

타 직업군으로부터의 사이버보안 전문인력으로서의 직무전환을 위한 재교육과정 설계 연구*

지 주 연*, 박 상 호**, 유 하 랑***, 장 향 배****

요 약

최근 제 4차 산업혁명이 도래함에 따라서 기존 산업환경이 기술중심 구조에서 가치중심으로 확장되는 산업융합 환경으로 변화함에 따라 보안위협 또한 융·복합적으로 변화하여 그 범위가 커지고 있다. 이러한 변화에 따라 사이버보안 전문인력의 수요는 매년 증가하고 있지만, 이에 비하여 공급은 매우 부족한 실정이다. 향후 2020년 까지 21,704명의 사이버보안 전문인력이 필요한 것으로 조사되고 있으나, 신규 인력 공급은 11,850명에 그쳐 9,854명의 신규 인력 공급이 부족할 것으로 전망되고 있다. 이러한 수급차 문제를 해결하기 위한 방법으로는 사이버보안 전공교육을 통한 신규인력 양성방법에 관한 연구에 비해 타 직업군의 재직자나 타 학문분야 전공자를 대상으로 하는 재교육형 인력양성방법에 관한 연구는 상대적으로 부족한 실정이다. 따라서 본 논문에서는 국내 교육기관 중 가장 규모가 크고 배출 인력이 많은 인문·사회계열의 대표 전공분야들을 선정하여 각 전공분야의 공통교육과정을 분석한 후, 기존 선행연구를 통해 도출된 사이버보안 전문인력 양성과정과 비교한다. 이를 통해 각 전공분야별 배출인력이 사이버보안 전문인력이 되기 위해 어떠한 과목들에 대한 재교육(추가교육)이 필요할 것인지 분석하여 사이버보안 전문인력 양성을 위한 재교육과정을 설계하고자 한다. 본 연구결과를 활용하여 타 직업군의 재직자나 타 학문분야 전공자를 대상으로 사이버보안 전문인력 재교육과정 운영 시, 교육대상자들에게 필요한 역량을 효율적으로 학습할 수 있게 하는 기초자료로 활용될 것으로 기대되며, 사이버보안 전문인력의 수급차 해소에 기여할 것으로 예상된다.

A Study on the Design of Re-training Courses for Nurturing Cybersecurity Professionals from Other Occupational Groups

Juyeon Ji*, Sangho Park**, Harang Yu***, Hangbae Chang****

ABSTRACT

Recently, with the arrival of the 4th industrial revolution, the security risks are converging and complexly changing, and the demand of cybersecurity experts is increasing. Therefore, in this paper, it is the largest of the domestic educational institutions, it has the largest number of emissions talent, and selects the representative major field of humanities and society. Then, after analyzing the common curriculum in each major field, compare it with the training course of cybersecurity experts derived through existing previous research. Through analysis results, we try to design a retraining course for cybersecurity professional human resources. Utilizing the results of this research, it is expected that it will be used as the basic material necessary for the subjects of the re-curriculum education. It is also expected to contribute to resolving the supply-demand gap of cybersecurity professionals.

Key words : Cybersecurity, Security Education, Human Resource Training, Re-training Course

접수일(2018년 1월 27일), 수정일(1차: 2018년 03월 23일,

계재확정일(2018년 03월 30일)

★ 본 논문은 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음.
(IITP-2017-2014-0-00636)

* 중앙대학교/일반대학원 산업융합보안학과
** 중앙대학교/일반대학원 융합보안학과
*** 중앙대학교/경영경제대학 산업보안학과(교신저자)

1. 서 론

4차 산업혁명이 도래함에 있어 사회 전반에 인공지능, 사물인터넷, 사이버 물리시스템, 빅데이터 등 다양한 기술이 결합된 새로운 산업 생태계환경 조성을 촉진시키고 있으며 사람과 사물, 공간 등이 인터넷을 매개로 연결돼 정보의 생성·수집·공유·활용이 수시로 이뤄지는 ‘초연결사회’로 진입하고 있다. 이는 곧 우리가 지켜내야 할 대상이 단순 컴퓨터나 인터넷 정도가 아니라 이를 매개로한 모든 사람과 사물, 공간으로 범위를 확대하며 보안에서의 큰 위협이 됨을 의미한다[1]. 과거에는 불법적으로 기업의 중요 정보를 획득하려고하는 단순 산업스파이와 같은 위협이 존재하였으나, 현재는 정보기술의 발달과 함께 조직 내의 산업스파이뿐만 아니라, 인터넷으로 연결된 외부에서의 조직적 기술 탈취, 해커의 정보 불법 수집 등 다양한 위협이 발생할 수 있다. 즉, 산업환경 자체가 인터넷에 연결됨으로써 다양한 정보 접근 경로가 노출되고 기존에는 생각지 못한 다양한 형태의 보안 위협이 발생할 수 있다. 이렇게 사이버 위협들이 복잡화, 다양화, 지능화, 지속화됨에 따라 사이버보안 전문인력의 수요는 매년 증가 하는 반면에 공급이 매우 부족한 실정이다. 향후 2020년 까지 21,704명의 사이버보안 전문인력이 필요한 것으로 조사되고 있으나, 신규 인력 공급은 11,850명에 그쳐 9,854명의 신규 인력 공급이 부족할 것으로 전망되고 있으며 자세한 내용은 <Table 1>과 같다 [2].

<Table 1> Cybersecurity Expert Supply and Demand

division	New supply (A)	New demand (B)	Supply vehicle (A-B)	Number of employees (persons)
2016년	2,886	-	-	123,743
2017년	2,915	4,786	-1,871	128,529
2018년	2,945	5,189	-2,244	133,718
2019년	2,977	5,627	-2,650	139,345
2020년	3,013	6,102	-3,089	145,447
17년 Sum	11,850	21,704	-9,854	

이러한 수급차 문제를 해결하기 위한 방법으로는 사이버보안 전공교육을 통한 신규인력 양성방

법과 타 직업군의 재직자나 타 학문분야 전공자를 대상으로 하는 재교육형 인력양성 방법이 있다. 그러나 신규인력 양성을 위한 교육과정 설계나 운영에 관한 연구는 꾸준히 진행되고 있으나, 타 직업군의 재직자나 타 학문분야 전공자를 대상으로 한 재교육형 교육과정 설계나 운영에 관한 연구는 상대적으로 매우 부족한 실정이다.

사이버보안 전문인력의 신규인력 양성만으로는 수급차 문제를 해결하는데 한계가 있으며, 재교육형 인력양성이 함께 뒷받침되어야만 사이버보안 전문인력의 효과적인 공급을 수행할 수 있음에도 불구하고 관련 연구가 매우 부족하여 어려움을 겪고 있다. 따라서 본 논문에서는 사이버보안 전공교육을 통한 신규인력 양성방법과 타 직업군의 재직자나 타 학문분야 전공자를 대상으로 하는 재교육형 인력 양성방법 중에서 상대적으로 연구가 부족한 재교육형 인력양성방법을 연구하고자 한다.

세부적으로, 기존 사이버보안 전문인력 양성을 위한 교육과정 선행연구들을 분석하여 사이버보안 표준교육과정을 도출한 후, 국내 4년제 대학에서 가장 배출(예정)인력이 많은 인문·사회계열의 대표 전공분야들을 선정하여 각 전공분야의 공통 교육과정을 분석한 내용과 비교분석하고자 한다. 사이버보안 표준 교육과정과 인문·사회계열의 대표 전공분야의 공통 교육과정을 비교한 내용을 바탕으로 각 전공분야의 배출인력이 사이버보안 전문인력으로 전환하기 위해서는 어떠한 추가교육이 필요할지, 사이버보안 전문인력의 세부 분야 중 어떠한 분야로 진출하는 것이 가장 효과적일지에 대한 분석을 실시한다.

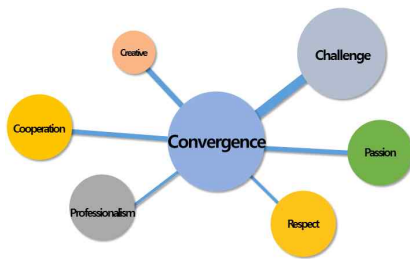
제 4차 산업혁명 시대의 흐름에 따라 융합인재 교육 도입이 확산되고 사회적으로 융·복합적 소양을 지닌 인력을 선호하는 시점에서 인문·사회적 소양을 지닌 기존 인력들을 대상으로 과학기술(공학)과 인문·사회적 소양을 고루 갖출 수 있게 설계된 사이버보안 전문인력 재교육과정을 적용하여 인력을 양성한다면 조직의 업무 프로세스에 적합한 사이버보안 활동을 수행하여 사이버보안 역량을 강화시킬 수 있는 전문인력을 양성할 수 있을 것이다.

2. 선행 연구

2.1 사이버보안 전문인력의 요구역량 분석

사이버보안 관련 조직들이 선호하는 사이버보안 전문인력의 핵심 요구역량을 알아보기 위해, 사이버보안과 관련 있는 여러 조직의 채용공고를 기반으로 키워드 분석을 수행하여 (Figure 1)과 같이 나타내었다. (Figure 1)에서 나타내고 있는 원의 크기는 해당 키워드를 언급한 빈도수를 나타내었으며, 서로 연관성이 있는 키워드들을 선으로 연결하고 연관성의 정도를 선의 굵기로 나타내었다. 키워드 분석 결과 조직에서 요구하는 사이버보안 전문인력의 핵심 역량에서 융합이 가장 빈도수가 많은 것으로 조사되었으며 다음으로 도전, 열정, 협력 등이 나왔다.

이에 따라서 융복합 시대에 사이버보안과 관련된 조직에서 선발하고자 하는 인재를 양성하기 위해서는 융합형 교육이 필요하며, 이러한 실정을 반영하기 위해 문·이과통합 교육이 확정되는 등 변화의 움직임이 나타나고 있다[3]. 융합형인재 양성을 위해서는 교육의 목표와 구체적 실현과정 즉, 교육과정에서 전반적으로 융합형교육이 실시되어야 한다.



(Figure 1) Analyzing the Needs of Cybersecurity Professionals

2.2 NICE(National Initiative for Cybersecurity Education)의 개요

기존 사이버보안 교육 분석 및 표준 교육과정을 개발하기 위해 우선 사이버보안 인력 그리고 지식체계를 정의하고자 한다. 본 연구에서는 국외에서 가장 많이 활용되어지고 신뢰성이 있는 미국

의 NICE(National Initiative for Cybersecurity Education)를 기준으로 사이버보안 인력 및 지식체계를 정의하였다.

NICE는 21세기의 신인 사이버 보안 교육, 훈련, 인식을 통해 국가 보안능력을 갖추고 미국 내의 사이버 보안을 향상하는데 그 목적을 두고 있으며, 온라인 활동의 위협에 대한 미국 내 국민의 인식을 높이고, 사이버 보안 국가를 지원할 숙련된 인력 풀(pool)을 확대하며, 최고의 글로벌 경쟁력을 갖는 사이버보안 인력 을 양성하고 유지하는 것을 목표로 하고있다[4].또한 국가의 디지털 활용능력과 사이버보안 지식의 제도화를 목표로 하고 있으며 '비교할 수 없는, 세계적으로 경쟁력 있는 사이버 보안 인력'을 유지하도록 연방정부에 권고하고 있다.

NICE의 Workforce Framework는 사이버보안과 관련된 업무 및 전문기술을 카테고리 별로 분류하고 특정 업무마다 개인에게 요구되는 역량을 세밀히 분석한 정보보호 지식체계이다. 사이버 영역 전반을 포괄하는 범위에서 사이버보안 인력 양성을 다루기 위한 것으로 각 업무 분류별 세부 직종마다 주요 업무 내용과 필요한 지식 등을 구체적으로 정리하고 기업 및 단체가 현재 필요한 인재를 파악해 추가 인력 확보와 사이버보안 교육 프로그램 기획 등 폭넓게 활용 되도록 제작 되었다[5].이러한 Workforce Framework는 31개 전문영역을 Securely Provisio, Protect and Defend, nvestigate, Collect and Operate, Analyze, Operate and Maintain 그리고 Oversight and Development 7개 분야로 분류하여 제시하고 있으며, 자세한 내용은 <Table 2>와 같다.

<Table 2> NICE Workforce Framework

Categories	Descriptions
Securely Provision (SP)	Conceptualizes, designs, procures, and/or builds secure information technology (IT) systems, with responsibility for aspects of system and/or network development

Operate and Maintain (OM)	Provides the support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.
Oversee and Govern (OV)	Provides leadership, management, direction, or development and advocacy so the organization may effectively conduct cybersecurity work.
Protect and Defend (PR)	Identifies, analyzes, and mitigates threats to internal information technology (IT) systems and/or networks.
Analyze (AN)	Performs highly-specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence
Collect and Operate (CO)	Provides specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.
Investigate (IN)	Investigates cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

2.3 NICE 기반 타 선행연구

2.3.1 정보보호 직업별 교육 훈련 로드맵 구축

한국인터넷진흥원[6] 에서 연구한 정보보호 직업별 로드맵 구축 연구에서는 정보보호 직업분류 체계를 정립함으로써 직업에 따른 단계별 정보보호 지식 습득 체계를 정립하기 위하여 NICE 분류 체계를 기반으로 정보보호 직업별 맞춤형 교육·훈련 로드맵을 구축하였다.

대표직업 7개를 선정하고 직업군별로 필요한 교과목을 도출하였으며 빈도가 높은 직업별 이동 경로를 선정하여 동일 직업군 내 이동 외에 다른 직업군으로 이동할 경우, 추가적으로 학습이 필요한 교과목이 수준별로 기재되어 있다.

정보보호 직업군 설계를 통하여 총 28개의 직업을 도출하고 정보보호 일반 과목 15개와 정보보호 전문 과목 35개를 합하여 정보보호 교과목을 총 50개 도출하였다.

향후 국내 정보보호 교육과정이나 교육기관 제도에 도입이 가능할 것으로 보이며 균형감 있는 정보보호 공학과 경영 공진화 교육 체계 수립이 도움이 될 것으로 보인다. 자세한 내용은 (Figure 2)과 같다.

2.3.2 정보보호 표준 교육과정 정립 및 확산방안 연구 보고서

한국인터넷진흥원[7]에서 연구한 정보보호 표준 교육과정 정립 및 확산방안 연구 보고서에 따르면 교육기관별 상이한 정보보호 교육 시스템을 표준화 하고 이를 확산할 수 있는 방안을 마련하여 학생·대학·산업의 정보 보호 역량 강화 추진을 목표로 하고 있다.

NICE에서 제시한 7가지 직업군 중 제품개발 및 영업을 보안개발자 직업군으로, 분석 및 대응, 관제, 사고조사 및 수사 그리고 코드분석 및 암호해독을 침해사고 대응 전문가 직업군으로 컨설팅, 진단, 평가, 인증 그리고 보안관리 및 운영을 보안관리자 직업군으로 묶어 3가지 직업군 분류체계로 도출하였으며 이 분류 체계를 본 연구에서 도출한 사이버보안 전문인력 교육과정에 적용하였다. 보안개발자 직업군, 침해사고 대응 전문가 직업군 그리고 보안 관리자 직업군별 교과목을 사이버보안 표준교육과정 교과목 모형에 적용하여 도출한 사이버보안 표준교육과정 교과목 로드맵의 상세내용은 <Table 3>과 같다.

<Table 3> Information Security Standard Curriculum Course Roadmap

	Security Developer	Incident Response	Security Management
Fresh man	Introduction to Information Security		
	Information Security Law and Ethics		
	Cybercrime		Cybercrime
	Cryptology		

Sophomore	Digital Forensics		
	Information Security Management System		
	Hacking and Virus		
		Cyber Crisis Management	
		Information Security System Audit	
		Information Security Policy	
		Reverse Engineering	
		Operation and Management of Information Security System	
		Cyber Investigation	
Junior	Network Security		
	Database Security		
	Information Security Diagnosis and Consulting		
	Information Security System Design and Development		Information Security System Design and Development
	System Security		
	Computer Security		
			Risk Management
			Business Continuity
Senior			Evaluation of Information Security System
	Privacy		
	Mobile Security		
	Web Security		
		Convergence Security	
	Digital Content Security		
	Cloud Security		
		Cyber Terrorism and Information Warfare	
			Industrial Security

2.3.3 보안전문인력 양성을 위한 직업분류체계별 정보보호 핵심지식 설계

이효직 외[8]의 정보보호 산업분야 신규 인력 양성을 위한 NICS 기반 교육과정 설계에 관한 연구 예를 보면 정보보호의 직업분류 체계를 미국의 NICE를 기반으로 하여 총 35개의 세분화된 정보보호 직업군을 국내 실정에 적합한 형태로 직업군 및 직업군별 필요역량을 재분류한 후 유사한 직업끼리 묶었다.

크게 Security Provision(개발), Protect and Defend (사전 침투/방어), Investigate(사후 조사), Collect and Operate(수집/해독), Analyze(분석), Operate and Maintain(운영 및 유지보수), Oversight and Development(감독 및 개발)의 7가지 직업군으로 분류하였다[9]. 상세 내용은 <Table 4>와 같다.

<Table 4> Information Security Job Classification Design

Occupational Groups	Occupation
Security Provision	Security Product Developer
	SW Analysis/Design Expert
	SW Developer
	Security Product Engineer
	SW Test Engineer(Quality Manager)
	Security Product Sales Engineer
Protect and Defend	Cyber Security Controller (Security Controller)
	Vulnerability Analyst
	Simulation Hacking Expert
	CERT Expert
Investigate	Cyber Crime Investigator
	Digital Forensic Expert
Collect and Operate	Cryptography Expert
	Malware Analyst
Analyze	Information System Supervisor
	Information System Security Inspector
	Security Product Certification Expert
	Security Management Certification Expert
	Security Technology Consultant
	Security Management Consultant

	Cyber Security Controller(Security Controller)
Operate and Maintain	Knowledge Manager
	DB Security Manager
	Information System(Network) Manager
	Security System Manager
	Personal Information Security Manager
	Security Manager
Oversight and Development	Security Management Director
	Law-abiding monitor
	Security Education Expert (Change Management Expert)
	Security Prosecutor/Lawyer
	Personal Information Security Manager
	Chief Security Manager (Security Strategic Expert)
	Security Professor/Reporter

2.3.4 미래 융합환경 기반의 정보보호 직업군 설계

이윤수 외[10]의 미래 융합환경 기반의 정보보호 직업군 설계연구에서는 정보보호 교과목 분류체계를 도출하였다. 선행연구조사 분석과 전문가 자문 위원회의 회의를 통해 기술적인 교육과 경영·관리적인 교육이 적절히 배분된 정보보호 교과목을 도출하였다.

국내 실정에 적합한 형태로 분류된 정보보호 직업 분류체계와의 연결을 통해 균형감 있는 정보보호 교과목 분류체계를 도출하였다. 상세 내용은 <Table 5>와 같다.

<Table 5> Information Security Core Knowledge Design by Occupational Classification System

Classification	A → B	B → A
Security Development ↔ Incident Response	Security Operation	Cybercrime
	Information System Inspection	Secure Coding
	Information Security Policy	System Security
	Cyber Investigations	Computer Security
	Convergence Security	Digital Content Security

	Information Warfare	Cloud Security
Incident Response ↔ Security Management	Cybercrime	Cryptography
	Secure Coding	Reverse Engineering
	Risk Management	Information Security System Administration
	Business Continuity	Cyber Investigations
	Information Security System Verification	Web Security
	Industrial Security	Information Warfare
Security Management ↔ Security Development	Cryptography	Security Operation
	Reverse Engineering	Information System Inspection
	Information Security System Administration	Information Security Policy
	System Security	Risk Management
	Computer Security	Business Continuity
	Digital Content Security	Information System Security Audit
	Cloud Security	Convergence Security
	-	Industrial Security

2.4 선행연구 분석을 통한 사이버보안 전문인력 교육과정 도출

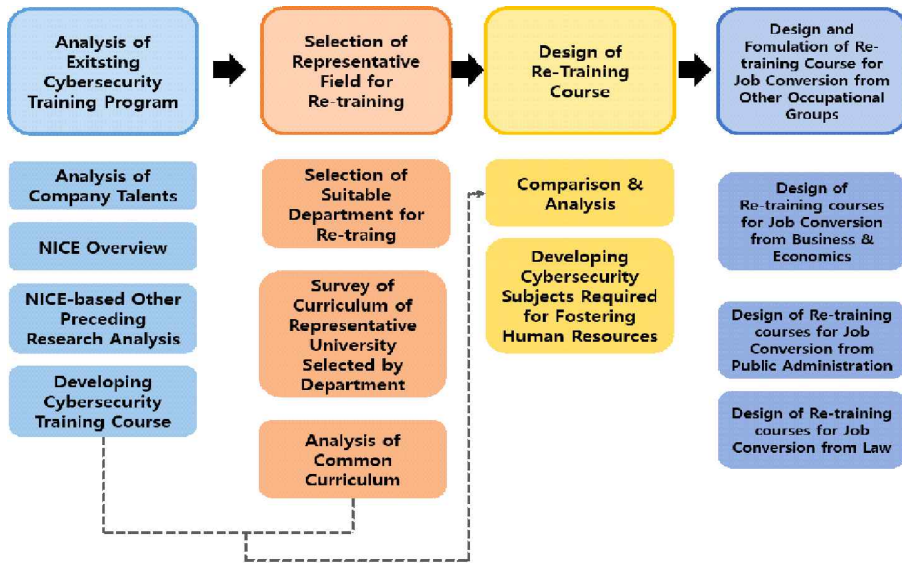
기술혁신과 새로운 산업이 등장하면서 제 4차 산업혁명을 주도하는 혁신기술로 인공지능, 사물인터넷(IoT), 클라우드, 빅데이터, 인공지능(AI) 등이 있다[11]. 이러한 변화에 따라 최신 트렌드가 반영된 국내외 사이버보안 인력양성 교육과정과 선행연구를 분석하여 도출된 사이버보안 전문인력 양성 교육과정에 사물인터넷(IoT)보안, 사이버물리시스템(CPS)보안, 인공지능(AI)보안, 블록체인 보안 과목을 추가하였으며 선행연구에서 언급된 NICE의 7가지 직업군을 보안개발자 직업군 (Security Developer Incident Response Security

Management), 침해사고 대응 전문가 직업군 (Incident Response) 그리고 보안 관리자 직업군 (Security Management) 3가지 직업군으로 묶은 분류를 적용하여 사이버보안 전문인력 교육과정을 도출하였다. 상세한 내용은 <Table 6>와 같다.

<Table 6> Analysis of Preceding Research

Classification	Security Developer	Incident Response	Security Management
Introduction	Introduction to Cybersecurity	Introduction to Cybersecurity	Introduction to Cybersecurity
	Ethics of Cybersecurity Law	Ethics of Cybersecurity Law	Ethics of Cybersecurity Law
	Cybercrime		Cybercrime
	Cryptology	Cryptology	
Foundation			Security Statistics
	Digital Forensic	Digital Forensic	Digital Forensic
	Cybersecurity Management System	Cybersecurity Management System	Cybersecurity Management System
	Hacking and Virus	Hacking and Virus	Hacking and Virus
		Cyber Crisis Management	Cyber Crisis Management
		Cybersecurity System Security Audit	Cybersecurity System Security Audit
		Cybersecurity Policy	Cybersecurity Policy
	Reverse Engineering	Reverse Engineering	
	Operation Management of Cybersecurity System	Operation Management of Cybersecurity System	
		Cyber investigation	
	Network Security	Network Security	Network Security
	Database Security	Database Security	Database Security
	Cybersecurity Diagnosis and Consulting	Cybersecurity Diagnosis and Consulting	Cybersecurity Diagnosis and Consulting
	Cybersecurity System		Cybersecurity System

	Design and Development		Design and Development
	System Security		
	Computer Security		
			Risk Management
			Business Continuity
			Cybersecurity System Assessment
Intensive	Privacy	Privacy	Privacy
	Mobile Security	Mobile Security	Mobile Security
	Web Security	Web Security	
		Convergence Security	Convergence Security
			Security Organization Management
	Digital Content Security		
	Cloud Security		
	IoT Security		
	Cyber Physical System security		
	AI Security		
	Blockchain Security		
		Cyber Terrorism and Information Warfare	Cyber Terrorism and Information Warfare
			Industrial Security
			Security Investment Analysis
	Estimate the Size of Security Accidents	Estimate the Size of Security Accidents	
	Intensive Cybersecurity Law	Intensive Cybersecurity Law	



(Figure 2) Research Methodology

3. 재교육과정 설계

3.1 연구 방법론

본 연구는 (Figure 3)과 같은 연구 방법론에 따라, 타 직업군으로부터 사이버보안 전문인력으로의 직무전환을 위한 재교육과정을 설계하고자 한다. 사이버보안 전문인력 양성을 위한 교육과정을 도출하기 위해 기업의 인재상을 분석하고 21세기의 사이버 보안 교육, 훈련, 인식을 통해 국가 보안능력을 갖추고 미국 내의 사이버 보안을 향상하는데 그 목적을 둔 NICE를 기반한 선행연구들을 분석하여 사이버보안 전문인력 양성을 위한 교육과정을 도출한다. 국내 교육기관 중 배출(예정)인력이 많은 인문·사회계열 전공분야들을 선정하여 각 학과별 재적학생수가 많은 대표 6개 학교의 교육과정을 조사 후 비교·분석하여 공통 교육과정을 도출한다. 선행연구 분석을 통해 도출된 사이버보안 표준 교육과정과 인문·사회계열의 대표 전공분야의 공통 교육과정을 비교한 내용을 바탕으로 각 전공분들의 배출인력이 사이버보안 전문인력으로 전환하기 위해 필요한 추가교육과 어떠한 사이버보안 전문인력의 세부 분야로 진출하는 것이 가장 효과적인지에 대해 분석하여 타직업군으로부터 사

이버보안 전문인력으로의 직무전환을 위한 재교육과정을 설계한다. 자세한 내용은 (Figure 3)과 같다.

3.2 재교육과정 설계를 위한 대표 전공분야 선정

재교육과정을 설계하기 위한 전공분야를 선정하기 위해 국내 4년제 대학교의 인문·사회계열 학과 중 재적학생수가 가장 많은 3개 학과를 선정하고, 해당 학과의 공통교육과정을 도출하기 위하여 해당 학과에서 가장 많은 재적학생수를 가진 6개 대표학교를 선정하여 교육과정 분석 및 공통교육과정을 도출한다.

3.2.1 재교육형에 적합한 학과 선정

대학정보공시 자료는 각 대학이 ‘대학알리미’에 게시한 2017년도 대학정보공시자료를 활용하였다.

대학정보 공시 내용기반으로 4년제 대학교 인문·사회계열의 재적 학생 현황을 조사 하여 나온 데이터이며 전국 대학교들의 재적학생수를 조사한 결과 중 가장 재적학생수가 많은 3개 학과를 선정하였다.

첫 번째로 상위학과인 경영학, 경제학, 무역·유통학의 공통 교육과정을 비교한 결과 교과과목이 중복되고 유사한 교과내용이 다수 포함되어 같은 중분류인

경영·경제로 통합하여 선정하였다. 다음으로 재적 학생수가 많은 행정학을 두 번째로 선정하였으며 세 번째로 재적 학생수가 많은 사회복지학과와 영어·영문학과는 선행연구에서 나온 최종 로드맵과 비교·분석해본 결과 맵핑률이 낮아 재교육형에 적합한 과가 아니라 판단되어 제외하였으며 그다음으로 많은 법학과를 세 번째로 선정하였다. 즉, 재교육형 인재육성에 적합한 학교로 판단되며 재적학생수가 많은 학과로 경영·경제, 행정 그리고 법학으로 선정하였으며 자세한 내용은 <Table 7>과 같다.

<Table 7> Ranking of Students Enrolled in the Department Surveyed

	Category	Department	Rank
Department of Humanities & Social Sciences	Business & Economics	Business	1
		Economics	3
		Trade & Commerce	4
		Finance, Accounting and Taxation	8
		Tourism	10
	Social Science	Public Administration	2
		Social Welfare	5
		Journalism and Mass Communication	9
	Language & Literature	English Language and Literature	6
	Law	Law	7

3.2.2 선정된 학과별 공통교육과정 분석

재적학생수가 많으며 사이버보안 전문인력으로서의 직무전환을 위한 재교육형 인재육성에 적합하다고 판단된 경영·경제, 행정 그리고 법학과를 조사하였다. 이들의 공통 교육과정을 도출하기 위해 각 학과별 재적 학생수가 가장 많은 6개 대학을 선정하여 대학별 교육과정을 조사하였다. 조사된 교육과정을 비교·분석하여 맵핑률이 50%이상인 과목을 공통 교육과정으로 선정하였다. 경영·경제에서는 경영학과와 경제학과 그리고 무역·유통학과 교육과정을 각각 조사하여 맵핑률이 높은 과목을 취합하였다. 경영학과 교육과정조사

를 위해 [C]대학교, [K]대학교, [S]대학교, [H]대학교, [S]대학교 의 경영학과 전공과목을 조사하였으며 경제학 교육과정조사는 [K]대학교, [Y]대학교, [S]대학교, [S]대학교, [K]대학교의 경제학 전공과목을 조사하였다. 그리고 무역·유통학과에서는 [J]대학교, [K]대학교, [G]대학교, [J]대학교, [I]대학교의 교육과정을 조사하였다. 선정된 과목은 경제학원론, 회계학원론, 경영통계학 등이 있다.

이와 같이 도출된 공통교육과정을 선행연구 분석 결과로 도출된 사이버보안 전문인력 양성 교육과정과 비교한 결과, 보안개발자 직업군과 침해사고 대응 전문가 직업군이 되기 위한 교육과정의 사이버보안 시스템 운영관리와 보안 관리자 직업군이 되기 위한 교육과정의 보안통계학, 리스크 매니지먼트, 비즈니스 연속성, 보안 투자효과 분석, 보안사고 피해규모 산정 과목과 유사한 내용을 학습하는 것으로 연결되었다.

행정학과 교육과정 조사를 위해 일반 행정학과와 경찰 행정학과를 분류하여 조사한 후 취합하였다. 일반 행정학과에서는 [K]대학교, [S]대학교, [M]대학교, [I]대학교, [K]대학교, [B]대학교의 행정학과과목을 조사하였다. 선정된 과목은 행정조직론, 인사행정론, 정책학원론 등이 있다.

경찰행정학과로는 [B]대학교, [K]대학교, [J]대학교, [J]대학교, [K]대학교, [D]대학교의 경찰행정학과 과목을 조사하였다. 선정된 과목은 행정조직론, 인사행정론, 정책학원론 등이 있다.

이와 같이 도출된 공통교육과정을 선행연구 분석 결과로 도출된 사이버보안 전문인력 양성 교육과정과 비교한 결과, 보안개발자 직업군이 되기위한 교육과정의 사이버보안 법과 윤리, 사이버 범죄과목, 침해사고 대응 전문가 직업군이 되기위한 교육과정의 사이버보안 법과 윤리, 사이버 수사, 사이버보안 법률 심화과목, 보안 관리자 직업군이 되기위한 교육과정의 사이버보안 법과 윤리, 사이버범죄, 사이버보안 법률 심화 과목과 유사한 내용을 학습하는 것으로 연결되었다. 마지막 학과인 법학과 교육과정 조사를 위해 [J]대학교, [D]대학교, [D]대학교, [S]대학교, [G]대학교, [M]대학교의 법학과 과목을 조사하였다. 선정된 과목은 민법총칙, 헌법, 형법 등이 있다.

이와 같이 도출된 공통교육과정을 선행연구 분석

결과로 도출 된 사이버보안 전문인력 양성 교육과정과 비교한 결과, 보안개발자 직업군이 되기 위한 교육과정의 사이버보안 법과 윤리, 사이버 범죄과목, 침해 사고 대응 전문가 직업군이 되기 위한 교육과정의 사이버보안 법과 윤리, 사이버 수사, 사이버보안 법률 심화과목, 보안 관리자 직업군이 되기 위한 교육과정의 사이버보안 법과 윤리, 사이버범죄, 사이버보안 법률 심화 과목과 유사한 내용을 학습하는 것으로 연결되었다. 공통 교육과정의 상세내용은 <Table 8>과 같다.

<Table 8> Common Curriculum by Department

Business & Economics	Public Administration	Law
Principles of Economics	Administrative Organization Theory	General Civil Law
Principles of Accounting	Personnel Administration	Constitution
Principles of Economics	Principles of Policy	Criminal Law
Financial Management	Financial Administration	Administrative Law
Financial Accounting	Urban Administration	Company Law
Organizational Behavior	Social Welfare Policy	
Marketing	Introduction to Police	
Management Information System	Criminology	
Management Strategy	Criminal Law	
Production Management	Criminal Procedure Law	
International Business	Administrative Law	
Macroeconomics	Investigate	
Microeconomics		
Economic Mathematics		
Business Statistics		
Economic Statistics		

3.3 전공분야별 공통교육과정 재구성

선행연구 분석 결과로 도출 된 사이버보안 전문인력 양성 교육과정과 재교육훈련을 위한 대표 전공분야의 교육과정을 비교 분석 하였다. 학과별 공통 교육과정에서 사이버보안 전문인력 양성 교육과정과 관련 있는 교과목을 선정하여 교과 내용에 따라 표준 교과명으로 재구성 하였다.

경영·경제학과에서는 경영,경제 통계학과목은 보안 통계학으로 경영정보시스템 과목은 사이버보안 시스템 운영관리로 경영전략은 리스크 매니지먼트와 비즈니스 연속성으로 재무관리, 경영통계학, 거시·미시경제학은 보안 투자효과 분석과 보안사고 피해규모 산정으로 연결되었다.

행정학과에서는 범죄학이 사이버범죄로 법관련 과목은 사이버보안 법과 윤리, 사이버보안 법률 심화로 그리고 수사학은 사이버수사로 연결되었다.

마지막으로 법학과의 법관련 과목은 사이버보안 법과 윤리, 개인정보보호 그리고 사이버보안 법률 심화로 연결되었으며 자세한 결과는 <Table 9>과 같다.

<Table 9> Standardization of Common Curriculum by Department

Business & Economics	Public Administration	Law
Security Statistics	Cybersecurity Law and Ethics	Cybersecurity Law and Ethics
Operation Management of Cybersecurity System	Cyber Crime	Privacy
Risk Management	Cyber Investigation	Deepening Cybersecurity law
Business Continuity	Intensive Cybersecurity Law	
Security Investment Analysis		
Estimate the Size of Security Accidents		

3.4 사이버보안 전문인력 양성 재교육과정 최종 설계 및 정립

앞서 도출한 학과별 공통 교육과정사이버보안 전문인력 양성 교육과정을 비교하여 각 학과별로 배우지 않아도 되는 과목들을 표시하였으며 나머지 과목들을 재교육하여 사이버보안 전문인력으로서의 직무전환을 위한 재교육과정을 설계하였다. 또한 교육의 수준을 고려하여 입문, 기초, 심화로 구분하였다.

3.4.1 사이버보안 전문인력으로서의 직무전환을 위한 재교육과정 설계(경영·경제학)

경영·경제학과의 대표 학과를 조사하여 도출된 공통교육과정에는 경제학원론, 회계학원론, 경영통계학 등이 있으며 상세한 내용은 <Table 10>과 같다.

이와 같이 도출된 공통교육과정을 선행연구 분석 결과로 도출된 사이버보안 전문인력 양성 교육과정과 비교한 결과, 보안개발자 직업군과 침해사고 대응 전문가 직업군이 되기 위한 교육과정의 사이버보안 시스템 운영관리와 보안 관리자 직업군이 되기 위한 교육과정의 보안통계학, 리스크 매니지먼트, 비즈니스 연속성, 보안 투자효과 분석, 보안사고 피해규모 산정 과목과 유사한 내용을 학습하는 것으로 연결되며 자세한 내용은 <Table 11>과 같다.

가장 맵핑률이 높은 분야는 보안 관리자 직업군이다. 경영·경제학과 출신자들은 보안 관리자 직업군 재교육이 가장 효과적인 것으로 분석되어진다.

<Table 10> Standardization of Common Curriculum in Business & Economics

Business & Economics		
Security Statistics	Operation management of Cybersecurity System	Risk Management
Business Continuity	Security Investment Analysis	Estimate the Size of Security Accidents

<Table 11> Mapping Result of Common Education Curriculum and Occupational Course by Business & Economics

Classification	Security Developer	Incident Response	Security Management
Introduction	Introduction to Cybersecurity	Introduction to Cybersecurity	Introduction to Cybersecurity
	Ethics of Cybersecurity Law	Ethics of Cybersecurity Law	Ethics of Cybersecurity Law
	Cybercrime		Cybercrime
	Cryptology	Cryptology	
			Security Statistics
Foundation	Digital Forensic	Digital Forensic	Digital Forensic
	Cybersecurity Management System	Cybersecurity Management System	Cybersecurity Management System
	Hacking and Virus	Hacking and Virus	Hacking and Virus
		Cyber Crisis Management	Cyber Crisis Management
		Cybersecurity System Security Audit	Cybersecurity System Security Audit
		Cybersecurity Policy	Cybersecurity Policy
	Reverse Engineering	Reverse Engineering	
	Operation Management of Cybersecurity System	Operation Management of Cybersecurity System	
		Cyber investigation	
	Network Security	Network Security	Network Security
	Database Security	Database Security	Database Security
	Cybersecurity Diagnosis and Consulting	Cybersecurity Diagnosis and Consulting	Cybersecurity Diagnosis and Consulting
	Cybersecurity System Design and Development		Cybersecurity System Design and Development
	System Security		
	Computer Security		

Intensive			Risk Management
			Business Continuity
			Cybersecurity System Assessment
	Privacy	Privacy	Privacy
	Mobile Security	Mobile Security	Mobile Security
	Web Security	Web Security	
		Convergence Security	Convergence Security
			Security Organization Management
	Digital Content Security		
	Cloud Security		
	IoT Security		
	Cyber Physical System security		
	AI Security		
	Blockchain Security		
		Cyber Terrorism and Information Warfare	Cyber Terrorism and Information Warfare
		Industrial Security	
		Security Investment Analysis	
	Estimate the Size of Security Accidents	Estimate the Size of Security Accidents	
	Intensive Cybersecurity Law	Intensive Cybersecurity Law	

3.4.2 사이버보안 전문인력으로서의 직무전환을 위한 재교육과정 설계(행정학)

행정학과의 대표 학과를 조사하여 도출된 공통 교육과정에는 행정조직원, 인사행정론, 정책학원론 등이 있으며 자세한 내용은 <Table 12>과 같다.

이와 같이 도출된 공통교육과정을 선행연구 분석 결과로 도출된 사이버보안 전문인력 양성 교

육과정과 비교한 결과, 보안개발자 직업군이 되기 위한 교육과정의 사이버보안 법과 윤리, 사이버 범죄과목, 침해사고 대응 전문가 직업군이 되기 위한 교육과정의 사이버보안 법과 윤리, 사이버 수사, 사이버보안 법률 심화과목, 보안 관리자 직업군이 되기 위한 교육과정의 사이버보안 법과 윤리, 사이버범죄, 사이버보안 법률 심화 과목과 유사한 내용을 학습하는 것으로 연결되며 자세한 내용은 <Table 13>와 같다.

가장 맵핑률이 높은 분야는 침해사고 대응 전문가 직업군과 보안 관리자 직업군이다. 행정학과 출신자들은 침해사고 대응 전문가 직업군과 보안 관리자 직업군 재교육이 가장 효과적일 것으로 분석되어진다.

<Table 12> Standardization of Common Curriculum in Administration

Public Administration			
Cybersecurity Law and Ethics	Cyber Crime	Cyber Investigation	Intensive Cybersecurity Law

<Table 13> Mapping Result of Common Education Curriculum and Occupational Course by Administration

Classification	Security Developer	Incident Response	Security Management
Introduction	Introduction to Cybersecurity	Introduction to Cybersecurity	Introduction to Cybersecurity
	Ethics of Cybersecurity Law	Ethics of Cybersecurity Law	Ethics of Cybersecurity Law
	Cybercrime		Cybercrime
	Cryptology	Cryptology	
			Security Statistics
Foundation	Digital Forensic	Digital Forensic	Digital Forensic
	Cybersecurity Management System	Cybersecurity Management System	Cybersecurity Management System
	Hacking and Virus	Hacking and Virus	Hacking and Virus
		Cyber Crisis Management	Cyber Crisis Management
		Cybersecurity System Security	Cybersecurity System Security

		Audit	Audit
		Cybersecurity Policy	Cybersecurity Policy
	Reverse Engineering	Reverse Engineering	
	Operation Management of Cybersecurity System	Operation Management of Cybersecurity System	
		Cyber Investigation	
	Network Security	Network Security	Network Security
	Database Security	Database Security	Database Security
	Cybersecurity Diagnosis and Consulting	Cybersecurity Diagnosis and Consulting	Cybersecurity Diagnosis and Consulting
	Cybersecurity System Design and Development		Cybersecurity System Design and Development
	System Security		
	Computer Security		
			Risk Management
			Business Continuity
			Cybersecurity System Assessment
Intensive	Privacy	Privacy	Privacy
	Mobile Security	Mobile Security	Mobile Security
	Web Security	Web Security	
		Convergence Security	Convergence Security
			Security Organization Management
	Digital Content Security		
	Cloud Security		
	IoT Security		
	Cyber Physical System security		
	AI Security		
	Blockchain		

	Security		
		Cyber Terrorism and Information Warfare	Cyber Terrorism and Information Warfare
			Industrial Security
			Security Investment Analysis
		Estimate the Size of Security Accidents	Estimate the Size of Security Accidents
		Intensive Cybersecurity Law	Intensive Cybersecurity Law

3.4.3 사이버보안 전문인력으로서의 직무전환을 위한 재교육과정 설계(법학)

법학과의 대표 학과를 조사하여 도출된 공통교육과정에는 헌법, 민법, 형법 등이 있으며 자세한 내용은 <Table 14>과 같다.

이와 같이 도출된 공통교육과정을 선행연구 분석 결과로 도출된 사이버보안 전문인력 양성 교육과정과 비교한 결과, 보안개발자 직업군이 되기 위한 교육과정의 사이버보안 법과 윤리, 사이버 범죄과목, 침해사고 대응 전문가 직업군이 되기 위한 교육과정의 사이버보안 법과 윤리, 사이버 수사, 사이버보안 법률 심화과목, 보안 관리자 직업군이 되기 위한 교육과정의 사이버보안 법과 윤리, 사이버 범죄, 사이버보안 법률 심화 과목과 유사한 내용을 학습하는 것으로 연결되며 자세한 내용은 <Table 15>와 같다.

가장 맵핑률이 높은 분야는 침해사고 대응 전문가 직업군과 보안 관리자 직업군이다. 법학과 출신자들은 침해사고 대응 전문가 직업군과 보안 관리자 직업군 재교육이 가장 효과적일 것으로 분석되어진다.

<Table 14> Standardization of Common Curriculum in Law

Law		
Cybersecurity Law and Ethics	Privacy	Intensive Cybersecurity Law

<Table 15> Mapping Result of Common Education Curriculum and Occupational Course by Law

Classification	Security Developer	Incident Response	Security Management
Introduction	Introduction to Cybersecurity	Introduction to Cybersecurity	Introduction to Cybersecurity
	Ethics of Cybersecurity Law	Ethics of Cybersecurity Law	Ethics of Cybersecurity Law
	Cybercrime		Cybercrime
	Cryptology	Cryptology	
			Security Statistics
Foundation	Digital Forensic	Digital Forensic	Digital Forensic
	Cybersecurity Management System	Cybersecurity Management System	Cybersecurity Management System
	Hacking and Virus	Hacking and Virus	Hacking and Virus
		Cyber Crisis Management	Cyber Crisis Management
		Cybersecurity System Security Audit	Cybersecurity System Security Audit
		Cybersecurity Policy	Cybersecurity Policy
	Reverse Engineering	Reverse Engineering	
	Operation Management of Cybersecurity System	Operation Management of Cybersecurity System	
		Cyber investigation	
	Network Security	Network Security	Network Security
	Database Security	Database Security	Database Security
	Cybersecurity Diagnosis and Consulting	Cybersecurity Diagnosis and Consulting	Cybersecurity Diagnosis and Consulting
	Cybersecurity System		Cybersecurity System

	Design and Development		Design and Development
	System Security		
	Computer Security		
			Risk Management
			Business Continuity
			Cybersecurity System Assessment
	Privacy	Privacy	Privacy
	Mobile Security	Mobile Security	Mobile Security
	Web Security	Web Security	
		Convergence Security	Convergence Security
Intensive			Security Organization Management
	Digital Content Security		
	Cloud Security		
	IoT Security		
	Cyber Physical System security		
	AI Security		
	Blockchain Security		
		Cyber Terrorism and Information Warfare	Cyber Terrorism and Information Warfare
			Industrial Security
			Security Investment Analysis
		Estimate the Size of Security Accidents	Estimate the Size of Security Accidents
		Intensive Cybersecurity Law	Intensive Cybersecurity Law

5. 결론

사이버 위협의 고도화, 지능화됨에 따라, 사이버 침해사고로 인한 피해사례가 꾸준히 증가하고 있으며 이에 따른 사이버 대응 전문 인력의 수요 또한 급증하고 있다. 하지만, 사이버보안 교육프로그램 관련하여 정확한 업무 구분이나 직무에 대해서 제대로 파악되지 않고 있으며 직무에 맞는 교육과정을 제공하는 것이 쉽지 않은 상황이다.

향후 2020년 까지 21,704명의 사이버보안 전문 인력이 필요한 것으로 조사되고 있으나, 신규 인력 공급은 11,850명에 그쳐 9,854명의 신규 인력 공급이 부족할 것으로 전망되고 있다. 이러한 수급차 문제를 해결하기 위한 방법으로는 사이버보안 전공교육을 통한 신규인력 양성방법과 타 직업군의 재직자나 타 학문분야 전공자를 대상으로 하는 재교육형 인력양성방법이 있지만, 신규인력 양성방법에 관한 연구에 비해 재교육형 인력양성방법에 관한 연구는 상대적으로 부족한 실정이다. 따라서 본 논문에서는 타 직업군의 재직자나 타 학문분야 전공자를 대상으로 사이버보안 양성교육을 실시하는 재교육형 교육과정을 설계 하였다.

각 전공분야의 공통 교육과정을 분석한 결과 경영·경제학과는 경제학원론, 회계학원론, 경영통계학 등이 있었으며, 행정학과는 행정조직론, 인사행정론, 정책채학원론 그리고 법학과는 민법총칙, 헌법, 형법이 있다. 이렇게 도출된 공통 교육과정과 기존 선행연구를 통해 도출된 NICE 기반 사이버보안 전문인력 양성과정을 비교 분석한다.

이를 통해 각 전공분야별 배출인력이 사이버보안 전문인력이 되기 위해 어떠한 과목들에 대한 재교육(추가교육)이 필요할 것인지 분석하여 사이버보안 전문인력의 직무전환을 위한 재교육과정을 설계하였다.

연구결과 경영·경제학과 출신자들은 보안 관리자 직업군으로의 재교육이 사이버보안 전문인력으로서의 직무전환에 가장 효과적인 것으로 분석되었으며 행정학과 출신자들은 침해사고 대응 전문가 직업군과 보안 관리자 직업군 재교육이 사이버보안 전문인력으로서의 직무전환에 가장 효과적인

것으로 분석되어졌다. 마지막으로 법학과 출신자들은 침해사고 대응 전문가 직업군과 보안 관리자 직업군 재교육이 사이버보안 전문인력으로서의 직무전환에 가장 효과적인 것으로 분석되어졌다.

결과적으로 경영·경제학과 출신자들이 보안 관리자 직업군으로 직무전환을 위해서는 사이버보안 개론, 사이버보안 법과 윤리, 사이버 범죄 등 총 16과목을 교육 하였을 때 사이버보안 전문 인력 양성에 도움이 될 것이며, 행정학과 출신자들이 침해사고 대응 전문가 직업군으로 직무전환을 위해서는 사이버보안 개론, 암호학, 디지털포렌식 등 총 19과목, 보안 관리자 직업군으로 직무전환을 위해서 사이버보안 개론, 보안통계학, 디지털포렌식 등 총 23과목을 교육 하였을 때 사이버보안 전문 인력 양성에 도움이 될 것이다. 마지막으로 법학과 출신자들이 침해사고 대응 전문가 직업군으로 직무전환을 위해서는 보보호 개론, 암호학, 디지털포렌식 등 총 19과목, 보안 관리자 직업군으로 직무전환을 위해서 사이버보안 개론, 보안통계학, 디지털포렌식 등 총 23과목을 교육 하였을 때 사이버보안 전문 인력 양성에 도움이 될 것이며 세 학과 출신자들이 사이버보안 전문인력으로서의 직무전환을 위해 필요한 재교육과정은 <Table 16>와 같다.

향후 연구에서는 본 연구에서 설계한 교육과정의 적합성에 대하여 전문가들의 검증할 필요가 있다. 1차 전문가 회의 및 설문조사를 통하여 적합성을 확인하고 부족한 부분을 보완하여 2차 전문가 설문조사 및 라운드 회의를 통해 최종적으로 개선된 재교육과정을 도출해야 할 필요가 있다.

본 연구결과를 활용하여 타 직업군의 재직자나 타 학문분야 전공자를 대상으로 사이버보안 전문인력 재교육과정 운영 시, 교육대상자들에게 필요한 역량을 효율적으로 학습할 수 있게 하는 기초 자료로 활용될 것으로 기대되며, 사이버보안 전문인력의 수급차 해소에 기여할 것으로 기대된다.

<Table 16> Design of Re-training Courses for Job Conversion from Occupational Groups

Classification	Business & Economics → Security Management	Public Administration → Incident Response	Public Administration → Security Management	Law → Incident Response	Law → Security Management
Introduction	Introduction to Cybersecurity	Introduction to Cybersecurity	Introduction to Cybersecurity	Introduction to Cybersecurity	Introduction to Cybersecurity
	Ethics of Cybersecurity Law				
	Cybercrime				Cybercrime
		Cryptology		Cryptology	
			Security statistics		Security Statistics
Foundation	Digital Forensic	Digital Forensic	Digital Forensic	Digital Forensic	Digital Forensic
	Cybersecurity Management System	Cybersecurity Management System	Cybersecurity Management System	Cybersecurity Management System	Cybersecurity Management System
	Hacking and Virus	Hacking and Virus	Hacking and Virus	Hacking and Virus	Hacking and Virus
	Cyber Crisis Management	Cyber Crisis Management	Cyber Crisis Management	Cyber Crisis Management	Cyber Crisis Management
	Cybersecurity System Security Audit	Cybersecurity System Security Audit	Cybersecurity System Security Audit	Cybersecurity System Security Audit	Cybersecurity System Security Audit
	Cybersecurity Policy	Cybersecurity Policy	Cybersecurity Policy	Cybersecurity Policy	Cybersecurity Policy
		Reverse Engineering		Reverse Engineering	
		Operation Management of Cybersecurity System		Operation Management of Cybersecurity System	
				Cyber investigation	
	Network Security	Network Security	Network Security	Network Security	Network Security
	Database Security	Database Security	Database Security	Database Security	Database Security
	Cybersecurity Diagnosis and Consulting	Cybersecurity Diagnosis and Consulting	Cybersecurity Diagnosis and Consulting	Cybersecurity Diagnosis and Consulting	Cybersecurity Diagnosis and Consulting
	Cybersecurity System Design and Development		Cybersecurity System Design and Development		Cybersecurity System Design and Development
			Risk Management		Risk Management
			Business Continuity		Business Continuity
	Cybersecurity System Assessment		Cybersecurity System Assessment		Cybersecurity System Assessment
Intensive	Privacy	Privacy	Privacy		
	Mobile Security	Mobile Security	Mobile Security	Mobile Security	Mobile Security
		Web Security		Web Security	
	Convergence Security	Convergence Security	Convergence Security	Convergence Security	Convergence Security
	Security Organization Management		Security Organization Management		Security Organization Management
	Cyber Terrorism and Information Warfare	Cyber Terrorism and Information Warfare	Cyber Terrorism and Information Warfare	Cyber Terrorism and Information Warfare	Cyber Terrorism and Information Warfare
	Industrial Security		Industrial Security		Industrial Security
			Security Investment Analysis		Security Investment Analysis
		Estimate the Size of Security Accidents	Estimate the Size of Security Accidents	Estimate the Size of Security Accidents	Estimate the Size of Security Accidents
	Intensive Cybersecurity Law				

참고문헌

- [1] Seung-ju Kim, "[CHAPTER 6] Cyber Security Policy in the Age of the Fourth Industrial Revolution," Advance Policy Series, pp. 235-271, 2017.
- [2] Future Creation Science Department, "Survey on the status of supply and demand of information protection personnel," 2016.
- [3] Future Creation Science Department, "SurvJi-Hye Bae, Young-Min Lee, "Analyzing Talent of Top 30 Companies in Korea and Policy Implications for Talent Development," pp. 721-729, 2015ey on the status of supply and demand of information protection personnel," 2016.
- [4] Jun-in Kwon, Soon-tai Park, Seong-jin Ahn "A Study on the Introduction of Domestic Cybersecurity Education with the NICE," Korean Computer Education Society pp. 108-111, 2012
- [5] Won-hyung Park, Seong-jin Ahn, "Enhancing Education Curriculum of Cyber Security Based on NICE," Journal of The Korea Information Processing Society. Computer and communication systems pp. 321-328, 2017.
- [6] Korea Internet Promotion Agency, "Establish roadmap for education and training by occupation," 2013.
- [7] Korea Internet Promotion Agency, "Research Report on Establishment and Proliferation of Information Standard Education Curriculum," 2014.
- [8] Hyojik-Lee, One-chul Na, So-young Sung, Hang-bae Chang, "A Design on Information Security Core Knowledge for Security Experts by Occupational Classification Framework," Journal of Korea Society of Electronic Commerce pp. 113-125, 2015.
- [9] Jeong-Ho Song, Hwang-Rae Kim, "A Study on the NCS based Curriculum for Educating Information Security Manpower," Journal of the Korean Academic Society of Industrial Science, pp. 537-544, 2016.
- [10] Yun-soo Lee, Yong-tae Shin, "A design on information security occupational classification for future convergence environment," Journal of Applied Computer Science, pp. 201-215, 2015.
- [11] Do-Hyun Kim, Hyun-Je Park, "Next-generation IoT technology and services," Electromagnetic wave technology, pp. 2-10, 2016.

————— [저 자 소 개] —————



지 주 연 (Juyeon Ji)

2017년 03월 중앙대학교
산업융합보안학
석사과정
email : juyeonie@cau.ac.kr



박 상 호 (Sangho Park)

2016년 03월 중앙대학교
융합보안학 박사과정
email : sanghopark@cau.ac.kr



유 하 랑 (Harang Yu)

2018년 03월 중앙대학교
융합보안학 석사과정
email : hryu356@cau.ac.kr



장 향 배 (Hangbae Chang)

2006년 02월 연세대학교
정보시스템관리 박사
2014년 03월 중앙대학교
산업보안학과 부교수
email : hbchang@cau.ac.kr