http://www.jsebs.org
ISSN: 2288-3908

The Journal of Society for e-Business Studies
Vol.20, No.4, November 2015, pp.151-175
http://dx.doi.org/10.7838/jsebs.2015.20.4.151

정보보안기술 사용의 영향요인에 관한 실증적 연구

An Empirical Study on Influencing Factors of Using Information Security Technology

김상훈(Sang-Hoon Kim)*, 이갑수(Gab-Su Lee)**

초 록

조직의 정보보안을 위해서는 세 가지 유형의 정보보안(기술적, 물리적 및 관리적 보안) 모두가 중요하며 병행 추진되어야 할 것이지만, 본 연구는 관리적 보안대책의 수립 및 추진의 효과성을 보다 높이기 위한 이론적 근거를 확보하는데 연구목표를 설정하였다. 즉, 기술적 및 물리적 보안대책이 철저하게 정비되고 추진된다고 하더라도 이를 준수하고 실행하는 주체는 결국 조직구성원들이므로 기술적 및 물리적 보안대책이 소기의 성과를 이루기 위해서는 이에 부응한 관리적 보안대책이 균형 있게 추진되는 것이 필수적이기 때문에 관리적 보안을 보다 효과적으로 수행할 수 있기 위한 이론적 근거를 확보하는 것은 매우 중요한 의미를 지닌다고 본다.

특히, 본 연구에서는 효과적인 관리적 보안대책의 수립・추진의 핵심과제라고 할 수 있는 조직구성원들의 정보보안기술 사용의도를 향상시키기 위한 방안 마련 시에 적용될 수 있는 이론적 모형을 개발・제시하고자 하였다. 이를 위해 정보보안기술 사용의도에 영향을 미치는 요인들을 주요 관련 이론 및 선행연구들에 대한 체계적 고찰을 통해 도출하고 이들 간의 인과적 관계를 논리적으로 추론함으로써 연구모형 및 가설을 도출하였다. 실증분석을 위해서는 국내 대기업들의 직원들을 대상으로 현장서베이를 통한 자료수집을 하였고 부분최소자승법(PLS: Partial Least Squares)기법에 의한 구조방정식 모형분석을 실시하였다. 본 연구의 유의한 결과는 이론적인 측면에서 관리적 정보보안 분야 연구의 외연을 확대하는데 기여할 수 있다고 보며, 실무적인 측면에서는 제반 조직들이 관리적 정보보안 방안 및 대책 수립을 함에 있어서 업무지침의 일부로 적용될 수 있을 것으로 예상된다.

ABSTRACT

Although three types of the information security measures (technical, physical and managerial ones) are all together critical to maintaining information security in the organizations and should be implemented at the same time, this study aims at providing theoretical basis of establishing and implementing effective managerial security measures. The rationale behind this research objective is that it is very important to effectively perform the managerial security measures to achieve the target performance level of the technical and the physical security measures because main agents of practicing the information

이 논문은 2014년도 광운대학교 교내학술연구비 지원에 의해 연구되었음.
* Corresponding Author, School of management, Kwangwoon University(shk5432@gmail.com)
** Co-Author, Consulting Team 1, SK infosec(gslee@skinfosec.co.kr)
Received: 2015-09-23, Review completed: 2015-10-20, Accepted: 2015-11-06

security measures in the organizations are staff members even though the technical and the physical ones are well constructed and implemented.

In particular, this study intends to develop and propose the theoretical model applicable to providing the way of improving organizational members' intention to use information security technologies since the very intention to use them is essential to effectively establishing and promoting managerial security measures. In order to achieve the objective of this study, the factors critical to influencing upon the intention to use information security technologies are derived through systematically reviewing related theories and previous studies, and then the research model and hypotheses are proposed by logically reasoning the casual relationship among the these factors. Also, the empirical analyses are performed by conducting the survey of the organization members of domestic large companies and analyzing the structural equation model by PLS (Partial Least Squares) method. The significant results of this study can contribute to expanding the research area of managerial information security and can be applied to suggesting the practical guidelines for effectively establishing and implementing the managerial security measures in various organizations.

키워드 : 정보보안기술, 관리적 보안대책, 사용의도
Information Security Technologies, Managerial Security Measures, Intention to Use

1. 서 론

정보보안에 대하여 정보화촉진기본법 제2조(정의)에서는 '정보의 수집·가공·저장·검색·송신·수신 중에 정보의 훼손·변조·유출 등을 방지하기 위한 관리적·기술적 수단을 강구하는 것'이라고 명시하고 있으며, 정보보호기술 전문용어사전[31]에서는 '정보의 수집·가공·저장·송신·수신 도중에 정보의 훼손·변조·유출 등을 방지하기 위한 관리적·기술적 수단 또는 그러한 수단으로 이루어지는 행위로서, 내·외부의 위협요인들로부터 네트워크, 시스템 등의 H/W와 S/W, 데이터베이스, 통신 및 전산시설 등 정보자산을 안전하게 보호·운영하기 위한 일련의 행위'로 정의하고 있다.

정보보안에 대한 위와 같은 정의의 내용 중 '정보의 수집·가공·저장·송신·수신 도중에 정보의 훼손·변조·유출 등을 방지'라는 말은 정보보안의 목적으로 시스템 및 정보의 '기밀성(Confidentiality)', '무결성(Integrity)', '가용성(Availability)', '인증성(Authentication)', '부인방지(Non-repudiation)'를 확보하는 것을 의미한다[25]. 우선 기밀성(Confidentiality)이란 정보가 인가된 자에 의해서만 접근이 가능해야 한다는 원칙이다. 즉, 정보는 소유자의 인가를 받은 사람만이 알아야 하며 인가되지 않은 사람에 의한 정보의 공개는 절대로 방지되어야 함을 의미한다. 또한 무결성(Integrity)이란 정보는 정해진 절차에 의해 그리고 주어진 권한에 의해서만 변경될 수 있다는 것을 의미한다. 즉, 정보는 항상 일정하게 유지되어야 하며 단지 인가 받은 방법에 의해서만 변경될 수 있으며 우발적이건 고의적이건 간에 허가 없이 변경되어서는 안 됨을 의미한다. 가용성(Availability)이란 정보시스템이 적절한 방법으로 작동되어야 하며, 적법한 방법으로 권한이 주어진 사용자에게 정보서비스가 거부되어서는 안 된다는

것이다. 또한 다양한 응용 프로그램별로 적정한 반응시간이 요구된다. 교통통제나 병원의 응급 시스템, 금융시스템과 같이 트랜잭션 자체가 민감한 경우에 적시적절하게 시스템을 사용할 수가 없다면 그 정보는 이미 소유의 의미를 잃게 되거나 정보자체의 가치를 상실하게 되고 나아가 2차적인 인적, 금전적 피해를 일으키게 된다. 인증성(Authentication)이란 정보교환에 의해 실체의 식별을 확실하게 하거나 임의 정보에 접근할 수 있는 개체의 자격이나 객체의 내용을 검증하는데 사용되는 성질을 말하며, 정보시스템의 부당한 사용이나 정보의 부당한 전송 등을 방어하는데 사용된다. 부인방지(Non-repudiation)란 행위나 이벤트의 발생을 증명하여 나중에 그런 행위나 이벤트를 부인할 수 없도록 하는 것으로서, 정보보안의 방법에 의하여 데이터의 송수신자가 송수신 사실을 부인하지 못하도록 방지하는데 사용된다.

이상과 같은 정보보안의 목적을 달성하기 위하여 정보보안을 위한 업무 수행범위는 기술적, 물리적, 관리적 보안의 세 가지 측면을 포함한다. 우선 기술적 보안은 정보시스템, 통신망, 정보(데이터)를 보호하기 위한 가장 기본적인 대책으로서 정보보호 솔루션을 이용한 정보시스템 접근통제, 저장된 데이터나 송신 및 수신 중에 데이터를 은폐하는 암호기술 적용, 재난 복구를 대비하기 위한 백업 체제, 정보시스템 자체에 보안성이 강화된 시스템 소프트웨어 사용 등이 이에 속한다. 물리적 보안은 화재, 수해, 지진, 태풍 등과 같은 자연재해로부터 정보시스템이 위치한 정보처리시설을 보호하기 위한 자연 재해대책과 조직내부 불순 세력이나 적의 파괴로부터 정보시스템을 보호하기 위한 출입통제, 시건장치 등의 물리적 보안대책으로 구분된다. 관리적 보안은 법・제도・규정・교육 등을 확립하고, 보안계획을 수립하고 이를 운용(보안 등급, 엑세스 권한 등)하며, 위험분석 및 보안감사를 시행하여 정보시스템의 안전성과 신뢰성을 확보하기 위한 대책이다. 조직의 정보보안을 효과적으로 보장하기 위해서는 다양한 기술적 및 물리적 보안대책 뿐만 아니라 이들을 계획하고 설계하며, 관리하기 위한 제도와 정책 및 절차 등의 관리적 보안대책도 매우 중요하다[21, 25].

본 연구는 위의 세 가지 정보보안 활동 영역 중 관리적 보안에 초점을 두며, 관리적 보안업무에서 핵심사항들 중 하나인 조직구성원들의 정보보안의지 및 능력 강화를 위한 정책 수립 및 방안 마련을 위한 이론적 근거를 제공하는데 목표를 둔다. 조직구성원들의 정보보안의지 및 능력은 조직구성원 개개인이 정보보안을 위해 일상 업무에서 조직이 제공하고 있는 정보보안기술을 얼마나 적극적으로 사용하는가에 의해 좌우될 것으로 판단되며, 이에 본 연구는 조직행태적 연구접근방법에 기반하여 조직구성원들의 정보보안기술 사용에 영향을 미치는 요인들을 제반 관련 이론들의 통합적 고찰을 통해 이론적으로 도출하고 현장 서베이 조사를 통해 도출된 요인들을 실증적으로 확인하고자 한다.

이와 같은 연구목표를 달성하기 위하여 본 연구의 구성은 서론(제1장)에 이어서 제2장에서는 조직구성원들이 정보보안기술을 사용하는데 영향을 미치는 요인들을 이론적으로 도출하기 위한 논리적 근거가 될 수 있는 주요 선행이론들을 고찰하고, 제3장에서는 주요 선행이론들 간의 연관관계를 고려한 논리적 추론과정(Logical Reasoning)을 통해 연구모형

과 가설을 도출하고, 제4장에서는 실증분석을 위한 연구 설계방안을 제시한다. 그리고 제5장에서는 수집된 자료에 대한 통계적 분석을 통한 연구모형 및 가설검증을 실시하고, 제6장에서는 결론 및 연구의 한계점 등을 논하기로 한다.

2. 주요 선행이론 고찰

2.1 합리적 행동이론(Theory of Reasoned Action)

합리적 행동이론은 Fishbein[13]의 기대-가치(Expectancy-Value) 이론을 확장하여 정립된 이론으로서 사회심리학에서 오랫동안 지지되어 온 이론으로서 인간의 행동을 예측하는데 이용되었다[14]. 인간의 행동(Behavior)을 결정하는 요소는 행동의도(Behavioral Intention)이며, 행동의도는 다시 2가지 선행요인에 의해서 결정이 되는데, 그것은 태도(Attitude)와 주관적 규범(Subjective Norm)이다. 태도(Attitude)란 '행위를 수행하는 것에 대한 개인의 긍정적 또는 부정적인 느낌'이며, 주관적 규범(Subjective Norm)이란 '행위를 수행하는 것이 다른 사람들에게 중요한 것인지에 대한 개인의 인식'으로 보고 있다.

그러나 여러 실증적 연구를 통해 나타난 합리적 행동이론의 한계점은 서로 영향을 미치지 않는다고 본 태도(Attitude)와 주관적 규범(Subjective Norm)이 추후의 연구에서는 둘 간에 영향관계가 있음이 실증적으로 나타난 점이며, 태도(Attitude)와 규범(Subjective Norm)의 두 요인만으로는 행동에 대한 설명력이 모자란 것도 한계점으로 지적되었다[5, 6, 35, 36, 37, 38].

2.2 계획된 행동이론(Theory of Planned Behavior)

Ajzen[2, 3]의 계획된 행동이론은 합리적 행동이론[14]을 확장한 연구로 인지된 행동통제(Perceived Behavioral Control) 요인을 추가하였다. 즉, 인간의 행동을 결정하는 데에는 행동의도와 인지된 행동통제가 선행변수로 영향을 미치며, 행동의도에는 태도, 주관적 규범, 그리고 인지된 행동통제가 영향을 미치게 된다고 보고 있다.

여기서 인지된 행동통제는 자원과 기회에 따른 통제신념(Control Belief)과 인지된 촉진(Perceived Facilitation)에 의하여 결정되는데 통제신념(Control Belief)이란 개인들이 자원과 기회의 가용성(Availability)을 지각하는 정도를 말하며, 인지된 촉진(Perceived Facilitation)은 결과를 얻는데 있어서의 이들 자원과 기회의 중요도에 대한 인식정도를 의미한다.

그러나, 이후의 연구자들에게서 인지된 행동통제의 특성과 측정에 문제가 있음이 지적됨에 따라 Ajzen[3]은 이 문제를 해결하기 위하여 인지된 행동통제를 인지된 통제성(Perceived Controllability)과 인지된 자기효능감(Perceived Self-Efficacy)의 두 가지 하위개념으로 나누었는데 인지된 자기효능감(Perceived Self-Efficacy)이란 '행동을 취하는데 요구되는 기술, 능력에 대한 자신감'이라고 말할 수 있으며[7], 인지된 통제성(Perceived Controllability)이란 '행동을 취하는데 요구되는 자원과 기회의 가용성에 대한 판단'이라고 할 수 있다[3].

2.3 기술수용모형(Technology Acceptance Model)

Davis[9]는 합리적 행동이론(Theory of Reasoned Action)을 발전시켜 기술수용모형(Technology Acceptance Model)을 제시하였는데, 이 이론적 모형을 통하여 사용자의 정보기술 수용과정을 잘 설명할 것으로 기대하였다. 또한, 기술수용모형이 넓은 의미로는 최종사용자 컴퓨팅(End-User Computing)환경에서 사용자의 행동을 잘 설명할 것이며, 연구모형의 간명성(Parsimony)과 이론적 정당성을 획득할 것으로 기대하였다. 기술수용모형에서 중요한 변수는 두 가지로, 인지된 유용성(Perceived Usefulness)과 인지된 사용 용이성(Perceived Ease of Use)이 있다. Davis[9]는 인지된 유용성(Perceived Usefulness)을 '조직 환경에서 해당 정보시스템의 사용으로 직무성과를 증대시킬 수 있다고 믿는 사용자의 주관적 평가정도'로 정의하였고, 인지된 용이성(Perceived Ease of Use)을 '사용자가 목표한 시스템을 많은 노력을 기울이지 않고도 이용할 수 있다고 기대하는 정도'로 정의하였다.

이어서 Davis et al.[10]은 기술수용모형에서 주요한 두 가지 신념 변수인 인지된 유용성과 용이성에 대한 측정도구를 개발하여 기업과 학교에 있는 152명의 사용자들에게 설문과 실험을 통하여 신뢰성과 타당성을 획득하였고, 인지된 사용용이성보다 인지된 유용성이 정보시스템 이용의도에 영향력이 크다는 것을 검증하였다.

그러나, Davis et al.[10]은 초기의 기술수용모형에서 포함되었던 '태도(Attitude)'변수의 매개적 역할이 미약하고, 인지된 유용성과 용이성이 행동의도에 직접적인 영향이 있음을 연구를 통하여 증명하고 '태도(Attitude)'변수가 제거된 기술수용모형을 제시하였고, 이 연구 이후의 다른 연구자들도 '태도(Attitude)'변수를 생략한 기술수용모형을 주로 연구하게 되었다[10, 20, 30, 32, 33, 34].

2.4 혁신확산이론(Innovation Diffusion Theory)

조직 내에서의 혁신의 수용·확산 현상을 설명하는데 중요한 이론인 Rogers[28]가 제시한 혁신확산이론에서는 혁신을 "정성적으로(Qualitatively) 기존과 다른 기술, 아이디어, 행동, 사물"로 정의하고 있으며, 확산에 대한 정의는 "사회 시스템(Social System)내의 구성원들 간에 시간이 경과되어 특정 경로(Channel)를 통하여 의사소통 되어지는 혁신(새로운 아이디어)과정"이라고 정의하고, 혁신은 일반적으로 5단계(지식단계(Knowledge) → 설득단계(Persuasion) → 결정단계(Decision) → 수행단계(Implementation) → 확정단계(Confirmation))를 거쳐서 확산이 된다고 주장하고 있다. 아울러, Rogers[28]는 혁신의 확산에 영향을 주는 요인들로서 상대적 이점(Relative Advantage), 호환성(Compatibility), 복잡성(Complexity), 시도성(Trialability), 관찰성(Observability) 등 다섯 가지의 요인들을 들고 있는데 상대적 이점(Relative Advantage)은 사용자에 의하여 기존의 것보다 혁신의 결과물이 더 낫다고 지각되는 정도를 의미하고, 호환성(Compatibility)은 사용자에 의하여 혁신의 결과물이 기존 것의 가치, 필요성, 경험 등과 일치되는 정도를 의미한다. 또한 복잡성(Complexity)는 사용자에 의하여 혁신이 이용하기가 어렵다고 지각

되는 정도를 의미하고, 시도성(Trialability)은 사용자에 의하여 혁신이 수용되기 이전에 시도 및 실험될 수 있는 정도를 말한다. 마지막으로 관찰성(Observability)이란 사용자에 의하여 혁신의 결과물이 타인(가족, 친구 등)들로부터 관찰될 수 있는 정도를 의미한다. 앞서 고찰한 Davis et al.[10]의 기술수용모델에서의 인지된 유용성과 인지된 용이성개념은 혁신확산을 구성하는 다섯 가지 특징 중 상대적 이점, 복잡성과 동일한 개념으로 사용되고 있는데 이는 기술수용모형이 Rogers[28]의 혁신확산이론으로부터 이들 요인들을 차용한 것임을 알 수 있다.

2.5 공포소구이론(Fear Appeal Theory)

앞서 고찰한 합리적 행동이론, 계획된 행동이론, 기술수용모델 및 혁신확산이론들은 모두 그 대상이 긍정적 기술(Positive Technology)이었다. 긍정적 기술(Positive Technology)이란 사용자들에게 생산성, 효율성, 경쟁력, 오락성 등의 혜택을 가져다주도록 만들어진 기술을 의미한다. 사용자는 이러한 혜택을 인지함으로써 기술의 필요성을 느끼게 된다[18].

그러나, 보안기술(Security Technology or Protective Technology)은 DoS(Denial of Service)나 맬웨어(Malware: Malicious Software) 등과 같은 보안을 위협하는 부정적 요소들에 대처키 위한 기술로서, 기존 이론들만으로는 정보보안 행동의도를 설명하기에는 한계가 있다. 왜냐하면 긍정적 기술(Positive Technology)을 사용할 경우에는 사용자에게 업무 효율성 및 오락적 혜택을 가져다주는 직접적인 효익이 뒤따르지만, 보안기술(Security Technology) 사용에서는 이와 달리 사용자에게 보안위협(Security Threat)을 막아주는 간접적인 효익만을 제공하기 때문이다. 즉, 사용자는 보안기술(Security Technology) 사용에 대하여 조직 내 사용자들은 일반적인 업무에 추가된 귀찮은 짐으로 느끼거나[18], 개인 사용자들은 짜증나는 일로 인지하는 경향이 있다[17].

따라서 정보보안기술 수용행태를 보다 명확히 규명하기 위해서는 사용자들에게 긍정적 기술(Positive Technology)과는 다르게 인지되는 보안기술(Security Technology)의 특성을 반영할 필요성이 크며, 이에 대한 이론적 근거를 기존의 사회심리학분야에서 활발히 연구되어 온 '공포소구이론(Fear Appeal Threory)'에서 찾을 수 있다고 본다.

공포(Fear)는 인간이 가지고 있는 기본적 감정의 하나로, 심각하고 개인에게 관계가 있는 위협(Threat)이 지각될 때 환기(Arousal)되는 심리적 차원과 생리적 차원으로 구성된 내적 감정반응이다[39]. 공포는 환기의 유발과 같은 생리적 표현, 말이나 글과 같은 언어적 표현, 그리고 얼굴의 표정 변화와 같은 행동적 표현 등 매우 다양하게 표현된다[23]. 또한, 공포는 부정적인 유발성(Valence)을 지닌 감정이기 때문에, 공포가 발생하게 되면 개인에게는 이것을 제거하기 위한 동기가 부여되는 것이 일반적이다.

일반적으로 "위협 기법(Scare Tactic)"으로 알려져 있는 공포소구(Fear Appeal)는 공익광고, 상품광고 등 설득 커뮤니케이션 분야에서 가장 널리 이용되고 있는 기법 중 하나이다. 에이즈예방 캠페인, 금연 캠페인, 비듬방지 샴푸 광고, 구강청정제 광고 등은 공포소구가 이용되고 있는 대표적인 사례라고 할 수가 있다. 이와 같은 공포소구는 특정한 행동을 하지 않음으로 해서 발생되는 부정적인 결과를 메시지

속에 제시하여 공포를 야기한다. 일반적으로 사람들은 그러한 부정적인 결과가 발생하는 것을 원하지 않을 뿐만 아니라, 그것을 경험하는 것 자체를 두려워하기 때문에 메시지에서 권고된 방향대로 행동할 가능성이 높다[43].

공포소구이론분야에서 현재까지 가장 지지를 높게 받고 있는 이론적 모델은 Witte[39]의 연구에서 제시된 “병행과정 확장모델(EPPM: Extended Parallel Process Model)”이다. 본 모델은 크게 두 단계로 나뉘는데 첫 단계는 사람들이 공포소구메시지를 접하게 되면 위협에 대한 평가와 권고된 대응의 효능감에 대한 평가를 수행하게 되는 단계이며, 두 번째 단계는 이러한 평가를 토대로 행동으로 반응하는 단계로 세 가지 유형의 행동(즉, 무반응, 위험통제반응 및 공포통제반응)중 한 가지의 행동을 취하게 된다. 무반응은 개인이 공포소구 메시지를 통하여 위협을 느끼지 못하고 아무 행동도 취하지 않는 상태를 의미하며, 위험통제반응은 고위협-고효능감 하에서 발생되는 것으로 메시지 속에 제시된 권고사항을 이행하는 적응적 변화를 일으키는 것을 말한다. 반면에, 공포통제반응은 고위협-저효능감 하에서 발생하는 것으로 방어적 회피, 거부, 그리고 반발 등과 같은 부적응 변화를 가져온다. 이와 같은 병행과정모델에 의하면 공포소구 메시지가 성공하기 위해서는 사람들이 그 메시지를 접한 이후에 높은 위협과 동시에 높은 효능감을 인지해야 함(위험통제반응)을 알 수 있으며, 공포소구 메시지가 실패하는 이유는 사람들이 그 메시지를 접하고 나서도 위협을 높게 지각하지 못하였든지(무반응), 아니면 위협은 높게 지각하고 효능감은 작게 지각했기 때문으로 설명할 수 있다(공포통제반응).

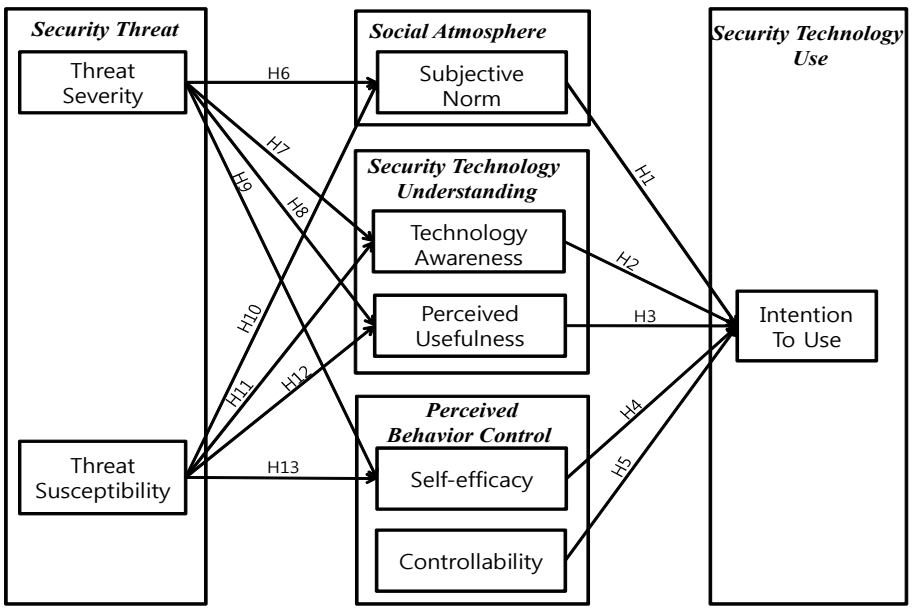
이와 같이 병행과정 확장모델에 의하면 공포소구효과가 사람들에게 영향을 미치려면, 인지된 위협이 우선적으로 높아야 한다는 것을 알 수가 있다. 인지된 위협이 높지 않다면 무반응을 일으키기 때문이다. 여기에서 인지된 효능감이 인지된 위협보다 강하다면 사람들은 위협을 줄이기 위한 인지통제과정을 수행하게 되며, 이와는 반대로 인지된 효능감이 인지된 위협보다 약하면 사람들은 공포를 줄이기 위한 공포통제과정에 들어가게 된다. 즉, 병행과정 확장모델에 의하면 권장되는 행동을 사람들이 수행하게 만들기 위해서는 위협의 심각성 및 취약성 인지정도와 자기 효능감을 높이는 것이라는 시사점을 얻게 된다.

3. 연구모형 및 가설 도출

3.1 연구모형

이상에서 고찰한 5가지 선행 관련 이론들이 정보보안기술 사용과 관련하여 어떻게 상호 연계되는지에 대한 논리적 추론과정(Logical Reasoning)을 통해 정보보안기술 사용에 영향을 미치는 요인들을 포괄적으로 도출하고 이들 간의 인과적 관계를 반영하여 <Figure 1>과 같은 연구모형을 설정하였다.

연구모형의 설정과정을 보다 구체적으로 기술하면 우선 Fishbein and Ajzen[14]의 합리적 행동이론(Theory of Reasoned Action)에 의하면 정보보안기술 사용의도에는 조직원들이 인식하고 있는 주관적 규범이 영향을 미친다고 추론할 수 있으며, 합리적 행동이론을 보완한 Ajzen [2, 3]의 계획된 행동이론(Theory of Planned



〈Figure 1〉 Research Model

Behavior)에 따르면 주관적 규범 외에 조직원들이 느끼는 정보보안기술 획득 및 통제가능성과 정보보안기술 사용에 대한 자기효능감이 정보보안기술 사용의도에 영향을 미친다고 추론된다. 그리고 MIS 분야에서 가장 활발히 연구되며 지지되고 있는 Davis et al.[10]의 기술수용모형(Technology Acceptance Model)에 의하면 인지된 유용성과 사용용이성이 영향을 주는 요인으로 추론될 수 있으나 사용용이성은 자기효능감과 개념적인 중복이 커서 제외하고 인지된 유용성만을 영향요인으로 취하였다. 아울러 Rogers[28]의 혁신확산이론(Innovation Diffusion Theory)에서 제시된 기술수용 및 확산에 영향을 미치는 요인들 역시 정보보안기술 수용에 대한 영향요인으로 볼 수 있을 것이나, 이상의 세 가지 이론적 모형에서 도출된 변수들과 개념적 중복가능성이 높은 요인들을 제외하고 기술인식도만을 영향요인으로 선정하였다. 마지막으로 앞에서 제시된 이론들이 모두 기술을 사용함에 의해 혜택을 누리는 긍정적 기술들을 대상으로 한데 비해 공포소구이론은 부정적 결과에 대처하기 위한 기술의 사용에 영향을 미치는 요인들을 제시한 이론으로서 정보보안기술 역시 보안침해 등과 같은 부정적 결과를 방지하기 위한 기술로서 공포소구이론이 적용되어야 할 기술이다. 공포소구이론에 의하면 기술에 대한 자기효능감과 위협의 정도가 해당 기술사용에 영향을 미친다고 보며, 이에 따라 보안침해 위협의 정도도 정보보안기술의 사용의도에 영향을 미치는 요인으로 추가되어야 할 것으로 추론되어 본 연구에서는 공포소구이론 분야의 대표적인 이론적 모델인 Witte[39]의 확장된 병행프로세스 모델(Extended Parallel Process Model)에서 제시된 위협 심각성, 위협 취약성 변수를 연구모형에 포함시켰다.

3.2 연구가설

<Figure 1>과 같이 제시된 연구모형에 포함되어 있는 변수들 간의 관계에 관한 가설들을 도출한 구체적인 논리적 추론과정(Logical Reasoning)을 각 가설별로 기술하면 아래와 같다.

3.2.1 정보보안기술에 관한 주관적 규범과 사용의도간의 관계

합리적 행동이론과 계획된 행동이론에서는 개인 행동의도에 주관적 규범이 직접적인 영향을 미치는 요인으로 나타나는데, 이는 개인이 어떤 대상에 대해 자신이 가지는 호감 또는 비호감의 반응과 상관없이 행동을 수행해야 하는 당위성을 갖는 경우가 많다는 것을 보여준다. 이러한 경향이 나타나는 원인은 자신이 중요하다고 생각하는 주변인을 지시자(Referent)로 생각하며, 이들에 순응하려는 동기를 갖기 때문으로 해석되고 있다[2, 14].

또한, Venkatesh and Davis[33]의 기술수용모형 2(TAM 2: Technology Acceptance Model 2)에서 주관적 규범은 강제적 또는 자발적 이용상황에서 모두 행동의도에 영향을 주는 것으로 분석되었다. 이들은 이러한 결과에 대하여 사용자가 지시자와 준거집단의 신념을 자신의 신념으로 내부화(Internalization)하기 때문으로 해석하였다. 이와 같이 주관적 규범은 그 동안 많은 연구들에서 정보기술 사용의도에 주요 영향요인으로 설명되거나 조직 내의 정보시스템 성공과 아주 밀접한 관계를 가지고 있는 것으로 고려되어 왔다[4, 19, 22]. 따라서 본 연구에서도 정보보안기술에 대한 개인의 주관적 규범이 정보보안기술 사용에 영향을 미칠 것으로 추론하여 다음의 가설을 설정하였다.

가설 1(H1): 정보보안기술에 대한 주관적 규범 수준이 높을수록, 정보보안기술에 대한 사용의도 수준도 높아질 것이다.

3.2.2 정보보안기술 인식도와 사용의도간의 관계

혁신확산이론[27]에 의하면 인식(Awareness) 단계는 '혁신확산 단계모형'에서의 초기 단계로서 '하나의 집단이 혁신을 의식하고 이것이 무엇을 가져올 수 있는지에 대한 일반적 인식을 형성하는 단계'이라고 할 수가 있으며, 기술인식 단계에 있는 개인 또는 조직원들은 혁신(기술)을 경험하고, 혁신이 어떠한 기능을 하는지 어떠한 혜택을 줄 수 있는지 판단하게 된다.

사회과학, 범죄재판, 의학적 행태과학 연구들에서도 인식(Awareness)의 개념은 인간행동의 중심에 위치하고 있다고 보는 바, Goodhue and Straub[16]은 정보보안에서 개인의 신념을 구성하는 중요한 요소가 인식(Awareness)이라고 주장하였고, 이어서 Dinev and Hart [11]의 연구에서는 기술 인식도(Technology Awareness)를 '사용자가 기술적 이슈와 그것을 다루는 전략에 대하여 아는 것에 흥미를 느끼고 의식을 높이게 되는 것'이라고 정의를 내리고 정보보안기술에 대한 인식이 정보보안기술 사용의도 형성에 중심적 요소임을 밝히고 있다. 이러한 선행연구들은 토대로 정보보안기술에 대한 기술 인식도가 사용의도에 영향을 미칠 것이라는 다음의 가설을 설정할 수 있다.

가설 2(H2): 정보보안기술에 대한 기술 인식도 수준이 높을수록, 정보보안기술에 대한 사용의도 수준도 높아질 것이다.

3.2.3 정보보안기술에 대한 인지된 유용성과 사용의도간의 관계

Davis[9]는 초기 기술수용모형에서 인지된 유용성은 개인이 사용하는 특정 시스템이 업무향상에 도움을 준다고 느끼는 정도라고 정의하고 인지된 유용성 수준이 높을수록 시스템의 사용의도 수준이 높아진다고 보았으며, 이 연구에서의 인지된 유용성은 정보기술을 사용하는 개인의 업무생산성 및 효율성의 측면에서 특정 기술을 선택하고 사용하는 것이 업무수행을 향상시킬 것이라는 신념수준으로 보았다. 한편, 인지된 유용성은 정보기술을 사용함에 있어서 사용자가 느끼는 만족의 정도로 정의되기도 하며, 이는 인지된 과업 성과와는 무관하게 사용자가 정보기술을 사용하면서 만족을 느끼는 만족감과 같은 주관적 태도라고도 할 수가 있다[1].

그러나 정보보안기술의 경우에는 인지된 유용성을 사용자의 업무생산성이나 만족감의 수준으로만 측정한다면 정보보안기술의 목적인 '보안위협으로부터 보호, 예방 및 치료'의 측면을 반영할 수가 없을 것이며, 이에 대처키 위하여 정보보안기술이 과연 보안위협으로부터 정보시스템을 막아낼 수가 있을 것인가에 대한 대응 효능감(Response Efficacy) 개념도 인지된 유용성에 추가될 필요가 있다. 여기서 대응 효능감이란 '권고되는 행동이 효과적으로 위협을 피하도록 해줄 것이라는 것에 대한 개인적 신념의 정도'라고 정의할 수가 있다[27, 39].

즉, 이상의 연구들로부터 정보보안기술에 대한 인지된 유용성은 정보보안기술의 사용이 개인의 업무 및 작업의 향상성을 증진시키고, 보안위협으로부터 정보시스템을 보호해줄 것이라고 믿는 신념정도로 정의될 수 있을 것이며 정보보안기술에 대한 인지된 유용성과 사용의도에 관한 관계에 관한 가설을 다음과 같이 설정할 수 있을 것이다.

가설 3(H3): 정보보안기술에 대한 인지된 유용성 수준이 높을수록, 정보보안기술에 대한 사용의도 수준도 높아질 것이다.

3.2.4 정보보안기술에 대한 자기 효능감, 통제성과 사용의도간의 관계

Ajzen[3]은 인지된 행동통제 수준이 높을수록 행동의도 및 실제 행동 수준이 높아짐을 주장하며 인지된 행동통제 개념을 자기 효능감(Self-Efficacy)과 통제성(Controllability)의 하위 개념으로 구분하였다. 즉, 자기 효능감(Self-Efficacy)은 행동을 취하는 개인의 기술, 능력에 대한 자신감으로 정의하고, 통제성(Controllability)은 행동을 취하는데 요구되는 자원의 기회와 가용성 수준으로 정의함으로써 자기 효능감과 통제성이 클수록 인지된 행동통제 수준도 높아진다고 보았다. 여기서 자기 효능감의 개념은 Ajzen 이전에 Bandura[7]의 연구에서 인간 행동의 변화를 설명하고, 예측하기 위하여 인지적 관점의 하나로 제시된 개념인데 Bandura[7]는 구체적 자신감(Specific Self-Confidence)을 자기 효능감이라 지칭하고, 인간 행동의 변화가 결국은 행위자 자신이 그 행동을 충분히 해낼 수 있겠다는 자신감으로 인해 일어난다고 주장하였다. 또한, 공포소구이론의 연구들 중 하나인 Rogers[27]의 보호동기이론(Protection Motivation Theory)에서도 자기 효능감의 제공이 특정한 행동에 대한 설득을 강화시킨다고 주장하였다.

이상의 연구들로부터 정보보안기술에 대한 자기 효능감과 통제성이 정보보안기술 사용의도에 영향을 줄 것으로 추론되어 다음의 가설이 설정될 수 있을 것이다.

가설 4(H4): 정보보안기술에 대한 자기 효능감 수준이 높을수록, 정보보안기술에 대한 사용의도 수준도 높아질 것이다.

가설 5(H5): 정보보안기술에 대한 통제성 수준이 높을수록, 정보보안기술에 대한 사용의도 수준도 높아질 것이다.

3.2.5 위협 심각성과 주관적 규범, 기술 인식도, 인지된 유용성 및 자기 효능감 간의 관계

Witte[39]는 위협(Threat)에 대하여 '개인에 의하여 인지되든지 아니든지 존재하는 외부의 자극(External Stimulus)'이라고 정의하고 있는데, 개인이 위협에 대하여 인지하게 되면 위협에 대하여 위협의 심각성을 전달할 뿐만 아니라, 목표 군중에 대하여 위협에 대한 취약성도 유발시킨다[27, 39].

위협 심각성(Threat Severity)의 개념은 Rogers[27]에 의하여 처음 사용된 개념으로서 개인의 반응에 영향을 미치는 공포소구에 있어서 우선되는 개념인데 위협의 중대성에 대하여 공포소구 청자가 가지게 되는 신념수준을 의미한다[27, 39]. 또한 Rogers[27, 28]의 보호동기이론(Protection Motivation Theory)에서는 위협 심각성을 대응의 강도에 영향을 미치게 할 정도의 위협의 중대성이라고 정의하고 위협 심각성은 대응 효능감과 자기 효능감에 영향을 미치게 된다고 주장하였다. 즉, 보안위협(Security Threat)인 부정적 기술(Negative Technology)이 심각한 피해를 입힐만한 기술일 경우, 이에 대응할 수 있는 정보보안기술에 대한 신뢰성은 의심이 갈 것이고, 이것을 사용할 개인의 자기 효능감의 수준도 낮아질 것으로 보았는데 본 연구에서 사용된 인지된 유용성은 앞서 서술된 대로 대응 효능감의 개념을 내포하고 있으므로 위협 심각성이 인지된 유용성에도 영향을 미칠 것으로 예상할 수 있을 것이다.

주관적 규범은 '행위를 수행하는 것이 다른 사람들에게 중요한 것인지에 대한 개인의 인식'이라고 정의할 수가 있는데[14] 정보보안을 위협하는 보안위협(Security Threat)의 심각성을 개인이 크게 인지하면 인지할수록, 보안기술 사용에 대한 사회적인 압력을 인지하는 주관적 규범의 수준도 높아질 것이다. 이것은 개인이 보안위협의 심각성을 높은 수준으로 인지하게 될 경우, 보안위협을 예방 또는 치료하기 위한 정보보안기술 사용에 대한 당위성을 높게 인식할 것이기 때문이다. 이와 마찬가지로 기술 인식도 역시 위협 심각성이 높은 수준인 경우에는 이에 대처키 위한 보안기술에 대한 관심이 높아지고 보안기술에 관한 자료를 자발적으로 습득하고자 할 가능성이 커지게 될 것이다.

반면에, 높은 수준의 위협 심각성은 인지된 유용성과 자기 효능감에는 부(-)의 영향을 미칠 것이다. 이는 높은 수준의 위협 심각성이 보안위협을 막아줄 정보보안기술 자체의 신뢰성을 의심하게 만들어 인지된 유용성을 낮추게 될 것이고, 동시에 정보보안기술을 사용하는 개인의 자신감 역시도 낮추게 될 것이기 때문이다.

이상의 같이 추론된 위협 심각성과 주관적

규범, 기술 인식도, 인지된 유용성, 자기 효능감 간의 관계는 다음의 4개의 가설로 설정할 수 있을 것이다.

가설 6(H6): 정보보안위협에 대한 위협 심각성 수준이 높을수록, 정보보안기술에 대한 주관적 규범 수준은 높아질 것이다.

가설 7(H7): 정보보안위협에 대한 위협 심각성 수준이 높을수록, 정보보안기술에 대한 기술 인식도 수준은 높아질 것이다.

가설 8(H8): 정보보안위협에 대한 위협 심각성 수준이 높을수록, 정보보안기술에 대한 인지된 유용성 수준은 낮아질 것이다.

가설 9(H9): 정보보안위협에 대한 위협 심각성 수준이 높을수록, 정보보안기술에 대한 자기 효능감 수준은 낮아질 것이다.

3.2.6 위협 취약성과 주관적 규범, 기술 인식도, 인지된 유용성 및 자기 효능감 간의 관계

Witte[39, 40]는 위협 취약성(Threat Susceptibility)을 개인이 인지하는 위협이 발생할 가능성이라고 정의하였는데 Rogers[27]는 위협 취약성을 공포소구에서 개인의 반응에 영향을 미치는 중요한 요소로서 공포소구의 중요한 구성개념으로 보았다. Witte[40]의 AIDS 예방 내용의 공포소구이론 연구에 의하면, 급속하면서도 유행처럼 퍼지는 AIDS의 측면을 강조한 문서를 개인에게 제공하면 그 개인은 위험으로부터 자기 자신을 보호할 능력이나 콘돔의 효능감을 약하게 인지하는 결과가 나타났으며, 이와 비슷하게 성병과 관련한 공포소구이론 연구에서도 동일한 결과가 나타났다[43].

이로부터 정보보안위협에 대한 취약성의 수준이 강하면 강할수록, 정보보안기술에 대한 대응 효능감과 자기 효능감은 낮아질 것으로 추론된다. 즉, 높아진 위협 취약성이 정보보안기술 자체 능력에 대한 의심을 품게 만들어, 보안위협을 막아줄 것이라는 혜택을 인식하는 인지된 유용성 수준을 낮출 것이며 또한 높은 수준의 위협 취약성은 정보보안기술을 사용하는 개인의 자신감 수준도 낮출 것이다. 또한 보안위협에 영향을 받을 가능성을 인식한 위협 취약성의 수준이 높으면 높을수록, 정보보안기술을 사용하여 이를 막는 것에 대한 자신감 부족 및 회의감 증대로 인해 정보보안기술 사용의 사회적 당위성에 대한 인식을 나타내는 주관적 규범 수준은 낮아질 것이다. 그러나 위협 취약성을 크게 인식할 경우, 이를 막아줄 정보보안기술에 대한 관심은 높아질 것으로 예상되며 자발적으로 정보보안기술에 대한 자료를 습득하는 노력은 커져 정보보안기술 인식도의 수준은 높아질 것으로 추론된다.

이상에서 추론된 위협 취약성과 주관적 규범, 기술 인식도, 인지된 유용성 및 자기 효능감 간의 관계는 다음의 4개의 가설로 설정할 수 있을 것이다.

가설 10(H10): 정보보안위협에 대한 위협 취약성 수준이 높을수록, 정보보안기술에 대한 주관적 규범 수준은 낮아질 것이다.

가설 11(H11): 정보보안위협에 대한 위협 취약성 수준이 높을수록, 정보

보안기술에 대한 기술 인식도 수준도은 높아질 것이다.

가설 12(H12): 정보보안위협에 대한 위협 취약성 수준이 높을수록, 정보보안기술에 대한 인지된 유용성 수준은 낮아질 것이다.

가설 13(H13): 정보보안위협에 대한 위협 취약성 수준이 높을수록, 정보보안기술에 대한 자기 효능감 수준은 낮아질 것이다.

4. 실증분석을 위한 연구설계

4.1 변수에 대한 조작적 정의 및 측정지표 개발

<Figure 1>에서 보는 바와 같이 본 연구의 연구모형에 포함된 8개 변수들(정보보안기술 사용의도, 위협 심각성, 위협 취약성, 주관적 규범, 기술 인식도, 인지된 유용성, 자기 효능감, 통제성)에 대한 조작적 정의는 기존의 관련 연구를 참고하되 정보보안 분야에 부합하도록 수정・보완하여 확정하였으며, 조작적 정의에 입각한 측정지표 개발은 모두 7점 Likert 척도로 개발하되 가급적 선행 연구들에서 신뢰성 및 타당성이 입증된 측정지표들을 최대한 활용하였다. 그리고 정보보안기술은 H/W 및 S/W 보안뿐 만아니라 네트워크보안, DB 보안, 물리적 시설 및 장비 보안 등 다양한 부문의 매우 많은 기술들로 구성되어 있으나, 본 연구의 측정지표 상에서 반영한 정보보안기술은 백신프로그램에 국한하였다. 이는 본 연구가 일반적인 조직구성원들의 정보보안기술 사용에 초점이 맞추어져 있어서 정보시스템 업무 담당요원들의 작업범위에 속한 보안기술이 아니라 자신의 업무수행 시에 정보시스템을 이용하는 현업부서 직원들이 보편적으로 가장 많이 접하는 정보보안기술에 국한하는 것이 유효한 응답을 이끌어 낼 수 있을 것으로 판단하였으며, 백신프로그램이 이에 부합하는 대표적인 정보보안기술로 보았기 때문이다.

4.1.1 사용의도(Intention to Use)

정보보안기술에 대한 '사용의도' 측정을 위한 조작적 정의와 측정지표 개발은 Fishbein and Ajzen[14], Ajzen[2, 3] 등의 연구에 근거하여 이루어졌다. '사용의도'에 대한 조작적 정의는 '정보보안기술의 설치, 사용, 업데이트를 수행할 의지 정도'이며, 측정지표는 1) '나는 악성 소프트웨어로부터 내 컴퓨터를 보호하기 위해 백신 프로그램을 설치하고 사용할 것이다' 2) '나는 스파이웨어로부터 내 컴퓨터를 보호하기 위해 안티스파이웨어(또는 백신)를 설치하고 사용할 것이다' 3) '나는 스파이웨어로부터 내 컴퓨터를 안전하게 보호하기 위해 검사와 치료 및 업데이트를 정기적으로 할 것이다' 등의 세 가지 지표들로 구성된다.

4.1.2 위협 심각성(Threat Severity)

정보보안이 요구되는 '위협의 심각성' 측정을 위한 조작적 정의와 측정지표 개발은 Rogers [27], Witte[41] 등의 연구에 근거하여 이루어졌다. '위협 심각성'에 대한 조작적 정의는 '보안위협의 발생이 미칠 부정적 영향을 인식한 정도'이며, 측정지표는 1) '내 컴퓨터는 악성 소프트웨어로 인해 저장정보가 유출될 확률이

높다' 2) '나의 인터넷 활동정보는 악성 소프트웨어로 인해 제3자에게 전송될 가능성이 높다' 3) '나의 개인정보는 악성 소프트웨어로 인해 유출되어 2차적으로 무단 사용될 확률이 높다' 4) '내 컴퓨터는 악성 소프트웨어로 인해 속도가 느려질 가능성이 높다' 5) '내 컴퓨터는 악성 소프트웨어로 인해 고장 날 확률이 높다' 등의 다섯 가지 지표들로 구성된다.

4.1.3 위협 취약성(Threat Susceptibility)

정보보안이 요구되는 '위협의 취약성' 측정을 위한 조작적 정의와 측정지표 개발은 Rogers [27], Witte[41] 등의 연구에 근거하여 이루어졌다. '위협 취약성'에 대한 조작적 정의는 '보안위협이 발생할 가능성을 인식한 정도 보안위협의 발생이 미칠 부정적 영향을 인식한 정도'이며, 측정지표는 1) '나는 악성 소프트웨어가 첨부된 e-mail을 받아볼 확률이 높다' 2) '나는 웹서핑을 하는 동안 악성 소프트웨어에 감염될 확률이 높다' 3) '내 컴퓨터는 P2P사이트를 통해 악성 소프트웨어에 감염될 가능성이 높다' 4) '내 컴퓨터는 USB로 인해 악성 소프트웨어에 감염될 확률이 높다' 5) '내 컴퓨터는 Active X로 인해 악성 소프트웨어에 감염될 가능성이 높다' 등의 다섯 가지 지표들로 구성된다.

4.1.4 주관적 규범(Subjective Norm)

정보보안기술에 대한 '주관적 규범' 측정을 위한 조작적 정의와 측정지표 개발은 Fishbein and Ajzen[14], Ajzen[2, 3], Venkatesh and Davis[33], Venkatesh et al.[34], Dinev and Hu[12]의 연구에 근거하여 이루어졌다. '주관적 규범'에 대한 조작적 정의는 '정보보안기술 사용에 대한 사회적 당위성을 인식한 정도'이며, 측정지표는 1) '나와 개인적으로 친한 사람들은 백신 프로그램을 사용하는 것이 올바른 행동이라 생각한다' 2) '내가 속한 조직의 사람들은 백신 프로그램을 사용해야만 한다고 생각한다' 3) '우리 사회의 구성원들은 백신 프로그램을 사용해야만 한다고 생각한다' 등의 세 가지 지표들로 구성된다.

4.1.5 기술 인식도(Technology Awareness)

정보보안기술에 대한 '기술 인식도' 측정을 위한 조작적 정의와 측정지표 개발은 Rogers [27], Dinev and Hu[12]의 연구에 근거하여 이루어졌다. '기술 인식도'에 대한 조작적 정의는 '정보보안기술에 대한 평소의 관심 및 인식 수준'이며, 측정지표는 1) '나는 백신 프로그램에 대한 기사(정보)를 찾아 읽어보는 편이다' 2) '나는 인터넷 보안 이슈에 대해 주변 사람들과 이야기 한다' 3) '나는 개인 컴퓨터에 침입하는 악성 소프트웨어에 대한 글을 읽어보는 편이다' 등의 세 가지 지표들로 구성된다.

4.1.6 인지된 유용성(Perceived Usefulness)

정보보안기술에 대한 '인지된 유용성' 측정을 위한 조작적 정의와 측정지표 개발은 Davis [9], Venkatesh[32], Venkatesh and Davis[33], Venkatesh et al.[34] 등의 연구에 근거하여 이루어졌다. '인지된 유용성'에 대한 조작적 정의는 '정보보안기술 사용을 통해 얻는 혜택을 인식한 정도'이며, 측정지표는 1) '나는 백신 프로그램 사용이 개인정보의 유출을 막아줄 것이라고 확신한다' 2) '나는 백신 프로그램 사용이 인터넷 활동정보의 유출을 막아줄 것이라고 확신한다' 3) '나는 백신 프로그램 사용이 악성

소프트웨어의 악영향으로부터 보호해 줄 것이라고 확신한다' 4) '나는 백신 프로그램의 사용이 업무수행의 신속성을 향상시킨다고 생각한다' 5) '나는 백신 프로그램의 사용이 업무 생산성을 증진시킨다고 믿는다' 등의 다섯 가지 지표들로 구성된다.

4.1.7 자기 효능감(Self-Efficacy)

정보보안기술에 대한 '자기 효능감' 측정을 위한 조작적 정의와 측정지표 개발은 Bandura[7], Witte[41], Ajzen[3] 등의 연구에 근거하여 이루어졌다. '자기 효능감'에 대한 조작적 정의는 '정보보안기술 사용에 대한 자신감 정도'이며, 측정지표는 1) '나는 내 컴퓨터에 백신 프로그램을 설치하고 사용할 수 있다' 2) '나는 백신 프로그램의 사용방법을 쉽게 익힐 수 있다' 3) '나는 백신 프로그램을 쉽게 사용할 수 있다' 4) '나는 백신 프로그램의 사용자 인터페이스가 명확하면서도 직관적이라고 생각한다' 등의 네 가지 지표들로 구성된다.

4.1.8 통제성(Controllability)

정보보안기술의 '통제성' 측정을 위한 조작적 정의와 측정지표 개발은 Bandura[7], Witte[41], Ajzen[3] 등의 연구에 근거하여 이루어졌다. '통제성'에 대한 조작적 정의는 '보안기술(백신 프로그램)의 획득, 통제 가능성, 가용시간 수준'이며, 측정지표는 1) '나는 내가 원할 때 백신 프로그램을 쉽게 구할 수 있다' 2) '나는 백신 프로그램 사용방법을 익히고, 사용할 시간적 여유가 있다' 3) '나는 내 컴퓨터에 백신 프로그램을 설치, 사용, 업데이트를 할 수 있는 통제권한을 가지고 있다' 등의 세 가지 지표들로 구성된다.

4.2 자료수집 및 분석 방법

본 연구는 개인들의 정보보안기술 사용에 영향을 미치는 인지요인을 규명하는 연구이기 때문에 설문대상을 개인단위의 정보시스템 최종사용자로 결정하였다. 자료의 수집은 파일럿 조사를 거쳐 만들어진 설문을 토대로 구글독스(Google Docs)의 리서치기능을 기반으로 제작된 웹 설문과 온라인 및 오프라인 페이퍼백 설문지를 배포하여 이루어졌다.

그리고 자료수집대상 선정을 위한 표본 추출은 정보보안투자 규모가 타 업종에 비해 상대적으로 큰 업종들인 금융 및 보험업, 정보서비스업, 유통업, 제조업에 속한 기업들 중 대기업을 중심으로 50개사 이상을 접촉하여 각 기업 당 10명 이상의 직원들을 설문응답자로 선정하였다(중소기업의 경우는 정보보안기술의 중요성에 대한 인식수준이나 정보보안기술에 대한 투자여력이 미흡할 것으로 판단되어 이번 연구에서는 포함시키지 않았음).

자료수집 결과 총 573개의 설문이 수집되었고, 이 중 불성실하게 응답되거나, 다수의 결측치가 있는 11부를 제외한 562부를 대상으로 분석함으로써 회수율은 98.08%를 상회하였다. 인구통계학적 분석은 SPSS 18.0 프로그램을 사용하여 분석하였고, 측정지표의 신뢰도 및 타당성 검증과 정보보안기술 수용모형에 대한 검증을 위한 통계분석기법은 부분최소자승법(PLS: Partial Least Squares)에 의하였고, 이를 위해 Smart PLS V.2.0 M3 소프트웨어를 사용하였다. PLS는 구조방정식모형(SEM: Structural Equation Model)에 사용하는 분석기법으로 계층적 구조로 된 다수의 변수를 포함한 이론적인 모델과 측정모델의 적합성을 함께 분석할 수 있는 분석

기법이다[8].

5. 실증분석 결과

5.1 측정지표의 신뢰성과 타당성 검증

5.1.1 신뢰성 검증 결과

측정지표의 신뢰성을 검증하기 위해서는 복합신뢰도(CSRI: Composite Scale Reliability Index)값이 0.7 이상이 되어야 하며, 내적 일관성 확보를 위해 평균분산추출(AVE: Average Variance Extracted)값이 기준치인 0.5 이상이어야 하고[8, 26], 크론바하 알파값(Cronbach's α)이 0.6~0.7 이상이면 측정도구의 신뢰성이 있는 것으로 볼 수 있다[26]. PLS분석 결과, 아래의 <Table 1>에서 보는 바와 같이 연구모형에 포함되어 있는 8개 변수들 모두의 경우 이 기준을 충족하고 있어 이들 변수들의 측정을 위해 개발된 측정지표들의 신뢰성이 확보되는 것으로 나타났다.

5.1.2 타당성 검증 결과

5.1.2.1 집중 타당성(Convergent Validity)

PLS 분석에서는 각 변수별로 포함된 측정지표들의 집중 타당성 검증을 위해 탐색적 요인분석(EFA: Exploratory Factor Analysis)보다는 확인적 요인분석(Confirmatory Factor Analysis)을 요구한다[15]. 또한 집중 타당성이 확보되기 위해서는 확인적 요인분석(CFA) 결과, 변수별 즉, 잠재변인별로 포함된 지표들의 요인적재량(Loadings)이 0.7 이상이 되어야 하고[29], 그 요인적재량은 그 외의 잠재변인들에 포함된 지표들 간의 교차 요인적재량(Cross-Loadings)보다 커야 한다. 본 연구에서의 확인적 요인분석 결과는 모든 잠재요인들 별로 포함된 측정지표의 요인적재량이 0.7 이상으로 나타났으며, 다른 잠재요인들에 포함된 측정지표들과의 교차요인적재량 값보다 해당 잠재요인에 속한 측정지표들의 요인 적재량이 큰 것으로 나타남으로써 집중타당성이 확보된 것으로 볼 수 있다.

〈Table 1〉 The Result of Reliability Testing

Variable	No. of Measurement Items	Composite Reliability	Average Variance Extracted	Cronbach's α
Intention to Use	3	0.879	0.708	0.794
Threat Severity	5	0.934	0.739	0.915
Threat Susceptibility	5	0.850	0.533	0.791
Subjective Norm	3	0.919	0.791	0.868
Technology Awareness	3	0.900	0.749	0.833
Perceived Usefulness	5	0.917	0.690	0.886
Self-efficacy	4	0.935	0.785	0.904
Controllability	3	0.895	0.740	0.825

5.1.2.2 **판별 타당성**(Discriminant Validity)

각 변수별 측정지표들의 판별 타당성은 확인적 요인분석에서 각 측정지표들의 요인 적재량(Loadings)이 다른 요인 적재량(Cross Loadings)보다 커야 하며, 각 변수의 평균분산추출(AVE)값의 제곱근(Square Root)이 해당 변수와 다른 변수들 간의 상관계수보다 모두 커야 한다[15]. 확인적 요인분석 결과에서 나타났듯이 각 변수별 측정지표들의 적재량이 다른 변수에 적재된 요인 적재량보다 모두 크게 나타났을 뿐만 아니라 아래의 <Table 2>에서 보는 바와 같이 각 변수에 대한 AVE의 제곱근 값인 대각선상의 진하게 표시된 값들이 다른 변수들과의 상관계수 값보다 모두 큰 것으로 나타남으로써 각 변수별 측정지표들의 판별 타당성이 확보됨을 확인할 수 있다.

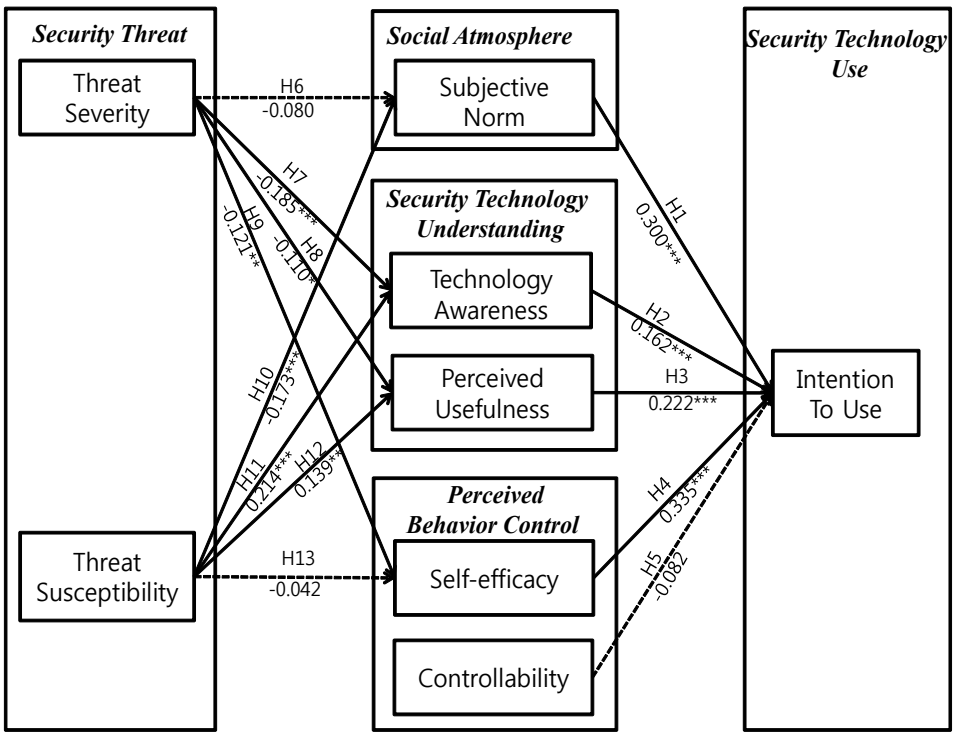
5.2 구조방정식 모형 분석 결과

PLS 분석에서 나타난 정보보안기술 수용에 관한 연구모형상의 경로계수들에 대한 유의성 검증을 통해 가설들을 검증하기 위해 부트스트랩(BootStrap)을 사용하였다. 이는 PLS 분석에서는 경로계수(Path Coefficients)는 제시하나 경로계수의 유의성 검증 및 신뢰구간 추정을 직접적으로 제시하여 주지는 않기 때문이다. 부트스트랩이란 수집된 원시 데이터 군에서 재추출한 유사 데이터군으로 원시 데이터를 추론하는 비모수적 기법을 말한다. PLS를 적용한 연구들에서는 주로 500개~1,000개의 서브샘플링을 통하여 가설의 유의성을 검증한다. 본 연구에서는 500개의 서브샘플링을 통해 경로계수에 대한 통계적 유의성을 검증하였으며 검증결과는 <Figure 2>와 같이 나타났다.

PLS 분석의 결과로 나타난 경로계수 및 유의성 검증결과를 변수별로 살펴보면 정보보안기술 사용에 대한 주관적 규범 수준이 높을수록, 즉 조직 내 분위기가 정보보안기술 사용에 대한 당위성을 강하게 느끼게 할수록(H1), 조직구성원들의 정보보안 기술에 대한 인식수준(H2)과 기술의 유용성 인지수준이 높을수록(H3) 그리고 정보보안기술 사용에 대한 자신감, 즉 자기효능감이 강할수록(H4) 조직구성원들의 정보보안기술 사용의지가 높아짐이 통계적으로 유의적으로 나타났다. 그러나

〈Table 2〉 The Result of Discriminant Validity Testing

Variable	BI	TSE	TSU	SN	TA	PU	SE	CTR
Intention to Use (BI)	**0.841**							
Threat Severity (TSE)	-0.010	**0.859**						
Threat Susceptibility (TSU)	0.096	0.599	**0.730**					
Subjective Norm (SN)	0.516	0.023	0.125	**0.889**				
Technology Awareness (TA)	0.361	-0.057	0.103	0.266	**0.865**			
Perceived Usefulness (PU)	0.364	-0.026	0.074	0.234	0.201	**0.830**		
Self-efficacy (SE)	0.491	-0.147	-0.115	0.451	0.297	0.160	**0.886**	
Controllability (CTR)	0.378	-0.227	-0.165	0.373	0.308	0.181	0.770	**0.860**



*t > 1.645, p < 0.1; **t > 1.965, p < 0.05; ***t > 2.58, p < 0.01.

〈Figure 2〉 The Result of Structural Equation Model Analysis

보안자원 활용가능성 변수들 중 정보보안기술의 획득 및 통제가능성(H5)은 정보보안 사용의도에 유의한 영향을 주지 못하는 것으로 나타났다. 그리고 정보보안 위협의 심각성을 크게 인식할수록 정보보안 기술에 대한 인식수준(H7)과 유용성 인지도(H8)가 낮아지는 경향이 있고, 정보보안기술의 대한 자기효능감(H9)도 낮아지는 것이 통계적으로 유의하게 나타난 반면, 정보보안기술에 대한 주관적 규범수준(H6)에는 위협 심각성이 통계적으로 유의한 영향을 주지 못하는 것으로 나타났다. 한편, 정보보안 위협 발생가능성, 즉 위협 취약성의 인식수준이 높을수록 정보기술사용에 대한 주관적 규범수준(H10)은 낮아지나 정보보안기술에 대한 인식도(H10)나 유용성 인지수준(H12)은 높아지는 것이 통계적으로 유의하게 나타난 반면 정보보안 기술에 대한 자기 효능감(H13)에는 통계적으로 유의한 영향을 주지 못하는 것으로 나타났다.

이상의 경로계수 유의성 검증에 근거한 가설검증 결과를 요약하여 제시하면 아래의 <Table 3>과 같으며, 연구모형 내에 포함된 13개의 가설들 중 8개의 가설(H1, H2, H3, H4, H8, H9, H10, H11)이 채택되었으며, 3개의 가설(H5, H6, H13)은 통계적으로 유의성이 없어 기각되었고, 통계적으로 유의하기는 하나 방향성이 역전되어 나타난 2개의 가설(H7, H12)도 기각되었다.

〈Table 3〉 The Result of Hypotheses Testing

Hypothsis	Path	Path coefficient	t-value	Adoption/ Rejection
H1	Subjective Norm → Intention to Use	0.300***	6.088	Adopted
H2	Technology Awareness → Intention to Use	0.162***	4.550	Adopted
H3	Perceived Usefulness → Intention to Use	0.222***	6.228	Adopted
H4	Self-efficacy → Intention to Use	0.335***	5.167	Adopted
H5	Controllability → Intention to Use	-0.082	1.452	Rejected
H6	Threat Severity → Subjective Norm	-0.080	1.251	Rejected
H7	Threat Severity → Technology Awareness	-0.185***	3.340	Rejected (Opposite Result)
H8	Threat Severity → Perceived Usefulness	-0.110*	1.745	Adopted
H9	Threat Severity → Self-efficacy	-0.121**	2.252	Adopted
H10	Threat Susceptibility → Subjective Norm	-0.173***	2.644	Adopted
H11	Threat Susceptibility → Technology Awareness	0.214***	3.669	Adopted
H12	Threat Susceptibility → Perceived Usefulness	0.139**	2.033	Rejected (Opposite Result)
H13	Threat Susceptibility → Self-efficacy	-0.042	0.743	Rejected

*$t > 1.645$, $p < 0.1$; **$t > 1.965$, $p < 0.05$; ***$t > 2.58$, $p < 0.01$.

6. 결 론

기존의 정보보안 관련 연구에서는 기술적 보안이나 물리적 보안의 측면이 주로 강조되어 왔으며 상대적으로 관리적 보안에 대한 연구는 미진한 수준에 머물고 있다. 특히, 관리적 보안영역 중 개인의 정보보안기술 사용에 관한 행태론적 연구는 더욱 미진한 상태인 바, 이와 같은 정보보안에 관한 기존 연구들의 한계를 극복하기 위해 본 연구는 조직구성원들의 정보보안기술의 사용의도에 영향을 미치는 요인들을 체계적이고 통합적으로 도출하기 위하여 기존의 기술수용에 관련된 제반 이론적 모형을 고찰함과 동시에 정보보안 분야의 특수성을 반영할 수 있는 이론적 근거를 확보하고자 했다. 아울러 도출된 영향요인들 간의 인과적 관계를 논리적으로 규명하여 연구모형을 구축하고 13개의 연구가설을 도출하였다.

연구모형 및 가설들에 대한 검증을 위한 자료 수집을 위해 정보보안투자규모가 타 업종에 비해 상대적으로 큰 금융 및 보험업, 정보서비스업, 유통업과 제조업에 속한 대기업에 근무하는 직원들을 임의 표본 추출하여 이들에 대한 설문조사를 실시하였다. 수집된 자료에 대한 통계분석기법은 다수의 변수를 포함하고 계층적 구조로 된 이론적인 모형과 측정모형의 적합성을 함께 분석하는데 적합한 부분최소자승법(PLS: Partial Least Squares)에 의한 구조방정식모형(Structural Equation Model) 분석기법에 의하였고, 이를 위해 Smart PLS V.2.0 M3 소프트웨어를 사용하였다.

구조방정식모형 분석의 결과로 나타난 변수

들 간의 인과관계를 나타내는 경로계수 및 이의 유의성 검증결과를 변수별로 살펴보면 정보보안기술 사용에 대한 주관적 규범수준이 높을수록, 즉 조직 내 분위기가 정보보안기술 사용에 대한 당위성을 강하게 느끼게 할수록, 조직구성원들의 정보보안기술에 대한 인식수준과 기술의 유용성 인지수준이 높을수록 그리고 정보보안기술 사용에 대한 자신감, 즉 자기효능감이 강할수록 조직구성원들의 정보보안기술 사용의지가 높아짐이 통계적으로 유의적으로 나타났다. 그러나 보안자원 활용가능성 변수들 중 정보보안기술의 획득 및 통제가능성은 정보보안 사용의도에 유의한 영향을 주지 못하는 것으로 나타났다. 그리고 정보보안 위협의 심각성을 크게 인식할수록 정보보안기술에 대한 인식수준과 유용성 인지도가 낮아지는 경향이 있고, 정보보안기술의 대한 자기효능감도 낮아지는 것이 통계적으로 유의하게 나타난 반면, 정보보안기술에 대한 주관적 규범수준에는 위협 심각성이 통계적으로 유의한 영향을 주지 못하는 것으로 나타났다. 한편, 정보보안위협 발생가능성, 즉 위협취약성의 인식수준이 높을수록 정보기술사용에 대한 주관적 규범수준은 낮아지나 정보보안기술에 대한 인식도나 유용성 인지수준은 높아지는 것이 통계적으로 유의하게 나타난 반면, 정보보안기술에 대한 자기 효능감에는 통계적으로 유의한 영향을 주지 못하는 것으로 나타났다.

본 연구의 이론적 측면에서의 기여도는 우선 제반 조직들에서의 정보보안기술의 수용 및 확산 현상을 보다 정확히 이해하고 관리적 정보보안수준의 제고방안을 수립함에 있어서 요구되는 이론적 기반을 강화하는데 기여할 수 있다는 점이다. 즉, 본 연구는 정보보안기술 사용의 영향요인을 도출함에 있어서 효익과 혜택과 같은 긍정적 결과를 지향하는 기술의 수용에 관련된 제반 대표적인 이론들을 통합·적용하였을 뿐 아니라 정보보안기술과 같은 부정적 결과를 방지하기 위한 기술을 수용하는 현상을 설명해 주는 공포소구이론을 접목시킴으로써 보다 현실성 있는 영향요인들을 체계적이고 포괄적으로 제시하고 실증적인 규명을 함으로써 향후 관리적 보안 분야 연구의 외연을 확장하는데 기여할 것으로 본다. 또한 조직 행태론적 접근방법에 의한 정보보안 기술의 조직 내 수용 및 확산에 관한 연구 수행 시에 포함되어야 할 변수들에 대해 본 연구에서 개발된 신뢰성(reliability)과 타당성(validity)이 확보된 측정지표들을 활용함으로써 실증분석 시 요구되는 측정지표 개발의 노력을 크게 절감할 수 있을 것이다. 아울러 실무적인 측면에서는 본 연구에서 실증적으로 규명된 조직 내에서의 정보보안기술 사용에 영향을 주는 요인들 간의 인과적 메커니즘(Mechanism)이 정보보안 관리방안 및 정책 수립을 하는데 있어서 업무지침(guideline)으로 활용될 수 있을 것으로 기대되며, 조직 내 정보보안기술 확산을 위한 교육이나 홍보프로그램의 개발 및 추진 시에 역점을 두어야 하는 요인들을 체계적으로 도출함에 있어서 기준점으로서 기여할 수 있을 것이다.

그러나 본 연구는 정보보안기술 사용의도에 영향을 미치는 요인들을 규명함에 있어서 아직 탐색적(exploratory) 수준의 연구이며 보다 현실적 타당성 및 설명력을 높이기 위해서는 향후 연구에서 극복하여야 할 과제들이 있다. 우선 본 연구에서 지지되지 못한 가설들에 대한 이론적 추론 과정이 재검증 되어져야 할 것

이다. 특히, 통계적으로 유의한 관계가 있는 것으로 나타났으나 가설과 상반되게 나온 위협심각성의 기술인식도에 대한 영향과 위협심각성의 인지된 유용성에 대한 영향은 공포소구이론을 정보보안기술 분야에 접목시키는 과정에서 보다 충분한 논증이 되지 못했음을 알 수 있다. 또한 자료수집시의 예상되는 어려움으로 인해 종속변수를 정보보안기술 사용행위 그 자체로 하지 못하고 정보보안기술 사용의도로 하였는데 사용의도가 사용행위의 강력한 예측변인이기는 하지만[14], 향후 연구에서는 사용행위 자체를 종속변수로 하여 이에 대한 영향요인들을 규명해 볼 필요가 있다.

References

[1] Adams, D. A., Nelson, R. R., and Todd, P. A., "Perceived Usefulness, Ease of Use, and Usage of Information Technology: a Replication," MIS Quarterly, Vol. 16, No. 2, pp. 227-247, 1992.

[2] Ajzen, I., "The theory of planned behavior," Organizational Behavior and Human Decision Processes, Vol. 50, pp. 179-211, 1991.

[3] Ajzen, I., "Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior," Journal of Applied Social Psychology, Vol. 32, pp. 665-683, 2002.

[4] Amoroso, D. L., "Organizational issues of end-user computing," Data Base, Vol. 19, No. 3-4, pp. 49-58, 1988.

[5] Bagozzi, R. P., "Attitudes, intentions, and behavior: A test of some key hypotheses," Journal of Personality and Social Psychology, Vol. 41, No. 4, pp. 607-627, 1981.

[6] Bagozzi, R. P., "A Field Investigation of Causal Relations among Cognitions, Affect, Intentions, and Behavior," Journal of Marketing Research, Vol. 19, No. 4, pp. 562-583, 1982.

[7] Bandura, A., "Self-efficacy: toward a unifying theory of behavioral change," Psychological Review, Vol. 84, No. 2, pp. 191-215, 1986.

[8] Chin, W., "Issues and Opinion on Structural Equation Modeling," MIS Quarterly, Vol. 22, No. 1, pp.7-16, 1998.

[9] Davis, F. D., "Perceived usefulness, perceived ease of use, and user acceptance of information technology," MIS Quarterly, Vol. 13, No. 1, pp. 319-340, 1989.

[10] Davis. F. D., Bagozzi. R. P., and Warshaw, P. R., "User acceptance of computer technology: a comparison of two theoretical models," Management Science, Vol. 35, No. 8, pp. 982-1003, 1989.

[11] Dinev, T. and Hart, P., "Internet privacy concerns and social awareness as determinants of intention to transact," International Journal of E-Commerce, Vol. 10, No. 2, pp. 7-31, 2006.

[12] Dinev, T. and Hu, Q., "The centrality of awareness in the formation of user behavioral intention toward protective in-

formation technologies," Journal of the Association for Information Systems, Vol. 8, pp. 386-408, 2007.

[13] Fishbein, M., "An investigation of relationships between beliefs about an object and the attitude toward that object," Human Relations, Vol. 16, pp. 233-240, 1963.

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

[15] Gefen, D. and Straub, D. W., "A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example," Communications of the Association for Information Systems, Vol. 16, No. 5, pp. 91-109, 2005.

[16] Goodhue, D. L. and Straub, D. W., "Security concerns of system users: A study of perceptions of the adequacy of security," Information and Management, Vol. 20, No. 1, pp. 13-27, 1991.

[17] Hu, Q. and Dinev, T., "Is Spyware an Internet Nuisance or Public Menace?," Communications of the ACM, Vol. 48, No. 8, pp. 61-66, 2005.

[18] Hu, Q., Hart, P., and Cooke, D., "The Role of External Influences on Organizational Information Security Practices: An Institutional Perspective," Proceedings of the 39th Hawaii International Conference on Systems Science (HICSS 39), January 4-7, Hawaii, USA. CD-ROM, IEEE Computer Society, 2006.

[19] Igbaria, M., "An examination of the factors contributing to microcomputer technology acceptance," Accounting Management and Information Technologies, Vol. 4, No. 4, pp. 205-224, 1994.

[20] Jackson, C. M. and Chow, S., "Toward an Understanding of the Behavioral Intention to Use an Information System," Decision Sciences, Vol. 28, No. 2, pp. 357-389, 1997.

[21] Kim, S. and Park, S., "Influencing Factors for Compliance Intention of Information Security Policy," The Journal of Society for e-Business Studies, Vol. 16, No. 4, pp. 33-51, 2011.

[22] Kwon, T. H. and Zmud, R. W., "Unifying the fragmented models of information systems implementation," Critical Issues in Information Systems Research(edited by Hirschheim, R. J. and Boland, R. A.), John Wiley and Sons, pp. 227-251, 1987.

[23] Lang, P. J., "Cognition in emotion: Concept and action," Emotions, Cognition and Behavior(edited by Izard, C. E., Kagan, J. and Zajonc, R.), Cambridge University Press, pp. 192-226, 1984.

[24] Lee, S. and Lee, M., "An Exploratory Study on the Information Security Culture Indicator," Informatization Policy, Vol. 15, No. 3, pp. 100-119, 2008.

[25] Nam, G. H. and Won, D. H., Information System Security, Green Publishing Co., Seoul, 2010.

[26] Nunnally, J. C., Psychometric Theory (2nd ed.), New York: McGraw-Hill, 1987.

[27] Rogers, R. W., "A Protection Motivation Theory of Fear Appeals and Attitude Change," Journal of Psychology, Vol. 91, pp. 93-114, 1975.

[28] Rogers, E. M., Diffusion of Innovations (4th ed.), The Free Press, New York, 1983.

[29] Srite, M. and Karahanna, E., "The Role of Espoused National Cultural Values in Technology Acceptance," MIS Quarterly, Vol. 30, No. 3, pp. 679-704, 2006.

[30] Szajna, B., "Empirical Evaluation of the Revised Technology Acceptance Model," Management Science, Vol. 42, No. 1, pp. 85-92, 1996.

[31] Telecommunication Technology Association, Dictionary of Information Security Technology, Telecommunication Technology Association, 2006.

[32] Venkatesh, V., "Creation of Favorable User Perceptions: Exploring the Role of Intrinsic Motivation," MIS Quarterly, Vol. 23, No. 2, pp. 239-260, 1999.

[33] Venkatesh, V. and Davis, F. D., "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies," Management Science, Vol. 46, No. 2, pp. 186-198, 2000.

[34] Venkatesh, V. and Morris M. G., "User Acceptance of Information Technology: Toward a Unified View," MIS Quarterly, Vol. 27, No. 3, pp. 425-478, 2003.

[35] Warshaw, P. R., "A New Model for Predicting Behavioral Intentions: An Alternative to Fishbein," Journal of Marketing Research, Vol. 17, No. 2, pp. 153-172, 1980(a).

[36] Warshaw, P. R., "Predicting Purchase and Other Behaviors from General and Contextually Specific Intentions," Journal of Marketing Research, Vol. 17, No. 1, pp. 26-33, 1980(b).

[37] Warshaw, P. R. and Davis, F. D., "Self-Understanding and the Accuracy of Behavioral Expectations," Personality and Social Psychology Bulletin, Vol. 10, No. 2, pp. 111-118, 1984.

[38] Warshaw, P. R. and Davis, F. D., "Disentangling Behavioral Intention and Behavioral Expectation," Journal of Experimental Social Psychology, Vol. 21, No. 2, pp. 213-228, 1985.

[39] Witte, K., "Putting the Fear Back into Fear Appeals: The Extended Parallel Process Model," Communication Monographs, Vol. 59, pp. 329-349, 1992.

[40] Witte, K., "Fear Control and Danger Control: A Test of the Extended Parallel Process Model(EPPM)," Communication Monographs, Vol. 61, pp. 113-134, 1994.

[41] Witte, K., Cameron, K. A., McKeon, J. K., and Berkowitz, J. M., "Predicting Risk Behaviors: Development and Validation f a Diagnostic Scale," Journal of Health Communication, Vol. 1, pp. 317-341, 1996.

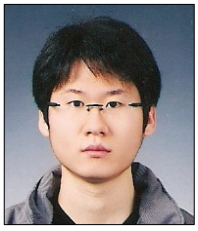
[42] Witte, K., "Fear as motivator, fear as in-

hibitor: Using the extended parallel process model to explain fear appeal successes and failures," Handbook of communication and emotion: Research, theory, applications, and contexts (edited by Andersen, P. A. and Guerrero, L. K.), San Diego, CA, US: Academic Press, pp. 423-450, 1998.

[43] Witte, K., Meyer, G., and Martell, D., Effective health risk message: A step-by-step guide, Thousand Oaks, California: Sage, 2001.

저 자 소 개

김상훈 (E-mail: shkim@kw.ac.kr)
1978년 서울대학교 경제학과 (학사)
1982년 한국과학기술원(KAIST) 경영과학과 (석사)
1991년 한국과학기술원(KAIST) 경영과학과 (박사)
1993년~현재 광운대학교 경영대학 교수
관심분야 정보화전략, 정보보안, 정보시스템 평가, ERP 등



이갑수 (E-mail: gslee@skinfosec.co.kr)
2007년 광운대학교 경영정보학과 (학사)
2012년 광운대학교 일반대학원 경영정보학과 (석사)
2013년~현재 SK인포섹 컨설팅본부 전임컨설턴트
관심분야 정보보안, 정보보안기술, 정보보호관리체계 등