조직의 보안 분위기가 개인의 기회주의 행동에 미치는 영향에 관한 실증 연구

임명성*

An Effect of Organizational Security Climate on Individual's Opportunistic Security Behavior: An Empirical Study

Myung-Seong Yim*

요 약 보안 분위기에 대한 연구를 위해 안전 분위기에 관한 선행연구와 성과모델을 기반으로 본 연구는 정보보안 분위기 모델을 제안하였다. 연구모델은 정보보안 분위기, 보안 정책 준수 태도, 그리고 기회주의적 보안 행위로 구성되었다. 분석 결과 조직의 보안 분위기는 보안정책 준수태도에 영향을 미쳤으며, 태도는 기회주의적 보안 행위에 유의한 영향을 미치는 것으로 나타났다. 즉, 보안 분위기는 기회주의적 보안행위에 직접적인 영향을 미치기보다는 보안 정책 준수태도를 통해 간접 효과를 나타내는 것으로 나타났다.

주제어 : 정보보안, 보안 분위기, 안전 분위기, 보안 정책

Abstract Drawing upon Griffin and Neal's safety climate and performance model, this study developed an information security climate model. Research model is composed of three research variables that include information security climate, information security compliance attitude, and opportunistic security behavior. Results of the study strongly support the fundamental proposition that the organizational security climate has significant positive influence on the individual's opportunistic security behavior. However, the study also reveals that the organizational climate may not directly associate with the reduction of opportunistic security behavior. Rather the organizational security climate nurtures the favorable attitude of the employee towards the compliance of information security, which in turn discourages opportunistic security behavior.

Key Words : Information Security, Security Climate, Safety Climate, Security Policy

1. 서론

작금 전 세계적으로 많은 기업들의 정보보안에 대한 관심은 그 어느 때 보다 높다. 최근에 정보 보안 사고가 그 어느 때 보다 빈번하게 발생하고 있으며, 그 피해 또한 치명적이라는 것을 보여주고 있다. 한국의 경우 대표 금융기업인 농협, 현대 캐피탈, 삼성카드와 같은 금융회사들이 2011년 한 해 동안에 정보 보안 사고로 인해 고통받고 있으며 이로 인한 피해액도 1,000억 원에 달하는 것으로 보고되고 있다.

Computer Crime and Security Survey의 조사결과에 따르면 미국의 경우에도 2007년 한 해 동안 응답기업 중 46%가 자사 내에서 크고 작은 보안사고가 발생하였다고 보고하고 있으며[35], 미국 내 5,412명의 보안 실무자를 대상으로 수행한 2011년도 Computer Crime and Security Survey의 보고에서도 약 45.6%의 기업이 2009년 7월부터 2010년 6월 사이에 적어도 한번 이상 자사 내에서 보안 사고가 발생하였다고 보고하였다[55]. 피해액도 약 $100,000에 달한다고 보고하였다[55]. 이와 같이 정보보안에 대한 중요성이 높아짐에 따라 보안 사고를 어떻게 줄일 수 있는지에 대한 관심도 고조되고 있다. 일반

*삼육대학교 경영학과 조교수
논문접수: 2012년 9월 19일, 1차 수정을 거쳐, 심사완료: 2012년 10월 29일

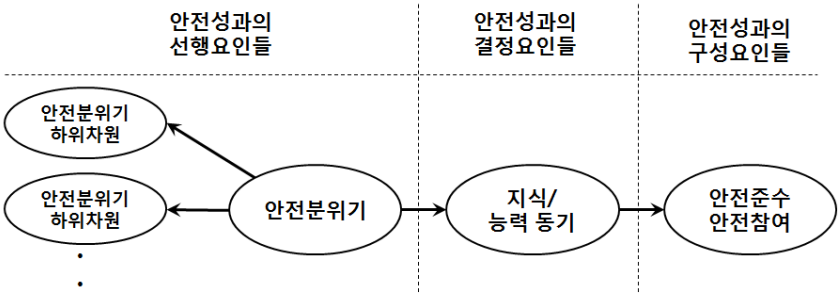
적으로 보안 사고는 인적 문제(human error)인지 기술적 문제인지(non-human error)와 내부적 문제(internal)인지 외부적 문제(external)인지에 따라서 4가지 차원으로 나뉜다. 여기서 많은 연구에서 관심을 두고 있는 것은 내부적으로 발생하는 인간적 문제이다. 여러 조사결과에 따르면 기업 내부에서 발생하는 보안 사고의 경우 해커와 같은 외부인에 의해 발생하는 빈도보다 내부인에 의해 발생하는 사고건수가 월등히 많다는 것을 제시하고 있다. Cardinali(1995)에 따르면 데이터베이스 보안사고 중 80%가 내부인에 의해 발생한다고 보고하고 있으며, Enrnst and Young[20][21] 역시 보안 사고의 50-75%가 조직 내부인에 의해서 발생하고 있음을 제시하고 있다. 이처럼 내부인에 의한 보안사고가 더 큰 비중을 차지하고 있음에 따라 많은 연구들은 어떻게 하면 조직 내부의 개인들로 인해 발생하는 보안 사고를 줄일 수 있는지 연구해 왔다. 특히 정보보안 문제를 해결하기 위한 핵심이 조직원들의 보안 정책 준수라는 점에서 보안 사고를 줄일 수 있는 방안으로 보안 정책의 준수 및 미 준수에 관한 연구를 지속적으로 수행하여 왔다[16][17][31][32]. 이러한 연구의 공통점은 주로 인적 요인을 중심으로 연구하였다는 것이다. 물론 기존 연구가 개인이 정보보안 정책을 준수하도록 유도할 수 있는 요인들을 다양한 측면에서 규명했다는 점에서는 의미가 있으나 상황적 요인에 대한 고려가 부족하다는 점에서는 한계점이 존재한다. 정보보안과 관련된 기존 문헌에 대해서 <표 1>에 정리하였다.

사회적 정보 관점에 따르면 개인의 성향(personal predispositions) 요인보다 상황적 요인(contextual factors)이 개인의 행동에 더 큰 영향을 미칠 수 있음을 제시하면서 조직의 분위기(organizational climate)와 같은 조직 환경(organizational environment)에 대한 인식의 중요성을 강조하고 있다[10][34][56][57]. 최근 Chan et al.(2005)은 안전 분위기(safety climate) 개념을 차용하여 사회적 영향(social influence)측면에서 정보보안 분위기(information security climate)를 개념화하여 이와 정보보안 정책 준수행위간의 관계를 실증적으로 분석하였다.

조직 분위기에 관한 선행연구에서는 조직의 분위기가 단일 차원이 아닌 다차원적 특성을 가지고 있음을 제시하고 있다[3][6][28][34][46][66][68][69][70]. 조직 내 개인들은 자신의 가치관을 기반으로 자신이 속한 환경의 구체적인 특성과 해당 특성의 중요성을 평가하게 되는데 이러한 특성들이 조직의 분위기를 형성하기 때문에 조직의 분위기는 고차원적 요인으로 구성된다[28][34]. 정보보안 분위기도 다양한 특성들로 구성된 고차원적 요인임에도 불구하고 기존 연구에서는 단일 차원 관점에서 접근하고 있다는 점에서 문제점으로 제시된다. 따라서 본 연구는 고차원적 관점에서 정보보안 분위기를 제시하고 정보보안 분위기가 개인의 기회주의적 보안 행위에 어떠한 영향을 미치는지 실증적으로 분석하고자 한다. 구체적으로 본 연구에서는 조직적 요인으로 정보보안 분위기와 개인적 요인인 기회주의적 보안 행위간의 관계를 실증분석해 보고자 하는데 이는 사회 심리학적 관점에서 제시하고 있는 바와 같이 조직과 개인은 지속적으로 상호작용하는 관계에 있기 때문에[3], 이 둘 간의 관계를 살펴보는 것이 매우 중요하다.

2. 정보 보안 분위기 (Information Security Climate)

조직의 분위기(organizational climate)는 관찰 가능한



[그림 1] 안전 분위기(Safety Climate) 모형 [28]

〈표 1〉 주요 선행 연구 정리

연구자	기반이론	주요성과변수	연구결과
Herath and Rao(2009a)	-General Deterrence Theory	-Penalty -Social Pressures -Perceived Effectiveness	General Deterrence 이론을 기반으로 보안 정책 준수를 위한 Extrinsic Motivation과 Intrinsic Motivation을 규명함
Herath and Rao(2009b)	-Protection Motivation Theory -General Deterrence Theory	-Detection Certainty -Self-Efficacy -Organizational Commitment	Protection Motivation 이론과 General Deterrence Theory를 관점을 통합함
Johnston and Warkentin(2010)	-General Deterrence Theory	-Response Efficacy -Self Efficacy -Social Influence	Theory of Planned Behavior와 General Deterrence 이론을 접목함
Puhakainen and Siponen(2010)	-Universal Constructive Instructional Theory -Elaboration Likelihood Model	-IS Security Training Program	정보보안 훈련의 이론적 기반을 제시함
Goel and Chengalur-Smith (2010)	-Information Quality	-Effectiveness of IS Security Policy	정보보안 정책의 효과성을 사용자 측면에서 측정할 수 있는 측정도구 제시
Siponen and Vance(2010)	-Neutralization Theory	-Intention to Violate IS Security Policy -Neutralization	조직원들이 정보보안정책을 준수하지 않는 이유를 규명함
Bulgurcu et al.(2010)	-Rational Choice Theory	-Benefit of Compliance -Cost of Compliance -Cost of Noncompliance	인지적 이익과 비용관점에서 정보보안 정책을 왜 준수해야 하는지를 규명
Herath et al.(2011)	-Moral Disengagement Theory	-IS Security Violation Likelihood -Moral Disengagement	조직원들이 정보보안정책을 준수하지 않는 이유를 규명함
D'Arcy and Herath(2011)	-General Deterrence Theory	-Self-Control -Computer Self-Efficacy -Moral Beliefs -Employee Position	상황적 요인(contingency variables)에 대한 필요성 규명
Goo et al.(2013)	-Safety Climate	-Security Climate -Organizational Commitment	정보보안 분위기가 보안정책준수 미치는 영향 규명

실행(practices)과 절차(procedures)에 대한 조직원들의 인식에 초점을 두고 있다. 그리고 이러한 실행과 인식은 연구자에 의해 분석 가능한 다양한 차원으로 세분화된다[18]. 조직의 분위기에 관한 최근의 연구는 기존의 연구보다 더욱더 구체성을 띄고 있는데 이는 조직의 다양한 정황(context)을 반영하고 있기 때문이다. 이전의 연구의 경우 포괄적 관점에서의 분위기를 중심으로 연구가 진행된 반면[34], 최근의 연구는 안전 분위기[28]나 정보보안 분위기[10]와 같이 조직 내 구체적인 특성을 반영하고 있다. 본 연구는 정보보안에 대해 종업원들이 경험하는 조직적 특성을 반영하고 있기에 정보보안 분위기에 초점을 두고 있다. 이 개념을 설명하는데 있어서 본 연구는 안전 분위기에 대한 연구를 중심으로 기술하고자 하는데 이는 안전 분위기와 보안 분위기 간의 다음과 같은 공통점이 존재하기 때문이다. 첫째, 정보보안과 안전이 기업의 가치를 창출하는 것은 아니나 기업의 지속적 운영을 위해서는 필수적이다[10]. 둘째, 정보보안과 안전의 성과는 무사고(non-occurrences of accidents)를 통해 달성된다[10]. 물론 정보보안 사고로 인해 신체적 손상이 발생되는 것은 아니나 안전과 정보보안 모두 기업의 손실을 유발할 수 있는 잠재성을 보유하고 있다. 셋째, 안전과 정보보안 모두 조직이 제시하고 있는 정책이나 안전 수칙의 준수를 강조하는데 이를 따라야 하는 개인은 불편함을 느낄 뿐만 아니라 업무의 효율성 및 생산성과의 상충관계를 유발할 수 있다[10][32].

이러한 관련성을 근거로 본 연구는 안전 분위기에 대한 연구 중 다른 연구에 기반으로 자주 활용되는 모형인 Griffin and Neal(2000)의 안전 분위기 모형을 기반으로 보안 분위기를 형성하고자 한다. 우선 안전 분위기 연구에서 안전 분위기는 일반적 조직 분위기와 안전과 관련

된 특성으로 구성된다. 본 요인은 기존의 조직 분위기와 마찬가지로 안전을 구성하는 구체적인 1차 요인들(first-order factors)로 구성된 고차요인(higher order factor)으로 개념화된다. 왜냐하면, 안전 분위기는 조직 내에서 직원들이 안전이 가치가 있다고 믿게 만드는 다양한 조직의 속성(organizational attributes)을 반영해야 하기 때문에 1차 요인이 아닌 고차요인으로 구성된다[28]. 하지만, 학자들 간에 안전 분위기가 고차요인이라는 합의는 존재하나 고차요인을 구성하는 1차 요인이 무엇인가에 대해서는 여전히 학자마다 이견이 존재한다. Griffin and Neal(2000)은 그 동안의 연구를 기반으로 가장 많이 인용되는 1차 요인들을 제시하고 2차 요인 구조로 구성된 안전 분위기 모형을 실증적으로 분석하였는데 여기에 포함된 요인은 경영진의 가치(management values), 안전 의사소통(safety communication), 안전 훈련(safety training), 안전 정책(safety inspection) 등이다. 본 연구에서는 이를 기반으로 정보보안 분위기를 최고 경영진의 관심(top management attention), 보안 강조(security reinforcement), 보안 인식 훈련(security awareness training), 보안 정책의 효과성(effectiveness of security policy)등으로 구성하였다. 각각의 개념에 대한 구체적인 설명은 다음과 같다.

2.1 최고 경영진의 관심 (Top Management Attention)

안전 분위기를 형성하는 1차 요인이 무엇인가에 대해서는 다양한 차이가 존재한다. 그러나 많은 연구자들 사이에서 안전 분위기를 형성하는 요인으로 가장 많이 회자되는 요인은 경영진의 가치(management values)이다[28]. 경영진의 가치는 지금까지 조직원들의 안녕(well-being)에 대한 경영진의 관심, 안전에 대한 경영진의 태도, 안전이 회사의 경영을 위해 중요하다고 인식하는 수준 등으로 측정되어 왔다(예. [48]). 즉, 이러한 측정지표들을 결과적으로 경영진의 관심(attention)을 평가하는 것으로 경영진의 관심이 분위기를 구성하는 매우 중요한 요소임을 강조하고 있다고 볼 수 있다. 정보보안 측면에서도 경영진의 관심이 정보보안 분위기를 형성하는 매우 중요한 요소로 볼 수 있는데, Chan et al.(2005)의 연구를 보면 경영진의 관심이 보안 정책을 준수하도록 하는 중요한 요인으로 작용하고 있음을 실증분석을 통해 제시하고 있다.

2.2 보안 강조 (Security Reinforcement)

보안에 대한 강화란 종업원들에 의해 관찰되는 경영진의 반복적인 행위를 말하는 것으로[10], 보안에 대해 경영진이 조직원들과 의사소통하고 보안의 중요성에 대해 강조하는 행위를 포함한다. Griffin and Neal(2000)은 안전 측면에서 안전과 관련된 의사소통이 결국 안전 분위기를 형성하는 중요한 요인으로 작용함을 실증분석을 통해 규명하였다. 결국, 경영진의 이러한 행위는 조직원들이 어떠한 행위에 몰입하도록 유도하는 역할을 한다는 점에서[52] 보안 분위기를 형성하는 중요한 요인으로 볼 수 있다.

2.3 보안 인식 교육 (Security Awareness Training)

보안 인식 교육은 조직이 사용하는 보안 대책(security countermeasures) 중의 하나로 조직원들에게 보안 정책의 준수를 강화시키며, 시스템 오용으로 인한 잠재적 결과를 주지시키는 역할을 수행한다[16]. 또한 기업이 제시하는 정보보안 정책을 정확히 이해하고 이를 받아들이도록 하는 요인으로도 작용한다. 보안 인식 교육은 조직원들에게 보안 환경에 대한 지식을 전달하기 위해 다양한 형태로 제공되는데 온라인, 오프라인 훈련뿐만 아니라 뉴스레터나 이메일을 통해서도 제공된다. 보안 인식 교육의 주된 목적은 조직 환경 내에서 발생할 수 있는 정보 위험에 대한 지식을 전달, 최근의 보안 정책 침해 사례 제공, 조직의 정보 자원과 관련된 책임 의식을 고양시키는 것이다[16]. 이러한 보안 인식 교육은 조직의 실행활동(practice) 중 하나로 정보보안 분위기를 형성하는 핵심 요인 중 하나다[10].

2.4 보안 정책의 효과성 (Effectiveness of Security Policy)

보안 정책(security policy)은 일반적으로 두 가지 형태가 존재하는데 네트워크 접근 통계 규칙을 기술한 컴퓨터/네트워크 보안 정책과 조직의 전반적인 정보보안을 보장하기 위한 전략과 계획을 포함하는 조직의 정보 보안 관리 정책이 있다[26]. 정보보안 연구에서 가장 강조하는 정책은 후자인 정보보안 정책으로 조직 내 모든 조직원들이 준수할 것을 강조한다. 특히, 본 정책이 중요하다 인식되는 것은 조직 구성원 전체와 직접적으로 관련이 있을 뿐만 아니라 그들이 수행하는 업무 중에 반드시

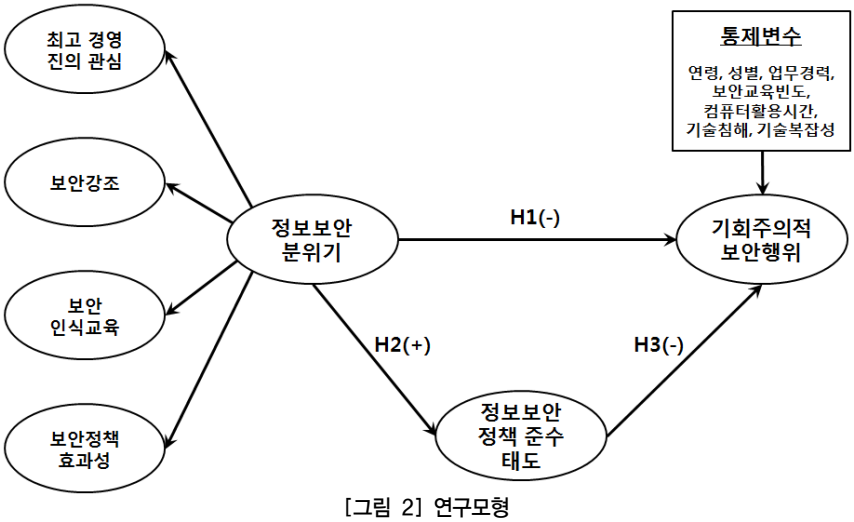
지켜져야 하기 때문이다. 하지만 정보 보안 정책이 궁극적으로 그 효력을 발휘하기 위해서는 효과적이어야 한다[26]. 기존 문헌에서 검증한 정보보안 정책의 효과성은 다르게 나타나고 있는데 예를 들어, Straub(1990)은 보안 정책이 컴퓨터 오남용(computer abuse)을 줄이는데 영향을 미친다고 제시한 반면 Foltz(2000)는 보안 정책이 정보시스템의 오용(IS misuse)에 아무런 영향도 미치지 못한다고 제시하였다. 이처럼 일관되지 못한 결과는 정보보안 정책의 효과성에 대한 평가가 없이 사용되기 때문이다. Goel et al.(2010)은 보안 정책의 효과성을 평가하는 기준으로 내용(content)과 형식(form)을 제안하였는데, 이중 내용은 지금까지 폭 넓게 연구되어온 반면 보안 형식에 대해서는 관련 연구가 매우 부족하다. 내용은 국제적 표준을 기준이 마련되어 있기 때문에 이를 기반으로 작성되는 경우가 많고 정책이라는 특성 때문에 정책 입안자들에 의해 작성되는 것이 일반적이다. 이 때문에 기존의 연구들은 정보보안 정책에 대한 연구 시 정책의 존재 여부를 인지하고 있는지를 주로 평가해왔다. 하지만 보안 정책을 준수해야 하는 대상은 모든 조직원들이기 때문에 정책은 조직원들이 이해하기 쉽고, 읽기 편하고, 명확하게 전달되어야 한다. 보안 침해 행위의 억제를 위해 자주 차용되는 행위 억제 이론(General Deterrence Theory)의 기본 가정은 모든 사람들이 보안 정책은 이해하고 있다는 것을 기반으로 하고 있는데[23] 이는 결국 사용자 중심의 보안 정책을 수립의 중요성을 강조하고 있음을 나타낸다고 볼 수 있다. 이러한 정책은 조직이 또 다른 실행활동 중 하나로 조직의 보안 분위기를 형성하는 중요한 요인으로 작용한다[10].

3. 연구모형 및 가설수립

본 연구는 Griffin and Neal(2000)과 Neal et al.(2000)의 연구에서 제시한 안전 분위기 모형을 기반으로 정보보안 분위기를 다차원적 요인으로 구성하고 정보보안 분위기가 개인의 보안 정책 준수 태도와 개인의 기회주의적 보안 행위에 어떠한 영향을 미치는지 살펴보고자 한다. 기회주의적 보안 행위는 정보보안 정책을 준수하지 않음으로 인해 개인이 얻게 되는 반사이익을 나타내는 것으로 업무를 수행하는데 발생하는 다양한 불편함, 그리고 업무상 생산성 저하 등으로 인해 정보보안에 대해 부정적으로 인식함으로 보안 정책을 준수하지 않는 것이 개인의 가치를 상승시킨다고 생각하는 것을 나타낸다. 이러한 개인적 요인이 보안 분위기라는 조직적 요인과 어떠한 관계를 형성하는지 규명하는 것은 중요하다. 이를 위해 그림 2의 연구모형 및 관련 가설을 수립하여 실증 분석해 보고자 한다.

3.1 정보 보안 분위기 (Information Security Climate)

조직의 분위기는 조직원들의 행위에 영향을 미친다[10]. 사회적 정보 처리(social information processing) 관



[그림 2] 연구모형

〈표 2〉 응답자의 인구 통계학적 특성 (N=581)

		빈도	비율(%)			빈도	비율(%)
성별	남성	440	75.7	직위	상위관리자	22	3.8
	여성	127	21.9		중간관리자	133	22.9
	무응답	14	2.4		전문직	46	7.9
연령	18-24	3	0.5		기술직	88	15.1
	25-34	253	43.5		사무직	257	44.2
	35-44	212	36.5		기타	3	0.5
	45 이상	112	19.2		무응답	32	5.5
	무응답	1	0.2			581	100%

점에 따르면 개인의 행동은 개인이 가진 기질이나 특성보다 상황적 요인에 의해 더 큰 영향을 받는다고 제시하고 있다[34]. 이는 개인이 지속적으로 조직과 상호작용하는 과정에서 조직의 분위기를 경험하기 때문이다[3][68]. 결국 이러한 경험은 개인의 행위를 유발하는 요인으로 작용하게 된다. 정보보안 측면에서 가장 중요한 행위 중 하나는 조직원들이 정보보안 정책의 준수이다. 하지만 매일의 업무를 수행함에 있어서 정보보안 정책을 준수해야 한다는 것은 조직원들로 하여금 불편함을 느끼게 할 수 있다[32]. 뿐만 아니라 정보보안 정책의 준수는 개인의 업무 생산성과 효율성을 향상에 부정적 영향을 미칠 수 있다[10]. 이러한 부정적 영향은 결과적으로 개인의 기회주의적 보안 행위를 유발할 수 있다. 기회주의적 보안 행위(opportunistic security behavior)란 보안 행위란 보안 정책을 준수하지 않았을 때 개인이 인지하게 효익을 나타낸다. 예를 들어, 시스템 접속 상황에서 자리를 잠시 비울 경우 로그아웃해야 한다는 것이나, 회사의 시스템에 접근 시 복잡한 절차를 거쳐야 한다는 것은 개인이 보안 정책의 준수에 거부감을 느끼게 할 수 있는 부정적 요인으로 작용할 수 있다. 하지만 조직이 정보보안을 강조하는 분위기가 형성되어 있을 경우 개인의 행동에 영향을 미쳐 기회주의적인 보안 행위가 감소시킬 수 있을 뿐만 아니라 정보보안 정책을 준수하는 것이 옳은 행동이라는 판단을 하게 된다. 따라서 다음과 같은 가설을 수립할 수 있다.

[H1] 정보보안 분위기는 기회주의적 보안 행위에 음(-)의 영향을 미칠 것이다.

[H2] 정보보안 분위기는 정보 보안 정책 준수 태도에 정(+)의 영향을 미칠 것이다.

3.2 정보 보안 정책 준수 태도(Information Security Policy Compliance Attitude)

태도란 자신의 행위에 대한 옳고 그름의 판단을 말한다[1]. 만약 개인이 행위의 결과가 긍정적이라 인지할 경우 긍정적인 태도를 형성하게 된다. 반대로 개인이 행위의 결과가 부정적이라 판단될 경우 부정적 태도를 형성하게 된다[65]. 정보보안 관점에서 기업 내 조직원들이 기업의 정보보안 정책 및 다양한 지침을 따르는 것이 결과적으로 기업에 긍정적 영향을 미친다고 인지할 경우 이들은 사적인 가치를 추구하고자 하는 행위는 줄어들 것이다. 이러한 이론적 근거를 기반으로 다음과 같은 가설을 수립할 수 있다.

[H3] 정보 보안 정책 준수 태도는 기회주의적 보안 행위에 음(-)의 영향을 미칠 것이다.

4. 연구방법

4.1 자료수집 및 표본

본 연구는 설문 조사법을 활용하여 데이터를 수집하였다. 수집된 데이터에 대한 기초 통계량 분석은 SPSS v19를 활용하였고 측정모형(measurement model)과 구조모형(structural model)에 대한 분석은 AMOS v18을 활용하였다. 본 연구의 핵심 연구 변수가 분위기(climate) 이고 이것은 조직의 특성에 대한 개인의 인식(perception)을 기반으로 평가되기 때문에[28] 개인을 분석 단위로 하였다.

표본 수집을 위해 ITSMF(Information Technology Service Management Forum) Korea의 회원사의 CIO를 대상으로 미리 사전에 본 설문에 대한 목적을 설명한 뒤

〈표 3〉 2차 요인 모형의 타당성 검증 결과

Model #	χ2	d.f.	χ2/d.f.	NFI	NNFI	CFI	GFI	RMSEA
Model 1	5708.549	275	20.758	.627	.605	.638	.434	.185
Model 2	2924.016	275	10.633	.809	.808	.824	.684	.129
Model 3	1893.360	275	6.885	.876	.882	.892	.769	.101
Model 4	1886.477	271	6.961	.877	.881	.892	.770	.101

Target Coefficient (T) = 0.998175(99.8%)

T value is calculated as F/T.(e.g., 1883.035/1886.477)

T lower limit is calculated as F/FU.(e.g., 1883.035/2924.016=0.643989)

본 설문에 참여의사를 문의하였다. 참여에 대한 문의는 본 연구에 참여 연구자와 각 회원사의 CIO와의 직접 접촉 방법을 통해 이루어졌으며, 이 과정에서 참여 의사를 밝히 핵심 관계자를 중심으로 설문을 배포하였다. 핵심 관계자는 설문 배포과정에서 자사 내 각 부서에 설문이 최대한 고르게 배포되도록 하였다. 배포된 설문은 우편과 이메일을 통해 수집되었다. ITSMF Korea는 IT 서비스 관리와 관련되어 유일하게 국제적으로 인정되는 독립조직인 ITSMF의 한국지사로 멤버쉽에 의해 운영되는 비영리단체이다. 본 포럼의 회원은 정보시스템을 사용하는 사용자 기업과 시스템을 개발하는 SI(Systems Integration) 기업들로 구성되어 있다. 설문은 약 900부가 배포되었으며 이 중 761부가 회수되었다. 이중 연구변수에 결측치(missing value)를 포함하고 있는 180부를 제외하고 총 581부(64.6%)를 최종 분석에 사용하였다. 먼저 Babbie(1990)가 제안한 절차에 따라, 응답자와 무응답자와 구조적으로 다르지 않음을 independent t-test를 통해 확인하였다. 응답자와 무응답자 각 50 개를 무작위로 선택하여 기업의 연 매출과 고용인수를 비교한 결과, 신뢰도 95% 수준에서 응답자와 무응답자간의 유의한 차이가 존재하지 않았다.

총 수집된 581부에 대한 표본 특성은 <표 2>와 같다. 응답자 중 남성이 약 76%를 차지하였다. 연령별로는 25세에서 44세가 80%를 차지하였으며, 45세 이상도 19.2%를 나타내어 특정 연령군에 편중되지 않고 고른 분포를 보이는 것으로 나타났다. 직업군으로는 관리자 그룹이 26.7%로 적지않은 비율로 관리자들의 참여가 있었다. 특히, 응답자 중 상당수의 상위관리자는 본 연구결과에 대해 많은 관심을 보였으며, 연구결과를 공유해 줄 것을 요청하였다. 이는 정보보안이 많은 기업에서 주목받고 있는 이슈가 되고 있다는 것을 반증하고 있다고 볼 수 있다. 다음으로는 사무직이 44.2%로 나타나 정보보안 정책을 준수해야 하는 직접적인 대상들이 많이 참여했다는 것을 알 수 있다.

4.2 변수의 조작적 정의

각각의 설문문항은 기존이론에서 사용된 문항을 사용하였으며, Likert 7점 척도법을 활용하여 응답지를 구성하였다.

각각의 구성개념에 대한 조작적 정의를 살펴보면 다음과 같다. 정보보안 분위기란 정보보안 측면에서 현재 조직의 상태에 대해 조직원들이 경험하고 인지하는 것을 말한다[10]. 본 개념은 조직의 분위기 개념을 기반으로 2차 요인으로 구성되었으며, 각각의 1차 요인은 최고경영진의 관심, 보안 강조, 보안 인식교육, 보안 정책 효과성으로 구성된다. 최고 경영진의 관심은 “보안 측면에서 조직원들에게 관찰되는 경영진의 일상적 행위”를 나타내는 것으로[10]. Purvis et al.(2001)과 Chatterjee et al.(2002)의 연구에서 사용된 측정항목을 활용하여 총 7개의 측정항목으로 측정하였다. 보안 강조는 “정보 보안을 위해 경영진이 수행하는 반복정인 행위”를 말하며, 대표적으로 의사소통이나 정보보안 목표의 강조 등이 포함된다[10]. 본 개념에 대한 측정항목은 Chan et al.(2005)에서 사용된 항목들을 기반으로 3개의 항목으로 측정하였다. 보안 인식 교육은 “정보보안을 위해 관련 지식을 조직원들에게 전달하는 조직의 다양한 활동”을 의미하며, 측정은 D’Arcy et al.(2009)의 연구를 기반으로 7개의 항목으로 측정하였다. 보안 정책 효과성은 “조직원에게 인식되는 조직의 보안 정책 형식의 명확성과 깊이”를 의미하며, Goel et al.(2010)의 연구를 기반으로 총 8개의 항목으로 측정하였다. 보안 정책 준수 태도는“보안 정책을 준수하는 행위에 대한 옳고 그름에 대한 개인의 판단”을 의미하며, Dinev et al.(2009), Herath and Rao(2009b), Pavlou and Fygenson(2006)의 연구에서 사용된 변수를 활용하여 총 6개의 항목으로 측정하였다. 마지막으로, 기회주의적 보안 행위는 “회사의 정보보안 정책을 따르지 않음으로 인해 개인이 얻게 되는 이익에 대한 인식”을 말하는 것으로. Kim et al.(2008), Yoon(2011)의 연구에서 사용된 측정항목을 기반으로 총 5개의 설문항목으로 측정하였다.

〈표 4〉 탐색적 요인분석 및 신뢰도/타당성

	성분						평균분산 추출(AVE)	복합신뢰성 (CR)	크론바흐 α
	1	2	3	4	5	6			
SAT1	0.726	0.326	0.249	0.117	-0.054	0.084	0.736	0.951	0.956
SAT2	0.725	0.282	0.255	0.122	-0.104	0.232			
SAT3	0.821	0.253	0.214	0.108	-0.046	0.204			
SAT4	0.792	0.225	0.214	0.072	-0.027	0.254			
SAT5	0.839	0.277	0.242	0.115	0.041	0.079			
SAT6	0.841	0.28	0.254	0.127	0.067	0.06			
SAT7	0.79	0.222	0.298	0.154	0.025	0.086			
TMA1	0.204	0.813	0.235	0.157	-0.025	0.114	0.74	0.952	0.954
TMA 2	0.212	0.766	0.314	0.176	-0.06	0.14			
TMA 3	0.297	0.823	0.19	0.189	-0.006	0.087			
TMA 4	0.295	0.764	0.277	0.153	-0.022	0.159			
TMA 5	0.343	0.764	0.275	0.172	0.047	0.09			
TMA 6	0.322	0.753	0.251	0.13	0.002	0.18			
TMA7	0.273	0.7	0.213	0.141	-0.024	0.302			
ESP1	0.131	0.206	0.815	0.137	-0.005	0.129	0.646	0.936	0.94
ESP2	0.179	0.159	0.821	0.113	-0.016	0.175			
ESP3	0.28	0.276	0.747	0.199	0.013	0.174			
ESP4	0.277	0.161	0.777	0.071	-0.019	0.189			
ESP5	0.202	0.148	0.799	0.11	-0.043	0.146			
ESP6	0.279	0.351	0.658	0.124	-0.024	0.074			
ESP7	0.324	0.393	0.614	0.114	0.025	0.083			
ESP8	0.304	0.428	0.642	0.104	0	0.072			
SPCA1	0.151	0.243	0.116	0.776	-0.076	0.081	0.717	0.938	0.941
SPCA2	0.119	0.126	0.131	0.796	-0.026	0.063			
SPCA3	0.082	0.157	0.115	0.881	-0.086	0.049			
SPCA4	0.092	0.068	0.097	0.883	-0.054	0.023			
SPCA5	0.103	0.132	0.114	0.883	-0.109	0.027			
SPCA6	0.059	0.086	0.094	0.877	-0.116	0.037			
OSB1	-0.056	0.042	0.016	-0.137	0.72	0.1	0.691	0.917	0.924
OSB2	0.001	-0.047	0.017	-0.032	0.896	0.006			
OSB3	0.006	-0.033	-0.036	-0.073	0.9	0.025			
OSB4	0.001	0.005	-0.016	-0.083	0.92	-0.038			
OSB5	0.012	-0.023	-0.037	-0.066	0.918	-0.036			
SR1	0.263	0.311	0.265	0.127	0.032	0.705	0.716	0.883	0.879
SR2	0.201	0.25	0.284	0.119	0.045	0.806			
SR3	0.3	0.211	0.286	0.017	0.032	0.77			

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.
SAT: 보안인지교육;TMA:경영진의관심;ESP:보안정책의효과성;SPCA:보안정책준수태도;OSB:기회주의적보안행위;SR:보안강화

4.3 정보 보안 분위기의 타당성 검증

본 연구 모형에서 정보보안 분위기 개념은 2차 요인구조 개념 (second order construct)으로 구성하였다. 2차 요인 모형의 차원성(dimensionality) 뿐만 아니라 집중 타당성 판별 타당성을 검증하기 위해, Tanriverdi(2005)의 제안한 검증 절차를 활용하여 일차 요인과 2차 요인 모형을 비교 검증하였다. 모델 1 은 모든 측정항목을 가지고 1개의 잠재변수로 구성된 1차 요인 모형을 나타낸다. 모델 2는 정보 보안 분위기의 4개의 1차 요인으로 구성된 모형을 나타내며, 각각의 잠재변수 간에는 서로 상관관계가 존재하지 않는다. 모델 3은 4개의 1차 요인이 제약없이 서로 상관관계를 가진다는 것을 가정한 모형을 나타낸다. 마지막으로, 모델 4는 정보 보안 분위기라는 2차 요인 모형을 나타낸다. 분석 결과 모형4 (second-order construct)의 적합성이 가장 좋은 것으로 나타났다. 모델 1 (χ^2 = 5708.549, d.f. = 275)과 모델 2(χ^2 = 2924.016, d.f. = 275)간의 비교 결과 모델 2가 더 나은 적합도를 갖는 것으로 나타났다(동일한 자유도 내에서 더 낮은 chi-square를 갖음). 모델 2(χ^2 = 2924.016, d.f. = 275)와 모델 3(χ^2 = 1893.360, d.f. = 275)간의 비교에서는 모델 3 (비제약 모형)이 모델 2(제약 모형)보다 더 나은

〈표 5〉 판별타당성 분석

	평균	표준편차	TMA	SR	SAT	ESP	SPCA	OSB
TMA	4.9321	1.36203	0.86					
SR	3.9185	1.38432	.584**	0.846				
SAT	4.3479	1.40035	.670**	.567**	0.858			
ESP	4.329	1.1855	.665**	.593**	.641**	0.804		
SPCA	5.8962	0.9244	.390**	.251**	.319**	.344**	0.847	
OSB	3.717	1.38795	-0.045	0.029	-0.036	-0.039	-.178**	0.831

**. Correlation is significant at the 0.01 level (2-tailed).

AVE: Average Variance Extracted; CR: Composite (Factor) Reliability

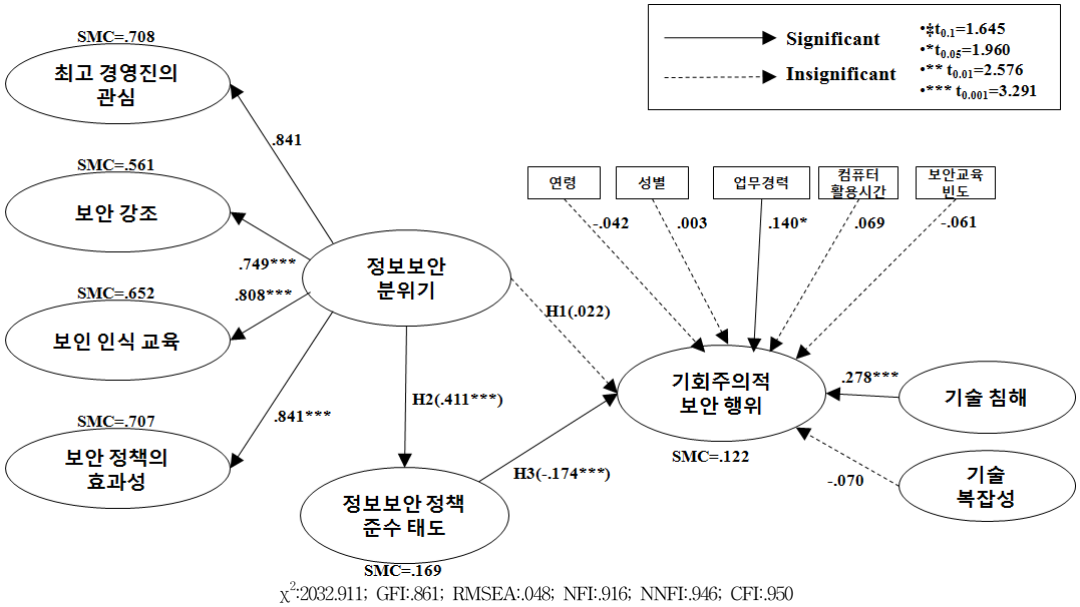
대각선 값은 AVE의 제곱근 값을 나타냄

chi-square ($\Delta\chi^2$ = 1030.656)를 갖는 것으로 나타났다. 모델 3에서 모든 관측변수의 표준화 요인 적재치가 모두 유의한 것으로 나타났으며 ($p < 0.001$), 이러한 결과는 잠재변수의 집중 타당성이 존재한다고 볼 수 있다. 또한 1차 요인 간의 상관관계가 0의 상관관계와 유의한 수준에서 차이가 있었고 기준치인 0.9이하의 값을 나타낸 것은 모델 3 (비제약모형)이 모델 2 (제약모형)보다 더 우수하다는 것을 의미한다. 본 결과는 각각의 1차 요인에 의해 설명되는 이론적 개념간의 차이가 존재함을 의미하며 결국 정보보안 분위기의 판별타당성이 존재함을 나타낸다고 볼 수 있다[2].

마지막으로 본 연구에서는 모델 4 (2차 요인 모델)와 모델 3 (비제약 1차 요인 모델)간의 비교를 통해 2차 요인의 설명력을 평가하였다. 평가에는 외부 준거 변수인 보안 정책 준수 태도가 사용되었다(cf., [63]). 모델 3은 직접효과를 나타내며, 정보보안 분위기의 1차 요인들이 보안 정책 준수태도에 미치는 영향을 직접효과를 살펴본 것이다. 모델 4는 2차 요인 모델로써 1차 요인간의 상간관계와 이들 요인들이 2차 요인인 정보보안 분위기를 통해 보안정책준수 태도에 미치는 영향을 살펴본 것이다.

2차 요인 모델이 1차 요인 모델보다 더 우수한지를 평가하기 위해서 다음의 두 가지 기준을 활용하였다: (1) 모델의 통계량과 (2) 목표 계수(target coefficient, T). 2차 요인 모형은 더 낮은 모수와 더 많은 자유도를 나타내어 간명도가 뛰어나 더 유용한 모형이라는 결과를 확인할 수 있었다. 목표계수 역시 이론적 최고값인 1에 매우 근사하게 접근하였는데(T = 0.99) 이는 2차 요인 모델이 1차 요인간의 관계를 99%이상 설명한다고 해석할 수 있으며, 2차 요인 모델이 더 우수하다고 평가할 수 있다. 더 나아가, 2차 요인간과 보안 정책 준수태도간의 관계에서 β 계수가 권장 기준치인 0.2이상의 값을 갖는 것으로 나타났으며[13], t-value도 유의하게 나타났다. 정리하면, 이론적으로나 실증적으로 정보보안 분위기는 2차원적 개념이라는 것을 확인할 수 있었다.

마지막으로 본 연구에서는 인구통계학적 데이터 중 정보 보안 행위에 잠재적으로 영향을 미칠 수 있는 요인으로 제시된 나이(age), 성별(gender), 업무 경력(years of working experience)[41][72]과 보안 교육 빈도(security training frequency)와 컴퓨터 활용시간(computer use at work)[31]을 통제 변수로 추가 하였다. 이때 각각의 변수는 표준화하여 사용하였다. 예를 들어 남성은 1, 여성은 2등이 해당된다. 또한 최근 많은 연구에서는 대두된 이론적 견해인 기술적인 스트레스(techno-stress)의 보안 행위에 대한 잠재적 영향을 통제하기 위해 기술 침해(techno-invasion)와 기술 복잡성(techno-complexity) 변수를 추가하였다. 일반적으로 정보통신기술이 개인에게 미치는 영향으로 우선 거론되는 것이 기술적 스트레스(techno-stress)인데 본 개념이 중요하게 언급되는 이유는 이러한 스트레스가 직무의 만족뿐만 아니라 조직에 대한 개인의 몰입에도 영향을 미쳐서 종국에는 개인의 직무성과를 경감시키는 결과까지 초래하기 때문이다[32][54][62][67]. Ragu-Nathan et al.(2008)이 제시한 기술적 스트레스를 유발하는 다섯 가지 요인 중에 침해(techno-invasion), 복잡성(techno- complexity)은 정보보안 측면에서 매우 중요하게 살펴보아야 할 요인이다. 침해란 정보기술의 발전으로 인해 언제 어디서나 업무를 수행할 수 있게 됨으로써 업무와 사생활간에 경계가 모호해지는 상태를 말하는데 개인이 회사를 떠나 업무를 수행하는 경우 정보 보안의 중요성에 대해 사내에서보다 덜 민감해질 수 있기 때문에 매우 중요한 요소라 할 수 있다. 기술의 복잡성은 개인으로 하여금 컴퓨터 역량의 부족함을 느끼게 하여 결국 정보기술에 대한 학습과 이해를 위해 시간을 투자하게 만드는 것을 말하는데, 정보보안 역시 조직원들에게 보안교육 수행 시 정보보안 기술에 대한 이해를 학습시키고 있기 때문에 개인이 느끼는 기술적 복잡성을 가중시킬 수 있다는 점에서



χ^2:2032.911; GFI:.861; RMSEA:.048; NFI:.916; NNFI:.946; CFI:.950

[그림 3] 구조모형 분석 결과

중요하게 고려되어야 하기 때문에 본 연구에서 통제변수로 사용하였다. 모든 인구통계학적 통제변수는 단일 항목으로 측정된 반면에 이 두 통제변수는 다문항 모형으로 측정하였다.

5. 분석 및 결과

5.1 측정모형

본 연구에 사용된 모든 다항변수들의 특성을 표준화된 방법과 탐색적 요인분석을 이용하여 검증하였고, 그 결과가 <표 4>에 나타나 있다. 단일차원성(Unidimensionality), 집중 타당성(convergent validity), 판별 타당성(discriminant validity), 내적일관성(internal consistency)을 요인분석과 Cronbach's alpha를 통해 검증하였다. 탐색적 요인분석 결과 요인 적재치(factor loading)가 0.5이상[8][29]인 값을 갖는 총 6개의 요인이 도출되었고 주목할만한 교차 적재치(cross loading)가 발견되지 않아 본 연구에서 사용된 모든 변수들의 단일차원성이 검증 되었다. 추출된 요인들의 내적일관성(internal consistency)을 측정하는 Cronbach's alpha값도 Nunnally(1978)가 제시한 0.7 보다 훨씬 상회하는 값을 갖는 것으로 나타나 신뢰성 역시 매우 높은 수준을 나타내고 있다.

다음으로 평균분산추출(Average Variance Extracted, AVE)을 평가하여 집중 타당성(convergent validity)을 검증하였는데, 일반적 기준에 의하면 모든 값이 0.7이상이 되어야 신뢰성이 높다고 평가하는데 본 연구의 경우 최소값이 .883으로 나타내 모든 구성개념이 높은 신뢰성을 보유하고 있다고 평가할 수 있다[24][58].

5.2 공통 방법 편의 분석

공통 방법 편의(Common Method Bias)를 사후적으로 검증하기 위해 본 연구에서는 다음의 두 가지 통계적 분석을 수행하였다: (a) Harman의 일요인(one-factor) 검증[50], (b) Lindell and Whitney(2001)의 마커 변수 검증[50]. Harman의 일요인 검증에서, 요인 회전 시 하나의 요인으로 수렴되며 그 분산 설명력이 큰 부분을 차지할 경우 공통방법 편의에 의해 오염되었다고 판단한다[50]. 본 연구에서는 요인 회전 시 단일 요인으로 수렴되지 않았으며, 첫 번째 요인에 의해 설명되는 분산도 전체 77.6%에서 15.9%만 차지하는 것으로 나타났다. 둘째, Lindell and Whitney(2001)의 마커 변수 검증은 모형의 주요 잠재 변수간의 상관관계를 조정하기 위해 이론적으로 관련성이 낮은 마커 변수를 사용하는 방법이다. 마커 변수가 연구에서 제시한 다른 주요 잠재변수와 이론적으

로 관련성이 낮아야 하는 이유는, 높은 상관관계는 공통 방법 편의에 의한 오염으로 발생하기 때문이다. 본 연구에서는 다른 변수와의 이론적 연관성이 매우 적은 변수인 외부활동 선호도(α= 0.95)를 마커 변수로 사용하였다. 본 연구에서 주요 잠재변수간의 평균 상관관계 계수는 낮았으며(r = 0.060, T = 0.448) 유의하지도 않았기 때문에 공통 방법 편의의 증거를 찾아 볼 수 없었다. 정리하면, 본 연구에서 수행한 검증에서 공통 방법 편의에 의한 오염은 심각하지 않다고 결론 내릴 수 있다.

다음으로 AVE의 제곱근 값과 구성개념들 간의 상관관계 계수를 비교하는 방법으로 판별타당성(discriminant validity) 검증을 수행하였다. 표3에서 볼 수 있듯이 모든 AVE 제곱근 값이 구성개념간의 상관관계 계수보다 높게 나타나 각 구성개념이 구별됨을 알 수 있다. 이러한 결과를 통해 개념 타당성(construct validity)도 확보되었다고 볼 수 있는데 일반적으로 표준요인 적재치가 0.5 이상이고, AVE값이 0.5이상이며, 이 값이 구성개념간의 상관관계 계수의 제곱 값 보다 크며, 복합신뢰성이 0.7이상일 경우 개념 타당성이 존재한다고 볼 수 있다[29][42].

5.3 구조 모형(Structural Model)

구조 모형에 대한 검증에 앞서 적합도 점증을 수행하였다. 검증 결과 두 가지 지수가 권장 기준치를 만족시키지 못하였는데(χ^2, GFI) 이에 대한 구체적인 원인을 살펴보면 다음과 같다. 첫째, χ^2(2032.911; df:874; p-value: .000) 검증은 가설모형이 모집단에서 “정확하게” 성립한다는 가설을 가지고 있으므로 모형이 아주 커질 때까지는, 모형과 자료 사이에 심각한 괴리가 있다는 신호를 보낸다. 따라서 가설모형이 대략적으로 적절한 경우에도 χ^2 값은 매우 크게 나와 모형을 기각해야 되는 경우가 많다. 이러한 문제를 보완한 Normed χ^2값은2.32로 나타나 기준값인 1과 3사이의 값을 나타나 만족하고 있다[29]. GFI(0.861)도 마찬가지로 표본크기가 크면 값이 커지게 되며, 표본 크기에 비해 자유도가 상대적으로 크면 값은 작아지게 된다[29]. 하지만 표본 크기에 비교적 덜 민감한 적합도인 CFI, NNFI, RMSEA를 살펴보면 권장 기준치를 훨씬 상회하는 것으로 나타나, 본 연구에서 제안한 모델은 적합한 것으로 볼 수 있다.

본 연구에서 제안한 모형의 가설 검증 결과에 대한 요약은 그림 3과 같다. 첫째, 보안 분위기와 보안 정책 준수 태도간의 경로 계수는 0.411로 가설 2는 유의수준 99.9%에서 통계적으로 지지되는 것으로 나타났다. 이러한 결과는 조직 전반에 걸쳐 보안에 대해 중요하게 여기는 분위기가 조성되면 개인이 인지하여 보안정책을 왜 따라야 하며 보안 정책 준수가 조직의 보안 강화를 위해 매우 중요한 요소라는 것을 깨닫게 된다는 것을 의미한다. 둘째, 보안 정책 준수 태도와 기회주의적 보안 행위간의 경로계수는 -0.174로 가설 3은 99.9% 유의 수준에서 지지 되었다. 하지만 우리가 예상 했던 것과는 달리, 조직의 보안 분위기와 기회주의적 보안 행위간의 경로계수는 0.022로 통계적으로 유의하지 않은 것으로 나타나 가설 1은 기각되었다.이 결과는 조직의 보안 분위기 자체가 개인의 기회주의적 행위를 감소시키는데 직접적으로 기여하는 것이 아니라 이러한 분위기가 개개인의 기업의 보안 정책을 따르려 하는 태도를 바꾸었을 때 이를 통해 개인이 기회주의 적인 보안행위를 지양하게 된다는 것으로 해석되며, 이는 합리적 행위 이론 (Theory of Reasoned Action)의 주장과 일치함을 보여 주고 있다. 이외에 통제변수 중 업무 경력과 기술적 침해가 보안 행위에 유의한 영향을 미치는 것으로 나타났는데, 이는 업무 경력이 많을 경우 보안 정책 준수에 대해 더욱더 불편함을 느껴 정책을 미준수할 가능성이 높음을 의미한다. 또한, 다양한 정보기술로 인해 개인의 사생활이 침해당하고 있다고 느낄 경우 정보 보안에 대해 더욱더 이질감을 느끼게 될 가능성이 높아질 수 있고 볼 수 있다.

6. 결론 및 시사점

본 연구의 목적은 조직 내 보안분위기가 개인의 기회주의적 보안 행위에 미치는 영향을 실증분석하는 것이다. 정보보안 관련 선행연구에서 중요하게 살펴보았던 요소는 기업 내 수립된 보안정책의 준수이다. 즉, 조직원들이 조직에서 수립한 정보보안 정책을 제대로 잘 준수할 경우 정보보안이 향상될 것이라는 것이다[32]. 하지만 여전히 내부직원으로 인한 보안 사고는 끊이지 않고 있다. 이에 대한 원인으로 Chan et al.(2005), Herath and Rao(2009b)는 개인이 느끼는 보안준수와 업무간의 생산성의 상충효과가 존재하기 때문이라 설명하고 있다. 이로 인해 개인은 기회주의적 행동을 선택하게 되고 결국 보안정책준수가 제대로 이루어지지 않고 있다는 것이다.

하지만 이러한 주장은 실증적으로 분석되지 않았다. 이를 본 연구에서는 실증적으로 분석하고자 하였다.

연구목적을 달성하기 위해 본 연구에서는 사회적 정보 처리 접근법(social information processing approach)을 기반으로 하였다. 본 접근법은 조직의 상황적 요인(contextual factors)들이 개인의 직무 인식(job perceptions)을 설명해주고 있다고 제시하고 있다[56]. 본 관점을 기반으로 선행 연구들은 조직 분위기 인식(organizational climate perceptions)이 조직 내 개인의 행동을 결정하는 핵심요인이라는 것을 검증하였다[10]. 본 연구에서는 보안 분위기라는 조직적 요인과 개인의 기회주의적 보안행위와 보안준수 태도라는 개인적 요인간의 관계를 기반으로 연구모형을 수립하였다. 그 이유는 개인과 조직 간에 지속적인 상호작용이 이루어지기 때문에 개인의 행위에 대한 변화 혹은 특정 행위의 유발이 개인적 요인으로만 설명되기에는 한계가 있기 때문이다.

본 연구를 통해 검증된 결과를 살펴보면 다음과 같다. 첫째, 조직의 정보보안 분위기는 조직원들의 기회주의적 보안 행위에 영향을 미치지 않는 것으로 나타났다. 정보보안 분위기에 대한 인식이 증가한다 하더라도 개인의 가치를 기반으로 보안에 대해 거부감을 느끼는 기회주의적 행위의 변화를 유도하지는 못한다고 볼 수 있다. 그러나 본 결과만으로 보안 분위기 자체가 전반적인 보안 행위의 변화를 야기하지 못한다고 볼 수는 없으며 추후 연구에서는 보안 준수행위와 보안 미준수 행위 등의 변수와의 관계를 규명해볼 가치가 있다. 둘째, 정보보안 분위기와 보안정책 준수 태도 간에는 유의한 관계가 존재하는 것으로 나타났다. 본 결과는 행위의 옳고 그름을 판단하는 개인의 판단에 정보보안 분위기가 유의한 영향을 미치는 것으로 행위의 변화에 정보보안 분위기가 행위의 변화에 영향을 미칠 수 있는 가능성이 존재함을 나타낸다. 이를 통해 이미 언급한 바와 같이 본 연구에서 제시한 기회주의적 행위뿐만 아니라 다른 보안 행위를 결과변수로 살펴봄으로 정보보안 분위기가 이러한 행위에 어떠한 영향을 미치는지 살펴볼 가능성을 추가적으로 제시하고 있음을 알 수 있다. 마지막으로 보안정책 준수 태도는 기회주의 행위와 부정적 관계가 존재하는 것으로 나타났다. 즉 조직 내 개인의 기업의 보안을 준수하는 행위가 긍정적 효과를 발생시킨다고 판단할 경우 자신이 그동안 가지고 있던 보안에 대한 부정적 인식 및 행위를 변화시킬 수 있다는 것을 의미한다. 또한 보안 분위기가 기회주의적 보안 행위에 대해서 직접적 영향을 미치지는 않았으나 개인의 태도를 변화시킴으로 간접적으로 태도의 변화를 유발할 수 있다는 점도 발견할 수 있다.

본 연구는 다음과 같은 한계점을 가지고 있다. 첫째, 본 연구는 연구모형의 검증을 위해 설문조사법을 사용하였는데 설문 조사 시 선행변수와 결과변수에 대한 응답을 각각의 응답자가 모두 수행함으로 인해 공통방법오류(common method bias)의 문제에서 자유로울 수는 없다. 물론 사후 검증(post-hoc analysis)을 통해 이를 검증하여 문제가 없음을 제시하기는 하였으나 완전한 해결책이 될 수는 없다는 점이 한계로 제시될 수 있다. 둘째, 잠재변수 중 기회주의적 행위(SMC=.122)와 정보보안 정책준수태도(SMC=.169)의 경우 설명력(explanatory power)이 다소 낮다. 물론 두 변수 모두 최소 기준인 10%를 상회하기는[14] 하나 변수의 설명력을 높일 필요가 있다. 이를 위해 추후 연구에서는 설명력 향상을 위해 해당 변수에 추가적인 측정항목을 개발하여 포함시키거나, 연구모형에 해당 변수의 설명력을 높여줄 수 있는 잠재변수를 추가할 필요가 있다. 셋째, 본 연구에서 사용한 표본추출방법은 비확률표본추출방법(non-probability sampling method) 중 판단표본추출법(purposive sampling)을 사용하였다. 이는 연구문제를 잘 알고 있거나 모집단의 의견을 효과적으로 반영할 수 있을 것으로 판단되는 특정집단을 표본으로 선정하여 조사한 것이다. 그러나 연구결과의 정확한 일반화를 위해서는 확률표본추출방법을 통한 연구도 필요할 것으로 판단된다.

이러한 한계점에도 불구하고 본 연구는 다음과 같은 학술적 그리고 실무적 의의가 있다. 첫째, 기존의 연구가 정보 분위기를 단일 차원에서 접근한 반면[10], 본 연구는 조직 분위기에 관한 기존 문헌을 기반으로 다차원적 접근을 함으로 인해 보안 분위기에 대한 더욱더 구체적인 설명이 가능하다. 즉, 본 연구에서 제시한 보안 분위기의 하위 요인들을 강화함으로써 기업 내 조직원들의 보안 인식 강화 및 전체적인 정보보안 분위기의 활성화가 가능하다. 둘째, 본 연구는 조직적 요인인 보안 분위기와 기회주의적 보안 행위라는 개인적 요인간의 관계를 규명함으로 인해 조직에서 정보보안 방안(countermeasures)을 수립하는데 있어서 실무적인 가이드라인으로 활용될 수 있다. 선행연구의 경우 개인적 요인에 초점을 둔 연구가 주를 이루었는데 이 경우 조직차원에서의 정보보안 대안을 수립하는데 있어서 조직적 관점을 반영하지 못하

고 있기 때문에 실무적 대안을 수립하는데 기여할 수 있는 부분이 제한적이나 본 연구의 경우 조직적 요인과 이를 준수하는 개인과 관련된 요인을 함께 고려함으로 인해 실제 조직차원에서 보안을 효과적으로 관리하는데 기여를 할 수 있다.

D'Arcy and Hovav(2007)는 조직의 정보보안을 위해서는 기술적 접근법(조직원들의 컴퓨터 모니터링, 보안 예방 소프트웨어 설치)이 효과적이기는 하나 이는 단기적 효과를 유발하는데는 적절하나 장기적 효과를 유발하기 위해서는 보안 정책과 보안 인식교육훈련이 요구된다고 제시하였다. 따라서 조직은 장기적인 정보보안을 위해서는 조직원들의 보안정책준수와 보안인식교육을 지속적으로 유지해야 한다. 그러나 D'Arcy et al.(2009)이 제시한 바와 같이 두 가지 보안 대안이 항상 효과적이지는 못하다. 선행연구에서 수행한 실증분석에서도 이 주장과 같은 결과를 제시하고 있다. 이는 본 연구에서 주장하고 있는 바와 같이 모든 보안 대안들이 하나로만 그 효과성을 발현하기 보다는 여러 가지 대안이 종합적으로 작용하여(예, 보안 분위기) 개인에게 인지될 경우 그 본연의 효과를 발휘할 수 있음을 나타낸다고 볼 수 있다. 따라서 실무적으로 정보보안을 위해서는 정보보안에 대한 경영진의 지속적 관심의 표명과 강조가 필요하며, 지속적인 보안인식교육이 함께 수행되어야 한다. 또한 보안 정책도 정책수립자의 관점이 아닌 정책을 따르는 사용자의 입장에서 정책을 수립해야 기업의 추구하는 정보보안 대안들이 그 효과를 발휘할 수 있다.

참 고 문 헌

[1] Ajzen, I., & Fishbein, M. (1980) Understanding Attitudes and Predicting Social Behavior. Englewood Cliff, NJ: Prentice-Hall.

[2] Anderson, J. C., & Gerbing, D. W. (1988). Structural Equation Modeling in Practice: A Review and Recommended Two-step Approach, Psychological Bulletin, 103(3), 411-423.

[3] Ansari, M. A., Baumgartel, H., & Sullivan, G. (1982). The Personal Orientation-Organizational Climate Fit and Managerial Success, Human Relations, 35(12), 1159-1178.

[4] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness, MIS Quarterly, 34(3), 523-548.

[5] Bentler, P. M., & Chou, C. P. (1987). Practical Issues in Structural Equation Modeling, Sociological Methods & Research, 16, 78-117.

[6] Burke, M. J., Borucki, C. C., & Hurley, A. E. (1992). Reconceptualizing Psychological Climate in a Retail Service Environment: A Multiple-Stakeholder Perspective, Journal of Applied Psychology, 77(5), 717-729.

[7] Byrne, B. M. (2010). Structural Equation Modeling with AMOS: Basic Concepts, Applications, and Programming, 2nd ed, New York, NY: Routledge.

[8] Campbell, D. T., & Fiske, D. W. (1959). Convergent and Discriminant Validation by the Multitrait-Multimethod Matrix, Psychological Bulletin, 56(2), 81-105.

[9] Cardinali, R. (1995). Safeguarding Databases: Basic Concepts Revisited, Information Management & Computer Security, 3(1), 30-37.

[10] Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior, Journal of Information Privacy & Security, 1(3), 18-41.

[11] Chan, F., Lee, G. K., Lee, E. J., Kubota, C., & Allen, C. A. (2007). Structural Equation Modeling in Rehabilitation Counseling Research, Rehabilitation Counseling Bulletin, 51(1), 53-66.

[12] Chatterjee, D., Grewal, R., & Sambamurthy, V. (2002). Shaping Up for E-Commerce: Institutional Enablers of the Organizational Assimilation of Web Technologies, MIS Quarterly, 26(2), 65-89.

[13] Chin, W. W. (1998). The Partial Least Squares Approach to Structural Equation Modeling, In G. A. Marcoulides (ed.) Modern Methods for Business Research, Mahwah, NJ: Lawrence Erlbaum Associates, 295-336.

[14] Cohen, J., Cohen, P., West, S. G., & Aiken, L. S. (2003). Applied Multiple Regression/Correlation

Analysis for the Behavioral Sciences, 3rd ed., Erlbaum Associates, NJ:Mahwah.

[15] D'Arcy, J., & Hovav, A. (2007). Deterring Internal Information Systems Misuse, Communications of the ACM, 50(10), 113-117.

[16] D'Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach, Information Systems Research, 20(1), 79-98.

[17] D'Arcy, J., & Herath, T. (2011). A Review and Analysis of Deterrence Theory in the IS Security Literature: Making Sense of the Disparate Findings, European Journal of Information Systems, 20, 643-658.

[18] Denison, D. R. (1996). What is the Difference Between Organizational Culture and Organizational Climate? A Narative's Point of View on a Decade of Paradigm Wars, Academy of Management Review, 21(3), 619-654.

[19] Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User Behaviour towards Protective Information Technologies: The Role of National Cultural Differences, Information Systems Journal, 19, 391-412.

[20] Ernst and Young, (2003). Global Information Security Survey, New York.

[21] Ernst and Young, (2008). Global Information Security Survey, New York.

[22] Foltz, C. B. (2000). The Impact of Deterrent Countermeasures upon Individual Intent to Commit Misuse: A Behavioral Approach, Unpublished doctoral dissertation, University of Arkansas, Fayetteville.

[23] Foltz, C. B., Schwager, P. H., & Anderson, J. E. (2008). Why Users [Fail to] Read Computer Usage Policies, Industrial Management & Data Systems, 108(6), 701-712.

[24] Fornell, C., & Larcker, D. E. (1981). Evaluating Structural Models with Unobservable Variables and Measurement Error, Journal of Marketing Research, 28, 39-50.

[25] Gefen, D., & Straub, D. (2005). A Practical Guide To Factorial Validity Using PLS-Graph: Tutorial And Annotated Example, Communications of the Association for Information Systems, 16, Article 5.

[26] Goel, S., & Chengalur-Smith, I. N. (2010). Metrics for Characterizing the Form of Security Policies, Journal of Strategic Information Systems, 19, 281-295.

[27] Goo, J., Yim, M. S., & Kim, D. (2013). A Path Way to Successful Management of Individual Intention to Security Compliance: A Role of Organizational Security Climate, 46th Hawaii International Conference on System Sciences.

[28] Griffin, M. A., & Neal, A. (2000). Perceptions of Safety at Work: A Framework for Linking Safety Climate to Safety Performance, Knowledge, and Motivation, Journal of Occupational health Psychology, 5(3), 347-358.

[29] Hair, Jr. J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). Multivariate Data Analysis, 7th ed., Upper Saddle River, NJ: Prentice Hall.

[30] Harrington, S. J. (1997). A Test of a Person-Issue contingent Model of Ethical Decision Making in Organization, Journal of Business Ethics, 16, 363-375.

[31] Herath, T., & Rao, H. R. (2009a). Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness, Decision Support Systems, 47(2), 154-165.

[32] Herath, T., & Rao, H. R. (2009b). Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations, European Journal of Information Systems, 18(2), 106-225.

[33] Herath, T., Yim, M. S., D'Arcy, J., Nam, K., & Rao, H. R. (2011). Examining Employee Security Behavior: A Moral Disengagement Perspective", IFIP 2011 Dewald Roode Information Security Workshop.

[34] James, L. A., & James, L. R. (1989). Integrating Work Environment Perceptions: Explorations into

the Measurement of Meaning, Journal of Applied Psychology, 74(5), 739-751.

[35] Johnston, A. C., & Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study, MIS Quarterly, 34(1), 1-20.

[36] Joshi, A. W., & Sharma, S. (2004). Customer Knowledge Development: Antecedents and Impact on New Product Performance, Journal of Marketing, 68, 47-59.

[37] Kim, D. J., Ferrin, D. L., & Rao, H. R. (2008). A Trust-based Consumer Decision-making Model in Electronic Commerce: The Role of Trust, Perceived Risk, and Their Antecedents, Decision Support Systems, 44, 544-564.

[38] Kline, R. B. (2005). Principles and Practice of Structural Equation Modeling, 2nd ed., Guilford Press.

[39] Lindell, M. K., & Whitney, D. J. (2001). Accounting for Common Method Variance in Cross-Sectional Research Designs, Journal of Applied Psychology, 86(1), 114-121.

[40] Loch, K. D., Carr, H. H., & Warkentin, M. E. (1992). Threats to Information Systems: Today's Reality, Yesterday's Understanding, MIS Quarterly, 16(2), 173-186.

[41] Loe, T. W., Ferrell, L., & Mansfield, P. (2000). A Review of Empirical Studies Assessing Ethical Decision Making in Business, Journal of Business Ethics, 25, 185-204.

[42] Malhotra, M. K., and Grover, V., "An Assessment of Survey Research in POM: From Constructs to Theory", Journal of Operations Management, Vol. 16, 1998, pp. 407-425.

[43] Malhotra, N. K., Kim, S. S., & Patil, A. (2006). Method Variance in IS Research: A Comparison of Alternative Approaches and a Reanalysis of Past Research, Management Science, 52(12), 1865-1883.

[44] Meyers, L. S., Gamst, G., & Guarino, A. J. (2006). Applied Multivariate Research: Design and Interpretation, Thousand Oaks, California:SAGE Publications.

[45] Neal, A., Griffin, M. A., and Hart, P. M., "The Impact of Organizational Climate on Safety Climate and Individual Behavior", Safety Science, Vol. 34, 2000, pp. 99-109.

[46] Neubaum, D. O., Mitchell, M. S., & Schminke, M. (2004). Firm Newness, Entrepreneurial Orientation, and Ethical Climate, Journal of Business Ethics, 52, 335-347.

[47] Nunnally, J. C. (1978). Psychometric Theory, 2nd ed., New York, McGraw-Hill.

[48] Ocasio, W. (1997). Towards an Attention-based View of the Firm, Strategic Management Journal, 18, 187-206.

[49] Pavlou, P. A., & Fygenson, M. (2006). Understanding and Predicting Electronic Commerce Adoption: An Extension of the Theory of Planned Behavior, MIS Quarterly, 30(1), 115-143.

[50] Podsakoff, P. M., & Organ, D. W. (1986). Self-Reports in Organizational Research: Problems and Prospects, Journal of Management, 12(4), 531-544.

[51] Preston, D. S., & Karahanna, E. (2009). Antecedents of IS Strategic Alignment: A Nomological Network, Information Systems Research, 20(2), 159-179.

[52] Purvis, R. L., Sambamurthy, V., & Zmud, R. W. (2001). The Assimilation of Knowledge Platforms in Organizations: An Empirical Investigation, Organization Science, 12(2), 117-135.

[53] Puhakainen, P., & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study, MIS Quarterly, 34(4), 757-778.

[54] Ragu-Nathan, T. S., Tarafdar, M., Ragu-Nathan, B. S., & Tu, Q. (2008). The Consequences of Technostress for End Users in Organizations: Conceptual Development and Empirical Validation, Information Systems Research, 19(4), 417-433.

[55] Richardson, R. (2012). 2010/2011 Computer Crime and Security Survey, Computer Security Institute.

[56] Salancik, G. R., & Pfeffer, J. (1977). An Examination of Need-Satisfaction Models of Job Attitudes, Administrative Science Quarterly, 22(3),

427-456.

[57] Salancik, G. R., & Pfeffer, J. (1978). A Social Information Processing Approach to Job Attitudes and Task Design, Administrative Science Quarterly, 23(2), 224-253.

[58] Segars, A. (1997). Assessing the Unidimensionality of Measurement: A Paradigm and Illustration within the Context of Information Systems Research, Omega, 25(1), 107-121.

[59] Siponen, M., & Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations, MIS Quarterly, 34(3), 487-502.

[60] Straub, D. W. (1990). Effective IS Security: An Empirical Study, Information Systems Research, 1(3), 255-276.

[61] Tagiuri, R., & Litwin, G. (1968). Organizational Climate: Explorations of a Concept, Boston: Harvard Business School.

[62] Tarafdar, M., Tu, Q., Ragu-Nathan, B. S., & Ragu-Nathan, T. S. (2007). The Impact of Technostress on Role Stress and Productivity, Journal of Management Information Systems, 24(1), 301-328.

[63] Tanriverdi, H. (2006). Performance Effects of Information Technology Synergies in Multibusiness Firms", MIS Quarterly, 30(1), 57-77.

[64] Treiblmaier, H., & Filzmoser, P. (2010). Exploratory Factor Analysis: How Robust Methods Support the Detection of Hidden Multivariate Data Structures in IS Research, Information & Management, 47, 197-207.

[65] Theoharidou, M., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2005). The Insider Threat to Information Systems and the Effectiveness of ISO17799, Computers & Security, 24, 472-484.

[66] Victor, B., & Cullen, J. B. (1988). The Organizational Bases of Ethical Work Climates, Administrative Science Quarterly, 33, 101-125.

[67] Wang, K., Shu, Q., & Tu, Q. (2008). Technostress under Different Organizational Environments: An Empirical Investigation, Computers in Human Behavior, 24, 3002-3013.

[68] Wimbush, J. C., & Shepard, J. M. (1994). Toward an Understanding of Ethical Climate: Its Relationship to Ethical Behavior and Supervisory Influence, Journal of Business Ethics, 13, 637-647.

[69] Wimbush, J. C., Shepard, J. M., & Markham, S. E. (1997). An Empirical Examination of the Relationship between Ethical Climate and Ethical Behavior form Multiple Levels of Analysis, Journal of Business Ethics, 16, 1705-1716.

[70] Wyld, D. C., & Jones, C. A. (1997). The Importance of Context: The Ethical Work Climate Construct and Models of Ethical Decision Making- An Agenda for Research, Journal of Business Ethics, 16, 465-472.

[71] Yoon, C. (2011). Theory of Planned Behavior and Ethics Theory in Digital Piracy: An Integrated Model, Journal of Business Ethics, 100(3), 405-417.

[72] Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of Perceived Technical Protection on Security Behaviors, Information Management & Computer Security, 17(4), 30-340.

임 명 성

- 2002년 2월: 삼육대학교 경영정보학과 경영학사
- 2004년 2월: 한국외국어대학교 경영정보대학원 M.B.A.
- 2011년 8월: 서강대학교 경영전문대학원 Ph.D.
- 2011년: 서강대학교 경영학부 대우교수
- 2012년~현재: 삼육대학교 경영학과 조교수
- 관심분야: 정보보안, 서비스 시스템, 기술 혁신
- E-Mail: msyim@syu.ac.kr