Information Security Outreach and Awareness Program

July 8, 2011
Established by the Information Security Policy Council

Table of contents

1. Preface

As economic activities and social life have been increasingly relying on information communication technologies in recent years, information security risks have also been becoming more complex and diverse. Therefore, it is an urgent matter to establish information security that is far superior to the current practice. In response to such changes in the social situation, the Information Security Policy Council (Chairperson: Chief Cabinet Secretary) has developed the "Information Security Strategy for Protecting the Nation" (May 11, 2010, hereinafter "Strategy") and the annual plan of information security strategy the "Information Security 2010" (July 22, 2010, hereinafter "Annual Plan") to promote general information security policies among public and private sectors.

Dissemination of and enlightenment on information security is one of the particularly important policies and there have been various measures taken in the concerned agencies in order to secure and improve the overall information security level in Japan and to fulfill our role and responsibilities in the international society. However, information security is a broad and varied area and cannot be understood and correctly dealt with without technical and specialized knowledge. Also, effects of our activities for outreach and awareness so far have not been enough.

Therefore, the "Information Security Outreach and Awareness Program" (hereinafter "Outreach and Awareness Program") is developed to systematically organize outreach and awareness policies based on the Strategy and Annual Plan and execute more effectively under close collaboration of public and private sectors.

2. People and enterprise awareness of information security

Roles of "information" in people's lives have become very important and people's lives are increasingly dependent on information communications technologies. Protecting people's information assets and establishing information security have become more crucial than ever since rights and benefits of people as the users of the information communications technologies must be protected. At the same time an environment should be established for the people who are aware of risks concerning information communications technologies can apply information security measures. Currently, approximately 80% of individuals and enterprises have concerns in information security, and this issue should be resolved quickly for the further promote the use of information communication technologies. Therefore, it is extremely important to vigorously promote dissemination of and enlightenment on information security.

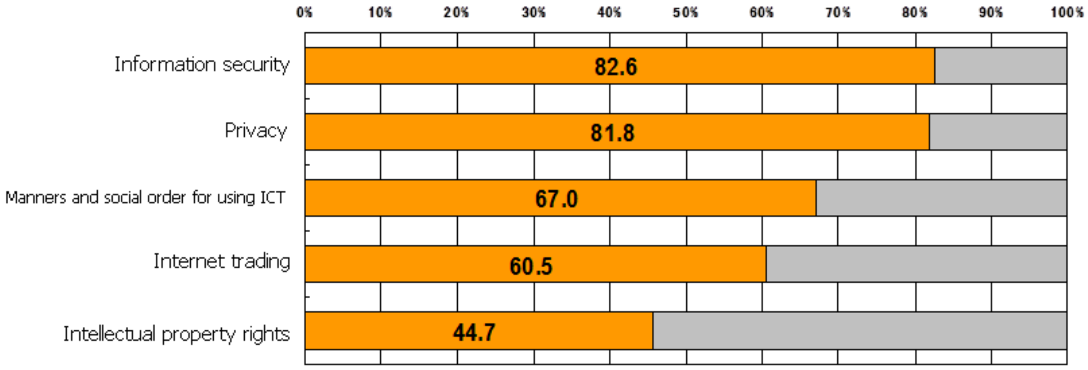


Figure 1-1. Concerns about safety of information communications (individuals)[1]

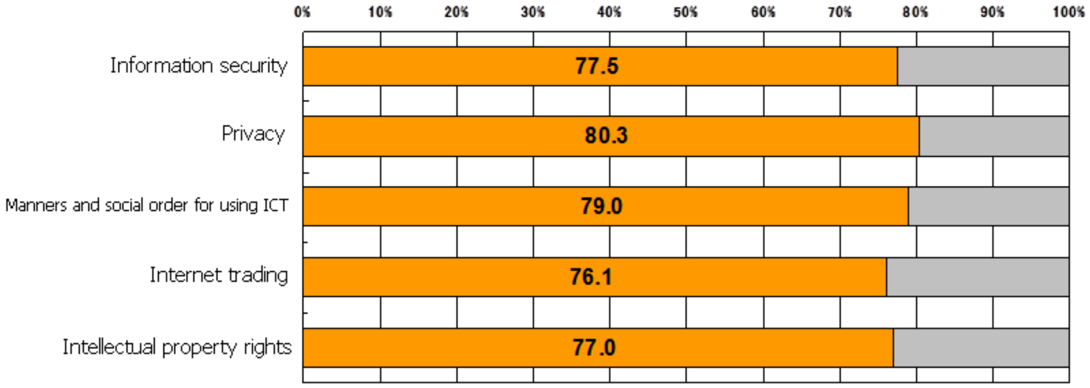


Figure 1-2. Concerns about safety of information communications (enterprises)[2]

[1] Source: "Research on Safe and Secure Use of ICT in the Ubiquitous Net Society" (2009) by the Ministry of Internal Affairs and Communications

[2] Source: "Research on Safe and Secure Use of ICT in the Ubiquitous Net Society" (2009) by the Ministry of Internal Affairs and Communications

While individuals and enterprises are highly concerned about information security in Japan, approximately 80% of households have implemented some form of information security measures.

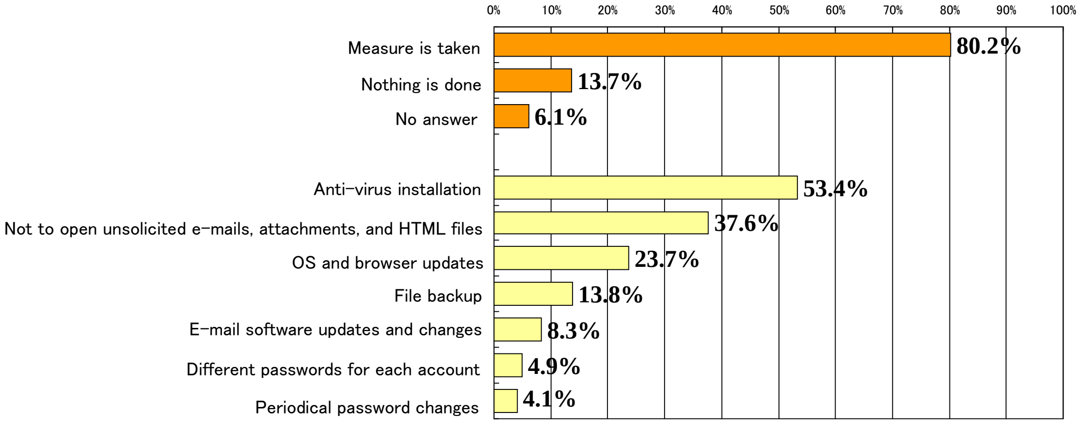


Figure 2-1. Security measures application (households) (multiple-choice question)[3]

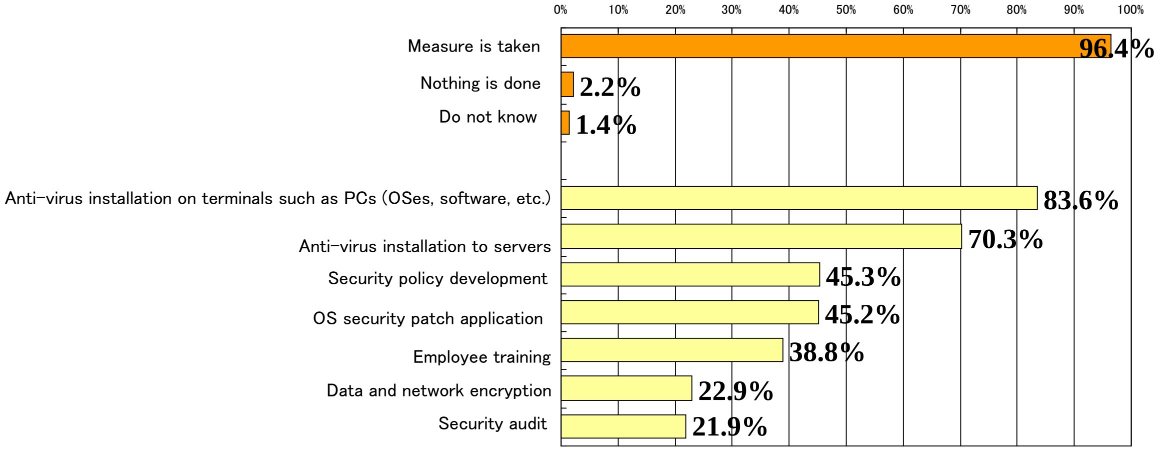


Figure 2-2. Security measures application (enterprises) (multiple-choice question)

[3] Source: "Communications Usage Trend Report 2010" (2011) by the Ministry of Internal Affairs and Communications.

International comparison shows Japanese have the least confidence in safety of information communications as 34.3% among 7 most advanced countries in ICT (Japan, U.S.A., U.K., Korea, Singapore, Denmark, and Sweden).

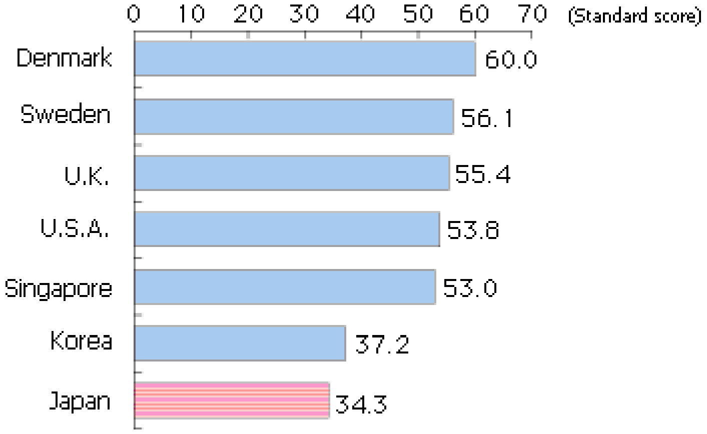


Figure 3. International ranking of confidence in information communications[4]

Also another research over 12 countries found only 11% (lowest among 12 countries) of Japanese answered "My computer has been remotely hacked" whereas 55% (highest among 12 countries) of them answered "Concerned about safety of my private information". This shows that Japanese information communication technology users do not always relate the secure state to the sense of security; therefore, outreach and awareness should also target to improve the sense of security in addition to the promoting security measures.

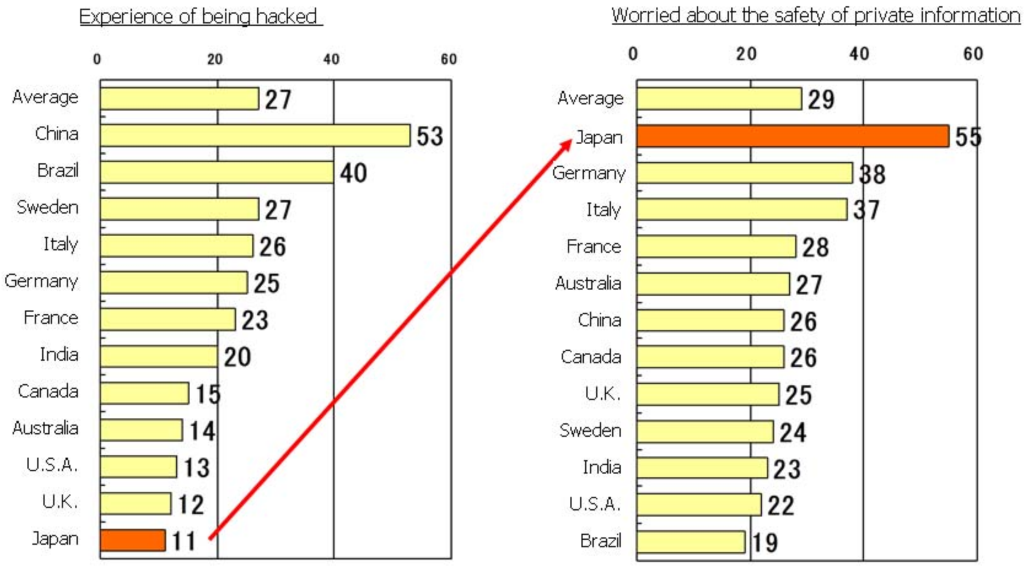


Figure 4. Relationships between "Experience of the own PC being hacked" and "Safety of private information"[5]

[4] "International Comparison of ICT Trend" by the Ministry of Internal Affairs and Communications (2009)

[5] Source: "Norton Online Living Report 2009" by Symantec (2009).

3. Previous approaches and issues dissemination of and enlightenment on information security

This chapter describes the previous approaches and issues dissemination of and enlightenment on information security for each intended subject.

(1) General pubic

Most popular concerns about Internet among general public are "Virus infection", "Don't know which security measures are needed", and "Security threats are too difficult to understand"[6].

On the other hand, another research shows[7] the sense of insecurity in the use of information communication technologies is higher among users with little and infrequent experience in the Internet whereas it becomes lower as users gain more experience and use information communications more frequently.

Therefore, it is important to promote the proactive use of information communication technologies and encourage users with little interest in information security (hereinafter "IS indifferent group") to gain more experience and naturally learn the necessary practice. Information security should be communicated with plain and simple languages without causing the sense of anxiety unnecessarily. A point of contact may be established to give advice to users concerned about information security.

It is also very important that users should be made aware that leaving their own virus infection makes themselves part of the attackers such as spreading the virus, transmitting e-mail spam, illegal access, DoS attacks, etc. without knowing as it was shown in the recent spread of bots[8].

The government has been making outreach and awareness efforts though various seminars and websites. Appropriate information should be provided to all individuals though different methods to promote understanding of the IS indifferent group.

(2) Senior citizens

Aging is rapidly progressing in Japan and it is very important to accelerate information security measures in senior citizens. The approach should be worked out carefully and must be communicated intelligibly, in plain language, and patiently for senior citizens. Special consideration should be given to avoid the situation where they feel scared of using information communications technologies due to difficult terminologies in the Internet and fail to get the benefit they could have enjoyed.

[6] Source: "Communications Usage Trend Report 2009" (April 2010) by the Ministry of Internal Affairs and Communications.

[7] Source: "Research on Safe and Secure Use of ICT in the Ubiquitous Net Society" (March 2009) by the Ministry of Internal Affairs and Communications

[8] "Bots" were malware that the malicious third party can remotely control the infected computer through the internet.

(3) Teachers

According to the research by the Ministry of Education, Culture, Sports, Science and Technology, 30% of teachers[9] are not confident in their educational abilities in information ethics[10] and the use of information communication technologies. Teachers' knowledge in information security is not sufficient to teach pupils and students who are digital native. Also, schools are the place where sensitive personal information of students is handled, and teachers are responsible for appropriately managing the information. It is important to provide appropriate information concerning information security at the right time to teachers who are guiding pupils and students, and managing information.

(4) Pupils and students

Outreach and awareness in schools should be effective to raise awareness of information security among the young generation. Education on information ethics has been incorporated into Government course Guidelines and proactive outreach and awareness efforts to promote information security should be continuously made.

(5) Households

Outreach and awareness in households should be necessary to raise awareness of information security among the young generation. According to the research by the Cabinet Secretariat[11] parents' concerns on the children's use of the Internet are "Giving the name and address too easily" and "Virus infection". To the question who knows the Internet more, the answer is increasingly "Children" as the children's grade increases. Meanwhile, only about a half of households have any rules for the use of mobile phones and personal computers in place. This shows that outreach and awareness in households are still an important issue.

(6) Enterprise management

Enterprise management should develop profound understanding that establishing and maintaining information security is the enterprise's management issue. Should a large scale information leakage occur in today's environment where national awareness of information security such as private information protection is high, it is unavoidable that the leakage will become a critical problem that directly impacts the enterprise management.

On the other hand, establishing and maintaining information security is vital for enterprise management regardless of the size of the enterprise in order to protect intellectual assets such as technical information, remain highly competitive, and develop the enterprise further.

Vitality of Japanese economy depends upon management ' attitude to proactively establish and maintain information security as their own problem without leaving it to

[9] Teachers in public schools (elementally, junior high, high, secondary education, and special support education schools) in Japan.

[10] Basic concept and attitude for appropriate activities in the information society

[11] Source: "Internet Usage by Youth Report 2009" (March 2010) by the Cabinet Secretariat

employees or related companies.

(7) Enterprise employees

More than 40% of enterprises identified low security awareness among employees as the problem in the use of information communication networks. This is particularly serious problem in small to medium-sized enterprises with limited human resources, and special considerations should be given in dissemination of and enlightenment on information security.

The following common issues are also pointed out in addition to the above issues specific to the subject.

- Sharing lessons learned from information security incidents

In today's world with highly developed information communication technologies, an information security incident on an individual or enterprise may spread across the whole society. It is very important for everyone to apply information security measures to prevent an incident from occurring, and be ready to respond swiftly after an incident.

However, currently the lessons learned from information security incidents are not shared among organizations and individuals. It is important to learn from such lessons to reinforce information security measures.

4. Environmental changes around information security

The implemented environments and users of information communication technologies, and changes in information security threats should be considered as described below when examining the specific approach for dissemination of and enlightenment on information security.

(1) Environmental changes

There are 94 million Internet users in Japan in 2010. The diffusion rate is 78.0% of the population, and more than 60% use the Internet with their mobile phones. The number of SNS users are expected to raise rapidly due to the development of the mobile environment as their functionalities develop further such as smartphones, while new media such as social network services (hereinafter "SNS") are becoming popular.

The environment of information communications technologies is rapidly becoming more complex and diverse as indicated by the expanding use of cloud computing. Information security threats to users are changing day-to-day as new services emerge and information communication devices become diverse.

(2) User changes

The Internet usage is growing most rapidly in the generation over 60. The Internet usage of senior citizens is expected to continue rising as the aging progresses.

Also, 80% of elementary school pupils, approximately 85% of junior high school pupils, and 90% of high school pupils use personal computers and most of those use the Internet. Also the use of the Internet with mobile phones is high in the young generation. Those digital natives[12] are building the network using SNS through new social media such as social games, micro blogs.

While emerging new users and diverse life styles will increase socioeconomic activities' dependency on the Internet, a growing number of users with low information security awareness will also increase risks such as unintended personal information leakage and malicious falsification of information.

(3) Information security threats with more complexity and diversity

[12] "Digital natives" are the generation who were born in and grew up in the environment with the Internet and personal computers. They have familiarized themselves with mobile phones, homepages, and Internet search engines ever since they were very young, and are able to skillfully use social media such as blogs, SNS, and movie sharing sites, and cloud computing. (Source: Research commissioned by the Ministry of Internal Affairs and Communications "Social Media Usage Report" on March, 24, 2010)

Previously computer viruses only caused problems on the infected computers and spread themselves; however, in recent years, a type of viruses called Bots is spreading. The malicious third party can remotely control the infected computers via the Internet. The attackers launch DoS attacks on web sites and transmit e-mail spam by remotely controlling many infected computers.

Meanwhile, viruses with multiple infection routes and viruses designed to attack a specific organization or system have emerged and there was an extremely sophisticated large scale attack (Stuxnet) on the control system of plants which are not connected to the Internet occurred overseas. Therefore, we must respond to attacks which were previously unthinkable.

5. Basic approach

The following describes the government's basic approach to promote dissemination of and enlightenment on information security based on the environmental changes of information security and the past approach and issues concerning information security outreach and awareness.

Basic policies

Information security measures for government agencies and critical infrastructure are the area where the government takes initiative. On the contrary, information security measures for individuals and enterprises are their initiative based on the individual's behavioral principles, and are the area where the government should provide active support. Therefore, dissemination of and enlightenment on information security are not particular matters which should be left to individuals or enterprises. The outreach and awareness program defines common sense, manners, and customs of information security for each subject as "Culture of Information Security", and describes where to focus and what to do in order to spread this "Culture of Information Security". When this "Culture of Information Security" takes root in Japan, dissemination of and enlightenment of information security are in progress.

"Culture of Security" is a concept proposed in OECD (Organization for Economic Co-operation and Development) in 2002. It is defined as "a focus on security in the development of information systems and networks, and the adoption of new ways of thinking and behaving when using and interacting within information systems and networks". This concept is very important in dealing with the ever-changing information security environment and it has been mentioned in the "First National Strategy on Information Security" (February 2006) to disseminate it.

However, public awareness of information security has not been raised as it was revealed by the recent events. We should renew our efforts to define and spread "Culture of Information Security".

(1) Definition of "Culture of Information Security"

"Culture of Information Security" in Japan is defined as follows based on the Basic Act on the Formation of an Advanced Information and Telecommunications Network Society (Act No. 144 of 2000) Article 22 (Ensuring of Security of Advanced Information and Telecommunications Networks, etc.)[13].

"Culture of Information Security" is "ways of thinking and behaving for security and reliability in development and operation of information communication networks, and the safe and secure use of people's information networks".

[13] Basic Act on the Formation of an Advanced Information and Telecommunications Network Society
Article 22
Strategies developed to form an advanced information and telecommunications network society shall ensure that action is taken to achieve and maintain security and reliability of advanced information and telecommunications networks, to protect personal information and other actions necessary to enable citizens to use such networks without anxiety.

(2) 6 principles of "Culture of Information Security"

The following are 6 principles of "Culture of Information Security" and should be established in day-to-day socioeconomic activities.

1) Awareness

Users of information communication technologies should be aware of what they can do to secure and reinforce safety and reliability in the development, operation, and use of information communication networks. Users should be aware of information security risks and available preventive measures first. Also they should be aware that they might cause a nuisance to other users by not applying their own information security measures because they are all connected via information communication networks.

2) Responsibility

Users of information communication technologies should be aware of their responsibilities to secure safety and reliability of information communication networks according to their roles. They should be aware of their responsibilities according to their roles such as ones who implements should endeavor to implement and operate safe and secure information communication network systems, and ones who uses should endeavor to use the information communication networks in the latest and safe status.

3) Response

Users of information communication technologies should be aware of the changes caused by the progress of information communication technologies and respond appropriately. They should take swift and effective action for preventing, detecting, and responding to information security issues.

4) Cooperation

Users of information communication technologies should cooperate with other users to resolve information security problems and issues. They should be aware that the damage may spread rapidly and widely because they are connected via information communication networks. Users should be encouraged to cooperate through appropriate information sharing and coordinated responses in public-private sector collaboration and international collaboration.

5) Ethics

Inappropriate information security measures may cause a nuisance to third parties in addition to the user himself. Each user should have autonomous standards of conduct and take social responsibilities without being forced by others. Safe and secure society can only be implemented by everyone's autonomous cooperation.

6) Reassessment

Users of information communication technologies should assess the safety and reliability of information communication networks and adjust the response to the information security issues.

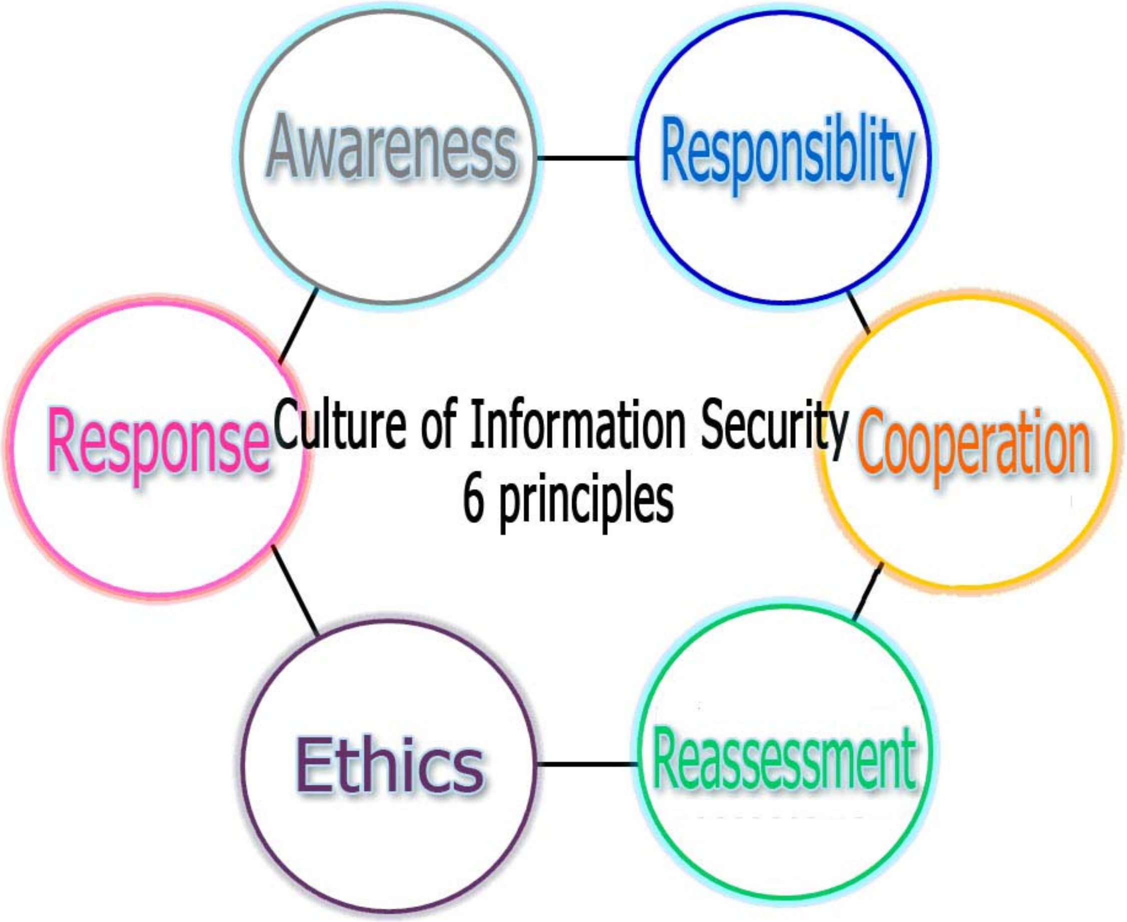


Figure 5. 6 principles of "Culture of Information Security"

(3) Approach for establishing "Culture of Information Security"

The following basic approaches are taken to establish "Culture of Information Security".

1) Establishment of "Culture of Information Security" while promoting the use of information communication technologies

We should not scare the users and deter them from using information communication technologies when explaining the importance of information security by putting too much emphasis. All users should share basic understanding that outreach and awareness are designed to help them use information communication technologies better.

2) Establishment of constant endeavors

The government has established "Information Security Awareness Month" to outreach and awareness and intensive efforts are made within the time. While this is an effective approach, continuous activities throughout the year to establish constant endeavors are important.

3) Promotion of measures fine-tuned for the usage of information communication technologies

The way they use the Internet and mobile phones varies widely depending on the user's age group and who they are. Therefore measures should be fine-tuned for different age groups and different types of users.

4) Promotion for the IS indifferent group

How to approach the IS indifferent group is a big issue. As the internet has spread, all users are connected via networks. Even if part of users apply advanced information security measures, a weakness can be created by other users' not applying measures and may result in computer virus infection in the entire network. It is important for all users to understand that information security cannot improve unless all users apply measures.

Reference: Relationships between "Outreach and Awareness" and "Human Resource Development"

Dissemination of and enlightenment on information security also play a role as the foundation for developing excellent human resources. Well balanced improvement of information security in Japan can only be achieved when outreach and awareness policies for wide-ranging general public and advanced human resource development for high-level information communication technologies are both applied.

Information security human resource development policies are promoted based on the "Information Security Human Resources Development Program" and we are planning to improve information security measures in Japan by executing this program together with the Outreach and Awareness Program.

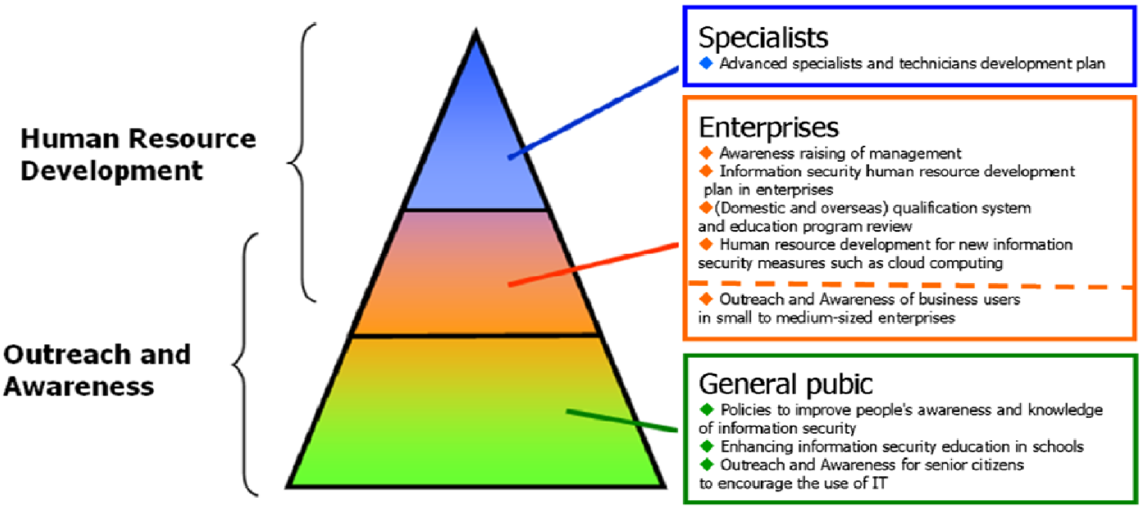

Human Resource Development
Outreach and Awareness
Specialists
◆ Advanced specialists and technicians development plan
Enterprises
◆ Awareness raising of management
◆ Information security human resource development plan in enterprises
◆(Domestic and overseas) qualification system and education program review
◆ Human resource development for new information security measures such as cloud computing
◆ Outreach and Awareness of business users in small to medium-sized enterprises
General pubic
◆ Policies to improve people's awareness and knowledge of information security
◆ Enhancing information security education in schools
◆ Outreach and Awareness for senior citizens to encourage the use of IT

Figure 6. Relationships between "Outreach and Awareness" and "Human Resource Development" in information security

6. Promotion system and scheme

The following promotion system and scheme should be implemented in order to endorse outreach and awareness policies to establish "Culture of Information Security".

(1) Establishing the HR Expert Committee for Outreach and Awareness (tentative name)

The "Information Security Policy Council" specializes dissemination of and enlightenment on information security. In order to clarify its "control tower" function, the "HR Expert Committee for Outreach and Awareness" (tentative name) will be established to advice and assess the outreach and awareness, and human resource development policies for information security. Also, the "Public-Private Sector Alliance Working Group" (tentative name) will be established under the "HR Expert Committee for Outreach and Awareness" (tentative name) to plan and promote public-private collaboration projects since public-private sector collaboration is essential to endorse outreach and awareness.

(2) Organization networks

Information security outreach and awareness policies are promoted in government agencies, incorporated administrative agencies, groups, and enterprises; however, these organizations should be networked for even more efficient and effective implementation. Also, the use of volunteers such as information security supporters would be effective to promote information security outreach and awareness policies.

(3) Policy effectiveness measurements

Although no internationally standardized method is established for quantifying the effects of outreach and awareness, we can improve the policy assessment and improve the effectiveness of outreach and awareness using the results of periodical questionnaires. Other assessment methods for the effect of policies will be examined. The results of the assessment of outreach and awareness policies will be reported to the "HR Expert Committee for Outreach and Awareness" (tentative name) to request their advice.

(4) Follow-up and review of the outreach and awareness program

The outreach and awareness program is a 3 years long (2011 to 2013) program. Related measures are reviewed at the same timing as the "Information Security 20xx" and the results are reflected on the subsequent measures. The outreach and awareness program is reviewed as necessary in order to understand the current status of information security in Japan, the current status of information security education, outreach and awareness, and awareness of general public and enterprises, as well as to respond appropriately to the changes in domestic socioeconomic status and the international trend.

7. Points in promoting the outreach and awareness program

It is important to reinforce public-private sector collaboration and international collaboration to promote the outreach and awareness program under the above system.

(1) Reinforcement of public-private sector collaboration

It is important to reinforce public-private sector collaboration since outreach and awareness will be more effective when more organizations are proactively working together. Specific plan should be made to reinforce public-private sector collaboration.

(2) Reinforcement of international collaboration

International cooperation is essential in promoting information security policies since information is freely moving beyond international boundaries today. Each country should take specific actions for international collaboration in information security outreach and awareness such as sharing domestic and overseas best practice. Specific measures will be described later.

8. Specific efforts

The outreach and awareness program focuses on the continuity of measures and the following actions will be taken over its lifespan of 3 years.

(1) General and intensive outreach and awareness

1) Enhancement of "Information Security Awareness Month"

"Information Security Awareness Month" has been established since 2009 by the Cabinet Secretariat in collaboration with other concerned government agencies in order to encourage everyone's interest and understanding as part of outreach and awareness policies. However, "Information Security Awareness Month" has not been promoted fully and is still relatively unknown. Therefore, the government should publicize "Information Security Awareness Month" more and enhance the associated events during this month.

"Information Security Awareness Month" in 2010 involved new approach such as posters, stickers, web banners, "Website on Information Security Awareness Raising", and the government Internet TV. The effects will be reviewed for further enhancement.

The "Public-Private Sector Alliance Working Group" (tentative name) will be newly established to reinforce public-private sector collaboration. They will exchange information and advice on plans for events during "Information Security Awareness Month".

2) October for the "Information Security Awareness Month"

October is "National Cyber security Awareness Month" in the U.S.A. while APEC (Asia-Pacific Economic Cooperation) has instituted "APEC Annual Cyber Security Awareness Day" towards the end of October. The Japan - ASEAN Information Security Policy Meeting is considering to establish "Japan - ASEAN Information Security Awareness Week" (tentative name). It may be more effective for international collaboration that our "Information Security Awareness Month" be moved from February to October from 2012, or newly establish "International Collaboration Information Security Awareness Week" in October while retaining February's event.

(2) Dissemination among and enlightenment of general public

1) Enhancement of "Website on Information Security Awareness Raising"

A portal site was established during "Information Security Awareness Month" in 2010 to introduce information security measures for different users such as home, school, and work users. The site should be enhanced further. It is important to continue the endeavors based on the slogan for "Information Security Awareness Month" in 2010, "Aware, Secure, Vigilant"[14].

- "Aware" of how to implement safe and secure Internet environments

It is essential that each person have correct awareness and knowledge of information security in order to respond appropriately. Accurate and intelligible information according to the user's needs should be provided.

- "Secure" oneself from information security threats

Knowing information security is not enough; it should be practiced. Therefore, specific and practical information should be provided.

- "Vigilant" measures against ever-changing information security threats

Information communication technologies progress day-to-day and the same apply to threats and measures of information security. Associated information should be provided in a timely manner to make users aware of the necessity of continuous measures.

2) Self diagnosis check list

It is important for individuals to know where they are objectively in the information security roadmap in order to encourage people's interest and further outreach and awareness. Therefore, a self diagnosis check list will be designed for general public and users in 2012.

3) Materials for senior citizens

Aging is rapidly progressing in Japan. Information security outreach and awareness should be accelerated among senior citizens to encourage their use of information communication technologies. Care should be taken not to unnecessarily scare senior citizens. Materials to describe information security measures written in plain language should be prepared in 2012. Also deployment and support of senior volunteers should be examined.

4) Dissemination among and enlightenment of the IS indifferent group and others

[14] "Aware, Secure, Vigilant" was the slogan to communicate 6 principles of "Culture of Information Security" to general public. "Aware" indicates "1. Awareness", "2. Responsibility" and "5. Ethics", "Secure" indicates "3. Response" and "4. Cooperation", and "Continue" indicates "3. response" and "6. Reassessment".

- Dissemination among and enlightenment of the IS indifferent group

Spread of various information security related devices and services may cause an increase in the number of users with little knowledge in information communication technologies and little awareness of information security. Such users may make setting mistakes, or may even be targeted by attackers. Dissemination of and enlightenment on information security among general public should also be intensified for this IS indifferent group; however, currently no specific measures are in place. Therefore, the first step would be to create the common consensus to recognize the importance of measures for the IS indifferent group.

It will be followed by the promotion of outreach and awareness policies at home and school, and other innovative endeavors, for example, using mass media, with help of information security supporters, and application of overseas best practice.

- Dissemination among and enlightenment of beginners

Basic knowledge of information security should be provided to Internet beginners by establishing "Internet safety classes" and via the Internet.

5) Enhancement of Information Security Consultation Service

Information Security Consultation Services which are established by government agencies should be enhanced to be more helpful for users such as reinforcing the collaboration between them. Also improving the ability to provide consumer advice should be examined in between the Consumer Affairs Agency which is in change of consumer protection in general, Cabinet Secretariat, and concerned government agencies.

The "Information Security Consultation Service"[15], established by the Information-technology Promotion Agency (hereinafter "IPA") in 2010 to provide general advice on malware[16] and illegal access should be publicized widely. Also, "Frequently Asked Questions (FAQ)" on the IPA website should be improved.

6) Collecting and sharing information security incident cases

Examining information security incidents in the past, learning lessons, and sharing such lessons are important for preventing information security incidents and taking appropriate actions in the event of an incident. We should collect publicized cases, and consider the method such as anonymity to collect other

[15] The general term for illegal programs which do what the computer user does not intend. It includes computer viruses, spyware such as keyloggers which steal private information and backdoors which enable the attackers to remotely operate the personal computer, rogue security software which provides fake information and prompts the user to purchase it, and one-click ware which continuously display billing screens for adult sites. (Source: IPA website)

[16] http://www.ipa.go.jp/security/anshin/index.html

unobtainable cases due to company secrets or privacy protection. The collected information security incidents should be made available for everyone by publicizing on websites.

(3) Education enhancement and learning opportunities of information security

1) Enhancement of information security education

The necessary foundation should be arranged and related policies should be practiced to improve information security education in schools. Pupils' basic knowledge and skills in information security should be improved and they should be able to actively use information communication technologies.

Information ethics should be continuously taught to pupils and students throughout school education according to their development stages. It is important to consider collaboration with their families and local communities for the ethics education. Also individual teachers should improve their teaching ability in information security in order to further enhance the contents of information security education.

2) Enhancement of information security education materials

Education materials for information security should be developed and disseminated. Providing information which pupils and students could not have before will motivate their learning and help their understanding. Beneficial education materials should be made available in information security portal sites of various organizations including the National Information Security Center in 2012 to encourage education and learning through the Internet.

(4) Dissemination among and enlightenment of enterprises

1) Awareness raising of management

Stakeholders such as society and customers are increasingly demanding transparency and information disclosure, and enterprises are under pressure to disclose information such as risks, and to fulfill accountability. It is considered that leaders of organizations rarely consider information security as their strategic issues and often leave the risk management of information assets to the information system department or similar divisions in the workplace. Such attitude will only result in the situation where the intention of management remains unclear in addition to lagging application of information security measures in the workplace. There may be lack of regulation in information security among management themselves such as information security measures are not assessed properly to assist decision-making of the management.

Information security measures in organizations have often been left to the information systems personnel in the workplace as it was ridiculed as "chief clerk security". This is not the way to manage risks in enterprises. Enterprises should move away from "chief clerk security" towards "CEO security" where management of enterprises takes initiative in information security.

The above recognition should be shared and information security should be taken as an important issue in activities in economic organizations.

2) Measures for small to medium-sized enterprises

It is especially important to enhance dissemination among and enlightenment of small to medium-sized enterprises than others. Specifically, enhancing events such as "information security leadership nurturing seminar for small to medium-sized enterprises" and provide information security guidelines and various tools along the lifecycle of information systems (planning, design and development, operation and using, disposal).

(5) Cyber crime prevention campaign

1) Information security courses

In order to plan for the improvement of information security awareness and knowledge, lectures with topics including cybercrime situations and arrest cases will be held throughout the country. Also, cyber crime measures including information security measures should be promoted through various councils in collaboration with concerned vendors.

2) Promotion of cybercrime damage prevention measures

Pamphlets for cybercrime prevention and leaflets for crime prevention in online dating sites for junior and senior high school pupils should be created and distributed. PR activities such as publishing basic measures for common Internet problems and cybercrime methods on websites should be encouraged.

3) Promoting cyber volunteer training

Activities and training methods of volunteers should be examined in order to create safe and secure cyberspace. We should encourage cyber volunteers in cyberspace and support their activities.

(6) Incentive scheme for promoting outreach and awareness

1) Commendations and information security contests

Incentive scheme such as financial support for information security outreach and awareness should be considered in order to reinforce public-private sector collaboration and international collaboration. Also, commending individuals and enterprises who have contributed greatly towards information security will strengthen public-private sector collaboration in outreach and awareness.

Technology contests concerning Information security are popular in overseas countries and winners will receive commendation or a grant. We should consider nation-wide information security contests since it will give incentive to superior human resources in information security.

(7) Reinforcement of international collaboration

Dissemination of and enlightenment on information security are proactively promoted in Asian countries as well as Western countries. No geographical or temporal restriction applies to cyber attacks on the Internet and the impact of an attack may spread everywhere in the world spontaneously. Therefore, international collaboration for information security improvement is urgently required in addition to measures in each country.

We have collaborated with the U.S.A., APEC, and ASEAN in several frameworks for information security outreach and awareness, and we will also focus on the following in the future.

1) Reinforcement of Japan - ASEAN collaboration

Specific actions have been discussed with ASEAN though the framework such as "Japan - ASEAN Information Security Policy Meeting. Resolutions[17] from the "Third Japan - ASEAN Information Security Policy Meeting" in March 2011 will be steadily executed and enhanced.

- Establishment of "Japan - ASEAN Information Security Awareness Month/Week"

Establishment of "Japan - ASEAN Information Security Awareness Month" or "Japan - ASEAN Information Security Awareness Week" from 2012 should be considered since the use of the Internet is rapidly spreading in ASEAN countries. The pre-events such as information security awareness poster exhibitions in 2011 should be considered.

- PR media preparation

PR media should be prepared within 2011 to promote Japan - ASEAN information security awareness policies. For example, a common logo, and recommended information security measures to help general users use the Internet safely and securely and disseminate them widely.

2) Reinforcement of Japan - APEC collaboration

APEC Cyber Security Awareness Day was established[18] in APEC Ministerial Meeting on Telecommunications and Information Industry was held in Okinawa in October 2010 and the "APEC Cyber Security Awareness Poster Exhibition"

[17] Resolutions from the Third Japan - ASEAN Information Security Policy Meeting
http://www.nisc.go.jp/press/pdf/3rd_aseanj_meeting_result_press.pdf

[18] Establishment of APEC Cyber Security Awareness Day
http://www.nisc.go.jp/press/pdf/apec_csaday_press.pdf

was held jointly by Japan and Korea. We will support such activities and contribute towards improvement of information security awareness in the APEC region.

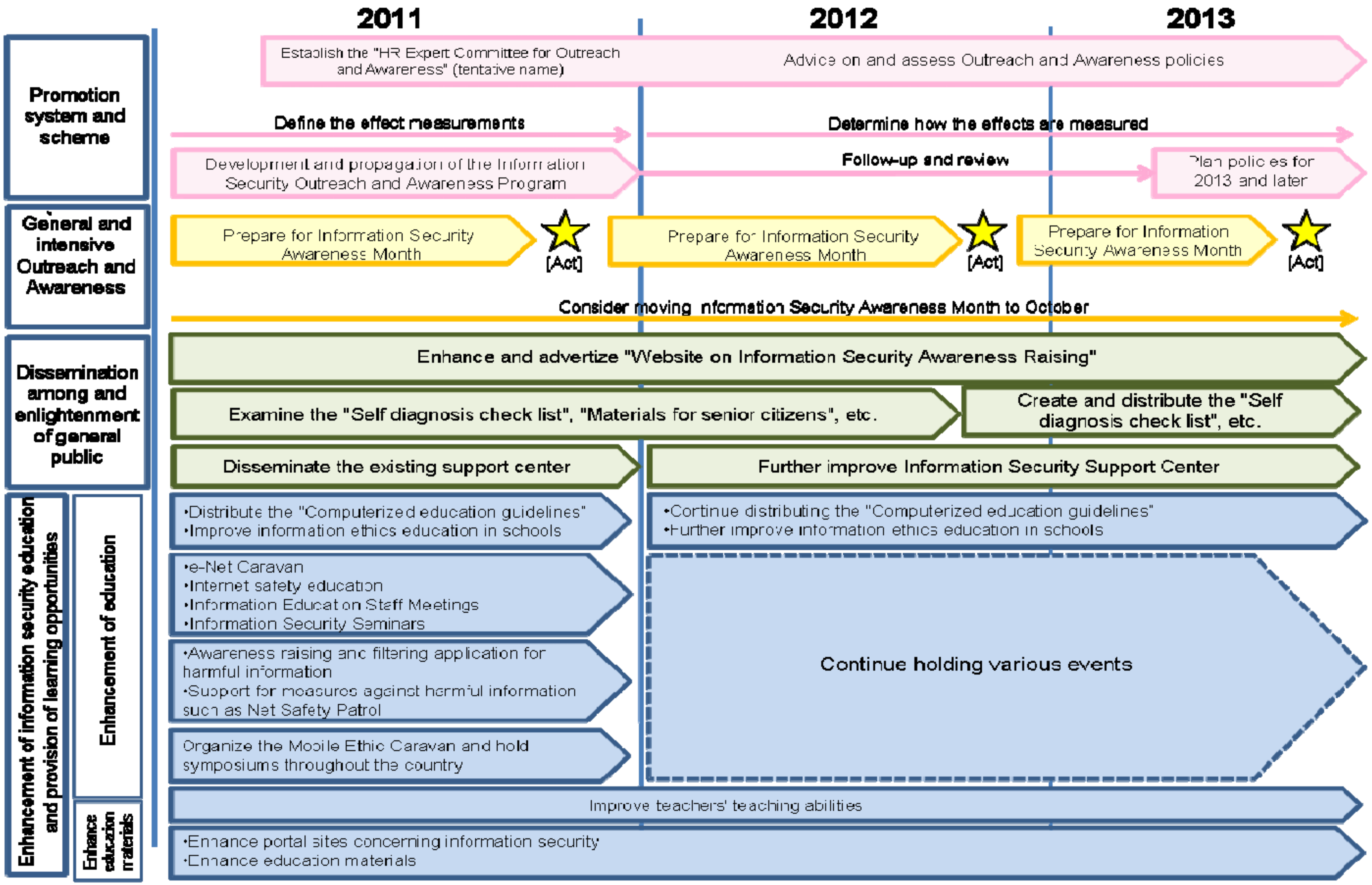
3) Reinforcement of Japan - West collaboration

Dissemination of and enlightenment on information security are promoted also in the U.S.A., Australia, Canada, and EU countries with various activities such as establishing awareness months and creating and distributing education materials. It is important to promote information security outreach and awareness with international collaboration. We should aim at further reinforcement of collaboration and examine issues such as sharing best practice concerning those countries' activities and specific collaboration areas by 2013.

4) Outreach and Awareness portal site in English

The English version of "Website on Information Security Awareness Raising" was established in April 2011. This site should be positioned as the outreach and awareness portal site and used to introduce various overseas efforts in addition to activities of outreach and awareness in Japan.

Work schedule for major policies in the "Information Security Outreach and Awareness Program"



2011 | 2012 | 2013

Promotion system and scheme

- Establish the "HR Expert Committee for Outreach and Awareness" (tentative name) → Advice on and assess Outreach and Awareness policies
- Define the effect measurements → Determine how the effects are measured
- Development and propagation of the Information Security Outreach and Awareness Program → Follow-up and review → Plan policies for 2013 and later

General and intensive Outreach and Awareness

- Prepare for Information Security Awareness Month ☆ [Act] → Prepare for Information Security Awareness Month ☆ [Act] → Prepare for Information Security Awareness Month ☆ [Act]
- Consider moving Information Security Awareness Month to October

Dissemination among and enlightenment of general public

- Enhance and advertize "Website on Information Security Awareness Raising"
- Examine the "Self diagnosis check list", "Materials for senior citizens", etc. → Create and distribute the "Self diagnosis check list", etc.
- Disseminate the existing support center → Further improve Information Security Support Center

Enhancement of information security education and provision of learning opportunities

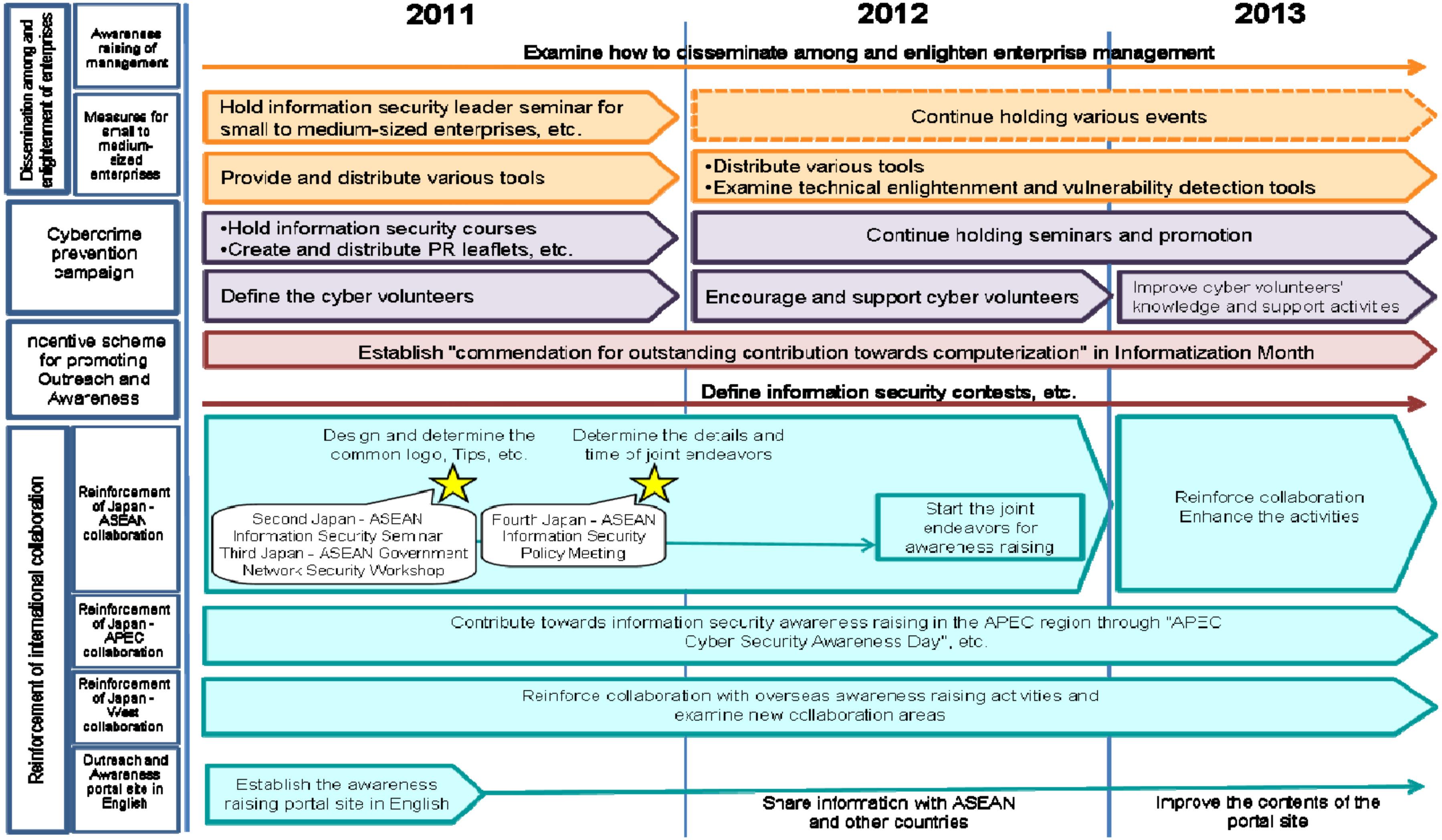
Enhancement of education

- ・Distribute the "Computerized education guidelines"
・Improve information ethics education in schools → ・Continue distributing the "Computerized education guidelines"
・Further improve information ethics education in schools
- ・e-Net Caravan
・Internet safety education
・Information Education Staff Meetings
・Information Security Seminars
- ・Awareness raising and filtering application for harmful information
・Support for measures against harmful information such as Net Safety Patrol
- Organize the Mobile Ethic Caravan and hold symposiums throughout the country
- → Continue holding various events
- Improve teachers' teaching abilities

Enhance education materials

- ・Enhance portal sites concerning information security
・Enhance education materials

Work schedule for major policies in the "Information Security Outreach and Awareness Program"



Dissemination among and enlightenment of enterprises

Awareness raising of management

Measures for small to medium-sized enterprises

Cybercrime prevention campaign

ncentive scheme for promoting Outreach and Awareness

Reinforcement of international collaboration

Reinforcement of Japan - ASEAN collaboration

Reinforcement of Japan - APEC collaboration

Reinforcement of Japan - West collaboration

Outreach and Awareness portal site in English

2011

2012

2013

Examine how to disseminate among and enlighten enterprise management

Hold information security leader seminar for small to medium-sized enterprises, etc.

Continue holding various events

Provide and distribute various tools

•Distribute various tools
•Examine technical enlightenment and vulnerability detection tools

•Hold information security courses
•Create and distribute PR leaflets, etc.

Continue holding seminars and promotion

Define the cyber volunteers

Encourage and support cyber volunteers

Improve cyber volunteers' knowledge and support activit es

Establish "commendation for outstanding contribution towards computerization" in Informatization Month

Define information security contests, etc.

Des gn and determine the common logo, Tips, etc.

Determine the details and time of joint endeavors

Second Japan - ASEAN Information Security Semnar
Third Japan - ASEAN Government Network Security Workshop

Fourth Japan - ASEAN Information Security Policy Meeting

Start the joint endeavors for awareness raising

Reinforce collaboration
Enhance the activities

Contribute towards information security awareness raising in the APEC region through "APEC Cyber Security Awareness Day", etc.

Reinforce collaboration with overseas awareness raising act vities and examine new collaboration areas

Establish the awareness raising portal site in English

Share information with ASEAN and other countries

Improve the contents of the portal site