Regular paper | Journal of the KIECS. pp. 337-348, vol. 18, no. 2, Apr. 30. 2023, t. 118, pISSN 1975-8170 | eISSN 2288-2189
http://dx.doi.org/10.13067/JKIECS.2023.18.2.337

정보보안 정책 및 제재 인식이 공정성을 통해 준수 의도에 미치는 영향: 공정 민감성의 역할

황인호*

The Impact of IS Policy and Sanction Perceptions on Compliance Intention through Justice: The Role of Justice Sensitivity

In-Ho Hwang*

요 약

조직의 정보 자산에 대한 보호가 조직의 지속가능성에 영향을 주면서, 조직들은 체계적인 정보 자산관리 및 보호를 위한 정책, 규정, 그리고 기술 등에 대한 투자를 높이고 있다. 본 연구는 조직 내 도입된 정보보안 정책을 실제 업무에 적용하는 조직원의 관점에서 보안 준수에 미치는 영향을 확인한다. 특히, 본 연구는 억제 이론 확장의 관점에서 정보보안 정책 인식, 제재의 방식, 공정성, 그리고 정보보안 준수로 이어지는 메커니즘을 밝힌다. 본 연구는 정보보안 규정을 업무에 적용한 조직의 근로자를 대상으로 확보된 316개의 표본을 적용하였으며, AMOS 및 SPSS 패키지를 활용하여 메커니즘의 연관 관계를 확인하였다. 가설 검증 결과, 정보보안 정책 인식이 제재의 심각성과 명확성을 통해 조직 공정성 및 준수 의도를 높이는 것을 확인하였으며, 개인의 공정 민감성이 공정의 원인과 결과의 과정에 조절 효과를 가지는 것을 확인하였다. 본 연구에서 확인한 제재의 영향 메커니즘은 조직 내부의 보안 행동 수준 강화를 추구하는 조직에서 조직원의 참여 증진을 위한 방법 마련에 도움을 줄 것으로 기대한다.

ABSTRACT

As protecting organizations' information assets affects their substantiality, they are increasing their investments in policies, regulations, and technologies for systematic information asset management and protection. This study confirms the impact on information security(IS) compliance from the perspective of employees who apply IS policies to actual work. In particular, this study identifies mechanisms linked to IS policy awareness, sanction, justice, and IS compliance from the perspective of expanding deterrence theory. We applied 316 samples obtained from workers of organizations that applied IS policies and regulations to work and verified the relationship between mechanisms by using AMOS and SPSS packages. As a result of the verification, IS policy awareness had a positive effect on organization justice and compliance intention through the severity and clarity of sanctions. Individual justice sensitivity had a moderating effect on the cause and outcome of justice. The sanction-related mechanism presented in this study provides strategic implications for organizations that require active IS activities by insiders.

키워드

Compliance Intention, Justice Sensitivity, Organization Justice, Policy Awareness, Sanction
준수 의도, 공정 민감성, 조직 공정성, 정책 인식, 제재

* 교신저자: 국민대학교 교양대학
• 접 수 일 : 2023. 02. 23
• 수정완료일 : 2023. 03. 19
• 게재확정일 : 2023. 04. 17
• Received : Feb. 23, 2022, Revised : Mar. 19, 2023, Accepted : Apr. 17, 2023
• Corresponding Author : In-Ho Hwang
College of General Education, Kookmin University,
Email : hwanginho@kookmin.ac.kr

Ⅰ. 서 론

조직 내 생성되는 정보 자원에 대한 체계적인 관리가 조직의 성과 향상에 영향을 주고, 국가 차원에서 정보 자원 관리의 요구가 강화되면서, 조직들은 정보보안 체계 구축 및 운용에 대한 투자를 높이고 있다[1]. 실제로, 글로벌 사이버 보안 시장은 2030년까지 연평균성장률 12.3%에 이를 것으로 기대된다[2]. 특히, 팬데믹 사태를 겪으면서 많은 조직이 재택근무, 온라인 미팅 등과 같은 비대면 네트워크 활동을 확대하였는데, 오히려 사이버 보안 위협이 증가하여 보안 솔루션 투자로 이어지고 있다[3]. 조직들은 내부 정보보안 정책 및 규정을 확립하고, 엄격한 보안 기술을 도입하는 등 전사적 차원에서 정보자산관리를 위한 투자 활동을 높이고 있다[1]. 하지만, 조직이 정보보호를 위한 환경을 구축하더라도 실제 업무에 정보보안 관련 활동을 수행해야 하는 조직원들의 참여가 저조할 경우, 정보보안 투자의 회수는 실질적으로 어려워질 가능성이 있다[4]. 즉, 내부자의 정보보안 준수 수준 향상이 무엇보다 중요하다. 실제로, 글로벌 보안 사고의 2/5는 내부자 및 파트너에 의한 악의적 또는 비 악의적인 정보 노출 사고에 기인한다[5].

내부자의 정보 준수 행동 증진과 관련된 선행연구는 개인의 정보보안 관련 다양한 행동 동기를 제시해왔다. 대표적으로, 내부자의 정보보안 미준수 행동에 대한 제재 및 처벌에 대한 인식이 중요하다고 본 연구[6, 7], 개인은 정보보안과 관련하여 합리적 선택을 하고자 하는데, 보안 준수 행동의 이익과 손실을 종합적으로 고려한다고 본 연구[8], 그리고 정보보안 미준수 시 발생할 위협에 대한 인식과 대처방법에 대한 인식이 연계되어 행동으로 이어질 수 있음을 밝힌 연구[1, 9] 등이 있다. 해당 연구들은 정보보안과 관련된 조직의 요구사항에 대한 개인의 인식과 행동을 설명한 측면에서 시사점을 가진다.

본 연구는 조직이 정보보안 정책을 도입할 때, 가장 일반적으로 활용하는 개념인 제재(Sanction)가 보안 준수로 이어지는 메커니즘을 밝히는 것을 목적으로 한다. 제재는 대표적인 억제 이론(Deterrence Theory)의 적용 개념으로서, 특정 활동에서 개인에게 손실을 입힐 수 있는 조건인 명료한 처벌에 대한 인식이 강화될 때, 개인들은 손실 최소화를 위해 억제 행동을 한다는 관점이다[6]. 본 연구는 억제 이론의 요소인 제재에 대한 사용자 인식은 단순히 행동에 단일 차원으로 연계되는 것이 아닌, 정보보안 정책에 대해 인식(Awareness)을 기반으로 제재에 대한 손익을 판별하고, 나아가 명료하고 심각한 제재는 조직에 대한 공정성(Justice) 인식을 높여 준수 행동으로 이어진다고 본다. 즉, 제재의 수준이 개인의 보안 준수로 이어지는 흐름을 밝히고자 한다. 이를 위해, 본 연구는 정보보안 정책 인식, 제재 유형(심각성, 명확성), 조직 공정성, 공정 민감성, 그리고 준수 의도를 메커니즘 요소로 제시하고 가설 검증을 수행하고자 한다. 본 연구는 2장 이론적 배경 부분에 적용 요인들의 선행연구를 통해 적용 필요성과 가설을 제시하고, 3장에 연구모델 및 측정 방법을 소개하고, 4장에 표본을 활용한 구조모델 분석을 수행하여 결론을 제시한다.

Ⅱ. 이론적 배경

2.1 조직 보안 환경 및 조직원의 준수

최근, 정보보안 사고가 지속해서 발생하고, 규모가 커짐에 따라, 정보 노출 사고는 단순히 조직만의 문제가 아니라 사회 구성원의 정보 자원이 노출되는 사건으로서 인식되고 있다[4]. 이에, 국가들은 정부 주도로 국가와 관련 있거나, 중요도가 높은 기업의 데이터 보호를 위해 법적 보호를 위한 방법을 마련하고 있다. 우리나라의 경우 정보통신망법과 개인정보 보호법을 기반으로 정보통신 분야 또는 매출 등의 일정 조건이 갖추어진 기업에 정보보호 및 개인정보보호관리체계 인증(ISMS-P)을 받도록 함으로써[10], 정보보안의 의무를 부여하고 있다. 미국 행정부는 한발을 더 나아가 제로 트러스트(Zero Trust)를 요구하고 있다. 제로 트러스는 내부자, 외부자 관련 없이 정보관리 체계를 엄격하게 갖추고 적용하라는 것으로서[11], 사람에 의한 정보 노출 가능성을 억제하기 위한 조직의 관리를 요구한다. 즉, 사회적으로 조직이 사람에 의한 정보 노출 최소화 전략을 수립하길 요구하고 있다.

따라서, 조직은 정보보안 위협을 최소화하는 정책,

규정, 그리고 기술 등의 도입에 투자하는 것 이외, 조직과 관련된 이해관계자(조직원, 파트너 등)가 악의적이지 않더라도 정보를 노출하지 않도록 하는 노력이 요구된다[12]. 하지만, 조직원의 관점에서 정보보안은 본인에게 부여된 원천의 업무가 아니고, 업무 성과 달성을 위해서는 정보를 적극적으로 교류해야 하는데 보안 활동은 이러한 활동을 억제하도록 하므로, 자발적인 정보보안 준수 행동을 갖추도록 하는 것은 어려움이 크다[6]. 준수 의도(Compliance Intention)는 조직의 정보 자산을 외부 또는 내부의 위협 등에서 보호하고자 하는 행동 의지로서[13], 준수 의도가 강화되면 자발적인 준수 행동으로 이어진다. 본 연구는 제재의 확장 관점에서 정책 인식과 공정성을 반영하여 준수 의도 향상을 위한 메커니즘을 제안한다.

2.2 공정성

공정성(Justice)은 거래 대상자와의 거래가 상대적으로 공평하다고 판단하는 개념이다[14]. 나아가, 조직 공정성(Organization Justice)은 조직원이 조직, 동료 등과의 거래 관계에서 공평함을 느끼는 수준을 의미한다[15]. 특히, 공정성은 상대성에 기인하는데, 나의 거래 과정 및 결과에 대하여 유사한 상황에서의 타인의 거래 과정 및 결과를 비교함으로써 공정성을 판단한다[16]. 즉, 사람은 상대적 만족감을 형성할 때 공정한 대우를 받았다고 인식한다.

공정성은 행동 결과에 대한 배분에서 크게 인식되나, 최근에는 결과를 일어나게 하는 과정에서 충분히 공정한 대우가 존재하는지 또한 중요한 요소로 인식된다[17]. 즉, 행동 결과에 대한 분배, 행동 과정의 절차, 행동에 필요한 정보제공 등이 중요한 공정성 요소로 인식되어 분야별 맞춤형으로 활용되고 있다[18, 19]. 또한, 사람의 공정성에 대한 인식은 전체적인 공정한 수준의 판단을 통해 발현된다고 보고, 단일의 조직 공정성을 제시하기도 한다[20]. 본 연구는 정보보안에 대한 전체적인 공정성에 대한 인식이 중요하다고 판단하여 전체적인 조직 공정성 요인을 반영한다.

집단 내 개인의 공정성 인식은 집단이 요구하는 행동에 대한 변화로 이어진다. Li et al.[2014]는 인터넷 사용 정책 준수에 있어, 절차적, 정보적, 분배적 공정성에 대한 인식의 향상은 준수 의도를 높이는 선행 조건이라고 하였으며[14], Alshare et al.[2018]은 고등 교육 부문에서 개인들의 정보보안에 대한 공정한 대우를 인식할 경우 정보보안 회피 행동을 감소할 수 있다고 하였다[15]. Lee and Hwang[2021]은 정보 관리에 대한 절차 및 정보 공정성은 조직에 대한 동질성을 형성하여, 조직원의 이타적 정보제공 행동인 제언 행동에 기여한다고 하였다[16]. 나아가, 개인이 조직으로부터 받은 공평함에 대한 인식은 단순히 개인 중심의 행동을 넘어선 이타적 행동까지 보이도록 하는데, 대표적으로 조직시민행동을 보이는 모습까지 나타나도록 한다[17]. 즉, 정보보안 공정성은 조직이 요구하는 보안 관련 준수 수준을 높이는 선행 조건이며, 본 연구는 준수 의도와 연계하여 다음의 가설을 제시한다.

H1. 정보보안 관련 공정성은 개인의 준수 의도에 긍정적 영향을 줄 것이다.

2.3 제재

범죄학 등에서 활용되던 억제 이론(Deterrence Theory)이 정보보안 분야에 활용되면서, 조직들은 정보보안 정책과 규정을 체계화하고 미준수 행동에 대한 제재를 강화하고 있다[21]. 제재(Sanction)는 대표적인 외재적 동기 요인으로서, 특정 요구사항의 결과에 대한 강력한 억제 수단을 제시하는 개념이다[22]. 즉, 정보보안 미준수 행동의 결과를 일으킨 사람에게 직, 간접적으로 손실을 줄 수 있음을 밝히고 실제 행동으로 보일 때, 사람들은 본인의 손실을 최소화하기 위하여 억제 행동을 한다는 관점이다[6].

제재가 사람들에게 명료하게 인식되기 위해서는 제재의 수준과 일정함에 대한 고려가 요구된다. 즉, 제재가 심각하게 받아들여지고, 누구나 미준수 시 제재를 받게 됨을 전달하는 것이 필요하다[9, 22]. 첫째, 제재의 심각성(Severity of Sanction)이 요구된다. 정보보안 미준수 관련 결과에 대하여 사람들의 인식 수준을 높이기 위해서는 관련 처벌의 수준이 높아야 한다[9]. 조직 내 제재의 유형은 벌금과 같은 금전적 형태, 법적 고발 등과 같은 비금전적 형태로 나뉠 수 있는데, 정보보안 미준수 행동의 수준에 따라 조직은 경고, 감봉, 퇴사, 그리고 법적 조치 등을 취하게 된다[23]. 이러한 조직의 처벌에 대한 행동이 조직원에게 심각하게 받아들여질 때, 그들은 정보보안 준수의 필

요성을 강하게 인식하고 준수 행동을 보이는 경향이 있다[1]. 둘째, 제재의 명확성(Clarity of Sanction)이 요구된다. 제재의 명확성은 제재의 가능성에 대한 사람들의 인식 수준으로서, 누구나 조직이 결정한 정책에 위반 사항이 드러날 경, 명확하게 제재한다는 것을 의미한다[15]. 이러한 명확성은 결과의 공정함과 연계되는데, 직장 내 위치, 권력의 차이에 따라 불분명한 제재가 일어난다고 판단할 경우, 개인들은 충분히 규정이 아닌 암묵적 계약으로 해결할 수 있다고 판단하여 미준수 행동으로 이어질 가능성이 존재한다[9]. 역으로, 정보보안 정책, 규정에 대한 명료한 결과는 개인들이 반드시 지켜야 하는 조건으로 인식되어 준수 행동을 높일 수 있다[6].

정보보안 관련 제재는 조직이 요구하는 보안 준수 행동을 따르도록 하는 선제 조건이다. Alshare et al.[2018]은 정보관리에 대한 회피 행동을 감소하는 요인으로 처벌의 명확성과 심각성이 선제적으로 필요하다고 하였으며[15], Liu et al.[2021]은 정보보안 활동에 대한 보상 및 제재에 대한 기대가 강화될수록 준수 행동에 영향을 준다고 하였다[6]. 또한, Hong and Furnell[2022]은 조직 내 공식화된 정책에 대한 억제 인식은 보안 준수 행동에 영향을 준다고 하였다[1]. 즉, 정보보안 관련 제재의 심각성과 제재의 명확성은 조직이 공식화한 보안 준수 절차를 따르도록 하는 선행 조건이며, 다음의 연구가설을 제시한다.

H2. 정보보안 관련 제재 심각성은 개인의 준수 의도에 긍정적 영향을 줄 것이다.

H3. 정보보안 관련 제재 명확성은 개인의 준수 의도에 긍정적 영향을 줄 것이다.

조직 내 특정 정책 및 규범에 대한 처벌의 강화는 행동에 대한 공정한 결과를 기대하도록 한다. 즉, 조직 구성원의 보안 행동의 결과가 권력이나 위치에 따라 다르게 반영되는 것이 아닌, 엄격하지만 모든 사람에게 공평하게 적용된다고 판단할 때, 사람들은 대상에 대한 공정함을 인정한다. Xue et al.[2011]는 실제 조직의 처벌 활동을 통해 형성된 처벌 기대 인식은 처벌에 대한 공정성을 높여 준수 행동으로 이어질 수 있음을 밝혔으며[23], Merhi and Ahluwalia[2019]는 정보보안 처벌의 심각성과 명확성이 강화될 때, 개인들은 조직 내 일관된 규범의 수준을 인식하고, 저항 감소로 이어진다고 하였다[7]. 즉, 일관된 처벌 활동은 정보보안의 공정성 인식으로 이어지며, 처벌 심각성과 명료성, 그리고 공정성과의 관계를 기반으로 다음 가설을 제시한다.

H4. 정보보안 관련 제재 심각성은 개인의 공정성에 긍정적 영향을 줄 것이다.

H5. 정보보안 관련 제재 명확성은 개인의 공정성에 긍정적 영향을 줄 것이다.

2.4 보안 정책 인식

조직은 정보보안 등 그들이 목적으로 하는 특정 활동에 대하여 조직원의 능동적인 참여를 기대한다[24]. 개인의 특정 활동에 대한 참여가 이루어지기 위해서는 참여 활동을 통한 가치 등을 확보해야 하는데, 사전에 해당 활동의 필요성, 방향 등에 대한 인식이 명료하게 갖추어질 필요가 있다[25].

인식(Awareness)은 특정 목적에 대한 전반적인 지식과 이해의 수준을 의미한다[8]. 정보보안 활동과 관련하여, 조직원들은 정보보안의 필요성과 가치 등의 기본적인 지식을 보유하고 있어야 한다[25]. 즉, 조직의 정보보안 정책과 규정, 기술 등에 대한 투자는 사용자인 조직원들이 해당 자원에 대한 이해를 요구하는데, 사전에 기본적인 인식이 갖추어져 있지 않을 경우, 추가적인 교육 또는 훈련을 통해 필요한 정보를 확보하지 않으려고 하는 모습을 보일 수 있다[26]. 보안 정책 인식(Information Security Policy Awareness)은 개인을 둘러싼 정보보안 행동 규정, 방법 등에 대한 이해의 수준으로서, 조직의 보안 목적 및 가치를 이해하고, 헌신하고자 하는 수준을 의미한다[8]. 정보보안 정책의 가치와 준수의 필요성, 기본적인 방법 등을 이해하고 있을 때, 조직이 요구하는 정보보안 준수 활동을 이해하고 따르려는 모습을 보일 수 있다[25]. 즉, 인식은 개인이 동기를 형성하도록 돕는 기본적인 이해의 수준으로서, 정보보안 관련 동기 형성에 선행적으로 요구되는 조건이다.

정보보안 관련 정책 인식은 정보보안 정책 준수 활동 및 이행 결과를 판단하도록 돕는 선행 조건이다. Li et al.[2019]는 조직의 보안 정책에 대한 인식을 보유한 사람은 조직 내 다른 사람들의 정보보안 활동 등을 평가하고, 심각성 등을 이해하고 있어 준수 행동을 보인다고 하였으며[25], Bulgurcu et

al.[2010]은 정보관리 및 정책 인식이 선행될 때, 사람들은 정보보안 처벌 등으로 인한 미준수 비용과 준수 비용 등을 합리적으로 판단할 수 있다고 하였다[8]. 또한, D'Arcy et al.[2009]는 정보시스템 오남용과 관련하여, 사용자들의 보안 정책에 대한 인식은 제재의 심각성과 명확성에 영향을 주어 오남용 행동을 감소시킬 수 있다고 하였다[26]. 즉, 정보보안 행동 결과에 대한 처벌에 대한 인식은 정책 가치와 목적을 명료하게 인식하고 있을 때 형성된다. 선행연구에 따라 본 연구는 정보보안 정책 인식과 제재 간에 영향 관계가 형성될 것으로 판단하고, 다음의 가설을 제시한다.

H5a. 정보보안 관련 정책 인식은 제재 심각성에 긍정적 영향을 줄 것이다.

H5b. 정보보안 관련 정책 인식은 제재 명확성에 긍정적 영향을 줄 것이다.

2.5 공정 민감성

공정성은 특정 거래 관계에서의 과정과 결과가 상대적으로 공평하게 이루어졌다는 믿음의 수준이므로[20], 동일 조직 내에서, 동일한 결과의 평가에 대해서도 개인의 공정성 인식은 다르게 나타날 수 있다[27]. 즉, 공정함에 대한 개인의 평가는 상황별, 조건별 다르게 나타날 수 있다. 공정 민감성(Justice Sensitivity)은 개인이 특정 상황에서 공평 또는 불공평을 인식하는 수준의 차이로서, 공정 민감성이 높을수록 엄격한 평가를 한다[28].

공정 민감성은 조직 및 특정 결과에 대한 개인의 평가를 다르게 한다. 특정 상황에서 개인이 판단하는 공정함의 수준은 환경에 대한 개인의 민감성에 따라 다를 수 있는데, 유사한 거래 과정에서의 과정 및 결과가 민감성이 높을수록 다른 공평함의 수준으로 나타날 수 있다[29]. 관련하여, Gollwitzer et al.[2009]는 공정 민감성에 따라 조직이 요구하는 사항에 대한 위반 행동을 다르게 가진다고 하였으며[29], Schmitt et al.[2005]는 사람별 공정 민감성의 차이가 있으며, 공정 민감성이 높은 사람에게 신뢰의 상황은 크게 받아들여져 조직에 대한 긍정적 태도를 보유하도록 한다고 하였다[28]. Lee and Hwang[2021]은 절차 및 정보 공정성이 보안 준수 원인에 미치는 영향에 민감성이 조절 효과를 가져, 민감성이 높을수록 공정한 상황에 대한 긍정적 반응을 이끌 수 있다고 하였다[16]. 즉, 공정 민감성은 공정성에 대한 인식과 이에 따른 행동에 영향을 줄 것으로 판단한다.

H6a. 공정성과 준수 의도 간의 관계는 공정 민감성에 의해 조절될 것이다.

H6b. 제재 심각성과 공정성 간의 관계는 공정 민감성에 의해 조절될 것이다.

H6c. 제재 명확성과 공정성 간의 관계는 공정 민감성에 의해 조절될 것이다.

III. 연구모델의 구성 및 측정 방법

3.1 연구모델

조직의 정보보안 정책과 이행 방식인 제재에 대한 인식이 공정성을 통해 개인의 준수 의도로 이어지는 메커니즘을 제시하는 것을 목적으로 하며, 제안하는 연구모델은 그림 1과 같다.

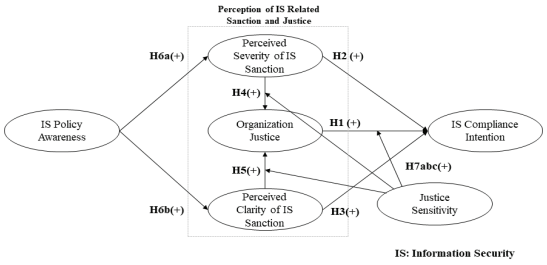

그림 1. 연구모델
Fig. 1 Research Model

3.2 측정 도구

연구모델 기반 제시한 가설 검증을 위한 데이터 확보는 선정된 연구 대상별 설문지 기법을 통해 수행한다. 본 연구는 적용 모델에 대하여 다 항목 중심의 측정 도구와 요인별 7점 리커트 척도를 반영하였다.

정보보안 정책 인식은 Bulgurcu et al.[2010] 연구에서 항목을 도출하였으며[8], "우리 조직의 정보보안 정책에서 규정한 규칙을 알고 있음", "우리 조직의 정보보안 정책에서 규정한 규칙을 이해하고 있음", "조직의 정보보안을 강화하기 위해 보안 정책에 규정

된 책임을 알고 있음"과 같이 3개 문항을 반영하였다. 제재 심각성은 Herath and Rao[2009] 연구에서 항목을 도출하였으며[9], "조직은 보안 규칙을 어긴 조직원에 대하여 징계를 함", "반복적으로 보안 규칙을 어긴 조직원에게 더욱 강력한 징계함", "내가 보안 정책을 위반할 경우, 심각한 처벌을 받을 것"과 같이 3개 문항을 반영하였다. 제재 명확성은 Son[2011] 연구에서 항목을 도출하였으며[21], "조직은 엄격하게 정보보안 정책을 적용", "보안 정책을 위반 시, 제재받을 가능성이 높음", "보안 정책을 위반 시, 명시적으로 제재가 발생한다는 것을 제시"와 같이 3개 문항을 반영하였다. 조직 공정성은 Ambrose and Schminke[2009] 연구에서 항목을 도출하였으며[20], "조직은 정보보안과 관련하여 전체적으로 공정한 대우를 함", "나는 조직이 정보보안에 대하여 공정하게 대우한다고 믿음", "조직은 일반적으로 정보보안 관련 활동을 공정하게 함", "조직은 조직원에게 공평하게 정보보안 관련한 활동을 수행함"과 같이 4개 문항을 반영하였다. 준수 의도는 Chen et al.[2012] 연구에서 항목을 도출하였으며[13], "앞으로 우리 조직의 보안 정책과 관련된 요구사항을 준수할 의향이 있음", "앞으로 우리 조직의 보안 정책의 요구사항에 따라 정보와 기술 자원을 보호할 의향이 있음", "앞으로 정보기술 사용 시 조직에서 정한 규칙과 책임에 따라 행동할 의향이 있음"과 같이 3개 문항을 반영하였다. 공정 민감성은 Schmitt et al.[2005]의 연구 항목을 도출하였으며[28], "다른 사람이 내 것이어야 할 무엇인가를 가져갈 때 신경 쓰임", "다른 사람이 나로부터 이익을 취할 때 견딜 수 없음", "다른 사람보다 나의 기술을 개발할 기회가 적어지면 실망감에 빠짐", "다른 사람들이 나보다 더 나아질 때 화가 남"과 같이 4개 문항을 반영하였다.

3.3 대상 및 표본 확보

본 연구는 정보보안 제재와 공정성에 따라 개인의 행동 의도 변화를 확인하는 것을 목적으로 하므로, 정보보안 정책과 규정을 자사의 특성에 맞게 도입한 기업에서 근무하는 조직원을 대상으로 설문한다. 본 연구는 100만 명 이상의 직장인 회원을 보유한 M 리서치를 통해 온라인 설문을 하였으며, 설문 설계 시, 연령, 직장, 그리고 정보보안 정책 유무를 사전에 확인하고, 대상인 사람만 본 응답에 참여할 수 있도록 구조화하였다. 그리고, 결과의 통계적 활용에 대하여 알렸으며, 응답을 허가한 사람만 참여하도록 하며, 316개의 표본을 확보하였다. 수집된 316개 데이터에 대한 통계적 특성을 살펴보면, 성별은 남성 202명(63.9%), 여성 114명(36.1%)으로 나타났으며, 나이는 20대 101명(32.0%), 30대 110명(34.8%), 40대 77명(24.4%), 50대 이상 28명(8.8%)으로 나타났다. 근무하는 회사의 업종은 제조업 57명(18.0%), 서비스업 259명(82.0%)으로 나타났으며, 직급은 사원급 103명(32.6%), 대리·과장급 140명(44.3%), 차·부장 이상급 73명(23.1%)으로 나타났다.

Ⅳ. 분 석

4.1 신뢰성 및 타당성

본 연구는 다 항목으로 구성된 설문을 통해 데이터를 확보했으므로, 가설 검정 전, 요인의 신뢰성과 타당성을 확인하였다.

표 1. 타당성 및 신뢰성

Table 1. Construct Validity and Reliability

Constructs		Factor Loading	Cronbach's Alpha	CR	AVE
PA	PA3	0.903	0.899	0.874	0.699
	PA2	0.836			
	PA1	0.855			
SS	SS3	0.835	0.894	0.859	0.671
	SS2	0.897			
	SS1	0.850			
CS	CS3	0.867	0.895	0.863	0.678
	CS2	0.896			
	CS1	0.819			
OJ	OJ4	0.868	0.935	0.863	0.678
	OJ3	0.892			
	OJ2	0.893			
	OJ1	0.885			
Int	Int3	0.908	0.876	0.913	0.777
	Int1	0.874			
Sens	Sens4	0.811	0.912	0.872	0.630
	Sens3	0.831			
	Sens2	0.894			
	Sens1	0.866			

PA(Policy Awareness), SS(Severity of Sanction), CS(Clarity of Sanction), OJ(Organization Justice), Int(Compliance Intention), Sens(Justice Sensitivity)

첫째, 신뢰성은 SPSS 21.0에서 제공하는 크론바흐 알파를 활용하였으며, 선행연구는 0.7 이상의 요인별 크론바흐 알파를 요구한다. 연구모델의 6개 요인의 측정 항목은 총 20개이지만, 신뢰성에 문제를 보인 1개 문항을 제외하였다(Int 2). 분석 결과는 표 1과 같으며, 가장 낮은 값이 0.876(준수 의도)으로 모든 요인이 신뢰성을 확보하였다[30]. 둘째, 타당성은 AMOS 22.0 패키지의 확인적 요인분석을 활용하였다. 확인적 요인분석을 반영한 모델의 적합도는 χ^2/df = 1.612, RMSEA = 0.044, GFI = 0.928, AGFI = 0.903, NFI = 0.956, TLI = 0.979, 그리고 CFI = 0.983으로 나타나, 적합도 요구사항은 모두 충족하였다[31]. 집중 타당성은 요인의 일관성을 확인하는 것으로, 개념 신뢰도(CR), 평균분산추출(AVE)을 각각 구하되 요인별 0.7과 0.5 이상을 요구한다. 분석 결과는 표 1과 같으며, 집중 타당성을 모두 확보하였다[31].

판별 타당성은 요인별 차별성을 검증하는 것으로, 선행연구는 평균분산추출의 제곱근과 상관계수를 비교하되, 모든 상관계수가 평균분산추출의 제곱근보다 적은 것을 요구한다[31]. 확인 결과는 표 2와 같으며, 판별 타당성이 있는 것으로 검증되었다.

표 2. 판별 타당성 결과
Table 2. Result for Discriminant Validity

Constructs	1	2	3	4	5	6
PA	0.836[a]					
SS	.483[**]	0.819[a]				
CS	.474[**]	.678[**]	0.823[a]			
OJ	.469[**]	.575[**]	.621[**]	0.823[a]		
Int	.546[**]	.636[**]	.693[**]	.668[**]	0.881[a]	
Sens	.595[**]	.531[**]	.519[**]	.556[**]	.632[**]	0.793[a]

**: p < 0.01, a = square root of the AVE
PA(Policy Awareness), SS(Severity of Sanction), CS(Clarity of Sanction), OJ(Organization Justice), Int(Compliance Intention), Sens(Justice Sensitivity)

4.2 주 효과 분석

주 효과 분석은 정보보안 정책 인식, 제재, 공정성, 그리고 준수 의도로 이어지는 메커니즘을 검증하는 것이다. 연구는 AMOS 22.0 패키지의 구조방정식 모델링을 반영하여 검증하였다. 우선 주 효과 모델의 적합도를 확인하였다. 결과는 χ^2/df = 3.316, RMSEA = 0.086, GFI = 0.902, AGFI = 0.858, NFI = 0.931, TLI = 0.937, 그리고 CFI = 0.950으로 나타났다. 비록, RMSEA, AGFI가 각각의 요구사항인 0.05, 0.900보다 약간 부족하게 나타났으나, 허용할만한 수치이며 전체적인 맥락을 살펴보는 구조방정식 특성상 적합도는 문제가 되지 않는다고 판단하여 주 효과 분석을 하였다[31]. 결과는 그림 2와 같다.

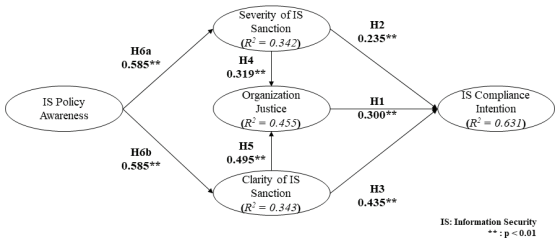

그림 2. 주 효과 (경로 분석) 결과
Fig. 2 Results of Main Effect Tests

가설 1은 조직 공정성이 준수 의도에 긍정적 영향을 미친다는 것으로서, 구조방정식 모델링 내 해당 경로는 유의수준 5%에서 채택되었다(H1: β= 0.300, p < 0.01). 가설 2와 3은 제재의 심각성(H2)과 제재의 명확성(H3)이 준수 의도에 긍정적 영향을 미친다는 것으로, 유의수준 5%에서 채택되었다(H2: β= 0.235, p < 0.01; H3: β= 0.435, p < 0.01). 가설 4와 5는 제재의 심각성(H4)과 제재의 명확성(H5)이 조직 공정성에 긍정적 영향을 미친다는 것으로, 유의수준 5%에서 채택되었다(H4: β= 0.319, p < 0.01; H5: β= 0.495, p < 0.01). 마지막으로, 가설 6은 정보보안 정책 인식이 제재의 심각성(H6a)과 제재의 명확성(H6b)에 긍정적 영향을 준다는 것으로, 동일 기준에서 채택되었다(H6a: β= 0.585, p < 0.01; H6b: β= 0.585, p < 0.01).

4.3 조절 효과 분석

가설 6a, 6b, 6c는 개인의 공정 민감성이 공정성에 대한 선행요인과 결과에 각각 차별적 영향을 미친다는 조절 효과를 검증하는 것으로서, 본 연구는 SPSS 21.0 패키지와 연동한 Process 3.1 툴을 반영하였다. 본 연구는 해당 툴의 조절 효과 검증 모델

인 모델 1을 반영하되 붓스트랩핑 5,000과 신뢰수준 95%를 적용하였으며, 결과는 표 3과 같다[32]. 가설 6a는 공정 민감성이 조직 공정성과 준수의도 간의 관계를 조절한다는 것으로, 공정 민감성과 조직 공정성의 상호작용 효과는 유의수준 5%에서 채택되었다. 또한, 제재 심각성(H6b), 제재 명확성(H6c)이 공정 민감성과 연계하여 조직 공정성에 영향을 줄 것이라는 가설 또한 유의수준 5%에서 각각의 상호작용 효과가 존재하는 것으로 나타났다.

표 3. 조절 효과 결과

Table 3. Results of Moderating Effect Tests

		Coefficient	t-value	Result
H6a	Constant	5.619	133.949**	Support
	OJ	0.354	7.889**	
	Sens	0.303	6.913**	
	Interaction	-0.117	-4.945**	
	F = 142.2329, R^2 = 0.5776			
H6b	Constant	5.532	110.948**	Support
	SS	0.323	5.966**	
	Sens	0.309	6.076**	
	Interaction	-0.116	-4.178**	
	F = 84.8092, R^2 = 0.4492			
H6c	Constant	5.530	114.985**	Support
	CS	0.407	7.821**	
	Sens	-.269	5.443**	
	Interaction	-0.118	-4.182**	
	F = 99.4140, R^2 = 0.4887			

SS(Severity of Sanction), CS(Clarity of Sanction), OJ(Organization Justice), Sens(Justice Sensitivity)

*: $p < 0.05$, **: $p < 0.01$

공정 민감성의 조절 효과가 인정되어, 공정 민감성이 각 요인에 미치는 영향에 대하여 SPSS 21.0 패키지의 단순 기울기 그래프로 확인하였다. 그림 3은 공정 민감성이 조직 공정성과의 상호작용 효과 결과로써, 조직 공정성이 준수 의도에 미치는 긍정적 영향에서 공정성이 낮더라도 공정 민감성이 높을 경우, 준수 의도가 높아지는 것을 확인하였다. 그림 4와 5는 공정 민감성이 제재 심각성, 제재 명확성과 상호작용 효과 결과로써, 제재 심각성과 명확성이 조지 공정성에 미치는 긍정적 영향에서 각각의 선행요인이 낮더라도 공정 민감성이 높을 경우, 조직 공정성이 높아지는 것을 확인하였다.

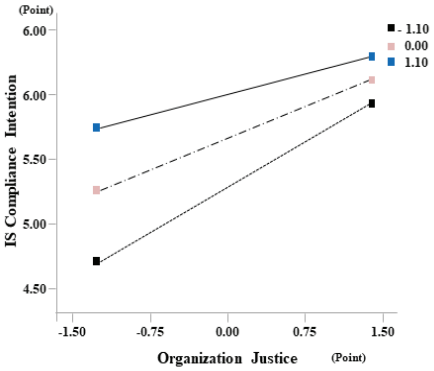

그림 3. 공정 민감성 조절 효과 (H6a)

Fig. 3 Moderation Effect of JS (H6a)

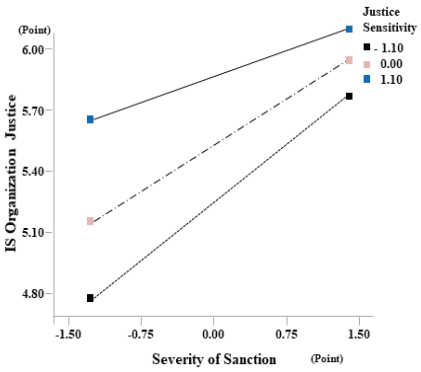

그림 4. 공정 민감성 조절 효과 (H6b)

Fig. 4 Moderation Effect of JS (H6b)

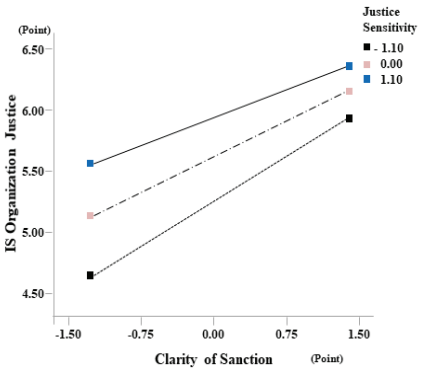

그림 5. 공정 민감성 조절 효과 (H6c)

Fig. 5 Moderation Effect of JS (H6c)

Ⅴ. 결 론

조직이 보유한 정보 자산의 체계적 관리에 대한 중요성이 높아지면서, 조직들은 정보보안 정책, 기술 등에 투자를 강화하고 있다. 그러나, 정보보안을 위해 도입한 기술, 정책들은 실제 업무에 적용해야 하는 조직원이 능동적으로 활용해야만 성과로 반영될 수 있다. 본 연구는 조직이 도입한 정보보안 규정에 따른 제재에 대한 조직원의 인식 메커니즘을 밝힘으로써, 시사점을 제시하고자 하였다.

첫째, 본 연구는 억제 이론에 대한 실무자 인식의 변화에 기반한 이론적 확장을 추구하였다. 즉, 본 연구는 정보보안 정책 인식 - 정보보안 제재 수준 - 공정성 인식 - 준수 의도로 이어지는 메커니즘을 제안하였으며, 연관 관계가 있음을 데이터로 확인하였다. 학술적 관점에서 결과는 억제 이론이 반영되는 과정을 구조화한 측면에서 의미를 지니며, 실무적 관점에서 본 연구는 조직이 구축한 정보보안 정책에 대한 사용자 수용은 정보보안 정책에 대한 기본적인 가치, 필요성 등을 인식한 사람이 정책과 결과와 관련된 판단을 하고, 공정한 상황에서 준수 활동으로 이어질 수 있음을 밝혔다. 둘째, 본 연구는 정보보안에 대한 조직 공정성에 대한 인식이 개인별 상황에 따라 다르게 판단될 수 있음을 밝힌 측면에서 의미를 지닌다. 즉, 공정성 판단은 개인별 특정 과정 및 결과에 대한 상대적 비교를 통해 이루어지는데, 공정의 과정에 대한 개인적 민감성의 차이가 존재할 수 있음을 밝혔다. 따라서, 학술적 관점에서 본 연구는 공정 민감성이 개인의 공정성 판단의 원인과 이에 따른 행동 과정에 영향을 주는 것을 밝힌 측면에서 의미를 지닌다. 또한, 실무적 관점에서 본 연구는 조직원의 행동 변화가 공정 민감성에 있음을 밝혔기 때문에, 조직원이 받아들일 수 있는 객관화된 공정한 환경의 필요성을 제시하였다.

본 연구는 억제 이론의 확장 관점에서 시사점을 가지나, 다음 측면에서의 연구적 한계를 지닌다. 첫째, 본 연구는 개인의 인식을 기반으로 조직 지원 요소의 수준을 판단하고 행동에 미치는 영향을 확인하였다. 일반적으로 설문 기법에서 활용하는 방식이기는 하나, 조직 특성별 명확한 차별성을 확인하기 위해서는 해당 기법의 변화가 요구된다. 즉, 실험 등의 방법으로 조직 특성별 정보보안 지원 체계와 행동 간의 연계를 확인한다면, 강화된 시사점을 제공할 수 있을 것이다. 둘째, 본 연구는 개인의 특성인 공정 민감성을 조절 효과로 반영하였다. 조직에서 공정성에 대한 사람들의 평가는 개인이 보유한 위치, 권력 등에서 영향을 받을 수 있는데, 이러한 특성 등을 고려한 연구가 진행된다면 내부의 정보보안 목적 달성에 도움이 될 것으로 기대한다.

References

[1] Y. Hong and S. Furnell, “Motivating information security policy compliance: Insights from perceived organizational formalization,” *J. of Computer Information Systems*, vol. 62, no. 1, 2022, pp. 19-28.

[2] GrandViewResearch, “2022 cyber security market size, share & trends analysis report by component, by security type, by solution, by services, by deployment, by organization size, by applications, by region, and segment forecasts, 2023 – 2030,” *Report*, Dec. 2022.

[3] Z. Tang, A. S. Miller, Z. Zhou, and M. Warkentin, “Does government social media promote users’ information security behavior towards COVID-19 scams? Cultivation effects and protective motivations,” *Government Information Quarterly*, vol. 38, no. 2, 2021, pp. 101572.

[4] I. Hwang, “The effect on the IS role stress on the IS compliance intention through IS self-determination: Focusing on the moderation of person-organization fit,” *J. of the Korea Institute of Electronic Communication Sciences*, vol. 17, no. 2, 2022, pp. 375-386.

[5] Verizon, “2021 data breach investigations report,” *Report,* Dec. 2021.

[6] C. Liu, H. Liang, N. Wang, and Y. Xue, “Ensuring employees’ information security policy compliance by carrot and stick: The moderating

roles of organizational commitment and gender," *Information Technology & People*, vol. 35, no. 2, 2021, pp. 802-834.

[7] M. I. Merhi and P. Ahluwalia, "Examining the impact of deterrence factors and norms on resistance to information systems security," *Computers in Human Behavior*, vol. 92, 2019, pp. 37-46.

[8] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness," *MIS Quarterly*, vol. 34, no. 3, 2010, pp. 523-548.

[9] T. Herath and H. R. Rao, "Protection motivation and deterrence: A framework for security policy compliance in organisations," *European J. of Information Systems*, vol. 18, 2009, pp. 106-125.

[10] S. Hong and J. Park, "Effective management of personal information & information security management system(ISMS-P) authentication systems," *J. of the Korea Academia-Industrial Cooperation Society*, vol. 21, no. 1, 2020, pp. 634-640.

[11] Nettgov, "Biden administration releases draft zero-trust guidance," *Report*, Sept. 2021.

[12] J. D'Arcy and P. L. Teh, "Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization," *Information & Management*, vol. 56, no. 7, 2019, pp. 103151.

[13] Y. Chen, K. Ramamurthy, and K. W. Wen, "Organizations' information security policy compliance: Stick or carrot approach?," *J. of Management Information Systems*, vol. 29, no. 3, 2012, pp. 157-188.

[14] H. Li, R. Sarathy, J. Zhang, and X. Luo, "Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance," *Information Systems J.*, vol. 24, no. 6, 2014, pp. 479-502.

[15] K. A. Alshare, P. L. Lane, and M. R. Lane, "Information security policy compliance: A higher education case study," *Information & Computer Security*, vol. 26 no. 1, 2018, pp. 91-108.

[16] W. Lee and I. Hwang, "Sustainable information security behavior management: An empirical approach for the causes of employees' voice behavior," *Sustainability*, vol. 13, no. 11, 2021, pp. 6077.

[17] H. Zhang and N. C. Agarwal, "The mediating roles of organizational justice on the relationships between HR practices and workplace outcomes: An investigation in China," *The Int. J. of Human Resource Management*, vol. 20, no. 3, 2009, pp. 676-693.

[18] T. A. Judge and J. A. Colquitt, "Organizational justice and stress: The mediating role of work-family conflict," *J. of Applied Psychology*, vol. 89, no. 3, 2004, pp. 395-404.

[19] I. Hwang, "Reinforcement of IS voice behavior within the organization: A perspective on mitigating role stress through organization justice and individual social-identity," *J. of the Korea Institute of Electronic Communication Sciences*, vol. 17, no. 4, 2022, pp. 649-662.

[20] M. L. Ambrose and M. Schminke, "The role of overall justice judgments in organizational justice research: A test of mediation," *J. of Applied Psychology*, vol. 94, no. 2, 2009, pp. 491-500.

[21] J. Son, "Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies," *Information & Management*, vol. 48, no. 7, 2011, pp. 296-302.

[22] K. H. Guo, Y. Yuan, N. P. Archer, and C. E. Connelly, "Understanding nonmalicious security violations in the workplace: A composite behavior model," *J. of Management Information Systems*, vol. 28, no. 2, 2011, pp. 203-236.

[23] Y. Xue, H. Liang, and L. Wu, "Punishment, justice, and compliance in mandatory IT settings," *Information Systems Research*, vol. 22, no. 2, 2011, pp. 400-414.

[24] L. Jaeger and A. Eckhardt, "Eyes wide open: The role of situational information security awareness for security related behaviour," *Information Systems J.*, vol. 31, no. 3, 2021, pp. 429-472.

[25] L. Li, W. He, L. Xu, I. Ash, M. Anwar, and X. Yuan, "Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior," *Int. J. of Information Management*, vol. 45, 2019, pp. 13-24.

[26] J. D'Arcy, T. Herath, and M. K. Shoss, "Understanding employee responses to stressful information security requirements: A coping perspective," *J. of Management Information Systems*, vol. 31, no. 2, 2014, pp. 285-318.

[27] R. Cropanzano, L. Paddock, D. E. Rupp, J. Bagger, and A. Baldwin, "How regulatory focus impacts the process-by-outcome interaction for perceived fairness and emotions," *Organizational Behavior and Human Decision Processes*, vol. 105, no. 1, 2008, pp. 36-51.

[28] M. Schmitt, M. Gollwitzer, J. Maes, and D. Arbach, "Justice sensitivity," *European J. of Psychological Assessment*, vol. 21, no. 3, 2005, pp. 202-211.

[29] M. Gollwitzer, T. Rothmund, A. Pfeiffer, and C. Ensenbach, "Why and when justice sensitivity leads to pro-and antisocial behavior," *J. of Research in Personality*, vol. 43, no. 6, 2009, pp. 999-1005.

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

[31] C. Fornell and D. F. Larcker, "Evaluating structural equation models with unobservable variables and measurement error," *J. of Marketing Research*, vol. 18, no. 1, 1981, pp. 39-50.

[32] A. F. Hayes, *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach*. New York: Guilford Publications, 2017.

저자 소개

황인호(In-Ho Hwang)

2007년 중앙대학교 대학원 졸업 (경영학석사)
2014년 중앙대학교 대학원 졸업 졸업(경영학 박사)
2018년 한국공학대학교 연구교수
2020년 ~현재 국민대학교 교양대학 조교수
※ 관심분야 : IT 핵심성공요인(IT CSF), 디지털 콘텐츠(Digital Content), 정보보안(Information Security), 프라이버시(Privacy) 등