International Journal of Advanced Culture Technology Vol.9 No.4 355-362 (2021)
DOI https://doi.org/10.17703/IJACT.2021.9.4.355

IJACT 21-12-42

A Study on the Security Management System for Preventing Technology Leakage of Small and Medium Enterprises in Digital New Deal Environment

Sun-Jib Kim

Prof., Dept. of IT, Hansei Univ., Korea
kimsj@hansei.ac.kr

Abstract

Through the Korean version of the New Deal 2.0, manufacturing-oriented SMEs are facing a new environmental change called smart factory construction. In addition, SMEs are facing new security threats along with a contactless environment due to COVID-19. However, it is practically impossible to apply the previously researched and developed security management system to protect the core technology of manufacturing-oriented SMEs due to the lack of economic capacity of SMEs. Therefore, through research on security management systems suitable for SMEs, it is necessary to strengthen their business competitiveness and ensure sustainability through proactive responses to security threats faced by SMEs. The security management system presented in this study is a security management system to prevent technology leakage applicable to SMEs by deriving and reflecting the minimum security requirements in consideration of technology protection point of view, smart factory, and remote access in a non-contact environment. It is also designed in a modular form. The proposed security management system is standardized and can be selectively used by SMEs.

Keywords: *Security Management System, Security Threat, Smart Factory*

1. INTRODUCTION

In order to proactively respond to changes in economic and social structure, Korea analyzed the results of the "Korean New Deal 1.0" promotion to solve new problems and develop a better society and economy, and established the "Korean New Deal 2.0" in July 2020. The Korean version of the New Deal 2.0 analyzes the strategies of resolving polarization as internal and external demand factors, securing digital competitiveness, and carbon neutrality as important factors, and presents "Digital New Deal," "Green New Deal" and "Human New Deal" as tasks. The "Digital New Deal" aims to enhance non-face-to-face infrastructure and foster new hyper-connected industries through the existing New Deal 1.0. In addition, as an expected effect, it is pursuing not only to lead new digital industries but also to secure a convenient and safe daily life. This aims to implement a safe digital environment such as providing digital convergence services, innovation in overall corporate production and distribution such as smart factories, fostering future industries that combine new technologies such as cloud and block-chain, as well as convenient and safe personal information management and data protection. It is also planned to expand online business support for small and medium-sized enterprises and small business owners [1].

Manuscript received: November 22, 2021 / revised: November 30, 2021 / accepted: December 7, 2021
Corresponding Author: kimsj@hansei.ac.kr
Tel: +82-31-450-9884, Fax: +82-31-450-5172
Professor, Dept. of IT, Hansei Univ., Korea

However, an analysis report by the International Chamber of Commerce(ICC) suggests that more than 40% of cyberattacks after COVID-19 were SMEs, which increased year-on-year, and that the important reason was security awareness and investment by SMEs, which are relatively lower than large companies. It was analyzed that damage such as malicious mail, phishing, and smishing using COVID-19 occurred due to the network environment without security [2].

In addition, according to an analysis report by PriceWaterhouse Coopers(PWC), CEOs of companies predict positive economic forecasts as COVID-19 spreads around the world, but recently recognize cybersecurity threats as the next problem to consider in the health sector [3].

Therefore, this study compares existing domestic and foreign security management systems and proposes a technology security management system for small and medium-sized enterprises that reflects the current status of Korean New Deal 2.0 and COVID-19.

The composition of this paper is as follows. Chapter 2 presents an analysis of the relevant security certification system, and presents the security requirements to be considered when building a smart factory applied to manufacturing-oriented SMEs. Chapter 3 establishes and presents a security management system applicable to the reality facing SMEs, and Chapter 4 presents conclusions and implications.

2. PRIOR RESEARCH

2.1 Security management system

ISMS(Information Security Management System) is a representative security management system for domestic information protection established by the Ministry of Science and ICT and operated by the Korea Internet & Security Agency in accordance with Article 47 of the Information and Communication Network Act. The certification system of this security management system includes the Korea Internet & Security Agency and the Financial Security Agency as certification bodies that the Ministry of Science and ICT fulfills its role as a policy body and operates a certification committee. In addition, it has a certification system divided into screening agencies that only conduct screening [4].

This ISMS certification system is operated as ISMS-P, including control items related to personal information. The total control items are 80 information protection-related management items and 22 personal information-related items. In addition, legal based mandatory targets are specified, and administrative standards for non-compliance with certification obligations are established, which is used in Korea as a strong security management system [5].

The International Standard ISO 27001 is an international standard for information security management systems established by the International Standard Organization(ISO) and the International Electro technical Commission(IEC), and was developed to include information security management systems for all for-profit companies, governments and non-profit organizations. This gives stakeholders trust that risks are properly managed by operating the risk management process to ensure confidentiality, integrity, and availability of information. In addition, it should be integrated with them as part of the organization's process and overall management system, and information security should be considered when designing processes, information systems and controls. These ISO27001 are used by internal and external stakeholders to evaluate an organization's ability to meet its information security requirements, and consists of 114 control items in 14 control areas, including information security policies, organizations, and human resource security [6].

The Ministry of SMEs and Startups is promoting a technology protection fence project to protect intellectual property of SMEs. The fence project is carrying out a support project to strengthen the technology protection capabilities of SMEs with the aim of preventing technology theft, relieving damage, and enhancing technology protection capabilities to protect SMEs [7]. Among the projects for pre-prevention of fences, a total of 27 control items are presented reflecting the minimum technical protection requirements by classifying "Technology protection policy estimation", "Security Management Effects", and "Technology protection human resource management". Table 1. shows the comparison of control items specified in the security authentication system described above.

Table 1. Comparison table of security certification system

Control Items	ISMS-P	ISO27001	SM Security Level
1.1. Establishment of management system foundation	√	√	√
1.2. Risk management	√	√	
1.3. Management system operation	√	√	√
1.4. Management system inspection and improvement	√	√	
2.1. Policy, Organization, and Asset Management	√	√	√
2.2. Human security	√	√	√
2.3. Outsider security	√	√	√
2.4. Physical security	√	√	√
2.5. Authentication and Permission Management	√	√	
2.6. Access Control	√	√	
2.7. Encryption applied	√	√	
2.8. Information system introduction and development security	√	√	
2.9. System and service operation management	√	√	
2.10. System and service security management	√	√	√
2.11. Accident Prevention and Response	√	√	√
2.12. Disaster recovery	√	√	√
3.1. Protection measures when collecting personal information	√		
3.2. Protection measures for retention and use of personal information	√		
3.3. Protection measures when providing personal information	√		
3.4. Protection measures when personal information is destroyed	√		
3.5. Protection of data subject rights	√		

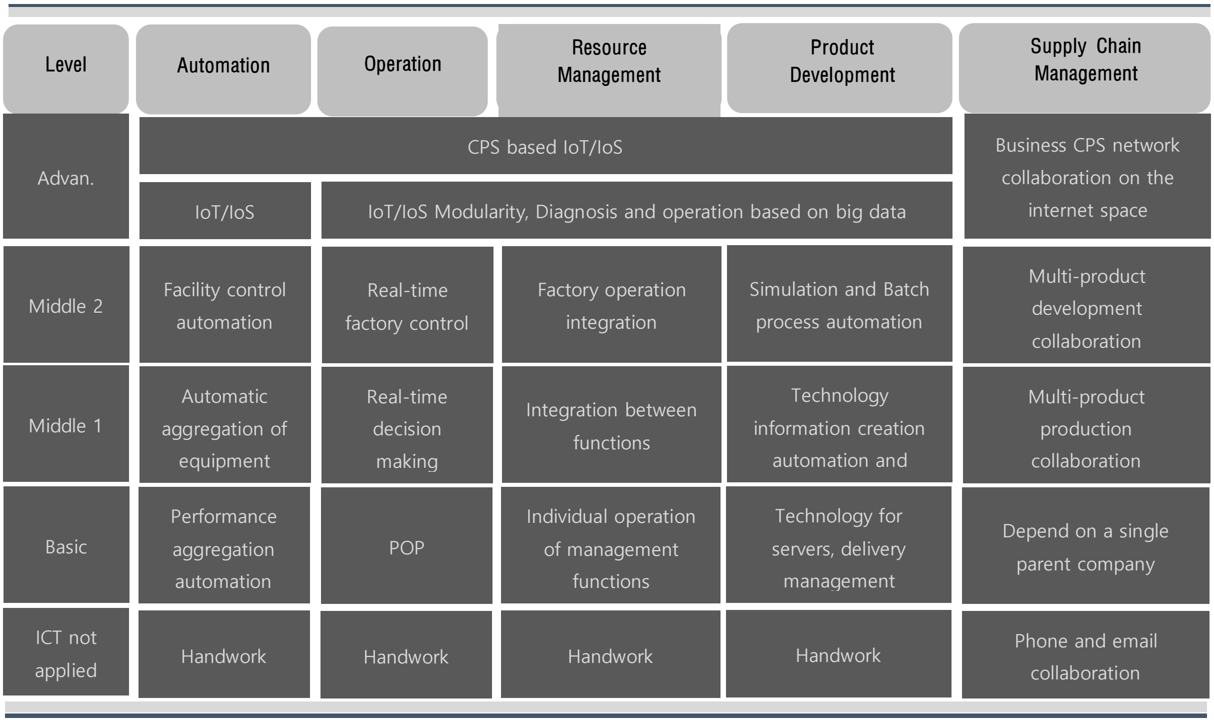
2.2 Smart Factory Security Management System

2.2.1 The necessity of smart factory security management

With manufacturer innovation among SMEs, smart factories that combine all production processes from product planning to sales with information and communication technology to minimize the cost and time required for production and produce customer-centered products are becoming an issue. This is to improve global competitiveness by utilizing the infrastructure technology presented in the 4th Industrial Revolution in each country's manufacturing sector, along with Germany's Industry 4.0, the U.S. innovation strategy of advanced manufacturing 2.0, and Japan's intelligent manufacturing system [8].

Accordingly, the Smart Manufacturing Innovation Promotion Group divides the level of smartization of the construction system into levels 1 to 5 based on smart capabilities of companies as shown in Figure 1, and announces continuous support plans to expand smart factories [9].

However, due to the development of the network, data utilization in smart factories is naturally increasing as the spread and spread of smart factories are promoted along with environmental changes such as the entry into the hyper-connected era, that is, the supply of smart devices. In addition, technology infringement accidents targeting operational technology of smart factories are also increasing. Accordingly, smart factories should recognize the risk of technology leakage in collecting, processing, and utilizing IoT-connected equipment and cloud-based data through networks, and take appropriate countermeasures.



Level	Automation	Operation	Resource Management	Product Development	Supply Chain Management
Advan.	CPS based IoT/IoS				Business CPS network collaboration on the internet space
	IoT/IoS	IoT/IoS Modularity, Diagnosis and operation based on big data			
Middle 2	Facility control automation	Real-time factory control	Factory operation integration	Simulation and Batch process automation	Multi-product development collaboration
Middle 1	Automatic aggregation of equipment	Real-time decision making	Integration between functions	Technology information creation automation and	Multi-product production collaboration
Basic	Performance aggregation automation	POP	Individual operation of management functions	Technology for servers, delivery management	Depend on a single parent company
ICT not applied	Handwork	Handwork	Handwork	Handwork	Phone and email collaboration

Figure 1. Level of Smart Factory

2.2.2 IEC 62443 & Smart Factory Cyber Security Guide

IEC 62443, an industrial control system security standard proposed by IEC, is an international cybersecurity standard for plants, facilities, and systems across the industry. In the IEC 62443 series, the general domain stipulates descriptions of the concepts and terms of standards, policies and procedures, security requirements for industrial control systems, and functional requirements for guarantees. IEC 62443-2-1 presents a total of 115 control items in seven fields in three areas: "Risk Analysis", "Risk Resolution", and "Monitoring and Improvement" for the elements necessary to establish a security management system for industrial automation and control systems [10]. Also, The Korea Internet & Security Agency has published the ‘Smart Factory Cyber Security Guide’ to internalize security in ICT convergence products and services of smart factories. This guide defines 34 detailed requirements in 6 security requirements of access control, data protection, safe status, information security operation policies and procedures, asset management and security incident prevention and response [11].

3. SECURITY MANAGEMENT SYSTEM FOR SMES

Through the promotion of the New Deal 2.0 project, SMEs have faced opportunities for innovation in overall production and distribution of companies such as digital convergence and complex services and smart factories. In addition, COVID-19 has led to a new paradigm of a non-face-to-face environment that has never been experienced before.

Amid these changes in the surrounding environment, it is necessary to apply security management matters to preemptively respond to security threats in the existing IT environment and possible security threats in the convergence environment in order to incorporate new 4th industrial technology into production facilities and secure communication stability among suppliers.

However, according to the small and SMEs survey conducted by the Ministry of SMEs and Startups, the technology protection capacity of SMEs is about 70% of that of large companies. The process of technology data leakage by SMEs was analyzed in the order of copying and stealing technology data, using e-mail and portable devices, joint or joint research, and scouting of key personnel.

The main causes of the technology leak were analyzed to be job insecurity, such as security management and supervision system establishment, lack of security-related investment, pursuit of personal financial interests, lack of security personnel, complaints about the company's treatment, and job cuts. The analysis results suggest that SMEs cannot build various security solutions due to economic costs, that is, lack of investment, and lack of security personnel and continuous education, as well as low loyalty among executives and employees compare with large companies.

Considering the reality of these SMEs, it is not easy to meet the existing domestic and foreign security management system in which costs and manpower must be invested.

Therefore, the security management system for preventing technology leakage of SMEs presented in this study was designed and presented in consideration of the following matters.

First, it is an approach in terms of the difference between information and technology. Existing ISMS-P, ISO27001, etc. are approaches from the perspective of information protection, while SMEs need to establish a security management system from the perspective of preventing technology leakage.

Second, for the existing domestic and foreign security management system, if the establishment of a management system under the PDCA structure and various security requirements for each security field were derived as control items, rather than securing systematically, the security management system for preventing technology leakage of SMEs needs to derive the most efficient security requirements considering cost-effectiveness as control items.

Third, for SMEs that need to improve productivity through changes and applications of various technologies, it is desirable to provide modularity and secure connection between modules rather than applying a management system reflecting separate security requirements to ensure stable business continuity. For example, it is desirable to selectively apply security management requirements for smart factories and non-face-to-face environments through modularization, which is an additional form of security requirements.

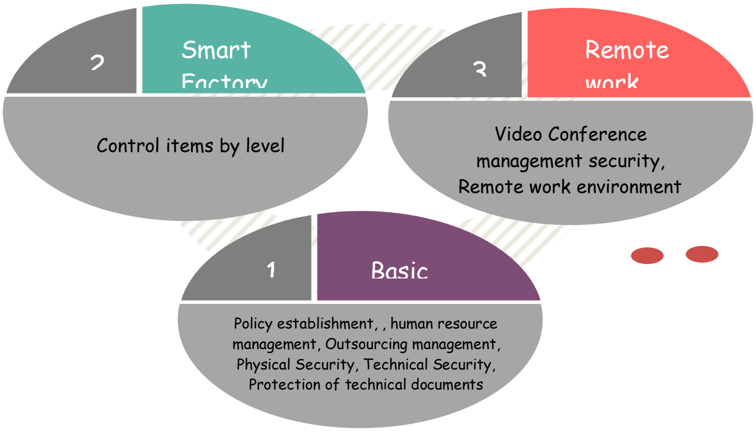

2
Smart Factory
Control items by level
3
Remote work
Video Conference management security, Remote work environment
1
Basic
Policy establishment, , human resource management, Outsourcing management, Physical Security, Technical Security, Protection of technical documents

Figure 2. Module type security management

Figure 2. explains the connection of the security management system module to prevent technology leakage for SMEs. Basic security requirements were presented as a "Basic" module by reflecting the causes and problems of technology leakage accidents of SMEs. Security requirements for smart factories were presented as modules for "Smart factories", and non-face-to-face environmental requirements for COVID-19 were presented as modules for "Remote access". As each is presented as a different type of module, it can be selectively applied according to the current status of SMEs, and it is configured to be supported without mutual redundancy. The advantages of the proposed module-type security management system are the application of new businesses and technologies and the convenience of applying new threat countermeasures.

The security requirements for smart factories were derived as minimal security requirements, focusing on the digitalization of production information, use of cloud systems, and use of AI technology in step-by-step security requirements analysis. For remote access, basically, from the standpoint of SMEs, security requirements applicable to at least remote access were derived and applied. In addition, Table 2. Shows the relationship between the technology leakage accident rate and the control items of the model presented in this study.

Table 2. Basic technology protection requirements modules based on technology leakage accident analysis

Indicator category			Causes of Technology Leakage Accidents			
			(1) Insufficient security management and supervision system(34.9%)	(2) Insufficient security-related investment(30.6%)	(3) Lack of security personnel(21.7%)	(4) Lack of security awareness(32.4%)
Basic	1. Policy establishment	- Technology protection policy establishment - Establishing relevant regulations as needed - Management approval Notice to staff	√	√	√	√
	2. Human resource management	- Assignment of person in charge (concurrent osition) - Continuous technology protection awarness and training - Confidentiality Pledge			√	√
	3. Outsourcing management	- Confidentiality Pledge & NDA	√	√	√	√
	4. Physical security	- Security area separation & management	√	√		
	5. Technical security	- Access control - Password management - PC security - Data Backup - Security solutions management	√	√		√
	6. Protection of technical documents	- Intellectual Property Rights Acquisition	√	√	√	
Smart factory	1. Device Control	- Industrial automatic control system access control - IoT Device control - Remote access management	√	√	√	√
	2. Techical security	- Wireless access control - Protection of data in transit - Protection of saved data	√	√	√	
	3. Cloud Security	- Safe use of cloud systems	√	√	√	√
	4. Prevention and response	- System anomaly detection - Vulnerability analysis	√	√	√	

Remote work	Use of dedicated space	√	√		
	Use of dedicated equipment	√	√	√	√
	Use of paid remote access program	√	√	√	√

4. CONCLUSION

The "Korean version of the New Deal 2.0" will bring about structural innovation across our industry. In addition, it is a good opportunity for domestic SMEs centered on manufacturing to pursue strengthening competitiveness through smart factories. However, as a counter benefit, security infringement accidents are expected to affect the business continuity of SMEs in various forms. Despite the increase in risk awareness, existing security requirements proposed by domestic and foreign related organizations and standardization organizations are difficult to apply to SMEs considering the view of technology protection and the reality of SMEs' economies.

Therefore, in this study, a modular security management system was presented by deriving the minimum security requirements for technology protection possessed by SMEs in the reality of SMEs. Although it was suggested as a minimum requirement, it is judged that these security requirements will not be easy to access and apply to most SMEs.

Accordingly, it is judged that the government should support SMEs to improve their competitiveness by improving the level of technology protection for SMEs through continuous interest and support for SMEs. In addition, considering that it is a modularized and presented security management system, it is necessary to change and expand and supplement it through additional research.

ACKNOWLEDGEMENT

This work was supported by Hansei University Research Grant in 2020.

REFERENCES

[1] H. W. Lim, & S. J. Kim, “A study on ways to make employment improve through Big Data analysis of university information public", *The International Journal of Advanced Culture Technology,* Vol. 9, No. 3, pp. 174-180. 2021.

[2] D. S. Seo, & H. W. Lim, “A study on cultural understanding and regional cooperation in Yemen and Ethiopia", *The International Journal of Advanced Culture Technology,* Vol. 7, No. 3, pp. 147-154. 2021.

[3] H. W. Lim, “A Study on Countermeasures Against Cyber Infringement Considering CPTED", *The International Journal of Advanced Culture Technology,* Vol. 9, No. 2, pp. 106-117. 2021.

[4] H. W. Lim, & S. J. Kim, “Improvement Strategy According to the Change of Hotel Environment", *The International Journal of Advanced Culture Technology,* Vol. 9, No. 2, pp. 72-79. 2021.

[5] T. D. Kim, “The ISO the research also the ISMS security maturity of 27001 regarding a measurement modeling (ISO 27004 information security management measurement and metric system)”, *The Korean Society Of Computer And Information*, Vol. 12, No. 6, pp. 153-160, 2007.

[6] ISO, International Standard ISO/IEC 27001 Second Edition, 2013.

[7] SMEs Ultari, *https://www.ultari.go.kr.*

[8] J. M. Park, “Technology and Issue on Embodiment of Smart Factory in Small-Medium Manufacturing Business”, *The Journal of Korean Institute of Communications and Information Sciences*, Vol. 40, No. 12, pp. 2491-2502, 2015.

[9] H. W. Lim, “Analysis of Psychological Factors Inducing Cybercrime", *The International Journal of Advanced Culture Technology,* Vol. 7, No. 2, pp. 157-163. 2021.

[10] Smart Factory, *https://smart-factory.kr.*

[11] Korean Agency for Technology and Standards, KS X IEC 62443-2-1: 2010 Industrial communication networks – Network and system security – Part 2-1: Establishing an industrial automation and control system security program, 2020.

[12] Korea Internet & Security Agency, Smart Factory Cybersecurity Guide, 2019.