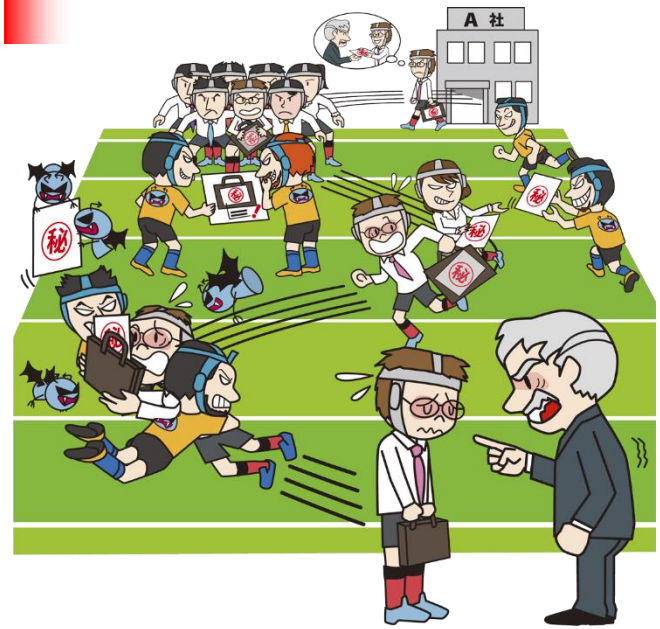
IPA Better Life with IT

10 Major Security Threats 2020

～Let’s work together on security measures! Try it!～

[For Organizations]



IT Security Center (ISEC)
Information-Technology Promotion Agency (IPA), Japan
July 2020

What is “10 Major Security Threats”?

- Report issued by IPA every year since 2006
- IPA determines candidate threats based on security incidents and attack 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”

Various entities and people against threats

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”

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

10 Major Security Threats 2020

- Contents
  - Chapter 1. Useful Terms and Mechanisms

    Explanation for the terms and mechanisms that often appear when learning how to safely use computers, smartphones, and the Internet
  - Chapter 2. 10 Major Security Threats 2020

    Explanation for the outline and countermeasures etc. of each threat of “10 Major Security Threats” selected based on cases and trends in 2019
  - Chapter 3. How to use “10 Major Security Threats”

    Explanation for the procedures for taking countermeasures effectively, utilizing the “10 Major Security Threats”, after determining the ‘things should be protected’ such as services or customer information etc. since critical threats vary depending on the organization or individual

10 Major Security Threats – Threat Ranking

Threats for Individuals	Rank	Threats for Organizations
Unauthorized Use of Smartphone Payment	1	Confidential Information Theft by APT
Phishing Fraud for Personal Information	2	Information Leakage by Internal Fraudulent Acts
Unauthorized Use of Leaked Credit Card Information	3	Financial Loss by Business E-mail Compromise
Unauthorized Use of Internet Banking Credentials	4	Attacks Exploiting Supply Chain Weaknesses
Extortion of Money by Blackmail or Fraudulent Methods with E-mail, SNS, etc.	5	Financial Loss by Ransomware
Malicious Smartphone Applications	6	Suspension of Business due to Unexpected IT Infrastructure Failure
Cyberbullying and Fake News	7	Careless Information Leakage
Unauthorized Login to Services on the Internet	8	Personal Information Theft from Services on the Internet
Internet Fraud by Fake Warnings	9	Unauthorized Use of IoT Devices
Personal Information Theft from Services on the Internet	10	Business Service Outage caused by Denial of Service Attacks

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 & 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

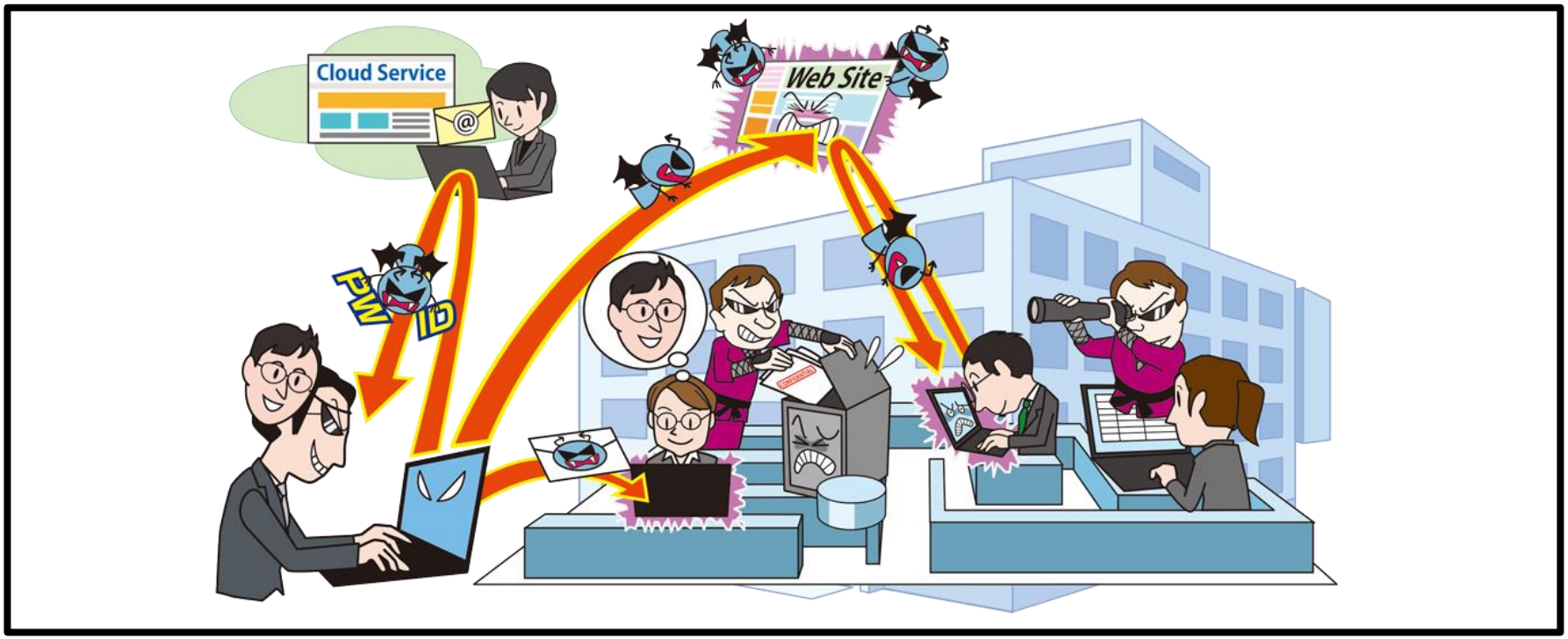
10 Major Security Threats 2020
For Organizations

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】Confidential Information Theft by APT (Advanced Persistent Threat)

～APT attacks continue / various tricks delay the detection of the attack～



- Infect computers with virus by e-mail etc. and intrude organization’s network
- Increase the impact range of attacks persistently
- Steal organization's confidential information

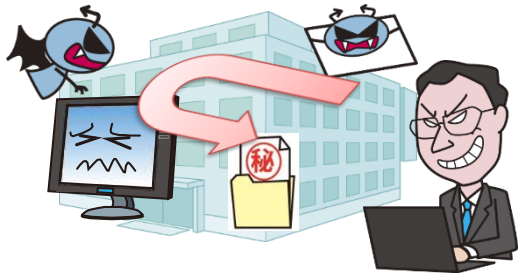
【1】Confidential Information Theft by APT (Advanced Persistent Threat)

～APT attacks continue / various tricks delay the detection of the attack～

- Attack Methods

•Infect the target 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 a link to malicious 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



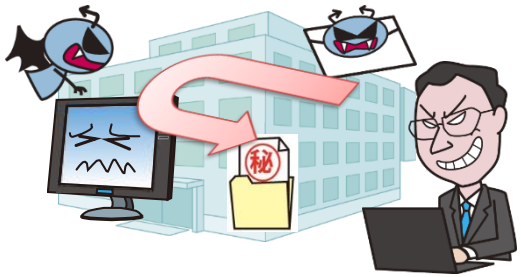
【1】Confidential Information Theft by APT (Advanced Persistent Threat)

～APT attacks continue / various tricks delay the detection of the attack～

- Attack Methods

•Infect the target with virus by unauthorized access

- Methods by unauthorized access
  - login improperly to the cloud service used by the target organization
  - Access improperly to target organization's in-house systems by exploiting legitimate routes
  - Infect in-house systems with virus



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

～APT attacks continue / various tricks delay the detection of the attack～

- Cases and Trends in 2019
  - Report by J-CSIP
    - •Observed many e-mails targeting plant-related companies
    - •Observed viruses containing ingenious gimmicks
      （”Spoof icons or extensions”, “Disable specific security software”, “Operate only at specific time”, etc.）
    - •Observed the attack e-mail with attached Word document file with embedded macros
      （If you open the attachment and activate the macro, you may be infected with virus）

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

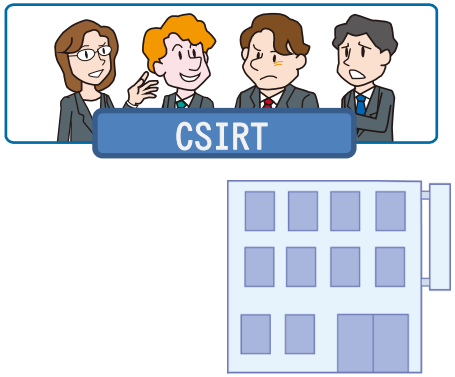
～APT attacks continue / various tricks delay the detection of the attack～

- Cases and Trends in 2019
  - Reports of unauthorized access to multiple defense-related companies
    - Major general electronics manufacturer revealed that they had unauthorized access from out side for years
    - Following the company, some companies also made public that they had unauthorized access
    - Critical information may have leaked

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

～APT attacks continue / various tricks delay the detection of the attack～

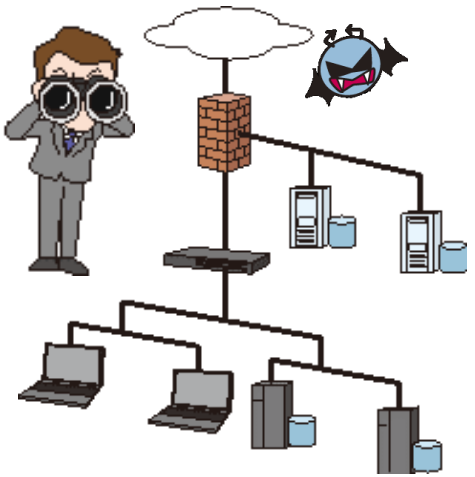
- Countermeasures
  - Senior Management
    - •Establishment of organizational framework
      - Establish CSIRT that can respond promptly and continuously
      - Secure budget for countermeasures and perform countermeasures continuously
      - Develop security policy



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

～APT attacks continue / various tricks delay the detection of the attack～

- Countermeasures
  - Information Security Officers, System Administrators
    - •Preventions / Improvement of response ability
      - Manage information and develop rules
      - Gather and share information on cyber attacks continuously
      - Implement security education and incident training
      - Understand the status of security measures using integrated operation management tools, etc.
      - Understand the implementation status of security measures of business partners
      - Design systems securely
      - Segregate networks
      - Fortify critical servers (access control, encryption, etc.)
      - Improve security measures including overseas offices, etc.



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

～APT attacks continue / various tricks delay the detection of the attack～

- Countermeasures
  - Information Security Officers, System Administrators

•Early detection

- Monitor and protect network

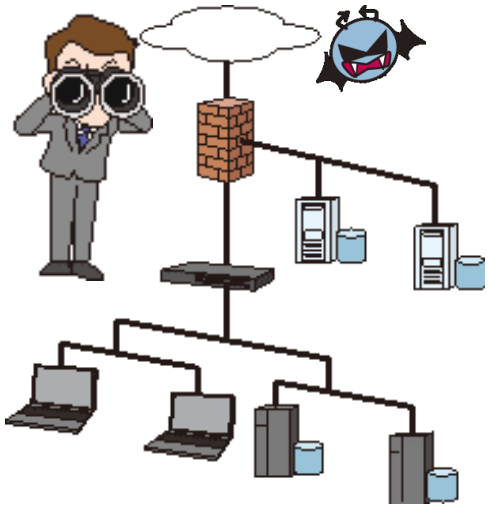
  Implement UTM•IDS / IPS • WAF etc.

- 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 Information Protection Commission, police, etc.



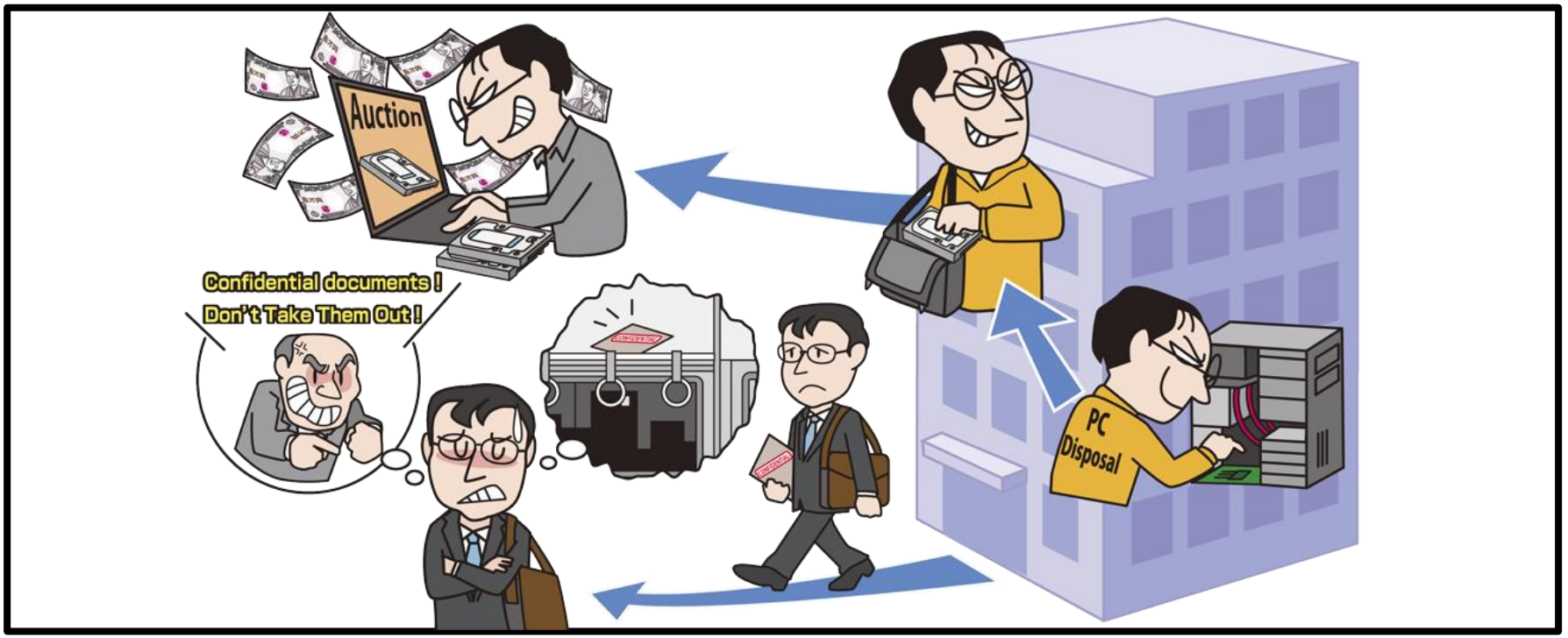
【1】Confidential Information Theft by APT (Advanced Persistent Threat)

～APT attacks continue / various tricks delay the detection of the attack～

- Countermeasures
  - Employees, Staff
    - Improvement of information literacy
      - -Take security trainings
        - “Don’t easily open email attachments”
        - “Don’t easily enable macros in Office files”
        - “Report any damage or impact promptly”
    - Actions after attack detected
      - -Contact/report to CSIRT

【2】Information Leakage by Internal Fraudulent Acts

～Establish and implement management and monitoring framework/system to prevent internal fraudulent acts～



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

【2】Information Leakage by Internal Fraudulent Acts

～Establish and implement management and monitoring framework/system to prevent internal fraudulent acts～

Attack Methods

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

Abuse of access authority

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

Abuse of former employee's account

- Obtain information using the account used before leaving the job

Bring out data with USB flash drive or e-mail etc.

【2】Information Leakage by Internal Fraudulent Acts

～Establish and implement management and monitoring framework/system to prevent internal fraudulent acts～

- Cases and Trends in 2019
  - Employee illegally took out HDDs planned to be destroyed
    - Employee of information device recycle company stole HDDs planned to be destroyed and sold them at online auctions etc.
    - HDDs were used in Kanagawa Prefectural Government
    - Internal documents and personal information of Kanagawa Prefectural Government left in the HDDs were leaked
    - The company dismissed the employee on disciplinary and filed a damage report to the police

【2】Information Leakage by Internal Fraudulent Acts

～Establish and implement management and monitoring framework/system to prevent internal fraudulent acts～

- Cases and Trends in 2019
  - Former employee illegally took out confidential information
    - Former employee of a medical device manufacturer/distributor fraudulently took out patient information, personal information of customers and survey respondents, and technical and sales information
    - Stolen information was copied from a company computer to a private computer using a USB flash drive
    - The former employee was sent papers to prosecutors on charges of violating the Unfair Competition Prevention Act

【3】Business E-mail Compromise (BEC)

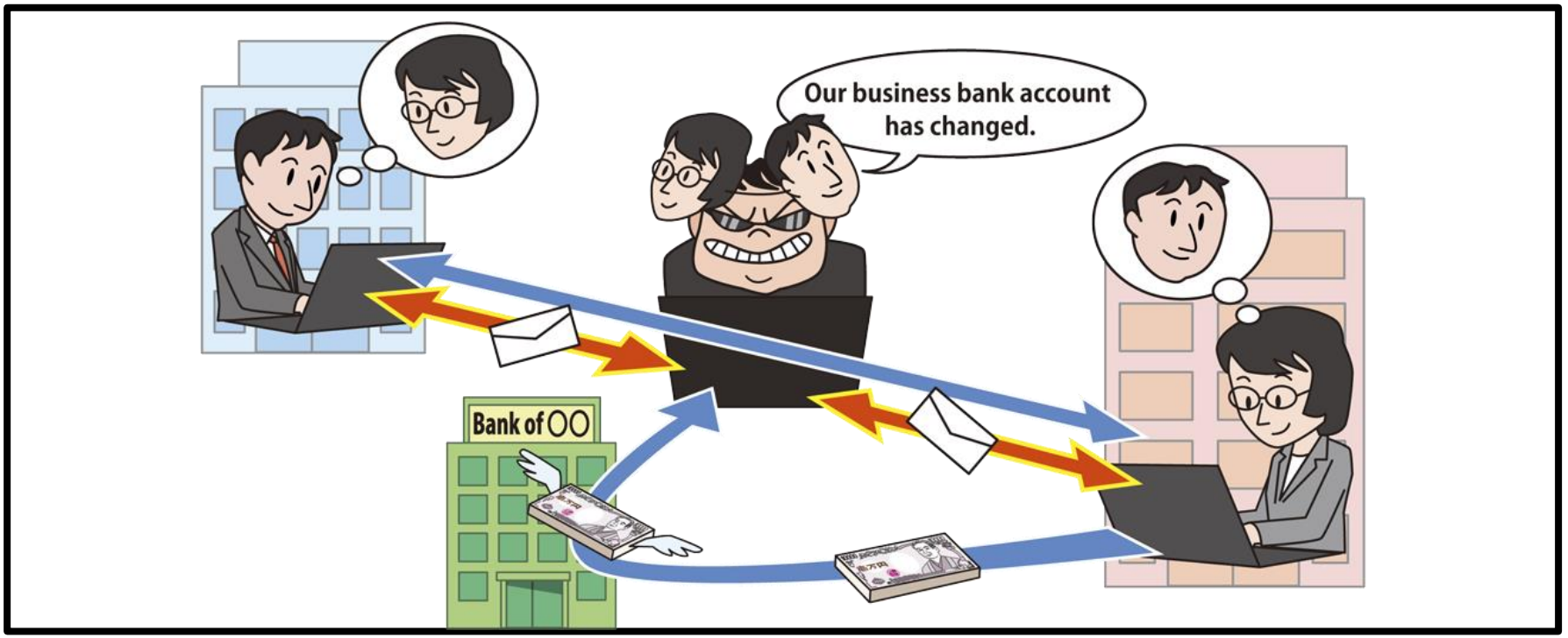
～BEC has transformed into a major cyber risk over the last few years～

- Countermeasures
  - Senior Management, Administrators

    - Preventions
      - Develop basic policy for fraudulent act measures
      - Identify assets which should be protected
      - Manage and protect critical/sensitive information
    - Improvement of information ethics
      - Enforce workforce management and compliance education/training
    - Early detection
      - Monitor system operation log
    - Actions after attack detected
      - Contact the relevant person and government agencies
        Supervisory authorities, Personal Information Protection Commission, police, etc.
      - Appropriate punishment for internal fraudulent actors

【3】Business E-mail Compromise (BEC)

～BEC has transformed into a major cyber risk over the last few years～



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

【3】Business E-mail Compromise (BEC)

～BEC has transformed into a major cyber risk over the last few years～

- Attack Methods

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

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

【3】Business E-mail Compromise (BEC)

～BEC has transformed into a major cyber risk over the last few years～

- Cases and Trends in 2019
  - Two Japanese arrested in BEC
    - Two Japanese were arrested on suspicion of fraud and violation of the Organized Crime Punishment Act
    - Hacked e-mail account of a company representative of an overseas company
    - Made the company transfer about 110 million yen to a shinkin bank in Japan

【3】Business E-mail Compromise (BEC)

～BEC has transformed into a major cyber risk over the last few years～

- Cases and Trends in 2019
  - J-CSIP Operation Status Report [Apr.-Jun. 2019]

<Methods Observed>

- Malicious actor intervened the e-mail communication between the target organization and their business partner
- Malicious actor sent quotation contains false bank account as a 'replacement'

※Sent a fake email requesting changes to the estimated price and the bank account to be transferred into as well

【3】Business E-mail Compromise (BEC)

～BEC has transformed into a major cyber risk over the last few years～

- Countermeasures
  - Organization

•Prevention of BEC

- Build business flows which make corporate governance works
- Grant electronic signature (S/MIME) to emails ※Prevent spoofing

<Verification of the e-mail authenticity>

- Confirm facts by means other than e-mail
- Pay attention to the sender's mail domain
- Be careful with e-mails that urge quick decision

<Proper management of e-mail accounts>

- Manage passwords properly
- Implement measures against unauthorized login with login notification function etc.

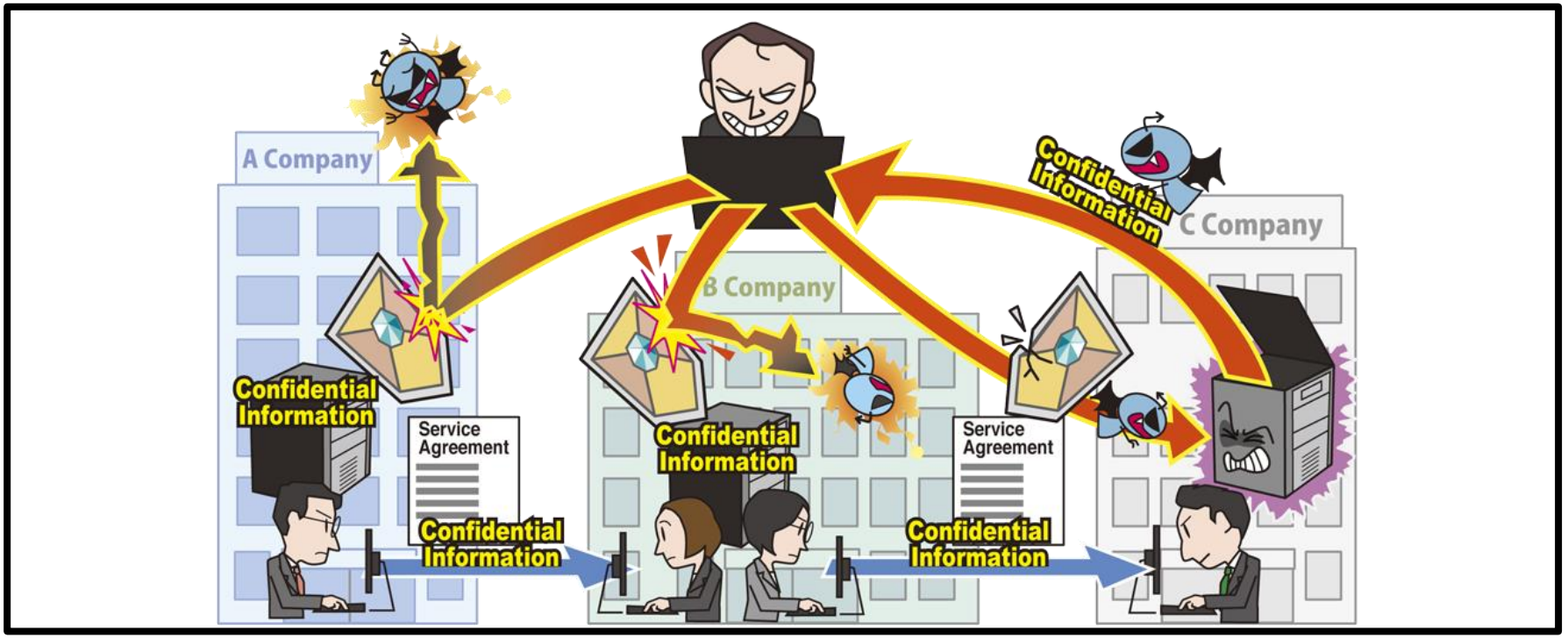
【3】Business E-mail Compromise (BEC)

～BEC has transformed into a major cyber risk over the last few years～

- Countermeasures
  - Organization（Accountant or Financial Officer）
    - •Actions after BEC recognition
      - Contact/report to CSIRT
      - Consult with police
      - Contact organizations which is being used as springboard or being spoofed.
      - Investigate the impact and the cause, strengthen the measures

【4】Attacks Exploiting Supply Chain Weaknesses

～Appropriate security management is also required for outsourcing partners～



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

【4】Attacks Exploiting Supply Chain Weaknesses

～Appropriate security management is also required for outsourcing partners～

- Causes

• Lack of security measures of companies in supply chain

- Outsourcing partners are not properly selected and not managed
- Difficult to manage security measures for all companies in supply chain
  - Entruster is unable to manage subcontractors or sub-subcontractors of outsourcing partners, so has difficulty managing security measures of all of those companies

【4】Attacks Exploiting Supply Chain Weaknesses

～Appropriate security management is also required for outsourcing partners～

- Cases and Trends in 2019
  - Unauthorized access to the development environment in the subcontractor of JSPO
    - Subcontractor of JSPO (Japan Sports Association) detected unauthorized access
    - Found data deleted in the server in the development environment
    - Deleted data was of the National Sports Festival contestants etc. which contains personal information such as name and birth date
    - Data leakage or publication has not been confirmed
    - Inadequate security settings of the development environment

【4】Attacks Exploiting Supply Chain Weaknesses

～Appropriate security management is also required for outsourcing partners～

- Cases and Trends in 2019
  - IPA published the research report regarding supply chain
    - IPA has released the “The Survey Report on the Scope of Information Security responsibility in IT Supply Chain”
    - In IT outsourcing contracts, about 80% of entrusters do not specify the scope of responsibility for “response to new threats as they emerge”
    - The highest reason of above was “lack of expertise and skills” comprising of 79.6%

【4】Attacks Exploiting Supply Chain Weaknesses

～Appropriate security management is also required for outsourcing partners～

- Countermeasures

  - Entruster
    - •Preventions
      - Enforce rules for outsourcing and information management
      - Select trusted organizations
      - Verify the deliverables from outsourcing partners
      - 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

～Appropriate security management is also required for outsourcing partners～

- Countermeasures
  - Outsourcing partners
    - •Preventions
      - - As the attacker's purpose and attack method vary, it is necessary to make a wide range of countermeasures depending on the business, referring measures for other threats.
    - •Actions after attack detected
      - - Contact/report to entruster

【4】Attacks Exploiting Supply Chain Weaknesses

～Appropriate security management is also required for outsourcing partners～

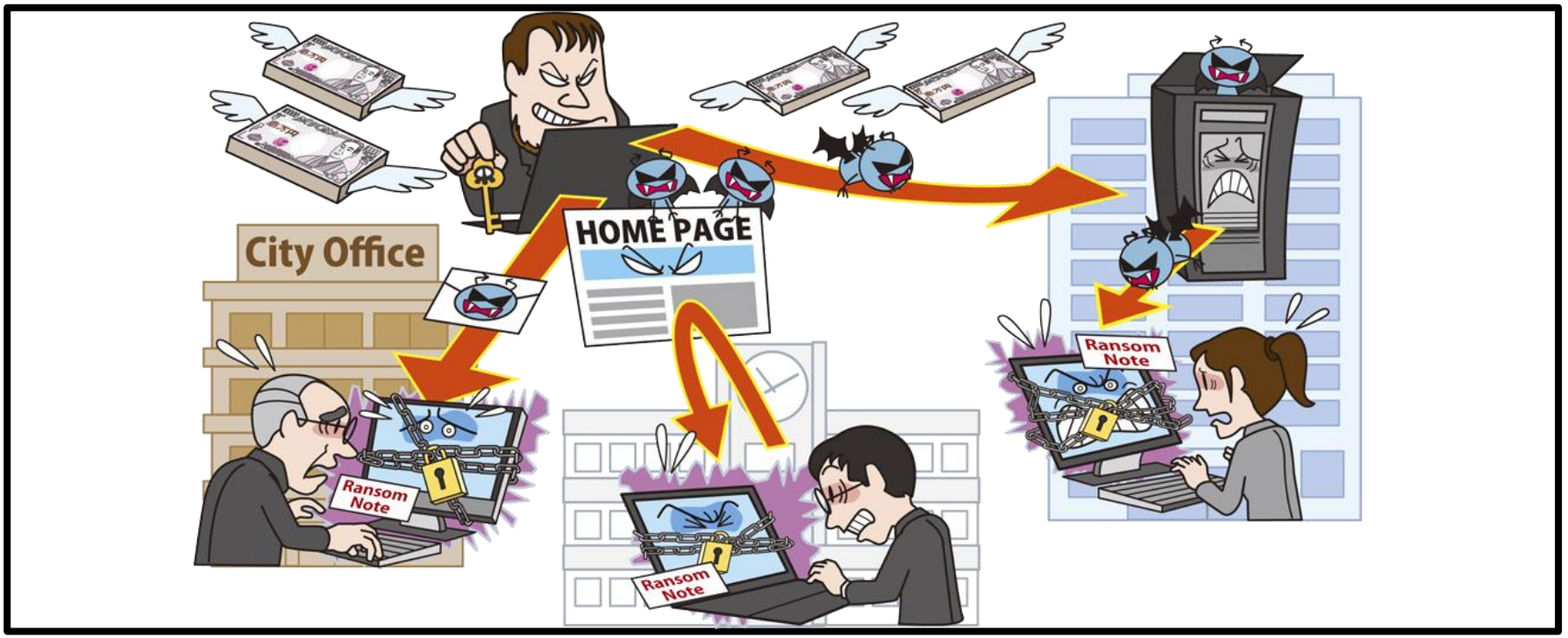
- Countermeasures
  - Entruster /Outsourcing partners
    - •Preventions
      - - Utilize guidelines published by public authorities

        “Cybersecurity Management Guidelines” (METI/IPA)

        “Guidelines for Information Security Measures for Small and Medium-sized Enterprises” (IPA)

【5】Financial Loss by Ransomware

～Know measure to avoid ransomware infection and to address when get infected～



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

【5】Financial Loss by Ransomware

～Know measure to avoid ransomware infection and to address when get infected～

IPA

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 targeted user into browsing the falsified website using e-mail etc.

【5】Financial Loss by Ransomware

～Know measure to avoid ransomware infection and to address when get infected～

IPA

- Attack Method

• 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
  - •Access improperly to target's servers via RDP (Remote Desktop Protocol) etc.
  - •Execute (infect) virus on the server

【5】Financial Loss by Ransomware

～Know measure to avoid ransomware infection and to address when get infected～

- Cases and Trends in 2019
  - Municipal high school's server infected with ransomware
    - Staff of the municipal high school detected the infection of Word documents in the network server
    - Blackmail message in English was displayed on the screen suggesting infection
    - Data such as students' work was no longer available
    - The cause of infection was unclear

【5】Financial Loss by Ransomware

～Know measure to avoid ransomware infection and to address when get infected～

- Cases and Trends in 2019
  - Ransomware attacks targeting Japan
    - Attack e-mails attempting to infect receivers with ransomware such as “Gandcrab” were distributed to Japan
    - Names of Japanese female entertainers were used in the subject line of the e-mails
    - Especially on January 29, 2019, 95% of this attack was detected in Japan

【5】Financial Loss by Ransomware

～Know measure to avoid ransomware infection and to address when get infected～

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

【5】Financial Loss by Ransomware

～Know measure to avoid ransomware infection and to address when get infected～

- Countermeasures
  - System Administrators, Employees
    - •Preventions
      - Check incoming e-mails and visiting websites carefully
      - Don’t easily click on attachments and URLs
      - Do not execute suspicious software
      - Stop using expired OS and migrate to effective OS
      - Use filtering tools (e-mail, web)
      - Segment network
      - Minimize access privileges of shared servers
      - Perform data backup

【5】Financial Loss by Ransomware

～Know measure to avoid ransomware infection and to address when get infected～

- Countermeasures
  - System Administrators, Employees

•Actions after attack detected

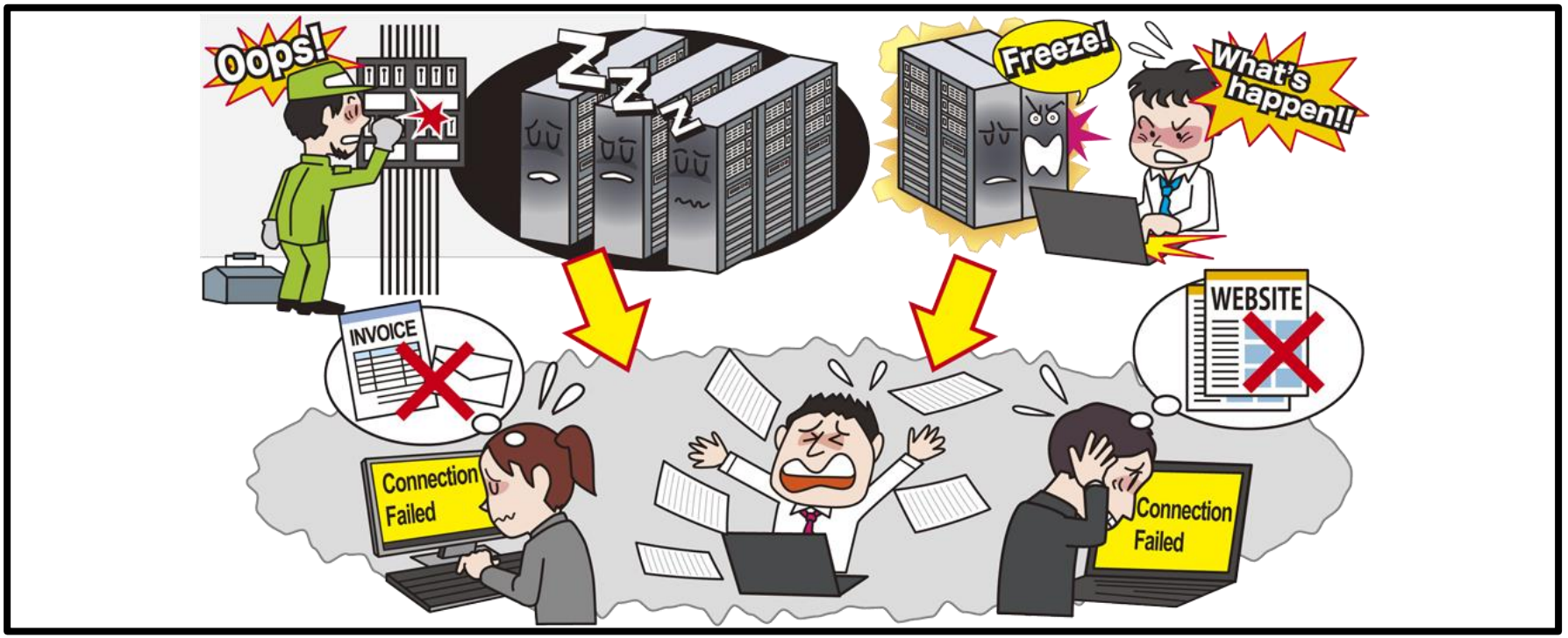
- Contact/report to CSIRT
- Recover from backup
- Use file decryption tools
- Investigate impact and detect causes, strengthen countermeasures

<Exceptional measure>

Not recommended, but there were cases in which ransom was paid when encrypted files were life-threatening.

【6】Business suspension due to unexpected It infrastructure failures

～It comes suddenly without notice～



- IT infrastructure of the data center or cloud services stops
- Suspension of business leads to financial loss such as profit drop

【6】Business suspension due to unexpected It infrastructure failures

～It comes suddenly without notice～

Causes

- Unpredictable events stop IT infrastructure
- Business continuity management is not properly practiced

Natural Disaster

- Natural phenomena such as earthquakes, typhoons, and floods

Operational Work Accidents

- Human error during maintenance work of infrastructure equipment etc.

Equipment Failures

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

【6】Business suspension due to unexpected It infrastructure failures

～It comes suddenly without notice～

- Cases and Trends in 2019
  - System failure in the IaaS service for local governments
    - System failure occurred in the IaaS ‘Jip-Base’ for local governments
    - About 50 local governments across the country were affected
    - Counter services and the business systems of local governments were interfered
    - Took a long time to recover

【6】Business suspension due to unexpected It infrastructure failures

～It comes suddenly without notice～

- Cases and Trends in 2019
  - System disruption in the data center caused by power supply failure
    - Power supply stopped for 7 seconds due to an accident in maintenance work on the power supply equipment
    - About 260 customer systems became unavailable
    - Customer services such as credit card payments and smartphone payments were affected

【6】Business suspension due to unexpected It infrastructure failures

～It comes suddenly without notice～

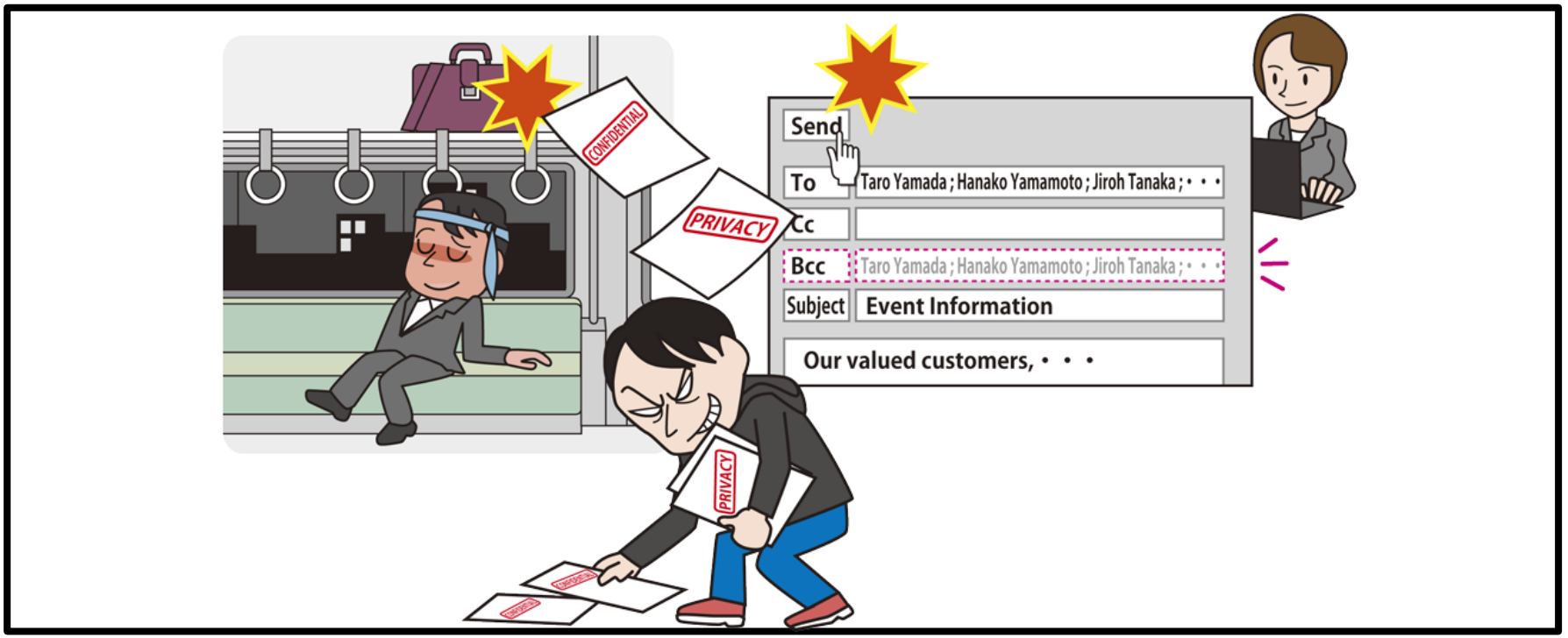
- Countermeasures
  - Service Providers
    - •Preventions
      - Practice BCM (establish and operate BCP)
      - Ensure and maintain availability (system design, monitoring)
      - Perform data backup (recovery measures)
      - Confirm contracts, SLA etc.

        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

【7】Unintentional/Accidental Information Leakage

～'Carelessness' leads to significant incident～



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

【7】Unintentional/Accidental Information Leakage

～'Carelessness' leads to significant incident～

- Causes

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

  - Carelessness from lack of awareness of the importance of handling information
    - Bring out confidential information with a bag, lose the bag and leak the information
    - Send an e-mail 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 information, handling rules, take-out permission procedure etc. are not defined or insufficient

【7】Unintentional/Accidental Information Leakage

～'Carelessness' leads to significant incident～

- Cases and Trends in 2019
  - Employee lost a laptop containing personal information of customers
    - Employee of a restaurant company lost a laptop containing personal information of customers who made a reservation at the company's restaurants
    - Employee left the laptop at a retail store stopped at on his/her way home
    - Up to 67,280 personal information of customer names, company names, and phone numbers were stored on the laptop
    - The company made the login password of the laptop complicated by remote control after the loss was turned out, and then reported it to the police

【7】Unintentional/Accidental Information Leakage

～'Carelessness' leads to significant incident～

- Cases and Trends in 2019
  - E-mail delivery with putting destination addresses into 'To' in place of 'Bcc' by mistake
    - When sending reminder emails for the explanatory meeting, sender mistakenly put applicant's email addresses which should be put into 'Bcc' to 'To'
    - Recipients of the email were able to know the email addresses of all the applicants
    - Sender apologized to all the applicants who received the e-mail and asked them to delete the e-mail

【7】Unintentional/Accidental Information Leakage

～'Carelessness' leads to significant incident～

- Countermeasures
  - Senior Management, Administrators, Person concerned

•Improvement of information literacy and information ethics

- Provide employees with security awareness education/training
- Develop organizational rules and work check procedures

•Preventions

- Follow work check procedures
- Protect information（encryption, access restriction）
- Limit information or devices brought out to the outside
- Implement preventive measures for mistakenly sending email, etc.
- Activate loss prevention function for business-use mobile devices

【7】Unintentional/Accidental Information Leakage

～'Carelessness' leads to significant incident～

- Countermeasures
  - Senior Management, Administrators, Person concerned

•Early detection

- Establish internal reporting system when problems occur
- Set up a Point of Contact with outsiders

•Actions after information leakage occurred

- Prevent damage expansion and eliminate secondary damage factors
- Disclose the content and cause of the leakage
- Contact the relevant person and government agencies
  Supervisory authorities, Personal Information Protection Commission, etc.

【7】Unintentional/Accidental Information Leakage

～'Carelessness' leads to significant incident～

- Countermeasures

  - Victims of Information Leakage
    - •Actions after information leakage occurred
      - Follow information or instructions from the organization where the leakage occurred

        ※Change of password, reissue of credit card, etc.

【8】Personal Information Theft from Services on the Internet

～Website vulnerabilities are not ‘somebody else's problem’～

- Steal personal information by attacks or unauthorized logins on the Internet exploiting vulnerabilities
- Abuse obtained information

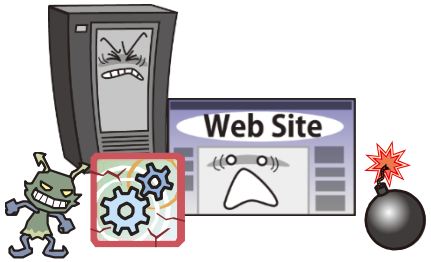
【8】Personal Information Theft from Services on the Internet

～Website vulnerabilities are not ‘somebody else's problem’～

- Attack Methods

•Exploit vulnerabilities in commonly used software

- Server software vulnerabilities exploitation
  - •Exploit multiple software vulnerabilities of server OS, middleware, CMS etc.
- Web application vulnerabilities exploitation
  - •Exploit web application vulnerabilities running on services on Internet （SQL Injection attack, Formjacking etc.）



【8】Personal Information Theft from Services on the Internet

～Website vulnerabilities are not ‘somebody else's problem’～

- Cases and Trends in 2019
  - Customer information leaked by falsification of payment module
    - Payment module of online shopping site was falsified exploiting vulnerabilities of the site
    - Information for 34 customers who entered the credit card information for payment leaked

【8】Personal Information Theft from Services on the Internet

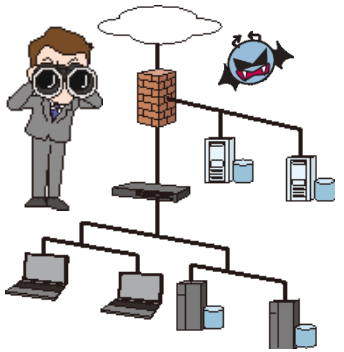
～Website vulnerabilities are not ‘somebody else's problem’～

- Cases and Trends in 2019
  - Unauthorized access to the file transfer service
    - Unauthorized access exploiting vulnerabilities of the server
    - Over 4.8 million personal information leaked
    - Service providing company decided to terminate the service because extensive modification would be required to fix vulnerabilities

【8】Personal Information Theft from Services on the Internet

～Website vulnerabilities are not ‘somebody else's problem’～

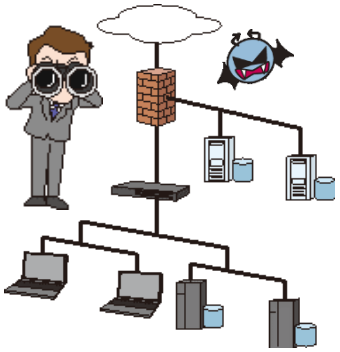
- Countermeasures
  - Web Service Operators, etc.
    - •Preventions
      - Secure budget for security measures and establish organizational framework
      - Create secure web services
      - Practice ‘secure development lifecycle’
      - Practice ‘security by design’
      - Implement security diagnosis
        （Web application diagnosis, platform diagnosis, etc.）
      - Implement WAF, IPS
      - Provide security features for users
        Provide multi factor authentication, features to check login history or purchase history, etc.
      - Understand the status of usage of middleware and libraries



【8】Personal Information Theft from Services on the Internet

～Website vulnerabilities are not ‘somebody else's problem’～

- Countermeasures
  - Web Service Operators, etc.



•Early detection

- Perform appropriate logging and monitor continuously

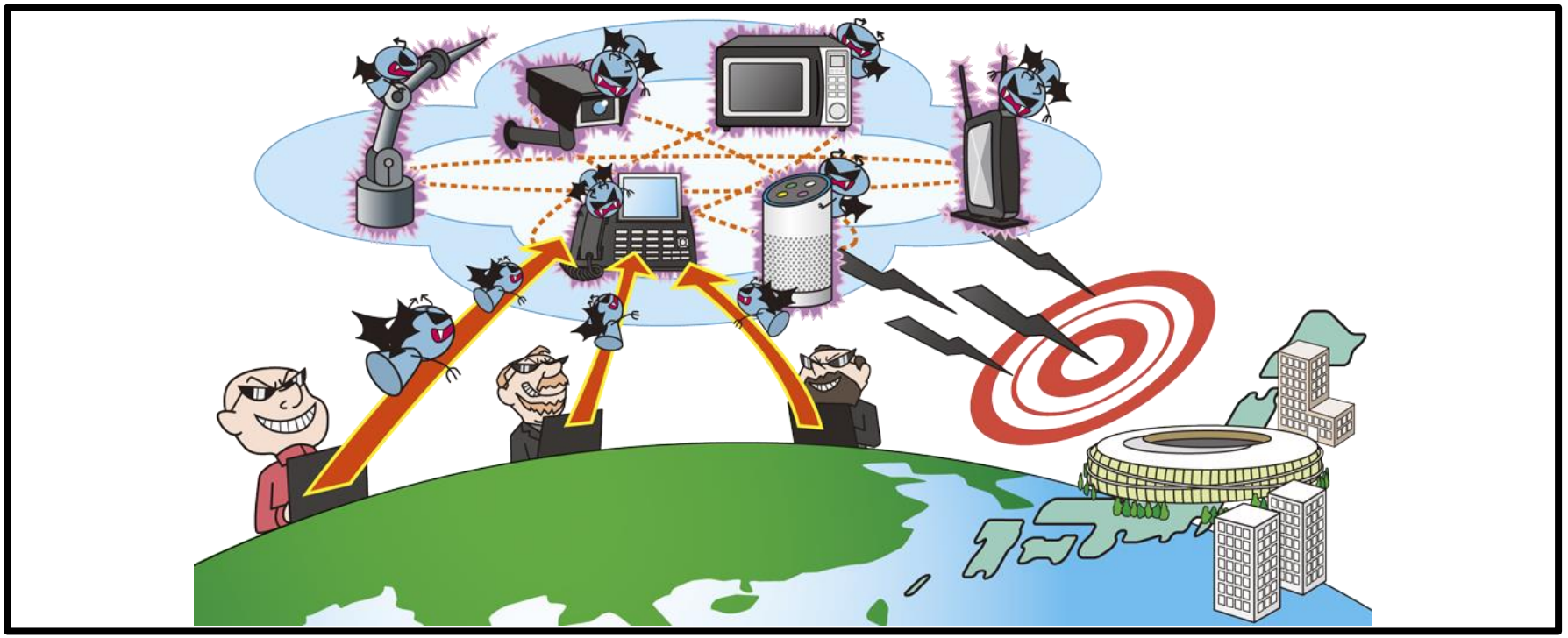
•Actions after attack detected

- Contact/report to CSIRT
- Ask a security specialized company to conduct an investigation
- Investigate impact and detect causes, strengthen countermeasures
- Promptly contact the victims of information leakage and compensate them
- Disclose the content and cause of the leakage
- Contact the relevant person and government agencies

  Supervisory authorities, Personal Information Protection Commission, police, etc.

【9】Fraudulent Use of IoT Devices

～Attacks exploiting vulnerabilities diversify with the spread of IoT devices, Product developers need countermeasures urgently～



- Exploit vulnerabilities in IoT devices and take control of devices
- Interfere with business by abusing the function, etc.
- Use IoT devices as a DDoS attack platform

【9】Fraudulent Use of IoT Devices

～Attacks exploiting vulnerabilities diversify with the spread of IoT devices, Product developers need countermeasures urgently～

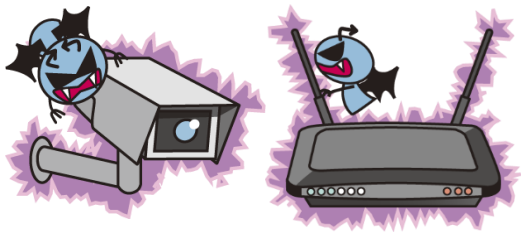
IPA

- Attack Methods

  - IoT devices are connected to the Internet
  - IoT device vulnerability allows unauthorized access or virus infection

  - Attacks exploiting vulnerabilities
    - Exploit vulnerabilities of IoT devices and perform unauthorized access and virus infection

  - Virus infection activities on the Internet
    - Search for IoT devices with the same vulnerability on the Internet, and if found, infect them with virus



【9】Fraudulent Use of IoT Devices

～Attacks exploiting vulnerabilities diversify with the spread of IoT devices, Product developers need countermeasures urgently～

- Cases and Trends in 2019
  - MIC (Ministry of Internal Affairs and Communications) published the guidelines
    - “Guidelines for standard certification of terminal equipment based on the Telecommunications Business Act”
    - Part of the “Terminal Equipment Rules” was revised in order to add security measures to the technical standards of IoT devices [Date of enforcement Apr. 1, 2020]
    - IoT device manufacturers and service providers will be required to take security measures in accordance with the above rule

【9】Fraudulent Use of IoT Devices

～Attacks exploiting vulnerabilities diversify with the spread of IoT devices, Product developers need countermeasures urgently～

- Cases and Trends in 2019
  - MIC released the survey results on vulnerable IoT devices
    - MIC and NICT (National Institute of Information and Communications Technology) conducted a 'NOTICE' survey on IoT devices that could be exploited for cyberattacks
    - About 111,000 of surveyed 110 million IP addresses allow entering IDs and passwords, and 1,328 were able to login [survey results for the 3rd quarter of fiscal 2019]
    - The Maximum detected number of virus-infected IoT devices per day was 598 and the lowest was 60

【9】Fraudulent Use of IoT Devices

～Attacks exploiting vulnerabilities diversify with the spread of IoT devices, Product developers need countermeasures urgently～

- Countermeasures
  - IoT Device Developers

•Preventions

- Practice ‘secure development lifecycle’
- Practice ‘security by design’
- Force initial password change
- Eliminate the vulnerability
  (Secure programming, vulnerability inspection, fuzzing etc.)
- Automate software updates
- Provide easy-to-understand instruction manuals (promote proper device management)
- Quickly deliver security patches
- Disable unnecessary functions for users
- Make secure default settings
- Cleary define the software support period

【9】Fraudulent Use of IoT Devices

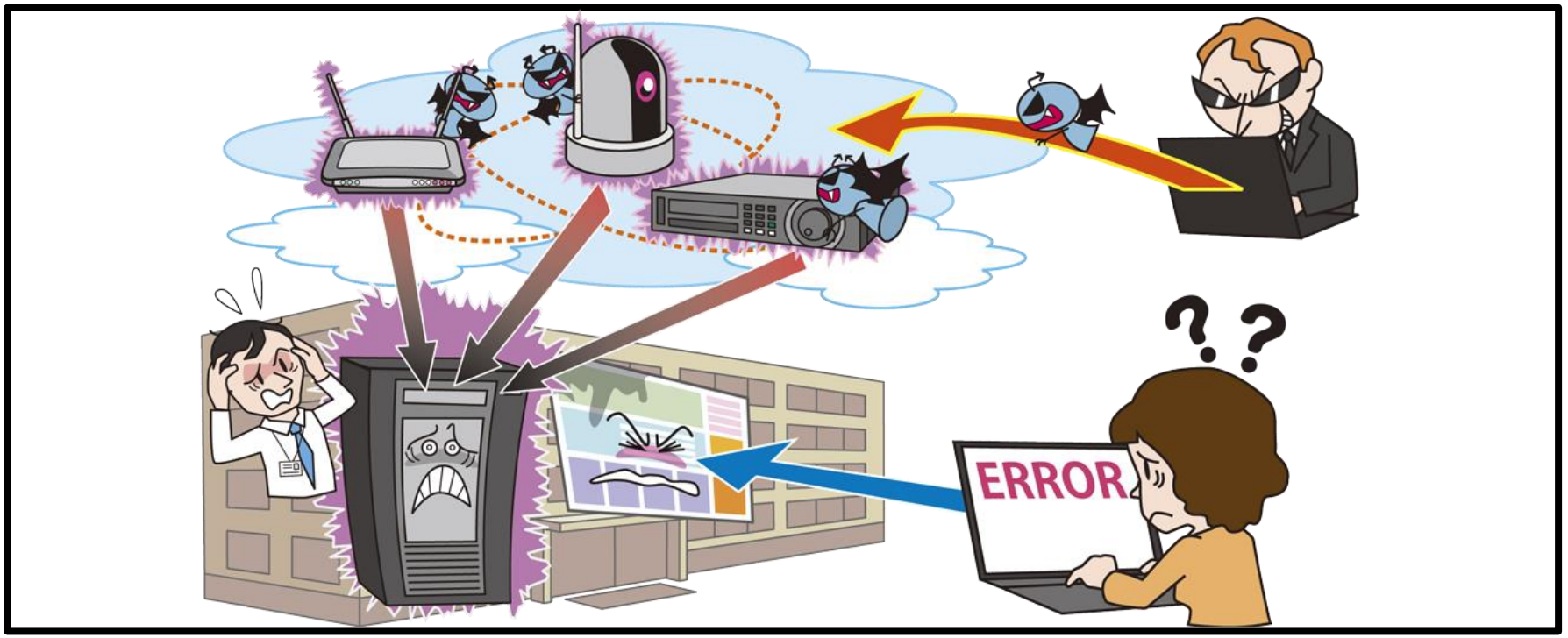
～Attacks exploiting vulnerabilities diversify with the spread of IoT devices, Product developers need countermeasures urgently～

- Countermeasures
  - System Administrators, Users

  - •Information literacy improvement
    - Check the instruction before using the equipment
  - •Preventions
    - Update as soon as patches become available
      （Enable automatic update function etc.）
    - Appropriate access restrictions to the device management screen or management ports
    - Initialize the device before disposal
  - •Actions after attack detected
    - Contact/report to CSIRT
    - Power off IoT devices
    - Implement above "Preventions" after initializing IoT devices
    - Investigate impact and detect causes, strengthen countermeasures

【10】Business Service Outage Caused by DoS Attacks

～Strengthen advance preparations to avoid falling victim to DDoS attacks～



- Overload servers etc. of target organization by superfluous traffic
- Overloaded servers cause process delay or service outage
- Service outage leads loss of business opportunity, damage to organization's credibility etc.

【10】Business Service Outage Caused by DoS Attacks

～Strengthen advance preparations to avoid falling victim to DDoS attacks～

- Attack Methods

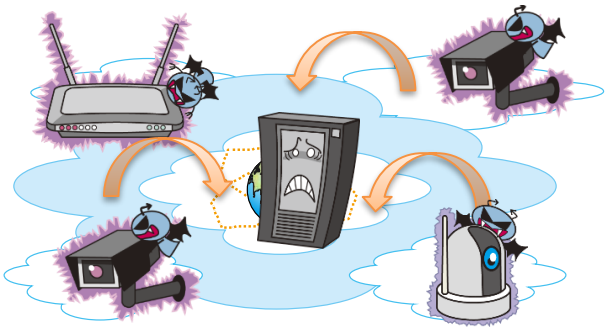
•Overload servers by large amount of request

- DDoS Attack using botnet
  - •Create botnet from virus infected devices etc. and use it for DDoS attack
- Reflector/Reflective DoS Attacks
  - •Send packets whose source IP address is spoofed to the target organization's server to many DNS servers, SNMP servers, etc.
- Use of DDoS as-a-Service
  - •Use DDoS attack agency services in dark web markets etc.
  - •Able to attack relatively easily without specialized technical skills

【10】Business Service Outage Caused by DoS Attacks

～Strengthen advance preparations to avoid falling victim to DDoS attacks～

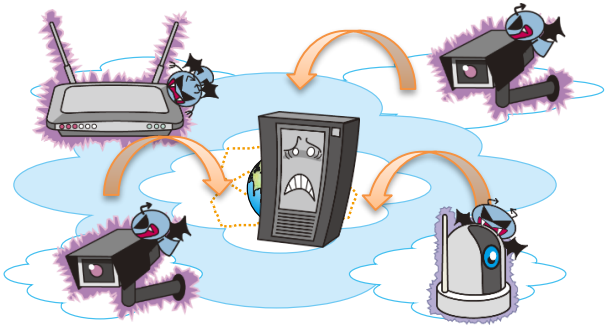
- Cases and Trends in 2019
  - Communication failures occurred at ISP for condominiums
    - Communication failures occurred intermittently in some condominiums due to DDoS attacks from Oct. 2 to 21, 2019
    - The attack source IP address changed overtime and the damage was prolonged
    - To prevent recurrence, the ISP continued to replace equipment installed in the common are in turn and took measures against the attacks



【10】Business Service Outage Caused by DoS Attacks

～Strengthen advance preparations to avoid falling victim to DDoS attacks～

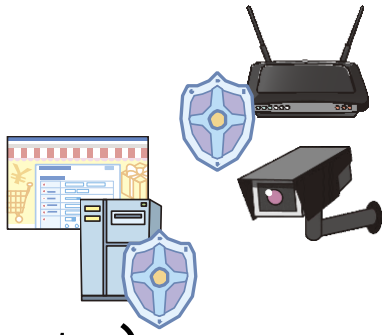
- Cases and Trends in 2019
  - Blackmails suggesting DDoS attack and requesting cryptocurrency
    - German security vendor observed that blackmails had been sent to multiple organizations suggesting DDoS attack and requesting cryptocurrency
    - The attack method was a reflection attack using DNS, NTP, and CLDAP
    - JPCERT/CC observed similar cases in Japan



【10】Business Service Outage Caused by DoS Attacks

～Strengthen advance preparations to avoid falling victim to DDoS attacks～

- Countermeasures
  - Website Operator
    - •Preventions
      - Use ISP or CDN etc. to mitigate the impact of DDoS attacks
      - Implement mitigation measures such as system redundancy
      - Redundant network
      - Prepare alternative servers and establish notification means for while the website stops
    - •Actions after attack detected
      - Contact/report to CSIRT
      - Control communications
        （Communication block from attack source IP address etc.）
      - Notify the situation to service users
      - Investigate impact and detect causes, strengthen countermeasures



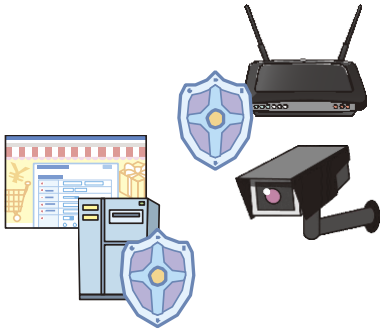
【10】Business Service Outage Caused by DoS Attacks

～Strengthen advance preparations to avoid falling victim to DDoS attacks～

- Countermeasures
  - Service Provider
    - •Preventions
      - Double-check the settings of public servers

        DNS server, NTP server, etc.
      - Strengthen security measures for IoT device vulnerabilities

        Strengthen security measures for IoT devices to prevent them from being used as a stepping stone for attacks as a botnet



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 2020 (in Japanese only)
https://www.ipa.go.jp/security/vuln/10threats2020.html