www.calsec.or.kr
http://dx.doi.org/10.7838/jsebs.2013.18.1.147

정보보호 거버넌스 효율성 제고를 위한 조직원의 정보보호 행위에 관한 실증 연구

An Empirical Study of Employee's Deviant Behavior for Improving Efficiency of Information Security Governance

김혜정(Hye Jung Kim)*, 안중호(Joong Ho Ahn)**

초 록

지속적인 정보보호 거버넌스를 위해서는 단순히 접근통제, 문서보안 등 기술적인 측면이 아닌 개인의 보안 행위, 문화, 규범, 개인적 가치 등 비공식적인 정보보호 행위를 관리하는데 초점을 맞추어야 한다. 그러나 많은 연구들이 정보보호 규정과 같은 공식적인 수준의 거버넌스나 기술과 같은 수단에 집중하고 있는 실정이며, 개인의 정보보호 위반 행위와 개인적 신념, 규범, 문화, 개인적 가치 등 비공식적인 수준에 대한 연구는 거의 이루어지지 않고 있다. 이에 본 연구는 정보보호 문화, 규범적 신념, 행위, 가치가 정보보호 규정 위반 행위에 어떠한 영향을 미치는 지에 대해 실증하였다. 또한 본 연구에서는 사회조직적 관점의 아노미 개념을 이용하여 조직 내에서 정보보호 규정의 중요성에 대한 인식 결핍과 정보보호 규정의 가치 결여를 '정보보호 아노미 현상'으로 정의하고, 이를 바탕으로 정보보호 문화, 규범, 행위, 가치가 정보보호 규정 위반 행위에 미치는 영향에 있어 정보보호 아노미 현상이 어떠한 역할을 하는지에 대해 실증분석을 수행하였다.

ABSTRACT

For the continuous information security governance, we have to focus on not just technical aspects like access control and DRM, but informal level management like information security(IS) behavior, culture, and personal value. But there are few informal level studies, while many formal level studies of IS governance or technical means. This study is an empirical test that how IS culture, normal beliefs, personal behavior and value affect employee's deviant behavior. And we define a lack of an awareness of value and importance on IS regulations in organizations as "Information Security Anomie" with the concept of anomie, a viewpoint on social organization.

키워드 : 정보보호 거버넌스, 정보보호 아노미, 정보보호 문화, 정보보호 규범적 신념, 정보보호 행위, 정보보호 개인적 가치
Information Security Governance, Information Security Anomie, Information Security Normal Beliefs, Information Security Personal Behavior, Information Security Perceived Effectiveness

* KPMG Samjong Accounting Corp. MCS(Management Consulting Service)/Manager
** Corresponding Author. Seoul National University. Department of Business Administration/Professor (E-mail : jahn@snu.ac.kr)
2012년 11월 14일 접수, 2012년 12월 05일 심사완료 후 2012년 12월 25일 게재확정.

1. 서 론

지속적이고, 변화무쌍한 실시간 정보를 관리해야 하는 조직의 목표 달성을 위해서는 “사람(people)”에 대한 지속적인 정보보호 거버넌스 관리 노력을 기울여야 한다. 사람을 관리하기 위한, 포괄적인 정보보호 거버넌스를 수립하기 위해서 조직에서는 보안 행위, 문화, 규범, 개인적 가치 등의 비공식적인 정보보호 행위를 관리하는데 초점을 맞추어야 한다[6, 27]. 이러한 정보보호 거버넌스의 중요성이 커지는 반면, 최근 은행을 대상으로 수행되었던 정보보호를 위한 내부통제 수준 진단 결과에 따르면 보안관련 정책과 절차가 정해져 있지만 대다수의 조직원들과 외부 관계자들은 이를 잘 지키지 않고 있는 것으로 조사되었다[24]. 그 이유는 보안 규정 준수에 대한 중요성이 강조될수록 직원들에게는 더 많은 업무 혼선이 생기게 되고, 이로 인해 직원들은 그들의 일상 업무에서의 효율성 향상을 위해 보안 정책을 자주 무시하게 되기 때문이다[30]. 그러나 많은 연구들이 정보보호 규정과 같은 공식적인 수준의 거버넌스나 기술과 같은 수단에 집중하고 있는 실정이며, 정보보호 위반 행위와 개인적 신념, 규범, 문화, 개인적 가치 등 비공식적인 수준에 대한 연구는 거의 이루어지지 않고 있다[27]. 이에 본 연구에서는 조직원의 정보보호 위반 행위에 영향을 미치는 요인을 조직의 문화, 규범, 개인의 행동과 가치에서 찾고자 한다.

이러한 문화, 규범, 행동, 가치와 같은 요인들은 많은 기업들에서 관찰되었던 조직원들의 정보보호 규정 위반 행위에 대한 묵인과 정보보호 규정이나 절차가 강조되기 보다는 성과 중심의 운영으로 인해 가볍게 여겨지고 있는 정보보호의 위상으로 인해 달라질 수 있다. 정보보호 규정 위반에 대한 조직차원의 처벌이나 보상의 수준이 강할수록 이러한 위반행위는 줄어들게 되지만, 솜방망이 처벌이라면 복잡하고 귀찮게 여겨지는 정보보호 규정은 잘 지켜지지 않을 것이라는 것은 자명하다. 따라서 본 연구에서는 사회조직적 관점의 아노미의 개념을 이용하여 조직 내에서의 정보보호 규정의 중요성에 대한 인식 결핍과 정보보호 규정의 가치 결여를 ‘정보보호 아노미 현상’으로 정의하고, 이를 바탕으로 정보보호 아노미 현상이 조직원의 정보보호 규정 위반 행위에 어떠한 영향을 미치는가에 대해 연구함으로써 정보보호 거버넌스의 실효성을 향상시킬 수 있는 방안에 대해 연구하고자 한다.

2. 이론적 배경 및 연구가설

2.1 정보보호 문화에 대한 인식 수준

조직의 정보보호 문화는 조직의 내/외부 이해관계자들을 통해 조직원들에게 인식되어 있는 조직의 정보 보안 상황으로 정의할 수 있으며, 이는 환경의 객관적 특성(규정, 정책, 절차 등)과 개인의 업무 행위 사이의 관계를 조절함으로써 개인의 행동을 결정하는데 중요한 요인이 되고, 개인 행동에 대한 가이드라인이 될 수 있다[4, 5, 6, 33]. 개인에 의해 관찰되는 조직의 문화적 사건들은 조직이 어떠한 사상을 우선시 하는지에 대한 신호로서 개인의 행동에 작용하게 되기 때문에 조직원

의 행동을 통해 반영되는 하나의 자각적인 수단으로서 조직원의 정보보호 위반 행위를 결정하는 중요한 요인으로 작용하는 것이다[6]. Vroom and von Solms[40]은 컴플라이언스를 위반하는 조직원의 행동은 조직의 문화를 바꾸거나 정보 보호에 대한 인식을 바꾸는 것과 같은 접근을 해야 한다고 주장하였고[41], Dinev et al.[15]은 예방 기술에 대한 사용자 행위를 연구하면서 조직 문화적 차원을 활용한 연구모델을 제시하기도 하였다[15]. McCoy and Stephens[24]은 정보보호 행위에 있어 조직 문화의 영향을 연구하였고, Chan[6] 등은 조직의 정보보호 문화가 정보 보호 정책 컴플라이언스에 있어서 유의한 영향을 미친다는 것을 실증하기도 하였다[6, 24]. 이러한 내용을 바탕으로 조직의 정보보호 문화가 정보보호 위반 행위에 미치는 영향에 대해 조사하기 위해 가설 1을 도출하였다.

H1(-) : 조직원의 정보보호 문화에 대한 인식 수준은 정보보호 규정 위반행위에 부정적인 영향을 미칠 것이다.

2.2 정보보호 규범적 신념에 대한 인식 수준

규범적 신념이란 자신이 속한 사회에서 자신에 대한 다른 구성원들의 생각이나 기대이며, 이러한 생각이나 기대는 자신의 행위에 대한 가치를 인식하고 그러한 행동을 하도록 유도하는 요인이 된다[36]. 규범적 신념은 느끼고, 믿고, 행동하는 원인이 되고, 다른 사람의 자신에 대한 기대에 영향을 받게 된다. 정보시스템에 대한 많은 연구들이 사회적 영향에 대한 역할로서 규범적 신념을 다루고 있다[20]. 이를 바탕으로 본 연구에서는 정보보호에 대한 규범적 신념을 조직 내에서 특정 개인이 인식하고 있는, 자신의 정보 보호 행위에 대한 타인의 인식 상태로 정의하였다[20, 22].

Venkatesh 등은 기술 수용 여부를 결정하는 데 있어 다양한 구성 요소들을 제시하면서, 사회적 영향의 역할에 대해 주장하였다[40]. Herath and Rao는 외적 동기로서 규범적 신념을 자신의 행위에 대한 타인들의 인식으로서 사회적 압력으로 작용한다고 보고 이를 활용하여 정보 보호 규정 컴플라이언스 준수 의도에 대한 효과를 측정하였다[20]. Venkatesh 등도 기술 수용을 결정하는 데 있어 규범적 신념과 개인의 행위, 개인적 가치(Perceived Effectiveness) 들이 복잡하게 작용하고 있다고 주장하면서 이를 활용하여 사람들의 기술 수용 결정에 대한 연구를 수행하였다[40]. McCoy and Stephens는 경영관리층, 상사, 동료 등 조직구성원들에 대한 개인의 인식이 정보보호 규정 행위에 유의한 영향을 미친다는 것을 주장하기도 하였다[24]. 이렇듯 정보보호에 대한 규범적 신념은 타인의 인식을 통해 조직원의 정보보호 위반 행위를 결정하는 중요한 요인으로 작용하게 된다. 이러한 내용을 바탕으로 조직원의 정보보호에 대한 규범적 신념이 정보보호 위반 행위에 미치는 영향에 대해 조사하기 위해 가설 2를 도출하였다.

H2(-) : 조직원의 정보보호 규범적 신념에 대한 인식 수준은 정보보호

규정 위반행위에 부정적인 영향을 미칠 것이다.

2.3 타인의 정보보호 행위에 대한 인식 수준

정보보호에 대한 개인적 행위는 조직 내에서 타인의 정보 보호 행위에 대한 개인의 인식 상태[6, 20, 32]를 의미한다. 즉, 한 조직의 구성원으로서의 개인은 다른 구성원들의 행동에서 나타나는 메시지나 신호를 통해 그 행동에 대한 가치를 판단하고, 자신의 행위에도 영향을 받게 된다[36].

타인의 정보보호 행위는 규범적 신념과 달리 자신에게 간접적 경험이 되어 그 행위에 대한 동기부여가 될 수 있다[31]. 일반적으로 관찰된 타인의 행동은 자신의 행동에 대한 동기가 되고, “만약 모든 사람들이 그 행동을 한다면, 그것은 그렇게 해야만 하는 행동”이 되는 것이다[9]. 사람들이 어떠한 행위를 하느냐 하지 않느냐에 대한 선택은 다른 사람들이 그것을 어떻게 하느냐에 따라 결정되게 된다[20].

Thompson 등과 Venkatesh는 어떤 행동을 유발하는 동기적 요인으로써 개인의 행위에 대한 역할에 대해 연구하였는데, Venkatesh 등은 기술 수용을 결정하는 데 있어 개인의 행위를 사회적 영향요인 중 하나로 사람들의 기술 수용에 대한 외적 요인으로 이용하였다[37, 40]. Herath and Rao는 외적 동기로서 규범적 신념과 함께 타인들의 행위에 대한 개인의 인식이 사회적 압력으로 작용한다고 보고 이러한 요인이 정보보호 컴플라이언스 준수 의도에 효과가 있음을 실증하였다[20]. 이러한 내용을 바탕으로 조직원의 정보보호에 대한 개인의 행위가 정보보호 위반 행위에 미치는 영향에 대해 조사하기 위해 가설 3을 도출하였다.

H3(-) : 타인의 정보보호 행위에 대한 인식 수준은 조직원의 정보보호 규정 위반행위에 부정적인 영향을 미칠 것이다.

2.4 정보보호 가치에 대한 인식 수준

정보보호에 대한 개인적 가치는 정보보호 규정에 대해 개인이 유용하다고 느끼는 정도를 의미한다[18, 21, 28]. 조직 내에서 정보보호 행위에 대한 내적 동기 요인으로서 개인이 느끼는 가치는 정보보호 행위의 가치에 대해 인식하는 만큼 규정을 더 잘 지키게 되는 등의 유형적인 형태로 나타나게 된다.

Wasko and Faraj[41], Ardichvili[2] 등은 개인적 가치가 그들 자신에게 뿐만 아니라 개인이 속한 사회와 다른 조직원들 및 전체 조직에 까지도 어떠한 결과물의 형태로 나타나게 된다는 것을 실증분석을 통해 밝혀냈다[2, 41]. 이러한 개인적 가치들의 조직 및 조직원들 사이의 교환은 자신만의 관심사에 의해서가 아니라 도덕적 의무와 조직의 관심사에 의해 동기부여가 된다[41]. 실제로, 조직원들은 조직에 대한 소속감을 느끼고 그들의 행위가 조직적 성과를 향상시킬 수 있다고 생각하기 때문에 조직에 이익이 되는 행동에 관심을 갖게 된다[20].

최근에 이러한 개념들을 고려한 정보보호 행동 연구들이 다수 수행되고 있다. 일반

시민들의 정보보호 행위를 다루는 조사에서 Culnan은 인지된 시민의 효과성을 고려하였으며, Aderson도 또한 이를 이용하여 집에서 이용하는 컴퓨팅 환경의 정보 보호 행동에 대한 연구를 수행하였다[1, 13]. 이러한 연구들에서 시민들에게 인지된 효과성은 인터넷 보안에 대한 개인의 행동에서 차이를 나타내는 것으로 조사되었다. 이러한 인지된 효과성에 따라 개인의 정보 보호 행위가 더 잘 이루어지는 것으로 나타났다[13]. 이러한 내용을 바탕으로 조직원의 정보보호에 대한 개인적 가치가 정보보호 위반 행위에 미치는 영향에 대해 조사하기 위해 가설 4를 도출하였다.

H4(-) : 조직원의 정보보호의 개인적 가치에 대한 인식 수준은 정보보호 규정 위반행위에 부정적인 영향을 미칠 것이다.

2.5 정보보호 아노미 현상에 대한 인식 수준

아노미는 사회자체가 그 목적과 목적을 달성하는 수단 사이에서 모순과 갈등을 통하여 사회구성원들에게 범죄적 행동을 하도록 압력을 가한다는 것을 의미한다. 아노미는 조직 구성원들이 조직에 대한 충성이나 몰입, 일에 대한 헌신, 적극성 등을 마비시키는 것으로 해석할 수 있다[23]. 아노미 이론은 특정 그룹에 속해있는 개인의 일탈 행위를 이해할 수 있는 개념적인 근간이 되므로, 많은 연구자들이 이를 활용하여 일탈 행위 및 범죄 행위 등에 대한 연구를 수행하였으며[16, 26], 최근까지 많은 사회학적, 범죄학적 연구에서 이용되고 있다.

정보보호와 관련된 연구에서는 개념적인 수준에서 아노미 이론이 다루어지고 있다. 특히 Dhillon and Backhouse는 사회구조가 개인의 정보보호 위반 행위에 영향을 주는 하나의 원인이 된다고 주장하였고[14], Vroom and von Solms는 조직원들의 정보 보호 행위는 기술적 요소뿐 아니라 조직적 문화와 조직적 행동과 같은 사회-조직적 구조를 통해 그 원인을 파악해야 한다고 주장하고 있다[41]. 정보보호 규정의 위반 행위의 원인을 파악하기 위해 Mishra and Dhillon은 아노미 이론을 통한 개념적 모델을 제시하는 연구를 수행하기도 했다[27]. 또한 Herath and Rao는 규범적 신념과 개인 행동이라는 사회적 압력 요인이 정보보호 컴플라이언스 의도에 긍정적인 효과를 보인다는 것을 연구하였다[20].

조직의 목표나 관리시스템이 조직의 목적이나 방향을 설정하는 중요한 도구가 되는 것처럼 신념이나 가치는 조직 내 근로자들의 행동 방향이나 의사결정을 정하는 데 매우 중요하다. 사전적 의미로 아노미 상태를 '개인이나 사회의 목표 의식, 정체성, 가치의 결여, 조직 붕괴, 이탈, 불안정성', 또는 '인간의 행위나 사회 질서를 규정하는 규범의 파괴가 특징인 무규범성', '목표나 이상의 결핍에서 오는 개인적인 불안, 소외, 불확실성이다'라고 정의한다. 결국, 아노미는 개인이나 조직이 가치나 규범을 상실하였을 때 생기며, 조직 내 근로자들이 고립감, 환멸감, 이탈감을 갖게 되므로 조직이 분열되고 효과적인 관리시스템이 기능을 발휘하지 못한다. 따라서 아노미가 지배하는 조직은 조직소통의 단절로 인

해 조직 내 사회적 결속을 약화 및 조직구성원들의 가치적 행동이나 기존의 규범을 따르지 않도록 유도한다. 이러한 조직은 조직에 대한 정체성, 임무, 목표에 대한 의식이 사라지게 된다. 이러한 개념은 정보보호 규정이나 프로세스, 시스템 등의 통제장치에도 불구하고 제대로 이루어지지 않고 있는 조직의 정보보호 거버넌스에 대한 실마리를 제공해 줄 수 있을 것으로 기대된다. 따라서 본 연구에서는 사회조직적 관점의 아노미의 개념을 이용하여 정보보호 아노미를 '조직 내에서의 정보보호 규정의 중요성에 대한 인식 결핍과 정보보호 규정의 가치 결여'로 정의하고자 한다. 이를 바탕으로 정보보호 아노미 현상이 조직원의 정보보호 규정 위반 행위에 어떠한 영향을 미치는가에 대해 연구하고자 다음과 같은 가설 5, 6, 7, 8을 도출하였다.

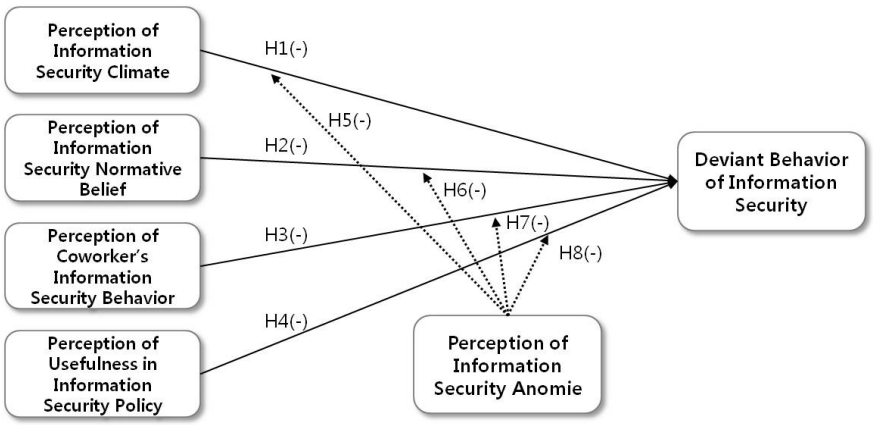
H5(-) : 정보보호 아노미에 대한 인식수준은 조직원의 정보보호 문화에 대한 인식수준이 정보보호 규정 위반행위에 미치는 영향에 있어 부정적인 영향을 미칠 것이다.

H6(-) : 정보보호 아노미에 대한 인식수준은 조직원의 정보보호 규범적 신념이 정보보호 규정 위반행위에 미치는 영향에 있어 부정적인 영향을 미칠 것이다.

H7(-) : 정보보호 아노미에 대한 인식수준은 타인의 정보보호 행위가 정보보호 규정 위반행위에 미치는 영향에 있어 부정적인 영향을 미칠 것이다.

H8(-) : 정보보호 아노미에 대한 인식수준은 조직원의 정보보호 개인적 가치가 정보보호 규정 위반행위에 미치는 영향에 있어 부정적인 영향을 미칠 것이다.

앞에서 언급된 가설들을 토대로 정보보호 위반 행위에 있어 아노미의 역할을 살펴보기 위해 다음과 같은 연구 모형을 구성하고 분석하고자 한다.



〈Figure 1〉 Research Model

3. 연구 방법

3.1 변수의 조작적 정의

가능한 한 선행연구 논문들의 측정문항을 원용하고자 하였으나 연구 목적의 달성을 위하여 필요한 경우, 측정문항을 수정하였으며 개별 구성개념에 대한 조작적 정의는 다음 <Table 1>과 같다.

3.2 자료수집 및 표본 특성

본 연구에서는 제안된 연구 모형을 평가하고 구성 개념의 조작적 정의를 위하여 관련 선행연구를 심층적으로 분석하였고 이를 토대로 최초 설문문항을 개발하였다. 이러한 과정에서 높은 수준의 신뢰성과 타당성을 확보하고자 예비조사를 실시하였으며, 확인적 요인분석을 통해 요인 적재값 0.5 이하의 항목(정보보호 아노미 측정항목 8개중 2개, 정보보호 규정위반행위 측정항목 6개중 1개)을 제거함으로써 측정문항을 재조정하였다.

또한 설문 분석에 필요한 최소 표본수는 통계적 검정력 분석을 지원하는 소프트웨어 G*Power 3.0을 이용하여 계산하였다. G*Power 3.0의 경우 PLS(부분최소자승법: Partial Least Square)만을 위한 별도의 기능은 제공되지 않지만 PLS는 회귀분석과 많은 유사점이 있으므로 G*Power 3.0을 이용해 최소 필요 표본수를 계산할 수 있다. 유의수준 α 값은 일반적인 수준의 0.05와 Power(1-β error)는 Cohen[11]이 제시한 0.8로 설정하여 계산한 결과 최소 필요 표본수는 85개로 도출되었다.

자료 수집은 2012년 7~8월까지 2달간 직접대면조사를 통해 이루어졌으며, 정보보호의 개념과 중요성에 대한 이해도가 타 산업에 비해 상대적으로 높은 금융산업 종사자들을 대상으로 설문조사를 수행하였다. 설문 응답은 최소필요표본의 50% 정도를 추가한 120부를 목표로 하였고, 최종 응답은 143개의

〈Table 1〉 Definition of Constructs

Constructs	Definition	Advance research
Perception of Information Security Climate	Perceived information security condition through stakeholders	Schnake[30], Chan[6], Neal and Griffin[27]
Perception of Information Security Normative Belief	The perception of the information security compliance expectation of others	Kreps[22], Herath and Rao[20]
Perception of Coworker's Information Security Behavior	The perception of other's information security behavior	Sutinen and Kuperan[34], Herath and Rao[20]
Perception of Usefulness in Information Security Policy	The perceived effectiveness of information security policy	Gordineer[18], Kankanhalli[21], Park et al.[28]
Perception of Information Security Anomie	The lack of importance and value of information security	Susan Kusmaski and Thomas Kusmaki[33], Lee et al.[23]
Deviant Behavior of Information Security	The tacitly deviant behavior of information security policy	Neal and Griffin[27], Hayes et al.[19], Chan et al.[6]

〈Table 2〉 Descriptive Statistics (N=117)

Division		Frequency	Percentage
Gender	Male	58	47.6
	Female	59	52.4
Age	21~30	23	19.7
	31~40	76	65.0
	Over 40	18	15.4
Type	Banking	55	47.0
	Insurances	25	21.4
	Securities	37	31.6
Years	Under 1 year	15	12.8
	Over 1 year ~ under 3 years	19	16.2
	Over 3 year ~ under 5 years	25	21.4
	Over 5 year ~ under 10 years	33	28.2
	Over 10 years	25	21.4
Position	Staff	39	33.3
	Assistant manager	33	28.2
	Manager	24	20.5
	Deputy manager	14	12.0
	General manager	7	6.0

샘플을 확보하였으며 응답이 불성실하거나 답변이 이상한 표본수를 제거하여 총 117개의 표본이 분석에 사용되었다(<Table 2> 참조).

본 연구에 사용된 표본의 특성은 남자가 47.6%, 여자가 52.4%이었으며, 연령은 20대가 19.7%, 30대 65%, 40대가 15.4%였다. 업종별로는 은행업이 47.0%, 보험업 21.4%, 증권업이 31.6%였다. 근속년수는 1년 미만이 12.8%였고, 1년 이상에서 3년 미만이 16.2%, 3년 이상에서 5년 미만이 21.4%, 5년 이상에서 10년 미만은 28.2%, 10년 이상이 21.4%였다. 직급은 사원급이 33.3%, 주임/대리급이 28.2%였고, 과장급은 20.5%, 차장급은 12.0%, 부장/팀장급이 6.0%로 나타났다.

3.3 실증 분석

본 연구에서 자료분석을 위해 부분최소자승법을 이용하는 SmartPLS 2.0이 사용되었다. PLS는 LISREL, EQS, AMOS 등의 구조 모델링 분석기법에 비해 상대적으로 적은 샘플 수에서도 복잡한 인과모형의 설명력을 나타낼 수 있을 뿐만 아니라, 변수의 타당성을 측정하는 측정모형과 변수의 경로와 설명력을 나타내는 구조모형을 동시에 측정할 수 있다[7].

PLS에서 구조 모형의 검증은 경로계수의 크기와 부호, 통계적 유의성, 선행 변수를 통해 설명되는 종속변수의 결정 계수 값을 통하여 이루어진다. 또한 모든 경로의 유의성을 검증하기 위하여 부트스트랩 재표본(Bootstrap

Resampling) 절차를 수행하였다. 부트스트랩 재표본 기법은 표본자료로부터 복원추출에 의해 동일한 분포를 갖는 측정치를 추정하는 방법으로서 PLS 경로 모형에서 주로 경로계수의 유의성을 평가하기 위해 일반적으로 사용되는 방법이다[12].

3.4 측정도구의 타당성 및 신뢰도 분석

측정모형에 대한 평가는 일반적으로 수렴타당성(Convergent Validity)과 판별 타당성(Discriminant Validity)을 통해 이루어진다. 수렴타당성은 구성개념에 대한 복합신뢰도인 CR(Composite Reliability)와 평균분산추출값인 AVE(Average Variane Extracted) 등에 의해 평가될 수 있다[17]. 복합신뢰도(CR)는 측정변수의 내적 일관성을 평가하는 기준으로 0.7 이상이면 타당한 것으로 판단하고, 평균분산추출(AVE)은 구성개념에 대하여 측정변수들이 설명할 수 있는 분산의 크기를 의미하는 것으로 0.5 이상이면 타당한 것으로 판단한다. 판별 타당성의 경우 구성개념 사이의 상관계수가 평균분산 추출 값의 제곱근보다 작은지 여부를 검증함으로써 평가하게 된다[3, 17].

본 연구는 측정도구의 타당성과 신뢰성 분석을 위하여 확인적 요인분석을 수행하였다. 요인분석 결과는 다음 <Table 3>에 나타나 있다. 신뢰성 검증을 위한 크론바하 알파값(Chronbach's alpha)이 0.6 이상이면 신뢰도가 있는 것으로 판단하고 0.8~0.9 이상이면 신뢰도가 높은 것으로 판단하는데[37], 본 연구의 측정항목들의 크론바하 알파값은 최소 0.942 이상으로 신뢰도가 높은 것으로 분석되었다. 일반적으로 요인 적재값이 통계적으로 유의하면 단일 차원성이 존재한다고 할 수 있는데, 분석 결과 모든 요인과 변수에 대한 요인 적재값이 0.866~0.971로 최소 요구치인 0.5를 만족하고 있으며, 복합신뢰도(CR)가 모두 0.7 이상이고, 평균분산추출값(AVE)도 기준치인 0.5 이상을 상회하고 있어 구성개념들의 수렴타당성을 확보한 것으로 나타났다.

판별 타당성은 일반적으로 AVE 제곱근 값이 0.5 이상이고 다른 구성개념의 상관관계 값보다 높으면 타당성이 확보된 것으로 판단한다. 본 연구 모형의 판별 타당성 분석 결과

〈Table 3〉 Results of Validity and Reliability

Scale Items	Factor loadings	t-value	CR	AVE	Cronbach's Alpha
ISCL 01	0.928*	53.952	0.964	0.871	0.951
ISCL 02	0.930*	39.000			
ISCL 03	0.954*	68.520			
ISCL 04	0.921*	41.411			
ISNB 01	0.936*	9.187	0.962	0.836	0.948
ISNB 02	0.971*	9.286			
ISNB 03	0.934*	8.855			
ISNB 04	0.872*	7.638			
ISPB 01	0.956*	10.642	0.973	0.923	0.959
ISPB 02	0.958*	10.949			
ISPB 03	0.968*	9.534			
ISPV 01	0.909*	40.562	0.959	0.856	0.944
ISPV 02	0.955*	61.889			
ISPV 03	0.938*	45.925			
ISPV 04	0.896*	25.616			
ISDB 01	0.866*	23.922	0.956	0.812	0.942
ISDB 02	0.878*	26.711			
ISDB 03	0.924*	45.761			
ISDB 04	0.932*	55.389			
ISDB 05	0.904*	40.555			

* $p < 0.01$.

〈Table 4〉 Results of Discriminant Validity

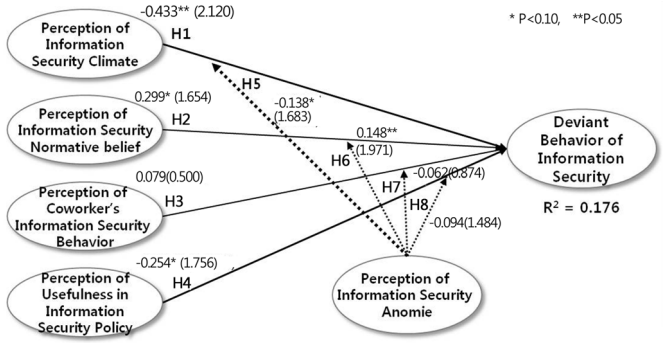
Constructs	[1]	[2]	[3]	[4]	[5]	[6]
Perception of Information Security Climate [1]	**0.940**					
Perception of Information Security Normative Belief [2]	0.860	**0.935**				
Perception of Coworker's Information Security Behavior [3]	0.785	0.761	**0.967**			
Perception of Usefulness in Information Security Policy [4]	0.731	0.681	0.697	**0.929**		
Perception of Information Security Anomie [5]	-0.354	-0.231	-0.402	-0.402	**0.813**	
Deviant Behavior of Information Security [6]	-0.329	-0.23	-0.347	-0.347	0.381	**0.915**

AVE 제곱근 값이 각 요인별 상관계수 값보다 높으므로 판별 타당성을 확보한 것으로 나타났다(<Table4> 참조). 따라서 각 차원의 지시변수들의 타당성 및 신뢰성이 확보되었다고 볼 수 있다.

3.5 경로분석 결과 및 가설 검증

본 연구의 SmartPLS를 통한 경로분석 결과는 다음 <Figure 2>와 같고, 모형상 경로에 표시된 결과 값은 표준경로계수의 값이다.

최근 PLS는 모델의 전반적인 적합도를 평가하는 객관적 평가기준이 없다는 한계점의 지적과 함께 모델의 적합성을 평가하는 인덱스를 개발하여 적합성 평가에 적용하고 있다. Tenenhaus et al.[35]은 PLS 구조모형의 적합성을 평가하기 위하여 GoF 인덱스를 개발하였고, GoF 값은 공통성 즉, Communality의 평균과 R^2 값의 평균을 곱한 값의 기하평균으로 정의된다[33]. 일반적으로 GoF값은 0에서 1 사이의 값을 가지며, PLS 모델의 적합성을 평가하기 위한 GoF값은 소 = 0.10, 중 = 0.25, 대 = 0.36으로 평가 기준 값을 제시하고 있다. 본 연구에서는 GoF = 0.28를 얻었으며, 이 값은 조직원의 정보보호 규정 위반 행위를 설명하는 데 있어, 정보보호의 문화에 대한 인식, 규범적 신념, 타인의 행위, 개인적 가치만을 사용하는 것보다 정보보호의 아노미 현상에 대한 인식 수준이 포함된 본 연구의 구조모형이 정보보호 규정 위반 행위를



〈Figure 2〉 Results of Path Analysis

조금 더 잘 설명하는 구조적인 모형이라는 것을 의미한다.

정보보호 문화, 규범적 신념, 개인의 행위, 개인적 가치가 정보보호 위반 행위에 미치는 영향에 대해 부트스트랩 재표본(Bootstrap Resampling) 절차를 수행하여 각 연구가설의 검정을 실시한 결과, 가설 2와 가설 3은 그 결과가 통계적으로 유의하지 못하여 지지되지 않았다(<Table 5> 참조).

조직구성원이 정보보호 규정을 잘 지킬 것인지에 대한 타인의 기대 수준에 대한 인식 수준을 의미하는 규범적 신념의 경우, 경로계수와 t-값은 통계적으로 유의하게 나타났으나, 그 방향성이 가설과 달라 기각되었다. 또한 타인의 정보보호 행위에 대한 인식 수준은 조직원들이 정보보호 규정을 잘 준수할 것인지에 대한 기대 수준을 측정한 변수로, 조직의 정보보호 문화에 대한 인식 수준이나 정보보호로 개인이 느끼는 가치 수준에 비해 정보보호 아노미에 대한 인식 수준에 대한 영향력은 다소 떨어질 수 있을 것으로 보이며, 정보보호에 대한 중요성이 강조되고 있는 금융산업의 특성 상 타인의 행위에 대한 개인의 기대 수준보다는 전반적인 조직의 정보보호 문화와 개인적 가치 등의 상대적인 중요도가 더 높았을 것으로 추정해 볼 수 있다.

정보보호 문화, 규범적 신념, 개인적 행위, 개인적 가치에 대한 인식 수준이 정보보호 위반행위에 주는 영향에 있어서 정보보호 아노미 현상에 대한 인식 수준이 어떠한 역할을 하는지에 대해 조사하기 위해 각 독립변수로부터 정보보호 아노미 현상을 거쳐 정보보호 위반 행위에 이르게 되는 각 경로들의 결합경로계수와 Sobel Z값(Z = a×b/SQRT(b2×Sa2+A2×Sb2)을 계산하여 각 가설(5, 6, 7, 8)들의 통계적 유의성을 검증하였다(<Table6>

〈Table 5〉 Results of Statistical Hypothesis Testing

Hypothesis	Path Coefficient	t-value	Directions	Test of Hypothesis
H1	-0.342*	1.771	-	Supported
H2	0.397**	2.568	+	Non-supported
H3	-0.160	0.968	-	Non-supported
H4	-0.311**	2.395	-	Supported

*p < 0.10, **p < 0.01.

〈Table 6〉 Results of Statistical Hypothesis of Information Security Anomie

Hypothesis	Integration of path coefficient	Z-value	Test of Hypothesis
H5	-0.138*	-1.683	Supported
H6	0.148**	1.971	Non-supported
H7	-0.062	-0.874	Non-supported
H8	-0.094	-1.484	Non-supported

*p < 0.10, **p < 0.05.

참조).

정보보호 아노미 현상에 대한 효과에 대한 가설들의 통계적 유의성을 검증한 결과, '정보보호 문화 인식 수준×정보보호 아노미 현상에 대한 인식 수준 → 정보보호 규정 위반 행위'를 나타내는 경로와, '정보보호의 규범적 신념×정보보호 아노미 현상에 대한 인식 수준 → 정보보호 규정 위반 행위'로 이어지는 두 개의 경로가 유의한 것으로 나타났다. 그러나 H2와 마찬가지로 정보보호 규범적 신념에 대한 정보보호 아노미 현상의 효과를 측정한 H6의 경우 통계적으로 유의한 결과가 나타났으나 가설의 방향성이 '+'로 나타나 기각되었다. 즉, 정보보호 문화에 대한 개인의 인식 수준이 정보보호 규정 위반 행위로 이어지는 데 있어 정보보호 아노미 현상에 대한 인식 수준이 부정적인 영향을 미치고 있는 것으로 분석되었으며, 정보보호 규범적 신념에 대한 인식 수준은 긍정적인 영향을 미치고 있는 것으로 나타나 가설이 지지되지 않았다.

4. 결 론

최근 금융사고의 특징 및 문제는 사고금액의 대형화, 사고 발생기간의 장기화, 과도한 영업 압박으로 인한 사고, 기초적인 내부통제 기능 미작동으로 요약할 수 있다. 한 컨설팅 기업에서 실시한 금융기관의 내부통제 진단 컨설팅 결과(KPMG, 2010)를 보면 대형 금융사고는 영업점에서 기본적으로 준수되어야 할 규정이 쉽게 위반되는 관행에서부터 시작된다는 것을 알 수 있다[24]. 영업점 진단 결과, 영업 및 고객 편의를 이유로 내부통제 규정을 준수하지 않는 경우가 많으며, 내부통제 업무의 가치 및 위상이 저하되는 분위기가 형성되어 있었다. 또한, 누구보다도 더 직원들을 관리해야 하고 정보보호 준수 여부를 확인해야 하는 책임자들의 경우 영업과 고객관리를 더욱 중요시하고 정보보호는 중요한 업무가 아니라고 인식하고 있었고, 습관적으로 책임자의 형식적인 승인, 결재 및 확인 절차가 진행되고 있었다.

본 연구는 이러한 현상의 원인을 아노미라는 사회학적 개념을 도구화시켜 조직원들의 정보보호 규정 위반 행위에 있어 조직의 정보보호 아노미 현상이라는 새로운 개념을 검증해 보고자 하였다.

그 결과 첫째, 자신이 속한 기업이 정보보호 규정에 대한 관심이 높다고 생각할수록 정보보호 아노미에 대한 인식 수준은 낮아지는 것으로 나타났다. 기업의 경영진이나 관리자, 직장동료 등 조직원들 사이에 정보보호를 중요시하는 문화가 강할수록 기업의 정보보호 아노미 현상은 줄어들게 되고 이로 인해 정보 보호 규정 위반 행위가 줄어들게 된다는 것을 의미한다. 조직원들 사이에 정보보호의 중요성을 강조하고 정보보호 행위를 강화하는 기업문화를 조성하기 위한 교육 및 캠페인 등의 활동이 정보보호 규정 위반 행위를 감소시킬 수 있는 중요한 관리 포인트임을 확인하는 결과라 할 수 있다.

둘째, 정보보호 규정에 대해 조직원이 유용하다고 느끼는 정도가 높을수록 정보보호 아노미에 대한 인식 수준은 낮아지는 것으로 나타났다. 이는 정보 보호 정책이 실제 업무 수행에 적용하는 것이 용이할수록, 정보보호

활동으로 인한 가치가 유용하다고 느낄수록 조직의 정보보호 아노미 현상은 줄어들게 되고 이로 인해 정보보호 규정 위반 행위가 줄어들게 된다는 것을 의미한다. 따라서 기업에서는 조직원들로 하여금 정보보호 규정을 준수하는 데 따르는 성과나 보상을 강조하고 규정위반으로 인한 처벌을 강화함으로써 정보보호 규정 준수에 대한 동기를 부여하는 것이 정보보호 아노미 현상을 지양할 수 있는 현실적인 대안이 될 수 있다. 기업에서 정보보호 규정이나 절차 등을 수립하는 것도 중요하지만 상위차원의 개념적인 규정보다는 실제 업무 수행에 도움이 되는 내용들로 구성하고 이에 대해 직원들의 접근성을 높이는 등 정보보호 규정에 대한 효용성을 향상시키기 위한 노력이 필요하다.

셋째, 연구가설은 기각되었으나 정보보호 규범적 신념에 대한 인식 수준은 조직원의 정보보호 아노미 인식 수준에 통계적으로 유의한 영향을 주는 것으로 나타났다. 조직원들의 상사나 동료들이 조직구성원 당사자가 얼마나 정보보호 규정을 준수할 것으로 기대하고 있는지에 대해 조직원들 개개인이 어떻게 인식하고 있느냐가 조직의 정보보호 아노미 현상에 유의한 영향을 미치는 것으로 해석된다. 정보보호에 대한 규범적 신념은 타인이 특정 개인의 정보보호 행위에 대해 기대하고 있는 수준을 특정 개인이 어떻게 인식하고 있느냐를 측정한 변수이다. 분석결과는 경로계수 방향이 정 '+'의 방향으로, 즉 타인이 특정 개인에 대해 정보보호 규정을 잘 지킬 것이라고 생각하고 있을 것이라는 기대에 대해 개인이 인식하고 있는 수준이 높을수록 정보보호 아노미 현상에 대한 인식수준이 높아지는 것으로 나타났다. 이는 한 금융기관의 내부통제 진단 컨설팅에서 "다른 직원을 믿지 못하면서 어떻게 같이 근무를 할 수 있느냐? 그냥 잘 지킬 것이라고 믿는다."라는 응답이 대다수였으나, 편법이나 비합법적 업무처리 또한 대다수를 차지하고 있었던 조사 결과를 보면 알 수 있듯이 규범적 신념 즉, 개인에 대한 타인의 기대수준에 대해 "over expected" 되어있기 때문에 보다 쉽게 정보보호 규정에 대한 가치나 중요성에 대한 인식 수준이 결여될 수 있는 것으로 생각된다.

금융사 직원들을 대상으로 추가적으로 실시한 심층 인터뷰 결과, 직원의 70%가 정보보호 통제 기능이 제대로 운영되지 않는 원인으로 직원 간 상호 견제나 불신적 사고에 익숙하지 않은 분위기를 선택하였다. 대부분의 조사대상 기업에서 조직 내 과도한 관용 분위기가 만연해 있고, 직원 상호 간 신뢰하는 분위기가 형성되어 견제와 감시를 하는 문화에 익숙하지 않으며, 상대방에 대한 견제나 의심으로 인해 조직 내에서 소외되는 것에 대한 두려움을 가지고 있는 것으로 나타났다. 이러한 의식이 본 연구 설문조사에도 반영되어 정보보호에 대한 규범적 신념의 수준은 높은 것으로 나타났고, 조직 내 과도한 관용 분위기로 인해 정보보호 아노미 현상 또한 높게 나타나는 것으로 해석할 수 있다. 이러한 현상은 대다수 국내 금융기관에서 발생하는 문제이다. 기본적인 감시와 견제 기능이 제대로 수행되지 않음으로 인해 장기간 동안 발생하는 금융사고를 발견하지 못하고 있고 이러한 사고의 장기화는 결국 손실의 대형화로 이어질 가능성이 높아지는 것이다. 따라서 금융기관의 이러한 문제들을 해결하

기 위해서는 조직원들의 정보보호에 대한 규범적 신념을 관리할 필요가 있다. 직원간 감시와 견제를 꺼려하는 분위기를 관리함으로써 정보보호 아노미 현상이 줄어들도록 해야 할 것이다. 그러나 연구결과를 보면 신입사원을 대상으로는 쉽게 정보보호의 중요성과 가치를 체계적으로 인식시킬 수 있는 반면, 연령이 많고 직급이 높아질수록 더욱 만연해 있는 정보보호 아노미 현상을 제거하는 것이 어렵다는 것을 알 수 있다. 따라서 정보보호 아노미 현상을 제거하고 정보보호 규정 위반 행위를 줄이기 위해서는 연령과 직급을 고려하여 정보보호에 대한 차별화된 교육 및 관리/감독이 필요하다.

References

[1] Anderson, C., "Creating conscientious cybercitizen : An examination of home computer user attitudes and intentions towards security," Conference on Information Systems Technology(CIST)/INFORMS, San Francisco, California. 2005.

[2] Ardichvili, A., Page, V., and Wentling, T., "Motivation and barriers to participation in virtual knowledge-sharing communities of practice," Journal of Knowledge Management, Vol. 7, No. 1, pp. 64-77, 2003.

[3] Bagozzi, R. P. and Yi, Y., "On the evaluation of structural equation models," Journal of the Academy of Marketing Science, Vol. 16, No. 2, pp. 74-94, 1988.

[4] Campbell, J. P., Dunnette, M. D., Lawler, E. E. III., and Weick, K, Jr., Managerial behavior, performance and effectiveness, McGraw-Hill, New York, 1970.

[5] Campbell, J. P. and Beaty, E. E., Organizational Climate : Its Measurement and Relationship to Work Group Performance. Paper presented at the Annual meeting of the American Psychological Association, Washington D. C., 1971.

[6] Chan, M., Woon, I., and Kankanhalli, A., "Perceptions of information security at the workplace : Linking information security climate to Compliant Behavior," Journal of Information Privacy and Security, Vol. 1, No. 3, pp. 18-41, 2005.

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

[8] Chin, W. W., Marcolin, B. L., and Newsted, P. R., "A partial least squares latent variable modeling approach for measuring interaction effects : Results from a monte carlo simulation study and voice mail emotion/adoption study," Paper presented at the Proceedings of the Seventeenth International Conference on Information Systems, Cleveland, Ohio, 1996.

[9] Cialdini, R. B., Reno, R. R., and Kallgren, C. A., "A focus theory of normative conduct : Recycling the concept of norms to reduce littering in public places," Journal

of Personality and Social Psychology, Vol. 58, No. 6, pp. 1015-1026, 1990.

[10] Cloward, R. A., "Illegitimate means, anomie, and deviant behavior," Americal Sociological Review, Vol. 24, No. 2, pp. 164-176, 1959.

[11] Cohen, J., Statistical power analysis for the behavioral sciences (2nd ed.). Hillsdale, NJ : Lawrence Erlbaum, 1988.

[12] Cotterman, W. and Senn, J., Challenges and strategies for research in information systems development, John Wiley & Sons, 1992.

[13] Culnan, M., Bentley survey on consumers and internet security : Summary of findings, http://www.bentley.edu/events/iscw2004/survey_findings.pdf, 2004.

[14] Dhillon, G. and Backhouse, J., "Current directions in IS security research : Towards socio-organizational perspectives," Information Systems Journal, Vol. 11, No. 2, pp. 127-153, 2001.

[15] Dinev, T., Goo, J., Hu, Q., Nam, K., "User behavior toward preventive technologies cultural differences between the United States and South Korea," ECIS 2006 Proceedings. Paper 9. http://aisel.aisnet.org/ecis2006/9, 2006.

[16] Durbin, R., "Deviant behavior and social structure : Continuities in social theory," American Sociological Review, Vol. 24, No. 2, pp. 147-164, 1959.

[17] Fornell, C. and Larcker, D. F., "Evaluating structural equation models with unobservable variables and measurement error," Journal of Marketing Research, Vol. 18, No. 1, pp. 39-50, 1981.

[18] Gordineer, J., "Blended threats : A new era in anti-virus protection," Information Systems Security, Vol. 12, No. 3, pp. 45-47, 2003.

[19] Hayes, B. E., Perander, J., Smecko, T., and Trask, J., "Measuring perceptions of workplace safety : Development and validation of work safety scale," Journal of Safety Research Vol. 29, No. 3, pp. 145-161, 1998.

[20] Herath, T. and Rao H. R, "Encouraging information security behaviors in organizations : Role of penalties, pressures and perceived effectiveness," Decision Support Systems, Vol. 47, pp. 154-165, 2009.

[21] Kankanhalli, A., Teo, H. -H., Tan, B. C. Y., and Wei, K.-K., "An integrative study of information systems security effectiveness," International Journal of Information Management, Vol. 23, No. 2, pp. 139-154, 2003.

[22] Kreps, D. M., "The interaction between norms and economic incentives," AEA Papers and Proceedings, 1997.

[23] Lee, S. J., Yoo, W. J., Jung, D. W., and Lee, D. M., "The effects of entrepreneurship and leadership of small and medium companies on organizational effectiveness : Focusing on the effect of Anomie," Journal of the Korea Management Engineers Society, Vol. 15, No. 2. pp. 159-176,

2010.

[24] McCoy, B., Stephens, G., and Stevens K. J., “An investigation of the impact of corporate culture on employee information systems security behavior,” ACIS Proceedings, 2009.

[25] Merton, R. K., “Social conformity, deviation, and opportunity structure : A comment on the contributions of Durbin and Cloward,” American Sociological Review, Vol. 24, No. 2, pp. 177-189, 1959.

[26] Mishra, S. and Dhillon, G., “Information systems security governance research : A behavioral perspective,” 1st Annual Symposium on Information Assurance, Academic Track of 9th Annual NYS Cyber Security Conference, New York, USA, 2007.

[27] Neal, A. and Griffin, M. A., “Perceptions of safety at work : Developing a model to link organizational safety climate and individual behavior,” Paper presented to the 12th Annual Conference of the Society for Industrial and Organizational Psychology, St. Louis, MO, 1997.

[28] Park, J. K., Kim, B. S., and Cho, S. W., “Primary factors affecting corporate employees’ attitudes toward Information Security,” Korean Management Review, Vol. 40, No. 4, pp. 955-985, 2011.

[29] Post, G. V. and Kagan, A., “Evaluating information security tradeoffs : Restructuring access can interfere with user tasks,” Computers and Security, Vol. 26, No. 3, pp. 229-237, 2007.

[30] Schnake, M. E., “An Empirical assessment of the effects of affective response in the measurement of organizational climate,” Personnel Psychology, Vol. 36, No. 4, pp. 791-804, 1983.

[31] Schneider, E. K., The Hadley circulation of the Earth’s atmosphere. Ph.D thesis, Harvard University, 1975.

[32] Sheeran, P. and Orbell, S., “Augmenting the theory of planned behavior : Roles for anticipated regret and descriptive norms,” Journal of Applied Social Pshchology, Vol. 29, No. 10, pp. 2107-2142, 1999.

[33] Susan Kusmaski and Thomas Kusmaski, 가치중심의 리더십, 학지사, 2000.

[34] Sutinen, J. G. and Kuperan, K., “A socio-economic theory of regulatory compliance,” International Journal of Social Economics, Vol. 26, No. 1/2/3, pp. 174-193, 1999.

[35] 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.

[36] Thompson, R. L., Higgins, C. A., and Howell, J. M., “Influence of experience on personal computer utilization,” Journal of Management Information Systems, Vol. 11, No. 1, pp. 167-187, 1994.

[37] Van de Ven, Andrew H., Ferry, D. L., Measuring and assessing organizations. NY : John Wiley, 1980.

[38] Venkatesh, V. and Brown, S., “A longi-

tudinal investigation of personal computers in homes : Adoption determinants and emerging challenges," MIS Quarterly, Vol. 25, No. 1, pp. 71-102, 2001.

[39] 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, pp. 425-478, 2003.

[40] Vroom, C. and von Solms, R., "Towards information security behavioral compliance," Computers and Security, Vol. 23, No. 3, pp. 191-198, 2004.

[41] Wasko, M. M. and Faraj, S., "It is what one does : Why people participate and help others in electronic communities of practices," Journal of Strategic Information Systems, Vol. 9, pp. 155-173, 2000.

저 자 소 개

김혜정 (E-mail : hyejung0213@gmail.com)
2003년 건국대학교 일반대학원 (경영학석사)
2013년 서울대학교 경영학과 (경영학박사)
2010년~현재 삼정KPMG 회계법인, Manager
관심분야 IT 거버넌스, ISP, BPR/PI, e-비즈니스 전략 등

안중호 (E-mail : jahn@snu.ac.kr)
1975년 서울대학교 문리과대학 외교학과 (정치학사)
1980년 서울대학교 행정대학원 (행정학석사)
1987년 New York University (Stern School, 경영학 석·박사)
1987년~1988년 미국 Fordham 대학, Baltimore 대학, 동국대학교 조교수
1994년 서울대학교 연구부처장
1999년 한국경영정보학 회장
2000년 한국퍼실리티메니지먼트학 회장
1989년~현재 서울대학교 경영대학 및 경영전문대학원 교수
관심분야 IT 거버넌스, BPM, e-비즈니스 전략, BPR, ERP 등