http://www.jsebs.org
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.20, No.3, August 2015, pp.47-58
http://dx.doi.org/10.7838/jsebs.2015.20.3.047

미래 융합보안 인력양성을 위한 보안교육과정 분류체계 설계

Security Knowledge Classification Framework for Future Intelligent Environment

나원철(Onechul Na)*, 이효직(Hyojik Lee)**
성소영(Soyung Sung)***, 장항배(Hangbae Chang)****

초 록

근래에 들어 정보보안 환경이 ICT와 융합됨에 따라 새로운 취약성 지속적으로 증가하고 있다. 이에 따라 새로운 유형의 사이버범죄가 대두되고 있으며 사이버 공격, 내부자 유출 등 보안문제로 인하여 보안사고 사례가 급증하고 있다. 또한 기존의 기술적인 보안위협처럼 취약점을 악용한 외부의 해킹이 아닌 내부직원에 의한 정보유출 등의 신종 보안위협이 등장하고 있으며 산업과 기술이 융합되는 새로운 환경으로 발전함에 따라 그 위협은 더욱 증가하고 있는 실정이다. 따라서, 본 논문에서는 고도화된 정보위협에 능동적으로 대처하기 위한 전문 보안관리 인재를 양성하기 위해 균형있는 정보보호 교과목을 설계하여 정보보호 교과목 분류체계를 도출하고자 하였다. 이를 위해 선행연구조사 분석과 전문가 자문위원회의 회의를 통해 기술적인 교육과 경영・관리적인 교육이 적절히 배분된 정보보호 교과목을 도출하고 국내 실정에 적합한 형태로 분류된 정보보호 직업분류체계와의 연결을 통해 균형감있는 정보보호 교과목 분류체계를 도출하였다. 본 연구결과는 미래 산업융합 환경의 신종 보안위협을 막아낼 수 있는 지능형 보안인재를 양성하는데 긍정적인 효과를 미칠 것으로 기대된다.

ABSTRACT

Recently, new information security vulnerabilities have proliferated with the convergence of information security environments and information and communication technology. Accordingly, new types of cybercrime are on the rise, and security breaches and other security-related incidents are increasing rapidly because of security problems like external cyberattacks, leakage by insiders, etc. These threats will continue to multiply as industry and technology converge. Thus, the main purpose of this paper is to design and present

본 연구는 미래창조과학부산하 정보통신기술진흥센터(IITP)의 방송통신정책연구센터(CPRC) 지원사업의 연구결과로 수행되었음(R0880-15-1007).

* First Author, Department of Security Convergence, Graduate School, Chung-Ang University (nastop@cau.ac.kr)
** Second Author, Department of Security Convergence, Graduate School, Chung-Ang University (leehyojik@cau.ac.kr)
*** Third Author, Department of Security Convergence, Graduate School, Chung-Ang University (bellessy@cau.ac.kr)
**** Corresponding Author, Department of Industrial Security, Chung-Ang University(hbchang@cau.ac.kr)
Received: 2015-06-25, Review completed: 2015-07-30, Accepted: 2015-08-03

security subjects in order to train professional security management talent who can deal with the enhanced threat to information. To achieve this, the study first set key information security topics for business settings on the basis of an analysis of preceding studies and the results of a meeting of an expert committee. The information security curriculum taxonomy is developed with reference to an information security job taxonomy for domestic conditions in South Korea. The results of this study are expected to help train skilled security talent who can address new security threats in the future environment of industrial convergence.

키워드 : 정보보호, 융합, 지식 분류체계, 교육과정, 인간 중심
Information Security, Convergence, Knowledge Classification, Curriculum, Human-centric

1. Research Background and Rationale

Recently, a new type of cybercrime is on the rise stemming from new vulnerabilities due to information security environment changes. The number of security incidents and the damage caused thereby are increasing because of security problems like external cyberattacks using methods such as hacking and virus circulation that exploit the vulnerabilities of information systems, and internal information leakage through the abuse of information systems by authorized users [5]. Recent trends in information security thus need to address both these kinds of vulnerabilities in an environment where they are proliferating due to industry and technology convergence [2, 7, 8].

However, information security personnel training is unsystematic; in particular, existing information security education may concentrate overmuch on developing technology and lack practical applicability in security management and security control. Information security curriculum that balances technical topics with applied information security training, in particular in business settings, is necessary [3, 9].

Accordingly, this paper will design an information security curriculum taxonomy to deliver a balanced treatment of information security subjects in order to train skilled security management talent who can deal with the enhanced information threats that now exist [10, 11]. The paper will research existing information security curriculum and information security job taxonomy in order to develop this approach, and will distribute technical and practical information security topics on the basis of a literature review and expert committee meeting, to foster the development of more effective information security professionals, with a focus on the South Korean context [4, 6].

2. Preceding Studies

The section presents information on in-

formation security curriculum in universities, graduate schools, and professional educational institutions worldwide, with a focus on South Korea. It analyzed 36 domestic (South Korean) institutions and 15 foreign (non-South Korean) institutions, for a total of 51 institutions. With regard to the foreign, 3 were in the United States, 2 in China, 2 in Japan, 2 in the United Kingdom; the foreign institutions also included 4, 3 American and 1 Japanese.

Lee [5] analyzed and classified topics represented in information security courses, based on the US National Initiative for Cybersecurity Education (NICE). Information security jobs were classified into 7 categories: "Within these 7 job categories, a total of 35 information security jobs are included ("Security Provision," 6 jobs with titles like "Security Product Developer" and "Analysis/Design Expert"; under "Protect and Defend, 4 jobs with titles like "Cybersecurity Controller (Security Control Agent)" and "Vulnerability Analysis Expert"; under "Investigate," 2 jobs: "Cybercrime Investigator" and "Digital Forensic Expert"; under "Collect and Operate," 2 jobs: "Encryption/Decryption Expert" and "Malware Analysis Expert" under "Analyze," 7 jobs with titles like "Information System Supervisor" and "Information System Security Inspector"; under "Operate and Maintain," 6 jobs with titles like "Knowledge Manager" and "DB Security Manager" under "Oversight and Development," 8 jobs with titles like "Security Management Planner" and "Compliance Officer").

3. Information Security Curriculum Taxonomy Design and Visualization

3.1 Design and Visualization Methodology

The method adopted to develop and schematically represent the information security curriculum taxonomy presented here has the following features. First, preceding studies about information security curriculum and information security job taxonomy are investigated (in section 2 above). Next, design an information security curriculum suitable for the domestic South Korean situation through the design step 4 based on content analyzed in preceding studies, and have the information security curriculum verified by an expert committee. After that, draw up a final information security curriculum taxonomy with reference to the information security curriculum and the information security job taxonomy.

〈Figure 1〉 Information Security Curriculum Taxonomy Design and Visualization Methodology

3.2 Information Security Curriculum Design and Verification

This section discusses the design and ver-

ification of the information security curriculum.

In the first step, similar topics with different names are integrated into a single subject (under a single name) based on curriculum data. For example, as shown in <Table 1> blow, courses in “Intrusion Detection Systems” at University A in Korea, “Incident Response System Construction” at Institution B in Korea, “Defense Hacking Tactical and Strategy” at foreign University C, and “Advanced Computer Forensic Analysis and Incident Response” at foreign Institution D are integrated. Similarly, “Malware,” “Principles and Response Technology of Hacking” and “Hacker Techniques, Exploits, and Incident Handling” from various institutions are integrated.

In the second step, subjects were grouped on the basis of previous studies into 3 categories: computer engineering, business administration, and information security. These were then subdivided: computer engineering into computer systems and computer programs; business administration into business management and business analysis; and information

〈Table 1〉 Information Security Curriculum Design Step 1

University A in Korea	Institution B in Korea	Foreign University C (International)	Foreign Institution D (International)	Open or not the same subject
Introduction to Information Security	-	Introduction to Information Security Management	Intro to Information Security	O
Intrusion Detection System	Incident Response System Construction	Defence Hacking Tactical and Strategy	Advanced Computer Forensic Analysis and Incident Response	O
Malware	Principle and Response Technology of Hacking	-	Hacker Techniques, Exploits, and Incident Handling	O
Database Security	Finance Security	Telecommunication Management	Network Forensic	X
Advanced Telecommunication Security	Knowledge Information Security Consulting	Statistics for IT Managers	VoIP Security	X
Security Software Development Methodology	Security Control	Economic Analysis	Law of Data Security and Investigations	X
Risk Management	Internet Ethics Education	IT Project Management	Secure Coding in C and C++	X
Information Economics	Secure Server Introduction and Construction	Network Situational Awareness	IT Strategic Planning, Policy and Leadership	X
...				

〈Table 2〉 Information Security Curriculum Design Step 2

Classification	Core subject
Information Security Basic	Introduction to Information Security
	Legal & Ethical Issues in Information Assurance
	Cybercrime
	Cryptography
Information Security Management	Information Security Policy
	Security Management
	Information Security System Administration
	Information System Inspection
	Security Economics
Information Security Level Diagnosis	Penetration Testing
	Security Investigations and Consulting
Cyber Crime and Crisis Response	Hacking and Virus
	Reverse Engineering
	Security Operation
	Cyber Investigations
	Digital Forensics
Information Security System Engineering	Secure Coding
	Information Security System Verification
Technical Information Security System (General)	Electronic Signature
	Computer Security
	Systems Security
	Database Security
	Network Security
The Latest Technical Information Security System	Web Security
	Digital Content Security
	Mobile Security
	Infrastructure Security
	Cloud Security
	Convergence Security
Security System by Field (Specialization)	National Cyber Security
	Information Warfare
	Industrial Security
	Private Security
	E-Commerce Security
	Electronic Finance Security

security into basic information security, information security management, information security level diagnosis, cybercrime and crisis response, information security system engineering, technical information security systems (general), the latest technical information security systems, and security systems by field (specialization). Below, core subjects are reclassified according to these groups in <Table 2>.

In the third step, the information curriculum taxonomy drawn up in step 2 is verified by consultation with an expert advisory committee and in expert interviews; it is ensured that all missing subjects are added. Computer engineering and business administration areas are integrated into a “general information” subject (group) parallel to the specialized subject of information security. An example of this organization of information security subjects is shown in <Table 3> below.

In the fourth step, the preceding studies are organized based on the final verified information security curriculum design plan. Data for final completed curriculum design is broken down by core subjects/similar subjects/preceding study subjects.

A total of 50 subjects-15 general information security subjects and 35 specialty subjects-are drawn through the information security curriculum design step 4. There are 9 general subjects in the computer engineering field, “Computer Structure,” “Operating Systems,” “Databases,” “Computer Networks,” “Computer Program-

ming," "Information Mathematics," "Data Structure," "Computer Algorithms," and "Software Engineering." Business administration general subjects are 6: "Human Resource Administration," "Financial Accounting," "Management Information Systems," "Production Management," "Business Strategy," and "Business Statistics."

Information security specialty subjects are 35: "Introduction to Information Security," "Legal & Ethical Issues in Information Assurance," "Cybercrime," "Cryptography," "Information Security Policy," "Security Management," "Information Security System Administration," "Information System Inspection," "Security Economics," "Penetration Testing," "Security Investigation and Consulting," "Hacking and Viruses," "Reverse Engineering," "Security Operations," "Cyber-Investigation," "Digital Forensics," "Secure Coding," "Information Security System Verification," "Electronic Signatures," "Computer Security," "Systems Security," "Database Security," "Network Security," "Web Security," "Digital Content Security," "Mobile Security," "Infrastructure Security," "Cloud Security," "Convergence Security," "National Cybersecurity," "Information Warfare," "Industrial Security,"

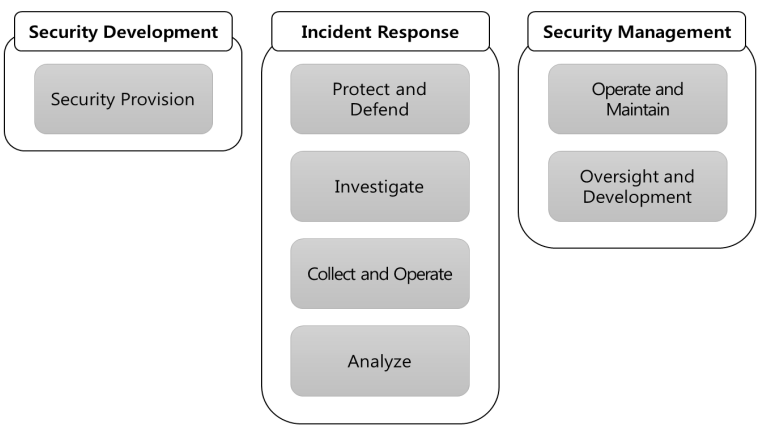
〈Table 3〉 Information Security Curriculum Design Step 3

Classification		Core subject	Similar subject
Information	Information Security Basic	Introduction to Information Security	
		Legal & Ethical Issues in Information Assurance	Information Ethics Cyber Law Copyright Protection and Management
		Cybercrime	Cybercrime Psychology
		Cryptography	Cryptogram Mathematics Cryptogram Algorithm Public Key/Block/Stream/ Quantum Cryptography
	Information Security Management	Information Security Policy	Information Security Policy and Management
			Service Security and Policy
		Security Management	Security Management Certification
			Convergence Security Management
			Personnel Security
		Information Security System Administration	Security Solution Operation Technology
		Information System Inspection	Security Log Analysis
		Security Economics	
	Information Security Level Diagnosis	Penetration Testing	Simulation Hacking
		Security Investigations and Consulting	
...			

"Private Security," "E-Commerce Security," and "Electronic Finance Security."

3.3 Information Security Job Taxonomy and Main Jobs

This study classified jobs on the basis of Lee [5], who translated the convergence-oriented classification by NICE to the Korean context. The categories are as follows: "Security Provision" (conceptualization, design, and construction of IT safety systems, represented by 6 main jobs: "Security Product Developer," "SW Analysis/Design Expert," "SW Developer," "Security Product Technician," "SW Test Technician (Product Quality Manager"); "Protect and Defend" (identification, analysis, and relaxation about threats to IT systems or networks, represented by 4 main jobs: "Cybersecurity Controller (Security Control Agent)," "Vulnerability Analysis Expert," "Simulation Hacking Expert," and "Incident Response Expert"); "Investigate" (investigation of cyber-incidents or crimes in IT systems or networks, represented by 2 main jobs: "Cybercrime Investigator" and "Digital Forensic Expert"); "Collect and Operate" (gathering information including potentially sensitive or secret information, represented by 2 main jobs: "Encryption/Decryption Expert," "Malware Analysis Expert"); "Analyze" (reviewing and evaluating security information, represented by 7 main jobs: "Information System Supervisor," "Information System Security Inspector," "Security Product Certification Expert," "Security Management Certification Expert," "Security Technology Consultant," etc.); "Operate and Maintain" (supporting, managing, and maintaining IT system performance and security, represented by 6 main jobs: "Knowledge Manager," "Database Security Manager," "Information System (Network) Manager," "Security System Manager," "Privacy Manager," etc.); and "Oversight and Develop-



〈Figure 2〉 Information Security Job Knowledge Classification Draw

ment" (supporting security work overall, represented by 8 main jobs: "Security Management Planner," "Compliance Officer," "Security Training Expert (Change Management Expert)," "Prosecutor/Lawyer Specializing in Security," "Privacy Expert," etc.).

3.4 Curriculum Taxonomy-Job Relationships

The job taxonomy presented in the previous section was connected to our taxonomy of subjects, with each subject weighted according to the expert committee and survey. The result was a final integrated information security curriculum taxonomy. Both core and priority subjects were designated.

Required subjects (and weights) in the job category of "Security Provision" are 18: "Introduction to Information Security" (0.09), "Cryptography" (0.08), "Hacking and Viruses" (0.07), "Reverse Engineering" (0.03), "Secure Coding" (0.09), "Electronic Signatures" (0.02), "Computer Security" (0.08), "Systems Security" (0.10), "Database Security" (0.08), "Network Security" (0.15), "Web Security" (0.05), "Digital Content Security" (0.03), "Mobile Security" (0.04), "Infrastructure Security" (0.02), "Cloud Security" (0.01), "Convergence Security" (0.01), "E-Commerce Security" (0.02), and "Electronic Finance Security" (0.02). The core subject is "Secure Coding" and priority subjects are "Electronic Signatures," "Computer Security," "Systems Security," "Database Security," "Network Security," "Web Security," "Digital Content Security," "Mobile Security," "Infrastructure Security," "Cloud Security," and "Convergence Security."

Required subjects in the job category of "Protect and Defend" are 11: "Introduction to Information Security" (0.06), "Legal & Ethical Issues in Information Assurance" (0.08), "Cybercrime" (0.08), "Cryptography" (0.06), "Information System Inspection" (0.09), "Hacking and Viruses" (0.17), "Reverse Engineering" (0.08), "Security Operations" (0.09), "Penetration Testing" (0.17), "National Cybersecurity" (0.05), and "Information Warfare" (0.06). The core subject is "Security Operations" and priority subjects are "Hacking and Viruses," "Reverse Engineering," and "Penetration Testing."

Required subjects in the job category of "Investigate" are 6: "Introduction to Information Security" (0.15), "Legal & Ethical Issues in Information Assurance" (0.18), "Cybercrime" (0.18), "Cryptography" (0.13), "Cyber-Investigations" (0.18), and "Digital Forensics" (0.18). The core subject is "Cyber-Investigations" and the sole priority subject is "Digital Forensics."

Required subjects in the job category of "Collect and Operate" are 10: "Introduction to Information Security" (0.06), "Legal & Ethical Issues in Information Assurance" (0.07), "Cybercrime" (0.08), "Cryptography" (0.11), "Information System Inspection" (0.12), "Hacking and Viruses" (0.17), "Reverse Engineering" (0.13), "Penetration Testing" (0.18), "National Cybersecurity" (0.05), and "Information Warfare"

〈Table 4〉 Information Security Curriculum Taxonomy

Classification	Subject	Weight	Classification	Subject	Weight
Security Provision	*Secure Coding*	0.09	Protect and Defend	*Security Operation*	0.09
	Electronic Signature	0.02		Hacking and Virus	0.17
	Computer Security	0.08		Reverse Engineering	0.08
	Systems Security	0.10		Penetration Testing	0.17
	Database Security	0.08		Introduction to Information Security	0.06
	Network Security	0.15		Legal & Ethical Issues in Information Assurance	0.08
	Web Security	0.05		Cybercrime	0.08
	Digital Content Security	0.03		Cryptography	0.06
	Mobile Security	0.04		Information System Inspection	0.09
	Infrastructure Security	0.02		National Cyber Security	0.05
	…	…		…	…
Investigate	*Cyber Investigations*	0.18	Collect and Operate	*Reverse Engineering*	0.13
	Digital Forensics	0.18		Cryptography	0.11
	Introduction to Information Security	0.15		Introduction to Information Security	0.06
	Legal & Ethical Issues in Information Assurance	0.18		Legal & Ethical Issues in Information Assurance	0.07
	Cybercrime	0.18		Cybercrime	0.08
	Cryptography	0.13		Information System Inspection	0.12
				Hacking and Virus	0.17
				Penetration Testing	0.18
				National Cyber Security	0.05
				Information Warfare	0.04
	…	…		…	…
Analyze	*Information Security System Verification*	0.14	Operate and Maintain	*Information Security System Administration*	0.06
	Information System Inspection	0.14		Introduction to Information Security	0.05
	Security Investigations and Consulting	0.13		Legal & Ethical Issues in Information Assurance	0.05
	Introduction to Information Security	0.06		Cybercrime	0.01
	Legal & Ethical Issues in Information Assurance	0.09		Information Security Policy	0.08
	Hacking and Virus	0.06		Security Management	0.09
	Digital Forensics	0.07		Information System Inspection	0.07
	Penetration Testing	0.10		Hacking and Virus	0.05
	Industrial Security	0.06		Security Operation	0.03
	Private Security	0.08		Penetration Testing	0.04
	…	…		…	…
Oversight and Development	*Security Economics*	0.04	※ Subjects are shown in italics refers to the core, Subjects are shown in shading refers to the priority		
	Information Security Policy	0.12			
	Security Management	0.17			
	Introduction to Information Security	0.08			
	Legal & Ethical Issues in Information Assurance	0.10			
	Cybercrime	0.03			
	Information Security System Administration	0.13			
	Information System Inspection	0.13			
	Security Operation	0.06			
	Security Investigations and Consulting	0.13			
	…	…			

(0.04). The core subject is “Reverse Engineering” and the sole priority subject is “Cryptography.”

Required subjects in the job category of “Analyze” are 12: “Introduction to Information Security” (0.06), “Legal & Ethical Issues in Information Assurance” (0.09), “Information System Inspection” (0.14), “Hacking and Viruses” (0.06), “Digital Forensics” (0.07), “Information Security System Verification” (0.14), “Penetration Testing” (0.10), “Security Investigation and Consulting” (0.13),” “Industrial Security” (0.06), “Private Security” (0.08), “E-Commerce Security” (0.02), and “Electronic Finance Security” (0.06). The core subject is “Information Security System Verification” and priority subjects are “Information System Inspection” and “Security Investigation and Consulting.”

Required subjects in the job category of “Operate and Maintain” are 28: “Introduction to Information Security” (0.05), “Legal & Ethical Issues in Information Assurance” (0.05), “Cybercrime” (0.01), “Information Security Policy” (0.08), “Security Management” (0.09), “Information Security System Administration” (0.06), “Information System Inspection” (0.07), “Hacking and Viruses” (0.05), “Security Operations” (0.03), “Penetration Testing” (0.04), “Security Investigation and Consulting” (0.07), “Electronic Signatures” (0.00), “Computer Security” (0.06), “Systems Security” (0.05), “Database Security” (0.05), “Network Security” (0.07), “Web Security” (0.03), “Digital Content Security” (0.01), “Mobile Security” (0.02), “Infrastructure Security” (0.01), “Cloud Security” (0.03), “Convergence Security” (0.02), “National Cybersecurity” (0.01), “Information Warfare” (0.00), “Industrial Security” (0.01), “Private Security” (0.03), “E-Commerce Security” (0.00), and “Electronic Finance Security” (0.00). The core subject is “Information Security System Administration,” and no priority subject is selected.

Finally, required subjects in the job category of “Oversight and Development” are 10: “Introduction to Information Security” (0.08), “Legal & Ethical Issues in Information Assurance” (0.10), “Cybercrime” (0.03), “Information Security Policy” (0.12), “Security Management” (0.17), “Information Security System Administration” (0.13), “Information System Inspection” (0.13), “Security Economics” (0.04), “Security Operations” (0.06), and “Security Investigation and Consulting” (0.13). The core subject is “Security Economics” and priority subjects are “Information Security Policy” and “Security Management.”

The final information security curriculum taxonomy is shown in truncated form in <Table 4> below.

4. Conclusion

This study has developed an information security curriculum taxonomy for 6 job categories, including required, core, and priority subjects for each. This taxonomy is expected

to serve as part of an education/training road map for information security jobs in a state of convergence of information security personnel. An expected positive effect of its application is expected be the production of information security talents who can counteract new security threats.

References

[1] Amankwa, E., “A conceptual analysis of information security education, information security training and information security awareness definitions,” IEEE, Internet Technology and Secured Transactions (ICITST), 2014 9th International Conference for, pp. 248-252, 2014.

[2] Brown, M., “Toward a taxonomy of communications security models,” Journal of Cryptographic Engineering, Vol. 3, No. 3, pp. 181-195, 2013.

[3] Dayarathna, R., “Taxonomy for information privacy metrics,” Journal of International Commercial Law and Technology, Vol. 6, No. 4, pp. 194-206, 2011.

[4] Lee, C. S. and Kim, Y. H., “An Analysis of Relationship between Industry Security Education and Capability: Case Centric on Insider Leakage,” The Journal of Society for e-Business Studies, Vol. 20, No. 2, pp. 27-36, 2015.

[5] Lee, Y. S., “A Design on Information Security Occupational Classification for Future Convergence Environment,” The Journal of Society for e-Business Studies, Vol. 20, No. 1, pp. 201-215, 2015.

[6] Long, J. and White, G., “On the global knowledge components in an information security curriculum-a multidisciplinary perspective,” Education and Information Technologies, Vol. 15, No. 4, pp. 317-331, 2010.

[7] Ouedraogo, M., Savola, R. M., Mouratidis, H., Preston, D., Khadraoui, D., and Dubois, E., “Taxonomy of quality metrics for assessing assurance of security correctness,” Software Quality Journal, Vol. 21, No. 1, pp. 67-97, 2013.

[8] Padayachee, K., “Taxonomy of compliant information security behavior,” Computers & Security, Vol. 31, No. 5, pp. 673-680, 2012.

[9] Savolainen, P., Niemelä, E., and Savola, R., “A Taxonomy of Information Security for Service-Centric Systems,” Software Engineering and Advanced Applications, pp. 5-12, 2007.

[10] Smith, K., “Designing flexible curricula to enhance critical infrastructure security and resilience,” International Journal of Critical Infrastructure Protection, Vol. 7, No. 1, pp. 48-50, 2014.

[11] Woodward, B., Imboden, T., and Martin, N. L., “An Undergraduate Information Security Program: More than a Curriculum,” Journal of Information Systems Education, Vol. 24, No. 1, pp. 63-70, 2013.

저 자 소 개

나원철 (E-mail: nastop@cau.ac.kr)
2014년 한성대학교 컴퓨터공학과 졸업
2015년~현재 중앙대학교 융합보안학과 (석사과정)
관심분야 산업보안 메타분석, 빅데이터 분석

이효직 (E-mail: leehyojik@cau.ac.kr)
2015년 숭실대학교 글로벌통상학과 졸업
2015년~현재 중앙대학교 융합보안학과 (석사과정)
관심분야 정보보호, 산업보안, 개인정보보호

성소영 (E-mail: bellessy@cau.ac.kr)
2013년 상명대학교 경영학과 졸업
2015년~현재 중앙대학교 융합보안학과 (석사과정)
관심분야 보안문화, 성과분석 체계, 보안경제성 측정

장항배 (E-mail: hbchang@cau.ac.kr
2006년 연세대학교 정보시스템관리 전공 (박사)
2007년~2011년 대진대학교 경영학과 조교수
2012년~2013년 상명대학교 경영학과 조교수
2014년~현재 중앙대학교 산업보안학과 부교수
관심분야 중소기업 정보보호, 정보 오남용 및 유출방지, 성과분석 체계