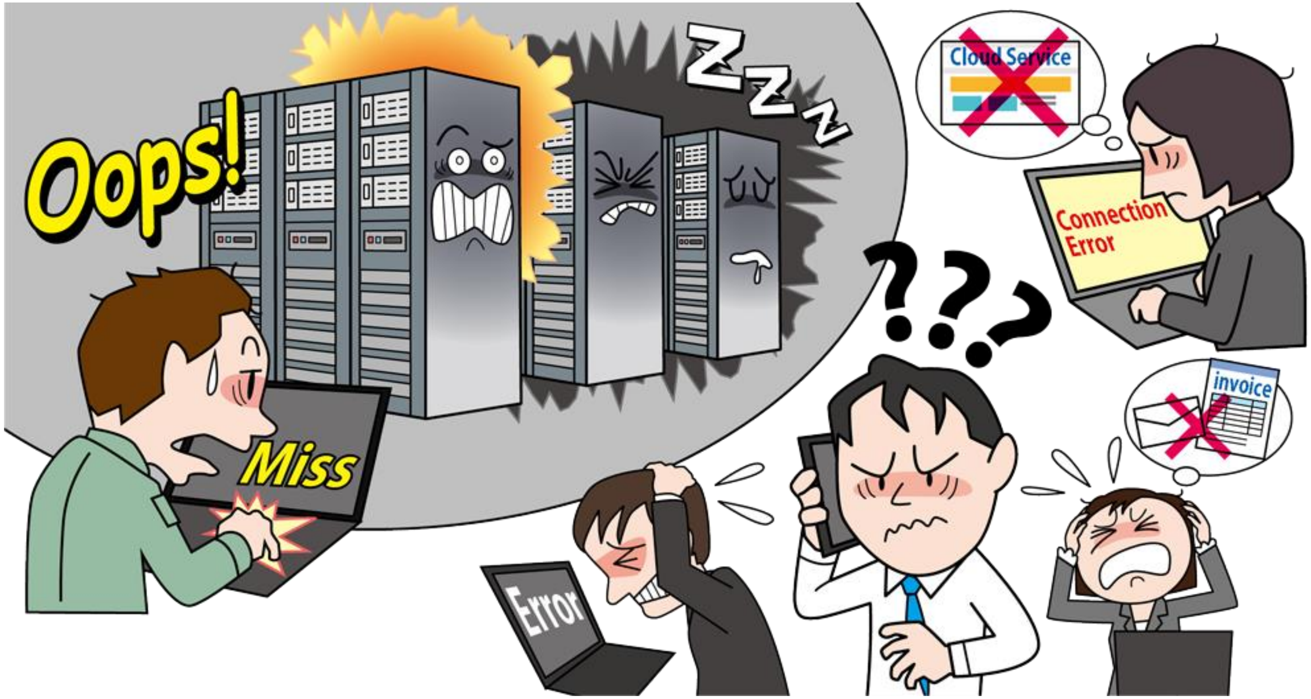
      - Investigate impact and detect causes, strengthen countermeasures Check if there are any unintended forwarding settings or folder sorting settings in email accounts

      - Change passwords for all email accounts on the affected server

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【9】Suspension of Business due to Unexpected IT Infrastructure Failure

～ Prepare alternative ways for business continuity ～



- Suspension of IT infrastructure of data center or cloud service which are currently used occurs
- Risk of a serious impact on the business of organizations using the IT infrastructure

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【9】Suspension of Business due to Unexpected IT Infrastructure Failure

〜 Prepare alternative ways for business continuity 〜

● Causes

- Unpredictable events stop IT infrastructure
- BCM (Business Continuity Management) is not properly practiced

Natural Disaster

- Natural phenomena such as earthquakes, typhoons, and floods

Operation Work Accidents

- Human error during maintenance work of infrastructure equipment or work of system configuration change, etc.

Equipment/System Failures

- Failures of control systems such as power supply, air conditioning equipment, etc.
- Defects in the hardware or software of the equipment comprising the IT infrastructure, etc.

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【9】Suspension of Business due to Unexpected IT Infrastructure Failure

〜 Prepare alternative ways for business continuity 〜

● Cases and Trends in 2021(1)

Failure occurred in Amazon Web Services (AWS)

- In September 2021, the AWS Direct Connect cloud service, a dedicated network connection to AWS provided by AWS, experienced a failure.
- The cause was a failure of network equipment in the Tokyo Region data center due to a newly introduced mechanism to optimize network response time.
- The failure affected banking applications, online securities websites, and smartphone payment deposits, etc.

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【9】Suspension of Business due to Unexpected IT Infrastructure Failure

～ Prepare alternative ways for business continuity ～

● Cases and Trends in 2021(2)

Communication failure occurred in NTT DoCoMo

- In October 2021, voice and data communication services provided by a major mobile carrier, NTT DoCoMo, experienced a failure.
- The cause was network congestion caused by traffic increase due to server switch back.
- Although recovery was announced on the same day as the failure, users continued to experience difficulties until the following day.
- The failure affected a total of 12.9 million users.

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【9】Suspension of Business due to Unexpected IT Infrastructure Failure

～ Prepare alternative ways for business continuity ～

● Countermeasures

Organization (System administrators)

- Preventions
  - - Practice BCM (establish and operate BCP (Business Continuity Plan))
  - - Ensure and maintain availability (system design, monitoring)
  - - Perform data backups (recovery measures)
  - - Confirm contracts, SLA (Service Level Agreement) , etc.

    Contracts/SLA with IT infrastructure providers

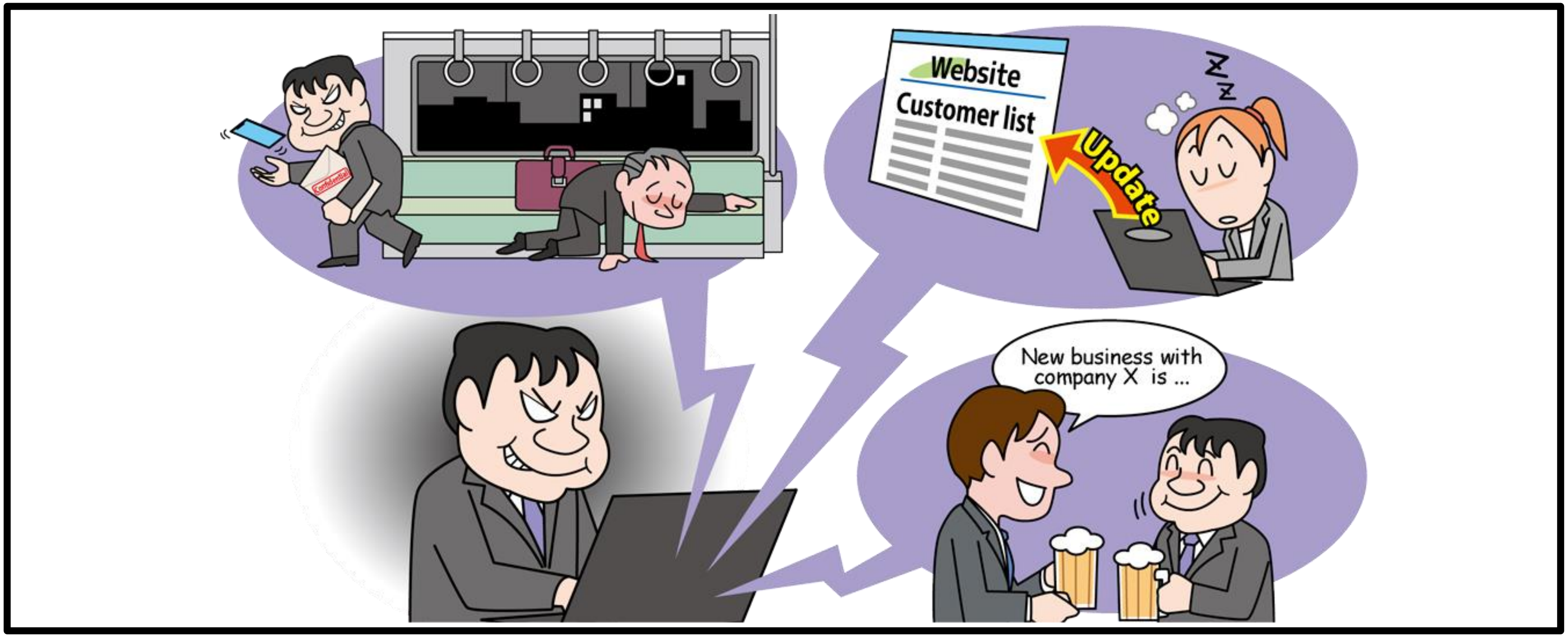
    Contracts/SLA with customers
  - - Confirm coordination with IT infrastructure providers in anticipation of business impacts
- Actions after business suspension occurred
  - - Respond according to BCP
  - - Report to and consult with predefined contacts in accordance with the organization's policy

    ※Supervisors, CSIRT, related organizations, public agencies, etc.

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【10】Unintentional/Accidental Information Leakage

〜Are you sure that the address of the email is correct?〜



- Unintentional confidential information leakage due to employee's carelessness
- Loss of social trust due to information leakage, secondary damage due to abuse of leaked information

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【10】Unintentional/Accidental Information Leakage

～Are you sure that the address of the email is correct?～

- Causes

  - Carelessness of individuals from lack of information literacy and information ethics
  - Insufficient organizational management framework

  - Low security awareness among employees
    - Bring out confidential/sensitive information with a bag, then lose the bag and leak the information
    - Send an email without enough confirmation of address, etc.
  - Situation of individuals
    - Lack concentration or attention due to poor health or urgent works
  - Insufficiency of organizational rules and work check procedures
    - Definition of confidential/sensitive information, handling rules, bring-out permission procedure, etc. are not defined or insufficient

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【10】Unintentional/Accidental Information Leakage

〜Are you sure that the address of the email is correct?〜

- Cases and Trends in 2021(1)
  - Information leakage of source code for a major bank's system for private use by an outsourced SE
    - In January 2021, source code for a major bank's system was disclosed on a publicly available website.
    - A system engineer of a company outsourced by the bank uploaded the source code he wrote to a publicly available website in order to use a service that allows users to diagnose their annual income by uploading the source code.
    - The bank stated that no customer information was leaked, and no problem in their security.

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【10】Unintentional/Accidental Information Leakage

〜Are you sure that the address of the email is correct?〜

- Cases and Trends in 2021(2)
  - Information leakage caused by mistakenly sending data that should not be sent
    - •In September 2021, a company engaged in credit card and other consumer credit services mistakenly sent IDs and passwords for 475,813 users of the company's cardholder web services to two subcontractors, who did not need to receive them.
    - •The cause was a flaw in the confirmation method used to send the information to subcontractors.
    - •As a countermeasure, the company is reviewing the system of data delivery and improving employee awareness.

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【10】Unintentional/Accidental Information Leakage

～Are you sure that the address of the email is correct?～

● Countermeasures

Organization (Person concerned)

- Improvement of information literacy and information ethics
  - Conduct security awareness training for employees
  - Establish organizational rules and confirmation processes
  - Review organizational rules and confirmation processes
- Preventions
  - Operate according to confirmation processes
  - Protect information (encryption, authentication), understand and visualize exactly where sensitive information is stored
  - Implement DLP (Data Loss Prevention) products
  - Restrict the information and devices that can be brought out
  - Implement measures to prevent wrong email transmission, etc.
  - Activate the loss prevention function of mobile devices for business use

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【10】Unintentional/Accidental Information Leakage

～Are you sure that the address of the email is correct?～

● Countermeasures

- Early detection
  - Establish internal reporting system when problems occur
  - Set up a point of contact with outsiders
- Actions after information leakage occurred
  - Report to and consult with predefined contacts in accordance with the organization's policy

    ※Supervisors, CSIRT, related organizations, public agencies, etc.
  - Investigate impacts and detect causes, strengthen countermeasures
  - Prevent damage expansion and eliminate secondary damage factors
  - Disclose the content and cause of the leakage

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

【10】Unintentional/Accidental Information Leakage

～Are you sure that the address of the email is correct?～

- Countermeasures
  - Individuals/Organizations (Victims)
    - Actions after information leakage occurred

      - Suspend credit cards

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

Conclusion

Implement Basic Security Measures

- The order of "10 Major Security Threats" changes every year, but the importance of basic security measures have not changed for many years.

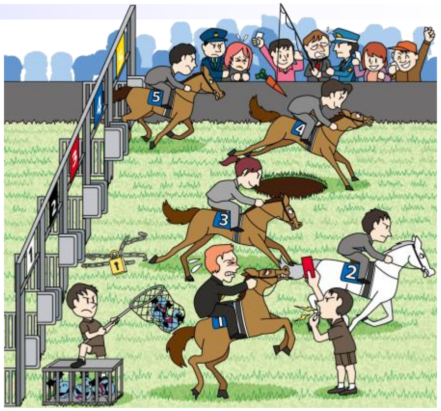
Know about Threats
Implement Countermeasures

- To prepare for threats, it is important to understand attack methods and trends, and risk factors that the organization has.
- The ranking of "10 Major Security Threats" does not necessarily coincide with the priority of measures to be implemented in each organization. Perform risk analysis for each organization and prioritize measures.

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan

Download of Detailed Documents

■ 10 Major Security Threats 2022



For detailed information regarding this document, please visit following website (in Japanese only).

※Please access the following URL or read the QR code with your smartphone's QR code reader application to view the website.

https://www.ipa.go.jp/security/vuln/10threats2022.html

■ Request for cooperation with a survey

In order to improve the quality of the tools and documents released by IPA, we would appreciate your cooperation with a survey (in Japanese only).

https://touroku.ipa.go.jp/?url=http%3A%2F%2Fspd-evsan-ap01.ipa.go.jp%2Fentry%2FMemberLogin%3Fevent_id%3DEAO000000074

Copyright © 2022 Information-Technology Promotion Agency (IPA), Japan