기본연구
2013-42

이슈페이퍼

미래지향 대학특성화를 위한 공학부문 교육과정 분석 연구 : 정보보안 전공을 중심으로

황규희

한국직업능력개발원

이슈페이퍼 2013-7

기본연구
2013-42

이슈페이퍼

미래지향 대학특성화를 위한 공학부문 교육과정 분석 연구 : 정보보안 전공을 중심으로

황규희

한국직업능력개발원

미래지향 대학특성화를 위한 공학부문 교육과정 분석 연구: 정보보안 전공을 중심으로

황규희[1)]

〈목 차〉

본 연구는 대학특성화와 관련하여, 근래 많은 관심이 고양되는 정보보안 부문을 대상으로 교육과정 분석을 수행하였다. 정보보안 관련 학부 및 학과를 가지고 있는 16개의 4년제 대학에 대하여, 미래숙련수요에 대한 교육과정 대응성 분석을 수행하였다. 미래 지향적 대학특성화를 위하여 다음 사항들이 제언되었다: 내부자원(자체 전임교원) 및 외부자원(유관학과 및 산학협력 등) 운영계획에 기반하여 미래수요에 대응하는 세부 특성화 방향 요구; 미래유망기술, 미래유망산업에서 요구되는 숙련단위에 대응하는 교과구성단위를 마련하고 자체 평가를 수행할 수 있도록 유인; 특허정보 등을 이용한 기술전망을 미래숙련수요 전망에 활용; 교육과정 수집 및 교육과정 개발을 위한 정책 지원 강화.

- 주제어: 미래숙련수요, 대학특성화, 정보보안, 특허분석, 교육과정 분석

1) 한국직업능력개발원 연구위원(E-mail: g.hwang@krivet.re.kr).

I. 연구의 필요성과 목적

본 연구는 대학특성화와 관련하여 근래 많은 관심이 고양되고 있는 정보보안 부문을 대상으로 교육과정 분석을 수행하고, 향후 적용대상 확대 방안 및 관련 정책개발을 위한 정책협의를 도모하는 정책기반연구의 성격을 가진다.

대학특성화 지원을 위해 미래 지향적 공학계열 커리큘럼 개발 지원이 준비될 필요가 있다. 미래인재 양성은 국가적으로 중요한 사항이며, 대학특성화 방향설정에서도 중요한 요소 중 하나이다. 인력수요에 대한 대응으로의 인력양성은 일정 기간을 요구하며 나아가 인력활용까지는 상당한 시간이 소요된다는 것을 고려했을 때 대학 교육과정 개발에서도 미래숙련수요 전망과의 연계성을 강화할 필요가 있다. 특히, 2014년 대학특성화알리미에서 특성화학과 교과과정 개선실적을 템플릿 방식으로 수집할 예정이고, 2015년 대학정보공시에서 특성화학과 교과과정 개선실적이 의무적으로 탑재될 예정인바, 관련한 기초연구를 수행하고 특성화 관련 교과과정 수집 및 개선 지원을 체계적으로 수행할 필요가 있다.

본 연구에서는 정보보안을 사례로 하여 미래숙련수요에 대한 관련 학과 교육과정을 분석하고자 한다. 이에 그간 정보보안의 역사적 측면을 간략히 살펴보는 것이 유용한데, 본 연구에서의 정보보안이 주로 네트워크 보안의 의미를 가지기에 이를 중심으로 살펴보기로 한다. 먼저 해킹이란 용어 자체는 1960년대부터 있었으나, 네트워크 해커라는 개념은 PC와 함께 1980년대에 등장하였고, 1980년대 후반 이후 해킹 및 정보보안이 본격적으로 사회문제로 부상하였다. 특히, 2001년 9.11사건에서 보안의 문제가 세계적 관심사가 되고, 한국에서도 2009년 DDoS 공격, 2011년 은행 전산망 마비, 2012년 통신사 개인정보 대규모 유출 등이 나타나는 가운데 정보보안에 대한 국가적 관심이 높아지게 되었다.

세계적인 보안업체 시만텍의 2003년 보고서에 따르면, 당시 한국은 국제적 해킹에 악용되는 세계 순위가 무려 2~15위 수준으로 제시되었다. 이런 가운데, 2003년 1월 25일 한국 전역의 네트워크가 약 2일간 마비되는 사태를 겪으면서 네트워크 보안이 기업의 핵심적 문제로 대두하였다. 이에 네트워크 장비 및 서비스 관련 기업 등 네트워크 보안기술의 확보가 매우 심각한 현안이 되었다. 이는 신규기술 개발에 박차를 가하게 하는 한편, 기존 기술에 대해서도 적극적인 보호를 도모하게 되었으며, 이러한 여러 상황들로 인해 2000년대 중반에 정보보안 특허의 폭발적인 증가를 가져오게 되었다고 여겨진다.

미래인재 양성을 위한 이공계 교과과정 분석 및 교육과정 개선을 도모하기 위해, 먼저

특허분석을 수행하여 미래숙련수요를 제시하고, 이어서 정보보안학과 교과과정을 대상으로 미래수요 대응성을 분석함과 동시에 타 분야 확장가능성을 마련하고자 한다.

- 정보보안은 정보화 사회의 핵심적 요소로 전세계적으로 그 중요성이 강조되며 한국으로서도 중요성이 매우 높음. 특히, IT 기반 미래 성장산업 육성에서 산업적 중요성이 강조될 뿐 아니라 안보 등의 측면에서도 국가전략적 중요성이 높음.
- 대학에서도 정보보안 전문학과가 근래 신설됨에 따라, 대학특성화와 관계가 높아지고 있음.

〈표 1〉 정보보안인력 양성 관련 주요 선행연구

연구	연구방법	주요 연구내용
- 연구제목: Development and Application of Skill Standards for Security Practitioners - 연구자(년도): Simpson 외(2006), - 연구목적: 정보보안 전문가 직무분석	관련 자료 분석 직무분석	- 보안담당자를 위한 숙련 표준의 개발과 적용
- 연구제목: 정보보호인력 양성정책 - 연구자(년도): 김태성(2010), - 연구목적: 정보보호인력 및 양성 교육체계 제시	- 기존 연구 정리	- 직무분석에 기반하여 교육체계 제시
- 연구제목: 정보보호 분야 직무별 필요 지식 및 기술 분석 - 연구자(년도): 김정덕 외(2011) - 연구목적: 교육 프로그램 제안	- 정보보호와 관련된 직업 도출 · 각 직업별 역할 정의 · 미국 IT 보안 필수요구지식을 참조하여 각 역할별 필수요구지식 선정	- 직무별 요구 지식분야 선정
- 연구제목: IT Security Essential Body of Knowledge (EBK): A Competency and Functional Framework - 연구자(년도): IT Security EBK(2012) - 연구목적: 정보보안 전문가 양성을 위한 직무분석	관련 자료 분석 직무분석	- 보안담당자를 위한 숙련 표준의 개발과 적용
- 연구제목: 지식정보보안 분야 인력현황 및 중장기 인력수급 전망 분석 - 연구자(년도): 한국정보보호학회(2010) - 연구목적: 지식정보보안 분야 인력현황 및 전망 제시	법제 사항 및 제 규정에 대한 규정 명문화	- 2009년 국내 지식정보보안인력 규모를 26,078명으로 추정하였고, 이를 출발점으로 하여 2011년 30,209명, 2018년 49,692명으로 전망
- 연구제목: 정보보호 관리체계 인증 제도 안내 - 연구자(년도): 한국인터넷 진흥원(2013) - 연구목적: 정보보호 관리체계 관련 사항 구체화	성장수요(취업계수 이용) 대체수요(탈락률 이용) 신규수요=성장수요+대체수요 취업자 수 = 전년도 취업자 수 + 올해 성장수요	- 정보보호 관리체계(ISMS) 인증 제도의 개요, 인증 대상자, 인증 절차 및 기준, 주요 추진체계, 구축 및 운영 등 구체화
- 연구제목: 미래숙련수요 분석을 위한 특허정보 활용의 현실적합성 분석 - 연구자(년도): 황규희 외(2013) - 연구목적: 미래숙련수요 전망방법 제시	- 특허분석 - 전문가 자문 - 기업조사	- 특허를 이용한 정보보안 부문 미래숙련수요 전망 - 전망결과의 현실적합성 검증

Ⅱ. 정보보안기술과 정보보안인력

1. 정보보안기술

정보통신과 컴퓨터 관련 기술의 비약적 발달과 더불어 정보 유출이나 정보 시스템 파괴 등 각종 정보보안 위협이 사회문제로 대두되고 있다. 여기에서의 정보보안(Information Security)이란, 단순한 컴퓨터 조작 능력을 넘어 정보 시스템이나 네트워크에 존재하는 데이터와 같은 정보의 보호와 관련된 제반 사항을 일컫는다.

지식경제부(2011)의 「대한민국 산업기술 비전 2020: 정보통신」은 정보보안 기술동향을 다음과 같이 정리하고 있다.

<표 2> 정보보안 기술동향

구분	기술동향
공통 기반 보안	● 모바일 환경을 고려한 온/오프라인 연계 및 사물 간 연동 환경인 유비쿼터스 환경에 대응하기 위한 기술의 확장 및 보호 범위 확대 * 스마트폰 등 모바일 환경에서 사용되는 기술과 이를 통해 온/오프라인 연계를 제공하는 데 필요한 인증 기술과 유비쿼터스 환경을 고려한 경량 암호 및 암호 프로토콜 기술 개발이 활발히 진행되고 있음. * 개인정보보호 범위를 확대하여, 개인정보 유출을 방지하는 수준을 넘어 유출된 개인정보의 악용을 방지하는 기술로 확장하여 개발이 진행 중임.
네트워크, 시스템 보안	● 지능화, 복합화, 조직화되고 있는 사이버 공격 기술의 발전 추세에 따라 네트워크/시스템 보안 기술도 고도화, 통합화, 능동화, 선제적 대응화되는 추세임. * 네트워크의 가용성을 저해하는 DDoS 공격 대응과 악성코드에 대한 근원적 대응을 위해 지능형 DDoS 공격 대응 및 악성코드 분석기술 개발과 모바일 단말 임의조작 방지 및 보호를 위한 보안 플랫폼 개발에 집중함. * 통신망 융·복합화, 사이버공격 고도화 환경에서 네트워크/시스템 보호를 위한 모바일 단말 플랫폼 보안, 지능형 악성코드 자동 분석, 클라우드 컴퓨팅 보안, 고성능/응용계층 DDoS 탐지/대응, 신종 봇넷 탐지 등 사이버 공격 조기 탐지/차단/대응 기술
응용 서비스 보안	● 서비스 등 IP 기반 데이터 중심의 서비스 보안기술에서 VoIP, IPTV 등 멀티미디어 중심의 방송·통신 융합 서비스 보안기술이 개발되어 시장 보급 중임. * VoIP, IPTV 등 방송·통신 융합 서비스의 본격적 활성화에 따른 VoIP·IPTV 서비스 대상 해킹, 도청, 스팸 등 침해사고 대응 기술이 개발되고 있음. * 전통적인 웹 서비스 보안기술은 비즈니스 차원의 웹 응용 서비스, 웹 취약성 점검, 웹 방화벽 분야를 중심으로 개발되고 있으며, 패턴 학습을 통한 정교한 탐지 기능들이 강화되면서 점차 지능화되고 있음. * 지식 콘텐츠 보호기술은 웹 중심의 온라인에서 디지털 방송, IPTV, 스마트폰, e-book 등 다양한 플랫폼·서비스로 활용 범위가 확산되는 추세임.

출처: 지식경제부(2011: 278-279).

한국정보처리학회(2010)는 EU FP7(7th Framework Programme for Research Technological Development)에서 제시하는 미래 인터넷 보안 자료에 대한 전문가 분석을 통하여 보안 이슈 분류체계와 우선순위를 제시하였다. 대항목 간 보안 이슈에서의 우선순위는 네트워크 보안 이슈가 최우선적으로 나타났고, 이어서 미래서비스 및 인증 보안 이슈, 클라우드 및 모바일 보안 이슈, 통합·관리 보안 이슈의 순으로 나타나고 있다. 세부 항목 간 보안 이슈는 라우터, 무선통신(wireless communication), 데이터 인증, 네트워크 복잡성, IPv6, 서비스 거부(Denial of Service) 방지기술, 소셜 네트워크, 모바일 기기(Mobile device), 모바일 오픈마켓, 표적공격, 클라우드 컴퓨팅, USN, 이종 단말기 통합관리, DNS의 순으로 나타났다.

미래 인터넷 보안 능력의 핵심은 사회 곳곳에 산재해 있는 데이터의 인터넷 편입, 무선 디바이스의 확산, 조직범죄형 해킹 등에 대처하는 것이다. 이를 위해서는 시스템적 방어체계를 갖추어야 하는데, 방어체계의 핵심이 라우터이기 때문에 라우터가 가장 중요한 보안 이슈로 간주된 것으로 여겨진다.

우선순위가 두 번째로 높은 보안 이슈는 유비쿼터스 환경에서 중요할 것으로 파악되는 무선통신(wireless communication) 보안 이슈이다. 이는 유비쿼터스 환경에서의 무선통신 비중 증대가 반영된 것으로 여겨진다.

데이터 인증은 모든 네트워크를 이용할 때 기본적인 사항으로서의 중요성이 반영된 것으로 여겨진다. 네트워크 복잡성, IPv6는 아직 중요성이 높게 여겨지나, 보안 관련 안정화가 진행되면서 중요도가 감소할 전망이다.

반면, 미래 인터넷 환경에서 사회공공데이터에 대한 공격의 증대는 서비스 거부 형태를 취할 것으로 예상되는 가운데, 이의 중요성 또한 증대할 것이다. 클라우드 컴퓨팅 보안 이슈는 하위권에 속하고 있는데, 이는 라우터, 인증 등이 해결되면 클라우드 컴퓨팅 보안 문제가 해결되는 측면과 클라우드 컴퓨팅의 확산에 대한 불확실성이 반영된 것으로 여겨진다.

한편, 표적공격의 경우 조직범죄형 해킹의 급증과 관련하여 미래 인터넷 환경에서 주요 문제가 될 가능성이 높은 것에 비하여 우선순위가 낮게 나왔는데, 이는 문제의 심각성이 과소평가된 측면이 있다.

〈표 3〉 보안 기술 이슈

대항목	세부 항목	설명	우선 순위
네트워크	라우터 보안 이슈 (Backbone)	미래 인터넷 환경에서 발생할 수 있는 라우터를 중심으로 발생할 수 있는 보안 이슈	1
	IPv6 보안 이슈 (Protocol)	미래 인터넷 환경에서 발생할 수 있는 IPv4로의 전환 시에 발생할 수 있는 보안 이슈를 포함한 IPv6와 관련된 보안 이슈	5
	DNS 보안 이슈 (Edge 라우터)	미래 인터넷에서는 DNS를 통해 네트워크를 위협할 가능성이 높은 보안 이슈	14
	무선통신(Wireless communication) 보안 이슈 (Transmission)	미래 무선 통신(Wireless communication) 환경에서 발생할 수 있는 여러 가지 보안 이슈	2
	서비스 거부(Denial of Service) 보안 이슈 (Gateway)	미래 인터넷 환경에서 지속적으로 심화될 가능성이 높은 DDoS 관련 보안 이슈	6
클라우드	USN 보안 이슈	미래 인터넷 환경에서는 비교적 소형 커뮤니케이션 기기들 간에 보안 이슈	12
	클라우딩 컴퓨팅 보안 이슈 (IaaS/PaaS)	미래 인터넷 환경에서 대두될 클라우딩 컴퓨팅 인프라 및 플랫폼에서 발생할 보안 이슈	11
	모바일 오픈 마켓과 콘텐츠 보안 이슈 (SaaS)	모바일 시장의 확대로 인한 애플리케이션 마켓(App Market) 또는 콘텐츠 (DRM) 등의 클라우딩 컴퓨팅 서비스 관련 보안 이슈	9
	모바일 기기(Mobile device) 보안 이슈	미래 인터넷 환경에서 발생할 수 있는 스마트폰, 태블릿 PC 등의 모바일 디바이스에서 발생할 수 있는 해킹, 악성코드, 개인정보 유출 등의 보안 이슈	8
통합·관리	네트워크 복잡성 보안 이슈	미래 인터넷 환경에서 네트워크 복잡성으로 인해 발생할 수 있는 보안 이슈	4
	이종단말기 간 통합 관리 보안 이슈	미래 인터넷 환경에서 네트워크에 이종(Heterogeneous)의 구성 요소들이 동시에 연결되어 시스템에 문제가 생길 가능성이 높으므로 이와 관련된 보안 이슈	13
미래 서비스 및 인증	데이터 인증 보안 이슈	잠재적인 버그 또는 공격자에 의한 데이터 조작으로 센서의 데이터를 신뢰할 수 없게 되는 경우 발생할 보안 이슈	3
	표적 공격 보안 이슈	미래 인터넷 환경에서 개인, 기업 또는 국가에 직접적인 피해를 입히는 표적 공격에 대한 보안 이슈	10
	소셜 네트워크 보안 이슈	개인 정보 유출, 사칭, 악성코드 유포 등 미래 인터넷 환경에서의 소셜 네트워크 서비스에 대한 보안 이슈	7

출처: 황규희 외(2013: 46-47), 한국정보처리학회(2010: 55, 123)를 정리함.

2. 정보보안인력 수요

한국인터넷진흥원(2011)은 2011년도 정보보안 관련 236개 사업체를 조사하였고, 여기에 종사하는 인력 규모를 26,458명으로 제시하였다. 이들의 전공별 현황을 보면, 정보보안 전공자가 6.05%인 1,603명, IT 관련 전공자가 57.9%인 15,321명, 비 IT전공자가 36.0%인 9,534명으로 조사되었다. 성별로는 남자가 78.6%인 20,788명이었으며, 여자는 21.4%인 5,670명이다.

<표 4> 전공별 성별 인력현황

(단위 : 명)

구분		남자	여자	합계	
IT관련 학과	정보보안(호)학과	1,350	253	1,603	16,924
	전자, 통신 컴퓨터 관련 학과	12,366	2,955	15,321	
인문사회 등 비 IT학과		7,072	2,462	9,534	
합계		20,788	5,670	26,458	

출처: 한국인터넷진흥원(2011: 136).

이들 26,458명은 순수 정보보안 관련 이외의 IT, 분야 인원을 포함하는 것으로, 순수 정보보안 관련 종사자는 8,589명으로 조사되었다. 정보보안 관련 기술 및 연구인력 수준별 종사자 수는 초급>중급>고급>특급의 순으로 많은 것으로 조사되었다. 기술 등급별로 살펴보면, 특급은 총 1,307명이었고, 이 중 '암호 및 인증 기술' 부문이 327명으로 가장 많았으며, 다음으로 '시스템 및 네트워크 기술' 부문이 325명, '정보보안 마케팅' 부문이 202명, '정보시스템 관리' 부문이 189명의 순으로 많은 것으로 조사되었다. 고급의 경우, '정보시스템 관리' 부문이 430명으로 가장 많았고, 다음으로 '암호 및 인증 기술' 부문이 420명, '시스템 및 네트워크 기술' 부문이 377명의 순으로 많은 것으로 조사되었다. 중급의 경우, '암호 및 인증 기술' 부문이 530명으로 가장 많았고, '정보시스템 관리' 부문이 527명으로 뒤를 이었다. 초급의 경우, '정보시스템 관리' 부문이 657명으로 가장 많았으며, '암호 및 인증 기술' 부문이 654명으로 뒤를 이었다.

<표 5> 정보보안인력 수준별 종사자 현황

(단위 : 명)

구분	세부 분류	특급	고급	중급	초급	합계	비중 (%)
정보보안 연구 및 개발직	암호 및 인증 기술	327	420	530	654	1,931	22.5
	시스템 및 네트워크 기술	325	377	511	551	1,764	20.5
	응용기술 및 서비스	92	213	276	283	864	10.1
정보보안 관리직	정보시스템 관리	189	430	527	657	1,803	21.0
	정보보안 컨설팅	103	198	175	183	659	7.7
정보보안 영업직	정보보안 마케팅	202	290	280	277	1,049	12.2
기타 정보보안 관련직	정보시스템 감리 및 인증	19	35	45	31	130	1.5
	정보보안 교육	13	12	21	8	54	0.6
	기타	37	76	100	122	335	3.9
합계		1,307	2,051	2,465	2,766	8,589	100.0

출처: 한국인터넷진흥원(2011: 139).

한국정보보호학회(2010)의 “지식정보보안 분야 인력현황 및 중장기 인력수급 전망 분석”에서는 2009년 국내 지식정보보안인력 규모를 26,078명으로 추정하였고, 이를 출발점으로 하여 2011년 30,209명, 2018년 49,692명으로 전망하였다. 이는 지식정보보안산업의 지속적 매출액 증가를 전제로, 지식정보보안산업 성장률을 2009~2012년 연평균 10.4%, 2013~2018년 연평균 13.9%로 가정한 것에 기인하였다.

<표 6> 지식정보보안인력 수요 전망

(단위: 명)

연도	산업전망	매출액 (십억 원)	성장수요	대체수요	신규수요	취업자수
2009	10.4%	3,546	-	-	-	26,078
2010	10.4%	3,915	2,079	272	2,351	28,157
2011	10.4%	4,322	2,053	294	2,347	30,209
2012	10.4%	4,772	2,034	316	2,350	32,243
2013	13.9%	5,435	2,699	337	3,036	34,943
2014	13.9%	6,190	2,771	365	3,136	37,714
2015	13.9%	7,051	2,851	394	3,245	40,565
2016	13.9%	8,031	2,942	424	3,365	43,506
2017	13.9%	9,147	3,040	454	3,494	46,546
2018	13.9%	10,419	3,146	486	3,632	49,692

출처: 한국정보보호학회(2010: 38, 표 3-24).

주: 1. 성장수요: 매출액 증가에 따른 인력수요.
2. 대체수요: 기존인력의 퇴직에 의한 인력수요.
3. 신규수요 = 성장수요 + 대체수요.

앞서 한국인터넷진흥원(2012)에서 2011년도 정보보안 관련 236개 사업체를 조사하여 종사인력 규모로 26,458명과 신규채용 규모로 2,117명을 제시한 것에 비추어 보았을 때, 2011년 국내 지식정보보안인력에 대한 수요로 30,209명과 신규수요로 2,347명을 제시한 것은 납득할 수 있는 오차범위 내에 있다고 여겨진다. 다소의 오차는 주로 초기 전망(2009년) 인력규모의 차이에서 기인한 것으로 보여진다.

지식정보보안인력의 공급전망에서는 한국정보보호학회(2010)에 따르면, 신규공급규모가 2009년 832명에서 2018년 1,871명으로 지속적으로 증가할 것이라고 전망하고 있다. 앞서 신규수요와 차이를 보면, 신규인력의 수급차가 2013년 가장 크고 이후 수급차가 지속적으로 다소 완화될 것으로 여겨진다.

<표 7> 지식정보보안인력 공급전망 및 수급차 분석

연도	졸업생수 전망	신규공급	신규수요	수급차
2009	1,497	832	-	-
2010	1,624	896	2,351	- 1,455
2011	1,866	967	2,347	1,380
2012	2,032	1,046	2,350	1,304
2013	2,245	1,133	3,036	1,903
2014	2,485	1,247	3,136	1,889
2015	2,755	1,375	3,245	1,870
2016	3,060	1,521	3,365	1,844
2017	3,405	1,685	3,494	1,809
2018	3,794	1,871	3,632	1,761

출처: 한국정보보호진흥원(2007), 정보보호 직무체계 개발 및 인력수급 실태조사. ;
한국정보보호학회(2010: 40), <표 3-25> 재인용.

Ⅲ. 정보보안 미래숙련수요

황규희 외(21013)에서는 국내외 정보보안 직무분석을 정리하여 직무분류 소분류에 대응하는 필요숙련을 도출하였다. 도출된 필요숙련에 대한 향후 전망을 특허분석을 통해 수행함에 있어 특허로 식별될 수 없는 직무 또는 일반적인 사항이 포함된 직무는 배제하고 기술적 사항에 한정하여(고딕체로 표시) 분석을 수행하였다.

〈표 8〉 정보보안 직무에 대응하는 필요숙련

직무 분류		숙련
중	소	
전략 및 기획	위험 분석(A)	(A-1) 보안 취약점 분석
		(A-2) 네트워크 보안 스캐너
		(A-3) 모의해킹, 모의침투
	정보보호 정책 및 계획 수립(B)	(B-1) 정보보호 관리체계
		(B-2) 보안정책
		(B-3) 외부위탁보안관리
		(B-4) 직무분리
		(B-5) 감사 로깅
		(B-6) PC 보안
		(B-7) 데이터(Data) 보안
		(B-8) 네트워크(Network) 보안
		(B-9) server 보안
	개인정보보호 관리(C)	(C-1) 개인정보보호법
		(C-2) 개인정보 암호화
마케팅 및 영업	마케팅 매니지먼트(D)	(D-1) 마케팅 매니지먼트
	기술영업(E)	(E-1) 보안 컨설팅, 보안 컨설팅 방법
		(E-2) 위험 분석
		(E-3) 보호대책
연구개발 및 구현	연구개발(F)	(F-1) 암호화 알고리즘
	구현(G)	(G-1) 연구개발 구현
교육 및 훈련	일반인 및 사용자 교육(H)	(H-1) 일반인 및 사용자 교육
	전문가 교육(I)	(I-1) 전문가 교육

〈표 계속〉

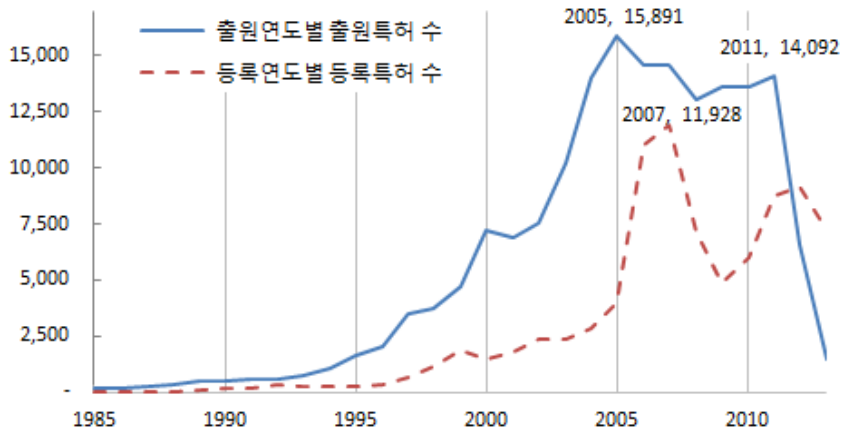
직무 분류		숙련
중	소	
관리 및 운영	프로젝트 관리(J)	(J-1) 보안 구조
	정보인프라 보안관리(K)	(K-1) Firewall 방화벽 구성
		(K-2) virus 백신
		(K-3) 스파이웨어
		(K-4) 피싱
		(K-5) 스팸
		(K-6) DB 보안 암호화
		(K-7) OTP
		(K-8) 공개키 기반구조 (PKI)
		(K-9) VPN
		(K-10) DDOS
		(K-11) 모바일 디바이스 관리 (MDM)
		(K-12) IPS 침입방지
		(K-13) 인증서비스
	물리적 보안(L)	(L-1) 물리적 보안
사고 대응	모니터링 및 대응(M)	(M-1) 취약점 분석
		(M-2) 로그 분석
		(M-3) 보안 관제
		(M-4) 지능형 지속 공격 (APT)
	디지털 포렌식(N)	(N-1) 포렌식 이해
		(N-2) 암호학
		(N-3) 해킹 기법
		(N-4) 사이버 공격
	업무 지속성 관리(O)	(O-1) 업무 지속성 관리
평가 및 인증	평가인증 및 품질보증(P)	(P-1) 평가인증 및 품질보증
	정보시스템 보안 감사(Q)	(Q-1) 보안 감사
		(Q-2) 정보보안 이벤트 관리

출처: 황규희 외(2013: 81-82).

황규희 외(2013)는 한국특허청 각 연도 등록특허를 2013년 9월 30일 기준으로 174,119건의 출원특허에 대하여 분석을 수행하였다. 연도별 추이를 볼 때, 1990년대 초·중반에서 2000년대 중반까지 성장기를 거쳐 이후 성숙기를 경과하는 것으로 나타나고 있다. 특허 출원이 2005년 15,891건, 2011년 14,092건을 보이고 있는 가운데, 2012년과 2013년의 특허

출원된 것 중 아직 심사과정 중에 있는 등 공개되지 않은 특허가 다수 있을 것이기에, 2012, 2013년을 포함한 추세에 대한 판정은 유보되어야 할 것이다. 한편, 등록특허를 점선으로 표시하였는데, 출원특허 추이와 등록특허 추이 간 일정 시차가 있음을 보인다. 출원은 2005년에 최고점을 지났고, 등록은 2007년에 12,892건으로 최고점을 지났는데, 이는 통상 특허 출원에서 등록까지 18개월 이상 소요된다는 것을 보여준다.

[그림 1] 정보보안 특허출원



출처: 황규희 외(2013: 94).

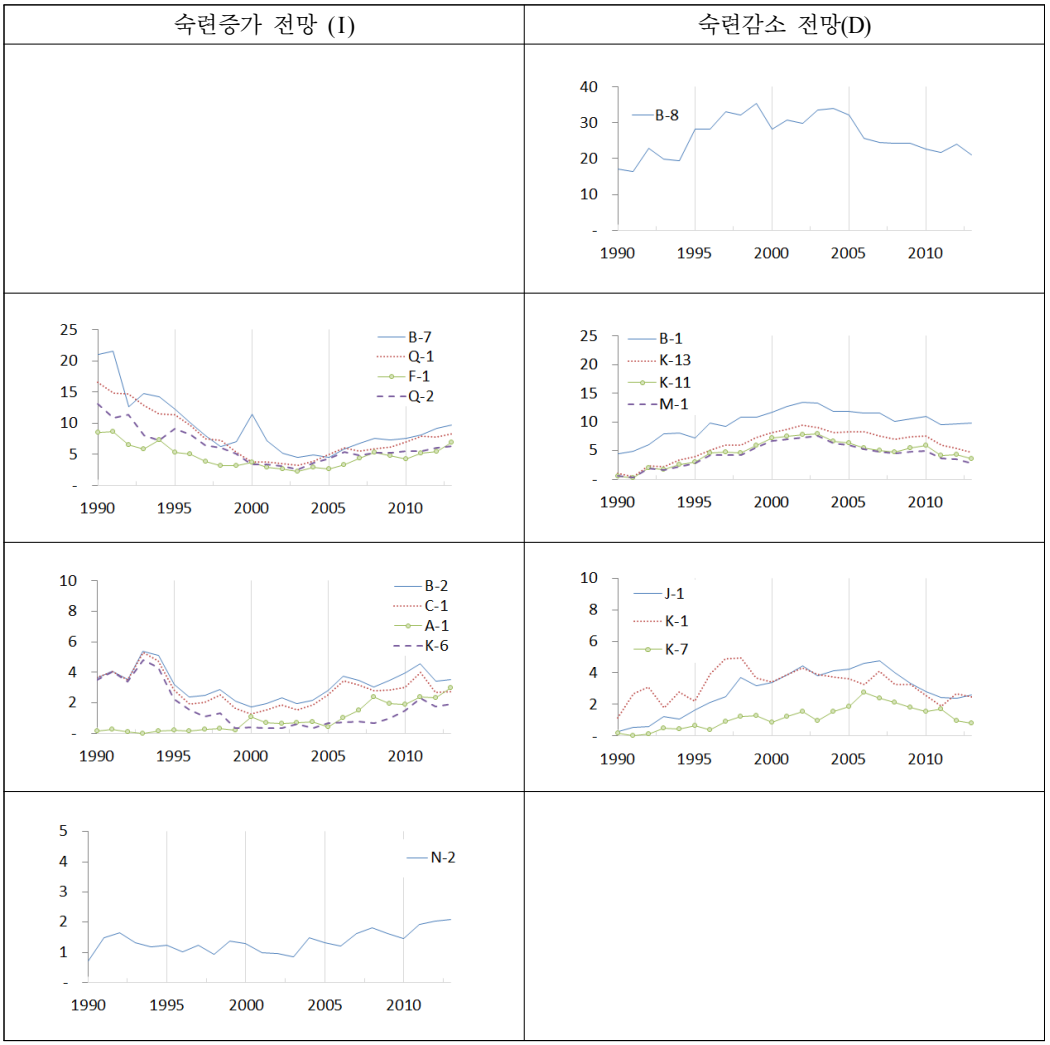
추출된 특허에서 나타나는 IPC(International Patent Classification, 이하 IPC) 일곱 자릿수 분류를 직무분석에서 제시된 필요숙련에 대응시키고, IPC 분포추이로부터 숙련전망을 제시하였다([그림 2] 참조).[2] 보안직무 숙련수요 추세를 전체와 20위 출원기업으로 구분하고, 다시 범용기술 관련 IPC 포함 여부를 구분하여 총 네 가지 추세를 분석하였는데, 최종적으로 다음의 세 가지 범주로 전망결과가 제시되고 있다. ① 지속적으로 중요성이 유지되는 숙련으로 '(B8) Network 보안'이 보이며, ② 새롭게 부상하는 숙련으로 '(F1) 암호화 알고리즘', '(B7) Data 보안', '(N-2) 암호학', '(A-1) 보안 취약점 분석', '(A-3) 모의해킹, 모의침투', '(B-6) PC 보안', '(B-2) 보안정책', '(Q-1) 보안 감사', '(Q-2) 정보보안 이벤트 관리' '(C-1) 개인정보보호법', '(C-2) 개인정보 암호화', '(K-6) DB 보안 암호화' 등이 포함되고 있다. ③ 예전에 비하여 독립적인 성격이 쇠퇴하여 기초숙련으로 편입되는 숙

2) 상세한 사항에 대해서는 황규희 외(2013) 미래숙련수요 분석을 위한 특허정보활용의 현실적 합성 분석의 5장을 참조하시오.

련으로 '(B1) 정보보호 관리체계', '(K13) 인증서비스', '(K-11) 모바일 디바이스 관리', '(M1) 취약점 분석', '(J-1) 보안 구조', '(K-1) 방화벽 구성', '(K-7) OTP' 등이 제시되고 있다(<표 9> 참조).

정보보호안업체 및 관련 전문가를 대상으로 수행한 이러한 조사결과는, 본 연구에서 수행된 숙련수요 전망의 현실적합성을 통계적으로 유의하게 지지하는 것으로 나타나고 있다(유의수준 5%에서 Fisher's Exact-Test 유의).

[그림 2] 출원특허 IPC 추이로부터 숙련수요 추이 전망



출처: 황규희 외(2013: 110), [그림 5-4] 인용.

〈표 9〉 IPC 추세로부터 숙련수요에 대한 전망

질적 숙련수요 전망 분류	숙련수요
① 지속적으로 중요성이 유지되는 숙련	(B-8) Network 보안
② 새롭게 부상하는 숙련	(A-1) 보안 취약점 분석 (A-3) 모의해킹, 모의침투 (B-2) 보안정책 (B-6) PC 보안 (B-7) Data 보안 (C-1) 개인정보보호법 (C-2) 개인정보 암호화 (F-1) 암호화 알고리즘 (K-6) DB 보안 암호화 (N-2) 암호학 (Q-1) 보안 감사 (Q-2) 정보보안 이벤트 관리
③ 예전에 비하여 범용숙련으로 전환	(B-1) 정보보호 관리체계성 (J-1) 보안 구조 (K-1) 방화벽 구성 (K-11) 모바일 디바이스 관리 (K-13) 인증서비스 (K-7) OTP (M-1) 취약점 분석

출처: 황규희 외(2013: 121)

Ⅳ. 정보보안학과 교육과정 분석

1. 학과목 단위로의 숙련단위 조정

본 절에서는 교과과정 정보가 공개된 16개 분석대상학교[3]의 교과과정과 앞 절에서의 숙련수요 전망 간의 대응성을 검토한다. 그런데 전문가들에 의한 1단계 검토과정에서 앞 절에서의 숙련수요 전망이 '기술'에 편중되어 있는 한편, 현재의 숙련항목은 정보보안 교육과정의 분류항목으로 정의되기 어렵고 체계적으로 분류되지 못하는 문제가 제기되었다.[4] 교과목 구성의 측면에서, 현재의 숙련항목들이 하나의 독립 과목으로 분류되기에는 작은 단위이기 때문에 유사 분류로 묶는 작업이 필요하다는 지적에 따라 <표 9>를 조정하였다.<표 10>과 같이 개인정보 암호화/ DB 보안 암호화/ 암호화를 '암호화'로 묶고, OTP/ 인증서비스도 '정보보호 프로토콜'로 묶으며, 보안취약점 분석/ 취약점 분석 도 'OS 보안'에 묶을 수 있을 것이다. Data 보안도 '암호화, 암호화 알고리즘'과 유사 분류로 묶을 수 있다. 방화벽 구성은 'Network 보안'에 포함될 수 있으며, 정보보안 이벤트 관리도 '시스템 보안'으로 포함될 수 있다. 그 외 모바일 디바이스 관리도 '시스템 보안'(혹은 '네트워크 보안)에서 수용될 수 있다. 이러한 재분류를 통해 미래숙련수요와 교육과정의 연계를 진단하고 개선 방안을 검토하기로 한다.

3) 4년제 대학에서 정보보안학과가 개설된 학교 중, 고려대 사이버 보안학과는 비공개인 가운데, 본 연구에서 분석대상이 된 학교는 건양대, 경동대, 동명대, 동신대, 목포대, 서울여대, 서원대, 성신여대, 세종대, 순천향대, 숭실사이버대, 영산대, 우석대, 중부대, 호서대, 호원대 등 16개교이다. 2013년 국가정보보호백서에 따르면, 이외에도 경기대학교, 고려사이버대, 광주대, 대전대, 동양대, 서남대, 세종사이버대, 한북대, 수원대, 경일대, 위덕대에도 정보보안 관련 학과가 있는 것으로 파악되고 있다(한국인터넷진흥원, 2013b: 207).

4) 앞 절에서의 숙련단위는 직무분석에서 기원한 것으로서, 교육과정 분석에 대응시키기 위해서는 조정이 요구된다. 이는, 근래 국가직무능력표준(NCS) 기반 학습모듈 개발에서 직무분석 단위와 교과목 단위의 매칭에 있어 문제가 제기되는 것과 유사한 문제이다.

<표 10> 교과단위 조정을 거친 숙련수요 전망

교과단위 조정 후		교과단위 조정 전	
질적 숙련수요 전망 분류	숙련수요	숙련수요	질적 숙련수요 전망 분류
① 지속적	시스템 보안	Network	① 지속적
		정보보안 이벤트 관리	② 새롭게 부상하는 숙련
		모바일 디바이스 관리	③ 예전에 비하여 범용숙련으로 전환
② 새롭게 부상하는 숙련	모의해킹, 모의침투	모의해킹, 모의침투	② 새롭게 부상하는 숙련
	보안정책	보안정책	
	PC 보안	PC 보안	
	OS 보안	보안 취약점 분석	
		취약점 분석	③ 예전에 비하여 범용숙련으로 전환
	암호학, 암호알고리즘	암호학	② 새롭게 부상하는 숙련
		개인정보 암호화	
		DB 보안 암호화	
		암호화 알고리즘	
		Data 보안	
	정보보호 관련법	개인정보보호법	
	보안 감사	보안 감사	
	디지털 포렌식	디지털 포렌식	
③ 예전에 비하여 범용숙련으로 전환	정보보호 관리체계	정보보호 관리체계	③ 예전에 비하여 범용숙련으로 전환
	Network 보안	방화벽 구성	
	보안 구조	보안 구조	
	정보보호 프로토콜	인증 서비스	
		OTP	

2. 정보보안학과 교육과정 분석

교과목 수준으로 구성한 숙련단위 13항목에 대하여 분석대상 16개교에서의 관련 교과목 개설 유무를 살펴보면(<표 11>참조), 관련 교과목 개설이 12개 항목에 해당하는 학교가 2개교, 11개 항목 4개교, 10개 항목 8개교, 9개 항목 1개교, 7개 항목 1개교로 나타나고 있다.[5] 이에 대하여 항목별로 살펴보기로 하자.

지속적으로 중요성이 유지되고 있는 '시스템 보안'에 대하여 관련 과목이 개설된 학교

는 총 15개로서 전체의 94%이다. 새롭게 부상하는 숙련으로 전망된 '암호학 및 암호알고리즘'. '디지털 포렌식'에 대해서는 모든 학교에서 관련 과목이 개설되고 있다. 그러나 역시 새롭게 부상하는 숙련으로 중요성이 증대되고 있는 '모의해킹 및 모의침투'에 대해서는 7개교, 'PC 보안'에 대해서는 6개교가 관련 과목을 개설하고 있으며, '보안 감사'에 대해서는 8개교, '보안정책'에 대해서는 15개교, '정보보보호법'에 대해서는 13개교가 개설하고 있다. 한편, 예전에 비해 범용숙련으로 전환하고 있는 '정보보호 프로토콜'에 대해서는 8개교, '보안 구조'에 대해서는 15개교가 각각 관련 과목을 개설하고 있다.

이에 대하여, '모의해킹 및 모의침투'는 이론보다는 실습 위주의 기능적인 사항으로서 4년제 대학에서 교육하기에는 다소 무리가 따른다는 평가가 제시될 수 있다(전문가 면담). 4년제 대학의 정규교과목으로보다는 2년제 대학 혹은 훈련기관에서 이수되는 것이 타당할 수 있는 가운데, 4년제 대학의 관련과목 개설이 실제 낮은 비율을 보인다고 여겨진다. 혹은 모의해킹/모의침투는 웹해킹/ 네트워크해킹 등 다양한 교과에 포함되어서 교육이 가능할 수도 있을 것이다. 한편, 'PC 보안'도 기능적인 사항으로서, 4년제 대학의 교과목으로 적절하지 않을 수 있다는 판단이 제기될 수도 있고, 혹은 서버를 포함한 시스템 보안의 차원으로 'OS 보안'과목에 통합되어 다루어질 수도 있을 것이다. 이상의 기능적인 부분들이 4년제 대학에서 교과목으로 다루어지기에 적합하지 않다거나 유관과목에서 다루어질 수 있다는 것을 인정한다면, 전반적인 교과과정 구성에서 정보보안의 숙련수용에 대한 대응성에 별다른 문제점이 없다고 할 수 있을 것이다.

5) 현재의 분석에서 숙련항목 간 크기가 동일하지 않다는 지적이 제기될 수 있다. 예를 들어 '암호학 및 암호알고리즘'이 'PC 보안'과 'OS 보안'을 합한 것보다 크다는 판단이 있을 수 있다. 이를 고려한 가중치 부여 및 관련 과목 수(부록 1 참조)가 고려될 수 있으나, 본 연구에서는 단기 과제의 한계 속에 후속 연구과제로 남긴다.

〈표 11〉 미래숙련수요 대응 관련 과목 개설 유무

	① 지속적 중요	② 새롭게 부상하는 숙련								③ 예전에 비하여 범용숙련으로 전환				대응교과가 있는 미래숙련 수요 항목 수
	시스템 보안	모의해킹, 모의침투	보안 정책	PC 보안	OS 보안	암호학, 암호 알고리즘	정보보호 관련법	보안 감사	디지털 포렌식	정보보호 관리체계	Network 보안	보안 구조	정보보호 프로토콜	
관련 과목 개설 유무	15	7	15	6	14	16	13	8	16	15	16	15	8	계
	94%	44%	94%	38%	88%	100%	81%	50%	100%	94%	100%	94%	50%	
U01	1	1	1	1	1	1	1	1	1	1	1	1	0	12
U02	1	1	1	1	1	1	0	1	1	1	1	1	1	12
U03	1	1	1	1	0	1	1	0	1	1	1	1	1	11
U04	1	1	1	0	1	1	1	0	1	1	1	1	1	11
U05	1	0	1	1	1	1	1	0	1	1	1	1	1	11
U06	1	0	1	1	1	1	1	1	1	1	1	1	0	11
U07	1	0	1	0	1	1	1	1	1	1	1	1	0	10
U08	1	0	1	0	1	1	1	0	1	1	1	1	1	10
U09	1	0	1	0	1	1	0	1	1	1	1	1	1	10
U10	0	0	1	1	1	1	1	1	1	1	1	1	0	10
U11	1	0	1	0	1	1	1	1	1	1	1	1	0	10
U12	1	1	1	0	1	1	1	0	1	1	1	1	0	10
U13	1	1	1	0	1	1	1	0	1	1	1	1	0	10
U14	1	0	1	0	1	1	1	0	1	1	1	1	1	10
U15	1	0	1	0	0	1	0	1	1	1	1	1	1	9
U16	1	1	0	0	1	1	1	0	1	0	1	0	0	7

출처: 전문가그룹 자문에 기반하여 작성.

그러나 '모의해킹 및 모의침투'가 학원이나 전문대 수준에서만 다루어질 사항이 아니라 정보보안의 가장 핵심적인 사항의 하나로 여겨질 수도 있다. 또, 교과목 개설만으로 보았을 때 '보안정책', '정보보보호법' 등의 경우 비교적 많은 학교에서 관련 과목이 개설된 것으로 나타나나, 관련 전임교원 확보 등 교육과정의 측면에서는 개선이 여지가 있는 것으로 여겨진다. 이에 대하여 세부 영역별로 문제점 및 개선방향을 진단하기로 한다.

첫째, 정보보호 관련 기능교육의 강화 및 실습 강화가 이루어져야 할 것이다. '모의해킹, 모의침투'는 이론보다는 실습 위주의 과목으로서 각 부문(OS, 시스템, 네트워크)별 보안과목 내 모의해킹 및 모의 침투 과정의 포함이 필요하다고 여겨진다. 다만, 각 부문(OS, 시스템, 네트워크)별 차이에 따라 모의해킹 및 모의침투 시나리오 구상에 어려움이 따르는 문제가 있기에, 모의해킹 및 모의침투 시나리오 구상에 맞는 필수 과목 선정이 필요하며, 이에 대한 실습이 강화될 필요가 있다. 한편, 보안 구조에 대해서도 타 공학부문(통신, 설계 등)과의 연계가 강화되는 것이 바람직한데, 이를 위하여 물리, 시스템, 네트워크 등을 포함한 전반적인 보안 구조를 설계하고 테스트할 수 있는 실습 과정의 개설이 요구된다.

둘째, 외견상 관련 과목의 개성에도 불구하고 관련 전임교원 및 전공자 확보가 제대로 이루어지지 않아 이의 개선이 시급히 요구된다. 개인정보보호법, 저작권법, 개인정보보호법 등이 포함되는 '정보보호 관련 법제'는 그 중요성이 매우 높은 가운데 관련 과목이 개설된 학교가 16개교 중 13개교(81%)로서 개설과목 비율이 그리 낮다고 할 수는 없으나, 이에 대한 전임교원이 확보된 학교가 거의 없는 상황이다. 유사하게 'OS 보안'의 경우에도 14개교(88%)가 관련 과목을 개설하고 있으나, 이를 전공한 교수는 많지 않은 상황이다.

셋째, 정보보호의 수요 대응성을 제고하기 위해 학과 간 융합 및 산학협력에 의한 교육과정 개발이 필요하다. 정책적인 측면에서 그 중요성이 증대되고 있는 '보안정책'에 대하여 12개교(94%)가 관련 과목을 개설하고 있으나, 실제는 정보보호개론 내에 포함한 수준이라고 여겨진다. 이는 '보안 감사' 관련 과목을 개설하고 있는 학교가 8개교(50%)에 머물고 있는 것과도 연관된다고 판단된다. 보안정책은 '정책-법제-경영' 등과의 연계가 필요하며, 대학보다는 각 기관 및 기업 등의 실정에 맞는 교육과정이 필요할 것이다. 이에 대한 대응을 정보보안학과 단독으로 수행하기에는 어려움이 있을 것이며, '법학·행정학·경영학' 등과 연계한 '보안정책개론(가칭)'과 같은 전문적인 보안정책에 대한 과목 신설 및 산학협력을 통한 보안정책과목의 개설이 요구된다.

넷째, 정보보안의 심화 전문과정과 체계적인 연관성을 가진 교육과정 구성이 요구된다. 예를 들어 '보안 감사'는 경영 및 법률 등과의 연계가 필요한 과목으로, 보안 실무자보다 상위 관리자(임원 등)에게 적합한 과정으로 판단된다. 대학 수준에서 보안정책, 법률 등과 연계한 기초 감사 과목을 개설하고, 전문 심화과정으로서 대학원 및 산학협력을 통한 상위 관리자 및 임원급 교육과정 내에 전문적인 보안 감사 과목의 개설이 도모될 수 있을 것이다. 또 다른 사례로, '정보보호 프로토콜'은 정보보호이론을 기반으로 하여 실생활에 적용되는 응용 프로토콜을 이해하는 과목으로, 대학교보다는 대학원에서 개설되는 것이 적합한 과목이라고 여길 수 있다. 내용 분류를 통해 기초적인 부분의 정보보호 프로토콜과 심화적인 부분의 정보보호 프로토콜로 분류하여 기초적인 부분은 대학교에서, 심화적인 부분은 선택적으로 대학원에서 개설될 수 있도록 세부적인 작업이 요구된다.

다섯째, 정보보안 내 세부 과목 신설이 강화되어야 한다. 예컨대. 'PC 보안'의 경우 많은 학교에서 이에 대한 과목이 소홀히 다루어지고 있는데, 이는 대부분의 대학이 서버/DB 등의 전문 시스템 보안에 치중하기 때문으로 여겨진다. 그러나 PC를 서버/데이터베이스로 사용하는 경우가 많고, 시스템/OS/네트워크 보안과도 일정부분 연관된다고 할 수 있으며, 최종사용자에 대한 보안을 통합(PC 보안, DB 보안 등)하여 전문과목으로 개설하는 것이 적절할 것이다. 이와 유사하게 사고조사를 위한 '디지털 포렌식' 항목은 모든 학교에서 수행되고 있으며, 중요성이 강화되고 있는 가운데 이에 대한 세부 과목의 개발이 필요할 것으로 여겨진다.

여섯째, 정보보안 내 특성화가 모색될 필요가 있다.[6] 위에서 제시되는 개선 필요 사항을 모든 학교에서 수행하기에는 제반 여건상 현실적인 어려움이 있을 수 있다. 학교급별로 고등학교, 전문대에서는 기능 위주 및 자격증 중심의 교육을 강조할 수 있고, 4년제 대학에서는 이론과 고급기술 중심, 대학원에서는 제도, 법규 등을 다루며 보안정책연구를 수행할 수 있을 것이나, 구체적인 사항은 학교의 주안점에 따라 상이할 수 있을 것이다. 이에 학교별로 정보보안 내 특성화 부문을 발전시키는 노력이 요구된다.

6) 국제적으로 가장 널리 알려진 정보보호 2대 자격증인 CISSP(Certified Information System Security Professional)와 CISA(Certified Information Systems Audit)의 정보보호 분야 구분 및 시험영역을 참고로 할 수 있을 것이다.

Ⅴ. 요약 및 정책적 시사

본 연구는 대학 교육과정 개발에서 미래숙련수요 전망과의 연계성이 어떻게 이루어질 수 있을지를 보이고자 하였다. 관련 선행연구(황규희 외, 2013)에서 구해진 정보보안 부문의 미래숙련수요 전망을 활용하여, 정보보안학과가 있는 4년제 대학 16개교의 교육과정을 분석하였다. 이러한 분석결과에 기반하여 향후 대학특성화 지원을 위한 교육과정의 수집·분석 및 미래숙련수요에 대응하는 교육과정 개발 방안을 제시하고자 한다.

먼저, 교과목 수준으로 재구성한 미래숙련수요 13항목에 대하여, 분석대상 16개교에서의 관련 교과목 개설을 중심으로 교육과정 분석을 수행하였으며, 과정 분석을 통해 도출된 주요 제언은 다음과 같다.

첫째, 정보보호 관련 기능교육의 강화 및 실습 강화가 이루어져야 한다. '모의해킹, 모의침투'는 이론보다는 실습과정의 강화가 필요하다고 여겨진다. 보안 구조에 대해서도 타 공학부문(통신, 설계 등)과의 연계가 강화되는 것이 바람직한데, 이를 위하여 물리, 시스템, 네트워크 등을 포함한 전반적인 보안 구조를 설계하고 테스트할 수 있는 실습 과정의 개설이 요구된다.

둘째, 외견상 관련 과목의 개설에도 불구하고 관련 전임교원 및 전공자 확보가 제대로 이루어지지 않아 이의 개선이 시급히 요구된다. 개인정보보호법, 저작권법, 개인정보보호법 등이 포함되는 '정보보호 관련 법제'는 그 중요성이 매우 높은 가운데 이에 대한 전임교원의 확보가 요구된다. 유사하게 'OS 보안'의 경우에도 이를 전공한 전임교원의 확보가 강화되어야 한다.

셋째, 정보보호의 수요 대응성을 제고하기 위해 학과 간 융합 및 산학협력에 의한 교육과정 개발이 필요하다. 정책적인 측면에서 그 중요성이 증대되고 있는 '보안정책'에 대하여 '정책-법제-경영' 등과의 연계가 필요하며, 대학보다는 각 기관 및 기업 등의 실정에 맞는 교육과정이 필요할 것이다. 이에 대한 대응을 정보보안학과 단독으로 수행하기에는 어려움이 있을 것이며, '법학-행정학-경영학' 등과 연계한 '보안정책개론(가칭)'과 같은 전문적인 보안정책에 대한 과목의 신설 및 산학협력을 통한 보안정책과목의 개설이 요구된다.

넷째, 정보보안의 심화 전문과정과 체계적인 연관성을 가진 교육과정 구성이 요구된다. 예를 들어 '보안 감사'는 대학 수준에서 보안정책, 법률 등과 연계한 기초 감사 과목을 개설하고, 전문 심화과정으로서 대학원 및 산학협력을 통한 상위 관리자 및 임원급 교육과

정 내에 전문적인 보안 감사 과목의 개설이 도모될 수 있을 것이다. '정보보호 프로토콜'은 기초적인 부분의 정보보호 프로토콜과 심화적인 부분의 정보보호 프로토콜로 분류하여, 기초적인 부분은 대학교에서, 심화적인 부분은 선택적으로 대학원에서 개설되될 수 있도록 세부적인 작업이 요구된다.

다섯째, 정보보안 내 세부 과목 신설이 강화되어야 한다. 예컨대 'PC 보안'의 경우 최종사용자에 대한 보안을 통합(PC 보안, DB 보안 등과 통합)하여 전문과목으로 개설하는 것이 적절할 것이다. 이와 유사하게 사고조사를 위한 '디지털 포렌식' 항목도 그 중요성이 강화되고 있는 가운데 이에 대한 세부 과목의 개발이 필요할 것으로 여겨진다.

여섯째, 정보보안 내 특성화가 모색될 필요가 있다. 위에서 제시되는 개선 필요 사항을 모든 학교에서 수행하기에는 어려움이 현실적인 있을 수 있으며, 학교의 주안점에 따라 정보보안 내 특성화 부문을 발전시키는 노력이 요구된다.

이상의 분석 및 제언 사항은 ICT 인력 종합계획 등에서 활용될 수 있을 것이다. 아울러 향후 미래숙련수요 분석을 활용한 교육과정 분석의 확장을 도모하고 인프라로서의 교육과정 수집 체계 구축에서 유용한 시사점을 제공할 것이다. 특히, 2014년 대학특성화알리미에서 특성화학과 교과과정 개선실적이 템플릿 방식으로 수집되고, 2015년 대학정보공시에서 특성화학과 교과과정 개선실적의 의무 탑재가 계획되고 있는 가운데, 미래숙련수요에 대한 대응성을 높이기 위한 교육과정 수집 및 분석 체계를 다음과 같이 고려할 수 있을 것이다.

첫째, '정보보안'이라는 영역 내에서도 세부 특성화의 방향이 (1) '모의해킹, 모의침투'와 같은 실습 중심의 특성화, (2) '정보보호 관련 법제', '보안정책', '보안 감사'과 같이 기술 이외에 정책-법제-경영 등과의 학제간 융합 및 산학협력 특성화, (3) 보안 구조와 같이 타 공학부문(통신, 설계 등)과 연계된 공학 내 융합 특성화, (4) 세부 과목 확장에 의한 전문화 특성화 등으로 구체화될 수 있을 것이다. 유사하게 특정 영역에 대한 특성화가 미래수요에 대응하는 구체적인 영역에 집중할 수 있도록 유도되어야 할 것이다. 이러한 특성화는 해당학과의 전임교원 구성 및 충원 계획에 기반하거나 외부 자원(유관학과 및 산학협력 등)에 기반한 교과목 개발 및 운영 가능성 등이 전제되어야 한다. 이에 특성화 계획 수립 및 운영에서 내부(자체 전임교원) 및 외부(유관학과 및 산학협력 등) 자원 운영에 대한 사항이 고려될 필요가 있다.

둘째, 미래숙련수요 분석 및 전망 단위와 교과구성의 연계성이 강화될 필요가 있다. 모

든 경우에 이러한 요구가 가능하지는 않을 것이나 미래유망기술, 미래유망산업과 연계성을 표방하는 특성화의 경우라면 해당 기술 및 산업에서 요구되는 숙련단위에 대응하는 교과구성을 마련하도록 하고, 이에 대한 자체 진단 및 평가를 유인하는 것이 필요하다.

셋째, 미래숙련수요 분석 및 전망이 기술전망에 한정될 수는 없을 것이나 미래유망기술, 미래유망산업과 연계성을 표방하는 특성화의 경우에는 특허정보 등을 이용한 기술전망이 교과구성의 대응성 제고에 도움이 될 수 있다고 여겨진다. 특허정보 이외에도 각종 기술정보 분석(논문 분석, 인터넷 정보 분석 등) 결과를 반영하는 것도 적극 장려되어야 할 것이다.

넷째, 특성화 정보 수집에 있어서 교육과정(교과과정뿐 아니라 관련 전임교원 확보 포함) 관련 사항을 특성화 세부 방향성을 확인할 수 있는 수준에서 모으는 것이 특성화 정책의 효율적 운영을 위해 필요하다. 수집된 정보를 분석하고, 나아가 미래숙련수요 대응성을 높이기 위한 교과구성 설계를 지원하도록 하는 정책 지원 방안이 마련되어야 한다.

참고문헌

김정덕·백태석(2011).「정보보호 전문인력 양성을 위한 필수요구지식 및 교육인증 프로그램」,『디지털정책연구』, 제9권 제5호, 113~121쪽.

김태성(2010).「정보보호인력 양성정책」, 충북대출판부.

신현석(2009).「대학경쟁력 제고를 위한 대학특성화의 방향」,『고등교육정책연구』, 제2권 제1호, 47~73쪽.

전효정·유혜원·김태성(2008).「정보보호 분야 직무별 필요 지식 및 기술 분석」,『한국경영정보학회지』, 제10권 제2호, 253~267쪽.

정대율(1999).「정보시스템 전문가의 요구지식 및 기술능력에 기초한 MIS 교과과정 개발에 관한 연구」,『한국경영정보학회지』, 제1권 제1호, 137~163쪽.

지식경제부(2011).「대한민국 산업기술 비전 2020: 정보통신」.

최명길·김세헌(2004).「정보보호 전문가의 직무수행을 위한 지식 및 기술 분석」,『한국경영정보학회지』, 제14권 제4호, 71~85쪽.

한국인터넷진흥원(2010).「지식정보보안 분야 인력현황 및 중장기 인력수급 전망 분석: 정보보안인력을 중심으로」.

한국정보보호학회(2010).「지식정보보안 분야 인력현황 및 중장기 인력수급 전망 분석」, 한국인터넷진흥원.

한국정보처리학회(2010).「미래 인터넷 보안기술 및 정보보호 등에 대한 이유 및 개발수요조사」, 한국인터넷진흥원.

한국인터넷진흥원(2013a).「정보보호 관리체계(ISMS) 인증 제도 안내서」.

_____(2013b).「국가정보보호백서」.

_____(2011).「2011 국내정보보안산업 실태조사」.

황규희(2013). "대학특성화알리미 자료 분석을 통해 본 대학특성화 현황과 개선 과제," 제46차 인재개발정책 포럼 발표자료.

황규희 외(2013).『미래숙련수요 분석을 위한 특허정보활용의 현실적합성 분석』, 한국직업능력개발원.

Irvine, C.E. and Shiu-Kai Chin(1998). "Integrating security into the curriculum", *Computer*,

Vol.31 No.12, pp. 25~30.

IT Security EBK(2012). *IT Security Essential Body of Knowledge(EBK): A Competency and Functional Framework*, U.S. Department of Homeland Security.

Simpson, Henry K., Lynn F. Fischer, John D. Tippit, Alissa Hayes(2006). *Development and Application of Skill Standards for Security Practitioners*, US Department of Defense Technical Report, 06-1.

Abstract

Analysis on Engineering School Curriculum for Future oriented higher education specialization : with the case of Information Security major

Gyu-hee Hwang

Analysis on Engineering School Curriculum for Future oriented higher education specialization : with the case of Information Security major

This study attempts to analyze the curriculum of information security which is recently drawing hot attention, in connection with higher education specialization. Corresponding analysis of curriculum to future skills needs was conducted with the 16 Universities, which have information security department in undergraduate course. For the future-oriented higher education specialization, the followings are suggested: to require detailed specialization master-plan corresponding to future needs based on execution plan of the internal resource (faculty) and external resource (relevant department and industry-academy cooperation; to provide subject unit corresponding to the skills unit, which is required by the prospective future technology and industry, and to attract conducting self-evaluation of the curriculum; to utilize technological forecast using patent information, etc. in forecasting future skills needs; to strengthen the policy assistance to collect curriculum and to develope it.

- Keywords: future skills needs, higher education specialization, information security, patent analysis, curriculum analysis

<부록 1> 미래숙련수요 대응 관련 과목 개설 수

	정보보호 관리체계	모의해킹, 모의침투	보안 정책	PC 보안	OS 보안	시스템 보안	Network 보안	보안 구조	암호학, 암호 알고리즘	정보보호 프로토콜	정보보호 관련법	보안 감사	디지털 포렌식
관련 과목 개설 수	41	13	27	6	25	62	58	20	25	10	16	8	33
U01	1	2	3	1	2	7	2	1	2	0	1	1	1
U02	4	2	5	1	1	5	2	3	2	2	0	1	2
U03	2	1	2	1	0	3	4	1	1	1	1	0	1
U04	4	2	2	0	3	8	6	1	1	1	1	0	2
U05	3	0	1	1	1	3	3	1	3	2	2	0	1
U06	2	0	1	1	2	2	2	1	2	0	1	1	1
U07	3	0	3	0	3	6	3	2	2	0	1	1	1
U08	1	0	1	0	1	3	2	1	4	1	1	0	1
U09	3	0	1	0	1	5	2	1	1	1	0	1	1
U10	2	0	2	1	1	0	2	1	1	0	1	1	5
U11	3	0	2	0	1	2	1	1	1	0	2	1	5
U12	4	1	1	0	3	5	6	2	1	0	2	0	1
U13	4	4	1	0	2	3	5	1	1	0	1	0	4
U14	3	0	1	0	2	4	11	1	1	1	1	0	1
U15	2	0	1	0	0	3	3	2	1	1	0	1	1
U16	0	1	0	0	2	3	4	0	1	0	1	0	5

<부록 2> 2013년 정보보호 관리체계 인증기준

분야		통제항목 수	세부점검항목	통제항목 수	세부점검항목
정보보호 관리과정	정보보호 정책 수립	2	7	-	-
	관리체계 범위 설정	2	4	-	-
	정보보호정책수립 및 범위설정	-	-	2	4
	경영진 책임 및 조직구성	-	-	2	4
	위험 관리	5	19	3	11
	구현	2	7	-	-
	정보보호대책 구현	-	-	2	3
	사후 관리	3	10	3	6
	소계	14	47	12	28
문서화	분서 요건	1	1	-	-
	문서의 통제	1	1	-	-
	운영기록의 통제	1	1	-	-
	소계	3	3	-	-
정보보호 대책	정보보호 정책	5	10	6	13
	정보보호 조직	4	11	4	7
	외부자 보안	4	8	3	4
	정보자산 분류	4	7	3	7
	정보보호 교육 및 훈련	4	14	-	-
	정보보호교육	-	-	4	10
	인적 보안	5	18	5	11
	물리적 보안	12	36	9	21
	시스템 개발 보안	13	53	10	22
	암호 통제	3	6	2	8
	접근 통제	14	38	14	46
	운영 관리	22	99	-	-
	운영 보안	-	-	22	56
	전자거래 보안	5	21	-	-
	보안사고 관리	7	20	-	-
	침해사고 관리	-	-	7	14
	검토·모니터링·감사	11	37	-	-
	업무 연속성 관리	7	18	-	-
	IT재해복구	-	-	3	6
	소계	120	396	92	225
총계		137	446	104	253

출처: 한국인터넷진흥원(2013a: 38).

<부록 3> 숙련 영역별 교육과정 진단

숙련 영역	과목 개설률	과목 개설률	미개설 학교
모의해킹, 모의침투	44%	U01	U05
		U02	U06
		U03	U07
		U04	U08
		U012	U09
		U013	U10
		U016	U11
			U14
			U15
진단	- OS/시스템/네트워크 등 각 부문 보안과 직간접적으로 연관된 부분으로, 정의 및 범위가 매우 광범위함. - 이론보다는 실습 위주의 과목 - 전공과목들이 필수/선택 과목으로 분류되어 학생들이 습득한 분야(N/W, OS 보안 등)가 다름. - 습득된 분야가 다르므로 모의해킹 및 모의침투 시나리오 구상에 어려움이 따름.		
개선 필요	- 각 부문(OS, 시스템, 네트워크)별 보안과목 내 모의해킹, 모의침투 과정의 포함이 필요함. - 각 부문별 보안과목의 시험(실습)으로 활용 - 모의해킹, 모의침투 시나리오 구상에 맞는 필수 과목 선정이 필요함.		

숙련 영역	과목 개설률	개설 학교	미개설 학교
보안정책	95%	U01	U16
		U02	
		U03	
		U04	
		U05	
		U06	
		U07	
		U08	
		U09	
		U10	
		U11	
		U12	
		U13	
		U14	
		U15	
진단	- 개설 학교들도 정보보호개론 내에 포함한 수준으로, 전문적인 보안정책 과목 개설 학교는 6개(38%)에 불과함.		
개선 필요	- 보안정책은 경영, 법률 등과의 연계가 필요하며, 대학보다는 각 기업 및 기관 등의 실정에 맞는 교육과정이 필요할 것으로 보임. - 보안정책개론(가칭) 등 전문적인 보안정책에 대한 과목의 신설 및 산학협력을 통한 보안정책 지식 습득과정의 신설이 필요함.		

숙련 영역	과목 개설률	개설 학교	미개설 학교
PC 보안	38%	U01	U04
		U02	U07
		U03	U08
		U05	U09
		U06	U11
		U10	U12
			U13
			U14
			U15
			U16
진단	- 대부분의 대학이 서버/DB 등의 전문 시스템 보안에 치중한 것으로 판단됨. - 대다수의 PC가 Windows OS를 사용 중이며, PC를 서버/데이터베이스로 사용하는 경우도 많으므로 시스템/OS/네트워크 보안과도 일정부분 연관됨.		
개선 필요	- 엔드포인트에 대한 보안을 통합(PC 보안, DB 보안 등)하여 하나의 과목 신설이 필요		

숙련 영역	과목 개설률	개설 학교	미개설 학교
보안 구조	94%	U01	U16
		U02	
		U03	
		U04	
		U05	
		U06	
		U07	
		U08	
		U09	
		U10	
		U11	
		U12	
		U13	
		U14	
		U15	
진단	- 개설 학교들도 정보보호개론 내에 포함한 수준으로, 전문적인 보안 구조 과목 개설 학교 는 1개(1%)에 불과함. - 각 부분별 보안 과목과 직/간접적인 영향이 있는 과목이며, 타 공학(통신, 설계 등)과의 연계가 필요할 것으로 판단됨.		
개선 필요	- 보안 구조에 대해 교육할 수 있는 별도의 과정 개설 필요. - 물리, 시스템, 네트워크 등을 포함한 전반적인 보안 구조를 설계하고 테스트 할 수 있는 실습 과정의 개설이 필요함.		

숙련 영역	과목 개설률	개설 학교	미개설 학교
정보보호 프로토콜	50%	U02	U01
		U03	U06
		U04	U07
		U05	U10
		U08	U11
		U09	U12
		U14	U13
		U15	U16
진단	- 정보보호이론을 기반으로 하여 실생활에 적용되는 응용 프로토콜을 이해하는 과목으로 대학교보다는 대학원에서 개설되는 과목으로 보임		
개선 필요	- 내용 분류를 통해 기초적인 부분의 정보보호 프로토콜과 심화적인 부분의 정보보호 프로토콜로 분류하여 기초는 대학교에서 개설되고, 심화적인 부분은 선택적으로 대학원에서 개설되는 작업이 필요		

숙련 영역	과목 개설률	개설 학교	미개설 학교
보안 감사	50%	U01	U03
		U02	U04
		U06	U05
		U07	U08
		U09	U12
		U10	U13
		U11	U14
		U15	U16
진단	- 경영, 법률 등과의 연계가 필요한 과목으로, 보안 감사는 보안 실무자보다 상위 관리자(임원 등)에 적합한 과정으로 판단됨.		
개선 필요	- 대학교에서는 보안정책, 법률 등과 연계한 기초 감사 과목의 개설이 필요. - 대학원 및 산학협력을 통한 상위 관리자 및 임원급 교육과정 내에 전문적인 보안 감사 과목 개설 필요.		

□ **저자 약력**

• 황규희
- 한국직업능력개발원 연구위원

미래지향 대학특성화를 위한 공학부문 교육과정 분석 연구: 정보보안 전공을 중심으로

· 발행연월일 2013년 12월 25일 인쇄
2013년 12월 27일 발행

· 발 행 인 박 영 범

· 발 행 처 한국직업능력개발원
135-949, 서울특별시 강남구 삼성로 147길 46
홈페이지: http://www.krivet.re.kr
전 화: (02)3485-5000, 5100
팩 스: (02)3485-5200

· 등 록 일 자 1998년 6월 11일

· 등 록 번 호 제16-1681호

· I S B N 978-89-6355-654-3 93320

· 인 쇄 처 (주)한국장애인문화인쇄협회 (02)2683-0955

 〈값 4,000원〉