Information Security Research and Development Strategy

July 8, 2011
Information Security Policy Council

CONTENTS

1 Preface

Japan's information security policy is based on the "Information Security Strategy for Protecting the Nation" (released by the Information Security Policy Council on May 11, 2010; hereafter, "Information Security Strategy") and its annual plan, "Information Security 2010" (released by the Information Security Policy Council on July 22, 2010; hereafter, "Annual Plan") and is pursued by alliances between the public and private sectors.

Research and development concerning information security is referred to as follows: "Information Security Strategy" states, "To strategically propel information security research and development, taking account of US movements, formulate a new information security research and development strategy"; and the Annual Plan states, "In order to strategically promote information security R&D, a new information security R&D Strategy is to be formulated with June 2011 as the target." The "Information Security Research and Development Strategy" (hereafter, "R&D Strategy") will be formulated accordingly.

Research and development concerning information security is closely connected with Japan's science and technology strategy. The Report to Consultation No. 11, Regarding the Basic Policy on Science and Technology (by the Council for Science and Technology Policy on (December 24, 2010), which forms the basis of the "Fourth Science and Technology Basic Plan" (hereafter, "Fourth Basic Plan") for the next five years (from FY2011 to FY2015), expresses the "promotion of research and development of active and dependable information security technologies" as a measure for "conserving the basis of the nation's existence" under "Promotion of measures for accomplishing critical tasks." This R&D Strategy is regarded as the basis for realizing the science and technology strategy.

Although the period subject to this R&D Strategy is specified basically to FY2011 to 2015, in order to ensure consistency with the Information Security Strategy and the Fourth Basic Plan, the strategy includes medium and long-term tasks so that R&D can be promoted strategically.

For the promotion of such R&D Strategy, the Technological Strategy Special Committee regularly evaluates all measures, including alliances between the public and private sectors and international alliances, and reviews the contents when necessary.

2 Previous Efforts

(1) Background

In 2005, when the Council for Science and Technology Policy was formulating the Third Science and Technology Basic Plan (hereafter, “Third Basic Plan”), technological strategies focused on information security were discussed, and the “Report from the Technological Strategy Special Committee” was produced in November 2005.

The promotion strategies specific to the information and telecommunications sector in the “Third Basic Plan” decided on by the Cabinet in March 2006 included a variety of measures presented in the report and ranked information strategy as one of priority science and technology fields.

Then, follow-ups to reflect the latest trends and overviews of the implementation state of R&D into information security technologies in Japan were made, and the “Report 2006 from Committee for Security Technology Strategy” was produced in June 2007, and the “Report 2008 from Committee for Security Technology Strategy” was produced in April 2009. R&D into related technologies has thus been conducted on the basis of these reports.

(2) Goals of Information Security Technology Development in the Past

Two major goals were specified in R&D into information security technologies in the past.

One goal was the development of technologies for measuring risks accompanying currently operated information systems and for reducing risks and bringing such risks closer to zero.

Another goal was R&D into technologies for implementing a new architecture for simulating threats and removing risks in information processing systems and networks, with medium and long-term targets.

The environment in which advanced information and telecommunications networks can be used safely has been defined as follows:

[1] To begin with, advanced information and telecommunications networks should be safe.

[2] Users should be able to perceive that advanced information and telecommunications networks are safe.

[3] In the event of an incident, the damage should be confined, assistance provided, and

business continuity maintained.

R&D of technologies serving those purposes have thus been promoted.

While R&D into those technologies is in progress, new problems emerge year by year. For example:

[1] With the rapid spread and sophistication of information appliances and devices and with the diversification of services, the nation's dependence on ICT has increased, and the range of issues concerning information security has expanded greatly. Development of information security technologies cannot keep up with the rapidly expanding usage and application of ICT.

[2] Increasing malware, accelerated discovery of vulnerabilities, and accelerated development of attack methods have increased the number of problems that cannot be resolved by conventional information security measures.

[3] Organizational or human management methods that should compensate for limitations of existing information security technologies are not well balanced. In spite of changes in the generational structure, such as aging, improvements of services and products made to facilitate usability and prevent user's mistakes from leading to high risks are not sufficient.

Viewed from the life cycle of information systems, solving problems concerning information security for evolving information system architectures from one generation to the next is like trying to hit a moving target. More specifically:

- Transition to a new-generation architecture changes the risks and also changes the target values of system availability and business continuity dynamically.
- Newly introduced technologies or system components change the risk.
- Attackers can always attack target systems by using new technologies, putting defenders at a great disadvantage.

The combination of the factors given above always changes the surroundings of the problems. In these circumstances, information system architecture and development, operation, and maintenance processes that can resolve those problems must be established, and in the end, [1] information resources and information processing must be protected, and [2] smooth business continuity must be ensured.

Since 2005, research and development concerning information security has been conducted to resolve those problems under the banner of "Grand-Challenge project for R&D and technology development." The growing problems of recent scientific and technological studies include fractionalized or radicalized research fields causing short-term objects to be set, and relations with other research fields are left out of consideration. As a solution to such problems, the "Grand-Challenge project for R&D

and technology development" sets a huge goal, taking research and development that would continue for the long term, ten years, for example, into consideration, and research and development of the constituent technologies is conducted to achieve this major goal in an integrated manner.

Since it is predicted that the problems described earlier are likely to become more complicated and more diverse, a new R&D Strategy, including the concepts described above, is formulated here.

3 Environmental Changes Concerning Information Security

(1) Changes in the Environment Surrounding Japan's Information Security

[1] Innovative ICT

Cloud computing (or simply, "the cloud") using virtualized computer resources, ubiquitous terminals, and systematized advanced embedded software have made remarkable progress in recent years, and such progress will accelerate in the future. It is also presumed that trends towards enhanced real-time sensing functionality using a variety of sensors installed in homes and offices and Context Awareness,[1] making use of positional information and user information, will also accelerate. Moreover, new communication services, such as smartphones and social network services (SNSs), are rapidly spreading.

It may be hard to predict the trends of rapidly changing ICT, but it is believed that ubiquitous techniques, techniques that merge real and virtual worlds, and the like will grow further. Information security technologies supporting this new ICT are now demanded.

[2] Sophisticated and Diversified Threats against Information Security

Threats concerned with information security, such as large-scale cyber attacks, large-scale system failures, and massive leakages of personal information have been scaled up and have become more sophisticated and complex. This obviously rising tendency can be presumed from the increasing variety of types of computer viruses.

Representative examples of new types of attacks include the Operation Aurora[2] attack and the attack by the Stuxnet[3] virus. These attacks are elaborate combinations of existing attack methods that can avoid general protection systems, and are designed for specific targets. A new threat called APT (Advanced Persistent Threat[4]) has also

---

[1] Concept in which computers can automatically recognize changes in circumstances through sensors or networks and can respond to such changes.

[2] Cyber attack that gains control of an end-user's computer by a "zero-day attack" aiming at vulnerabilities in Internet Explorer, breaks into the system of a specific enterprise by remote control, and commits espionage or theft of intellectual property.

[3] A computer virus that infects a Windows PC by utilizing a plurality of vulnerabilities, breaks into the control system of a nuclear power plant, and attacks a unit on the control system. The virus was devised to affect the control system of the nuclear power plant by writing malicious code into a programmable logic controller (PLC) of Siemens AG (Germany), capitalizing on vulnerabilities in the WinCC/Step7, software of the PLC.

[4] An adversary that possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors. These objectives typically include establishing and extending footholds within the information technology infrastructure of targeted organizations for the purposes of stealing information; undermining or impeding critical aspects of a mission; or positioning itself to

emerged. Other new threats include threats against the rapidly growing number of smartphones and threats against cloud computing, which has been attracting attention as a new business model.

There is also a black market: Tools that can easily create malware are traded, and stolen certification information and credit card information can be turned into money. Adversaries that are believed to be profit-making parties have been appearing on the scene.

This situation indicates that the attacker's advantage over the defender still remains in cyberspace and may even have been reinforced. How to relieve and resolve the situation is a major issue.

③ Great East Japan Earthquake

The Great East Japan Earthquake (hereafter, "the Great Earthquake") was an unprecedented and complex disaster. The large-scale earthquake, giant tidal wave, and accidents at the nuclear power plant, etc. have seriously damaged the community and economy of not only Eastern Japan, but the whole of Japan. The existing information communications infrastructure suffered devastating damage, and the interruption of communications delayed rescue and recovery operations and made people very concerned. The interrupted distribution of information, which forms the foundation of so many socioeconomic activities, have caused delays to variety of activities. On the basis of the experience of the Great Earthquake, a disaster-resistant information and telecommunications system should be studied and re-constructed by reinforcing the backup system and emergency power sources and by making use of cloud computing, and business continuity plans (BCP) must be seriously reviewed.

Dynamic changes triggered by the Great Earthquake have changed the way that society views risks and the permissible levels of such risks. In the event of a disaster, it is important to have the idea of dynamic risk management for adapting optimally to changing conditions. The importance of risk communication and risk management has been recognized again, but knowledge in this field is not sufficient at present. Immediate action should be taken.

(2) Changes in Information Security R&D Budgets

Japan's information security R&D budget was 9.12 billion yen in FY2006 and 4.86 billion yen in FY2010, showing a dramatic reduction of about 47% in the five years.

---

carry out these objectives in the future (NIST SP800-39 "Managing Information Security Risk: Organization, Mission, and Information System View" [Appendix B GLOSSARY]).

The R&D budget of the United States was on the rise from FY2007 to FY2011. The increase in the five years was about 91%, and the budget in FY2010 was 36.6 billion yen (407 million dollars).[5]

In FY2007, the budget of the United States was 19.2 billion yen (213 million dollars), and the budget of Japan was 7.71 billion yen. The budgets of the two countries as a percentage of GDP were almost the same. In FY2010, the United States increased its budget to 36.6 billion yen while Japan decreased its budget to 4.86 billion yen, and the difference as a percentage of GDP is a factor of 3.02.

While overseas countries focus on R&D for information security, Japan's situation could only be described as alarming.

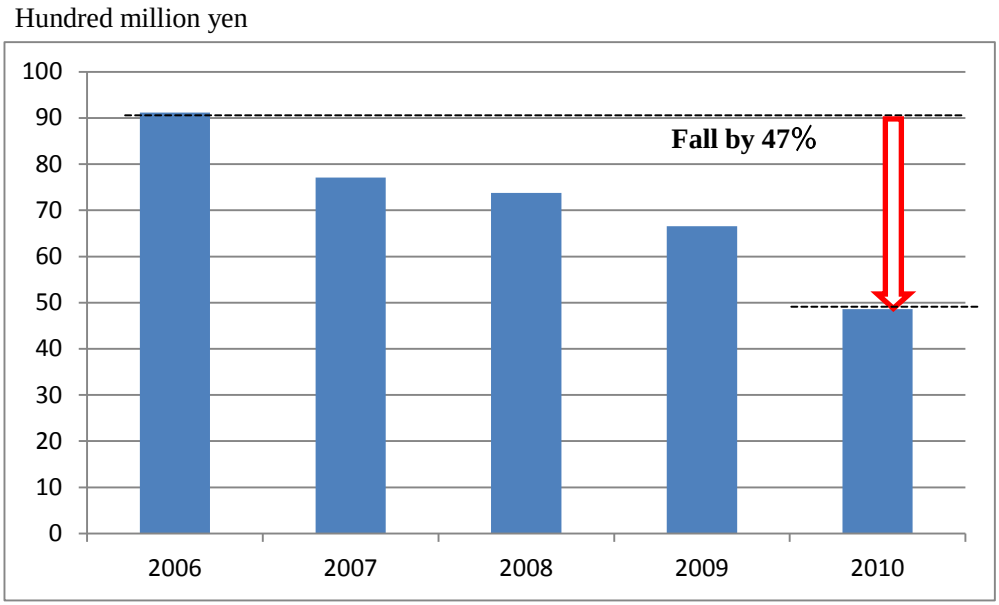


Fig. 1 Changes in Japan's Information Security R&D Budget[6]

Hundred million dollars

[5] Converted at an exchange rate of 90 yen to one dollar.
[6] Based on the FY2009 Follow-Up Survey by the Expert Panel on Basic Policy, the Council for Science and Technology Policy.

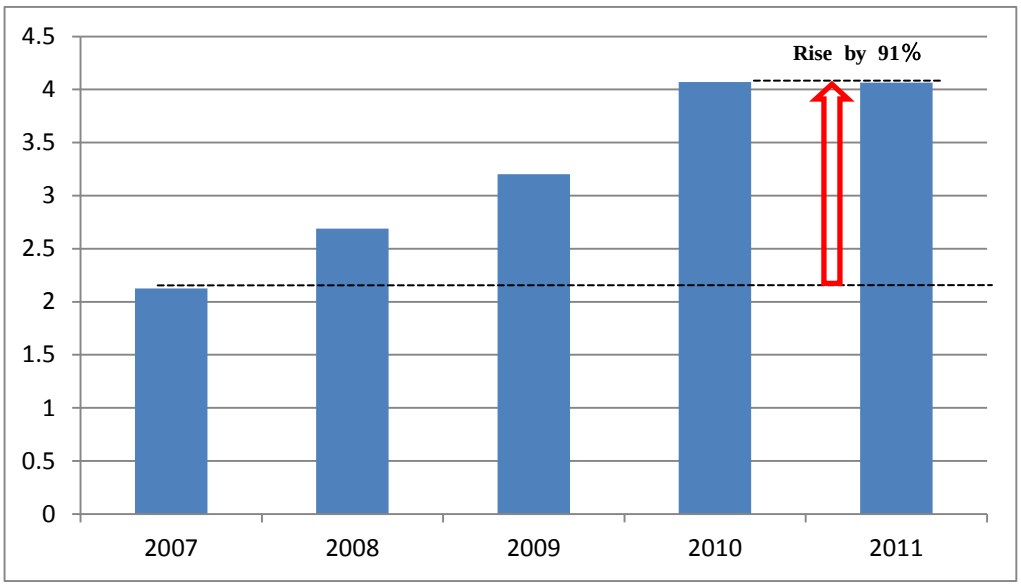


Fig. 2 Changes in Information Security (NITRD CSIA) Research Budget in the US[7]

	2007	2010
GDP (US/Japan)	2.12	2.49
Percentage of R&D budget (US/Japan)	2.48	7.53
Percentage of R&D budget in relation to GDP (US/Japan)	1.17	3.02

Fig. 3 Percentage of R&D Budget in Relation to GDP in Japan and US

(3) R&D Strategies in Overseas Countries

[1] R&D Trends in the United States

A variety of government agencies in the United States are concerned with R&D of information security from aspects of enhancement of competitiveness of the information and communications industry, national security, and so on, and each government agency has its own specific research field and budget scheme. The federal government thus coordinates the government agencies to formulate an effective federal R&D Strategy.

A budgetary procedure based on a top-down policy, a budgetary procedure based on the technical reasons for conducting actual research and development, and bottom-up examinations, such as adjustment of research fields based on the technical

[7] Based on NITRD supplementary material for the Budget Message.

reasons for conducting actual research and development, and coordination among organizations are repeated to select studies based on needs on the ground, and quick responses can be made to dynamic changes in society. (See Reference Material 4.(1)).

[2] R&D Trends in EU

In the EU, the objects of R&D in the information and telecommunications fields are to reinforce the competitiveness of the European information and communications industry and to spread ICT in the European region, and programs focused on socioeconomic aspects have also been set up. Accordingly, major subjects of study concerning information security are tools, standards, metrics, evaluation methods, best practice, and other topics with a view to commercialization. Their research schemes incorporate systems for reinforcing their competitiveness and for spreading ICT, such as the establishment of strategic ties with regions outside Europe, R&D aid for small-to-middle sized businesses, and the publication of results to the public. (See Reference Material 4.(2).)

4 Information Security R&D Strategies

(1) Principles

R&D and technology development concerning information security has been promoted in accordance with the “Report from the Technological Strategy Special Committee,” however, a new R&D Strategy will now be formulated with recent environmental changes and trends in overseas countries taken into consideration. Since the R&D strategies are medium and long-term subjects, the new R&D Strategy basically includes conventional promotion concepts. The new strategy also contains new R&D subjects to respond to novel environmental changes and places an emphasis on them.

Although the goal of conventional R&D and technology development has been “implementing a new architecture for removing risks in the medium and long-term,” attackers and defenders have become asymmetric in recent information security circumstances. In other words, the advantages of the attackers have not yet been removed. The most distinctive feature of this R&D Strategy is to focus on innovation to manifest a “Game Change” from the attacker’s advantage to the defender’s advantage. In other words. R&D concerning information security can be roughly divided into the offensive field and the defensive field (to minimize damage by cyber attacks). This R&D Strategy focuses on the offensive (to invalidate cyber attacks and to increase the economic burden placed on the attackers), and to promote R&D to realize a safe and secure information communications system that can create new value and can support the society.

For the promotion of R&D, it is important to take active steps to create a virtuous circle of leading R&D, encourage advanced information security human resource development, and stimulate the information security industry.

The Great Earthquake has raised a large question, what science and technology should actually be. To contribute to rehabilitation, reconstruction, and renewed growth, priority is given to R&D of items closely connected with information security, such as new dependable information and telecommunications systems, risk management, and risk communication, for improving safety and security in the event of disaster.

The principle of the R&D Strategy is as follows:

[1] R&D concerning active and dependable information security (hereafter, “New Dependability”)(Note) is promoted. By switching from passive study following

threats on information security to active study to remove the imbalance in cyber attacks, cyber attacks will be invalidated, and by facilitating an innovation (so-called “Game Change”) that increases the economic burden on the attacker, Japan can lead the world. Especially, it is very important to secure the New Dependability of the entire information system.

(Note) One of the main focuses of conventional information security was incidents based on human wrongdoing. As the degree to which society depends on ICT has increased, the object needs to include all related types of occurrences, such as natural phenomena, aging degradation, and human error. New Dependability includes active information security factors, such as disabling cyber attacks, supplementary to the issues covered by the former dependability.

[2] To improve safety precautions against disasters, R&D for creating a disaster-resistant information and telecommunications system in terms of information security and R&D concerning risk management or risk communication is to be promoted.

[3] “Green innovation” and “Life innovation” are ranked as central pillars for Japan’s sustainable growth in the future. To ensure these innovations on the society level, ICT is essential, and particularly, the establishment of an advanced information security infrastructure is very important. R&D for building an advanced information security infrastructure will be promoted in coordination with R&D supporting social innovation.

[4] To resolve the problems of information security thoroughly, cooperation with innovative R&D for the next-generation Internet that realizes a paradigm shift in ICT, for example, is to be built up. This is related also to [1] above. Active contributions are to be made to new topics of study in the science and technology field, in order to solve problems concerning information security.

[5] R&D concerning information security will be promoted to contribute to the global expansion of Japan’s information security industry.

[6] Each country conducts strategic R&D concerning information security in a society in which information is exchanged across borders, and problems that cannot be resolved by a single country have been increasing; thus, further international alliance are being encouraged.

[7] In the promotion of R&D Strategy, the division of roles played by the public and private sectors are to be clarified, and alliances between the two sectors will be encouraged through the market mechanism. R&D will be evaluated appropriately, and efforts are to be made to ensure sufficient budget and to provide motivation in each phase of R&D.

Fig. 4 Principles of the Information Security R&D Strategy

Principles

[1] Facilitation of innovation to switch to active study that removes the imbalance in cyber attacks (disabling cyber attacks and increase economic burden on the attacker).

[2] Promotion of studies to create a disaster-resistant information and telecommunications system in terms of information security and studies concerning risk management and risk communication.

[3] Promotion of R&D for building an advanced information security infrastructure in coordination with R&D supporting social innovation.

[4] Cooperation in innovative R&D for next-generation Internet.

[5] Contribution to global expansion of Japan’s information security industry.

[6] Promotion of international alliances in R&D.

[7] Promotion of cooperation between the public and private sectors and clarification of their roles. Efforts are to be made to ensure sufficient budget and to provide motivation in each phase of R&D.

(2) Concepts of R&D Strategy

The R&D Strategy focuses on a “Game Change” to increase the economic burden of the attacker by taking aggressive steps, such as by invalidating cyber attacks, and promotes R&D for realizing a secure and safe information and telecommunications system that can create a new value as an infrastructure supporting society. For that purpose, the subjects of R&D are classified roughly into attackers, the information system, users, and surrounding infrastructure, as shown in Fig. 4, and necessary technologies are mapped out accordingly. Further, information security that protects the information system from cyber attacks, in the narrower, conventional sense, is being combined with a new perspective of supporting the next-generation Internet environment in a broader sense. The latter corresponds to technology for ensuring: [1] New Dependability of the entire information system, and the former corresponds to [2] Zero-Day Defense based on the attacker’s behavior analysis. Users should also improve their techniques of [3] user control of personal information in terms of the methods of managing organizations and human resources. Since one object of the R&D Strategy is to stimulate information security studies, [4] establishing an infrastructure for stimulating research and development is also an important concept.

These four concepts are described in more details below.

[1] New Dependability of the entire information system

To clarify technologies that are needed to realize an active and dependable information system, environmental changes related to information systems must be considered. In the social system based on the next-generation Internet, a cyber physical system (CPS) is expected to be realized with advanced cloud computing and virtualization, more ubiquitous terminals, enhanced real-time sensing functions, and context awareness (actively collecting and processing physical statuses using sensors) and utilizing positional information. In the CPS, ties between the real and cyber worlds will be strengthened more firmly than ever. Since high reliability will be demanded of such systems, including sensors that connect the computer with the real world, and control devices, technologies for building a new dependable information and telecommunications system are required.

[2] Zero-Day Defense based on the attacker’s behavior analysis (advance defense)

The role of “information” in socioeconomic activities has increased, and the factors concerning incidents of leakages of national secrets, the intellectual properties of enterprises, and personal information from corporations have become diversified and more complex. Although cyber attack methods tend to become more complicated and subtle, measures against cyber attacks are lagging behind, so that a fundamental solution to correct the present situation should be pursued. Therefore, advance defense technologies are required to optimize measures by profiling the internal attackers that are causing leakages of information and external attackers working through networks, based on behavioral observations, analyzing behavioral models based on incentives and game theories, and pinpointing threats from the attackers’ behavioral prediction models.

[3] Flexible management of personal information

Although personal information, such as positional information and life logs, will be put to expanded use in the future, a simple either-or decision, whether to provide such personal information or not, can be made at present, and it is difficult to legitimately utilize such personal information in an effective manner. In addition, stakeholders related with information systems have diversified, and both users and vendors have a variety of levels of awareness and skills concerning information security. Therefore, technologies for improving user-controlled capabilities in accordance with this diversity, such as a balance between active utilization and protection of personal information, are required.

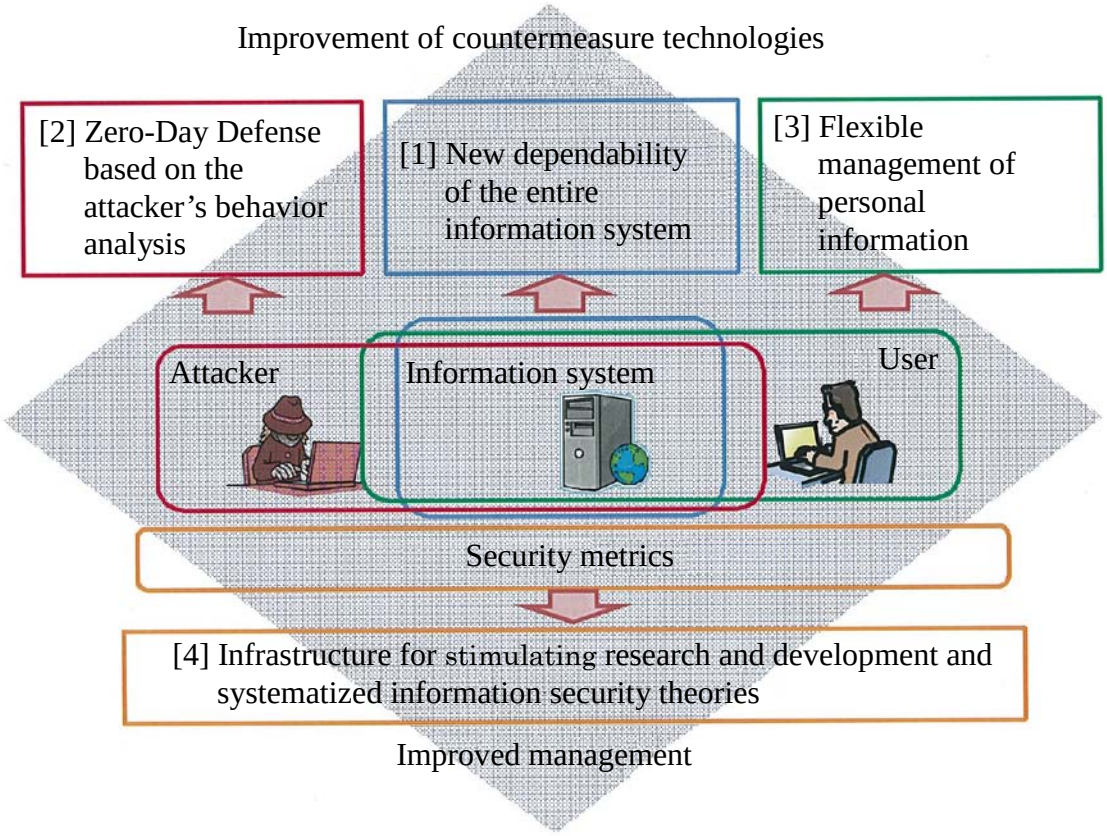
[4] Infrastructure for stimulating research and development and systematized information security theories

The current R&D into information security is a collection of know-how on measures corresponding to individual risks. Since information security technologies are not logically organized, there is little hope for further progress. Through objective evaluations of studies, better studies and an appropriate spreading method can be clarified.

Data from demonstration studies is needed to confirm that a theoretical study is correct. For that purpose, the following are required: standardization and provision of data for such demonstration studies, establishment of an evaluation system for making studies more efficient, and the development of cryptographic technology forming the basis of these studies.

Fig. 5 Important Concepts

Concepts



(3) Types of R&D Investment

R&D investment by the government is examined from two angles: [1] success rate of the project, and [2] R&D period, which are the same in the Europe and the United States. Those angles are closely related with the R&D budget. In accordance with these two angles, types of R&D investment that require government support are divided into three groups. By dividing the important topics of R&D concerning information security into the three groups, strategic promotion of R&D under corresponding time frames will become possible.

[1] Emergency response investment

Concerned with R&D projects that consider rapid responses to new needs and

threats brought by environmental changes. Because of the clear needs, the success rate of such projects is high, and the study period is generally short. However, some projects that require large-scale trials need government support to advance the study.

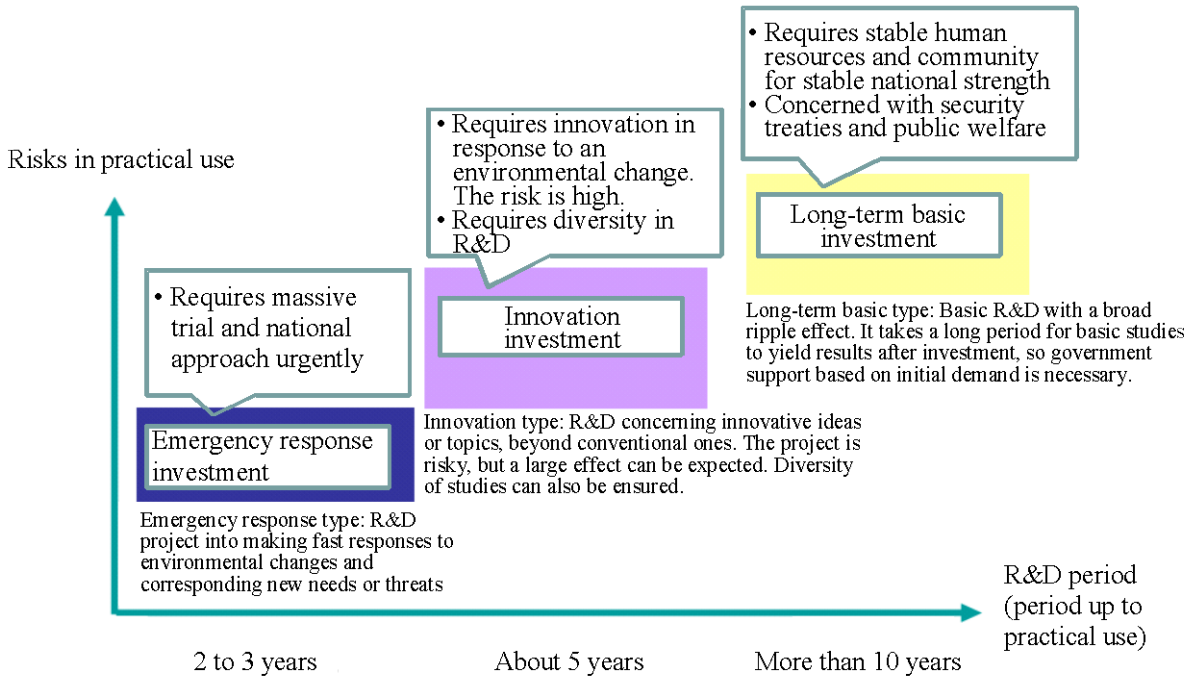
[2] Innovation investment

For R&D project concerning an innovative idea or topic, that differ from conventional areas. Since an innovative topic is being studied, the project is risky, but a large effect can be expected if the project succeeds. This type of project requires government support to ensure a diversity of studies.

[3] Long-term basic investment

For basic R&D projects concerned with nurturing stable human resources and communities for enhanced national strength. These projects are somewhat risky and have a broad ripple effect. Generally, it takes a long time for the basic study to yield results after receiving investment, so government support is necessary.

Fig. 6 Types of R&D investment



5 Important Subjects in R&D into Information Security

In terms of the principles for R&D Strategy, subjects that are expected to become important in the future are listed in Fig. 7 below:

.

New Dependability of the entire information system	
[1]	Information security infrastructure technology for next-generation networks where the real world and the virtual model in the computer are combined
[2]	Technology for maintaining a consistency of security configurations between layers automatically
[3]	Technology for building a computer network architecture that can perform automatic recovery from failures
[4]	System design technology for combining biometrics information with ID management under control of a computer
Zero-Day Defense based on attackers' behavior analysis	
[5]	Preventive base technology using attackers' behavior analysis
[6]	Combination of a wide-area observation technology in a large-scale network and malware behavior analysis technology
Flexible Management of personal information	
[7]	User control technology of personal information for promoting utilization
[8]	Data control/pursuit technology for supporting forensics
[9]	Systematization of theory-to-practice concerning IT risks
Infrastructure for stimulating research and development and systematized information security theories	
[10]	Systematized basis for information security studies
[11]	Product evaluation certification technologies for ensuring correct implementation of security components
[12]	Theoretically secure cryptographic technology

Fig. 7 Important Subjects in R&D into Information Security

(1) New Dependability of the Entire Information System

The social system realized on the basis of the next-generation Internet will have closer ties between the real world and the cyber world than ever before. People will be surrounded by a variety of sensors, and a variety of situation within actual society will be sensed and incorporated into the information space. At the same time, the data in the

information space will be reflected back to real society through control systems. Since high reliability is demanded of the information and telecommunications systems, including sensors that connect the real world and the virtual model in the computer and control devices, technologies for building a New-Dependable information and telecommunications system are required.

Such sensor network and actuator networks are too large to perform centralized control of their collaborative operations. In order to maintain a large-scale sensor network, it will be necessary to establish, operate, and control local networks autonomously. In addition, local networks should have self-innovation capabilities to make mutual connections among themselves. Further, an autonomous distributed collaboration function is required to transmit information freely and autonomously on the network.

Important subjects are as follows: [1] Information security infrastructure technology in next-generation network where the real world and the virtual model in the computer are combined; [2] Technology for ensuring all the security settings of a system automatically; [3] Technology for building a computer network architecture that can perform automatic recovery from failures; and [4] System design technology for combining biometrics information with ID management under control of a computer.

Each subject will be described in more detail below.

[1] Information security infrastructure technology for next-generation networks where the real world and the virtual model in the computer are combined

In the social system where the real world is combined with the virtual world, a variety of sensors will be provided in homes and offices, and high energy efficiency will be realized. The system will also work well in grasping the situation in the event of a disaster and contribute to the realization of a safe and secure society. However, since leakage of sender information from individually-owned smartphones or the like or of somatic health information from sensors is feared, the establishment of a protection system is required. Besides leakage of personal information from terminals, presumed information security issues concerning smartphones include fraudulent access to a smartphone Web site by terminal identity spoofing. An information security infrastructure for smartphones must be developed quickly.

In a sensor network, the utilization of ad-hoc networks external to the backbone is expected. However, information security technologies for wireless communications are in the physical layer and below. An information security infrastructure that provides the right combination of convenience and security must be established.

For that purpose, R&D of (a) information security infrastructure technology of sensor networks, and (b) information security infrastructure technology that provides the right combination of convenience and security in ad-hoc networks will be promoted.

[2] Technology for maintaining a consistency of all the security configurations between layers automatically

As the component-based configuration of a system grows, a technology for establishing an information system that ensures consistency of information security from the top layer to the bottom layer of the system is required. For that purpose, a framework for managing information security policy and configuration on the basis of the system architecture will be developed. In order to ensure that the policy and configuration are protected on the framework, R&D into an automated verification technology using formal methods will be promoted. Studies of this automated verification technology should be based on research trends in information security automation in the United States and should be conducted by utilizing the results of overseas studies.

Fears concerning information security accompanying the migration to IPv6 are not limited to the network layer, and overall consistency up to the application layer must be ensured. Related R&D is to be promoted as part of a framework for managing information security policy and configuration.

[3] Technology for building a computer network architecture that can perform automatic recovery from failures

Loss of a communications infrastructure that forms part of a chain of command in the situation in which a quick response is needed will bring devastation. However, enormous costs are incurred in protecting a network completely from a disaster beyond expectation and from a variety of threats and faults. A system for avoiding network service suspension from the supposition that network failures cannot be eliminated (technology for establishing a self-curing network) should be developed.

More specifically, by using network virtualization technologies, R&D into diverse network architectures that possess a resistance to failures caused by cyber attacks improved by enhancing diversity and redundancy in network communication systems is to be promoted.

By utilizing the diversity and redundancy of the network, R&D into self-curing functionality in the event of a failure will be promoted. This study can utilize the results of another important subject, “Combination of wide-area observation technology in a

large-scale network and malware behavior analysis technology," and a cure function that can make a quick responses to an attack will be developed.

[4] System design technology for combining biometrics information with ID management under control of a computer

In a social system where the real world is combined with the virtual world, the integration of biometrics information and ID management is needed to take identifiable information of a real person into the computer. The constituent technologies in the biometrics field have been matured in terms of performance, and an R&D subject in the future will be to find the technology for combining an authentication system by open ID management system architecture design, including biometrics, standardization of system architecture, and Security Assertion Markup Language (SAML). This can be used in the immigration examination system, for instance.

Japan has the advantage of biometrics constituent technologies, and in order to maintain this advantage, it is desirable that Japan takes the initiative in the international framework for evaluating the compatibility of biometrics authentication technology used as a part of the combined system.

More specifically, development of an OpenID-based middleware architecture,[8] and development of an interface and a protocol for biometric devices using SAML is needed. An international framework for evaluating the compatibility of biometrics authentication technology to be used in such an integrated system will be established. For international standardization by the ISO, coordination with domestic parties concerned and a new work item proposal (NP) will be organized.

(2) Zero-Day Defense Based on Attackers' Behavior Analysis

The APT attack that has attracted attention recently attacks a specific target, lurks in it, and performs espionage and sabotage persistently using a variety of methods. Cyber attack methods are becoming more complex and subtle, but measures against cyber attacks are falling behind, so that R&D that pursues a fundamental solution should be promoted. Therefore, an advance defense technology for optimizing measures by observing the behavior of internal attackers causing leakage of information and external attackers working through networks in a wide area, profiling such attackers, and analyzing the behavior model is required.

The important subjects here are: [5] Preventive base technology utilizing attackers' behavior analysis, and [6] Combination of a wide-area observation

[8] An authentication system standard and its identifier that can be used independently of a Web site.

technology in a large-scale network and malware behavior analysis technology.

Each subject will be described below.

[5] Preventive base technology utilizing attackers' behavior analysis

The present Internet environment is advantageous to the attacker, and the increased cost of measures cannot be suppressed as long as the countermeasures remain only as reactive after an attack. In the United States, R&D for halting the situation advantageous to attackers is being conducted as an urgent task. The same rapid reaction is anticipated in Japan.

More specifically, R&D into a technology that can predict the likelihood and effect of an attack and optimizes measures by profiling internal attackers perpetrating leakages of information and external attackers working through networks, based on behavior observation and analyzing behavior models based on incentives and game theories is being conducted.

[6] Combination of a wide-area observation technology in a large-scale network and malware behavior analysis technology

The explosive spread of smartphones, the appearance of viruses targeted at them, and increased cyber attacks using the Internet and SNSs have raised the risk of a pandemic network failure. Since there will be limitations to the conventional monitoring and measures taken by people, technologies for observing and analyzing the Internet and technologies for detecting and handling malware automatically (such as controlling traffic) will become indispensable. Therefore, R&D into technologies for observing the extensive IPv6 address space efficiently is needed.

In addition, technology for controlling traffic automatically when a problem is detected should be developed.

Recent cyber attacks are cleverly designed to avoid protection systems. Therefore, a system that conceals the observation network from attackers' eyes should also be developed for malware behavior analysis.

(3) Flexible Management of Personal Information

Stakeholders related with information systems have diversified, and users and vendors have a variety of levels of awareness and skills concerning information security. Therefore, technologies for improving user-control capabilities in accordance with such diversity, such as the balance between active utilization and protection of personal

information, are required. In addition, as how to handle personal information and ways of seeing related risks change in the event of disaster, a risk communication system for adjusting the allowable risks will be needed.

Accordingly, important subjects here are [7] User control technology for promoting utilization of personal information, [8] Data control/pursuit technology for supporting forensics, associated with information control, and [9] Systematization of theory-to-practice concerning IT risks.

Each subject will be described below.

[7] User control technology of personal information for promoting utilization

Since a simple either-or decision, whether to provide personal information or not, can be made at present, it is difficult to utilize personal information effectively. If personal information can be controlled appropriately, people can enjoy the advantages of utilization of such information.

For example, in order to use personal information, such as positional information and life logs appropriately, basic research is needed into a system that: allows flexible specification of privacy protection levels and the policy of each user; computation and data mining that are able to extract relevant data items while maintaining privacy protection.

For utilization of information that needs to be dealt with carefully and sensitively, such as medical information, a legal system adapted to the social environment must be studied, an industry consensus formed, and the technology for utilizing data in cooperation with medical information systems must be developed.

The leakage of personal information is also a major issue concerning information security in cloud computing, which has attracted attention as a new business model. R&D into other information security issues concerning cloud computing should also be conducted.

[8] Data control/pursuit technology for supporting forensics

The leakage of personal information is a big problem for individuals. In the same way, big problems for the government are leakage of state secrets and the drain of intellectual property from the country. Urgent development of technologies for preventing such problems is demanded. Since incidents of information leakage through networks have been increasing, a network trace-back technology for locating the destination of such information thefts and the technology for collecting evidence of falsification and leakages will be required.

Specific study subjects include (a) preservation and examination of real-time evidence, (b) network forensics, and (c) evidence reliability evaluations. Since an extremely large amount of data is handled in network forensics, efficient data collection and analysis must also be studied.

[9] Systematization of theory-to-practice concerning IT risks

In the event of a disaster, the ways of seeing risks will change (for example, personal information should not be displayed on the Internet in ordinary times, but safety confirmation takes precedence in the event of disaster). In the process of recovery from a disaster, values are diversified, and a risk communication system for adjusting allowable risks becomes important.

Risk management is indispensable and at the core of critical infrastructures supporting society. However, risks are complex, and one measure corresponding to a particular risk may itself generate another risk.

Therefore, (a) “risk vs. risk avoidance measures” should be studied; (b) communication measures for reaching agreement among the multiple parties concerned should be studied; and (c) a system for obtaining the optimum combination of measures should be developed.

(4) Infrastructure for stimulating research and development and systematized information security theories

Current R&D for information security is really a collection of know-how on measures corresponding to individual risks. Since information security technologies are not logically organized, there is little hope for further progress. Through appropriate evaluation of studies, improved studies and an appropriate method of dissemination can be clarified. Data for a demonstration study is needed to confirm that a theoretical study is correct.

In order to promote wide-ranging R&D into information security, common fundamental technologies forming the basis of studies must be developed.

For that purpose, the following are required: standardization and provision of data for demonstration studies; establishment of an evaluation system for making studies more efficient; and development of common fundamental technologies.

Here, the important subjects are: [10] Systematized basis for information security studies; [11] Product evaluation certification technologies for assuring correct implementation of security components; and [12] Theoretically secure cryptographic technology.

Each subject will be described below.

[10] Systematized basis for information security studies

R&D of information security should be refined from a collection of know-how on certain measures to a branch of science that can be evaluated as a study. To confirm that a particular theoretical study is correct, data for a demonstration study is needed, and a system for continuously observing the data is also needed.

As a basis for stimulating cyber security studies, the following are needed: (a) establishment of a scientific evaluation framework for cyber security studies, and (b) provision of a database for demonstration studies. For (a), R&D concerning methods of evaluating threats and risks, methods of evaluating effects of technologies, and scientific evaluation systems are required. For (b), data that needs to be provided should be clarified, data configurations should be designed, and data provision systems should be studied.

[11] Product evaluation certification technologies for ensuring correct implementation of security components

A software quality evaluation method and defect characterization based on the attributes of software quality (security, safety, reliability, etc.) are necessary. If the quality evaluation criteria for security components, which are constituents of an information system, are standardized, the system can be composed of appropriate security products meeting security requirements. This is useful also for improving the cost effectiveness of security measures. Realizing a certification system based on quality evaluation and its basis before the rest of the world will improve Japan’s industrial competitiveness.

Specifically, (a) a reference design for security level evaluation of security products, (b) a method of evaluating the validity of a combination of security products, and (c) standardization of evaluation processes, are all necessary.

[12] Theoretically secure cryptographic technology

Theoretically secure cryptographic technology is comparable with computational cryptography, which used to be the mainstream. Malware targeted at the control systems of critical infrastructures has appeared in recent years, and the necessity of security measures for control systems has risen. Since computational cryptography, such as DES and RSA, is inseparable from the endangerment caused by improved

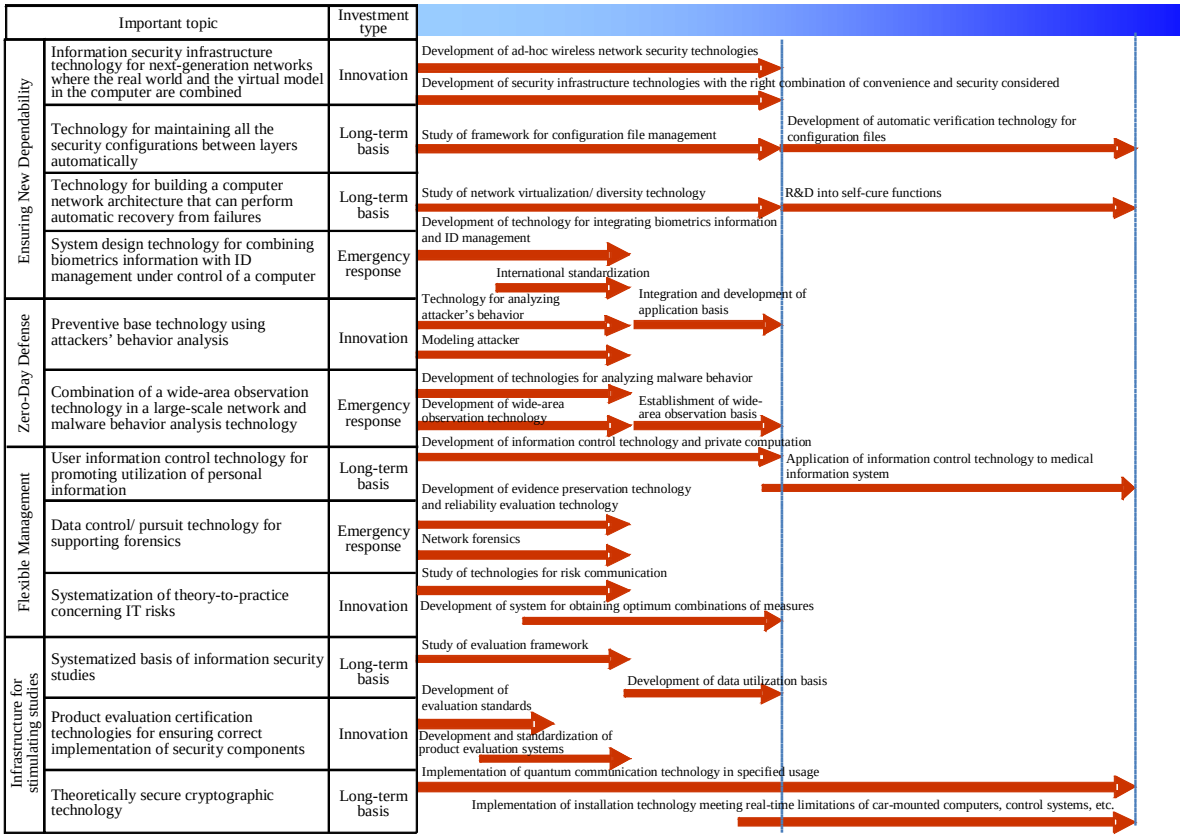
processing speed, security cannot be guaranteed for the entire duration of the operational period (perhaps a long period of ten years or so) of the control system.

Embedded devices with sensor functionality have been placed in homes and offices and connected to networks, and security measures for embedded devices are demanded. Theoretically secure cryptographic technology, which can be made up of linear operations and can be processed at a high speed, is thought to be applicable to embedded systems with small computational resources.

In order to put theoretically secure cryptographic technology to practical use, studies on its introduction into embedded systems are necessary. Car-mounted computers, control-system computers, electrical systems, and other types of systems all require R&D that takes both the resources and limitations of real-time characteristics into consideration.

A quantum cryptographic technology, which is a type of theoretically secure cryptographic technology requires a mechanism for sharing a big private key in advance, and one promising measure is quantum communication. The realization of quantum communication in a specified environment is set as a subject for a 10 to 20-year study. It would be efficient to conduct this study by utilizing internationally proved outcomes.

Fig. 8 Technology Road-Map of Important Subjects



6 Important Subjects after the Great East Japan Earthquake

Information security is to be promoted with priority attached to security of confidentiality (information can be accessed just by an authorized person), completeness (complete information is maintained without change), and availability (information and services can be used when necessary). In the event of a large-scale disaster, it will become especially important to ensure availability.

In this section, high-priority information security subjects identified after the Great Earthquake will be extracted. It is important to promote R&D by making a sharp distinction between subjects that require urgent measures for rehabilitation and reconstruction, and subjects needed to implement increased disaster resistance, such as ensuring New Dependability from the medium and long-term standpoints.

(1) Establishing Disaster-Resistant Information and Telecommunications System

Agenda arising from the Earthquake include fast information transmission in the event of disaster, difficulty in sharing information, suspension of information and telecommunications systems caused by a long power outage or a combination of several outages, collapse of the supply chain, and temporary loss of the detailed Basic Resident Register and the Family Register data kept by local governments. Therefore, a disaster-resistant information and telecommunications system must be examined and reconstructed, and BCPs must be reviewed to include remotely stored information backups and decentralization. Since cyber security and physical security are very closely connected, BCPs must be reviewed on the assumption that multiple disasters will occur.

[1] Disaster-resistant information communication infrastructure

Disaster-resistance, network systems including organic links between wireless and wired connections, and reinforcement of emergency power supply equipment must be studied.

[2] Information system in the event of disaster

In the event of disaster, a fast information communication sharing system must be established urgently.

- In the Earthquake, examples of effective use of SNS were reported. Although there

are concerns about the reliability of information on SNSs, social literacy has matured sufficiently for users to select neutral information. Better use of SNSs should be examined, with information security taken into consideration.[9]

- Information systems that enable information to be shared appropriately are needed for personal information such as the resident registry and medical records, assets and liabilities (smooth withdrawal during an emergency), collation of residents' IDs with specified emergency evacuation areas, traffic control information for facilitating logistics during an emergency, and information on the whereabouts of foreigners and overseas students studying in Japan. System design with information security taken into consideration should be examined to collect, manage, and operate such information during an emergency.
- Mirror sites that provide disaster-related information were started up one after another and played an important role. Since a quick response is demanded, the means of ensuring the security of mirror sites in the event of disaster should be studied in advance.
- Measures for configuring a quick and easy route to carry emergency information in the event of disaster and the technology for rearranging a dynamic network for recovery from disaster must be studied.

[3] Backup and decentralization of information and telecommunications systems

In preparation for future disasters, it is very important to take a backup of information and telecommunications systems and to decentralize them. After the Great Earthquake, backup and decentralization measures using new technologies, such as cloud computing, must be studied.

- As a method for taking backups and implementing decentralization at a low cost, use of cloud computing is attracting attention. However, the information security issue is pointed out as a serious impediment. Efforts to remove this concern in terms of R&D and operationally should be accelerated.
- If the system is decentralized, remote authentication in the event of disaster should also be studied. Shibboleth authentication, used among universities, could not be used in the event of disaster. Measures for avoiding the risk of unserviceable systems should be considered. The risk of unusable cryptography or authentication in the event of disaster should also be verified.

[9] The Cabinet Secretariat (National Information Security Center, ICT(IT) Section), Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry released the "Information Provision through Commercial Social Media by National and Local Governments and Other Public Institutions" (For details, see http://www.meti.go.jp/press/2011/04/20110405005/20110405005-2.pdf).

(2) Risk Management

After the Great Earthquake, the importance of risk management and risk communication has been recognized.

As described earlier, ways of seeing risks change in the event of a disaster (for example, personal information should not be displayed on the Internet in ordinary times, but safety confirmation takes precedence in the event of disaster). In the process of recovery from a disaster, values are diversified, and a risk communication system for adjusting the allowable risks becomes important.

Therefore, measures must be studied not from the viewpoint of information security in the conventional narrow sense of ensuring security, but from the broader viewpoint of information for reducing social risks.

Risk management is indispensable and at the core of critical infrastructures supporting society. However, risks become complex, and one measure corresponding to a particular risk may generate another risk.

Risk communication is the means whereby a variety of stakeholders have common and accurate information about risks in their surroundings and communicate with one another. Risk management is a process of conducting further evaluation, taking measures, and reducing risks to an acceptable level.

If a disaster occurs, the situation will alter greatly, and the means of seeing risks also change, and the acceptable levels of risks will change greatly. In the event of a disaster, it is important to have the idea of dynamic risk management for adapting optimally to changing conditions. Since one measure corresponding to a risk may generate a new risk, optimum measures should be found (risk management) by comparing risks (risk vs. risk).

We are apt to dream of a zero-risk state, but if we stick to that dream, we will not develop appropriate risk management. By clarifying the risks in organizations and evaluating and responding to those risks, security can be ensured as a total system. In risk communications, there are many issues to be studied, such as in what form information should be transmitted to the nation and how an enterprise should transmit and control information in its crisis management.

In addition, we should have the ideas of BCPs and business continuity management (BCM) together with the applicable skills for unexpected events. For that purpose, it would be useful to conduct simulations on the supposition of a severe emergency situation.

More specifically, as described in [9] Systematization of theory-to-practice concerning IT risks, (a) study of measure for avoiding “risk vs. risk,” (b) study of communication measures for forming consensus among multiple parties concerned, and

(c) development of a system for obtaining an optimum combination of measures are required.

(3) Flexible Management of Personal Information

The importance of technologies for improving user-controlling capabilities in accordance with diversity, such as the balance between active utilization and protection of personal information was described in (3) “Flexible Management of Personal Information” of Section 5. How to handle personal information and ways of seeing related risks change in the event of a disaster—for example, safety confirmation takes precedence. Since it is very difficult to remove information leaked to the Internet, it is preferable to conduct R&D into technologies for controlling personal information appropriately and a system for specifying flexible personal information protection levels and a flexible policy in ordinary times, in preparation for possible disasters in the future.

More specifically, the R&D mentioned in (3) “Flexible Management of Personal Information” of Section 5 should be conducted taking the occurrence of a future disaster fully into account.

(4) New Dependability

As described earlier, the degree of dependence on advanced information systems has been increasing in society. In the event of a disaster, information systems should provide high-quality, reliable services in particular. The information handled there should be accurate and consistent, and its confidentiality must be protected according to the rules. The social system developed following the Earthquake should be a system satisfying these requirements of New Dependability.

To ensure New Dependability of information systems, the component-based configuration of the system has grown, and the technology for establishing an information system that ensures consistency of information security from the top layer to the bottom layer is required. Since enormous costs are incurred in completely protecting the network from a disaster beyond expectation, and a variety of threats and faults, the importance of R&D into systems such as a diversity network for preventing a network service from stopping will also increase.

R&D mentioned in (1) “New Dependability of the entire information system” of Section 5 must be conducted, with great importance attached to the viewpoint of preparing for the occurrence of a major disaster.