A Comparison of Information Security Certification Architectures

Seong-Kyu Kim*

*Assistant Professor (Tenure Track) of Department of Information Security, Joongbu University, Gyeonggi-do Goyang-Si 10279, Republic of Korea.

Department of Public Policy and Information Technology, Seoul National University of Science and Technology, Seoul 01811, Korea.(e-mail : skkim@joongbu.ac.kr or guitara77@gmail.com)

Jun-Ho Huh**

** Assistant Professor (Tenure Track) of Department of Data Informatics, (National) Korea Maritime and Ocean University, 727, Taejong-ro, Yeongdo-gu, Busan, Republic of Korea (e-mail : 72networks@pukyong.ac.kr or 72networks@kmou.ac.kr)

Abstract

This paper needs to have a standardized legal and management system as the development of AI, artificial intelligence, IOT, etc. developed through the 4th industrial era, and the use of personal information is increased in the era of global connection. Therefore, through this paper, I would like to compare and analyze the privacy management system in the U.S. and Korea, which emphasized technical protection measures, to find a more advanced direction of protection measures.

I. Introduction

In this paper, the growing importance of information security and personal information has led to an increase in crimes exploiting it. Previously, crimes for self-disclosure were prevalent, but as financial transactions through personal information became possible and the number of cases of personal privacy exposure increased, and more accidents caused corporate and individual damage due to personal mental damage, corporate image damage, and legal litigation costs [1].

To address these risks, countries have developed laws on privacy and management systems for privacy protection, and technologies to de-identify specific personal information to promote business activation have also developed. Global countries have enacted laws based on OECD 8 principles and protect personal information based on related laws, but as some different legal systems between countries have increased the number of cases of excessive fines on companies, global businesses have frequently been closed. It will be necessary to look at and operate this globalized personal information in various fields of view [2]. In this paper, we want to compare and analyze the operation method of personal information operated abroad compared to the US personal information management system, which leads the personal information management system, and find ways to expand and use Korea's personal information management system in global countries [3].

II. Related Work

Representative compliance and management systems related to information protection and personal information include HIPAA(Health Insurance Portability and Accountability), the US Privacy Framework CSF-P, the International Privacy Standards ISO27701, the European Union General Privacy Act GDPR(General Data Protection Regulation), and Korea's ISMS-P. The relevant management systems for personal information protection are structured based on laws enacted in each country. The basic principles of privacy in each country are mostly similar. However, there are some differences in the operation of the US and Korea's privacy management system, so we want to compare and analyze relevant protection items to find ways to improve privacy [4].

2.1. ICT and Cybersecurity Status

The International Telecommunications Union (ITU) compared ICT(Information & Communications Technology) development and cybersecurity indicators between countries through measurements of ICT development index (IDI) by weighting measurements such as Internet use, wired and wireless high-speed Internet subscribers, and ICT utilization. When comparing the ICT development index of the U.S. and South Korea[5], it can be confirmed that South Korea ranks second in the global ICT rankings, far superior to the U.S. It can be seen that South Korea is actively investing in network infrastructure and ICT businesses in global countries[6].

2.2. Understand of Cyber Security Framework

The United States issued the Cyber Security Framework (CSF) by President Obama in 2013 and NIST issued a final security framework and roadmap in response to cybersecurity threats to its major infrastructure, finance, health and energy, under executive order 13636. After February 12, 2014, the core areas were supplemented to implement an information security roadmap applicable to the marketplace by combining private, public and academic circles[7].

Initially, CSF version 1.0 established a framework to reduce the security risk of major national infrastructure, and on 16 April 2018, version 1.1 was revised to add protection measures for supply chains. CSF implements a life cycle with five functions: identification, protection, detection, response, and recovery, and guides the organization to select and perform targets appropriate to the organization's situation among four levels of partial response, risk information utilization, iterative action, and continuous improvement.

III. Information Security and Privacy Framework

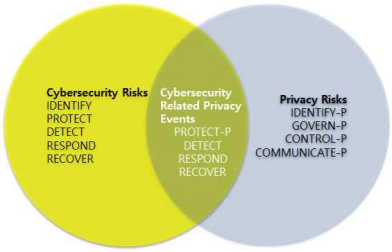
3.1. CSF

The CSF is structured in stages of systematic operations based on a set of information protection activities, from identification of assets to recovery, and is structured in a structure that is common to major infrastructures [8]. The basic security control of an organization is to establish policies, processes, and procedures to share the entire organization's activities with its members to operate and manage them systematically. CSF can operate and maintain

the five-step capabilities of identification, protection, detection, response, and recovery simultaneously or continuously, and can also perform high-level risk strategies through life cycles such as asset identification, evaluation, response and maintenance.

3.2. CSF-P

NIST (National Institute of Standards and Technology) has released PRIVACY FRAMEWORK through transparent and agreed-upon procedures, including private and public stakeholders, to encourage autonomous compliance with the privacy management system. It was used as a tool for personal information protection through risk management through the corporate privacy framework and developed into a technology for personal information protection for organizations and individuals. The privacy framework supports five functions. The five functions defined below, Identification-P, Gov-P, Control-P, Communicate-P and Protect-P, can be used to manage the risk of privacy arising from privacy data processing. Protect-P is particularly focused on risk management. CSF is intended to address all types of cybersecurity incidents but has been utilized to further support risk management related to cybersecurity-related privacy events using Detect, Response, and Recover Functions. The organization has comprehensively addressed privacy and cybersecurity risks using all five cybersecurity framework features, along with Identification-P, Gov-P, Control-P and Communicate-P. [Fig. 1] shows how to manage various aspects of privacy and cybersecurity risks by using the features of the two frameworks in various combinations. The five privacy framework functions are as follows.



[Fig. 1] Using Functions to Manage Cybersecurity and Privacy Risks

[Tab. 1] Using Functions to Manage

Function Unique Identifier	Function	Category Unique Identifier	Category
ID-P	Identify-P	ID.IM-P	Inventory and Mapping
		ID.BE-P	Business Environment
		ID.RA-P	Risk Assessment
		ID.DE-P	Data Processing Ecosystem Risk Management
GV-P	Govern-P	GV.PO-P	Governance Policies, Processes, and Procedures
		GV.RM-P	Risk Management Strategy
		GV.AT-P	Awareness and Training
		GV.MT-P	Monitoring and Review
CT-P	Control-P	CT.PO-P	Data Processing Policies, Processes, and Procedures
		CT.DM-P	Data Processing Management
		CT.DP-P	Disassociated Processing
CM-P	Communicate-P	CM.PO-P	Communication Policies, Processes, and Procedures
		CM.AW-P	Data Processing Awareness
PR-P	Protect-P	PR.PO-P	Data Protection Policies, Processes, and Procedures
		PR.AC-P	Identity Management, Authentication, and Access Control
		PR.DS-P	Data Security
		PR.MA-P	Maintenance
		PR.PT-P	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Identification-P develops organizational understanding to manage personal privacy risks arising from data processing. The activity of the Identification-P function is a fundamental step in the effective use of the privacy framework. By investigating the environment in which data is processed,

understanding the privacy of individuals directly or indirectly provided or affected by the organization, and conducting risk assessment, organizations can understand the business environment in which data operates, identify and prioritize privacy risks [Tab. 1].

3.3. ISMS-P

Personal information in ISMS-P consists of five areas of certification, including personal information collection, privacy measures, privacy measures, privacy measures, and privacy rights protection, which emphasize the life cycle analysis of personal information only applied in Korea.

IV. Future research and conclusions

Unlike the U.S. management system, the domestic privacy management system is designed to manage the flow of personal information by preparing flow charts and flow charts. It analyzes and schematizes the flow of personal information when it is introduced or changed. Based on this schematic document, the risk of personal information is quickly recognized and maintained to check the risk area. On the other hand, CSF-P in the U.S. is actually establishing a countermeasure step by step to check the actual response attack flow in preparation for hacking attacks or attacks by external intruders. Therefore, it is possible to make practical judgments and respond to dangerous behavior is possible. Therefore, it is necessary to operate a personal information management system in an easy-to-access manner in identifying and responding to risks in small and medium-sized enterprises as a management procedure for identifying, managing, controlling, communicating, detecting, blocking, responding and recovering assets required by CSF-P. And depending on the size, a response system will be needed to understand and analyze risks through the management of detailed personal information flow through the preparation of Korea's personal information flow chart.

[Reference]

[1] J. L. Hennessy and D. A. Patterson, "Instruction-level parallelism and its exploitation," in Computer Architecture: A Quantitative Approach, 4th ed., San Francisco, CA: Morgan Kaufmann Pub., pp.66-153, 2007.

[2] S. Y. Hea, E. G. Kim, "Design and implementation of the differential contents organization system based on each learner's level," The KIPS Transactions: Part A, Vol.18, No.6, pp.19-31, 2011.

[3] S. Russell, P. Norvig, "Artificial Intelligence: A Modern Approach," 3th ed., New York: Prentice Hall, 2009.

[4] D. B. Lenat, "Programming articitical interlligence," in Understanding Artificial Intelligence, Scientific American, Ed., New York: Warner Books Inc., pp.23-29, 2002.

[5] Paul Dunphy, and Fabian A. P. Petitcolas. "A First Look at Identity Management Schemes on the Blockchain," IEEE Security and Privacy Magazine special issue on "Blockchain Security and Privacy", August 2018.

[6] A. Stoffel, D. Spretke, H. Kinnemann, D.A. Keim, "Enhancing document structure analysis using visual analytics," Proceedings of the ACM Symposium on Applied Computing, 2010, pp .8-12.

[7] J. Y. Seo, "Text driven construction of discourse structures for understanding descriptive texts," Ph.D. Dissertation, University of Texas at Austin, TX, USA, 1990.

[8] Park, Kyeong-tae, "A Study on the Obstacle Factors during ISMS Certification: Focused on SMEs," KAIST, 2015.