국내 정보보호학과의 교육과정 분석을 통한 개선방안 연구

임원규† · 안성진††

요 약

최근 사이버테러 및 개인정보유출 등의 정보보안관련 이슈가 대두됨에 따라 정보보호 인력 양성을 위해 많은 정보보호관련 학과가 신설되고 있다. 하지만 컴퓨터공학 등의 기존 IT 학과와의 차별성이 부족하고 실제 현장에서 원하는 인재를 양성하지 못하고 있는 실정이다. 이러한 문제를 개선하기 위해 정보보호 직무체계와 각 직무에 필요한 역량 및 기술들을 제시한 기존의 연구를 조사했다. 그리고 미국의 NICE에서 제시된 역량을 중심으로 국내 대학 정보보호관련 학과의 교육과정을 분석했다. 그 결과 정보보호 제품을 개발하는 분야를 위주로 교육과정이 편성되어 있는 것을 확인했고 교육과정이 정보보호 직무체계별 역량을 중심으로 개선할 필요가 있었다. 이 결과를 통해 이후 정보보호 학과의 교육과정 개선을 위한 기초 연구로 활용되고자 한다.

주제어 : 정보보호, 직무체계, 역량중심 교육과정

A Study on Improvements of the Information Security Department via the Curriculum Analysis

Wongyu Lim† · Seongjin Ahn††

ABSTRACT

Accidents for information disclosure occurred in a steady increase, so many information security department has been established recently. But there was a lack of differentiation between department of IT department and they cannot train appropriate students for companies. This research examined the Workforce framework and competencies, the related research for improving information security curriculum. And then this research analyzed status and characteristics of the curriculum to the information security department, based on the Workforce framework and competencies presented by NICE. The result of the research confirmed that the current curriculum mainly consists of courses dealing with development of products that secure information, so the curriculum is needed to improve by focusing on workforce framework competencies. The result will be utilized as fundamental research for improving the curriculum of information security major in the future.

Keywords : Information Security, Workforce Framework, Competency Based Curriculum

† 정 회 원: 성균관대학교 교과교육학과 컴퓨터교육전공 박사수료
†† 종신회원: 성균관대학교 교과교육학과 교수(교신저자)
논문접수: 2014년 9월 1일, 심사완료: 2014년 10월 24일, 게재확정: 2014년 11월 15일

1. 서론

사이버 테러 및 카드사 개인정보 유출 정보보호 관련 이슈가 증가하고 있는 요즘 정보보호 인력에 대한 수요도 꾸준히 증가하고 있다. 이에 따라 대학은 꾸준히 인력을 양성하여 배출하고 있지만, 정작 기업에서는 적절한 인재를 찾는 데 어려움을 겪고 있다. 이러한 불균형이 사회적 쟁점으로 부각되면서 이를 제대로 파악하고 해결하기 위한 다양한 의견들이 제시되고 있다.

그 중에서도 역량을 중심으로 한 교육과정이 하나의 설득력 있는 대안으로 여겨지고 있다. 한국교육개발원의 유현숙이 2011년 '역량기반 교육의 필요성과 시사점'에서 제시한 자료를 통해 보면 대학은 지식과 가치창출이 가능한 창의적 인재를 양성해야하고 사회가 원하는 구체적이고 실질적인 '역량'을 갖춘 인재를 육성하는 기관으로서의 역할을 해야 한다고 주장한다. 또한 동일연구에서 대학교육 평가의 패러다임이 학생들의 역량증진에 기여한 정도를 중심으로 한 성과위주로 변화되고 있는 것이 일반적이 추세라고 제시하고 있다[1].

교육부에서 2013년도 진행한 '핵심역량 중심의 교육과정 재구조화 방안 연구'는 핵심역량을 교육과정에 반영하는 방안을 탐색하고자 하는 연구로, 정부 차원에서도 역량중심의 교육과정을 강조하고 있음을 알 수 있다. 해당 연구에서는 캐나다, 뉴질랜드, 영국, 미국, 핀란드 등의 해외사례를 조사해 국제적 교육과정의 추세가 역량중심으로 재구조화 되고 있음을 보여준다. 연구 내용을 보면 성공적인 삶을 영위하기 위해 역량의 개발을 교육과정의 주요 목표로 삼고, 핵심역량의 설정이나 반영 방식이 절대적인 기준이 아니라 상황과 맥락에 따라 선택되는 것을 주장한다. 추가적으로 핵심역량에 대한 동질성과 당위성 등에 대한 소통이 필요하고, 핵심역량 실천 방식에는 폭 넓은 자율성과 다양성을 강조하는 동시에 책무성을 강화하기 위한 방안도 제시되고 있다[2].

이러한 상황에서 정보보호산업 분야에서도 앞서 말한 역량중심 교육에 필요한 직무체계 및 직무에 필요한 지식과 필요 기술들이 제시되고 있다. 2008년 전효성 등의 연구의 선행연구로 제시된 내용을 보면 최명길, 김세헌(2004)은 관리적 정보보호 대책 수립, 정보보호 정책 수립, 보안감사에 대한 이해, 애플리케이션 보안기술에 대한 이해, 위험 관리 능력, 정보보보 시스템 취약점 분석 능력, Cyber Law에 대한 이해를 필요한 기술 및 지식으로 정의하였고 이외에도 Irvine et al.(1998), Wright(1998), Logan(2002), Cockcroft(2002), Rainer et al.(2007), Cheney, Lyons(1980), Nelson(1991), Trauth et al.(1993), Lee et al(2002), Yen et al.(2003)에 의해 정의된 기술과 지식을 제시한다. 이같이 정보보호산업 분야의 필요 역량에 대한 연구도 지속적으로 이루어지고 있다[3]. 이외에도 정보통신부에서 2004년 제시한 대학IT 인력 전공역량 혁신 방안, 한국직업능력개발원의 IT 전략기획 및 관리 운영 분야 직무능력 모형 개발 및 김태성 교수가 2007년 제시한 정보보호 분야 직무체계 개발을 통한 정보보호 인력의 직무역량 분석 등 다양한 연구에서 직무 역량 위주의 교육과정의 중요성과 필요 지식과 기술이 제시되고 있다.

이외의 연구로 IT 및 정보보호 관련 학과의 교육과정에 대한 연구에 대해 살펴보면 삼성경제연구소의 류지성 연구전문위원은 연구보고서인 "IT 인재 양성을 위한 한국 대학교육의 과제"를 통해 학생 수준과 산업 니즈를 고려한 수요자 중심의 차별화된 교육목표를 수립하고 산업 리더, 실용능력을 갖춘 인재 육성을 목적으로 교육과정이 개성되어야 한다고 주장하고 있다. 그리고 대학의 문제점으로 교수 1인당 학생 수 과다, 프로그램 개발 및 실습 지원 조교 부족, 산업수요에 대한 커리큘럼 부족, 산학 프로그램 부족을 제시하고 있다[4].

2. 관련연구

2.1 역량중심 교육과정 개발 방법론

역량(Competency)은 1970년대 초 사회심리학자인 David McClelland에 의해 처음 소개되었으며, 많은 학자들에 의해 다양하게 정의되었으나 일반적으로 조직 환경 속에서 탁월하고 효과적으로 업무를 수행해 낼 수 있는 조직원의 행동 특성으

로 정의된다.

역량은 목표를 달성할 수 있는 능력으로 직종이나 직책 또는 비즈니스 성격에 따라 다양하게 구성되어질 수 있으며 그 유형에 따라 직무 특성 역량 모델(Job Specific Competency Model), 탁월한 수행자 모델(High Performer Model), 핵심 역량 모델(Core Competency Model), 과정 역량 모델(Process Competency Model) 등 다양한 역량 모델을 개발할 수 있다[5].

전통적인 수업체계설계 모델로서는 기업의 경영성과 향상에 한계가 있음을 자각하여, Motorola 대학에서 역량중심의 수행체제 속에서 수업체제 설계 모델을 접목시켜 개발한 기법이 역량중심 교육과정(CBC : Competency Based Curriculum)이다. 이 교육과정은 구성원들의 업무수행능력을 향상시키기 위해 업무기능과 성과에 직접적으로 관련된 교과목을 도출하는 Top-Down 방식의 교육과정을 개발하는 방법이다.

정보보호학과 교육과정이 세분화된 실무 위주로 개선되어야 한다는 주장이 지속적으로 제기되고 있는 시점에서 이를 효과적으로 교육과정에 적용할 수 있는 방법은 역량중심 교육과정 개발 방법론으로 판단된다. 이를 바탕으로 어떤 분야로 정보보호 교육과정을 세분화 하고 그에 적합한 실제 직무는 무엇인지에 대한 조사가 필요하다.

다음 절에서는 교육과정에 반영되어야 하는 직무와 실무에 필요한 역량이 무엇인지 알아 볼 것이다.

2.2 정보보호 직무 체계 및 필요 역량

역량중심의 교육과정을 구축하기 위해 필요한 다음 과정은 정보보호 분야의 직무 분류에 관해 조사하는 것이다. 그래서 이번 절에서는 직무를 분류하고 해당 직무에 필요한 역량 혹은 지식 및 기술이 제시된 연구를 알아본다.

2.2.1 한국인터넷진흥원(KISA) 제시 직무체계

정보보호 분야의 직무 체계는 2013년 한국산업기술진흥원에서 제시한 산업기술분류표에 대분류 정보통신, 중분류 정보보호, 소분류 서비스 및 응용보안, 네트워크 시스템 보안, 공통 보안기술, 산업보안 및 융합보안으로 분류되어 있다[6]. 그리고 2008년 한국인터넷진흥원(KISA)의 위탁을 받아 한국침해사고대응팀협의회(CONCERT)에서 진행한 정보보호 직무체계 개발 및 인력수급 실태 조사에서는 아래 <표 1>과 같이 정보보호 직무를 분류하고 있다.

<표 1> KISA에서 제시된 정보보호 직무체계[6]

직무군	세부직무
전략 및 기획	위험 분석
	정보보호 정책 및 계획 수립
	개인 정보보호 관리
마케팅 및 영업	마케팅 매니지먼트
	기술 영업
연구개발 및 구현	연구개발
	구현
교육 및 훈련	일반일 및 사용자 교육
	전문가 교육
관리 및 운영	프로젝트 관리
	정보인프라 보안관리
	물리적보안
사고 대응	모니터링 및 대응
	디지털 포렌식
	업무 지속성 관리
평가 및 인증	평가인증 및 품질보증
	정보시스템 보안감사

2.2.2 NICE(National Initiative For Cybersecurity Education) 제시 직무체계

해외의 직무분류 연구는 NICE(National Initiative For Cybersecurity Education)에서 발표한 Workforce Framework에 7개의 카테고리와 31개의 세부영역을 제시하고 있다. 20여개 이상의 미연방 부처와 기관 그리고 다수의 공공 및 민간 조직이 참여한 NICE에서 사이버보안 업무를 정의하고 사이버보안의 기반 마련을 위해 National Cybersecurity Workforce framework[7]를 개발했다.

<표 2> NICE에서 제시된 정보보호 직무체계[7]

Categories (직무군)	Specialty areas (세부직무)
Securely Provision (정보보호 제품 및 시스템 개발)	Information Assurance Compliance (정보시스템 인증)
	Software Assurance and Security Engineering (소프트웨어 개발 및 정보보호 공학 기술)

Securely Provision (정보보호 제품 및 시스템 개발)	System Development (시스템 개발)
	System Requirements Planning (시스템 요구분석)
	Systems Security Architecture (보안 시스템 구조)
	Technology Research and Development (최신동향 연구 및 개발)
	Test and Evaluation (테스트 및 평가)
Protect and Defend (네트워크 보안)	Computer Network Defense Analysis (네트워크 위협분석)
	Computer Network Defense Infrastructure Support (기반시설 네크워크 방어)
	Incident Response (사고대응)
	Vulnerability Assessment and Management (취약점 분석 및 관리)
Oversight and Development (정보보호 총괄 및 개발 지원)	Education and Training (교육 및 훈련)
	Information Systems Security Operations (Information Systems Security Officer) (정보시스템 보안 운영)
	Legal Advice and Advocacy (법률 자문)
	Security Program Management (Chief Information Security Officer) (최고정보보호 관리자)
	Strategic Planning and Policy Development (정보보호 전략 기획 및 정책 수립)
Operate and Maintain (관리 및 유지보수)	Customer Service and Technical Support (고객 관리 및 지원)
	Data Administration
	Knowledge Management (지식 경영)
	Network Services (네크워크 서비스)
	System Administration (시스템 관리)
	Systems Security Analysis (시스템 보안 관리)
Investigate (사이버 범죄)	Digital Forensics (디지털 포렌식)
	Investigation (사이버 수사)
Collect and Operate (정보 수집 및 운영)	Collection Operations (데이터 수집 관리)
	Cyber Operations (사이버 범죄 및 테러 관련 증거 수집)
	Cyber Operations Planning (사이버 운영 계획)
Analyze (정보 검토)	All Source Intelligence (정보종합 분석)
	Threat Analysis (위협 분석)
	Exploitation Analysis (공격 분석)
	Targets (신지식 적용)

NICE에서 제시된 직무분류는 Specialty areas (세부직무) 이외에 각 직무에 필요한 KSAs(Knowledges, Skills, Abilities), 역량 그리고 각 분야별 직업까지 정의되어 있어 KISA에서 정의된 것에 비해 구체적이다[7]. 또한 KISA의 직무분류는 정보보호 전문기업을 중심으로 구성되어 있어 정보보호 제품을 사용하는 일반기업에 필요한 역량을 도출해 분류하기는 부족하다. 따라서 NICE에서 제시된 직무체계를 기반으로 연구를 진행 할 것이다.

2.2.3 NICE(National Initiative For Cybersecurity Education) 제시 역량

이번 절에서는 미국의 NICE가 제시한 National Cybersecurity Workforce framework에는 직무별 필요 Competency(역량)을 알아 볼 것이다. 아래 <표 3>에서 NICE에서 제시된 역량들을 확인할 수 있다. <표 3>에 제시된 것은 그 중 일부를 나열한 것이다.

<표 3> Specialty areas별 필요 역량 일부[7]

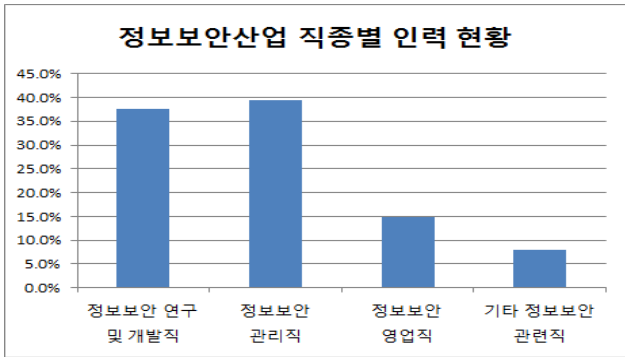
Specialty areas (세부직무)	Competencies(역량)
Information Assurance Compliance (정보시스템 인증)	정보시스템 및 네크워크 보안 형법 정보 보증 네트워크 보안 입찰 및 조달 기업 구조 정보시스템 보안 인증 IT장비 성능 평가 인프라 설계 논리 시스템 설계 기업 의식 위험 관리 보안 규제 시스템 테스트 및 평가 최신 기술 동향

Vulnerability Assessment and Management (취약점 분석 및 관리)	취약점 분석 네트워크 보안 인프라 설계 컴퓨터 언어 인증 관리 정보 보증 정보시스템 및 네트워크 보안 컴퓨터 포렌식 입찰 및 조달 형법 인적요서 시스템 테스트 및 평가
Incident Response (사고 대응)	네트워크 보안 정보 시스템 및 네트워크 보안 정보 보증 컴퓨터 포렌식 사고 관리 인프라 설계 취약점 관리

그리고 각 Specialty areas(세부직무) 별로 필요 Task와 KSAs(Knowledges, Skills, Abilities)들이 조사한 역량의 모델을 제시하고 있다.

2.3 국내 정보보호 산업 분류 및 인력 현황

2013년 지식정보보안산업협회(KISIA)에서 조사된 “2013 국내 정보보호산업 실태조사”에서 제시된 정보보안산업 직종별 인력 현황을 보면 아래 <그림 1>와 같다.



<그림 1 > KISIA에 제시된 직종별 인력 현황[8]

해당 조사에서는 정보보안 제품과 서비스로 정보보호 인력현황을 분류하였다. 정보보호 제품은 네크워크 보안, 시스템 보안, 콘텐츠/정보유출 방지보안, 암호/인증, 보안관리 및 기타제품으로 세분화되어 정보보호 관련 제품의 설계, 기획 및 개발 분야로 위의 <그림 1>에서 정보보안 연구 및 개발직과 정보보안 관리직에 해당한다. 그리고 정보보호 서비스는 정보보안 영업직과 기타 정보보안 관리직으로 보안컨설팅, 유지보수, 보안관제, 교육/훈련 및 인증 서비스로 세분화되어 제시하고 있다[8].

3. 정보보호 교육과정 분석

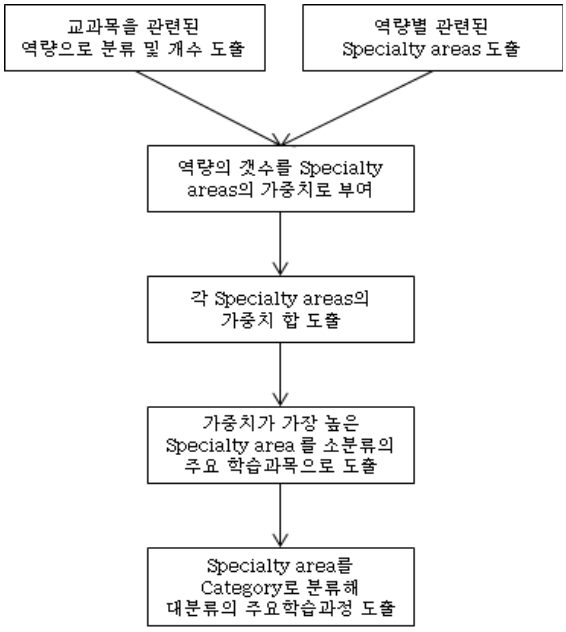
3.1 연구절차

본 연구에서는 국내 대학의 정보보호관련 학과의 교육과정이 어떠한 역량을 중심으로 구성되어 있는지 그리고 정보보호 직무의 어느 분야를 중심으로 이루어져 있는지를 분석하고자 한다. 이를 위해 KISA에서 제시한 “2012년도 정보보호 교육과정 및 커리큘럼 현황조사”에 사용된 28개 대학의 1,111개의 교과목을 대상으로 분석을 진행 할 것이다[9].

NICE의 자료는 Categories ⇒ Specialty Areas ⇒ Competencies 로 분류해 역량 모델을 제시하였다. 이를 직접비교가 가능한 역량으로 교과목을 분류해 이후 Specialty Areas, Categories 순으로 역추적 할 것이다. 우선 국내 대학 정보보호 관련 학과의 교과목을 모두 나열해 각각을 NICE에서 제시된 역량의 정의와 KSAs를 이용해 분류한다. 이후 해당 분류를 통해 역량별로 포함된 교과목의 개수를 확인한다. 이와 별도로 역량과 관련된 Specialty areas를 분류 한다.

이러한 두 가지의 분류작업 이후 역량에 포함된 교과목의 수를 Specialty areas(세부직무)에 가중치로 부여할 것이다. 그 결과로 역량과 관련된 Specialty areas(세부직무)를 확인할 수 있을 것이다. 이후 Specialty areas(세부직무)를 기준으로 대분류의 학습과정을 확인 할 것이다.

연구의 절차는 아래의 <그림 2>과 같이 진행될 것이다.



<그림 2> 교육과정 분석 절차

그리고 분석 결과를 지식정보보안산업협회(KISIA)에서 발표한 “2013 국내 정보보호산업 실태조사”에서 제시하고 있는 정보보안산업의 매출 현황 및 성장률과 비교할 것이다[9]. 지식정보보안산업협회(KISIA)의 자료 역시 정보보호 기업을 대상으로 조사된 것으로 교육과정의 방향을 산업 동향과 정확하게 비교할 수는 없을 것이나, 공식 조사와 비교하는 것은 의미 있는 일일 것이다.

3.2 자료 분석

각 역량에 따른 교과목을 분류한 결과는 아래 <표 4>와 같다.

<표 4> NICE 제시 역량과 관련 교과목

NICE 역량	교과목
컴퓨터 포렌식	과학수사개론, 네트워크 포렌식 총론, 디지털 포렌식, 컴퓨터 포렌식 , 시스템 포렌식
컴퓨터 언어	마이크로프로세서/어셈블리어, 윈도우즈 프로그래밍, 자바프로그래밍, C 프로그래밍, C++ 프로그래밍 , GUI 프로그래밍
네트워크 보안	네트워크전문가실무, 공격자 모니터링, 네크워크 해킹과 보안, 네트워크 보안, 네트워크 보안솔루션구축, 네트워크 분석
컴퓨터 기술	컴퓨터정보 활용 실습, 인터넷정보검색,
컴퓨터 및 전자회로	논리회로, 컴퓨터구조, 컴퓨터관리
형법	개인정보법, 범죄론, 법학개론, 사이버법률, 인터넷윤리 및 법, 정보통신법규 및 정책
암호학	현대암호론, 암호알고리즘
Database Administration	데이터베이스설계
DB 관리 시스템	데이터구조, 데이터마이닝, 데이터베이스, 데이터베이스 보안
암호화 통신	IPSec과 VPN, 네트워크보안프로토콜, 암호프로토콜, 저작권보호시스템
임베디드 컴퓨터	임베디드시스템실습, 내장형시스템개론, 임베디드 시스템보안
포렌식	수사, 수사강론, 수사학
하드웨어	컴퓨터하드웨어
인증 관리	보안전자상거래, PKI
사고 관리	침해사고와 대응
정보 보증	경영정보시스템설계 및 감사, 보안감사, 보안관리, 시스템감리론, 정보보안통신감리, 정보보호 관리체계 인증
정보 관리	보안정보처리
정보시스템 및 네트워크 보안	보안정책, 시스템관리, 시스템보안, 정보보호전문가실무, 경영정보학개론, 보안시스템구조, 사이버보안개론
정보기술 아키텍처	모바일시스템보안, 모바일컴퓨팅, 유비쿼터스 컴퓨팅, 정보기술아키텍처
인프라 설계	시스템 분석 및 설계, 컴퓨터 시스템 설계
논리 구조 설계	보안알고리즘, 알고리즘 분석 및 설계
수학적 사고	이산수학, 정수론
멀티미디어 관련 기술	영상보안시스템, 멀티미디어보안
네크워크 관리	홈네트워크보안, 관리/인터넷보안, 네트워크장비운용
운영체제	웹 서버 보안 설정, 서버시스템구축설계, 운영체제보안, 운영체제, 리눅스서버
개인 및 공공보안	개인정보보호 및 관리, 개인정보관리체계
프로젝트 관리	IT프로젝트관리론
위험 관리	위험관리, 정보시스템위험관리
보안 규제	스마트카드보안
소프트웨어 공학	소프트웨어 공학, 소프트웨어개발보안
소프트웨어 개발	프로그래밍프로젝트, 객체지향프로그래밍 활용, 보안 솔루션 프로젝트, 시스템분석 및 설계
시스템 테스트 및 평가	소프트웨어품질관리
기술 문서	해킹보안비즈니스커뮤니케이션
최신기술 동향	u-컴퓨팅해킹보안, 보안기술 특강, 사이버보안기술, 사이버안보동향과 분석
전자 통신	보안컴퓨터네트워크, 정보통신 시스템, 정보통신 실습, 정보통신 실험, 정보통신 시스템, 인터넷 프로토콜, 데이터통신, 통신망이론
취약점 분석	컴퓨터바이러스, 네트워크 해킹 및 보안 실습, 네트워크 해킹과 보안, 네트워크해킹보안, 리버스엔지니어링, 모의해킹, 보안과 해킹, 보안취약점분석, 사이버모의해킹
웹 관련 기술	HTML/CSS, 닷넷웹 해킹보안, 웹 어플리케이션보안, 웹보안 실습

분류에 포함되지 않은 기타 항목으로는 캡스톤 디자인, 영어, 무술, 윤리 등의 교과목이 있다.

4. 정보보호 교육과정 분석 결과

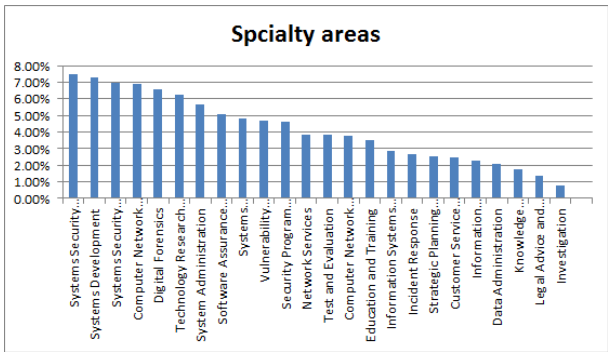
정보보호 교과목을 NICE에서 제시된 역량과 비교한 결과 Computer Languages가 분류 가능한 교과목 중 가장 많은 13.5%의 비율을 차지하고 있었고 Information Systems/Network Security 8.28%, Operating Systems 6.75.%로 나타났다. 이를 통해 일반 IT 학과의 교육과정에 포함된 컴퓨터 언어와 운영체제, 데이터 통신, 데이터베이스 등의 과목의 비율이 높은 것을 확인 할 수 있다. 그리고 역량으로 분류하기 힘든 기타영역이 21.06%의 비율을 차지하고 있다. 여기에는 정보윤리, 경영학, 행정학, 경찰학, 조직관리 및 정보기술과 경영 등 타 학문과의 융합을 위한 교과목과 인턴쉽, 확률과 통계 등 기초 교양항목 등이 포함되어 있었다.

아래 <표 5>에서 교과목을 역량별로 분류한 비율을 확인 할 수 있다.

<표 5> 교과목과 관련된 역량의 비율

역량	교과목 수	비율
기타	234	21.06%
컴퓨터 언어	150	13.50%
정보시스템 및 네트워크 보안	92	8.28%
운영체제	75	6.75%
전자 통신	67	6.03%
DB 관리 시스템	46	4.14%
컴퓨터 포렌식	41	3.69%
네트워크 보안	40	3.60%
취약점 분석	40	3.60%
컴퓨터 및 전자회로	33	2.97%
암호학	32	2.88%
수학적 사고	27	2.43%
형법	24	2.16%
정보 보증	20	1.80%
최신기술 동향	20	1.80%
소프트웨어 개발	18	1.62%
소프트웨어 공학	17	1.53%
네트워크 관리	16	1.44%
웹 관련 기술	13	1.17%
멀티미디어 관련 기술	12	1.08%
암호화 통신	10	0.90%
논리 시스템 설계	10	0.90%
인증 관리	9	0.81%
임베디드 컴퓨터	9	0.81%
프로젝트 관리	9	0.81%
정보기술 아키텍처	8	0.72%
포렌식	7	0.63%
컴퓨터 기술	5	0.45%
인프라 설계	5	0.45%
개인 및 공공 보안	5	0.45%
DB 관리 시스템	3	0.27%
글쓰기	3	0.27%
사고 관리	2	0.18%
정보 관리	2	0.18%
위험 분석	2	0.18%
Database Administration	1	0.09%
하드웨어	1	0.09%
보안 규제	1	0.09%
시스템 테스트 및 평가	1	0.09%
기술 문서	1	0.09%
교과목 합계	1,111	100.00%

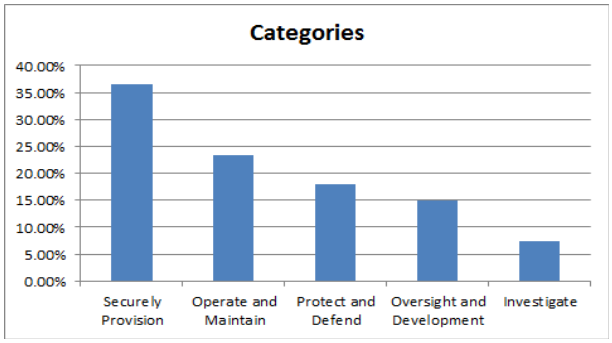
그리고 Specialty areas(세부직무)는 교과목 분류에서 확인한 개수를 가중치로 하여 계산했다. 그 결과 Systems Security Analysis가 7.47%로 가장 많은 부분을 차지하고 있음을 확인했다. Systems Security Analysis는 보안시스템의 유지보수, 운영 및 통합과 테스트를 담당하는 것으로 보안 운영에 속하는 직무이다. 이어 시스템의 라이프사이클 개발을 담당하는 Systems Development 7.26%, 위의 Systems Development와 유사한 개발군에서 시스템 설계 및 프로세스와 관련된 법률 또는 규제 등의 분야직무인 Systems Security Architecture 6.99%, 네트워크 이벤트를 수집, 분석하고 발생 가능한 위협에서 네트워크를 보호하는 직무인 Computer Network Defense Analysis 6.93% 순으로 나타났다. 이를 그래프로 나타내면 아래의 <그림 3>과 같다.



<그림 3> Specialty areas(세부직무) 의 비율

Specialty areas(세부직무)로 분류한 자료를 보면 제품개발과 시스템 운영 및 네트워크 분석 등 다양한 분야의 직무에 적합하도록 교육과정이 구성되어 있는 것으로 보인다. 하지만 이를 NICE에

서 제시한 Categories(대분류)로 다시 분류해 보면 정보보호 제품 개발 관련인 Securely Provision이 차지하는 비율이 눈에 띄게 높은 것을 알 수 있다. 아래 <그림 4>은 Categories로 분류 한 것이다.



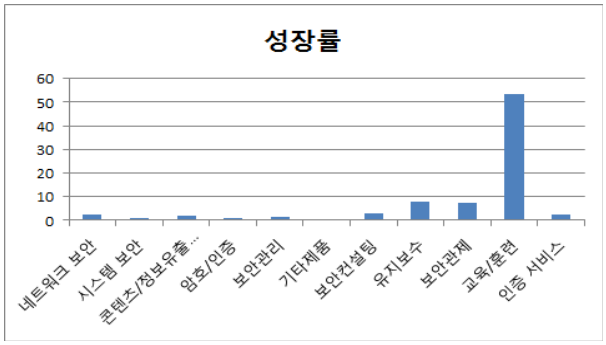
<그림 4> Categories의 비율

여기서 보면 정보보호 시스템의 기획, 디자인 및 개발 직군인 Securely Provision이 36.5%로 가장 많은 것으로 나타났다. 그리고 정보기술 시스템을 효율적이고 효과적으로 관리 운영 직군인 Operate and Maintain이 23.28%, 내부 정보시스템 또는 네트워크의 위협을 식별, 분석 및 방어하는 직군 Protect and Defend가 17.99%, 기업의 정보보호 조직을 효율적으로 관리 감독하고 방향을 설정하는 직군 Oversight and Development가 14.89%, 디지털 및 네트워크 증거 수집 또는 사이버 범죄 수사에 관한 직군인 Investigate가 7.34% 순으로 확인된다.

이를 통해 정보보호 교육은 기본적으로 IT기반 교과목을 중심으로 이루어져 있다고 할 수 있다. 이것은 '2012년 한국인터넷진흥원의 정보보호업체에서는 보안프로토콜을 전공한 고급인력 보다는 ' 코딩을 할 줄 아는' 일반IT인력의 수요가 더 많고, 코딩 및 개발 보다는 설계 및 기획 분야의 인력에 대한 수요가 더 시급하다.'[10]는 조사 내용과 유사한 인력 수급의 문제점을 드러내고 있다. 정보보호학과가 컴퓨터공학 등의 IT학과에서 정보보호 관련 교과목이 추가된 교육과정이라는 한계가 드러난다고 할 수 있다.

추가적으로 2.3절의 국내 정보보호 산업 분류 및 인력 현황과 현재의 교육과정을 비교해보면 정보보안 제품의 개발 직군 뿐아니라 관리 분야의 인력 수요가 많다는 것을 확인할 수 있다. 또한 정보보호 산업 성장률 역시 정보보호 서비스 분야인 보안컨설팅, 유지보수, 교육/훈련, 인증서비스의 증가가 두드러진다.

해당 조사에서 2012년도 정보보안 제품의 매출액이 전체의 79.28%를 차지하고 있고 정보보안 서비스 부분이 나머지인 20.72%로 나타난다. 하지만 세부 항목별 성장률을 보면 아래의 <그림 5>와 같다.



<그림 5> KISIA에 제시된 분야별 성장률

위의 <그림 5>에서 보면 보안컨설팅부터 인증서비스까지의 정보보안 서비스 부분의 성장률이 높은 것을 알 수 있다. 이것으로 각 정보보안 전문업체 뿐아니라 일반 기업에서 정보보안 관련 직무를 담당하는 인력의 수요가 높아지고 있다고 확인 할 수 있을 것이다.

전체적으로 정보보호 인력의 수요가 정보보호 제품개발 분야를 넘어 다양한 분야가 융합된 인재를 필요로 하고 있음을 알 수 있다.

5. 결론

본 연구에서는 국내 대학의 정보보호 관련 학과의 교육과정을 NICE에서 제시된 역량과 비교하여 분석하였다. 이를 통해 국내대학은 정보보호 제품을 개발하는 분야의 역량을 중심으로 교육과정이 편성되어 있음을 확인하였다. 이는 이전의 연구들에서 문제로 제시되어 오던 IT학과에서 정보보호 인력을 양성되고 있는 한계를 보여 주고 있다. 이런 한계의 극복을 위해 각 대학별로 전공 교과목의 범위를 정보보호 직무체계별 역량을 중

심으로 확대할 필요가 있고 직무별 수요를 조사해 학교에 수요에 맞는 인력을 공급할 수 있도록 관리하는 것이 필요 할 것이다.

그리고 이번 연구는 미국에서 조사된 직무체계 및 역량을 중심으로 비교 분석되었기 때문에 국내 환경에 적합한 직무와 역량 등이 추가적으로 조사되어 교육과정이 구성될 필요가 있다. 또한 지식정보보안산업협회(KISIA)에서 조사된 정보보호 산업 실태조사가 정보보호 전문 기업의 매출, 성장률 및 직종별 인력현황, 일반 기업에서 정보보호 제품을 운영 및 관리 직무 또는 비용 등도 조사 범위에 추가해 사회 전반적인 정보보호 관련 인력에 대한 수요가 조사되어야 할 것이다. 그리고 이런 수요조사가 대학의 인력양성 과정과 연계되어야 한다.

이후 정보보호 관련 대학교육에 포함되어야 할 전공교과목의 구성 역시 기존의 IT교과목 중심을 탈피하여 정보보호 직무체계에 따라 다루고자 하는 직무를 선정하고, 이에 따른 역량을 중심으로 교과목을 구성해 타 학과와의 차별화 및 특성화를 고려해야 할 것이다. 그리고 심리학, 경영학, 경제학, 윤리학 및 법학 등 다양한 학문과의 학제간의 교육과정 구성으로 융합된 인재양성이 이루어져야 할 것이다.

향후 국내 환경에 적합하도록 정보보호 직무체계를 수정하고 각 직무별 역량의 우선순위를 조사, 이를 반영한 교육과정이 제시되어야 하며, 인력의 수요와 공급이 유기적으로 관리될 수 있는 방안에 대한 연구 및 정보보호분야와 연계되어 학습되어야할 학제간의 교과목의 구성도 제시되어야 할 것이다.

참 고 문 헌

[1] 유현숙 (2011). **역량기반 교육의 필요성과 시사점**. 한국교육개발원

[2] 이근호 (2013). **핵심역량 중심의 교육과정 재구조화 방안 연구**. 교육부

[3] 재인용, 전효성・유해원・김태성 (2008). **정보보호 분야 직무별 필요 지식 및 기술 분석**

[4]류지성・이성호・김재원・김종만・강홍준・이성식 (2011). **IT 인재 양성을 위한 한국 대학교육의 과제**. 삼성경제연구소

[5]정영일・이명호・최철용・조태경・김성태 (2001). **전문대학 정보기술(IT) 교육과정 모형 개발**. 한국전문대학교육협의회

[6]심상현・임재우・신미애・김태성・전효성 (2008). **정보보호 직무체계 개발 및 인력수급 실태조사**. 한국인터넷진흥원

[7] NICE (2014). THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK, http://csrc.nist.gov/nice/framework.national_cybersecurity_workforce_framework_03_2013_version1_0_for_printing

[8] 지식정보보안산업협회 (2013). **2013 국내 정보보호산업 실태조사**

[9]채승완・배승태・김주희・신은희・김장호・이승호 (2012). **2012년도 정보보호 교육과정 및 커리큘럼 현황조사 최종 결과보고서**. 한국인터넷진흥원

[10] 김태성 (2013). **사이버위협에 대비한 정보보호 인력양성**, 재인용

[11] 진주현・박준성 (2010). 표준역량개발

[12] CHIEF HUMNA CAPITAL OFFICERS COUNCIL (2011). MEMORANDUM FOR CHIEF HUMAN CAPITAL OFFICERS, http://www.chcoc.gov/transmittals/TransmittalDetails.aspx?TransmittalID=3436

[13] NICE (2014). Cybersecurity Competency Model, http://www.careeronestop.org/competencymodel/competency-models/cybersecurity.aspx

[14] 정보통신부 (2004). **대학 IT인력 전공역량 혁신방안**

[15] 이숙정・박소연・유지현 (2013). **교수・학습 방법에 따른 역량중심 교육과정의 효과 연구: 대학 신입생을 중심으로**. 숙명여자대학교

[16] 장항배 (2013). **정보보호 직업별 교육 훈련 로드맵 구축**. 한국인터넷진흥원

임 원 규

2008 서울산업대학교
산업정보시스템공학과
(학사)

2010 서울산업대학교 IT정책전문대학원
산업정보시스템공학과(석사)

2011～현재 성균관대학교 대학원 컴퓨터교육과
박사과정

관심분야: 정보보안, 교육과정, 인력정책

E-Mail: wglim@skku.edu

안 성 진

1988 성균관대학교
정보공학과(학사)

1990 성균관대학교
정보공학과(석사)

1998 성균관대학교 정보공학과(박사)

1990～1995 KIST/SERI 연구원

1996 정보통신기술사

1999～현재 성균관대학교 컴퓨터교육과 교수

관심분야: SW교육, 정보윤리, 정보보안

E-Mail: sjahn@skku.edu