정보보안 정책 준수 의도에 대한 영향요인

Influencing Factors for Compliance Intention of Information Security Policy

김상훈(Sang-Hoon Kim)*, 박선영(Sun-Young Park)**

초 록

본 연구는 중화이론, 계획된 행동이론, 보호동기이론에 기반하여 조직원들의 정보보안 정책 준수에 영향을 미치는 요인들을 도출하고 이들 요인들의 관계에 관한 연구모형 및 가설을 설정하였다.

연구모형 및 가설에 대한 실증분석을 위해 웹 서베이를 통해 자료를 수집하였고 총 207개의 설문 중 194개 설문이 사용가능하였다. 통계분석은 PLS 방법에 의하였고 신뢰도, 타당도, 모형의 적합도가 모두 적정한 것으로 나타났으며, 가설검증 결과는 총 8개의 가설 중 7개의 가설이 모두 지지되는 것으로 나타났다.

본 연구의 이론적인 시사점은 첫째, 조직원들의 정보보안 정책 준수에 대한 향후 연구들의 초석이 될 것으로 기대된다. 둘째, 심리학에서 근거한 요인을 접목하여 IS 연구와 심리학 연구의 고찰을 통해 정보보안연구의 학제 간 접근을 시도한 것과 마지막으로 이론적 고찰을 통해 정보보안 정책 준수에 관한 요인들에 대한 조작적 정의를 구체화시켜 제시하였다는 점이다. 아울러 실무적 시사점은 첫째, 조직에서 정보보안 정책의 성공적인 실행을 위한 전략 방안을 수립할 때 본 연구결과에 근거한 가이드라인을 제공할 수 있다는 점이며, 둘째, 조직원들의 정보보안 정책 위반에 대한 중화심리를 억제시키기 위해 조직구성원들에 대한 의식교육 및 훈련 프로그램 실시에 대한 필요성을 부각시켰다는 점이다.

ABSTRACT

This research derived the influencing factors for employees' compliance with the information security policy in organizations on the basis of Neutralization Theory, Theory of Planned Behavior and Protection Motivation Theory.

To empirically analyze the research model and the hypotheses, data were collected by conducting web survey, 194 of 207 questionnaires were available. The test of causal model was conducted by PLS. Reliability, validity and model fit were found to be statistically significant. the results of hypotheses tests showed that seven ones of eight hypotheses could be accepted.

The theoretical implications of this study are as follows : 1) this study is expected to play a role of baseline for future research about employee compliance with the information security policy, 2) this study attempted interdisciplinary approach through combining

이 논문은 2011년도 광운대학교 교내학술연구비 지원에 의해 연구되었음.

* 교신저자, 광운대학교 경영학부 교수

** 광운대학교 경영정보학과 석사과정

2011년 10월 12일 접수, 2011년 10월 28일 심사완료 후 2011년 11월 12일 게재확정.

psychology and information system security research, and 3) it suggested concrete operational definitions of influencing factors for information security policy compliance through comprehensive theoretical review. Also, this study has some practical implications. First, it can provide the guideline to support the successful execution of the strategic establishment for implement of information system security policies in organizations. Second, it is proved that the need for conducting education and training program suppressing employees' neutralization psychology to violate information security policy should be emphasized in the organizations.

키워드 : 정보보안 정책, 준수의도, 계획된 행동이론, 중화이론, 보호동기이론
Information Security Policy, Compliance Intention, Theory of Planned Behavior, Neutralization Theory, Protection Motivation Theory

1. 서 론

기업들은 보안을 위해 종종 기술기반의 솔루션들에 투자하고 이에 의존하여 왔으나 정보보안과 관련된 위험들을 충분히 제거하지 못했다[1]. 그러므로 물리적, 기술적 보안도 물론 중요하지만 관리적 보안도 역시 중요하다고 할 수 있다. 이렇듯 정보보안의 초점이 점차 조직과 개인적인 측면으로 옮겨옴에 따라 직원들의 정보보안 정책 준수여부가 사회조직적 요소의 핵심으로 떠오르고 있다[7, 31]. 조직은 직원들에게 정보보안을 위한 정책과 교육을 제공하고 있지만 이것이 효과를 보기 위해서는 직원의 실제적인 보안행동과 정책 준수가 뒷받침되어야 한다. 그러므로 이에 대한 연구가 필요한 시점이다.

이러한 측면에서 본 연구에서는 직원들이 조직의 정보보안 정책을 준수하려는 의도에 영향을 미치는 요인들이 어떤 것들이 있는지를 알아보고자 한다. 이를 위해 정보보안 정책 준수와 관련된 이론적 문헌을 토대로 모델을 제시하고, 본 연구에서 제시한 모형의 타당성을 검증함으로써 직원들의 정보보안 정책 준수의 선행 요인들을 파악할 수 있는 방안을 모색함과 함께 향후 이 내용을 적용하여 직원들의 정보보안 정책 준수성을 높일 수 있는 방안과 앞으로의 연구방향을 제시하고자 한다.

2. 정보보안 정책준수에 관한 이론적 고찰

2.1 정보보안 정책의 준수 필요성

흔히 전문가들은 정보보안 문제를 시스템 오류(error), 오작동(malfunction), 또는 고장(failure)이라는 개념을 통해서 표현하는데 익숙하다. 그만큼 정보보안을 기술공학적 인식과 시각으로 보는 것이 지배적이라고 할 수 있다. 이러한 접근으로 인해 보안문제 해결을 위한 대응조치 역시 기술 영역에서 찾는 노력으로 연결되고, 이를 정당화하게 된다. 이처럼 기술적 대응책을 중심으로 정보보안을 논한다면, 모든 보안문제의 근본적인 해결은 첨단 기술과 새로운 보안 알고리즘 개발에 의해서 가

능하며, 이를 능가하는 혁신적인 위협 기술의 등장에 의해서 또 다른 대응 기술 개발이 이루어져야 하는 끝없는 순환과정으로 귀착된다[7]. 그러므로 기술적, 물리적인 보안 측면도 중요하지만 여기에서 나아가 보안 방안을 직접 행하는 주체인 사람에게 초점을 맞추어 조직의 보안투자가 기술적, 사회조직적 자원 양쪽 측면에서 이루어져야 성공적인 정보보안이 이루어질 수 있을 것이다. 이러한 시각에 따라 정보보안의 초점이 기술적인 것에서 개인과 조직적 관점으로 옮겨오면서 특히 조직원들의 정보보안 정책 준수가 사회조직적 측면의 핵심이슈로 대두되고 있다. 또한 Bulgurcu et al.[8]도 정보보안의 인간적 측면(Human perspective)에서 시도되고 있는 연구의 주류는 최종 사용자(End-user)의 행위와 조직원들을 정보보안과 관련한 준수 행위에 이르도록 하는 요인들을 밝혀내려는 연구들이라고 하였다. 조직원의 정보자원 사용시의 무지, 실수, 부당한 행동 등은 조직의 정보보안을 위태롭게 한다[14]. 이렇듯 정보자원의 보호를 위해서는 조직구성원의 정보보안 실천이 무엇보다도 절실하게 요구되며, 정보보안은 조직구성원의 실천적 행동에 의하여 많은 영향을 받게 된다[3]. 또한 조직원들의 정보보안 실천적 행동은 조직에서 정한 룰을 잘 따르는 데서 출발하므로 조직원들의 정보보안 정책 준수가 무엇보다도 중요하다고 볼 수 있다.

2.2 정보보안 정책준수 관련 선행 연구

2.2.1 계획된 행동이론

사회심리학 분야에서 태도는 행동을 예측하는 가장 설명력 있는 변수로 인식되었지만, 점차 태도 이외에 다른 변인도 함께 고려되어야 한다는 주장이 제기되었고, 이러한 태도, 행위의도, 행위 간의 관계를 설명하는 대표적인 이론이 Fishbein and Ajzen[15]이 제시한 합리적 행동이론(TRA : Theory of Reasoned Action)이다. 하지만 합리적 행동이론은 타당성과 적용성에 있어서 한계점이 지적되어왔는데, 합리적 행동이론은 행위가 개인의 통제 하에 실행될 경우를 가정하고 있지만. 현실상황에서는 개인이 자신의 행동을 통제할 수 없는 경우가 얼마든지 있기 때문이다[20]. 즉, 개인이 어떤 행동 수행과 관련하여 아무리 긍정적인 태도와 주관적 규범을 가지고 있다 하더라도 그 행동수행의 기회와 필요한 자원을 갖지 못하는 경우에는 그 행동을 수행할 수 없다. 이에 따라 지각된 행동통제의 요소를 추가하여 합리적 행동이론의 한계점을 보완하여 확장, 발전시킨 이론이 바로 Azjen[6]의 계획된 행동이론(TPB : Theory of Planned Behavior)이다[2]. 계획된 행동이론에 의하면 개인은 행동수행과 관련하여 긍정적인 태도와 주관적 규범을 가질 뿐만 아니라 자신이 그 행동을 수행할 수 있는 기회와 행동수행에 필요한 자원을 가진 경우 비로소 자신이 그 행동을 자신의 뜻대로 통제할 수 있다고 지각하게 되며, 이 때 비로소 행동의도를 형성한다고 본다.

Bulgurcu et al.[8]은 계획된 행동 이론, 합리적 선택 이론(Rational choice theory)과 정보보안 지각을 기반으로 조직원들의 정보보안 정책 준수와 관련된 연구를 하였다. 합리적 선택 이론이란 개인이 선택의 상황에 놓였을 때 어떻게 결정을 내리는지에 대한 설

명으로, 개인이 자신이 생각하는 혜택과 비용을 저울질하여 합리적인(개인의 선호에 따른)쪽으로 결정한다고 가정한다. 그리고 이러한 개인의 선호는 선택의 결정의 혜택과 비용에 대한 개인의 인식에 영향을 받는다.

2.2.2 중화이론

기존 연구에서는 억제이론을 바탕으로 다양한 조직에서 정보보안 정책 위반자에 대해 벌금징수, 징계 등을 통해 처벌(Sanctions)을 제안하였다[37, 30, 34, 18]. 처벌에 바탕을 둔 억제모델이 일부 성공적이긴 했지만, 인간의 정보보안 위반 이유에 대한 잠재요인들이 잘 이해되지 않음으로써 그 성공은 다소 제한적이었다.

Siponen and Vance[32]는 조직원들이 중화기법을 사용할 수 있기 때문에 처벌의 공포가 항상 정보보안 정책 위반 행위를 잘 설명할 수는 없다고 주장하였다. 중화이론은 범죄학에서 처음 연구되었던 개념으로[24], 법을 준수하는 사람이나 범죄를 저지르는 사람이 모두 규범과 공동체의 가치를 믿는다고 주장한다. 그럼에도 사람들이 범죄를 저지르는 이유는 규칙을 위반하거나 반사회적 행동을 할 때 중화기법을 적용함으로서 심리적으로 이를 가능하게 한다는 것이다[35]. 중화기법은 규범을 위반하는 행동을 정당화시킴으로써 존재하는 규범을 무력화시키는 방법을 제공한다[27]. 즉, 규범 위반 행위 이후의 변명이나 합리화가 아닌 행위발생 이전에 규범의 위반 억제기능을 무력화하는 논리로 Sykes and matza[35]는 5가지의 중화기법을 제시하였다. 첫 번째는 “책임의 부인(denial of responsibility)”으로 부정한 행위를 저지른 사람들이 자신의 책임이 없다고 정의하는 것을 말한다[27, 35]. 두 번째는 “피해의 부인(denial of injury)”으로 행위가 불러올 피해를 최소화시키는 것을 정당화하는 기법이다. 세 번째는 “충성심에의 호소(appeal to higher loyalties)”로 자신의 행위가 옳지 않은 줄은 알지만 친구, 가족과 같은 친근 집단에 대한 충성심에서 부득이 그러한 행동을 할 수 밖에 없다고 여기는 등 법이나 규칙을 위반하는 비용을 수반해야 문제 해결을 할 수 있는 딜레마에 빠진 사람들이 사용하는 기법이다. 네 번째는 “비난자 비난(condemnation of condemners)”으로 행위의 목표대상을 비난함으로써 자신의 행동을 중화시키는 것을 말한다. 다섯 번째는 “피해자의 부인(denial of victim)”이다. 예를 들어 동성애자들이나 창녀들처럼 사회적 멸시를 받는 소수자들에 대한 범죄에서 피해자들을 벌을 받아야 마땅한 사람들로 인지하여 이들에 대한 공격행위를 정당한 복수나 당연한 응보로 간주하는 것이다[4].

Siponen and Vance[32]는 중화기법이 조직원들이 정보보안 정책을 위반하는데 어떠한 영향을 미치는지를 연구하였으며, 이들의 연구에서는 Sykes and matza[35]가 제안한 중화기법 중 “피해자의 부인”을 제외하고 Klockars [21]가 제안한 “회계원장 은유(metaphor of the ledger)”와 Minor[22])가 제안한 “필연성 항변(defense of necessity)”을 추가하였다. “회계원장 은유”는 나쁜 행동을 좋은 행동으로 보상하려는 심리이다. 즉, 개인이 이전에 수많은 좋은 행동을 행했고 그로 인한 선의와 호의를 받아왔으면 약간의 나쁜 행동을 해도 된다고 믿는 것을 말한다[21, 24]. “필연성 항변”은 규칙을 위반하는 것이 반드시 필요하

다는 관점에서 위반 행위 시 죄책감을 느끼지 않아도 된다고 심리적으로 정당화하는 것을 말한다[22].

그 외에 Cressey[13]는 연구에서 “편재성의 항변(defense of ubiquity)”이란 개념을 처음으로 소개하였고 후에 Coleman[12]이 화이트칼라 범죄의 중화기법을 추가적으로 개발하면서 “편재성의 항변”을 중화기법의 보기로 제시하였다. 편재성의 항변이란 누구나 그렇게 하므로 자신의 부당한행위도 정당화될 수 있다고 여기는 것이다. 이철[4]은 편재성 항변을 포함한 6개의 중화기법이 순응자 일탈에 미치는 영향에 대한 연구를 진행하였고 편재성 항변이 다른 기법들과 마찬가지로 중화효과를 보임을 밝혀내었다.

2.2.3 보호동기이론

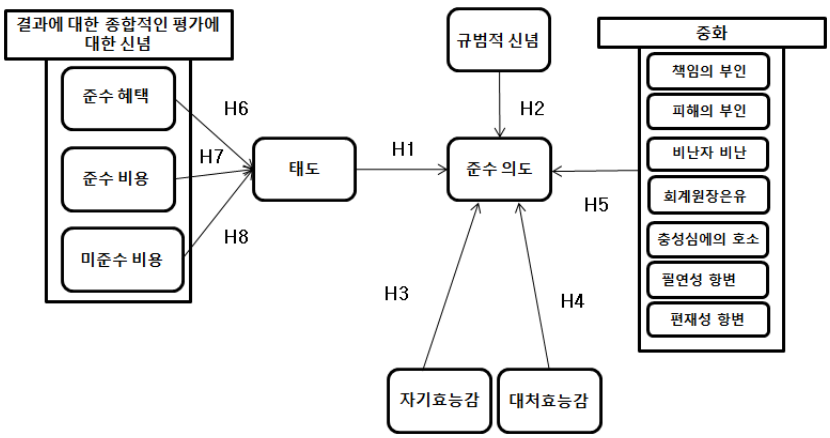
보호동기 이론이란 개인이 위험 메시지에 반응하여 어떻게 태도와 행동을 바꾸는지를 설명하는 이론이다. Rogers[28]의 연구에서 그동안 심리학에서 논의되어왔던 공포소구(Fear Appeal)와 관련하여 행동의도에 영향을 미치는 변수들을 정리하여 변수간의 관계를 포괄적으로 알아보고자 함에서 처음 논의되었다. 보호동기이론에 의하면, 개인이 심리적으로 위협을 느낄 만한 외부 메시지에 노출될 경우, 행위에 자극이 되는 몇 가지 심리적 보호동기들이 만들어진다. 보호동기이론은 공포소구에 세 가지의 중요한 구성요소들이 있다고 가정하고 있다. (1)위협의 크기를 의미하는 심각성(severity), (2)자신이 그 위협에 노출될 가능성(exposure), (3)위협에 대처하는 방안이 얼마나 효과적인지 판단하는 대처효능감(response efficacy)이 그것이다. 그 이후 연구[29]에는 자기효능감(Self-efficacy)이 추가되었다.

Johnston and Warkentin[19]은 공포소구가 조직원들의 보안행위에 어떠한 영향을 미치는지를 알아보는 연구를 진행하였고, 보호동기이론을 기반으로 하여 연구모형을 도출하였다. 기술수용에 관한 문헌고찰을 통해 ‘사회적 영향’과 ‘행동 의도’의 변수를 추가함으로써 기존의 보호동기모형을 확장시켰다. 또한 기존 보호동기이론에 대한 문헌 고찰을 통해 위험 심각성과 위험민감성이 효능감에 영향을 미친다고 가정하였고, 효능감이 행동의도에 바로 영향을 미친다고 가정하여 기존의 모형을 간명화 하였다.

3. 연구모형 및 가설

본 연구는 계획된 행동 이론에 따라 정보보안 정책 준수에 대한 태도, 규범적 신념, 자기효능감이 정보보안 정책 준수의도에 영향을 미친다는 큰 틀에, 중화기법을 참조하여 중화기법 또한 정보보안 정책 준수의도에 영향을 미친다고 가정하였다. 그리고, Ajzen[15]과 Bulgurcu et al.[8]의 연구에 근거하여 ‘결과에 대한 전체적 평가에 대한 신념’이 정보보안 정책 준수에 대한 태도에 영향을 미친다고 가정하였다. 마지막으로 보호동기이론을 참조하여 대처효능감 역시 정보보안 정책 준수 의도에 영향을 미친다고 가정하였다. 앞서 기술한 이론적 고찰을 바탕으로 한 본 연구의 연구모형은 <그림 1>과 같다.

계획된 행동 이론에서는 행동 의도를 형성하는 3가지 독립된 선행 독립변수들을 태도, 주관적 규범, 지각된 행동통제로 보았다. 이



〈그림 1〉 연구모형

를 본 연구의 주제에 맞게 적용하여 태도를 정보보안 정책 준수에 대한 태도로, 규범적 신념을 정보보안 정책 준수에 대한 규범적 신념으로 정의하였다. 또한 계획된 행동 이론에서의 지각된 행동통제는 자기효능감의 개념에서 유래되었고[6], 그 구성개념이 거의 같기 때문에 본 연구에서는 지각된 행동통제를 자기효능감으로 보고자 하여 정보보안 정책 준수에 대한 자기효능감이라고 정의하였다. 계획된 행동이론에 입각할 때 태도가 호의적일수록, 어떤 행동을 함에 있어 행위자가 중요하게 여기는 사람들이 그 행동에 대해 호의적으로 생각할수록, 특정 행동 수행에 있어 능력과 자신감을 많이 가지고 있다고 여길수록 행동하고자 하는 의도가 강해진다고 할 수 있으므로, 정보보안 준수에 대한 태도가 긍정적일수록, 조직원의 주변에서 정보보안 정책 준수행동에 대해 호의적으로 생각한다고 여길수록, 정보보안 정책 준수를 할 수 있는 능력을 가지고 있다고 생각할수록 정보보안 정책에 대한 태도가 긍정적으로 형성될 것으로 추론된다. 위의 내용들을 바탕으로 하여 다음의 가설 1~가설 3을 도출하였다.

가설 1 : 조직원의 정보보안 정책 준수에 대한 태도가 긍정적일수록 정보 보안 정책 준수의도가 높을 것이다.

가설 2 : 조직원의 정보보안 정책 준수에 대한 규범적 신념이 강할수록 정보보안 정책 준수의도가 높을 것이다.

가설 3 : 조직원의 정보보안 정책 준수에 대한 자기효능감이 강할수록 정보보안 정책 준수의도가 높을 것이다.

대처효능감이란 권고된 대처 방안이 위협을 효과적으로 막을 수 있을 것이라는 개인의 믿음의 정도이다[28]. 보호동기이론에 의하면, 적절히 높은 대처효능감은 권고되는 대처방안을 선택하게 함으로써 위협의 감소에 긍정적인 영향을 준다. 위의 이론을 본 연구 주제에 적용시켜보면, 정보보안의 위협에 대해 권고되는 대응방안을 정보보안 정책으로 볼 수 있다. 그러므로 정보보안 정책이 정보보안에 효과적일 것이라고 믿는 정도가 본 연

구에서의 대처효능감이다. 즉, 조직원들이 정보보안 정책이 정보보안에 효과적이라고 믿는 정도가 클수록 권고된 방안인 정보보안 정책을 준수할 의도가 높아질 것이다. 이러한 이론적 추론을 바탕으로 다음의 가설 4가 도출될 수 있다.

가설 4 : 조직원의 정보보안 정책 준수에 대한 대처효능감이 강할수록 정보보안 정책 준수의도가 높을 것이다.

기존 연구들에 의하면 사람들은 보통 자기 자신과 다른 사람들에게 호의적으로 보이고 싶은 자연스러운 욕망을 가지고 있다[17, 26]. 그러므로 조직원들이 조직생활에서 정당치 못한 행위를 할 경우 이러한 부정행위에 대해 변명하고 정당화시킴으로써 자신은 원래 도덕적이고 곧은 사람이라는 점을 유지시키고자 한다. 이렇게 부정한 행위를 변명하고 정당화시킬 때 중화기법이 사용되어질 수 있다. 이를 본 연구 주제에 적용해보면, 조직원들이 정보보안 정책을 위반하려고 할 때 중화기법을 사용함으로써 자신의 행위를 정당화시켜 위반 행위를 좀 더 쉽게 할 수 있을 것이다.

하지만 중화이론이 주로 범죄나 비행행위를 설명하였기 때문에 정책을 위반하는 것을 범죄를 저지르는 행위와 동일시하여 적용하기에 적절치 않다는 견해가 있을 수 있다. 비록 정보보안 정책 위반은 범죄행위는 아니지만, 사회적 규범을 위반하는 것으로 볼 수 있고, Akers and Sellers(2004)는 범죄학 이론에서 설명하기를 '위반'이 법을 어기는 것이거나 비록 법을 어기지 않더라도 사회적 규범을 위반하는 부당한 행위 모두를 지칭한다고 하였다. 그러므로 정보보안 정책 위반 행위도 중화이론으로 설명될 수 있다.

그리고 본 연구에서는 중화를 다차원의 2차적 구성(second-order construct)으로써 분석하고자 한다. 그 이유로 이론 고찰에서 살펴보면 중화이론은 몇 가지의 뚜렷한 차원을 보여주고 있다는 것을 들 수 있다. Petter et al.[23]에 따르면 이러한 복합적 구성(Complex construct)을 연구에서 다룬다면 이를 다차원적인 구성으로 모델링하여 좀 더 철저한 측정과 분석을 해야 한다고 하였다. 또한 2차적 구성은 반영적인 하위 구성들로 형성된다. 이러한 방식으로 구성된 construct는 전체적인 개념의 구성영역을 보고자 하여 다수의 하위 구성과 측정 항목들이 필요한 상황에서 유용하다. 이러한 구성은 특히 중화이론에 잘 적용될 수 있다. 중화이론의 경우 이론을 구성하는 다양한 차원들이 이미 범죄학 연구를 통해 많이 밝혀졌기 때문이다[32]. 이에 근거하여 본 연구에서는 '중화'를 2차적 구성으로 개념화하였다. 이를 토대로 하여 다음의 가설 5가 도출 가능할 것이다.

가설 5 : 조직원의 중화수준이 높을수록 정보보안 정책 준수의도가 낮을 것이다.

기존 문헌에 따르면 행동을 수행하는 것에 대한 개인의 태도는 행동에 관련된 결과에 대한 개인의 신념과 관련이 있다[6, 15]. 또한 합리적 선택이론(Rational Choice Theory : RCT)에 의하면 개인은 어떤 행동여부를 결정할 때 양자택일의 상황이 오면 비용과 혜택에 대해 고려한 후 혜택이 큰 경우 행동을

하게 된다. 이를 적용하여 본 연구에서는 태도와 관련된 결과에 대한 개인의 신념을 합리적인 선택 이론을 적용하여 알아보고자 하였다. 조직원들의 정보보안 정책 준수 행동에 대한 양자선택은 정책을 준수하는 것과 준수하지 않는 것으로 볼 수 있고, 조직원들은 종합적인 내용에 대한 고찰을 거친 후에 이익이 크고 비용이 작은 쪽으로 최종 결정을 내리게 될 것이다. 위의 고찰을 바탕으로, 정보보안 정책 준수와 관련된 결과에 대한 전체적인 평가에 대한 개인의 신념을 세 가지 개념으로 묶었다. 첫 번째는 '준수에 따른 혜택', 두 번째는 '준수에 따른 비용', 세 번째는 '미준수에 따른 비용'이다. 조직원들이 정보보안 정책을 준수하는 것에서 혜택이 따르고, 준수하지 않음에서 비용이 수반되며, 정책을 준수함에 적은 노력이 든다고 인지한다면 정책 준수에 대한 태도가 호의적으로 형성될 것이다. 이러한 가정은 준수 행동이 정책을 준수할 때의 혜택과 준수하지 않을 시의 비용들로 이루어진 판단과 긍정적인 영향관계가 있다는 기존 연구[38]와도 일치한다. 또한 보안의 상황에서는 요구되는 보안 행동을 하기 위해 좀 더 비용을 들여야 하는데, 여기서 비용이란 시간과 노력을 의미한다. 이러한 비용이 많이 들게 되면 조직원들은 요구되는 보안 행동을 하지 않으려 할 것이다[25]. 그러므로 위의 이론적 추론을 통해 준수 행동에 대한 선행요인으로서의 태도에 대해 다음과 같은 가설 6~가설 8이 도출될 수 있을 것이다.

가설 6 : 조직원의 정보보안 정책 준수에 대한 혜택의 인지수준이 높을수록 정보보안 정책을 준수하고자 하는 태도가 강할 것이다.

가설 7 : 조직원의 정보보안 정책 준수에 대한 비용의 인지수준이 높을수록 정보보안 정책을 준수하고자 하는 태도가 약할 것이다.

가설 8 : 조직원의 정보보안 정책 미준수에 대한 비용의 인지수준이 높을수록 정보보안 정책을 준수하고자 하는 태도가 강할 것이다.

4. 변수의 조작적 정의 및 측정방법

4.1 변수에 대한 조작적 정의

본 연구에서 사용된 변수는 관련 연구들을 바탕으로 본 연구의 목적에 맞게 수정하였다. 각 변수에 대한 조작적 정의 및 관련 연구들은 <표 1>과 같다.

4.2 자료수집 및 분석방법

본 연구의 설문대상은 '정보보안 정책이 있는 조직에서 정보시스템을 사용하는 사용자들'로 하였다. 자료의 수집은 웹 설문 및 온·오프라인 설문 배포를 통해 이루어졌고, '중화'를 측정하기 위해 시나리오 기법을 사용하여 설문 중간에 짧은 상황시나리오를 읽고 중화에 대한 항목에 답하도록 하였다. 시나리오는 총 3개로 이 중 한 개씩 응답자에게 무작위 배포되었다. 총 207개의 설문이 수집되었고 이 중 결측치가 있거나 불성실하게

응답한 13부를 제외한 194부를 분석하였다. 응답자의 특성은 SPSS 18.0, 변수의 신뢰도 및 타당성 검증과 가설검증은 PLS를 통해 분석하였다. PLS는 연구모델이 이론개발의 초기단계에 있어 아직 철저히 검증되지 않았을 때 적합한 분석방식이고 비교적 적은 샘플에서도 복잡한 인과관계 모형의 설명력을 잘 나타낸다. 또한 중화와 같은 2차적 구성의 경우 LISREL로 분석하면 문제가 발생할 가능성이 있다[10]. 이러한 점들을 고려하여 자료분석 도구로 SmtartPLS ver 2.0.M3을 채택하였다.

〈표 1〉 변수에 대한 조작적 정의

변수		조작적 정의	측정항목	관련연구
준수 의도		정보보안 정책을 준수함으로써 잠재적인 보안 위협으로부터 조직의 정보, 기술 자원을 보호하려는 의도의 정도	IN1~3	Bulgurcu et al.[8]
규범적 신념		정보보안 정책을 준수할 때 개인이 지각하는 중요한 참고인들(임원, 동료, 매니저 등)의 사회적 압박수준	NB1~3	Bulgurcu et al.[8]
중화		정보보안 정책 준수 위반 행위 발생 이전에 심리적으로 위반 행위를 정당화시킴으로써 사회적 규범인식을 희석시켜 정책위법행위를 할 수 있도록 하는 논리에 의존하는 정도		Sykes and Matza[35] Siponen and Vance[32] 이철[4]
중화기법	책임의 부인	정보보안 정책 위반행위 시 자신의 책임이 없다고 여기는 정도	DR1~3	
	피해의 부인	정보보안 정책 위반행위 시 행위의 피해가 적다고 여기는 정도	DI1~3	
	충성심에의 호소	정보보안 정책 위반행위가 자신이 속한 집단을 위한 일이라고 여기는 정도	AL1~3	
	비난자 비난	정보보안 정책 위반행위를 비난하는 대상이 더 비난 받아야 한다고 여기는 정도	CC1~3	
	회계원장 은유	이전에 행한 좋은 행위들이 정보보안 정책 위반행위를 상쇄시켜줄 것이라 여기는 정도	ML1~3	
	필연성 항변	정보보안 정책 위반행위가 꼭 필요한 상황이므로 용인될 수 있다고 여기는 정도	DN1~3	
	편재성 항변	누구나 정보보안 정책 위반행위를 하므로 용인될 수 있다고 여기는 정도	DU1	
태도		정보보안 준수행동의 결과가 긍정적으로 평가되는지의 정도	AT1~4	Bulgurcu et al.[8]
준수 혜택		정보보안 정책을 준수함에 따라 기대되는 호의적 결과수준	BE1~4	Bulgurcu et al.[8]
준수 비용		정보보안 정책을 준수함에 따른 호의적이지 않은 결과수준	CO1~3	Bulgurcu et al.[8]
미준수 비용		정보보안 정책을 준수하지 않음에 따른 호의적이지 않은 결과수준	NC1~4	Bulgurcu et al.[8]
자기효능감		정보보안 정책 준수 시 필요한 개인적 기술, 지식, 능력에 대한 스스로의 자신감 정도	SE1~3	Bulgurcu et al.[8]
대처효능감		정보보안위협을 줄이기 위한 대처방안인 정보보안 정책에 대한 개인의 믿음 정도	RE1~3	Johnston and Warkentin[19]

5. 가설검증 및 결과분석

5.1 변수의 타당도와 신뢰도 검증

5.1.1 신뢰도 검증

복합신뢰도(CSRI)값이 0.7 이상이고, 평균분산추출(AVE)값이 기준치인 0.5 이상일 경우 내적일관성이 있다고 볼 수 있다[10]. 모든 변수들에 있어서 평균분산추출값(AVE)은 0.73 이상의 값을 보였고, 복합신뢰도(Composite Reliability)는 0.95 이상의 값을 보였으며, 크론바흐 알파(Cronbach's Alpha)값도 0.93 이상을 보임으로써 모든 변수들이 신뢰성을 확보하고 있는 것으로 나타났다.

5.2.2 타당도 검증

타당성 검증 대상 변수에 대한 요인적재량 값이 0.7 이상이 되어야하고 그 요인적재량은 그 외의 변수들에 대한 교차 요인적재량보다 커야 집중타당성을 확보한다고 본다[16, 33]. 요인분석의 결과인 <표 2>에 따르면 모든 변수들에 있어서 잠재변인별 측정항목의 요인적재량이 0.7 이상이고, 다른 측정항목과의 교차요인적재량 값보다 해당 측정항목의 값이 큰 것으로 나타났으므로 집중타당성이 확보되는 것으로 나타났다. 또한 판별타당성을 확인하기 위해 우선 각 측정항목들의 적재량이 다른 요인들과의 교차요인 적재량보다 큰지를 확인한 결과, <표 2>에서 나타난 바와 같이 각 측정항목들의 적재량이 다른 요인에 적재된 요인 값보다 모두 큰 것을 확인할 수 있다.

판별타당성을 확보하기 위한 두 번째 조건으로서 해당 변수의 평균분산추출(AVE)값의 제곱근이 다른 변수들 간의 상관계수보다 모두 커야 하는 바, 모든 변수들에 있어서 이 조건이 충족된 것을 확인할 수 있는 것으로 나타나, 두 가지 조건이 모두 충족된 것으로 보아 변수들 모두 판별 타당성이 확보되었다고 할 수 있다.

5.2 연구모형의 적합성 검증

PLS에서는 내생변수의 설명된 분산을 극대화하는 것이 목표이고, 분포에 대한 가정을 하지 않기 때문에 공분산구조분석 모델에서 이용되는 전체 적합도 측정치(goodness-of-fit measures)보다는 연구 단위들과 내생변수들의 설명된 분산들 간의 관계에 대한 전체적인 유의수준에 의한 적합도가 주로 평가된다. 따라서 예측적합도, 전반적 적합도의 2가지의 적합도를 고려해야한다. 예측 적합도는 R^2값을 사용하여 도출하며, 상(0.26 이상), 중(0.13 이상~0.26 미만), 하(0.02 이상~0.13 미만)로 구분하여 판단한다[10]. 그러나 이러한 R^2값은 모수를 추정하는 데 사용되는 자료의 편의성을 충분히 고려하지 못하기 때문에 주로 Stone-Geisser Q2 test 통계량인 중복성(Redundancy)값을 이용하며[11], 중복성 값이 0보다 클 경우 예측적합도가 있는 것으로 해석한다. 다음으로 전반적 적합도는 모든 내생변수의 분산설명력(R^2)값의 평균과 공통성(communality)의 평균값을 곱한 값에서 제곱근을 통해 산출한다[36]. 적합도의 크기는 최소 0.1 이상이어야 하고 상(0.36 이상), 중(0.25~.36), 하(0.1~0.25)로 구분된다. <표 3>에서 나타난 결과를 보면 분산설명력 값(R^2)이 준수의도는 81.6%, 태도는 61.1%를 보이고 있고 중복성 값은 모두 양수

〈표 2〉 요인 적재량과 교차요인 적재량

변수 / 항목	충성심 호소 (AL)	태도 (AT)	준수혜택 (BE)	비난자 비난 (CC)	준수비용 (CO)	피해부인 (DI)	필연성 항변 (DN)	책임부인 (DR)
AL1	**0.967**	-0.591	-0.431	0.823	0.528	0.756	0.818	0.725
AL2	**0.976**	-0.596	-0.429	0.812	0.508	0.747	0.826	0.729
AL3	**0.958**	-0.571	-0.394	0.804	0.547	0.724	0.842	0.712
AT1	-0.641	**0.920**	0.640	-0.593	-0.493	-0.645	-0.604	-0.656
AT2	-0.499	**0.933**	0.737	-0.467	-0.415	-0.523	-0.457	-0.576
AT3	-0.574	**0.957**	0.714	-0.491	-0.499	-0.580	-0.540	-0.620
AT4	-0.560	**0.949**	0.747	-0.527	-0.456	-0.553	-0.523	-0.614
BE1	-0.484	0.734	**0.902**	-0.457	-0.422	-0.581	-0.450	-0.552
BE2	-0.433	0.723	**0.956**	-0.396	-0.410	-0.538	-0.427	-0.569
BE3	-0.345	0.680	**0.951**	-0.305	-0.393	-0.460	-0.354	-0.486
BE4	-0.343	0.671	**0.920**	-0.311	-0.401	-0.435	-0.367	-0.463
CC1	0.773	-0.488	-0.347	**0.949**	0.476	0.739	0.740	0.699
CC2	0.841	-0.551	-0.404	**0.971**	0.536	0.749	0.818	0.705
CC3	0.812	-0.556	-0.391	**0.967**	0.536	0.716	0.785	0.721
CO1	0.596	-0.515	-0.441	0.556	**0.871**	0.498	0.601	0.572
CO2	0.421	-0.408	-0.362	0.413	**0.893**	0.333	0.444	0.424
CO3	0.373	-0.351	-0.320	0.412	**0.867**	0.292	0.392	0.383
DI1	0.701	-0.553	-0.495	0.700	0.371	**0.956**	0.707	0.704
DI2	0.757	-0.599	-0.532	0.757	0.448	**0.978**	0.724	0.721
DI3	0.775	-0.631	-0.551	0.763	0.467	**0.977**	0.737	0.742
DN1	0.763	-0.515	-0.362	0.724	0.506	0.669	**0.924**	0.624
DN2	0.835	-0.536	-0.416	0.784	0.544	0.723	**0.968**	0.683
DN3	0.848	-0.564	-0.448	0.810	0.555	0.734	**0.965**	0.701
DR1	0.711	-0.678	-0.580	0.672	0.513	0.714	0.685	**0.941**
DR2	0.665	-0.523	-0.451	0.655	0.502	0.612	0.611	**0.909**
DR3	0.710	-0.628	-0.519	0.728	0.492	0.748	0.669	**0.944**

변수 / 항목	편재성 항변 (DU)	준수의도 (IN)	회계원장은유 (ML)	규범적신념 (NB)	미준수비용 (NC)	대처효능감 (RE)	자기효능감 (SE)
DU1	**1.000**	-0.551	0.722	-0.468	-0.291	-0.482	-0.351
IN1	-0.541	**0.982**	-0.677	0.811	0.488	0.794	0.579
IN2	-0.543	**0.980**	-0.668	0.788	0.496	0.789	0.582
IN3	-0.536	**0.977**	-0.669	0.829	0.511	0.798	0.583
ML1	0.704	-0.666	**0.974**	-0.602	-0.323	-0.578	-0.355
ML2	0.708	-0.679	**0.984**	-0.616	-0.361	-0.597	-0.380
ML3	0.708	-0.666	**0.977**	-0.587	-0.345	-0.589	-0.337
NB1	-0.409	0.685	-0.499	**0.893**	0.473	0.642	0.524
NB2	-0.455	0.824	-0.616	**0.960**	0.506	0.738	0.582
NB3	-0.458	0.817	-0.613	**0.972**	0.524	0.746	0.604
NC1	-0.237	0.431	-0.291	0.433	**0.926**	0.405	0.312
NC2	-0.323	0.527	-0.368	0.536	**0.972**	0.478	0.361
NC3	-0.298	0.514	-0.358	0.529	**0.980**	0.464	0.365
NC4	-0.255	0.475	-0.323	0.534	**0.964**	0.453	0.353
RE1	-0.467	0.763	-0.571	0.713	0.465	**0.956**	0.638
RE2	-0.443	0.748	-0.535	0.693	0.412	**0.963**	0.628
RE3	-0.477	0.818	-0.619	0.763	0.474	**0.960**	0.624
SE1	-0.340	0.558	-0.330	0.578	0.382	0.613	**0.961**
SE2	-0.333	0.581	-0.352	0.601	0.319	0.650	**0.973**
SE3	-0.344	0.579	-0.376	0.577	0.353	0.637	**0.963**

로 나타났으며 연구모형의 전반적 적합도는 0.857로 상급의 유의한 수준임을 알 수 있다. 따라서 본 연구모형은 통계적으로 적합성을 확보한 것으로 판단할 수 있다.

〈표 3〉 연구모형의 적합성 검증결과

	분산설명력	공통성	중복성
규범적신념		0.888	
대처효능감		0.921	
미준수비용		0.923	
비난자비난		0.926	
자기효능감		0.932	
준수비용		0.770	
준수의도	0.816	0.960	0.336
준수혜택		0.870	
중화*	1	0.735	0.221
책임부인		0.868	
충성심호소		0.935	
태도	0.611	0.884	0.084
편재성 항변		1	
피해부인		0.942	
필연성항변		0.907	
회계원장은유		0.957	
평균값	0.809	0.901	0.214
모형 전체 적합도	0.857		

주) *중화는 2차적 구성(second-order construct)임).

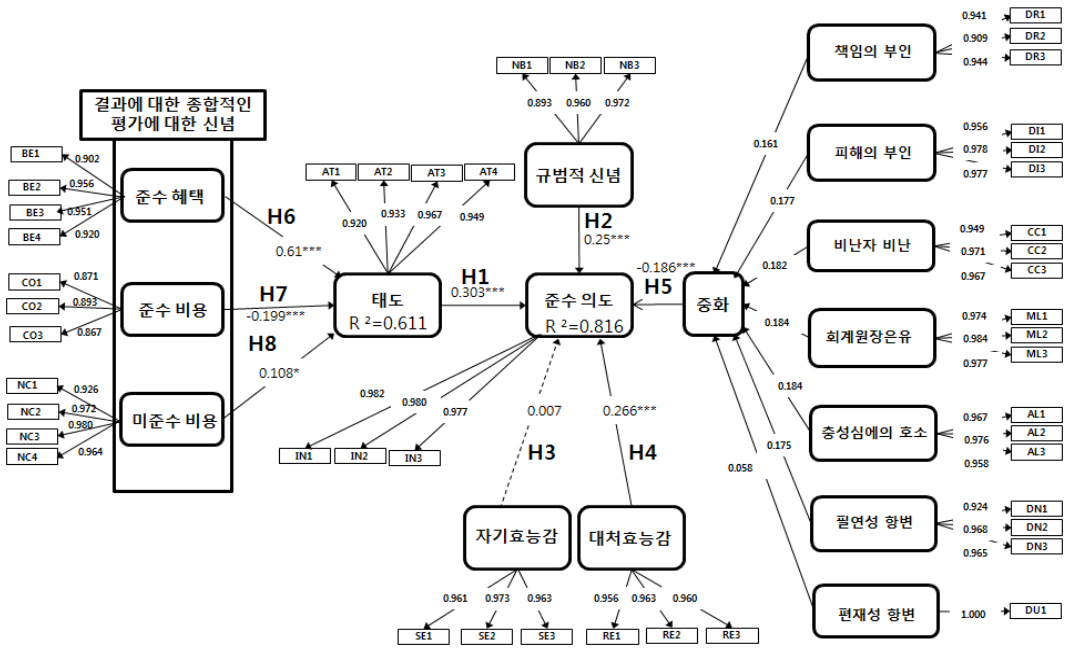
5.3 가설검증 결과

PLS에서는 경로계수의 유의성 검증 및 신뢰구간 추정을 직접 제시해주지 않으므로 가설검증은 부트스트랩을 사용하여 경로계수의 유의성을 추정하여 평가하였고, 분석 결과는 <그림 2>와 같다.

가설 1은 경로계수가 0.303이고 t값이 3.895로 태도가 긍정적일수록 준수의도가 높은 것으로 나타나 채택되었다. 이는 계획된 행동 이론에 근거한 변수 간 관계가 정보보안 분야에도 적용될 수 있음을 보이는 것이다. 즉. 조직원들의 정보보안 정책에 대한 태도가 긍정적이면 준수의도에 강한 영향을 미치고 결국 행동을 하게 됨을 의미한다. 그러므로 조직원의 정보보안 정책 준수에 대한 태도가 긍정적인 방향이 되도록 유도함이 정책 준수를 위한 선행 요소로 중요한 것임을 알 수 있다.

가설 2는 경로계수가 0.25이고 t값이 3.136으로 규범적 신념이 강할수록 준수의도가 높을 것으로 나타나 채택되었다. 이것은 조직원들이 정보보안 정책을 준수할 때에 자기 자신 내면의 상황만이 아닌 주변의 상황과 시선등 사회적 영향요인을 함께 강하게 고려한다는 사실을 의미한다. 조직생활에서의 사회적 영향요인이란 경영진, 상사, 동료 등이 있다. 이들과의 영향관계가 개인의 정보보안 정책 준수 의도에 중요한 역할을 함을 추측할 수 있다.

가설 3은 경로계수가 0.007이고 t값이 0.128로 두 변수 사이에 통계적 유의성이 없는 것으로 나타나 기각되었다. 본 연구결과를 토대로 보면, 정보보안 정책 준수에 대한 자기효능감의 높거나 낮음은 정보보안 정책 준수의도와 아무런 상관관계가 없다는 것으로 판단된다. 즉, 정보보안 정책을 충분히 지킬 수 있다는 자신감이나 역량은 실제 준수 의도에는 별다른 영향을 미치지 못한다고 해석할 수 있다. 그러므로 조직원이 정보보안 정책을 지킬 능력이나 자신감이 있다고 해서 반드시 정보보안 정책을 준수하는 것은 아니라고 판단된다. 이는 기존연구에서 어떠한 행동 수행



〈그림 2〉 가설검증(경로분석) 결과

에 있어 개인의 역량이 높다고 판단되면 그것을 토대로 행동을 하고자하는 의도가 높게 나타난다는 결과와 상이한 내용이다. 정보보안 정책 준수의 상황에서만 적용된 결과인 것인지에 대한 추후 연구가 필요할 것이다.

가설 4는 경로계수가 0.266이고 t값이 4.395로 대처효능감이 강할수록 준수의도가 높은 것으로 나타나 채택되었다. 즉, 정보보안 정책이 정보보안에 있어 효과적인 대처방안이라고 생각할수록 정책을 준수할 의도가 높아진다는 것이다. 그러므로 조직차원에서 정보보안 정책이 실제로 정보보안 역할을 한다고 조직원들이 여기도록 하는 것이 중요하다는 것을 알 수 있다.

가설 5는 경로계수가 -0.186이고 t값이 4.552으로 중화수준이 높을수록 준수의도가 낮은 것으로 나타나 채택되었다. 즉, 조직원들이 정책준수에 앞서 중화의 7가지 기법을 통해 준수하지 않으려는 마음을 합리화시키는 정도가 클수록 준수의도가 실제로 낮아진다고 판단할 수 있다. 또한 중화를 이루는 하위 구성요소 모두 중화구성에 유의한 값을 보였으므로 중화의 구성이 잘 이루어졌다고 볼 수 있다. 다만 다른 요인에 비해 '편재성 항변'의 경로계수 값이 0.058로 다른 요인의 계수 값에 비해 낮은 것으로 나타났다. 그러나 경로계수 값이 다른 계수에 비해 작게 나왔을 뿐, 통계적인 유의성은 확보되었고, 다른 요인의 측정개수보다 적은 점을 고려하여 중화의 구성요소로 보아야 한다고 판단하였다.

가설 6은 경로계수가 0.61이고 t값이 9.181으로 혜택의 인지수준이 높을수록 준수의도가 높은 것으로 나타나 채택되었다. 특히 t값과 경로계수 값이 결과에 대한 종합적인 평

가에 대한 세 가지 신념 중에 제일 높은 것으로 나타났다. 이는 곧 다른 요인들보다 정보보안 정책 준수에 대한 혜택의 인지가 클수록 정보보안에 대한 태도에 매우 긍정적인 영향을 미침을 뜻한다. 정보보안 정책 준수에 대한 혜택은 금전적 혜택이나 주위의 평판의 상승, 인사고과에 긍정적으로 반영되는 것, 개인이 느끼는 보람, 뿌듯한 감정 등이 있을 수 있다. 이러한 요인들을 부각시켜 조직원들이 인지하는 정책 준수에 대한 혜택수준이 높아지도록 하는 것이 중요함을 알 수 있다.

가설 7은 경로계수가 -0.199이고 t값이 3.669으로 비용에 대한 인지수준이 높을수록 준수에 대한 태도가 호의적이지 못한 것으로 나타나 채택되었다. 이 결과로 정보보안 정책을 지킬 때에 수반되는 비용, 즉 번거로움, 시간, 노력 등의 정도가 클수록 정보보안 정책을 준수에 대한 태도가 부정적으로 된다는 것을 알 수 있다. 그러므로 조직원들이 이에 대한 인식을 줄일 수 있게 하는 방안이 모색되어야 할 것이다.

가설 8은 경로계수가 0.108이고 t값이 1.716으로 정보보안 정책의 미준수에 대한 비용의 인지수준이 높을수록 준수에 대한 태도가 강한 것으로 나타나 채택되었다. 정보보안 정책 미준수에 대한 비용이란, 정보보안 정책을 지키지 않음으로써 생기는 비용으로, 개인적인 죄책감, 사회적 평판의 악화, 인사고과상의 불이익 등이 있을 수 있다. 다른 2개의 신념보다는 영향력이 약한 것으로 나타났지만, 태도와의 상관관계가 있는 것으로 나타났으므로 조직원들에게 정보보안 정책 미준수에 대한 비용을 인지시키는 것 또한 준수의도를 높이기 위해 필요하다고 할 수 있다.

6. 결 론

본 연구는 조직원들의 정보보안 정책의 준수 의도에 영향을 미치는 요인들이 무엇인지 규명하고 향후 조직원들의 정보보안 정책 준수성을 높이기 위한 향후 방안을 제시하고자 함을 목표로 설정하였다. 이를 위해 우선 정보보안과 정보보안 정책의 개념, 정보보안 정책 준수의 필요성을 문헌고찰을 통해 살펴본 뒤 준수 의도에 영향을 미치는 요인들을 계획된 행동이론을 통해 태도, 규범적 신념, 자기효능감, 결과에 대한 종합적인 평가에 대한 신념을 도출해 내었다. 또한 억제이론, 중화이론을 통해 중화기법 7가지가 준수의도를 약화시킬 것이라는 가정을 내렸다. 마지막으로 보호동기이론을 통해 대처효능감은 준수의도에 긍정적인 영향을 미칠 것이라 추론하였다. 이러한 문헌고찰을 통해 연구모형을 도출하였고 연구가설을 설정하였으며 조작적 정의를 통해 측정항목을 도출하였다. 그리고 모형의 검증을 위해 수집한 자료를 PLS방법론을 이용하여 검증하였다. 분석 결과, 8개의 가설 중 자기효능감이 태도에 영향을 미친다는 가설을 제외한 7개의 가설이 지지됨을 확인할 수 있었다.

본 연구의 이론적 측면의 시사점으로는 첫째, 조직원들의 정보보안 정책 준수의도에 영향을 미치는 요인들을 폭넓게 살펴봄에 따라 향후 정보보안 정책 준수 의도에 영향을 미치는 요인들을 규명하는 연구들의 기반 연구가 될 것으로 기대한다. 둘째, 기존 IT관련 연구에서 흔히 규명되었고 볼 수 있었던 변수들 외에 범죄학 등 심리학에서 근거한 요인을 접목하여 IS 연구와 심리학 연구의 고찰을 통해 연

구의 폭을 넓혔다는 점이다. 셋째, 이론적 고찰을 통해 정보보안 정책 준수에 관한 요인들에 대한 조작적 정의를 구체화시켜 제시하였다는 점이다. 본 연구는 모형 상으로는 일반적인 변수를 사용함으로써 정보보안 분야만이 아닌 다양한 분야에 적용될 수 있으나 조작적 정의를 정보보안 정책 준수와 관련해 재정의함으로써 정보보안 상황에 맞게 연구를 진행하였다. 향후 정보보안 정책 분야에서 이에 대한 연구를 지속시키거나 다른 분야에서도 사용될 수 있을 것으로 기대된다.

본 연구의 실무적 시사점으로는 첫째, 조직에서 정보보안 정책 입안 및 실행 시 본 연구결과가 가이드라인이 될 수 있을 것으로 기대된다. 본 연구는 조직원들의 정보보안 정책 준수 의도에 영향을 미치는 제반 요인들을 규명하고자 한 연구였으므로, 이러한 요인들 간의 관계를 실무에 적용할 수 있을 것으로 예상한다. 둘째, 정보보안 정책 준수에 대한 전체적 평가에 대한 신념이 준수태도에 영향을 미치는 것으로 나타남에 따라 정책 준수에 따른 비용과 혜택에 대한 조직 내 제도의 설립과 이에 대한 홍보방안 수립시의 이론적 토대를 제공하였다. 신념 중에는 특히 준수 혜택에 대한 인식이 클수록 태도에 가장 큰 영향을 미치는 것으로 나타났으므로 이를 부각시킬 수 있는 제도의 마련이 시급하다고 할 수 있다. 셋째, 본 연구결과에 따르면 중화기법이 정보보안 정책 준수의도를 약화시키는 것으로 나타났으므로 조직원들의 중화심리를 억제시키기 위해 조직구성원들에 대한 의식교육 및 훈련프로그램 실시에 대한 필요성을 부각시켰다. 넷째, 자기효능감이 준수의도에 영향을 미치지 못하고, 대처효능감은 준수의도에 큰 영향을 미치는 것으로 나타났으므로 조직에서는 정책 준수를 위한 조직원들의 보안능력강화보다는 정보보안 정책이 실제로 정보보안에 효과가 있다는 점을 주지시킬 수 있는 교육과 홍보방안을 마련해야 한다는 시사점을 도출해 내었다.

본 연구의 한계점 및 향후 연구방향은 다음과 같다.

첫째, 본 연구의 샘플 수는 194개로 연구결과를 일반화시키기에 다소 적은 수이다. 또한 설문 응답자가 주로 남성이고, 20대 사원이며 일부 업종 종사자의 응답비율이 높은 것으로 나타났다. 향후 연구결과의 일반화 가능성을 보다 제고하기 위해 샘플수를 확대하고 설문대상 집단도 다양화해야 할 필요가 있다.

둘째, 자기효능감의 경우 정보보안 정책 준수 의도에 영향을 미치지 못한다는 연구결과가 나타나 정의 결과를 보인다는 실증적 분석결과를 보인 기존 연구와 상이한 결과를 보였다. 이것이 정보보안 정책을 주제로 한 본 연구에서만 적용된 결과인지를 정확히 알기 위해서 향후 연구에서 이에 대한 재검증이 요구된다.

셋째, 본 연구에서 제시된 요인들 외에 정보보안 정책 준수의도에 영향을 미칠 가능성이 큰 요인들, 예를 들어 조직 내 정보보안 공감대 형성 노력, 인사제도와의 연계, 현업 업무 특성 등의 요인들을 감안한 연구모형의 확장이 시도될 필요성이 크다.

참 고 문 헌

[1] 김윤호, “네트워크 노드에 대한 포렌식

분석기법을 적용한 감사시스템의 구현", 한국전자거래학회지, 제14권 ,제3호, pp. 169- 181, 2009.

[2] 안중호, 최규철, 성기문, 이재홍, "보안위험 수준이 지식관리시스템의 성공에 미치는 영향 : '신뢰'를 매개변인으로", 한국전자거래학회지, 제15권, 제4호, pp. 143- 163, 2010.

[3] 이선중, 이미정, "정보보호 문화의 평가지표에 관한 탐색적 연구", 정보화정책, 제15권, 제3호, pp. 100-119, 2008.

[4] 이철, "순응자 일탈에 대한 중화기술의 영향에 관한 연구", 형사정책연구, pp. 243-278, 2008.

[5] 정익재, "정보사회 위험관리로서 정보보안의 정책 논리", 한국행정학회 2005년도 추계학술대회, pp. 19-34, 2005.

[6] Ajzen, I., "The Theory of Planned Behavior," Organizational Behavior and Human Decision, Vol. 50, pp. 179-211, 1991.

[7] Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., and Boss, R. W. "If Someone Is Watching, I'll Do What I'm Asked : Mandatoriness, Control, and Information Security," European Journal of Information Systems, Vol. 18, No. 2, pp. 151-164, 2009.

[8] Bulgurcu, Burcu Cavusoglu, Hasan Benbasat and Izak, "Information Security Policy Compliance : An Empirical Study of Rationality-Based Beliefs and Information Security Awareness," MIS Quarterly, Vol. 34, No. 3, pp. 523-A7, 2010.

[9] Chen, C., Medlin, B., and Shaw, R., "A cross-cultural investigation of situational information security awareness programs," Information Management and Computer Security, Vol. 16, No. 4, pp. 360-376, 2008.

[10] Chin, W., "Issues and opinion on structural equation modeling," MIS Quarterly, Vol. 22, No. 1, pp. 7-16, 1998.

[11] Cohen, J., Statistical Power Analysis for the Behavioral Sciences(2nd ed.), Lawrence Erlbaum, 1988.

[12] Coleman, James, W., "Toward an Integrated Theory of Whitte-Collar Crime," American Journal of Sociology, Vol. 93, pp. 406-439, 1987.

[13] Cressey, Donald R., "Other People's Money : A study in the Social Psychology of Embezzlement," Glencoe, IL : Free Press, 1953.

[14] Durgin, M., "Understanding the Importance of and Implementing Internal Security Measures," SANS Institute Reading Room, 2007.

[15] Fishbein, M. and Ajen, I., Belief, Attitude, Intention, and Behavior : An Introduciton to Theory and Research, Reading, Addison-Wesley, 1975.

[16] 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.

[17] Greenberg, J., The cognitive geometry of

employee theft : negotiating 'the line' between taking and stealing. In R. Griffin, A. O'Leary-Kelly, and J. Collins (Eds.), Dysfunctional behavior in organizations : Nonviolent behaviors in organizations. Part B. Stamford, CT : JAI Press, 1998.

[18] Hoffer, J. A. and Straub, D. W., "The 9 to 5 underground : Are you policing computer crimes?," Sloan Management Review, Vol. 30, pp. 35-43, 1989.

[19] Johnston, Allen C. Warkentin and Merrill, "Fear Appeals and Information Security Behaviors : An Empirical Study," MIS Quarterly, Vol. 34, No. 3, pp. 549-A4, 2010.

[20] Johnston, K. L. and White, K. M., "Binge-drinking : A test of the roll of group norms in the roy of planned behavior," psychology and Health, Vol. 18, No. 1, pp. 63-77, 1995.

[21] Klockars, C. B., "The Professional Fence," New York, FreePress, 1974.

[22] Minor, W. W., "Techniques of Neutralization : A Reconceptualization and Empirical Examination," Journal of Research in Crime and Delinquency, Vol. 18, No. 2, pp. 295-318, 1981.

[23] Petter, S., Straub, D. and Rai, A., "Specifying Formative Constructs in IS Research," MIS Quarterly, Vol. 31, No. 4, pp. 623- 656, 2007.

[24] Piquero, N. L., Tibbetts, S. G., and Blankenship, M. B., "Examining the Role of Differential Association and Techniques of Neutralization in Explaining Corporate Crime," Deviant Behavior, Vol. 26, No. 2, pp. 159-188, 2005.

[25] Price waterhouse Coopers., "Employee Behavior Key to Improving Information Security, New Survey Finds," 2008.

[26] Robinson, S. L. and Kraatz, M. S., Constructing the reality of normative behavior : the use of neutralization strategies by organizational deviants. In R. Griffin, A. O'Leary-Kelly, and J. Collins (Eds.), Dysfunctional behavior in organizations : Violent and deviant behavior. Part A. Stamford, CT : JAI Press, 1998.

[27] Rogers, J. W. and Buffalo, M. D., "Neutralization Techniques : Toward a Simplified Measurement Scale," Pacific Sociological Review, Vol. 17, No. 3, pp. 313-331, 1974.

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

[29] Rogers, R. W., Cognitive and psychological process in fear appeals and attitude change : A revised theory of protection motivation. In J. Cacioppo and R. Petty (Eds.), Social Psychology, NY : Guilford, 1983.

[30] Scholtz, J. T., "Enforcement policy and corporate misconduct : The changing perspective of deterrence theory," Law and Contemporary Problems, Vol.60, pp. 253-268, 1997.

[31] Siponen, M. T., Pahnila, S., and Mah-

mood, A., “Employees’Adherence to Information Security Policies : An Empirical Study,” in New Approaches for Security, Privacy and Trust in Complex Environments, H. Venter, M. Eloff, L. Labuschagne, J. Eloff, and R. von Solms, Boston : Springer, 2007.

[32] Siponen, Mikko Vance and Anthony, “Neutralization : New Insights into the Problem of Employee Information Systems Security Policy Violations,” MIS Quarterly, Vol. 34, No. 3, pp. 487-A12, 2010.

[33] 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.

[34] Straub, D. W. and Nance, W. D., “Discovering and disciplining computer abuse in organizations : A field study,” MIS Quarterly, Vol. 14, pp. 45-60, 1990.

[35] Sykes, G. and Matza, D., “Techniques of Neutralization : A Theory of Delinquency,” American Sociological Review, Vol. 22, No. 6. pp. 664-670, 1957.

[36] Tenenhaus, M., Vinzi, V. E., Chatelin, Y. M., and Lauro, C., “PLS path modeling,” Computational statistics and Data analysis, Vol. 48, No. 1. pp. 159-205, 2005.

[37] Theoharidou, M., Kokolakis, S., Karyda, M., and Kiountouzis, E., “The insider threat of information systems and the effectiveness of ISO17799,” Computers and Security, Vol. 24, pp. 472-484, 2005.

[38] Tyler, T. R. and Blader, S. L., “Can Businesses Effectively Regulate Employee Conduct? The Antecedents of Rule Following in Work Settings,” Academy of Management Journal, Vol. 48, No. 6, pp. 1143-1158, 2005.

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

박선영 (E-mail : sun277@kw.ac.kr)
2009년 광운대학교 미디어영상학과 신문방송학 전공 (학사)
2011년 광운대학교 대학원 경영정보학과 (석사)
관심분야 ERP, 정보보안, 정보화전략 등