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.

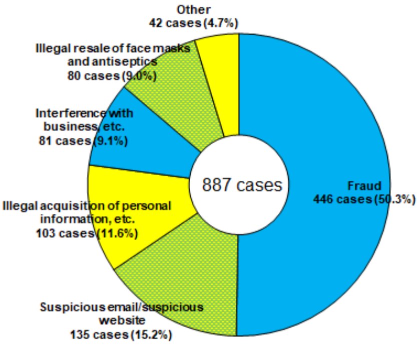
1. Status of Cybercrimes

(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

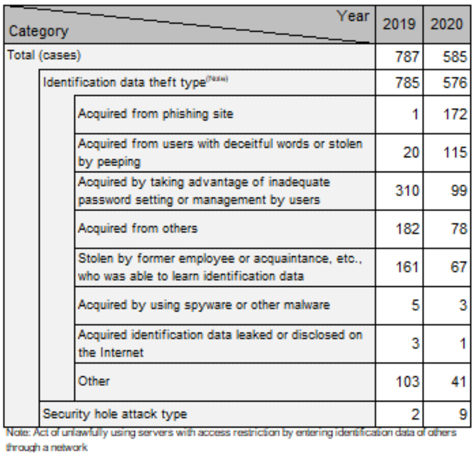
The number of suspected cybercrime cases related to COVID-19 reported by the prefectural police to the National Police Agency (NPA) in 2020 was 887.



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

(3) Number of Cleared Cybercrime Cases

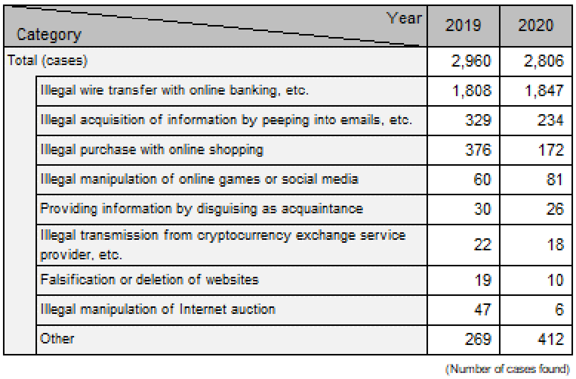
The number of cleared violations of the Act on Prohibition of Unauthorized Computer Access in 2020 was 609, which is 207 (25.4%) fewer than in the previous year. The number of cleared crimes targeting computers or electromagnetic records in 2020 was 563, which is 127 (29.1%) more than in the previous 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.



Year / Category	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)



Year / Category	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

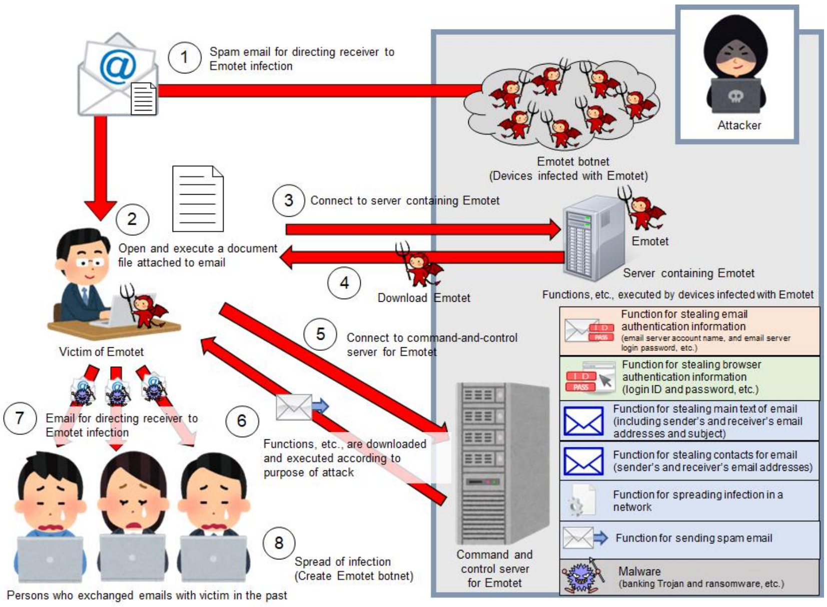
(Number of cases found)

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

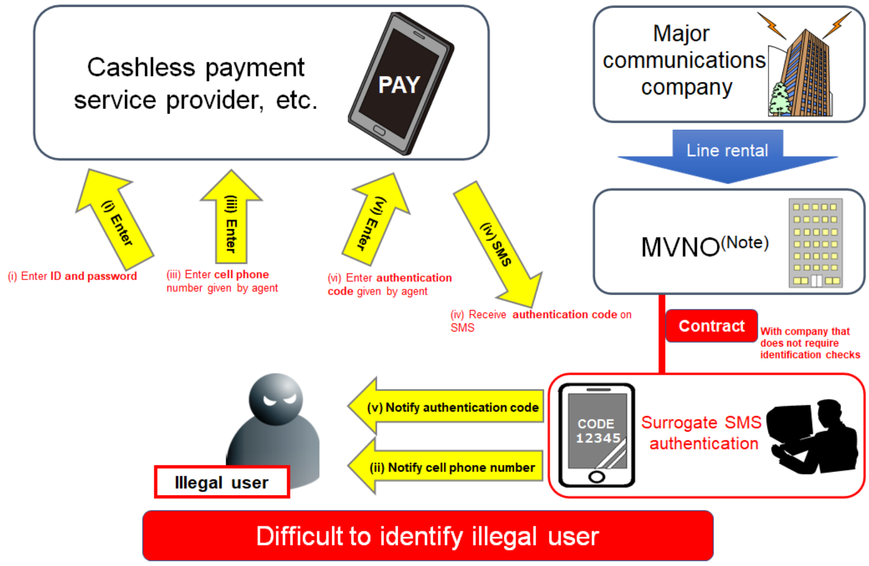
The amount of loss due to online banking fraud decreased substantially in 2020 compared to the previous year; however, the number of cases remained high with only a slight decrease. While the majority of loss appears to have been caused by visiting phishing websites, the police also detected cases where 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.


1 Spam email for directing receiver to Emotet infection
Attacker
Emotet botnet (Devices infected with Emotet)
2 Open and execute a document file attached to email
3 Connect to server containing Emotet
Emotet
Server containing Emotet
4 Download Emotet
Victim of Emotet
5 Connect to command-and-control server for Emotet
Functions, etc., executed by devices infected with Emotet
Function for stealing email authentication information (email server account name, and email server login password, etc.)
I D
PASS
Function for stealing browser authentication information (login ID and password, etc.)
Function for stealing main text of email (including sender's and receiver's email addresses and subject)
Function for stealing contacts for email (sender's and receiver's email addresses)
Function for spreading infection in a network
Function for sending spam email
Malware (banking Trojan and ransomware, etc.)
7 Email for directing receiver to Emotet infection
6 Functions, etc., are downloaded and executed according to purpose of attack
8 Spread of infection (Create Emotet botnet)
Command and control server for Emotet
Persons who exchanged emails with victim in the past

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.


Cashless payment service provider, etc.
PAY
Major communications company
Line rental
MVNO(Note)
(i) Enter
(iii) Enter
(vi) Enter
(iv) SMS
(i) Enter ID and password
(iii) Enter cell phone number given by agent
(vi) Enter authentication code given by agent
(iv) Receive authentication code on SMS
Contract
With company that does not require identification checks
(v) Notify authentication code
(ii) Notify cell phone number
CODE 12345
Surrogate SMS authentication
Illegal user
Difficult to identify illegal user

(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.

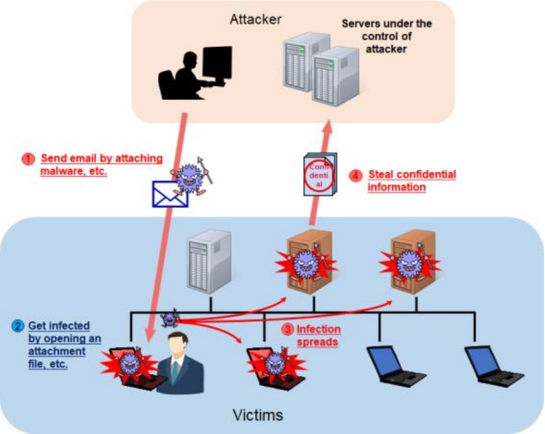
In addition, NPA has detected domestically a number of accesses suspected to be scanning in cyberspace. The number of these accesses has been on the rise, suggesting the spread of potential preparations for cyberattack.

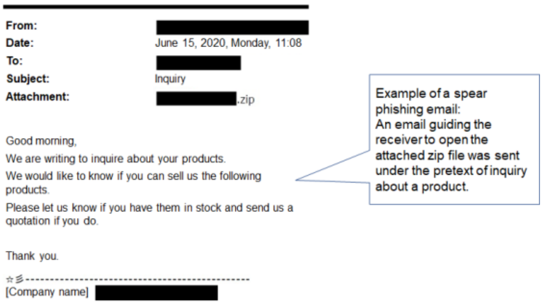
○ COVID-19-related Cyberattacks

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.


Attacker
Servers under the control of attacker
① Send email by attaching malware, etc.
Confidential
④ Steal confidential information
② Get infected by opening an attachment file, etc.
③ Infection spreads
Victims



From: [redacted]
Date: June 15, 2020, Monday, 11:08
To: [redacted]
Subject: Inquiry
Attachment: [redacted].zip

Good morning,

We are writing to inquire about your products.

We would like to know if you can sell us the following products.

Please let us know if you have them in stock and send us a quotation if you do.

Thank you.

☆彡---
[Company name] [redacted]

Example of a spear phishing email:
An email guiding the receiver to open the attached zip file was sent under the pretext of inquiry about a product.

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

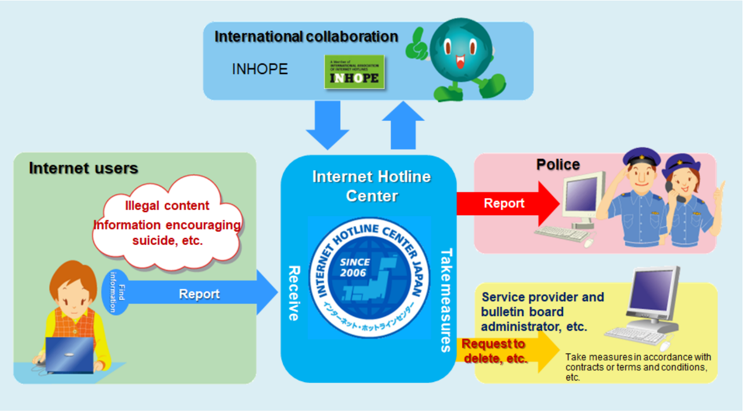
The police have been promoting the prompt investigation of and crackdown on online banking fraud, which have become more sophisticated. In order to prevent illicit transfers via online banking, the police effectively raise awareness and share phishing-site information with anti-virus venders.

○ 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.

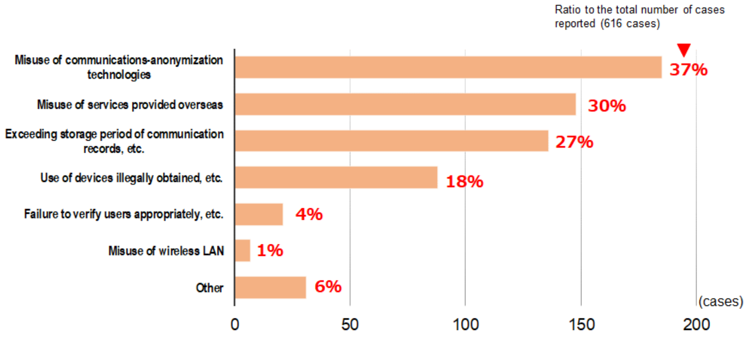

International collaboration
INHOPE
INHOPE
Internet users
Illegal content
Information encouraging suicide, etc.
Find information
Report
Receive
Internet Hotline Center
INTERNET HOTLINE CENTER JAPAN
SINCE 2006
インターネット・ホットラインセンター
Take measures
Police
Report
Service provider and bulletin board administrator, etc.
Request to delete, etc.
Take measures in accordance with contracts or terms and conditions, etc.

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.

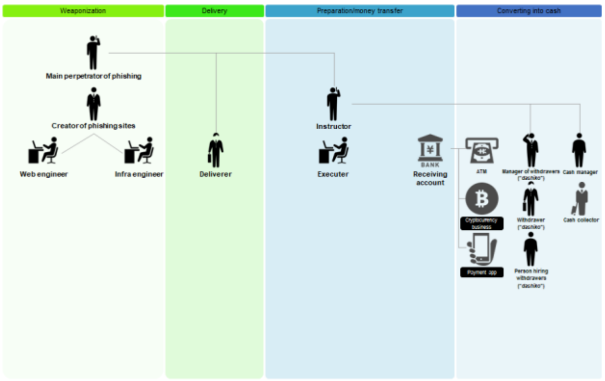
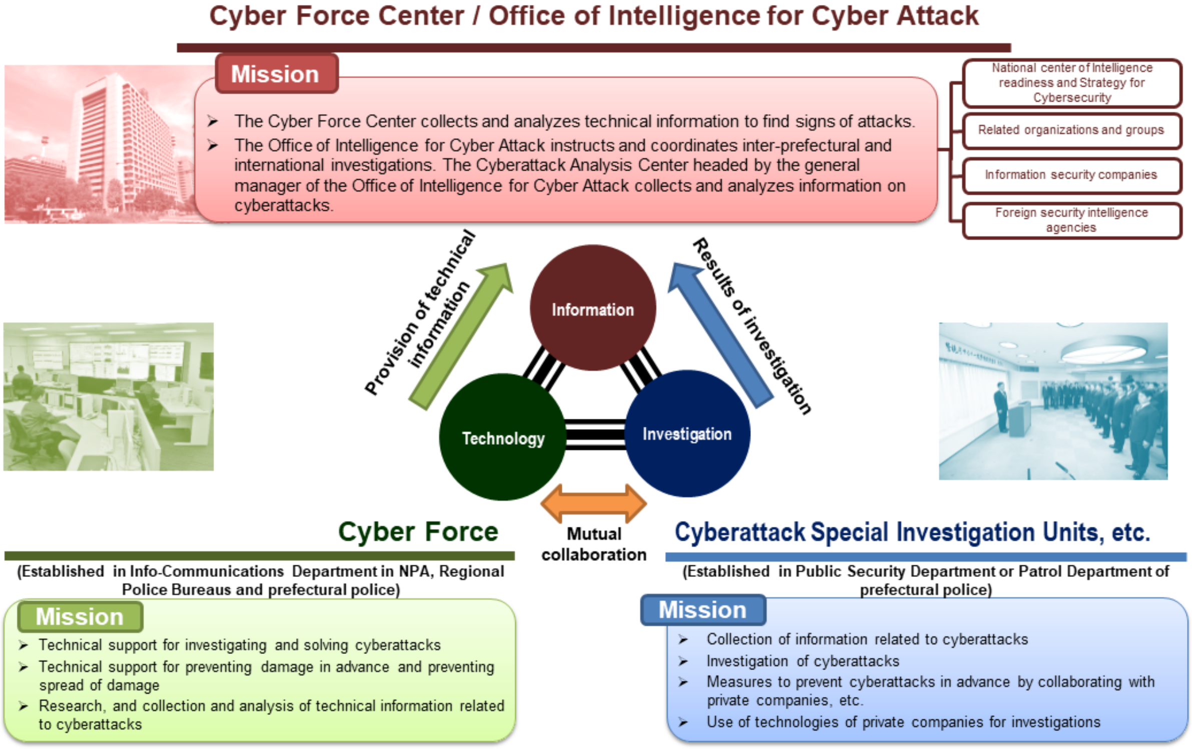


Image of a crime group structure (provided by JC3)

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.



Cyber Force Center / Office of Intelligence for Cyber Attack

Mission

- The Cyber Force Center collects and analyzes technical information to find signs of attacks.
- The Office of Intelligence for Cyber Attack instructs and coordinates inter-prefectural and international investigations. The Cyberattack Analysis Center headed by the general manager of the Office of Intelligence for Cyber Attack collects and analyzes information on cyberattacks.

National center of Intelligence readiness and Strategy for Cybersecurity

Related organizations and groups

Information security companies

Foreign security intelligence agencies

Cyber Force

(Established in Info-Communications Department in NPA, Regional Police Bureaus and prefectural police)

Mission

- Technical support for investigating and solving cyberattacks
- Technical support for preventing damage in advance and preventing spread of damage
- Research, and collection and analysis of technical information related to cyberattacks

Cyberattack Special Investigation Units, etc.

(Established in Public Security Department or Patrol Department of prefectural police)

Mission

- Collection of information related to cyberattacks
- Investigation of cyberattacks
- Measures to prevent cyberattacks in advance by collaborating with private companies, etc.
- Use of technologies of private companies for investigations

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.

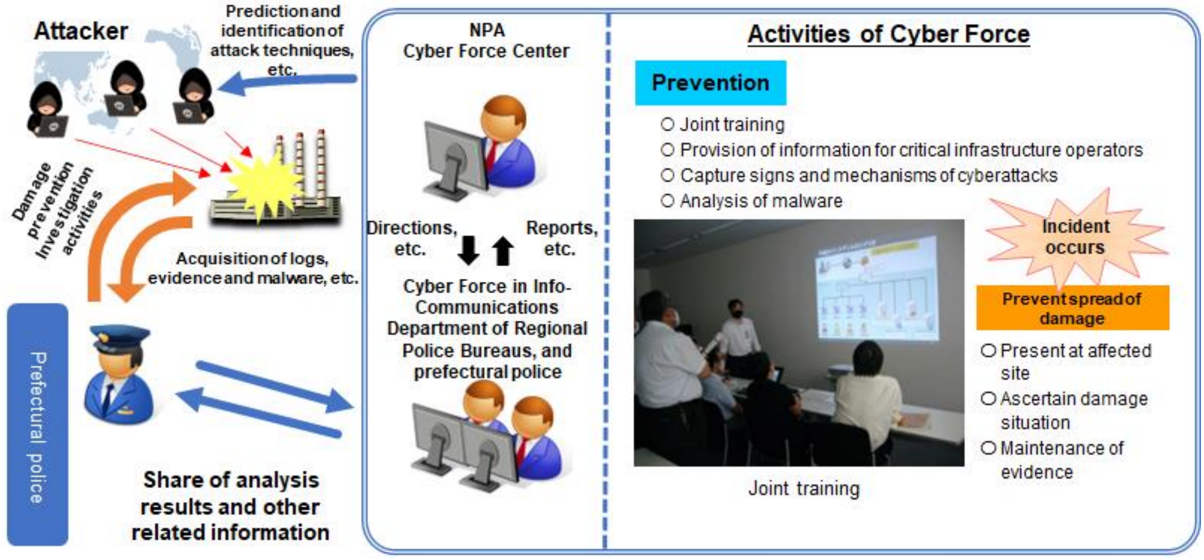
Council for Countermeasures against Cyber Terrorism in Tottori

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.

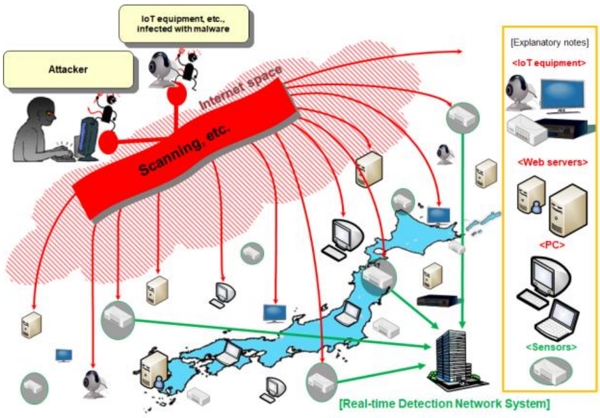

Attacker
Prediction and identification of attack techniques, etc.
Damage prevention Investigation activities
Acquisition of logs, evidence and malware, etc.
Prefectural police
Share of analysis results and other related information
NPA
Cyber Force Center
Directions, etc.
Reports, etc.
Cyber Force in Info-Communications Department of Regional Police Bureaus, and prefectural police
Activities of Cyber Force
Prevention
○ Joint training
○ Provision of information for critical infrastructure operators
○ Capture signs and mechanisms of cyberattacks
○ Analysis of malware
Incident occurs
Prevent spread of damage
○ Present at affected site
○ Ascertain damage situation
○ Maintenance of evidence
Joint training

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.

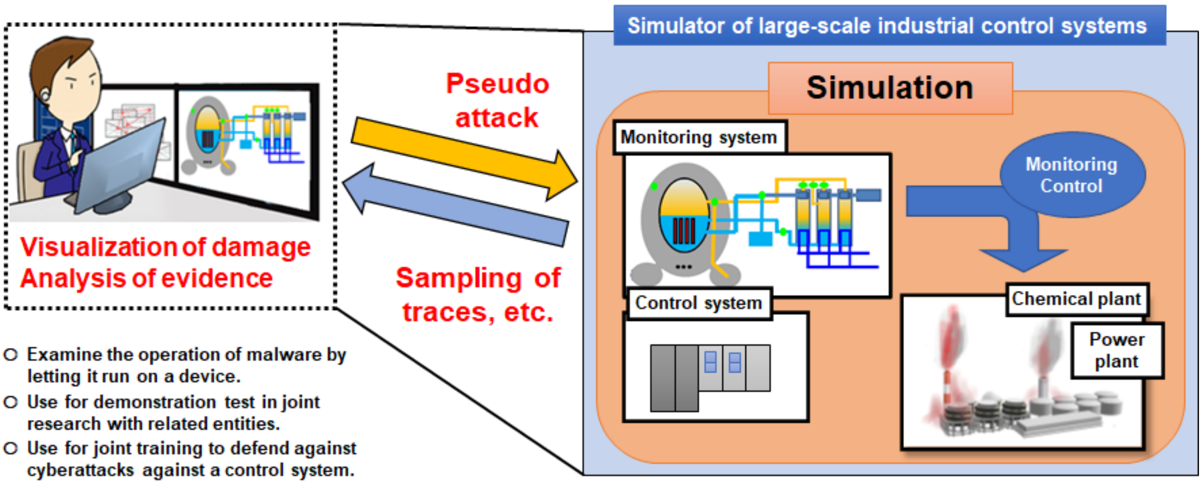
In 2020, the center detected that each sensor of the system received suspicious accesses from all over the world approximately once every 13.3 seconds.



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.



- ○ Examine the operation of malware by letting it run on a device.
- ○ Use for demonstration test in joint research with related entities.
- ○ Use for joint training to defend against cyberattacks against a control system.

Utilization of the large-scale industrial control system simulator

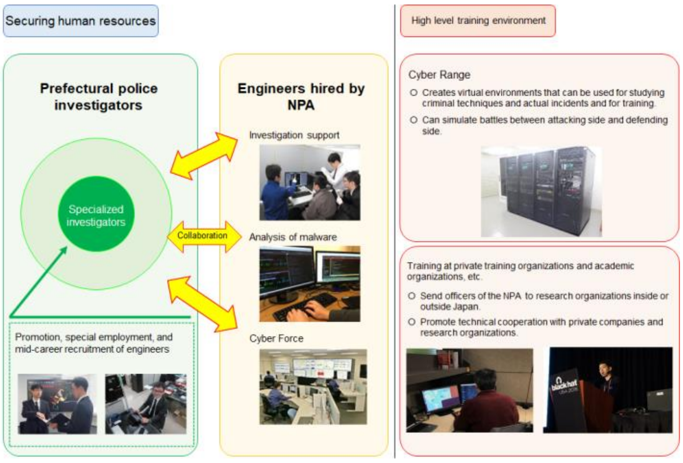
4. Advancing International Cooperation

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.


Securing human resources
High level training environment
Prefectural police investigators
Specialized investigators
Promotion, special employment, and mid-career recruitment of engineers
Engineers hired by NPA
Investigation support
Collaboration
Analysis of malware
Cyber Force
Cyber Range
○ Creates virtual environments that can be used for studying criminal techniques and actual incidents and for training.
○ Can simulate battles between attacking side and defending side.
Training at private training organizations and academic organizations, etc.
○ Send officers of the NPA to research organizations inside or outside Japan.
○ Promote technical cooperation with private companies and research organizations.

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.

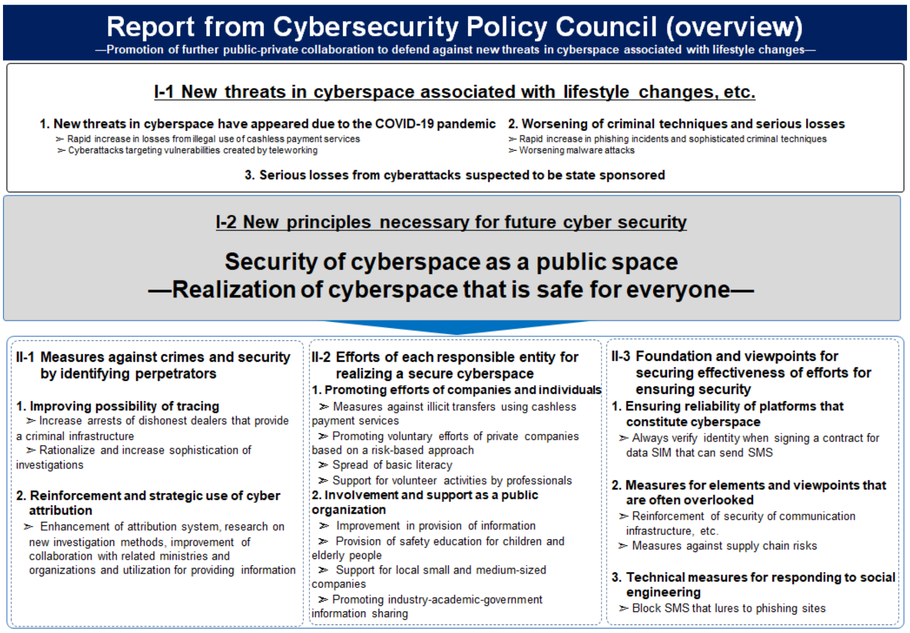
Section 3: Future Efforts

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.



Report from Cybersecurity Policy Council (overview)

—Promotion of further public-private collaboration to defend against new threats in cyberspace associated with lifestyle changes—

I-1 New threats in cyberspace associated with lifestyle changes, etc.

1. New threats in cyberspace have appeared due to the COVID-19 pandemic
- ➢ Rapid increase in losses from illegal use of cashless payment services
- ➢ Cyberattacks targeting vulnerabilities created by teleworking

2. Worsening of criminal techniques and serious losses
- ➢ Rapid increase in phishing incidents and sophisticated criminal techniques
- ➢ Worsening malware attacks

3. Serious losses from cyberattacks suspected to be state sponsored

I-2 New principles necessary for future cyber security

Security of cyberspace as a public space
—Realization of cyberspace that is safe for everyone—

II-1 Measures against crimes and security by identifying perpetrators

1. Improving possibility of tracing
- ➢ Increase arrests of dishonest dealers that provide a criminal infrastructure
- ➢ Rationalize and increase sophistication of investigations

2. Reinforcement and strategic use of cyber attribution
- ➢ Enhancement of attribution system, research on new investigation methods, improvement of collaboration with related ministries and organizations and utilization for providing information

II-2 Efforts of each responsible entity for realizing a secure cyberspace

1. Promoting efforts of companies and individuals
- ➢ Measures against illicit transfers using cashless payment services
- ➢ Promoting voluntary efforts of private companies based on a risk-based approach
- ➢ Spread of basic literacy
- ➢ Support for volunteer activities by professionals

2. Involvement and support as a public organization
- ➢ Improvement in provision of information
- ➢ Provision of safety education for children and elderly people
- ➢ Support for local small and medium-sized companies
- ➢ Promoting industry-academic-government information sharing

II-3 Foundation and viewpoints for securing effectiveness of efforts for ensuring security

1. Ensuring reliability of platforms that constitute cyberspace
- ➢ Always verify identity when signing a contract for data SIM that can send SMS

2. Measures for elements and viewpoints that are often overlooked
- ➢ Reinforcement of security of communication infrastructure, etc.
- ➢ Measures against supply chain risks

3. Technical measures for responding to social engineering
- ➢ Block SMS that lures to phishing sites

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.