情報保護學會論文誌
第20卷 第2號, 2010. 4

보안 인지 및 실천 현황 분석을 통한 대학 연구정보보안 수준 제고 방안

박 일 형,† 김 성 우, 서 승 우‡
서울대학교 전기·컴퓨터공학부

Improving Research Information Security in Academic Institutes through the Analysis of Security Awareness and Activities

Il-hyung Park,† Seong-woo Kim, Seung-woo Seo‡
School of Electrical Engineering and Computer Science, Seoul National University

요 약

대학은 국가적으로 연구개발비 및 연구인력 측면에서 큰 비중을 차지하고 있는 핵심연구기관임에도 불구하고 연구정보보안에 대한 투자가 소홀하여 연구정보 유출이 우려되고 있는 것이 현실이다. 이와 관련, 본 논문에서는 연구정보 유출을 예방하기 위한 노력의 일환으로 대학 구성원의 보안 인지수준과 실천수준을 분석하고 대학내 연구정보보안 수준 제고를 위한 구체적 방안을 제시한다. 이를 위해 먼저 대학 구성원을 대상으로 실시한 설문조사 결과를 분석하여 연구정보보안 및 보안의식에 관련된 현황을 파악한다. 이를 바탕으로 상관관계분석, 일원배치 분산분석, 다중회귀분석 등 통계분석을 실시하여 정보보안의식 및 보안실천수준, 전임교원 보안수준, 연구실 정보보안 관리절차와 같은 문제점들이 존재함을 보인다. 마지막으로 분석결과를 기반으로 교육·홍보를 통한 보안지식 및 의식 개선, 연구책임자 의무사항을 포함하는 연구실 보안관리 규정 제정, 정보유출방지·출입자 통제 솔루션 등의 보안수준 향상을 위한 대책들을 제시한다.

ABSTRACT

Universities are one of leading R&D institutes, however, their scarce security investment allows research information to leak outside. This paper proposes methods for improving security level of academic institutes to protect research information by analyzing security awareness and activities. To do that, we verified the current status of information security and awareness level by analyzing the survey which was conducted for a member of Seoul National University. As a result of statistical analysis using correlation, analysis of variance, multi regression and so on, we concluded that it is essential to improve security awareness, activities, professor's security level and management process for research labs. Thus, we suggest the following methods, security awareness and knowledge development through education, security management for research labs through provision, introduction of data protection softwares and physical control of visitors which are to be adopted to improve security level.

Keywords: Academic Security, Research Information Protection, Security Awareness, Security Level, Survey

I. 서 론

IT기술의 발전 및 정보화의 진전에 따라 정보를 저장하거나 공유하는 수단이 다양화·보편화되었다. 대용량의 파일 전송이 가능한 이메일이나 웹하드, P2P 사용이 일반화되었으며 최근에는 크기가 수센티미터에 불과한 USB 메모리 저장장치에 수십GB의 자료를 저장할 수 있는 제품이 시판되기도 하였다. 그러나 내부자료 유출에 민감한 국가기관이나 기업의 입장에서는 자료공유 수단이 다양화되는 현상이 결코 달갑지

접수일(2009년 9월 12일), 수정일(2009년 12월 21일), 게재확정일(2010년 1월 3일)
† 주저자, ihpark@cnslab.snu.ac.kr
‡ 교신저자, sseo@snu.ac.kr

않은 것이 사실이다. 내부직원이 중요한 자료를 손쉽게 외부로 유출할 수 있기 때문이다. 2008년 9월 GS 칼텍스 직원은 개인정보 판매를 목적으로 1,125만명의 고객정보를 DVD에 저장해 외부로 유출하기도 하였다[1].

첨단기술 역시 동일한 위험에 직면에 있다. 정보 소통이 용이해지면서 막대한 예산과 인력, 시간이 투입된 산업기술 역시 정보보안 대책이 부재할 경우 언제든지 외부로 유출될 가능성이 존재한다. 2008년 기준 5년 동안 해외유출 시도 중 적발된 산업기술의 경제적 가치를 환산하면 254조원에 달한다는 통계도 내부자료 유출의 위험성을 입증하고 있다[2].

이와 같이 국가, 기업을 막론하고 산업기술유출로 인한 피해가 막대하고 그 규모도 급증하는 추세이기 때문에 기술유출 방지를 위한 노력이 절실히 요구된다. 실제로 국내·외 대기업의 경우 관리적, 기술적, 물리적 보안관리 방안을 다양하게 활용하며 산업기술 유출 방지를 위한 투자를 아끼지 않고 있다.

반면, 대학은 국가연구개발비의 1/4이 투자되고 있고 석박사급 인력의 절반이상이 연구에 종사하고 있는 핵심연구기관임에도 불구하고 구성원의 연구정보보안 의식이 부재하고 아직까지 연구정보 보안관리체계가 확립되어 있지 않아 연구정보 유출이 우려되고 있는 것이 현실이다[3].

이와 관련, 본 논문은 대학 연구정보보안 수준을 향상시키기 위한 노력의 일환으로 실증적인 측면에서 당면 문제에 접근하였다. 첫째, 학내 구성원의 정보보안 의식 및 보안 실천수준을 파악하기 위해 서울대 교직원, 연구원, 대학원생 등 1,913명을 대상으로 설문조사를 실시하였다. 둘째, 통계분석을 통해 정보보안 전문성에 비해 연구정보보안 필요성에 대한 인식이 낮고 학내 구성원들이 인식하고 있는 연구정보보안 수준과 보안실천 수준 사이에 괴리가 존재한다는 사실을 확인하였다. 또한, 전임교원의 보안수준에 개선이 필요하며 연구실 연구정보 관리절차가 부재한 것으로 나타났다. 셋째, 대학이 직면하고 있는 연구정보보안 취약점을 개선하기 위해 관리적, 기술적, 물리적 분야로 세분화되는 개선방안을 제시하였다. 보안의식 및 보안지식 개선, 보안생활화를 위한 교육과 연구책임자의 의무사항을 포함하는 연구실 보안규정 제정, 보안 실천수준 및 연구정보보안 수준 향상을 위한 보안솔루션 도입과 CCTV·전자적 잠금장치 등 출입자 통제를 위한 투자가 필요하다.

본 논문의 순서는 다음과 같다. 2장에서는 설문 및 연구모형 구성을 위한 이론적 배경을 소개하고 3장에서는 연구정보보안 수준에 영향을 미치는 요인을 파악하기 위해 연구모형과 연구가설을 설정한다. 4장에서는 구성원의 정보보안 전문성, 연구정보보안 의식, 개인정보보안 실천수준, 연구정보보안 수준을 측정하기 위해 교직원, 연구원, 대학원생 등을 대상으로 설문조사를 시행한 후, 상관관계 분석, 일원배치 분산분석, 다중회귀분석 등을 통해 연구가설 검증 및 통계분석을 실시한다. 5장에서는 분석 결과가 함의하고 있는 개선필요사항과 그에 따른 연구정보보안 향상 방안을 제안하며 6장에서는 결론으로 시사점 및 향후 연구방향을 도출한다.

II. 이론적 배경

2.1 정보보안 전문성

보안지식 및 경험 등으로 대변되는 정보보안 전문성은 정보시스템 이용과 성과에 영향을 주는 정보보호와 관련된 지식의 정도로 정의할 수 있으며 정보보안 관련 배경지식이 풍부한 사람은 그렇지 않은 사람에 비해 더 높은 보안수준을 가질 수 있다[4]. 또한, 정기적인 훈련을 통해 조직 구성원의 정보보안 전문성을 향상시킬 수 있으며 이는 전반적인 정보보안 수준 개선에 기여한다[5]. Lee et al.[6]는 사용자 능력이 보안측면의 정보시스템 이용성과에 영향을 주는 중요한 요인이라고 하였다. 따라서, 정보보안 전문성은 연구정보보안 의식, 개인정보보안 실천수준에 긍정적인 영향을 미치며 궁극적으로 연구정보보안 수준 향상에 기여하는 주요 요소라고 할 수 있다.

2.2 연구정보보안 의식

Post & Kagan[4]은 컴퓨터 보안지식과 보안의식 수준은 다르다고 강조하고 있다. 즉, 보안지식과 보안의식을 같은 개념으로 생각할 수 없으며 보안지식 개선이 반드시 보안의식 향상으로 직결되는 것은 아니라는 것이다. Goodhue & Straub[7]는 사용자가 잠재적인 보안위험을 더 많이 인식하고 있을 경우 정보시스템 보안에 더 높은 관심을 나타낼 것이라고 하였다. ISACA[5]에서는 정보보안 관리의 핵심 요소로 보안인식 및 교육을 언급하고 있다. 조직의 정책 및 규정을 통해 보안이 차지하는 중요성에 대한 교육을 강조하며 보안 요구사항, 법적인 책임, 경영 통제

등을 포함한 교육과 그에 따른 의식 개선이 이루어져야 한다고 하였다. 임채호[8]는 정보보호인식 제고 프로그램을 통해 정보보호 수준 개선이 가능하다고 하였다. '08년 정보보호실태조사 결과에서는 인터넷 이용자의 98.2%가 정보보호에 대하여 중요하다고 인식하고 있으며 매우 중요하다고 응답한 비율도 59.9%로 정보화 역기능에 대한 두려움이 정보보호에 대한 실질적인 관심으로 나타나고 있다[9]. 그러므로 대학 구성원의 연구정보보안 의식은 연구정보보안 수준 및 연구정보 유출 예방과 밀접한 관련이 있다.

2.3 개인별 침해빈도

'08년 인터넷 이용자 및 기업의 침해사고로 인한 경제적 피해 발생률이 전년에 비해 크게 증가하였으며 이에 따른 정보화 역기능 대응활동 역시 함께 증가하고 있는 것으로 나타났다. '08년 인터넷 이용자의 백신 S/W 이용률은 '07년에 비해 15.2% 증가하여 침해사고 증가에 따른 정보보호 S/W 이용 증가 추세를 반영하고 있다. 방송통신위원회에서도 점증하고 있는 인터넷 침해사고에 대한 대응력 강화를 위해 정보보호 관련 제도 개선, 보안기술 개발·보급, 홍보활동 등이 요구된다고 강조하고 있다[9, 10]. 그러므로 개인이 보안위협 또는 침해에 노출되는 정도는 보안의식 제고에 긍정적인 영향을 미칠 수 있으며 이는 궁극적으로 보안수준 향상으로 이어질 것이다.

2.4 개인정보보안 실천수준

방송통신위원회 및 ISO[11, 12]는 정보보호시스템관리체계 평가 등급의 기준으로 비밀번호 관리, 보안시스템 운영, 매체 취급 및 보관, 악성 소프트웨어 통제, 장비의 안전한 폐기 및 재사용 등의 항목을 제시하고 있다. 또한, 한국정보화진흥원[13] 및 국가사이버안전센터[14]는 비밀번호 설정, 화면보호기 사용, 백신 S/W 활용, PC 개인방화벽 사용, 보안 업데이트, 보조기억매체 관리를 통해 개인 및 조직의 정보보안 수준을 개선할 수 있다고 하였다. 따라서 이러한 기준을 활용하여 개인정보보안 실천수준을 설명할 수 있다.

2.5 연구정보보안 수준

ISACA[5]는 정보보안 향상을 위해 번호조합 또는 카드키 잠금 장치, 출입용 신분증, CCTV 등의 물리적 시설 접근통제가 필요하다고 하였다. Harris[15]는 기업의 생존과 지속성을 위해 재난에 대비한 백업계획이 필수적으로 요구되며 비상계획에 자료 백업절차가 포함되어야 한다고 강조하였다. 또한, 조직의 정보보안 관리를 위해 보안 관리자가 필요하며 구성원에 대한 정기적·주기적 보안 교육과 논리적 접근통제를 위한 방화벽, 침입탐지시스템, 자료 암호화 기술, 바이러스 및 웜통제 소프트웨어 등이 구축되어야 한다고 하였다. 김종기[16] 역시 정보보안 수준 제고를 위해 정보보안 조직에 요구되는 새로운 보안대책을 기존 시스템에 설치하고, 보안대책을 효과적으로 운영하기 위해서 사용자와 관리자에 대한 보안교육이 실시되어야 한다고 하였다. 대학 연구실 역시 장기간에 걸쳐 축적된 연구자료가 재난, 분실, 도난 등으로 사라졌을 때 복구가 불가능하다면 크나큰 어려움에 직면할 것이며 보안 교육 및 보안 관리자 지정, 보안솔루션 등을 활용해 연구정보유출 위험을 감소시킬 수 있다.

III. 연구모형 및 연구가설

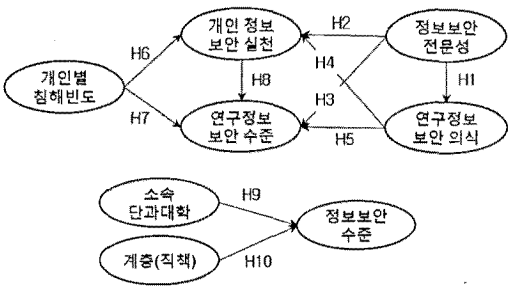
3.1 연구모형

본 연구에서는 정보보안 전문성, 연구정보보안 의식, 개인별 침해빈도, 개인정보보안 실천수준, 연구정보보안 수준 등의 상호 관계와 소속 단과대학 및 계층(직책) 등의 요소들이 정보보안 수준에 미치는 영향을 실증적으로 규명하고자 [그림 1]과 같이 연구모형을 설정하였다.

3.2 연구가설

3.2.1 정보보안 전문성과 연구정보보안 의식

연구가설1(H1)은 정보보안 전문성이 연구정보보안 의식에 영향을 미치는 인과관계에 대한 가설이다. 정보보안 전문성은 정보보안 S/W 제작능력, 전문기술 및 용어 이해, 상용 S/W 사용능력, 해킹사고시 대처능력 등을 의미한다. 구성원의 정보보안 전문지식이 높을수록 정보보안 위협의 심각성을 이해할 뿐만 아니라 해킹에 따른 연구정보 유출 위협에 대한 경각심을 갖고 있다고 할 수 있기 때문에 정보보안 전문성 향상이 연구정보보안 의식에 긍정적인 영향을 미칠 것이라는 가설을 도출하였다.



〔그림 1〕 연구모형

H1 : 정보보안 전문성은 연구정보보안 의식에 정(+)의 영향을 미칠 것이다.

3.2.2 정보보안 전문성과 개인정보보안 실천수준

연구가설2(H2)는 정보보안 전문성이 개인정보보안 실천수준에 영향을 미치는 인과관계에 대한 가설이다. 정보보호 S/W 사용능력, 해킹사고시 대처능력, 정보보안을 위한 필수 지식 등으로 구성되는 정보보안 전문성이 높을수록 비밀번호 설정, 보안 업데이트, 보안 프로그램 활용 등 개인 정보보안을 위한 노력이 증대될 것이라는 예상이 가능하다. 즉, 정보보안 전문성이 높은 사람은 조직의 정보보안 수준 유지를 위해 요구되는 보안기준에 대한 이해도가 높기 때문에 정보보안 실천수준 역시 높게 나타날 것이다. 따라서 정보보안 전문성의 향상은 개인정보보안 실천수준 향상에 긍정적인 영향을 미칠 것이라는 가설을 도출하였다.

H2 : 정보보안 전문성은 개인정보보안 실천수준에 정(+)의 영향을 미칠 것이다.

3.2.3 정보보안 전문성과 연구정보보안 수준

연구가설3(H3)은 정보보안 전문성과 연구정보보안 수준의 관계에 대한 가설이다. 연구 관리자 및 연구실 구성원의 정보보안 전문성 향상은 연구보안 개선 필요사항을 자각하게 하고 연구실 연구정보보안 수준 개선을 위한 투자를 유도한다. 보안 프로그램 활용 등 기술적 투자와 더불어 자체 보안관리 지침 시행, 보안관리자 지정, 연구정보 백업 관리 강조, 주기적인 보안교육 등의 관리적 투자는 전반적인 연구정보보안 수준 향상으로 직결된다. 따라서 정보보안 전문성은 연구정보보안 수준에 긍정적인 영향을 미친다는 가설을 도출하였다.

H3 : 정보보안 전문성은 연구정보보안 수준에 정(+)의 영향을 미칠 것이다.

3.2.4 연구정보보안 의식과 개인정보보안 실천수준

연구가설4(H4)는 연구정보보안 의식이 개인정보보안 실천수준에 영향을 미치는 인과관계에 대한 가설이다. 연구실 구성원이 소속 연구실에서 관리하고 있는 연구자료의 중요도를 높게 생각하고 연구자료는 반드시 임의로 외부에 유출되지 않도록 보호되어야 한다고 생각한다면 연구정보보안을 위해 보안 요구사항들을 수행하고자 하는 의지 역시 강해질 것이다. 즉, 비밀번호 설정, 화면보호기 설정, 보조기억매체 자료 보호대책, 보안패치 및 백신 S/W 활용, PC 개인 방화벽 사용 등 개인정보보안 실천수준 역시 향상될 것이라는 가설을 도출하였다.

H4 : 연구정보보안 의식은 개인정보보안 실천수준에 정(+)의 영향을 미칠 것이다.

3.2.5 연구정보보안 의식과 연구정보보안 수준

연구가설5(H5)는 연구정보보안 의식이 연구정보보안 수준에 영향을 미치는 인과관계에 대한 가설이다. 연구실 구성원이 소속 연구실에서 관리하고 있는 연구자료를 중요하게 생각하고 연구정보 보호를 위해 정보보안 관리를 위한 방안이 필요하다고 인식한다면 연구정보보안 향상을 위한 투자가 증가할 것이고 연구정보보안 수준이 향상될 것이라고 기대할 수 있다. 그러므로 연구정보보안 의식 수준은 연구정보보안 수준 향상에 긍정적인 영향을 미친다는 가설이 도출되었다.

H5 : 연구정보보안 의식은 연구정보보안 수준에 정(+)의 영향을 미칠 것이다.

3.2.6 개인별 침해빈도와 개인정보보안 실천수준

연구가설6(H6)은 해킹피해, 바이러스 감염, 개인정보 유출 등 개인이 경험한 침해빈도가 개인정보보안 실천수준에 영향을 미치는 인과관계에 대한 가설이다. 개인별로 해킹사고에 대한 노출빈도가 높을수록 이에 대한 경각심을 갖게 되고 해킹피해 예방을 위해 정보보안 요구사항에 대한 관심이 증가한다. 따라서 비밀번호 설정 및 변경, 보안 프로그램 활용, 보안업데이트 생활화 등 개인정보보안 실천수준이 향상될 것이므로 개인별 침해빈도가 개인정보보안 실천수준 향상에 긍정적인 영향을 미칠 것이라는 가설을 도출하였다.

H6 : 개인별 침해빈도는 개인정보보안 실천수준에 정(+)의 영향을 미칠 것이다.

3.2.7 개인별 침해빈도와 연구정보보안 수준

연구가설7(H7)은 해킹피해, 바이러스 감염, 개인 연구정보 유출 등 개인이 경험한 정보보안 침해빈도가 연구정보보안 수준에 영향을 미치는 인과관계에 대한 가설이다. 개인별 침해빈도가 높을수록 보안 경각심이 높아지며 따라서 침해 가능성을 예방하기 위해 연구정보 백업, 외부인 출입 통제, 연구자료 보안관리 방안 등 연구정보보안 수준에 대한 투자가 향상될 것이므로 개인별 침해빈도가 연구정보보안 수준 향상에 긍정적인 영향을 미칠 것이라는 가설을 도출하였다.

H7 : 개인별 침해빈도는 연구정보보안 수준에 정(+)의 영향을 미칠 것이다.

3.2.8 개인정보보안 실천수준과 연구정보보안 수준

연구가설8(H8)은 개인정보보안 실천수준과 연구실별로 수행되고 있는 연구정보보안 수준 간의 관계에 대한 가설이다. 비밀번호 설정, 보조기억매체 관리, 보안 업데이트 및 보안 S/W 활용 등 연구실원 개인의 평소 정보보안 실천수준이 높을수록 자연스럽게 연구실내에서의 연구정보보안 수준도 향상될 것이다. 개인정보보안 실천수준이 생활화되어 보안의식 및 보안수준이 높아진다면 연구실 보안 관리자 운영, 주기적인 보안교육, 정보보안 시스템 운영 등 연구정보보안 수준을 구성하는 요소에 긍정적인 영향을 미칠 것이라는 가설을 도출할 수 있다.

H8 : 개인정보보안 실천수준은 연구정보보안 수준에 정(+)의 영향을 미칠 것이다.

3.2.9 소속 단과대학과 정보보안 수준

연구가설9(H9)는 소속 단과대학(대학원)과 정보보안 수준과의 인과관계를 나타내는 가설이다. 동일한 대학내에서도 단과대학별로 환경 및 구성원 특성이 다르기 때문에 보안수준 역시 차이가 존재한다는 가정이 가능하다. 특히, 연구정보보안의 주요한 대상이 되는 이공계대학과 비이공계 대학의 보안수준을 비교하고 가설검증 결과를 바탕으로 단과대학에 따라 차별화된 정보보안 방안을 마련하는데 중요한 자료로 활용할 수 있을 것이다. 따라서 소속 단과대학별로 정보보안 수준에 차이가 있다는 가설을 도출하였다.

H9 : 소속 단과대학별로 정보보안 수준에 차이가 있을 것이다.

3.2.10 계층(직책)과 정보보안 수준

연구가설10(H10)은 대학 구성 계층과 정보보안 수준간의 인과관계를 설명하는 가설이다. 본 논문은 연구정보보안을 주제로 하고 있기 때문에 대학 구성원을 연구기능을 기준으로 교직원, 대학원생, 연구원, 직원으로 분류한다. 만약 4개의 계층이 차별화된 정보보안 수준을 보인다면 연구정보보안 향상 방안 역시 정보보안 수준이 낮은 계층에 집중되어야 할 것이다. 특히, 조직 관리자의 정보보안 수준이 매우 중요한데 연구관리를 책임지는 관리자의 정보보안 수준이 높아야 정보보안 향상을 위한 관리적, 기술적, 물리적 투자가 뒷받침될 수 있기 때문이다[15]. 따라서 구성원 계층별로 정보보안 수준의 관계를 파악하고 이에 상응하는 대책을 세우는 것이 매우 중요하므로 계층별로 정보보안 수준에 차이가 있다는 가설을 도출하였다.

H10 : 구성원 계층별로 정보보안 수준에 차이가 있을 것이다.

3.3 연구변수의 조작적 정의 및 측정항목

정보보안 전문성, 연구정보보안 의식, 개인별 침해빈도, 개인정보보안 실천수준 요인들로 연구정보보안 수준을 검정하기 위해 수립한 연구개념들을 [표 1]과 같이 정의하였다. 정보보안 전문성은 정보보안과 관련된 개인지식과 능력이라고 정의하였다. 정보보안 전문성을 측정하기 위한 변수로는 정보보안 기술 및 용어 이해, 보안 소프트웨어 사용 능력 등을 사용하였다. 연구정보보안 의식은 연구정보의 중요도, 연구정보보안 필요성에 대해 인지하는 수준이라고 정의하였으며 본인 및 본인의 연구실에서 보유하고 있는 연구정보의 중요도에 대한 평가와 해당 연구정보를 보호하기 위해 요구되는 보안수준 체감도를 측정변수로 하였다. 개인별 침해빈도는 웜바이러스 감염, 개인정보 유출 등의 해킹피해 경험정도라고 정의하였으며 응답자가 최근 3년 동안 경험한 해킹, 바이러스 감염, 연구정보 유출 등의 보안사고 횟수를 측정변수로 하였다. 개인정보보안 실천수준은 개인적인 차원에서 정보보안을 위해 실천하고 있는 기술적 보안관리 방안이라고 정의하였으며 측정변수로는 PC · 학내포털 · 인터넷 사용시 비밀

〔표 1〕 변수의 조작적 정의 및 측정항목

연구변수	조작적 정의	측정항목	관련문헌
정보보안 전문성 (KNW)	정보보안과 관련된 개인지식 및 능력	KNW1 정보보안 이해도	ISACA(2008) A. Kagan(2007) Lee et al.(1995)
연구정보보안 의식 (AWN)	연구정보의 중요도, 연구정보 보안 필요성에 대해 인지하는 수준	AWN1 연구정보 중요도와 보안 필요성에 대한 인식	A. Kagan(2007) Goodhue et al.(1991) 임채호(2006)
개인별 침해빈도 (HAC)	웜바이러스 감염, 개인정보 유출 등의 해킹피해 경험 정도	HAC1 해킹사고 경험횟수	방송통신위원회(2009)
개인정보보안 실천수준 (ACT)	개인적인 차원에서 정보보안을 위해 실천하고 있는 기술적 보안관리 방안	ACT1 비밀번호 변경주기 ACT2 화면보호기 설정 ACT3 PC 비밀번호 설정 ACT4 보조기억매체 자료 보호대책 ACT5 하드디스크 폐기 방법 ACT6 사용 중인 보안솔루션 ACT7 보안패치 및 백신S/W 활용도 ACT8 PC 개인 방화벽 사용	한국정보화진흥원(2003) 방송통신위원회(2008) NCSC(2008) ISO(2004)
연구정보보안 수준 (LAB)	연구실 소속원 및 연구실의 연구정보보안 수준	LAB1 연구정보 백업 LAB2 연구실 물리적 보안 LAB3 연구실 자료 유출방지 대책 LAB4 연구실 정보보안 수준 인지도	ISACA(2008) Harris(2005) 방송통신위원회(2008) 김종기(2008)

번호 변경 주기, PC 화면보호기 동작시간과 비밀번호 설정 여부, 부팅 비밀번호 및 윈도우 비밀번호 설정 여부, 비밀번호 설정시 문자·숫자·특수문자 조합 여부, 보안 기능이 있는 보조기억매체를 사용하거나 또는 보조기억매체 사용시 자료 암호화 저장 여부, 하드디스크 폐기시 물리적 파손·여러번 덮어쓰기 등 자료 완전소거 대책 시행 여부, 보안 프로그램 활용도, 보안패치 및 백신프로그램 업데이트 설정 상태, PC 개인방화벽 활용도 등을 측정변수로 하였다. 연구정보보안 수준은 연구실 소속원 및 연구실의 연구정보보안 수준으로 정의하였으며 중요 연구정보에 대한 백업 방법과 백업 주기, CCTV 운영 및 ID카드 또는 출입증 발급 등 연구실 외부인 출입통제 방안, 연구실 보안관리자 지정, 정기·수시 보안교육 여부, 본인이 보유하고 있는 연구정보를 보호하기 위해 현재 수행하고 있는 정보보안 수준 평가 등을 측정변수로 하였다.

IV. 실증분석

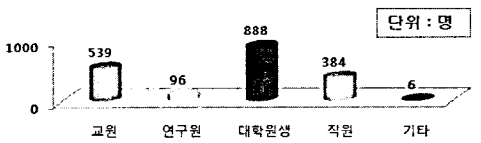
4.1 자료수집 및 분석

대학 구성원의 정보보안수준을 조사하기 위해 서울대학교 교직원, 연구원, 대학원생 1,913명을 대상으로 2009년 5월 11일부터 5월 25일까지 온라인 및 오프라인 설문조사를 실시하였다〔17〕. 온라인 설문의 경우, 서울대 인터넷 포털의 설문조사 시스템을 이용하여 교직원, 연구원, 대학원생 대상 26,723명에게 설문 메일을 발송하였으며 1,610명이 응답하였다. 오프라인 조사는 교원(조교 포함) 2,430명에게 설문지를 배포하여 303부를 회수하였고 온·오프라인 설문을 모두 종합하여 1,913명(응답률 6.5%)의 설문지가 분석에 사용되었다.

설문조사를 통해 수집된 자료는 SPSS 12.0을 이용하여 분석하였다. 인구통계변수를 파악하기 위해 빈도분석을 하였고, 신뢰도 검증을 통해 각 변수들에 대한 설문문항의 내적 일관성을 조사하였다. 또한, 개인정보보안 실천수준, 연구정보보안 수준 등 각 변수들의 구성개념 타당성을 검증하기 위해 요인분석을 하였다. 연구가설을 검증하기 위해 피어슨의 상관관계 분석, 크루스칼-왈리스 검정(Kruskal-Wallis Test) 및 일원배치 분산분석을 하였고 연구변수 및 측정항목과의 관계를 추가로 분석하기 위해 상관관계 분석 및 다중회귀분석을 실시하였다.

4.2 표본의 특성

계층별 설문 응답자 분포는 〔그림 2〕와 같다. 대학원생이 47%(888명)로 가장 많았으며 교원(전임, 비



〔그림 2〕 설문 응답자 분포

전임, 조교 포함) 28%(539명), 직원(자체직원 포함) 20%(384명) 순이었다. 대학별 응답률은 공과대 28%(544명), 자연대 13%(244명), 의과대 10%(195명), 농생대 6%(114명), 사범대 5%(88명), 인문대 4%(84명), 사회대 3%(63명) 순으로 상대적으로 이공계 대학의 응답률이 높았다. 연구정보보안의 대상이 되는 대부분의 연구가 이공계 대학 연구실에서 이루어지고 있음을 감안한다면, 위 응답률은 연구정보보안 실태 파악과 개선방안을 도출하는데 있어 모집단에 대한 표본이 적절하게 분포되어 있음을 보이고 있다.

4.3 설문결과 분석

4.3.1 설문구성

설문 응답자의 정보보안수준을 조사하기 위해 설문문항을 주제별로 분류하였다. 설문은 정보보안 전문성, 연구정보보안 의식, 개인별 침해빈도, 개인정보보안 실천수준, 연구정보보안 수준을 파악하기 위한 문항으로 구성된다. 측정항목은 총 15문항으로 정보보안 전문성 및 연구정보보안 의식 수준 관련 2문항, 개인별 침해빈도 관련 1문항, 개인정보보안 실천수준 관련 8문항, 연구자료 정보보안수준 관련 4문항으로 구성되어 있다. 복수응답이 가능한 문항을 제외하고 설문응답자가 각 문항별로 (1) 매우 높다, (2) 높다, (3) 보통, (4) 낮다, (5) 매우 낮다를 선택하는 5점척도 방식을 택하였다.

4.3.2 설문결과 요약

〔표 2〕는 설문응답 내용을 종합한 결과이다. 문항1 ~ 7, 9 ~ 15의 항목 1 ~ 5는 각각 매우 높다, 높다, 보통, 낮다, 매우 낮다를 의미하며 문항8은 복수응답을 허용하였다. 설문응답을 종합한 결과, 대학 구성원의 연구정보보안 필요성에 대한 인식은 낮은 반면, 정보보안 전문성 수준은 비교적 높은 것으로 나타났다. 대부분이 비밀번호를 한번 설정한 이후에는 주기적으로 변경하지 않는 경향이 뚜렷했다. 화면보호기를 설정하지 않는 경우도 1/3 가량 되었고 PC BIOS 비밀번호를 설정하지 않는 경우도 다수였다. 보조기억매체에 저장하는 자료를 암호화하거나 비밀번호를 설정하는 등 보조기억매체 분실시 연구정보 유출에 대비하기 위한 보안조치를 하는 경우도 드물었다. 하드디스크에 잔존하는 데이터를 완전히 소거하기 위한 대책 역시 미흡한 수준으로 보완대책이 미비할 경우 향후 연구정보 유출이 우려된다〔18, 19〕. 백신·방화벽 사용률은 타 보안솔루션에 비해 월등히 높은 수준이나 보안패치 수동 업데이트 수준이 19%로 비교적 높게 나타나 업데이트가 자동 적용되도록 하기 위한 방안이 요구된다. 연구정보 백업은 월1회 주기로 수동백업 하거나 전혀 백업하지 않는 경우가 많아 현실적으로 연구정보 백업이 이루어지지 않고 있음을 알 수 있다. 또한, 외부인 출입통제를 위한 물리적 보안이 적절하지 않은 것으로 나타났으며 연구실별 보안관리절차가 부재하여 관련 내용을 규정에 반영해 의무사항으로 적용하는 방안이 요구된다. 마지막으로, 응답자의 89%가 본인이 수행하는 연구정보보안 수준이 낮다고 평가한 점은 연구정보보안이 매우 미흡한 수준임을 나타낸다.

특기할 만한 사항으로 백신 S/W와 PC 개인방화벽 사용률은 높은 반면, 학내 정보보안센터에서 제공하고 있는 PMS(Patch Management System) 사용률은 낮은 것으로 확인되었는데 PC 개인방화벽은 사용률이 높은 백신 S/W 또는 윈도우에 포함되어 있어 높은 사용률을 보이고 있는 것으로 조사된 만큼, 보안 S/W 사용률 제고를 위해서는 홍보와 더불어 보안솔루션을 백신 S/W와 패키지 형식으로 함께 묶어 배포하는 방안이 요구된다.

4.4 측정도구의 신뢰성 및 타당성 검증

4.4.1 측정도구의 신뢰성 검증

측정도구의 신뢰성을 검증하기 위해 크론바흐 알파계수(Cronbach's α)를 사용하였다. 크론바흐 알파 검증은 동일한 개념을 묻는 문항들에 대한 내적일치도를 측정하는 방법으로 일반적으로 알파계수가 0.6이상이면 신뢰할만한 측정이라고 본다. 〔표 3〕은 개인정보보안 실천수준과 연구정보보안 수준 관련 변수들에 대한 크론바흐 알파 검증 결과이다. 개인정보보안 실천수준 관련 문항의 신뢰도 분석 결과 크론바흐 알파계수가 0.664로 나타나 신뢰할만한 수준으로 나타났

〔표 2〕 설문조사 결과

문항	설문내용	항 목	응답자수	백분율(%)	문항	설문내용	항 목	응답자수	백분율(%)
문항1	정보보안에 대한 이해 수준	1	29	2	문항9	보안패치 및 백신 S/W 활용도	1	980	51
		2	636	39			2	532	28
		3	578	36			3	202	11
		4	302	19			4	158	8
		5	65	4			5	41	2
문항2	연구정보 중요도와 보안 필요성에 대한 인식	1	327	17	문항10	PC 개인 방화벽 사용	1	222	14
		2	1054	56			2	566	35
		3	303	16			3	178	11
		4	134	7			4	476	30
		5	76	4			5	168	10
문항3	비밀번호 변경주기	1	10	0	문항11	해킹사고 경험횟수	1	892	47
		2	87	5			2	712	37
		3	248	13			3	241	12
		4	450	24			4	30	2
		5	1118	58			5	38	2
문항4	화면보호기 설정	1	535	33	문항12	연구정보 백업 여부	1	294	16
		2	155	10			2	65	3
		3	160	10			3	145	8
		4	56	3			4	777	41
		5	704	44			5	610	32
문항5	PC 비밀번호 설정	1	281	17	문항13	출입통제 등 연구실 물리적 보안	1	270	14
		2	398	25			2	393	21
		3	493	31			3	383	20
		4	87	5			4	272	14
		5	351	22			5	591	31
문항6	USB 등 보조기억 매체 자료 보호대책	1	64	3	문항14	연구실 내부자료 유출방지 대책	1	98	5
		2	70	4			2	165	9
		3	80	4			3	294	15
		4	253	13			4	471	25
		5	1446	76			5	881	46
문항7	하드디스크 폐기 방법	1	282	15	문항15	연구실 정보보안 수준 평가	1	19	1
		2	203	11			2	187	10
		3	745	39			3	768	40
		4	469	24			4	656	34
		5	213	11			5	279	15

문항	설문내용	항목	응답자수	백분율(%)
문항8	사용 중인 보안 소프트웨어	백신 S/W	1806	94
		개인용 방화벽 S/W	693	36
		자료 완전삭제 S/W	227	12
		개인용 침입방지 S/W	144	8
		보안패치관리 S/W	621	32
		안전한 운영체제 S/W	220	12
		자료암호화 S/W	106	6
		내부 문서유출방지 S/W	34	2
		기타	28	1

으며 연구정보보안 수준 관련 문항은 크론바흐 알파 계수가 0.579이나 표준화된 크론바흐 알파 계수가 0.614이므로 신뢰성이 보장되는 것으로 판단하였다.

4.4.2 측정도구의 타당성 검증

측정도구의 구성개념 타당성을 검증하기 위해 요인분석을 실시하였다. 하나의 특성을 측정하기 위해 여러 개의 측정항목을 사용했을 경우 이 항목들이 요인

〔표 3〕 크론바흐 알파 검증 결과

복합지표	크론바흐 알파계수	표준화된 크론바흐 알파계수	항목수
개인정보보안 실천수준	0.664	0.697	8
연구정보보안 수준	0.579	0.614	4

분석을 통해 동일한 요인으로 묶여진다면 그 측정도구가 타당하다고 볼 수 있다. 또한, 각 변수들에 대한 요인분석 가능여부를 검증하기 위해 KMO(Kiaser-Meyer-Olkin) 측도 및 바틀렛(Bartlett)의 구형성(Sphericity) 검정을 사용하였다. KMO 측도는 변수들 간의 상관성을 나타내는 측도인데 이 값이 0.6이상이면 요인분석의 변수로 적당하다고 할 수 있다. 또한 바틀렛의 구형성 검정은 변수들의 상관행렬이 단위행렬이라는 귀무가설을 검정하는데 p값이 유의수준에 포함되면 귀무가설을 기각하고 요인분석이 가능하다.

〔표 4〕 개인정보보안 실천수준 관련 변수들의 KMO 측도와 바틀렛의 구형성 검정 결과에서 KMO 측도가 0.752이고 구형성 검정 결과 p값이 0.000으로 상관행렬이 단위행렬이라는 귀무가설이 기각되기 때문에 요인분석이 가능함을 알 수 있다. 또한, 표본화 적합성 측도가 모두 0.68이상이므로 모든 변수를 포함시켜도 무방하며 주축요인추출법에 의한 공통성(communality)의 초기추정값과 최종추정값은 상호 큰 편차 없이 안정됨을 보이고 있어 최종적으로 개인정보보안 실천수준 관련 변수로 요인분석을 하는데 문제가 없다.

〔표 5〕는 개인정보보안 실천수준 관련 변수들을 이용한 요인분석 결과이다. 고유값이 1이상인 요인이 2개가 있으며 전체 변이의 31.104%를 설명하고 있다. 회전된 요인행렬에서 요인1, 2가 차례로 각 변수들과 높은 상관관계를 보이고 있음을 알 수 있다. 따라서 2개의 요인이 추출되었으므로 개인정보보안 실천수준 복합지수를 측정하기 위한 측정도구의 타당성이 검증되었다.

〔표 6〕은 연구정보보안 수준 관련 변수들의 KMO 측도와 바틀렛의 구형성 검정 결과이다. 여기서 KMO 측도가 0.672이고 구형성검정 결과 p값이 0.000으로 상관행렬이 단위행렬이라는 귀무가설이 기각되기 때문에 요인분석이 가능하다. 또한, 표본화 적합성 측도가 모두 0.63이상이므로 모든 변수를 포함

〔표 4〕 개인정보보안 실천수준 요인분석 가능여부 검정

복합지수	변수	KMO 측도	구형성 검정 p값	표본화 적합성 측도	공통성	
					초기	추출
개인정보보안 실천수준	ACT1	0.752	0.000	0.799	0.098	0.109
	ACT2			0.687	0.270	0.532
	ACT3			0.701	0.293	0.464
	ACT4			0.807	0.167	0.197
	ACT5			0.771	0.225	0.338
	ACT6			0.755	0.239	0.416
	ACT7			0.791	0.149	0.171
	ACT8			0.785	0.196	0.262

〔표 5〕 개인정보보안 실천수준 요인분석

요인	초기 고유값		회전 제곱합 적재값		회전된 요인행렬		
	전체	% 누적	전체	% 누적	변수 (문항)	요인	
						1	2
1	2.582	32.281	1.374	17.171	ACT1	0.282	0.171
2	1.117	46.246	1.115	31.104	ACT2	0.143	0.715
3	0.975	58.429			ACT3	0.229	0.642
4	0.886	69.506			ACT4	0.351	0.272
5	0.699	78.239			ACT5	0.565	0.135
6	0.675	86.674			ACT6	0.640	0.078
7	0.568	93.768			ACT7	0.367	0.191
8	0.499	100.00			ACT8	0.484	0.167

〔표 6〕 연구정보보안 수준 요인분석 가능여부 검정

복합지수	변수	KMO 측도	구형성 검정 p값	표본화 적합성 측도	공통성	
					초기	추출
연구정보보안 수준	LAB1	0.672	0.000	0.729	0.090	0.121
	LAB2			0.731	0.138	0.199
	LAB3			0.662	0.240	0.387
	LAB4			0.636	0.284	0.565

〔표 7〕 연구정보보안 수준 요인분석

요인	초기 고유값		추출 제곱합 적재값		적재된 요인행렬	
	전체	% 누적	전체	% 누적	변수 (문항)	요인
						1
1	1.881	47.032	1.271	31.785	LAB1	0.347
2	0.886	69.189			LAB2	0.446
3	0.703	86.753			LAB3	0.622
4	0.530	100.00			LAB4	0.751

시켜도 무방하며 주축요인추출법에 의한 공통성의 초기추정값과 최종추정값은 상호 큰 편차 없이 안정되어 있으므로 연구정보보안 수준 변수로 요인분석을 하는데 문제가 없다.

〔표 7〕은 연구정보보안 수준 관련 변수들을 이용한

요인분석 결과이다. 고유값이 1이상인 요인이 1개이며 전체 변이의 31.785%를 설명하고 있다. 따라서 여러개의 변수들이 한 개의 요인으로 묶여지므로 연구정보보안 수준 관련 측정도구의 타당성이 검증되었다.

4.5 연구가설 검증 및 분석

4.5.1 상관관계 분석

연구가설1(H1) ~ 연구가설8(H8)을 검증하기 위하여 피어슨의 상관관계 분석을 사용하였다. [표 8]은 연구변수의 평균 및 표준편차이고 [표 9]는 각 연구변수간의 상관관계 분석결과이다.

정보보안 전문성이 연구정보보안 의식에 미치는 영향을 평가하기 위한 가설1(H1)은 변수간의 상관계수가 0.181이고 유의수준 0.01에서 통계적으로 유의한 것으로 나타나 가설을 채택한다. 정보보안 전문성이 개인정보보안 실천수준에 영향을 미친다는 가설2(H2)는 상관계수가 0.373이고 유의수준 0.01에서 통계적으로 유의하여 가설을 채택한다. 정보보안 전문성이 연구정보보안 수준에 영향을 미친다는 가설3(H3)은 변수간의 상관계수가 0.201이고 유의수준 0.01에서 통계적으로 유의하여 가설을 채택한다. 연구정보보안 의식이 개인정보보안 실천수준에 영향을 미친다는 가설4(H4)는 상관계수가 0.238이고 유의수준 0.01에서 통계적으로 유의하여 가설을 채택한다. 연구정보보안 의식이 연구정보보안 수준에 영향을 미친다는 가설5(H5)는 상관계수가 0.285이고 유의수준 0.01에서 통계적으로 유의한 것으로 나타나 가설을 채택한다. 개인별 침해빈도의 개인정보보안 수준에 대한 영향을 평가하기 위한 가설6(H6)은 변수간의 상관계수가 0.068이고 유의수준 0.01에서 통계적으로 유의한 것으로 나타났으나 상관계수가 낮아 영향이 없는 것으로 본다. 개인별 침해빈도가 연구정보보안 수준에 미치는 영향을 평가하기 위한 가설7(H7)은 유의수준 0.01에서 유의하지 않은 것으로 나타나 기각한다. 개인정보보안 실천수준이 연구정보보안 수준에 미치는 영향을 평가하기 위해 설정한 가설8(H8)은 변수간의 상관계수가 비교적 높은 0.434이고 유의수준 0.01에서 통계적으로 유의한 것으로 나타나 가설을 채택한다.

4.5.2 집단간 평균 비교

이번에는 가설9(H9), 가설10(H10)을 검증하기 위해 각각 비모수적 검정방법인 크루스칼-왈리스 검정방법과 모수적 검정방법인 일원배치 분산분석을 이용하여 집단간 평균을 비교하였다. 집단간 평균 비교를 위한 사전작업으로 소속 단과대학별 설문 응답자수를 분석한 결과, 간호대, 미술대, 음악대 등의 표본수가 정규성(일반적으로 30 이상) 만족 기준을 충족하지 않아 소속 단과대학별 보안수준 비교를 위한 통계분석 방법으로 비모수적 검정방법인 크루스칼-왈리스 방법을 사용하였다. 또한, 정확한 검정으로 몬테 카를로(Monte Carlo) 검정(신뢰수준 99%, 표본수 10,000)을 사용하였다. 크루스칼-왈리스 검정 결과 [표 10], 근사 유의확률, 몬테 카를로 유의확률이 모두 유의수준 0.01에서 통계적으로 유의한 것으로 나타났다. 따라서 소속 단과대학별로 보안수준에 차이가 존재한다고 가정하는 가설9(H9)를 채택한다.

[표 11]은 크루스칼-왈리스 검정 결과 계산된 평균순위 값을 단과대학(대학원)별 보안수준 순위로 변환한 자료이다. 단과대학별 순위의 민감도를 고려하여 단과대학명은 표기하지 않고 단과대학 및 대학원으로만 분류하였다. 연구소의 정보보안수준이 모든 측면에서 가장 높았고 전체평균을 소속 대학별로 비교하면

[표 8] 연구변수간 평균, 표준편차 비교

구 분	평 균	표준편차
정보보안 전문성	2.84	0.89
연구정보보안 의식	2.26	0.96
개인정보보안 실천수준	2.91	0.63
연구정보보안 수준	3.62	0.82
전체 보안수준	2.91	0.56

[표 9] 변수간의 상관관계

연구변수	정보보안 전문성	연구정보 보안 의식	개인별 침해빈도	개인정보 보안 수준	연구정보 보안 수준
정보보안 전문성	1				
연구정보 보안의식	0.181** (0.000)	1			
개인별 침해빈도	0.019 (0.437)	-0.039 (0.088)	1		
개인정보 보안 수준	0.373** (0.000)	0.238** (0.000)	0.068** (0.003)	1	
연구정보 보안 수준	0.201** (0.000)	0.285** (0.000)	0.019 (0.396)	0.434** (0.000)	1

(** : 유의수준 0.01)

〔표 10〕 크루스칼-왈리스 검정 결과

구분	정보 보안 전문성	연구정보 보안 의식	개인정보 보안 실천수준	연구정보 보안수준	전체 보안 수준
카이제곱	62.75	65.24	76.59	147.46	114.52
자유도	22	22	22	22	22
근사 유의확률	0.000	0.000	0.000	0.000	0.000
Monte Carlo 유의확률	0.000	0.000	0.000	0.000	0.000

단과대1(이공계), 대학원1(이공계), 단과대2(이공계), 단과대3(이공계), 단과대4(이공계), 단과대5(이공계), 단과대6(이공계) 등의 순으로 높게 나타나고 있다. 전체평균을 낮은 순으로 비교하면 단과대16(비이공계), 대학원5(비이공계), 단과대15(비이공계), 단과대14(이공계), 단과대13(비이공계), 단과대12(비이공계) 등의 순으로 분포되어 있다. 따라서 전반적으로 이공계 대학의 정보보안수준은 높은 반면, 비이공계 대학의 정보보안수준은 하위권에 분포되어 있는 것으로 나타났다.

이번에는 일원배치 분산분석을 통해 구성원의 계층별 정보보안 수준에 차이가 있는지를 평가하기 위해 가설10(H10)을 검증한다. 〔그림 1〕에서 전임교원(539명), 연구원(96명), 대학원생(888명), 직원(384명) 모두 표본수가 30 이상이므로 정규성을 만족하는 것으로 간주한다. 레벤(Levene)의 등분산 검정 결과, 등분산이 가정되지 않는 것으로 나타나 등분산이 가정되지 않을 때 F통계량보다 선호되는 브라운-포시(Brown-Forsythe) 통계량을 이용하여 집단평균이 동일한지 검정하였고 연구변수별로 유의한 차이를 갖는 계층이 어느 것인가를 파악하기 위해 던넷(Dunnett)의 T3를 이용하여 다중비교를 하였다.

〔표 12〕 일원배치 분산분석 결과, p값이 유의수준 0.05 이하로 정보보안 전문성, 연구정보보안 의식, 개인정보보안 실천수준, 연구정보보안 수준, 전체 보안수준 등 모든 연구변수에서 계층간 평균차가 존재하는 것으로 나타났다. 따라서 연구가설10(H10)은 통계적으로 유의하므로 채택된다.

〔표 13〕 다중비교 결과는 유의수준 0.05에서 평균차가 존재하는 연구변수·계층을 나타내고 있다. 정보보안 전문성은 전임교원-직원, 연구원-직원, 대학원생-직원간 유의한 평균차가 존재하며 연구정보보안 의식은 대학원생-직원간 유의한 평균차가 존재한다. 또한,

〔표 11〕 소속별 보안수준 순위

소속	연구변수별 순위				
	전체 보안 수준	정보 보안 전문성	연구 정보 보안 의식	개인 정보 보안 실천수준	연구 정보 보안
연구소	1	5	2	1	1
단과대1*	2	3	6	6	4
대학원1*	3	17	1	17	7
단과대2*	4	4	4	5	9
단과대3*	5	19	10	7	2
단과대4*	6	14	5	8	5
단과대5*	7	7	3	4	11
단과대6*	8	10	7	10	6
대학원2*	9	2	11	2	20
대학원3*	10	1	21	3	14
대학원4*	11	15	13	12	8
단과대7*	12	11	12	13	12
단과대8**	13	18	17	11	3
단과대9**	14	9	19	9	17
단과대10**	15	16	8	19	16
단과대11**	16	6	18	14	15
단과대12**	17	13	16	18	19
단과대13**	18	12	20	16	18
단과대14*	19	22	9	22	13
단과대15**	20	8	15	21	22
대학원5**	21	20	22	15	10
단과대16**	22	21	14	20	21

(* : 이공계대학, ** : 비이공계 대학)

개인정보보안 실천수준은 전임교원-연구원, 전임교원-직원, 대학원생-직원간 유의한 평균차가 존재하고 연구정보보안 수준은 전임교원-연구원, 전임교원-직원, 연구원-대학원생, 대학원생-직원간 유의한 평균차가 존재한다. 마지막으로 전체 보안수준은 전임교원-연구원, 전임교원-대학원생간에 유의한 평균차가 존재하는 것으로 나타났다. 이를 해석하면 직원이 전임교원, 연구원, 대학원생보다 정보보안 전문성이 낮고 연구정보보안 의식 측면에서는 대학원생보다 낮은 것으로 나타났다. 반면에 전임교원은 연구원, 교원보다 개인정보보안 실천 수준이 낮고 연구정보보안 수준에 있어서는 연구원, 직원보다 낮은 것으로 나타났으며 전체 보안수준은 연구원, 대학원생보다 낮다. 추가적으로 응답평균을 기준으로 계층별 보안수준을 비교하였다〔표 14〕〔그림 3〕. 다중비교 결과와 동일하게 전반적으로 전임교원의 보안수준이 가장 낮고 다음으로 대학원생, 직원, 연구원순으로 나타났다.

4.5.3 검증결과 분석

연구변수 및 측정항목간 관계를 추가적으로 분석하

〔표 12〕 일원배치 분산분석 결과

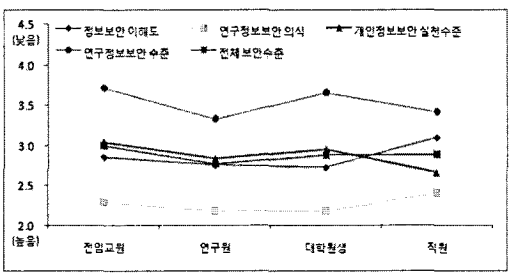
구 분	통계량(a)	자유도1	자유도2	p값
정보보안 전문성	12.615	4	96.663	0.000
연구정보보안 의식	4.647	4	244.817	0.001
개인정보보안 실천수준	24.514	4	99.279	0.000
연구정보보안 수준	12.404	4	187.407	0.000
전체 보안수준	6.389	4	292.765	0.000

〔표 13〕 다중비교 결과

종속변수	(I)계층	(J)계층	평균차 (I-J)	표준 오차	p값
정보보안 전문성	전임교원	직원	-0.240	0.071	0.008
	연구원	직원	-0.336	0.109	0.024
	대학원생	직원	-0.371	0.054	0.000
연구정보보안의식	대학원생	직원	-0.222	0.066	0.008
개인정보보안실천	전임교원	연구원	0.203	0.067	0.030
	전임교원	직원	0.376	0.043	0.000
	대학원생	직원	0.289	0.039	0.000
연구정보보안수준	전임교원	연구원	0.396	0.093	0.000
	전임교원	직원	0.299	0.059	0.000
	연구원	대학원생	-0.342	0.899	0.002
	대학원생	직원	0.244	0.054	0.000
전체 보안수준	전임교원	연구원	0.222	0.062	0.005
	전임교원	대학원생	0.115	0.030	0.001

〔표 14〕 계층별 보안수준 비교

계 층	정보보안 전문성	연구정보 보안 의식	개인정보 보안 수준	연구정보 보안 수준	전체 보안수준
전임교원	2.86	2.29	3.04	3.72	3.00
연구원	2.76	2.18	2.84	3.33	2.77
대학원생	2.73	2.18	2.95	3.66	2.88
직원	3.10	2.41	2.66	3.42	2.89



〔그림 3〕 계층별 보안수준 비교

기 위해 연구가설 검증결과를 종합하고 연구가설 검증결과를 바탕으로 상관관계 분석 및 다중회귀분석을 실시하였다.

〔표 15〕 연구가설 검증결과 요약

연구가설	상관계수	검증결과
〔H1〕 정보보안 전문성은 연구정보보안 의식에 정(+)의 영향을 미칠 것이다.	0.181	채택
〔H2〕 정보보안 전문성은 개인정보보안 실천수준에 정(+)의 영향을 미칠 것이다.	0.373	채택
〔H3〕 정보보안 전문성은 연구정보보안 수준에 정(+)의 영향을 미칠 것이다.	0.201	채택
〔H4〕 연구정보보안 의식은 개인정보보안 실천수준에 정(+)의 영향을 미칠 것이다.	0.238	채택
〔H5〕 연구정보보안 의식은 연구정보보안 수준에 정(+)의 영향을 미칠 것이다.	0.285	채택
〔H6〕 개인별 침해빈도는 개인정보보안 실천수준에 정(+)의 영향을 미칠 것이다.	0.068	불채택 (영향없음)
〔H7〕 개인별 침해빈도는 연구정보보안 수준에 정(+)의 영향을 미칠 것이다.		기각
〔H8〕 개인정보보안 실천수준은 연구정보보안 수준에 정(+)의 영향을 미칠 것이다.	0.434	채택
〔H9〕 소속 단과대학별로 정보보안 수준에 차이가 있을 것이다.	-	채택
〔H10〕 구성원 계층별 정보보안 수준에 차이가 있을 것이다.	-	채택

4.5.3.1 연구가설 검증결과

연구가설 검증결과는 〔표 15〕와 같다. 가설1(H1) ~ 가설5(H5), 가설8(H8) ~ 가설10(H10)은 채택되었으며 가설6(H6)은 통계적으로 유의하나 상관관계가 거의 존재하지 않는 것으로 나타났다. 가설7(H7)은 통계적으로 유의하지 않아 기각되었다. 따라서, 정보보안 전문성은 연구정보보안 의식, 개인정보보안 실천수준, 연구정보보안 수준에 정의 영향을 미치고 연구정보보안 의식은 개인정보보안 실천수준, 연구정보보안 수준에 정의 영향을 미친다는 사실을 확인하였다. 또한, 소속 단과대학 및 구성원 계층별로도 정보보안수준 차가 존재한다. 반면, 개인별 침해빈도는 정보보안 수준 향상과 관계가 없는 것으로 나타났다.

4.5.3.2 연구변수 및 측정항목 상관관계 분석

학내 구성원의 연구정보보안 향상을 위한 구체적 문제점을 분석하고 개선방안을 마련하기 위해 정보보안 전문성(KNW), 연구정보보안 의식(AWN), 그리고 개인정보보안 실천수준의 기준이 되는 측정항목(ACT1 ~ ACT8)과 연구정보보안 수준의 기준이 되는 측정항목(LAB1 ~ LAB4)의 상관관계를 분석하였다[표 16]. 연구정보보안 수준 인지도 또는 연구정보보안 수준 평가(LAB4)와 개인정보보안 실천수준의 상관계수는 0.2 ~ 0.3 사이로 유의미한 상관관계가 있는 것으로 나타났다. 그러나 높은 수준의 상관관계가 있는 것은 아니어서 보안 인지수준과 보안 실천수준 사이에 괴리가 존재한다는 분석이 가능하다.

이번에는 정보보안 전문성과 개인정보보안 실천수준을 비교하기 위해 상관계수를 분석하였다. [표 17]에서 비밀번호 변경주기, 화면보호기 설정, 보조기억매체 자료 보호대책, 중요연구정보 백업주기는 정보보안 전문성과 상관관계가 매우 낮고 PC 비밀번호 설정, 개인 PC 방화벽 사용은 유의수준 0.01에서 기각되어 정보보안 전문성과 관련성이 없는 것으로 나타났다. 그리고 하드디스크 폐기방법, 보안패치 및 백신 업데이트는 상관계수가 각각 0.289, 0.311로 정보보안 전문성과 상관관계가 있는 것으로 분석되었다. 따라서 하드디스크 폐기방법, 보안패치 및 백신 업데이트 수준 향상을 위해서는 정보보안 지식 향상을 위한 보안기술 교육이 요구되고 기타 실천 수준 항목은 정보보안 생활화를 위한 보안인식 교육이 필요한 것으로 풀이된다.

[표 18]은 연구정보보안 의식과 연구정보보안 수준 사이의 상관계수를 구한 결과이다. 각 문항별 상관계수는 0.1 ~ 0.2 사이로 높은 상관관계가 존재하는 것은 아니지만 낮은 수준이나마 연구정보보안 의식이 높을수록 연구정보보안 실천수준에 긍정적인 영향을 미친다고 볼 수 있다. 연구정보 백업 여부, 연구실 물리적 보안은 개인차원의 보안실천보다는 대학 차원의 보안 솔루션 도입과 투자에 영향을 많이 받기 때문에 상관계수가 낮은 것으로 분석된다. 또한, 연구정보보안 의식과 연구정보보안 수준 평가의 상관계수는 0.250으로 비교문항 중 가장 높은 수치를 보이고 있다. 그러므로 연구정보보안 중요도와 보안 필요성에 대한 인식이 개선될수록 연구정보보안 수준이 개선되는 경향도 큰 것을 알 수 있다.

[표 19]는 정보보안 전문성과 연구정보보안 수준의 상관계수 분석결과이다. 정보보안 전문성과 연구정보보안 의식, 연구정보 백업 여부, 물리적 보안, 내부자료 유출방지 대책의 상관계수는 낮게 나타났고 정보보안 전문성과 본인 연구정보보안 수준 평가 사이의 상관계수는 0.265로 좀 더 의미 있는 것으로 나타났다. 그러므로, 정보보안 전문성 개선은 개인의 연구정보보

[표 16] 연구정보보안 수준 평가와 개인정보보안 실천수준의 상관계수

기 준 / 실천수준	연구정보보안 수준평가	p값
비밀번호 변경주기	0.236	0.000
화면보호기 설정	0.289	0.000
PC 비밀번호 설정	0.314	0.000
보조기억매체 자료 보호대책	0.321	0.000
하드디스크 폐기방법	0.295	0.000
보안패치 및 백신 업데이트	0.226	0.000
개인 PC 방화벽 사용	0.303	0.000
중요 연구정보 백업주기	0.287	0.000

(유의수준 : 0.01)

[표 17] 정보보안 전문성과 개인정보보안 실천수준의 상관계수

기 준 / 실천수준	정보보안 전문성	p값
비밀번호 변경주기	0.174	0.000
화면보호기 설정	0.169	0.000
PC 비밀번호 설정	0.174	0.129
보조기억매체 자료 보호대책	0.128	0.000
하드디스크 폐기방법	0.289	0.000
보안패치 및 백신 업데이트	0.311	0.000
개인 PC 방화벽 사용	0.270	0.233
중요 연구정보 백업주기	0.122	0.000

(유의수준 : 0.01)

[표 18] 연구정보보안 의식과 연구정보보안 수준의 상관계수

기 준 / 실천수준	연구정보 보안 의식	p값
연구정보 백업 여부	0.164	0.000
연구실 물리적 보안	0.169	0.000
연구실 내부자료 유출 방지 대책	0.207	0.000
연구정보보안 수준 평가	0.250	0.000

(유의수준 : 0.01)

[표 19] 정보보안 전문성과 연구정보보안 수준의 상관계수

기 준 / 실천수준	정보보안 전문성	p-value
연구정보보안 의식	0.181	0.000
연구정보 백업 여부	0.122	0.000
출입통제 등 연구실 물리적 보안	0.089	0.000
연구실 내부자료 유출방지 대책	0.114	0.000
연구정보보안 수준 평가	0.265	0.000

(유의수준 : 0.01)

안 수준 향상에 영향을 미친다고 분석된다. 정보보안 전문성과 연구정보보안 의식은 낮은 상관관계가 존재하므로 전문성이 높다고 해서 연구정보보안 의식도 비례하여 향상되는 것은 아님을 알 수 있다. 특히, [표 2] 문항1에서 응답자의 89%가 본인의 정보보안 전문성이 보통 이상이라고 평가하였음을 감안하면 정보보안 전문성에 비해 정보보안의식 수준이 낮은 상태로 분석된다. 따라서 전문지식 이외에 보안의식 자체를 향상시킬 수 있는 방안이 필요하다고 할 수 있다. 연구정보 백업, 물리적 보안, 내부자료 유출방지대책 분야에서 상관관계가 낮은 것으로 나타났는데 이는 개인의 정보보안 전문성 향상이 이들 요인의 보안수준 개선에 큰 영향이 없음을 의미한다.

4.5.3.3 연구변수 및 측정항목 다중회귀분석

각 연구변수 및 측정항목이 연구정보보안 수준에 미치는 상대적인 영향을 파악하기 위해 정보보안 전문성, 연구정보보안 의식, 개인정보보안 실천수준을 독립변수로 하고 연구정보보안 수준을 종속변수로 하여 다중회귀분석을 실시하였다. [표 20]은 단계선택(stepwise) 방법을 이용한 다중회귀분석 결과이다. 분산분석에서 모든 모형이 0.000의 유의확률을 가지기 때문에 데이터에 적합하다고 할 수 있으며 2가지의 회귀모형(모형1, 모형2)이 제시되었다. 정보보안 전문성은 회귀식에 진입하지 못하여 정보보안 전문성이 연구정보보안 수준에 영향을 미치지 못하고 있음을 알 수 있다. 이러한 결과는 4.5.3.2 연구변수 및 측정항목 상관관계 분석에서 정보보안 전문성과 연구정보보안 수준의 상관계수 분석 결과와 일치한다. 이에 대한 해석으로는 정보보안 전문성 향상이 연구정보보안 수준 향상에 미치는 영향 자체가 없다기보다는 전문성이 있다 하더라도 연구정보보안 수준 향상을 위한 보안요구사항들을 실천하지 않고 있다고 해석해야 옳을 것이다.

다음으로 개인정보보안 실천수준 측정항목(ACT1 ~ ACT8)을 독립변수로 하고 연구정보보안 수준을 종속변수로 하여 회귀분석을 실시하였다[표 21]. 분산분석에서 모든 모형이 0.000의 유의확률을 가지므로 데이터에 적합하다. 회귀모형에서 ACT6(사용 중인 보안솔루션)은 탈락하였고 7개의 모형이 선택되었다. 모형1 ~ 7까지 R^2 값이 낮은 수준이기는 하나 모형을 가장 잘 설명하는 순으로 측정항목을 나열하면 ACT4(보조기억매체 자료 보호대책), ACT8(PC 개인 방화벽 사용), ACT2(화면보호기 설정), ACT5

[표 20] 연구정보보안 수준 회귀분석 결과1

모형		계수			분산분석		R^2
		비표준화 (표준화)	t	p값	F	p값	
1	(상수)	1.911	22.270	0.000	398.975	0.000	0.199
	개인정보 보안 수준	0.577 (0.446)	19.974	0.000			
2	(상수)	1.714	19.716	0.000	245.664	0.000	0.234
	개인정보 보안 수준	0.515 (0.398)	17.688	0.000			
	연구정보 보안 의식	0.166 (0.194)	8.614	0.000			

[표 21] 연구정보보안 수준 회귀분석 결과2

모형		계수			분산분석		R^2
		비표준화	t	p값	F	p값	
1	(상수)	2.342	26.381	0.000	205.484	0.000	0.113
	ACT4	0.275	14.335	0.000			
2	(상수)	2.090	22.984	0.000	149.153	0.000	0.157
	ACT4	0.242	12.700	0.000			
	ACT8	0.139	9.078	0.000			
3	(상수)	2.023	22.418	0.000	117.490	0.000	0.180
	ACT4	0.216	11.205	0.000			
	ACT8	0.123	8.068	0.000			
	ACT2	0.074	6.770	0.000			
4	(상수)	1.901	20.697	0.000	98.050	0.000	0.196
	ACT4	0.192	9.823	0.000			
	ACT8	0.108	6.984	0.000			
	ACT2	0.069	6.299	0.000			
	ACT5	0.097	5.723	0.000			
5	(상수)	1.853	20.055	0.000	81.850	0.000	0.203
	ACT4	0.193	9.954	0.000			
	ACT8	0.093	5.918	0.000			
	ACT2	0.063	5.782	0.000			
	ACT5	0.086	5.055	0.000			
	ACT7	0.071	3.728	0.000			
6	(상수)	1.613	14.259	0.000	70.950	0.000	0.210
	ACT4	0.183	9.333	0.000			
	ACT8	0.085	5.332	0.000			
	ACT2	0.060	5.455	0.000			
	ACT5	0.082	4.791	0.000			
	ACT7	0.070	3.713	0.000			
	ACT1	0.078	3.648	0.000			
7	(상수)	1.592	14.078	0.000	62.521	0.000	0.215
	ACT4	0.174	8.821	0.000			
	ACT8	0.082	5.178	0.000			
	ACT2	0.044	3.616	0.000			
	ACT5	0.077	4.512	0.000			
	ACT7	0.064	3.386	0.000			
	ACT1	0.078	3.657	0.000			
	ACT3	0.050	3.106	0.000			

(하드디스크 폐기방법) 등의 순이다. ACT7(보안패치 및 백신 S/W 활용도), ACT1(비밀번호 변경주기), ACT3(PC 비밀번호 설정)는 회귀식에 진입하였으나 모형을 설명하는데 있어 기여도가 매우 낮다. 그러므로 연구정보보안 수준은 보조기억매체 자료 보호대책, PC 개인방화벽 사용, 화면보호기 설정과 더 큰 인과관계가 있다고 할 수 있다. 특히, 보조기억매체를 통한 연구자료 외부 유출을 예방하는 것이 연구정보보안 향상에 대한 상대적 기여도가 높은 것으로 분석되었다.

V. 연구정보보안 향상 방안

5장에서는 4장 설문결과 및 연구가설 검증·분석 결과를 바탕으로 도출된 문제점에 대한 관리적, 기술적, 물리적 측면의 연구정보보안 향상 방안을 제안한다[표 22].

5.1 연구정보보안 의식과 관리적 방안

설문 및 상관관계·다중회귀분석 결과, 정보보안 전문성에 비해 연구정보보안 의식이 낮은 것으로 나타나 정보보안 전문성 향상을 위한 보안지식 교육과는 별개로 보안의식 개선을 위한 방안이 요구된다. 또한, 설문 응답자의 89%는 소속 연구실 및 본인의 연구정보가 중요하다고 평가하면서도 73%는 기본적인 보안관리만 필요하거나 보안관리가 전혀 필요 없다는 상반된 반응을 나타냈다. 그러므로 연구정보를 보호하기

[표 22] 연구정보보안 향상 방안

문제점	개선방안			
	관리적 방안		기술적 방안	물리적 방안
	교육	규정		
정보보안 전문성 대비 연구정보보안 의식 수준 낮음	보안의식 개선 - 연구정보보안 필요성 - 정보보안 인식제고 프로그램			
인지수준 대비 보안실천 수준 낮음	정보보안 생활화 교육 - 비밀번호 설정 - 비밀번호 주기적 변경 - 화면보호기 설정 - 보안패치 - 백신업데이트 - 연구정보 백업 보안지식 개선 - 하드디스크 폐기 - 보조기억매체 자료보호	연구실 보안규정 - 정보보안 책임과 위반시 처벌 규정 - 대학 보안부서 차원의 연구실 보안감사, 보안점검	보안솔루션 도입 - 하드디스크 폐기 - 보조기억매체 자료보호 - 연구정보 백업 - 보안 USB - 보안S/W 패키지화 - 보안S/W 자동 설치	물리적 보안 강화 - CCTV, 전자적 잠금장치 등 출입자 통제 장치 설치
전임교원의 보안수준 낮음	전임교원 교육 프로그램 - 역할과 책임 - 연구정보 관리 - 연구원 관리	연구책임자의 의무사항 - 연구실 및 연구원 관리 책임		
연구실 연구정보 관리절차 부재함	전임교원 교육 - 책임 및 의무 - 연구정보 관리절차 보안관리자 교육 - 책임 및 의무 - 연구정보 관리절차	연구실 보안규정과 보안가이드라인 - 보안관리자 지정 - 연구정보 관리 - 출입자 통제 - PC관리 - 보조기억매체 관리 - 이메일·메신저 관리 - 연구정보 백업 - 퇴직자 관리 - 인쇄물 관리	연구실 보안솔루션 - 문서유출방지체계 중심의 보안솔루션 구축 - 문서파쇄기 활용	

위해 보안은 언제나 필수불가결하다는 인식을 제고시킬 필요가 있으며 이를 위해 보안대책 부재로 인한 연구정보 유출 위험을 강조하고 연구정보보안의 필요성을 지각할 수 있도록 정보보안 인식제고 프로그램을 시행하는 방안이 요구된다.

5.2 보안실천수준 개선과 관리적·기술적·물리적 방안

응답자의 정보보안 인지수준과 보안 실천수준 사이에 괴리가 발견되었다. 즉, 응답자가 인지하는 연구정보보안 수준은 상대적으로 높은 반면, 연구정보보안 실천수준은 낮은 것으로 분석되었다. 보안 실천 수준을 향상시키기 위해 관리적, 기술적, 물리적 방안이 요구되며 관리적 방안으로는 첫째, 정보보안을 생활화·습관화하여 보안 실천수준을 개선해야 한다. 비밀번호 설정 및 주기적 변경, 화면보호기 설정 등은 대부분의 응답자가 해야 한다는 사실을 알고 있으면서도 하지 않는 사항이므로 정기·수시 보안교육, 전자메일 홍보, 보안 포스터 등 반복 교육을 통해 습관화되도록 해야 한다. 이외에도 관련 전문지식이 부족해서 실천하지 않는 경우를 고려할 수 있다. 하드디스크 폐기, 보조기억매체 자료보호 미흡 등이 대표적인 경우인데 이러한 경우는 잔존데이터를 완전히 삭제하지 않을 경우 하드디스크에 저장되어 있는 자료가 유출되거나 보조기억매체 자료보호대책이 부재하여 발생하는 위험을 이해하고 자발적인 실천을 유도하기 위해 보안기술 교육에 주력해야 한다. 다음으로 연구실 보안규정을 정비해야 한다. 연구정보보안 실천수준이 낮은 이유는 강제하는 규정 또는 지침이 없기 때문이기도 하다. 정보보안 책임, 위반시 처벌 규정을 구체화하고 보안규정이 조기에 정착될 수 있도록 필요시 대학차원에서 보안감사나 보안지도를 시행한다면 실천수준이 향상될 것이다.

기술적 방안 역시 연구정보보안 향상을 위해 필수적인 사항이다. 하드디스크 폐기, 보조기억매체 자료보호 대책, 보안 업데이트, 연구정보 백업 등은 교육을 통해서도 효과가 있으나 자기소거 장치, 보안 USB, PMS, 백업솔루션 등 보안솔루션을 연구실에 지원하면 더욱 효과적이다. 연구정보백업에 대한 설문문항에서 연구정보를 백업한다는 응답자 68% 중 수동 백업하는 경우가 52%로 조사되었는데 자동화된 백업솔루션이 지원된다면 실천수준이 큰 폭으로 향상될 것이다. 보조기억매체 자료보호 대책에 관한 질문에서 보안 USB 사용률이 7% 밖에 되지 않았는데 보안담당부서에서 보안 USB 사용을 확대하는 정책을 시행한다면 보조기억매체 자료보호 수준 향상이 가능하다. 또한, 백신 S/W나 윈도우처럼 사용률이 높은 S/W에 함께 포함되어 있는 PC 개인방화벽의 사용률이 높았는데 백신 S/W에 보안 프로그램을 패키지화해서 제공하거나 백신 S/W 설치 또는 대학 인터넷 포털 접속시 필수 보안 S/W가 PC에 자동으로 설치되도록 한다면 사용률을 높일 수 있다.

이외에도 물리적 보안 분야 역시 개선이 필요한 분야로 나타났음은 주지의 사실이다. 특히, 외부인 출입이 빈번한 대학시설은 물리적 보안 강화가 반드시 필요하므로 연구실·연구소 출입통제를 위한 전자적 출입통제장치와 CCTV 설치·운영에 관심을 갖고 투자해야 한다.

5.3 전임교원의 보안수준 개선과 관리적 방안

직원, 연구원, 대학원생에 비해 전임교원의 보안수준이 낮은 것으로 나타났다. 대학 연구정보를 관리하는 최종 책임자인 전임교원의 보안수준이 가장 낮은 것은 매우 심각한 문제이다. 연구실, 연구소 등의 전반적인 관리자 역할을 수행하고 있는 전임교원의 보안수준이 낮다면 연구원, 대학원생, 직원 등의 보안 수준 역시 적절히 관리되지 않을 수 있기 때문이다. 전임교원을 대상으로 하는 별도의 보안교육 프로그램이 요구되는데 특히, 연구실 정보보안업무, 연구정보 및 연구원 관리 등에 대한 역할과 책임 등의 보안교육이 수반되어야 하며 이와 더불어 연구책임자의 의무사항이 규정에 반영되어 강제성이 부과되어야 한다.

5.4 연구실 연구정보관리절차 개선과 관리적·기술적 방안

대학 정보보안의 주 대상이 되는 연구실 다수가 연구정보 관리절차가 부재한 것이 가장 큰 문제였다. 연구실 연구정보 관리에 관한 규정이 부재하기 때문에 그 어떠한 통제도 없이 연구원 개별적으로 연구정보를 관리하고 있어 임의로 자료 유출이 가능한 것으로 조사되었다. 89%가 본인의 연구정보보안 수준이 보통 이하이고 71%가 연구실에 보안담당자가 없으며 연구원에 대한 주기적인 보안교육이 없다고 응답하였다. 그러므로 보안담당자 지정, 연구정보 관리, 출입자 통제, PC·보조기억매체 관리, 이메일·메신저 관리, 연구정보 백업, 퇴직자 관리, 인쇄물 관리 등에 대한

사항을 연구정보 관리규정에 반영하고 연구실에 공통으로 적용할 수 있는 보안가이드라인을 제시해야 한다. 또한, 연구실의 최종책임자인 전임교원과 연구실 보안관리자를 대상으로 연구정보보안 책임 및 의무, 연구정보 보안관리 절차를 교육하여 연구실 보안규정, 보안가이드라인을 준수하도록 유도해야 한다. 마지막으로 대학 차원에서 연구실 내부자료 유출을 통제할 수 있는 보안솔루션 도입이 검토되어야할 것이다.

VI. 결 론

대학은 과학기술 연구의 핵심기관으로 연구정보보안을 위한 체계적인 노력이 요구되나 정보보안측면에서 적지 않은 문제점이 발견되어 보안수준 향상을 위한 투자가 시급히 요구되는 것으로 나타났다. 특히, 연구실 보안관리절차가 부재하고 전임교원의 보안수준이 낮다는 점은 대학이 국가 연구개발을 이끌어가는 전초기지이면서도 연구정보보안 투자에는 얼마나 무관심한가를 여실히 보여주고 있다. 이제부터라도 대학 차원에서 연구정보보안의 중요성을 인식하고 연구정보보안 향상을 위한 투자에 집중해야 할 때다.

다만, 본 연구는 특정 대학교의 구성원을 대상으로 설문조사가 이루어졌기 때문에 타 대학과는 조사결과에 있어 일정부분 차이가 발생할 수 있다. 따라서 연구결과를 전체 대학으로 일반화하는데 다소 무리가 있을 수 있으나 타 대학의 경우에도 대학 연구정보보안 정책을 수립하는데 있어 본 연구결과를 참고한다면 많은 도움이 되리라 생각한다. 또한, 본 논문에서는 단과 대학별 연구정보보안 수준을 비교하고 순위를 평가하여 이공계 대학에 비해 비이공계 대학의 연구정보보안 수준이 낮다는 결론을 도출하였으나 각 대학별·구성원별로 세분화된 연구정보보안 실태분석이 이루어지지는 않았다. 따라서 향후 연구과제로 각 대학별 구성원의 보안수준을 분석하고 해당 대학의 실정에 맞는 맞춤형 보안지원 방안에 대한 연구가 필요할 것이다. 추가로, 본 논문에서 제시한 연구정보보안 향상 방안을 적용한 후 대학 구성원의 보안의식 및 보안 실천수준을 재분석하여 보안수준 개선 추이를 파악하거나 타 종합대학과도 연계하여 대학별 정보보안 수준을 상호 비교할 수 있도록 설문조사 결과를 지수화하고 공통 설문조사를 시행한다면 보다 일반화된 연구결과를 얻을 수 있을 것이다.

참 고 문 헌

[1] 연합뉴스, "1천만명 정보유출 돈노린 내부자 소행," 2008년 9월.

[2] 연합뉴스, "〈연합시론〉 기술유출 범국가적 대응 필요하다," 2008년 8월.

[3] 국가정보원, "대학산업기술보호 매뉴얼," 2007년 8월.

[4] G.V. Post and A. Kagan, "Evaluating information security tradeoff: restricting access can interfere with user tasks," Computers & Security, vol. 26, no. 3, pp. 229-237, May 2007.

[5] ISACA, "CISA review manual," Dec. 2008.

[6] S.M. Lee and Y.R. Kim, "An empirical study of the relationships among end-user information systems acceptance, training, and effectiveness," Journal of Management Information Systems, vol. 12, no. 2, pp. 189-202, Jan. 1995.

[7] D.L. Goodhue and D.W. Straub, "Security concerns of system users: a study of perception of the adequacy of security," Information & Management, vol. 20, no. 1, pp. 13-27, Jan. 1991.

[8] 임채호, "효과적인 정보보호인식제고 방안," 정보보호학회지, 16(2), pp. 30-36, 2006년 4월.

[9] 방송통신위원회, "2008년 정보보호 실태조사 결과," 2009년 2월.

[10] 국가정보원, "2009 국가정보보호 백서," 2009년 4월.

[11] 방송통신위원회, "방송통신위원회고시 제2008-11호 정보보호관리체계 인증 등에 관한 고시," 2008년 5월.

[12] ISO, "ISO/IEC 13335-1:2004," 2004.

[13] 한국정보화진흥원, "정보보호 가이드북," 2003년 4월.

[14] 국가사이버안전센터, "정보보호생활수칙," 2008년.

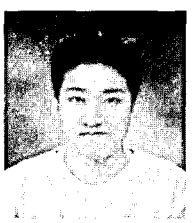
[15] S. Harris, CISSP certification all-in-one exam guide, McGraw-Hill Osborne Media, Nov. 2007.

[16] 김종기, 강다연, "패스워드의 정보시스템 보안효과에 영향을 미치는 요인에 관한 연구," 경영정보학연구, 18(4), pp. 1-26, 2008년 12월.

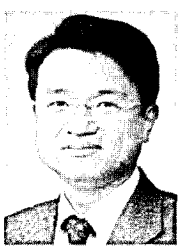
[17] 서울대학교 중앙전산원, "서울대학교 정보보안 현황 및 대책에 관한 연구," pp. 102-139, 2009년 6월.
[18] P. Gutmann, "Secure deletion of data from magnetic and solid-state memory," 6th USENIX Security Symposium, pp. 77-90, July 1996.
[19] S. Garfinkel and A. Shelat, "Remembrance of data passed: a study of disk sanitization practices," IEEE Security & Privacy, pp. 17-27, Feb. 2003.
[20] 서의훈, SPSS 12.0 한글판을 이용한 SPSS 통계분석, 자유아카데미, 2005년 9월.
[21] 최현철, 사회통계방법론(SPSS/PC WINDOWS 12.0), 나남, 2007년 7월.

〈著者紹介〉

박 일 형 (Il-hyung Park) 학생회원
2001년 3월: 공군사관학교 전산과학과 졸업
2009년 3월~현재: 서울대학교 전기·컴퓨터공학부 석사과정
〈관심분야〉 정보보호기술, 컴퓨터·네트워크 보안



김 성 우 (Seong-woo Kim) 학생회원
2005년 8월: 고려대학교 전자공학과 졸업
2007년 8월: 고려대학교 전자컴퓨터공학부 석사
2007년 9월~현재: 서울대학교 전기·컴퓨터공학부 박사과정
〈관심분야〉 내부자 보안, 자원 최적화, 제어 통신망



서 승 우 (Seung-woo Seo) 정회원
1987년 2월: 서울대학교 전기공학과 졸업
1989년 2월: 서울대학교 전기공학과 석사
1993년 12월: 미국 펜실베니아 주립대학 전기공학 박사
1993년~1994년: 미국 펜실베니아 주립대학 컴퓨터공학과 조교수
1996년~현재: 서울대학교 전기·컴퓨터공학부 교수
〈관심분야〉 컴퓨터·네트워크 보안, 무선·센서 네트워크, 보안 경제학