금융회사 정보보안정책의 위반에 영향을 주는 요인 연구 : 지각된 고객정보 민감도에 따른 조절효과

이정하* · 이상용**

A Study on the Factors for Violation of Information Security Policy in Financial Companies : Moderating Effects of Perceived Customer Information Sensitivity

Jeong-Ha Lee* · Sang-Yong Tom Lee**

Abstract

This paper analyzed factors for employees to violate information security policy in financial companies based on the theory of reasoned action (TRA), general deterrence theory (GDT), and information security awareness and moderating effects of perceived sensitivity of customer information. Using the 376 samples that were collected through both online and offline surveys, statistical tests were performed. We found that the perceived severity of sanction and information security policy support to information policy violation attitude and subjective norm but the perceived certainty of sanction and general information security awareness support to only subjective norm. Also, the moderating effects of perceived sensitivity of customer information against information policy violation attitude and subjective norm were supported. Academic implications of this study are expected to be the basis for future research on information security policy violations of financial companies; Employees' perceived sanctions and information security policy awareness have an impact on the subjective norm significantly. Practical implications are that it can provide a guide to establish information security management strategies for information security compliance; when implementing information security awareness training for employees to deter violations by emphasizing the sensitivity of customer information, a company should make their employees recognize that the customer information is very sensitive data.

Keywords : Information Security Management, Information Security Compliance, Information Security Policy, Information Privacy

논문접수일 : 2015년 11월 14일 논문게재확정일 : 2015년 12월 24일

* 제1저자, 서울과학종합대학원대학교 경영학과 박사과정, e-mail : jasonlee2484@gmail.com
** 교신저자, 한양대학교 경영대학 교수, e-mail : tomlee@hanyang.ac.kr

1. 서 론

금융회사의 전자금융거래는 다양한 정보보안 위협에 직면하고 있으며, 금융회사의 정보보안 사고는 지속해서 발생하고 있다. 2014년에는 금융회사 직원에 의한 대량의 개인정보 유출사고가 발견되어 사회적인 이슈가 되었다. 과거 정보보안은 계획을 수립하고 체계적인 보안통제를 구현하기보다는 사고가 발생하면 임기응변식으로 정보보호시스템을 도입하였으나[정해철, 김현수, 2000], 정보보안 관리체계에서는 정보보호 경영을 위해 체계적으로 정보보안통제를 기술적, 관리적, 물리적 보안통제의 영역으로 나누어 설명하고 있으며, 현재까지의 정보보안에 대한 연구는 기술적 영역에서 많이 이루어지고 있다[윤일한, 권순동, 2015].

하지만 보안사고의 발생이 조직원에 의해 발생되고 있고, 이러한 사고는 회사에 치명적인 악영향을 미치고 있으며, 이러한 실정에 맞추어 사람에 의해 준수되어야 할 정보보안정책의 관리적 보안 통제에 대한 연구가 중요해지고 있다[Ophoff et al., 2014]. 2014년 카드사의 대량 개인정보 유출사고는 내부자의 정보보안정책 위반으로 발생한 사고였으며, 이를 통제하기 위해 관리적 보안은 다시 강조되었고[윤일한, 권순동, 2015], 내부자에 의한 고의적인 사고였기에 내부자에 대한 정보보안정책 위반에 영향을 주는 요인을 분석하고 예방하기 위한 활동이 더욱 중요하게 되었다. 이 개인정보 유출사고로 인해 금융규제 당국은 '금융분야 개인정보 유출 재발방지 종합대책'을 발표하고 이와 같은 개인정보 유출사고에 대하여 처벌을 강화하고, 내부자에 대한 정보보안인식을 강화하기 위해 정보보안교육 훈련을 의무화하였다[이강신, 2015].

허츠버그는 사람들이 직업에서 원하는 것이 무엇인가를 연구하면서 하나의 요인이 충분하면 자신의 직무에 만족하고, 그 요인이 부족하면 불만족한 것이 아니라 자신이 수행하는 직무를 만족스럽게 생각하는 요인과 만족스럽지 않게 생각하는 요인이 각각 다르다는 것을 발견하였고 이론으로 발전시켰다. 다시 말해, 직무의 만족요인과 직무 불만족요인이 하나의 선상의 양극단에 있는 것이 아니라, 서로 다른 두 개의 선상에 있다는 것이다. 직무만족에 영향을 주는 동기요인과 직무 불만족에 영향을 주는 위생요인을 나누어 설명하였고, 동기요인을 충족하는 것은 직무만족에 영향을 주는 것일 뿐이며, 직무 불만족을 제거하는 것이 아니라고 설명하였다[Herzberg, 1964].

조직원이 생각하는 정보보안정책이라는 규정에 대한 준수요인과 위반요인도 같은 개념으로 해석할 수 있다. 즉, 정보보안정책을 준수한다는 것이 위반하지 않는다는 것과 반드시 일치하지는 않을 수 있다는 것이다. 하나의 요인이 충분하면 정보보안정책을 준수하고자 하지만, 그 요인 부족하다고 하여 위반을 하는 것이 아니라, 준수하고자 하는 의도가 약해질 뿐인 것이다. 정보보안정책의 준수의도가 부족하다는 것은 정보보안정책을 위반하는 것으로 설명되기보다는 정보보안정책의 준수의도가 낮다고 해석을 하여야 할 것이다.

금융회사는 정보보호경영을 위해 정보보안정책을 수립하고 정보보안교육훈련을 수행하고 있으나, 개인정보 유출사고는 지속해서 발생하고 있으며 정보보안정책의 위반으로 인한 사고가 금융회사에 치명적인 악영향을 미치고 있다. 기존 연구는 정보보안정책의 준수에 영향을 주는 요인을 분석하는 것을 강조하고 있지만, 금융회사의 보안사고를 예방하여 정보보호경영을 안정적으로 운영하기 위해서는 정보보안정책의 위반에 영향을 주는 요인을 분석하는 다른 관점에서의 연구가 필요하며, 금융회사의 정보보호경영

을 강화하기 위해 금융회사 조직원의 정보보안 정책 위반의도에 영향을 주는 요인을 분석하고 정보보안교육을 통해 활용하는 정보보호활동이 중요하다고 할 수 있다. 따라서 사회적 이슈가 되고 있는 조직원에 의한 정보보안정책 위반으로 발생하는 개인정보 유출사고는 정보보안정책의 준수를 강화하는 것에 대한 연구뿐 아니라, 정보보안정책의 위반의도를 제거하는 연구도 함께 진행되어야 한다.

정보보안정책에 영향을 주는 연구는 다양하게 이루어지고 있으며, 정보보안정책의 영향요인들에 대한 메타분석 연구에 따르면, 정보보안정책의 준수에 영향을 주는 요인과 위반에 영향을 주는 요인들은 다르게 나타나고 있다고 설명하였다[Sommestad et al., 2014]. 또한, 다수의 연구는 정보보안정책 준수에 대한 영향요인을 분석하고 있으며[Vance and Siponen, 2012], 정보보안정책에 대한 준수를 강화하는 것에 초점을 맞추고 설명하고 있다.

정보시스템 위협의 분류에 따르면 정보보안정책의 위반은 비의도적인 것과 의도적인 것으로 구분되며, 내부자에 의한 정보보안정책에 대한 위반은 오용, 남용 및 고의에 의한 것으로 나타나며, 악의적인 경우에는 회사에 미치는 부정적 영향이 치명적일 수 있다[Willison and Warkentin, 2013]. Theoharidou et al.[2005]는 접근 권한이 허용된 내부자가 조직의 정보보안정책을 위반하여 발생하는 권한 남용 및 오용에 대해 내부자 위협으로 정의하였다. 정보보호경영을 위협하는 주요 요인으로는 정보보안정책을 위반하는 조직원이 있으며[Siponen et al., 2014; Vance et al., 2012], 리비히의 '최소량의 법칙'을 응용하면 정보보호경영을 하기 위해서는 가장 취약한 영역에 대해 보호대책을 강화하여야 전체적인 정보보호경영의 수준을 높일 수 있다[장상수 외 3인, 2013]. 2014년 보고된 국내 카드사의 개인정보 유출 사고는 내부자의 의도적인 행동 때문에 발생한 사고였으며, 금융회사의 개인정보 유출사고를 예방하기 위해 내부자 위협에 대한 예방이 중요하고 정보보안정책의 준수에 대한 영향의 연구와 같이 중요하게 연구되어야 할 분야는 내부자의 의도적인 정보보안정책 위반에 대한 영향요인의 분석이라 할 수 있다[윤일한, 권순동, 2015].

본 연구에서는 기존 연구들이 정보보안정책 준수의 영향요인 분석을 강조하고 있지만, 위반의 연구에 대한 기여를 하고자 금융회사 조직원에 대한 정보보안정책의 위반을 억제할 수 있는 요인을 탐색하는 연구목적을 달성하기 위해, 첫째, 규정에 대한 위반을 억제하기 위해 사용되는 처벌의 영향 요인을 확인하기 위해 '억제이론에서의 처벌에 대한 지각이 정보보안정책의 위반의도에 영향을 주는가?' 둘째, 금융감독당국의 규제에 따라 의무적으로 수행되는 정보보안교육을 통해 금융회사 조직원의 강화된 정보보안인식은 정보보안정책 위반에 효과가 있는지를 확인하기 위해 '정보보안정책 및 일반적인 정보보안인식이 정보보안정책의 위반의도에 영향을 주는가?' 셋째, 업무상 반드시 취급하여야 하는 고객정보에 대해 조직원이 인지하는 중요성에 따른 효과가 있는지를 확인하기 위해 '금융회사 조직원이 취급하는 고객정보에 대한 민감도가 정보보안정책의 위반의도를 조절하는 효과가 있는가?'에 대하여 금융회사 조직원의 설문조사를 통해 실증분석을 하였다.

본 연구의 구성은 행동이론, 억제이론 및 정보보안인식에 대한 이론을 살펴보고, 연구모형과 가설을 설정하고 설문 시나리오 설계에 대한 내용을 설명하였다. 다음으로 금융회사의 조직원을 대상으로 설문하여 수집된 데이터를 기반으로 PLS(Partial Least Squares)를 이용하여 분석하였으며, 결과를 해석하고 본 연구의 학문적, 실무적 기여와 한계점에 대하여 기술하였다.

2. 이론적 배경

2.1 정보보안정책에 대한 조직원의 행동연구 동향

정보보안정책에 대한 조직원의 행동에 대한 연구는 국내·외에서 다양하고 활발하게 이루어지고 있으며, 정보보안정책 준수에 대한 영향요인을 다양하게 설명하였다. 다양한 정보보안정책에 영향을 주는 연구에서 정보보안정책의 영향요인들에 대한 문헌연구를 보면, 정보보안정책의 준수에 영향을 주는 요인으로는 변화에 대한 개방성(Openness to change), 지각된 행동 통제(Perceived behavioral control), 처벌에 대한 지각된 정의(Perceived justice to punishment), 보수(Conservation), 지각된 정당성(Perceived legitimacy), 위협 평가(Threat appraisal), 정보보안 인식(Information security awareness), 서술적 규범(Descriptive norm), 반응 효능감(Response efficacy), 지각된 가치 적합성(Perceived value congruence), 주관적 규범(Subjective norm), 정보보안정책의 품질(Information security policy quality)이 높은 영향을 주는 것으로 나타났으나, 위반에 영향을 주는 요인으로는 훈련의 유형(Type of training), 지각된 처벌의 심각성(Perceived severity of sanctions), 중화기술(Neutralization), 주관적 규범(Subjective norm), 도덕적 신념(Moral beliefs), 지각된 고유 혜택(Perceived intrinsic benefits), 참여도(Involvement), 자기방어 의도(Self-defense intention)로 다르게 나타나고 있다고 설명하였다[Sommestad et al., 2014].

연구의 결과에 따르면, 조직원의 정보보안정책 준수의도와 위반의도는 다른 요인에 의해 영향을 받는 것을 알 수 있으며[Sommestad et al., 2014], 정보보안정책에 대한 연구에서 사용되는 주요 이론적 프레임은 합리적 행동이론, 계획적 행동이론, 합리적 선택이론, 보호동기이론, 억제이론, 조직몰입, 공정성이론, 정보보안인식, 위험보상이론, 중화기술이론, 스트레스 인지이론 등으로 다양하게 이용되었다.

<표 1>에 요약된 정보보안정책에 대한 연구동향을 보면 대부분이 보안정책 준수에 관한 것임을 알 수 있다. 준수에 대한 연구가 아닌 정보보안정책 위반에 관한 연구로서는 도덕적 해방이 정보보안정책 위반의도에 매개효과가 있음을 주장하고[임명성, 2013b] 중화기술과 억제이론이 정보보안정책 위반의도에 영향이 있음을 주장하며[Siponen and Vance, 2010], 남용에 대한 연구로는 금융회사 내부직원의 불필요한 고객정보조회 행동의도에 영향을 주는 요인으로 인지된 예방활동 및 교정활동이 합리적 행동이론의 태도, 주관적 규범 및 행동통제를 통해 영향을 주는 것으로 나타났으며[정우진 외 2인, 2012], 오용에 대한 연구로서는 정보보안정책, 정보보안교육훈련 및 모니터링 활동이 처벌의 확실성을 통해 정보시스템 오용의도에 영향을 주장한 연구[D'Arcy, 2009] 정도가 전부라 할 수 있다.

하지만 금융규제 당국에서 강조하는 처벌의 강화와 정보보안교육훈련의 효과성을 분석하는 데는 한계가 있다. 금융회사 조직원의 정보보안정책 위반의도에 대해 정보보안교육훈련을 통해 강화된 정보보안인식과 강화된 처벌로 인해 인지된 처벌의 확실성과 심각성이 정보보안정책 위반의도에 어떤 영향을 주는지는 제대로 다루지 못하였다. 따라서 본 논문은 금융규제 당국의 정책 효과를 고려한 모형을 통해 보안정책 위반의도에 관한 요인 연구의 실무적 의미의 공백을 메우고자 하는 연구라 할 수 있다. 또한, 개인정보 유출사고로 인해 개인정보의 중요성이 강조되는 시대적 상황을 반영해 개인정보를 취급하는 금융회사의 인지된 고객정보 민감도를 조절요인으로 모형에 추가하여 금융회사의 특성을 고려한 연구를 하고자 한다.

〈표 1〉 정보보안정책에 대한 연구 동향

구 분	연구자	연구내용
준수요인 연구	이성규, 채명신 [2014]	산업보안정책 준수의지에 영향을 주는 요인으로 내적 동기(윤리의식, 직간접 경험, 업무관련성)와 외적 동기(보안교육, 처벌 명확성)로 분류한 요인의 영향을 분석, 조직공정성(분배공정성, 절차공정성, 상호작용공정성)을 조절요인으로 제시하고 공정성이 높은 집단과 낮은 집단 간의 차이를 분석
	강 욱, 전용태 [2014]	보안정책 준수에 처벌의 확실성과 처벌의 심각성이 미치는 영향을 세부적으로 처벌의 인식, 특별 억제효과, 일반 억제효과로 분류하여 영향을 분석
	Kim et al. [2014]	정보보안정책 준수의도에 영향을 주는 요인으로 태도, 규범적 신념, 자기효능감, 반응효능감, 중화기술이론을 분석
	임명성 [2013c]	금융서비스업을 중심으로 정보보안정책 준수의도에 영향을 주는 요인으로 보안정책의 효과성, 정보보안인식교육, 경영진의 보안관심, 경영진의 보안강조, 보안정책 준수비용을 분석
	Wall et al. [2013]	자율성과 효능감의 역할을 기반으로 정보보안정책 준수의도에 영향을 주는 요인으로 자기효능감, 반응효능감, 자기결정권, 심리적 저항감을 분석
	김상현, 송영미 [2011]	보안정책 준수의도에 미치는 요인으로 외적 동기요인(페널티 강도, 보안위반 적발도, 규범적 신념, 동료들의 영향)과 내적 동기요인(보안 심각성, 보안 불안감, 보안 상식)을 분석
	Bulgurcu et al. [2010]	정보보안인식과 합리적 선택이론을 기반으로 정보보안정책 준수의도에 미치는 요인으로 준수이익, 준수비용, 미준수비용의 영향을 분석
	Herath and Rao [2009b]	보호동기이론 및 억제이론은 기반으로 정보보안정책 준수의도에 영향을 미치는 요인으로 처벌의 심각성, 적발 확실성, 자기효능감, 반응효능감, 반응비용, 조직몰입, 주관적 규범, 기술적 규범, 보안위반우려를 분석
	Pahnila et al. [2007]	정보보안정책 준수의도에 영향을 미치는 요인으로 처벌, 위협평가, 대처평가, 규범적 신념, 정보의 품질, 촉진조건, 습성, 보상을 분석
위반요인 연구	임명성 [2013b]	도덕적 해방이론을 기반으로 정보보안정책 위반에 영향을 주는 요인으로 정보보안인식교육, 도덕적 신념, 처벌에 대한 인지, 도덕적 해방을 분석
	Siponen and Vance [2010]	중화기술, 공식적 처벌, 비공식적 처벌 및 치욕이 정보보안정책 위반의도에 미치는 영향을 분석
남용요인 연구	정우진 외 2인 [2012]	금융회사 내부직원의 기업정보보호활동(억제활동, 예방활동, 탐지활동, 교정활동)의 인지수준이 불필요한 고객정보조회 태도, 주관적 규범 및 인지된 행동통제를 통해 불필요한 고객정보조회 행동의도에 주는 영향을 분석
오용요인 연구	D'Arcy et al. [2009]	보안정책, 보안교육훈련, 모니터링이 처벌에 미치는 영향과 정보시스템 오용의도에 영향을 미치는 요인으로 지각된 처벌의 심각성과 지각된 처벌의 확실성을 분석

2.2 합리적 행동이론

합리적 행동이론은 원래 사회 심리학에서 나온 이론으로 조직행동, 건강 관련 의사결정, 정보시스템 채택 등과 같은 다양한 분야에서 개인의 행동을 탐색하기 위한 이론적 프레임으로써 성공적으로 적용되어 왔다[Fishbein and Ajzen, 1975]. 행동연구에 따르면, 행동은 신념 → 태도 → 의도 → 행동으로 영향을 주는 것으로 나타난다[Ajzen, 1991]. 의도는 행동에 영향을 주는 요인으로 행동과 같은 개념으로 이용되기도 한다. 합리적 행동이론은 특정 행동을 수행하기 위한 개인의 결정은 행동을 수행하고자 하는 의도에 의해 결정되고, 의도는 행동에 대한 주관적 규범과 행동하려는 태도에 의해 결정된다고 가정하였다[Ajzen, 1991]. 행동에 대한 태도는 특정 행동의 결과에 대해 좋고 나쁨을 나타내는 신념에 의해 나타나며, 주관적 규범은 특정 행동에 대해 타인들로부터의 사회적 압력에 대한 지각된 신념에 의해 나타난다[Ajzen, 1991].

계획된 행동이론[Ajzen, 1991]은 합리적 행동이론[Fishbein and Ajzen, 1975]의 확장된 버전으로 행동의 직접적인 요인으로 행동의 의도를 제시하고, 이 행동의 의도는 다시 세 요인에 의해서 나타난다고 보는데, 즉, 행동에 대한 태도와 주관적 규범, 그리고 인식된 행동 통제이다. 계획된 행동이론에 새로 추가된 요인인 인식된 행동 통제는 행동의 용이성 및 행동과 관련된 자원과 장애에 관한 신념에 의해서 결정된다[Ajzen, 1991].

2.3 일반억제이론

일반억제이론은 확실하고, 심각하며, 신속한 처벌이 범죄를 억제한다고 주장하였다[D'Arcy and Herath, 2011; Williams and Hawkins, 1986]. 즉 사람들이 특정 범죄에 대해 처벌이 확실하며, 심각하게 이루어지고, 신속하게 집행이 된다고 인식할수록 범죄는 감소한다는 것이다[Siponen and Vance, 2010]. 억제는 타인에게 처벌이 집행되는 것을 보거나 인식함으로써 자기 자신도 범죄를 저지르면 처벌을 받게 될 수 있다고 생각하기 때문에 이러한 위협으로 인해 범죄 행동을 하지 않는다는 것이다. 즉 사람들은 해당 범죄를 저지르지는 않았지만, 타인의 사례를 통해 그 범죄를 저지르게 되면 처벌을 받게 될 수 있다는 것을 인식함으로써 해당 범죄를 저지르지 않는다는 것이며, 이를 통해 잠재적인 범죄 행위가 억제될 수 있는 것이다[강욱, 전용태, 2014]. 정보보안정책에 대한 위반태도 및 주관적 규범은 처벌에 대한 확실성과 심각성에 의해 영향을 받을 수 있다.

2.4 정보보안인식

조직원의 정보보안인식은 정보보호경영의 중요한 부분이며[Bulgurcu et al., 2009b], 정보보안인식은 조직의 정보보안 목적을 달성하기 위한 직원의 상태이고[Siponen, 2000], 정보보안정책이 조직 내에서 적용되는 것을 보증하기 위해 조직원이 해당 정책을 이해할 수 있도록 하여야 한다[Whitman et al., 2001]. 정보보안인식은 정보보안에 대한 조직원의 일반적인 이해와 조직의 정보보안정책에 대한 이해로 정의되고, 일반적인 지식은 조직원의 정보보안 관련 잠재된 이슈와 파급효과에 대한 전반적인 지식과 이해이며 조직은 조직원에게 정보보안정책이 반영된 일반적인 정보보안인식을 기대하고 정보보안정책에 대한 인식은 조직의 정보보안정책에 기술된 요구사항들과 목적에 대한 조직원의 이해와 지식을 말한다[Siponen, 2000].

3. 연구모형 및 가설

3.1 연구모형

본 연구의 목적은 금융회사의 정보보안정책 위반에 영향을 주는 요인을 분석하기 위해 합리적 행동이론, 일반억제이론 및 정보보안인식에 대한 이론을 통합하여 연구모형을 제시하고, 금융회사의 특성상 조직원이 고객정보를 취급함으로써 지각된 고객정보의 민감도가 위반의도를 조절하는 효과가 있는지를 분석하여 금융회사의 조직원이 준수해야 할 정보보안정책 교육에 활용할 수 있는 기준을 제시하고자 한다. 정보보안정책의 위반의도를 설명하기 위해 합리적 행동이론이 많이 사용되었으며[Bulgurcu et al., 2009a; Bulgurcu et al., 2010; Herath and Rao, 2009b; Ifinedo, 2012; Li et al., 2010; Zhang et al., 2009] 다양한 분야에서 특정 행동을 설명하는데 이용되어[Lin et al., 1999], 이를 기반으로 연구모형을 설계하였다.

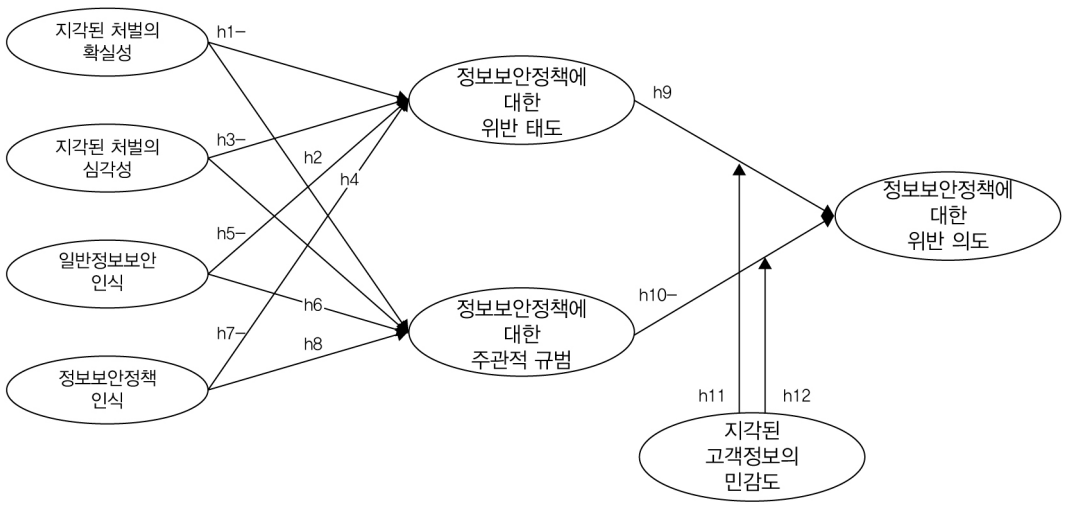
3.2 가설 설정

억제이론에는 처벌의 심각성, 확실성 및 신속성이 요인으로 있으나, 신속한 처벌이 법규를 위반하는 것을 억제하는 것에 대한 연구는 거의 없으며, 실증을 통한 통계적인 유의성을 찾는 것은 어렵다[Nagin and Pogarsky, 2001]. 선행연구들에 의하면, Straub Jr[1990]는 처벌의 확실성과 심각성은 컴퓨터 남용을 억제하는 효과가 있다고 주장하였고, Kankanhalli et al.[2003]는 처벌의 심각성은 조직의 정보시스템 보안 효과성에 영향을 미치지 못한다고 하였으며, D'Arcy et al.[2009]는 처벌의 심각성은 정보시스템 오용의도를 억제하는 효과가 있으나, 처벌의 확실성의 효과는 유의하지 않다고 하였다. 반면, Herath and Rao[2009b]와 Herath and Rao[2009a]처벌의 확실성이 조직원의 정보보안정책 준수의도에 긍정적 영향을 미치고, 처벌의 심각성은 부정적인 영향을 미친다고 하였다. 강욱, 전용태[2014]는 특별 억제효과에 대해 처벌의 확실성과 심각성이 모두 보안정책 준수에 긍정적 영향을 미친다고 하였고, 김상현, 송영미[2011]는 페널티 강도와 보안위반 적발도가 보안정책 준수의도에 긍정적 영향을 미친다고 하였다.

처벌을 하나의 변수로 선정한 연구에서는 처벌이 정보보안준수에 긍정적 영향을 미친다고 하였고[Siponen et al., 2010; 안중호 외 3인, 2010], 처벌이 정보보안정책 준수의도에 미치는 영향은 유의하지 않는다고도 하였다[Guo et al., 2011; Hu et al., 2011; Pahnila et al., 2007; Son, 2011; 강다연, 장명희, 2014]. Vance and Siponen [2012]는 공식적인 처벌은 영향을 미치지 않지만, 비공식적인 처벌이 영향을 미치는 것으로 나타났다. 선행연구들을 보면, 억제 이론의 요인이 정보보안정책의 준수 및 위반에 대하여 다양하게 연구되었고 다른 결론으로 나타났다.

본 연구에서는 금융회사 조직원에게 지각된 처벌의 확실성과 처벌의 심각성이 정보보안정책 위반에 대한 태도 및 주관적 규범에 영향을 주는 요인인 것을 탐색하기 위해 가설을 설정하였다.

[가설 1] 지각된 처벌의 확실성은 정보보안정책을 위반하고자 하는 태도에 음(-)의 영향을 미칠 것이다.



〈그림 1〉 정보보안정책 위반의도에 대한 연구모형

[가설 2] 지각된 처벌의 확실성은 정보보안정책에 대한 주관적 규범에 양(+)의 영향을 미칠 것이다.

[가설 3] 지각된 처벌의 심각성은 정보보안정책을 위반하고자 하는 태도에 음(-)의 영향을 미칠 것이다.

[가설 4] 지각된 처벌의 심각성은 정보보안정책에 대한 주관적 규범에 양(+)의 영향을 미칠 것이다.

정보보안인식은 정보시스템 보안인식을 위한 기본적인 개념을 설명한다[Siponen, 2000]. 정보보안 연구자들은 정보보안교육, 훈련 및 인식(Security Education, Training, Awareness, SETA) 프로그램이 정보보안정책을 통제하는 데 필요하다고 하였고[Whitman, 2004], SETA 프로그램은 다양한 형태로 구성될 수 있으며 내부자에게 요구되는 정보보안정책의 절차를 지키는 방법을 포함하는 일반적인 지식을 제공할 수 있고[D'Arcy et al., 2009; Lee and Lee, 2002; Whitman et al., 2001], SETA 프로그램의 수행은 정보보안정책의 기반을 세우는 것이며, 가장 기본적인 도구로 활용될 수 있다고 주장하였다[Peltier, 2005].

개인마다 다르고 직접적인 경험 또는 외부에서 터득한 지식을 통해 만들어지는 정보보안인식은 합리적 행동이론의 배경요소로 논의될 수 있다[Fishbein et al., 2007]. Bulgurcu et al.[2010]은 조직원의 정보보안정책 준수의 선행요인을 계획된 행동이론 기반으로 분석하면서 정보보안인식이 조직원의 신념 결과에 영향을 주는 요인으로 주장하였고, Leach[2003]는 조직원은 업무에서 발생하는 보안이슈에 대해 스스로 해결을 해야만 할 때가 있으며, 때때로 참고할 자료나 문서 없이 결정하여야 하는 상황이 있기 때문에 보안에 대한 일반적인 이해가 정보보안 행동에 중요한 요인이라고 주장하였다. 정보보안인식은 조직원의 정보보안정책 준수에 대한 태도에 긍정적 영향을 미치고[Bulgurcu et al., 2009a], 정보보안인식은 정보시스템 오용의도에 부정적인 영향을 주며 조직원의 정보보안에 대한 이해는 정보보호 활동이 조직에 소모되는 비용이 아니라는 것을 이해하는 데 도움을 준다[D'Arcy and Hovav, 2007].

금융회사는 전자금융거래법 및 개인정보보호법을 준수하기 위해 정보보호 컴플라이언스 활동을 수행하고 있으며, 관리적 정보보호 활동 중 정보보안인식교육이 중요한 역할을 수행하고 있다. 정보보안에 대한 지식을 설명하는 조직원의 정보보안인식이 높을수록 정보보안정책에 대한 위반의도는 낮아진다고 할 수 있으며, 정보보안인식을 일반적인 정보보안 상식과 정보보안정책에 대한 지식으로 정의하고 태도와 주관적 규범에 영향을 미치는 신념으로써 연구모형에 가설을 추가하였다.

[가설 5] 일반적인 정보보안인식은 정보보안정책을 위반하고자 하는 태도에 음(-)의 영향을 미칠 것이다.

[가설 6] 일반적인 정보보안인식은 정보보안정책에 대한 주관적 규범에 양(+)의 영향을 미칠 것이다.

[가설 7] 정보보안정책에 대한 인식은 정보보안정책을 위반하고자 하는 태도에 음(-)의 영향을 미칠 것이다.

[가설 8] 정보보안정책에 대한 인식은 정보보안정책에 대한 주관적 규범에 양(+)의 영향을 미칠 것이다.

많은 연구자가 정보보안 행동과 관련하여 합리적 행동이론을 이론적 배경으로 사용하였고[Anderson and Agarwal, 2010; Aurigemma, 2013; Bulgurcu et al., 2010; Herath and Rao, 2009b;

Kankanhalli et al., 2003; Pahnila et al., 2007; Siponen et al., 2014; Yoon, 2011; Yoon and Kim, 2013; 강다연, 장명희, 2012; 김상훈, 박선영, 2011; 박철주, 임명성, 2012b; 임명성, 2012a; 임명성, 2013a; 정우진 외 2인, 2012], 실증분석에서 유의하고 만족스러운 결과로 나타났다[Yoon and Kim, 2013]. 지각된 내용이 신념에 영향을 주며 신념이 태도에 영향을 주어 의도에 영향을 주는 것으로 행동을 설명함으로써, 정보보안정책의 위반의도는 위반에 대한 태도와 주관적 규범에 의해 영향을 받게 된다는 기본적인 이론적 프레임을 이용하여 가설을 설정하였다.

[가설 9] 정보보안정책의 위반태도는 정보보안정책의 위반의도에 양(+)의 영향을 미칠 것이다.

[가설 10] 정보보안정책에 대한 주관적 규범은 정보보안정책의 위반의도에 음(-)의 영향을 미칠 것이다.

금융회사 조직원은 업무상 부득이하게 고객정보를 취급하게 되며, 최근 고객정보를 포함한 개인정보의 중요성이 이슈로 나타나고 있다. 2011년 개인정보보호법을 제정되면서 금융회사의 조직원은 업무상 취급하는 고객정보에 대하여 더욱 민감하게 다루고 있으며, 내부적으로도 많은 정보보안인식교육을 수행하여 인식을 개선하고 있다. 금융회사의 특성으로 보면 고객정보의 취급자에게 지각된 고객정보의 민감도에 따라 정보보안정책의 위반의도에 영향을 주는 태도와 주관적 규범에 조절효과를 줄 것으로 예측할 수 있으며, 이를 실증하고자 가설을 설정하였다.

[가설 11] 지각된 고객정보의 민감도는 정보보안정책의 위반태도와 정보보안정책의 위반의도와의 관계를 조절할 것이다.

[가설 12] 지각된 고객정보의 민감도는 정보보안정책에 대한 주관적 규범과 정보보안정책의 위반의도와의 관계를 조절할 것이다.

3.3 정보보안정책 위반 시나리오 설계

Siponen and Vance[2010]의 연구를 기준으로 정보보안정책에 대한 위반태도 및 위반의도를 측정하기 위해 설문 시나리오를 설계하였다. 일반적으로 위반에 대한 태도나 의도를 파악하기 위해 직접적인 설문으로 할 경우, 응답자들이 사회적으로 바람직한 방향으로 답하는 경향이 있어 간접적인 설문을 사용하게 된다. 간접적인 설문으로는 시나리오를 제시하고 시나리오의 주인공에 대하여 설문을 하여, 응답자의 태도나 의도를 파악하게 된다.

시나리오의 선정과 질문의 내용에 대해 사전에 금융회사의 직원 50명을 대상으로 설문을 진행하였으며, 시나리오 설문은 시나리오에 대한 현실성이 높을 경우에 현실적인 응답이 나오기에 세 개의 시나리오를 기준으로 금융회사 조직원을 대상으로 현실성을 검토한 결과를 반영하여 '비밀번호 유출'에 대한 시나리오로 결정하여 설문을 진행하였다[Siponen and Vance, 2010].

〈표 2〉 정보보안정책 위반에 대한 시나리오

위반사항	시나리오
비밀번호 유출	최근 이대리는 A 금융회사에 입사를 하였다. 그 회사는 비밀번호에 대한 강력한 정책을 시행하고 있다. 모든 컴퓨터는 비밀번호로 보호되어야 하며, 비밀번호를 공유해서 사용하는 것이 금지되어 있다. 그러나 이 대리가 출장 중에 그의 동료가 급하게 그의 컴퓨터에 있는 중요한 파일이 필요하게 되었다. 그는 비밀번호를 알려주는 것이 회사의 시간적인 비용을 절감하는 것으로 생각하고 있다. 또한, 그는 며칠 전에 회사의 정보보안 교육을 이수하였다. 현재, 이 대리는 그의 동료에게 비밀번호를 알려주었다.

〈표 3〉 변수의 조작적 정의와 참고문헌

변수	조작적 정의	참고문헌
지각된 처벌의 확실성 (PCS)	정보보안정책 위반에 대한 처벌이 확실하게 있다고 지각하는 정도	Nagin and Paternoster[1993], Paternoster and Simpson[1996], Siponen and Vance[2010]
지각된 처벌의 심각성 (PSS)	정보보안정책 위반에 대하여 처벌이 심각하다고 지각하는 정도	Nagin and Paternoster[1993], Paternoster and Simpson[1996], Siponen and Vance[2010]
일반정보보안인식 (GISA)	보안사고의 부정적인 결과에 대한 이해, 보안사고 해결에 필요한 비용 이해, 보안사고에 대한 우려에 대한 정도	Bulgurcu et al.[2010]
정보보안정책인식 (ISP)	정보보안정책에 대한 이해, 정보보안정책에 대한 책임	Bulgurcu et al.[2010]
정보보안정책에 대한 위반태도 (ATTV)	정보보안정책 위반 시나리오에 대한 태도의 필요성, 유용성 및 혜택	Ajzen[1991], Bulgurcu et al.[2010]
정보보안정책에 대한 주관적 규범 (SN)	동료, 상사와 경영진이 정보보안정책이 준수될 것으로 생각하는 정도	Ajzen[1991], Bulgurcu et al.[2010], Siponen and Vance[2010]
정보보안정책에 대한 위반의도 (INTV)	정보보안정책 위반 시나리오에 대해 같은 행동을 할 것이라는 의도	Paternoster and Simpson[1996], Siponen and Vance[2010], Siponen et al.[2010]
지각된 고객정보의 민감도 (PCIS)	업무상 취급하는 고객정보가 유출되었을 때, 심각하게 생각하는 민감도의 정도	Bansal and Gefen[2010]

3.4 변수의 조작적 정의와 측정항목

설문의 척도는 7점 척도를 사용하였으며, 전혀 그렇지 않다(1)는 것에서 매우 그렇다(7) 혹은 전혀 동의하지 않는다(1)에서 매우 동의한다(7)로 산정하였다. 지각된 고객정보의 민감도는 금융회사에서 취급하는 정보를 네 가지로 구분하여 전혀 민감하지 않다(1)는 것에서 매우 민감하다(7)로 설문을 구성하였다(<부록 1> 참고). PCS, PSS, PCIS는 네 개의 측정문항으로 구성되며, GISA, ISP, ATTV, SN은 세 개의 측정문항, INTV는 두 개의 측정문항으로 구성되었다. 구조방정식에서 일반적으로 하나의 잠재변수에 세 개의 측정변수를 권고하고 있으나, INTV에 대한 측정변수는 선행연구를 참고하여 두 개의 측정변수만으로 정의하였다.

4. 연구방법

4.1 데이터 수집 및 분석방법

설문은 2015년 3월 13일부터 4월 20일까지 금융회사 조직원을 대상으로 진행하였으며, 온라인과 오프라인을 함께 진행하였다. 다수의 금융회사가 회사에서 외부 인터넷을 사용하는 것을 차단하고 있어 온라인 설문보다는 오프라인 설문의 응답이 높게 나타났다. 오프라인 설문지는 400부를 배포하여 350부를 수거하였으며, 온라인 설문은 79명이 참석을 하였다. 수집된 자료 중 불성실하게 응답한 53명의 설문을 제외하고 376부의 설문을 최종으로 선정하여 분석을 수행하였다.

본 연구는 SPSS 22와 SmartPLS 2.0 M3의 PLS Algorithm, Bootstrapping, Blindfolding을 이용하여 분석하였다. 구조방정식은 다변량 데이터와 복잡한 인과모형을 위한 행동 과학 연구에 많이 사용되고 있으며[Hair et al., 2012], PLS 기법은 엄격한 이론적 기반을 요구하는 AMOS나 LISREL과 달리 탐색적 연구를 지원하며[Barclay et al., 1995; Bollen, 2014; Hair et al., 2012; Gefen and Straub, 2005; Jöreskog and Sörbom, 1989], 측정모형과 구조모형을 함께 분석할 수 있는 장점이 있다[Chin et al., 2003].

측정모형은 신뢰성과 타당도를 검증하기 위해 내적일관성(Internal consistency), 집중타당도(Convergent validity), 판별타당도(Discriminant validity)를 분석하였고, 구조모형은 경로분석을 통해 적합도, R^2, 경로계수 및 t 값을 이용하여 가설을 검증하였다. 최종분석을 위해 부트스트래핑 재표집 절차를 사용하였으며, 재표집을 위해 사용된 표본의 수는 SmartPLS에서 권장하는 5,000개를 설정하였고, PLS 기법에서 모형의 품질을 평가하기 위해 사용되는 지표인 R^2, f^2, Q^2와 전반적 적합도(Goodness of Fit, GoF)를 평가하였다[Hair et al., 2012].

4.2 기술통계

본 연구에서 사용되는 응답자의 성별 구성을 보면 남자는 237로 전체 응답자의 63%를 차지하고 있으며 여자는 139명으로 37%를 차지하고 있다. 연령은 30대(30~39세) 집단이 177명으로 47.1%로 가장 높으며, 그 다음으로 40대(40~49세) 집단이 142명으로 37.8%를 차지하고 20대(20~29세)가 31명(8.2%), 50대(50~59세)가 26명(6.9%) 순으로 분포되어 있다. 학력은 대졸이 295명으로 78.5%를 차지하여 가장 높았으며, 다음으로 대학원졸 이상이 48명(12.7%), 고졸이 33명(8.8%)으로 분포되어 나타났다. 업무경력은 10~15년이 92명(24.2%)으로 가장 많으며, 그 다음으로 5~10년이 87명(23.1%), 15~20년이 58명(15.4%) 등 순으로 분포되어 있다. 업종은 256명(68.1%)이 보험회사에 종사하고 있으며, 107명(28.5%)이 은행에 종사하는 것으로 나타났다.

〈표 4〉 기술통계 결과

변수	구 분	빈도(명)	구성비(%)
성별	남성	237	63.0
	여성	139	37.0
연령	20대	31	8.2
	30대	177	47.1
	40대	142	37.8
	50대	26	6.9
학력	고졸	33	8.8
	대졸	295	78.5
	대학원졸 이상	48	12.7
업무 경력	1년 미만	17	4.5
	1~3년	34	9.0
	3~5년	35	9.3
	5~10년	87	23.1
	10~15년	92	24.5
	15~20년	58	15.4
	20년 이상	53	14.2
금융 회사	은행	107	28.5
	보험	256	68.1
	기타금융	13	3.4

5. 실증분석

5.1 측정모형의 신뢰성 및 타당도 분석

PLS 분석을 이용한 방법은 집중타당성과 판별타당성의 검증이 필요하다[Gefen and Straub, 2005]. 수집된 측정변수들이 구성 개념에 잘 적재되었는지를 확인하기 위해 탐색적 요인분석(<부록 2> 참고)을 수행하고 신뢰성 및 타당성을 검증하였다. 잠재변수의 복합신뢰도(Composite Reliability, CR)와 Cronbach's α 가 모두 0.7 이상이고, 모든 잠재변수의 평균분산추출(Average Variance Extracted, AVE)이 0.5 이상으로 신뢰성이 검증되었다[Chin, 1998; Fornell and Larcker, 1981]. 또한, 집중타당성 분석을 위해 측정항목에 대한 요인 적재량을 평가하였으며, 측정모형에서 각 항목의 요인 적재량이 0.7 이상이며 요인 적재량의 t 값의 절대값들이 유의수준 0.05에서 1.965 이상으로 유의하게 나타났기 때문에 집중타당도가 검증되었다[Bagozzi and Yi, 1988; Barclay et al., 1995; Fornell and Larcker, 1981; Hair, 2010].

두 잠재변수 사이에 구한 AVE 값이 잠재변수 간의 상관계수 제곱 값보다 크면 판별타당성이

확보되었다고 할 수 있다[Fornell and Larcker, 1981; Hulland, 1999]. AVE의 제곱근 값 중 가장 작은 값(0.862)이 상관계수의 가장 큰 값(0.841)보다 높으므로 판별타당성이 검증되었다. 또한, 측정모형의 외생변수 구성개념 간의 상관계수가 모두 0.9 이하이므로 차원 간의 다중공선성은 없는 것으로 나타났다[Kutner et al., 2004; Yang et al., 2011; 김중인, 2012]. 측정모형에 대해 내적일관성, 집중타당성 및 판별타당성이 검증되었기 때문에 단일차원성이 있다고 검증되었다[Anderson and Gerbing, 1988; Bagozzi and Yi, 1988; Fornell and Larcker, 1981].

5.2 구조모형의 경로분석

측정모형에 대한 신뢰성과 타당성 검증 후, 본 연구에서 제안하는 변수들 사이의 영향 관계를 검증하기 위해 SmartPLS 2.0 M3를 사용한 구조방정식 분석(Structural Equation Modeling, SEM)을 수행하였다. PLS-SEM은 종속변수의 근사값과 모형에서 예측된 값 사이의 차이에 초점을 맞추어 분석하는 방법이다[Hair et al., 2012]. PLS 분석을 사용한 이유는 본 연구는 탐색적 연구의 성격이 강하여 수집된 데이터에 적합한 연구모형 탐색뿐 아니라 변수들 사이의 인과관계를 알아보기 위해서이다. 이러한 구조방정식 분석을 통해 일반적으로 두 가지 결과의 도출을 해석할 수 있다. 첫 번째 구조방정식 분석의 결과는 경로계수(β)이다. 이는 두 변수 간의 인과관계 정보를 나타낸다[Wixom and Watson, 2001]. 두 번째 정보는 내생변수에 대한 결정계수인 R^2 결과 값을 보여준다. 결정계수 R^2는 변수들에 의해 설명되는 비율을 의미하며, 이 정보들은 본 연구의 구조모형이 가설된 인과관계를 얼마나 잘 나타내고 있는지를 보여준다.

〈표 5〉 내적일관성 및 집중타당도 검증

변수	항목	Cronbach's α	CR	AVE	β	SE	t value
PCS	PCS1	0.933	0.952	0.833	0.879	0.016	55.577***
	PCS2				0.922	0.011	85.031***
	PCS3				0.924	0.010	89.874***
	PCS4				0.925	0.011	86.433***
PSS	PSS1	0.883	0.920	0.743	0.866	0.018	48.690***
	PSS2				0.877	0.018	49.530***
	PSS3				0.767	0.034	22.453***
	PSS4				0.929	0.009	106.261***
GISA	GISA1	0.882	0.927	0.809	0.855	0.031	27.806***
	GISA2				0.908	0.016	55.506***
	GISA3				0.934	0.011	86.285***
IPS	ISP1	0.946	0.965	0.902	0.944	0.010	91.839***
	ISP2				0.948	0.009	103.111***
	ISP3				0.957	0.007	141.072***
ATTV	ATTV1	0.959	0.973	0.924	0.962	0.006	162.808***
	ATTV2				0.974	0.004	250.829***
	ATTV3				0.947	0.009	106.485***
SN	SN1	0.910	0.943	0.847	0.914	0.012	78.530***
	SN2				0.901	0.017	53.225***
	SN3				0.944	0.007	139.738***
INTV	INTV1	0.942	0.972	0.945	0.973	0.006	168.071***
	INTV2				0.972	0.006	162.422***

주) $^{***}p < 0.001$, CR : 복합신뢰도, AVE : 평균분산추출, β : 경로계수, SE : 표준오차.

〈표 6〉 구성개념 간 판별타당성 분석표(상관계수와 AVE의 제곱근 값)

	1	2	3	4	5	6	7
1 : PCS	**0.913**						
2 : PSS	0.743	**0.862**					
3 : GISA	0.314	0.426	**0.899**				
4 : ISP	0.326	0.389	0.669	**0.950**			
5 : ATTV	-0.377	-0.417	-0.224	-0.271	**0.961**		
6 : SN	0.565	0.651	0.538	0.529	-0.367	**0.920**	
7 : INTV	-0.326	-0.386	-0.197	-0.295	0.841	-0.372	**0.972**

주) 굵게 표시된 대각선은 AVE의 제곱근 값임.

PLS 분석은 내생변수의 설명력을 나타내는 결정계수 R^2 값을 예측적합도 지수로 사용하며, 상(0.26 이상), 중(0.13~0.26), 하(0.02~0.13)로 판단한다[Barclay et al., 1995; Chin, 1998; Chin and Gopal, 1995; Hulland, 1999; Tenenhaus et al., 2005]. 외생변수로 설명되는 내생변수의 설명력은 R^2로 평가하는데 10% 이상 되어야 한다[Sosik et al., 2009]. 구조모형 분석을 위해 내생변수의 설명력을 확인한 결과, 0.197, 0.544, 0.712로 모두 중 이상으로 구분되어 설명력은 확보되었다고 할 수 있다. 또한, 모든 외생변수의 Stone-Geisser's Q^2의 값은 0.172, 0.455, 0.668로 0 이상으로 나타나 중복성(Redundancy) 값을 이용한 예측적합도가 있는 것으로 판단되었다[Geisser, 1975; Stone, 1974; Tenenhaus et al., 2004; Tenenhaus et al., 2005].

전반적 적합도는 모든 내생변수의 R^2 값의 평균과 요인분석에서 사용되는 모든 잠재변수의 공통성(Communality) 값의 평균을 곱한 값의 제곱근으로 계산하여, 상(0.36 이상), 중(0.25~0.36), 하(0.10~0.25)로 판단한다[Chin, 1998; Hulland, 1999; Tenenhaus et al., 2005]. 계산된 GoF 값은 0.644 ($\sqrt{0.484 \times 0.858}$)로 매우 높은 적합도로 나타났다.

연구모형에 대한 구성개념의 효과 크기를 확인하기 위해 경쟁모형과 비교하여 효과 크기를 분석하며 계산된 영향도 f^2의 효과 크기는 상(0.36 이상), 중(0.15~0.35), 하(0.15 이하)로 판단한다[Chin, 1998; Cohen, 2013; Henseler et al., 2009]. 이에 따라 매개변수가 포함된 완전모형(Full Model)과 매개변수를 포함하지 않은 감소모형(Reduced Model)을 비교하여 구성개념의 영향도를 계산하여 효과 크기를 확인하였다.

〈표 7〉 내생변수의 예측적합도 분석

	R^2 value	Communality	Q^2 value
PCS		0.833	
PSS		0.743	
GISA		0.809	
ISP		0.902	
ATTV	0.197	0.924	0.174
SN	0.544	0.847	0.455
INTV	0.712	0.945	0.668
평균	0.484	0.858	

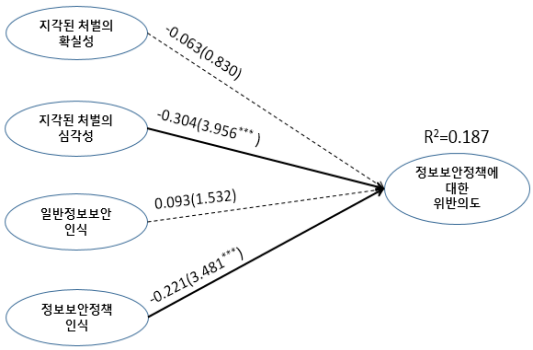
$$f^2 = \frac{R^2full - R^2reduced}{1 - R^2full},$$

R^2_{full}: 완전모형, $R^2_{reduced}$: 감소모형

〈표 8〉 완전모형과 감소모형의 효과 비교

감소모형 R^2	완전모형 R^2	f^2 value	효과 크기	Pseudo F statistic
0.187	0.712	1.823	상	659.896***

주) $^{***}p < 0.001$.



주) $^{***}p < 0.001$.

〈그림 2〉 감소모형의 경로분석 결과

억제이론에 대한 가설검증의 결과, 처벌의 확실성은 주관적 규범에 영향을 주고 있으나 정보보안정책에 대한 위반태도에는 영향을 주지 않고 있으며, 처벌의 심각성은 태도와 규범에 모두 통계적으로 유의하게 나타났다. 이는 억제이론에서 주장하는 억제의 요인이 정보보안정책의 위반태도를 억제하기보다는 주관적 규범에 영향을 주는 규범적인 신념으로 작용하는 것으로 설명할 수 있다. 결국, 처벌에 대한 확실성은 주관적 규범에 영향을 주어 정보보안정책에 대한 위반의도를 억제하는 효과가 있으며, 처벌의 심각성은 정보보안정책에 대한 위반태도와 주관적 규범에 영향을 주어 위반의도를 억제하는 것으로 나타났다. 금융회사 조직원은 처벌의 확실성에 따라 위반태도의 변화는 유의하지 않고 처벌의 심각성은 위반태도를 억제하였다. 위반태도와 주관적 규범에 대한 설명력을 보면, 독립변수들이 주관적 규범에 높은 설명력으로 나타나 조직원에게 지각된 억제 요인은 규범적 신념으로 더 크게 작용한다고 할 수 있다.

정보보안인식에 대한 가설검증의 결과, 일반보안 인식이 위반태도에 주는 영향은 유의적이지 않으나 정보보안정책 인식은 위반태도에 유의적으로 나타났으며, 주관적 규범에는 모두 유의적으로 나타났다. 금융회사 조직원의 정보보안정책에 대한 인식은 위반태도에 영향을 주고 있으나, 일반적인 정보보안에 대한 상식적인 인식은 위반태도에 유의적인 영향을 주지 않는 것으로 나타났다. 이는 일반적인 정보보호에 대한 상식이 높다고 정보보안정책의 위반태도가 감소할 것이라는 가정은 유의하지 않다는 것이다.

행동이론의 가설검증 결과는 기존 연구와 같은 결과로 나타났으며, 합리적 행동이론에 따라 태도와 주관적 규범이 의도에 영향을 주는 이론을 지지하였다. 정보보안정책의 위반에 대한 태도 및 주관적 규범이 위반의도에 영향을 주는 결과는 금융회사 조직원의 행동의도는 정보보안정책의 위반에 대하여도 태도와 주관적 규범에 의해 영향을 받는 것을 설명해준다.

〈표 9〉 가설검증 결과

	경로	β	SE	t value	결과
H1	지각된 처벌의 확실성 → 정보보안정책에 대한 위반태도	-0.138	0.080	1.733	기각
H2	지각된 처벌의 확실성 → 정보보안정책에 대한 주관적 규범	0.167	0.058	2.877**	채택
H3	지각된 처벌의 심각성 → 정보보안정책에 대한 위반태도	-0.272	0.084	3.229**	채택
H4	지각된 처벌의 심각성 → 정보보안정책에 대한 주관적 규범	0.363	0.069	5.316***	채택
H5	일반정보보안인식 → 정보보안정책에 대한 위반태도	0.028	0.064	0.447	기각
H6	일반정보보안인식 → 정보보안정책에 대한 주관적 규범	0.196	0.062	3.132**	채택
H7	정보보안정책 인식 → 정보보안정책에 대한 위반태도	-0.139	0.059	2.362*	채택
H8	정보보안정책 인식 → 정보보안정책에 대한 주관적 규범	0.205	0.056	3.654***	채택
H9	정보보안정책에 대한 위반태도 → 정보보안정책에 대한 위반의도	0.815	0.026	31.703***	채택
H10	정보보안정책에 대한 주관적 규범 → 정보보안정책에 대한 위반의도	-0.073	0.028	2.640**	채택

주) $^{*}p < 0.05$, $^{**}p < 0.01$, $^{***}p < 0.001$, β : 경로계수, SE : 표준오차.

5.3 조절효과 분석

지각된 고객정보의 민감도에 따른 조절효과를 분석하기 위해 지각된 고객정보의 민감도의 합을 기준으로 낮은 집단과 높은 집단을 나누고, 정보보안정책에 대한 위반태도와 주관적 규범이 정보보안정책에 대한 위반의도에 주는 경로에 영향을 미치는지에 대한 조절효과를 분석하였다.

두 집단에 대한 경로분석을 수행한 결과, 전체를 대상으로 분석한 결과와 다른 부분이 나타났다. 높은 집단에서는 처벌의 확실성이 위반태도에 영향을 미치나, 처벌의 심각성은 위반태도에 영향을 미치지 않는 것으로 나타났다. 이는 고객정보에 대해 민감하게 생각하는 조직원은 처벌의 심각성보다는 확실성에 영향을 받는 것으로 해석할 수 있다. 또한, 낮은 집단에서는 정보보안정책에 대한 인식이 위반태도에 영향을 미치지 않는 것으로 나타났다. 이는 고객정보에 대해 덜 민감하게 인식하는 조직원은 정보보안정책에 대한 인식이 정보보안정책에 대한 위반태도에 영향을 미치지 않는 것으로 해석된다. 가장 크게 다른 점은 낮은 집단에서는 주관적 규범이 정보보안정책에 대한 위반의도에 영향을 미치지 않는다는 것이다. 지각된 고객정보의 민감도가 낮은 집단의 조직원은 위반태도에 따라 위반의도가 설명되고 주관된 규범의 영향은 유의하지 않다는 것이다.

두 집단 간의 경로분석 결과로 두 집단 간의 조절효과를 분석하기 위해 집단 간의 경로계수의 차이를 분석하는 식[Keil et al., 2013; Keil et al., 2000]을 사용하였으며, 연구모형에서 제시한 조절효과에 대한 가설이 모두 채택되었다. 지각된 고객정보의 민감도가 높을수록 정보보안정책 위반태도와 주관적 규범에 대해 상호작용하여 정보보안정책 위반의도를 줄여주는 효과가 나타났다.

$$t = \frac{Path_{sample1} - Path_{sample2}}{\sqrt{\frac{(m-1)^2}{(m+n-2)} \times SE^2_{sample1} + \frac{(n-1)^2}{(m+n-2)} \times SE^2_{sample2}} \times \sqrt{\frac{1}{m} + \frac{1}{n}}},$$

m : sample 1의 개수, n : sample 2의 개수

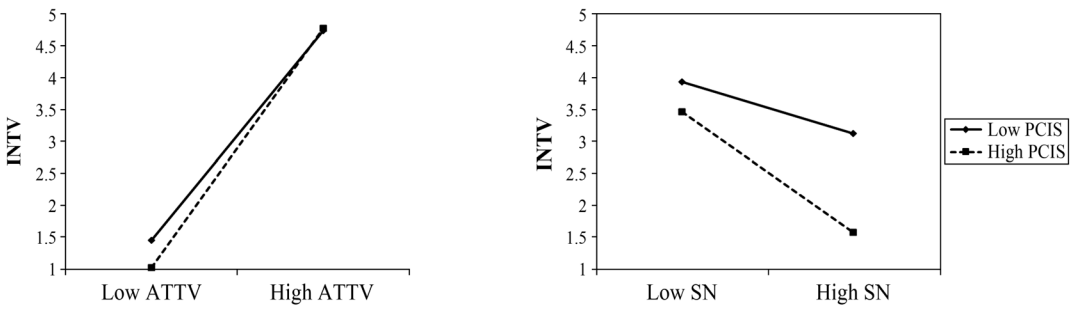
〈표 10〉 지각된 고객정보의 민감도에 따른 집단 구분

변수 구분		낮은 집단(N = 204)		높은 집단(N = 172)	
		빈도(명)	구성비(%)	빈도(명)	구성비(%)
성별	남자	142	69.6	95	55.2
	여자	62	30.4	77	44.8
연령	20대	19	9.3	12	7.0
	30대	90	44.1	87	50.6
	40대	77	37.8	65	37.8
	50대	18	8.8	8	4.6
학력	고등학교 졸업	12	5.9	21	12.2
	대학교 졸업	163	79.9	132	76.7
	대학원 졸업/이상	29	14.2	19	11.1
업무경력	1년미만	8	3.9	9	5.2
	1~3년	14	6.9	20	11.6
	3~5년	16	7.9	19	11.0
	5~10년	48	23.5	39	22.7
	10~15년	47	23.0	45	26.2
	15~20년	41	20.1	17	9.9
	20년이상	30	14.7	23	13.4
업종	은행	62	30.4	45	26.2
	보험	134	65.7	122	70.9
	기타금융	8	3.9	5	2.9

〈표 11〉 두 집단의 경로분석 결과

경로	낮은 집단				높은 집단			
	β	SE	t value	R^2	β	SE	t value	R^2
PCS → ATTV	-0.002	0.076	0.012	0.727	-0.268	0.082	3.320**	0.662
PCS → SN	0.187	0.063	2.959**		0.112	0.053	2.099*	
PSS → ATTV	-0.358	0.075	4.729***		-0.073	0.087	0.810	
PSS → SN	0.332	0.061	5.466***		0.393	0.088	4.504***	
GISA → ATTV	0.045	0.067	0.677		0.024	0.050	0.513	
GISA → SN	0.248	0.056	4.435***		0.094	0.070	1.302	
ISP → ATTV	-0.085	0.060	1.435		-0.155	0.052	2.971**	
ISP → SN	0.134	0.051	2.593*		0.309	0.067	4.609***	
ATTV → INTV	0.850	0.021	40.719***		0.770	0.030	25.698***	
SN → INTV	-0.007	0.026	0.298		-0.141	0.032	4.384***	

주) $^{*}p < 0.05$, $^{**}p < 0.01$, $^{***}p < 0.001$, β : 경로계수, SE : 표준오차.

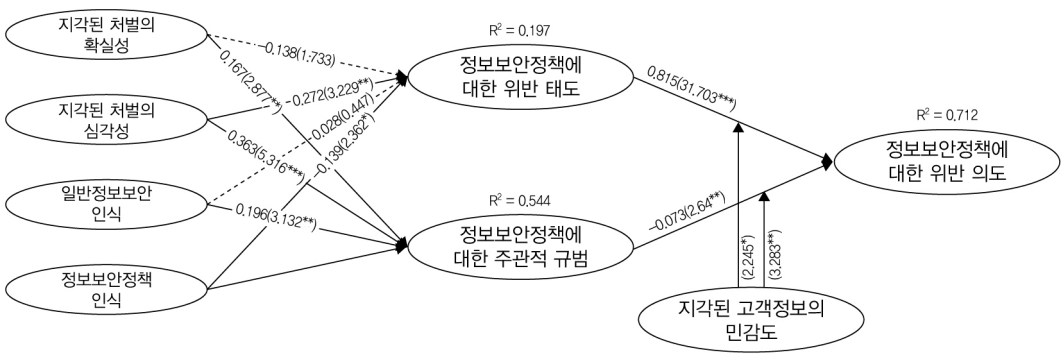


〈그림 3〉 정보보안정책 위반의도에 대한 상호작용효과

〈표 12〉 조절효과 가설검증 결과

	경로	t value	p value	결과
H11	정보보안정책에 대한 위반태도 → 정보보안정책에 대한 위반의도 ↑ 지각된 고객정보의 민감도	2.245*	0.025	채택
H12	정보보안정책에 대한 주관적 규범 → 정보보안정책에 대한 위반의도 ↑ 지각된 고객정보의 민감도	3.283**	0.001	채택

주) $^{*}p < 0.05$, $^{**}p < 0.01$.



주) $^{*}p < 0.05$, $^{**}p < 0.01$, $^{***}p < 0.001$, ()안의 값은 t 값임.

〈그림 4〉 구조방정식 검증 결과

6. 결 론

본 연구에서는 금융회사 정보보안정책의 위반에 영향을 주는 요인에 대해 억제이론, 정보보안인식, 행동이론의 요인을 도출하여 통합된 모형을 제시하였으며, 추가로 금융회사의 조직원이 고객정보의 민감도에 대한 조절효과를 분석하였다. 도출된 연구모형을 금융회사의 조직원 대상으로 실증 분석한 결과, 10개의 기본가설 중 8개의 가설이 유의하게 지지되는 것으로 나타났으며, 금융회사의 정보보안정책에 대한 위반의도에 영향을 주는 요인으로는 정보보안정책에 대한 위반태도와 주관적 규범이 있으며, 이러한 영향요인에는 금융회사의 직원이 취급하는 고객정보에 대한 지각된 민감도에 따라 조절효과가 있는 것으로 나타났다. 각 이론적 관점에서 논의를 정리할 수 있다.

첫째, 처벌에 대한 요인 관점에서 보면, 처벌의 심각성은 정보보안정책 위반에 대한 태도와 주관적 규범에 유의하게 영향을 미치는 것으로 나타났으나, 처벌의 확실성은 주관적 규범에 유의미한 영향을 주는 것으로 나타났고 정보보안정책 위반에 대한 태도에 미치는 영향은 유의하지 않게 나타났다. D'Arcy et al.[2009]는 처벌의 확실성이 유의하지 않으므로 심각성을 보다 강조하고 있으며 금융회사 조직원의 정보보안정책 위반에 영향을 주는 요인을 분석하는 것도 같은 결과로 나타났다.

이는 억제이론의 처벌이 행동이론의 행동에 대한 태도의 좋고 나쁨으로 이해되기보다는 규범적 신념으로써 이해하여야 할 것으로 여겨진다. 따라서 금융회사에서 정보보안정책의 위반행동에 대한 조직원 입장에서는 정보보안정책은 당연하게 지켜야 할 규범으로 여겨지지만, 고객정보의 민감도가 낮은 집단에서는 정보보안정책에 대한 주관적 규범이 위반의도에 유의하지 않게 나타났으므로 조직원의 정보보안인식교육을 통해 취급되는 고객정보의 민감도를 인지시켜 조직원의 고객정보를 민감하게 취급하는 집단으로 이끌어야 할 것이다.

금융회사의 정보보안정책 위반을 예방하기 위해 처벌의 확실성보다는 처벌의 심각성을 강조하는 것이 효과적이라고 할 수 있다. 하지만 본 이론은 조직원이 처벌에 대해 완전하게 이해하고 있음을 가정하고 있다[Bryan Foltz et al., 2008]. 즉, 자신의 행동이 어떠한 처벌을 유발하는지 개인들은 충분히 인지하고 있음을 가정하고 있다.

따라서 개인들이 처벌에 대해 인지하지 못할 경우, 억제 행위가 발생되지 않을 가능성이 존재한다[Nagin and Pogarsky, 2001]. 또한, 정보보안정책에 대해 몰라서 지키지 않는 것이나 사소한 것을 지키지 않는 것에 대한 처벌을 인식하지 않는 조직원에 대해 정보보안정책이 잘 지켜지게 하려면 위반 시 처벌이 발생한다는 것에 대한 인식을 강조할 필요가 있다. 처벌의 효과는 개인의 고유 경험에 의해 영향을 받아 정보보안정책 위반을 억제하는 것으로 나타난다. 따라서 정보보안정책 위반에 대한 처벌이 확실하게 이루어진다는 것에 대해 경험적으로 인식할 수 있도록 작은 처벌이라고 이루어지도록 하며, 처벌에 대해 조직 내에 인식될 수 있도록 하여야 할 것이다.

둘째, 정보보안정책에 대한 인식 관점에서 보면, 정보보안정책 위반에 대한 태도와 주관적 규범에 유의하게 영향을 미치는 것으로 나타났으나, 일반적인 정보보안에 대한 상식적인 이해는 주관적 규범에는 유의한 영향을 미치나 태도에는 유의하게 영향을 미치지는 않았다. 이는 일반적인 정보보안에 대한 이해가 위반태도를 억제하는 요인으로 작용한다고 볼 수 없다는 결과이다. 또한, 고객정보의 지각된 민감도가 높은 집단에서는 태도와 주관적 규범에 대하여 지지하

지 않는 결과로 나타났다. 금융회사 조직원에게는 정보보안정책에 대한 위반의도를 억제하기 위해 전반적인 정보보안인식에 대해 이해를 높이는 인식교육보다는 정보보안정책에 대한 사례를 통해 정보보안정책의 이해와 필요성을 강조하여야 할 것이다.

셋째, 금융회사에서는 불가피하게 고객정보를 취급하여야 하며, 사회적으로 개인정보 유출 사고에 대한 우려가 커지고 있으므로 조직원이 느끼는 민감도는 증가할 것이다. 또한, 금융회사는 조직원을 대상으로 개인정보보호법의 의무교육을 지속해서 수행하고 있으므로, 고객정보의 민감도에 대한 지각을 높이는 방향으로 교육을 진행하여야 할 것이다. 지각된 고객정보의 민감도가 높은 집단은 주관적 규범에 영향을 주는 규범적 신념으로 처벌과 보안인식이 정보보안정책에 대한 위반의도를 억제하는 효과가 있으므로, 금융회사의 정보보호 컴플라이언스를 강화하기 위해 정보보안교육을 통해 고객정보의 중요성을 강조하고, 정보보안정책에 대한 인식을 높여주며, 처벌에 대해 인식할 수 있는 방향으로 진행되어야 할 것이다. 취급하는 고객정보가 민감하다고 인식할수록 정보보안정책의 위반태도와 주관적 규범에 상호작용효과를 증가시켜 정보보안정책의 위반의도는 감소하고 있으므로, 내부직원에 대하여 정보보안 교육에 취급하는 고객정보의 민감도에 대한 부분을 강조한다면 조직원의 정보보안정책 위반의도는 유의하게 감소할 것으로 여겨진다. 따라서 정보보안 교육의 내용에 정보의 민감도에 대한 교육을 필수적으로 포함할 수 있도록 하여야 할 것이다.

넷째, 가설의 검증결과를 보면, 금융규제 당국이 금융회사의 개인정보 유출사고를 예방하기 위해 발표한 종합대책에 포함된 처벌의 강화와 정보보안교육훈련의 강화는 정보보안정책 위반을 예방하는 효과가 있다는 것이다.

본 연구의 학문적 시사점은 첫째, 금융회사 조직원의 정보보안정책 위반에 대한 향후 연구들의 기초가 될 것으로 기대된다. 둘째, 금융회사 조직원의 정보보안정책 위반태도에 영향을 주는 요인은 기존 학술 연구와 차이가 있다는 것이다. 실무적 시사점은 첫째, 금융회사 조직에서 정보보호 컴플라이언스 강화를 위한 정보보안정책의 전략을 수립할 때 본 연구결과에 근거한 가이드를 제공할 수 있다는 점이며, 둘째, 금융회사 조직원의 고객정보에 대한 지각된 민감도가 정보보안정책 위반에 대한 조절 효과가 있으므로, 위반행위를 억제하기 위해 조직원에 대한 정보보안인식교육을 실시할 때 취급하는 고객정보에 대한 민감도를 강조하여 조직원이 인지할 수 있도록 하여야 한다는 교육 방향을 제시하였다는 점이다.

본 연구의 한계는 정보보안정책 위반에 대한 대상을 금융회사로 한정하여 연구하였으므로 다른 산업에서 분석할 경우 결과가 다르게 나올 수 있으며, 국내의 금융회사 조직원을 대상으로 수행한 연구로써 제한이 있다. 향후 다른 산업에서의 정보 민감도에 대한 내용을 추가하여 분석하여 일반화할 수 있는 이론인가를 추가로 연구해 볼 필요가 있으며, 정보보안정책에 대한 위반의도에 큰 영향을 주는 것이 위반태도임에도 불구하고 독립변수로 선정한 처벌과 보안인식은 주관적 규범을 더 크게 설명하고 있어, 향후 위반태도에 대한 설명력이 큰 독립변수를 찾는 연구의 진행이 필요하다.

참 고 문 헌

[1] 강다연, 장명희, “해운항만조직 구성원들의 정보보안정책 준수에 영향을 미치는 요인”, *한국항만경제학회지*, 제28권 제1호, 2012, pp. 1-23.

[2] 강다연, 장명희, “정보보안정책 준수가 정보보안능력 및 행동에 미치는 영향 분석 : 해운항만조직 구성원을 대상으로”, *한국항만경제학회지*, 제30권 제1호, 2014, pp. 97-118.

[3] 강 욱, 전용태, “산업보안 담당자의 보안정책 준수에 영향을 미치는 요인 : 억제이론과 합리적 선택이론을 중심으로”, *한국경찰연구*, 제13권 제3호, 2014, pp. 273-298.

[4] 김상현, 송영미, “조직 구성원들의 정보보안정책 준수 동기요인에 관한 연구”, *e-비즈니스연구*, 제12권 제3호, 2011, pp. 327-349.

[5] 김상훈, 박선영, “정보보안정책 준수 의도에 대한 영향요인”, *한국전자거래학회지*, 제16권 제4호, 2011, pp. 33-51.

[6] 김중인, “반영지표 vs. 조형지표”, *마케팅연구*, 제27권 제4호, 2012, pp. 199-226.

[7] 박철주, 임명성, “기술스트레스가 정보보안에 미치는 영향에 관한 연구”, *디지털융복합연구*, 제10권 제5호, 2012a, pp. 37-51.

[8] 박철주, 임명성, “보안 대책이 지속적 보안 정책 준수에 미치는 영향”, *디지털정책연구*, 제10권 제4호, 2012b, pp. 23-35.

[9] 안중호, 박준형, 성기문, 이재홍, “처벌과 윤리교육이 정보보안준수에 미치는 영향 : 조직유형의 조절효과를 중심으로”, *Information Systems Review*, 제12권 제1호, 2010, pp. 23-42.

[10] 윤일한, 권순동, “정보보안 컴플라이언스와 위기대응이 정보보안 신뢰에 미치는 영향에 관한 연구”, *Information Systems Review*, 제17권 제1호, 2015, pp. 141-169.

[11] 이강신, “전자금융거래 시 보안 통제 사항의 개선 연구”, *정보보호학회논문지*, 제25권 제4호, 2015, pp. 881-888.

[12] 이성규, 채명신, “산업보안정책 준수의지에 영향을 미치는 요인분석”, *대한경영학회지*, 제27권 제6호, 2014, pp. 927-953.

[13] 임명성, “조직 구성원들의 정보보안정책 준수 행위 의도에 관한 연구”, *디지털정책연구*, 제10권 제10호, 2012a, pp. 119-128.

[14] 임명성, “조직의 보안 분위기가 개인의 기회주의 행동에 미치는 영향에 관한 실증 연구”, *디지털융복합연구*, 제10권 제10호, 2012b, pp. 31-46.

[15] 임명성, “정보보안정책의 특성이 구성원들의 보안정책 준수 행위에 미치는 영향에 관한 연구”, *디지털정책연구*, 제11권 제1호, 2013a, pp. 27-38.

[16] 임명성, “조직 구성원들의 정보보안정책 위반에 영향을 미치는 요인”, *디지털융복합연구*, 제11권 제2호, 2013b, pp. 19-32.

[17] 임명성, “조직 구성원들의 정보보안정책 준수에 영향을 미치는 요인에 관한 연구 : 금융서비스업을 중심으로”, *서비스경영학회지*, 제14권 제1호, 2013c, pp. 143-171.

[18] 임명성, 한군희, “정보보안정책 준수에 영향을 미치는 요인 : 위험보상이론 관점에서”, *디지털융복합연구*, 제11권 제10호, 2013, pp. 153-168.

[19] 장상수, 조태희, 신승호, 신대철, 정보보호관리체계의 구축과 활용, 제1판, 생능출판사, 2013.

[20] 정우진, 신유형, 이상용, “금융회사의 고객정보보호에 대한 내부직원의 태도 연구”, *Asia Pacific Journal of Information Systems*, 제22권 제1호, 2012, pp. 53-77.

[21] 정해철, 김현수, “조직구성원의 정보보안 의식과 조직의 정보보안 수준과의 관계 연구”, *Journal of Information Technology Applications and Management*, 제7권 제2호, 2000, pp. 117-134.

[22] Ajzen, I., “The theory of planned behavior”, *Organizational behavior and human decision processes*, Vol. 50, No. 2, 1991, pp. 179-

211.

[23] Anderson, C. L. and Agarwal, R., "Practicing safe computing : A multimedia empirical examination of home computer user security behavioral intentions", *Mis Quarterly*, Vol. 34, No. 3, 2010, pp. 613-643.

[24] Anderson, J. C. and Gerbing, D. W., "Structural equation modeling in practice : A review and recommended two-step approach", *Psychological Bulletin*, Vol. 103, No. 3, 1988, p. 411.

[25] Aurigemma, S., "A composite framework for behavioral compliance with information security policies", *Journal of Organizational and End User Computing*, Vol. 25, No. 3, 2013, pp. 32-51.

[26] Bagozzi, R. P. and Yi, Y., "On the evaluation of structural equation models", *Journal of the Academy of Marketing Science*, Vol. 16, No. 1, 1988, pp. 74-94.

[27] Bansal, G. and Gefen, D., "The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online", *Decision Support Systems*, Vol. 49, No. 2, 2010, pp. 138-150.

[28] Barclay, D., Higgins, C., and Thompson, R., "The partial least squares (pls) approach to causal modeling : Personal computer adoption and use as an illustration", *Technology Studies*, Vol. 2, No. 2, 1995, pp. 285-309.

[29] Bollen, K. A., *Structural equations with latent variables*, John Wiley and Sons, 2014.

[30] Bulgurcu, B., Cavusoglu, H., and Benbasat, I., "Effects of individual and organization based beliefs and the moderating role of work experience on insiders' good security behaviors", *Computational Science and Engineering, 2009 CSE'09 International Conference on*, Vol. 3, 2009a, pp. 476-481.

[31] Bulgurcu, B., Cavusoglu, H., and Benbasat, I., "Roles of information security awareness and perceived fairness in information security policy compliance", *Proceedings of the Americas Conference on Information Systems*, Vol. 15, No. 5, 2009b, pp. 3269-3277.

[32] Bulgurcu, B., Cavusoglu, H., and Benbasat, I., "Information security policy compliance : An empirical study of rationality-based beliefs and information security awareness", *MIS quarterly*, Vol. 34, No. 3, 2010, pp. 523-548.

[33] Chin, W. W., "The partial least squares approach to structural equation modeling", *Modern Methods for Business Research*, Vol. 295, No. 2, 1998, pp. 295-336.

[34] Chin, W. W. and Gopal, A., "Adoption intention in gss : Relative importance of beliefs", *ACM SigMIS Database*, Vol. 26, No. 2-3, 1995, pp. 42-64.

[35] 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 an electronic-mail emotion/adoption study", *Information Systems Research*, Vol. 14, No. 2, 2003, pp. 189-217.

[36] Cohen, J., *Statistical power analysis for the behavioral sciences*, Academic press, 2013.

[37] D'Arcy, J. and Herath, T., "A review and analysis of deterrence theory in the is security literature : Making sense of the disparate findings", *European Journal of Infor-*

mation Systems, Vol. 20, No. 6, 2011, pp. 643-658.

[38] D'Arcy, J. and Hovav, A., "Deterring internal information systems misuse", *Communications of the ACM*, Vol. 50, No. 10, 2007, pp. 113-117.

[39] D'Arcy, J., Hovav, A., and Galletta, D., "User awareness of security countermeasures and its impact on information systems misuse : A deterrence approach", *Information Systems Research*, Vol. 20, No. 1, 2009, pp. 79-98.

[40] Fishbein, M. and Ajzen, I., *Belief, attitude, intention and behavior : An introduction to theory and research*, MA : Addison-Wesley, 1975.

[41] Fishbein, M., Ajzen, I., Albarracin, D., and Hornik, R. C., *Prediction and change of health behavior : Applying the reasoned action approach*, Psychology Press, 2007.

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

[43] Foltz C. B., Schwager, P. H., and Anderson, J. E., "Why users (fail to) read computer usage policies", *Industrial Management and Data Systems*, Vol. 108, No. 6, 2008, pp. 701-712.

[44] Gefen, D. and Straub, D., "A practical guide to factorial validity using pls-graph : Tutorial and annotated example", *Communications of the Association for Information Systems*, Vol. 16, 2005, p. 1.

[45] Geisser, S., "The predictive sample reuse method with applications", *Journal of the American Statistical Association*, Vol. 70, No. 350, 1975, pp. 320-328.

[46] Guo, K. H., Yuan, Y., Archer, N. P., and Connelly, C. E., "Understanding nonmalicious security violations in the workplace : A composite behavior model", *Journal of Management Information Systems*, Vol. 28, No. 2, 2011, pp. 203-236.

[47] Hair, J. F., Sarstedt, M., Ringle, C. M., and Mena, J. A., "An assessment of the use of partial least squares structural equation modeling in marketing research", *Journal of the Academy of Marketing Science*, Vol. 40, No. 3, 2012, pp. 414-433.

[48] Henseler, J., Ringle, C. M., and Sinkovics, R. R., "The use of partial least squares path modeling in international marketing", *Advances in International Marketing (AIM)*, Vol. 20, 2009, pp. 277-320.

[49] Herath, T. and Rao, H. R., "Encouraging information security behaviors in organizations : Role of penalties, pressures and perceived effectiveness", *Decision Support Systems*, Vol. 47, No. 2, 2009a, pp. 154-165.

[50] Herath, T. and Rao, H. R., "Protection motivation and deterrence : A framework for security policy compliance in organisations", *European Journal of Information Systems*, Vol. 18, No. 2, 2009b, pp. 106-125.

[51] Herzberg, F., "The motivation-hygiene concept and problems of manpower", *Personnel Administration*, 1964.

[52] Hu, Q., Xu, Z., Dinev, T., and Ling, H., "Does deterrence work in reducing information security policy abuse by employees?", *Commu-*

nications of the ACM, Vol. 54, No. 6, 2011, pp. 54-60.

[53] Hulland, J., "Use of partial least squares (pls) in strategic management research : A review of four recent studies", *Strategic Management Journal*, Vol. 20, No. 2, 1999, pp. 195-204.

[54] Ifinedo, P., "Understanding information systems security policy compliance : An integration of the theory of planned behavior and the protection motivation theory", *Computers and Security*, Vol. 31, No. 1, 2012, pp. 83-95.

[55] Jöreskog, K. G. and Sörbom, D., *Lisrel 7 : A guide to the program and applications*, SPSS, 1989.

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

[57] Keil, M., Rai, A., and Liu, S., "How user risk and requirements risk moderate the effects of formal and informal control on the process performance of it projects", *European Journal of Information Systems*, Vol. 22, No. 6, 2013, pp. 650-672.

[58] Keil, M., Tan, B. C., Wei, K. K., Saarinen, T., Tuunainen, V., and Wassenaar, A., "A cross-cultural study on escalation of commitment behavior in software projects", *MIS Quarterly*, Vol. 24, No. 2, 2000, pp. 299-325.

[59] Kim, S. H., Yang, K. H., and Park, S. Y., "An integrative behavioral model of information security policy compliance", *The Scientific World Journal*, Vol. 2014, 2014.

[60] Kutner, M. H., Nachtsheim, C., and Neter, J., *Applied linear regression models*, McGraw-Hill/Irwin, 2004.

[61] Leach, J., "Improving user security behaviour", *Computers and Security*, Vol. 22, No. 8, 2003, pp. 685-692.

[62] Lee, J. T. and Lee, Y. H., "A holistic model of computer abuse within organizations", *Information Management and Computer Security*, Vol. 10, No. 2, 2002, pp. 57-63.

[63] Li, H., Zhang, J., and Sarathy, R., "Understanding compliance with internet use policy from the perspective of rational choice theory", *Decision Support Systems*, Vol. 48, No. 4, 2010, pp. 635-645.

[64] Nagin, D. S. and Paternoster, R., "Enduring individual differences and rational choice theories of crime", *Law and Society Review*, Vol. 27, No. 3, 1993, pp. 467-496.

[65] Nagin, D. S. and Pogarsky, G., "Integrating celerity, impulsivity, and extralegal sanction threats into a model of general deterrence : Theory and evidence", *Criminology*, Vol. 39, No. 4, 2001, pp. 865-892.

[66] Ophoff, J., Jensen, A., Sanderson-Smith, J., Porter, M., and Johnston, K., "A descriptive literature review and classification of insider threat research", *Proceedings of Informing Science and IT Education Conference (InSITE)*, 2014.

[67] Pahnila, S., Siponen, M., and Mahmood, A., "Employees' behavior towards is security policy compliance", *System Sciences, 2007 HICSS 2007 40th Annual Hawaii International Conference on*, 2007, p. 156b.

[68] Paternoster, R. and Simpson, S., "Sanction

threats and appeals to morality : Testing a rational choice model of corporate crime", *Law and Society Review*, Vol. 30, No. 3, 1996, pp. 549-583.

[69] Peltier, T. R., "Implementing an information security awareness program", *Information Systems Security*, Vol. 14, No. 2, 2005, pp. 37-49.

[70] Siponen, M., Mahmood, M. A., and Pahnila, S., "Employees'adherence to information security policies : An exploratory field study", *Information and Management*, Vol. 51, No. 2, 2014, pp. 217-224.

[71] Siponen, M., Pahnila, S., and Mahmood, M. A., "Compliance with information security policies : An empirical investigation", *Computer*, Vol. 43, No. 2, 2010, pp. 64-71.

[72] Siponen, M. and Vance, A., "Neutralization : New insights into the problem of employee information systems security policy violations", *MIS quarterly*, Vol. 34, No. 3, 2010, pp. 487-502.

[73] Siponen, M., "A conceptual foundation for organizational information security awareness", *Information Management and Computer Security*, Vol. 8, No. 1, 2000, pp. 31-41.

[74] Sommestad, T., Hallberg, J., Lundholm, K., and Bengtsson, J., "Variables influencing information security policy compliance", *Information Management and Computer Security*, Vol. 22, No. 1, 2014, pp. 42-75.

[75] Son, J. Y., "Out of fear or desire? Toward a better understanding of employees' motivation to follow is security policies", *Information and Management*, Vol. 48, No. 7, 2011, pp. 296-302.

[76] Sosik, J. J., Kahai, S. S., and Piovoso, M. J., "Silver bullet or voodoo statistics? A primer for using the partial least squares data analytic technique in group and organization research", *Group and Organization Management*, Vol. 34, No. 1, 2009, pp. 5-36.

[77] Stone, M., "Cross-validatory choice and assessment of statistical predictions", *Journal of the Royal Statistical Society Series B (Methodological)*, 1974, pp. 111-147.

[78] Straub, D., "Effective is security : An empirical study", *Information Systems Research*, Vol. 1, No. 3, 1990, pp. 255-276.

[79] Tenenhaus, M., Amato, S., and Esposito, Vinzi V., "A global goodness-of-fit index for pls structural equation modelling", *Proceedings of the XLII SIS scientific meeting*, Vol. 1, 2004, pp. 739-742.

[80] Tenenhaus, M., Vinzi, V. E., Chatelin, Y. M., and Lauro, C., "PLS path modeling", *Computational Statistics and Data Analysis*, Vol. 48, No. 1, 2005, pp. 159-205.

[81] Theoharidou, M., Kokolakis, S., Karyda, M., and Kiountouzis, E., "The insider threat to information systems and the effectiveness of iso17799", *Computers and Security*, Vol. 24, No. 6, 2005, pp. 472-484.

[82] Vance, A., Siponen, M., and Pahnila, S., "Motivating is security compliance : Insights from habit and protection motivation theory", *Information and Management*, Vol. 49, No. 3-4, 2012, pp. 190-198.

[83] Vance, A. and Siponen, M., "Is security policy violations : A rational choice perspective", *Journal of Organizational and End User Computing (JOEUC)*, Vol. 24, No. 1,

2012, pp. 21-41.

[84] Wall, J. D., Palvia, P., and Lowry, P. B., "Control-related motivations and information security policy compliance : The role of autonomy and efficacy", *Journal of Information Privacy and Security*, Vol. 9, No. 4, 2013, pp. 52-79.

[85] Whitman, M. E., "In defense of the realm : Understanding the threats to information security", *International Journal of Information Management*, Vol. 24, No. 1, 2004, pp. 43-57.

[86] Whitman, M. E., Townsend, A. M., and Aalberts, R. J., "Information systems security and the need for policy", *Information Security Management : Global Challenges in the New Millennium*, 2001, pp. 9-18.

[87] Williams, K. R. and Hawkins, R., "Perceptual research on general deterrence : A critical review", *Law and Society Review*, Vol. 24, No. 4, 1986, pp. 545-572.

[88] Willison, R. and Warkentin, M., "Beyond deterrence : An expanded view of employee computer abuse", *MIS Quarterly*, Vol. 37, No. 1, 2013.

[89] Yang, Y., Stafford, T. F., and Gillenson, M., "Satisfaction with employee relationship management systems : The impact of usefulness on systems quality perceptions", *European Journal of Information Systems*, Vol. 20, No. 2, 2011, pp. 221-236.

[90] Yoon, C. H., "Theory of planned behavior and ethics theory in digital piracy : An integrated model", *Journal of Business Ethics*, Vol. 100, No. 3, 2011, pp. 405-417.

[91] Yoon, C. H. and Kim, H. G., "Understanding computer security behavioral intention in the workplace", *Information Technology and People*, Vol. 26, No. 4, 2013, pp. 401-419.

[92] Zhang, J., Reithel, B. J., and Li, H., "Impact of perceived technical protection on security behaviors", *Information Management and Computer Security*, Vol. 17, No. 4, 2009, pp. 330-340.

〈부록 1〉 변수의 설문문항

변수	설문문항	관련연구
지각된 처벌의 확실성 (PCS)	1. 정보보안정책을 위반한다면 확실히 처벌이 있다. 2. 내가 회사의 정보보안정책을 위반한다면 반드시 처벌이 있을 것이다. 3. 상사가 나의 정책위반 사실을 안다면, 나를 공식적으로 처벌할 것이다. 4. 동료나 상사가 정보보안정책을 위반한다면 반드시 처벌이 있을 것이다.	Nagin and Paternoster[1993], Paternoster and Simpson[1996], Siponen and Vance [2010]
지각된 처벌의 심각성 (PSS)	1. 내가 정보보안정책을 위반할 경우, 나는 동료들로부터 신뢰를 잃을 것이다. 2. 내가 정보보안정책을 위반할 경우, 나의 진급에 부정적인 영향을 줄 것이다. 3. 나는 처벌을 인생의 심각한 사건으로 여긴다. 4. 내가 정보보안정책을 위반할 경우, 나는 상사의 신뢰를 잃을 것이다.	Nagin and Paternoster[1993], Paternoster and Simpson[1996], Siponen and Vance [2010]
일반정보보안인식 (GISA)	1. 나는 보안사고로 인한 부정적인 결과를 알고 있다. 2. 나는 정보보안 문제를 해결하기 위해 많은 노력과 비용이 필요하다는 것을 알고 있다. 3. 나는 정보보안 위험에 대한 걱정을 이해하고 있다.	Bulgurcu et al. [2010]
정보보안정책인식 (ISP)	1. 나는 회사의 정보보안정책을 알고 있다. 2. 나는 회사의 정보보안정책에 대한 나의 책임을 알고 있다. 3. 나는 회사의 정보보안정책을 이해하고 있다.	Bulgurcu et al. [2010]
정보보안정책에 대한 위반태도 (ATTV)	1. [시나리오 주인공]의 태도는 [시나리오 주인공]에게 필요하다. 2. [시나리오 주인공]의 태도는 [시나리오 주인공]에게 유용하다. 3. [시나리오 주인공]의 태도는 [시나리오 주인공]에게 혜택을 가져다 준다.	Ajzen[1991], Bulgurcu et al. [2010]
정보보안정책에 대한 주관적 규범 (SN)	1. 나의 동료들은 내가 정보보안정책을 반드시 준수해야 한다고 생각한다. 2. 나의 경영진은 내가 정보보안정책을 반드시 준수해야 한다고 생각한다. 3. 나의 상사는 내가 정보보안정책을 반드시 준수해야 한다고 생각한다.	Ajzen[1991], Bulgurcu et al. [2010], Siponen and Vance [2010]
정보보안정책에 대한 위반의도 (INTV)	1. 내가 [시나리오의 주인공]라면, 나도 그렇게 행동할 것이다. 2. 내가 [시나리오]와 비슷한 상황에 처해진다면, 나도 같은 행동을 할 것이다.	Paternoster and Simpson[1996], Siponen and Vance [2010], Siponen et al.[2010]
지각된 고객정보의 민감도 (PCIS)	업무상 취급하는 고객정보가 유출되었을 때, 심각하게 생각하는 민감도의 정도는 1. 고객의 고유식별정보(주민등록번호, 여권번호, 운전자등록번호, 외국인 등록번호) 2. 고객의 지급결제정보(신용카드번호, 계좌번호 등) 3. 고객의 신용정보(연봉, 대출 정보, 금융 신용정보 등) 4. 고객의 연락처(전화번호, 이메일, 주소 등)	Bansal and Gefen [2010]

〈부록 2〉 독립변수의 탐색적 요인분석 결과

	PCS	PSS	GISA	ISP	ATTV	SN
PCS2	0.876	0.141	0.137	0.065	-0.133	0.181
PCS4	0.846	0.254	0.020	0.145	-0.168	0.144
PCS3	0.844	0.245	0.018	0.150	-0.150	0.168
PCS1	0.834	0.107	0.167	0.075	-0.121	0.200
PSS3	0.228	0.772	0.173	0.230	-0.064	0.161
PSS4	0.452	0.666	0.180	0.062	-0.245	0.314
PSS2	0.541	0.597	0.144	0.044	-0.123	0.258
PSS1	0.554	0.576	0.087	0.099	-0.237	0.166
GISA2	0.128	0.048	0.817	0.315	-0.081	0.186
GISA1	0.107	0.186	0.810	0.249	-0.046	0.090
GISA3	0.085	0.150	0.780	0.369	-0.077	0.261
ISP1	0.104	0.088	0.279	0.878	-0.107	0.143
ISP3	0.109	0.118	0.277	0.878	-0.085	0.178
ISP2	0.149	0.123	0.341	0.830	-0.125	0.163
ATTV2	-0.176	-0.086	-0.062	-0.108	0.940	-0.108
ATTV1	-0.127	-0.129	-0.086	-0.121	0.929	-0.089
ATTV3	-0.202	-0.098	-0.037	-0.055	0.912	-0.122
SN2	0.278	0.165	0.216	0.100	-0.094	0.842
SN3	0.288	0.209	0.198	0.234	-0.181	0.801
SN1	0.262	0.264	0.179	0.371	-0.165	0.691

저자소개

이 정 하

숭실대학교 정보과학대학원에서 공학석사(정보통신융합학 전공) 학위를 취득하였고, 서울과학종합대학원대학교에서 경영학 박사과정(정보보호경영 전공)을 수료하였다. 현재 외국계 생명보험회사에서 IT 보안관리자로 재직 중이며, (사)한국씨아이에스에스피협회 보안연구실 연구위원, (사)한국정보시스템통제감사협회 아카데미 연구위원 및 보안부문 간사로 활동 중이다. 주요 관심분야는 정보보호경영, 정보보호거버넌스, 개인정보보호, 금융정보보호, 사물인터넷, 빅 데이터 등이다.

이 상 용

현재 한양대학교 경영대학 교수로 재직 중이다. 서울대학교 경제학과를 졸업하고, Texas A&M University에서 박사학위를 취득하였다. 주요 관심분야는 정보경제, 개인정보보호(privacy) 및 보안, 소셜미디어, 정보통신정책, 기술경영 등이다. 관련 연구들을 Management Science, MIS Quarterly, Journal of Management Information Systems를 비롯한 다수의 저널에 게재하고 있다.