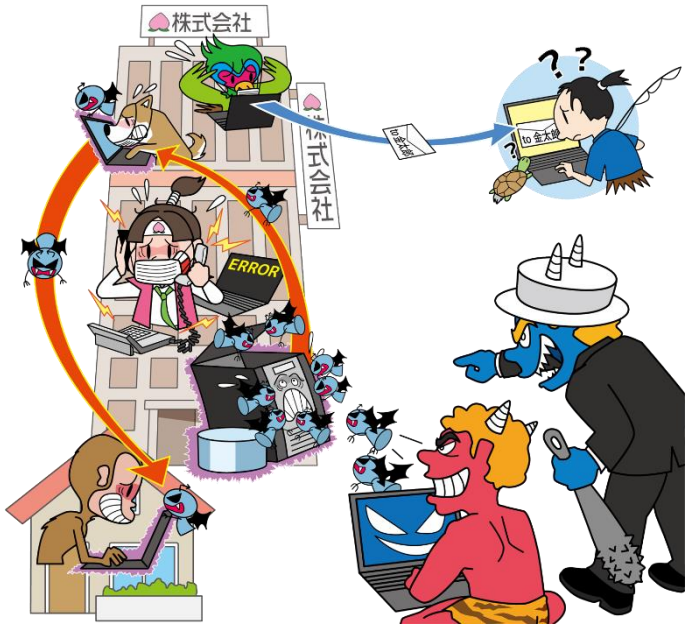
IPA Better Life with IT

10 Major Security Threats 2021

～No Way! Our organization has been compromised!
Be united and defend with full effort!～

[For Organizations]



IT Security Center (ISEC)
Information-Technology Promotion Agency (IPA), Japan
July 2021

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”

IPA

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”

Explain threats from two perspectives:
“Individuals” and “Organizations”

10 Major Security Threats – Threat Ranking

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

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

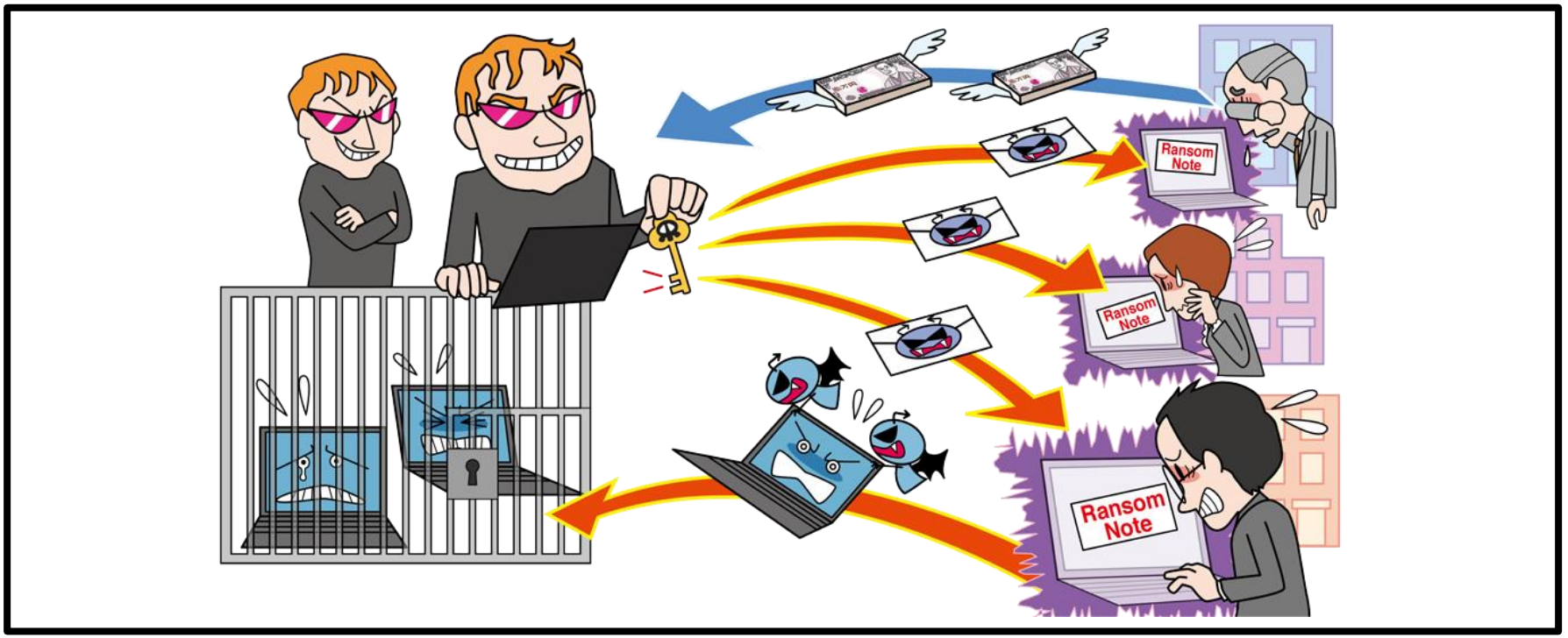
10 Major Security Threats 2020
For Organizations

Explanation of Each Threat

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

【1】Ransomware Attacks

～Ransomware attacks targeting organizations increased～



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

【1】Ransomware Attacks

～Ransomware attacks targeting organizations increased～

Attack Methods

- Infect computers with virus (ransomware) and extort money

- E-mails
  - Trick a target user into opening an attachment
- Drive-by downloads from compromised websites
  - Falsify websites to trick a target user into downloading ransomware
  - Trick a target user into browsing the falsified website using e-mail etc.

【1】Ransomware Attacks

～Ransomware attacks targeting organizations increased～

Attack Methods

- Infect computers with virus (ransomware) and extort money

Exploiting Vulnerabilities

- Exploit OS 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 attacks targeting organizations increased～

- Cases and Trends in 2020 (1)
  - Video game developer's servers infected with ransomware
    - Data in the video game developer's in-house system was encrypted and operations including e-mail and file access were temporary suspended
    - Attackers threatened the company to expose customer and shareholder information, etc.
    - Ransomware operator demanded to pay ransom if the company would like to get the decryption key and avoid data exposure.

【1】Ransomware Attacks

～Ransomware attacks targeting organizations increased～

- Cases and Trends in 2020 (2)
  - Ransomware specifically targeting a particular organization
    - Automobile manufacturer hit by cyberattack and large-scale system failure occurred
    - Shipments at domestic and overseas factories temporary suspended
    - Office network system was also affected such as employees unable to use computers

【1】Ransomware Attacks

～Ransomware attacks targeting organizations increased～

- Countermeasures
  - Senior Management
    - Establishment of organizational framework
      - Secure budget for countermeasures and perform countermeasures continuously

【1】Ransomware Attacks

～Ransomware attacks targeting organizations increased～

- Countermeasures
  - System Administrators, Employees

  - Preventions

- Check incoming e-mails and visiting websites carefully
- Don’t easily click on attachments and URLs
- Stop using expired OS and migrate to effective OS
- Make an application permission list
- Use filtering tools (e-mail, web)
- Segregate networks
- Minimize access privileges of shared servers and strengthen administration
- Perform data backups

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

※Regularly check that you can recover from the data backups

- Overall security measures equivalent to those against targeted attacks are required

【1】Ransomware Attacks

～Ransomware attacks targeting organizations increased～

- Countermeasures
  - System Administrators, Employees
    - Actions after attack detected

- Contact/notify predefined contact such as CSIRT
- Recover from backups
- Use file decryption tools
- Investigate impact and detect causes, strengthen countermeasures
- Isolate the breach to prevent the damage from spreading to related organizations and business partners

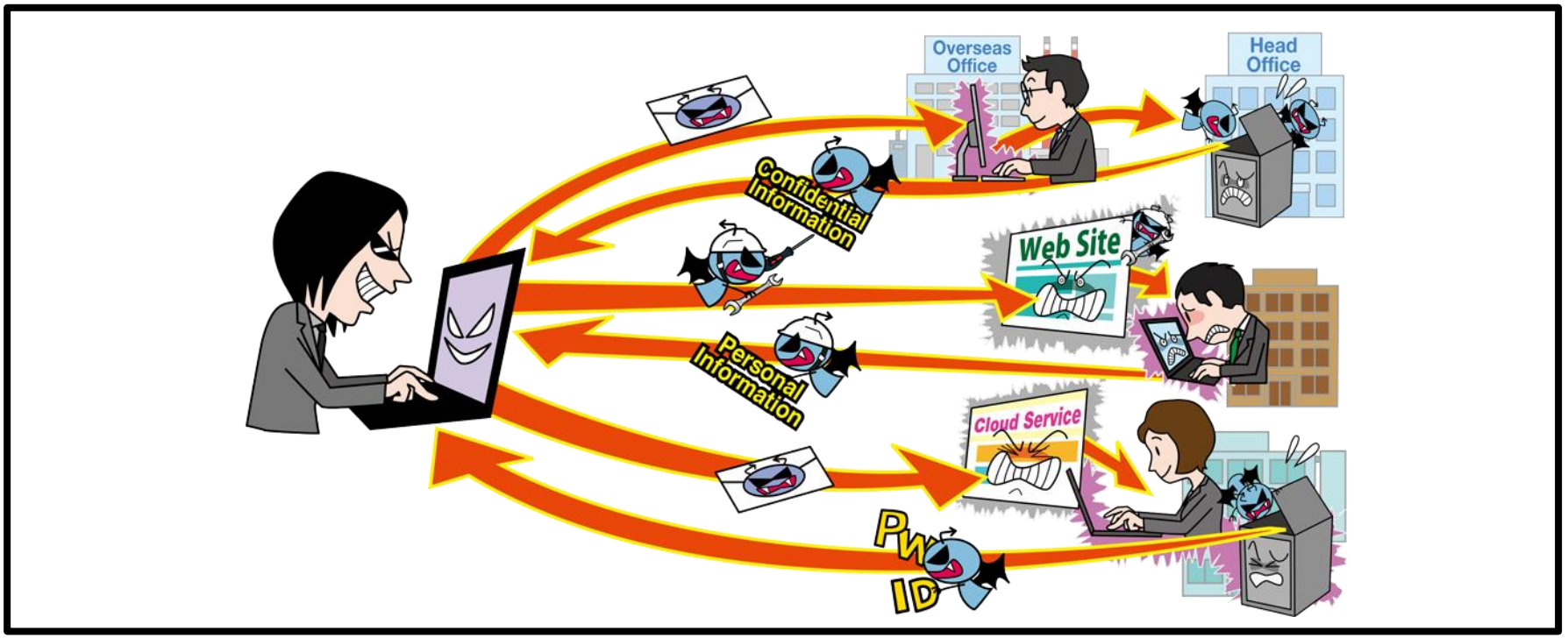
<Exceptional measure>

Pay ransom, although not recommended (e.g., when encrypted files are life-threatening)

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

IPA

～Targeted attack emails that took advantage of the COVID-19 pandemic were observed～



- 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

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

IPA

～Targeted attack emails that took advantage of the COVID-19 pandemic were observed～

Attack Methods

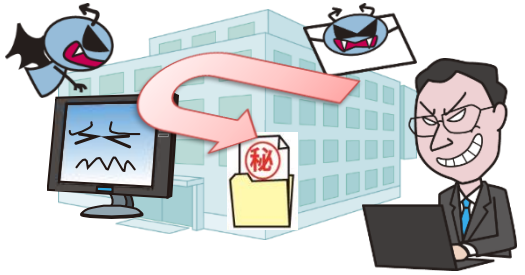
- Infect the target of attack with virus by e-mail, website, etc.

Targeted E-mail 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
- Falsify those websites to download viruses
- Employees of the target organization access those websites and get infected with viruses



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

IPA

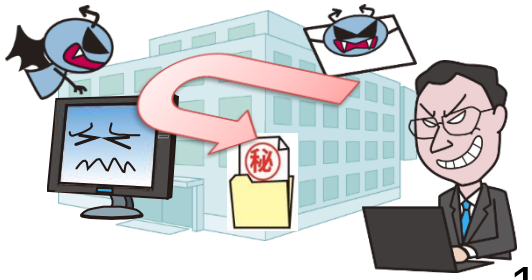
～Targeted attack emails that took advantage of the COVID-19 pandemic were observed～

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 or web servers 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



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

～Targeted attack emails that took advantage of the COVID-19 pandemic were observed～

Cases and Trends in 2020 (1)

Multiple reports of unauthorized access believed to be APT attacks

[Electronics manufacturer]

- Gained unauthorized access to the defense division's server
- Gained unauthorized access to the defense division's server
- The manufacturer had been attacked since December 2016, but could not detect

[Heavy industry manufacturer]

- Suspicious communications between multiple overseas and domestic sites were detected, and attacks were uncovered
- Attacks were sophisticated and left no traces

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

～Targeted attack emails that took advantage of the COVID-19 pandemic were observed～

Cases and Trends in 2020 (1)

Information sharing on cyber attacks

- Reports from the Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP)
- Reports of information on cyber attacks to IPA from J-CSIP participating organizations

[October to December 2020]

Reports of information on cyber attacks: 479 cases

※ Information considered to be APT attack email: 16 cases

[November 2020]

Reports of information on suspicious Japanese emails with virus attached

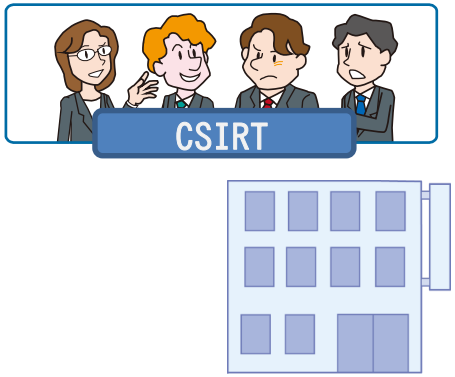
※ZIP file attachments, EXE files disguised as Excel icon

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

IPA

～Targeted attack emails that took advantage of the COVID-19 pandemic were observed～

- 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



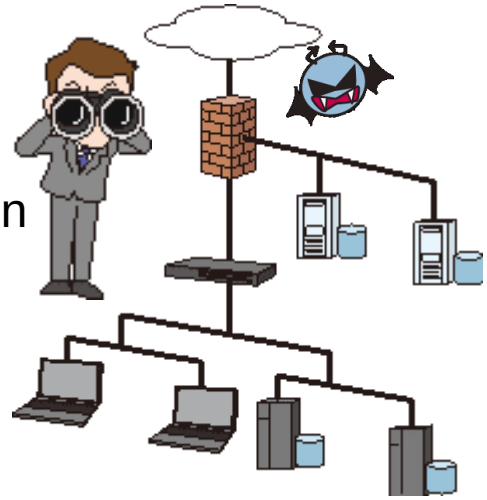
【2】Confidential Information Theft by APT (Advanced Persistent Threat)

IPA

～Targeted attack emails that took advantage of the COVID-19 pandemic were observed～

- Countermeasures
  - Information Security Officers, System Administrators
    - Preventions / Improvement of response ability

- Manage information and develop rules
- Collect and share information on cyber attacks continuously
- Implement cybersecurity training and incident response drill
- Understand the status of security measures using integrated operation management tools, etc.
- Understand the implementation status of security measures of business partners
- Minimize access privileges and strengthen administration
- Segregate networks
- Fortify critical servers (access control, encryption, etc.)
- Improve security measures including overseas offices, etc.



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

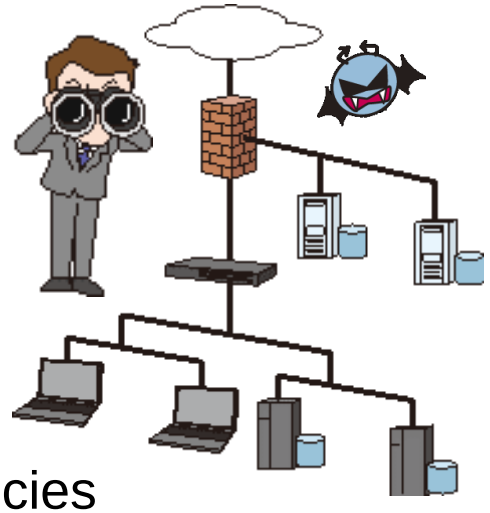
IPA

～Targeted attack emails that took advantage of the COVID-19 pandemic were observed～

Countermeasures

Information Security Officers, System Administrators

- Early detection
  - Monitor and protect networks
    Implement UTM•IDS / IPS • WAF etc.
  - Monitor and protect endpoint
- Actions after attack detected
  - Respond to the incident with CSIRT operation
  - Investigate impact and detect causes, strengthen countermeasures
  - Contact the relevant person and government agencies
    Supervisory authorities, personal data protection committee, police, etc.



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

～Targeted attack emails that took advantage of the COVID-19 pandemic were observed～

- Countermeasures
  - Employees, Staff
    - Improvement of information literacy

      - Take cybersecurity trainings

        “Don’t easily open email attachments”

        “Don’t easily enable macros in Office files”

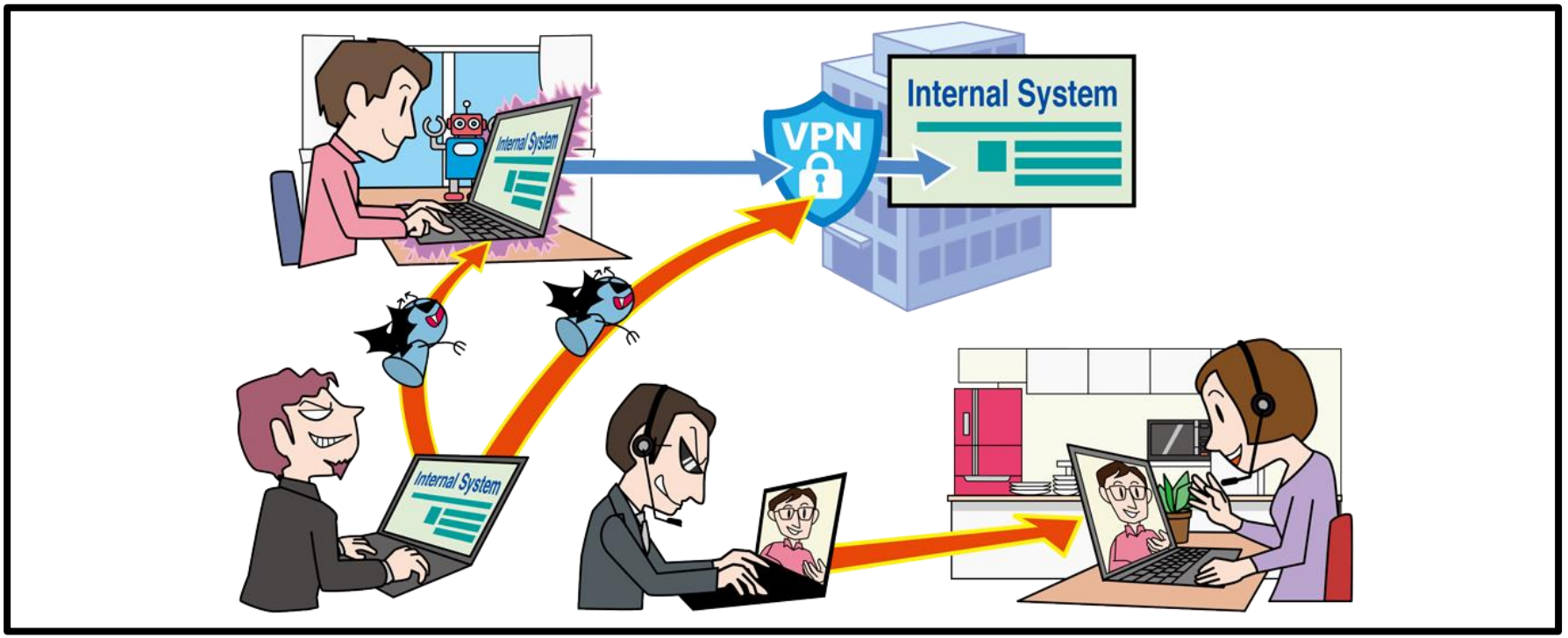
        “Notify any damage or impact promptly
    - Actions after attack detected

      - Contact/notify predefined contact such as CSIRT

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

IPA

～Implement countermeasures taking teleworking environments in consideration～



- Shifting to teleworking increased in 2020 due to COVID-19 pandemic
- As utilization of video conferencing services and VPN began in earnest, attacks targeting them occurred
- Risks of prying on video conferencing and virus infection of computers for teleworking

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

〜Implement countermeasures taking teleworking environments in consideration〜

Attack Methods / Occurrence Factors

- Inadequate teleworking environment and administration system

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

  ※ Risk of information leakage from private computers

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

～Implement countermeasures taking teleworking environments in consideration～

- Cases and Trends in 2020 (1)
  - VPN passwords leaked due to exploitation of vulnerabilities
    - In August 2020, vulnerabilities in a VPN product were exploited and about 900 stolen credentials were published online
    - Information and countermeasures of exploited vulnerabilities had already disclosed in April 2019
    - VPN products that had not been applied update program were targeted

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

〜Implement countermeasures taking teleworking environments in consideration〜

Cases and Trends in 2020 (2)

Company-owned computer infected with a virus during teleworking and the infection spread throughout the company

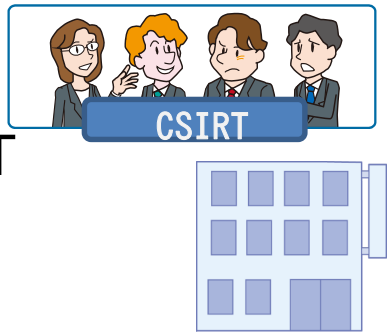
- An employee worked at home with a company-owned computer
- Connected to an external network without going through the in-house network
- Infected with a virus when using a social networking service
- When the employee came to office, connected the infected computer to the in-house network
- Virus infection spread to the in-house network

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

IPA

～Implement countermeasures taking teleworking environments in consideration～

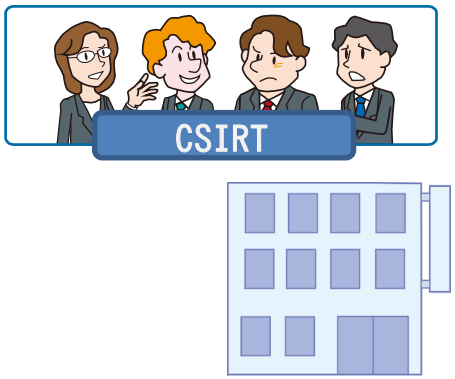
- Countermeasures
  - Organizations (Teleworkers)
    - Improvement of information literacy and information ethics
      - Take cybersecurity trainings
    - Preventions
      - Comply with the organization's teleworking rules (Devices to be used, network environment, work locations, etc.)
    - Actions after attack detected
      - Contact/notify predefined contact such as CSIRT



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

～Implement countermeasures taking teleworking environments in consideration～

- Countermeasures
  - Organizations (Senior Management)
    - Establishment of organizational framework
      - Establish CSIRT
      - Secure budget for countermeasures and perform countermeasures continuously
      - Develop a security policy of teleworking



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

IPA

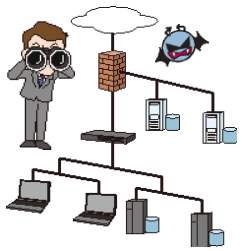
～Implement countermeasures taking teleworking environments in consideration～

Countermeasures

Organizations (Information Security Officers, System Administrators)

- Preventions (including preparations)

  - Adopt secure technologies for teleworking environment
    (Thin client, VPN, ZTNA, etc.)
  - Establish teleworking regulations and operation rules
    Consider the difference between company-owned computers and private computers
  - Implement security trainings
  - Collect and disseminate information on vulnerabilities of software used in teleworking and manage the status of countermeasures
  - Apply security patches
    (VPN devices, network equipment, computers)



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

IPA

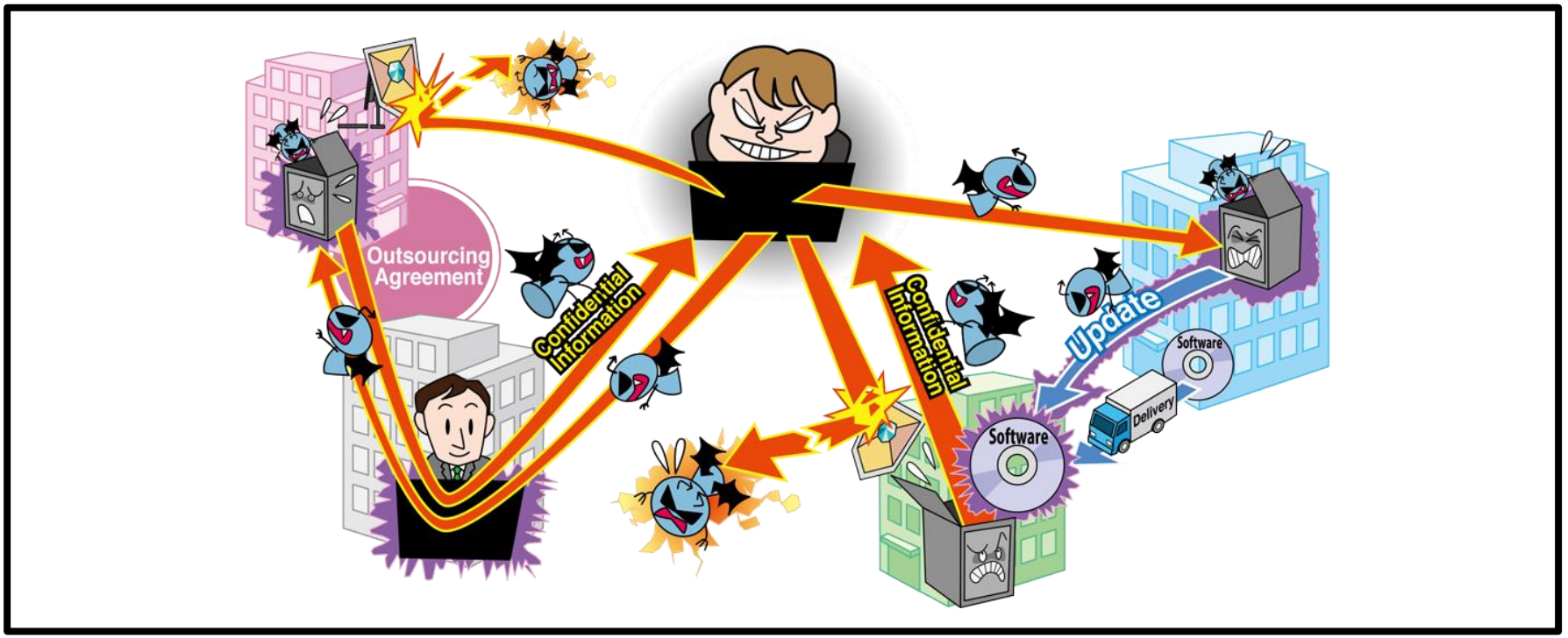
～Implement countermeasures taking teleworking environments in consideration～

- Countermeasures
  - Organizations (Information Security Officers, System Administrators)
    - •Early detection
      - Perform appropriate logging and monitor continuously
      - Monitor and protect networks

        Implement UTM•IDS / IPS etc.
    - •Actions after attack detected
      - Respond to the incident with CSIRT operation
      - Investigate impact and detect causes, strengthen countermeasures

【4】Attacks Exploiting Supply Chain Weaknesses

～ Countermeasures for own organization are not enough?
Supply chain attacks are on the rise～



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

【4】Attacks Exploiting Supply Chain Weaknesses

～ Countermeasures for own organization are not enough? Supply chain attacks are on the rise～

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, etc., as a foothold to attack the target
    - Embed virus in a software update to infect users who apply the update, etc.

【4】Attacks Exploiting Supply Chain Weaknesses

～ Countermeasures for own organization are not enough?
Supply chain attacks are on the rise～

- Cases and Trends in 2020 (1)
  - Attacker infiltrated a network of domestic bases using a network of Chinese bases as foothold
    - Information leakage from a major electronics manufacturer in 2019 was exposed in 2020
    - Server at the Chinese base was infected with a virus
    - Attacker infiltrated a network of domestic bases via a network of Chinese base and spread viruses
    - Number of suspected infected devices was 132, both in Japan and overseas
    - Attack was advanced and sophisticated enough to pass through existing defenses

【4】Attacks Exploiting Supply Chain Weaknesses

～ Countermeasures for own organization are not enough?
Supply chain attacks are on the rise～

- Cases and Trends in 2020 (1)
  - Backdoors were planted in a legitimate software update
    - In December 2020, American cybersecurity company announced the occurrence of a supply chain attack
    - Backdoors were planted in a legitimate software update
    - Organizations that applied the update file were infected
    - Then attackers infiltrated infected organizations through backdoors
    - Many U.S. organizations, including the U.S. government, reported infections

    ※Traces of infection were also confirmed in Japan

【4】Attacks Exploiting Supply Chain Weaknesses

～ Countermeasures for own organization are not enough?
Supply chain attacks are on the rise～

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

【4】Attacks Exploiting Supply Chain Weaknesses

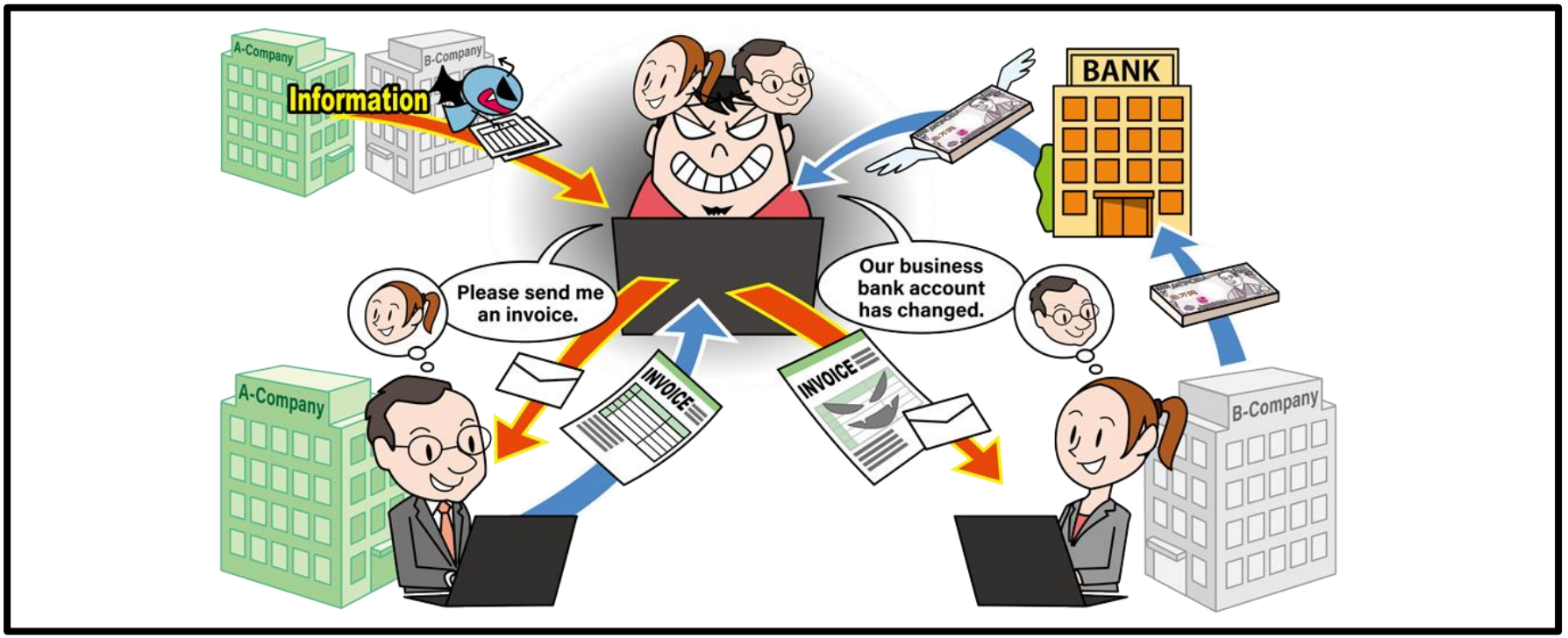
～ Countermeasures for own organization are not enough? Supply chain attacks are on the rise～

- Countermeasures
  - Organizations (Organizations involved in supply chains）
    - Preventions
      - Obtain security certifications
        （ISMS, Privacy mark, SOC2, ISMAP, etc.）
      - Utilize documents published by public authorities
        「Preparation for security threats against supply chains」（IPA）
        「Cybersecurity Management Guidelines」（METI/IPA）
    - Actions after attack detected
      - Contact/notify entruster

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

IPA

～Are you sure whether the invoice is a real one?～



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

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

～Are you sure whether the invoice is a real one?～

Attack Methods

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

- Falsify invoice 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

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

～Are you sure whether the invoice is a real one?～

- Cases and Trends in 2020 (1)
  - Increasingly sophisticated fake Japanese emails
    - Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP) issued an alert
    - Observed cases of fake emails related to COVID-19
    - Seems there are attackers who can use Japanese like a native

    ⇒Domestic organizations have become full-scale targets

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

～Are you sure whether the invoice is a real one?～

Cases and Trends in 2020 (2)

Most BEC involve "falsified invoices with business partners"

- JPCERT/CC released a survey of BEC
- Most of attack methods are ”falsified invoices with business partners”
- You can notice BEC in the process of communication from the following points
  - Received invoice is unnatural
  - Request to make a remittance to unfamiliar area
  - Remittance account is frozen
  - Unnatural local language is used, etc.

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

IPA

～Are you sure whether the invoice is a real one?～

Countermeasures

Organizations

- Preventions

- Establish business workflows which make corporate governance works

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

- Establish business workflows that does not rely on email

- Grant electronic signature (S/MIME) to emails ※Prevent spoofing

<Verification of the e-mail authenticity>

- Confirm facts by multiple means other than email

- Pay attention to unusual emails

- Pay attention to the sender's mail domain

<Proper management of email accounts>

- Manage passwords properly

- Implement measures against unauthorized login with login notification function, two-factor authentication, etc.

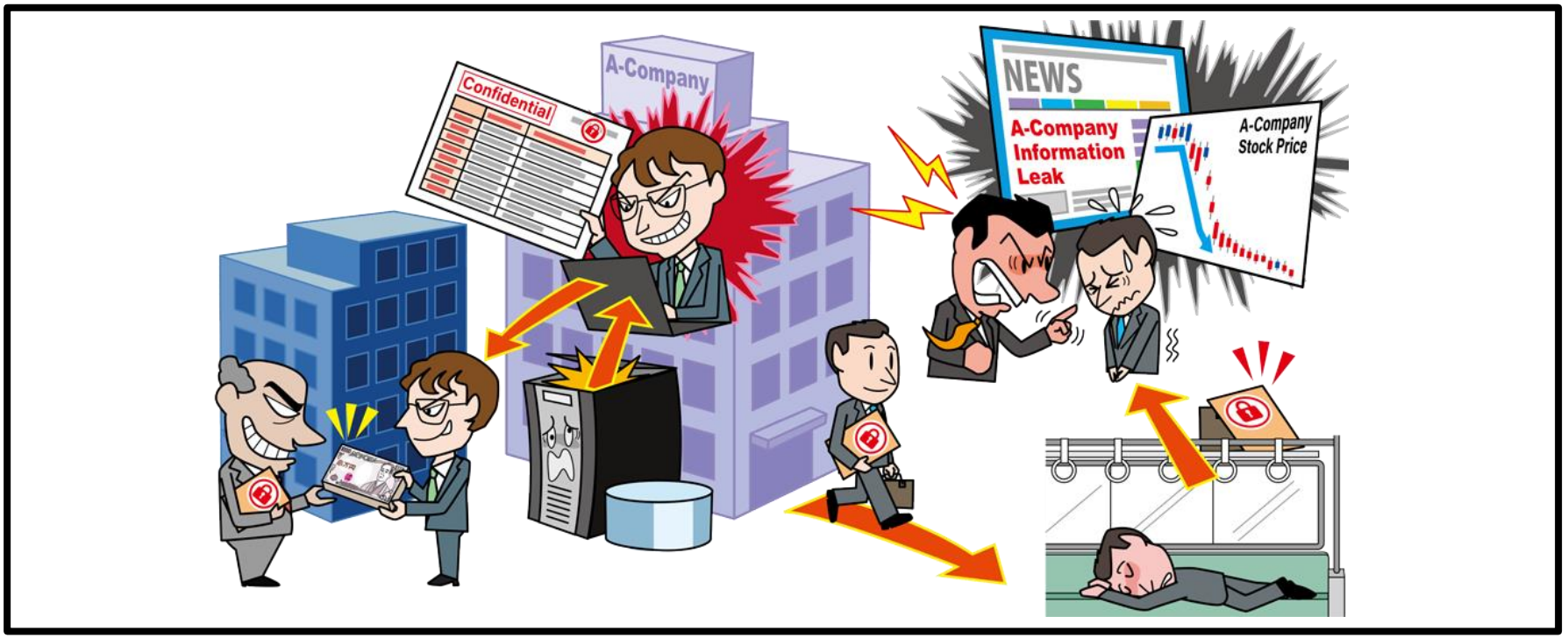
【5】Financial Loss by Business Email Compromise (BEC)

～Are you sure whether the invoice is a real one?～

- Countermeasures
  - Organizations
    - Actions after BEC recognition
      - Contact/notify predefined contact such as CSIRT
      - Consult with police or bank
      - Contact organizations which is being used as springboard or being spoofed
      - Investigate impact and detect causes, strengthen countermeasures
      - Check if there are any unintended forwarding settings or folder sorting settings in email accounts
      - Change passwords for all email accounts on the affected server

【6】Information Leakage by Internal Fraudulent Acts

～Do not create environments where internal fraudulent act is possible～



- 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

【6】Information Leakage by Internal Fraudulent Acts

～Do not create environments where internal fraudulent act is possible～

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.

【6】Information Leakage by Internal Fraudulent Acts

～Do not create environments where internal fraudulent act is possible～

Cases and Trends in 2020 (1)

Public servant leaked information

- Public servant working in the city office sent the personal information of about 2,700 public servants to the email address of a local newspaper from his business use computer
- Information leakage was disclosed, and the public servant was dismissed
- The public servant found the information in the trash of the computer which was dumped by previous user of the computer, and stored
- Inadequate city office's information management was also pointed out

【6】Information Leakage by Internal Fraudulent Acts

～Do not create environments where internal fraudulent act is possible～

Cases and Trends in 2020 (2)

Company employee leaked information to enhance his performance appraisal

- An employee stored confidential information about the material used for smartphone screens on his USB flash drive
- He sent the information by email to a Chinese company from his private computer at home
- He was sent papers to prosecutors on suspicion of violating the Unfair Competition Prevention Act
- He contacted a Chinese company employee through SNS and to enhance his performance appraisal he agreed to a proposal of technical information exchange from the employee

【6】Information Leakage by Internal Fraudulent Acts

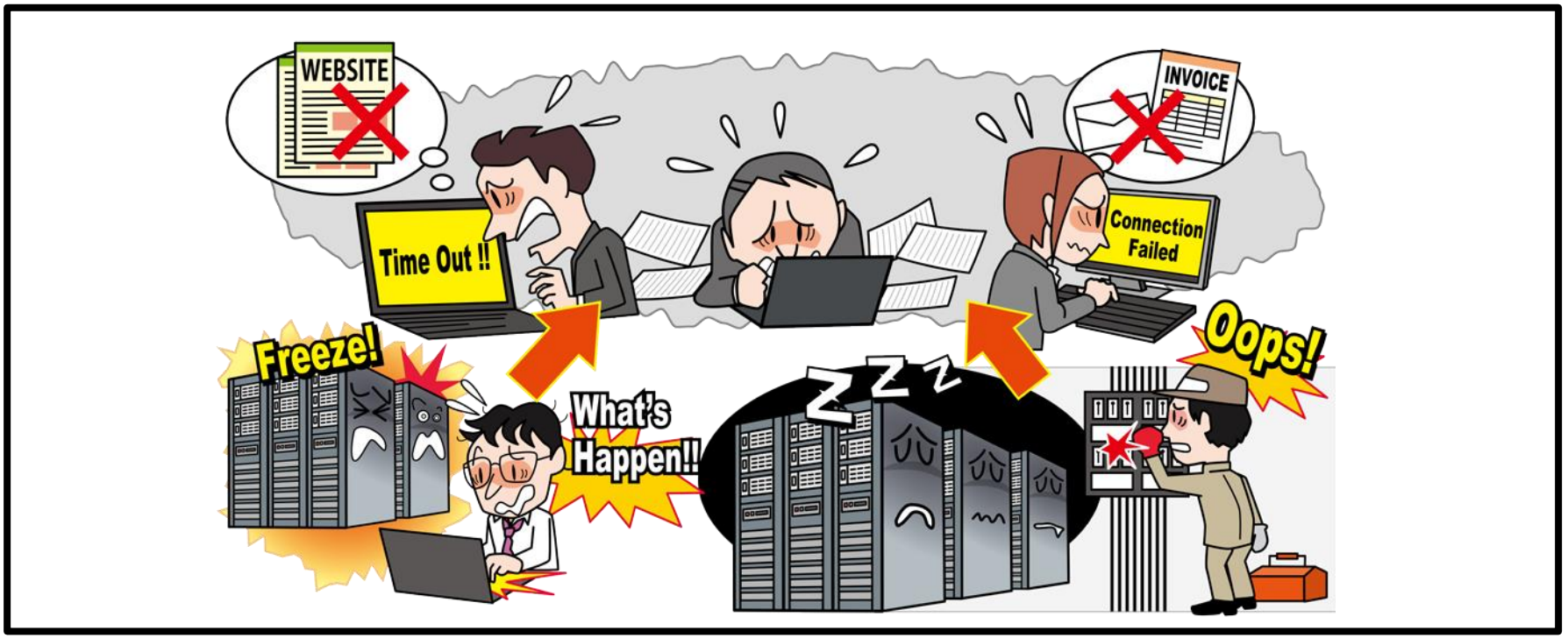
～Do not create environments where internal fraudulent act is possible～

- Countermeasures
  - Senior Management, Administrators
    - Preventions
      - Develop basic policy for fraudulent act measures
      - Identify information assets and lay out a response framework
      - Identify critical assets and establish a management system
      - Implement physical control
    - Improvement of information literacy/ethics
      - Enforce workforce management and compliance trainings
    - Early detection
      - Monitor system operation log
    - Actions after attack detected
      - Contact/notify relevant people and government agencies (Supervisory authorities, personal data protection committee, police, etc.)
      - Appropriate punishment for internal fraudulent actors

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

IPA

～Keep in mind the possibility of IT infrastructure outages～



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

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

～Keep in mind the possibility of IT infrastructure outages～

Causes

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

Natural Disaster

- Natural phenomena such as earthquakes, typhoons, and floods

Operation Work Accidents

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

Equipment Failures

- Failures of control systems such as power supply, air conditioning equipment, etc.

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

～Keep in mind the possibility of IT infrastructure outages～

- Cases and Trends in 2020 (1)
  - Suspension of many critical services due to IT infrastructure failure
    - In December 2020, a large-scale failure occurred in the IT infrastructure
    - The failure was caused by a bug of automatic storage quota management system
    - Other work carried out separately in October was also an indirect cause
    - Many services using the IT infrastructure became inaccessible

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

～Keep in mind the possibility of IT infrastructure outages～

- Cases and Trends in 2020 (2)
  - All-day suspension of trading due to a stock trading system failure
    - In October 2020, a large-scale failure occurred in the stock trading system
    - The cause of failure was a firmware misconfiguration at the time of NAS implementation
    - Although the NAS was configured redundantly, switching to fallback mode of operation did not work properly when the NAS failure occurred

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

IPA

～Keep in mind the possibility of IT infrastructure outages～

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

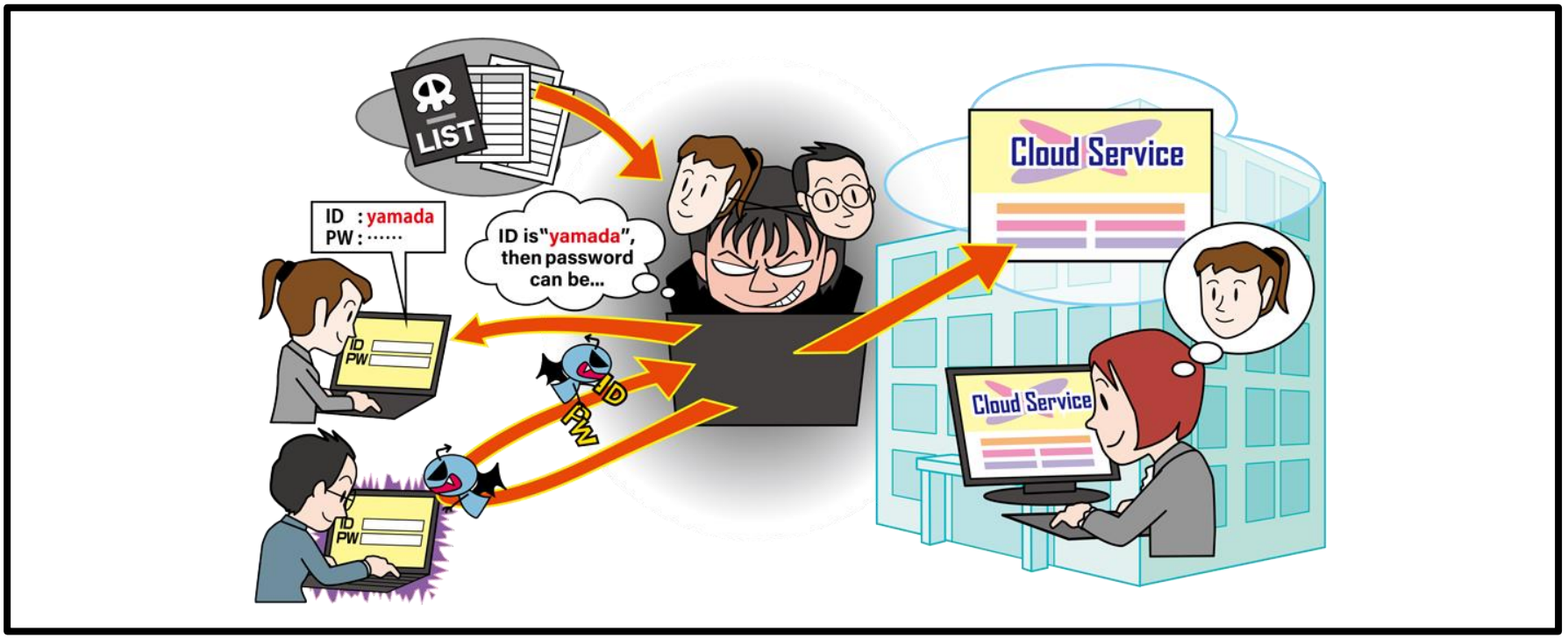
        Contracts/SLA with IT infrastructure providers

        Contracts/SLA with customers
      - Confirm coordination with IT infrastructure providers in anticipation of business impacts
    - Actions after business suspension occurred
      - Respond according to BCP

        Investigate impacts, strengthen countermeasures, and promptly notify CSIRT and related people, etc.

【8】Unauthorized Login to Services on the Internet

～ Call for people to stop reusing passwords and using easy passwords ～



- Credentials (ID, password) of services on the Internet you use are stolen or guessed, and attackers gain unauthorized access
- Damages to occur are vary depending on the function of the Internet service

【8】Unauthorized Login to Services on the Internet

～ Call for people to stop reusing passwords and using easy passwords ～

Attack Methods

- Perform unauthorized login with illegally obtained credentials

Password list attack

- Attackers make a list of credentials obtained in some way and attempt to login to multiple services by using the list
- When the same password is used in multiple services, unauthorized login to multiple services may occur if the password is leaked

【8】Unauthorized Login to Services on the Internet

～ Call for people to stop reusing passwords and using easy passwords ～

- Attack Methods

•Perform unauthorized login with illegally obtained credentials

- Password Guessing Attack
  - Attackers attempt unauthorized login by guessing a password that the user is likely to use (it is easier to be guessed if you use your name or birthday, etc. as a password)
  - Passwords may be guessed from information, etc. disclosed on SNS
- Virus infection
  - Infect a computer with a virus using malicious websites or emails, and steal password, etc. of services accessed with the computer

【8】Unauthorized Login to Services on the Internet

～ Call for people to stop reusing passwords and using easy passwords ～

- Cases and Trends in 2020 (1)
  - Leakage of business partner information due to unauthorized login
    - Attacker performed unauthorized login to the cloud service used by a major electronics manufacturer
    - 8,635 data including information of the names of business partners and bank accounts, etc., leaked
    - Attacker seemed to impersonate the company's employee using ID and password obtained in some way
    - The company said that they couldn't prevent unauthorized login because the attacker used legitimate ID and password

【8】Unauthorized Login to Services on the Internet

～ Call for people to stop reusing passwords and using easy passwords ～

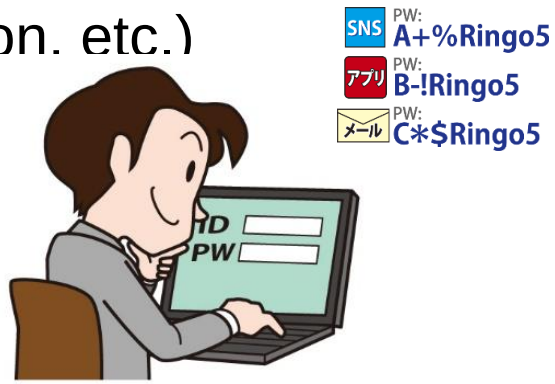
- Cases and Trends in 2020 (2)
  - Large number of unauthorized login attempted in the facility reservation system
    - Large number of unauthorized logins were attempted in the city's public facility reservation system
    - Approximately 1,300 user accounts were locked, and the system was unable to operate properly.
    - The city announced that it had filed a complaint with police accusing the attacker of fraudulent obstruction of business

【8】Unauthorized Login to Services on the Internet

～ Call for people to stop reusing passwords and using easy passwords ～

- Countermeasures
  - Organizations (Service Users)
    - Preventions

      - Don’t easily click on attachments and URLs
      - Make passwords long and complex
      - Don’t reuse passwords
      - Use password management software
      - Use the authentication method recommended by the service provider (two-factor authentication, etc.)



【8】Unauthorized Login to Services on the Internet

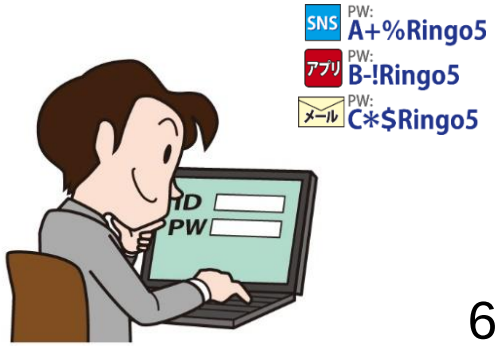
～ Call for people to stop reusing passwords and using easy passwords ～

- Countermeasures
  - Organization (Service Providers)
    - Preventions

- Secure budget for countermeasures and organizational framework
- Provide security functions to users

  Provide functions such as two-factor authentication, risk-based authentication, and the ability to check usage history
- Design services that cannot be exploited to verify the existence of an account

  Suppress the display of authentication errors that could indicate whether an account exists or not, and detect continuous access, etc.



【8】Unauthorized Login to Services on the Internet

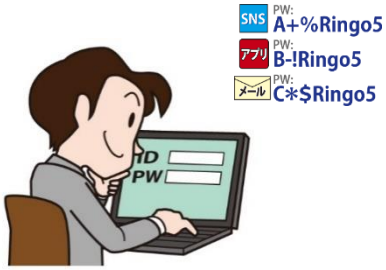
～ Call for people to stop reusing passwords and using easy passwords ～

- Countermeasures
  - Organization (Service Providers)
    - Early detection

      - Perform appropriate logging and monitor continuously
    - Actions after unauthorized login detected

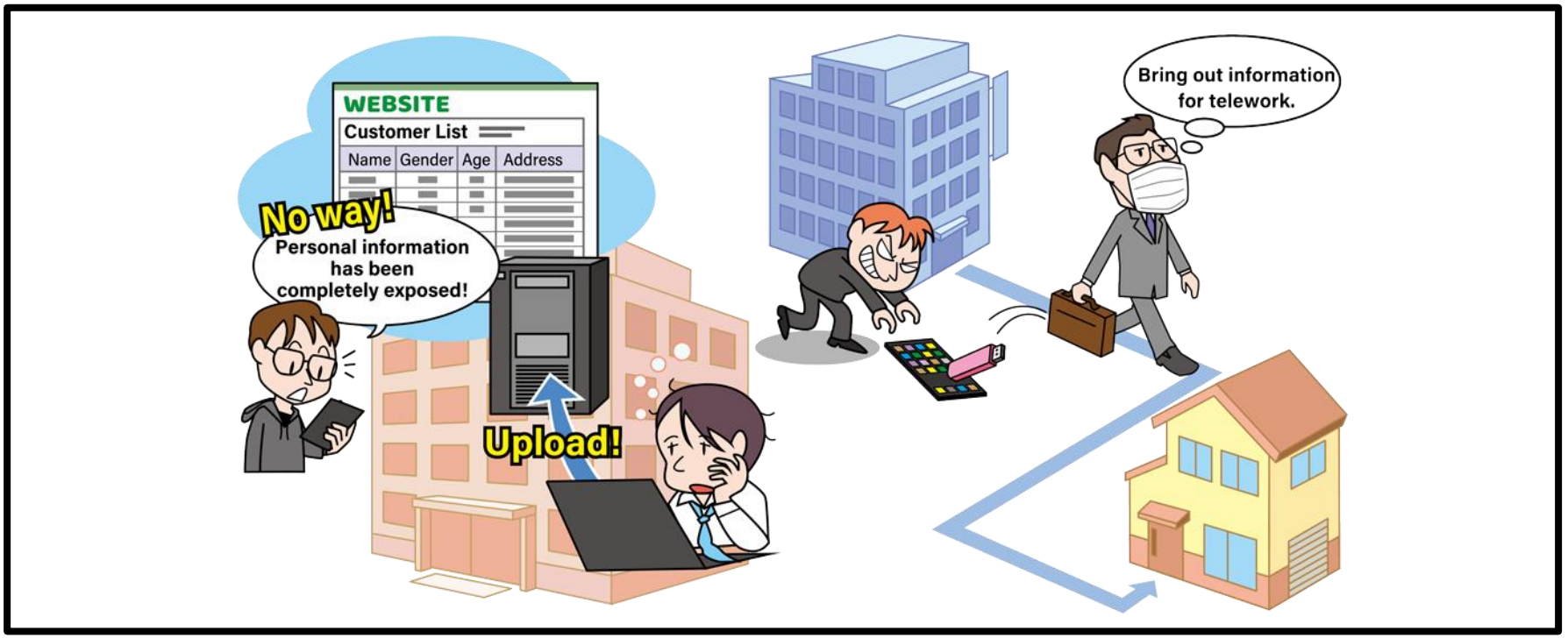
      - Contact/notify predefined contact such as CSIRT
      - Ask a specialized cybersecurity company to conduct investigation
      - Investigate impacts and detect causes, strengthen countermeasures
      - Promptly contact and compensate victims
      - Disclose leaked information and causes, etc.
      - Contact/notify relevant people and government agencies

        Supervisory authorities, personal data protection committee, police, etc.



【9】Unintentional/Accidental Information Leakage

～Review countermeasures in line with changes in the business environment～



- 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

～Review countermeasures in line with changes in the business environment～

Causes

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

Low security awareness among employees

- Bring out confidential/sensitive information with a bag, then lose the bag and leak the information
- Send an email without enough confirmation of address, etc.

Situation of individuals

- Lack concentration or attention due to poor health or urgent works

Insufficiency of organizational rules and work check procedures

- Definition of confidential/sensitive information, handling rules, bring-out permission procedure, etc. are not defined or insufficient

【9】Unintentional/Accidental Information Leakage

～Review countermeasures in line with changes in the business environment～

- Cases and Trends in 2020 (1)
  - Information leakage due to wrong email transmission and inadequate response
    - Personal information of about 9,700 COVID-19 positive patients held by the prefectural government was leaked
    - Email with access rights to a folder on the cloud which contains patient information etc. was mistakenly sent to a third party with a similar email address to the right recipient email address
    - Although access restrictions were implemented after the wrong transmission was discovered, there was a misconfiguration and the files kept available for viewing by third parties

【9】Unintentional/Accidental Information Leakage

～Review countermeasures in line with changes in the business environment～

Cases and Trends in 2020 (2)

Loss of storage media containing customer information

- A company lost magnetic tapes for backup that contained critical information
- The magnetic tapes contained about 2.5 million pieces of information, including customers' personal information, service usage records, information on outsourced operations, etc.
- The company stated that it was highly likely that the tapes were accidentally disposed and confirmed no information leakage

【9】Unintentional/Accidental Information Leakage

～Review countermeasures in line with changes in the business environment～

- Countermeasures
  - Organization (Person concerned)

    - Improvement of information literacy and information ethics
      - Conduct security awareness training for employees
      - Establish organizational rules and confirmation processes
      - Review organizational rules and confirmation processes
    - Preventions
      - Operate according to confirmation processes
      - Protect information (encryption, authentication) and understand 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

～Review countermeasures in line with changes in the business environment～

- Countermeasures
  - Early detection
    - Establish internal reporting system when problems occur
    - Set up a point of contact with outsiders
  - Actions after information leakage occurred
    - Contact/notify predefined contact such as CSIRT
    - Investigate impacts and detect causes, strengthen countermeasures
    - Prevent damage expansion and eliminate secondary damage factors
    - Disclose the content and cause of the leakage
    - Contact/notify the relevant person and government agencies

      Supervisory authorities, personal data protection committee, etc.

【9】Unintentional/Accidental Information Leakage

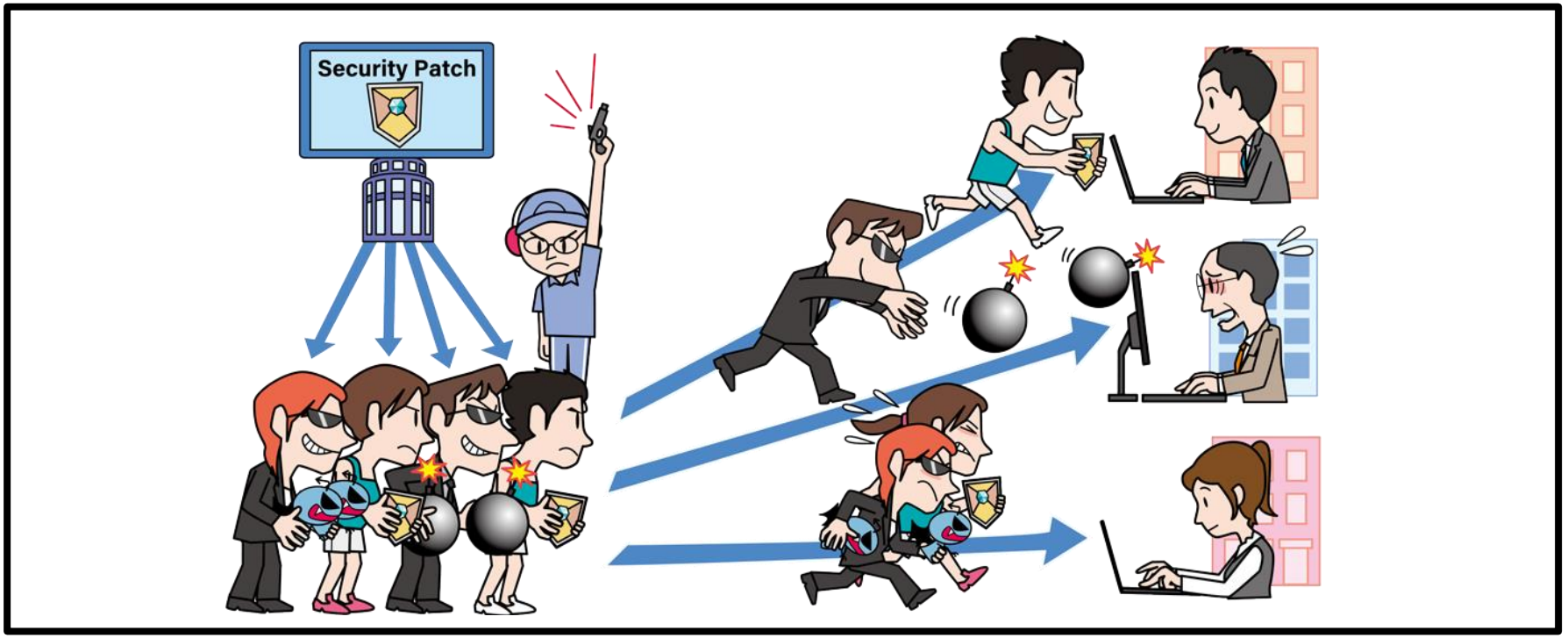
～Review countermeasures in line with changes in the business environment～

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

- Follow information or instructions from the organization where the leakage occurred
- Change passwords or credit card information, etc.

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

～Malicious actors also know disclosed vulnerabilities～



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

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

～Malicious actors also know disclosed vulnerabilities～

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

- Attack tools that exploit released vulnerabilities are created in a short period of time and become available and being distributed on the Internet
- Vulnerability exploitation features may be implemented in open-source tools, and these can be exploited by attackers

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

～Malicious actors also know disclosed vulnerabilities～

- Cases and Trends in 2020 (1)
  - Attacks targeting product vulnerabilities were observed
    - On July 1, 2020, vulnerability information of network products that could allow remote code execution was disclosed
    - Four days after the vulnerability information disclosure, the exploit code to exploit the vulnerability was published on the Internet
    - The next day, attacks using the exploit code were observed

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

～Malicious actors also know disclosed vulnerabilities～

- Cases and Trends in 2020 (2)
  - ”Zerologon” vulnerability in Windows server products
    - On August 11, 2020 (U.S. time zone), an update was released for a privilege escalation vulnerability called "Zerologon" in Windows server products
    - On September 15, 2020, a proof of concept (PoC) for this vulnerability was released
    - On September 24, 2020 (U.S. time zone), attacks that exploited the PoC were observed

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

～Malicious actors also know disclosed vulnerabilities～

- Countermeasures
  - Individuals/Organizations (System Administrators/Software users)
    - Preventions
      - Identify critical assets and establish a management system
      - Collect vulnerability countermeasure information and take prompt actions based on the information
      - Implement UTM・IDS / IPS etc.
      - Monitor networks and block attack communications
      - Use software and versions that are provided excellent security support
      - Temporary server shut down, etc.
    - Actions after attack detected
      - Contact/notify predefined contact such as CSIRT
      - Investigate impacts and detect causes, strengthen countermeasures

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

～Malicious actors also know disclosed vulnerabilities～

- Countermeasures
  - Organization (Development vendors)
    - Management of product security, laying out a response framework
      - Grasp software embedded 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

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 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.

For detailed contents of this document

- Please refer to the PDF document on the following website

10 Major Security Threats 2021 (in Japanese only)
https://www.ipa.go.jp/security/vuln/10threats2021.html