Threats in Cyberspace in the First Half of 2019

1. Cyber-attacks

(1) Scanning Activities in Cyberspace

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

Number of the unexpected connection attempts detected at the sensors has risen to 3,530.8 per IP address per day in the first half of 2019, showing an upward trend.

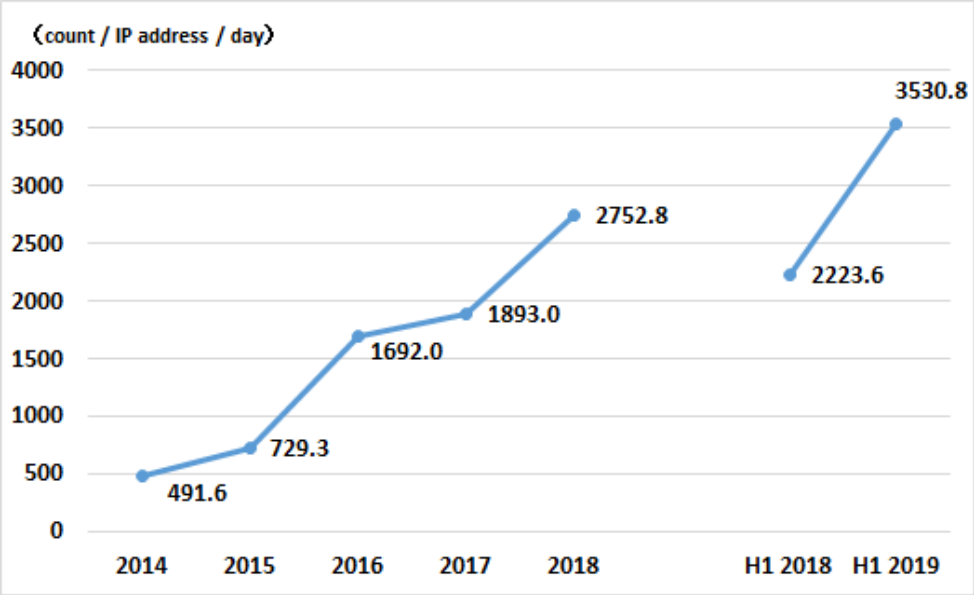

Figure 1 [Number of connection attempts detected at the sensors]

b. Characteristics

- **Connection attempts targeting vulnerabilities of IoT devices**

  Since mid-June 2019, connection attempts with the feature of the Mirai[2]-compromised bots to ports[3] 5500/TCP and 60001/TCP, which are used for foreign digital video recorders, started being observed. These include attempts to download and execute malware from external servers presumably to spread infection by exploiting vulnerabilities of the IoT devices.

---

[1] The sensors here refer to components of the Real-time Detection Network System operated around-the-clock by the NPA, placed at the Internet connection points of the police institutes throughout Japan. The NPA aggregates and analyzes the extraordinary connection data detected at these sensors including scanning attempts for diverse cyber-attacks.

[2] Malware targeting to compromise the IoT device.

[3] 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 65535 is assigned to each port.

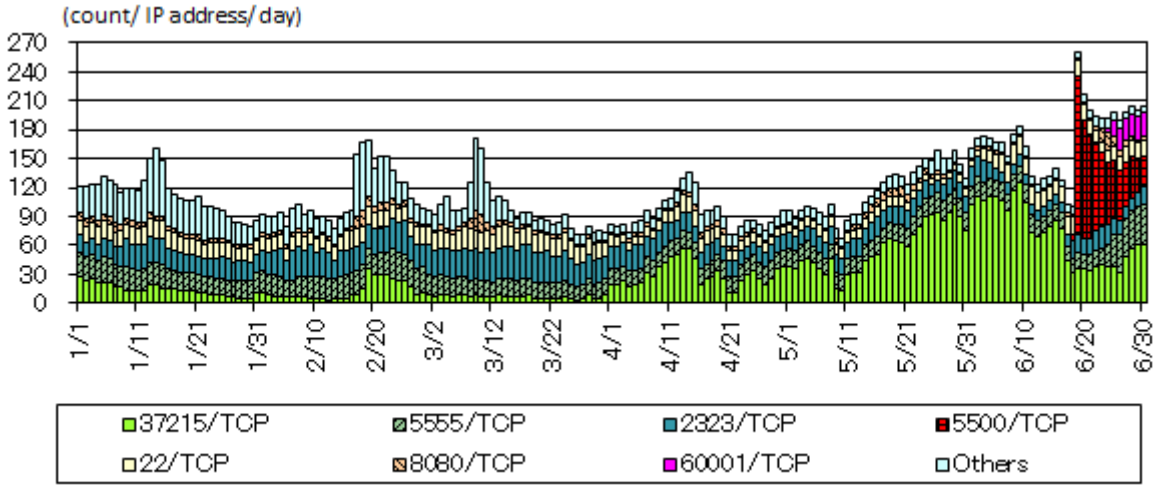

Figure 2 [Connection attempts with Mirai bots' feature by destination port (except port 23/TCP)]

- **Surge of connection attempts targeting Remote Desktop services** [*4]

  From early January to mid-February and from late March to late May, a surge of connection attempts to wide range of ports targeting the Remote Desktop services used for remote control of the Microsoft Windows was observed.

  In mid-May, Microsoft released the urgent update patches to fix the exploitable vulnerabilities. They may be abused to take over the administrative privileges to remotely execute arbitrary commands.

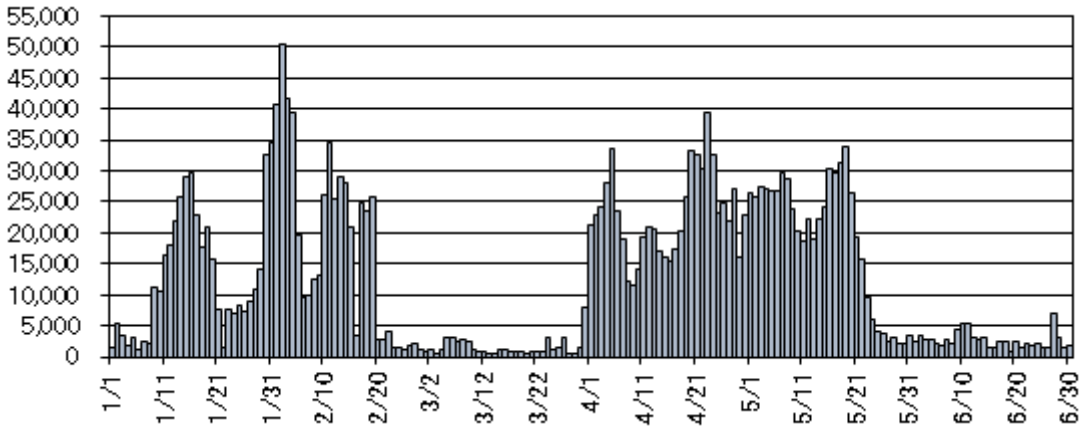

Figure 3 [Connection attempts to wide range of ports targeting Remote Desktop Services]

*4 Services used for remote monitoring and control of the desktop environments of computers, such as those placed in the workplaces, by computers placed in other locations. The function is used to enable remote working.

(2) Cyberattack Status and Countermeasures

a. Status

(a) Overview

Through the Counter Cyber-intelligence Information-Sharing Network[5], the Japanese police share information of cyberattacks which appear to aim at stealing data, conduct comprehensive analysis of the aggregated information and provide the feedback to business operators and pertinent organizations.

Number of the spear phishing e-mail attacks[6] identified by the Japanese police through the Network in the first half of 2019 was 2,687, increasing from that of the first half of 2018.

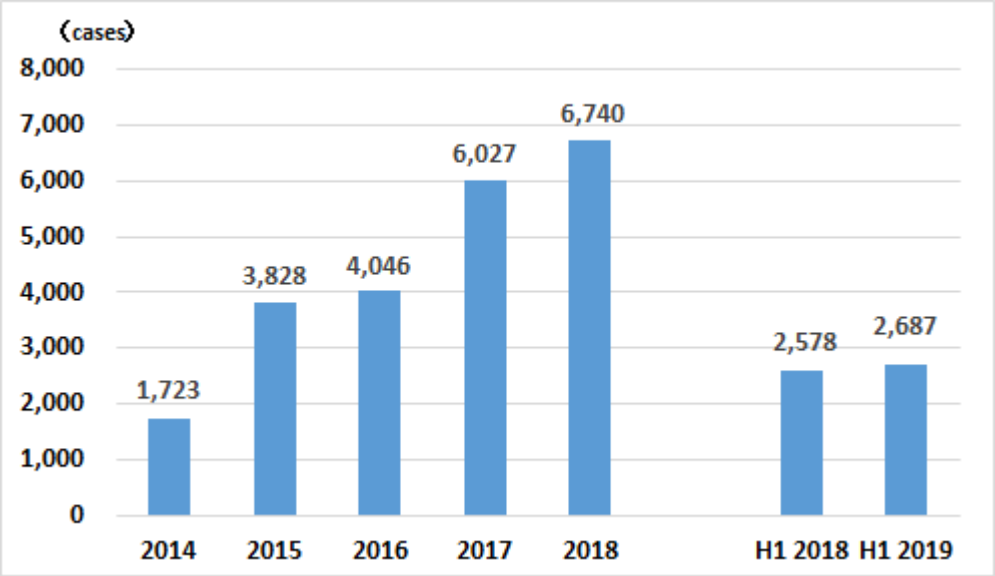

Figure 4 [Number of spear phishing e-mail attacks]

[5] A nationwide network which consists of the police and approximately 8,100 pertinent organizations (as of July 2019) with 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 email attacks against the governmental entities through this network in coordination with the National Center of Incident-readiness and Strategy for Cybersecurity (NISC)

[6] The NPA defines the "spear phishing e-mail attacks" as malicious attempts to infect other computers to steal data by sending the disguised business e-mails with/attaching malware undetectable by the commercial anti-virus software.

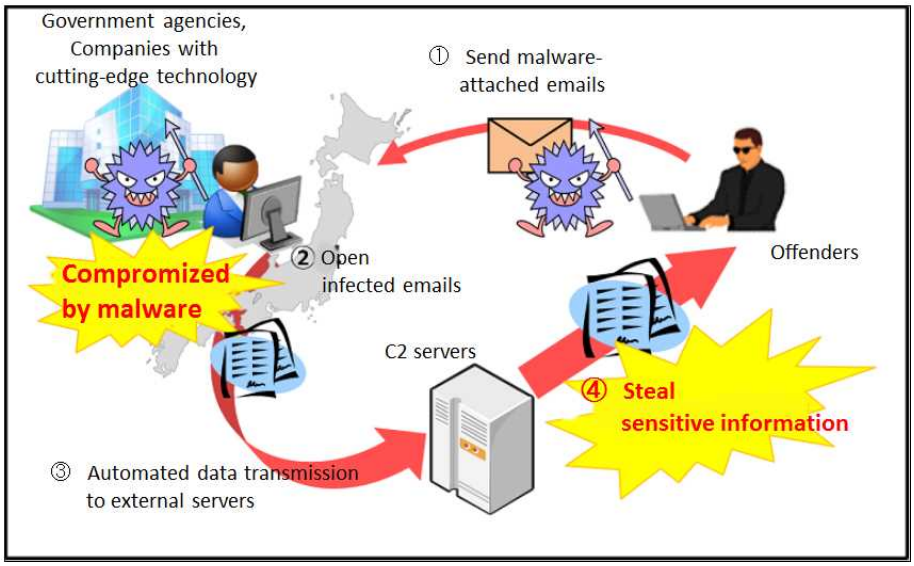

Figure 5 [Mechanism of spear phishing email attacks]

Browsing failures of websites of a Japanese public transport and a museum were observed in the first half of 2019, as in 2018.

The Japanese police confirmed that a party who claimed to be an international hacker group "Anonymous" posted on the social media the apparent claims of responsibility for cyber-attacks conducted against 3 organizations in Japan.

(b) Modus operandi of spear phishing email attacks

- **Continuous rash of 'indiscriminate'[7] spear phishing email attacks**

High level occurrence of 'indiscriminate' spear phishing email attacks continued, accounting for 85% of the total spear phishing email attacks.

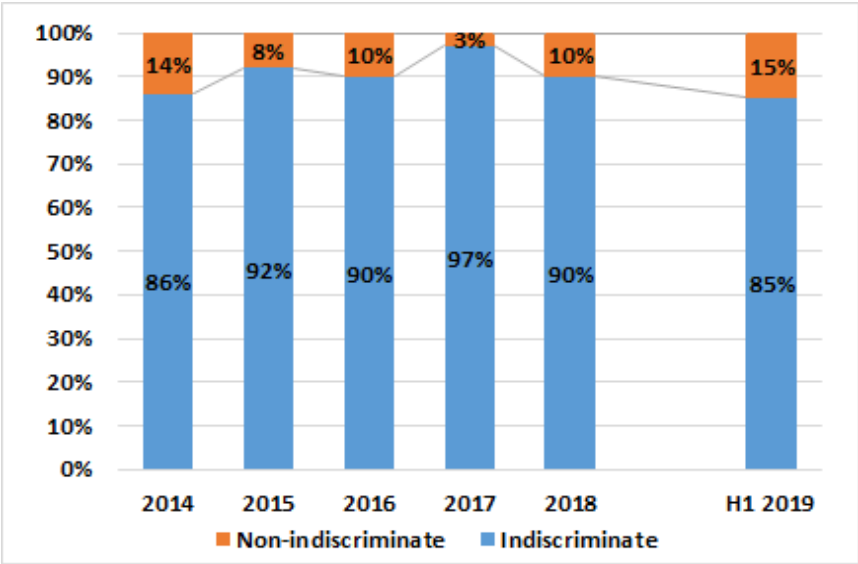

Figure 6 [Ratio of 'indiscriminate' and other types of spear phishing email attacks]

[7] The NPA tallies the spear phishing email attacks which send out emails with the same text or malware to 10 or more destinations as the 'indiscriminate' attacks.

- **Most spear phishing emails target undisclosed email addresses**

82 % (of the entire spear phishing emails) targeted the undisclosed email addresses.

- **Most originating addresses (of spear phishing emails) forged**

90% of the originating addresses of the spear phishing emails appeared to be forged.

- **Changing attachment types (of the spear phishing e-mails)**

Ratios of the MS-Word and Excel files, which accounted for approx. 70% of the attachments to the spear phishing emails in the first half of 2018, have declined, while ratio of the compressed attachments has increased in the first half of 2019.

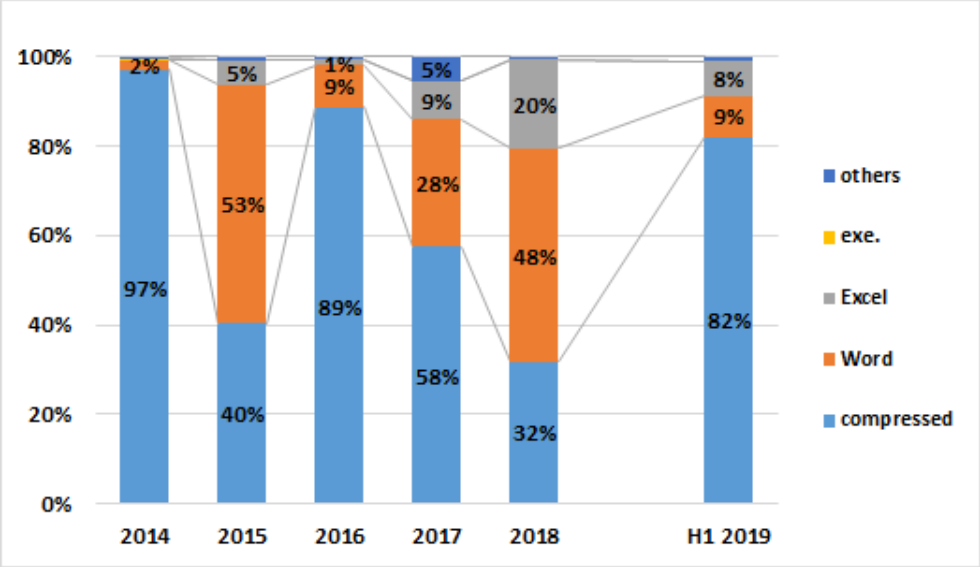

Figure 7 [Ratios of the spear phishing emails' attachment types]

Among the compressed attachments to the spear phishing emails, ratio of the script files[8], which was more than 50% in 2016 and 2017, has resurged in the first half of 2019.

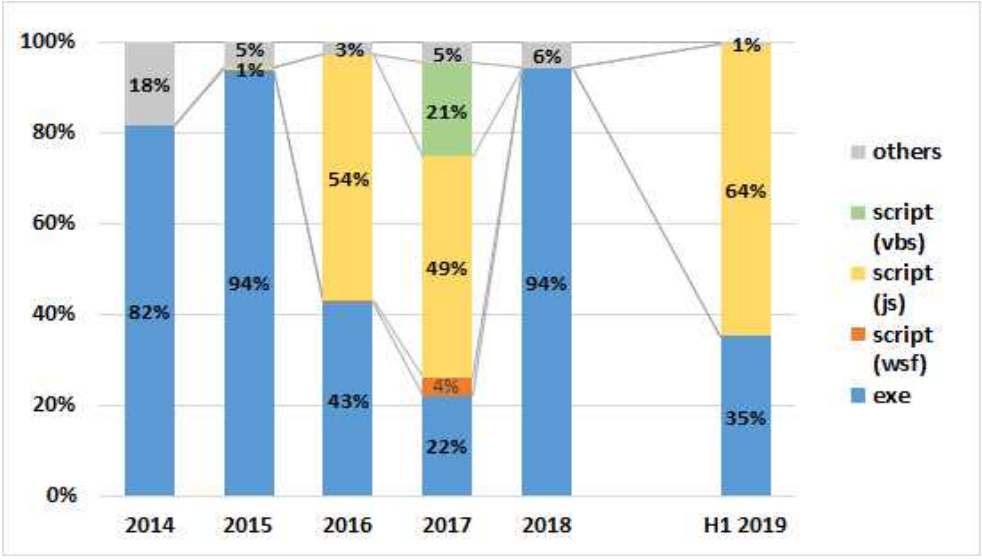

Figure 8 [Ratios of compressed attachment types to spear phishing emails]

[8] The script files here refer to the files written in simple programing languages (scripts). This file type is occasionally abused to induce download of the malicious executable files.

Countering the spear phishing email attacks requires continuous monitoring of their trends as their modus operandi appear to be constantly changing.

○ Case Examples:

・Emails disguised as order confirmations to falsely induce opening of the attachments were sent to the undisclosed email accounts of the businesses.

・Emails with compressed attachments disguised as international affairs reports to falsely induce decompressing and opening of them were sent from the forged originating addresses to email accounts of the businesses.

b. Countermeasures

(a) Council for Countermeasures against Cyber Terrorism

The Council consists of the prefectural police departments and pertinent organizations including major critical infrastructure operators, providing opportunities for the police to visit the companies to share insights on the threat of cyber-attacks and on information security. The Council also strives to enhance the emergency response capability by exercising joint drills simulating occurrence of the cyber-attacks.

(b) Takedowns of C2 Servers[9] Used for Cyber-attacks

The Japanese police have been encouraging the server hosting services to take down the C2 servers in Japan, which had been identified through malware analysis as abused for cyber-attacks. In this endeavor, one C2 server was disabled in the first half of 2019.

(c) Promotion of Countermeasures against Cyber-attacks toward Tokyo 2020 Olympic and Paralympic Games

In preparation for the Tokyo 2020 Olympic and Paralympic Games, the Japanese police have promoted diverse measures against cyber-attacks including the joint drills with the pertinent organizations simulating occurrence of the cyber-attacks and information exchange with the pertinent foreign authorities.

[9] 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 malware-compromised computers.

2. Cybercrimes

(1) Cybercrimes crackdown

a. Number of cleared cybercrime cases

Number of the cleared cybercrime cases has been on the rise, reaching 4,243 in the first half of 2019, almost equivalent to that of the first half of 2018.

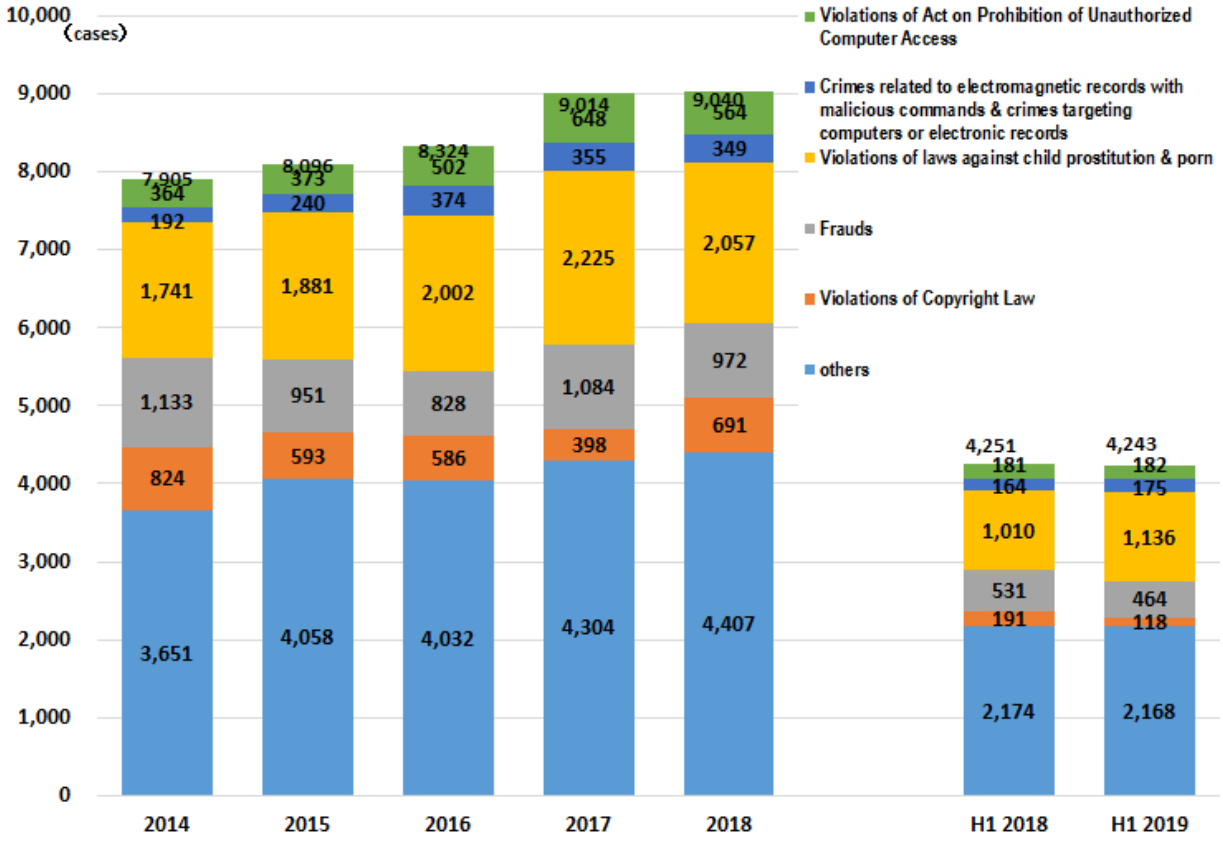

Figure 9 [Number of cleared cybercrime cases]

b. Violations of the Act on Prohibition of Unauthorized Computer Access[10]

(a) Number of cleared cases

- Number of the cleared cases of violations of the Act on Prohibition of Unauthorized Computer Access was 182 in the first half of 2019, almost equivalent to that of the first half of 2018. 159 of all the cleared cases were classified as the identification-code-abuse type[11] and accounted for approx. 87.4% of the total.

[10] 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 .

[11] A type of unauthorized computer access in which the offenders wrongfully input the other persons' identification codes via networks into the access-controlled servers.

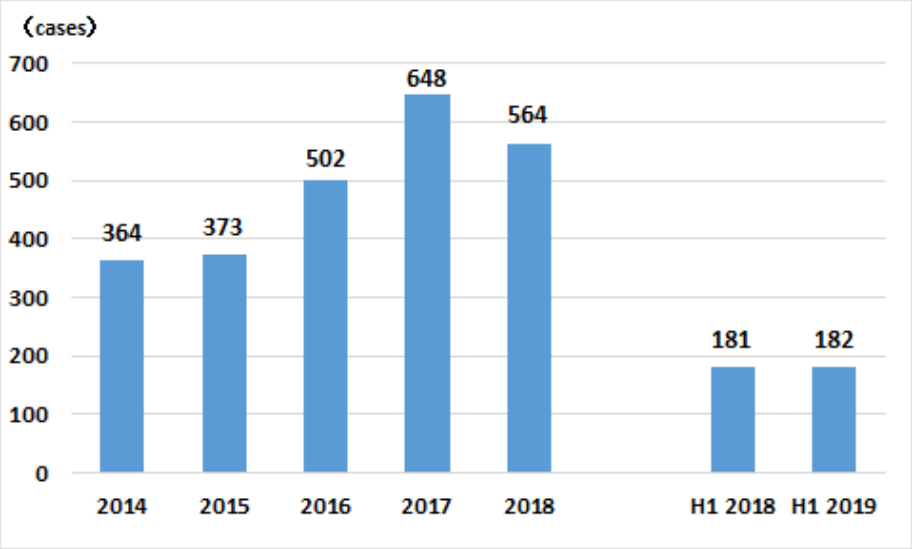

Figure 10 [Number of cleared violations of unauthorized computer access]

- **Identification codes most abused by those in positions to learn of them e.g. ex-employees or acquaintances**

  The most dominant method of identification code abuse in unauthorized computer access was abuse by those in positions to learn of them e.g. the ex-employees or acquaintances, which accounted for 37 cases and 23.3% of the total, followed by abuse of the codes obtained from others, which accounted for 28 cases and 17.6% of the total.

- **Members/employees-only websites most abused**

  The most abused service was the employees/members-only websites, reaching 37 cases and occupying approximately 23.3% of the total, followed by the online game community sites, accounting for 34 cases and approximately 21.4% of the total.

(b) Internet banking frauds

- **Overview**

  Number of the internet banking fraud cases in the first half of 2019 was 182 with total loss of approximately 165 million yen, both declined compared to that of the first half of 2018.

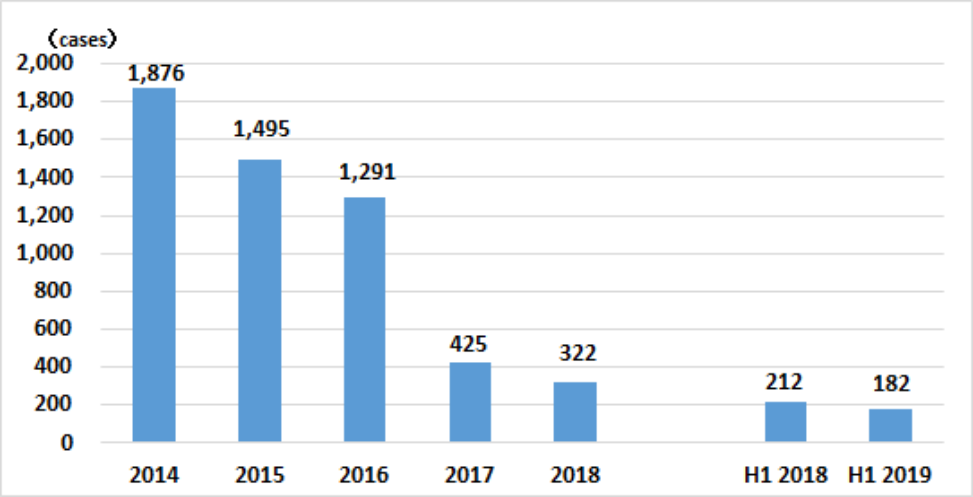

Figure 11 [Number of internet banking fraud]

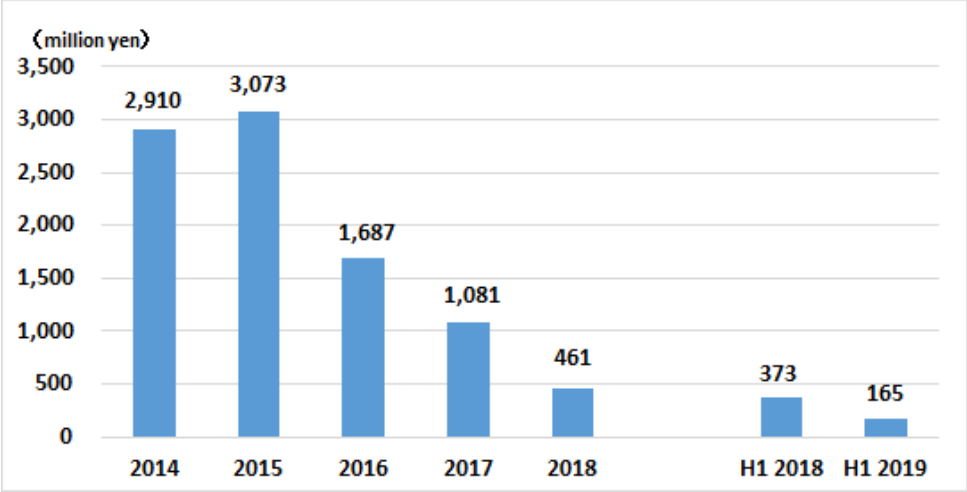

Figure 12 [Total loss of internet banking fraud]

- **Characteristics**

Due to countermeasures e.g. enhanced monitoring[12] and adoption of the onetime-password authentications, number and loss of the internet banking frauds have both been on the decline since 2016. In the first half of 2019, as to the nationalities of the holders of the 194 accounts identified as the primary destinations of illicit remittances, 44.3 were Vietnamese, followed by Japanese (15.5%) then Chinese (11.9%).

(c) Illicit cryptoassets transmission through unauthorized computer access to cryptoassets exchanges

Number of the detected illicit cryptoasset transmissions through unauthorized computer access to cryptoassets exchanges in the first half of 2019 was 9, with total loss of approx. 1.21 million yen, both remarkably declined compared to those of the first half of 2018. In

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

the first half of 2018, number of the detected illicit cryptoasset transmissions was 158 cases, with total loss of approx. 60.5 billion yen.

While the cryptoassets exchanges have been taking protective measures, caution is still required as suspected illegal transmissions of cryptoassets equivalent of approx. 3 billion yen from a cryptoassets exchange in Japan occurred in July 2019.

c. Crimes related to electromagnetic records with malicious commands[13] and crimes targeting computers or electromagnetic records[14]

- **Number of cleared cases**

Total number of the cleared cases related to the electromagnetic records with malicious commands and crimes targeting computers or electromagnetic records in the first half of 2019 was 175, increasing from that of the first half of 2018.

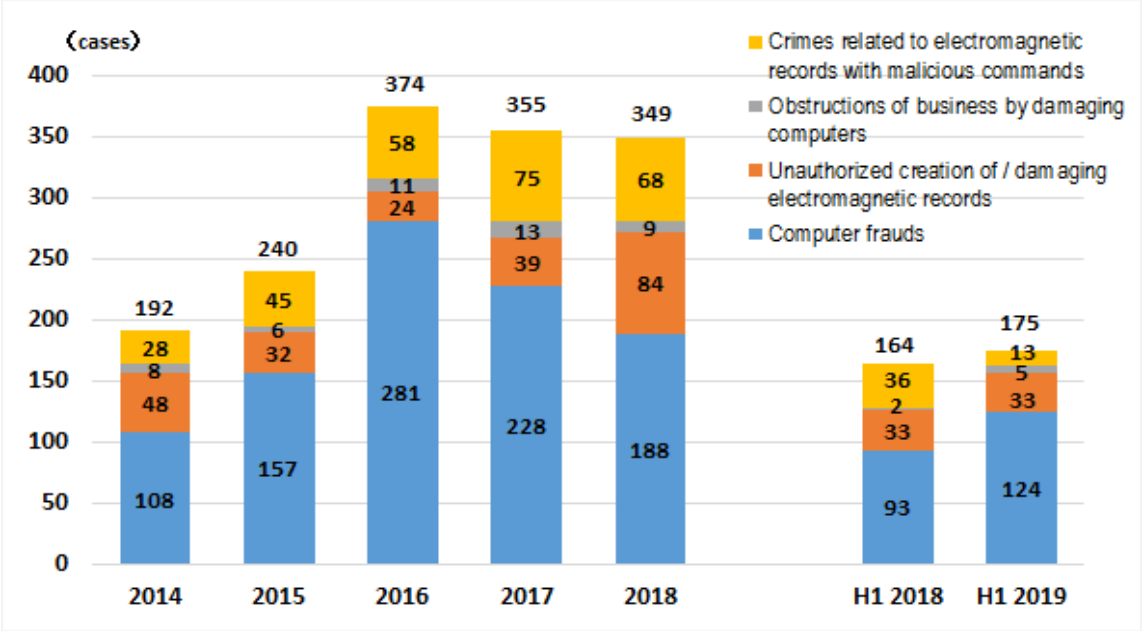

Figure 13 [Number of cleared cases related to electromagnetic records with malicious commands and crimes targeting computers or electromagnetic records]

[13] 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).

[14] 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)

- **Characteristics**

The most dominant crime type among the cleared cases in this category was the computer fraud, reaching 124 cases and 70.9% of the total.

d. Others

- Number of the cleared cases of violations of the Act on Punishment of Activities Relating to Child Prostitution and Child Pornography, and Protection of Children in the first half of 2019 was 1,136, increasing from that of the first half of 2018.
- Number of the cleared cases of violations of the Copyright Act in the first half of 2019 was 118, decreasing from that of the first half of 2018.

(2) Countermeasures

- **Prevention of internet banking fraud**

In response to occurrence of the illegal remittance by abuse of repetitious and massive purchase of the prepaid cards, the police requested the financial institutions to enhance preventive measures e.g. monitoring of their transactions and setting limits to the number of daily purchases.

- **Prevention of SMS Phishing**

The police implemented an awareness-raising campaign with the Japan Cybercrime Control Center (JC3) on the SMS phishing methods e.g. forging of the originating numbers, insertion of the scam text and URL's into the same threads with the authentic carriers', or impersonating SMS messages from the courier companies with misleading scam URL's to steal the victims' phone numbers and authentication codes in order to create the cashless payment accounts; and preventive measures e.g. confirming authenticity of the URL's sent via SMS.

- **Countermeasures for e-commerce scam websites with JC3**

The police implement preventive measures by utilizing the tools jointly developed by the Aichi Prefectural Police and the JC3 to report the scam website URL's detected by the JC3 to the pertinent organizations including the APWG[15].

(End)

[15] *Anti-Phishing Working Group*: An international nonprofit organization founded in 2003 in the United States to address the phishing scams.