IPA Better Life with IT

10 Major Security Threats 2023

～Laying the groundwork for security measures should be done on a company-wide basis, rather than leaving everything to security personnel～

[For Organizations]

IT Security Center (ISEC)
Information-Technology Promotion Agency (IPA), Japan
July 2023

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

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”

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	Attacks Exploiting Supply Chain Weaknesses
Extortion of Money by Blackmail or Fraudulent Methods with Email, SNS, etc.	3	Confidential Information Theft by APT
Fraudulent Use of Leaked Credit Card Information	4	Information Leakage by Internal Fraudulent Acts
Fraudulent Use of Smartphone Payment	5	Attacks on New Normal Work Styles such as Teleworking
Malicious Smartphone Applications	6	Attacks Targeting before the Release of Security Patches (Zero-day Attacks)
Internet Fraud by Fake Warnings	7	Financial Loss by Business Email Compromise
Personal Information Theft from Services on the Internet	8	Increase in Exploitations following the Release of Vulnerability Countermeasure Information
Unauthorized Login to Services on the Internet	9	Unintentional/Accidental Information Leakage
Financial Loss by Fraudulent Billings such as One Click Fraud	10	Commercialization of Crime (Underground Services)

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

"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)

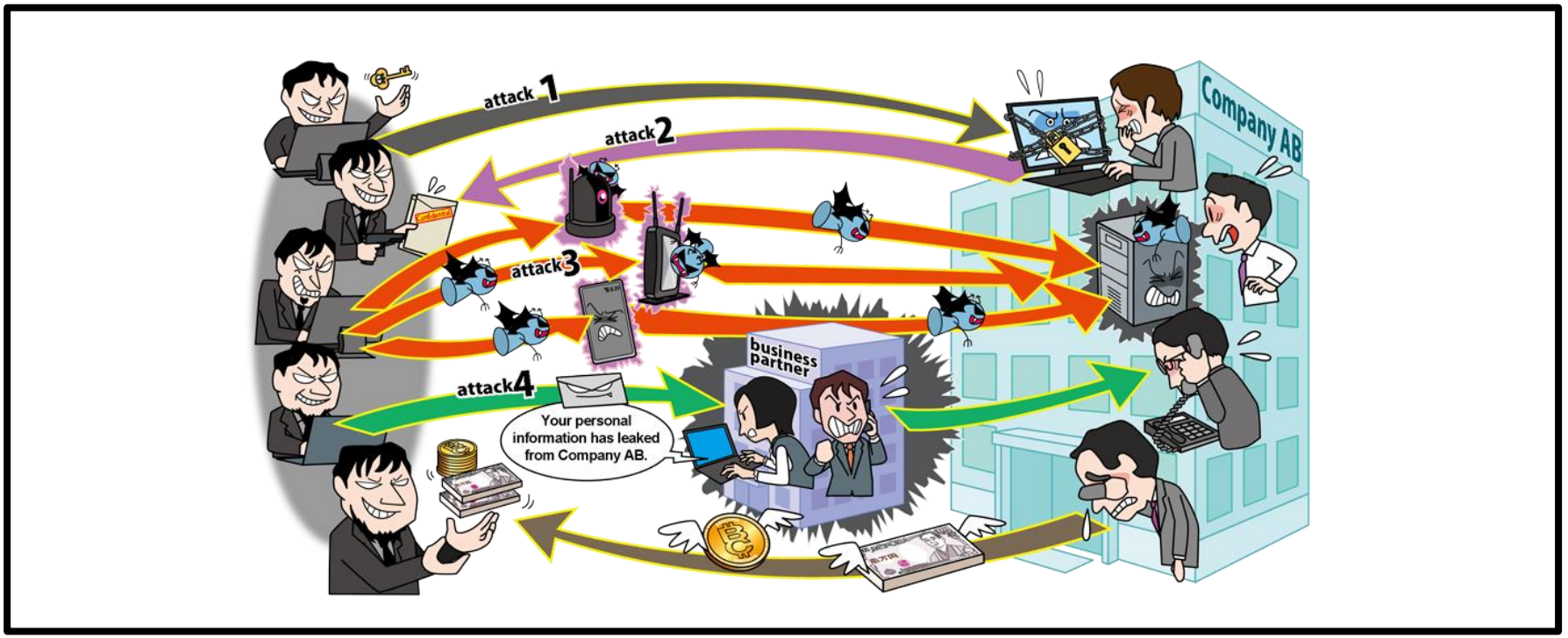
10 Major Security Threats 2023
For Organizations

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.

【1】Ransomware Attacks

～Ransomware's been on the rampage. Quadruple extortion threatens victims.～



- Encrypt files stored on computers, etc. with ransomware and make them unavailable
- Extort money in exchange for restoration of encrypted files
- Extort ransom payment to not release the exfiltrated data, or to not notify business partners, etc. of being under attack

【1】Ransomware Attacks

～Ransomware's been on the rampage. Quadruple extortion threatens victims.～

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.

【1】Ransomware Attacks

～Ransomware's been on the rampage. Quadruple extortion threatens victims.～

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

【1】Ransomware Attacks

～Ransomware's been on the rampage. Quadruple extortion threatens victims.～

- Cases and Trends in 2022(1)
  - **Vulnerability exploitation and ransomware deployment**
    - In March 2022, Tokyo Computer Service Co., Ltd. had its systems infected with ransomware, and some information, such as internal management information and customer information was stolen.
    - The attacker accessed the web service used to manage Active Directory via a reverse proxy server, and then infiltrated the Active Directory server exploiting a vulnerability in the web service.
    - The attacker sets up a batch file that automatically distributed ransomware, infecting devices in the organization with the ransomware.

【1】Ransomware Attacks

～Ransomware's been on the rampage. Quadruple extortion threatens victims.～

- Cases and Trends in 2022(2)
  - **Ransomware Infection via Remote Desktop**
    - In June 2022, VIAX Co., Ltd. revealed that the server of its attendance management system was infected with ransomware.
    - The ransomware encrypted the information of 1,871 employees and 2,167 retirees.
    - For maintenance use, remote desktop connection of the web server of the attendance management system was available.
    - The attacker infiltrated the web server likely using a brute-force attack.

【1】Ransomware Attacks

～Ransomware's been on the rampage. Quadruple extortion threatens victims.～

- Countermeasures
  - Senior Management
    - Establishment of organizational framework

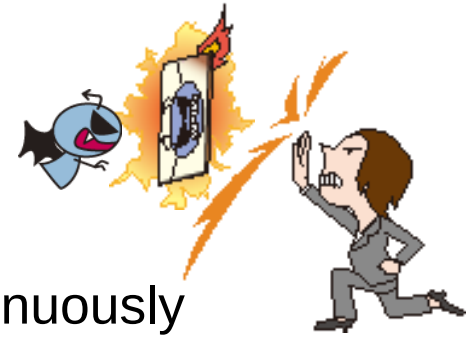
      - Secure budget for countermeasures and perform countermeasures continuously

      - Assign a CISO/CIO or other responsible person with expertise

【1】Ransomware Attacks

～Ransomware's been on the rampage. Quadruple extortion threatens victims.～

- Countermeasures
  - System Administrators, Employees
    - Preventions

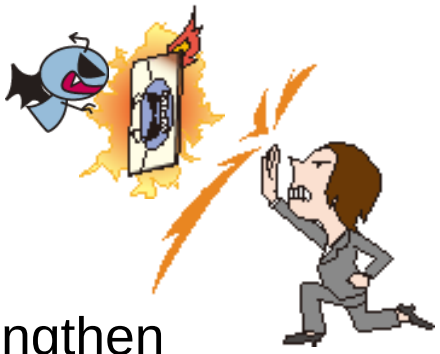


- Establish CSIRT that can respond promptly and continuously
- Enable multi-factor authentication settings
- Don't easily click on attachments and URLs
- Don't run software of unknown origin
- Expedite equipment vulnerability countermeasures
  - Apply patches promptly
  - Stop using OS that are no longer 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
  - Perform security assessments or penetration testing

【1】Ransomware Attacks

～Ransomware's been on the rampage. Quadruple extortion threatens victims.～

- 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

【1】Ransomware Attacks

～Ransomware's been on the rampage. Quadruple extortion threatens victims.～

- 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.

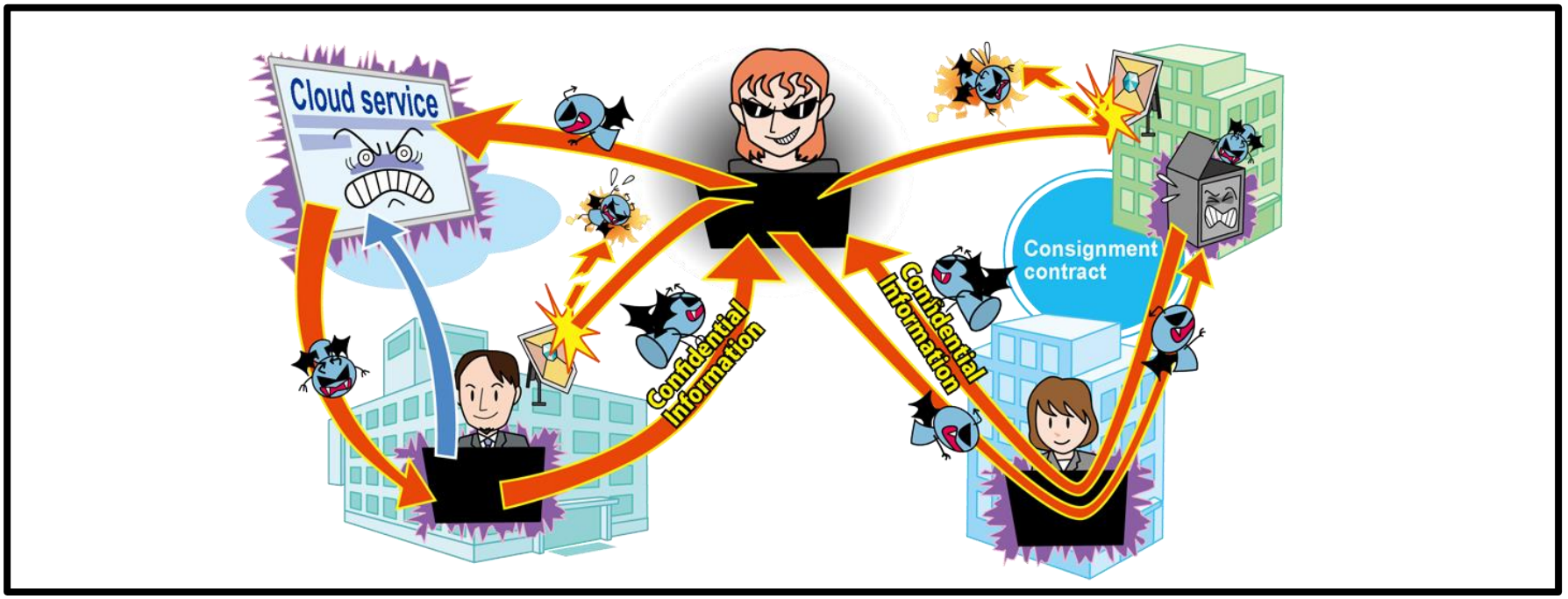
- Recover from backups
- Use decryption tools
- Investigate impact and detect causes, strengthen countermeasures
- Execute quarantine quickly to prevent expanding the damage to related organizations and business partners

<About ransom payment and selection of vendors for recovery>

Paying a ransom doesn't always recover data and prevent information leakage

【2】Attacks Exploiting Supply Chain Weaknesses

～ Ensure proper management of not only your organization
but also of the contractors and services you use ～



- Organizations with lax security measures in supply chain (i.e., procurement, sales, outsourcing) are attacked as a foothold for attacks
- There are also software supply chain attacks that use the connections between goods and people involved in the software development lifecycle as a foothold
- Information leaks from business partners, or outsourcing partners which are delegated partial work

【2】Attacks Exploiting Supply Chain Weaknesses

～ Ensure proper management of not only your organization
but also of the contractors and services you use ～

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.

【2】Attacks Exploiting Supply Chain Weaknesses

～ Ensure proper management of not only your organization
but also of the contractors and services you use ～

- Cases and Trends in 2022(1)
  - **Shutting down all domestic factories due to a cyber attack on a subsidiary of a partner company**
    - In March 2022, TOYOTA MOTOR CORPORATION shut down all domestic factories due to a system failure at Kojima Industries Corporation Co., Ltd
    - The system failure was caused by a ransomware attack that an attacker infiltrated the company's internal network through the internal network of a subsidiary of Kojima Industries Corporation
    - A vulnerability in the subsidiary's remote connection equipment for dedicated communication with external companies was exploited to gain unauthorized access

【2】Attacks Exploiting Supply Chain Weaknesses

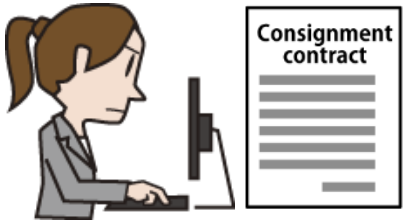
～ Ensure proper management of not only your organization but also of the contractors and services you use ～

- Cases and Trends in 2022(2)
  - **Information leakage due to tampering with services used**
    - In October 2022, Showcase revealed that several of its services had been tampered with.
    - The attacker gained unauthorized access exploiting a vulnerability in the company's system and tampered programs.
    - Personal information of customers was leaked from several services of business partners using the tampered services.

【2】Attacks Exploiting Supply Chain Weaknesses

～ Ensure proper management of not only your organization
but also of the contractors and services you use ～

- Countermeasures
  - Organizations (Your own organization)
    - Preventions



- Enforce rules for outsourcing and information management
- Implement operational rules of incident response including a reporting structure
- Verify deliverables

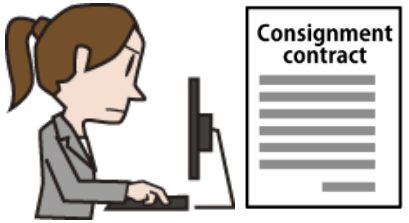
Identify embedded software and implement vulnerability countermeasures

- Obtain security certifications (ISMS, Privacy mark, SOC2, ISMAP, etc.)
- Utilize documents published by public authorities

【2】Attacks Exploiting Supply Chain Weaknesses

～ Ensure proper management of not only your organization
but also of the contractors and services you use ～

- Countermeasures
  - Organizations (Your own organization)
    - Actions after attack detected



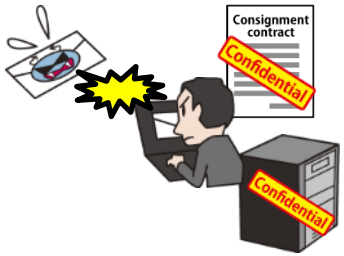
- Report to and consult with predefined contacts in accordance with the organization's policy

  ※Supervisors, CSIRT, related organizations, public agencies, etc.
- Investigate impact and detect causes, strengthen countermeasures
- Compensation to damage or impact of the attack

【2】Attacks Exploiting Supply Chain Weaknesses

～ Ensure proper management of not only your organization
but also of the contractors and services you use ～

- Countermeasures
  - Organizations (Organizations involved in supply chains)
    - Preventions



- Select reliable contractors, suppliers, and services
- Confirm the coverage of the contract

  Confirm the rules of information management and other matters at the time of contract
- Manage suppliers, business partners and outsourced organizations

  Periodically check and audit information security measures

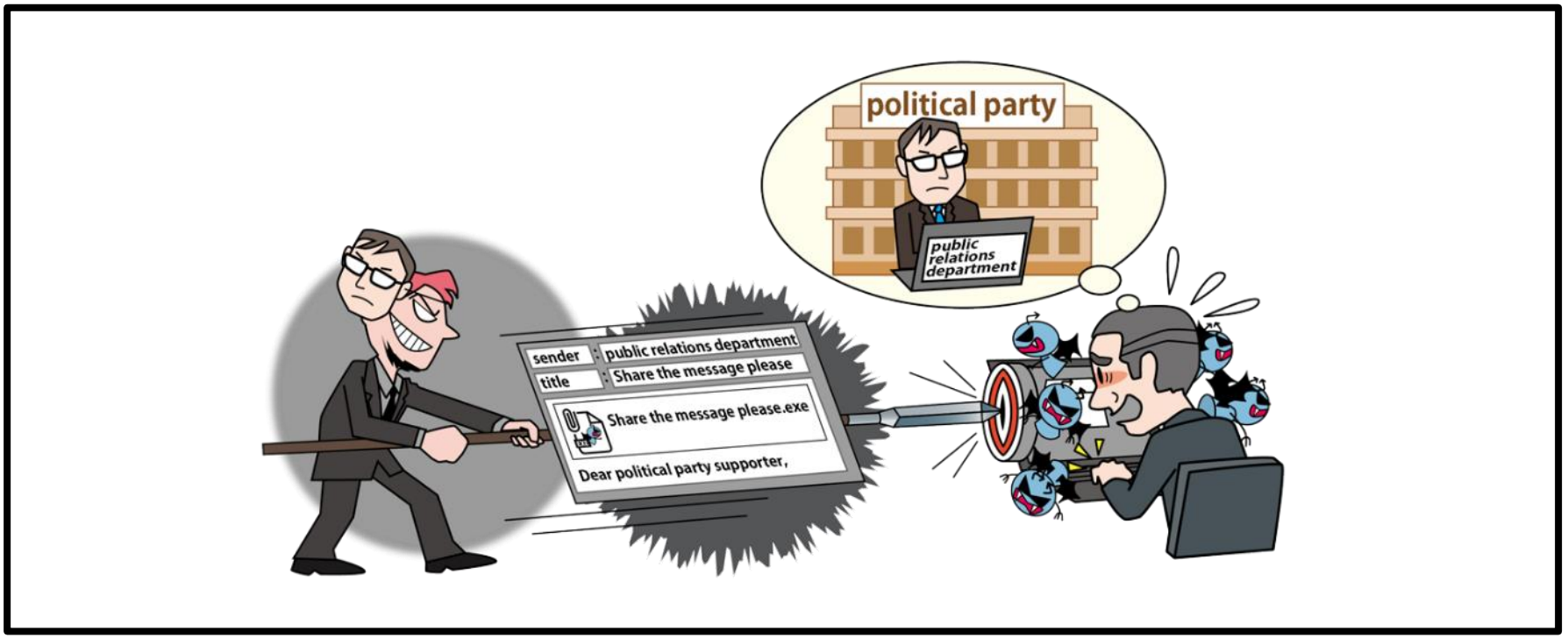
    - Actions after attack detected

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

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

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

～When you get an email, be suspicious first. Always keep your security awareness high～



- 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

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

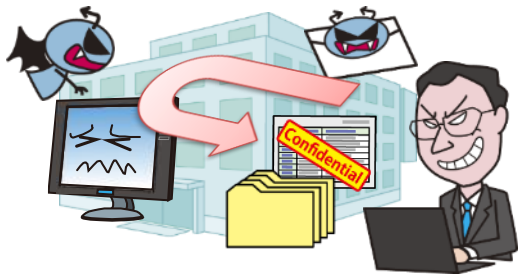
IPA

～When you get an email, be suspicious first. Always keep your security awareness high～

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



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

IPA

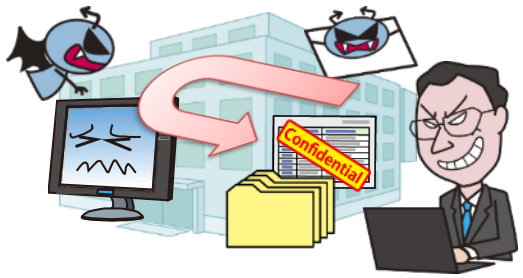
～When you get an email, be suspicious first. Always keep your security awareness high～

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



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

～When you get an email, be suspicious first. Always keep your security awareness high～

- Cases and Trends in 2022(1)
  - **Targeted email attacks on think tanks**
    - The National Police Agency disclosed targeted email attacks on think tanks in June 2022.
    - The email contained a compressed file of personal information, and the content was related to business, requesting data registration on its behalf.
    - The National center of Incident readiness and Strategy for Cybersecurity (NISC) has alerted about the attack targeting think tanks. IPA urges organizations to coordinate with government agencies in responding to attacks.

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

IPA

～When you get an email, be suspicious first. Always keep your security awareness high～

- Cases and Trends in 2022(2)

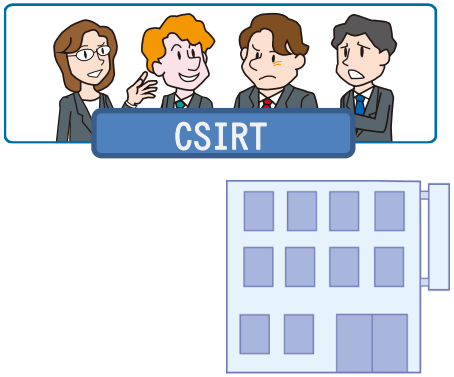
Spear phishing campaign targeting Japanese political groups

- ESET Research disclosed that a spear-phishing campaign was conducted during the period just prior to the House of Councilors in 2022.
- Emails were sent posing as public relations for a political party, making election-related requests, and posing as prominent politicians.
- The email contained a malicious attachment that, when executed, the receiver would infect with a virus called "LODEINFO".
- Once infected, commands are executed unlawfully, resulting in information theft and other damage.

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

～When you get an email, be suspicious first. Always keep your security awareness high～

- 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

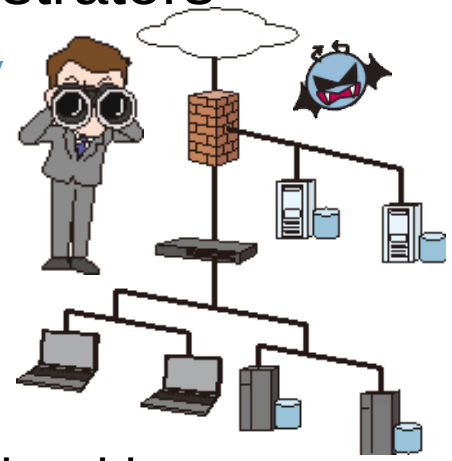


【3】Confidential Information Theft by APT (Advanced Persistent Threat)

IPA

～When you get an email, be suspicious first. Always keep your security awareness high～

- 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

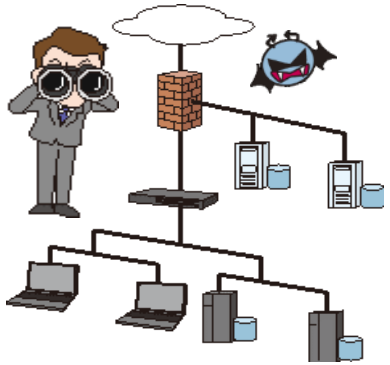
- Apply security patches to management terminals continuously
- Understand the status of security measures using integrated operation management tools, etc.

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

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

～When you get an email, be suspicious first. Always keep your security awareness high～

- 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.
      - Perform security assessments
      - Perform penetration testing



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

IPA

～When you get an email, be suspicious first. Always keep your security awareness high～

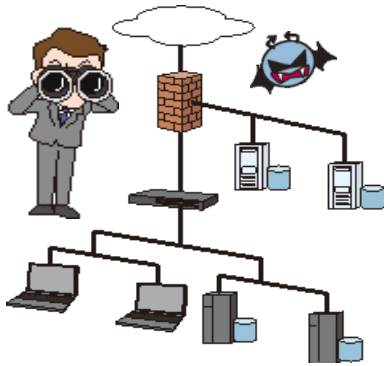
- Countermeasures
  - Information Security Officers, System Administrators
    - Early detection

      - Implement UTM, IDS / IPS, WAF, Virtual patching, etc.
      - Monitor and defend endpoints using EDR,NDR etc.
      - Perform logging, monitoring, and analysis.

        System logs, application logs, server access logs, authentication logs, database operation logs, communication logs, etc.

    - Actions after attack detected

      - Respond to the incident with CSIRT operation
      - Investigate impact and detect causes, strengthen countermeasures



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

～When you get an email, be suspicious first. Always keep your security awareness high～

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

      - Do not easily click on attachments or links

    - Actions after attack detected

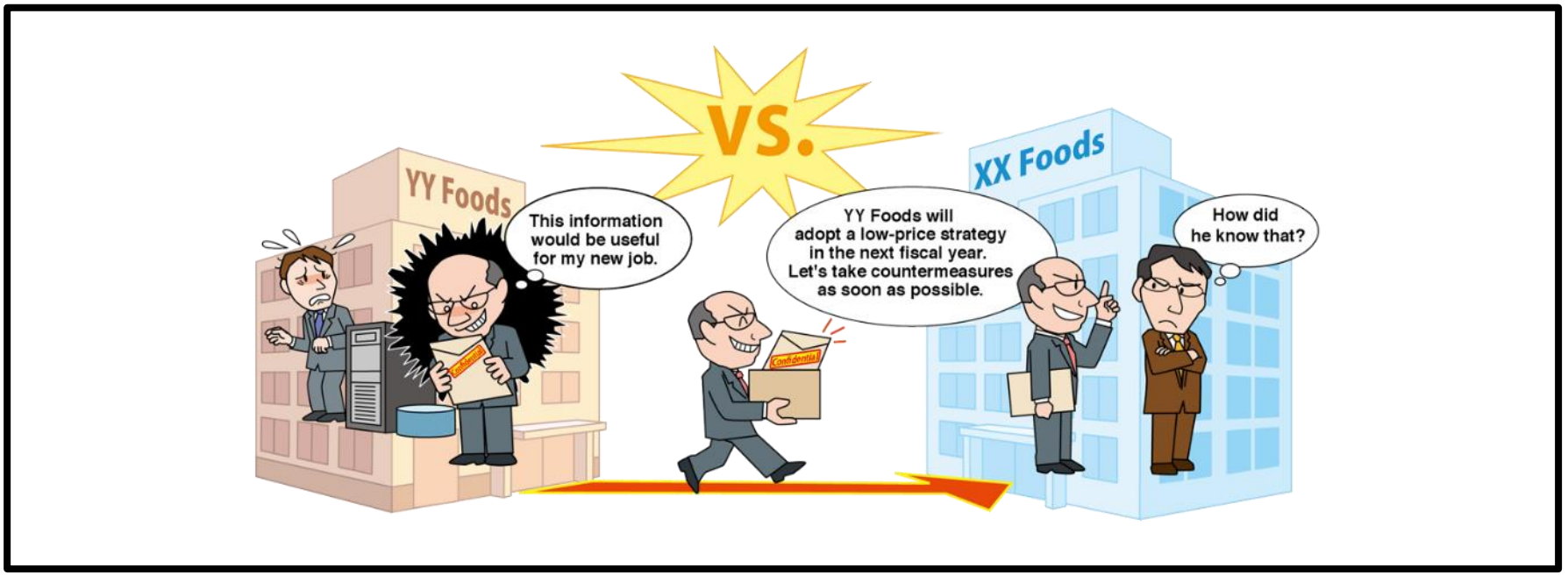
      - Report to and consult with predefined contacts in accordance with the organization's policy

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

【4】Information Leakage by Internal Fraudulent Acts

IPA

～Do not get, allow to get, or use information improperly!～



- 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
- Organizations which bring improperly obtained information to other organizations may also be subject to compensation for damages, etc.

【4】Information Leakage by Internal Fraudulent Acts

IPA

～Do not get, allow to get, or use information improperly!～

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.

【4】Information Leakage by Internal Fraudulent Acts

～Do not get, allow to get, or use information improperly!～

- Cases and Trends in 2022(1)
  - **Grade results leakage at city high school, possibly done by an insider**
    - In July 2022, the personal information of three city high school students including their grade results, was posted on Instagram and viewed by approximately 90 people.
    - Someone may have obtained the information by using a teacher's ID and password to access the learning support software used to manage students' grade results and other information and obtained the information.
    - Student tablets were allowed to access the learning support software, meaning anyone could view the personal information through those tablets.

【4】Information Leakage by Internal Fraudulent Acts

〜Do not get, allow to get, or use information improperly!〜

- Cases and Trends in 2022(2)
  - **President of sushi restaurant chain illegally took trade secrets from previous job**
    - In September 2022, the president of Kappa Create Co., Ltd. was arrested by the Tokyo Metropolitan Police Department on suspicion of violating the Unfair Competition Prevention Act.
    - The president had changed jobs from a rival company in November 2020, and used his former subordinates to steal trade secrets, such as product costs.
    - The head of Kappa Create's product planning department was arrested for misuse of data, and his former subordinate was arrested for leaking the password to the data.

【4】Information Leakage by Internal Fraudulent Acts

IPA

～Do not get, allow to get, or use information improperly!～

- Countermeasures
  - Senior Management, Administrators
    - Preventions(1)

- Develop basic policy for fraudulent act measures

  Develop an information handling policy, and establish work rules, etc. that provide for disciplinary action against internal wrongdoers.

- 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

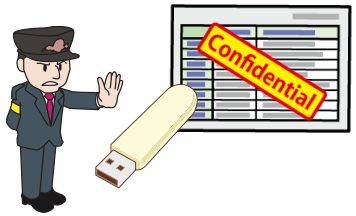
【4】Information Leakage by Internal Fraudulent Acts

IPA

～Do not get, allow to get, or use information improperly!～

- Countermeasures
  - Senior Management, Administrators
    - Preventions(2)

      - Implement physical controls
        - Control access to where critical information is stored and to the office
        - Restrict the use of recording media, and control the bringing out/bringing in of such media
        - When disposing of recording media, implement appropriate data erase operations
        - If data cannot be erased, consider the physical destruction of the media
        - Initialize leased items before returning them, etc.



【4】Information Leakage by Internal Fraudulent Acts

IPA

～Do not get, allow to get, or use information improperly!～

- Countermeasures
  - Senior Management, Administrators

- Improvement of information literacy/ethics

  - Enforce workforce management and compliance trainings

- Early detection

  - Monitor system operation logs

    Record and monitor logs and audit trails, such as access history to critical information and user operation history. In addition, inform employees about it.

- 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.

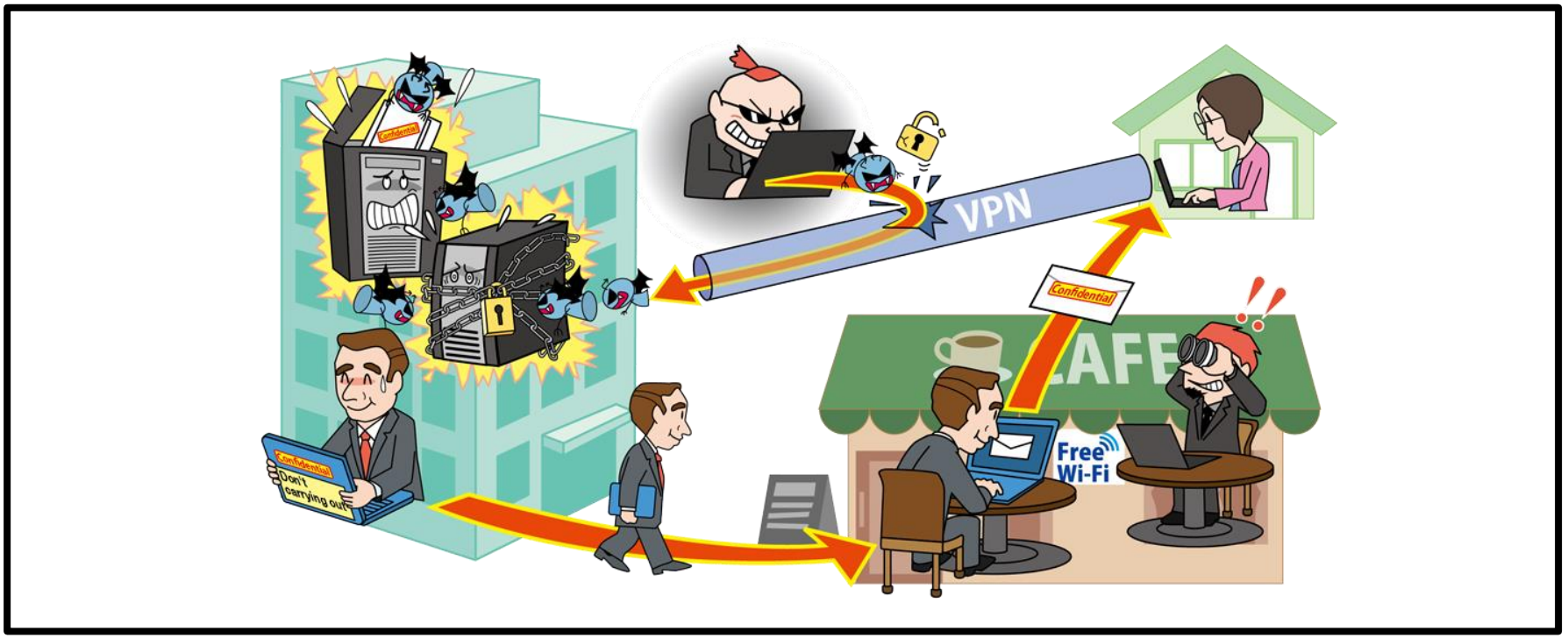
  - Investigate impact and detect causes, strengthen countermeasures

  - Punish internal fraudulent actors appropriately

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

IPA

～ Vulnerable teleworking environments are being targeted～



- Teleworking has spread rapidly as one of the responses to the COVID-19
- 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

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

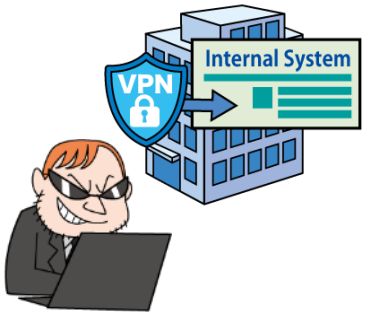
～ Vulnerable teleworking environments are being targeted～

Attack Methods / Occurrence Factors

- Inadequate teleworking environment and administration system

  - Unauthorized access by exploiting vulnerabilities in teleworking software
  - Ongoing operation of teleworking environment in interim state with inadequate security measures and management systems.
  - Use of private computers and home networks

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



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

～ Vulnerable teleworking environments are being targeted～

- Cases and Trends in 2022(1)

Ransomware attacks targeting remote connections

- In June 2022, Nichirin-Flex U.S.A., Inc. a subsidiary of Nichirin Co., Ltd. announced that it had been infected with the "mlock" ransomware.
- The attacker exploited a vulnerability in the configuration of external remote connections and infiltrated a server.
- After the infiltration, the attacker installed remote access tools on another server and performed network reconnaissance. The attacker then distributed the ransomware throughout the network.

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

IPA

～ Vulnerable teleworking environments are being targeted～

- Cases and Trends in 2022(2)
  - **Landscape of vulnerabilities of remote connections and security of teleworking**
    - According to the National Police Agency, more than 80% of ransomware infections in Japan in the first half of 2022 were caused by remote connection vulnerabilities, with 68% of infiltrations from VPN devices and 15% of infiltrations from remote desktops.
    - According to IPA's survey results, although there is an improving trend in confirming compliance with teleworking rules, 35.5% of IT users and 10.7% of IT vendors still have not yet confirmed compliance.
    - In terms of confirmation methods, 49.5% of IT users and 40.8% of IT vendors have only performed self-checks.

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

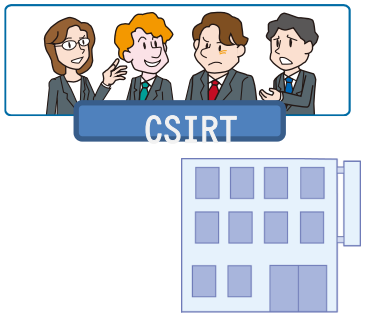
IPA

～ Vulnerable teleworking environments are being targeted～

- 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.

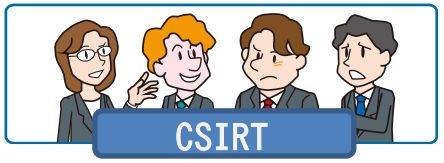


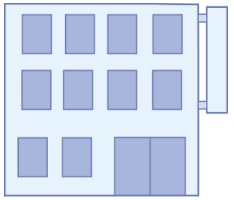
【5】Attacks on New Normal Work Styles such as Teleworking

IPA

～ Vulnerable teleworking environments are being targeted～

- 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

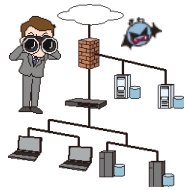




【5】Attacks on New Normal Work Styles such as Teleworking

～ Vulnerable teleworking environments are being targeted～

- 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

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

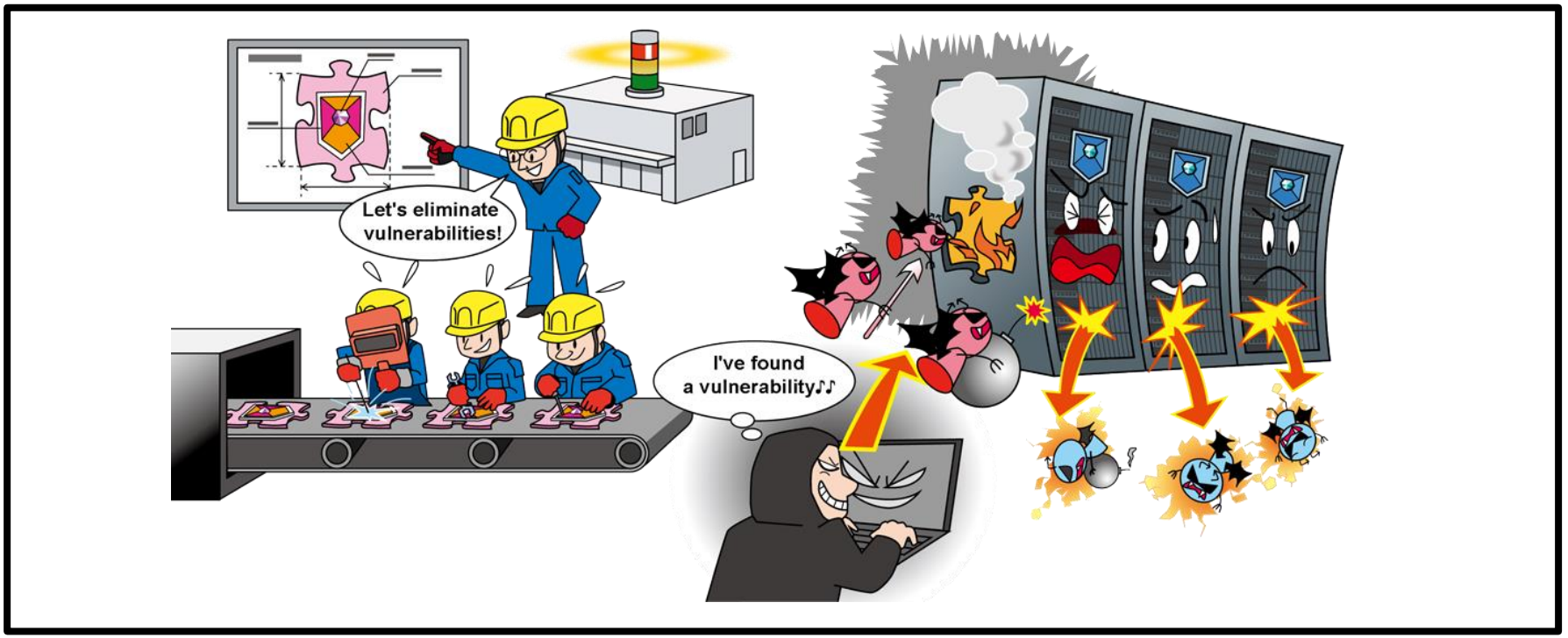
～ Vulnerable teleworking environments are being targeted～

- 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

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

～Difficult to take precautionary measures for attack prevention.
Take actions soon after the release of information about exploitation! ～



- 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

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

～Difficult to take precautionary measures for attack prevention.
Take actions soon after the release of information about exploitation! ～

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

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

～Difficult to take precautionary measures for attack prevention.
Take actions soon after the release of information about exploitation! ～

- Cases and Trends in 2022(1)
  - **Zero-day Attacks on Fortinet Products**
    - In December 2022, a vulnerability in FortiOS (the operating system for FortiGate and other security appliance products) was disclosed.
    - The vulnerability could allow malicious actors to bypass authentication and execute arbitrary code or commands.
    - Affected products included versions that are no longer supported.
    - In addition to countermeasures and mitigations, it was recommended that logs and traces of attacks exploiting the vulnerability be examined.

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

～Difficult to take precautionary measures for attack prevention.
Take actions soon after the release of information about exploitation! ～

- Cases and Trends in 2022(2)
  - **Zero-day Attacks on Microsoft Exchange Server**
    - In September 2022, a Vietnamese security firm published the occurrence of attacks exploiting an unpatched vulnerability in Microsoft Exchange Server.
    - Microsoft released information and mitigations for the vulnerability in the same month.
    - Microsoft said it had confirmed a limited targeted attacks that exploited the vulnerability to infiltrate users' systems, and announced interim mitigations until it released a fix in November.

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

～Difficult to take precautionary measures for attack prevention.
Take actions soon after the release of information about exploitation! ～

- Countermeasures
  - Organizations (System Administrators)
    - Preventions
      - Identify information assets and lay out a response framework
      - Monitor networks and block the communications for attacks using NDR and other methods
      - 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
      - Perform security assessments or penetration testing
    - Early detection
      - Implement UTM, IDS / IPS, WAF, Virtual patching, etc.

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

～Difficult to take precautionary measures for attack prevention.
Take actions soon after the release of information about exploitation! ～

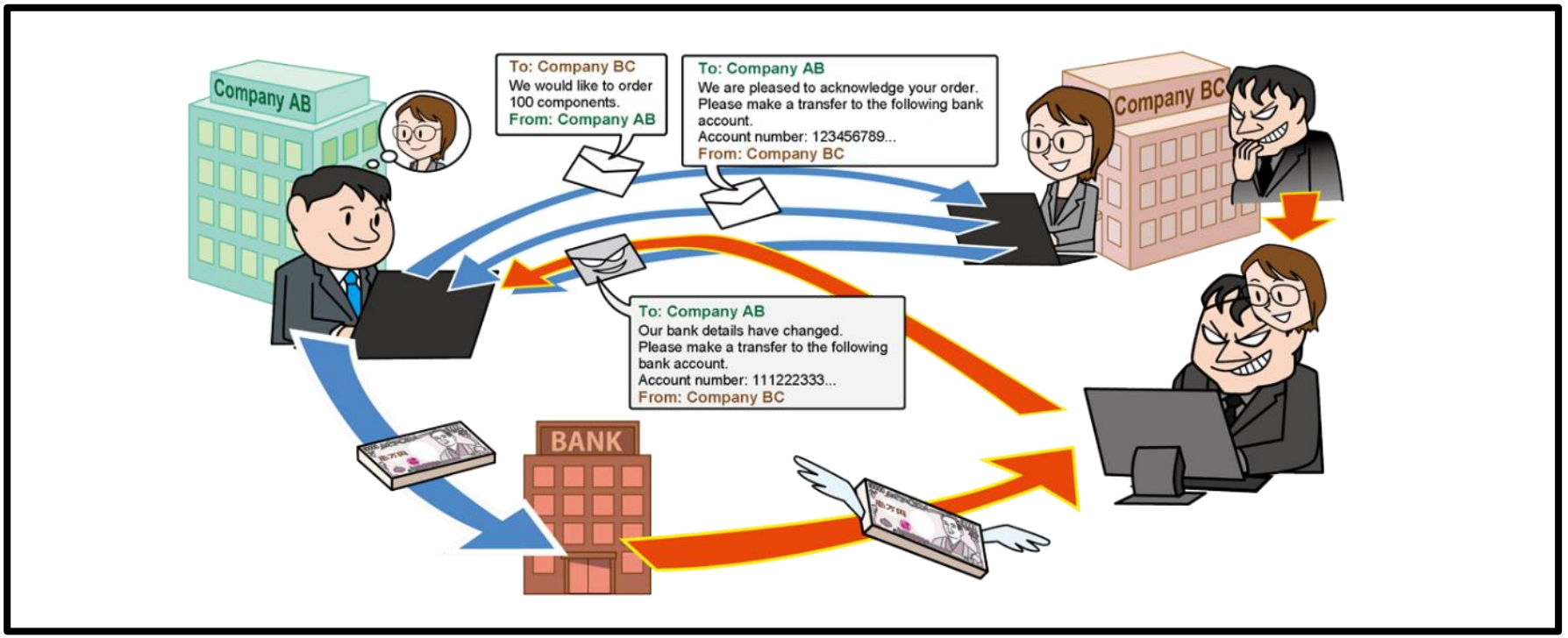
- Countermeasures
  - Organizations (System Administrators)
    - Actions before the release of a fix
      - Apply workarounds or mitigations
      - Stop using the software temporarily
    - Actions after the release of a fix
      - Apply the fix

        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

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

～Do you know who sent the email ?～



- 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

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

～Do you know who sent the email ?～

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

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

～Do you know who sent the email ?～

- Cases and Trends in 2022(1)

BEC - An attacker hijacked a legitimate email address

- In July 2022, Company A, a participant in the Cyber Information Sharing Initiative (J-CSIP), received a fraudulent billing email impersonating a representative of Company B.
- The attacker hijacked the Company B representative's email address and instructed Company A to change the account to which payment should be made.
- In the email correspondence, the attacker used a clever tactic to avoid detection of the scam by specifying a fake email address, similar to the email address of a person associated with Company B, as a Cc.

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

～Do you know who sent the email ?～

- Cases and Trends in 2022(2)
  - **Followed a fake email and sent money; later discovered to be fraudulent**
    - In November 2022, Wilson Learning Worldwide Inc., a human resources training company, disclosed that two of its subsidiaries had been victims of BEC in September of that year.
    - The two subsidiaries had received an email from a malicious actor instructing them to send money and had transferred a total of approximately 5.3 million yen.
    - After the transfer, the two subsidiaries became aware of the possibility of fraud, and conducted fact-finding through digital forensics, etc., and consulted with their insurance companies and investigative authorities.

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

～Do you know who sent the email ?～

Countermeasures

Organizations

- Preventions

- Gain a better understanding of BEC
- 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
- Implement DMARC ※Determine mail handling when domain authentication fails.

<Verification of the email authenticity>

- Confirm authenticity by multiple means other than email
- Pay attention to the following in emails

  Unusual phrases/Sender's email domain/Rushing a decision

<Proper management of email accounts>

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

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

～Do you know who sent the email ?～

- Countermeasures
  - Organizations
    - Actions after BEC recognition

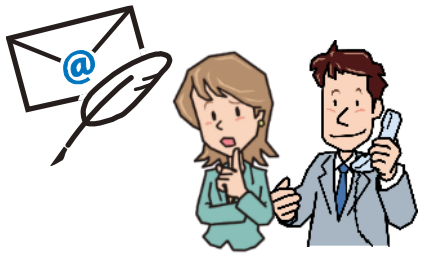
- Report to and consult with predefined contacts in accordance with the organization's policy

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

- Check email account settings

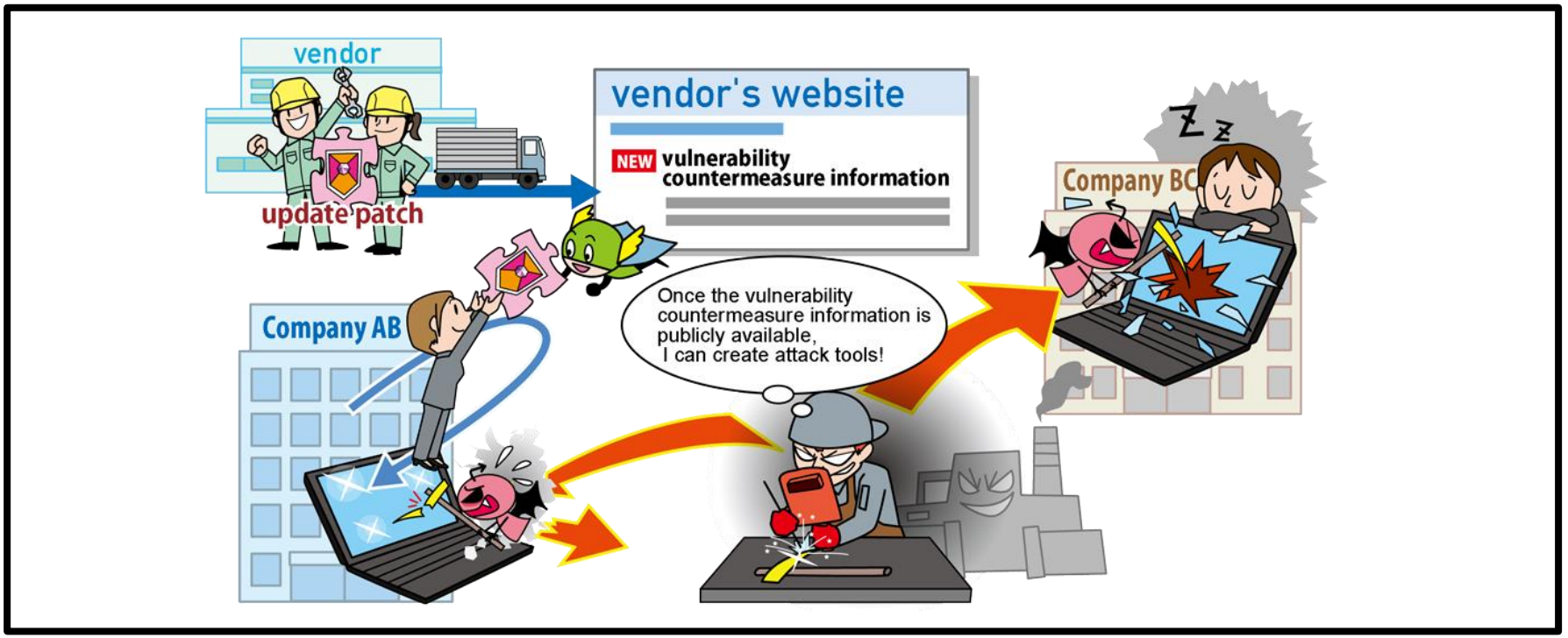
Check for unauthorized forwarding settings, folder sorting settings, etc. by the attacker

- Change passwords for all email accounts on the affected server



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

～”We’ll deal with it later.” Those few days can be fatal.～



- 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

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

～”We’ll deal with it later.” Those few days can be fatal.～

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

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

～”We’ll deal with it later.” Those few days can be fatal.～

- Cases and Trends in 2022(1)

Attacks targeting unpatched devices

- On May 4, 2022 (U.S. time), F5 Networks Inc. disclosed a vulnerability in its BIG-IP networking product.
- Remote attackers could exploit this vulnerability to bypass authentication, execute arbitrary code, or perform unauthorized operations.
- A proof of code (POC) was released by a security vendor on May 9, and around that time, communications and attempts to exploit the vulnerability to scan for unpatched devices that had not been patched were observed.

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

～”We’ll deal with it later.” Those few days can be fatal.～

- Cases and Trends in 2022(2)

Attacks targeting "Spring4Shell“

- On March 31, 2022 (U.S. time), VMware disclosed a vulnerability in the Spring Framework, a framework for developing Java web applications.
- The proof of code (POC) had already been released at the time of the vulnerability disclosure.
- Exploitations of the vulnerability was observed on the day of the announcement, and up to 37,000 attempted exploits were observed over a four-day period, affecting approximately 16% of the world's organizations.

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

～”We’ll deal with it later.” Those few days can be fatal.～

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

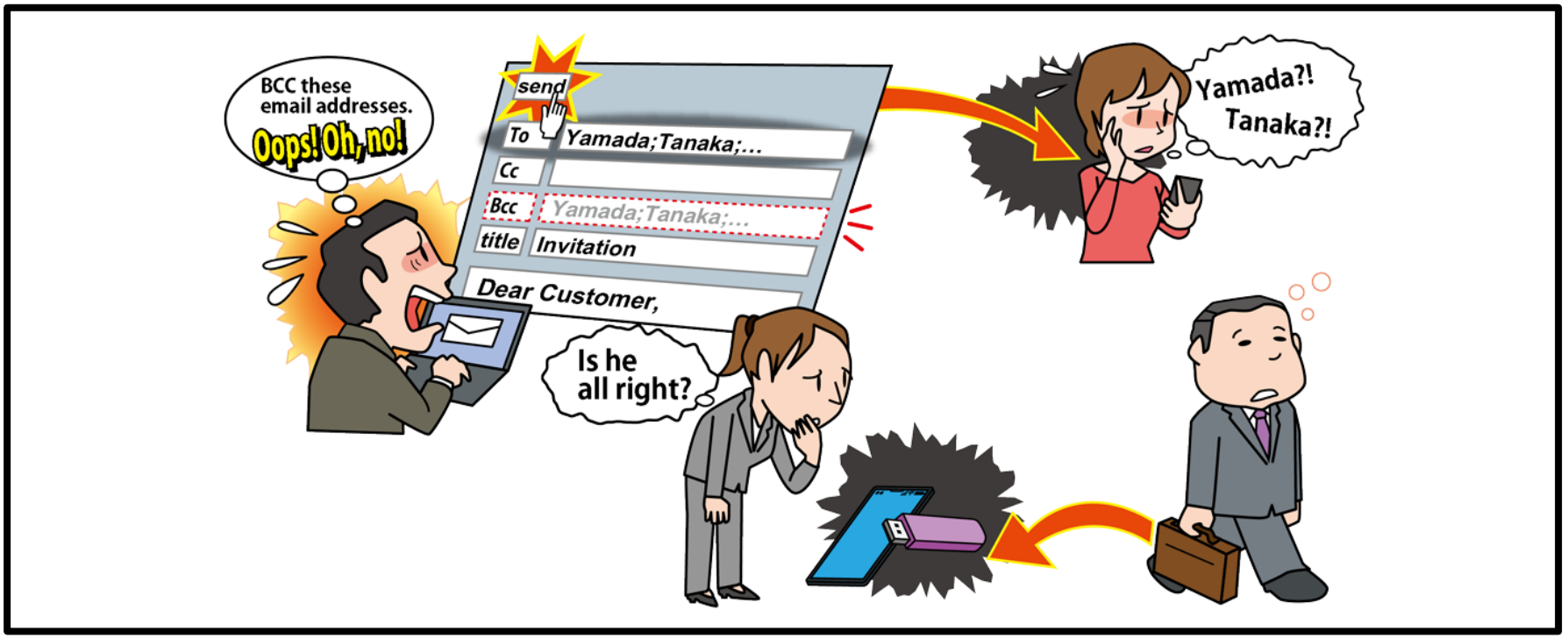
【8】Increase in Exploitations following the Release of Vulnerability Countermeasure Information

～”We’ll deal with it later.” Those few days can be fatal.～

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

【9】Unintentional/Accidental Information Leakage

～One carelessness can lead to a major incident…～



- 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

【9】Unintentional/Accidental Information Leakage

～One carelessness can lead to a major incident…～

- Causes

  - Carelessness of individuals from lack of information literacy and information ethics

    - 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.
    - Existence of fake email addresses that are designed to be misdirected
      - Malicious actors prepare email addresses for domains similar to those used by organizations
      - Information leaks at the time when an employee sends an email to these email addresses

【9】Unintentional/Accidental Information Leakage

～One carelessness can lead to a major incident…～

- Causes

• Insufficient organizational management framework ethics

- 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

【9】Unintentional/Accidental Information Leakage

～One carelessness can lead to a major incident…～

- Cases and Trends in 2022(1)
  - Loss of a USB flash drive containing personal information
    - In June 2022, Amagasaki City, Hyogo Prefecture, disclosed the loss of a USB flash drive containing information on the Basic Resident Register and resident tax, etc., of all its citizens.
    - An employee of the city's subcontractor went out for a drink with the USB flash drive.
    - After returning home, the employee noticed that he had lost his bag containing the USB flash drive.
    - Amagasaki City announced that the USB flash drive was password-protected and encrypted, and that no personal information had been leaked.

【9】Unintentional/Accidental Information Leakage

～One carelessness can lead to a major incident…～

Cases and Trends in 2022(2)

Personal information leaked due to misconfiguration of cloud access privileges

- In October 2022, JTB Corp., a travel agency, announced that it had leaked the personal information of 11,483 business operators who had applied for subsidies under a regional development project that the company was implementing as a subsidized business operator for the Japan Tourism Agency.
- The leak occurred because the data of users with login privileges to the cloud service used for information sharing were mutually visible, allowing them to download other users' subsidy application forms.
- The cause of the leak was a misconfiguration of access privileges for the cloud service.

【9】Unintentional/Accidental Information Leakage

～One carelessness can lead to a major incident…～

- Countermeasures
  - Organization (Person concerned)
    - Improvement of information literacy and information ethics

- Conduct security awareness training for employees
- Establish and regularly review organizational rules and verification processes

- Preventions

- Operate according to confirmation processes
- Define the importance of the information to be handled and operate accordingly
- 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

【9】Unintentional/Accidental Information Leakage

～One carelessness can lead to a major incident…～

- 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

【9】Unintentional/Accidental Information Leakage

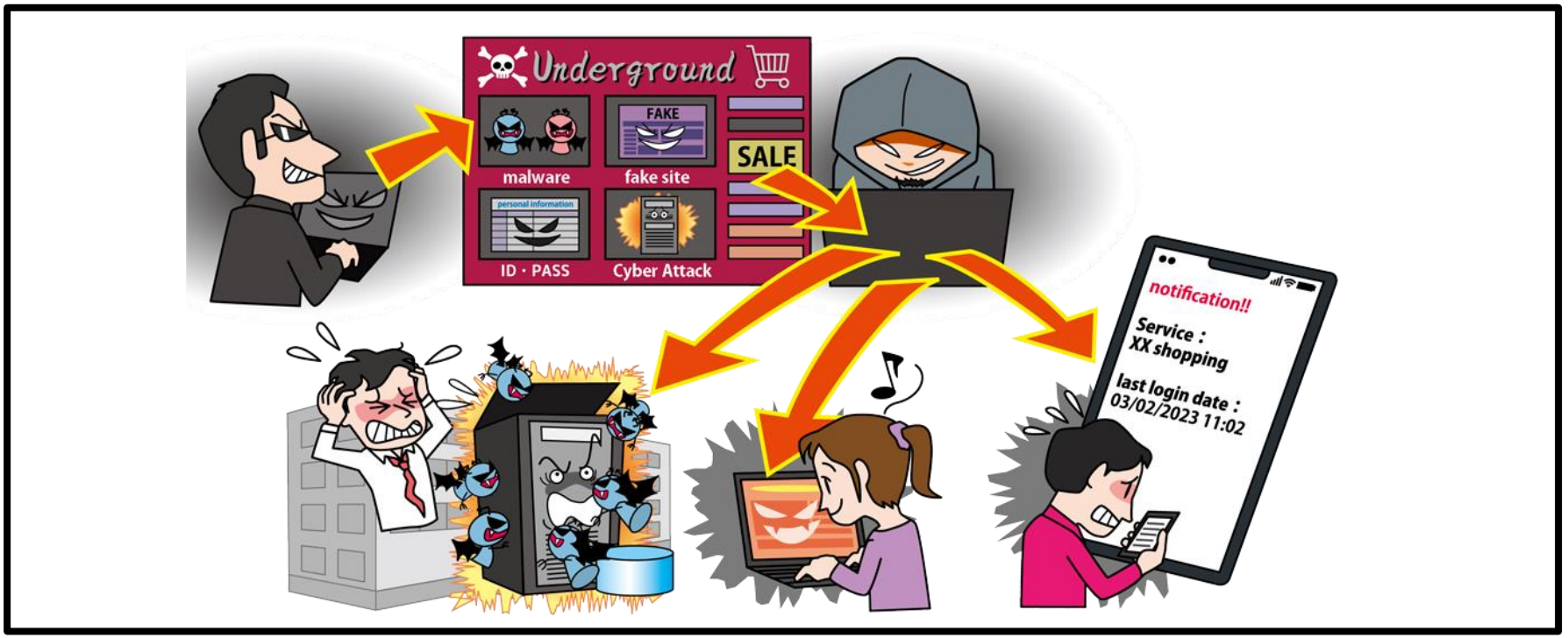
～One carelessness can lead to a major incident…～

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

    - Suspend credit cards
    - Consult with the police or public agencies about impacts of the incident

【10】Commercialization of Crime (Underground Services)

～Attackers buy your information as a commodity～



- Trading markets for services, tools, etc. used in cybercrime exist on websites that cannot be searched with common browsers
- Anyone can carry out cyber attacks without special knowledge

【10】Commercialization of Crime (Underground Services)

～Attackers buy your information as a commodity～

- Attack Methods
  - Attacks using purchased services or tools
    - Outsourced services for attacks, trade of attack tools
  - Unauthorized login to websites using purchased credentials
    - Selling or buying stolen personal information or credentials
  - Recruiting personnel to commit cybercrime
    - Securing personnel to commit organized cybercrime

【10】Commercialization of Crime (Underground Services)

～Attackers buy your information as a commodity～

- Cases and Trends in 2022(1)
  - Buying and selling stolen information on the dark web
    - According to a TV documentary broadcasted in January 2022, personal information stolen through phishing and other means was being sold on the black market on the dark web.
    - The information included account information and personal information from major shopping sites.
    - Personal information being traded included credit card information with a security codes, driver's license and insurance card information, and passport images.
    - The information is believed to have been stolen illegally from companies as well as through phishing.

【10】Commercialization of Crime (Underground Services)

～Attackers buy your information as a commodity～

- Cases and Trends in 2022(2)
  - Stolen personal information leaked to the dark web

•In September 2022, Dynam Japan Holdings Co. Ltd., a pachinko hall operator, disclosed that it had confirmed a personal information leakage.

•The company's server was attacked by ransomware and data was encrypted. The company noticed the attack by an alert.

•2,042 of names and account information of real estate owners of pachinko halls operated by related companies, 172 of payment information, and 1,218 of business cards and brokerage account information of business partners were leaked.

•All of the leaked information was publicly available on the dark web.

【10】Commercialization of Crime (Underground Services)

～Attackers buy your information as a commodity～

- Countermeasures
  - Senior Management
    - •Establishment of organizational framework
      - Establish a system (CSIRT, etc.) that can respond to problems
      - Secure budget for countermeasures and perform countermeasures continuously

【10】Commercialization of Crime (Underground Services)

～Attackers buy your information as a commodity～

- Countermeasures
  - System Administrators
    - Preventions
      - -Use services (ISP, CDN, etc.) to mitigate the impact of DDoS attacks
      - -Implement mitigation measures such as system redundancy
    - 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.
      - -Control communications (block DDoS attack sources, etc.)
      - -Prepare an alternative server in the event of a website outage and develop a means of notification
      - -Investigate impacts and detect causes

【10】Commercialization of Crime (Underground Services)

～Attackers buy your information as a commodity～

- Countermeasures
  - PC Users
    - Preventions

-Conduct security training

-Carefully check incoming emails and websites you visit

Do not click on links or open attachments in suspicious emails

-Apply updates and patches promptly

-Install security software

-Use authentication methods such as multi-factor authentication

【10】Commercialization of Crime (Underground Services)

～Attackers buy your information as a commodity～

- Countermeasures
  - PC Users
    - Early detection

      -Check suspicious login history
    - 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.

      -Restore from backups

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.

Conclusion

Practice common countermeasures

- Among countermeasures, there are effective countermeasures for multiple threats.
- By implementing the following "common countermeasures" together with the "basic security measures," it is possible to promote more efficient and extensive measures.

※ Detailed explanatory materials on common countermeasures are available on the 10 Major Security Threats 2023 website.

Common Countermeasures
Manage passwords properly
Improve information literacy and ethics
Do not easily open email attachments or click on links or URLs in emails or SMS
Report/communicate/consult appropriately
Establish an incident response system and activate it when an incident occurs
Implement appropriate security measures for servers, clients, and networks
Perform appropriate backup operations

Download of Detailed Documents

■ 10 Major Security Threats 2023

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/10threats/10threats2023.html