「정보시스템연구」 제21권 제4호
한국정보시스템학회
2012년 12월, pp. 01~29
http://dx.doi.org/10.5859/KAIS.2012.21.4.1

최종사용자의 인터넷과 소셜 네트워크 보안 행동에 대한 실증 연구

박경아* · 이대용** · 구철모***

〈목 차〉

Ⅰ. 서 론

오늘날 세계는 과학기술과 정보통신의 비약적인 발전으로 정보화 기반 아래 실시간 정보공유와 의사소통이 가능한 거대한 하나의 공동체로 발전되고 있으며 전통적으로 중시된 물리적인 가치보다는 정보의 가치가 더욱 중요하게 되고 있다(이준택, 2007). 또한 정보시스템의 확대 및 컴퓨터, 인터넷 및 소셜 네트워크 사용의 급격한 증가에 따라 정보시스템 사용자 개인 및 기업정보 유출에 의한 피해가 급격히 증가하고 있고 심각성에 대한 인식이 고조되고 있다. 이러한 정보화의 이면에 존재하는 해킹, 바이러스 등에 의한 정보자산의 침해, 사이버 테러, 개인 정보 및 중요 정보 자산의 무단 유출과 같은 역기능은 지속적으로 증가하여 심각한 문제로 대두되고 있으며, 이에 대한 사회적 관심과 정보보안을 위한 다양한 노력이 요구되고 있다(차인환, 2009).

정보화 사회에서 정보의 수집, 분석 및 활용 능력은 국내·외의 정보보안 경쟁력을 좌우하는 중요한 자산이다. 이러한 정보자산의 중요성

* 조선대학교 경영학부 박사과정, 주저자, pka@hanmail.net
** 조선대학교 경영학부 교수, 공동저자, dyblee@Chosun.ac.kr
*** 경희대학교 호텔관광대학 조교수, 교신저자, helmetgu@khu.ac.kr

은 정보에 대한 무단유출 및 파괴, 변조 등과 같은 공격의 대상이 된다. 예를 들면 인가받지 않은 불법적인 사용자에 의한 정보시스템의 파괴, 개인 신상 비밀의 누설 및 유출, 불건전 정보의 유통들과 같은 피해도 증가하고 있는 실정이다. 이러한 피해를 줄이기 위해서는 정보보안을 위한 방안을 적절히 강구하는 것이 중요하다(김종기, 2008).

개인정보 유출은 관련 유출사건에 대한 대규모 소송 등의 사회적 비용을 유발할 뿐 아니라 사회 전반적인 정보 프라이버시 및 보안 침해 우려를 발생시킴으로써 인터넷 사용자의 온라인 활동을 저해하는 요인으로도 작용하고 있다.

개인의 정보보안을 위해서는 최종 사용자가 적절한 정보보안실천 행동에 따라 달라진다고 볼 수 있다. 이는 사회인지 이론을 바탕으로 하고 있으며, 개인사용자의 보안에 관한 태도가 보안행위의도에 영향을 주며 이러한 의도가 행동에 영향을 준다고 볼 수 있다. 행동 의도는 실제 행동에 영향을 주는 동기유발 요인을 내포하는 것으로 추정되며, 행동에 대한 태도는 행동평가와 관련된 선호의 정도로 표현된다. 인간은 합리적인 존재이기 때문에 행동에 대한 태도와 주관적 규범은 행동의도에 영향을 주고, 행동의도는 실제적 행동과 높은 상관관계를 가진다는 가정으로 본 연구에서는 합리적 행동이론(TRA)을 바탕으로 하고 있다.

또한 본 연구는 개인 사용자가 가진 컴퓨팅 사용자 역량이 보안과 관련된 태도에 어떠한 영향을 미치며, 보안과 관련된 태도가 인터넷과 소셜 네트워크 사용에 있어 보안 관련 행위 의도와 이러한 의도가 보안기술사용과 보안행동실행에 미치는 영향에 대해 연구하고자 하는데 본 연구의 목적이 있으며, 이는 개인정보 보안의 중요성을 감안할 때 개인 사용자의 인터넷 사용과 소셜 네트워크 사용에 있어서 각각 다른 보안관련 태도와 의도를 보이며 이러한 의도가 최종사용자의 개인보안을 위한 행동과 실질적인 기술사용으로도 이루어질 것으로 생각된다. 이러한 연구 목적을 달성하기 위해 선행연구를 참고하여 사용자 역량, 보안과 관련된 태도, 주관적 규범, 인터넷과 소셜 네트워크 보안행위의도, 개인보안 행동에 대한 항목으로 나누어 설문조사를 실시하였다.

따라서 본 연구의 범위는 아래와 같다.

첫째, 개인컴퓨터를 사용하는 개인 사용자를 중심으로 인터넷과 소셜 네트워크 등의 정보시스템 사용능력과 컴퓨팅(정보시스템)의 사용범위, 깊이, 활용능력 등을 통해 사용자 역량을 알아보고, 이러한 사용자 역량과 보안태도와의 관계를 알아본다. 또한 자신의 동료 또는 자신의 영향을 받는 사람들의 기대에 의해 행동을 취하게 하는 보이지 않는 규범인 주관적 규범과 보안태도와의 관계도 알아보고자 한다.

둘째, 이러한 보안과 관련된 태도가 인터넷 보안 행위 의도와 소셜 네트워크 보안 행위 의도에 어떠한 영향을 미치는지에 대해 알아본다.

셋째, 인터넷 사용과 소셜 네트워크 사용에 있어서 보안행위 의도가 개인보안 성과인 보안기술사용과 보안행동실행에 어떠한 영향을 미치는지 알아보고, 개인보안성과 행동인 보안행동실행이 보안기술사용에 어떠한 영향을 미치는지도 알아본다.

본 연구의 구성은 다음과 같다. 먼저 이론적 배경에서 개인정보보안, 인터넷 보안과 소셜 네트워크 보안, 합리적 행동이론과 관련된 기존 문

헌을 살펴보고 이를 바탕으로 연구모델과 가설을 설정하였다. 또한 연구모델을 검증하기 위한 방법론을 설명하고, 통계적 분석을 통해 얻어진 연구결과를 밝혔다. 마지막으로 연구결과의 시사점과 향후 연구 과제를 제시하였다.

Ⅱ. 이론적 배경

2.1 개인정보 보안

개인정보는 개인과 관련된 모든 자료가 아니라 본의 의사에 반하거나 본인이 알지 못하는 상태에서 이용될 경우 당사자인 정보 주체의 안녕과 이해관계에 영향을 미칠 수 있는 개인을 식별할 수 있는 정보를 개인정보라고 할 수 있다. 이는 생존하는 자연인의 내면적 사실, 실제나 재산상의 특질, 사회적 지위나 손상에 관하여 식별되거나 또는 식별할 수 있는 정보의 총체를 일컫는 것으로 정의할 수 있다(김용재, 2009).

개인정보관리(Personal Information Management)는 우리가 개인들로서 획득, 조직, 유지, 검색과 정보의 공유를 통해 우리의 일상생활을 관리하기 위해 실행하는 활동들을 지원하기 위한 것이라 생각한다. 거의 모든 사람이 PIM 기술을 그들의 생활에 적용해야하지만 PIM에 대한 대중의 관심은 최근에야 알려지게 되었다. 개인정보관리는 정보를 처리하고 관리하기위한 우리 인간 능력을 크게 확장시키기 위해 개인용 컴퓨터가 출현하였던 1980년대에 처음 사용되었고 이러한 발전에서 개인정보관리를 잘하게 됨으로 인해 사람들의 귀중한 시간이 더 효율적으로 사용된다(Jaime, William and Benjamin, 2006).

인터넷 포털 사이트에서 회원가입을 전제로 우리는 상세한 신상정보를 제공함으로서 인터넷 커뮤니티 포털에 가입되고 사이트 내에서는 우리가 제공한 정보를 동일한 커뮤니티에 가입한 다른 회원들이 자유롭게 검색할 수 있게 된다. 어떤 사이트들은 이름, 생년월일, 전화번호, 주소, 직업, 관심분야, 최종접속시간 등까지 기입해야 한다. 이러한 정보는 동일그룹에 소속되어 있는 다른 회원들에게 공개되는 일이 많으며 쿠키(cookie)나 웹버그(webbug)와 같은 추적 및 감시 기술을 이용하여 우리가 접촉한 사람들의 e-메일주소, 방문한 웹사이트, 인터넷을 통해 구입한 상품, 가입한 온라인 커뮤니티에 대한 정보를 손쉽게 획득할 수 있다(이향우, 2006). 게다가 정보화 시대의 프라이버시가 정보통신 및 생체기술의 광범위한 사회적용으로 인해 예를 들어 CCTV인 폐쇄회로 텔레비전과 각종 감시카메라, 얼굴과 지문과 같은 생체인식기술, 위치추적 시스템으로 침해의 가능성이 높아지고 있다(Dubbeld, 2005; Ploeg, 2003).

개인이 자신에 대한 정보 혹은 개인정보를 보호할 수 있는 권리는 민주주의 사회에서 반드시 존중되어야 하는 인권으로서 프라이버시를 지키는데 핵심적인 요소가 된다. Warren and Brandeis(1890)는 “혼자 있을 권리(the right to be let alone)” 혹은 외부의 간섭이나 침해를 받지 않을 권리가 되며 프라이버시는 소극적 자유 혹은 가치로 이해된다. 즉, 규범적 측면에서 개인정보를 규정하면 개인의 특별한 속성이 누구에게도 드러내거나 양도할 수 없는 기본 권리가 되는 것이다. 개인들의 정보를 기업의 이윤증대를 위한 기업자산 혹은 마케팅 자원으로 인식하거나 개인들이 가지고 있는 정보, 레포트 등의

자료를 이용하여 이윤추구나 경제적 보상을 받는 등 경제성을 가진 가치로 인식하고 있다.

이러한 개인정보 노출은 일반 인터넷 사용자가 해킹 등 특별한 방법을 이용하지 않고 정상적으로 인터넷을 이용하면서 타인의 개인정보를 취득할 수 있도록 방치되어 있는 것을 말한다. 홈페이지에 개인정보가 노출되는 경우, 악의적인 목적을 가진 사람이 노출된 개인정보를 이용하여 스팸(spam) 발송 등으로 프라이버시를 침해할 수 있을 뿐 아니라, 명의도용 등을 통해 경제적인 손실을 가져올 수 있다. 더구나 정상적인 인터넷 이용만으로도 개인정보를 쉽게 취득할 수 있어 개인정보 침해사고의 발생 가능성이 매우 높다고 할 수 있다(교육과학기술부, 2008).

개인정보 노출은 홈페이지의 모든 콘텐츠(contents)에서 나타날 수 있다. 즉, 일반 웹 페이지에서부터 게시판과 첨부파일, 또는 각 페이지의 소스코드 등 홈페이지의 모든 영역에서 다양한 방식으로 나타날 수 있다는 것이다. 이 중 홈페이지에서 주로 나타나는 개인정보 노출 유형으로는 웹 페이지 노출, 첨부파일 노출, 외부 검색엔진(구글 등) 노출 등 4가지로 분류할 수 있다(교육과학기술부, 2008). 웹 페이지 노출은 업무담당자 부주의, 민원인의 개인정보 보호 인식 부족 등에 의해서 나타날 수 있으며, 공지사항, 휴면 웹 사이트, 게시판 답 글 등에 개인정보가 포함되어 노출되는 경우 등을 말한다. 첨부파일 노출은 게시판에 등록된 엑셀, 한글, 파워포인트, PDF, ZIP 등의 첨부파일에 개인정보가 노출되는 경우이고, 소스코드 노출은 해당 웹 페이지의 '소스보기'에 웹 사이트 설계 시 게시물에 대한 구분자로 사용한 게시자의 개인정보나 파일명, URL 등에 개인정보가 노출되는 경우이다. 외부검색엔진 노출은 외부 검색엔진을 통해 개인정보가 노출되는 경우를 말한다.

김동원(2003)은 개인정보를 개인적 인권으로만 환원하여 이해할 수는 없다고 주장하고 개인정보는 개인적 가치와 사회적 가치 그리고 경제적 가치를 동시에 지니고 있다고 말하고 있다. 사회적 가치는 개인정보의 수집 및 활용으로서 사회질서와 행정효율을 향상시켜 궁극적으로 공익을 증대하려는 노력과 연관된다고 보며 경제적 가치는 개인정보를 상품화하여 최대한의 이윤을 획득하고자 하는 기업 활동의 자율성을 적극적으로 옹호하는 입장으로 보고 있다.

많은 연구자들은 현대 자본주의 사회에서 개인정보는 우리가 편하고 효율적인 일상을 누리고 각종 범죄로부터 안전한 사회적 생활을 영위하기 위해 불가피하게 제공되어야 하는 재화가 되어버려 이미 하나의 경제적 거래대상 즉 상품이 되었다고 주장한다(Davies, 1998). 오늘날 정보통신 기술의 발전에 따라 경제적 보상에 근거한 감시체계가 더욱 고도화되고 정밀화 되어가고 있으며 개인정보는 이제 대중이 기업이나 시장이 제공하는 서비스를 얻기 위해 치르는 대가와 같은 것으로 취급되고 있다(Whitaker, 1999). 또한, Westin(1967)은 개인정보를 상품화하여 사고팔고 임대하는 것이 이미 관행이었다는 사실을 개인정보가 인권의 측면만이 아닌 또 하나의 사적 재산권이라는 견지에서 이해될 수도 있음을 보여준다.

개인정보에 대한 다른 접근법은 개인정보를 개인적인 가치로만 이해하지 않고 일종의 공유체로 접근한다. Regan(2002)은 프라이버시는 공통적 가치, 공공적 가치, 집합적 가치를 지니고 있으므로 프라이버시는 개인적 가치만으로 이

해해선 안 된다고 말한다. 또한, 개인정보를 사적 권리나 재산권으로 환원해서 이해를 하는 것이 아닌 공유재로 인식해야 한다고 주장하고 있다. 공유자원이란 주차장, 교량, 어장, 지하수 터, 방목지, 삼림, 강, 호수, 중앙컴퓨터, 인터넷 등과 같이 그러한 것들을 사용함으로 인해 얻어진 혜

<표 1> 개인정보보안 관련 선행연구

저자	분야	관련 이론	종속변수	독립변수	설명(결과)
Catherine and Ritu(2010)	최종사용자의 안전한 컴퓨팅 사용	보호동기부여 이론, 대중 소유물 연구, 심리적 소유권	인터넷과 컴퓨터 보안 행위 의도	보안 위협걱정, 보안 행동, 시민의식, 보안 동작 자기효능, 주관적 규범, 주변행동규범	가정용 컴퓨터 사용자를 중심으로 더욱더 양심적인 컴퓨터 시민을 만드는 방법에 대한 중요한 새로운 시각과 이론 및 연구를 제시함
Rhee and Kim and Young(2009)	최종사용자의 정보보안	사회인지이론, 자기효능 보안	자기효능, 보안기술, 보안노력을 강화하는 의도	컴퓨터/인터넷 환경, 보안위반 사례, 자기효능보안, 정보 보안 의도	정보보안의 궁극적인 성공은 최종 사용자가 적절한 정보보안실천행동에 따라 다름을 제시함.
Munro et.al.(1997)	최종사용자의 이해와 사용자의 능력	사용자 능력	개별실적	조직요인, 개별요인, 기술요인, 사용자 능력(폭, 깊이 기교)	사용자의 실력, 최종사용자의 기술의 지식의 깊이 그리고 창의적으로 이러한 기술(기교)에 적용하여 자신의 능력으로 구성
Janine(2010)	정보시스템 사용자 참여 보안 위험관리	information systems development (ISD) 사용자 참여, 보안위험관리	제어성능	사용자 참여, SRM 정렬, 조직개발, 제어개발	사용자의 참여는 비즈니스 프로세스에 민감한 정보를 사용자 보호에 참여시키는 수단
Liang et al. (2010)	개인 컴퓨터 사용에 대한 이해 보안 행위	위험 회피 이론 (TTAT)	회피행동	인식심각, 인식민감, 위협인식, 보호효과, 보호비용, 자기효능, 회피동기부여	개인용 컴퓨터에 사용자의 IT 위협 회피 행동에 대해 풍부한 지식제공
Mikko(2010)	정보시스템 보안	중립화 이론, 억지 이론	의도 위반 보안 정책	중립화, 공식적 제재, 비공적 제재, 부끄러움	정보시스템 보안 정책을 준수하는 중요한 요소로서 우리의 경험적 결과와 중립화 개발, 조직의 보안정책 및 관행을 고려해야 한다.
Bulgurcu et al.(2010)	정보보안 인식	계획된 행동 이론, 합리적 선택 이론	정보보안 인식	태도, 규범적인 신념, 자기효능, 서비스 태도	직원의 의도는 태도, 규범적인 신념, 그리고 준수하는 자기 효능에 영향을 받는다. 정보보안 인식인 긍정적 태도와 신념은 결과에 영향을 미친다.
Johnston and Warkentin (2010)	컴퓨터보안	보호 동기 부여 이론	최종 사용자의 행동 의도	자기효능, 응답효능, 위협의 심각도, 사회적 영향력의 인식	최종 사용자가 준수하여야 하는 컴퓨터 보안권장 사항에 대한 공포가 최종 사용자의 행동의도에 영향을 미치는 역할을 함

택을 누릴 수 있는 잠재적인 수혜자들을 배제하는 것이 어려운 자연적, 인공적 자원을 지칭한다(Ostrom, 2002).

이종구 외(2005)는 개인정보는 많은 기업들에게 전략적으로 매우 중요한 자산이기에 수집하거나 이용을 통한 수익을 창출하는 과정에 오용 및 과용으로 인한 개인 프라이버시 침해를 하는 경향을 지니고 있다고 말한다. 다음의 <표 1>은 개인정보보안과 관련된 주요 연구를 정리한 것이다.

이러한 주요 선행연구들을 바탕으로 본 연구에서는 선행변수의 사용자 역량과 주관적 규범이 최종사용자의 정보보안 태도에 미치는 영향과 인터넷과 소셜 네트워크에 대한 보안 행위 의도로 나누어 보안걱정에 대한 행동을 실행할 것인지, 또한 이러한 보안걱정 행동이 보안기술 사용으로 이어질 것인지에 대한 관계를 살펴보고자 한다.

2.2 사용자 역량과 주관적 규범, 보안태도

사용자 역량에 관한 연구는 1973년 하버드 대학교의 사회 심리학자인 McClelland가 업무성과를 위해 지능을 측정하는 것보다 개인역량을 측정하는 것이 더 합리적임을 연구하면서 시작되었다(McClelland, 1973). Mclagan(1989)은 지식, 기술, 태도 및 지적 전략 등의 개인역량을 통해 조직의 성과를 극대화할 수 있음을 주장하였고, Parry(1996)는 그의 연구에서 역량은 지식, 기술, 태도의 결합으로 사람들의 행동, 생각 등의 행위에 영향을 미쳐 제품과 서비스 등을 생산하는데 영향을 주고 결국 조직성과를 결정한다고 분석하였다.

개인역량은 기존연구에서 폭넓게 정의되어 있는데 특히, Torkzadeh and Lee(2003)는 정보기술 환경에서 컴퓨터를 활용할 수 있는 지식과 같은 숙련된 능력이 더욱 중요해지고 있다고 주장하였고, Harison and Boonstra(2009)는 기술변화에 대응하기 위한 역량을 정보시스템 조직의 변화, 기술변화, 위험과 성공요소에 대한 지식과 커뮤니케이션, 프로세스 관리, 리더십, 변화대응에 관한 숙련된 능력으로 나누어 정보기술에 집중된 개인역량으로 연구하였다. 본 연구에서는 사용자 역량을 컴퓨팅사용에 대한 활용범위(영역-폭), 수준(깊이), 활용능력으로 나누어 살펴보았으며, 측정방법으로 먼저 활용범위(영역-폭)는 지식이 있는지 없는지에 대한 유무(예, 아니오)에 대한 답변으로 처리하고 그 점수를 합산하여 처리하였고, 수준(깊이)은 각 7개의 질문에 매우 풍부한 지식부터-지식이 없음까지 7점 척도를 이용하여 7개의 질문에 대한 점수를 모두 합산해서 컴퓨팅 사용에 대한 수준을 살펴보았다.

주관적 규범과 보안태도로 행동에 대한 예측인자는 태도이며(Engel and Miniard, 1995), 도덕적인 추론 수준(Rholes and Baile, 1983)과 행위자의 자아개념(Bansal, 1997; McArthur and Cook, 1969)이 태도와 행동의 양에 영향을 미친다는 주장이 있다(Eagly, 1993). 뿐만 아니라 주관적 규범은 태도와 의도의 유의한 예측인자로 행동의도에 대해서 유의한 영향력을 지니고 있으며(박기정, 1998). 박혜정(2002)의 연구에서는 주관적 규범을 태도, 의도, 행동에 대해서 중요한 예측인자인 것으로 밝히고 있다.

유사한 관점에서 Fishbein은 소비자의 제품에 대한 태도(attitude)를 중심으로 소비자 행동을

예측하였던 자신의 다속성 모델에 주관적 규범(Subjective Norms)이라는 요인을 포함시켜 소비자 행동의 결정요인에 대한 설득력을 높인 이성적 행동이론(TRA; Theory of Reasoned Action)이라고 하였는데, 이성적 행동이론의 구체적인 내용을 살펴보면 다음과 같다. 한 제품에 대한 구매행동은 그 제품에 대한 구매의도(Behavioral Intention)에 의해서 결정되는데, 구매의도는 그 제품의 구매에 대한 본인의 태도(attitude)와 주관적 규범(Subjective Norms)에 의해서 결정된다는 것이다. 한편, 개인적 태도는 구매결과에 대한 믿음(Belief)과 그와 같은 결과에 대한 평가(Evaluation)가 곱해진 형태에 의해서 결정된다. 그리고 사회적 압력을 나타내는 주관적 규범은 자기에게 중요한 위치를 차지하는 준거집단의 자신에 대한 기대(Expection)와 이와 같은 기대에 따르려는 동기(Motivation to comply)가 곱해진 형태에 의해서 결정된다. 그리고 구매의도는 소비자의 구매행동을 결정하는 직접적인 요인이 된다고 보고 있다(Scott 1974).

2.3 인터넷 보안과 소셜 네트워크 보안

인터넷 보안은 인터넷을 통해 권한이 없는 컴퓨터 시스템의 접근이나 위험을 막는 것을 말하는데, 대부분의 자료의 암호화와 암호를 통해 보호를 받는다. 정보 네트워크의 중심으로 자리 잡고 있는 인터넷이 해커들의 공격대상이 되는 이유는 인터넷의 개방성, 소스 개방, 용이한 침입자간의 상호 정보교환 등 보안상의 취약한 특성을 갖고 있기 때문이다. 이 같은 취약성을 극복하기 위해 구현되는 인터넷 보안 기술은 허가되지 않은 정보에 대해서 우연히 혹은 의도적으로 누출, 전송, 수정, 파괴되지 않도록 보호하기 위한 것으로서 다른 분야의 기술과 달리 고유의 특성을 갖고 있다. 인터넷 정보보안을 위한 제반 시스템은 사회적으로 사이버 공간에서의 활동 증가에 따른 개인 프라이버시 보장과 정보 범죄의 차단 등 독자적 침해사고 대응환경을 구축함으로써 상호 협력관계 유지가 필요하며, 국가의 중요한 정보기반 구조를 보호하기 위해 필수적으로 요구되는 기술적 특징을 갖추어야 한다.

소셜 네트워크(Social Network)란 행위자가 선택하는 행위의 결과이기도 하며, 동시에 행위자의 차후 행위 선택을 제약하는 역할을 한다(손동원, 2002). 소셜 네트워크는 인터넷을 통하여 우연한 접촉에서부터 친밀한 유대까지 다양한 형태의 사회적 관계를 제공하는 일종의 가상 커뮤니티라고 할 수 있으며, 사회학에서 연구되고 있는 사회 연결망 이론(Social Network Theory)은 인간이 여러 사람들과 관계를 형성하는 양태를 통해 인간관계를 행위(action)와 구조(structure)의 상호역동성을 설명하는 이론이다. 소셜 네트워크이론은 노드들 사이의 사회적 관계에 관심을 갖는다(김효준·곽기영, 2011).

관계를 지향하는 인간의 성향은 소셜 네트워크의 예상을 뛰어 넘는 성공으로 이어지고 있으며, 사람들은 자신의 관심사나 일상 등을 관리하거나 타인과 공유하기 위해 소셜 네트워크를 사용하고 있다. 그러한 결과로 소셜 네트워크에는 방대한 개인정보가 존재하게 되었으며 이러한 데이터들은 향후 여러 분야에서 활용될 것으로 예상되고 있다(Adam, 2010; Weiss, 2007).

그러나 자유로운 정보의 공유로 인하여 여러 가지 보안상의 문제점들이 야기되고 있다. 개인

정보 수집을 통한 프라이버시 침해 위협, 수집된 정보를 이용한 스토킹 등의 2차적 위협, 무분별한 메시지나 스팸 메일 등으로 인한 피해는 해결해야할 당면과제가 되었다(행정안전부, 2008). 소셜 네트워크의 사용자 그 누구도 자신의 개인정보가 원치 않는 누군가에 의해 열람되거나 원치 않는 누군가에게 전달되는 것을 바라지 않을 것이다. 그럼에도 불구하고 소셜 네트워크의 각 사용자들이 온라인 공간에 존재하는 자신의 정보를 관리하는 일에 주의를 기울이지 못하는 경우가 많다.

소셜 네트워크서비스는 단순한 개인정보의 수집 및 저장뿐 만 아니라 2차적인 개인정보를 수집할 수 있다. 기술의 발전은 개인의 성격, 취미, 관심사, 종교, 정치적 성향 등의 광범위하고 방대한 정보의 수집과 분석이 가능하도록 하였다. 이는 개인 식별정보가 아니더라도 여러 정보들이 결합되어 개인의 식별이 가능하게 하고, 개인의 성향을 파악할 가능성이 크다. 이러한 정보를 이용하여 불법광고・스팸 등의 수단으로 악용할 수도 있다(Ina o'merchu et al., 2004). 소셜 네트워크에서는 개인정보 노출이 자연스럽게 발생하므로 이에 대한 보호 수단이 제공되어야 한다.

2.4 합리적 행동이론

합리적 행동이론(Theory of reasoned action)은 Ajzen and Fishbein (1975)이 처음으로 제시한 이론이다. 이 이론은 기존의 Fishbein이론에서 발전되어왔기 때문에 확장된 Fishbein이론이라고 하며 태도에 대한 심리학연구로부터 시작된 것이다. 합리적 행동이론에서는 행동(behavior)의 선행변수로서 행동의도(behavior intention), 행동에 대한 태도(attitude toward behavior), 그리고 주관적 규범(subjective norm)이 있다. 여기에서 행동 의도는 사람들이 어떤 행동을 시행할 동기가 얼마나 강한지를 의미하고(홍광표, 2011), 태도는 행동실행의 결과에 대한 여러 가지 신념과 각 신념의 평가에 의해 구성된다. 마지막으로 주관적 규범은 행동실행에 대해 주변에 관련된 사람들의 기대에 대한 자신의 지각과 자신이 그 사람들의 의견을 얼마나 수용하는가에 따라 행동의도에 영향을 미친다.

또한 사용자 역량에 있어 합리적 행동이론으로 Lee et al(1995)은 개인특성 또는 사용자 능력이 정보시스템 이용과 성과에 영향을 주는 중요한 요인이라고 지적하였다. 최종사용자 능력인 개인적 특성이 성과변수인 정보시스템 만족도에 직접적인 영향을 준다고 하였다. Baldwin and Rice(1997)와 King and Xia(1997)의 연구에서는 최종사용자 능력을 향후 사용자 특성, 또는 개인적 특성이라는 구성개념으로 사용되고 있었다. 보안의식에 따른 조직의 정보보안 수행의 중요한 역할은 사용자인 개인이 보안의식을 지니는 것이라고 볼 수 있다. Albrechtsen(2007)은 사용자를 위해 개인적인 보안의식과 행동에 영향을 주는 요소들을 가지고 정보보안의 취약점을 해결하기 위한 가이드라인을 제시하였다. 이에 본 연구에서는 선행변수들이 태도, 의도, 행동의 흐름에 영향을 미치는 변수간의 관계를 알아보고자 한다.

Ⅲ. 연구 설계 및 연구가설 설정

3.1 연구모형 설계

본 연구에서는 <그림 1>에서 보는 바와 같은 연구모형을 제안한다. 기존의 선행연구 고찰을 통해 사용자 역량의 영향요인과 보안과 관련된 태도와 주관적 규범과의 변수관계를 검토하였다. 또한 보안과 관련된 태도가 인터넷과 소셜 네트워크 사용에 있어서의 보안 관련 행위 의도가 개인보안성과인 보안실행기술과 보안행동실행에 영향을 미치는 변수간의 관계를 검토하였다.

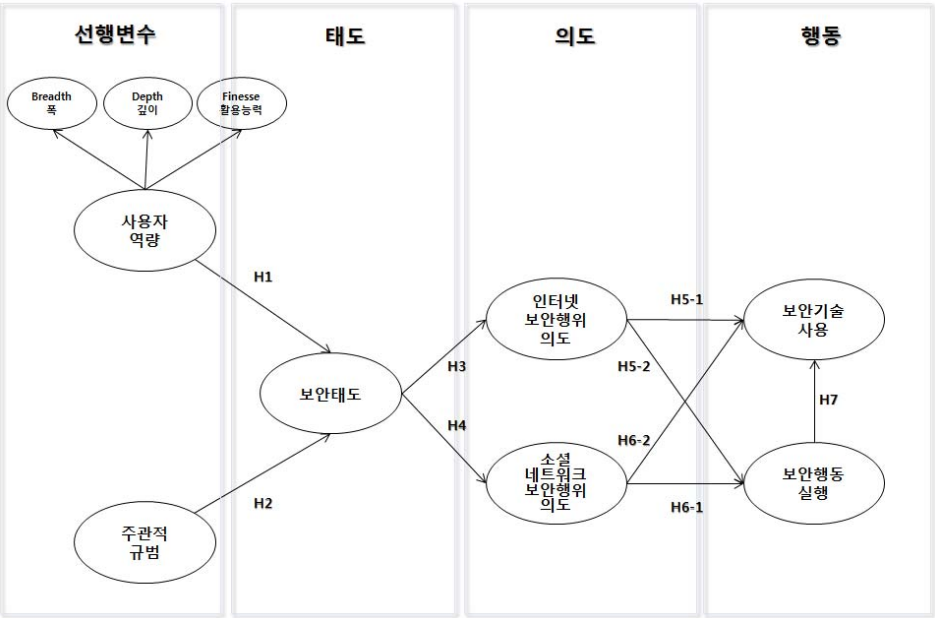
3.2 연구가설 설정

이 연구 모형에 포함된 변수들을 통계적으로 검증하기 위해 주요 변수들의 관계를 설명하고 각 개념들에 대한 기존 문헌연구를 바탕으로 가설을 설정하고자 한다.

3.2.1 사용자 역량과 보안태도

Spencer and Spencer(1993)는 역량을 다양한 상황에서도 행동 및 사고방식을 장시간 지속할 수 있는 내적 특성으로 정의 내리고 286개의 역량 모델을 구하여 관리자의 역량을 6개의 역량군과 20개의 역량으로 모델화하였고 또한 동기부여, 개인특성, 자기개념, 지식, 숙련된 능력 이라는 개인역량으로 도출하기도 하였다.

Marrelli(1998)은 역량을 업무와 관련된 지식과 숙련된 능력을 수행하는 행위(Enabled behavior)를 추가하여 개인역량 측정이 가능함을 제시하였다.



<그림 1> 연구모형

Torkzadeh and Lee(2003)는 정보기술 환경에서 컴퓨터를 활용할 수 있는 지식과 같은 숙련된 능력이 더욱 중요해지고 있다고 주장하였으며, Harison and Boonstra(2009)는 기술변화에 대응하기 위한 역량을 정보시스템, 조직의 변화, 기술변화, 위험과 성공요소에 대한 지식과 커뮤니케이션, 프로세스 관리, 리더십, 변화대응에 관한 숙련된 능력으로 나누어 정보기술에 집중된 개인역량으로 연구하였다.

이외에도 Goodhue and Straub(1991)는 보안관심모형에서 개인적 역량은 잠재적인 문제발생의 지각정도를 의미하며, 보안문제의 발생정도를 심각하게 수용할 경우 보안 만족도에 영향을 미친다는 것을 강조함으로써 사용자의 보안관심이 정보시스템 보안효과를 높이는 것으로 평가하였다.

본 연구에서 사용자 역량은 정보시스템 활용과 관련된 최종 사용자의 컴퓨팅 특성을 의미한다. 사용자 컴퓨팅 관련 지식과 자발적 활용에 대한 특성은 개인의 컴퓨팅 관련 우위를 평가하는 주요요인으로 객관적 및 주관적 경험에 따라 달라진다(Smith et al., 2000). 이에 따라 다양한 컴퓨팅 관련 지식을 확보하고 있고, 활용을 즐기는 사용자일수록 자신의 컴퓨팅 관련 행동과 태도를 통제할 수 있다고 굳게 믿는 경향을 가지게 된다(Winter, et al., 1998). 이러한 논의를 바탕으로 본 연구의 가설에서는 컴퓨팅 사용에 대한 개인 사용자의 활용범위, 활용수준, 활용능력이 포함된 사용자 역량이 보안태도에 미치는 영향을 살펴본다.

H1 : 사용자 역량은 보안태도에 정(+)에 영향을 미칠 것이다.

3.2.2 주관적 규범과 보안태도

주관적 규범(Subjective Norms)은 인지행동과학에서 주목받고 있는 계획된 행동이론(theory of planned behavior: TPB)으로부터 도출된 요인이다. 이는 개인이 집단에서 다른 구성원들로부터 느끼는 압력의 정도를 의미하며, 행위의도에 영향을 미치는 요인으로 알려져 있다(Ajzen and Fishbein, 1980). 또한 주관적 규범은 행동을 할 것인지 아니면 말 것인지에 영향을 미치는 사회적 압력을 말한다(Ajzen and Fishbein, 1980; Eagly and Chaiken, 1993; Ajzen and Fishbein , 1975). 즉, 한 개인의 주관적 규범은 각 규범적 신념의 강도에 준거집단을 따르려는 동기의 강도를 곱한 것을 모든 준거집단에 대하여 합해 줌으로써 측정이 가능하다(Fiske and Taylor, 1991; Lee and Green, 1991).

Brown and Venkatesh (2005)는 가정에서 사용하는 컴퓨터 구입과 사용에 있어 친구와 가족이 중요한 역할을 한다고 하였다. 따라서 자신의 동료나 자신의 영향을 받는 사람들의 기대에 의해 행동의도를 취하게 하는 결정적인 역할을 한다는 것이다. 이러한 이론적 근거와 선행연구의 결과를 토대로 다음과 같은 연구가설을 도출하였다.

H2 : 주관적 규범은 보안태도에 정(+)에 영향을 미칠 것이다.

3.2.3 보안태도와 인터넷, 소셜 네트워크 보안행위의도

Ajzen and Fishbein(1980)은 개인의 태도를 주어진 문제에 대해 긍정적 혹은 부정적 방식으로 응답하는 감정으로 정의하고, 특정 정보

를 통해 좋거나 나쁜 감정을 학습하게 되어 행동의도에 선행함을 논하였다. 또한, 합리적 행동 이론(Davis et al., 1989)과 계획된 행위 이론(Mathieson, 1991) 모형에서도 태도는 행동에 대한 믿음과 결과의 평가로부터 형성되는 것으로 설명하고 있다. 이처럼 특정 보안 활동으로부터 학습된 사용자의 태도는 적극적인 보안의도를 형성하는데 있어 주요한 역할을 하게 된다(Lee and Kozar, 2005).

인터넷 보안은 개인정보가 노출되어 공개되거나 악의적인 사용이 될 수 있는 경우를 대비하여 개인정보 노출에 대한 대응 노력의 중요성이 강조된다(이정호, 2008). 인터넷 사용자가 행할 수 있는 개인정보 보호 노력은 주기적인 쿠키관리 패스워드 변경, 광고링크의 클릭 자제, 스팸메일 차단 서비스 등의 기능을 이용하는 것이다(KISA, 2010).

소셜 네트워크 서비스에서는 개인정보를 사이버 공간에 노출함으로써 개인의 정체성이 형성이 되고 타인과의 관계를 이룬다. 이러한 소셜 네트워크 서비스는 현재 대부분의 서비스 제공자들이 정보수집 및 공개 관행의 투명성이 결여되어 있으며, 개인 정보와 2차 정보에 대한 공개 항목과 범위에 대한 기준이 모호하기 때문에 서비스 제공자가 상업적으로 소비자 정보를 사용할 가능성이 크다(남기효 외, 2008).

본 연구에서는 인터넷과 소셜 네트워크를 보호하는 보안행위의도를 구분해야 한다. 두 의도가 매우 관련이 있을 가능성이 있는 것으로 인정 되지만, 이 두 가지 구성을 차별하여 연구하는 것은 중요하다 할 수 있다. 이는 보안 태도에 있어서도 인터넷과 소셜 네트워크는 다른 보안태도를 보일 것이다. 이러한 논의를 바탕으로 다음과 같은 연구가설을 도출하였다.

H3 : 보안 태도는 인터넷 보안행위의도에 정(+)에 영향을 미칠 것이다.

H4 : 보안 태도는 소셜 네트워크 보안행위의도에 정(+)에 영향을 미칠 것이다.

3.2.4 인터넷, 소셜 네트워크 보안행위의도와 보안성과(보안기술사용, 보안행동)

태도와 행동의도의 관계에 대한 이론은 여러 분야에서 활발하게 연구되었다(Armitage and Conner 2001; Sheeran and Taylor 1997; Venkatesh et al. 2003). Ajzen and Fishbein (1980)은 구체적인 행동에 대한 태도는 개인이 감정과 행동 사이에 조화를 추구하기 때문에 의도가 행동을 수행하기 위해 영향을 준다는 것이다.

합리적 행동 이론(Davis et al., 1989)에서 개인의 의도는 특정 행동에 영향을 미치는 동기적 요인으로 개인이 행동을 완수하기 위해 기꺼이 시도한다든지, 실행 계획이 어느 정도 잘 수립되었는지에 대해 설명하는 개념이다. 이때 강력한 의도가 행위와 결합될 경우 특정 과업이 완수될 수 있음을 지적하였다. 또한 Choi et al.(2008)은 그의 연구에서 보안인식과 행동사이의 관계의 실제적 유효성을 살펴보았다. 이 연구에서는 관리적 정보보안 인식을 하나의 독립변수로 두고 정보보안에 대한 관리적 행동의 5가지 요인을 종속변수로 설정하여 보안인식이 정보보안에 대한 각각의 행동에 미치는 영향을 가설로 설정하여 이의 관계를 보았다.

또한, Ajzen and Fishbein(1997)은 사용자의 행위의도가 특정상황에 처했을 때 이미 정해놓은 방식으로 행동하고자 하는 계획으로 개념적인 정의를 내리고 있다. 결과적으로 개인은 행위 지향적인 태도와 해당 행위에 대한 믿음이 강할수록 행위를 수행하고자 하는 의도가 더욱 강해지게 되며, 더욱이 행위에 대한 충분한 통제 능력과 기회가 주어진다면 자신의 의도를 실행하기를 원한다고 설명하였다.

본 연구에서는 인터넷과 소셜 네트워크 보안 행위의도가 보안성과인 보안기술사용과 보안행동실행에 영향을 미친다는 것이다. 따라서 이러한 이론적 근거와 선행연구의 결과를 토대로 다음과 같은 연구가설을 도출하였다.

H5-1 : 인터넷 보안행위의도는 보안기술사용에 정(+)에 영향을 미칠 것이다.
H5-2 : 인터넷 보안행위의도는 보안행동에 정(+)에 영향을 미칠 것이다.
H6-1 : 소셜 네트워크 보안행위의도는 보안행동실행에 정(+)에 영향을 미칠 것이다.
H6-2 : 소셜 네트워크 보안행위의도는 보안기술사용에 정(+)에 영향을 미칠 것이다.

3.2.5 보안행동실행과 보안기술사용

효과적인 보안 태도는 최종 사용자가 적절한 보안행동 실행과 보안기술 사용을 결정한다고 할 수 있다. 그러나 정보보안이 전통적으로 전문가나 정보 보안 팀과의 협력결과와 기술적인 문제로 취급되어 왔다. 정보보안의 이러한 이상한 관점은 종종 보안체인의 가장 취약한 부분으로 인간에 대한 배려의 문제로 언급되고 있다 (Angel, 1993).

본 연구에서는 보안에 대한 개인의 노력 강화와 보안에 대한 개인정보의 걱정행동이 보안을 실행시키는 기술사용으로 이어질 것 이라는 것이다. 따라서 이러한 이론적 근거와 선행연구의 결과를 토대로 다음과 같은 연구가설을 도출하였다.

H7 : 보안행동실행은 보안기술사용에 정(+)에 영향을 미칠 것이다.

Ⅳ. 연구방법론 및 실증분석

4.1 자료수집과 표본의 특성

본 연구는 컴퓨팅 사용자의 역량과 주관적 규범인 보안과 관련된 태도가 인터넷과 네트워크 보안 행위 의도에 영향을 미치며 이는 다시 개인 보안성과 행동에 영향을 미치는 연구를 분석하기 위하여 일반 개인 사용자를 중심으로 실증분석하였다. 연구의 목적을 분석하기 위하여 기존의 이론 및 선행연구를 중심으로 연구모형과 설문문항을 작성하였다. 설문문항에 대한 신뢰도와 타당도를 조사하기 위하여 이를 작성한 후 선행조사를 실시하였다. 선행조사는 경영학을 전공하는 교수 및 대학원생과 대학생 20명을 대상으로 설문을 수집하였으며, 수집하는 과정에서 응답자들에게 표현이 모호하거나 적절하지 않은 문항에 대해 수정을 부탁하면서 설문 항목에 대한 피드백을 하였다. 선행조사를 통해 초기 개발된 측정항목들 중에서 일부는 수정하거나 삭제되었고, 측정항목의 타당성과 신뢰성에 문제를 야기할 수 있을 것으로 판단되는 항목들을 수정 및 보완하여 최종 측정도구의 개발을 완료

하고 실제 자료 수집에 활용하였다.

이에 본 연구에서는 일반 개인 사용자를 중심으로 온라인과 오프라인을 통해 설문조사를 실시하였으며, 실증연구 조사는 2011년 4월 25일부터 2011년 6월 12까지 이루어졌다. 연구모형의 분석을 위해 전체 250부의 온·오프라인으로 설문지를 배포하여 230부를 회수하였으며, 이중 결측치가 있거나 불성실하게 응답한 6부의 설문지를 제외한 총 224부를 최종분석에 활용하였다.

응답자에 대한 성별을 살펴보면, 남자는 41.4%, 여자는 58.5%로 나타났으며, 연령별 특성을 살펴보면 18-29세 이하가 80.8%, 30-39세가 6.3%, 40-49세가 7.6%, 50-59세가 5.4%, 60세 이상은 응답자가 없는 것으로 나타났다. 응답자의 교육수준을 살펴보면 대학원이상이 5.8%, 대학이 92.0%, 고등학교가 1.3%, 기타 0.9%로 응답한 응답자의 대부분이 대학생 이상이였으며, 응답자의 직업을 살펴보면 대학생과 대학원생이 76.8%, 자영업이 0.4%, 생산직이 5.4%, 사무직이 8.0%이며, 전문직이 1.8%, 판매서비스직이 7.6%로 나타났다.

<표 2> 인구통계학적 특성

구분		빈도	백분율(%)
성별	남	93	41.4%
	여	131	58.5%
연령	18-29세	181	80.8%
	30-39세	14	6.3%
	40-49세	17	7.6%
	50-59세	12	5.4%
	60세 이상	0	0.0%
교육수준	대학원	13	5.8%
	대학	206	92.0%
	고등학교	3	1.3%
	기타	2	0.9%
직업	대학생, 대학원생	172	76.8%
	자영업	1	0.4%
	생산직	12	5.4%
	사무직	18	8.0%
	전문직	4	1.8%
	판매서비스직	17	7.6%

4.2 자료 분석 방법

본 연구를 수행하는데 있어서 수집된 224부의 응답설문지는 코딩과정을 거쳐 통계분석에 이용되었다. 수집된 데이터는 응답자의 인구통계적 특성을 위해 SPSS 12.0이 사용되었으며,

<표 3> 설문지의 구성

연구변수			설문 내용	연구자
사용자 역량	폭	BR	소프트웨어에 관한 지식수준에 대한 질문으로 컴퓨터, 인터넷, 소셜 네트워크, 엑셀, 데이터베이스, 워드프로세싱, 그래픽처리 등의 지식유무	Munro et al. (1997)
	깊이	DE	소프트웨어에 관한 지식수준에 대한 질문으로 컴퓨터, 인터넷, 소셜 네트워크, 엑셀, 데이터베이스, 워드프로세싱, 그래픽처리에 대한 지식수준 정도	
	활용 능력	FN1	일반적인 문제해결을 위해 컴퓨터를 얼마나 활용하고 있는지의 정도	
		FN2	업무에서 문제해결을 위해 컴퓨터를 얼마나 자신 있게 사용하는지 정도	
		FN3	업무에서 문제해결을 위해 소프트웨어 패키지의 창의적 사용정도	
		FN4	업무에서 문제해결을 위해 소프트웨어 패키지 혁신적 사용정도	
		FN5	문제해결을 위해 컴퓨터 사용을 새로운 방식으로 사용하는지의 정도	
주관적 규범		SN1	나에게 영향을 주는 내 친구들이 내가 내 가정용 컴퓨터를 보호하기 위해 보안대책을 세워야 한다고 생각하는 정도	Catherine and Ritu(2010)
		SN1	나에게 중요한 주변사람들은 내가 내 가정용 컴퓨터를 보호하기 위해 보안대책을 세워야 한다고 생각하는 정도	
		SN1	내 동료들은 내가 인터넷을 보호하기 위해 내 가정용 컴퓨터를 보호하는 보안대책을 세워야 한다고 생각하는 정도	
보안태도		SA1	컴퓨터에 바이러스백신프로그램이나 소프트웨어, 방화벽, 시스템 업데이트 구현과 같은 보안대책을 사용해야 하는 생각 정도	Catherine and Ritu(2010)
		SA1	컴퓨터를 보호하기 위해 보안조치를 취하는 것의 중요정도	
		SA1	컴퓨터 보호를 위하여 보안대책을 세우는 것이 옳다고 생각하는 정도	
인터넷 보안 행위 의도		ISI1	인터넷을 보호하기 위해 컴퓨터에 대한 보안조치를 취하는 것이 좋다고 생각하는 정도	Catherine and Ritu(2010)
		ISI2	인터넷을 보호하기 위해 컴퓨터에 보안조치를 취할 정도	
		ISI3	인터넷을 보호하는 게 가정용 컴퓨터에 보안대책을 세우는 것이라고 확신하는 정도	
소셜 네트워크 보안 행위 의도		SSI	소셜 네트워크를 보호하기 위해 내가 사용하는 소셜 네트워크에 대한 보안조치를 취하는 것이 좋다고 생각하는 정도	Catherine and Ritu(2010)
		SS2	내가 사용하고 있는 소셜 네트워크를 보호하기 위해 소셜 네트워크에 보안조치를 취할 정도	
		SS3	내가 사용하고 있는 소셜 네트워크를 보호하는게 소셜 네트워크에 보안대책을 세우는 것이라 확신하는 정도	
보안기술 사용		SPT1	가정용 컴퓨터에 바이러스 백신 프로그램을 설치하여 사용하고 있는 정도	Rhee and Kim and Young(2009)
		SPT2	컴퓨터에 바이러스 백신 프로그램이 설치되어있고, 얼마나 자주 업데이트 하는가의 정도	
		SPT3	가정용 컴퓨터에 스파이웨어 방지 소프트웨어를 현재 사용하고 있는가의 정도	
		SPT4	가정용 컴퓨터에 이메일 소프트웨어의 스팸 필터링기능 사용 정도	

연구변수		설문 내용	연구자
	SPT5	가정용 컴퓨터나 네트워크에 방화벽을 사용하는 정도	
	SPT6	컴퓨터의 운영체제 및 중요 애플리케이션 패치를 통한 보안 업데이트를 자주 사용하는 정도	
	SPT7	컴퓨터 기능 중 팝업창 차단 기능을 사용하고 있는 정도	
	SPT8 (삭제)	무선 연결에 있어 암호화 기능을 사용하고 있는 정도	
보안행동 실행	SPB1 (삭제)	인터넷을 통해 공유소프트웨어(토렌트, 당나귀) 사용에 주위를 기울여 사용하는 정도	Rhee and Kim and Young(2009)
	SPB2 (삭제)	중요한 파일의 경우 백업 사본을 만들어 사용하고 있는 정도	
	SPB3	금융 및 의료기록등과 같은 중요한 개인정보를 컴퓨터 이외에 별도로 저장하는 정도	
	SPB4	다른 사람에게 개인 중요 정보(계좌번호, 비밀번호, 주민등록번호)를 보낼 때 이메일 사용을 가급적 피하는 정도	
	SPB5	다른 온라인 계정들에 대해 서로 다른 암호를 사용하는 정도	
	SPB6	인터넷에서 개인 주요 정보를 보낼 때, 사이트에서 전송된 데이터에 암호화 여부를 확인하는 정도	
	SPB7	컴퓨터를 다른 사람과 공유할 때 주위를 기울여 사용하는 정도	
	SPB8	특수기호 및 숫자와 조합하여 추측하기 어려운 암호를 사용하고 있는 정도	

본 연구에서 수집된 자료와 분석은 PLS(Partial Least Square) 소프트웨어 중의 하나인 SmartPLS 2.0을 사용하여 부트스트랩(bootstrap) 분석을 통한 가설 검증용 경로분석을 수행하였다. PLS는 컴포넌트(component)를 기반으로 하는 접근방식에 의해 추정하여 표본의 크기와 잔차 분포(residual distribution)에 대한 요구 사항이 비교적 엄격하지 않다(Chin, 1998a). 또한 이론적 구조모형에 대한 평가와 측정모형에 대한 평가를 동시에 할 수 있는 기법이며, 측정항목과 구성개념 간의 관계가 인과관계일 경우에 적절하다. 본 연구에서 채택하고 있는 구성개념의 대부분이 인과관계의 성격을 지니고 있으므로 PLS를 분석도구로 채택하였다.

변수들 간의 판별타당성이 확보되었는지 확인하기 위해 확인적 요인분석(Confirmatory Factor Analysis: CFA)과 PLS(Partial Least Square) 경로모형을 사용하여 연구모형의 적합도 평가 및 가설검증을 실시하였다.

4.3 연구변수의 조작적 정의 및 측정

본 연구에서는 앞서 기존 연구에 대한 종합적인 검토와 분석을 통해 연구모형을 정립하였으며 관련문헌을 바탕으로 측정모형을 검증하기 위해 각 지표에 대한 5점 Likert 척도(보안기술 사용, 보안행동 실행)와 7점 Likert 형식으로 신뢰성과 타당성을 가질 수 있도록 다항목 척도로 측정하였다.

실증연구를 위해서는 현상에 대한 계량적인

측정이 요구되며 이러한 측정을 통해서 현상 속에 내재되어 있는 특성변수의 상태와 변수들 간의 관계를 분석할 수 있다. 따라서 연구에서 사용되는 주요 용어들이 다양한 의미를 포함하고 있을 뿐만 아니라 연구 목적에 따라서도 학자들마다 다르게 정의하고 있기 때문에 여기에서도 본 연구목적에 맞도록 기존의 정의된 개념들을 보다 주체적이고 관찰 가능한 조작적 정의를 한다.

4.4 측정모형 검증

측정모형의 분석을 위해서 본 연구에서 사용된 측정 항목들에 대한 집중타당성(Convergent Validity), 내적일관성(Internal Consistency), 그리고 판별타당성(discriminant validity)에 대해 살펴보기 위해 PLS를 이용하여 확인적 요인분석(confirmatory factor analysis)을 수행하였고, 그 결과는 <표 4-3>과 같다.

첫째, 집중 타당성은 개별 측정항목의 신뢰성(individual item reliability)을 통해서 파악할 수 있다. 개별 측정항목이 신뢰성을 가지기 위해서는 개별 측정항목과 해당 변수가 서로 공유한 분산(shared variance)이 오차분석(errorvariance)보다 커야 하기 때문에 최소 0.6, 이상적으로는 0.7이상의 표준화된 로딩값(standardized loading)이 요구된다(Chin,1998a; 김진완, 2011). 확인적 요인분석을 통해서 모든 측정항목의 로딩값을 구한 결과, 전체 측정항목 중에서 3개의 항목을 삭제하였다. 보안기술사용(SPT8), 보안행동실행(SPB1), 보안행동실행(SPB2)이 로딩값이 0.6 이하로 나타나 삭제하였다.

<표 4>에 제시된 확인적 요인분석의 결과 값은 개별 측정항목의 신뢰성을 저해하는 3개의 항목을 삭제한 후에 다시 확인적 요인분석을 수행하여 제시된 것이다. 결과적으로 살펴보면, 보안행동실행(SPB4), 보안행동실행(SPB5), 보안기술사용(SPT4), 보안기술사용(SPT7)가 0.7에는 미치지 못하였다. 0.7에 미치지 못한 측정항목도 최소 기준값 0.6이상을 상회하고 있으므로 분석에는 무리가 없음이 입증되었다. 이러한 결과는 본 연구에서 사용된 측정항목들이 개별적으로 해당 변수를 측정하기에 신뢰할 만하다고 해석할 수 있다. 또한 개별 측정항목의 신뢰성이 높다는 것은 각 측정항목이 집중 타당성을 지니고 있다고 볼 수 있다.

둘째, 측정모형의 내적일관성에 대해서는 크론바하 알파계수(Cronbach's α), 평균분산추출값(Average Variance Extracted: AVE), 그리고 복합신뢰도(Composite reliability)로 평가할 수 있다. 먼저 여러 개의 항목을 이용하는 경우 일반적으로 신뢰성을 평가하는 크론바하 알파계수(Cronbach's α)는 0.6에서 0.7이상이면 신뢰성이 있는 것으로 간주한다. AVE 값은 구성개념에 의해 설명되는 분산의 양을 나타내며, 그 값이 0.5보다 클 경우에는 측정오차가 구성개념에 의해 설명되는 분산보다 작기 때문에 구성개념의 신뢰성이 있는 것으로 판단한다(Fornell and Larcker, 1981). 복합신뢰도는 다른 요인들을 함께 고려하여 계산한 각 요인별 신뢰성을 평가하는 방법으로 0.7이상이면 내적 일관성이 있는 것으로 본다.

PLS 경로모형의 전체 적합도는 <표 5>에 나타나 있다. 본 연구에서는 모든 지표들의 Cronbach α가 모두 0.6이상의 값을 보이고 있고, AVE값도 모두 기준치인 0.5보다 높은 것으로 나타나 신뢰성을 확보하고 있다. 또한 내적일관

<표 4> PLS 확인적 요인분석

	DE	BR	SA	SPB	SPT	SSI	ISI	SN	FN
DE	**1.00**	0.53	0.20	0.45	0.53	0.19	0.20	0.22	0.67
BR	0.53	**1.00**	0.16	0.30	0.33	0.20	0.18	0.15	0.31
SA1	0.20	0.16	**0.94**	0.19	0.39	0.51	0.67	0.30	0.30
SA2	0.18	0.14	**0.96**	0.20	0.35	0.52	0.72	0.32	0.26
SA3	0.20	0.14	**0.95**	0.24	0.36	0.54	0.72	0.33	0.30
SPB3	0.42	0.30	0.05	**0.65**	0.29	0.11	0.12	0.17	0.37
SPB4	0.31	0.17	0.25	**0.65**	0.34	0.17	0.23	0.21	0.30
SPB5	0.34	0.22	0.08	**0.67**	0.32	0.10	0.09	0.18	0.29
SPB6	0.37	0.19	0.14	**0.81**	0.39	0.18	0.23	0.33	0.39
SPB7	0.34	0.28	0.23	**0.84**	0.47	0.29	0.27	0.35	0.37
SPB8	0.27	0.20	0.18	**0.78**	0.44	0.29	0.27	0.31	0.29
SPT1	0.35	0.24	0.46	0.41	**0.85**	0.30	0.48	0.31	0.41
SPT2	0.42	0.29	0.28	0.39	**0.80**	0.28	0.40	0.31	0.47
SPT3	0.33	0.15	0.27	0.39	**0.80**	0.18	0.31	0.26	0.44
SPT4	0.42	0.19	0.19	0.37	**0.65**	0.11	0.15	0.25	0.48
SPT5	0.47	0.24	0.30	0.36	**0.75**	0.24	0.35	0.32	0.43
SPT6	0.51	0.35	0.13	0.48	**0.69**	0.23	0.21	0.31	0.48
SPT7	0.33	0.27	0.33	0.37	**0.68**	0.24	0.42	0.35	0.35
SSI1	0.19	0.18	0.53	0.27	0.31	**0.94**	0.62	0.38	0.24
SSI2	0.18	0.19	0.53	0.27	0.30	**0.95**	0.63	0.46	0.21
SSI3	0.17	0.17	0.47	0.23	0.25	**0.90**	0.62	0.47	0.15
ISI1	0.19	0.16	0.76	0.23	0.42	0.62	**0.93**	0.38	0.24
ISI2	0.20	0.18	0.68	0.30	0.45	0.67	**0.95**	0.52	0.28
ISI3	0.18	0.16	0.61	0.28	0.41	0.58	**0.92**	0.51	0.20
SN1	0.19	0.15	0.37	0.33	0.40	0.47	0.53	**0.95**	0.23
SN2	0.19	0.14	0.28	0.36	0.34	0.42	0.44	**0.96**	0.24
SN3	0.23	0.14	0.29	0.35	0.39	0.44	0.45	**0.94**	0.27
FN1	0.48	0.22	0.41	0.32	0.47	0.17	0.30	0.21	**0.78**
FN2	0.55	0.27	0.34	0.32	0.40	0.16	0.24	0.13	**0.83**
FN3	0.62	0.30	0.20	0.38	0.52	0.15	0.21	0.23	**0.90**
FN4	0.63	0.28	0.18	0.43	0.55	0.21	0.19	0.24	**0.90**
FN5	0.59	0.26	0.18	0.48	0.52	0.25	0.18	0.30	**0.86**

참고: DE=깊이(Depth), SPT=보안기술사용(Security Practice Technology), SPB=보안행동실행(Security Practice Behavior), SSI=소셜네트워크보안의도(Social Web Security Behavior Intentions), ISI=인터넷보안의도(Internet Security Behavior Intentions), SN=주관적 규범(Subjective Norm), SA=보안태도(Security Related attitude), BR=폭(BR), FN=활용능력(Finesse)

<표 5> PLS 경로모형의 전체 적합도(Overall Model Fit)

	AVE	복합 신뢰도	R^2	Cronbach α	공통성	중복성
DE	1.00	1.00	0.66	1.00	1.00	0.66
SPT	0.56	0.90	0.38	0.87	0.56	0.15
SPB	0.54	0.87	0.10	0.83	0.54	0.03
SSI	0.87	0.95	0.30	0.92	0.87	0.26
ISI	0.87	0.95	0.55	0.92	0.87	0.47
SN	0.90	0.96		0.94	0.90	
SA	0.90	0.97	0.16	0.95	0.90	0.08
BR	1.00	1.00	0.26	1.00	1.00	0.26
FN	0.73	0.93	0.93	0.91	0.73	0.68

성을 평가하기 위한 복합신뢰도가 모두 0.8이상으로 기준치인 0.7을 상회하고 있다. 이러한 결과로 볼 때, 본 측정모형에서 사용된 모든 구성개념들은 높은 수준의 내적 일관성을 가지고 있다고 할 수 있다.

또한 측정모형에 대한 통계량으로는 측정모형의 적합성(Quality)을 나타내는 공통성(Communality) 값이 있다. 공통성이란 추출된 요인이 변수가 가지는 분산의 몇 퍼센트를 설명할 수 있는가를 나타내는 값으로 일반적으로 공통성 값은 최소 0.5 이상이어야 한다(Tenenhaus et al., 2005). <표 5>에 지시된 공통성 값을 살펴보면, 모든 요인의 공통성 값이 0.5이상인 것으로 나타났다. 따라서 본 연구의 측정모형에 대한 적합성은 충분하다고 할 수 있다.

셋째, 판별타당성은 어떤 잠재변수가 의미하는 개념이 다른 잠재변수의 개념과 구별되는 정도로 확인적 요인분석에서 각 측정항목들은 이론적으로 관계를 갖는 요인에 적재된값(로딩값)이 그렇지 않은 요인에 적재된 값 (크로스 로딩값)보다 클 경우에 판별타당성을 확보하게 된다. 확인적 요인분석의 결과인 <표 4>를 보면 각 요

<표 6> 변수간 상관관계 및 AVE 제곱근

Construct	AVE	DE	SPT	SPB	SSI	ISI	SN	SA	BR	FN
DE	1.00	**1.00**								
SPT	0.56	0.53	**0.75**							
SPB	0.54	0.45	0.52	**0.74**						
SSI	0.87	0.19	0.31	0.28	**0.93**					
ISI	0.87	0.20	0.46	0.29	0.67	**0.93**				
SN	0.90	0.22	0.40	0.37	0.47	0.50	**0.95**			
SA	0.90	0.20	0.39	0.22	0.55	0.74	0.34	**0.95**		
BR	1.00	0.53	0.33	0.30	0.20	0.18	0.15	0.16	**1.00**	
FN	0.73	0.67	0.58	0.45	0.22	0.26	0.26	0.30	0.31	**0.86**

참고: 음영으로 표시된 대각선의 계수는 AVE값을 제곱근 한 값임.

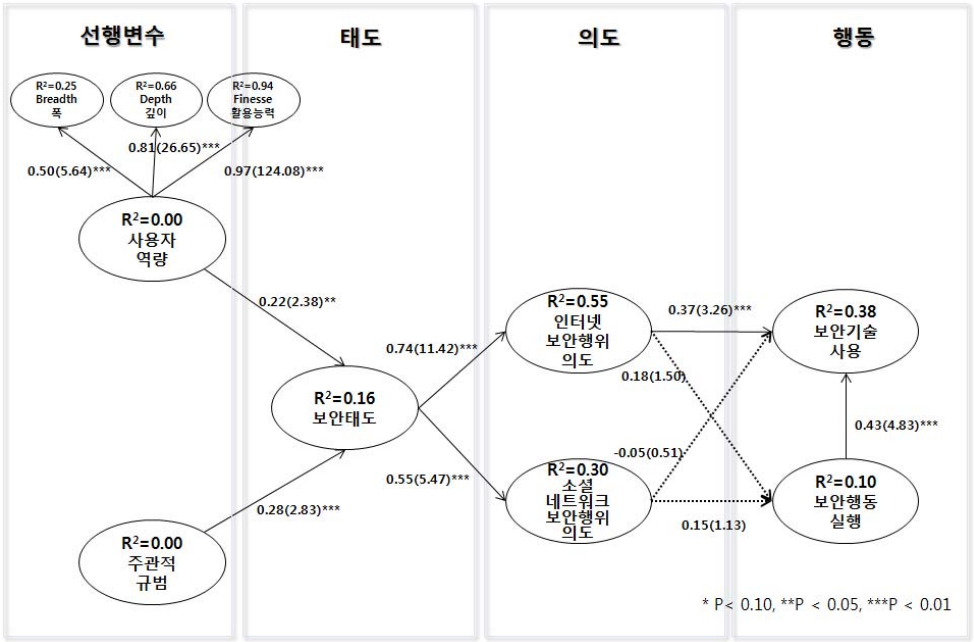
인에 적재된 로딩값들이 다른 요인에 적재된 크로스 로딩값 보다 모두 높기 때문에 판별타당성이 있다고 할 수 있다. 또한 모든 구성개념에 대한 평균분산추출값(AVE)의 제곱근이 다른 구성 개념과의 상관계수보다 커야한다고(Gefen et al., 2003) 제시하였다. <표 6>에서 음영으로 표시된 대각선 부분에는 변수의 평균분산추출값(AVE)의 제곱근 값을 나타냈는데, 이들은 다른 변수들과의 상관관계 값보다 모두 크다는 것을 알 수 있다. 따라서 본 연구의 측정도구는 판별타당성을 갖추고 있다고 볼 수 있다.

4.5 연구가설의 검증

본 연구의 가설에 대한 검증결과는 PLS 구조모형의 경로계수를 통해 분석되었다. 본 연구는 Williamson(1993)의 반영적 2nd-Order Construct 처리방법 중 계층적 성분 접근법으로 처리하였다. PLS에서는 구조방정식의 측정치로서 R^2가 보고된다. 이는 회귀분석에서 얻어지는 R^2와 유사한 것으로서 구조방정식에 포함된 독립변수에 의해 설명되는 종속변수의 분산의 양을 의미하며, R^2가 높을수록 구조방정식모형이 잘 수립되었다고 볼 수 있다. PLS 경로모형을 분석한 결과는 <그림 2>과 같다.

본 연구의 가설검증에 대한 요약은 다음과 같다.

가설 1의 “사용자의 역량은 보안태도에 정(+)에 영향을 미칠 것이다.” 라는 가설은 유의수준 95%에서 통계적으로 유의한(H1; β=0.22, t=2.38, p < 0.05) 관계가 있는 것으로 분석되어 해당 가설은 채택되었다. 이는 컴퓨터, 인터넷, 소셜 네트워크, 엑셀, 데이터베이스, 워드프로세싱, 그래픽처리에 대한 지식유무와 수준, 활용능



<그림 2> 연구분석 결과

력이 보안과 관련된 태도에 영향을 주고 있다는 것을 보여주고 있다.

가설 2의 “주관적 규범은 보안태도에 정(+)에 영향을 미칠 것이다.”라는 가설은 유의수준 99%에서 통계적으로 유의한(H2; β=0.28, t=2.83, p < 0.01) 관계가 있는 것으로 분석되어 해당 가설은 채택되었다. 이러한 결과는 자신의 동료 또는 자신의 영향을 받는 사람들의 기대에 의해 행동을 취하는 보이지 않는 규범이 보안과 관련된 태도에 영향을 주고 있다는 것을 보여주고 있다.

가설 3의 “보안과 관련된 태도는 인터넷 보안행위의도에 정(+)에 영향을 미칠 것이다.”라는 가설은 유의수준 99%에서 통계적으로 유의한(H3; β=0.74, t=11.42, p < 0.01) 관계가 있는 것으로 분석되어 해당 가설은 채택되었다. 이러한 결과는 보안과 관련된 태도가 인터넷 사용에 있어서 자신의 인터넷을 보호하기 위한 보안조치와 같은 보안관련 행위를 하려는 의도가 충분히 있다고 판단된다.

가설 4의 “보안과 관련된 태도는 소셜 네트워크 보안행위의도에 정(+)에 영향을 미칠 것이다.” 라는 가설은 유의수준 99%에서 통계적으로 유의한(H4; β=0.55, t=5.47, p < 0.01) 관계가 있는 것으로 분석되어 해당 가설은 채택되었다. 이러한 결과는 보안과 관련된 태도가 소셜 네트워크 사용에 있어서 자신의 소셜 네트워크를 보호하기 위한 보안조치와 같은 보안관련 행위를 하려는 의도가 충분히 있다고 판단된다.

가설 5-1의 “인터넷 보안행위 의도는 보안기술사용에 정(+)에 영향을 미칠 것이다.” 라는 가설은 유의수준 99%에서 통계적으로 유의한(H5-1; β=0.37, t=3.26, p < 0.01) 관계가 있는 것으로 분석되어 해당 가설은 채택되었다. 이러한 결과는 인터넷을 보호하기 위한 보안조치와 같은 보안관련 행위는 행동으로 이어져 기술적인 부분의 보안행동을 할 것이라고 판단된다.

가설 5-2 “인터넷 보안행위 의도는 보안행동에 정(+)에 영향을 미칠 것이다.” 라는 가설은 유의한 영향(H5-2; β=0.18, t=1.50)을 미치지 않아서 가설이 기각되었다. 이러한 결과는 인터넷을 보호하기 위한 보안조치와 같은 보안관련 행위를 지각하고는 있지만 개인보안노력 강화와 보안행동실행은 이루어지지 않고 있음을 알 수 있었다. 이는 실제로 보안에 대한 걱정은 하고 있지만 행동으로 직접 이어지지 않고 있다는 것을 보여주고 있다.

가설 6-1 “소셜 네트워크 보안행위 의도는 보안행동실행에 정(+)에 영향을 미칠 것이다.” 라는 가설은 유의한 영향(H6-1; β=0.15, t=1.13)을 미치지 않아서 가설이 기각되었다. 이러한 결과는 소셜 네트워크를 보호하기 위한 보안조치와 같은 보안관련 행위를 지각하고는 있지만 개인보안노력 강화와 보안행동실행은 이루어지지 않고 있음을 알 수 있으며, 아직까지 소셜 네트워크에 대한 사용이 활발하게 이루어지고 있지 않음을 알 수 있었다.

가설 6-2 “소셜 네트워크 보안행위 의도는 보안기술사용에 정(+)에 영향을 미칠 것이다." 라는 가설은 유의한 영향(H6-2; β=-0.05, t=0.51)을 미치지 않아서 가설이 기각되었다. 이러한 결과는 소셜 네트워크를 보호하기 위한 보안조치와 같은 보안관련 행위를 지각하고는 있지만 기술적인 부분의 보안행동사용으로는 이어지고 있지 않음을 알 수 있다.

가설 7 “보안행동실행은 보안기술사용에 정(+)에 영향을 미칠 것이다.” 라는 가설은 유의수

<표 7> 가설 검증 결과

H	Paths	Coefficient	t-value	Support
1	사용자 역량 → 보안태도	0.22	2.38	채택
2	주관적 규범 → 보안태도	0.28	2.83	채택
3	보안태도 → 인터넷 보안행위 의도	0.74	11.42	채택
4	보안태도 → 소셜 네트워크 보안행위 의도	0.55	5.47	채택
5-1	인터넷 보안행위 의도 → 보안기술 사용	0.37	3.26	채택
5-2	인터넷 보안행위 의도 → 보안행동 실행	0.18	1.50	기각
6-1	소셜 네트워크 보안행위 의도 → 보안행동 실행	0.15	1.13	기각
6-2	소셜 네트워크 보안행위 의도 → 보안기술 사용	-0.05	0.51	기각
7	보안행동 실행 → 보안기술 사용	0.43	4.83	채택

준 95%에서 통계적으로 유의한(H7; β=0.43, t=4.83, $p < 0.05$) 관계가 있는 것으로 분석되어 해당 가설은 채택되었다. 이는 보안노력을 강화하기 위한 보안행동을 실행하는 사람은 개인용 컴퓨터의 바이러스 백신 프로그램이나 방화벽 사용 보안 업데이트, 암호화 기능 등 기술적인 부분의 보안기술 사용으로 이어지고 있음을 알 수 있다.

Ⅴ. 결 론

본 연구에서는 최종사용자를 중심으로 인터넷과 소셜네트워크의 개인정보보안에 대해 알아보고자 하였다. 선행변수인 사용자역량과 주관적 규범이 보안태도에 영향을 주며, 이러한 보안태도는 인터넷사용에 있어 보안 행위의도와 최근 많은 영역에서 활발하게 이루어지고 있는 소셜 네트워크에 대한 보안 행위 의도와의 관계를 살펴보았으며, 이러한 인터넷과 소셜 네트워크 행위는 보안을 직접 실행하는 행동과 보안기술적인 부분까지 사용하는 행동으로 나누어 살펴보았다

본 연구의 이론적 시사점은 개인정보 보안태도가 인터넷과 소셜 네트워크 보안행위의도에 영향을 주며 이는 행동으로 이어진다는 목적을 달성하기 위해 최종사용자를 대상으로 자료를 수집하여 실증 분석하였다. 또한 본 연구의 목적을 달성하기 위해 합리적 행동 이론(TRA)을 중심으로 개인의 의도가 특정 행동에 영향을 미치는 동기적 요인으로 개인이 행동을 완수하기 위해 기꺼이 시도한다든지, 실행 계획이 어느 정도 잘 수립되었는지에 대해 설명하는 이론을 살펴보았다. 분석한 연구 결과를 살펴보면 다음과 같다.

첫째, 선행변수인 사용자 역량인 컴퓨터, 인터넷, 소셜 네트워크 등 소프트웨어에 대한 지식 유무와 수준, 활용능력이 보안과 관련된 태도에 영향을 주며, 자신의 동료 또는 자신의 영향을 받는 사람들의 기대에 의해 행동을 취하는 보이지 않는 규범인 주관적 규범 또한 보안태도에 영향을 미치는 것으로 나타났다. 이는 사용자의 역량과 주관적 규범이 컴퓨팅를 보호하기 위한 보안과 관련된 태도인 보안 조치나 보안대책을

세우는 것이 중요하다 할 수 있다.

둘째, 보안과 관련된 태도는 인터넷 보안과 소셜 네트워크 보안 행위 의도에 영향을 미치게 된다. 인터넷과 소셜 네트워크(모바일, facebook, twitter)에 보안조치나 보안대책을 세우는 것은 개인 컴퓨터를 해커들로부터 보호하기 위한 미래행동이라 할 수 있다. 이러한 행위의도 중 인터넷 보안 행위 의도는 보안과 관련된 기술사용인 바이러스 백신프로그램설치나 스파이웨어방지 소프트웨어, 스팸필터링 기능, 방화벽사용, 보안 업데이트, 팝업창 차단 기능 등 기술적인 성과에 영향을 주는 것으로 나타났으며, 보안노력 강화와 보안걱정행동인 보안행동실행에는 유의성을 발견하지 못했다. 이는 인터넷이 우리 주변에서 너무 쉽게 일상적으로 접하게 되므로 해서 보안과 관련된 걱정행동과 보안에 대한 노력 강화에 특별한 신경을 쓰지 않고 인터넷을 실행하는 것으로 나타났다.

소셜 네트워크 보안 행위 의도는 보안기술사용과 보안행동 실행에서 모두 유의하지 않은 결과를 보였는데, 이는 아직도 소셜네트워크에 대한 사용에 있어서 한정된 부분에서 사용되어지고 있으며, 소셜 네트워크에 대한 보안의식을 많이 인식하고 있지 않다고 볼 수 있다. 또한 기존의 선행연구에서는 인터넷과 컴퓨터를 중심으로 연구되어진 반면 본 연구에서는 소셜 네트워크를 추가하여 연구하므로 해서 변화하는 기술의 적용을 알아보았다.

셋째, 선행연구인 사용자 역량이 보안행동인 보안기술사용과 보안행동실행에 모두 유의한 결과를 가져왔다. 이는 사용자 역량이라는 태도가 직접적으로도 보안기술사용과 보안행동 실행에 영향을 미치는 것을 알 수 있다. 또한 보안행동실행이 보안기술사용에도 영향을 미치는 것으로 나타났다. 이는 보안에 대한 노력 강화와 보안 적정 행동이 보안을 실행하는 기술적인 부분으로 이어져 보안행동이 적용되고 있음을 시사하고 있다.

이상과 같은 연구결과를 토대로 다음과 같은 실무적 시사점을 제공할 수 있다.

첫째, 컴퓨팅 사용에 대한 활용범위, 수준, 활용능력인 사용자역량은 보안과 관련된 태도에 영향을 주며 이러한 소프트웨어에 관한 지식수준과 태도는 개인 사용자가 새로운 문제를 해결하기 위해 또는 업무에 접하게 되는 문제해결을 위해 컴퓨터와 소프트웨어 패키지를 얼마나 능숙하게 다루는지에 영향을 주는 것을 의미하므로 개인 사용자의 역량에 따라 보안조치와 보안대책에 대한 지침서의 사용 및 교육이 이루어져야 개인 보안에 대한 피해를 최소화 시킬 수 있다.

둘째, 보안과 관련된 태도는 인터넷 보안행위 의도와 소셜 네트워크 보안행위의도에 영향을 주는데 해커들로부터 인터넷과 소셜 네트워크의 개인정보를 보호하기 위해서는 인터넷과 소셜 네트워크의 특성이 다르며 개인 사용자의 보안행동에도 다른 특성을 보인다. 이는 각각의 특성에 맞는 적절한 보안대책과 보안조치를 통해 보안행동과 보안 기술사용이 필요할 것이다. 또한 인터넷과 소셜 네트워크 보안행위 의도는 보안에 대한 걱정은 하지만 실질적으로 보안행동으로 이어지지 않고 있다는 것이며 이는 보안을 유지할 수 있는 암호화, 보안 업데이트, 백신 프로그램, 주기적인 암호변경 등 지속적인 보안 노력 강화가 필요하다.

이러한 연구 과정에서 나타난 연구의 한계점

과 향후 연구에 대한 몇 가지 방향을 제시해 볼 수 있다.

첫째, 개인보안 성과에 대한 기존 연구들을 바탕으로 본 연구에 맞게 수정하고 일부 구성항목에 대한 측정항목을 개발하여 사전 조사를 통해 측정항목의 정교화 과정을 거쳤으나 변수 측정의 정교성이 떨어져 변수 중 삭제된 변수(SPT8, SPB1, SPB2)가 발생하였다. 그러므로 후속 연구를 통해 더 정교화 할 필요성이 있으며, 본 연구에서 제시된 구성요인 이외에 추가적인 구성요인에 관한 연구가 이루어져야 할 것으로 보인다.

둘째, 본 연구의 인구 통계적 특성에 따르면 응답자의 연령 중 18-29세가 80.8%로 차지하는 비중이 매우 높게 나타났다. 물론 소셜 네트워크를 사용하는 연령층이 젊은층에 집중되어 있으므로 10-20대의 젊은층이나 대학생이 높을 수는 있지만 30-40대의 직장인 등 다양한 계층의 사람들을 연구대상으로 하지 못했다는 점에서 연구의 결과를 일반화 시키는 데에 한계가 있으며 추후 연구에서는 다양한 연령과 직업의 표본을 확보하여 조사가 이루어질 필요가 있다.

참고문헌

교육과학기술부, 교육과학기술부 및 각급기관 웹사이트 개인정보 노출방지 가이드라인(개정판), 2008.

김동원, “개인정보수집에서 프라이버시와 경쟁가치들의 경합과 균형,” 정보화정책, 제10권, 제4호, 2003, pp.73-91.

김용재, “정보보안을 위한 내부통제 진단 모델 연구,” 금오공과대학교 석사학위논문, 2009.

김종기, “패스워드의 정보시스템 보안효과에 영향을 미치는 요인에 관한 연구,” 경영정보학연구, 제18권, 제4호, 2008, pp.1-26.

김진완, 홍태호, “지식검색 서비스에서 집단지성 품질이 지속사용 의도에 미치는 영향: 기대일치이론과 신뢰를 중심으로,” 정보시스템연구, 제20권, 제4호, 2011, pp.1-22.

김효준, 곽기영, “조직 내 중심성이 IT활용능력에 미치는 영향: 소셜 네트워크 관점,” 정보시스템연구,” 제20권, 제1호, 2011, pp.147-169.

남기효, 박상중, 강형석, 남기환, 김성인, “개인정보보호기술의 최신 동향과 향후 전망,” 한국정보보호학회, 제18권, 제6호, 2008, pp.11-19.

박기정, “학생들의 세금회피에 대한 태도, 주관적규범, 의도에 관한 연구,” 교육이론과 실천, 경남대학교 교육문제연구소, 1998, pp.249-263.

박혜정, “수입 캐주얼의류 구매에 대한 태도, 주관적 규범 의도에 관한 연구,” *Journal of the Korean Society of Clothing and Textiles*, 제26권, 제12호, 2002, pp.1791-1803.

손동원, 사회 네트워크 분석, 경문사, 2002.

이정호, 전자금융 침해사고 예방 및 대응 방안, 정보보호학회지, 제18권, 제5호, 2008, pp.1-20.

이종구, 조형제, 정준영외, 정보사회의 이해, 서울 미래 M&B, 2005.

이준택, 정보보호학 개론, 생능출판사, 2007.

이향우, “개인정보 보호와 공유자원 관리,” 사이버커뮤니케이션학보, 통권 제17호, 2006, pp.163-192.

차인환, “정보보안에서의 인원보안 관리지표 개발을 위한 실증적 연구,” 광운대학교 박사학위논문,” 2009,

행정안전부 “온라인 소셜네트워크 환경에서의 보안위협과 시사점,” 기술보고서, 2008.

홍광표, “ERP 사용자의 조직시민행동과 확장이용의도 간의 관계에 영향을 미치는 요인에 관한 연구,” 정보시스템연구, 제20권, 제1호, 2011, pp.75-105.

Adam, M., "Moving Toward Black Hat Research in Information Systems Security: An Editorial Introduction to The Special Issue," *MIS Quarterly*, Vol.34, No.3, 2010, pp.431-433.

Ajzen, I., and Fishbein, M., *Belief, Attitude, Intention, and Behavior: An Introduction to Theory an Research*, Reading, MA: Addison-Wesley, 1975.

Ajzen, I., and Fishbein M., "Attitude-Behavior Relation: A Theoretical Analysis and Review of Empirical Research," *Psychological Bulletin*, Vol.84, No.5, 1997, pp.888-918.

Ajzen, I., and Fishbein, M., *Understanding Attitudes and Pprediction Social Behavior*, Englewood Cliffs, NJ: Prentice Hall, 1980.

Albrechtsen, E., "A Qualitative Study of Users' View on Information Security," *Computers & Security*, Vol.26, No.4, 2007, pp.276-289.

Angel I., "Computer Security in these Uncertain Times: The Nneed for a New Approach," *In: Proceedings of the 10th International Conferences on Computer Security*, Audit and Control (CompSec), London, 1993.

Armitage, C. J., and Conner, M., "Efficacy of the Theory of Planned Behavior: A Meta-Analytic Review," *British Journal of Social Psychology*, Vol.40, No.4, 2001, pp.471-499.

Baldwin, N. S., and Rice, R. E., "Information-Seeking Behavior of Securities Analysis: Individual Institutional Influences, Information Sources and Channels and Outcomes," *Journal of The American Society for Information Science*, Vol.48, No.8. 1997, pp.674-693.

Bansal, H. S., *Service Switching Model(SSM): A Model of Customer Switching Behavior in the Service Industry*, Queen’s University, in Canada, Dissertation paper, 1997.

Brown, S. A., and Venkatesh, V., "Model of Adoption of Technology in Households: A Baseline Model Test and Extension Incorporating Household Life Cycle," *MIS Quarterly*, Vol.29, No.3, 2005, pp.399-426.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I., "Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security

Awareness," *MIS Quarterly*, Vol.34, No.3, 2010, pp.523-548.

Catherine, L., A., and Ritu, A., "Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions," *MIS Quarterly*, Vol.34, No.3, 2010, pp.613-644.

Chin, W. W., *The Partial Least Squares Approach to Structural Equation Modeling, in Marcoulides*, G.A.(Eds), Modern Methods for Business Research, Lawrence Eelbaum Associates, Mahwah, NJ, 1998a.

Choi, N. J., Kim, D., Goo, J. Y., and Andrew W., "Knowing Is Doing: An Eempirical Validation of the Rrelationship between Managerial Information Security Awareness and Action," *Information Management & Computer Security* Vol.16, No.5, 2008, pp.484-501.

Davies, S., "Re-Engineering the Right to Privacy: How Privacy Has Been Transformed from a Right to a Commodity," In P. Agre and M. Rotenberg(ed.), *Technology and Privacy*, 1998.

Davis, F. D, Bagozzi, R. P., and Warshaw, P. R., "User Acceptance of Computer Technology: A Ccomparison of Two Theoretical Models," *Management Science*, Vol.35, No.8, 1989, pp.982-1003.

Dubbeld, L., "The Role of Technology in Shaping CCTV Surveillance Practices," *Information Communication & Society*, Vol.8, No.1, 2005, pp.84-100.

Eagly, A. H., and Caiken, S., *The Psychology of Attitudes*, Harcourt Brace Jovanvich. TX: Forth Worth, 1993.

Engel, J. F., Blackwell, R. D., and Miniard, P. W., *Consumer Behavior: International Edition* (8 ed.), Forth Worth: The Dryden Press, 1995.

Fiske, S. T., and Taylor, S. E., *Social Cognition*, NY: McGraw-Hill, Inc, 1991.

Fornell, C. R., and Larcker, D. F., "Sturctural Equation Models with Unobservable Variables and Measurement Error," *Journal of Marketing Research*, Vol.18, No.3, 1981, pp.312-325.

Gefen, D., Karahanna, E., and Straub, D. W., "Trust and TAM in Online Shopping: An Integrated Model," *MIS Quarterly*, Vol.27, No.1, 2003, pp.51-90.

Goodhue D., and Straub, D., "Security Concerns of System Users: A Study of Perception of the Adequacy of Security," *Information & Management*, Vol.20, No.1, 1991, pp.13-27.

Harison, E., and Boonstra, A., "Essential Competencies for Technochange Management: Towards an Assessment Model," *International Journal of Information Management*, Vol. 29, No.4, 2009, pp.283-294.

Jaime T., William J., and Benjamin B. B., "Personal Information Management,"

Communications of the ACM , Vol.49, No.1, January 2006, pp.412-425.

Janine, L., "User Participation in Information System Security Risk Management," *MIS Quarterly*, Vol.34, No.3, 2010, pp.503-522.

Johnston, A. C., and Warkentin, M., "Fear Appeals and Information Security Behaviors: An Empirical Study," *MIS Quarterly*, Vol.34, No.3, 2010, pp.548-566.

Ina o'merchu, Jahn, G. B., and Stefan, D., *Online Social and Business Networking Communities*, Digital Enterprise Research Institute Technical Report, 2004.

King, R. C., and Xia, W., "Media Appropriateness: Effects of Experience on Communication Media Choice," *Decision Sciences*, Vol. 28, No.4. 1997, pp.877-910.

Lee, C., and Green, R. T., "Cross-Cultural Examination of the Fishbein Behavioral Intention Model," *Journal of International Business Studies*, Vol.22, No.2, 1991, pp.289-305.

Lee, S. M., and Kim, Y. R., and Lee, J., "An Empirical Study of the Relationships among End-User Information Systems Acceptance, Training and Effectiveness," *Journal of Management Information Systems*, Vol.12, No.2. 1995, pp.189-202.

Lee, Y., and Kozar, K. A., "Investigating Factors Affecting the Adoption of Anti-Spyware Systems," *Communications of the ACM* , Vol.48, No.8, 2005, pp.72-77.

Liang. H., and Xue. Y., "Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective," *Journal of the Association for Information Systems*, Vol.11, No.7, 2010, pp.394-413.

Marrelli, A., "An Introduction to Competency Analysis and Modeling," *Performance Improvement*, Vol.37, No.5, 1998, pp.8-16.

Mathieson, K., "Predicting User Intentions: Comparing the Technology Acceptance Model with the Theory of Planned Behavior," *Information Systems Research*, Vol.2, No.3, 1991. pp.173-191.

McArthur, L. Z., Kiesler, C. A., and Cook, B. P. "Acting on an Attitudes as a Function of Delf-Percept and Iinequity," *Journal of Personality and Social Psychology*, Vol.12, No.1, 1969, pp.295-302.

McClelland, D., "Testing for Competence Rather than for Intelligence," *American Psychologist*, Vol.28, No.1, 1973, pp.1-14.

McLagan, P., *Models of HRD Practice*, ASTD Press, 1989.

Mikko, S., "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations" *MIS Quarterly*, Vol.34, No.3, 2010, pp.487-502.

Munro, M. C., Huff, S. L., and Marcolin, B. L., and Compeau, D. R., "Understanding and Measuring User Competence," *Information & Management*, Vol.33, No.1, 1997, pp.45-57.

Ostrom, E., Private and Common Property Rights, On-line, Available : http://allserv.rug.ac.be/~gdegeest/2000book.pdf, 2002.

Parry, S., "The Quest for Competencies," *Training*, Vol.33, No.7, 1996, pp.48-56.

Ploeg, I. V. D., "Biometrics and Privacy," *Information Communication & Society*, Vol.6, No.1, 2003, pp.85-104.

Regan, P., "Privacy As a Common Good in the Digital World," *Information Communication & Society*, Vol.5, No.3, 2002, pp.382-405.

Rhee, H. S., and Kim, C. T., and Young U. R., "Self-efficacy in Information Security: Its Influence on End Users' Information Security Practice Behavior," Science Direct, C*omputers & Security*, Vol.28, No.8, 2009, pp.816-826.

Rholes, W. S., and Bailey, S. "The Effects of Level of Moral Reasoning on Consistency between Moral Attitudes and Related Behaviors," *Social Cognition*, Vol.2, No.1, 1983, pp.32-48.

Scott, W., "Consumer Socialization," *Journal of Consumer Reserch*, Vol.1, No.2, 1974, pp.2-3.

Sheeran, P., and Taylor, S., "Predicting Intentions to Use Condoms: Meta-Analysis and Comparison of the Theories of Reasoned Action and Planned Behavior," *Journal of Applied Social Psychology*, Vol.29, No.3, 1997, pp.1624-1675.

Smith B., Caputi P., and Rawstorne P., "Differentiating Computer Experience and Attitudes toward Computers: An Empirical Investigation," *Computers in Human Behavior*, Vol.16, No.1, 2000, pp.59-81.

Spencer, L., and Spencer, S., *Competence at Work: A Model for Superior Performance*, New York : Wiley, 1993.

Tenenhaus, M., Vinzi, V. E., Chatelin, Y. M., and Lauro, C., "PLS Path Modeling," *Computational Statistics & Data Analysis*, Vol.48, No.1, 2005, pp.159-205.

Torkzadeh, G. and Lee, J., "Measures of Perceived End-User's Computing Skills," *Information and Management*, Vol.40, No.7, 2003, pp.607-615.

Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D., "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly*, Vol.27, No.3, 2003, pp.425-478.

Warren, S. D., and Brandeis, L. D., "The Right to Privacy," *Harvard Law Review*, Vol.4, No.5, 1890, pp.193-220.

Weiss, S., "Online Social Networks and the Need for New Privacy Research in Information and Communication Technology," *Third*

International Summer School Organized by IFIP WG 9.2, 9.6/117, 11.6, 2007.

Westin, A., *Privacy and Freedom*, NY: Atheneum, 1967.

Whitaker, R., *The End of Privacy: How Total Surveillance is Becoming a Reality*, New York: New Press, 1999.

Williamson, O. E., "Calculativeness, Trust, and Economic Orhanization," *The Jouranl of Law & Economics*, Vol.34, No.1, 1993, pp.453-502.

Winter, S. J., Chudoba, K. M., and Gutek, B. A., "Attitudes Toward Computers: When Do They Predict Computer Use?," *Information & management*, Vol.34, No.5, 1998, pp.275-284.

KISA, http://www.kisa.or.kr, 2010.

박경아(Park, Kyung-Ah)

현재 조선대학교 경영학과 MIS 전공 박사과정 중이며, 조선대학교 경영학부 시간강사로 재직 중이다. 한국지식경영학회, 한국경영정보학회, 한국정보시스템학회, 한국산업경제학회 등의 학술지에 논문 게재와 발표하였다. 연구 관심 분야는 정보보안, 소셜네트워크, 정보윤리이다.

이대용(Lee, Dae-Yong)

전남대학교 경영학과를 졸업하고, University of Iowa에서 박사학위를 취득하였다. 현재 조선대학교 경영학부 교수로 재직 중이다.

Decision Support Systems, 경영정보학회지, 대한경영학회지 등의 학술지에 논문을 게재해 왔으며, 한국경영정보학회 등의 학회에서 다수의 논문을 발표하였다. 연구 분야는 전자상거래, 스프레드시트, 비즈니스 게임, 의사결정지원시스템이다.

구철모(Koo, Chul-Mo)

경희대학교 호텔관광대학 컨벤션경영학과에 조교수로 재직 중이다. 서강대학교에서 경영학박사를 취득한 후, 미네소타 대학 MISRC 연구원, Marshall University 교수, 조선대학교 교수직을 재직하였다. 주요 관심분야는 관광산업과 환대산업의 IT 역할과 효과에 대한 연구를 수행중이다. 주요 논문을 국제학술지와 국내학술지에 게재하고 있다.

<Abstract>

An Empirical Study about Internet and Social Network Security Behavior of End User

Park, Kyung-Ah · Lee, Dae-Yong · Koo, Chul-Mo

The purpose of this study was to find about personal information security of internet and social networks by focusing on end users. User competence and subjective criterion, which are the antecedents, are affecting security behaviors For these security behaviors, the study examined the relationship between security behavior intention on internet use and security behavior intention about social network that is actively achieved in many fields. Behaviors of internet and social network were classified into an action of executing security and an action of using a security technology. In addition, this study investigated a theory about motivational factors of personal intention on a certain behavior based on theory of reasoned action in order to achieve the purpose of this study. A survey was conducted on 224 general individual users through online and offline, and the collected data was analyzed with SPSS 12.0 and SmartPLS 2.0 to verify demographic characteristics of respondents, exploratory factor analysis, and suitability of a study model. Interesting results were shown that security behavior intention of social network is not significant in all security behavior execution, which is security performance behavior, and security technology use. Internet security behavior is significant to security technology use but it does not have an effect on behavior execution.

Keywords : Social Network, User Competency, Subjective Norm, Security Practice-Technology Aspect, Security Conscious Care Behavior

* 이 논문은 2012년 3월 20일 접수되어 1차수정(2012년 5월 18일)을 거쳐 2012년 6월 27일 게재 확정되었습니다.