연구논문 정보화정책 제25권 제3호, 2018년 가을호, pp. 95-115
https://doi.org/10.22693/NIAIP.2018.25.3.095

조직 구성원들의 보안정책 위반에 관한 연구*

김 종 기**, 오 다 운***

요 약 본 연구는 조직 구성원들의 보안정책 위반의도를 설명하기 위해 사람-환경 적합 모델(P-E Fit Model: Person-Environment Fit Model)을 기반으로 연구하였다. 보안정책 위반의도에 있어서 조직이 제공하는 보안 환경과 보안에 대한 개인의 가치 간 관계가 어떤 영향을 미치는지 설명하고자 하였다. 조직 구성원이 관찰할 수 있는 보안 환경을 조직의 정보보안 문화와 동료의 보안 준수 행동으로 설정하였고 보안에 대한 개인적 가치는 도덕 이탈 이론에서 제시하는 행동의 재구성, 결과의 왜곡, 조직의 가치감소로 설정하였다. 도덕 이탈 이론의 구성 개념을 바탕으로 조직원의 보안 위반에 대한 인식을 2차 요인(Second Order)으로 측정하였다. 인식의 측정은 조직 내에서 흔히 일어날 수 있는 패스워드 공유 상황을 시나리오로 제시하여 설문을 조사하였다. 연구 결과, 정보보안 문화가 조직의 가치감소에 통계적으로 유의한 영향을 미쳤으나 행동의 재구성과 결과의 왜곡에는 유의한 영향을 미치지 않았다. 동료의 보안 행동은 보안 위반 행동에 대한 재구성, 결과의 왜곡, 조직의 가치감소에 유의한 영향을 미쳤으며 행동의 재구성, 결과의 왜곡, 조직의 가치감소는 조직원의 보안정책 위반의도에 유의한 영향을 미쳤다. 본 연구는 실제 조직 내에서 발생하는 문제를 적용했다는 점에서 실무적인 기여도가 있을 것으로 판단된다.

주제어: 정보보안, 보안정책위반, 사람-환경 적합 모델, 도덕 이탈 이론

A Study on Security Policy Violations of Organization Members

Kim, Jong-Ki, Oh, Da-Woon

Abstract This study aims to examine organization members' intention to violate security policies based on the Person-Environment Fit Model. This study investigated the effect of the relationship between organizational security environment and the individual security value on the intention of organizational security policy violation. The security environments are classified into the organizational information security culture and peers' behavior of security compliance, while the personal values are classified into reconstructing the conduct, distorting the consequence, and devaluing the organization as presented in the moral disengagement theory. Based on the concept of the moral disengagement theory, we measured the individual security values as a second order factor. This study found that the information security culture had a statistically significant impact on devaluing the organization, but did not have as much impact on reconstructing the conduct and distorting the consequence. Peers' behavior of security compliance had a significant impact on reconstructing the conduct, distorting the consequence and devaluing the organization, all of which also had relevant impact on the organizational members' intention of security policy violation.This study measured a persons' perception on security policy breach by presenting scenarios of password sharing that is common in many organizations. This study is expected to make practical contributions, as it deals with challenges that many organizations are actually faced with.

Keywords: information security, security policy violation, person-environment fit model, moral disengagement theory

2018년 7월 12일 접수, 2018년 7월 17일 심사, 2018년 8월 22일 게재확정
* 이 논문은 부산대학교 기본연구지원사업(2년)에 의하여 연구되었음
** 부산대학교 경영학과 교수(jkkim1@pusan.ac.kr)
*** 교신저자, 부산대학교 경영학과 박사과정(odw@pusan.ac.kr)

Ⅰ. 서론

기업은 시스템의 결함과 기술적 문제, 조직 구성원들의 정보 자원 오·남용 등 내·외부로부터 다양한 보안 위협에 노출되어 있다. 그러므로 정보를 보호하기 위해 체계적인 보안 관리 시스템을 도입하고 자체적으로 보안정책 수립 및 교육을 실시하는 기업이 증가하고 있다. 그러나 실제로 기업 차원에서 행하는 보안위반 행위의 규제가 미흡하고 조직 구성원들의 낮은 보안 인식으로 외부로 기업 정보가 유출되거나 취약점이 노출되는 등 문제가 급격히 증가하고 있다.

보안 기술이 향상되면서 최종 사용자에게 요구되는 작업 지식이나 시간 부담을 줄이기 위해 보안 패치 관리, 업데이트 등 다양한 작업들이 자동화되고 있다(Herath & Rao, 2009). 컴퓨터와 네트워크 자원을 올바르게 사용하는 법, 주기적인 패스워드 관리, 데이터 백업 관리 등은 보안 기술보다 조직 내 보안정책을 통해 다루어진다. 즉, 기술적인 부분에서 발생할 수 있는 취약점은 사용자의 올바른 관리 습관으로 예방할 수 있으며 조직 내에서 보안 교육을 실시함으로써 최종 사용자의 보안 인식을 높일 수 있다.

정보시스템에 대한 조직원의 비윤리적 행동은 정보보안 위험에 영향을 미치며 조직의 문제로 대두되었다(Chu & Chau, 2014). 버라이즌 데이터 유출 조사 보고서(Enterprise Verizon, 2017)에 따르면 조직 내 보안 위반 행위에 있어 내부자 소행은 전체의 25%에 달했다. KISA Report(2018)에서는 미국 500개 기업을 대상으로 한 조사에서 보안 사고의 52.5%가 내부자와 연관이 있으며 연평균 27.5%씩 증가한다고 하였다. 조직에 악의적인 의도를 가지고 보안 위반을 하는 경우도 있으나 악의적 의도 없이 개인의 업무 성과나 효율성을 높이기 위해 가볍게 행할 수 있는 보안 위반 행동이 조직 내에서 흔히 발생하고 있다. 그러나 위반 행위의 경중을 떠나 조직에 잠재적 손실 가능성을 제공하는 것은 마찬가지다.

많은 기업은 특정 보안 사고를 겪지 않아도 매년 동일한 방어 체계를 유지해야 하는데 기업의 방어 체계가 조직이 당면한 위협에 부합하는지 확인해야 한다. 그 중 내부자 위협은 기술적 조치와 더불어 조직 차원에서 제공되는 보안 교육으로 다루어져야 한다. 내부자는 조직의 정보 기술 인프라에 합법적으로 접근할 수 있기 때문에 악의적 의도를 가진다면 다른 사람의 개인정보와 기록을 보고 신원 도용이나 복사를 할 수 있다(Siponen & Vance, 2010; Padayachee, 2016). 특정 권한이 요구되는 ID의 비밀번호를 공유함으로써 문제가 발생할 수 있으므로 사전에 예방교육이 필요하다.

조직의 성공적인 정보보안 달성은 조직에서 제공하는 보안 관련 체계를 효과적으로 사용하는 개인의 행동에 달려 있다(Stanton, et al., 2003). 전제 정보시스템 보안정책 위반의 반 이상은 직원들이 자신의 업무에 적용되는 보안정책을 무시하거나 부주의함으로써 나타났다(Vroom & von Solms, 2004). 정보시스템 보안 거버넌스가 개인의 가치, 신념, 정책 준수를 장려하지 않는다면 조직 내 직원의 보안 위반 행동을 예방하는 프로그램이 실패할 수 있다(Mishra & Dhillon, 2006).

조직은 사회적 집단이자 구성원 개인들의 집합이므로 개개인이 형성한 집단의 보안문화와 조직에서 나타나는 개인의 행동을 분리해서 이해할 수 없다. 본 연구에서는 조직에서 형성된 보안 문화와 동료의 보안 관련 행동이 보안정책 위반 의도에 어떤 영향을 미치는지 연구하고자 하였다. 또한 이 과정에서 개인의 심리적 합리화가 어떻게 적용되는지 도덕 이탈 이론을 기반으로 실증적으로 분석하였다.

Ⅱ. 이론적 배경

1. 정보보안 위반 연구

정보보안에 있어서 조직 구성원들의 일탈 행동이란 “조직원들이 자발적으로 조직 내의 정보보안 규범과 다르게 행동하는 것”으로 정의한다(Chu & Chau, 2014). Chu & Chau(2014)는 일탈 행동의 세 가지 구

〈표 1〉 정보보안 위반 관련 개념

개념	정의	예시	선행연구
정보시스템 자원 오용	직장의 애플리케이션, 인터넷, 네트워크 등을 포함하는 정보시스템 자원을 내부자가 의도적으로 오용	부적절한 이메일 전송, 불법 소프트웨어 사용, 비 인가된 데이터 접근 및 변경	Hovav & D'Arcy (2012), Chu, et al. (2015), Guo(2013)
정보보안 일탈 행동	조직 구성원들이 조직의 중요한 보안정책을 자발적으로 위반하는 행동	정보시스템 자원 남용, 게으른 보안 행동	Chu & Chau(2014)
정보보안정책 위반 행동	조직 구성원들의 정보보안정책 무시 및 부주의한 행동	민감한 데이터 USB에 복사, 외부에 기밀 데이터 노출	Cheng, et al.(2013), Guo(2013)
게으른 보안 행동	정보시스템 보안에 대해 인식을 하지만 보안 위협이나 대처 행동을 무시하는 행위	패스워드 미변경, 보안 패치 업데이트 하지 않음, 백업하지 않음	Workman, et al.(2008), Cox(2012)

성요소로 자발적 행위를 뜻하는 의도성, 행동의 부정적인 특성, 조직 내 위반 행동을 하는 사람으로 구분하였다. 해커와 같이 외부인이 연루되거나 우발적으로 발생하는 사고, 인적 자원과 관련 없는 사고는 이 세 가지 구성요소를 충족시키지 못하므로 일탈 행동에서 제외한다. Guo, et al.(2011)은 정보보안 위반 행동의 특성을 네 가지로 구분하였다. 첫째, 사용자의 의도적인 행동으로 "의식적으로 결정"하는 것을 강조하였다. 둘째, 악의적인 의도 없이 스스로 이득을 얻고자 하는 것이다. 기업의 정보를 외부로 파는 등의 범죄 행위가 아니라 조직 내에서 처리되는 비 범죄적 행위를 말한다. 조직 내 규칙과 정책을 따르는 데 소모되는 시간과 노력을 절약하고자 행동하는 것으로 금전적 이득을 취하는 행동은 포함하지 않는다. 셋째, 자발성으로 조직의 보안 정책을 자신의 의지에 따라 선택적으로 위반하는 것이다. 넷째, 보안의 위험이나 손상을 초래할 수 있다. 정보보안 위반을 하는 데 있어 악의적인 의도가 없더라도 결과적으로 조직의 정보 자원을 노출하거나 위험에 처하게 만들 수 있다. 정보보안 위반 관련 개념은 〈표 1〉과 같다.

정보보안 위반 행동에 사용되는 대표적인 이론으로는 억제 이론(Deterrence Theory)이 있다. 억제 이론은 개인이 범죄 행위를 하기 전에 그 행위에 대한 처벌의 확실성, 심각성, 신속성이 범죄 의사결정에 영향을 미친다는 것이다. Guo & Yuan(2012)은 조직의 처벌과 직무 그룹의 처벌, 개인적 자기 처벌이 정보보안 위반에 미치는 영향을 연구하였다. Siponen & Vance(2010)는 중화 이론(Neutralization Theory)을 바탕으로 여섯 가지 중화 요인과 억제 요인이 보안정책 위반 의도에 미치는 영향을 연구하였다. Chu & Chau(2014)는 이중 처리 이론(Dual-Process Theory)과 계획된 행동 이론(Theory of Planned Behavior)을 적용하여 IS 자원 남용 의도에 대해 연구를 하였으며, Vance & Siponen(2012)은 합리적 선택 이론(Rational Choice Theory) 관점에서 IS 보안정책 위반을 연구하였다.

정보보안 위반 관련 선행 연구로 Cheng, et al.(2013)은 정보시스템 보안정책 위반 의도에 있어서 공식적인 통제와 사회적 유대, 사회적 압력이 미치는 영향을 연구하였다. Guo, et al.(2011)은 악의적이지 않은 보안 위반 의도에 대해 연구하였으며, Workman, et al.(2008)은 게으른 보안 행동에 있어서 위협 평가와 대처 평가를 적용하여 연구하였다. D'Arcy, et al.(2009)은 정보시스템 남용의도에 있어서 보안정책, SETA 프로그램 인식, 컴퓨터 모니터링과 인지된 처벌의 인식이 미치는 영향을 연구하였다. 정보보안 위반 관련 연구는 〈표 2〉와 같다.

〈표 2〉 정보보안 위반 관련 연구

연구자	선행요인	매개요인	결과요인
Safa, et al.(2018)	• 상황적 범죄 예방 이론 - 노력의 증가 - 위험의 증가 - 보상 감소 - 자극 감소 - 구실 제거 • 사회 유대 이론 - 애착 - 헌신 - 참여 - 개인적 규범	• 부정행위에 대한 부정적 태도 • 부정행위 의도 감소	• 내부자 위협 감소
Hsu, et al.(2015)	• 부서 차원 - 외부 역할 행동 - 내부 역할 행동 • 개인 차원 - 사회 통제(참여, 애착, 신념, 헌신) - 공식 통제(명시, 평가, 보상)	**상호작용 효과** 사회통제×공식통제	• 부서 차원 - 정보보안정책 효과 • 개인 차원 - 외부 역할 행동 - 내부 역할 행동
Chu, et al.(2015)	• 정보시스템 자원 남용 태도 • 주관적 규범 • 인지된 행동 통제	• 정보시스템 자원 남용 의도 • 정보시스템 자원 남용 욕구	• 정보시스템 자원 남용
Cheng, et al.(2013)	• 공식적 통제 - 인지된 확실성 - 인지된 엄격성 • 사회적 유대 - 애착 - 전념 - 참여 - 신념 • 사회적 압력 - 주관적 규범 - 동료의 행동	-	• 정보시스템 보안정책 위반의도
이정하··이상용(2015	• 지각된 처벌의 확실성 • 지각된 처벌의 심각성 • 일반 정보보안 인식 • 정보보안정책 인식	• 정보보안정책 태도 • 정보보안정책에 대한 주관적 규범 **조절 효과** • 지각된 고객정보의 민감도	• 정보보안정책 위반의도

2. 사람-환경 적합 모델

사람-환경 적합 모델(P-E Fit Model: Person-Environment Fit Model)은 상호 심리학을 기반으로 하며, 개인의 특성과 환경의 조화는 개인의 행동에 영향을 미친다고 가정한다(Chatman, 1989). 초기의 행동 연구는 개인의 행동에 영향을 주는 요인을 개인적 관점과 환경적 관점으로 분류하여 제안하였으나 사람-환경 적합 모델은 두 가지 관점을 포괄하여 설명한다(Lee, et al., 2016). 이 관점은 환경의 요구와 개인의

능력이 부합할 때 상호적으로 만족된다는 작업 조정 이론에서 개발되었다. 본 모델은 사람-직무 적합, 사람-상사 적합, 사람-그룹 적합, 사람-조직 적합 등을 설명하기 위해 다양한 연구에서 적용되어 왔다(Edwards, 2007).

사람-환경 적합 모델에서는 환경적인 특성과 개인적 특성이 조화를 이룰 때 '적합(Fit)하다' 표현하며 적합의 효과가 높을수록 긍정적인 결과로 이어진다고 가정한다. 그러나 환경적 특성과 개인의 특성 사이에 차이가 발생할 때 부적합이 발생한다. 부적합(Misfit) 또는 차이(Gap)는 접근 방식과 상관없이 두 가지로 설명할 수 있다(Edwards, 1996). 첫 번째 유형은 개인이 선호하고 의식하는 가치(Values)와 그 가치를 충족시킬 수 있는 환경적 제공(Supplies) 사이에서 발생한다. 개인이 원하는 것과 조직에서 제공하는 것 간의 차이를 평가하거나 개인의 욕구가 조직을 통해서 어떻게 충족될지 평가함으로써 판단 할 수 있다. 두 번째 유형은 개인의 능력(Abilities)과 환경적 요구(Demands) 사이에서 발생한다. 능력은 개인이 가지는 기술, 지식, 시간, 에너지이며 요구는 개인에게 주어진 요구사항에 대한 주관적 평가를 말한다. 개인의 능력보다 조직의 요구가 초과할 때 부적합이 발생한다. 가치-제공(Values-Supplies)과 능력-요구(Abilities-Demands) 적합은 상호 보완적 접근법을 통해 형성된다(Ayyagari, et al., 2011).

Lee, et al.(2016)은 정보보안정책에 있어서 조직의 요구가 개인의 능력을 초과할 때 정보보안 스트레스가 발생하며, 직원들이 정보보안을 준수할 능력이 될 때 스트레스가 최소화된다고 보았다. Ayyagari, et al.(2011)은 ICT 환경의 기술적 특성과 개인적 스트레스 요인의 부적합을 테크노 스트레스로 설명하였다. Silverthorne(2004)는 조직 몰입과 직무 만족에 있어서 조직 문화의 영향을 설명하였고, D'Arcy, et al.(2014)은 조직원의 스트레스를 유발하는 보안 요구사항의 특성과 도덕 이탈 요인의 관계를 설명하여 조직원의 정보보안정책 위반 의도를 연구하였다.

3. 도덕 이탈 이론

도덕 이탈 이론은 사회 인지 이론을 기반으로 하며, 자신의 행동이 올바르지 못하다고 인지함에도 불구하고 이 행동이 타당하다고 합리화하는 과정을 설명한다. 서로 관계가 있는 여덟 가지 인지적 메커니즘을 세 가지 카테고리로 분류하여 개념화하고 이 메커니즘은 행동을 통제하는 내부적 자기 처벌에서 자유로운 상태로 만든다(D'Arcy, et al., 2014).

도덕 이탈 이론은 부적절하고 비정상적인 행동을 예측할 수 있다. 일부 사람들은 자신의 행동을 부도덕하거나 비윤리적 행동으로 인지하지 못하고 보안 위반 행동을 하는 것으로 나타났다(D'Arcy, et al., 2014). Bandura, et al.(1996)은 사람들이 자신의 행동을 올바르다고 정당화하기 전까지 비난받는 행동을 하지 않으며, 인지적 재구성을 통해 비난받는 행동을 옳은 것으로 간주한다고 설명하였다.

비난받는 행동을 자신 또는 조직을 위한 행동으로 정당화하거나 해를 가하는 정도를 감소시켜 표현하여 타인이 건전한 행동으로 받아들이도록 한다. 또한 상대적으로 비난받는 강도가 높은 다른 행동과 비교하여 자신의 행동이 덜 해로운 것처럼 인지하게 만듦으로써 유해한 행동을 용인 가능한 행동으로 재구성한다.

사람들은 자신의 행동으로 발생한 문제의 책임을 묻게 될 경우 그들이 야기한 피해를 회피하거나 최소화하며 결과를 왜곡하는 경향이 있다. 이 과정에서 책임을 다른 사람에게 전가하거나 여러 사람과 분담할 수 있는 상황이 생길 경우 자기 통제력이 더 약해지게 되어 비도덕적으로 행동할 수 있다. 그리고 자신들이 해를 가한 행동의 원인을 피해 받은 대상의 문제로 돌림으로써 자신의 행동을 합리화할 수 있다. D'Arcy, et al.(2014)의 연구에서 제시한 도덕 이탈 메커니즘에 대한 설명은 〈표 3〉과 같다.

도덕 이탈 이론을 적용한 선행 연구들은 Bandura, et al.(1996)이 제시한 32가지 측정 항목 중 연구와 부합하는 내용을 적용하여 조직 구성원들의 사회적 태만,

〈표 3〉 도덕 이탈 메커니즘(D'Arcy, et al., 2014)

카테고리	메커니즘	정의
행동의 재구성	도덕적 정당화	유해한 행동을 가치 있고 도덕적인 목적을 가진 것으로 묘사함으로써 개인적으로나 사회적으로 용인될 수 있는 것으로 재구성
	완곡한 표현	건전한 행동으로 표현하거나 왜곡된 단어, 개념을 사용하여 유해한 행동을 듣기 좋게 표현
	경감식 비교	유해한 행동을 더 비난받는 행동과 비교함으로써 용인될 수 있는 것으로 고려
결과의 모호성 또는 곡해	책임의 전가	유해한 행동에 대한 책임의 소재가 자신보다 사회적 압력 또는 상급자의 지시로 인한 것으로 여김
	책임의 분산	유해한 행동에 대한 개인적 책임은 스스로 지는 것 보다 집단적으로 분산하여 가져야 한다고 생각
	결과의 왜곡	개인의 유해한 행동으로 인한 결과를 의식적으로 무시, 축소, 왜곡하는 것
대상의 가치 감소	비인간화	유해한 행동의 원인을 피해받는 대상의 인격적 문제로 돌림
	비난의 귀속	유해한 행동을 개인적 결정이라기보다는 환경이나 통제할 수 없는 상황 탓으로 돌림

〈표4〉 도덕 이탈 이론 관련 연구

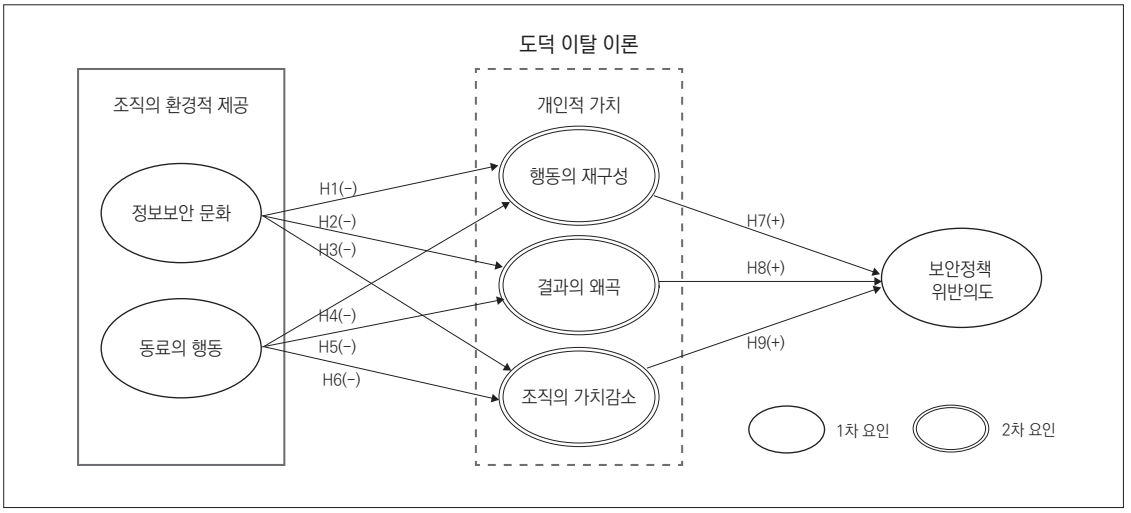
연구자	선행요인	매개요인	결과요인
Alnuaimi, et al.(2010)	• 팀 규모 • 팀 분산	• 책임의 분산 • 비인간화 • 비난의 귀속	• 사회적 태만
임명성(2013)	• 도덕적 해방 • 정보보안 인식 • 도덕적 신념 • 처벌에 대한 인지	-	• 보안정책 위반
Deter, et al.(2008)	• 이해심 • 냉소주의 • 통제의 소재 • 도덕성	• 도덕 이탈	• 비윤리적 의사결정
Moore, et al.(2012)	• 도덕 이탈 성향	• 도덕 인식	• 비윤리적 의사결정

보안정책 위반, 비윤리적 의사 결정 등 조직 내에서 발생할 수 있는 일들을 실증적으로 연구하였다. 도덕 이탈 이론 관련 연구는 〈표 4〉와 같다.

Ⅲ. 연구모형 및 가설

1. 연구모형

본 연구는 사람-환경 적합 모델을 기반으로 보안정책 위반에 있어서 조직에서 제공하는 환경적 요인과 보안 위반에 대한 개인적 가치의 부적합을 측정하기 위해 〈그림 1〉과 같은 연구 모형을 설계하였다. 개인이 선호하는 가치와 그 가치를 충족시키는 환경적 제공 간 관계를 설명하기 위해 환경적 요인은 객관적으로 판단하고 측정이 가능한 정보보안 문화와 동료의 행동으로 설정하였다. 개인의 도덕적 자기 통제감을 설명하는 행동의 재구성, 결과의 왜곡, 조직의 가치감소를 2차 요인으로 설정하여 도덕 이탈 이론에서 제시하는 여덟 가지



〈그림 1〉 연구모형

개념을 포괄적으로 설명하고자 하였다. 본 연구의 모형은 〈그림 1〉과 같다.

2. 연구 가설

문화란 조직을 구성하는 개인들이 공유하는 신념 또는 가치관, 관행 등 모든 의미를 포함하는 포괄적인 개념이다. 기업이나 조직은 개개인의 집단으로 이루어진 하나의 사회집단이며, 집단에서 형성된 문화는 개인의 행동에 영향을 미친다.

보안 문화는 조직의 모든 구성원에 의해 형성된 정보보안의 가치와 신념을 반영한다(Greene & D'Arcy, 2010). 보안 문화는 조직 내 적절한 정보보안 수준을 유지시키는 주요한 요인이며, 조직원들의 보안 관련 의사결정을 장려하고 정책 준수 행동에 영향을 미친다.

적절하게 구축된 보안 문화는 조직 구성원의 책임감을 증진시키고 보안 관련 의사결정에 대한 소유의식을 고취시킨다. 구성원들이 보안에 대한 가치의 중요성을 인지한다면 가벼운 보안 위반으로 인해 야기되는 조직의 위험을 이해할 수 있다. 조직 구성원들은 조직의 정보보안 수행의 목표보다 개인적 업무 성과에 중점을 두고 있으므로 정보보안 관련 상황에 직면했을 때 자신을 둘러싼 환경과 보유한 정보를 기반으로 의사결정을 한다(황인호 외, 2016). 직무 성과 및 효율성 등 개인적 가치를 위해 보안 위반 행위를 정당화하는 비윤리적 행동을 감소하기 위해 조직의 보안 문화 정립이 필수적이다. 이러한 내용을 바탕으로 다음과 같은 가설을 설정하였다.

H1. 조직의 정보보안 문화는 보안정책 위반에 있어서 행동의 재구성에 부(-)의 영향을 미칠 것이다.

H2. 조직의 정보보안 문화는 보안정책 위반에 있어서 결과의 왜곡에 부(-)의 영향을 미칠 것이다.

H3. 조직의 정보보안 문화는 보안정책 위반에 있어서 조직의 가치감소에 부(-)의 영향을 미칠 것이다.

정보보호와 관련된 개인의 행동은 조직 내 다른 사람의 정보보호 행동을 반영한 개인의 인식 상태이다(김혜정·안중호, 2013). 개인은 조직 내 다른 구성원에게서 볼 수 있는 표현이나 행동을 보고 가치를 판단하면서 직·간접적인 영향을 받는다.

다른 조직원들의 보안 준수 행동은 개인이 관찰할 수 있는 보안 환경이 되며, 보안의 우선순위를 촉구하고 보안 준수 분위기를 장려할 수 있는 환경적 요인이다(Dang, et al., 2015). 개인은 다른 구성원들의 보안 행동을 보고 사회적 영향을 받아 비윤리적 행위를 쉽게 할 수 없다. 이러한 내용을 바탕으로 다음과 같은 가설을 설정하였다.

H4. 조직원의 행동은 보안정책 위반에 있어서 행동의 재구성에 부(-)의 영향을 미칠 것이다.

H5. 조직원의 행동은 보안정책 위반에 있어서 결과의 왜곡에 부(-)의 영향을 미칠 것이다.

H6. 조직원의 행동은 보안정책 위반에 있어서 조직의 가치감소에 부(-)의 영향을 미칠 것이다.

행동의 재구성은 도덕적 정당화, 완곡한 표현, 경감식 비교를 바탕으로 설명할 수 있다. 도덕적 정당화란 유해한 행동을 사회적, 도덕적으로 가치 있는 행동으로 묘사함으로써 개인과 사회에서 받아들여 지도록 한다(Bandura, 1999). 사람들은 사회적, 도덕적 의무에 따라 행동하므로 일상에서 비난받을 수 있는 행동을 개인의 명예와 평판을 보호하거나 더 큰 이익을 위한 행동으로 정당화한다. 예를 들어, 자신의 업무를 더 효율적으로 수행하거나 조직에 향상된 서비스를 제공하기 위해 정보보안 위반행위를 정당화 할 수 있다(D'Arcy, et al., 2014).

완곡한 표현은 유해한 행동을 점잖은 행동으로 만들고 그 행동에 대한 개인적 책임을 감소시키는 데 사용된다(Bandura, et al., 1996). 예를 들어, 정보보안정책 위반 행동을 잘못된 것이 아닌 '별일 아닌 것'으로 완곡하게 표현할 수 있다. 위반 행동을 완곡하게 표현함으로써 직원들이 정보보안 위반에 대한 문제를 대수롭지 않게 받아들일 수 있으며 직장 내에서 흔히 일어나는 일이라고 생각하여 위반 행동 의도가 증가될 수 있다.

개인의 행동은 무엇과 비교되느냐에 따라 다른 문제로 가정할 수 있다. 더 비난받는 행동과 비교함으로써 부적절한 행동이 문제가 없는 것처럼 보이거나 사소한 문제로 보일 수 있다. 상대적으로 비교되는 문제가 더 심각할수록 자신의 부적절한 행동을 사소하거나 자비로운 것으로 느낄 수 있다(Bandura, et al., 1996). 예를 들어, 기업의 정보 도난과 같은 심각한 사건과 조직 내에서 패스워드를 공유하거나 데스크톱 로그아웃을 하지 않는 등 흔히 볼 수 있는 정보보안 정책 위반 행동을 비교하며 상대적으로 무해한 보안 위반 행동으로 재구성할 수 있다(D'Arcy et al., 2014). 그러므로 다음과 같은 가설을 설정하였다.

H7. 보안정책 위반에 있어서 행동의 재구성은 보안정책 위반 의도에 정(+)의 영향을 미칠 것이다.

본인의 부적절한 행동으로 인한 결과의 왜곡은 책임의 전가, 책임의 분산, 결과의 축소의 형태로 나타날 수 있다. 개인에 따라 정보보안 가치를 이해하기 어려워하거나 보안의 중요성을 가볍게 여길 수 있다. 책임의 전가는 행동과 행동을 야기하는 영향 간 관계가 왜곡되면서 작용한다. 사람들은 그들의 부적절한 행동이 다른 사람의 지시나 압력으로 인해 일어나는 것으로 인지한다. 예를 들어, 직원이 업무가 과부하 된 상황에서 보안 위반 행동을 했을 경우, 조직에서 업무를 완수할 수 있는 대체 방안을 수립하지 않았으므로 보안 위반 행동에 대한 책임은 조직에게 있다고 판단할 수 있다. 이러한 인식은 보안정책 위반 의도를 높일 수 있다.

도덕적 책임은 개인이 야기한 문제 행동에 대한 책임이 분산되어 애매해질 때 약해진다(Bandura, 1999). 집단행동은 도덕적 통제를 약화시키는 수단으로 자신의 행동에 대해 개인이 책임지는 것보다 조직원들과 책임이 분산되는 상황에서 더 무책임하게 행동한다. 그러므로 IS 보안 측면에서 경영진, IT 부서, 그 외 다른 직원들과 책임이 분산되어 있다고 인지할수록 보안정책 위반 의도가 높아진다(D'Arcy, et al., 2014).

자기 억제력을 약화시키는 방법은 행동의 결과를

축소시키는 것이다. 개인의 이익을 위해 다른 사람에게 피해 주는 행동을 한 경우, 그들의 행동으로 야기된 문제를 피하거나 최소화하는 경향이 있다(Bandura, 1999). 예를 들어, 직원들이 적어도 조직에 직접적으로 손해를 입히지 않았다고 간주함으로써 보안 위반 행동의 결과를 축소시킬 수 있다. 이러한 왜곡은 보안정책 위반 의도를 높일 수 있으므로 다음과 같은 가설을 설정하였다.

H8. 보안정책 위반에 있어서 결과의 왜곡은 보안정책 위반 의도에 정(+)의 영향을 미칠 것이다.

대상의 평가 절하 또는 가치감소는 인지적 이탈 메커니즘으로 피해 받는 대상에게 문제와 비난을 돌린다. 직원은 조직이 정보보안을 관리하는 방식을 평가절하 함으로써 보안정책 위반을 정당화할 수 있다. 비난의 귀속이란 개인의 보안정책 위반 행위를 개인적 결정보다 환경이나 환경 주변과 같이 자신의 통제를 벗어난 부득이한 상황 탓으로 설명한다(D'Arcy, et al., 2014). 개인은 강제적 자극 또는 도발로 인해 부적절한 행동을 할 수밖에 없었던 희생자로 보고 스스로에게 면죄를 준다(Bandura, et al., 1996). 예를 들어, 보안정책 위반은 정책의 엄격성이나 부당한 특성의 결과로 일어난다고 보며 이러한 인식은 보안 위반 의도를 높일 수 있다. 그러므로 다음과 같은 가설을 설정하였다.

H9. 보안정책 위반에 있어서 조직의 가치감소는 보안정책 위반 의도에 정(+)의 영향을 미칠 것이다.

Ⅳ. 실증분석

1. 조작적 정의

본 연구는 조직 내 보안 환경과 개인적 가치의 부적합이 보안정책 위반의도에 미치는 영향을 살펴보기 위하여 도덕 이탈 이론의 구성 개념을 개인적 가치로 설정하고 2차 요인으로 조직 구성원의 인식을 실증적으로 측정하였다. 연구모형에서 사용되는 개념들을 구체적이고 명확하게 이해할 수 있도록 변수의 조작적 정의를 내렸다. 도덕 이탈 이론에서 행동의 재구성을 형성하는 요인은 도덕적 정당화, 완곡한 표현, 경감식 비교로 구성하였다. 결과의 왜곡은 책임의 전가, 책임의 분산, 결과의 축소로 구성하였으며 조직의 가치감소는 비인간화, 비난의 귀속으로 구분하여 측정항목을 개발하였다. 연구의 측정항목은 부록A와 같다.

본 연구에서는 사회과학 연구에서 흔히 사용되는 리커트 척도를 통해 응답자의 인식을 측정하였다. 구성개념의 측정 항목에 대한 응답자의 정밀성을 높이기 위해 리커트 7점 척도로 "매우 동의하지 않음"에서 "매우 동의함"으로 설정하여 개인의 인식과 의도를 측정하였다. 본 연구의 조작적 정의는 〈표 5〉와 같다.

2. 자료수집 및 분석

본 연구의 설문조사는 부산대학교 MBA 학생들을 대상으로 실시하였다. 회수된 설문지 172부 중 불성실한 응답(전체 항목을 동일하게 답하거나 중간 값으로 응답)을 하거나 결측치를 포함한 설문지를 제외한 156부를 최종 분석 데이터로 사용하였다. SPSS Statistics 21을 사용하여 기초적인 분석을 실시하였고 연구모형을 분석하기 위해 SmartPLS 2.0을 사용하였다.

본 연구에서는 시나리오 기법을 적용하여 개인의 행동의도를 측정하였다. 응답자들이 시나리오를 읽는 즉시 본인에게 이입하여 답변할 수 있는 방법이나, 반사회적 및 비윤리적 행동을 측정하는데 흔히 사용되는 기법인 만큼 자신이 사회적으로 추구하는 모습을 응답에 반영할 수 있다는 한계가 존재한다. 본 연구에서는 '조직 내 개인의 보안 위반 행동'이라는 주제가 설문을 답하는 직장인에게 다소 민감한 주제로 받아들여 질 수 있으며 위반이라는 단어에 편향(Bias)이 발생할 수 있다고 판단하였다. 그러므로 조직 내에서 악의적인 의도

〈표 5〉 조작적 정의

개념			정의	관련 연구
행동의 재구성	개인의 보안정책 위반 행위를 용인될 수 있는 행동으로 재 개념화 하는 정도	도덕적 정당화	보안정책 위반행위를 정당한 것으로 인지하는 정도	Bandura, et al.(1996); D'Arcy, et al.(2014)
		완곡한 표현	건전하게 표현된 보안정책 위반행위를 인지하는 정도	
		경감식 비교	상대적으로 더 심각한 사건과 비교하여 보안정책 위반행위를 인지하는 정도	
결과의 왜곡	개인의 보안정책 위반 행위로 인한 결과의 책임을 왜곡하여 인지하는 정도	책임의 전가	개인의 보안정책 위반행위에 대한 책임이 조직에게 있다고 인지하는 정도	
		책임의 분산	개인의 보안정책 위반행위의 책임이 여러 사람에게 있다고 인지하는 정도	
		결과의 축소	개인의 보안정책 위반행위로 인한 문제의 심각성을 축소하여 인지하는 정도	
조직의 가치감소	개인의 보안정책 위반 행위를 조직의 제도적 문제로 인지하는 정도	비인간화	개인의 보안정책 위반행위를 조직의 비인격적 문화의 문제로 인지하는 정도	
		비난의 귀속	개인의 보안정책 위반 행위를 조직의 정책 문제로 인지하는 정도	
정보보안 문화			조직에서 공유되고 있는 정보보안 상황에 대한 구성원들의 인식	Greene & D'Arcy(2010)
동료의 행동			동료들의 보안 인식에 대해 인지하는 정도	Chan, et al.(2005)
보안정책 위반의도			보안정책을 위반하고자 하는 정도	Guo, et al.(2011); Siponen & Vance(2010)

〈패스워드 공유 상황 시나리오〉

당신은 A 회사의 직원입니다. 당신이 외근을 나간 사이(또는 부득이하게 회사에서 자리를 비운 경우) 업무상 급하게 필요한 파일이 생겼습니다. 조직 내 패스워드 공유가 금지된 경우 당신은 가까운 동료에게 본인 컴퓨터의 패스워드를 알려주며 파일을 보내 달라고 하시겠습니까?

〈그림 2〉 시나리오

없이 가볍게 행할 수 있는 보안 위반 상황을 시나리오로 설정하여 설문지에 명시하고 상황을 인지 후 답변을 하도록 요청하였다. 본 연구에서 사용된 설문의 시나리오는 〈그림 2〉와 같다.

설문 대상 전체 응답자 156명 중 남성이 120명(76.9%)으로 여성보다 비율이 높았으며, 산업 분야는 제조 분야가 45명(28.8%)으로 가장 높았다. 부장/차장 직위가 49명(31.4%)으로 가장 높았으며, 조직 내 보안 위반 행동에 대한 제재로 경영진의 견책이 53명(34.0%)으로 가장 높았다. 조직에서 수행되는 보안 활동으로 운영체제 및 고급 보안 소프트웨어 설치가 35명(22.4%)으로 가장 높았다. 본 연구의 표본 특성은 〈표 6〉과 같다.

〈표 6〉 표본의 특성

변수	구분	빈도(명)	비율(%)
성별	남성	120	76.9
	여성	36	23.1
	계	156	100.0
산업분야	제조	45	28.8
	물류/유통/서비스	36	23.1
	금융/보험	22	14.1
	전자 전기/정보통신	10	6.4
	기타	43	27.6
	계	156	100.0
직위	이사급 이상	34	21.8
	부장/차장	49	31.4
	과장/대리	47	30.1
	사원	26	16.7
	계	156	100.0
보안위반 행동제재	정해진 제재 없음	51	32.7
	경영진 견책	53	34.0
	직무 정지	11	7.1
	직무 해임	17	10.9
	기타	24	15.4
	계	156	100.0
보안 활동	바이러스 백신 및 방화벽 설치	28	37.2
	데이터 손실 방지 백업 시스템	24	15.4
	운영체제 및 고급 보안 소프트웨어 설치	35	22.4
	보안 취약성 지속 점검	16	10.3
	보안 교육 및 훈련	21	13.5
	보안 위반 규제 강화	2	1.3
	계	156	100.0

3. 측정도구의 평가

1) 1차 요인분석

본 연구 모형의 경로를 분석하기에 앞서 구성개념에 대한 변수의 신뢰성과 타당성을 평가 하였다. 신뢰성과 집중 타당성을 분석하기 위해 Cronbach's α와 합성 신뢰도(C.R: Composite Reliability), 요인적재량(Factor Loading), 평균분산추출(AVE: Average Variance Extracted) 값으로 평가한다(Kim, et al., 2004). 판별 타당성은 구성개념의 평균분산추출 제곱근이 구성개념들 간 상관계수보다 크고 0.7 이상을 기준으로 판단한다(김계수, 2013). 본 연구에서 1차 요인의 신뢰성과 집중타당성을 평가한 결과는 〈표 7〉과 같다.

조직의 환경적 제공은 정보보안 문화와 동료의 행동

〈표 7〉 1차 요인의 신뢰성 및 집중 타당성

잠재변수		측정변수	요인적재량	AVE	C.R	Cronbach's α
정보보안문화		문화1	0.965	0.962	0.990	0.987
		문화2	0.989			
		문화3	0.987			
		문화4	0.982			
동료의 행동		동료1	0.957	0.912	0.976	0.968
		동료2	0.951			
		동료3	0.962			
		동료4	0.951			
행동의 재구성	도덕적 정당화	정당1	0.984	0.984	0.941	0.980
		정당2	0.953			
		정당3	0.973			
	완곡한 표현	표현1	0.940	0.860	0.948	0.919
		표현2	0.913			
		표현3	0.929			
	경감식 비교	비교1	0.980	0.957	0.985	0.978
		비교2	0.971			
		비교3	0.984			
결과의 왜곡	책임의 전가	전가1	0.982	0.982	0.966	0.986
		전가2	0.993			
		전가3	0.974			
	책임의 분산	분산1	0.979	0.965	0.988	0.982
		분산2	0.988			
		분산3	0.981			
	결과의 축소	축소1	0.969	0.922	0.973	0.958
		축소2	0.958			
		축소3	0.953			
조직의 가치감소	비인간화	비인간1	0.967	0.967	0.959	0.986
		비인간2	0.991			
		비인간3	0.979			
	비난의 귀속	비난1	0.986	0.977	0.992	0.988
		비난2	0.988			
		비난3	0.991			
보안위반의도		의도1	0.974	0.953	0.988	0.984
		의도2	0.975			
		의도3	0.981			
		의도4	0.976			

〈표 8〉 1차 요인의 판별 타당성

	문화	동료	정당	표현	비교	전가	분산	축소	비인간	비난	의도
문화	**0.981**										
동료	0.605	**0.955**									
정당	-0.204	-0.293	**0.970**								
표현	-0.207	-0.342	0.753	**0.927**							
비교	-0.294	-0.380	0.470	0.517	**0.978**						
전가	-0.056	-0.217	0.435	0.409	0.182	**0.983**					
분산	-0.015	-0.078	0.294	0.282	0.246	0.441	**0.982**				
축소	-0.253	-0.380	0.664	0.654	0.560	0.361	0360	**0.960**			
비인간화	-0.488	-0.534	0.520	0.495	0.535	0.215	0.152	0.596	**0.979**		
비난	-0.358	-0.408	0.528	0.498	0.575	0.198	0.179	0.634	0.771	**0.988**	
의도	-0.359	-0.487	0.761	0.700	0.574	0.411	0.303	0.722	0.673	0.692	**0.976**

※진하게 표시된 부분은 AVE 제곱근 값

으로 측정하였다. 행동의 재구성은 도덕적 정당화, 완곡한 표현, 경감식 비교로 측정하였고 결과의 왜곡은 책임의 전가, 책임의 분산, 결과의 축소로 측정하였다. 조직의 가치감소는 비인간화, 비난의 귀속으로 측정하였으며 개인적 가치로 설정한 구성개념은 모두 2차 요인으로 측정하였다. 마지막 보안정책 위반의도까지 도출한 결과 Cronbach's α와 합성 신뢰도 값이 권장되는 기준 0.7 이상, 요인 적재량이 0.7 이상, AVE값이 0.5 이상으로(Kim, et al., 2004) 신뢰성과 집중 타당성이 있다고 판단된다. 또한 1차 요인의 판별 타당성 분석 결과 평균분산추출 제곱근 값이 각 구성개념 간 상관계수보다 크게 나타나 판별 타당성이 있는 것을 확인하였다. 본 연구의 판별 타당성 결과는 〈표 8〉과 같다.

2) 2차 요인 분석

본 연구는 구성개념과 측정변수 간 관계를 형성지표로 측정하였다. 형성지표는 측정변수들 간 관계가 서로

〈표 9〉 형성지표의 다중공선성 분석

잠재변수	측정변수	가중치	t값	공차	VIF	상태지수
행동의 재구성	도덕적 정당화	0.519	5.661	0.356	2.806	22.681
	완곡한 표현	0.283	2.650	0.373	2.677	16.746
	경감식 비교	0.374	4.317	0.540	1.852	8.757
결과의 왜곡	책임 전가	0.257	2.809	0.666	1.501	14.775
	책임 분산	-0.064	0.645	0.749	1.336	13.282
	결과 축소	0.904	15.293	0.370	2.699	15.377
조직의 가치감소	비인간화	0.701	6.635	0.317	3.153	12.815
	비난의 귀속	0.354	3.001	0.342	2.923	10.236

독립적이고 상관관계가 낮기 때문에 반영지표에서 측정되는 내적일관성 기준을 적용하지 않는다. 형성지표 측정 시 지표 간 높은 상관관계를 가질 경우 공선성이라 부르며 2개 이상의 형성지표가 포함될 경우 다중공선성이라고 한다.[1] 본 연구의 다중공선성 분석 결과는 〈표 9〉와 같이 나타나 신뢰성이 있는 것을 확인하였다.

4. 구조모형의 설명력

구조모형의 설명력는 R^2 값과 중복성(Redundancy), 공통성(Communality)을 통해서 전체 모형의 평균 설명력을 나타낼 수 있다(Tenenhaus, et al., 2005). 중복성은 양수이며 공통성은 0.5 이상의 값으로 유의하다는 것을 확인하였고 연구모형의 전체 설명력[2]은 0.482로 판단 기준에서 상(0.36 이상)으로 높다고 판단된다. 구조모형의 설명력 결과는 〈표 10〉과 같다.

5. 연구 가설 검정

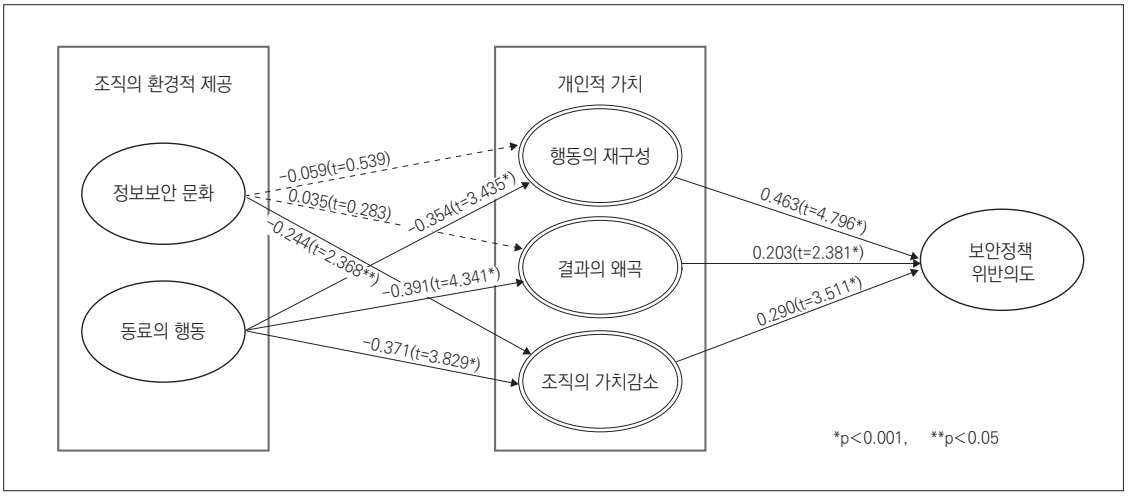
본 연구모형의 독립변수, 매개변수, 종속변수의 관계를 분석하기 위해 구조방정식을 실시하였다. 모형의 신뢰성과 타당성, 모형의 평균 설명력 검증을 전제로 구성개념 간 관계를 추정하였고 사회과학 분야 연구에서 주로 적용되는 0.05 이하의 유의수준을 기준으로 측정하였다. 본 연구에서 제시된 연구모형을 분석한 결과는 〈그림 3〉과 같다.

조직에서 제공하는 환경적 요인인 정보보안 문화는 행동의 재구성과 결과의 왜곡에 통계적으로 유의하지 않은 것으로 나타났다. 이것은 조직에서 정보보안의 중요성을 교육하고 보안 관련 규칙을 수립하고 있음에도 불구하고 개인의 업무 성과나 효율성을 높이기 위해 스스로 보안 위반 행위를 용인 가능한 행동으로 재개념화하는 것으로 볼 수 있다. 또한 보안 문화의 정립으로 보안 관련 의사결정에 대한 책임감이나 소유의식이 생기더라도 주변 환경에 책임을 전가하거나 다른 사람과 책임을 분산시킬 수 있는 상황이라면 개인의 도덕적 자기 통제감이 약화되는 것으로 볼 수 있다. 정보보안 문화와 조직의 가치감소 간 경로계수는 -0.244(t=2.368, p〈0.05)로 부의 영향을 미치는 것을 확인하였다. 조직 내 정보보안 문화가 잘 구축되어 있을수록 개인의 보안 위반 행위를 피해 받는 조직의 문제로 인지하는 경향이 감소하는 것으로 나타났다. 조직 내에서 보안을 관

〈표 10〉 모형의 설명력

변수	R^2	중복성	공통성
정보보안문화	-	-	0.962
동료의 행동	-	-	0.912
행동의 재구성	0.154	0.110	0.717
결과의 왜곡	0.155	0.064	0.568
조직 가치감소	0.307	0.208	0.875
정책위반의도	0.731	0.507	0.953
평균값	0.337	0.222	0.831
모형의 설명력	$\sqrt{0.337 \times 0.831} = 0.482$		

1) 공차값이 0.1보다 작고 VIF가 10보다 크며, 상태지수가 30을 초과하면 다중공선성이 존재
2) R^2 값이 0.26 이상이면 '상', 0.13 이상 0.26 미만이면 '중', 0.02 이상 0.13 미만이면 '하'로 판단(Cohen, 1988)



〈그림 3〉 연구모형 분석결과

찰 할 수 있는 환경으로 작용하는 동료의 행동과 행동의 재구성 간 경로계수는 -0.354(t=3.435, p〈0.001)로 부의 영향을 미치는 것을 확인하였다. 가까운 동료들의 보안 인식이 높거나 보안 준수 행동을 할수록 개인의 부정 행동을 정당화하기 위해 행동을 재구성하여 인지하지 않는 것으로 볼 수 있다. 동료의 행동과 결과의 왜곡 간 경로계수는 - 0.391(t=4.341, p〈0.001)로 부의 영향을 미치는 것을 확인하였다. 동료의 보안 행동에 따라 일종의 사회적 영향을 받음으로써 개인의 보안 위반 행위로 인한 책임을 상급자에게 돌리거나 주변 동료들과 분담하는 것, 또는 결과의 문제를 축소시켜 이해할 가능성이 낮은 것으로 볼 수 있다. 동료의 행동과 조직의 가치감소 간 경로계수는 - 0.371(t=3.829, p〈0.001)로 부의 영향을 미치는 것을 확인하였다. 주변 동료들이 각자의 업무 목표와 더불어 조직의 보안 준수가 업무의 일부라고 내재화함으로써 형성되는 인식들이 다른 개인에게 영향을 줄 수 있다. 타인의 내재화된 인식이 조직 내 저변에 깔려 있을 경우 개인은 자

〈표 11〉 가설 검정 결과

가설	모형의 경로	경로계수	t값	채택여부
H1(-)	보안문화 → 행동의 재구성	-0.059	t=0.539	기각
H2(-)	보안문화 → 결과의 왜곡	0.035	t=0.283	기각
H3(-)	보안문화 → 조직의 가치감소	-0.244	t=2.368**	채택
H4(-)	동료의 행동 → 행동의 재구성	-0.354	t=3.435*	채택
H5(-)	동료의 행동 → 결과의 왜곡	-0.391	t=4.341*	채택
H6(-)	동료의 행동 → 조직의 가치감소	-0.371	t=3.829*	채택
H7(+)	행동의 재구성 → 보안정책 위반 의도	0.463	t=4.796*	채택
H8(+)	결과의 왜곡 → 보안정책 위반 의도	0.203	t=2.381*	채택
H9(+)	조직의 가치감소 → 보안정책 위반 의도	0.290	t=3.511*	채택

신의 위반행위를 조직의 보안 관리 방식이나 직원을 비인격적으로 대하는 태도에서 비롯된 문제라고 돌리지 않을 가능성이 높다.

행동의 재구성과 보안정책 위반 의도 간 경로계수는 0.463(t=4.796, p<0.001)로 정의 영향을 미치는 것을 확인하였다. 결과의 왜곡과 보안정책 위반 의도 간 경로계수는 0.203(t=2.381, p<0.001)로 정의 영향을 미치는 것을 확인하였으며 조직의 가치감소와 보안정책 위반 의도 간 경로계수는 0.290(t=3.511, p<0.001)로 정의 영향을 미치는 것을 확인하였다. 이러한 결과를 바탕으로 개인의 도덕적 이탈 행동을 정당화하고자 하는 개인의 가치가 높을수록 보안정책 위반 의도 가능성이 높은 것을 확인할 수 있다. 본 연구의 가설 검정 결과는 〈표 11〉과 같다.

Ⅴ. 결론

본 연구는 조직이 제공하는 보안 환경과 보안 위반에 대한 개인적 가치의 부적합 결과로 보안정책 위반 의도를 연구하고자 하였다. 본 연구의 분석 결과를 요약해보면 첫째, 정보보안 문화가 행동의 재구성과 결과의 왜곡에 영향을 미치지 않는 것으로 나타났다. 조직에서 구성원이 지켜야 할 보안 관련 규칙이나 표준, 지침을 명확히 수립하고 있고 정보보안에 대한 교육도 이루어지고 있는 조직이라면 조직 구성원들은 조직에서 요구하는 보안 사항이 무엇인지 인지하고 수행할 수 있다. 그러나 조직마다 보유하는 문화적 특성이 다르며 구성원 중 조직 내에 수립된 보안정책에 대한 내용의 인지가 부족한 직원도 다수이다. 이러한 상황을 간과하고 보안 행동에 대한 예방 및 관리 방안을 설명하고 이해시키려 한다면 어려움이 발생할 수 있다(황인호 외, 2016). 그러므로 정보보안 환경이 잘 구축되어 있음에도 불구하고 개인의 업무를 빨리 끝내거나 효율적으로 진행하기 위해 보안정책 위반이 타당하다고 합리화할 수 있다. 그리고 직원이 필요 시 패스워드를 공유하는 것은 그리 나쁜 일이 아니며 실제로 많은 기업에서 흔히 일어나는 일이라고 판단할 수 있다.

조직원 개인이 보안에 대한 책임이나 소유의식을 가지고 있더라도 그 책임을 전가하거나 분산시킬 대상이 있다면 도덕 통제감이 약화되는 것으로 판단된다. 직원이 업무를 수행하는 데 문제가 발생한 경우 조직에서 이를 대처할 다른 방안을 구축하지 못했기 때문이라고 책임을 전가할 수 있다. 본 연구의 분석 결과, 개인이 느끼는 보안에 대한 책임감과는 별개로 집단의 책임 하에 더 무책임하게 행동한다는 Bandura(1999)의 연구 내용과 일치한다고 볼 수 있다.

조직이 보안정책을 수립하고 있고 직원이 보안의 중요성에 대해 인지한다면 조직의 보안정책이 융통성이 없거나 불합리하다는 등 피해 대상의 가치를 감소시키면서 보안 위반 행동을 합리화하지 않는다. 이러한 맥락에서 조직에서 제공하는 정보보안 문화와 보안과 관련된 개인의 가치에서 차이(Gap)가 발생할 경우 부적합(Misfit)의 결과인 보안정책 위반 의도에 영향을 줄 수 있다는 것을 확인하였다.

둘째, 주변에서 가장 간접적이면서도 직접적으로 느낄 수 있는 동료의 보안 행동은 개인의 보안 위반 행동에 대한 행동의 재구성과 결과의 왜곡, 조직의 가치 감소에 유의한 영향을 미치는 것으로 나타났다. 동료가 조직의 보안에 대해 염려하고 보안 절차를 철저히 지키며 성과에 있어서 보안이 중요하다고 판단할수록 개인은 동료의 행동에 사회적 영향을 받는다. 사회적 영향은 본인도 모르게 동료의 관념이나 행동을 판단하고 내재화할 수 있다. 동료의 행동이나 시선이 자신의 행동에 대한 압력으로 행사되어 보안정책 위반 행동을 쉽게 할 수 없다. 그러므로 동료의 보안 행동과 개인의 가치 간 차이가 발생할 때 부적합의 결과인 보안정책 위반 의도에 영향을 줄 수 있다는 것을 확인하였다.

셋째, 행동의 재구성과 결과의 왜곡, 조직의 가치감소가 높을수록 보안정책 위반의도가 높아지는 것을 확인하였다. 본인의 행동이 조직의 규율에 어긋난다는 것을 인지함에도 불구하고 도덕적 이탈을 제공할 환경이 주어진다면 행동에 대한 자기 통제감이 약화된다. 자

기 통제력이 낮은 사람은 충동적이고 우발적으로 행동할 수 있으며(이성식, 2015), 도덕 이탈 행위를 합리화하는 성향이 강해지기 때문에 보안정책 위반 행동을 할 의도가 높아지는 것으로 판단할 수 있다.

패스워드 공유를 비롯하여 패스워드 받아 적기, 데이터 백업하지 않기, 자리를 비운 경우 로그아웃하지 않기 등 악의적이지 않지만 구성원의 무관심 또는 부주의로 인해 보안에 위협을 줄 수 있는 행동들이 흔히 이루어지고 있다. 이러한 문제를 설명하기 위해 도덕 이탈 이론을 적용하여 실무적으로 직원의 행동을 이해할 수 있는 연구를 수행하였다.

본 연구의 한계점으로 첫째, 경영대학원에 재학 중인 직장인을 대상으로 설문을 실시하였으나 보안 인식에 대한 향상된 연구를 위해 다양한 연령층을 대상으로 포괄적인 연구를 수행할 필요가 있다. 둘째, 표본의 크기가 작은 경우 연구하고자 하는 현상의 범위를 포함하기에 불충분할 수 있으므로(Pinsonneault & Kraemer, 1993), 향후 연구에서 더 많은 표본의 크기를 확보한다면 한 층 질 높은 연구가 수행될 것으로 판단된다.

기존의 선행연구에서는 보안 준수 행동과 관련된 연구가 많이 있으나(김보라 외, 2018; 김상현·송영미, 2011; 김상훈·박선영, 2011), 보안 위반 연구는 직원들을 대상으로 연구하기에 직원들이 민감하게 여기는 주제이며 다소 편향이 존재할 수 있으므로 국내에서는 연구가 많지 않다. 도덕 이탈 이론을 적용한 국내 연구는 주로 심리학 분야 또는 아동 및 청소년의 일탈 행동 연구에서 개인의 반사회적 행동을 설명하기 위해 적용되었다(곽금주, 1998; 김지미·김정민, 2013). 정보시스템 분야에서는 조직 내의 보안 위반 행동을 설명하기 위해 연구되었으나(임명성, 2013), 최근 이 이론을 적용한 연구는 확인할 수 없었다.

도덕 이탈 이론이 개인의 합리화 과정을 설명함으로써 비윤리적 행동을 예측할 수 있는 중요한 이론임에도 불구하고 국내에서 많이 다루어지지 않은 이유는 실증적으로 측정하고 분석하기에 어려움이 있기 때문이다. Bandura(1996)의 연구에서 32가지 측정항목을 제시하고 있으나 이 항목만으로 개인의 도덕 이탈 과정을 모두 설명하기에는 항목들이 특정적이고 구체적이다. 이러한 문제로 32가지 측정항목 중 필요한 항목만 선택적으로 적용하거나 일부 카테고리만 측정하는 연구가 많다. 그러나 본 연구에서는 합리화 과정을 행동의 재구성, 결과의 왜곡, 조직의 가치감소로 구성하여 이론에서 제시하는 세 가지 카테고리를 모두 포함하였고 이를 형성지표로 측정함으로써 기존 연구에서 한 가지 구성개념으로 측정되던 도덕 이탈 요인을 세분화하여 분석하였기 때문에 학문적 시사점이 있다고 판단된다. 또한 개인이 추구하는 가치와 환경적 제공의 부적합 결과로 보안위반 행동이 나타나는 것을 실증적으로 연구함으로써 사람-환경 적합 모델을 설명하는 데 학문적 기여를 도모하였고 향후 사람-직무, 사람-조직 등 다양한 특성에 접목하여 연구를 수행하는 데 도움이 될 수 있을 것이라 판단된다.

본 연구의 실무적 기여도는 조직 내에서 흔히 발생하는 패스워드 공유 상황을 기반으로 연구를 수행하였다는 것이다. 패스워드 공유는 시스템 이용자가 비밀번호를 공개적으로 노출하는 것과 같은 이치로 볼 수 있어 이러한 취약점으로 인해 보안 위협이 발생할 수 있다(이경률 외, 2017). 악의적인 의도로 행하는 것이 아니라 업무의 효율성을 높이거나 상황의 융통성을 위해 조직을 보안 위험에 노출 시킬 수 있는데 이것은 직무 윤리의식이 해이해지거나 책임감이 낮아지는 데서 비롯된다. 개인의 사소한 행동이 보안 위험 발생 가능성을 높인다는 인식을 심어주기 위해 기업에서는 지속적인 보안 교육을 제공하는 것이 필요하다.

최근 조직 구성원의 보안 인식 및 행동을 연구하는 데 있어 정보보호 교육의 중요성이 강조되고 있다. 구성원의 보안 위반 행동의 대표적인 교정 조치로 교육의 효과성을 제시하고 있는 바, 현 연구에서 향후 발전된 연구를 위해 보안 위반 의도에서 실제 위반 행동 측정, 보안 교육의 효과를 실험적으로 연구한다면 더욱 심도 있는 연구가 될 것으로 판단된다. 보안 교육과 더불어 내부자가 쉽게 시스템에 접근함으로써 발생하는 취약

점을 보완하기 위해 기업에서 자체적으로 인증 강화 제도를 구축한다면 내부자 위협으로부터 한층 더 강화된 보안 체계를 갖출 수 있다고 예상된다.

■ 참고문헌

곽금주 (1998). "자기효능감과 도덕적 이탈 (I)." 「한국심리학회지: 발달」, 11(1): 1-11.

김계수 (2013). 「Smartpls 이용 쉬운 구조방정식모델」. 청람

김보라·이종원·김범수 (2018). "보안교육 및 보안서비스가 조직구성원의 정보보안정책 준수에 미치는 영향." 「정보화정책」, 25(1): 99-114.

김상현·송영미 (2011). "조직 구성원들의 정보보안 정책 준수 동기요인에 관한 연구." 「e-비즈니스연구」, 12(3): 327-349.

김상훈·박선영 (2011). "정보보안 정책 준수 의도에 대한 영향요인." 「한국전자거래학회지」, 16(4): 33-51.

김지미·김정민 (2013). "부모의 심리적 통제와 아동의 도덕적 이탈이 또래 괴롭힘 참여자 역할행동에 미치는 영향." 「아동학회지」, 34(6): 13-29.

김혜정·안중호 (2013). "정보보호 거버넌스 효율성 제고를 위한 조직원의 정보보호 행위에 관한 실증연구." 「한국전자거래학회지」, 18(1): 147-164.

이경률·이선영·임강빈 (2017). "인터넷 뱅킹 서비스에서의 보안위협 분류 및 분석." 「정보화정책」, 24(2): 20-42.

이성식 (2015). "SNS상의 범죄행위 설명에 있어 사회학습이론과 보완적 논의의 검증." 「정보화정책」, 22(4): 91-104.

이정하·이상용 (2015). "금융회사 정보보안정책의 위반에 영향을 주는 요인 연구: 지각된 고객정보 민감도에 따른 조절효과." 「JITAM」, 22(4): 225-251.

임명성 (2013). "정보보안 상황에서의 도덕적 해방: 선행요인과 결과요인에 대한 연구." 「디지털융복합연구」, 11(11): 1-13.

한국인터넷진흥원 (2018). "KISA Report." RSA Conference 2018 특집편

황인호·김대진·김태하·김진수 (2016). "조직의 정보보안 문화형성이 조직 구성원의 보안지식 및 준수의도에 미치는 영향 연구." 「Information Systems Review」, 18(1): 1-23.

Alnuaimi, O. A., Robert, 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.

Ayyagari, R., Grover, V. & Purvis, R. (2011). "Technostress: Technological Antecedents and Implications." *MIS Quarterly,* 35(4): 831-858.

Bandura, A. (1999). "Moral Disengagement in the Perpetration of Inhumanities." *Personality and Social Psychology Review,* 3(3): 193-209.

Bandura, A., Barbaranelli, C., Caprara, G. V. & Pastorelli, C. (1996). "Mechanisms of Moral Disengagement in the Exercise of Moral Agency." *Journal of Personality and Social Psychology*, 71(2): 364-373.

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 and Security,* 1(3): 18-41.

Chatman, J. A. (1989). "Matching people and organizations: Selection and socialization in public accounting firms." *Academy of Management Proceedings,* 1989(1): 199-203.

Cheng, L., Li, Y., Li, Y., Holm, E. & Zhai, Q.(2013). "Understanding the Violation of IS Security Policy in Organizations: An Integrated Model Based on Social Control and Deterrence Theory." *Computers & Security,* 39(Part B): 447-459.

Chu, A. M. & Chau, P. Y. (2014). "Development and Validation of Instruments of Information Security Deviant Behavior." *Decision Support Systems,* 66: 93-101.

Chu, A. M., Chau, P. Y. & So, M. K. (2015). "Explaining the misuse of information systems resources in the workplace: A dual-process approach." *Journal of Business Ethics,* 131(1): 209-225.

Cohen, J. O. (1988). *Statistical Power analysis for the behavioral science(2nd ed.)*, Hillsdale, New Jersey, Lawrence erlbaum associates.

Cox, J. (2012) "Information systems user security: A structured model of the knowing-doing gap." *Computers in Human Behavior,* 28(5): 1849-1858.

D'arcy, J., Herath, T. & Shoss, M. K. (2014). "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective." *Journal of Management Information Systems,* 31(2): 285-318.

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.

Dang, D., Pittayachawan, S. & Bruno, V. (2015). "Factors of people-centric security climate: Conceptual model and exploratory study in Vietnam." *ACIS 2015 Proceedings.*

Detert, J. R., Treviño, 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.

Edwards, I. R. & Shipp, A. I. (2007). "The relationship between person-environment fit and outcomes: An integrative." *Perspectives on organizational fit,* 1-75.

Edwards, J. R. (1996). "An Examination of Competing Version of the Person-Environment Fit Approach to Stress." *Academy of Management Journal,* 39: 292-339.

Enterprise, Verizon. (2017). *2017 Data Breach Investigations Report.*

Greene, G. & D'Arcy, J. (2010). "Assessing the Impact of Security Culture and the Employee-Organization Relationship on IS Security Compliance." *In 5th Annual Symposium on Information Assurance,* 1-8.

Guo,, K. H. (2013) "Security-related behavior in using information systems in the workplace: A review and synthesis." *Computer & Security,* 32: 242-251.

Guo, K. H., Yuan, Y., Archer, N. P. & Connelly, C. E. (2011). "Understanding Nonmalicious Security Violations in the Workplace: A Composite Behavior Model." *Journal of Management Information Systems,* 28(2): 203-236.

Guo, K. H. & Yuan, Y. (2012). "The Effects of Multilevel Sanctions on Information Security Violoations: A Mediating Model." *Information & Management,* 49(6): 320-326.

Herath, T. & Rao, H. R. (2009). "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness." *Decision Support Systems,* 47(2): 154 - 165.

Hovav, A. & D'Arcy, J. (2012). "Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea." *Information & Management,* 49(2): 99-110.

Hsu, J. S. C., Shih, S. P., Hung, Y. W. & Lowry, P. B. (2015). "The role of extra-role behaviors and social controls in information security policy effectiveness." *Information Systems Research,* 26(2): 282-300.

Kim, H. W., Y. Xu, & J. Koh. (2004). "A comparison of online trust building factors between potential customers and repeat customers." *Journal of the Association for Information Systems,* 5(10): 392-420.

Lee, C., Lee, C. C. & Kim, S. (2016). "Understanding information security stress: Focusing on the type of information security compliance activity." *Computer & Security,* 59: 60-70.

Mishra, S. & Dhillon, G. (2006). "Information systems security governance research: a behavioral perspective." In 1st Annual Symposium on Information Assurance, *Academic Track of 9th Annual NYS Cyber Security Conference.* 27-35.

Moore, C., Detert, J. R., Klebe Treviño, L., Baker, V. L. & Mayer, D. M. (2012). "Why employees do bad things: Moral disengagement and unethical organizational behavior." *Personnel*

Psychology, 65(1): 1-48.

Padayachee, K. (2016). "An assessment of opportunity-reducing techniques in information security: An insider threat perspective." *Decision Support Systems,* 92: 47-56.

Pinsonneault, A. & Kraemer, K. (1993). "Survey research methodology in management information systems: an assessment." *Journal of Management Information Systems,* 10(2): 75-105.

Safa, N. S., Maple, C., Watson, T. & Von Solms, R. (2018). "Motivation and opportunity based model to reduce information security insider threats in organisations." *Journal of Information Security and Applications*, 40: 247-257.

Silverthorne, C. (2004). "The Impact of Organizational Culture and Person-Organization Fit on Organizational Commitment and Job Satisfaction in Taiwan." *Leadership & Organization Development Journal,* 25(7): 592-599.

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

Stanton, J. M., Stam, K. R., Guzman, I. & Caledra, C. (2003). "Examining the linkage between organizational commitment and information security." *Presented at the SMC '03 2003 IEEE International Conference on Systems, Man and Cybernetics, IEEE.* 3: 2501-2506.

Tenenhaus, M., Vinzi, V. E., Chatelin, Y. M. & Lauro, C. (2005). "PLS path modeling." *Computational Statistics & Data Analysis,* 48(1): 159-205.

Vance, A. & Siponen, M. (2012). "IS Security Policy Violations: A Rational Choice Perspective." *Journal of Organizational and End User Computing,* 24(1): 21-41.

Vroom, C. & Solms, von, R. (2004). "Towards information security behavioural compliance." *Computers & Security,* 23(3): 191 - 198.

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.

〈부록 A〉

구성개념		측정 항목
행동의 재구성	도덕적 정당화	업무를 빨리 끝내기 위해 패스워드를 공유할 수 있다고 생각한다.
		업무를 효율적으로 진행하기 위해 패스워드를 공유할 수 있다고 생각한다.
		업무를 서둘러야 할 때 패스워드를 공유할 수 있다고 생각한다.
	완곡한 표현	상황에 따라 필요하면 암호를 공유하는 것이 그리 나쁜 것은 아니라고 생각한다.
		패스워드 공유는 직장에서 실제로 일어날 수 있는 일이라고 생각한다.
		가까운 동료와 패스워드를 공유하는 것은 큰 문제가 아니라고 생각한다.
	경감식 비교	기밀 데이터 유출과 같은 심각한 상황과 비교했을 때, 패스워드 공유는 큰 문제가 아니라고 생각한다.
		기업의 정보 도난과 같은 심각한 상황과 비교했을 때, 패스워드 공유는 큰 문제가 아니라고 생각한다.
		기업의 시스템 해킹과 같은 심각한 상황과 비교했을 때, 패스워드 공유는 큰 문제가 아니라고 생각한다.
결과의 왜곡	책임의 전가	조직에서 직원들의 패스워드 공유를 반대할 경우, 조직은 더 나은 대안을 마련해야 한다.
		조직에서 직원들의 패스워드 공유를 반대할 경우, 조직에서 문제 해결 방안을 모색해야 한다.
		조직에서 직원들의 패스워드 공유를 반대할 경우, 조직은 이를 대체할 방법을 제시해야 한다.
	책임의 분산	다른 많은 직원들이 패스워드를 공유하는 상황에서 한 명의 직원만 제재를 받는 것은 불공평하다고 생각한다.
		조직 내에서 패스워드가 쉽게 공유되는 상황에서 한 명의 직원만 제재를 받는 것은 불공평하다고 생각한다.
		조직 내에서 암묵적으로 패스워드가 흔히 공유되는 상황에서 한 명의 직원만 제재를 받는 것은 불공평하다고 생각한다.
	결과의 왜곡	패스워드를 공유하는 것은 실제로 조직에 큰 해를 끼치지 않는다고 생각한다.
		패스워드가 필요한 직원에게 공유하는 것은 조직에 큰 해를 끼치지 않는다고 생각한다.
		조직에 직접적인 해를 끼치지 않으므로 패스워드를 공유하는 것은 괜찮다고 생각한다.
조직의 가치감소	비인간화	나의 조직은 직원의 행동에 큰 신경을 쓰지 않으므로 패스워드 공유 정도는 괜찮다고 생각한다.
		나의 조직은 직원의 정보보안 위반 행동에 엄격하지 않으므로 패스워드 공유 정도는 괜찮다고 생각한다.
		나의 조직은 직원의 정보보안 준수 행동을 강요하지 않으므로 패스워드 공유 정도는 괜찮다고 생각한다.
	비난의 귀속	패스워드 공유를 금지하는 정책은 융통성이 없으므로 패스워드를 공유하는 것은 괜찮다고 생각한다.
		패스워드 공유를 금지하는 정책은 너무 불합리하므로 패스워드를 공유하는 것은 괜찮다고 생각한다.
		패스워드 공유를 금지하는 정책은 너무 제한적이므로 패스워드를 공유하는 것은 괜찮다고 생각한다.
정보보안문화		나의 조직은 정보보안의 중요성에 대해 교육한다.
		나의 조직은 구성원이 지켜야 할 보안 관련 규칙을 수립하고 있다.
		나의 조직은 정보 자산을 보호하기 위한 표준을 수립하고 있다.
		나의 조직은 적절한 정보보안 행동을 위한 지침을 수립하고 있다.
동료의 행동		조직의 다른 구성원들은 조직의 정보보안에 대해 염려하고 있다.
		조직의 다른 구성원들은 정보보안 절차를 철저히 지킨다.
		조직의 다른 구성원들은 나와 함께 보안 이슈를 논한다.
		조직의 다른 구성원들은 정보보안을 준수하는 행동이 조직의 성과를 평가하는 주요 요인이라고 생각한다.
보안정책 위반의도		나는 필요하다면 패스워드를 공유할 의도가 있다.
		나는 상황에 따라 다른 구성원과 패스워드를 공유할 것이다.
		나는 향후 다른 구성원과 패스워드를 공유할 수 있다고 생각한다.
		나는 다른 구성원과 패스워드를 공유할 의사가 있다.