World Academy of Science, Engineering and Technology
International Journal of Information and Communication Engineering
Vol:1, No:6, 2007

ISCS (Information Security Check Service) for the Safety and Reliability of Communications

Jong-Whoi Shin, Jin-Tae Lee, Sang-Soo Jang, and Jae-Il Lee

***Abstract*—**Recent widespread use of information and communication technology has greatly changed information security risks that businesses and institutions encounter. Along with this situation, in order to ensure security and have confidence in electronic trading, it has become important for organizations to take competent information security measures to provide international confidence that sensitive information is secure. Against this backdrop, the approach to information security checking has come to an important issue, which is believed to be common to all countries. The purpose of this paper is to introduce the new system of information security checking program in Korea and to propose synthetic information security countermeasures under domestic circumstances in order to protect physical equipment, security management and technology, and the operation of security check for securing services on ISP(Internet Service Provider), IDC(Internet Data Center), and e-commerce(shopping malls, etc.)

***Keywords*—**Information Security Check Service, safety criteria, object enterpriser.

I. Introduction

CYBER attacks to networks are gradually becoming large-scale and high-speed, so the Internet related services such as electronic transaction and so on may be interrupted for a long time, and examples of infringement accidents such as outflow of the personal information on customers and so on have been greatly increasing[1].

TABLE I
NUMBER OF INFRINGEMENTS REPORTED TO KR-CERT

Year	Number of infringements	Increase ratio versus last year
1998	158	247 %
1999	572	362 %
2000	1,943	340 %
2001	5,333	274 %
2002	15,192	285 %
2003	26,179	172 %
2004	29,780	113 %

Therefore, social expense due to infringements is gradually increasing, and large-scale attacks to network such as 1.25 Internet disaster may take place with gradually increasing possibility to cause national confusion and economic loss of astronomical amount. Regardless of such a situation, the information security level of Internet service providers such as ISP, IDC, electronic transaction enterprises, etc. still stays at an elementary level, so as to be in very disadvantageous position for actively coping with infringements that are increasing. Accordingly, in order to enhance real stability of Internet network, it was necessary to arrange a set of safety criteria and enlarge the range of enterprises for which the safety criteria concerned shall be compulsively fulfilled. Especially in cases of ISP and electronic transaction enterprises, although there may be concern about extensive social and economic damage when Internet infringements such as hacking and so on are carried out, there is big possibility of the occurrence of Internet infringements because the fulfillment of safety criteria is not compulsory. Accordingly, the Ministry of Information and Communication (hereinafter referred to as "MIC") in Korea established minimum physical, administrative, technical safety criteria which should be observed by Internet enterprisers, and enlarged the duty for fulfillment of safety criteria which applied to existing IDC only to the entire Internet related service enterprisers[2][3]. Recognizing the problems as above, MIC introduced a system to revise the laws concerned from the last 2000, established information security measures which should be observed by information communications service provider, and then carry them out. In addition, various supports were promoted in order to enhance the recognition of enterpriser information security for promoting a trend of making enterprisers carry out information security measures for themselves by introducing the initial intent of legislation, and guidance for publicity was strengthened for recommending government security measures with respect to information communications service providers, but the trend of carrying out government security measurement autonomously did not spread in the short term. So, the press, citizen group, research institution, etc. became to present necessity of strengthening information security measures for internet business field by taking into consideration the nationwide social propagation effect of changed information communications environment and information side-effect, and MIC arranged the existing cyber attack prevention system by in order to reflect such change of policy

Manuscript received May 13, 2005. This work was supported in part by the Korean Ministry of Information and Communication.

Jong-Whoi Shin (phone:+82 2 405 5256; fax: +82 2 405 5219; e-mail: jshin@kisa.or.kr), Jin-Tae Lee (e-mail: cybermax@kisa.or.kr), Sang-Soo Jang (e-mail: ssjang@kisa.or.kr), and Jae-Il Lee (e-mail: jilee@kisa.or.kr) are with the Korea Information Security Agency(KISA), 78, Garak-Dong, Songpa-Gu, Seoul, Korea.

environment change, etc. and introduced "Information Security Check Service"(hereinafter referred to “ISCS”) as a part of this.

II. 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[4]. 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 analyzes 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[5]. 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 that 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[6].

III. ISCS

A. Outline of Service

Enterpriser for ISCS are supposed to be provider of service who has effect on the entire national information communications network during infringement or may cause inconvenience or economical damage to a large number of people. Service works of object enterprisers shall be divided into the following 3 kinds depending on characteristics of service.

1) A person who provides nationwide information communications network connection service (ISP)

2) An enterpriser who operates and controls the integrated information communications facility in order to provide other person’s information communications service (IDC)

3) An enterpriser who provides internet service used by general persons(electronic transaction enterprises such as shopping mall, portal search, internet game site, etc.)

At this time, ISCS will be conducted first for the enterprisers who secured more than designated size of sale amount or customers in order to minimize side-effect of damaging development of internet industry due to uniform control. ISCS has been conducting by the information security consulting professional enterprise, which was designated according to the information communications base protection law. They would be persons who can guarantee fairness in diagnostic work as well as wide technological ability in information security field in order to perform ISCS. So, we selected as diagnosis enterprise the information security consulting professional enterprise which is embodied for the designated requirement such as technical requirements, etc. and examined periodically by the information communications base security law. As of 2004, ten enterprises were designated as information security consulting professional enterprises and are under action, and additional designations may be conducted by considering market demand, enterprise qualification, etc. Because the ISCS sponsored by the government is supposed to be conducted by the information security consulting professional enterprises that are private enterprises, they imposed sincere and fair diagnostic testing on the information security consulting professional enterprises and made MIC check the progress situation of safety diagnosis as necessary.

B. Procedure

Work process of ISCS is divided into 4 stages as shown in the Figure 1.

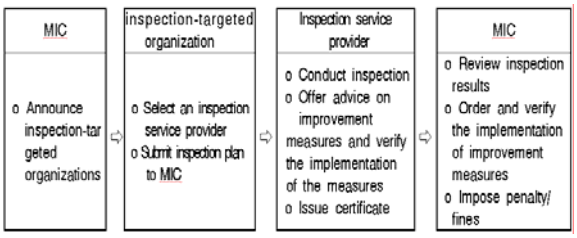

Fig. 1 ISCS Procedure

The above procedure can be arranged in more detail as follows.

1) MIC decides and notifies the enterprise concerned of next year in June every year in order to announce the object for ISCS clearly in advance.

2) The enterprise concerned for ISCS designates the enterprise specializing in information security consultation which will execute ISCS, and then submit to MIC safety diagnosis plan, description of information communications equipment and facility being the object of safety criteria, etc. MIC can review the safety diagnosis plan submitted by the enterpriser concerned and then make the unreasonable content corrected.

3) The enterprise specializing in information security consultation checks if the enterprise concerned is carrying out safety criteria sincerely (execution of ISCS).

4) Provided the enterprise specializing in information security consultation sends the result of ISCS to the enterprise concerned, the enterprise concerned submit to MIC the diagnosis results concerned together with self opinion attached within 30 days.

5) If the enterprise concerned is not carrying out safety criteria or other necessity of correction is found, the enterprise specializing in information security consultation recommend improvement to the enterprise concerned, check if the improvement recommendation is well carried out within one or two months, and then submit the result to MIC.

6) MIC commands improvement to carry out safety criteria for the enterprise concerned which does not carry out improvement recommendation, and then check the result. It is possible to impose negligence fine on the enterprise concerned which does not carry out safety criteria regardless of improvement command.

In order to clearly notify the object of ISCS in advance, the object enterprises of the next year are concluded and notified in June of each year, and examination certificate is distributed to object enterpriser who sincerely conducted protection measures of ISCS.

C. Safety Criteria

The object enterpriser for ISCS observe "information security guidance regarding information communications network and information communications service"(hereinafter referred to as "information security guidance") according to the regulation of article 45 section 2 of information communications network law. ISCS is a process to check if object enterprisers observe this information security guidance. General content of information security guidance is specified in article 45 section 2 of information communications network law, but detailed content is determined by notification from MIC, and the matters to be observed in each service area are differently treated to reflect service characteristics of object enterpriser. Information security guidance is composed of technical, administrative, and physical fields, and composed of detail and actual security measures rather than typical and symbolic measures to help object enterprisers review security level actually through conducting this. Information security guidance for ISCS emphasizes technical field in general as compared to other information security guidance presented before; and in detail, ISP focuses on network control part, IDC focuses on physical security, and electronic transaction enterprise (multiple usage service) focuses on server control part.

Detail criteria for information security guidance are shown in the following Table 3.

D. Method

ISCS shall be conducted in the following 2 kinds of methods.

1) Written inspection to check the document, which certifying execution of information security guidance.

2) Site inspection to take a look at equipment operation and facility purchasing situation by directly paying a visit to site.

TABLE II
FEATURES OF WRITTEN INSPECTION AND SITE INSPECTION

Division	Features
Written inspection	Performance of information security guidance (law article 45 sections 2) shall be inspected primarily based on related proof data.
Site Inspection	Inspection by paying a visit to site in order to check execution of items which are difficult to confirm in writing as a result of written inspection

TABLE III
DETAIL CRITERIA FOR INFORMATION SECURITY GUIDANCE

Division		Detail content
Administrative Measures	Setup and operation of information security organization	o Constitution of Information Security Organization o Appointment of a Responsible Person in charge of Information Security o Assignment of Information Security Organization Member Role
	Establishment and management of information security planning and so on	o Information Security Policy o Information Security Execution Planning o Information Security Practical Guide
	Personal security	o Internal Personal Security o External Personal Security o Consignment Operation Security
	User security	o Information Offer of Information Security
	Intrusion incident response	o Establishment and Execution of Intrusion Incident Response Planning
	Information security measure check	o Self Check of Security Measure
	Information asset management	o Status Management of Information Communication Equipment and Facility
Technical measures	Network security	o Traffic Monitoring o Wireless/Mobile Network Service Security o Setup and Operation of Information Security System
	Information communication equipment security	o Web Server Security o DNS(Domain Name System) Server Security o DHCP(Dynamic Host Configuration Protocol) Server Security o DB(Database) Server Security o Router/Switch Security o Information Security System Security o Vulnerability Check o Access Control and Security Configuration Management o Administrator's Password Management o Log Management o Security Patch Management o Backup and Recovery
Physical measures	Security for entrance and access control	o Access Control of Information Communication Facility
	Operation and management of subsidiary equipment and facility	o Setup and Operation of Backup Equipment and Facility

IV. Conclusion

The purpose of MIC preparing and notifying safety criteria is to make the enterpriser concerned secure professional control systems and technology for information security, enhance the level of information security recognition for employees including CEO of the enterpriser concerned, and then eventually secure stability of national Internet network. The safety criteria are expected to steadily maintain growth situation of Internet related industry by securing stability of Internet network and be able to prepare basis for sincerely conducting the core role of national, social operation.

References

[1] Korea Information Security Agency, CERTCC-KR (KOREA Computer Emergency Response Team Coordination Center), http://www.kisa.or.kr , http://www.krcert.or.kr .
[2] MIC, revised plan for the law regarding the information communications network usage promotion, information protection, etc., 2003.
[3] MIC, data on the ISCS hearing, 2003.
[4] IT Health Check, 2005 http://www.cesg.gov.uk/
[5] IT Baseline Protection Certification process, 2005 http://www.bsi.bund.de/english/gshb/zert/index.html .
[6] Information Technology Infrastructure Security and Protection Services (ITISPS), 2005 http://www.cse-cst.gc.ca/en/services/industrial_services/itisps_program .

Jong-Whoi Shin received his M.S. degree in Computer Science and Technology from Korea University, South Korea, in 2001. He is currently working to information infrastructure protection division in Korea Information Security Agency as a senior researcher. His research interests include security for information infrastructure, mobile ad hoc wireless networks, and RFID.
Jin-Tae Lee received his M.S. degree in Computer Science from Yonsei University, South Korea, in 2005. He is currently working to information infrastructure protection division in Korea Information Security Agency as a researcher. His research interests include security for information infrastructure, and mobile ad hoc wireless networks.
Sang-Soo Jang received his M.S. degree in Information Security from Dongkook University, South Korea, in 2003. He is currently working to information infrastructure protection division in Korea Information Security Agency as a director. His research interests include security for information infrastructure, and information security management system.
Jae-Il Lee received his M.S. degree in Computation & Statistics from Seoul National University, South Korea, in 1988. He is currently working to information infrastructure protection division in Korea Information Security Agency as a vice president. His research interests include security for information infrastructure, and PKI.