World Academy of Science, Engineering and Technology
International Journal of Information and Communication Engineering
Vol:2, No:4, 2008

Many-Sided Self Risk Analysis Model for Information Asset to Secure Stability of the Information and Communication Service

Jin-Tae Lee, Jung-Hoon Suh, Sang-Soo Jang, and Jae-Il Lee

Abstract—Information and communication service providers (ICSP) that are significant in size and provide Internet-based services take administrative, technical, and physical protection measures via the information security check service (ISCS). These protection measures are the minimum action necessary to secure the stability and continuity of the information and communication services (ICS) that they provide. Thus, information assets are essential to providing ICS, and deciding the relative importance of target assets for protection is a critical procedure. The risk analysis model designed to decide the relative importance of information assets, which is described in this study, evaluates information assets from many angles, in order to choose which ones should be given priority when it comes to protection. Many-sided risk analysis (MSRS) grades the importance of information assets, based on evaluation of major security check items, evaluation of the dependency on the information and communication facility (ICF) and influence on potential incidents, and evaluation of major items according to their service classification, in order to identify the ISCS target. MSRS could be an efficient risk analysis model to help ICSPs to identify their core information assets and take information protection measures first, so that stability of the ICS can be ensured.

***Keywords*—**Information Asset, Information Communication Facility, Evaluation, ISCS (Information Security Check Service), Evaluation, Grade.

I. Introduction

THE informatization infrastructure in Korea has developed rapidly, to the extent that Korea is now recognized worldwide as a “strong Internet country”. Many efforts are being made quickly, to establish a well-founded infrastructure for the ICS and to take the high ground as a strong IT country in the future. According to the “IT 2005 in Numbers” survey published by the Korean Ministry of Information and Communication (MIC), 7 out 10 people in Korea are connected to the Internet (6th highest rank in the world), and 7 out of 10 households are wired with high-speed Internet (1st rank in the world) as well. This report proves that the informatization level of Korea is the highest in the world, both in terms of infrastructure and utilization. The number of people connected to the Internet was reported as 32.57 million as of June 2005, which is 71.9% of the total population of Korea.

In addition, regarding e-commerce trade, the number of Internet banking accounts and online stock trading ratio, we can see that online transactions are continuously on the rise as shown in Table I. This trend tells us that development of the ICS has been accelerated even further by consumers sensitive to new technologies in the world’s best IT environment [1].

TABLE I
Size of E-Commerce, Number of Internet Banking Accounts, and Online Stocking Trade in Korea

Type	1999	2000	2001	2002	2003	2004	2005
e-Commerce size (billion won)	-	-	118,976	177,809	223,090	314,079	171,131 (JUN)
Internet banking accounts (10,000)	12	401	1,131	1,771	2,275	2,427	2,543 (SEP)
Online stock trading ratio (%)	25.4	55.9	66.6	64.3	60.3	77.1	64.0 (NOV)

Source: National Statistical Office, Statistical Information System (http://kosis.nso.go.kr)

On the other hand, it is true that countermeasures against informatization dysfunctions such as hacking, virus, and privacy violation, are not complete enough, when compared with the well-established informatization environment and fast Internet growth[2]. Problems occurring from these vulnerabilities are serious. As seen in Table II “Hacking and virus damages by year,” the number of worm/virus incidents is decreasing but the number of hacking incidents is on the rise.

TABLE II
Hacking and Virus Damages by Year

Type	1999	2000	2001	2002	2003	2004	2005
Hacking	572 (262%)	1,943 (240%)	5,333 (175%)	15,192 (185%)	26,179 (72%)	24,297 (-7.2%)	33,633 (34.3%)
Worm/Virus	-		65,033	38,677 (-41%)	85,023 (120%)	107,994 (66%)	16,093 (-85%)

Source : Monthly report on hacking virus statistics and analysis, Korea Internet Security Center, KISA

Korea experienced major damage from nationwide Internet service interruption due to the Slammer Worm on January 25, 2003. Clearly, the “January 25th Internet Incident” serves as a reminder that ICSPs, government, private enterprises, and all users must understand the importance of information security. Taking that incident as an opportunity, the Minister of Information and Communication presented the ISCS standard

Manuscript received August 31, 2006. This work was supported in part by the Korean Ministry of Information and Communication.

Jin-Tae Lee (phone:+82 2 405 5567; fax: +82 2 405 5219; e-mail: cybermax@kisa.or.kr), Jung-Hoon Suh(e-mail:sjhoon@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.

and stipulated that security checks must be implemented from July 2004, in order to encourage ICSPs to ensure service stability and enhance Internet information security. The purpose of mandating the implementation of security checks by regulation is to enhance the stability and reliability of our national information and communication network and protect the rights of Internet service users[3].

From the viewpoint of ICSPs, service interruptions may cause a decrease in revenue, increased customer complaints, and deteriorated employee productivity. Likewise, ICSPs need to manage risk in order to increase ICS user's satisfaction and protect their rights, as well as their survival. On the other hand, their information asset, particularly the ICF, plays a major role in providing service. It is expected to continue to play a role of the subject that provides the actual service using information, even though the ICS is diversifying and information technology will continue to evolve in the future.

It is evident that risk analysis of the ICF should be carried out, in order to manage risk of the service that will decide success in the market. However, it is not easy to take complete preventive measures against attacks on the numerous ICFs possessed by the ICSPs. Nevertheless, risk management of the major information assets cannot be ignored, as they are critical to service operations. Most studies on risk analysis of information assets have focused on general circumstances, or on one major factor only. As a result, a study that takes the comprehensive ICS types into account has previously not been available. This paper presents an evaluation model through risk analysis of the information asset, in order to select major ICFs that should receive security checks. That is, this study illustrates the necessary scope of evaluations, and major evaluation items so that these items can be analyzed from multilateral perspectives for the purpose of risk analysis on the ICFs possessed by ICSPs. Through this approach, the reliability of the evaluation result with respects to information assets is enhanced, so that ICFs that are indispensable and significantly important for the service can be identified and isolated[4][5].

II. Concept of the ISCS

1) Overview of the ISCS

The ISCS was enacted to cope with information security incidents that have been continuously occurring in the information and communication network since the "January 15th Internet Incident" in 2003. Designed to secure the stability and reliability of the information and communication network and service, the ISCS stipulates that security checks should be performed between July 30 and July 29 of the next year by the specialized security check agency for major Internet service providers(ISPs), integrated ICF providers (Internet Data Center), and Internet business companies that have over 10 billion won annual revenue from their information and communication area, or over 1 million hits per day on average.

2) Object of Security Check

An ICSP is subject to the ISCS if it provides an Internet-based service that can affect the national information and communication network, or cause inconvenience or economic loss to a large number of people, if a security incident occurs. According to characteristics of the ICS, services can be grouped into three categories that are provided by the applicable ICSP.

- The party that provides nationwide network access service by providing Internet access, a telecommunication line facility, or network service. (Major ICSPs/ISPs)
- The party that operates/manages the integrated ICF to provide ICS for others through co-location, server hosting, and network service. (Integrated ICF providers/IDCs)
- The party that provides the ICS for enterprises and individuals with over 10 billion won annual review from the ICS area or over 1 million visitors per day on average (Shopping mall, portal, Internet game, education, reservation, newspaper and broadcasting, and etc.)

A party which fits one of the classifications above and is subject to the ISCS is required to select the ICF that should be checked and the scope of the ICS as well. In selecting the applicable facility, it should be considered first that any information asset contributing to stability of the service should be included. Selection of the information asset varies according to the ICS provided by the object.

3) Criteria of Security Check

Security check criteria is divided into three groups – administrative, physical, and technical protection measures, which was announced by the MIC to secure stability of the information and communication network and reliability of the information. The criteria must be complied with by law. Table III summarizes the details of the security check criteria.

TABLE III
MAJOR CONTENTS OF THE SECURITY CHECK CRITERIA

Contents		
1. Administrative protection measures	1.1. Establishment and operation of the information security organization	1.1.1. Establishment of the information security organization
		1.1.2. Appointment of the information security manager
		1.1.3. Establishment of the roles of information security team members
	1.2 Making and managing the information security plan and others	1.2.1. Establishment and implementation of the information security policy
		1.2.2. Establishment and implementation of the information security implementation plan
		1.2.3. Preparation and compliance with information security working guidelines
	1.3. Human resource security	1.3.1. Security of internal staff
		1.3.2. Security of external staff
		1.3.3. Security of commissioned operations
	1.4. User protection	1.4.1. Providing information on the security of information
	1.5. Coping with incidents	1.5.1 Establishment and implementation of the incident response plan
	1.6. Checking information protection measures	1.6.1. Internal check of protection measures

	1.7. Managing information assets	1.7.1 Managing the status of ICF
2. Technical protection measures	2.1. Network security	2.1.1. Traffic monitoring
		2.1.2. Wireless service security
		2.1.3. Installation and operation of the information security system
	2.2. Security of the ICF	2.2.1. Web server security
		2.2.2. DNS server security
		2.2.3. DHCP server security
		2.2.4. Database server security
		2.2.5. Router/Switch security
		2.2.6. Security of the information security system
		2.2.7. Vulnerability check
		2.2.8. Managing access control and security settings
		2.2.9. Managing administrator password
		2.2.10. Log management
		2.2.11. Security patch management
		2.2.12. Backup and recovery
3. Physical protection measures	3.1. Entry/Exit and access control	3.1.1. Controlling entry/exit and access to the ICF
	3.2. Operating/Managing incidental facilities and equipments	3.2.1. Installing/Running backup facilities and equipments

48items in total including 21 administrative, 24 technical and 3 physical protection measures.

4) Security Check Status of ICFs

Table IV shows the list of ICFs possessed by 142 ICSPs (13 ISPs, 63 IDCs, and 66 shopping malls) that have received the ISCS in 2005. The term ICF generally refers to servers, network equipment, and information security systems that are critical to providing ICS. The ICSPs that should receive the ISCS according to the regulations have the obligation of selecting the core ICF required for service provision and complying with the information security guidelines proposed in the ISCS. As shown in Table IV, the type of information asset possessed may be quite different, depending on the type of ICS provided. ISPs typically possess a lot of network equipment, whereas IDCs possess servers, network equipment, and information security systems, while internet shopping malls usually possess many servers. This variation in information assets could be important criteria to use when evaluating risk factors, as explained in "Evaluation by major factors according to the service classification system," which is one of the risk analysis methods proposed by this paper.

TABLE IV
FACILITIES AND AVERAGE EQUIPMENTS SUBJECT TO INFORMATION SECURITY CHECK

(Unit: set)

Classification			All	ISP	IDC	Shopping mall & others
Middle category		Small category				
ICF	Server	DNS server	1.5	5.0	2.2	1.0
		DHCP server	2.1	21.8	0.1	0.2
		DB server	9	19.0	5.3	13.3
		Public server	14.5	12.6	6.1	25.8
		Administrative server	4.5	27.6	3.4	2.9
		Application server	22.9	44.7	1.6	39.0
		Log server	0.4	1.3	0.4	0.5
		Other	41.6	6.3	8.0	83.0
	Network equipment	Router	5.6	40.3	6.5	2.0
		Switch	14.9	79.4	19.2	9.1
	Information security system	Firewall	3.3	10.7	6.1	2.9
		Intrusion detection system	1.5	5.3	3.9	0.8
		Authentication system	0.2	0.5	0.4	0.1
Others			19.9	183.3	4.8	5.6
Total			141.7	457.8	68.0	186.2

The "Other" item under "Server" in the middle category shows the number of total servers provided by companies that did not provide specific information regarding equipment in their small category.

III. RISK SELF-ANALYSIS METHOD BASED ON INFORMATION AND COMMUNICATION SERVICE TYPE

A. *Concept of Many-Sided Risk Self-Analysis*

An ICSP subject to the ISCS should identify and classify their information asset first, in order to manage it efficiently and provide it to customers. The "information asset" means everything that is valuable to the organization. Most enterprises have procedures and methods of protecting the information asset used to provide the ICS. The many-sided self-analysis proposed in this paper allows the subject of a security check to analyze the risk of its information asset from multiple aspects. The subject of a security check can perform risk analysis on the ICF, such as evaluation of major security check items, evaluation of dependency on the information and communication facility (ICF) and impact of potential incidents, and evaluation of major items considering the type and characteristics of the ICS. This model has a simple structure that can be applied to most normal circumstances. The many-sided risk analysis procedure is composed of 4 steps as described in Fig. 1.

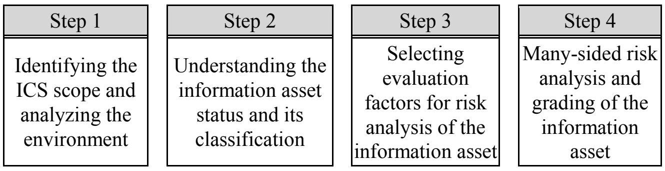
Step 1
Identifying the ICS scope and analyzing the environment
Step 2
Understanding the information asset status and its classification
Step 3
Selecting evaluation factors for risk analysis of the information asset
Step 4
Many-sided risk analysis and grading of the information asset

Fig. 1 Procedure for many-sided risk self-analysis

▪ Step 1: Identifying the ICS scope and analyzing the environment

In the first step, objectives, targets, and details of the ICS provided should be identified and defined. In particular, the characteristics and the environment of the ICS need to be analyzed.

▪Step 2: Understanding the information asset status and its classification

Among the information asset possessed by the check target, the status of the ICF that is actually running should be identified and listed. The ICF status serves as basic data to identify the object of a security check. Then, the found ICF should be classified according to factors that significantly affect the internal and external environment. Based on this classification, the purpose, type, characteristic, owner, manager, and location of the ICF should be listed and managed properly.

▪Step 3: Selecting evaluation factors for risk analysis of the information asset

In this step, the evaluation area needs to be set, which is required for many-sided risk analysis of the ICF in deciding the security check object, and major elements needs to be identified that will be evaluated in each area. This paper proposes three evaluation methods for risk analysis of the information asset. Each method focuses on a different aspect of ICF evaluation. For risk analysis, the evaluation area should be determined first, and major evaluation items should be set for each area.

▪ Step 4: Many-sided risk analysis and grading of the information asset

In this final step, core ICFs are selected that should be protected in line with the purpose of the ICS. In this paper, the importance of the ICF is evaluated, using three evaluation methods – evaluation by major security check item, evaluation of dependency on the information and communication facility (ICF) and impact of potential incidents, and evaluation by major items. The core ICF for the security check is determined by comprehensively considering the result of each evaluation, and the ICF's importance and influence on service provision.

B. *Procedure of Many-Sided Risk Self-Analysis*

1) Step 1: Identifying the ICS scope and analyzing the environment

To identify the scope of a security check, the definition scope of the ICS provided by object of the check should be determined and the service detailed should be understood. To finalize the security check's scope, it is most important to define the definition scope and details of the ICS for each security check object. Once the security check scope and service details are clarified, the ICF for service provisioning can be broadly classified into servers, network equipment, information security system, etc. Risk analysis of the ICF, which is performed to identify ISCS objects and their importance, starts from service scope definition and analysis of the environment that significantly affects the internal and external corporate environment. In this study, ISCS objects are classified again with reference to "Standard of Products and Services Classification for the Information and Communication Industry" – the standard of the Korea Association of Information & Telecommunication (KAIT).

First, major ICSP should analyze the risk centered on network equipments to secure service stability and continuity, because they are the main providers of Internet service.

TABLE V
SERVICE CLASSIFICATION OF MAJOR ICSP

ICS area	Service	Means	Function	Type	Product
Major ICSP	Infrastructure communication	Fixed line communication service	High-speed Internet network	High-speed Internet service	Cable modem service
					XDSL service
					Other high-speed Internet service
				High-speed access network service	
				Other high-speed communication service	
		Wireless communication service		Wireless data access service	
	Value-added communication	Internet access and management service	Internet access-based service	Internet access service (ISP)	

To guarantee stability and continuity of each other's customer service, IDCs need to focus on servers and network equipment at the time of risk analysis, since they operate and manage concentrated information system equipment like computers, commissioned by the customer who provides the ICS.

TABLE VI
SERVICE CLASSIFICATION OF IDC

ICS area	Service	Means	Function	product
IDC	Value-added service	Internet access and management service	Hosting and management service	Server hosting
				Storage hosting
				Co-location
				Network service (including line lease)
				Security management service (if provided)
				Domain management service (if provided)

Other ICSPs provide various contents and e-Commerce such as Internet shopping malls, portals, games, reservations, content provision, credit card information retrieval and payment switching. Therefore, risk analysis should be performed mainly for the servers that can directly/indirectly affect these services.

TABLE VII
SERVICE CLASSIFICATION OF OTHER ICSPS

ICS area	Service	Means	Function	product
Other ICSPs, like shopping malls	Value-added communication	Internet access and management service	Internet access-based service	PC communication service
	Value-added communication	Value-added application service	Services like credit card information retrieval/payment switching	
			Computer reservation systems	
			Electronic document exchange	
			Network service (including line lease)	
			Internet information provisioning service	Internet portal service
				e-Commerce (shopping mall)
				Internet broadcasting (newspaper/broadcasting)
				Internet game
				Other Internet information provisioning service (music, education, and etc.)
	Broadcasting	CATV		CATV (Cable-SO)

2) Step 2: Understanding the information asset status and its classification

Once the ICS scope is determined and the environment is analyzed, the service provider needs to identify, maintain, and manage the ICF. In particular, the service provider should list all servers, network equipment, and information security systems that should be protected to provide the ICS and identify the ICF subject to the ISCS. For detailed analysis of the ICF, the list needs to include as much information as possible, such as purpose, type, characteristic, owner, manager, asset ID, and location.

TABLE VIII
MANAGEMENT FORMAT OF INFORMATION ASSETS

□	□		□	Characteristics				Possession type		Management type			□
	ICF classification			□	□	□	□	□	□	□	□	□	
Service	Middle	Small	No. of sets	Code	Model	Location	Usage	Own/Leased	Owner (Dept/ name)	Own/ Outsourcing	Administrator (Dept/ name)	Contact Information	Remark
ICS	Server	DNS server	2	Sdns01	IBM	The first floor	DNS Service	Own	e-Biz Dept/ Gil-Dong Hong	Own	System Operation Dept/ Gap-Dol Kim	123-4567/admin@xxx.xx.kr	
		DHCP server											
		DB server											
		others.											
	Network equipment	Router											
		Switch											
		others											
	Information security system	Firewall											
		IDS											
		Authentication system											
		Virus wall and others											
	Others												

3) Step 3: Selecting evaluation factors for risk analysis of the information asset

In this step, evaluation factors are drawn out and determined that will be used in the three evaluation methods which are proposed by this paper for the many-sided risk analysis of the ICF. It is important to select the item that enables evaluation of the value of the ICF in detail, using each evaluation method. The list of the ICF status created in the previous step is useful in deciding many-sided evaluation factors. The optimal item needs to be selected, which enables evaluation and quantification from several aspects, in order to select the security check object that plays a crucial role in providing the service.

4) Step 4: Many-sided risk analysis and grading of the information asset

In the final step, the ICF is graded and classified, based on the result of risk analysis of the ICF, which is performed to classify the security check. When the ICF is graded according to the evaluation result obtained from evaluation factors (determined in the previous step), different protection measures can be applied in line with the grade that has been given. It is advisable to grade an ICF that is subject to the ISCS by considering all results obtained from each evaluation method, as well as the conditions and the environment of the object that has been checked.

C. Methods of Many-Sided Risk Self-Analysis

1) Method 1: Evaluation by major security check item

The first method presented in this paper for many-sided risk self-analysis is involved with evaluation of the ICF of the ICSP being checked, such as its various servers and network equipment. Major evaluation items include confidentiality, integrity, and availability. To further elaborate: confidentiality means the prevention of unauthorized access to secret information to ensure safety against security risks. Integrity means resistance against illegal information alteration and breakdown. Availability means that the information service is kept running without interruption.

When evaluating confidentiality, various affects on business operation, service provisioning, and corporate image of the ICSP being checked were considered, for example if information stored in the ICF concerned had been leaked (confidentiality), altered (integrity), or damaged or interrupted (availability). This evaluation method sets 5 evaluation levels and scores for the information asset, mainly depending on the importance of the information stored at the facility concerned. Evaluation scores are defined as VH (Very High) = 4, H (High) = 3, M (Medium) = 2, L (Low) = 1, and N (None) = 0. The question of whether to apply a security check to the object is determined by the total score of the three items. The example in the below Table IX shows that the security check should be applied if the evaluation level is H or the sum of the evaluation score is over 6.

TABLE IX
EXAMPLE OF INFORMATION ASSET SCORING BASED ON EVALUATION BY MAJOR SECURITY CHECK ITEMS

Classification of information asset			Confidentiality	Integrity	Availability	Evaluation result		Check object
						Evaluation level	Evaluation score (sum)	
ICF	Server	e-Commerce server	H(3)	H(3)	VH(4)	VH	10	Yes
		Information management server	M(2)	M(2)	M(2)	M	6	Yes
		…	…	…	…	…	…	…
	Network equipment	Backbone router	H(3)	H(3)	VH(4)	VH	10	Yes
		Layer 3 switch	L(1)	L(1)	M(2)	M	4	No
		…	…	…	…	…	…	…
	Information security system	Firewall	H(3)	H(3)	H(3)	M	9	Yes
		Authentication system	VH(4)	M(2)	H(3)	VH	9	Yes
		…	…	…	…	…	…	…

2) Method 2 : Evaluation of dependency on the ICF and influence of potential incidents

The second method takes the degree of influence as the major evaluation item, such as dependency on the ICF used to provide the ICS, size and scope of potential damage caused by an incident in the facility concerned, possibility of an incident occurring, ease of recovery, relationship with other ICFs, etc. Evaluation scores are also defined as VH (Very High) = 4, H (High) = 3, M (Medium) = 2, L (Low) = 1, and N (None) = 0. Selection of whether a security check must be applied to the item is based on the sum of the pre-defined evaluation scores. The selection threshold score can be selected. The example in the below Table X shows that a security check must be applied to the object if the sum of the evaluation score is over 18.

TABLE X
EVALUATION OF DEPENDENCY ON THE ICF AND IMPACT OF A POTENTIAL INCIDENT

Classification of ICF			Evaluation item				Evaluation score (sum)	Check object
			1. Dependency on the ICF concerned (sum)	2. Scope and size of the incident damage (sum)	3. Possibility of incident occurrence and ease of recovery (sum)	4. Inter-dependency with other ICFs (sum)		
ICF	Server	e-Commerce server	6	7	4	3	20	Yes
		Information management server	3	3	5	3	14	No
		…	…	…	…	…	…	…
	Network equipment	Backbone router	6	6	3	5	20	Yes
		Layer 3 switch	4	3	0	2	9	No
		…	…	…	…	…	…	…
	Information security system	Firewall	5	6	5	4	20	Yes
		Authentication system	6	6	4	7	23	Yes
		…	…	…	…	…	…	…

TABLE XI
EVALUATION OF DEPENDENCY ON THE ICF AND IMPACT OF A POTENTIAL INCIDENT

Evaluation item			Applicable object				Evaluation score					
							e-Commerce server	Information management server	Backbone router	Layer 3 switch	Firewall	Authentication system
Dependency on the ICF concerned	1	How seriously does the ICF concerned affect the core service?	Indispensable	Directly related	Indirectly related	Not related						
			3	2	1	0						
	2	Is the ICF concerned currently designated as active, replacement, development, or test equipment?	Operation equipment	Replication facility	Backup/ Replacement facility	Development / Test facility						
			3	2	1	0						
Scope and size of incident damage (sum)	1	What is the predicted economic loss or scope of confusion if information or equipment becomes obsolete due to any leak or alteration of the core information caused by an incident in the ICF concerned?	Would affect other SPs and services	Would affect the entire company	Would affect some of the company	None						
			3	2	1	0						
	2	How many customers will be affected if information or equipment becomes obsolete due to any leak or alteration of core information caused by an incident at the ICF concerned?	Over 100,000	Over 10,000	Under 10,000	None						
			3	2	1	0						

	3	Is their any possibility of legal action if the information or equipment becomes obsolete due to a leak or alteration of core information caused by an incident at the ICF concerned?	Very high	High	Medium	None					
			3	2	1	0					
Possibility of incident occurrence and ease of recovery	1	Is the possibility of incident occurrence high because the ICF concerned is connected to a public network like the Internet, to perform regular business?	Directly connected	Indirectly connected	Loosely connected	Dedicated to internal network					
			3	2	1	0					
	2	To what extent can the ICF concerned be recovered in real time, if a large amount of data is leaked/altered, or if the information is unavailable due to a large-scale network shutdown?	No recovery	Recovery of core parts	Recovery of some parts	Complete recovery					
			3	2	1	0					
Inter-relationship with other ICFs	1	To what extent is the ICF concerned connected to other security check ICFs? (To what extent could a fatal problem of the ICF concerned affect these others?)	Many (more than 3)	1 – 2	Corresponding system	No affect					
			3	2	1	0					
	2	What is the effect on other ICFs, if the ICF concerned leaks or alters important information due to an incident, or the information in the ICF concerned cannot be accessed due to a breakdown of the IT infrastructure?	Affect with the same level	Partial influence	Insignificant influence	No influence					
			3	2	1	0					

3) Method 3: Evaluation of major items according to their service classification

The third method - evaluation of major items according to their service classification, depends on the type and characteristics of the ICS provided by the ICSP concerned. The evaluation item differs according to the ICS, because security check objects (ICSP, IDC, and shopping mall) provide different services, using different servers, network equipment, and information security systems. As a result, these circumstances must be taken into account during evaluation. Evaluation items include those that delicately affect the service, such as total line capacity, daily average use amount, implementation cost, recovery cost, and number of customers for the network, whereas the amount of transactions processed, database capacity, and the number of accessing users per day on average are considered for servers. Evaluation scores are also defined as VH (Very High) = 4, H (High) = 3, M (Medium) = 2, L (Low) = 1, and N (None) = 0. Selection of the security check item is based on the sum of pre-defined evaluation scores.

TABLE XII
EVALUATION BY MAJOR ITEMS ACCORDING TO THE SERVICE CLASSIFICATION

Information asset classification			Evaluation Item								Evaluation score (sum)	Check object
			Total line capacity	Daily average use amount	Implementation cost	Recovery cost	Number of customers	Number of transactions processing	Database capacity	Average number of users per day		
ICF	Server	e-Commerce server	-	1	H (3)	VH (4)	H (3)	VH (4)	H (3)	VH (4)	21	Yes
		Information management server	-	-	M (2)	M (2)	L (1)	M (2)	M (2)	M (2)	11	No
		…	…	…	…	…	…	…	…	…	…	…
	Network equipment	Backbone router	VH (4)	VH (4)	VH (4)	VH (4)	VH (4)	-	-	-	20	Yes
		Layer 3 switch	M (2)	M (2)	L (1)	L (1)	M (2)	-	-	-	8	No
		…	…	…	…	…	…	…	…	…	…	…
	Information security system	Firewall	-	-	H (3)	H (3)	M (2)	M (2)	L (1)	M (2)	13	Yes
		Authentication system	-	-	VH (4)	VH (4)	H (3)	H (3)	H (3)	H (3)	20	Yes
		…	…	…	…	…	…	…	…	…	…	…

4) Grading and classification of the information asset

At the final stage, the security check object that provides the ICS should grade the ICF and assign a risk code, based on the comprehensive evaluation results obtained using the three evaluation methods as described above. Grading and classification will become the important index for ICF selection that is subject to the ISCS, and required for continued management. In addition, each object can apply its standard when assigning the classification code and the evaluation result (grade) that are designed to set the management and protection level of the ICF. Evaluation grades are defined as VH (Very High) = over 50, H (High) = 49 through 40, M (Medium) = 39 through 30, L (Low) = below 30. The question of whether to apply a security check to the object is determined by the total score of the three items. The following Table XIII shows the example of evaluation grading and asset classification code assignment for the ICF.

TABLE XIII
GRADING AND CLASSIFICATION OF THE INFORMATION ASSET

Type of the ICS		Classification of the information assets			Evaluation Result(ER)						Check object (Evaluation grade)	Information asset classification code
					ER1		ER2		ER3			
					Evaluation score	Check object	Evaluation score	Check object	Evaluation score	Check object		
ICS	ICSP	ICF	Server	e-Commerce server	10	Yes	20	Yes	21	Yes	Yes (VH:51)	
				Information management server	6	Yes	14	No	11	No	No (M:31)	
				…	…	…	…	…	…	…	…	…
	IDC		Network equipment	Backbone router	10	Yes	20	Yes	20	Yes	Yes (VH:50)	
				Layer 3 switch	4	No	9	No	8	No	No (L:21)	
				…	…	…	…	…	…	…	…	…
	Other ICSPs (shopping malls, etc)		Information security system	Firewall	9	Yes	20	Yes	13	Yes	Yes (H:42)	
				Authentication system	9	Yes	23	Yes	20	Yes	Yes (VH:52)	
				…	…	…	…	…	…	…	…	…

IV. CONCLUSION

Recently, u-City and U-Government is drawing public attention as Korea transforms into a wired society and a broadband convergence network (BcN) is rapidly established. Like this, Korea is in the vortex of the change to the new IT environment and the ICS is evolving in diverse ways. This phenomenon implies that we have to provide ICS in a complex IT environment, and the value of the information assets we need to protect is increasing. Therefore, to protect information assets, we need to scrutinize the types and characteristics of the current ICS as well as the new ICS and IT technology that will be available in the future. This paper presented a risk analysis model for identifying the most critical information assets in the current service environment, which means that more evaluation indices are required to evaluate the information assets that will be available in future IT environments. For accurate evaluation of information assets in the future IT environment to secure service availability and continuity, the trend of new IT technology and service needs to be analyzed, from home networks, to wireless Internet, mobile banking, and DMB. In addition, an improved risk analysis model needs to be proposed that defines classification and major evaluation items more clearly with respects to evaluation of the information asset that provides the service.

REFERENCES

[1] Korea National Statistical Office, Statistical Information System, “Size of e-Commerce, number of Internet banking accounts, and online stocking trade in Korea“, http://kosis.nso.go.kr

[2] Korea Information Security Agency, Korea Internet Security Center, “Monthly report on hacking virus statistics and analysis, http://www.krcert.or.kr

[3] J. H. Shin, “ISCS (Information Security Check Service) for the Safety and Reliability of Communications”, WEC ICIS 2005 Proceeding, June 2005.

[4] Korea Information Security Agency, “Vulnerability Analysis & Assessment Methodology version”, 2002.

[5] NIST, “Risk Management Guide for Information Technology Systems” 2001.

[6] J. Heo, “Risk Analysis Methodology for New IT Service”, 18th Annual FIRST Conference, June 2006.

Jin-Tae Lee received his M.S. degree in Computer Science from Yonsei University, South Korea, in 2005. He is currently working to IT 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.

Jung-Hoon Suh received his M.S. degree in Information Security from Kyungpook National University, South Korea, in 2001. He is currently working to IT infrastructure protection division in Korea Information Security Agency as a director. His research interests include security for information infrastructure, and PKI..

Sang-Soo Jang received his M.S. degree in Information Security from Dongkook University, South Korea, in 2003. He is currently working to IT 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 IT infrastructure protection division in Korea Information Security Agency as a vice president. His research interests include security for information infrastructure, and PKI.