

CYBERSECURITY ANNUAL REPORT

**FISCAL YEAR 2013
<OVERVIEW>**

July 10, 2014

**Information Security Policy Council
The Government of Japan**

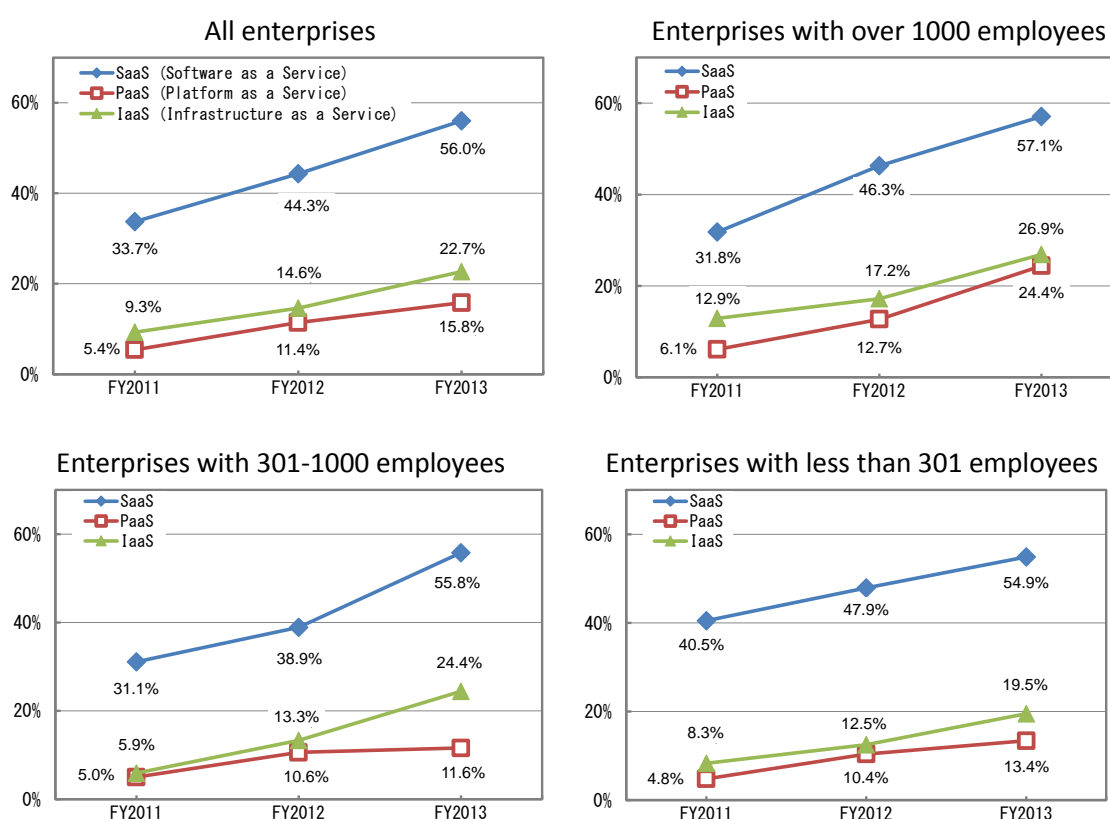
THE STATE OF CYBERSECURITY IN FY2013

17.2%

1. Overall Status of Japan's Cybersecurity

These days, there has been remarkable progress in the sophistication of information and communications technologies. This has resulted in the widespread use of a variety of services harnessing information and communications technologies, such as cloud computing and SNS, by organizations including enterprises as well as people. For example, the use of cloud computing related services by small, medium sized, and large enterprises — in other words, regardless of business size— rose, and it indicates the increasing dependence of business operations on cyberspace (Figure 1-1).

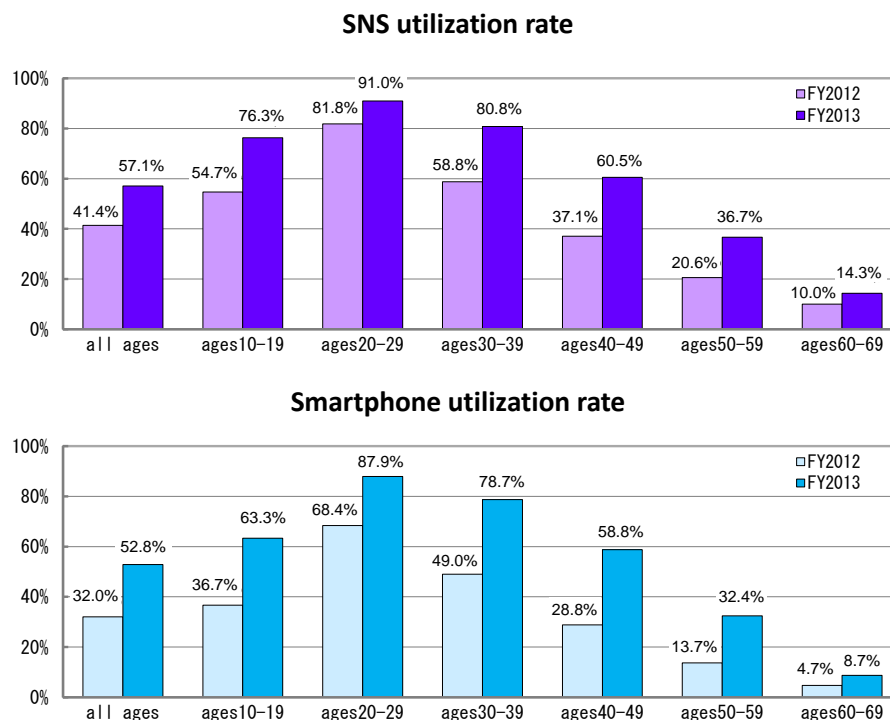
Figure 1-1 Trends in use of cloud-related services¹ (Utilization rate)



¹ Based on "Data: Survey results on IT human resources trends (for user enterprises)" in the "White Paper on IT Human Resources" of the cited fiscal years by Information-Technology Promotion Agency, Japan (IPA).

As to the activities of people, the SNS utilization rate for communications and other purposes was on the rise not only among young people but also among other generations. It indicates that individuals' social activities became deeply dependent on cyberspace (Figure 1-2). In fact, local enterprises can operate global business directly through the Internet, etc., and individuals can share common experiences in real time with people all over the world with their smartphones and tablets. This will certainly lead to the significant advancement in people's empowerment and potential for development.

Figure 1-2 Trends in Use of SNS and Smartphones²



These are the aspects towards positive evaluation on the explosive diffusion of information and communications technologies. On the other hand, increasing risks in cyberspace cannot be overlooked. For example, in one fiscal year, namely FY2013, there were more than 1 million cases of divulging users' information caused by unauthorized access to major Internet service providers. In addition, there were incidents involving unauthorized access (illegal logins) by third parties stealing login IDs and passwords for online services, such as Internet banking and SNS, with some methods. General IT users were under threats. In 2013, the number of

² Based on preliminary data from "2013 Survey on utilization time of information telecommunications media and Information activities" by Institute for Information and Communications.

unauthorized access attempts (the number of detected cases) was nearly 2.4 times higher than 2012 (Figure 1-3). In terms of the purposes of these malicious activities, in 2012, the majority of cases was to manipulate online games; but in 2013, it shifted to a monetary gain purpose targeting internet banking and/or shopping (Table 1-1).

Figure 1-3 Status of unauthorized access incidents³:

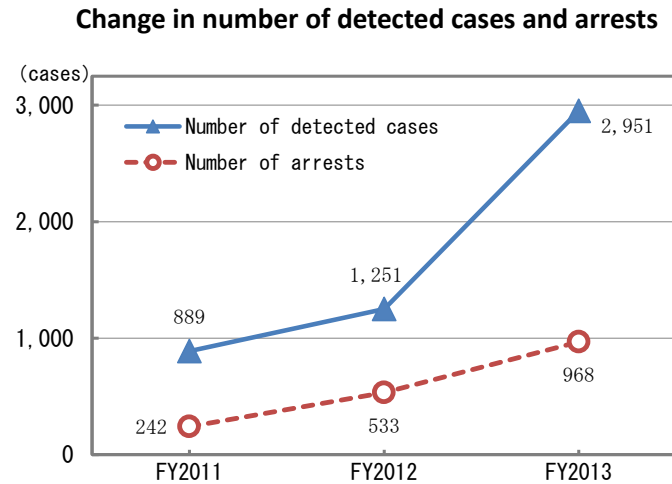


Table 1-1 Malicious actions taken after unauthorized access

	FY2011	FY2012	FY2013
Illegal money transfers using Internet banking	188	95	1,325
Illegal online shopping	172	223	911
Manipulation of online games and community websites	358	662	379
Site manipulation/elimination	28	42	107
Illegally obtaining information	74	99	92
Manipulation of Internet auctions	22	29	36
Illegal information storage	4	1	20
Other	3	100	81

The tactics of unauthorized access became manipulative, too. In terms of the number of arrests concerning unauthorized access to steal identification codes, such as IDs and passwords, "verbal manipulation of authorized users or shoulder hacking" was the most frequently used tactic to obtain information in 2012, but "abuse of

³ Based on data of the "Status of occurrence of unauthorized access and R&D on technologies of access control functions" (released on March 27, 2014, by the National Police Agency and the Ministry of Economy, Trade and Industry).

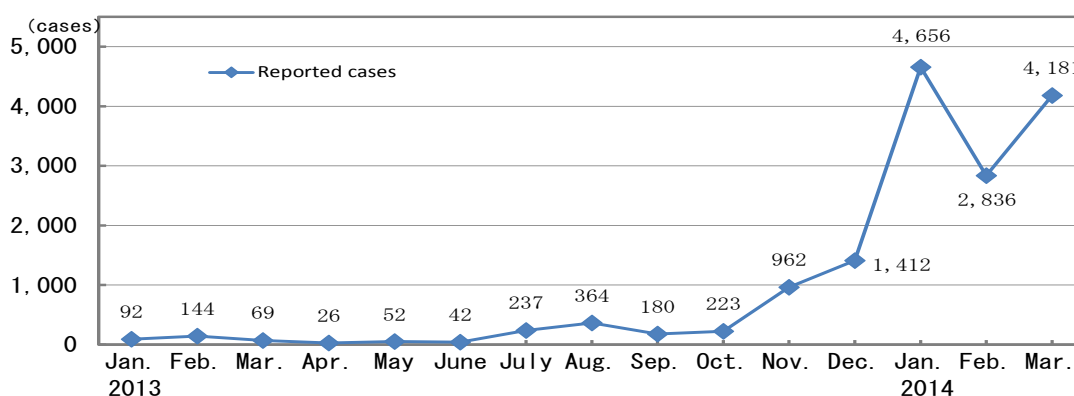
insufficient setting/management of users' passwords" increased rapidly and became the majority of the tactics in 2013 (Table 1-2).

Table 1-2 Unauthorized access-related crime by method⁴

	2011	2012	2013
Number of arrests related to divulging identification codes	241	532	965
Abuse of insufficient setting/management of users' passwords	59	122	767
Verbal manipulation of authorized users or shoulder hacking	29	299	64
By someone previously having access to identification codes (ex-employees, friends, etc.)	52	101	56
Obtaining from malicious actors such as accomplice(s)	38	22	35
Use of malware such as spyware	1	29	25
Use of phishing sites	59	18	9
Purchasing from the third person	0	0	7
Other	3	11	2
Number of arrests related to attacks by exploiting security holes	1	1	3

This trend in the increase in malicious actions for monetary purposes was also found in rapidly increasing phishing, that is, an attempt to fraudulently steal personal information, such as login IDs and passwords, addresses, names, bank account numbers, credit numbers, by sending e-mails that appear to originate from a legitimate service providers. For example, in the continued rise of reported incidents from the end of the year, the number of "phishing incidents" (including overseas incidents) reported to the Council of Anti-Phishing Japan reached 4,181 in March 2014 (Figure 1-4).

Figure 1-4 Change in reported phishing incidents⁵



⁴ Based on data of the "Status of occurrence of unauthorized access and R&D on technologies of access control functions" (released on March 27, 2014, by the National Police Agency and the Ministry of Economy, Trade and Industry).

⁵ Based on the monthly status of phishing report of the Council of Anti-Phishing Japan.

It is reported that most of them were phishing by masquerading as online games and/or financial institutions (about 97 percent of the total reported incidents in that month)⁶; moreover, there were repeated media reports on phishing incidents masquerading as major financial institutions. All these reports reveal that unauthorized access for the monetary purposes became an immense cyber threat.

In organizations such as enterprises, managers are usually responsible for the operation of information systems. With regard to the number of unauthorized access incidents reported by manager, private enterprises particularly became the largest victims (Table 1-3). In terms of motivation, while "illegally obtaining monetary gain" was a marked motivation for unauthorized access, it is also noteworthy that "illegally obtaining information such as clients' data" was on the rise.

Table 1-3 Number of unauthorized access incidents reported by manager⁷

	2011	2012	2013
Private enterprises	762	1,163	2,893
Internet service providers	115	22	9
Universities, research institutes, etc.	1	12	9
Administrative organs, etc.	6	52	24
Other	5	2	16

In terms of the trends in targeted e-mail attacks, the number of targeted e-mail attacks identified by the National Police Agency during 2013 was 492⁸; it was a decrease of 517 from the previous year (a year-on-year decline of 51 percent). With these numbers, the threats of targeted e-mail attacks were seemingly declining. According to an analysis made by the National Police Agency, however, while there was a decline in "phishing email campaigns", which are launched with a large number of e-mails, there was an increase in so-called "spear-phishing" attacks, in a form of social engineering. The methods of attacks were evolving, too, due to emerging tactics, for example, to avoid the detection of unauthorized external connections.

⁶ Based on the "Status of Phishing Report 2014/03" (released on April 1, 2014 by the Council of Anti-Phishing Japan").

⁷ Based on data of the "Status of occurrence of unauthorized access and R&D on technologies of access control functions" (released on March 27, 2014, by the National Police Agency and the Ministry of Economy, Trade and Industry).

⁸ Based on the "Status of cyber attacks and progress of countermeasures in 2013" (released on February 27, 2014 by the National Police Agency). The cases were those identified by the National Police Agency through the "Cyber Intelligence Information Sharing Network" as targeted e-mail attacks aiming at divulging information.

Given that, it is also pointed out that the threats of targeted attacks became rather greater than ever before.

Such targeted attacks mainly aim at security breaches, for example, stealing critical information including confidential data on business operations, by infiltrating malware into a targeted organization's information systems. There is an increase in attacks with such diversified and manipulative methods in recent years, and there is a growing concern of additional targeted attacks using the stolen information by the attacks. Under these circumstances, in order to enhance the quality of enterprise management, the Intellectual Property Strategy Headquarters has discussed the topics including the use of case examples and best practices in the Trade Secret Management Guidelines.⁹

⁹ Based on "Report of Task Force for Trade Secret" (released on April 23, 2014, by the Task Force for Trade Secret, the Verification, Evaluation, Planning Committee, the Intellectual Property Strategy Headquarters).

2. Status of Cybersecurity Concerning Government-related entities ¹⁰ and Critical Information Infrastructure Operators

(1) Status of cybersecurity concerning government-related entities

In fiscal year 2013, “external attacks” and “unintentional information leakages” were the two main causes of information security incidents involving government-related entities. The following are the trends in information security incidents by major cause, in terms of cybersecurity concerning these entities in the fiscal year.

A. Information security incidents caused by external attacks

As same as the previous fiscal year, there were a large number of information security incidents aiming at stealing critical information from the government bodies, the incorporated administrative agencies, and so on, by attacks such as the use of unauthorized access and malware. In general, targeted e-mail attacks are frequently used tactics in the initial stage of cyber attacks. They are typically initiated by sending targets e-mails that contain malware in an attached file or URL links to malicious servers, and, as a result, e-mail recipients' terminals are infected with malware by opening these attached files or clicking the indicated URLs.

The GSOC¹¹ of the National Information Security Center or NISC has collected information and issued alerts on suspicious e-mails received by the governmental bodies, and it issued 381 alerts during fiscal year 2013 (Table 2-1).

Table 2-1 Change in alerts concerning suspicious e-mails

	FY2011	FY2012	FY2013
Number of alerts concerning suspicious e-mails	209	415	381

¹⁰ Besides governmental bodies, they include incorporated administrative agencies, national university corporations, etc.

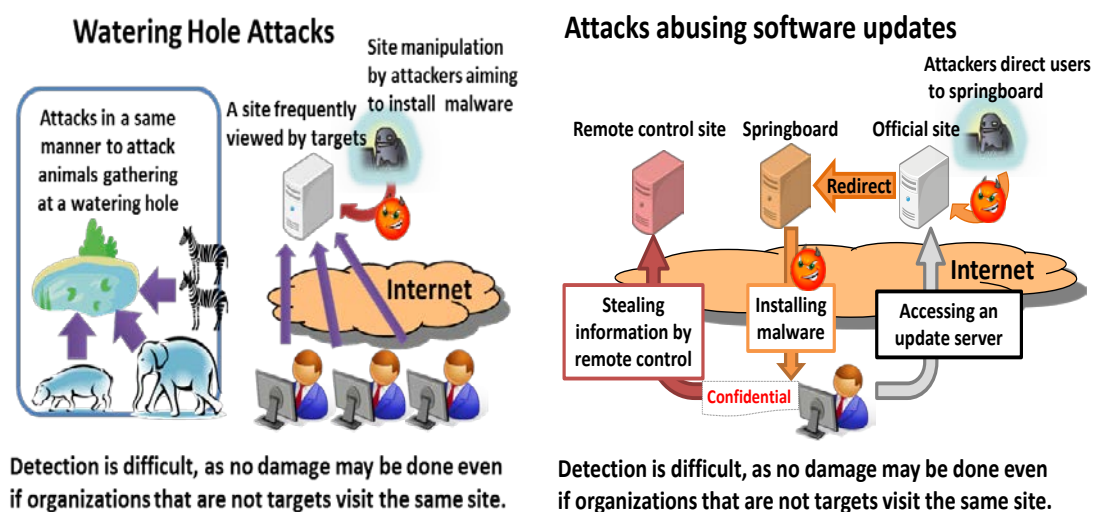
¹¹ The Government Security Operation Coordination Team. The GSOC's missions include: Government-wide information gathering, analyses and diagnoses of cyber attacks and other cyber incidents, assistance for the governmental bodies, and the promotion of mutual coordination and information sharing among the governmental bodies.

Putting aside an extraordinary situation where a large number of suspicious e-mails were sent to the governmental bodies in December 2012, there was a general tendency towards increasing alerts over the past few years.

With regard to targeted attacks, in addition to targeted e-mail attacks, so-called “watering hole” attacks emerged in 2013. In this type of attack, malware is sent to site viewers visiting from pre-selected IP address of the targeted organization, and these viewers become sole victims of the infection. In October 2013, this attack was reported by media as “cyber attacks targeting at least twenty organizations such as governmental bodies and major enterprises”. In this incident, as to the governmental bodies, automatic virus downloads were detected in the terminals of seven ministries and agencies, but no information leakage was confirmed.

Furthermore, the cyber attacks showed tendencies towards evolution and diversification; for example, in February 2014, there was a report of an information security incident or virus infection caused by updating a specific video player software (case confirmed at an incorporated administrative agency). As for a targeted attack taking advantages of vulnerabilities that have not been patched or made public, i.e. before the release of security patches, or so-called a “Zero-day attack”, the prevention of malware infection is technically difficult. Therefore, it cannot be overemphasized that it is indispensable to implement preventive measures against the penetration of malware into information systems, including the enhancement of the network monitoring and communication systems.

Figure 2-1 Examples of emerging threats (targeted attacks)



To remind government-related entities to be vigilant against cyber threats, the GSOC has disseminated security tips on countermeasures to tackle software vulnerabilities that would possibly be targeted by cyber attacks such as web attacks. In fiscal year 2013, the GSOC provided 78 security tips including information on vulnerabilities (Table 2-2).

Table 2-2 Change in number of GSOC security tips on software vulnerabilities, etc.

	FY2011	FY2012	FY2013
Number of disseminated security tips on vulnerabilities, etc.	68	74	78

Website manipulation is one of the major attacks exploiting vulnerabilities. Previously, ensuring the governmental bodies' security measures was the top priority. However, since attacks targeting the incorporated administrative agencies have been expanding, the enhancement of security measures not only for the governmental bodies but also for the incorporated administrative agencies is currently most needed.

As a countermeasure against cyber attacks targeting the governmental bodies, the GSOC has carried out the detection of cyber attacks or signs of cyber attacks by using a government-wide information collection and monitoring function, namely, the "GSOC Sensor". The number of detected incidents that were considered as threats against the governmental bodies through this detection function was approximately 5.08 million in fiscal year 2013 (Table 2-3).

**Table 2-3
Change in number of threats to governmental bodies detected through GSOC Sensor**

	FY2011	FY2012	FY2013
Approximate number of threats to governmental bodies	660,000	1,080,000	5,080,000

The number was almost five times higher, compared with fiscal year 2012; and it made up roughly one detection per every six seconds. It is considered that this rise was affected by the increasing threats to the governmental bodies; and that the improvements made during the fiscal year such as the improvement of sensor

capability also contributed to this rise. It is critical to capture and analyze cyber threats in more detail by continuously improving the GSOC Sensor, and so on.

The GSOC has sent a notification to a relevant governmental body when detecting unauthorized access (including suspected cases) through its monitoring activities with the GSOC Sensor, etc. In fiscal year 2013, the number of the notifications reported to the relevant bodies was 139 (Table 2-4).

Table 2-4
Change in number of notifications reported through monitoring by GSOC Sensor, etc.

	FY2011	FY2012	FY2013
Number of notifications through monitoring by GSOC Sensor, etc.	139	175	139

The number of notifications in fiscal year 2012 was particularly high, because a large number of suspicious e-mails were sent to the governmental bodies in December 2012, as previously stated. As a result, more than half of these notifications were concerned with the detection of targeted e-mails.

In fiscal year 2013, the notifications concerning targeted e-mails accounted for one-fourth of the total notifications. The detection of suspicious communications¹² was one of the significant figures of this fiscal year. It was significant because there was almost no detection of such a communication prior to fiscal year 2013, but, in contrast, the number represented 30 percent of the total in fiscal year 2013. It is considered that "malware infections by targeted e-mail attacks" and "malware downloading by viewing manipulated websites like web-based watering hole attacks" were possibly the major causes of the detection of these suspicious communications.

With regard to targeted attacks, although they had been existing dangers in prior years, most of them had been "e-mail phishing campaigns" and their success rate against the governmental bodies had remained low. However, it is considered that the detection of suspicious communications increased due to the rising success rate of customized targeted e-mail attacks to specific organizations and/or employees,

¹² Not all of "suspicious communications" are necessarily "malicious communications". For example, if connectivity tests to access blacklisted websites are conducted without previous notice, it could be considered as suspicious communications by the GSOC.

as significantly observed in fiscal year 2013. The number of notifications reported by the GSOC in this fiscal year remained same as the previous years, if excluding the extraordinary factor such as the numerous suspicious e-mails. Meanwhile, as previously stated, there were the changes in the types and the ratio of threats, e.g. unauthorized access, reported by the GSOC. Indeed, risks in cyberspace appeared to be spreading with acceleration. Since targeted e-mails and watering hole attacks are mostly combined with Zero-Day attacks, it is hard to block all penetration of malware. Hence, further enhancement of the GSOC is a must.

Figure 2-2 Outline of GSOC

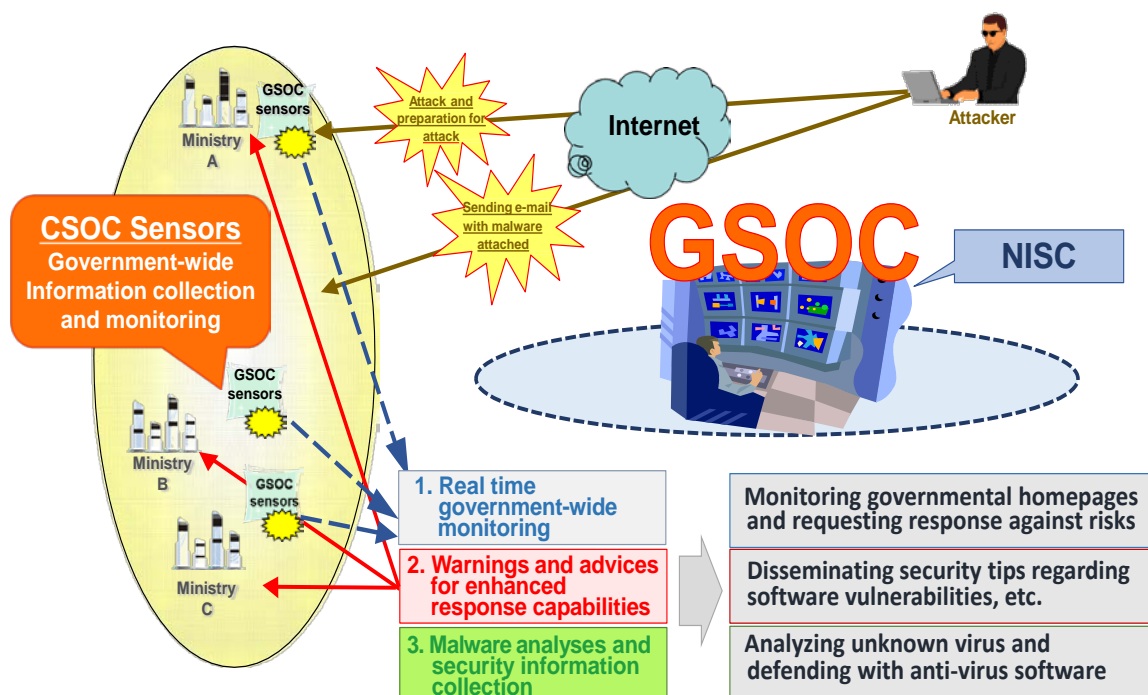
< The Government Security Operation Coordination team> (GSOC)

April 2008: GSOC became operational (8 hours per weekday).

April 2009: GSOC began 24/7 operation (throughout the year).

April 2013: GSOC began the operation of its current system.

2017: GSOC is scheduled to launch its next generation system.



B. Information security incidents caused by unintentional information leakages

While cyber attacks by external actors increased, there were occasional information security incidents concerning unintentional information leakages caused by employees' low awareness of cybersecurity or mistakes, and so on. Previously, the majority of these incidents was accidental and caused by careless mistakes such as the loss of computers or USB flash drives or sending e-mails to wrong e-mail addresses. Recently, however, different types of incidents have occurred in relation to the improper use of Internet connected devices and/or cloud-based services and the inadequate connection settings of these devices and/or cloud-based services.

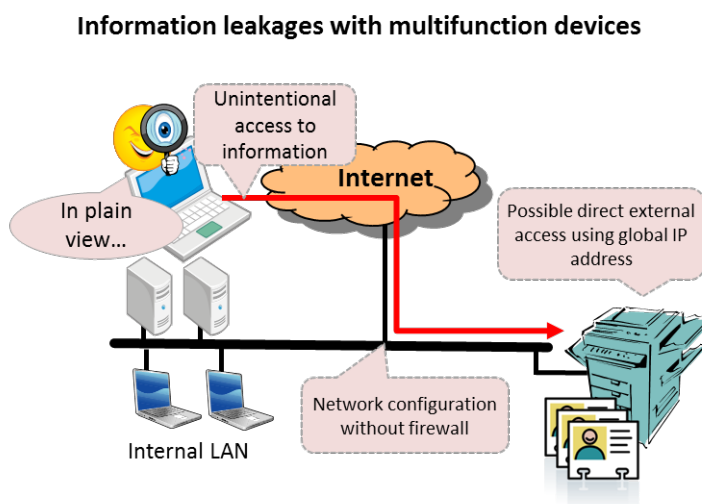
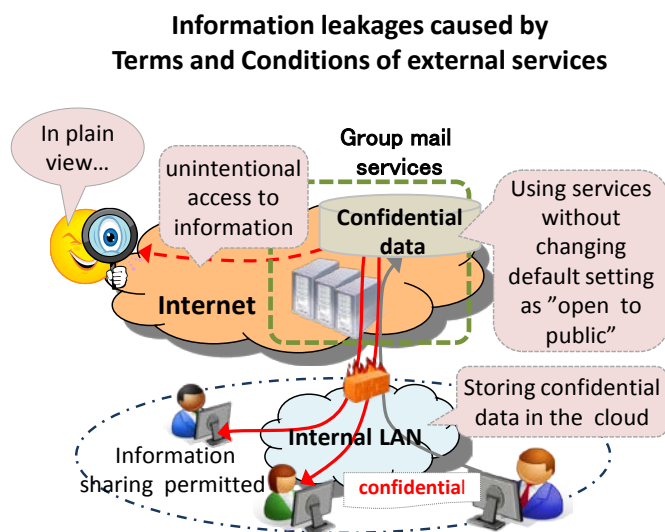
The following are examples of such incidents:

- A case, made public in July 2013, in which personal information and internal information of the central governmental bodies stored in a free cloud service to share e-mails on the Internet remained accessible by everyone;
- A case, made public in November 2013, in which personal information of students and others scanned or faxed at universities remained viewable to everyone on the Internet; and,
- A case, made public in December 2013, in which the computer systems of government-related entities were compromised with a Japanese input software automatically transmitting all characters entered with the software to the software company's cloud server.

As to the case involving the free-cloud service, this free cloud-based service enabled e-mail sharing on the Internet, and the root cause of this incident was that the service was used by the employees of multiple governmental bodies on business trips to share internal information with their colleagues or for communications with external persons.

In the past, from a viewpoint of information security assurance, the government-related entities used to be conservative in utilizing external cloud services. On the other hand, the needs for highly convenient services have been rising in business operations. The above-mentioned incident can be considered as an example that such needs produced undesirable results in terms of information security. Consequently, with regard to information and data that require extra care in handling, it is an utmost necessity to create an IT environment to respond to business operational needs and, at the same time, to assure information security.

Figure 2-3 Example of emerging threats (unintentional information leakages)



(2) Status of cybersecurity concerning critical information infrastructure operators

In terms of situational reports such as in the event of accidents involving IT system failures at critical information infrastructure (CII) operators and relevant parties¹³, the number of communications to NISC via the governmental bodies

¹³ In the first and second Action Plans on Information Security Measures Concerning Critical Infrastructure, the following were identified as critical infrastructure sectors: "information and communication services", "financial services", "aviation services", "railways services", "electrical power supply services", "gas supply services", "governmental and public administrative services (including local government organizations)", "medical services", "water services", and "logistics services". Among business operators and other relevant parties of these sectors, critical information infrastructure operators and relevant parties mean a body comprised of those specified in the Action Plans. From fiscal year 2014, in line with the newly established third edition, "chemical industries", "credit card services", and "petroleum industries" industries are added to the critical information infrastructure sectors.

responsible for CII increased by 1.5 times, from 110 in fiscal year 2012 to 153 in fiscal year 2013. Among those, communications on cyber attacks (intentional cases) also increased to 133 in fiscal year 2013, up from 76 in the previous fiscal year (Table 2-5). It should be noted that these increases do not necessarily illustrate the more frequent failures of IT systems caused by cyber attacks and so on; rather, it can be considered that the increased awareness of the importance of information sharing among critical information infrastructure operators and others as well as a more active use of the information sharing system with NISC largely contributed to these increases.

Table 2-5
Number of communications to NISC from critical information infrastructure operators

	FY2011	FY2012	FY2013
Number of communications from CII operators	43	110	153
Communications on cyber attacks	15	76	133
Communications on unauthorized access and Dos attacks	12	55	121
Communications on computer virus infections	2	6	7
Communications on other intentional cases (suspicious e-mails, etc.)	1	15	5

The cyber attacks concerning CII can be broken down into two common categories: unauthorized access and DoS attacks. The following are examples of these attacks.

- The login IDs and encrypted passwords to access a membership website managed by a business operator were leaked by exploiting the vulnerabilities of middleware.
- Due to website manipulation caused by the exploitation of vulnerabilities in a website managing system, the visitors of the said website were directed to external malicious websites.
- Website display speed became unusually slow due to a huge number of access requests from various overseas regions, presumably caused by DNS server-related insufficient settings (related to open resolvers).

The “Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP)” is an initiative for information sharing among the member organizations of this partnership through IPA as an information hub. The number of information provided from the member organizations to IPA regarding suspicious e-mails, which were apparently targeted e-mail attacks, through J-CSIP was 385. It increased by approximately 1.5 times from 246 in the previous fiscal year. The number of information sharing conducted by IPA for member organizations based on the provided information, etc. was 180 (Table 2-6). It is required that CII operators will continuously enhance information security measures, taking into account these situations.

Table 2-6 Number of provided and shared information through J-CSIP

	FY2012	FY2013
Provision of information from member organizations to IPA	246	385
Information sharing with member organizations	160	180

3. Major governmental policies and achievements in FY 2013

In June 2013, the Information Security Policy Council chaired by the Chief Cabinet Secretary established the “Cybersecurity Strategy”, as a new national strategy to respond to increasing risks in cyberspace.

The basic principles of this strategy, which covers the triennium FY2013 - FY2015, are: (1) Ensuring the free flow of information; (2) adapting to growing risks; (3) enhancing risk-based responses; (4) actions with a sense of social responsibility and reciprocal assistance. Based on these principles, the Strategy illustrates its overarching goal to build “the most advanced cybersecurity nation” with efforts made by stakeholders, e.g. governmental bodies and CII operators, for mutual collaboration, while harnessing NISC as the focal point, and establish a world-leading cyberspace, which is resilient and dynamic, by promoting such activities: upgrading cybersecurity standards, expanding capabilities to counter cyber attacks, improving the basic capabilities related to cybersecurity, for example, with the promotions of human resources development and R&D, the enhancement of international collaboration, and the betterment of the Government’s organizational system (Figure 3-1).

This Strategy incorporates such approaches: for stakeholders, including the governmental bodies, the incorporated administrative agencies, CII operators and relevant organizations, enterprises, and the public, to take enhanced protection for achieving resilient cyberspace; for Japan to build dynamic cyberspace by enhancing the information security related foundations to develop core capabilities for IT utilization, for example, human resources development and the advancement of technological capabilities; and for Japan to play a leading role in the world, e.g. to contribute the international community, bearing in mind that cyberspace is a global domain (Figure 3-2).

Figure 3-1 Outline of the “Cybersecurity Strategy”

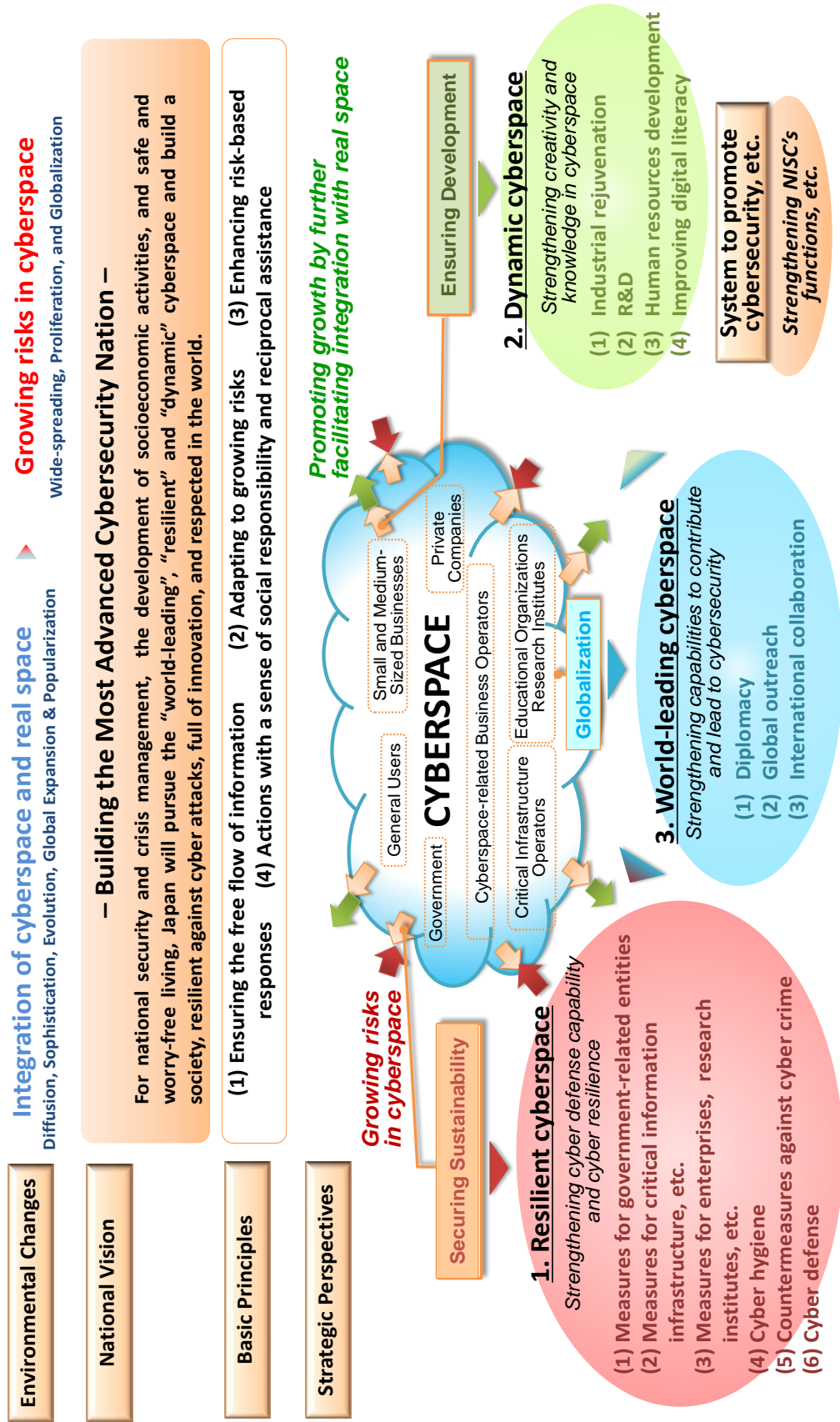


Figure 3-2 Primary approaches of the "Cybersecurity Strategy" (FY2013 - FY2014)

	Government Bodies, Incorporated Administrative Agencies, etc.	Critical Information Infrastructure Operators	Enterprises and Individuals
Resilient Cyberspace (Enhanced protection)	<ul style="list-style-type: none"> ✓ Review of the Common Standards and adoption of risk assessment methodology to protect sensitive information ✓ Reinforcement of GSOC; accurate and quick responses through cooperation with CYMAT and CSIRT ✓ Implementation of Incident response drills; specification of roles of related parties such as the police and the Self Defense Forces ✓ Arrangement of countermeasures for emerging threats related to new services such as SNS and group mails ✓ The 3.18 Cyber Training 	<ul style="list-style-type: none"> ✓ Review of the Basic Policy including expanding the scope of critical information infrastructure and review of the Safety Standards ✓ Improvement of information sharing among governmental bodies, system vendors, etc. ✓ Implementation of cross-sectoral exercises to ensure business continuity ✓ Creation of platforms for assessment and authentication systems, such as control systems used by critical information infrastructure, in compliance with international standards 	<ul style="list-style-type: none"> ✓ Adoption of countermeasures against malicious smartphone applications ✓ Launch of Information Security Awareness Month (February) and "Cyber Security Day" ✓ Revision of the Information Security Outreach and Awareness Program of 2011 (Information Security Policy Council) ✓ Promotion of security investment by small and medium-sized businesses through incentives such as tax systems ✓ Promotion of IT related business operations' activities, e.g. security advice such as virus warnings for users by Internet service providers ✓ Assurance of cyber crime traceability, e.g. by examining log storage methods
Dynamic Cyberspace (Basic capability)	<ul style="list-style-type: none"> ✓ Revision of Information Security Human Resource Development Program 2011 (Information Security Policy Council) ✓ Review of Information Security Research and Development Strategy 2011 (Information Security Policy Council) 		
World-leading Cyberspace (International strategy)	<ul style="list-style-type: none"> ✓ Japan-US ✓ Japan-UK ✓ Japan-India ✓ Japan-EU ✓ Japan-ASEAN ✓ Conferences on international norms and rulemaking in cyberspace, etc. ✓ IWWN (*1) 	<ul style="list-style-type: none"> * 1 Dialogues for the promotion of international activities to counter vulnerabilities, threats, and attacks in cyberspace among governmental entities and CERTs of the US, Germany, the UK, Japan, etc. * 2 Dialogues on best practices and international coordination, etc. among the US, the UK, Germany, Japan, etc. 	<ul style="list-style-type: none"> ✓ Joint awareness raising activities in October
Organizational Reform	<ul style="list-style-type: none"> ✓ Enhancement of NISC's functions (scheduled to be reorganized as "Cybersecurity Center" [tentative], targeting FY2015) <p>Main purposes: Enhancement of GSOC; arrangement of information sharing between GSOC and CII operators; enhancement of cybersecurity human resources, etc.</p>		

The following are the summary of main activities promoted in fiscal year 2013 in line with the Strategy. As for a set of the Common Standards of Information Security Measures for Government Agencies, after reviews were conducted for the purpose of enhancing the responses to emerging threats and technologies as well as improving the effectiveness of the management standards, a revision was made in May 2014. As one of the responses to emerging threats, and so on, the adjustments of the provisions have been carried out to counter the threats of targeted attacks. Together with the common standards related guidelines¹⁴, which were discussed separately, they specifically aim to: identify prioritized tasks, etc. for the protection from targeted attacks; detect malicious infiltration into the inner information systems concerned; and prepare contingency plans to deactivate such attacks. Additionally, in view of recent environmental changes, new provisions were added in relation to: supply chain risk management, so to speak, to require strict management systems to prevent the infusion of malicious actors into information systems of outsourcing contractors, etc.; the strict management of the use of personal smartphones and other devices for business purposes; the prohibition of sending confidential information in use of the governmental SNS and relevant services; the management of USB flash devices, multifunction devices, and so on.

In the revision process, special attentions were paid to making the standards better understood and more respected, with such efforts, e.g. the clarification and simplification of definitions and terms, the non-use of lengthy descriptions, the compiling the employee compliance provisions by each staff category; the reexamination of the obsolete provisions (Figure 3-3).

Figure 3-3 Example of reexamined provision

<Sample provision of the previous Common Standards>

Employees must inform the concerned parties and the chief information security officer according to the reporting procedure formulated by the head of information security officers through the incident response officer when a failure, accident, etc., or the like comes to their notice. However, if it is impossible to report to the person in charge of failure, accident etc. due to unavoidable emergency circumstances, they should report to the chief information security officer according to the defined procedure.



<After reexamination>

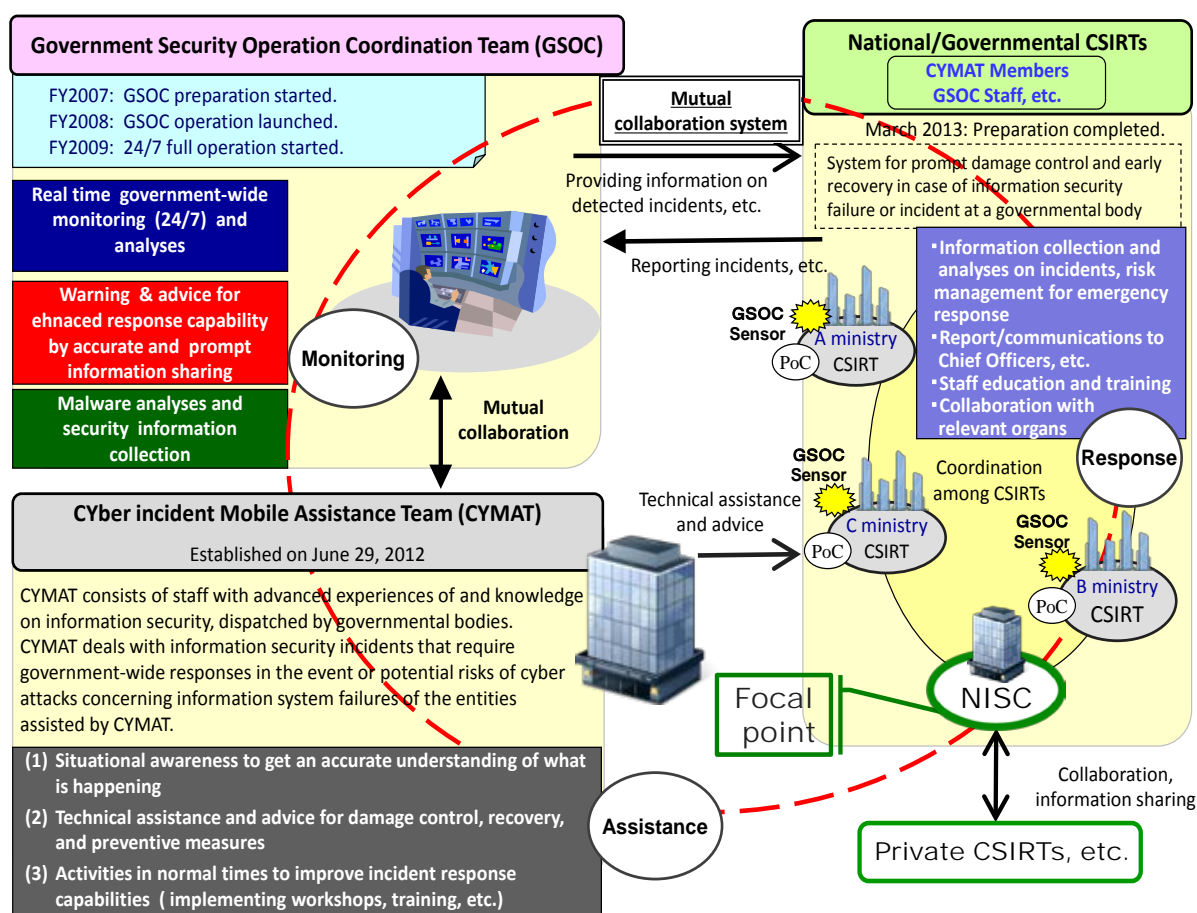
Administrative employees shall report to the ministry's reporting point of contact when an information security incident is discovered and shall act in accordance with instructions received.

¹⁴ The guidelines for risk management of countering advanced cyber attacks, etc. They became preliminarily operational in October 2013, and are scheduled to become officially operational in fiscal year 2014.

Furthermore, the governmental bodies made progress in the expansion and enhancement of risk management systems in the event of cyber attacks, by improving the coordination among the GSOC, the CYMAT, and the CSIRT and implementing the 3.18 Cyber training, and so on (Figures 3-4 and 3-5).

In terms of information security measures concerning CII operators, certain results were achieved based on the second edition of “the Basic Policy of Critical Information Infrastructure Protection”¹⁵. However, since there were various environmental changes in societal and technological aspects, compared with when the second edition had been adopted, discussions were made on a new policy in line with the Cybersecurity Strategy.

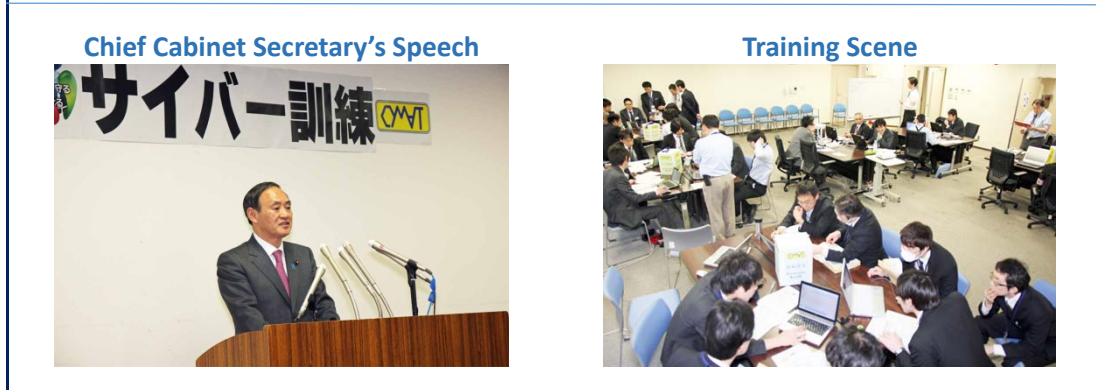
Figure 3-4 Enhancement of coordination among GSOC, CYMAT, and CSIRT



¹⁵ Originally entitled as “The Second Action Plan on Information Security Measures for Critical Infrastructures” (February 3, 2009).

Figure 3-5 The 3.18 Cyber Training

Under the circumstances where cyber attacks against Japan had become more complex and manipulative, training was carried out to handle multiple simultaneous cyber attacks against various governmental bodies. Aiming to improve the coordination among relevant parties, the training was conducted with a combination of (a) information gathering and sharing exercises among NISC, governmental entities, and CII operators, etc., and (b) emergency response drills by the CYMAT members.



In the third edition of “the Basic Policy of Critical Information Infrastructure Protection” that was established in May 2014, each component was revised and reinforced, while the basic framework of the second edition was maintained. More specifically, the third edition includes: the creation of guidelines to enable relevant parties, especially, small and medium-sized enterprises to upgrade their standards of information security measures step by step; the establishment of an information sharing system in the event of accidents including extensive IT system failures, as the extension of the system in normal times; the expansion of the scope of CII from the existing ten sectors to thirteen sectors, with addition of three sectors, namely, chemical industries, credit card services, and petroleum industries. Furthermore, the overall contents were elaborately structured, for example, in a way that enables top business management to obtain the full picture of information security measures by adding a chapter summarizing the Basic Policy (Figure 3-6).

In addition, with regard to CII, necessary measures, such as the implementation of cross-sectoral exercises, have been undertaken.

Figure 3-6

Highlights: “The Basic Policy of Critical Information Infrastructure Protection (3rd edition)”

Components and major points

- Maintenance and promotion of safety principles:** Appealing to CII operators in the process of preparing measures as well as small and medium-sized CII operators, etc. for the importance to develop information security measure with a “growth model”.
- Enhancement of information sharing system:** Clarification of information sharing system in case of IT crisis, as an extension of the system in normal times.
- Enhancement of incident response capability:** Overall enhancement of incident response capability by obtaining the full picture of exercises/training by stakeholders and mutual coordination.
- Risk management:** Comprehensive risk management support for CII operators, etc., including risk assessment.
- Enhancement of basis for CIIP:** Preparation, utilization, and international development of relevant international standards, regulations and references, etc.

- Expanding the scope of critical infrastructure from 10 to 13 sectors (with addition of chemical industries, credit card services, and petroleum industries).
- Showcasing the major points, e.g. “expectation for executive management”; making a list of CII operators’ sample measures based on the PDCA cycle and related governmental programs/activities.
- Developing objective assessment criteria and implementing periodic assessment and review based on these criteria.

In terms of the promotion of information security measures used by enterprises and people, it is critical to build awareness of the safe utilization of information and communications technologies without making trouble for other people. As to outreach and awareness raising on information security, various activities were promoted for the enhanced public awareness raising of information security, in addition to publicity activities using the homepages of the governmental bodies and relevant organizations as well as their information security related events.

With respect to the “Information Security Awareness Month” that has been implemented in February since fiscal year 2009, the first working day of this Month was designated as “the Cybersecurity Day” in the fifth celebration in fiscal year 2013, with the aim to raise public awareness more widely about the main idea of this Month. At the same time, creative approaches have been taken to make the activities people-friendly, by using PR tools such as the newly created “Information Security Outreach and Awareness Raising” logomark and animation videos (Figure 3-7).

Given the recent situation where cyberspace has growingly expanded and spread to all generations, in all places, and in all activities, the “Information Security Outreach and Awareness Program” (established in July 2011) was revised with aim to enhance national awareness of, understanding of, and response capabilities for information security, and the “New Information Security Outreach Awareness Program” was established in July 2014 (Figure 3-8).

Figure 3-7 Information security outreach and awareness raising activities

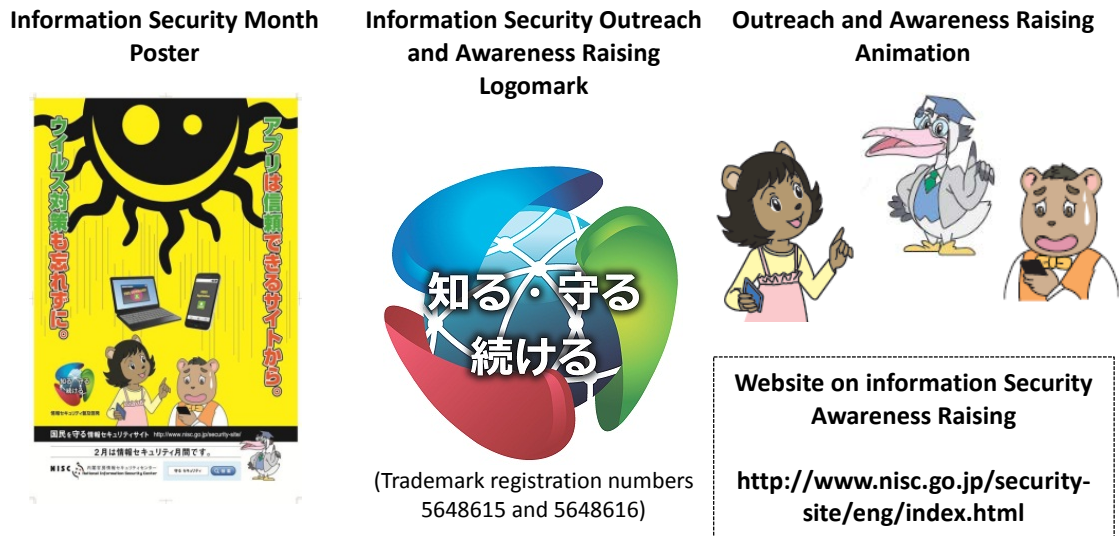


Figure 3-8 Highlights of the “New Information Security Outreach and Awareness Program”

Basic Ideas	<u>Enhancing and promoting nationwide awareness, understanding, and response capabilities of information security</u>
Promotion Scheme	<ul style="list-style-type: none"> - Creating a consortium consisting of multi-stakeholders from industry, academia, and the public-private sectors; and, establishing a scheme to promote outreach and awareness raising activities as a national movement. - Creating an environment which enables each stakeholder's self-motivating actions; and, promoting collaboration between citizens and their local communities.
Major Activities	<p>(1) Further promotion of comprehensive and focused outreach/awareness raising activities</p> <ul style="list-style-type: none"> • Expanding the “Information Security Awareness Month” period (from February to March 18 or “Cyber Training Day”) and raising public awareness widely. • Using PR tools, e.g. the logomark and the media throughout the year; promoting people-friendly activities; and striving to make them become common practice. • Promoting information security measures and training, etc. as a national movement so that citizens can protect themselves from cyber threats. <p>(2) Promotion of regional and local activities</p> <ul style="list-style-type: none"> • Promoting regional/local stakeholders' activities and information sharing; developing the consortium activities in collaboration among industry, academia, and the public-private sectors as nationwide movements. <p>(3) Promotion of extended outreach and awareness raising for vulnerable people</p> <ul style="list-style-type: none"> • In addition to the activities targeting the whole citizens, promoting extended outreach and awareness raising activities for vulnerable people (elementary and secondary education age-groups, people with less learning opportunity, people lacking interest in information security, enterprises including small and medium-sized enterprises, etc.); the consortium can be utilized for outreach/awareness raising activities tailored for the vulnerable groups.

Similarly, with respect to human resources development, the “Information Security Human Resource Development Program” (established in July 2011) was also revised and the “New Information Security Human Resources Development Program” was established in May 2014. This new program sets its goal to create a virtuous cycle of “supply” of information security experts to meet “demand” in Japan, and it incorporates activities aiming to: resolve the qualitative and quantitative shortages of information security professionals; and promote a culture of information security awareness among executive and senior management for the inclusion of information security in strategic business planning (Figure 3-9).

Figure 3-9

Highlights of the “New Information Security Human Resource Development Program”

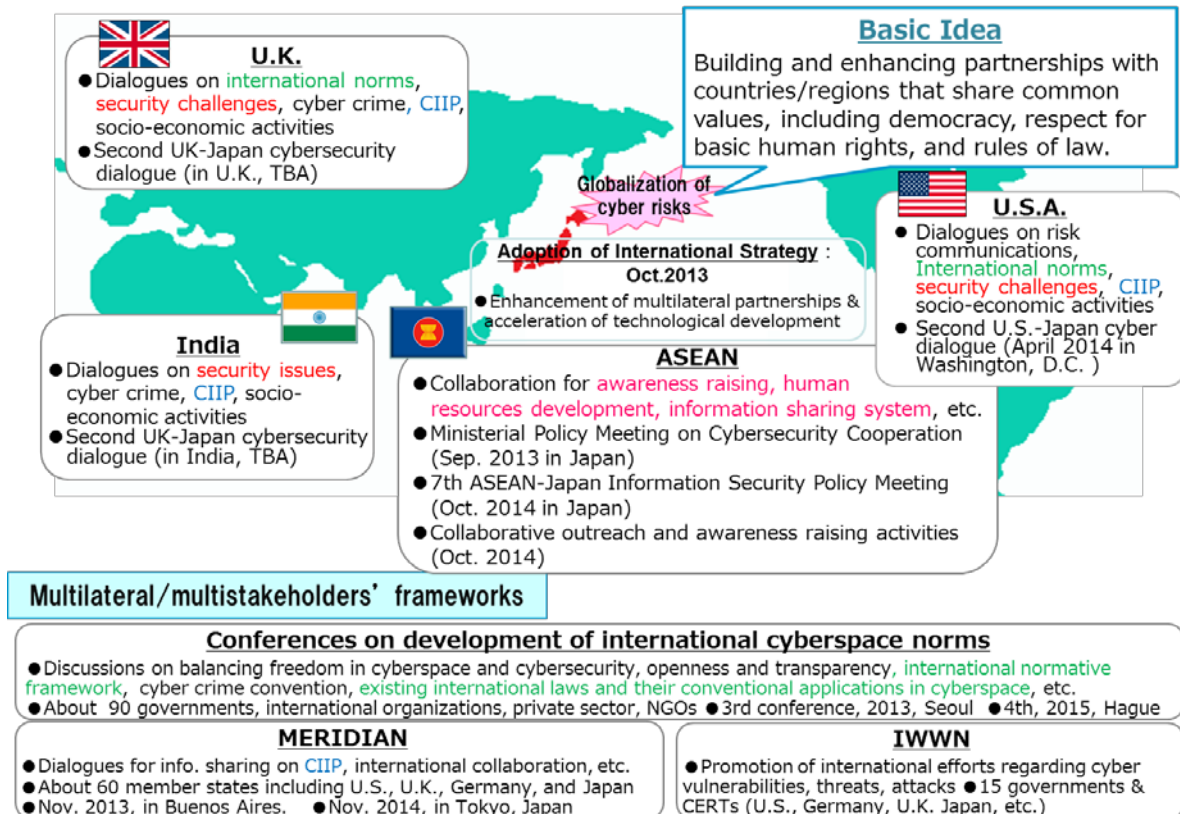
Main Objective	<p align="center"><u>Creating a virtuous circle of human resources <u>supply</u> and <u>demand</u> to improve the national level of information security</u></p>
[Demand] Information Security Awareness Raising among Executive Management	<p><u>Executive Management</u></p> <ul style="list-style-type: none"> ➤ Raising information security awareness for the incorporation of information security in strategic business planning. ➤ Encouraging investment to create human resources demand by setting out information security requirements in products/services procurement. <p><u>Leading Professionals</u></p> <ul style="list-style-type: none"> ➤ Strategic thinking on information security challenges and future directions, and building communication capabilities to facilitate relationships between executive management and professionals.
[Supply] Quantitative Expansion and Qualitative Improvement of Human Resources	<ul style="list-style-type: none"> ➤ Encouraging <u>existing IT engineers</u> to consider information security as essential capability, and carrying out reviews to create training materials and to establish performance evaluation criteria and a qualification system. ➤ Finding and nurturing <u>highly skilled and outstanding</u> human resources, and promoting their activities as cybersecurity experts in society. ➤ Creating human resources development environment by providing international learning opportunity and sharing information, for the purpose of developing <u>world-class human resources</u>. ➤ Enhancing employment, development, training/education of information security experts <u>by and in governmental bodies</u>. ➤ Enhancing practical IT education <u>in educational institutes/schools</u>, and promoting teacher training on information security.

With regard to research and development, the “Information Security Research and Development Strategy” (established in July 2011) was revised in July 2014, based on the analyses of the current environmental changes in cyberspace as well as the opinions of the Technological Strategy Special Committee. The revised strategy includes not only the review on R&D priorities but also the approaches for the improvement of detection and prevention capabilities against cyber attacks, the enhancement of security technologies to protect social systems, etc. (Figure 3-10).

Figure 3-10 Highlights of the “Information Security Research and Development Strategy”

Promotion policy of information security R&D	Priority issues of information security R&D (※ identified based on the promotion policy)
1. Improvement of capabilities to detect and defend against cyber attacks <ul style="list-style-type: none"> Strengthening collaboration among relevant bodies to share information, including information on cyber attacks, which are held separately and not yet shared. Sharing cyber-attack samples from the Government to researchers, etc. (to be considered) 	(1) Improvement of security of entire information and telecommunications system <p>Detection of cyber attacks, authentication, next-generation network security, etc.</p>
2. Reinforcement of security technology to protect social systems <ul style="list-style-type: none"> Promoting international standardization and certification system of security technology such as control systems. 	(2) Improvement of hardware and software security <p>Control system, devices, safety assurance of software, etc.</p>
3. Security R&D on new services which lead to industrial vitalization <ul style="list-style-type: none"> Promoting the inclusion of security quality in the upper process (R&D planning and designing stage) in the field of IT utilization, which is expected to be growing. 	(3) Realization of secured management of personal information, etc. <p>Privacy protection, utilization of personal data, etc.</p>
4. Maintenance of core information security technology <ul style="list-style-type: none"> In view of the creation of Japan's new industries, national security, etc., it is important to maintain and enhance core technology including cryptographic technology. 	(4) Establishment of R&D promotion base and creation of a new paradigm <p>Theory systematization, research and studies, standardization, evaluation, cryptographic technology etc.</p>
5. Enhancement of research and development through international collaboration <ul style="list-style-type: none"> Promoting international collaboration, for example, hosting foreign researchers, in order to integrate and progress “advanced” technologies of various countries. 	(5) Information security R&D in growth industries <p>Medical/ health, agriculture, next-generation infrastructure, Big Data, connected vehicle, etc.</p>
Approaches to advanced R&D effectiveness and achievement	
<ol style="list-style-type: none"> Promoting the utilization of R&D achievement for society Securing necessary R&D resources and flexibility Integrating information security technology and other fields such as social science 	

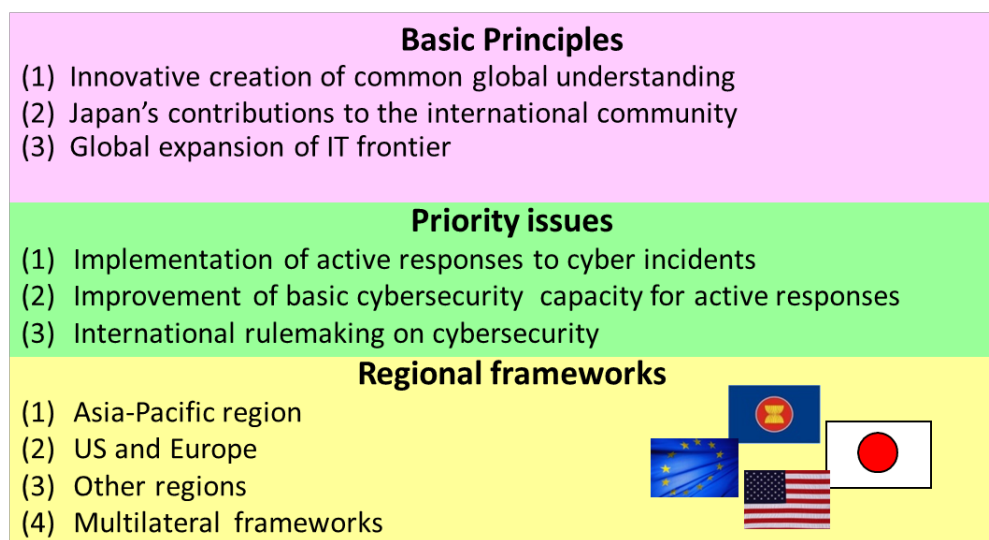
Figure 3-11 Achievements of international collaboration



In terms of international collaboration, in addition to the periodic “ASEAN-Japan Information Security Policy Meeting” and bilateral cyber meetings with the U.K. and India, a cybersecurity dialogue with the U.S. was held in fiscal year 2013. In particular, with respect to ASEAN, the “ASEAN-Japan Ministerial Policy Meeting on Cyber Security Cooperation” was held in Tokyo in September 2013, and the joint ministerial statement for the enhancement of cybersecurity was declared (Figure 3-11). Similar dialogues are scheduled to be held with other countries, including Russia, Estonia, Australia, and France. In this way, international partnerships have been substantially developed over the years.

In October 2013, in accordance with the “Cybersecurity Strategy”, the “International Strategy on Cybersecurity Cooperation”, which identifies the future directions of Japan’s international contributions towards enhanced international collaboration, was established. This international strategy indicates its aim to foster common global understanding of cybersecurity by using all occasions including the bilateral, multilateral, and regional frameworks and UN meetings, and demonstrates Japan’s commitment to active engagement in international collaboration (Figure 3-12).

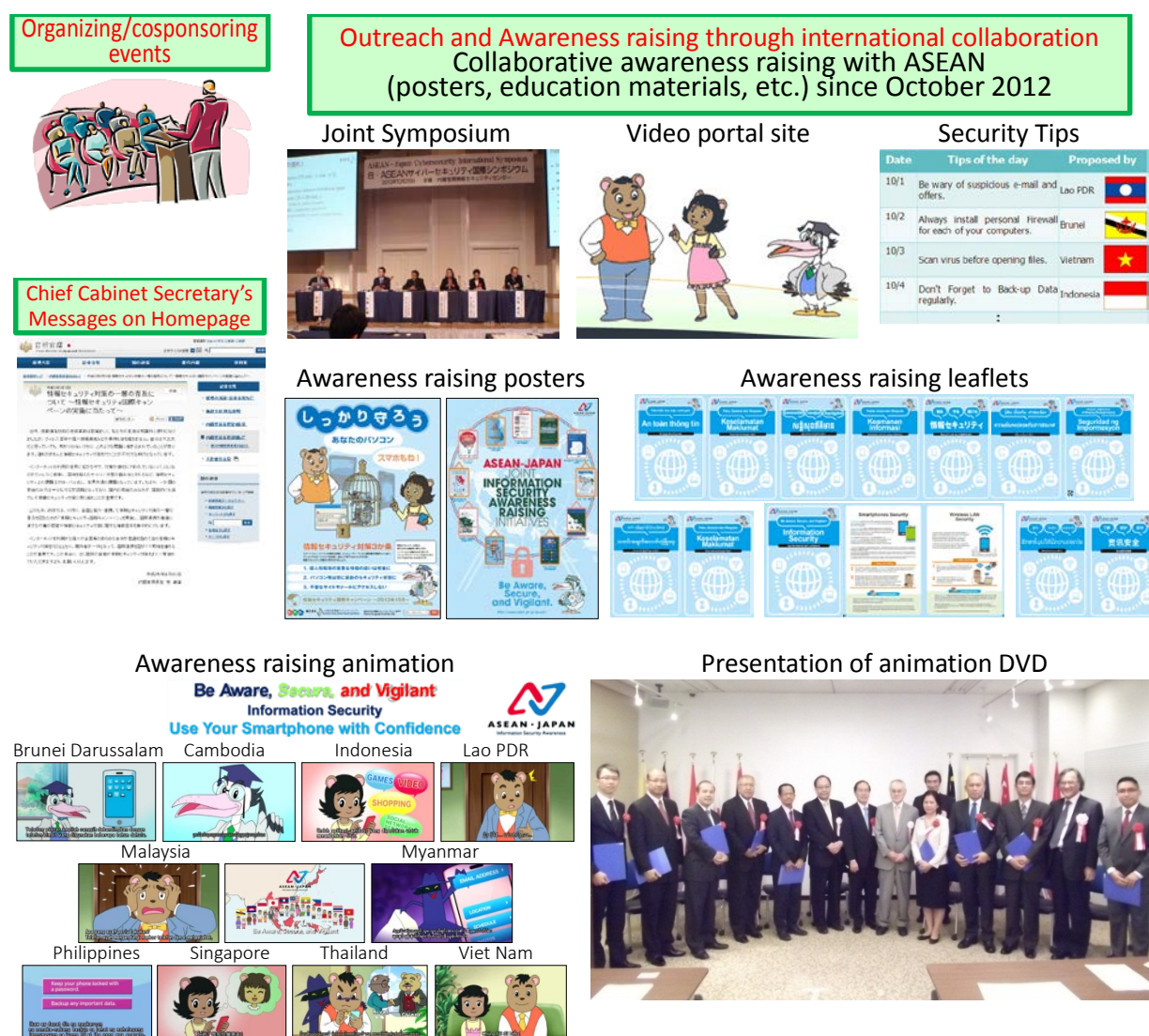
Figure 3-12 Highlights of the “International Strategy on Cybersecurity Cooperation”



Meanwhile, in order to tackle information security challenges in cooperation and coordination with foreign partners, the “International Cybersecurity Campaign” has been carried out every October since 2012. For further promotion of information

security measures in ASEAN countries, focused activities have been implemented, including collaborative awareness raising activities with ASEAN countries, international events organized by the governmental bodies and relevant organizations, and the provision of information on information security measures. In fiscal year 2013, in addition to the posters and the leaflets, the animation videos for awareness raising of smartphone information security (in Japanese, English, and with subtitles in ASEAN languages) and a video portal site were created (Figure 3-13).

Figure 3-13 Joint Awareness raising activities with ASEAN countries



The Information Security Policy Council has discussed a wide range of issues in its subcommittees and with relevant parties. In order to make the action plans concerning these issues more effective and more sustainable, it is required that professionals with various specialties take part in discussions in a cross-sectoral manner, deepen their mutual understandings, and strengthen coordination among them. Given that cybersecurity risks increase as socio-economic activities become more dependent on information and communications technologies, in pursuit of the world's most advanced IT-based society, it is indispensable to comprehensively and strategically promote the policies with a good balance between the promotion of IT utilization and the assurance of cybersecurity. From this viewpoint, the "Executive Panel on Security Strategy Promotion for IT Utilization" chaired by the Minister in charge of Information Technology Policy was newly created under the Information Security Policy Council, with coordination between the National Strategy Office of Information and Communications Technology and NISC, and the Panel has actively engaged in cross-sectoral discussions on necessary measures and activities.

4. Future Policy Directions

(1) Organizational enhancement to promote Japan's cybersecurity

Making NISC as the focal point, the Government has tirelessly worked to promote its information security policies in the Information Security Policy Council, and is now observing diverse demands for the reinforcement of its command center functions, in consideration of spreading cyber threats as well as the needs for improving national capabilities in organizing the Olympic and Paralympic Games coming to Tokyo in 2020. In this circumstance, for the purpose of enhancing the system to promote nation's cybersecurity (scheduled in fiscal year 2015), as illustrated in the "Cybersecurity Strategy", the Information Security Policy Council and relevant parties have engaged in a series of discussions since January 2014. At present, the following are the three major issues found in these discussions.

- i. Capacity building for incident readiness to expanding cyber threats: It is necessary to create a framework to make the knowledge and experiences accumulated in NISC available for the use by governmental and relevant entities; and, it is also necessary to strengthen the governmental system well in advance to prepare the Tokyo Olympic and Paralympic Games. For these purposes, further consideration should be given to: the reinforcement of the GSOC's functions; the enhancement of post-incident analysis functions to identify the causes of critical incidents; and, the development and deployment of cybersecurity human resources, etc. to conduct research and analyses on cybersecurity policies and cyber trends of other countries.
- ii. Need, expected role, and aim for government-wide functional enhancement: There is a need for the enhancement of inter-governmental cross-functional approaches in response to the proliferation of cyber threats; NISC should make active contributions to upgrade the security standards of the governmental bodies and other relevant parties; and, concerted efforts of relevant governmental bodies should be made to assure inter-governmental cross-sectoral effectiveness of their cybersecurity policies. To these ends, further consideration should be given to: the reinforcement of the governmental bodies' information security monitoring functions in accordance with the Common Standards of Information Security Measures for Government Agencies and other

relevant guidelines and regulations; the enhancement of the assessment function related to IT security investment, in collaboration with Deputy Chief Cabinet Secretary for Information Technology Policy, for the improvement of the identified matters, etc.; and, the advancement of the overall coordination functions regarding cybersecurity policies.

- iii. The needs for the enhancement of information gathering and international collaboration operations to respond to globalized cyber threats: From this viewpoint, further consideration should be given to such issues; the enhancement of functions for information gathering on cybersecurity incidents among the governmental bodies as well as among CII operators; the possible consolidation of multiple international contact points currently existing across the public and private sectors; and, the increase in personnel in charge of inter-governmental coordination.

During fiscal year 2013, several steps were taken to pass a cybersecurity legislation by the Diet¹⁶, and given that, discussions were made on the directions of the operational system reinforcement. For instance, it was discussed that it would be necessary to reorganize the Information Security Policy Council, currently under the IT Strategic Headquarters (or the Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society), as a headquarters stationed in Prime Minister's Cabinet; and that the new headquarters should be given legal authorities including those to conduct information security monitoring and examinations on the causes of critical incidents involving the governmental bodies, etc., to request governmental entities' mandatory submission of documents, and, to make recommendations to governmental entities. In addition, considerations were made on other issues including a need for establishing a new organ acting as a secretariat of the new headquarters.

Based on these discussions, the Information Security Policy Council undertakes further debates for the establishment of the "Policy directions for the functional enhancement of the system to promote Japan's cybersecurity" (Figure 4-1).

¹⁶ A cybersecurity bill was passed on June 13, 2014 by the Lower House and was sent to the Upper House that decided on June 20 to carry it over to the next legislative session.

(2) Promotion of other cybersecurity policies

For the systematical promotion of the cybersecurity policies, the annual plans have been periodically adopted and implemented in line with the “Cybersecurity Strategy” that is a medium-term plan covering about three years. In fiscal year 2014, based on the results of activities implemented during fiscal year 2013 and other relevant factors, the “Cybersecurity 2014” was established in July. In line with this annual plan, the governmental bodies will make a concerted effort to promote specific cybersecurity policies (Figure 4-2).

For example, with regard to countermeasures concerning the governmental bodies, while the cloud-based services had been considered as a form of outsourcing in the set of the Common Standards of Information Security Measures for Government Agencies, it was pointed out that these standards could not be considered as applicable standards for the diversified cloud services such as SaaS, PaaS, and IaaS. In addition, foreign governments have begun to set out the requirements of cloud-based services for government procurement. Given that, the Government will make its effort to carry out activities for examining necessary information security requirements in the use of these services, taking into account a characteristic of the services that the location and the management status of information are critical from a security perspective but hard to be known by users of the diversified cloud-based services.

Moreover, aiming at improving Japan's information security environment, as for CII, the Government makes its effort, for example, to develop the information sharing system of the newly added three sectors, i.e., petroleum industries, chemical industries, and credit card services; and, as for human resources development, the Government promotes activities including those to increase the strategic awareness of information security at the board level that has a strong influence on organizational information security management, including the recruitment of cybersecurity specialists.

Figure 4-1 Summary of the “Policy Directions for the Functional Enhancement of the System to Promote Japan’s Cybersecurity” (proposal)

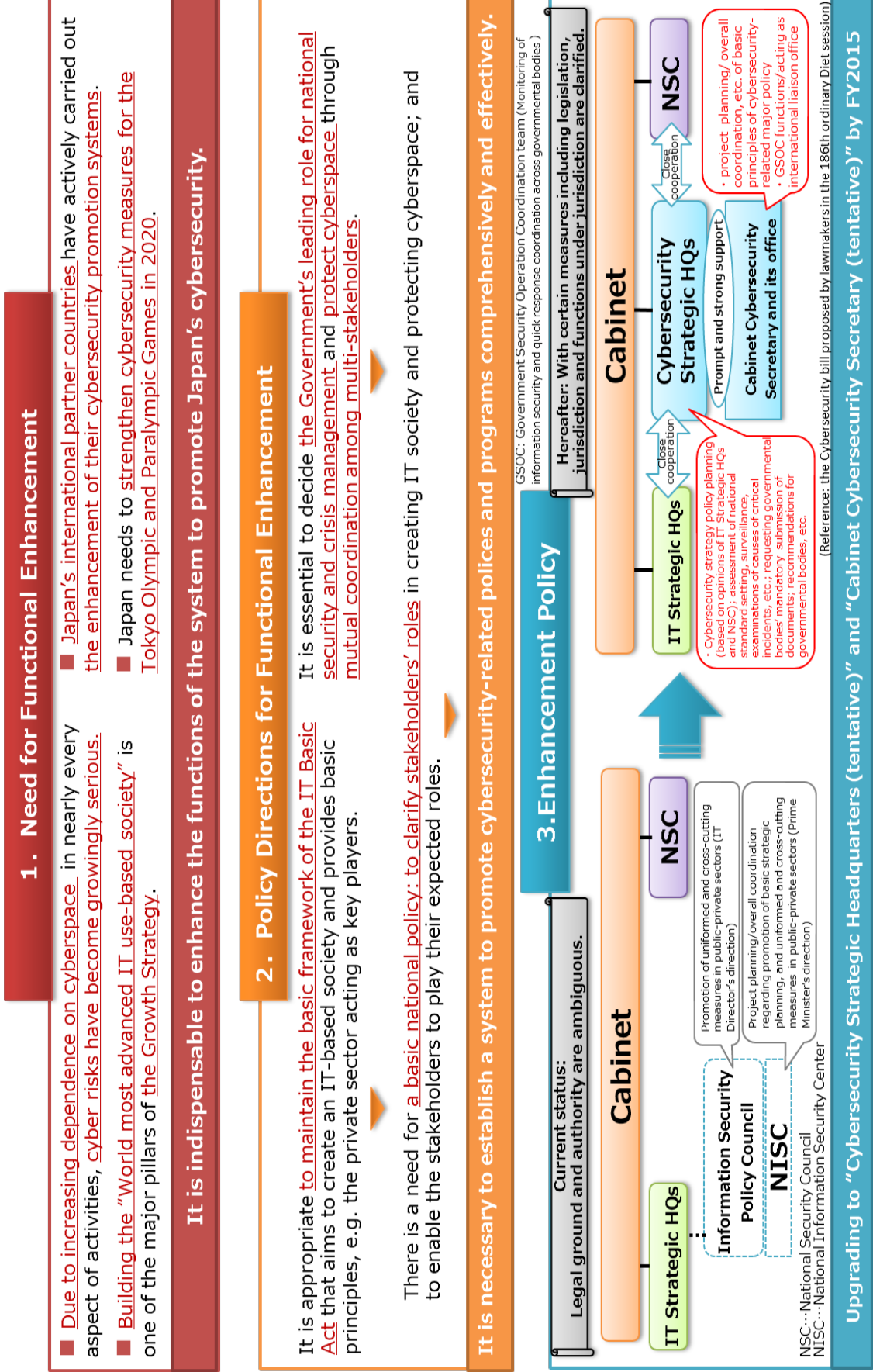
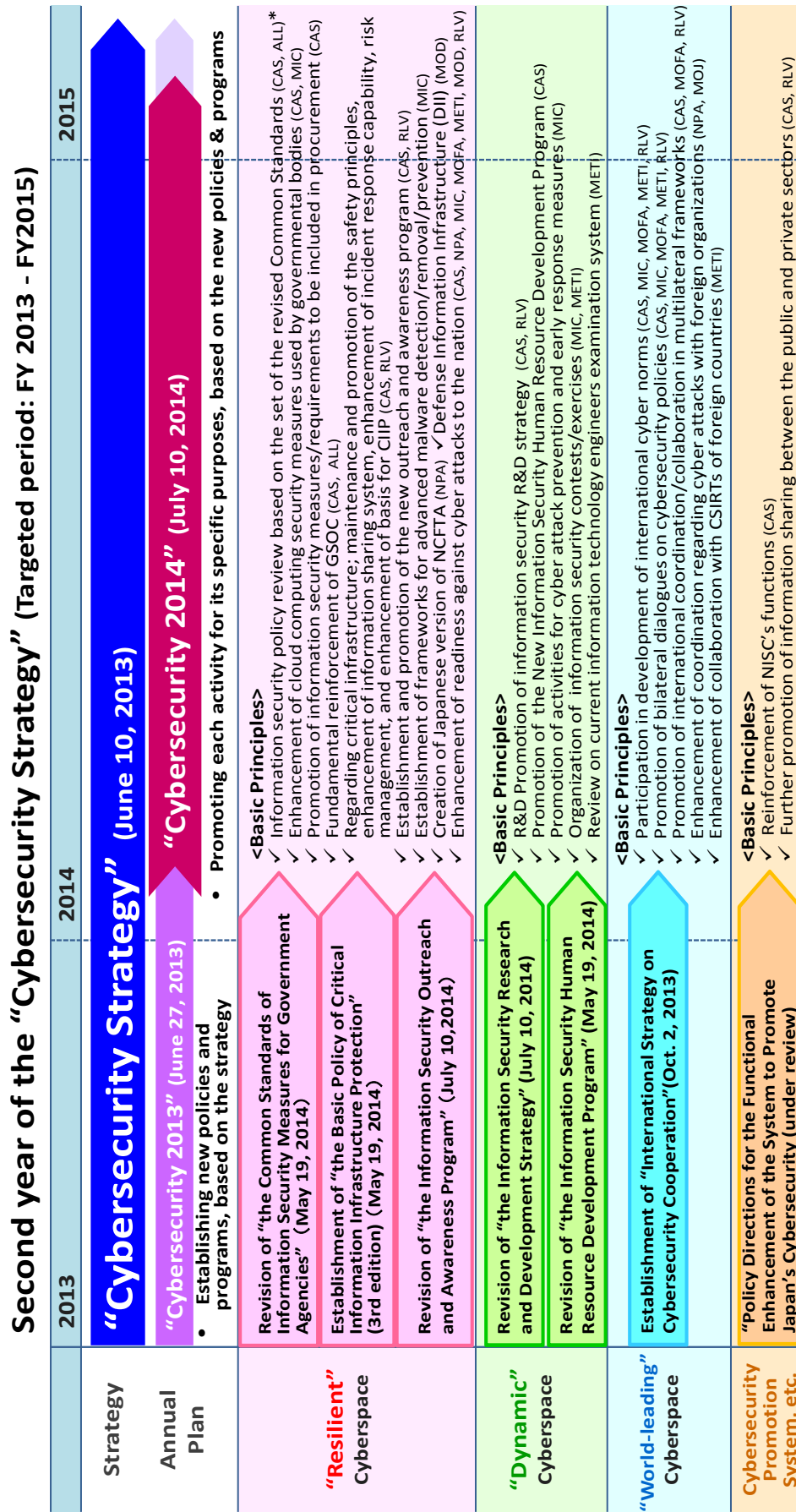


Figure 4-2 Outlines of the “Cybersecurity 2014”



* CAS:Cabinet Secretariat; MIC:Ministry of Internal Affairs and Communications; METI:Ministry of Economy, Trade and Industry; NPA:National Police Agency; MOD:Ministry of Defense; MOFA:Ministry of Foreign Affairs; MOI:Ministry of Justice; ALL: All governmental bodies; RLV: Relevant governmental bodies