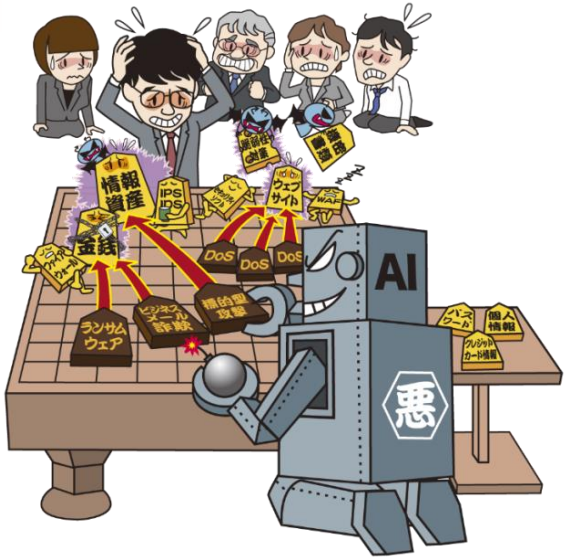
IPA Better Life with IT

10 Major Security Threats 2019

～10 Major Security Threats for Organizations～

～Apply the best security measure depending on the ever-changing situation～



IT Security Center (ISEC)
Information-Technology Promotion Agency (IPA), Japan
August 2019

10 Major Security Threats 2019

- What is “10 Major Security Threats” ?
  - Report issued by IPA every year since 2006
  - IPA explains the outline of the cyber security threats surrounding information systems which is ranked by the vote of “10 Major Security Threats Committee”

10 Major Security Threats 2019

IPA

- Contents

10 Major Security Threats 2019 - Threat Ranking

Threats for Individuals	Rank	Threats for Organizations
Unauthorized Use of Leaked Credit Card Information	1	Advanced Persistent Threat
Phishing Fraud for Personal Information	2	Business E-mail Compromise
Malicious Smartphone Applications	3	Financial Loss by Ransomware
Extortion of money by E-mail etc.	4	Emergence of Attacks Exploiting Supply Chain Weaknesses
Cyberbullying and Fake News	5	Information Leakage by Internal Fraudulent Acts
Internet Fraud by Fake Warnings	6	Business Service Outage Caused by Denial of Service Attacks
Unauthorized Use of Internet Banking Credentials	7	User Information Leakage from Services on Internet
Unauthorized Login to Services on Internet	8	Exposure of IoT Device Vulnerability
Financial Loss by Ransomware	9	Increase of Exploitation Associated with Disclosure of Vulnerability Countermeasure Information
Improper Management of IoT Devices	10	Unintentional/ Accidental Information Leakage

Basic Security Measures

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

- Various threats - “Attack Vectors” can be categorized to some major attack vectors
- Importance of basic security measures has not changed for many years
- In addition to measures for each threat described later, always keep the above measures in mind

10 Major Security Threats 2019
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】Advanced Persistent Threat (APT)

～Many targeted attack e-mails abuse MS Office document files～

- 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

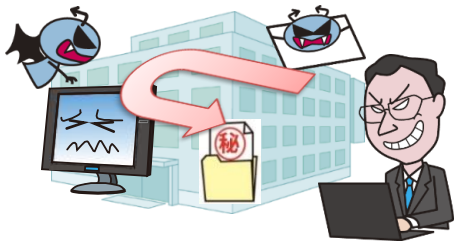
【1】Advanced Persistent Threat (APT)

～Many targeted attack e-mails abuse MS Office document files～

- Attack Methods

•Steal confidential information by virus infection

- Targeted E-mail Attacks
  - Trick users to open malicious attached files
  - Trick users to click on a link to malicious websites
- Watering Hole Attack
  - Observe websites which the target organization often uses
  - Falsify those websites to download viruses
  - Employees of the target organization access those websites and get infected with viruses



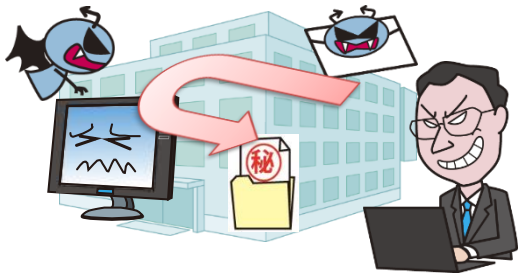
【1】Advanced Persistent Threat (APT)

～Many targeted attack e-mails abuse MS Office document files～

- Attack Methods

  - Steal confidential information 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】Advanced Persistent Threat (APT)

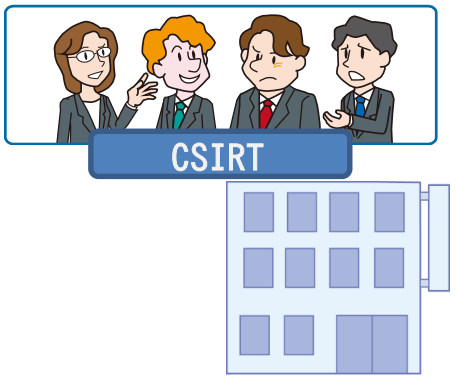
～Many targeted attack e-mails abuse MS Office document files～

- Cases and Trends in 2018
  - Report by J-CSIP
    - Observed e-mails with malicious CSV files attached
      (Abuse the function to execute the program when Excel starts)
    - Also observed abuse of MS Office document files
      The file extensions are ".wiz", ".iqy", ".slk", etc.
      (Abuse the function to execute the program when Word or Excel starts)

【1】Advanced Persistent Threat (APT)

～Many targeted attack e-mails abuse MS Office document files～

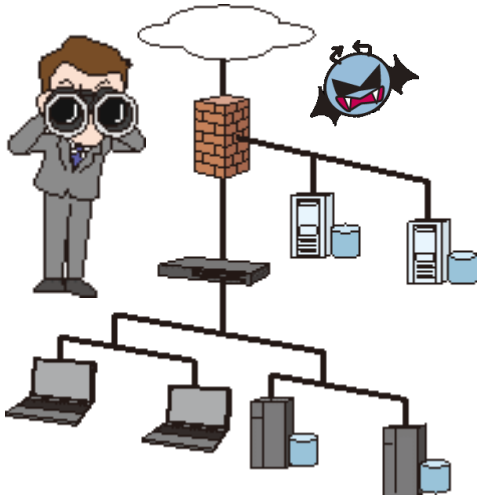
- Countermeasures
  - Senior Management
    - •Establishment of organizational framework
      - - Establish CSIRT that can respond promptly and continuously
      - - Secure budget for countermeasures and perform countermeasures continuously
      - - Develop security policy
  - Information Security Officers
    - •Preventions/ Improvement of response ability
      - - Manage information and develop rules
      - - Implement security education and Incident training
      - - Gather information on cyberattacks
    - •Actions after attack detected
      - - Activate CSIRT
      - - Investigate impact and detect causes, strengthen countermeasures



【1】Advanced Persistent Threat (APT)

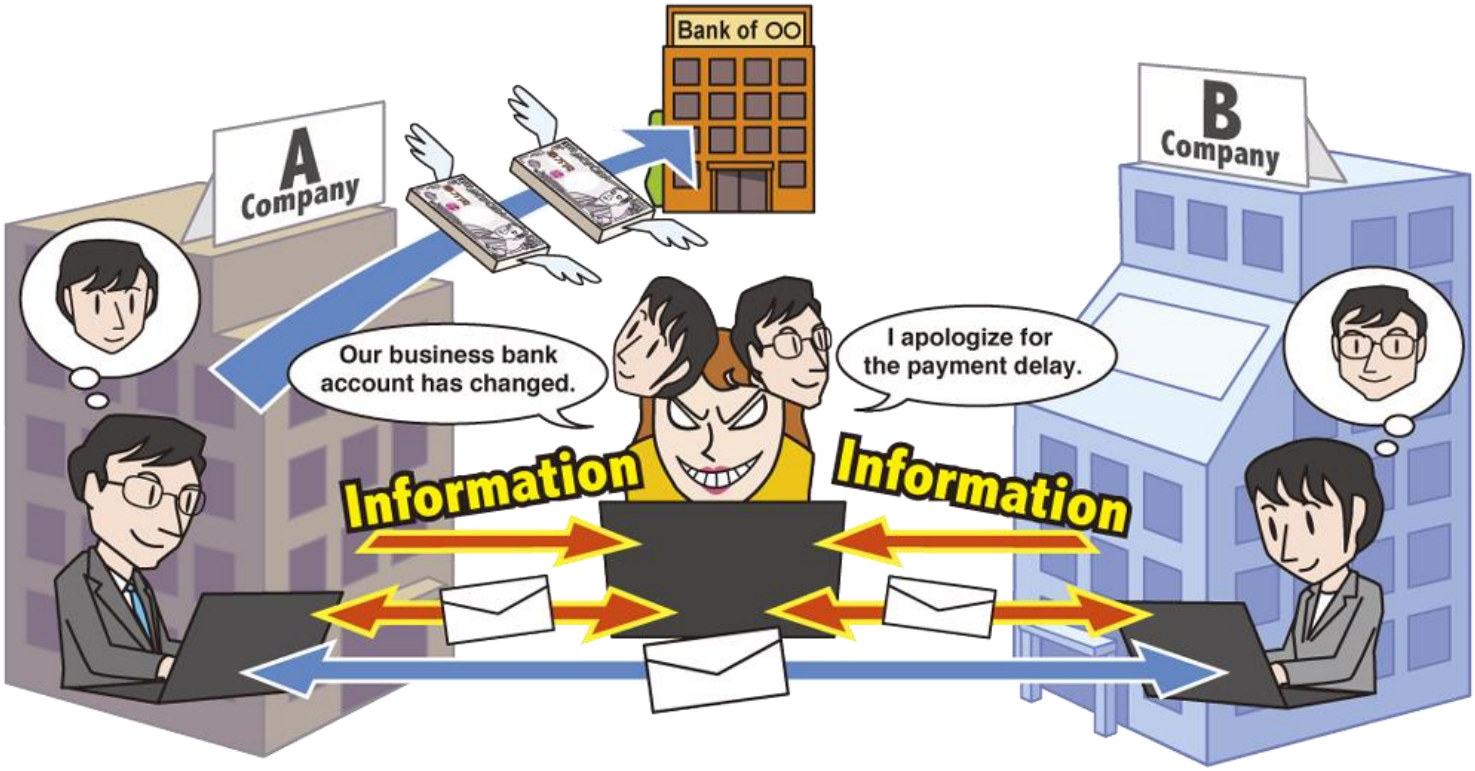
～Many targeted attack e-mails abuse MS Office document files～

- Countermeasures
  - System Administrators
    - •Preventions
      - Design secure system
      - Control access and encrypt data
      - Segment network
    - •Early detection of damage
      - Monitor and protect network
      - Monitor and protect endpoint
  - Employees, Staff
    - •Improvement of information literacy
      - -Take security trainings
    - •Actions after attack detected
      - -Contact/report to CSIRT



【2】Business E-mail Compromise (BEC)

～Cases in which Japanese language is used emerged～



- 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

【2】Business E-mail Compromise (BEC)

～Cases in which Japanese language is used emerged～

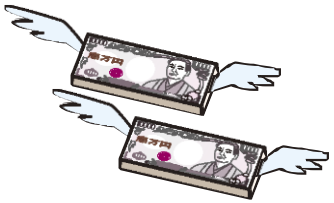
- Attack Methods

  - 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

【2】Business E-mail Compromise (BEC)

～Cases in which Japanese language is used emerged～



- Cases and Trends in 2018
  - Four Japanese arrested in BEC
    - •U.S. agricultural company was extorted about 78 million yen in July 2018
    - •Japanese men and women including company executive are arrested
  - BEC in which Japanese language is used
    - •In 2018, IPA received report regarding BEC in which Japanese language is used
    - •In Aug. 2018, IPA carried out a warning about cases and method of BEC

    (Note also for domestic organizations that do not have transactions with foreign countries or exchange of English e-mail)

【2】Business E-mail Compromise (BEC)

～Cases in which Japanese language is used emerged～

- Countermeasures
  - Organization（Accountant or Financial Officer）

•Prevention of BEC

<Verification of the e-mail authenticity>

- Beware of unusual e-mails
- 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
- Grant electronic signature

<Proper management of e-mail accounts>

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

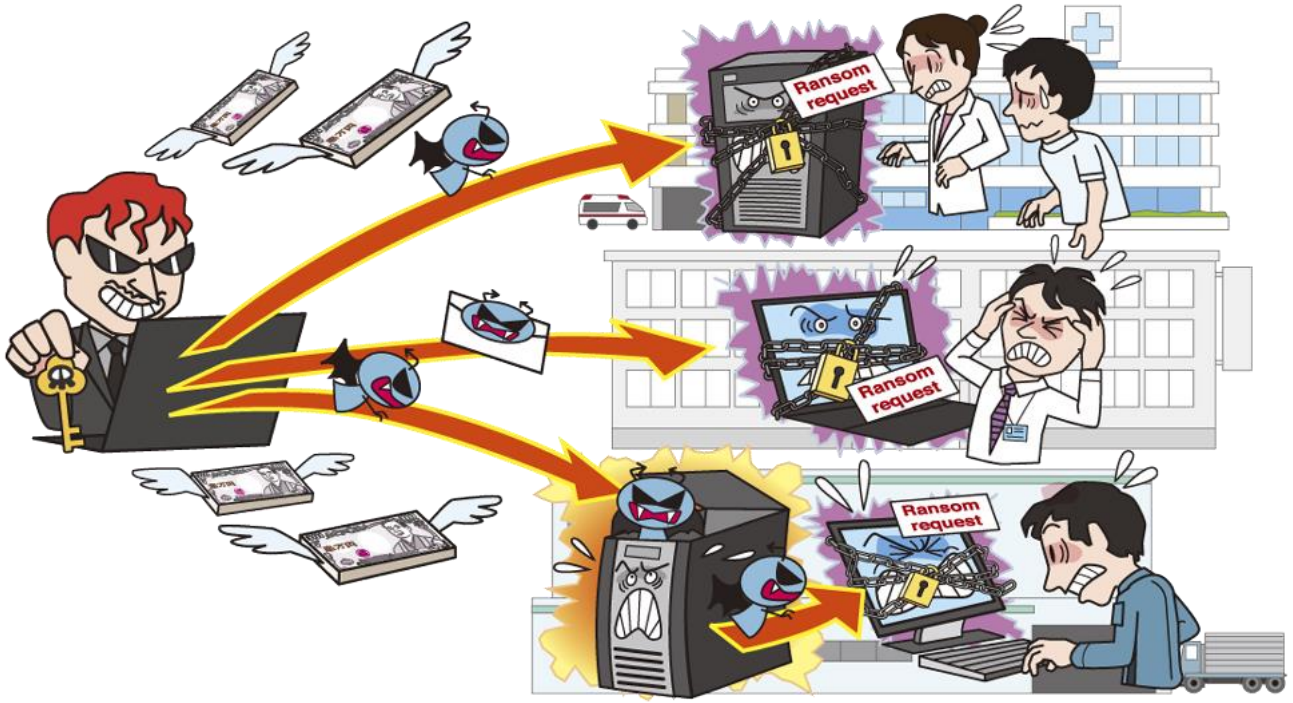
【2】Business E-mail Compromise (BEC)

～Cases in which Japanese language is used emerged～

- 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

【3】Financial Loss by Ransomware

～Attackers infect target organization with ransomware, extort money and disturb business～



- Lock the computer/smartphone screen or encrypt files with ransomware until a ransom is paid
- If important files are encrypted, business continuity may be interfered

【3】Financial Loss by Ransomware

～Attackers infect target organization with ransomware, extort money and disturb business～

- Attack Methods

  - Infect computers with virus (ransomware) and extort money

  - E-mails
    - Trick a target user into opening an attachment

  - Unauthorized Access
    - Access improperly to servers via RDP (Remote Desktop Protocol) etc.
    - Execute (infect) virus on server

【3】Financial Loss by Ransomware

～Attackers infect target organization with ransomware, extort money and disturb business～

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.
- Drive-by downloads from compromised websites
  - •Falsify websites to trick a target user into downloading ransomware
  - •Trick a targeted user into browse the website using e-mail etc.

【3】Financial Loss by Ransomware

～Attackers infect target organization with ransomware, extort money and disturb business～

- Cases and Trends in 2018
  - Electronic medical record system infected with ransomware
    - Electronic medical record system halted for 2 days
    - Ransom was not paid
    - Partial data failed to restore due to flaw in backup system
  - Total financial damage of 「SamSam」is about 670 million yen
    - 「SamSam」is a ransomware observed since around 2015
    - Attackers access servers with RDP used for server management etc. and execute (infect) ransomware

【3】Financial Loss by Ransomware

～Attackers infect target organization with ransomware, extort money and disturb business～

- Countermeasures
  - Senior Management
    - Establishment of organizational framework
      - Establish CSIRT that can respond promptly and continuously
      - Secure budget for countermeasures and perform countermeasures continuously
  - System Administrators, Employees
    - Preventions
      - Check incoming e-mails and visiting websites carefully
      - Stop using expired OS and migrate to effective OS
      - Use filtering tools
      - Segment network
      - Minimize access privileges of shared servers
      - Perform data backup

【3】Financial Loss by Ransomware

～Attackers infect target organization with ransomware, extort money and disturb business～

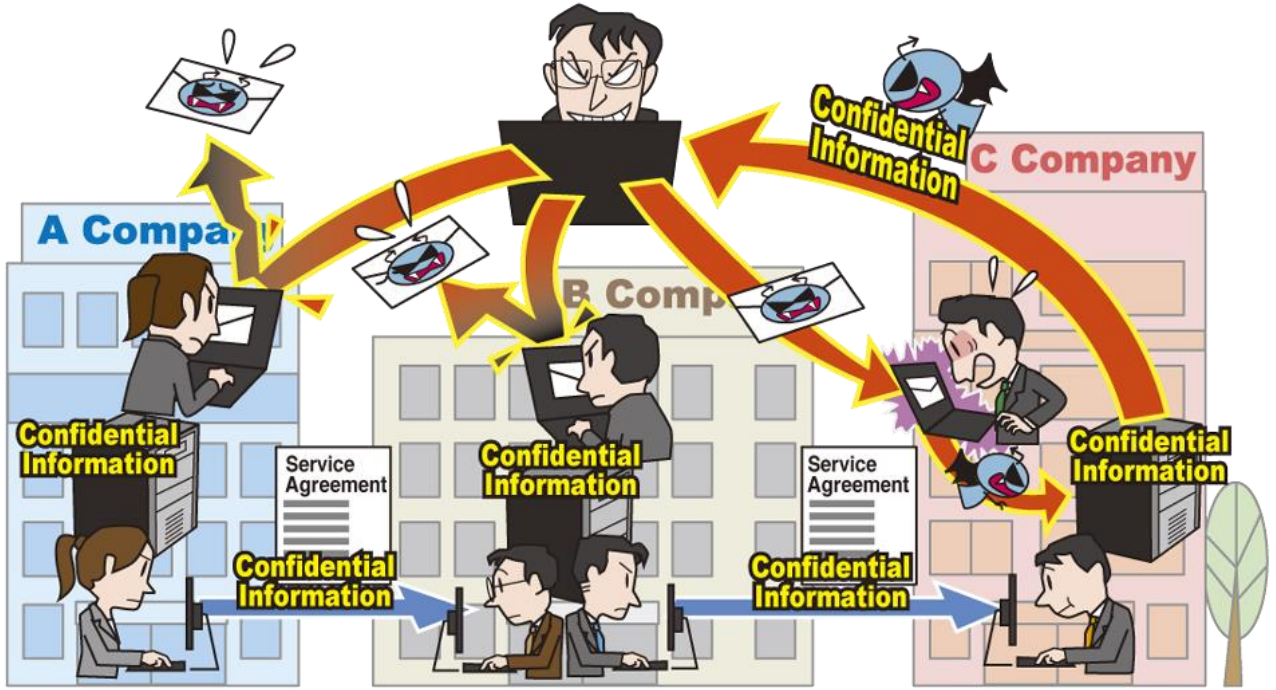
- Countermeasures
  - System Administrators, Employees
    - Actions after attack detected
      - Contact/report to CSIRT
      - Recover from backup
      - Use file decryptor tools
      - Investigate impact and detect causes, strengthen countermeasures

<Exceptional measure>

Not recommended, but there are cases in which ransom is paid if encrypted files are life-threatening.

【4】Emergence of 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】Emergence of Attacks Exploiting Supply Chain Weaknesses

～Appropriate security management is also required for outsourcing partners～

- Causes

• Security measures only for own organization is not perfect

- Companies with lack of security measures 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】Emergence of Attacks Exploiting Supply Chain Weaknesses

～Appropriate security management is also required for outsourcing partners～

- Cases and Trends in 2018
  - Information leakage from an outsourcing company by unauthorized access
    - E-mail addresses were leaked due to unauthorized access to the outsourcing company
  - Many organizations do not clearly articulate must-do information security measures in specification document etc.
    - According to the research results published by IPA, the majority of entrusters other than the information and telecommunications industry have not articulated security measures. (In particular, 71% for manufacturing, 74% for wholesale and retail)

【4】Emergence of Attacks Exploiting Supply Chain Weaknesses

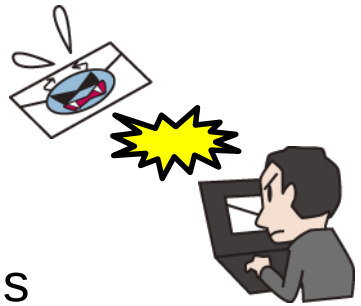
～Appropriate security management is also required for outsourcing partners～

- 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

【4】Emergence of Attacks Exploiting Supply Chain Weaknesses

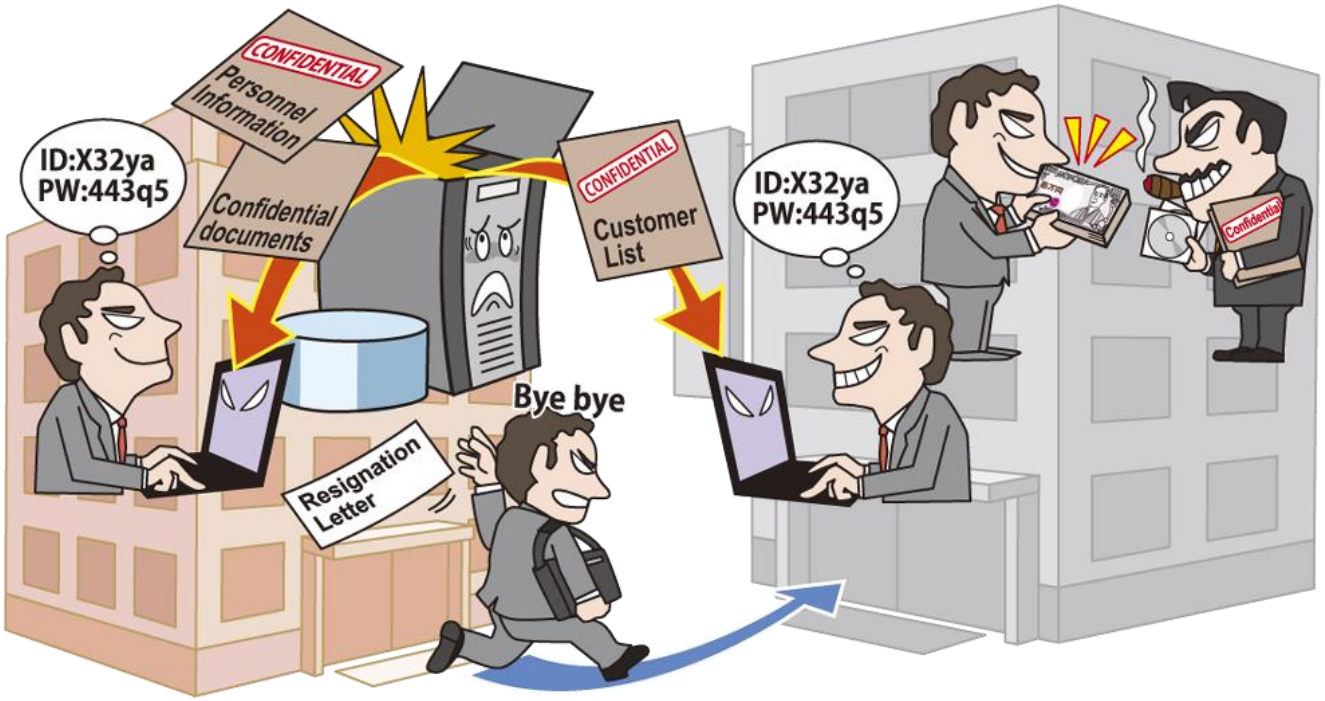
～Appropriate security management is also required for outsourcing partners～

- 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



【5】Information Leakage by Internal Fraudulent Acts

～Establish and implement management and monitoring framework/system to prevent 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

【5】Information Leakage by Internal Fraudulent Acts

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

IPA

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 memory or e-mail etc.

【5】Information Leakage by Internal Fraudulent Acts

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

- Cases and Trends in 2018
  - Employee transferred data of employees to the private computer
    - Disassembled the business-use computer and removed the hard disk, transferred wage data etc. to the private computer and sent it to other organization with malicious intent
  - Employee stole customer credit card information
    - Former part-time employee stole customer credit card information during the job and used it in online shopping

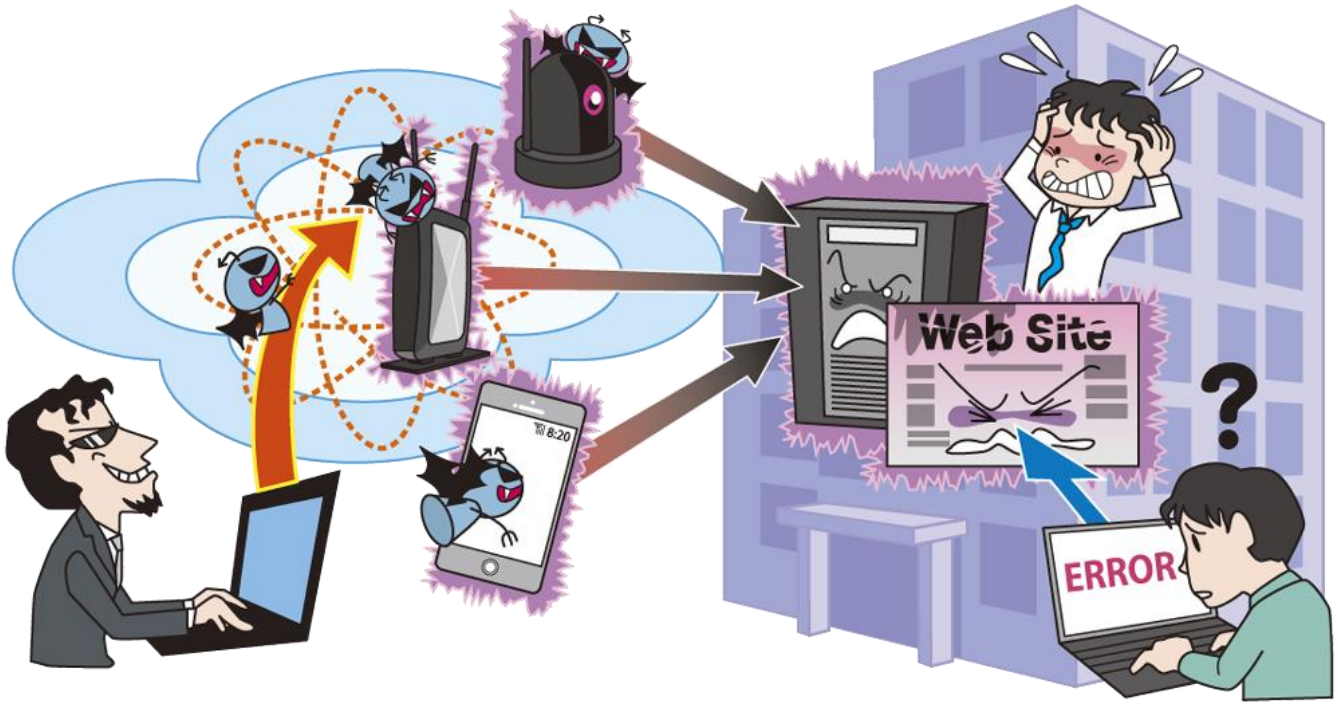
【5】Information Leakage by Internal Fraudulent Acts

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

- Countermeasures
  - Senior Management, Administrators
    - •Preventions
      - Develop basic policy for fraudulent act measures
      - Identify assets which should be protected
      - Establish organizational framework
      - 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/report to CSIRT, police etc.
      - Investigate impact and detect causes, strengthen countermeasures
      - Appropriate punishment for internal fraudulent actors

【6】Business Service Outage Caused by DoS Attacks

～Large-scale DDoS attacks occur both domestically and abroad～



- 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.

【6】Business Service Outage Caused by DoS Attacks

～Large-scale DDoS attacks occur both domestically and abroad～

- Attack Methods

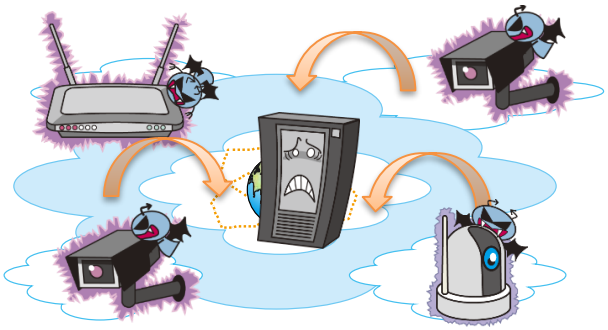
•Overload servers by large amount of request

- 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

【6】Business Service Outage Caused by DoS Attacks

～Large-scale DDoS attacks occur both domestically and abroad～

- Cases and Trends in 2018
  - Large-scale DDoS attack by Memcached
    - Used open source memory cache system as a springboard
    - Transaction volume of 33.08 Gbps by packets of up to 3.35 million pps
  - Service-use restriction by DDoS attack
    - DDoS attack to video site caused process delay and service outage
    - Even after blocking communications, DDoS attack continued relentlessly by changing means



【6】Business Service Outage Caused by DoS Attacks

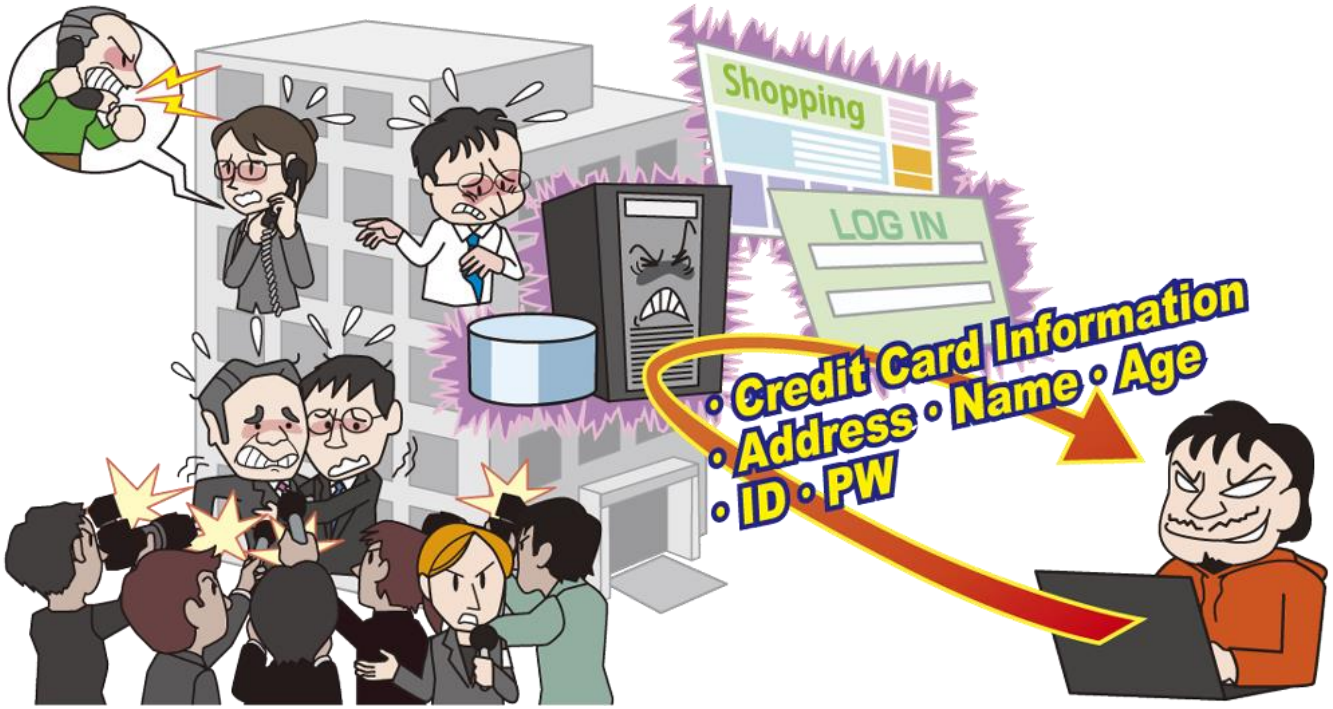
～Large-scale DDoS attacks occur both domestically and abroad～

- Countermeasures
  - Website Operator
    - •Preventions
      - Use ISP or CDN etc. to mitigate the impact of DDoS attacks
      - Control communications with outside to servers/services
      - Implement mitigation measures such as system redundancy
      - 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

【7】User Information Leakage from Services on Internet

～Review security measures for services on Internet～



- Steal personal information etc. stored in services on Internet
- Abuse obtained information

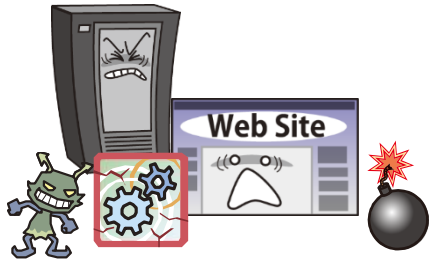
【7】User Information Leakage from Services on Internet

～Review security measures for services on Internet～

- Attack Methods

•Steal information from services on Internet by unauthorized access

- 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.）



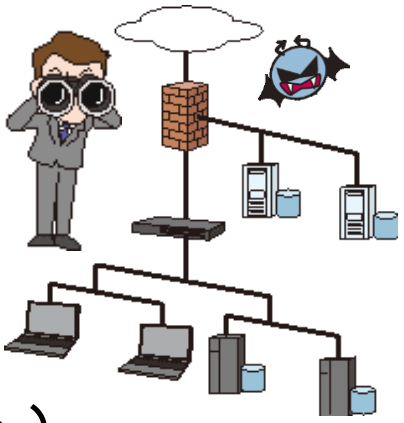
【7】User Information Leakage from Services on Internet

～Review security measures for services on Internet～

- Cases and Trends in 2018
  - Attack on the website of leading contact lens seller
    - Exploited known vulnerability of server software OpenSSL, "Heartbleed"
    - Leaked credit card information of up to 3,412
  - Attack on the website of healthcare related organization
    - SQL injection attack that exploits system vulnerability
    - Leaked e-mail addresses and passwords of more than 20,000 people registered in the system

【7】User Information Leakage from Services on Internet

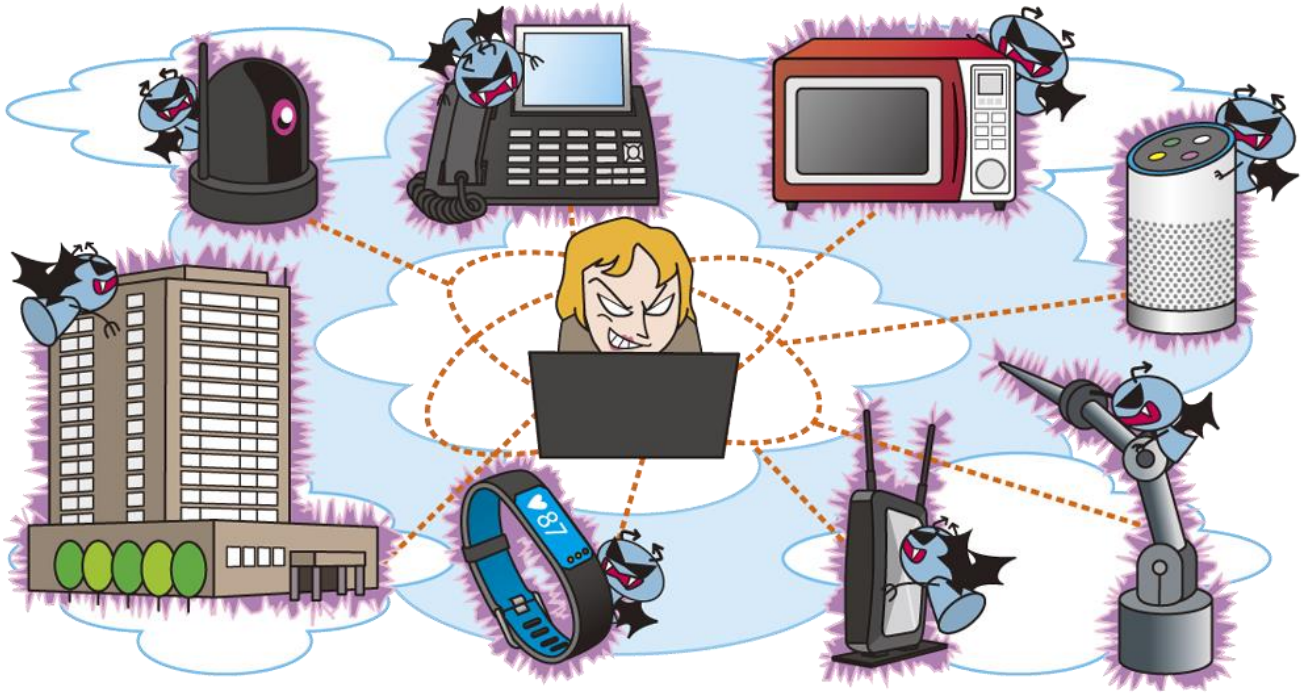
～Review security measures for services on Internet～



- Countermeasures
  - Web Service Operators, etc.
    - •Preventions
      - Create secure web services
      - Implement security diagnosis
        （Web application diagnosis, platform diagnosis etc.）
      - Implement WAF, IPS
    - •Early detection
      - Perform appropriate logging and monitor continuously
    - •Actions after attack detected
      - Contact/report to CSIRT
      - Investigate impact and detect causes, strengthen countermeasures
      - Compensate users for leaked information

【8】Exposure of IoT Device Vulnerability

～Attacks on IoT device vulnerabilities are increasing
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

【8】Exposure of IoT Device Vulnerability

～Attacks on IoT device vulnerabilities are increasing
Product developers need countermeasures urgently～

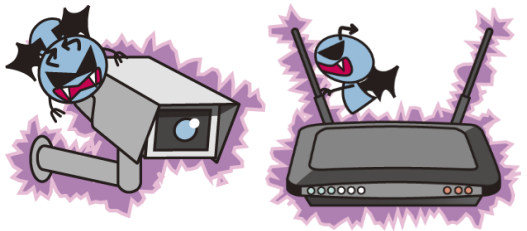
IPA

- Attack Methods

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

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

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



【8】Exposure of IoT Device Vulnerability

～Attacks on IoT device vulnerabilities are increasing
Product developers need countermeasures urgently～

- Cases and Trends in 2018
  - Unauthorized access to river surveillance camera
    - Accessed to the camera and manipulated to display characters such as "I'm hacked bye2“
  - Intrusion on routers and rewriting the DNS settings
    - Directed users to access the malicious website via routers with rewritten DNS settings
    - A message was displayed on the visited website which indicate the function improvement of Facebook. When user followed the instructions, a malicious smartphone app was downloaded.

【8】Exposure of IoT Device Vulnerability

～Attacks on IoT device vulnerabilities are increasing
Product developers need countermeasures urgently～

- Countermeasures
  - IoT Device Developers

•Preventions

- Force initial password change
- Eliminate the vulnerability
  (Secure programming, vulnerability inspection, fuzzing etc.)
- Automate software updates
- Provide easy-to-understand instruction manuals
- Disable unnecessary functions
- Make secure default settings
- Call for appropriate management on users
- Cleary define the software support period

【8】Exposure of IoT Device Vulnerability

～Attacks on IoT device vulnerabilities are increasing
Product developers need countermeasures urgently～

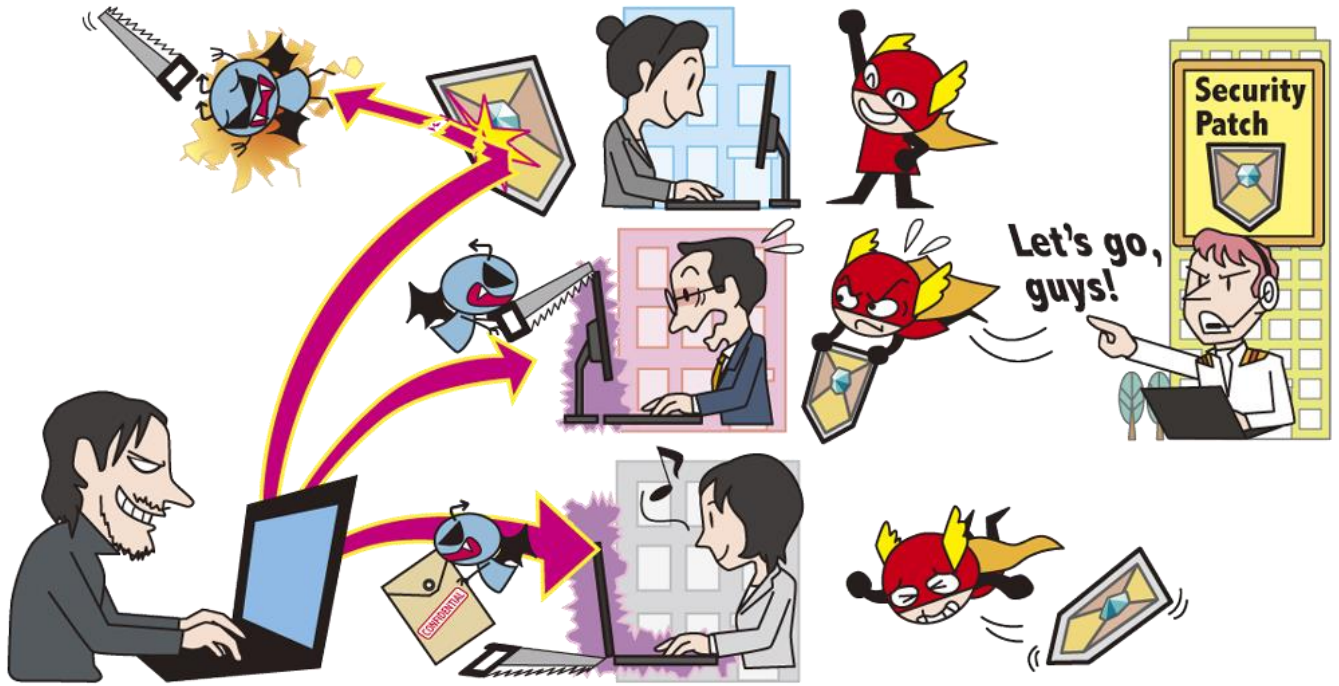
- Countermeasures
  - System Administrators, Users

•Preventions
- Update as soon as patches become available
  （Enable automatic update function etc.）
- Appropriate access restrictions to the device management screen or management ports

•Actions after attack detected
- Contact/report to CSIRT
- Power off IoT devices
- Implement "Preventions" after initializing IoT devices
- Investigate impact and detect causes, strengthen countermeasures

【9】Increase of Exploitation Associated with Disclosure of Vulnerability Countermeasure Information

～Capability for quick and appropriate response to vulnerabilities is required～



- Exploit published vulnerability countermeasure information
- Attack users who have not applied the vulnerability countermeasures
- Impacts are information leakage or falsification, virus infection etc.

【9】Increase of Exploitation Associated with Disclosure of Vulnerability Countermeasure Information

～Capability for quick and appropriate response to vulnerabilities is required～

- Attack Methods

  - Countermeasures are published when vulnerability is found
  - The information can be used for attacks

- Exploit vulnerabilities having no implemented countermeasure
  - Attack users who have not implemented the published countermeasures against the vulnerability
  - Popular products can be exploited by same attack methods so damage may expand

【9】Increase of Exploitation Associated with Disclosure of Vulnerability Countermeasure Information

～Capability for quick and appropriate response to vulnerabilities is required～

- Cases and Trends in 2018
  - Attacks exploiting Apache Struts 2 vulnerability
    - Apache Struts2 vulnerability was published in Aug. 2018
    - A few days later, exploit code for the vulnerability was disclosed
    - About 2 weeks later, attacks which install a cryptocurrency mining software using the exploit code were observed
  - Attacks exploiting Drupal vulnerability
    - Drupal vulnerability was published in March 2018
    - Exploit code for the vulnerability was disclosed in April
    - Same attacks that seems to have aimed at this vulnerability was also activated in Japan

【9】Increase of Exploitation Associated with Disclosure of Vulnerability Countermeasure Information

～Capability for quick and appropriate response to vulnerabilities is required～

- Countermeasures
  - System Administrators, Users
    - •Preventions
      - Identify assets which should be protected
      - Establish organizational framework
      - Collect vulnerability related information
      - Implement WAF, IPS
      - Monitor network and block communications used for attacks
      - Use software with fulfilling security support and secure version
      - Suspend servers temporarily etc. to prevent attacks, if security patch cannot apply immediately
    - •Actions after attack detected
      - Contact/report to CSIRT
      - Investigate impact and detect causes, strengthen countermeasures

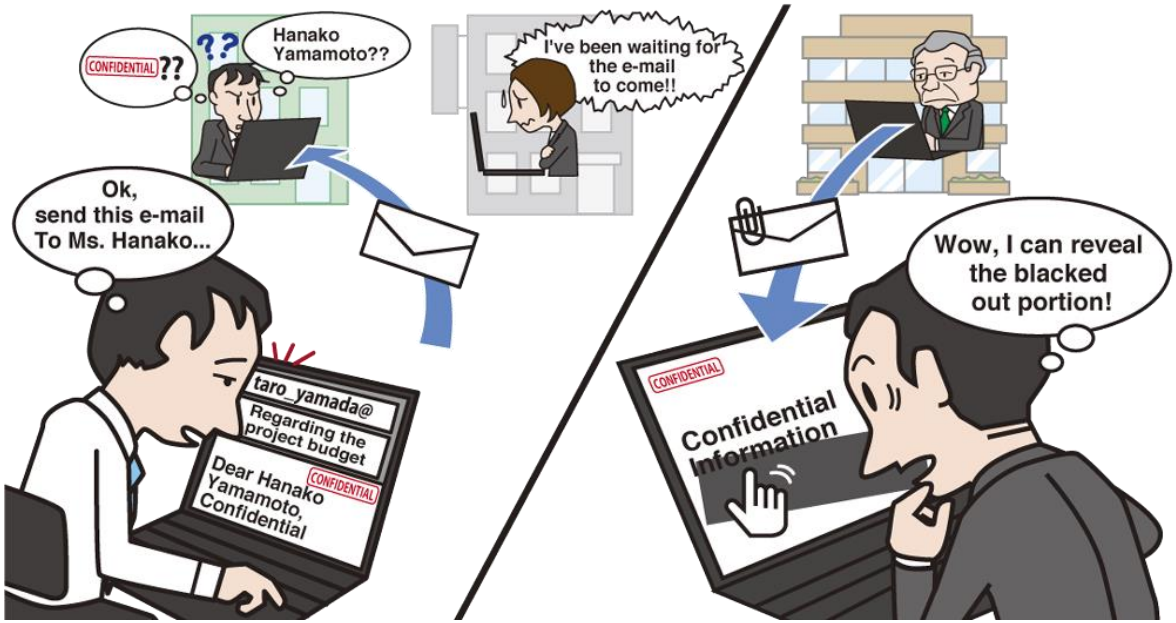
【9】Increase of Exploitation Associated with Disclosure of Vulnerability Countermeasure Information

～Capability for quick and appropriate response to vulnerabilities is required～

- Countermeasures
  - Product Developers
    - •Preventions
      - Identify and strictly manage software embedded in products
      - Collect vulnerability related information
      - Create response procedures for when vulnerability detected
      - Establish mechanism for transmitting information quickly

【10】Unintentional/Accidental Information Leakage

～One careless mistake can seriously harm an organization's credibility～



- 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

【10】Unintentional/Accidental Information Leakage

～One careless mistake can seriously harm an organization's credibility～

- 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.
- Individual situation
  - 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

【10】Unintentional/Accidental Information Leakage

～One careless mistake can seriously harm an organization's credibility～

- Cases and Trends in 2018
  - Wrong transmission of e-mail including TV interview information
    - E-mail, including download URL of interview audio files of residents concerning a certain religious group, was sent to the religious group by mistake
  - Loss of business-use mobile terminal
    - Gas company's employee lost a shoulder bag containing a mobile terminal in which customer information for 421 households recorded
    - Gas company reported that there was no information leakage since security measures have been applied to the terminal

【10】Unintentional/Accidental Information Leakage

～One careless mistake can seriously harm an organization's credibility～

- 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
- Activate loss prevention function for business-use mobile devices

•Early detection

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

【10】Unintentional/Accidental Information Leakage

～One careless mistake can seriously harm an organization's credibility～

Countermeasures

- Actions after information leakage occurred
  - Contact/report to CSIRT
  - Investigate impact and detect causes, strengthen countermeasures
  - Prevent damage expansion and eliminate secondary damage factors
  - Disclose the content and cause of the leakage

Victims

- Actions after information leakage occurred
  - Follow information from the organization where the leakage occurred

    ※Change of password, change of credit card information etc.

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 2019 (in Japanese only)
https://www.ipa.go.jp/security/vuln/10threats2019.html