World Academy of Science, Engineering and Technology
International Journal of Information and Communication Engineering
Vol:1, No:12, 2007

Improve of Evaluation Method for Information Security Levels of CIIP (Critical Information Infrastructure Protection)

Dong-Young Yoo, Jong-Whoi Shin, Gang Shin Lee, and Jae-Il Lee

***Abstract*—**As the disfunctions of the information society and social development progress, intrusion problems such as malicious replies, spam mail, private information leakage, phishing, and pharming, and side effects such as the spread of unwholesome information and privacy invasion are becoming serious social problems. Illegal access to information is also becoming a problem as the exchange and sharing of information increases on the basis of the extension of the communication network. On the other hand, as the communication network has been constructed as an international, global system, the legal response against invasion and cyber-attack from abroad is facing its limit. In addition, in an environment where the important infrastructures are managed and controlled on the basis of the information communication network, such problems pose a threat to national security. Countermeasures to such threats are developed and implemented on a yearly basis to protect the major infrastructures of information communication. As a part of such measures, we have developed a methodology for assessing the information protection level which can be used to establish the quantitative object setting method required for the improvement of the information protection level.

***Keywords*—**Information Security Evaluation Methodology, Critical Information Infrastructure Protection.

I. Introduction

IN accordance with the ongoing development of informatization, intrusion problems such as spam mail, phishing and pharming as well as threats to the national infrastructure are increasing. As the network of the national infrastructure is extended and spreads, and information is widely exchanged and shared, illegal access to information is becoming a serious problem. The legal response against foreign invasions and cyber-attacks is facing its limit as the communication network is transformed into an international, global system. From the international perspective, in an environment where major infrastructures are managed and controlled on the basis of the information communication network, such problems pose a serious threaten to national security.

To address this issue, many nations around the world are researching and developing various techniques and information security policies as a government-wide effort to protect their infrastructures from newly emerging threats. In the U.S., the National Information Infrastructure Protection Act was enacted in 1996, and the Presidential Decision Directive (PDD) 63 was issued on May 1998 to establish a government-wide security system for major infrastructures. In addition, the Department of Homeland Security (DHS) was founded with the issue of Executive Order-13284 on Jan 2003, and the National Strategy to Secure Cyberspace was announced on Feb 2003 [1]. Japan administered laws against illegal access acts on Feb 2000, and has established 『Information Security Measure Committee』 and 『Civilian Experts Council』 under the 『IT Strategy Center』. Korea has established Information & Telecommunication Infrastructure Security Committee under the prime minister in accordance with the Infrastructure Security Law enacted in 2001, and has been building systematic and comprehensive measures against electronic intrusions for critical information & Telecommunication infrastructures. Since the protection for operation and control of major social infrastructures requires involvement of various sectors such as communication, finance, military and energy, the committee was founded under the prime minister to direct and coordinate the establishment and execution of information & Telecommunication infrastructure security policies of various agencies. In particular, the head of a central administrative agency managing a critical information infrastructure designates critical information & Telecommunication infrastructures for each jurisdiction, establishes and executes yearly security plans, and enacts security policies and recommends them to the managing agencies of critical information infrastructures or orders actions required for security. However, such security policies have usually been established without consideration for security levels. Therefore, in order to establish a more effective security policy, methodologies must be developed to assess the security level for the managing agencies based on vulnerability analysis and result analysis. This paper

Manuscript received November 15, 2007. This work was supported in part by the Korean Ministry of Information and Communication.

Dong-Young Yoo (phone:+82 2 405 5266; fax: +82 2 405 5219; e-mail: ydy@kisa.or.kr), Jong-Whoi Shin (e-mail: jshin@kisa.or.kr), Gang-Shin Lee (kslee@kisa.or.kr) Jae-Il Lee (jilee@kisa.or.kr) are with the Korea Information Security Agency(KISA), 78, Garak-Dong, Songpa-Gu, Seoul, Korea..

intends to check the current security status and establish security measures accordingly to protect infrastructures effectively, and will propose a methodology of evaluation for the information security level for CIIP, which can enhance the security level of critical information infrastructure. The Information Security Evaluation Method will provide specific assessment schemes and methods that can be used for constant and active enhancement of security level.

II. Literature

Many related standards and guidelines have been drawn up for the effective assessment of security levels. In the U.S., SP800 – 53 (Recommended Security Controls for Federal Information Systems)[2] and SP 800 – 26 (Security Self-Assessment Guide for Information Technology System)[3] were developed by the NIST. As for the cases of information protection level assessment in the United States, in Part 3 of the e-Government Act, the FISMA (Federal Information Security Management Act) was enacted in 2002 to protect the information and information system of federal agencies. In compliance with the FISMA, the information protection management statuses of the federal agencies are assessed on a yearly basis. The top management and auditors of the federal agencies inspect the information security programs of the agencies on a yearly basis and report the results to the Office of Management and Budget (OMB) which then assesses the reports and submits them to the Congress. The assessment results are reviewed by the Government Supervision and Inspection Committee using the FIPS 200 (Federal Information Processing Standard), which was developed by reflecting the SP800-53A Guidelines of the NIST. The results of the review by the standing committee are published in the Federal Computer Security Report Card. The Act provides a comprehensive framework to strengthen the efficiency of the control items of information security for the operation and properties of the federal agencies, and efficient management and control strategies against the threats to the information security. It develops the methods of minimum control and maintenance for the protection of federal information and the federal information system, and provides a mechanism for strengthening the information security program management of the federal agencies. Through the guidelines of the NIST, it recommends the type of information and information system to be implemented, and develops the minimum information security requirements such as management, operation and technical control. The assessment results are indicated according to a scale of points from zero to 100, and marked with F for a score of zero to under 60, D- for 60 to under 63, D for 64 to under 67, and D+ for 67 to under 70, and so on up to A+.

TABLE I
FIPS200 vs IPLA

	FIPS 200 (NIST SP 800-53)	Information Protection Level Assessment
Assessment Categories and Items	Broad Classification (3) Middle Classification (17) Assessment Items (166)	Broad Classification (12) Middle Classification (54) Assessment Items (89)
Object	An act to protect the information and information systems of the federal agencies of USA	Supports stable operation and management of major information communication infrastructures, and assess the maturity
Features	- Information Audit Committee conducts assessment according to the FIPS 200 and SP 800-53 of NIST - Disclose the performance marks of the federal agencies (A+~F) every year	- Maturity assessment for the information protection level - Improve the levels of the infrastructures through maturity assessment stably

On the other hand, SSE-CMM (Systems Security Engineering-Capability Maturity Model)[4] serves as standard criteria that can be widely used by governments and businesses. SSE-CMM is intended to enhance the quality, economy and availability of products and services related to information security by developing security engineering into a well defined and mature sector.

BS7799 [5] is focused on public verification of businesses ensuring the secrecy, integrity and availability of customer information. BS7799 was developed by the Treasury Dept of U.K. under the title of "A Code of Practice for Information Security Management" as a general document that can be used as a reference by managers responsible for information security of organization and has become the standard for information security of organizations.

III. Proposal

A. Methodology

The proposed assessment method includes procedures for measuring the security level of an organization and deriving the maturity of the security level by analyzing the measured data. Developed by referring to the control category of SP800-53 and the detail assessment items of SP800-26, BS7799, and ISMS[1][6], detail control items for checking the security level includes 12 control categories, 54 control items, and 89 detail control items. Also, 89 detail control items can be divided into 48 function level items and 41 function process items, respectively. The function level items are purely related to provide any function. On the other hand, the function process items can be defined as

[1] Information Security Management System (ISMS) is a Korean security standard developed for administrative, physical and technical security management of an organization.

sub-process. Figure 1 illustrates how the items were derived. Table I shows the number of detail control items. Fig. 1 illustrates the distribution of control items over 12 control categories, which include general security management items such as policies and procedures, risk assessment, incident response.

TABLE II
NUMBER OF CONTROL AND DETAIL CONTROL ITEMS FOR EACH CATEGORIES

Control Categories	Control Items	No. of Detail Control Items
Information Protection Policy	Information protection organization	1
	Information protection plan	1
Risk Assessment	Assets classification	2
	Resources allocation	3
	Review security requirement	1
	Risk assessment	4
	Weakness diagnosis	1
Configuration Management	Configuration change control	3
	Configuration security setting	2
Maintenance	Maintenance tool	1
	Remote maintenance	1
Media Protection	Media output indication	1
	Media access control	1
	Media transportation method	1
	Document control	3
	Media and record destruction	1
Security Awareness and Training	Security awareness training	2
Emergency Plan/Work Continuity Plan	Emergency training	1
	Simulated training and grading of emergency plan	1
	Communication service dualization	1
	Information system backup and recovery	3
Physical /Environmental Protection	Physical access control	3
	Display media access control	1
	Physical access monitoring	1
	Power facilities and lines protection	2
	Emergency power	1
	Emergency lighting	1
	Environmental control	1
Personnel Security	Antecedents inspection	1
	Personnel management	1
	Internal human resources management	1
	Third party security	1
Accident Response	Simulated training for accident	1
	Accident monitoring	1
	Security accident report	2
Audit and Responsibility Traceability	Audit object event creation function	2
	Audit information management	1
	Audit monitoring, analysis, and report	1
	Audit record time branding function	1
	Denial prevention	1
System Access Control and Communication Protection	Account control	1
	Password control	3
	Setting control	1
	Access control	6
	Access trial failure control function	1
	Notice function of the cautions for system use	2
	Previous login information report function	1
	Session control function	2
	Isolation of system and application software	2
	Shared system resources control	1
	Protection from software defect and malicious code	3
	Tools and technologies for invasion detection and interruption	2
	Service reject protection	1
	Security communication route	1
	Creation and control of encryption key	2
	Internet telephone	1

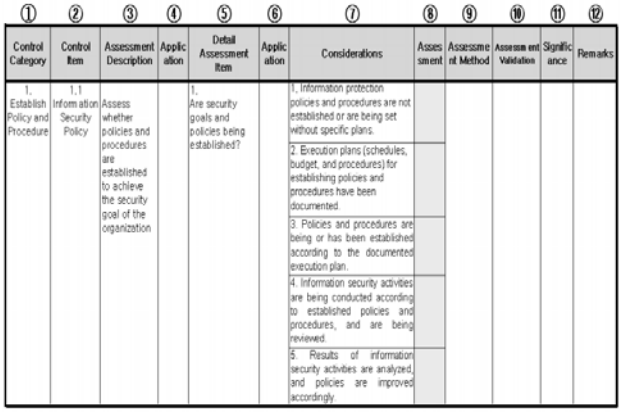
B. Evaluation of Information Security Level

The checklists for the 12 control categories, 54 control items and 89 detail control items presented in this paper are developed to be assessed through five levels. Based on the maturity measurement model of SSE-CMM and SP800-26, the proposed five levels were developed as a checklist that can be used for self assessment. The result of a self-assessment is certified through manager interviews, verification of related documents and on-site inspections. Table 2 provides definitions on the five levels of information security level assessment.

TABLE III
FIVE LEVELS OF INFORMATION SECURITY LEVEL ASSESSMENT

Level	Description
Level 1	Detail control items are not executed or are executed without specific plans.
Level 2	Execution plans (e.g. detailed procedures, schedules, and budget) for detail control items have been established and documented.
Level 3	Detail control items are being or have been executed according to documented plans.
Level 4	Results are measured for detail control items and are executed consistently for a certain period.
Level 5	Results are reviewed and improved accordingly.

Figure 1 shows the structure of the checklist, which contains 12 fields, used for assessment.



① Control Category	② Control Item	③ Assessment Description	④ Application	⑤ Detail Assessment Item	⑥ Application	⑦ Considerations	⑧ Assessment	⑨ Assessment Method	⑩ Assessment Validation	⑪ Significance	⑫ Remarks
1. Establish Policy and Procedure	1.1 Information Security Policy	Assess whether policies and procedures are established to achieve the security goal of the organization		1. Are security goals and policies being established?		1. Information protection policies and procedures are not established or are being set without specific plans.					
						2. Execution plans (schedules, budget, and procedures) for establishing policies and procedures have been documented.					
						3. Policies and procedures are being or has been established according to the documented execution plan.					
						4. Information security activities are being conducted according to established policies and procedures, and are being reviewed.					
						5. Results of information security activities are analyzed, and policies are improved accordingly.					

Fig. 1 Assessment Template Examples

① Control Category: Names of 12 control categories

② Control Item: Names of 54 control items

③ Assessment Description: Description of assessment for 54 control items

④ Application: Whether the control item is applicable

⑤ Detail Control Item: 89 control items used for checking control items

⑥ Application: Whether the detail control item is applicable

⑦ Considerations: Facts to consider for 5-level assessment of detail control items

⑧ Assessment: Assessment of detail control items according to 5-level assessment considerations

⑨ Method: Interview and document evaluation, on-site evaluation

⑩ Verification: Note the target of assessment and the target document name

⑪ Significance: Note the significance of the detail control item as High/Middle/Low

⑫ Remarks: Note remarks on assessment

Two methods are available for the estimation of the assessment result of the domestic information protection level. The first method consists in estimating the maturity result of the information protection level, by calculating the sum of the assessment values of the detail control items for the 54 control items;

$$S = \sum_{i=0}^{n} L_i \quad (1)$$

(S: Scores for control items, L_i : Score of detail control items)

Here, the lowest detail assessment step of the control items is estimated with the lowest step of the information protection maturity steps as the reference. The AL (Assessment Level), which is the sum total of the assessment values of the detail control items divided by the number of the detail assessment items, is the information protection level of the agency that was assessed.

$$AL = \frac{S}{N_{items}} \quad (2)$$

(S: Scores for control items, AL: Assesment Level)

The second method consists in calculating the percentage assessment of the information protection level, where the sum total of the assessment values of the detail control items of the respective control categories of the 54 control categories is calculated.

$$M = \sum_{i=1}^{n} SAi \quad (3)$$

(M: Sum total of the assessment values of the detail control items of the respective control categories, SAi: Assessment values of the detail control items, n: Number of applied items by control category)

The mean value of the sum of the assessment values of the detail control items by control category is calculated, and the values of each control category are expressed as a percentage.

$$LP = \frac{M}{N(sum\_of\_iems)} X100 \quad (4)$$

(Sum of the number of the applied items of the respective control category)

The sum total of the percentage values (LP) by each control category divided by the value of the control category is the percentage value of the information protection level assessment of the assessed agency.

$$AP = \frac{\sum_{i=1}^{12} LP}{N_{items}}$$

(N_{items} : Number of control categories)

Figure 2 below shows an example of the assessment result of the information protection level.

Control Categories (count of items : 89)		Value of Control Items				Level (1 ~ 5)
		Select Items	Result	Record	%	
Categories Result	1. Security Policy(2)	1	3	5	60.0%	3 level
	2. Risk Analysis(11)	11	55	55	100.0%	5 level
	3. Configuration Management(5)	5	25	25	100.0%	5 level
	4. A/S(2)	2	10	10	100.0%	5 level
	5. Media Protection(7)	7	35	35	100.0%	5 level
	6. Security Education(2)	2	10	10	100.0%	5 level
	7. Emergence and BCP Plan(6)	6	30	30	100.0%	5 level
	8. Physical Protection(10)	10	50	50	100.0%	5 level
	9. Personal Security(4)	4	20	20	100.0%	5 level
	10. Incident Response(4)	4	20	20	100.0%	5 level
	11. Audit and Trail(6)	6	30	30	100.0%	5 level
	12. Access Control(30)	28	140	140	100.0%	5 level
Record	Total	86	428	430	99.5%	4.83

Fig. 2 Example of the Assessment Result

Figure 3 is an example of assessing control items (e.g. establishment of information policies and procedures, risk assessment) and displaying the result in a spider graph. The graph shows that the access control & communication protection has the lowest security level.

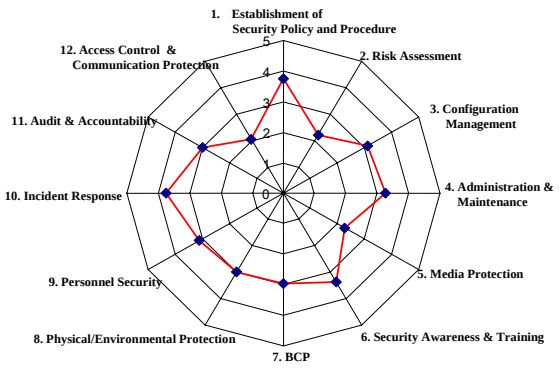


Fig. 3 Example of Level Distribution Diagram for Control Items

The level distribution diagram for control items shows which control items are strong or vulnerable to security threats, allowing managers to recognize and correct the vulnerabilities more easily. Eventually, this can used by managers of critical information infrastructure managers as a tool for conveniently measuring the information security level.

IV. Conclusion

In this study, an improved method was developed in order to solve the problems of the information protection level assessment - namely the lack of understanding of the managers with regard to the assessment items and the lack of clearly defined objects as regards the level assessment items, and the lack of reliability of the level assessment results - and to improve the reliability of the assessment. The suggested method describes the objects and contents of the control categories, and improves the degree of understanding by providing a template for the control items to assess the detail control items. In addition, in order to reduce the ambiguity of the step-wise points of the 89 detail control items, the points were refined, and explanations and case descriptions were added. Model assessments were conducted for the infrastructures of Korea to compare the previous results with the results obtained after the improvement of the points of the detail control items and the development of the explanatory note in accordance with the present study. The result of the comparison showed that the information protection level had been lowered. This was because the step-wide definitions of the points were clarified and any ambiguity was eliminated by including additional descriptions of the steps and cases. In particular, the difference in the assessment results of the categories that require clarity were interpreted to mean that the results of the information protection level assessment of the infrastructures obtained by this study are objective. The suggested method is expected to contribute to improving the understanding of the assessors of the information protection levels of major information communication infrastructures, as well as to provide an objective assessment. In addition, the presented explanation will constitute a guideline for the categories and items of control to improve the information protection levels of major national infrastructures.

References

[1] FISMA FRAMEWORK, September 19. 2006.
[2] NIST SP800-53(Recommended Security Controls for Federal Information System) http://www.nist.gov/
[3] NIST SP800-53A(Guide for Assessing the Security Controls in Federal Information Systems)
[4] NIST SP800-80(Guide for Developing Performance Metrics for Information Security) [1] The White House (The Department of Homeland Security), http://www.whitehouse.gov/deptofhomeland/
[5] NIST SP800-26 (Security Self-Assessment Guide for Information Technology System) http://www.nist.gov
[6] SSE-CMM
[7] http://www.kisa.or.kr/isms/
[8] http://www.iwar.org.uk/