Improvement of Guideline for Infrastructure Security

Jin Yong Park and Tae-Sung Kim

April 29, 2024

Improvement ways of guideline for infrastructure security

Completed Research Paper

Abstract

The information security of critical infrastructure is very important because it is connected to the safety and lives of the people, and a successful cyber-attack can cause catastrophic damage. According to Korean laws, all infrastructures were required to confirm the implementation of infrastructure security plans at least once a year. However, the guideline for checking the implementation of infrastructure security plans has problems such as not being suitable for infrastructures that use special systems. This study aims to identify the problems in the structure, check items, and scoring of the guideline, and seek solutions through defining principles and interviewing with infrastructure operators and security experts. The results of this study can be used to efficiently conduct security vulnerability checks and implementation checks of critical infrastructure, and the improved guideline was expected to contribute to the improvement of security levels.

Keywords: Critical IT infrastructure Security, Security countermeasure, Criteria for checking compliance, Analytic hierarchy process

Introduction

Advances in information and communication technologies are rapidly driving the digital transformation and automation of workplaces across all industries. As a result, threats such as spear-phishing and ransomware are also increasing. Infrastructures that were previously managed by being physically isolated from external networks have also begun to be exposed to spear-phishing and ransomware as information systems are introduced. Attacks targeting infrastructure, such as Industroyer, which attacked the Ukrainian power grid in December 2016 and caused a blackout, and Conti ransomware, which targeted wind turbine company Nordex, are gradually increasing (Idaho National Laboratory, 2018; Kaspersky ICS CERT, 2022). As critical infrastructures are directly related to the safety and lives of people, such as electricity, hydropower, gas, and transportation, information system security is becoming increasingly important as accidents can cause catastrophic problems for the entire society. According to the Korean law on information security, all infrastructures are required to check the compliance of infrastructure security plans at least once a year to protect infrastructure from threats (Article 5).

However, the guideline, which was designed to check whether infrastructure security plans have been implemented, has problems. First, there were duplicate check items. Secondly, the arrangement of the check items was not appropriate. Third, the gap between the score of the check items was not objective. Last, it was not suitable for infrastructures that use unique systems.

This study identified these problems by comparing with Korean standards and guidelines on information security. To solve the identified problems, we defined principles and improved the guideline by adapting the principles. After improved guideline, we validated the improved guideline through interviews with infrastructure operators and experts who have experience securing infrastructure. Last, we used AHP to derive the relative importance of the checked items and assign score according to importance.

The results of this study can be used to efficiently check critical infrastructure for security vulnerabilities and verify their compliance of infrastructure security plans, and the guideline can be improved through feedback from infrastructure and security experts in various fields to contribute to improving security levels.

Literature reviews

Critical infrastructure

Critical infrastructure was a facility that can have a significant impact on the national economy, the safety and health of the people, and the core functions of the government, such as energy, information and communication technology, transport, and healthcare.

In Korea, there are 143 management organizations under 11 main departments to manage 360 designated facilities (Ministry of the Interior and Safety). And the Korean law requires the establishment and implementation of information security plans to protect infrastructure (Article 5-2). In addition, cyber-attacks on critical infrastructure have been increasing as information systems have been installed in critical infrastructure due to the development of IT technology (Idaho National Laboratory, 2018; Kaspersky ICS CERT, 2022). Therefore, the National Institute of Standards and Technology (NIST) developed the guidelines to protect the operational and information systems of infrastructure (NIST, 2022).

Trends in information security standards for infrastructure

Korean information security standard

The Korean information security standard was aimed at regulating the basic tasks of information security for various government departments designated by the Korean government through the establishment of security countermeasures, operational and information system security plans. Recently, as of January 31, 2023, new provisions related to cloud computing have been added (Korean Government, 2023).

Guideline for critical infrastructure

Facilities designated as critical infrastructure were legally encouraged to check the compliance of infrastructure security plans at least once a year by the Korean law. The Korean Government released guideline to infrastructure to check compliance of infrastructure security plans annually.

The guideline was designed based on Korean information security standard and consisted of two fields, four areas, and 31 check items. The check items were applicable to all infrastructures and consisted of items to check essential requirements security that must be checked for infrastructure security. The check items were composed of four areas. First, the scoring criteria that indicates the results of the check items. Second, the fundamental policies that present the basis for checking the check items. Third, the evaluation criteria, which show the criteria for scoring points. Last, the documenting evidence that required for verification.

Security assessment

There are three main security assessments for critical infrastructure in Korea. First, security assessment for government and public institution, conducted by the Korean Government. Second, the personal information & information security management system (ISMS-P), conducted by the Korea Internet & Security Agency (KISA) (KISA, 2022). Last, Critical Infrastructure Vulnerability and Analysis Evaluation Standard, designed by the Ministry of Science and ICT (Ministry of Science and ICT, 2021). The security assessment conducted by the Korean government was designed to evaluate how government and public institution respond to cyber threats and assessed a total of 40 check items in three areas: administrative security, technical security, and crisis response.

The ISMS-P was a framework that grants certification after the certification agency evaluates that a series of measures and activities established by an organization to secure the stability of information and communication networks and protect personal information comply with certification standards. ISMS-P consisted of 102 certification criteria in three areas: 'Management System Establishment and Operation', 'Security Measures Requirements', and 'Personal Information Processing Requirements'. The Critical Infrastructure Vulnerability Analysis Evaluation Standard performed risk assessment that assigned risk rating to vulnerability check items for the stable operation of critical infrastructure. The check items of vulnerability analysis and assessment are divided into administrative, physical, and technical areas. It is divided into three levels (upper, middle, and lower) according to the risk of vulnerabilities, and the check items with level of "upper" are required to be checked once a year.

Analytic Hierarchy Process (AHP)

AHP is a multi-criteria decision-making model that systematically analyses the decision-making process and derives the relative weights of multiple evaluation items by pairwise comparison to support rational decision-making (Hee-Kyung et al., 2008). AHP shows a more detailed logical representation of each factor and the relationship between factors by hierarchizing the factors required for decision making. Unlike other decision-making methodologies, AHP measures the reliability of the survey responses based on the Consistency Ratio (CR), which shows whether the decision maker's responses are consistent across surveys. Saaty (1980) suggests that the value of the consistency ratio should generally be less than or equal to 0.1 for the survey responses to be considered consistent. However, some research in the social sciences allows for consistency ratios up to 0.2 due to the nature of the survey questions (Saaty and Luis, 1998).

Methodology

The Korean Government released guideline to infrastructure to check compliance of infrastructure security plans annually. The reason why the South Korean government releases the guidelines every year is due to the development of IT technology and the advancement of cyber-attacks, which requires revisions to ensure effective checks.

Due to frequent revisions, Guideline released by Korean Government has various problems. To solve the problems, this study will identify the problems comparing with standards and guidelines on information security. And we defined consistent principles to prevent problems caused by frequent guidelines revisions. Next, we improved guideline by adapting consistent principles. After improved guideline, we validated the improved guideline through interviews with infrastructure operators and experts who have experience securing infrastructure. During the interview, we used AHP to derive the relative importance of the check items. Last, we assigned score according to result of relative importance.

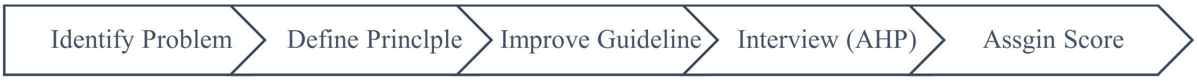

Figure 1. Research process

Result

Identify problem

To identify problems that exist in the guideline, the structure of the guideline, the check items, the fundamental policy within the check items, the evaluation criteria, and the documenting evidence were reviewed.

The structure of guideline was operation system field and information system field. Each field had administrative security area, system security area, personnel and asset security area, crisis response area. The number of check items was 31, which was the same for the operation system field and information system field. First, we reviewed the guideline’s check items, fundamental policy within the check items, evaluation criteria and documenting evidence to identify overlapping check items. There was one overlapping check item in operation system field, and two in the information system field. Operation system field was overlapping check item for vaccine update and information system field was overlapping check items for security measures related to network connectivity and blocking access to unauthorized devices. Next, to determine whether there are any missing or revised check items in the guidelines, we compared guideline with Table 1.

Type	Document	Revision
Standard	Korean information security standard	2023.01.
Security assessment	Critical infrastructure vulnerability and analysis evaluation standard	2021.03.
Security assessment	Personal information & information security management system	2022.04.

Table 1. Comparison document

Korean information security standard revised for cloud security on 31 January 2023, but guideline was not reflected due to concerns about whether cloud security is timely for applying to critical infrastructure. And result of comparison with security assessment, there were a lot of problems such as the guideline's check items and scoring criteria were not clearly explained, so the scoring criteria, evaluation criteria, etc. could be judged differently by different inspectors.

Through the review of guideline, the following problems were identified.

1. there were duplicate checks for the same item.
2. There were missing check items in the guideline compared to the standard and security assessment.
3. There were check items that inspect multiple targets in one check item.
4. the description of the check items and scoring criteria in the documentation was not clear and may be subject to the inspector's interpretation.
5. inconsistent scoring method of points such as selective and summative method.
6. There were check items that are not assigned points equitably.
7. There were check items that do not consider the situation (specificity) of critical infrastructure.

Define principle

To solve identified problems, we defined the principles as shown in Table 2 and improved the guideline based on the principles.

Application	Principle	Description	Problem
Check item	Do not Overlapping	Don't double-measure the same item	1
	Prevent missing	The content of the standards and security assessment must be included in the guideline	2
	Single target	There must be one target for each item	3
Scoring criteria	Clear criteria	Scoring criteria must be clear and valid	4
	Selective criteria	Do not use summative scoring criteria	5
	Distribute equitableness	Scoring point should be distributed equitably	6
	practicality	Scoring criteria must be practical	7

Table 2. Defining principles

Defined the principles had following effects. First, it prevents the inclusion of duplicate or missing content within the guideline. Second, it minimizes the subjective involvement of revisors and ensures consistency when revising the guideline. Third, it provides a revision process that can be utilized on a long-term basis rather than as a one-off exercise.

Improve guideline

The current guideline had four areas: administrative security, system security, personnel and asset security, and crisis response. But system area was not representative of the checked items, and the standard and security assessment were described as technical rather than system. So, it was deemed appropriate to change it to technical security area.

In addition, the personnel and asset security area was deleted because the check items included in the personnel and asset security area correspond to the administrative security area and technical security area. The check items that were included in the personnel and asset area was categorized and included in their respective areas. Finally, the improved guideline had 3 areas: administrative security, technical security, crisis response.

Interview with experts

We interviewed Infrastructure operators and experts with more than 10 years of experience in various fields such as energy, transport to review the improved guideline.

Infrastructure operators and experts mentioned 2 reviewed opinions. First, Selective criteria were harder to evaluate for security compliance efforts than summative criteria. Last, to ensure that clear and valid scoring criteria, essential requirements must be defined first.

After the reviewed the improved guideline, we conducted AHP with infrastructure operators and experts to measure the relative importance of the check items in the guideline.

Results of a two-week survey from September 20, 2023 to October 4, 2023, 11 out of 14 respondents had a consistency ratio less than 0.2, and there were no missing values among those with a consistency ratio less than 0.2. The consistency percentages of valid respondents in the operational systems field were 0, 0.008, 0.008, 0, 0, 0, 0.13, 0, 0, 0, 0, 0.008, 0.05. The consistency percentages of valid respondents in the information systems field were 0, 0.008, 0.008, 0, 0, 0, 0.13, 0, 0, 0, 0, 0.008, 0.05. In this study, we used the geometric mean to derive the relative importance of each check item to derive a unified collective opinion from a group of experts. The consistency ratio of the collective opinion was 0.004 for operational systems and 0.00001 for information systems, indicating that both fields had significant level of responses. Tables 3 and 4 showed the relative importance that experts considered the top criteria and the bottom criteria in the operational systems and information systems respectively.

There were two things to highlight from result of AHP. First, the relative importance of the top criteria in the operating system field was shown by technical security (0.363), administrative security (0.348), and crisis response (28.9). The relative importance of the top criteria in the information system field was shown by technical security (0.391), administrative security (0.351), and crisis response (0.257). In other words, the relative importance order of the top criteria was the same for both fields. It was shown that infrastructure operators and experts considered the technical security was the most important to protect infrastructure. Last, among the bottom criteria for each area, the first rank was human resource deployment (0.131) for administrative security area, network segmentation (0.11) for technical security area, and cyber crisis training (0.368) for crisis response in operation system field. Among the bottom criteria for each area, the first rank was human resource deployment (0.131) for administrative security area, network segmentation (0.093) for technical security area, and cyber crisis training (0.372) for crisis response in information system field. In other words, for each area, the most important check items for the bottom criteria were the same for both fields. It was shown that infrastructure operators and experts considered the human resource deployment for administrative security, network segmentation for technical security and cyber crisis training for crisis response were the most important to protect infrastructure.

Assign Score

The scoring points were based on the relative importance of the check items as calculated by result of AHP, which was considered more valid than current scoring. In addition, relative importance was appropriate because it reflected the current condition and the needs of the infrastructure. Therefore, we suggested to assign the scoring point based on Global relative importance of AHP result.

Top criteria	Relative importance	Bottom criteria	Relative importance	Global relative importance
Administrative security	0.348	A-1(Guidelines)	0.075	0.026
		A-2(Organization)	0.101	0.035
		A-3(Human resource deployment)	**0.131**	0.046
		A-4(Chief Executive Officer)	0.085	0.030
		A-5(Budget)	0.097	0.034
		A-6(Education)	0.061	0.021
		A-7(Asset management)	0.108	0.038
		A-8(Asset disposal)	0.059	0.021
		A-9(Security inspection for outsourcing)	0.102	0.035
		A-10(Violation measures of outsourcing)	0.089	0.031
		A-11(Risk analysis)	0.092	0.032
Technical security	0.363	B-1(Validation of security system)	0.054	0.020
		B-2(Network segmentation)	**0.110**	0.040
		B-3(Simplex communication)	0.105	0.038
		B-4(Access control management)	0.065	0.024
		B-5(Administrator account security)	0.068	0.025
		B-6(PC and server security management)	0.048	0.017
		B-7(Exceptional PC management)	0.050	0.018
		B-8(Vulnerability updates)	0.050	0.018
		B-9(Security patches)	0.047	0.017
		B-10(Anti-virus inspection)	0.050	0.018
		B-11(CCTV security management)	0.038	0.014
		B-12(Port sealing)	0.047	0.017
		B-13(Importable device management)	0.060	0.022
		B-14(Network segmentation of outsourcing)	0.075	0.027
		B-15(Access control management of outsourcing)	0.064	0.023
		B-16(Remote prohibition of outsourcing)	0.070	0.025
Crisis response	0.289	C-1(Cyber crisis training)	**0.368**	**0.106**
		C-2(Log management and time synchronization)	0.122	0.035
		C-3(Incident response system)	0.254	**0.073**
		C-4(Security inspection)	0.256	**0.074**

Table 3. Operation system field

Top criteria	Relative importance	Bottom criteria	Relative importance	Global relative importance
Adminis trative security	0.351	A-1(Guidelines)	0.080	0.028
		A-2(Organization)	0.103	0.036
		A-3(Human resource deployment)	**0.131**	0.046
		A-4(Chief Executive Officer)	0.087	0.031
		A-5(Budget)	0.096	0.034
		A-6(Education)	0.060	0.021
		A-7(Asset management)	0.104	0.037
		A-8(Asset disposal)	0.061	0.021
		A-9(Security inspection for outsourcing)	0.100	0.035
		A-10(Violation measures of outsourcing)	0.087	0.031
		A-11(Risk analysis)	0.090	0.032
Technical security	0.391	B-1(Network Segmentation)	**0.093**	0.036
		B-2(Network Segmentation Configuration)	0.068	0.027
		B-3(Data Transmission Security)	0.069	0.027
		B-4(Access control management)	0.065	0.025
		B-5(Account Authentication Measures)	0.056	0.022
		B-6(Account Access Management)	0.053	0.021
		B-7(Administrator Account Security)	0.059	0.023
		B-8(Data Leakage Prevention Measures)	0.058	0.023
		B-9(PC and Server Security)	0.050	0.020
		B-10(Security Patches)	0.049	0.019
		B-11(Antivirus Inspection)	0.052	0.020
		B-12(Antivirus and Patch Server Management)	0.054	0.021
		B-13(CCTV Security Management)	0.032	0.013
		B-14(portable Storage Management)	0.045	0.018
		B-15(Network segmentation of outsourcing)	0.073	0.029
		B-16(Access control management of outsourcing)	0.061	0.024
		B-17(Remote prohibition of outsourcing)	0.064	0.025
Crisis response	0.257	C-1(Cyber crisis training)	**0.372**	**0.096**
		C-2(Log management and time synchronization)	0.127	0.033
		C-3(Incident response system)	0.239	**0.061**
		C-4(Security inspection)	0.263	**0.068**

Table 4. Information system field

Conclusion

As the number of cyber-attacks against critical infrastructure increases, it was important to ensure that critical infrastructures had security plans to protect their infrastructures, and which were properly implemented.

In this study, we identified the problems by comparing standard and security assessments and defined the principles to solve the problems. Next, we applied the principles on the guideline and validated the guideline by interviewing infrastructure operators and experts in various fields. Finally, we suggested to assign the scoring points of check items based on result of AHP.

This study was contributed to following implications. First, by comparing standard and security assessment, identifying problems in guideline and defining principles to solve them, it can prevent redundant or missing content and maintain the consistency of the guideline. It also improved work efficiency because the defined principles were applicable for the long term, not just temporarily. Second, the guidelines were reviewed by experienced experts in various infrastructure fields to ensure their reliability and practicality. Finally, AHP was used to derive the relative importance of the check items in the guideline, which can be considered more valid than current scoring points.

However, there were limitations of this study. First, only Korean information security standards and security assessments were analyzed for improving guideline. Security for infrastructure should be considered international standards such as SP 800-82 of NIST, SOCs (Security Operation Centres) of NCSC. Second, the AHP survey was conducted to assign the scores, but the number of bottom criteria was not equitable, so the relative importance value was not valid. Last, the relative importance values were not valid because the check items had different check levels. For example, the check items for crisis management include check items for administrative security and technical security, so the relative importance was unbalanced.

References

Act On the Protection of Information and Communications Infrastructure Article 5 (Establishment of Measures to Protect Critical Information and Communications Infrastructure), 2022.09.

Act On the Protection of Information and Communications Infrastructure Article 5-2 (Verifying Implementation of Measures to Protect Critical Information and Communications Infrastructure), 2022.09.

Hee-Kyung Kong, Hyo-Jung Jun and Tae-Sung Kim. 2008. "A Study on Information Security Investment by the Analytic Hierarchy Process," Journal of Information Technology Applications & Management, vol. 15, no. 1, pp. 139-152.

Idaho National Laboratory. 2018. "Interaction Process Analysis: A Method for the Study of Small Groups," Cambridge, MA: Addison-Wesley.

Kaspersky ICS CERT. 2022. H1 2022-A Brief Overview of the Main Incidents in Industrial Cybersecurity.

KISA, Personal Information & Information Security Management System, 2022.04.

Korean Government, Korean information security standard, 2023.01.

Ministry of the Interior and Safety, Status of National Critical Infrastructure Designation, https://www.mois.go.kr/frt/sub/a06/b13/protectNationCoreFoundation/screen.do, accessed on 2023. 11. 01.

Ministry of Science and ICT, Criteria for analyzing and assessing ICT infrastructure vulnerabilities, 2021.03.

NIST, Guide to Operational Technology (OT), *NIST Special Publication, 800-23r3,* 2022. 04.

Saaty, T. L. 1980. "*The Analytic Hierarchy Process*," McGraw Hill, New York.

Saaty, T. L. and Luis, G. V. 1998. "Diagnosis with Dependent Symptoms: Bayes Theorem and the Analytic Hierarchy Process," *Operations Research*, vol. 46, no.4, pp. 491-502.