

정보보안전공 대학생을 위한 보안 윤리의식 분석 및 교육 방안

Situation Analysis and Education Plan of Security Ethics for Training College Students Majoring in Information Security

김태희

동신대학교 정보보안학과

Tae-Hee Kim(thkim@dsu.ac.kr)

요약

최근 정보보안을 전공하는 대학생과 보안 업무를 담당하는 내부자가 사이버범죄의 유혹에 넘어가 범죄에 가담하는 사건이 잇따라 발생함에 따라 컴퓨터 및 보안전문가들의 직업윤리의식 부재가 심각하다는 지적이 나오고 있다. 본 논문에서는 정보보안을 전공하는 대학생들을 대상으로 보안윤리에 대한 인식과 교육 실태를 조사하여 분석하고, 인성과 자질을 갖춘 인재양성을 위한 보안윤리 교육 방안을 고찰하였다. 정보화 사회 기반이 확대될수록 직업윤리가 더욱 중요해지고 있는 시점에서 정보보안을 전공하는 대학생들의 보안윤리에 대한 인식과 교육, 그리고 정보보안 전문가의 일탈행위에 대한 인식 등 윤리성과 직업의식이 미흡한 것으로 확인되었다. 이러한 문제를 해결하기 위한 방안으로 제안한 정보보안 전공 대학생들의 보안윤리를 제고하는 교육 방안을 통해 소명의식을 갖춘 보안전문가의 양성이 가능할 것으로 기대된다. 논문에서 제안한 보안윤리 교육체계에 따라 교육을 받은 그룹에서 보안윤리 의식이 현저하게 개선된 것으로 분석되었다.

■ 중심어 : | 보안윤리 | 정보유출 | 보안전문가 | 사이버범죄 | 직업윤리 |

Abstract

Recently, it has been pointed out that the lack of professional ethics of computer and security experts is serious as college students majoring in information security and insiders who are in charge of security work are involved in crimes after being tempted to cyber crimes. In this paper, we investigate and analyze the security ethics awareness and education situation of college students majoring in information security, and examine the security ethics education method for human resource development with personality and qualities. As the information society becomes more widespread, the ethics and occupational consciousness of the university students who are majoring in information security are recognized as lack of awareness and education about security ethics, As a solution to solve these problems, it is expected that it will be possible to nurture security experts who are aware of their vocation through the educational plan to enhance the security ethics of the information security major college students. According to the security ethics education system proposed in the paper, the security ethical consciousness of the group that received education was remarkably improved.

■ keyword : | Security Ethics | Information Leakage | Security Experts | Cyber Crime | Vocational Ethics |

I. 서론

미래사회 변화를 예측한 연구결과에 따르면, 4차 산업혁명이 선도하는 미래사회는 모바일(Mobile)과 인터넷 중심(All-IP)으로 진화할 것으로 예측하고 있다. 또한, 모바일과 사물 인터넷(IoT : Internet of Things)의 융합을 통해 스마트밴드, 스마트워치 등 모바일 IoT 시대로 발전하고 있다. All-IP는 네트워크상의 모든 장비에 IP가 부여되고 기존의 다양한 통신망 모두가 하나의 IP 기반망으로 통합되는 것을 말한다[1].

인터넷의 발전과 더불어 일상생활에 많은 편리함을 제공하고 있지만, 인터넷을 기반으로 발전하는 미래 핵심기술인 클라우드(Cloud)와 사물 인터넷 등 새로운 환경에 대한 보안위험은 계속해서 증가할 것으로 내다보고 있다. 왜냐하면 지금보다 훨씬 더 많은 인터넷 관련 서비스가 범죄로부터 노출될 가능성이 많으며, 조직화된 사이버범죄 조직의 능숙화로 인해 아무리 보안기술이 발전한다고 해도 시간이 지나면 이를 능가하기 때문이다. 이로 인해 인터넷을 사용한 30년 동안 발생한 사건사고보다 훨씬 더 큰 사건사고가 발생할 수 있다 [1-4].

특히, 정보보안을 전공하는 대학생, 화이트 해커, 프로그래머, 정보보안 관련 업무 종사자들이 해킹이나 내부 정보유출 등 사이버범죄의 유혹에 넘어가 범죄에 가담하는 사건이 잇따라 발생하고 있다. 이로 인해 정보기술 및 보안전문가들의 직업의식과 윤리성 문제가 또 다시 수면위로 부상하고 있다. 더욱이 소프트웨어 교육을 초·중등으로 확대시키게 된 상황에서 10대와 20대의 사이버범죄가 끊임없이 발생하고 있어 윤리와 인성교육이 갈수록 중요해지고 있다[5-10].

본 논문에서는 정보보안 전문 인력을 양성하는 과정에서 보안윤리교육을 강화시키기 위한 교육 방안을 도출하기 위하여 정보보안학과 대학생들을 대상으로 정보보안윤리의식에 대한 인식, 정보보안윤리의식에 대한 교육, 그리고 정보보안 전문가들의 일탈행위에 대한 생각을 조사하여 분석하고, 정보보안 전문가들이 반드시 갖추어야 하는 보안윤리교육체계를 제시하였다. 대학생들의 보안윤리 및 교육효과를 분석하기 위하여 정보보안윤

리 교과목을 수강한 학생들과 수강하지 않은 학생들을 대상으로 설문조사를 실시하여 분석한 결과, 보안윤리의식에 현저한 차이가 있는 것으로 나타났다. 즉, 정보보안전공을 희망하는 대학생들의 보안윤리의식은 보통 정도로 나타났지만, 보안윤리에 대한 교육을 받은 정보보안전공 대학생들의 보안윤리의식이 상대적으로 높게 나타났다. 이러한 결과를 토대로 초·중등학교의 SW 교육과정, 대학에서 신입생 선발 및 정보보안 교육과정, 기업 및 기관에서 정보보안인력을 선발하고 관리하는 과정에서 보안윤리를 검증하여 선발한 후 직무 수행 및 교육, 사후관리를 체계적으로 실시하기 위한 교육 방안을 제시하였다. 제한한 정보보안 인력의 보안윤리를 제고하는 교육 체계를 통해 소명의식을 명확하게 갖춘 보안전문가의 양성이 가능할 것으로 기대된다.

본 논문의 구성은 다음과 같다. 2장에서는 정보보안 관련 인력의 범죄사례, 보안윤리 교육과 유사한 관련 연구를 살펴보고, 3장에서는 연구의 대상, 범위 및 방법을 설명한다. 4장에서는 정보보안을 전공하는 대학생들의 보안윤리에 대한 인식에 대한 분석 결과에 근거하여 제안한 예방대책을 설명하고, 5장에서는 결론 및 향후 연구방향을 기술한다.

II. 보안인력의 범죄사례 및 관련 연구

1. 보안인력의 범죄사례

최근 들어 정보보안을 공부하는 대학생이나 관련 업무를 수행하는 종사자들이 사이버 범죄의 유혹에 넘어가 범죄에 가담하는 사건이 잇따라 발생하고 있다. 따라서 보안인력의 범죄사례는 청소년(10~20대), 대학생, 화이트해커, 보안관련 업무종사자 등으로 구분하여 사례를 정리하였다.

청소년들이 저지른 사이버범죄로는 고교생 3명이 웹하드 사이트를 통해 악성 프로그램을 유포해 쯤비PC를 만들고 벡스 게임 서버에 장애를 일으켰으며, ‘번개장터’ 어플에 엑소 콘서트 티켓과 박서준 팬미팅 티켓을 양도한다는 허위 글로 유인해 돈을 가로챈 10대도 경찰에 붙잡혔다. 또한, ‘좋아요’ 수가 많은 페이스북 페이지

의 관리자 계정 해킹프로그램을 판매한 고등학생 ○○군은 ‘악성코드 백신 우회’, ‘디도스 공격’, ‘해킹툴’ 등 기능별 프로그램 제작 의뢰 등의 광고 글을 게시하고, ‘○○소프트’ 라는 회사이름까지 만들었다[5][8][10].

지방의 한 대학 사이버보안학과 재학 중인 대학생 ○○씨가 자신의 해킹 지식으로 국내외 인터넷 사이트를 해킹해 수집한 개인정보를 유포시키다 경찰에 붙잡혔고, H대학교 학생들은 조직적으로 교수의 계정과 전산 시스템을 해킹해 출결, 과제, 성적 등을 조작한 사실이 드러났다. 이들은 H대학교 해킹보안동아리 출신으로 당시 사건은 경찰조사까지 이어지지 않았고, 학교 측의 징계로 마무리된 것으로 알려졌다. 지방 P대학에서 외식업을 전공하는 대학생인 ○○씨는 포털사이트 네이버를 타겟으로 개인정보를 도용해 포털사이트 접속하는 기능, 자동으로 카페 가입을 해주거나 카페회원 명단을 자동으로 추출해주는 기능을 포함시켰다[1][5][8].

블랙해킹과 화이트해킹의 구분이 점점 모호해지고 허가 없는 침투 테스트가 마구 발생하면서 보안 솔루션들이 표적이 되고 있으며, 대표적인 사례가 파이어아이(FireEye)와 카스퍼스키(Kaspersky)를 분석하여 오류를 공개한 전문가들은 블랙 해커와 다를 바가 없다[7][11].

해외에 서버를 두고 800억 원대 도박 사이트를 운영해온 ○○씨가 경찰에 붙잡혔다. 그는 7년 정도 네트워크 관련 회사를 운영한 바 있는데, 네트워크 운영 경험과 전문지식을 이용해 VPN으로 일본에서 접속한 것처럼 IP를 위장했다. 전국 7,459개 PC방의 약 47만대 PC를 감염시키고, 4년간 좀비PC로 악용한 ○○씨는 IT 벤처 사업가와 수도권 지역의 유명대학 컴퓨터학과 중퇴 출신으로 알려졌다. 2015년 3월에는 인터넷 보안전문가가 불법 도박업자로부터 10억 원을 받고 경쟁 도박 사이트를 해킹해 마비시킨 혐의로 구속됐으며, 2014년 11월 온라인결제 취약점을 이용해 부당이득을 챙긴 프로그래머 ○○씨는 명문대 컴퓨터공학과 출신의 6년 경력 프로그래머로 알려졌다[3][5][7][12].

2. 보안윤리 관련 연구

한국인터넷진흥원에서 발행한 “2015 국내 정보보호

산업 실태조사[13]”에서 보안분야 인력규모는 35,536명으로 정보보안 관련 사업체와 물리보안 사업체에 종사하고 있다. 2015년 정보보호 사업체의 신규 채용자는 2,236명이며, 2016년은 2,308명 수준으로 예상되며, 매년 증가하는 추세이므로 정보보안진공 대학생들을 대상으로 보안윤리 교육이 더욱 강화되어야 할 것으로 판단된다. 그러나 보안윤리에 대한 직접적인 연구는 미미한 상황이고, 인터넷 윤리 또는 정보보안 인식과 행위 등에 대한 연구 정도만 진행되고 있다.

인터넷 윤리에 관한 연구로는 스마트 환경에서 다양한 SNS를 가장 많이 이용하고 있는 대학생들을 대상으로 탈억제 효과로 인한 부정적 행위에 대한 인식을 조사하여 분석한 후 SNS 저격의 피해자와 가해자를 줄이기 위한 예방 대책을 제시한 연구 결과와 스마트폰 이용 목적별 위험 요인을 중심으로 부작용 유형과 유형별 핵심 이슈를 도출하고 이를 토대로 사회적 영향을 진단한 후 바람직한 스마트폰 활용에 대한 사회적 이해와 공감대가 형성될 수 있도록 부작용을 최소화하기 위한 대응 방안을 제시한 연구 결과가 있다[14][15].

정보보안 인식과 행위에 대한 연구로는 개인의 보안 관련 경험적 요인으로 인해 개인별 낙관적 편견이 존재하고, 낙관적 편견은 정보보안 인식에 영향을 미치며, 낙관적 편견이 많을수록 정보보안에 대한 인식은 부정적인 영향을 미침으로서 정보보안 인식이 낮아진다는 것을 확인한 연구 결과, 조직유형에 관계없이 처벌과 윤리교육이 정보보안준수에 긍정적 영향을 주는 핵심 요인임을 확인한 연구 결과, 그리고 공기업의 정보보안 인력의 적정성과 정보보안 담당자의 역할에 대한 인식을 파악함으로써 현 공기업의 정보보안 문제점을 분석하고, 이를 해결할 수 있는 방안을 제시한 연구 결과가 있다[16-18].

III. 연구대상 및 방법

1. 연구 대상

본 논문에서는 D대학교 정보보안학과에서 정보보안을 전공하는 대학생들을 대상으로 보안윤리의식에 대

한 인식, 보안윤리의식에 대한 교육, 그리고 정보보안 전문가의 일탈행위에 대한 인식을 조사하기 위하여 2016학년도 2학기 기말고사 직전인 15주차에 설문조사를 실시하여 분석하였다. 설문조사는 전공교과목으로 2학년 1학기에 개설된 정보보안윤리(1학점, 2시간) 교과목을 수강한 2학년과 3학년 41명, 수강하지 않은 1학년 31명을 대상으로 실시하였다.

2. 연구 도구

본 논문에서 정보보안전공 대학생들의 보안윤리의식을 조사하여 분석하고 윤리성과 직업윤리를 갖춘 정보보안 전문가를 양성하기 위한 보안윤리 교육 방안을 도출하기 위한 설문지를 만들어 활용하였다[16-18]. 설문지는 정보보안전공 대학생들의 직업윤리와 인성에 대한 인식, 대학생이나 정보보안 전문가들의 일탈행위에 대한 인식을 조사하여 분석하기 위한 목적으로 사례들을 조사하여 연구 목적에 적합하도록 작성하였다. 설문지는 3개 영역으로 나누어 각 영역마다 5개 문항으로 구성되어 있고, 각 문항은 5점 척도(매우 그렇지 않다 : 1, ... , 매우 그렇다 : 5)로 응답하도록 하였다.

3. 연구 절차

연구 대상을 두 개의 그룹으로 나누어 동일한 설문지를 이용하여 정보보안전공 대학생들이 생각하고 있는 보안윤리의식에 대한 인식, 보안윤리의식에 대한 교육, 그리고 정보보안전공 전문가의 일탈행위에 대한 인식을 조사하였다. 그룹 A는 정보보안윤리 교과목을 아직 수강하지 않고 보안윤리에 대한 사전 교육을 실시하지 않은 1학년 학생들을 대상으로 보안윤리의식을 조사하여 분석하였다. 그룹 B는 정보보안윤리 교과목을 수강하고 정보보안관련 전공기초교과목을 수강한 2학년과 3학년 학생들을 대상으로 보안윤리의식을 조사하여 분석하였다.

4. 자료 분석

정보보안전공 대학생들의 보안윤리의식을 분석하고 교육 방안을 도출하기 위하여 실시된 설문조사 데이터는 엑셀(Excel)의 통계 함수와 데이터 분석(t-검정) 기

능을 이용하여 보안윤리의식에 대한 그룹별 인식과 그룹간의 차이를 분석하였으며, 유의수준은 $\alpha=0.01$ 로 설정하였다.

IV. 분석 결과 및 교육 방안

1. 조사대상자의 인구통계학적 특성

조사대상자의 인구통계학적 특성을 살펴보면, [표 1]에서 볼 수 있듯이 전체 대상자 72명 중 정보보안윤리 교과목을 아직 수강하지 않아 보안윤리 교육을 받지 않은 그룹 A가 43.1%(31명), 정보보안윤리 교과목을 통해 보안윤리 교육을 받은 그룹 B가 56.9%(41명)였으며, 성별 구성에서는 남학생(56명, 77.8%)이 여학생(16명, 22.2%)보다 많은 것으로 나타났다.

표 1. 조사대상자의 인구통계학적 특성

그룹	남학생	여학생	전체(%)
A	28	3	31(43.1)
B	28	13	41(56.9)
A+B(%)	56(77.8)	16(22.2)	72(100.0)

2. 보안 윤리의식에 대한 인식

정보보안전공 대학생들의 보안윤리 의식에 대한 인식을 조사 및 분석하기 위하여 5점 척도의 질문을 실시하였다.

정보보안 전문가를 희망하는 정보보안전공 대학생들이 생각하는 보안윤리에 대한 인식을 파악하기 위하여 ‘직업윤리와 인성의 중요성(q01)’, ‘해킹과 크래킹의 개념에 대한 이해(q02)’, ‘그레이 해커의 개념(q03)’, ‘사이버 범죄의 인식, 합법과 불법에 대한 인식(q04)’, ‘정보보안전공 대학생들의 윤리의식 부재에 대한 생각(q05)’을 조사하여 분석한 결과는 [표 2]와 [그림 1]과 같다.

표 2. 보안윤리의식에 대한 인식

그룹	q01	q02	q03	q04	q05	합계
A	3.77	3.16	2.71	3.68	3.32	16.64
B	4.29	3.46	3.59	3.85	3.39	18.58
A+B	4.07	3.33	3.21	3.78	3.36	17.75

두 그룹 간에 보안윤리의식에 대한 인식의 차이가 있음을 알 수 있으며, 다섯 가지의 질문에 대해 두 그룹에서 ‘보통’ 이상(5점 척도 기준 3.55)의 긍정적인 응답을 하였고, 특히 정보보안 전문가를 희망하는 대학생들의 직업윤리와 인성은 특별히 중요하다(q01)는 질문에는 두 그룹의 학생들이 매우 긍정적으로 응답하였다.

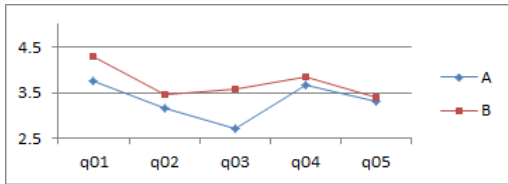


그림 1. 보안윤리의식에 대한 인식의 비교

다만, 해킹, 크래킹 및 그레이 해킹의 개념, 대학생들의 윤리의식 부재가 심각함에 대한 인식이 다섯 가지의 질문 중에서 상대적으로 낮게 나타나 보안윤리 뿐만 아니라 정보보안에 대한 기본 지식에 대한 교육도 충실하게 이루어져야 한다는 것을 알 수 있었다.

또한 보안윤리에 대한 인식을 알아보기 위해 전공교과목으로 정보보안윤리 교과목을 수강하지 않은 그룹 A와 해당 교과목을 수강한 그룹 B에 대하여 t-검정(등분산 가정 두 집단)을 실시하여 분석한 결과는 [표 3]과 같다.

표 3. 보안윤리의식의 인식에 대한 분석 결과

그룹	평균	분산	관측수	자유도	t 통계량	P(T<=t)	t 기각치
A	16.64	3.90	31	70	-3.348	0.0006	1.667
B	18.58	7.45	41				

두 모집단의 분산이 동일하다고 가정하였으므로 엑셀의 「통계 데이터 분석」 중에서 「t-검정 : 등분산 가정 두집단」을 이용하여 귀무가설 $H_0 : \mu_A = \mu_B$ 와 대립가설 $H_1 : \mu_A < \mu_B$ 를 검정하였다. 분석 결과를 살펴보면, 공동 분산이 5.929, 자유도 70이며, 검정통계량 T-통계량의 값이 -3.347로 나타났다. 대립가설 $H_1 : \mu_A < \mu_B$ 이므로 단측 검정을 수행하는 경우로 유의확률인 p-값이 0.0006이고, 기각역이 $t_{\alpha,df} = t_{0.01,70} = 1.667$ 이므로 귀무가설을 기각하여 통계적으로 그룹 A의 모집

단 평균이 그룹 B의 모집단 평균보다 작다.

분석 결과를 살펴보면, t-검정에서 p-값이 유의수준 1%보다 작게 나타났으므로 보안윤리에 대한 교육을 받지 않은 그룹(그룹 A)과 교육을 받은 그룹(그룹 B)에 따라 유의미하게 차이가 나타났다. 즉, 전공교과목으로 개설된 정보보안윤리 교과목을 통해 보안윤리에 대한 교육을 받은 학생들(그룹 B)이 받지 않은 학생들(그룹 A)보다 보안윤리의식에 대한 인식이 높은 것으로 분석되었다.

3. 보안 윤리의식에 대한 교육

정보보안전공 대학생들을 대상으로 보안윤리에 대한 교육의 필요성을 살펴보기 위하여 보안윤리의식의 교육에 대한 생각을 조사 및 분석하기 위하여 5점 척도의 질문을 실시하였다.

정보보안을 전공하는 대학생들이 사이버 범죄에 가담하는 사례가 증가함에 따라 보안윤리 교육의 필요성이 증가하고 있다. 이러한 시점에서 정보보안을 전공하는 대학생들은 보안윤리의식의 교육에 대해 어떠한 생각을 가지고 있는가를 살펴보기 위하여 ‘입학 면접에서 인성과 자질의 검증 여부(q06)’, ‘교육과정을 통해 인성, 직업윤리 및 소명의식에 대한 교육 여부(q07)’, ‘인성과 자질, 윤리교육의 강화 여부(q08)’, ‘인성과 직업윤리가 전제되지 않은 전문기술인 양성 교육에 따른 부작용 여부(q09)’, ‘정보보안전문가에 필요한 자질 및 직업윤리를 갖추기 위한 노력 여부(q10)’를 조사하여 분석한 결과는 [표 4]와 [그림 2]와 같다[1][5][8].

표 4. 보안윤리 교육에 대한 인식

그룹	q06	q07	q08	q09	q10	합계
A	3.52	3.32	3.55	3.13	3.77	17.29
B	3.73	3.85	3.76	3.39	4.00	18.73
A+B	3.64	3.63	3.67	3.28	3.90	18.12

두 그룹에서 보안윤리의식을 검증, 또는 교육을 받았거나 받을 예정이라는 생각에도 차이가 있음을 알 수 있었으며, 다섯 가지의 질문에 대해 두 그룹에서 모두 ‘보통’ 이상(5점 척도 기준 3.62)의 긍정적인 응답을 하였고, 정보보안전문가에 필요한 자질 및 직업윤리를 갖

추기 위해 노력하겠다(q10)는 질문에는 두 그룹의 학생들이 매우 긍정적으로 응답하였다. 다만, 인성과 직업윤리가 전제되지 않는 교육이 정보보안을 공부하는 대학생이나 업무담당자들의 일탈행위에 대한 원인이다(q09)라는 질문에 대해서는 두 그룹이 보통이라고 응답하여 보안윤리의 중요성(q01)과 상반되는 것으로 분석되었다.

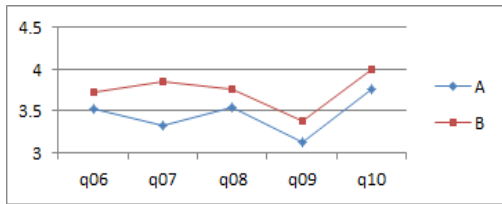


그림 2. 보안윤리 교육에 대한 인식의 비교

두 그룹에서 보안윤리의식을 검증, 또는 교육을 받았거나 받을 예정이라는 생각에도 차이가 있음을 알 수 있었으며, 다섯 가지의 질문에 대해 두 그룹에서 모두 ‘보통’ 이상(5점 척도 기준 3.62)의 긍정적인 응답을 하였고, 정보보안전문가에 필요한 자질 및 직업윤리를 갖추기 위해 노력하겠다(q10)는 질문에는 두 그룹의 학생들이 매우 긍정적으로 응답하였다. 다만, 인성과 직업윤리가 전제되지 않는 교육이 정보보안을 공부하는 대학생이나 업무담당자들의 일탈행위에 대한 원인이다(q09)라는 질문에 대해서는 두 그룹이 보통이라고 응답하여 보안윤리의 중요성(q01)과 상반되는 것으로 분석되었다.

또한, 보안윤리 교육의 필요성을 알아보기 위해 전공교과목으로 개설된 정보보안윤리 교과목을 수강하지 않은 그룹 A와 해당 교과목을 수강한 그룹 B에 대하여 t-검정(등분산 가정 두 집단)을 실시하여 분석한 결과는 [표 5]와 같다.

표 5. 보안윤리 교육에 대한 인식 분석 결과

그룹	평균	분산	관측수	자유도	t 통계량	P(T<t)	t 기각치
A	17.29	1.28	31	70	-3.036	0.0013	1.667
B	18.73	6.00	41				

두 모집단의 분산이 동일하다고 가정하였으므로 엑셀의 「통계 데이터 분석」 중에서 「t-검정 : 등분산 가정 두집단」을 이용하여 귀무가설 $H_0 : \mu_A = \mu_B$ 와 대립가설 $H_1 : \mu_A < \mu_B$ 를 검정하였다. 분석 결과를 살펴보면, 공동 분산이 3.977, 자유도 70이며, 검정통계량 T-통계량의 값이 -3.036로 나타났다. 대립가설 $H_1 : \mu_A < \mu_B$ 이므로 단측 검정을 수행하는 경우로 유의확률인 p-값이 0.0016이고, 기각역이 $t_{\alpha,df} = t_{0.05,70} = 1.667$ 이므로 귀무가설을 기각하여 통계적으로 그룹 A의 모집단 평균이 그룹 B의 모집단 평균보다 작다.

분석 결과를 살펴보면, t-검정에서 모두 p-값이 유의수준 2%보다 작게 나타났으므로 보안윤리에 대한 교육을 받지 않은 그룹(그룹 A)과 교육을 받은 그룹(그룹 B)에 따라 유의미하게 차이가 나타났다. 즉, 전공교과목으로 개설된 정보보안윤리 과목을 통해 보안윤리에 대한 교육을 받은 학생들(그룹 B)이 받지 않은 학생들(그룹 A)보다 보안윤리의식에 대한 교육의 필요성이나 교육에 참여하겠다는 인식이 높은 것으로 분석되었다.

4. 정보보안 전문가의 일탈행위에 대한 인식

정보보안전공 대학생들이 생각하고 있는 정보보안 전문가의 일탈행위에 대한 인식을 조사 및 분석하기 위하여 5점 척도의 질문을 실시하였다.

정보보안 전문가나 정보보안 업무담당자들이 사이버 범죄에 가담하는 사례가 증가함에 따라 보안윤리 교육의 필요성이 더욱 증가하고 있다. 이러한 시점에서 정보보안을 전공하는 대학생들은 정보보안 전문가나 정보보안 업무담당자들의 일탈행위에 대해 어떠한 생각을 가지고 있는가를 살펴보기 위하여 ‘인력 채용과정에서 직업윤리와 인성 등의 자질을 평가해야 하는지?(q11)’, ‘정보보안 전문가나 정보보안 업무담당자들의 직업윤리와 인성을 신뢰하는지?(q12)’, ‘소명의식이 부족한 인재양성으로 사이버범죄에 가담하는 사건이 증가하고 있다고 생각하는지?(q13)’, ‘블랙해커들의 행동으로 정보보안 전문가의 사기가 저하된다고 생각하는지?(q14)’, ‘사이버범죄를 저지른 사람의 징계수준을 높이고 부당수익을 환수하여야 한다고 생각하는지?(q15)’를 조사하여 분석한 결과는 [표 6]과 [그림 3]과 같다[3][5][7][11][12].

표 6. 일탈행위에 대한 인식

그룹	q11	q12	q13	q14	q15	합계
A	3.71	3.29	3.52	3.55	3.77	17.84
B	4.20	3.49	3.80	3.71	4.24	19.44
A+B	3.99	3.40	3.68	3.64	4.04	18.75

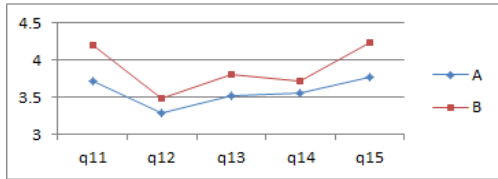


그림 3. 일탈행위에 대한 인식의 비교

두 그룹에서 정보보안 전문가 또는 정보보안 업무담당자가 사이버범죄에 가담하는 일탈행위에 대한 생각에도 차이가 있음을 알 수 있었으며, 다섯 가지의 질문에 대해 두 그룹에서 모두 '보통' 이상(5점 척도 기준 3.75)의 긍정적인 응답을 하였고, 정보보안 인력을 채용할 때 직업윤리와 인성 등의 자질을 집중적으로 검증하고(q11), 사이버범죄를 저지른 사람들의 징계수위를 높이고 부당수익을 환수해야 한다(q15)는 질문에는 두 그룹의 학생들이 매우 긍정적으로 응답하였다. 다만, 일반인들은 정보보안 전문가들의 직업윤리와 인성을 신뢰하고 있다고 생각하는가(q12)라는 질문에 대해서는 두 그룹이 모두 보통이라고 응답하여 정보보안 전문가나 정보보안 업무담당자들의 직업윤리와 인성에 문제가 있다고 생각하고 있는 것으로 나타났다. 또한, 보안윤리 교육의 필요성과 중요성을 살펴보기 위해 전공교과목으로 개설된 정보보안윤리 교과목을 수강하지 않은 그룹 A와 해당 교과목을 수강한 그룹 B에 대하여 t-검정(등분산 가정 두 집단)을 실시하여 분석한 결과는 [표 7]과 같다.

표 7. 일탈행위의 인식에 대한 분석 결과

그룹	평균	분산	관측수	자유도	t 통계량	P(T<=t)	t 기각치
A	17.84	2.34	31	70	-3.360	0.0006	1.667
B	19.44	5.25	41				

두 모집단의 분산이 동일하다고 가정하였으므로 엑셀의 「통계 데이터 분석」 중에서 「t-검정 : 등분산 가정 두집단」을 이용하여 귀무가설 $H_0 : \mu_A = \mu_B$ 와 대립가설 $H_1 : \mu_A < \mu_B$ 를 검정하였다. 분석 결과를 살펴보면, 공동 분산이 4.004, 자유도 70이며, 검정통계량 T-통계량의 값이 -3.361로 나타났다. 대립가설 $H_1 : \mu_A < \mu_B$ 이므로 단측 검정을 수행하는 경우로 유의확률인 p-값이 0.0006이고, 기각역이 $t_{\alpha,df} = t_{0.01,70} = 1.667$ 이므로 귀무가설을 기각하여 통계적으로 그룹 A의 모집단 평균이 그룹 B의 모집단 평균보다 작다.

분석 결과를 살펴보면, t-검정에서 모두 p-값이 유의수준 1%보다 작게 나타났으므로 보안윤리에 대한 교육을 받지 않은 그룹(그룹 A)과 교육을 받은 그룹(그룹 B)에 따라 유의미하게 차이가 나타났다. 즉, 전공교과목으로 개설된 정보보안윤리 교과목을 통해 보안윤리에 대한 교육을 받은 학생들(그룹 B)이 받지 않은 학생들(그룹 A)보다 정보보안 전문가나 정보보안 업무담당자들이 사이버범죄에 가담하는 일탈행위가 심각한 문제라고 생각하는 것으로 분석되었다.

5. 보안윤리 교육방안

최근 들어 정보보안관련 기술을 습득하여 사이버범죄에 악용하는 사례가 잇따라 발생하고 있다. 즉, 중·고생을 포함한 10대 청소년, 20대 대학생, 정보보안전공 대학생, 화이트해커, 프로그래머, 정보보안 관련 업무종사자들이 사이버범죄의 유혹에 넘어가 범죄에 가담하는 사건이 끊임없이 발생하고 있다. 이는 직업윤리가 전제되지 않은 전문기술인 양성제도의 부작용이 서서히 나타나고 있는 것이며, 특히 보안 분야는 양날의 검처럼 양면성이 있기 때문에 잘 사용하면 좋을 수 있지만 나쁘게 사용하면 독이 된다. 따라서 정보보안 전문가는 무엇보다도 인성과 직업윤리가 중요하고, 인재양성 시스템에서 태도와 자세, 인성 등의 자질을 집중적으로 점검해야 한다.

본 논문에서는 보안윤리교육의 중요성이 강조되는 상황에서 정보보안 전문가를 희망하는 정보보안학과 학생들을 대상으로 정보보안윤리 교과목을 통한 보안윤리 교육의 효과를 분석하였다. 즉, 보안윤리 교육을

받은 학생들이 받지 않은 학생들보다 보안윤리의식이 높은 것으로 확인되었다. 따라서 정보보안 인력을 양성하는 프로그램에서의 인성 및 윤리교육이 더욱 강화되어야 한다는 결론을 도출하고, [그림 4]와 같이 초등학교부터 정보보안 업무종사자들에 이르기까지 인터넷 공간에서 발생할 수 있는 다양한 윤리의식 확립을 위한 체계적인 교육 방안을 제시하였다.

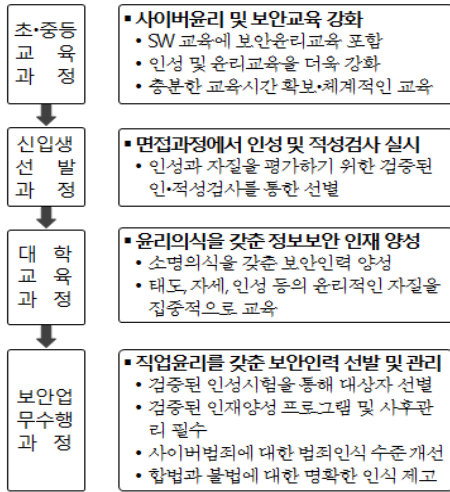


그림 4. 보안윤리 교육체계

첫째, 초·중등학교에서 SW교육의 의무화 방침이 확정되었지만, 미래 인재에 요구되는 핵심역량인 컴퓨팅사고력과 문제해결 능력 함양을 위한 내용을 가르치기에도 턱 없이 부족한 시간이라는 지적이다. 또한 사회생활의 일원으로써 살아가는데 필요한 교육을 어릴 적부터 받는 것과 마찬가지로 우리 삶의 매우 중요한 도구로 자리 잡은 인터넷 공간에서 요구되는 보안관련 윤리교육도 초·중등학교의 SW 교육에 포함시켜 가르쳐야 한다.

둘째, 정보보안 전문가를 희망하는 대학의 관련 학과에서 신입생을 선발하는 과정에 인성 및 적성검사를 실시하여 검증된 인성과 자질을 갖춘 학생들을 선발함으로써 보안윤리 관련 교육을 점점 더 강화시켜야 한다.

셋째, 인성, 윤리성 및 직업의식 등 소명의식을 갖춘 정보보안 인력을 양성하는데 필요한 보안윤리교육을

전공필수 교과목으로 지정하여 강화시켜야 한다. 보안에서의 윤리는 기본이다. 일탈행위에 대한 징계도 필요하겠지만, 무엇보다도 보안관련 지식과 기술을 익히는 과정에서 법적·윤리적 사항을 반드시 알아야 하며, 범죄 전력이 있는 사람들에게는 취업 제한 등의 불이익이 발생한다는 것을 인지할 수 있어야 한다. 특히, 화이트 해킹과 블랙 해킹의 구분이 점점 모호해지면서 인성과 보안윤리를 갖추지 못한 정보보안 전문가는 블랙 해커와 다를 바가 없기 때문에 보안윤리 교육이 점점 더 많이 필요하다.

마지막으로 보안관련 업무에 종사하는 사람들이 보안윤리와 프라이버시에 대해 명확한 자질을 갖추도록 교육하고 사후관리를 해야 한다. 보안관련 인력을 선발하는 과정에서 검증된 인성 및 적성검사를 실시하여 선별하고, 프라이버시 관련 문화 변화를 따라 잡을 수 있도록 지속적인 교육을 실시하여 사이버범죄에 대한 인식 수준을 개선시키고, 합법과 불법에 대한 명확한 인식을 갖추도록 해야 한다. 또한 정보보안 인력을 포함한 IT 전문가들은 다른 직업에 비해 기술의 발전 속도가 빠르기 때문에 어렵게 배우고 오랜 기간 훈련한 전문인인 만큼 사회적으로 적절한 대우도 보안윤리교육 만큼 중요한 요소이다.

V. 결 론

소프트웨어 교육 의무화 방침이 확정되면서 관련 업계와 학계의 관심이 뜨겁지만, 충분한 준비가 되지 않은 상태에서 교육이 진행되면 오히려 역효과가 날 수 있다는 우려도 적지 않다. 즉, 기본적인 인문학적 지식이나 보안윤리교육이 전제되어야 소명의식을 갖춘 정보보안 인력을 양성할 수 있다.

본 논문에서는 정보보안 전문가를 희망하는 정보보안 전공 대학생들을 대상으로 보안윤리에 대한 인식 정도와 교육의 필요성, 정보보안 전문가의 일탈행위에 대한 생각을 설문조사를 통하여 분석하고, 정보보안 인력에게 반드시 선행되어야 하는 보안윤리교육체계를 제시하였다. 정보보안전공 대학생들의 보안윤리에 대한

인식 정도를 분석하기 위하여 “정보보안윤리” 교과목을 수강한 대학생들과 수강하지 않은 대학생들을 대상으로 설문조사를 실시하여 분석한 결과, 두 그룹 사이에서 보안윤리에 대한 인식, 보안윤리에 대한 교육의 필요성, 그리고 정보보안 전문가들의 일탈행위에 대한 생각에서 현저한 차이가 있는 것으로 분석되었다. 이러한 분석결과를 토대로 초·중등학교, 대학의 신입생 선발과정, 대학의 교육과정, 그리고 기업 및 기관의 정보보안인력의 선발 및 관리과정에서 필요한 보안윤리 교육체계를 제시하였다. 본 논문에서 제시한 보안윤리 교육체계를 적용하여 보안윤리 교육을 체계적으로 실시한다면, 보안 분야에 종사를 희망하는 청소년 및 대학생, 보안 분야에서 업무를 수행하는 보안전문가들의 일탈행위를 최소화시키는데 큰 도움일 될 것으로 생각한다.

한편, 본 논문에서 제안한 보안윤리 교육체계에 따라 교육받은 정보보안전공한 학생들이 졸업한 후 현업에 종사하는 과정에서의 보안윤리 교육의 효과측정에 대한 어려움이 있다.

우선 대학에서 신입생을 선발하는 과정에서 인성과 자질을 검증하여 신입생을 선발하고, 전공교육과정에서 보안윤리 교육을 강화시킨 정보보안학과 대학생들을 대상으로 설문조사를 실시하여 본 논문에서 제안한 보안윤리 교육체계의 타당성을 검증하는 연구를 진행할 예정이다. 또한 보안윤리 교육체계를 타 대학에도 적용하여 정보보안전공자들의 보안윤리 교육을 확대시키고 교육효과를 측정할 결과를 보안윤리 교육체계에 반영할 계획이다.

참 고 문 헌

- [1] <http://www.boannews.com/media/view.asp?idx=49695>, 2016.02.24.
- [2] <http://www.boannews.com/media/view.asp?idx=51992>, 2016.10.07.
- [3] <http://www.boannews.com/media/view.asp?idx=52121>, 2016.10.23.
- [4] E. J. Lee, H. J. Jun, T. S. Kim, and Y. B. Kim, “Development of Information Security Education

- Framework for Information Security Employees: A Case of Educational Institutions,” J. of Korea Contents Association, Vol.14, No.1, pp.386-399, 2014.
- [5] <http://www.boannews.com/media/view.asp?idx=49328>, 2016.01.22.
- [6] K. C. Lee, “Measures for Enhancing System of Crime Victim’s Information Protection,” J. of Korea Contents Association, Vol.16, No.10, pp.175-187, 2016.
- [7] <http://www.boannews.com/media/view.asp?idx=52412>, 2016.11.18.
- [8] <http://www.boannews.com/media/view.asp?idx=49254>, 2016.01.15.
- [9] <http://www.boannews.com/media/view.asp?idx=42506>, 2014.08.17.
- [10] <http://www.boannews.com/media/view.asp?idx=42670>, 2014.08.25.
- [11] <http://www.boannews.com/media/view.asp?idx=47779>, 2015.09.09.
- [12] <http://www.boannews.com/media/view.asp?idx=52675>, 2016.12.13.
- [13] KISA, Survey for Information Security Industry in Korea : Year 2015, contents Pub, 2015.
- [14] M. S. Kang, “Status and Prevention of Negative Behavior due to Disinhibition Effect in SNS(Social Network Service),” Journal of the Korea Institute of Information and Communication Engineering, Vol.20, No.12, pp.2370-2378, Dec. 2016.
- [15] T. H. Kim and M. S. Kang, “Type Analysis and Countermeasures of Side Effects of using Smart Phone,” Journal of the Korea Institute of Information and Communication Engineering, Vol.17, No.12, pp.2984-2994, Dec. 2013.
- [16] J. G. Choi and M. S. Che, “An empirical study on the relationship of personal optimistic bias and information security awareness and behavior in the activity of information ethics,” Journal of the Korea Academia-Industrial cooperation Society,

Vol.17, No.5, pp.538-547, May. 2016.

[17] J. H. Ahn, J. H. park, K. M. Sung, and J. H. Lee, "Impacts of Punishment and Ethics Training of Information Security Compliance : Focus on the Moderating Role of Organizational Type," *Information System Review*, Vol.12, No.1, pp.23-42, Mar. 2010.

[18] H. K. Bang, *A Study on the Appropriateness of Information Security Manpower of Public Enterprises*, M.S. Theses, Korea University, Seoul, 2011.

저 자 소 개

김 태 희(Tae-Hee Kim)

정회원



- 1991년 2월 : 동신대학교 전자계산학과(공학사)
- 1993년 2월 : 전남대학교 전산통계학과(이학석사)
- 1999년 2월 : 전남대학교 전산통계학과(이학박사)
- 1998년 2월 ~ 현재 : 동신대학교 정보보안학과 교수
<관심분야> : 정보공학, 데이터베이스보안, 정보보안 윤리