J. Inf. Technol. Appl. Manag. 26(5): 13~25, October 2019
https://doi.org/10.21219/jitam.2019.26.5.013

ISSN 1598-6284 (Print)
ISSN 2508-1209 (Online)

Developing a Framework for the Implementation of Evidence Collection System: Focusing on the Evaluation of Information Security Management in South Korea

Myeonggil Choi* · Sungmin Kang** · Eunju Park***

Abstract

Recently, as evaluation of information security (IS) management become more diverse and complicated, the contents and procedure of the evidence to prepare for actual assessment are rapidly increasing. As a result, the actual assessment is a burden for both evaluation agencies and institutions receiving assessments. However, most of them reflect the evaluation system used by foreign government agencies, standard organizations, and commercial companies. It is necessary to consider the evaluation system suitable for the domestic environment instead of reflecting the overseas evaluation system as it is.

The purpose of this study is as follows. First, we will present the problems of the existing information security assessment system and the improvement direction of the information security assessment system through analysis of existing information security assessment system. Second, it analyzes the technical guidance for information security testing and assessment and the evaluation of information security management in the Special Publication 800-115 'Technical Guide to Information Security Testing and Assessment' of the National Institute of Standards and Technology (NIST). Third, we will build a framework to implement the evidence collection system and present a system implementation method for the '6. Information System Security' of 'information security management actual condition evaluation index'.

The implications of the framework development through this study are as follows. It can be expected that the security status of the enterprises will be improved by constructing the evidence collection system that can collect the collected evidence from the existing situation assessment. In addition, it is possible to systematically assess the actual status of information security through the establishment of the evidence collection system and to improve the efficiency of the evaluation. Therefore, the management system for evaluating the actual situation can reduce the work burden and improve the efficiency of evaluation.

Keywords : Evidence Collection System, IS Management, IS Assessment, Evaluation of IS

Received : 2019. 07. 04. Final Acceptance : 2019. 10. 31.

* College of Business and Economics, Chung-Ang University, e-mail : mgchoi@cau.ac.kr
** Corresponding Author, Professor of MIS, College of Business Administration and Economics Chung-Ang University, 84 Heukseok-ro, Dongjak-gu, Seoul, 06974, Korea, Tel : +82-2-820-5555, e-mail : smkang@cau.ac.kr
*** Department of Business Administration, Chung-Ang University, e-mail : ejlm2000@hanmail.net

1. Introduction

As the contents of evaluation of information security (IS) management in recent years become more diverse and complicated, the contents and procedure of the evidence to prepare for actual assessment are rapidly increasing. As a result, the actual assessment is a burden for both evaluation agencies and evaluation institutions.

In the case of the United States, it collects evidence at all times using automated tools such as SCAP and Cyberscope. The automation tool enhances the efficiency of work and relieves the burden of evaluating agencies and evaluation institutions. US automation tools are efficient and convenient, but they are difficult to apply to Korea. The federal government provides automated support tools for FISMA operations to each agency. In conjunction with the federal agency's information system, it automatically collects information security status during work, simplifying the preparation for evaluation. SCAP, which automatically detects vulnerabilities and CyberScope are data collection tool for reporting. CyberScope is an automated online data collection tool for FISMA reporting, and OMB was distributed to each government agency in October 2009. We have established an effective and efficient reporting system that is more efficient than conventional passive data collection methods through online data access with extensive data collection and two-factor authentication. Language type is the same XML method as SCAP, and NIST provides Schema for interworking with SCAP. CyberScope automatically collects data on FISMA compliance from the organization's information system. CyberScope automatically converts the organization's business data into SCAP-based metadata (CVE, CCE, CPE, CVSS) and then generates reports that can be used to assess the vulnerability.

In Korea, several reports have been made on how to strengthen the self-evaluation of information security management. However, most of them reflect the evaluation system used by foreign government agencies, standard organizations, and commercial companies. It is necessary to consider the evaluation system suitable for the domestic environment instead of reflecting the overseas evaluation system as it is.

In order to enhance the self-evaluation, it is necessary to analyze NIST's Special Publication 800-115 'Technical Guide to Information Security Testing and Assessment: Technical Guidance for Information Security Testing and Evaluation'. 'SP 800-115' was developed to provide technical information security testing and evaluation of organizations and to provide guidelines for planning, analysis, discovery and mitigation strategies development. 'SP 800-115' is not intended to present an evaluation program or an integrated information security test, but rather present an overview of the key elements for testing and evaluating, focusing on specific technologies, advantages and limitations, and requirements for use.

It verifies compliance with policies or other requirements and provides practical recommendations for designing, implementing and maintaining technical information related to procedures and evaluation procedures and security tests that can be used for various purposes, such as finding vulnerabilities in systems or networks. Therefore, you should refer to this document to possibly configure and actualize the evidence collection system framework for information that can be collected by automated systems such as electronic documents, log records, computer policies, system configuration values, network diagrams, and file security status.

In case of evaluation item related to system security among 'Information security management actual condition evaluation index,' it can be replaced with a system that can collect and automate system log records and agents in real time. Therefore, we propose a framework for creating evaluation automation design tool by collecting system log records, agents, and other data in real time. This framework aims to provide documentation on the architectural and subcritical requirements. Ultimately, this study is expected to improve the efficiency of evaluation by developing a framework for analyzing technical guidance on existing information security testing and evaluation and establishing a data collection system for assessing the actual condition of information security management for domestic environments.

The purpose of this study is as follows. First, we will present the problems of the existing information security assessment system and the improvement direction of the information security assessment system through analysis of existing information security assessment system. Second, it analyzes the technical guidance for information security testing and assessment and the evaluation of information security management in the Special Publication 800-115 'Technical Guide to Information Security Testing and Assessment' of the National Institute of Standards and Technology (NIST). Third, we will build a framework to implement the evidence collection system and present a system implementation method for the '6. Information System Security' of 'information security management actual condition evaluation index'.

The composition of this study is as follows. Chapter 1 explains the necessity and purpose of this study. In chapter 2, the outline of the existing information security assessment, problems, and improvement directions are explained. Chapter 3 presents the framework of the evidence collection system as an alternative to the existing information security assessment. Chapter 4 analyzes the necessary skills and functions at each stage of the framework presented. In chapter 5, we propose a method to implement system by item in information system security. Chapter 6 presents the implications and limitations of this study.

2. Analysis of Existing Information Security Situation

The national information security management status evaluation in Korea is determined annually by the National Intelligence Service, and it is notified to the target organizations, and the evaluation cost and standard are applied to the revised and complementary evaluation after reflecting the change of the information security environment and the latest cyber threat situation. The existing information security situation assessment is divided into five stages: (1) self-assessment by organization, (2) on-site inspection, (3) analysis of results and score calculation, (4) review and approval of evaluation results, (5) notification of evaluation result.

Existing condition evaluation system reflects the actual condition of security management in the evaluation score in order to strengthen evaluation system focusing on on-site inspection such as diagnosis of system vulnerabilities and checking of security documents than verification and confirmation of supporting documents. In addition, it has the advantage that it can evaluate the score by importance by assigning the key evaluation items (five) and weighted items (ten) by applying different weightings to the evaluation items. The final evaluation score is calculated by summing the field survey scored based on the evaluation index and the self-evaluation non-evaluation (deduction) and effort to improve the complementary level (dead point).

The existing information security situation assessment system is divided into five stages (① self-assessment by organization, ② site survey, ③ analysis of results and score calculation, ④ deliberation and evaluation of evaluation result, and ⑤ notification of evaluation result). There are some problems in existing information security assessment.

First, there is too much evidence to prepare before the on-site inspection. The process of preparing the evidence in the evaluation of the information security situation leads to workload and workload for both the due diligence team and the evaluation target organization. The evaluation institutions are making efforts to match the format of the supporting documents in accordance with the actual evaluation period rather than increasing the actual security status. The evaluation agency may have a problem about the scope of the evaluation and the result of the inspection depends on the equity. In addition, most of the time and effort are spent because the actual evaluation is done manually. Second, the evidence required by (Information Security Management Index) is not systematically collected, categorized, or stored. Third, the preparation of evidence is ready for on-site assessment rather than for information security management at all times. Fourth, the existing information security assessment is repeatedly and manually recorded (written), which makes it difficult to make an objective judgment in the evaluation and it may be difficult to make a quantitative comparison. This makes it difficult to make objective comparisons at the time of field inspection, and thus it can be detected according to the circumstances.

If these problems are remedied, it will be possible for organizations of all levels to systematically perform information security tasks, to improve the level of information security and to secure national cyber security.

3. Evidence Collection System Framework Overview

In case of evaluation item related to 'system security' in order to supplement the problems of the existing evaluation system in accordance with the domestic environment, evidence can be replaced with system log of the relevant institution. Chapter 6, 'Information System Security' in 'Information Security Management Status Indicator', consists of evaluation items related to system security. Therefore, this study aims to develop integrated manual and a standard for policy implementation to implement items that can be implemented in the system by dividing the items into that can be evaluated in person by the appraisers' team and that can be implemented by the system automatically.

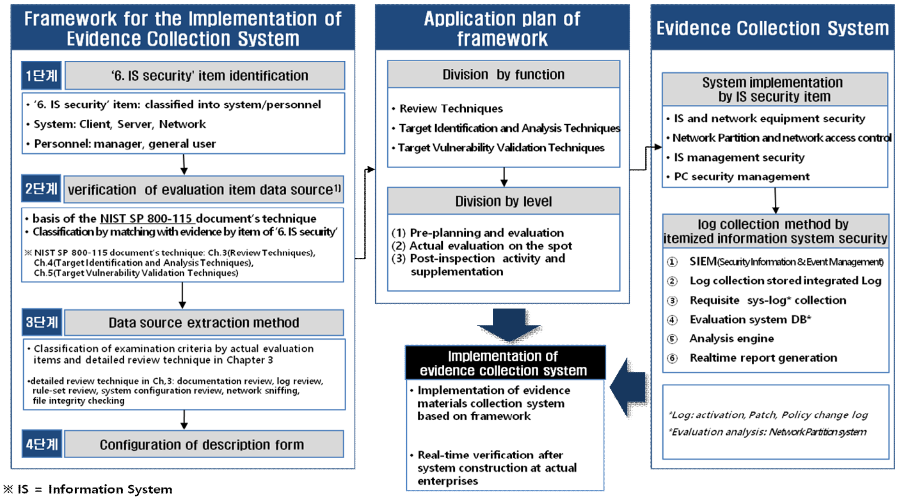
By constructing a system that can automatically collect and collect the collected evidence, it is expected that it will increase the security status of the company at all times and reduce the burden on both the due diligence team and the evaluation subject. This has the advantage that the evaluation of information security can be more systematic and the efficiency of evaluation can be improved. Therefore, we intend to build an automation system evaluation system framework to reduce the burden of work and increase the efficiency of evaluation. It includes required

〈Table 1〉 Evaluation Index Classification of Information Security Management Actual Condition

Category (Number of Items)	Evaluation Index	#of Indicators	Rating (Points)	
			Sector	
1. Information Security Policy (11)	1.1 Information security basic activities	6	8	19
	1.2 Information security organization and budget	3	9	
	1.3 Affiliate · affiliate security management	2	2	
2. Information Asset Security Management (12)	2.1 Introduction and management of information system	8	10	14
	2.2 National security system and media management	4	4	
3. Personnel Security (17)	3.1 Information security education	4	4	17
	3.2 Information technology business security management	13	13	
4. Cyber Crisis Management (10)	4.1 Cyber crisis response activities	4	4	12
	4.2 Cyber crisis response training	3	3	
	4.3 Understand the staff cyber crisis response procedures	3	5	
5. Electronic Information Security (10)	5.1 Electronic information leakage prevention measures	6	9	13
	5.2 User authentication	4	4	
6. Information System Security (20)	6.1 Information security system and network equipment security	3	4	25
	6.2 Network separation and network access control	6	10	
	6.3 Information system operation security	7	7	
	6.4 PC security management	4	4	
Total	16 indices	80	100	

technical manuals by details items and architecture by presenting the framework for building the evaluation automation design tool. In addition, the system implementation method of information system security is further explained to improve the efficiency of information security assessment on information system security (Review Techniques, Target Identification and Analysis Techniques, and Target Vulnerability Validation Techniques). 〈Table 1〉 shows the evaluation index classification of the 'Information Security Management Status Assessment Manual'.

The management framework for evaluating the management status of this study is shown in 〈Figure 1〉.


Framework for the Implementation of Evidence Collection System
1단계
'6. IS security' item identification
• '6. IS security' item: classified into system/personnel
• System: Client, Server, Network
• Personnel: manager, general user
2단계
verification of evaluation item data source1)
• basis of the NIST SP 800-115 document's technique
• Classification by matching with evidence by item of '6. IS security'
※ NIST SP 800-115 document's technique: Ch.3(Review Techniques), Ch.4(Target Identification and Analysis Techniques), Ch.5(Target Vulnerability Validation Techniques)
3단계
Data source extraction method
• Classification of examination criteria by actual evaluation items and detailed review technique in Chapter 3
•detailed review technique in Ch,3: documentation review, log review, rule-set review, system configuration review, network sniffing, file integrity checking
4단계
Configuration of description form
Application plan of framework
Division by function
• Review Techniques
• Target Identification and Analysis Techniques
• Target Vulnerability Validation Techniques
Division by level
(1) Pre-planning and evaluation
(2) Actual evaluation on the spot
(3) Post-inspection activity and supplementation
Implementation of evidence collection system
• Implementation of evidence materials collection system based on framework
• Real-time verification after system construction at actual enterprises
Evidence Collection System
System implementation by IS security item
• IS and network equipment security
• Network Partition and network access control
• IS management security
• PC security management
log collection method by itemized information system security
① SIEM(Security Information & Event Management)
② Log collection stored integrated Log
③ Requisite sys-log* collection
④ Evaluation system DB*
⑤ Analysis engine
⑥ Realtime report generation
*Log: activation, Patch, Policy change log
*Evaluation analysis: NetworkPartition system

※ IS = Information System
1) refer to the classified table

〈Figure 1〉 Automation Framework of Management Practices Assessment

4. Framework Analysis: Step-by-Step

The first step in the Evidence Collection System framework is to divide the items that can be evaluated by the due diligence team and implemented in the system in Chapter 6, 'Information System Security'. We will classify the items that can systemize the 'Information System Security' part of (Sector 6) among the evaluation indicators of the 'Information Security Management Status Assessment Manual' and build it as an automation system. Information systems are largely classified into 6.1 Information protection system and network equipment security, 6.2 Network separation and network access control, 6.3 Information system operation security, and 6.4 PC security management.

Next, identify the contents and requirements of each category by technology and stage. Classification by technology includes review technology, object identification and analysis technique, and target vulnerability verification technique.

① Identification of information system security item: It is divided into system (client, server, and network) and person (administrator, general user).

② Evaluation items Confirmation of data source: review techniques, target identification and analysis techniques, target vulnerability validation techniques

③ Data source extraction method: Detailed review technology (documentation review, log review, rule set review, system configuration review, network sniffing, file integrity checking)

First, Review Techniques are used to assess systems, applications, networks, policies and procedures, to detect vulnerabilities, and are typically performed manually. Documents, logs, ruleset, system configuration review, network sniffing, and file integrity checking.

Second, Target Identification and Analysis Techniques can identify systems, ports, services, and potential vulnerabilities and are performed passively, but are typically performed using automated tools. This technique is included Network discovery, network port and service identification, vulnerability scanning, wireless scanning, and application security checks.

<Table 2> Review Techniques

Technology	Function
Documentation Review	• Evaluates policies and procedures for technical accuracy and completeness
Log Review	• Provides historical information on system use, configuration, and modification • Could reveal potential problems and policy deviations
Ruleset Review	• Reveals holes in ruleset-based security controls
System Configuration Review	• Evaluates the strength of system configuration • Validates that systems are configured in accordance with hardening policy
Network Sniffing	• Monitors network traffic on the local segment to capture information such as active systems, operating systems, communication protocols, services, and applications • Verifies encryption of communications
File Integrity Checking	• Identifies changes to important files; can also identify certain forms of unwanted files, such as well-known attacker tools

〈Table 3〉 Target Identification and Analysis Techniques

Technique	Function
Network Discovery	• Discovers active devices • Identifies communication paths and facilitates determination of network architectures
Network Port and Service Identification	• Discovers active devices • Discovers open ports and associated services/applications
Vulnerability Scanning	• Identifies hosts and open ports • Identifies known vulnerabilities (note: has high false positive rates) • Often provides advice on mitigating discovered vulnerabilities
Wireless Scanning	• Identifies unauthorized wireless devices within range of the scanners • Discovers wireless signals outside of an organization's perimeter • Detects potential backdoors and other security violations

〈Table 4〉 Target Vulnerability Validation Techniques

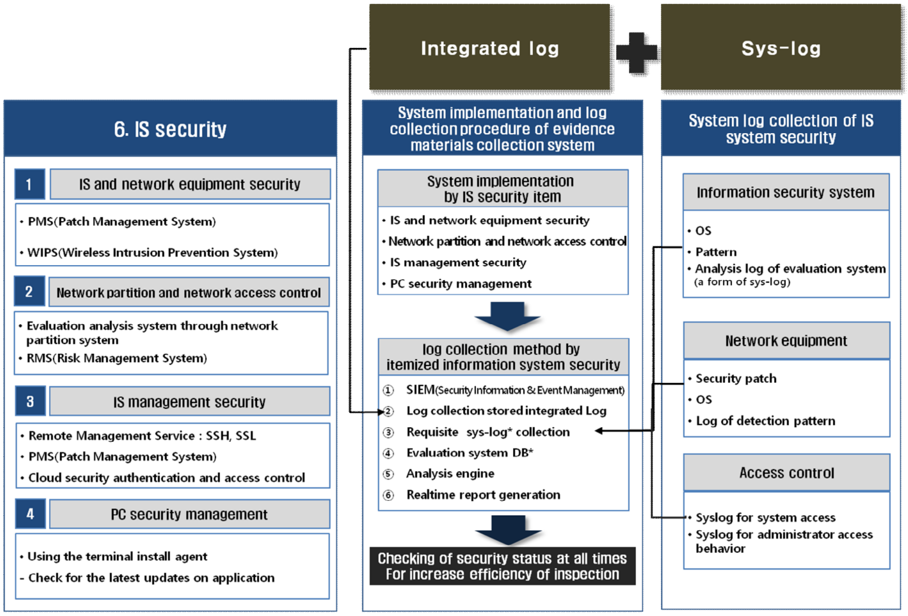
Technique	Function
Password Cracking	• Identifies weak passwords and password policies
Penetration Testing	• Tests security using the same methodologies and tools that attackers employ • Verifies vulnerabilities • Demonstrates how vulnerabilities can be exploited iteratively to gain greater access
Social Engineering	• Allows testing of both procedures and the human element (user awareness)

Third, Target Vulnerability Validation Techniques can be performed using automated tools or manually, depending on the specific technology used and the skill of the test team, and confirm the existence of vulnerabilities. Target vulnerability verification includes password cracking, penetration testing, social engineering, and application security testing.

The stages are divided into pre-evaluation stage, evaluation implementation stage, and post evaluation stage. We present the requirements for each technology and try to improve the security environment by reflecting the advance and post evaluation stages in actual work. We will build an automated system by classifying the evidence collection system into system implementation and log collection method of information system security. The required event logs are collected by the evaluation system, and the analysis results from the analysis engine are generated as a report, and the necessary logs include start, patch, and policy change history logs.

In 〈Figure 2〉, the main purpose of the evidence collection system is system implementation and log collection to automate security checks. In order to construct the framework of the evidence collection system, we developed a framework for the system that collects and automates the log (integrated log, syslog) and agent through the integrated log in real time, and we also design log automation collection method development and analysis engine of automation management check tool.

The methodology of the evidence collection system is as follows. First, the log related to the management status check item in the integrated log is brought to the evaluation system (analysis engine) and analyzed. Second, there is a method of receiving the syslog which is needed when an event occurs and analyzing it through an analysis algorithm (evaluation system) adapted to the security evaluation item. The system collects necessary syslog information for information protection system, network equipment and access control, analyzes the collected logs through


Integrated log
Sys-log
6. IS security
1 IS and network equipment security
• PMS(Patch Management System)
• WIPS(Wireless Intrusion Prevention System)
2 Network partition and network access control
• Evaluation analysis system through network partition system
• RMS(Risk Management System)
3 IS management security
• Remote Management Service : SSH, SSL
• PMS(Patch Management System)
• Cloud security authentication and access control
4 PC security management
• Using the terminal install agent
- Check for the latest updates on application
System implementation and log collection procedure of evidence materials collection system
System implementation by IS security item
• IS and network equipment security
• Network partition and network access control
• IS management security
• PC security management
log collection method by itemized information system security
① SIEM(Security Information & Event Management)
② Log collection stored integrated Log
③ Requisite sys-log* collection
④ Evaluation system DB*
⑤ Analysis engine
⑥ Realtime report generation
Checking of security status at all times
For increase efficiency of inspection
System log collection of IS system security
Information security system
• OS
• Pattern
• Analysis log of evaluation system
(a form of sys-log)
Network equipment
• Security patch
• OS
• Log of detection pattern
Access control
• Syslog for system access
• Syslog for administrator access behavior

〈Figure 2〉 System Implementation and Log Collection Plan of Evidence Collection System

the evaluation system (security audit system), and generates the report with analyzed contents. Third, there is a way to build an agent. There is a prerequisite that agents should be planted for each equipment. However, this is almost impossible and there are risks. There is also a problem that it may be too dependent on the agent.

Therefore, in this study, the log collection method to implement the evidence data collection system is used in this study by combining the integrated log and the syslog. The integrated log is mostly used by each institution, but it does not have an analysis engine, it only collects and stores logs, and practically does not use analysis and management. In addition, there is a limitation that the scope of the integrated log is limited to the server and some networks.

Therefore, we want to collect the necessary logs by using the integrated log used by most institutions. However, since the scope of the integrated log is limited to the server and some networks, logs that can't be collected by the integrated log are collected through Syslog and analyzed and managed by the analysis engine.

The log collection of information system security can be broadly classified into the following.

(1) Information protection system: analysis log of OS, pattern, evaluation system (syslog form)
(2) Network equipment: logs of security patches, OS, detection patterns
(3) Access control: syslog for system access, syslog for administrator access behavior,

Therefore, the security audit passes through the security audit system through the server, PC, and network equipment based on the above classification. The logs collected here are stored in the analysis engine and analyzed in conjunction with the UI (dashboard) and the integrated log.

5. System Implementation Method by Security Item of Information System

We analyze system implementation method by item to implement evidence collection system about the 6. Information System Security of 'information security management actual condition evaluation index'. The evaluation index of information system security is divided into four as shown in 〈Table 1〉.

The method for implementing information system security as a system has been described for each item. First, the items that can be automated are classified into 'automation' (9), 'partial automation' (4), and 'no automation solution' (7). 〈Table 5〉 shows the solutions according to the information system classification and evaluation items.

〈Table 5〉 Classification and Solution of Information System Security by Item

Information System Classification	Evaluation Index	Automation Identification and Solution
6.1 Information Security Systems and Network Equipment Security	6.1.1 Do you periodically check and update the access control policies of information protection systems and network equipment and update the detection patterns and security patches to the latest?	〔Partial automation〕 1. Automatic (SA): Periodic information protection system IP and Port scanning result secured 2. Manual: Check the date of the security patch. Registration (Internal)
	6.1.2 Has the Vaccine and Patch Management Server been deployed and addressed the security vulnerabilities identified?	〔Partial automation〕 1. Automatic (SA): patch management server IP registration, port scan, linkage collection of date of update by type, etc., history management 2. Automatic (DA): Collection comparison, including vaccine update date - Vulnerability check script for the subject - Vaccine and patch management server security status and security check measures The result should not only identify the vulnerability check port - Check that the vaccine and patch management server is secure against hacking - Check that unauthorized ports are not open
	6.1.3 Have you reviewed the security of your wireless LAN and have implemented security measures accordingly?	〔No automation solution〕
6.2 Network Separation and Network Access Control	6.2.1 Is the business network separated from the Internet?	〔Partial automation〕 o Proposed IP band scanning (url, IP (port)) o Check if network disconnect works properly √ Physical network separation: can be confirmed by exchange √ Separation of Logical Network: Network isolation check with MAC address in addition to IP - Make sure you are working with remote control systems, windows, etc. - Checking with existing document can be confirmed by scanning guide etc. - IP can be checked by inserting - Because the IP bandwidth is different, check the PIN to see if the ID and password reach the network band PIN
	6.2.2. Do you perform network disconnection and check periodically for network disconnection violations?	〔Automation〕 o Periodic confirmation and call record of IP access attempts such as usb, wifi, bluetooth, usage record, printer, etc. to terminal agent o Confirm the agent Bluetooth driver √ Separation of physical network: Confirm by interchanging √ Logical network separation: Switch (judged by network) - Periodic scanning check - Check periodically by bandwidth division (*check unregistered MAC address) (1) Wi-Fi tethering check (2) Check by changing Bluetooth tethering network ⇒ Check whether there is a standard for performing and preventing actual inspection. * Confirmation of P-rating agency's efforts with scanner and IP

〈Table 5〉 Classification and Solution of Information System Security by Item (Continue)

Information System Classification	Evaluation Index	Automation Identification and Solution
	6.2.3 In the case of a network separation institution, is it prohibited to install the document editing program on the internet PC and save the business data and restrict access to the online document editing service?	〔Automation〕 1. Definition of representative document editing program list - Editing program installation and execution trace check (Server/PC Sampling) - Check for blocking measures and methods such as Word, Hangul, online document editing program (Google Docs, Office 365, Notepad, etc.) 2. Contrast the known document editing process list 3. Edit the known document editing web page list 4. Checking operation status such as installed data storage prevention solution
	6.2.4 Do you establish and enforce security measures for secure data transmission between network and Internet?	〔No automation solution〕
	6.2.5 Do you block the use of bypassing information networks through unauthorized wired / wireless Internet (Wibro, HSDPA, smart phone tethering, etc.) within the organization?	〔Automation〕 o Confirmation of use of bypass information network by PC log check: Attempt detection and log acquisition with terminal agent
	6.2.6 Do you block unauthorized PCs, notebooks, etc. when connecting to the information network?	〔Automation〕 o Confirm blocking through unauthorized IP and MAC combination session connection attempts o Inspect network equipment for unauthorized PC / laptop connection 1. Check that Network Access Control (NAC) functions properly - NAC authorization and access control ⇒ Check the NAC check results (eg., build a list DB, etc.) 2. Check the scanner - Verify by mapping IP and MAC address in addition to NAC
6.3 Information System Operation Security	6.3.1 Do you use the information system remote management service safely?	〔Automation〕 1. Automate access attempts after securing unregistered administrator IP+MAC 2. Automate access attempts of telnet, #22, rlogin, rsh, rcp, and ftp with information of registered administrator
	6.3.2 Does the information system control the service port?	〔Partial automation〕 o Automate port access attempts o No need for service port information per server
	6.3.3 Has the OS (Windows Server 2003, etc.) with security support been stopped replaced?	〔No automation solution〕
	6.3.4 Do you manage passwords for information systems?	〔No automation solution〕
	6.3.5 When using Internet telephony Is Internet telephone network and general network separated and security measures performed?	〔No automation solution〕
	6.3.6 When implementing cloud computing, have you completed security review and implemented security measures based on security review at the stage of business planning?	〔No automation solution〕
	6.3.6 Do you control access to critical systems that make up the cloud?	〔No automation solution〕
6.4 PC Security Management	6.4.1 Do you carry out security management for terminal such as PC and notebook?	〔Automation〕 Information collection through terminal agent
	6.4.2 Do you perform the latest update on the target operating system of PC, notebook, etc.?	〔Automation〕 Log collection such as update date through terminal agent
	6.4.3 Do you carry out the inspection more than once a month with the vaccine program applying the latest update of PC, notebook, etc.?	〔Automation〕 Ability to collect logs such as execution date, time, etc. through terminal agent
	6.4.4 Do you perform the latest updates on your device target applications (Internet Explorer, document editing programs, plug-ins, etc.) such as PCs and laptops?	〔Automation〕 Update record performed by target program selection terminal agent

6. Conclusion

In recent years, the process of preparing evidence in the evaluation of information security has become a burden for both evaluation agencies and institutions receiving assessments. In the case of the United States, the SCAP, Cyberscope, and other automated tools are used to collect the evidence, but the evaluation environment differs from that of the domestic environment. Therefore, in this study, we developed a framework for the implementation of the evidence collection system for the evaluation of the actual situation of information security management in Korea. In the case of evaluation items related to system security among (Information Security Management Actual Condition Evaluation Index), it can be replaced with a system that can automate the real-time collection through the system log record and agent of the relevant institution. Therefore, it presents a framework for creating evaluation automation design tools, and provides documentation on the architectural and subcritical requirements.

In order to build a framework for implementing the evidence system of information security management, we implement the '6. Information System Security' part of the evaluation index. First, we distinguish between people (general staff, manager) and systems (network, client, server). Next, the source of the evaluation item data is confirmed and a classification table is presented. Based on the techniques (Review Techniques, Target Identification and Analysis Techniques, Target Vulnerability Validation Techniques) of NIST SP 800-115 document, it is classified according to the itemized evidence of '6. Information System Security'. The method of extracting data sources is categorized into Chapter 3: Detailed Review Techniques (Documentation Review, Log Review, Ruleset Review, System Configuration Review, Network Sniffing, and File Integrity Checking) of NIST SP 800-115 document and evaluation criteria for each item. Expression style consists of user interface.

Information system security items are divided into system implementation method and log collection method, and a method for implementing each item as a system and a method of collecting logs are described. This framework collects necessary logs when event occurs with Security Information and Event Management (SIEM) and analyzes the collected logs through analysis system DB. Also, it can improve the utilization of evidence data collection system by using integrated log. To do this, we distinguish between logs that can be used in the integrated log and those that can't be used. Logs that can't be collected from the consolidated log are analyzed through the syslog.

The implications of the framework development through this study are as follows. It can be expected that the security status of the enterprises will be improved by constructing the evidence collection system that can collect the collected evidence from the existing situation assessment. In addition, it is possible to systematically assess the actual status of information security through the establishment of the evidence collection system and to improve the efficiency of the evaluation. Therefore, the management system for evaluating the actual situation can reduce the work burden and improve the efficiency of evaluation.

The limitations of this study are as follows. First, this framework is built on the evaluation of information security situation in Korea. Therefore, there is a limitation that it is difficult to generalize in all other countries. Future studies will need to develop a framework that can be generalized in other countries. Second, we proposed an alternative method to automate information system security. It does not offer an alternative for items that do not have an automation solution. Therefore, in future research, it is possible to consider methods to automate existing information system security items by considering items without automation method. Thirdly, this study is to analyze 'Information Security Management Status Indicator' among '6. Information System Security'. Future researches need to implement evidence collection system for information security policy, information asset security management, personnel security, cyber crisis management, and electronic information security.

References

〔1〕 Bahsi, H., "Analysis of National Cyber Situational Awareness Practices", *Strategic Cyber Defense: A Multidisciplinary Perspective*, Vol. 48, 2017, pp. 31-41.

〔2〕 FIPS, PUB 199, 'Standards for Security Categorization of Federal Information and Information Systems', February 2004.

〔3〕 FISMA, Section 3544.

〔4〕 Gikas, C., A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards", *Information Security Journal: A Global Perspective*, Vol. 19, No. 3, 2010, pp. 132-141.

〔5〕 Hulitt, E. and Vaughn, R. B., "Information system security compliance to FISMA standard: a quantitative measure", *Telecommunication Systems*, Vol. 45, No. 2-3, 2010, pp. 139-152.

〔6〕 Miller, D., Harris, S., Harper, A., VanDyke, S., and Blask, C., Security information and event management (SIEM) implementation, McGraw Hill Professional, 2010.

〔7〕 NIST, Special Publication 800-37, 'Guide for the Security Certification and Accreditation of Federal Information Systems', Section 3.4. May 2004.

〔8〕 NIST, Special Publication 800-53 'Guide for Assessing the Security Controls in Federal Information Systems' Ver. 4, February 2014.

〔9〕 NIST, Special Publication 800-115 'Technical Guide to Information Security Testing and Assessment', September 2008.

〔10〕 National Intelligence Service, 2016 National and Public Sector, "Explanation of Indicators of Information Security Management Status Indicators", 2016.

〔11〕 Rouillard, J. P., Real-time Log File Analysis Using the Simple Event Correlator (SEC), In LISA, 4, 2004, pp. 133-150.

Author Profile

Dr. Myeonggil Choi

He earned Ph.D. at KAIST (Korea Advanced Institute of Science and Technology). and has researched in the information security and IT Business Entrepreneurship. He currently served an full professor in the department of Business Administration, at Chung-Ang University, Seoul. His paper appeared in Government Information Quarterly (GIQ), International Journal of Information and Management (IJIM), International Journal of Entrepreneurial Behaviour & Research.

Sungmin Kang

Sungmin Kang is a professor of MIS at College of Business and Economics, Chung-Ang University, Seoul, Korea (ROK). He earned his B.S. and MBA in business administration from Carnegie Mellon University. He also received his Ph.D. in information systems from the University of Texas at Austin. His research interests include the electronic commerce, information security, knowledge management, mobile computing, and organizational impact of information technologies. He has published related papers in domestic and foreign journals and conference proceedings.

Eunju Park

Eunju Park is a Ph.D. Candidate in Department of Business Administration of Chung-Ang University. She has received master's degree in Department of Business Administration of Chung-Ang University. Her major research areas include Business Management, Management Information System, Security, Information security, Entrepreneurship.