# Threats in Cyberspace in 2021

With the progress of digitalization, cyberspace is acceleratingly becoming a public space. At present, cyberspace has comparable functions and roles to public facilities in real space such as schools, parks and libraries, which are broadly open to and used by citizens as places for social and economic activities. *1

While a wide range of people from children to elderly are participating in cyberspace, crimes exploiting new services and technologies are flooding with the increasingly malicious and sophisticated modus operandi.

In Japan, the number of cleared cybercrime cases in 2021 reached a record high of 12,209 as cashless payments spread. The threats in cyberspace remained grave in 2021 with the expanding ransomware damage, unauthorized accesses causing data leaks and cyberattacks conducted by state-sponsored groups.

The number of ransomware cases reported to the police during 2021 was 146, continuously increasing since the previous year, and their damage is widespread regardless of the size, or type of industry of the victim entities.

As the number of companies adopting VPN devices as part of their security measures is increasing due to the rapid expansion of the remote work-driven external connections to their internal networks, ransomware infections are mostly caused by infiltration into the organizations' internal networks through vulnerabilities in the VPN devices.

Furthermore, there have been cases of extensive damage, such as a case in which more than 2 months were required for restoring the infected systems, and one which costed more than 50 million yen for investigation and restoration. The police also confirmed cases where critical infrastructure operators were targeted and a serious impact on the citizens' lives was caused such as a ransomware attack against a medical institution, which encrypted the electronic medical records to be unbrowsable. As a result, the victim institution was forced to suspend acceptance of new or emergency patients.

Ransomware attacks, such as the attack against a U.S. oil pipeline in May 2021, are creating serious impacts on the lives of citizens around the world and addressing them is becoming an urgent global issue.

In response to the need for close international cooperation to tackle ransomware, the "G7 Extraordinary Senior Officials' Forum on Ransomware" was held in

---

*1 Cybersecurity Policy Council Report（December 2021）
（https://www.npa.go.jp/cybersecurity/CS.html）

December 2021 with the participation of law enforcement agencies from the G7 countries.

Cyberattacks continue to cause rash of datatheft. In 2021, a number of government agencies and research institutes in Japan received unauthorized external accesses, and personal data of their employees may have been stolen. There was also a case where the involvement of foreign country was revealed in the process of clarifying the details of cyberattacks.

In April 2021, the police concluded that the Chinese People's Liberation Army (PLA) Unit 61419 was likely behind a group which carried out cyberattacks against the Japan Aerospace Exploration Agency (JAXA) and other Japanese companies.

In December 2021, the police identified a person who had attempted to illegally obtain annual usage rights of a corporate edition antivirus software produced by a Japanese company under instructions from an individual allegedly related to the PLA. This investigation revealed a high possibility that the PLA is gathering various types of information on Japan.

In addition, the UK, the US and other countries issued public statements in July 2021, condemning China about a cyberattack group known as "APT40". Japan also issued a statement by the Press Secretary of Ministry of Foreign Affairs based on an assessment that the Chinese government is highly likely behind APT40.

The police announced that they will continue to work with the National center of Incident readiness and Strategy for Cybersecurity (NISC) to gather information and implement countermeasures in cooperation with other related organizations. The police also alerted businesses and provided information to each company that had been targeted of cyberattack.

The number of the alleged scanning practices in cyberspace domestically detected by the NPA has constantly been on the rise. A breakdown analysis of these accesses shows that the majority of them are from offshore, suggesting the continuous rise of cyberattack threats from offshore.

In addition, surge in the number of accesses targeting vulnerabilities of “Apache Log4j” was confirmed immediately after their announcement in December 2021.

During the Tokyo 2020 Olympic and Paralympic Games (the Tokyo 2020 Games) held from July to September 2021, all possible measures against cyberattack were taken including joint training exercises through public-private partnership and alerts to businesses involved in the Tokyo 2020 Games.

Consequently, no major cyberattacks which affected operations of the Tokyo 2020 Games occurred, despite the fake websites disguised as video streaming

channels of the torch relay and the opening ceremony, and the calls for cyberattacks targeting the Tokyo 2020 Games-related organizations placed on social media platforms were confirmed.

Many of online banking fraud cases appear to have been caused by the same technique used since 2020, i.e., use of the bank SMS scams, the delivery SMS scams or phishing emails to trick recipients into accessing phishing websites.

The number of reports about malicious shopping websites received by the Japan Cybercrime Control Center (JC3) through the Safer Internet Association (SIA) in 2021 reached 17,717, an increase of 7,622 from 2020. The JC3 attributes the increase to the expanded use of the Internet partly driven by the COVID-19 pandemic, as well as to a growing interest in reporting such websites.[*2]

The sense of cyber insecurity among the public is also growing as evidenced by the result of a public safety survey conducted by the NPA in 2021, where 79.4% of respondents mentioned that they were "concerned" or "somewhat concerned" about the risk of becoming a cybercrime victim.

In April 2022, the NPA established the Cyber Affairs Bureau and the National Cyber Unit in order to strengthen the ability to address the threats in cyberspace and to enhance international cooperation.

The NPA and the prefectural police departments will continue to work together in cyber investigations and countermeasures, while enhancing international cooperation and joint investigation, as well as the public-private partnerships to ensure the equivalent level of safety and security in cyberspace as in real space.

---

*2 JC3 “Statistics on malicious shopping websites”
https://www.jc3.or.jp/threats/topics/article-431.html

1 Threat trend in 2021

(1) Ransomware situation and countermeasures

A) Overview

Ransomware is a malware which infects devices to encrypt stored data to be unusable, then demands ransom in exchange for decrypting the data.

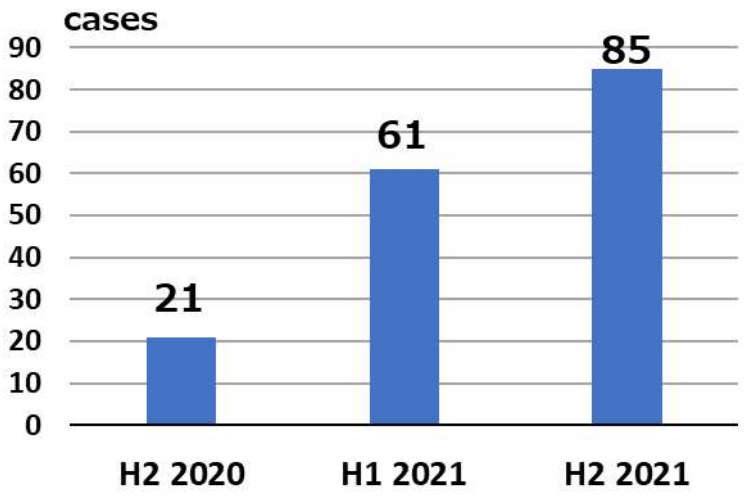
Previously, ransomware has tended to send e-mails targeting a large number of unspecified users. However, the current trend is that they are targeting specific individuals, companies or organizations by infiltrating through vulnerabilities in corporate network infrastructures including VPN equipment.

In many recent cases, the double extortion method, in which the perpetrators not only encrypt the victims' data, but also steal them and demand ransom, extorting "If you refuse to pay, we will expose your data".

B) Ransomware damages

i. Number of cases

In 2021, the number of ransomware cases reported to the NPA by the prefectural police departments was 146 (61 in the first half and 85 in the second half of 2021), indicating a continuous increase from 21 cases in the second half of 2020.




【Fig 1: No. of reported ransomware cases】

ii. Major Observation

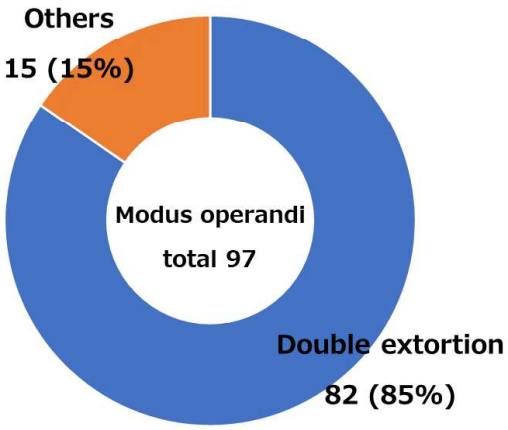
Double extortion is the most common cause of damage

○ Among the 146 cases of ransomware damage, the police could confirm that money was demanded in 97 cases, and the double extortion

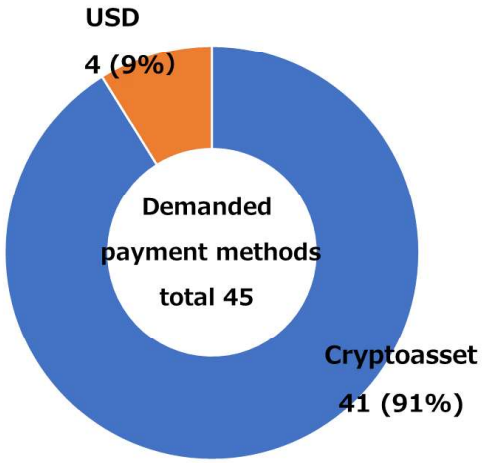
methods were used in 82 cases (85%).

○ Cryptoassets account for a large portion of money demands

Among the 146 cases of ransomware damage, 45 cases directly demanded money, of which 41 cases (91%) requested cryptoassets.



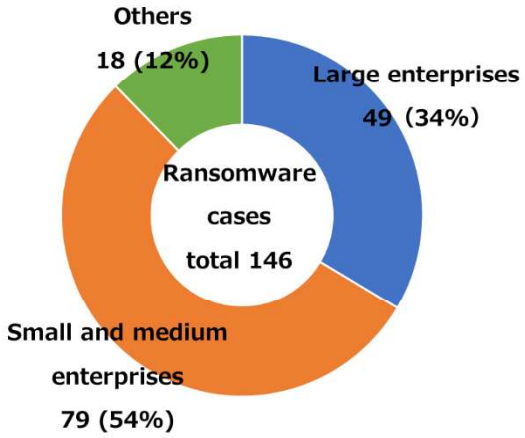

【Fig 2: No. of reported cases by modus operandi】




【Fig 3: No. of reported cases by demanded payment method 】

○ Entities of all sizes victimized

Figure 4 shows that a breakdown of the 146 ransomware cases by the size of the affected businesses[*3], in which large enterprises accounted for 49 cases, while small and medium enterprises accounted for 79 cases, indicating the occurrence of damage regardless of their business sizes.




【Fig 4: No. of reported cases by the size of victims】

---

*3 Classified in accordance with Article 2, Paragraph 1 of the Small and Medium-sized Enterprise Basic Act

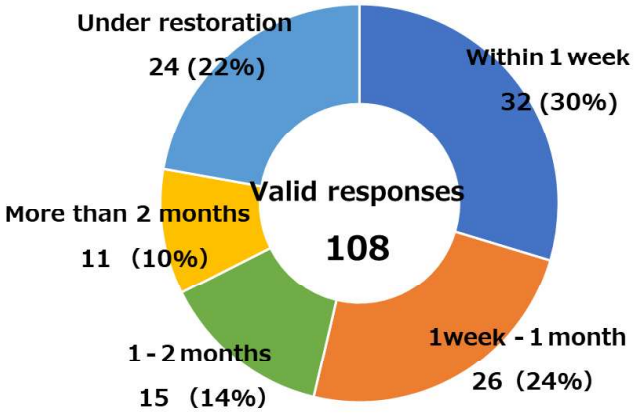
C) The state of ransomware damage

In order to grasp the actual damage by ransomware, the police sent a survey to 146 victim entities and received 123 responses by the deadline and analyzed them.

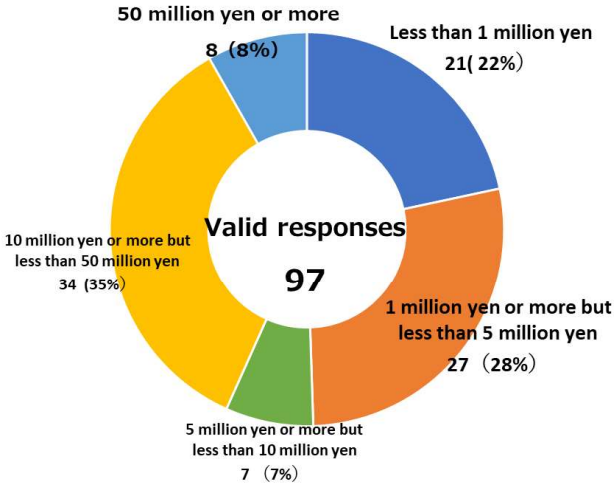
i. Time and costs required for restoration

Regarding the time required for restoration, 108 valid responses were received, of which 32 respondents took 1 week, while some others needed more than 2 months.

Regarding the total investigation and restoration costs incurred due to ransomware, 97 valid responses were received, of which 42 (43%) respondents paid 10 million yen or more.



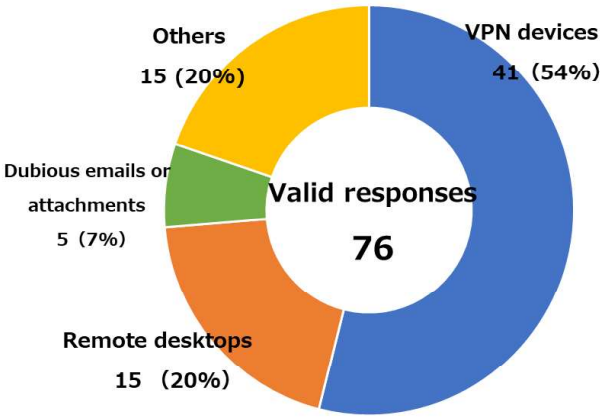

【Fig 5: Time required for restoration】




【Fig 6: Total cost of investigation and restoration】

ii. Infection Routes

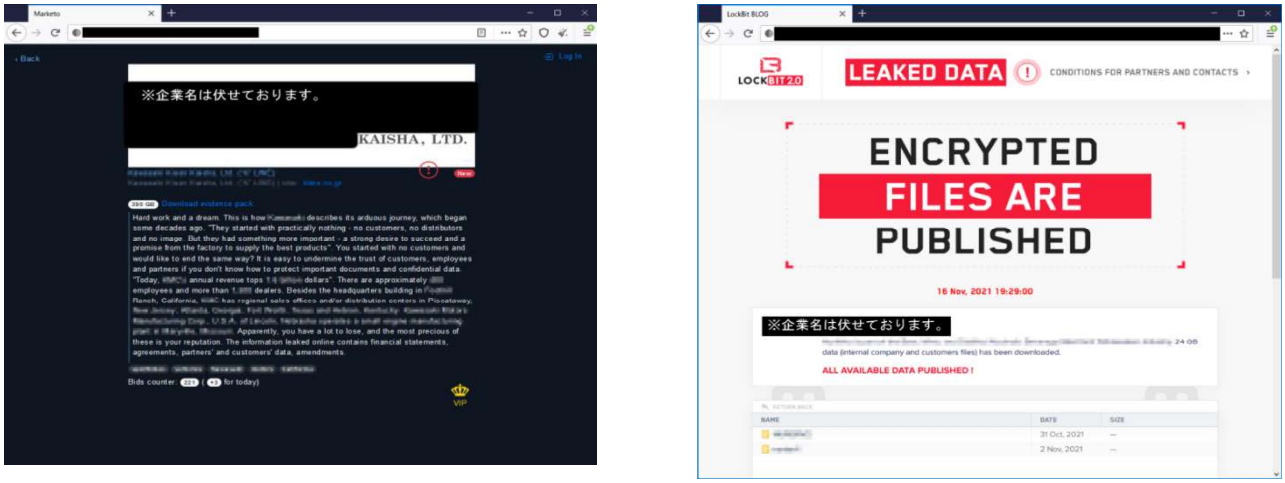
Regarding the infection routes of ransomware, 76 valid responses were received, of which 41 (54%) were through VPN devices and 15 (20%) were through remote desktops, indicating the majority of infections appeared to have exploited vulnerabilities and weak authentications in the devices often used for remote work.




【Fig 7: Infection Routes】

D) Status of ransomware leak sites

The police have been observing websites on the Dark Web and confirmed in 2021 that the data of Japanese businesses leaked by ransomware was posted on the leak sites. The exposed data included the victims' financial information, business contacts and consumers' information with descriptions hurting the companies' reputations.



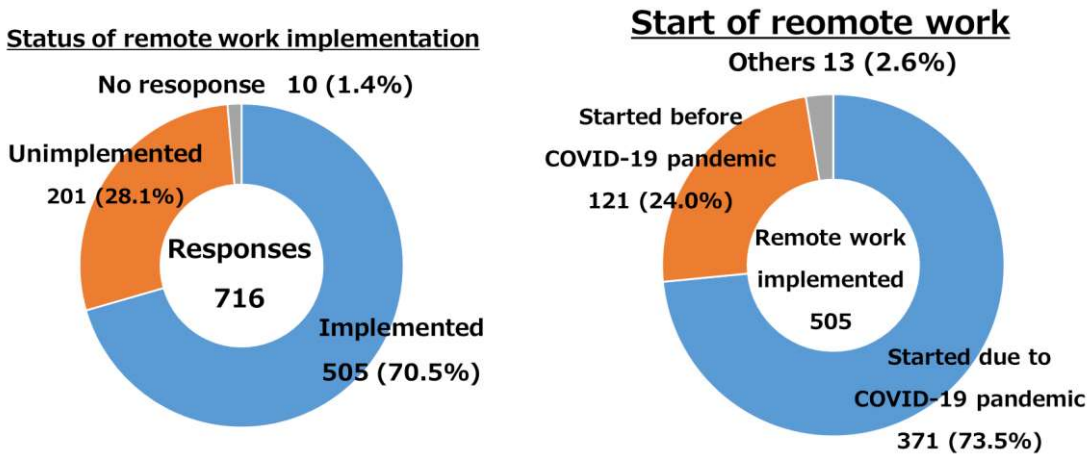

【Fig 8: Examples of leak sites on the Dark Web】

E) Survey on prevention of cybercrimes[*4]

Every year, the police conduct a “Survey on Countermeasures against Unauthorized Computer Access” targeting private companies and government organizations with the aim of contributing to public relations and awareness-raising to prevent damage caused by unauthorized computer access. In 2021, 2,950 companies and organizations were randomly selected for the survey, 716 responses were received, and they were analyzed.

i. Status of remote work implementation

70.5% of the respondents answered that they were implementing remote work, and more than 70% of them responded that they had started remote work due to the COVID-19 pandemic.

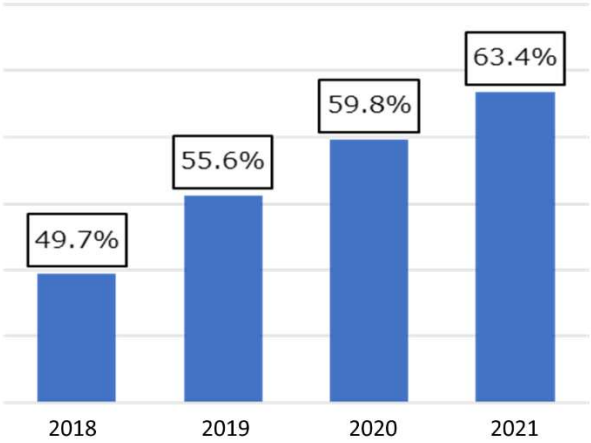



【Fig 9: Status of remote work implementation】

*4 NPA website “Cybercrime Project”
https://www.npa.go.jp/cyber/research/index.html

ii. Percentage of external connections to internal networks

The percentage of companies and organizations which allow external connections to their internal networks for business purposes due to the implementation of remote work accounted for 63.4% in 2021 and is increasing year by year.




【Fig 10: Percentage of external connections to internal network】

F) Countermeasures against ransomware

i. Warning on the NPA website

In September 2021, the NPA issued a warning on its website regarding measures to prevent ransomware damage, based on the results of their survey on ransomware victims conducted in the first half of 2021.

ii. Promotion of measures in cooperation with the General Insurance industry

To improve the concealment of damage, the elements and environments which constitute the hotbeds of cybercrimes including ransomware, the police are promoting public relations and awareness-raising regarding cybercrime prevention measures, as well as encouraging report of cybercrimes to the police in cooperation with the General Insurance Association of Japan.

iii. Alert regarding leaked VPN authentication information

In September 2021, it was confirmed that the authentication information for VPN equipment used for remote work was posted on the Dark Web. To prevent its abuse for ransomware attacks, the NPA analyzed the leaked information and alerted the companies involved with the leaked information through the prefectural police departments.

iv. Countermeasures against ransomware targeting medical institutions

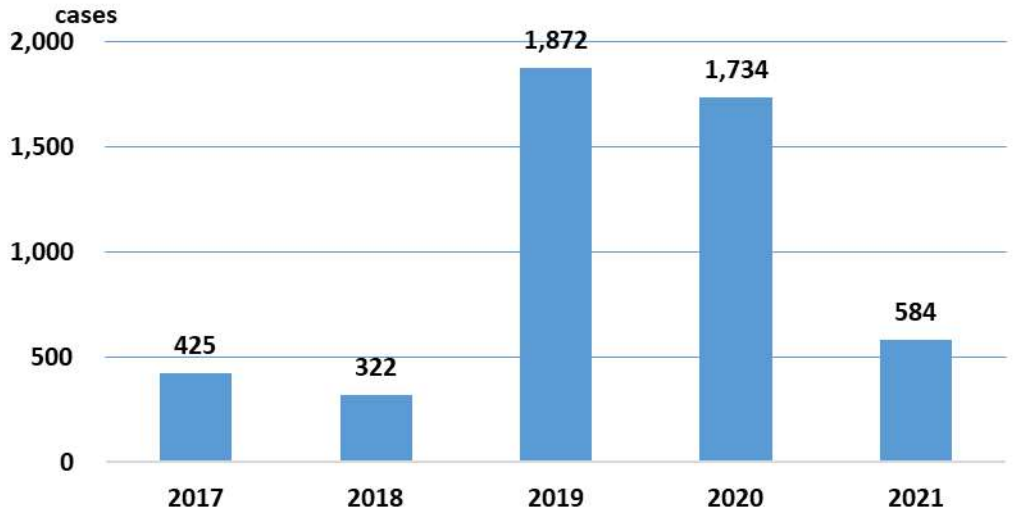
Ransomware has been targeting medical institutions in Japan,

infecting systems including electronic medical record systems, and suspending acceptance of new or emergency patients requiring medical treatments. To address the situation, the NPA provides relevant information to the Ministry of Health, Labor and Welfare, and works with the related organizations to prevent damage.

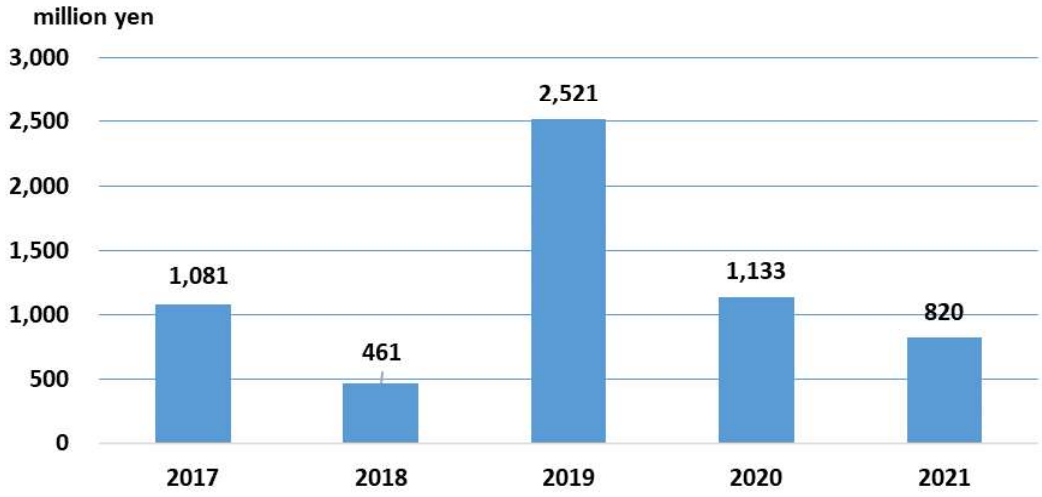
(2) Phishing-based Online Banking Fraud and Police Countermeasures

A) Online Banking Fraud

The number of online banking fraud cases in 2021 was 584 with total loss of approx. 820 million yen, both declined from those in 2020 as a result of efforts such as prompt information sharing with related organizations on modus operandi.




【Fig. 11: No. of online banking fraud】



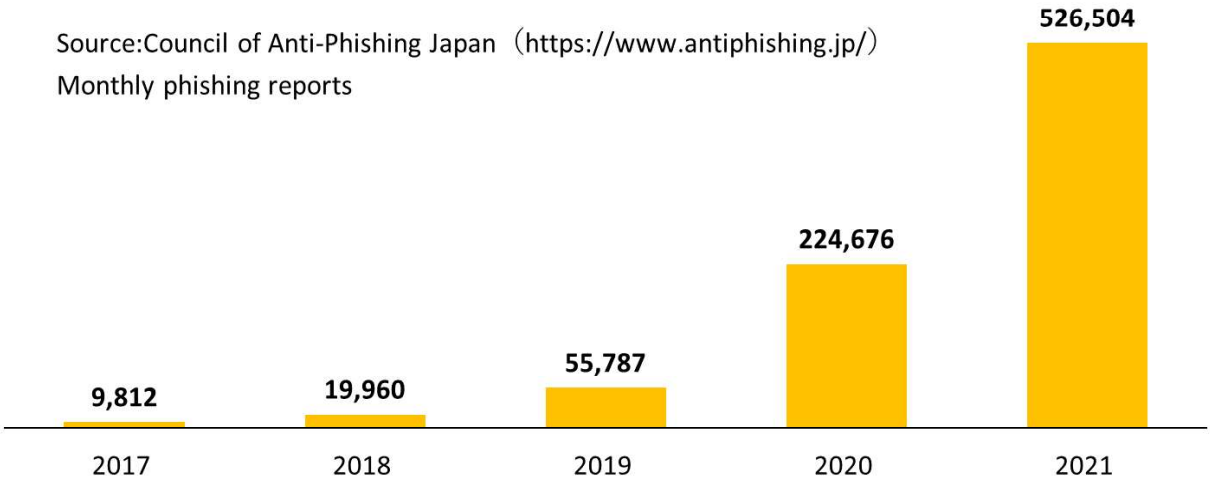

【Fig. 12: Total loss from online banking fraud】

B) Damage from Phishing

In 2019, it is shown that in regard to online banking fraud methods, perpetrators used SMS scams to trick recipients into accessing the spoofed bank websites, then stole their IDs, passwords and one-time passwords, causing 1,872 illicit transfers and 2.5 billion yen worth of damage.

Under such circumstances, financial institutions worked closely with the police and the JC3 to enhance monitoring and warnings to their customers, resulting in the decline of phishing-based online banking fraud both in terms of number of cases and amount of damage in 2021.

Meanwhile, the Council of Anti-Phishing Japan observed constant rise in phishing reports, reaching 526,504 cases in 2021[*5]. According to the JC3's analysis[*6], the spoofed bank websites were few, on the other hand, far outnumbered by those spoofing e-commerce, telecoms and credit card companies among the phishing websites observed in 2021.

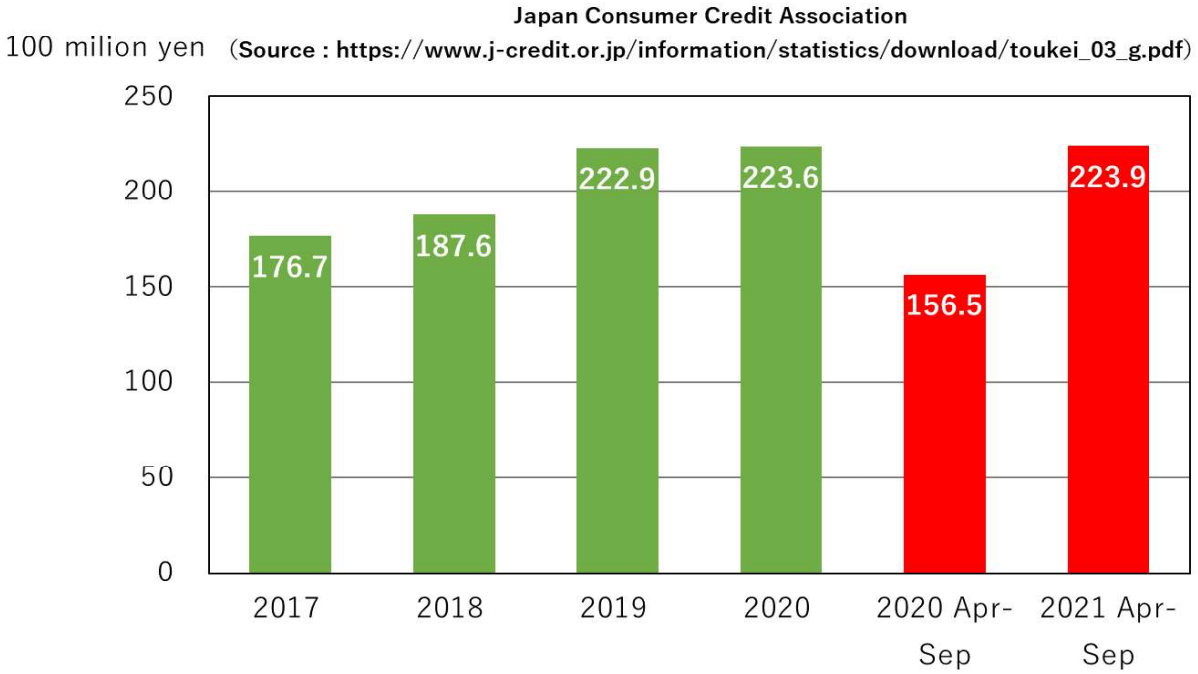



【Fig. 13: Number of Phishing Reports (Source: JC3)

*5 Council of Anti-Phishing Japan "December 2021 phishing reports" et al.
https://www.antiphishing.jp/report/monthly/202112.html

*6 JC3 "Transition of phishing targets"
https://www.jc3.or.jp/threats/topics/article-430.html

The Japan Consumer Credit Association also reported that the total damage from the credit card identity fraud during the period of January to September 2021 has amounted to 22.4 billion yen, surpassing that of the entire year 2020[*7].




【Fig. 14: Damage from credit card identity fraud】

The JC3 points out that there were phishing websites to be set up in order to steal credit card data as one of the triggers behind the surge in credit card fraud. It appears that perpetrators have been shifting the phishing target from the financial institutions, which have tightened security through the public-private initiative, to the e-commerce and credit card companies.

C) Police Endeavors

○ Crackdown on Illicit Transfer Groups

・ Crackdown on Illicit Transfer Groups

In regard to serial illicit transfer cases targeting major financial institutions which occurred from September 2019 through February 2020, the police arrested 29 men and women including the designated Boryokudan members who played the roles of crime controllers, holders of the illicit transfer destination accounts, and withdrawers from the said

---

*7 Japan Consumer Credit Association: "Credit card fraud statistics, December 2021" https://www.j-credit.or.jp/information/statistics/download/toukei_03_g.pdf

accounts.

- Enhanced Cooperation with Financial Institutions

To prevent damage from online banking fraud, the police enhanced cooperation with financial institutions by jointly conducting the Cybercrime Prevention Knowledge Conference and sharing insights learned from the crime methods.

○ Crackdown on an Account Trafficking Network

- Crackdown on an Account Trafficking Network

Starting from the illicit transfer case occurred in December 2019, the police arrested 7 perpetrators including the crime controller, and account seller of an account trafficking network by October 2021.

- Shutdown of Crime Tools

The police took measures against crime tools including requests for the victimized financial institutions to verify their customers' purposes of account openings and to freeze crime-abused accounts.

○ Request to note-taking app provider for crime prevention measures and warning about its use

As the cases where a note-taking app storing online banking IDs and passwords had been hacked and led to damage from illicit transfers were detected, the police requested the note-taking app provider to tighten crime prevention measures, resulting in publication of a warning on its websites.

The police and the JC3 also have jointly published a warning about the use of the note-taking app on the JC3 website.

○ Request to financial sectors for financial crime prevention measures in partnership with organizations.

As the police had promptly shared crime methods and damage status of online banking fraud with organizations which address financial crimes, they issued request for financial institutions to enhance the customer identification scheme and to alert their customers.

○ Warning against the telecom phishing scam

Based on information from the JC3 that telecom phishing SMS to entrap the recipients to download malware and enter their PINs were now targeting iPhones in addition to Androids, the police and the JC3 jointly issued alerts through social media platforms.

(3) Cybersecurity Initiative for the Tokyo 2020 Olympics and Paralympics

While cyberattacks occur on a global scale, the systems used for operations of the PyeongChang 2018 Olympic and Paralympic Games were targeted of cyberattacks, which however did not affect the operations. Considered the continuing serious situation of the threats in cyberspace, the Tokyo 2020 Games also required special attention as there were concerns about potential cyberattacks against the athletic facility management entities or the critical infrastructure operators to sabotage the Games or to steal data. Potential damage could not be denied as the scam websites spoofed as the streaming channels of torch relay or the opening ceremony appeared, malware as a lure for the Tokyo 2020 Games created, IDs and passwords of the volunteers and ticket purchasers leaked allegedly not from the systems of the Organizing Committee, and calls for cyberattacks targeting the related organizations found on the social media.

Under such circumstances, the police worked with the Organizing Committee, athletic facility management entities and critical service providers to prevent the damage from cyberattacks.

Immediately after the IOC had awarded the 2020 Summer Games to Tokyo, the police started the implementation of public-private cyberattack prevention initiative as proactive measure. This included confirmation of the system security status of and provision of advice to the stadiums management entities and critical service providers, implementation of joint exercises with the stadiums management entities anticipating cyberattacks against the facility control systems, and notice about cyberattacks targeting vulnerabilities of IT monitoring systems and server software for the critical service providers and the game-related entities.

During the period of the Games, the police and the game-related organizations closely worked together to set up and run a 24/7 immediate response scheme to fully address the potential cyberattacks.

Based on the report of a tampered domestic website misdirecting the viewers to false live streaming websites from JC3, the responsible prefectural police department requested the website administrators for redresses, while reporting the tampered content embedded in the foreign government websites with the cooperation of the commissioned counter-cybercrime technical advisor to the competent foreign investigative agencies through the NPA.

Consequently, no grave cyberattacks which could affect the operations of the Games were detected.

(4) Major Cyberattack Cases and Police Endeavors

A) Cyberattack cases

- Malware detected in the Immigration Services Agency system

In July 2021, the Immigration Services Agency of Japan announced that they had detected malware in May 2021 in their Trusted Traveler Program (TTP) system which registers users of the automated gates at the airports. Based on their inspection, the Agency suggested potential leak of the system configuration data.

- Public attribution of the “APT40” cyberattack group

In July 2021, the US Department of Justice (DoJ) announced indictment of 4 Chinese members of APT40 for hacking various countries including the US, the UK and Germany, targeting data in the areas of aviation, defense and biopharmaceuticals. The US DoJ stated that the targeted data included sensitive technical information on submarines and self-driving vehicles, as well as research information on infectious diseases.

The UK and the US issued statement criticizing Chinese government, alleging their support for APT40. Japan also issued a MOFA press secretary statement keeping pace with the UK and the US, presuming the probable support of Chinese government for APT40, and criticizing the malicious cyber activities and Japan’s tough stance against them.

- Unauthorized access to a major electronic manufacturer

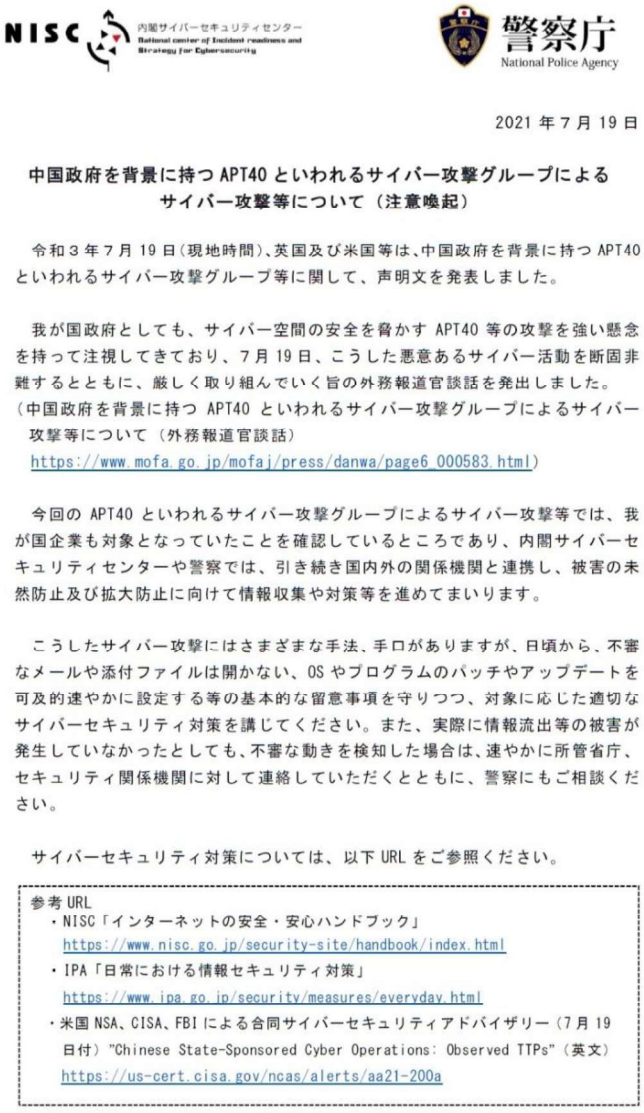
In November 2021, a major Japanese electronics manufacturer announced that they had found out a incident of unauthorized access to their networks and unauthorized read of partial data from the file servers. Inspection results indicated that the unauthorized access had been implemented through the victim company’s offshore subsidiary, and the targeted file servers contained the company’s internal data, operational data of their clients and personal data of their job applicants.

B) Police Endeavors

- Warning for the victimized companies

In July 2021, the NPA and the National center of Incident readiness and Strategy for Cybersecurity (NISC) of Japan announced that they continue to work with the pertinent organizations from in and outside of Japan to gather information about cyberattacks by APT40 and take necessary measures to prevent and minimize damage. They also encouraged businesses to adopt appropriate cybersecurity measures, and to report to the relevant government agencies and private cybersecurity organizations as well as to consult the police when detecting suspicious phenomena even before confirmation of actual damage e.g., data leaks.

In addition, the police immediately notified each victim company of cyberattacks they had detected and individually provided information on the possibility of malware infection and effective solutions to prevent the spread of damage. *8



NISC 内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity

警察庁 National Police Agency

2021年7月19日

**中国政府を背景に持つAPT40といわれるサイバー攻撃グループによるサイバー攻撃等について（注意喚起）**

令和３年７月19日（現地時間）、英国及び米国等は、中国政府を背景に持つAPT40といわれるサイバー攻撃グループ等に関して、声明文を発表しました。

我が国政府としても、サイバー空間の安全を脅かすAPT40等の攻撃を強い懸念を持って注視してきており、７月19日、こうした悪意あるサイバー活動を断固非難するとともに、厳しく取り組んでいく旨の外務報道官談話を発出しました。
（中国政府を背景に持つAPT40といわれるサイバー攻撃グループによるサイバー攻撃等について（外務報道官談話）
https://www.mofa.go.jp/mofaj/press/danwa/page6_000583.html）

今回のAPT40といわれるサイバー攻撃グループによるサイバー攻撃等では、我が国企業も対象となっていたことを確認しているところであり、内閣サイバーセキュリティセンターや警察では、引き続き国内外の関係機関と連携し、被害の未然防止及び拡大防止に向けて情報収集や対策等を進めてまいります。

こうしたサイバー攻撃にはさまざまな手法、手口がありますが、日頃から、不審なメールや添付ファイルは開かない、OSやプログラムのパッチやアップデートを可及的速やかに設定する等の基本的な留意事項を守りつつ、対象に応じた適切なサイバーセキュリティ対策を講じてください。また、実際に情報流出等の被害が発生していなかったとしても、不審な動きを検知した場合は、速やかに所管省庁、セキュリティ関係機関に対して連絡していただくとともに、警察にもご相談ください。

サイバーセキュリティ対策については、以下URLをご参照ください。

参考URL
・NISC「インターネットの安全・安心ハンドブック」
https://www.nisc.go.jp/security-site/handbook/index.html
・IPA「日常における情報セキュリティ対策」
https://www.ipa.go.jp/security/measures/everyday.html
・米国NSA、CISA、FBIによる合同サイバーセキュリティアドバイザリー（7月19日付）"Chinese State-Sponsored Cyber Operations: Observed TTPs"（英文）
https://us-cert.cisa.gov/ncas/alerts/aa21-200a

【Fig. 15: Joint warning from the NPA and the NISC】

○ Warning for critical infrastructure operators

The police continue to issue cyberattack warnings to the critical infrastructure operators. In 2021, in order to prevent them from the

*8 As of March 2022, no actual damage including the data leak from these companies has been confirmed.

occurrence and expansion of cyberattack damage, the police issue alerts against the IP addresses allegedly abused as malware spreading infrastructure, and the alerts concerning vulnerabilities in a content management system Movable Type and those in Apache Log4j[*9] logging servers.

○ Obtaining arrest warrant and spreading a dragnet for a suspect in fraud attempt

In December 2021, the Public Security Bureau of the Tokyo Metropolitan Police Department obtained arrest warrant of a former international student of Chinese nationality who planned to illicitly obtain annual usage rights of a corporate edition antivirus software produced by a Japanese company and applied for a licensing contract providing false corporate information and a non-existent contact name to a software distributor in Tokyo in November 2016 under instructions from an individual allegedly related to the People's Liberation Army of China over allegation of fraud attempt and put him on the wanted list.

This case emerged in the process of investigating the cyberattack case against JAXA[*10] which had been conducted from June through December 2016 by a cyberattack group potentially linked to the PLA, suggesting the PLA's wide-ranging potential espionage against Japan.

○ Takedown of C2 servers[*11] used for cyberattack

The police continue to tackle the C2 servers by means including requests to the responsible operators to take down the illicit functions of C2 servers in Japan which are run by the illicitly loaded files, resulting in takedown of 27 C2 servers in 2021.

○ Conducting joint response drills

The police continue to conduct the joint response drills anticipating the occurrence of cyberattacks with the critical infrastructure operators. In 2021, the police and entities ranging from power companies, financial institutions to local governments conducted drills using simulated spear phishing emails, and on-site drills to ascertain the joint operations with the police to enhance cyberattack response capability of each entity.

---

*9 See details of Apache Log4j vulnerability targeting in pp. 20-21.

*10 See pp.9-10, "Threats in Cyberspace in the First Half of 2021".

*11 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.

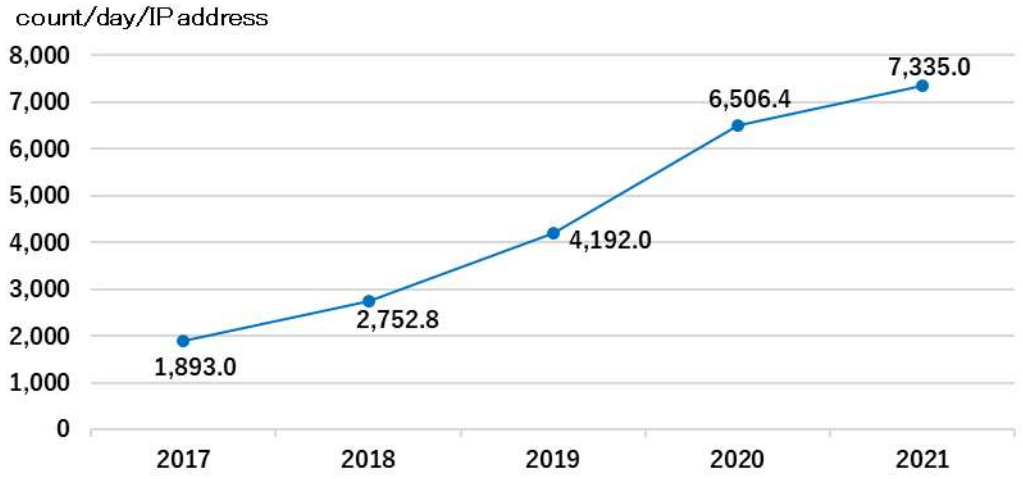
## 2 Threats in Cyberspace

### (1) Monitoring vulnerability scanning in the cyberspace

#### A) Unexpected connection attempts

The NPA sets up sensors on the internet to gather communication packets*12 sent to the sensors. As these sensors do not provide any services, they usually do not receive external communication packets except for the observable ones sent indiscriminately to the unspecified number of IP addresses by cyberattackers to search for potential targets. Analysis of these communication packets facilitates understanding of the phenomena taking place on the internet e.g., vulnerability scanning of the connected devices, consequent attacks, and behaviors of the malware-infected computers.

The number of unexpected connection attempts detected at the sensors has risen to 7,335.0 per IP address per day in 2021, showing an upward trend. Reasons for surge in extraordinary access attempts may include the increase of potential targets resulting from the diffusion of IoT devices, and continual evolvement of attackers' methods enabled by the advancement of technology.




【Fig. 16: No. of unexpected connection attempts detected at the sensors】

#### B) Major Observation

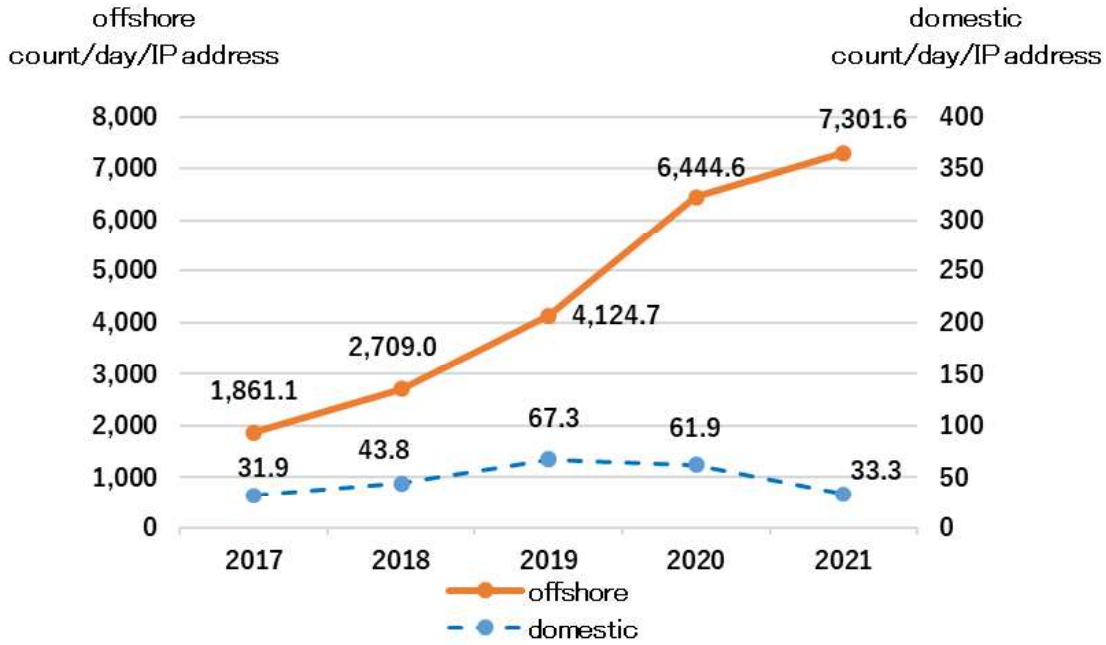
- Surge in Access from offshore

---

*12 The communication packets are the data chunks divided when transmitted through the networks. Each packet is tagged with data e.g., the IP addresses of the destinations and origins.

In the past 5 years, the share of offshore access among all the detected access has been high.

In 2021, while the daily average number of domestic access declined from 61.9 in 2020 to 33.3, that of offshore access largely increased from 6,444.6 in 2020 to 7,301.6, implying the continuous significance of response to the threats from offshore.




【Fig 17: No. of unexpected connection attempts by originating IP addresses】

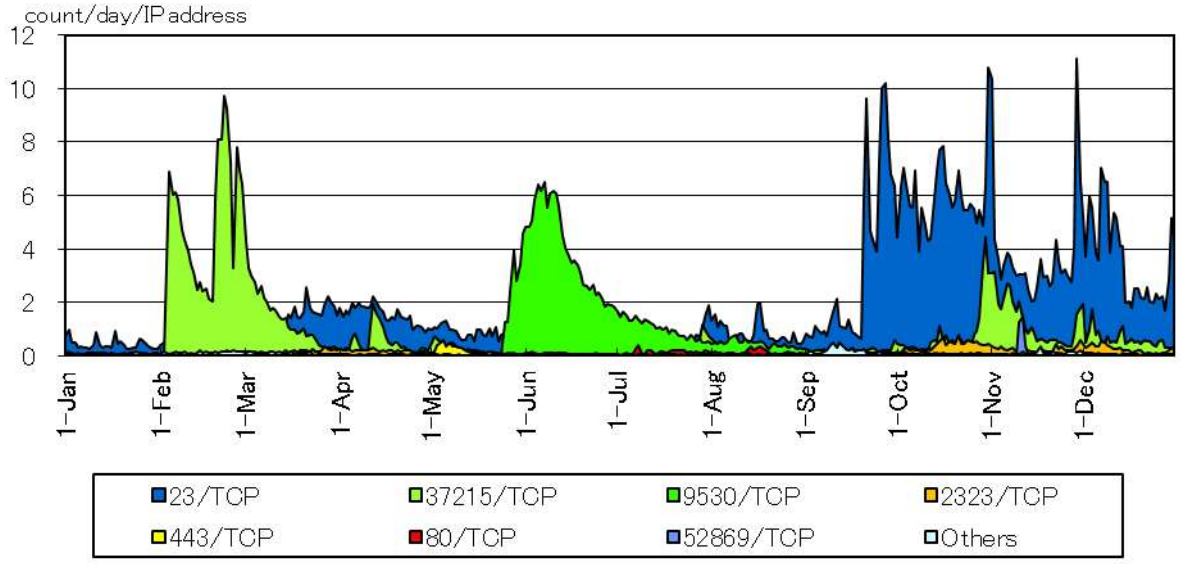
○ Surge in domestic access targeting vulnerabilities of IoT devices

The daily average number of accesses with Mirai bot characteristics decreased from 461.7 per IP address per day in 2020 to 257.3 in 2021. Meanwhile, the daily average number of accesses with Mirai bot characteristics originating from Japan increased from 2.8 per IP address per day in 2020 to 3.6 in 2021. The increase in accesses with Mirai bot characteristics amid decrease of overall domestic accesses suggests the potential presence of a certain number of IoT devices with vulnerabilities in Japan which appear to be continuing the spread of secondary infections to other IoT devices after being compromised.

Followings are the distinctions of domestically originating accesses with

Mirai bot characteristics by the targeted port[*13] observed in 2021. The threats against IoT devices in Japan continue as scanning for known vulnerabilities occasionally surges.

- From the beginning of February, increase of accesses to port 37215/TCP apparently intended to exploit vulnerabilities of the foreign-made routers to spread malware infection was observed.
- From the end of May, increase of accesses to port 9530/TCP apparently scanning for vulnerabilities which would enable remote manipulation was observed.
- From the end of September, increase of accesses to port 23/TCP apparently targeting vulnerabilities in network devices was observed.




【Fig. 18：Transition of No. of domestic accesses with Mirai bot characteristics (by targeted port)】

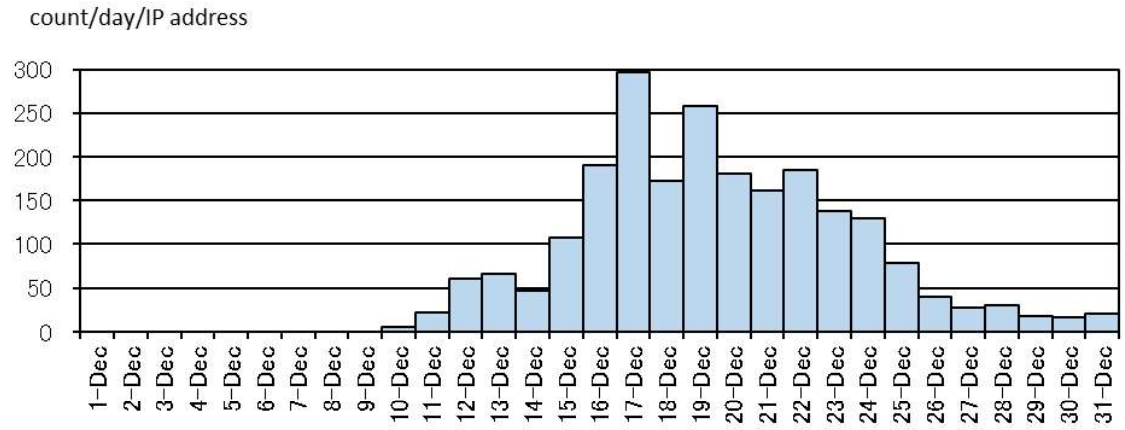
○ Observation of accesses targeting vulnerabilities of Apache Log4j Java library

Apache Log4j Java library is an opensource Java logging library developed by the Apache Software Foundation used in many software applications developed on Java for server logging and management. Triggered by the alert of Apache Log4j vulnerabilities on December 10th, surge in accesses targeting the said vulnerabilities was observed.

---

*13 A number used to identify the service used in TCP/IP communications (an arrangement for exchanging data over a network used for the Internet). A number from 0 through 65535 is assigned to each port.

The cyberattacks appeared as attempts to exploit vulnerabilities of Apache Log4j which would enable external manipulation of the targeted devices when the attack strings sent by the remote third parties to the logging software using Apache Log4j are recorded into the logs.

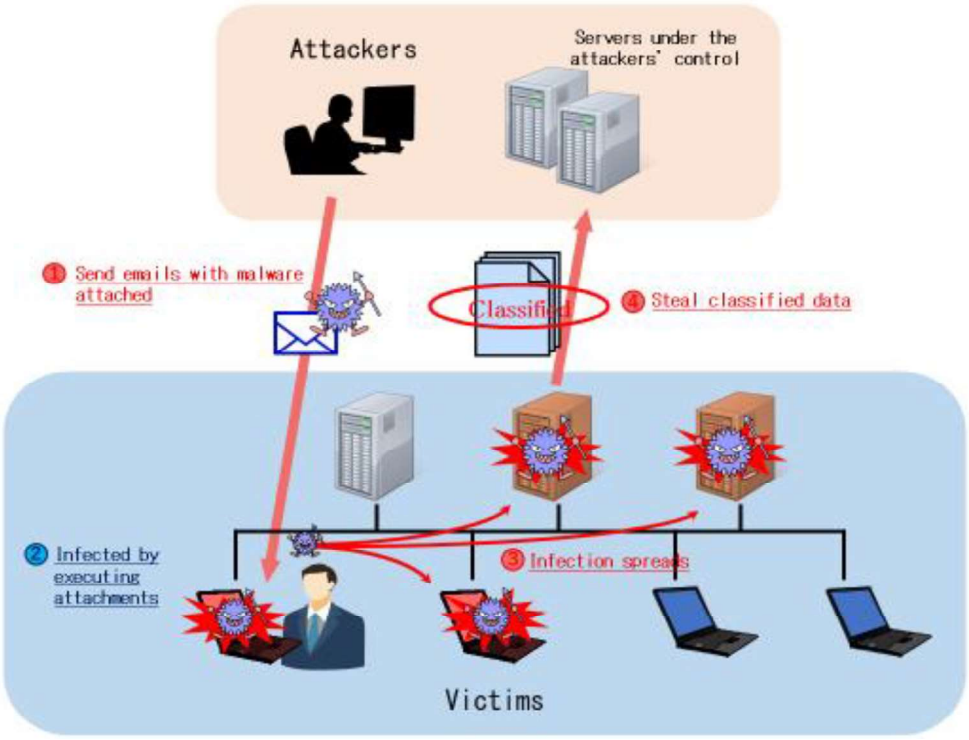



【Fig. 19：Transition of No. of accesses targeting vulnerabilities of Apache Log4j Java library (by targeted port)】

(2) Spear Phishing Attack

A) Counter Cyber-intelligence Information-Sharing Network

The police and approximately 8,200 organizations nationwide (as of April 1st, 2022) with cutting-edge technologies have established the Counter Cyber-intelligence Information-Sharing Network to integrate and analyze information on cyberattacks including the spear phishing attacks to provide warnings to businesses. The Network also shares analyses on spear phishing attacks against government agencies provided from the National center of Incident readiness and Strategy for Cybersecurity (NISC) with businesses.




【Fig 20: Sample scheme of data theft by spear phishing attack】

B) Case Examples

In 2021, the Counter Cyber-intelligence Information-Sharing Network continued to confirm the well-crafted and business-disguised spear phishing emails as well as other types of phishing emails apparently intended to steal the victims' passwords sent to businesses. The followings are examples of spear phishing emails shared by the targeted businesses through the Network.

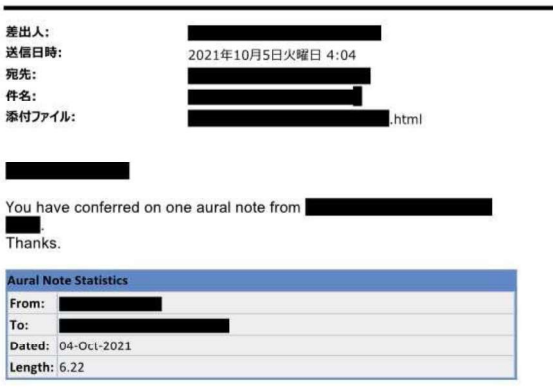
① Spear phishing attack targeting a machine parts manufacturer

Spear phishing email titled ‘New ID Notice’ to induce the recipient to download the malware-embedded file was sent to a machine parts manufacturer.


【Fig. 21: Spear phishing email】

② Spear phishing attack targeting a semiconductor manufacturer

Spear phishing email to induce the recipient from the attachment to a fake password entry page to input their business account password was sent to a semiconductor manufacturer.



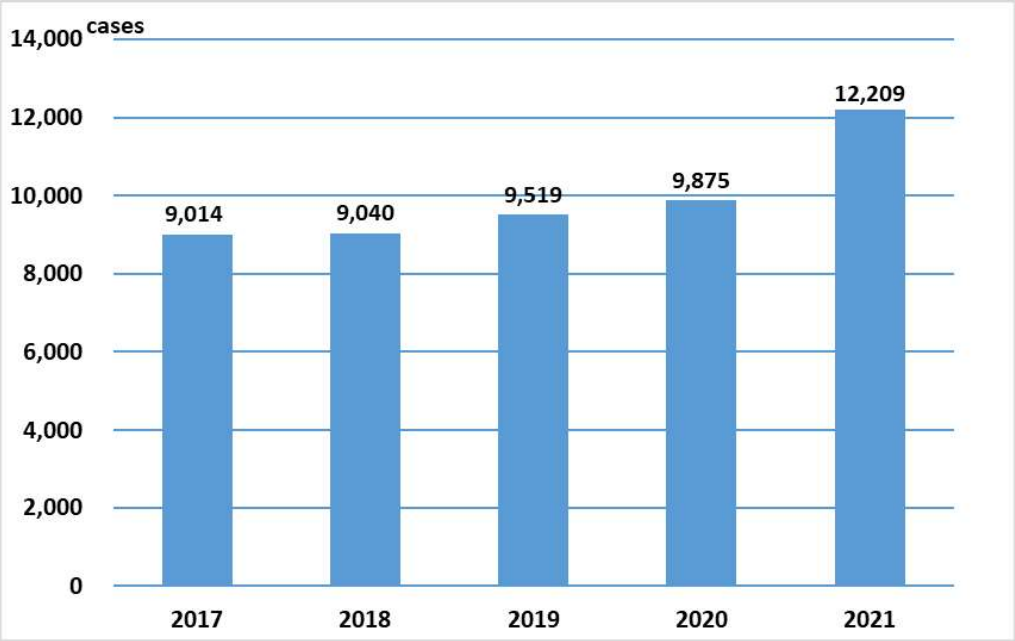

【Fig. 22: Spear phishing email】


【Fig. 23:Fake password entry page】

(3) Cybercrime Status

A) The number of cleared cybercrime cases

The number of cleared cybercrime cases reached 12,209 in 2021, increasing from 2020.




【Fig 24: No. of cleared cybercrime cases】

B) Violations of the Act on Prohibition of Unauthorized Computer Access*14

i. The number of cleared cases

The number of cleared violations of the Act on Prohibition of Unauthorized Computer Access reached 429 in 2021, declined from 2020.

ii. Major Observation

398 of all the cleared cases were classified as the identification-code-abuse type*15 and accounted for approx. 92.8% of the total.

---

∗14 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.

∗15 Unauthorized access can be categorized as the 'identity theft' which abuse the identifiers of others, and the 'security hole attack' which abuse the non-identifier data or commands to evade specific access restrictions.

○ ‘Authorized users’ lax password management’ most exploited

Among the crime methods used in identity theft types of unauthorized accesses, ‘exploited the authorized users’ lax password management’ was the most prevalent with 153 cases (38.4%), followed by ‘obtained from the phishing websites’ with 70 cases (17.6%).

○ Online game community websites were most abused

The services most abused by suspects of the password theft-based unauthorized accesses in 2021 were online game community websites with annual 144 incidents (36.2%), followed by online banking with 96 incidents (24.1%).

C) Crimes targeting computers or electromagnetic records*16

i. The number of cleared cases

The number of cleared cases regarding crimes targeting computers or electromagnetic records in 2021 was 729, increasing from 2020.

ii. Major Observations

The most dominant crime type among the cleared cases in this category was computer frauds, reaching 692 cases and 94.9% of the total.

---

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