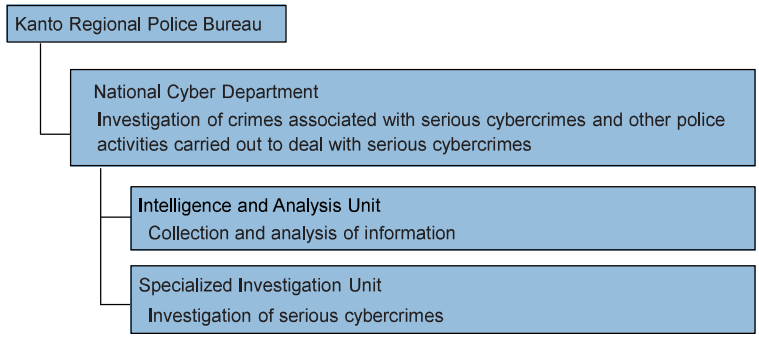
Police Efforts in Response to Serious Cybercrimes

Cyberspace has transformed into a public space where important social and economic activities occur, and it is increasingly fusing with physical space in all respects.
At the same time, however, cyberspace faces extremely serious threats. In particular, once serious cybercrimes (Note) occur, they can cause grave harm—for example, by affecting the social functions that are essential for people's lives, such as logistics and medical care, or threatening the safety of the nation and its people through theft of information from companies that possess advanced technologies.

(1) Establishment of the National Cyber Department

Given such circumstances, the National Cyber Unit was set up within the Kanto Regional Police Bureau in April 2022 as a national investigative organization responsible for investigations of serious cybercrimes, with the goal of enhancing the police's ability to deal with cybercrimes. This unit is made up of personnel with rich knowledge and experience in the field of cyberspace selected from police forces across Japan. These personnel utilize advanced equipment and carry out investigations and fact-finding activities in relation to serious cybercrimes, sometimes through international investigative collaboration.
In April 2024, the unit was reorganized into a new department named the "National Cyber Department," under which specialized units were established. The purpose is to further strengthen the systems for carrying out investigations of serious cybercrimes, collecting and organizing the information required to deal with such offenses, conducting comprehensive and cross-case analysis of such information, and so on.

Chart III-1: Organization of the National Cyber Department within the Kanto Regional Police Bureau



National Cyber Department logo

(2) Procurement and development of human resources for handling serious cybercrimes

The police are enhancing the procurement and development of human resources with advanced knowledge and skills related to cyber offenses—for example, by carrying out mid-career and fixed-term employment of people who have working experience in the private sector, with the goal of becoming better able to deal with a wide variety of challenges associated with cyberspace threats. This is also true of the National Cyber Department, Kanto Regional Police Bureau, in which personnel with diverse backgrounds and qualifications—appointed not only from the National Police Agency but police forces in various parts of Japan—are responding to serious cybercrimes every day.

MEMO Functions of executive police officers appointed through the Public-Private Personnel Exchange Program

Chief Superintendent Yoshitaka Hamaishi, a former employee of a cyber security company, was employed by the National Police Agency in October 2023 through the Public-Private Personnel Exchange Program. As an executive police officer, he has been working for the Cyber Affairs Bureau of the National Police Agency and the National Cyber Department of the Kanto Regional Police Bureau to further sophisticate their information gathering and analysis operations with respect to cyber offenses.

Superintendent Yoshitaka Hamaishi analyzing information

Note: Cases in which serious problems occur or are at risk of occurring to the operations of important information systems of the national government or municipalities or the implementation of business activities by critical infrastructure operators, cases that involve use of advanced techniques etc. (e.g. malware cases) or cases committed by cyber attackers located overseas

(3) Promotion of international cooperation

Serious cybercrimes committed beyond the nation's borders cannot be properly handled without close cooperation with overseas investigative organizations and other relevant parties.

In June 2022, the Cyber Affairs Bureau of the National Police Agency began stationing a liaison officer to engage full-time in measures against cyber offenses at EUROPOL (Note 1) to act as a bridge between Japan and European nations to implement international joint investigations and other activities to strengthen partnerships with overseas investigative organizations, etc. The bureau is also working daily to exchange information with overseas investigative organizations, etc. regarding trends in criminal methods and cybercrime techniques that are used overseas and other related matters.

EUROPOL

The National Cyber Department within the Kanto Regional Police Bureau uses advanced technologies to carry out various types of analyses of evidence collected by prefectural police departments through initial investigations, and it shares the results with overseas investigative organizations, etc., thus striving to deal with serious cybercrimes committed beyond the nation's borders by making use of international networks, including international joint investigations.

CASE

The National Cyber Unit and other related police forces carried out international joint investigations with EUROPOL and other partners regarding LockBit, a cybercriminal group that damages companies, etc. in Japan and other countries by means of ransomware. Consequently, two suspects that were allegedly members of the group were arrested by an involved country's investigative organization in February 2024; the servers, etc. used by the group were taken offline; and "splash pages" were displayed on websites where leaked information, etc. had been published to announce the takedowns.

Splash page

In this case, the National Cyber Unit developed its own original tool to decrypt data encrypted by LockBit, put it into use in the process of recovering from damages caused within Japan, and provided it to EUROPOL in December 2023. In February 2024, the National Police Agency distributed information about this tool in cooperation with EUROPOL and other partners to help companies, etc. around the world recover from the damage, and issued a press release to encourage use of the tool (Note 2).

MEMO

Promotion of fact-finding efforts through investigations into serious cybercrimes, etc.

In dealing with serious cybercrimes, the National Cyber Department has been conducting fact-finding efforts to learn about attackers and their criminal methods by carrying out joint investigations with prefectural police departments and analyzing the results of analyses of malicious programs, etc. and information obtained in the course of criminal investigations in a comprehensive manner. Such information is used not only in initiatives aimed at preventing damage from occurring and spreading but also in public attribution (Note 3). Taking the results of these fact-finding efforts, etc. into consideration, the National Police Agency jointly issued an alert with the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) regarding DDoS attacks on the websites of critical infrastructure operators, etc. in May 2023, and with related organizations in the US regarding cyberattacks by People's Republic of China-sponsored cyber actors known as BlackTech, in September 2023.

Note 1: "EUROPOL" refers to the European Union Agency for Law Enforcement Cooperation. Although it is a law enforcement agency of the European Union (EU), it has no investigative authority. Its main missions include promoting information exchanges among member countries and analyzing collected information.

2: https://www.npa.go.jp/news/release/2024/20240214002.html

3: See page 118 (Chapter 3).