4th WSEAS Int. Conf. on E-ACTIVITIES, Miami, Florida, USA, November 17-19, 2005 (pp174-181)

ISCS(Information Security Check Service for Strengthening the Stability and Reliability of Information Communication Service

JIN-TAE LEE, JONG-WHOI SHIN, SANG-SU JANG, and JAE-IL LEE
Korea Information Security Agency (KISA)
78, Garak-Dong, Songpa-Gu, Seoul
KOREA

Abstract: Widespread use of Internet-based information communication service has recently increased the possibility of information security risks and incidents that business and institutions encounter. Along with this situation, these incidents are having increasingly serious effects on the nation's economy and society, by bringing about infringements of human rights, financial damage to corporations, and the failure of the access to information system. Under these circumstances, the approach to information security checking has come to an important issue. Especially, security checking service has become important for organizations to maintain confidence in the area of Internet-based communication service such as electronic trading. The purpose of this paper is to introduce the new system of information security checking service(ISCS) on ISP(Internet Service Provider), IDC(Internet Data Center), and e-Commerce company(internet shopping malls, portal site, etc) in Korea. Also, this study is designed to draw out the methods that are required to consolidate and promote the ISCS policy, and figure out the agreed policy that can be practically implemented, in order to effectively cope with cyber infringement incidents and enhance the information security capability.

Key-Words: ISCS(Information Security Check Service), Security Check Standard, Objects

1 Introduction

The Internet usage infrastructure is well established in Korea, and the number of Internet users passed 30 million in 2004, which is over 70% of the total population in Korea. Additionally, the number of high-speed Internet users is 23.3 users per 100 persons, which is assuredly the highest ratio in the world [1]. As these indices indicate, the Internet became a part of our daily life and necessities long time ago. However, the advancement of computerization and expanded application of the information communication service resulted in mutual connection of various social sectors through the computer network and unconditional dependency on the information system. Information stored and transmitted in the Internet cyber space is exposed to various threats such as unauthorized access/usage, misuse/alteration, and denial of service, which always entails the possibility of incidents of infringement. On the other hand, as cyber attacks against the communication network have increased in scale, and have become faster and more intelligent in recent times, there is a possibility that the Internet-based information communication service can be interrupted nationwide for a long time, which could cause unexpected social chaos and economic loss in astronomical figures[2].

As we have experienced on January 25, 2003, the Slammer Worm virus impeded normal Internet service throughout the country[3]. The January 25th incident evidently provided an opportunity for information communication service providers, government, private enterprises, and users to understand the importance of information security. After the incident, the government established the NCSC(National Cyber Security Center) and the KISC(Korea Internet Security Center) to quickly respond to Internet incidents and to identify their causes. Using these organizations, the government endeavored to prevent the incident in the domestic communication network, and enhance the stability of the communication usage environment. However, those measures were based on ex post factor/defensive concepts of countermeasures are taken after the event.

The proportion of e-Commerce and Internet banking is continuously increasing. However, it is worrisome that hacking and virus attack patterns will be more diversified, and the attack

target will be expanded to include mobile devices, pocket PCs, and smart phones, not to mention personal computers. Table 1 shows the number of incidents reported to KrCERT from Korea and overseas countries, which were caused by hacking and virus spreading. According to the table, the number of hacking incidents has decreased by 5% compared with the previous year, but that of viruses increased by 66% [2].

Table 1. Number of Hacking&Virus reported to KrCERT

Type	2000	2001	2002	2003	2004
Hacking	1,943	5,333 (175%)	15,192 (185%)	26,179 (72%)	21,288 (5%)
Virus	-	65,033	38,677 (415%)	85,023 (120%)	103,056 (66%)

[Source: KrCERT]

The level of information security of major ISP (Information Service Providers), IDC (Integrated Data Center), shopping mall, and e-Commerce companies still remains in the incipient stage up to now. They also cannot actively cope with the cyber attack that becomes more advanced and larger in scale. Accordingly, the government started to set up a concrete and practical information security policy to protect the user who actually uses the service, and improve the information communication service environment in Korea, in consideration of its public characteristics. The Ministry of Information and Communication(hereinafter referred to "MIC") proposed the information security guidelines(hereafter referred to as "security check standards") that the service providers should comply with, in order to encourage many enterprises and information communication service providers to fulfill their responsibilities and roles. The MIC revised the related laws and regulations and introduced "ISCS(Information Security Check Service)" policy, which took effect from July 2004[4][5]. The basis of the change by the government with regards to the communication usage environment was that it aimed for enhancement of the national information security level by enabling enterprises and individuals to use the information communication service safely without interruption through application of the security check policy. However, more efforts and changes in attitude among various subjects of security check are needed for early establishment of the policy and efficient policy application, as well as achievement of the basic purpose of the ISCS policy in the first year of implementation (2005).

2 Related Work

The UK Government's CESG(Communications Electronics Security Group) has traditionally provided IT health check services, which checks identify vulnerabilities in IT systems and networks, for HMG and the wider public sector of systems handling protectively marked information[6]. The IT Health Check Service was developed to enhance the availability and quality of the IT health check services that are provided to government in line with HMG policy. An IT Health Check Service Provider analyze the systems or networks of customer by conducting a number of tests designed to identify any weaknesses utilizing publicly known vulnerabilities and common configuration faults. Consequently, the customer will receive a report detailing any vulnerabilities and recommending effective security counter measures. The BSI(the Federal Office for Information Security) in Germany provides the IT Baseline Protection Certificate service, which offers companies and agencies the possibility of making transparent their efforts regarding IT security[7]. After consulting with registered IT baseline protection users and IT security experts, the BSI has defined three variants of the IT Baseline Protection qualification: the IT Baseline Protection Certificate and the self-declarations "IT Baseline Protection entry level" and "IT Baseline Protection higher level". Issue of the IT Baseline Protection Certificate is based on an audit carried out by an external auditor licensed with the BSI. The outcome of the audit is an audit report which is submitted to the certification authority that decides on the issue of IT Baseline Protection Certificates. The baseline set of criteria on which the procedure is based is the latest version of the BSI's IT Baseline Protection Manual. The CSE(The Communications Security Establishment), which is Canada's national cryptologic agency, has established the ITISPS(Information Technology Infrastructure Security and Protection Services) Supply Arrangements with 4 firms through Public Works and Government Services Canada to provide

Federal Government Departments and Agencies with a contractual vehicle that can be used to requisition Information Technology Security(ITS) and Information Infrastructure Protection(IIP) Professional Services. The ITISPS Supply Arrangements consist of three Tiers such as Risk Management Services, Information Infrastructure Protection Services, and Research and Development Services[9].

3 Outline of ISCS

3.1 Outline

The ISCS policy which was legislated to cope with the information infringement incidents is designed to secure the stability and reliability of the communication network and information communication service. For this purpose, major ISPs, IDCs, and Internet business companies that have more than 10 billion won in annual revenue or 1 million visitors per day on average should receive the ISCS some time between July 30 of the corresponding year and 29 July of the next year from the specialized information security consulting company, in accordance with the "Communication Infrastructure Protection Law."

3.2 Subjects of Security Check

The subjects of the ISCS policy include MIC, KISA, ISCS objects, and specialized information security consulting company. Each player should perform the tasks as described in the Fig 1.

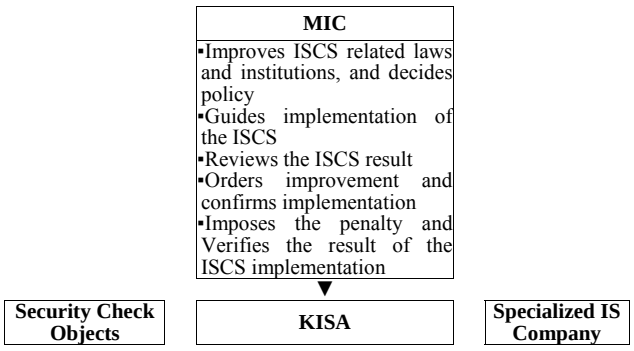

Fig.1 Each player's role of ISCS

3.2.1 MIC(The Ministry of Information and Communication)

The MIC should identify the target service providers that should carry out the security standard and receive the information security check, based on decision making about the ISCS policy. It also should notify the corresponding objects to receive the security check, and establish, revise, and arrange laws and regulations related with the information security check. Additionally, the MIC issues the instruction to improve the shortcomings in complying with the security standards, or imposes the penalty, by reviewing the prior ISCS plan submitted by the target service providers, and the result of carrying out the information security check.

3.2.2 KISA(Korea Information Security Agency)

KISA is entrusted by the MIC to set up and distribute the security check standard, guidelines, and manual. Additionally, it supports preparation of prior examination receiving plan for the ISCS, and review on the security check implementation result, and on-site examination. KISA educates the ISCS objects and the specialized information security consulting company with regards to the overall security check matters such as the security check method and procedures.

3.2.3 ISCS Objects

Service providers for whom the ISCS is mandatory should take administrative, technical, and physical measures against the communication facilities and equipment. They also should receive the ISCS every year from the specialized information security consulting company according to the pre-defined procedure

and methods. The MIC periodically identifies major ISPs, IDCs, and other information communication service providers, such as Internet shopping malls, so that they receive the ISCS every year. Jobs that should be performed by the ISCS object can be grouped into three categories as described below, according to the characteristics of their information communication service.

- Companies that provide nationwide communication connection service by providing the Internet connection, and communication line facility and network service.(Major information communication service providers/ISP)
- Companies that run and manage the integrated communication facility to provide the information communication service for others such as co-location service, server hosting service, or network service. (Integrated communication facility providers/IDC)
- Companies that secure the certain level of sales revenue or the number of users specified by MIC, and provide the information communication service, while the sales revenue from the information communication service sector is over ten billion won, or the average daily visitors are more than one million users.(Shopping mall, portal site, and so on.)

3.2.4 Specialized IS(Information Security) Consulting Company

The ISCS jobs, which are to check whether the security check standard is complied with or not, are carried out by the company designated as the specialized information security consulting company by the MIC in accordance with the Communication Infrastructure Protection Law. These company have to satisfy qualifications such as over 20 technical staffs, company capitalized at 2 thousand million won, etc. Once the company has successfully carried out the security check, the certificate will be issued. As of May 2005, ten specialized information security consulting companies are designated. More companies can be designated or re-designated if they satisfy the standard requirements, as the ISCS object company increases.

3.4 Procedure of ISCS

Normally, the ISCS is carried out in three stages. The first stage is the period that the ISCS objects set up the information security check plan. The second stage is the period in which objects receive the security check from the specialized company. The last stage is the period when the MIC instructs improvements based on the security check result of the specialized company, and confirms whether the improvement instruction has been complied with or not (such as penalty charging).

MIC	Security Check Receiving Company (Objects)	Check Implementation Company (IS Company)	MIC
▪Identifies and notifies the ISCS target. service providers	▪Prepares and set ups the plan for security check ▪Selects and contracts the check implementation company	▪Carries out security check ▪Recommends and confirms. improvement ▪Issues the certificate	▪Reviews the ISCS result ▪Improvement order and confirmation ▪Imposes the penalty

Fig.2 Stages of ISCS

3.5 Method of ISCS

The ISCS objects must abide by the “Instruction about Information Security Measures, and Method, Procedure, and Commission of Security Check" that was notified by the MIC(MIC Public Notice No. 2004-54). To confirm whether the ISCS objects have complied with the security protection measures, document inspection or on-site inspection can be performed. Inspection is performed for the core communication facilities and equipments, which can affect stabilized operation of the communication network significantly at the time of an incident or emergency.

- Document Inspection : Primary document inspection using the evidencing documents or photographs that verify implementation of administrative, technical, and physical protection measures as specified in the information security guideline. These documents that objects provide for IS consulting company staff’s inspection are just checked in designated place such as object’s office room.
- On-site Inspection : Inspection performed at the business site to visually check facility and equipment arrangement and operation status, in

order to verify genuineness of the document inspection result and implementation status of the items that cannot be easily confirmed by documents.

3.6 Criteria of ISCS

The security check standard is divided into three areas(administrative, technical, and physical protection measures) that were indicated by the MIC to secure the stability and reliability of the communication network. This standard specifies the minimum requirement that should be met mandatory. Table 2 shows the summary of the security check standard.

Table 2. Security check standard of ISCS

Contents		
1. Administrative Protection Measures	1.1. Organizes and runs information security organization	1.1.1. Composition of the information security organization
		1.1.2. Appointing the information security management
		1.1.3. Roles of information security organization members
	1.2. Set up and manage information security planning and so on	1.2.1. Setting up/Implementing the information security policy
		1.2.2. Setting up/Implementing the information security implementation plan
		1.2.3. Preparing/Complying with the working-level security instructions
	1.3. Personnel security	1.3.1. Security of internal personnel
		1.3..2. Security of external personnel
		1.3.3. Outsourcing/Consignment Operation Security
	1.4. User security	1.4.1. Providing security information
	1.5. Intrusion incident response	1.5.1 Setting up/Implementing countermeasure plan against the incident
	1.6. Information security measures check	1.6.1. Internal review of the protection measures
	1.7. Information asset management	1.7.1 Information communication equipment and facility status management
2. Technical Protection Measures	2.1. Network security	2.1.1. Traffic monitoring
		2.1.2. Wireless/Mobile Network service security
		2.1.3. Installing/Operating information security system
	2.2. Information communication facility security	2.2.1. Web server security
		2.2.2. DNS(Domain Name System) server security
		2.2.3. DHCP(Dynamic Host Configuration Protocol) server security
		2.2.4. DB(Database) server security
		2.2.5. Router/Switch security
		2.2.6. Information protection system security
		2.2.7. Vulnerability check
		2.2.8. Access control and security setting management
		2.2.9. Administrator account password management
		2.2.10. Log management
		2.2.11. Security patch management
		2.2.12. Backup and recovery
3. Physical Protection Measures	3.1. Entry and access control security	3.1.1. Entry/Access control of the information communication facility
	3.2. Operation and management of subsidiary equipment and facility	3.2.1. Installing/Operating the backup facility and equipment

Total 48 protection measure items including 21 administrative items, 24 technical items, and 3 physical items.

4. Efficient Operation Method to Secure Effectiveness of ISCS

The ISCS system is implemented for 142 companies at the initial stage, which includes 13 ISPs, 63 IDCs, and 66 companies that many users are accessing, such as shopping malls. It is expected that more than 150 companies will receive the ISCS by July 29, 2005. Considering that it is the first year of policy implementation, emphasis was put on education and training for the corresponding personnel about standard, method, and procedure for ISCS preparation, and holding the case study seminar to enhance recognition on the information security.

However, it is most important that all that efforts should be made to appeal to the service users for proper establishment and promotion of the policy, not simply encourage the objects to receive the ISCS. For this purpose, priority should be given to early identification of the ISCS problems and legal and institutional improvement for problem resolution, as well as autonomous participation and efforts of the ISCS subjects. Besides, the security check standard should evolve with changes in the IT environment.

4.1 Legal and Institutional Improvement and Support for Early Establishment of ISCS Policy

The initial purpose of the ISCS regulation could not be achieved if the ISCS objects are dissatisfied or the initial objectives of the regulation are distorted frequently. This would result in the deteriorating effectiveness of the ISCS policy. The MIC is endeavoring to solve the issues of introducing the ISCS system, and

encourage voluntary examination receiving. The government needs to find out and improve the legal and institutional barriers that hinder introduction of the ISCS system and complaint elements of the objects, in order to secure effectiveness of the policy and promote policy implementation. For this purpose, the relevant laws and regulations in Korea and overseas countries should be scrutinized in details to identify the problems and improvements, and set up the countermeasures. Second, the proper communication channel should be established to resolve complaints about the policy and demand, so that various opinions can be collected from the ISCS objects, specialized companies, and related organizations. Third, the government should prepare for the support measures for early establishment of the ISCS policy, and implement it proactively. These strategies should be carried out, considering the requirement that the government should play a major role. If necessary, these strategies should be improved through discussion between related government agencies.

4.2 Autonomous Effects to Promote ISCS Policy

Efforts and cooperation among the ISCS subjects are required to secure the stability of the information communication service environment in Korea, and meet up with service user's demand. Up to now, the process of coordinating the opinions about necessity of the ISCS system was the main issue. However, it should be changed to a large extent for the proper establishment and promotion of the policy, and priority should be given to autonomous and voluntary participation of each subject. The role of the ISCS policy is important as the means of enhancing the information security at the national level, as well as service for the customers. For this purpose, it is the time point that efforts of the subject are required for effective utilization of the policy and achievement of the ultimate aims. Table 3 shows the items that each subject needs to attend to proactively and continuously for policy establishment and promotion.

Table 3. Each subject's effort of ISCS

Government (MIC, KISA)	▪Ascertains development methods such as safety check policy improvement and support method ▪Various studies of the expertise on revision and application of the security check standard ▪Objective evaluation and verification of the ISCS result, Education and PR about the ISCS policy ▪Opinion collection from diverse channels such as related associations and service users ▪Supports for coping with the cyber incidents and finds out the successful case study
Information communication service provider	▪Enhances the information communication service quality and invests in information security ▪Continuous education of the employees about information security ▪Provides information security and security training opportunity to the customer ▪Autonomous implementation and evaluation of the security check standard
Specialized information security consulting company	▪Continuous development and accumulating know-how about the ISCS implementation technique ▪Fair and objective ISCS implementation ▪Improves the information security products and emphasizes R&D ▪Joint research between specialized companies to enhance the security check quality

4.3 Development of Security Check Standard in line with IT Environment Change

Seen from the ISCS objects, the practical benefits from ISCS implementation should be those that enhance the security level of the enterprises, secure the stability of the service usage environment, and contribute to the protection of the customer's information, satisfying all requirements. Therefore, the formative and symbolic protection measures item should be removed from the security check standard. To do so, continuous study is required for the detailed

protection items of the security check standard. If the standard fails to reflect the social demand and change, and cope with the IT environment actively, the original purpose of the ISCS system cannot be achieved. This could result in the loss of effectiveness and deterioration of the policy. There is a high possibility that the threat to the individual network can spread out to the entire communication network with the introduction of the converged broadband network that integrates wire/wireless network, communication/broadcasting network, and voice/Internet network. It can also spark a chain reaction in the industry converged with IT, such as energy, logistics, finance, broadcasting service, and social infrastructure. Additionally, as the ubiquitous environment comes about, various devices in our daily life are connected through the network. As a result, the possibility of private infringement is increasing due to the concentration and disclosure of the private information that is collected massively from various sources and paths. Cyber attack thread can also proliferate in our daily life. As mentioned above, efforts should be made to set up the security check standard in consideration of the items described in Table 4, in order to actively cope with the IT environment that is changing quickly in various areas.

Table 4. Development direction of security check standard

▪Network infrastructure becomes broadband and mobile
▪Provides the service that integrates wire broadband and wireless mobility
▪Integration, customization, intelligence, and diversification of the information communication service
▪Increased user and social demand on stability and reliability of the information communication service

5 Conclusion

The purpose for which the MIC established and announced the security check standard as an effort of active and preventive measures was to secure stability of the communication network at the national level, and enhance the level of information security management system, by encouraging the top management and employees of the ISCS objects that provide the information communication service to set up and run the professional and systematic information security management system through more in-depth understanding on the necessity of information security.

The ISCS policy should be considered most important for convenient Internet usage and coping with explosive growth of the Internet business. To make the reliable information communication service usage environment through promotion of the ISCS policy that took effect from July 2004, many things are required, aside from the conceptual and superficial efforts, such as the improvement and support for ISCS laws and regulations, efforts of each ISCS subjects, continuous study on the security check standard in line with the IT development trend, and establishment of the joint response system of government and private enterprises against the incidents. At this stage, the safety check policy seems to be well established through discussion among ISCS subjects.

However, long-term efforts are required to sustain the fundamental purpose of the ISCS policy. Most of all, cooperation among Internet business companies, specialized security companies, related associations, and government agencies are required to make the secure environment for the information communication service in Korea and improve the cyber security environment. Based on cooperation, it is expected that continuous growth trend of the Internet related industries and the utilization of the infrastructure can be maintained, and the foundation can be laid down that enables the role as the core player national and social administration to be faithfully carried out.

References :

[1] National Internet Development Agency of

Korea, Internet Statistics Information System, http://nida.or.kr, http://isis.nic.or.kr
[2] Korea Information Security Agency, CERTCC-KR(KOREA Computer Emergency Response Team Coordination Center), http://www.kisa.or.kr, http://www.krcert.or.kr
[3] MIC, A Report of Investigation on Incident of Information Communication Network by Slammer Worm on February 18. 2003, http://www.mic.go.kr
[4] MIC, revised plan for the law regarding the information communication network usage promotion, information protection, etc., 2003
[5] MIC, data on the ISCS hearing, 2003, 2004, 2005
[6] IT Health Check, 2005 http://www.cesg.gov.uk/
[7] IT Baseline Protection Certification process, 2005
http://www.bsi.bund.de/english/gshb/zert/index.htm
[8] Information Technology Infrastructure Security and Protection Services(ITISPS), 2005
http://www.cse-cst.gc.ca/en/services/industrial_services/itisps_program.html