JDCS
디지털콘텐츠학회논문지
Journal of Digital Contents Society
Vol. 20, No. 2, pp. 431-442, Feb. 2019

ICT 융합 환경에서 인간중심의 보안역량 강화방안 연구

나 원 철[1] · 장 항 배[2*]
[1]중앙대학교 대학원 융합보안학과(산업보안전공)
[2]중앙대학교 산업보안학과

Human-Centric Security Capability Enhancement in ICT Convergence Environment

Onechul Na[1] · Hangbae Chang[2*]
[1]Department of Security Convergence(Major in Industrial Security), Chung-Ang University, Seoul 06974, Korea
[2]Department of Industrial Security, Chung-Ang University, Seoul 06974, Korea

[요 약]

4차 산업혁명 시대 도래에 따라 초 지능, 초 연결 사회로 진입하면서 보안 위협이 다양화 되고 있다. 이에 따라 조직에서는 서비스 단말기 중심의 보안환경에서 서비스 사용자 중심의 보안환경으로의 혁신적 전환이 필요한 실정이다. 따라서 본 연구에서는 조직 구성원의 보안 의식 형성을 위한 핵심요소를 추출하고, 새로운 보안 역량을 제안하였다. 그 결과 조직 구성원의 보안의식 구성요소들은 조직의 보안체계와 긍정적인 연관성이 있는 것으로 분석되었다. 또한 조직의 보안 성숙도 향상을 위해 각 성숙도 단계별로 보안의식을 분석하여 개선항목을 도출하였다. 본 연구는 정부 차원의 보안 산업에 대한 투자타당성을 제시하고, 보안정책 및 지원 사업에 대한 효율적인 관리에 도움이 될 것으로 기대된다.

[Abstract]

With the emergence of the Fourth Industrial Revolution, security threat is being diversified as society is entering to hyper-intelligence and hyper-connected society. Accordingly in organization, it is necessary for service-terminal-based security environment to be converted into service-user-based security environment. In this study, core components for developing organization members' security consciousness is extracted and suggested a new security capability. As a result, it was analyzed for organization members' security consciousness components to have positive correlation with organizations' security system. Also, items that are to be improved is also drawn through analyzing security consciousness by each maturity level in order to improve organizations' security maturity. This study is expected to suggest investment feasibility of security industry at the government level and be a help to effective management of security policy as well as support project.

색인어 : 보안역량, ICT 융합 환경, 보안의식, 보안체계, 보안 상관분석

Key word : Security capability, ICT convergence environment, Security consciousness, Security system, Security correlation analysis

http://dx.doi.org/10.9728/dcs.2019.20.2.431

Received 20 January 2019; **Revised** 01 February 2019
Accepted 20 February 2019

***Corresponding Author; Hangbae Chang**
Tel: +※ 개인정보 표시제한
E-mail: hbchang@cau.ac.kr

Ⅰ. Introduction

For an organization to promptly respond the current rapidly changing business environment, its informatization is considered to be the first priority[1]. Organizational informatization is not just a change in a business environment but a means to secure organizational competitiveness through an improvement in productivity and a reduction in transaction costs[2]. Recently, with the emergence of the Fourth Industrial Revolution on the basis of the Iot and Big data technology, changes to ICT convergence environment is being made, such as convergence of every industry based on ICT being rapidly proceeding, entering to hyperconnection society where everything gets connected to internet and etc[3]. In the changed ICT convergence environment, organization's core technology, which is to be safely protected is converged with ICT and be informatized, causing a leakage with ease to a competitive organization or overboard. Also, a rapid expansion of space through hyper-connection is causing difficulty in loading a security system on every subject[4]. Therefore, it has been increasingly necessary to convert the current service-terminal-based security environment into a service-user-based[5]. However, the existing security activities for resolving security incident issues within a ICT convergence environment mainly review technical solutions through the introduction/establishment of a security system. Considering the characteristics of security breaches, such as the difficulty of accident tracking due to advanced technology or an information leak by an insider, we see that such an approach has limitations. In particular, even if a cutting-edge security system is established in multiple layers, the malicious behavior of an insider can invade the system and leak information easily. Therefore, it is currently necessary to convert the security capacity system into a user-based one focusing on security consciousness. This study aims to extract the core factors for generating the security consciousness of organization members and proposes a new design for the security capability (security consciousness + system) based on the formation of a human-centric security consensus developed from existing security solutions and rule-based security capabilities.

Ⅱ. Previous Studies

2-1 Studies on Security Consciousness and Characteristics

Security consciousness is composed of three factors: security awareness, security knowledge, and security behavior[6]. In order to understand the notion of security consciousness, one should clearly comprehend the characteristics of security awareness, knowledge, and behaviors.

The notion of "awareness" has been widely used in multiple fields including the social sciences, psychology, and medicine. As one of the main components of "consciousness," it is at the center of "behavior" and defined as a heightened interest in active individual participation and certain events[7]. When we define the concept of security awareness on the basis of such a notion, we can also state that it is similar to the awareness of security and interest in security-related activities[8] or general knowledge of group individuals regarding the security and cognition of organizational security[9].

Next, "knowledge," an individual's insight or know-how obtained from their experience or value, is defined as information, either in an explicit or implicit format[10]. On the basis of this notion, we can define the concept of "security knowledge" as the level of knowing the required security level to perform activities to protect the assets of an organization. The range of security knowledge includes cognition of the security policy compliance/work process, work application of the security equipment and processes, and the maintenance of security levels[11, 12].

Lastly, unlike reflexive or instinctive ones, a "behavior" is defined as thinking and executing a certain purpose; we can say that the concept of "security behavior" is the level of group members' security policy compliance[13] and the behavior of group members to protect intellectual assets within their organization[14].

Thus, security consciousness comprehensively includes the level of all group members' cognition of the significance of security, proper security knowledge for an organization, and the responsibility of individuals and their following behaviors[15]. These factors cannot be distinguished, and security awareness/knowledge stimulates changes in the behaviors of group members through interactions, ultimately strengthening the security capacity of an organization.

According to the characteristics of security consciousness, previous projects conducted research considering the security awareness, knowledge, and behavior.

Eloff and Eloff[16] studied a comprehensive package of security components to deal with standardized approaches for the maintenance of security programs and mentioned the security awareness or behaviors of group members. Our study approached this topic on the basis of ethical values for the security awareness or behaviors of organization members stating that their security-related ethical actions or behaviors should be merged with the routine work processes of their organization.

The study by Tudor[17] stated that it becomes easier to execute

a new process and order behavior changes on the basis of security if management trusts its employees and vice-versa. It also mentioned that such mutual trust among group members is a significant factor for their security awareness and behaviors. In addition, this research also proposed different security components to enhance the level of security capacity within an organization.

2-2 Previous Studies on Security Systems and Measurements

A security system is a managerial, physical, and technical system for enhancing the safety and credibility of organizational assets. The most widely used methods for measuring the levels of security systems are ISO/IEC 27001 and 27002, the certified standards for information security maintenance systems issued by the joint commission of the International Organization for Standardization and the International Electrotechnical Commission. Besides these methods, there is SP800-53, a tool for diagnosing the security of an information system, enacted by the National Institute of Standards and Technology. Moreover, different studies have been conducted to measure the level of security systems.

The study of Oh[18] analyzed the cases of security level evaluation such as NIST SP 800-53, NIST SP 800-26, and ISO27001 and determined the fields and items to be controlled for level evaluation in order to assess the security levels of information communication services. In total, 12 control fields were determined for the assessment: security policy, risk evaluation, configuration management, maintenance, media protection, security awareness/education, contingency plan/business continuity plan, physical/environmental protection, personnel security, accident response, audit/responsibility traceability, and system access control/communication protection. In addition, we proposed a quantitative evaluation index (SSE-CMM analysis) for security level assessment and developed evaluation items to suggest a method for performing the evaluation.

Ko et al.[19] conducted a study on a method that evaluated the security level of corporations using a balanced score card. In their study, an integrated evaluation system of the security level based on the balanced score card was designed, and the measurement items in the design were the security policies and plan, the security organization and human resources, security education and investment, the security infrastructure, asset management, operation management, customer satisfaction, internal user satisfaction, supplier/partner satisfaction, risk management, and business performance management. The integrated evaluation system designed for the security level calculated the weight of each section and evaluation viewpoints via related field experts using an analytical hierarchy process and an additional case study to verify the integrated evaluation system of the security level.

A study by Kim et al.[20] investigated the methodological security elements specified in ISO 27002 and identified the factors that affect the security levels in organizations, thereby evaluating the security levels of governmental institutions. In their study, the support of the top management layer (governing body), the relatedness between a task and security in each governmental institution, and the awareness and culture of security were set as the measurement items in the design. However, the scope of their study was limited to governmental institutions only; thus, it cannot be applied to the present study.

Ⅲ. Analysis and Measurement of the Human-Centric Security Capability Level in the ICT Convergence Environment

3-1 Design of the Study Methodology for Improving Human-Centric Security Consciousness and the Capability Level

The security activities of organization members are interpreted as a set of security activities that are considered valuable by organization members, in which security consciousness is a prerequisite. The security consciousness means demonstrations of organization-expected behaviors through education and training and the concentration of awareness by members. Such enhancement activity of security consciousness support to secure stability of information asset from the threat that can occur due to misbehavior of organization members. The present study designed a conceptual model to measure the security system of organizations in response to security incidents in order to construct a robust security environment in the ICT convergence environment from a macroscopic perspective. This study aims to employ the methodology shown in Fig. 1 to measure the security system and the level of security consciousness of organization members based on the basic model.

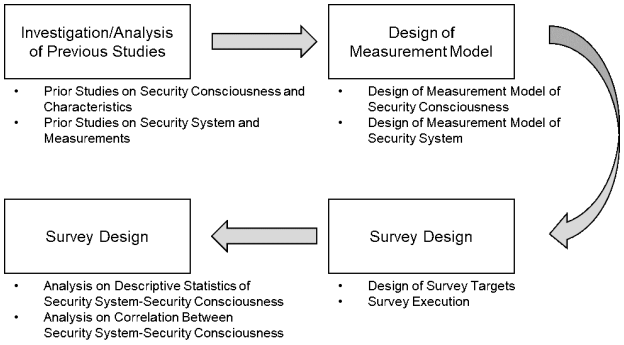

그림 1. 연구 방법론 및 개념 모델
Fig. 1. Conceptual model and study methodology

This study analyzes the correlation between the organization security system and the level of security consciousness of organization members as well as the factors of influence between detailed indexes. To derive the measurement sections of organization security system, the organizational security maturity models including the model in ISO/IEC 27001[21] models along with those by McCarthy and Campbell[22] and Tudor[17] mentioned in previous studies were analyzed to connect components related to the organizational security system and derive the most frequent components (See Table 1).

표 1. 조직 보안체계 측정 영역 도출과정
Table 1. Process for deriving the measurement sections of an organizational security system

Component	ISO/IEC 27001	McCarthy & Campbell	Tudor	Accepted
Security policy, standards and guidelines	○	○	○	√
Certificate of the standards	○	×	×	
Measurement/Metric/Return on investment	×	○	×	
User management	○	○	×	√
User awareness, training and education	○	○	○	√
Privacy	×	○	×	
Asset management	○	×	○	√
Physical/environmental control device	○	○	○	√
Technical operation	○	○	○	√
Accident management	○	○	×	√
Business continuity plan	○	○	○	√

As a result, the “security policy” section was derived from the factors of security policy, standards, and guidelines related to the support environments of security management; “asset management” from the factor of asset management; “human resource management” from user management, user awareness, and training and education; “facility (equipment) management” from the physical and environmental control device; and “IT security management" from technical operation. Finally, the “response to security incidents” section was derived from the security management and business continuity plan (BCP) related to security continuity management. Thus, a total of six sections were finally derived, and 50 measurement items were designed in detail.

Next, an analysis of previous studies was conducted to derive the measurement sections of security consciousness of organization members. According to a study by Robbins[23], security awareness and behaviors are variously revealed depending on the applied target tier, and a tier was differentiated into individual and organizational tiers. On the basis of this differentiation, an organizational security maturity model including ISO/IEC 27001 was analyzed along with the studies by Eloff and Eloff[16] and Tudor[17] mentioned in Section 2, and the components related to the security consciousness measurement sections of organization members were derived by connecting the analysis results of a previous study by Robbins [23] related to security awareness and behaviors (See Table 2).

표 2. 조직 구성원 보안의식 측정영역 도출과정
Table 2. Process of deriving the measurement sections of security consciousness in organization members

Component	Robbins	ISO/IEC 27001	Eloff and Eloff	Tudor	Accepted
User awareness, training and education	Individual	○	○	○	√
Ethical value and behaviors		×	○	×	√
Privacy		×	○	×	
Trust between organization members	Organization	×	×	○	
Corporate governance		×	×	×	√
Security organization activities		○	○	○	√
Compliance and monitoring		○	○	○	√
Consideration on best practice and standards		○	○	○	√

As a result, the sections of “individual security awareness” and “individual security education and training” were derived from user awareness and training and education in the individual tier where security awareness and behaviors are differentiated according to individual values and the consciousness of each organizational member. In addition, the section “individual security ethics” was derived from the ethical value and behaviors. The organization tier where security awareness and behaviors were differentiated according to a type of organizational structure and culture was redefined as a group tier, which was more appropriate in this study that measured security consciousness at the enterprise level. Thus, in the group tier, the “execution of group security regulations” section was derived from security organization activities and compliance and monitoring, the

"mutual trust between group members" section from trust between organization members, and the "group change management" section from consideration of the best practice and standards. Accordingly, a total of six sections were finally derived, and 22 detailed measurement items were designed for the security consciousness of organization members. These six measurement sections of the organization security system and six measurement sections of the security consciousness of organization members are summarized in Table 3.

표 3. 조직 보안체계 및 조직 구성원 보안의식 상관관계 분석모형
Table 3. Measurement sections of the organization security system and the security consciousness of organization members

Analysis Target		Section
Organization security system		Security policy
		Asset management
		Human resource management
		Facility (equipment) management
		IT security management
		Response to security incidents
Security consciousness of organization members	Individual tier	Individual security awareness
		Individual security education and training
		Individual security ethics
	Group tier	Execution of group security regulations
		Mutual trust between group members
		Group change management

To verify the designed evaluation items and survey questionnaire, a group of experts in related fields was configured, and the first revision of the design model was conducted using the Delphi method. Then, the second revision was conducted by analyzing the reliability and validity through statistical validation utilizing a survey with experts in related fields. Finally, the third revision was completed by selecting a potential target organization where the designed model would be applied in practice and by performing prior verification with regard to the organization. Using the method described above, the correlation between the level of the security system of the target organization and the security consciousness of organization members was analyzed. More specifically, the factors influencing the security consciousness of organization members that form the security level of an organization were analyzed (See Fig. 2).

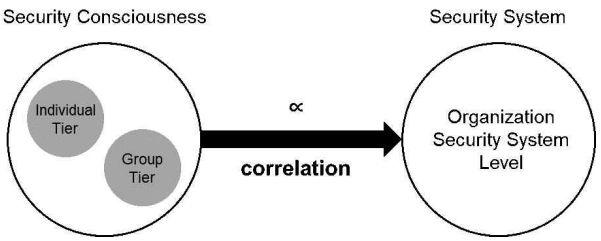

그림 2. 조직 보안체계 및 조직 구성원 보안의식 상관관계 분석모형

Fig. 2. Model for analyzing the correlation between the organization security system and the security consciousness of organization members

To measure the security system of an organization and the level of security consciousness of organization members, 502 organizations in the field of cyber-physical sensor systems in Korea were selected. Considering that the study targeted organizations in Korea, the 502 organizations were classified into electric and electronic businesses, chemical textile businesses, mechanical material businesses, and information and communication (ICT) businesses according to the "Korea Standard Industry Classification." They were also classified according to the business process. The organizations were also divided by a business scale into large and small & medium enterprises (SMEs) according to the number of employees. A large enterprise was defined as a company whose number of employees was more than 300, and an SME was defined as a company that had less than 300 employees. The organization members were divided into a manager level over team leaders and general employees inside the organization to measure the level of security consciousness of organization members. The scale of the measurement items was from 0 to 100 points and defined as follows: less than 20 points: "risky," 20 to 40 points: "vulnerable," 40 to 60 points: "average," 60 to 80 points: "good," and 80 points or higher: "excellent."[24]

3-2 Measurement and Analysis of the Security Consciousness of an Organization

The level of security consciousness of all organizations was 67.9 points. More specifically, the individual security consciousness was the highest at 76.4 points, whereas the level of security consciousness for individual security education and training was the lowest.

The security consciousness of the group tier did not show a significant difference, as it tended to converge to the mean, whereas the security consciousness of the individual tier showed that the level of individual security education and training was nearly half (51.8 points) of that of individual security consciousness and security ethics, which was relatively high. This result implies that all organizations were exposed to an environment that lacked security education and training in the individual tier (See Fig. 3).

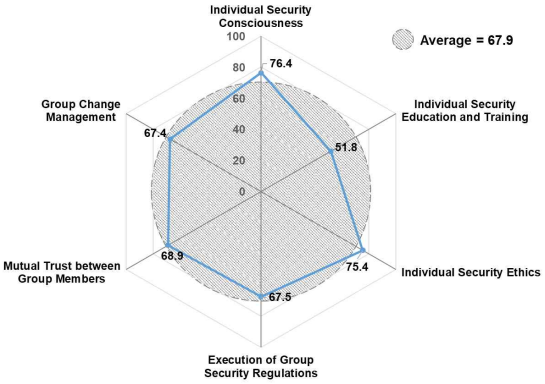

그림 3. 조직 보안의식 수준현황
Fig. 3. Current status of the level of security consciousness of an organization

The analysis results according to the business scale showed that SMEs scored 67.4 points while large enterprises scored 74.1 points, which is a difference in the security consciousness level of 6.7 points between the two groups. More specifically, the individual security consciousness section exhibited the closest level between the two groups with a 3.6-point difference, whereas the individual security education and training section had the largest difference of 11.6 points. This was because large enterprises were more resourceful than SMEs; thus, they were equipped with more resources for inputs to education and training in the individual tier (See Fig. 4).

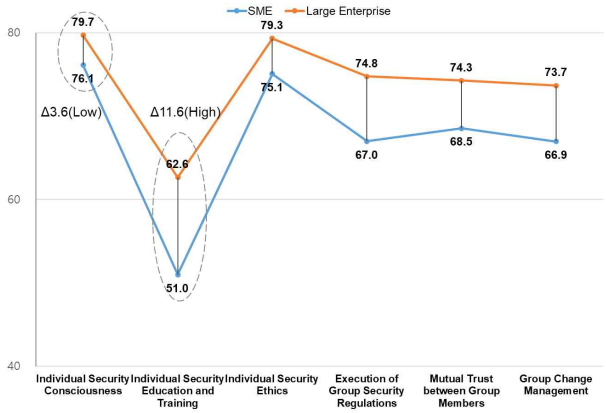

그림 4. 기업규모 별 보안의식 수준비교
Fig. 4. Comparison of the security consciousness level by business scale

The organization security consciousness according to the business scale had a slight difference on average (within 10 points). Accordingly, this study conducted a t-test to verify whether there was a difference in the security consciousness level of organization members according to the business scale.

The independent sample test results revealed that the significance probability of the Levene test for the equality of variances was 0.463. Thus, the analysis results were investigated on the basis of the assumption of the equality of variances. The significance probability of the two-sided t value was calculated as 0.00, which is smaller than 0.05. This result indicated that the mean difference in the security consciousness level of organization members between two groups was significant according to the business scale (large and SMEs) (See Table 4).

표 4. 조직 규모에 따른 보안의식수준 차이성 검증
Table 4. Tests of the difference in the security consciousness level according to the organization scale

Category	Mean	Standard Deviation	t value	p value
Large enterprises	74.068	6.4445	5.667	0.000
SMEs	67.447	6.5870		

The results for a comparison of the security consciousness level according to the organization business sectors showed that the ICT sector and the electric and electronic sector had the same level of 68.6 points up to the first decimal place. If the points were analyzed beyond the significant figure, then the electric and electronic sector (68.64 points) was slightly higher than the ICT sector (68.58 points). In addition, the mechanical material sector had the lowest score (67.4 points). The electric and electronic and ICT sectors were both closely related to information technology, which is why they were more concerned about security consciousness than other sectors.

More specifically, the largest difference (Δ24.9) was observed between the individual security consciousness and security education and training sections in the electric and electronic sector. The above-analyzed results for security consciousness level (electric and electronic > ICT > chemical textile > mechanical material sectors) were only equivalent to those of the security regulation execution section in the group tier, whereas the other sections showed a different priority. In particular, the mechanical material sector, which showed a relatively lower level of security consciousness overall, had slightly higher levels of individual security consciousness and mutual trust between group members than those of the chemical textile sector by 0.3 and 0.5, respectively.

The electric and electronic sector showed the highest level of security consciousness compared to the other sectors. This was because the ICT internalization is being progressed at a relatively fast rate compared to the other sectors, and various efforts of an organization are being made to improve members' security consciousness level according to these kinds of environmental

changes.

3-3 Measurements and Analysis of the Levels of Security Systems in Organizations

The level of the security system of all organizations was 47.5 points, which was the average level that was close to the vulnerable level. More specifically, the level of the response to security incidents was 34.4 points, which was the only vulnerable level among all sections, and the facility (equipment) management section scored 57.2 points, which was the average level that was close to the good level. The next highest level was the asset management section that scored 52.7 points. This result implies that organizations made an effort to arrange physical facilities and equipment management to be equipped with security systems as a priority, and these efforts were accompanied with asset management for facilities and equipment. Moreover, the analysis results showed that the response capability of organizations to security incidents or accidents was very low if cyberattacks occurred from the outside or core technologies were leaked from the inside (See Fig. 5).

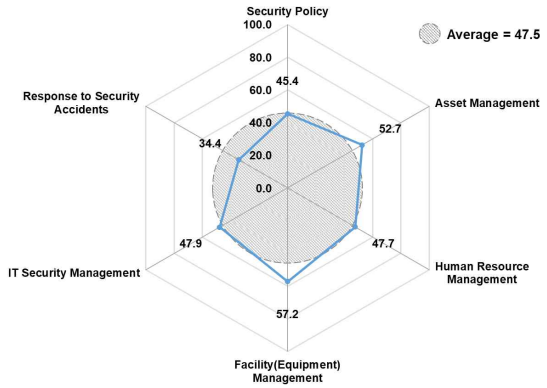

그림 5. 조직 보안체계 수준현황
Fig. 5. Current status of the level of security systems in organizations

The capability level of a security system was 45.8 points for SMEs and 70.9 points for large enterprises on average according to the organization scale. The large enterprises, which were richer in human resources and materials than SMEs, had a higher security capability by 25.1 points on average than that of SMEs in all sections of security capability. More specifically, the SMEs and large enterprises showed the largest difference of 29.3 points for the "response to security incidents" section, whereas the smallest difference of 19.6 points was observed for the human resource management section that managed people. The reason for the smallest difference in the human resource management sector between two groups was due to the relatively lower level of human resource management by large enterprises rather than the high level of human resource management by SMEs. This was because large enterprises prioritized facility (equipment) management the most, followed by asset management, IT security management, security policy, and then human resource management, which was quite a low priority. In contrast, SMEs prioritized facility (equipment) management the most, followed by asset management and then human resource management as the third priority as a core component of organizations (See Fig. 6).

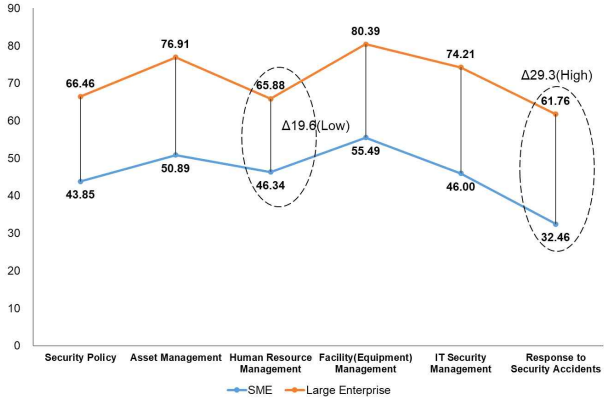

그림 6. 기업규모 별 보안체계 수준비교
Fig. 6. Comparison of the security system level by business scale

The "response to security incidents" section had the lowest capability level for both large enterprises and SMEs. In particular, SMEs had a vulnerable level for this section (20–40 points), which implies no response was available when security incidents occurred. The security management for the facility (equipment) section, which was the highest capability in large enterprises, was also the highest capability in the SMEs, which implied that both of them had invested in facility (equipment) management as a top priority to improve security capabilities.

Although a significant difference in the means of the organization security system was revealed according to the enterprise scale, a t-test was conducted to verify whether there was a significant difference according to the enterprise scale.

The independent sample test results revealed that the significance probability of the Levene test for equality of variances was 0.906. Thus, the analysis results were investigated on the basis of the assumption of the equality of variances. The significance probability of the two-sided t value was calculated as 0.00, which is smaller than 0.05. This result indicated that the mean difference in the security system level of an organization between two groups was significant according to the business scale (large and SMEs) (See Table 5).

표 5. 조직 규모에 따른 보안의식수준 차이성 검증
Table 5. Tests of the difference in the security consciousness level according to the organization scale

Category	Mean	Standard Deviation	*t* value	*p* value
Large Enterprises	70.944	21.7067	6.567	0.000
SMEs	45.834	21.5154		

The results of a comparison of the security system level according to the organization sector showed that the mechanical material sector was the highest at 51.1 points, whereas the chemical textile sector was the lowest at 43.1 points. The results indicate that the high level of security capabilities is made centrally in the sectors such as mechanical material, ICT and electric and electronic, where ICT internalization is progressing relatively rapidly.

More specifically, the largest difference (Δ28.2) was observed between the facility (equipment) management section in the chemical textile sector and the IT security management section in the same sector. The above-analyzed results for the security consciousness level (mechanical material > ICT > electric and electronic > chemical textile sectors) were only equivalent to those of the asset management and response to security incident sections, whereas the other sections showed a different priority. In addition, the largest difference (15.6 points) was observed for the human resource management section between the ICT and chemical textile sectors. The electric and electronic sector had the same level for the human resource management and IT security management sections. Since the mechanical material sector mainly focused on businesses utilizing facility (equipment) management, the mechanical material sector had the highest level of security systems in the facility (equipment) management section. In addition, the level of response to security incidents in the chemical textile sector was 28.6 points, which was close to the risk level, indicating defenselessness against security incidents .

The results showed that increasing the response capability to security incidents will improve the overall level of the security system in all sectors, and the ICT sector was equipped with a balanced level of security capability. In addition, the level of security capability for the sections according to the organization sector showed a similar overall pattern, although the security capability in the ICT sector was slightly different according to the measurement section. The ICT sector was focused on the security management of human resources the most (56.3 points) followed by IT security management (54.2 points) and asset management (54.0 points) because this sector was engaged in IT business. In particular, the ICT sector showed levels of more than the half (50 points) for all sections except for the "response to security incidents" section. Since the main business space and deliverables in the ICT sector were the ICT space itself, the ICT sector had a lower physical security management score in facility (equipment) management than the other sectors in the relative sense.

3-4 Investigation and Analysis of the Level of Human-Centric Security Capability

To calculate the overall level of security capability (consciousness and system), a ratio of 20% for security consciousness and 80% for the security system was applied. Since the security system referred to the management, physical, and technical systems provided in organizations, a high proportion of importance was given, whereas a lower proportion was given to security consciousness because it was reflected according to the individual opinions of the members. The mean and standard deviation of the security capability were 51.61 and 18.5 points, respectively (See Fig. 7).

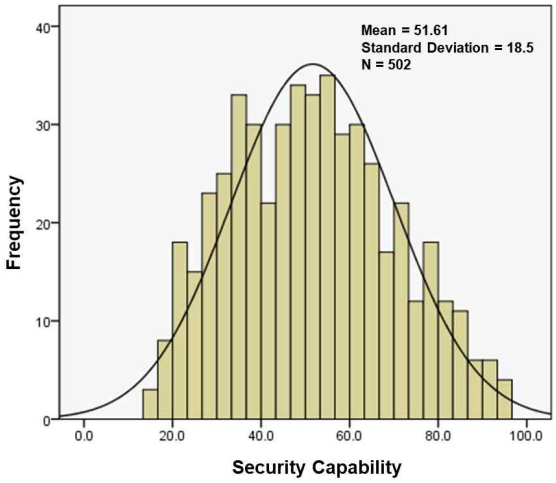

그림 7. 전체 보안역량(의식+체계) 수준
Fig. 7. Overall security capability level (consciousness + system)

The security capability level by enterprise scale showed that SMEs scored 50.16 points, which was classified as the average level, whereas large enterprises scored 71.57, which was the good level. More specifically, the SMEs scored 36.67 points for the security system and 13.49 points for security consciousness, whereas large enterprises scored 56.76 points for the security system and 14.81 points for security consciousness (See Fig. 8).

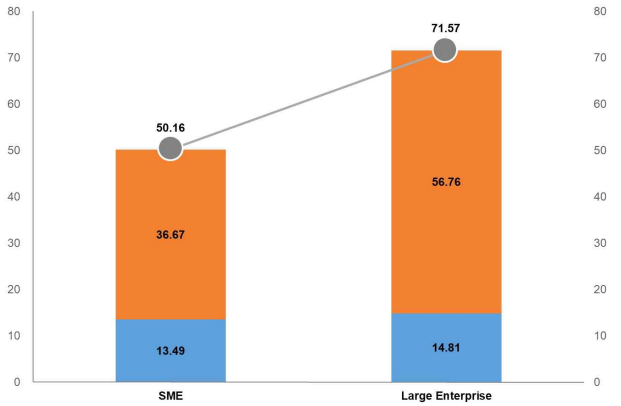

그림 8. 기업규모별 보안역량 수준
Fig. 8. Security capability level by enterprise scale

The analysis results for the security capability by business sector showed that the mechanical material sector was the highest at 54.34 points, followed by the ICT sector at 53.99 points, the electric and electronic sector at 50.96 points, and the chemical textile sector at 48.13 points.

Additionally, the correlation between the security consciousness of organization members and the security system was analyzed. In the individual tier, a correlation of 0.343 ($p < 0.01$) between the "individual security education and training" section and the security system was observed. In the group tier, a correlation of 0.368 ($p < 0.01$) between the "group security regulation execution" section and the security system was observed. A gap analysis of the detailed measurement items of the organization members between top (upper 10%) and bottom (lower 10%) groups was conducted on the basis of the above correlation results for the security consciousness. The highest item of the top group of security capability in organizations was "individual security consciousness" (91.7), and the lowest item was "individual security education and training" (81.7). The highest item of the bottom group was "investment in security by organization" (74.2), and the lowest item was "individual security education and training" (23.3). In addition, the largest difference between the top and bottom groups was found for the item "individual security education and training" at 58.3, whereas the lowest difference was found for "investment in security by organization." In this regard, in-depth interviews were conducted, and the interview results found that the top group of organization security capability constructed a security management system inside the organization first and then efficiently invested to raise individual security as well. Although enterprises whose security capability was low made an effort to invest in security capability, they were limited to the adoption of simple systems only or the operation of temporary measures that incurred an excessive cost investment only at the time of security incidents (See Fig. 9).

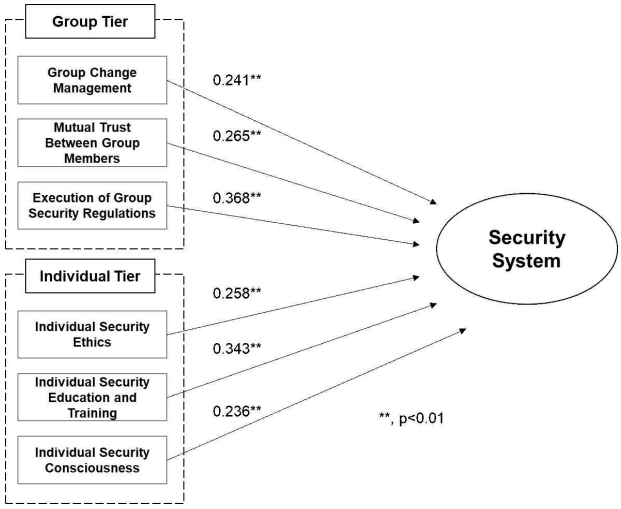

그림 9. 조직 구성원 보안의식과 보안체계와의 상관관계
Fig. 9. Correlation between the security consciousness of organization members and the security system

In order to analyze the maturity according to the security capability of organizations, a K-means clustering analysis was conducted with three (upper, middle, lower) levels first. The K-means clustering analysis is an algorithm that groups the given data into k clusters. It minimizes the variance of the differences in the distance to each cluster. That is, the center of the data is searched with regard to dispersed data first, and data are collected according to the characteristics. Ultimately, the items of improvement (trigger point) that are required for iterative improvements are derived as follows. The analysis results showed that efforts should be made to supply a security system focusing on the "asset management" and "facility management" sections and to improve security consciousness focusing on the "individual security education and training" section in order to upgrade the security from Group 1 to Group 2. Furthermore, the analysis results indicated that the security system level for the sections "response to security incidents" and "IT security management" should be improved, and the security consciousness for the sections of "individual security education and training" and "execution of security regulations within the group" should be strengthened to mature the security capability from Group 2 to Group 3 (See Fig. 10).

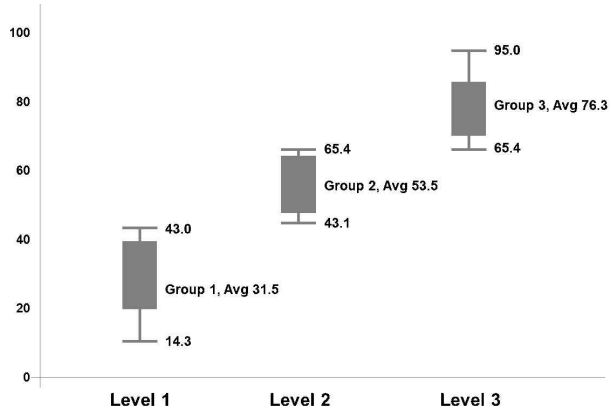

그림 10. 기업규모별 성숙도 분석
Fig. 10. Analysis of the maturity by enterprise scale

Ⅳ. Conclusions and Future Research

Most existing security activities for resolving security incident issues have focused on security measures from technical viewpoints through the adoption and implementation of security systems. However, these approaches have limitations due to difficulties in tracking accidents utilizing state-of-the-art technologies and security incidents such as information leakage via insiders. In particular, information can be infringed upon and leaked easily through the malicious activities of members inside the organization, even if multiple advanced security systems are put into place. In this regard, this study extracted the core factors for forming the security consciousness of organization members and proposed a new evaluation method for the security capability by changing from existing security solutions and regulation-based security capabilities to human-centric security capabilities based on consensus formation. More specifically, the correlation between security consciousness and security system levels was analyzed with regard to 502 organizations and the derived items of improvement after analyzing the security consciousness required to improve the security maturity of organizations for each maturity level. As a result, the following five conclusions were derived.

① The correlation of the security consciousness level of organization members was investigated to improve the level of security system in organizations, and the results showed that a positive (+) correlation was found for all security consciousness components of organization members with an improvement in the security system level. Thus, the above analysis results indicated that the security consciousness level of organization members influenced the level of the security system in organizations.

② This study identified that the level of security consciousness of organization members revealed different characteristics according to the business characteristics and organization scale. The level of security consciousness of organization members was the highest for the electric and electronic sector according to the business characteristics. In addition, large enterprises had high levels of security consciousness of organization members and security capabilities because of their richness in resources. Moreover, SMEs, which had relatively low human resources or budget, had the lowest level of security consciousness, and the largest difference between large enterprises and SMEs was observed for the individual security education and training section. Thus, priority investment in this section would be effective for improving the level of security consciousness of an organization.

③ This study also identified that the level of the security system of an organization revealed different characteristics according to the business characteristics and organization scale. The level of the security system of an organization was the highest for the ICT sector according to the business characteristics. In addition, large enterprises had high levels for the security system of an organization because of their richness in resources. Moreover, the analysis results indicated that all sectors should improve the “response to security incidents” section because it was the lowest level for the security system and the largest difference between large enterprises and SMEs. Thus, increasing the level of this section as a priority would be effective for improving the level of the security system of an organization.

④ The analysis results determined that the improvements in the security consciousness level of individual security education and training were required as a priority to improve the level of the security system in organizations. Furthermore, the analysis results showed that if items that can improve individual security ethics were added when an individual security education and training program was designed, effective performance can be achieved to increase the level of the security system of organizations.

⑤ The items of improvement that were required to improve the maturity for each level were derived when the security capability of organizations was divided into three levels: upper, middle, and lower levels. In order for the lower maturity group to be upgraded to the middle maturity group, a security system focusing on the “asset management” and “facility management” sections should be supplied. Furthermore, in order for the middle maturity group to be upgraded to the upper maturity group, the security system level in the “response to security incidents” and “IT security management” sections should be improved, and the security consciousness in the “individual security education and training” and “execution of security regulations within the group” sections should be strengthened.

This study is expected to contribute to the revision of existing security knowledge or the development of new security knowledge through the interdisciplinary fusion of security theories, which were previously separate owing to the limitations of each academic field. Practically, the results of this study can be used as foundational data to present a fundamental and integrated resolution method for security incidents, which have recently received attention. More specifically, the results of the present study can be used to develop criteria to set an appropriate level of security investment through the evaluation and management activities of the member-centric security consciousness of an organization by extending existing access-control-based security studies. In addition, invested security activities (e.g., behavioral changes in organization members) can be assessed. Because of this, prior consideration of the security consciousness of organization members is essential for security elements such as security policy, security human resources, and the security system to be applied effectively. That is, a single security control environment can be constructed, and a work environment can be provided for responsibility tracking for the cause analysis of security incidents. Moreover, the investment feasibility of the security industry at the government level can be assessed, and efficient management of security policies and support projects can be enabled.

Acknowledgments

This research was supported by the Chung-Ang University Research Scholarship Grants in 2017.

References

[1] R. Ibrahim, I. Primiana, “Influence Business Environment on the Organization Performance,” *International journal of scientific & technology research*, Vol. 4, No. 4, pp. 283~293, 2015.

[2] A. Rizescu, C. Tileag, “Factors influencing continuous organisational change,” *Journal of Defense Resources Management,* Vol. 7, No. 2, pp. 139, 2016.

[3] Y. S. Jee, “Exercise rehabilitation in the fourth industrial revolution,” *Journal of exercise rehabilitation*, Vol. 13, No. 3, pp. 255, 2017.

[4] S. Karnouskos, F. Kerschbaum, “Privacy and integrity considerations in hyperconnected autonomous vehicles,” *Proceedings of the IEEE*, Vol. 106, No. 1, pp. 160~170, 2018.

[5] C. Lee, H. Chang, “A Study on Security Strategy in ICT Convergence Environment,” *The Journal of Supercomputing*, Vol. 70, pp. 211~223, 2014.

[6] N. S. Safa, M. Sookhak, R. Von Solms, S. Furnell, N. A. Ghani, T. Herawan, “Information security conscious care behaviour formation in organizations,” *Computers & Security,* Vol. 53, pp. 65~78, 2015.

[7] J. Choi, M. Che, “An Empirical Study on the Relationship of Personal Optimistic Bias and Information Security Awareness and Behavior in the Activity of Information Ethics,” *Journal of the Korea Academia-Industrial Cooperation Society,* Vol. 17, pp. 538-54, 2016.

[8] N. Choi, D. Kim, A. Whitmore, “Knowing is doing,” I*nformation Management & Computer Security*, Vol. 16, pp. 484-501, 2008.

[9] H. Cavusoglu, J. Son, I. Benbasat, Information Security Control Resource in Organizations: A Multidimensional View and Their Key Drivers, UBC Working Paper, 2009.

[10] K. C. Desouza, “Facilitating Tacit Knowledge Exchange,” *Communications of ACM*, Vol. 46, pp. 85~88, 2003.

[11] A. Neal, M. A. Griffin, P. M. Hart, “The Impact of Organizational Climate on Safety Climate and Individual Behavior,” Safety Science, Vol. 34, pp. 99~109, 2000.

[12] I. Hwang, D. Kim, T. Kim, J. Kim, “Effect of Security Culture on Security Compliance and Knowledge of Employees,” *Information Systems Review*, Vol. 18, pp. 1~23, 2016.

[13] M. Kim, “Determinants of Computer Users’ Safety Behaviors in Korea,” *Information Society & Media*, Vol. 6, pp. 83~104, 2004.

[14] M. Baek, S. Sohn, “A Study on the Effect of Information Security Awareness and Behavior on the Information Security Performance in Small and Medium Sized Organization,” *Asia Pacific Journal of Small Business*, Vol. 33, pp. 113~132, 2011.

[15] H. A. Kruger, W. D. Kearney, “A Prototype for Assessing Information Security Awareness,” *Computer & Security,* Vol. 25, pp. 289~296, 2006.

[16] J. H. P. Eloff, M. Eloff, “Integrated Information Security Architecture,” *Computer Fraud and Security*, Vol. 2005, pp. 10~16, 2005.

[17] J. K. Tudor, Information Security Architecture: An Integrated Approach to Security in the Organization, 6000 Broken Sound Pkwy NW 300, USA: Auerbach Publications Taylor & Francis Group, 2006.

[18] N. Oh, Y. Han, C. Eom, K. Oh, B. Lee, “Developing the Assessment Method for Information Security Levels,” *The Journal of Society for e-Business Studies*, Vol. 16, pp.

159~169, 2011.
[19] M. Ko, H. Kong, T. Kim, “Using a Balanced Scorecard Framework to Evaluate Corporate Information Security Level,” *Telecommunications Review*, Vol. 19, pp. 925~935, 2009.
[20] J. Kim, M. Choi, “A Study on the Evaluation of the Information Security Level of National Organizations,” *Journal of The Korea Institute of Information Security and Cryptology,* Vol. 18, pp. 6~10, 2008.
[21] International Organization for Standardization. ISO/IEC 27001: information technology-security techniques-information security management systems-requirements. ISO, 2005.
[22] M. P. McCarthy, S. Campbell, Security transformation, 2 Pennsylvania Plaza NW 10121, USA: McGraw-Hill, 2001.
[23] S. P. Robbins, T. A. Judge, A. Odendaal, G. Roodt, Organisational Behaviour: Global and Southern African perspectives, 3rd ed. 19 Hertzog Blvd, Cape Town City Centre, Cape Town, 8000, South Africa: Pearson Holdings Southern Africa, 2016.
[24] R. L. Armstrong, “The midpoint on a five-point Likert-type scale,” *Perceptual and Motor Skills*, Vol. 64, No. 2, pp. 359~362, 1987.

나원철(Onechul Na)

2017 : 중앙대학교 융합보안학 석사

2009 ~ 2012 : ㈜알엘케이
2017 ~ 현재 : 중앙대학교 일반대학원 융합보안학과 박사과정
※관심분야 : 산업보안(Industrial Security), 연구보안(Research Security), 기업정보 보안(Corporate Information Security

장항배(Hangbae Chang)

2006 : 연세대학교 정보시스템관리 박사

2007 ~ 2011 : 대진대학교 경영학과 조교수
2012 ~ 2013 : 상명대학교 경영학과 조교수
2014 ~ 현재 : 중앙대학교 산업보안학과 교수
※관심분야 : 산업보안(Industrial Security), 보안 데이터 분석(Security Data Analyzing), 인간중심 보안(Human-Centric Security)