Special Feature I: Countermeasures against Threats in Cyberspace

Section 1: Threats in Cyberspace

The Internet has become entrenched as social infrastructure essential to citizens' lifestyles and economic activities, and cyberspace has now become an integral part of citizens' lives. Within this backdrop, as well as a rush of cybercrimes such as online banking frauds, cyber-attacks such as cyber-terrorism attacks that disable the fundamental systems of government agencies and critical infrastructure companies and paralyze social functions, and cyber-espionage that use info-communications technologies to steal classified information from government agencies or companies with advanced technology, are occurring frequently on a global scale, reflecting the escalating threat levels in cyberspace.

(2) Case

○ Advance-notice crime/virus distribution cases using the Internet

In relation to advance-notice crime/virus distribution cases using the Internet that occurred between June and September 2012, the Kanagawa Prefectural Police, Osaka Prefectural Police, the MPD and Mie Prefectural Police arrested four men on charges of Forcible Obstruction of Business. Subsequent investigations, however, revealed that the computers of the arrested four had been infected by malware that could not be detected by commercially available anti-virus software, allowing a third party to operate their computers remotely, and that the arrested four had no involvement in the cases.

Threats in Cyberspace

1 Status of Cybercrime

(1) Cleared Cybercrime Cases

2012 witnessed the occurrence of criminal incidents such as advance-notice crime/virus distribution cases using the Internet and online banking frauds. The number of cleared cybercrime cases in 2012 was 7,334, an increase of 1,593 cases (27.7%) over the previous year and the highest number of cases recorded to date, representing a roughly 4.6 times increase over ten years since 2002, during which 1,606 cases were cleared.

The relevant four prefectural police reviewed this case, and the NPA issued instructions to all prefectural police forces nationwide regarding preventive measures against recurrence, such as the enhancement of knowledge related to cybercrime investigation and comprehensive evaluation of evidence.

In February 2013, the joint investigation headquarters, comprised of the four relevant prefectural police forces, arrested a suspect on charges of Forcible Obstruction of Business for perpetrating advance-notice crime using the said malware.

Trend in Cleared Cybercrime Cases (2008 – 2012)

Classification \ Year	2008	2009	2010	2011	2012
Total (cases)	6,321	6,690	6,933	5,741	7,334

2 Cyber-attack Status

(1) Modus Operandi of Cyber-attacks

1) Modus Operandi of Cyber-terrorism

Info-communications technologies have permeated modern society, and critical infrastructure essential to our lifestyles, such as electrical power, gas and water supply are also supported by information systems.

The threat of cyber-terrorism, which can cause significant damage to citizens' lifestyles and economic activities by hindering the maintenance of infrastructure functions and provision of services through cyber-attacks on key systems in critical infrastructure, is now a reality. To date, Japan has not experienced any damage due to cyber-terrorism such as social disruption caused by cyber-attacks targeting the key systems of critical infrastructures. However, incidents that have disrupted the functions of financial institution systems or the control systems of nuclear power plants have occurred overseas. Techniques that can be used in cyber-terrorism include DDoS attacks that disable the provision of services from a victim's computer by using multiple computers to overload it with massive data transmissions, and the illegal access of computers and planting of malware that allows the perpetrator to instruct a computer to execute actions not intended by the computer's administrator or user.

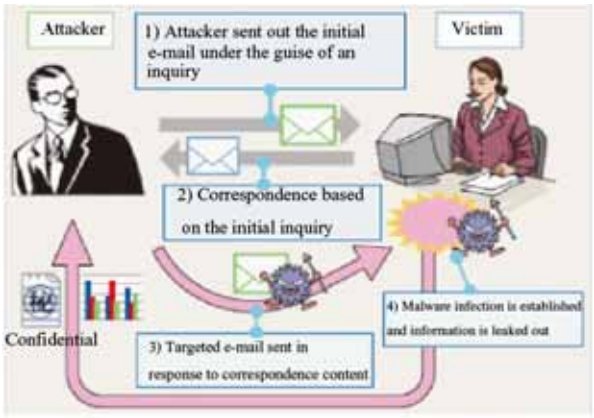
A disabled ATM of a Korean financial institution

2) Modus Operandi of Cyber-espionage

In recent years, with the storage of information as electronic data now commonplace, the threat of cyber-intelligence for the objective of stealing advanced technologies that can be converted to military technologies or classified information on national strategies in diplomatic negotiations, etc. has become a global issue.

Techniques that may be used in cyber-espionage typically include the sending of targeted e-mails, designed to steal information by infecting recipient computers with malware that cannot be detected by commercially available anti-virus software, which masquerade as legitimate business related correspondence.

NPA has confirmed that 1,009 targeted e-mail attacks sent to private sector companies, etc. in Japan during the year 2012. Of these, some employed a subtle approach whereby e-mails under the guise of legitimate inquiry were sent to public e-mail addresses set up for general inquiries, and e-mails with attached malware were later sent after further exchange of e-mail communications.



"Exchange style" targeted e-mail attack

(2) Case

○ Cyber-attack case targeting the Japan Aerospace Exploration Agency (JAXA)

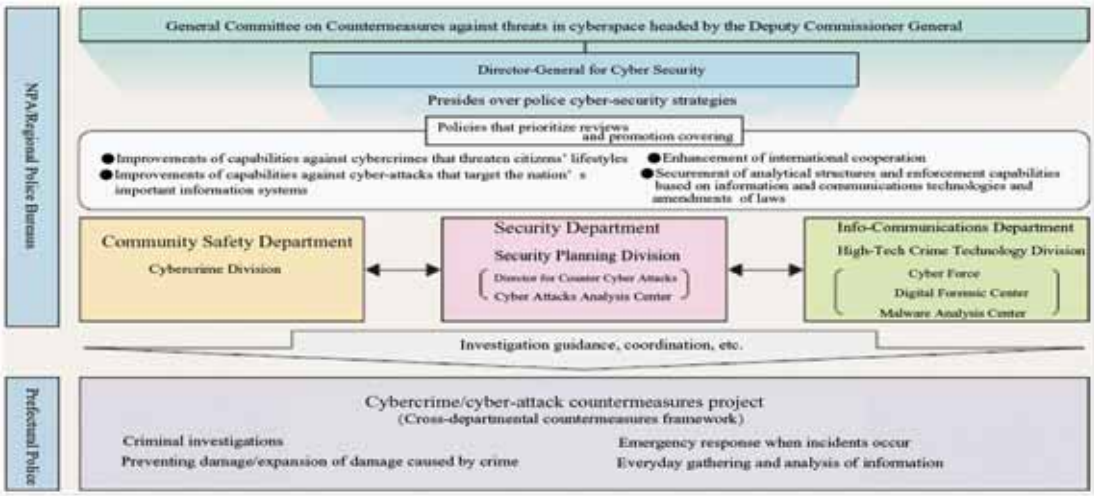
A targeted e-mail attack was launched against the Japan Aerospace Exploration Agency (JAXA) in January 2012. An employee computer was consequently infected with malware and it was revealed that this resulted in the leaking of information in the computer and on-screen information during operations, as well as log-in information, etc. for systems accessed by the infected computer between July and August 2011. Furthermore, in November 2012, another employee computer was infected with malware, revealing the possibility that information on rocket specifications and operations may have been stolen.

Section 2: Measures against Threats in Cyberspace

1 Reinforcing Cyber-security Measures

In July 2012, the NPA established the new position of Director-General of the Commissioner General's Secretariat to preside over cyber-security strategies, with a view towards reinforcing strategic responses spanning all departments in relation to the numerous difficult issues of dealing with threats in cyberspace. Under the Director-General, a cross-organizational structure has been established which undertakes priority reviews and enhancement of policies related to while taking into consideration issues such as the improvement of capabilities against cybercrimes and cyber-attacks, the enhancement of international cooperation based on securing analytical structures and enforcement powers, the upgrading of information and communications technologies and the amendment of laws.

Polices structures promoting cyber-security measures



2Countermeasures against Cybercrimes

An immense amount of information is in circulation on the Internet, and cooperation between the police and private businesses, etc. is essential for measures concerning this information. Consequently, as with other countries, the NPA has entrusted the operation of hotline services to private sector organizations. In addition, for measures against illegal/harmful information, in order to undertake coordinated measures while avoiding overlapping investigations by the related prefectural police forces, enforcement utilizes a nationwide cooperative investigation method.

(1) The Internet Hotline Center Approach, etc.

Since June 2006, the NPA has commenced operation of the Internet Hotline Center (IHC) that accepts reports from general Internet users concerning illegal/harmful information, and handles reports submitted to the police concerning illegal information and undertakes actions such as requesting website administrators, etc. to delete illegal/harmful contents, and is promoting coordination between member organizations of "INHOPE", which was set up as a liaison organization for the hotline of each nation.

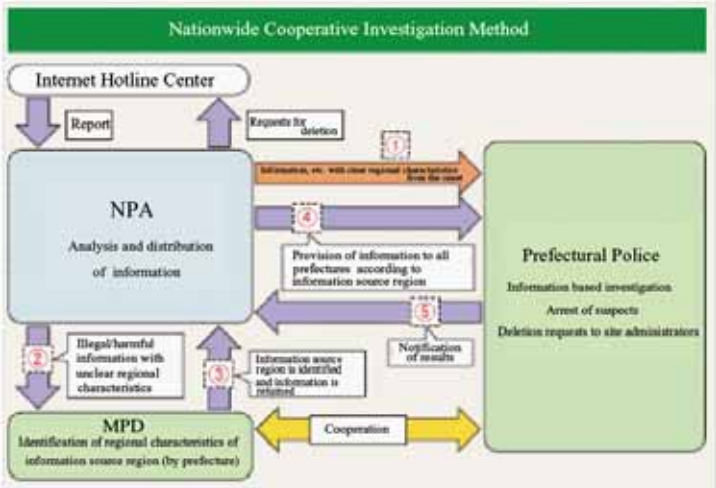
196,474 reports were received by the IHC in 2012. Of these, 38,933 concerned illegal information and 12,003 concerned harmful information. In addition, the IHC issued 17,503 requests for the deletion of illegal information, of which 15,872 were complied with to achieve a deletion rate of 90.7%.Regarding harmful information, 6,167 out of 7,738 cases were deleted to achieve a deletion rate of 79.7%.

The IHC Approach

(2) Effective Enforcement against Illegal/Harmful Information

Based on IHC reports and other information, the police endeavour to collect illegal/harmful information, and using the nationwide cooperative investigation method, undertake effective enforcement against illegal information and promote enforcement that primarily targets harmful information. In 2012, the number of cases cleared based on reports from the IHC was 3,303, an increase of 1,704 cases (106.6%) over the previous year.

Overview of nationwide cooperative investigation method

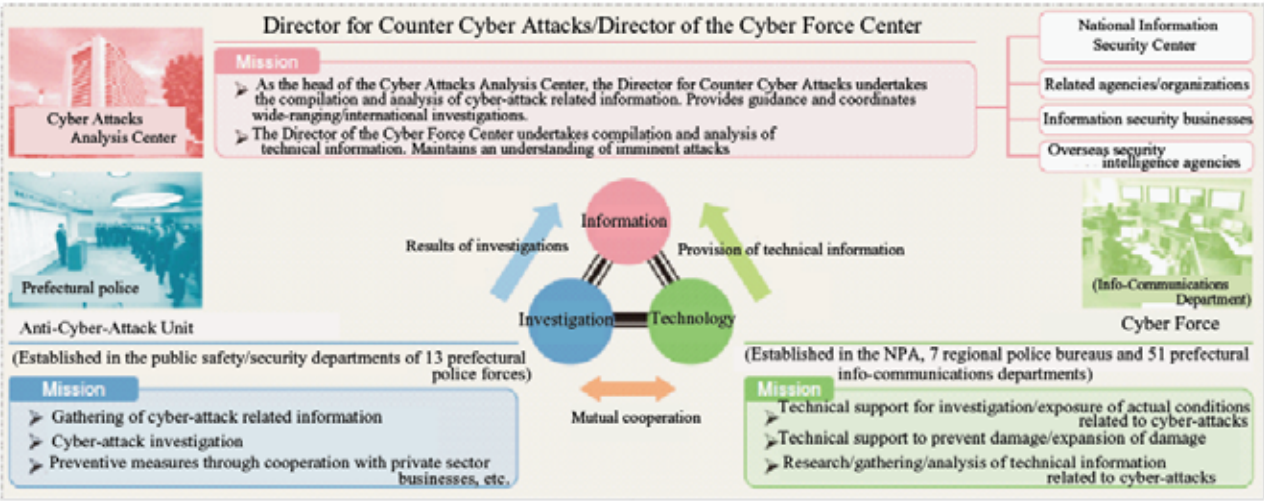


3 Measures against Cyber-attacks

(1) Reinforcement of Structures

In May 2013, the Cyber Force Center in the NPA established the position of Director for Counter Cyber-Attacks, to provide guidance and coordinate investigations by prefectural police, promote public/private cooperation and information exchange with overseas security intelligence agencies, and established the Cyber-Attack Analysis Center headed by said Director for Counter Cyber-Attacks to reinforce cyber-attack related information gathering/analysis functions. In addition, in April of the same year, Anti-Cyber-Attack taskforces were established in the 13 prefectures in which many government agencies and critical infrastructures are located. Anti-Cyber-Attack Units aim to improve investigative capabilities in relation to cyber-attack cases occurring nationwide by providing technical, technological and structural support for other prefectural police forces, and to perform central roles in the promotion of information gathering activities and the establishment of cooperative relationships with private sector businesses, etc.

Structure promoting cyber-attack countermeasures

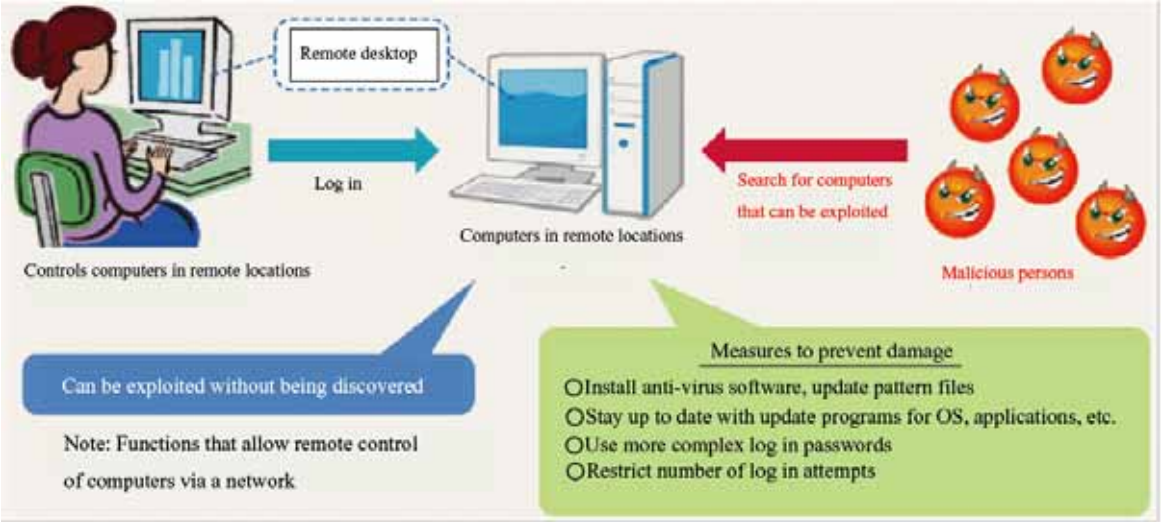


(2) Exposing Actual Conditions

While promoting investigations into illegal activities, police also analyze computers that have been subjected to cyber-attacks as well as malware to promote the exposure of actual conditions related to the attackers and the techniques used. If, in the course of investigating a cyber-attack case, it becomes clear that the source computer, etc. is overseas, the police issue requests for international investigative cooperation through the International Criminal Police Organization (ICPO) and other organizations and promote the exposure of actual conditions related to cyber-attacks by exchanging information with overseas security intelligence agencies.

Column: 2012 Internet observation results

During 2012, Cyber Force Center in the NPA observed a high rate of suspicious access attempts occurring at about once every 5 minutes and 20 seconds in relation to each sensor set up at connection points to the Internet, originating not only within Japan but from overseas as well. In particular, during 2012, there was an increase in access attempts targeting remote desktop functions that more than doubled the figure for 2011. Remote desktop functions are widely used in the management of remotely located computers, and although these functions are convenient, if they are exploited by a third party, the computer can be hijacked. Consequently, it can be inferred that individuals seeking to exploit the computers of others are randomly searching for computers that can be exploited. In addition, many access attempts believed to be by malware designed to attack remote desktop functions were also observed.

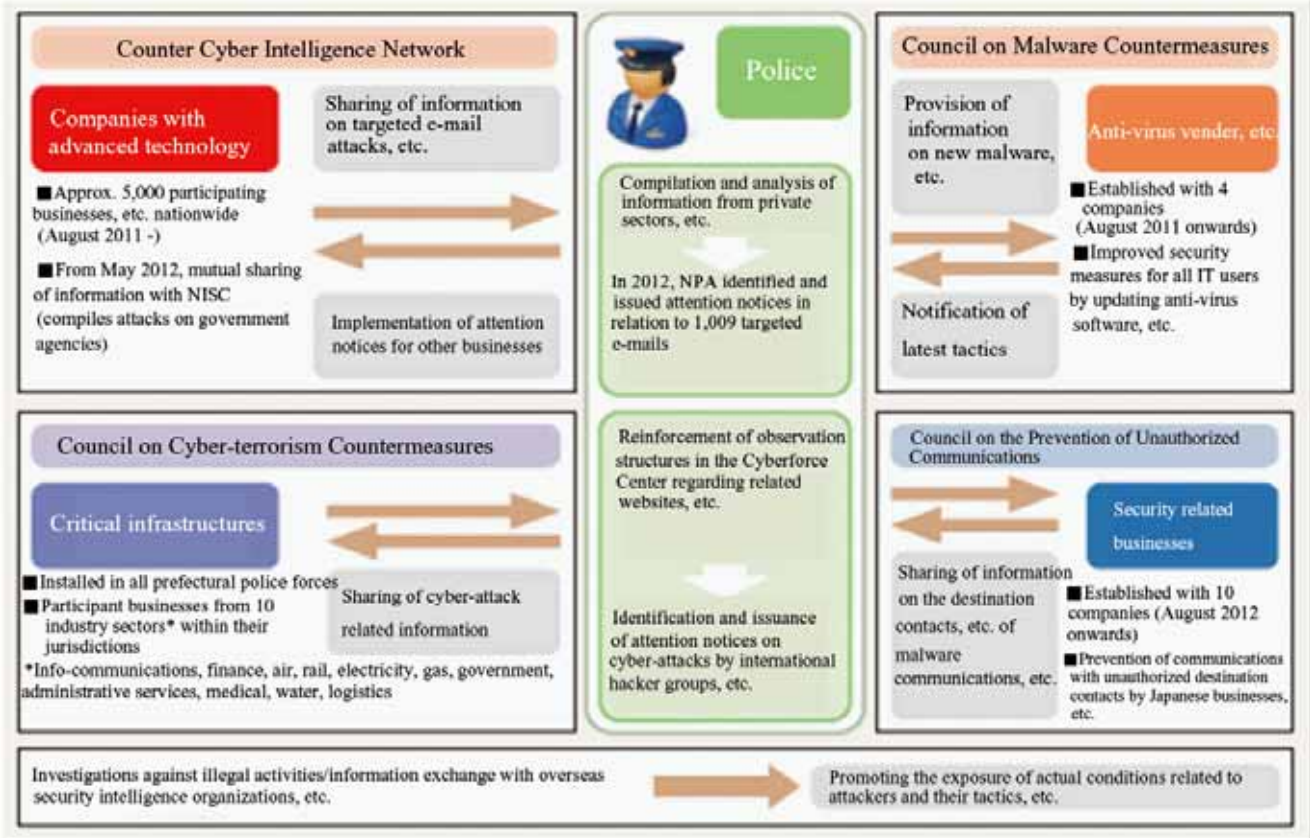


Access attempts targeting remote desktop functions* and measure to prevent damages

(3) Preventing Damage through Cooperation with Private Sector Companies

In order to deal with cyber-attacks, it is important for society as a whole, with public and private sectors working together, to deal with these issues, without relying solely on approaches taken by the police. In order to prevent damages of cyber-attacks and to respond appropriately when attacks do occur, the police have established cooperative frameworks with private sector companies, etc. as shown in the figure below, and are promoting approaches that utilize private sector know-how.

Unified public/private approach to cyber-attack countermeasures



4 Technological Support for Enforcement against Crime

With new electronic devices such as smartphones increasingly exploited in various criminal activities, the police established High-Tech Crime Technology Divisions in the Info-Communications Bureau of the NPA and prefectural info-communications departments to provide technological support for criminal investigations by prefectural police. Of these, the NPA Info-Communications Bureau retains personnel possessing high level specialist knowledge and technological expertise, high performance analytical equipment, and is implementing IT analyses requiring particularly high-level expertise such as extraction and analysis of data on damaged hard-disks and other memory formats and the analysis of malware, etc.

5 Enhancement of International Cooperation on Cybercrime Investigations

With regards to transnational cybercrime, when domestic investigations fail to identify the criminal, it is necessary to seek the cooperation of foreign investigations agencies. The NPA utilizes frameworks on international assistance in investigation such as Mutual Legal Assistance Treaties (Agreements) the ICPO to deal with transnational cybercrime. In addition, the NPA is actively engaged in information exchanges with foreign investigation agency personnel and the establishment of cooperative relations, etc. through international conferences and discussions with international investigations agencies.

Section 3: Future Approach

In April 2013, the "Act on the Partial Amendment of the Public Offices Election Act" was enacted, and with the consequent lifting of bans such as the prohibition of electoral campaigns using the Internet, resulting in the further expansion of areas in which the Internet is used, we have entered an era in which it is ever more difficult to imagine life without the Internet. Within this backdrop, if a serious cybercrime or cyber-attack does occur, the impact on socioeconomic activities in real-space will be incalculable. Now, in terms of citizens' everyday lives and economic activities, the importance of cyberspace is on a par with that of real-space, making cyberspace another new field alongside real-space in which the police should endeavour to ensure safety and security.

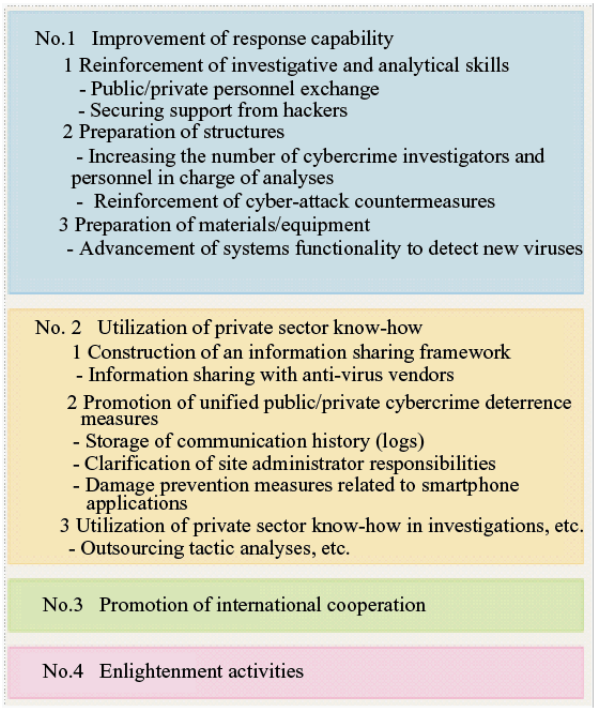
In light of advance-notice crime/virus distribution cases using the Internet that occurred between June and September 2012, the NPA compiled and announced "The Immediate Action Programme for the Reinforcement of the Abilities to cope with Cybercrimes in January 2013, to enable the police to deal with a wide range of incidents that may arise in cyberspace in the future. This program centers on the improvement of response capabilities, the utilization of private sector know-how, the promotion of international cooperation and enlightenment activities. The police have steadily promoted policies such as this program and are committed to reinforcing response capabilities in relation to the various situations that may arise in cyber-space.

Above all, with the aim of enhancing deterrence measures against cybercrime and cyber-attack and investigative capabilities in cyberspace, the most urgent tasks are to establish frameworks for cooperation between industry, academia and the government and to develop environments that will enable proper investigations against cybercrimes that exploit the anonymity and other weaknesses of the Internet.

Up to now, the main bodies in industry, academia and the government have each been promoting their own approaches relevant to their own positions, and have amassed an abundance of knowledge and experience. However, approaches that effectively integrate the compilation and analyses of information these sectors hold for deterrence measures against cybercrime and cyber-attacks and investigations in cyberspace have not always been sufficient. In order to efficiently identify and mitigate threats in cyberspace, the United States has already established a non-profit organization called the National Cyber-Forensics & Training Alliance (NCFTA) with the aim of promoting information sharing and cooperation between industry, academia and the government. In Japan also, it will be necessary to promote an approach that includes the establishment of this type of cooperative framework.

In addition, the possibility of tracking events after they have occurred has not been secured in Japan as there is no system for retaining traffic data of telecommunications (logs), and this is proving to be an issue in dealing with cybercrime, etc. The "Cybersecurity Strategy" drafted by the government's Information Security Policy Council in June of the same year states that, "In order to secure the possibility of tracking events after they have occurred, the retention of traffic data of telecommunications (logs), etc. of related businesses… (omitted)… must be reviewed". On this point, recent technological advancements have reduced the price of electromagnetic storage media by capacity, which has in turn reduced the burden on communications businesses, etc. in terms of log retention. The police are committed to taking part in reviews concerning the retention of logs with the relevant ministries and agencies, while taking into consideration aspects such as the types of logs that would be beneficial in terms of security, log storage periods that are applied overseas, and the diverse opinions of citizens.

By steadily promoting this type of approach, the police are working towards the construction of the safe and secure cyberspace that is essential to the realization of a world leading IT society.



The Immediate Action Programme for the Reinforcement of the Abilities to Cope with Cybercrimes (Overview)