The POLICE WHITE PAPER 2021

[Digest Edition]

Contents

Part 1: Features

Part 2: Topics

Feature 1: 10 Years since the Great East Japan Earthquake (pp. 3–14)

1. Police Activities after the Great East Japan Earthquake

(1) Overview

The Great East Japan Earthquake, with a moment magnitude of 9.0, occurred off the coast of Sanriku at 2:46 p.m. on March 11, 2011, and resulted in 15,900 deaths and 2,525 missing persons identified as of June 10, 2021.

Ever since, the police have dispatched up to approximately 4,800 staff per day, totaling approximately 1,420,000 staff including the Interprefectural Emergency Rescue Units (IERU) from all over Japan to the disaster-hit area. These staff continue to conduct crime prevention in temporary housing neighborhoods, carry out search and rescue for missing persons, and do vigilance and patrol activities in the evacuation zone 10 years after the accident.

Searching for missing persons (Miyagi, 2020)

(2) Police Activities

Police officers dispatched from across the nation have rescued victims, searched for missing people, identified deceased persons, ensured traffic flow, and maintained security of the disaster-affected area together with the local police.

Search operations around the Fukushima Daiichi Nuclear Power Plant

Forensics for identification

Manual traffic control in place of damaged traffic lights

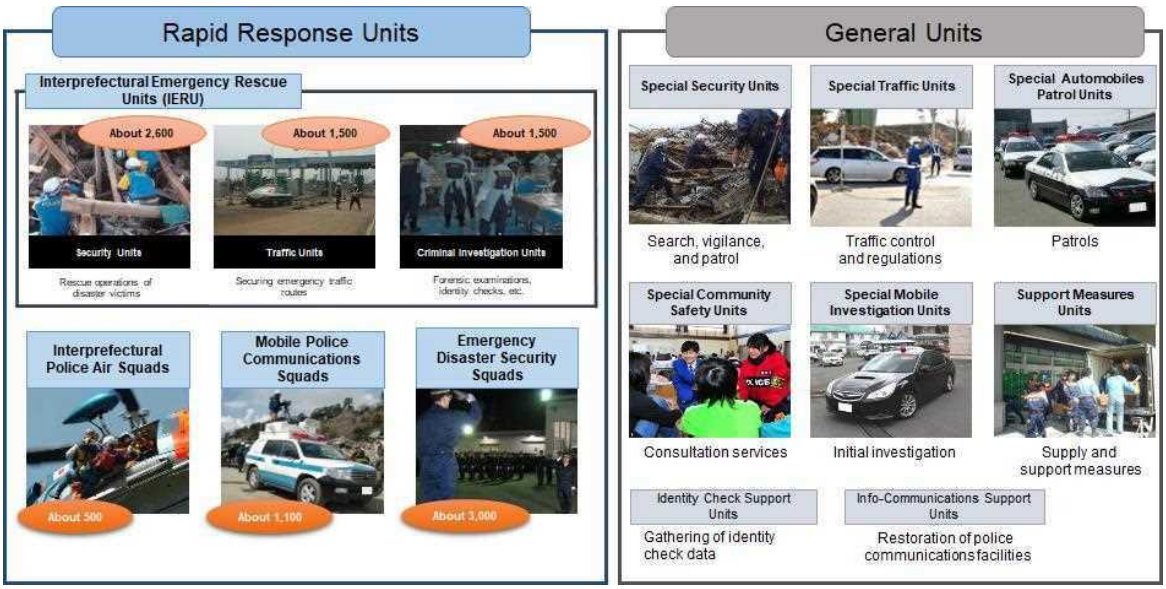
Police officers providing consultations at temporary housings

2. Improving Capacities for Handling Large-Scale Disasters

(1) Quick Response Capacities

○ Organization of units for quick dispatched to affected areas

In May 2012, the size of the Rapid Response Units, which are dispatched from across Japan to the affected areas in cases of large-scale disasters, were expanded to a maximum of ten thousand personnel. In addition, the General Units, which are dispatched to complement the Rapid Response Units in cases of prolonged disasters, and the Disaster Response Units, which consist of both of the above units, were established. Further in March 2017, the Police Team of Rescue Experts (P-REX), which provide an extremely high level of rescue capability, were established in 4 prefectural police forces and are currently operated by approximately 240 personnel from 16 prefectural police forces.



Disaster Response Units

○ Equipment and Training for Rescue Capability Improvement

The police have been working to improve their rescue capabilities to prepare for operations in diverse disaster circumstances, such as in collapsed houses and submerged areas, and by establishing a special training facility for police activities in disaster situations. The police also prepare equipment to protect their officers and ensure effective rescue operations in the case of landslides and floods.

○ Collaboration with Municipal, Private and Professional Sectors for Quick Implementation of Police Activities

Since 2011, each prefectural police and municipality has jointly designated multiple autopsy and morgue facilities in each municipality to prepare for disasters. The police have also signed agreements and conduct joint training with professional associations for physicians, dentists and forensic experts in order that they can be promptly dispatched in cases of disaster.

Joint training with dentists (using a manikin)

(2) Improving Information-gathering Capabilities

As an immediate assessment of the scale of damage is crucial for an appropriate response to large-scale disasters, the police have been enhancing their information-gathering capabilities through performance upgrade of the police aircraft, which are indispensable for disaster response, equipment such as small underwater ROVs and telescopic image searchers for examining hard-to-reach disaster areas, the utilization of ICT, and collaboration with private companies.

○ Early Assessment of the Damage Scale by Police Aircraft

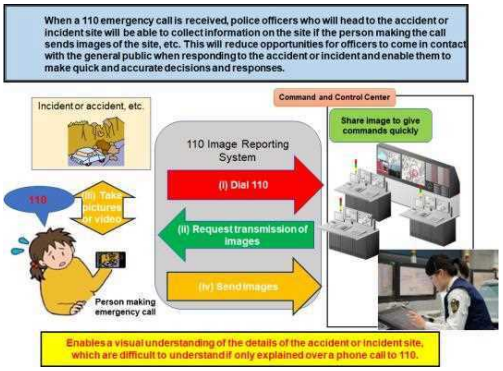
The police have been enhancing their night flight training, while installing one after another night-vision systems to assist the pilots, and portable ultra-high-resolution cameras for the crewmembers in the rear.

Training for a portable high sensitivity camera

○ Utilizing Information Provided by Citizens and Private Companies

The police are working to effectively utilize the information sent by citizens and private companies for rescue operations.

The plan includes the launch of a nationwide system which enables people calling 110 in an emergency to send visual images of disaster areas.



110 Image Reporting System

(3) Securing Disaster-resistant Infrastructures for Police Activities

Learning from the Great East Japan Earthquake, where police activities were hindered by the interruption of lifelines and damage to police facilities, and by 30 police officers being killed in the line of duty by tsunamis, the police have been working to enhance the disaster resistance of their facilities to ensure safety during disaster response.

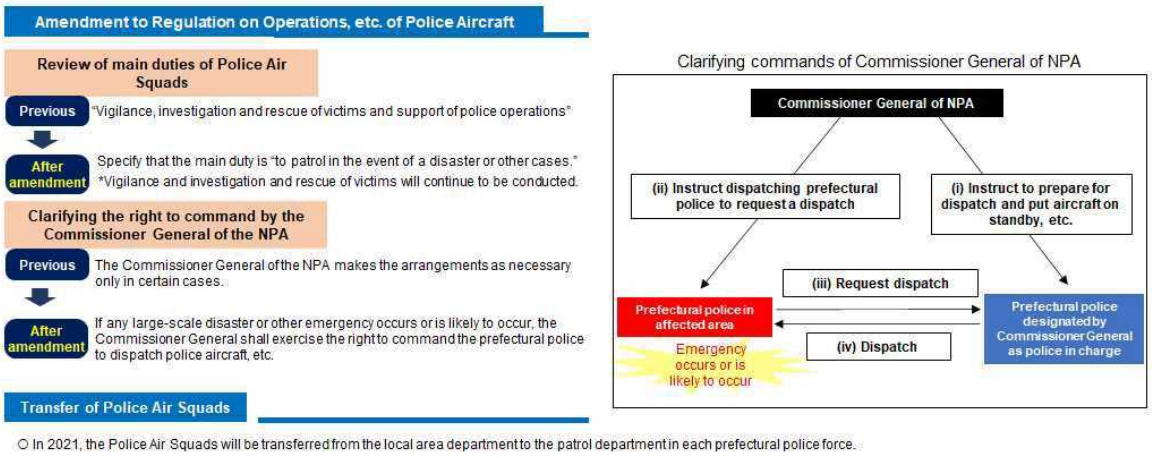
A floor higher than the surrounding streets and office space on the second floor or higher (measures against flooding of the Kanie police station of the Aichi Prefectural Police)

Carrying out rescue boat operations (measures against flooding of the Kanie police station of the Aichi Prefectural Police)

3. Additional Efforts for Managing Large-Scale Disasters in the Future

(1) Improving the Rapid Deployment Capabilities of the Police Nationwide

In order to promptly deploy police forces from all over Japan to disaster areas to enhance efforts for rescue operations, the regulations concerning the operations of police aircraft were amended in February 2021 for the purpose of designating police aircraft as the core element of police mobility during disaster response and utilizing their capabilities to the greatest extent in collaboration with the rescue units led by the mobile police. In addition, the police decided to further promote the enhancement of collaboration with the rescue units and to enhance the disaster response training programs by transferring the air squads of the nationwide police forces to the security departments to integrate the chains of command during disaster response.



Amendments to the Regulations concerning Police Aircraft

(2) Improving Capabilities to Direct and Operate Units by Using ICT and Other Advanced Technologies

The police have been working to direct and operate the units efficiently by fully utilizing ICT and other advanced technologies. These efforts include the installation of the JAXA-developed Disaster Relief Aircraft Management Network System (D-NET) onto police aircraft, which enables command transmissions to be made instantaneously to the aircraft to optimize the task assignment to each unit in cases of disaster.

Training using the D-NET system (provided by JAXA)

(3) Constant Review of the Crisis Management System

The police not only enhance the existing disaster prevention measures, but also constantly review their former efforts based on new knowledge on disasters and their prevention. In addition, the police will further improve their disaster response capabilities through the constant enhancement of inspections and the establishment of a risk management system for disasters to prepare for any large-scale disasters that may occur in the future.

Feature 2: Ensuring Security of Cyberspace (pp. 15–36)

Chapter 1: Threats in Cyberspace

In recent years, threats in cyberspace have become extremely grave with cybercrimes and cyberattacks becoming even more severe and sophisticated.

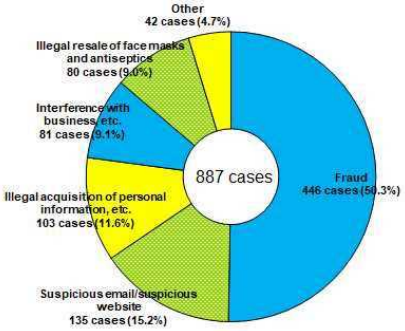
1. Status of Cybercrimes

(1) Types and Number of Cybercrimes in 2020

In 2020, the number of cybercrime cases cleared by the police reached a record high. The number of online banking fraud cases and the amount of loss also remained high. The majority of loss appears to have been caused by visiting phishing sites disguised as the sites of financial institutions. In addition, the police have found cases of illicit transfers via smartphone payment services and cases of the illicit acquisition of application accounts through surrogate SMS authentication.(Note)

(2) Number of Cybercrimes Related to COVID-19

The number of suspected cybercrime cases related to COVID-19 reported by the prefectural police to the National Police Agency (NPA) in 2020 was 887.



Number of reported cybercrime cases potentially related to COVID-19 (2020)

(3) Number of Cleared Cybercrime Cases

The number of cleared violations of the Act on Prohibition of Unauthorized Computer Access in 2020 was 609, which is 207 (25.4%) fewer than in the previous year. The number of cleared crimes targeting computers or electromagnetic records in 2020 was 563, which is 127 (29.1%) more than in the previous year. The number of cleared cybercrime cases has been on the rise, reaching 9,875 in 2020, which is 356 (3.7%) more than in the previous year.

Category \ Year	2019	2020
Total (cases)	787	585
Identification data theft type[Note]	785	576
Acquired from phishing site	1	172
Acquired from users with deceitful words or stolen by peeping	20	115
Acquired by taking advantage of inadequate password setting or management by users	310	99
Acquired from others	182	78
Stolen by former employee or acquaintance, etc., who was able to learn identification data	161	67
Acquired by using spyware or other malware	5	3
Acquired identification data leaked or disclosed on the Internet	3	1
Other	103	41
Security hole attack type	2	9

Note: Act of unlawfully using servers with access restriction by entering identification data of others through a network

Breakdown of types of cleared cases of unauthorized access (2019 and 2020)

Category \ Year	2019	2020
Total (cases)	2,960	2,806
Illegal wire transfer with online banking, etc.	1,808	1,847
Illegal acquisition of information by peeping into emails, etc.	329	234
Illegal purchase with online shopping	376	172
Illegal manipulation of online games or social media	60	81
Providing information by disguising as acquaintance	30	26
Illegal transmission from cryptocurrency exchange service provider, etc.	22	18
Falsification or deletion of websites	19	10
Illegal manipulation of Internet auction	47	6
Other	269	412

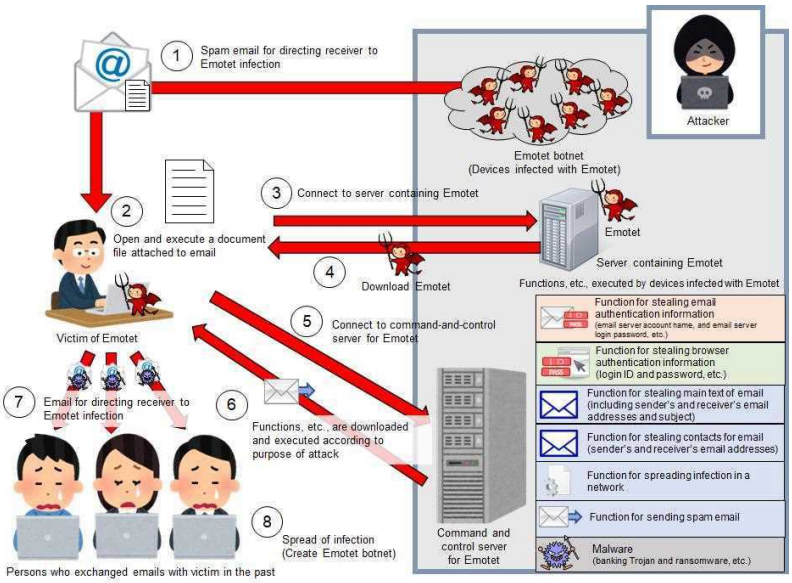
(Number of cases found)

Breakdown of acts committed after unauthorized access (2019 and 2020)

Note: A surrogate SMS authentication is the ability to authenticate a SMS application on behalf of a user.

(4) Number of Online Banking Fraud

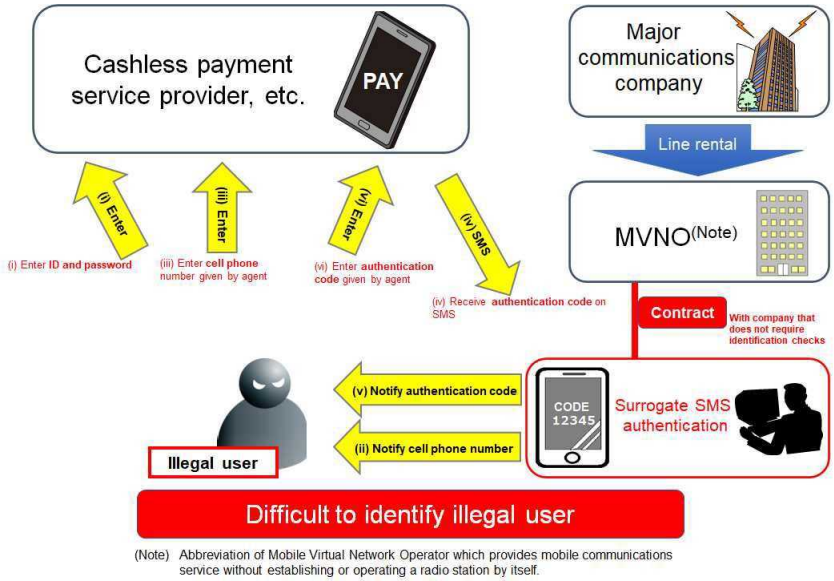
The amount of loss due to online banking fraud decreased substantially in 2020 compared to the previous year; however, the number of cases remained high with only a slight decrease. While the majority of loss appears to have been caused by visiting phishing websites, the police also detected cases where malware called Emotet was suspected to have infected the target computers, which then downloaded another malware to steal the victims' online banking IDs and passwords.



Spreading mechanism of Emotet

(5) Cybercrime Related to Cashless Payment Services

As cashless payments become more popular, the police continue to detect cases exploiting vulnerabilities in identification checks when linking mobile payment services with bank accounts, as well as cases of surrogate SMS authentication where the surrogates abuse the widely used SMS authentication system to provide the illicit acquisition of online banking accounts to third parties.



(Note) Abbreviation of Mobile Virtual Network Operator which provides mobile communications service without establishing or operating a radio station by itself.

Surrogate SMS authentication mechanism

2. Status of Cyberattacks

Cyberattacks including cyberterrorism and cyber espionage are occurring globally and increasing in intensity. In 2020, cyberattacks exploiting vulnerabilities in software and systems, as well as spear phishing email campaigns for infecting devices with malware, were rampant, including some cases that were suspected to be state-sponsored.

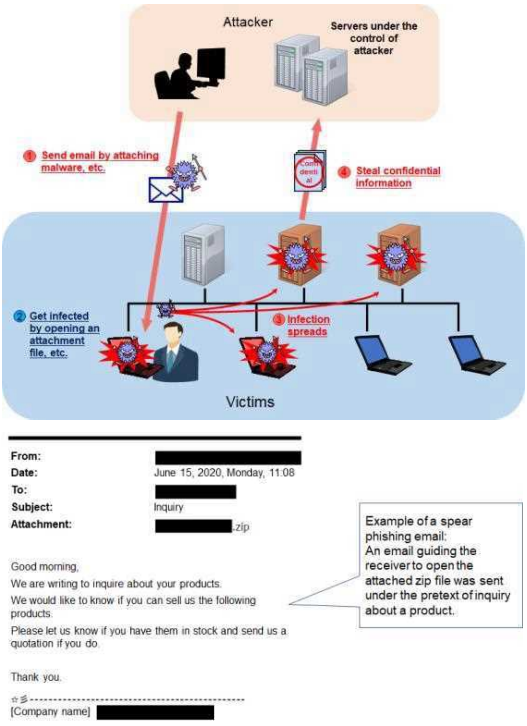
In addition, NPA has detected domestically a number of accesses suspected to be scanning in cyberspace. The number of these accesses has been on the rise, suggesting the spread of potential preparations for cyberattack.

○ COVID-19-related Cyberattacks

The characteristics of COVID-19-related cyberattacks include attacks on medical and research institutions in and outside of Japan.

Spear phishing email campaigns using COVID-19-related disinformation, and the exploitation of vulnerabilities in online meeting systems for teleworking have been detected.

Some companies appear to use systems or devices without sufficient security protection, or their measures against cyberattacks on their internal systems may be delayed because teleworking is hindering their staff members from monitoring their systems.



Data theft mechanism of spear phishing campaigns

[MEMO] Police Attribution Clarified State Involvement in Cyberattacks

A man belonging to the Chinese Communist Party entered into contracts to rent servers in Japan by providing fictious address, name and other information 5 times in total during the period from September 2016 to April 2017. In April 2021, the Public Security Bureau of the Metropolitan Police Department arrested the man for unauthorized creation and provision of electromagnetic records.

During the investigation, the police found that the illicitly rented servers were exploited for a cyberattack or cyberattacks against JAXA, and the same attackers were suspected to have been engaged in other cyberattacks targeting approximately 200 Japanese companies. The police individually alerted each affected company, and concluded that these cyberattacks were launched by a cyberattack group called Tick and it could likely be related to Unit 61419 of the People's Liberation Army of China based in Qingdao, Shandong.

Section 2: Combating Threats in Cyberspace

1. Measures against Cybercrime

○ Unauthorized Access

The police have been working to raise public awareness to prevent unauthorized access in collaboration with associated organizations based on criminal methods analysis.

○ Online Banking Fraud

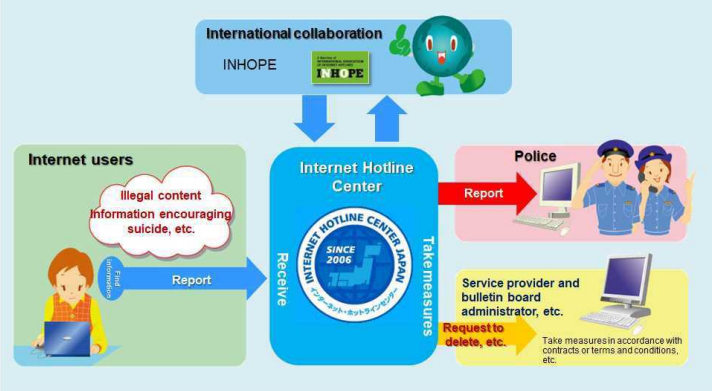
The police have been promoting the prompt investigation of and crackdown on online banking fraud, which have become more sophisticated. In order to prevent illicit transfers via online banking, the police effectively raise awareness and share phishing-site information with anti-virus venders.

○ Cybercrime related to Cashless Payment Services

The NPA, associated with the Financial Service Agency, has published an alert on its website to prevent illegal withdrawals from bank accounts through smartphone payment services. In addition, the NPA has provided the financial sector with information on criminal methods identified through criminal investigations and requested them to reinforce their preventive measures accordingly.

○ Illegal and Harmful Information on the Internet

The NPA operates the Internet Hotline Center (IHC) to receive reports on illegal content and information encouraging suicide and to request the website administrators to delete them. The police promote efficient crackdown on illegal content and cases traceable from harmful content, and take active measures including the arrest of website administrators who do not delete the illegal content without justifiable reasons despite police requests.

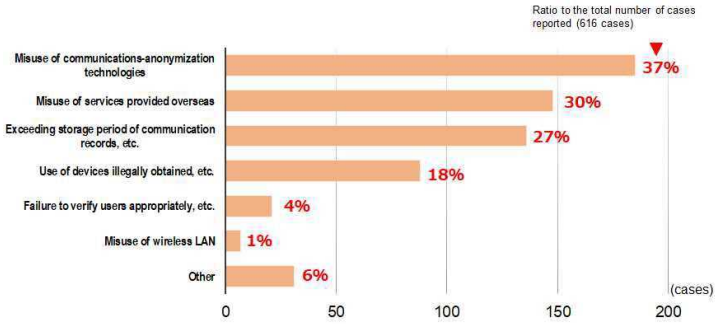


Efforts at the Internet Hotline Center

[MEMO] Issues in Tracking Down Cyber-offenders

The figure on the right shows the major issues in the investigative tracking of cybercrime offenders.

In order to solve these issues, the police request telecommunication companies to appropriately store logs, and to verify and authenticate users according to the Guidelines for Protection of Personal Information in the Telecommunications Business established by the Ministry of Internal Affairs and Communications.



Issues in investigative tracking of cyber-offenders

○ Collaboration with the Japan Cybercrime Control Center

The police share information related to their investigations with the Japan Cybercrime Control Center (JC3) to contribute to improvements in cyber security, while promptly and accurately utilizing the information shared by the JC3 for police activities.

In collaboration with the JC3, the NPA classifies the cybercrime groups by their crime methods and analyzes each group in detail to examine how cybercrimes are committed.

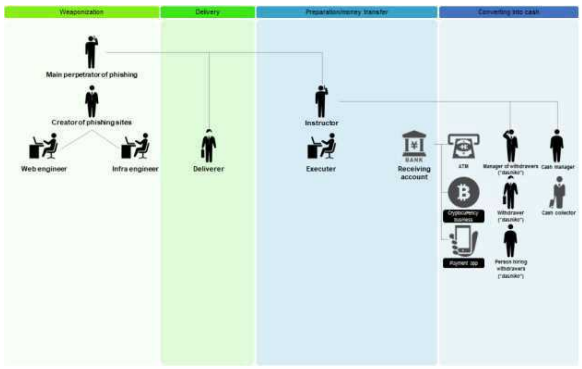
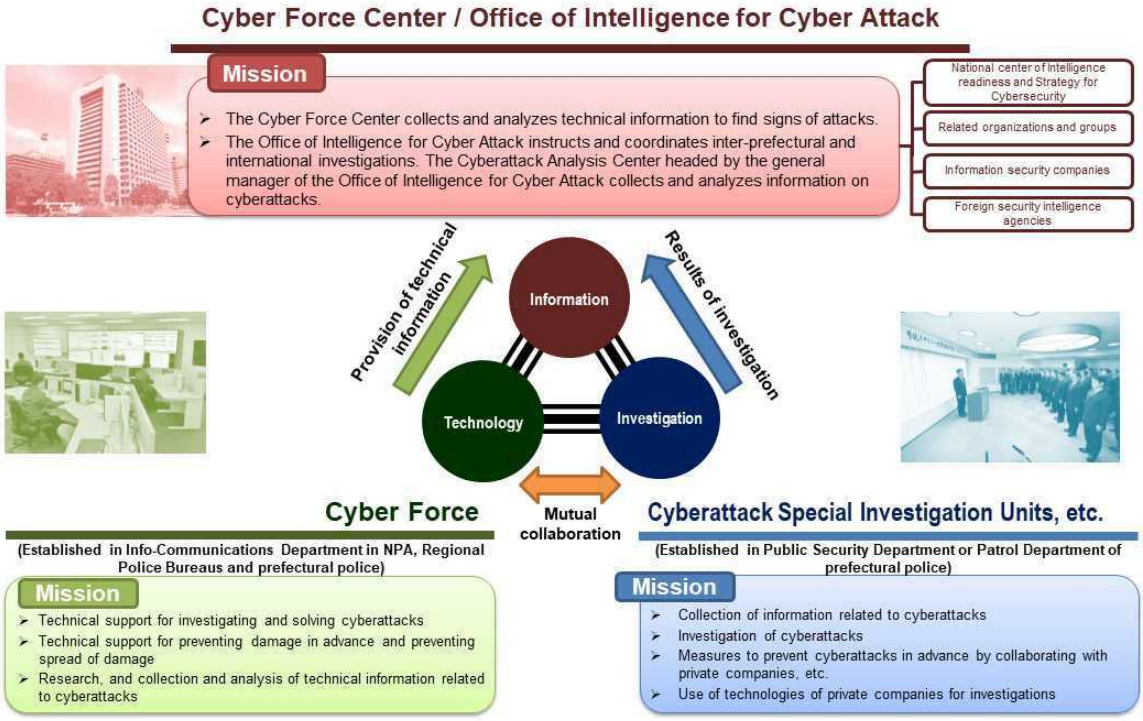


Image of a crime group structure (provided by JC3)

2. Measures against Cyberattacks

The NPA and each prefectural police force have their own unit responsible for measures against cyberattacks, and also examine cyberattacks and take measures to prevent them.



Systematic enhancement for addressing cyberattacks

The police have established Councils for Countermeasures against Cyber Terrorism which consist of each prefectural police force and critical infrastructure operators in all prefectures to share information on cyberthreats and cyber security, as well as hosting lectures by private sector experts and conducting joint exercises in countering cyberattacks. The police also share information with companies that possess advanced technologies and with councils of anti-virus software venders.

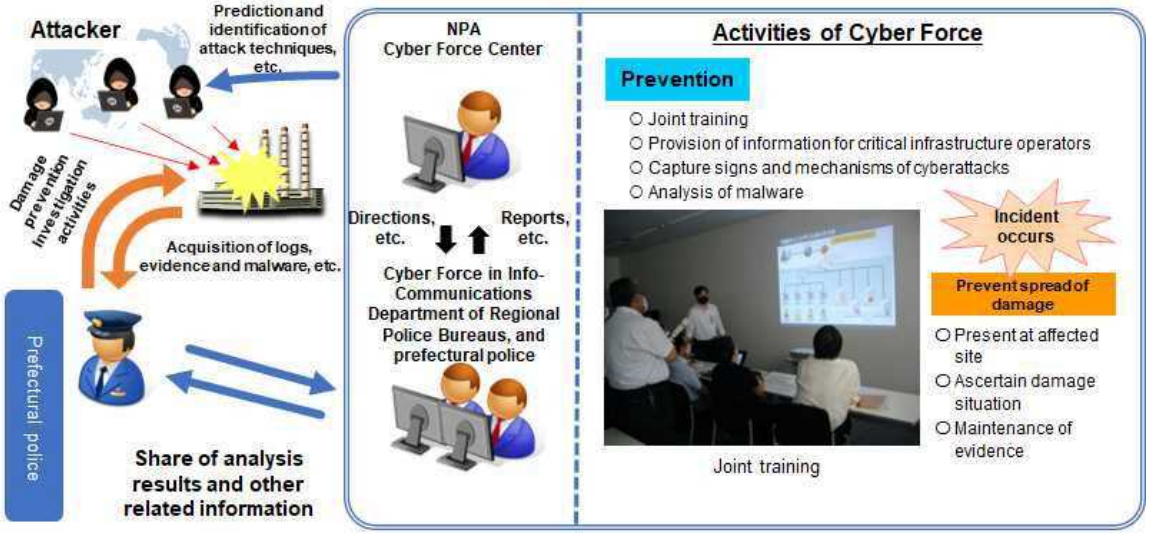
Council for Countermeasures against Cyber Terrorism in Tottori

3. Technical Support and Analytical Skills Improvement

(1) Roles of Cyber Forces for Countermeasures against Cyberattacks

The police have established Cyber Forces in the NPA and in the Info-Communications Departments in all prefectural police forces, which provide technical support for divisions responsible for measures against cyberattacks.

The Cyber Force Center in the NPA serves as the control center that directs Cyber Forces across the country.

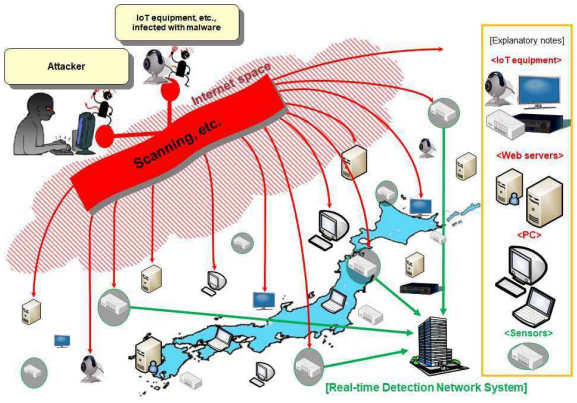


Roles and activities of cyber forces

(2) Capturing the Signs and Mechanisms of Cyberattacks

The Cyber Force Center operates a Real-time Detection Network System around the clock to capture the signs and mechanisms of cyberattacks. The center provides analysis results to critical infrastructure operators and also publicizes the results for open access.

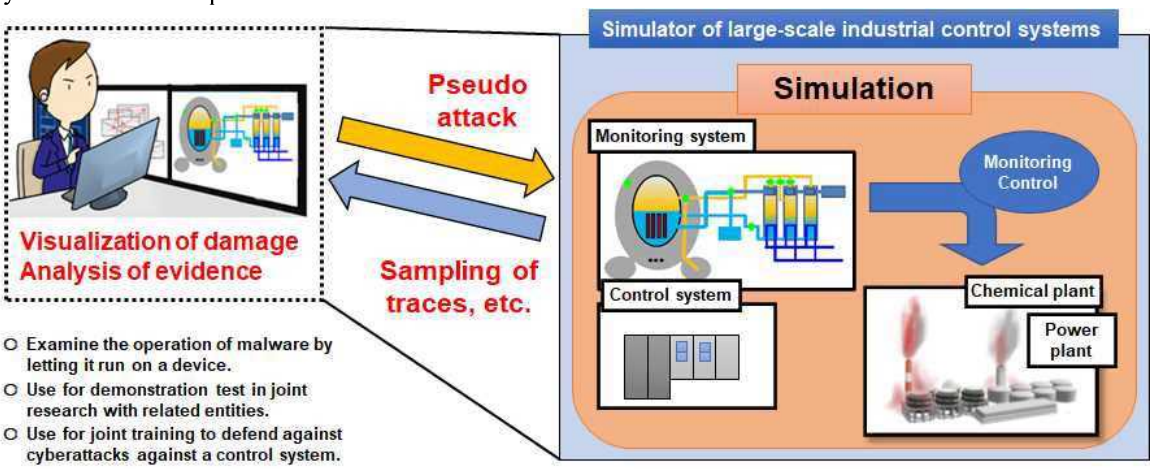
In 2020, the center detected that each sensor of the system received suspicious accesses from all over the world approximately once every 13.3 seconds.



Overview of Real-time Detection Network System

(3) Malware Analysis for Combating Cyberattacks

The Cyber Force Center on operation analyses of malware and development of the analysis measures. The Center has introduced a simulator of large-scale industrial control systems to enhance capabilities to respond to cyberattacks against industrial control systems. The simulator can test whether the systems work without any issues when malware is executed, which enhances the capability to promptly analyze causes of cyberattacks and respond to them.



Utilization of the large-scale industrial control system simulator

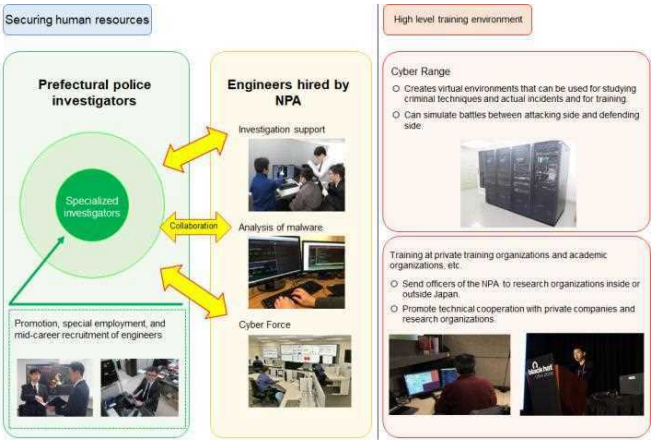
4. Advancing International Cooperation

The NPA responds to transnational cybercrimes and cyberattacks through international cooperation in criminal investigations, such as the Convention on Cybercrime, mutual legal assistance treaties and agreements, INTERPOL, and the G7 24/7 High Tech Crime Network (HTCN) points of contact(Note). The NPA also actively works to exchange information and to establish cooperative relationships in multilateral settings.

5. Advancing Cybersecurity Strategies and Developing Human Resources in Police Forces

The police collectively promote effective measures by building organizational capacity based on the Cyber Security Strategies of the Police.

In order to develop human resources for responding to threats in cyberspace, the police take cross-sectional and systematic measures to employ, promote, educate, train, and build career paths for officers in the cybersecurity sections of the police.



HR development to address threats in cyberspace Principles and Action Plan to Combat High-Tech Crime

Note: The HTCN of contact points was established based on the Principles and Action Plan to Combat High Tech Crime, which had been formulated at the G8 Justice and Home Affairs Ministerial Meeting in December 1997, and is operating in 88 countries and regions as of October 2020.

Section 3: Future Efforts

In recent years, threats in cyberspace have become extremely grave; new forms of cybercrime have been taking place on a daily basis, such as those related to COVID-19 and highly infectious malware, including "Emotet." There are also cases of potential data breaches of confidential data from defense contractors.

As cyberspace has turned into a public space where important social and economic activities are conducted as part of people's daily lives, ensuring the safety and security of cyberspace shall continue to increase its importance and indispensability.

The police have taken measures against threats in cyberspace by cracking down on cybercrimes and cyberattacks, utilizing data forensics capabilities, including malware analysis, and cooperating with foreign law enforcement agencies.

As society becomes more digitalized and the role of cyberspace expands, the police have been expected to play a more significant role than ever in ensuring safety and security in cyberspace as part of their responsibility to ensure safety and security for people in Japan.

Overview of the report from the Cybersecurity Policy Council

The NPA is reviewing the organizational structure of the police in order to enhance their capabilities to tackle cybercrimes and cyberattacks as the Cybersecurity Policy Council underscored the threats in cyberspace, and recommended that the police should take comprehensive cybersecurity measures. The NPA will draw a conclusion by the end of FY2021 to reorganize the police in FY2022.

Special Feature 3: Police Efforts in Combating COVID-19 (pp. 37–42)

1. COVID-19 Response System

In order to cope with the spread of COVID-19, the NPA has established the COVID-19 Task Force headed by its Commissioner General, and works together with associate organizations to respond to the pandemic, based on the Action Plans for Measures against Novel Influenza of the National Public Safety Commission and the National Police Agency (formulated in October 2013, revised in April 2019).

2. Efforts after the Spread of COVID-19

(1) Vigilance and Security at the Points of Entry

In line with the reinforcement of COVID-19-related quarantine, the NPA shares information and cooperates closely with the Ministry of Health, Labour and Welfare and other associate organizations.

Related prefectural police forces have been cooperating for the smooth implementation of quarantine, while conducting vigilance and security activities at points of entry such as airports to prevent problems and prepare for contingencies.

Vigilance activities at airport

(2) Crackdown on Related Crimes and Provision of Crime Prevention Information

Based on the Basic Action Policy on COVID-19, the police work together with associate organizations to obtain information and crackdown on crimes that exploit the pandemic-induced confusion.

(3) Response to Governors' Stay-home Requests

In response to the prefectural governors' stay-home requests, the police have taken the necessary measures such as the reinforcement of patrols in downtown to prevent problems.

(4) Temporary Measures in Police Administrative Procedures

To prevent the spread of COVID-19, the police have introduced temporary measures to extend the driving permission and the renewal period for drivers who may face difficulties in renewing their driving licenses by the expiration date, and to extend the instruction period for those who intend to acquire driving licenses.

(5) Prevention of the Spread of COVID-19

The police require all officers and other staff to wash and sanitize their hands and practice cough etiquette, while improving their working environments by installing clear plastic shields.

Police officer wearing protective equipment to serve residents

3. Enhancement of Usability for Citizens to Meet Social and Economic Changes

○ Streamlining and Advancement of Police Information Management Systems for Enhanced Usability for Citizens

The NPA has been working to streamline and advance the usability of systems by integrating the systems of the NPA and those of the prefectural police forces in order to develop a new synergistic system, which shall enable administrative procedures to be carried out online, while substantially reducing the costs for streamlining the administrative procedures as well as those for developing and maintaining the police information management system.

○ Digital Driving Licenses

The NPA is considering the integration of driving licenses and Individual Number Cards, which will start from the end of FY2024. Due to this integration, the driving license procedures will become convenient for people, providing them with a “one-stop shop” where they can change their address, promptly renew their driving licenses outside of their place of residence, and access online training for the renewal of driving licenses.

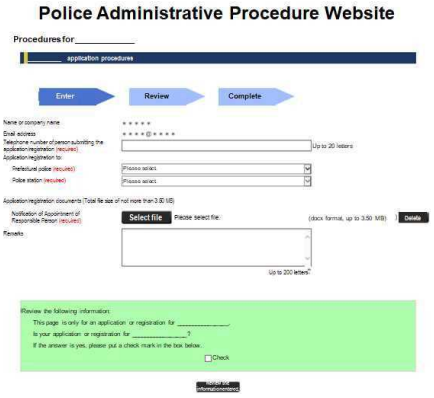
Integration of driving license and Individual Number Card (Example)

Online training (Example)

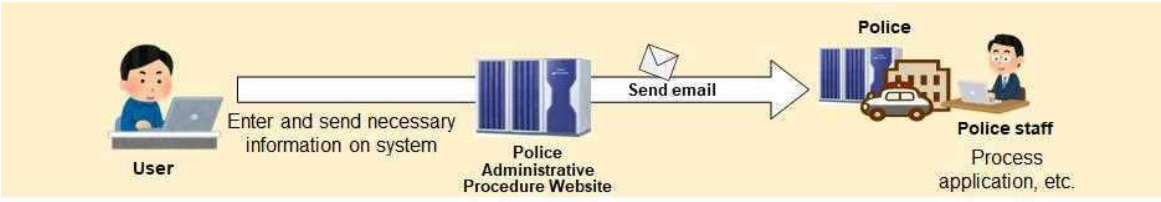
○ Online Administrative Procedures

Since June 2021, the NPA has started the trial operation of the Police Administrative Procedure Website to enable several application procedures to be carried out by email. Many citizens requested that these procedures be put online.

Meanwhile, the NPA is developing a new system which shall enable the completion of more procedures online. In order to develop a system to provide usability to people, the NPA is also reviewing the procedures themselves by eliminating unnecessary attachments.



Input screen of Police Administrative Procedure Site (image)



Application flow for Police Administrative Procedure Website (Example)

Special Feature 4: Police Initiatives to Restrict Crossbows (pp. 43–46)

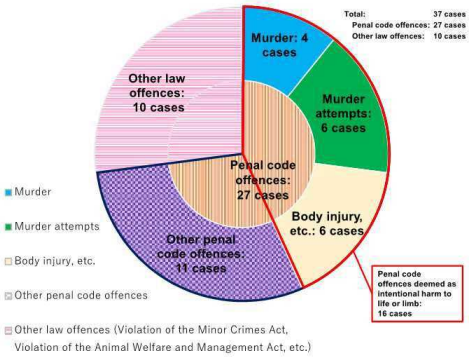
1. Crossbow-related Incidents and Consultations with the Police

(1) Murders

In June 2020, a 23-year-old man used a crossbow to kill and wound 4 people. After this incident, murder attempts using crossbows occurred one after another.

(2) Number of Processed Crossbow-related Cases

The number of cases in which crossbows were used from 2010 to 2020 was 27. Among these, 16 cases, over half of them, were deemed as intentional harm to life or limb, which includes 4 murder cases and 6 murder attempt cases.



Number of cleared cases in which crossbows were used (Total between 2010 and 2020)

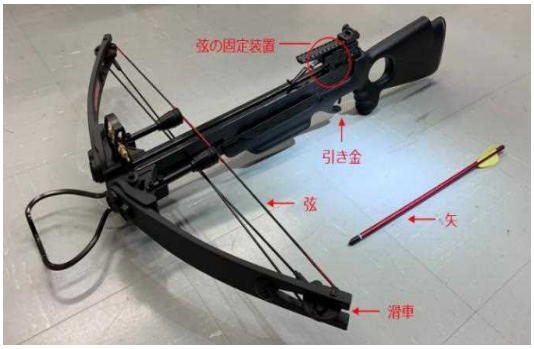
(3) Consultation with the Police on the Usage of Crossbows

The number of cases reported to the police from 2010 to 2020 regarding crossbows was 172. The reports included concerns about crossbow owners, actual harm to private houses, as well as threats and other damage.

2. Overview of Crossbows

(1) What are Crossbows

A crossbow has a device that fixes a string in a drawn position. A user attaches an arrow after fixing a string, and shoots it by pulling a trigger just like a gun. It is used for shooting competitions and other target shooting as a sport, and for tranquilizing wild animals.

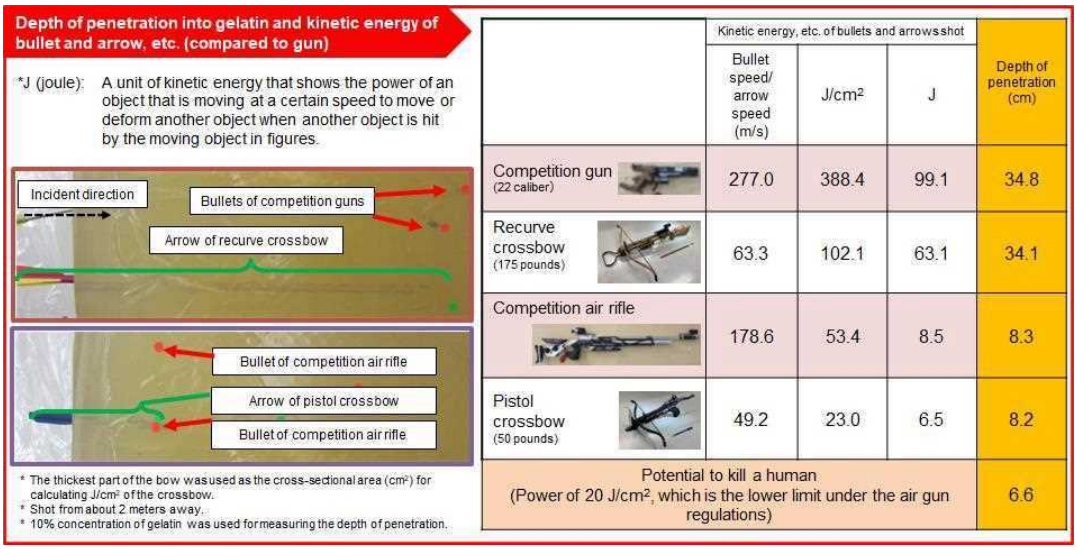


Example of a crossbow (compound crossbow)

Crossbow shooting competition

(2) Testing the Lethal Power of Crossbows

The National Research Institute of Police Science tested the lethality of crossbows and found that they have comparable lethal power to air guns and handguns, which are subject to regulations under the Act for Controlling the Possession of Firearms or Swords and Other Such Weapons.

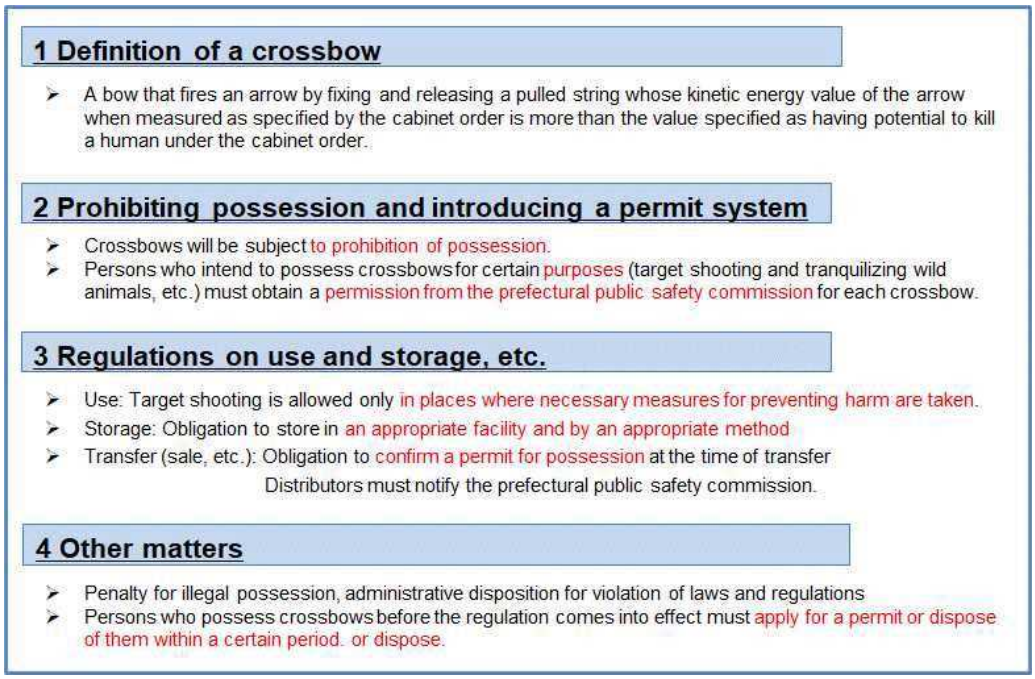


	Kinetic energy, etc. of bullets and arrows shot			Depth of penetration (cm)
	Bullet speed/ arrow speed (m/s)	J/cm²	J	
Competition gun (22 caliber)	277.0	388.4	99.1	34.8
Recurve crossbow (175 pounds)	63.3	102.1	63.1	34.1
Competition air rifle	178.6	53.4	8.5	8.3
Pistol crossbow (50 pounds)	49.2	23.0	6.5	8.2
Potential to kill a human (Power of 20 J/cm², which is the lower limit under the air gun regulations)				6.6

Test of penetration depth into gelatin

(3) Policies Concerning Crossbows Ownership

Taking in account the occurrence of crossbow incidents, the NPA established the Academic Experts Committee on Ownership of Crossbows, and the Committee submitted the Report on Ownership of Crossbows in December 2020. Based on the discussions and the report, a bill for the partial amendment to the Act for Controlling the Possession of Firearms or Swords and Other Such Weapons was passed during the 204th Diet in June 2021.



Amendments to the Act for Controlling the Possession of Firearms or Swords and Other Such Weapons

Topic I: Police Efforts to Combat Organized Communications Fraud (pp. 51–52)

(1) Characteristics of Communications Fraud

Communications fraud groups are led by leading suspects and divided into roles such as perpetrators called *ukeko* (who actually contact victims to receive money from them), and *dashiko* (who withdraw money from ATMs) in addition to collectors and deliverers of the money stolen from the victims. Members in these groups do not disclose their identities to one another in order not to leave traces of communication.

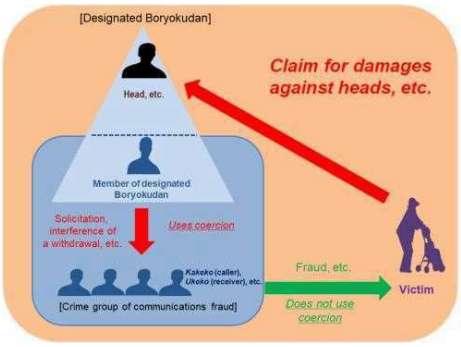
(2) Situation Analysis on Boryokudan's Participation in Fraud and Enhancement of Effective Countermeasures

While the ratio of Boryokudan members among persons arrested for communications fraud has decreased, their occupancy remains higher than those among persons violating the penal code and other laws.

The police are reinforcing cross-sectional countermeasures against Boryokudan members, while proactively analyzing the situation of Boryokudans' participation in communications fraud.

(3) Supporting Lawsuits Claiming Damages against Heads of Designated Boryokudan

As the Anti-Boryokudan Act stipulates that the heads of designated Boryokudan shall be liable to pay damages for any harm to the life, limb or property of others caused by their members' coercive activities to acquire money. The police actively support lawsuits to claim damages against the heads of designated Boryokudan so the victims of communications fraud can recover from the harm they suffered.

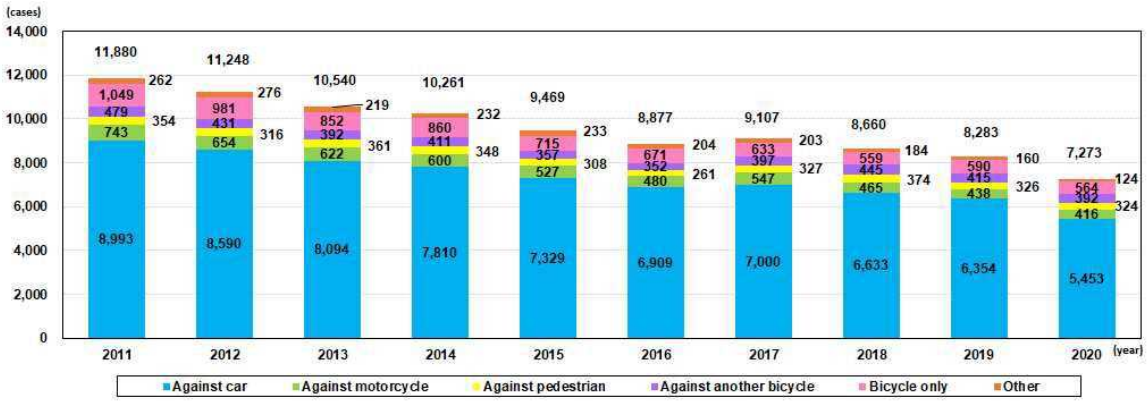


Claiming damages against the heads of designated Boryokudan concerning communications fraud

Topic II: Traffic Rules on Bicycles and Police Efforts in Enforcing the Rules' Effectiveness (pp. 53–54)

(1) The Current Situation of Bicycle Accidents

Although the numbers of deaths and serious injuries in bicycle accidents have been decreasing, approximately 70% of these accidents occurred in 2020 due to violations of laws by bicycle riders.



Trends in numbers of deaths and serious injuries in bicycle accidents by type of the other parties in the accidents (2011–2020)

(2) Traffic Rules on Bicycles and Safety Tips for Bicycle Riders

As the Road Traffic Act categorizes bicycles into a type of vehicle, principally, a bicycle must be ridden on the roadway when a road is divided into a roadway and pedestrian sidewalk. If there are signs or notices indicating that standard bicycles are allowed on sidewalks, bicycles may exceptionally be ridden on the sidewalks slowly.

As a type of vehicle, bicycles must obey the traffic signals, and must stop before a stop line when there is a stop sign.

Sign indicating standard bicycles are allowed on sidewalks

(3) Police Efforts in Enforcing Traffic Rules

The police widely publish traffic rules for bicyclists of all ages, while encouraging them to wear helmets. The police also cooperate with associated organizations to promote bicycle safety education for children, students and elderly people. In addition, the police instruct and give warnings to bicyclists who ignore traffic signals or do not stop at stop signs, while strictly enforcing the traffic rules by arresting bicyclists who commit malicious or dangerous traffic violations.

Ignoring traffic signals	No entry	Entering blocked railroad crossing	Not stopping at stop sign	Brake system malfunction	Drunk	Other	Number of cases of arrest (cases)	Number of cases of warning given (cases)
14,344	236	6,005	1,804	446	119	2,513	25,467	1,437,748

Warnings to and arrests of bicyclists (2020)

Topic III: Mobile Police Communications Squads Enhancing Local Police Operations (pp. 55–56)

(1) Overview of Mobile Police Communications Squads

The Mobile Police Communications Squads have been established in the Info-Communications Departments of police districts across Japan to implement operations for securing communications, which serve as essential foundations for police activities in the field. Specifically, the Squads establish and operate communications in zones with no radio reception or where radio usage is prohibited, and provide real-time video of incident sites in cases of disaster or accidents, for the protection of the Japanese Imperial Family or dignitaries, crowd control at large events or festivals, and for criminal investigations.

Photographing, filming and transmitting images of river flooding by using an unmanned air vehicle image transmission system

(2) Training Programs

Each Mobile Police Communications Squad continually conducts practical joint drills with prefectural police forces, to prepare for all kinds of disasters, accidents, and serious incidents.

Additionally, to respond to the geographic expansion of criminal activities and large scale disasters, the Mobile Police Communications Squad conducts practical joint drills with other squads in different prefectures and with other organizations.

Installing a temporary radio relay station

Topic IV: Police Efforts for Successful Completion of the Tokyo 2020 Olympic and Paralympic Games (pp. 57–58)

(1) Tokyo 2020 Olympic and Paralympic Games

Since the Tokyo 2020 Olympic and Paralympic Games (the Tokyo 2020 Games) were an event that attracted global attention, the police needed to make best efforts in taking all possible measures for the safe and successful completion of the Games, including information gathering and analysis, vigilance and security, as well as ensuring traffic safety.

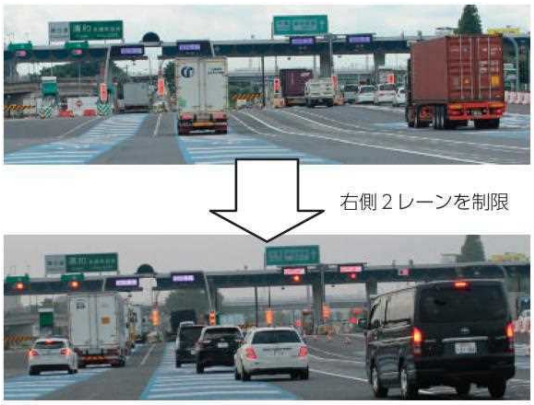
(2) Police Efforts

The police worked to prepare for diverse issues in collaboration with the relevant ministries. The police also conducted joint training with associated organizations and private sectors to reinforce their counterterrorism operations, promoting the collection and analysis of information on cyberattacks and attackers targeting the Tokyo 2020 Games, and conducted joint training to defend against cyberattacks that might have occurred during the period of the event.

Sign indicating standard bicycles are allowed on sidewalks

Joint training to deter cyberattacks

In order to ensure the safe and smooth transportation of people involved in the Games, while maintaining the stability of urban activities, the police took traffic management measures in collaboration with associated organizations, including restrictions on open lanes at highway tollgates.



Test for restriction of open lanes
(Urawa Tollgate, Tohoku Expressway. July 2019)

Test for closing highway entrances
(Sangenjaya Entrance, Metropolitan Expressway. July 2019)