經營科學
第31卷 第4號
2014年 12月, pp.1-13
http://dx.doi.org/10.7737/KMSR.2014.31.4.001

# 특허분석을 통한 정보보안 부문 미래교육 수요분석

황규희[1] · 임명환[2] · 송경석[3] · 이중만[3†]
[1]한국직업능력개발연구원, [2]한국전자통신연구원 기술전략본부, [3]호서대학교 경영학부

# Future Education Skills Needs Analysis through Patent Analysis in the field of Information Security

Gyuhee Hwang[1] · Myung-Hwan Rim[2] · Kyungseok Song[3] · Jung Mann Lee[3†]
[1]KRIVER
[2]ETRI
[3]Hoseo University

■ Abstract ■

This study aims to expand the future study methodology and to develop a methodology of future-oriented curriculum analysis with future skills needs derived from patent analysis. With the case of information security, the methodology is applied to the 16 universities, which have information security department in undergraduate course. From the results, the followings are suggested : 1) for the increasing importance area including hacking, infiltration and PC security, a practical exercise should be emphasized; 2) for the convergence area including security policy, security legislation and OS security, proper faculties should be filed with recruiting field-based experts; 3) for the increasing importance area including professional area including security audit and information security protocol, the advanced curriculum related to graduate level should be provided.

Keywords : Future Study, Future Skills Needs, Information Security, Patent Analysis

논문접수일 : 2014년 09월 12일 논문게재확정일 : 2014년 10월 14일
논문수정일 : 2014년 10월 16일
† 교신저자, mann@hoseo.edu

# 1. 서 론

기술혁신의 가속화 가운데, 향후 20년간 아직 등장하지 않은 많은 직업들이 새로 생겨날 것이고 또한 기존 직업에서 요구하는 숙련사항도 지속적으로 변화할 것으로 생각된다. 이에 대하여 각급 학교-훈련기관들이 대비하여야 한다는 인식은, 지난 2010년 서울 정상회의의 일환으로 추진된 G20 훈련전략에서 미래숙련수요 전망과 대응이 주요 의제의 하나로 제기되었다. 이는 또한 각국 정부뿐 만 아니라 World Bank, ILO 및 OECD 등에서도 미래숙련에 대한 대응 필요성을 지속적으로 제기하는 이유이다.

그간의 미래숙련수요전망은 노동시장 정보에 주로 의존하는 가운데, 고용주 조사 또는 산업구조분석을 통한 수요예측으로 수행되고 있다. 이는 기존 직업분류에 기반을 두고 현재 직무에서 요구되는 업무수행능력에 초점을 두는 것으로서, 가까운 미래에 대한 숙련수요 조사로 간주되어야 할 것이다. 산업수요와 밀접한 연관성을 가지는 교육과정에서 현재의 산업요구에 대한 대응성이 중요시되는 데, 기존 직무분석 기반의 교육과정 개발만으로는 빠른 기술변화에 대응하는 데 한계를 가질 수밖에 없다는 문제가 제기된다. 기술진보가 빠르게 진행되는 경우에, 보다 직접적으로 기술변화추이를 분석하고 이러한 기술변화에 선제적으로 대응하기 위한 노력이 필요할 것이다.

분석대상으로는 근래 많은 관심이 고양되고 있는 정보보안을 사례로 한다. 정보보안과 관련된 용어를 살펴보면, 해킹이란 용어 자체는 1960년대부터 있었으나 1980년대 후반 이후 네트워크 확대에 따라 정보보안이 본격적인 사회문제로 부상하였다. 특히, 2001년 9.11 사건에서 보안의 문제가 세계적 관심사가 되고, 한국에서도 2009년 DDoS 공격, 2011년 은행 전산망 마비, 2012년 통신사 및 2014년 금융기관 개인정보 대규모 유출 등이 나타나는 가운데 정보보안에 대한 국가적 관심이 고양되고 있다. 정보보안은 IT 기반 미래 성장산업 육성에서 산업적 중요성이 강조될 뿐만 아니라, 안보 등의 측면에서도 국가 전략적 중요성이 매우 높은 가운데 근래 정보보안학과가 급속히 증가하고 있다. 이에 대하여 본 연구에서는 미래지향 교육훈련을 위하여, 특허분석에 기반한 미래숙련수요전망 결과를 활용하여 현행 관련 교과과정의 대응성을 분석하며 기술변화에 선제적으로 대응하는 교과과정의 개발 방안을 제안하고자 한다.

본 연구[1]는 먼저 제 2장에서 정보보안 부문의 기술변화에 대응한 인력양성에 대한 국내외 동향을 살펴보고, 관련 연구를 검토한다. 제 3장에서는 본 연구에서 수행되는 분석체계 및 분석방법을 소개하고, 제 4장에서는 정보보안 부문의 미래 숙련수요 전망하고, 제 5장에서는 본 연구의 핵심으로 선행연구에서 제시된 정보보안 부문의 미래 숙련수요 전망을 기준으로, 기존의 교과과정의 대응성을 분석한다. 그리고 마지막 결론에서는 본 연구의 성과와 한계, 후속연구과제 등이 논의된다.

# 2. 선행연구 검토

본 연구에서의 정보보안(Information Security)이란, 정보시스템이나 네트워크에 존재하는 데이터와 같은 정보의 보호와 관련된 제반 사항을 일컫는다. 한국정보처리학회[11]는 EU FP7(7th Framework Programme for Research Technological Development)에서 제시한 미래 인터넷 보안 자료를 기반으로, 이에 대한 국내 전문가들에 의한 정보보안 이슈의 우선순위를 선정하였다. 이에 따르면, 네트워크 보안 이슈가 최우선적인 이슈로 제시되며, 이어서 인증 보안 이슈, 클라우드 및 모바일 보안 이슈, 통합 · 관리 보안 이슈의 순으로 나타날 것을 예상된다.[2]

선진 각국을 중심으로 정보보안이 지속적인 문제가 되는 가운데 정보보안 교육과정 등에 대한 관

1) 본 연구는 미래숙련수요전망에 기반한 교육과정개발을 위한 방법론의 본격적 개발에 앞선 탐색적 수준의 방법론적 모색으로 여겨져야 할 것이다

2) 한국정보처리학회([11], 55, 123)를 정리하였다.

심이 증대하고 있다. 가장 앞서가고 있다고 여겨지는 미국의 경우에 정보보호 표준교육과정에 대한 지침이 지난 1994년에 제시되었으며, 근래 2014년 2월 국가표준기술연구원(NIST)에서 국가 사이버 보안 프레임웍을 제시하였다(NIST[23]). 전통적으로 기술 분야의 교육과정 개발은 과학기술의 발전에 따른 기초과목 구성 뿐 아니라 관련 직무분석에 기반한 응용과목이 제시되고 있는데, 미국의 경우 Simpson et al.[25]은 정보보안 전문가 직무분석에서 보안담당자를 위한 숙련 표준의 개발과 적용을 도모하였으며, IT Security EBK[22]에서는 정보보안 전문가 양성을 위한 직무분석을 수행하고 보안 담당자를 위한 숙련 표준의 개발과 적용을 제시하고 있다.

미국의 정보보호 표준교육과정은 1994년에 NSA (National Security Agency)에서 제정한 NSTISS (National Training Standard for Information Systems Security) 4011 : National Training Standard for INFOSEC Professionals에 따르고 있다. 이를 기반으로 현재 NSA/CSS(Cnetral Security Service) 산하 국가 정보보호 교육훈련 프로그램(National Information Assurance Education and Training Program)이 정보보호 교육훈련을 총괄하며, Committee on National Security Systems와 함께 정보보호 훈련표준을 개발하고 있다[24].

이러한 미국의 교육과정에 대한 분석하기 위하여, Chen et al.[17]은 미국 190개 대학과 중국 64개 대학의 정보보안 교육과정을 비교하였다. 분석결과 통신관련 교육 과정의 경우에, 미국에서는 일반적으로 정보보안 교육과정에서 다루어지지 않으나, 중국에서는 기본적인 정보보안 교육과정에 포함된다. 반면, 정보보안 관리, 보안 정책 및 사이버 범죄 등은 통상적으로 미국의 정보보안과정에 포함되고 있으나, 중국의 정보보안과정에서는 드물게 다루어지고 있는 점을 보이고 있다. 한편, 전산학에 대한 지식은 대부분의 중국 대학의 정보보안 교육과정에서 정보보안의 기초로 간주되며 이를 핵심과목으로 포함되는데 반해, 미국의 경우에는 데이터베이스 관리 및 프로그램 작성 정도에 대해서만 일부 대학에서 핵심과목으로 인정하고 있다고 평가한다. 이들에 따르면, 전반적으로, 미국에서는 보안정책, 사이버윤리, 컨설팅 등 관리측면이 강조되며, 관련 과목들이 정보보안과정에서 일반적으로 포함되나, 중국의 정보보안과정에서는 기술적 측면이 강조되며 미국에서 강조되는 정보보안 관리, 보안정책 및 사이버 범죄 등의 과정이 거의 다루어지지 않고 있다고 평가된다. 또 다른 측면으로 수업 진행에 있어서도, 정형화된 교재에 대한 의존도가 중국에서 상대적으로 높은 반면, 미국은 산업체 종사자에 의한 강의가 상대적으로 많다고 분석하고 있다.

또한, 미국의 정보보안 교육과정에 대해서 Woodward and Young[26]은 미국 중서부지역의 정보보안 경연 대회 우승대학팀을 분석하여 근래 정보보안교육에서 강의기반 교육 대비 실무경험을 통한 적극적 학습의 확대가 필요함을 보이며, 특히 팀작업을 통한 문제대응능력 개발의 중요성을 제기하였다. 이들은 분석결과를 기반으로 단계별로 구성되는 교육과정을 제안하였는데, 각 단계는 학생들로 하여금 현실에서 발생할 수 있는 다양한 상황에 노출되도록 하고 이에 대하여 팀작업을 통해 극복하도록 하는 방식을 제안하고 있다. 단계적으로 네트워킹과 보안 환경에 대한 지식 및 문제해결을 심화시켜며, 체계적으로 최종 단계에서 고차원의 문제해결에 필요한 모든 기초지식을 갖추도록 하는 것이다.

한국에서도 정보보안 인력양성과 관련된 연구가 2000년대 중반 이래 제시되고 있는데, 이들은 주로 직무분석에 기반한 연구들이다. 최명길 외[10], 전효정 외[8], 김태성[3] 등은 기존 연구 정리 및 직무분석에 기반하여, 정보보호 인력 및 양성 교육 체계를 제시하였다. 김정덕 외[2]은 정보보호와 관련된 교육 프로그램 제안을 위해, 정보보호와 관련된 직업을 도출하고 미국 IT 보안 필수요구지식을 참조하여 각 직업 및 직무별 필수요구지식 선정하였다. 그런데 이러한 직무분석 기반의 교육과정개발만으로는 기술변화가 빠른 경우에 한계를 가진다.

근래의 국내의 정보보호 교육과정에 대한 연구에서는 교과과정 자체에 대한 분석, 타국과의 비교분석, 장기적 관점의 필요 등을 제시하고 있다. 박재

용[5]은 부산 인근 대학의 정보보안 관련학과의 개설 교과목을 분류하고 개설비율을 분석하였다. 이에 따르면, 정보보안 교육이 대체로 이론 지향 교육에 치우쳐 있으며, 실제 산업·현장에서 필요로 하는 과목의 개설비율이 상대적으로 낮은 가운데 정보보안 전문성의 취약하다고 평가된다. 오경선, 안성진[6]는 보안인력 양성을 위한 정규교육에 대하여 미국, 영국, 일본과 한국을 비교분석하였는데, 주로 국내 대학 보안관련 학과의 교과목을 정리하고 있다. 가장 앞서가고 있다고 여겨지는 미국의 경우에는 산업요구에 부응하고자 하고자 하며 표준교육과정을 통한 질 관리를 수행하는 것과 비교하면, 한국 등은 이러한 노력이 상대적으로 미흡하다고 평가하고 있다. 한편, 김동우 외[1]는 전반적인 정보보호 교육체계를 검토하며, 포괄적인 수준의 논의로서 국내 정보보호 교육의 문제점으로 정보보호 교육 중장기 계획 부재 등을 지적하고 있다.

전반적으로 한국의 정보보안 교육에서 산업수요에 맞는 교과과정의 개발이 강화되어야 한다고 여겨지는 가운데, 특히 정보보안 부문의 빠른 기술변화의 특성을 함께 고려할 때 현재의 기술수준만이 아니라 기술추이를 반영하는 정보보안 인력양성의 마련되어야 할 것이다. IT 부문의 빠른 기술변화 속에, Cusumano[19], Cusumano et al.[18]는 새로운 기술에 지속적으로 대응할 수 있는 능력을 강조하였다. 그러나 인력양성에 있어서, 기술추이의 선제적 반영이 포함되거나 기반이 된 연구는 국내의 경우 황규희 등[13-15]에서 탐색적 수준으로 시도된 것에 불과하며, 해외에서도 이러한 연구는 보기 드물다.

이에 비하여, 기술전망 자체 및 기술전망에 기반한 미래전망 등은 상당히 발전되어 있으며, 근래 2012년 세비아 미래기술분석 국제학술대회(Seville International Conference on Future-oriented Technology Analysis) 등의 미래전망과 관련한 다양한 논의 및 방안은 이를 잘 보인다. 그러나, 특허정보의 활용, 데이터마이닝, 네트워크 분석 등의 측면에서 제시된 제 논의는 기술전망을 중심으로 미래전망에 집중되어 있는 가운데, 인력양성측면으로의 숙련수요전망 및 교육훈련의 대한 논의는 보여지지 않고 있다.

이에 대하여 본 연구는, 앞서 황규희 등[15]에서 수행된 정보보안 부문 미래숙련수요 전망을 기반으로 '정보보안 부문 미래숙련수요 전망에 대한 교육과정에서의 대응성'을 분석하고자 한다. 2012년 세비아 미래기술분석 대회에서 Cagnin et al.[16]은 양적 질적 방법의 결합을 통한 분석방법 개발을 제안하는 가운데 이러한 방법론적 개발이 단순한 조합이 아닌 분석 대상의 속성에 따라 차별적이어야 함을 요구하고 있으며, Haegeman et al.[20]도 미래분석에서의 적용 대상 등의 특성을 고려한 전망방법의 다양성 모색 필요성을 제시하고 있다. 본 연구는 초기 방법론 개발 단계의 탐색적 수준이나. 이러한 미래분석의 방법론 확장의 일환으로 간주될 수 있을 것이다.

## 3. 연구 분석체계 및 방법론

본 연구는 주로 특허정보, 직무분석정보, 교과과정정보 등의 양적정보에 대한 분석과정에서 전문가 자문을 활용하는 질적분석이 결합하는 방식으로 이루어 졌다. 전반적인 연구체계는 크게 2단계로 구성되었는데, 1단계에서 특허분석과 직무분석을 연결하여 미래숙련수요 전망을 수행하였고, 2단계에서는 앞서 구해진 미래숙련전망을 교과과정과 비교분석하는 단계적 분석으로 수행되었다.

먼저 특허분석을 위한 기본자료는 한국특허청 각년도 출원특허(2013년 9월 30일 기준)이며, 이를 KIPRIS DB(http://kpat.kipris.or.kr/)를 통해 추출하였다. IPC 분석을 통해 검색식을 반복적으로 수정하여 진행되었으며, 숙련 분석을 거치며 정보보안 전문가들의 지속적인 자문을 통해 최종검색식을 확정하였다. 검색식의 구성은 1차로 국제특허분류(IPC, International Patent Classification)를 이용하여 기초 검색을 수행하였고, 2차로 1차 검색결과에서 적합 IPC 코드를 재추출(7digit 수준)하였으며, 3차로 IPC 검색만으로 검색할 경우 누락가능성을 고려하여 주제어 검색을 'or' 조건으로 결합하였

〈표 1〉 분석 체계 및 전문가 참여 사항

| 사항 | | 년월 | 외부 전문가 활용 |
|---|---|---|---|
| 미래 숙련 수요 | 초기 검색식(1, 2) 자문 및 결과 자문 | 2013년 4월~5월 | 특허분석전문가 4인, 업계 관계자 3인 |
| | 숙련단위와 IPC 연계 | 2013년 6월 | 특허분석전문가 1인, 변리사 1인, 업계 관계자 2인 |
| | 검색식 수정(3, 4차) 및 결과 자문 | 2013년 8월 | 특허분석전문가 4인, 업계 관계자 1인, 정보보안학과 박사급 연구원 1인 |
| | 전망결과 타당성 전문가 검토 | 2013년 10월 | 특허분석전문가 4인, 업계 관계자 1인, 정보보안학과 교수 1인 박사급 연구원 2인, 협회 3인 |
| 교과 과정 | 교과과정 분석 1/2차 | 2013년 1월~2월 | 정보보안학과 교수 및 박사급 연구원 각 1인, 업계 관계자 1인 |
| | 교과과정 분석 3/4차 | 2014년 1월 | 정보보안학과 교수 및 박사급 연구원 각 1인, 업계 관계자 2인 |

주) 본 연구에 참가한 협회 및 업체는 한국인터넷진흥원, 한국지식정보산업협회, 한국해킹보안협회, KT 내부 보안팀, 한국지식정보산업협회 회원사 등이다.

다. 주제어는 특허요약에 적용하였다. 이러한 3차 검색식을 기반으로 미래숙련수요 전망을 수행하고 결과에서 검색과정에서의 오류 가능성을 확인 후, 검색식을 보완 수정하여 4차 검색식을 최종 검색식으로 하여 정보보안 출원특허 총 174,155건을 최종 추출하였다.

최종 검색된 특허에서 추출된 국제특허분류(IPC)를 직무별 요구숙련과 매칭하고, 직무별 요구숙련 대응 IPC 출현 도수로부터 숙련수요의 상대빈도(%)를 구하고 추이를 검토하였다. 직무에서 숙련 단위의 추출은 국내외 관련 정보보안 직무분석 연구에 대한 메타 분석을 통해 수행되었다. 특히 미국의 직무분석 자료로부터 많은 도움을 받았다. 기존 직무분석연구를 종합화하며 얻어진 정보보안 부문 숙련단위와 IPC 코드의 연계는 정보보안 전문들과 연구진 간의 공동작업으로 얻어졌다. 정보보안 부문 숙련단위와 IPC 코드의 연계는 특허추이로부터 숙련추이를 분석할 수 있도록 한 핵심적인 연결고리이다. 이때, 범용기술 관련 IPC 포함, 전체 숙련수요 추이, 범용기술 관련 IPC 포함, 20대 출원기업 숙련수요 추이 등을 각각 구하여 비교하였다.

특허추이로부터 숙련추이를 도출하고, 이의 시계열적 추이분석을 통해 정보보안 미래숙련수요전망을 수행하였다. 분석결과에 대한 반복적인 전문가 자문을 거치며, 정보보안 부문 숙련단위와 IPC 코드의 연계를 넓게 한 경우와 좁게 한 경우를 구분하였으며, 전체 특허에 대한 분석과 출원기준 상위 20위 출원기업에 대한 분석을 구분함으로써, 2×2 = 4가지의 전망결과 집합을 구하였다. 4가지 전망에서 일관된 전망이 제시되는 숙련단위도 있고, 각각의 전망결과에서 차이를 보이는 숙련단위도 나타났다. 상이한 결과를 보이는 전망결과에 대하여, 어떠한 전망방식을 도입하는 것이 현실적합성을 높일지를 타진하고, 일관된 전망결과를 포함하여 전반적인 전망결과가 어느 정도 현실적합성을 가지는지에 대하여 전문가 조사 및 업계 조사를 수행하였다.

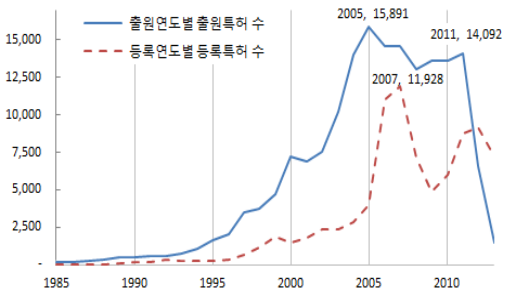
교과과정의 분석은 정보보안학과가 개설된 16개 4년제 대학을 대상으로 하여[3] 인터넷으로 교과과정을 수집하고 이를 분석하였다. 이에 대한 분석은,

3) 분석대상이 된 학교는 건양대, 경동대, 동명대, 동신대, 목포대, 서울여대, 서원대, 성신여대, 세종대, 순천향대, 숭실사이버대, 영산대, 우석대, 중부대, 호서대, 호원대 등 16개교이다. 고려대 사이버 보안학과는 교과과정 정보가 비공개인 가운데 포함하지 않았다. 이외에도 2013년 국가 정보보호백서(한국인터넷진흥원[12], 207)에서는 경기대학교, 고려사이버대, 광주대, 대전대, 동양대, 서남대, 세종사이버대, 한북대, 수원대, 경일대, 위덕대에도 정보보안 관련 학과를 제시하고 있으나, 금번 분석에서는 이를 포함하지 못하였으며, 이들을 포함하여 연구범위를 확대하는 것은 후속과제로 남긴다.

1단계 미래숙련수요전망에서 구해진 숙련수요항목에 대응하는 교과목이 해당학교에 존재하는지 여부를 전문가 협조아래 판단하는 방식으로 진행되었다. 교과과정 분석 1/2차 과정을 거쳐 수행된 숙련수요-교과과정 대응에 대하여, 숙련수요항목이 기술사항에 맞추어지는 과정에서 교과과정의 분류보다 상대적 크기가 과대/과소한 경우가 발견되어 3차과정에서 이를 보정하여 재수행하였다. 즉, 교과목 크기에 대응하는 수준으로 숙련수요항목을 조정하고 이에 대응한 교과목 존재 유무를 3차 과정에서 조정하여 판단하였으며, 이를 4차에서 최종 확인하는 방식으로 수행되었다. 14개 대학에 대하여 관련 전문가 총 4인(정보보안학과 교수 및 박사급 연구원 각 1인, 업계 관계자 2인)의 체계적인 정성분석 및 질적 판단을 활용하였다.[4)]

## 4. 정보보안 미래숙련 전망[5)]

미래숙련수요 전망을 위해, 한국특허청 각 연도 등록특허를 2013년 9월 30일 기준으로 정보보안 관련 174,119건의 출원특허에 대한 분석이 수행되었다. <그림 1>의 연도별 추이를 볼 때, 1990년대 초·중반에서 2000년대 중반까지 성장기를 거쳐 이후 성숙기를 경과하는 것으로 나타나고 있다. 특허출원이 2005년 15,891건, 2011년 14,092건을 보이고 있는 가운데, 2012년과 2013년의 특허출원된 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.




출처 : KIPRIS DB에서 추출하여 정리.

〈그림 1〉 정보보안 특허출원

〈표 2〉 정보보안 직무에 대응하는 숙련요소 중 미래숙련수요 전망 대상(고딕체 표시)

| 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 |

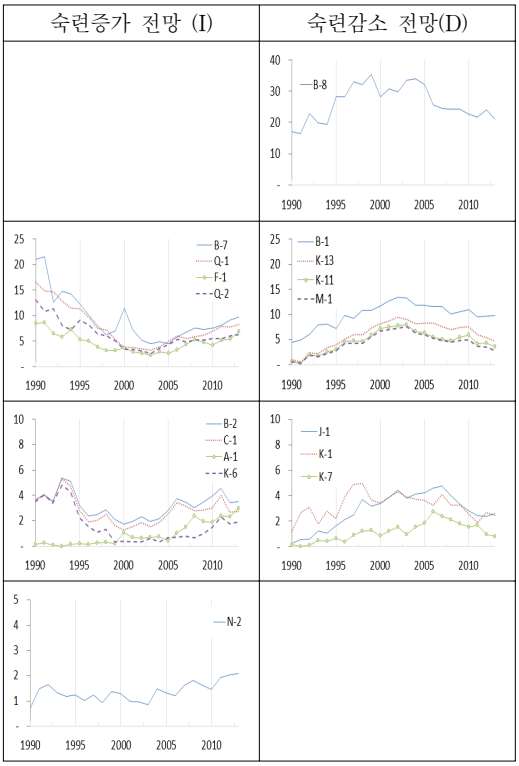
4) 장기적으로는 다수참여자에 기반한 계량분석의 강화가 모색될 수도 있으나, 통상의 직무분석 및 국가직무능력(NCS) 분석, 국가직무능력(NCS) 기반 학습모듈개발 등에서도 기존 직무분석체계 등을 이용하여 전문가 정성분석으로 수행되는 것이 일반적이다.

5) 본장은 본 논문의 핵심인 제 5장과 긴밀하게 연계된 핵심적인 구성요소이기는 하나, 본장 자체는 독립적인 연구는 아니며 기존 선행연구[15]에 기반한 것이다. 본 논문에서는 제 5장과의 연계에 필요한 사항 중심으로 정리하기로 하며, 세부적인 사항은 황규희 외[15]에 남긴다.

| | | |
|---|---|---|
| 연구 개발 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 |
| 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 : 전효정 외[8]를 기반으로, 국내외 정보보호 부문 직무구성을 결합하여 작성.

숙련수요전망은 1990년 이후의 출원특허를 중심으로 하여 이루어졌다. 추출된 특허의 국제특허분류(International Patent Classification, 이하 IPC) 일곱 자릿수 분류를 직무분석에서 제시된 숙련요소(<표 2>의 고딕체)와 대응시키고, 이의 상대비율 추이로부터 얻어졌다(<그림 2> 참조). 이때 추출된 숙련요소의 미래전망을 특허분석을 통해 수행하는 과정에서, 기술적 요소와 연관성이 높아 특허를 통해 식별될 수 있는 숙련요소(<표 2>에서 고딕체로 표시)에 한정하여 전망을 수행하였으며, 특허를 통한 분석이 무의미하다고 여겨지는 숙련요소(<표 2>에서 고딕체로 표시되지 않은 숙련)에 대해서는 전망을 수행하지 않았다.




〈그림 2〉 출원특허 IPC 추이로부터 숙련수요 추이

<그림 2>의 숙련요소에 대응된 IPC 의 상대비율 추이로부터, <표 3>의 세 가지 범주로 구분한 숙련수요전망결과가 제시된다. 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 숙련으로 '(B1) 정

보보호 관리체계', '(K13) 인증 서비스', '(K-11) 모바일 디바이스 관리', '(M1) 취약점 분석', '(J-1) 보안 구조', '(K-1) 방화벽 구성', '(K-7) OTP' 등이 제시되고 있다.

〈표 3〉 IPC 추세로부터 숙련수요에 대한 전망[6]

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

## 5. 정보보안 교육과정의 미래숙련 대응성 분석

본 장에서는 교과과정 정보가 공개된 16개 분석 대상학교의 교과과정과 앞 절에서의 숙련수요 전망 간의 대응성을 검토한다. 그런데 교과과정 분석 과정에서, 전문가들에 의해 앞 절에서의 숙련수요 전망이 '기술'에 편중되어 있는 한편 정보보안 교과과정의 분류항목으로 정의되기 어렵고 체계적으로 분류되지 못하다는 문제가 제기되었다. 교과목 구성의 측면에서, 현재의 숙련항목들이 하나의 독립 과목으로 분류되기에는 작은 단위인 경우가 있는 바 유사 분류로 조정하여 <표 3>을 <표 4>로 재구성하였다.

〈표 4〉 교과단위 조정을 거친 숙련수요 전망

| 교과단위 조정 후 | | 교과단위 조정 전 | |
|---|---|---|---|
| 숙련수요 전망 | 숙련수요 | 숙련수요 | 숙련수요 전망 |
| ① 지속적 중요 | 시스템 보안 | Network | ① 지속적 중요 |
| | | 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, 암호 알고리즘 | 암호학 | ② 새롭게 부상하는 숙련 |
| | | 개인정보 암호화 | |
| | | DB 보안 암호화 | |
| | | 암호화 알고리즘 | |
| | | Data 보안 | |
| | 정보보호 관련법 | 개인정보 보호법 | |
| | 보안 감사 | 보안 감사 | |
| | 디지털 포렌식 | 디지털 포렌식 | |
| ③ 예전에 비하여 범용 숙련으로 전환 | 정보보호 관리체계 | 정보보호 관리체계 | ③ 예전에 비하여 범용숙련으로 전환 |
| | Network 보안 | 방화벽 구성 | |
| | 보안 구조 | 보안 구조 | |
| | 정보보호 프로토콜 | 인증 서비스 | |
| | | OTP | |

6) 정보보안 업체 및 관련 전문가를 대상으로 수행한 조사결과는, 숙련수요 전망의 현실적합성이 통계적으로 유의한 것으로 나타났다(유의수준 5%에서 Fisher's Exact-Test 유의).

<표 5>에서 분석대상 16개교에서 교과목 수준으로 구성한 숙련단위 13항목에 대한 관련 교과목 개설 유무를 살펴보면, 관련 교과목 개설의 대응이 12개 항목에 해당하는 학교가 2개교, 11개 항목 4개교, 10개 항목 8개교, 9개 항목 1개교, 7개 항목 1개교로 나타나고 있다.[7] 교과목 수준으로 구성한 미래숙련단위 13개에 대하여, 10개 미만(80% 미만)의 숙련단위에 대응한 교과과목을 가지는 학교가 16개 학교 중 63%인 11개교에 이르는 것을 보이는데, 이는 미래숙련수요에 대한 교과과정 대응성의 미흡을 암시하는 것으로 해석된다. 현재의 분석이 제한적이고 비교대상을 가지지 못하기에 엄격한 해석은 유보되어야 할 것이나, 기술발전이 빠르다고 여겨지는 정보보안 분야 인력양성에서의 미래대응성의 강화 필요성을 보인다고 여겨진다.

세부 항목별 미래 대응성을 살펴보면, 먼저 지속적으로 중요성이 유지되고 있는 '시스템 보안'에 대하여 관련 과목이 개설된 학교는 16개 학교 중 15개 94%이다. 새롭게 부상하는 숙련으로 전망된 '암호학 및 암호알고리즘'. '디지털 포렌식', '보안정책', '정보보보호법'에 대해서도 거의 대부분의 학교에서 관련 과목이 개설되고 있는 것으로 나타난다. 그러나 역시 새롭게 부상하는 숙련으로 중요성이 증대되고 있는 '보안 감사'에 대해서는 8개교, '모의해킹 및 모의침투'에 대해서는 7개교, 'PC 보안'에 대해서는 6개교만이 이에 대한 관련 과목을 개설하고 있다. 예전에 비해 범용숙련으로 전환하고 있는 '정보보호 프로토콜'에 대해서는 8개교, '보안 구조'에 대해서는 15개교가 각각 관련 과목을 개설하고 있다.

'모의해킹 및 모의침투'에 대한 일부 전문가 의견으로는 이론보다 실습 위주의 기능적인 사항으로서 4년제 대학의 정규교과목으로는 타당하지 않고 2년제 대학 혹은 훈련기관에서 이수되는 것이 타당하다고 제시되기도 하였으나, 이와는 달리 '모의해킹 및 모의침투'가 근래 정보보안의 가장 핵심적인 사항의 하나이며 학원이나 전문대 수준에서만 다루어질 사항이 아니라는 의견도 제기되었다. 근래 지속적인 보안사고의 확대 및 정보보안 실무적인 대응의 중요성이 강조되는 가운데, 4년제 대학에서도 '모의해킹, 모의침투'에 대한 교육이 필요한 한편 이론보다 실습 위주의 과목으로 강화되는 것이 요구된다고 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 강화되어야 할 것이다. 한편, 'PC 보안'의 경우에도 많은 학교에서 이에 대한 과목이 소홀히 다루어지고 있는데, 이는 대부분의 대학이 서버/DB 등의 전문 시스템 보안에 치중하기 때문으로 여겨진다. 일상적으로 PC를 서버/데이터베이스로 사용하는 경우도 상당하기에, 시스템/OS/네트워크 보안과도 일정부분 연관된다고 할 수 있으며, 최종 사용자에 대한 보안을 통합한 전문과목(PC 보안, DB 보안 등) 개설이 기대된다.

유관 분야와의 융합현상이 강화되는 영역에서는, 그 중요성이 증대하는 가운데 관련 과목의 개설자체는 상대적으로 높은 수준이나, 해당 전임교원 확보가 만족스럽지 않은 것으로 조사된다. 정책적인 측면에서 그 중요성이 증대되고 있는 '보안정책'에 대해서 15개교(94%)가 관련 과목을 개설하고 있으나, 대부분 정보보호개론 내에 포함한 수준에 불과한 상황이다. 보안정책은 '정책-법제-경영' 등과의 연계가 필요하며, 이를 위한 전임교원이 강화되어야 할 것으로 여겨진다. 정보보호법, 저작권법, 개인정보보호법 등이 포함되는 '정보보호 관련 법제'도 그 중요성이 매우 높은 가운데 관련 과목이 개설된 학교가 16개교 중 13개교(81%)이나, 이 역시 관련 교원의 확보가 많지 않은 가운데 교원 확보가

7) 현재의 분석에서도 여전히 숙련항목 간 크기가 동일하지 않다는 지적이 제기될 수 있다. 예를 들어 '암호학 및 암호알고리즘'이 'PC 보안'과 'OS 보안'을 합한 것보다 크다는 판단을 내릴 수 있다. 이를 고려한 가중치 부여 및 관련 과목 수가 고려될 수 있으나, 이에 대한 고려는 본 연구의 한계를 넘어서며 후속 연구과제로 남긴다.

〈표 5〉 미래숙련수요 대응 관련 과목 개설 유무

| 대학 (U) | ① 지속적 중요 | ② 새롭게 부상하는 숙련 | | | | | | | | ③ 예전에 비하여 범용숙련으로 전환 | | | | 대응 교과가 있는 미래숙련 수요 항목 수 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 시스템 보안 | 모의 해킹, 모의 침투 | 보안 정책 | PC 보안 | OS 보안 | 암호학, 암호 알고리즘 | 정보 보호 관련법 | 보안 감사 | 디지털 포렌식 | 정보 보호 관리 체계 | Network 보안 | 보안 구조 | 정보 보호 프로 토콜 | |
| 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 |
| 계 | 15 | 7 | 15 | 6 | 14 | 16 | 13 | 8 | 16 | 15 | 16 | 15 | 8 | |
| | 94% | 44% | 94% | 38% | 88% | 100% | 81% | 50% | 100% | 94% | 100% | 94% | 50% | |

시급하다. ‘OS 보안’의 경우에도 14개교(88%)가 관련 과목을 개설하고 있으나, 이를 전공한 교수는 많지 않으며, 전문교원 확보가 중요한 과제로 제기된다.

‘보안 감사’는 경영 및 법률 등과의 심층적인 연계가 필요한 과목으로, 보안 실무자보다 상위 관리자(임원 등)에게 적합한 과정으로 간주되며, 정보보안의 심화 전문과정과 체계적인 연관성을 가진 교과과정 구성이 요구된다. 대학 수준에서 보안정책, 법률 등과 연계한 기초 감사 과목을 개설하고, 전문 심화과정으로서 대학원 및 산학협력을 통한 상위 관리자 및 임원급 교과과정 내에 전문적인 보안 감사 과목의 개설이 도모될 수 있을 것이다. ‘정보보호 프로토콜’도 정보보호이론을 기반으로 하여 실생활에 적용되는 응용 프로토콜을 이해하는 과목으로서, 학부과정에서보다는 대학원 수준에서 개설되는 것이 적합하다고 여겨진다. 기초적인 부분의 정보보호 프로토콜과 심화적인 부분의 정보보호 프로토콜로 분류하여 기초적인 부분은 학부과정에서, 심화적인 부분은 대학원과정에서 개설되는 것이 적절할 것이다.

이렇게 정보보안 내 다양한 세부영역의 존재가 강화되면, 향후에 모든 학교가 정보보안 내 세부영역을 다 갖출 수는 없을 것이며, 정보보호의 수요대응성을 선별적으로 제고하기 위해서 산학협력에 의해 수요우선 순위가 높은 교과과정을 개발하거나 정보보안 내 세부특정 분야로의 특화가 요구될 것이다. 현재 사고조사를 위한 ‘디지털 포렌식’은 거의 모든 학교에서 수행되고 있는데, 그 중요성이 강화되는 가운데 이에 대한 세부 과목의 개발이 필요할 것으로 여겨진다.

# 6. 결론 및 시사점

본 연구는 정보보안 부문의 특허분석 기반 미래 숙련수요 전망과 정보보안학과가 있는 4년제 대학 16개교의 교과과정 분석을 결합하여 다음의 시사점을 얻었다.

첫째, 새롭게 부상하는 숙련 중에서 중요성이 증대되고 있는 영역인 '모의해킹 및 모의침투', 'PC 보안'등의 기능적인 부분에 대응한 실습교육의 강화가 이루어져야 한다.

둘째, 융합현상이 강화되는 가운데 새롭게 부상하는 숙련으로 그 중요성이 증대하는 숙련영역인 '보안정책', '정보보호 관련 법제', 'OS 보안' 등의 경우에는, 관련 과목의 개설자체는 상대적으로 높은 수준이나 해당 전임교원의 확보가 중요한 관건이 되고 있다. 이에 대해 산학협력 등을 통해 현장 경력자의 교원활용 등이 강화될 필요가 있다

셋째, 또 다르게 새롭게 부상하는 전문영역으로의 '보안감사', '정보보호 프로토콜' 등의 경우에는, 체계적인 심화 전문과정의 개발이 요구된다. 학부수준에서 관련 기초과목을 제공하고, 심화과정으로의 대학원 과정이 개발되어야 할 것이다.

이러한 정보보안 내 새롭게 부상하는 다양한 세부영역의 등장에 대하여, 개별 대학에서 향후에 모두 대응하기에는 상당한 어려움이 있을 수 있다. 이에 대해, 정보보호의 수요 대응성을 선별적으로 제고하기 위해서 산학협력에 의해 수요우선 순위가 높은 교과과정을 개발하거나 정보보안 내 세부특정분야로의 특화가 가능할 수 있을 것이다. 정보보안 내에서도 (1) '모의해킹, 모의침투'와 같은 실습 중심 특화 (2) '정보보호 관련 법제', '보안정책', '보안감사'와 같이 기술 이외에 정책-법제-경영 등과의 학제간 융합 및 산학협력 특화, (3) 보안 구조와 같이 타 공학부문(통신, 설계 등)과 연계된 공학 내 융합 특화, (4) 세부 과목 확장에 의한 전문화 등의 구분이 가능할 것이다. 이러한 정보보안 내 세부 특화를 위해서는 해당학과의 전임교원 구성 및 충원 계획에 기반하거나 외부 자원(유관학과 및 산학협력 등)에 기반한 교과목 개발 및 운영 가능성 등이 전제되어야 할 것이다.

본 연구에서 수행한 미래숙련수요 전망과 교과과정 간 연계 분석의 핵심적 요소는 국제특허분류(IPC)에 기반한 숙련단위와 교과과정의 대응성이다. 기술변화가 없거나 변화에 대한 예측이 불가능하게 급변하는 경우에는 이러한 연계 및 이에 기반한 분석이 의미를 가지기 어려울 것이다. 그러나, 기술변화가 상당한 가운데 기술전망에 대한 분석이 가능한 경우에는 기술변화전망으로부터 미래숙련수요를 전망하고 교과과정에 대한 분석과 연계할 수 있음을 제시하였다. 나아가 미래숙련수요에 대한 현행 관련 교과과정의 대응성을 분석하며, 기술변화에 선제적으로 대응하는 교과과정의 개선방향을 제시하였다. 그간 정보보안 인력양성과 관련된 국내외 연구가 직무분석기반으로 진행된 것에 비하여, 본 연구에서는 특허정보를 이용한 패턴 분석이라는 새로운 분석방법을 적용하며 미래숙련수요 분석을 도모 하였다. 통상 미래기술분석에서 사용되어온 특허정보의 활용, 데이터마이닝 등을 미래숙련수요 및 교육수요의 관점에서 적용한 것은 미래숙련수요 분석방법의 확대를 가져온 것으로 여겨질 수 있을 것이다.

다만, 현재의 연구에서 제시한 결과는 제한된 수준에서의 교과과목 중심 비교이며, 제한된 인원의 전문가 의견을 반복적으로 수렴한 것이라는 한계를 가진다. 또한 국제특허분류(IPC)에 대한 숙련단위의 대응성에 대한 문제점이 제기될 수 있는 가운데 국제특허분류(IPC)를 이용한 미래숙련수요전망의 불완전성도 있으며, 이를 다시 교과과정에 대응시키고 이를 해석하는 과정에서의 문제점도 지적될 수 있다. 나아가 교과과정 보다 상위의 개념인 교육과정에 대한 분석이 적절할 것이나: 현재의 분석은 교과과정 분석수준에 머무는 수준인 것도 한계로 지적 될 수 있을 것이다. 이러한 제반 문제점은 지속적으로 미래숙련수요전망 방법론 개발 및 교육과정분석의 응용과정에서 보완되어야 할 것이다. 본 연구는 이러한 기존의 기술분석을 중심으로

한 미래연구(Future Analysis)의 방법론을 숙련 분석 및 교육과정으로 확장시키고자 하는 지속적인 과정의 초기 단계로 간주되어야 할 것이다.

## 참 고 문 헌


[1] 김동우, 채승완, 류재철, “국내 정보보호 교육 체계 연구”, 「Journal of The Korea Institute of Information Security and Cryptology」, 제23권, 제3호(2013), pp.545-55.

[2] 김정덕, 백태석, “정보보호 전문인력 양성을 위한 필수요구지식 및 교육인증 프로그램”, 「디지털정책연구」, 제9권, 제5호(2011), pp.113-121.

[3] 김태성, 「정보보호인력 양성정책」, 충북대출판부, 2010.

[4] 나현미, 「미국의 정보보호 표준교육과정 분석 연구」, 한국직업능력개발원, 2004.

[5] 박재용, “정보보호 전문인력 양성을 위한 교육과정 분석”, 「경영정보연구」, 제31권, 제1호(2012), pp.149-165.

[6] 오경선, 안성진, “국내외 정보보안 교육과정 현황 비교분석”, 「2013년 한국컴퓨터교육학회 하계 학술발표논문지」, 제17권, 제2호(2013), pp. 15-20.

[7] 전효정, 유혜원, 김태성, “정보보호 분야 직무별 필요 지식 및 기술 분석”, 「한국경영정보학회지」, 제10권, 제2호(2008), pp.253-267.

[8] 전효정, 김태성, 유진호, 지상호, “정보보호 분야 직무체계 개발”, 「정보보호학회논문지」, 제19권, 제3호(2009), pp.143-152.

[9] 지식경제부, 「J대한민국 산업기술 비전 2020, 정보통신」, 2011.

[10] 최명길, 김세헌, “정보보호 전문가의 직무수행을 위한 지식 및 기술 분석”, 「한국경영정보학회지」, 제14권, 제4호(2004), pp.71-85.

[11] 한국정보처리학회, 「미래 인터넷 보안기술 및 정보보호 등에 대한 이유 및 개발수요조사」, 한국인터넷진흥원, 2010.

[12] 한국인터넷진흥원, 「국가정보보호백서」. 2013.

[13] 황규희, 이중만, “기술혁신과 미래숙련수요 대응”, 「기술혁신학회지」, 제13권, 제3호(2010), pp.399-422.

[14] 황규희, 고병열, 이중만, “미래숙련수요 분석에서 특허분석의 활용 : 철강산업 녹색기술을 중심으로”, 「직업능력개발연구」, 제14권, 제3호(2011), pp.79-104.

[15] 황규희, 주인중, 반가운, 「미래숙련수요 분석을 위한 특허정보활용의 현실적합성 분석」, 한국직업능력개발원, 2013.

[16] Cagnin, C., A. Havas, and O. Saritas, "Future-oriented technology analysis : Its potential to address disruptive transformations," *Technological Forecasting and Social Change*, Vol.80(2013), pp.379-385.

[17] Chen, H., S.B. Maynard, and A. Ahmadhen, "A Comparison of Information Security Curricula in China and the USA," *Australian Information Security Management Conference*, 2013.

[18] Cusumano, M.A. and D.B. Yoffie, *Competing on Internet Time : Lessons from Netscape and its battle with Microsoft*, New York : Touchstone, 2000.

[19] Cusumano, M.A., "Shifting economies : From craft production to flexible systems and software factories," *Research Policy*, Vol.21(1992), pp.453-480.

[20] Haegeman, K., E. Marinelli, F. Scapolo, A. Ricci, and A. Sokolov, "Quantitative and qualitative approaches in Future-oriented Technology Analysis (FTA) : From combination to integration?," *Technological Forecasting and Social Change*, Vol.80(2013), pp. 386-397.

[21] Irvine, C.E. and S. Chin, "Integrating security into the curriculum," *Computer*, Vol.21,

No.12(1998), pp.25-30.

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

[23] NIST, *Famework for Imptroving Critical Infrastructure Cybersecurity*, 2014.

[24] NSA, *National Training Standard for INFO SEC Professionals*, NSTISS, Vol.4011(1994).

[25] Simpson, H., K., Lynn, F. Fischer, J.D. Tippit, and A. Hayes, "Development and Application of Skill Standards for Security Practitioners," *US Department of Defense Technical Report*, 06-1, 2006.

[26] Woodward, B. and T. Young, "Redesigning an Information Security Curriculum through Application of Traditional Pedagogy and Modern Business Trends," *Information Systems Eduction Journal*, Vol.5, No.11(2007), pp. 3-11.