

정보보안 준수 의도에 대한 사회심리적 요인 분석: 정보보안과 조직시민행동이론 융합

한진영*, 김유정**

중앙대학교 창의ICT공과대학*, 호서대학교 경영학부 디지털기술경영**

Investigating of Psychological Factors Affecting Information Security Compliance Intention: Convergent Approach to Information Security and Organizational Citizenship Behavior

Jin-Young Han*, Yoo-Jung Kim**

College of ICT Engineering, Chung-Ang University*

Dept. of Business Administration, Hoseo University**

요약 융·복합 시대 도래로 인한 옴니 채널 환경에서 기술적 및 관리적 정보보안대책 확충과 더불어 기업구성원의 자발적 참여를 통해 정보보안대책이 효과적으로 실행되는 것이 매우 중요하다. 이러한 맥락에서 기업구성원이 정보보안대책 인식 이후 자발적으로 조직시민행동을 전개하면 정보보안 대책에 대한 준수 의도가 형성될 것으로 본다. 따라서 본 연구에서는 기업의 정보보안대책(정보보안정책, 정보보안 교육훈련)이 조직시민행동을 매개로 정보보안 준수 의도에 미치는 영향을 실증연구를 통해 검증하고자 한다. 이를 위해 문헌연구를 기반으로 설문문항을 작성하였으며 다양한 업종의 기업을 대상으로 설문조사를 실시하였다. 수집된 설문자료를 분석한 결과, 정보보안정책과 정보보안 교육훈련이 정보보안 준수 의도에 영향을 주는 것으로 나타났다. 또한 정보보안정책과 정보보안 교육훈련 모두 조직시민행동(참여 활동)을 매개로 정보보안 준수 의도에 영향을 주는 것으로 나타났다.

주제어 : 정보보안이론과 조직시민행동이론의 융합, 정보보안정책, 정보보안 교육훈련, 정보보안정책 준수 의도

Abstract In digital convergence environment, information security management plays crucial role in maintaining firms' competitiveness. Organizational citizenship behavior(OCB) enables informations security countermeasures to be more effectively worked by helping employees to have much knowledge of information security policy, by facilitating employees to participate in information security education/training. Thus, the purpose of this study is to investigate the mediating effect of OCB on the relationships between information security countermeasures and compliance intention. Questionary was designed based on prior information security research, and survey was conducted among companies' employees across the industry. Results showed that information security policy and information security education/training were found to be key predictors of compliance intention. In addition, OCB was proven to mediate the relationships between information security countermeasures and compliance intention.

Key Words : Convergent approach to information security and organizational citizenship behavior, Information security countermeasures, Intention to comply with information security policy

Received 13 June 2015, Revised 29 July 2015

Accepted 20 August 2015

Corresponding Author: Yoo Jung Kim

(Dept. of Business Administration, Hoseo University)

Email: faith@hoseo.edu

ISSN: 1738-1916

© The Society of Digital Policy & Management. All rights reserved. This is an open-access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (<http://creativecommons.org/licenses/by-nc/3.0>), which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

1. 서론

통신·방송 융합 및 유무선 네트워크 통합이 가속화됨에 따라 기업의 정보보안에 대한 내·외부 위협의 경로 및 방법이 점점 다양화되고 있다. 기업에서는 융·복합 시대 도래로 인한 오픈 채널 환경에서의 기업 정보보안관리가 더욱 중요한 과제로 부각되고 있다. 이로 인해 기업의 정보보안을 위한 기술, 시스템과 인력 확충에 대한 투자가 매년 크게 증가하고 있으며, 기업의 정보보안 관리체계도 보다 고도화 되고 있다[1].

기업에서 정보보안 정책과 정보보안 교육훈련과 같은 절차적 보안대책이 도입되는 등 정보보안 시스템 확충과 관리체계가 구축되어 정보보안에 대한 기술적 위협의 예방과 대처 능력이 강화되었음에도 불구하고[2], 많은 기업에서 정보보안 사고가 지속적으로 발생하고 있다. 특히 정보보안 대책 준수에 대한 인식이 부족하거나 약의적인 의도를 지닌 기업 구성원(정보시스템 관리자, 일반 관리자 등)에 의해 발생하는 정보보안 침해사고가 점점 증가하고 있다[1]. 이는 기업이 정보보안 시스템 확충(기술적 능력)과 정보보안 관리체계 도입(관리 능력) 만으로 기업의 정보보안 능력을 강화하는데 한계가 있음을 의미한다.

따라서 정보보안 관리 시스템과 관리정책을 기업구성원이 제대로 인지하고 기업의 정보보안 정책을 제대로 준수하는데 필요한 기업의 내·외부 요인을 통합적으로 규명하는 것이 매우 중요하다[3, 4]. 이런 추세를 반영한 듯, 최근 조직원들의 정보보안대책 준수 의도에 영향을 미치는 요인에 대한 연구들이 활발히 진행되고 있다[3, 5, 6, 7, 8, 9]. 특히, 김상현과 김근아[3]은 기업의 정보보안에 대한 의식수준 향상이 정보보안 대책 준수 의도에 영향을 주어 침해사고를 예방하는데 중요한 역할을 할 수 있다고 제시하였다. 정보보안에 대한 의식수준은 정보보안 교육훈련, 정보윤리실천[10] 등을 통해 향상시킬 수 있다. 조직원들의 조직에 대한 결속을 강화함으로써 조직원들의 정보보안 준수를 향상시킬 수 있다는 연구도 있다[11]. 더 큰 맥락에서 볼 때, 조직시민행동(Organizational Citizenship Behavior, OCB)이 기업구성원의 정보보안 의식 수준을 높여 정보보안 대책에 대한 이해와 이를 준수하고자 하는 의도를 강화 할 수 있다고 본다.

조직시민행동은 조직구성원들의 상호작용, 조직지원 및 신뢰에 기초한 창의적이고 능동적이고 자발적인 공식 업무이외의 활동 및 행동을 의미한다[12]. 조직시민행동은 이타주의, 양심, 참여 활동, 스포츠맨십 및 예의 차원으로 구성된다[13].

이러한 조직시민행동은 조직원의 마찰을 줄이고, 유연성을 제고하며, 좋은 조직 문화 및 심리적 배경을 형성하고, 조직의 효율성과 효과성을 향상시킨다[14]. 실제로 조직시민행동 수준이 높은 정보시스템 업무 담당자(IS personnel)는 직무 생산성과 변화하는 환경에 대한 적응 능력이 높다[14]. 또한 조직구성원의 양심(consciousness)과 친화성(agreeableness)에 따라 정보보안 소프트웨어 수용의도가 수용행위로 연결되는 정도가 차이가 나므로 밝혀졌다[15]. 이러한 내용을 종합해 볼 때, 조직시민행동은 기업 구성원이 정보보안 대책을 인식한 후 정보보안 준수 의도를 갖는데 중요한 매개역할을 할 수 있다 본다. 특히, 조직시민행동 중 참여활동(civic virtue)은 조직 구성원이 조직관리(governance)에 건설적이고 책임감 있게 참여하는 것으로[14], 기업구성원이 정보보안 대책을 적극적으로 책임감 있게 수행하고 준수하고자 하는 의도를 갖게 하는 매개 역할을 할 것으로 본다. 그러나 이전 연구에서는 조직시민행동이 정보보안대책과 정보보안 준수 의도 간의 관계를 매개하는 역할을 간과해왔다. 따라서 본 연구에서는 정보보안 대책이 조직시민행동을 매개로 정보보안 준수 의도에 미치는 영향을 실증적 연구를 통해 검증하고자 한다.

2. 이론적 배경

2.1 정보보안 준수

정보보안 관련 선행연구는 주로 침입탐지나 방화벽과 같은 기술적인 연구들이 주를 이루었으며[16] 조직 내에서 구성원들의 행동이 정보보안에 미치는 영향에 대한 연구들은 미흡하다고 할 수 있다. 정보보안 관련 학계, 산업계 전문가들로 구성된 워킹그룹인 International Federation for Information Processing (IFIP) Working Group 8.11/11.13 on Information Systems Security Research 에서 조직행동관점으로 향후 정보보안 연구가 진행될 필요가 있다는데 의견을 모았다[16]. 특히, 조직원

들의 정보보안정책 준수에 영향을 미치는 요인에 대한 연구가 확대되어야 한다는 의견을 제시하였다. 이런 추세를 반영한 듯, 최근 조직원들의 정보보안정책준수 의도에 영향을 미치는 요인에 대한 연구들이 활발히 진행되고 있다[5, 17, 18, 19].

조직원들이 정보보안정책을 준수할 수 있도록 하기 위해서 조직은 정보보안 사고를 방지하거나 해결하기 위한 대책을 수립해야 한다. 보안대책은 절차적 대책과 기술적 대책을 구분되며 절차적 보안대책으로는 보안정책 수립, 정보보안인식 교육프로그램 등이 있고 기술적 보안대책으로는 컴퓨터 모니터링이나 안티바이러스 소프트웨어 등이 있다[20]. Hovav와 D'Arcy[20]은 절차적 보안 대책과 기술적 보안대책을 통합하여 마련되어야 한다고 권고한다. 그러나 기술적 보안대책은 실제 업무환경에서 영향을 적게 미치는 것으로 나타나서 업무환경에서 보안대책으로서의 효과가 적다고 볼 수 있다. 본 연구에서도 절차적 보안대책에 초점을 두어 조직원들의 정보보안준수 의도에 긍정적인 영향을 미치는 요인을 연구하고자 한다.

Anderson과 Agawal[21]의 정보보안준수 의도 및 준수 행위에 대한 리뷰연구에서 제시한대로, 이 분야 선행연구에서는 주로 일반억제이론, 합리적 선택이론, 중성화이론 등과 같이 범죄학에 기반을 둔 관점이나 보호동기이론 관점에서 연구가 진행되어 왔다[21]. 조직행동, 사회심리학 등 다른 관점에 기반을 두어서 정보보안준수에 영향을 미치는 요인들을 살펴보는 것은 정보보안준수와 관련한 연구 분야를 확장하고 업무환경에서의 정보자원의 오남용을 막을 수도 있을 것이다[17]. <Table 1>는 절차적 보안대책과 정보보안 준수 의도 사이에 조직행동 및 사회심리학에 기반을 둔 요인들을 조절 혹은 매개변수로 두고 이들이 어떤 영향을 미치는지를 살펴본 연구들이다.

이들 연구들은 합리적 선택이론에 근거해 정보보안 준수 결과에 따르는 손익을 평가하고 그 결과에 따라 조직원의 준수태도 및 준수 의도가 결정되는 것을 보였다 [8, 22]. 또한 일반억제이론에 근거하여 적발가능성이 보안대책과 보안준수 의도 사이에서 매개역할을 한다는 연구결과가 있다[8]. 이들 선행연구에서 절차적 보안대책과 정보보안준수 의도 사이에 조직행동관점의 요인으로 긍정성을 도입한 연구가 있긴 하나[5, 18] 아직 미흡하다고 할 수 있다.

<Table 1> Prior Literatures related to procedural information security policy compliance

Independent variable [references]	Moderator / Mediator	Methodology	Research results
Information Security policy awareness [5]	Attitude toward security compliance Procedural justice	Survey Employees (464)	Information security policy awareness → Attitude(+), Justice(+) Attitude, Justice → Security policy Compliance intention (+)
Penalty Ethics education [6]	Organizational type	Survey Employees (492)	Penalty → Compliance (+) Ethics education → Compliance (+)
Security awareness education/training Individual attachment [8]	Detection certainty Social norms Response cost	Survey Employees of SI industry (143)	Security awareness education/ training → Detection certainty(+) Detection certainty → Social norms(-) Detection Certainty → Compliance intention(+) Response cost → Compliance intention(-) Attachment → Compliance intention(+)
Security policy effectiveness Security awareness program Top management attention Security enforcement [19]	Response cost	Survey Employees of Banking industry (118)	Security policy effectiveness → Compliance intention(+) Security awareness program → Response cost(-) Top management attention → Compliance intention(+) Security enforcement → Compliance intention(-) Security enforcement → Response cost(+)
Personal moral belief Direct & Indirect experience Task relatedness Security awareness education/training	Organizational justice (distribution/procedural/interactional)	Survey Employees (437)	Personal moral belief → Compliance intention(+) Security awareness education/training → Compliance intention(NS) Direct & Indirect experience → Compliance intention(+) Certainty of sanction → Compliance intention(+)

Perceived certainty of sanctions [18]			
---------------------------------------	--	--	--

NS: Non-significant

2.2 조직시민행동

(Organizational Citizenship Behavior: OCB)

조직시민행동은 조직의 구성원의 자발적 조직행동으로서, 공식적으로 또는 직접적으로 성과가 인정되지 않고 보상도 이뤄지지 않지만 전체 조직의 효과적 운영을 촉진하는 역할을 하는 것으로 알려져 있다[22, 23]. 조직시민행동에 대한 개념은 다양하게 정의되어 왔는데, 명시적으로 정의된 조직에서의 역할 외의 행동(extra-role behavior)이라는 의미로 정의하기도 한다[13, 24]. 조직시민행동은 조직의 성과에 긍정적인 영향을 미치는 것으로 나타나는데, 조직원들의 자발적인 참여가 조직운영을 개선하고 조직의 관리비용을 줄일 수 있는 것으로 나타났다[25, 26]. 조직시민행동은 다차원의 요소로 구성된 개념으로 알려져 있다. 가장 일반적인 분류로는 이타주의(altruism), 예의(courtesy), 스포츠맨십(sportsmanship), 양심(conscientiousness), 그리고 참여 활동(civic virtue)이 있다[12, 13]. 본 연구에서는 절차적 보안대책과 보안 준수이도 사이에 조직시민행동이 매개역할을 하는지 살펴보았다. 특히 조직시민행동의 하위차원 중에서 정책 준수와 관련된 요인으로 참여활동을 선택하여 연구를 진행하였다. 조직시민행동은 조직의 성과에 영향을 미치며 고객만족[27], 영업설적[28, 29], 직원들의 협업[30]에 긍정적인 영향을 미치는 것으로 나타났다. 또한 조직이나 팀에서 조직시민행동을 매개요인으로 두고, 지식공유의도[31], 정보시스템성공[32, 33] 등을 살펴본 연구들이 있다.

3. 연구가설 및 모형

조직은 정책을 수립함으로써 조직 구성원에게 어떤 행위가 조직에서 수용되는지를 명시적으로 제시하고 구성원들의 의사결정이나 행위에 영향을 미친다[34]. 조직이 수립한 보안정책은 조직 구성원들의 정보보안 행위나 의도에 영향을 미칠 것이며, 이에 대한 다수의 연구가 존재하나 연구결과는 일치하지는 않는다. 예를 들어,

Bulgurcu et al.[5]의 연구에서 조직원들이 보안정책을 인식하면 정보보안준수이도도 높아진다는 연구결과를 보여 주었고, 내용이나 형식에 기반을 둔 보안정책의 효과성은 보안정책 준수이도에 긍정적인 영향을 미치는 것으로 나타났다[19]. 반면에 보안정책은 조직원에 대한 경영진의 감시수단으로 인식하고 업무의 생산성을 저해하는 요인으로 인식하는 경우도 있다[35]. 또한 한국 기업과 미국 기업의 조직원을 대상으로 한 비교연구에서 미국 그룹에서는 보안정책 인식이 보안준수이도에 긍정적인 영향을 미치는 것으로 나타났으나 한국 그룹에서는 유의한 결과를 얻지 못했다[36]. 본 연구에서는 한국기업의 조직구성원을 대상으로 하여 조직의 정보보안정책에 대해 직원들이 인지하면 보안정책 준수이도에 긍정적인 영향을 미칠 것이라는 가설을 다음과 같이 수립한다.

H1 정보보안 정책은 정보보안 준수이도에 정(+)의 영향을 미친다.

정보보안 교육훈련은 조직의 정보자원에 대한 적절한 사용에 대한 교육과 훈련을 의미하며, 조직구성원들의 정보보안에 대한 인식전환을 통해 장기적인 정보보안 효과를 가져 온다[37]. 또한 정보보안 교육프로그램은 조직의 정보자원에 대한 오·남용에 대한 억제수단 중의 하나로 사용되어 왔다. 일반억제이론에 의하면, 조직은 보안 교육과 훈련 프로그램을 통해 보안인식을 높일 수 있고, 이를 통해서 내부직원들의 정보보안사고를 감소시킬 수 있다[37, 38]. 따라서 정보보안 관련 교육이나 훈련은 조직구성원의 정보보안 준수이도에 긍정적인 영향을 미칠 것이며 이에 대한 가설을 다음과 같이 수립한다.

H2 정보보안 교육훈련은 정보보안 준수이도에 정(+)의 영향을 미친다.

정보보안정책과 정보보안 교육훈련이 조직구성원들의 정보보안준수이도에 미치는 직접적인 영향에 대한 연구 결과는 일관되지 않는다. 보안정책에 관한 연구에서는 국가별 비교연구에서는 미국기업 그룹에서는 유의한 결과를 얻었으나 한국기업 그룹에서는 유의한 결과를 얻지 못했다[36]. 정보보안정책이 수립되어 있는 것을 조직원이 인지하는 것만으로는 충분하지 않을 수 있으며, 정보보안정책이 효과적으로 수립되어야 정보보안준수이도에 긍정적인 영향을 준다는 연구결과도 있다[19]. 보안교

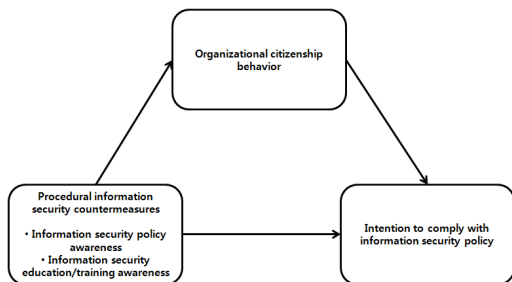
육 및 훈련의 경우에서도 조직원의 정보보안준수도도에 긍정적으로 영향을 미치는 경우와[6, 39] 유의한 결과를 얻지 못한 연구가 존재한다[18]. 이는 조직원들이 절차적 보안대책을 인지하는 것만으로 정보보안준수도도를 향상시키기에 충분하지 않을 수 있다는 증거로 볼 수 있다.

조직시민행동, 특히 참여활동은 역할 외 활동을 통해 조직의 목표달성, 효율적인 업무수행에 긍정적인 영향을 미친다고 알려져 있다[13]. 또한 조직원의 조직시민활동은 구성원의 만족도를 높이고 직원들의 협업이나 지식공유도를 높이는 것으로 나타났다[30, 31]. 이러한 성향, 즉 조직 내에서 공식적으로 정의된 역할 외에 자발적이고 능동적으로 참여하는 성향은 조직에 수립된 정보보안 정책준수에 긍정적인 역할을 하게 될 것이다. 이를 기반으로 조직원의 조직시민행동은 절차적 보안대책과 정보보안 준수도도 사이에서 매개역할을 할 것으로 다음과 같은 가설을 수립하였다.

H3 정보보안 정책과 정보보안 준수도도 관계에서 조직시민행동은 정(+)¹의 매개역할을 한다.

H4 정보보안 교육훈련과 정보보안 준수도도 관계에서 조직시민행동은 정(+)¹의 매개역할을 한다.

다음 [Fig. 1]은 상기 가설들을 그림으로 나타낸 것으로, 절차적 보안대책을 정보보안 준수도도의 직접 선행요인으로 두었다. 또한 이들 관계에서 조직원의 조직시민행동이 부분매개를 할 것을 표현한 것이다.



[Fig. 1] Research Model

4. 연구방법

4.1 연구대상 및 측정방법

본 연구의 가설검증을 위해서 100명 이상 조직원을 보

유하고 있는 기업의 직원을 대상으로 설문조사를 실시하였다. 본 연구 모형에서 제안하는 잠재변수들의 측정을 위한 항목들은 기존의 연구를 바탕으로 추출하여 1차적으로 연구의 목적과 내용에 맞게 수정 및 보완하였다. 관측변수의 내용타당성(content validity) 검증을 위해서 경영관리 및 경영정보시스템 연구자들의 검토를 거쳤다. <Table 2>는 연구모형에서 제안하는 각 변수의 조작적 정의, 측정항목, 관련연구를 보여주고 있다. 연구모형의 잠재변수를 측정하기 위한 설문항목은 7점 리커트 척도(Likert scale)로 측정하였다.

<Table 2> Research variables definition

Construct [references]	Conceptual definition
Information Security Policy Awareness(SP) [37]	Awareness of "guiding statements of goals to be achieved with regard to information security"
Information Security Education Training Awareness Program(SETA) [37]	Awareness of general knowledge of the information security environment, along with the skills necessary to perform any required security procedures
Organizational Citizenship Behavior(OCB) [12, 14]	Individual behavior that is discretionary, not directly or explicitly recognized by the formal reward system, and that in the aggregate promotes the effective functioning of the organization
Intention to Comply with Information Security Policy (CI) [40]	Employees' continuous efforts and intention to compliance with information security policy

* () Acronym of constructs

데이터 수집은 설문을 웹페이지로 제작하여 온라인으로 응답할 수 있도록 하였다. 설문은 357부가 회수되었으며 이 중 미완성 설문 등 유효하지 않은 설문을 제거하고 연구에서는 324부를 사용하였다. 본 연구의 자료 분석에 사용된 설문응답자의 인구통계 특성 및 참여 프로젝트 팀의 특성은 <Table 3>, <Table 4>와 같다.

<Table 3> Demographics of Samples

		Frequency	Percentage (%)
Gender	Male	160	49.4
	Female	164	50.6
Age	20-29	85	26.2
	30-39	87	26.9
	40-49	87	26.9
	50-59	65	20.1
Total		324	100

<Table 4> Characteristics of Respondents' Organization

		Frequency	Percentage (%)
No. of employees	100~149	42	13.0
	150~299	71	21.9
	300~449	49	15.1
	500~999	44	13.6
	1,000~4,999	62	19.1
	5,000 and over	56	17.3
Industry	Manufacturing	114	35.2
	Utility	3	0.9
	Construction	21	6.5
	Wholesaler and retailer	19	5.9
	Telecommunication	13	4.0
	Financial services	31	9.6
	Business services	37	11.4
	Public administration and Defense	17	5.2
	Education service	34	10.5
	Health and Social Welfare	14	4.3
	Entertainment, culture, and athletics services	6	1.9
	Other	15	4.6
	Total	324	100

5. 연구결과

5.1 측정모형 검증

측정모형 검증은 구조방정식 접근방법인 부분최소자승(Partial least Square: PLS) 방식을 사용하였으며, 주요 분석 도구로는 SmartPLS 2.0 M3을 사용하였다. PLS의 경우 컴포넌트를 기반으로 한 접근 방식에 의해 추정하기 때문에 표본의 크기와 잔차분포에 대해 다른 구조방정식 접근방법보다 엄격하지 않아 표본수가 적은 경우 유용하다고 할 수 있다. 또한 PLS는 추정모형에 대한 평가와 구조모형에 대한 평가를 동시에 할 수 있는 기법으로, 본 연구에서 측정항목과 구조모형 검증을 실시하기 위해 PLS를 분석도구로 채택하였다[41]. 측정모형의 수렴타당성(Convergent validity), 구성신뢰성(Composit Reliability), 판별타당성(Discriminant validity)을 검증하였다. 수렴타당성은 구성신뢰도와 평균분산추출(Average Variance Extracted: AVE)에 의해 평가하며 <Table 5>에서 보는 바와 같이 모든 잠재변수의 AVE의 값이 임계치인 0.5를 충족한다[42]. 구성신뢰성 역시 임계치인 0.7보다 큰 것으로 나타나 측정변수들이 수렴 타당성을 가지고 있음을 보여준다[42]. 내적일관성을 평가하는 지표로 Cronbach's α 는 0.7 이상으로 기준을 충족하는 것으로 나타났다[42].

<Table 5> Reliability and Validity of Variables

Construct	Mean	Std.	AVE	CR	CA
CI	5.363	1.102	0.876	0.966	0.953
SP	5.362	1.275	0.638	0.898	0.857
SETA	4.978	1.317	0.714	0.926	0.899
OCB	5.177	1.086	0.635	0.897	0.855

* AVE: Average Variance Extracted CR: Composite Reliability, CA: Cronbach's Alpha

마지막으로 판별타당성은 AVE의 제곱근 값과 잠재변수들 간의 상관관계 분석 방법을 통해 판단하였다[42]. 연구모형에 포함된 각 잠재변수의 AVE 제곱근 값이 해당 잠재변수와 다른 잠재변수 간의 종과 횡의 상관계수 값보다 높게 나타나면 판별타당성이 존재하는 것으로 판단한다. <Table 6>에서 보는 바와 같이 모든 잠재변수에 대한 AVE의 제곱근 값이 인접하고 있는 종과 횡의 변수들 간의 상관관계보다 높게 나타났다. 또한, 모든 잠재변수를 측정하는 측정항목의 요인 값이 타 변수의 측정항목 요인 값 보다 크다는 것을 알 수 있어 판별타당성을 확보하였다.

<Table 6> Discriminant Validity of Latent Variables

Construct	CI	SP	SETA	OCB
CI	0.936			
SP	0.505	0.799		
SETA	0.446	0.659	0.845	
OCB	0.554	0.427	0.053	0.797

* 진하게 표시된 대각선 값은 AVE의 제곱근 값

<Table 7> Cross Loadings of Latent Variables

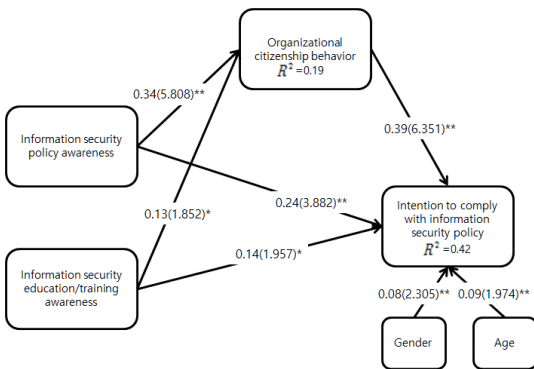
	CI	SP	SETA	OCB
CI1	0.904	0.434	0.414	0.504
CI2	0.945	0.483	0.431	0.519
CI3	0.947	0.489	0.414	0.537
CI4	0.946	0.483	0.409	0.514
SP1	0.316	0.681	0.523	0.281
SP2	0.349	0.807	0.628	0.354
SP3	0.415	0.826	0.440	0.364
SP4	0.466	0.844	0.503	0.397
SP5	0.448	0.823	0.563	0.299
SETA1	0.371	0.540	0.794	0.263
SETA2	0.343	0.522	0.821	0.225
SETA3	0.328	0.495	0.827	0.317
SETA4	0.421	0.602	0.886	0.336
SETA5	0.409	0.610	0.892	0.334
OCB1	0.474	0.372	0.279	0.852
OCB2	0.485	0.399	0.346	0.859
OCB3	0.351	0.293	0.270	0.721
OCB4	0.446	0.317	0.238	0.808
OCB5	0.439	0.309	0.266	0.735

5.2 구조모형 검증 결과

5.2.1 경로분석

본 연구에서 제안한 4개 가설에 대한 검증은 각 개념 간의 경로계수를 부분최소제곱(partial least squares: PLS)에 의해 구하고, PLS의 부트스트랩 리샘플링 방법에 의해 각 경로계수의 t-값을 구해 각 가설에 대한 통계적 지지여부를 검증하였다[Fig. 2]. 본 연구에서 제안한 가설에 대한 검증은 각 개념 간의 경로계수를 PLS에 의해 구하고, PLS의 부트스트랩 리샘플링 방법에 의해 각 경로계수의 t-값을 구해 각 가설에 대한 통계적 지지여부를 검증하였다.

PLS 모형의 적합성에 대한 평가는 R²를 통해 예측타당성을 검토할 수 있으며, 매개요인인 조직시민행동과 보안준수의도의 R²는 각각 0.19, 0.42로 예측타당성이 확보되었다고 할 수 있다. 구조모형의 적합도(Global of Fit, GoF)는 0.1 이하는 낮은 수준, 0.25이하는 중간수준, 0.36 이상은 높은 수준으로 평가할 수 있다[43]. 본 연구의 분석결과 GoF값은 0.61로, 상위 기준(0.36)을 상회하여 본 연구의 구조모형이 적합하다고 판단할 수 있다.



() 안은 t-값

*** : p < 0.01, ** : p < 0.05, * : p < 0.1

[Fig. 2] Resulting Structural Model

정보보안 정책 및 정보보안 교육훈련의 종속변수(정보보안 준수 의도)에 대한 경로계수와 매개변수(조직시민 행동)에 대한 경로계수, 그리고 보안정책준수의도에 대한 조직원의 조직시민행동의 경로계수를 나타내면 <Table 8>과 같다.

<Table 8> Path coefficients

Path	Path coefficients	t-값	p-값	Results
SP → CI	0.24	3.882	<0.01	Support
SETA → CI	0.14	1.957	<0.1	Support
SP → OCB	0.34	5.808	<0.01	Support
SETA → OCB	0.13	1.852	<0.1	Support
OCB → CI	0.39	6.351	<0.01	Support

정보보안 정책은 조직원의 정보보안 준수 의도에 긍정적인 영향으로 미치는 것으로 나타나서($\beta = 0.24, p < 0.01$) 가설H1은 채택되었다. 정보보안 교육훈련도 조직원의 정보보안 준수 의도에 긍정적인 영향을 미치므로($\beta = 0.14, p < 0.1$) 가설H2를 채택할 수 있다.

5.2.2 매개효과분석

매개효과가 통계적으로 유의한가를 확인하기 위해 소벨 테스트(Sobel test)와 이를 보완하기 위해 아로이안 테스트(Aroian test)를 이용하여 분석하였다. Sobel[44]는 독립변수와 종속변수 사이에서 매개변수의 효과를 분석하기 위한 Sobel's Z-Score를 계산할 수 있는 방정식을 제시하였다. 일반적으로 소벨 테스트와 아로이안 테스트의 Z값은 1.96보다 크거나 -1.96보다 작으면 영가설이 기각되므로 매개효과는 통계적 유의성을 갖는 것으로 판단된다[45]. 매개변수와 종속변수의 관계가 독립변수와 매개변수간의 관계보다 클 때 매개효과의 검증력이 커질 수 있기 때문에 매개변수를 선택할 때 독립변수와 종속변수 모두에 대해 동일한 크기를 갖는 매개변수를 선택하거나 독립변수보다 종속변수와의 관계가 더 큰 매개변수를 선택하는 것이 검증력을 높일 수 있다[44]. 소벨 테스트와 아로이안 테스트 결과는 <Table 9>와 같다.

<Table 9> Analysis results of mediating effect of OCB using Sobel test

Path	Standard error	Sobel-Z Score	Aroian-Z Score	Results
SP → OCB	0.06	4.27***	4.24***	Support
OCB → CI	0.06	(0.000)	(0.000)	
SETA → OCB	0.07	1.79**	1.76**	Support
OCB → CI	0.06	(0.03)	(0.03)	

*** : p < 0.01, ** : p < 0.05, () 안은 p-값

Sobel's Z-value = $a*b/\sqrt{b^2*sa^2+a^2*sb^2}$

a : 독립변수와 매개변수간의 비표준화 경로계수

sa : a의 표준오차

b : 매개변수와 종속변수간의 비표준화 경로계수

sb : b의 표준오차

위의 표에서 보는 바와 같이 조직원의 조직시민행동은 정보보안 정책 및 정보보안 교육훈련과 정보보안 준수이도 사이에서 매개효과를 가지는 것으로 나타나고 있다. 먼저, 정보보안 정책과 정보보안 준수이도 관계에서 조직원의 조직시민행동은 매개효과가 있는 것으로 나타났다(Sobel-Z Score = 4.27, $p < .01$; Aroian-Z Score = 4.24, $p < .01$). 따라서 조직시민행동은 두 변수의 중간에서 매개효과가 있어 가설 H3은 채택된다. 둘째로 정보보안 교육훈련과 정보보안 준수이도 관계에서 조직원의 조직시민행동은 매개효과가 있는 것으로 나타났다(Sobel-Z Score = 1.79, $p < .05$; Aroian-Z Score = 1.76, $p < .05$). 따라서 조직시민행동은 두 변수의 중간에서 매개효과가 있어 가설 H4는 채택된다. 조직시민행동은 절차적 보안대책과 정보보안 준수이도 사이에서 부분적 매개역할을 한다고 할 수 있다.

(Table 10) Summary of hypotheses test results

Hypotheses	Path	Results
H1	Information security policy awareness influences positively on security policy compliance intention.	Support
H2	Awareness of information security education/training influences positively security compliance intention.	Support
H3	Organizational citizenship behavior mediates the relationships between information security policy awareness and compliance intention	Support
H4	Organizational citizenship behavior mediates the relationships between information security education/training awareness and compliance intention	Support

6. 결론 및 시사점

본 연구는 절차적 정보보안대책(정보보안정책, 정보보안 교육훈련)이 조직시민행동의 하위차원 중의 하나인 참여 활동(civic virtue)을 매개로 정보보안 준수이도에 영향을 주는 것을 검증하였으며 연구결과는 다음과 같다.

첫째, 기업구성원이 정보보안정책을 인식하고 있을 경우 정보보안을 준수하고자 하는 의도를 갖게 된다는 연구결과가 제시되었다. 이는 기업구성원이 정보보안정책을 인식하게 될 경우 정보보안의 중요성과 준수해야 할 정보보안 활동에 대한 이해가 증진되어 정보보안 준수의

도를 갖게 된다는 것을 의미한다.

둘째, 기업구성원이 자신이 참여할 수 있는 정보보안 교육훈련에 대한 인식과 이해가 제대로 이루어지면, 교육훈련을 통해 개인의 정보보안 능력을 강화할 수 있다는 것을 인식하게 될 것이고, 이로 인해 정보보안 준수이도가 강화될 것이다.

셋째, 기업구성원이 정보보안정책을 인식하게 되면 구성원의 참여 활동(civic virtue)이 활발해지면서 정보보안 준수이도가 강화되는 것으로 나타났다. 이는 기업구성원이 자신의 기업의 정보보안정책을 인식한 후 업무적/공식적인 정보보안정책 준수 활동뿐만 아니라 업무외적으로도 정보보안정책을 준수하기 위해 책임감을 가지고 자발적인 정보보안정책 준수 활동에 참여하게 되기 때문인 것으로 해석된다.

넷째, 정보보안 교육훈련이 조직시민행동(참여 활동)을 매개로 하여 정보보안 준수에 영향을 주는 것으로 나타났다. 이는 기업구성원이 정보보안 교육훈련을 인식하게 될 경우 자발적으로 책임감을 가지고 의무적 정보보안 교육훈련에 참여 할뿐만 아니라 업무외적 또는 비의무적인 정보보안 교육훈련 활동에도 참여 하게 될 것이며, 이러한 참여 활동이 정보보안 준수이도를 형성하는데 기여하는 것으로 해석된다.

본 연구결과의 시사점은 다음과 같다. 본 연구의 학문적 시사점은 절차적 정보보안대책을 기업구성원이 인식한 이후 실제 정보보안 준수이도를 갖게 하는데 조직시민행동(참여 활동)이 중요한 매개 역할을 한다는 이론을 정립한 것이다. 본 연구결과는 기업에서 정보보안관리가 실효성을 거두기 위해서 절차적 정보보안대책 수립 및 기업구성원의 정보보안대책 인식이후 보다 자발적이고 적극적으로 정보보안정책을 이해하고, 교육훈련에 참여하려는 조직시민행동이 전개되면서 정보보안 준수이도가 형성되는 과정을 체계적으로 설명할 수 있는 이론을 제시하였다.

본 연구의 실무적 시사점은 기업에서 절차적 정보보안대책을 수립하여 정보보안 관리를 효과적으로 실행하기 위해서 기업구성원의 조직시민행동이 중요하다는 것을 인지하여야 한다는 것이며, 나아가, 조직시민행동이 활발하게 전개될 수 있는 기업문화를 조성하는 것이 중요하다는 것을 제시한 것이다.

본 연구의 한계점은 절차적 정보보안대책과 정보보안

준수의도간의 관계에서 조직시민행동의 매개효과를 검증하는데 있어 참여 활동(civic virtue) 차원만을 이용한 것이다. 향후 연구에서는 조직시민행동의 다른 네 개 차원인 이타주의, 스포츠맨십, 예의, 양심을 동시에 고려하여 절차적 정보보안대책과 정보보안 준수이도간의 관계에서의 조직시민행동의 매개효과를 검증할 필요가 있다. 또한 정보보안 준수이도의 다른 선행 변수들과 조직시민 행동 간의 관계도 다차원적인 관점에서 연구할 필요가 있다고 본다.

REFERENCES

- [1] H. B. Kim, D. S. Lee, & S. Ham, Impact of hotel information security on system reliability, *International Journal of Hospitality Management*, Vol. 35, pp. 369 - 379, 2013.
- [2] Y. H. Kim, An Implementation of Audit System Applying Forensic Analysis Technology Over Network Node, *Journal of Society for e-Business Studies*, Vol. 4, No. 1, pp. 169-181, 2009.
- [3] S. H. Kim & G. N. Kim, Firm's Environmental Determinants Impacting the Information Security Management and the Moderating Effects of Regulatory Influence, *Journal of the Korean Operations Research and Management Science Society*, Vol. 37, No. 3, pp. 79-94, 2012.
- [4] J. M. Do & J. Kim, A Study on Critical Success Factors for Enterprise Security Collaboration, *Journal of Digital Convergence*, Vol. 12, No. 10, pp. 235-242, 2014.
- [5] B. Bulgurcu, H. Cavusoglu, & I. Benbasat, Roles of Information Security Awareness and Perceived Fairness in Information Security Policy Compliance. *AMCIS 2009 Proceedings*, 419, 2009.
- [6] J. H. Ahn, J. H. Park, G. M. Sung, & J. H. Lee, Impacts of Punishment and Ethics Training on Information Security Compliance: Focus on the Moderating Role of Organizational Type. *Information Systems Review*, Vol. 12, pp. 23-42, 2010.
- [7] S. H. Kim & S. Y. Park, Influencing Factors for Compliance Intention of Information Security Policy, *Journal of Society for e-Business Studies*, Vol. 16, No. 4, pp. 34-51, 2011.
- [8] M. S. Yim, A Path Way to Increase the Intention to Comply with Information Security Policy of Employees, *Journal of Digital Convergence*, Vol. 10, No. 10, pp. 119-128, 2012.
- [9] M. S. Yim & K. H. Han, An Investigation of the Factors that Influence the Compliance to Information Security Policy : From Risk Compensation Theory, *Journal of Digital Convergence*, Vol. 11, No. 10, pp. 153-168, 2013.
- [10] M. J. Baek & S. H. Sohn, A Study on the Effect of Information Ethics on the Information Security Awareness and Behavior in Organization, *Koreanische Zeitschrift fu'r Wirtschaftswissenschaften*, Vol. 28 No. 4, pp. 119-145, December 2010.
- [11] T. S. Jung, M. S. Yim, & J. B. Lee, A Development of Comprehensive Framework for Continuous Information Security, *Journal of Digital Convergence*, Vol. 10, No.2, pp. 479-498, 2012.
- [12] D. W. Organ, *Organizational Citizenship Behavior: The Good Soldier Syndrome*: Lexington books, 1988.
- [13] D. W. Organ, P. M. Podsakoff, & S. B. MacKenzie, *Organizational Citizenship Behavior: Its Nature, Antecedents, and Consequences*: Sage Publications, Inc., 2006.
- [14] T. Y. Chou, S. C. T. Chou, J. J. Jiang, & G. Klein, The organizational citizenship behavior of IS personnel: Does organizational justice matter?, *Information & Management*, Vol. 50, pp. 105-111, 2013.
- [15] J. Shropshire, M. Warkentin, & S. Sha, Personality, attitudes, and intentions: Predicting initial adoption of information security behavior, *Computers & Security*, Vol. 49, pp. 177-191, 2015.
- [16] R. E. Crossler, A. C. Johnston, P. B. Lowry, Q. Hu, M. Warkentin, & R. Baskerville, Future directions for behavioral information security research. *Computers & Security*, Vol. 32, pp. 90-101, 2013.
- [17] P. Ifinedo, Information systems security policy

- compliance: An empirical study of the effects of socialization, influence, and cognition. *Information & Management*, Vol. 51, No. 1, pp. 69-79, 2014.
- [18] S. G. Lee & M. S. Chae, An Study on the Factors that Motivate The Compliance of the Organizational Security Policy. *Korean Journal of Business Administration*, Vol. 27, No. 6, pp. 927-953, 2014.
- [19] M. S. Yim, The Effect of Characteristics of Information Security Policy on Security Policy Compliance Intention of Employees in Financial Firms, *Journal of the Korea Service Management Society*, Vol. 14, No. 1, pp. 143-171, 2013.
- [20] A. Hovav & J. D'Arcy, Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea. *Information & Management*, Vol. 49, No. 2, pp. 99-110, 2012.
- [21] C. L. Anderson & R. Agarwal, Practicing safe computing: a multimedia empirical examination of home computer user security behavioral intentions. *MIS quarterly*, Vol. 34, No. 3, pp. 613-643, 2010.
- [22] B. Bulgurcu, H. Cavusoglu, & I. Benbasat, Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness, *MIS quarterly*, Vol. 34, No. 3, pp. 523-548, 2010.
- [23] T. Bateman & D. Organ, Job Satisfaction and the Good Soldier: The Relationship between Affect and Employee Citizenship. *Academy of Management Journal*, Vol. 26, No. 4, pp. 587-595, 1983.
- [24] S. W. Lee, Y. E. Cho, & K. S. Lee Y. E., The Role of Justice and Organizational Citizenship Behaviour in the Relation between Measurement Diversity and Managerial Performance, *Journal of Digital Convergence*, Vol. 11, No. 11, pp. 219-231, 2013.
- [25] J. W. Graham & L. V. Dyne, Gathering information and exercising influence: Two forms of civic virtue organizational citizenship behavior. *Employee Responsibilities and Rights Journal*, Vol. 18, No. 2, pp. 89-109, 2006.
- [26] D. W. Organ, The Motivational Basis of Organizational Citizenship Behavior. *Research in Organizational Behavior*, Vol. 12, No. 1, pp. 43-72, 1990.
- [27] D. J. Koys, The effects of employee satisfaction, organizational citizenship behavior, and turnover on organizational effectiveness: a unit-level, longitudinal study, *Personnel Psychology*, Vol. 54, No. 1, pp. 101-114, 2001.
- [28] P. M. Podsakoff & S. B. MacKenzie, Organizational citizenship behaviors and sales unit effectiveness, *Journal of Marketing Research*, Vol. 31, No. 3, pp. 351-363, 1994.
- [29] P. M. Podsakoff, M. Ahearne, & S. B. MacKenzie, Organizational citizenship behavior and the quantity and quality of work group performance, *Journal of Applied Psychology*, Vol. 82, No. 2, pp. 262-270, 1997.
- [30] H. J. R. Yen & B. P. Niehoff, Organizational citizenship behaviors and organizational effectiveness: examining relationships in Taiwanese banks, *Journal of Applied Social Psychology*, Vol. 34, No. 8, pp. 1617-1637, 2004.
- [31] S. C. Yang & C. K. Farn, Exploring tacit knowledge sharing intention and behavior within workgroup from the perspectives of social capital and behavioral control. *PACIS 2007 Proceedings*, 38, 2007.
- [32] H. R. Yen, E. Y. Li, Brian, & P. Niehoff, Do organizational citizenship behaviors lead to information system success?: Testing the mediation effects of integration climate and project management, *Information & Management*, Vol. 45, No. 6, pp. 394-402, 2008.
- [33] C. Yoon, The effects of organizational citizenship behaviors on ERP system success, *Computers in Human Behavior*, Vol. 25, No. 2, pp. 421-428, 2009.
- [34] K. L. Thomson, Rossouw von Solms, & Lynette Louw, Cultivating an organizational information security culture, *Computer Fraud & Security*, Vol. 10, pp. 7-11, 2006.
- [35] S. Goel & I. N. Chengalur-Smith, Metrics for

characterizing the form of security policies. *The Journal of Strategic Information Systems*, Vol. 19, No. 4, pp. 281-295, 2010.

[36] T. Dinev, J. Goo, Q. Hu, & K. Nam, User Behaviour towards Protective Information Technologies: The Role of National Cultural Differences. *Information Systems Journal*, Vol. 19, No. 4, pp. 391-412. 2009.

[37] J. D'Arcy, A. Hovav, & D. Galletta, 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.

[38] S. M. Lee, S. G. Lee, & S. Yoo, An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management*, Vol. 41, No. 6, pp. 707-718, 2004.

[39] C. J. Park & M. S. Yim. An Understanding of Impact of Security Countermeasures on Persistent Policy Compliance. *Journal of Digital Convergence*, Vol. 10, No. 4, pp. 23-35, 2012.

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

[41] W. Chin, B. Marcolin, & P. Newsted, A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. *Information Systems Research*, Vol. 14, No. 2, pp. 189-217, 2003.

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

[43] M. Wetzels, Using PLS path modeling for assessing hierarchical construct models: Guidelines and empirical illustration, *MIS Quarterly*, Vol. 33, No. 1, pp. 177-195, 2009.

[44] M. Sobel, Asymptotic confidence intervals for

indirect effects in structural equation models. *Sociological methodology*, Vol. 13, pp. 290-312, 1982.

[45] R. M. Baron & D. A. Kenny, The moderator-mediator variable distinction in social psychological research: Conceptual, strategic, and statistical considerations. *Journal of Personality and Social Psychology*, Vol. 51, No. 6, pp. 1173-1182, 1986.

부록 1. 설문문항

Construct	Survey Items	Sources
SP	<ol style="list-style-type: none"> 1. My organization has specific guidelines that describe acceptable use of e-mail. 2. My organization has established rules of behavior for use of computer resources. 3. My organization has a formal policy that forbids employees from accessing computer systems that they are not authorized to use. 4. My organization has specific guidelines that describe acceptable use of computer passwords. 5. My organization has specific guidelines that govern what employees are allowed to do with their computers. 	[37]
SETA	<ol style="list-style-type: none"> 1. My organization provides training to help employees improve their awareness of computer and information security issues. 2. My organization provides employees with education on computer software copyright laws. 3. In my organization, employees are briefed on the consequences of modifying computerized data in an unauthorized way. 4. My organization educates employees on their computer security responsibilities. 5. In my organization, employees are briefed on the consequences of accessing computer systems that they are not authorized to use 	[37]
OCB	<ol style="list-style-type: none"> 1. Being willing to volunteer for tasks 2. Often sharing knowledge and information with others 3. Frequently offering suggestions 4. Not being absent from work 5. Showing enthusiasm about my work 	[14]
CI	<ol style="list-style-type: none"> 1. I am likely to follow organizational security policies. 2. It is possible that I will comply with organizational IS security policies to protect the organization's information systems. 3. I am certain that I will follow organizational security policies. 4. It is clear that I will follow organizational security policies. 	[40]

한진영(Han, Jin Young)



- 1997년 2월 : 외국어대학교(이학석사)
- 2013년 2월 : 고려대학교(경영학박사)
- 2015년 2월 ~ 현재 : 중앙대학교 창의ICT공과대학 산학협력중점 교수
- 관심분야 : 정보보안, 프로젝트관리
- E-Mail : win1999@naver.com

김유정(Kim, Yoo Jung)



- 1990년 2월 : 외국어대학교 경영정보대학원(경영학석사)
- 1999년 2월 : 고려대학교(경영학박사)
- 2006년 3월 ~ 현재 : 호서대학교 경영학부 교수
- 관심분야 : 디지털비즈니스모델, 정보보안
- E-Mail : faith@hoseo.edu