

Part 1 Feature and Topics

Police Efforts Against Crime Involving Social Media

About the feature

The theme of this year's police whitepaper feature is "police efforts against crime involving social media."

While the remarkable advance of information and communications technology has brought various benefits to society, some of the technologies and services provided via the Internet are being misused as criminal infrastructure, making it easier to commit crimes and encouraging criminal activities. Addressing such misuse has become an urgent issue.

For example, widely used social media platforms are also being misused as criminal infrastructure. In particular, damage caused by investment/romance fraud via social media—where offenders build relationships without meeting in person, communicate repeatedly to build trust, and induce romantic feelings or a sense of familiarity in order to defraud victims of money—has reached an extremely alarming level. In addition, anonymous and fluid criminal groups—characterized by an anonymized core that absorbs proceeds from various crimes and by loose connections among members through social media and other means—have been observed recruiting criminal perpetrators on social media by suggesting high pay. These groups have individuals carry out crimes such as fraud, robbery, and theft while treating the low-level criminal perpetrators as effectively "expendable." The situation surrounding these crimes is extremely serious and has become a major factor contributing to the deterioration of perceived public safety.

Furthermore, social media is also being misused for illegal activities such as drug trafficking and child prostitution. In addition to illegal content such as child pornography and other harmful information that may incite criminal activity, the posting and dissemination of disinformation and misinformation on social media have become social issues.

In this feature, Section 1, entitled "Situation and Countermeasures Concerning Crime Involving Social Media," provides an overview of the types of crime involving misuse of social media and the countermeasures taken in response. Section 2, entitled "Technological Foundation for Addressing Crime Involving Social Media," introduces initiatives undertaken by digital analysis divisions. Lastly, Section 3 presents perspectives on future countermeasures in light of the current situation and existing countermeasures concerning crime involving social media.

Widespread use of social media has made it easier for criminals—including anonymous and fluid criminal groups—to approach members of the public and carry out crimes, posing a significant challenge to public safety. Cases have been observed in which the identity verification carried out upon social media account creation is insufficient, and social media and other highly anonymous means of communication have become obstacles to investigations.

We hope that this feature will contribute to deepening public understanding of the situation surrounding crime involving social media and police efforts, and will also serve as a reference for considering appropriate measures to prevent victimization from such crimes and to ensure public safety and security.

MEMO



The situation concerning social media

Social media platforms are widely used not only as a means of everyday communication by individuals but as platforms for disseminating information by a wide range of actors, including businesses and government agencies, and have become widely embedded in people's daily lives and socioeconomic activities as a form of public infrastructure. At the same time, because social media platforms enable anyone to communicate anonymously and bidirectionally, they can be misused for criminal purposes. Moreover, as many social media platforms are provided by overseas operators, operators without a local subsidiary in Japan or a domestic point of contact poses challenges for smooth criminal investigations and prompt information provision. This feature introduces initiatives aimed at addressing crime involving the misuse of social media, which has rapidly expanded and evolved in recent years.

Section 1

Situation and Countermeasures Concerning Crime Involving Social Media

1 The Current Situation and Countermeasures Concerning Crime Involving the Misuse of Social Media

(1) Investment/romance fraud via social media

Damage caused by investment/romance fraud via social media—where offenders build relationships without meeting in person, communicate repeatedly to build trust, and induce romantic feelings or a sense of familiarity in order to defraud victims of money—has reached an extremely alarming level.

Reported cases and amount of damages from investment and romance fraud via social media

In 2024, the number of reported cases of investment/romance fraud via social media totaled 10,237, and the amount of damages reached approximately 127.2 billion yen. Both figures increased significantly compared to the previous year.

Chart F-1 Numbers of reported cases of investment/romance fraud via social media and amounts of damages (monthly figures for 2023 and 2024)



Note: For the 2023 survey, the cases of romance fraud via social media were limited to those in which the offender claimed to be a foreign national or an overseas resident.

In these types of fraud, criminal groups contact victims via social media or dating apps, move them to another social media app for further communication, exchange messages repeatedly to build trust, and ultimately defraud victims of money through methods such as bank account transfers. In 2024, many victims—both men and women—were in their 40s to 60s, and the average amount of damages per case exceeded 12 million yen.

Chart F-2 Age groups of victims (Investment fraud via social media)

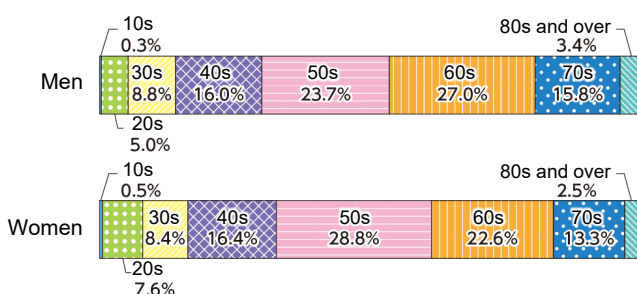
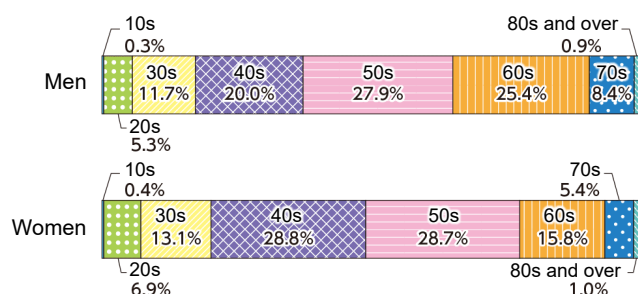


Chart F-3 Age groups of victims (Romance fraud via social media)



② Arrest status and countermeasures for investment/romance fraud via social media

In recent years, amid widespread use of social media and cashless payment systems, fraud schemes exploiting new services have rapidly grown more sophisticated and diverse, leading to a sharp increase in damages caused by investment/romance fraud via social media and creating an extremely serious situation.

In 2024, the number of individuals arrested for investment/romance fraud via social media totaled 129, comprising 58 for investment fraud and 71 for romance fraud. It remains an urgent priority to further strengthen crackdowns and fact-finding efforts targeting anonymous and fluid criminal groups suspected of involvement in such crimes (see Note), while vigorously promoting countermeasures in cooperation with relevant organizations and institutions.

A Promotion of effective public information and awareness-raising activities based on the circumstances of victimization

Based on the actual circumstances of damages caused by investment/romance fraud via social media, the National Police Agency is implementing targeted advertisements on web news apps and similar platforms to alert Internet users, while cooperating with government public information authorities in conducting public information and awareness-raising activities.

In addition, in light of widespread use of social media and dating apps in committing such fraud, the National Police Agency is urging service providers to issue timely, appropriate alerts to individual users of their services.

B Prompt suspension of social media accounts used in crimes, etc.

Given that social media accounts and dating apps are misused by criminal groups to contact victims in investment/romance fraud via social media, a scheme has been established and is being operated under which, based on reports from victims and requests from the police, social media service providers and other relevant operators identify social media accounts and similar tools used by criminal groups and then promptly implement measures, such as usage suspensions.

C Promotion of crackdown measures in cooperation with financial institutions

As the number of cases of investment/romance fraud via social media has increased sharply and cases involving the misuse of corporate accounts have also been observed, countermeasures against financial crimes through bank accounts have become an urgent issue. In August 2024, acting in cooperation with the Financial Services Agency, the police requested that the Japanese Bankers Association and other relevant organizations strengthen information sharing and cooperation with the police in order to further enhance measures to prevent fraudulent use of bank accounts, including corporate accounts. Based on this, the police are working to establish a cooperative framework under which financial institutions promptly provide information to prefectural police when transaction monitoring detects activity that poses a high risk of fraud.

CASE

From February to July 2024, a 29-year-old restaurant owner and others, posing as instructors on the topic of binary options trading, used social media to show victims images and other materials while falsely claiming that students who had received instruction from those instructors had earned substantial profits. By leading the victims to believe that they could absolutely earn large profits within a short period by investing as instructed, the suspects defrauded them of a total of approximately 7.6 million yen under the pretext of payment for investment-related informational materials. By October 2024, 41 individuals, including the man, had been arrested on suspicion of fraud. (Osaka Prefectural Police)

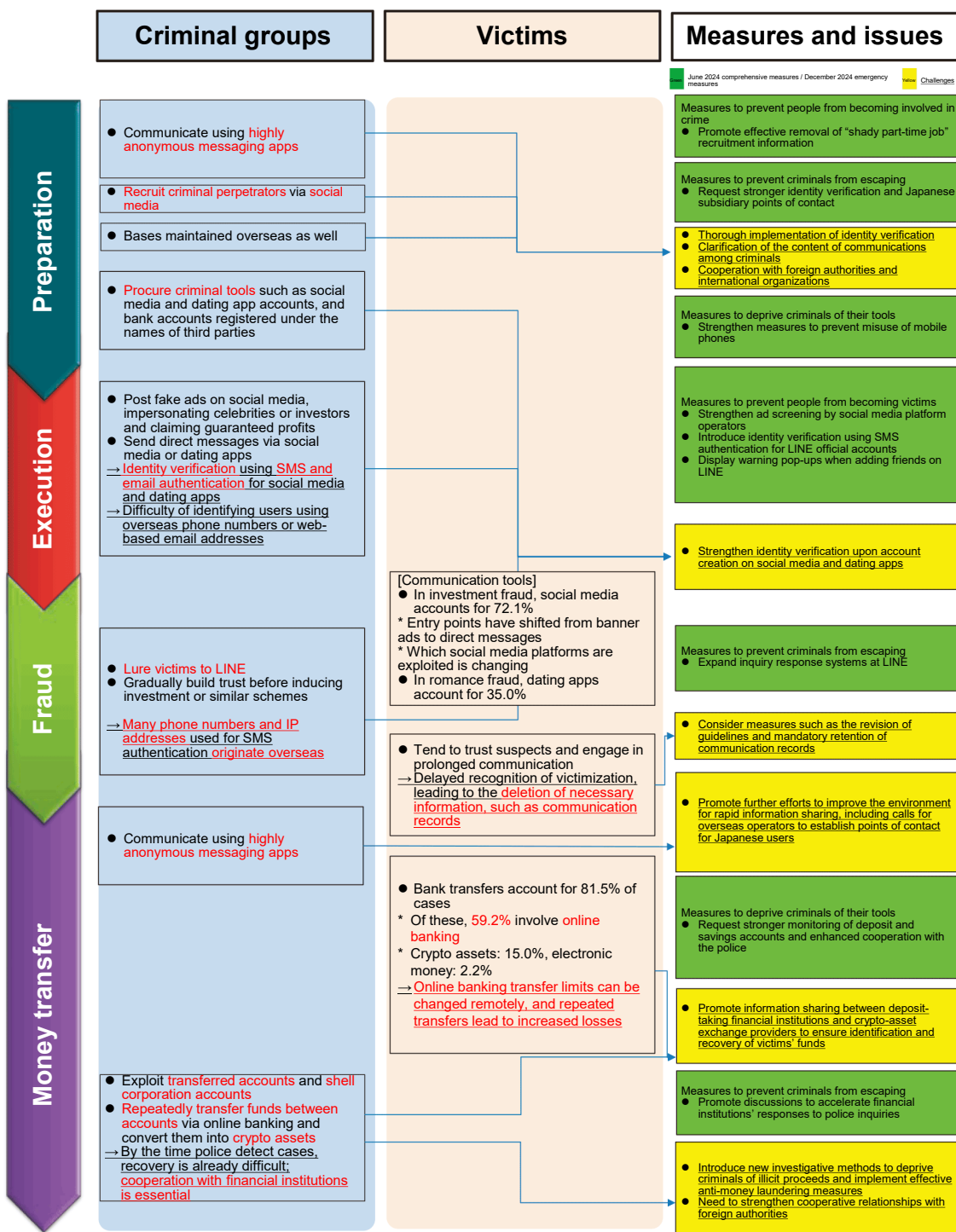
CASE

In January 2022, a 61-year-old Nigerian national and others, posing as a woman, made contact with victims through social media and sent fraudulent emails claiming that it was necessary to pay fees for asset transfers. Under the pretext of fees and other charges related to such asset transfers, the suspects defrauded the victims of approximately 600,000 yen. By July 2024, three individuals, including the man, had been arrested on suspicion of fraud and other related offenses. (Tokyo Metropolitan Police Department)



Formulation of the Comprehensive Measures to Protect People from Frauds 2.0 (Government-wide initiative)

Chart F-4 Flow of victimization in investment/romance fraud via social media



Note: Excerpt from materials of the 42nd Meeting of the Ministerial Conference on Measures against Crime (held on April 22, 2025)

In June 2024, the Government of Japan formulated the Comprehensive Measures to Protect People from Frauds (adopted at the Ministerial Conference on Measures against Crime on June 18, 2024), which consolidate countermeasures against fraud in general, including investment/romance fraud via social media, and has vigorously promoted measures to halt damage caused by fraud and other crimes, foster the sound development of Japanese society based on trust, and realize a safe and secure society. In December of the same year, after reviewing the progress of the various measures implemented to date, the Government of Japan compiled the Emergency Measures to Protect People's Lives and Property from Robbery and Other Crimes Committed Through "Shady Part-time Jobs" in order to further strengthen

countermeasures. These measures, which were adopted at the Ministerial Conference on Measures against Crime on December 17, 2024, have been implemented to address robbery and other crimes committed by criminal perpetrators recruited via social media and other online platforms to do “shady part-time jobs.” (Note 1)

However, as public- and private-sector efforts have progressed, offenders have adapted their methods accordingly. To protect the public from fraud and other crimes that are becoming ever more complex and sophisticated, without falling behind such evolving criminal tactics, it is necessary not only to swiftly update countermeasures in response to changes in criminal methods, but to strengthen fundamental measures, including efforts to clarify the actual conditions of criminal groups and to sever points of contact between such groups and their victims. As shown in Chart F-4, the Government of Japan examined existing

measures and issues at each stage of the points of contact between criminal groups and victims for each category of fraud and other crimes. In April 2025, the Government of Japan formulated the Comprehensive Measures to Protect People from Frauds 2.0 (adopted at the Ministerial Conference on Measures against Crime on April 22, 2025) (Note 2), integrating the Emergency Measures to Protect People’s Lives and Property from Robbery and Other Crimes Committed Through “Shady Part-time Jobs.” The Government of Japan has decided to fundamentally strengthen government-wide efforts against fraud and other crimes. The main measures to be undertaken by the Government to prevent abuse of financial and telecommunications services and infrastructure are as follows.

❶ Promotion of crackdowns and clarification of actual conditions in light of the presence of anonymous and fluid criminal groups

To respond flexibly to changes in how anonymous and fluid criminal groups operate as well as to weaken and dismantle criminal groups, including ringleaders and masterminds operating behind the scenes, the Government of Japan will promote effective crackdowns that transcend organizational boundaries, while advancing efforts to clarify the actual conditions of the revenue-generating activities and other activities of anonymous and fluid criminal groups.

❷ Strengthening identity verification requirements for social media and dating app service providers

As cases have been confirmed in which social media and dating app accounts are misused to gain users’ trust and lead to fraud victimization, the Government of Japan will continue to encourage social media service providers and dating app operators to implement identity verification at the time of account creation.

❸ Mandating the retention of communication records

There have been a certain number of cases in which investigative authorities have sought to obtain communication records from telecommunications carriers after having become aware of victimization but such communication records are no longer available. The Government of Japan will consider the approach to communication record retention by telecommunications carriers, including the necessity and appropriateness of retention, retention periods, cost-related issues, revisions to the Guidelines on the Protection of Personal Information in the Telecommunications Business, and the introduction of a mandatory retention requirement.

❹ Strengthening screening at the time of applying for Internet banking

As use of Internet banking appears to be a factor contributing to higher losses, the Government of Japan will promote measures such as appropriate setting of initial transaction limits for Internet banking as well as user confirmation and alerts when transaction limits are increased.

❺ Creating a framework for information sharing among financial institutions

Criminal groups hold accounts at multiple deposit-taking financial institutions, which makes it difficult to freeze such accounts before victim funds are transferred to such groups. To enable rapid sharing of information regarding accounts used in crimes with investigative authorities, to prevent withdrawals of victims’ funds by criminal groups, and to promote loss recovery, the Government of Japan will consider creating a framework that allows deposit-taking financial institutions to share information on fraudulently used accounts and promptly freeze such accounts.

The police will continue to promote these measures in cooperation with relevant organizations to address investigative challenges related to crimes committed using social media.



The 42nd Meeting of the Ministerial Conference on Measures against Crime (Prime Minister’s Office of Japan website)

Note 1: The term “information on ‘shady part-time jobs,’ etc.” refers to posts and related information that seek to recruit individuals to carry out crimes using expressions such as “shady part-time job” or “under-the-table job,” or by suggesting exceptionally high pay without clearly specifying the nature of the work. Such expressions have been pointed out as making it easy to become casually involved in criminal activities. The police refer to such information as criminal perpetrator recruitment information.

2: For an overview of the decision, please refer to the QR code.



MEMO

Promotion of enhanced international cooperation against organized fraud

Amid growing international momentum to combat cross-border organized fraud—driven by events such as the G7 Interior and Security Ministers' Meeting held in Mito City, Ibaraki Prefecture in December 2023, and the Global Fraud Summit held in London in March 2024—the Global Fraud Meeting was held in Tokyo in September 2024, with the participation of 16 countries and 3 organizations.

Aiming to further strengthen international cooperation, the meeting featured a keynote address by the Commissioner General of the National Police Agency. In addition, participants shared key observations and lessons learned, drawing from the latest threat information and countermeasures as well as cases of arrests identified by governments and international organizations. Based on presentations given by participating countries and organizations, practical discussions were held on international investigative cooperation related to cracking down on overseas criminal bases, and on the fraud countermeasures implemented by each country.



The Global Fraud Meeting in session



Keynote address by the Commissioner General of the National Police Agency

(2) Disinformation and misinformation

① Disinformation and misinformation on the Internet

In recent years, with the spread of digital services such as social media as well as video-sharing and posting platforms, anyone can become a sender of information, and vast amounts of information circulate on the Internet and are easily accessible to everyone. At the same time, disinformation and misinformation online can spread widely within a short period, posing a serious challenge that may have significant impacts on people's daily lives as well as on social and economic activities.

For example, during large-scale disasters, it may require time to verify and assess the credibility of disinformation and misinformation on the Internet, potentially hindering rescue operations in affected areas and causing social disruption.

The police request the removal of such information from the service providers in question based on information identified through police activities. The police also promptly and effectively issue warnings via social media and other channels regarding disaster-related disinformation and misinformation, while taking strict enforcement action against illegal acts.

サイバー警察局便り
Cyber Police Agency Letter R6 Vol.6

令和6年宮崎県日向灘を震源とする地震におけるインターネット上の偽・誤情報にご注意！

1 被害状況や救助に関する偽・誤情報

- 過去の災害画像を転用して被害状況を伝える投稿
- 存在しない住所と共に救助を求める投稿

チェックポイント

- 画像は本物？過去の災害等の無関係のものではない？
- 災害の専門家が発信している情報？
- 信頼できる提供元からの情報？（他のメディアでも報じられている等）

！ 不確かな情報は安易に拡散しないで！
迅速な救助や復旧・復興の妨げになる可能性があります。

2 災害に乗じた詐欺関連の投稿やメール

- 二次元コードを添付して寄附金を求める投稿
- 支援物資や義援金を募るEメールやSMS

チェックポイント

- 支援を求めるアカウントは、実在する団体等のもの？
- 文字や文章の一部がおかしかったり送信元メールアドレスが海外ドメインであるといった不審点はない？

！ 安易にコードの読み取りやリンクのクリックをしないで！
詐欺サイトやフィッシングサイトに誘導されるおそれがあります。

不審な投稿やメール等で不安を感じた場合は警察に通報、相談してください。

最寄りの警察署又は警察相談専用電話 ☎ #9110 (全国共通)

サイバー事案に関する通報等のオンライン受付窓口 (警察ウェブサイト)
<https://www.nipou.go.jp/bureau/cyber/soukan.html>

警察庁

Advisory on disinformation and misinformation following the Hyuga-nada earthquake off the coast of Miyazaki Prefecture

CASE

A 25-year-old male company employee posted false information on “X” (formerly Twitter) during the 2024 Noto Peninsula Earthquake ^(Note), posing as a disaster victim and claiming to require rescue. The police officers who found the post were led to carry out unnecessary search activities, hindering the proper execution of their duties and obstructing police operations. Following an investigation conducted based on information provided by the National Cyber Department of the Kanto Regional Police Bureau, the individual who made the post was identified. In July 2024, the man was arrested on suspicion of fraudulent obstruction of business. (Ishikawa Prefectural Police)

Note: An earthquake with a magnitude of 7.6 that occurred at 4:10 p.m. on January 1, 2024, with its epicenter in the Noto region of Ishikawa Prefecture

② Threats posed by foreign disinformation and countermeasures

In recent years, beyond the realm of traditional security, the international community has increasingly expressed concern over the spread of disinformation. Dissemination of disinformation has in some overseas cases been used in combination with military means, and it has also been pointed out that such dissemination may undermine the integrity of elections. As such, the spread of disinformation constitutes not only a threat to universal values but a factor that may adversely affect public security in Japan. With the advance of generative AI technologies, it has become a key issue how to address the risks regarding the mass production of sophisticated disinformation and its dissemination via social media and other platforms.

In February 2024, a Canadian research institute released a report stating that a Chinese company was operating fake websites impersonating local news organizations in 30 countries, including Japan, and disseminating information aligned with the views of Chinese authorities. In September of the same year, the United States Department of Justice announced an indictment against two employees of a Russian state-run media organization for disseminating disinformation intended to amplify divisions within the United States during the U.S. presidential election.

In Japan, during the 2024 Noto Peninsula Earthquake, cases were confirmed in which foreign-language disinformation was disseminated via social media, portraying a deterioration in public security in the affected areas, by, for example, misusing photographs taken during the Great East Japan Earthquake.

In Japan, based on the National Security Strategy approved by the Cabinet in December 2022, a framework was established within the Cabinet Secretariat to strengthen capabilities to address dissemination of disinformation by foreign actors, under which relevant agencies work together to carry out collection, consolidation, and analysis of information as well as dissemination of accurate information. The police, in coordination with relevant agencies and other bodies, are also working to appropriately address dissemination of disinformation by foreign actors through collection and analysis of information.

(3) Drug offenses

① The reality of drug trafficking using social media and other platforms

Japan's drug situation remains severe. In recent years, drug trafficking methods have become increasingly sophisticated, such as posting information on social media to solicit purchases and then, when prospective buyers express interest, directing them to highly anonymous communication tools to conduct the transactions. For example, according to a survey of cannabis abusers, methods classified as "via the Internet," including social media, accounted for just under 40 percent of responses regarding how abusers learned of sources for obtaining cannabis. The percentage increases as the age group becomes younger, suggesting that drug trafficking using social media may be fueling drug abuse among young people. Aiming to cut off supply and demand for illicit drugs, the police are promoting enforcement measures alongside effective public awareness and education activities, while working in coordination with relevant organizations.

Chart F-5 How users learned of cannabis sources

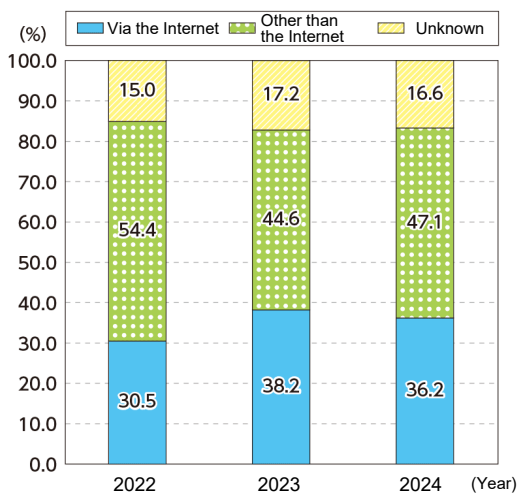
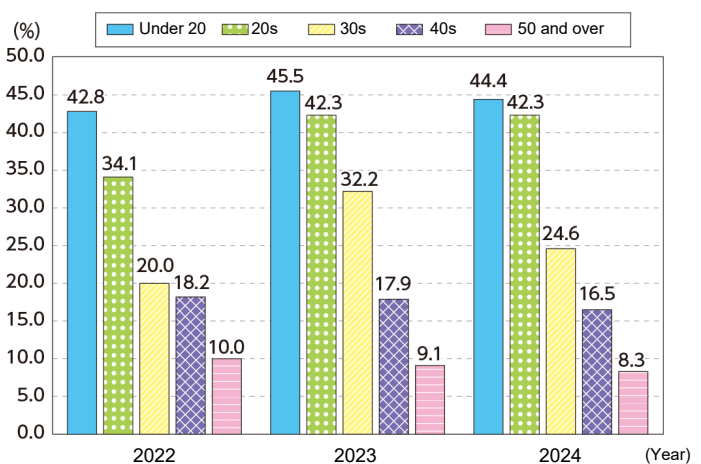


Chart F-6 Percentage by age group who learned of cannabis sources via the Internet, including social media



Note: The data covers individuals arrested for violations of the Cannabis Control Act (possession) during the period from October to November of each year from 2022 to 2024, as identified through investigations and other means.

CASE

From October 2022 to January 2024, a 28-year-old unemployed man and others attracted customers by posting messages on social media offering cannabis and related substances for sale in Chiba Prefecture and elsewhere, and engaged in the illicit sale of cannabis and related activities. By July 2024, four individuals, including the man, had been arrested for violations of the Act Concerning Special Provisions for Narcotics (engaging in transfer as a business) and other offenses, while seven customers who had purchased cannabis from the group had been arrested for violations of the Cannabis Control Act (possession). (Chiba Prefectural Police)



Seized cannabis and related items

② Promotion of public awareness activities using social media, etc.

Through public awareness activities, the police communicate the dangers and harmful effects of drugs as well as work to prevent their spread. In particular, following the December 2024 enforcement of the Act to Partially Amend the Cannabis Control Act and the Narcotics and Psychotropics Control Act—which made illegal use of cannabis subject to penal provisions—the police distributed educational videos on cannabis abuse prevention via video-sharing platforms to raise public awareness of the system and related matters.

The police also disseminate information using social media and other platforms, including targeted advertising aimed at individuals who have shown interest in cannabis on such platforms.



Cannabis abuse prevention awareness video on a video-sharing platform



Targeted advertising on social media

(4) Child sexual exploitation (Note 1)**① The reality of social-media-related child sexual exploitation**

As social media platforms offer a high degree of anonymity and enable users to communicate easily with unknown individuals, they have been misused as a venue for malicious offenses, including child prostitution, that exploit children's immaturity and vulnerable positions. Some cases have even resulted in the killing of children.

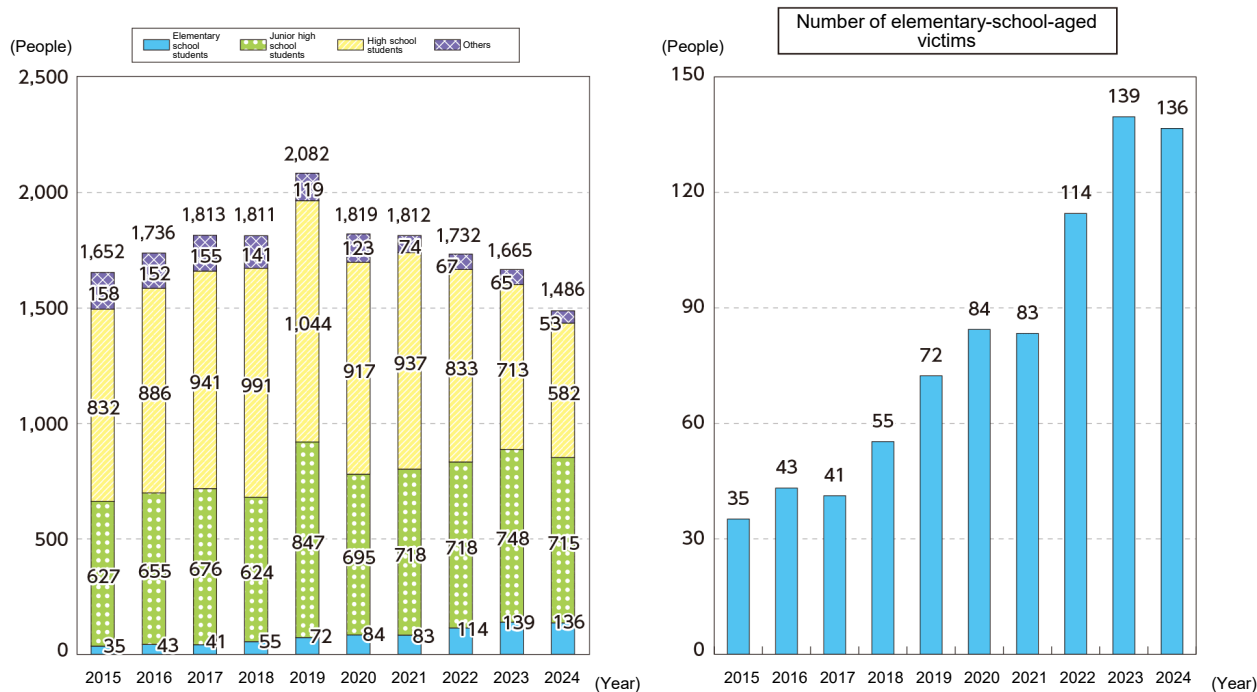
In 2024, the number of child victims of social-media-related offenses (Note 2)—including sexual crimes such as child prostitution, child pornography, and penetrative sexual assault—totaled 1,486. Although this figure decreased from the previous year, in recent years the number of child victims of such offenses has remained at a high level. In particular, the number of elementary-school-aged victims has been increasing, raising concerns about a reduction in the ages of victims.

Recognizing that child sexual exploitation causes serious harm to children's physical and mental well-being and constitutes an extremely heinous act that severely infringes upon children's human rights, the police are promoting initiatives such as strengthening enforcement efforts to eradicate child sexual exploitation.

Note 1: Sexual exploitation of children (this refers to acts committed against children for the purpose of satisfying one's own sexual curiosity or obtaining benefits for oneself or a third party, and these acts include engaging in child prostitution, the production of child pornography, and other criminal acts that cause sexual harm to children as well as engaging in business activities focused on the sexuality of children that fall under Article 60 of the Child Welfare Act, and other acts similar thereto) and acts that facilitate such exploitation (this refers to intermediation in child prostitution, trafficking in children for the purpose of child prostitution and related acts, providing locations for business activities focused on the sexuality of children, establishing websites for the purpose of distributing child pornography, and similar acts).

- 2: These cases refer to incidents in which a suspect and a child victim who were previously unacquainted met via social media (including via online video games) and the child was victimized before any relationship, such as dating or friendship, developed. 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.

Chart F-7 Number of child victims of social-media-related offenses by school age group, and number of elementary-school-aged victims (2015-2024)



CASE

From June to July 2023, a 54-year-old self-employed man gave cash to a 13-year-old girl whom he had met via social media under the pretext of “cosplay photography” and engaged in sexual intercourse with her. In February 2024, he was arrested for penetrative sexual assault and violation of the Act on Punishment of Activities Relating to Child Prostitution and Child Pornography, and the Protection of Children (child prostitution). (Osaka Prefectural Police)

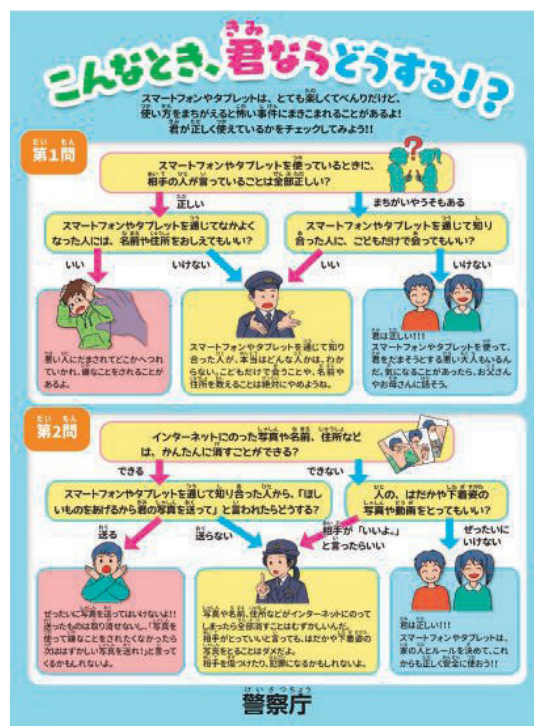
CASE

In July 2023, a 38-year-old male convenience store employee requested via social media that a 12-year-old boy whom he had met via an online video game record footage exposing the boy’s genitals and send the footage to the man’s smartphone. In February 2024, the man was arrested on suspicion of soliciting the transmission of images from a person under 16. (Nagasaki Prefectural Police)

2 Measures to address social-media-related child sexual exploitation

While cracking down on offenses involving child sexual exploitation, the police are also implementing measures focused on preventing harm before it occurs, including issuing cautions and warnings using reply functions on social media platforms and elsewhere in response to inappropriate posts that may lead to child sexual exploitation, such as posts appearing to be made by children seeking partners for child prostitution, or by children planning to run away from home and seeking accommodations.

In addition, in cooperation with relevant organizations and groups, the police are promoting initiatives to raise awareness among parents and children about appropriate use of the Internet, including social media, to encourage wider adoption of filtering functions (Note), particularly on smartphones, and to encourage social media platform providers to implement their own harm prevention measures through provision of information to the Social Media Association of Japan (SMAJ).



Public awareness leaflet

Note: Programs and services that screen websites and other online content based on certain criteria in order to prevent minors from accessing information that is harmful to them

2

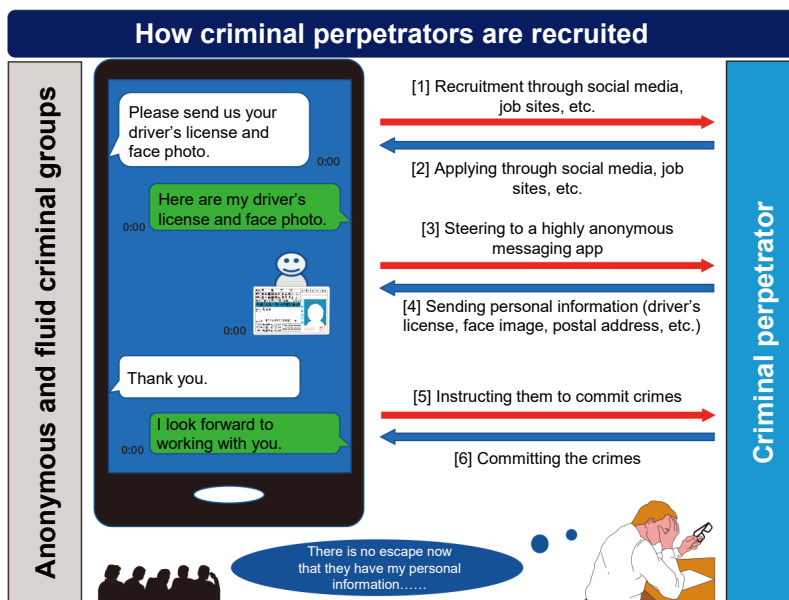
The Reality of and Countermeasures Against the Recruitment of Criminal Perpetrators Through the Misuse of Social Media

(1) Recruitment of criminal perpetrators by anonymous and fluid criminal groups

Anonymous and fluid criminal groups have been observed recruiting people to commit crimes via social media and other channels, not clearly specifying the nature of the work and instead using phrases such as “high pay,” “paid on the spot,” and “job with good conditions” to suggest work that is “easy,” “simple,” and “high-paying.”

There are cases in which these groups require applicants for such jobs (to commit crimes) to send them personally identifiable information, such as the applicant’s driver’s license, face photo, and so on, in advance via a highly anonymous means of communication so that they can make use of their advantageous position of possessing the applicant’s personal information to compel the person to submit and force the person to commit crimes repeatedly if the person hesitates to commit a crime or expresses an intention of breaking away from the group. There are also cases in which applicants are not paid as specified even when they have committed crimes.

Chart F-8 How criminal perpetrators are recruited

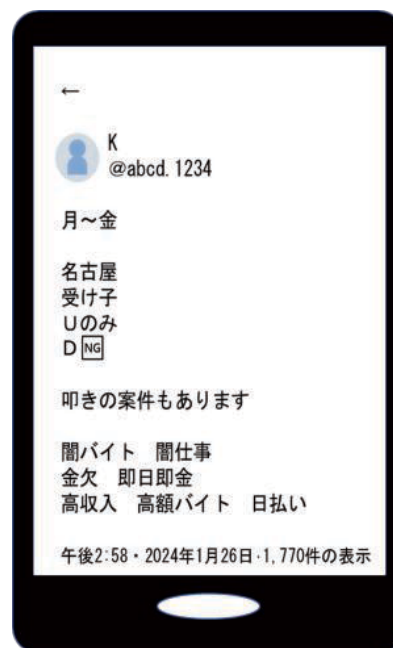


① Communications (Note) fraud and investment/romance fraud via social media

Anonymous and fluid criminal groups that carry out communications fraud and investment/romance fraud via social media recruit criminal perpetrators by suggesting high pay via social media and other channels, and involve recruits in criminal activities.

In many cases, they use varied tactics to destroy the evidence of their crimes. For example, they often adopt highly anonymous means of communication that can automatically delete messages exchanged between the ringleader, masterminds, and those who actually commit the crimes.

Furthermore, there are cases in which organized crime group members, as well as ringleaders and masterminds located overseas, use social media to recruit criminal perpetrators and have applicants carry out communications fraud and related offenses. There are also cases in which applicants are sent overseas and compelled to participate in criminal activities.



Example of criminal perpetrator recruitment information

Note: A collective term for crimes in which perpetrators gain the trust of victims without meeting them in person, such as by making phone calls, and fraudulently obtain cash and other valuables from an unspecified number of people through transfers to designated bank accounts or other methods (including extortion involving coercive acquisition of cash and fraudulent theft of cash cards)

CASE

From July 2023 to June 2024, a 36-year-old man of unknown occupation and others sent emails containing false information to users who had registered as members of a website purporting to introduce them to individuals seeking consultation, claiming that they could earn pay by responding to such consultations. In reality, the website had no users who were consulting, and no pay was provided even if users responded to the consultations conducted through the website. The emails falsely stated that users would be able to receive pay if they became official members of the site and paid various procedural fees as instructed on the website. Through this scheme, they fraudulently obtained approximately 2.8 million yen under the pretext of procedural fees. By July 2024, 45 suspects, including the man, had been arrested on suspicion of fraud. It was also revealed that some of the criminal perpetrators had applied to recruitment postings disguised as ordinary job advertisements on social media and job-search websites, featuring phrases such as “average monthly income of 480,000 yen,” and had participated in the scheme as so-called “decoy” users who approached victims with fictitious consultations. (Tokyo Metropolitan Police Department and Saitama, Chiba, and Fukuoka Prefectural Police)

② Robberies, thefts, and similar crimes (Note)

There are also cases in which the perpetrators who actually commit robberies, thefts, and similar crimes are recruited through social media, job sites, or other channels using phrases like “high pay,” “paid on the spot,” and “job with good conditions.” Some robberies and similar incidents believed to have been carried out by anonymous and fluid criminal groups have involved particularly heinous methods, including restraining victims and subjecting them to violence. In particular, a series of such robbery incidents that occurred in Tokyo and the three neighboring prefectures of Saitama, Chiba, and Kanagawa from August 2024 onward significantly worsened the public’s sense of security. In response to this series of robbery incidents, the police established a joint investigation headquarters in October 2024, led by the Tokyo Metropolitan Police Department and involving the relevant prefectural police, and have been vigorously conducting investigations aimed at apprehending the ringleaders. By the end of April 2025, 48 suspects had been arrested.

CASE

In September 2024, a 29-year-old male construction worker and others broke into a pawnshop and threatened a store employee by smashing a display case with a crowbar, suppressing the employee when the employee resisted, and robbing the store of wristwatches having a total retail value of approximately 20,000 yen. During the incident, they assaulted the store employee who attempted to restrain them, injuring the employee. One of the criminal perpetrators was arrested at the scene, and subsequent investigations revealed that the suspects had applied to criminal perpetrator recruitment postings on social media and had carried out the offense under instructions from a mastermind via highly anonymous means of communication. By November 2024, four suspects, including the man, had been arrested on suspicion of robbery resulting in injury and related offenses. (Kanagawa Prefectural Police)

(2) Police measures against criminal perpetrator recruitment

① Operation of the Internet Hotline Center

The National Police Agency operates the Internet Hotline Center (IHC), which receives reports from general Internet users concerning illegal information and related matters, reports such information to the police, and requests site administrators and others to remove the content. Criminal perpetrator recruitment information has proliferated on the Internet in recent years. In response to the Emergency Measures to Protect People’s Lives and Property from Robbery and Other Crimes Committed Through “Shady Part-time Jobs,” the IHC designated such information as illegal information in February 2025 in order to promote its effective removal. In March of the same year, the operational framework was further strengthened.

In addition, the police are issuing individual warnings and implementing other measures directed at posters of criminal perpetrator recruitment information by using reply functions on social media platforms.

The status of IHC operations is shown in Charts F-9 to F-11.

令和7年3月1日からIHCでは
犯罪実行者募集情報を
いわゆる闇バイト投稿「違法情報」
として通報を受け付けます。
※ IHC：インターネット・ホットラインセンター（Internet Hotline Center）
IHCの運用ガイドラインを改定しました！
▲ 次のような投稿は、違法情報（職業安定法違反等）として、IHCへの通報対象となります。
犯罪実行者募集情報
▶ 公衆衛生又は公衆道徳上有害な業務に就かせる目的での労働者の募集
「闇バイト」「ホワイト案件」「叩き」「受け子」「出し子」「運びの仕事」等の犯罪の実行者の募集を示唆する表現が記載された投稿
▶ 虚偽に当たる又は誤解を生じさせるような労働者募集の表示
募集者の氏名（名称）、住所、連絡先、業務内容、就業場所、賃金について記載のない求人投稿
ホワイト案件 即日即金 運びの仕事 詳細はテレグラムで
高収入バイト 全国で募集 振りスク 詳しくはDMで
▲ 今回の改定では、次の情報も違法情報として新たに通報対象に追加されました。
○ 無登録経営企業による広告（いわゆる「ヤミ金」の広告）
○ 拳銃等又は人の生命、身体若しくは財産を害する目的での拳銃等以外の銃砲等の所持を、公然、あおり、又は唆す行為
インターネット・ホットラインセンター
https://www.internethotline.jp
警察庁
厚生労働省

Public information and awareness-raising material related to the IHC

Note: Robberies, thefts, unlawful entry into residences and other buildings, etc.

Chart F-9 Number of cases analyzed by the IHC ^(Note)

Category \ Year	2020	2021	2022	2023	2024
Total (cases)	67,518	44,555	28,585	44,685	87,565
Illegal information	63,189	41,944	25,895	33,200	66,834
Suicidogenic information	4,329	2,611	2,690	6,609	6,582
Information closely related to serious crimes	—	—	—	4,876	14,149
Criminal perpetrator recruitment information	—	—	—	4,411	13,852
Others	—	—	—	465	297

Note: Excludes information not subject to analysis.

Chart F-10 State of criminal perpetrator recruitment information handling ^(Note)

Category \ Year	2023	2024
Cases analyzed (cases)	4,411	13,852
Response requests (cases)	2,979	9,234
Removals completed (cases)	2,136	7,860

Note: The number of removals refers to cases confirmed as of the end of January of the following year. Criminal perpetrator recruitment information was added to the scope of information handled by the IHC in September 2023.

Chart F-11 Number of reports of illegal information to the police and number removed ^(Note)

Category \ Year	2020	2021	2022	2023	2024
Reports to the police (cases)	3,099	3,795	3,490	2,818	2,898
Removal requests (cases)	2,161	2,206	2,433	1,913	2,186
Removals (cases)	1,787	1,846	2,026	1,645	1,991

Note: The number of cases in which removal was confirmed five business days after a request for removal was made to a service provider or other responsible party.

2 Elimination of illegal and harmful job recruitment

Prefectural police and prefectural labor bureaus identify and share information on illegal and harmful job postings on social media, job sites, and other channels that appear to be legitimate job offers but actually recruit criminal perpetrators to carry out communications fraud, including “ukeko” and “withdrawers.” Recognizing that the dissemination of criminal perpetrator recruitment information and similar content constitutes illegal conduct under the Employment Security Act, including the “recruitment of workers” for the “purpose of having them engage in work harmful to public morals,” the police are implementing crackdowns on this type of crime.

CASE

In October 2024, a 28-year-old senior member of an organization affiliated with the Dojin-kai (yakuza syndicate) and others posted job recruitment information on social media with descriptions such as “Looking for people who want a one-week, high-income job.” The suspects used highly anonymous means of communication to encourage applicants to work as “ukeko” and other roles in communications fraud schemes, thereby engaging in illegal job placement and worker recruitment intended to involve them in work harmful to public morals. By November of the same year, four suspects, including the man, had been arrested on suspicion of violating the Employment Security Act (recruitment of workers for harmful work). (Kumamoto Prefectural Police)

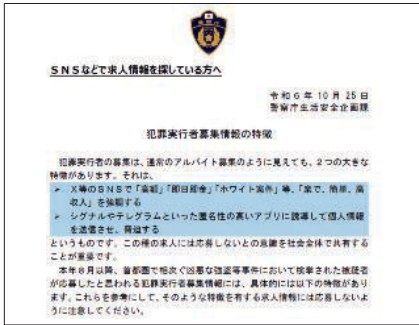
3 Promotion of public information and awareness-raising activities to prevent involvement in crime

In responding to crimes committed through methods that recruit criminal perpetrators via social media, it is important not only to implement crackdowns, including the arrest of ringleaders and criminal perpetrators, but to conduct public information and awareness-raising activities to prevent individuals from becoming involved in crime and to discourage those who have responded to recruitment offers from committing criminal acts.

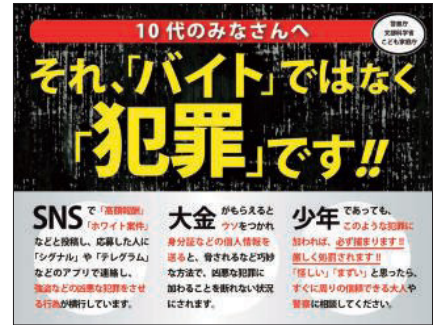
Following a series of robberies and similar cases that occurred mainly in the Kanto region from August 2024 and involved the recruitment of criminal perpetrators via social media, the police have implemented effective measures by making the most of various opportunities to reach individuals who attempt to become involved in crime or who attempt to apply to such job postings.

As part of these efforts, the National Police Agency has prepared and released public information materials to raise awareness of the characteristics of criminal perpetrator recruitment information. Such information typically emphasizes phrases such as “high pay,” “paid on the spot,” and “job with good conditions,” suggesting that the work is “easy,” “simple,” and “high-paying,” and often directs individuals to use highly anonymous messaging apps and induces them to send their personal information. The materials summarize common wording used in the recruitment of criminal perpetrators from a series of robberies and similar cases, as well as examples of consultations received by the police concerning criminal perpetrator recruitment.

To prevent minors from naively responding to criminal perpetrator recruitment postings without fully recognizing the seriousness of the situation and subsequently being threatened with harm to themselves or their families and thereby being coerced into committing serious crimes, the police have prepared and released public information materials in cooperation with relevant organizations. These materials warn of the dangers of criminal perpetrator recruitment information and encourage minors to consult trusted adults or the police.



Public information and awareness-raising materials summarizing the characteristics of criminal perpetrator recruitment information and examples of related consultations



Public information and awareness-raising materials

In addition, the police have implemented targeted online advertising to convey the dangers of criminal perpetrator recruitment information to individuals who have expressed strong interest in high-paying part-time jobs online, based on their online activity. The police are also working to raise awareness among young people by using advertising trucks in busy entertainment districts and other areas where many such people gather in Tokyo, Saitama, Chiba, and Kanagawa prefectures, urging them not to respond to criminal perpetrator recruitment postings.



Public awareness messaging using an advertising truck

MEMO

Calls by the National Police Agency using social media, etc.

Among the individuals who respond to criminal perpetrator recruitment information and attempt to become involved in crime, some do so because they are being threatened with harm to themselves or their families. When consultations are received from such individuals, it is necessary to respond appropriately according to the circumstances, including by taking protective measures. Through social media and video-sharing platforms, the National Police Agency has called on individuals who may become involved in crime to consult with the police on two occasions, announcing, "If you come to the police for advice, you will definitely be protected." Since initiating these calls, the police have provided protection to those who sought advice and their family members in connection with 345 consultations as of the end of April 2025.



Message by a senior official of the National Police Agency

MEMO

Government-wide public information efforts (including messages from the Prime Minister)

Public information and awareness-raising activities concerning criminal perpetrator recruitment information are being carried out not only by the police but by the government as a whole.

In October 2024, the Prime Minister, Shigeru Ishiba, disseminated messages via social media and other platforms stating that working a “shady part-time job” constitutes a crime and that the police will ensure the safety of those who seek consultation.

The government also released videos introducing the realities and dangers of “shady part-time jobs” and implemented advertising on social media. These initiatives raised awareness that individuals who respond to criminal perpetrator recruitment information may be exploited and discarded by criminal organizations, and that they risk being arrested if they become involved in serious crimes.



Message from Prime Minister Shigeru Ishiba



Government online public information: “The truth about ‘shady part-time jobs’— recruitment of criminal perpetrators promising high pay on social media” #SNS #crime-executor



Government online public information: “There’s no such job—it’s not a part-time job, it’s a crime.”

1 Initiatives of the Digital Analysis Division

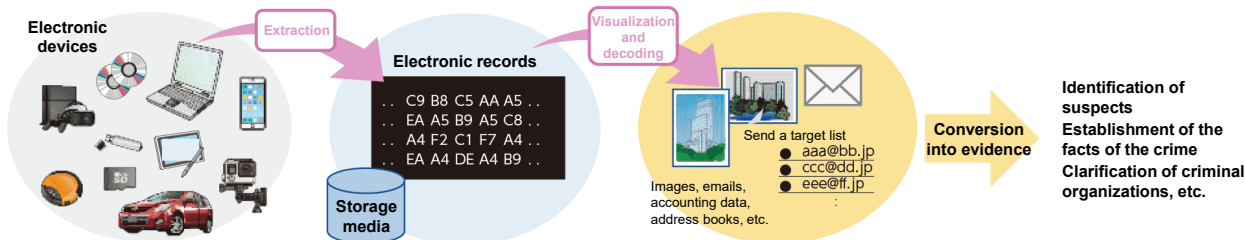
(1) The importance of digital analysis

As services utilizing electronic devices (such as computers and smartphones) and networks (such as social media) have become widespread and increasingly diverse—and as these are being exploited for a wide range of crimes—the importance of analyzing electronic records stored on electronic devices and network communications has grown ever more critical to support police investigations.

① Use of digital forensics (Note 1) in criminal investigations

Electronic records stored on electronic devices that were exploited for criminal activities may, in some cases, serve as important objective evidence in criminal investigations. To use information stored on electronic devices as evidence, it is necessary to extract electronic records from such devices and analyze the records by converting them into forms recognizable to humans, such as text and images. However, because electronic records can easily be deleted or altered, it is essential that they be analyzed and converted into evidence through procedures appropriate for criminal investigations. Therefore, the police provide technical support using digital forensics to criminal investigations conducted by prefectural police via the Digital Analysis Divisions of the National Police Agency Analysis Divisions of the National Police Agency and Info-Communications Departments (Note 2) nationwide.

Chart F-12 Overview of digital forensics



CASE

From August to September 2024, the Digital Analysis Division of the Info-Communications Department of the Kinki Regional Police Bureau analyzed a large number of smartphones and other devices that required advanced forensic examination. These devices were among approximately 2,400 smartphones and around 60 personal computers seized during simultaneous raids conducted by the Osaka Prefectural Police of multiple locations linked to a group involved in investment fraud carried out via social media. Through collaboration with the Digital Analysis Division of the Kinki Regional Police Bureau as well as dispatch of personnel from the National Police Agency, the Chubu Regional Police Bureau, and the Shikoku Police Branch, among others, a framework was established to analyze the large volume of seized evidence, which enabled rapid analysis of electronic records that required advanced technical expertise and significantly contributed to fully clarifying the facts of the case.



Technical support through analysis of smartphones and other devices

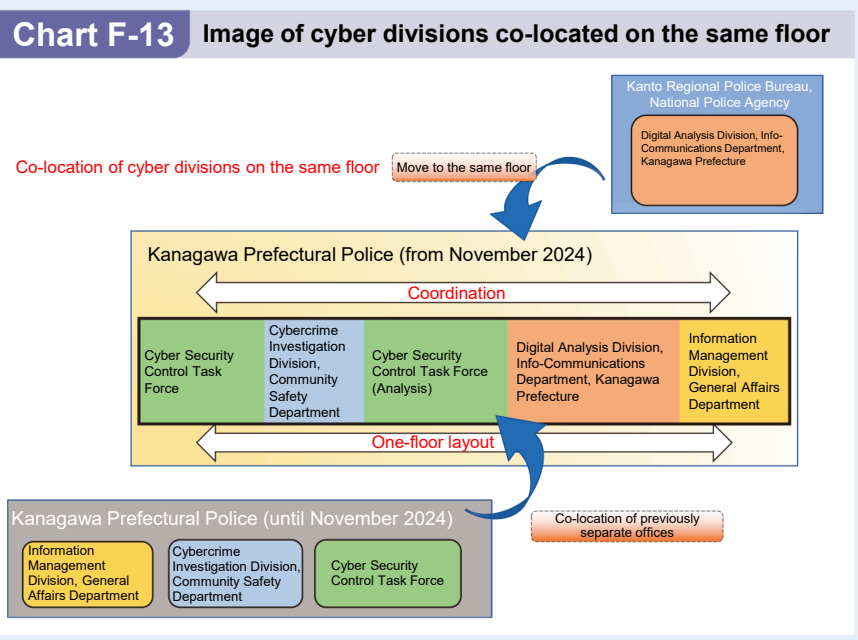
Note 1: Analytical techniques and procedures for analyzing electronic records to establish the facts of a crime

Note 2: Info-Communications Departments of Regional Police Bureaus (including the Info-Communications Department of the Shikoku Police Branch; hereinafter, the same shall apply), the Tokyo Metropolitan Police Info-Communications Department, the Hokkaido Prefectural Police Info-Communications Department, Prefectural Info-Communications Departments (including those within the jurisdiction of the Shikoku Police Branch; hereinafter, the same shall apply), and Area Info-Communications Departments

MEMO

Initiatives for integrated operations of cyber-related divisions

Within the cyber division, the police are working to fundamentally strengthen their overall organizational response capacity by providing support in cases in which the investigative capabilities of other divisions alone are insufficient. From the perspective of effective utilization of human and material resources, the police have co-located the cyber divisions of prefectural police and the nationwide Info-Communications Departments on the same floor as well as consolidated support request contact points for investigations that require advanced and specialized knowledge and technical expertise, thereby promoting further integrated operations among the investigation, support, and digital analysis divisions. For example, in the Kanagawa Prefectural Police, starting from November 2024,



cyber-related divisions (the Cyber Security Control Task Force, the Cybercrime Investigation Division, and the Information Management Division of the Kanagawa Prefectural Police Headquarters as well as the Digital Analysis Division of the Kanagawa Prefecture Info-Communications Department, Kanto Regional Police Bureau) were co-located on the same floor of the headquarters building, and a new operational framework was introduced under which support request contact points were consolidated into a single contact point within the Cyber Security Control Task Force.

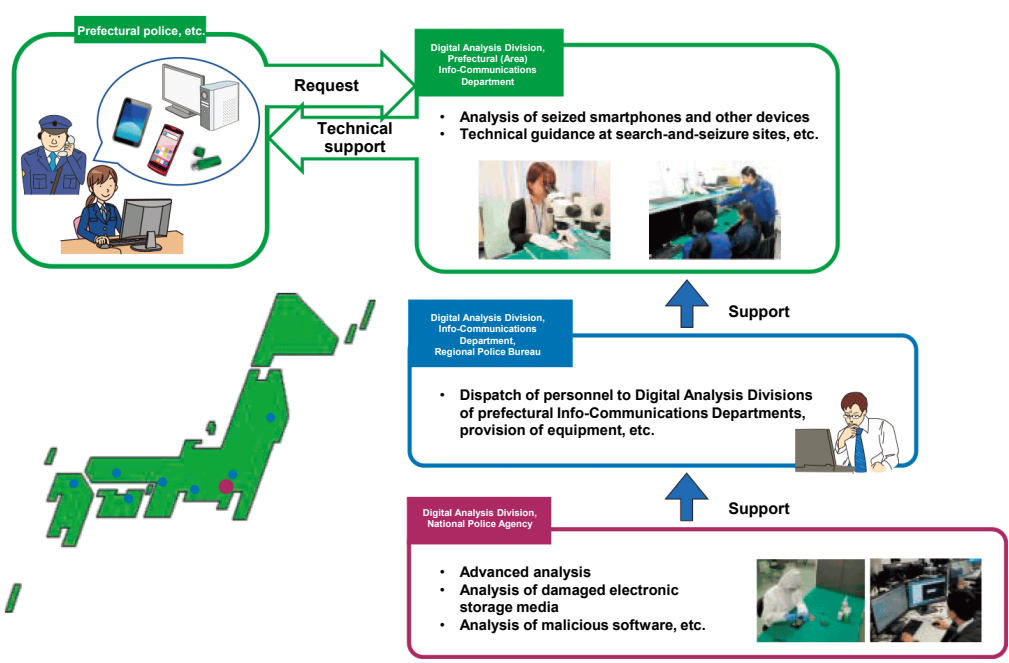
2 Technical support system for crime investigations

The development of an information society has facilitated a wide range of crimes committed via cyberspace, where individuals can act anonymously and activities are difficult to trace. To investigate these kinds of crimes, a high level of technical knowledge is required.

Accordingly, the police have established Digital Analysis Divisions within the National Police Agency and the nationwide Info-Communications Departments. These divisions provide technical support to prefectural police and other relevant bodies through technical guidance on the proper seizure of computers and other devices at search-and-seizure sites, and by conducting analyses to extract evidentiary information from seized smartphones and other such devices.

The Digital Forensic Center of the National Police Agency is staffed with personnel having advanced and specialized technical expertise and is equipped with high-performance analytical equipment. The Center conducts extraction and visualization of information from damaged electronic storage media as well as analysis of malicious software.

Chart F-14 Technical support system for crime investigations



③ Initiatives to enhance analytical capabilities

In recent years, cyber incidents involving the misuse of malicious software have become increasingly frequent, and the growing sophistication and diversification of the associated methods have significantly increased the level of technical expertise required for malicious software analysis. As new electronic devices such as IoT devices and related services become more widely integrated into society, as smartphone apps become increasingly diverse and complex, and as technological development toward the realization of automated driving systems advances, there is a need to enhance analytical capabilities to keep pace with the latest technologies in order to support police investigations.

To this end, the police are promoting the development of analytical methods, enhancement of equipment, development of personnel with advanced analytical technical expertise, and research into cutting-edge information and communications technologies that may be exploited for criminal purposes.

MEMO

Training to enhance analytical capabilities

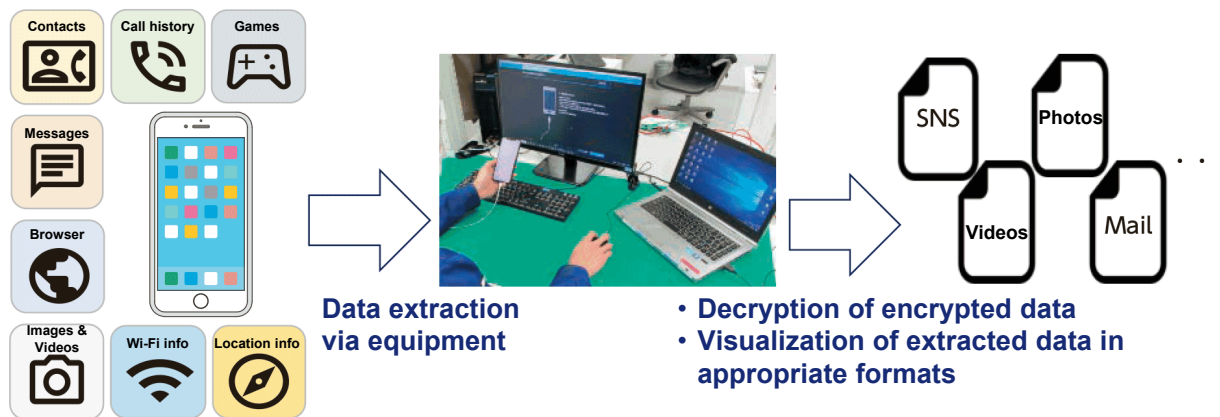
To enhance analytical capabilities in response to the increasingly sophisticated and diverse methods used in cyber incidents and the latest technology, personnel of the National Police Agency with advanced and specialized knowledge and technical expertise provide a range of training programs to personnel of Info-Communications Departments nationwide on analytical methods suitable for the latest technologies. The police also commission private-sector companies possessing advanced technological expertise to provide training programs, thereby working to enhance analytical capabilities across the National Police Agency and Info-Communications Departments nationwide.

(2) Specific initiatives

① Analysis of smartphones

In recent years, smartphones have come to be widely used as mobile devices capable of accessing a wide range of content and applications, and information stored on smartphones that have been exploited in crimes can serve as important objective evidence in criminal investigations. Accordingly, the police conduct analyses of seized smartphones to extract evidentiary information such as communication histories, location data, and photos.

Chart F-15 Overview of analysis of smartphones

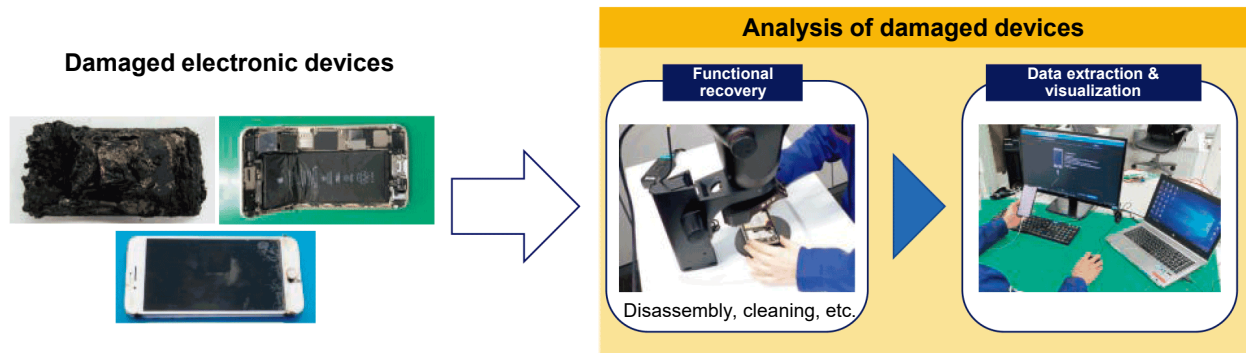


The Digital Forensic Center of the National Police Agency is also working to develop new analytical methods, including techniques for visualizing encrypted message data stored in smartphone messaging applications. These analytical methods are being used to support prefectural police investigations through analyses conducted by Info-Communications Departments nationwide.

② Analysis of damaged electronic devices

Electronic devices such as smartphones that are seized in the course of criminal investigations are often damaged due to deformation, fire, or water immersion. In such cases, the police conduct analyses by attempting to restore the functionality of the damaged electronic devices and to extract and visualize information.

Chart F-16 Overview of analysis of damaged electronic devices



CASE

From April to May 2024, the Digital Forensic Center of the National Police Agency worked on a case of theft in which a 22-year-old unemployed man and others withdrew cash from ATMs using cash cards fraudulently obtained in the names of other individuals. The Center disassembled a smartphone that had been seized in a damaged, non-operational condition and restored it to a state in which data could be extracted. As a result, electronic records obtained from the smartphone were able to corroborate the suspect's criminal conduct, helping to fully clarify the facts of the case.

2

Use of AI Technologies for Detection and Analysis of Illegal and Harmful Information on Social Media

(1) The importance of measures against illegal and harmful information on social media

On the Internet, including on social media, there is a large volume of illegal information, such as content related to child sexual exploitation and advertisements for illicit drugs, and harmful information that is not illegal but that cannot be left unaddressed from the perspective of maintaining public safety and order, as such information may induce crimes or incidents.

In recent years, information posted by anonymous and fluid criminal groups and similar groups that directly and explicitly lures (recruits) criminal perpetrators (criminal perpetrator recruitment information) has proliferated. Applicants have in fact gone on to commit crimes such as robbery and communications fraud, making the spread of such information an increasingly serious threat to public safety.

To ensure safety and security in cyberspace, given the vast volume of information circulating on the Internet, it is necessary to prevent the dissemination and spread of illegal and harmful information by using advanced technologies, including AI.

(2) Use of AI technologies

The police work to identify illegal and harmful information through cyber patrols and other means, and based on such information, carry out enforcement actions and request site administrators and other responsible parties to remove the identified content. The National Police Agency operates the Internet Hotline Center (IHC), which receives reports concerning illegal and harmful information from Internet users and others, reports such information to the police, and requests site administrators and others to remove the content. The Agency also operates the Cyber Patrol Center (CPC), which collects illegal and harmful information on the Internet and reports it to the IHC.

Chart F-17 Implementation of individual warnings using AI



To improve the efficiency of detection and analysis of information on social media, in 2023 the CPC introduced an AI-based search system that automatically collects information closely related to serious crimes (Note 1) and determines its relevance, thereby enhancing the sophistication of cyber patrols.

In addition, in fiscal 2021, the National Police Agency conducted a pilot project that used AI to detect and analyze information related to illicit drugs on social media. Specifically, the Agency trained AI on social media posts that involved advertising of illicit drugs, enabling such posts to be extracted efficiently from social media content.

As a result of the pilot project, which confirmed that posts that involved advertising of illicit drugs could be extracted with a high degree of accuracy, the National Police Agency has developed a system that uses AI to efficiently extract information related to the recruitment of criminal perpetrators on social media. While receiving advice and support from the Digital Agency regarding the advance of AI utilization, the Agency is working to improve the efficiency of issuing prompt individual warnings to the posters of such information using reply functions.

3 Tracking of Crypto-assets by the National Cyber Department

In crimes that exploit social media, criminal proceeds are sometimes concealed in the form of crypto-assets. The National Cyber Department of the Kanto Regional Police Bureau tracks the transfer of crypto-assets used for such crimes; conducts cross-sectoral and comprehensive analyses of the tracking results; and shares the findings with prefectural police. These analyses have discovered links between cases that would not necessarily have been found through conventional investigations, as well as underlying organizational structures and higher-level suspects. Efforts to further undermine the anonymity of such crimes are expected to continue.

The Cyber Affairs Bureau of the National Police Agency is promoting research into tracking technologies and strengthening its tracking capabilities through international cooperation, including inviting personnel from foreign investigative agencies, to address technologies and methods that may hinder the tracking of crypto-asset transfers.

CASE

In response to financial crimes committed by organized crime groups in West Africa, Operation Jackal, an international joint investigation led by ICPO (Note 2), is underway, and the Japanese police have been participating since April 2024.

In investigations into investment/romance fraud via social media that have occurred in Japan, the National Cyber Department of the Kanto Regional Police Bureau conducted cross-cutting analyses of information obtained through investigations by relevant prefectural police, along with tracking of crypto-assets. As a result, the unit identified cases in which funds from multiple incidents were being transferred to crypto-asset accounts under Nigerian names. The information was provided to the Nigerian police, leading to the arrest of suspects in Nigeria. Intermediaries based in Japan were also arrested by the relevant prefectural police.

Note 1: Information that is closely related to serious crimes and poses a high risk of harm to individuals' lives or physical safety. This includes, for example, information that is deemed to directly and explicitly assist in the manufacture of explosive devices, or information that directly and explicitly solicits murder or similar acts.

2: ICPO stands for the International Criminal Police Organization.

While the spread of new technologies and services, including social media, has improved convenience in people's daily lives and socioeconomic activities, it has been observed that these technologies and services are being misused as criminal infrastructure. As described above, offenders have also become increasingly sophisticated in their methods. In order to address crime involving social media, the police need to advance initiatives related to new investigative techniques and to promote the development of cyber personnel. This section outlines the main issues that should be addressed with even greater emphasis.

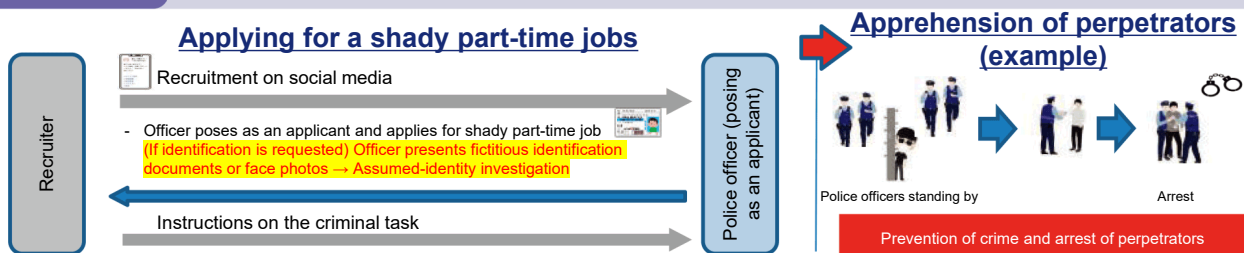
1

Establishment of New Investigative Techniques

① Introduction of "assumed-identity investigation"

In order to appropriately respond to crimes committed by perpetrators recruited via the Internet, including social media, procedures and compliance requirements for investigators properly and effectively conducting an "assumed-identity investigation," which involves the use of documents to establish a fictitious identity, were established in January 2025. This investigative method is applied during a "pose-as-applicant" operation, where investigators use such documents to conceal their real identities to get recruited, with the aim of making arrests and preventing crime. Some prefectural police forces have begun conducting "assumed-identity investigations." The police will use this method to facilitate the early apprehension of the perpetrators and arrest the ringleaders and those giving instructions.

Chart F-18 Overview of "assumed-identity investigation"



② Consideration of introducing investigations using fictitious-name accounts

As criminal groups illegally obtain bank accounts under other people's names and use them to commit crimes, the police will consider new investigative methods that use fictitious-name accounts managed by investigative authorities in order to apprehend higher-level suspects within criminal groups, confiscate criminal proceeds, and deter the misuse of accounts.

③ Investigations and research related to encryption technologies and consideration of introducing new legal frameworks

To dismantle criminal groups, it is important to promptly obtain communications content and subscriber information between suspects on communication applications that are misused for criminal activities, including highly anonymized messaging applications.

The police will consider measures deemed effective for promptly obtaining such communications content, drawing on initiatives in other countries, while also examining technological approaches and the potential introduction of new legal frameworks.

2 Strengthening Frameworks to Promote the Systematic Development of Cyber Personnel

As cyber threats are extremely serious—including the conversion of criminal proceeds into crypto-assets, the use of highly anonymized communication methods, and the recruitment of criminal perpetrators on social media—it is essential to enhance the cyber incident response capabilities of all police personnel. The police will expand cyber education at the National Police Academy and prefectural police academies, and will further strengthen organizational frameworks for the development of cyber personnel within the National Police Agency and prefectural police.

3 Continuous Review of Countermeasures Based on Investigative Activities

Anonymous and fluid criminal groups are exploiting new technologies and services—including social media, highly anonymized communication applications, Internet banking, and crypto-assets—while increasingly complicating and sophisticating their methods. The police will promptly identify changes in criminal methods through investigations and other means, and will strengthen countermeasures by working closely with a wide range of relevant agencies and organizations.

4 Thorough International Investigations and Further Cooperation with Foreign Authorities

Anonymous and fluid criminal groups commit crimes such as communications fraud by recruiting criminal perpetrators on social media and involving them in criminal activities. In some cases, ringleaders or masterminds are located overseas and recruit criminal perpetrators through social media, or have applicants travel abroad to participate in criminal activities. From this perspective, addressing organized fraud and other crimes that cross national borders has become an urgent issue.

When the National Police Agency obtains information on criminal groups operating overseas, it actively exchanges information with the investigative authorities of the countries concerned in order to facilitate detection. In addition, to enable the transfer of suspects and evidence, the Agency is promoting investigative cooperation through ICPO and other channels, as well as international mutual legal assistance using diplomatic channels, treaties and agreements. The police will continue to strengthen cooperation with foreign authorities.

MEMO



Consultations with a senior official of the Royal Thai Police

On April 9, 2025, in order to further strengthen cooperative relations in addressing fraud bases in the border areas between Thailand and Myanmar, a senior official of the Royal Thai Police visited Japan and paid a courtesy call on the Commissioner General of the National Police Agency. During the consultations held with the senior official of the National Police Agency, the two sides exchanged information on organized fraud and efforts to crack down on such crimes in both countries, shared a common recognition of the importance of addressing cross-border organized fraud, and confirmed the need to further strengthen bilateral cooperation and information sharing.



Courtesy call by a senior official of the Royal Thai Police

5 Implementing Effective Public Information and Awareness Activities Based on Current Conditions

The police keep abreast of constantly evolving criminal methods and swiftly and accurately select means of public information and awareness activities to reach individuals who are particularly vulnerable to fraud and other crimes, and put such means into practice in a timely manner to ensure effective crime prevention.

In order to prevent individuals from responding to recruitment information for criminal perpetrators on social media and becoming involved in criminal activities, the police will, after considering factors such as the age groups and regions of the intended audiences, examine effective content, media, and methods for public information and awareness activities, including the cooperation of influential public figures with strong public appeal. The police will also work closely with a wide range of relevant agencies and organizations in implementing these efforts.

The police will accurately grasp crime trends that change significantly in response to social conditions, including crime involving social media, and vigorously promote crime prevention measures to meet public expectations and trust by realizing a “Japan that is the safest country in the world.”