Information Systems Review
Vol. 18, No. 4 December 2016 http://dx.doi.org/10.14329/isr.2016.18.4.017

금융회사의 정보보안정책 위반요인에 관한 연구: 내부직원과 외주직원의 차이

Violations of Information Security Policy in a Financial Firm: The Difference between the Own Employees and Outsourced Contractors

이 정 하 (Jeong-Ha Lee) 서울과학종합대학원대학교 경영학 박사과정
이 상 용 (Sang-Yong Tom Lee) 한양대학교 경영대학 교수, 교신저자

요 약

금융회사의 정보보안사고는 정당한 접근 권한을 가진 내부자에 의해 발생하는 사례가 증가하고 있으며, 특히 외주직원에 의한 사고가 증가하고 있다. 금융회사의 외주용역 증가에 따라, 내부자 위협 관점에서 정당한 권한을 가진 외주직원은 조직의 정보보안정책을 위반할 수 있는 위협적인 존재가 되고 있다. 본 연구의 목적은 내부직원과 외주직원의 차이를 분석하고 정보보안정책의 위반요인을 확인하여 금융회사의 정보보안정책이 바르게 작용할 수 있도록 하기 위함이다. 금융회사 조직원의 정보보안정책에 대한 위반요인에 대해 계획된 행동이론, 일반억제이론 및 정보보안인식을 기초하여 연구모형을 설계하고, 내부직원과 외주직원 간의 차이를 분석하였다. 분석에 사용된 설문은 온라인과 오프라인으로 수집된 363개의 샘플이 사용되었으며, 그룹 간 차이를 분석하기 위해 내부직원 246명(68%)과 외주직원 117명(32%)을 두 그룹으로 나누어 다중 집단 분석을 이용하였다. 차이 분석을 수행한 결과, 외주직원은 내부직원과 달리 정보보안정책에 대한 위반의도가 정보보안정책에 대한 주관적 규범에 영향을 받지 않고 정보보안정책에 대한 행동통제에 영향을 받아 억제되는 것으로 나타났다. 이는 외주직원은 자신이 스스로 할 수 있다고 여기는 자기효능감과 같은 요인에 의해 정보보안정책에 대한 위반의도가 통제되는 것을 나타내는 것이며, 외주직원관리에 이를 응용하여 정보보안교육을 내부직원과 달리 정보보안정책에 대한 조직의 기대를 강조하기보다는 스스로 지킬 수 있을 정도로 외주직원이 기술을 가지고 있음을 강조하고 쉽게 지킬 수 있다는 것을 강조하면 더욱 효과적일 것이다. 결론적으로 금융회사의 외주직원에 대한 정보보안교육 프로그램은 정보보안정책에 대한 이해도를 높일 수 있도록 하여야 하며, 외주직원관리에서는 외주직원이 스스로 지킬 수 있도록 쉬운 보안체계를 유지하는 것이 효과적이라 할 수 있다.

키워드 : 정보보안정책, 외주직원관리, 정보보안교육, 정보보안인식, 정보보안훈련

Ⅰ. 서 론

전통적으로 정보보호는 내부자 위협보다는 외부자 위협을 중심으로 다루어져 왔고(Hamin, 2000), 내부자 위협(Insider Threat)은 외부자 위협보다 위험과 가능성이 작다고 평가됐다(Hong *et al*., 2009). 그러나 외부자 위협이 일반적이지만, 내부자 위협이 기업에 더 해로운 것으로 나타나고 있다. 대표적인 보안사고로는 2014년 3개 카드사에서 1억 400만 건이 넘는 개인정보가 유출되는 사건이 발생하였다. 이 사건은 외주직원이 업무를 위해 부여된 접근 권한을 악의적으로 이용하여 개인정보를 유출한 사례였다.

금융회사를 비롯한 기업들은 핵심업무에 집중하기 위하여 핵심업무 외의 업무들을 외주직원이 수행하도록 하는 사례가 증가하고 있으며(Lacity and Hirschheim, 1993), 대외 개방으로 인한 경쟁심화의 변화와 혁신에 적극적인 대응으로 우선하여 제안되는 전략 중의 하나가 외주용역 전략이다(장효강 등, 2009). 업무의 특성상 외주직원도 업무를 위하여 정당한 권한을 부여받아 업무를 수행하고 있고, 정당한 권한을 부여받은 직원이 의도적으로 정보보안정책을 위반하거나 권한의 오용으로 기업의 정보를 유출할 수 있는 위험이 존재하며, 이를 내부자 위협이라고 말한다(Theoharidou *et al*., 2005). 내부자 위협은 다양한 관점으로 설명되고 있으며, 조직의 데이터, 프로세스, 또는 자원을 파괴하거나 부당한 방법으로 위험하게 만드는 행동이라고 말한다(Pfleeger, 2008).

보안전문가들은 직원의 의도적인 정보보안정책의 위반이나 오용이 조직에 치명적인 피해를 주며, 정보보안 방어 영역에서 직원이 가장 취약한 연결고리 중 하나라고 주장한다(Aurigemma and Panko, 2012). 일반적으로 대중 매체에서는 외부 해커에 의한 유출에 관심을 가지지만, 주요 정보보안사고는 신뢰받던 직원의 행동으로 발생했고(Hu *et al*., 2012), 전체 정보보안 사고의 과반수는 정보보안정책을 준수하지 않아 발생한 것으로 나타난다(Ifinedo, 2012). 내부자는 업무를 수행하면서 실수로 혹은 악의적으로 권한을 사용할 수 있고(Sarkar, 2010), 내부자 위협은 우연히 혹은 의도적으로 나타날 수 있다(Carroll, 2006). 일부 연구자는 의도적인 행동에 의해서만 내부자 위협이 나타난다고 주장하기도 한다(Schultz, 2002).

외주용역 시장의 성장에 따라 증가하는 외주직원은 내부의 중요시스템에 접근해 내부직원과 같은 인가된 사용자로서 업무를 수행하기 때문에 금융회사는 외주직원에 의한 내부자 위협에 직면하고 있다. <표 1>의 감사원 보고서에 따르면 금융회사에서 2009년부터 2013년까지 발생한 개인정보 유출 사고 건수의 97%가 내부직원 및 외주직원에 대한 관리부실에서 발생한 것으로 나타났으며, 특히 금융회사의 외주직원에 의한 권한의 남용과 정보보안정책 위반으로 발생하는 보안사고의 문제는 심각하다고 할 수 있다.

즉 최근 금융보안사고는 외주직원에 의한 사고가 증가하고 있어 외주직원에 대한 정보보안관리의 강화가 필요하다. 외주직원은 내부직원과 상의한 특징을 가지고 있어, 회사의 정보보안관리를 위해 외주직원에 대해 특별한 관리가 필요하며 내부자 위협의 관점에서 외주직원의 정보보호관리에 영향을 주는 요인을 내부직원과 비교하여 연구할 필요가 있다.

내부자 위협은 정보보호 영역에서 가장 중요한 영역 중 하나라고 할 수 있으며, 최근 금융회사의 정보보안사고는 내부자에 의해 발생하는 사고가 건수도 많았으며, 특히 외주직원에 의한 보안사고가 발생하였다. 보안 통제는 관리적, 기술적, 물리적 통제의 통합된 정보보호 관리체계를 구성하여 정보보호 경영을 위해 필요하며, 관리적 보안 통제의 취약한 부분이 인적 보안이라고 할 수 있다.

본 연구는 내부직원과 외주직원의 정보보호 인식 및 행동에 관한 초기 연구로서 의의가 있다. 이에 내부직원과 외주직원의 특징을 살펴보고 정보보안정책 위반의 요인들이 어떻게 차이가 발생하는지 통계적으로 검정하고자 한다. 이러한 연

구를 통하여, 외주직원에 대한 정보보호 인식 및 행동을 이해하고 정보보호관리에 관한 시사점을 찾아보고자 하는 것이다.

본 연구의 연구모형은 정보보안정책 연구에서 많이 사용되는 계획된 행동이론을 기반으로 일반억제이론과 정보보안인식을 선행요인으로 추가하여 설계하였다(Siponen and Vance, 2010; 이정하, 이상용, 2015; 임명성, 2012). H1~H5까지는 기존에 많이 연구된 이론들을 이용하여 벤치마크 모형으로 설계하고, 본 연구의 중요 관심사항인 내부직원과 외주직원에 대한 차이에 대해서는 H6을 통해 검증하였다.

본 연구의 구성은 외주용역의 특징과 변화, 금융회사의 외주용역 및 보안사고 현황, 내부자 위협 및 관련 선행연구를 살펴보고, 연구모형을 설계하여 PLS(Partial Least Squares)를 이용한 측정모형 및 구조모형을 분석하고 가설을 검증하였다. 마지막으로 분석결과를 해석하며 연구의 시사점과 한계를 설명하였다.

Ⅱ. 연구 배경 및 선행연구

2.1 금융회사의 외주용역과 보안사고 현황

외주용역(Outsourcing)은 외부의 자원이라는 사전적 의미를 지니며, 이 용어는 1900년대 후반부터 사용되어 왔다(Apte, 1990; Lee, 1997). 외주용역은 직원과 자산의 전환이 포함되며, 실제 계약은 국내 혹은 국외와 체결되기도 한다(Bardhan and Kroll, 2003). 비용절감을 위해 낮은 임금체계를 가진 나라에 업무를 외주용역으로 수행하며, 외주용역으로 수행되는 서비스는 IT서비스가 상대적으로 많고 회계/채권 추심 및 세금 처리가 다음으로 높게 나타나고 있다(강주영, 이재규, 2005).

우리나라의 여러 산업 중에서 금융과 유통서비스 업종의 외주용역 비율이 상대적으로 높게

〈표 1〉 최근 5년간 개인정보 유출 현황

(단위: 건)

구 분	원인	합계	2009년	2010년	2011년	2012년	2013년
외부	외주직원 관리부실	91,327,562	186,012	5,145	2,516,048	24,284,796	64,335,561
	해킹 취약점 방치	2,449,658	185,903		2,263,755		
내부	내부직원 열람권한 과다설정	88,686,777			246,482	24,268,743	64,171,552
	내부직원 열람권한 남용	190,711		4,838	5,811	16,053	164,009

주) 감사결과보고서-금융회사 개인정보 유출 관련 검사·감독 실태(2014).

〈표 2〉 외주용역에 의한 금융회사 보안사고 사례

일시	금융회사	외주용역 운영방법	보안사고 발생방법
2014. 1	A 카드 3사	고객정보 관리를 외주직원에게 맡김	외주직원들이 의도적으로 유출
2013. 12	B 은행	고객정보를 외부 재위탁 계약업체 직원에게 맡김	외부 재위탁 계약업체 직원 등이 의도적으로 고객정보 유출
2011. 4	C 은행	외주업체에서 서버 관리	외주업체 직원 노트북을 통해 해킹으로 전산망 마비
2011. 3	D 캐피털	외주업체에서 보안업무 위탁관리	미삭제된 퇴직자 계정 정보를 활용하여 중요시스템 접근

주) 김양훈 등(2014)의 연구내용을 연구자가 다시 편집함.

나타나고 있다. 이 두 업종의 외주용역 비율은 각각 87%, 74%에 달하지만, 제조업의 경우는 49%의 기업만이 외주용역을 활용하고 있는 것으로 나타났다(KRG, 2002). 규모별로는 기업의 규모가 클수록 외주용역을 하는 비율이 높아지고 있음을 볼 수 있고, 외주용역의 방법은 타 회사 방식, 자회사 방, 공동 방식으로 나타나고, 외주용역의 범위, 적용 업무 및 자산의 이용 여부에 따라 구분될 수 있다(강주영, 이재규, 2005).

외주용역에 의한 보안사고는 외부업체 담당자의 의도적인 유출, 부주의로 중요정보가 저장된 매체의 분실, 부주의로 인가되지 않은 사용자에게 중요정보 유출, 퇴사자 계정의 미삭제로 인한 정보 유출 및 고의로 해킹 도구를 이용하여 정보유출 등의 사례로 나타나며(김양훈 등, 2014), 금융회사의 외주용역에 의한 보안사고는 <표 2>와 같이 나타난다. 이러한 정보보안사고의 주요 발생원인은 외주용역 서비스의 운영방법에서 찾아볼 수 있으며, 금융회사의 고객정보를 포함한 중요정보를 보관하는 정보처리시스템에 대해 강화된 접근제어와 같은 정보보호 관리통제의 고려없이 외주용역을 수행하는 외주직원에게 전반적인 관리를 맡기는 것이 큰 원인이다.

2.2 외주용역 보안에 관한 선행연구

외주용역 보안에 관한 선행연구는 <표 3>처럼 기업이 외주용역을 선택하는 데 있어 위험으로써 정보보안을 고려하고 있으며, 정보보안 수준을 관리하기 위한 기준 및 정보보호 시스템의 구성을 제안하고 있다. 이러한 연구의 결과가 금융회사의 외주직원관리에 기준을 제공하고 있으나, 정보보안정책 위반의도에 대해 다루고 있는 연구는 찾아볼 수 없었다.

최창래 등(2014)의 연구는 금융보안 위험을 감소시키기 위해 IT 도급 정책의 결정 절차에 따른 분석 및 설계 등의 본질적인 업무는 내부 직원이 수행하고 검증된 요구사항에 따라 외부 직원이 업무를 수행함으로써 비용, 품질 및 위험에 대한 만족도를 높일 수 있고 외주직원에 의한 내부시스템 접근을 제한함으로써 보안 위험을 줄일 수 있다고 하였고, 김양훈 등(2014)은 ICT 환경에서의 외주용역의 보안관리를 위한 기준으로써 사용할 수 있는 보안 통제 항목을 도출하여 보안수준을 높이기 위한 보안관리 방안을 제시하였다.

Gaonjur and Bokhoree(2006)는 IT 외주용역에 대한 보안 위험을 설명하고, 내부자 위협의 중요한 위험임을 설명하고 위험을 감소시키는 방안으로 IDS와 Honey pot의 구성을 제안하였으며, Loh and Venkatraman(1995)은 IT 외주용역의 이득과 위험 요인에 대해 분석하고 통제와 기회주의 위험이 IT 외주용역에 부(-)의 영향을 준다고 설명하였다. Lee(1997)는 은행을 중심으로 설문하여

〈표 3〉 외주용역 보안에 관한 선행연구

구 분	연구자	연구 주요 내용
ITO	최창래 등(2014)	금융보안 위험 기반의 IT 도급 정책 결정 방안에 대해 외주직원 문제를 해결하기 위한 정책 결정 흐름을 제공하고 사례를 통한 효율적인 운영정책을 제시
	김양훈 등(2014)	외주용역에 대한 보안 통제 항목을 도출하고 이를 바탕으로 외주용역 보안수준을 향상하기 위한 보안관리 추진방향을 제시
	Gaonjur and Bokhoree(2006)	IT 외주용역에 대한 IT 보안에 대해 내부자 위협 관점의 위험을 설명하고 네트워크 보안관리를 통한 위험 감소 방안을 제시
	Loh and Venkatraman (1995)	IT 외주용역에 대해 이득 요인과 위험 요인에 대해 통계적으로 분석
BPO	Yang *et al.*(2007)	BPO의 영향요인을 AHP(Analytic Hierarchy Process)를 이용하여 2단계 계층적 의사결정 요인을 분석.

보안 위험이 외주용역을 결정하는 요인으로 통계적으로 유의하게 나타났다고 설명하였다.

Yang *et al.*(2007)의 연구에 의하면, BPO의 영향요인을 1단계와 하부요인인 2단계로 나누어 설명하였다. 1단계 요인은 기대요인(Expectation), 위험요인(Risk), 환경요인(Environment)으로 설명하고, 위험요인의 하부요인인 2단계 요인으로 정보보안(Information Security), 통제력 상실(Loss of Control), 노동조합(Labor Union), 도덕적 해이(Morale Problem)를 설명하였다.

2.3 정보보안정책 위반요인에 관한 선행연구

정보보안정책 위반요인에 관한 선행연구는 <표 4>와 같이 위반의도 자체를 연구한 연구자와 위반을 남용 혹은 오용으로 해석하여 연구한 연구자로 구분할 수 있다. 위반의도를 연구한 결과는 정보보안인식 및 지각된 처벌이 정보보안정책 위반의도에 영향을 주는 것으로 나타났으며, 남용 및 오용에 관한 연구에서도 같은 결과가 나타났다고 해석할 수 있다.

이정하, 이상용(2015)의 연구는 금융회사의 조직원을 대상으로 정보보안정책에 대한 위반의도에 영향을 주는 요인에 대해 일반억제이론, 정보보안인식 및 합리적 행동이론을 기초로 한 연구모형을 설계하고 실증 분석하여 통계적으로 유의미한 요인들을 설명하였다. 임명성(2013b)의 연구는 도덕적 해방이론을 토대로 정보보안정책의 위반에 대한 모형을 설계하고 분석을 수행하였으며, Siponen and Vance(2010)의 연구에서는 중화기술이론을 적용하여 중화기술과 지각된 처벌이 정보보안정책 위반의도에 영향을 미치는 것으로 실증 분석하였다.

D'Arcy *et al.*(2009)의 연구는 오용의도에 영향을 주는 요인을 분석하여 처벌이 정보시스템 오용의도에 영향을 미친다고 설명하였으며, 정우진 등(2012)의 연구는 정보보안정책에 대한 금융회사 조직원의 남용에 관한 연구로 내부직원의 정보보호활동의 인지 수준에 따라 불필요한 고객정보를 조회하는 행동에 미치는 영향을 분석하였다.

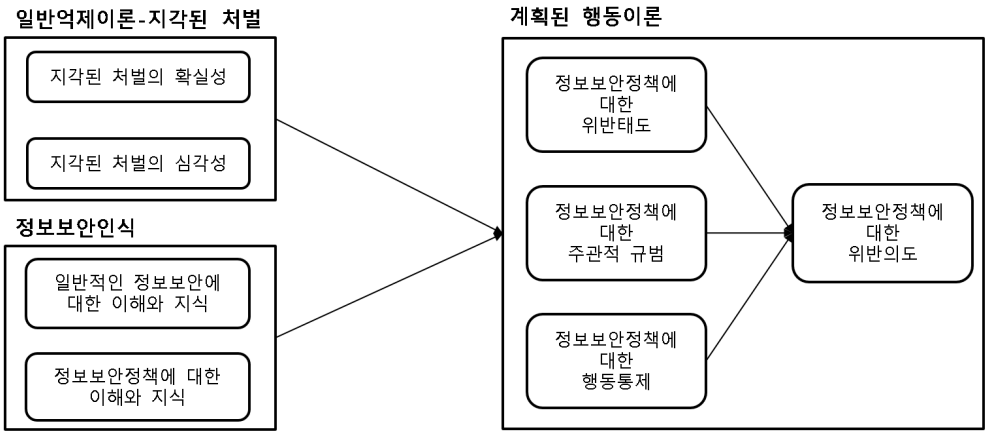
Ⅲ. 연구모형 및 가설

3.1 연구모형

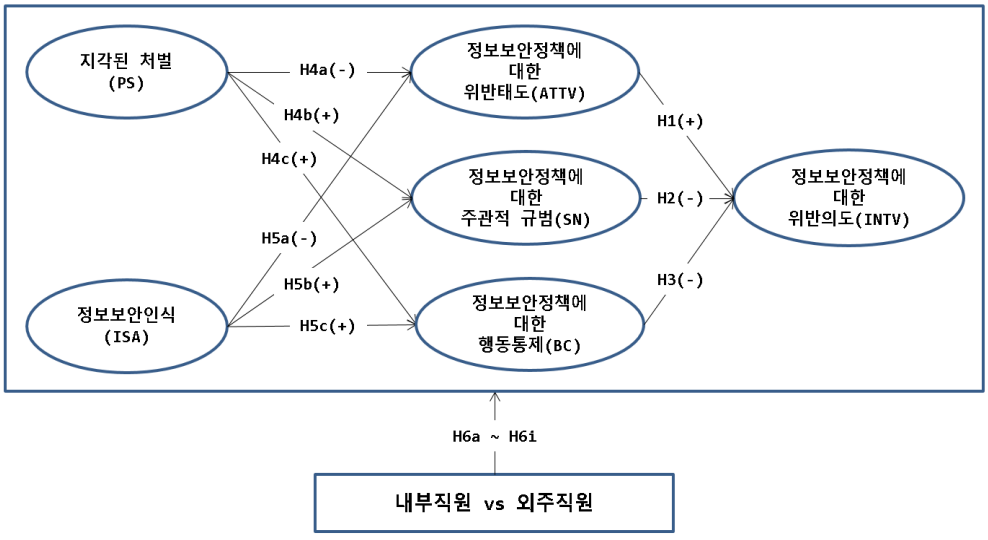
정보보안정책의 위반에 영향을 주는 요인을 분석하기 위해 일반억제이론, 정보보안인식 및 계획된 행동이론을 기초하여 연구모형을 설계하였으며, 조직원의 행동에 영향을 주는 요인을 분석하

〈표 4〉 정보보안정책 위반요인에 관한 선행연구

구 분	연구자	연구 주요 내용
위반요인 연구	이정하, 이상용(2015)	금융회사의 조직원을 대상으로 일반억제이론과 정보보안인식이 정보보안정책의 위반의도에 주는 영향을 분석
	임명성(2013b)	정보보안정책에 대한 위반요인으로 정보보안인식 교육, 도덕적 신념, 처벌에 대한 인지 및 도덕적 해방을 분석
	Siponen and Vance (2010)	중화기술, 공식적 처벌, 비공식적 처벌 및 치욕이 정보보안정책에 대한 위반의도에 미치는 영향을 분석
오용요인 연구	D'Arcy *et al.*(2009)	보안정책, 보안교육훈련, 모니터링이 처벌에 미치는 영향과 지각된 처벌의 심각성 및 지각된 처벌의 확실성이 정보시스템에 대한 오용의도에 미치는 영향을 분석
남용요인 연구	정우진 등(2012)	금융회사 내부직원의 기업정보보호활동(억제활동, 예방활동, 탐지활동, 교정활동)의 인지 수준이 불필요한 고객정보조회 태도, 주관적 규범 및 인지된 행동통제를 통해 불필요한 고객정보조회 행동의도에 주는 영향을 분석



〈그림 1〉 이론적 개념의 연구설계도



〈그림 2〉 연구모형

기 위하여 정보보안정책 연구에 많이 사용되는 계획된 행동이론의 변수를 사용하였다. 정보보안정책의 위반의도에 영향을 주는 요인으로 정보보안정책에 대한 위반태도, 주관적 규범 및 행동통제를 선행요인으로 선정하고, 이러한 선행요인에 영향을 주는 배경요인으로 지각된 처벌과 정보보안인식을 사용하였다. 본 연구의 관심사항은 H6에 관한 내용이며, H1~H5까지는 출발점이 되는 벤치마크 모형에 의해 설계하였다.

3.2 연구가설

3.2.1 계획된 행동이론(Theory of Planned Behavior)

정보보안정책의 위반 및 준수에 관한 연구에서 많은 연구자가 계획된 행동이론을 이론적 배경으로 사용하였고(Aurigemma, 2013; Bulgurcu *et al.*, 2010; Herath and Rao, 2009b; Kim *et al.*, 2014; Siponen *et al.*, 2014; Sommestad *et al.*, 2014; Yoon,

2011; 임명성, 2013a; 정우진 등, 2012), 연구의 결과에서 통계적으로 유의적인 결과로 나타났다. 조직원에게 지각된 정보보안정책의 내용이 정보보안정책에 대한 신념으로 나타나는 위반태도, 주관적 규범 및 행동통제가 정보보안정책의 위반의도에 영향을 주는 것으로 정보보안정책에 대한 위반 행동을 설명함으로써 전체 연구모형의 기본적인 가설로 설정하였다.

H1: 정보보안정책에 대한 위반태도는 정보보안정책에 대한 위반의도에 정(+)의 영향을 미칠 것이다.
H2: 정보보안정책에 대한 주관적 규범은 정보보안정책에 대한 위반의도에 부(-)의 영향을 미칠 것이다.
H3: 정보보안정책에 대한 행동통제는 정보보안정책에 대한 위반의도에 부(-)의 영향을 미칠 것이다.

3.2.2 일반억제이론(General Deterrence Theory)

일반억제이론은 지각된 처벌의 하부요인으로 처벌의 심각성, 처벌의 확실성 및 처벌의 신속성이 구성되어 있으나, 신속한 처벌이 정책을 위반하는 행위를 억제하는 것을 설명한 연구는 거의 없으며, 실증 분석을 통해 통계적 유의성을 증명하는 것은 어렵다(Nagin and Pogarsky, 2001). Straub(1990)는 처벌의 확실성과 처벌의 심각성이 컴퓨터 남용을 억제하는 효과가 있다고 주장하였고, Kankanhalli *et al.*(2003)은 처벌의 심각성이 조직의 정보시스템 보안 효과성에 미치는 영향은 통계적으로 유의하지 않게 나타났으며, D'Arcy *et al.*(2009)은 처벌의 심각성이 정보시스템의 오용의도를 억제하는 효과가 있고, 처벌의 확실성은 효과가 유의하지 않다고 설명하였다. 반면, Herath and Rao(2009a, 2009b)의 연구에서는 처벌의 확실성이 조직원의 정보보안정책에 대한 준수의도에 긍정적인 영향을 유의적으로 미치고, 처벌의 심각성은 부정적인 영향을 유의적으로 미친다고 설명하였다. 강욱, 전용태(2014)의 연구는 억제 효과를 특별 억제 효과와 일반 억제 효과로 나누어 설명하면서, 특별 억제 효과에 대한 처벌의 확실성과 처벌의 심각성이 정보보안정책에 대한 준수에 정(+)의 영향을 미친다고 설명하였고, 김상현, 송영미(2011)는 처벌의 강도와 보안위반의 적발도가 정보보안정책에 대한 준수의도에 정(+)의 영향을 미친다고 설명하였다. 특히, 일반억제이론에서 설명하는 하부요인을 묶어 하나의 변수로 설정한 연구에서는 처벌이 정보보안준수에 정(+)의 영향을 미친다고 설명하였고(Siponen *et al.*, 2010; 안중호 등, 2010), 다른 연구자들은 처벌이 정보보안정책에 대한 준수의도에 미치는 영향은 유의하지 않는다고 설명하였다(Guo *et al.*, 2011; Hu *et al.*, 2011; Pahnila *et al.*, 2007; Son, 2011; 강다연, 장명희, 2014). 또한, Vance and Siponen(2012)은 처벌에 대한 공식적인 처벌과 비공식적인 처벌로 구분하여 변수를 선정하여 분석을 수행하여 공식적인 처벌이 미치는 영향은 유의하지 않지만, 비공식적인 처벌은 유의하게 영향을 미치는 것으로 설명하였다. 이러한 선행연구들을 보면, 일반억제이론의 요인들이 정보보안정책의 준수 및 위반의도에 대해 미치는 영향을 다양하게 연구하였고 다양한 결론으로 나타났다.

본 연구에서는 처벌에 대한 변수를 하나의 변수로 선정하여 지각된 처벌이 정보보안정책에 대한 위반태도, 주관적 규범 및 행동통제에 영향을 주는 요인인 것을 탐색하기 위해 가설을 설정하였다.

H4a: 지각된 처벌은 정보보안정책에 대한 위반태도에 부(-)의 영향을 미칠 것이다.
H4b: 지각된 처벌은 정보보안정책에 대한 주관적 규범에 정(+)의 영향을 미칠 것이다.
H4c: 지각된 처벌은 정보보안정책에 대한 행동통제에 정(+)의 영향을 미칠 것이다.

3.2.3 정보보안인식(Information Security Awareness)

정보보안인식은 정보시스템에 대한 보안인식의 기본적인 개념을 설명한다(Siponen, 2000). 정보보안 관련 연구자들은 정보보안교육, 훈련 및 인식(Security Education, Training, Awareness, SETA) 프로그램이 정보보안정책에 영향을 주는 요인으로써 필요하다고 하였고(Whitman, 2004), SETA 프로그램은 다양하게 구성될 수 있으며 조직원에게 요구되는 정보보안정책을 준수하기 위한 절차를 포함하는 일반적인 지식을 제공하고(D'Arcy *et al*., 2009; Lee and Lee, 2002; Whitman *et al*., 2001), 조직 내에서 SETA 프로그램의 실행은 정보보안정책의 기반을 수립하는 것이며, 가장 기본적인 도구로서의 구실을 한다고 설명하였다(Peltier, 2005).

조직원의 직접적인 경험과 외부로부터 터득한 지식을 통해 생성되는 정보보안인식은 행동이론의 배경요인으로 논의될 수 있다(Ajzen *et al*., 2007). Bulgurcu *et al*.(2010)의 연구에 의하면 조직원이 정보보안정책에 대한 준수에 영향을 주는 선행요인으로 계획된 행동이론 기반으로 실증 분석을 하여 정보보안인식이 조직원의 신념에 영향을 주는 요인으로 설명하였고, Leach(2003)의 연구는 조직원이 업무에서 발생한 보안이슈에 대해 스스로 해결해야만 할 때가 있으며, 때로는 참고할만한 자료나 문서 없이 해결해야만 하는 상황이 발생할 수 있으므로 정보보안에 대한 일반적인 이해 및 지식이 정보보안정책을 준수하기 위한 행동에 중요한 요인이라고 설명하였다. 정보보안인식은 조직원의 정보보안정책에 대한 준수태도에 정(+)의 영향을 주고(Bulgurcu *et al*., 2009), 정보보안인식은 정보시스템에 대한 오용의도에 부(-)의 영향을 미치며, 조직원의 정보보안에 대한 이해는 조직 내에서 정보보호를 위한 활동이 소모성 비용이 아님을 설명하였다(D'Arcy and Hovav, 2007).

금융회사는 전자금융거래법 및 개인정보보호법을 준수하기 위해 정보보호 컴플라이언스 활동을 수행하고 있으며, 관리적 정보보호 활동 중 정보보안교육이 중요한 역할을 수행하고 있다. 정보보안에 대한 지식을 설명하는 조직원의 정보보안인식이 높을수록 정보보안정책에 대한 위반 의도는 낮아진다고 할 수 있으며, 정보보안인식을 일반적인 정보보안 상식과 정보보안정책에 대한 지식으로 정의하고 하나의 통합된 변수로 선정하여 정보보안정책에 대한 위반태도, 주관적 규범 및 행동통제에 영향을 미치는 요인으로 가설을 설정하였다.

H5a: 정보보안인식은 정보보안정책에 대한 위반태도에 부(-)의 영향을 미칠 것이다.
H5b: 정보보안인식은 정보보안정책에 대한 주관적 규범에 정(+)의 영향을 미칠 것이다.
H5c: 정보보안인식은 정보보안정책에 대한 행동통제에 정(+)의 영향을 미칠 것이다.

3.3.4 내부직원과 외주직원 간의 차이

내부자 위협은 정당한 권한을 가진 사용자가 보안사고를 발생시킬 수 있는 위험이 존재하고 있으며, 내부직원과 외주직원의 특징에 의해 두 그룹 간의 보안인식 차이가 발생할 것이다. 본 연구에서 중점적으로 탐구하고자 하는 가설로써, 내부자 위협관점에서 내부직원과 외주직원으로 모두 위협 요인을 포함하고 있으며, 조직 내에서 내부직원과 외주직원의 가지는 특징으로 인하여 정보보안정책에 대한 위반태도, 주관적 규범 및 행동통제를 매개하는 선행요인이나 종속요인에 대해 차이가 있을 것이다. 두 그룹 간의 특징으로 인해 나타나는 차이를 탐색하고자 아래와 같이 가설을 설정하여 통계 분석을 시행하였다.

H6a: 내부직원과 외주직원 그룹의 특징은 정보보안정책에 대한 위반태도와 정보보안정책에 대한 위반의도 간에 조절적인 영향을 미칠 것이다.
H6b: 내부직원과 외주직원 그룹의 특징은 정보보안정책에 대한 주관적 규범과 정보

보안정책에 대한 위반의도 간에 조절적인 영향을 미칠 것이다.

H6c: 내부직원과 외주직원 그룹의 특징은 정보보안정책에 대한 행동통제와 정보보안정책에 대한 위반의도 간에 조절적인 영향을 미칠 것이다.

H6d: 내부직원과 외주직원 그룹의 특징은 지각된 처벌과 정보보안정책에 대한 위반태도 간에 조절적인 영향을 미칠 것이다.

H6e: 내부직원과 외주직원 그룹의 특징은 지각된 처벌과 정보보안정책에 대한 주관적 규범 간에 조절적인 영향을 미칠 것이다.

H6f: 내부직원과 외주직원 그룹의 특징은 지각된 처벌과 정보보안정책에 대한 행동통제 간에 조절적인 영향을 미칠 것이다.

H6g: 내부직원과 외주직원 그룹의 특징은 정보보안인식과 정보보안정책에 대한 위반태도 간에 조절적인 영향을 미칠 것이다.

H6h: 내부직원과 외주직원 그룹의 특징은 정보보안인식과 정보보안정책에 대한 주관적 규범 간에 조절적인 영향을 미칠 것이다.

H6i: 내부직원과 외주직원 그룹의 특징은 정보보안인식과 정보보안정책에 대한 행동통제 간에 조절적인 영향을 미칠 것이다.

〈표 5〉 변수의 조작적 정의

변수	조작적 정의	측정항목	관련 연구
지각된 처벌 (PS)	정보보안정책 위반에 대하여 심각하고 확실한 처벌이 있다고 지각하는 정도	① 내가 회사의 정보보안정책을 위반한다면 반드시 처벌이 있을 것이다. ② 상사가 나의 정책위반 사실을 안다면, 나를 공식적으로 처벌할 것이다. ③ 동료나 상사가 정보보안정책을 위반한다면 반드시 처벌이 있을 것이다. ④ 내가 정보보안정책을 위반할 경우, 나는 동료들로부터 신뢰를 잃을 것이다. ⑤ 내가 정보보안정책을 위반할 경우, 나의 진급에 부정적인 영향을 줄 것이다. ⑥ 내가 정보보안정책을 위반할 경우, 나는 상사의 신뢰를 잃을 것이다.	Nagin and Paternoster(1993), Paternoster and Simpson(1996), Siponen and Vance (2010)
정보보안인식 (ISA)	정보보안정책과 일반적인 정보보안에 대한 인식된 이해와 지식의 정도	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. ④ 나는 회사의 정보보안정책을 알고 있다. ⑤ 나는 회사의 정보보안정책에 대한 나의 책임을 알고 있다. ⑥ 나는 회사의 정보보안정책을 이해하고 있다.	Bulgurcu *et al.*(2010)
정보보안정책에 대한 위반태도 (ATTV)	정보보안정책 위반 시나리오에 대해 위반태도의 필요성, 유용성 및 혜택의 인식	① 이 대리의 태도는 이 대리에게 필요하다. ② 이 대리의 태도는 이 대리에게 유용하다. ③ 이 대리의 태도는 이 대리에게 혜택을 가져다준다.	Ajzen(1991), Bulgurcu *et al.* (2010)
정보보안정책에 대한 주관적 규범 (SN)	자신의 동료, 상사나 경영진이 자신에 대해 생각하는 정보보안정책의 준수에 대한 인식	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 행동통제 (BC)	정보보안정책 준수를 위해 필요한 기술, 지식, 역량에 대해 인식된 행동통제의 정도	① 나는 정보보안정책 준수에 필요한 기술을 가지고 있다. ② 나는 정보보안정책 준수에 필요한 지식을 가지고 있다. ③ 나는 정보보안정책 준수에 필요한 역량을 가지고 있다.	Bulgurcu *et al.*(2010)
정보보안정책에 대한 위반의도 (INTV)	정보보안정책 위반 시나리오에 대한 자신의 위반의도에 대한 인식	① 내가 이 대리와 비슷한 상황에 처해진다면, 나도 같은 행동을 할 것이다.	Paternoster and Simpson(1996), Siponen *et al.*(2010), Siponen and Vance (2010)

Ⅳ. 연구방법

4.1 변수의 조작적 정의와 측정항목

본 연구에 사용한 설문은 7점 척도를 이용하였으며, 전혀 그렇지 않다(1)는 것에서 매우 그렇다(7) 혹은 전혀 동의하지 않는다(1)에서 매우 동의한다(7)로 산정하였다.

독립변수인 지각된 처벌(PS)에 대한 변수는 Nagin and Paternoster(1993)와 Paternoster and Simpson(1996)의 연구를 응용하여 사용한 Siponen and Vance (2010)의 12개 설문에서 6개의 설문을 선택하여 사용하였고, 정보보안인식(ISA)은 Bulgurcu *et al.*(2010)의 연구에서 사용한 설문에서 6개는 가져와 사용하였다.

매개변수인 정보보안정책에 대한 위반태도(ATTV)와 정보보안정책의 행동통제(BC)는 Ajzen(1991)의 연구에 기초하여 Bulgurcu *et al.*(2010)이 정의한 설문항목을 가져와 각각 3개의 항목으로 측정하였으며, 정보보안정책에 대한 주관적 규범(SN)은 Ajzen(1991)의 연구에 기초하여 Bulgurcu *et al.* (2010)이 정의한 설문항목과 Siponen *et al.*(2010)이 정의한 설문항목에서 가져와 3개의 설문항목을 정의하여 사용하였다.

종속변수인 정보보안정책에 대한 위반 의도는 Paternoster and Simpson(1996)의 연구에 기초하여 Siponen and Vance(2010)가 사용한 설문항목을 가져와 사용하였다.

4.2 자료수집 및 표본의 특징

본 연구의 설문조사는 은행과 보험회사의 조직원을 대상으로 설문지와 온라인 설문을 시행하였으며, 설문지 387부를 배포하여 367부(회수율 94.8%)를 거둬들이고 온라인 설문 도구는 79부를 거두었다. 전체 446개의 자료 중 83개의 불성실치를 제외하고 최종으로 363개의 자료를 사용하여 연구가설을 분석하고 검증하였다.

〈표 6〉 표본의 인구통계학적 특징

구 분		빈도	비율(%)
성별	남자	225	62.0
	여자	138	38.0
나이	20~29세	31	8.5
	30~39세	172	47.4
	40~49세	135	37.2
	50~59세	25	6.9
학력	고등학교 졸업	33	9.1
	대학교 졸업	287	79.1
	대학원 졸업 이상	43	11.8
경력	1년 미만	17	4.7
	1년~3년 미만	33	9.1
	3년~5년 미만	35	9.6
	5년~10년 미만	85	23.4
	10년~15년 미만	89	24.5
	15년~20년 미만	53	14.6
	20년 이상	51	14.0
조직	은행	107	29.5
	보험	256	70.5
직원 그룹	내부직원	246	67.8
	외주직원	117	32.2

수집된 자료에 대한 표본의 특징은 <표 6>과 같이 나타났다. 남녀의 비율은 62%, 38%로 남자의 비율이 높게 나타났으며, 나이는 30대가 47.4%로 가장 높게 나타났고 다음으로 40대가 37.2%로 나타났다. 학력은 대학교 졸업이 79.1%로 높게 나타났으며, 경력은 10~15년이 24.5%로 높고 다음으로 5~10년이 23.4%로 나타났다. 은행과 보험의 비율은 29.5%, 70.5%로 보험회사의 조직원이 높게 나타났으며, 내부직원과 외주직원의 비율은 67.8%, 32.3%로 나타났다.

본 연구는 내부직원과 외주직원의 특징이 정보보안정책에 대한 조직원의 행동에 주는 영향에 차이가 있는지는 확인하는 것으로 각 그룹에 대한 표본의 특징을 <표 7>과 같이 살펴보았다. 내부직원과 외주직원에 대한 표본의 특징에서 차이를 보면, 외주직원의 학력은 고등학교 졸업이

〈표 7〉 그룹별 인구통계학적 특징

구 분		내부직원 (N = 246)		외주직원 (N = 117)	
		빈도	비율 (%)	빈도	비율 (%)
성별	남자	167	67.9	58	49.6
	여자	79	32.1	59	50.4
나이	21~29세	21	8.5	10	8.5
	30~39세	109	44.3	63	53.8
	40~49세	92	37.4	43	36.8
	50~59세	24	9.8	1	0.9
학력	고등학교 졸업	10	4.1	23	19.7
	대학교 졸업	198	80.5	89	76.1
	대학원 졸업 이상	38	15.4	5	4.3
경력	1년 미만	11	4.5	6	5.1
	1년~3년 미만	11	4.5	22	18.8
	3년~5년 미만	15	6.1	20	17.1
	5년~10년 미만	47	19.1	38	32.5
	10년~15년 미만	71	28.9	18	15.4
	15년~20년 미만	42	17.1	11	9.4
	20년 이상	49	19.9	2	1.7
조직	은행	90	36.6	17	14.5
	보험	156	63.4	100	85.5

19.7%로 내부직원 4.1%에 비해 높게 나타났으며, 외주직원의 경력은 5년 미만이 41%로 내부직원 15.1%에 비해 높게 나타났다.

4.3 자료 분석 도구 및 분석 방법

본 연구에서 사용된 설문자료 분석 도구는 SPSS 22와 SmartPLS 2.0이며, 표본의 빈도분석, 측정모형의 신뢰성과 타당도를 검증하기 위해 탐색적 요인 분석, 신뢰성 분석, 수렴 타당도 및 판별 타당도 분석을 하였다. 구조모형의 가설을 검증하기 위해 예측적합도, 구조방정식 경로 분석, 다중집단 분석을 사용하였으며 인과관계의 가설을 검증하기 위해 부트스트래핑(Bootstrapping)을 이용하였다.

Ⅴ. 자료 분석 및 가설 검정

5.1 측정모형의 분석

5.1.1 신뢰성 분석 및 요인 분석

연구모형을 검증하기 위해 SPSS 22를 이용하여 탐색적 요인 분석을 시행하였다. 요인 분석을 수행하기 전에 의미가 있는지 확인하기 위해 변수 간의 상관계수 행렬을 도출하였고, 단위행렬에 따르는 행렬인지 여부를 검증하기 위해 바틀렛(Bartlett) 검증과 변수 간의 편상관계수가 얼마나 작은지 확인하기 위해 KMO(Kaiser-Meyer-Olkin) 검증을 시행하였다. 바틀렛 검증 결과, 유의수준 0.000 (Approx. Chi-Square: 7639.229, *df*: 210)으로 0.05보다 작아 유의미하게 나타났으며, KMO 표본 적합도는 0.894로 0.7보다 높게 나타나 요인 분석을 하기에 적절하게 나타났다. 요인 분석은 주성분 구성요소 추출방법으로 고유 값이 1 이상인 것을 기준으로 베리맥스 회전방법을 이용하였다. 추출된 요인의 전체 설명력은 81.1%로 나타났으며, 본 연구의 설명력은 유의미한 수준으로 나타났다(이학식, 임지훈, 2013). 탐색적 요인 분석의 결과, 독립변수들의 측정항목의 요인 적재량이 0.641 이상으로 나타났으며, 각 측정항목의 요인 적재량이 0.6 이상이고 교차요인 적재량보다 크다면 측정항목의 타당성은 있다(Chin *et al*., 2003)고 하므로, 본 연구의 측정항목은 타당하다고 할 수 있다.

연구가설을 검증하기 위해 사용할 설문조사 결과의 신뢰성 검증을 위해 SPSS 22를 이용하여 내적 일관성을 확인하는 신뢰성 분석을 하였다. 신뢰성 분석의 결과, 모든 요인의 크롬바흐 알파 값(Cronbach's α)은 0.909 이상으로 나타났으며, 신뢰성 계수 값은 0.9 이상이면 신뢰성이 우수하다(Chin *et al*., 2003). 따라서 본 설문조사의 결과는 신뢰성이 있다고 나타났다.

5.1.2 타당도 분석

신뢰성 분석과 탐색적 요인 분석을 통해 내적

〈표 8〉 탐색적 요인 분석

변수	항목	공통성	요인 1	요인 2	요인 3	요인 4	요인 5
지각된 처벌 (PS)	PS3	0.853	0.895	0.131	0.055	-0.158	0.081
	PS2	0.841	0.893	0.127	0.050	-0.129	0.095
	PS1	0.766	0.835	0.169	-0.044	-0.137	0.140
	PS4	0.735	0.788	0.121	0.134	-0.212	0.191
	PS5	0.709	0.759	0.143	0.079	-0.096	0.313
	PS6	0.726	0.694	0.173	0.110	-0.229	0.387
정보보안인식 (ISA)	ISA3	0.796	0.113	0.813	0.107	-0.086	0.320
	ISA2	0.721	0.100	0.803	0.040	-0.082	0.239
	ISA5	0.801	0.196	0.799	0.324	-0.124	0.061
	ISA6	0.782	0.167	0.781	0.367	-0.075	0.059
	ISA4	0.777	0.156	0.778	0.372	-0.096	0.022
	ISA1	0.596	0.147	0.731	0.090	-0.020	0.178
정보보안정책에 대한 행동통제 (BC)	BC3	0.897	0.061	0.233	0.898	-0.111	0.142
	BC1	0.862	0.080	0.239	0.883	-0.110	0.087
	BC2	0.904	0.053	0.318	0.881	-0.126	0.088
정보보안정책에 대한 위반태도 (ATTV)	ATTV2	0.948	-0.216	-0.107	-0.123	0.931	-0.091
	ATTV1	0.922	-0.195	-0.128	-0.141	0.917	-0.085
	ATTV3	0.897	-0.251	-0.064	-0.082	0.900	-0.113
정보보안정책에 대한 주관적 규범 (SN)	SN2	0.855	0.335	0.232	0.084	-0.077	0.822
	SN3	0.863	0.373	0.309	0.128	-0.171	0.763
	SN1	0.773	0.377	0.364	0.259	-0.141	0.641
회전 제곱합 로딩	고유 값		4.664	4.348	2.937	2.824	2.250
	분산 설명력(%)		22.210	20.703	13.988	13.449	10.715
	누적분산(%)						81.064

일관성과 타당도를 검증한 후, 관측변수들의 일치성 정도를 확인하기 위해 수렴 타당도 분석을 하였다. 수렴 타당도를 확인하기 위해 요인 적재량(표준화 경로계수, β), 복합신뢰도(Composite Reliability, CR), 평균분산추출(Average Variance Extract, AVE) 값을 사용하여 분석하였다. <표 9>와 같이 요인 적재량은 0.741~0.973, 복합신뢰도는 0.937~0.972, 평균분산추출은 0.713~1.000으로 나타났다. 요인 적재량이 0.7 이상이고 복합신뢰도는 0.7 이상, 평균분산추출은 0.5 이상이면 수렴 타당도가 있다(Hair *et al*., 2006). 따라서 본 연구의 측정항목과 변수들은 수렴 타당도가 있다고 나타났다.

판별 타당도는 두 가지 방법을 통해 검증하였다. SmartPLS 2.0을 이용하여 판별 타당도 분석을 수행한 결과, <표 10>에서와 같이 평균분산추출과 상관계수를 비교한 분석에서는 평균분산추출의 제곱근 값 중 가장 작은 값인 0.845가 상관계수 중 가장 높은 값인 0.804보다 크게 나타났으며, 평균분산추출의 제곱근 값이 상관계수보다 크고 0.7 이상이면 판별 타당도가 있다(Chin, 1998; Fornell and Larcker, 1981). 교차요인분석에서는 <표 11>과 같이 잠재변수의 요인 적재량이 다른 요인의 적재량보다 적어도 0.10보다 크기에 판별 타당도가 있다(Gefen and Straub, 2005)고 할 수 있다. 따라서 본 연구의 변수들은 판별 타당도가 있다고 나타났다.

〈표 9〉 신뢰성 분석과 수렴 타당도 검정

변수	항목	β	SE	t value	Cronbach's α	CR	AVE
지각된 처벌 (PS)	PS1	0.849	0.022	39.440***	0.934	0.948	0.752
	PS2	0.882	0.016	56.458***			
	PS3	0.888	0.017	52.771***			
	PS4	0.868	0.016	53.997***			
	PS5	0.853	0.019	44.419***			
	PS6	0.858	0.016	53.449***			
정보보안인식 (ISA)	ISA1	0.741	0.036	20.384***	0.919	0.937	0.713
	ISA2	0.804	0.026	30.937***			
	ISA3	0.857	0.019	44.424***			
	ISA4	0.875	0.017	53.158***			
	ISA5	0.897	0.014	63.324***			
	ISA6	0.885	0.016	55.586***			
정보보안정책에 대한 위반태도 (ATTV)	ATTV1	0.961	0.006	154.005***	0.957	0.972	0.921
	ATTV2	0.973	0.004	236.007***			
	ATTV3	0.945	0.009	104.737***			
정보보안정책에 대한 주관적 규범 (SN)	SN1	0.913	0.012	76.173***	0.909	0.942	0.845
	SN2	0.901	0.017	52.350***			
	SN3	0.944	0.007	131.961***			
정보보안정책에 대한 행동통제 (BC)	BC1	0.941	0.010	90.470***	0.946	0.965	0.903
	BC2	0.960	0.007	145.469***			
	BC3	0.950	0.009	103.432***			

주) Bootstrapping samples: 5000, β: 표준화 경로계수, SE: 표준오차, CR: 복합신뢰도, AVE: 평균분산추출, $^{***}p < 0.001$.

〈표 10〉 판별 타당도

	변수	평균	표준편차	1	2	3	4	5	6
1	지각된 처벌(PS)	5.462	1.510	**0.867**					
2	정보보안인식(ISA)	6.195	1.043	0.396	**0.845**				
3	정보보안정책에 대한 위반태도(ATTV)	3.191	1.997	-0.443	-0.280	**0.960**			
4	정보보안정책에 대한 주관적 규범(SN)	6.010	1.110	0.641	0.575	-0.365	**0.919**		
5	정보보안정책에 대한 행동통제(BC)	5.217	1.452	0.236	0.547	-0.286	0.371	**0.950**	
6	정보보안정책에 대한 위반의도(INTV)	3.850	2.205	-0.397	0.236	0.804	-0.378	-0.309	**1.000**

주) 상관계수의 대각선 굵게 표시된 값은 AVE의 제곱근 값임.

〈표 11〉 교차 요인 분석

변수	항목	평균	표준편차	요인 1	요인 2	요인 3	요인 4	요인 5
지각된 처벌 (PS)	PS1	5.70	1.384	0.850	0.321	-0.351	0.115	0.515
	PS2	5.36	1.456	0.883	0.313	-0.361	0.171	0.529
	PS3	5.29	1.500	0.888	0.319	-0.388	0.179	0.525
	PS4	5.14	1.664	0.868	0.341	-0.422	0.253	0.536
	PS5	5.73	1.487	0.853	0.351	-0.326	0.216	0.569
	PS6	5.56	1.552	0.858	0.400	-0.439	0.268	0.638
정보보안인식 (ISA)	ISA1	6.22	1.148	0.328	0.740	-0.164	0.364	0.412
	ISA2	6.42	0.880	0.319	0.805	-0.213	0.353	0.464
	ISA3	6.37	0.903	0.357	0.857	-0.237	0.416	0.554
	ISA4	6.02	1.122	0.312	0.875	-0.255	0.541	0.470
	ISA5	6.10	1.053	0.367	0.897	-0.288	0.523	0.507
	ISA6	6.04	1.118	0.329	0.884	-0.241	0.539	0.498
정보보안정책에 대한 위반태도 (ATTV)	ATTV1	3.25	2.024	-0.408	-0.293	0.961	-0.301	-0.344
	ATTV2	3.19	1.987	-0.425	-0.277	0.973	-0.285	-0.351
	ATTV3	3.14	1.970	-0.444	-0.234	0.945	-0.235	-0.356
정보보안정책에 대한 주관적 규범 (SN)	SN1	5.75	1.210	0.230	0.492	-0.265	0.941	0.330
	SN2	6.21	1.095	0.221	0.563	-0.282	0.960	0.353
	SN3	6.07	1.017	0.223	0.501	-0.268	0.950	0.375
정보보안정책에 대한 행동통제 (BC)	BC1	5.05	1.563	0.596	0.592	-0.354	0.424	0.913
	BC2	5.34	1.361	0.557	0.445	-0.272	0.261	0.901
	BC3	5.26	1.424	0.610	0.533	-0.370	0.323	0.944

5.2 구조모형의 분석 및 가설 검정

5.2.1 구조모형 분석

측정모형에 대한 신뢰성과 타당성 검증 후, 본 연구에서 제안하는 잠재변수들 사이의 영향 관계를 검증하기 위해 SmartPLS 2.0을 사용한 구조방정식 분석(Structural Equation Modeling, SEM)을 시행하였다. PLS-SEM 분석은 종속변수의 근삿값과 모형에서 예측된 값 사이의 차이에 초점을 맞추어 분석하는 방법이다(Hair *et al*., 2012). PLS-SEM 분석을 사용한 이유는 수집된 데이터에 적합한 연구모형의 탐색뿐 아니라 변수들 사이의 인과관계를 알아보기 위해서이다.

PLS-SEM 분석은 이를 통해 두 가지 결과의 도출을 확인할 수 있다. 첫째, 잠재변수 간의 인과관계를 나타내는 경로계수(β)를 확인할 수 있다. 이는 두 잠재변수 간의 인과관계를 나타낸다(Wixom and Watson, 2001). 둘째, 내생변수들의 설명력을 나타내는 R^2값을 확인할 수 있다. R^2값은 연구모형 내 독립변수들에 의해 설명되는 종속변수의 설명비율을 나타낸다(Hair *et al*., 2012).

SmartPLS 2.0을 이용하여 구조모형의 분석을 하기 위해 연구모형의 적합도를 검증하였다. 본 연구에서 설계한 연구모형은 매개변수가 있는 구조모형으로 매개변수의 효과를 검증하기 위해 완전모형과 감소모형에 대한 종속변수의 설명력(R^2)을 비교하여 분석하였다. 완전모형과 감소모형의 비교를 위해 f^2 값을 사용하였으며 1.389로 나타났다.

f^2의 값을 이용하여 효과 크기(0.36 이상: 상, 0.15~0.35: 중, 0.15 이하: 하)를 분석하면 매우 높은 것으로 나타났다(Chin, 1998; Cohen, 2013; Henseler *et al.*, 2009).

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

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

〈표 12〉 감소모형과 완전모형의 비교

감소모형	완전모형	f^2	효과 크기
0.183	0.658	1.389	상

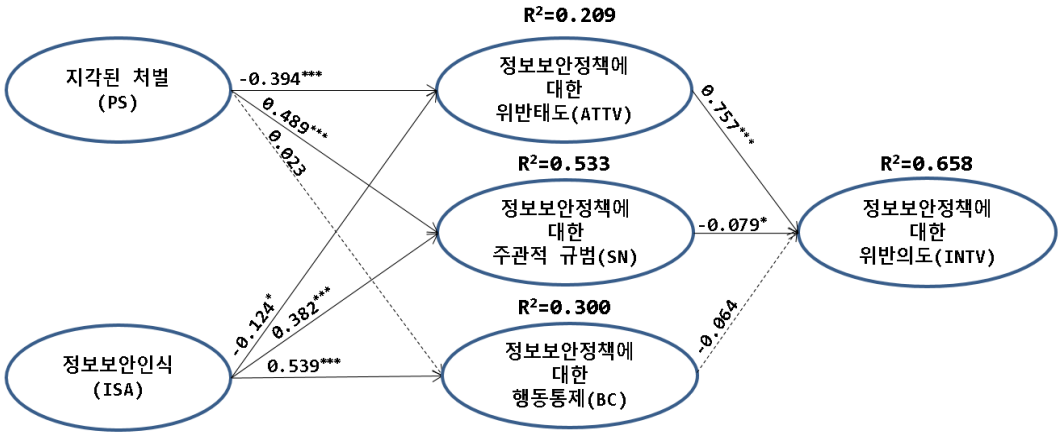
〈표 13〉 적합도 검증

변수	설명력 (R^2)	공통성 (Communality)	중복성 (Redundancy)
PS		0.752	
ISA		0.713	
ATTV	0.209	0.921	0.050
SN	0.533	0.845	0.244
BC	0.300	0.903	0.269
INTV	0.658	1.000	0.644
평균	0.425	0.856	0.302

PLS-SEM 분석의 예측 적합도 검증은 내생변수의 설명력을 나타내는 R^2의 평균값과 모든 잠재변수 공통성(Communality)의 평균값을 곱한 값의 제곱근인 적합도지수(Goodness of Fit, GoF)을 이용하여 분석하였으며, 0.603(0.36 이상: 상, 0.25~0.35: 중, 0.10~0.25: 하)으로 적합도 지수가 높게 나타났다(Chin, 1998; Hair *et al.*, 2012; Hulland, 1999; Tenenhaus *et al.*, 2005). 잠재변수들의 공통성 값은 0.713 이상으로 나타났으며, 공통성 값이 0.5 이상이면 기준 이상이라고 할 수 있다(Chin, 1998; Hulland, 1999; Tenenhaus *et al.*, 2005). 모든 내생변수들의 중복성(Redundancy) 값은 0.05 이상으로 나타났으며, 중복성 값은 0 이상이면 기준 이상이라고 할 수 있다(Geisser, 1975; Stone, 1974; Tenenhaus *et al.*, 2004; Tenenhaus *et al.*, 2005)

5.2.2 가설 검증

SmartPLS 2.0 Bootstrapping 분석을 이용하여 가설검증을 한 결과, <표 14>와 같이 9개의 가설 중 7개(H1, H2, H4a, H4b, H5a, H5b, H5c)의 가설은 채택되었으며 2개(H3, H4c)의 가설은 기각되었다. 기각된 가설은 정보보안정책에 대한 행동통제(BC)가 정보보안정책에 대한 위반의도(INTV)에 통계적으로 유의미한 영향이 없게 나타났으며,



$^{*}p < 0.05$, $^{**}p < 0.01$, $^{***}p < 0.001$.

〈그림 3〉 경로 분석 결과

〈표 14〉 가설 검증

가설	경로	β	SE	t value	채택여부
H1	정보보안정책에 대한 위반태도(ATTV) → 정보보안정책에 대한 위반의도(INTV)	0.757	0.031	24.495***	채택
H2	정보보안정책에 대한 주관적 규범(SN) → 정보보안정책에 대한 위반의도(INTV)	-0.079	0.033	2.354*	채택
H3	정보보안정책에 대한 행동통제(BC) → 정보보안정책에 대한 위반의도(INTV)	-0.064	0.036	1.768	기각
H4a	지각된 처벌(PS) → 정보보안정책에 대한 위반태도(ATTV)	-0.394	0.057	6.980***	채택
H4b	지각된 처벌(PS) → 정보보안정책에 대한 주관적 규범(ATTV)	0.489	0.049	10.014***	채택
H4c	지각된 처벌(PS) → 정보보안정책에 대한 행동통제(BC)	0.023	0.052	0.436	기각
H5a	정보보안인식(ISA) → 정보보안정책에 대한 위반태도(ATTV)	-0.124	0.049	2.504*	채택
H5b	정보보안인식(ISA) → 정보보안정책에 대한 주관적 규범(SN)	0.382	0.057	6.673***	채택
H5c	정보보안인식(ISA) → 정보보안정책에 대한 행동통제(BC)	0.539	0.046	11.633***	채택

주) Bootstrapping samples: 5000, β: 표준화 경로계수, SE: 표준오차, $^{*}p < 0.05$, $^{**}p < 0.01$, $^{***}p < 0.001$.

지각된 처벌(PS)이 정보보안정책에 대한 행동통제(BC)에 주는 영향이 통계적으로 지지가 되지 않았다.

지지가 된 가설인 H1과 H2는 정보보안정책에 대한 위반태도(ATTV)와 정보보안정책에 대한 주관적 규범(SN)이 정보보안정책에 대한 위반의도(INTV)에 영향을 주는 것으로 나타났다. 이는 계획된 행동이론(TPB)과 합리적 행동이론(TRA)에서 행동에 대한 의도에 영향을 주는 요인들로 나타나는 태도와 주관적 규범이 정보보안정책에 대한 위반의도를 설명할 때도 적용된다는 것을 설명할 수 있다.

또한, 지지가 된 가설 중 H4a, H4b, H5a, H5b는 지각된 처벌(PS)과 정보보안인식(ISA)이 각각 정보보안정책에 대한 위반태도(ATTV)와 정보보안정책에 대한 주관적 규범(SN)에 영향을 주는 것으로 나타났다. 이는 선행연구에서 많은 연구자가 주장하는 바와 마찬가지로 지각된 처벌(PS)과 정보보안인식(ISA)은 정보보안정책에 대한 위반태도(ATTV)에 부(-)의 영향을 미치는 요인으로써 조직원의 정보보안정책에 대한 위반태도를 억제하는 효과가 있다는 것이며, 지각된 처벌(PS)과 정보보안인식(ISA)이 정보보안정책에 대한 주관적 규범(SN)에 정(+)의 영향을 미치는 것은 조직원의 정보보안정책에 대한 주관적 규범에 영향을 미치는 신념과 같은 선행요인으로 효과를 준다는 것을 나타낸다.

마지막으로 지지가 된 가설인 H5c는 지각된 처벌(PS)이 정보보안정책에 대한 행동통제(BC)에는 영향을 미치지 않으나, 정보보안인식(ISA)이 정보보안정책에 대한 행동통제(BC)에 정(+)의 영향을 유의적으로 미치는 것은 지각된 처벌이 조직원 스스로 정보보안정책에 대해 통제할 수 있는 기술이 있고 이러한 역량이 올바르게 동작한다는 믿음에 영향을 미치지 않지만, 정보보안에 대한 이해와 지식을 나타내는 정보보안인식은 이러한 행동통제에 정(+)의 영향을 미친다고 설명할 수 있다. 즉 지각된 처벌이 조직원이 정보보안정책

을 준수하는 데 필요한 자신의 행동을 스스로 통제할 수 있는 자기효능감에 영향을 미치지 않지만, 정보보안정책에 대한 이해와 지식을 나타내는 정보보안인식은 이러한 자기효능감에 영향을 미친다는 것이다.

5.2.3 다중 집단 분석(Multiple Group Analysis)

SmartPLS 2.0을 이용하여 내부직원과 외주직원 그룹을 나누어 PLS-SEM분석을 수행하였고, 그룹 간의 경로 분석 결과를 기준으로 다중 집단 분석을 위해 차이 분석 식(Keil *et al*., 2013; Keil *et al*., 2000)을 사용하였다.

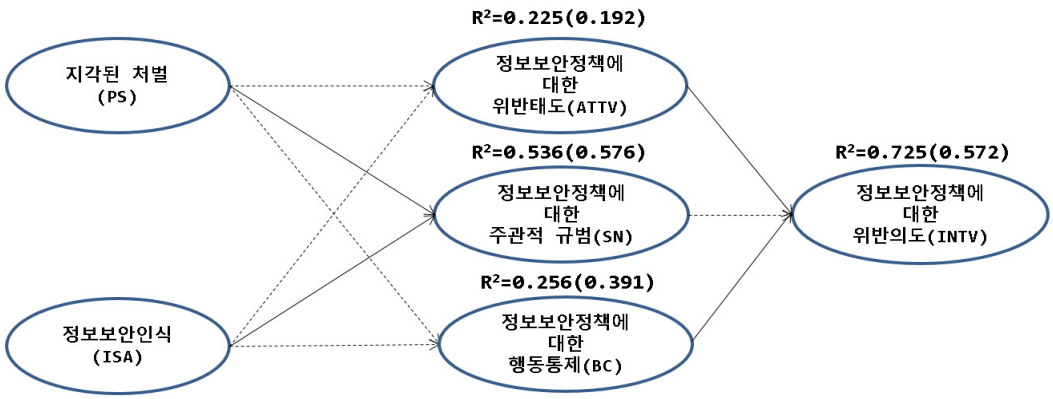
다중 집단 분석을 수행한 결과, <표 15>와 같이 9개의 가설 중 4개(H6a, H6c, H6e, H6h)의 가설은 채택되었고 5개(H6b, H6d, H6f, H6g, H6i)의 가설은 기각되었다.

$$t = \frac{\beta_{sample_1} - \beta_{sample_2}}{\sqrt{\frac{(m-1)^2}{(m+n-2)} \times SE^2_{sample_1} + \frac{(n-1)^2}{(m+n-2)} \times SE^2_{sample_2}} \times \sqrt{\frac{1}{m} + \frac{1}{n}}}$$

m: *sample 1*의 개수, n: *sample 2*의 개수,
β: 표준화 경로계수, *SE*: 표준오차

가설검증에서 나타난 결과는 내부직원과 외주직원 간의 특징으로 인해 정보보안정책에 대한 위반의도(INTV)에 미치는 매개변수와 독립변수의 영향요인은 서로 차이가 있다는 것을 통계적으로 지지하는 것으로 나타났다. 구체적으로는 내부직원과 외주직원 간에는 정보보안정책에 대한 위반태도(ATTV)와 정보보안정책에 대한 행동통제(BC)가 정보보안정책에 대한 위반의도(INTV)에 주는 영향에 차이가 있다고 나타났으며, 지각된 처벌(PS)과 정보보안인식(ISA)이 정보보안정책에 대한 주관적 규범(SN)에 주는 영향에 차이가 있게 나타났다. <그림 4>는 채택된 가설과 기각된 가설에 대해 그림으로 정리한 것으로, 채택된 가설들은 실선으로 표기하였고 기각된 가설들은 점선으로 표기하였다.

지지가 된 가설인 H6a와 H6c는 정보보안정책에 대한 위반태도(ATTV)와 정보보안정책에 대한 행동통제(BC)가 정보보안정책에 대한 위반의도(INTV)에 주는 영향에 차이가 있는 것으로 나타났다. 두 그룹 모두 정보보안정책에 대한 위반태도(ATTV)가 정보보안정책에 대한 위반의도(INTV)에 미치는 영향에 대한 경로계수가 유의하게 나타나지만, 외주직원의 경로계수는 내부직원보다 작게 나타났다. 하지만 정보보안정책에 대한 행동통제(BC)가 정보보안정책에 대한 위반의도(INTV)에 미치는 영향을 나타내는 외주직원의 경로계수가 내부직원보다 크게 나타났다. 이는 외주직원에



주) 차이 분석 결과가 유의한 경로는 실선으로 표기, ( )안의 값은 외주직원에 대한 값임.

〈그림 4〉 다중 집단 분석 결과

〈표 15〉 다중 집단 분석 가설 검증

가설	경로	내부직원(N = 246)			외주직원(N = 117)			차이검증	
		β	SE	t value	β	SE	t value	t value	채택여부
H6a	ATTV → INTV	0.811	0.029	27.710***	0.625	0.073	8.577***	2.854**	채택
H6b	SN → INTV	-0.103	0.035	2.925**	0.026	0.074	0.338	1.799	기각
H6c	BC → INTV	0.016	0.036	0.461	-0.261	0.081	3.218**	3.648**	채택
H6d	PS → ATTV	-0.428	0.068	6.314***	-0.245	0.103	2.314*	1.519	기각
H6e	PS → SN	0.551	0.055	9.978***	0.316	0.077	4.048***	2.444*	채택
H6f	PS → BC	-0.044	0.061	0.746	0.111	0.103	1.126	1.375	기각
H6g	ISA → ATTV	-0.097	0.062	1.571	-0.269	0.092	2.960**	1.570	기각
H6h	ISA → SN	0.309	0.063	4.866***	0.558	0.084	6.689***	2.317*	채택
H6i	ISA → BC	0.523	0.053	9.881***	0.568	0.086	6.555***	0.461	기각

주) Bootstrapping samples: 5000, β: 표준화 경로계수, SE: 표준오차, $^{*}p < 0.05$, $^{**}p < 0.01$, $^{***}p < 0.001$.

대하여는 정보보안정책에 대한 위반태도(ATTV)가 정보보안정책에 대한 위반의도(INTV)에 영향을 미치지만, 정보보안정책에 대한 행동통제(BC)가 정보보안정책에 대한 위반의도(INTV)에 미치는 영향으로 인해 정보보안정책에 대한 위반태도(ATTV)가 정보보안정책에 대한 위반의도(INTV)에 주는 영향을 감소시킨 결과로 해석할 수 있다.

또한, 지지가 된 가설인 H6e에 의하면 외주직원은 내부직원과 달리 외주직원들이 가지는 지각된 처벌(PS)이 정보보안정책에 대한 주관적 규범(SN)에 미치는 경로계수가 유의하지만, 내부직원보다 작게 나타났다. 지각된 처벌은 사람의 경험으로 형성되는 것을 포함하고 있으며 외주직원은 주변에서 처벌을 받는 상황을 보는 경험이 내부직원보다 적고, 조직 내부의 규정에 대해 인지할 수 있는 경로가 없어 이러한 현상이 발생하는 것으로 여겨진다.

마지막으로 지지가 된 가설인 H6h는 정보보안인식(ISA)이 정보보안정책에 대한 주관적 규범(SN)에 미치는 영향을 나타내는 경로계수도 유의하게 나타나고 있으나, 내부직원보다 크게 나타났다. 이는 외주직원의 정보보안정책에 대한 주관적 규범(SN)을 형성하는 데 있어, 지각된 처벌(PS)보다는 정보보안을 위해 실질적인 지침이 되는 정보보안인식(ISA)이 더 큰 영향을 주는 것으로 해석할 수 있다. 정보보안인식은 일반적인 정보보안 이해와 정보보안정책에 대한 지식으로 구성되어 있어 외주직원을 관리하는 데 있어 외주직원에 대한 처벌의 확신성과 심각성을 강조하는 것보다는 정보보안인식을 강화하기 위해 정보보안정책에 대해 인식시키는 교육을 강조하고 일반적인 정보보안 이해도를 높이기 위한 교육프로그램의 개발을 수행하여야 더욱 효과적일 것이다.

정보보안정책에 대한 위반의도에 주는 영향에 대한 내부직원과 외주직원 간의 차이는 큰 의미가 있다. 외주직원은 내부직원과 달리 정보보안정책에 대한 행동통제(BC)가 정보보안정책에 대한 위반의도(INTV)에 유의한 영향을 미치는 것으로 나타났으며, 주관적 규범(SN)은 유의하게 나타나지 않았다. 이는 내부직원은 자신이 가지는 조직의 신념에 의해 정보보안정책에 대한 위반의도가 영향을 받고 자신이 정보보안정책에 대해 수행할 수 있는 능력이 있다고 믿는 신념은 영향이 유의하지 않지만, 외주직원은 이와 달리 자신이 정보보안정책을 지킬 수 있다는 외부인의 생각보다는 자신의 정보보안정책을 지킬 수 있다는 자신의 의지 및 신념에 의해 영향을 더 받는다는 것이다.

이를 외주직원관리를 위한 교육 프로그램에 적용하면, 외주직원에게는 정보보안정책을 지켜야 한다는 것을 강조하기보다는 외주직원들이 지

킬 수 있는 정보보안정책을 수립하고 이를 강조할 필요가 있다. 정보보안정책을 너무 엄격하여 지키기가 어렵게 수립하여 적용할 경우, 정보보안정책을 준수하지 않는 사례가 많이 발생하는 것으로 나타났다. 특히 외주직원에게는 권한을 허용하고 복잡한 정책으로 통제하기보다는 권한을 제한하고 쉽게 지킬 수 있는 정보보안정책을 적용하는 것이 더 효과적이라고 할 수 있다.

Ⅵ. 결 론

본 연구에서는 금융회사의 조직원을 대상으로 내부직원과 외주직원 간의 특징을 이해하고, 정보보안정책에 대한 위반의도에 영향을 주는 요인을 분석하기 위한 모형을 제시하였으며, 다중 집단 분석을 통해 내부직원과 외주직원 간의 차이를 분석하였다. 금융회사의 조직원을 대상으로 설문을 시행하고 실증 분석한 결과, 벤치마크 모형에 대한 9개 기본가설 중 7개의 가설이 통계적으로 유의하게 나타났으며, 두 그룹 간의 차이를 검증하기 위해 실시한 다중 집단 분석에서는 9개의 가설 중 4개의 가설이 통계적으로 유의하게 나타났다.

벤치마크 모형에서 설정된 가설 9개 중 지지가 되지 않은 가설 2개는 지각된 처벌(PS)이 정보보안정책에 대한 행동통제(BC)에 유의하지 않고, 정보보안정책에 대한 행동통제(BC)가 정보보안정책에 대한 위반의도(INTV)에 주는 영향이 유의하지 않는다는 것이다. 이는 Kim *et al.*(2014)과 임명성(2013a)의 연구에서 인지된 행동 통제와 자기 효능감이 정보보안정책 준수 의도에 주는 영향이 유의하게 나타나지 않은 것과 같은 결과로 해석하여 금융회사 조직원의 정보보안정책에 대한 위반의도에 영향을 주는 요인으로는 작동하지 않는 것으로 이해할 수 있다. 자기효능감은 인지된 행동통제와 같은 개념으로 사용되므로 행동통제로 인식하여 해석이 가능하다(Aurigemma, 2013). 금융회사 조직원의 정보보안정책에 대한 위반의도(INTV)는 정보보안정책에 대한 위반태도(ATTV)와 주관적 규범(SN)에 의해 영향을 받으며, 정보보안정책의 위반태도(ATTV)와 주관적 규범(SN)은 지각된 처벌(PS)과 정보보안인식(ISA)에 의해 영향을 받게 된다. 따라서 금융회사 조직원의 정보보안정책에 대한 위반의도를 감소시키기 위해서는 조직원에게 지각된 처벌과 정보보안인식을 강화하여야 할 것이다.

본 연구에서 중점적으로 탐색하고자 하는 것은 내부직원과 외주직원 간의 정보보안정책에 대한 위반의도(INTV)에 영향을 주는 요인 간의 차이를 확인하는 것이다. 다중 집단 분석의 결과에 의하면, 지각된 처벌(PS)과 정보보안인식(ISA)이 정보보안정책에 대한 주관적 규범(SN)에 주는 영향에서 유의적인 차이가 있다고 나타났다. 이는 외주직원이 가지는 정보보안정책에 대한 신념으로서의 주관적 규범(SN)이 정보보안정책에 대한 위반의도(INTV)에 영향을 주지 않는 것으로 나온 결과를 설명하는 것이다.

내부직원 그룹은 정보보안정책에 대한 주관적 규범(SN)이 정보보안정책에 대한 위반의도(INTV)에 영향을 미치지만, 외주직원 그룹에서는 유의하게 나타나지 않았다. 외주직원은 자신의 동료, 상사나 경영진이 자신에 대해 생각하는 정보보안정책의 준수에 대한 인식을 나타내는 정보보안정책에 대한 주관적 규범(SN)이라는 요인보다 정보보안정책 준수를 위해 필요한 기술, 지식, 역량에 대해 인식된 행동통제의 정도를 나타내는 정보보안정책에 대한 행동통제(BC)에 영향을 받아 정보보안정책에 대한 위반의도(INTV)가 억제된다는 것이다. 이는 외주직원을 관리하는 정보보안정책을 수립할 때와 외주직원에 대한 정보보안교육을 수립할 때 중요하게 고려되어야 하는 사항이다. 내부직원에 대한 정보보안교육은 자신이 정보보안정책에 대해 지킬 것이라는 상사와 회사 동료의 기대가 있음을 강조하여야 하지만 외주직원에 대한 정보보안교육은 자신이 현재 배우는 내용을 통해 스스로 정보보안정책을 잘 지킬 수 있고, 충

분하게 지킬 수 있을 정도로 쉽게 설명하여야 할 것이다. 단순하게 정보보안정책에 대한 지식을 전파하면서 준수하여야 한다는 것만 강조하면 교육의 효과는 감소할 것이다.

금융회사의 보안사고는 증가하고 있으며, 외주직원에 의해 발생하는 비율이 증가하고 있다(감사원, 2014). 이러한 외주직원의 보안사고가 증가하는 환경은 금융회사의 외주용역 증가도 원인 중의 하나다. 하지만 전문적인 업무의 영역 외의 서비스에 대해 외주용역을 선택하는 것이 금융회사의 비용 절감에 효과가 있고 급변하는 시장환경에 지속적인 경영성과를 내기 위해선 선택할 수밖에 없는 경영전략이라고 할 수 있다. 이러한 경영전략의 선택에서 금융회사의 보안사고를 관리하기 위해선 외주용역으로 금융회사에 투입되어 업무를 수행하는 외주직원에 대한 관리를 강화되어야 할 것이다. 내부직원과 같은 업무를 수행하기 때문에 같은 권한을 주어 업무를 수행하도록 하는 것은 내부자 위협 관점에서 위험을 알고 있으면서 통제하지 않는 것과 같다. 외주직원 관리는 외주직원이 정보보안정책에 대한 위반의도에 영향을 주는 요인들을 응용하여 정보보안정책은 외주직원이 쉽게 이해하고 스스로 지킬 수 있도록 설계되어야 하며, 내부직원과 같은 업무를 수행할지라도 정보보안교육의 내용은 다르게 진행하여야 더욱 효과적이다.

본 연구에서 주는 시사점은 외주직원은 내부직원과 정보보안정책에 대한 위반의도에 영향을 주는 요인 간에 차이가 있다는 것으로 이를 실무적으로 이용할 수 있는 외주직원관리를 위한 교육 프로그램의 방향을 제시하였으며, 학술적으로 내부직원과 외주직원 간의 차이에 대해 정보보안정책에 대한 위반의도를 통해 살펴본 초기 논문으로 앞으로의 연구에 초석이 될 수 있다.

본 연구의 한계점은 금융회사의 조직원을 대상으로 설문을 시행하고 분석한 결과를 기준으로 설명한 것으로 전체 산업으로 일반화하여 설명하기에는 부족한 점이 있어 앞으로 다른 산업을 대상으로 연구를 수행하여 일반적인 이론으로 설명할 수 있는지 확인이 필요하다. 또한, 내부직원과 외주직원의 다중 집단 분석에 사용된 표본의 크기가 246 대 117로 두 배의 차이가 나는 것도 한 계점으로 지적할 수 있다. 금융회사 조직구성원의 특성상 외주직원을 내부직원에 비해 적은 인원으로 운영하고 있어 비슷한 수의 표본을 획득하여 연구를 수행하는 데 어려움이 있었다. 향후 더욱 일반화된 이론으로 발전시키기 위해 더 많은 표본을 대상으로 실증 분석을 수행하여, 본 연구의 결과를 일반화시킬 필요가 있을 것이다.

참 고 문 헌

[1] 감사원, *감사결과보고서-금융회사 개인정보 유출 관련 검사 · 감독 실태*, 감사원, 2014.

[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] 강주영, 이재규, “산업은행: 금융 IT 아웃소싱 -공동협력으로 안전한 문을 연다”, *Information Systems Review*, 제7권, 제2호, 2005, pp. 229-255.

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

[6] 김양훈, 문제욱, 황선호, 장항배, “ICT 아웃소싱 환경에서 보안관리 방안 연구”, *정보보호학회지*, 제24권, 제1호, 2014, pp. 23-31.

[7] 삼정KPMG 경제연구원, *Asian Outsourcing: the next wave*, SAMJONG Insight, 제4권, 2007, pp. 1-7.

[8] 송지호, *전략적 Outsourcing-은행산업을 중심*

으로, Opentide ViSTA, 2001.

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

[10] 이민화, “The factors affecting outsourcing of data processing services”, *정보시스템연구*, 제6권, 제2호, 1997, pp. 1-28.

[11] 이정하, 이상용, “금융회사 정보보안정책의 위반에 영향을 주는 요인 연구: 지각된 고객정보 민감도에 따른 조절효과”, *Journal of Information Technology Applications and Management,* 제22권, 제4호, 2015, pp. 225-251.

[12] 이학식, 임지훈, *SPSS 20.0 매뉴얼*, 집현재, 2013.

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

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

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

[16] 장효강, 류황건, 배성권, “병원 아웃소싱 직원과 정규직원의 조직문화 인식이 직무에 미치는 영향”, *한국콘텐츠학회논문지*, 제9권, 제2호, 2009, pp. 279-288.

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

[18] 최창래, 윤장호, 이경호, “금융보안 리스크 기반의 IT도급 정책 연구”, *정보보호학회논문지*, 제24권, 제4호, 2014, pp. 681-694.

[19] KRG, *IT 아웃소싱 동향 보고서*, KRG Report, 2002.

[20] Ajzen, I., “The theory of planned behavior”, *Organizational Behavior and Human Decision Processes*, Vol.50, No.2, 1991, pp. 179-211.

[21] Ajzen, I., D. Albarracin, and R. Hornik, *Prediction and change of health behavior: Applying the reasoned action approach*, Lawrence Erlbaum Associates, New Jersey, 2007.

[22] Apte, U., “Global outsourcing of information systems and processing services”, *The Information Society*, Vol.7, No.4, 1990, pp. 287-303.

[23] 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.

[24] Aurigemma, S. and R. Panko, “A composite framework for behavioral compliance with information security policies”, *2012 45th Hawaii International Conference on System Science*, 2012, pp. 3248-3257.

[25] Bardhan, A. D. and C. A. Kroll, “The new wave of outsourcing”, *Fisher Center for Real Estate and Urban Economics*, 2003, pp. 1-12.

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

[27] Bulgurcu, B., H. Cavusoglu, and I. Benbasat, “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.

[28] Carroll, M. D., “Information security: Examining and managing the insider threat”, *Proceedings of the 3rd annual conference on Information security curriculum development*, 2006, pp. 156-158.

[29] Chin, W. W., “The partial least squares approach

to structural equation modeling", in Marcoulides G. A.(eds), *Modern Methods for Business Research*, Lawrence Erlbaum Associates, New Jersey, 1998, pp. 295-336.

[30] Chin, W. W., B. L. Marcolin, and P. R. Newsted, "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.

[31] Cohen, J., *Statistical power analysis for the behavioral sciences*, Lawrence Erlbaum Associates, New Jersey, 2013.

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

[33] D'Arcy, J., A. Hovav, and D. Galletta, "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.

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

[35] Gaonjur, P. and C. Bokhoree, "Risk of insider threats in information technology outsourcing: Can deceptive techniques be applied?", *Proceedings of the 2006 International Conference on Security and Management*, 2006, pp. 522-529.

[36] Gefen, D. and D. Straub, "A practical guide to factorial validity using PLS-Graph: Tutorial and annotated example", *Communications of the Association for Information Systems*, Vol.16, 2005, pp. 91-109.

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

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

[39] Hair, J. F., W. C. Black, B. J. Babin, R. E., Anderson, and R. L. Tatham, *Multivariate data analysis, 6th edition*, Pearson, 2006.

[40] Hair, J. F., M. Sarstedt, C. M. Ringle, and J. A. Mena, "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.

[41] Hamin, Z., "Insider cyber-threats: Problems and perspectives", *International Review of Law, Computers and Technology*, Vol.14, No.1, 2000, p. 105.

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

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

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

[45] Hong, J., J. Kim, and J. Cho "The trend of the security research for the insider cyber threat", *International Journal of Future Generation Communication and Networking*, Vol.3, No.2, 2010, pp. 31-40.

[46] Hu, Q., T. Dinev, P. Hart, and D. Cooke, "Managing employee compliance with information security policies: The critical role of top management and organizational culture", *Decision Sciences*, Vol.43, No.4, 2012, pp. 615-660.

[47] Hu, Q., Z. Xu, T. Dinev, and H. Ling, "Does deterrence work in reducing information security policy abuse by employees?", *Communications of the ACM*, Vol.54, No.6, 2011, pp. 54-60.

[48] 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.

[49] 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.

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

[51] Keil, M., A. Rai, and S. Liu, "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.

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

[53] Kim, S. H., K. H. Yang, and S. Park, "An integrative behavioral model of information security policy compliance", *The Scientific World Journal*, Vol.2014, 2014, pp. 1-12.

[54] Lacity, M. C. and R. A. Hirschheim, *Information systems outsourcing; myths, metaphors, and realities*, John Wiley & Sons, Inc., New York, 1993.

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

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

[57] Loh, L. and N. Venkatraman, "An empirical study of information technology outsourcing: Benefits, risks, and performance implications", *ICIS 1995 Proceedings*, 1995, pp. 277-288.

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

[59] Nagin, D. S. and G. Pogarsky, "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.

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

[61] Paternoster, R. and S. Simpson, "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.

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

[63] Pfleeger, C. P., "Reflections on the insider threat", in Stolfo, S. J., S. M. Bellovin, A. D. Keromytis, S. Hershkop, S. W. Smith, and S. Sinclair(eds),

Insider Attack and Cyber Security: Beyond the Hacker, Springer US, Boston, 2008, pp. 5-16.

[64] Sarkar, K. R,, "Assessing insider threats to information security using technical, behavioural and organisational measures", *Information Security Technical Report*, Vol.15, No.3, 2010, pp. 112-133.

[65] Schultz, E. E., "A framework for understanding and predicting insider attacks", *Computers and Security*, Vol.21, No.6, 2002, pp. 526-531.

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

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

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

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

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

[71] 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.

[72] Stone, M., "Cross-validatory choice and assessment of statistical predictions", *Journal of the Royal Statistical Society. Series B (Methodological)*, Vol.36, No.2, 1974, pp. 111-147.

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

[74] Tenenhaus, M., S. Amato, and V. E. Vinzi, "A global goodness-of-fit index for PLS structural equation modelling", *Proceedings of the XLII SIS Scientific Meeting*, Vol.1, 2004, pp. 739-742.

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

[76] Theoharidou, M., S. Kokolakis, M. Karyda, and E. Kiountouzis, "The insider threat to information systems and the effectiveness of ISO17799", *Computers and Security*, Vol.24, No.6, 2005, pp. 472-484.

[77] Vance, A. and M. Siponen, "Is security policy violations: A rational choice perspective", *Journal of Organizational and End User Computing*, Vol.24, No.1, 2012, pp. 21-41.

[78] Whitman, M. E., A. M. Townsend, and R. J. Aalberts, "Information systems security and the need for policy", In Dhillon, G.(eds), *Information Security Management: Global Challenges in the New Millennium*, IGI Global, Pennsylvania, 2001, pp. 9-18.

[79] Wixom, B. H. and H. J. Watson, "An empirical investigation of the factors affecting data warehousing success", *MIS Quarterly*, Vol.25, No.1, 2001, pp. 17-41.

[80] Yang, D. H., S. Kim, C. Nam, and J. W. Min, "Developing a decision model for business process outsourcing", *Computers and Operations Research*, Vol.34, No.12, 2007, pp. 3769-3778.

[81] Yoon, C., "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.

Information Systems Review
Volume 18 Number 4
December 2016

Violations of Information Security Policy in a Financial Firm: The Difference between the Own Employees and Outsourced Contractors

Jeong-Ha Lee* · Sang-Yong Tom Lee**

Abstract

Information security incidents caused by authorized insiders are increasing in financial firms, and this increase is particularly increased by outsourced contractors. With the increase in outsourcing in financial firms, outsourced contractors having authorized right has become a threat and could violate an organization's information security policy. This study aims to analyze the differences between own employees and outsourced contractors and to determine the factors affecting the violation of information security policy to mitigate information security incidents. This study examines the factors driving employees to violate information security policy in financial firms based on the theory of planned behavior, general deterrence theory, and information security awareness, and the moderating effects of employee type between own employees and outsourced contractors. We used 363 samples that were collected through both online and offline surveys and conducted partial least square-structural equation modeling and multiple group analysis to determine the differences between own employees (246 samples, 68%) and outsourced contractors (117 samples, 32%). We found that the perceived sanction and information security awareness support the information security policy violation attitude and subjective norm, and the perceived sanction does not support the information security policy behavior control. The moderating effects of employee type in the research model were also supported. According to the t-test result between own employees and outsourced contractors, outsourced contractors' behavior control supported information security violation intention but not subject norms. The academic implications of this study is expected to be the basis for future research on outsourced contractors' violation of information security policy and a guide to develop information security awareness programs for outsourced contractors to control these incidents. Financial firms need to develop an information security awareness program for outsourced contractors to increase the knowledge and understanding of information security policy. Moreover, this program is effective for outsourced contractors.

Keywords: Information Security Policy, Outsourced Contractor Management, Information Security Education, Information Security Awareness, Information Security Training

* Ph.D. Candidate in Business Administration, Seoul School of Integrated Sciences and Technologies
** Corresponding Author, Professor, School of Business, Hanyang University

◐ 저 자 소 개 ◑

이 정 하 (jasonlee2484@gmail.com)

숭실대학교 정보과학대학원에서 공학석사(정보통신융합학 전공) 학위를 취득하고, 서울과학종합대학원대학교에서 경영학 박사(정보보호경영 전공)를 수료하였다. 현재 외국계 생명보험회사에서 IT 기획관리팀장으로 재직 중이며, (사)한국씨아이에스에스피협회 보안연구실 연구위원, (사)한국정보시스템통제감사협회 아카데미 연구회 이사 및 보안부문 간사로 활동 중이다. 주요 관심분야는 정보보호경영, 정보보호 거버넌스, 개인정보보호, 금융정보보호, 사물인터넷, 빅 데이터 등이다.

이 상 용 (tomlee@hanyang.ac.kr)

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.

논문접수일 : 2016년 06월 03일 **게재확정일 : 2016년 11월 11일**
1차 수정일 : 2016년 09월 08일