

정보보안 인력양성을 위한 탐색적 연구: 정부, 기업, 학계, 인력 관점 기반*

서경진** · 최지은*** · 김희웅****

< 목 차 >

I. 서론	4.4 기업관점의 인과관계 다이어그램
II. 개념적 배경	4.5 인력관점의 인과관계 다이어그램
2.1 정보보안 인력양성의 필요성	4.6 분석결과 요약
2.2 정보보안 인력양성 현황	4.7 정보보안 인력양성 방안
III. 연구방법론	V. 토의 및 시사점
3.1 인터뷰 연구 대상	5.1 연구의 한계 및 향후 연구 방향
3.2 인과관계 다이어그램	5.2 결론 및 시사점
IV. 분석결과	참고문헌
4.1 인과관계 다이어그램 분석틀	<Abstract>
4.2 정부관점의 인과관계 다이어그램	
4.3 학계관점의 인과관계 다이어그램	

I. 서론

최근 전 세계적으로 사이버보안에 대한 각계 각층의 관심이 크게 증가하고 있으나, 사이버보안 업무를 효과적으로 수행할 전문 인력이 부족한 실정이다. 글로벌 IT 벤더 시스코(Cisco)의 연례 보안 리포트(Cisco 2014 Annual Security Report, 2014)에 따르면, 최근 수 년 간

모바일과 클라우드 기술이 급격히 성장했음에도 불구하고, 그에 상응하는 전문 보안 시스템이 부족해 사이버범죄 피해가 급증한 것으로 파악된다. 시스코는 특히 사이버보안 전문 인력이 전 세계적으로 100만 명 이상 부족하다며, 이로 인해 단순 피싱 공격에서부터 특정 대상을 직접 겨냥한 대규모 사이버공격에 이르기까지 다양한 위협에 노출될 것이라고 경고한다.

* 본 논문은 2012년 정부(교육과학기술부)의 재원으로 한국연구재단의 지원 (NRF-2012-2012S1A3 A2033291)을 받아 수행된 연구임.

** AhnLab, 주저자, kyungjin4090@naver.com

*** 연세대학교 정보대학원, picastle@yonsei.ac.kr

**** 연세대학교 정보대학원 교수, kimhw@yonsei.ac.kr(교신저자)

사이버 보안 업계에서는 더욱 고도화된 위협에 대응하기 위해 일회성 보안 기술 및 솔루션 보다는 인력에 투자해야 할 시기라는 의견이 대두되고 있다 (KISA, 2014). 특히, 인터넷의 개방성과 표준화의 정도가 심화되고, 시스템의 복잡도(complexity)가 증가하면서, 새로운 서비스 및 시장이 형성되었다. 이러한 시장은 인터넷을 통해 악의적인 정보가 쉽게 유통될 수 있는 구조로 되어 있기 때문에 IT 자산에 대한 보호가 점차 어려워지고 있다 (김지훈·조시행, 2010). 보안 관련 업무를 전담할 인력양성 및 교육에 대한 투자의 필요성이 높아지고 있는 실정인 것이다. 이러한 인터넷 환경의 변화에 맞물려 대중들의 데이터 및 어플리케이션(application)으로의 접근성이 강화되면서 보안 피해의 가능성도 증가할 것이다 (Nazareth and Choi, 2015). 물리적인 제약이 사라지면서 악플로 인한 개인의 피해, 그리고 사회적인 손실도 늘어나고 있는 실정이다. 온라인상의 선플 활동을 촉진시켜 더불어 사는 공동체를 위해 사생활 및 정보 보안 관련 인력의 필요성이 증가하고 있는 것이다. 또한, 최근 주목받고 있는 ICT(Information and Communication Technology) 산업에서의 패러다임의 변화는 정보보안에 있어서 주요한 변화를 이끌어내는 계기가 될 것으로 보이며, 이러한 ICT의 변화는 정보보안 인력의 새로운 수요를 창출해 낼 전망이다 (Park et al., 2008).

이제 정보보안은 국가안보에 있어 필수요소가 되고 있다. 여러 국가가 정부 차원에서 정보보안 인력양성에 적극적으로 나서고 있는 이유는 정보보안 분야가 단기간이 아니라 장기간의 교육과 투자를 통해서만 현실필드에서 필요로

하는 고급전문인력 배출이 가능하기 때문이다. 한국인터넷진흥원(KISA)의 2014년 정보보호 업계 인력 수급 차이에 관한 발표 자료를 보면, 인력에 대한 신규 수요는 2014년 2,579명에서 2017년 4,581명까지 가파르게 증가할 것으로 예상되는 반면, 보안 전공자 신규 공급은 2014년 435명에서 2017년 921명으로 이에 훨씬 못 미치는 수준으로 증가하여 그 수급 차이는 더욱 커질 전망이다. 그러므로 관련 주체의 다양한 관점을 고려하여 실질적인 인력양성 수요와 공급 구조를 파악해 효과적인 인력양성 정책이 뒷받침 되어야 한다.

정보보안 분야의 고급인력의 수급 차 문제는 이를 해결하려는 지속적인 노력에도 불구하고, 계속해서 다양해지고 고도화되고 있는 보안사고에 따른 인력수요 증가와 함께 수급 차는 더욱 증가할 것으로 전망된다. 이제는 시간의 흐름에 따른 동태적 변화 및 지연된 피드백의 효과, 그리고 관련 주체 간의 유기적 연관관계를 고려한 거시적 관점의 접근이 필요하다. 정보보안 산업은 정부의 정책과 방향성, 기업이 요구하는 인력에 대한 니즈, 전문교육기관의 역할 등 여러 주체 간의 유기적 연관관계를 다차원적으로 고려해야 하며, 인력의 수요가 급증함에도 불구하고 산업에서 요구하는 인력을 양성하기까지 오랜 시간이 소요되는 특징을 고려하여 중장기적 계획을 수립하여야 한다.

이에 본 연구의 목적은 인터뷰 기반의 정성적 연구를 통해 빠르게 성장하고 있는 정보보안 산업에서의 인력 수급 불균형 현상의 원인을 정부·학계·기업·인력의 4가지 관점에서 동태적 관계를 분석하고, 각 요인들 간의 인과관계와 영향 분석을 통해 다양한 관점의 이슈를

도출하고 실질적인 대안을 제시하는 것이다. 본 연구 결과를 통해 국가 미래 전략 차원의 정보보안 인력양성을 위한 효과적인 추진방향을 제시할 수 있을 것으로 기대한다. 본 연구는 1차적으로 기존 문헌자료를 기반으로 정보보안 인력양성의 촉진요인과 저해요인에 대해 사전 조사를 수행하고, 이를 기반으로 정부, 학계, 기업, 인력 4가지 관점의 전문가 인터뷰를 통해 문헌자료를 검증하고 추가적인 이슈 및 인과관계를 도출하였다. 수집된 자료에 대해서는 변수간의 상호 동태적인 관계와 시간의 흐름에 따른 행태를 분석하는데 용이한 시스템사고 방법론에 기초하여 정보보안 산업에서의 인력 수급 불균형 현상을 해소하고 중장기적인 인력양성 방안에 기여할 수 있기를 희망한다.

연구의 주요 학술적 시사점은 다음과 같다. 국내의 정보보안 인력양성과 관련된 선행 연구에서는 주로 인력 공급측면에서 논의하였다(김동우 외, 2013; 김정덕, 2012; 김용겸·최우승, 2009; 김용훈, 2011; 권문택, 2005). 반면에, 본 연구는 정부·학계·기업·인력 4가지 관점에 기반을 두어 정보보안 인력수급 영향요인을 다각도로 살펴봄으로써 인력양성 생태계를 좀 더 다양한 측면에서 분석했다는 점은 기존 연구들과는 차별성을 지니고 있다고 할 수 있다. 또한, 인터뷰 기반의 정성적 연구를 시도함으로써 변수간의 유기적 관계에 대한 의미를 분석할 수 있었다. 선행연구들에서 제시된 정보보안 인력양성 관련요인들에 대해 인과관계 분석을 시도하고, 시스템 차원에서 분석할 수 있는 인과관계 다이어그램을 제시하여 종합적인 인력양성 과제와 나아가야 할 방향을 제시했다는 점에서 그 학술적 의의를 찾아볼 수 있다고 하겠다.

II. 개념적 배경

2.1 정보보안 인력양성의 필요성

해커들은 국경 없는 온라인 네트워크의 특징을 이용하여 공격 대상을 개인 또는 기업에서 국가 범위로 확대해 나가고 있으며, 이는 전 세계적인 사이버 보안 위협 증가로 이어지고 있다(이동범·곽진, 2014). 2007년 미국 국무부와 상무부에 기존에 알려지지 않은 일명, 제로데이(zero-day) 취약점을 이용한 해킹이 발생하였다. 두 기관 모두 안정성이 평가·인증된 최신 보안 제품들을 설치해놓고 있었지만 해커가 제로데이 취약점을 이용한 터라 모두 무용지물이었다. 그런데 흥미로운 것은 국무부의 경우 네트워크 포렌식 조사관, 패킷 분석 전문가, 보안 프로그래머 등으로 구성된 전담 보안 팀이 해커의 침입시도를 즉각 탐지하고 조치를 취한 반면, 이러한 보안 팀이 없는 상무부의 경우에는 해커의 침입이 있었는지 파악조차 못하고 있었다는 사실이다. 이 사건 이후 미국 정부는 조직의 보안을 단순히 제품에만 의존하는 경우 날로 발전해가는 해킹에 효과적으로 대응하기 어렵다고 판단, 검증된 보안 전문 인력을 체계적으로 발굴·육성 및 채용하기 위한 계획을 마련하게 된다.

물론 우리나라도 ITRC(IT Research Center, 대학 IT 연구센터)사업이란 것이 있다. ITRC 사업은 ‘정보통신분야의 석박사급 고급인력 양성 및 대학의 우수인력을 활용한 R&D 활동 적극 지원’을 목표로 1998년에 시작하였으며, 전국적으로 연평균 40여개의 센터가 운영되고 있다. 정보보호분야는 대표적인 통섭분야이며 그

트렌드가 시시각각 변화하는 것이 특징이다. 게다가 해킹 등 몇몇 분야에서는 그 재능이 타 분야에 비해 일찍 발견되기도 한다. 정보기술과 비즈니스 양자에 대한 충분한 이해가 있어야만 기업목표의 효과적 달성을 위해 정보기술을 적절히 활용할 수 있을 것이기 때문에(조세형·김기문, 2008), 이제는 우리 정부도 이러한 정보보호 분야의 특성을 인식하고 대학원 중심의, SCI급 논문 일변도의 인력양성정책에서 탈피해 보다 더 체계적이고 중장기적인 정책 수립이 필요하다.

보안은 정보시스템의 신뢰성을 확보하고 정보를 활용하는 기업환경을 성공적으로 이끄는 중요한 요인 중의 하나이며 (이장형·김종원, 2010), 지속적인 정보보호 분야의 다양화 및 규모의 성장이 이루어짐에 따라 관련 업무를 수행할 정보보호 전문 인력에 대한 수요는 계속해서 증가하고 있다. 또한, 다양한 산업이 융복합되어 창출되는 보안 관련 서비스 및 제품이 지속적으로 증가할 것을 판단됨에 따라 보안인력도 이러한 추세에 맞추어 양성하는 것이 바람직한 것으로 보인다 (홍진근, 2014). 보안 전문 인력에 의한 제어 시스템의 취약점 분석 및 평가를 주기적으로 수행하여 알맞은 보안 대책을 수립하는 노력이 필요하다 (민병길 외, 2014). 하지만 정부와 학계의 인력양성을 위한 노력에도 불구하고 현재 정보보호 전문 인력의 공급은 양적으로나 질적으로나 그 수요를 만족시키지 못하고 있다. 2010년 지식정보 보안 분야 인력현황 및 중장기 인력수급 전망 분석에 따르면 정보보호관련 전체 신규 공급 규모는 2009년 832명에서 2018년 1,871명까지 매년 늘어날 것으로 전망되고 있다. 하지만 신규공급

대비 수요는 줄지 않아 수급 간의 격차가 지속되어 공급부족으로 인한 어려움은 계속 될 것으로 전망된다. 아울러, 우수한 전문 인력 확보가 기업의 핵심경쟁력과 직결되고 있으나 고급 인력은 부족한 실정인 것으로 조사되었으며, 수요자 중심의 인재양성을 위해 대학의 정보보호 교육의 질적 수준을 향상시키고 정보보안시대를 견인할 창의적 인재 및 고급 인력 양성이 시급하다.

2.2 정보보안 인력양성 현황

정부는 미래 창조경제산업에서 정보보호산업이 지닌 중요성에 주목하고, 정보보호산업 발전 종합대책 수립을 통해 시장 확대, 기술력 강화, 전문인력양성 등 전략 방향을 제시하였다. 정보보호 전문인력양성 측면에서는 업계의 높은 인력 수요를 충족시키고 새로운 창조시장을 선도할 인재를 만들기 위한 체계적인 인력양성 계획을 제시하고, 2017년까지 최정예 정보보호 전문 인력을 5,000명 양성할 목표를 설정하였다 (한국경제, 2014). 초·중고 정보보호 영재 발굴, 정보보호 관련 학과 및 대학원 연구 지원 및 전문교육과정 지원 확대를 통해 석·박사급 인력을 확보하고, 우수 인재를 위한 특별 교육 프로그램, 기업 대상의 정보보호 최고위과정 및 분야별 보안담당자 교육 등 실제 업계 수요를 반영한 전문 인력 양성책을 도모하겠다고 밝혔다. 또한, 정보보호 인력의 체계적인 관리를 위한 정보보호 인력 통합관리 지원 시스템 구축 및 인력의 전문성 확보를 위한 국가기술 자격제도 확대 등 체계적인 인력 공급체계도 구축할 계획에 있다. 그러나 전문가들은 현재 사이

며 전문 인력 양성은 단기 전문교육을 통한 양적 확대에 치중하고 있음을 우려하며, 앞으로 국가 사이버 안보 강화를 위해 사이버 전문 인력 양성을 위한 구체적 실현방안에 대한 논의와 이를 바탕으로 한 정책 추진이 필요하다고 지적한다.

정부의 정보보안 인력양성의 움직임과 함께, 학계에서는 이러한 인력수요에 따라 보안학과 신설, IT기반 학과에서의 보안과목 개설, 정부 지원의 고용계약석사과정 운영 등 인력양성과정에 참여하고 있다. 대학교의 정보보호 관련 학과는 구 정보통신부의 IT 인력양성 사업 지원으로 2002년부터 개설되기 시작했으며, 2014년 기준 정보보호학과, 융합보안학과, 컴퓨터정보전학과, 사이버보안학과, 사이버경찰학과 등 28개 대학에 개설되었고, 2015년 기준 926명의 신입생을 모집한다.

미래창조과학부와 한국인터넷진흥원은 정보보호 기술 환경 변화에 신속히 대응할 수 있는 고급인력을 양성하기 위해 지난 2009년부터 고용계약형 석사과정을 운영하고 있고, 올해 지원된 금액은 8개 대학원에 총 22억6000만원에 이른다. 이 과정은 정보보호 고급인력을 확보할 수 있는 예산과 경험이 부족한 중소기업을 지원해 정보보호산업 역량을 강화하는 데 그 목적이 있다. 고용계약형 석사과정에 참여하는 학생들은 정부와 기업으로부터 등록금 및 학업장려금 등을 지원받아 석사학위를 취득하는 동시에 참여기업에 취업해 2년간 정보보호 실무를 담당하게 된다. 이로 인해 학생들은 석사학위 취득과 취업을 한꺼번에 해결할 수 있으며, 참여기업도 우수한 인재를 안정적으로 확보할 수 있는 장점이 있다. 고려대, 동국대, 아주대를 시

작으로 2014년에는 총 8개 학교와 안랩, 인포섹 등 관련 기업 64개가 이 프로그램에 참여하고 있으며, 지금까지 223명이 과정을 거쳐 현장에 투입되었고, 졸업을 앞둔 145명이 추가될 예정이다.

한편, 정부와 학계의 정보보안 인력양성 노력에도 불구하고 최근 악성코드 유포 및 개인 정보 유출사건이 계속해서 증가하면서 보안담당자들의 업무가 가중돼, 이와 관련 공공 및 기업의 보안담당자들이 업무수행에 있어 가장 큰 애로사항으로 꼽은 것은 ‘보안전문인력 부족(40.3%)’인 것으로 나타났다(보안뉴스, 2014). 기업 니즈를 반영해 인력수요에 기반을 둔 좀 더 체계적인 인력양성 계획이 필요한 시점이다.

해외의 정보보안 인력양성 현황을 살펴보면, 미국의 경우 2010년 ‘사이버보안 교육 계획’인 NICE(National Initiative for Cybersecurity Education)을 공표하는 등 본격적으로 국가 차원의 사이버보안 인력양성에 주력하고 있다(KISA, 2014). 또한, 영국은 정보안보국 정보통신본부(Government Communications Headquarter, CGHQ) 산하의 정보보호 전문기관인 전자통신보안그룹(Communications-Electronics Security Group, CESG)은 사이버보안 전문 인력에 대한 수요 증가에 대응하기 위해 사이버보안 전문가 인증제도(Certified Professionals)를 시행 중에 있다(KISA, 2014). 이렇듯 해외 보안 산업 선진국들의 인력양성 현황을 보면, 주요 나라들이 국가적 차원에서 인력 양성에 주력해 왔음을 알 수 있다.

이와 관련하여 국내 정보보안 인력양성과 관련된 선행연구를 살펴보면, 주로 정보보안 인적 자원 개발의 중요성을 지적하고 관련한 인력자

<표 1> 정보보안 인력양성 관련 선행연구

관점	연구주제	연구 방법	저자
교육 기관	정보보호 교육수요와 교육과정과의 비교 분석: 정보보호 교육센터 사례	설문 분석	강미화 외, 2014
	친융합형 IT 전문인력 양성 교육시스템 효과성 검증분석 연구	설문 분석	임양섭·김윤배, 2013
	국내 정보보호 교육체계 연구	사례 조사	김동우 외, 2013
	정보보호 전문 인력 양성을 위한 필수요구지식 및 교육인증 프로그램	문헌 연구	김정덕·백태석, 2011
	정보교육 및 실무활용을 위한 정보보호 관련 지식 및 기술에 대한 분류체계 연구	문헌 연구	김용겸·최우승, 2009
	정보보호 분야 직무별 필요 지식 및 기술 분석	문헌 연구	전효정 외, 2008
정부	국가 정보보안 이슈 및 정책방안에 관한 연구	문헌 연구	김정덕, 2012
	시스템 사고를 이용한 사이버전 보안 정책 레버리지 전략 연구	시스템 다이내믹스	양호경 외, 2013
인력	사이버 정보보호 인력의 양성과 유지를 위한 방향: 정보보호 전공자들의 직업 선택 의도에 관한 연구	설문 조사	채상마·김민균, 2012
시스템	유비쿼터스컴퓨팅환경의 정보보안 인력공급시스템 연구	문헌 연구	김용훈, 2011
	사이버테러정보전 전문인력 양성 및 관리 방향에 대한 연구	문헌 연구	권문택, 2005
	시스템 다이내믹스 방법론을 이용한 정보보호인력 공급체계 분석	시스템 다이내믹스	김태성 외, 2004
	인력 공급 계획 수립을 위한 시스템 다이내믹스의 활용 - UIT 도입에 따른 정보보호 환경 변화를 중심으로	시스템 다이내믹스	박상현 외, 2003

원의 개발 실태와 문제점, 정보보안 인력이 반드시 거쳐야 할 교육과정 등 주로 인력의 공급 측면에서의 연구에 초점을 두고 있다 (김동우 외, 2013; 김정덕, 2012; 김정덕·백태석, 2011). 일부 연구에서는 기업 수요 분석을 바탕으로 교육과정의 개선 등을 제안하고 있지만 이 역시 연구시점의 공급현황 파악과 충원 계획을 파악하는 조사 분석에 그쳐 향후 시장변화를 고려한 장기적 관점에서의 문제를 해결하기에는 한계가 있다 (정효정 외, 2008; 양호경 외, 2013) (<표 1> 참조).

Ⅲ. 연구방법론

본 연구에서는 정보보안 인력양성의 촉진 요인과 저해 요인을 도출하기 위해 인터뷰 기반의 탐색적 연구 방법을 채택하였다. 수집된 자료는 인과관계 다이어그램(Causal Loop Diagram, 이하 CLD)을 통해 각 요인들 간의 연관성 및 인과관계를 도식화하였다. CLD는 정성적 모델로서 시스템 분석을 통해 다양한 현상들에 대한 상호작용을 분석하고 그 영향을 예측하는데 이용되기에 (Akkermans and Helden, 2002; Kim et al., 2011; Sutanto et al., 2008-9; 손정은

외, 2013) 인터뷰 내용 분석을 위한 체계로서 활용하였다.

3.1 인터뷰 연구 대상

인터뷰 기반의 탐색적 연구를 위한 자료 수집은 크게 두 가지 방식으로 진행하였다. 우선 정보보안 인력양성에 대한 언론자료(예: 보안뉴스, 2014), 보고서(예: KISA, 2014), 그리고 기존 문헌 연구 자료(예: 강미화 외, 2014)를 통해 1차 자료를 수집하였다. 정보보안 인력양성에 대한 언론자료, 보고서, 그리고 기존 문헌 연구자료 등 1차 자료를 기반으로 정부·학계·기업·인력 4가지 관점으로 인력 양성과 관련된 주요 이슈들을 구분하였으며, 각 주체별 인력양성 관련 핵심 변수들을 도출할 수 있었다. 이러한 분석을 토대로 주체별 인터뷰 목적과, 보안인력 현황 및 인력양성 방안 도출을 위한 인터뷰 방

향을 구체적으로 설립하였다.

인터뷰 대상자는 전체 46명으로, 정보보안 관련 정부 부처의 교육관련 직무자 7명, 보안 관련 교수 및 박사 7명, 보안회사 팀장급 이상 11명, 정보보안 인력 21명으로 구성되었다 (<표 2> 참조). 주체별 인터뷰 목적에 따라 그룹별 인터뷰 내용이 다르게 설정되었으며, 시스템 다이내믹스 기반의 연구 흐름에 따라 1차 문헌조사 및 인터뷰를 통하여 인력양성 수급 차의 원인변수를 도출하는 방식으로 연구를 진행하였다.

인터뷰 목적은 대상자에 따라 구분되며, 정부 부처의 교육관련 직무자의 인터뷰는 정보보안 인력양성을 위한 정책수립 과정, 인력수급차 지표관련 이슈, 개선 의견 등 정부관점에서의 전반적 현황 파악을 통해 인력양성 관련 요인을 도출하고자 하였다. 정보보안 교수 및 박사 인터뷰는 보안학과 신설 배경, 고용계약석사

<표 2> 인터뷰 구성내용

분류	인터뷰대상자	인원	인터뷰 주요 목적 및 질문내용
정부	KISA 교육관련 직무자	3명	정보보안 인력양성을 위한 정책수립 과정, 인력 수급차 지표관련 이슈, 개선 의견 등 정부 관점에서의 전반적인 현황 파악
	NIA 교육관련 직무자	2명	
	NIPA 교육관련 직무자	2명	
학계	정보보안 교수	5명	보안학과 신설 배경, 보안학과 학생의 보안업계 진출, 고용계약석사과정 운영 효과 및 애로사항, 전반적 개선 의견 등 학계입장에서의 관련이슈와 전문가의견 도출
	정보보안 박사	2명	
기업	보안회사 팀장급 이상	11명	보안학과 출신의 보안업계 진출현황, 기업에서 원하는 보안인력, 정부와 학계노력에 대한 기업반응 등 기업입장에서의 관련이슈와 전문가의견 도출
인력	고용계약석사과정 재학생	14명	기업-정부-학계가 연계되어 있는 실제 양성과정에서의 만족 및 개선사항에 대한 의견
	보안회사 3년 미만 보안인력	7명	보안인력 수급실태, 근무처우, 높은 이직 및 퇴직률과 관련된 이슈에 대한 의견
합계		46명	-

과정 운영 효과 및 애로사항, 학생의 보안업계 진출을 위한 전반적 개선 의견 등을 파악하여 기존 문헌자료를 통해 파악하기 어려운 요인들을 도출하고자 하였다. 보안기업 팀장급 이상의 전문가인터뷰는 보안학과 출신의 보안업계 진출현황, 기업에서 원하는 보안인력, 정부와 학계노력에 대한 기업반응 등 정보보안인력 수요 측면에서의 이슈 및 해결과제를 도출하였다. 마지막으로, 인력관점의 인터뷰는 정보보안회사에서 인턴경험을 하고 곧 취업이 예정되어있는 고용계약석사과정 학생 인터뷰, 그리고 현재 보안회사에 근무 중인 3년 미만의 경력을 가진 인력 인터뷰로 진행되었다. 고용계약석사과정 인터뷰에서는 주로 기업-정부-학계가 연계되어 있는 실제 인력양성과정에서의 만족 및 개선사항에 대한 의견을 도출하였고, 보안인력의 인터뷰에는 현재 근로자로서 느끼는 보안인력 수급 실태, 근무처우, 높은 이직 및 퇴직률과 관련된 이슈에 대한 의견을 도출하였다.

3.2 인과관계 다이어그램

본 연구는 시스템적 사고를 기반으로 한 질적 연구방법론에 해당하는 시스템 다이내믹스(system dynamics) 방법론을 추가로 적용하고자 한다. 시스템 다이내믹스는 Forrester (1961)에 의해 체계화된 시스템 분석 및 설계 방법론으로 (Forrester, 1961), 복잡한 시스템을 전체적이고 구조적으로 바라봄으로써 관련된 다양한 요소들이 미치는 영향에 대해 분석하고 제반 문제점을 해결하는데 용이하다 (유상인 외, 2013).

시스템 다이내믹스에서 사용되는 CLD는 잠

재적인 원인들의 상호작용 구조를 도식화하여 피드백 루프를 구성하는데, 세 가지 기본요소로 구성된다. 인과관계의 방향은 화살표로 나타내고, 원인요소가 결과요소에 영향을 미치는 방향이 어떤가 하는 부분에 따라 (+)부호와 (-)부호를 이용하여 표시한다. 화살표의 시작점은 원인 변수이며, 종착점은 영향을 받는 결과변수이다. (+)부호는 원인변수와 결과 변수가 동일한 방향으로 변화하는 것을 의미하며, (-)부호는 반대 방향으로 변화하는 것을 의미하고, (=)부호는 Time Delay를 나타낸다 (Sterman, 2001).

인력계획은 미래지향적이고 동태적인 과정이기 때문에 장기적인 관점으로 분석해야 하며, 변화하는 환경에 맞추어 올바르게 대처해야 하는 속성을 지니기 때문에 (정재림 외, 2007) 인과관계 다이어그램을 통하여 전문가 등의 인터뷰를 보다 체계적으로 분석함이 마땅하다고 판단하였다. 더 나아가, 시스템 다이내믹스 방법론은 단기에서 중장기까지의 기간에 대하여 통계적 기법보다 신뢰할 만한 예측을 제공해 준다는 점에서 더 나은 결론을 도출할 수 있기에 (Pardue et al., 1999) 본 연구에서는 인터뷰에 기반을 둔 시스템 다이내믹스를 추가로 적용하였다.

IV. 분석결과

4.1 인과관계 다이어그램 분석틀

정보보안 인력양성 영향 요인은 인력양성수급 차를 중심으로 크게 인력공급요인과 인력수요요인으로 나뉘며, 인력공급보다 인력수요가

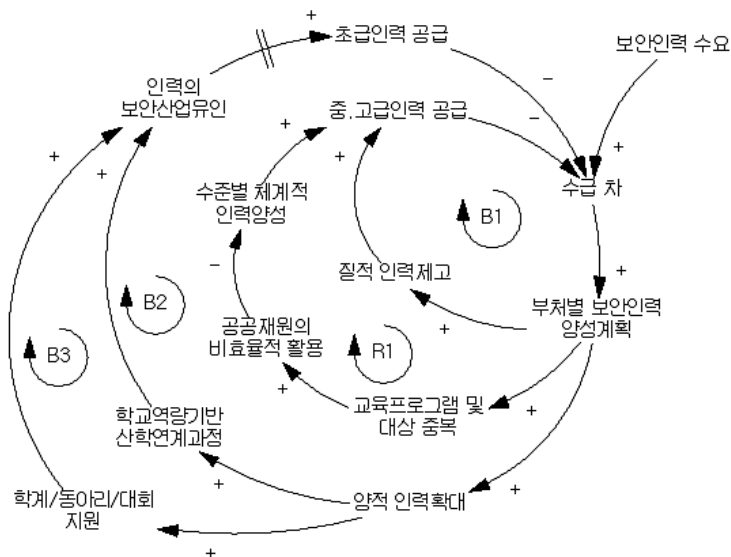
큰 현상을 반영해 수요증가는 수급차를 증가(+) 하고 공급증가는 수급차를 감소(-)시키는 기본 구조를 바탕으로 한다. 이것은 세부적으로 정부, 학계, 기업, 인력 4가지 관점에 따라 공급측 진요인, 공급저해요인, 수요측진요인, 수요저해요인으로 구분된다. 인력공급측면에서의 촉진요인은 인력공급에 긍정적인 영향을 미쳐 인력 수급차를 줄여주는 요인으로 Balancing Loop를 형성하게 되고, 저해요인은 인력공급을 저해하여 수급차를 줄이는데 방해되는 요인으로 Reinforcing Loop를 형성한다. 인력수요측면에서의 촉진요인은 보안사고 증가, 정보보호 전담 부서운영 증가 등 인력수요를 더욱 증가시켜 수급차를 증가시키는 요인들을 의미하며 Reinforcing Loop를 형성하게 되고, 저해요인은 인력수급과 산업성장의 트레이드오프 관계를 설명하는 요인들로 Balancing Loop를 형성한다.

분석 결과는 정부, 학계, 기업, 인력 4가지 관

점에 따라 크게 4가지 관점별 루프로 구성되며, 분석결과를 바탕으로 이슈 도출 및 최종 대안 인과관계 다이어그램을 제안한다.

4.2 정부관점의 인과관계 다이어그램

정부관점의 CLD를 <그림 1>과 같이 작성하였다. 미래창조과학부는 사이버위협에 대응하고, 정보보호산업 발전을 리드할 화이트해커를 2017년까지 정부차원 총 5,000명을 양성한다는 계획에 따라 ‘최정예 정보보호 실무자 양성’과 ‘차세대 보안리더양성’ 2개 과정을 운영한다고 밝혔다 (미래창조과학부 보도자료, 2013). 한국인터넷진흥원(KISA)에서 주관하는 ‘최정예 정보보호 실무자 양성(교육기관: KISA 아카데미)’ 과정은 기업의 정보보호 분야 재직자 120명을 선발하여 5개월간 시스템 해킹·대응, 네트워크 해킹·대응, 웹 해킹·대응 총 3개 과정의 전문 교육을 실시하며, ‘차세대 보안리더 양성 과



<그림 1> 정부 관점의 정보보안 인력양성 루프

정(교육기관: 한국정보기술연구원 BOB교육장)은 수학·과학 경시대회 및 해킹방어대회 입상자 등 우수한 고등·대학(원)생과 구직자를 대상으로 120명을 선발하여 총 6개월간 모의 사이버전, 디지털수사사례연구 등 전공과정 및 실습·실무 과정의 교육훈련을 실시한다. 2014년 초부터 미래창조과학부와 한국정보통신산업진흥원(NIPA)은 ‘클라우드 전문 인력 양성 과정(협력교육기관: IT뱅크멀티캠퍼스)’를 위해 산학연관 전문가 교육협의체를 통해 커리큘럼을 개발하고 있으며, 이 커리큘럼에 해당하는 4개 교육과정 중에는 보안기술 관리가 포함된다. 이렇듯 정부는 2012년을 기점으로 양적 인력제고뿐만 아니라 질적 인력제고를 통한 고급 인력확보를 위해 다각도의 노력을 하고 있다 [B1].

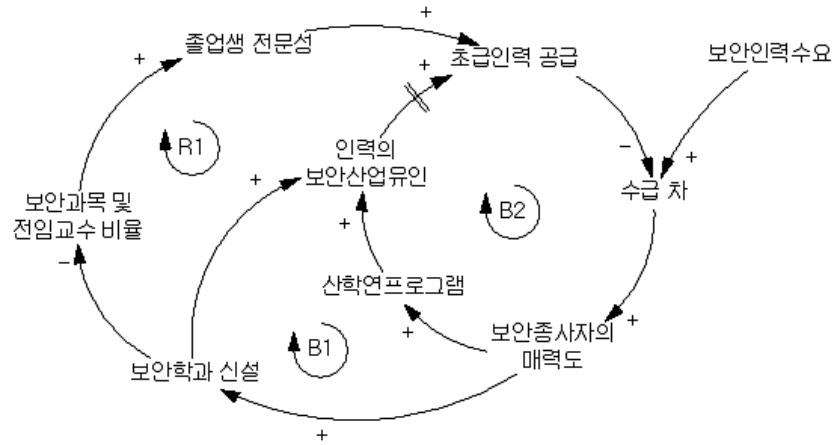
미래창조과학부와 한국인터넷진흥원은 정보보호 기술 환경 변화에 신속히 대응할 수 있는 고급인력을 양성하기 위해 지난 2009년부터 고용계약형 석사과정을 운영하고 있고, 올해 지원된 금액은 8개 대학원에 총 22억6000만원에 이른다. 이 과정은 정보보호 고급인력을 확보할 수 있는 예산과 경험이 부족한 중소기업을 지원해 정보보호산업 역량을 강화하는 데 그 목적이 있다. 고용계약형 석사과정에 참여하는 학생들은 정부와 기업으로부터 등록금 및 학업장려금 등을 지원받아 석사학위를 취득하는 동시에 참여 기업에 취업해 2년간 정보보호 실무를 담당하게 된다. 이로 인해 학생들은 석사학위 취득과 취업을 한꺼번에 해결할 수 있으며, 참여기업도 우수한 인재를 안정적으로 확보할 수 있는 장점이 있다. 2009년 고려대, 동국대, 아주대를 시작으로 2014년에는 총 8개 학교와 안랩, 인포섹 등

관련 기업 64개가 이 프로그램에 참여하고 있으며, 지금까지 223명이 과정을 거쳐 현장에 투입되었고, 졸업을 앞둔 145명이 추가될 예정이다 [B2]. 이와 더불어, 한국인터넷진흥원은 사이버 보안에 관심을 갖는 대학생들에게 올바른 정보보호 윤리관과 보안 관련 실무 경험을 제공하기 위해 대학 정보보호 동아리 지원 사업을 시행 중이며, 2012년 기준 총 37개 대학교의 40개 동아리를 선정해 연구 활동, 정보보호 세미나, 실습교육 등을 지원하여 보안 산업으로 인력을 유인하고 있다[B3]. 그러나 각 정부부처의 정보보안 업무처리의 중복성과 모호성으로 인해 효과성 및 효율성이 저하되고 있으며, 미국과 같이 국가적인 차원의 종합 계획이 존재하지 않는 가운데 다양한 교육 프로그램의 부재, 정보보호 교육기관의 정보 교류 부재 등으로 인해 큰 실효를 거두지 못하고 있는 실정이다 (김동우 외, 2013; 김정덕, 2012)[R1].

실제 전문가 인터뷰에서는 “과거에는 학계지원 및 산학연계과정을 통한 초급인력 확대에 초점을 두었으나, 시간이 흐름에 따라 고급인력 부족현상에 따른 인력의 질 제고를 위한 교육 프로그램 개발에 중점을 두고 있다.”는 의견이 다수였다[B1][B2][B3]. 그러나 “부처별로 인력양성계획을 따로 추진하고 있는 상황에서 교육대상과 교육프로그램의 중복을 배제하고, 좀 더 체계적인 인력양성 계획을 통해 효율성을 높일 필요가 있다.”라는 의견도 있었다[R1].

4.3 학계관점의 인과관계 다이어그램

학계 관점의 CLD는 <그림 2>와 같이 작성하였다. 대학교의 정보보호 관련 학과는 구 정



<그림 2> 학계 관점의 정보보안 인력양성 루프

보통신부의 IT 인력양성 사업 지원으로 2002년부터 개설되기 시작해 2010년 13개였던 정보보안학과가 2014년 기준으로 정보보호학과, 융합보안학과, 컴퓨터정보전학과, 사이버보안학과, 사이버경찰학과 등 28개 대학교에 개설되었으며, 2015년에 926명을 모집한다[B1]. 특히, 국방부와 고려대학교는 졸업 후 장교로 임관해 일정 기간 동안 사이버사령부 등에서 사이버국방을 위해 일하는 채용조건형 계약학과인 사이버국방학과를 신설하였다.

한편, 각 대학원에서는 2009년부터 정부지원 하에 고용계약형 석사과정을 운영하고 있고 고려대, 동국대, 아주대를 시작으로 2014년에는 총 8개 학교와 안랩, 인포섹 등 관련 기업 64개가 이 프로그램에 참여하여 정보보안 고급인력을 양성하는데 주력하고 있다[B2].

2010년 ‘지식정보보안 분야 인력현황 및 중장기 인력수급 전망 분석’에 따르면, 정보보안 컨설팅분야 전문 업체에 근무 중인 전체인력의 6.4%만이 ‘정보보호학과’ 출신인 것으로 조사되었으며, 68.8%가 ‘정보보호 관련학과’,

24.8%가 ‘비관련학과’ 출신인 것으로 조사되었다 (KISA, 2010). 이 가운데 신규 채용인력의 14.5%가 ‘정보보호학과’ 출신이며, 51%가 ‘정보보호 관련학과’ 출신인 것으로 조사되었다. 특히, 정보보호 부문의 신규채용 인력의 68%는 일정기간의 경력을 가진 경력자인 것으로 조사되었으며, 신규 채용인력의 8% 만이 졸업 직후 취업한 인력에 해당한다. 이렇듯 정보보호학과의 정보보호 업체 취직비율이 상대적으로 낮은 것으로 나타나며, 관련학과 졸업자의 수 및 정보보호 업체 취직률은 증가하는 반면 정보보호 관련 과목 및 전임교원의 수는 상대적으로 낮게 나타나 (KISA, 2010), 이는 대학에서 배출되는 정보보호 인력의 전문성 부족으로 이어질 수 있다 (김정덕, 2012)[R1]. 이와 관련해 정보보안 교수는 “정보보호는 컴퓨터 공학에서 분리된 학문으로 컴퓨터, 네트워크 등에 대한 기술적 지식뿐만 아니라 경영·법·제도 등 학제간 다양한 지식이 요구된다.”고 밝히고 있으며, “한 분야에 대한 집중적인 교육보다는 컴퓨터 기초분야를 중심으로 한 다양한 분야의 고른

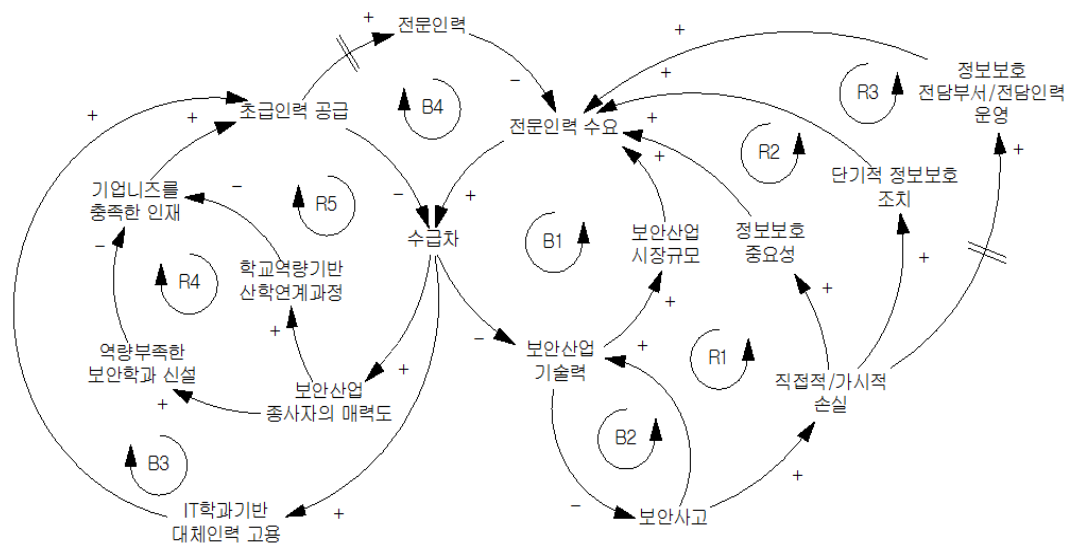
교육이 필요한데, 교육프로그램에 대한 충분한 고민 없이 시장성만보고 보안학과를 신설하는 것은 시장에서 원하는 인재를 길러내기 어렵다.”라고 언급하였다[R1].

4.4 기업관점의 인과관계 다이어그램

기업관점의 인과관계 다이어그램은 <그림 3>와 같이 나타내었다. 세계 각국의 정보 통신 기술 이용 확대로 국경 없는 사이버 공간에서의 위협이 경계 없이 파급됨에 따라 정보 보안 위협 역시 전 세계로 확대되고 있다. 이러한 가운데, 고급 정보 보안 전문 인재뿐만 아니라 정보 시스템 제어 기술 등 다양한 분야에서의 정보 보안 대책 및 정보 보안 시스템 설계 대응에 필요한 인재가 부족하며, 국가적 인력양성의 고도화에 따라 국가적 기술력에 차이가 나타나고 있다 (KISA, 2010; KISIA 2013)[B1]. 2013년 보안인력실태조사에 따르면, 정보보호산업 매

출액은 2010년 4조6696억원에서 연평균 15.2% 씩 성장하는 등 고성장을 기록하고 있다. 이 중에서 정보보안 매출액은 2010년 1조2378억원에서 연평균 9.3%씩 성장하고 있으며, 물리보안 매출액은 2010년 3억4318억원에서 연평균 17.2%씩 성장하고 있다. 정보보호산업 매출액이 높은 성장을 지속하고 있는 것은 정부의 법·제도 및 규제의 강화, 여러 차례의 보안사고로 인한 경각심 고조, 정부 및 기업의 보안 투자 강화, 물리보안 수출의 확대 등이 주요 원인인 것으로 분석된다[B2].

한편, 116개 국가공공부문 주요 기관의 정보보호 담당자들을 대상으로 실시한 설문조사에 따르면, 정보보호 전담부서 최상급자의 직급은 중간관리자급(공무원의 경우 3~4급)이 46.3%로 가장 많았고, 실무자급(공무원의 경우 5~6급)은 27.8%, 관리자급(공무원의 경우 1~2급)은 25.9%로 조사되었다. 2012년도와 비교하면 관리자급이 정보보호 전담부서의 최상급자



<그림 3> 기업 관점의 정보보안 인력양성 루프

인 경우가 증가세를 보였으며, 이는 정보보호의 중요성이 반영돼 보안전문인력 수요증가에 영향을 미친 것으로 볼 수 있다[R1]. 민간부분의 경우, 2012년 한 해 동안 정보화 예산의 일부를 정보보호에 투자한 사업체는 45.9%로 2011년 대비 19.2%p 증가한 것으로 나타나, 보안사고 증가에 따른 단기적 관점에서의 정보보호 투자가 늘어나고 있음을 확인할 수 있다[R2]. 국내 민간 사업체 중 공식적인 정보보호 전담조직을 설치·운영하고 있는 업체는 9.8%로 2011년 대비 1.3%p 증가하였고, 사내 정보보호 및 개인 정보보호 관련 전략구축 정책수립을 담당하는 IT 책임자로 CIO(정보관리 책임자, Chief Information Officer)를 임명한 사업체는 23.5%로 2011년 대비 6.6%p 증가하였으며, CISO(정보보호책임자, Chief Information Security Officer) 임명률은 2011년 대비 4.2%p 증가한 19.9%로 조사되어 그에 따른 보안전문인력 수요가 증가하였음을 파악할 수 있다[R3].

보안업계 전문가인터뷰 결과 “고급 정보 보안 전문 인재뿐만 아니라 정보 시스템 제어 기술 등 다양한 분야에서의 정보 보안 대책 및 정보 보안 시스템 설계에 대응할 인재 부족하다.”는 의견과 함께 “최근 보안 산업이 이슈화되면서 대학교에 정보보안학과가 많이 생겨나고 있지만, 실제 그 졸업생을 인터뷰를 해보면 기업 니즈에 필적한 인재를 찾기 어렵다.”는 의견이 다수였다[R4]. 산학연계과정에 대해서는 “근본적으로 학교 기반 및 역량에 기반을 둔 연계과정은 기업 니즈를 반영하여 교육프로그램을 개선하기가 매우 어렵다.”고 밝혔다[R5]. 또한, 정보보안 컨설팅분야 전문 업체에 근무 중인 전체인력의 6.4%만이 ‘정보보호학과’ 출신이며,

68.8%가 ‘정보보호 관련학과’, 24.8%가 ‘비관련학과’ 출신으로 조사된 것과 더불어 (KISA, 2010), 보안컨설팅 부서장은 “아직까지는 컴퓨터공학과 출신들이 IT자체를 깊이 이해하고 있어 채용 시 대체적으로 선호하는 편이다.”라고 밝혔다[B3].

문헌연구에 따르면, 국가적으로 정보보호의 필요성에 대한 인식은 높을지라도 실질적으로 산업의 배가적인 성장과는 무관한 상황이며 이로 인해 정보보호 전문 인력 양성의 필요성에 대해서도 국가적인 주목을 받지 못하고 있다 (김태성 외, 2004). 이는 국가, 산업체, 개인 모두가 정보보호 침해사고나 정보유출사건 등이 터져 직접적이고 가시적인 손실이 나야 정보보호를 위한 조치를 취하는 사후약방문식 또는 단기적이고 일시적인 정보보호 조치가 반복되고 있기 때문이다. 따라서 국가나 산업체 모두 장기적인 비용이 드는 정보보호 전문 인력 확보 및 정보보호부서의 상시 운영을 꺼려하는 것이고 인력은 좋은 대우를 바라기 어려운 정보보호 분야에 들어오기를 주저하여, 막상 사건이 터지면 전문 인력을 확보할 수 없어 사건이 커지거나 재발하는 문제가 지속적으로 반복되고 있다 (김태성 외, 2004). 장기적 관점에서 인력양성에 투자하고 있는 기업이 점차 증가하고 있지만[B4], 대부분의 기업들이 단기적 정보보호 조치에 집중하다 보니 늘 인력이 부족한 상황에 놓여있는 것이다[R3].

2014 정보보호백서에 따르면, 정보보호 전담 조직이 없는 경우 전담조직의 필요성을 어느 정도 느끼는지에 대해 필수적이며 조직발전을 위해 반드시 필요하다는 응답이 85.2%이며, 필수적이지는 않지만 필요하다는 응답은 14.8%

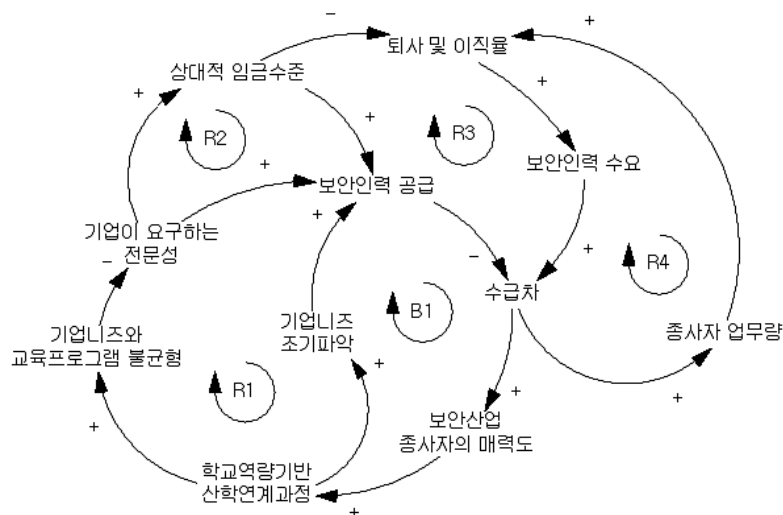
이다. 정보보호 전담조직이 신설되지 않는 이유는 예산인력 부족이라는 응답이 무려 85.2%를 나타냈으며, 그 외에 업무-조직체계상 불필요, 기관장 인식 부족등의 순으로 나타났다. 이는 보안사고가 증가하면서 정보보호에 대한 중요성과 함께 단기적인 정보보호 조치는 바로 이뤄질 수 있으나, 정보보안 전담부서를 운영하는 것은 필요의식이 있더라도 예산과 인력부족으로 지연될 수 있음을 시사한다[R3].

4.5 인력관점의 인과관계 다이어그램

인력관점의 CLD는 <그림 4>와 같이 작성하였다. 2009년부터 고려대, 동국대, 아주대는 정부지원아래 정보보안 고급인력양성을 위한 고용계약형 석사과정을 최초로 운영하기 시작하였으며, 2014년에는 총 8개 학교와 안랩, 인포섹 등 관련 기업 64개가 이 프로그램에 참여하고 있다. 고용계약석사과정의 재학생 인터뷰에서는 “기업 니즈를 미리 파악하고, 2년 동안 그

니즈에 맞춰 역량을 증진할 수 있는 고용계약 석사과정은 보안전문가로 나아가는데 도움이 된다.”는 의견이 다수였다[B1]. 그러나 “기업 니즈를 미리 파악했음에도 불구하고 기업이 요구하는 역량과 학교프로그램과 맞지 않을 경우에는 석사과정을 통해 기업이 요구하는 전문성을 갖추기 어렵다.”는 의견이 있었다[R1].

한편, 전 세계적으로 보안사고 증가에 따른 보안인력에 대한 요구사항은 늘어나면서도 상대적으로 임금이 적고 처우가 좋지 않다는 점은 인력난을 더욱 심화시키고 있다[R2]. 미국의 경우, 2014년 5월 21일 미국 상원 위원회가 국토안보부의 보다 원활한 사이버 보안 전문 인력 확보를 도모하고자 급여수준 향상을 통한 관련 인력 처우 개선을 주요 골자로 하는 법안을 통과하였다. 국토안보부는 처우 개선에 따른 무분별한 사이버 보안 인력의 지원 및 채용을 방지하기 위해 미국국립표준기술연구소의 ‘사이버 보안 인력체계 프레임워크 가이드라인’을 준용하기로 하고, 보안 인력의 직능별 세부 업



<그림 4> 인력 관점의 정보보안 인력양성 루프

무 내역이 명시된 해당 가이드라인을 기준으로 인력 배치 및 인센티브 지급 등을 결정하기로 하였다.

국내의 경우, 정보보안에 많은 관심이 몰리고 있지만 아직까지 정보보호 기술자나 보안 전문가의 급여에 대한 산정 기준이 없는 실정이다. 이와 관련해 A보안회사의 사원인터뷰에서는 “정보보안 산업은 타 산업 군에 비해 상대적으로 낮은 인센티브로 인해 우수 인력의 유입에 있어서도 제약이 존재한다.”, “근무 처우와 복지가 떨어지다 보니 우수인력들은 빠져나갈 수밖에 없는 상황이 발생하고, 상황이 이렇다 보니 업계에서는 인력 수급이 우선시 되어 단기학원 인력을 어쩔 수 없이 쓰게 되어 보안 서비스의 질이 낮아질 수밖에 없다. 여기에 업계에서는 전문성이 떨어지니 다시 신입을 채용하지 않으려는 움직임을 보이는 등 악순환이 계속되고 있다.”는 의견이 다수였다[R3].

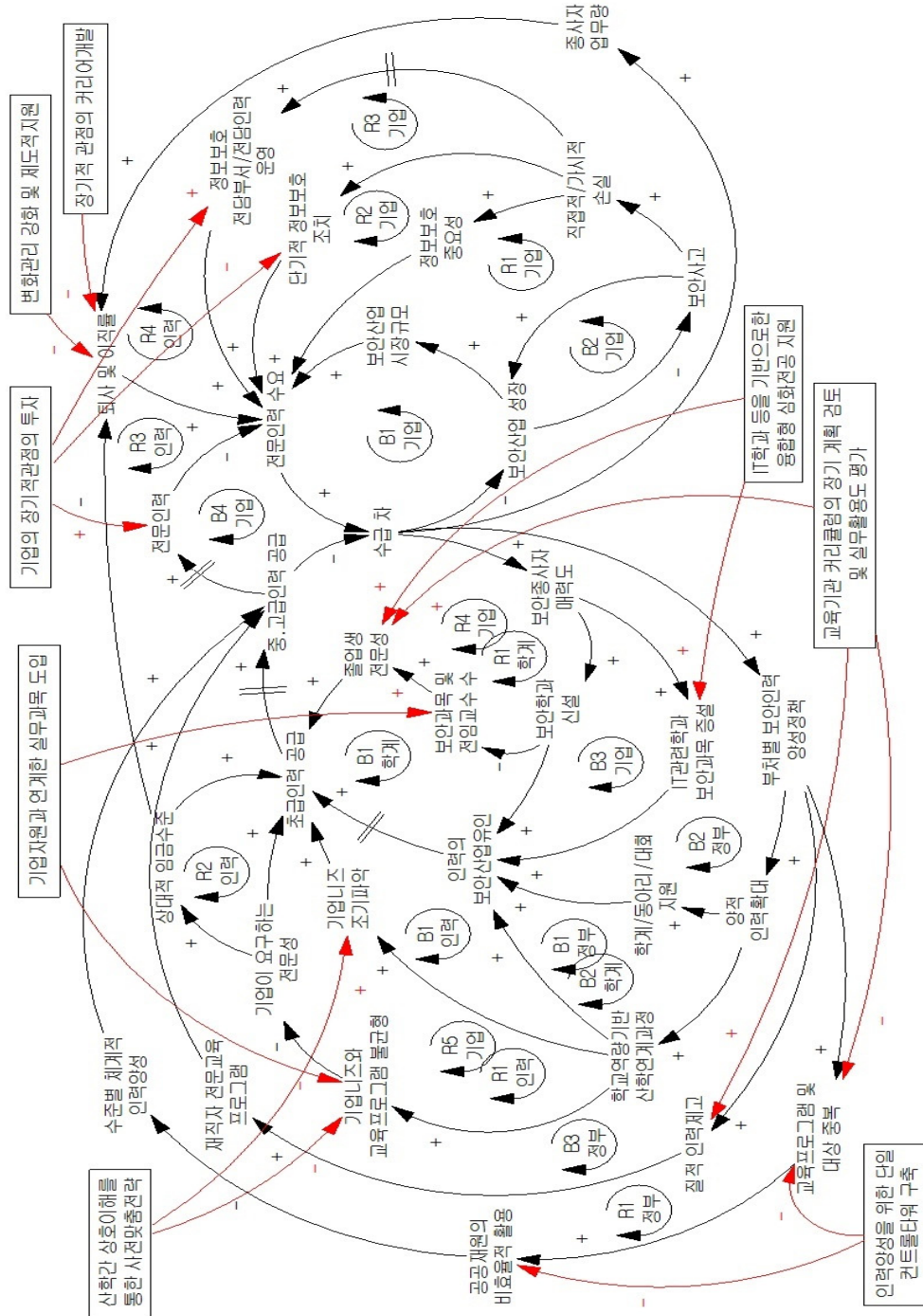
악성코드 유포 및 개인정보 유출사건이 증가하면서 보안담당자들의 업무가 가중되는 것 또한 인력난을 심화시키는 원인으로 작용한다. 이와 관련 공공 및 기업의 보안담당자들이 업무 수행에 있어 가장 큰 애로사항으로 꼽은 것은 ‘보안전문인력 부족으로 보안인력 업무 부담 증가(40.3%)’인 것으로 나타났다 (보안뉴스, 2014). A기업의 보안컨설턴트는 “새로운 IT 기술은 쏟아져 나오고 보안인력이 대응해야 되는 범위는 넓어졌음에도 불구하고 대부분의 기업 보안인력은 IT 인력 전체의 1% 미만”이라고 전했다. 이는 보안인력의 과도한 업무량에 따른 퇴사 및 이직률 증가로 인력수요는 더욱 증가하게 되는 강화루프를 형성한다[R4].

4.6 분석결과 요약

정부, 학계, 기업, 인력 4가지 관점의 인과관계 다이어그램 분석 결과를 정리해보면, 인력양성에 긍정적인 영향을 미치는 요인과, 앞으로 해결해야 할 이슈로 구분할 수 있다.

먼저, 인력양성에 긍정적인 영향을 미치는 요인을 살펴보면, 양적 인력양성을 넘어서 이제는 질적 인력제고를 위한 다양한 교육프로그램이 개발되고 있다는 것이다. 이와 관련해 보안 기업 인터뷰에 따르면, 최근 KISA 주도의 교육 프로그램은 신규인력의 역량개발뿐만 아니라 재직자의 역량을 개발하는데 매우 긍정적인 영향을 미치는 것으로 검증되었다. 또한, 최근 들어 정보통신공학, 컴퓨터공학과 같은 IT기반의 학과에서 보안과목을 도입해 보안 산업으로 인력을 유도하는 것은 기업 입장에서 매우 긍정적인 흐름으로 보고 있다. 보안 산업이 급성장함에 따라 정보보안학과가 신설되고 있지만, 아직까지 기업에서 원하는 인재를 길러내기 위한 교육 프로그램에 대한 고민이 많이 부족하다는 것이 기업의 입장이다.

하지만 아직까지 인력양성 시스템을 개선하기 위해 앞으로 해결해야 할 이슈도 있다. 정부 관점에서는 부처별로 각기 다른 보안인력 양성 정책 수립, 그로 인한 교육프로그램과 대상 중복이 주요이슈이며, 학계 관점에서는 기업니즈와 학교프로그램의 불균형, 신설된 보안학과 졸업생의 전문성 결여가 그것이다. 기업관점에서는 기업 니즈와 학계 프로그램의 불균형, 신설된 보안학과 졸업생의 전문성 결여, 기업들의 단기적 정보보호 조치, 고급인력양성까지 장시간 소요 등이 주요한 과제로 도출되었다. 마치



〈그림 5〉 최종 인과관계 다이어그램

막으로, 보안인력 입장에서는 과도한 업무량과 그로 인한 높은 이직률 및 퇴사율이 가장 주요한 해결과제로 도출되어 좀 더 장기적 관점에서 자기개발 및 커리어를 구축하기 위한 노력이 필요하겠다.

앞서 도출된 4개 관점의 인과관계 다이어그램에 대해, 하나의 통합된 시스템인 최종 인과관계 다이어그램을 <그림 5>와 같이 제안하며, 도출된 이슈에 대한 대안은 붉은색 선으로 표현하였다.

4.7 정보보안 인력양성 방안

본 장에서는 앞 장에서의 사례 분석 결과를 토대로 국내 정보보안 인력양성을 위한 상위 수준의 대안을 제시하고자 한다. 주제 별로 정부주축, 학계주축, 기업주축, 인력주축의 대안으로 구분할 수 있다.

먼저 정부 관점에서는 첫째, 지속적으로 양질의 전문 인력 양성을 유도할 수 있는 단일 컨트롤타워를 구축할 필요가 있다. 현재 분권형 형태를 띠고 있는 정보보안 인력양성 시스템은 업무처리의 중복성과 업무영역의 모호성 등으로 인한 효과성 및 효율성 저하를 개선하기 위해 전 국가차원의 연방형 체제 구축 및 보안 분야 간 통합

및 조정을 통하여 정보보안 인력양성 체제를 개선해야 한다. 정보보안과 관련된 정보공유, 의식고취, 전문교육, 고용 4단계 사이클을 포함하는 장기적 관점의 단계별 추진계획이 필요하다.

둘째, 교육기관 커리큘럼의 장기 계획 검토 및 실무활용도를 지속적으로 평가하여 교육프로그램에 대한 기여도를 개선해 나아가야 한다.

참고로 미국에서는 국가안보국과 국토안보부가 중심이 되어 학제간 성격을 갖는 정보보안 교육 프로그램을 개발하고 이를 인증함으로써 인력양성을 위한 기반구조를 구축하고 있으며, 이러한 인증프로그램에 가입된 140여개의 대학 및 대학원 재학생과 졸업생에게 공공기관 우선 채용 등 많은 인센티브를 제공하고 있다 (김정덕, 2012). 우리나라의 경우, 교육 프로그램이 따로 개발되어 있지 않아 각 대학의 기존 인프라에 기반을 두어 대학마다 다른 정보보안 교육 프로그램을 운영하고 있다. 기업 및 인력 인터뷰에서는 각기 다른 학교역량에 기반을 둔 교육프로그램에 의해 졸업생의 역량과 진로방향이 교육기관마다 다르게 나타날 수 있고, 그것이 기업에서 원하는 방향과 다를 수도 있다는 의견이 다수였으며, 국내에도 교육프로그램에 대한 명확한 평가기준과 인증제도 및 정보보안 필수요구지식 개발이 필요하다고 조언한다.

학계 관점에서는 3가지 대안을 제시할 수 있다. 첫째, 정보보안교육을 위한 산학프로그램 개발 시 기업과 학계의 상호이해를 통한 세밀한 사전 맞춤형 전략이 필요하다. 정부 관계자는 산학프로그램에서 기업 니즈가 충족되지 않는 것과 관련해, 학계역량에 의존하기보다는 기업이 교육프로그램에 대해 더욱 목소리를 높여야 한다고 입을 모았다. 학계 또한 기업의 요구사항을 반영해 교육프로그램을 개선하고 기업이 원하는 인재를 길러내어 산학간 시너지를 창출할 필요가 있다.

둘째, 학계는 교육프로그램 개선을 위해 기업자원과 연계한 실무과목을 도입할 필요가 있다. 기업과의 협의를 거쳐 실무에 우선적으로 필요한 과목 개설하고, 기업과 연계하여 인턴십

에 의한 학점대체과목을 개설하는 방안도 가능하다.

셋째, IT학과를 기반으로 한 융합형 심화전공을 지원하는 것이다. IT기반지식이 갖춰진 학생들을 보안 산업으로 유도하게끔 컴퓨터학과 내 보안과목 증설하는 방안, IT관련학과 주요과목을 융합하고 보안과목을 추가한 형태의 심화전공을 구축하도록 정부에서 지원하는 방안이 기업 및 학계인터뷰에서 제시된 바 있다.

기업이 주축이 되는 개선사항은 2가지로 요약된다. 첫째, 기업은 인력양성과 관련해 장기적 관점의 투자를 늘리게끔 정부의 지원이 필요하다. 기업이 장기적 인력양성에 투자하게끔

보안인식교육 강화하고, 제도적으로 이를 강제할 필요가 있다고 정부관계자는 조언한다.

둘째, 보안인력에 대한 변화관리를 강화하고 제도적 지원을 높여야 한다. 보안사고 증가에 따른 업무량 증가를 고려한 처우 개선과 인센티브 제공, 성과중심의 인력단가제도 개발 등을 통해 기존 인력이 업무를 지속적으로 해나갈 수 있도록 지원해야 한다.

마지막으로, 인력관점에서는 장기적 관점에서의 커리어를 개발할 필요가 있다. 다양한 커리어패스를 비교 분석하여 자신만의 장기적 목표를 세우고, 그것을 성취하기 위한 꾸준한 자기개발 강화를 통해 주체적으로 역량을 길러낼

<표 3> 분석을 통해 도출된 이슈 및 대안

인력양성 과제	제안 내용	주체	협업
인력양성을 위한 단일 컨트롤타워 구축	<ul style="list-style-type: none"> 단일 주체에 의한 전사적 국가 계획을 세우고 인력수요 측면에서 검토 정보공유 - 의식고취 - 전문교육 - 고용 4단계를 포함하는 장기적 관점의 단계별 추진계획 	정부	기업
교육기관 커리큘럼의 장기 계획 검토 및 실무활용도 평가	<ul style="list-style-type: none"> 교육 커리큘럼에 대한 명확한 평가기준을 제시하고 기준에 부합하는 경우에만 인증하는 제도 기업과 협업하여 교육의 실무활용도를 평가하고 커리큘럼 개선 	정부	학계 기업
산학 간 상호이해를 통한 사전맞춤전략	<ul style="list-style-type: none"> 기업은 원하는 인재상을 사전에 구체적으로 제시하고 학교는 그에 따른 적합한 육성프로그램을 갖추고 있는지 사전검토 기업의 지속적인 검토와 학교의 교육 커리큘럼 개선에 따른 시너지 창출 	학계	기업
기업자원과 연계한 실무과목 도입	<ul style="list-style-type: none"> 기업과의 협의를 거쳐 실무에 우선적으로 필요한 과목 개설 인턴십에 의한 학점대체과목 개설 	학계	기업
기존 IT학과를 기반으로 한 융합형 심화전공 개발	<ul style="list-style-type: none"> IT기반지식이 갖춰진 학생들을 보안산업으로 유도하게끔 컴퓨터학과 내 보안과목 증설 IT관련학과 주요과목을 융합하고 보안과목을 추가한 형태의 심화전공을 구축하도록 정부에서 지원 	학계	정부
기업의 장기적 관점의 투자	<ul style="list-style-type: none"> 기업이 장기적 인력양성에 투자하게끔 보안인식교육 강화 정부의 제도적 지원 	기업	정부
변화관리 강화 및 제도적 지원	<ul style="list-style-type: none"> 업무량 증가에 따른 처우 개선 및 인센티브 제공 성과중심의 인력단가제도 개발 	기업	정부
장기적 관점에서의 커리어 구축	<ul style="list-style-type: none"> 다양한 커리어패스를 비교 분석하여 자신만의 장기적 목표를 세우고 그것을 성취하기 위한 꾸준한 자기개발 강화 	인력	기업

필요가 있다. 이는 초급인력이 주요업무를 수행해나갈 수 있는 고급인력으로 거듭나는데 가장 중요한 과제라고 기업전문가는 조언한다.

위에 제시한 과제들과 주축 및 협업관계를 토대로 <표 3>과 같이 정보보안 인력양성 과제 및 주축과 협력관계를 제안하였다. 효과적인 정보보안 인력양성을 위해서 1차적으로는 정부, 학계, 기업, 인력 모두가 각 주체별 과제를 이행하기 위한 노력이 필요하며, 2차적으로는 각 과제 이행에 필요한 협업이 원활하게 이루어져 상호보완적 인력양성이 이루어져야 할 것이다.

V. 토의 및 시사점

5.1 연구의 한계 및 향후 연구 방향

본 연구는 정보보안 인력양성에 대한 각 주체의 노력에도 불구하고, 급증하는 인력수요에 비해 인력공급의 변화가 제자리걸음인 부분에 대해 탐색적인 연구를 수행한 것으로서 아래와 같은 한계점을 지니고 있다.

첫째, 문헌연구와 전문가 인터뷰를 통해 정성적 데이터를 수집하였으나 국내의 경우 아직까지 정보보안 인력양성을 위한 단일 체계가 정착되어있지 않고, 그로 인해 전사적으로 조사된 자료나 연구 자료가 매우 부족하여 정책 및 전략의 효과성에 대한 검증 및 입증이 부족하다는 것이다. 따라서 향후 정보보안 인력양성을 위한 단일 체계가 정착된 이후 대안 검증을 위한 정량적 효과 분석 등이 추가적으로 필요할 것으로 보인다.

둘째, 인터뷰 기반의 탐색적 연구를 진행함

에 있어 최대한의 대표성을 확보하기 위해 4가지 관점에서의 대표성을 지니는 전문가를 대상으로 인터뷰를 진행하였지만, 연구에서 채택하지 않은 다른 기업이나 다른 학계 전문가 의견에서 나타날 수 있는 다양한 영향요인들에 대해 살피지 못한 한계가 있을 수 있다. 따라서 보다 정확한 영향요인들의 인과관계 분석을 위해 다른 사례들도 추가하여 분석할 필요가 있겠다.

셋째, 인터뷰 기반의 탐색적 연구모형을 채택함에 따라 샘플 개수의 제약이 있을 수 있고, 전문가 인터뷰를 통해 도출한 자료 해석에 있어 연구자의 주관이 반영되었을 수 있다는 점이다.

향후 연구에서는 정보보안 인력양성 및 전략 성과에 대한 보다 많은 정량적 효과와 보다 다양한 사례분석을 통해 본 연구에서 제시된 인과관계 다이어그램을 보완 발전시킴으로써 보다 세밀하고 정교한 모델의 개발 등 실증적인 연구가 진행될 필요가 있다.

5.2 결론 및 시사점

본 연구는 최근 급성장하고 있는 정보보안 산업에서의 인력수급현상을 개선하기 위한 인터뷰 기반의 탐색적 연구를 수행하였다. 이는 시스템 사고 접근 방식에 기반을 둔 문제 분석을 통해 정보보안 인력양성을 위한 대안 제시를 목적으로 하였다. 개인들의 온라인상 활동이 급증하며 악플이 증가하고 사회적 문제가 야기되는 등의 문제점이 발생함에 따라, 더불어 사는 공동체를 위한 개인 사생활 및 정보 보안 전문가에 대한 수요가 증가하였기 때문에 사회적

발전을 위한 체계적인 정보보안 인력 양성이 필요한 시점이다.

시스템 사고 접근을 통하여 한국의 정보보안 인력양성 관련 이슈와 대안을 분석한 결과, 몇 가지 주요 사항들을 도출해 낼 수 있었다. 정부 입장에서는, 부처별 보안인력 양성정책에 따른 비효율성과 교육프로그램 및 대상 중복이 가장 큰 이슈로 부각되었으며, 이를 해결하기 위한 대안으로서는 인력양성을 위한 단일 컨트롤타워 구축과 교육기관 커리큘럼의 장기계획 검토 및 실무활용도 평가가 대두되었다. 학계 입장에서는, 기업 니즈와 교육기관 프로그램 불균형, 신설된 보안학과 졸업생의 전문성 결여, 그리고 IT관련학과 졸업생 선호 현상이 주요 이슈로 나타났으며, 이에 대한 대안으로서는 산학 간 상호이해를 통한 사전맞춤전략, 기업자원과 연계한 실무과목 도입, 그리고 기존 IT학과를 기반으로 한 융합형 심화전공 개발이 도출되었다. 기업 입장에서는, 기업의 단기적 정보보호 조치와 장기간의 고급인력 양성 과정, 그리고 보안인력의 과도한 업무량이 주요 이슈로 도출되었고, 대안으로는 기업의 장기적 관점의 투자와 변화관리 강화 및 제도적 지원이 대두되었다. 마지막으로, 인력 관점에서는, 높은 이직률 및 퇴사율, 그리고 기업 측 이슈와 중복되는 보안인력의 과도한 업무량이 이슈로 부각되었으며, 이에 대한 대안으로는 개인들의 장기적 관점에서의 자기개발 및 커리어 구축이 필요하다는 점이 도출되었다.

이러한 분석결과를 통해, 네 개의 주체 별 미시적 관점의 이슈를 보다 거시적인 관점에서 바라보며 동태적이고 상호 유기적인 관계를 파악할 수 있다는 점에서 그 의의가 있다고 할 수

있겠다. 앞에서 제시한 연구 결과를 토대로 다음과 같은 학술적 시사점을 제시할 수 있다.

첫째, 국내의 정보보안 인력양성과 관련된 선행 연구에서는 주로 인력 공급측면에서 논의한 반면 (김동우 외, 2013; 김정덕, 2012; 김용겸·최우승, 2009; 김용훈, 2011; 권문택, 2005), 본 연구는 정부, 학계, 기업, 인력 4가지 관점에 기반하여 정보보안 인력수급 영향요인을 다각도로 살펴봄으로써 인력양성 생태계를 좀 더 다양한 관점에서 분석하였다. 둘째, 정보보안 인력양성 관련 이슈와 대안을 도출함에 있어 인터뷰 기반의 정성적 연구를 시도함으로써 기존의 정량적 방법으로 도출하지 못한 새로운 영향변수를 도출하고 변수간의 유기적 관계에 대한 의미를 분석하였다. 셋째, 선행연구들에서 제시된 정보보안 인력양성 관련요인들에 대해 인과관계 분석을 시도하고, 복잡한 구조를 시스템 차원에서 가시적으로 살펴볼 수 있는 인과관계 다이어그램을 제시하여 정보보안 인력양성과 관련된 종합적인 이해를 돕는데 의의가 있다. 따라서 본 연구는 인터뷰를 기반으로 한 시스템 다이내믹스를 사용하여 단기적인 관점에서 탈피하고, 정보보안 산업의 다양한 주체 측면(정부·학계·기업·인력)에서 분석하고 인력수급 불균형 문제를 해소하기 위한 중장기적인 인력양성 방안을 제시했다는 점에서 기여가 있다고 할 수 있겠다.

또한, 본 연구의 실무적 시사점은 정보보안 인력양성의 개선을 위해 정부, 학계, 기업, 인력의 4가지 관점에서 전문가의견을 도출하고, 각 요인간의 인과관계와 영향 분석을 통해 다양한 관점의 이슈 도출 및 실질적인 대안을 제시함으로써 국가 미래 전략 차원의 정보보안 인력

양성을 위한 효과적인 추진방향을 제시하였다는 점에 있다. 더 나아가, 4가지 주체 간의 유기적 연관 관계를 다차원적으로 고려하여 정부, 기업, 학계 등 각 분야별 역할을 명확하게 부여하고 역량 통합을 위한 보안인력 양성의 시너지 제고 전략을 제시하였다는 점에서 실무적 의의를 지닌다.

참고문헌

- 권문택, “사이버테러정보전 전문인력 양성 및 관리 방향에 대한 연구”, 정보보안논문지, 제5권, 제3호, 2005, pp. 43-57.
- 김동우, 채승완, 류재철, “국내 정보보호 교육체계 연구”, *Journal of the Korea Institute of Information Security & Cryptology (JKIISC)*, 제23권, 제3호, 2013, pp. 545-559.
- 김용겸, 최우승, “정보교육 및 실무활용을 위한 정보보호 관련 지식 및 기술에 대한 분류 체계 연구”, 한국상업교육학회, 제23권, 제3호, 2009, pp. 123-140.
- 김용훈, “유비쿼터스컴퓨팅환경의 정보보안 인력공급시스템 연구”, 경영컨설팅연구, 제11권, 제3호, 2011, pp. 95-115.
- 김정덕, “국가 정보보안 이슈 및 정책방안에 관한 연구”, 디지털정책연구, 제10권, 제1호, 2012, pp. 105-111.
- 김정덕, 백태석, “정보보호 전문인력 양성을 위한 필수요구지식 및 교육인증 프로그램”, 디지털정책연구, 제9권, 제5호, 2011, pp. 113-121.
- 김지훈, 조시행, “사이버 환경에서의 보안위협”, 정보보호학회지, 제20권, 제4호, 2010, pp. 11-20.
- 김태성, 전효정, 박상현, 장석호, “시스템 다이내믹스 방법론을 이용한 정보보호인력 수급체계 분석”, 한국통신학회논문지, 제29권, 제2B호, 2004, pp. 228-239.
- 민병길, 안우근, 서정택, “사이버보안 위협 변화에 따른 취약점 분석 방안”, 정보보호학회지, 제24권, 제1호, 2014, pp. 7-12.
- 손정은, 장윤정, 이소현, 김희웅, “시스템 사고 접근을 통한 사회적 자본 증대 방안 연구: 소셜미디어 사용자를 중심으로”, *Information Systems Review(ISR)*, 제15권, 제2호, 2013, pp. 21-40.
- 양호경, 차현중, 신호영, 박호균, 유헌빈, “시스템 사고를 이용한 사이버전 보안 정책 레버리지 전략 연구”, 융합보안논문지, 제13권, 제4호, 2013, pp. 77-83.
- 유상인, 이소현, 김희웅, “스마트워크 활성화를 위한 탐색적 연구: 시스템 사고 접근”, *Enture Journal of Information Technology(EJIT)*, 제12권, 제3호, 2013, pp. 57-73.
- 이동범, 광진, “미국 정부의 사이버 공격에 대한 보안 전략”, 정보보호학회지, 제24권, 제1호, 2014, pp. 13-22.
- 이장형, 김종원, “보안 및 통제와 정보기술 사용자의 성격의 관계”, 정보시스템연구, 제19권, 제3호, 2010, pp. 1-12.
- 전효정, 유혜원, 김태성, “정보보호 분야 직무별 필요 지식 및 기술 분석”, *Information Systems Review*, 제10권, 제2호, 2008,

- pp. 253-267.
- 정재림, 전소연, 콰미애, 연승준, “시스템다이내믹스를 활용한 인력 수급 계획 모형설계”, 한국시스템다이내믹스 연구, 제8권, 제1호, 2007, pp. 49-66.
- 조세형, 김기문, “기업규모에 따른 정보기술 인력의 지식유형과 기업성과 간의 관계”, 정보시스템연구, 제17권, 제4호, 2008, pp. 181-206.
- 지식정보보안산업협회(KISIA), 2013 국내 정보보호산업 실태조사, KISIA, 2013.
- 채상미, 김민균, “사이버 정보보호 인력의 양성과 유지를 위한 방향: 정보보호 전공자들의 직업 선택 의도에 관한 연구”, 정보보호학회논문지, 제22권, 제2호, 2012, pp. 295-316.
- 한국인터넷진흥원(KISA), “지식정보보안 분야 인력현황 및 중장기 인력수급 전망 분석”, 2010, pp. 36-41.
- 한국인터넷진흥원(KISA), 주요국 사이버보안 인력양성 정책 분석, KISA, 2014.
- 홍진근, “국내대학 정보보호전공 교육과정 분석 및 융합교육정책”, *Journal of Digital Convergence*, 제12권, 제1호, 2014, pp. 599-605.
- Akkermans, H., Helden K., "Vicious and virtuous cycles in ERP implementation: a case study of interrelations between critical success factors", *European Journal of Information Systems*, Vol.11, No.1, 2002, pp. 35-46.
- Cisco, Cisco 2014 Annual Security Report, 2014.
- For Forrester, J.W., “Industrial dynamic”, Cambridge, 1961.
- Forrester, J. W., *Industrial dynamic*, Cambridge, 1961
- Kim, Hee-Woong., Jung, Gi-Young., and Lee, Ji-Eun., "An Exploratory Study of the IPTV Business in Korea: Issues and Suggestions for the Success”, *정보시스템연구*, Vol.20, No.4, 2011/12, pp. 23-47.
- Pardue, J.H., Clark, T.D. and Wagner, D., “Modeling short- and long-term dynamics in the commercialization of technical advances in IT producing industries”, *System Dynamics Review*, Vol.15, No.1, 1999, pp. 97-105.
- Nazareth, Derek L., Choi, Jae., “A system dynamics model for information security management”, *Information & Management*, Vol.52, 2015, pp. 123-134.
- Park, Sang-Hyun., Lee, Sang M., Yoon, Seong No., and Yeon, Seung-Jun., “A dynamic manpower forecasting model for the information security industry”, *Industrial Management & Data Systems*, Vol.108, No.3, 2008, pp. 368-384.
- Sterman, J., “Systems dynamics modeling: tools for learning in a complex world”, *California Management Review*, Vol.43, No.4, 2001, pp. 8-25.
- Sutanto, J., Kankanhalli, A., Tay, J., Raman, K. S., and Tan, B., "Change Management in Interorganizational Systems for the Public", *Journal of Management Information Systems*, Vol.25, No.3,

2008-9. pp. 133-175.

김보영, 국내 보안인력 공급, 수요의 20%뿐,
Retrieved December 30, 2014, A-
vailable: [http://www.hankyung.com/news/
app/newsview.php?aid=2014122981151](http://www.hankyung.com/news/app/newsview.php?aid=2014122981151)

김지연, 보안담당자 애로사항 1순위 “인력 없어
죽겠어요”, Retrieved December 29,
2014, Available: [http://www.boanews.
com/media/view.asp?idx=42069](http://www.boanews.com/media/view.asp?idx=42069)

이수석, 정보보호 고용계약형 완전정복
프로젝트① 개관, Retrieved December
30, 2014, Available: [http://www.boanews.
com/media/view.asp?idx=40758](http://www.boanews.com/media/view.asp?idx=40758)

서경진(Seo, Kyung-Jin)



연세대학교 정보대학원에
서 석사학위를 취득하고, 현재
안랩(AhnLab)의 서비스컨설팅
사업본부에서 정보보안컨설턴
트로 근무중이다.

최지은(Choi, Jee-Eun)



연세대학교 불어불문학과를
졸업하고, 현재 연세대학교 정
보대학원 석사과정 중에 있다.

김희웅(Kim, Hee-Woong)



National University of
Singapore 정보시스템학과에
서 근무했으며, 현재 연세대학
교 정보대학원에 재직 중이다.
주요 연구분야는 소셜미디어,
디지털 비즈니스, 정보시스템
관리 및 활용이다. MIS
Quarterly, Information Systems Research, Journal of
Management Information Systems, Journal of the
Association for Information Systems, IEEE
Transactions on Engineering Management, Journal of
Retailing 등에 논문이 게재되었다. 지식경영연구의 편
집위원장, Journal of the Association for Information
Systems, IEEE Transactions on Engineering
Management의 편집위원으로 활동하였다.

<Abstract>

An Exploratory Study on Development of Information Security Manpower

Seo, Kyung-Jin · Choi, Jee-Eun · Kim, Hee-Woong

Purpose

Information security industry is rapidly growing, but has been confronted with many challenges in a business environment. One of them is the imbalance between supply and demand of information security manpower, which has caused an insecure market situation. Therefore, this study has derived factors of promoting and hindering information security manpower from governance, academics, corporations, and workforce perspectives, and has analyzed a sequence of cause and effect of each factor.

Design/methodology/approach

This study is an exploratory research based on the interviews. The causal loop diagram (CLD) was developed to deduce key issues and propose alternatives.

Findings

The result of this study is expected to help the development of information security manpower in Korea, by minimizing the potential negative effects as well as maximizing the positive effects. This study found out the dynamic causes and effects of the security manpower system in each stakeholder's perspective. The cause-and-effect relationships between the stakeholders will be able to contribute to solve the imbalance of supply and demand in security manpower system.

Keywords: Information Security Manpower, Demand and Supply, Causal Loop Diagram

* 이 논문은 2015년 1월 29일 접수, 2015년 5월 2일 1차수정, 2015년 5월 19일 게재 확정되었습니다.