10 Major Security Threats 2024

[For Organizations]

IPA Better Life with IT

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

“Individuals”

“Organizations”

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

10 Major Security Threats - Threat Ranking

Rank	Threats for Organizations	Year of first appearance	Ranking status
1	Ransomware Attacks	2016	9th consecutive year, 9th time
2	Attacks Exploiting Supply Chain Weakness	2019	6th consecutive year, 6th time
3	Information Leakage by Internal Fraudulent Acts	2016	9th consecutive year, 9th time
4	Confidential Information Theft by APT	2016	9th consecutive year, 9th time
5	Attacks Targeting before the Release of Security Patches (Zero-day Attacks)	2022	3rd consecutive year, 3rd time
6	Unintentional/Accidental Information Leakage	2016	6th consecutive year, 9th time
7	Increase in Exploitations following the Release of Vulnerability Countermeasure Information	2016	4th consecutive year, 7th time
8	Financial Loss by Business Email Compromise	2018	7th consecutive year, 7th time
9	Attacks on New Normal Work Styles such as Teleworking	2021	4th consecutive year, 4th time
10	Commercialization of Crime (Underground Services)	2017	2nd consecutive year, 2nd time

10 Major Security Threats - Threat Ranking

Rank	Threats for Organizations	Year of first appearance	Ranking status
1	Ransomware Attacks	2016	9th consecutive year, 9th time
2	Attacks Exploiting Supply Chain W ness	2019	6th consecutive year, 6th time
3	Information Leakage by Internal Fr t Acts	2016	9th consecutive year, 9th time
4	Confidential Information Theft by AP		9th consecutive ear, 9th time
5	Attacks Targeting before the R of Security Patches (Zero-d		utive
6	Unintentional/Accidental		
7	Increase in Exploitations of Vulnerability Counterm		
8	Financial Loss by Business Em		time
9	Attacks on New Normal Work Styles such as Teleworking	2021	4th consecutive year, 4th time
10	Commercialization of Crime (Underground Services)	2017	2nd consecutive year, 2nd time

It is important to begin countermeasures with threats that are more relevant to your organization

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

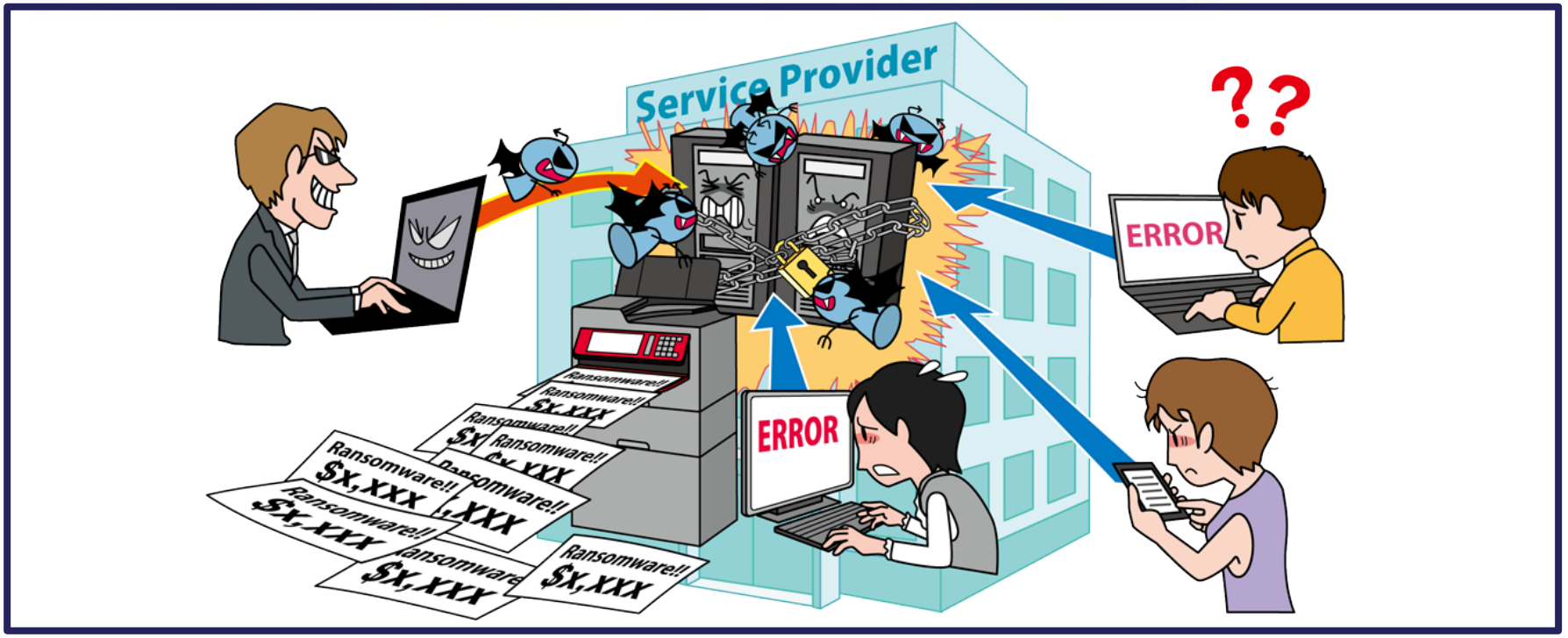
Target of Preparation	Additional Basic Security Measures	Purpose
All incidents	Clarify (understand) the scope of responsibility	Clarify (understand) who (which organization) is responsible for responding to incidents
Cloud Service Outage	Prepare alternative plans	Prepare alternative plans to ensure that 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)

Explanation of Each Threat

- From here, we will explain each threat.
- Start by learning about the threats that are more relevant to your organization.
- **The ”Basic Security Measures” described in the previous section are assumed to be in place and are not included in the following description.**

【1】Ransomware Attacks

～It doesn't matter what size or industry your organization is in! Your organization could be the next target...～



- Encrypt files stored on computers, etc. with ransomware and make them unavailable
- Extort money in exchange for restoration of encrypted files
- Steal and disclose information, and in some cases, threaten to disclose to business partners and others that the target organization is under attack
- Attack regardless of the size or industry of the target organization

【1】Ransomware Attacks

～It doesn't matter what size or industry your organization is in! Your organization could be the next target...～

♦ 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

～It doesn't matter what size or industry your organization is in! Your organization could be the next target...～

♦ 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

～It doesn't matter what size or industry your organization is in! Your organization could be the next target...～

- **Cases and Trends in 2023(1)**
  - **Disruption of port terminal operations due to ransomware infection**
    - In July 2023, the Nagoya Port Unified Terminal System (NUTS) was infected with ransomware.
    - This was caused by unauthorized access exploiting a vulnerability in remote access devices.
    - The physical server infrastructure and all virtual servers were encrypted.
    - Terminal operations had to be suspended for approximately two and a half days.

Cases and Trends in 2023(2)

Service outage due to ransomware infection

- In June 2023, MK System Co., Ltd.'s data center servers were infected with ransomware due to unauthorized access.
- Data was encrypted, and the company was unable to provide a service called Shalom, a cloud service for certified social insurance labor consultants.
- Approximately 3,400 users were affected, and a packaged version running on-premises was provided as an alternative.
- MK System lowered its earnings estimates due to the cost of rebuilding infrastructure facilities and other expenses.

Cases and Trends in 2023(3)

Infiltration of servers via VPN and the lateral deployment of ransomware

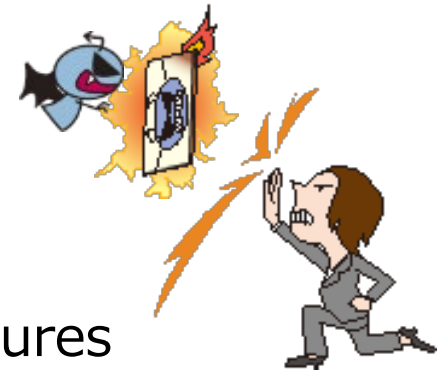
- In January 2023, the consumer cooperative Nara Coop announced that it had been hit by a ransomware attack.
- The attacker exploited a vulnerability in the network equipment and infiltrated servers via VPN, then collected internal information and deployed the ransomware laterally.
- Data containing the personal information of approximately 490,000 people was encrypted on 11 servers, but there is no confirmation of the data exfiltration.
- Databases that had been backed up had escaped infection and data could be recovered.

Countermeasures

Organizations (Senior management)

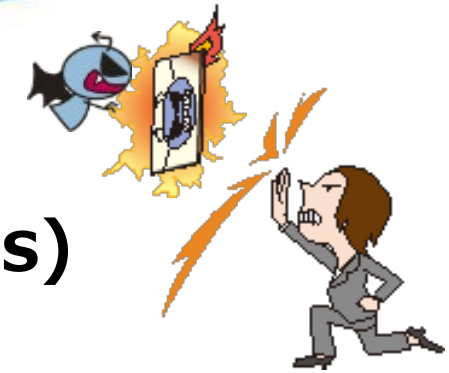
【Establishment of organizational framework】

- Establish the organization's incident response framework and respond to incidents
  - Appoint CISO
  - Establish CSIRT
  - Develop emergency response procedures
  - Notify employees about operational procedures
  - Conduct operational training
  - Prepare external cooperating partners
  - Establish internal rules and budget



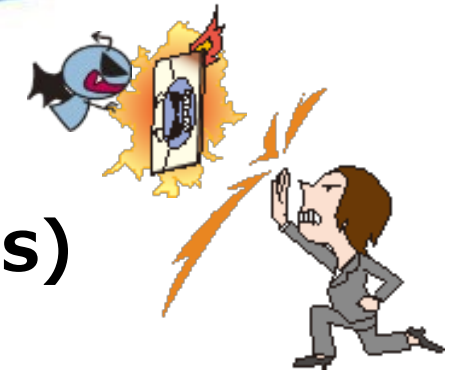
【1】Ransomware Attacks

～It doesn't matter what size or industry your organization is in! Your organization could be the next target...～



- **Countermeasures**
  - **Organizations (System Administrators, Employees)**

    【Preventions】
    - Establish the organization's incident response framework and respond to incidents
    - Do not easily open email attachments or click on links or URLs in emails or SMS messages
    - Enable multi-factor authentication settings
    - Do not run software from unknown sources
    - Implement appropriate security measures for servers, clients, and networks
    - Minimize and strengthen access controls on shared servers, etc.
    - Take measures to prevent unauthorized access to public server
    - Perform appropriate backup operations (acquisition, storage, and recovery training)



- **Countermeasures**
  - **Organizations (System Administrators, Employees)**
    【Actions after attack detection】
    - Report to, communicate with, and consult with predefined contacts as appropriate
      - Supervisors, CSIRT, related organizations, public agencies, etc.
    - Perform appropriate backup/recovery operations
    - Use decryption tools
    - Establish the organization's incident response framework and respond to incidents

【1】Ransomware Attacks

～It doesn't matter what size or industry your organization is in! Your organization could be the next target...～

- **Paying the ransom and choosing a ransomware recovery service provider**
  - In principle, data recovery should be performed without paying a ransom
  - Paying a ransom does not necessarily prevent data recovery or information leakage
  - If a ransomware recovery service provider was able to recover data by paying a ransom through a backroom deal with an attacker, the victim organization may be considered to have provided funds to the attacker
  - You need to be careful when choosing the ransomware recovery service provider you hire to handle the situation

【2】Attacks Exploiting Supply Chain Weaknesses

～Cooperate with partners in business and security measures, much like running a three-legged race～

- 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
～Cooperate with partners in business and security measures, much like running a three-legged race～

♦ 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
～Cooperate with partners in business and security measures, much like running a three-legged race～

- **Cases and Trends in 2023(1)**
  - **Customer information leakage from an outsourced vendor**
    - In January 2023, two insurance companies announced that their outsourced vendor had leaked personal information about their customers.
    - The cause was unauthorized access to the outsourced vendor's servers without appropriate security measures
    - The leaked personal information was posted on an overseas website.
    - At most, the personal information of approximately 1.3 million individuals was leaked, and the affected companies were forced to investigate and respond to the breach.

【2】Attacks Exploiting Supply Chain Weaknesses
～Cooperate with partners in business and security measures, much like running a three-legged race～

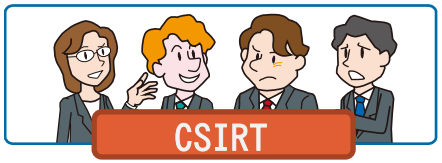
- **Cases and Trends in 2023(2)**
  - **Customer information leakage due to unauthorized access via a subcontractor's system**
    - In November 2023, LY Corporation, an Internet company, announced that its customer information had been breached.
    - Approximately 300,000 user information, 90,000 partner information, and 50,000 employee information were leaked.
    - The cause was unauthorized access to the company's internal system.
    - The breach was triggered by a virus infection on the PC of an employee of an outsourced company of NAVER Cloud Corporation, a contractor of LY Corporation.

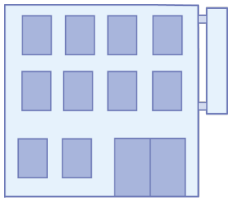
【2】Attacks Exploiting Supply Chain Weaknesses
～Cooperate with partners in business and security measures, much like running a three-legged race～

- **Cases and Trends in 2023(3)**
  - **Unauthorized access to partner company and leakage of customer information**
    - In November 2023, JCOM Co., Ltd. a provider of communications and broadcasting services, announced that its customer information had been breached.
    - The cause of the breach was unauthorized access to the access log server of a mobile application of Plume Design Inc., a U.S. partner company that provides the mesh Wi-Fi provided by JCOM.
    - Approximately 230,000 customer names and 5,000 customer email addresses were leaked.

【2】Attacks Exploiting Supply Chain Weaknesses
～Cooperate with partners in business and security measures, much like running a three-legged race～

- **Countermeasures**
  - **Organizations (Senior management)**
    【Preventions】
    - Establish the organization's incident response framework and respond to incidents
      - Appoint CISO
      - Establish CSIRT
      - Develop emergency response procedures
      - Notify employees about operational procedures
      - Conduct operational training
      - Prepare external cooperating partners
      - Establish internal rules and budget



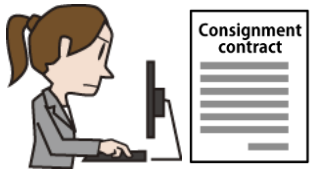


【2】Attacks Exploiting Supply Chain Weaknesses
～Cooperate with partners in business and security measures, much like running a three-legged race～

- **Countermeasures**
  - **Organizations (Your own organization)**

【Preventions】

- Ensure compliance with information management rules
- Assess the status of your organization's security measures with the Security Rating Service (SRS)
- Select trusted contractors, suppliers, and services
- Confirm contract content
- Manage contractor organizations
- Verify deliverables (e.g., understanding and managing software, implementing vulnerability countermeasures, etc.

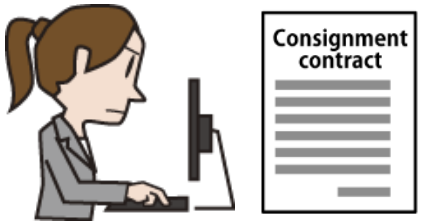


【2】Attacks Exploiting Supply Chain Weaknesses
～Cooperate with partners in business and security measures, much like running a three-legged race～

- **Countermeasures**
  - **Organizations (Your own organization)**

【Actions after attack detection】

- Establish the organization's incident response framework and respond to incidents
- Compensation to damage or impact of the attack

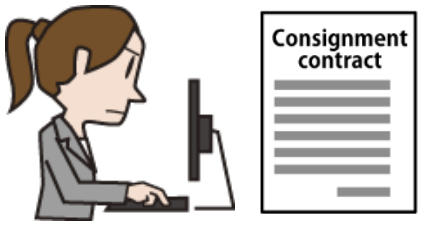


【2】Attacks Exploiting Supply Chain Weaknesses
～Cooperate with partners in business and security measures, much like running a three-legged race～

- **Countermeasures**
  - **Organizations (Your own organization and organizations involved in your supply chains)**

【Preventions】

- Establish a process for communicating with suppliers and contractors
- Review and audit the information security measures of suppliers and contractors
- Obtain information security certification
- Use publicly available materials from public organizations

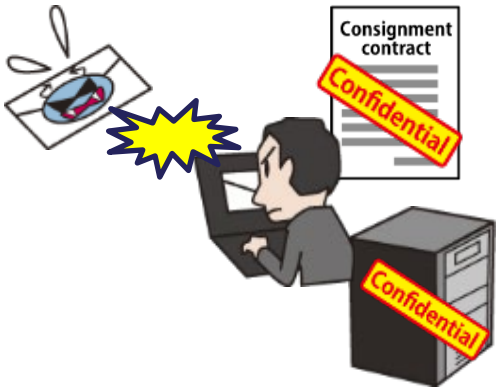


【2】Attacks Exploiting Supply Chain Weaknesses
～Cooperate with partners in business and security measures, much like running a three-legged race～

- **Countermeasures**
  - **Organizations (Your own organization and organizations involved in your supply chains)**

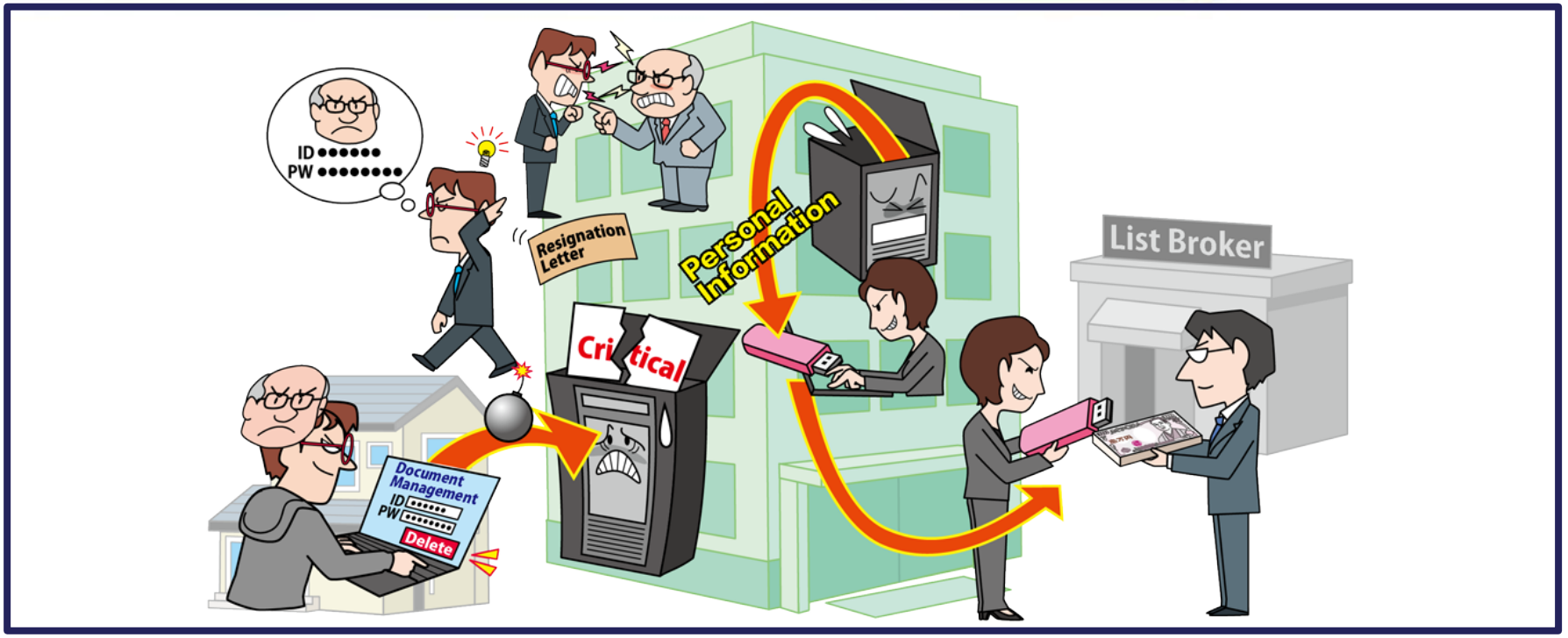
【Actions after attack detection】

- Report to, communicate with, and consult with predefined contacts as appropriate
  - Supervisors, CSIRT, related organizations, public agencies, etc.



【3】 Information Leakage by Internal Fraudulent Acts

～Your insiders could be targeting the organization's information. Create a system that doesn't allow internal fraud!～



- 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.

♦ 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.

Cases and Trends in 2023(1)

Customer information smuggled out and sold to a list broker

- In October 2023, NTT Business Solutions announced that a former temporary employee had smuggled out its customer information.
- Between July 2013 and January 2023, he exploited an administrator account to gain unauthorized access to systems in which he was involved.
- He copied customer information (at least 69 organizations, 9.28 million records) onto a USB flash drive and smuggled it out of the company.
- He is believed to have sold the customer information to a list broker for more than 10 million yen and was arrested.

Cases and Trends in 2023(2)

Improper provision of business card information to a new employer

- In September 2023, a former employee of World Corporation, an engineering outsourcing company, was arrested by the Tokyo Metropolitan Police Department on suspicion of violating the Act on the Protection of Personal Information (improper provision).
- Just before changing jobs to another company in the same industry, he shared his ID and password for logging into the business card information management system with an employee of the new employer.
- The new company used the illegally obtained business card information for sales activities, and there were instances of successful business contracts.

Cases and Trends in 2023(3)

Unauthorized access and deletion of internal information by a former employee

- In January 2023, a former employee of Kyoritsu Electrical Instruments Works, LTD. was arrested by the Metropolitan Police Department on suspicion of violating the Act Concerning the Prohibition of Unauthorized Computer Access and the Crime on Obstruction of Business by Damaging a Computer, etc..
- After leaving the company, he exploited the IDs and passwords of his former colleagues and supervisors to gain unauthorized access to the company's internal network and cloud to delete human resources, technical, and customer information.
- The employee resigned from the company for human relationship reasons, and it is believed that the purpose of his actions was to harass the employee.
- The cost of data recovery was approximately 6.6 million yen.

♦ Countermeasures

• Organizations (System Administrators)

【Preventions】

- Develop a basic policy
  - Pay attention to the "fraud triangle" *(three factors that create internal fraud: motivation/pressure, opportunity, and justification)
  - Create an information handling policy and establish work rules, etc., that provide for disciplinary action, etc., against internal fraudsters
- Identify information assets and establish a response framework
- Manage and protect critical information.
- Implement physical controls
- Improve employee information literacy and ethics
- Thoroughly train employees in human resource management and compliance

*Reference: Fraud Triangle – National Whistlebrower Center
https://www.whistleblowers.org/fraud-triangle

♦ Countermeasures

• Organizations (System Administrators)

【Early detection of attacks】

- Monitor system operation history
  - Monitor logs of access history to critical information, user operation history, etc.
  - Notify employees that the system is being monitored

♦ Countermeasures

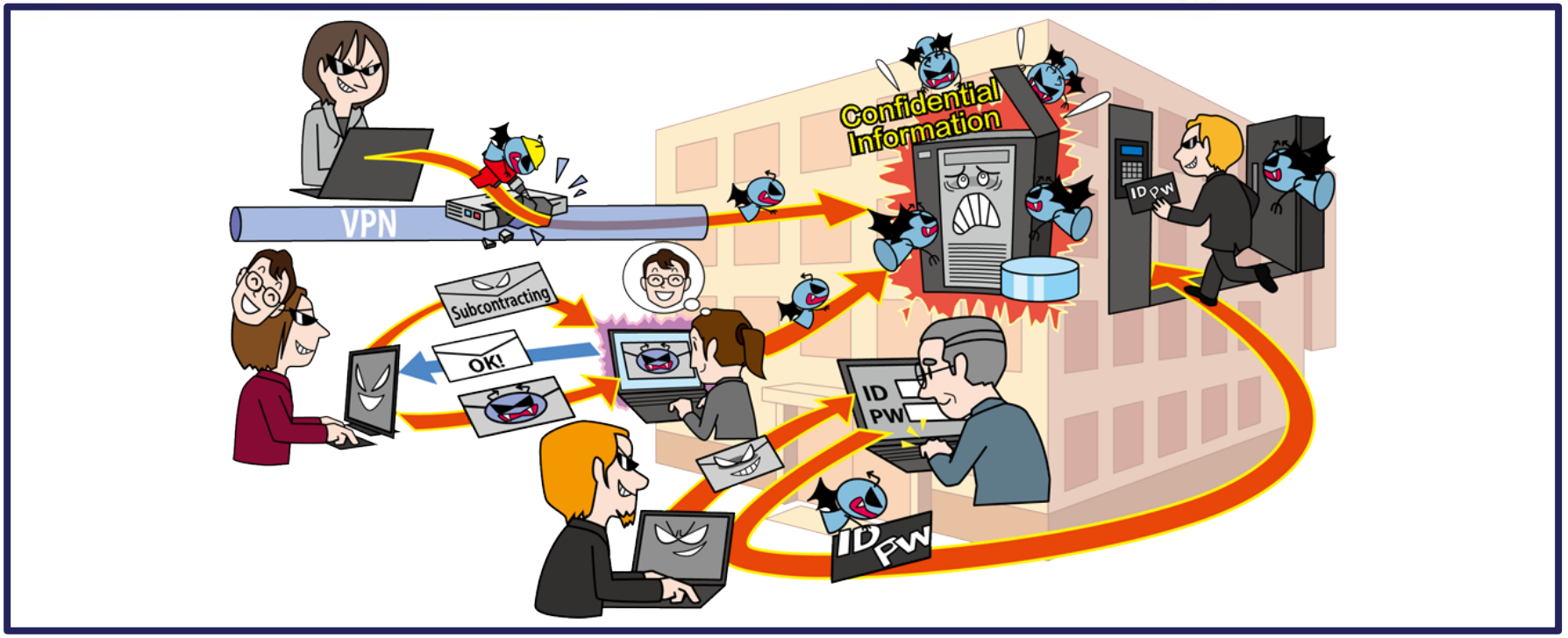
• Organizations (System Administrators)

【Actions after attack detection】

- Report to, communicate with, and consult with predefined contacts as appropriate
  - Supervisors, CSIRT, related organizations, public agencies, etc.
- Establish the organization's incident response framework and respond to incidents
- Punish internal fraudulent actors appropriately

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

～Attack methods are varied - do not create gaps in countermeasures～



- 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

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

～ Attack methods are varied - do not create gaps in countermeasures～

♦ Attack Methods

・Attack target organization with email

- Infect computers with a virus via email
  - Trick a target user into opening an attachment
  - Force a target user to click on links in emails
- Catch the target organization's employees or staff off guard and make them trust the attack email
  - Disguise the body of the email, the subject line, or the name of the attached file as being related to actual business or transactions
  - Use a real organization's sender name
  - Exchange multiple emails (interaction-type attack)

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

～ Attack methods are varied - do not create gaps in countermeasures～

♦ Attack Methods

・Tamper with websites

- Tamper with websites frequently used by the target organization
- Infect the PC with a virus when the target organization's employees or staff visit the tampered websites (Watering hole attack)

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

～ Attack methods are varied - do not create gaps in countermeasures～

♦ Attack Methods

・Unauthorized access

- Exploit vulnerabilities in equipment, devices, etc. used by the target organization to gain unauthorized access and infiltrate the organization
  - Cloud services
  - Web servers
  - VPN equipment
- Steal credentials, etc. and re-enter the organization's systems

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

～ Attack methods are varied - do not create gaps in countermeasures～

♦ Cases and Trends in 2023(1)

• Targeted email attack with multiple exchange

- In October 2023, the University of Tokyo announced that a targeted email attack had infected a faculty member's PC with a virus and stolen information.
- In July 2022, a faculty member received an email from a person claiming to be in charge of a real organization. In the course of exchanging messages, the faculty member clicked on a URL in the email and the PC was infected with a virus.
- Ultimately, the faculty member was unaware of the infection.
- A total of 4,341 records containing personal information of faculty members, students, and others, as well as past exam questions, may have been leaked.

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

～ Attack methods are varied - do not create gaps in countermeasures～

♦ Cases and Trends in 2023(2)

• Unauthorized access to JAXA, but no information stolen

- In November 2023, the Japan Aerospace Exploration Agency (JAXA) suffered a cyber attack and unauthorized access to its internal network.
- The unauthorized access was to an administrative server for general business use and did not contain any sensitive information.
- The unauthorized access is believed to have been caused by the exploitation of a vulnerability in the network equipment.
- JAXA, which was notified by an external organization, reported the incident to the MEXT (Ministry of Education, Culture, Sports, Science and Technology), and disconnected a part of the network, and began an investigation.

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

～ Attack methods are varied - do not create gaps in countermeasures～

♦ Cases and Trends in 2023(3)

• Warning about attacks on perimeter devices

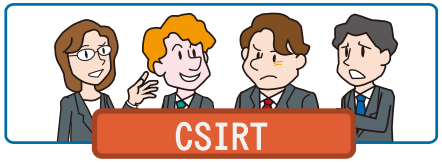
- In August 2023, IPA warned that vulnerabilities in security products installed at the boundary between a company or organization's network and the Internet have been targeted and used in APT attacks.
- Unauthorized access to the inside of the network carries the risk of leaking or falsifying information, or being used as a springboard to attack other organizations, so it is important to check daily and be prepared.
- It is also useful to use the "Guidance for Implementing ASM (Attack Surface Management) - Identify and Manage Your Organization's IT Assets Using Externally Available Information" published by the Ministry of Economy, Trade and Industry in May 2023.

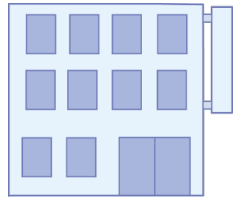
♦ Countermeasures

• Organizations (Senior management)

【Establishment of organizational framework】

- Establish the organization's incident response framework and respond to incidents
  - Appoint CISO
  - Establish CSIRT
  - Develop emergency response procedures
  - Notify employees about operational procedures
  - Conduct operational training
  - Prepare external cooperating partners
  - Establish internal rules and budget





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

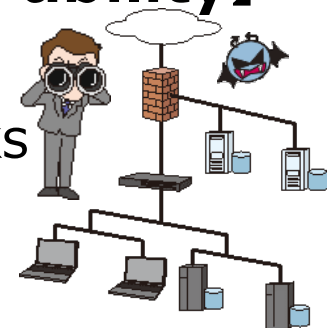
～ Attack methods are varied - do not create gaps in countermeasures～

IPA

♦ Countermeasures

• Organizations (Information Security Officers, System Administrators)

【Preventions / Improvement of response ability】



- Manage information and develop operation rules
- Continuously gather information about cyber attacks
- Improve information literacy and ethics
- Conduct regular incident response drills
- Implement appropriate security measures for servers, clients, and networks
- Create and maintain a list of application permissions
- Understand the implementation status of business partners' security measures
- Improve security measures including overseas offices, etc.

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

～Attack methods are varied - do not create gaps in countermeasures～

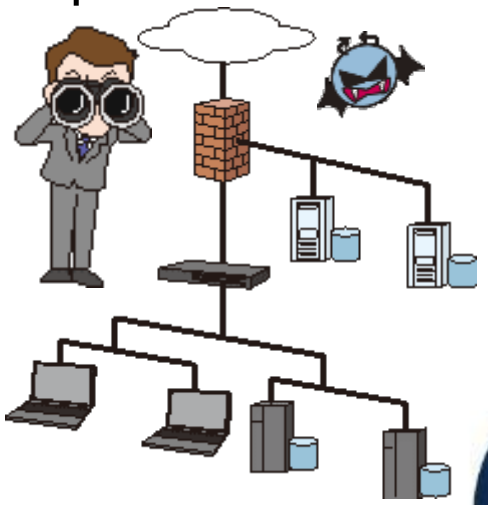
- **Countermeasures**
  - **Organizations (Information Security Officers, System Administrators)**

【Early detection of attacks】

- Implement appropriate security measures for servers, clients, and networks

【Actions after attack detection】

- Establish the organization's incident response framework and respond to incidents



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

～Attack methods are varied - do not create gaps in countermeasures～

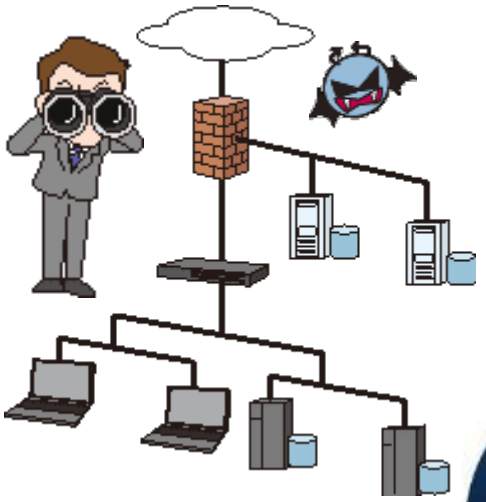
- **Countermeasures**
  - **Organizations (Employees, Stuff)**

【Preventions (Typically performed by organization-wide)】

- Do not easily open email attachments or click on links or URLs in emails or SMS messages

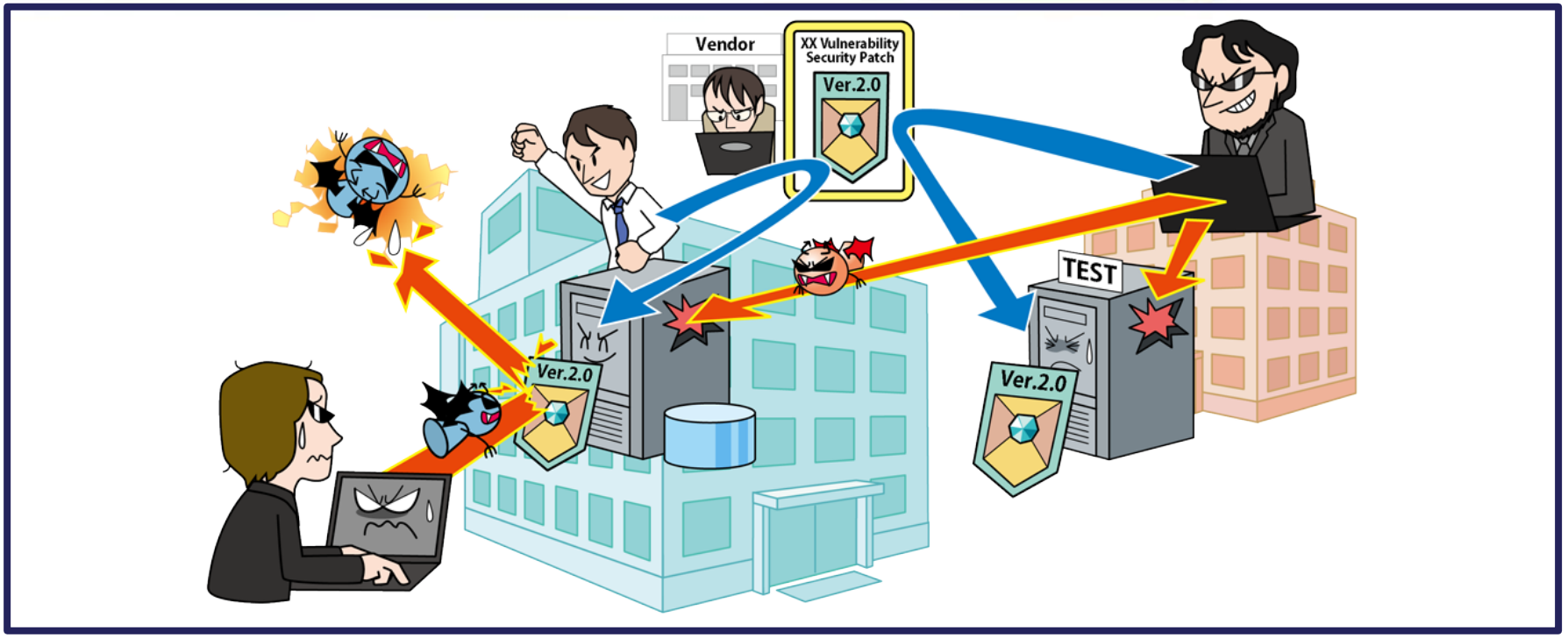
【Actions after attack detection】

- Establish the organization's incident response framework and respond to incidents



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

～Respond immediately when vulnerability countermeasure information is released～



- Attacks exploiting vulnerabilities are executed before the release of vulnerability fixes (patches) and workarounds
- Attacks affect many systems and users, including business and service outages
- When vulnerability countermeasure information is released, immediate action is required

【5】Attacks Targeting before the Release of Security Patches (Zero-day Attacks)
～Respond immediately when vulnerability countermeasure information is released～

♦ 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

- Attackers exploit vulnerabilities discovered that are discovered before fixes (patches) are released
- Exploitation techniques vary from vulnerability to vulnerability
  - Distributed Denial of Service (DDoS) attacks
  - Script-based attacks
  - Creation of privileged accounts

【5】Attacks Targeting before the Release of Security Patches (Zero-day Attacks)
～Respond immediately when vulnerability countermeasure information is released～

- **Cases and Trends in 2023(1)**
  - **Zero-day attacks exploiting HTTP/2 vulnerabilities**
    - In August 2023, large-scale DDoS attacks targeting vulnerabilities in the HTTP/2 protocol were observed.
    - In a series of attacks, over 398 million requests per second were observed, far exceeding the previous largest case of 46 million requests.
    - This attack, known as the HTTP/2 Rapid Reset attack, affects many software applications that support HTTP/2.
    - Vendors developing affected software shared information, and patches or updates were released.

Cases and Trends in 2023(2)

Zero-day attacks exploiting vulnerabilities in WinRAR

- In April 2023, it was discovered that the WinRAR, file compression software, contained several vulnerabilities, some of which were exploited in zero-day attacks.
- The vulnerabilities allowed a script placed in a folder of the same name to be executed when attempting to preview a file in a compressed file.
- On August 2, 2023, the developer, RARLAB, released an updated version, WinRAR 6.23, which fixed the vulnerability.

Cases and Trends in 2023(3)

Zero-day attacks on Cisco Systems Products

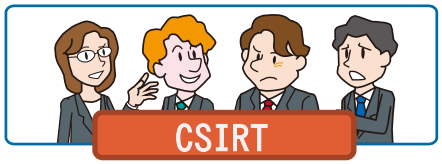
- In October 2023, Cisco Systems announced a vulnerability in Cisco IOS XE that allows remote creation of privileged accounts without authentication.
- The company also announced that zero-day attacks have been occurring since mid-September 2023.
- The company confirmed the vulnerability while assisting a customer.
- The company urged users of the product to take countermeasures recommended by the developer and others, and to confirm that they are not compromised.

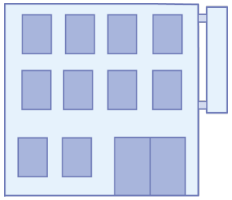
【5】Attacks Targeting before the Release of Security Patches (Zero-day Attacks)
～Respond immediately when vulnerability countermeasure information is released～

- **Reference Information (Latest Case Studies in 2024)**
  - **Zero-Day attacks on Ivanti VPN products**
    - On January 10, 2024 (U.S. time), Ivanti disclosed vulnerability information regarding Ivanti Connect Secure and Ivanti Policy Secure Gateways.
    - The vulnerabilities (CVE-2024-21887,CVE-2023-46805) could be exploited to bypass authentication and allow a third party to execute commands.
    - IPA also issued an advisory on January 11 (JST). On January 15, exploitation of these vulnerabilities was confirmed in Japan and the IPA recommended investigation of the breach and other measures.
    - Subsequently, vulnerabilities CVE-2024-21888, CVE-2024-21893 and CVE-2024-22024 were also identified and patches were released by February 16.

【5】Attacks Targeting before the Release of Security Patches (Zero-day Attacks)
～Respond immediately when vulnerability countermeasure information is released～

- **Countermeasures**
  - **Organizations (Senior management)**
    【Establishment of organizational framework】
    - Establish the organization's incident response framework and respond to incidents
      - Appoint CISO
      - Establish CSIRT
      - Develop emergency response procedures
      - Notify employees about operational procedures
      - Conduct operational training
      - Prepare external cooperating partners
      - Establish internal rules and budget





【5】Attacks Targeting before the Release of Security Patches (Zero-day Attacks)
～Respond immediately when vulnerability countermeasure information is released～

IPA

- **Countermeasures**
  - **Organizations (Software users, System Administrators)**

【Preventions】

- Identify information assets、establish a response framework
- Use software and software versions with good security support
- Collect and share vulnerability countermeasure information for software in use, and manage the status of countermeasures
- Implement appropriate security measures for servers, clients, and networks

【Early detection of attacks】

- Implement appropriate security measures for servers, clients, and networks

【5】Attacks Targeting before the Release of Security Patches (Zero-day Attacks)
～Respond immediately when vulnerability countermeasure information is released～

- Countermeasures
  - **Organizations (Software users, System Administrators)**

【Actions before vulnerability fixes (patches) are released】

- Apply workarounds and mitigations
- Temporarily stop using the software. In some cases, consider suspending service.

【Actions after vulnerability fixes (patches) are released】

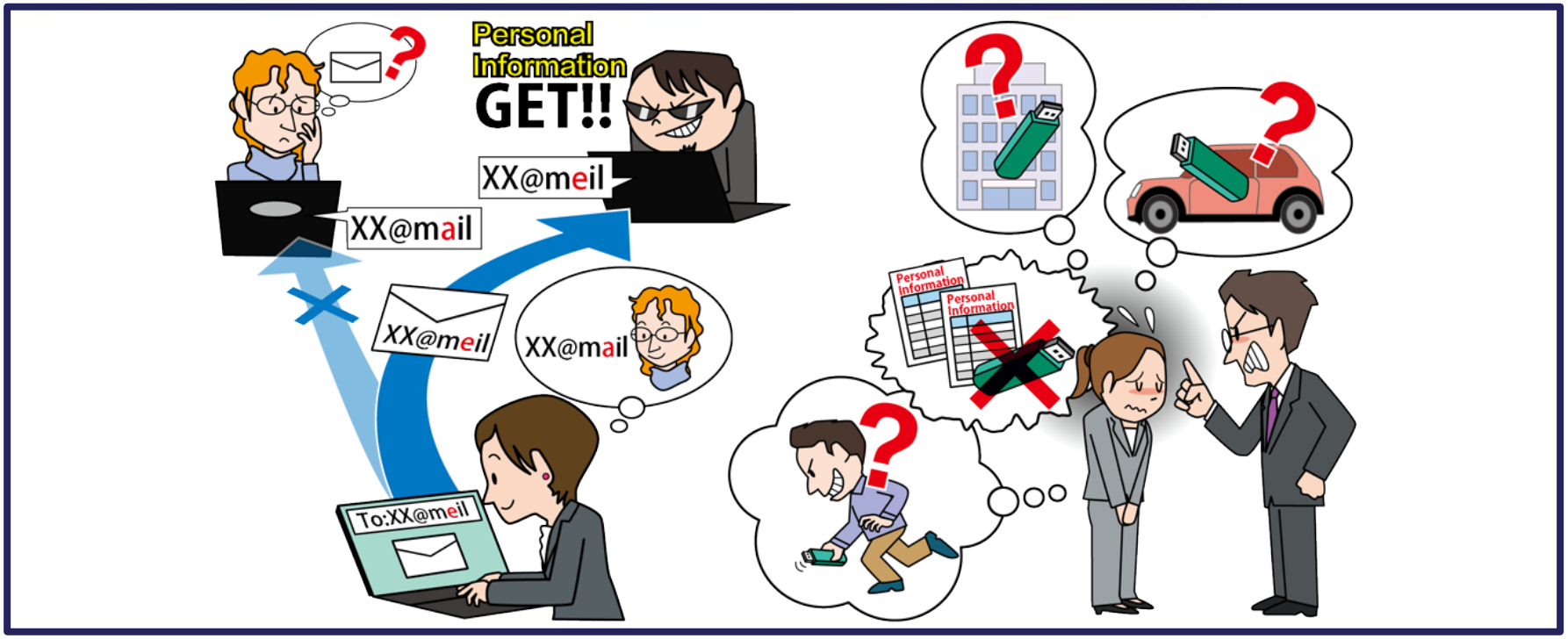
- Apply vulnerability fixes (patches)

【Actions after attack detection】

- Investigate impacts, determine causes, strengthen countermeasures
- Report to, communicate with, and consult with predefined contacts as appropriate
  - Supervisors, CSIRT, related organizations, public agencies, etc.

【6】Unintentional/Accidental Information Leakage

～Are you sure about the configuration? Check carefully!



- Unintentional confidential information leakage due to employee's carelessness
- Loss of social credibility of the organization and financial loss due to information leakage, secondary damage due to abuse of leaked information

【6】Unintentional/Accidental Information Leakage

～Are you sure about the configuration? Check carefully!

IPA

♦ Causes

・Problems with people handling information

- Low security awareness of the people who handling the information
  - Information is inadvertently leaked outside the organization due to a lack of understanding of the confidentiality and criticality of the information being handled.
    - Accidentally sending an email containing critical information to the wrong recipient
    - Losing a device containing critical information
    - Posting critical information on an external website, etc. for private purposes
- Situation of the individual when handling the information
  - Due to poor health or busy schedules, employees become distracted and cause information leakage through wrongly addressed emails, etc.

【6】Unintentional/Accidental Information Leakage

～Are you sure about the configuration? Check carefully!

IPA

- **Causes**

・Inadequate organizational rules and information handling procedures

- Inadequate process related to procedures for checking when information is taken outside the organization or when information is handled.

・Existence of spoofed email addresses intended for misdirection

- The malicious actor prepares an email address with a domain that is similar to the domain used by the organization (doppelganger domain).
  - Information is leaked when an employee accidentally sends a message to the email address.

【6】Unintentional/Accidental Information Leakage

～Are you sure about the configuration? Check carefully!

- **Examples of information leakage due to carelessness**
  - Misdirected emails (wrong address, wrong To/Cc/Bcc settings, wrong attachments, etc.)
  - Inadequate website settings (e.g., inadequate masking of critical information, incorrect public file or reference permissions, incorrect cloud settings, etc.)
  - Unconsidered posting of confidential information on external websites
  - Loss of information devices (PCs, smartphones, etc.) or storage media (USB flash drives, etc.) containing critical information
  - Loss of critical documents (paper media)

【6】Unintentional/Accidental Information Leakage

～Are you sure about the configuration? Check carefully!

- **Cases and Trends in 2023(1)**
  - **Personal information sent to an unintended email address**
    - In February 2023, Kagoshima University announced that it had sent the personal information of 829 people inside and outside the university to an unintended recipient due to an error in the email address of a mailing list.
    - The domain name "@gmail.com" was mistakenly listed as "@gmai.com" on the mailing list, resulting in emails containing personal information being sent to the doppelganger domain instead of the intended recipient.
    - After confirming the error, the university stopped sending email to the doppelganger domain and removed the incorrectly registered email address from the mailing list.

【6】Unintentional/Accidental Information Leakage

～Are you sure about the configuration? Check carefully!

- **Cases and Trends in 2023(2)**
  - **Personal information leakage due to misconfiguration**
    - In December 2023, the General Incorporated Foundation "Osaka Community Association" announced that personal information filled out on a Google form used for work commissioned by the Sumiyoshi Ward Office had been viewed online.
    - The reason was that the setting that allowed the personal information entered to be viewed was turned on, but when the form was created, the operation was started without confirming the screen that would be displayed after the responses were made.
    - This was discovered when a user who had filled out the Google Form pointed out the problem.
    - Shortly after being notified, the association corrected the Google Form, reported it to the appropriate parties, and is working on preventive measures.

【6】Unintentional/Accidental Information Leakage

～Are you sure about the configuration? Check carefully!

- **Cases and Trends in 2023(3)**
  - **Lost USB flash drive with copied personal information**
    - In December 2023, a person in charge of subcontracted work at Ushibuka Municipal Hospital in Amakusa City copied data containing personal information of 132 people onto a USB flash drive and took it out of the hospital.
    - The person noticed the loss of the USB flash drive while working at the company. The company searched for the possible location of the lost USB flash drive but could not find it. Three days after noticing the loss, the company filed a police report.
    - A few days after the missing report was filed, the rental car used by the person in charge was searched again, and the USB flash drive was found in the car.
    - Amakusa City reported and apologized to the patients involved.

【6】Unintentional/Accidental Information Leakage

～Are you sure about the configuration? Check carefully!

- **Countermeasures**
  - **Organizations (People concerned)**

【Preventions (includes measures to prepare for impacts)】

- Improve information literacy and ethics
- Operate according to confirmation processes
- Establish a system in which work is not concentrat individuals
- 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

【6】Unintentional/Accidental Information Leakage

～Are you sure about the configuration? Check carefully!

- **Countermeasures**
  - **Organizations (People concerned)**

【Early detection of attacks】

- Establish internal reporting system when problems occur
- Set up a point of contact with outsiders

【Actions after being a victim】

- Report to, communicate with, and consult with predefined contacts as appropriate
  - Supervisors, CSIRT, related organizations, public agencies, etc.
- Establish the organization's incident response framework and respond to incidents

【6】Unintentional/Accidental Information Leakage
～Are you sure about the configuration? Check carefully!

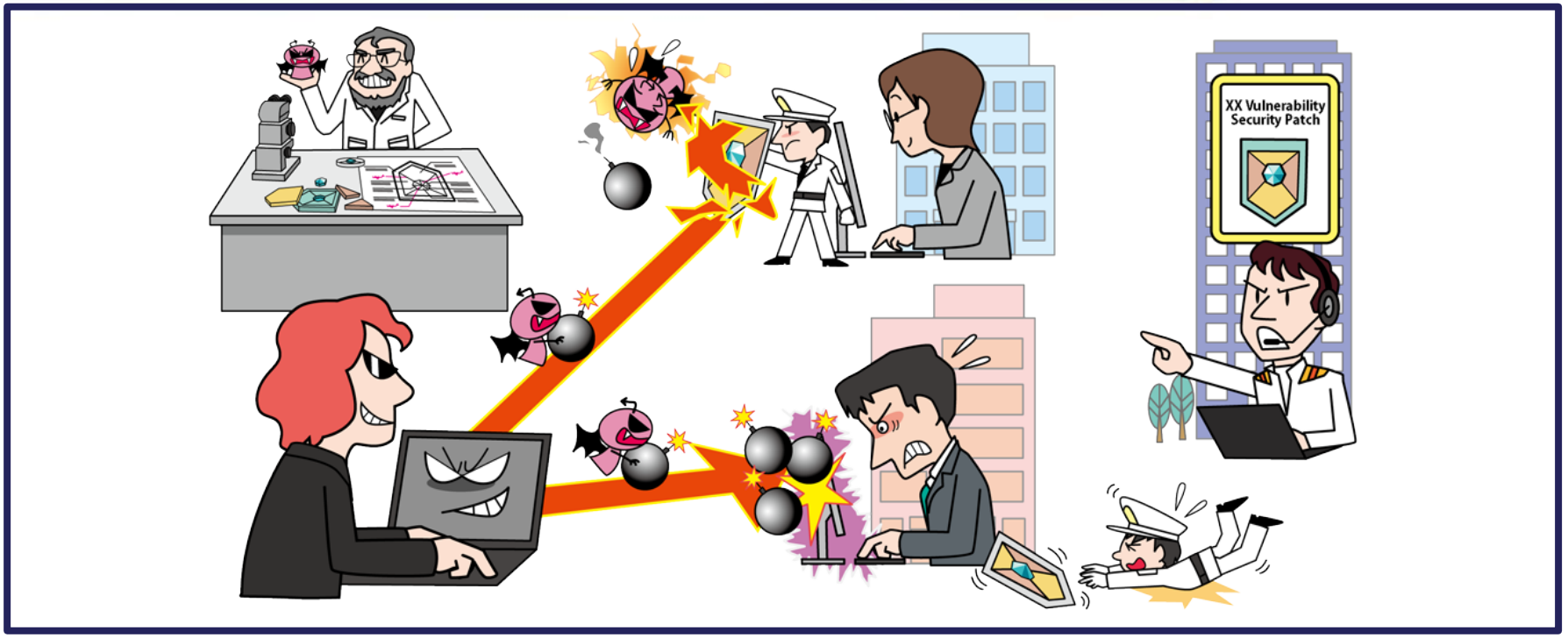
- **Countermeasures**
  - **Organizations (Victims)**

【Actions after being a victim】

- Suspend credit cards
- Report to, communicate with, and consult with predefined contacts as appropriate
  - Supervisors, CSIRT, related organizations, public agencies, etc.

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

～Do not leave vulnerabilities unaddressed but take immediate action before the damage spreads～



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

IPA

♦ Attack Methods

・Exploit vulnerabilities which have not yet taken countermeasures (N-day vulnerabilities)

- Vulnerabilities that remain open for a period of time (N days) before a publicly available patch is applied or a workaround is implemented are referred to as N-day vulnerabilities.
  - Organizations with poor software management are at greater risk of being victimized due to the longer period of time (N days) that the vulnerability remains unaddressed.
  - A PoC (proof-of-concept code) that demonstrates that the vulnerability can be exploited can be published and used in an attack.

IPA

♦ Attack Methods

・Use publicly available attack tools

- Attack tools for disclosed vulnerabilities are created in a short period of time.
- Attack tools are sold on Dark Web sites, etc., or provided as attack services.
- Vulnerability exploitation capabilities are implemented in open-source tools available to anyone and used for attacks.

Cases and Trends in 2023(1)

Attack activity increased after the release of the fixed software

- On October 25, 2023, the Apache Software Foundation released a fixed version of the Apache ActiveMQ and the Apache ActiveMQ Legacy OpenWire Module that fixed a remote code execution vulnerability.
- Technical information and PoC code for this vulnerability were publicly available, and according to Rapid7 Japan, on October 27, the company confirmed ransomware activity at several of its customers that appeared to exploit the vulnerability.
- NICT's (National Institute of Information and Communications Technology) darknet monitoring network, NICTERWEB, observed communications related to the vulnerability beginning around October 27, and a further increase in communications was observed around November 26, along with infection activity that appeared to be bots.

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

～Do not leave vulnerabilities unaddressed but take immediate action before the damage spreads～

- **Cases and Trends in 2023(2)**
  - **Vulnerabilities in VPN appliances had been the target of intermittent attacks**
    - In May 2023, the JPCERT Coordination Center issued an alert that targeted attacks exploiting vulnerabilities in the Array AG series of VPN appliances provided by Array Networks had been observed.
    - The IPA also issued an alert in August 2023 that vulnerabilities in security products installed at the Internet perimeter were being targeted in attacks on perimeter devices.
    - The two vulnerabilities were fixed in September 2022 and March 2022, respectively, and since overseas locations were also targeted, it is recommended that organizations take countermeasures and investigate breaches at their own overseas locations.

♦ Cases and Trends in 2023(3)

• Ongoing attacks on appliances with fixed vulnerabilities

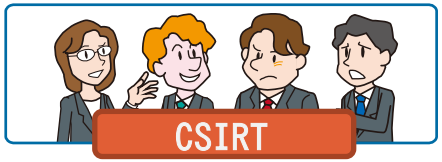
- On May 19, 2023, Barracuda Networks identified a remote command injection vulnerability in its Email Security Gateway (ESG) appliance and released a patch the following day.
- Even after the patch was applied, some organizations continued to experience attack activity.
- According to Barracuda Networks, the first exploitation of the vulnerability was in October 2022, and it recommends that compromised organizations replace their appliances.
- FBI, IPA, and JPCERT Coordination Center have issued an alert recommending further investigation of the breach, even for organizations that have applied the patch.

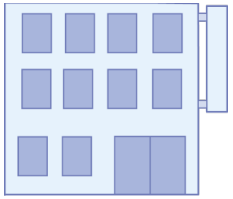
♦ Countermeasures

• Organizations (Senior management)

【Preventions】

- Establish the organization's incident response framework and respond to incidents
  - Appoint CISO
  - Establish CSIRT
  - Develop emergency response procedures
  - Notify employees about operational procedures
  - Conduct operational training
  - Prepare external cooperating partners
  - Establish internal rules and budget





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

～Do not leave vulnerabilities unaddressed but take immediate action before the damage spreads～

- **Countermeasures**
  - **Individuals、Organizations (System Administrators/Software users)**

【Preventions】

- Implement appropriate security measures for servers, clients, and networks
- Collect vulnerability countermeasure information and take prompt actions based on the information
- Shut down servers temporarily, etc.

【Early detection of attacks】

- Implement appropriate security measures for servers, clients, and networks

【Actions after attack detection】

- Report to, communicate with, and consult with predefined contacts as appropriate
  - Supervisors, CSIRT, related organizations, public agencies, etc.
- Establish the organization's incident response framework and respond to incidents

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

～Do not leave vulnerabilities unaddressed but take immediate action before the damage spreads～

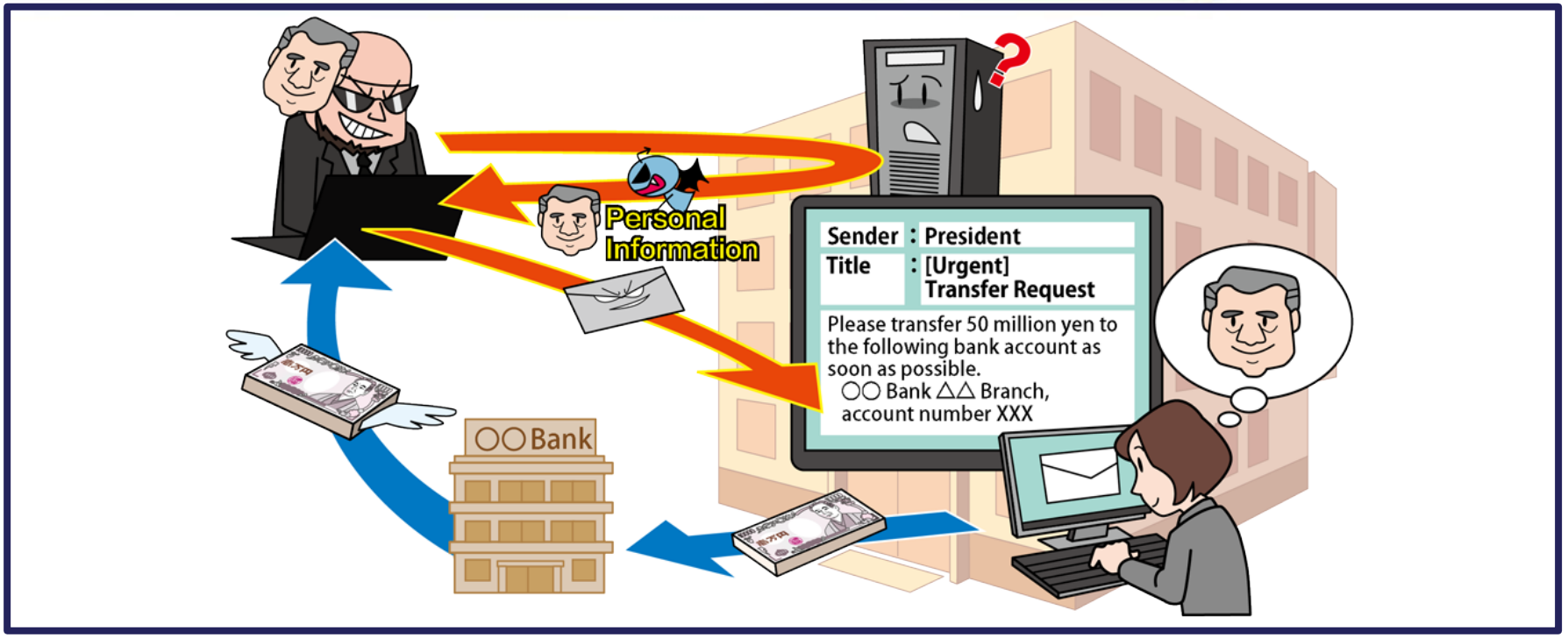
- **Countermeasures**
  - **Organizations (Development vendors)**

【Management of product security、establishing a response framework】

- Grasp embedded software in products and ensure its management
- Implement appropriate security measures for servers, clients, and networks
- Create a response procedure when vulnerabilities are discovered
- Establish a system to promptly disseminate information

【8】Financial Loss by Business Email Compromise

～Organizations have also become targets of bank transfer fraud～



- 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

【8】Financial Loss by Business Email Compromise

～Organizations have also become targets of bank transfer fraud～

IPA

♦ Attack Methods

・Disguise, Spoof, Abuse, Steal

- 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

【8】Financial Loss by Business Email Compromise

～Organizations have also become targets of bank transfer fraud～

- **Cases and Trends in 2023(1)**
  - **Spoofing using a combination of email and phone calls**
    - In August 2023, the J-CSIP (Initiative for Cyber Security Information Sharing Partnership of Japan) reported a business email compromise that combined email and phone calls that occurred in May 2023.
    - The attacker impersonated the chairman of the target organization and sent an email to the president of the organization's overseas subsidiary. In addition, the attacker impersonated the organization's senior managing director and contacted the president by phone, spoofing the caller ID as the organization's representative number.
    - When the president realized the spoofing from the conversation and pointed it out, the call was unilaterally disconnected, and no financial damage occurred.
    - Because of the potential for abuse of a deep-fake voice using generative AI technology, J-CSIP issued an alert to be on the lookout for similar tactics.

【8】Financial Loss by Business Email Compromise

～Organizations have also become targets of bank transfer fraud～

IPA

- **Cases and Trends in 2023(2)**
  - **Business email compromise impersonating a trusted business partner**
    - In December 2023, 3D MATRIX, a medical device company, announced that it had made a wire transfer to a fake bank account in response to an email impersonating one of its business partners requesting a payment account change.
    - The company also disclosed that it had subsequently made similar transfers, totaling 200 million yen on two occasions.
    - Since the company had a relationship of trust with the business partner, the company did not call the business partner directly to confirm the reason for the request to change the account to which the money was transferred.
    - The company cited measures to prevent a recurrence, including a review of the remittance process.

【8】Financial Loss by Business Email Compromise

～Organizations have also become targets of bank transfer fraud～

- **Countermeasures**
  - **Organizations**

【Preventions (includes measures to prepare for impacts)】

- Gain a better understanding of BEC
- Establish business workflows which make corporate governance works
- Establish business workflows that does not rely on email
- Grant electronic signature (S/MIME, PGP) to emails
- Implement DMARC
- Manage passwords properly
- Confirm authenticity by multiple means other than email
- Beware of emails that are out of the ordinary
- Beware of emails that urge you to make a decision

【8】Financial Loss by Business Email Compromise

～Organizations have also become targets of bank transfer fraud～

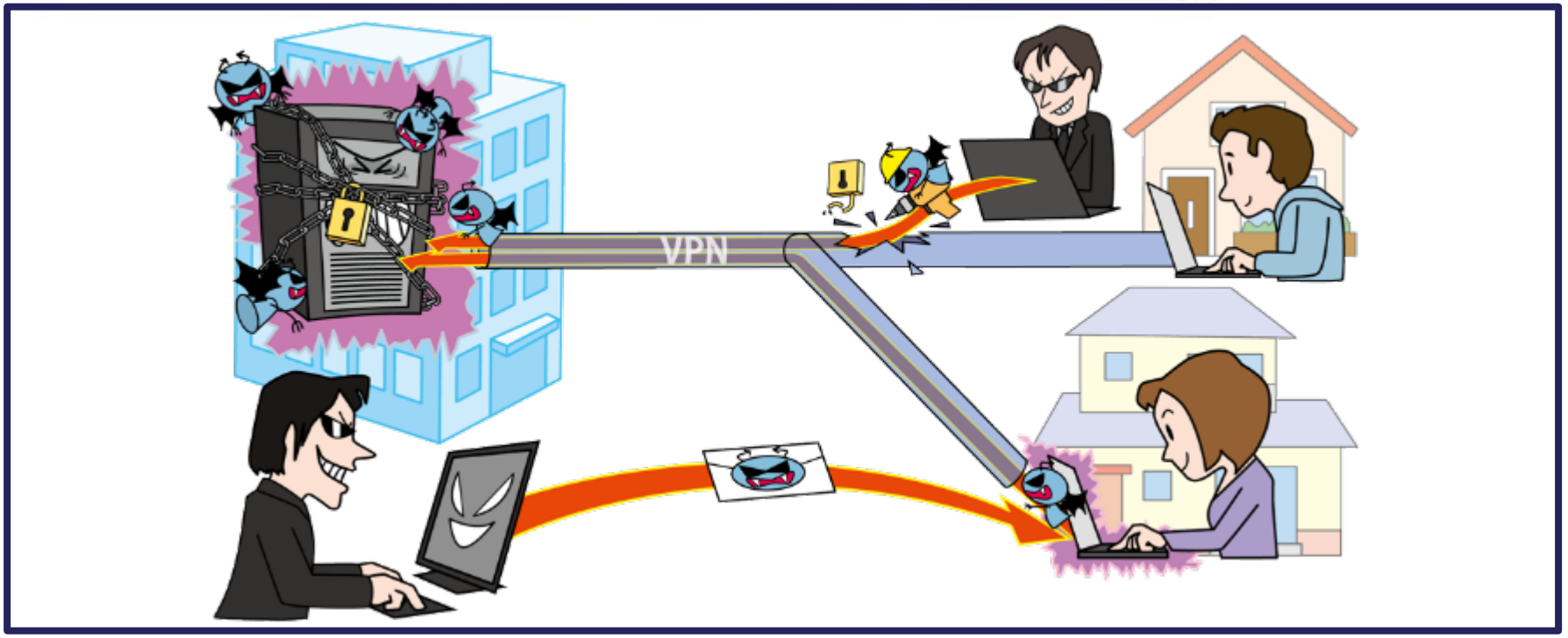
- **Countermeasures**
  - **Organizations**

【Actions after attack detection】

- Report to, communicate with, and consult with predefined contacts as appropriate
  - Supervisors, CSIRT, related organizations, public agencies, etc.
- Establish the organization's incident response framework and respond to incidents
- Check email account settings
- Manage passwords properly

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

～Teleworking environments continue to be targeted, take security measures～



- Since 2020, government agencies have been recommending teleworking as one of the new normal work styles, as part of their efforts to combat infectious diseases.
- While VPNs and other systems are being used in earnest, attacks targeting them are occurring.
- Vulnerabilities in the work environment increase the risk of web conferencing being eavesdropped on.

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

～Teleworking environments continue to be targeted, take security measures～

♦ Attack Methods / Occurrence Factors

・Inadequate teleworking environment and administration system

- Gain unauthorized access by exploiting vulnerabilities in teleworking software.
  - Exploit vulnerabilities, misconfigurations, etc. in products implemented for teleworking, such as VPNs.
    - Gain unauthorized access to internal systems or steal business information etc. from PCs.
    - Exploit vulnerable settings in web conferencing services to sneak a peek into web conferences.
- Attack vulnerable teleworking environments that are still operating as they were during the telework transition.
- Target the use of vulnerable home PCs or home networks.
  - Teleworking with personal devices and home network environments that lack adequate security measures can expose information to eavesdroppers.

【9】Attacks on New Normal Work Styles such as Teleworking
～Teleworking environments continue to be targeted, take security measures～

- **Cases and Trends in 2023(1)**
  - **Suspected intrusion through a remote access route set up for teleworking**
    - In October 2023, Seiko Group Corporation announced that the personal information of approximately 60,000 customers and business partners had been leaked.
    - The cause is believed to be an intrusion through a remote access route set up for teleworking.
    - The company was infected with ransomware that encrypted data stored on some servers in the data center and in the domestic offices.

- **Cases and Trends in 2023(2)**
  - **Vulnerabilities in Web conferencing services**
    - Microsoft addressed the vulnerability affecting Teams (CVE-2023-4863) in October 2023, and Zoom addressed the vulnerability affecting Zoom Rooms (CVE-2023-43590) in November 2023, with both companies releasing the latest versions.
    - Security measures are taken on a regular basis, and users are urged to update their products promptly, as not using the latest version of a product increases the risk of attack.

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

～Teleworking environments continue to be targeted, take security measures～

- **Cases and Trends in 2023(3)**
  - **Teleworking environments continue to be targeted**
    - According to the National Police Agency, the most common route of ransomware infection in the first half of 2023 was via VPN devices (35 cases), accounting for about 71% of the total.
    - Those infiltrated via remote desktops accounted for 5 cases, or about 10% of the total.
    - Vulnerabilities in teleworking devices and weak credentials were exploited in approximately 82% of cases.

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

～Teleworking environments continue to be targeted, take security measures～

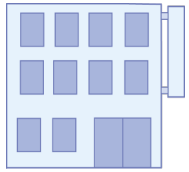
- **Countermeasures**
  - **Individuals(Teleworkers)**

【Preventions】

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

【Actions after attack detection】

- Report to, communicate with, and consult with predefined contacts as appropriate
  - Supervisors, CSIRT, related organizations, public agencies, etc.

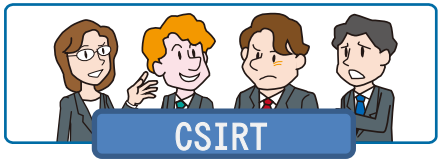


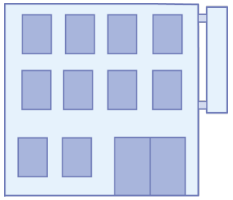
【9】Attacks on New Normal Work Styles such as Teleworking

～Teleworking environments continue to be targeted, take security measures～

- **Countermeasures**
  - **Organizations (Senior management)**

    【Establishment of organizational framework】
    - Establish the organization's incident response framework and respond to incidents
      - Appoint CISO
      - Establish CSIRT
      - Develop emergency response procedures
      - Notify employees about operational procedures
      - Conduct operational training
      - Prepare external cooperating partners
      - Establish internal rules and budget
      - Create communication and response procedures unique to the teleworking environment
    - Develop a teleworking security policy

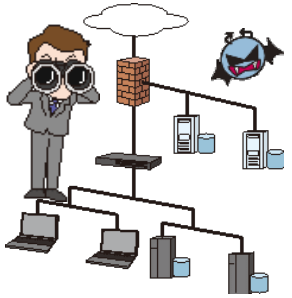




【9】Attacks on New Normal Work Styles such as Teleworking
～Teleworking environments continue to be targeted, take security measures～

- **Countermeasures**
  - **Organizations (Information Security Officers, System Administrators)**

    【Preventions】
    - 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
    - Improve information literacy and ethics
    - Implement appropriate security measures for servers, clients, and networks
    - Enforce network level authentication (NLA)
    - Enable multi-factor authentication settings



【9】Attacks on New Normal Work Styles such as Teleworking
～Teleworking environments continue to be targeted, take security measures～

- **Countermeasures**
  - **Organizations (Information Security Officers, System Administrators)**

【Early detection of attacks】

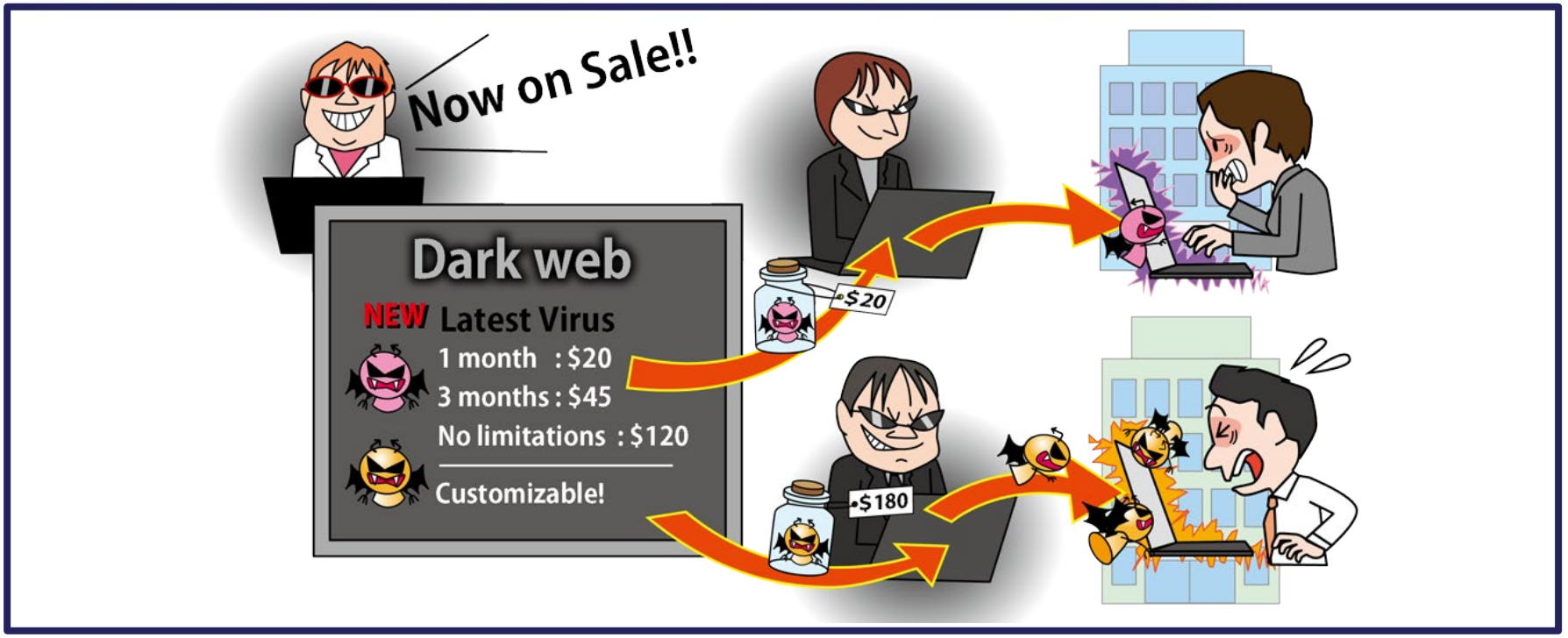
- Implement appropriate security measures for servers, clients, and networks

【Actions after attack detection】

- Establish the organization's incident response framework and respond to incidents

【10】Commercialization of Crime (Underground Services)

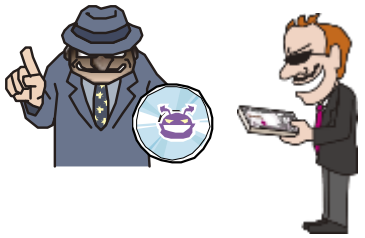
～The password, someone might already know it?～



- 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)
～The password, someone might already know it?～

- **Attack Methods**
  - **Attack using purchased services or tools**
    - Outsourced attack services and attack tools
      - Services that sell ransomware or means to gain unauthorized access have been identified.
  - **Use purchased credentials to gain unauthorized login to websites**
    - Purchase stolen personal information or credentials to gain unauthorized login to web services, etc.
  - **Recruit personnel to commit cybercrime**
    - Securing personnel to commit organized cybercrime



【10】Commercialization of Crime (Underground Services)
～The password, someone might already know it?～

- **Cases and Trends in 2023(1)**
  - **Trading of stolen ChatGPT accounts**
    - In April 2023, Check Point Software Technologies Ltd. warned of an increase in the trading of stolen ChatGPT paid accounts.
    - Account takeover (ATO) fraud leads to information leakage and enables the theft of credit card and other information associated with a paid account.
    - Some share stolen ChatGPT paid accounts for free to promote their own services and account theft tools.

【10】Commercialization of Crime (Underground Services)
～The password, someone might already know it?～

- **Cases and Trends in 2023(2)**
  - **Information of domestic manufacturing companies leaked to the Dark Web**
    - In June 2023, Aegis Tech announced the results of a survey of 30 major domestic manufacturing companies regarding account information leaked to the Dark Web.
    - All 30 companies surveyed were found to have account information and confidential documents uploaded to the Dark Web.
    - In particular, the number of information leaks and hacks in the manufacturing industry exceeded that of financial institutions and government agencies surveyed in the past.

【10】Commercialization of Crime (Underground Services)
～The password, someone might already know it?～

- **Cases and Trends in 2023(3)**
  - **Information-stealing malware sold for monthly fee with support**
    - In October 2023, Fortinet, Inc. alerted the public to the appearance of the ExelaStealer information-stealing malware.
    - This malware targets Windows platforms and steals credit card and other information.
    - It is being offered on the dark web for $20/month and one-time purchase options are available. Customization services are also offered.

【10】Commercialization of Crime (Underground Services)
～The password, someone might already know it?～

- **Countermeasures**

Countermeasures vary depending on the purpose and specifications of the tools and services used in the attack.
For more specific countermeasures, refer to other threats in this document.

- **Organizations (Senior management)**

【Establishment of organizational framework】

- Establish the organization's incident response framework and respond to incidents
  - Appoint CISO
  - Establish CSIRT
  - Develop emergency response procedures
  - Notify employees about operational procedures
  - Conduct operational training
  - Prepare external cooperating partners
  - Establish internal rules and budget

【10】Commercialization of Crime (Underground Services)
～The password, someone might already know it?～

- **Countermeasures**
  - **Organizations(System administrators)**

【Preventions】

- Use ISP (Internet Service Provider) or CDN (Content Delivery Network), etc. to mitigate the impact of DDoS
- Consider mitigation measures such as system redundancy
- Detect and block access from Tor nodes
- Implement appropriate security measures for servers, clients, and networks

【Early detection of attacks】

- Monitor the dark web
  - Use monitoring services and other means to confirm the existence of attack information or leaked information that could affect your organization.

【10】Commercialization of Crime (Underground Services)
～The password, someone might already know it?～

- **Countermeasures**
  - **Organizations(System administrators)**

【Actions after attack detection】

- Report to, communicate with, and consult with predefined contacts as appropriate
  - 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
- Perform appropriate backup/recovery operations
- Establish the organization's incident response framework and respond to incidents

【10】Commercialization of Crime (Underground Services)
～The password, someone might already know it?～

- **Countermeasures**
  - **Organizations(PC users)**

【Preventions】

- Improve information literacy and ethics
- Do not easily open email attachments or click on links or URLs in emails or SMS messages
- Implement appropriate security measures for servers, clients, and networks
- Use authentication methods such as multi-factor authentication

【10】Commercialization of Crime (Underground Services)
～The password, someone might already know it?～

- **Countermeasures**
  - **Organizations(PC users)**

【Early detection of attacks】

- Check suspicious login history

【Actions after attack detection】

- Establish the organization's incident response framework and respond to incidents

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 2024 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 messages
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 2024

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

https://www.ipa.go.jp/security/10threats/10threats2024.html

*You can also access the website by scanning the QR code below with a QR code reader application on your smartphone.