情報保護學會論文誌
第 21 卷 第 4 號, 2011. 8

지식정보보안의 인력양성 유망 분야 선정 : KISA 고용계약형 석사과정 지원사업 사례*

전 효 정,† 김 태 성‡
충북대학교 경영정보학과/BK21사업팀

Promising Fields for Promoting Workforce in Knowledge Information Security Sector: A Case of KISA Employment-Contract Master Program*

Hyo-Jung Jun† Tae-Sung Kim‡
Department of Management Information Systems, Chungbuk National University

요 약

다양한 기기와 서비스를 기반으로 정보서비스가 민간 및 공공 부문에 보편화됨에 따라 제품 및 서비스의 개발 및 관리, 개인정보보호, 위기관리 및 안전보장 등의 업무를 수행하기 위해 지식정보보안이 중요한 역할을 담당하고 있다. 이에 따라, 지식정보보안산업의 중요성은 더욱 부각되고 있으며 장기적이고 안정적인 산업의 발전을 위하여 실제 보안 업무를 수행하는 지식정보보안인력 확보에 많은 관심이 쏠리고 있다. 본 연구에서는 지식정보보안 전문인력에 대한 효율적인 양성방안을 한국인터넷진흥원(KISA)이 2009년부터 운영하고 있는 'KISA 고용계약형 석사과정 지원사업'의 유망지원분야 선정의 예를 들어 제시한다. 사업에 참여자 및 참여 희망자 대상의 설문 조사와 전문가 대상의 인터뷰 결과를 정리한 결과, KISA 고용계약형 석사과정 지원사업의 유망 지원 분야로는 모바일 보안, 융합 보안의 순서로 유망한 것으로 분석되었다.

ABSTRACT

As information services have been widely used in various environments, the knowledge information security sector plays a significant role in development and management of products and services, information privacy management, risk management and safety, etc. Thus, the process of acquiring knowledge information security professionals is getting more attention for promoting the stable and long-term development of the knowledge information security sector. This study identifies and analyzes the promising fields for the KISA Employment-Contract Master Program and suggests promotion strategies for knowledge information security professionals. By surveying participants and would-be participants, and interviewing experts, it is analyzed that 'mobile security' and 'convergence security' are the two most important fields to be included in the program.

Keywords: Workforce Promotion, Promising Fields, Knowledge Information Security, Analytic Hierarchy Process

I. 서 론

최근 지식경제부는 지식정보보안산업을 암호, 인증, 인식, 감시 등의 보안기술이 적용된 제품을 생산하거나, 관련 보안기술을 활용하여 재난·재해·범죄 등을 방지하는 서비스를 제공하는 산업으로 정의하고, 2007년 현재 약 3조 1천억원 규모인 지식정보보안산

접수일(2010년 11월 17일), 게재확정일(2011년 5월 23일)
* 이 논문은 2010학년도 충북대학교 학술연구지원사업에 의하여 연구되었음.
† 주저자, phdhyo@naver.com
‡ 교신저자, kimts@chnugbuk.ac.kr

업을 2013년에는 18조 4천억원 규모로 성장시키기 위한 전략을 발표하였다[3]. 더욱이, 정부나 기업의 정책에서 정보보호가 제품 및 서비스의 생산 및 제공뿐만 아니라 위기관리 및 안전에서 중요한 역할을 담당하게 된 만큼 지식정보보안산업의 중요성은 더욱 크게 부각될 것으로 전망되고 있다. 그러나, 우리나라의 정보화 수준은 세계 1위를 기록할 만큼 인프라나 인터넷 사용자의 양적인 증가가 이루어졌지만, 2009년에만 3만 5천여건의 개인정보 침해사고와 2만여 건의 해킹사고가 신고될 만큼 정보화의 역기능 문제, 즉 보안침해사고는 심각한 수준으로 증가하고 있다[22]. 더욱이, 현재 공급가능한 정보보호인력은 연간 최대 약 1,900명 정도로 잠재인력수요에 비해 매우 제한적인 규모에 불과한 것으로 파악되고 있으며[4], 2010년 정보보호학과를 운영중인 4년제 대학은 15개 내외에 불과한데다 대다수 지방에 소재하고 있어 규모나 내용 면에서도 안정적인 인력공급에 한계를 드러내고 있는 것이 현실이다[1].

정보보호 관련 기관 및 부처가 모두 동의한 정보보호인력에 대한 정의는 아직 없으며 같은 맥락에서 정보보호인력의 범주에 대해서도 합의된 바가 없는 것으로 파악된다. 정보보호 산업 및 인력현황 파악을 위한 실태조사에서도 딱히 정해진 기준 없이 매해 상이한 분류와 기준에 의거한 조사가 반복되고 있어 정보보호 인력에 대한 통계치 확보에 어려움이 있는 것이 현실이다. 다만, 미국 표준기술연구소(NIST)가 1998년 보고서를 통해 "정보보호 전문인력이란 정보보호에 관한 고도의 지식과 기술수준을 가지고 미래지향적으로 정보보호 업무를 수행할 수 있는 능력을 가진 인력"이라고 정의한 바 있으며[17], 우리나라에서는 이 정의를 준용하여 "정보보호인력은 정보보호에 관한 고도의 지식과 기술수준을 가지고 미래지향적으로 정보보호 업무를 수행할 수 있는 능력을 가진 인력"으로 정의하고 있다[7].

장기적이고 안정적인 산업의 발전을 꾀하고 국가 정보보호 기반 확보를 위해 지식정보보안인력 양성을 위한 체계적인 인력양성정책의 마련이 필요하다. 특히, 정보보호 분야의 경우 소관부처가 방송통신위원회, 지식경제부, 행정안전부 등으로 범부처적인 협력을 통한 시너지효과를 기대해 볼 수 있다. 따라서, 어떠한 기준을 가지고 어떠한 분야의 전문인력을 집중 육성할 것인지, 산업계에서 필요로 하는 인력의 구비요건은 무엇이며 수요맞춤형 인력양성을 위한 공급방안은 무엇인지, 부처별 정책수행의 목적과 수단의 특징은 무엇인지 등에 대해 분석을 하고 범부처적인 협력을 유도한다면, 보다 안정적이고 효율적인 지식정보보안인력의 양성이 가능할 것이다.

본 연구에서는 지식정보보안에서 인력양성 정책방안의 도출과정을 한국인터넷진흥원(KISA)이 2009년부터 운영하고 있는 'KISA 고용계약형 석사과정 지원사업'의 유망분야를 도출하는 과정을 예를 들어 제시한다. 사업에 참여하고 있거나 참여를 희망하는 사람들을 대상으로 설문조사를 실시하고, 전문가 대상의 인터뷰를 실시하였으며, 조사 및 인터뷰 결과를 AHP 방법을 이용하여 분석하여 최종 결과를 도출하였다. 2장에서는 유망지원 분야의 대안을 도출하기 위한 문헌고찰과 설문조사에 대해 설명하고, 3장에서는 AHP 모델을 구성하기 위한 의사결정의 목적, 대안선정 기준, 최종대안 도출 과정에 대해 설명한다. 4장에서는 AHP 분석 결과를 바탕으로 선정기준 및 유망분야간 우선순위(및 상대적 중요도)를 제시하고, 선정기준의 중요도의 변화에 따른 유망분야간 우선순위의 변화를 민감도 분석을 통해 제시한다. 5장에서는 조사결과의 시사점과 정책 활용 방안을 제시하고, 6장에서는 본 연구의 한계와 향후 연구 주제에 대해 논의한다.

II. 유망분야 후보군 도출

2.1 국외 문헌분석

국내외 정부, 국제기구, 리서치 기관 등의 간행물과 연구문헌 등에 대한 고찰을 통해 지식정보보안 분야의 유망 분야를 도출하였다[표 1].

시스코(Cisco)는 보고서를 통해 기업들이 고객을 위한 유연한 네트워크 기술계획을 수립하는데 도움이 될 수 있을 것이라고 제안하였다. 또한, 보안위협의 진화에 대비하면서도 모든 기업들의 보안성이 더욱 강화할 수 있도록 내/외부의 위협으로부터 보호해야 하고, 조직원 및 원격근무자 모두에게 보안성이 확보된 네트워크 연결성을 제공해야 하고, 기업자산의 보호를 위한 물리적 보안도 필요하고, 기업 및 고객 데이터가 적절하게 보호되고 있음을 보장해야 한다고 제시하였다[10].

유럽연합은 ERCIM(European Research Consortium for Informatics and Mathematics)을 통해 미래 정보사회기술의 새로운 트렌드에 대해 고찰하고 전략적인 연구분야를 설정하기 위해 Beyond the Horizon(BtH)이라는 프로젝트를 추진하였다.

〔표 1〕 국외 문헌분석 결과의 정리

문헌구분	세부 보안 분야
Cisco(2006)	네트워크보안, 물리적보안, 데이터보안
EU(2006)	암호(양자암호), 지능화된 보안, 네트워크보안, 식별과 인증, 생체인식, IS보안, 나노기술보안, 지능형 더스트 보안
Rand Corporation(2006)	프라이버시, 익명성, 바이오인식, 바이오정보에 대한 보안
VTT (2007)	에너지 네트워크, 정보 네트워크, 교통 및 운송수단 등 8개 애플리케이션에 대한 보안
IBM(2008, 2009)	가상화 보안, 신원확인, 애플리케이션 보안, 진화네트워크보안, 모바일단말보안, 물리보안
IDC(2006, 2009)	메시징 보안, 웹보안, 단말보안, 네트워크 보안, 보안취약점분석
CheckPoint (2009)	최종단 네트워크 보안
Alcatel-Lucent(2009)	위험관리, 데이터보호, 비용통제
MS(2009)	협업 솔루션 보안, 메시징 솔루션 보안, 엔드포인트 솔루션 보안, 신원확인 및 액세스 관리 솔루션, 정보보호 솔루션

바로 이 BtH 프로젝트의 한 주제로 보안이 포함되어 있다. 보안 분야 보고서에서 EU는 유비쿼터스 시대의 도래로 보안이슈에 대해서도 pervasiveness가 요구된다고 제안하고 있다. 단기적으로 보안관련 연구는 암호, 가상공간에서의 지능화된 보안, 네트워크 보안, 식별과 인증, 생체인식, IS 보안 등이 주제가 되어야 할 것이며 장기적으로는 나노기술 및 바이오 컴퓨팅 보안에 대한 연구(양자암호, 나노기술보안, 지능형 더스트 보안) 등이 필요하다고 제안하고 있다. 또한, 신뢰할만한 디지털 보안을 위해서는 디지털 프라이버시(digital privacy)와 정보 수집적 보안(collective security) 간의 이중성을 보장하는 디지털 위엄(digital dignity)과 제공된 보안에 대한 신뢰를 보장하는 디지털 주권(digital sovereignty)의 원칙이 지켜져야 한다고 제시하고 있다[11].

미국의 랜드연구소는 2020년 글로벌 기술 트렌드와 전세계에 미치는 시사점을 바탕으로 미래에 대한 전망을 제시하였는데, 바이오기술, 나노기술, 재료기술, 정보기술 분야를 중점적으로 다루고 있으며, 세계 29개국을 대상으로 보고서에서 선정한 16개 핵심기술 애플리케이션(저가의 태양열 에너지, 시골의 무선통신 등)을 획득하고 실행할 수 있는 능력을 평가하여 제시하고 있다. 특히, 이 보고서에서는 정보기술 분야에 대한 미래 전망을 통해 보안이슈를 다루고 있는데, 유비쿼터스화에 따라 사람에 대한 다양한 유형의 정보가 양산되고 개개인이 매우 많은 센서에 연결되게 되면서 프라이버시와 익명성은 매우 중요한 이슈가 될 것이며 바이오인식 기술도 널리 활용될 것으로 전망하고 있다. 또한, 프라이버시와 보안의 관점에서 바이오정보 자체에 대한 보안 즉 바이오정보를 저장하는 저장매체 및 백업시스템에 대한 보안도 매우 중요한 요소가 될 것이라고 제시하고 있다[18]. 또한, IDC는 보고서를 통해 오늘날 IT운영자들이 직면하고 있는 현재의 또는 새로이 떠오르고 있는 보안이슈들에 대해 분석하여 제시하였다. 경험에 비추어 봤을 때, 보안을 위한 모든 구성요소들이 유기적으로 통합되어 운영되어야만 고도로 보안이 확보되고 비용 효율적인 보안 인프라가 달성될 수 있다고 평가하면서, 기업의 보안전략은 메시징보안, 웹보안, 단말보안, 네트워크 보안, 보안취약점 분석 등으로 나눠서 수립해야 한다고 주장하였다[14]. VTT는 많은 기술분야에 대해 지속적이고 광범위한 연구를 계속하여 왔지만 그 중에서도 공공안전(public safety)과 보안(security)에 대해 가장 집중하고 있는데, 2007년 VTT가 발표한 보안연구에 대한 기술로드맵은 중요한 사회기간인프라에 대한 보장, 기업가정신의 활동에 대한 보장, 보안기술과 서비스 등의 측면을 시험해보고자 작성된 것이며, 선택된 애플리케이션(로드맵의 대상)은 에너지 네트워크, 정보네트워크, 수자원공급시설, 교통 및 운송수단, 시민보호, 제품 및 운영에 대한 보호, 장소 및 자산에 대한 보호, 제품 및 시스템에 대한 정보보호 등 8개이다[21].

2008년 IBM은 미래 시점의 고객들에게 제공 가능한 보안제품 및 솔루션 개발을 위한 가이드라인 마련을 목표로 향후 2년~5년 사이 출현할 것으로 예상되는 보안기술 트렌드를 전망한 보고서를 발표하였다. IBM이 밝힌 9개 미래 보안기술 트렌드는 가상화 환경에서의 보안(securing virtualized environments), 보안구현을 위한 대책마련(alternatives ways to deliver security), 신뢰할만한 신원확인

(trusted identity), 정보보안(information security), 예측가능한 애플리케이션 보안(predictable security of applications), 진화하는 네트워크에 대한 보호(protecting the evolving network), 모바일 단말보안(securing mobile devices), 물리 보안(sense and response physical security) 등이다[12].. IBM은 2009년에는 비즈니스에 기반한 보안프레임워크 구성을 위한 방법을 제시한 보고서를 발표하였다. 보안은 조직내 비즈니스 활동과 동떨어져 생각할 수 없으며 보안을 비즈니스 프로세스를 보호하고 강화하는 수단으로 활용해야 할 것이라고 주장하고 있다. 보안대상은 사람과 신원확인(people and identity), 데이터와 정보(data and information), 애플리케이션과 프로세스(application and process), 네트워크/서비스와 엔드포인트(network/service and endpoint), 물리인프라(physical infra) 등을 제시하고 있다. 보안 측면에서 이 보고서는 두 가지 비즈니스 시나리오를 해결할 수 있다고 주장하고 있다. 첫째는 비밀번호 관리와 관련된 비용이며 둘째는 IBM 보안 프레임워크와 IBM 보안 청사진이 가장 잘 이용될 수 있는 PCI 준수(PCI compliance)에 관한 것이다[13].

한편, IDC는 보고서를 통해 전세계적으로 경기침체로 인해 전체적인 IT투자가 줄고 있지만 견고한 네트워크 보안 및 통신능력에 대한 요구는 지속적으로 증가하고 있다고 평가하였다. 외부공격에 대해 네트워크 인프라를 전략적으로 지켜내는 것은 모든 기업 CIO들의 가장 중요한 역할이라고 주장하면서 보안설비(security appliances)는 네트워크 인프라 장비 중에서도 가장 가파른 성장세를 보이고 있는 분야이며 자산보호를 위해 기업들은 지속적으로 이 분야에 대해 투자해야 한다고 주장하고 있다. 또한, 보안은 네트워크 및 IT 관리자의 가장 큰 우려사항으로 남아 있다고 평가하면서 보안투자를 결정하기 이전에 기존의 보안 솔루션들을 운영함에 있어 문제되었던 잠재적인 보안 취약성에 대해 철저히 분석해야 한다고 제안하고 있다[15].

CheckPoint사는 최종단(endpoint)에서의 보안의 중요성에 대해 강조한 보고서를 발표하였으며, 대표적인 최종단으로 네트워크에 연결하고자 하는 조직원들의 랩탑이나 PC를 제시하면서 이에 대한 보안방법으로 데스크탑 방화벽(desktop firewall), 프로그램 통제(program control), NAC, 브라우저 가상화(browser virtualization) 등을 제시하고 있다. 또한, 새로운 전략으로서 최종단과 네트워크 보안을 통합적으로 고려해야 함을 강조하였다[9]. 한편, Alcatel-Lucent사는 보고서를 통해 오늘날과 같이 경쟁이 심한 기업환경에서 조직원들의 이동단말기와 같은 모든 음성 및 데이터 통신 애플리케이션들에 대한 보안을 확보하는 것은 새로운 비즈니스 모델을 따르면서도 신뢰할만한 동태적인 기업을 구현하는 지름길이 될 것이라고 주장하였다. 또한, Alcatel-Lucent의 보안청사진은 사용자 중심적인 보안을 구현하고자 하는 기업들을 안내할 것이라 하면서 기업보안의 3가지 요구사항으로 위험을 관리하고(managing risk), 데이터를 보호하고(protecting data), 비용을 통제하는(controlling cost) 것이라고 제시하였다[8]. MS사는 보안 비즈니스의 대상으로 협동 솔루션 보안, 메시징 솔루션 보안, 엔드포인트 솔루션 보안, 신원확인 및 액세스 관리 솔루션, 정보 보호 솔루션 등 5가지를 제시한 보고서를 발표하였다. 협동 솔루션 보안은 표준기반의 상호운용적인 신원확인을 통해 보다 안전한 조직 내외부 협동체계를 확보하는 것이며, 메시징 솔루션 보안은 장소와 기기의 구애됨 없이 가상적으로 사용하는 메시징 서비스의 이용을 보장하는 것이다. 엔드포인트 솔루션 보안은 개인사용자가 조직 네트워크에 접속시 자동적으로 보안 스캐닝을 실시하도록 하는 것이며, 신원확인 및 액세스 관리 솔루션은 장소나 기기의 구애됨 없이 on-premises와 in-the-cloud 모두에서의 애플리케이션 액세스가 가능하도록 해주는 신원확인 기반 액세스를 제공하는 것을 말한다. 마지막으로, 정보보호 솔루션은 기존의 플랫폼 및 애플리케이션들과의 융합을 통해 조직의 중요한 정보를 자동발견/탐지/보호/관리할 수 있는 기능을 말한다[16].

2.2 유망분야에 대한 설문조사

KISA 고용계약형 석사과정의 사업실태 현황 파악을 위해 실시하였던 1차 및 2차 조사[1]에 신규개설을 위한 또는 향후 지식정보보안산업에서의 유망분야에 대한 항목을 삽입하여 이에 대한 의견을 구한 결과를 정리하여 활용하였다[표 2].

1) 1차 조사는 KISA 고용계약형 석사과정 지원사업 참여자(참여교수, 참여기업, 참여학생)를 대상으로 2010년 5월 17일부터 5월 28일까지 실시되었으며, 2차 조사는 지식산업협회 회원사 및 임원사, 한국정보보호학회 교수회원 및 2009/2010년도 사업설명회 참석자 등을 대상으로 2010년 7월 14일부터 8월 13일까지 실시

〔표 2〕 문답형조사를 통해 도출한 유망분야 후보군

석사과정 개설 분야	빈도
모바일 보안	22%
디지털 포렌식	11%
융합보안	11%
접속보안	11%
소프트웨어기획, 품질관리	8%
네트워크 보안	8%
개인 정보보호	6%
지식콘텐츠 보안	6%
영상 분석	3%
국가/국방보안	3%
주력산업보안	3%
클라우드 컴퓨팅 보안	3%
헬스케어 보안	3%
사이버 보안	3%

2.3 지식경제부의 2009년 지식정보보안기술로드맵

우리나라 지식정보보안산업 및 기술의 가이드라인이라 할 수 있는 2009년 발표된 지식경제부의 '지식정보보안기술로드맵'의 기술분류표를 참조하였다〔표 3〕. 이 기술분류표는 1/2차 KISA 고용계약형 사업 참여자 및 참여 희망자 대상 조사시 미래 유망분야 도출의 참고자료로도 제시되었다〔3〕.

〔표 3〕 지식경제부의 지식정보보안로드맵 기술분류

중분류 (1단계)		소분류 (2단계)
정보보안	공통기반 보안	암호알고리즘
		네트워크/시스템보안
		서비스/응용보안
		인증인프라
		부채널공격대응
		개인정보보호
	네트워크/시스템 보안	네트워크 침입대응
		악성코드대응
		보안운영체계
		디지털포렌식
		보안전용칩셋
		접속보안
		보안관리
	서비스/응용보안	지식콘텐츠보안
		응용서비스보안
물리보안		재난관제
		보안모니터링
		바이오인식
융합보안		지능형차량보안
		u-헬스케어보안
		금융보안
		로봇보안
		스마트그리드 보안
		주력산업보안

III. 조사설계

3.1 조사방법론: AHP

AHP(Analytic Hierarchy Process)는 1980년대에 토마스 사티(Thomas L. Saaty) 교수에 의하여 제안된 다기준 의사결정방법론이다〔20〕. AHP는 의사결정문제를 계층구조화하고 쌍별비교(pair-wise comparison)를 기초로 평가기준들 간의 가중치(상대적 중요도)와 각 평가기준 하에서의 평가대안들 간의 상대적 선호도를 도출한 후, 이를 계층구조에 따라 종합화하여 비교대안들의 평가순위와 종합적 선호도를 구하는 방법이다〔20〕.

일반적으로, AHP를 이용하여 의사결정 문제를 해결하고자 하는 경우에는 다음과 같은 3단계를 거친다. 첫째, 의사결정 문제를 계층화(hierarchy of decision problem)한다. 의사결정 문제를 서로 관련된 의사결정 사항들의 계층으로 분류하여 의사결정계층(decision hierarchy)을 설정하게 되는데, 이 단계는 종합적 목표(overall goal), 평가기준(criteria), 대안(alternative)으로 분류하고, 이를 계층화 하는 단계이다. 둘째, 기준과 대안들의 상대적 가중치를 결정한다. 이 단계를 통해 기준과 대안의 중요도를 평가하게 된다. 기준 또는 대안들을 쌍별비교한 결과는 일관성(consistency)이 있어야 하는데, 쌍별비교는 주관적인 판단이므로 완벽한 일관성은 불가능하지만 지나치게 부족하다고 판단되면 쌍별비교를 다시 해야 한다. 셋째, 다수의견을 종합한다. 일반적으로 다수 전문가들의 가중치 종합화를 위한 방법으로 개인별 쌍별비교 행렬을 기하평균으로 통합한 '기하평균행렬'을 이용하여 종합적인 가중치를 산정하는 방식이 널리 활용된다〔20〕.

3.2 1차 조사: AHP 모델 구성을 위한 기준/대안 선정

일반적으로, AHP를 이용하여 의사결정 문제를 해결하고자 하는 경우에는 이를 위한 AHP 모델을 구성해야 하는데, AHP 모델은 의사결정 목표, 평가기준, 대안의 계층을 갖도록 구성된다. 이를 위해 2010년 8월 27일부터 8월 29일까지 지식정보보안 분야의 전문가 7명(정보보호 전공 교수 5명, 통신서비스, 운송장비 등 정보보호 제품 및 서비스 수요업체의 정보보호

팀장 2명)을 대상으로 일대일 면대면 인터뷰를 진행하고 유망분야 도출을 위한 목표, 기준, 대안(유망분야)을 도출하였다. 전문가 인터뷰에는 문헌고찰과 설문조사를 통해서 취합된 유망 분야 후보군에 대한 자료를 제시하고, KISA 고용계약형 석사과정 지원사업에 대한 이해를 돕기 위한 자료 제시와 함께 구두 설명을 실시하였다.

본 조사가 '인력양성이 시급한 분야를 선정'한다는 취지임을 감안하여 지식정보보안 분야의 유망분야 도출의 원칙도 정하였다. 첫째, 일반적으로 인력양성 사업의 취지가 수요 지향적인 인력의 효과적인 양성이 목적이고 기본적으로 산업 수요를 기반으로 지원 분야를 선정하는 것이므로, 양성 인력에 대한 수요 기반을 확대할 수 있고(채용기관 수요 확대), 우수 학생들의 지원을 유인할 수 있도록 지원 분야를 도출하여야 한다. 둘째, 특정 수요 산업으로 한정하는 명칭을 사용하거나, 수요 분야가 모호하거나 너무 규모가 작은 명칭을 사용하는 경우를 지양하여야 한다. 셋째, 유망분야 선정대안이 서로 완전하게 독립적으로 구분되는 분야들은 아닐 수 있다. 즉, 모바일 보안 분야에 대한 지원을 통해 양성된 인력이 클라우드 컴퓨팅 보안, 융합보안 등의 분야에 종사할 수 있다. 넷째, 세부 분야에서 각 분야에서의 소요 인력이 모두 신규 인력은 아닐 수 있으며, 기존 보안 인력이 직종이나 세부 종사 분야를 전환하여 종사할 수도 있음을 감안하여야 한다.

유망 분야 선정의 목적은 '지식정보보안 분야에서 기업수요에 맞는 전문성과 숙련도를 갖춘 고급 석사 인력 양성'으로 의견이 종합되었다. 유망분야 선정기준은 '인력 수요의 시급성', '산업의 규모', '인력 확보의 용이성', '국가 차원의 전략적 중요성' 등 4가지로 설정하였으며〔표 4〕, 대안(유망분야)는 모바일 보안, 융합보안, 클라우드 컴퓨팅 보안, 산업보안, 컨텐츠 및 응용보안 등 5가지로 최종 도출되었다〔표 5〕. 5가지 유망분야는 설문조사를 실시할 때, 문헌연구의 결과인 〔표 1〕, 〔표 2〕, 〔표 3〕에서 제시된 미래 지식정보보안 분야의 유망기술 또는 산업을 계위별로 정리하고 각기 다른 용어로 표현된 동일 또는 유사한 분야들을 통합하여 제시하였으며 설문조사를 진행하면서 전문가들의 의견을 수렴하여 용어를 최종 정리하였다.

〔표 4〕 AHP 모델 구성을 위한 기준

기 준	상세설명
인력 수요의 시급성	수요 대비 공급 부족의 정도(수급차가 큰, 즉 수요에 비해 공급이 부족할수록 우선 지원해야 함)
산업의 규모	현재 시장 규모 및 예상 성장률(현재 시장의 규모가 크고, 향후 높은 성장이 기대될수록 우선 지원해야 함)
인력 확보의 용이성	인력 공급 기반의 준비도(기존 공급 기반을 통한 인력 양성이 용이하지 않은 분야에 대해 우선 지원해야 함)
국가 차원의 전략적 중요성	세부분야 보안인력의 균형적인 육성(보안 분야간에 균형적으로 발전할 수 있도록 지원해야 함)

〔표 5〕 AHP 모델 구성을 위한 대안

대 안	상세설명
모바일 보안	스마트폰 등 모바일 기기를 기반으로 한 정보서비스 제공 및 이용을 위한 보안
융합보안	산업 특화 보안 수요를 충족하기 위하여 다양한 보안 수단을 결합하여 제공하는 보안(금융보안, 영상보안, 지능형차량보안, 헬스케어보안, 스마트그리드보안 등)
클라우드 컴퓨팅 보안	클라우드 컴퓨팅 환경에서의 정보서비스 제공 및 이용을 위한 보안
산업보안	기업비밀, 국가기밀, 개인정보 등의 노출 및 오남용을 예방하거나 책임추적을 위한 보안(개인정보보호, 공공보안, SCADA, 모의훈련, IT 감사, 디지털 포렌식, e-discovery 등)
컨텐츠 및 응용 보안	컨텐츠 및 애플리케이션의 개발, 설치, 운영, 이용 등에 관련된 보안

3.3 2차 조사: 유망분야간 우선순위 도출

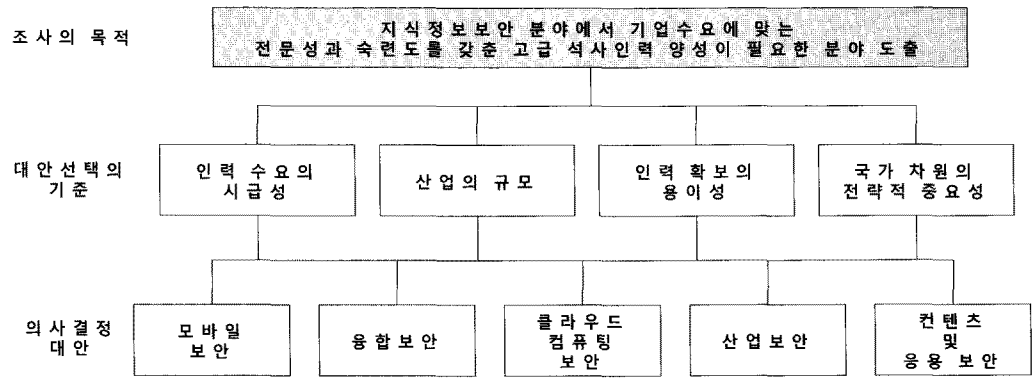
2차 조사를 위한 조사지는 〔그림 1〕의 모형에 기반하여 작성하였으며, 인력양성 유망분야간의 우선순위(가중치) 도출과 유망분야 선정기준 간의 우선순위(가중치) 도출을 목표로 하였다.

조사는 2010년 8월 30일부터 9월 20일까지 진행하였으며, 조사대상은 지식정보보안 분야의 전문가 및 KISA 고용계약형 석사과정의 관련자(참여희망자, 사업책임자(교수), 참여기업, 참여학생)였으며, 최종적으로 51명으로부터 응답을 받았다. 본 조사는 기본적으로 일대일 면대면 인터뷰를 통해 조사의 취지를 설명하면서 설문지를 배포하였으며, 직접 방문 또는 이메일을 통해 회수하였다.

IV. 조사결과 분석

4.1 선정기준 및 유망분야간 우선순위 분석

AHP는 응답결과에 대해 일관성 지수(Consistency



〔그림 1〕 AHP 모델

Index, CI)를 계산하여 응답결과의 신뢰성을 검토하는데, 일반적으로 CI가 10% 이하인 결과를 채택하며 사회과학 분야 연구에서의 기준 및 대안에 대한 설명의 어려움, 독립성 확보의 어려움 등으로 CI가 20% 이하인 결과까지 허용하고 있다〔19〕.

회수된 51건의 응답결과에 대하여 CI를 분석한 결과, CI가 20% 이하로 비교적 신뢰성 있게 응답된 결과는 최종 38건으로 나타났다. 분석은 AHP 분석툴인 Expert Choice 2000 소프트웨어를 이용하였다.

신뢰성있게 응답된 38건의 응답결과에 대해 기하평균을 이용하여 전체 및 응답자 그룹별로 종합하여 인력양성 유망분야 선정기준간 및 선정대안(유망분야)간 우선순위를 도출하였다. 응답자 그룹은 KISA 고용계약형 석사과정 지원사업과 이해관계가 전혀 없는 지식정보보안 분야의 전문가 그룹인 '외부전문가', 인력양성에 대한 지대한 관심을 가지고 있는 KISA 고용계약형 석사과정 지원사업에 대한 잠재적인 '참여희망자', 현재 KISA 고용계약형 석사과정 지원사업에 참여중인 관계자인 '참여교수', '참여기업', '참여학생' 등 5개 그룹으로 구성하였다. 전체적으로 외부전문가와 참여희망자들의 향후 지식정보보안산업에 대한 전망에 기반한 인력양성유망분야에 대한 의견과 현재 인력양성사업 참여자들의 사업운영실태를 감안한 인력양성유망분야에 대한 의견이 다를 수 있을 것임을 기대하였다.

결과적으로, 〔표 6〕과 〔표 7〕를 통해서도 알 수 있듯이 전체 응답자의 의견을 종합한 결과에서는 '산업의 규모(기준2)'가 가장 중요한 인력양성 유망분야 선정기준으로 분석되었으며, 5개 응답자 그룹별로도 '인력 수요의 시급성(기준1)'과 '산업의 규모(기준2)'를 제일 중요한 인력양성 분야 선정기준으로 여기고 있는 것으로 분석되었다. 또한, 전체의견 종합결과에서는 1순위로 모바일 보안이 2순위로 융합보안이 인력양성 유망분야로 분석되었으며, 외부전문가 그룹은 모바일 보안, 참여희망자 그룹은 산업 보안, 참여교수 그룹은 모바일 보안, 참여기업 그룹은 융합보안, 참여학생 그룹은 모바일 보안 등을 각각 1순위로 여기고 있는 것으로 분석되었다. 전체적으로 '모바일 보안' 분야에 대한 인력양성의 시급성에 대해 동의하는 것으로 종합해 볼 수 있으며, 인력양성을 위한 유망분야 선정시 참여

〔표 6〕 선정기준간 우선순위

구 분	응답자 전체	응답자 그룹별				
		외부전문가	참여희망자	참여교수	참여기업	참여학생
인력 수요의 시급성	0.281 (2순위)	0.298 (1순위)	0.219 (3순위)	0.430 (1순위)	0.142 (3순위)	0.333 (1순위)
산업의 규모	0.340 (1순위)	0.246 (2순위)	0.432 (1순위)	0.351 (2순위)	0.383 (1순위)	0.167 (3순위)
인력 확보의 용이성	0.140 (4순위)	0.210 (4순위)	0.054 (4순위)	0.156 (3순위)	0.128 (4순위)	0.167 (3순위)
국가 차원의 전략적 중요성	0.239 (3순위)	0.246 (2순위)	0.295 (2순위)	0.089 (4순위)	0.348 (2순위)	0.333 (1순위)

* 수치는 분야별 가중치이며, 응답자별 가중치의 합은 각 1.000

〔표 7〕 선정대안(유망분야)간 우선순위

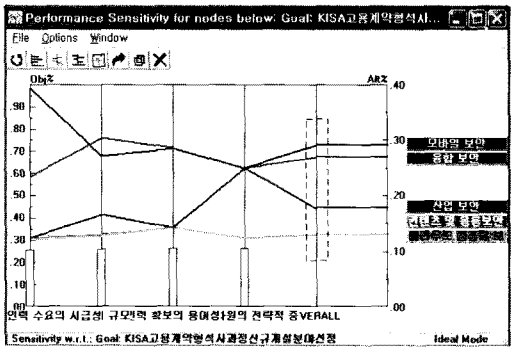
구 분	응답자 전체	응답자 그룹별				
		외부전문가	참여희망자	참여교수	참여기업	참여학생
모바일 보안	0.294 (1순위)	0.413 (1순위)	0.200 (2순위)	0.337 (1순위)	0.232 (2순위)	0.304 (1순위)
융합 보안	0.270 (2순위)	0.244 (2순위)	0.200 (2순위)	0.230 (2순위)	0.283 (1순위)	0.244 (2순위)
클라우드 컴퓨팅 보안	0.129 (4순위)	0.129 (3순위)	0.117 (5순위)	0.193 (3순위)	0.119 (5순위)	0.130 (5순위)
산업 보안	0.178 (3순위)	0.128 (4순위)	0.356 (1순위)	0.109 (5순위)	0.196 (3순위)	0.189 (3순위)
컨텐츠 및 응용보안	0.129 (4순위)	0.085 (5순위)	0.127 (4순위)	0.131 (4순위)	0.171 (4순위)	0.133 (4순위)

* 수치는 분야별 가중치이며, 응답자별 가중치의 합은 각 1.000

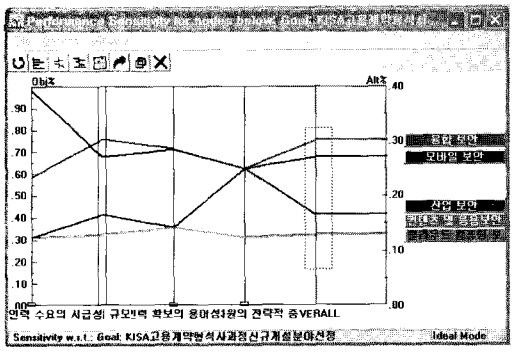
희망자 그룹이 1순위로 '산업보안' 분야를 선호하고 있는 것이 특이한 점이다. 참여희망자 그룹은 기존에 본 사업에서 지원되고 있는 분야인 '금융보안', '홈네트워크보안' 분야 이외에, 추가 신설이 필요하고 사업신청을 희망하고 있는 분야로 산업보안을 가장 중요하게 고려하고 있는 것으로 판단된다.

4.2 민감도 분석

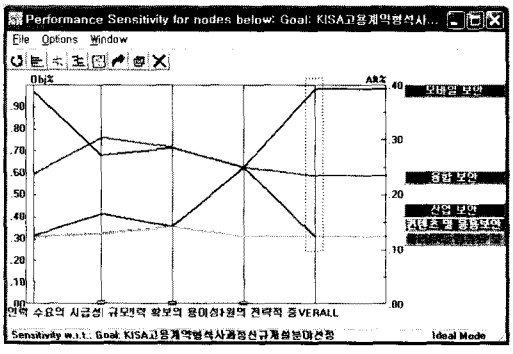
성과민감도(performance sensitivity)는 각 기준에 대해 대안들이 어떻게 움직이는가에 관한 정보가 하나의 그래프에 나타나도록 하는 분석이다. 각 기준은 수직선에 의해 표현되고 각 기준의 중요도는 막대



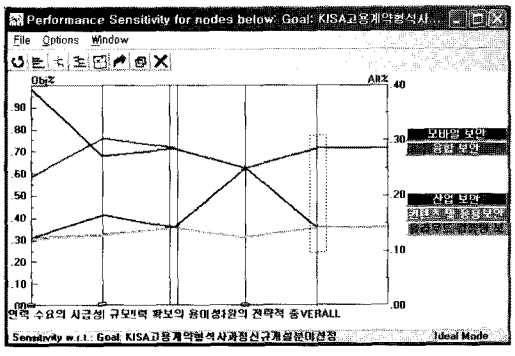
〔그림 2〕 성과민감도 분석 (선정기준간 중요도 동일)



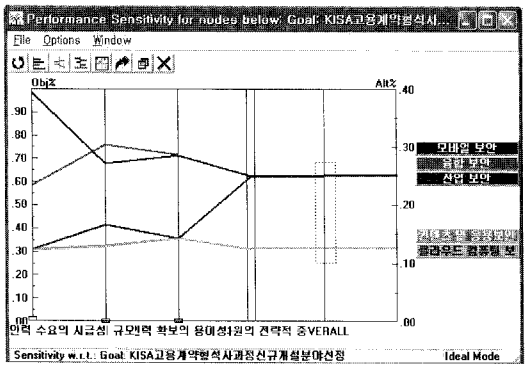
〔그림 4〕 성과민감도 분석 (제2기준 중요도 1.000)



〔그림 3〕 성과민감도 분석 (제1기준 중요도 1.000)



〔그림 5〕 성과민감도 분석 (제3기준 중요도 1.000)



〔그림 6〕 성과민감도 분석 (제4기준 중요도 1.000)

그래프의 높이로 표현된다.

〔표 7〕의 전체의견 종합결과에 대한 성과민감도 분석 결과, 각 기준별 중요도를 모두 같다고 설정할 경우에도 '모바일 보안'이 가장 유망한 인력양성 분야인 것으로 분석되었다〔그림 2〕. 또한, 기준1에서부터 기준4까지 각각을 중요도 1로 놓고 다른 기준들의 중요도는 0으로 설정한 경우의 성과민감도 분석결과는 〔그림 3〕, 〔그림 4〕, 〔그림 5〕, 〔그림 6〕과 같다. '인력 수요의 시급성(기준1)'의 중요도를 1로 설정한 경우에는 모바일 보안에 대한 선호도가 월등하게 높게 분석되었으며〔그림 3〕, '산업의 규모(기준2)'의 중요도를 1로 설정한 경우에는 융합 보안(금융 보안)이 유망분야 1순위로 분석되었다〔그림 4〕.

'인력 확보의 용이성(기준3)'의 중요도를 1로 설정한 경우에는 모바일 보안과 융합 보안이 유망분야 1순위로 분석되었으며〔그림 5〕, '국가 차원의 전략적 중요성(기준4)'의 중요도를 1로 설정한 경우에는 모바일 보안, 융합 보안, 산업 보안이 유망분야 1순위로 분석되었다〔그림 6〕.

4.3 조사결과의 시사점 및 활용방안

기업의 수요를 파악하고 그에 맞는 맞춤형 인재를 양성하여 보급하는 것은 많은 시간과 비용이 소요되며 정부의 적극적인 협조와 기업과 양성기관 모두의 지속적인 노력이 필요한 과제이다. 현재, 우리나라의 지식정보보안 분야 인력양성은 정부, 기업, 학교 모두가 그 필요성에 대해서는 동의하고 있으나 구심적인 역할을 수행하고 있는 뚜렷한 주체가 없는 실정이다. 기업과 학교를 설득할 수 있는 정부의 적극적이고 장기적인 정책추진이 필요하지만 아직도 인력양성을 위한 적극적인 움직임은 없으며, 이것이 확보되지 않은 상태에서 학교는 적극적인 학과(전공) 운영 및 인력양성에 어려움을 겪을 수밖에 없다. 이러한 상황에서 기업은 수요에 맞는 인력이 없다며 인력난을 호소하며 산업발전의 저해요소로 인력의 부족을 꼽고 있는 것이다.

본 논문에서는 인력양성을 위한 프로세스에 최소 2년 이상의 시간이 소요되어야 한다는 점을 감안하여, 지식정보보안 분야의 전문가 및 KISA 고용계약형 석사과정 지원사업 관련자들을 대상으로 향후 3~5년 내에 시급히 인력이 양성되어 공급되어야 할 것으로 생각되는 지식정보보안 분야의 유망분야에 대해 설문을 진행하고 이 결과를 분석하여 정책적인 시사점을 도출하고자 하였다.

우선, 인력양성 유망분야 선정을 위한 기준을 4개 선정하고 여러 유망분야를 제시하고 전문가들의 합의를 거쳐 5개 분야를 최종 선정하였으며, 이를 기준으로 기준 및 대안별 우선순위를 도출하였다. 또한, 민감도분석을 통해 각 기준별 중요도를 조정하고 유망분야간의 선호도가 어떻게 변경되는지를 분석해 봄으로써 정책적인 선호도에 따라 어떠한 분야를 최우선적으로 고려하여야 할 것인지 즉 예산배분을 실행해야 할 것인지 등에 대한 시사점을 도출하였다.

예를 들어, 정부가 인력양성정책을 인력을 얼마나 빨리 확보해야 하는가(인력 수요의 시급성, 〔그림 3〕 참조)에 초점을 맞출 경우, 모바일 보안 분야에 대한 예산배분을 높여 해당분야의 인력을 집중적으로 양성하는 정책이 펼쳐져야 할 것이며, 국가전략 차원에서 보안인프라를 확대하고 보안강국이 되기 위한 것(국가차원의 전략적 중요성, 〔그림 6〕)에 초점을 맞출 경우에는 모바일 보안은 물론 융합 보안과 산업 보안에 대해서도 그 중요성을 고려하는 정책이 펼쳐져야 할 것이다.

V. 결 론

본 논문은 2009년부터 운영되고 있는 대표적인 지식정보보안 분야의 인력양성사업인 'KISA 고용계약형 석사과정 지원사업'의 유망 지원 분야의 선정을 예로 들어 효율적인 지식정보보안 인력양성 정책의 결정에 필요한 의사결정 과정을 제시하였다. 즉, 문헌분석과 전문가 설문조사를 바탕으로 지식정보보안 분야의 미래를 전망함으로써 현 시점에서 미래 수요가 예측되는 분야의 인력을 양성하여 대비할 수 있는 보다 실효성있는 인력양성 정책이 필요함을 제시하고 있다. 2010년에 한국인터넷진흥원이 진행한 KISA 고용계

약형 석사과정 지원사업에 대한 실태조사 결과에서 참여기업들의 인턴학생의 수준에 대한 만족도와 참여학생의 학업과정에 대한 만족도가 매우 높았다는 점은 사업이 매우 성공적으로 운영되고 있음을 보여주는 결과라 할 수 있으며[5], 같은 맥락에서 기업과 학교의 수요가 반영된 인력양성 유망분야를 선정하고 미리 인력을 양성하여 산업의 형성 및 성장에 맞춰 인력을 공급하는 체계를 마련하는 것은 지식정보보안 산업 발전을 위한 매우 중요한 작업임을 반증하는 것이라 할 수 있다. 이는, 본 논문이 지식정보보안 분야의 유망 분야에 대해 연구한 기존의 많은 연구들과 비교했을 때 갖는 가장 큰 차별점이기도 하다. 단순히 미래 유망 분야를 제시한 수준이 아니라 유망 분야간 우선순위를 분석하여 제시함으로써 실질적으로 우선적 인력양성 분야를 결정할 수 있는 정책의사결정의 과정을 보여주고 있기 때문이다.

그러나, 본 논문에서 제시한 5개 지식정보보안 분야의 인력양성 유망분야는 국내외 유명 연구기관들이 현재 시점에서 예측하고 있는 유망 분야에 대한 문헌연구와 그 결과에 대한 설문조사를 통해 도출한 것으로 이미 시장이 형성되었거나 기술적으로 구현이 이미 끝나 유망분야라 하기엔 다소 애매한 분야도 있으며 보다 획기적인 유망 분야의 발굴에 대한 아쉬움도 남는다. 따라서, 향후 새로운 인력양성사업을 구상하거나 현재 진행되고 있는 KISA 고용계약형 석사과정 사업의 사업분야를 변경 또는 확대하고자 할 경우에는 정부의 적극적인 지원을 바탕으로 산학연관 전문가들을 대상으로 한 대규모의 유망분야 선정을 위한 자료조사 및 의견수렴 작업이 필요하다. 또한, 해마다 기업 및 대학을 대상으로 지식정보보안 분야의 기술수요 조사를 정기적으로 실시하고, 신규개설의 필요성 및 분야선정에 대한 심층적인 검토를 실시할 수 있는 체계를 마련하는 정책도 필요하며 이와 함께 어떠한 인력을 어떻게 양성할 것인지를 결정하는 지식정보보안 분야 직무체계 및 직무수준도 개발하여야 할 것이다[2]. 장기적으로는 지식정보보안 분야에서 수요에 기반해서 인력을 양성할 수 있는 체계(수요기반 인력양성 체계, knowledge supply chain management system)의 구축 및 운영이 필요하고, 지식정보보안 분야로 우수한 인력이 지원할 수 있도록 유인하고 종사자들의 지속적인 근무 유도 및 경력 개발을 위한 경력개발맵(career development map)을 개발할 필요가 있다. 지식정보보안 분야의 정책을 수행하고 있는 여러 부처별 업무 분장에 적합한 정책 목표와 정책 수단을 조화시킬 수 있는 조정역할도 매우 필요하다. 이러한 작업들은 장기적이고 합리적인 지식정보보안 분야의 인력양성체계 수립을 위한 중요한 기초작업들이며 이러한 밑작업이 있어야만 보다 안정적인 인력양성이 가능할 것이다.

참고문헌

[1] 방송통신위원회, 행정안전부, 지식경제부, 2010 국가정보보호백서, pp. 1-333, 2010년 4월.

[2] 전효정, 김태성, 유진호, 지상호, "정보보호 분야 직무체계 개발," 정보보호학회논문지, 19(3), pp. 143-152, 2009년 6월.

[3] 지식경제부, 지식정보보안 IT전략기술로드맵 2015, pp. 1-29, 2009년 7월.

[4] 한국인터넷진흥원, 국가 정보보호 교육 프레임워크 개발, pp. 1-92, 2009년 11월.

[5] 한국인터넷진흥원, 지식정보보안 분야 인력 현황 및 중장기 인력수급 전망 분석, pp. 1-242, 2010년 10월.

[6] 한국정보보호진흥원, 유비쿼터스 환경에서의 정보보호 정책 방향, pp. 1-326, 2008년 3월.

[7] 한국정보보호진흥원, 2007 국내 정보보호산업 시장 및 동향 조사, pp. 1-227, 2007년 11월.

[8] Alcatel-Lucent, Creating the Trusted, Dynamic Enterprise: An Enterprise Security Blueprint, pp. 1-12, Jul 2009.

[9] CheckPoint, Comprehensive Endpoint Security, pp. 1-10, 2009.

[10] Cisco, Cisco Smart Business Roadmap - Security, pp. 1-8, 2006.

[11] EU, Beyond the Horizon: Thematic Group 3 - Security, Dependability and Trust, pp. 1-23, Jan. 2006.

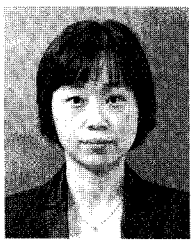
[12] IBM, IBM Security Technology Outlook: An Outlook on Emerging Security Technology Trends, pp. 1-16, Oct. 2008.

[13] IBM, Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security, pp. 1-8, Mar. 2009.

[14] IDC, Secure Enterprise Threat Management through an Integrated Security Framework, pp. 1-13, Aug. 2006.

[15] IDC, Utilizing Professional Services to Cut Costs by Minimizing Deployment Risks, pp. 1-9, Sep. 2009.
[16] Microsoft, Business-Ready Security, pp. 1-10, Nov. 2009.
[17] NIST, Information Technology Security Training Requirements: A Role- and Performance-based Model, Special Publication 800-16, pp. 1-171, Apr. 1998.
[18] Rand Corporation, The Global Technology Revolution 2020: In-depth Analyses, pp. 1-281, 2006.
[19] T.L. Saaty, "Diagnosis with dependent symptoms: Bayes theorem and the Analytic Hierarchy Process," Operations Research, Vol.46, No.4, pp. 491-502, Aug. 1998.
[20] T.L. Saaty, The Analytic Hierarchy Process: Planning, Priority Setting, Resource Allocation, McGraw-Hill, pp. 1-287, Jan. 1980.
[21] VTT, Technology Roadmap of Security Research, pp. 1-33, 2007.
[22] www.itstat.go.kr (IT통계포탈), 2010.11.
[23] www.kisa.or.kr (한국인터넷진흥원), 2010.11.
[24] www.kisia.or.kr(지식정보보안산업협회), 2010.11.

〈著者紹介〉



전 효 정 (Hyo-Jung Jun) 학생회원
2001년 2월: 충북대학교 경영정보학과 학사
2003년 8월: 충북대학교 경영정보학과 석사
2003년 9월~2007년 5월: 한국전자통신연구원 사업기획팀 기술원
2006년 9월~현재: 충북대학교 경영정보학과 박사과정
〈관심분야〉 정보시스템 정보보안, 보안감사, 정보보호정책

김 태 성 (Tae-Sung Kim) 종신회원
1997년 2월: KAIST 산업경영학과 박사
1997년 2월~2000년 8월: 한국전자통신연구원 정보통신기술경영연구소 선임연구원
2005년 1월~2006년 2월: Univ. of North Carolina at Charlotte 방문교수
2010년 7월~현재: Arizona State University 방문연구원
2000년 9월~현재: 충북대학교 경영정보학과 조교수, 부교수, 교수
〈관심분야〉 정보보호 분야의 경영 및 정책 의사결정