Journal of Digital Convergence
Vol. 16. No. 3, pp. 225-236, 2018

ISSN 1738-1916
https://doi.org/10.14400/JDC.2018.16.3.225

조직원의 정보보안 정책 준수의도에 미치는 영향 연구: 계획된 행동이론, 공정성이론, 동기이론의 적용

황인호[1], 허성호[2*]
[1]중앙대학교 지식경영학부, [2]중앙대학교 심리학과

A Study on the Influence of Information Security Compliance Intention of Employee: Theory of Planned Behavior, Justice Theory, and Motivation Theory Applied

In-Ho Hwang[1], Sung-Ho Hu[2*]
[1]School of Knowledge-Based Management, Chung-Ang University
[2]Department of Psychology, Chung-Ang University

요 약 조직은 정보 보안 기술에 대한 지속적인 투자를 통하여 다른 기업들보다 정보자원에 대한 경쟁력을 높이고 있다. 그러나 정보보안 기술 및 정책을 실행에 옮기는 조직원의 정보보안에 대한 관심이 상대적으로 저조하다. 본 연구는 정보보안 분야에 계획된 행동이론, 공정성이론, 그리고 동기이론을 적용하여 조직원의 정보보안 준수의도를 높이기 위한 메커니즘을 찾는다. 연구대상은 정보보안 정책을 도입한 조직의 조직원들이며, 서베이를 통하여 유효샘플 383개를 수집하였다. 연구가설 검증은 구조방정식 모델링을 실시하였다. 결과는 조직공정성, 외재적 동기(제재), 내재적 동기(조직일체화)가 계획된 행동이론의 세부 요인들에 영향을 주고 개인의 정보보안준수의도에 영향을 주는 것으로 나타났다. 분석 결과는 조직의 보안 정책에 대한 조직원들의 준수의도 향상을 위한 전략적 접근 방향을 제시한다.

주제어 : 정보보안 준수의도, 공정성이론, 계획된행동이론, 제재, 조직일체화

Abstract Organizations continue to invest in the security of information technology as a means to be more competitive than others in their industry do. However, there is a relatively lack of interest in the information security compliance of employees who implement information security technologies and policies of organization. This study finds mechanisms for enhancing security compliance by applying theory of planned behavior, justice theory, and motivation theory in information security field. We use structural equation modeling to verify the research hypotheses, and conducted a survey on the employees of organization with information security policy. The results showed that organizational justice, sanction, and organizational identification affect the factors of the planned behavior theory and affect the employee's compliance intention. As a result, this research suggested directions for strategic approach for enhancing employee's compliance intention on organization's security policy.

Key Words : Information Security Compliance Intention, Justice Theory, Theory of Planned Behavior, Sanction, Organizational Identification

*This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2017S1A5A8021221)
*Corresponding Author : Sungho Hu(powerrcy@daum.net)
Received January 24, 2018 Revised February 28, 2018
Accepted March 20, 2018 Published March 28, 2018

1. 서론

정보 관리가 조직의 중요한 이슈로 부각되면서, 많은 조직들은 정보 보호를 위한 기술 및 정책 도입을 위한 노력을 지속적으로 해오고 있다. IDC[2016]에 따르면 전 세계 정보보안 관련 기술 시장은 지속적으로 성장하고 있으며, 2020년에 101.6억 달러에 이를 것으로 판단되고 있다. 조직에서 투자하고자하는 정보보안 기술에는 디바이스 통제 기술, 네트워크 방화벽 기술, 네트워크 모니터링 기술, 문서 보호 기술, 그리고 보안 관리 기술 등이 다각적으로 제시되고 있다[2,3]. 이러한 기술들은 외부 침입을 사전에 차단함으로써, 자신들의 정보 자산을 보호하고자 하기 때문에, 전 세계 보안 사고의 60~70%를 형성하고 있는 외부의 침입에 의한 사고를 예방함에 있어 중요한 기술로서 평가받고 있다.

반면, 전 세계 정보보안 사고의 15~20%를 형성하고 있는 조직 내부 및 조직의 이해관계자들에 의한 보안 위협 노력은 상대적으로 저조하다[4-6]. 많은 기업들이 체계적인 정보 기술 및 정책을 도입한다면 중요 정보를 보호할 수 있을 것으로 판단하고 있으나, 실상은 조직원의 행동에 의해 정보보안이 유지되는 경우가 빈번하다[7,8]. 정보화 시대, 조직의 데이터를 활용하여 정보화하고 업무의 성과를 내는 부분은 조직의 일반적인 업무를 보고 있는 조직원들에 의해 발생한다. 즉, 정보 관리의 많은 부분이 일상적 업무 성과를 내야하는 조직원들에 의해 조정되고 관리되고 있다[9]. 따라서 조직에서 도입한 보안 정책 및 기술에 대한 체계적인 활용을 통한 보안 목표 수준을 달성하기 위해서는 조직 구성원들의 보안 관련 행동 준수가 무엇보다 중요하다[10].

조직원의 보안 준수와 관련된 선행 연구를 살펴보면, 사회학, 심리학, 범죄학 등에서 활용되던 중요 이론을 정보보안 분야에 접목시키는 연구가 대부분이다. 첫째, 정보보안 미준수 행동에 대한 억제적 관점에서, 미준수행동에 대한 명확하고 상세한 제재를 제시함으로써, 조직원의 보안 준수 행동을 높일 수 있다는 연구가 제시되고 있다[11-13]. 둘째, 억제와 같은 외적 동기 영역보다는 개인의 내적 동기를 개선함으로써, 장기적인 관점에서 능동적인 보안 행동을 추구할 수 있다고 본 동기 이론 관련 연구가 진행되어 왔다[14,15] 셋째, 개인의 의사결정은 관련 행동 준수에 대한 비용 및 혜택을 종합적으로 고려해서 판단하게 되기 때문에, 정보보안 준수행동 또한 보안 관련 준수에 따른 혜택 및 비용을 합리적으로 고려해서 접근한다는 합리적 선택이론 관련 연구가 진행되어 왔다[4]. 선행 연구들은 조직원들의 동기 형성이 조직에서 추구하는 특정 목표에 대한 수준 달성에 중요한 영향을 끼친다는 관점에서 중요한 시사점을 제시하고 있다. 하지만, 조직원의 보안 준수는 개인의 의사결정으로만 결정되는 것이 아닌 조직 문화 및 분위기 등 조직이 추구하고자 하는 조직적 관점에 의해서 영향을 많이 받는데 [16], 이러한 조직에서 개인에게 제시해야할 보안 행동 준수 개선 요인에 대한 연구는 상대적으로 부족한 면이 있다.

특히, 조직은 조직원에게 특정 행동 수준에 대한 목표를 제시하고 성과 달성을 독려하기 위한 노력을 하는데, 이중 공정성이 개인의 만족도 및 성과달성 수준을 높일 수 있는 중요한 요인이다[17,18]. 공정성 이론은 일찍부터 공정성 유형 및 유형별 관련 개인 및 조직의 성과, 그리고 부정적 행동을 감소시키는 중요한 선행 요인임을 제시하고 많은 연구가 진행되어 왔다. 하지만, 최근 중요성이 더욱 강조되고 있는 정보 자산에 대한 관리 영역인 정보보안 관점에서는 공정성이 조직원의 보안 준수에 어떠한 과정으로 영향을 미치고 행동 수준을 변화시키는지에 대한 연구가 미진하다. 즉, 정보보안 관점에서 조직의 공정성 수준이 조직원의 준수 관련 행동에 어떻게 영향을 미치는지에 대한 연구가 필요하다.

본 연구는 개인의 행동에 강력한 영향요인을 제시하는 계획된 행동이론(Theory of Planned Behavior)을 기반으로 조직의 보안 관련 공정 수준이 어떻게 개인의 보안 준수에 영향을 주는지를 파악하고자 한다. 더불어, 개인에게 형성되는 외적, 내적 동기가 계획된 행동이론과 연계되어 복합적으로 형성되는 보안 준수의도에 미치는 영향관계를 함께 검증하고자 한다. 즉, 개인의 보안 관련 행동을 설명하기 위하여 계획된 행동이론을 기반으로 조직의 공정성 수준과 개인에게 형성된 다양한 동기적 관점이 정보보안 준수에 미치는 영향 관계를 제시한다.

연구의 결과는 정보보안과 관련된 조직의 공정성 수준과 개인에게 형성된 동기가 개인의 보안 준수에 미치는 긍정적 효과를 체계적으로 설명할 수 있으며, 이에 따라 이론적 측면 및 실무적 측면에서의 시사점을 제시한다.

2. 이론적 배경

2.1 정보보안 준수의도

West[2008]는 조직과 조직원 사이에서의 보안 준수

관계는 대리인 문제를 형성한다고 보았다. 조직은 보안 관련 목표를 제시하고 있으며, 조직원에게 목표 수준에 이르기 위한 행동 수준을 요구한다. 하지만, 조직원이 보유한 행동의 정보는 조직보다 많기 때문에, 대리인 문제가 발생하게 되며, 이는 기술적으로 해결하기 어렵기 때문에, 정보보안은 심리적 문제로 해결해야한다고 보았다. Loch, Carr and Warkentin[1992]은 정보보안 위협 요인에 대한 프레임워크에서 조직 내부 및 인간에 의한 보안 위협이 지속적으로 문제가 될 것으로 보았으며, Verizon[2016]에서 제시하는 보안 관련 리포트에서 조직의 이해관계자들에 의한 보안 사고가 적지 않음을 증명하고 있다.

조직의 정보 노출 사고 중 내부자에 의한 보안 사고는 지속적으로 증가할 가능성이 높은데, 정보 기술의 발전은 조직원들에게 생산성 및 성과를 높이기 위한 정보시스템에 대한 접근을 용이하게 만들고, 접근 가능성의 높음은 정보 위협을 함께 높이기 때문이다 [22,23]. 더불어, 조직원들은 조직에서 제시한 업무 상 정보보안 관련 요구사항을 자신들의 행동에 적용할 것인지에 대한 합리적이고 감정적인 판단을 통해 정보보안 관련 행동을 수행하게 된다[4,24]. 즉, 정보보안 위협 최소화를 위해서는 조직원의 자발적인 정보보안 준수행동이 우선시되어야 하며, 보안 준수 행동 수준을 높이기 위한 개인의 동기 개선 및 조직 차원의 다양한 노력이 필요하다[25,26]. 따라서 연구는 정보보안 준수의도를 높이기 위하여 계획된 행동이론에서 제시하는 세부 요인을 활용하고, 정보보안 관련 공정성 수준과 개인에게 형성된 동기의 연관성을 제시함으로써 조직원의 정보보안 준수의도를 높이기 위한 방향을 제시하고자 한다.

2.2 계획된 행동이론

계획된 행동이론(Theory of Planned Behavior)은 인간의 행동 예측에 있어서 매우 높은 설명력을 제시하는 이론으로서, Ajzen[1991]이 합리적 선택이론(Theory of Reasoned Action)을 발전시켜 주관적 규범, 지각된 행동통제, 그리고 태도를 세부요인으로 적용시켜 설명력을 높인 이론이다. 즉, 계획된 행동이론은 개인이 자신의 행동에 대한 긍정적 유형의 태도를 가지고, 자신을 둘러싼 외부에서 제시하는 주관적인 규범에 대하여 긍정적 인식을 하고, 자신의 행동 수준이 통제 될 수 있다는 인식을 할 경우 관련 행동을 형성한다고 본다[28].

정보보안 영역에서 계획된 행동이론은 개인의 보안 준수의도를 형성시키는 이론으로서 중점적으로 활용되고 있으며, 연구자별로 각 변수들을 유사하게 보안 분야에 접목시킴으로써 활용하고 있다. Cox[2012]와 Safa, Sookhak, Von Solms, Furnell, Ghani and Herawan[2015]은 계획된 행동이론과 동기이론을 연결하여 사용자의 보안 행동을 설명하고자 하였으며, 태도, 주관적 규범, 인지된 행동 통제의 3요인을 선행요인으로 제시하였다. Bulgurcu et al.[2010]은 합리적 선택이론과 계획된 행동이론을 연계하여 조직원의 보안 준수의도를 설명하고자 하였으며, 태도, 준수관련 자기효능감, 규범적 믿음(Normative Beliefs)으로 제시하였다. Zhang, Reithel and Li[2009]는 인지된 보안 보호 매커니즘과 계획된행동이론을 연계하여 정보보안 행동을 설명하고자 하였으며, 그들은 계획된 행동이론 세부 요인으로 주관적 규범, 태도, 행동 통제를 제시하였다. 또한, Johnston and Warkentin[2010]은 보호동기이론을 정보보안 분야에 접목하여, 개인에 대한 공포 형성이 보안 준수에 미치는 영향을 설명하고자 하였다. 그들은 보안 준수를 설명하기 위하여 계획된 행동이론을 도입하였으며, 자기효능감, 대처효능감, 그리고 사회적 영향을 주요 요인으로 제시하였다.

본 연구는 계획된 행동이론의 세부 요인으로서, 태도, 자기효능감(인지된 행동 통제 요인), 그리고 사회적 영향(주관적 규범 요인)을 보안 분야에 적용하고 선행요인인 공정성과 동기와의 관련성을 제시하고자 한다.

사회적 영향은 사회적 또는 주관적 규범과 유사한 관점으로서, Johnston and Warkentin[2010]은 특정한 조직의 보안관련 사회적 상황에 따라 형성된 주관적 문화에 대한 개인의 내재화 정도로 정의하고 있다. Flores and Ekstedt[2016]과 Safa and Von Solms[2016]은 조직에서 제시하는 보안관련 규범은 보안 관련 의도 형성에 중요한 영향을 미치게 되는데, 조직에서 제시하는 조직의 문화 및 특성에 의하여 자체적으로 형성된 외부적 영향요인은 개인에게 동일시 할 수 있도록 유도하기 때문이라고 보았다.

태도는 개인의 과거와 현재의 경험에 기반으로 형성되며, 관련 대상에 대한 호의 또는 불만으로 정의된다[33]. 이러한 대상은 장소, 사람, 아이디어, 특정 사건과 같은 자신을 둘러싼 환경일 수 있다[28]. 정보보안 영역에서 개인의 보안과 관련된 과거 및 현재의 경험으로 인하여 발생한 태도는 조직원의 보안 준수의도에 긍정적인

영향을 미친다[34]. 즉, 개인을 둘러싼 조직의 보안 환경에 의해 개인은 호의 또는 불만을 가지게 되고, 이를 통해서 보안 준수에 영향을 주는 것을 의미한다.

자기효능감은 특정 목표에 대하여 달성할 수 있는 능력에 대하여 자체적인 평가 수준을 의미한다[31]. 자기효능감은 외부적 측면이 아닌 스스로의 관련 대상에 대하여 통제하고 행동할 수 있다는 평가 수준이기 때문에, 자기효능감이 높아지면, 관련 행동 수준을 높이고자 한다[4]. 특히 정보보안과 관련해서, 선행연구들은 스스로의 보안 행동관련 평가 수준 영역인 자기효능감이 보안 행동에 중요한 영향을 미치는 영향요인이라고 하였다[14,35,36].

즉, 계획된 행동이론의 세부 변수들인 사회적 영향, 태도, 그리고 자기효능감은 조직원의 정보보안 준수의도에 긍정적 영향을 미치는 선행 요인이며, 다음과 같은 연구가설을 제시한다.

H1 : 사회적 영향은 정보보안 준수의도에 정(+)의 영향을 미칠 것이다.

H2 : 태도는 정보보안 준수의도에 정(+)의 영향을 미칠 것이다.

H3 : 자기효능감은 준수의도에 정(+)의 영향을 미칠 것이다.

2.3 공정성 이론

공정성은 일찍이 사회학, 심리학 등 여러 학문에서 중점적으로 연구한 요인으로서, 조직 관점에서는 조직과 조직원간의 관계, 행동 개선 등의 성과 달성 관점에서 중점적으로 제시되고 있는 분야이다[37]. 조직공정성(Organizational Justice)은 조직구성원들에게 특정 행동에 대한 공정한 지원 및 대우와 연계된 이론적 개념이다[38]. 조직에서 공정성의 기본적인 가정은 조직 내 이해관계자들은 특정 행동 과정 및 결과를 평가함에 있어서 공정함에 많은 가치를 두며, 개인은 공정성을 기반으로 조직에서 행동을 한다고 본다[39]. 즉, 조직에서의 행동에 대한 조직 구성원들의 평가는 공정한 정보 제공, 상호작용, 절차, 성과의 수준에 대한 이해 및 판단을 통해서 이루어지게 된다[17].

공정성은 연구자별로 차이가 있지만, 분배공정성(Distribution Justice), 절차공정성(Procedural Justice), 상호작용공정성(Interactional Justice) 등으로 구분된다[17,18,40-42]. 즉, 특수한 활동에 대한 결과를 분배함에 있어 공정한 수준을 보여야 한다는 분배공정성, 결과를 성취하기 위한 수단에 대한 공정한 수준을 제시해야 한다는 절차공정성, 대상자와의 상호작용을 함에 있어 관련된 정보 제공 등의 행동이 공정해야한다는 상호작용공정성 등이 공정성을 구성하고 있으며, 조직은 통합적인 관점에서 공정한 문화를 만들고 제시해야한다고 본다.

Ambrose and Schminke[2009]는 조직원은 조직에서 제시하는 분배공정성, 절차공정성, 상호작용 공정성에 대하여 각각 다르게 고려하는 것이 아닌 전체적인 공정성 수준(Overall Justice)으로 인지한다고 보았으며, 이러한 공정성 수준을 높게 평가할수록 자신들의 직업 만족도, 조직 몰입 수준을 높게 평가함을 증명하였다.

조직공정성은 조직과의 관계에서 개인의 행동에 영향을 주는 요인이다. Chou, Seng-cho, Jiang and Klein[2013]은 조직공정성이 직업 몰입을 높여 조직 시민 행동 수준에 긍정적인 영향을 준다고 했으며, Demirtas[2015]는 개인이 조직공정성에 대한 수준이 높다고 판단할 경우 조직 목표에 반하는 행동을 감소시킨다는 것을 증명하였다. Yoon[2011]은 조직 공정성이 개인의 행동에 미치는 영향관계를 계획된 행동이론을 연계하여 적용하였으며, 공정성이 주관적 규범에 긍정적인 영향을 미치는 것을 증명하였다.

정보보안 영역에서 공정성은 정보보안 준수행동에 긍정적인 영향을 미칠 것으로 판단된다. 조직에서 제시하는 정보보안 정책은 조직구성원 모두가 동일하게 규정을 적용받아야한다. 즉 조직의 보안 규정은 정확하게 정보가 모든 사람들에게 제공되어야 하고, 관련 절차 및 미준수 행동에 대한 제재 및 준수행동에 대한 인센티브가 명확하게 제시되어야 한다. Hwang et al. [2017]은 정보보안 정책이 명확하고 체계적으로 조직원들에게 제시될 때, 정보보안 미준수원인을 감소시킬 수 있으며, 준수의도를 높일 수 있다고 하였다. 또한, Hwang and Lee[2016]는 보안 정책의 목표가 명확하게 조직원에게 전달될 때, 자기 통제수준을 높여 준수의도에 영향을 준다고 하였다. 즉, 정보보안 분야에서도, 조직공정성이 개인의 행동에 영향을 줄 것으로 판단하며, Yoon[2011]이 제시한 공정성이 주관적 규범에 미치는 영향 관계를 통하여 계획된 행동에 영향을 줄 것으로 판단하며, 다음과 같은 연구가설을 제시한다.

H4 : 정보보안관련 조직공정성은 사회적 영향에 정(+)의 영향을 미칠 것이다.

2.4 동기 이론

동기는 개인의 행동을 시작하고, 형태, 방향, 강도 및 지속 기간을 결정하는 힘의 집합으로서 행동의 에너지이며 행동을 지속적으로 유지시키는 원천이다[47]. 정보보안 분야에서의 여러 동기관련 연구들은 동기가 정보보안 기술 및 정책을 자신들의 업무에 적용함으로써, 조직에서 요구하는 수준의 보안 목표를 달성하고 준수행동을 유지하게 하는 중요한 선행요인임을 제시하고 있다[14,15,33].

동기는 외재적 동기와 내재적 동기로 구분된다. 외재적 동기는 외부로부터 보상을 얻으려는 것과 관련된 동기로서, 돈, 보너스 등과 같은 것이 있다. 내재적 동기는 외부의 보상과 관련 없이 주어진 과제를 하거나 활동하는 자체가 보상이 되는 동기이며, 성취감 등이 내재적 동기에 속한다[48].

조직과 조직원의 관계에서 외재적 동기는 전통적으로 조직원이 조직의 규정 및 규칙 등을 따르게 하는 행동 원천으로서 활용되어 왔다[15]. 정보보안은 조직원이 반드시 업무 과정에서 이행해야할 행동이기 때문에 일반적으로 규칙에 준수에 대한 제재(Sanction)를 강조한다[14,49]. 대부분의 조직들은 보안 정책 미준수에 대한 징계를 명확하게 제시하고 하고 있다[3]. 억제이론(Deterrence Theory)에 따르면, 확립되고 보다 엄격한 수준의 제재의 제시 및 조직원의 인식은 보안 미준수 행동을 억제하는 역할을 한다[26]. 반면, 조직의 제재에 대하여 조직원이 명확하게 인식하지 못할 때, 조직원들은 조직의 정보보안 정책을 이행하지 않는다[13]. 따라서 제재와 같은 외재적 동기를 조직원에게 정확하게 전달하고 이해시킴으로써, 정보보안 준수행동의 필요성을 강조하는 것이 필요하다.

내재적 동기는 개인들이 각기 다르게 보유하고 있는 도덕적 믿음, 조직 일체화 수준의 차이에 의해 조직의 규정을 따르는 것의 차이가 발생한다는 관점이다. Bulgrucu et al[2010]은 정보보안 정책을 준수하는 것에 대하여 조직원이 판단하는 내재적 혜택은 긍정적 정보보안 준수 태도를 결정하는데 중요한 원천이 된다고 하였으며, Son[2011]은 조직의 정보보안 정책에 대한 조직원의 지속적 보안 행동은 제재를 기반으로 하는 외재적 동기뿐 아니라 가치를 기반으로 한 내재적 동기가 중요한 역할을 하는 것을 증명하였다. Li, Zhang, and Sarathy[2011]은 조직 일체화(Organizational Identification)가 보안 관련 개인의 규범을 형성하고, 인터넷 사용 정책 준수의도에 긍정적인 영향을 미친다고 하였다. 조직 일체화는 조직의 특성에 대하여 연결하고자 하는 자신만의 심리적 형태로 정의되며[51], 조직 일체화는 구성원으로서 애착, 소속감, 자부심을 보유하게 함으로써, 조직과 강력한 관계를 맺고자하고 조직의 관점에서 생각하는 경향이다[50].

외재적 동기인 제재와 내재적 동기인 조직일체화는 정보보안 준수에 긍정적인 영향을 미치며, Guo et al.[2011]는 외재적 동기가 태도에 영향을 주고 Safa and Von Solms[2016]은 외재적 동기와 내재적 동기가 계획된 행동에 영향을 줌에 있어 태도에 연관관계가 있음을 증명하였다. 즉, 조직원의 제재와 조직 일체화가 계획된 행동 이론의 구성요인인 태도에 긍정적인 영향을 미칠 것으로 판단하며, 다음과 같은 연구가설을 제시한다.

H5 : 제재는 태도에 정(+)의 영향을 미칠 것이다.

H6 : 조직일체화는 태도에 정(+)의 영향을 미칠 것이다.

3. 연구 모델 및 방법

3.1 연구 모델

본 연구는 보안 관련 조직의 공정성과 동기가 조직원의 보안 준수에 미치는 영향관계를 파악하기 위함이다. 세부적으로, 계획된 행동 관점에서 보안 관련 조직 공정성, 제재 그리고 조직 일체화가 보안 관련 계획된 행동에 미치는 일련의 절차를 파악함으로써, 조직원의 보안 준수의도를 높이기 위한 방향을 제시하고자 하며, 연구 목적에 맞는 연구 모델을 제시한다(Fig. 1 참조).

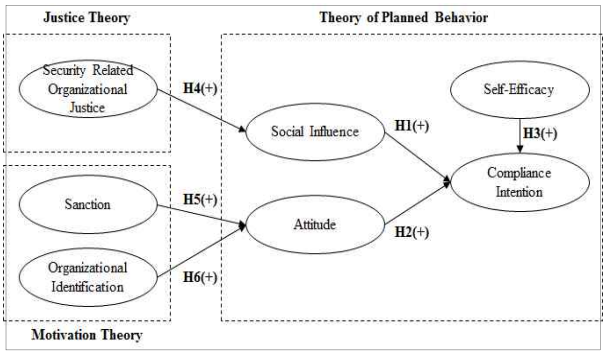

Fig. 1. Research Model and Proposed Hypotheses

Table 1. Questionnaire

Constructs	Items		Source
Organizational Justice	OJu1	Overall, I have been fairly treated by the organization in relation to information security.	[43]
	OJu2	In general, I can believe that our organization is fair in relation to information security.	
	OJu3	In general, our organization's information security-related activities are fair.	
	OJu4	In relation to information security, our organization treats its members fairly.	
Sanction	San1	My employer strictly enforces sanction for security non-compliance behaviors with employees.	[13]
	San2	I am likely to incur sanctions if I violate information security policy.	
	San3	My employer explicitly communicates that sanctions will follow if information security policy is violated.	
Organizational Identification	Old1	I am proud to be an employee of my organization.	[50]
	Old2	I am glad I chose to work for my organization rather than another company.	
	Old3	I am willing to put in a great deal of effort beyond that normally expected to help my organization to be successful.	
Self-Efficacy	SE1	I could comply with information security..	[4]
	SE2	SE1: If there was no one around to tell me what to do as I go.	
	SE3	SE2: If I could call someone for help if I got stuck.	
	SE4	SE3: If I had a lot of time to complete the job for which the software was provided. (Drop)	
		SE4: If I had just the built-in help facility for assistance.	
Social Influence	SI1	People who influence my behavior think that I should comply with information security.	[31]
	SI2	People who are important to me think that I should comply with information security.	
	SI3	The security management of this business has been helpful in the compliance of information security.	
	SI4	In general, the organization has supported the compliance of information security.	
Attitude	Att1	Adopting security technologies and practices is important.	[14]
	Att2	Adopting security technologies and practices is beneficial.	
	Att3	Adopting security technologies and practices is helpful.	
Compliance Intention	CI1	It is possible that I will follow information security policies.	[10]
	CI2	It is probable that I will follow information security policies.	
	CI3	I am likely to follow information security policies.	
	CI4	I am certain that I will follow information security policies (Drop).	

3.2 데이터 측정 방법 및 수집

본 연구는 구조방정식모델링을 기반으로 연구 모델을 검증하고자 한다. 구조방정식모델링은 사회학 등의 확인적 요인분석과 경로분석이 결합된 방법론으로서, 특정 분야에 대한 이론을 기초로 연구자가 사전에 수립한 모델에 대한 검증을 수행한다. 본 연구는 정보보안 분야에 기존의 공정성이론 및 동기이론, 그리고 계획된 행동이론을 적용하여, 보다 명확한 조직원 보안 준수의도 원인을 찾는 인관관계를 증명하고자 본 기법을 적용한다. 이에, 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 7개 변수의 측정항목들은 총 25개이며 Table 1과 같다.

본 연구는 조직원의 정보보안 준수의도를 높이기 위한 방향을 제시하고자 한다. 연구 가설 검증 결과의 시사점을 높이기 위하여, 정보보안 정책을 엄격하게 적용하고 있는 대기업 및 금융기업에서 근무하는 조직원들을 대상으로 하고자 한다. 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 하였다.

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

이중 정보보안 정책을 보유한 사람들만 설문을 하도록 하였다. 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.

4. 가설 검증

4.1 신뢰성 및 타당성 분석

본 연구는 신뢰성과 타당성 검증을 통하여 연구 모델의 적정성을 검증한다. 첫째, 모델의 신뢰성 분석을 테스트하기 위하여 SPSS 21.0을 이용하여 Cronbach's alpha를 측정한다. Cronbach's Alpha는 0.7이상[52]을 요구하며, 분석 결과 총 25개의 설문항목 중 문제가 있는 2개 항목(SE3, CI4)을 제외한 23개를 분석에 활용하였다. Cronbach's alpha가 가장 낮은 변수인 자기효능감이 0.899로 나타나 적합한 것으로 나타났다(Table 3 참조).

Table 3. Result for Construct Validity and Reliability

Construct	Item	Factor Loading	Cronbach's Alpha	CR	AVE
Organizational Justice	OJu1 OJu2 OJu3 OJu4	.801 .791 .808 .803	0.943	0.910	0.717
Sanction	San1 San2 San3	.815 .808 .768	0.932	0.881	0.711
Organizational Identification	OId1 OId2 OId3	.833 .881 .834	0.938	0.911	0.772
Social Influence	SI1 SI2 SI3 SI4	.813 .846 .822 .823	0.926	0.898	0.689
Attitude	Att1 Att2 Att3	.789 .856 .837	0.915	0.884	0.718
Self-Efficacy	SE1 SE2 SE4	.856 .843 .824	0.899	0.852	0.658
Compliance Intention	CI1 CI2 CI3	.707 .708 .677	0.950	0.924	0.802

그리고 타당성 분석은 개념신뢰도(Construct Reliability: CR)와 평균분산추출(Average Variance Extracted: AVE)을 실시하며, CR의 기준은 0.8, AVE의 기준은 0.5을 요구한다 [53,54]. 분석결과 확인적요인분석의 적합도는 권장치에 부합하는 것으로 나타났으며(χ^2/df = 1.501, GFI = 0.938, AGFI = 0.917, CFI = 0.988, NFI = 0.966, RMSEA = 0.036), 신뢰성 및 타당성 모두 요구 기준에 적합한 것으로 나타났다(Table 3 참조). 추가적으로 판별타당성 분석을 실시하였으며, AVE의 제곱근 값이 변수들의 상관계수 값보다 큰 것으로 나타나[54], 판별타당성이 있는 것으로 나타났다(Table 4 참조).

Table 4. Result for Discriminant Validity

Constructs	1	2	3	4	5	6	
Organizational Justice	**0.847**						
Sanction	.632**	**0.843**					
Organizational Identification	.566**	.479**	**0.879**				
Social Influence	.550**	.553**	.456**	**0.848**			
Attitude	.517**	.523**	.483**	.453**	**0.811**		
Self-Efficacy	.377**	.408**	.342**	.363**	.419**	**0.811**	
Compliance Intention	.694**	.668**	.617**	.588**	.587**	.523**	**0.895**

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(χ^2/df = 2.116, GFI = 0.908, AGFI = 0.883, CFI = 0.972, NFI = 0.948, RMSEA = 0.05).

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

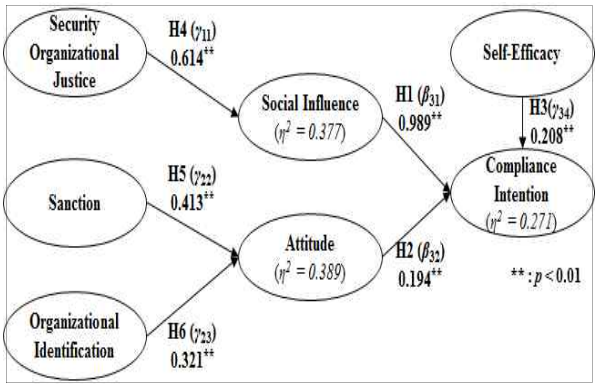

Fig. 2. Results of the Structural Model

Table 5. Summary of Hypothesis Tests

	Path	Coefficient	t-value	Results
H1	SI → CI	0.989**	10.328	Support
H2	Att → CI	0.194**	4.418	Support
H3	SE → CI	0.208**	5.269	Support
H4	OJ → SI	0.614**	11.841	Support
H5	San → Att	0.413**	7.882	Support
H6	Old → Att	0.321**	6.238	Support

**: $p < 0.01$
OJ(Organizational Justice), San(Sanction), Old(Organizational Identification), SI(Social Influence), Att(Attitude), SE(Self Efficacy), CI(Compliance Intention)

분석 결과 사회적 영향, 태도, 그리고 자기효능감이 정보보안 준수의도에 정(+)의 영향을 미칠 것이라는 가설 H1, H2, H3을 분석한 결과 변수간의 긍정적 영향관계가 있는 것으로 나타났다(H1: β_{31}= 10.328, p<0.01, H2: β_{32}= 4.418, p<0.01, H3: γ_{34}= 5.269, p<0.01). 이러한 결과는 계획된 행동이론이 정보보안 분야에 적용되어 행동을 예측할 수 있으며, 정보보안과 관련하여 사회적 영향, 태도, 그리고 자기효능감이 행동에 긍정적인 영향을 증명한 선행연구[4,30,31]와 같은 결과이다. 즉, 정보보안 영역에서 개인의 정보보안 준수 행동은 개인을 둘러싼 외부적 환경에 대한 인식, 자신의 태도 형성, 행동 통제 수준을 판단하여 결정된다는 점이다. 첫째, 조직원의 정보보안 준수는 개인을 둘러싼 외적 환경 요인에 의하여 영향을 받기 때문에, 조직은 적정하게 보안 준수 규범을 제시함으로써 개인이 이해할 수 있도록 유도하는 것이 필요하다. 둘째, 개인이 정보보안에 대한 긍정적 태도를 형성할 수 있도록 지원하는 것이 필요하다. 셋째, 자신이 정보보안 준수에 대한 통제를 할 수 있음을 인식하는 것이 필요하다. 즉, 사회적영향, 태도, 자기효능감이 높아질수록 조직원의 정보보안 준수의도는 높아진다.

공정성이 사회적 영향에 정(+)의 영향을 미칠 것이라는 가설 H4를 분석한 결과 두 변수간의 긍정적 영향관계가 있는 것으로 나타났다(γ_{11}= 11.841, p<0.01). 이러한 결과는 조직과 조직원의 관계에서 조직이 제시하는 공정성 수준이 계획된 행동이론 중 사회적 영향에 영향을 미친다는 선행연구[46]와 같은 결과이다. 즉, 정보보안과 관련하여 조직의 공정성은 다양한 부분에서 발생하며, 조직원들은 통합적으로 공정성을 이해한다. 정보보안 성과에 대한 명확한 분배, 관련 절차 수준의 체계적 이행, 그리고 보안 관련 정보의 제공 및 커뮤니케이션 활동은 정보보안 공정성 인식 수준을 높이게 되며, 계획된 행동이론 세부 요인 중 사회적 영향에 긍정적인 영향을 미치게 된다. 즉, 개인을 둘러싼 보안 관련 외적 요인 중 공정성이 중요한 요인이기 때문에, 조직은 공정성 수준을 높이고 있음을 제시할 필요가 있다.

외재적 동기인 제재가 태도에 정(+)의 영향을 미칠 것이라는 가설 H5를 분석한 결과 두 변수간의 긍정적 영향관계가 있는 것으로 나타났다(γ_{22}= 7.882, p<0.01). 이러한 결과는 조직의 정책 준수에 있어 행동에 대한 제재 수준이 조직원의 행동 태도에 영향을 미친다는 선행연구[14,15,33]와 같은 결과이다. 즉, 정보보안은 조직원이 반드시 업무 수행과정에서 행동으로 옮겨야하는 필수 행동 조건이기 때문에, 미준수에 따른 제재가 어떻게 영향을 주는지를 이해시키는 것이 필요하다. 연구는 제재가 태도에 영향을 주는 것을 검증하였다. 즉 보안 관련 제재는 개인의 계획된 행동을 형성하는 요인 중 태도를 형성시켜 준수의도를 높일 수 있음을 제시한다. 내재적 동기인 조직 일체화가 태도에 정(+)의 영향을 미칠 것이라는 가설 H6를 분석한 결과 두 변수간의 긍정적 영향관계가 있는 것으로 나타났다(γ_{23}= 6.238, p<0.01). 이러한 결과는 조직의 정책 준수에 있어 행동에 대한 내재적 동기가 조직원의 행동 태도에 영향을 미친다는 선행연구[14,15,33]와 같은 결과이다. 즉, 개인이 조직에 대하여 각자 다르게 판단하는 내재적 동기 중 조직과 일치하고자 하는 성향 수준이 높아지면 보안 관련 조직의 요구 수준을 달성하고자 하는 경향이 있다. 특히 계획된 행동이론 중 태도에 긍정적인 영향을 미침을 증명하였기 때문에, 내재적 동기가 개인의 정보보안 관련 태도를 형성하여 준수의도에 긍정적인 영향을 미칠 수 있음을 제시한다.

마지막으로, 내생변수의 결정 계수를 도출하였다. 준수의도는 사회적 영향, 태도, 자기효능감의 27.1%의 설명력을 가지고 있는 것으로 나타났으며, 사회적 영향은 조직 공정성의 37.7%의 설명력을 가지고 있는 것으로 나타났다. 태도는 제재와 조직일체화의 38.9%의 설명력을 가지고 있는 것으로 나타났다.

5. 결론

본 연구는 조직원의 정보보안 준수의도를 설명하는 이론인 계획된 행동이론을 중심으로 조직원의 정보보안 준수의도 향상을 위한 방향을 제시한다. 세부적으로 정

보보안 준수의도를 설명하기 위하여 계획된 행동이론의 세부 요인인 사회적 영향, 태도, 그리고 자기효능감이 정보보안 준수에 영향을 주는지를 파악하고자 하였으며, 정보보안 관련 조직의 전반적인 공정성 수준이 계획된 행동 요인 중 사회적 영향에 영향을 미침으로써 준수의도로 연계되는지를 파악하고자 하였다. 그리고 정보보안 관련 동기(외재적, 내재적)가 태도에 긍정적인 영향을 미침으로써 준수의도로 연계되는지를 파악하고자 하였다. 이를 위하여 정보보안 정책을 엄격하게 도입하고 있는 국내 대기업 및 은행권에 종사하고 있는 일반적인 업무를 수행하고 있는 조직원들을 대상으로 설문을 실시하였으며, 구조방정식모델링을 통한 가설 검증을 실시하였다.

연구 결과는 다음과 같은 이론적, 실무적 관점에서의 시사점을 가진다. 첫째, 연구는 조직원의 정보보안 준수 행동을 높이기 위하여 개인의 행동에 대한 높은 설명력을 가진 계획된 행동이론을 기반으로 준수의도에 영향을 미치는 요인들을 제시하였다. 이론적 관점에서 계획된 행동이론의 세부 요인(사회적 영향, 태도, 자기효능감)이 정보보안 준수의도에 긍정적인 영향 관계에 있음을 증명하였다. 즉 정보보안 연구적 영역에서 계획된 행동이론이 조직원의 정보보안과 관련된 행동에 높은 설명력을 지님을 제시하였다. 실무적 관점에서 정보가 기업의 중요한 가치로 인식되고, 정보시스템에 접근하기가 용이해지면서 정보관리의 중요성은 더욱 커지고 있다. 하지만 정보 보호를 실행에 옮겨야하는 조직원의 보안 준수와 관련된 실행적 접근은 아직 미진하였다. 이에 계획된 행동이론의 중요요인들인 사회적 영향, 태도, 자기효능감이 준수의도에 긍정적 영향을 미침을 증명하였기 때문에, 조직원들의 자발적인 정보보안 준수의지를 가지도록 유도하기 위한 전략적 관점의 실무적 시사점을 제시한다.

둘째, 연구는 정보보안 분야에 공정성 이론을 적용하여 개인의 보안 준수에 어떤 과정으로 영향을 미치는지를 검증하였다. 이론적 관점에서 조직과 조직원의 관계에 있어 높은 설명력을 가진 조직공정성을 정보보안 분야에 적용시켰을 뿐 아니라, 조직에서 제시하는 공정성이 계획된 행동이론 중 사회적 영향에 긍정적인 영향 관계에 있음을 검증하였다. 즉, 정보보안 관련 연구 관점에서 정보보안 관련 공정성이 개인의 계획된 행동을 결정함에 있어 중요한 선행 요인임을 제시하였기 때문에, 향후 조직원의 보안 준수 관련 연구에 기반이 될 것으로 판단한다. 실무적 관점에서 조직이 조직원에게 제시해야할 외부적 요인 중 공정성이 중요함을 검증하였다. 정보보안 분야에서의 공정성은 다양한 관점에서 제시된다. 보안 행동에 대한 결과 제시의 공정함, 보안 준수 절차에 대한 공정함. 그리고 조직과 조직원간의 상호작용의 공정함은 통합적인 공정함으로 인식되고 형성된 공정성은 사회적 영향에 높은 긍정적 영향을 미친다. 따라서 조직은 정보보안 기술 및 정책을 막연히 실행에 옮기도록 강조하는 것이 아닌 공정한 보안 준수 체계를 갖추었음을 제시하는 것이 필요하다.

셋째, 연구는 정보보안 관련 동기 이론을 적용하여 개인의 보안 관련 행동 준수에 미치는 영향 관계를 증명하였다. 이론적 관점에서 개인에게 형성된 외재적 동기(제재)와 내재적 동기(조직일체화)가 계획된 행동 이론의 세부요인 중 태도에 긍정적 영향을 미치는 것을 검증하였다. 즉, 정보보안 준수 행동을 유도하는 것은 개인의 동기 형성이 매우 중요한데, 계획된 행동과 관련하여 영향관계가 있음을 증명하였기 때문에, 향후 보안 관련 동기 및 행동과의 연관관계를 찾고자하는 연구의 기반이 될 것으로 판단한다. 실무적 관점에서 조직은 조직원의 정보보안 준수 행동 수준을 높이기 위하여 정책 미준수에 대한 억제 관점에서 접근을 하고자 한다. 개인의 동기는 외재적 동기 뿐 아니라 내재적 동기 형성이 무엇보다 중요한 요인이다. 즉, 조직은 조직원이 내재적 동기 형성을 할 수 있도록 지원하는 것이 필요함을 제시하였으며, 이중 조직일체화 관점에서의 내재적 동기가 개인의 보안 관련 태도 형성에 긍정적 영향관계가 있음을 증명하였다. 따라서 조직은 제재와 같은 외재적 동기 형성과 더불어 조직일체화와 같은 내재적 동기 형성을 위한 노력이 필요함을 제시한다.

본 연구는 몇 가지 측면에서의 연구의 한계점이 있으며, 향후 추가적 연구를 통해 보완될 필요성이 있다. 첫째, 본 연구는 조직원의 정보보안 준수를 설명하기 위하여 계획된 행동이론, 공정성이론, 동기이론을 기반으로 연구 모델 및 가설을 설정하였으며, 가설검증을 하고자 하였다. 설문은 조직원의 조직에 대한 인식 및 현재의 동기 수준, 그리고 준수의도 등 인식 수준을 기반으로 측정하였다. 즉, 결과는 조직 차원의 공정성 수준을 명확하게 측정하지 못하였다는 한계를 가진다. 향후 연구에서는 보안 관련 공정성 수준을 명확하게 측정하기 위한 도구를 개발 및 측정하는 것이 필요하다. 둘째, 본 연구는 보안 관련 행동을 측정한 것이 아니라 준수의도를 측정하

였다. 물론 준수의도가 행동으로 연결되는 중요 요인임은 명확하지만, 실제 행동 수준을 높이기 위한 실험관점의 연구를 추가적으로 진행한다면, 실무적 관점에서의 명확한 시사점을 제시할 수 있을 것으로 판단한다. 셋째, 본 연구의 설문 대상은 정보보안 정책을 보유한 기업에서 근무하는 일반 업무를 수행하는 조직원이다. 정보보안 관련 공정성 수준은 업종과 직무별로 차이가 발생할 것으로 판단된다. 예를 들어 영업 부서의 조직원은 정보보안 보다 실무적 성과가 더욱 중요할 것으로 판단할 수 있으며, 이에 따라 정보보안을 보다 덜 중요하게 여길 가능성이 존재한다. 반면, IT 부서의 조직원은 정보 관리의 중요성을 인식하고 있을 것으로 판단한다. 이러한 조직내 역할의 차이는 보안 행동에 대한 인식 차이를 가지고 올 것으로 판단되기 때문에, 향후 업종별 직무별 특성을 함께 고려하여 정보보안 연구가 실행된다면, 분야별 정보보안에 대한 인식 및 대응 방법을 제시함으로써 맞춤형 시사점을 제시할 수 있을 것으로 판단된다. 더불어, 정보보안은 최신의 기술을 정책적으로 적용함으로써, 정보를 보호하고자 하기 때문에, 필연적으로 기술적 활용능력에 기반하여 행동하고자 한다. IT 활용 능력 수준이 높은 사람과 그렇지 못한 사람과의 준수의도의 차이가 나타날 수 있을 것으로 판단한다. 따라서 정보보안 활용 역량 수준에 따른 준수의도 변화에 대한 연구가 추가 된다면, 조직원의 특성별 대응 전략 수립에 도움을 줄 수 있을 것으로 판단된다.

넷째, 정보보안 공정성 및 동기를 높이기 위한 조직차원의 노력요인의 연구가 필요하다. 지속적으로 엄격해지고 발전하고 있는 정보보안 기술의 적용 및 보안 정책의 공정함에 대한 이해는 보안 관련 조직의 교육 및 훈련이 필요하다. 즉, 보안 공정성 수준을 이해하고 준수의도를 높이기 위해서는 조직차원의 보안 문화 형성을 위한 노력 요인이 제시되어야하며, 이에 대한 연관관계를 연구하는 것이 필요하다.

REFERENCES

[1] IDC. (2016). Worldwide Semiannual Security Spending Guide, 2016.

[2] J. Do & J. Kim. (2014). A study on critical success factors for enterprise security collaboration. *Journal of Digital Convergence, 12(10),* 235-242.

[3] I. Hwang & O. Cha. (2018). Examining technostress creators and role stress as potential threats to employees' information security compliance. *Computers in Human Behavior, 81,* 282-293.

[4] 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.

[5] A. Vance, M. Siponen & S. Pahnila. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management, 49(3),* 190-198.

[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] S. R. Boss, D. F. Galletta, P. B. Lowry, G. D. Moody & P. Polak. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly, 34(3),* 523-548.

[8] 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.

[9] C. Park & M. Yim. (2012). An understanding of impact of security countermeasures on persistent policy compliance. *Journal of Digital Convergence, 10(4),* 23-35.

[10] 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.

[11] 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.

[12] 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.

[13] K. H. Guo & Y. Yuan. (2012). The effects of multilevel sanctions on information security violations: A mediating model. *Information & Management, 49(6),* 320-326.

[14] 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.

[15] J. Y. Son. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management, 48(7),* 296-302.

[16] A. B. Ruighaver, S. B. Maynard & S. Chang. (2007). Organizational security culture: extending the end-user perspective. *Computers & Security, 26(1),* 56-62.

[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] 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.

[19] R. West. (2008). The psychology of security. *Communications of the ACM, 51(4),* 34-40.

[20] 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.

[21] Verizon. (2016). 2016 Data Breach Investigations Report.

[22] M. Siponen, S. Pahnila & M. A. Mahmood. (2010). Compliance with information security policies: An empirical investigation. *Computer, 43(2),* 64-71.

[23] T. Jeong, M. Yim & J. Lee. (2012). A development of comprehensive framework for continuous information security. *Journal of Digital Convergence, 10(2),* 1-10.

[24] J. Han & Y. Kim. (2015). Investigating of psychological factors affecting information security compliance intention: Convergent approach to information security and organizational citizenship behavior. *Journal of Digital Convergence, 13(8),* 133-144.

[25] M. 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.

[26] 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.

[27] I. Ajzen. (1991). The theory of planned behavior. *Organizational Behavior and Human Decision Processes, 50(2),* 179-211.

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

[29] N. S. Safa, M. Sookhak, R. Von Solms, S. Furnell, N. A. Ghani & T. Herawan. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security, 53,* 65-78.

[30] J. Zhang, B. J. Reithel & H. Li. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security, 17(4),* 330-340.

[31] A. C. Johnston & M. Warkentin (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34(3),* 549-566.

[32] W. R. Flores & M. Ekstedt. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security, 59,* 26-44.

[33] N. S. Safa & R. Von Solms. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior, 57,* 442-451.

[34] M. Siponen, M. A. Mahmood & S. Pahnila. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51(2),* 217-224.

[35] C. Posey, T. L. Roberts & P. B. Lowry (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems, 32(4),* 179-214.

[36] H. L. Chou, & C. Chou. (2016). An analysis of multiple factors relating to teachers' problematic information security behavior. *Computers in Human Behavior, 65,* 334-345.

[37] R. Cropanzano, L. Paddock, D. E. Rupp, J. Bagger & A. Baldwin. (2008). How regulatory focus impacts the process-by-outcome interaction for perceived fairness and emotions. *Organizational Behavior and Human Decision Processes, 105(1),* 36-51.

[38] P. M. Muchinsky. (2006). *Psychology Applied to Work: An Introduction to Industrial and Organizational Psychology.* Cengage Learning.

[39] P. E. Spector. (2008). *Industrial and Organizational Psychology.* Research and. Practice.

[40] 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.

[41] J. R. Fu, P. H. Ju & C. W. Hsu. (2015). Understanding why consumers engage in electronic word-of-mouth communication: Perspectives from theory of planned behavior and justice theory. *Electronic Commerce Research and Applications, 14(6),* 616-630.

[42] 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.

[43] M. L. Ambrose & M. Schminke. (2009). The role of overall justice judgments in organizational justice research: a test of mediation. *Journal of Applied Psychology, 94(2),* 491-500.

[44] T. Y. Chou, T. C. Seng-cho, J. J. Jiang & G. Klein. (2013). The organizational citizenship behavior of IS personnel: Does organizational justice matter?. *Information & Management, 50(2),* 105-111.

[45] O. Demirtas. (2015). Ethical leadership influence at organizations: Evidence from the field. *Journal of Business Ethics, 126(2),* 273-284.

[46] C. Yoon. (2011). Theory of planned behavior and ethics theory in digital piracy: An integrated model. *Journal of Business Ethics, 100(3),* 405-417.

[47] C. C. Pinder. (1998), *Work motivation in organizational behavior*. Upper Saddle River, NJ: Prentice Hall.

[48] E. M. Fair, & L. Silvestri. (1992). Effects of rewards, competition and outcome on intrinsic motivation. *Journal of Instructional Psychology, 19(1),* 3.

[49] K. H. Guo, Y. Yuan, N. P. Archer & C. E. Connelly. (2011). Understanding nonmalicious security violations in the workplace: A composite behavior model. *Journal of Management Information Systems, 28(2),* 203-236.

[50] H. Li, J. Zhang & R. Sarathy. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems, 48(4),* 635-645.

[51] J. E. Dutton, J. M. Dukerich & C. V. Harquail. (1994). Organizational images and member identification. *Administrative Science Quarterly, 39(2),* 239-263.

[52] J. C. Nunnally. (1978). *Psychometric theory* (2nd ed.). New York: McGraw-Hill.

[53] B. H. Wixom & H. J. Watson. (2001). An empirical investigation of the factors affecting data warehousing success. *MIS Quarterly, 25(1),* 17-41.

[54] C. Fornell & D. F. Larcker. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research, 18(1),* 39-50.

황 인 호(Hwang, In Ho) [정회원]

- 2004년 8월 : 건국대학교 경영학과 (경영학사)
- 2007년 6월 : 중앙대학교 경영학과 (경영학석사)
- 2014년 2월 : 중앙대학교 경영학과 (경영학박사)
- 2014년 2월 ~ 현재 : (사)한국창업경영연구원 정보전략 연구 팀장
- 관심분야 : IT 핵심성공요인, 디지털 콘텐츠, 정보보안 및 프라이버시 분야 등
- E-Mail : hwanginho@nate.com

허 성 호(Hu, Sung Ho) [정회원]

- 2004년 2월 : 홍익대학교 신소재공학과(공학사)
- 2006년 2월 : 중앙대학교 심리학과 (문학석사)
- 2012년 8월 : 중앙대학교 심리학과 (문학박사)
- 2016년 3월 ~ 현재 : 한양대학교 산업융합대학원 겸임교수
- 관심분야 : 문화차원, 성인발달, 인지과학, 정보관리, 공정사회 분야 등
- E-Mail : powerrcy@hanmail.net