Threats in Cyberspace in 2019

Circumstances surrounding threats in cyberspace remain critical.

The number of cybercrimes cleared by the Japanese police has reached a record high. Online banking fraud had been declining both in the number of incidents and loss since 2016, consequent to the measures taken by the financial institutions including security enhancement. However, the number of incidents and loss of the online banking fraud have largely resurged since September 2019 compared to 2018. Besides, cybercrimes relevant to the citizens such as abuse of the 'QR code payment' have been confirmed[1].

[Ref]

According to the online survey conducted by the National Police Agency (NPA) of Japan in September 2019 to the respondents whose composition was allocated by age, gender and residential location in line with the 2015 census, 28.9% (2,888 respondents) have experienced potential damage from cybercrime in the preceding 1 year, and 13.7% (1,373 respondents) have experienced damage from cybercrime in the same period.

Cyberattack also remains rife. While cyberattack targeting the anti-doping organizations and Australia's Federal Parliament took place outside Japan, access to the websites of local governments and the private businesses in Japan were jammed, presumably attributable to a transnational hacker group. Additionally, a major electronics company announced that they had had unauthorized access which potentially led to the data leak. The number of suspicious connection attempts detected by the NPA as apparent scanning activities has also been on the rise.

In order to address such threats in cyberspace, the Japanese police have been promoting effective measures by utilizing its comprehensive capacity. Particularly in 2020, expecting the Tokyo Olympic and Paralympic Games (hereafter 'the Tokyo Games'), the police have been consolidating cooperation with the government and private sector partners to ascertain security and smooth implementation of the event through collecting and analyzing cyberattack intelligence, sharing information about the Tokyo Games' operation, as well as conducting the joint drills.

[1] Cashless payment method using barcode or QR code (registered brand of Denso Wave Incorporated)

1. Cyberattack

(1) Major Cyberattack Incidents

○ Cyberattack targeting Australian Federal Parliament & political parties

February 2019: Australia's Prime Minister Scott Morrison confirmed at the House of Representatives that the Australian Parliament House and 3 major political parties were struck by cyberattack possibly conducted by state actors. Although the details of damage were not publicized, the computer networks of Liberal, Labor and National parties were reportedly under attack.

○ Designation of North Korean hacker groups as subjects of sanctions

September 2019: The U.S. Department of Treasury's OFAC (Office of Foreign Assets Control) designated 3 North Korean state-sponsored hacker groups "Lazarus", "Bluenoroff" and "Andariel" as subjects of sanctions to freeze their assets held under U.S. jurisdiction for their involvement in the "WannaCry" ransomware attack.

○ Report to U.N. Security Council North Korea sanctions committee

September 2019: The Panel of Experts submitted a report to the United Nations Security Council North Korea sanctions committee on allegation that North Korea had used cyberattack targeting financial institutions and cryptoasset (cryptocurrency) exchanges to illicitly raise fund estimated to be 2 billion U.S. dollars for its WMD (weapons of mass destruction) development programs.

○ Cyberattacks targeting anti-doping organizations

October 2019: Microsoft announced that at least 16 sporting and anti-doping organizations had been targeted in the cyberattack by the hacker group "Strontium", also known as "Fancy Bear" or "APT28", since September 16.

○ Unauthorized access targeting major Japanese electronics company

January 2020: A major Japanese electronics company announced that investigation of the suspicious behaviors detected on their internal terminals in June 2019 disclosed that the data they held had been transmitted to the outside as a result of unauthorized access by a third party.

○ Access to Japanese websites jammed

Access to websites of 8 Japanese organizations including the local governments and private businesses were jammed. The police observed that apparent claims of responsibility for cyberattack targeting the Japanese organizations had been posted on the social media by the self-proclaimed members of an international hacker group "Anonymous".

Besides the above incidents, diverse cyberattacks have been observed both domestically and internationally, including unauthorized access to another Japanese electronics company's internal servers, which was announced in 2020. Occurrence of cyberattacks on a global scale remains an issue of concern.

(2) Scanning Activities in Cyberspace

a. Overview of the unexpected connection attempts detected at the sensors[2]

The number of unexpected connection attempts detected at the sensors has risen to 4,192 per IP address per day in 2019, showing an upward trend.

[2] 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.

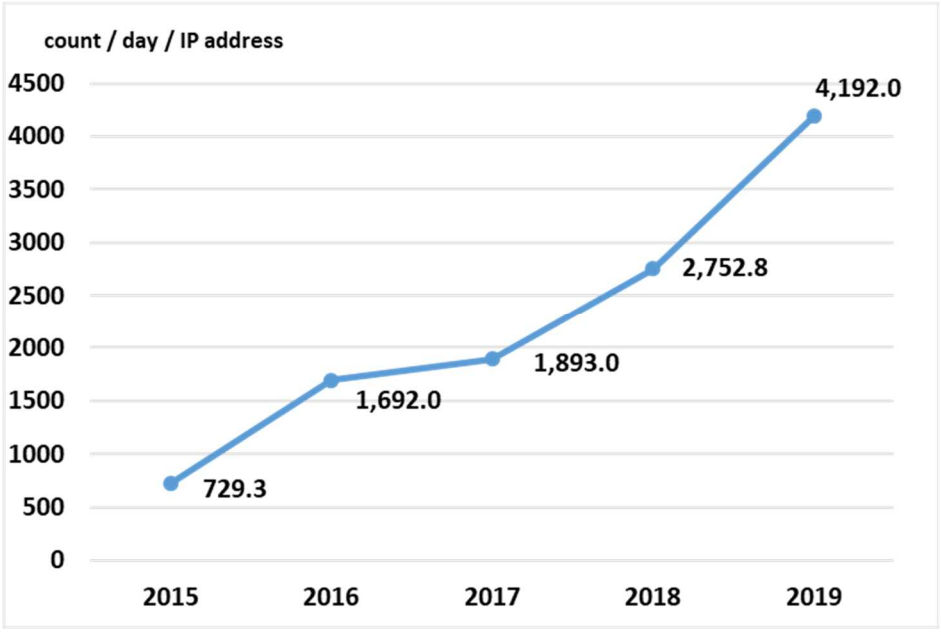

Figure 1 [Number of unexpected connection attempts detected at the sensors]

b. Characteristics

- **Connection attempts with features of the Mirai-compromised bots**

Connection attempts with features of the Mirai-compromised bots have increased throughout 2019. Since mid-June 2019, the connection attempts started targeting the ports which had not been markedly targeted before, including the ports used for devices known for their vulnerabilities. Such connection attempts are presumed intended to expand infection among the devices taking no security measures.

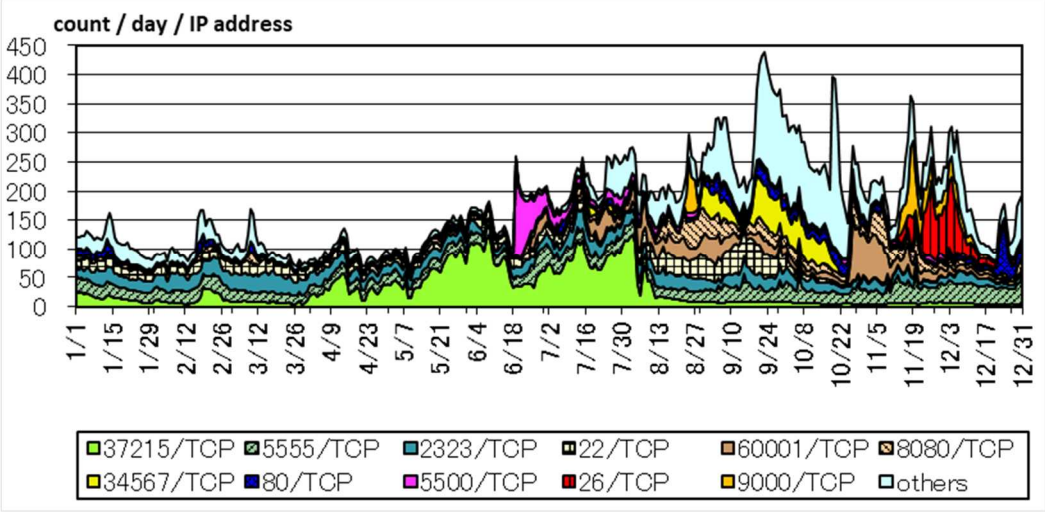

Figure 2 [Connection attempts with features of Mirai-compromised bots by destination port (except port 23/TCP)]

- **Surge of connection attempts targeting Remote Desktop services** [*3]

A surge of connection attempts to remote control services, which are provided by Microsoft Windows as the Remote Desktop services, was observed from early January to mid-February, from late March to late May, and in early December in 2019. Especially, connection attempts to a wide range of ports including the default port for the Remote Desktop services: 3389/TCP were observed in the first half of 2019.

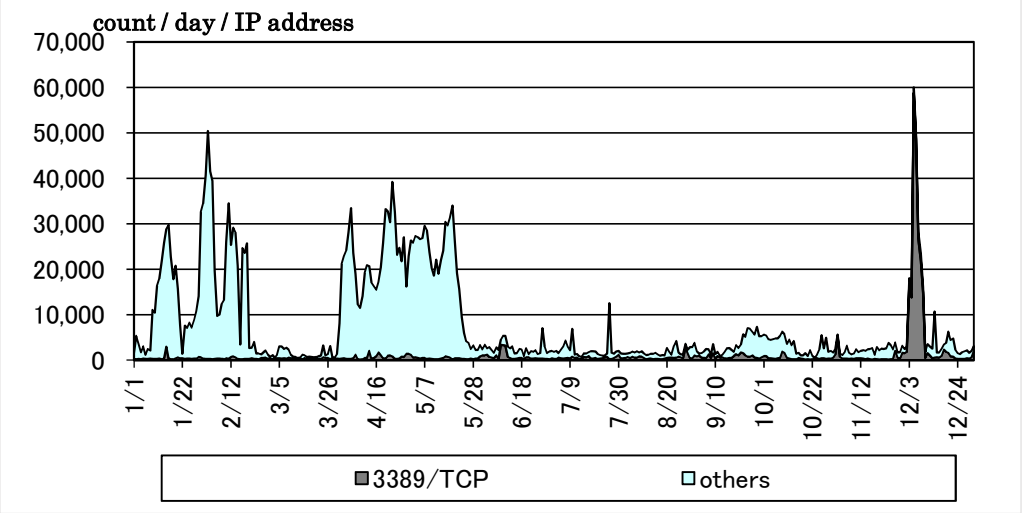

Figure 3 [Connection attempts to a wide range of ports for targeting the Remote Desktop services]

With regards to the Remote Desktop services, Microsoft released the urgent patches for the vulnerabilities in mid-May. These vulnerabilities could be exploited to take over the administrator privilege for remote execution of any commands. Security measures should be taken by applying the patches to the vulnerabilities.

*3 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.

(3) Spear Phishing Attack

a. The number of spear phishing attack

The number of spear phishing attack[4] identified by the Japanese police through the Counter Cyber-intelligence Information-Sharing Network[5] in 2019 was 5,301.

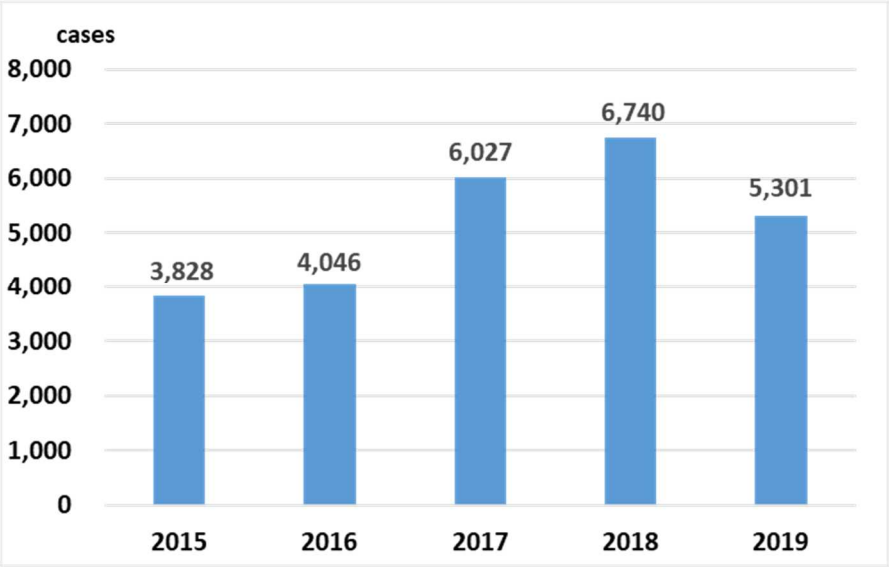

Figure 4 [Number of spear phishing attacks]

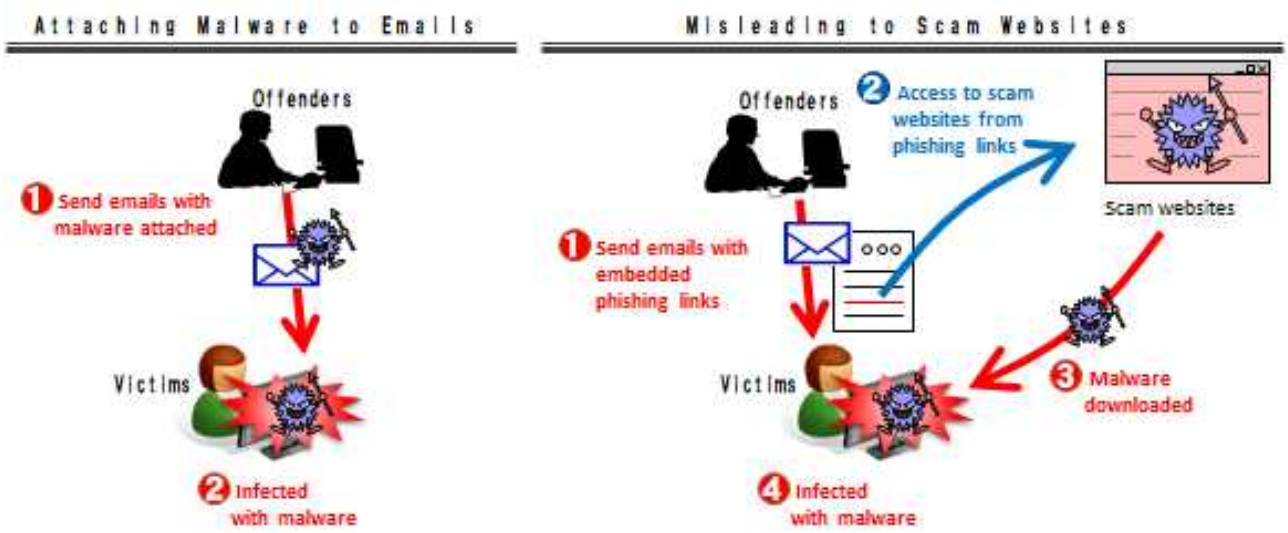

Figure 5 [Sample scheme of malware infection]

b. Modus operandi of spear phishing attacks

- **Continuous rash of 'indiscriminate'[6] spear phishing attacks**

High level occurrence of 'indiscriminate' spear phishing attacks continued, accounting

---

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

[5] A nationwide network which consists of the police and approximately 8,100 pertinent organizations (as of January 2020) 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 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 tallies the spear phishing attacks which send out emails with the same text or malware to 10 or more destinations as the 'indiscriminate' attacks.

for 90% of the total spear phishing attacks.

- **Spear phishing emails targeting the undisclosed email addresses**

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

- **Forged originating email addresses of the spear phishing emails**

  92% of the originating email addresses of the spear phishing emails appeared to have been forged.

- **Shift in attachment types of the spear phishing emails**

  The following charts show composition of the overall file types attached to the spear phishing emails, and composition of the compressed attachments.

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

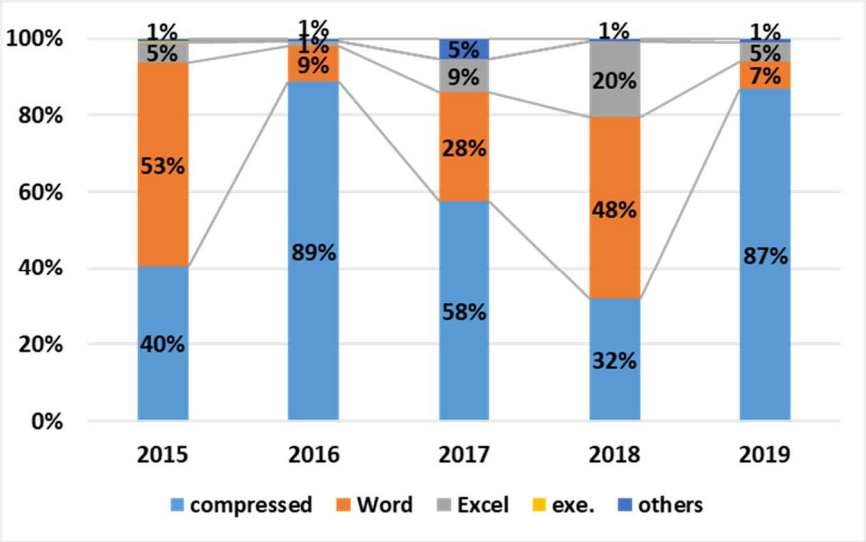

Figure 6 [Composition of attachments to spear phishing emails]

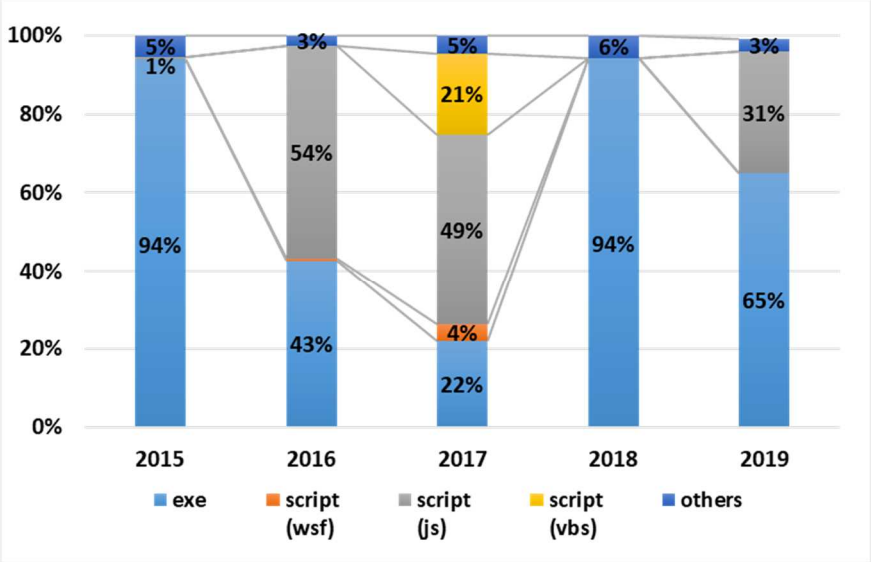

Figure 7 [Composition of compressed attachments to spear phishing emails]

c. Case Examples

The followings are examples of the spear phishing emails obtained through the Counter Cyber-intelligence Information-Sharing Network:

- Emails titled “Invitation to the Health & Safety Committee” sent to the undisclosed business email addresses to mislead the recipients to open the compressed attachments.

・ Emails titled “Bonus Payment Notice” sent to the undisclosed business email addresses to mislead the recipients to access the links embedded in the content.

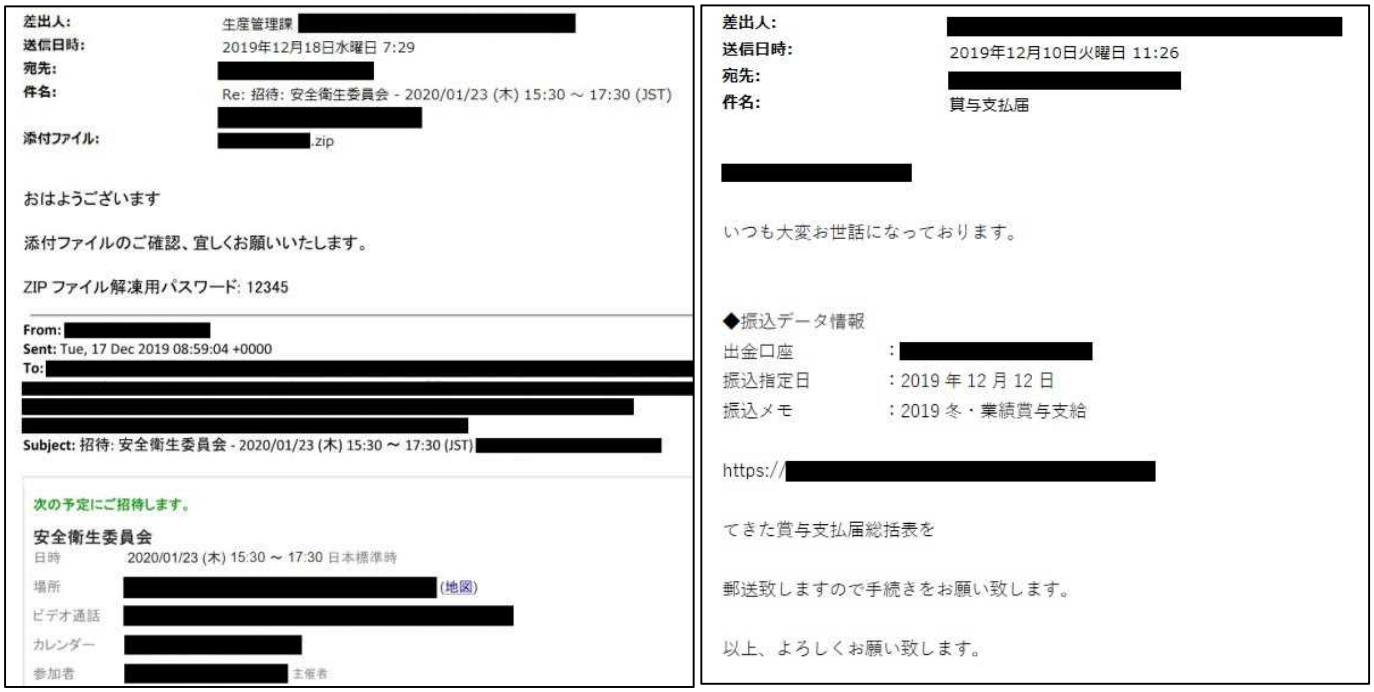

Figure 8 [Spear Phishing Emails Sent to Businesses]

(4) Countermeasures

a. Counter Cyber-intelligence Information-Sharing Network

The Japanese police conduct comprehensive analysis of the information provided by the private sector partners on suspected cyberattacks for data theft, and provide the results to businesses through the Counter Cyber-intelligence Information-Sharing Network.

b. Takedown of C2 Servers[7] Used for Cyberattack

The Japanese police have been encouraging the server hosting operators to take down the C2 servers in Japan, which were identified as abused for cyberattack through the malware analysis. The police have taken the nullification measures of these servers such as requesting the hosting operators to delete the stored malicious contents. In this endeavor, 16 C2 servers were disabled in 2019.

c. Promotion of Countermeasures against Cyberattack toward the Tokyo 2020 Olympic and Paralympic Games

In 2019, the Japanese police took preventive measures against cyberattack to secure implementation of the G20 Osaka Summit and the 2019 Rugby World Cup, and observed no hindrance to these events. Nevertheless, occurrence of cyberattack to disrupt or steal data related to the Tokyo Games is concerned, considered the past occurrence of cyberattack.

In preparation for the Tokyo Games, the Japanese police have been engaged in prevention of damage

[7] 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.

from cyberattack in cooperation with the critical infrastructure operators, the Tokyo Olympics and Paralympics Organizing Committee, stadiums and other stakeholders. The police also share the cyberthreat information with businesses to develop a collaboration network to address the cyberattack, provide necessary advice on each business operator's system, and implement joint drills simulating occurrence of cyberattack to enhance the incident response capacity.

○ **Joint Preparation for the Tokyo Games**

- January 2019: Conducted a joint technical drill simulating response to cyberattack incident with the critical infrastructure operators in Tokyo.
- September 2019: Conducted a cyber incident response drill with official partner companies of the Tokyo Games.
- November 2019: Conducted a joint response drill simulating cyberattack incidents with stakeholder companies of the Tokyo Games.

The Japanese police will continue to promote coordination and confirmation with the stakeholder organizations to ensure the safe and smooth implementation of the Tokyo Games.

2. Cybercrime

(1) Cybercrime Status

Major points of cybercrime confirmed in 2019 are as follows:

- **Illicit remittance via online banking**

  Both the number and loss of the illicit remittance via online banking, which had been on the decline since 2016 due to the enhanced security measures of the financial institutions, have surged again since September 2019.

- **Abuse of 'QR code payment'**

  Abuse of 'QR code payment' accounts or credit card data for mass purchase of goods in outlets such as the convenience stores has been observed.

- **'Emotet' infection**

  Infection of malware called 'Emotet', which steals the email destinations and content data sent by the computer users, to spread infection by generating and transmitting the fraudulent emails, was confirmed.

(2) Cybercrime crackdown

a. The number of cleared cybercrime cases

The number of cleared cybercrime cases has been on the rise, reaching a record high of 9,519 in 2019.

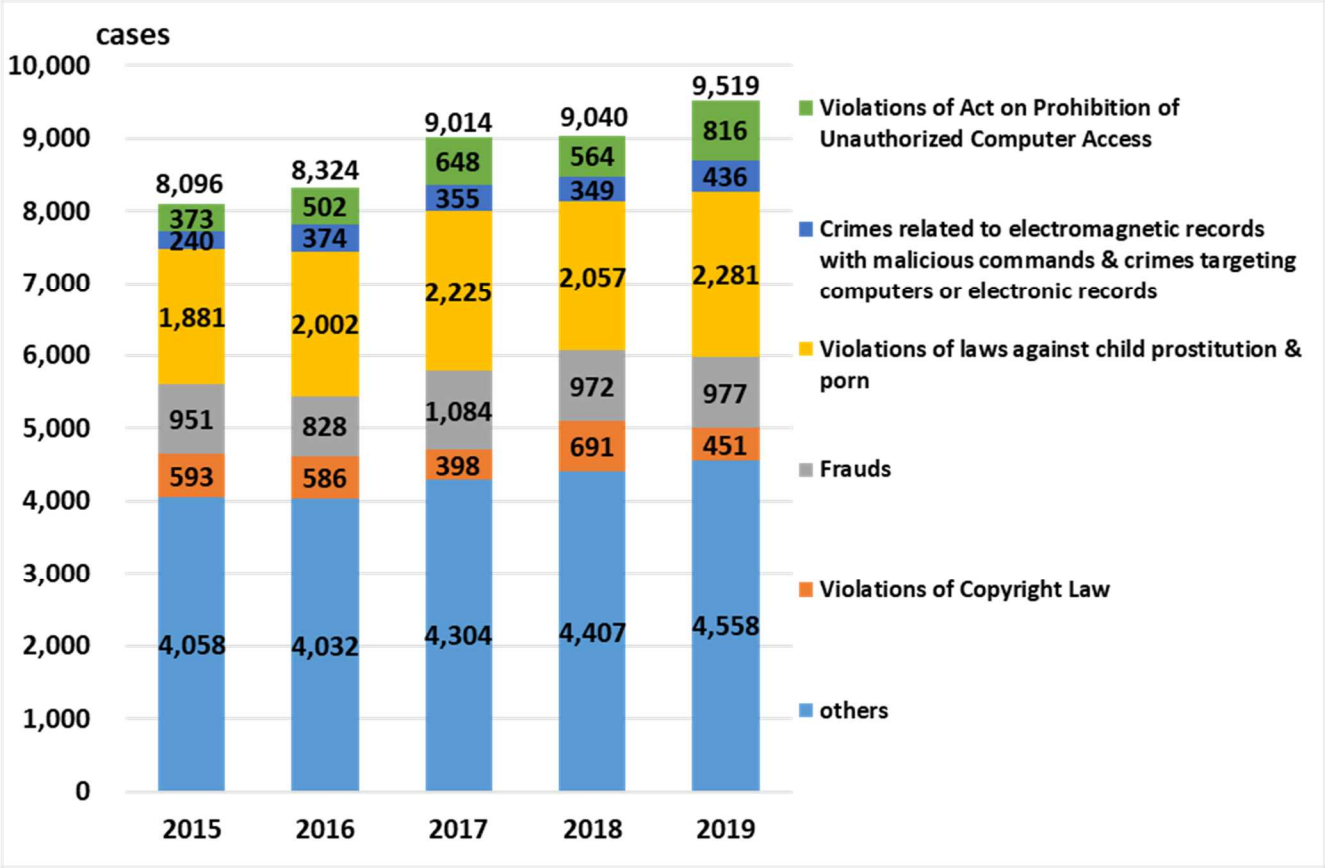

Figure 9 [Number of cleared cybercrime cases]

b. Violations of the Act on Prohibition of Unauthorized Computer Access[8]

(a) The number of cleared cases

- The number of cleared violations of the Act on Prohibition of Unauthorized Computer Access reached 816 in 2019, exceeding the previous year. 785 of all the cleared cases were classified as the identification-code-abuse type[9] and accounted for approx. 96.2% of the total.

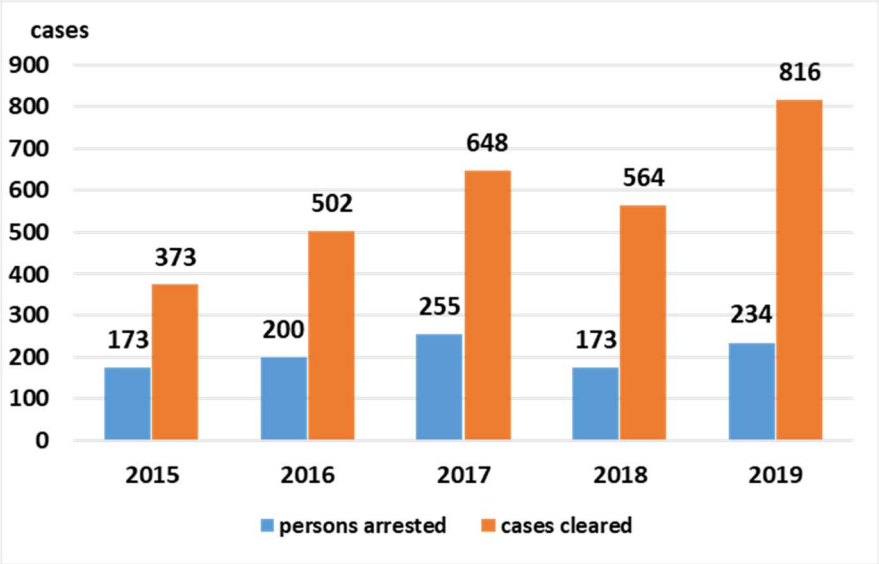

Figure 10 [Number of cleared violations of unauthorized computer access]

- **"Abuse of lax password setting & management" dominant**

The most dominant method of identification code abuse in the unauthorized computer access was the abuse of lax password setting and management of the authorized users, which accounted for 310 cases and 39.5 % of the total, followed by the abuse of the codes obtained from others, which accounted for 182 cases and 23.2% of the total.

- **Online game community websites most abused**

The most abused service was the online game community websites, reaching 224 cases and occupying approximately 28.5% of the total, followed by the members/employees-only websites, accounting for 151 cases and approximately 19.2% of the total.

---

[8] 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.

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

(b) Online Banking Fraud

- **Overview**

The number of online banking fraud in 2019 reached 1,872, second highest to 2014. Its total loss in 2019 also drastically increased from 2018 to approximately 2.5 billion yen.

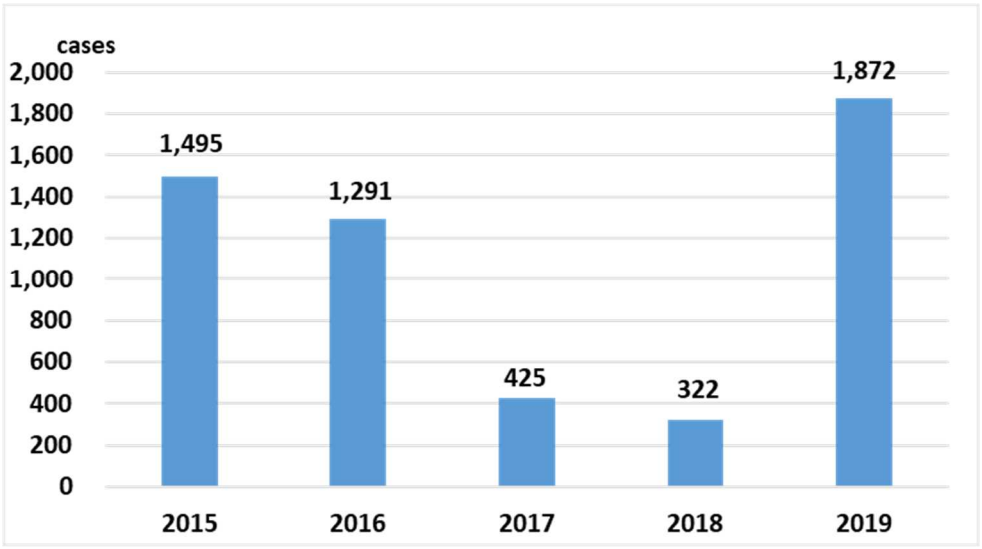

Figure 11 [Number of online banking fraud]

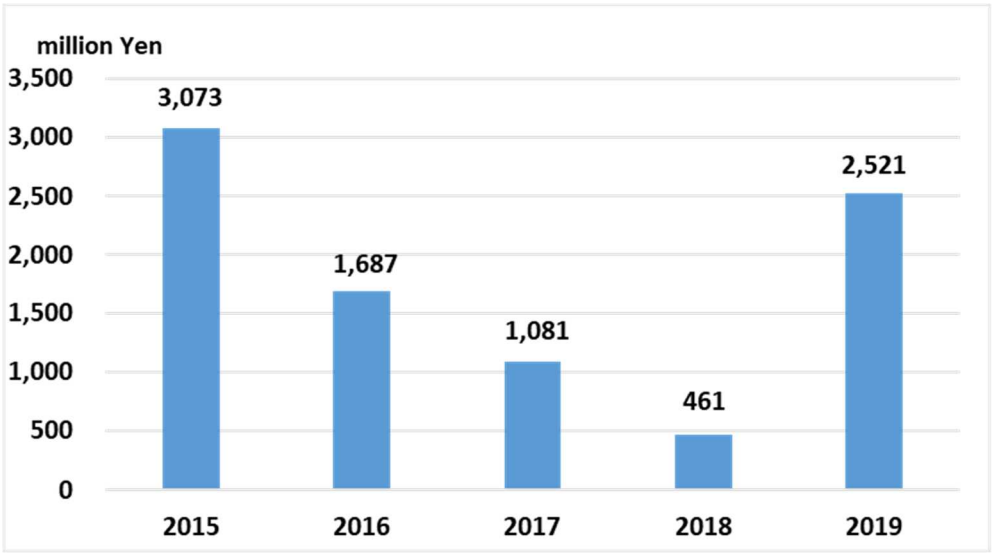

Figure 12 [Total loss from online banking fraud]

- **Characteristics**

- Although both the number and loss from online banking fraud in the 1st half of 2019 were lower than the 1st half of 2018, they surged since September 2019. Many of the fraud incidents are presumed to have been caused by the SMS messages or emails impersonating the financial institutions to mislead the recipients to the phishing websites.
- The theft of IDs, passwords or one-time passwords on the phishing websites, which led to the illicit remittance from the financial institutions' websites, as well as the theft of IDs, passwords, birthdates and telephone numbers, which led to the illicit remittance using the official applications of the financial institutions have been confirmed.
- Among the confirmed primary destinations of illicit remittance, 58.6% of the accounts were held

by Japanese nationals, followed by 13.5% by Vietnamese and 8.8% by Chinese.

- Methods of online banking fraud have been diversifying. Besides the conventional illicit remittance to the bank accounts, purchase of e-money or major e-commerce services' e-gift cards, and deposit on the prepaid virtual credit cards have been confirmed.

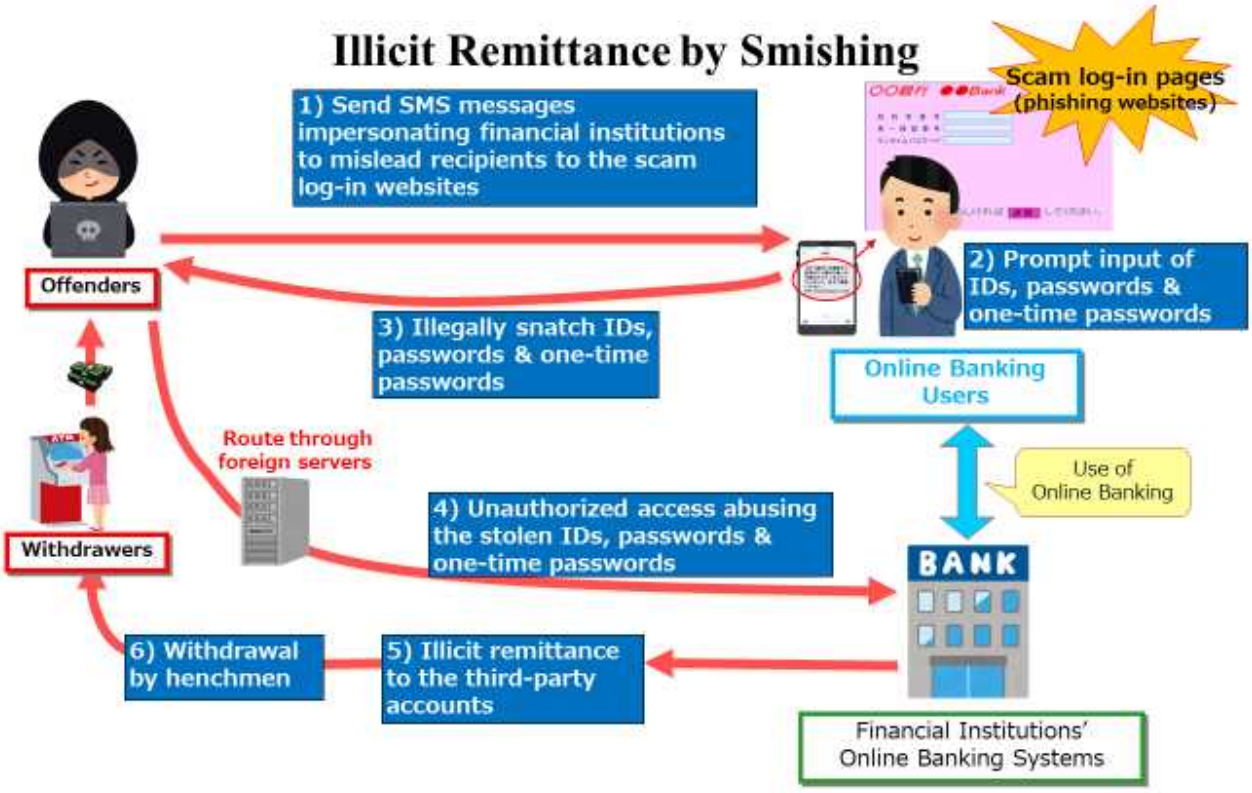

Figure 13 [SMS abuse-based illicit remittance scheme]

(c) Illicit cryptoasset remittance through unauthorized computer access to cryptoasset exchanges

The number of detected illicit cryptoasset remittance through unauthorized computer access to the cryptoasset exchanges in 2019 was 22, with total loss of approx. 3,128.6 million yen, both remarkably declined from 2018. In 2018, the number of detected illicit cryptoasset remittance was 169 cases, with total loss of approx. 67.7 billion yen.

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

[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)

- **The number of cleared cases**

The total number of cleared cases related to the electromagnetic records with malicious commands and crimes targeting computers or electromagnetic records in 2019 was 436, increasing from 2018.

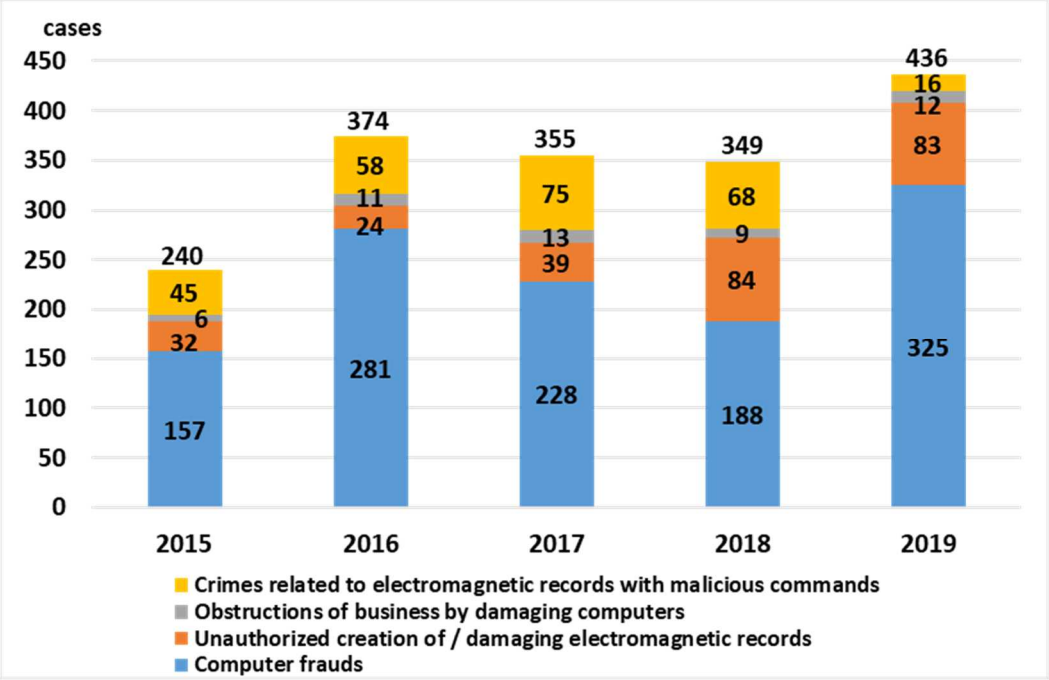

Figure 14 [Number of cleared cases related to electromagnetic records with malicious commands & crimes targeting computers or electromagnetic records]

- **Characteristics**

The most dominant crime type among the cleared cases in this category was the computer fraud, reaching 325 cases and 74.5% of the total.

d. Others

- The number of cleared violations of the Act on Punishment of Activities Relating to Child Prostitution and Child Pornography, and Protection of Children in 2019 was 2,281, increasing from 2018.
- The number of cleared fraud cases accounted for 977, at the equivalent level from 2018.
- The number of cleared violations of the Copyright Act in 2019 was 451, decreasing from 2018.

(3) Countermeasures

- **Prevention of online banking fraud**

In response to surge of the illicit money remittance victims, the NPA partnered with the JC3 and implemented a warning campaign on the respective websites in October 2019.

The NPA also shared information on the criminal methods and damages of online banking fraud with the Japanese Bankers Association, and conducted a joint alarming campaign to prevent damage on the respective websites in December 2019.

- **Joint countermeasures with JC3 against e-commerce scam websites**

The NPA implements preventive measures by utilizing the tools jointly developed by the Aichi Prefectural Police and the JC3 to report the scam websites' URLs detected by the JC3 to the pertinent organizations including the APWG[12].

- **Prevention of Credit Card Data Theft**

In response to disclosure of the mechanism of online credit card data theft through the falsified e-commerce websites, the NPA implemented a warning campaign in cooperation with the JC3 toward the website operators and users.

(End)

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