

조직의 정보보안 목표 설정과 공정성이 보안정책 준수 의도에 미치는 영향

황인호¹, 김승욱^{2*}

¹중앙대학교 지식경영학부 겸임교수, ²평택대학교 경영학과 교수

A Study on the Influence of Organizational Information Security Goal Setting and Justice on Security Policy Compliance Intention

In-Ho Hwang¹, Seung-Wook Kim^{2*}

¹Adjunct Professor, School of Knowledge-Based Management, Chung-Ang University

²Professor, Department of Business Administration, Pyeong-Taek University

요 약 전 세계적인 정보보안 위협의 증대에 따라 조직들은 보다 전문화된 정보보안 정책 및 시스템을 도입 및 활용에 투자 비중을 높이고 있다. 정보보안은 보안 시스템 및 정책을 이행하는 조직원들의 참여가 무엇보다 필요하며, 조직 내부의 보안 수준을 높이기 위해서는 조직원들의 정보보안 준수 의도 향상을 위한 조직의 체계적인 지원이 무엇보다 필요하다. 본 연구는 정보보안 분야에 공정성이론과 목표설정이론을 적용하여 조직원의 정보보안 준수 의도를 높이기 위한 매커니즘을 찾는다. 즉, 보안정책 목표설정이 조직원들의 보안관련 공정성 인식수준에 긍정적인 영향을 미치고, 공정성은 준수 의도에 긍정적인 영향을 미친다는 연구모델 기반 가설 검증을 실시한다. 연구대상은 정보보안 정책을 도입한 조직의 조직원들이며, 설문조사를 통하여 유효샘플 383개를 수집하였다. 연구가설 검증은 구조방정식 모델링을 실시하였다. 보안정책 목표 요인(목표 난이도, 목표 구체성)이 조직원의 보안관련 공정성 인식을 높이며, 보안관련 공정성(분배, 절차, 그리고 정보 공정성)이 준수 의도에 긍정적 영향을 주는 것으로 나타났다. 결과는 조직의 보안 정책에 대한 조직원들의 준수 의도 향상을 위한 전략적 접근 방향을 제시한다.

주제어 : 정보보안 정책 준수 의도, 분배공정성, 절차공정성, 정보공정성, 정보보안 목표 설정

Abstract The threat to information security is growing globally. To this, organizations are increasing the weight of adapting and operating the more specialized information security policy and system. Information security requires participation from the employees who execute the security system and policy, and to increase the level of organization's internal security, requires organization's systematic support to improve employees' information security compliance intention. This research finds the mechanism for improving employee's information security compliance intention by applying justice theory and goal setting theory in information security. We use structural equation modeling to verify the research hypothesis, and conducted a survey on the employees of organization with information security policy. In other words, this research performs verification of the research model based hypothesis which claims that security policy goal setting has positive influence on employee's level of security related justice recognition, and claims that justice has positive influence on compliance intention. The object of study is the employees of the organization that adapts information security policy, and 383 valid samples were collected via survey. Structural equation modeling was performed to verify the research hypothesis. The result shows that security policy goal factor (goal difficulty, goal specificity) improves employee's security related justice recognition, and that security related justice (distribution, process, and information justice) has positive influence on compliance intention. The result suggests the strategic approach directions for improving employees' compliance intention on organization's security policy.

Key Words : Information Security Policy Compliance Intention, Distribution Justice, Procedural Justice, Informational Justice, Security Goal Setting

*This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF- 2016S1A5A8019240)

*Corresponding Author : Seung-Wook Kim (swkim@ptu.ac.kr)

Received November 30, 2017

Revised January 2, 2018

Accepted February 20, 2018

Published February 28, 2018

1. 서론

정보 가치의 중요성 증대와 더불어 다양한 채널을 통한 정보 위협 요인의 증가에 따라, 많은 조직들은 정보보안 시스템에 투자를 높이고 있다. IDC(2016)에 따르면 2020년까지 전 세계의 보안관련 하드웨어, 소프트웨어, 서비스에 투자하는 비율은 101.6억 달러에 달할 것으로 판단되고 있다.

Loch et al.(1992)는 정보보안 위협은 다양한 루트를 통해서 발생하는데, 지속적으로 위협요인이 커지는 부분은 내부자에 의한 정보보안 사고 및 위협요인이라고 하였다. 실제 Verizon(2017) 보고서에 따르면, 외부로 결과가 드러난 내부자에 의한 정보보안 사고는 매년 15~20% 수준에 이르고, 드러나지 않는 사고까지 추가할 경우 높은 수준의 위협을 가지게 될 것으로 판단하고 있다. 즉, 정보보안 위협 중 내부자에 의한 정보보안 위협 최소화를 위한 노력이 필요하다[4-6].

조직원의 정보보안 준수와 관련된 연구를 살펴보면, 조직원의 보안 동기와 관련한 접근 연구가 대부분이다 [7-15]. 대표적으로 억제이론(Deterrence Theory), 보호 동기이론(Protection Motivation Theory), 계획된 행동이론(Theory of Planned Behavior), 그리고 합리적선택이론(Rational Choice Theory) 등의 이론적 기반을 통하여, 조직원의 정보보안 준수를 위한 동기를 높이기 위한 연구적 접근이 실시되었다. 선행연구들은 동기개선이 자발적 보안준수로 이어지는 관점을 명확하게 제시했다는 연구적 성과를 제시하고 있으나, 조직원의 보안 준수를 위한 조직적 관점에서 수행해야할 접근 연구는 상대적으로 부족한 면이 있다.

특히, 조직에서 특정한 활동에 대한 조직원들의 행동은 조직에서 제시 및 평가하는 공정성에 의해서 개선될 수 있으며[16-19], 정보보안 정책을 조직원에게 체계적으로 제공하고 실행에 옮기도록 하기 위해서는 보안 정책의 명확한 목표 수준 및 행동 방향을 제시할 때 실현가능성이 높아질 수 있다[15]. 즉, 일찍부터 조직과 조직원의 관계에 대한 이론적 근거가 마련되어 왔던 공정성이론(Justice Theory)과 목표설정이론(Goal Setting Theory)의 조직원의 정보보안 준수와 관련된 연구는 상대적으로 부족하여, 조직의 공정성 수준과 목표 체계 등이 보안 준수에 어떻게 영향을 줄 수 있는지 연구가 필요한 실정이다.

이에, 본 연구의 목적은 조직원의 정보보안 준수의를 높임으로써 내부자의 정보보안 위협을 최소화하기 위

한 원인 요인을 도출하는 것이다. 특히, 조직에서 제공하는 정보보안 공정성 수준에 대한 조직원의 인지 수준이 보안 준수 의도에 미치는 영향을 찾음으로써, 조직차원의 공정한 보안 활동이 조직원에게 미치는 결과를 제시한다. 세부적으로 공정성의 세부 요인인 분배공정성(Distribution Justice), 절차공정성(Procedural Justice), 정보공정성(Information Justice)을 정보보안 관련 세부 요인으로 적용하여 보안준수에 미치는 영향을 검토한다. 또한, 조직원이 인지하는 공정성 수준을 높이기 위해 조직에서 구축한 정보보안정책 목표 수준이 중요한 원인이 될 것으로 판단하고 선행연구를 기반으로 목표설정이론의 세부요인 (보안정책 목표 난이도(Goal Difficulty) 및 구체성(Goal Specificity))이 보안관련 공정성에 미치는 영향관계를 검토한다.

결과는 보안 정책 목표 수립(목표 난이도, 목표 구체성)이 조직원이 인식하는 정보보안관련 공정성 수준 및 나아가 정보보안 준수 의도에 미치는 긍정적 효과를 체계적으로 설명할 수 있으며, 이론적 측면과 실무적 측면의 시사점을 제시한다.

2. 이론적 배경

2.1 정보보안 정책 준수 의도

웹 및 모바일 기반의 정보시스템의 발전은 조직의 정보관련 획득 및 확보, 공유, 그리고 확산의 활동 수준을 높여 조직원에게 정보활용을 통한 생산성 확보 및 성과 도출에 긍정적인 영향을 미치는 것으로 나타나고 있다 [20]. 반면, 조직 정보시스템 접근 방법 등의 다양성은 정보 노출 위협을 높여 정보보안 사고로 이어질 가능성을 높인다[6,8,15]. 정보시스템을 활용하는 조직원의 관점에서, 조직 내 정보보안 위협은 자신이 자각하지 않는 한 지속적으로 발생가능성이 높아 정보보안에 대한 능동적 행동 수준이 요구된다[9,21]. 정보보안 준수 의도에 대한 정의를 살펴보면, Vance et al.(2012)는 조직 내부, 외부의 보안 위협으로부터 조직의 정보자원을 보호하려는 의도로서 준수 의도를 정의하고 있으며, 정보보안 준수 의도를 높이기 위한 선행요인을 제시하고 지원할 때 자발적인 정보보안 준수 행동으로 이어진다고 보았다.

2.2 조직공정성이론(Justice Theory)

조직공정성(Organizational Justice)은 조직에서 사람

들에 대한 공정한 대우와 관련된 포괄적인 이론적 개념으로서[23], 공정성의 기본적인 가정은 사람들은 공정성에 많은 가치를 두며, 자신과 조직간의 관계에서의 공정성을 확보하기 위하여 동기화된다는 관점이다[24]. 즉, 특정 활동에 있어 구성원들의 평가는 공정한 과정 및 절차 등으로 진행되었는가를 통해 이루어지며, 조직은 활동 과정에서 나타날 수 있는 공정성 문제를 명확하게 제시할 경우 조직원의 성과가 높아진다[17]. 조직공정성은 크게 분배공정성(Distribution Justice), 절차공정성(Procedural Justice), 그리고 정보공정성(Information Justice)로 구분되어 조직 관련 연구에서 활용되고 있다[25,26].

분배공정성은 특정 활동에 대한 결과를 분배 또는 결과와 관련된 공정한 수준에 대한 인식으로 정의된다[27]. Muchinsky(2006)에 따르면 분배공정성은 가치에 기반을 두고 있으며, 상황적 특성에 따라서 형평(Equity), 평등(Equality), 그리고 필요(Needs)의 유형에 따라 구성원은 분배공정성의 수준을 평가하게 된다고 보았다. 조직에서 분배공정성은 구성원의 조직시민행동을 높이고, 이직의도를 감소시킬 수 있는 요인이며, 이를 높이기 위해서는 조직차원의 공정성에 대한 인식지원 활동이 선행되어야 한다[17].

절차공정성은 결과를 성취하기 위해 사용되는 수단의 수준에 대한 인식으로 정의된다 [28]. Muchinsky(2006)는 절차공정성을 의사결정을 수행하는데 사용하는 정책과 절차들에 대하여 지각하는 정도로 정의하며, 절차를 수행하는 수단의 수준에 대한 평가가 구성원들의 행동을 이끈다고 하였다. 즉, 일관적이고, 편파가 없고, 정확하다고 인식하는 것이 중요한 관점이다. Colquitt(2001)은 절차공정성이 조직에서 제시하는 규칙준수(Rule Compliance)를 높이기 때문에, 절차공정성을 높이기 위한 노력이 필요하다고 보았다.

정보공정성은 사람들이 관심을 가지는 절차에 대한 지식 제공하는 것과 관련된 인식의 수준으로 정의된다[29]. Muchinsky(2006)는 바람직한 성과를 결정하는 데 사용되는 절차에 대한 명확한 정보를 제공하는 것이 우선적으로 필요하며, 충분한 사전 설명이 공정하다고 평가될 경우 관련 행동으로 이어진다고 하였다. Judge and Colquitt(2004)는 정보공정성은 스트레스를 감소시키는 요인임을 제시하였으며, 그들은 업무와 가족 간 갈등을 정보공정성이 감소시키며, 결과적으로 조직원의 스트레스 및 직업만족도의 부정적 결과를 낮출 수 있음을 증명

하였다.

정보보안 관점에서 공정성은 조직원들의 행동을 변화시키는 요인이다. 외부의 보안 위협으로부터 조직의 데이터를 보호하기 위해서 조직은 정보보안 관련 정책을 지속적으로 변화시키고 및 기술을 지속적으로 향상시키고자 한다[6,8-10]. 더불어, 변화하는 조직의 보안 정책 및 기술은 조직원에게 재빠른 대응 및 보안 관련 성과를 달성하길 요구한다[15]. 공정성은 조직의 변화하는 기술 및 정책에 대한 조직원의 참여를 유도할 수 있는 선행 조건이다[26]. 즉, 정보보안 준수 및 미준수에 따른 결과의 적용을 공정하게 하는 분배공정성, 결과를 성취하기 위하여 적용하는 절차 공정성, 그리고 모든 사람들에게 명확하게 보안 관련 정보를 제공하는 것은 조직원들의 보안 관련 참여수준을 높일 수 있다.

조직공정성은 조직원의 성과 달성에 영향을 미친다. Colquitt(2001)은 분배공정성이 조직원의 결과 또는 만족도에 영향을 주고, 절차 공정성은 규정 준수, 그리고 정보공정성은 협력성에 영향을 준다고 하였다. 또한, Zhang et al.(2014)는 업무 성과에 조직차원의 공정성이 긍정적인 영향을 미친다는 것을 검증하였다. 더불어 조직공정성은 조직원의 준수 의도에 긍정적인 영향을 미치는데, Li et al.(2014)은 공정성이 인터넷 사용 정책 준수 의도를 높이는 것을 증명하였다. 또한, Son and Park(2016)은 컴퓨팅 관련 비업무 준수 의도를 절차 공정성이 높이는 것을 증명하였다. 반대로 Zhang and Aqarwal(2009)은 조직공정성이 낮을 경우 이직의도를 높이는 것을 증명하였다. 즉, 조직공정성은 보안 분야에서도 조직원들의 준수 의도를 높일 것으로 판단되며, 특히 세부변수들인 분배공정성, 절차공정성, 그리고 정보공정성이 준수 의도를 높일 것으로 판단하여, 다음과 같은 연구가설을 제시한다.

H1 : 정보보안관련 분배 공정성은 보안정책 준수 의도에 정(+)의 영향을 미칠 것이다.

H2 : 정보보안관련 절차 공정성은 보안정책 준수 의도에 정(+)의 영향을 미칠 것이다.

H3 : 정보보안관련 정보 공정성은 보안정책 준수 의도에 정(+)의 영향을 미칠 것이다.

2.3 목표설정이론 (Goal Setting Theory)

목표는 개인에게 의도적인 행동방향을 제시하는 개념으로서, 목표는 행동방향을 의도적으로 설정하고, 구체적으로 구성될 경우 보다 체계적으로 노력해야 할 부분을

제시한다. 목표설정이론은 개인들은 설정된 목표를 동기를 삼아 이를 성취하기 위하여 노력한다는 동기 이론이다[32]. 목표는 개인의 성과뿐 아니라 조직과 조직원의 관계에서 조직의 성과 달성을 위하여 긍정적인 영향을 미치는 중요한 동기가 된다[15].

Locke and Latham(2002)은 조직의 목표가 조직원의 성과에 미치는 관계를 제시하였는데, 조직 수준에서 정립된 목표는 개인 수준의 목표로 긍정적으로 영향을 미치고, 형성된 개인 목표는 성과를 높인다고 하였다. 반대로, Wright and Davis(2003)는 조직 목표를 달성하는데 부정적인 업무 환경에 의해 개인의 목표 구체성이 낮아질 경우, 개인의 업무 만족이 감소한다고 하였다.

Wright (2004)는 조직원의 업무 동기 향상은 개인의 목표 속성(Goal Attribute)에 따라 영향을 주기 때문에 조직차원의 목표 속성을 명확하게 제공하는 것이 중요하다고 보았다. 목표설정이론에서 제시하는 대표적인 목표 속성으로는 목표 난이도(Goal Difficulty)와 목표 구체성(Goal Specificity)가 있다.

목표난이도는 달성은 가능한 수준이지만, 실행하기 어려운 수준의 목표 상태를 의미하며, 목표 구체성은 대상 목표가 구체적인 상태를 의미한다[36]. 목표의 난이도와 구체성은 복합적으로 나타나 개인 및 조직의 성과에 영향을 미친다[37,38]. 즉, 보다 어렵지만 대상 목표 달성을 위한 과정 및 활동이 체계적으로 구축되어 있을 때, 목표에 대한 성과를 이룰 수 있다.

정보보안 분야에서도 조직의 정보보안 정책의 목표는 조직원의 보안 관련 긍정적 결과를 도출하도록 동기를 부여하는 요인이다[15]. 조직의 정보보안 성과는 실제 업무에 정보보안 규칙 및 기술을 적용하는 조직원에 의해서 결정되기 때문에, 조직원이 이해할 수 있는 정보보안 정책에 대한 목표를 제시하는 것이 중요하다[39]. Hu et al.(2012)는 조직의 정보보안은 보안 관련 조직문화가 구축되는 것이 선행되어야 하며, 조직문화는 조직원에게 목표 방향을 제시하고, 조직원이 보안에 대한 가치(value)를 인지함으로써 형성된다고 하였다. Koskosas(2008)은 정보보안 관리 관점에서 목표 설정의 중요성을 제시한다. 그들은 조직에 맞는 정보보안 정책 및 기술을 채택 및 활용하기 위해서는 조직 구조에 맞는 목표 설정 계획, 이행, 평가 단계별 접근의 필요성을 제시하며, 단계적 목표가 완료될 때 조직원들이 비로소 목표를 이행할 수 있다고 하였다.

명확한 목표 설정은 조직의 공정성에 영향을 준다. Li and Butler(2004)은 목표 설정이 조직 몰입에 영향을 주며, 공정성이 매개 효과를 가진다고 하였다. 즉, 목표설정이 조직의 공정성에 긍정적인 영향을 미치고, 나아가 조직원의 몰입에 긍정적인 영향을 미친다. 따라서 정보보안 관련 조직공정성에 목표 설정요인들이 긍정적인 영향을 미칠 것으로 판단하고, 다음과 같은 연구가설을 제시한다.

- H4a : 정보보안관련 목표 난이도는 분배 공정성에 정(+)의 영향을 미칠 것이다.
- H4b : 정보보안관련 목표 난이도는 절차 공정성에 정(+)의 영향을 미칠 것이다.
- H4c : 정보보안관련 목표 난이도는 정보 공정성에 정(+)의 영향을 미칠 것이다.
- H5a : 정보보안관련 목표 구체성은 분배 공정성에 정(+)의 영향을 미칠 것이다.
- H5b : 정보보안관련 목표 구체성은 절차 공정성에 정(+)의 영향을 미칠 것이다.
- H5c : 정보보안관련 목표 구체성은 정보 공정성에 정(+)의 영향을 미칠 것이다.

3. 연구 모델 및 방법

3.1 연구 모델

본 연구의 목적은 조직원의 정보보안 준수 의도 향상을 위하여 조직에서 고려해야 할 요인을 공정성 이론 및 목표설정이론 관점에서 각 선행 요인을 도출하고, 각 요인간의 영향관계를 도출하는 것이다. 즉, 보안 관련 공정성(분배, 절차, 정보적 공정성)이 보안 준수 의도에 미치는 영향 관계와 보안 정책 목표 설정(목표 난이도, 목표 구체성)이 보안 관련 공정성에 미치는 긍정적 영향 관계를 파악하기 위하여 연구 모델을 제시하며, 다음 Fig. 1과 같다.

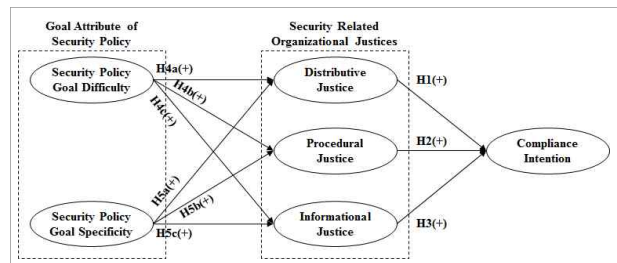


Fig. 1. Research Model and Proposed Hypotheses

3.2 데이터 측정 방법 및 수집

본 연구는 구조방정식모델링을 기반으로 연구 모델을 검증하고자 하며, 관련 데이터는 서베이 기법을 통해 확보하였다. 측정변수 도출과정은 우선 선행 이론 연구를 기반으로 다항목 지표를 확보하였으며, 정보보안 분야에 맞게 재정립하여 7점 리커트 척도를 사용하여 구성하였다. 더불어 설문항목의 정보보안 영역에서의 타당성을

확보하기 위하여, 설문지 개발 전 정보보안 정책을 보유한 기업에서 근무하고 있는 10명의 사람들에게 사전 인터뷰를 실시하였으며, 1차 개발 후 정보보안 정책을 보유한 기업에 근무하고 있는 경영학과 대학원생 10명에게 내용타당성을 확인하였다. 이를 통해 도출된 6개 변수의 측정항목들은 총 22개이며 Table 1과 같다.

Table 1. Questionnaire

Constructs	Items	Source
Goal Difficulty	GD1 Organization's information security policy is easy to understand.	[35]
	GD2 The writing of organization's information security policy facilitates understanding.	
	GD3 Organization's information security policy is provided as a clear information.	
Goal Specificity	SP1 A lot of effort is required to achieve organization's information security policy goal.	[35]
	SP2 High level of security technology and know-how is required to achieve the organization's information security.	
	SP3 Organization's information security goal requires a high level of information security behavior from employees.	
Distributive Justice	DJ1 My information security behavior is reflected on the result of my security related work.	[27]
	DJ2 My information security behavior is appropriate for performing security related work.	
	DJ3 My information security behavior contributes to organization's information security.	
	DJ4 My information security behavior is valid, considering my information security performance (Drop).	
Procedural Justice	PJ1 Organization's information security process influences the result of my information security behavior.	[28]
	PJ2 Organization's information security process is applied consistently.	
	PJ3 Organization's information security process is applied without prejudice.	
	PJ4 Organization's information security process is ethically and morally acceptable (Drop).	
Informational Justice	IJ1 Organization communicates about information security.	[29]
	IJ2 Organization clearly explains the information security process.	
	IJ3 Organization logically explains the information security process.	
	IJ4 Organization provides details about information security compliance.	
Compliance Intention	C11 It is possible that I will follow information security policies.	[42]
	C12 It is probable that I will follow information security policies.	
	C13 I am likely to follow information security policies.	
	C14 I am certain that I will follow information security policies.	

본 연구는 정보보안 관련 조직의 공정성 수준에 대한 조직원들의 인식이 준수 의도에 미치는 영향 및 공정성 인식 수준을 높이기 위한 조직차원의 노력요인을 목표설정이론 관점에서 찾고자 한다. 연구 모델의 결과의 시사점을 높이기 위하여, 본 연구는 정보보안 정책을 엄격하게 적용하고 있는 대기업 및 금융기업에서 근무하는 조직원들을 대상으로 하고자 한다. 정보보안 정책에 대한 공정성 및 목표 수준을 파악하기 위함이다. 반면, 보안 부서의 조직원은 업무 목표가 보안이 아닌 업무 성과인 일반 조직원과 달리 엄격한 보안 체계 구축에 있기 때문에 본 연구의 목적과 맞지 않아 제외하였다.

설문은 2017년 4월 1일부터 5월 15일까지 대학의 사회교육원에서 공부하는 직장인들을 대상으로 하였으며, 이중 정보보안 정책을 보유한 사람들만 설문을 하도록 하였으며, 모든 설문 응답자들에게 설문 전 사전 설문 목적 및 허가를 받고 설문에 응답하도록 하였다. 총 700부를 배포하여 453개의 응답을 확보하였다. 이중 미진한 응답치 70개를 제외하고 383개를 본 연구에 활용하였다. 응답의 인구통계학적 특성은 Table 2와 같다.

Table 2. Demographic Characteristics

Demographic Categories		Frequency	%
Total		383	100.0
Gender	Male	235	61.4
	Female	148	38.6
Age	< 30	109	28.5
	31~40	125	32.6
	41~50	109	28.5
	> 50	40	10.4
Type of Industry	Manufacturer	74	19.3
	Service	309	80.7
Job Position	Staff	123	32.1
	Assistant Manager	102	26.6
	Manager	115	30.0
	General Manager	43	11.2

4. 가설 검증

4.1 신뢰성 및 타당성 분석

연구 가설 및 모델 검증은 SPSS 21.0과 AMOS 22.0을

활용하였다. 우선 Cronbach's Alpha 값을 활용하여 신뢰성 분석을 실시하였다. Cronbach's Alpha는 0.7이상[43]을 요구하며, 분석 결과 총 22개의 설문항목 중 문제가 있는 2개 항목(DJ4, PJ4)을 제외하였다. 그리고 확인적 요인분석을 통하여 타당성 분석을 실시하였다. 타당성 분석은 개념신뢰도(Construct Reliability: CR)와 평균분산추출(Average Variance Extracted: AVE)을 실시하며, CR의 기준은 0.8, AVE의 기준은 0.5을 요구한다[44,45]. 분석결과 확인적요인분석의 적합도는 권장치에 부합하는 것으로 나타났으며($\chi^2/df = 1.492$, GFI = 0.949, AGFI = 0.929, CFI = 0.989, NFI = 0.967, RMSEA = 0.036), 신뢰성 및 타당성 모두 요구 기준에 적합한 것으로 나타났다(Table 3 참조).

Table 3. Result for Construct Validity and Reliability

Construct	Item	Factor Loading	Cronbach's Alpha	CR	AVE
Goal Difficulty	GD1	.738	0.929	0.900	0.693
	GD2	.812			
	GD3	.741			
Goal Specificity	SP1	.808	0.890	0.828	0.616
	SP2	.839			
	SP3	.683			
Distributive Justice	DJ1	.734	0.906	0.847	0.649
	DJ2	.760			
	DJ3	.744			
Procedural Justice	PJ1	.740	0.901	0.814	0.594
	PJ2	.792			
	PJ3	.802			
Informational Justice	IJ1	.788	0.925	0.875	0.635
	IJ2	.805			
	IJ3	.784			
	IJ4	.791			
Compliance Intention	CI1	.853	0.915	0.884	0.718
	CI2	.836			
	CI3	.864			
	CI4	.814			

추가적으로 판별타당성 분석을 실시하였으며, AVE의 제공근 값이 변수들의 상관계수 값보다 큰 것으로 나타나, 판별타당성이 있는 것으로 나타났다.

더불어 연구는 동일한 응답자를 대상으로 다수의 문항들을 측정하였다. 또한 분석 결과 상관관계가 비교적 높게 나타나, 동일방법편의 발생가능성이 있다. Podsakoff et al.(2003)의 SMF(Single Method Factor) 접근법을 통하여 동일방법편의를 검증하였다. 분석한 결과 $\Delta\chi^2$ 값이 54.46로서 변화량이 $p < 0.01$ 수준에서 유의한 것으로 나타나, 동일방법편의 문제가 있을 수 있는 것으로 나타났다. 하지만, 변화량이 높지 않고, 공통요인 적용 전과 후의 문항들의 표준적재치들의 차이가 0.2 미만으로 나타나 동일방법편의의 문제는 낮은 것으로 나타났다[48].

Table 4. Result for Discriminant Validity

Constructs	1	2	3	4	5	6
Goal Difficulty	0.832					
Goal Specificity	.48**	0.785				
Distributive Justice	.61**	.56**	0.805			
Procedural Justice	.61**	.51**	.68**	0.771		
Informational Justice	.63**	.49**	.62**	.57**	0.797	
Compliance Intention	.52**	.43**	.54**	.50**	.55**	0.848

Note: Values in bold type along the diagonal indicate the square root of the AVE
 **: $p < 0.01$

4.2 구조모형 평가

구조모형 평가는 구조모형의 적합도, 경로계수 (β), 그리고 내생 변수에 대한 결정 계수 (R^2)를 통하여 실시한다. 첫째, 구조모형의 적합도 검정을 실시하였다. 결과는 구조방정식모델링에서 요구하는 수준을 상회하는 것으로 나타났다($\chi^2/df = 1.791$, GFI = 0.931, AGFI = 0.901, CFI = 0.981, NFI = 0.958, RMSEA = 0.46).

둘째, 구조모형의 경로간의 인과관계를 통하여 가설 검정을 실시한다(Fig. 2, Table 5 참조).

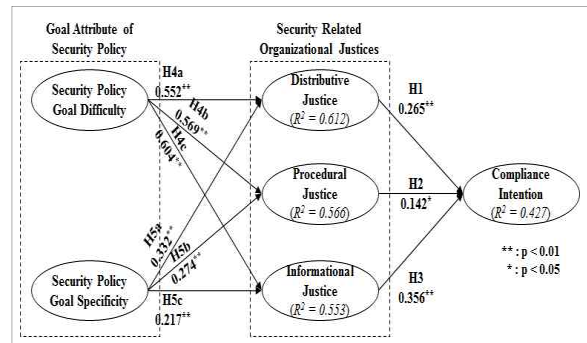


Fig. 2. Results of the Structural Model

Table 5. Summary of Hypothesis Tests

	Path	Coefficient	t-value	Results
H1	DJ → CI	0.265**	4.205	Support
H2	PJ → CI	0.142'	2.251	Support
H3	IJ → CI	0.356**	5.837	Support
H4a	GD → DJ	0.552**	10.359	Support
H4b	GD → PJ	0.569**	9.926	Support
H4c	GD → IJ	0.604**	10.927	Support
H5a	GS → DJ	0.332**	6.565	Support
H5b	GS → PJ	0.274**	5.117	Support
H5c	GS → IJ	0.217**	5.252	Support

*: $p < 0.05$ / **: $p < 0.01$

DJ(Distributive Justice), PJ(Procedural Justice), IJ(Informational Justice), CI(Compliance Intention), GD(Goal Difficulty), GS(Goal Specificity),

정보보안 관련 분배공정성이 조직원의 정보보안 준수 의도에 정(+의 영향을 미친다는 가설[H1])은 채택되었다. 이는 분배공정성이 인터넷 사용 정책 준수 의도에 긍정적인 영향을 미친다는 선행연구[26]와 같은 결과이다. 즉, 조직의 정보보안 정책이 직원들의 보안 행동에 공정하게 적용되어, 정보보안 행동이 개인의 업무 결과에 반영된다고 판단될 때, 직원들은 준수 의도를 높이는 것으로 판단된다.

정보보안 관련 절차공정성이 조직원의 정보보안 준수 의도에 정(+의 영향을 미친다는 가설[H2])은 채택되었다. 이는 절차공정성이 컴퓨팅 관련 비업무준수에 긍정적인 영향을 미친다는 선행연구[30]와 같은 결과이다. 즉, 정보보안 관련 절차가 편견없이 일관되게 적용되고 있다고 판단될 때, 자신들의 정보보안 준수 의도가 높아지는 것을 의미한다.

정보보안 관련 정보공정성이 조직원의 정보보안 준수 의도에 정(+의 영향을 미친다는 가설[H3])은 채택되었다. 이는 정보공정성이 인터넷 사용 정책 준수 의도에 긍정적인 영향을 미친다는 선행연구[26]와 같은 결과이다. 즉, 조직구성원들에게 정보보안 관련 정책 및 활동 규정을 명확하게 제공하기 위한 활동과 체계적인 설명이 제공될 때, 직원들의 정보보안 준수 의도는 높아짐을 의미한다.

보안정책 목표 난이도가 보안관련 조직공정성(분배공정성, 절차공정성, 정보공정성)에 정(+의 영향을 미친다는 가설[H4a, H4b, H4c])은 모두 채택되었다. 이러한 결과는 목표 설정이 조직의 공정성에 의해 매개 효과를 가지고 조직 몰입에 긍정적인 영향을 미친다는 선행연구 [41]와 유사한 결과이다. 즉 정보보안 역량 수준을 높이기 위한 조직차원의 정책 개발 시 보안 목표의 수준을 보다 높은 수준으로 제시할 경우, 직원들은 조직 차원의 보안 노력 및 체계적인 보안시스템을 구축한다고 판단하여, 보안관련 공정성이 높다고 인식함을 의미한다.

보안정책 목표 구체성 보안관련 조직공정성(분배공정성, 절차공정성, 정보공정성)에 정(+의 영향을 미친다는 가설[H5a, H5b, H5c])은 모두 채택되었다. 이러한 결과는 목표 설정이 조직의 공정성에 의해 매개 효과를 가지고 조직 몰입에 긍정적인 영향을 미친다는 선행연구[41]와 유사한 결과이다. 즉, 정보보안 목표 달성을 위한 보다 세분화된 규정 및 행동 수준의 제시가 직원들에게 공정성을 부여한다는 것을 의미한다.

마지막으로, 내생변수의 결정 계수를 도출하였다. 준수 의도는 분배공정성, 절차공정성, 그리고 정보공정성의 42.7%의 설명력을 가지고 있는 것으로 나타났으며, 분배공정성은 목표설정이론 요인들의 61.2%, 절차공정성은 동일요인들의 56.6%, 그리고 정보공정성은 55.3%의 설명력을 가지고 있는 것으로 나타났다.

5. 결론

본 연구는 중요성이 더해지고 있는 직원들의 정보보안 준수 수준을 높이기 위한 방법을 설명하기 위하여, 공정성이론과 목표설정이론을 정보보안 분야에 적용하여, 구성원들의 준수 의도를 높이기 위한 조직의 보안 정책 목표수립과 이행과정의 공정성의 중요성을 제시하고자 하였다. 이를 위하여 정보보안 정책을 도입한 기업에 근무하는 일반 직원들에게 연구모델에 대한 구성요소들을 설문 조사 및 구조방정식 모델링을 기반으로 변수들간의 영향관계를 증명하였다.

연구 결과는 다음과 같은 이론적 관점과 실무적 관점에서 시사점을 가진다.

첫째, 조직에서 직원의 정보보안 준수가 무엇보다 중요해지는 시점에서 공정성 이론과 목표설정이론을 정보보안 분야에 적용하여, 직원의 준수 의도를 높이기 위한 선행요인을 제시하고 결과를 검증함으로써, 보다 높은 수준의 정보보안 체계를 구축하기 위한 방향을 제시하였다. 즉, 이론적 측면에서 공정성이론과 목표설정이론을 조직과 직원의 관계에서 보안 준수 수준을 높이기 위한 방법으로 적용하였기 때문에, 향후 직원의 보안 준수 의도 향상 관련된 조직의 활동과 관련된 연구에 대한 이론적 기반이 될 것으로 판단된다. 더불어, 실무적 측면에서 이론기반 변수들간의 영향관계를 증명함으로써, 직원의 보안위협이 높아지는 현 시점에 조직차원의 실무적 대응 모델을 제시한 것에 의미를 가진다.

둘째, 공정성이론 상 세부변수(분배공정성, 절차공정성, 정보공정성)들이 준수 의도에 어떠한 영향을 미치는 것을 상세히 검증하였다. 이론적 관점에서 조직과 직원의 관계에서 공정성이 긍정적인 결과를 미친다는 결과가 정보보안 분야에 적용됨을 증명하였으며, 이러한 결과는 조직의 공정한 활동에 대한 인식이 준수 의도를 높임을 제시하였기 때문에, 공정성관련 향후 연구의 선행

연구로서 의미를 가진다. 실무적 관점에서 조직원들의 공정성에 대한 인식을 분배, 절차, 정보 제공 차원에서 세부적으로 관련성을 증명하였기 때문에, 조직이 조직원들의 정보보안 준수수준을 높이기 위한 공정 활동의 방향을 제시한다. 즉, 조직에서 보안 관련 공정함을 조직원들에게 제시하는 것이 준수행동을 높일 수 있기 때문에, 정보보안 규정에 맞는 성과를 명확하게 제시하고 모든 조직원들이 알 수 있도록 공유하는 것이 필요하다. 또한, 관련 정보보안 준수 절차에 대한 명확한 체계를 제시하는 것이 필요하다.

셋째, 목표설정이론의 세부변수(목표 난이도, 목표 구체성)가 보안관련 공정성에 어떠한 영향을 미치는지를 검증하였다. 이론적 관점에서 목표설정이론은 조직과 관련 분야에서 다양하게 활용되던 이론임에도 불구하고 조직과 조직원들의 보안관계를 설명하기 위한 연구에 적용이 미진하였다. 연구는 목표설정이 조직원의 보안 관련 공정성에 대한 인식을 높이는 것을 증명하였다. 실무적 관점에서 조직원의 공정성 인식을 높이기 위해, 조직은 보안 정책을 보다 높은 수준으로, 보다 명확하게 제시하는 것이 필요함을 제시하였기 때문에, 보안정책 관련 목표 수립 및 이행 전략 수립 시 활용 방향을 제시한다. 즉, 보안 정책 목표가 조직원들에게 현재 수준보다 달성하기 어려운 수준으로 제시가 되어야 하지만, 달성하기 위한 세부적인 절차를 목표에서 제시하는 것이 필요하다.

본 연구는 몇 가지 측면에서 연구의 한계점이 있으며, 향후 추가적 연구를 통해 보완될 필요성이 있다. 첫째, 연구에 활용된 요인인 조직의 목표 설정과 공정성, 조직원들의 준수도의간의 관계를 설명하기 위하여, 조직원들의 조직에 대한 인식 수준을 기반으로 측정하였다. 즉 결과는 조직의 보안 목표 및 공정성 수준을 명확하게 측정하지 못하였다는 한계를 가진다. 향후 연구에서는 보안 목표 수준을 보다 명확한 기준으로 분류하여 준수행동에 미치는 영향관계를 파악한다면, 조직원의 행동을 알 수 있는 중요한 연구가 될 것으로 판단된다. 둘째, 결과변수로서 조직원의 준수도의를 파악하였다. 물론, 준수도의가 행동으로 이어지는 핵심 요인임은 명확하지만, 준수도의가 행동으로 이어지는 영향관계 및 행동 수준을 높이기 위한 선행연구를 기반으로 추가적 연구를 한다면, 실무적 시사점을 높일 수 있을 것으로 판단된다. 셋째, 설문 대상은 정보보안 정책을 도입한 기업의 일반 근로자를 대상으로 하였다. 정보보안 목표 및 관련 규정은 업종별,

직무별 차이가 발생한다. 예를 들어, 영업 부서와 일반 내근직 부서의 보안 행동의 차이가 발생한다. 이러한 역할의 차이는 보안 행동에 대한 인식의 차이를 가지고 올 것으로 판단된다. 향후 산업 및 직무별 특성을 반영한 정보보안 연구가 실행되고, 정보보안 관련 교육을 실시 전, 후의 통계 분석을 실행한다면, 정보보안 인식관점에서의 높은 수준의 시사점을 제시할 수 있을 것으로 판단된다.

REFERENCES

- [1] IDC. (2016). Worldwide semiannual security spending guide.
- [2] K. D. Loch, H. H. Carr & M. E. Warkentin. (1992). Threats to information systems: today's reality, yesterday's understanding, *MIS Quarterly*, 16(2), 173-186.
- [3] Verizon. (2017). 2017 data breach investigations report.
- [4] I. Hwang & D. Kim. (2016). The effect of organizational information security environment on the compliance intention of employee, *The Journal of Information Systems*, 25(2), 51-77.
- [5] D. Kim, I. Hwang & J. Kim. (2016). A study on employee's compliance behavior towards information security policy: A modified triandis model, *Journal of Digital Convergence*, 14(4), 209-220.
- [6] I. Hwang, D. Kim, T. Kim & S. Kim. (2017). Why not comply with information security? An empirical approach for the causes of non-compliance, *Online Information Review*, 41(1), 1-17.
- [7] J. D'Arcy, A. Hovav & D. Galletta. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach, *Information Systems Research*, 20(1), 79-98.
- [8] T. Herath & H. R. Rao. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness, *Decision Support Systems*, 47(2), 154-165.
- [9] B. Bulgurcu, H. Cavusoglu & I. Benbasat. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness, *MIS Quarterly*, 34(3), 523-548.
- [10] M. Siponen, S. Pahlila & M. A. Mahmood. (2010). Compliance with information security policies: An empirical investigation. *Computer*, 43(2), 64-71.
- [11] Q. Hu, Z. Xu, T. Dinev & H. Ling. (2011). Does

- deterrence work in reducing information security policy abuse by employees?, *Communications of the ACM*, 54(6), 54-60.
- [12] Y. Chen, K. Ramamurthy & K. W. Wen. (2012). Organizations' information security policy compliance: Stick or carrot approach?, *Journal of Management Information Systems*, 29(3), 157-188.
- [13] C. Park & M. Yim. (2012). An understanding of impact of security countermeasures on persistent policy compliance. *Journal of Digital Convergence*, 10(4), 23-35.
- [14] A. Vance, M. Siponen & S. Pahlila. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory, *Information & Management*, 49(3), 190-198.
- [15] I. Hwang & Y. Lee. (2016). The employee's information security policy compliance intention: Theory of planned behavior, goal setting theory, and deterrence theory applied, *Journal of Digital Convergence*, 14(7), 155-166.
- [16] R. H. Moorman. (1991). Relationship between organizational justice and organizational citizenship behaviors: Do fairness perceptions influence employee citizenship?, *Journal of Applied Psychology*, 76(6), 845-855.
- [17] J. A. Colquitt. (2001). On the dimensionality of organizational justice: a construct validation of a measure. *Journal of Applied Psychology*, 86(3), 386-400.
- [18] M. T. Tsai & N. C. Cheng. (2012). Understanding knowledge sharing between IT professionals - an integration of social cognitive and social exchange theory. *Behaviour & Information Technology*, 31(11), 1069-1080.
- [19] Y. Zhang, J. A. LePine, B. R. Buckman & F. Wei. (2014). It's not fair... or is it? The role of justice and leadership in explaining work stressor - job performance relationships. *Academy of Management Journal*, 57(3), 675-697.
- [20] R. West. (2008). The psychology of security. *Communications of the ACM*, 51(4), 34-40.
- [21] M. S. Yim. (2012). A path way to increase the intention to comply with information security policy of employees. *Journal of Digital Convergence*, 10(10), 119-128.
- [22] A. Vance, M. Siponen & S. Pahlila. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory, *Information & Management*, 49(3), 190-198.
- [23] P. M. Muchinsky. (2006). *Psychology applied to work: An introduction to industrial and organizational psychology*. Cengage Learning.
- [24] P. E. Spector. (2009). *Industrial and organizational psychology*. Research and Practice.
- [25] T. A. Judge & J. A. Colquitt. (2004). Organizational justice and stress: the mediating role of work-family conflict. *Journal of Applied Psychology*, 89(3), 395-404.
- [26] H. Li, R. Sarathy, J. Zhang & X. Luo. (2014). Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance. *Information Systems Journal*, 24(6), 479-502.
- [27] Z. Ouyang, J. Sang, P. Li, P & J. Peng. (2015). Organizational justice and job insecurity as mediators of the effect of emotional intelligence on job satisfaction: A study from China. *Personality and Individual Differences*, 76, 147-152.
- [28] C. B. Meyer. (2001). Allocation processes in mergers and acquisitions: An organizational justice perspective. *British Journal of Management*, 12(1), 47-66.
- [29] S. W. Hystad, K. J. Mearns & J. Eid. (2014). Moral disengagement as a mechanism between perceptions of organisational injustice and deviant work behaviours. *Safety Science*, 68, 138-145.
- [30] J. Y. Son & J. Park. (2016). Procedural justice to enhance compliance with non-work-related computing (NWRC) rules: Its determinants and interaction with privacy concerns. *International Journal of Information Management*, 36(3), 309-321.
- [31] H. Zhang & N. C. Agarwal. (2009). The mediating roles of organizational justice on the relationships between HR practices and workplace outcomes: an investigation in China. *The International Journal of Human Resource Management*, 20(3), 676-693.
- [32] E. A. Locke & G. P. Latham. (2006). New directions in goal-setting theory. *Current Directions in Psychological Science*, 15(5), 265-268.
- [33] E. A. Locke & G. P. Latham (2002). Building a practically useful theory of goal setting and task motivation: A 35-year odyssey. *American Psychologist*, 57(9), 705-717.
- [34] B. E. Wright & B. S. Davis. (2003). Job satisfaction in the public sector: The role of the work environment. *The American Review of Public Administration*, 33(1), 70-90.
- [35] B. E. Wright. (2004). The role of work context in work motivation: A public sector application of goal and social cognitive theories. *Journal of Public Administration Research and Theory*, 14(1), 59-78.
- [36] J. M. Diefendorff & G. A. Seaton, G. A. (2015). *Work*

motivation. International encyclopedia of the social & behavioral sciences, 2nd edn. Elsevier, Oxford, pp.680-686.

- [37] C. C. Pinder. (1998). *Work motivation in organizational behavior*, Upper Saddle River, NJ: Prentice Hall.
- [38] E. A. Locke & G. P. Latham. (1990). Work motivation and satisfaction: Light at the end of the tunnel. *Psychological Science*, 1(4), 240-246.
- [39] A. B. Ruighaver, S. B. Maynard & S. Chang. (2007). Organisational security culture: Extending the end-user perspective. *Computers & Security*, 26(1), 56-62.
- [40] I. Koskosas. (2008). Goal setting and trust in a security management context. *Information Security Journal: A Global Perspective*, 17(3), 151-161.
- [41] A. Li & A. B. Butler. (2004). The effects of participation in goal setting and goal rationales on goal commitment: An exploration of justice mediators. *Journal of Business and Psychology*, 19(1), 37-51.
- [42] Y. Chen, K. Ramamurthy, & K. W. Wen. (2012). Organizations' information security policy compliance: Stick or carrot approach?. *Journal of Management Information Systems*, 29(3), 157-188.
- [43] J. C. Nunnally. (1978). *Psychometric theory* (2nd ed.). New York: McGraw-Hill.
- [44] B. H. Wixom & H. J. Watson. (2001). An empirical investigation of the factors affecting data warehousing success. *MIS Quarterly*, 25(1), 17-41.
- [45] C. Fornell & D. F. Larcker. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, 18(1), 39-50.
- [46] P. M. Podsakoff, S. B. MacKenzie, J. Y. Lee & N. P. Podsakoff. (2003). Common method biases in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, 88(5), 879-903.
- [48] L. J. Williams & S. E. Anderson. (1994). An alternative approach to method effects by using latent-variable models: Applications in organizational behavior research. *Journal of Applied Psychology*, 79(3), 323-331.

황 인 호(Hwang, In Ho)

[정회원]



- 2004년 8월 : 건국대학교 경영학과 (경영학사)
- 2007년 6월 : 중앙대학교 경영학과 (경영학석사)
- 2014년 2월 : 중앙대학교 경영학과 (경영학박사)

- 2014년 3월 ~ 현재 : (사)한국창업경영연구원 정보전략 연구팀장
- 관심분야 : IT 핵심성공요인, 디지털 콘텐츠, 정보보안 및 프라이버시 분야 등
- E-Mail : hwanginho@nate.com

김 승 옥(Kim, Seung Wook)

[정회원]



- 2003년 2월 : 중앙대학교 경영학과 (경영학박사)
- 1991년 5월 ~ 1996년 4월 : 연세대학교 경영연구소 선임연구원
- 1996년 11월 ~ 2000년 3월 : 안건 회계법인(Deloitte Touche

Tohmatsu Limited) 경영 컨설턴트

- 2000년 11월 ~ 2003년 2월 : SAP Korea, Digital Business Service 정보기술 컨설턴트
- 2017년 2월 ~ 2017년 12월 : 한국뉴욕주립대학교 (SUNY Korea) 경영학과 방문교수
- 2003년 3월 ~ 현재 : 평택대학교 경영학과 교수
- 관심분야 : 빅데이터 분석, 정보보안, 핀테크, 기술경영 등
- E-Mail : swkim@ptu.ac.kr