UNOFFICIAL TRANSLATION

Press release
March 22, 2018
National Police Agency

Situation of threats in cyberspace in 2017

1. Cyber-attacks

(1) Scanning activities in cyberspace

- The number of unexpected incoming packets in a day to the sensors deployed at the Internet connection points continued to increase to 1,893.0 per IP address. (Figure 1)
- It was observed on a world scale that exploits abused for such ransomware as “WannaCry” were used for cyber-attacks. (Figure 2)
- The main reason the number of unexpected incoming packets increased as compared to 2016 was that scanning activities targeting Internet of Things (IoT) devices remained at a high level in 2017.

(2) Situation of cyber-attacks and cybersecurity measures

a. Situation

- The number of spear phishing e-mail attacks the Japanese police confirmed through the framework between the police and organizations/business operators with cutting-edge technologies continued to increase to 6,027 cases in 2017. (Figure 4)
- The Japanese police confirmed that the self-styled international hacker group “Anonymous” posted messages on SNS which were believed to be claims of responsibility for the cyber-attacks against 65 organizations.

b. Efforts

- The police analyzed comprehensively information gathered through the abovementioned framework and provide results of analysis to the member organizations/business operators.
- The Japanese police prompted hosting service providers to stop a function of 61 domestic C2 servers which the police found through the analysis of malware used in cyber-attack cases.
- Preparing for the Tokyo 2020 Olympic and Paralympic Games, the Japanese police conducted several measures against cyber-attacks, such as joint response exercises with relevant organizations and sharing information with them.

2. Cybercrimes

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

The number of cleared cybercrime cases continued to increase to 9,015. And the number of consultation regarding cybercrimes was 130,011 cases and remaining at a high level. (Figure 9 and

10)

(2) Situation of unauthorized wire transfer in online banking

- The number of online banking fraud cases decreased to 425, which was a quarter of the highest record in 2016. (Figure11).
- The total amount of damage due to online banking fraud decreased to about 1,081 million yen, which was one third of the highest record in 2015. (Figure 12)
- The damage has decreased in recent years due to the countermeasures such as enhancement of monitoring and launch of onetime password authentication by financial institutions.
- Regarding financial institutions where accounts of victims were opened, the number of *shinkin* banks (credit association) and municipal-level agricultural cooperatives (running a credit business) significantly decreased in the past 3 years. The reason the number decreased is that almost all *shinkin* banks and municipal-level agricultural cooperatives, accepting a request from the police, launched onetime password authentication.

(3) The number of cleared cases of unauthorized computer access

- The number of suspects arrested or whose cases were sent to public prosecutors offices for the violation of Act on Prohibition of Unauthorized Computer Access continued to increase to 255 in 2017. And the Japanese police cleared 648 cases which was the second highest in this 5 years following the highest one in 2013. (Figure 13).
- As for unauthorized transmission by unauthorized computer access to virtual currency exchangers, the number of reported cases was 149, and the total amount of damage was about 662.4 million yen.

(4) Efforts

- Taking countermeasures, with public-private partnership, against tampering with websites to infect computers.
- Taking countermeasures against leaked IDs and infected computers which were identified in the international effort.
- Taking countermeasures against "DreamBot," online banking malware with a function to remit balance without being noticed by account holders.
- Taking countermeasures, in coordination with the Japan Cybercrime Control Center (JC3, a private foundation), against fraudulent websites related to online shopping.
- Providing information leading directly to prevention of damage, and requesting to enhance preventive measures.

3. Future initiatives

On the basis of the "Cybersecurity Strategy of the Japanese Police" dated September 4th, 2015, the Japanese police promote various initiatives or measures including the following;

- Promoting information gathering and analysis concerning cyberspace.
    - Enhancement of information gathering in the Darknet.

- Promoting partnership between the public and private sectors.
  - Partnership with the JC3.
    - Information sharing for ensuring the cyberspace security
    - Measures for preventing further damage, with public-private partnership, by disseminating information
  - Partnership with critical infrastructure providers, business operators with cutting-edge technology.
  - Promoting two-factor authentication.
- Human resource development for cybersecurity.
  - Developing specialized investigators (including enhancement of education and training in the Cybersecurity Research and Training Center, National Police Academy).
  - Developing highly professional human resources for digital forensics.
- International collaboration.
  - Collaboration with foreign law enforcement agencies.
- Promoting cybersecurity measures for the Tokyo 2020 Olympic and Paralympic Games (including information sharing and joint response exercises with relevant organizations).

(End)

The situation of threats in cyberspace in 2017

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 continued to increase to 1,893.0 per IP address in a day.

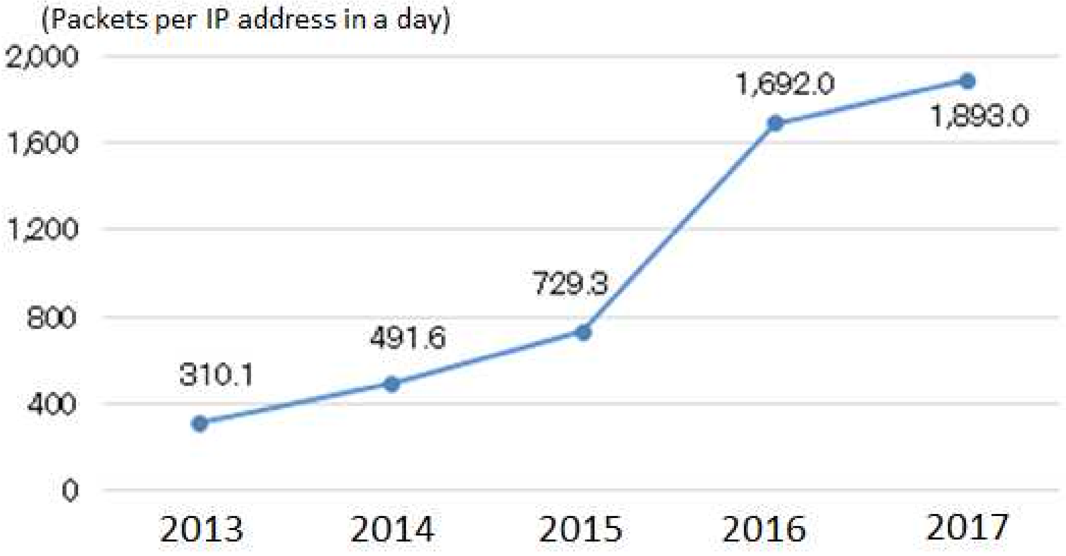


Figure 1 [The number of unexpected incoming packets to the sensors]

b. Characteristics

- Infection activities of ransomware "WannaCry."

In April, exploits "Eternalblue" and "Doublepulsar" whose target was Microsoft Windows were leaked to the public by a group calling themselves "Shadow Brokers," and scanning activities or cyber-attacks targeting infected devices by the exploits were observed thereafter.

In May, ransomware "WannaCry," that had been created by abusing "Eternalblue" and "Doublepulsar" spread worldwide, and the National Police Agency (NPA) observed its activities of infection. In and after June, the NPA confirmed that infection of WannaCry's variants was spreading, though users of computers, which the variants were infected, rarely noticed the infection. In and after December, the NPA observed the increase in unexpected incoming packets which seemed to be cyber-attacks exploiting "Eternalblue" and "Doublepulsar."

[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 trying cyber-attacks) which is not assumed to be ordinary use of the Internet, and the System assembles and analyzes the information.

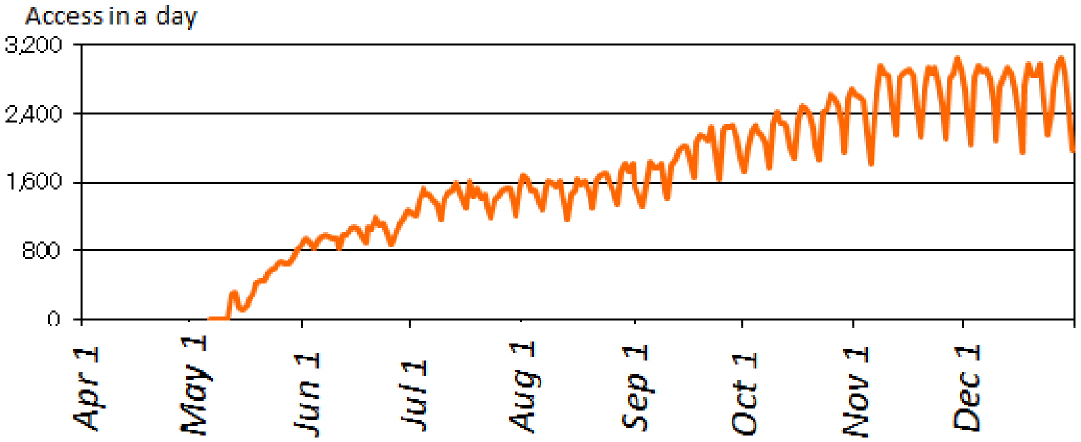


Figure 2 [The number of source IP addresses of access to port 445/TCP, which is characteristic of infectious activity of WannaCry]

- Scanning activities targeting IoT devices.

In and after November, the NPA observed the increase in unexpected incoming packets which seemed to be infection activities targeting vulnerabilities of specific routers. At the same time, the NPA observed the sharp increase in unexpected incoming packets which came from IP addresses allocated to Japan and which seemed to be scanning or infection activities targeting IoT devices.

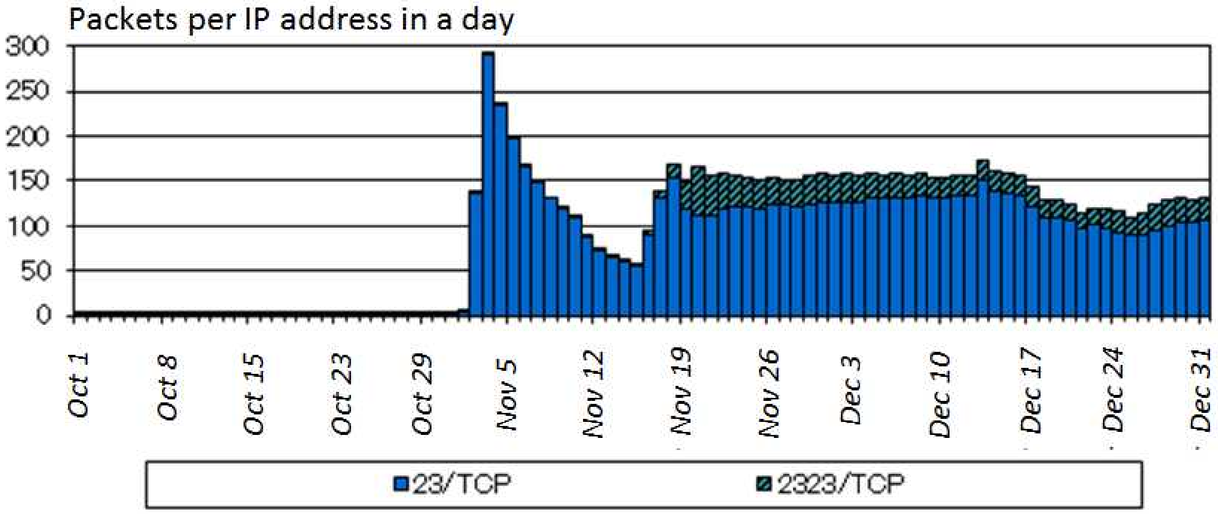


Figure 3 [The number of accesses originating from Japan to destination port 23/TCP or 2323/TCP]

- Scanning activities targeting vulnerabilities of Apache Struts 2[2] and Apache Tomcat[3]

The NPA observed scanning activities and cyber-attacks targeting critical vulnerabilities of Apache Struts 2 and Apache Tomcat.

[2] A software framework improving efficiency of application development by providing a versatile function which are used in developing web applications written in Java script.

[3] An application server (servlet container) which is used when a programmer creates, in Java script, a dynamic webpage called servlet and JSP (Java script page).

(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[4]. The number of spear phishing e-mail attacks the Japanese police confirmed through the Network continued to increase to 6,027.

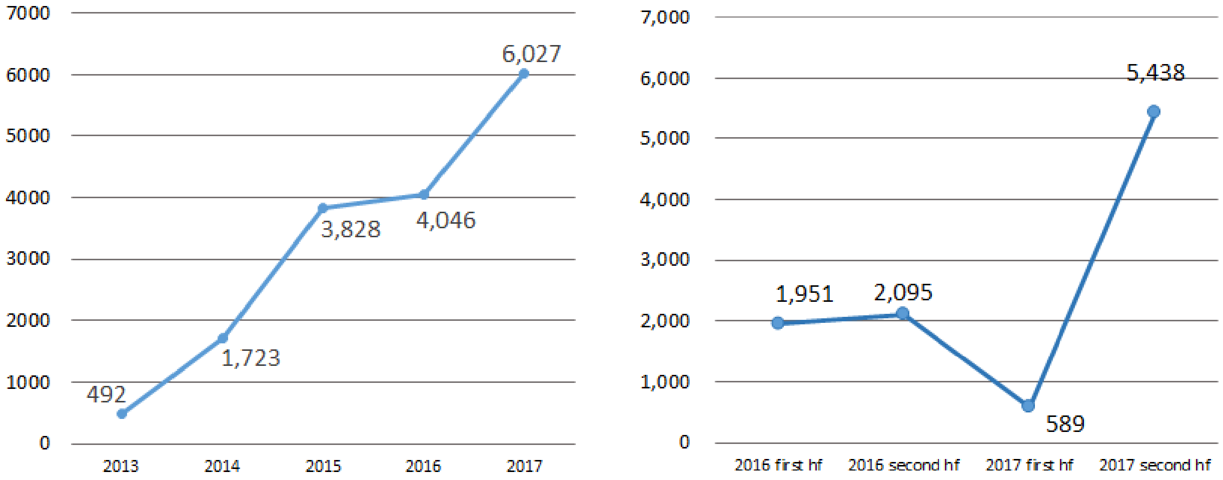
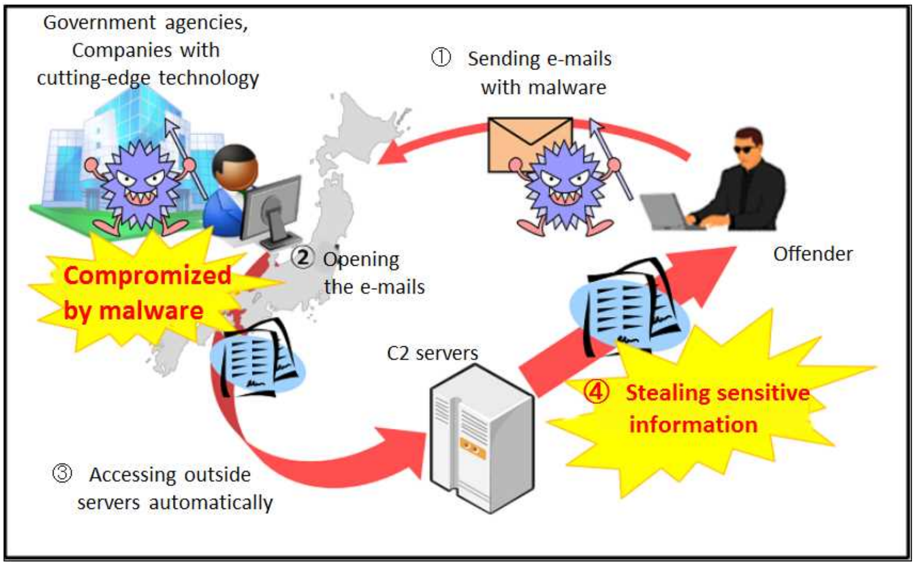


Figure 4 [The number of spear phishing e-mail attacks]



[4] A framework between the police and 7,737 organizations/business operators with cutting-edge technologies all over the country (as of January 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).

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

And web browsing failures in the websites of Japanese government agencies, public transport and aquariums occurred as in 2016.

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 65 organizations.

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

- "Indiscriminate style"[5] spear phishing e-mail attacks continued to occur frequently.

A lot of "indiscriminate style" spear phishing e-mail attacks occurred as in 2016, and accounted for about 97% of the total. It was confirmed that a large number of e-mails which had pretended that a home delivery company had notified its customers of redelivery had been sent in the cases of those "indiscriminate style" spear phishing e-mail attacks.

Year	Indiscriminate style	Non indiscriminate style
2013	53% (259 cases)	47% (233 cases)
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)

Figure 6 [Percentage of "indiscriminate style" spear phishing e-mail attacks and others]

- 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 90% of the total. The percentage remained high as in recent years.

- E-mail addresses of most of the spear phishing e-mails were forged.

In the spear phishing e-mail cases, 62% of the e-mail addresses of the addressers seemed to be forged.

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

As for the proportion of the formats of the files which were attached to spear phishing e-mails, compressed files and files of MS-Word and MS-Excel still commanded a majority. The proportion of files of MS-Word increased from 9% in 2016 to 28%, and the proportion of the files of MS-Excel increased from 1% in 2016 to 9%. And in those MS-Word or MS-Excel files, files

[5] The NPA defines an act that an offender, sending an e-mail where malware which anti-virus software on the market cannot detect is attached and which is disguised as what is related to business of an addressee, infects 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."

exploiting a function of DDE[6] or Macro were confirmed.

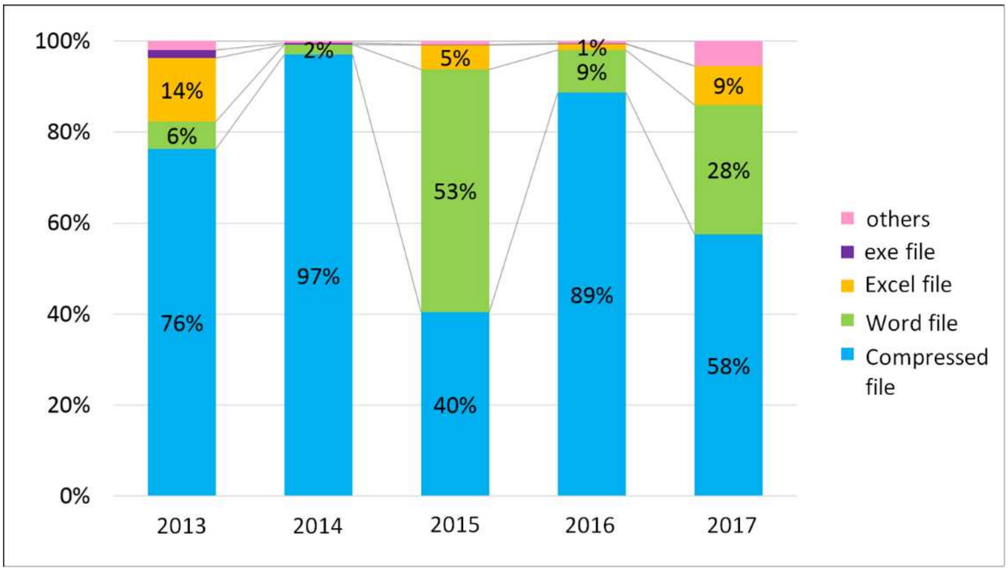


Figure 7 [Percentage of formats of files attached to spear phishing e-mails]

- Change in formats of compressed files.

As for formats of the compressed files which were attached to spear phishing e-mail, the proportion of executable files was high from 2013 through 2015. In 2016, script file[7] emerged, and in 2017, the proportion of script files increased.

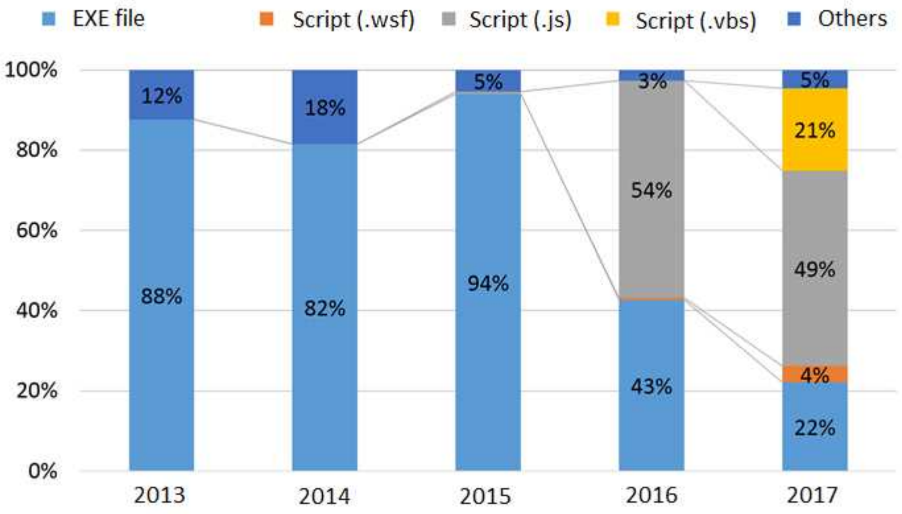


Figure 8 [Percentage of formats of compressed files attached to spear phishing e-mails]

[6] *D*ynamic *D*ata *E*xchange. A method of interprocess communication between applications in the Windows OS.

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

b. Efforts

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

The Japanese police encouraged hosting server businesses to take down C2 servers[8] which had been identified through the analysis of malware used in cyber-attack cases. Sixty one C2 servers were taken down in 2017.

(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 response exercises with relevant organizations on the supposition of cyber-attacks and information sharing with relevant organizations in the countries that had hosted the Olympic and Paralympic Games before.

【Examples of joint response exercises preparing for the Tokyo 2020 Olympic and Paralympic Games】

- In June 2017, the Metropolitan Police Department conducted the joint response exercise with the Organizing Committee of the Tokyo 2020 Olympic and Paralympic Games, critical infrastructure operators and so on, in the Tokyo Stadium that would be the venue of the Games, on the supposition of power cut and disrupted train services due to cyber-attacks.
- In December 2017, the Chiba Prefectural Police conducted the joint response exercise with organizations concerned in the *Makuhari Messe*, that would be the venue of the Tokyo 2020 Olympic and Paralympic Games, on the supposition that a terrorist group with intent to disrupt a large scale event in the *Makuhari Messe* had planted explosive devices there and had shut down the control system of power supply and lighting by cyber-attacks.

[8] Command and control server. It might be abbreviated to “C and 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.

2. Cybercrimes

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

The number of cleared cybercrime cases continued to increase to 9,014. And the number of consultation regarding cybercrime was 130,011, still remaining at a high level.

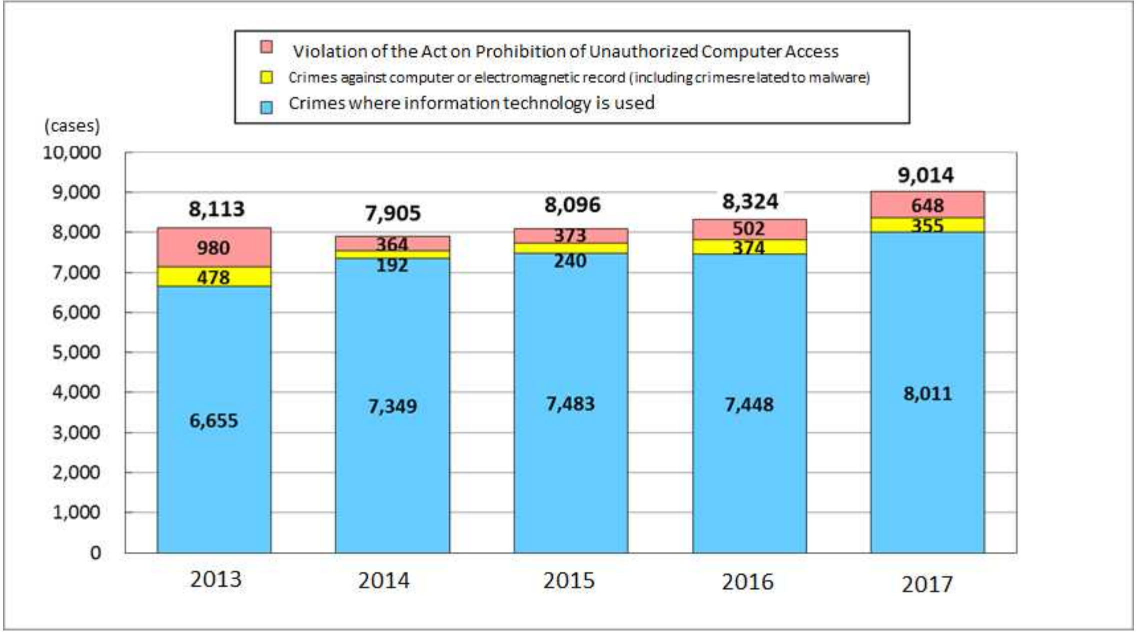


Figure 9 [The number of cleared cybercrime cases]

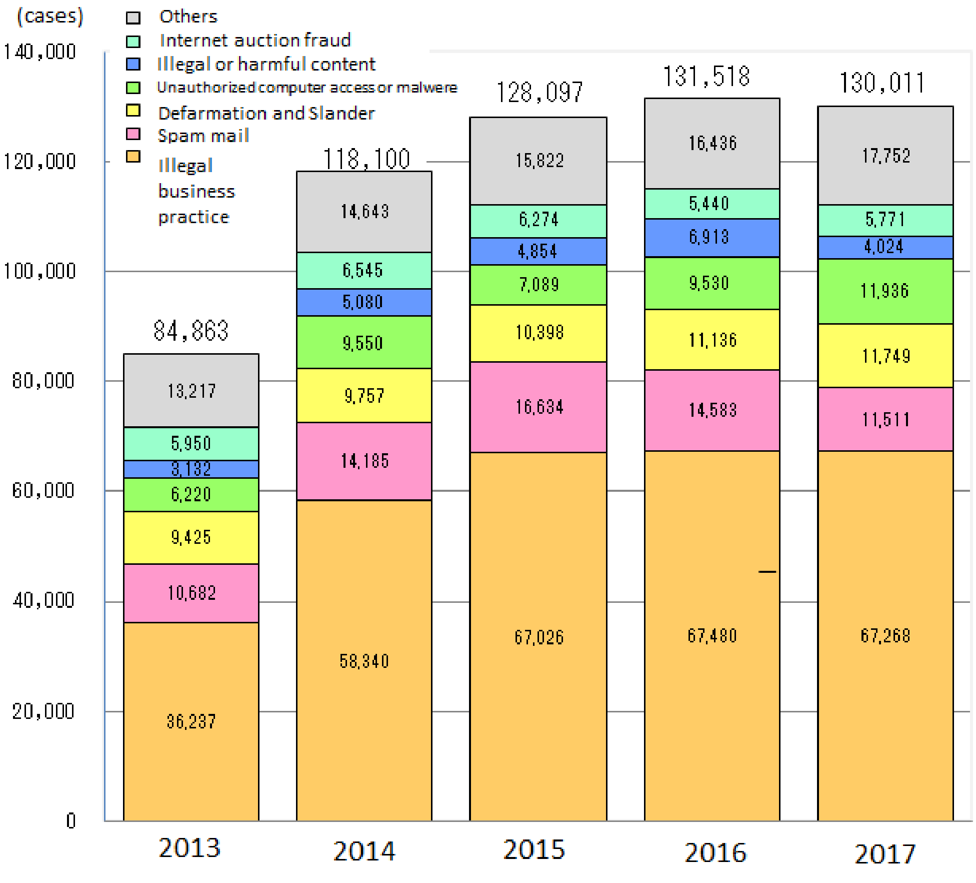


Figure 10 [The number of consultation regarding cybercrime]

(2) Situation of online banking fraud

a. Overview

The number of online banking fraud cases was 425, and the amount of damage was about 1,081 million yen (about 10 million US dollars). The number of cases decreased to less than a quarter of the highest record in 2014, and the amount of damage decreased to about one third of the highest record in 2015.

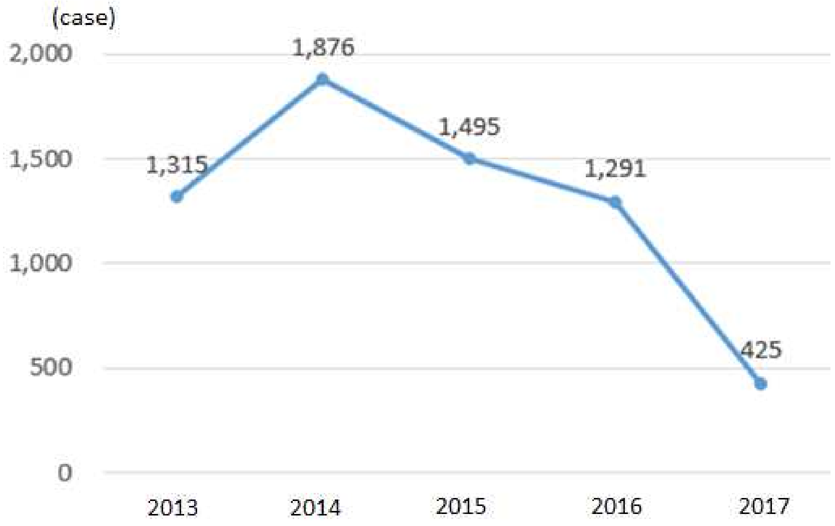


Figure 11 [The number of online banking fraud cases]

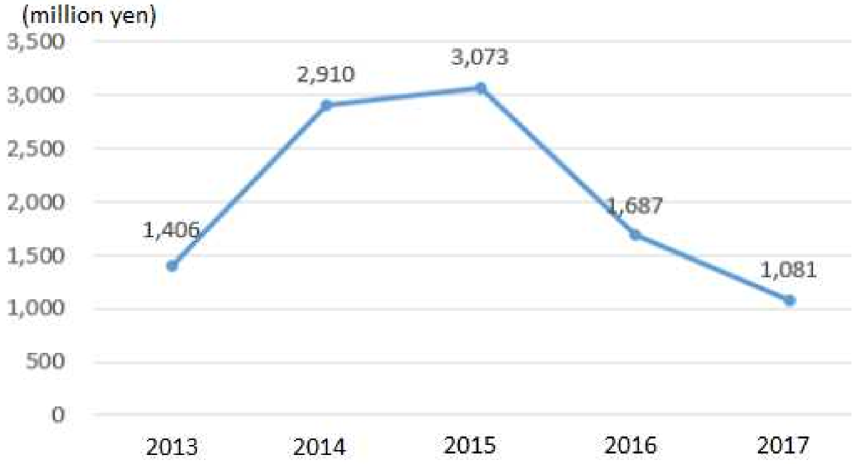


Figure 12 [The amount of damage of online banking fraud]

b. Characteristics

- Significant decrease in damage at major banks.

The damage decreased in recent years mainly at major banks due to the countermeasures such as enhancement of monitoring[9] and the launch of onetime password authentication.

- Unauthorized wire transfer by the new modus operandi that a suspect abuses electronic settlement service system.

After accessing unlawfully to victim’s PC used for online banking, a suspect, using electronic settlement service system, transfer money, as fund for purchasing virtual currency, from victim’s account to a cash account which the suspect had already opened at a virtual currency exchanger. Damage caused by this new modus operandi amounted to 212 million yen in total.

- Unauthorized wire transfer by the new modus operandi that a suspect drags a onetime password out of a victim.

Damage caused by the new modus operandi that a suspect dragged a onetime password out of a victim amounted to 34 million yen in total.

- 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 59%, China 20%, and Japan 12% of 765 accounts which were identified as the first destination accounts for the unauthorized wire transfer.

c. Clearance of related cases

The Japanese police cleared 49 cases, and the number of suspects arrested or whose cases were sent to public prosecutors offices, for trading financial institution accounts in connection with unauthorized wire transfer, was 77.

(3) Situation of clearance of unauthorized computer access

a. Clearance

- The number of suspects arrested or whose cases were sent to public prosecutors offices for violation of the Act on Prohibition of Unauthorized Computer Access continued to increase to 255, and the number of cleared cases in 2017 was 648, which was the second highest in past 5 years following the number in 2013.

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

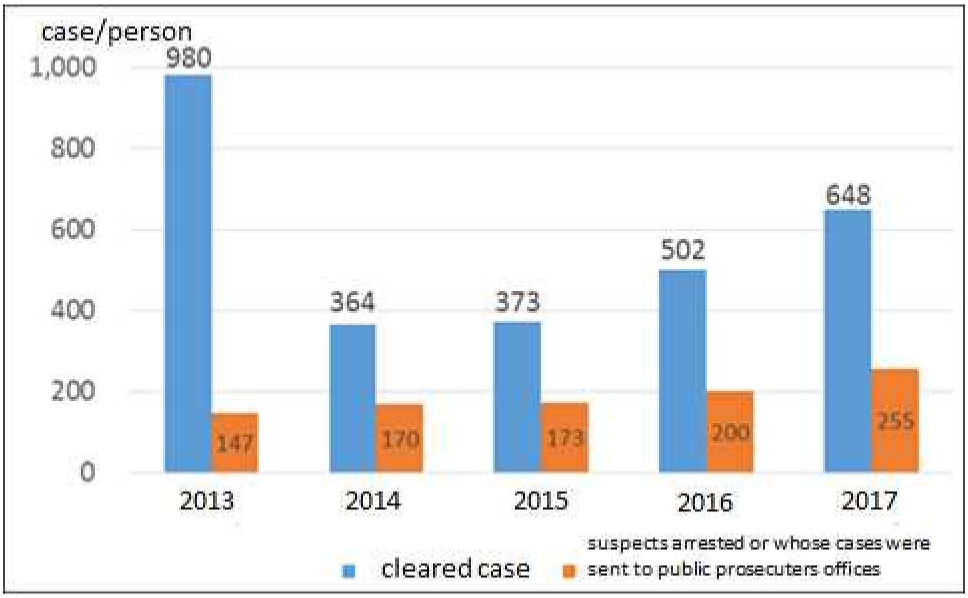


Figure 13 [Clearance of the violation of the Act on Prohibition of Unauthorized Computer Access]

- As for the number of cleared cases classified by acts of violation, the number of acts of unauthorized computer access was 599, and was the most numerous. 545 cases out of 599 were classified as the identification-code-abuse type[10].
- The most frequently committed modus operandi for unauthorized computer access is to take advantage of lax password management.

As for a breakdown of modus operandi concerning identification-code-abuse-type acts of unauthorized computer access, the most frequently committed modus operandi was to take advantage of lax password management, and the number of cases where this modus operandi was used and which were cleared in 2017 was 230. The acts by ex-employees or friends who were in a position to know an identification code were in the second place, and the number of cases where this modus operandi was used and which were cleared in 2017 was 113.

- The most abused service was "Online gaming and its community websites."

As for a breakdown of services which were abused by suspects, concerning identification-code-abuse-type acts of unauthorized computer access, the most abused service was online gaming and its community websites, and the number of cases where this service was abused and which were cleared in 2017 was 210. Website service dedicated to members or employees of a company was in the second place, and the number of cases where this service was abused and which were cleared in 2017 was 116. E-mail was in the third place, and the number of cases was 92.

- The age of offenders ranged widely.

The age of offenders violating the Act on Prohibition of Unauthorized Computer Access,

[10] 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

who were arrested, whose cases were sent to public prosecutors offices, or whose cases, juvenile delinquency cases, were sent to child consultation centers ranged widely from 13 to 60.

b. Unauthorized transmission of virtual currency caused by unauthorized computer access to virtual currency exchangers.

- The number of reported cases was 149, and the total amount of damage was about 662.4 million yen.
- Although most of the virtual currency exchangers introduced two-factor authentication[11], and recommended their customers to use it, few customers used it. In the 122 cases (81.9%) that were reported to the police out of 149, the customer used only ID-and-password authentication.

(4) Efforts

- Countermeasures, with public-private partnership, against tampering with websites to infect computers.

The Chiba Prefectural Police, forming a partnership with the Japan Cybercrime Control Center (JC3, a private foundation) analyzed information provided by the JC3. They established a technique to confirm authenticity of websites. And the police took such countermeasures that 38 prefectural police provided guidance for website administrators.

- Countermeasures against leaked IDs and infected computers which were found out in the international effort.

The international effort “Operation Avalanche” that was carried out mainly by German police helped the Japanese police acquire information on leaked IDs and passwords of online banking customers and information on virus-infected computers, and the Japanese police, cooperating with ministries, agencies and other organizations, urged online banking customers and users of the virus-infected computers to draw attention to prevent further damage.

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

Since the sharp increase in the infection with the malware “DreamBot” was confirmed, 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, 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

[11] An authentication method that 2 out of 3 factors, used in an authentication of a person, (something only the person knows, something only the person has, and characteristics of the person him/herself) are used. For example, an authentication by smartphone apps which only the person has is added to an ID-password authentication process.

tools, to the APWG[12]. And Prefectural Police urged administrators of the websites (which were manipulated to redirect signals transmitted from customers of online shopping site to fraudulent websites) to draw attention. In addition, 20 Prefectural Police, on the basis of information provided from the JC3, carried out investigation on account holders of destination accounts which were wrongfully used in the fraudulent websites.

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

The NPA requested financial institutions, the electronic settlement service system management organization and virtual currency exchangers to enhance monitoring their transactions, to urge their customers to use a onetime password and two-path authentication[13], and to implement thoroughly customer identification.

(End)

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

[13] 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.