The situation of threats in cyberspace in the first half of 2018

1. Cyber-attacks

(1) Scanning activities in cyberspace

a. Overview of unexpected incoming packets to the sensors[1]

The number of unexpected incoming packets to the sensors was 2,223.6 per IP address in a day, which has been shown an upward trend on the whole in recent years.

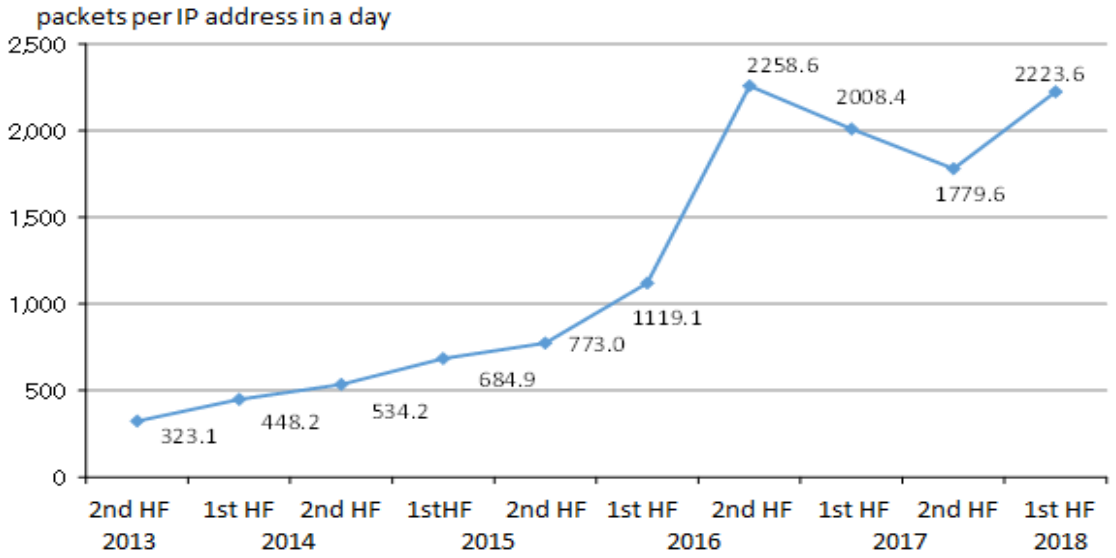

Figure 1 [Number of unexpected incoming packets to the sensors]

b. Characteristics

- Diversified targets of cyber-attacks and scanning activities

As for destination ports[2] where unexpected incoming packets were observed, the number of unexpected incoming packets to commonly used ports (port number 1023 and below) remained high and yet the number has been on a downward trend since the first half of 2017. On the other hand, the number of unexpected incoming packets to ports (port number 1024 and above) which are used for communications with IoT devices or specific parties has been on an upward trend, and the number exceeded that of unexpected incoming packets to ports 1023 and below in the first half of 2018.

[1] The sensors are components of the Real-time Detection Network System that the NPA operates around-the-clock, and are placed at the Internet connection points. These sensors detect connecting information (including scanning activities for attempting cyber-attacks) which is not assumed to be ordinary use of the Internet, and the system assembles and analyzes the information.

[2] Port is an interface of a computer for specifying which protocol is to be applied in TCP/IP communication, and a number 0 to 65525 is assigned to each port.

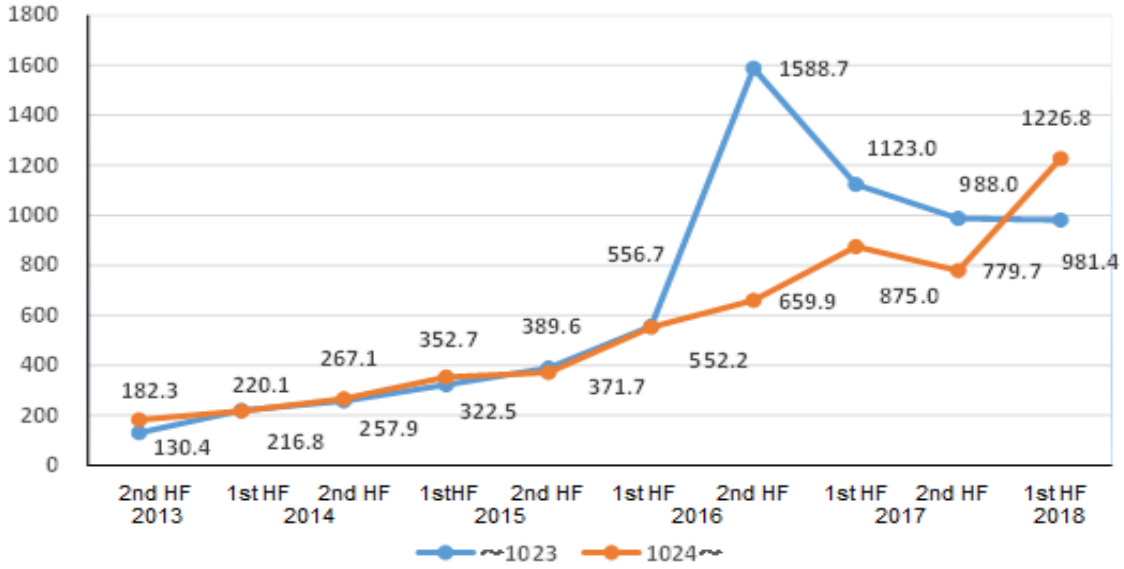

Figure 2 [Number of unexpected incoming packets by destination port per IP address in a day]

As for the percentage of the numbers of unexpected incoming packets to each destination port in the first half of 2018, "others" got increased and concentrative access to the specific ports decreased. The reason why the percentage of "others" got increased seems that the range of targets of scanning activities and cyber-attacks were diversified, expanding into networks of IoT or cryptocurrency.

One of other characteristics is that the percentage of unexpected incoming packets from bots of Mirai to 80/TCP and these packets, targeting vulnerability of Microsoft Windows, to 445/TCP got increased again.

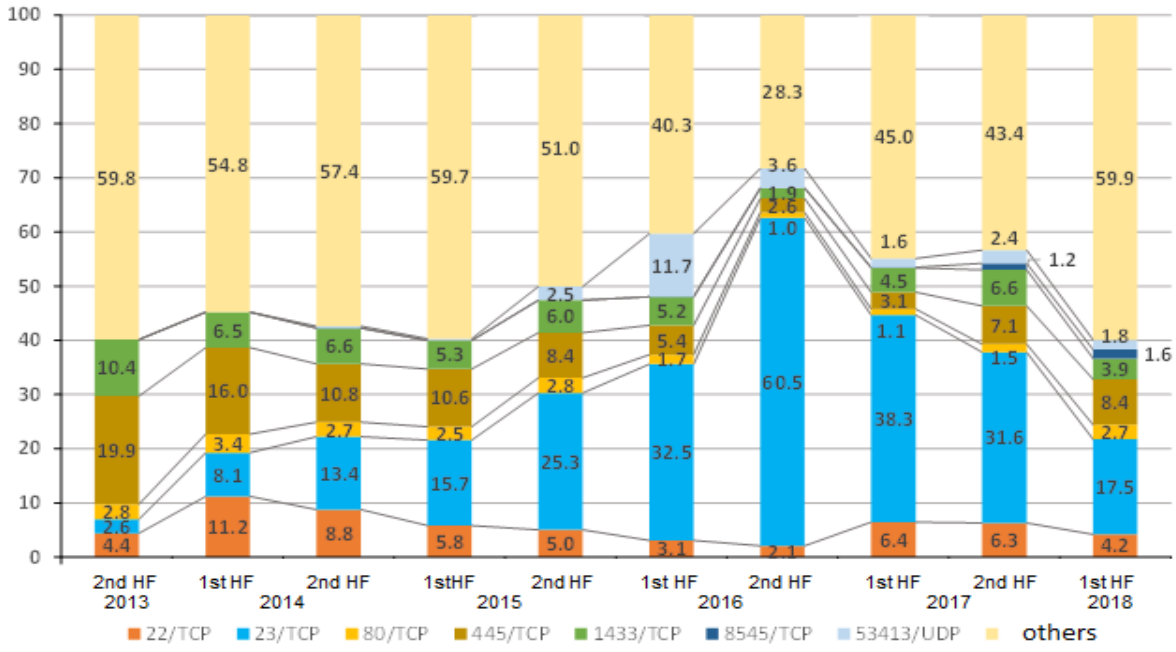

Figure 3 [Percentage of unexpected incoming packets by destination port]

- Observation of unexpected incoming packets targeting cryptocurrency network

Unexpected incoming packets targeting cryptocurrency network have been increasing in recent years. The NPA observed an increase in the number of IP addresses which were the sources of unexpected incoming packets presumably targeting Ethereum network in and after late March 2018, and observed a surge in the middle of June.

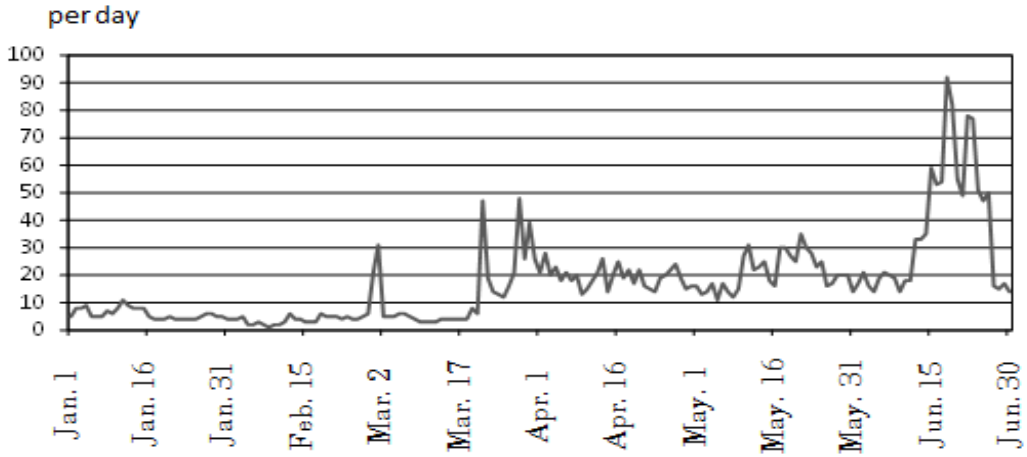

Figure 4 [Number of originating IP addresses of unexpected incoming packets, toward destination port 8545/TCP, which seemed to target Ethereum network]

The NPA observed unexpected incoming packets targeting "Claymore," which is mining tool for Ethreum, in and after January 2018, and observed an increase in the number of unexpected incoming packets which were presumably related to scanning activity targeting cryptocurrency "EOS" in and after late May 2018.

- Infection activity of malware which is furnished with a function of mining cryptocurrency

In February 2018, the NPA observed an increase in unexpected incoming packets which were presumably made by malware "ADB. Miner" that infected terminals of Android TV Box and mined cryptocurrency without permission of users of the terminals. And in and after March 2018, the NPA observed a lot of the unexpected incoming packets.

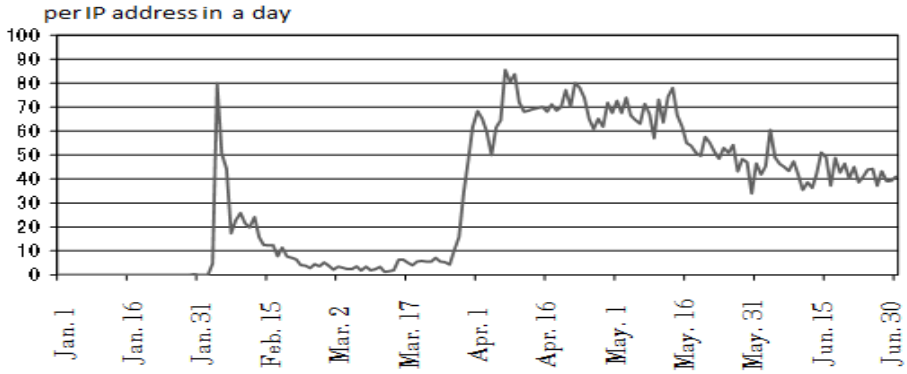

Figure 5 [Number of access to port 5555/TCP presumably targeting Android TV Box]

In addition, in and after late March 2018, the NPA observed unexpected incoming packets targeting NoSQL database "Redis," content management system "Drupal" and GPON routers, which once had vulnerability.

(2) Situation of cyber-attacks and efforts toward them

a. Situation

(a) Overview

The Japanese police share information on cyber-attacks, which seemed to intend to thieve information, with business operators through the Counter Cyber-intelligence Information-Sharing Network[3]. The number of spear phishing e-mail attacks the Japanese police confirmed through the Network has been on an upward trend in recent years, and yet the number in the first half of 2018 (2,578) was lower than the number in the second half of the last year which was the highest ever.

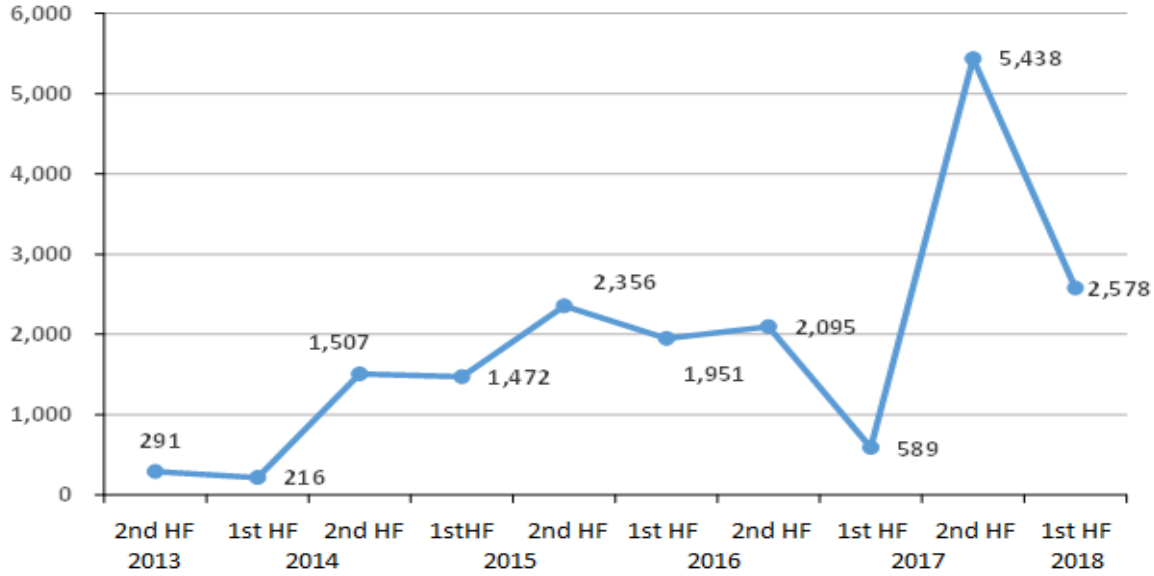

Figure 6 [Number of spear phishing e-mail attacks]

And web browsing failures in the websites of Japanese government agencies, public transport and aquariums occurred as in 2017.

The Japanese police confirmed that the self-styled international hacker group "Anonymous" posted SNS with messages which seemed to be claims of responsibility for the cyber-attacks against 15 organizations.

[3] A framework between the police and 7,769 organizations/business operators with cutting-edge technologies all over the country (as of July 2018) to share information on cyber-attacks which seem to intend to thieve information. Through the framework the police and the member organizations/business operators also share results of analysis on spear phishing e-mail attacks against governmental entities, in coordination with the National Center of Incident-readiness and Strategy for Cybersecurity (NISC).

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

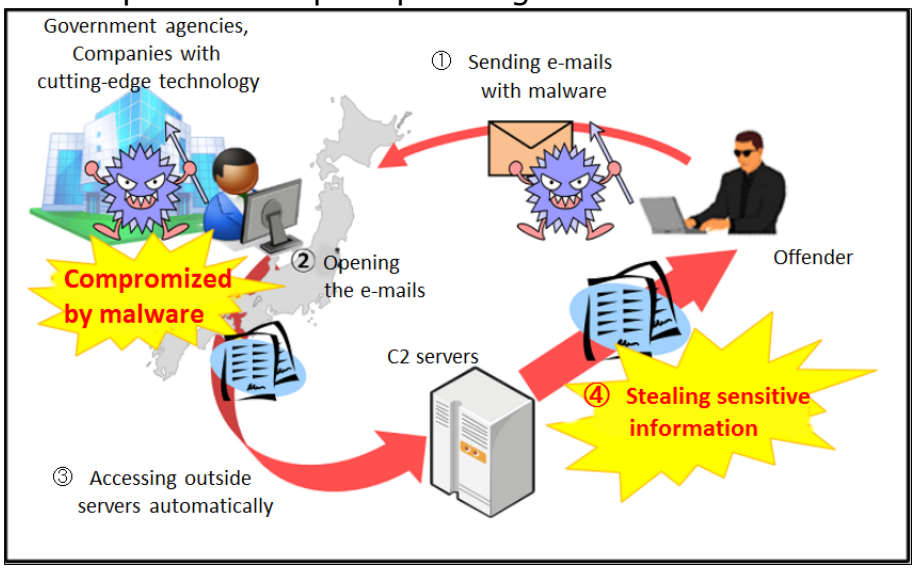

Figure 7 [Chart of spear phishing e-mail attacks]

- "Indiscriminate style"[4] spear phishing e-mail attacks continued to occur frequently

A lot of "indiscriminate style" spear phishing e-mail attacks occurred and accounted for about 87% of the total. The percentage remained high.

Year	Indiscriminate style	Non indiscriminate style
2013, 2nd half	63.6% (185 cases)	36.4% (106 cases)
2014, 1st half	39.8% (86 cases)	60.2% (130 cases)
2014, 2nd half	92.1% (1,388 cases)	7.9% (119 cases)
2015, 1st half	91.5% (1,347 cases)	8.5% (125 cases)
2015, 2nd half	91.7% (2,161 cases)	8.3% (195 cases)
2016, 1st half	85.4% (1,667 cases)	14.6% (284 cases)
2016, 2nd half	94.2% (1,974 cases)	5.8% (121 cases)
2017, 1st half	89.0% (524 cases)	11.0% (65 cases)
2017, 2nd half	97.9% (5,322 cases)	2.1% (116 cases)
2018, 1st half	87.1% (2,246 cases)	12.9% (332 cases)

Figure 8 [Percentage of "indiscriminate style" spear phishing e-mail attacks and others]

[4] The NPA defines an act that an offender, sending an e-mail to which malware anti-virus software on the market cannot detect is attached and which is disguised as what is related to business of an addressee, attempts to infect a computer of the addressee with the malware to thieve information as "spear phishing e-mail attack." The NPA categorizes a spear phishing e-mail attack which brings the same text or the same malware to 10 or more than 10 addressees as "indiscriminate style."

- Most of the spear phishing e-mails were sent to unpublicized e-mail addresses

As for destination of the spear phishing e-mails, unpublicized e-mail addresses accounted for about 85% of the total. The percentage remained high.

- Most of the e-mail addresses of the spear phishing e-mails were forged

In the spear phishing e-mail cases, 96% of the e-mail addresses of the addressers seemed to be forged.

- Change in the proportion of formats of files which were attached to spear phishing e-mails

As for the proportion of formats of files that were attached to spear phishing e-mails, the proportion of the MS-Excel file showed a big raise in the first half of 2018.

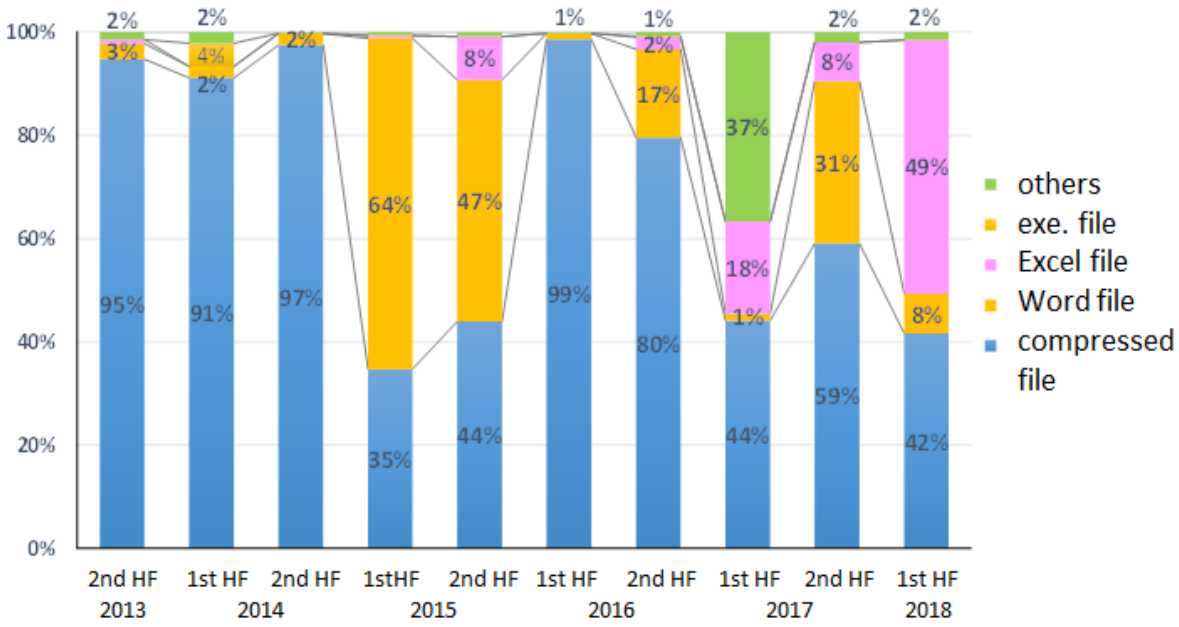

Figure 9 [Percentage of formats of files attached to spear phishing e-mails]

- Change in formats of compressed files

As for formats of the compressed files that were attached to spear phishing e-mail, script files[5] which had kept high proportion since the second half of 2016 was not found, and executable files showed high percentage.

[5] A file written by a simple programing language (scripting language). This file is often abused to download malicious executive files.

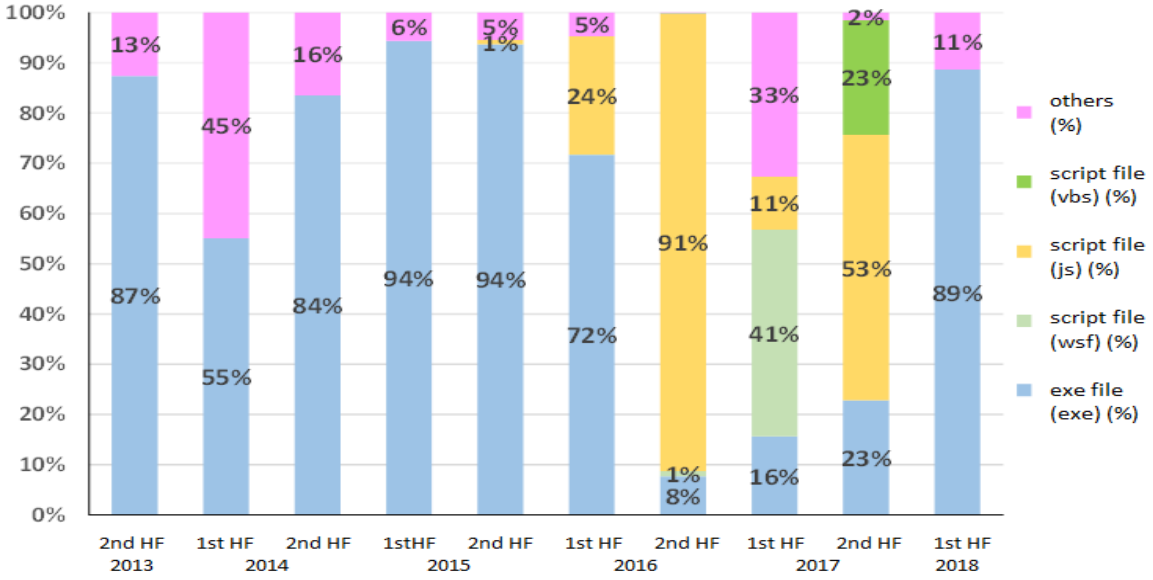

Figure 10 [Percentage of formats of compressed files attached to spear phishing e-mails]

b. Efforts

(a) Takedowns on C2 servers used for cyber-attacks

The Japanese police encouraged hosting server businesses to take down C2 servers[6] which had been identified through the analysis of malware used in cyber-attack cases. Six C2 servers were taken down in the first half of 2018.

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

Preparing for the Tokyo 2020 Olympic and Paralympic Games, the Japanese police conducted several measures against cyber-attacks, such as joint drills with relevant organizations on the supposition of cyber-attacks and information sharing with relevant organizations in the countries that hosted the Olympic and Paralympic Games before.

2. Cybercrimes

(1) The number of cleared cybercrime cases and consultation regarding cybercrime

The number of cleared cybercrime cases has been on an upward trend in recent years, and yet it slightly decreased as compared to the first half of 2017 which was the highest ever.

And the number of consultation regarding cybercrime was the highest in 2016, and yet it decreased in 2017. The number in the first half of 2018 was 61,473, and it was also lower than that in the first half of 2017.

[6] Command and Control Server. It might be abbreviated to "C&C server." A C2 server, operating in response to commands from an offender and giving commands to computers which are infected with malware, plays a central role of malicious operations of computers.

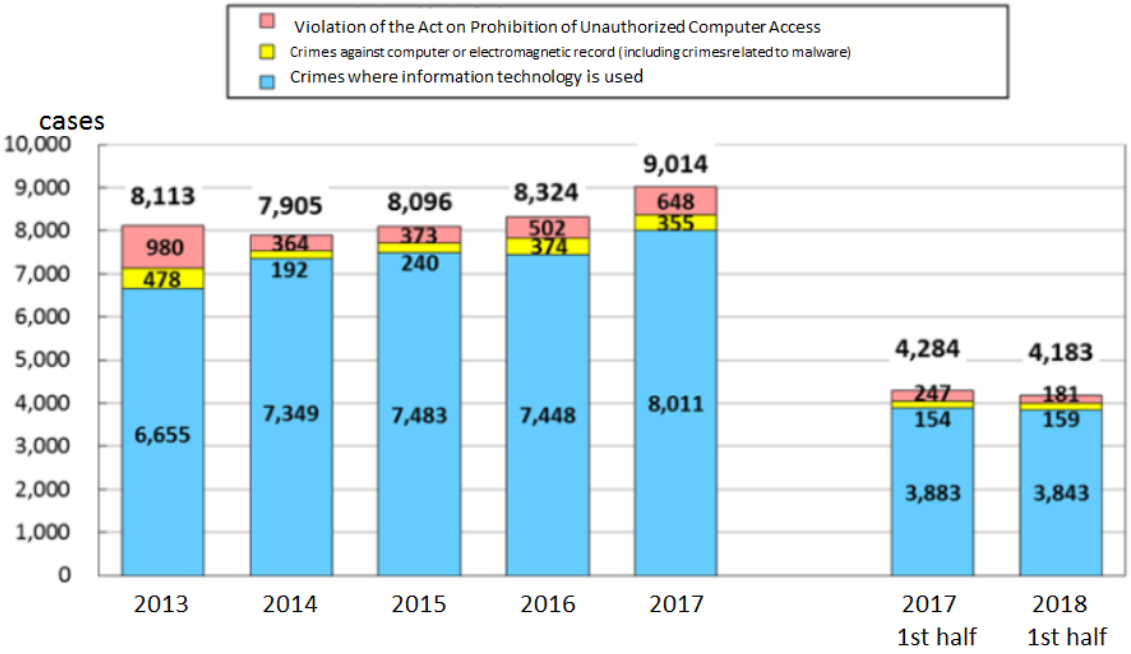

Figure 11 [Number of cleared cybercrime cases]

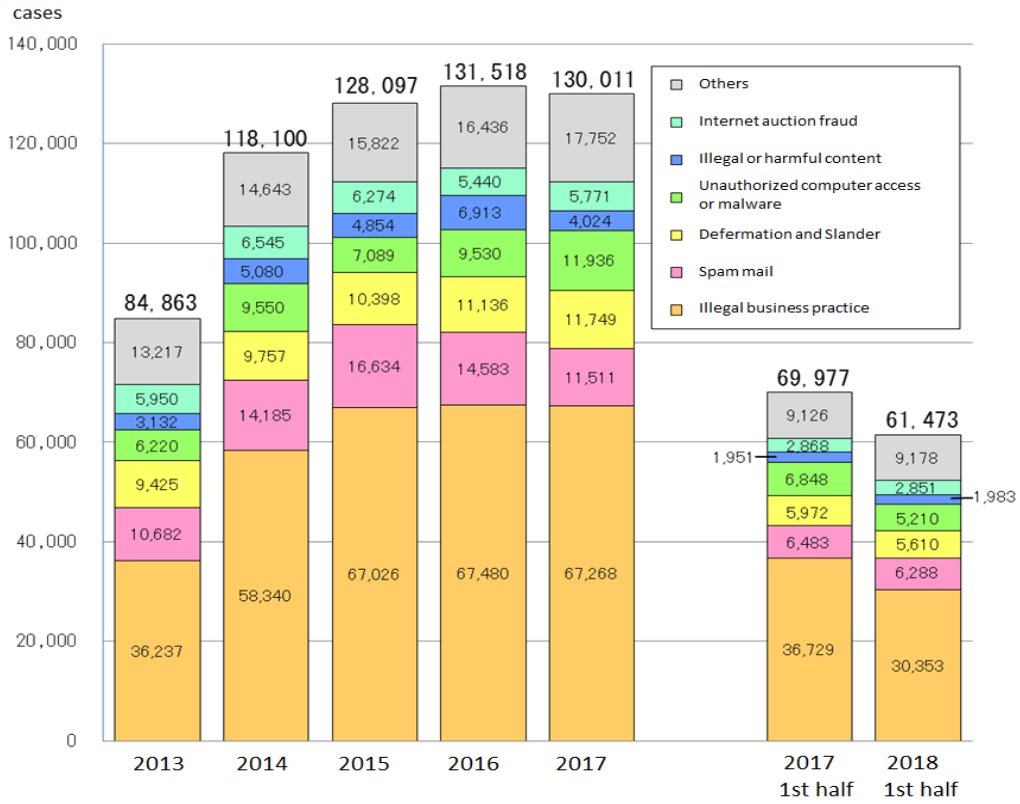

Figure 12 [Number of consultation regarding cybercrime]

(2) Situation of online banking fraud

a. Overview

The number of online banking fraud cases was 211, and the amount of damage was about 372 million yen (about 3.3 million US dollars), and both of them have been on a downward trend on the whole.

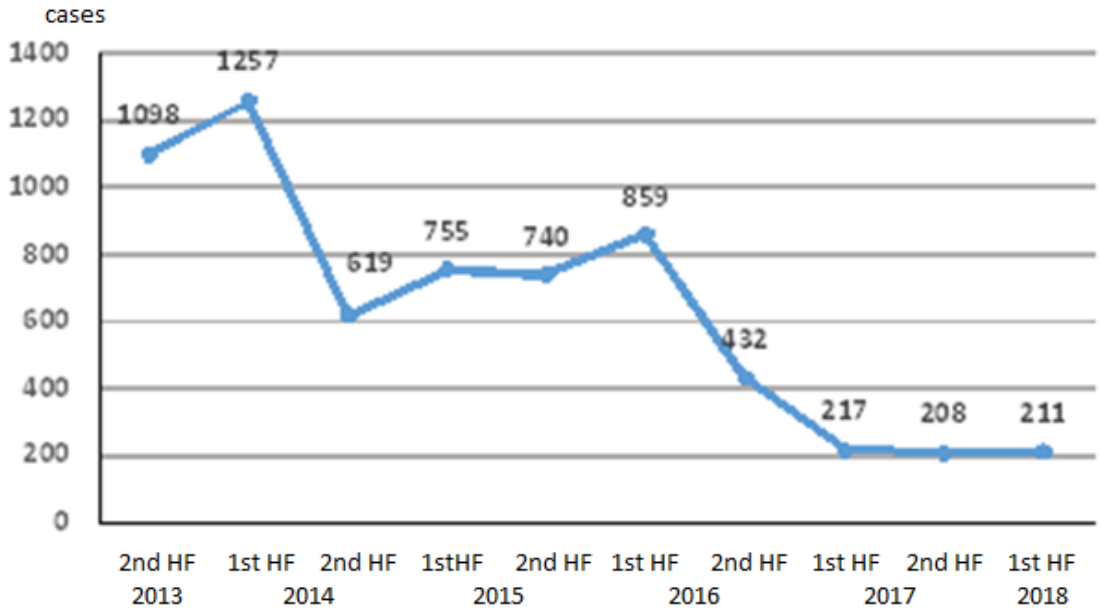

Figure 13 [Number of online banking fraud cases]

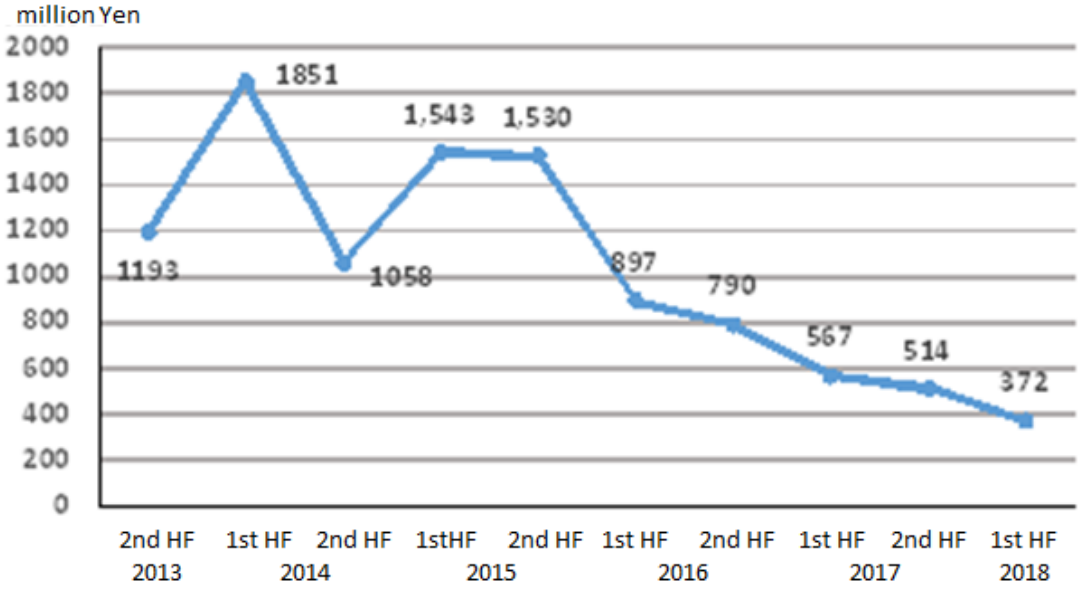

Figure 14 [Amount of damage of online banking fraud]

b. Characteristics

- Significant decrease in damage to corporate bank accounts

The damage caused in corporate accounts decreased as compared to the first half of 2017 mainly at regional banks and Shinkin banks due to the countermeasures such as enhancement of monitoring[7] and the launch of onetime password authentication.

- Significant decrease in the number of unauthorized wire transfer cases where electronic settlement service system was abused

As for unauthorized wire transfer cases where electronic settlement service system was abused, unauthorized wire transfer for purchasing cryptocurrency via electronic settlement service system was not confirmed, so that the number of those cases decreased significantly.

- About 60% of the destination accounts for the unauthorized wire transfer were under names of Vietnamese

As for nationalities of the account holders, Vietnam represented 65%, China 15%, and Japan 12% of 358 accounts which were identified as the first destination accounts for the unauthorized wire transfer.

(3) Unauthorized transmission of cryptocurrency caused by unauthorized computer access to cryptocurrency exchange operators

- The number of reported cases was 158, and the total amount of damage was about 60.53 billion yen, which exceeds the one in first half of 2017 (51 reported cases and 115 million yen) by 107 cases and 60.388 billion yen.
- In the 102 cases (64.6%) out of the 158 cases that were reported to the police, customers used the same ID and password as used for other services.

(4) Efforts

- Countermeasures against "DreamBot" that is malware with a function to remit balance without being noticed by account holders

Since the infection with the malware "DreamBot" still continued to occur, the police, in partnership with the JC3, urged Internet users and financial institutions to draw attention. And the JC3 created on its website the page where Internet users could check whether their computers were infected with "DreamBot."

- Countermeasures against unauthorized cryptocurrency transmission

The NPA provided the Financial Services Agency with information on situation of unauthorized cryptocurrency transmission, and secured cooperation of the Financial Services Agency in guidance to, and its assistance for cryptocurrency exchange operators.

- Countermeasures, in coordination with the JC3, against fraudulent websites related to online shopping

The JC3, collaborating with the Aichi Prefectural Police in developing tools to detect fraudulent websites, provided URLs of the fraudulent websites, which the JC3 detected with the

[7] Monitoring IP addresses which were used for unauthorized remittance.

tools, to the APWG[8].

- Providing information leading directly to prevention of damage, and requesting to enhance preventive measures

The NPA requested financial institutions to enhance monitoring their transactions, to urge their customers to use a onetime password and two-path authentication[9], and to implement thoroughly customer identification.

(End)

[8] *A*nti-*P*hishing *W*orking *G*roup. A nonprofit organization founded in 2003 in the United States in order to address phishing scam.

[9] An authentication method where information required to complete transaction is transmitted through 2 channels. For example, a customer inputs what is required for online banking transaction into his/her PC, and authenticates the transaction, inputting an ID, a password, and so on into his/her smartphone. Even if the PC used for online banking were operated without authority to wire-transfer due to computer-virus infection, unauthorized transaction will be prevented because an authentication through another (smartphone) channel is required to complete the transaction.