Threats in Cyberspace 2018

1. Cyber-attacks

(1) Scanning Activities in Cyberspace

a. Overview of the unexpected connection attempts to the sensors[1]

Number of the unexpected connection attempts to the sensors has risen to 2,752.8 per IP address per day in 2018, showing an upward trend.

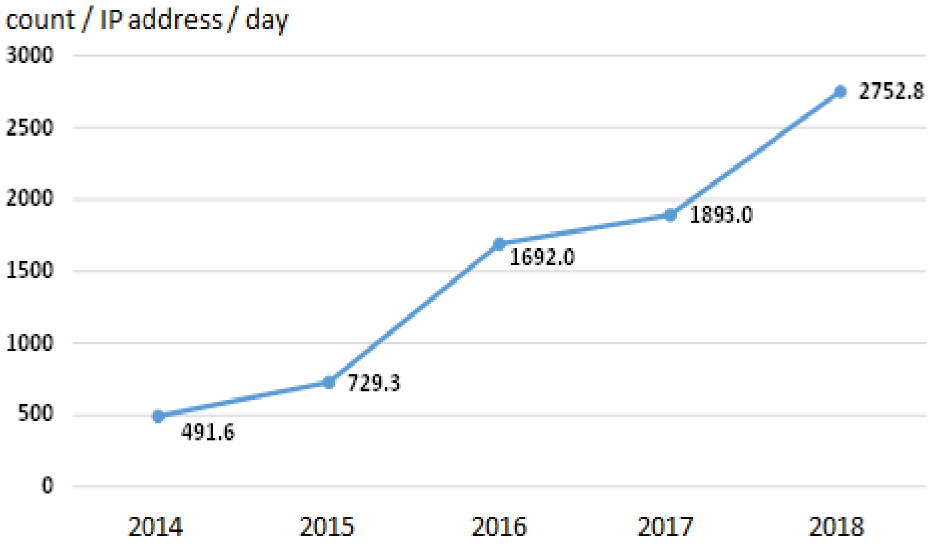

Figure 1 [Number of unexpected connection attempts to the sensors]

b. Characteristics

- **Increase of the unexpected connection attempts to the ports numbered 1024 and above**

As for the destination ports[2] where the unexpected connection attempts were observed, number of the unexpected connection attempts to the ports numbered 1023 and below, used for general purposes, e.g. sending/receiving e-mails and web browsing, has been declining since 2016. Meanwhile, number of the unexpected connection attempts to the other ports numbered 1024 and above has been on the rise, reaching 1,702.8 per IP address per day in 2018, approximately doubling that of 2017. A major reason for the increase is a surge of scanning activities from specific sources targeting broad range of ports in the 2nd half of 2018.

[1] The sensors here refer to the components of the Real-time Detection Network System operated around-the-clock by the NPA, placed at the Internet connection points of police institutes throughout Japan. These sensors detect, aggregate and analyze the connecting information presumed to be extraordinary use of the Internet including the scanning activities for attempting cyber-attacks.

[2] The ports here refer to the computer interfaces for identifying protocols to be applied in the TCP.UDP/IP communications. A number from 0 through 65525 is assigned to each port.

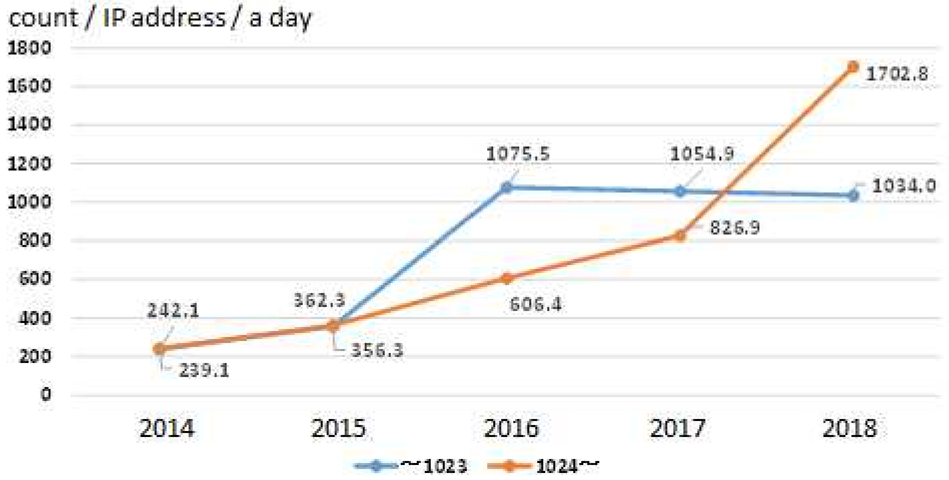

Figure 2 [Number of unexpected connection attempts classified by destination port]

- **Observation of the unexpected connection attempts targeting cryptoasset networks**

The NPA observed the unexpected connection attempts targeting cryptoassets and cryptoasset mining software throughout 2018 such as the connection attempts to the port 8545/TCP presumably targeting the Ethereum network.

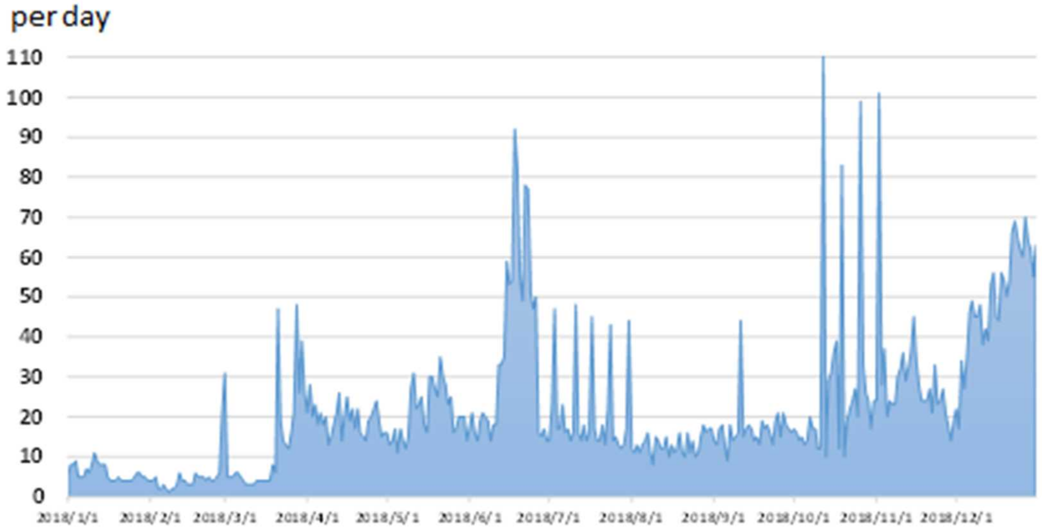

Figure 3 [Number of originating IP addresses of unexpected connection attempts to the (destination) port 8545/TCP presumably targeting the Ethereum networks]

- **Observation of SYN/ACK reflection attacks**

The NPA observed a surge of the unexpected connection attempts from September 2018 at the port 80/TCP used to display the websites, presumably a type of DoS attacks called “SYN/ACK reflection attacks” which abuses communication mechanisms necessary for web browsing by intensively accessing the targeted devices to flood and disable their services.

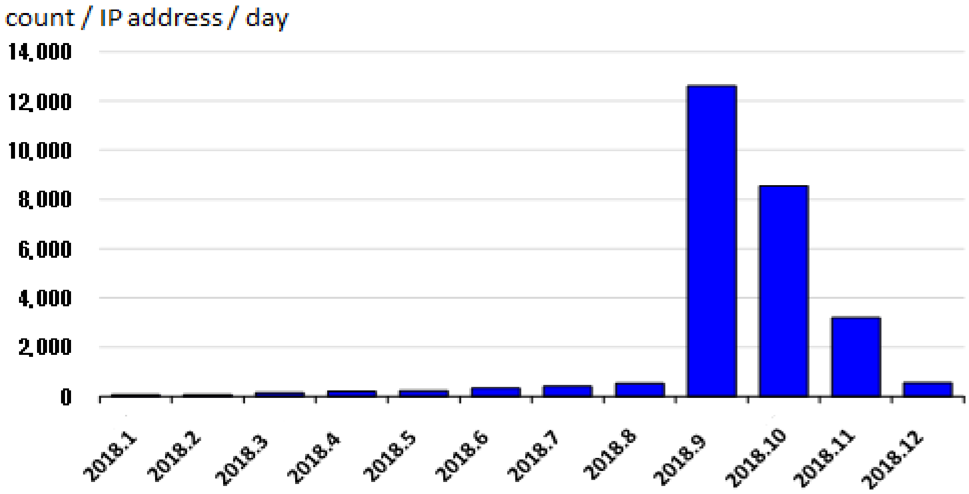

Figure 4 [Number of unexpected connection attempts to port 80/TCP]

(2) Status and Countermeasures

a. Status

(a) Overview

The Japanese police shares with business operators and other organizations information on cyber-attacks which appear to aim at stealing data through the Counter Cyber-intelligence Information-Sharing Network[3]. Number of the spear phishing e-mail attacks identified by the Japanese police through the Network has been on the rise in recent years, reaching 6,740 cases in 2018.

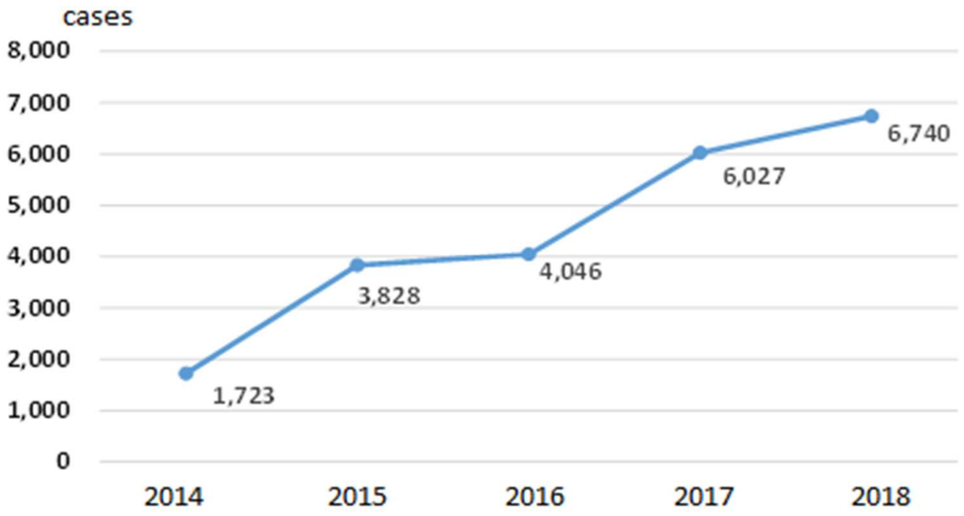

Figure 5 [Number of spear phishing e-mail attacks]

[3] A nationwide network consisting of the police and 7,777 business operators and other organizations (as of January 2019) with the cutting-edge technologies to share information on cyber-attacks which appear to aim at stealing data. The police and the member organizations also share analysis on spear phishing e-mail attacks against the governmental entities through this network in coordination with the National Center of Incident-readiness and Strategy for Cybersecurity (NISC).

Also, browsing failures of the websites of the Japanese government agencies, public transports and museums continued to occur as in 2017.

The Japanese police confirmed that the parties who claimed to be an international hacker group “Anonymous” posted on the SNS the apparent claims of responsibility for the cyber-attacks against 21 organizations.

(b) Modus operandi of spear phishing e-mail attacks

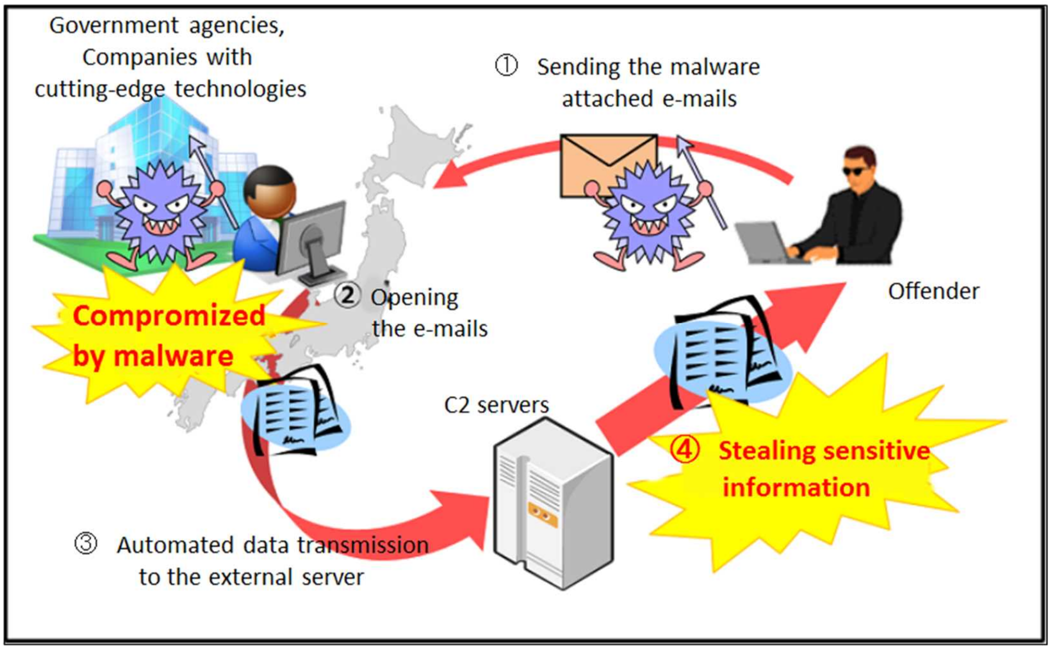

Figure 6 [Mechanism of spear phishing e-mail attacks]

- **Continued rash of the “indiscriminate”[4] spear phishing e-mail attacks**

High level occurrence of the “indiscriminate” spear phishing e-mail attacks continued, accounting for approx. 90% of the total number of spear phishing e-mail attacks.

Year	Indiscriminate Attacks	Non-indiscriminate Attacks
2014	86% (1,474 cases)	14% (249 cases)
2015	92% (3,508 cases)	8% (320 cases)
2016	90% (3,641 cases)	10% (405 cases)
2017	97% (5,846 cases)	3% (181 cases)
2018	90% (6,040 cases)	10% (700 cases)

Figure 7 [Ratio of the “indiscriminate” spear phishing e-mail attacks and others]

[4] The NPA defines the “spear phishing e-mail attacks” as sending e-mails in the disguise of legitimate business communications attaching malware undetectable by the commercial anti-virus programs to infect the targeted computers in the aim of stealing data. The NPA specifies the type of spear phishing e-mail attacks which distribute the same texts or malware to more than 10 destinations as the “indiscriminate” attacks.

- **Spear phishing e-mails mostly sent to the undisclosed e-mail addresses**

71% of the entire spear phishing e-mails destinations were the undisclosed e-mail addresses.

- **Most originating addresses of the spear phishing e-mails forged**

98% of the originating addresses of the spear phishing e-mails appeared to be forged.

- **Changing ratios of the file types attached to the spear phishing e-mails**

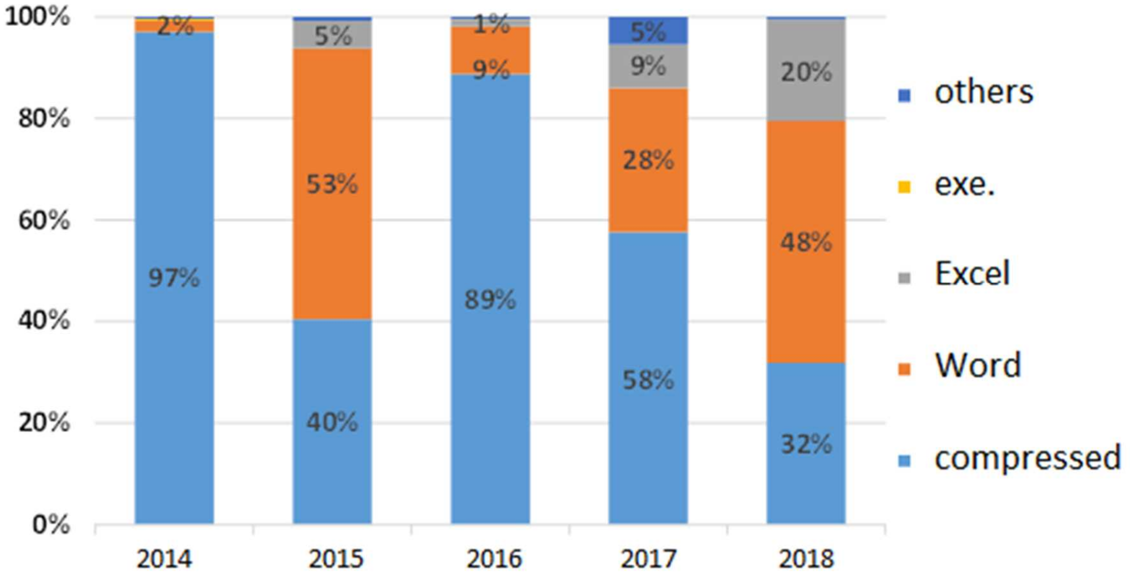

Figure 8 [Ratios of the file types attached to the spear phishing e-mails]

While the compressed, MS-Word and MS-Excel files continued to dominate the types of attachments to the spear phishing e-mails, shares of the MS-Word and MS-Excel files including the macro-abusing and vulnerability-targeting types increased.

- **Change of the attached compressed file types**

Among the compressed files attached to the spear phishing e-mails, script files[5] which had dominated since 2016 were not identified, while the executable files occupied a high level of share in 2018.

[5] The script files here refer to the files written in simple programing languages (scripting languages). This file type is often abused to induce downloading of the malicious executable files.

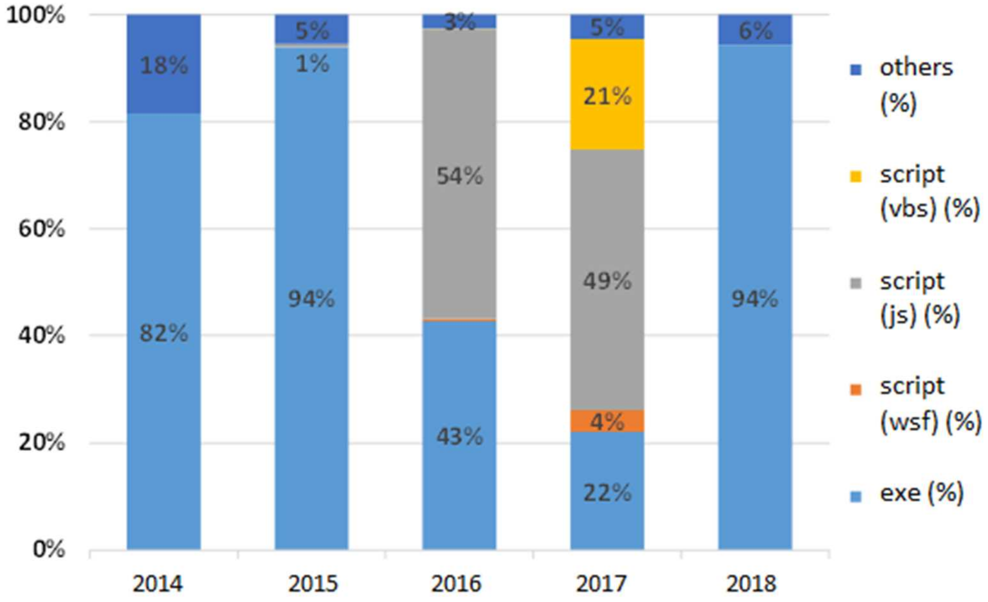

Figure 9 [Ratios of the compressed file types attached to the spear phishing e-mails]

b. Countermeasures

(a) Takedowns of C2[6] servers used for cyber-attacks

The Japanese police has been encouraging the server hosting services to take down the C2 servers in Japan which had been identified through analysis of the malware abused in the cyber-attack cases. In this endeavor, 12 C2 servers were disabled in 2018.

(b) Promoting countermeasures against cyber-attacks toward the Tokyo 2020 Olympic and Paralympic Games

In preparation for the Tokyo 2020 Olympic and Paralympic Games, the Japanese police has promoted diverse measures against cyber-attacks including joint drills simulating occurrences of the cyber-attacks, and information sharing with the pertinent organizations of the previous host countries of the Olympic and Paralympic Games.

【Joint drill toward the Tokyo 2020 Olympic and Paralympic Games】

In October 2018, the NPA, Tokyo Metropolitan Police Department, Ibaraki, Saitama, Chiba and Kanagawa Prefectural Police conducted a joint drill, simulating occurrence of the cyber-attacks targeting the core systems and facilities of the Olympics and Paralympics, critical infrastructural systems, e.g. electricity and railways, as well as spear phishing e-mail attacks and website attacks targeting business operators and organizations.

[6] C2 servers here refer to the Command and Control Servers, occasionally abbreviated as the “C&C servers” as well. C2 servers are the central regulator operated at the commands of the offenders to remotely send the commands into the computers compromised with malware.

2. Cybercrimes

(1) Cybercrimes crackdown

a. Number of the cleared cybercrime cases has been on the rise, reaching the record high of 9,040 in 2018. Meanwhile, the number of cybercrime-related consultations was 126,815 in 2018, on a declining trend after it hit the highest in 2016.

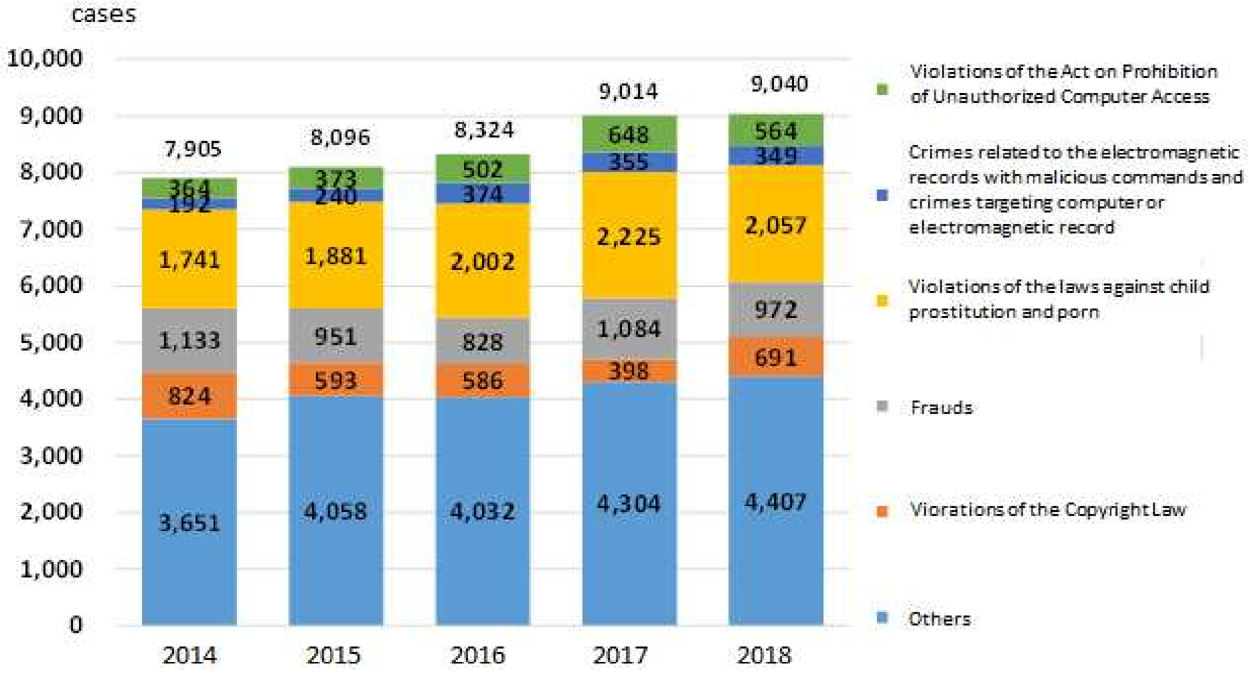

Figure 10 [Number of cleared cybercrime cases]

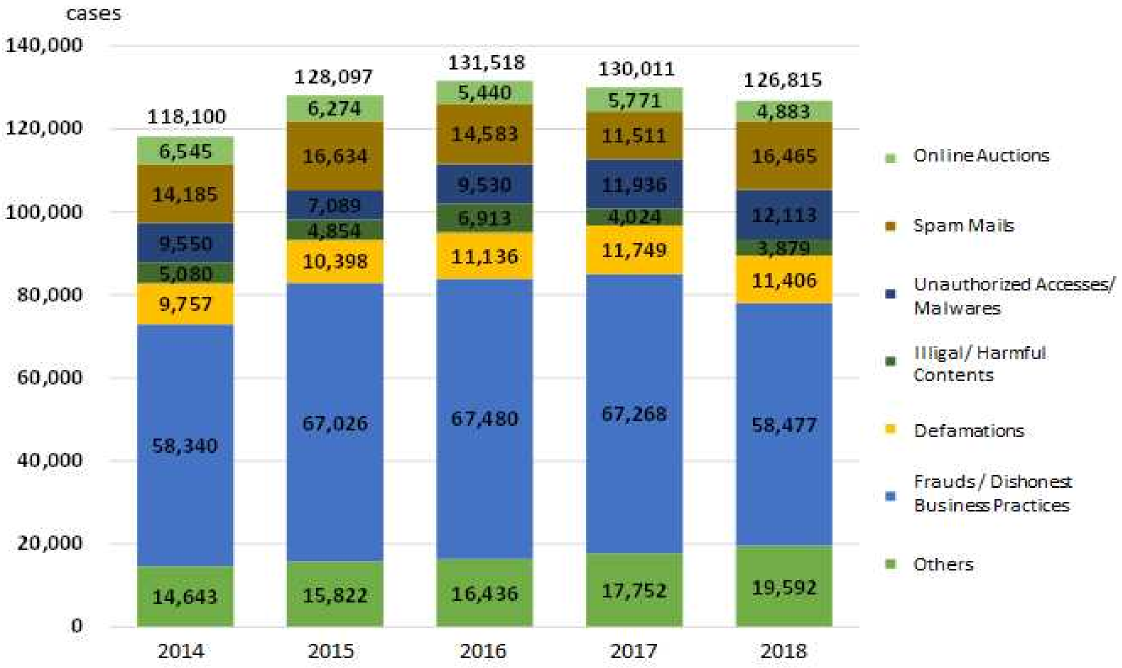

Figure 11 [Number of cybercrime-related consultations]

b. Violations of the Act on Prohibition of Unauthorized Computer Access[7]

(a) Number of the cleared cases

- Number of the cases cleared under the Act on Prohibition of Unauthorized Computer Access was 564 in 2018, declined by 84 cases from 2017, yet the 2nd highest to 2017 in the past 5 years. 502 of all the cleared cases were classified as the identification-code-abuse type[8]. Number of the arrested and/or referred individuals in 2018 was 173, down by 82 from 2017.

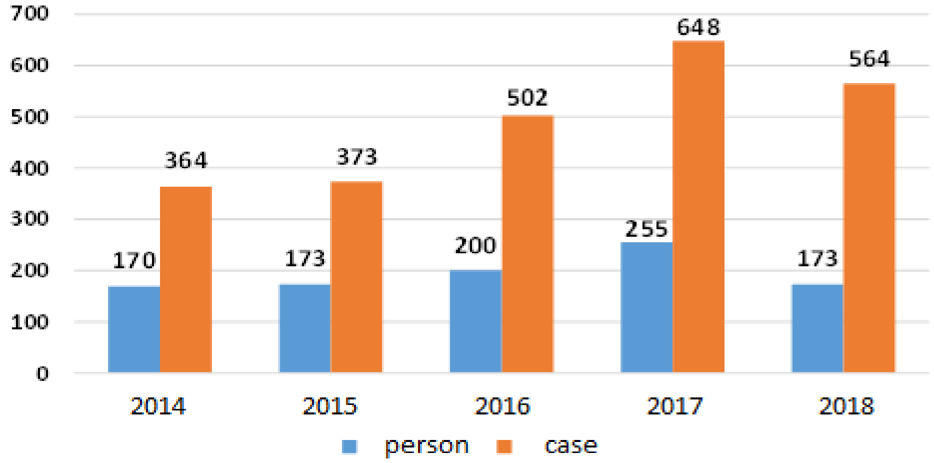

Figure 12 [Police crackdowns on unauthorized computer accesses]

- **Abuse of lax password management dominated the modus operandi**

  Dominant modus operandi of the identification-code-abuse-type of offenses in the unauthorized computer accesses was taking advantages of the users' lax password management, reaching 278 cases and occupying 55% of the total in 2018.

- **"Online gaming community websites" most abused**

  The services most abused by the suspects were the online gaming community websites, reaching 217 cases and occupying 43% of the total.

- **Diversely aged suspects**

  Ages of the suspects arrested and/or referred, and the juveniles who received guidance widely ranged from 11 to 66.

[7] The following 5 acts are defined as violations of the Act on Prohibition of Unauthorized Computer Access: 1) Acts of Unauthorized Computer Access, 2) Acts of Obtaining Someone Else's Identification Code, 3) Acts of Facilitating Unauthorized Computer Access , 4) Acts of Wrongfully Storing Someone Else's Identification Code, and 5) Acts of Illicitly Requesting the Input of Identification Codes .

[8] A type of unauthorized computer access that an offender wrongfully uses a computer by inputting someone else's identification code into a server with an access control feature via network.

(b) Online banking frauds

i. Overview

Number of the online banking fraud cases was 322 with total damage amount of approx. 461 million yen (ca. 4 million US dollars) in 2018, both on the decline.

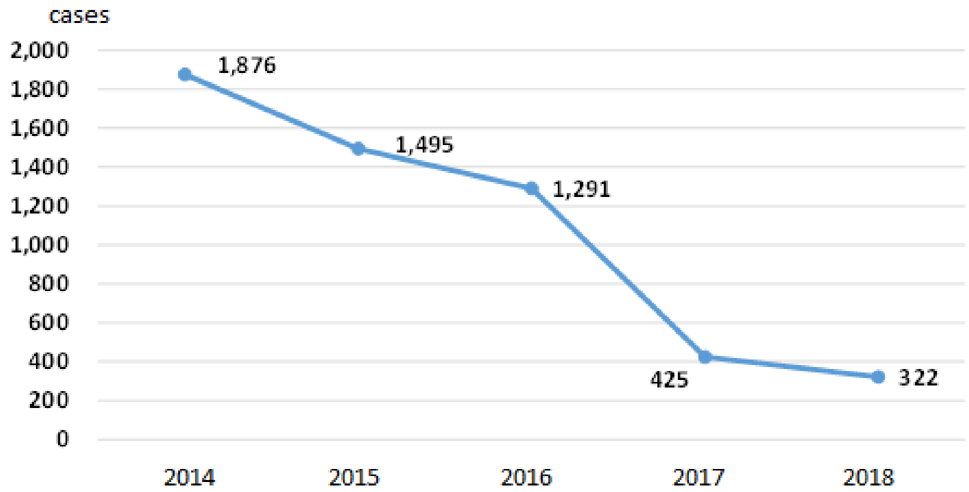

Figure 13 [Number of online banking frauds]

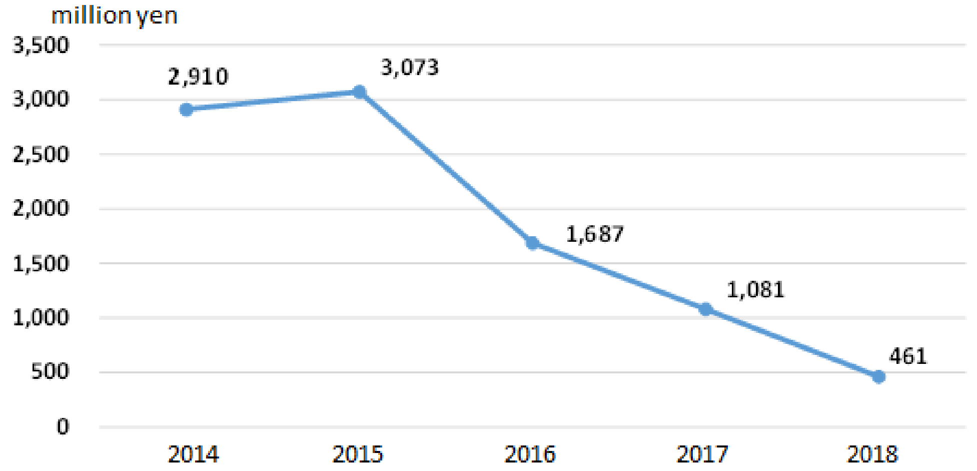

Figure 14 [Total financial damages of online banking frauds]

ii. Characteristics

- **Significant decline of damages to corporate bank accounts**

  Damages caused to the corporate accounts of the regional and Shinkin banks remarkably declined from 2017 consequent to countermeasures, e.g. enhanced monitoring[9] and adoption of the onetime-password authentications.

- **Approx. 60% of the illicit remittance destination accounts under the Vietnamese names**

  Vietnamese represented 62.8% of the holders of the 562 accounts identified as the primary destinations of the unauthorized wire transfer, followed by the Japanese (14.8%) then Chinese (13.3%).

[9] Monitoring of the IP addresses abused for illicit remittances.

(c) Unauthorized transmission of cryptoassets through unauthorized computer accesses to cryptoassets exchanges

i. Overview

- Number of the identified cases was 169, with total damage amounting to approx. 67.74 billion yen in 2018, both exceeding 149 cases and 662 million yen in 2017 by 20 cases and 67.08 billion yen.
- 2 grave cases occurred in January and September 2018, where the cryptoassets worth approx. 58 billion and 7 billion yen respectively, were illicitly remitted from the cryptoassets exchanges in Japan.

ii. Characteristics

- In 108 (63.9 %) of the identified 169 cases, the same ID's and passwords with other services had been used.

c. Crimes related to the electromagnetic records with malicious commands[10] and crimes targeting computers or electromagnetic records[11]

- **Number of the cleared cases**

  Total number of the cleared cases related to the electromagnetic records with malicious commands and crimes targeting computers or electromagnetic records in 2018 was 349, declining since 2016.

[10] Penal Code Article 168-2 (1): (Making or Providing of Electromagnetic Records with Malicious Commands), Article; 168-2 (2): (Offering for Execution of Electromagnetic Records with Malicious Commands); Article 168-3: (Obtaining or Storing of Electromagnetic Records with Malicious Commands).

[11] Penal Code Article 161-2(1) (Unauthorized Creation of Private Electromagnetic Records). Article 161-2(2) (Unauthorized Creation of Public Electromagnetic Records). Article 163-2(1) (Unauthorized Creation of Electromagnetic Records of Payment Cards). Article 234-2 (Obstruction of Business by Damaging a Computer (except cases of obstruction of business by physically damaging a computer)). Article 246-2 (Computer Fraud). Article 258 (Damaging Electromagnetic Records for Government Use). Article 259 (Damaging Electromagnetic Records for Private Use)

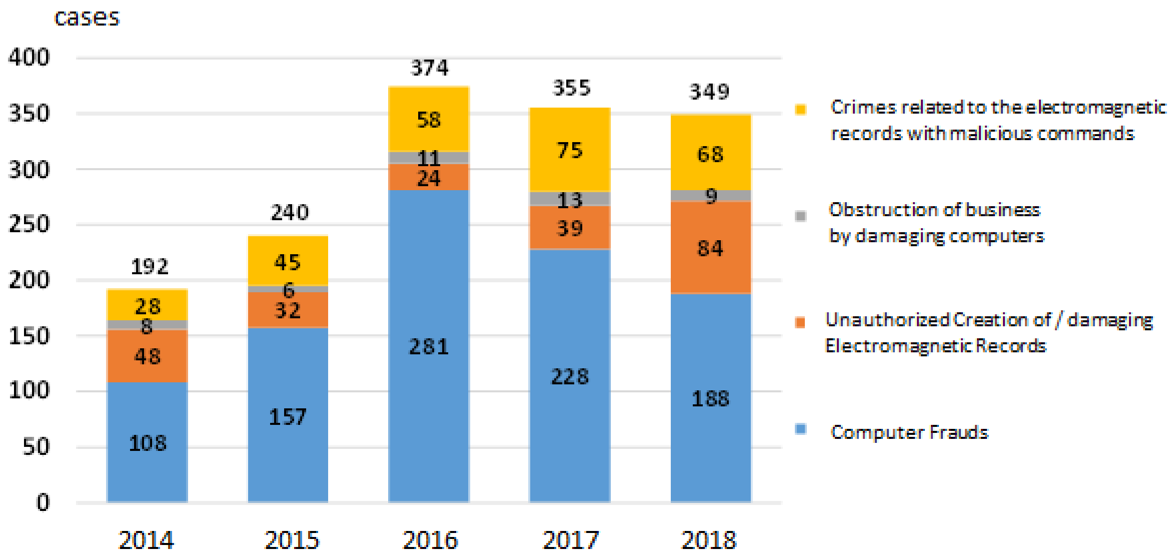

Figure 15 [Number of identified cases related to electromagnetic records with malicious commands and crimes targeting computers or electromagnetic records]

- **Crimes related to the electromagnetic records with malicious commands**
  - Number of the cleared cases related to the electromagnetic records with malicious commands in 2018 was 68, declined by 7 cases from 2017 yet the 2nd highest in the past 5 years. However, number of the cleared cases of execution of the electromagnetic records with malicious commands rose to 37, up 13 against 2017.
  - Modus operandi which executes malware to repeatedly display unjust billing messages on the PC's connected to particular websites was observed.
  - Ages of the suspects arrested and/or referred, and the juveniles who received guidance widely ranged from 10 to 58.

d. Others

- Number of the cleared violations of the Act on Punishment of Activities Relating to Child Prostitution and Child Pornography, and Protection of Children was 2,057 in 2018, outnumbering all other cybercrimes and reaching the 2nd highest to 2017 in the past 5 years.
- Number of the cleared violations of the Copyright Act in 2018 was 691, a large increase from 2017, reaching the 2nd highest to 2014 in the past 5 years.

(2) Countermeasures

- **Provision of information and request for enhanced measures to the pertinent stakeholders to effectively prevent damages of the illegal remittances**

The NPA and Prefectural Polices requested the financial institutions to enhance monitoring of their transactions, to urge use of the one-time passwords to their customers, to use the 2-path authentications[12], and to conduct strict identification of their users.

- **Countermeasures against illegal remittances of cryptoassets**

The NPA, Financial Services Agency and Consumer Affairs Agency held the trilateral director-general-level meetings in February, June and November 2018 to exchange views on issues including inspection and monitoring of the cryptoassets exchanges, measures against the unregistered operators and alarming the consumers.

- **Countermeasures against fraudulent acquisition of the account ID's in cooperation with Japan Cybercrime Control Center (JC3)**

Saitama Prefectural Police cracked down on the cases of fraudulent acquisitions of the account ID's for unlawful sale of the granted points in cooperation with the JC3, and requested the ID issuers and the online auction operators abused for the illegal ID trades to take necessary countermeasures.

Consequently, these companies tightened control on acquisition and banned sale of the account ID's, which led to decline of the fraudulent ID trades.

- **Countermeasures against travel booking scams**

Saitama Prefectural Police cracked down on the travel booking scams in which the offenders made travel reservations by abusing the unlawfully obtained other people's credit card information, and shared the related information with the travel industry in order the further damages would be prevented.

- **Countermeasures against e-commerce-related fraudulent websites**

The JC3 jointly developed the tools with the Aichi Prefectural Police to detect the fraudulent websites and provided their URL's to the APWG[13], in order the information would be shared with the pertinent businesses to prevent damages.

(End)

[12] An authentication method which requires authentication through 2 different channels, e.g. PC and smartphones, for concluding transactions. Even if one of the channels involved may be compromised to execute the fraudulent remittances, authentication requirement through another channel could reduce probability of the abuses.

[13] *A*nti-*P*hishing *W*orking *G*roup: An international nonprofit organization founded in 2003 in the United States to address the phishing scams.