資料４－４（参考）

Tentative Translation

New Information Security Human Resource Development Program (Draft)

1. Introduction

Circumstances towards preparation of this program

While information communications technologies have brought major benefits to economic activities and society and prevailed more as a source of innovation, the risks of information security are becoming more serious. These changes in the environment around cyberspace are extremely rapid, and at the same time, these risks are spreading rapidly since information communications technologies are connected globally and penetrating to every part of the society. To retain information security as a response to these risks, we need to make efforts, which should exceed those so far made from the viewpoints of both quality and quantity. Therefore, it is urgently necessary to develop and retain human resources to support the efforts.

As to human resource development in the information security field, in July 2011, the Information Security Policy Council reviewed the future direction of the human resource development policy for the three-year period from FY 2011 to FY 2013 and that for the medium to the long term, and determined the Information Security Human Resource Development Program. In May 2012, the Outreach/Awareness and Human Resource Development Committee prepared a document titled “Immediate Issues for after FY 2012 Information Security Human Resource Development Program”, which compiled the problems and concrete policy proposals with regard to information security human resource development in businesses, governmental organizations, etc.

Based on these, the government has fostered various programs for human resource development. However, because the risks related to cyberspace have recently become more serious, and the results from human resource development have not been obtained in a short time, it is difficult to say that we have had sufficient outcomes.

Under the circumstances, in June 2013, we developed the Cybersecurity Strategy as a new information security strategy, which basically targeted the making of a cybersecurity nation by establishing a world-leading, resilient and vigorous cyberspace for the purposes of national

security, crisis management, socioeconomic development, and the safety and security of the people. In this strategy, human resource development is considered a measure to activate industry, improve R&D and literacy, and at the same time establish a vigorous cyberspace for the enhancement of creativity and knowledge in cyberspace. As an active effort to solve the problem of the lack of human resources for information security, this strategy also targets, among others, improvement of the ability of workers engaging in information security, discovery and cultivation of extremely talented human resource, development of human resources that can work at a global level, and human resources development in governmental organizations, etc.

In addition, the National Security Strategy (Decision by the National Security Council and Cabinet Decision, December 2013) requires further enhancement of cyberspace defense and the ability to respond to cyber-attacks, a comprehensive review of the strengthening of the security human resources population, and taking other necessary measures.

In December 2013, the Strategic Headquarters for the Promotion of an Advanced Information and Telecommunications Network Society (IT Strategic Headquarters) decided on “The Strategy for Developing Human Resources with Creative IT Skills” This emphasizes the following two points: *(1) establishment of society where people can enjoy the life with the full advantage of IT,* and *(2) arrangement of the environment* and the *creation of world-class IT human resources that can lead Japan’s IT society*. The ministries and agencies are to discuss action plans in detail which they should implement.

Based on these, in this program, we reviewed the Information Security Human resource development Program. In principle, it targets the three-year period from now on (FY 2014 to FY 2016) but includes considerations of the medium- to long-term challenges, compiling the new strategy for human resources development with which we should proceed in the future.

2. Current Situation and Challenges with Regard to Human Resources for Information Security

(1) Increasingly serious risks surrounding cyberspace

The information communications technologies now penetrate to every space including the

private spaces, such as the individuals and the households, the public spaces, such as the social infrastructure, and even inside of equipment and devices, supporting the bases for living and economics and leading national growth. Therefore, if these systems and networks fail, it will seriously affect society. As shown by this, the risks surrounding cyberspace keep spreading and thus, the measures for information security[1] become more important than before.

[More severe risks]

Many more accidents related to information security occur by personnel within organizations through negligence or intension and therefore internal information management is important as before. In recent years, however, the risks of cyber-attacks from outside have been getting greater. In the past, many of the cyber-attacks were just to play tricks or take delight in people's reaction to the crimes, but thereafter, the cyber-attacks for economical purposes have increased. Recently, we see cyber-attacks having purposes of theft of confidential, technological, and other information from such organizations as governmental organizations, defense industry businesses, critical infrastructure operators, and research institutes. In addition, it is pointed out that threats that are likely to affect the critical infrastructure service providers become manifest.

Many of these attacks are considered so-called targeted attacks.[2] It can be thought that the damages by intrusion into the inside of the information systems, etc., can be greatly reduced by such means as appropriate system design, programing that does not create vulnerabilities, appropriate operation and monitoring. Therefore, not only experts of advanced information security but also such human resources are desired that can take basic information security measures in various fields as information and control systems and can respond to system designs that incorporate information security.

[More widespread risks]

[1] Not including simple compliance-based measures, but measures for the information security taken as part of risk management within an organization.
[2] Targeted attacks: Cyber-attacks targeting users of specific organizations. A typical example is impersonating an interested party or an employee of the targeted enterprise and sending the other employees, etc., mail with a malicious program attached.

As everything is now being connected to the Internet, we have devices that may be cyber-attacked anywhere around us, and this spreads the risks (Figure 1). Recently we have had information leaks from smart devices and digital multifunction printers and cyber-attacks where home appliances and security cameras are used as springboards. In addition, the independent systems, which are isolated from external networks, such as information networks, are also objectives of cyber-attacks. For example, as actual problems, using USB memory cards, etc., as media, hackers infect the control systems for critical infrastructures with malicious programs to make the systems and devices of the infrastructures malfunction.

As shown above, products and services related to the information communications technologies rapidly spread and along with it, the necessity of measures for information security heightens. Under the circumstances, the issues related to information security are not only those to which only information security experts can respond. However, all the persons that offer and operate products and services including IT products/services using various information communications technologies, such as control systems should have knowledge and ability to a certain degree to respond to the retention of information security.

Figure 1 Cyberspace spreading along with penetration of IT

Under the circumstances, as to “The Strategy for Developing Human Resources with Creative IT Skills”, we have acknowledged, as the common necessary skill, basic information development skill, system foundation development skill, software development skill, information services practical application/offer skill, which are required for human resources

that implement IT for products and services in a safe and reliable manner.

In the strategy, the following are pointed out: *generally speaking, downstream processes need more costs to solve problems, such as vulnerability of their systems, etc. Therefore, it is recommended for those who are involved in the planning and design phases, which are upstream processes, to have knowledge and skill of information security*.

Therefore, not only the experts in information security, but also those engineers and other persons involved in planning and designing of products and services using information communications technologies are required to have basic, necessary knowledge and ability with regard to information security.

[More globalized risks]

As use of the information communications technologies is spreading in the individual countries in the world, the risks surrounding cyberspace are also expanding globally. As the cyberspace has no border and the threats are permeable in a borderless manner, anyone is in a situation where he/she is exposed by global risks all the time even if he/she does not go abroad. For example, an overseas case occurred in which a home PC owned by a private individual was used as a springboard for a DDoS attack[3] on foreign governmental organizations, etc., and in foreign countries, such problems have been actualized as targeted attacks in an attempt to steal confidential business information, etc., from enterprises. There is also a threat that an attack to one point in a global supply chain, etc., may affect other bases.

(2) Lack of human resources having information security skills

Against the risks surrounding cyberspace that are getting severer, in the Cybersecurity Strategy, it is decided that the government, the critical infrastructure, and other businesses should strongly take measures, and to this end, enriching human resources in the information security field are indispensable as the basis. Human resources in the information security field are required to have the skills of management for awareness, education, and operation of information security, and the capability of understanding and executing in various fields,

[3] DDoS (distributed denial of service) attack: a type of attack through a network that brings the target computer in a service malfunction state by giving it a large amount of processing loads from multiple machines.

including computer network protection. With regard to human resourcess supporting information security as mentioned above, however, there are various problems to be solved.

[Problems with regard to recognition of management about information security]

Many organizations, such as enterprises, are today utilizing information systems as part of their business/operation strategies and processing the business operations and information important for those strategies by use of the information systems. In other words, utilization of the information communications technologies is the origin of profits for businesses and for other organizations—it helps them improve operations. Therefore, such items as maintaining the confidentiality of such important information as business secrets and confidential information, retention of the accuracy of such information, and the maintenance of the operation of information systems essential for business operation are indispensable factors for business strategies or project feasibilities. It is difficult to say, however, that, in businesses and other organizations in Japan, management is actively working on measures for information security as a business strategy while being conscious of the need thereof. This tendency also appears in investments in human resources for information security. Sixty percent of the businesses showed their consciousness of the need to make efforts to solve the problem of the lack of human resources in certain manners but almost half of them answered that they took no concrete measures. From this, we understand that the management of many businesses and other organizations do not acknowledge the realistic business risks with regard to information security and still fail to initiate concrete activities. (Figure 2)

We must recognize that what is important as a precondition of human resources that can appropriately consider and carry out measures for information security is the presence of human resources for software that firmly have basic skills with regard to information communications technologies, and that it is indispensable to understand the trend of human resources for software and to develop human resources that respond to the needs of Japanese industry.

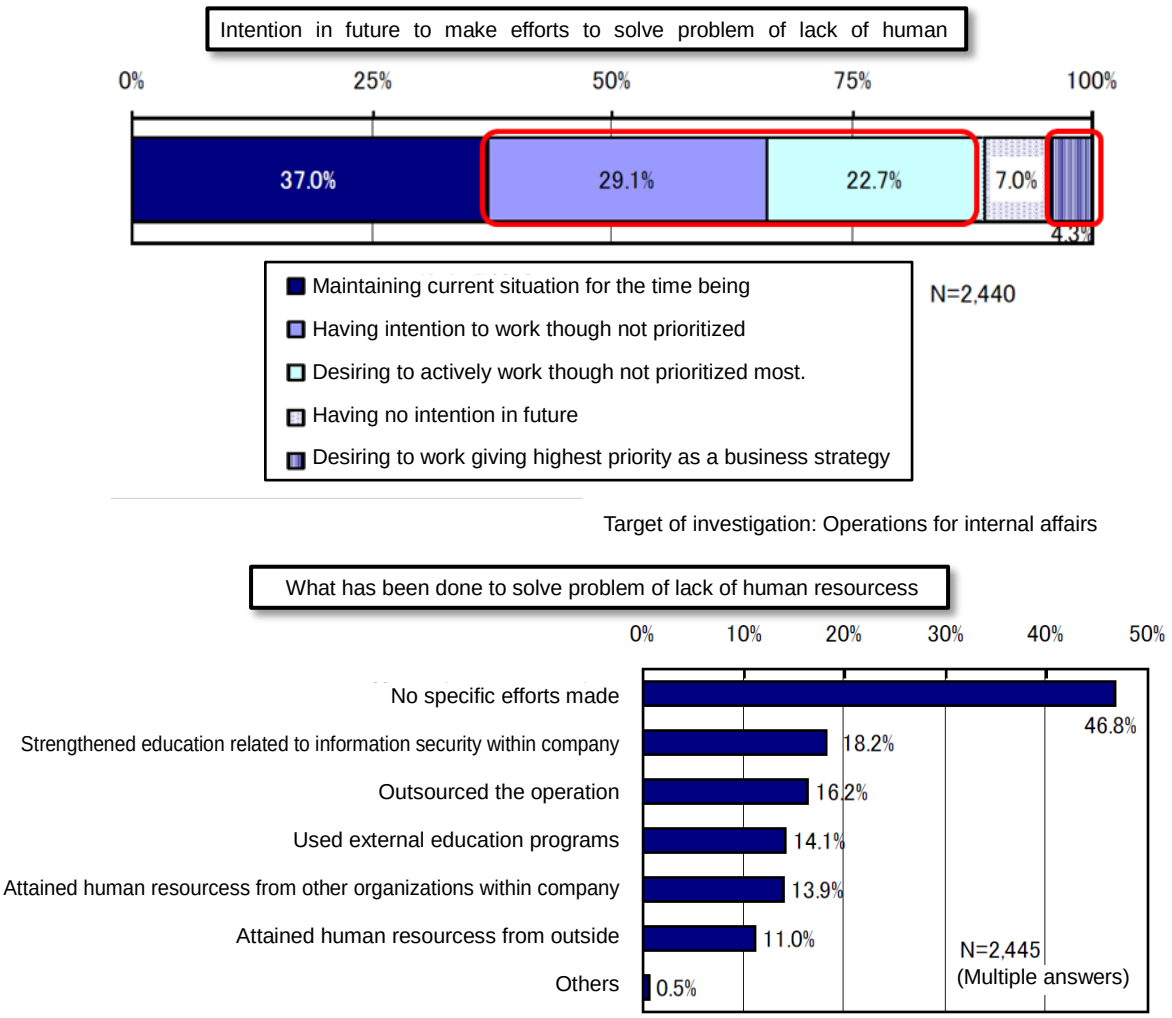

Figure 2 Efforts to solve problem of lack of human resources in enterprises and other organizations
Source: “Basic Assessment Concerning Development of Human Resources for Information Security”, Information-Technology Promotion Agency, April 2012

[Problems held by workers in enterprises, etc.]

Many of the information systems in Japan closely link to business operations of enterprises and other organizations. Establishment and operation of these information systems are entrusted to expert operators (IT vendors), and in many cases, the measures for information security are entrusted to them. Inherently, however, with regard to the establishment and operation of an information system that penetrates into sensitive parts of the business operation, it is essential for an organization, such as a user company, to involve persons who are familiar with the actual business operations of that organization.

According to trial calculations by the Information-technology Promotion Agency, Japan (IPA),

on the other hand, as shown in the Cybersecurity Strategy, of about 265,000 engineers who are engaged in information security in Japan, just 105,000 or a little more of them are thought to have the necessary skills. The reminders, i.e. more than 160,000 engineers, seem to need certain education/training. Furthermore, it is considered that the nation is potentially short by about 80,000 engineers, and thus, efforts to solve this problem are urgently required in order to retain a level with regard to information security measures in Japan.

[Necessity of human resources with high expertise and outstanding ability]

Changes in the information security field happen rapidly, and thus in order to respond to new incidents occurring day to day and to high level incidents, it is insufficient only to solve the problem of the qualitative and quantitative lack by improving the capabilities of general employees engaged in general information security, but it is essential to retain those human resources that have high expertise and outstanding ability to create new measures to respond to changes in the environment.

Projects by governmental organizations and colleges/universities have so far made efforts to find and develop human resources with high expertise and outstanding ability to lead the information security field. For example, we currently see a situation where information security (tool) depends on many overseas products and services (Figure 3). From the viewpoints of Japan's security and enhancement of industrial competitiveness as well, we need to make further efforts in the future to create new technologies in Japan and retain human resources that support them. The presence of human resources with high expertise will lead the engineers engaged in information communications and support, among others, to improve the ability of the next generation of human resources for information security, protection from global attacks, and creation of new industries.

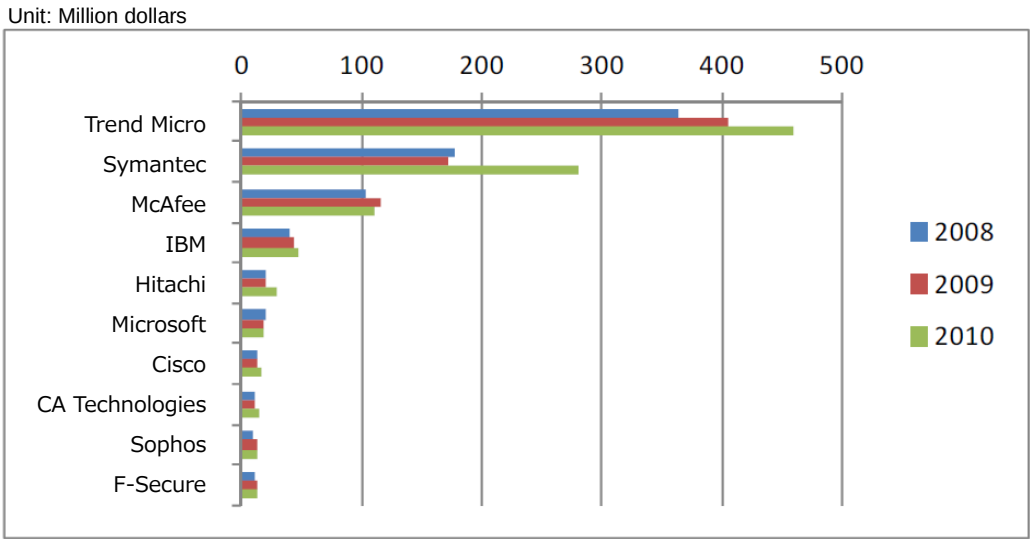

Figure 3 Information security (tool) sales by vendor [Japan]
(Ministry of Economy, Trade and Industry survey report “Projects of Promotion of Information Security Measures by Businesses and Individuals in FY 2011” (March 2012))

If the younger generations can be encouraged to become interested in the information security field as their future professions, and human resources for information security are created in Japan and play active roles both at home and abroad, then it will help expand the lower end of human resources. To this end, it is desired to arrange an environment where men of outstanding ability can be found in society for employment by the government, businesses, and other organizations to devote themselves to their studies.

[Necessity of human resources at a global level]

At present, mainly for the manufacturing industry, globalization of business activities is becoming quite natural, including overseas production, procurement, and sales; in addition, business is activated to enter markets, such as emerging countries. As the Japanese domestic market has been sluggish, the domestic demand-oriented industries, such as the distribution industry, retailing industry, and financial industry, are also actively developing business operations in Asia and other foreign countries. Therefore, while integration of the business operations and the information communications technologies is promoted, it is indispensable for enterprises to respond to globalization of the information communications technologies and develop and retain human resources that can respond thereto.

Under the circumstances, we cannot protect Japan and our organizations without human resources with higher ability than that of attackers so as to respond to the attacks because cyberspace has no border, and cyber-attacks are made across borders. To this end, it is important for individual human resource development courses to bring it into perspective to develop such human resources that can work at a global standard level.

(3) Classification of targets of measures and challenges to be reviewed

To respond to the above-mentioned risks becoming severer and the great lack of human resources on the other hand, we must form a virtuous circle of human resources by taking measures not only for the supply of human resources (cultivation and discovery), but also for demand thereof (employment, etc.).

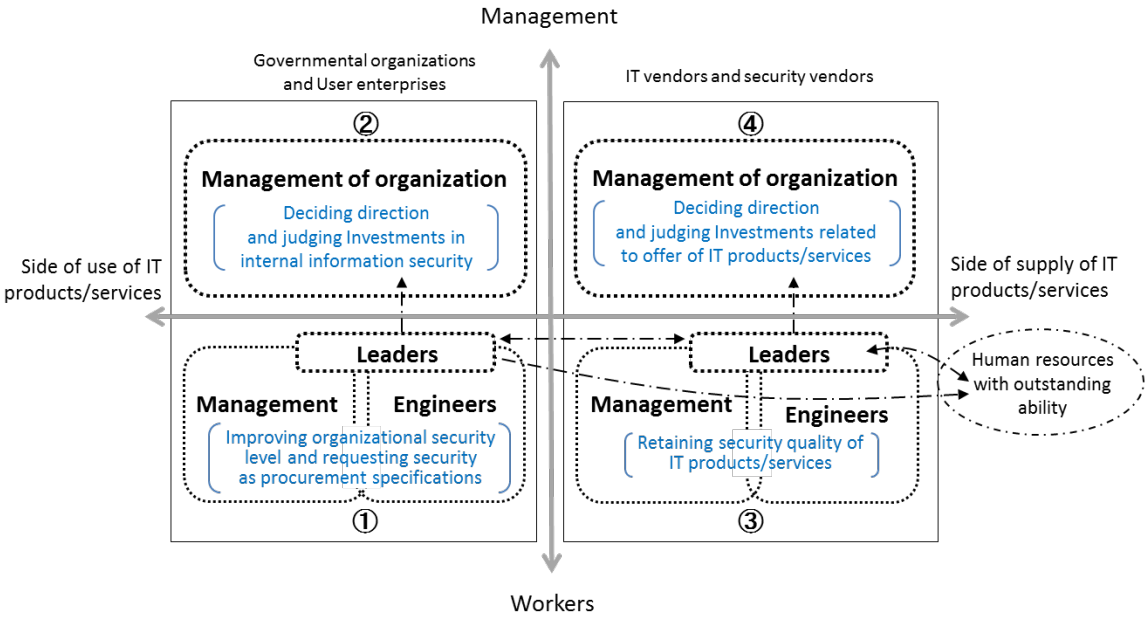

Figure 4 Classification of targets of measures

From the viewpoint of the supply of human resources, for example, governmental organizations, user enterprises, and other organizations need to make the workers on the side of use of IT products/services (① in Figure 4) be capable of determining necessary measures and taking them, so as to retain information security within their organizations. On the other hand, the workers on the side of supply (③) are naturally required to have the ability at a level necessary to respond to both apparent and potential demands from the side of use. From the viewpoint of demand of human resources, on the other hand, management on the side of use (②) is required to acknowledge information security as an operational strategy of their own organization and employ ① with appropriate treatment. Similarly, management on the side of supply (④) is required to employ ③ with appropriate treatment based on the strategy of development and the supply of the necessary services and products.

In addition, to improve Japan's entire information security level, human resources of

outstanding ability, as leaders, need to play an active role by involving themselves in various scenes in such ways as actively working as leaders of the workers, promoting communications between management and workers, and acting as an intermediary between the supply side and the use side.

Note that, as shown in Figure 1, as everything is now connected to the Internet, the phrase the “use side” is not limited only to the use of information systems, such as routers and servers in each organization, but includes the use of all IT products and services handled in the operation of each organization. Specifically, “use” includes the use of IT products and services by such infrastructures as financial, electric power, water supply, gas, and railroad industries in offering their services, and the use of IT products and services that are integrated into the home appliance, automotive, medical facility, and other industries.

As explained above, human resources in the individual classes are mutually related and there are challenges both in supply and demand of human resources. Under the circumstances, in order to improve Japan’s entire information security level, it is required to organically combine and promote various measures taken by industry, academia, and government.

Based on these, in chapter 3, we first describe the basic policy of efforts focusing on both the demand and supply of human resources and the concrete measures therefor. There, we describe the reform of consciousness of management by setting information security requirements in enlightenment and procurement of information security measures as part of the operation strategy, and efforts to make the thickly layered engineers engaged in the information communications (system engineers, network engineers, programmers, etc.) acquire knowledge of information security as an essential ability. Then, we describe the necessary efforts to find and develop human resources with high expertise and outstanding ability. In addition, we describe the development of human resources that can act at a global level while devoting themselves to their studies both at home and abroad, in order to respond to the threads in the cyberspace that is becoming globalized. As to the governmental organizations, in particular, it is strongly required for ministries, agencies, etc., to firmly promote measures for information security, in order to protect information and information

systems and assure safety and peace of mind for the public. In addition, the governmental organizations should voluntarily make efforts to develop related human resources. Thus, we also describe the concrete measures therefor.

Furthermore, we describe the challenges faced by educational institutes, including enrichment of basic scholastic achievement with regard to information communications in the primary and secondary education phases, enhancement of seminars to improve practical ability in the higher education phase, development of human resources that can teach information security, and indication of career paths of human resources for information security. Note that, as to the concrete measures for outreach and awareness to improve the information literacy among general people, we will prepare them in the future in the review of the Information Security Outreach and Awareness Program (the Information Security Policy Council decision in July 2011).

3. Future Policy of Efforts

[Basic policy]

Forming a virtuous circle of demand and supply of human resources to improve Japan's information security level

<Demand> Reforming consciousness of management

・To create demand for human resources by promoting reform of the management's awareness of management and heightening their willingness to invest in information security through promotion of efforts to let them recognize that information security is the basis of the business operation strategy, and by.

・To arrange an environment where we can develop human resources that can understand and explain both the business management and information security so that the management and the leaders of workers can review and communicate the challenges and the direction with regard to information security from the viewpoint of the business operation strategy.

<Supply> Quantitative expansion and qualitative improvement of human resources

・To let the thick layer of existing engineers who are engaged in actual performance understand that information security is an essential ability.

・To promote the development and discovery of human resources with high expertise and outstanding ability to respond to threats that are more and more globalized.

(1) Reform of management's consciousness

1) Promotion of information security measures as part of business operation strategy

For the management of an organization that makes decisions with regard to its operational strategies and directions, sufficient recognition of the meaning and importance of the business operation strategies concerning its own systems, intellectual properties, technologies, etc., is a precondition for autonomous thinking about the necessity of protection.

As a result, management will be aware of information security as an essential item for development of their own organizations, and thus will make efforts for investment of the business resources to make the information security level satisfy the requirements of the organization. In addition, against burgeoning threats, there will arise needs to appropriately assign necessary human resources to sections where information security measures are necessary.

In an organization, to what level information security should be set is inherently a matter of business operations and operational strategy. In other words, the management is to decide whether they will invest their necessary resources in retention of a high information security level and improvement of reliability from their customers and safety of their own information, or they will make a different decision, such as reception of risks, after considering the balance with the other risks. This decision will be inappropriate if it is made before the management sufficiently recognizes the situation of information security and the effects thereof to their business operation. It is necessary to arrange an environment where information is appropriately offered to the management so that they can appropriately make decisions with regard to their business operation as part of risk management in the entire organization.

Specifically, as before, we will hold seminars, etc., to explain the importance, etc., of information security measures and of the development of human resources for the business operation management of enterprises and other organizations, including management, management applicants, and personnel staff members of enterprises and other organizations, and at the same time, we will take actions for enlightenment with regard to information security as part of the business strategy by taking every chance where the management gathers, such as a meeting held by an economic organization, in order to reform the awareness of management. In addition, as part of active efforts to reform the awareness of management with regard to information security, the government will continuously make efforts, as before, to let the cabinet ministers and the high government officials directly ask for awareness reform through the seminars and other meetings held by the government for the management of various industries.

The issues of information security involve multiple business fields and thus often become factors of interference with business convenience and efficiency. Therefore, in order to prepare a strategy, make a decision, and carry out practical business in a cross-organizational manner, it is important for the individual organizations to appropriately and firmly position the CISO[4] and other staff members and clarify their responsibility. It will be more important in the future to link the information communications field and/or information security field with the business-related fields, aiming at enlightenment of the consciousness of management to make them think about how to position and utilize the information communications technologies in their business strategy, and aiming at development of management applicants, including CISOs who can completely think about, and explain, how information security will affect the business strategy. To this end, we will make efforts to arrange an environment where knowledge and corporate management skills can be obtained by such means as arrangements of educational courses in which the courses related to the information communications technologies will link closely with the business administration studies in such educational institutes as graduate schools.

In addition, it is important to make the management of small and medium enterprises, which occupy most of the number of Japanese enterprises, understand more about information security. Currently, as a concrete effort, the Ministry of Economy, Trade and Industry (METI) holds seminars for persons playing roles to instruct small and medium enterprises in an attempt to place instructors nationwide and network them. At the same time, through collaboration with the small and medium enterprises' organizations, etc., the METI is making efforts to support seminars held by these organizations with regard to information security measures in an attempt to improve information security levels of the small and medium enterprises. In addition, the METI is arranging materials and tools for enlightenment that can be used for staff education in enterprises and promoting use of them. Furthermore, the IPA is reviewing promotion of penetration of the Guidelines for Information Security Measures of the small and medium enterprises (IPA, March 2009) and efforts of the Hands-On Support[5],

[4] CISO: Chief Information Security Officer. Person responsible for planning and executing the information security strategy in an enterprise according to the management philosophy of the enterprise.
[5] Support activities and educational training courses provided on site while working there.

etc., for the enterprises that have undergone attacks, aiming at optimization of the costs for measures borne by enterprises and other organizations that think it difficult to take information security measures and at promotion of such measures.

We see some frameworks emerge that offers information security measures in a unified manner to such organizations as small and medium enterprises through utilization of the cloud systems. With regard to use, etc., of these frameworks in a safe and reliable manner, the government will give support to the persons responsible for actual operation through preparation and penetration of guidelines. Through these efforts, we will offer necessary information to the management, etc., and encourage them to change their consciousness according to the size, category, etc., of their organizations.

In recent years, we see that the small and medium enterprises review their business continuation plans (BCPs) for occurrence of disasters, etc., and their risk management schemes and that some financial institutes provide those enterprises with financing systems[6]. In response to this movement, we should actively make efforts to make information security be recognized as a factor necessary for business continuation including the viewpoint of availability[7]. To this end, while reviewing preparation of BCPs including IT-BCPs and the methodology of risk analyses as a precondition thereof and encouraging enterprises and other organizations to introduce them, we, both the governmental and private sectors in collaboration, will take actions to support efforts towards formation of common recognition in the management about the importance of development of human resources that will be able to work on these tasks.

In addition to these efforts, it is also important for management to explain their efforts with regard to information security as part of explanation about the risks in their operation strategies to their stakeholders. As a result, it is expected that the management will focus more on information security measures of their own. To this end, we should have a conclusion

[6] Small and Medium Enterprise BCP Guide (Small and Medium Enterprises Agency, March 2008) (http://www.chusho.meti.go.jp/bcp/download/bcp_guide.pdf)

[7] Availability: Characteristics in which access and use are allowed when an approved entity (organization, etc.) makes a request.

by referring, among others, the efforts[8] made by the SEC[9] in the USA with regard to the possibility, etc., of incidents by cyber-attacks to listed companies, and by reviewing the possibility of disclosure of the possibility of the incidents to the investors as risks of business operation, etc. At the same time, we should conclude by additionally reviewing the form the scheme should be in to promote incentives for disclosure including sharing of the related-information.

It is required to make people better understand the need for information security audits and ranking in order to retain accuracy, etc., of the disclosed information. Furthermore, in order to execute audits that is not superficial but practical, it is important to continuously review the audit methodology including arranging and reviewing the appropriate criteria. In addition, it is important to guarantee the validity of the audits, etc., and thus it is necessary to appropriate utilize the schemes of development of human resources to execute information security audits, etc., and the schemes of qualifications. Not only because development of human resources like this helps enlighten the awareness of management of enterprises and other organizations, but also because it helps improve Japan's information security level, we will continuously work on an increase in the skills of workers including auditors on a day-to-day basis (offer of latest information, etc.), establishment of codes of conducts, and arrangement/enrichment of an audit system. Specifically, we should help improve the quality levels of not only external audits but also internal audits by providing engineers who have knowledge of IT technologies with training courses to obtain audit certificates and other opportunities to obtain knowledge of the audit skills or with practices by using the standard audit methods and tools for specific services and specific protection purposes (measures against targeted attacks, etc.).

2) Improvement of communication ability of the worker leaders within organizations

Of the workers involving themselves in information security, the leaders necessitate to be coordinators within their organizations in order to create mutual understanding with the management about information security and to make the management share and

[8] SEC "CF Disclosure Guidance: Topic No. 2, Cyber security"
（http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm）
[9] Securities and Exchange Commission

communicate the challenges and policy with regard to information security. For these human resources, ability and experience are required to understand the roles of the management of organizations and to play a role in the arrangements with the management and connection to various organizational decision making phases (vertical crosslink). It is also necessary to arrange an environment where these human resources can utilize the technologies concerning business operation strategies and information communications that help understand the viewpoints of business operation strategies, and at the same time support the reform of thinking ways within the organizations, analyze the relationship, etc., between information security and the business risks, and improve their communication ability. For the industry, for example, we will promote measures including holding intensive, lodging seminars in which the participants will be given themes, such as reviews of business planning, business flows, and system requirements for it, and will be let them present their review results.

We will arrange an environment including offer and disclosure of information, in an attempt to make more enterprise managers recognize that information security measures are not costs they reluctantly pay but tools necessary to improve their own products and services, and thus are investments along with their business strategies.

3) Setting information security requirements for procurement

If a customer of a certain product or service asks the ordered company, etc., for information security as the product/service quality at the time of purchase to take an information security measure, it will be a strong incentive for the ordered company to be conscious of improvement of its information security level. As the “Cybersecurity Strategy” describes further improvement of information security level of governmental procurement, the government will actively standardize higher information security as a requirement for the governmental procurement. If higher information security is set at the time of procurement of systems, etc., by private companies, etc., then willingness of the management of companies, etc., to investments in information security will be encouraged, and as a result, it is expected that more human resources will be employed and better treated.

Currently, with regard to information security measures by the enterprises and other

organizations that handle important information concerning the national safety, based on “About Description of Information Security at the Time of Procurement” issued by the Deputy Chief Cabinet Secretary to the governmental departments, ministries and agencies in January 2012, it is decided that a Governmental department, ministry or agency should ask for preparation of a scheme to retain information security by a letter of procurement specifications, etc., when it concludes a contract in which a party other than the government shall handle important information concerning the national safety. The above-mentioned notice says, “The actual workers should include those persons who have qualifications with regard to information security based on the Act on Facilitation of Information Processing (law No. 90, 1970) or those who can prove that they have equivalent knowledge and skills, and those persons shall consider to continuously add new knowledge.”

To further strengthen these efforts, the “Standards for Information Security Measures for the Central Government Computer Systems (planned to be amended in March 2014)” states that the affiliations and specialties (qualifications, training course experiences concerning information security), etc., of the employees of the operation entrusted companies, including re-entrusted companies, shall be confirmed at the time of outsourcing of development and the operation of information systems. At the time of this confirmation, as it is important to check whether the employees have the latest skills, it is an idea to ask them to describe the year when they passed the Information Processing Engineer Test, by such mean as description of “Persons who passed the information security specialist test within three years or so” as a method to know that the employees can respond to changes in the situation of information security. In addition, for operation thereafter, it is not enough to simply ensure that the employees have qualifications and experiences of training courses: It should be required to further review the possibility of confirmation of whether persons having appropriate qualifications have worked at each phase, for example, whether the procedure for quality management of the delivered articles has been carried out by persons who were capable of inspection and audits with regard to information security. Where inspections and audits with regard to information security are carried out to improve information security quality, retention and improvement of the ability of the persons in charge are indispensable. It is required to attain it by such means as utilization of qualifications to prove the ability and provision of

training courses.

The efforts to improve information security quality through the setting of requirements for governmental procurement as mentioned above will broaden recognition of the importance of information security. In the same way, if making requirements for information security is widespread among contracts among private companies and other organizations, Japan's entire information security level will be improved, and thus it is expected that the demand for human resources for information security will increase.

(2) Information security as an essential ability

It is an urgent challenge to make efforts to solve the problem of qualitative and quantitative lack of workers engaged in information security. Considerable demand for human resources for information security is present, and thus it is strongly required to develop engineers who have the quality to meet that demand. At present, on the other hand, the number of the graduates from higher education institutes, such as universities, who have received education in information security is limited at a level of approximately 1,000 per year.[10] To solve problems of the qualitative lack of about 160,000 engineers and quantitative lack of about 80,000 engineers, efforts should be made not only to spread professional education at universities and other institutes, but also to improve information security skills of the existing engineers, such as system engineers, network engineers and programmers, the number of whom is estimated about 800,000[11] in Japan at present.

To this end, it is important for enterprises and other organizations to make efforts as follows for development of human resources for information security. To support these efforts, the government will actively make efforts for sharing of information on cyber-attack incidents, creation of cases based on that information, development of educational materials and programs, etc.

[10] Basic Investigation with Regard to Development of Human Resources for Information Security (April 2012, IPA)

[11] Of the number of persons by the IT skill standard profession described in the result of estimation of the number of persons related to IT skill standard profession (IT supply side) in "IT Human Resources White Paper 2013" (IPA), the total of the numbers of IT architects, project management, IT specialists, application specialists, software developers were added to the estimation of the number of IT human resources on the IT use side in order to calculate this number.

1) Efforts to make engineers engaged in information communications attain information security knowledge as their basic ability

It is important for enterprises, educational institutes, etc., to provide practical education to the engineers engaged in information communications, who form a volume zone of human resources expected to play practical roles in the information security field, which is essential to the design, development, and operation of information systems, and it is important for both vendors and users to share recognition of the necessity of information security as quality that takes information security measures from the system design phase and recognition of the essentiality of information security.

To heighten the reliability of the information communications technologies which will be required in the future growing fields (for example, fields, such as big data, agriculture, social infrastructures, health/medical care, etc., according to the Japan Revitalization Strategy (cabinet decision in June 2013)), it is essential to create products and services in a manner where information security is considered. From the viewpoint of strengthening of Japan's competitiveness, it is thought necessary for the engineers engaged in information communications to attain skills with regard to information security.

To this end, through activities, such as holding seminars for enterprises, the ministries concerned, industrial organizations, and other entities will actively foster activities of education and enlightenment towards engineers of enterprises, etc., aiming to let them consider information security as a factor in the quality of products/services offered by the enterprises, etc.

In addition, in order to fully respond to rapid advance in technologies, it is required to give not only opportunities of daily, continuously learning but also opportunities of systematic learning. For example, it is effective to provide a scheme in which people, after having a specific working experience, can receive intensive recurrent education at graduate schools, etc. Industry, academia, and government will, in collaboration, promote arrangement of an environment where it will be easy for people to receive this type of education.

It is also important to develop those human resources that can teach information security within an organization. As there are programs that create curricula and teaching materials used to teach basic contents of information communications technologies including information security and provide them to desiring organizations, it is important to effectively utilize these programs and at the same time to retain instructors. In addition, many enterprises and other organizations have already made efforts for leaning of basics of information security by such means as e-learning and it is important for them to improve the contents and quality of the learning. In addition, in order to obtain more practical knowledge, it is required to share incidents of cyber-attacks as described later, utilize education materials based on these cases, and review and improve the educational materials.

In particular, in the field of information security, or in the entire field of the information communications, it is urgently required to develop human resources that will involve themselves in the design and development of software that is related to the movement of everything. For example, when designing a system, engineers more often depend on general-purpose software and thus seldom create the software by themselves and understand its mechanism. In other words, the software products are becoming black boxes. Therefore, we now have a situation where we have to depend on the original software vendor in case of a failure.

On the other hand, in the control systems in Japan, there still exist some core software products that were developed by use of a unique OS, not the ready-made OS, and thus the systems, including their fine operation, have been controlled by use of what was built by the Japanese engineers. Recently, however, the time of retirement of many of these engineers is drawing near. Thus, it is important to communicate the basic technologies concerning the control systems to the subsequent generations. Under the circumstances, in order to enrich human resources for software as a basis, industry, academia, and the government will, in collaboration, foster educational programs to develop human resources that will be responsible for designing and development of software that will support the entire information communications technologies, and foster arrangement of an environment necessary to

communicate the fundamental technologies so far developed in Japan to the subsequent generations, by such means, for example, as making efforts to provide engineers after their retirement with opportunities to teach in educational institutes, etc.

2) Arrangements of evaluation criteria, qualification, etc., of information security ability

In order to evaluate the ability of human resources for information security and utilize the evaluation results in operation and treatment within the organization, the government needs to promote, among others, preparation of qualification tests with regard to information security, criteria to evaluate the skills, and educational programs.

As the required skills of human resources for information security greatly depend on their business fields, it is important to clarify the required ability and knowledge through improvement and utilization of the skill standards. At present the IPA presents the latest ability and knowledge with regard to human resources for information security in the common career and skill framework (CCSF)[12] and thus private enterprises, etc., should recognize the importance and actively promote efforts to utilize it. Based on this, it is required for enterprises to clearly show each employee the skill set required for his/her business by referring to the skill standards, visualize attainment of skills by each employee to objectively show it by utilization of the materials, etc., mentioned later, and show the meanings of, and how to use, the materials, etc., to indicate that the employee has the necessary skills at the time of new hiring, advancement, etc. In addition, a scheme is important by which the difference the levels of human resources educated in educational institutes and the levels required by enterprises can clearly be recognized by both. Therefore, the situation requires educational institutes, including universities and technical colleges, to review their education programs, etc., by employing needs of enterprises and in collaboration with them.

The IPA offers various information processing engineer tests from “IT Passport” putting

[12] A framework defined so as to be used as the common evaluation criteria in the individual occupational categories with regard to IT for development and evaluation of human resources for advanced IT. It is positioned as the common reference model of the IT skill standards (ITSS), the embedded technology skill standards (ETSS), and the users’ information systems skill standards (UISS). The information processing engineer tests are designed and conducted in conformity with the CCSF.

questions about basic knowledge to the “Information Security Specialist” putting questions about advanced expertise of information security. These tests are widely utilized by many enterprises and educational institutes, and thus fixed in the society. With regard to the test classification, the IPA reviewed the questioning configurations of tests to be provided in and after the spring of 2014 in order to respond to recent increased importance of information security. They enhance and broaden questioning with regard to information security by such means as increasing the rate of questions about information security field. Under the circumstances where the environment surrounding the information communications technologies is rapidly changing, the situation requires information processing engineer tests to always provide questions based on the latest technical trend, etc. In addition, to make the tests positioned as a test/qualification/certification system that can always evaluate and assure the practical ability about information security, we will review how the test system should be, by such means as offering continuous education after passing the test like overseas private qualifications and certifying the abilities of human resources for information security. Prior to this, it is important for the government and enterprises to encourage the staff to repetitively take the tests because they are judged by the year of passing am information processing engineer test and not only the pass/fail result but also the score is indicated.

As information security field is a considerably advancing field and the ability and knowledge required for an information security engineer are advancing, it is important for arrangement of qualifications, etc., to arrange an environment where educational materials and opportunities can be provided so that people can always obtain the latest information.

In addition, in order to gather excellent human resources in the information security field, it is necessary to widely gather human resources. Therefore, schemes are desired that re-utilize competent human resources after they reluctantly retire temporarily or need suspension from work. Thus, visualization of their abilities is effective as indices to be used for reemployment and job-changes. In addition, as it is necessary to arrange work environments as well as qualifications, we will review how the incentives should be for the workers having information security qualifications and will enlighten the consciousness with regard to the work environments, during the above-mentioned review of the qualification scheme.

3) Taking practical measures to improve skills of information security

A. Sharing of cyber-attack incidents and development of educational materials, etc., based on cases

For protection against cyber-attacks, it is important to accumulate practical knowledge, including the actual methods of cyber-attacks and the protection methods against them. To this end, it is very effective to utilize the past accidents and incidents with regard to information security as educational materials. For development of human resources for information security that can quickly and appropriately respond to actual accidents, etc., and for improvement of Japan's information security level, it is desired to effectively utilize the past accidents and incidents in higher education and human resource development within enterprises.

Therefore, we will review the methods to utilize, as educational materials, such information as the information on incidents concerning information security obtained by the administrative and other organizations, information on illegal programs, information on incidents detected by the administrative organizations, and information on incidents collected and analyzed by the investigating authorities, while considering the confidentiality of the information provider, the secret of investigation, etc., and obtaining consents of parties concerned. The government and the organizations concerned will actively promote arrangement of an environment including communities where these incidents will be studied and the information will be shared.

Specifically, the government-related organizations and the educational institutes will, in collaboration, analyze characteristic examples of cyber-attacks and create cases (forms that can be used as materials in analyses, studies and discussion of the accidents, etc., that have actually occurred, like the educational materials based on case studies used in business schools), and create practical educational materials and programs with which engineers and other human resources can think of countermeasures (including protection and attack methods) by use of the cases as subjects and can consider measures to be taken. At this time, it is important to develop contents of simulation types on which many people can easily work

and make them available to a wide range of engineers and education-related persons by use of the cloud and other technologies. Especially, ethics education is also important so that the engineers and other human resources will not pervert the attack methods after studying them.

B. Carrying out information security education, training, etc., by use of educational materials, etc.

It is important to provide the engineers who study information security with opportunities for education and training. We think it effective to use the various cyber-attack incidents mentioned above in the educational sites as educational materials. To this end, it is required to prepare curricula, manuals, etc., that correspond to the above-mentioned educational materials; collaborate with educational institutes, enterprises, etc., so that they can utilize the education materials; and when necessary, revise the educational materials based on the findings in the actual education courses.

Since FY 2013, the Ministry of Internal Affairs and Communications has provided LAN administrators, etc., of public agencies, enterprises, etc., with the CYDER[13] for incident response, etc., to the targeted attacks, with regard to practical training courses assuming actual cyber-attacks. In the future, we need to fully grasp the actual attack methods and to continuously promote practical training courses in environments similar to the actual operational environments.

At the Control System Security Center, the METI offers training and practice courses to control system engineers and user enterprises by using control security test beds. It is necessary as before to develop human resources through practical education and training by effectively using facilities like the above.

In Japan, unlike Europe and the USA, where career paths are formed by information security experts changing the organizations they belong to, persons who are not information security experts may be in charge of information security due to personnel reshuffles, etc., and therefore educational materials and programs are needed with which those persons can

[13] Cyber Defense Exercise with Recurrence

study information security in a short time. Under the circumstances, it is pointed out that experience-based learning methods including active learning and PBL[14] are effective. It is required to broaden these methods as we think that they support personnel exchanges between the generalists and the experts.

(3) Discovery and development of human resources with high expertise and outstanding ability

Those human resources are indispensable that have high expertise to respond to the daily changing cases and the advanced cases and lead information security field, and those that have outstanding ability. On the other hand, in order to find and develop such human resources, we need not only uniform educational materials and programs, but also human resource development through leading-edge R&D activities using test beds and support of growth by such means as preparing places that will help people exploit abilities.

1) Enhancement of higher education to develop human resources for information security that have high expertise

Information security experts are required to have advanced, wide knowledge and special abilities. In higher education institutes, such as universities, they must offer education that is the basis for this. At present, however, there are only very limited educational institutes that can, by themselves, prepare teachers who can sufficiently teach all the fields. Under the circumstances, it is effective that multiple universities arrange a scheme in collaboration. In addition, as putting into practice is important in the information security fields, it is desirable at the same time to promote collaboration between industry and academia.

The enPiT[15] by the Ministry of Education, Culture, Sports, Science and Technology (MEXT) fosters development of human resources having more practical information security abilities by forming a nationwide network of universities and industrial circles and providing practical education, such as problem based learning based on actual problems. We will continuously take action for collaboration among universities and between them and the industrial circles, aiming at development of advanced human resources.

[14] Problem Based Learning
[15] Education Network for Practical Information Technologies

Efforts to establish courses handling information security in universities and graduate schools are effective as efforts to provide enterprises and the like with those human resources that have specialist abilities and are immediately useful. In order to form a virtuous circle of demand and supply of human resources in the future, it is important for the government and the industrial circles to present the image of human resources they will need and thus, the government is required to play a leading role in the employment of those human resources that have advanced expertise.

Such educational institutes as technical colleges offer education in which the basic items and practical skills are combined. Such departments as information engineering departments have begun to introduce model core curricula aiming at the development of such engineers that firmly have the basic abilities concerning hardware and software and the abilities to develop practical information systems. In these curricula, they take up information security as a study item. It is expected that each school will continuously review retention of minimum ability criteria through introduction and promotion of the curricula In the future.

We think that the leaders in the workers mentioned in the “Promotion of information security measures as part of business operation strategy” ((1) 1)) play a role of linking the management and the workers. With regard to development of these persons, the higher educational institutes in the USA and South Korea are offering those human resources that are specialized in information security but also have knowledge in various special fields and knowledge necessary for operation of organizations, etc., and can respond to risks in cyberspace with a bird’s-eye view. In addition, there are some examples in which such human resources study more while going between the governmental organizations and private enterprises, etc., and lead the information security field. To heighten the international presence of Japan in the information security field in the future, the challenges include development of those human resources that have comprehensive abilities and rich experiences and can play active roles globally and establishment of a framework in which human resources can circulate between the governmental and private sectors. Thus, we will review these challenges specifically.

2) Discovery of outstanding human resources that can play active roles in the leading-edge fields and further improvement of their abilities

It is difficult to use ordinary education in order to develop those human resources that can play active roles not only in the information security field but also the leading-edge fields. In efforts to develop these human resources, it is important to find human resources by focusing their abilities and prepare places where they can work hard with competent engineers here and abroad to exploit their abilities.

Since 2004, the IPA has held the Security Camp program, which is an advanced educational program concerning information security and other fields offered to students under 22 years old, including those in primary and secondary education phases, by inviting top engineers who are successful at the forefront of the IT industry as instructors, aiming to find and develop young, excellent human resources that will be able to play important roles in the future IT industry.

Since 2000, in addition, the IPA has held the Exploratory IT Human Resources Project (the MITOH program) to find and develop young, outstanding resources (super creators) that have original ideas and skills to create innovations by fully utilizing the information communications technologies and have excellent abilities to utilize them. In this program, in order to actively evaluate originality, the IPA uses resources that have excellent abilities and experience in the software-related fields as the project managers (PMs) who examine the contents of proposals from their unique viewpoints, select development themes, instruct and advise the creators, manage progress in development, evaluate the development results, and take other actions. Furthermore, in FY 2014, the IPA will start a framework, the Cyber Rescue Party (provisional name), which will support organizations undergoing severe cyber-attacks that it will be difficult for only one organization to respond and that will make us entertain fears of expansion of social damage, aiming at restoration of ordinary activities and prevention of a recurrence. The framework will also respond to a short-term challenge of containment of damages from cyber-attacks, and at the same time aim to create human resources to work as leaders by hiring human resources having outstanding skills including the youth and by growing the

management abilities in OJTs under instructions by trainers. In addition, the Japan Network Security Association (JNSA) holds competition events called SECCON, in which the participants are grouped into the attacking team and the protecting team to test their abilities, aiming at development of Japanese information security engineers.

Through these frameworks including programs and contests, industry, academia, and the government will, in collaboration, firmly teach the importance and ethics of information security protection and continuously develop the necessary abilities and find human resources. It is important to enable the found human resources, etc., to fully utilize their abilities in the actual society. Consideration of collaboration among the ministries and agencies concerned and enterprises is also an issue to be reviewed in the future towards clarification of the image of human resources to be developed through these programs and contests.

Note that, if many more young people are interested in or attracted by the information security field, it will lead to not only discovery of excellent human resources but also broadening the range of human resources and strengthening of Japan's information security level. Furthermore, heightening of recognition in the society will lead to increase in the opportunities where human resources for information security actively work in enterprises, etc. Therefore, in order to appeal to the society, in particular to the youth, we will review enlightenment of contents with themes, such as the top-level human resources working in the information security field by use of the media that are helpful to broadening.

(4) Development of global level human resources

As globalization proceeds in every field including the enterprise activities, cyber-attacks have become borderless. To protect Japan from these cyber-attacks, we need to have global level abilities that exceed the attackers' abilities. Here, global level human resources do not simply mean excellence in use of foreign languages but mean such human resources that can sufficiently respond to global cyber-attacks[16] and to negotiate in international conferences,

[16] For example, the ability to set the subject of new methods of cyber-attacks and to cope with them.

etc., with state-of-the-art knowledge and abilities globally usable in their special fields. Not only those who are working overseas but also those working at home are required to have these abilities. In order to develop the global level human resources as mentioned above, it is desirable to make efforts to improve curricula in collaboration with overseas and domestic universities, enterprises, etc., aiming at active development of human resources at first in educational institutes, such as universities, based on the latest international trends and the like. In addition, for example, we think that lectures and exercises with overseas and domestic human resources having practical experiences with regard to information security is helpful to development of global level human resources. Thereafter, it is desirable that human resources that have received education as mentioned above should heighten their abilities in friendly rivalry and at the same time that a virtuous cycle should be created in the development of human resources in which these human resources will play roles of developing the next generation of human resources. Furthermore, it is expected that active employment of these human resources by enterprises, governmental organization, and the like will lead to improvement in Japan's information security level. As an example of improvement of curricula to development global level resources, in 2013, an education/research project started in universities and graduate schools under the Program of Evaluation Model/Base Model Demonstration in Collaboration between Industry and Academia of METI, aiming to develop human resources for information security that can work at global sites.

In order to develop global level human resources, in addition, it is necessary to share as many international experiences and as many pieces of information as possible. It is thought effective to increase opportunities to study hard with competent engineers overseas by such means as collaboration with foreign organizations, participation in international conferences, support of studying abroad, holding international conferences in Japan, and internationalization of competitions currently held domestically. To this end, the government will actively support international conferences gathering top-level human resources and competitions.

For example, we will continuously exchange information with NIST[17] in USA and KISA[18] in South Korea and participate in FIRST[19], which is an international conference consisting of governmental and private organizations concerning incident response. In addition, we will share information on threats with CSIRT[20] and proceed in review of establishment of a framework for collaborative response. Actively utilizing these opportunities, we will establish an environment where human resources for information security can work in friendly rivalry, by such means as sharing of the latest technical trends with regard to protection and attack, offering of opportunities of international information exchanges and human intercourse, promotion of collaboration in researches and projects, offering of opportunities of recruitment, and forming of international communities.

Referring to a competition event in USA, DEFCON CTF,[21] which gathers information security specialists worldwide and help them improve their abilities through the competition, we think it effective to increase opportunities where people can study by such means as supporting holding of international conferences and the like where top-level specialists globally gather, have discussions with globally top-level people and compare themselves with others. Therefore, we will foster such efforts as invitation of participants in various competition events from overseas and making participant qualifications open.

(5) Development of human resources in governmental organizations, etc.

In order to improve the level of Japan's information security, it is important for the governmental organizations, etc., in particular, to voluntarily and actively make efforts in the development of human resources. To this end, we will try to further improve the security level with regard to information and information systems and at the same time, continuously and firmly foster improvement of abilities of persons in charge of systems and heightening of managing persons' understanding of information security. Here we describe our concrete efforts with regard to human resource development, recruitment, etc., to retain necessary

[17] National Institute of Standards and Technology
[18] Korea Internet & Security Agency
[19] Forum of Incident Response and Security Teams
[20] Computer Security Incident Response Team
[21] Capture The Frag

human resources for information security by the government, aiming at enrichment and enhancement of schemes to respond to the future cyber-attacks and the like.

1) Recruitment and development of officers that can respond to risks in cyberspace

Based on increased risks in the cyberspace in these days, it is required to assign officers having a certain level of special knowledge as staff members in charge of information security who are daylily involved in system operation, etc. Therefore, not only the CISO advisers but also individual officers should enhance the scheme to substantially support CISO, and at the same time, the staff members in charge of information security should continuously and firmly make efforts in special consideration for recruitment and personnel rotation, active government-private exchanges with operators and the like specialized in information security, based on “About Development, etc., of Human Resources Concerning Staff Members in Charge of Information Security in Individual Ministries and Agencies” issued in June 2012 by the Deputy Chief Cabinet Secretary to the Director Generals, etc.

It is needed to reform the way of thinking concerning information security within the government to lead to personnel evaluation in which the officers in charge of information security should not be adversely evaluated with regard to occurrence of a trouble in the system of their own organization but should be positively evaluated with regard to appropriate system management and occurrence of nothing by prevention of trouble. In addition, we will review incentives to the officers who have information security-related qualifications in order to encourage the officers to deepen their knowledge about information security and obtain information security-related qualifications.

It is important for officers not to continuously work in a specific ministry or agency, but to work on business in different ministries/agencies, the Cabinet Secretariat, etc., which is similar to theirs in their own offices so that they can broaden their experiences and that the officers in charge of information security in different ministries/agencies can collaboratively respond to cyber-attacks. To this end, in June 2012, we founded CYMAT,[22] which offers swift support in

[22] CYber incident Mobile Assistance Team

cross-sectional collaboration aiming to prevent damages from broadening, etc., in case of occurrence of an incident, etc., such as a large-scale cyber-attack on a governmental organization to which governmental organizations should collaboratively respond in a quick and appropriate manner. To develop and maintain human resources that can respond to incidents with regard to information security to which the governmental organizations must make one body to respond, CYMAT is regularly offering training courses and the like. We will further strengthen collaboration to enhance the framework for retention of information security in collaboration among the governmental organizations.

At present, the Cabinet Secretariat Information Security Center (NISC) is making efforts to improve the abilities of the officers through training courses within the organization and CYMAT, and in the future, too, will proceed in development and recruitment of internal human resources that can summarize information and the like concerning incidents with regard to cyber-attacks, and analyze the overseas and domestic trends and the technical trends. In addition, we will incorporate the result of the risk evaluation we are currently carrying out into our human resources development.

As pointed out in the “Cybersecurity Strategy”, in addition, in an effort to strengthen its functions, NISC is to arrange its organizational scheme, setting 2015 as the target year of completion, by such means as retention of human resources by personnel management including recruitment and development of dedicated officers. As viewed in NISC, which promotes further efforts to make itself a career path of human resources for advanced information security, the government, as a whole, will continuously make efforts to effectively utilize not only the internal resources but also external excellent resources by personnel exchanges between the government and the private sector. The government will play a leading role in development and recruitment of specialists like this because it will indicates the image of desired image human resources to the society and trigger the demand for human resources for information security.

It is desired, in the future, to form career paths where as seen in the USA and South Korea, the specialists of information security will be able to gain experience in the individual

organizations, such as the government, private enterprises, research institutes, and educational institutes and enhance their skills as human resources for comprehensive information security.

Each ministry/agency has completed arrangement of CSIRT as a framework to quickly and appropriately respond to occurrence of an incidence concerning information security by the end of fiscal year 2012. In addition, in order to minimize the damages due to undergoing of a targeted e-mail attacks, etc., and quickly and appropriately respond, the CSIRT staff members of the individual ministries and agencies will hold response training assuming occurrence of a large-scale cyber-attack incident, etc. To appropriately respond to cybercrimes that are getting more complicated and sophisticated, in the Ministry of Justice, the prosecutors and their assistant officers hold nationwide training courses where participants can obtain knowledge and skills necessary for investigation as an effort to enhance the abilities of investigation. On the other hand, the National Police Agency strengthens the framework for patrolling by such means as development of human resources and at the same time strengthens support to establishment and development of volunteer organizations for cybercrime prevention and their activities. In order to make a safe and reliable cyberspace, as it is indispensable to enhance development of human resources for these measures for cybercrime prevention, we will firmly promote it.

2) Enlightenment of awareness of information security of entire government officials and holding of training and practice courses

In order to improve information security, it is insufficient to only make efforts to improve the abilities of the information systems and the workers handling them but it is needed to heighten the awareness and skills of the entire officials. Therefore, governmental organizations are required to make efforts to improve the skills by always holding training and practice courses.

At present, the Cabinet Secretariat is creating and distributing educational materials targeting government officials, incorporating programs concerning information security into various training curricula, and making efforts to share recognition with regard to information security and to further improve the knowledge and the skills. Utilizing the above-mentioned support,

etc., by the Cabinet Secretariat, the individual ministries and agencies are developing human resources for information security. In the future too, we will continue these practical training courses and the like while revising them according to changes in the environment whenever necessary.

As a measures to enlighten the awareness of information security of the entire government officials and to improve the abilities, in addition, the above-mentioned document, “About Development, etc., of Human Resources Concerning Staff Members in Charge of Information Security in Individual Ministries and Agencies” (June 2012) requests us to confirm grounding in information security of the applicants at the time of interviews for official employment examinations. Based on this, the government confirms possession of qualifications of the IT passport and other qualifications related to information security at the time of interviews for official employment examinations, and makes other various efforts to develop human resources for information security in the government, and therefore we will continuously and firmly take these actions.

3) Development of human resources in critical infrastructure operators, etc.

If the functionality of a critical infrastructure is shut down, degraded or becomes unavailable, the people’s lives and the social and economic activities in Japan may be considerably affected. Therefore, it is desired for the critical infrastructure operators and the like to more actively develop human resources within the organizations so that the necessary information security can be retained. Specifically, based on the “

The Third Action Plan on Information Security Measures for Critical Infrastructures (to be amended in March 2014), the critical infrastructure operators, etc., are required to continuously retain, as a type of resources for operation, human resources necessary for configuration and operation of systems, evaluation of risk origins, and preparation and taking of measures based on it. On the other hand, the Cabinet Secretariat will improve and continuously carry out the “Cross-Cutting Exercises” in collaboration with the ministries/agencies related to the critical infrastructures, and at the same time, gives necessary support to the critical infrastructure operators for development of human resources including enlightenment of awareness and improvement of skills, through the publicity and

hearing activities concerning information security of the critical infrastructures, the international collaborations, and the arrangements of regulations.

(6) Enhancement, etc., of information communications technology education in educational institutes

1) Enhancement of education with regard to information communications technologies at primary and secondary education phases

In the primary and secondary education phases, since FY 2003, the information has been taken up as a required subject. By amendments in the government Course Guidelines in 2008, the contents with regard to information security was enhanced. The information course target to grow abilities and attitudes to actively respond to progress computerization of the society by obtaining knowledge, skills and scientific ways of thinking to utilize information and information means and by making students understand roles played and effects made by information and information technologies in the society. Based on this intention, we will firmly promote education with regard to information security in senior high schools. By amendments in the government Course Guidelines for elementary schools and junior high schools in 2008, the learning activities were enhanced to develop information morality including information security through instructions of individual subjects according to the development stages. It is important to continuously and firmly promote education with regard to information morality. In addition, in learning of information communications technologies, which are the basis of information security, it is important to study, and get interested in, the computer principles and the basics of computer programming and the like. By amendments in the government Course Guidelines in 2008, in the technical arts section of the subject of technical arts and home economics for junior high schools, the learning contents were enhanced with regard to information communications technologies including programming. Continuously, we will actively promote education, etc., about programming and the like from the primary and secondary education phases. It is required to continuously promote this type of education with regard to information communications technologies and to enable it to more enhance logical ways of thinking necessary for information processing and understanding of the basics of information communications technologies.

2) Strengthening of practices to enhance practical abilities in higher education phase

In universities, technical colleges, and other institutes, it is desired to further heighten the practical abilities for information communications technologies necessary for information-related engineers. In particular, information security is a practical application field where the computer science including information communications technologies is fully utilized, and thus we should focus on it as one of items that are optimum to grow the future excellent information-related engineers.

The above-mentioned policy also stressed in “The Strategy for Developing Human resources with Creative IT Skills”: *the desire is to strengthen practical skills in information-related education in higher education institutes and to learn the ethics and basics that are the basis of the practical skills*. As measures to enhance the practical skills, it is required for higher educational institute to develop the courses with more practical workshops, which is conducted through the industry and the academia.

For colleges and departments specialized in information, it is desirable, at the time of entrance examinations, under their own admission policies, to appropriately evaluate applicants’ attainments of logical ways of thinking required for information processing and of understanding of the basics of information communications technologies that they have had at senior high schools, so that the students can smoothly proceed to the specialized education after entrance. For enterprises, in addition, it should be promoted to confirm basic knowledge and abilities of human resources at the time of employment to enhance the basic knowledge and practical skills of students who have received information-related education. Examples include indication of the skill standards required for the individual occupational categories and utilization of qualification programs.

3) Education of teachers with regard to information security

In order to further enhance the learning activities concerning information security in the primary and secondary education institutes, it is required to have teachers having sufficient abilities. To this end, through the supervisors of school education, in principle, of prefectures and ordinate-designated cities, the situation requires every teacher to continuously make efforts to improve his/her capability in the instruction of information security. “The Strategy for Developing Human resources with Creative IT Skills” states the importance of methodology

which can make contributions to enhance their teaching skills for all teachers. Here mentioned teaching skills include information security. The higher education institutes also offer education with regard to information security at their own discretion. However, for example, it is thought that the creators of education curricula concerning common/general education in a university do not have sufficient recognition to information security and in addition, it is pointed out, among others, that there are not many teachers with expertise. Therefore, it is necessary to clarify the level of human resources grown by the educational institutes. In addition, it is also necessary to review, in collaboration among industry, academia, and the government, the opportunities for the teachers growing those human resources to attain the necessary skills and the educational materials and the like for the teachers, by such means as utilization of the abilities in the private sector including arrangement of an environment where retired engineers and other human resources can actively work regardless of academic background such as Ph.D.

4) Indication of career paths of human resources for information security

Even if students, etc., are interested in the information security field and consider it as their future occupations, what types of career paths are present for the specialists and therefore the future perspective, the stability, etc., as specialists are not clear. This is pointed out as a factor of lack of human resources for information security.

Based on survey by interviews with human resources currently working in the information security field, therefore, the IPA has created career path models and made them open, and in addition, is making such efforts as offer of reference materials to potential information security specialists. In addition, the JNSA is holding a program to support internships in enterprises, aiming to provide those students that desire to work utilizing their information security skills in the future, with opportunities of working experiences that attract them to information security industry.

On consideration that information security is necessary along with the information communications technologies that are considered necessary in every growth sector in the future, it is required to develop those engineers that have knowledge of cross-sectional

information security technologies as the basic knowledge to engage themselves in the information communications. Therefore, it is needed to develop human resources and indication career paths by taking learning of information security knowledge as a precondition, not only for information security specialists but also for the entire engineers engaged in the information communications. By broadening information security among the engineers engaged in information communications as an essential ability and acquiring broad knowledge such as business economics, law, psychology etc., it is anticipated that career paths can be indicated where information security engineers engaged in information communications will enter the management in their organizations, and that these engineers will master information security technologies and actively work as advanced specialists. At this time, it is important to focus on those who have strategic ways of thinking concerning business management, information communications technologies, and information security, and have abilities to communicate with management.

Specifically, image of each layer of human resources are as mentioned below.

For leaders on the supply side of IT products and services, it would be expected that they have ability to understand and take into consideration users' needs, situation, cost etc. and coordinate workers, and make an appropriate proposal to management at each stage such as planning, design, development, operation etc. of the system of their products and services. For workers on this side, it would be expected that they acquire information security as a fundamental skill and put them into practice.

On the other hand, for leaders on the user side of IT products and services, it would be expected that they have ability to understand workflow and information flow of related section inside and outside an organization, and coordinate workers, and offer the requirement of information security to the supply side as one of the risks on execution of operation, and provide an explanation to management in terms of a business strategy. For workers on this side, it would be expected that they are able to understand information security and make everyday use and operation of information systems possible.

For management, it would be needed basic ability to consider how to utilize IT, where information security is positioned, and what business strategy is necessary at responding security incidents, as a part of business risks on reviewing and enforcement of business

strategy.

In addition, it would be hoped that career path which engineers engaged in information security are promoted to management in an organization will be formed by making engineers engaged in information communications attain information security knowledge as their basic ability, and diverse knowledge such as business economics, law, psycology, etc. and/or they play an active role as advanced specialist by making them master information security. In this regard, it is important to take particular note of strategic thinking skill about management, information communications, information security etc., and leaders who have communication skill between management and workers.

4. Conclusion

Based on the Cybersecurity Strategy created in June 2013, to solve problems, including qualitative and quantitative lack of human resources for information security, in addition to the discovery and development of outstanding human resources, which is the major part of measures to develop human resources for information security in the individual ministries, this program indicates the future policies and measures with regard to reform of awareness of the management, promotion of information security measures as part of the business management strategy, setting of information security requirements for procurement, information security as an essential capability for the engineers engaged in information communications, efforts to make engineers be aware of information security, arrangement of evaluation standards, qualifications, etc., concerning information security abilities, and practical efforts to improve information security skills by use of educational materials based on examples and cases of cyber-attacks. In addition to the continuous discovery and development of human resources having advanced specialties and outstanding abilities, we review development of human resources at a global level, human resources development in the governmental organizations, etc., and enhancement of education of information communications technologies in the educational institutes, and show the future policies and measures.

On the other hand, for example, although qualitative and quantitative lack of human resources for information security is made clear, the actual situation is ambiguous, including in what fields and for what abilities human resources are wanted. In the future, therefore, it is required to study and understand the results of execution of the measures shown here, and at the same time it is important to make arrangements, etc., for the indices showing the progresses of the measures (for example, enhancement of statistics about human resources for software and software industry dynamics) and constantly review the measures based on the result.

Also, it is also important to review, in collaboration among industry, academia, and the government, since arrangements of evaluation criteria, qualification, etc. should be related to the image of human resources needed actually by the society.

In addition, it has been decided that the Olympic Games and the Paralympic Games would be held in Tokyo in 2020 and thus, from the international viewpoint, it is required to enhance Japan's abilities to utilize the information communications technologies and protect from cyber-attacks. To support it, therefore, we think that human resources for information security will be more desired.

Development of human resources is not a matter that completes in a short time but a matter on which we have to work for a long time. In particular, in order to create an environment required to develop human resources concerning information security, we need to make cross-sectional efforts related to extensive knowledge of the entire information communications, various frameworks in other fields including education, future utilization of the information communications technologies in the Japanese industries, and finally, such items as frameworks, awareness, etc., in the Japanese society as a whole.

To this end, to make common recognition and awareness shared among the organizations and parties concerned in industry, academia, and the government, the government will comprehensively promote active measures, not only from the viewpoint of information security, but also considering the changes in the environment, and making collaboration with other related measures. Specifically, in the fiscal year plan to be prepared by the Information Security Policy Council, we will clarify the individual measures to be taken by the responsible ministries/agencies based on this program and take the measures from the viewpoints of both demand and supply aiming at a virtuous cycle of human resources for information security. In addition, the Information Security Policy Council, the working groups thereunder and the like will carry out evaluation in every fiscal year, execute follow-up including review of necessary measures, and disclose these evaluation results in the annual report of every fiscal year, so as to promote evaluations and measures from citizens' point of view by promotion of "visualization" of the measures in the efforts to establish the PDCA cycle.

For the private businesses, etc., in addition, it is expected that, if they can grasp information security as a means of risk management, the demand for human resources for information security including those who communicate with the management will be apparent and the

career paths for the management responsible for risk management in enterprises, etc., will be established.

We strongly expect that, through these efforts, a virtuous cycle will be created in the demand and supply of human resources and the level of Japan's information security will be improved.