조직 구성원들의 정보보안 정책 위반에 영향을 미치는 요인

임명성*

Understanding an Employee Information Systems Security Violations

Myung-Seong Yim*

요 약 본 연구의 목적은 왜 조직 구성원들이 정보보안 정책을 위배하는지에 대해 알아보기 위해 도덕적 해방이론을 기반으로 수행되었다. 분석 결과 도덕적 신념과 처벌에 대한 인지는 보안 정책 위배에 유의한 영향을 미치는 것으로 나타났다. 반면 도덕적 해당이 존재할 경우 처벌에 대한 인지는 유의하지 않은 것으로 나타났다. 마지막으로 정보보안 인식교육과 도덕적 신념, 그리고 처벌에 대한 인지는 도덕적 해방에 유의한 영향을 미치는 것으로 나타났으며, 도덕적 해방은 정보보안 정책 위배에 유의한 영향을 미치는 것으로 나타났다.

주제어 : 정보보안, 보안 정책, 도덕적 해방, 정책 위반, 정책 준수

Abstract The purpose of this paper is to find an answer why employees in organization violate the organizational information security policy. To do this, this study is rooted in the moral disengagment theory. This study found that moral belief and perceived sanction have an effect on security policy violation. However, if moral disengagement is involved in the research model, perceived sanction is not significant. Finally, SETA, moral belief, and perceived sanction have a negative effect on moral disengagement, which in turn moral disengagement influences positively the security policy violation. The conclusions and implications are discussed.

Key Words : Information Security, Security Policy, Moral Disengagement, Policy Violation, Policy Compliance

1. 서론

기업의 정보보안을 위해 중요한 것은 무엇인가? 물론 여러 가지가 있으나 가장 우선적으로 내부 단속, 즉 내부 직원들의 정보보안 정책 준수가 조직의 정보보안 문제의 핵심 중 하나이다[47]. 여러 연구에 따르면 정보시스템 보안사고의 절반이상이 조직원들의 보안 정책 준수가 제대로 이루어지고 있지 않아 발생하고 있다고 보고하고 있다[18][51]. 따라서 조직 구성원들의 정보시스템 보안 정책의 미준수 문제(정보보안 정책 위배)가 조직의 정보보안을 위해 시급히 해결되어야 한다. 정보보안 정책 위배(information security policy violation)란 조직 구성원들의 자신의 컴퓨터를 활용하여 스스로의 이익을 위해 수립된 조직의 규율이나 정책에 반하는 행위를 하는 것을 말한다[28]. 예를 들어, 인가되지 않는 데이터나 시스템에 접근하거나, 자신의 이익을 위해 회사의 기밀 데이터를 제 삼자에게 전달하거나 판매하는 행위 등 다양한 행위들이 해당된다[28].

정부 규제뿐만 아니라 보안 기술, 조직 정책과 절차와 같은 보안 체계(security system) 요소들의 효과는 주로 조직 내 구성원들의 노력에 달려 있다[28]. 따라서 기존 연구들은 어떻게 하면 정보보안 정책을 준수하도록 유도할 수 있는지에 대해 많은 연구를 수행해 왔으며, 이를 위해 다양한 이론들이 활용되어 왔다. 하지만 기존 연구에서 사용한 이론들은 다음과 같은 한계점이 있다.

*삼육대학교 경영학과 조교수
논문접수: 2013년 1월 2일, 1차 수정을 거쳐, 심사완료: 2013년 1월 20일, 확정일: 2013년 2월 20일

처벌에 대한 두려움을 유발시켜 비도덕적 행위를 억제시킨다는 일반제제이론(General Deterrence Theory)은 내부인들이 처벌에 대해 완전히 이해하고 있어야 본래의 효과를 발생시킬 수 있다[1]. 따라서 자신의 행위가 어떠한 처벌 대상이 되는지에 대해 인지하지 못하고 있을 경우 비도덕적 행위가 억제되기 어렵다.

예방동기이론(Protection Motivation Theory)은 위협의 심각성, 사건의 발생 가능성, 사건에 대한 대응을 위한 효용 등과 같은 공포전달에 의한 영향이 인간의 태도변화를 유발한다는 것을 규명한 이론으로 예방행위를 형성하는데 기여를 하였다. 그러나 여전히 공포위협메시지와 인간의 수용행위간의 관계는 여전히 명확하지 않다는 문제점이 존재한다[1].

또한 이들 이론들은 왜 조직구성원들이 보안정책을 위반하는지에 대한 이유를 설명하지 못한다. 단지 보안정책위반 행위를 억제 혹은 예방하는 사전적 행위를 설명해주기 때문에 현실적으로 많이 발생하는 보안 정책위반행위가 무엇 때문에 발생하고 있는지 그 이유를 설명하지 못한다.

따라서 본 연구는 다음과 같은 연구문제에 대한 해결책을 제시하고자 수행되었다. 첫째, 왜 조직 구성원들은 정보보안 정책을 위반하는가? 이를 위해 도덕적 해방(Moral Disengagement)이론을 활용하였다. Bandura에 의해 개발된 도덕적 해당이론은 왜 사람들이 사회적으로 부적절한 행위에 몰입하게 되는지를 설명해주는 이론으로 활용되어 왔다[2][17][29]. 본 이론에 따르면 사람들은 비윤리적 행위를 억제시켜주는 도덕적 자기 규제 과정(moral self-regulatory processes)이 여러 가지 상호연관된 인지적 메커니즘(도덕적 해방)을 활용함으로 인해 비활성화될 경우 비윤리적 행위를 하게 된다고 제시하고 있다[17]. 따라서 본 이론은 왜 일반적인 사람들이 명백한 죄책감 혹은 자기 질책 없이 비윤리적 행위에 몰입하게 되는지를 설명해준다[5]. 따라서 본 연구에서는 도덕적 해당이론을 활용하여 보안정책의 준수가 중요함에도 불구하고 조직 구성원들이 이를 따르지 않고 위반하려하는지를 설명하고자 한다. 둘째, 도덕적 해방이 기존 보안대책에 어떠한 영향을 미치는가? 도덕적 해방의 영향을 살펴봄으로 인해 본 개념이 기존이 보안 정책 중 무엇을 상쇄시키는지 살펴봄으로 인해 왜 도덕적 해방이 중요한지 살펴보고자 한다.

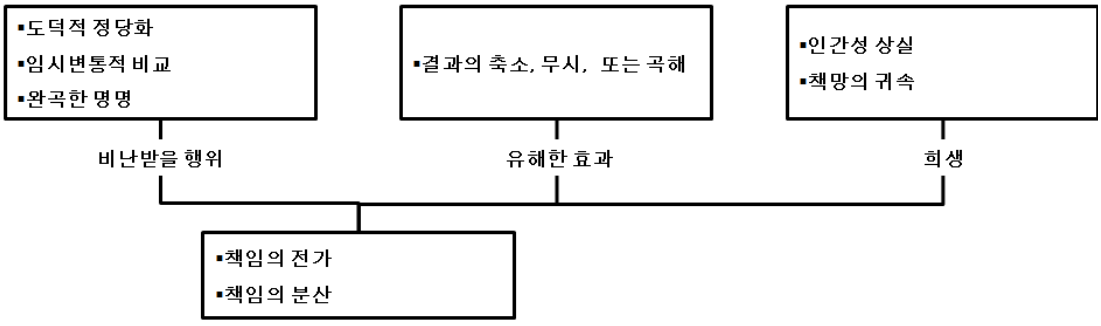
최근 연구에 따르면 포괄적인 정보 보안 정책과 절차를 수립하고 조직 구성원들을 대상으로 정보 보안에 대한 인지 훈련을 수행하고, 보안 위반 행위에 대한 명확하고, 강력한 처벌을 하게 되면 보안 정책 위배행위를 줄일 수 있다고 제시하고 있다[28]. 따라서 본 연구에서는 이러한 요인들이 보안 정책 위배를 줄일 수 있는지 또한 도덕적 해방과 어떠한 관련이 있는지 살펴보고자 한다.

본 연구는 다음과 같이 구성되었다. 2장에서는 도덕적 해방이론에 대해 구체적으로 살펴보고 관련 가설을 제시한다. 3장에서는 데이터 수집을 통해 제시된 가설을 검정하고 관련 결과를 정리하여 제시하였다. 마지막 4장에서는 3장에서 도출된 가설검정결과를 기반으로 결과를 해석하고 본 연구의 이론적 그리고 실무적 함의와 한계점에 대해 논의하였다.

2. 도덕적 해방이론과 가설

사회인지이론(Social Cognitive Theory)에 따르면 대부분의 사람들의 행동은 사전숙고(forethought)에 의해 통제받는다[6]. 사람들은 자신이 무엇을 할 수 있는지에 관한 신념을 형성하고, 자신이 수행할 활동으로 인한 가능한 결과를 예상하고, 그들 스스로 목표를 설정하고, 예상 결과를 달성하기 위해 필요한 행동방침(courses of actions)을 계획한다[6]. 사회인지이론에서, 도덕적 추론(moral reasoning)은 도덕적 대리(moral agency)가 활성화되는 경우 감성적 자기 규제 메커니즘(self regulatory mechanism)을 통해 도덕적 행위와 연결된다. 자기 규제 메커니즘은 활성화되기 전까지 발휘되지 않는다[7]. 이러한 선택적 활성화(몰입, engagement)와 내부 통제로부터의 해방(disengagement)은 동일한 도덕적 기준안에서 다른 유형의 행위를 유발하게 만든다[8].

옳은 행동으로 부터의 해방(이탈)은 이탈행위의 정당화, 비교완화, 해당 행위에 대한 언어적 유희 등을 활용하여 이탈 행위를 재정립하여 준다. 도덕적 해방은 [그림 1]에서 제시한 세 가지 집합으로 구성된다. 첫번째 집합은 유해한 행동을 수용할 수 있는 행동으로 인지적 변환을 시키는 요인들의 집합으로 도덕적 정당화(moral justification), 임시변통적 비교(behavioral contrast), 완곡한 명명(euphemistic labeling) 등이 해당된다[7]. 첫 번째 집합이 자기 규제 작용으로 부터의 해방을 위한 가장 효과적인 심리적 메커니즘이다. 도덕적 해방을 위한 두



[그림 1] 도덕적 해방이론

번째 집합은 올바른 행위와 올바르지 못한 행위간의 관계와 올바르지 못한 행위로 인해 발생하는 영향에 대해 왜곡하는 것을 포함한다[7]. 또한 가해자는 책임의 전가나 분산을 통해 피해를 발생시키는데 있어서 자신의 역할을 최소화하려 한다. 개인은 자신의 행동으로부터 발생할 수 있는 피해에 대해 축소하거나, 무시하거나 곡해함으로 인해 자신의 행위로 인해 발생하는 유해한 영향을 포장하려하며, 이를 통해 도덕적으로 해방된다. 세 번째 도덕적 해방을 위한 집합은 학대 희생자들(피해자들)을 비난이나 모욕하는 것을 포함한다.

다음은 세부적인 도덕적 해방 요인들과 해당 요인들이 정보보안과 어떻게 관련되는지 살펴보고자 한다.

도덕적 정당화: 개인은 자신의 행동이 옳다고 정당화할 수 있기 전까지 유해한 행동에 몰입하지 않는다. 따라서 개인의 잘못된 행동이 인지적 재구성(cognitive reconstruction)을 통해 옳은 것으로 바뀌게 되면 유해한 행동에 몰입하게 된다. 이 과정에서 개인은 자신의 잘못된 행위가 사회적으로 가치있거나 타당한 목적을 가지고 있는 것으로 여기면서 개인적으로나 사회적으로 수용할 수 있다고 여긴다. 따라서 많은 경우 개인의 잘못된 행위는 영예나 명성을 보호하기 위함이였다고 정당화하려한다[13]. 정보보안 행위 측면에서 도덕적 정당화는 업무 수행과 밀접하게 관련된다. 일반적으로 높은 수준의 정보보안은 조직 구성원의 수행하는 업무의 유연성을 제약하기도 하며, 심지어는 업무 생산성을 저해한다고 여겨지기까지 한다. Post and Kagan(2006)의 연구에 따르면, 기업이 높은 수준의 보안을 요구할 경우 조직 구성원은 자신의 업무 생산성에 장벽으로 느낀다는 실증분석 결과를 제시하였다. 따라서 조직 구성원들이 업무를 더욱 효율적으로 완료하거나 업무의 마감일정을 지키기기 위해서 정보보안 준수를 위배할 수 있다.

임시변통적 비교: 특정한 행위가 어떻게 보여지는 가는 부분적으로 비교 대상이 무엇인지에 의해 영향을 받는다. 수용되지 못할 행위는 때로 더욱더 비난받을 행위와 비교되어짐으로써 옳은 행위로 변모될 수 있다[8]. 따라서 지나친 비교 행위는, 자신의 비난받을 행위를 사소한 것으로 보여지는 데 일조한다. 정보보안 측면에서, 안티바이러스 프로그램을 끄거나 자신의 비밀번호를 타인과 공유하는 것과 같은 실수 행위를 사내 정보를 훔치는 행위와 같은 더욱더 심각한 행위와 비교함으로 자신의 행위를 정당화시키려고 하는 것이 해당된다.

완곡한 명명: 언어는 행위가 기반이 되는 사고 패턴을 형성하고, 행위는 스스로 어떻게 명명하느냐에 따라 다른 형태를 띨 수 있다[8]. 장황하게 포장된 언어로 인해 자신의 잘못된 행위는 이익이 되는 행위로 변환되며, 이로 인해 해당 행위에 대한 책임감으로부터 자유로워질 수 있다. 이러한 과정은 잘못된 행위를 포장할 수 있는 또 다른 도구중 하나이다. 정보보안 상황에서 보안 정책을 준수하지 않는 것이 자신의 업무를 달성하기 위해 어쩔 수 없었다는 말로 포장될 수 있다. 만약 조직원들에게 자신의 보안 정책 미준수 행위가 중차대한의 일이 아니라고 명명되어질 경우, 이러한 사고가 그들의 보안 행위로 이어질 수 있다.

결과의 축소, 무시, 또는 곡해: Bandura(1996)는 자신이 수행한 행위에 의한 결과에 대한 무시 혹은 곡해는 스스로 해당 행위에 대한 억제 반응을 약화시킨다고 주장하였다. 피해가 가시적이지 않을 경우, 개인은 피해를 주

는 행위를 지속할 가능성이 높다. 예방동기이론에 따르면, 전반적인 위협에 대한 평가 혹은 고려는 개인의 보안 행위 태도에 영향을 미친다[44][45]. 따라서 조직 구성원들의 보안 행위는 위협 혹은 피해에 대한 스스로의 이해에 의해 형성된다[24]. 인지된 보안 위협의 심각성과 인지된 보안 위배 가능성은 보안 위협에 대한 전반적 고려에 기인한다. Hu and Dinev(2005)에 따르면 조직 구성원이 잠재적 피해에 대해 인지할 경우, 스스로를 보호하는 행위를 취할 가능성이 높아진다고 제시하였다. 만약 자신의 행위로 인한 피해가 무시괴고, 축소되고, 곡해된다면 스스로를 책망할 이유가 줄어들게 된다[7].

인간성 상실: 자기 견책(self-censure)의 강도는 얼마나 가해자(perpetrator)가 피해를 입힌 사람들에 대해 생각하는지에 달려있다. 정보보안 측면에서 자신의 행위로 인한 피해는 조직에 가해지는 것이기 때문에 조직 구성원들의 행위는 조직과 밀접하게 관련된다. 구성원이 조직에 대한 애착심(commitment)이 결여된 경우 혹은 조직에 대한 반감(ill feeling)을 가지고 있는 경우 조직에 대해 이질감을 느끼게 되며, 결국 잘못된 보안 행위를 저지를 가능성이 높아진다. Bandura(2002)가 제시한 인간화(humanization)의 힘에 따르면, 대부분의 사람들은 자신이 어떠한 집단의 일원이라 느낄 경우 피해 행위를 수행하는 것을 거부한다고 제시하였다. 자신이 소속된 조직에 대한 소속감으로 정의되는 조직 몰입(organizational commitment)은 조직 구성원과 해당 조직 간의 관계에 대한 개념을 정립해 준다[36]. 조직 구성원들의 해당 조직에 대한 몰입은 조직의 보안 정책 준수와 같은 보안 행위에 몰입하는데 중요한 역할을 한다[24].

책망의 귀속: 환경에 대한 책망은 자신의 잘못된 행위를 스스로 면책할 수 있는 또 다른 수단이 된다. 자신의 피해 행위는 자신의 의사가 아닌 환경적 요인으로 인한 것으로 보이게 만들 수 있다. 개인은 자신의 행동이 통제할 수 없는 환경이나 주변 상황에 의한 것으로 주장할 수 있다[54]. 만약 환경이 옳은 행위를 촉진하거나 유발할 수 없을 경우, 피해행위를 수행한 것이 가해자에 의해 정당화 될 수 있다. 정보보안 측면에서 이는 보안정책 문서나 주기적 훈련과 같은 환경과 관련된다[16][24]. 만약 이러한 조건이 제대로 보급되지 않을 경우 조직 구성원들은 보안 행위에 몰입하지 않을 가능성이 높다.

책임의 전가: 개인은 어떠한 행위에 대한 자신의 책임에 대해 숙고하기보다는 타인을 비난하고자 한다. 이와 같은 책임의 전가는 결국 자신의 이탈 행위에 대한 책임을 거부하는 것이다[8][46][54]. 개인은 자신의 행위가 스스로의 책임보다는 지시에 의해 수행되었다고 보는 경향이 있다. 만약 상급자가 어떠한 행위과정에 대한 고려 없이 결과만 요구한다면, 자신의 행위에 대한 실제 주체는 자신이 아니라고 생각한다[7]. 따라서 자신의 유해한 행위에 대한 책임으로부터 자유로울 수 있다. 또한 개인은 자신이 수행한 행위가 지시를 전달받는 상황에서 오해로 인해 발생하였다고 항변할 수 있다.

책임의 분산: 책임은 분업(division of labor)에 의해 분산될 수 있다[8]. 집단 행위는 통제를 약화시킬 수 있는 수단중 하나로써[7], 모두가 책임이 있음에도 불구하고 누구도 책임을 통감하지 못한다. 정보보안 측면에서 정보시스템을 안전하게 유지하는 것은 관리자의 책임 혹은 IT(information technology) 부서의 책임이라고 구성원들은 인식할 있다. 또한 조직 내에서 다른 구성원들도 정보보안 정책에 위배된 행위를 하게 될 경우 이러한 행위는 자신만의 책임이 아니라고 인지할 수 있다. 이러한 책임의 분산은 조직 구성원들이 보안 정책 준수 행위로부터 자유롭게 만들 수 있다.

선행연구를 살펴보면 위에 제시한 8가지 도덕적 해당을 위한 기제가 하나의 요인으로 묶인다는 것을 알 수 있다[6][7][8]. 이는 본 이론을 활용한 응용 연구에서도 살펴볼 수 있는데 이러한 결과는 결국 자신을 정당화하는데 있어서 하나의 도덕적 해방 기제를 사용하기 보다는 여러 가지 도덕적 기제를 활용하여 자신을 최대한 방어하고자 함을 알 수 있다. 본 연구에서 역시 이 모든 기제가 하나의 요인 구조로 나타났다. 따라서 이를 하나의 요인으로 보는 것이 적절하다고 판단된다.

개인은 자신의 잘못된 행위에 대한 책임을 인정하기보다는 자신의 행위를 항변할 수 있는 여지가 있을 경우 이를 먼저 활용하는 경향이 있다. 따라서 이러한 도덕적 책임에서 자유로울 수 있는 도덕적 해방이 존재할 경우 자신의 행위가 정당화 될 수 있다고 믿게 된다. 따라서 보안 측면에서도 정보보안 정책을 준수하지 않는 것이 어떠한 이유가 있기 때문이라고 자신을 변호할 수 있다. 따라서 다음의 가설을 제시할 수 있다.

H1. 도덕적 해방은 보안 정책 위반에 정(+)의 영향을 미칠 것이다.

정보보안 인식 교육 프로그램(SETA, Security Education, Training, and Awareness Program)은 다양한 유형이 존재하지만, 그 목적은 조직 구성원에게 정보보안 환경에 대한 일반적인 지식을 전달함과 동시에 보안 절차를 준수함에 있어서 필요한 기술(Skills)을 고양할 할 수 있도록 하는 것이다[16].

기업에서 활용하는 다양한 정보보안 대책(countermeasures)들이 존재한다. 일반적으로 사용되는 보안 대책은 보안 정책, 정보보안 인식 교육 프로그램, 컴퓨터 모니터링, 예방 소프트웨어, 처벌 등이 있다. D'Arcy and Hovav(2007)의 조사에 따르면 많은 조직 구성원들이 보안정책에 대한 인식 수준은 가장 높은 반면, 보안 인식 교육프로그램에 대한 인식은 가장 낮은 것으로 나타났다. 이는 기업들이 단기적인 효과 혹은 즉각적인 효과를 볼 수 있는 방법이 보안정책 준수나 모니터링과 같은 보안 대책들이기 때문에 기업들은 빠른 시간 안에 가시적인 성과를 달성하기 위해 이러한 단기적인 접근에 의존하는 경향이 강하다고 볼 수 있다[15]. 하지만 장기적인 관점에서 조직 구성원들의 보안 강화를 위해서는 인식 전환이 선행되어야 하며 이를 위해서는 꾸준한 교육이 제공되어야 한다[15]. 이러한 관점에서 정보보안 인식 교육 프로그램은 보안 정책 위반을 억제시킬 수 있는 중요한 선행요인이 될 수 있다.

H2. 정보보안 인식 교육 프로그램은 보안정책 위반에 부(-)의 영향을 미칠 것이다.

도덕적 신념(moral belief)이란 자신의 행동이 도덕적으로 잘못된 것인지 스스로 인지하는 수준을 말한다[25]. 즉, 도덕적 신념은 특정한 행위에 대한 옳고 그름의 개인적 판단을 말한다[28]. 도덕적 신념이 강한 사람의 경우 자신이 도덕적으로 잘못된 행위를 수행하게 되면 죄책감 혹은 수치심을 느끼게 되어 해당행위에 몰입하는 것을 중단한다[25][28]. 따라서 도덕적 신념은 특정 행위를 수행함으로 인해 발생할 수 있는 무형의 비용으로 볼 수 있다[25]. 범죄행위로 인해 발생할 수 있는 이러한 잠재적 비용으로인해 도덕성(morality)은 사실상 옳은 행동을 위한 표준이 되어 도덕적 관점에서 법규, 절차, 규범 등을 준수하도록 한다[25].

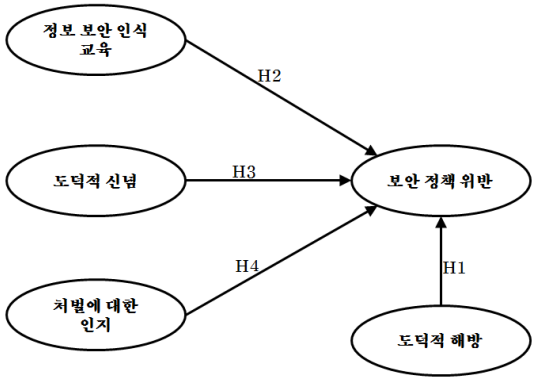
범죄자는 처벌에 대한 공포 때문이 아니라 해당 행동이 도덕적으로 잘못된 것이라고 판단될 경우 부적절한 행동을 스스로 억제하는 경향이 있다[49]. 왜냐하면 개인이 도덕적 숙고(moral consideration)를 하게 되면, 처벌 인식에 대한 영향은 줄어들기 때문이다[16]. 따라서 다음의 가설을 제시할 있다.

H3. 도덕적 신념은 보안정책 위반에 부(-)의 영향을 미칠 것이다.

일반적 제제 이론(GDT, General Deterrence Theory)에 따르면 잘못된 행동에 대한 처벌의 확실성(certainty)과 혹독함(severity)이 높을수록 개인은 해당 행위를 억제하게 된다고 한다[16]. 확실성이란 처벌될 가능성을 말하며, 혹독함이란 처벌 수위를 나타낸다[23].

처벌(formal sanctions)이란 위법행위에 부과되는 명시적 처벌(penalties)을 의미한다[49]. 혹독함(severity)과 확실성(certainty)은 처벌의 효과성을 결정하는 중요한 요인이다[49]. 더욱더 강력하거나 효과적인 처벌은 바람직하지 못한 행위에 대한 제약으로 작용한다[49]. 기존의 범죄학 분야에서 수행한 연구들에 따르면 처벌의 확실성이 혹독함보다 억제 효과가 더 크다고 제시한 반면 몇몇 연구들은 혹독함이 처벌의 확실성보다 억제 효과가 크기보다는 둘 다 모두 강력한 억제 효과가 있다고 주장하기도 하였다[16]. 즉, 처벌의 확실성과 혹독함은 모두 이탈행위, 비도덕적 행위 등 잘못된 행위를 억제하는 역할을 한다는 것이다.

H4. 처벌에 대한 인지는 보안 정책 위반에 부(-)의 영향을 미칠 것이다.



[그림 2] 연구모형

3. 분석

연구모형에서 제시된 관계와 가설을 검증하기 위해 필요한 데이터를 수집하기 위해 설문 조사법을 활용하였다. 본 연구에 사용된 측정항목들은 선행연구에서 신뢰성이 검증된 항목들을 사용하였다. 정보보안인식교육에 사용된 7개 항목과 처벌에 대한 인지에 관한 3개 항목은 D'Arcy et al.(2009)에서 사용된 측정항목들을 사용하였으며, 보안정책위반을 측정하기 위한 2개 항목은 Hu et al.(2011)에서 사용한 항목을 도덕적 신념을 위한 2개의 항목은 Siponen et al.(2012)에서 사용한 항목을 사용하였다. 도덕적 해방에 관한 항목은 Bandura(1986;1991;2002), Bandura et al.(1996)에서 사용한 항목을 본 연구의 정황에 맞게 수정한 후 사용하였다. 수정은 미국 소재 대학 교수 1명, 캐나다 소재 대학 교수 1명, 미국에 거주하는 한국인 IT전문가 한명, 미국에서 경영학 박사과정에 있는 한국인 학생 한명, 국내 소재 대학 교수 1명이 함께 설문문항의 타당성과 적합성을 검토하였으며 이들 간의 총 5회의 걸친 논의와 피드백을 통해 최종항목을 선정하였다. 각각의 측정항목들은 Likert type 7점 척도법을 활용하여 응답하도록 하였다.

설문은 2012년 3월부터 6월까지 3개월간 총 500개의 설문을 우편배포방식과 이메일 배포방식을 활용하여 배포 및 수집하였으며, 이중 266개의 응답을 받을 수 있었다. 이중 일관된 응답(동일한 값으로 대부분의 항목에 응답), 무응답과 같은 결측치가 있거나 중복응답이 있어서 최종분석에 사용하기에 적합하지 않은 27개를 제외하고 239개의 응답을 최종분석에 사용하였다. 응답자들의 특성에 대한 분석 결과는 <표 1>에 제시하였다.

3.1 측정모형 분석

본 연구에서는 제안 모형의 요인 타당성(factor validity)과 신뢰성(reliability)을 확보하기 위해 PLS 타당성 검증 절차를 따랐다. PLS기법은 탐색적 이론 구축 연구에 유용하며, 측정모형과 구조모형을 동시에 평가할 수 있다는 장점이 있기 때문에[11][49] 본 연구를 수행하는데 유용하다고 판단된다.

연구모형의 집중타당성(convergent validity)을 위해 bootstrapping을 이용한 재표집 방법을 통해 500개 표본을 활용한 분석을 수행하였다[53]. 확인된 개념들에 속한 항목들의 요인 적재값에 대한 t값을 살펴본 결과 모두 $p<0.001$ 수준에서 유의한 것으로 나타났다. 또한 평균분산추출 값은 0.5이상 되어야 한다[20]. <표 3>에 나타나 있듯이 평균분산추출의 최소값이 0.6455로 본 기준을 만족하고 있다.

〈표 1〉 응답자 특성 분석

항목	구분	빈도	비율
성별	남성	168	70.3%
	여성	68	28.5%
	무응답	3	1.3%
연령대	1	3	1.3%
	2	109	45.6%
	3	109	45.6%
	4	18	7.5%
학력	1	1	0.4%
	2	17	7.1%
	3	161	67.4%
	4	49	20.5%
	5	6	2.5%
	무응답	5	2.1%
직위	1	3	1.3%
	2	70	29.3%
	3	75	31.4%
	4	61	25.5%
	5	27	11.3%
	무응답	3	1.3%
컴퓨터 활용 지식수준 (1(매우낮다)-7(매우높다))		평균: 5.1967	
합계		239	100%

다음으로 판별타당성(discriminant validity)을 분석하였다. 판별타당성은 두 가지 방법을 통해 검정하였는데 첫째는 모든 항목들이 해당 개념에 0.7이상의 요인 적재값 수준에서 요인으로 적재되어야 한다. 이 경우 측정항목의 신뢰성(reliability of measurement items)이 존재한다고 본다[9]. 둘째, 구조모형에서 판별타당성을 주장하기 위해서 평균분산추출(AVE)의 제곱근 값이 각각의 개념간 상관관계 계수들보다 커야 한다. 본 연구의 경우 모든 요인들의 사전에 탐색적 요인 분석에서 확인된 요인에 높은 수준으로 적재되어 있는 것을 확인할 수 있었으며<표 2>, 상관관계 분석을 통해 확인된 개념간의 상관관계 계수와 평균분산추출의 제곱근 값간의 비교에서 모든 평균분산추출의 제곱근 값들이 상관관계 계수보다 크게 나타나 판별타당성이 존재한다고 볼 수 있다<표 3>.

다음으로 신뢰성 분석을 수행하였다. 대표적으로 신뢰성을 평가하는 내적 일관성(internal consistency) 평가하는 Cronbach's Alpha값을 통해 신뢰성을 평가하였는데

〈표 2〉 주성분 분석 및 교차요인 분석

	성분					공통성	정책 위반	도덕적 해방	도덕적 신념	처벌 인지	보안 교육
	1	2	3	4	5						
SETA_1	-.080	.834	.027	-.006	-.020	.704	-0.073	-0.205	0.120	0.204	0.819
SETA_2	-.077	.843	.094	-.055	-.095	.738	-0.136	-0.230	0.193	0.267	0.855
SETA_3	-.137	.894	.060	-.051	-.097	.834	-0.140	-0.281	0.184	0.277	0.932
SETA_4	-.097	.898	.071	-.052	-.010	.824	-0.136	-0.248	0.116	0.269	0.910
SETA_5	-.159	.886	.012	-.044	-.047	.814	-0.148	-0.297	0.203	0.230	0.908
SETA_6	-.140	.897	.088	-.041	-.001	.834	-0.145	-0.283	0.169	0.292	0.917
SETA_7	-.157	.826	.173	.074	-.035	.744	-0.079	-0.304	0.174	0.359	0.849
Moral_1	-.198	.038	.133	-.154	-.758	.657	-0.343	-0.351	0.919	0.343	0.125
Moral_2	-.249	.129	.148	-.028	-.806	.750	-0.275	-0.399	0.871	0.392	0.226
PunCer	-.326	.116	.627	-.295	-.313	.698	-0.412	-0.493	0.421	0.940	0.255
PunCert	-.173	.194	.888	-.001	-.092	.865	-0.137	-0.288	0.267	0.781	0.314
PunSev	-.152	.142	.924	-.011	-.082	.903	-0.129	-0.261	0.262	0.819	0.258
Likelihood_1	.314	-.026	-.052	.902	.125	.932	0.981	0.462	-0.338	-0.316	-0.118
Likelihood_2	.325	-.070	-.088	.899	.122	.942	0.983	0.484	-0.347	-0.355	-0.167
AtBlm_1	.832	-.128	-.078	.095	.172	.754	0.407	0.860	-0.380	-0.386	-0.281
AtBlm_2	.782	-.071	-.062	.032	-.028	.622	0.313	0.745	-0.210	-0.275	-0.210
AtBlm_3	.839	-.117	-.089	.048	.095	.737	0.360	0.850	-0.357	-0.355	-0.239
DHum_2	.776	-.078	-.099	.147	.090	.648	0.385	0.806	-0.331	-0.326	-0.226
DHum_3	.818	-.141	-.073	.001	-.071	.699	0.289	0.770	-0.257	-0.257	-0.265
DfR_1	.723	-.031	-.130	.129	.338	.672	0.387	0.795	-0.390	-0.426	-0.185
DfR_3	.583	-.099	-.058	.169	.354	.507	0.367	0.670	-0.371	-0.382	-0.231
DsR_2	.718	-.033	-.019	.291	.269	.675	0.483	0.797	-0.368	-0.388	-0.185
DstC_1	.742	-.140	-.182	.044	.222	.655	0.332	0.798	-0.350	-0.439	-0.281
DstC_2	.763	-.138	-.143	.097	-.020	.631	0.369	0.801	-0.303	-0.394	-0.241
DstC_3	.895	-.166	-.068	.023	.004	.834	0.337	0.874	-0.276	-0.343	-0.313
ELng_1	.606	-.080	-.028	.218	.333	.533	0.389	0.724	-0.347	-0.372	-0.206
ELng_2	.866	-.131	-.161	.091	.032	.802	0.395	0.868	-0.327	-0.430	-0.288
MJust_2	.814	-.074	.003	.190	.237	.761	0.451	0.863	-0.376	-0.345	-0.229
MJust_3	.797	-.062	-.111	.177	.247	.745	0.440	0.861	-0.401	-0.456	-0.229
PCmp_1	.636	-.121	-.057	.245	.206	.524	0.419	0.731	-0.321	-0.330	-0.240
PCmp_2	.772	-.086	-.086	.099	.042	.622	0.362	0.777	-0.251	-0.345	-0.233
PCmp_3	.839	-.106	-.086	.066	.060	.730	0.380	0.835	-0.305	-0.354	-0.263
고유값	13.715	4.853	2.071	1.631	1.120	Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization.					
분산설명력	42.859	15.166	6.471	5.098	3.501						
누적분산	42.859	58.025	64.496	69.594	73.095						
Kaiser-Meyer-Olkin Measure of Sampling Adequacy.						.923					
Bartlett's Test of Sphericity			Approx. Chi-Square			7273.597					
			degree of freedom			496					
			significance			.000					

탐색적 연구의 경우 본 값이 0.6이상 되어야 한다[37]. 본 연구의 경우 최하 값이 0.7544로 본 기준을 만족하고 있다. 본 연구는 또한 구조모형에서 신뢰성을 평가하는 또 다른 지표인 복합신뢰성(composite reliability)을 통해 신뢰성을 평가하였다. 본 값에 대한 절대적인 기준은 존재하지 않으며, 연구자들 간의 경험적 합의도 존재하지 않는다[4]. 따라서 많은 경우 전통적 신뢰성 기준을 준거로 사용하는 경우가 많은데 이 기준에 따르면 0.7이상 되어야 한다[4][20]. 본 연구에서 복합신뢰성에 대한 평가결과 최하 값이 0.8851로 나타나 신뢰성에 문제가 없다고 볼 수 있다.

마지막으로 개념 타당성(construct validity)을 평가하였다. 개념타당성이란 개념을 측정하기 위한 항목들이 의도된 목적에 맞게 측정되고 있는지 수준을 나타낸다[4]. 개념 타당성을 주장하기 위해서는 두 가지 기준이 충족되어야 하는데 첫째는 개념을 측정하는 가설화된 지표들을 일치 수준(집중 타당성)과 둘째로 해당 지표들과 다른 개념들을 측정하는 지표간의 구별(판별타당성)이 명확해야 한다[4]. 본 연구의 경우 집중타당성과 판별타당성에 문제가 없기 때문에 개념타당성이 확보되었다고 볼 수 있다.

다음으로 공통방법오류에 대한 검정을 수행하였다. 본

〈표 3〉 판별타당성 분석 및 신뢰성 분석

	정책 위반	도덕적 해방	도덕적 신념	처벌 인지	보안 교육	Cronbach's alpha	AVE	CR
정책위반	**0.9823**					**0.9636**	**0.9649**	**0.9821**
도덕적 해방	0.4821	**0.8034**				**0.9673**	**0.6455**	**0.9703**
도덕적 신념	-0.3486	-0.415	**0.8950**			**0.7544**	**0.8010**	**0.8895**
처벌인지	-0.3420	-0.4603	0.4064	**0.8492**		**0.8531**	**0.7211**	**0.8851**
보안교육	-0.1453	-0.2984	0.1894	0.3025	**0.8852**	**0.9541**	**0.7836**	**0.9620**

AVE: Average Variance Extracted(평균분산추출) / CR: Composite (Factor) Reliability(복합신뢰성)

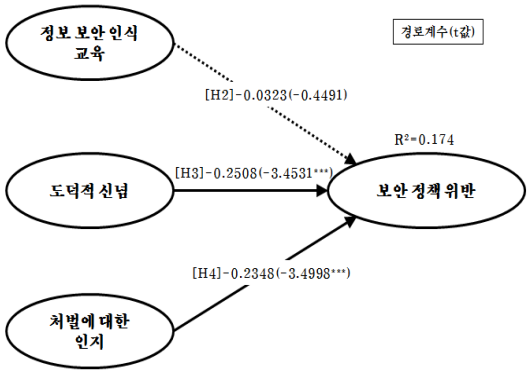
연구는 독립변수와 종속변수를 하나의 도구로 측정하였기 때문에 수집된 데이터가 공통방법오류(Common Method Bias)의 문제가 발생할 수 있다. 따라서 공통방법오류의 정도를 평가하는 과정이 필요하며, 이에 두 가지 방법을 통해 공통방법오류 여부를 측정하였다. 첫째, Harman의 일요인(Harman's One-factor test) 검정을 실시하여 데이터 내 분산의 대부분이 하나의 요인에 의해 설명되는지 여부를 분석해 보았다[40].

<표 2>에서 볼 수 있듯이 요인회전 전 탐색적 요인분석에서 총 설명력은 73.095로 요인분석이 갖아야 할 설명력인 75% 수준에 근사하는 것으로 나타났다[52]. 또한 가장 많은 설명력을 차지하는 요인의 설명분산은 42.859로 상대적으로 총 설명력의 과반이상을 차지하고 있는 것으로 나타났다. 따라서 공통방법오류의 문제가 심각한지 여부를 판단하기 위해서 추가적인 분석이 필요하다. 일반적으로 잠재변수간의 상관관계 계수 높은 경우(0.9 이상) 공통방법오류의 단서가 되는데[39], <표 3>에 나타나 있듯이 가장 높은 상관관계 계수가 0.4821로 높은 수준은 아니기 때문에 공통방법오류의 문제가 심각하지 않은 것으로 볼 수 있다[33]. 주의 할 것은 잠재변수간의 상관관계 계수(r)가 0.7이상[10] 혹은 0.8이상[3] 될 경우 다중공선성(multicollinearity)의 문제가 발생할 수 있다. 하지만 상관관계 분석에서 이 기준을 초과하는 값이 관측되지 않기 때문에 다중공선성의 문제도 심각하지 않은 것으로 볼 수 있다.

3.2 구조모형 분석

구조모형 분석을 위해 부분최소자승기법(PLS, Partial Least Squares)을 활용하였다. AMOS(Analysis of Moment Structures)나 LISREL(Linear Structural Relations)과 같은 구조방정식 모형 기법과 다르게 PLS 기법은 모수에 관한 여러 가지 엄격한 가정에서 자유롭다[21]. 본 연구에서는 구조모형 분석을 위해 PLS기법을 기반으로 하는 SmartPLS 2.0 M3 소프트웨어를 활용하였다[43]. 최종 분석을 수행하기 전에 분석을 위한 표본수가 적절한지 판단해 보아야 한다. 구조모형 분석을 위해 요구되는 경험적 최소 표본 수는 100개이다[49]. 본 연구에서 사용한 표본 수는 이보다 2배 이상 확보되었기 때문에 결과의 신뢰성을 위해 필요한 표본 수를 충분히 확보하였다고 볼 수 있다. 이에 최종 분석을 수행하였다.

최종 분석을 위해 bootstrap 재표집 절차(resampling procedure)를 따랐다. 본 방법의 경우 추정의 안정성(stability of estimates)이 보장되고 견고한 신뢰구간의 개발하는데 유용하다[11]. 재표집을 위해 사용된 표본 수는 가장 많이 활용되는 500개를 설정하였다. 또한 탐색 모형들의 품질을 평가하기 위해 사용되는 모형 평가 지표들인 R^2, f^2, Q^2와 GoF(Goodness of Fit)를 평가하였다[22]. 외생변수에 의해 설명되는 내생변수의 설명력은 R^2를 통해 평가하는데 일반적으로 10%이상 되어야 한다[50]. 본 연구에서 탐색한 3개의 모형에 대한 내생변수의 설명력은 모두 본 기준을 충족하고 있기 때문에 최소 설명력은 확보하고 있다고 볼 수 있다. f^2는 모형 1과 모형 2간의 차이에서 도덕적 해방 개념이 포함되었을 경우 설명력의 차이와 영향효과 크기를 살펴보기 위해 사용하였다. Q^2와 GoF는 모형 2의 적합도를 평가하기 위해 사용하였다.



[그림 3] 경쟁모형 검정 결과

우선 도덕적 해방의 영향을 살펴보기 위해 도덕적 해방이 존재하지 않을 경우 가설들의 인과관계를 살펴보았다[그림 2]. 또한 두 번째 모형에서는 도덕적 해방이 존재할 경우 가설들의 인관관계의 변화를 살펴보았다[그림 3]. 첫 번째 모형에서 정보보안 인식 교육은 보안정책 위반에 통계적으로 유의한 영향을 미치지 않는 것으로 나타났다(β=-0.0323). 반면 도덕적 신념은 보안정책 위반에 통계적으로 유의한 부(-)의 영향을 미치는 것으로 나타났다(β=-0.2508, p<0.001). 이는 개인이 옳고 그름을 판단할 수 있는 도덕적 판단기준이 존재할 경우 보안 정책을 위반할 가능성이 낮아진다는 것을 알 수 있다. 다음으로 처벌에 대한 인지가 보안 정책 위반에 통계적으로 유의한 부의 영향을 미치는 것으로 나타났다(β=-0.2348, p<0.001). 따라서 개인이 자신의 잘못된 행위가 어떠한 처벌이 주어질지, 그리고 그 처벌이 얼마나 강도가 높은 것인지 인지할 경우 보안정책을 위반할 가능성이 낮아질 수 있다는 것을 알 수 있다.

다음으로 본 연구에서는 도덕적 해방이 존재할 경우 기존 모형에서 어떠한 변화가 발생하는지 살펴보았다. 우선 통계적으로 도덕적 해방이 존재할 경우 설명력이 17.4%에서 26.9%로 높아져서 도덕적 해방으로 인해 보안 정책 위반에 대한 설명수준이 높아진다는 것을 알 수 있다. 다음으로 설명수준의 효과크기를 살펴보았다. Cohen(1988)은 연구모형에 새로운 변수가 추가되었을 경우 효과 크기(effect size)를 계산할 수 있는 공식(f^2)을 제안하였는데 해당 공식은 R^2를 기반으로 한다[11]. 본 값이 0.02 이상일 경우 낮은 효과, 0.15이상일 경우 중간 효과, 0.35이상일 경우 높은 효과가 있다고 정의한다[12][34].

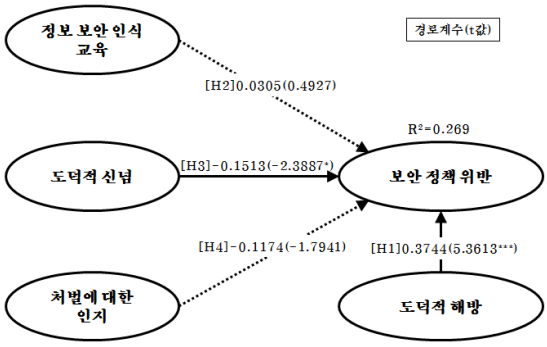
$$f^2 = \frac{R^2(full) - R^2(exduded)}{1 - R^2(full)} = \frac{0.269 - 0.174}{1 - 0.269} = 0.129959$$

$$Pseudo\,F\text{-}\,Test = f^2 \times (n - k - 1) = 0.129959 \times (239 - 4 - 1) = 30.4104$$

$where\ f^2 : effect\ sizes$(효과크기),
$n : sample\ size$(표본 수),
$k : the\ \nu mber\ of\ independent\ variables$(독립변수의 수)

다음으로 효과크기(f^2) 통계량의 유의수준(significance)을 평가하기 위해 Pseudo F검정을 수행하였다[34]. 본 연구에서는 효과크기(f^2)가 0.13으로 중간 수준보다 낮게 나타났으나, 효과의 유의수준이 30.4104 (p<0.001)로 나타나 R^2의 변화가 유의하게 나타났기 때문에[47] 도덕적 해방 요인의 추가가 설명력의 유의한 변화를 유발한다고 볼 수 있다.

첫 번째 모형과 달리 도덕적 해방이 구조 모형에 포함된 경우 도덕적 신념의 수치적 강도는 낮아졌지만 여전히 통계적으로 부의 영향을 미치는 것으로 나타났다(β=-0.1513, p<0.05). 이는 개인이 자신의 잘못된 행위를 항변할 수 있는 근거가 준비되어 있다 하더라도 옳고 그름을 판단할 수 있는 도덕적 판단 근거가 강하게 존재할 경우 보안 정책을 위반하지 않을 가능성이 높다는 것을 알 수 있다. 반면에 처벌에 대한 인지는 유의하지 않는 것으로 나타났다(β=-0.1174). 이는 도덕적 해방, 즉 개인의 잘못된 행동을 방어할 수 있는 어떠한 '변명'이 존재할 경우 자신의 행동이 불가피하다는 것을 피력할 수 있기 때문에 처벌에 대한 두려움이 감소한 다는 것을 알 수 있다.



GoF=0.4589, Stone-Geisser's Q^2=0.2377

[그림 4] 제안모형 검정 결과

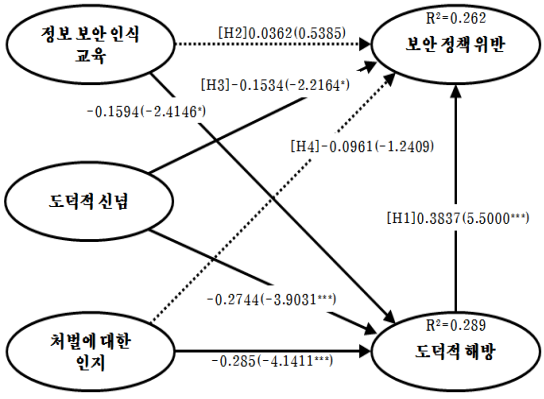
본 연구에서는 도출된 결과의 신뢰성을 높이기 위해 모형의 적합도를 평가하였다. 전반적인 모형 적합도를 평가하기 위해 GoF(Goodness of Fit)와 Stone-Geisser's Q^2를 평가하였다. 모형 적합도인 GoF가 0.35보다 클 경우 수집된 데이터와 모형간의 적합도가 매우 높다고 볼 수 있는데[56], 본 연구의 경우 본 지수가 0.4589로 나타나 높은 모형적합성을 확보하였다고 볼 수 있다. 또한 Stone-Geisser's Q^2가 0보다 클 경우 모형이 충분한 예측 타당성(predictive validity)을 가지고 있다고 본다[49]. 본 연구의 경우 0.2377로 나타나 모형이 충분한 예측타당성이 있음을 알 수 있다. 즉 해당 모형이 충분한 타당성이 존재하기 때문에 위와 같은 결과의 해석에 큰 무리가 없음을 알 수 있다.

마지막으로 도덕적 해방에 대한 구체적 설명을 위해 전체 경로의 인과과계를 살펴보았다.

〈표 4〉 경로분석 결과

모형 1 (도덕적 해방 포함되지 않은 경우)						
경로	평균	표준편차	경로계수	표준오차	t값	p값
H2. 보안교육→정책위반	-0.0431	0.0718	-0.0323	0.0718	0.4491	0.6536
H3. 도덕적신념→정책위반	-0.2513	0.0726	-0.2508	0.0726	3.4531	0.0006***
H4. 처벌인지→정책위반	-0.2432	0.0671	-0.2348	0.0671	3.4998	0.0005***
모형 2 (도덕적 해방이 포함된 경우)						
경로	평균	표준편차	경로계수	표준오차	t값	p값
H1. 도덕적 해방→정책위반	0.3736	0.0698	0.3744	0.0698	5.3613	0.0000***
H2. 보안교육→정책위반	0.0169	0.0620	0.0305	0.0620	0.4927	0.6224
H3. 도덕적신념→정책위반	-0.1580	0.0633	-0.1513	0.0633	2.3887	0.0173*
H4. 처벌인지→정책위반	-0.1181	0.0654	-0.1174	0.0654	1.7941	0.0734
모형 3 (모든 경로 가능성 검토)						
경로	평균	표준편차	경로계수	표준오차	t값	p값
H1. 도덕적 해방→정책위반	0.3814	0.0698	0.3837	0.0698	5.5000	0.0000***
H2. 보안교육→정책위반	0.0330	0.0671	0.0362	0.0671	0.5385	0.5905
H3. 도덕적 신념→정책위반	-0.1550	0.0692	-0.1534	0.0692	2.2164	0.0271*
H4. 처벌인지→정책위반	-0.0887	0.0775	-0.0961	0.0775	1.2409	0.2152
보안교육→도덕적해방	-0.1560	0.0660	-0.1594	0.0660	2.4146	0.0161*
도덕적신념→도덕적해방	-0.2793	0.0703	-0.2744	0.0703	3.9031	0.0001***
처벌인지→도덕적해방	-0.2877	0.0687	-0.2845	0.0687	4.1411	0.0000***

* p<0.05, **p<0.01, ***p<0.001



[그림 5] 전체 경쟁 모형 검정 결과

전체 경로에 대한 분석 결과, 모형 2에서 제시한 결과와 마찬가지로 정보보안 인식 교육은 보안 정책 위반에 통계적으로 유의한 영향을 미치지 않는 것으로 나타났다(β=0.0362). 처벌에 대한 인지 역시 보안 정책 위반에 유의한 영향을 미치지 않는 것으로 나타났다(β=-0.0961). 반면 도덕적 신념은 보안 정책 위반에 유의한 영향을 미치는 것으로 나타났다(β=-0.1534, p<0.05). 이 세 가지 결과는 [모형 2]에서 제시한 결과와 동일하게 나타났다.

추가적으로 외생변수와 도덕적 해방간의 경로를 추가로 살펴보았을 경우 세 개의 외생변수가 모두 도덕적 해방에 통계적으로 유의한 부의 영향을 미치는 것으로 나타났다. 이에 대한 의미를 살펴보면, 첫째, 정보보안 인식 교육은 도덕적 해방에 유의한 영향을 미치는 것으로 나타났는데(β=-0.1594, p<0.05), 이러한 결과는 기업 내에서 이루어지는 정보보안 교육을 통해 개인은 자신이 속한 조직의 보안이 중요하다는 것을 인식함으로 자신의 부도덕한 행위를 도덕적 해방이라는 자기 방어 기제를 통해 회피하기 보다는 해당 행위를 하지 않도록 유도할 수 있음을 의미한다. 이러한 결과는 또한 기존의 연구에서 정보보안 인식교육에 대한 영향이 연구마다 상충되는 것이[16] 이러한 방어적 기제의 존재를 고려하지 않았기 때문이라는 설명이 가능하다. 둘째, 도덕적 신념은 도덕적 해방에 유의한 영향을 미치는 것으로 나타났다(β=-0.2744, p<0.001). 이러한 결과는 도덕적 판단기준이 명확히 확립된 개인의 경우 도덕적 해방이라는 방어기제에 의지하지 않고 자신의 행동이 옳지 못함을 인식하여 스스로 해당 행위를 억제하려 하기 때문인 것으로 볼 수 있다. 마지막으로 처벌에 대한 인지는 도덕적 해방에 유의한 영향을 미치는 것으로 나타났다(β=-0.285, p<0.001). 이는 처벌로 인해 직접적으로 해당 행위를 억제하기 보다는 처벌로 인해 자신의 부도덕한 행위에 대한 방어가 불가하다는 것을 인지함으로 인해 잘못된 행위를 억제하게 됨을 보여주는 결과로 볼 수 있다.

지금까지 제시한 여러 연구 모형들에 대한 분석결과를 정리하면 <표 4>와 같다.

4. 결론

본 연구는 정보보안에 대한 중요성에 입각하여 보안을 강화하기 위한 방법을 탐색하기 위해 수행하였다. 구체적으로 정보보안에 있어서 가장 중요한 문제로 논의되는 조직 구성원들의 보안 행위를 유도할 수 있는 방안을 탐색하고자 하였다. 기존 연구의 경우 조직원들의 보안 행위 중 가장 중요한 기업 내에서 수립된 보안 정책준수를 유도할 수 있는 방안에 대해 주로 살펴보았으나 본 연구는 왜 조직구성원들이 보안정책을 제대로 준수하지 않는지를 살펴보고자 하였다. 이는 기존 연구에서 보안정책 준수를 중요하게 생각하고 해당 연구를 지속하였음에도 불구하고 왜 이들이 제시한 대책들이(countermeasures) 효과가 없는지에 대한 고려가 부족하였기 때문에 이러한 연구의 갭을 연결해 줄 수 있는 가교 역할을 하는 연구가 필요하다고 판단했기 때문이다.

이를 위해 제시한 탐색적 모형을 분석한 결과는 다음과 같다. 첫째, 정보보안 인식 교육은 보안정책 위반에 유의한 영향을 미치지 못하였다. 이는 다음의 세 가지 함의를 제시해 준다. 첫째, 지금까지 중요하게 제시된 정보보안 인식 교육이 일시적으로 이루어질 경우 효과가 없고 장기적으로 이루어질 경우 효과가 나타나기 때문에 이러한 결과가 나타나는 것인지 판단해 보아야 한다. 둘째, 정보보안 인식 교육의 콘텐츠가 적절한지, 그리고 그 빈도가 적절한지, 또한 전달 매체(예, 이메일, 뉴스레터, 등)가 적절한지, 여러 가지 관점에서 보안 인식 교육자체에 문제가 없는지 고려가 필요함을 의미한다. 셋째, 정보보안 인식 교육의 개인의 생산성을 저해하는지 고려해 보아야 한다. 조직 구성원들은 매일 많은 업무에 시달리고 있다. 따라서 업무 중 보안 교육이 이루어질 경우 자신의 업무 시간의 일부를 할애해야 하기 때문에 보안 교육 자체를 업무 생산성과 상충되는 방해요인으로 인식할 수 있다. 뿐만 아니라 업무 이외 시간에 보안 교육이 이루어질 경우 사적인 시간이 줄어들기 때문에 프라이버시 침해가 발생하고 있다고 느낄 수 있다. 따라서 현재 이루어지고 있는 정보보안 교육이 실제 조직 구성원들의 업무 생산성 혹은 프라이버시와 상충되는지 고려해 보아야 한다는 시사점을 제시해 준다. 물론 정보보안인식 교육이 완전히 효과가 없는 것은 아니다. 정보보안 인식 교육은 도덕적 해방에 부의 영향을 미치는 것으로 나타나났다는 것은 인식 교육으로 인해 보안에 대한 중요성을 인식시킬 수 있기 때문에 자신의 행동이 도덕적으로 잘못되었을 경우 자신의 행위를 정당화하려는 노력을 하기 보다는 잘못을 인정하도록 유도하는 장점도 있음을 알 수 있다.

다음으로 도덕적 신념은 보안정책위반과 도덕적 해방에 모두 유의한 영향을 미치는 것으로 나타났다. 이는 개인 스스로가 어떠한 행동에 대한 옳고 그름을 결정하는 도덕적 기준이 내재적으로 확립되어 있을 경우 보안정책 위반을 억제할 수 있다는 것을 알 수 있다.

마지막으로 처벌에 대한 인지는 도덕적 해방이 존재하지 않을 경우 보안정책위반에 유의한 영향을 미치는 것으로 나타났으나 도덕적 해방이 존재할 경우 유의한 영향이 존재하지 않았다. 이는 완전매개(full mediation) 효과를 나타내는 것으로 자신의 잘못된 행동을 방어할 수 있는 방어기제가 존재할 경우 처벌에 대한 두려움보다는 자신의 행위를 도덕적으로 정당화시킬 수 있는 방법을 탐색하고 이를 활용할 것을 우선적으로 고려하기 때문에 나타난 결과로 볼 수 있다. 즉 자신의 부도덕한 행위가 정당화될 수 있다고 느낄 경우 스스로 처벌을 받지 않을 가능성이 낮다고 판단하여 처벌에 대한 인지가 유의하지 않게 나타난 것으로 볼 수 있다.

본 연구는 위와 같은 시사적 함의를 발견하였음에도 불구하고 다음과 같은 한계점이 존재한다. 첫째, 표본의 선정이다. 본 연구에서는 표본 선정에 있어서 모두 현직 기업에 종사하는 사람들을 대상으로 하였으나 산업의 특성에 따라, 그리고 직급에 따라 보안에 대한 인식수준이 다를 수 있음에도 이를 고려하지 않았다. 둘째, 공통방법오류(common method bias)의 문제이다. 특정 시점에 설문응답자들에게 외생변수와 내생변수에 대해 모두 응답하게 하였기 때문에 공통방법오류의 발생가능성이 존재한다. 물론 분석부분에서 통계적인 접근을 통해 공통방법오류의 문제가 심각하지 않음을 규명하였으나 이는 어디까지나 사후적 평가방법일뿐 사전적 접근법은 아니다.

마지막으로 추후 연구에서는 다음과 같은 접근이 필요할 것으로 사료된다. 정보보안인식 교육이 유의하지 않은 것이 단기적 교육 때문인지 장기적 교육 때문인지 아니면 어떠한 다른 외생적 요인에 의한 것인지 깊이 있는 탐색이 필요할 것으로 보인다. 기존 연구에서 언급되어왔듯이 정보보안 인식교육의 효과에 대해서는 상반된 결과가 도출되는 경우가 많다. 따라서 이를 명확히 규명할 수 있는 연구가 필요할 것으로 판단된다. 둘째, 도덕적 신념이 보안정책 준수를 위해 중요한 요인으로 작용함을

확인하였다. 그러나 본 연구에서는 어떻게 도덕적 신념을 높일 수 있는지에 대한 고려가 없었다. 즉 도덕적 신념을 유발할 수 있는 선행요인을 규명하는 연구도 필요할 것으로 판단된다. 셋째, 기존 연구에서는 도덕적 신념이 존재 할 경우 처벌에 대한 두려움보다는 자신의 행동일 잘못되었기 때문에 해당 행위를 스스로 억제한다고 주장하였다. 따라서 도덕적 신념에 따라 처벌의 효과가 달라질 수 있다는 것을 제시하고 있다. 따라서 도덕적 신념과 처벌에 대한 인지간의 조절관계가 존재하는지 아니면 어떠한 인과관계가 존재하는지 규명하는 것도 의미있을 것으로 판단된다.

참 고 문 헌

[1] 임명성, 조직 구성원들의 정보보안 정책 준수행위 의도에 관한 연구. 디지털정책연구, 10(11), 119-128.

[2] Alnuaimi, O. A., Robert Jr., L. P., & Maruping, L. M. (2010). Team Size, Dispersion, and Social Loafing in Technology-Supported Teams: A Perspective on the Theory of Moral Disengagement. Journal of Management Information Systems, 27(1), 203-230.

[3] Bagozzi, R. P., Yi. Y., & Phillips, L. W. (1991). Assessing Construct Validity in Organizational Research. Administrative Science Quarterly, 36(3), 421-458.

[4] Bagozzi, R. P. & Yi, Y. (2012). Specification, Evaluation, and Interpretation of Structural Equation Models. Journal of the Academy of Marketing Science, 40, 8-34.

[5] Bandura, A. (1986). Social Foundations of Thought and Action: A Social Cognitive Theory. Englewood Cliffs, NJ: Prentice Hall.

[6] Bandura, A. (1991). Social Cognitive Theory of Self-Regulation. Organizational Behavior and Human Decision Processes, 50, 248-287.

[7] Bandura, A. (2002). Selective Moral Disengagement in the Exercise of Moral Agency. Journal of Moral Education, 31(2), 101-119.

[8] Bandura, A., Barbaranelli, C., & Caprara, G. V. (1996). Mechanism of Moral Disengagement in the Excercise of Moral Agency. Journal of Personality & Social Psychology, 71, 364-374.

[9] Barclay, D., Higgins, C., & Thompson, R. (1995). The Partial Least Squares (PLS) Approach to Causal Modeling: Personal Computer Adoption and Use as an Illustration. Technology Studies, 2(2), 285-309.

[10] Cassel, C., Hackl, P., & Westlund, A. H. (1999). Robustness of Partial Least-Squares Method for Estimating Latent Variable Quality Structures. Journal of Applied Statistics, 26(4), 435-446.

[11] Chin, W. W., Marcolin, B. L., & Newsted, P. R. (2003). 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, 14(2), 189-217.

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

[13] Cohen, D., & Nisbett, R. E. (1994). Self-Protection and the Culture of Honor: Explaining Southern Violence. Personality and Social Psychology Bulletin, 20, 551-567.

[14] D'Arcy, J., & Greene, G. (2009). The Multifaceted nature of Security Culture and Its Influence on End User Behavior. IFIP TC 8 International Workshop on Information Systems Security Research, South Africa.

[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] Deter, J. R., Trevinõ, L. K., & Sweitzer, V. L. (2008). Moral Disengagement in Ethical Decision Making: A Study of Antecedents and Outcomes. Journal of Applied Psychology, 93(2), 374-391.

[18] Dhillon, G., & Moores, S. (2001). Computer Crimes: Theorizing about the Enemy Within. Computers and Security, 20(8), 715-723.

[19] Dinev, T., Goo, J., Hu, Q., & Nam, K. (2008). User Behaviour Towards Protective Information Technologies: The Role of National Cultural Differences. Information Systems Journal, 19(4), 391-412.

[20] Fornell, C., & Larcker, D. F. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. Journal of Marketing Research, 18(1), 39-50.

[21] Haenlein, M., & Kaplan, A. M. (2004). A Beginner's Guide to Partial Least Squares Analysis. Understanding Statistics, 3(4), 283-297.

[22] Hair, J. F., Sarstedt, M., Ringle, C. M., & Mena, J. A. (2012). An Assessment of the Use of Partial Least Squares Structural Equation Modeling in Marketing Research. Journal of the Academy of Marketing Science, 40, 414-433.

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

[24] 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), 106-125.

[25] Hovav, A., & D'Arcy, J. (2012). Applying an Extended Model of Deterrence Across Cultures: An Investigation of Information Systems Misuse in the U.S. and South Korea. Information & Management, 49, 99-110.

[26] Hu, Q., & Dinev, T. (2005). Is Spyware and Internet Nuisance or Public Menace. Communications of the ACM, 48(8), 61-66.

[27] Hu, Q., Dinev, T., Xu, Z., & Ling, H. (2009). Why Individuals Abuse Computer Systems in Organizations: Perspectives from Multiple Theories. IFIP TC 8 International Workshop on Information Systems Security Research, South Africa.

[28] Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2011). Does Deterrence Work in Reducing Information Security Policy Abuse by Employees. Communications of the ACM, 54(6), 54-60.

[29] Hyde, L. W., Shaw, D. S., & Moilanen, K. L. (2010). Developmental Precursors of Moral Disengagement and the Role of Moral Disengagement in the Development of Antisocial Behavior. Journal of Abnormal Child Psychology, 38, 197-209.

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

[31] Karahanna, E., Straub, D. W., & Chervany, N. L. (1999). Information Technology Adoption Across Time: A Cross-Sectional Comparison of Pre-Adoption and Post-Adoption Beliefs. MIS Quarterly, 23(2), 183-213.

[32] 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

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

[34] Mathieson, K., Peacock, E., & Chin, W. W. (2001). Extending the Technology Acceptance Model: The Influence of Perceived User Resources. DATA BASE for Advances in Information Systems, 32(3), 86-112.

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

[36] Mowday, R. (1998). Reflections on the Study and Relevance of Organizational Commitment. Human Resources Management Review, 8(4), 387-401.

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

[38] Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' Behavior Towards IS Security Policy

Compliance. 40th Hawaii International Conference on System Science, Hawaii, USA.

[39] Pavlou, P., Liang, H., & Xue, Y. (2007). Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective. MIS Quarterly, 31(1), 105-136.

[40] Podsakoff, P. M., MacKenzie, S. B., Lee, J., & Podsakoff, N. P. (2003). Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies. Journal of Applied Psychology, 88(5), 879-903.

[41] Post, G. V., & Kagan, A. (2006). Evaluating Information Security Tradeoffs: Restricting Access Can Interfere with User Tasks. Computers & Security, 1-9.

[42] Posthumus, S., & von Solms, R. (2004). A Framework for the Governance of Information Security. Computers & Security, 23(8), 638-646.

[43] Ringle, C. M., Wende, S., & Will A. (2005). SmartPLS 2.0(beta). SmartPLS, Hamburg, Germany.

[44] Rippetoe, P. A., & Rogers, R. W. (1987). Effects of Components of Protection-Motivation Theory on Adaptive and Maladaptive Coping with a Health Threat. Journal of Personality & Social Psychology, 52(3), 596-604.

[45] Rodgers, R. W. (1975). A Protection Motivation Theory of Fear Appeals and Attitude Change. Journal of Psychology, 91, 93-114.

[46] Rodgers, R. W., & Buffalo, M. D. (1974). Neutralization Techniques: Toward a Simplified Measurement Scale. Pacific Sociological Review, 17(3), 313-331.

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

[49] Siponen, M., Vance, A., & Willison, R. (2012). New Insights into the Problem of Software Piracy: The Effects of Neutralization, Shame, and Moral Beliefs. Information & Management, 49, 334-341.

[50] Sosik, J. J., Kahai, S. S., & Piovoso, M. J. (2009). Silver Bullet or Voodoo Statistics? A Primer for Using the Partial Least Squares Data Analytic Technique in Group and Organization Research. Group Organization Management, 34(1), 15-36.

[51] Stanton, J., Stam, K., Mastrangelo, P., & Jolton, J. (2005). Analysis of End User Security Behaviors. Computers and Security, 24(2), 124-133.

[52] Stevens, J. (1996). Applied Multivariate Statistics for the Social Sciences. 3rd ed., Mahwah, NJ: Lawrence Erlbaum.

[53] Straub, G. A. (2005). A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example. Communications of the Association for Information Systems, 16(5), 91-109.

[54] Sykes, G. M., & Matza, D. (1957). Techniques of Neutralization: A Theory of Delinquency. American Sociological Review, 22(6), 664-670.

[55] Wang, J., Chen, R., Herath, T., & Rao, H. R. (2009). Visual E-Mail Authentication and Identification Services: An Investigation of the Effect on E-Mail Use. Decision Support Systems, 48(1), 92-102.

[56] Wetzels, M., Odekerken-Schröder, G., & van Oppen, C. (2009). Using PLS Path Modeling for Assessing Hierarchical Construct Models: Guidelines and Empirical Illustration. MIS Quarterly, 33, 177-195.

[57] Workman, M., Bommer, W. H., & Straub, D. (2008). Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test. Computers in Human Behavior, 24(6), 2799-2816.

임 명 성

- 2002년 2월 : 삼육대학교 경영정보학과(경영학사)
- 2004년 2월 : 한국외국어대학교 경영정보대학원(MBA)
- 2011년 8월 : 서강대학교 경영전문대학원(Ph.D.)
- 2011년 9월 : 서강대학교 경영학부 대우교수
- 2012년 3월~현재 : 삼육대학교 경영학과 조교수
- 관심분야 : 정보보안, 서비스 시스템, 정보심리학
- E-Mail : msyim@syu.ac.kr