Threats in Cyberspace in 2020

The global COVID-19 pandemic has drastically changed our living environment. In Japan, the pandemic preventive measures such as the adoption of the 'new normal' and the promotion of the remote work and cashless payment have transformed the cyberspace into a highly public sphere, where the citizens engage in diverse online activities such as the daily communications and business transactions.

Under such circumstances, the threats in cyberspace remained grave in 2020. Numerous cyberattacks and cybercrimes with aggravated and sophisticated methods occurred domestically and internationally.

○ Threats in Cyberspace

In 2020, a high number of attacks exploiting vulnerabilities of software and systems as well as spear phishing email attacks to infect the targeted systems with ransomware have occurred.

Internationally, a cyberattack exploiting vulnerabilities of a major US infrastructure management firm to target the government agencies, as well as those targeting the development of COVID-19 vaccines were identified.

In Japan, multiple defense contractors and telecom carriers announced potential data leaks due to unauthorized external accesses, and major manufacturers reported personal data leaks consequent to infection of the company devices while used by the employees to access the social media platforms during the remote work.

Both domestically and internationally, cyberattacks targeting the government agencies and critical infrastructures, including those allegedly involving the state actors, have intensified.

The number of the alleged scanning practices in the cyberspace domestically detected by the National Police Agency of Japan(NPA) has constantly been on the rise, which include numerous access attempts related to the Mirai bot[*1] and access attempts to wide-ranging ports to explore vulnerabilities of the online devices and services, implying the spread of the preliminary activities to cyberattacks.

The number of cybercrime cases handled by the police in 2020 reached a record high. While the amount of loss from illicit transfers via online banking drastically declined from 2019, the year in which the relevant damage had burgeoned, the number of incidents has remained high with slight decrease. Many of the related losses were presumably caused by the same crime methods which had been observed since 2019, i.e. deceptive derivations from the SMS or e-mail texts to the phishing websites spoofed as the financial institutions.

*1 Malware targeting to compromise the IoT devices.

Additionally, surrogate SMS authentication incidents, which discredit the widely used online identification method and serve to provide the crime tools for remote frauds, have been identified.

To address these cyberthreats, the police issued warnings for critical infrastructures operators, and conducted joint drills simulating cyberattack incidents together with stakeholders of the Tokyo 2020 Olympic and Paralympic Games to enhance the responsive capacities.

The police also issued joint warnings with the Financial Services Agency on the methods of the mobile payment-based illicit transfers, and continued to advance countermeasures against the scam websites together with the Japan Cybercrime Control Center (JC3).

○ Advancement of Digital Society and Emerging Threats

As the adoption of remote work expands as part of pandemic prevention across the organizations, cyberattacks targeting the vulnerabilities of the remote work software and the weakly secured household remote work environments have been emerging. The NPA's Real-time Detection Network System has also detected surge in dubious access attempts to diverse destination ports targeting the remote desk top services. Such cyberattacks suspected of exploiting the remote work-related vulnerabilities may continue to occur.

Consequent to the enhanced intersystem coordination among the offices and affiliated companies, cyberattack incidents routed through the less secure business facilities such as branches or overseas offices have been identified. In the cyberattack incident reported in the US in December 2010, malicious codes embedded into the update batch for the products of a major IT infrastructure management firm led to the spread of vulnerabilities across its customers who had applied the update and an unprecedented scale of impact. Addressing the supply chain risks is becoming a critical issue.

Additionally, aggravation of damage and methods of ransomware remains a global issue. While the conventional extortion scheme of ransomware used to be encrypting the victims' critical data to demand ransom for decoding, more heinous double extortion cases have been observed recently, in which the perpetrators encrypt and steal the data for ransom demands and publish the data if the victims refuse to pay ransom. Spreading of these heinous methods such as the sale of ransomware and the double extortion schemes on the dark web has also been observed. In June 2020, ransomware which affects the industrial control systems was identified also in Japan.

As the use of cashless payment grows among the citizens, theft and unconsented linkage of the users' bank details with the bogus payment accounts to make illicit transfers have occurred in the smartphone payment services operated by the domestic providers. While the growth in cashless payment generate new services, measures to ensure security and prevent exploitation in addition to user convenience need to be

taken according to the potential threats.

A new delivery method to spread Emotet[*2] by sending password-protected Zip attachments was also observed. As these techniques to evade the network-based malware detection complicates the pre-delivery elimination of malware, potential expansion of damage remains of concern.

Other suspected cybercrime incidents observed in 2020 included the scam websites exploiting the face mask shortages and the spoofed subsidy application websites. Scam emails, websites or frauds, which attempt to capitalize on the public anxiety such as the COVID-19 infection status or vaccines may continue to flourish.

*2 Malware which steals the email destinations and content data sent by the computer users, to spread infection by generating and transmitting the fraudulent emails.

In January 2021, Europol announced takedown of the Emotet botnets through a joint operation among the Dutch, German, US, UK, French, Lithuanian, Canadian and Ukrainian authorities.

1 Major Incidents in 2020

(1) Cyberattacks

○ Japan

- Cyberattacks targeting defense contractors

  In January 2020, a defense contractor reported the potential data leak consequent to cyberattack, then the possible inclusion of defense data in the leak in February 2020. In November 2020, the same defense contractor reported that they had become the subject of another cyberattack and their domestic clients' bank account data had been leaked. The methods used in the November attack appeared different from those used in January and February.

- Cyberattacks targeting telecom carriers

  In May 2020, a major telecom carrier reported the possibility of partial data leak as their domestic servers were compromised through hacking into their overseas facilities. In July 2020, the same carrier further reported the potential exposure of internal files consequent to unauthorized accesses through exploitation of the BYOD[*3] devices on remote access.

- Cyberattacks targeting manufacturers

  In August 2020, a major manufacture reported the leak of their employees' personal data consequent to the social media-based social engineering. The manufacture commented that the infection spread as an affiliated company employee had accessed the social media platforms using a company device during the remote work, downloaded the viruses-containing files, then connected the infected device to the corporate network while in the office.

○ International

- Cyberattacks targeting COVID-19 vaccine development

  In July 2020, the US, UK and Canada issued an alert that a cyberattack group called APT29 (Cozy Bear, The Dukes)[*4] was attempting to steal the research data and intellectual properties related to the development of the COVID-19 vaccines. According to their information, APT29 is presumed to belong to the Russian intelligence, and allegedly engaged in cyberattacks targeting the government agencies and medical institutions.

---

*3 Abbreviation of Bring Your Own Device, i.e. employees' use of personal devices for business.

*4 APT groups is a generally used abbreviation coined by the security vendors to refer to the cyberattack groups who are globally recognized for conducting advanced persistent threat attacks. Many of the APT cyberattack groups are allegedly state-sponsored.

・ US DOJ indictment against Chinese hackers

In July 2020, the US DOJ announced indictment of two Chinese nationals over allegation of conducting cyberattacks against businesses, government agencies and NGOs. The hackers were allegedly exploring network vulnerabilities of the companies related to the development of the COVID-19 vaccines on behalf of the Chinese government agencies.

・ US DOJ indictment against GRU hackers

In October 2020, the US DOJ announced indictment of 6 hackers belonging to the GRU (Russian Main Intelligence Directorate) over allegation of involvement in the cyberattack against the Pyeongchang Winter Olympic Games. The hackers were allegedly engaged in cyberattacks targeting the IOC staff and intrusion into the computers using malware called the "Olympic Destroyer".

・ Cyberattacks exploiting vulnerabilities of the IT infrastructure management software

In December 2020, the US CISA issued an alert that the US government agencies and the critical infrastructure operators were being struck by cyberattacks which exploited vulnerabilities of the products of a major IT infrastructure management software firm, and called for application of necessary measures. Further in January 2021, the US FBI and CISA issued a joint statement alleging the potential involvement of Russia in the said incidents.

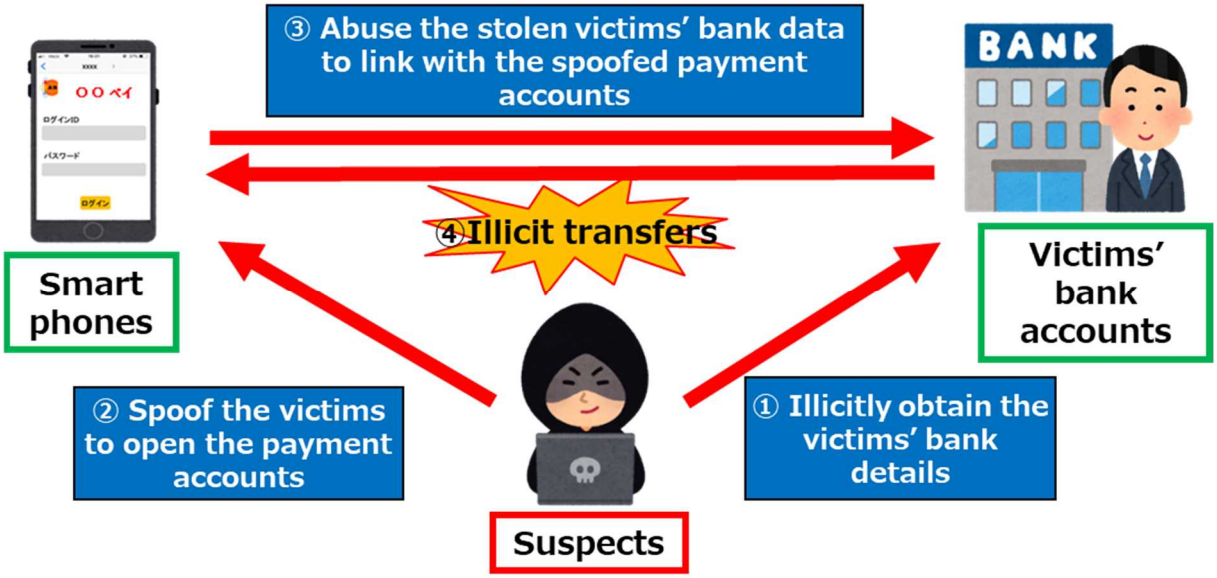
(2) Cybercrimes

○ Ransomware infection targeting businesses

In November 2020, an alleged double-extortion incident occurred, where a major company was struck by ransomware, the personal data they had possessed was stolen and encrypted, and the company was threatened to pay ransom in exchange for not disclosing the stolen data.

○ Illicit transfers via smartphone payment services

In September 2020, incidents involving the theft and unconsented linking of the victims' banking data to the bogus payment accounts and consequent illicit transfers over the smartphone payment services were detected.

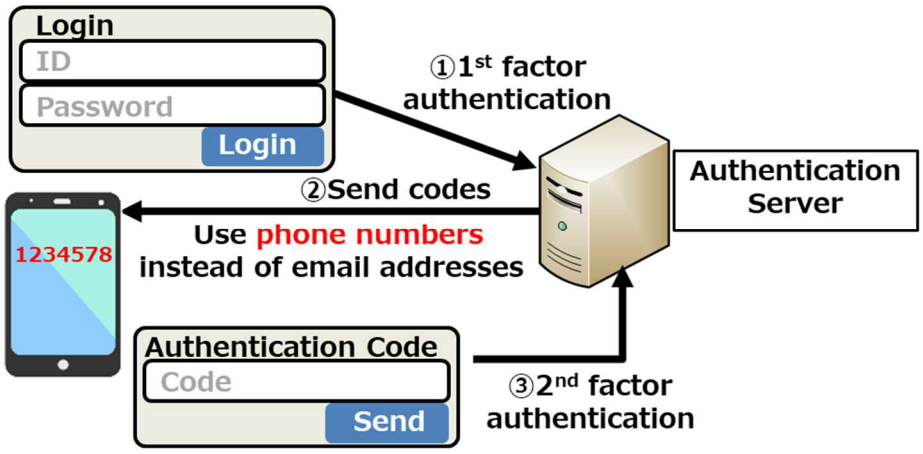


【Fig. 1: Illicit remittance via smartphone payment services】

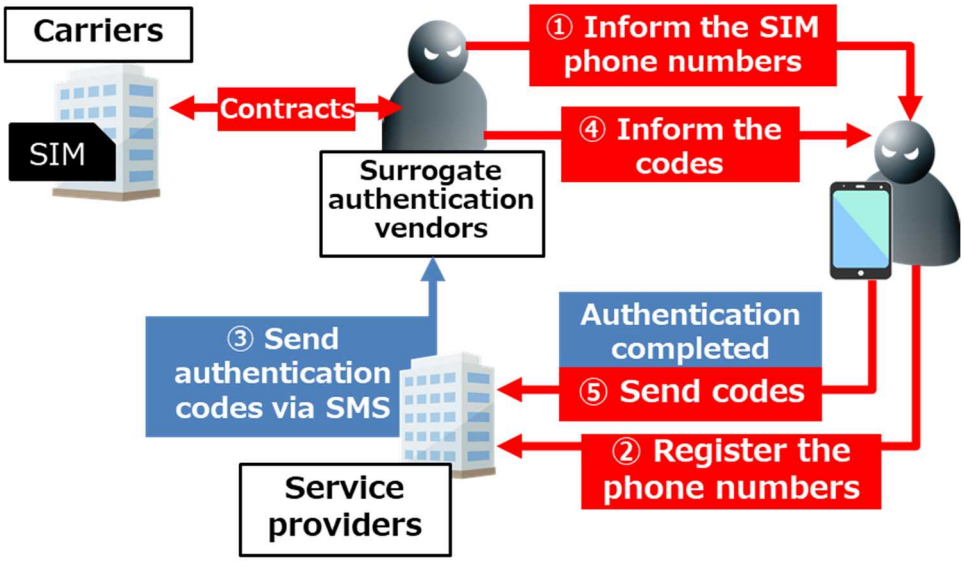
○ Surrogate SMS authentication abusing data SIM cards

In February 2020, a surrogate SMS authentication incident was detected, which abused unidentified SIM cards with SMS function to sell the phone numbers and authentication codes for creating the IP phone app accounts detached from the actual users.

In this case, approx. 100 SIM cards were abused to provide the fake mobile phone numbers and authentication codes. Some of the fabricated numbers were found to have been used for the IP phone apps involved in the remote scams.



SMS authentication mechanism



Surrogate SMS authentication

【Fig. 2: SMS authentication mechanism & surrogate SMS authentication】

○ Illicit withdrawals abusing official banking apps

16 illicit withdrawal incidents in June and 27 incidents in July 2020 were detected, where the unconsented withdrawals[*5] from the victims' bank accounts had been made through illicit activation of the official banking apps and abuse of their cardless payment functions resulting in approx. JPY14,000,000 loss.

○ Illicit sale and transfer of financial assets

During July and September 2020, 7 incidents which resulted in approx. JPY100,000,000 loss were detected. The new crime method involved unauthorized accesses to the victims' brokerage accounts for unconsented transfers and withdrawals of their financial assets to and from the illicitly opened bank accounts.[*6]

(3) Malware Analysis

○ Malware targeting ICSs

In June 2020, the NPA analyzed potential ransomware which targets the Industrial Control Systems (ICSs) regulating the factory lines by using a large-scale ICS simulator, and found that the malware appeared to be designed to run only on the targeted companies' corporate networks.

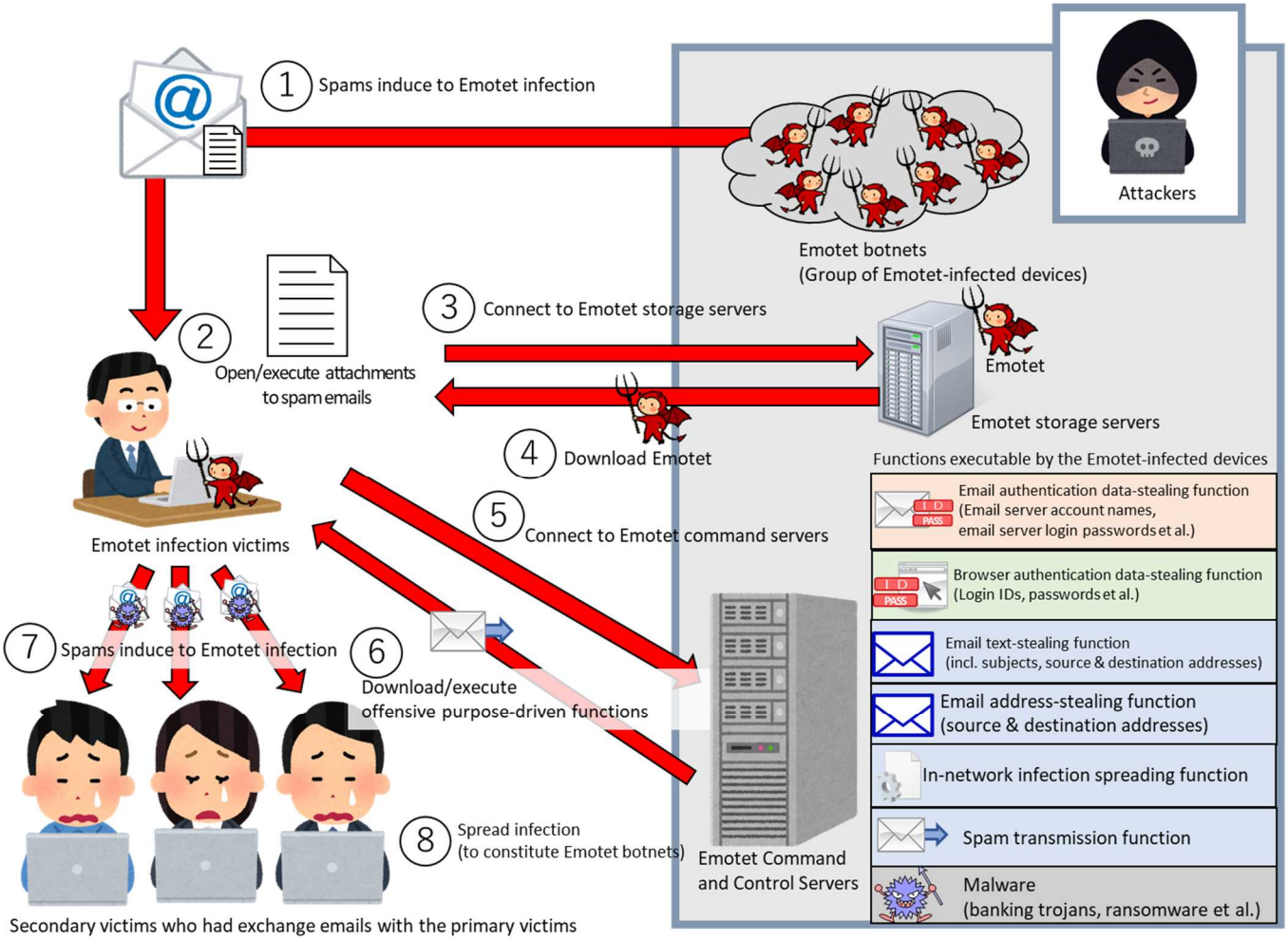
---

*5 As the incidents involve no transfers to other bank accounts, these incidents are not included in the case numbers and damage amounts of the online banking-related illicit remittance stats.

*6 As the incidents involve the sale of financial assets from the brokerage accounts, they are not included in the case numbers and damage amounts of the online banking-related illicit remittance stats.

○ Emotet Malware

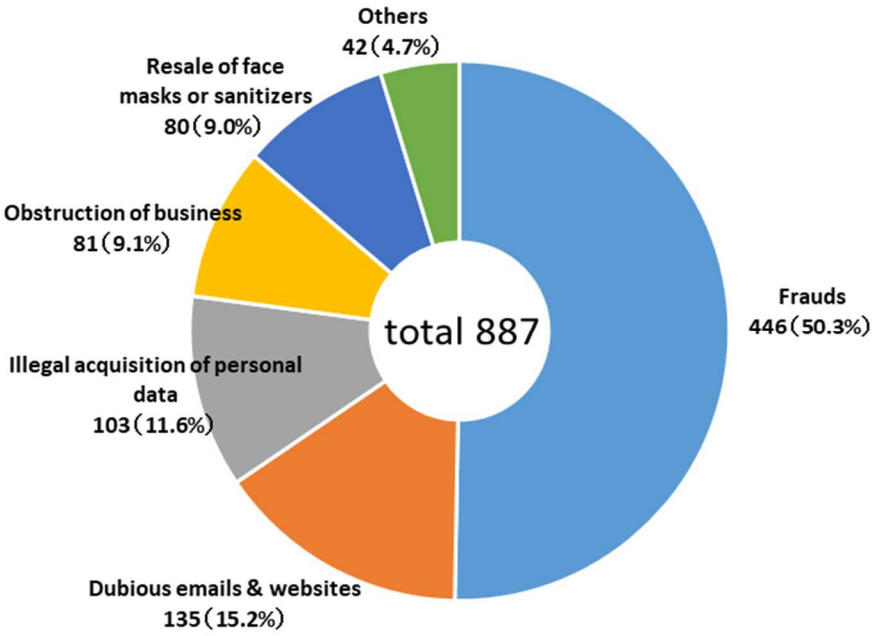
The NPA obtained and analyzed samples of Emotet malware which is mainly delivered through email attachments, and found that Emotet has the functions to steal data such as the email accounts, passwords and email content from the infected devices to transmit the fabricated emails to spread the infection.



【Fig. 3: Emotet's Operating Mechanism】

(4) Incidents potentially related to the COVID-19 pandemic

887 incidents reported to the metropolitan and prefectural police departments were identified as potentially related to the COVID-19 pandemic. Among the incidents, 446 fraud cases topped at 50.3% followed by 135 cases of dubious emails and websites at 15.2%.



【Fig. 4: No. of reported cybercrimes allegedly related to COVID-19】

○ Reported incidents

・ Fraud

Victims who had ordered face masks through e-commerce websites and paid to the designated bank accounts never heard back from the sellers even after the planned shipping dates nor received the products.

・ Dubious emails & websites

Victims received emails stating that ‘We are keeping subsidy for you. As we will remit the money to your account, please reply to this email if you wish to have more information.’

・ Illegal acquisition of personal data

Victims who had received emails spoofed as coming from the Ministry of Internal Affairs and Communications (MIC) stating that ‘We will pay you the 2nd Special Cash Payment’, accessed the designated URL and filled in their credit card details had the last stolen.

(5) Police Endeavors

○ Warning for critical infrastructure operators

In 2020, the police issued warnings to the pharmaceutical companies about cyberattacks related to COVID-19 vaccine development, and to the critical infrastructure operators about vulnerabilities of the online conference systems and of the IT infrastructure management software.

○ Conducting joint response drills

In 2020 as well, the police conducted joint response drills simulating occurrence of cyberattacks with the critical infrastructure operators and the stakeholders of the Tokyo 2020 Olympic and Paralympic Games. Specifically, the joint drills simulated malware infection of the remote work devices and the cyberattack-induced blackout targeting the Tokyo Games to enhance the response capability.

○ Takedown of C2 servers[*7] used for cyberattack

The police promoted nullification of the C2 servers identified through malware analysis as abused for cyberattacks by requesting the server hosting operators to delete the stored malicious contents and take down the abused servers, leading to disablement of 89 C2 servers.

○ Warning about the illicit transfer methods through the smartphone payment services

In cooperation with the Financial Service Agency and other stakeholders, the police issued warnings about the illicit transfer methods which involve unconsented obtainment of the user data from the bank accounts linked to the smartphone payment services to make illicit transfers of the victims' assets.

○ Encouragement for financial institutions and remittance operators to enhance security measures

For financial institutions and remittance operators intensely abused for the online banking-based illicit transfers, the police encouraged confirmation and enhancement of preventive measures such as the enhanced monitoring and user identification, as well as adoption of one-time passwords and two-factor authentications.

○ Audiovisual publication on data security

To prevent damage from phishing by disseminating the recent threats in cyberspace, the police publicized audiovisual contents on the NPA website specifically informing crime methods such as the Package Delivery SMS Spams intended to mislead the recipients to the scam websites, and countermeasures against phishing.

○ Joint alert with JC3 against tech support scam websites[*8]

To alert against the ongoing tech support scam, Yamagata prefectural police department jointly

---

*7 C2 servers here refer to the Command and Control Servers, occasionally abbreviated as the "C&C servers" as well, which function as the central controllers of the malware-infected devices by sending out commands to remotely manipulate the latter.

*8 Tech support scam here refers to the crime methods which display the false security warnings on the screens to foment anxiety of the users to make them call the displayed telephone number and purchase the unnecessary software or false support contracts.

produced awareness-raising videos with the JC3, and publicized them on the respective websites.

○ Joint countermeasures with JC3 against e-commerce scam websites

The NPA implements preventive measures against e-commerce scam websites by utilizing the tools respectively developed by Aichi and Saitama prefectural police departments in collaboration with the JC3 to report the scam websites' URLs detected by the JC3 to pertinent organizations including the APWG[*9].

○ Warnings against scam emails soliciting access to false subsidy application websites

The police and the JC3 jointly issued warnings on the JC3's website about the crime method of sending emails spoofing the Ministry of Internal Affairs and Communications (MIC) to solicit access to the false subsidy application websites.

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

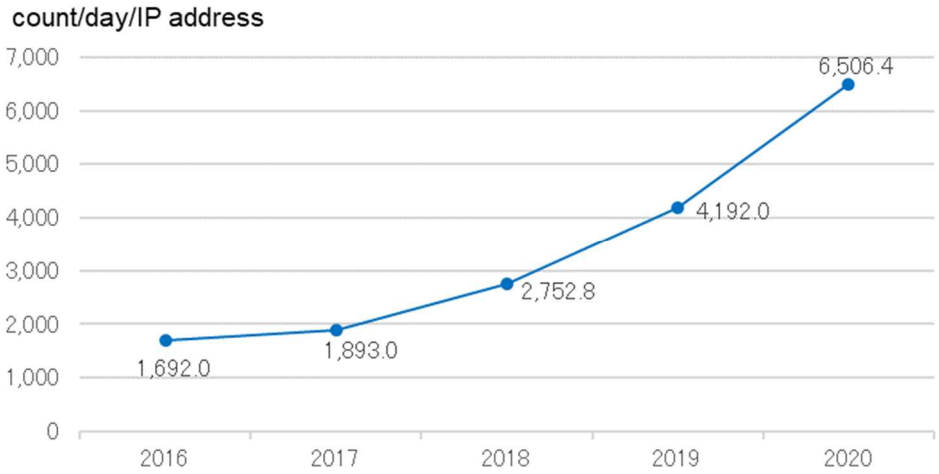
2 Threat in Cyberspace

(1) Monitoring of vulnerability scanning in the cyberspace

A) Unexpected connection attempts

The NPA places the sensors at the Internet connection points of the police institutes throughout Japan and operates the Real-time Detection Network System around the clock. The NPA aggregates and analyzes the extraordinary connection data detected at these sensors. Majority of dubious access attempts detected by this system appear to be cyberattacks targeting unspecified number of IPs, and vulnerability scanning of the networked devices preliminary to cyberattacks.

The number of unexpected connection attempts detected at the sensors has risen to 6,506.4 per IP address per day in 2020, showing an upward trend. Reasons for surge in extraordinary access attempts may include the increase of potential targets brought by the diffusion of IoT devices, and continual evolvement of the attackers' systems including the devices and servers abused as attacking proxies.



【Fig. 5: No. of unexpected connection attempts detected at the sensors】

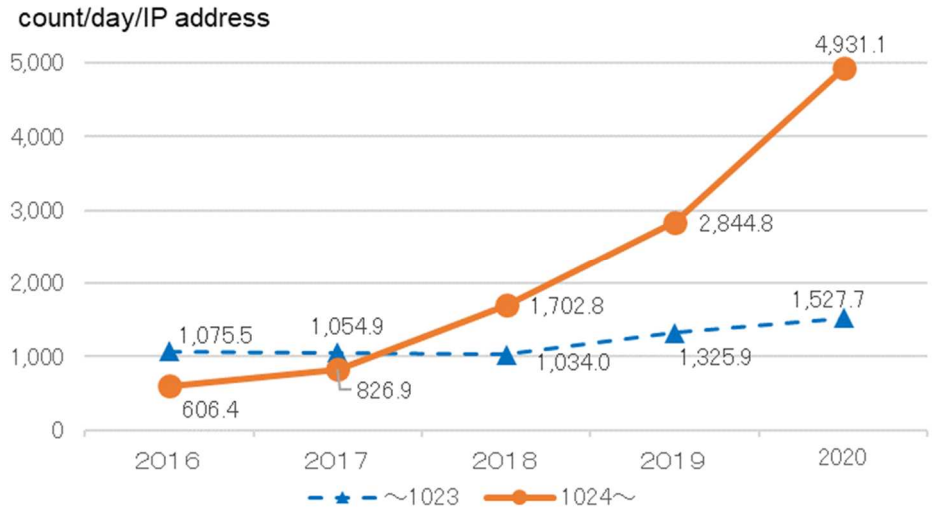
B) Major Observations

○ Surge in originating IPs attempting access to wide-ranging destination ports

Among the detected target destination ports[*10], the continual rise in number of access attempts to port 1024 and above have been a major driver for the overall surge in suspicious access attempts. As ports 1024 and above are mainly used by the IoT devices in the standard configurations, majority of these access attempts are alleged to be vulnerability scanning of or cyberattacks against the IoT

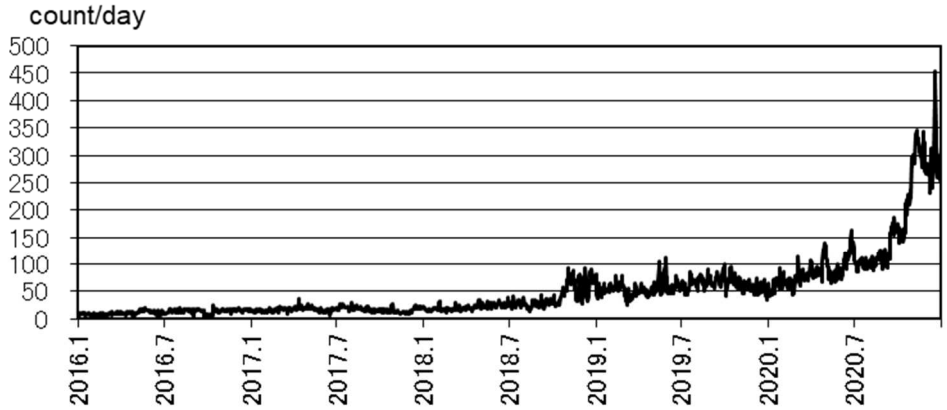
*10 The ports here refer to the computer interfaces identifying protocols to be applied in the TCP.UDP/IP communications. A number from 0 through 65535 is assigned to each port.

devices.



【Fig. 6: No. of unexpected incoming packets by destination port per IP address in a day】

In recent years, suspicious access attempts from particular IPs to wide-ranging destination ports are also on the rise. The number of originating IPs hitting over 100 destination ports per day had remained at the same level from 2016 through the 1st half of 2018, started rising from the 2nd half of 2018, then proliferated in the 2nd half of 2020. The number of IPs detected as origins of suspicious access attempts in 2020 reached 135.5 per day, increasing from 59.1 per day in 2019 by 76.4 per day (129.3%).

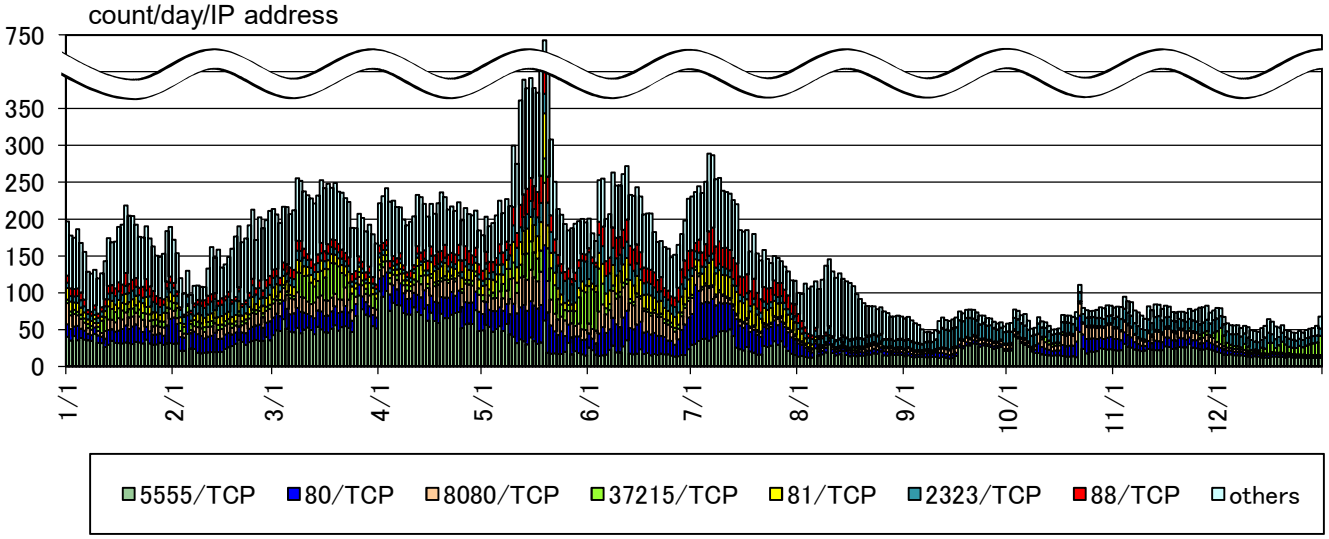


【Fig 7: No. of originating IP addresses attempting to access 100+/day destination ports】

The background of the surge in access attempts to wide-ranging destination ports is alleged to be the increase of groups who aim to exhaustively and quickly assess the devices connected to the Internet, the online services they provide with and the presence or absence of their vulnerabilities.

○ Access attempts targeting vulnerabilities of IoT devices

Daily average number of access attempts with characteristics of the Mirai bots in 2020 turned out to be 461.7 per IP address per day, down by 61.2 from 522.9 in 2019, however, a certain level of access attempts has continually been monitored since their outbreak in 2016. Among the targeted destination ports, surge in access attempts to port 37215/TCP used by the foreign-made routers started being monitored from the middle of May 2020, implying the potential exploitation of vulnerabilities to enable remote execution of any code to proliferate malware.



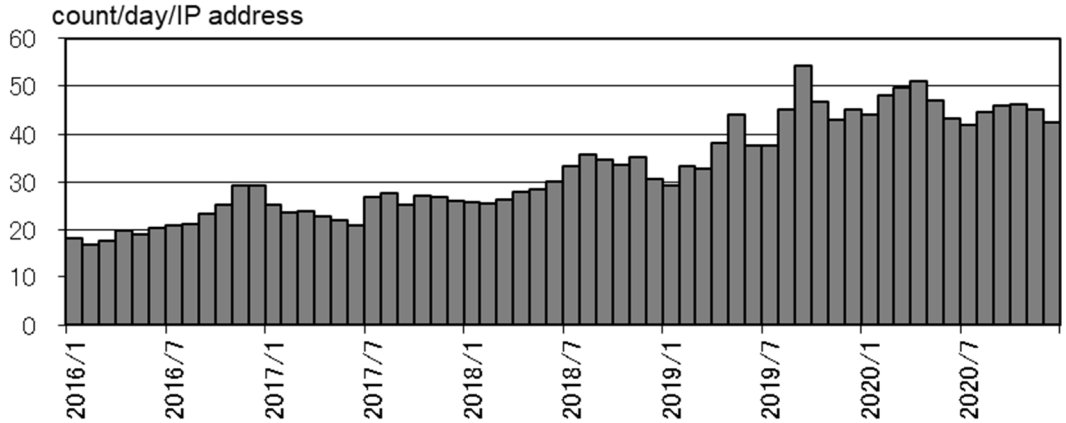
【Fig. 8: Access attempts with characteristics of the Mirai bots by destination port (except port 23/TCP)】

○ Access attempts to wide range of destination ports targeting Remote Desktop Services[*11]

From 2016 through 2020, access attempts to 3389/TCP, the standard Remote Desktop Services port used by Microsoft Windows for remote access, has been growing gradually.

In the middle of February 2020, sudden increase of access attempts to wide-ranging destination ports targeting Remote Desktop was also observed, which appeared to be exploring whether the Remote Desktop services were operating on the non-standard ports.

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



【Fig. 9: Access trend to Remote Desktop listening port TCP 3339】

(2) Spear Phishing Attack

A) Modus operandi of spear phishing attacks

The number of spear phishing attack*12 identified by the Japanese police through the Counter Cyber-intelligence Information-Sharing Network*13 in 2020 was 4,119.

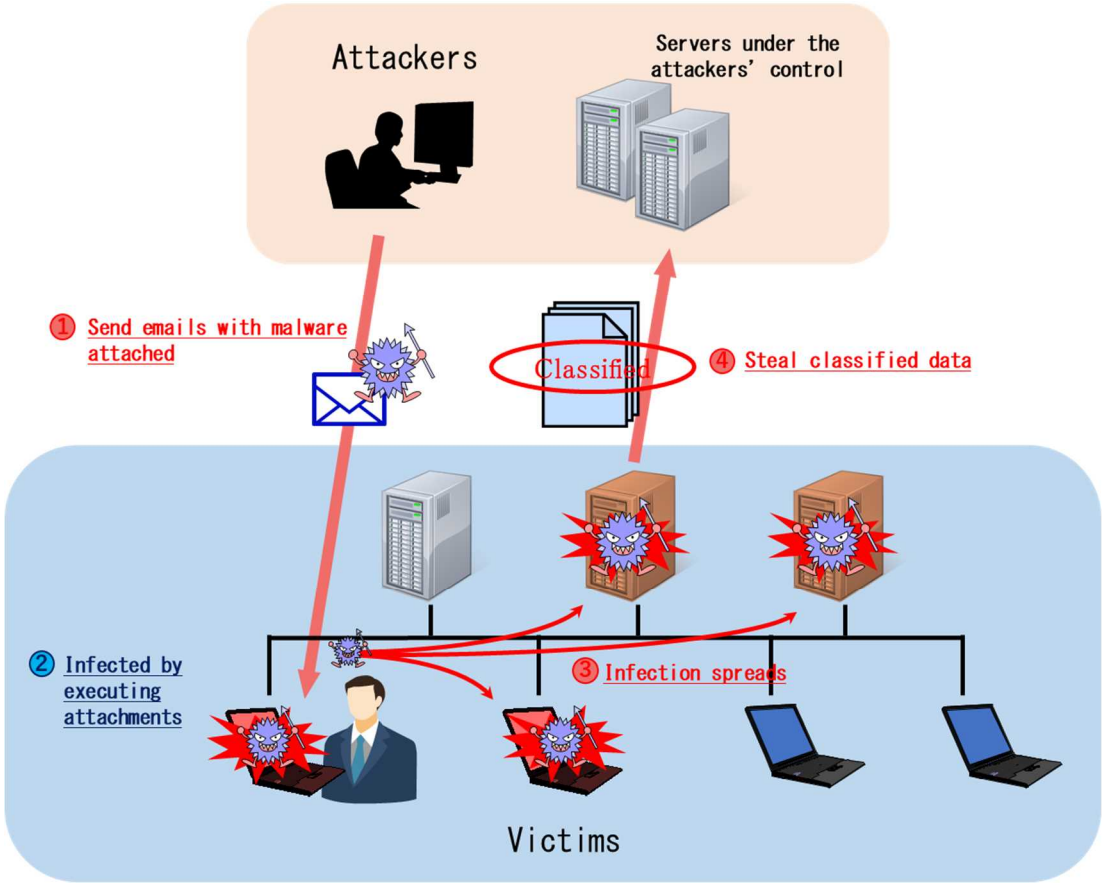
Major observations include the followings:

- "Indiscriminate" spear phishing attacks*14 account for 95% of the total spear phishing attacks.
- 75% of the entire spear phishing emails targeted the undisclosed email addresses.
- 97% of the originating email addresses of the spear phishing emails appeared to have been forged.

*12 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.

*13 A nationwide network which consists of the police and approximately 8,100 pertinent organizations (as of January 2021) 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 analyses on the spear phishing attacks against the governmental entities through this network in coordination with the National center of Incident readiness and Strategy for Cybersecurity (NISC).

*14 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.



【Fig. 10: Sample scheme of data theft by targeted email

B) Case Example

The following case is an example of the spear phishing email attack obtained through the Counter Cyber-intelligence Information-Sharing Network.

○ Emails disguised as Requests for Quotes (RFQs) to induce the recipients to open the compressed attachments were sent to manufacturers.


差出人: [redacted]
送信日時: 2020年11月16日月曜日 7:12
宛先: [redacted]
件名: 見積依頼
添付ファイル: PO-0905.zip

こんにちは

いつもお世話になっております。
見積依頼させて頂きたくご連絡致しました。

図面添付致しますのでご確認お願い致します。
以上、宜しくお願い致します。

****
[redacted]
〒[redacted]
[redacted]
TEl: [redacted] FAX: [redacted]
MOBILE: [redacted]
E-Mail [redacted]
****

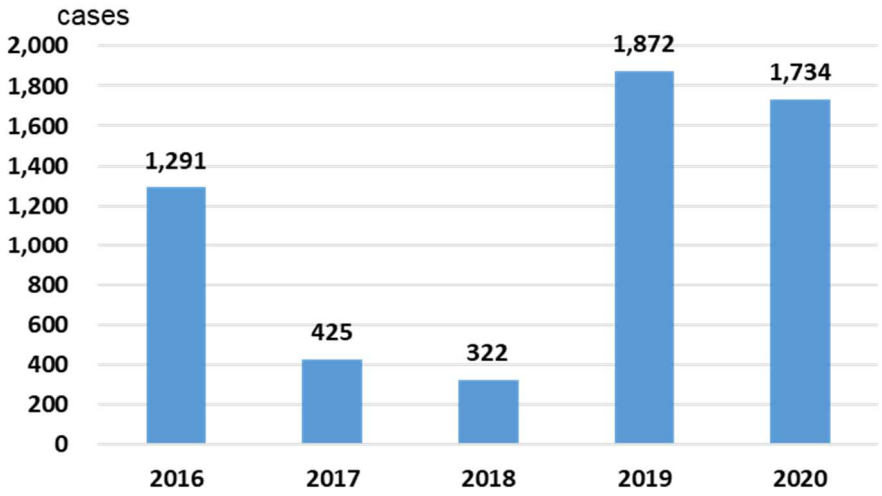
【Fig. 11: Sample of targeted attack emails】

Opening the attachments to or accessing the links embedded in the scam emails may lead to malware infection.

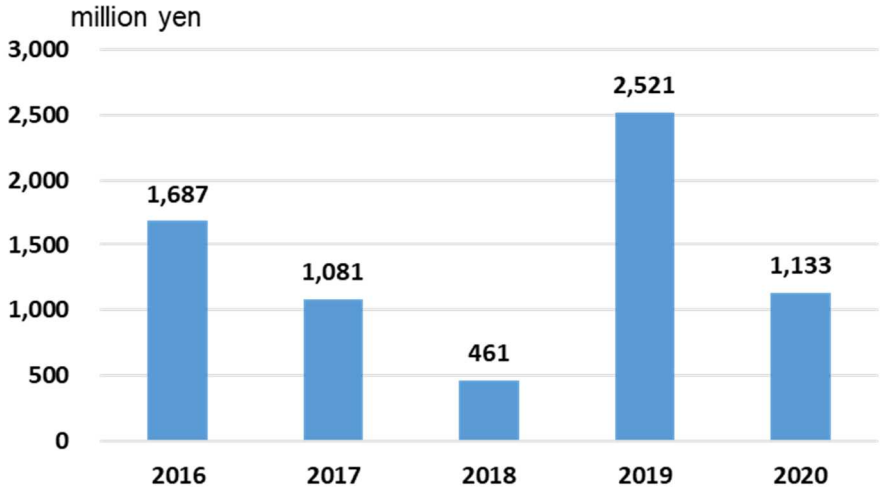
(3) Online Banking Fraud

A) Overview

The number of online banking fraud cases in 2020 was 1,734 with total loss of approx. 1.1 billion yen, both declined from those in 2019.



【Fig. 12: No. of online banking fraud】



【Fig. 13: Total loss from online banking fraud】

B) Major Observations

- The damage amount of the online banking fraud, which had proliferated in 2019, has significantly declined in 2020. However, the number of incidents remained at a high level with a slight decrease from 2019. The alleged crime method prevailing since 2019 is sending the phishing messages via SMS or email to mislead the recipients to the phishing websites disguised as those of financial institutions.

・ The identified crime methods include the use of Bank SMS scam and the Delivery SMS scam to mislead the recipients to the bank-disguised phishing websites. Another detected crime method abuses the scam SMS to coax the recipients to download the malware onto their devices, then misleads the potential victims to the phishing websites from the false message displayed by the said malware.

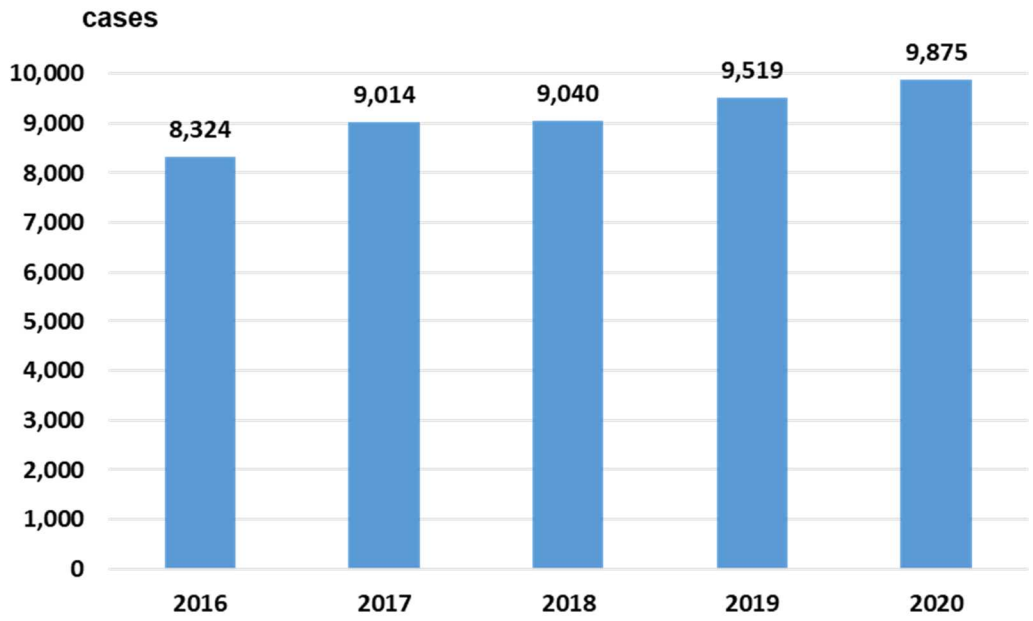
・ Of 2,181 accounts identified as the primary destinations of illicit remittances, 37.8% of the accounts were held by Japanese nationals, followed by 17.9% by Vietnamese and 2.4 % by Chinese.

Methods of online banking fraud have been diversifying. Besides the conventional illicit remittance to bank accounts, purchase of cryptoasset or e-money, and deposit to the prepaid cards have been detected.

(4) Cybercrime crackdown

A) The number of cleared cybercrime cases

The number of cleared cybercrime cases has been on the rise, reaching 9,875 in 2020, increasing from 2019.



【Fig 14: No. of cleared cybercrime cases】

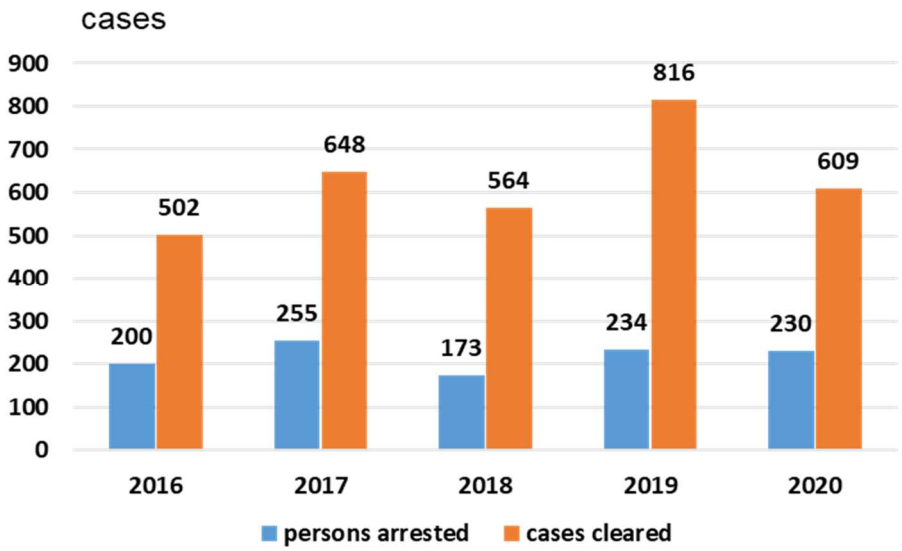
B) Violations of the Act on Prohibition of Unauthorized Computer Access*15

i. The number of cleared cases

The number of cleared violations of the Act on Prohibition of Unauthorized Computer Access reached 609 in 2020, declined from 2019.

ii. Major Observations

○ 576 of all the cleared cases were classified as the identification-code-abuse type*16 and accounted for approx. 94.6% of the total.



【Fig. 15: No. of cleared violations of the Act on Prohibition of Unauthorized Computer Access】

○ Passwords most stolen by phishing

Among the passwords theft methods for unauthorized accesses, 172 cases (29.9%) involved theft from the phishing websites, followed by 115 (20.0%) thefts through social engineering such as deceiving or peeping the authorized users.

○ Members/employees-only websites most abused

The services most abused by suspects of the password theft-based unauthorized accesses in

*15 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 .

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

2020 were the members/employees-only websites with annual 174 incidents (30.2%), followed by the online game community websites with 88 incidents (15.3%).

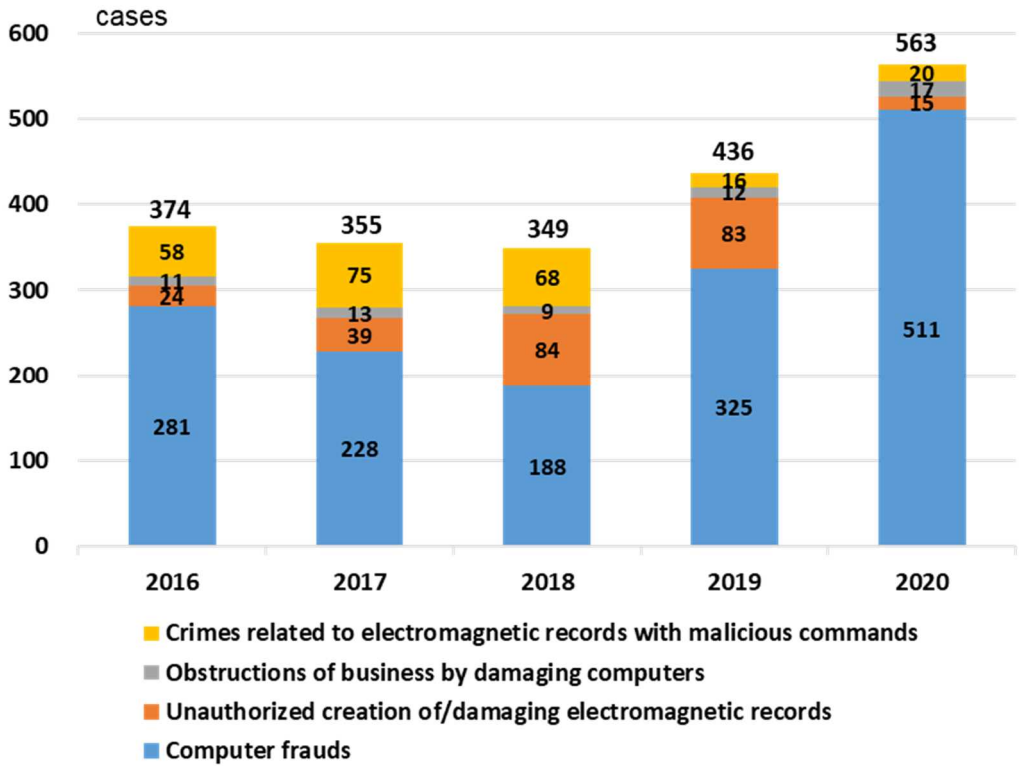
C) Crimes targeting computers or electromagnetic records*17

i. The number of cleared cases

The number of cleared cases regarding crimes targeting computers or electromagnetic records in 2020 was 563, increasing from 2019.

ii. Major Observations

The most dominant crime type among the cleared cases in this category was the computer frauds, reaching 511 cases and 90.8% of the total.



【Fig. 16: No. of cleared cases regarding crimes targeting computers or electromagnetic records】

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 2020 was 2,015, decreasing from 2019.

○ The number of cleared fraud cases accounted for 1,297, increasing from 2019.

*17 Crimes defined by the Penal Code as targeting computers or electronic records.

(5) Collaboration with Businesses

In response to the following comments from the business sector concerning the cybersecurity, the police have been enhancing collaboration with businesses and trade associations by signing pacts and setting up committees on cybersecurity as well as providing and sharing relevant information and alerts through the Council for Countermeasures against Cyber Terrorism*[18]:

- Due to the insufficiency of lendable routers for all employees caused by the sudden adoption of remote work, some staff are using their home routers.
- Recognition of cyberattacks is becoming increasingly difficult as the phishing emails are sent abusing the addresses used in business communications.
- The security levels of the overseas branches vary according to their scales. Evening the variations is a future issue.

○ Collaboration enhancement with the designated medical institutions for COVID-19

The Toyama prefectural police department has concluded an agreement with the Council of Toyama Public Hospital Directors, participated by 24 public hospitals in the prefecture including the designated medical institutions for COVID-19, to establish a reporting system to prevent the spread of damage from the pandemic-related cybercrimes through the provision of warnings and implementation of preventive trainings.

○ Establishment of an industry-government-academia Cybersecurity Council for collaboration enhancement among the diverse stakeholders

The Miyagi prefectural police department has been advancing collaboration with the Miyagi prefectural government through establishment of the Miyagi Cybersecurity Council composed of total 118 stakeholders including business operators and organizations, cybersecurity companies and educational institutions to enhance cybersecurity in the region and the society through the promotion of information sharing and implementation of lectures.

*18 The council consists of the prefectural police departments and pertinent organizations including major critical infrastructure operators which may be the target of cyberattacks. The council provides relevant information including about cyberattacks and also exercises joint drills.