http://dx.doi.org/10.14400/JDPM.2013.11.11.1

정보보안 상황에서의 도덕적 해방: 선행요인과 결과요인에 대한 연구

임명성*
삼육대학교 경영학과*

Moral Disengagement in Information Security Context: A Study of Antecedents and Outcomes

Myung-Seong Yim*
Dept. of Business Administration, Sahmyook University*

요 약 최근 정보보안사고의 가장 큰 문제 중 하나가 조직 내 내부인임에도 불구하고 아직까지 보안사고의 원인을 기술적 문제에만 초점을 맞추고 있다. 이에 본 연구는 도덕적 해방이론을 기반으로 조직 내부인의 보안정책 이탈의 도가 무엇인지 탐색해보고자 한다. 정보보안 분야에서 조직내부인의 보안정책 이탈을 설명하기 위해 사용되는 일반화된 이론은 전무하다. 따라서 본 도덕적 이탈 이론을 기반으로 정보보안을 위한 가이드라인을 제시하고자 한다. 분석결과 보안정책인지와 인지된 처벌은 도덕적 이탈에 부정적 영향을 미치는 것으로 나타났다. 반면에 정보보안에 대한 부정적 정서는 도덕적 해방에 긍정적 영향을 미치는 것으로 나타났다. 마지막으로 도덕적 해방은 보안정책 위반 의도에 긍정적 영향을 미치는 것으로 나타났다.

주제어 : 정보보안, 도덕적 해방, 정보보안 침해

Abstract Every big online security breach seems to end in a big lecture. Thus, although a predominant weakness in properly securing information assets is the individual user within an organization, much of the focus of extant security research is on technical issues. The purpose of this study is to explain why insiders breach security policy by applying the moral disengagement theory. There are no consistent, widely accepted theories or theoretical frameworks in the literatures as to why insiders breach of information security, and therefore no clear, effective guidance on what to do to prevent employees from violating information security policy in organization. To do this, we theorize that moral disengagement may play a mediating role connecting stable individual differences to intention to breach security policy, because of some of the individual differences. We found that policy awareness and perceived punishment have a negatively significant effect on moral disengagement. However, negative affectivity has a positively significant influence on moral disengagement. Furthermore, moral disengagement has a positive effect on intention to breach security policy. Conclusions and implications are discussed.

Key Words : Information Security, Moral Disengagement, Information Security Breach

Received 28 August 2013, Revised 25 September 2013
Accepted 20 November 2013
Corresponding Author: Myung-Seong Yim(Sahmyook University)
Email: msyim@syu.ac.kr

ISSN: 1738-1916

1. 서론

최근 메리츠화재에서는 내부직원이 16만 3925명의 고객정보를 유출한 사실을 파악했다[1]. 국정원에서도 내무기밀정보가 유출된 사고가 있었다. 내부직원이 국정원 내부기밀 자료를 민주당과 문재인 민주통합 후보캠프 소속 직원에게 건네준 사실이 최근 검찰의 조사를 통해 밝혀졌다. 해당 직원은 국정원에서 파면된 이후에도 국정원 전산망에 접속해 '원장님 지시·강조 말씀'이라는 제목의 게시자료 전체 54건 중 42건을 열람해 손으로 메모한 사실도 드러났다. 국정원이 해당 직원이 파면된 이후에도 내부전산망 접속자격을 차단하지 않았기 때문이다[2]. 호주에서는 최근 한국계 직원 한 명을 한국 당국자에게 기밀정보를 누설한 혐의로 해고했다. 호주연방경찰(AFP)은 해당 직원이 호주 정부의 테러 대응방안과 관련한 기밀정보를 시드니 주재 한국 공관원에게 누설하였다고 밝혔다[3].

처음부터 악의를 가지고 있거나, 또는 단순히 부주의하거나 잘 모르는 내부 직원들이 조직에서 공적으로나 사적으로 보안상의 위협을 야기할 수 있다[4]. 조직 구성원은 보안문제에서 상당한 권한을 이미 가지고 있기 때문이다. 따라서 조직은 악성해커들의 외부 공격을 차단하는 것보다 내부 직원들의 보안유지에 더 많은 노력을 해야 한다. 최근 포네몬 연구소(Ponemon Institute)가 전 세계 9개국 16개 산업에 속한 277기업을 대상으로 수행한 정보보안 관련 조사 결과에 따르면, 정보유출 사고 원인의 37%가 외부 공격(malicious or criminal attack), 35%가 조직 내부인에 의한 유출(human factor), 29%가 시스템 결함(system glitch)이라고 밝혔다[40].

위의 사례와 포네몬 연구소의 조사결과가 보여주듯이 조직 내부인에 의한 사고는 여전히 지속되고 있으며, 그 비중도 높다. 즉 조직에서 정보보안정책을 제대로 지키지 않는 경우가 많다. 이처럼 여전히 보안사고의 높은 비율이 내부 직원들에 의해서 발생하고 있는 상황에서 어떻게 하면 조직 내부에서 보안 사고를 줄일 수 있는지 고민해보아야 한다.

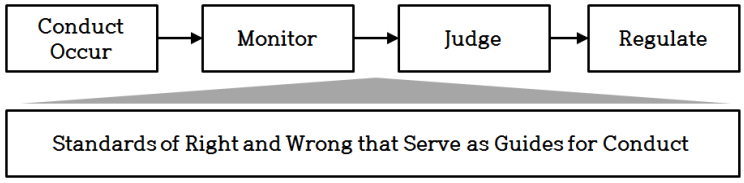
많은 학자들은 조직 내부인들에 의한 정보보안 사고를 줄이기 위해 가장 먼저 선행되어야 하는 것이 조직이 수립한 보안정책을 조직 구성원들이 준수하도록 유도하는 것이라고 주장한다[13][15][17][23][24][26][36]. 보안정책(security policy)이란 정보보안에 대한 기대를 명확하고, 구체적이고, 측정 가능한 목적과 의무사항들로 표현한 문서로 조직 구성원들이 조직의 정보시스템 보안 요구사항에 어긋나지 않도록 행동하게 해준다[17].

하지만 위의 사례와 포네몬 연구소의 조사결과가 보여주듯이 조직 내부인에 의한 사고는 여전히 지속되고 있으며, 기 비중도 높다. 즉 조직에서 정보보안정책을 제대로 지키지 않는 경우가 많다. 따라서 본 연구는 왜 조직 구성원들이 정보보안정책을 준수하지 않는지, 그 이유를 설명할 수 있는 탐색적 연구를 수행하고자 한다. 이를 위해 본 연구는 도덕적 해방 이론(Moral Disengagement Theory)을 사용하여, 왜 개인들이 잘못된 행위인지 알면서도 보안정책을 위반하는지에 대해 알아보고자 한다. 정보보안정책 위반/위배(information security policy violation)란 조직 구성원들이 자신의 이익을 위해 자신의 컴퓨터를 이용하여 조직의 규율이나 정책에 반하는 행위를 하는 것을 말한다[42]. 예를 들어, 인가되지 않는 데이터나 시스템에 접근하거나, 자신의 이익을 위해 회사의 기밀 데이터를 제 삼자에게 전달하거나 판매하는 행위 등 다양한 행위들이 해당된다[42].

Bandura(1986)는 사람들이 일반적으로 비윤리적 행위를 억제하는 도덕적 자기 규제 과정(moral self-regulatory processes)이 상호 연관된 다양한 인지적 메커니즘(Moral Disengagement, 도덕적 해방)의 활용을 통해 비활성화될(deactivated) 때 비윤리적 의사결정을 하게 된다고 주장하였다. 반대로 도덕적 행위를 관장하는 자기 규제 메커니즘은 활성화되지 않는(activated) 한 작동하지 않는다[1][10][14][25][30][32]. 개인은 사회화 과정(the course of socialization)을 거치면서 자신의 행동의 지침이 되는 옳고 그름의 표준을 만들어가게 되는데[41], 여기서 형성된 옳고 그름의 표준 자기 규제 메커니즘의 기반이 된다.

도덕적 해방이론의 이론적 및 실무적 가치에도 불구하고 여전히 도덕적 해방에 대한 이해는 초기단계이다[14]. 또한 도덕적 해방에 대한 원인 요인(antecedents)에

1) MK뉴스, 메리츠화재, 16만 4천명 고객 정보 유출... 직원 소행. 2013년 5월 28일
2) Donga.com, "승진 노리고 민주당에 심리전단 직원 정보 제공"… 공모한 정모 씨의 정보유출 전말. 2013년 6월 20일
3) 연합뉴스, 호주 연방경찰, 정보유출 혐의 한국계 직원 해고. 2013년 5월 6일
4) Armerding, T., 내부 직원의 정보 유출, 왜 막을 수 없나?, ITWorld, 2013년 6월 21일



[Fig. 1] Self-Regulatory Mechanism

대해서는 아직 많이 연구되지 않았다[14]. 따라서 본 연구는 개인적 차이에 의해 영향을 받는 도덕적 해방의 선행요인뿐만 아니라 이 요인들과 도덕적 해방간의 관계, 그리고 도덕적 해방과 보안정책 의도간의 관계를 탐색해 보고자 한다.

2. 이론적 배경

2.1 도덕적 해방 이론

Bandura(1986)에 의해 처음 소개된 개념이자 사회인지이론(Social Cognitive Theory)의 확장 개념인 도덕적 해방이론은 왜 사람들이 사회적으로 부적절한 행위에 몰입하게 되는지 설명해준다[7].

도덕적 해방은 중성화 이론(Techniques of Neutralization)[39]과 관념 합리화(Rationalizing Ideologies)[3]와 유사한 개념으로 개인의 이탈행위를 설명하기 위해 자주 사용된다.

해방(Disengagement)은 인지적 해방(Emotional Disengagement), 감성적 해당(Emotional Disengagement), 행동적 해방(Behavioral Disengagement) 등 세 가지 형태가 존재한다[29]. 도덕적 해방은 인지적 해방에 해당된다. 인지적 해방에서는 이탈행위를 범한 개인이 인지적으로 자신의 행위를 도덕적으로 정당한 것으로 재해석하는 과정을 포함한다.

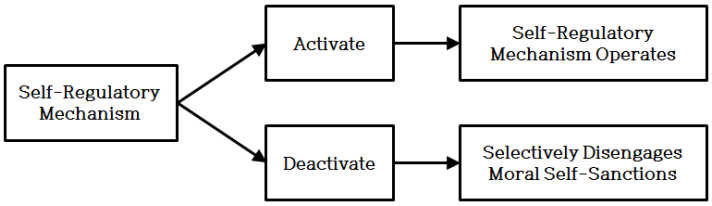
Bandura(1986)에 따르면 사람들은 윤리적 행위에 대한 개인적 기준에 의해 행동하며, 대부분의 사람들은 자신의 기준에 어긋나는 행동을 스스로 제약하는 경향이 있다고 한다(그림 1). 이러한 행위 표준 즉, 도덕적 행위 표준에 어긋나는 행위에 대한 부정적 자기 제재와 도덕적 행위 표준에 준하는 행위에 대한 긍정적 자기 제재에서 행위의 기준이 되는 행위 표준이 개인에게 수용되고 나면 행위를 규제하는 영향요인으로 작용한다[6]. 이러한 자기 반응적 영향은 동기적 그리고 인지적으로 도덕적 행위의 조절작용을 수행한다[8]. 이러한 감성적 반응은 자신의 행위의 도덕적 본질에 관한 스스로의 감시와 판단 과정의 결과물이다[1][10]. 하지만 이러한 과정을 통해 항상 행위가 도덕적으로 규제되는 것은 아니다.

Bandura(1991)에 따르면 사람은 8가지 심리학적 기교(maneuvers)를 선택적으로 사용함으로 자기제재(self-sanction) 없이 개인적 표준을 위배할 수 있다고 한다(그림 2). Bandura(1986)가 제시한 8가지의 상호연관된 자기 규제 메커니즘은 도덕적 정당화(Mora Justification), 임시변통적 비교(Advantageous Comparison), 완곡한 명명(Euphemistic Labeling), 결과의 축소, 무시, 또는 곡해(Disregarding or Distorting the Consequences), 인간성 상실(Dehumanization), 책망의 귀속(Attribution of Blame), 책임의 전가(Displacement of Responsibility), 책임의 분산(Diffusion of Responsibility) 등이다.

도덕적 정당화, 임시변통적 비교, 완곡한 명명은 도덕적 용인(Moral Acceptability)을 증가시킴으로 인해 비난받을 행위의 인지적 오해(Cognitive Misconstrual)를 유발하는 요인에 해당된다[14]. 대부분의 사람들은 타인에게 해를 주는 것은 잘못된 것이라는 것을 인지하고 있다. 하지만 도덕적 정당화를 가진 개인은 타인에게 피해를 주는 행위를 도덕적으로 정당한 것으로 포장한다.

책임의 전가, 책임의 분산, 결과의 축소, 무시, 또는 곡해는 개인이 유해한 행동의 결과를 왜곡할 때 발생한다. 예를 들어, 집단이 반사회적 행위를 수행할 경우 개인은 해당 행위에 대한 전적인 책임을 느끼지 못하는데 이는 집단 구성원 전체에 책임이 분산되어 있다고 느끼기 때문이다[14].

마지막으로 인간성 상실과 책망의 귀속은 행위자가 자신의 유해한 행위의 대상에 대해 제대로 식별하지 못하게 하여 도덕적 제재로부터 자유롭게 해준다. 예를 들어, 테러리스트들이 고문을 받게 되면 이들을 고문하는



[Fig. 2] How to (De)Activate The Self-Regulatory Mechanism

사람이 아니라 고문을 받는 테러리스트가 비난받는 것을 사필귀정이라 보는 것은 결국 책망의 귀속 때문이다[14]. 이러한 8가지 요인을 통한 도덕적 통제의 선택적 해방은 동일한 도덕적 표준 하에 여러 가지 형태의 행위를 유발한다[30]. 선택적 도덕적 해당은 개인 수준뿐만 아니라 사회적 시스템 수준에서도 발생할 수 있다[41].

개인은 자신의 행동이 도덕적 자아에 어긋나지 않게 도덕적이고 정당한 것으로 보이기를 원한다[29]. 따라서 개인은 도덕적 행위에 몰입할 때, 행위의 본질에 따라서 스스로 죄책감 혹은 자신감을 느끼게 된다[6]. 하지만 타인에게 피해를 주는 행위는 도덕적 진정성(moral integrity)을 억제시킨다[29]. 이 경우 개인은 자신의 잘못(피해를 주는 행위)로부터 위의 8가지 메커니즘의 구성요인들을 선택적으로 활용하여 자신의 행위가 도덕적으로 정당하며, 비난받을 행위가 아님을 주장한다[7].

3. 연구모형과 가설도출

본 연구에서는 정보보안 상황에서 도덕적 해방의 결과요인과 도덕적 해방에 영향을 미치는 원인요인을 규명하는데 중점을 두고 있다. 이에 그림과 같은 가설을 중심으로 도덕적 해방의 선행요인과 결과요인을 구성하였다.

3.1 보안정책 인지

보안정책은 정보보안을 위한 초석으로 조직 내에서 그 중요성이 점차 증가하고 있다[15]. 보안정책은 조직 구성원들이 업무환경에서 접근하지 말아야 하는 정보에 접근하지 않도록 해주며, 정보보안 위반으로 인해 어떠한 처벌을 받을 수 있는지 인지시켜준다[15]. 따라서 정보보안정책에 대해 인지하고 있을 경우 자사의 정보보안 관점에서 무엇을 하고, 무엇을 하지 말아야 하는지, 그리고 하지 말아야 하는 행위를 했을 경우 받게 될 처벌이 무엇인지 인지하게 되어 이탈행위에 몰입하지 않을 것이다. 따라서 다음의 가설을 제시할 수 있다.

H1. 보안정책 인지는 도덕적 해방에 음(-)의 영향을 미칠 것이다.

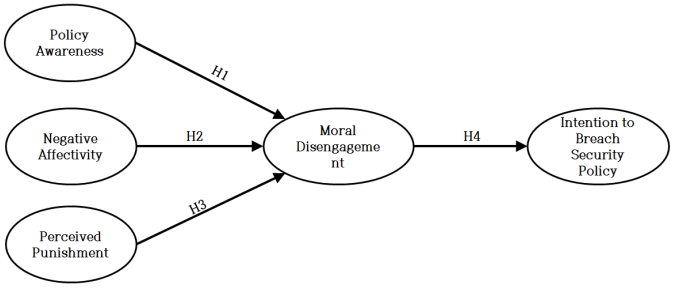
3.2 정보보안에 대한 부정적 정서

Herath and Rao(2009b)는 보안정책의 준수가 조직 구성원들로 하여금 자신의 업무를 수행하는데 있어서 불편함을 가중시킨다고 주장하였다. Chan et al.(2005)은 보안정책 준수가 불편함과 더불어 업무의 효율성 및 생산성과 직접적으로 충돌한다고 주장하였다. 즉, 보안정책을 준수함에 있어서 발생하는 다양한 절차의 준수는 자신의 생산성과 반대의 효과를 유발할 수 있다는 것을 조직 구성원들이 느끼게 된다는 것이다. 이럴 경우 구성원들은 정보보안정책을 당연히 지켜야할 규칙이 아니라 자신의 업무를 방해하는 장애물로 인식할 수 있다. 따라서 다음의 가설을 제시할 수 있다.

H2. 정보보안에 대한 부정적 정서는 도덕적 해방에 정(+)의 영향을 미칠 것이다.

3.3 처벌에 대한 인지

일반적 제재 이론(General Deterrence Theory)에 따르면 보안정책을 준수하는 구성원들로 하여금 정책을 위반하였을 경우 받게 될 처벌을 인지하게 되면 해당행위가 억제된다고 주장하였다[13]. 처벌은 두 가지 특성을 가지는데 하나는 처벌의 확신성(certainty of sanctions)으로 위반행위를 하였을 경우 처벌의 받게 될 가능성을 말하며, 두 번째는 처벌의 심각성(severity of sanctions)으로 처벌의 강도를 말한다. 처벌과 관련된 이 두 가지 특성이 조직 구성원들에게 인식될 경우 해당행위는 결국 처벌이라는 결과를 유발하기 때문에 억제된다고 볼 수 있다. 따라서 다음의 가설을 제시할 수 있다.



[Fig. 3] Research Model

H3. 처벌에 대한 인지는 도덕적 해방에 음(-)의 영향을 미칠 것이다.

3.4 도덕적 해방

도덕적 해방은 개인의 위반행위에 직접적인 영향을 미친다[7]. 자기 규제 기능은 인간의 내적 통제를 담당하는 메커니즘이 활성화되지 못할 경우 위반행위를 유발하게 된다. 정보보안 상황에서도 개인의 행동을 관장하는 도덕적 통제 메커니즘이 작용하지 않을 경우 정보보안에 어긋나는 행위가 억제되지 못하여, 위반행위가 발생할 가능성이 있다. 따라서 다음과 같은 가설을 제시할 수 있다.

H4. 도덕적 해방은 보안정책 위반 의도에 정(+)의 영향을 미칠 것이다.

4. 분석방법

본 연구에서는 제안한 연구모형을 검정하기 위해 설문기법을 사용하여 자료를 수집하였다. 설문 기법은 Likert type 7-points scales을 사용하였으며, 1점은 전혀 동의하지 않음을, 7점은 전적으로 동의함을 의미한다. 수집된 데이터에 대한 분석도구로는 기초통계분석을 위해 IBM SPSS Statistics version 19.0과 구조모형 분석을 위해 SmartPLS 2.0 M3[35]를 사용하였다.

각각의 측정항목들은 내용 타당성(content validity)을 확보하기 위해 기존 연구에서 실증 분석된 항목들을 차용하여 사용하였다.

보안정책 위반 의도(Intention to Breach Security Policy)는 D'Arcy et al.(2009)의 연구에서 사용된 2개의 항목으로 측정하였다. 도덕적 해방을 측정하기 위한 측정항목은 Bandura et al.(1996)이 사용한 32개의 항목들을 정보보안 상황에 맞추어 내용을 일부 변경하였다. 특히 측정항목의 간명성을 유지하기 위해 32개의 항목을 모두 사용하기 보다는 도덕적 해방의 하위 개념들을 적절히 설명하는 3개 항목을 선택하여 24개의 항목을 이용하여 도덕적 해방을 측정에 사용하였다[14]. 처벌에 대한 인지(Perceived Punishment)는 D'Arcy et al.(2009)의 연구에서 사용된 3개의 항목을 사용하였다. 보안정책에 대한 부정적 정서(Negative Affectivity)는 Yoon(2011)의 연구에서 사용된 5개의 항목을 사용하였다. 보안정책에 대한 인지(Policy Awareness)는 D'Arcy et al.(2009)의 연구에서 사용된 1개의 항목을 사용하였다.

〈Table 1〉 Profile of Respondents

Criteria		Frequency	Ratio(%)
Gender	Male	121	71.6
	Female	46	27.2
	No response	2	1.2
Age	18 to 24	3	1.8
	25 to 34	78	46.2
	35 to 44	74	43.8
	45 to 54	14	8.3
Education Level	High School	1	0.6
	College	16	8.9
	University	114	67.5
	Master	29	17.2
	Ph.D.	5	3.0
	No response	4	3.0
Current Position	Senior manager	1	0.6
	Middle manager	45	26.6
	Technical	51	30.2
	Administrative/clerical	51	30.2
	Professional Staff	19	11.2
	Other	2	1.2
Work Experience(average)		5.987 years	
Computer Knowledge(average)		8.835(1-10)	
Total		169	100%

4.1 자료 수집

자료를 수집하기 위해 7개의 IT(Information Technology) 기업의 핵심관계자에게 연구의 목적과 필요성을 설명하고 참여를 요청하였다. 이 중 참여의사를 밝힌 5개의 기업의 핵심 담당자에게 인쇄된 설문을 발송하였고, 설문의 배포와 수집은 해당 관계자가 담당하였다. IT기업을 선정한 이유는 정보보안 기술에 대해 선두적인 역할을 수행하고 있고 실제 정보보안 시스템을 판매하는 벤더 기업으로 정보보안에 민감할 것으로 판단되기 때문이다. 따라서 해당 기업은 비 IT기업보다 정보보안 시스템과 보안에 대한 인식 수준이 높을 것으로 판단된다.

자료 수집에 소요된 기간은 총 2개월이며, 178부가 수거되었다. 수거된 설문 중 같은 값으로 연속된 응답을 하였거나 무응답이 많은 설문의 경우 분석에서 제외하였다. 최종 분석에 사용된 설문은 169부이다.

수집된 응답자의 특성을 정리하면 표 1과 같다.

4.2 요인분석

본 연구에서는 요인분석에 앞서 수집된 자료가 요인분석에 적합한지를 두 가지 방법을 통해 평가하였다. 첫째는 정량적 평가로 수집된 데이터의 수가 요인분석을 수행하기에 적합한지 평가하였다. 선행연구에 따르면 100은 미약한 수준, 200은 평범한 수준, 300은 좋은 수준으로 본다[22][27]. 본 연구에서 분석에 사용된 표본은 169개로 다소 부족하지만 최저 수준인 50개 이상의 표본을 확보하였으며, 공통성(communality, h^2)이 0.5이상일 경우 최소 100에서 200개의 표본이 확보될 경우 요인분석에 문제가 되지 않는다[27]. 표 2에 나타나 있듯이 공통성의 최소값이 0.553으로 최소값인 0.5이상을 확보하고 있어서 169개의 표본으로 요인분석을 수행하는데 문제가 되지 않을 것으로 판단된다. 둘째로 정성적 평가를 수행하였다. 정성적 평가는 KMO(Kaiser-Meyer-Olkin Measure of Sampling Adequacy) 표본 적합성과 Bartlett의 구형성 검정 방법을 사용하였다. KMO는 0.8이상이면 우수하다고 판단하는데[19], 표 2에 나타나 있듯이 본 값이 0.907로 높은 수준의 표본 적합성을 나타내고 있다. 다음으로 Bartlett의 구형성 검정을 수행하였다. 본 값은 유의할 경우(sig.<0.05) 적합하다고 본다[19]. 표 2에 나타나 있듯이 본 값도 유의하게 나타났다($p<0.000$). 따라서 요인 분석을 수행하였다.

탐색적 요인 분석(EFA, Exploratory Factor Analysis)을 위해 주축 요인 추출(PAF, Principal Axis Factoring) 기법을 사용하였다[12][22]. 또한 몇 개의 요인을 추출할지를 결정하기 위해 고유값(eigenvalue)>1 기준을 사용하였다[12][22]. 회전은 카이저 표준화를 사용하는 Varimax 기법을 사용하였다(Varimax with Kaiser Normalization)[12]. 요인 분석을 통해 총 4개의 요인이 도출되었다. 도출된 요인은 모두 0.5이상의 요인값을 갖는 항목을 가지고 있으며, 각각의 항목은 교차요인(cross-loading) 적재값이 0.4이상인 항목은 제거하였다. 최종적으로 도출된 요인 구조는 표 2와 같다. 도출된 요인 구조의 설명력은 75.001로 기준 값인 75%를 상회하였다[19].

4.3 동일방법편의

다음으로 동일방법편의(Common Method Bias)의 수준을 평가하기 위해 Harman의 단일요인(Harman's Single-Factor Test) 검정을 수행하였다. 본 방법은 탐색적 요인분석에서 회전 전 해(unrotated solution)내에 하나의 지배요인(one dominant factor)이 존재하는지를 평가하는 기법이다[33]. 표 2에서 볼 수 있듯이 가장 많은 설명력을 차지하는 요인의 설명분산은 46.374로 상대적으로 총 설명력의 절반이상을 차지하고 있는 것으로 나타났다. 따라서 동일방법편의의 문제가 심각한지 여부를 판단하기 위해서 추가적인 분석을 수행하였다. 일반적으로 잠재변수간의 상관관계 계수 높은 경우(0.9이상) 동일방법편의가 존재할 수 있다고 보는데[31], 표 3에 나타나 있듯이 가장 높은 상관관계 계수가 -0.499로 매우 높은 수준은 아니기 때문에 동일방법편의의 문제가 심각하지 않은 것으로 볼 수 있다[28]. 또한 잠재변수간의 상관관계 계수(r)가 0.8 이상 될 경우 다중공선성(multicollinearity)의 문제가 발생할 수 있다[4]. 하지만 상관관계 분석에서 이 기준을 초과는 값이 관측되지 않기 때문에 다중공선성의 문제도 심각하지 않은 것으로 볼 수 있다.

4.4 측정모형의 신뢰성 및 타당성

다음으로 측정모형의 신뢰성 및 타당성을 평가하였다. 표준 지표 적재값(PLS 교차 요인 적재값)이 0.7이상일

〈Table 2〉 Factor Analysis with Reliability

	Principal Axis Factoring				Communality	PLS Crossloading Analysis				
	1	2	3	4		Negative	Likelihood	PerPunish	MD	PolAware
Negative2	.152	**.847**	.007	.013	.740	**0.909**	0.064	0.002	0.246	-0.104
Negative3	.151	**.882**	.062	.075	.810	**0.928**	0.116	0.032	0.253	-0.107
Negative4	.103	**.952**	.042	.034	.920	**0.953**	0.072	0.038	0.220	-0.072
Negative5	.143	**.888**	-.003	-.042	.810	**0.922**	0.021	0.008	0.234	-0.072
Likelihood_1	.241	.034	-.059	**.905**	.883	0.089	**0.978**	-0.274	0.400	-0.218
Likelihood_2	.285	-.001	-.094	**.872**	.850	0.058	**0.982**	-0.318	0.437	-0.240
PunCert	-.165	.036	**.817**	-.012	.695	0.041	-0.139	**0.845**	-0.283	0.159
PunSev	-.153	.101	**.959**	-.007	.953	0.115	-0.139	**0.887**	-0.279	0.138
PunCer	-.369	-.014	**.612**	-.323	.616	-0.046	-0.406	**0.893**	-0.510	0.254
MJust_2	**.775**	.170	-.071	.256	.699	0.277	0.414	-0.312	**0.844**	-0.379
MJust_3	**.744**	.096	-.201	.233	.657	0.203	0.383	-0.461	**0.826**	-0.388
PCmp_2	**.712**	.074	-.071	.186	.553	0.185	0.353	-0.314	**0.768**	-0.381
PCmp_3	**.789**	.131	-.108	.139	.672	0.239	0.355	-0.339	**0.831**	-0.496
ELng_2	**.860**	.108	-.160	.096	.787	0.233	0.355	-0.414	**0.881**	-0.446
DsR_2	**.651**	.059	-.068	.365	.565	0.153	0.456	-0.338	**0.741**	-0.323
DHum_2	**.735**	.095	-.113	.153	.585	0.196	0.359	-0.318	**0.778**	-0.348
DHum_3	**.813**	.066	-.033	.018	.667	0.184	0.267	-0.240	**0.798**	-0.378
DstC_1	**.701**	.163	-.275	.137	.613	0.242	0.313	-0.448	**0.791**	-0.409
DstC_2	**.759**	.103	-.176	.081	.624	0.202	0.324	-0.379	**0.796**	-0.386
DstC_3	**.905**	.063	-.079	.029	.830	0.190	0.292	-0.328	**0.889**	-0.460
AtBlm_1	**.818**	.143	-.130	.141	.726	0.257	0.361	-0.375	**0.859**	-0.419
AtBlm_2	**.747**	.050	-.045	.067	.566	0.155	0.279	-0.261	**0.762**	-0.416
AtBlm_3	**.832**	.083	-.109	.071	.717	0.198	0.307	-0.337	**0.845**	-0.410
DfR_1	**.657**	.122	-.257	.253	.577	0.201	0.366	-0.475	**0.768**	-0.423
Eigenvalue	11.130	3.331	1.885	1.655		-0.096	-0.234	0.226	-0.499	**1.000**
% of Var	46.374	13.877	7.853	6.897	α	0.946	0.959	0.859	0.963	α ≧ 0.7
Cumula %	46.374	60.251	68.104	75.001	AVE	0.861	0.960	0.766	0.661	α ≧ 0.5
KMO and Bartlett's Test					CR	0.961	0.980	0.908	0.967	α ≧ 0.7
Kaiser-Meyer-Olkin Measure of Sampling				.907						
Bartlett's Test of Sphericity		Approx. Chi-Square		3829.083						
		Degree of Freedom		276						
		Significance		.000						

Negative: Negative Affectivity, Likehood: Intention to Breach Security Policy, PerPunish: Perceived Punishment, MD: Moral Disengagement, PolAware: Policy Awareness

Extraction Method: Principal Axis Factoring.
Rotation Method: Varimax with Kaiser Normalization.
Rotation converged in 5 iterations.

〈Table 3〉 Latent Variable Correlations with Discriminant Validity

	Negative	Likelihood	PerPunish	MD	PolAware
Negative	**0.928**				
Likelihood	0.074	**0.980**			
PerPunish	0.021	-0.303	**0.875**		
MD	0.258	0.428	-0.444	**0.813**	
PolAware	-0.096	-0.234	0.226	-0.499	-

Note: Diagonal elements (in bold) represent the square root of the average variance extracted(AVE).
Off-diagonal elements represent the correlations among constructs.

〈Table 4〉 Research Results

Hypotheses	Path Coefficients	Standard Error	t value	p value	Results
H1.Policy Awareness→Moral Disengagement	-0.3955	0.0602	-6.5686***	0.0000	Support
H2.Negative Affectivity→Moral Disengagement	0.2271	0.0616	3.6877***	0.0003	Support
H3.Perceived Punishment→Moral Disengagement	-0.3593	0.0589	-6.0952***	0.0000	Support
H4.Moral Disengagement→Intention to Breach	0.4279	0.0741	5.7725***	0.0000	Support

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

〈Table 5〉 Results of Mediation Analysis

Types of Analysis Technique	z Score	p value	Results
Sobel Test	-4.3373	0.0000***	Support
Aroian Test	-4.3092	0.0000***	Support
Goodman Test	-4.3659	0.0000***	Support

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

경우 항목 신뢰성(indicator reliability)이 있다고 본다[21]. 이때 0.7이상을 갖는 교차요인이 없어야 한다. 본 연구의 경우 표 2에 나타나 있듯이 최소 요인 적재값이 0.741로 본 기준을 만족하고 있다.

내적 일관성(internal consistency reliability)은 Cronbach's Alph값과 복합 신뢰성 지수(CR, Composite Reliability)를 기준으로 평가하였다. 일반적으로 이 두 값이 모두 0.7이상일 경우 내적일관성에 문제가 없다고 본다[21]. 표 2에 나타나 있듯이 Cronbach's Alph의 최소값은 0.859, 복합 신뢰성 지수의 최소값은 0.908로 본 기준을 만족하고 있다.

집중타당성(convergent validity)은 평균분산추출(AVE, Average Variance Extracted)값을 가지고 평가하였는데, 본 값이 0.5이상일 경우 집중타당성이 존재한다고 본다[16].

판별타당성(discriminant validity)은 잠재개념간의 상관관계 분석에서 각각의 상관관계 계수와 평균분산추출(AVE)의 제곱근 값을 비교하여 평균분산추출의 제곱근 값이 각각의 상관관계 계수보다 클 경우 존재한다고 본다[21].

5. 분석결과

본 연구에서는 제안된 모형을 분석하기 위해 PLS기법을 사용하였다. PLS 구조모형 기법은 다변량분석 기법(multivariate analysis method) 중 하나로 회계, 마케팅, 경영정보, 운영관리, 전략 경영 등 다양한 분야에서 사용되고 있다[20]. 본 기법은 정규성 제약에서 다소 자유로우며, 적은 표본으로도 분석이 가능하다는 장점이 있다[20]. 또한 본 기법은 탐색적 연구에 적합하다[20].

모형 분석을 위해 필요한 표본 수는 가장 많은 관측변수를 가지고 있는 잠재변수에 의해 결정되는데, 일반적으로 해당 관측변수의 개수의 10배가 최소 기준이다[21]. 본 연구에서는 도덕적 해방이 15개의 관측변수를 가지고 있음으로 150개의 표본이 최소 표본의 기준이 된다. 본 연구에서 분석에 사용하는 표본 수는 169개로 본 기준을 만족하고 있다.

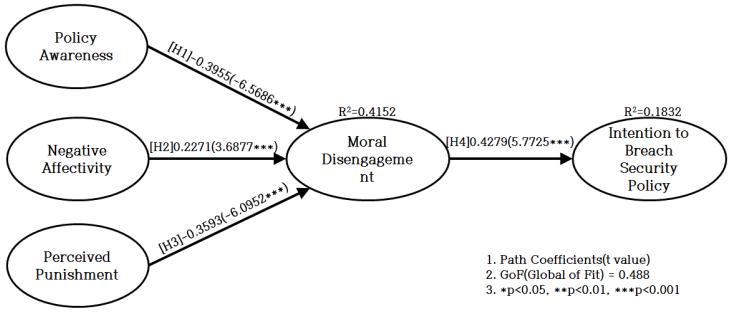
경로의 유의 수준을 도출하기 위해 필요한 표준오차를 도출하기 위해 bootstrapping resampling 기법을 사용하였으며, 사용된 재표집 표본은 500개이다.

일반적으로 연구모형 분석 시 연구모형의 R^2가 10% 이상 되어야 예측타당성이 있다고 본다[38]. 본 연구의 경우 매개변수와 종속변수의 설명력이 각각 0.4152, 0.1832로 모형의 예측타당성이 있다고 볼 수 있다.

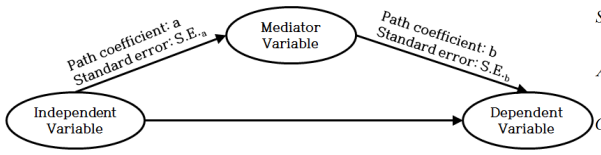
5.1 구조모형 분석 결과

제안 모형의 분석결과를 정리하면 다음과 같다. 보안정책의 인지는 도덕적 해방에 유의한 영향을 미치는 것으로 나탔다(β=-0.3955, p<0.001). 따라서 가설 1은 지지되었다. 다음으로 정보보안에 대한 부정적 정서는 도덕적 해방에 유의한 영향을 미치는 것으로 나타났다. 따라서 가설 2는 지지되었다(β=0.2271, p<0.001). 다음으로 처벌에 대한 인지는 도덕적 해방에 유의한 영향을 미치는 것으로 나타났다(β=-0.3593, p<0.001). 따라서 가설 3은 지지 되었다. 마지막으로 도덕적 해방은 보안정책 위반 의도에 유의한 영향을 미치는 것으로 나타났다(β=0.4279, p<0.001). 따라서 가설 4도 지지되었다.

지금까지 제시한 분석결과를 정리하면 표 4, 그림 4와 같다.



[Fig. 4] Results of PLS Structural Model Analysis



$$Sobel\_Test: z-value = \frac{a \times b}{\sqrt{(b^2 \times S.E._a^2) + (a^2 \times S.E._b^2)}}$$

$$Aroian\_Test: z-value = \frac{a \times b}{\sqrt{(b^2 \times S.E._a^2) + (a^2 \times S.E._b^2) + (S.E._a^2 \times S.E._b^2)}}$$

$$Goodman\_Test: z-value = \frac{a \times b}{\sqrt{(b^2 \times S.E._a^2) + (a^2 \times S.E._b^2) - (S.E._a^2 \times S.E._b^2)}}$$

[Fig. 5] Formulas for Mediation Analysis[2][9][18][34][37]

5.2 매개효과 분석 결과

심리학에서는 일반적으로 하나의 요인이 다른 요인에 영향을 미치는 관계를 주로 검증한다. 그러나 두 변수간의 관계는 심리학의 목적의 일부분일 뿐이다. 더 나은 이해를 위해서는 이러한 절차간의 과정(process)에 대한 폭넓은 이해가 필요하다(Preacher and Hayes, 2004). 이를 매개효과(mediation effect)라 정의하는데[9], 독립변수(predictor)와 종속변수(criterion)간의 관계가 매개변수(mediator)라는 변수에 의해 설명되는 정도를 의미한다. 또한 이를 효과 중심관점에서 독립변수가 종속변수에 직접영향을 미치는 관계를 직접효과(direct effect)라 정의하고 제 3의 변수인 매개변수에 의해 통제(controlled) 되는 관계를 간접효과(indirect effect)라 정의한다.

가장 흔하게 사용되는 매개효과의 검증방법은 Baron and Kenny(1986)에 의해 정립된 방법인데, 본 방법은 단순 매개효과(simple mediation)을 검증하는 데는 매우 유용하나 복잡한 관계(complex mediation)을 검증하는 데는 다소 한계가 있다는 것이 단점으로 지적된다[34]. 이러한 한계를 단순 매개효과 뿐만 아니라 복잡한 매개 효과 역시 검정하는데 유용하다 인정되는 것이 Sobel test (소벨 검정)이다[34]. 본 방법은 Baron and Kenny(1986)에 의해서도 이미 그 유용성을 인정받아온 방법으로 직접효과와 간접효과 상에 발생하는 오차항과 경로계수를 이용하여 검정결과 값을 도출하는 방법이다. 본 방법의 경우 2가지 가정을 기반으로 하는데 첫째는 다소 큰 표본을 요구한다는 것이다. 물론 표본 수에 대한 절대적인 기준은 존재하지 않기 때문에 어느 정도가 큰 표본인지에 대해 정의하기는 힘들다. 둘째, AMOS의 기본 가정과 마찬가지로 정규분포(normal distribution)를 가정하고 접근한다. 이를 기반으로 검정을 수행 시 양측검정(two-tailed)을 기반으로 z-value를 산출하여 이의 유의수준을 기반으로 매개효과를 평가한다[34].

z-value인 검정통계량(critical ratio)을 구하는 공식은 그림 5와 같다. a와 b는 각각의 경로계수를 의미하며, $S.E._a$와 $S.E._b$는 각각의 경로 a와 b의 표준오차(standard error)를 의미한다. 본 방법을 통해 도출한 매개효과 분석 결과는 표 5와 같다. 분석 결과 세 개의 경로가 모두 유의하게 나타났다.

6. 결론 및 함의

6.1 결론

본 연구는 조직 구성원들이 왜 정보보안정책을 위반하는지 그 이유를 찾고자 수행되었다. 구체적으로 도덕적 이탈행위를 유도하는 도덕적 해방이론을 기반으로 도덕적 해방이 정보보안 상황에서 보안정책 위반을 유발하는지, 그리고 무엇이 도덕적 해방을 유발하는지를 규명하고자 연구모형을 설정하고 실증적으로 분석하였다.

분석결과 도덕적 해방은 조직구성원들의 보안정책 위반 의도에 정의 영향을 미치는 것으로 나타났다. 즉, 조직구성원들이 자신을 정당화할 수 있는 수단이 존재할 경우 보안정책을 위반할 수 있다는 것을 시사한다.

다음으로 보안정책에 대한 인지, 보안정책에 대한 부정적 정서, 처벌에 대한 인식은 도덕적 해방에 유의한 영향을 미치는 것으로 나타났다. 이 중 보안정책에 대한 인지와 처벌에 대한 인식은 도덕적 해방에 부정적 영향을 미치는 것으로 나타났는데, 이는 구성원들이 정보보안정책을 명확히 인지하고 있을 경우 그리고 자신의 위반행위에 대한 처벌에 대해 인지하고 있을 경우 자신의 부도덕한 행위를 방어할 수 있는 행위가 억제된다는 것을 알 수 있다. 반대로 보안정책에 대한 부정적 정서는 도덕적 해방에 긍정적 영향을 미치는 것으로 나타났는데, 이는 보안정책의 준수가 구성원들의 업무 생산성과 상충될 경우 이러한 상황이 보안정책 미준수를 야기할 수 있는 도덕적 정당화의 기제가 될 수 있다는 점을 시사한다.

6.2 이론적 함의

본 연구는 도덕적 해방 이론을 정보보안 상황에 적용함으로 도덕적 해방을 위한 메커니즘이 보안상황에서도 적용됨을 규명하였다. 특히 정보보안에서의 이탈행위인 보안정책 미준수 행위가 도덕적 해방을 통해 유발될 수 있음을 규명하였다. 뿐만 아니라 정보보안 상황에서 도덕적 해방에 영향을 미치는 요인을 규명함으로 원인과 결과변수를 모두 규명하였다는 의의가 있다.

6.3 실무적 함의

본 연구의 결과는 실무적으로 다음과 같은 시사점을 제시해 준다. 첫째, 보안정책 미준수 행위를 정당화하려는 노력을 줄이기 위해서는 조직 내에서 구성원들이 정보보안정책을 명확히 인식하고 있도록 해야 한다. 조직의 보안정책이 모호하거나 정책입안자의 입장에서만 작성되는 경우 조직 구성원들이 보안정책을 제대로 이해하지 못하여 정책을 준수하기 어렵다. 따라서 보안정책의 품질을 정책을 준수하게 되는 구성원의 입장을 고려하여 작성하고 정책의 작성 시에도 명확하고, 이해하기 쉽고, 장황하지 않고, 전문용어 보다는 쉬운 용어로 작성되어야 한다. 또한 작성된 정책은 모든 구성원들에게 공유되어야 한다.

보안정책 미준수행위를 줄이기 위해서 위반행위로 인한 처벌에 대해 조직 구성원들이 명확히 인지하도록 해야 한다. 많은 경우 보안정책을 위반하여도 묵인하거나 가벼운 처벌로 마무리되는 경우가 많다. 하지만 모든 구성원들이 보안정책을 준수하도록 유도하기 위해서는 정책 위반 시 정해진 처벌을 받게 되며, 처해질 처벌의 강도는 어느 정도인지 명확히 인식시켜야 한다.

마지막으로 보안정책 준수를 유도하고 미준수 행위를 감소시키기 위해서는 보안정책을 준수함에 있어서 부정적 요소를 감소시켜야 한다. 보안정책 준수로 인해 발생할 수 있는 불편함이나 업무 생산성과 상충되는 상황에 대해 구성원들의 관점에서 관찰하고 이를 정책 수립 시 반영하여 보안정책 준수과정에서 발생하는 부정적 정서를 감소시킬 수 있어야 조직에서 목표로 하는 모든 구성원들의 보안정책 준수 행위를 유도할 수 있다.

6.4 연구의 한계점

본 연구의 한계점으로 첫째, 동일방법편의에서 자유로울 수 없다는 점이 있다. 사전적으로 동일방법편의를 해결한 것이 아니라 사후적인 통계 기법을 통해 동일방법편의의 영향을 낮다는 것을 규명하였기 때문에 완벽한 오류의 제거라 볼 수 없다. 이 문제를 해결하기 위해서는 데이터 수집 시 원인변수와 결과변수를 각각 다른 대상들에게 응답받고 뿐만 아니라 응답시점을 달리하는 노력이 필요하다. 둘째, 도덕적 해방을 위한 측정항목은 원 이론에 따르면 32개이다. 하지만 본 연구에서는 이 중 대표성이 있다고 판단되는 24개의 항목을 차용하였다. 물론 이러한 선택은 완벽하게 객관적이라고 볼 수는 없기 때문에 해당 항목들이 도덕적 해방의 하위 개념들을 완벽히 설명해주고 있다고 볼 수 없다. 셋째, 본 연구에서는 표본을 IT기업에 종사하는 구성원들을 대상으로 하였다. 따라서 IT기업으로부터 도출된 결과가 모든 상황에 포괄적으로 적용되는 것은 아니다. 따라서 일반화를 위해서는 다양한 표본 기업을 대상으로 연구해 볼 필요가 있다.

6.5 향후 연구 방향

도덕적 해방이론은 그 역사에도 불구하고 아직 많은 후속연구가 진행되진 않고 있다. 오늘날과 같이 도덕적 이탈행위가 많이 발생하고 있는 상황에서 본 이론의 활용가능성은 매우 높다고 볼 수 있다. 따라서 본 이론을 활용한 다양한 연구가 시도되는 것은 의미가 있다고 판단된다. 특히 도덕적 해방 이론에서 제시된 8개의 하위개념이 반드시 하나의 개념을 설명하고 있는 것은 아니다. Bandura et al.(1996)의 연구에서처럼 모든 하위 개념을 하나로 볼 수도 있으나 Alnuaimi et al.(2010)의 연구에서처럼 각각의 하위개념이 서로 구분되는 경우도 있다. 따라서 각각의 하위 개념과 정보보안 행위간의 관계를 구분하여 보는 것도 이론적 발전을 위해 의미 있다고 판단된다.

REFERENCES

[1] Alnuaimi, O. A., Robert Jr., L. P., and Maruping, L. M., Team Size, Dispersion, and Social Loafing in Technology-Supported Teams: A Perspective on

the Theory of Moral Disengagement. Journal of Management Information Systems, Vol. 27, No. 1, pp. 203-230, 2010.

[2] Aroian, L. A., The probability function of the product of two normally distributed variables. Annals of Mathematical Statistics, Vol. 18, pp. 265-271, 1944.

[3] Ashforth, B. E., and Anand, V., The Normalization of Corruption in Organizations. In R. M. Kramer and B. M. Shaw (Eds.), Research in Organizational Behavior, Vol. 25, Amsterdam: Elsevier, pp. 1-52, pp. 2003.

[4] Bagozzi, R. P., Yi. Y. and Phillips, L. W., Assessing Construct Validity in Organizational Research. Administrative Science Quarterly, Vol. 36, No. 3, pp. 421-458, 1991.

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

[6] Bandura, A., Social Cognitive Theory of Moral Thought and Action. In W. M. Kurtines & J. L. Gewirtz (eds.), Handbook of Moral Behavior and Development: Theory, Research, and Applications, Hillsdale, NJ:Erlbaum, pp. 71-129, 1991.

[7] Bandura, A., Barbaranelli, C., Caprara, G. V., and Pastorelli, C., Mechanisms of Moral Disengagement in the Excercise of Moral Agency. Journal of Personality and Social Psychology, Vol. 71, No. 2, pp. 364-374, 1996.

[8] Bandura, A., Caprara, G. V., Barbaranelli, C., and Pastorelli, C., Sociocognitive Self-Regulatory Mechanisms Governing Transgressive Behavior. Journal of Personality and Social Psychology, Vol. 80, No. 1, pp. 125-135, 2001.

[9] Baron, R. M., and Kenny, D. A., The Moderator-Mediator Variable Distinction in Social Psychological Research: Conceptual, Strategic, and Statistical Considerations. Journal of Personality and Social Psychology, Vol. 51, pp. 1173-1182, 1986.

[10] Broardley, I. D., and Kavussanu, M., Development and Validation of the Moral Disengagement in Sport Scale. Journal of Sport & Exercise Psychology, Vol. 29, pp. 608-628, 2007.

[11] Chan, M., Woon, R., and Kankanhalli, A., Perceptions of Information Security at the Workplace: Linking Information Security Climate to Compliant Behavior. Journal of Information Privacy and Security, Vol. 1, No. 3, pp. 18-41, 2005.

[12] Costello, A. B., and Osborne, J. W., Best Practices in Exploratory Factor Analysis: Four Recommendations for Getting the Most from Your Analysis. Practical Assessment, Research & Evaluation, Vol. 10, No. 7, pp. 1-9, 2005.

[13] D'Arcy, J., Hovav, A., and Galletta, D., User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research, Vol. 20, No. 1, pp. 79-98, 2009.

[14] Detert, J. R., Treviño, L. K., and Sweitzer, V. L., Moral Disengagement in Ethical Decision Making: A Study of Antecedents and Outcomes. Journal of Applied Psychology, Vol. 93, No. 2, pp. 374-391, 2008.

[15] Foltz, C. B., Schwager, P. H., and Anderson, J. E., Why Users (Fail to) Read Computer Usage Policies. Industrial Management & Data Systems, Vol. 108, No. 6, pp. 701-712, 2008.

[16] Fornell, C., and Larcker, D. F., Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. Journal of Marketing Research, Vol. 18, No. 1, pp. 39-50, 1981.

[17] Goel, S., and Chengalur-Smith, I. M., Metrics for Characterizing the Form of Security Policies. Journal of Strategic Information Systems, Vol. 19, pp. 281-295, 2010.

[18] Goodman, L. A., On the Exact Variance of Products. Journal of the American Statistical Association, Vol. 55, pp. 708-713, 1960.

[19] Hair, Jr., J. F., Black, W. C., Babin, B. J., Anderson, R. E., and Tatham, R. L., Multivariate Data Analysis, 6th eds. Pearson International Edition, 2006.

[20] Hair, Jr., J. F., Ringle, C. M, and Sarstedt, M., Partial Least Squares Structural Equation Modeling: Rigorous Applications, Better Results and Higher Acceptance. Long Range Planning, Vol. 46, pp. 1-12, 2013.

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

[22] Henson, R. K., and Roberts, J. K., Use of Exploratory Factor Analysis in Published Research: Common Errors and Some Comment on Improved Practice. Educational and Psychological Measurement, Vol. 66, No. 3, pp. 393-416, 2006.

[23] Herath, T., and Rao, H. R., Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness. Decision Support Systems, Vol. 47, No. 2, pp. 154-165, 2009a.

[24] Herath, T., and Rao, H. R., Protection Motivation and Deterrence: A Framework for Security Policy compliance in Organisations. European Journal of Information Systems, Vol. 18, No. 2, pp. 106-225, 2009b.

[25] Hyde, L. W., Sahw, D. S., and Moilanen, K. L., Developmental Precursors of Moral Disengagement and the Role of Moral Disengagement in the Development of Antisocial Behavior. Journal of Abnormal Child Psychology, Vol. 38, pp. 197-209, 2010.

[26] Johnston, A. C., and Warkentin, M., Fear Appeals and Information Security Behaviors: An Empirical Study. MIS Quarterly, Vol. 34, No. 1, pp. 1-20, 2010.

[27] Kahn, J. H., Factor Analysis in Counseling Psychology Research, Training, and Practice: Principles, Advances, and Applications. Counseling Psychologist, Vol. 34, No. 5, pp. 684-718, 2006.

[28] Malhotra, N., Kim, S. and Patil, A., Common Method Variance in IS Research: A Comparison of Alternative Approaches and a Reanalysis of Past Research. Management Science, Vol. 52, No. 12, pp. 1865-1883, 2006.

[29] Margolis, J. D., and Mlinsky, A., Navigating the Bind of Necessary Evils: Psychological Engagement and the Production of Interpersonally Sensitive Behavior. Academy of Management Journal, Vol. 51, No. 5, pp. 847-872, 2008.

[30] McAlister, A. L., Bandura, A., and Owen, S. V., Mechanisms of Moral Disengagement in Support of Military Force: The Impact of Sept. 11. Journal of Social and Clinical Psychology, Vol. 25, No. 2, pp. 141-165, 2006.

[31] Pavlou, P., Liang, H. and Xue, Y., Understanding and Mitigating Uncertainty in Online Exchange Relationships: A Principal-Agent Perspective. MIS Quarterly, Vol. 31, No. 1, pp. 105-136, 2007.

[32] Pelton, J., Gound, M., Forehand, R., and Brody, G., The Moral Disengagement Scale: Extension with an American Minority Sample. Journal of Psychopathology and Behavioral Assessment, Vol. 26, No. 1, pp. 31-39, 2004.

[33] Podsakoff, P. M., Lee, J. Y. and Podsakoff, N. P., Common Method Biases in Behavioral Research: A Critical Review of the Literature and Recommended Remedies. Journal of Applied Psychology, Vol. 88, No. 5, pp. 879-903, 2003.

[34] Preacher, K. J., and Hayes, A. F., SPSS and SAS Procedures for Estimating Indirect Effects in Simple Mediation Models. Behavior Research Methods, Instruments, & Computers, Vol. 36, pp. 717-731, 2004.

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

[36] Siponen, M., and Vance, A., Neutralization; New Insights into the Problem of Employee Information Security Policy Violations. MIS Quarterly, Vol. 34, No. 3, pp. 487-502, 2010.

[37] Sobel, M. E., Asymptotic Intervals for Indirect Effects in Structural Equations Models. In S. Leinhart (Ed.), Sociological Methodology. San Francisco: Jossey-Bass, pp. 290-312, 1982.

[38] Sosik, J. J., Kahai, S. S., and Piovoso, M. J., Silver Bullet or Voodoo Statistics? A Primer for Using Partial Least Squares Data Analytic Technique in Group and Organization Research. Group & Organization Management, Vol. 34, No. 1, 5-36, 2009.

[39] Sykes, G. M., and Matza, D., Techniques of Neutralization: A Theory of Delinquency. American Sociological Review, Vol. 22, pp. 664-670, 1957.

[40] Symantec, What's Yours is Mine: How Employees are Putting Your Intellectual Property at Risk. Ponemon Institute White Paper, 2013.

[41] White, J., Bandura, A., and Bero, L. A., Moral Disengagement in the Corporate World. Accountability in Research, Vol. 16, pp. 41-74, 2009.

[42] Yim, M. S., Understanding an Employee Information Systems Security Violations. Journal of Digital Policy and Management, Vol. 11, No. 2, pp. 19-32, 2013.

[43] Yoon, C., Theory of Planned Behavior and Ethics Theory in Digital Piracy: An Integrated Model. Journal of Business Ethics, Vol. 100, No. 3, pp. 405-417, 2011.

임 명 성(Yim, Myung-Seong)

・2002년 2월 : 삼육대학교 경영정보학과(경영 학사)
・2004년 2월 : 한국외국어대학교 경영정보대학원(경영학 석사)
・2011년 8월 : 서강대학교 경영전문대학원(경영학 박사)
・2011년 8월 ~ 2012년 2월 : 서강대학교 경영학부 대우교수
・2012년 3월 ~ 현재 : 삼육대학교 경영학과 조교수
・관심분야 : 정보보안, 서비스 시스템, 정보 심리학, 연구 방법론
・E-Mail : msyim@syu.ac.kr