Threats in Cyberspace in 2025
And
Police Efforts

March 2026

Cyber Affairs Bureau, National Police Agency

Preface

Because cyberattacks have a relatively low risk of detection and attackers hold the upper hand, the threat of cyberattacks that exploit the anonymity of cyberspace has been rapidly increasing. Furthermore, amid a severe and complex security environment, the cyberspace situation—which reflects geopolitical tensions—is becoming more serious and has the risk of rapidly escalating into a crisis. Specifically, it is believed that state-sponsored activities such as the theft of sensitive information through cyberattacks and interference in foreign elections are already taking place on a regular basis. In addition, it is highly likely that hybrid warfare will be conducted in a more sophisticated manner in the future.

Additionally, as digitalization has advanced across society, cyberspace has transformed into a public space. Consequently, the anonymity of cyberspace is being exploited in various ways, including communications fraud sophisticated fraud schemes social media investment and romance scams, and money laundering involving cryptoassets. Furthermore, there has been a lot of cases that misuse advanced technologies such as generative AI, as well as ransomware attacks.

These threats pose a challenge to public safety and order in our country and have the potential to seriously impact the lives of our citizens, economic activities, national security, and crisis management. Considering this point, it is necessary to deal with these threats with taking even the national security and crisis management perspectives into account.

On the other hand, when a cyber incident occurs, it is difficult to determine at the initial stage whether the incident is caused by state-sponsored or a financially motivated act by a criminal organization. Furthermore, even if a state-sponsored cyberattack is carried out as a preparatory act, it is difficult to immediately recognize this fact. Even in times of emergency, the police are expected to respond in the same manner as in peacetime. Therefore, the police are an organization capable of seamlessly handling everything from investigations and apprehensions to public attribution and even remote access – and - neutralization measures.

Based on the above assessment of the current situation, this report begins with Special Feature I on AI—which has been rapidly permeating society in recent years—and Special Feature II on ransomware, which has become a serious social problem. In Chapter 2, which details police efforts, we have included the following topics: “The Role of Cyber Police in National Security” and “Police Efforts to Combat Anonymity in Cyberspace.”

We hope this report will deepen understanding of the threat landscape in cyberspace and the police’s efforts to address it.

Table of Contents
【Special Features and Topics】

Table of Contents
【Annual Report】

List of Figures

List of Figures

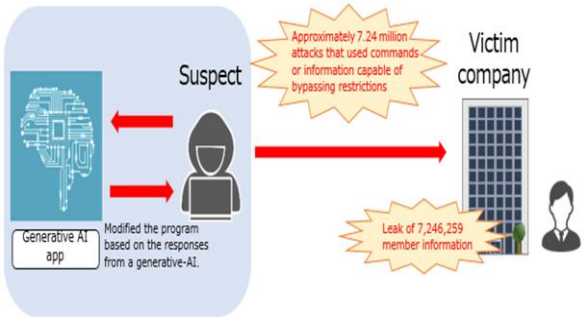
List of Columns

List of CASE

Overview: Special Features and Topics

Special Feature I: AI Threats and Police Efforts

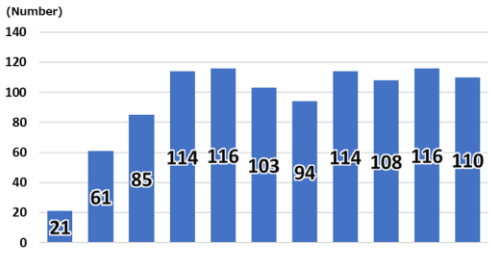
- A 17-year-old high school student misused generative AI to send malicious commands to the server of a café app, causing a leak of member information and disrupting some of the app's functions. In December 2025, the student was arrested on charges of violating the Unauthorized Access Prevention Act and obstruction of business by fraudulent means. (Tokyo)



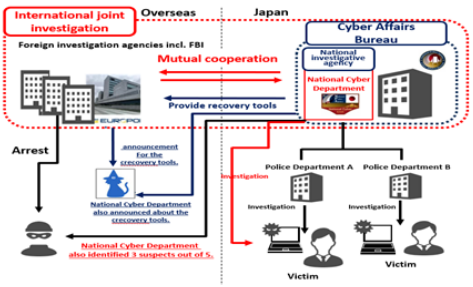
- In collaboration with ICPO and JC3, the National Police Agency of Japan (NPA) hosted an international conference on the theme of "AI and Digital Forensics," attended by experts from around the world. Participants shared information on topics such as cyberattacks involving the misuse of AI and deepfake detection technologies.

Special Feature Ⅱ: Ransomware Threats and Police Efforts

- In 2025, there were 226 reported cases of ransomware attacks. Several incidents resulted in prolonged disruptions to business operations and had an impact on the daily lives of citizens.

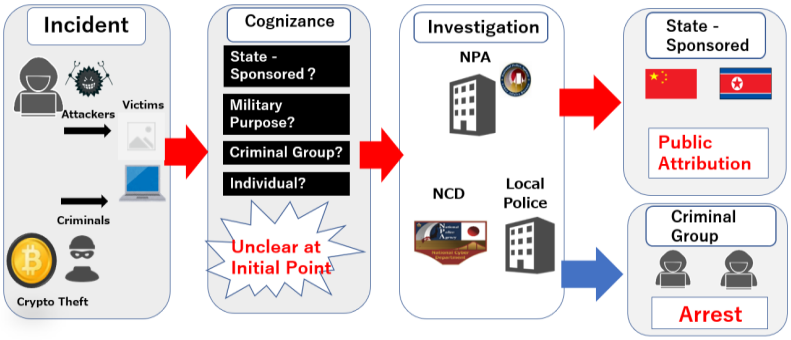


- With Europol and FBI, NPA conducted International joint investigations targeting ransomware groups "Phobos" and "8 Base". National Cyber Department (NCD) identified three suspects and developed a tool to decrypt the encrypted data.



Topic I: The Role of Cyber Police in National Security

- At the time a cyberattack occurs, it is not possible to immediately identify the perpetrator and the purpose. The police are investigating these incidents and working to uncover the facts, while recognizing that every cyber incident could be related to national security. The cyber police play a vital role in the context of national security in cyberspace, including responses to state-sponsored cyberattacks.

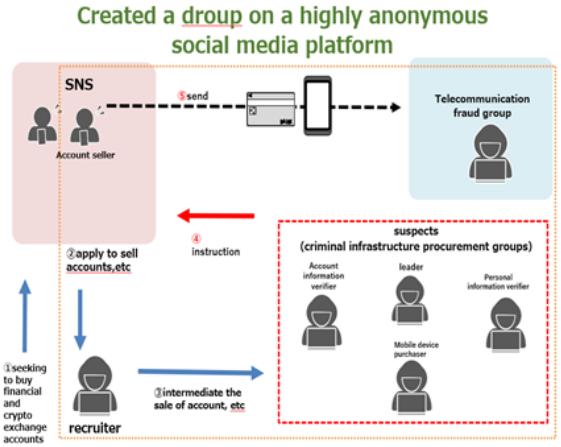


- In May 2025, Active Cyber Defense Act was passed by the Diet. This Act will enable the police to take remote access-and-neutralization measures to prevent serious harm caused by cyberattacks (scheduled to take effect on October 1, 2026).

Topics II: Police Efforts to Combat Anonymity in Cyberspace

- Anonymous - fluid criminal groups exploit the anonymity of cyberspace to evade police detection. For example, they disguise and conceal the flow of funds by converting criminal proceeds into cryptoassets.

- Police identified the leader of a "tool supplier" group that illegally obtained financial institution accounts and cryptoassets accounts via social media and sold them to multiple communications fraud groups. In October 2025, police arrested seven individuals of this group. (Aichi)

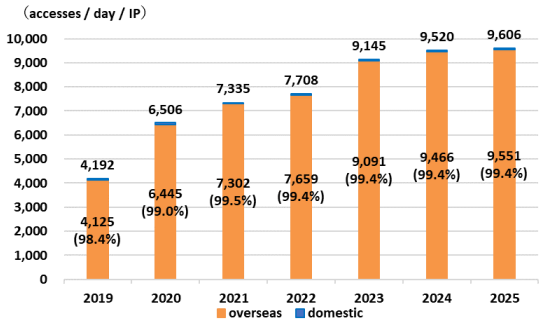


Overview

I Threats in Cyberspace in 2025

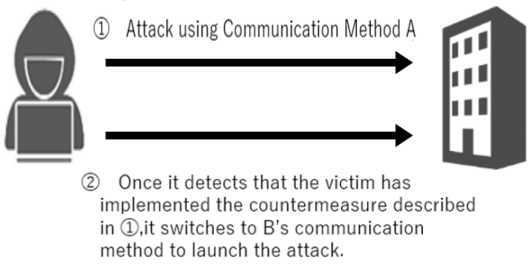
1 Cyberattacks using advanced technology

- The number of suspicious access attempts — such as vulnerability scanning — detected by sensors installed by NPA continues to rise. Most of these attempts come from overseas.



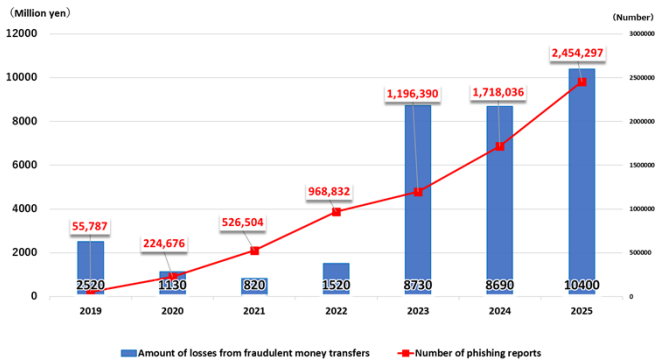
- There were several cyberattacks committed by state-sponsored groups. They were believed to be aimed at stealing information.

- From late 2024 through early 2025, a lot of DDoS attacks against critical infrastructures occurred, resulting in serious harm to the public. Even when the operators took measures to block the attacks, the attackers changed their attacking methods and continued their attacks.



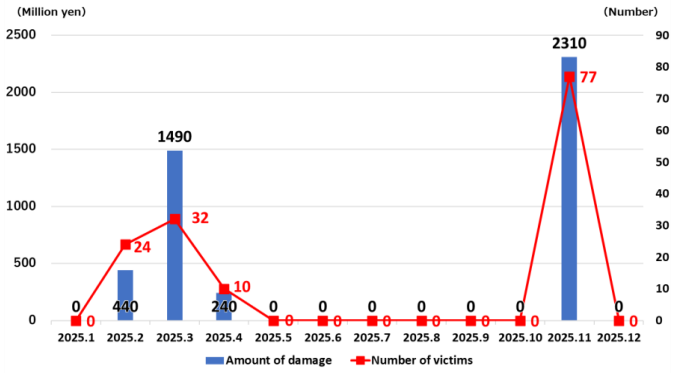
2 Cybercrimes

- The number of reported phishing cases was 2,454,297. There were 4,747 online banking fraud cases, and the total damage amounted to 10.397 billion yen. 90% of these cases were attributed to phishing.



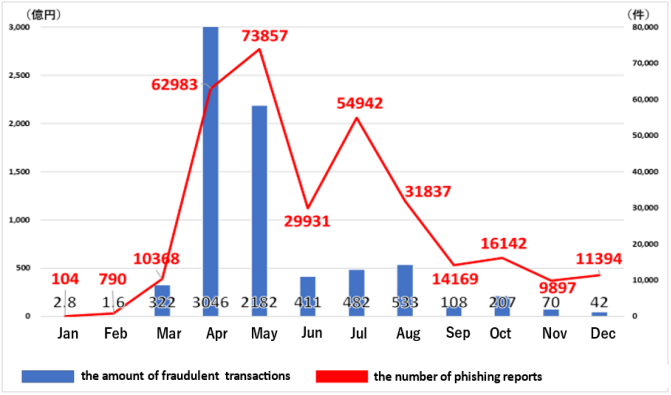
- The number of online banking fraud cases caused by voice phishing surged from fall 2024 to April 2025. The number of cases surged again in November 2025. In some case, one company suffered 400-million-yen damage.

Number of cases and total amount of online banking fraud from corporate accounts via voice phishing



- There were several phishing emails impersonating securities firms, as well as unauthorized access to securities accounts and unauthorized fund transfers. The total value of fraudulent trades amounted to approximately 740.8 billion yen, and 316,414 phishing emails that impersonating securities firms were reported.

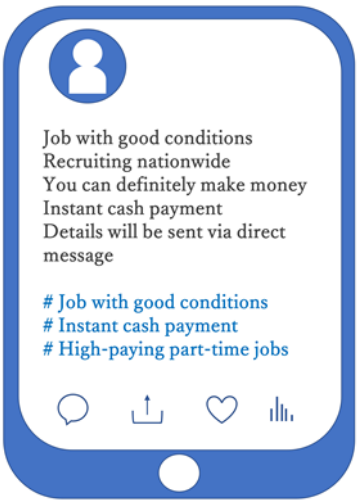
Amount of Fraudulent Transactions in Securities Accounts and Number of Phishing Reports



3 Illegal and harmful information

- On the internet, there is a lot of illegal and harmful information. In 2025, there were 105,553 cases of illegal information and 14,241 cases of criminal perpetrator recruitment information

Image of criminal perpetrator recruitment

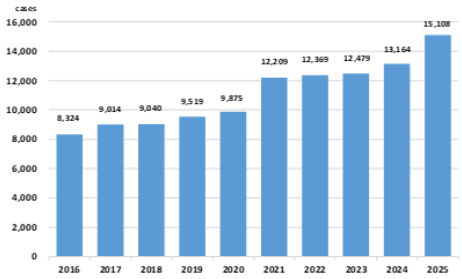


Ⅱ Police Efforts

1 Efforts for clearing crimes

- The National Cyber Department (NCD) of NPA handles serious cybercrimes. Cyber divisions of prefectural police handle cybercrimes that require advanced knowledge and technical expertise.

Trends in the Number of Cybercrime Cleared Cases



- The number of cybercrimes cleared cases in 2025 reached 15,108, marking a record high.

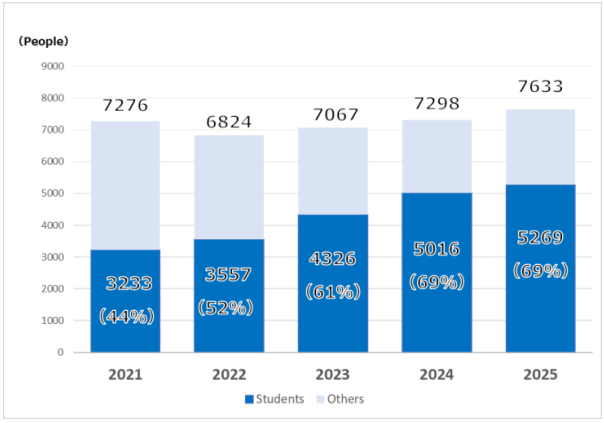
- The police, in collaboration with the Central Bureau of Investigation (CBI) of the Republic of India, conducted an international joint investigation into a support scam targeting Japanese nationals. As a result, in May 2025, CBI arrested six Indian suspects who were in the Republic of India. In January 2026, the Director of the Cybercrime Investigation Division of NPA visited the CBI and presented a letter of appreciation for their investigative cooperation.

- In November 2025, NCD and prefectural police arrested a 38-year-old Chinese national and others on charges of violating the Financial Instruments and Exchange Act and the Unauthorized Access Prevention Act for allegedly gaining unauthorized access to securities accounts and conducting fraudulent transactions.

2 Prevention of Damage Cyberattack

- In August 2025, NPA and the National Cybersecurity Office (NCO), together with the United States, Australia, New Zealand, and others, jointly signed an international advisory regarding cyberattacks carried out by the China- sponsored cyberattack group “Salt Typhoon” and published this advisory as a public attribution.

- "Cybercrime prevention volunteers" engage in voluntary crime prevention activities aimed at creating a safe and secure online environment. As of the end of December 2025, there are 332 groups and 7,633 volunteers. Students make up a significant proportion of the members, and crime prevention activities led by the younger generation are gaining momentum.

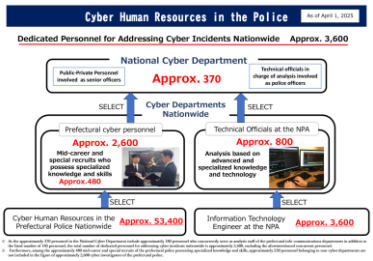


- In 2025, the Internet Hotline Center（IHC） operational guideline was revised to strengthen measures against illegal and harmful information infrastructure, adding criminal perpetrator recruitment information and information that uses the internet to lure unspecified individuals within Japan into illegal online gambling and similar activities to the list of illegal content. Regarding criminal perpetrator recruitment information, out of 6,679 removal requests, 6,351 were successfully removed (95% removal rate).

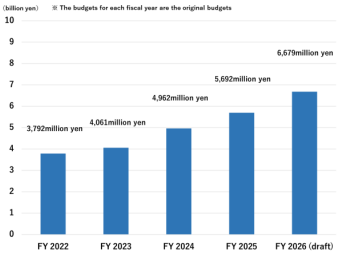
3 Development of Human and Physical Infrastructure

- In April 2025, the Specialized Response Unit was established within NCD. This strengthened NCD's capability for conducting investigations, collecting and analyzing intelligence, and preventing incidents before they occur.

- NPA hires technical staff dedicated exclusively to handling cyber incidents in FY 2026. At prefectural police, approximately 480 officers who were hired through mid-career and special recruitment programs serve as special cyber investigators.



- The budget for addressing cyber-space threats in the FY 2026 initial budget (draft) is 6,679 million yen.



Special Feature I: AI Threats and Police Efforts

1 AI Threats

While the use of AI is rapidly expanding in society and contributes to improving people's lives and developing the national economy, many citizens are concerned about the risks posed by AI. Considering this situation, the AI Act was enacted in May 2025 to promote AI innovation and to mitigate these risks. Furthermore, in December 2025, the AI Basic Plan was approved by the Cabinet, outlining comprehensive and systematic measures to be implemented by the government, and the AI Guideline was established to ensure the appropriate conduct of AI research, development, and utilization. NPA participates in deliberations based on the AI Act through bodies such as the Council for the Promotion of Artificial Intelligence Strategy, in order to promote initiatives related to AI research, development, and utilization in collaboration with relevant ministries and agencies.

Regarding the AI Safety Institute (AISI), established in February 2024 with the Information-technology Promotion Agency (IPA) serving as its secretariat, NPA is participating in discussions on standards and methodologies for AI safety assessment through the AISI Liaison Conference of Relevant Ministries and Agencies and other forums. In December 2025, the Prime Minister issued instructions at the Artificial Intelligence Strategic Headquarters regarding the fundamental strengthening of AISI. NPA is committed to providing the necessary cooperation to ensure comprehensive AI security.

2 Cases involving the misuse of AI

The misuse of AI presents a range of risks, including the development of malicious programs, development of phishing websites, dissemination of disinformation and misinformation, potential military applications, and leakage of confidential information. These risks raise concerns both in terms of criminal activity and national security.

Confirmed cases include arrests for developing malicious programs by using generative AI, as well as incidents involving the creation of fraudulent identification documents and obscene images using generative AI.

The Japanese police, in collaboration with the Central Bureau of Investigation (CBI) of the Republic of India, conducted an international joint investigation into a support scam targeting Japanese nationals (see page 53). The investigation revealed that the suspect group exploited generative AI to identify targets, generate fraudulent pop-up messages, and translate contents into Japanese.

(1) Cyberattacks using AI

As AI technologies continue to develop, there is a growing likelihood that cyberattacks will be increasingly automated, without human intervention. For example, a report from a private company indicates that state-sponsored cyberattack groups have carried out cyber operations using AI without human intervention.

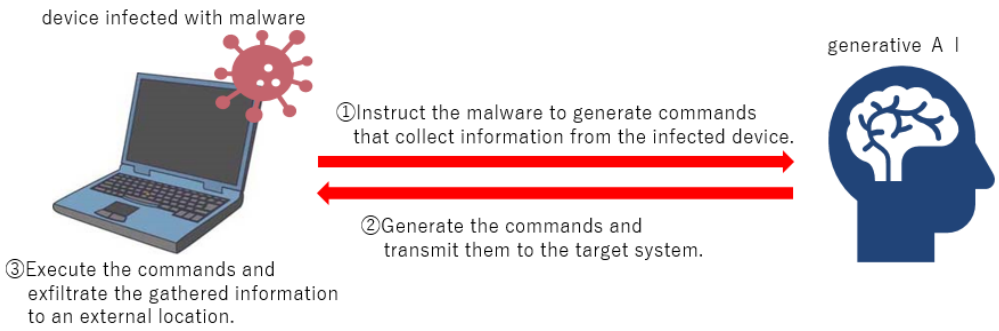
Systems capable of autonomously executing tasks are referred to as AI agents. This case demonstrates that AI agents are capable of autonomously executing nearly the entire lifecycle of cyberattacks

【CASE：Analysis of malware exploiting generative AI】

In July 2025, in a foreign country, an individual impersonating a government official sent emails containing malware that exploited generative AI, targeting government agencies.

This malware infected victim systems upon opening an attached file. Analysis conducted by NPA revealed that the malware itself did not contain embedded attack commands. Instead, it exploited generative AI services accessible from the infected system to generate malicious commands.

【Figure 1: Operational model of malware exploiting generative AI】



(2) Cybercrimes using AI

By using AI, people who have no technical expertise can easily access information and tools that could be used for cyberattacks.

【CASE：Arrest for developing phishing websites using generative AI】

In June and September 2024, a 36-year-old unemployed man launched phishing websites impersonating a major e-commerce platform with accomplices. In November 2024, they stored unlawfully obtained identification code belonging to third parties.

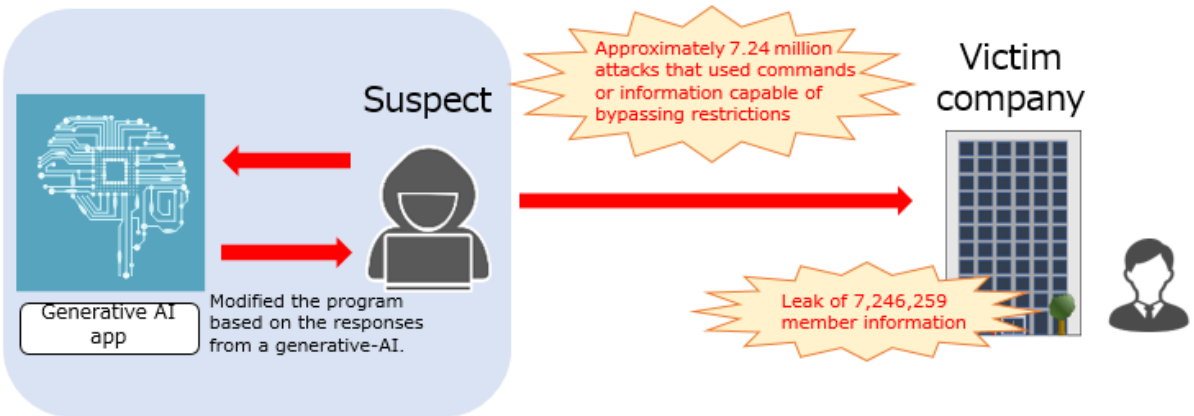
The investigation revealed that these suspects had exploited generative AI to enhance the sophistication of the phishing websites.

With investigative support provided by the Japan Cybercrime Control Center (JC3), the Osaka prefectural police arrested the suspects in June 2025 for the Act on Prohibition of Unauthorized Computer Access.

【CASE：Arrest for developing malicious programs using generative AI】

A 17-year-old high school student exploited generative AI to send approximately 7.24 million malicious commands to the server of a café app, causing a data leak of member information and disrupting some of the app's functions. In December 2025, the Tokyo metropolitan police arrested the student on charges of violating the Act on Prohibition of Unauthorized Computer Access and obstruction of business by fraudulent means. (Tokyo)

【Figure 2: Developing malicious programs using generative AI】

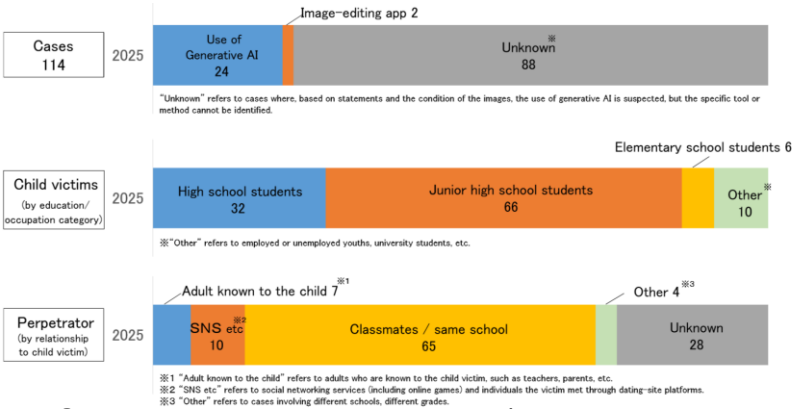


(3) Sexual altered images of Minors

NPA conducted a survey on the actual conditions in 2025 regarding cases handled by prefectural police involving the misuse of images of real minors that were altered using generative AI platforms and image-editing applications.

In 2025, there were 144 such cases were handled and 24 cases misused generative AI.

By student and occupation category of the victims, 32 cases involved high school students, 66 involved junior high school students, and 6 involved elementary school students.



children's images using generative AI and other

Regarding the relationship between victims and offenders, 7 cases involved adult acquaintances, 10 cases originated through Social Medias, and 65 cases involved classmates or individuals from the same school.

The police are taking actions such as making arrests for violating the Penal Code (e.g., defamation, distribution of obscene objects) and issuing instructions or warnings, based on the specifics of each case and with due consideration for the feelings of seeker and victims.

Column : an international conference of AI and Digital Forensics

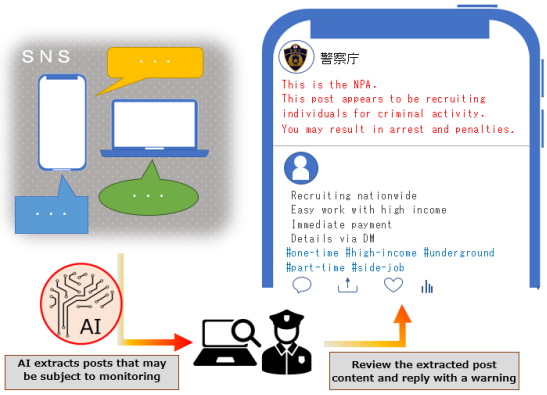
In October 2025, ICPO, NPA and JC3 jointly hosted "Interpol Conference on AI and Digital Forensics". There were over 90 practitioners and experts from foreign law enforcement agencies, private companies, and academic institutions. Participants shared information and held discussions on criminal tactics exploiting AI that are emerging in each country, as well as technologies for detecting deepfakes.

【Speech by Director General of Cyber Affairs Bureau】

3 Police Efforts for the Utilization of AI

(1) Police measures against criminal perpetrator recruitment

In February 2024, NPA developed a system that uses AI to efficiently extract information related to criminal perpetrator recruitment information on social media. Since April of the same year, NPA has been issuing prompt individual warnings to posters by utilizing the reply function. In 2025, a total of 6,829 individual warnings were issued.



【Figure 4： Warning by Using AI】

(2) Sophistication of Cyber Patrols

NPA outsources cyber patrol activities, which involve detecting illegal and harmful information on the internet. To improve the efficiency of detection and analysis of information on social media, the Cyber Patrol Center (CPC), the contracted organization, has introduced an AI-based search system that automatically collects illegal information or "information closely related to serious crimes" and determines its relevance, thereby enhancing the sophistication of cyber patrols.

(3) Enhancing the Sophistication and Efficiency of Phishing Website Detection

As part of its anti-phishing measures, NPA collects and evaluates phishing URL information obtained by prefectural police through consultations and other means, providing this data to filtering service providers. In February 2026, the NPA introduced an automated detection tool using generative AI to further enhance the sophistication and efficiency of phishing site detection.

(4) Optimization on Analysis of Malicious Program with Generative AI

The Digital Analysis Division of the NPA is promoting the sophistication and efficiency of digital analysis technologies. For example, the division dispatched a researcher to the Institute of Information Security

to conduct research on machine learning techniques aimed at improving the efficiency of malicious program analysis. To apply the generative AI, "RevLlama," which was developed in the research to estimate the functions of malicious programs, to real-world operations, the division trained it on the analysis results of malicious programs that had been conducted in the past, and the AI was able to infer some of the program's functions.

Column: Research at The Research Center for Cybersecurity

The Research Center for Cybersecurity of the National Police Academy conducts research on the analysis of electronic devices and advanced ICT that could be exploited for crime. To analyze malicious programs exploited in cybercrime, the Center is conducting research to enhance analysis sophistication using generative AI. In 2025, in collaboration with academic institutions, the Center developed and validated a system capable of autonomously analyzing malicious programs.

【Presentation of research results】

4 Future prospects

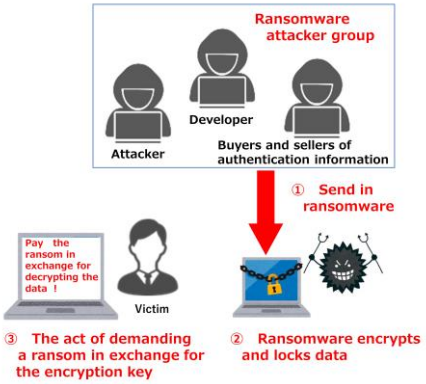
Considering AI's impact on society, the police must respond proactively. The police are already utilizing AI to collect criminal perpetrator recruitment information and are advancing efforts to apply AI in addressing threats posed by anonymous and fluid criminal groups, as well as lone offenders. At the same time, there have been cases in which AI has been exploited to develop malicious programs. The AI Basic Plan outlines the promotion of AI utilization for the advancement of police activities and responses to crimes that exploit AI. Furthermore, the Cybersecurity Strategy sets out the promotion of initiatives to ensure cybersecurity by using AI and to prevent damage from cyberattacks, that are expected to pose an even greater threat as AI advances. Accordingly, the police will robustly implement these policies to earn public trust.

Special Feature II　Ransomware threats and Police Efforts

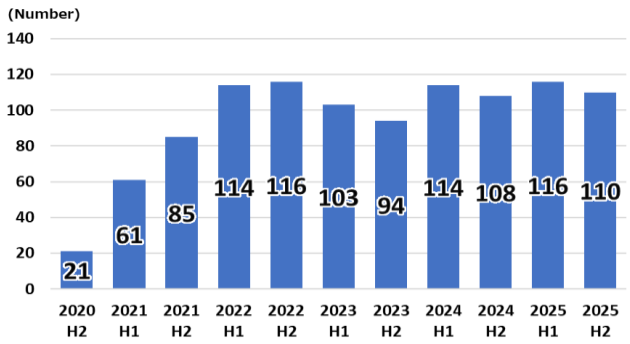
1　Ransomware Threats

Ransomware is malicious software that encrypts data stored on a device, rendering it unusable, and then demands payment (money or cryptoassets) to decrypt it. In recent years, a large proportion of victims have been victims of double extortion, where data is stolen and then compensation is demanded, such as "we will release the data if you do not pay us." In fact, there have been numerous cases where financial information and personal information have been posted on leak sites on the dark web. Furthermore, there have also been cases where data is stolen without encryption using ransomware, and then compensation is demanded by threatening to release confidential information.

【Figure 5：Image of Ransomware Attack】



【Figure 6：Number of ransomware attack reports】



In 2025, there were 226 reported cases of ransomware attacks, remaining at a high level. In addition, several attacks resulted in prolonged disruption of business activities and impacted the lives of citizens.

【CASE: Major Ransomware Attack Cases in the Second Half of 2025】

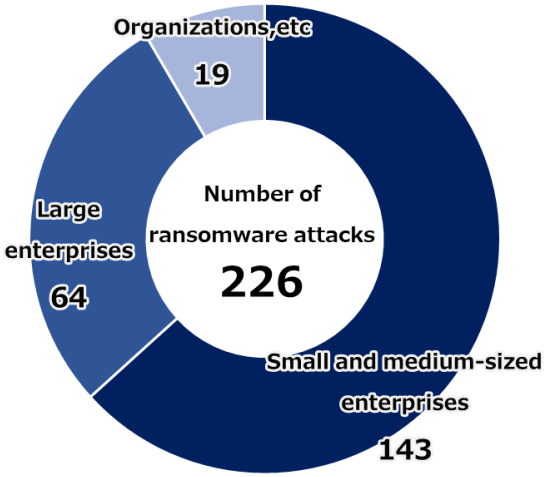
In September 2025, a major beverage company reported that its servers had suffered a ransomware attack. According to the company's investigation, the attacker intruded into the data center network via network equipment within the company's group and executed a ransomware attack, encrypting data on multiple servers. Due to this attack, the receipt of orders and shipment of products were suspended, and the company reported that approximately 1.91 million records of personal information of customers and employees might be leaked.

In October 2025, a major e-commerce company also announced that its servers had infected a ransomware attack. According to the company's

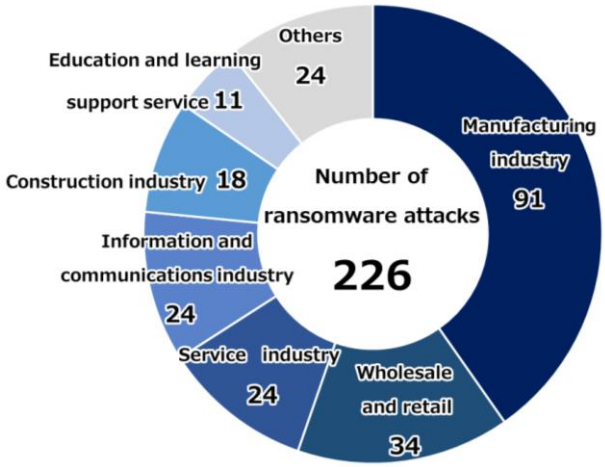
investigation, the attacker stole and illegally used authentication credentials to access multiple servers and executed a ransomware attack. This attack affected the receipt of orders and shipment of products, and approximately 740,000 records of personal information of customers and employees might be leaked.

Regarding the size of victim organizations, small and medium-sized entities (SMEs) account for approximately 60%, like the previous year. By industry, manufacturing accounts for approximately 40% of the damage, followed by wholesale and retail trade, services, and information and communications. However, damage has been confirmed in a variety of industries.

【Figure 7：Number of Cases by Victim Size】

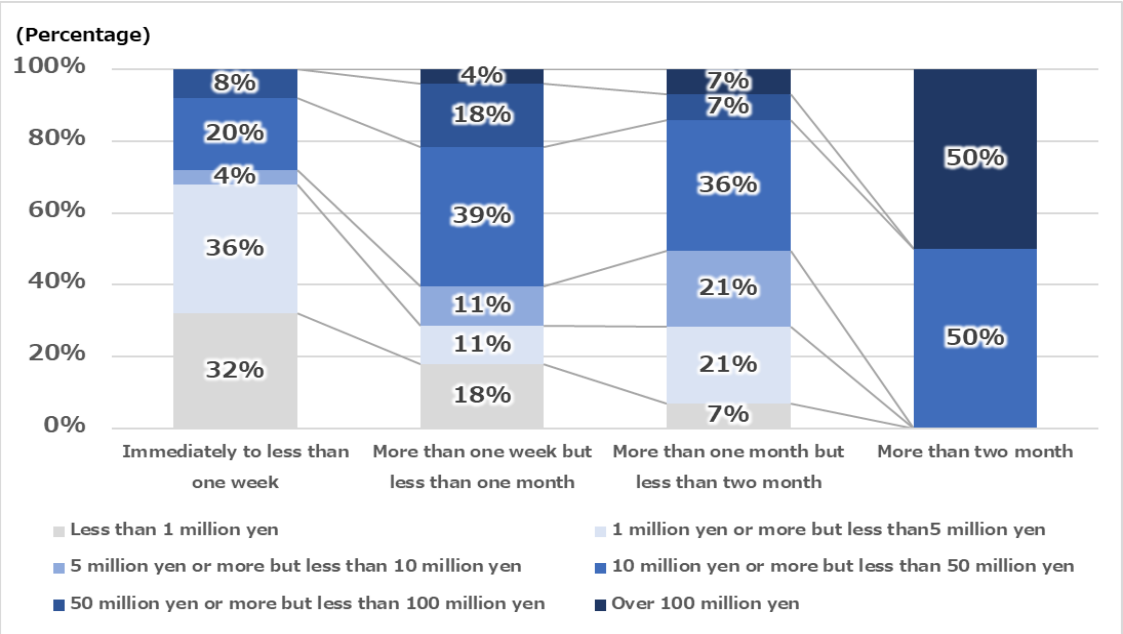


【Figure 8：Number of Cases by Industry】



According to a survey conducted in 2025 among victim entities, the costs of investigating and recovering from ransomware attacks remained high, as in 2024. More than half of the organizations surveyed incurred total costs of 10 million yen or more for recovery. Furthermore, regarding the time required for recovery, only slightly more than 50% of organizations recovered in less than a month, indicating a tendency for the damage to be prolonged. This is likely to have a significant impact on the management of affected organizations, and it could also have a major impact on the lives of citizens.

【Figure 9：Relationship between recovery time and cost from ransomware attacks】



※ The percentages in the diagram are rounded to the nearest tenth, so they do not necessarily add up to

2 Ransomware attack methods

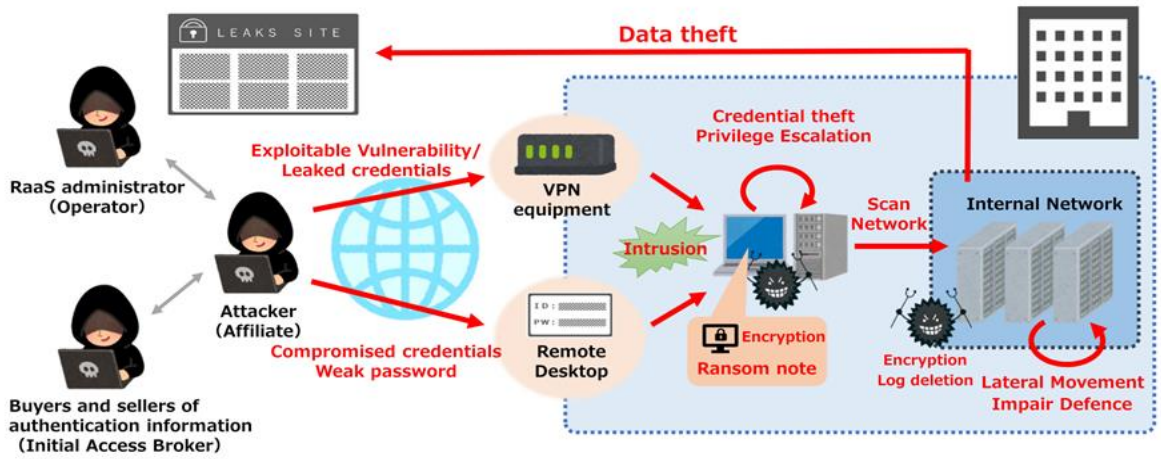
One method of ransomware attacks that has been observed is RaaS (Ransomware as a Service), where the group that develops and operates the ransomware provides the attacker with the necessary environment, such as ransomware and leak sites, and receives a portion of the ransom in return. As a result, even those without advanced technical expertise can carry out ransomware attacks, leading to a broadening of the base of attackers.

Attacks using RaaS are carried out by numerous perpetrators known as affiliates, so even though they use the same ransomware, the specific methods vary. The typical flow of a ransomware attack against a company or other organization is as follows.

In recent years, attackers have predominantly used methods where they remotely infiltrate networks from exposed points on the internet, while infections via attachments in targeted phishing emails and similar emails have become less common. According to a survey of affected organizations, VPN (Virtual Private Network) devices accounted for more than 60% of the intrusion routes. Attackers exploit unpatched vulnerabilities, leaked credentials, weak passwords, and misconfigurations to infiltrate an organization's network. Then, to gain access to a wider area, they explore the network's interior, attempting to seize administrator privileges and disable security measures, while searching for important data and backups. After completing a thorough internal search, the system uploads the data to cloud storage or similar locations for theft, then launches ransomware to encrypt it. Backups are often encrypted along with the original data to prevent recovery. Finally, the user saves the ransom

note on their desktop or elsewhere, requests contact from the attackers, demands payment of the ransom, and then erases all traces of the logs and tools used to end the attack.

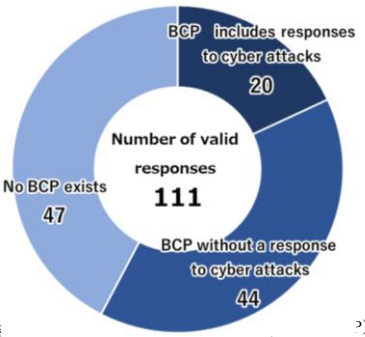
【Figure 10：Image of Ransomware Attack Flow】



3　Preparing for ransomware attacks

Ransomware attacks are fundamentally financially motivated, and attackers seek out targets with vulnerabilities to infiltrate. Therefore, to prevent ransomware attacks, it is necessary to thoroughly implement security and management measures within organizations and companies to eliminate these vulnerabilities, and for managers and employees to have a high level of digital literacy. Specifically, the most important thing is to continue to thoroughly implement basic security measures, such as software updates, proper password management, and appropriate settings for access rights. VPN devices, which are major entry points for intrusions, require prompt action.

On the other hand, because cyberattacks are constantly changing in methodology and becoming more sophisticated, it is difficult to completely prevent them. Therefore, the police are promoting the establishment of systems that anticipate cyberattacks on businesses and other organizations.



【Fig　　2)
Development by Affected Companies and Organizations】

While ransomware attacks disrupt business operations frequently, few organizations have developed a business continuity plan (BCP) that anticipate cyberattacks. According to the survey, only 18% of victim entities had BCP considering cyberattacks. Because ransomware attacks cause unique damages differently from physical disasters such as earthquakes, investigation, recovery work, and public announcement should be also special. Thus, it is necessary to prepare BCP for cyberattacks in advance. In addition, establishing a management system that takes cyberattack risks into consideration is effective in mitigating damage, including managing information assets such as offline backups as an encryption countermeasure, acquiring logs essential for identifying the scope of the breach, training on how to respond to ransomware

attacks, and coordinating with the police. In June 2025, NPA, in collaboration with the Cabinet Office's Public Relations Office, produced a public awareness video introducing ransomware countermeasures, demonstrating their broad efforts to raise awareness.

○Government of Japan Public Relations online:
Small-Medium Size Entities Attacked by Ransomware
https://www.gov-online.go.jp/useful/202506/video-298784.html

4 Response measures after ransomware attacks

If you become a victim of ransomware, the first thing you should do is isolate the infected device from the network to prevent further damage.

Turning off the power in a panic can erase logs and other evidence of the intrusion, potentially making subsequent forensic investigations difficult, so caution is necessary. In the initial stages, efforts should be made to prevent further damage and preserve data such as logs, and only after establishing the organization's response system should investigation and recovery work be undertaken. Furthermore, if damage is discovered, it is necessary to report it to the police and relevant organizations as soon as possible. Organizing and recording contact information in BCPs or similar documents will enable smooth coordination in the event of a disaster. Depending on the circumstances of the victimized organization, the police can provide support such as advice on initial response and provision of decryption tools and will also promote investigations aimed at apprehending suspects in cooperation with the relevant countries. Regarding the payment of money and other charges demanded by ransomware attack groups as payment for decrypting encrypted data, the police have explained to victims that "there are concerns that this may become funding for criminal groups" and "there is no guarantee that the encrypted data will be decrypted." We are also requesting cooperation in the investigation, including providing information about the ransomware attack, including whether the demanded money and other charges were paid.

5 Clearance of ransomware cases

The Japanese police, mainly the National Cyber Department (NCD), conduct international joint investigations into ransomware groups that damage to companies worldwide, including those in Japan.

[CASE: International joint Investigations into "LockBit"]

Regarding the ransomware group "LockBit," the Japanese police carried out international joint investigations with EUROPOL and other partners. In this case, NCD developed an original decryption tool and shared it to help the victim entities around the world to recover from the damage. Through this international joint investigation, four suspects were arrested in October 2024.

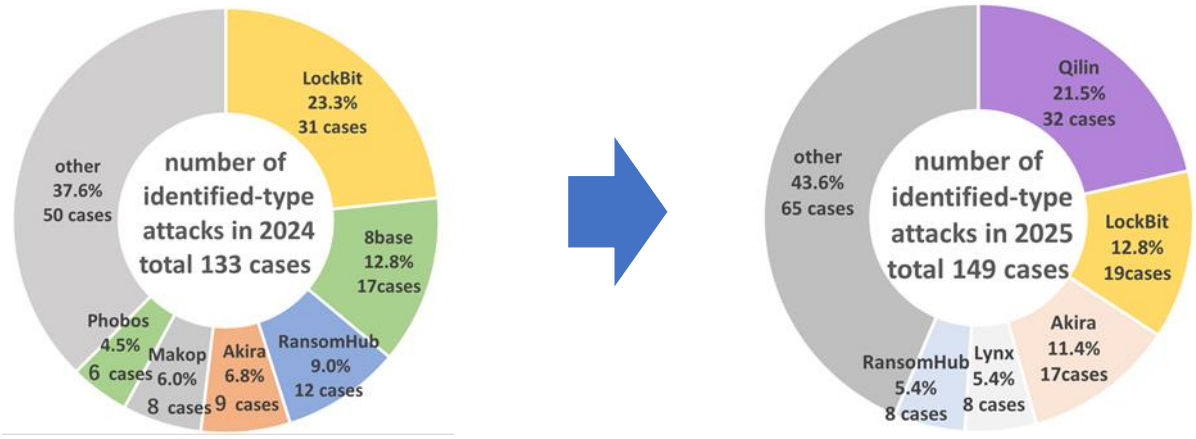
[CASE: International joint Investigations into "Phobos/8Base"]

Regarding the ransomware group "Phobos" and its affiliated organization "8Base," the Japanese police carried out international joint investigations with EUROPOL, FBI and other partners. As a result, five suspects were arrested through this joint investigation, three of them were identified by NCD. More importantly, in July 2025, with the cooperation of FBI, NCD developed a decryption tool.

Arrests of ransomware groups through international joint investigations have proven highly effective, significantly reducing the incidence of similar ransomware attacks. In fact, LockBit and Phobos/8Base—which were among the most frequently reported in 2024—experienced a substantial decline in cases in 2025 following these international collaborative efforts (LockBit: 31 → 19 cases; Phobos/8Base: 23 → 1 case).

In 2025, however, new ransomware threats have emerged, with the proportion of cases involving “Qilin” increasing sharply. To deal with such new threats, the police should continue to actively participate in international joint investigations and to promote the disruption and apprehension of ransomware groups.

【Figure 12：Change in Attack Group Trend】



1 Cyberattacks exploiting advanced technology

During 2025, a series of DDoS attacks (Distributed Denial of Service) against government agencies, financial institutions, and other critical infrastructure operators, as well as cyberattacks aimed at cyber espionage, occurred in rapid succession. Cyberattacks on the nation and its critical infrastructure raise security concerns and can threaten national security; thus, maintaining order in cyberspace is closely intertwined with Japan's overall security efforts.

As part of their preparation, attackers sometimes conduct reconnaissance of potential targets in advance. In this regard, the sensors installed by NPA in FY2025 detected a high volume of suspicious accesses that appear to be vulnerability-scanning activities. The number of such accesses was 9,605.7 per IP address per day (0.9 % increase year-on-year), remaining at a consistently high level. Most of these accesses originated from overseas (see Figure 13).

Similarly, the Network Incident analysis Center for Tactical Emergency Response (NICTER), a cyberattack monitoring and analysis system operated by the National Institute of Information and Communications Technology (NICT) recorded suspicious access counts that reached a record high in FY2025: 6,862.1 per IP address per day (3.4 % increase year-on-year). This is the highest figure observed since the monitoring began (see Figure 14). Of the accesses that NICT classified as "attack-related," about 45.0 % fell into this category, exceeding the 39.8 % recorded in FY2024. Moreover, accesses targeting numerous unspecified devices accounted for more than half of all observed accesses. This indicates that, rather than being limited to specific vulnerabilities or attack techniques, devices and services publicly exposed on the Internet are continuously being scanned by third parties constantly.

Figure 13: Suspicious access counts (NPA)

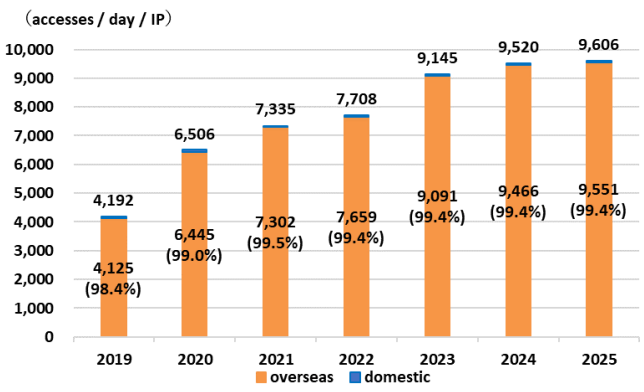
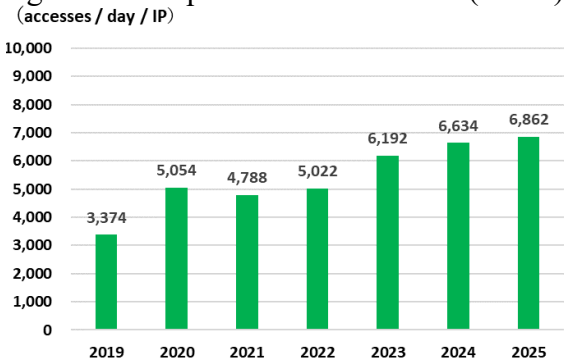


Figure 14: Suspicious access counts (NICT)



Source: National Institute of Information and Communications Technology (NICT), "NICTER Observation Report 2025"

When comparing the number of suspicious accesses observed by the NPA and the NICT, some differences can be seen, but both agencies show the same overall trend: the number of suspicious accesses is increasing.

(1) Cyberattack suspected of state involvement

Cyberattacks suspected of state involvement include cyber-terrorism that disables the core systems of critical infrastructure, thereby paralyzing societal functions, and cyber espionage that uses information-communication technology to steal confidential information from government agencies and companies possessing advanced technology.

Cyber-terrorism can make it difficult to maintain infrastructure functions and provide services, potentially causing severe damage to citizens' lives and socio-economic activities. For example, in May 2025, authorities in the United States and other Western countries issued a joint cybersecurity advisory concerning cyberattacks by the Russian General Staff Main Intelligence Directorate (GRU) targeting logistics and technology firms in the West. The advisory noted that GRU is also likely linked to a large-scale campaign against IP cameras in Ukraine and neighboring NATO states.

Cyber espionage not only deprives companies of sources of competitive advantage but can also have a serious impact on Japan's economic security. Moreover, it is feared that such espionage is conducted as a preparatory act for physical terrorism, aiming to steal confidential information about the security arrangements of critical infrastructure. In August 2025, the NPA and the National Cybersecurity Office (NCO) joined a U.S.-issued international advisory that identified the China-sponsored hacking group "Salt Typhoon" as conducting cyber espionage against telecommunications operators. Salt Typhoon's activities, which target networks worldwide, have been linked to several Chinese companies that supply cyber-related products and services to the People's Liberation Army (PLA) and the Ministry of State Security (MSS). Data obtained by Salt Typhoon are used to enable operations by Chinese intelligence agencies.

Cyberattacks suspected of state involvement have also been carried out to obtain foreign currency by stealing cryptoassets. A United Nations Security Council report released in March 2024 stated that roughly half of North Korea's foreign-currency earnings are derived from cyberattacks, and that these funds are being used to finance weapons of mass destruction programs. In Japan, a case was reported in May 2024 in which the North Korea-backed hacking group "TraderTraitor" stole cryptoassets worth approximately ¥48.2 billion from domestic cryptocurrency-related businesses.

Column: Trends in State-Sponsored Cyberattacks in 2025

In 2025, the police identified several cyberattacks that are suspected of involving state-sponsored APT (Advanced Persistent Threat) groups. These APT groups primarily target sectors such as information and communications, advanced technology and manufacturing, and academic research. During 2025, cyberattacks that appear to be aimed at stealing information were especially prevalent. It is expected that such cyberattacks targeting Japan will continue beyond 2026.

Chinese APT groups, such as Salt Typhoon, are believed to conduct cyberattacks mainly for the purpose of information theft. In 2025, intrusions into internal networks that exploited known vulnerabilities in network equipment and misconfigurations were confirmed, and activities that seem intended to build attack infrastructure were also observed. Moreover, there is concern that the attackers' improving technical capabilities could make information theft incidents more latent.

On the other hand, North Korea's APT groups are believed to carry out cyberattacks primarily to achieve political objectives and to obtain foreign currency, as exemplified by operations such as TraderTraitor. In 2025, authorities confirmed the construction and expansion of attack infrastructure designed to impersonate real or fictitious individuals by stealing information through targeted phishing emails aimed at private persons and then abusing the stolen data. Additionally, initial intrusion techniques that exploit social-media use against employees of cryptoassets firms have been observed. Given that large amounts of cryptoassets have previously been stolen from domestic companies, cyberattacks aimed at acquiring foreign currency are considered highly likely to continue.

(2) Cyberattacks by criminal groups

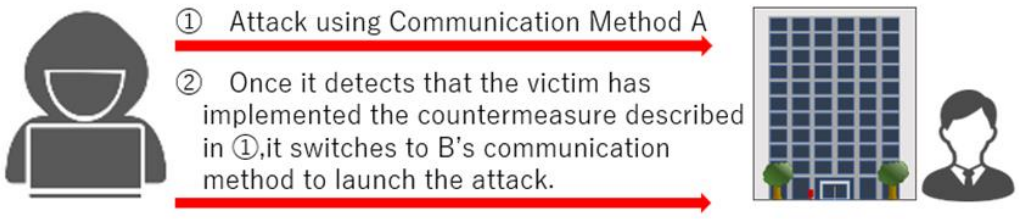
Ransomware is a major example of the cyberattacks by criminal groups. The current state of ransomware and countermeasures are discussed in detail in Special Feature II.

Next is the DDoS attack (Distributed Denial-of-Service). A DDoS attack is a cyberattack that makes the service of a specific computer unavailable by repeatedly generating a large volume of traffic from many computers to the specific computer.

For example, between late December 2024 and early January 2025, a series of incidents believed to be caused by DDoS attacks occurred at critical infrastructure operators such as transportation and financial institutions. These incidents disrupted daily life, including a malfunction that rendered automated baggage check-in machines at airports unusable or difficulties logging into internet-banking services.

The police have identified multiple tactics used in these DDoS attacks and have observed cases where, even after operators implemented blocking measures, the attackers altered their methods in response to the situation and continued the attacks. Furthermore, attacks have been observed in several incidents that bypass content delivery networks (CDNs) by targeting the origin server directly—specifying IP addresses and attacking the server that stores the original web content—thereby circumventing the load-balancing benefits provided by CDNs

【Figure15:Methods Used in DDoS Attacks Against Critical Infrastructures】

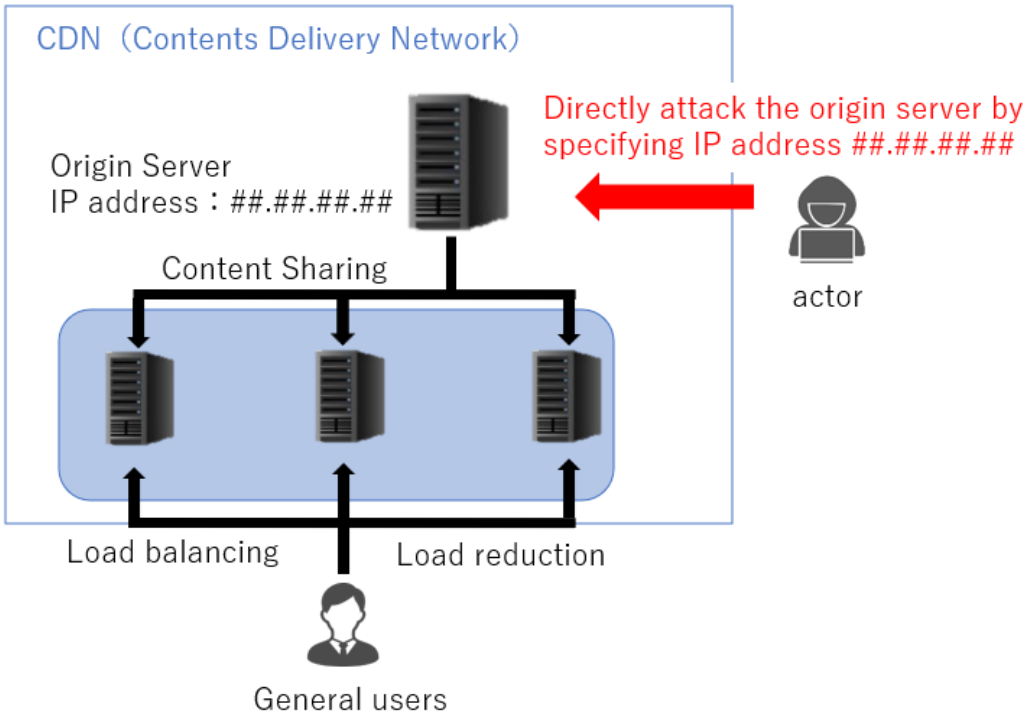


In June 2025, multiple websites operated by government agencies, local municipalities, and private businesses experienced several access disruptions that appear to have been caused by DDoS attacks. Around the same time, posts hinting at these incidents were observed on social media from accounts believed to belong to hacktivists.

To mitigate damage from DDoS attacks, it is necessary to implement measures such as blocking direct access to the origin server that bypasses the CDN, revising DNS settings to prevent the origin server's IP address from

being exposed outside the organization, blocking traffic from IP addresses allocated overseas, deploying mitigation devices or services that monitor traffic and detect and block attacks, and adding redundancy to servers, endpoints, network equipment, and communication lines.

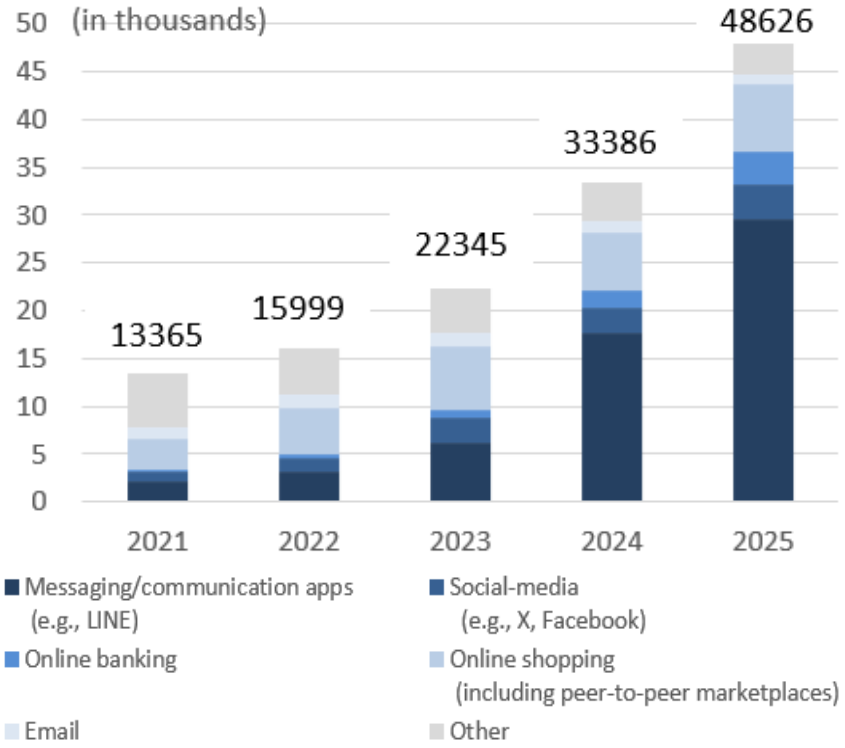
【Figure16：Image of Attack on the origin server during a DDoS attack】



2 Crimes exploiting Internet

While the remarkable advancement of information and communication technology and the integration of cyberspace into daily life and economic activities have brought various benefits to society, they have also given rise to and exacerbated new public safety challenges, including crimes committed in cyberspace. This is reflected in the 185,000 cyber-related police consultations recorded in 2025 and the steady rise of internet fraud—about 60 % of which involved voice or messaging-app scams that year.

【Figure 17：Number of reported cases of　Internet-based fraud and their breakdown】



Some of the technologies and services provided on the Internet facilitate or encourage the commission of crimes. For example, social media and highly anonymous messaging apps are used to recruit people to commit crimes and as a means of communication between criminal groups, while SMS and email are misused for phishing. Furthermore, online banking and cryptoassets are being misused as destinations for the transfer of funds obtained through communications fraud schemes and for money laundering. Data-only SIM cards with SMS functionality are being misused as criminal infrastructure because there is no requirement for identity verification at the time of contract.

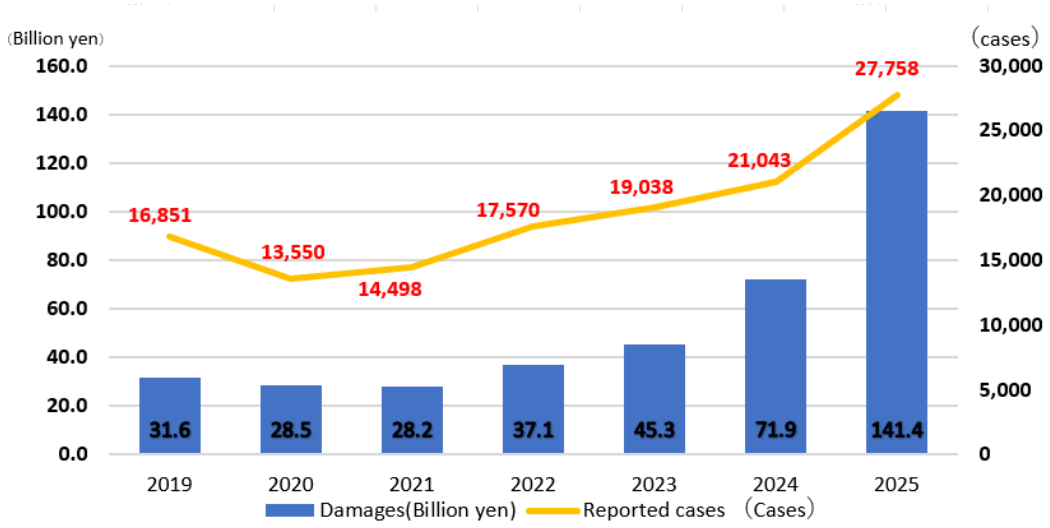
(1)　Crimes misusing Social Media and Messaging Apps

Social media, widely used by the public, is being abused as a criminal infrastructure. For example, “anonymous and fluid criminal groups” —with an anonymized core that siphons crime profits and loosely linked members via social media—are confirmed to be recruiting perpetrators on social media without disclosing the nature of the work, using phrases such as “high-paying” “same-day cash,” “legitimate deals,” and other phrases emphasizing “easy, simple, and high income” to recruit perpetrators and carry out communications fraud. High-anonymity communication tools that automatically delete messages are being misused for contact between ringleaders, coordinators and perpetrators. In addition, the anonymous and fluid criminal groups operate investment/romance fraud via social media,

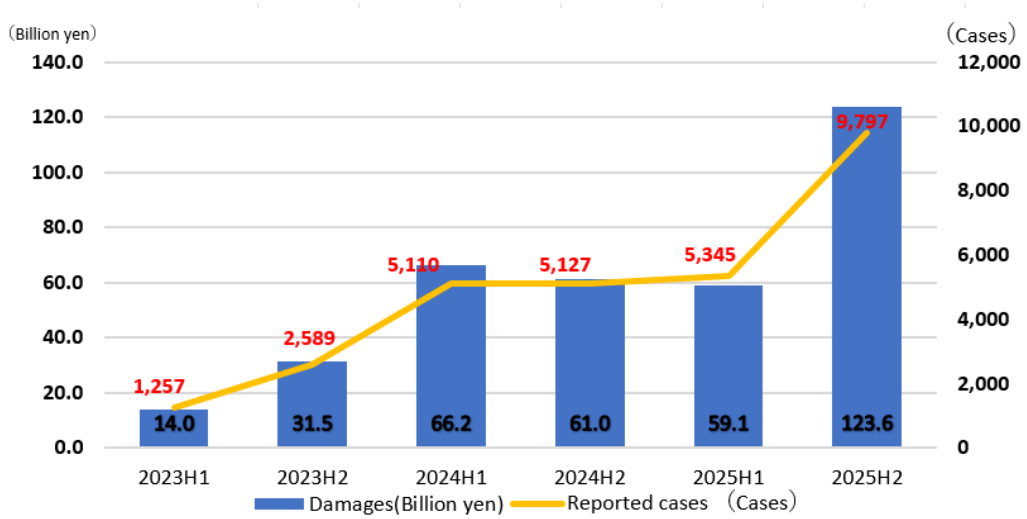
deepening trust through repeated online interactions without ever meeting in person and then defrauding victims with false investment or withdrawal-fee pretenses, or by exploiting romantic feelings. This clearly demonstrates that social media is being exploited as a criminal infrastructure.

In 2025, losses from communications fraud reached about 141.42 billion yen—a 96.7 % year-on-year increase that surpassed the 2024 record, and losses from investment/romance fraud via social media rose 43.6 % to roughly 182.7 billion yen.

【Figure 18：Numbers of reported cases of communications fraud and amounts of damages】



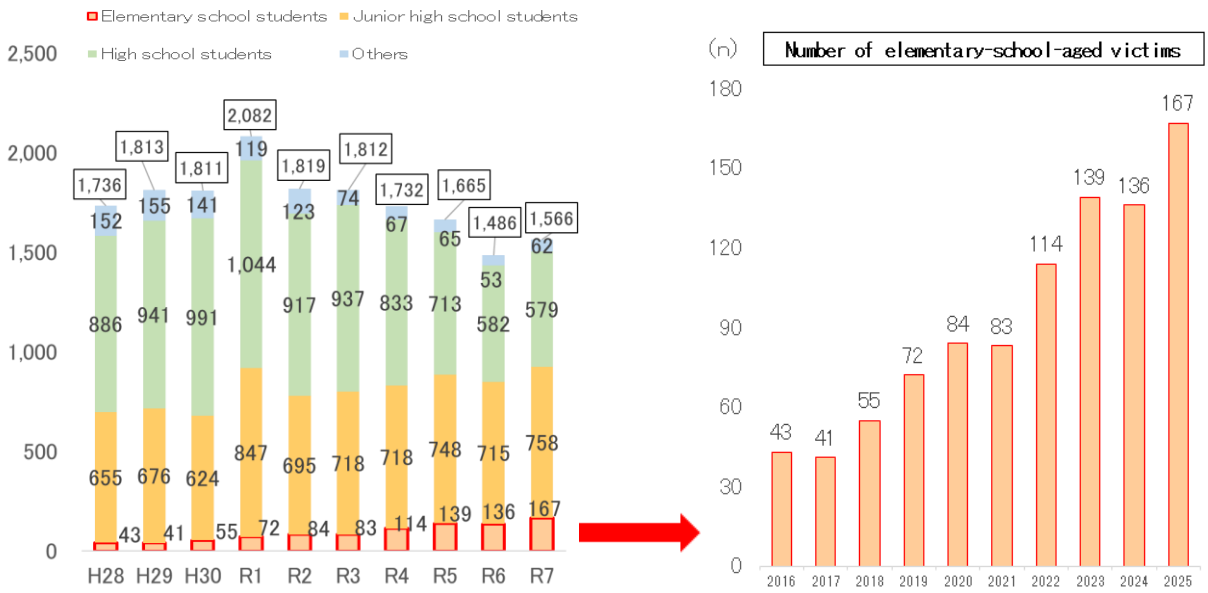
【Figure 19：Numbers of reported cases of investment/romance fraud via social media and amounts of damages】



there have been instances where individuals, after being lured by someone they met online, traveled abroad only to be coerced into participating in communications fraud.

In recent years, defamation and slander on social media have become a social issue, and because the platforms allow anonymous, instant contact with countless users, they have also become a “venue” for serious crimes such as child prostitution. The number of children victimized by sex-related offenses linked to social media remains high, with a notable rise in elementary-school-age victims indicating a trend toward younger victims.

【Figure 20：Number of child victims of social-media-related offenses by school age group】



Note: SNS in this statistic includes online communication games, but excludes any dating sites that are formally registered
Social-media-related offenses are crimes in which a child meets an unknown suspect on an SNS and is victimised before any relationship (dating, friendship, etc.) develops.
Applicable offenses include violations of the Child Welfare Act, the Act on Punishment of Activities Relating to Child Prostitution and Child Pornography, and the Protection of Children, prefectural Youth Protection and Development ordinances, serious crimes (including murder, robbery, arson, penetrative sexual assault, kidnapping by force or enticement, buying or selling of human beings, non-consensual indecent assault, and unlawful capture or confinement), requests to meet, and offenses prescribed in Articles 2 through 6 of the Act on Punishment for Filming Sexual Poses and the Erasure of Electronic or Magnetic Records of Sexual Images Recorded in Seized Articles

Furthermore, the spread of the internet and smartphones has made it easy to disseminate visual content to large, unspecified audiences, resulting in cases where victims suffer long-term psychological distress after non-consensual online publication of sexual images of former partners.

Crimes have also arisen from online-gaming activities, especially real-money trading in which in-game items or currency are exchanged for real-world money (including electronic money).

Japan Cybercrime Control Center (JC3) (See page 56), with the

cooperation of the police and cybercrime prevention volunteers, conducted a survey to understand the actual situation of troubles related to the use of online games, and published the results on the JC3 website in December 2025.

The survey results showed that the majority of those who reported having experienced trouble related to online games experienced communication issues such as in-game chat. Of those, about 30% were found to have been involved in account hijacking, DDoS attacks, or real money trading. The types of problems observed included many cases of users being subjected to verbal abuse through communication features such as chat functions, while multiple cases of phishing and account hijacking were also confirmed.

Furthermore, an analysis of how people responded to problems revealed that, although the accuracy is low due to the limited scale of the survey, problems were significantly more likely to be resolved when people sought advice or made contact compared to when they took no action.

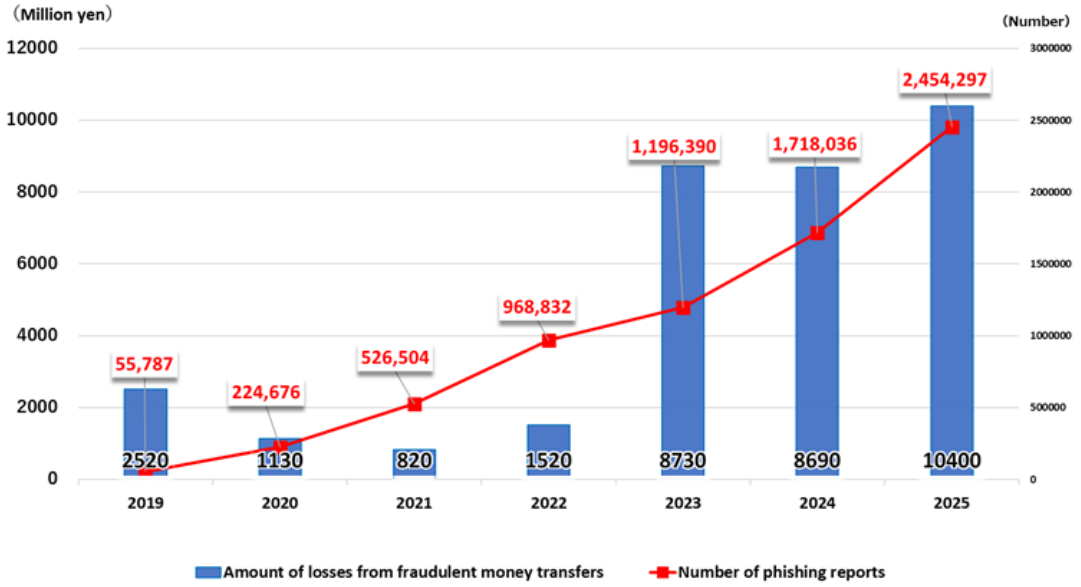
(2) Crimes Exploiting Email and SMS

Emails and SMS are frequently used for phishing. Phishing is a technique in which attackers impersonate real organizations and lure users to fake websites (phishing sites) via links in emails or SMS, thereby illegally obtaining account information, credit card numbers, and other sensitive data. The information gathered in this manner is then used for online banking fraud and fraudulent credit card transactions.

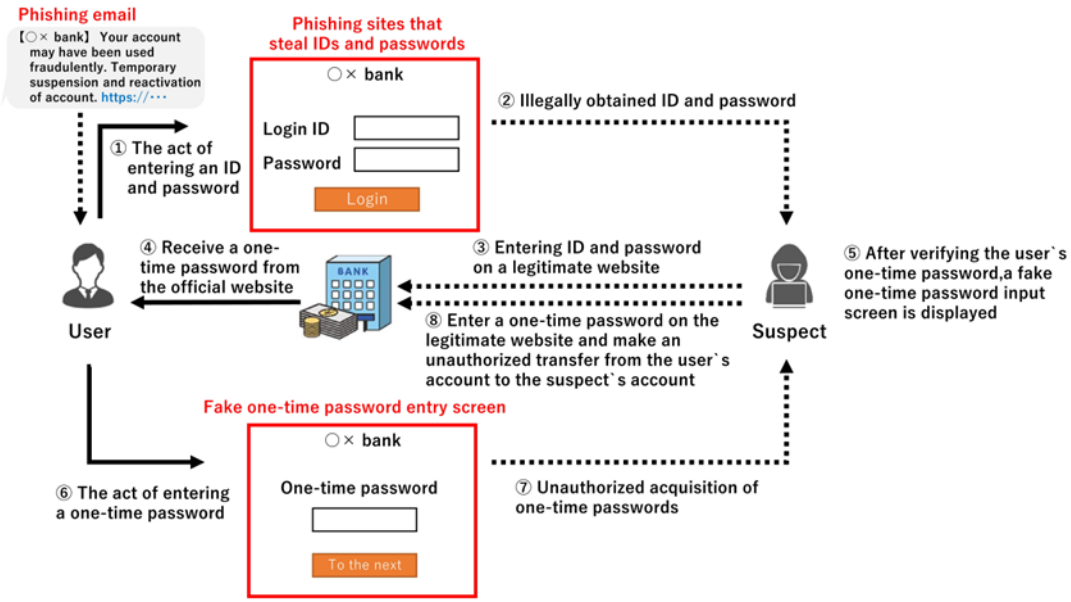
According to the Council of Anti-Phishing Japan, the number of phishing reports in 2025 reached 2,454,297, showing a consistent increase. Furthermore, in 2025, there were 4,747 cases of online banking fraud, with the total loss amounting to approximately 10.397 billion yen, and phishing accounted for about 90% of the methods used in these incidents.

The tactics used in phishing are becoming increasingly sophisticated; for instance, since around 2019, real-time phishing techniques to bypass two-factor authentication have become widespread

【Figure 21：Financial losses from online banking fraud and number of phishing reports】



【Figure 22：Real-Time Phishing Method】



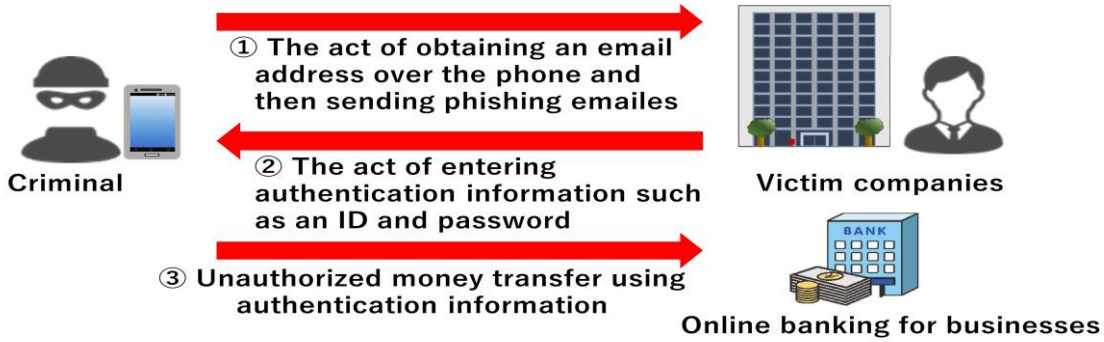
Column: Online Banking Fraud via Voice Phishing

From fall 2024 to April 2025, there was a sharp increase in online banking fraud from corporate accounts using a technique called voice phishing (vishing), in which criminal groups called companies under the guise of procedures like online banking renewals to extract email addresses, and then sent phishing emails. Although no such incidents were reported from May to October of the same year, online banking fraud surged again in November, with many small and medium-sized financial institutions based in regional areas suffering losses.

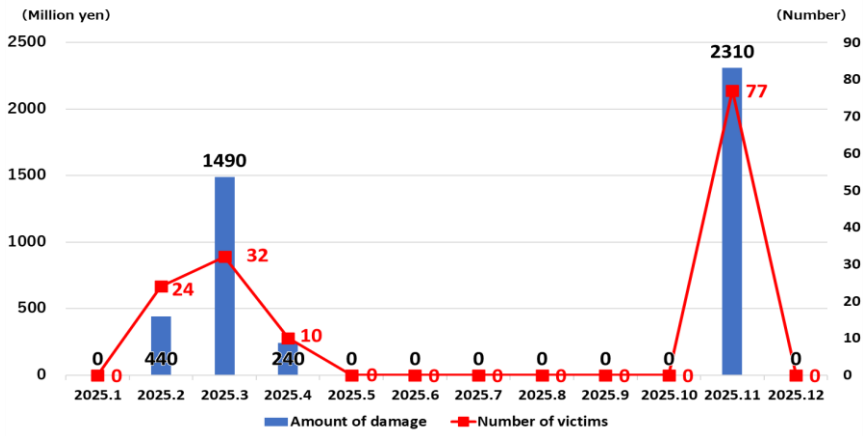
This voice phishing technique typically involves several key characteristics: the caller's number is an international number; an automated voice guidance message plays before switching to a human operator; and the target's email address is requested during the call, followed by an email containing a link.

To prevent voice phishing, it is necessary for companies to thoroughly implement internal security protocols such as calling back a bank's branch or official main number to verify the authenticity of a call from a bank, and accessing online banking services only through a bank's official website or app.

【The process of voice phishing】



【Figure 23：Number of cases and total amount of online banking fraud from cor porate accounts via voice phishing】



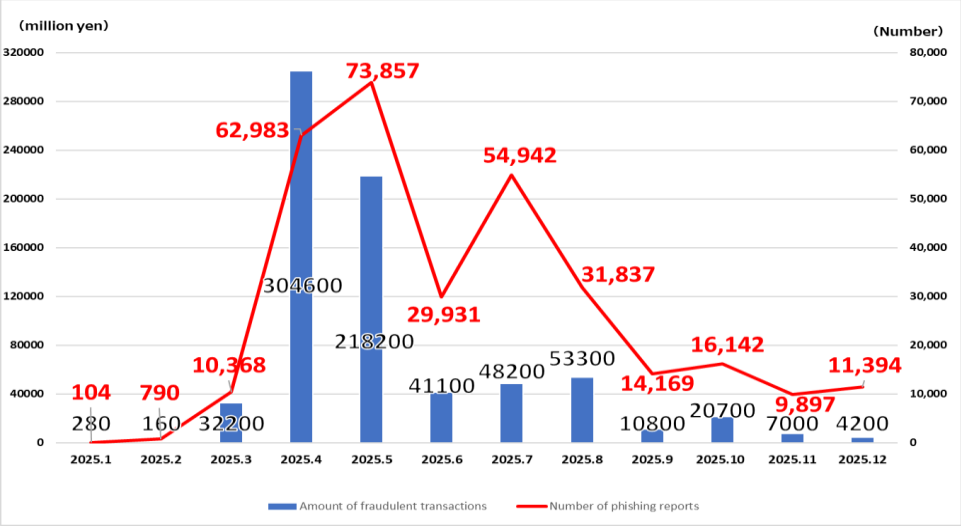
Column: Unauthorized Access to Securities Accounts

From March to May 2025, the transmission of phishing emails impersonating securities companies, as well as unauthorized access to and fraudulent transactions in brokerage accounts, surged. According to the Financial Services Agency and the Council of Anti-Phishing Japan, serious damage occurred in 2025, with 17,668 cases of unauthorized access to brokerage accounts, 9,824 cases of fraudulent transactions, approximately 740.8 billion yen in the amount of unauthorized trading, and 316,414 reports of phishing emails impersonating securities companies.

In November 2025, the National Cyber Department and prefectural police, including the Tokyo Metropolitan Police Department, promoted a criminal investigation with the cooperation of relevant agencies. As a result, they arrested a Chinese man (38) and his accomplices for Violation of the Financial Instrument and Exchange Act (prohibition of market manipulation, etc.) and the Act on Prohibition of Unauthorized Computer Access (prohibition of acts of unauthorized access). After purchasing a large amount of the stock targeted for market manipulation (hereinafter referred to as the "target stock") in advance using securities accounts managed by himself, the man, in conspiracy with an unidentified person, illegally accessed the brokerage accounts of others, secured funds by selling stocks held in the victim accounts, etc., and drove up the stock price by purchasing a large amount of the target stock. Subsequently, he placed orders to sell the target stock he held at a high price, and at the same time, established transactions by purchasing the target stock using the victim accounts, thereby obtaining the difference between the purchase price and the selling price as profit.

In response to the frequent occurrences of unauthorized access to and fraudulent transactions in securities accounts, including this case, the National Cyber Department contributes to criminal investigations by the relevant prefectural police by analyzing data regarding phishing emails and phishing sites impersonating securities companies, analyzing the destination addresses of cryptoassets, and aggregating information on similar cases occurring nationwide.

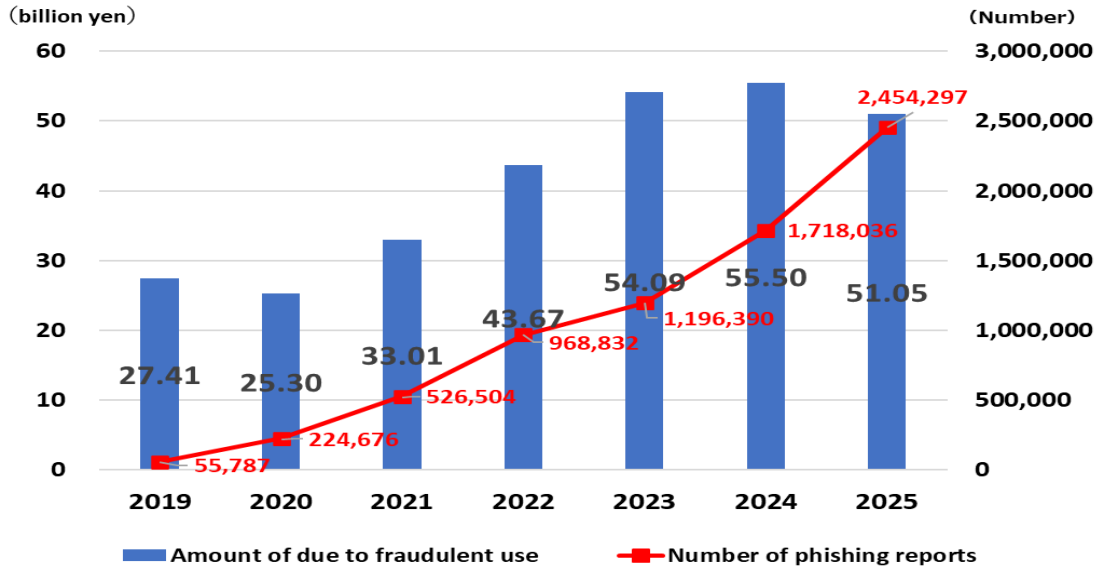
【Figure 24：Amount of Fraudulent Transactions in Securities Accounts and Number of Phishing Reports Related to Them】



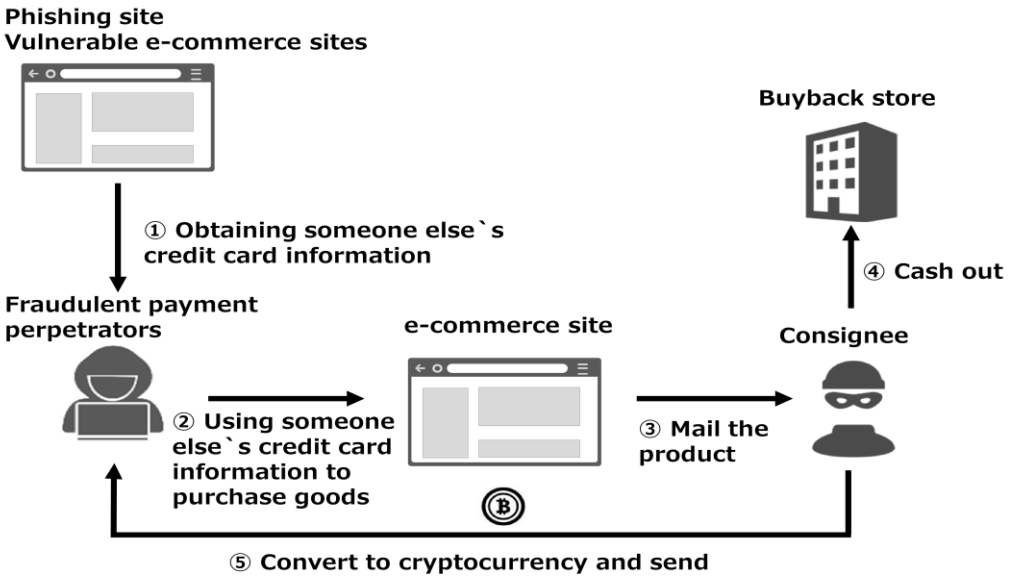
In addition to phishing, other methods of online banking fraud continued to be observed, including cases triggered by malware infections and methods that bypassed identity verification through SIM card swapping.

Furthermore, according to the Japan Consumer Credit Association, the amount of damage caused by fraudulent use of credit cards in 2025 was approximately 51 billion yen (a decrease of about 9% compared to the previous year), indicating that the situation remains severe.

【Figure 25：Credit card fraud losses and number of phishing reports】



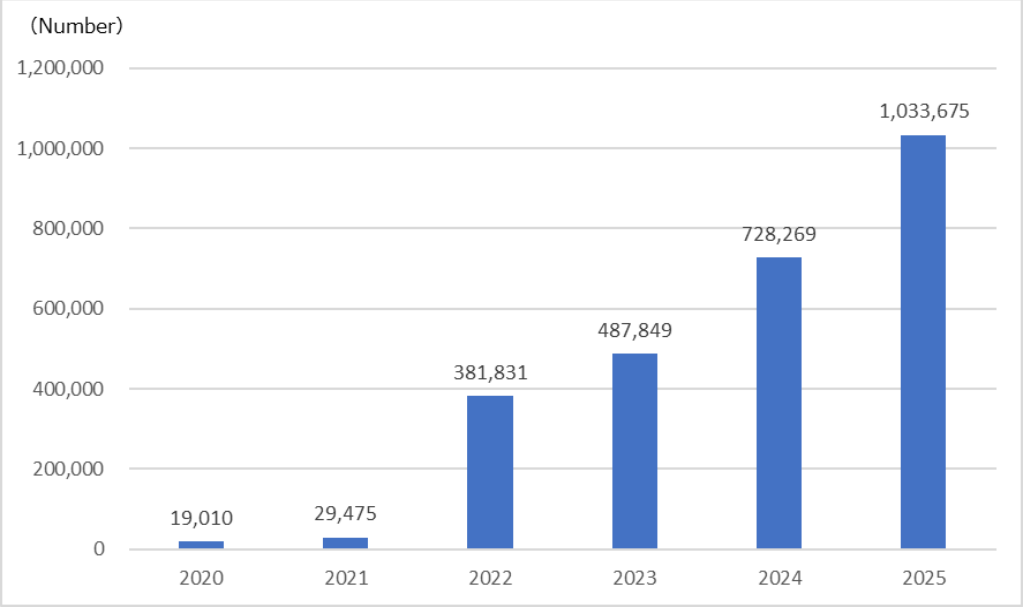
【Figure 26：The process of fraudulent use of a credit card】



(3) Crimes that exploit websites

In some cases, crimes are being committed by not using social media or SMS, but by exploiting websites themselves. For example, there has been a surge in damages related to phishing sites that mimic the websites of real companies and are posted on the internet via overseas servers, as well as sites that aim to commit fraud related to online shopping or sell counterfeit branded goods (hereinafter simply referred to as "fake sites, etc."). NPA is collecting URL information on fake sites, etc. that prefectural police and other authorities have identified through consultations, and the number of such sites is steadily increasing.

【Figure 27 : Number of reports of fake websites to the NPA】



In addition, support scams continue to occur in which users are deceived into believing that their computers have been infected with a virus through fake warning screens or alert sounds displayed while browsing the Internet, inducing them to call fraudulent support centers and pay money or install remote access software. In 2025, the number of recognized cases of fictitious billing fraud involving “technical support” scams—such as fraudulently obtaining electronic money under the pretext of virus removal services—stood at 1,066 (down 30.1% year on year), while losses totaled approximately ¥1.4 billion (up 39.6% year on year).

(4) Crimes Exploiting Online Fund Transfers

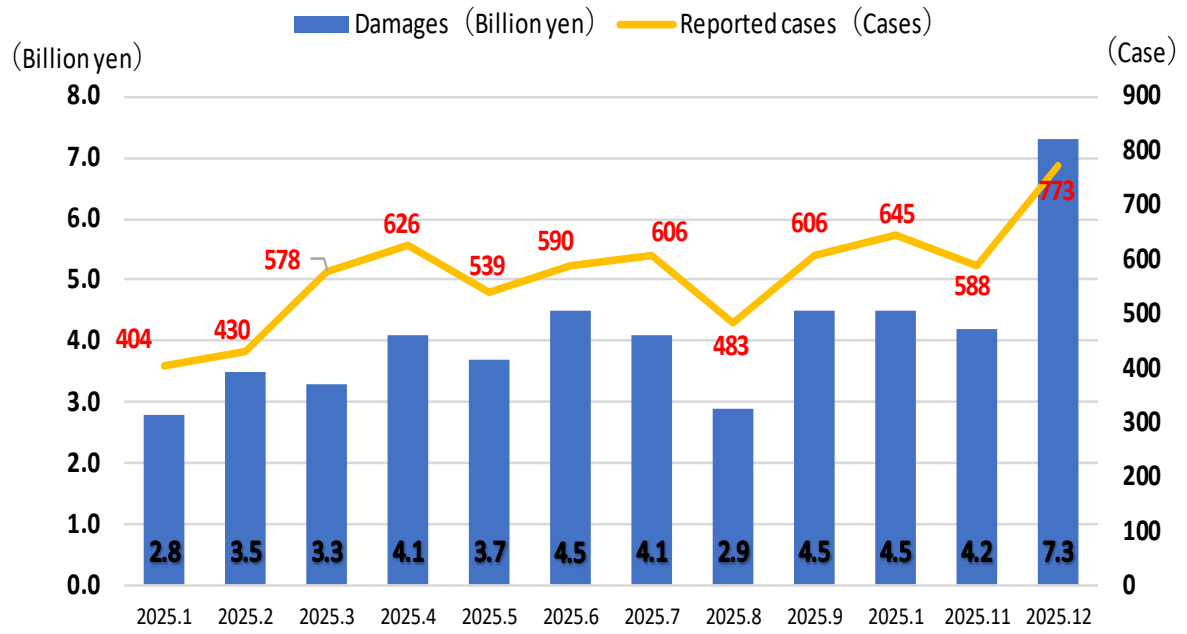
While moving funds online offers great convenience, online banking is being exploited for criminal purposes due to features such as the ease with which daily transfer limits can be increased and the difficulty of third-party oversight during transfers. Similarly, cryptoassets, with their high degree of anonymity, are also being utilized for money laundering.

① Online Banking Fraud

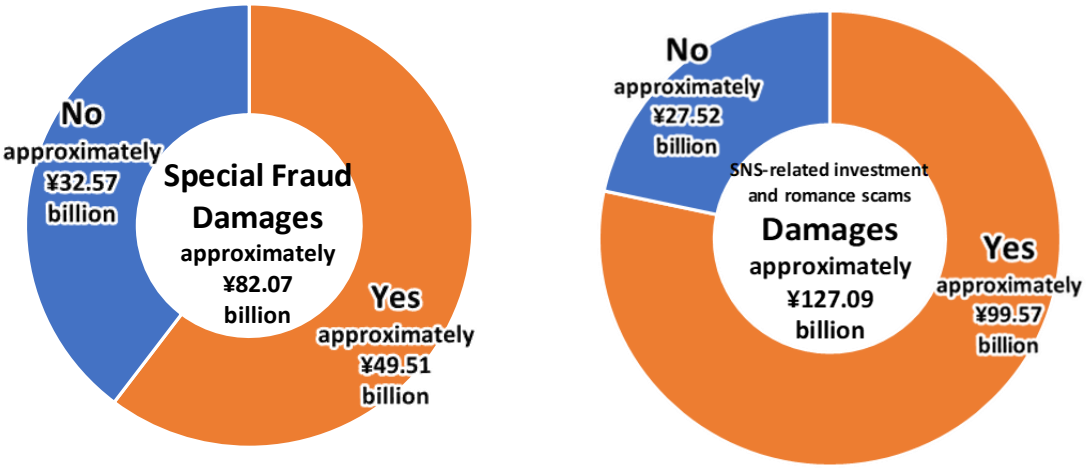
Analysis of transfer-based communications fraud losses (16,862 recognized cases; approximately ¥82.07 billion in losses) shows that cases involving Internet banking continue to increase, accounting for about 40% of all transfer-based cases and 60% of total losses.

Similarly, analysis of transfer-based losses from investment/romance fraud via social media (10,168 recognized cases; approximately ¥127.09 billion in losses) indicates that Internet banking was used in about 70% of such cases and accounted for 80% of total losses.

【Figure 28 : Damage of communications fraud using Online Banking】



【Figure 29 ： Whether Online Banking is used in Scams】



② Cryptoassets

Cryptoassets are abused for criminal activities due to their high degree of user anonymity and the ease of instantaneous transfers in cyberspace, and criminal proceeds are increasingly being concealed in the form of cryptoassets. Regulatory frameworks for cryptoassets differ across jurisdictions, and some countries and regions where cryptoassets exchange service providers operate do not require measures such as customer identity verification. In addition, certain cryptoassets handled by overseas exchange service providers are difficult to trace because transaction records are encrypted. Criminal groups also employ methods to further enhance anonymity, including repeated transfers through so-called unlicensed cryptoassets brokers and the use of “mixing services,” which obscure transaction flows by mixing cryptoassets and concealing links between sending and receiving addresses.

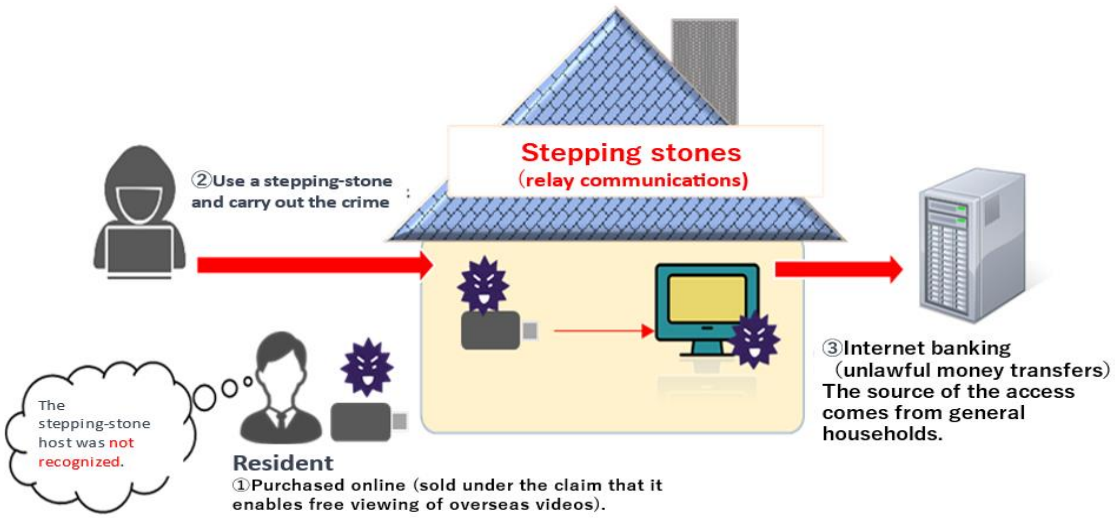
(5) Crimes Abusing IoT Devices as Stepping Stones

It has become clear that there are frequent cases where devices with network connection capabilities used in general households (IoT devices) operate as so-called "residential proxies" (proxies utilizing general household networks) without the knowledge of the device owners, and are abused as stepping stones.

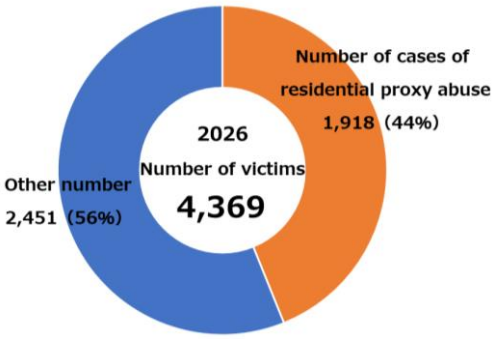
For example, illicit video streaming devices sold under claims such as "You can watch overseas videos for free by connecting it to your TV" are abused as stepping stones for unauthorized acces.

Among these devices, some are distributed with malicious software, such as downloaders, embedded in the stage prior to purchase. By connecting such devices to the internet, malware is installed without the user's knowledge, causing the device to operate as a proxy. When these devices become stepping stones and relay an attacker's communications, the IP address of the device used as the stepping stone, rather than the attacker's IP address, is recorded in the log of the destination server. Even for overseas attackers, by using domestic devices as stepping stones, it becomes possible to access servers that restrict access from overseas, which poses a grave threat to security measures as well as a serious obstacle to cybercrime investigations.

【Figure 30:Image of Cyberattack through IoT Device】



For example, among the online banking fraud that occurred in 2024 (4,369 cases, about 8.69 billion yen), residential proxies were used at least 1,918 cases, with the amount of damage reaching approximately 2.89 billion yen, accounting for 44% of the total number of cases and 33% of the total amount of damage. Furthermore, in 2025, the police have continued to recognize many cases where residential proxies were misused, and they remain a threat to security measures.



【Figure 31: Proportion of Residential Proxies Used】

3 Illegal and Harmful Information

In recent years, the internet has become a social problem due to illegal information such as "information related to recruiting perpetrators for crimes" and "information related to illegal online gambling," whose distribution on the internet itself violates the law. In addition,

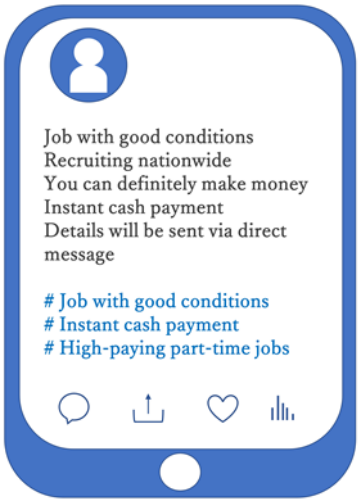
there is harmful information that, while not illegal, cannot be ignored from the perspective of maintaining public safety and order, as it may incite crimes or incidents, and thus poses a threat to public safety in cyberspace.

(1) Main types of illegal and harmful information

The main types of illegal information include obscene information such as "public display of child pornography" and "invitation for prostitution," drug-related information such as "advertisements for controlled substances" and "advertisements for unapproved drugs related to dangerous drugs," as well as information related to possession of firearms, information related to recruiting perpetrators of crimes, and information related to illegal online gambling. In addition, harmful information includes information closely related to serious crimes that pose a high risk of harming an individual's life or physical safety, such as "manufacturing explosives," "contract killing," and "human trafficking," as well as information that induces suicide, such as "involvement in suicide" and "inducement or encouragement of suicide."

(2) Criminal perpetrator recruitment information

【Figure 32 : Image of perpetrators for crimes】



In recent years, the internet has been flooded with criminal perpetrator recruitment information by anonymous and fluid criminal groups, and in 2025, 14,241 of the cases received by the Internet Hotline Center (IHC) were determined to be criminal perpetrator recruitment information. The proliferation of this type of information is becoming a more serious threat to public safety, as it has led to actual crimes such as robbery and fraud being committed by people who respond to such recruitment information.

Also, regarding robbery and theft, it appears that perpetrators who carry out the crimes are recruited through social media and job sites using phrases such as “high pay,” “paid on the spot,” and “job with good conditions”. Among the robberies and other crimes carried out using methods believed to be employed by such anonymous and fluid criminal groups, some involve particularly heinous acts, such as restraining victims and then assaulting them.

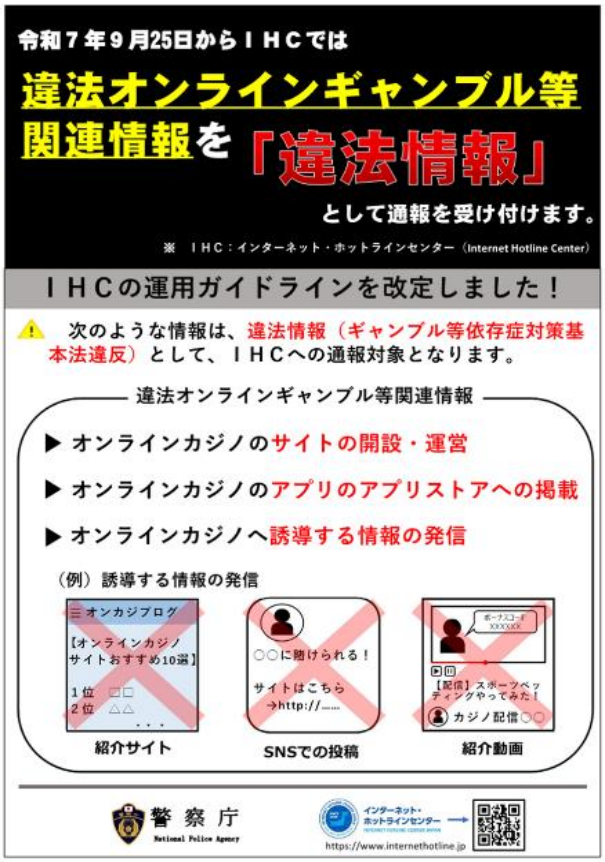
Column: Measures against Illegal Online Gambling

In fiscal year 2024, NPA conducted a survey to assess the current state of online casinos. The results showed that approximately 3.37 million people in Japan have used online casino websites, and the estimated annual amount wagered domestically totaled about 1.2423 trillion yen

"Non-store-based" online casinos accessed via smartphones and other devices have been widely identified as contributing to increased access to gambling and the accompanying problem of gambling addiction. Concerns have also been raised that such platforms may facilitate the outflow of Japan's national assets overseas and money laundering.

On June 18, 2025, the Basic Act on Measures Against Gambling Addiction was amended to prohibit acts such as disseminating information that directs users to illegal online gambling via the Internet. In conjunction with the law's enforcement on September 25, the Ministry of Internal Affairs and Communications revised the "Guidelines Concerning Article 26 of the Basic Act on Measures Against Rights Infringement, etc. Arising from Distribution of Information by Specified Telecommunications Additionally, the "Guidelines on Dealing with Illegal Information on the Internet" were revised.

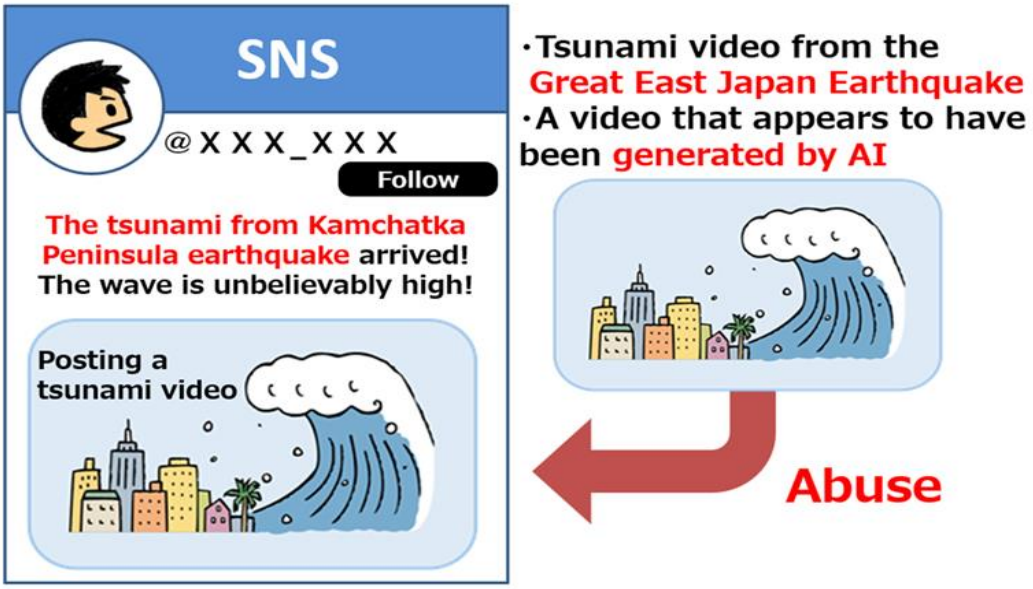
On the same day, the Internet Hotline Center (IHC) revised its operational guidelines, newly classifying information related to illegal online gambling as illegal information. It now accepts reports from internet users and strengthens its efforts to prevent the spread of this information, which has become a social problem, by reporting to the police and requesting website administrators to remove the content.



(3) Disinformation during disasters

Disinformation and misinformation on the Internet during large-scale disasters require time to verify and assess its reliability, and they likely hinder rescue operations and cause social disruption in the affected areas. In fact, there have been confirmed cases in which Japanese and foreign-language disinformation—such as the abuse of images taken during previous earthquakes to suggest deteriorating public safety or massive damage in the same region—has been spread on social media during disasters.

【Figure 33 : Image of Disinformation posted on SNS】



(4) Foreign Disinformation

In recent years, influence operations—including dissemination of disinformation—have been carried out internationally in various forms to affect public opinion and decision-making in other countries, and to create a favorable information environment to the perpetrating state.

The spread of disinformation is often used in conjunction with military means and to interfere in elections. This poses a security threat to our country; not only because it undermines the foundations of democracy, such as the integrity of elections and freedom of speech, but also because it may adversely affect public security in Japan. With the advance of generative AI technology, it has become a key issue how to address the risks regarding the mass production of sophisticated disinformation and its dissemination.

CHAPTER 2 Police Efforts

Topic Ⅰ: The Role of Cyber Police in National Security

1 Police initiatives in response to national security threats

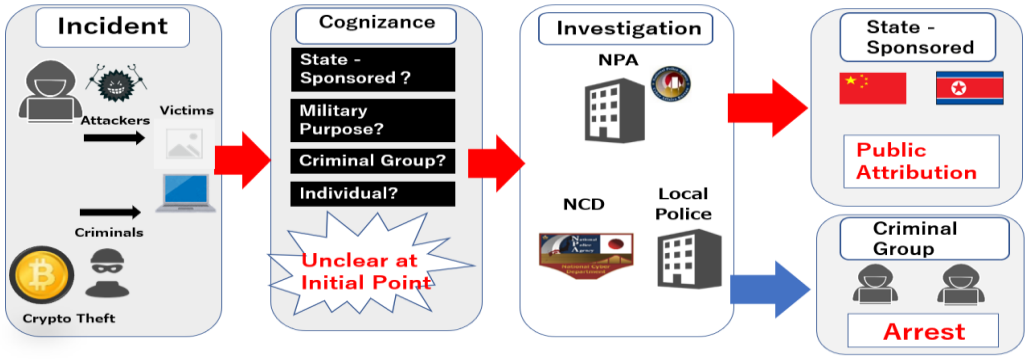
Cyberattacks targeting government agencies and critical infrastructures are threats threat to Japan's national security. However, due to the nature of cyberattacks, it is impossible to immediately determine the perpetrator or the purpose of the attack at the time it occurs. Therefore, the police must respond to all cyber incidents with the understanding that they could involve national security concerns, such as attacks backed by a state actor or those carried out for military purposes.

Specifically, the police first identify cyber incidents through various police activities, such as 110 emergency calls, public inquiries, and information provided by foreign law enforcement agencies. Then, while keeping in mind the possibility that these cyber incidents may be directly linked to national security, the police conduct investigations into the incidents and work to clarify the facts by collecting and analyzing threat intelligence related to cyberattacks and performing comprehensive analyses.

If police investigations reveal the possibility of state involvement in a cyberattack, they issue public warnings regarding the identified attack methods and infrastructure to prevent further damage. If state involvement can be identified in greater detail, the police collaborate with relevant agencies to conduct public attribution. When the investigation found that the cyber incident involves financial crimes committed by individuals or criminal organizations, the police will proceed with the arrest of suspects and work to resolve the case through international joint investigations.

In this way, the cyber police play a vital role in matters of national security related to cyberspace, such as responding to state-sponsored cyberattacks.

【Figure 34 : Image of Police Response against Cyberattacks】



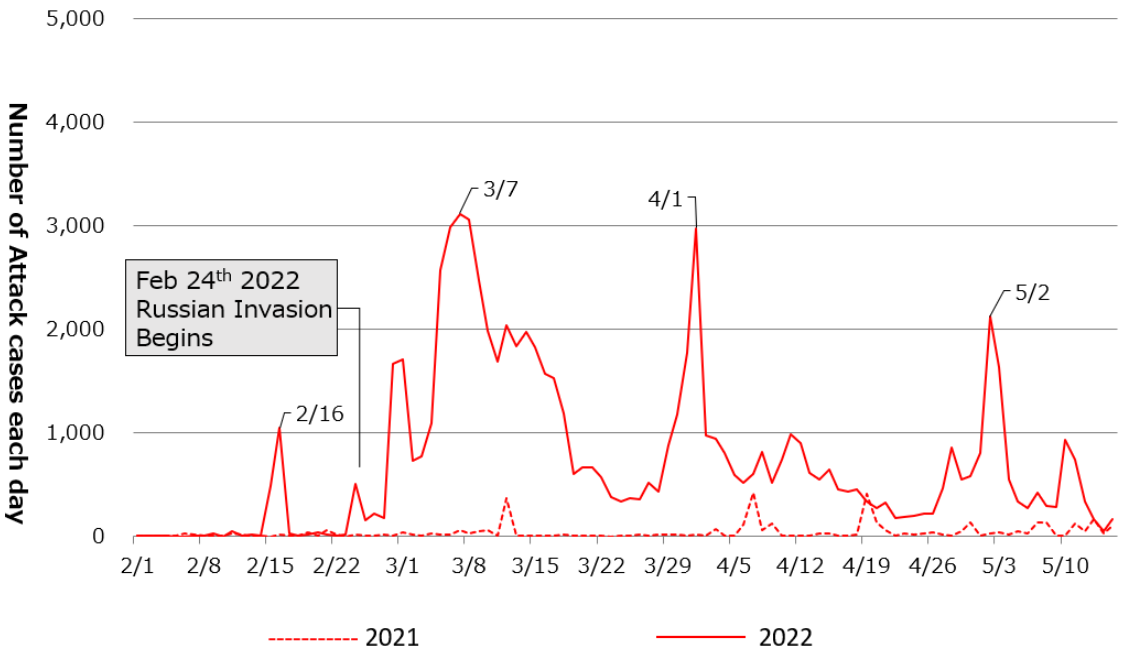
Column: Observations of Large-Scale DoS Attacks on Ukraine Against Ukraine

The following graph shows the status of DoS attacks on Ukraine observed by sensors installed by NPA between February and May of 2021 and 2022, respectively.

While in 2021, there were very few DoS attacks, in 2022, large-scale DoS attacks against Ukraine were observed on February 16—just before the Russian military launched its invasion of Ukraine—and after February 24, when the invasion began; this indicates a temporal and geographical correlation between the invasion of Ukraine and the occurrence of cyberattacks.

In fact, in May 2022, EU, Ukraine, and some countries issued statements condemning the Russian government for launching a cyberattack on international satellite communications one hour before the invasion of Ukraine, which affected the entire European continent. Given that cyberattacks against government agencies and critical infrastructures are likely to occur in the preliminary stages of an armed attack against Japan, and that such attacks are expected to continue as part of a hybrid war—combining military and physical means—even after an armed attack has commenced, it is critically important for the police to maintain a thorough understanding of this cyberattack landscape for the sake of national security.

【Figure 35:Observation of DoS Attack on Ukraine】



2　Active Cyber Defense（ＡＣＤ）

In recent years, cyberattacks that steal information from governments and corporations have become a major problem, and concerns about sophisticated cyberattacks equipped with advanced intrusion and persistence capabilities aimed at disabling critical infrastructure functions are rapidly increasing. In particular, serious cyberattacks intended to shut down or destroy critical infrastructure are carried out on a daily basis, even with state-sponsored, posing a major security concern.

In this context, the National Security Strategy, approved by the Cabinet in December 2022, set a goal of "enhancing our response capabilities in the cyber-security domain to a level equal to or greater than those of major Western countries" and decided to introduce active cyber defense to prevent and contain damage from serious cyberattacks.

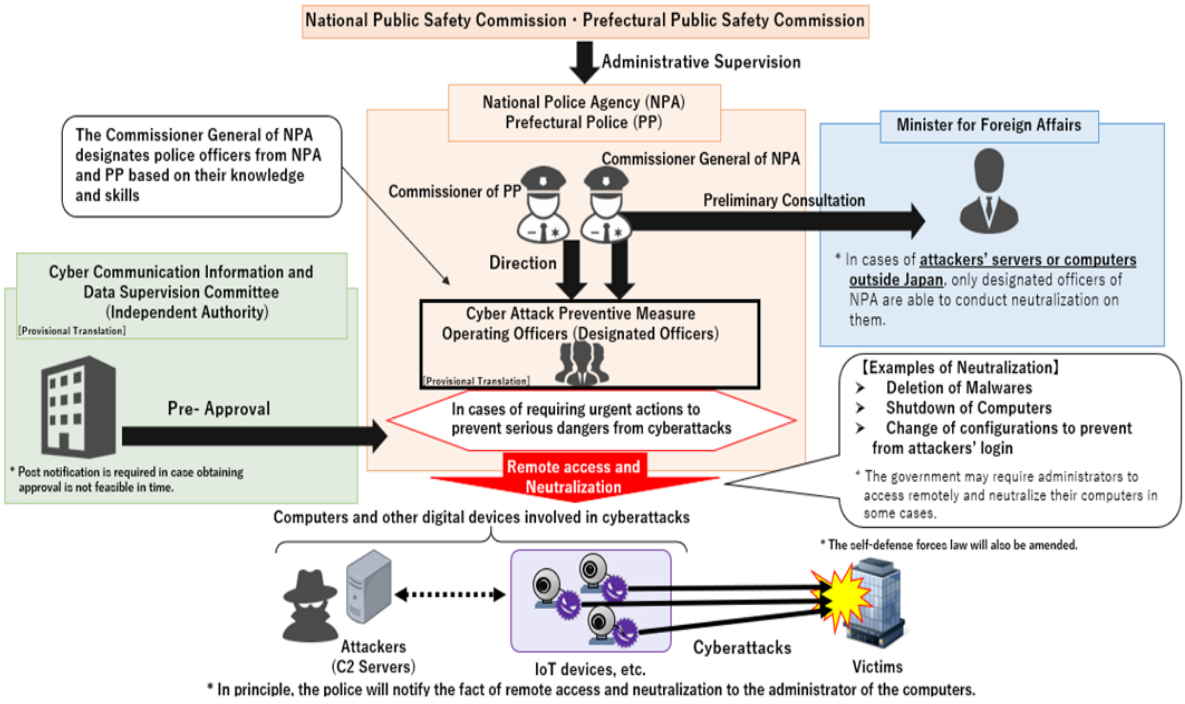
Based on the strategy, the government held an "Expert Conference on Enhancing Response Capabilities in the Cyber-Security Domain" in June 2024 to examine the legal framework and other measures needed to realize new initiatives in cyber security, and "Recommendations for Enhancing Response Capabilities in the Cyber-Security Domain" was compiled by the conference in November of the same year.

In May 2025, during the 217th Diet session, the Cyber Response Capability Strengthening Act (hereafter "Strengthening Act") and the Cyber Security Infrastructure Act (hereafter "Infrastructure Act"), reflecting the recommendations, were enacted. The Strengthening Act and the Infrastructure Act focus on three pillars: "strengthening public-private cooperation," "use of communications data," and "remote access and neutralization to attackers" servers and other assets."

In December 2025, the Cabinet approved the "Basic Policy for Preventing Damage Caused by Specific Illicit Acts Against Important Electronic Computers" which sets out fundamental matters to ensure that measures under the Strengthening Act function properly and that related administrative procedures are carried out appropriately.

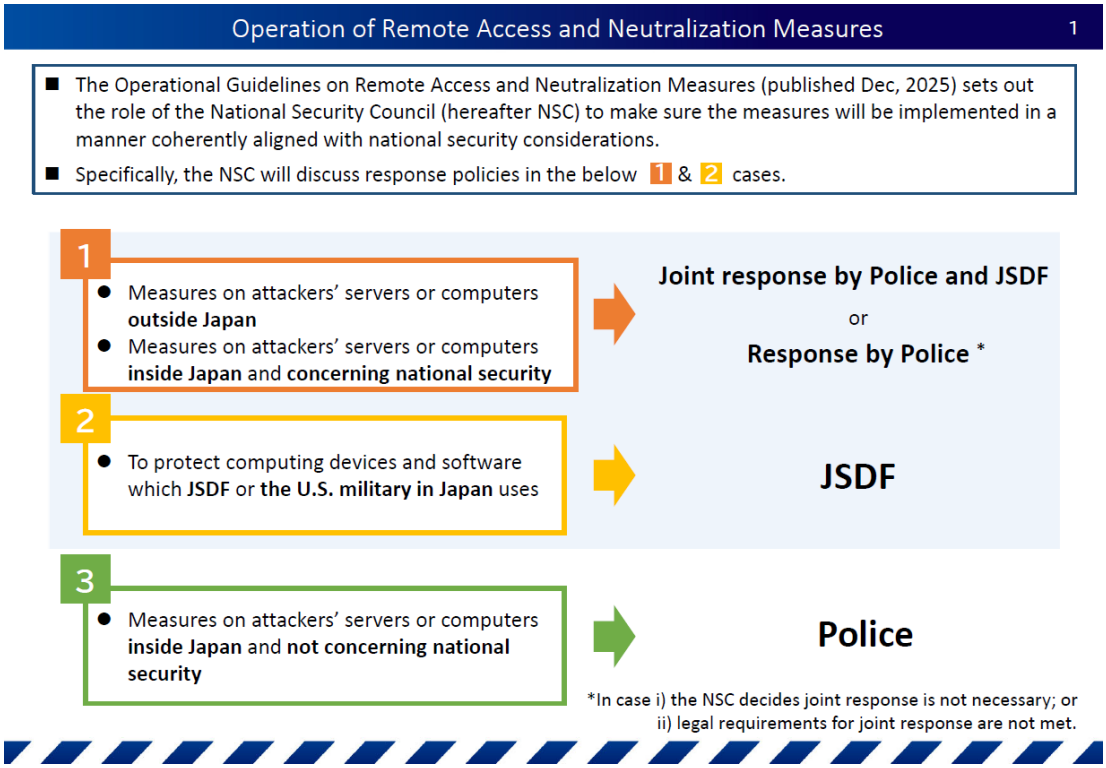
Regarding police matters, the Infrastructure Act amended part of the Police Duties Execution Act, creating a new provision that allows police to take "remote access and neutralization measures" to prevent serious harm from cyberattacks. This provision is scheduled to come into force on 1 October 2026. Accordingly, the police are strengthening coordination with the National Cybersecurity Office (NCO) of the Cabinet Secretariat, the Ministry of Defense and the Self-Defense Forces, the Ministry of Foreign Affairs, and other agencies, while taking into account the "Guidelines for the Operation of Remote Access and Neutralization Measures" decided by the National Security Council in December 2025. "Remote access and neutralization measures" will be carried out mainly by the Cyber Special Investigation Department, which will require high expertise and technology; therefore, further arrangements to provide technical support are considered necessary.

【Figure36: Overview of the Revised Police Officer Duty Execution Act】



【Figure 37 : Operation of Remote Access and Neutralization】

Topic II: Efforts Toward Breaking Anonymity in Cyberspace



【source : Cabinet Secretariat】

1 Crimes by Anonymous and Fluid Criminal Groups Abusing the Anonymity of Cyberspace

With the development of information and communications technology and the progress of digitalization in society, cyberspace is evolving into a public space where important socio-economic activities are conducted. While various socio-economic activities are significantly shifting to non-face-to-face and non-contact forms through cyberspace, immense damage is occurring due to cyberspace being abused for crimes such as organized fraud. For example, on SNS used by many citizens, anonymous and fluid criminal groups are recognized to be recruiting people to commit crimes, not clearly specifying the nature of the work, by using phrases such as "easy, simple, and high income," such as "high pay," " paid on the spot ," and " job with good conditions ." In addition, there is a reality that applicants to such recruitment are being guided by recruiters and instigators to use highly anonymous communication applications for contact. In this way, communication methods with high anonymity and mechanisms that automatically delete messages are being abused as a means of contact among masterminds, instigators, and perpetrators. Furthermore, while the transfer of funds in cyberspace is highly convenient, there is a reality that anonymous and fluid criminal groups abuse the anonymity of cyberspace to evade clearance by the police, such as by converting criminal proceeds into cryptoassets and transferring them to the accounts of overseas cryptoassets exchange service providers, thereby disguising and concealing the flow of funds.

2 Clearance of Anonymous and Fluid Criminal Groups

The National Cyber Department (NCD) tracks the transfer of cryptoassets abused for crimes, conducts cross-sectoral and comprehensive analysis of the tracking results, and shares the results with prefectural police. Through such analysis, the relevance among multiple cases, the underlying organizational structure, and higher-ranking suspects, which were not necessarily revealed through conventional criminal investigations, have been brought to light.

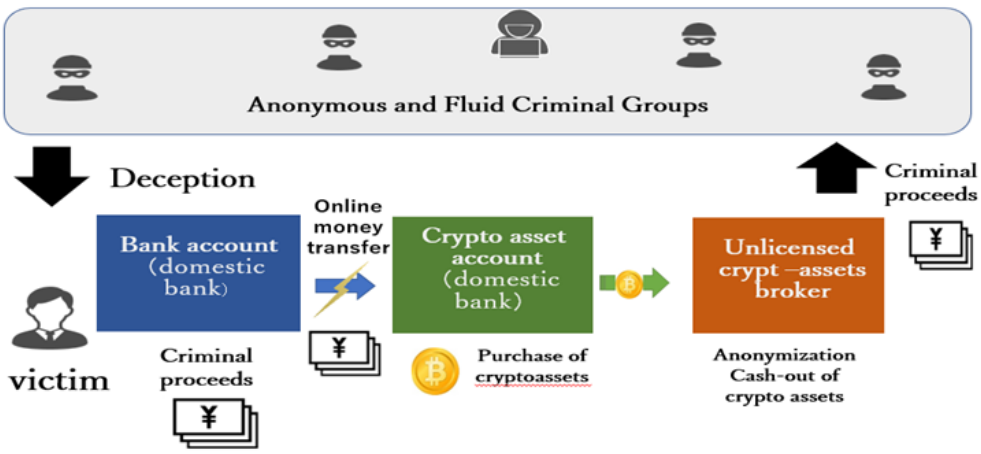
In addition, for the further clearance of anonymous and fluid criminal groups, in October 2025, upon strengthening the structure of NCD, it was decided that some staff members of the division would also serve as analysis personnel in the Anonymous and Fluid Criminal Groups Intelligence Analysis of NPA. The police are further strengthening their efforts so that multifaceted analysis conducted by such staff members, including other information possessed by the office, will lead to breaking the anonymity of cyberspace and clearance of core figures.

Column : Clearance of “Tool provider” and ”Unlicensed cryptoassets broker” Abusing the Anonymity of Cyberspace

Among anonymous and fluid criminal groups, there are those who obtain funds through illegal businesses built under core figures, such as so-called "Tool provider" and “Unlicensed cryptoassets broker”. The police are dismantling the criminal infrastructure by clearance of these criminal groups.

For example, regarding " Tool provider," as a result of cyber patrols, it was confirmed that a criminal group was involved in recruiting sellers of financial institution accounts, etc., and their brokers, illicitly procuring financial institution accounts and cryptoassets accounts to serve as criminal infrastructure using highly anonymous SNS, and then selling them to multiple communications fraud groups. A joint criminal investigation headquarters comprising relevant prefectural police, such as the Aichi Prefectural Police, and the National Cyber Department （NCD） conducted a criminal investigation. In the NCD, because of aggregating information provided by the prefectural police and JC3, conducting cross-sectoral and comprehensive analysis, and tracking concealed cryptoassets using highly specialized knowledge and skills, they identified the ringleader of the criminal group, a man (32), and his accomplices. In October 2025, they arrested seven individuals, including the man, for fraud and violating the Act on Prevention of Transfer of Criminal Proceeds.

In addition, regarding " Unlicensed cryptoassets broker," as a result of a joint criminal investigation by the Hiroshima Prefectural Police and the NCD, it was revealed that two men had cashed out and concealed cryptoassets, including criminal proceeds defrauded from victims of communications fraud cases. Furthermore, it was found that one of them had continuously exchanged cryptoassets for cash regarding criminal proceeds other than the defrauded money from this fraud case. Consequently, in November 2025, the two men were arrested for violating the Act on Punishment of Organized Crimes and Control of Crime Proceeds, etc. In this case, while a "mixing service" to enhance anonymity was used to transfer the cryptoassets, which were the defrauded money from the communication fraud, the advanced analysis by the NCD identified that the defrauded money was flowing into an account under the suspect's name, leading to the full elucidation of the entire structure of the case. In this way, there is a recognized reality that the anonymity of cyberspace is being abused for money laundering, such as making the tracking of cryptoassets difficult by routing them through Unlicensed cryptoassets broker.



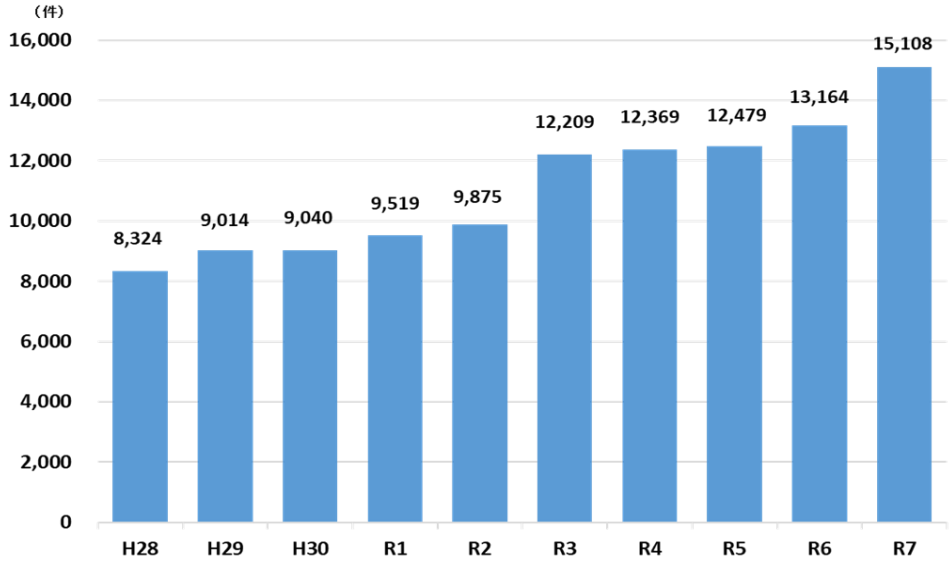
CHAPTER 2　Police Efforts

1　Efforts Toward Clearance

In response to the threats described in Part 1, the police are promoting initiatives for clearance; the National Cyber Department (NCD) handles serious cyber incidents, while prefectural cyber departments address cyber incidents requiring advanced expertise and technology. Furthermore, recognizing that cyberspace is exploited in all types of crime, the police maintain technical support systems to enable non-cyber investigation departments to address cyber incidents and cybercrimes.

Consequently, cybercrime clearance reached 15,108 in 2025. Among these, clearance under the Act on Prevention of Transfer of Criminal Proceeds totaled 2,868, including 1,012 cases also classified as cyber incidents for utilizing highly anonymous communication; both figures increased from the previous year.

【Figure38：Number of Cleared Cases of Cybercrime】



(1)　Clearance

①　The National Cyber Department (NCD)

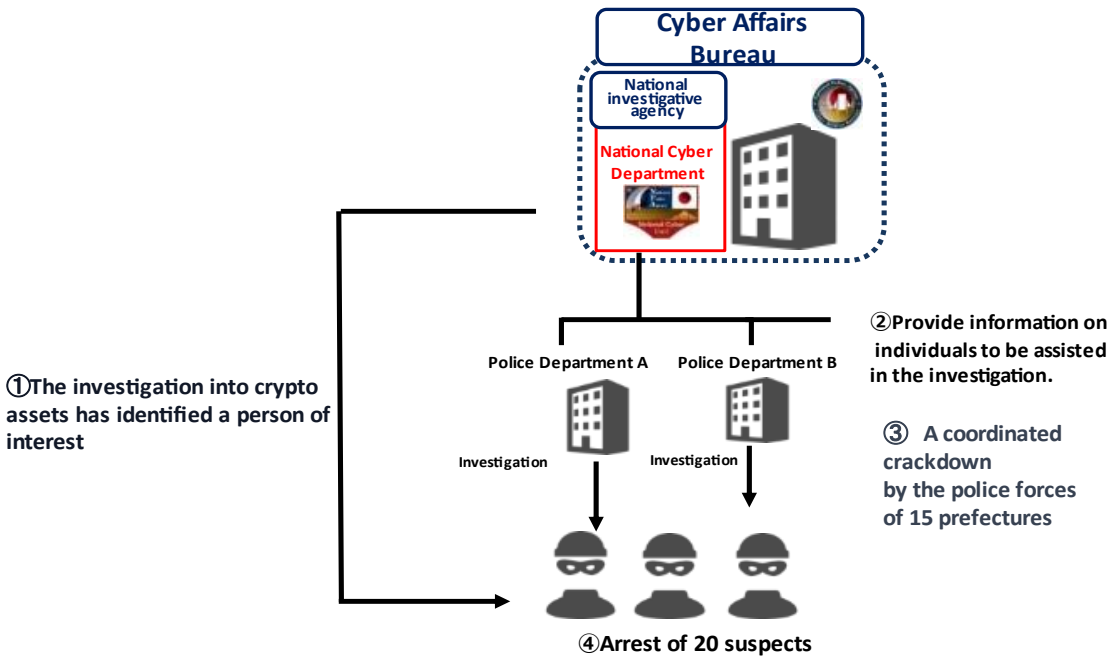
NCD plays a role as a hub for police nationwide through its advanced information aggregation and analysis functions. At the same time, leveraging the information thus obtained and its strong relationships of trust with foreign law enforcement agencies, etc., it tackles cyber cases committed across borders through international joint investigations, etc., acting as a so-called connecting node between the world and Japan.

【CASE：Intensive Crackdown Using cryptoassets Tracking Technology】

NCD recognized the reality that credit card information illegally obtained through phishing, etc., was being bought and sold via highly anonymous communication applications, etc., and that cryptoassets were being used for the payment. Consequently, the division analyzed information on crimes related to the illicit use of credit card information nationwide and investigated the flow of cryptoassets recognized as the payment for the credit card information. As a result, investigation targets were identified across the country.

Between September 2024 and March 2025, NCD and 15 prefectural police conducted an intensive crackdown in close cooperation, clearing 20 male and female suspects ranging in age from their teens to their 50s for the illicit purchase and illicit use of other people's credit card information.

【Figure 39：Image of Intensive Crackdown Using Cryptoassets Tracking Technology】



② Cyber Departments of Prefectural Police

The cyber departments of the prefectural police promote criminal investigations into those requiring highly specialized knowledge and skills.

Column: Arrest of a Juvenile Group in Cases of Illicit Acquisition of eSIM

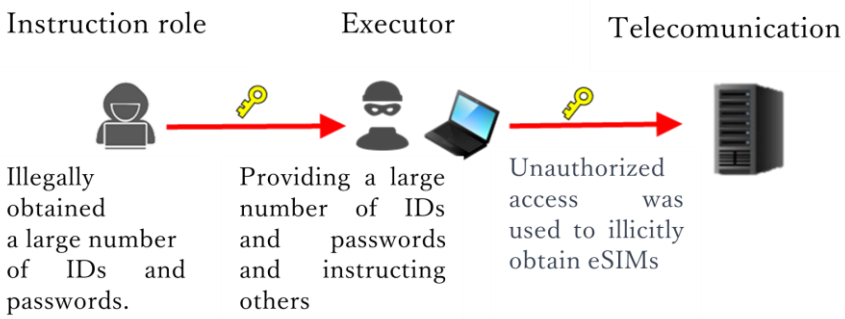
Three juvenile boys in junior and senior high school (aged 14 to 16) who connected through SNS intended to gain profit by selling illegally obtained eSIMs. Between May and August 2024, they each illegally accessed a server computer managed by a telecommunications carrier using the illegally obtained IDs and passwords of others, created false electromagnetic records pertaining to telecommunications contracts, and illegally obtained eSIMs. From January to February 2025, the Tokyo Metropolitan Police Department arrested the juveniles for violation of the Act on Prohibition of Unauthorized Computer Access, computer fraud, etc.

In this case, the fact that the carrier conducted simplified identity verification using only an ID and password when making additional contracts for a second or subsequent line was abused. It was also revealed that generative AI was abused.

Furthermore, intending to gain profit by selling illegally obtained eSIMs by imitating the modus operandi, two juveniles—an unemployed juvenile (16) and a high school student (16)—illegally obtained eSIMs using the imitated modus operandi. In response, in March and August 2025, the Tokyo Metropolitan Police Department and the Kanagawa Prefectural Police arrested the two juveniles for violating Act on Prohibition of Unauthorized Computer Access and computer fraud.

Under the Act on Prevention of Improper Use of Mobile Phones, identity verification at the time of contract is not mandatory for data-only SIMs, including eSIMs, and such cases of malicious use are endless. Therefore, NPA is providing information to the Ministry of Internal Affairs and Communications regarding the reality that data-only SIMs are being abused for crimes such as fraud. In addition, the government has included "Mandatory identity verification at the time of contracting data-only SIMs" as an effort to prevent the illicit use of various services and infrastructure in the "Comprehensive Measures to Protect the Public from Fraud 2.0" (decided by the Ministerial Meeting Concerning Measures Against Crime on April 22, 2025). Based on these facts, the government is considering revising the Act on Prevention of Improper Use of Mobile Phones, which includes making identity verification stricter at the time of contracting data-only SIMs.

【Overview of the eSIM Unauthorized‐Acquisition】



【CASE：Illegal Gambling Case Using Online Casinos by Juveniles】

As a result of a crackdown triggered by cyber patrols regarding online casinos, in October 2025, the Tokyo Metropolitan Police Department arrested a male university student (19) for habitual gambling, violating the Payment Services Act for converting electronic money into cryptoassets for online casino users without registration between May 2024 and May 2025. In this case, a total of 19 individuals were cleared or referred to a child guidance center for habitual gambling, including a junior high school boy (13).

(2) Investigative Support

Regarding cyber cases and cybercrimes, for those that do not require highly specialized knowledge and skills for criminal investigations, departments other than the cyber departments take charge of the cases and proactively conduct the criminal investigations, with the cyber departments providing appropriate support to the said departments.

【CASE ： Illegally Taking Out Customer Information】

To advance her job change, a female part-time employee (45) duplicated and acquired the customer information, which is a trade secret, of a nursing care facility located in Aomori Prefecture where she was working at the time, between February and March 2024. In January 2025, she was arrested for violating the Unfair Competition Prevention Act (acquisition of trade secrets). In this case, upon receiving a request for support from the security department of the prefectural police, the cyber department provided support such as the analysis and data scrutiny of electronic devices, including computers, installed at the nursing care facility to which she had transferred, thereby corroborating her crime. (Aomori)

【CASE ： Organized Habitual Gambling via an Online Casino】

A criminal group centered around a male company executive (42) conducted organized habitual gambling with an unspecified number of gamblers between April and May 2024 by continuously performing duties such as managing a payment system for depositing bets on overseas online casino sites and managing funds using the system. In June 2025, nine individuals, including the man, were arrested for violating the Act on Punishment of Organized Crimes and Control of Crime Proceeds (organized habitual gambling). In this case, upon receiving a request for support from the organized crime control department of the Kanagawa Prefectural Police, the cyber department provided support such as the identification of a domestic rental server where the deposit management system was stored, as well as server verification and analysis, thereby corroborating their crimes. (Kanagawa)

【CASE：Concealing the Proceeds of communications Fraud】

A male company executive (52) and his accomplices received a request from a communications fraud group in October 2023, and concealed criminal proceeds that the group had obtained through communications fraud, etc., by remitting them through multiple bank accounts to domestic cryptoassets accounts to acquire cryptoassets, and then transferring a portion of the acquired cryptoassets to coin addresses linked to accounts opened at overseas cryptoassets exchanges. In September 2025, four individuals, including the man, were arrested for violating the Act on Punishment of Organized Crimes and Control of Crime Proceeds.

In this case, upon receiving a request for support from the organized crime control department of the Fukui Prefectural Police, the cyber department supported the tracking of the defrauded money exchanged for cryptoassets, thereby corroborating their crimes. (Fukui)

Furthermore, NPA and the Digital Analysis Sections established within the nationwide Info-Communications Department of Regional Police Bureaus provide technical assistance to prefectural police and other police organizations. Their support includes:

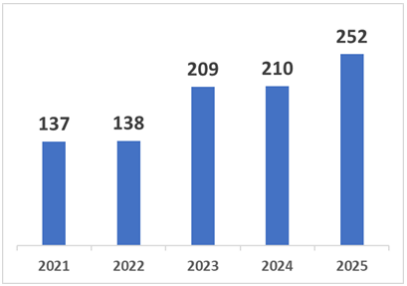
・Technical guidance for the proper seizure of computers and other electronic devices at search and seizure sites.

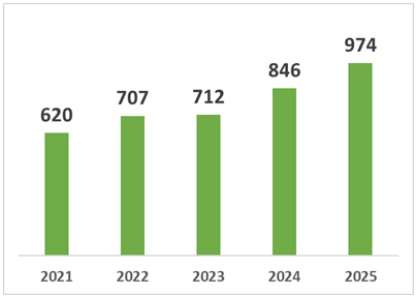
・Forensic extraction of evidential data from confiscated smartphones and similar devices.

・Analysis of malicious program and other digital artifacts

In addition, Digital Forensic Center established within the Digital Analysis Division of NPA, employs personnel with highly specialized knowledge and skills and installs high-performance analytical equipment. This center conducts complex examinations—such as extraction and visualization of data from damaged electronic media—that are beyond the capabilities of the regional Digital Analysis Sections.

【Figure 40: Number of analyzed and consulted at Digital Forensic Center】





【Case: Data Extraction from a Burnt Smartphone】

In December 2024, the Digital Forensic Center of the NPA succeeded in extracting data from a smartphone found at a fatal fire scene in Hiroshima Prefecture. Because the device was severely burnt, conventional forensic methods could not be applied. By removing the memory chip mounted on the circuit board and employing exceptionally advanced and sophisticated techniques, the center was able to recover the data, thereby contributing to a full elucidation of the incident.

【CASE：Data Extraction from Damaged Electronic Media】

From May to June 2025, the Digital Forensic Center of NPA handled a sexual-offense case involving a minor committed by an unemployed 36-year-old male. The USB flash drive and hard-disk drive seized from the suspect were so severely damaged that they could not be read by ordinary forensic techniques. By restoring the functionality of the devices, the Center was able to make the data extractable. As a result, electronic records retrieved from the USB flash drive and hard disk provided evidence of the offender's motive and other related offences, thereby contributing significantly to a full elucidation of the case.

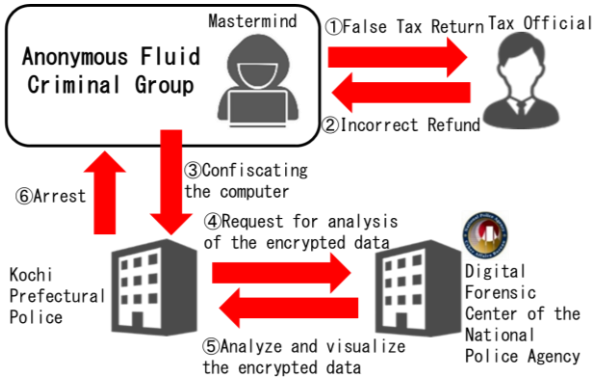
In addition, the police track the transfer of cryptoassets used for such crimes, and NCD conducts cross-sectoral and comprehensive analysis of the tracking results and shares the findings with the prefectural police. Through these efforts, for example, regarding investment/romance fraud via social media cases that occurred in Japan, as a result of cross-sectoral analyzing the investigative information of the relevant prefectural police and conducting cryptoassets tracking, the police ascertained the fact that the defrauded money from multiple cases was being remitted to cryptoassets accounts under Nigerian names. Upon providing this information to the Nigerian police, suspects within Nigeria were cleared by the Nigerian police. As seen in this example, the relevance among multiple cases and the underlying organizational structure, which were not necessarily revealed through conventional criminal investigations, are being brought to light.

Column: Strengthening Equipment and Materials to Enhance Analytical Capability

The Digital Forensic Center of the NPA is equipped with sophisticated analytical hardware—such as high-speed computing systems and analysis platform devices—and provides technical support for the advanced analysis of data hidden by encryption, damaged electronic equipment, and other complex cases.

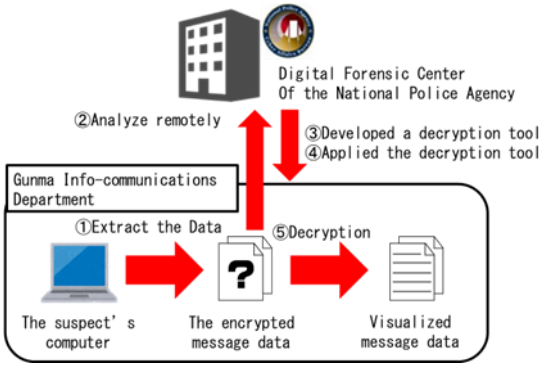
○Example of Case in which Extracting Encrypted Data Led to Arrests

A man in his 40s who works in the design industry, together with others, filed false income-tax returns from April 2024 through March 2025, deceiving tax-office officials and causing a refund surcharge to be transferred into an account. At first the man denied having committed the crime, and the data on the seized computer was encrypted. However, after NPA's Digital Forensic Center examined the data, electronic records relating to the false tax filings as well as electronic records concerning persons involved in the offense were discovered on the computer. Using these analysis results, the prefectural police determined that the case was the work of an anonymous and fluid criminal group that was directed by the man. By May 2025, the police had arrested ten people, including the man, on charges fraud and other offences.



○Example of Case in which Encrypted Data was Decrypted through Remote Assistance

In December 2025, regarding a case of forgery of sealed public documents carried out by a Vietnamese man in his 50s and his associates, NPA's Digital Forensic Center leveraged its analysis-platform equipment to remotely examine the encrypted data from the messaging app the suspect had been using and created a tool to decrypt it. When the Digital Analysis Section of Gunma Info-communications Department applied this tool, it was able to extract records that corroborated the disposition of the criminal proceeds, thereby contributing to the elucidation of the case.



(3) International Cooperation

Since many cybercrimes are committed across national borders, international cooperation is essential to address them. Police are actively working to establish multilateral cooperative relationships to share information on threats in cyberspace, strengthen cooperation on international mutual legal assistance in criminal investigations, and share knowledge and experience in information technology analysis. In 2025, the Cyber Affairs Bureau of NPA participated in international conferences such as the G7 High-Tech Crime Subgroup, the Committee of the Convention on Cybercrime, and the European Police Chiefs Convention hosted by EUROPOL. Through these meetings, NPA and counterparts shared countermeasures against cybercrimes and strengthened international information sharing. Since discussions between senior officials at international conferences are crucial for strengthening international cooperation, it will be more important for senior staff to proactively attend such conferences.

In addition, the police dispatched Japanese police personnel to training provided by the ICPO for law enforcement personnel of various countries concerning countermeasures against cybercrimes, etc. Furthermore, they are also promoting the strengthening of cooperation regarding international investigative collaboration, such as by inviting investigators, etc., of foreign law enforcement agencies, etc., to Japan to exchange investigative information, etc., related to international joint investigations.

Additionally, since 2016, the Japanese police have participated in the ICPO Digital Forensics Experts Group, which brings together law enforcement agencies of ICPO member countries as well as private-sector entities and academic institutions overseas to promote the sharing of expertise and experience in digital forensics. The Japanese police have also been a member of FIRST, an international framework of organizations responding to information security incidents, since 2005, and collect technical information useful for appropriate incident response through information sharing among member organizations.

Furthermore, NPA provides support to foreign law enforcement agencies in collaboration with the Ministry of Foreign Affairs and the Japan International Cooperation Agency (JICA), with the aim of enhancing other countries' capabilities to deal with threats in cyberspace and strengthening cooperative relationships with foreign law enforcement agencies. Since fiscal year 2014, NPA has conducted training programs that invite personnel from foreign law enforcement agencies and share the knowledge and skills necessary to combat threats in cyberspace.

Column: International Joint Investigation with India into Support Fraud

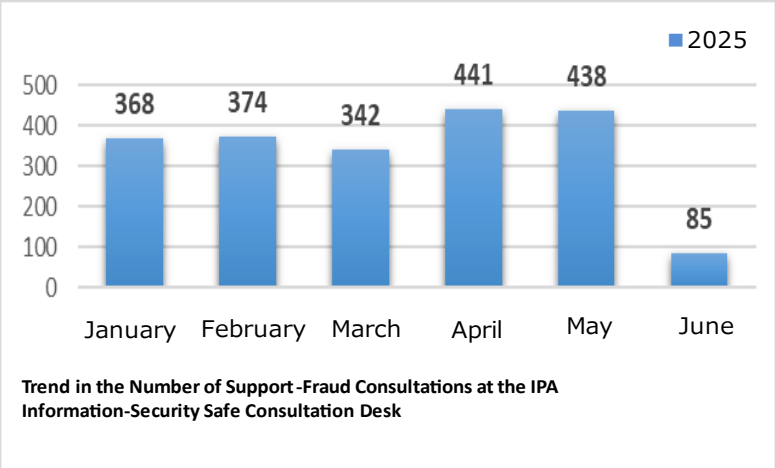
The Japanese police, in collaboration with the Central Bureau of Investigation (CBI) of the Republic of India, conducted international joint investigations into support fraud cases targeting Japanese people. As a result, in May 2025, the CBI arrested six Indian suspects located in the Republic of India.

In this case, the suspect group abused generative AI to identify targets, create pop-up windows, and translate text into Japanese, making it a case where AI was used in the commission of the crime. However, the arrest of the suspects was achieved through close cooperation between the Japanese police and the CBI, in addition to cooperation based on the unique initiatives of JC3 and Microsoft Corporation, serving as a new leading case for international public-private partnership.

Furthermore, the number of consultations regarding "fake virus detection alerts" received by the Information-technology Promotion Agency, Japan (IPA) in June 2025, following the clearance in this case, was 85, representing a significant decrease.

In January 2026, the Director of the Cybercrime Investigation Division of the Cyber Affairs Bureau, the NPA visited the CBI, presented a letter of appreciation for the investigative collaboration to the Additional Director (in charge of cyber) of the CBI and confirmed the further strengthening of international cooperation in the future.

【Figure 41: Trend in the Number of Reported Support-Fraud Cases】



Trend in the Number of Support-Fraud Consultations at the IPA Information-Security Safe Consultation Desk

【CASE：International Joint Investigation against Online Child Pornography 】

From February to March 2025, as part of efforts to strengthen international cooperation, the police (Community Safety Division) conducted joint international investigations into online child pornography offenses in six countries and regions (Japan, Singapore, South Korea, Hong Kong, Thailand, and Malaysia), resulting in the arrest of a total of 544 suspects.

【Scene of Arresting Criminal】

2 Efforts to prevent damage and mitigate its impact

To ensure safety in cyberspace, the police are not only working to apprehend those involved in cybercrimes but are also promoting efforts to investigate the nature of attackers and their methods, as well as measures to prevent crimes before they occur and limit their impact.

(1) Information dissemination

Based on information obtained through investigations and analysis, the police are engaged in public relations and awareness-raising efforts, such as issuing warnings to prevent new crimes and raising public awareness of criminal methods to prevent further victimization.

① Information dissemination through international cooperation

In dealing with state sponsored cyberattacks and other sophisticated attacks that exploit advanced technology, the police not only advance investigations to apprehend attackers but also analyze compromised computers and other assets to uncover the reality of the attackers and their methods, and issue alerts concerning preventive measures. For example, in January 2025, NPA and NISC confirmed that a cyberattack group called “MirrorFace” had been conducting information theft attacks against Japanese organizations, businesses, and individuals since around 2019. They assessed these attacks as organized cyberattack activity likely involving China and issued alerts about the group’s tactics and preventive measures.

In addition, Japan conducts public attribution—publicly naming and condemning attackers—to deter cyberattacks. For instance, in August 2025 a public attribution was made concerning the China backed cyberattack group “Salt Typhoon.”

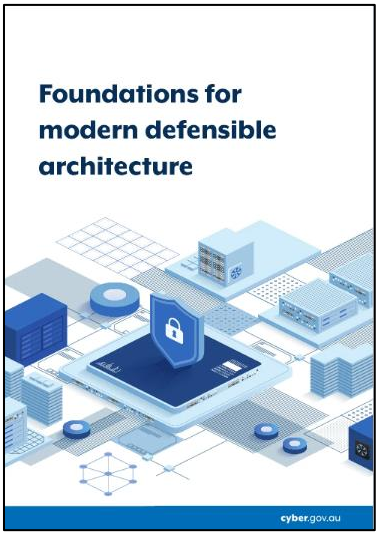
Column: Public Attribution on China-sponsored Group Salt Typhoon

In August 2025, NPA and the National Cybersecurity Office (NCO) joined counterpart agencies from the United States, Australia, Canada, New Zealand, the United Kingdom, the Czech Republic, Finland, Germany, Italy, the Netherlands, Poland, and Spain in co-signing the international advisory titled "Countering Chinese State-Sponsored Actors: Compromise of Networks Worldwide to Feed Global Espionage System," which addresses cyberattacks by the China-backed group known as "Salt Typhoon." The advisory was released as a public attribution.

The police are leveraging the Council for Countermeasures against Cyber Terrorism and the Counter Cyber Intelligence Network to inform businesses about Salt Typhoon's tactics, breach information, and mitigation measures, and to issue warnings.

Column: Joint Signature on an Australia-led International Document

In October 2025, NPA and NCO joined the joint signing of the document "Foundations for modern defensible architecture," which was developed by the Australian Signals Directorate (ASD)'s Australian Cyber Security Centre (ACSC), together with the relevant agencies of Australia, Germany, Canada, New Zealand, Republic of Korea, and the Czech Republic. The document provides engineers who design information systems with approaches useful for building systems that address cyber-space threats.



② Information dissemination through collaboration with related organizations

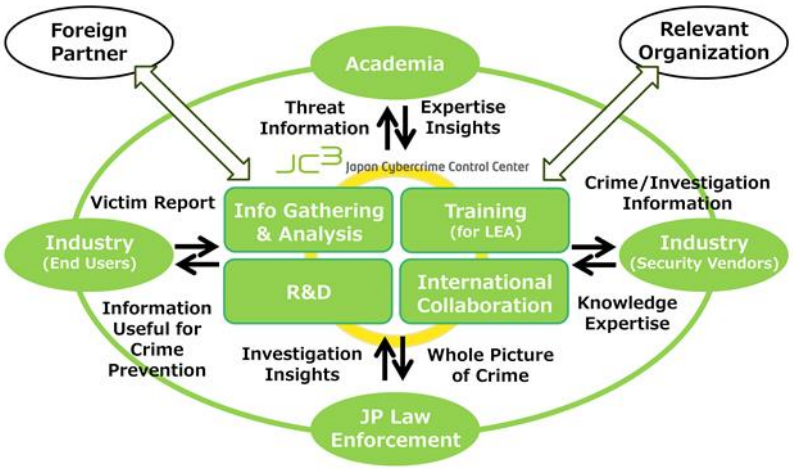
The police are disseminating information in cooperation with various related organizations and are particularly promoting collaboration with the JC3.

JC3 was established in response to the need to create a new organization similar to the NCFTA, a non-profit organization that has achieved success as a framework for industry-academia-government collaboration in the United States, as pointed out in the "Strategy for Creating the World's Safest Japan," which was approved by the Cabinet in December 2013. JC3 aims to contribute to creating an environment in which citizens can use the internet safely and with peace of mind by aggregating and analyzing information and knowledge from industry, academia, and government, and returning the results to the public, and commenced operations in November 2014.

The police share information with JC3 regarding the extent of cybercrime damage and modus operandi, which is then used to inform the countermeasures of member companies such as security vendors and financial institutions. In return, JC3 shares information about the damage situation and the implementation status of countermeasures at member companies, which the police utilize in their investigations and crime prevention activities.

JC3 has confirmed cases where users are tricked into installing fraudulent smartphone apps, resulting in many unsolicited SMS messages being sent from their personal smartphones and incurring high charges. Therefore, JC3 recognizes the existence of such malicious SMS messages and is issuing a warning about the dangers of easily accessing URL links or installing apps. Furthermore, they have recently confirmed instances where it appears that AI generation software is being misused to create fake SMS messages, and they have issued warnings about the increasing sophistication of attack methods.

【Figure 42 : Overview of the JC3】



Furthermore, each prefectural police department has concluded agreements with financial institutions, cryptocurrency exchange operators, medical institutions, chambers of commerce, and non-life insurance companies that handle cyber insurance, and is working to strengthen cooperation, such as information sharing, on a regular basis.

Furthermore, NPA is working to prevent ransomware and other cyber incidents and to mitigate the spread of damage, broadly raising awareness and acting on measures to address vulnerabilities in VPN equipment, propering management of credentials, propering acquisition of backups and logs, development of BCPs that anticipate cyberattacks, and prompting reporting and consultation with the police in the event of an incident. This is being done primarily with small and medium-sized enterprises, which are experiencing an increasing trend in such incidents.

In addition, we conducted outreach activities to industry associations and businesses in cooperation with relevant ministries and agencies, held seminars for small and medium-sized enterprises in collaboration with NISC during Cybersecurity Month 2025, and produced public awareness articles and videos in cooperation with the Cabinet Office's Public Relations Office and non-life insurance companies. (For information on public awareness videos introducing ransomware countermeasures, please refer to Special Feature II.)

Moreover, a “Council for Countermeasures against Cyber Terrorism” composed of prefectural police and critical infrastructure operators has been established in every prefecture, and joint response drills based on lessons from cyberattack incidents are being conducted. Through the Counter Cyber Intelligence Network (CCI Network), which includes the police and approximately 8,800 businesses nationwide, various information on cyberattacks suspected of aiming at data theft is aggregated, and alerts are issued to the participating organizations.

In January of 2025, in preparation for the Osaka-Kansai Expo, the Osaka Prefectural Police and Expo-related businesses jointly conducted an incident-response exercise simulating a real cyberattack (hosted by NPA). Participants acted as members of a fictitious company’s security response team, carrying out hands-on exercises using actual equipment, as well as customer communication and reporting the incident to the police. In addition, NPA performed security assessments at the request of the Expo-related organizations and other critical infrastructure operators nationwide, and issued alerts based on the findings. These efforts proved effective: the Osaka-Kansai Expo, which was held from April to October 2025, concluded successfully without any serious cyberattacks that disrupted its operation.

Column: JC3's Podcast on Countermeasures against Ransomware

In December 2025, JC3 launched the "JC3 Podcast: Ransomware Dialogue," a series aimed at improving the cybersecurity literacy of potential future ransomware victims through dialogue with experts such as lawyers, private-sector security engineers, cybercrime investigators, and prosecutors, and is promoting the prevention of such incidents.

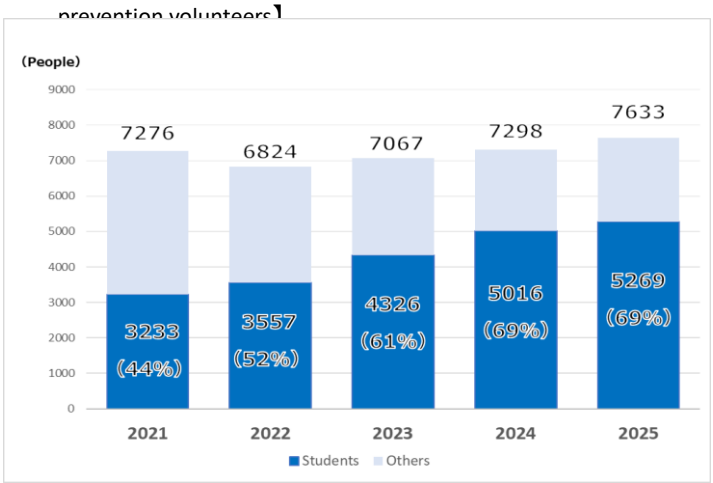
※ The content includes personal opinions and may differ from the official views of the performers' organizations or JC3

③ Information dissemination through collaboration with cybercrime prevention volunteer

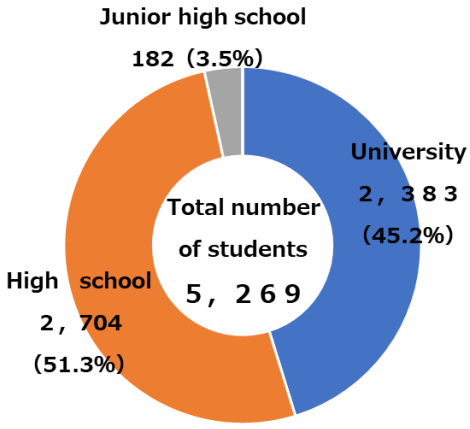
Cybercrime prevention volunteers are voluntary crime prevention activities aimed at creating a safe and secure internet space, based on the concept of "protecting the safety of the internet we use ourselves." As of the end of December 2025, there are 332 organizations and 7,633 individuals nationwide who are engaged in activities centered on "educational activities to prevent damage," "public awareness activities," and "cyber patrol activities." The police are providing support to expand and revitalize these activities.

The proportion of students among cybercrime prevention volunteers is increasing, indicating a growing trend of crime prevention activities led by younger generations.

【Figure43 : Trends in the number of cybercrime prevention volunteers】



【Figure44 : Breakdown of cybercrime prevention volunteers by student】



Column : Kanazawa Institute of Technology Cybercrime Prevention Volunteers Activities

At Kanazawa Institute of Technology (Ishikawa Prefecture), the "Information Security Skill-Up Project," a platform for students to share various knowledge, including security, also involves engaging in local cybercrime prevention activities. The specific activities include:

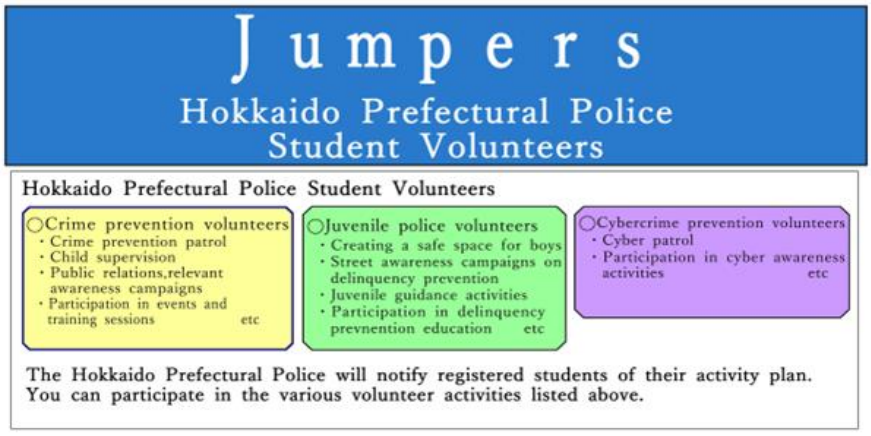
- Holding security classes for elementary and junior high school students.
- Production of public awareness videos to prevent harm
- Development and operation of a cybersecurity learning game website for elementary, middle, and high school students and their parents.

In November 2025, in recognition of their achievements in crime prevention activities, they were awarded the "Award for Meritorious Service in Creating a Safe and Secure Community" by the Prime Minister.

Column: Support for the expansion and revitalization of cybercrime prevention volunteers

The Hokkaido Prefectural Police have established and are operating a new student volunteer organization called "Jumpers," which integrates various volunteer activities, with the aim of creating an environment where students can easily participate in various volunteer activities by unifying the procedures for participation and registration of multiple volunteer activities. By registering with "Jumpers," users can participate in their preferred volunteer activities from a variety of options, thus contributing to the promotion of active participation in volunteer work.

Furthermore, the Hokkaido Prefectural Police and the Hiroshima Prefectural Police are implementing measures to expand and revitalize cybercrime prevention volunteers, such as giving extra points to applicants with a certain level of volunteer experience in some police officer recruitment exams.



NPA provides support by conducting inspections of activities, holding exchanges of opinions with cybercrime prevention volunteers nationwide, and hosting a contest for public awareness videos on cyber incidents, awarding prizes to organizations that create outstanding works.

Police departments in each prefecture are also working to support cybercrime prevention volunteers by providing training and offering advice on crime prevention to those volunteers, such as providing advice on creating quizzes to be used in crime prevention education at schools and other institutions, as well as in public awareness campaigns at large-scale events.

(2) Measures against Crime-Infrastructures

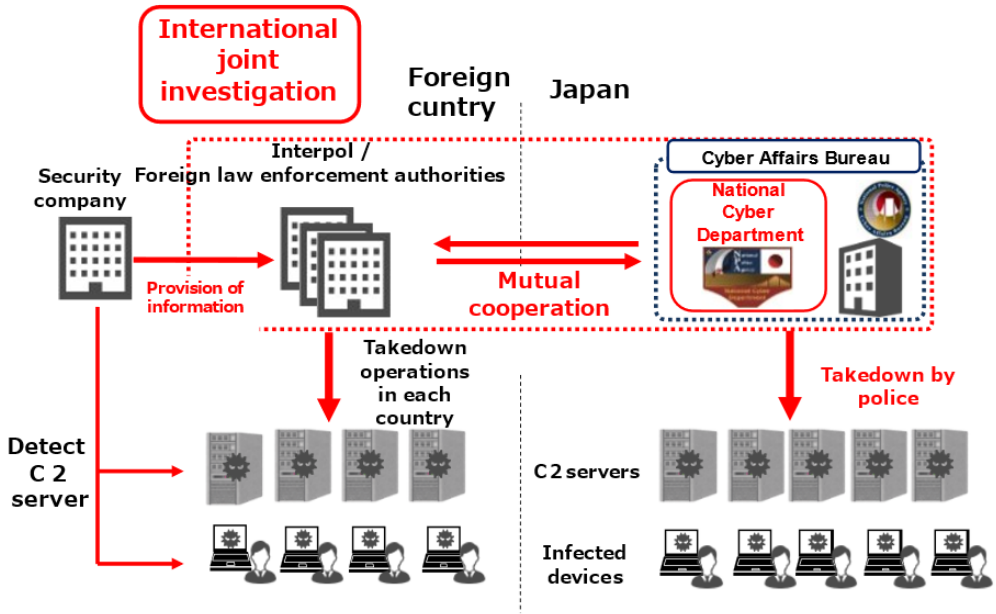
To prevent damage caused by cyber incidents, it is necessary to address the criminal infrastructure. In doing so, it is important to implement measures across society including not only police efforts but also private companies, academic institutions, and relevant government agencies. Since some new services and technologies have been exploited by attackers taking advantage of their vulnerabilities, effective countermeasures are being implemented through collaboration among industry, academia, and government to prevent such exploitation.

① Countering Infrastructure Used in Cyberattacks misusing Advanced Technologies

The police identify domestic servers functioning as command-and-control (C2) servers by analyzing malicious programs used in cyberattack cases, and they continuously take measures against these C2 servers, such as requesting the operators of the servers to disable the servers' illicit functions.

In June 2025, INTERPOL announced that, as part of the international joint investigation "Secure" aimed at countering the Infostealer malware that targets information in the Asia-South Pacific region, investigative agencies from 26 countries, including Japan, worked with private companies to pressure the administrators of relevant C2 servers, resulting in takedown actions that prevented further offenses and damage. Based on information supplied by INTERPOL, Japan's National Cyber Department and police forces from 18 prefectures coordinated closely and successively approached the operators of the compromised servers, leading the operators to takedown 129 C2 servers. These servers were ordinary corporate servers that had been compromised for undisclosed reasons and were being used for data-theft without the knowledge of the managing organizations.

【Figure 45 : International Joint Investigation with Interpol into Infostealer】



② Addressing crime-infrastructure related that exploit the internet

○ Measures against phishing sites

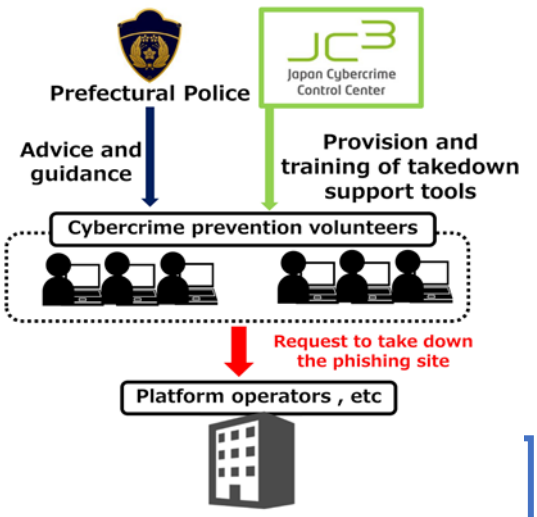
NPA collects URL information related to fake overseas websites that have been identified through consultations and other means by prefectural police forces and the JC3 and provides this information to antivirus software providers. These providers then take measures to prevent access to such websites, such as displaying warnings through the antivirus software's functions.

Furthermore, as a proactive measure based on the characteristics of phishing sites, such as the fact that hundreds of phishing sites are built on a single IP address, NPA is independently collecting domain information associated with the same IP address and discovering and providing information on previously unknown phishing sites.

In addition, in light of the increasing sophistication of phishing techniques and the sharp rise in victims, and in order to protect users, we have requested businesses, through the relevant ministries and agencies, to take measures to prevent access to phishing sites, including "promoting compliance with technologies to prevent spoofed emails (such as DMARC)," "promoting the closure of phishing sites," and "promoting the widespread adoption of authentication methods (passkeys) that allow for easy and secure login using biometric authentication instead of passwords."

As part of a public-private partnership to combat phishing sites, JC3 has developed a tool that allows even those without specialized knowledge to request platform operators to take down their sites. This tool is provided to cybercrime prevention volunteers, and JC3 is also holding the "Phishing Site Eradication Challenge Cup" for cybercrime prevention volunteers, with the support of NPA.

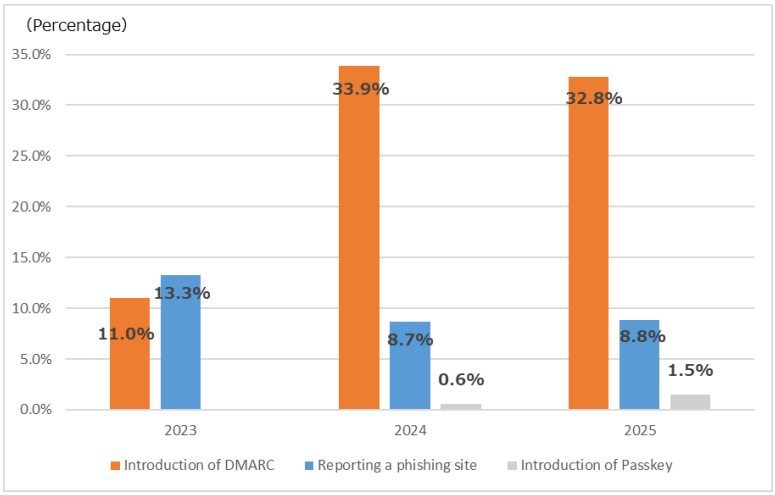
【Figure46：Phishing Site Eradication Challenge Cup】



Column: Survey Results on Measures Ag

NPA conducted a survey of randomly selected private companies and government agencies regarding measures against unauthorized access, and the results showed that the adoption rate of DMARC as a phishing countermeasure among private companies and other organizations increased significantly in 2024. Furthermore, compared to the past 10 years, the number of DDoS attacks and malware installations/infections suffered by private companies and other organizations in the past year have been halved, and the number of cyberattacks suffered has decreased significantly. In addition, approximately 55% of private companies and other organizations have developed response manuals and procedures, showing an increasing trend over the past 10 years.

【Figure47：private companies】



○ Countermeasures Against Online Banking Fraud

In response to the serious situation of a renewed surge in online banking fraud from corporate accounts via voice phishing since November 2025, NPA, in collaboration with the Financial Services Agency, the Japanese Bankers Association, and the Japan Cybercrime Control Center (JC3), created a public awareness document

titled "Cyber Police Agency Letter" and published it on the NPA website and other platforms to warn about the details of the methods used and countermeasures.

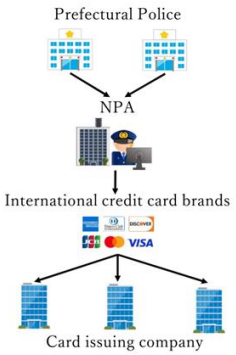
○ Measures against fraudulent trading in securities accounts

In light of the damage caused by fraudulent securities account transactions, NPA issued a warning in May 2025 regarding phishing attempts impersonating securities companies on websites and other platforms. Furthermore, in July of the same year, the agency, in conjunction with the Financial Services Agency, requested financial associations, including the Japan Securities Dealers Association, to strengthen measures against unauthorized access and transactions of customer accounts, outlining specific phishing methods and countermeasures based on the damages experienced.

○ Credit card fraud prevention measures

NPA promptly collects misused credit card numbers identified by prefectural police departments and provides them collectively to international brands that oversee the entire payment system, including card issuers. This information is used by credit card issuers to combat fraudulent use. In 2025, approximately 1.87 million credit card numbers were provided to international brands.

【Figure48： Providing information on fraudulent credit card numbers to international brands】



③ Addressing infrastructure related to illegal and harmful information

The police are working to identify illegal and harmful information through cyber patrols and other means and are using this as a starting point for enforcement actions and requests to site administrators to remove such content.

○ Initiatives at the Internet Hotline Center (IHC)

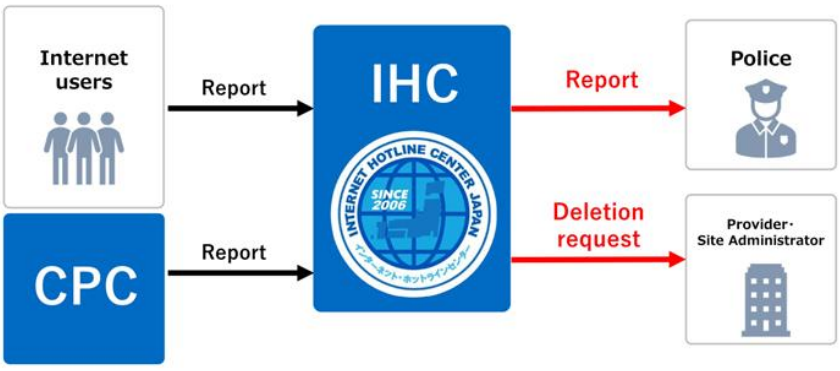
NPA has outsourced the operation of the IHC, which receives reports of illegal and harmful information from internet users and makes requests to the police and site administrators to remove the content. It has also outsourced the operation of the Cyber Patrol Center (CPC), which collects illegal information, information closely related to serious crimes and information that induces suicide and reports it to the IHC.

Based on an analysis of 633,036 cases received by the IHC in 2025, according to the operational guidelines, 105,553 cases were identified as illegal activity, 1,538 cases as closely related to serious crimes, and 5,321 cases as suicide inducement or similar activities.

Furthermore, the Ministry of Health, Labor and Welfare clarified that job postings that do not include the recruiter's name or company name, address, contact information, job description, place of work, and wages violate the Employment Security Act. In light of this and considering that this fact has been included in the draft guidelines for illegal information currently under consideration by the Ministry of Internal Affairs and Communications, the Ministry revised the IHC's operational guidelines in February 2025 to effectively remove criminal perpetrator recruitment information. This revised the IHC's guidelines, classifying "recruitment of criminals," which was previously a type of information closely related to serious crimes, as illegal information (violation of the Employment Security Act, etc.), and strengthened its system in March of the same year.

Furthermore, in June of the same year, a law amending part of the Basic Act on Measures Against Gambling Addiction was enacted, prohibiting acts such as disseminating information via the internet to unspecified persons in Japan that lure them to illegal online gambling. In conjunction with the enforcement of the law in September of the same year, the IHC revised its operational guidelines, adding this type of information to its scope of handling as illegal information, thereby strengthening efforts to prevent the distribution of this information, which has become a social problem. (See page 37)

【Figure49 : How the Internet Hotline Center works】



○ Police Initiatives

NPA is working to raise awareness of initiatives such as IHC, and in order to ensure the effectiveness of removing illegal and harmful information, in October 2025, it requested continued cooperation from domestic internet service providers and other related parties in removing illegal and harmful information. Prefectural police forces are also working to identify illegal and harmful information through cyber patrols and

other means, and in 2025, they made approximately 530,000 requests for the removal of illegal and harmful information.

Additionally, we operate a system to provide information to social networking service providers to encourage them to suspend or delete accounts used in investment/romance fraud via social media and other communications fraud cases that the police have become aware of. In 2025, we provided information on more than 18,500 cases.

In addition, as countermeasures against individuals who have become radicalized without any connection to specific terrorist organizations, so-called lone offenders, we are working to find information on the internet regarding the manufacture of firearms and explosives and are requesting site administrators to remove such information.

Furthermore, based on the "Comprehensive Measures to Protect Citizens from Fraud 2.0" (decided by the Cabinet Meeting on Crime Prevention on April 22, 2025), various measures are being promoted with the cooperation of relevant organizations, groups, and private businesses.

3 Development of Human and Physical Infrastructure

(1) Development of Organization

As of 2025, the number of personnel of Cyber Affairs Bureau of NPA is 260, and NCD has 185 officers and technicians, reflecting ongoing expansion.

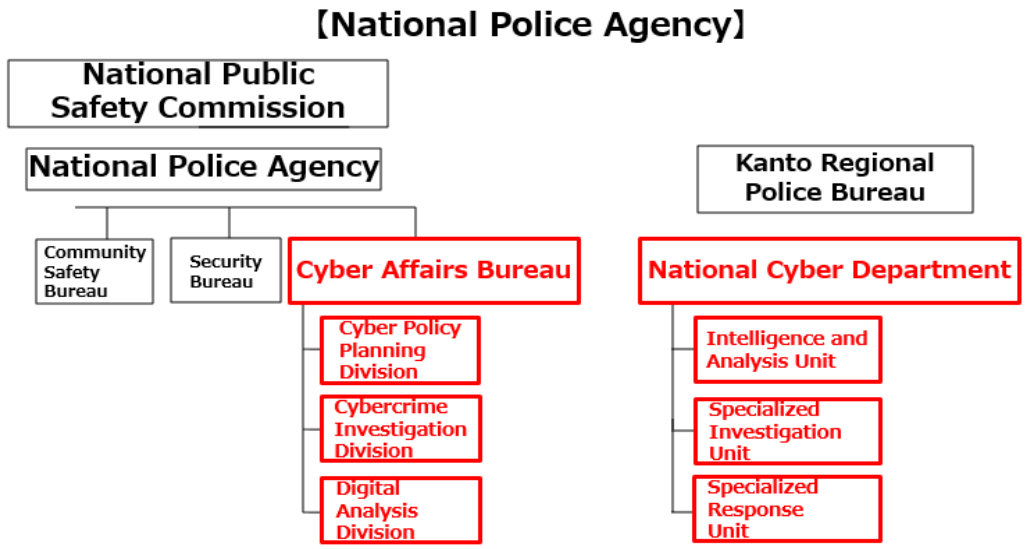
In April 2022, the Police Act was amended, and the National Cyber Unit was established within the Kanto Regional Police Bureau as a national investigative organization for serious cybercrimes.

The establishment of the National Cyber Unit enabled NPA—formerly only a coordinator between foreign agencies and prefectural police—to conduct direct nationwide investigations and arrest suspects through international collaboration. Accordingly, it recruits highly knowledgeable personnel from police forces across Japan and is equipped with advanced tools. With these capabilities it can now identify suspects and map criminal groups that were previously hard to tackle, and continuous information exchange with foreign security agencies has built strong mutual trust.

In April 2024 the unit was reorganized as the National Cyber Department, adding an Intelligence and Analysis Unit and a Specialized Investigation Unit; a Specialized Response Unit was added in April 2025. Consequently, capabilities for investigation,

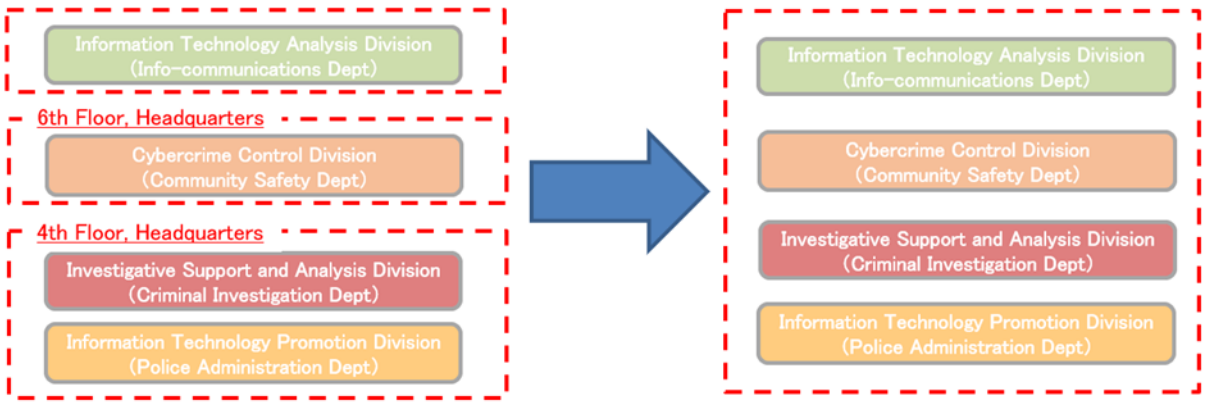
information collection, cross-case analysis, incident prevention and damage mitigation have been reinforced. The restructuring enables the Cyber Special Investigation Department to pool data from prefectural investigations, combine it with intelligence from foreign agencies and its own inquiries, and thus more effectively identify core suspects and clarify criminal activities.

【Figure 50 : Overview of the Cyber Affairs Bureau and the National Cyber Department】



Prefectural police also expand their structures to handle sophisticated cyber incidents, integrating investigative and support units and consolidating cyber-division workspaces.

【Figure 51: Example of floor integration in the Yamaguchi Prefectural Police】

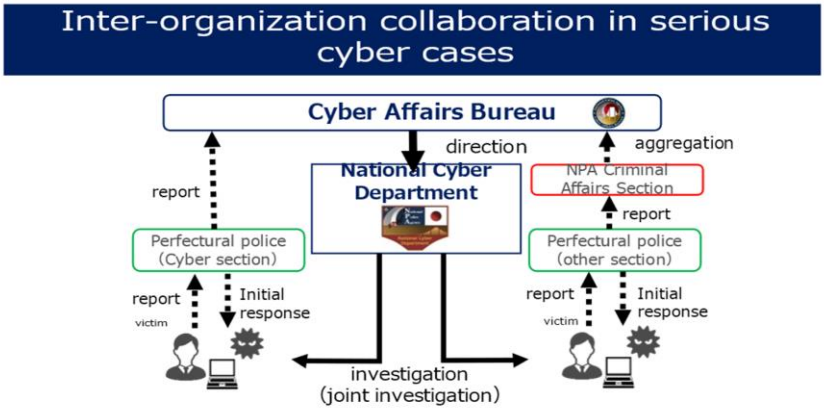


Column : Relationships Among Police Organizations in Criminal Investigations into Serious Cyber Cases

For individual cyber cases, at the time of their occurrence, the entity that caused the case, its intentions, background, and relevance are not clear. Therefore, to uncover organized crimes by criminal organizations and cyberattacks related to security backed by states, etc., and to deal with them appropriately, it is essential to steadily promote criminal investigations into individual cyber cases to elucidate their realities, as well as to aggregate the information, etc., obtained through the investigations and conduct comprehensive and cross-sectoral analysis.

For this reason, within the police, the prefectural police, who hold the responsibility for public security regarding individual cyber cases, primarily promote criminal investigations and proceed with the identification of suspects and the infrastructure used in the said cases, etc. At the same time, this information is aggregated in the National Cyber Department. By acting as an "information hub" and conducting comprehensive and cross-sectoral analysis, the division clarifies the relevance among cases, such as commonalities in entities and infrastructure, and elucidates their organizational structure and state involvement.

Based on these results, the police seamlessly deal with matters ranging from crimes to cases related to security and are working to ensure safety and security in cyberspace by identifying and clearing suspects through international joint investigations with foreign law enforcement agencies, etc., implementing public attribution, and, going forward, appropriately exercising the authority pertaining to remote access and neutralization measures scheduled to be enforced on October 1, 2026.



（Measures for Dealing with Wide-Area Organized Crime, etc.）

16-3

When the Director-General determines that it is necessary in order to deal with wide-area organized crime and related offenses, he may issue such instructions to the Prefectural Police as are necessary concerning the allocation of responsibilities among the relevant Prefectural Police for the handling of wide-area organized crime and related offenses (in the case of the handling of serious cyber incidents, the allocation of responsibilities between the National Police Agency and the relevant Prefectural Police), and any other matters relating to the police posture required for dealing with wide-area organized crime and related offenses.

(2) Human Resource recruiting and Development

○ Human Resource recruiting

To bolster the human foundation against cyber threats, the police have been committed systematically to promote cross-departmental initiatives to hire and train cyber personnel, manage career paths, and enhance the response capabilities of all staff, based on national policies for prefectural police and info-communications departments.

In prefectural police, approximately 480 officers who were hired through mid-career and special recruitment programs —based on private-sector experience or advanced ICT qualifications—serve as Cyber Special Investigators, utilizing their expertise on the front lines of cybercrime investigation.

Column: Senior Police Officers Recruited through Mid-career Recruitment and Public-Private Personnel Exchange Programs

○ **Executive Recruited as a Cyber Special Investigator**

Superintendent Maruyama Atsushi was recruited mid-career by the Chiba Prefectural Police in April 2000. Following roles as Chief of the Cybercrime Control Division and a Police Station Chief, he was appointed Chief of the Special Investigation Division within the Kanto Regional Police Bureau's National Cyber Department in March 2025. He now commands investigations into serious cyber incidents involving advanced technical methods.

Superintendent Maruyama Atsushi commanding a criminal investigation

○ **Executive Recruited via Public-Private Exchange**

Superintendent Hamaishi Yoshitaka, formerly of a cybersecurity firm, was seconded to the NPA in 2019 for three years under the public-private exchange programs. Re-recruited in 2023, he now leverages private-sector expertise at the NPA Cyber Affairs Bureau and the Kanto Regional Police Bureau's National Cyber Department to advance the aggregation and analysis of cyber incident information.

Superintendent Hamaishi Yoshitaka engaged in analysis work

NPA has recruited individuals with specialized ICT expertise as technical personnel and has developed them through practical training, as a result, approximately 800 personnel are serving on the front lines of information technology analysis.

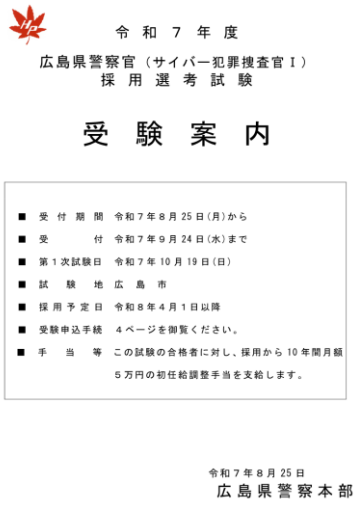
Furthermore, as an initiative to hire advanced cyber human resources, the NPA has promoted the appointment of private-sector talent through the public-private personnel exchange programs, under which the Cyber Affairs Bureau has recruited eight individuals with advanced expertise since its establishment in 2022. Additionally, starting from fiscal 2026, the bureau plans to recruit two technical personnel to engage exclusively in the handling of cyber incidents—a specialized process referred to as "Cyber Recruitment."

Column: New Measures for hiring Cyber Human Resources

To effectively counter cyber threats, the NPA will launch "Cyber Recruitment" in fiscal 2026, hiring two technical officials dedicated solely to cyber response. This inaugural initiative involves specialized NPA original recruitment exams for individuals with applied IT skills to appoint experts specializing in cyber department operations.

Staff hired through Cyber Recruitment will primarily serve in the NPA Cyber Affairs Bureau and the Kanto Regional Police Bureau's National Cyber Department. By prioritizing technical growth in personnel assignments, the NPA is establishing career paths for high-level experts and is currently inviting applications for the fiscal 2027 intake following the fiscal 2026 recruitment.

The Hiroshima Prefectural Police, recruiting for fiscal 2026 appointments since fiscal 2025, introduced a 50,000-yen monthly salary allowance for 10 years for experts with advanced IT qualifications; one candidate has already been selected for the Cybercrime Investigator I category. Additionally, exam bonus points are awarded to the applicants who have been engaged in cybercrime prevention volunteers under the Cybercrime Investigator II category.



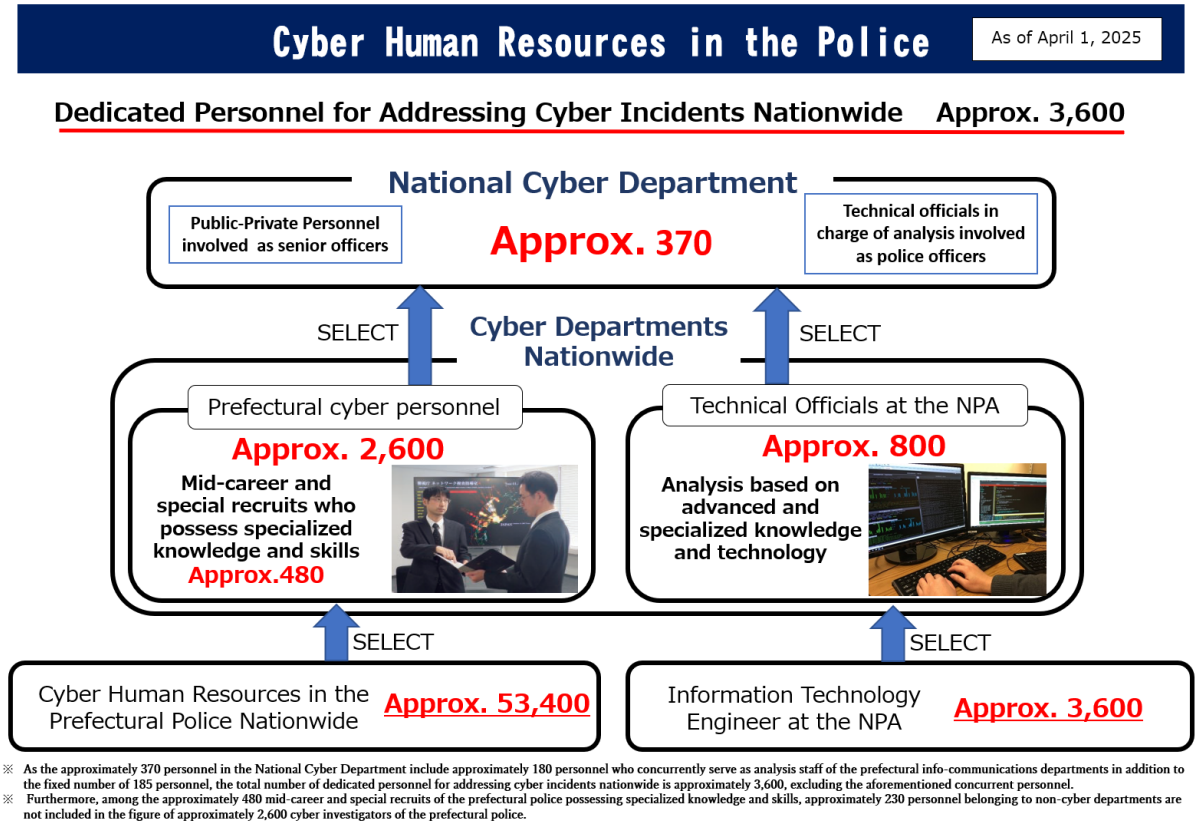
令 和 7 年 度
広島県警察官（サイバー犯罪捜査官Ⅰ）
採 用 選 考 試 験

受 験 案 内

■ 受 付 期 間　令和７年８月25日(月)から
■ 受　　付　令和７年９月24日(水)まで
■ 第１次試験日　令和７年10月19日(日)
■ 試 験 地　広 島 市
■ 採用予定日　令和８年４月１日以降
■ 受験申込手続　４ページを御覧ください。
■ 手　当　等　この試験の合格者に対し、採用から10年間月額５万円の初任給調整手当を支給します。

令和７年８月25日
広島県警察本部

【Figure52 ： Cyber Personnel in the Police】



※ As the approximately 370 personnel in the National Cyber Department include approximately 180 personnel who concurrently serve as analysis staff of the prefectural info-communications departments in addition to the fixed number of 185 personnel, the total number of dedicated personnel for addressing cyber incidents nationwide is approximately 3,600, excluding the aforementioned concurrent personnel.
※ Furthermore, among the approximately 480 mid-career and special recruits of the prefectural police possessing specialized knowledge and skills, approximately 230 personnel belonging to non-cyber departments are not included in the figure of approximately 2,600 cyber investigators of the prefectural police.

○ Human Resource Development

The Cyber Police Training Division, established at the National Police Academy in April 2025, provides advanced practical training for cyber investigators and proper command training for prefectural police executives. These programs simulate actual criminal techniques and large-scale attacks within virtual environments to conduct practical investigative exercises and drills against the latest cyber threats.

The police also promote technical cooperation with cutting-edge companies and research institutions to develop advanced analysis personnel. Furthermore, they hold cyber contests for prefectural police to compete in skills for addressing cyberspace threats; these contests utilizing realistic scenarios, aim to enhance cyber-related capabilities and identify outstanding talent nationwide.

Recognizing that cyber-related knowledge is essential for all investigations as cyberspace can be exploited in any crime, the police conduct a Cyber Response Capability Proficiency Test for all personnel, classified into beginner, intermediate, and advanced levels. As of April

2025, approximately 800 individuals passed the advanced level for high-tech incidents, and 53,400 passed the intermediate level for network-utilization crimes.

Moreover, as of April 2025, personnel holding advanced information security certifications included approximately 700 Registered Information Security Specialists and 50 CISSP holders, with roughly 40 individuals possessing both credentials concurrently.

To accurately address serious cyberspace threats, prefectural police are establishing guidance and education teams within cyber departments to develop personnel through school and on-the-job training. Furthermore, starting fiscal 2026, police academies will introduce new cyber subjects and expand class hours, while assigning specialized instructors to enhance the overall cyber education framework.

Furthermore, to drive cross-departmental initiatives for hiring and training cyber personnel, the NPA plans to strengthen its Guidance and Human Resource Development Department to act as a command center leading the guidance systems of prefectural police.

Column: Cyber Range

Since fiscal 2018, the National Police Academy has introduced the Cyber Range, a cyber exercise environment for practical training against cyber incidents; by replicating actual criminal techniques and damage scenarios within virtual environments, the Academy implements practical investigative exercises and drills assuming large-scale cyberattacks, thereby striving to enhance response capabilities for cyber incidents.

【Investigative Exercises Using the Cyber Range】

Column: Cyber Contest

Considering the scheduled enforcement on October 1, 2026, of the amended Police Duties Execution Act—stipulating remote access and neutralization measures—NPA newly established the "Offensive Security Category" in the fiscal 2025 Cyber Contest to verify practical capabilities such as discovering server vulnerabilities. This addition to the conventional "Cyber Investigation" and "Digital Forensics" categories aimed to confirm more practical skills.

Furthermore, prefectural police are implementing their original cyber contests not only for personnel to enhance response capabilities and identify talented individuals, but also for students to foster cybersecurity awareness among the youth and expand the pool of potential Cyber Special Investigators.

【Cyber Contests held in the Fukushima Prefectural Police】

(3) Research and Development

In recent years, cyber incidents that exploit malicious programs have become increasingly common. As the perpetrators' techniques have grown more sophisticated and varied, analyzing such malicious programs now requires an exceptionally high level of technical expertise. To support police investigations, it is necessary to continuously improve analytical capabilities that can keep pace with the latest technologies. Accordingly, the police are not only upgrading equipment and training staff with advanced analysis skills, but also promoting the development of analysis methods and the investigation-research of cutting-edge Information and Communications Technologies that could be misused for crime.

For instance, as part of efforts to elevate and streamline analysis, The NPA has introduced a lightweight analysis framework that (1) employs machine-learning-based functional estimation of malicious programs and (2) uses a sandbox that automatically runs the malicious code in a virtual environment to capture behaviors such as communication with other computers, file creation, and program execution. This framework is being utilized by information-technology analysis units nationwide; in 2025, it was employed in 5,808 cases by NPA and in 591 cases by local agencies.

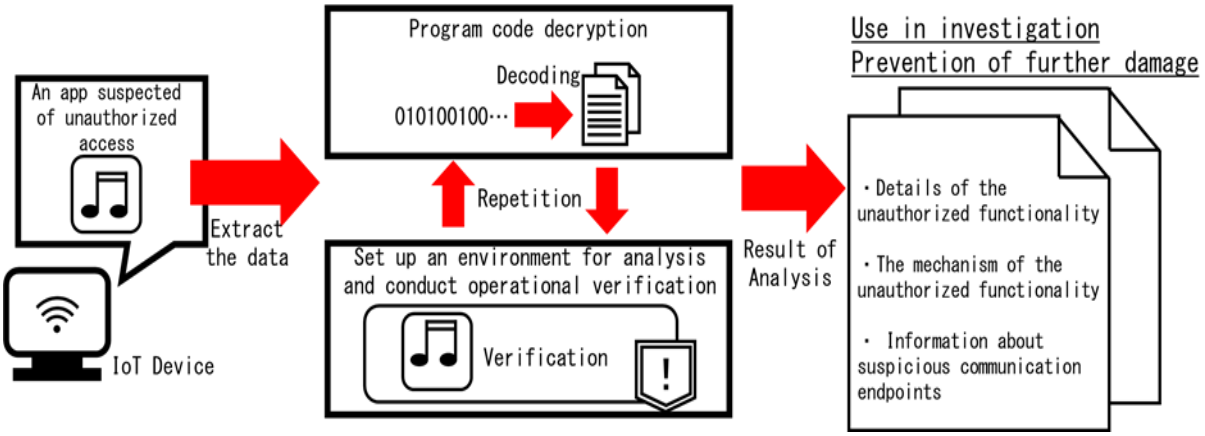
【CASE: Analysis of the Ransomware “VanHelsing”】

In May 2025, the NPA’s Digital Analysis Division analyzed the source code of the ransomware “VanHelsing,” which had first appeared in March of that year, and elucidated the encryption algorithm employed by the ransomware, the method used to generate the encryption keys, the structure of the encrypted files, and related details.

Column: Analyzing Malicious Programs Used as Gateways for Unauthorized Access

In recent years, there have been many incidents in which network-connected devices used in ordinary households (IoT devices) have been hijacked as gateways for unauthorized access without the owners’ awareness (see p. 34). The Digital Analysis Division investigates the tactics of such cyber cases by analyzing IoT devices and related software and uses the findings to help prevent and contain damage.

In 2025, NPA’s Digital Analysis Division conducted an analysis of a music-streaming application for IoT devices and found that the app includes a proxy function and other exploitable features. Consequently, the division disseminated this information to police forces nationwide. Based on that notice, the Nagano Prefectural Police, while conducting an ongoing investigation, confirmed that the IoT device and the app were indeed being used as a gateway for unauthorized access. They subsequently requested the app store to act, which led to the suspension of the application’s distribution.



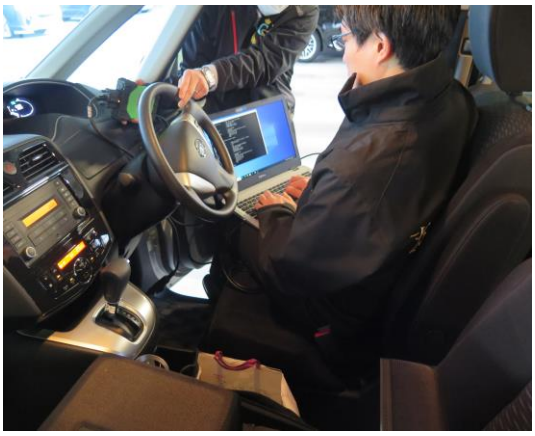
Column: Research on the Analysis of Autonomous Driving

The Research Center for Cybersecurity Measures at the National Police Academy conducts research on the analysis of electronic devices and on cutting-edge information and communication technologies that could be exploited for criminal purposes, utilizing its expertise in hardware and software.

For example, vehicles equipped with autonomous driving systems have connectivity features that link them to the outside world; if they are exploited to cause a security breach, it could lead to serious incidents or accidents. To prepare for these threats, the Center is conducting research on autonomous driving systems.

In fiscal year 2025, the Center conducted joint research with academic institutions to investigate security incidents, simulating cyberattacks against vehicles equipped with autonomous driving systems.

【Research on the Analysis of Autonomous】



(4) Maintenance of equipment and facilities

To effectively counter the escalating threats in cyberspace, it is imperative to upgrade and enhance equipment and facilities. Accordingly, NPA is advancing concentrated procurement of such equipment for government agencies, with the National Cyber Department at its core. For example, to aid in the apprehension of anonymous and fluid criminal groups and to prevent or mitigate damage from major cyberattacks, the agency is acquiring cryptocurrency analysis tools, cyber-investigation analysis equipment, smartphone-analysis equipment, analysis-platform devices, high-speed computing systems, and other related assets. It is also establishing a human-resource-development platform (a cyber range) to train cyber personnel. Considering the amendment to the Police Officer Duties Execution Act concerning remote access-and-neutralization measures, which is scheduled to take effect on October 1, 2026, the agency is likewise proceeding with the procurement of equipment and other resources that support active cyber defense.

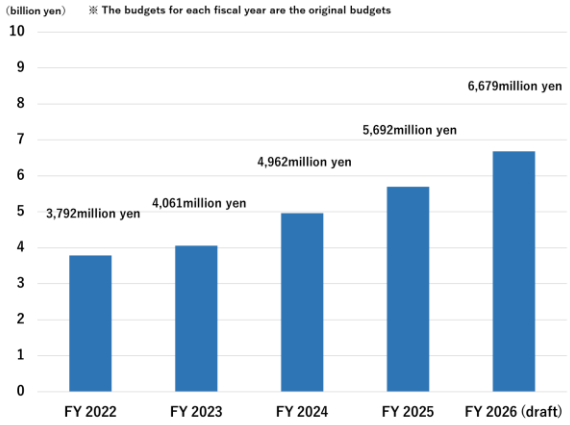
Specifically, the FY 2025 initial budget for addressing cyber-space threats is ¥5.692 billion, of which 4,459 million yen is allocated to improving response capabilities—including the procurement of investigative and IT-analysis equipment—

679 million yen to strengthening the human-resource foundation and promoting research, and 553 million yen to advancing public-private and international cooperation.

The budgets for strengthening cybersecurity measures in the FY 2024 supplemental budget and the FY 2025 supplemental budget are 8,876 million yen and 3,964 million yen.

The FY 2026 initial budget (draft) for addressing cyber-space threats is 6,679 million yen, of which 5,380 million yen is allocated to enhancing response capabilities—including the procurement of investigative and IT-analysis equipment—711 million yen to strengthening the human-resource foundation and promoting research, and 588 million yen to advancing public-private and international cooperation. As noted in Topic I, "The Role of the Cyber Police in National Security," cyberattacks, by nature, cannot be immediately identified in terms of the attacker or purpose at the moment an incident occurs; they must be clarified using the full response capabilities of the cyber police. Consequently, all budgets for addressing threats in cyberspace are classified as cyber-security-related expenditures.

【Figure 53: Budget for Addressing Cyberspace Threats at NPA】



The budget for addressing cyber-space threats at NPA has been increasing since Cyber Affairs Bureau was established in 2022. To respond effectively to cyber threats—including active cyber defense measures that consider national security and crisis management—further procurement and upgrading of equipment and facilities are essential. NPA will continue to work toward securing the necessary budget on an ongoing basis, considering the growing threats in cyberspace, including AI.


CYBER
SECURITY