J. Inf. Technol. Appl. Manag. 23(4): 127~138, December 2016
http://dx.doi.org/10.21219/jitam.2016.23.4.127

ISSN 1598-6284 (Print)
ISSN 2508-1209 (Online)

사이버보안 교육과정 특성에 따른 교육 프로그램 설계의 필요성에 대한 연구

박기태* · 전효정** · 김태성*** · 김인중****

A Study on the Cybersecurity Workforce Training Program Development by Level of a Characteristic of Training Program

Ki Tae Park* · Hyo-Jung Jun** · Tae-Sung Kim*** · In Jung Kim****

Abstract

The Korean government has implemented various policies such as establishing new major/department and operating a variety of education programs related with cybersecurity. However, it has not yet been constructed virtuous cycle that can provide appropriate education and training to professionals with the high level and quality. In this study, by surveying and analyzing satisfaction about education and training program aimed at employees in public sector who are in charge of cybersecurity, we suggest the direction of education and training for cybersecurity experts required at the national level.

Keywords : Cybersecurity Education and Training, Multiple Regression Analysis, MANOVA

Received : 2016. 11. 22. Revised : 2016. 12. 22. Final Acceptance : 2016. 12. 23.

* Professor of CSTEC, e-mail : parkkt@nsr.re.kr
** Post-Doctor, Department of Information Security Management, Chungbuk National University, e-mail : phdhyo@naver.com
*** Corresponding Author, Professor, Department of MIS, Chungbuk National University, 1 Chungdae-ro, Seowon-gu, Cheongju, Chungbuk, 28644, Korea, Tel : +82-43-261-3343, e-mail : kimts@cbnu.ac.kr
**** Director of CSTEC, e-mail : cipher@nsr.re.kr

1. 서 론

기업활동은 물론 개인생활까지도 인터넷으로 대표되는 사이버 공간에 대한 사회・경제적 의존도가 더욱 심화되고 있다. 포털에서 정보를 얻고, SNS로 실시간 소통을 하며, 인터넷뱅킹으로 금융거래를 하는 등 이제 사이버 공간은 일상생활의 가장 큰 활동 무대가 되고 있으며, 스마트폰 등의 스마트 기기들은 삶의 중요한 수단이 되고 있다. 그러나, 사이버 공간과 스마트 기기 등의 편리성의 이면에는 인터넷 서비스의 각종 취약점을 악용한 악성코드 감염, 개인정보 유출, 스미싱・파밍 등 전자 금융사기 등의 크고 작은 사이버 침해사고가 언제든지 발생가능하다는 위협이 존재한다. 보안업체 카스퍼스키 랩(Kaspersky Lab)의 2015년 2분기 Kaspersky DDoS 인텔리전스 통계 보고서에서는 봇넷 공격을 받은 곳 중 3/4 가량이 10개 국가에 집중되어 있고 그 중 한국은 3위에 올라 있는 것으로 분석한 바 있다[Securelist, 2015].

미국과 영국은 범정부 차원에서 2012년부터 본격적으로 '고도로 숙련된 사이버보안인력 확보'를 주요 아젠다로 추진하고 있다. 미국의 Cyber Corp : SFS, Cyber Challenge, Cyber Operations Academic Program 등과 영국의 사이버공격대응 전문가양성과정(박사급), 사이버보안 학위과정(석박사급) 등이 대표적인 사이버보안 전문 인력 양성 사업이다. 우리나라도 2013년 7월 미래창조과학부가 "화이트 해커 5,000명 육성"을 발표하였고, 2012년부터 사이버보안 전문 인력 양성을 위한 교육 프로그램이 진행되고 있다(K-Shield, Best of Best(BoB), 정보보호 특성화대학 등). 또한, 2014년 12월 발생한 한국수력원자력 원전도면 해킹 사건을 계기로 공공기관의 보안관리 강화를 위한 노력도 가속화되고 있다. 2015년 2월 산업통상자원부는 장관 주재로 "에너지 공공기관 정보보안 체제 강화방안 발표회"를 개최하고 산업부 산하의 17개 에너지 공공기관 및 4개 분야별(전력, 원전, 가스, 난방) 정보보안 체제 강화방안을 발표하였다. 여기에는 2017년까지 정보보안 전담인력을 432명으로 확대하고, 향후 3년간 총 2,457억원의 정보보안 예산을 투입해 정보보안 기반을 대폭 확충하는 내용이 담겨 있다[MOTIE, 2015]. 2015년 3월에는 관계부처 합동으로 "국가 사이버안보 강화방안"이 마련되기도 하였다. 중앙행정기관, 지방자치단체, 주요기반시설에 대한 사이버보안 전담조직을 신설・확대하는 계획인데, 여기에는 정보보호 특기자 전형의 사이버 특화고교 및 대학 확대, 군(軍)에서 전문 인력을 효과적으로 활용할 수 있도록 하는 '한국식 탈피오트' 체계 구축 등의 전문 인력 양성방안이 포함되었다[Evaluation, 2015].

정부의 이러한 노력에도 한국을 겨냥한 국제적인 해커들의 공격 또한 현재진행형인 가운데, 2015년 7월 23일 하루 동안 정부 및 국내 주요기관에 대해 해외에서 사이버 공격이 진행된 건수는 총 100만 건 이상인 것으로 알려져 있다[Chosun, 2015]. 이러한 상황에서 우리나라는 국가적인 차원에서 해킹에 대응할 수 있는 '사이버 전력'도 500여명 수준에 불과한 것으로 알려져 있다[KISA, 2013]. 이는 7,000명의 전문 해커를 보유한 것으로 평가되고 있는 북한이나 4성 장군이 사령관인 미국 '사이버 사령부'의 8만 명이나 최소 18만 명에서 최대 50만 명으로 추정되는 해커를 거느린 중국과는 비교조차 할 수 없는 매우 미약한 수준이라고 할 수 있다[Newscj, 2015].

정부나 민간기업 모두 대상과 파급효과를 고려하지 않은 무차별적 해킹공격이 발생할 때마다 보안전문 인력이 턱없이 부족하다고 토로한다. 그러나, 전문 인력 양성에는 시간이 필요하다. 신규인력 양성에는 최소한 정규교육기관을 졸업

하기까지의 시간이 필요하며, 경력인력 양성에는 전문스킬을 인정받을 수 있는 또는 전문가로서 경력개발하기 위한 추가적인 교육・훈련이 필요하다. 특히, 공공기관은 민간기업에 비해 급여체계의 한계로 인해 고도로 숙련된 보안인력(upper-tier professionals)의 확보가 어려우므로, 원활한 인력확보를 위해 국가 차원의 인력양성 및 기관 내 재교육을 통한 신규인력(entry-level works) 확보에 주안점을 두는 정책 추진이 필요하다[Libiki et al., 2014].

인력의 활용목적을 명확히 하고(직무명세 세분화), 인력의 자질과 능력에 따라 교육을 할 것인지 훈련을 할 것인지, 단기로 할 것인지 장기로 할 것인지 등을 나눠야 한다. 그래야 활용목적에 적합한 인력을 양성할 수 있다. 국민의 안전을 보장하고 세계적인 사이버 전쟁에 대비해야 하는 국가적인 필요와 당위성을 바탕으로, 우리 정부도 범부처적인 협력을 통해 사이버보안 전문 인력 양성에 힘을 기울여야 할 때이다.

본 논문에서는 국내 공공 부문에서 사이버보안 업무를 담당하고 있는 재직자들을 대상으로 시행한 교육・훈련의 내용(특징)에 따른 수강생들의 만족도의 차이를 분석하여 국가 차원에서 필요한 사이버보안 전문 인력 교육·훈련의 방향성을 제시하고자 한다.

2. 문헌연구

정보보호 인력 양성정책에 대한 특히 인력양성을 위한 교육・훈련 프로그램 설계에 대한 그간의 연구도 그 필요성을 강조하고 있는 수준이며 아직 구체적인 방법론이 존재하지는 않는다. 더욱이 대부분의 연구가 신규인력 양성을 주목적으로 하는 대학(원)에서의 보안교육을 위한 전문 커리큘럼 개발에 초점을 맞추고 있으며 재직자 대상의 교육에 대해 다루고 있는 연구는 많지 않다.

Siponen[2000]은 정보보호 교육이 정형화 되지 않았을 뿐만 아니라, 교육을 함에 있어 조직적인 정보보호 문제 해결의 동기와 인식 등이 부족하다고 지적하였다. 정보보호 교육의 새로운 접근방법으로는 기술과 비기술 측면을 적절히 분배해야 하면서, 정부, 산업, 공공기관 등의 정보보호와 관련된 요구사항을 지속적으로 반영한 교육이 진행되어야 한다고 밝혔다. Bishop[2000]은 많은 대학들이 정보보호나 컴퓨터 보안 등의 교육과정에서 기본적인 개념 전달에 치우쳐 있어 학생들이 직접 실습하고 운용할 수 있는 과정이 부족하다고 지적하였다. 이에 효과적인 정보보호 교육과정을 위해 기본개념과 실습과정을 통합할 수 있는 과정의 개발이 필요하다고 주장하였다. Kim[2001]은 교육학 분야에서 다루어 왔던 교육과정 개발의 일반적인 방법론과 국내외 정보보호 교육과정의 특징을 파악하였으며, 학부와 대학원에서의 정보보호 교육 교육과정 모델을 제시하였다. 그리고 학부의 전공과정을 법/경영/행정, 컴퓨터과학/공학, 전자공학, 통신공학, 수학/물리 등으로 나눠 제시하였다.

Yang et al.[2003]은 전국 4년제 주요 대학에 신・증설된 정보보호 관련 학과와 교육과정 현황을 수학, 전자/통신, 컴퓨터공학, 보안복합관련 기타 등으로 나눠 분석하고, 이를 근거로 정보보호 분야의 교육과정에 대한 모델을 제시하였다. Kim et al.[2004]은 한국교육개발원의 교육통계연보를 이용하여 학과명 키워드 검색을 통해 국내 정보보호 관련 학과의 현황을 파악하고, 전문대학/4년제 대학교/대학원(석사, 박사) 등으로 나눠 조사・분석하였다. Rha[2005]는 우리나라는 대학별로 교수 주도로 교육과정이 개발・운영되기 때문에 정보보호 교육과정 교과목 편성 및 운영에 관한 개발 모델이 없음을 지적하였다. 또한,

대학별로 교육과정을 개발・운영하는 한국의 체계와 국가 차원에서 산업체와 협력하여 교육과정을 개발・운영하는 미국체계를 비교・분석함으로써 차이점을 도출하면서 한국도 산업체와 협력하여 정보보호 교육해야 한다고 주장하였다. Conklin[2006]은 대다수의 정보보호 교육과정에 포함되어 있는 졸업작품(캡스톤 코스)을 학생들의 실무역량 강화를 위한 목적으로 활용될 수 있도록 이끌어야 한다고 주장하였다. 또한, 캡스톤 코스 이외에도 스스로 기술을 습득하고 문제해결 능력을 키워나갈 수 있는 교육과정을 확대해야 한다고 하였다. Kung et al.[2006]은 대학에서 정보보안과 관련된 기술적인 스킬만 가르치고 있는데, 실제 산업계 수요조사를 실시해 본 결과 대다수 기업들이 기술적인 스킬뿐만 아니라 비기술적인 스킬을 요구하고 있어 차이가 크다고 주장하였다. 해결책으로는 캡스톤 코스 등 비기술적인 교육과정을 다수 운영함으로써 학생들의 실무능력 향상을 위해 노력해야 한다고 하였다. Lee[2008]는 고등학교와 대학에서 운영되는 정보보호 교육을 분석한 결과 고등학교에서 정보보호 관련 교육이 많이 이뤄지지 않고 있다고 주장하면서, 정보보호 교육은 고등학교에서 시작하여 대학까지 이어지는 연계교육이 시급하다고 하였다. Kim and Baek[2011]은 대학의 정보보호 전문 인력 공급의 지역적 불균형이 상당히 크다고 주장하였다. 또한 정보보호 전문 인력에 대한 요구는 많이 늘어나고 있지만, 그에 반해 수요는 충족시키지 못하는 문제점이 있다고 하면서, 산업계의 수요에 맞는 교육이 실시될 수 있도록 해야 한다고 주장하였다.

Kim et al.[2004]은 교육을 함에 있어 정보보호 교육센터(교육부 산하 교육 공무원을 주 대상으로 정보보호 전문교육 제공)의 교육과정이 교육대상의 수요에 적합하게 운영되고 있는지를 확인하기 위해 수요조사를 실시하고 이를 분석하였다. 그 결과 필요수준의 기술 영역이 담당업무에 따라 차이가 있을 확인하고, 교육대상의 담당업무별(수준과 내용)로 각각의 교육수준에 적합한 교육과정이 차별적으로 운영되어야 한다고 주장하였다.

3. 조사설계 및 조사분석

3.1 조사의 필요성

인터넷상에서의 보안위협은 지속적으로 진화해 나가고 있는데 반해, 보안위협에 대해 국가나 기업 모두 근본적인 원인을 근절하지 못한 채 임기응변 방식의 대응에 머물고 있다. 또한, 인터넷의 복잡성 증가와 네트워크를 이용하는 기업과 디바이스들이 다양해지면서 이전에는 상상하지 못했던 부분에서 보안 문제가 발생하고 있으나, 이를 사전에 탐지하고 분석 할 수 있는 핵심 사이버보안 전문 인력은 세계적으로도 부족한 추세이다.

이러한 상황에서 2014년 10월 설립된 사이버안전훈련센터(www.nisa.or.kr)는 국가 사이버보안강화에 기여하고 나아가 글로벌 훈련 허브로 성장하여 국가 사이버 안보를 굳건하게 만들어 나가기 위한 목적으로 정부 및 공공기관에서 보안업무를 담당하고 있는 재직자들을 대상으로 사이버보안 분야의 전문 교육을 실시하고 있다. 여타 다른 공공 부문의 교육기관과 다른 점은 전문훈련이 가능한 수준의 모의훈련장을 구축하고 다년간의 경험을 갖춘 전문 인력이 상주하여 교육 및 훈련을 나눠 진행한다는 것이다.

국가 사이버안보능력 향상과 전문 인력 양성이라는 목적을 달성해 나가기 위해서는 사이버안전훈련센터의 교육・훈련 과정이 교육대상의 수요에 적합하게 진행되고 있는가에 대한 점검이 필요하며, 그 결과를 지속적으로 교육・훈련 과정의 개발에 반영해 나가는 것이 중요하다. 본

연구에서는 이를 위해 일부 교육·훈련과정의 수강생들을 대상으로 설문조사를 실시하고 이를 분석하여 향후 사이버안전훈련센터의 교육·훈련의 방향성을 제시해 보고자 한다.

3.2 연구조사

사이버안전훈련센터에서 2015년에 진행된 6개 교육·훈련 과정의 수강생들을 대상으로 설문지를 배포하였으며, 수강생의 자유의사에 따라 응답여부를 결정하도록 하였다. 최종 129부를 회수하였으며 불성실 응답 등을 제외하고 총 122부를 분석에 이용하였다.

3.3 조사결과 분석

수강생의 44.3%가 정부부처 소속이며, 83.6%가 실무자급으로 나타났다(<Table 1> 참조). 교육생 중 기타로 응답한 비율이 높은 이유는 훈련센터의 교육 특성상 군소속 인력을 대상으로 시행된 교육이 많은데 군소속 인력들이 모두 기타로 응답하였기 때문이다. 최종전공은 전체의 34.4%가 '전산관련학과', 21.3%가 '통신관련학과'로 응답하였다(<Table 2> 참조). 이를 교육·훈련과정별로 살펴보면, 전산관련학과의 비율이 높으나 암호기술전문훈련과정의 경우 다른 과정에 비해 '정보보호학과'의 비율이 다소 높게 나타난 것이 특징이다.

〈Table 1〉 Institution Type and Position of the Respondents

Category	%	Category	%
① Government Ministry(Central)	21.3	① Practician	83.6
② Government Ministry(Local)	23.0	② Middle Management(section chief, head of a department, etc.)	10.7
③ Public Enterprise	4.9	③ Project Manager(general manager, team leader, etc.)	3.3
④ Quasi-Governmental Institutions, Other Public Institution	15.6	④ Decision Maker(director, etc.)	0.8
⑤ Vendors	-	⑤ Head of Organization	-
⑥ Etc.	35.2	⑥ Etc.	1.6
	100		100

〈Table 2〉 Major of the Respondents

Curriculum / Major	Total (%)	Actual Cyber Training	Cryptography	Security Awareness
① Information Security	4.9	2.2	11.1	-
② Mathematics/Statistics	4.1	4.3	2.2	6.5
③ Electrical and Electronic	10.7	8.7	15.6	6.5
④ Information Communication	21.3	10.9	40.0	9.7
⑤ Data Processing	34.4	54.3	8.9	41.9
⑥ Business	1.6	2.2	2.2	-
⑦ Law	4.1	2.2	6.7	3.2
⑧ Language and Literature	0.8	-	2.2	-
⑨ Social Science	2.5	2.2	-	6.5
⑩ Etc.	15.6	13.0	11.1	25.8
Total(%)	100.0	100	100	100

현재의 주직무는 전체의 42.6%가 '관리 및 운영', 37.7%가 '전략 및 기획' 등으로 응답하였다(<Table 3> 참조). 수강생 대부분이 공공기관 종사자이기 때문에 '마케팅 및 영업' 계열의 업무담당자는 전혀 없는 것으로 보이며, '사고대응' 계열 업무담당자도 거의 없는 것으로 나타났다. 교육·훈련과정의 특성별로 현재의 주직무 구성을 살펴보면, 교육훈련연계과정과 일반 보안교육과정은 '전략 및 기획' 업무 종사자들의 입과 비율이 높았고, 암호기술전문훈련과정의 경우에는 '관리 및 운영' 업무 종사자들의 입과 비율이 높은 것으로 나타나 차이를 보였다. 훈련과정의 경우, 보안에 특화된 실무인력들의 입과가 많았던 때문으로 분석할 수 있다. 실무자급은 '관리 및 운영' 직무 종사자가 많았고, 책임자(중간, 사업)급은 '전략 및 기획' 직무 종사자가 가장 많았다. 특히, '사고대응' 직무와 '평가 및 인증' 직무는 실무자급에서만 종사중인 것으로 나타나 차이를 보였다.

응답자들의 주요 수강목적은 "업무에의 활용"이 41.0%로 가장 높게 나타났다. 교육·훈련과정의 특성을 3개로 분류하여 분석해 보면, '암호기술전문' 과정은 '보안기술능력 향상'과 '업무에의 활용'이 각각 42.2%, '교육훈련연계' 과정은 '보안기술능력 향상'이 39.1%, '일반보안교육' 과정은 '업무에의 활용'이 5.48%로 높게 나타나 과정별로 차이를 보였다(<Table 4> 참조). 암호기술전문 과정은 훈련 중심의 교육으로서 교육대상도 암호를 담당하고 있는 실무인력으로서 그

〈Table 3〉 Position and Curriculum for the Respondents' Major Skills

Major Skill / Category	① Strategic and Planning	③ R&D and Implementation	④ Education and Training	⑤ Management and Operation	⑥ Cyber Incident Response	⑦ Evaluation and Certification	Total (%)
Total(%)	37.7%	6.6%	3.3%	42.6%	4.1%	5.7%	100
Practician	34.3%	3.9%	2.9%	47.1%	4.9%	6.9%	100
Middle Management	53.8%	15.4%	7.7%	23.1%	-	-	100
Project Manager	100.0%	-	-	-	-	-	100
Decision Maker	-	-	-	100.0%	-	-	100
Etc.	-	100.0%	-	-	-	-	100
Actual Cyber Training	47.8%	8.7%	2.2%	37.0%	2.2%	2.2%	100
Cryptography	6.7%	6.7%	4.4%	62.2%	6.7%	13.3%	100
Security Awareness	67.7%	3.2%	3.2%	22.6%	3.2%	-	100

〈Table 4〉 The Purpose of Registration

Category	Total (%)	Characteristics of Education and Training curriculum		
		Cryptography (N = 45)	Actual Cyber Training (N = 46)	Security Awareness (N = 31)
① Improvement in Security Awareness	21.3	15.6	26.1	22.6
② Improvement in Security technical skills	34.4	42.2	39.1	16.1
③ Utilization at Work	41.0	42.2	30.4	54.8
④ Training for promotion	0.8	-	-	3.2
⑤ Acquisition of Security Certificate	-	-	-	-
⑥ Etc.	2.5	-	4.3	3.2
Total(%)	100.0	36.9	37.7	25.4

전문성이 매우 높다고 할 수 있다. 교육훈련연계과정은 교육과 훈련을 배분하여 교육하는 과정으로서 이론과 실습을 적정히 병행하는 과정이다. 일반 보안교육과정은 강의식 교육으로 일반적인 교양수준의 보안교육이 이루어지는 과정이다. 따라서, 응답자들의 주요 수강목적이 교육·훈련별로 차이가 있다는 것은 교육과정의 특성과 전문성의 정도에 따라 교육과정 설계와 수강대상을 달리 운영해야 함을 의미하는 것으로 분석해 볼 수 있다. 암호기술전문 과정의 경우 공공 부문 정보보호 전문 인력 중에서도 특히 전문성의 정도가 높으며, 일반 보안교육과정은 교양과목 수준으로 교육이 이루어진다는 점에서 수강생의 특성을 고려한 다양한 교육과정의 설계가 필요하며, 수강생의 전문성의 정도에 따라서도 교육과정별로 각기 다른 특수성을 지닐 수 있도록 설계해야 한다.

전체 응답자의 87%가 '만족도가 높은 이유'에 대해 응답하였는데(보기 중 중복선택 허용), 전체의 35%가 '강사진의 지도가 훌륭하였음'을 꼽아 강사진의 태도가 전체적인 만족도에 가장 높은 영향을 미친 요소였다는 것을 확인할 수 있다. 또한, 전체 응답자의 14%가 '만족도가 낮은 이유'에 대해 응답하였는데(보기 중 중복선택 허용), 전체의 44%가 '내가 보유한 스킬수준 대비 너무 어려웠음'을 꼽아 난이도가 전체적인 만족도를 낮추는 주요 요인이었다는 것을 확인할 수 있다(<Table 5> 참조).

추가적으로, 강의의 난이도, 강의의 진행속도, 업무에의 활용에 대한 기대정도, 강사의 태도 등이 교육·훈련 과정의 전체적인 만족도에 영향을 미치는지 분석하기 위해 SPSS를 이용하여 다중

〈Table 5〉 The Cause of Satisfaction with CSTEC's Differentiated Actual Level Education and Training

The reason of high satisfaction	%	The reason of low satisfaction	%
① Expectation for high utilization at work	27	① Expectation for rare utilization at work	11
② Suitability for my skill level	9	② Difficultness for my skill level	44
③ Excellence of teaching method	35	③ Lack of teaching method	11
④ Excellence of facilities/procedure/classroom	27	④ Lack of facilities/procedure/classroom	34
⑤ Etc.	2	⑤ Etc.	-
Total	100	Total	100

〈Table 6〉 The Result of Multiple Regression Analysis

Hypothesis 1. Course level will have an effect on Satisfaction. Hypothesis 2. Pace of course will have an effect on Satisfaction. Hypothesis 3. Expectation for utilization at work will have an effect on Satisfaction. Hypothesis 4. Attitude of instructor will have an effect on Satisfaction.						
DV	Category	SE	β	t-value	p-value	TL
Satisfaction	Constant	.562	-	-.427	.670	
	Course level(H1)	.168	-.023	-.218	.828	.331
	Pace of course(H2)	.192	.085	.798	.426	.326
	Expectation for utilization at work(H3)	.102	.197	2.230	.028*	.471
	Attitude of instructor(H4)	.101	.582	6.876	.000**	.511
	$R=.756,\ R^2=.571,\ Adjusted\ R^2=0.557,\ F=38.964,\ p=.000,\ Durbin-Watson=2.037$					

*$p < 0.05$, **$p < 0.01$.

※ Dependent Variable = DV, standard error = SE, Tolerance Limit = TL.

회귀분석을 실시하였다(<Table 6> 참조). 검정결과, 강의난이도가 만족도에 미치는 영향은 t값이 -.218로 나타나 가설 1은 기각되었으며, 강의진행속도의 t값도 .798로 나타나 가설 2도 기각되었다. 업무활용기대가 만족도에 미치는 영향의 t값은 .197로 나타나 채택되었으며, 강사태도 역시 t값이 6.876으로 나타나 채택되었다. 즉, 업무활용기대와 강사태도가 전체적인 교육·훈련 만족도에 영향을 미쳤음을 알 수 있다. 회귀모형은 F값이 p = .000에서 38.964의 수치를 보이고 있으며, 회귀식에 대한 R^2 = .571로 57.1%의 설명력을 보이고 있다. Durbin-Watson은 2.037로 잔차들 간에 상관관계가 없어 회귀모형이 적합한 것으로 나타났다.

교육·훈련과정의 특성에 따라 수료한 교육·훈련 교육과정에 대한 전체적인 만족도, 교육가치(일반사설교육기관 대비 금전적 가치), 차후참여의사(다른 교육·훈련과정에 다시 수강신청할 의사) 등에 차이가 있는지를 분석하기 위해 SPSS를 이용하여 다변량분산분석(MANOVA)을 실시하였다(<Table 7>, <Table 8> 참조). 분석결과, 교육·훈련 과정별 집단에 따른 차이에 대한 Wilk's λ 값은 0.628로 유의수준은 0.001로 나타나 유의수준 0.01을 기준으로 집단 간에 차이가 있는 것으로 나타났다. 개별 종속변수별로 살펴보면(<Table 9> 참조) 단변량 F검정에서 전체만족도, 교육가치, 차후참여의사 모든 변수에 대해 통계적으로 유의한 차이가 있는 것으로 나타났다. 특히, 기술통계량을 기준으로 교육가치에 대해 암호기술전문 과정과 교육훈련연계 과정의 평균은 유사한 수준으로 나타났지만, 일반보안교육 과정의 평균은 확연하게 낮게 나타나 일반적인 수준의 전문성을 보유한 인력들의 경우 수료한 교육·훈련 과정에 대한 만족도도 낮고 그만큼 해당 과정의 금전적 가치도 낮게 인식하고 있음을 알 수 있다.

〈Table 7〉 The Result of Multivariate Analysis of Variance : Descriptive Statistics

Category	Cryptography (N = 45)	Actual Cyber Training (N = 46)	Security Awareness (N = 31)	Total	Score Standard
Whole Satisfaction	5.78	5.25	5.04	5.40	7.00
Value of Education	3.39	3.27	2.35	3.08	4.00
Intention of Future Participation	6.50	5.86	5.81	6.09	7.00

〈Table 8〉 The Result of Multivariate Analysis of Variance : Wilk's λ

	Value	F	HDF	EDF	P-value
curriculum	.828	3 824	6.000	232.0000	.001

*$p < 0.01$.
※ Hypothesis Degree of Freedom = HDF, Error Degree of Freedom = EDF.

〈Table 9〉 The Result of Multivariate Analysis of Variance : Inter-subject Effect

Source	Dependent Variable	Type III SS	DF	Mean Square	F	P-value
Curri-culum	Whole Satisfaction	11.700	2	5.850	5.327	.006
	Value of Education	22.393	2	11.196	5.397	.006
	Intention of Future Participation	12.479	2	6.240	4.924	.009

*$p < 0.01$.

3.4 분석결과의 시사점

교육・훈련과정의 만족도에 대한 다중회귀분석결과는 수강생들의 주요 수강목적이 “업무에의 활용”으로 응답된 결과와 일맥상통하는 결과로서 이는 다음과 같은 시사점을 갖는다. 첫째, 교육・훈련과정 운영에 있어 수강생들의 직무(업무역할)를 분석하고 이를 과정운영에 반영할 수 있는 절차가 필요하다. 이를 위해서는 사이버보안 업무영역을 세분화하여 정의하는 표준직무체계의 개발이 필요하다. 직무체계 개발은 직무수행에 필요한 직무수행능력(수준)의 개발과 직무별 업무소요 지식・기술의 분류 등을 포함한다.

둘째, 정보보호 전문 인력(수강대상)의 수준별로 체계화된 교육・훈련이 제공되어야 한다(<Table 10> 참조). 교육・훈련생별로 보유하고 있는 지식 및 스킬의 수준이 각기 다르고 요구하는 교육・훈련의 수준도 다른데, 이를 측정할 수 없어 개인별 수준과 수요를 반영한 교육・훈련이 이루어지지 못하고 있다. 따라서, 교육・훈련과정에 수강신청을 하기 전에 교육・훈련생의 현재의 지식 및 스킬 수준을 객관적으로 평가할 수 있는 도구의 개발이 필요하다(1차적으로 체크리스트, 2차적으로 시스템 차원의 툴 개발). 교육과정은 보안 분야 기본 지식 및 스킬 교육과 간단한 실습교육 실시(정규교육과정의 교육기관들과 협력체계 구축), 훈련과정은 실전식 훈련 제공 등으로 교육・훈련 목적을 보다 세분화하여야 한다. 셋째, 차세대 사이버안보 리더 육성을 위한 학・연협력 모델의 구축이 필요하다. 학・연협력 모델을 통해 정규교육기관에서의 Level 1/Level 2 인력에 대한 교육을 지원(프로그램 및 교재 개발과 교수인력 파견 등)하고, 교육기관은 Level 3/Level 4 인력을 대상으로 하는 실전훈련에 집중할 수 있어야 한다. 또한, 학・연 협력 교과목의 개설을 통해 이론교육은 해당 대학의 교수가 담당하고 실습은 교육기관에서 파견된 교수가 담당하거나 교육기관에서 직접 훈련을 받는 것도 고려해 볼 수 있다. 이와 함께, 훈련컨설팅을 제공해주는 방안도 고려할 수 있다. 사이버보안 관련학과 및 전공과정의 실습실 운영이나 실습실(훈련장 수준의) 구축에 필요한 컨설팅을 지원할 수 있다. 훈련센터의 인적 네트워크를 기반으로 협력대상 학생들의 커리어패스에 대한 연계 지원도 가능하다. 넷째, 국가 차원에서의 체계적인 인력양성전략 수립을 위한 인력 연구・기획이 필요하

〈Table 10〉 The Classification of Students Level

Level		Definition for Levels	Know-ledge	Expe-rience	Institution
Level 1 (Awareness)	Who want to be Cyder security beginner	Someone understands how the skill should be applied but may have no practical experience of its application	L	-	Formal education (higher education)
Level 2 (Basic Application)	Cyder security beginner	Someone understands the skill and applies it to basic tasks under some supervision	M	L	Private&public educational institution
Level 3 (Skillful Application)	Cyder security practitioners	Someone understands the skill and applies it to complex tasks with no supervision	H	M	Institution with specialized facilities for cyber security training
Level 4 (Expert)	Cyder security Professionals	Someone has experience of applying the skill in circumstances without precedent	H	H	

※ IISP(2010), IISP Information Security Skills Framework[CESG Certified Training(CTT)] Revised.
※ H : High, M : Medium, L : Low.

〈Table 11〉 Comparison of the Domestic Public Sector Cyber Security Educational Institutions

Category	Cyber Security Training and Exercise Center (CSTEC)	Cyber Security Training & Certifications Center (former KISA Academy)	Korea Information Technology Research Institute (KITRI)	The Korea Association for Industrial Technology Security (KAITS)	Financial Security Institute
Feature	Training with scenario (based on actual training)	Training with scenario	Phased mentoring program, projet and practice, follow-up management	Demand-side visit education (Industrial Security)	Theory/practical education related financial security
Educational Place	Own facilities	Theory/practical training facility	Cyber war room	utilization of outside educational place	Theory/practical education facilities, Cyber lecture (Internet)
Main education object	Student, refresher	refresher	Student (or refresher)	refresher	refresher
Main Curriculum	War game for cyber security incidents	K-shield	Best of Best	Next generation CSO education programs, industrial security expert education programs	Finance and Personal Information Security education

※ All information collected at each institution's homepage.

며, 중장기전략의 실행을 위한 훈련교수(훈련별 조교인력 충원 필요) 및 기획・지원인력에 대한 보강이 필요하다. 이를 위해, 중장기적인 교육・훈련체계 개발이 국가전략으로 수립되어야 하며(부처간 협력방안 도출 및 역할분담, 보안인력의 커리어패스 및 경력개발 방향성 제공 등을 위한 체계적인 연구 필요), 보안인력양성을 연구하고 기획하는 전문 인력의 발굴과 전문연구센터((가칭) Cybersecurity Training Research Center)의 설립도 필요하다.

4. 결론 및 향후 연구방향

정부는 사이버보안 교육・훈련의 중요성에 동의하고 다양한 인력양성사업과 인력교육을 위한 정책을 추진 중에 있으며, 다수의 공공 주도의 교육기관이 운영되고 있다(<Table 11> 참조). 본 연구의 조사대상은 훈련・교육과정의 수강생이며, 이들 대부분은 '정부 및 공공기관에 재직중인 보안 담당자 및 관계자'이다. 따라서, 본 연구의 결과를 업체종사인력을 대상으로 하는 교육・훈련 과정의 방향성을 논의하는데 활용하는 데에는 다소 한계점이 있다. 그러나, 교육・훈련 과정의 특성별로 수강생이 원하는 교육목적(해당 과정을 수강하고자 하는 의도)이 각기 다르고 그로 인해 만족도와 차후의 교육계획도 매우 다르다는 분석 결과는 공공 주도의 사이버보안 부분 교육・훈련과 인력양성의 방향성을 설정하는 데에 많은 의의를 줄 수 있을 것으로 기대된다.

References

[1] Bishop, M., "Education in information security", *IEEE of Concurrency*, Vol. 8, No. 4, 2000, pp. 4-8.

[2] Chosun, Korea has been attacked 100 million hacker attack per day, 2015.

[3] Conklin, A., "Cyber defense competitions and

information security education : An active learning solution for a capstone course", Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06), Vol. 9, 2006, pp. 220b-220b.

[4] Evaluation, National cybersecurity ability to react will be reinforced by government, 2015.

[5] Kang, M. H., Jun, H. J., and Kim, T. S., "Difference between information security education demand of information security employees and curriculum of information security education center", *Information Systems Review*, Vol. 16, No. 3, 2014, pp. 179-190.

[6] Kim, C., "A study on information security curriculum development of university", *Korea Institute of Information Security and Cryptology*, Vol. 11, No. 3, 2001, pp. 75-89.

[7] Kim, T. S., Kim, J. H., and Kim, M. J., "Analysis on information security educational institutions with statistical yearbook of education", *The Journal of Korean Institute of Communications and Information Sciences*, Vol. 29, No. 10B, 2004, pp. 880-890.

[8] Kim, J. D. and Baek, T. S., "A study on essential body of knowledge and education certification program for information security professional development", *The Journal of Digital Policy and Management*, Vol. 9, No. 5, 2011, pp. 113-121.

[9] KISA, A Study on the System of Fostering National Cybersecurity Manpower and on Measures for the Utilization Thereof, 2013.

[10] Kung, M., Yang, S. C., and Zhang, Y., "The changing information systems (IS) curriculum : A survey of undergraduate programs in the United States", *Journal of Education for Business*, Vol. 81, No. 6, 2006, pp. 291-300.

[11] Lee, M. K., "Education Contents Research and Presentation for Professional Competent Man Cultivation of Information Security", Master's Degree Thesis of Mokpo National University, 2008.

[12] Libicki, M. C., Senty, D., and Pollak, J., "Hackers Wanted : An Examination of the Cybersecurity Labor Market," RAND Corporation, 2014.

[13] MOTIE, "Motie will innovate cybersecurity scheme of some organizations related with energy policy", 2015.

[14] Newscj, [IT Column] A Study on the System of Fostering National Cybersecurity Manpower and on Measures defence ability, 2013.

[15] Rha, H. M., "An analysis of United States curriculum standard for information systems security professionals", *Journal of Employment and Skills Development*, Vol. 8, No. 2, 2005, pp. 21-46.

[16] Securelist, Kaspersky DDoS Intelligence Report Q2 2015, 2015.

[17] Siponen, M. T., "A conceptual foundation for organizational information security awareness", *Information Management and Computer Security*, Vol. 8, No. 1, 2000, pp. 31-41.

[18] Yang, J. M., Lee, O. Y., Lee, H. W., Ha, J. C., and Yoo, S. J., "A study on analysis and development of education program in information security major", *Journal of the Korea Institute of Information Security and Cryptology*, Vol. 13, No. 3, 2003, pp. 17-16, 2003.

저자소개

No Image

Ki Tae Park

Ki Tae Park received the BS, MS, and Ph. D degrees in computer science from Hanyang University, Republic of Korea, in 2000, 2002, and 2007, respectively. He had worked in Samsung Electronics Co., Ltd.. And He worked as a research of professor from 2009 to 2011 and an assistant professor from 2012 to 2014 at Hanyang University. Since 2014, he has been currently working as a professor of CSTEC at the attached institute of ETRI. His major research interests are in the areas of multimedia security and security education/training.

Hyo-Jung Jun

Hyo-Jung Jun is an postdoctoral researcher in the Department of Information Security Management at the Chungbuk National University in South Korea. She worked at ETRI for four years as a researcher. She earned her doctoral degree and master's degree from the Chungbuk National University. Her main research interests are cybersecurity workforce management, information systems security management scheme and ICT ecology.

Tae-Sung Kim

Tae-Sung Kim has been working for Department of Management Information Systems at Chungbuk National University since September 2000. He received his bachelor, master, and doctoral degrees in engineering from the Department of Management Science at KAIST in 1991, 1993 and 1997. He worked for ETRI as a Senior Researcher from February 1997 to August 2000. His research areas include telecommunications management, information privacy, information security economics. His recent research papers have appeared in international journals, such as European Journal of Operational Research, Journal of the Operations Research Society, Operations Research Letters, Stochastic Analysis and Applications and Journal of Intelligent Manufacturing.

No Image

In Jung Kim

In Jung Kim is currently a director of CSTEC at the Attached Institute of the ETRI an adjunct professor of the Department of Electrical Engineering at Chungnam National University. He also was a private sector council menber at the Conference on Cyberspace in 2013. Additionally, he is the information director of the Korea Association of Cybersecurity Law Policy and a committee member of the National Cybersecurity Forum in the Korean Institute of Information Security and Cryptology.

The photos of authors could not be shown by the authors' request